



Red Hat Virtualization 4.2

管理ガイド

Red Hat Virtualization の管理タスク

Red Hat Virtualization 4.2 管理ガイド

Red Hat Virtualization の管理タスク

Red Hat Virtualization Documentation Team
Red Hat Customer Content Services
rhev-docs@redhat.com

法律上の通知

Copyright © 2018 Red Hat, Inc.

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

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

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

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

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, 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 Software Collections 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

本ガイドには、Red Hat Virtualization の管理者に役立つ情報と手順を記載しています。

目次

パート I. RED HAT VIRTUALIZATION 環境の管理とメンテナンス	6
第1章 グローバルの設定	7
1.1. ロール	7
1.2. システムパーミッション	10
1.3. スケジューリングポリシー	22
1.4. インスタンスのタイプ	28
1.5. MAC アドレスプール	30
第2章 ダッシュボード	33
2.1. 前提条件	33
2.2. グローバルインベントリー	33
2.3. システム全体の使用状況	35
2.4. クラスター使用率	36
2.5. ストレージ使用率	37
パート II. リソースの管理	38
第3章 QOS (QUALITY OF SERVICE)	39
3.1. ストレージの QOS	39
3.2. 仮想マシンネットワークの QOS	40
3.3. ホストネットワークの QOS	42
3.4. CPU の QOS	43
第4章 データセンター	45
4.1. データセンターについて	45
4.2. STORAGE POOL MANAGER	46
4.3. SPM の優先度	46
4.4. データセンターのタスク	46
4.5. データセンターとストレージドメイン	50
第5章 クラスター	54
5.1. クラスターについて	54
5.2. クラスターのタスク	54
第6章 論理ネットワーク	76
6.1. 論理ネットワークのタスク	76
6.2. 仮想ネットワークインターフェースカード	84
6.3. 外部プロバイダーネットワーク	91
6.4. ホストとネットワーク	93
第7章 ホスト	106
7.1. ホストについて	106
7.2. RED HAT VIRTUALIZATION HOST	107
7.3. RED HAT ENTERPRISE LINUX ホスト	107
7.4. SATELLITE ホストプロバイダーのホスト	108
7.5. ホストのタスク	108
7.6. ホストの耐障害性	128
第8章 ストレージ	138
8.1. ストレージドメインについての知識	139
8.2. NFS ストレージの準備と追加	139
8.3. ローカルストレージの準備と追加	142
8.4. POSIX 準拠ファイルシステムストレージの追加	143

8.5. ブロックストレージの追加	144
8.6. 既存のストレージドメインのインポート	150
8.7. ストレージのタスク	155
第9章 プール	164
9.1. 仮想マシンプールについて	164
9.2. 仮想マシンプールの作成	164
9.3. 新規プールおよびプールの編集ウィンドウの設定とコントロール	168
9.4. 仮想マシンプールの編集	176
9.5. プール内の仮想マシンの事前起動	176
9.6. 仮想マシンプールへの仮想マシン追加	177
9.7. 仮想マシンプールからの仮想マシンのデタッチ	177
9.8. 仮想マシンプールの削除	177
9.9. 信頼済みコンピュートプール	178
第10章 仮想ディスク	181
10.1. 仮想マシンストレージについての知識	181
10.2. 仮想ディスクについての知識	181
10.3. 削除後に仮想ディスクをワイプする設定	183
10.4. RED HAT VIRTUALIZATION の共有可能ディスク	184
10.5. RED HAT VIRTUALIZATION における読み取り専用ディスク	184
10.6. 仮想ディスクのタスク	185
第11章 外部プロバイダー	200
11.1. RED HAT VIRTUALIZATION の外部プロバイダーについて	200
11.2. 外部プロバイダーの追加	201
11.3. 外部プロバイダーの編集	223
11.4. 外部プロバイダーの削除	223
パート III. 環境の管理	224
第12章 バックアップと移行	225
12.1. RED HAT VIRTUALIZATION MANAGER のバックアップと復元	225
12.2. バックアップ/リストア API を使用した仮想マシンのバックアップと復元	232
第13章 RED HAT SATELLITE によるエラータ管理	236
第14章 ANSIBLE を使用した設定作業の自動化	238
14.1. ANSIBLE ロール	238
第15章 ユーザーとロール	241
15.1. ユーザーについて	241
15.2. ディレクトリーサーバーの概要	241
15.3. 外部の LDAP プロバイダーの設定	242
15.4. シングルサインオンのための LDAP と KERBEROS の設定	254
15.5. ユーザー認証	259
15.6. 管理ポータルからのユーザー管理タスク	260
15.7. コマンドラインからのユーザー管理タスク	261
15.8. 追加のローカルドメインの設定	266
第16章 クォータと SERVICE LEVEL AGREEMENT のポリシー	268
16.1. クォータについて	268
16.2. 共有クォータおよび個別に定義されたクォータ	269
16.3. クォータアカウンティング	269
16.4. データセンターのクォータの有効化/モードの変更	270
16.5. 新規クォータポリシーの作成	270

16.6. クォータの閾値設定	271
16.7. オブジェクトへのクォータ割り当て	272
16.8. クォータを使用したユーザー別のリソース制限	272
16.9. クォータの編集	273
16.10. クォータの削除	273
16.11. SERVICE LEVEL AGREEMENT ポリシーの有効化	273
第17章 イベント通知	275
17.1. 管理ポータルでのイベント通知の設定	275
17.2. 管理ポータルでのイベント通知のキャンセル	276
17.3. OVIRT-ENGINE-NOTIFIER.CONF 内のイベント通知パラメーター	277
17.4. RED HAT VIRTUALIZATION MANAGER が SNMP トラップを送信するための設定	281
第18章 ユーティリティー	284
18.1. OVIRT-ENGINE-RENAME ツール	284
18.2. ENGINE 設定ツール	286
18.3. USB FILTER EDITOR	287
18.4. ログ収集ツール	291
18.5. ISO アップローダーツール	294
18.6. ENGINE-VACUUM ツール	297
パート IV. 環境に関する情報の収集	300
第19章 ログファイル	301
19.1. MANAGER インストールのログファイル	301
19.2. RED HAT VIRTUALIZATION MANAGER のログファイル	301
19.3. SPICE のログファイル	302
19.4. ホストのログファイル	304
19.5. ホストのロギングサーバーの設定	304
第20章 プロキシ	306
20.1. SPICE プロキシ	306
20.2. SQUID プロキシ	308
20.3. WEBSOCKET プロキシ	310
付録A VDSM とフック	312
A.1. VDSM	312
A.2. VDSM フック	312
A.3. フックを使用したVDSM の拡張	312
A.4. サポートされている VDSM イベント	312
A.5. VDSM フックの環境	315
A.6. VDSM フックドメインの XML オブジェクト	315
A.7. カスタムプロパティの定義	315
A.8. 仮想マシンのカスタムプロパティの設定	317
A.9. VDSM フックの仮想マシンカスタムプロパティの評価	317
A.10. VDSM フッキングモジュールの使用方法	318
A.11. VDSM フックの実行	318
A.12. VDSM フックのリターンコード	319
A.13. VDSM フックの例	320
付録B カスタムのネットワークプロパティ	322
B.1. BRIDGE_OPTS パラメーター	322
B.2. RED HAT VIRTUALIZATION MANAGER で ETHTOOL を使用するための設定方法	324
B.3. RED HAT VIRTUALIZATION MANAGER で FCOE を使用するための設定方法	325

付録C RED HAT VIRTUALIZATION のユーザーインターフェースプラグイン	327
C.1. RED HAT VIRTUALIZATION のユーザーインターフェースプラグイン	327
C.2. RED HAT VIRTUALIZATION ユーザーインターフェースプラグインのライフサイクル	327
C.3. ユーザーインターフェースプラグイン関連のファイルおよびその場所	329
C.4. ユーザーインターフェースプラグインのデプロイメント例	329
付録D RED HAT VIRTUALIZATION と SSL	331
D.1. RED HAT VIRTUALIZATION MANAGER の SSL/TLS 証明書の変更	331
D.2. MANAGER と LDAP サーバー間の SSL または TLS 接続の設定	333
付録E ブランディング	335
E.1. ブランディング	335
付録F システムアカウント	338
F.1. システムアカウント	338

パート I. RED HAT VIRTUALIZATION 環境の管理とメンテナンス

Red Hat Virtualization 環境を継続的に稼働させ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/仮想リソースの管理。これには、ホストのアップグレードや追加、ドメインのインポート、異種のハイパーバイザーで作成された仮想マシンの変換、仮想マシンプールのメンテナンスなどが含まれます。
- 1 台のホストに対する過度の負荷やメモリー/ディスク容量の不足などの潜在的な問題を特定するために、システムリソース全体のモニタリングと必要措置を実施する (例: 仮想マシンを別のホストに移行して負荷を軽減したり、マシンをシャットダウンしてリソースを解放したりするなど)。
- 仮想マシンの新規要件への対応 (例: オペレーティングシステムのアップグレード、追加メモリー割り当てなど)。
- タグを使用してカスタマイズしたオブジェクトプロパティの管理
- 公開ブックマークとして保存した検索の管理
- ユーザー設定の管理やパーミッションレベルの設定
- 特定のユーザー、仮想マシン、またはシステム全体の機能のトラブルシューティング
- 一般レポートおよび明細レポートの生成

第1章 グローバルの設定

管理ポータルの **管理** → **設定** をクリックして **設定** ウィンドウを開くと、ユーザー、ロール、システム権限、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 環境のさまざまなグローバルリソースを設定することができます。このウィンドウで、ユーザーが環境内のリソースと対話する方法をカスタマイズすることが可能です。また、複数のクラスターに適用できるオプションを一元的に設定することができます。

1.1. ロール

ロールとは、Red Hat Virtualization Manager から設定することが可能な、事前定義済みの権限セットです。ロールは、データセンター内の異なるレベルのリソース、特定の物理/仮想リソースに対するアクセスと管理のパーミッションを提供します。

マルチレベルの管理では、コンテナオブジェクトに適用されるパーミッションは、そのコンテナ内の個々のオブジェクトすべてに適用されます。たとえば、特定のホストを対象とするホスト管理者ロールがユーザーに割り当てられると、そのユーザーには、使用できるすべてのホスト操作を実行するパーミッションが付与されますが、その対象は割り当てられたホストに限定されます。一方、データセンターを対象とするホスト管理者ロールが割り当てられると、そのユーザーには、データセンターのクラスター内の全ホストに対してホスト操作を実行するパーミッションが付与されます。

1.1.1. 新規ロールの作成

必要とするロールが Red Hat Virtualization のデフォルトロール一覧にない場合には、新規ロールを作成し、目的に応じてカスタマイズすることができます。

新規ロールの作成

1. **管理** → **設定** をクリックすると **設定** ウィンドウが開きます。デフォルトでは **ロール** タブが選択され、デフォルトのユーザー/管理者ロールとカスタムロールの一覧が表示されます。
2. **新規作成** をクリックします。
3. 新規ロールの **名前** と **説明** を入力します。
4. **アカウントタイプ** に **管理者** または **ユーザー** のいずれかを選択します。
5. **操作を許可するチェックボックス** の一覧に表示されているオブジェクトに対するパーミッションは、**すべてを展開** または **すべてを折りたたむ** ボタンを使用して表示を展開または折りたたむことができます。また、オブジェクト別にオプションを展開または折りたたむことも可能です。
6. オブジェクト別に、設定中のロールで許可するアクションにはチェックを入れ、許可しないアクションからはチェックを外します。
7. **OK** をクリックして、変更を適用します。ロールの一覧に新規ロールが表示されます。

1.1.2. ロールの編集とコピー

自分で作成したロールの設定は変更することができますが、デフォルトのロールは変更できません。デフォルトのロールを変更するには、そのデフォルトのロールをコピーしてから、コピーしたロールを要件に応じて変更してください。

ロールの編集とコピー

1. **管理** → **設定** をクリックすると **設定** ウィンドウが開きます。このウィンドウには、デフォルトのユーザー/管理者ロールとカスタムロールの一覧が表示されます。
2. 変更するロールを選択し、**編集** をクリックすると **ロールの編集** ウィンドウが開きます。また、**コピー** をクリックすると、**ロールのコピー** ウィンドウが開きます。
3. 必要な場合には、ロールの **名前** と **説明** を編集します。
4. 一覧表示されているオブジェクトに対するパーミッションは、**すべてを展開** または **すべてを折りたたむ** ボタンを使用して表示を展開または折り畳むことができます。また、オブジェクト別にオプションを展開または折り畳むことも可能です。
5. オブジェクト別に、編集時のロールで許可するアクションにはチェックを入れ、許可しないアクションからはチェックを外します。
6. **OK** をクリックして、変更を適用します。

1.1.3. ユーザーロールと認証の例

以下の例では、本章で説明する認証システムの多様な機能を使用して、さまざまなシナリオで認証管理を適用する方法について説明します。

例1.1 クラスターのパーミッション

Sarah は、ある企業の経理部門のシステム管理者です。この部門の全仮想リソースは、**Accounts** という名前の Red Hat Virtualization **クラスター** にまとめられています。Sarah は、このクラスターの **ClusterAdmin** ロールを割り当てられました。仮想マシンはクラスターの子オブジェクトであるため、クラスター内の全仮想マシンを管理できるようになります。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/削除や、スナップショットの作成などが含まれますが、このクラスター外のリソースは一切管理できません。**ClusterAdmin** は管理者ロールなので、管理ポータルまたは VM ユーザーポータルを使用してこれらのリソースを管理できます。

例1.2 VM PowerUser のパーミッション

John は経理部門のソフトウェア開発者です。仮想マシンを使用してソフトウェアの構築やテストを行います。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** 仮想マシンに対する **UserVmManager** ロールが割り当てられました。これによって、John は、VM ユーザーポータルを使用してこの 1 台の仮想マシンにアクセスすることができます。**UserVmManager** のパーミッションがあるので、仮想マシンの設定を変更することができます。**UserVmManager** はユーザーロールであるため、管理ポータルは使用できません。

例1.3 データセンターパワーユーザーロールのパーミッション

Penelope はオフィスマネージャーです。自分の責務以外に、人事部マネージャーの人事関連の業務を手伝って、面接の日取りを決めたり、身元照会の追跡調査を行ったりすることもあります。Penelope がこのような人事関連の業務を行う際には、会社の方針に従って、特定のアプリケーションを使用する必要があります。

Penelope にはオフィス管理業務用に自分のマシンがありますが、人事関連のアプリケーションを実行するためにもう 1 台別のマシンを必要としています。Penelope には、新たに提供されるマシンが属するデータセンターに対する **PowerUserRole** パーミッションが割り当てられました。新規仮想マシンを作成するには、ストレージドメイン内での仮想ディスク作成など、そのデータセンター内のいくつか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、**DataCenterAdmin** の権限を Penelope に割り当てるのとは異なる点に注意してください。Penelope はデータセンターの PowerUser として VM ユーザーポータルにログインし、そのデータセンター内の仮想マシンに対して仮想マシン固有のアクションを実行することができますが、データセンターへのホストやストレージのアタッチなど、データセンターレベルの操作は実行できません。

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として勤めています。日常業務には、その IT 部門の Red Hat Virtualization 環境内にあるネットワークの作成/操作/削除などが含まれます。Chris の役割には、リソースおよび各リソースのネットワークに対する管理者の権限が必要です。たとえば、IT 部門のデータセンターに対する **NetworkAdmin** の権限があると、そのデータセンター内でのネットワークの追加/削除や、そのデータセンターに属する全仮想マシン用のネットワークのアタッチ/デタッチが可能です。

例1.5 カスタムロールのパーミッション

Rachel は、IT 部門に勤めており、Red Hat Virtualization 内のユーザーアカウントを管理する責務を担っています。Rachel には、ユーザーアカウントを追加して、適切なロールとパーミッションを割り当てるためのパーミッションが必要です。自分では仮想マシンは使用しておらず、ホスト、仮想マシン、クラスター、データセンターの管理アクセスは必要はありません。このような特定のパーミッションセットを提供する既成のロールはありません。Rachel の立場に適したパーミッションセットを定義するには、カスタムロールを作成する必要があります。

図1.1 UserManager のカスタムロール

New Role

Name: Description:

Account Type:
☐ User ☒ Admin

Check Boxes to Allow Action

▼ ☐ System

▼ ☐ Configure System

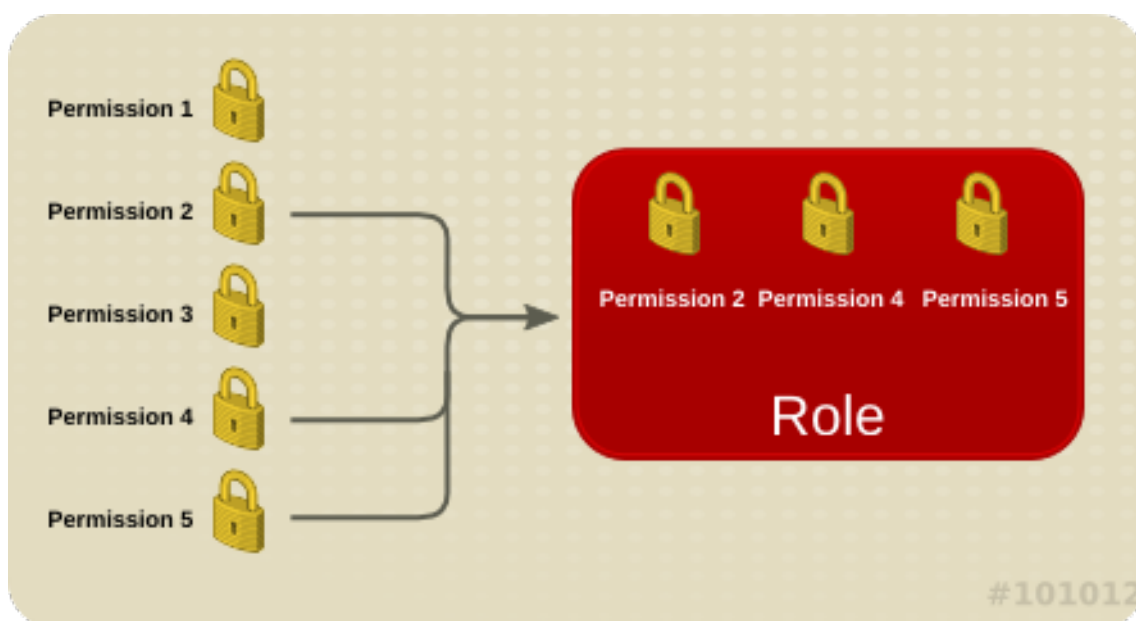
- ☒ Manipulate Users
- ☒ Manipulate Permissions
- ☐ Add users and groups from directory while adding permissions
- ☒ Manipulate Roles
- ☐ Login Permissions
- ☐ Tag management Permissions
- ☐ Bookmark management Permissions

上記に示した **UserManager** カスタムロールでは、ユーザー、パーミッション、ロールの操作ができます。これらの操作は、[図1.3「Red Hat Virtualization のオブジェクト階層」](#)に示した階層の最上位のオブジェクトである **システム** 下にまとめられており、システム内のその他すべてのオブジェクトに適用されることになります。ロールには、**管理者** の **アカウントタイプ** が指定されています。これにより、Rachel がこのロールを割り当てられると、管理ポータルと VM ユーザーポータルの両方を使用できます。

1.2. システムパーミッション

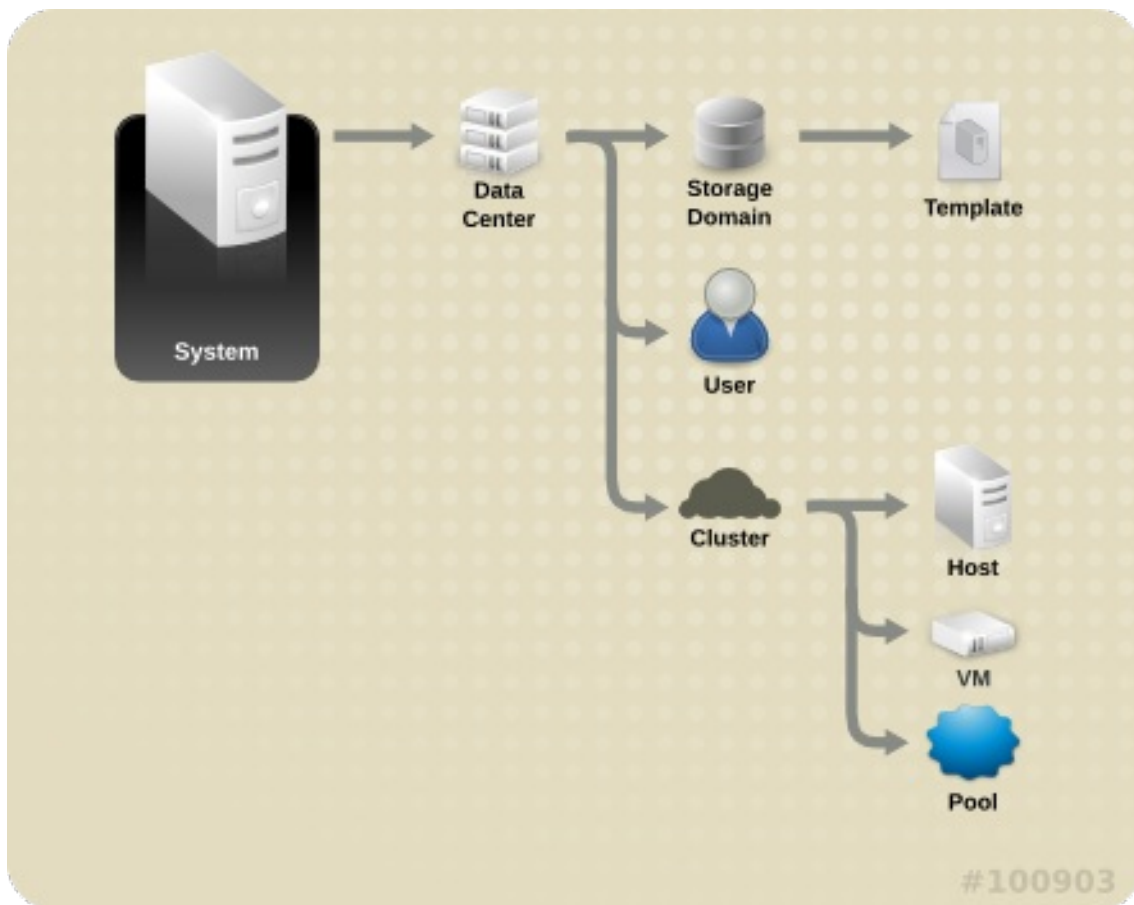
パーミッションによりユーザーは、オブジェクトに対するアクションを実行することができます。アクションの対象となるオブジェクトは、個別のオブジェクトもしくはコンテナオブジェクトです。

図1.2 パーミッション & ロール



コンテナオブジェクトに適用されるパーミッションは、そのコンテナの全メンバーに対しても適用されます。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1.3 Red Hat Virtualization のオブジェクト階層



1.2.1. ユーザーのプロパティ

ロールとパーミッションは、ユーザーのプロパティです。ロールは、さまざまなレベルの物理/仮想リソースへのアクセスを可能にする事前定義された一連の権限です。マルチレベルの管理により、粒度の細かいパーミッション階層が提供されます。たとえば、データセンター管理者には、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がある一方、ホスト管理者には、単一の物理ホストに対するシステム管理者のパーミッションがあります。また、あるユーザーには、仮想マシンを使用することができるが、その仮想マシンの設定変更はできないパーミッションを割り当てることができる一方、別のユーザーに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. ユーザーロールと管理者ロール

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単一の仮想マシンへのアクセス権限を持つエンドユーザーまで、さまざまな事前設定済みロールを提供しています。デフォルトのロールは、変更/削除することはできませんが、必要に応じてクローン作成、カスタマイズ、または新規作成することができます。ロールには2つのタイプがあります。

- **管理者ロール:** **管理ポータル** を使用して物理/仮想リソースを管理できます。管理者ロールにより、VM ユーザーポータルで操作を行うためのパーミッションも付与されますが、このパーミッションは VM ユーザーポータルでユーザーに表示される内容とは関係ありません。
- **ユーザーロール:** **VM ユーザーポータル** を使用して仮想マシンやテンプレートの管理とアクセスができます。ユーザーロールにより、VM ユーザーポータルでそのユーザーに表示される項目が決定します。管理者ロールが設定されたユーザーに付与されるパーミッションは、VM ユーザーポータルでそのユーザーが行うことができる操作に反映されます。

1.2.3. ユーザーロール

以下の表には、VM ユーザーポータルで仮想マシンへのアクセスと設定を行うための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の説明をまとめています。

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

ロール	権限	備考
UserRole	仮想マシンとプールにアクセスして使用することができます。	VM ユーザーポータルにログインし、割り当てられた仮想マシンとプールを使用したり、仮想マシンのステータスや詳細情報を確認したりすることができます。
PowerUserRole	仮想マシンとテンプレートの作成および管理ができます。	このロールをユーザーに適用するには、 設定 ウィンドウを使用して環境全体で設定するか、特定のデータセンターまたはクラスターで設定します。たとえば、PowerUserRole がデータセンターレベルで適用されると、PowerUser はそのデータセンター内で仮想マシンおよびテンプレートの作成ができます。
UserVmManager	仮想マシンのシステム管理者	仮想マシンの管理およびスナップショットの作成と使用ができます。VM ユーザーポータル内で仮想マシンを作成したユーザーには、そのマシンに対する UserVmManager ロールが自動的に割り当てられます。

以下の表には、上級のユーザーロールについての説明をまとめています。これらのロールにより、VM ユーザーポータルでリソースに対するパーミッションを細かく設定することができます。

表1.2 Red Hat Virtualization ユーザーロール (上級)

ロール	権限	備考
UserTemplateBasedVm	テンプレートのみを使用できる制限付き権限	テンプレートを使用して仮想マシンを作成することができます。
DiskOperator	仮想ディスクのユーザー	仮想ディスクの使用/表示/編集ができます。仮想ディスクがアタッチされた仮想マシンを使用するためのパーミッションを継承します。

ロール	権限	備考
VmCreator	VM ユーザーポータルで仮想マシンを作成することができます。	このロールは特定の仮想マシンに適用するのではなく、 設定 ウィンドウを使用して環境全体でユーザーに適用するか、特定のデータセンターまたはクラスターで適用します。クラスターにこのロールを適用する場合は、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対して DiskCreator ロールも適用する必要があります。
TemplateCreator	割り当てられたリソース内で仮想マシンのテンプレートの作成/編集/管理/削除ができます。	このロールは特定のテンプレートに適用するのではなく、 設定 ウィンドウを使用して環境全体でユーザーに適用するか、特定のデータセンター、クラスター、ストレージドメインに適用します。
DiskCreator	割り当てられたクラスターまたはデータセンター内で仮想ディスクの作成/編集/管理/削除ができます。	このロールは特定の仮想ディスクに適用するのではなく、 設定 ウィンドウを使用して環境全体でユーザーに適用するか、特定のデータセンターまたはストレージドメインに適用します。
TemplateOwner	テンプレートの編集や削除、またテンプレートのユーザーパーミッションの割り当てや管理ができます。	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。テンプレートに対する TemplateOwner パーミッションのないその他のユーザーは、その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ースのユーザー	特定の論理ネットワークにネットワークインターフェースをアタッチ/デタッチできます。

1.2.4. 管理者ロール

以下の表には、管理ポータルでリソースにアクセスして設定を行うためのパーミッションを付与する基本的な管理者ロールについての説明をまとめています。

表1.3 Red Hat Virtualization のシステム管理者ロール (基本)

ロール	権限	備考
-----	----	----

ロール	権限	備考
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に対する完全なパーミッションがあり、全データセンターの全オブジェクトを管理できます。
ClusterAdmin	クラスターの管理者	特定のクラスター下の全オブジェクトに対する管理者パーミッションがあります。
DataCenterAdmin	データセンターの管理者	ストレージを除く特定のデータセンター下の全オブジェクトに対する管理者パーミッションがあります。



重要

ディレクトリーサーバーの管理ユーザーは Red Hat Virtualization の管理ユーザーとしては使用せずに、Red Hat Virtualization の管理ユーザーとして専用使用するユーザーを作成してください。

以下の表には、上級の管理者ロールについての説明をまとめています。これらのロールにより、管理ポータルでリソースに対するパーミッションを細かく設定することができます。

表1.4 Red Hat Virtualization のシステム管理者ロール (上級)

ロール	権限	備考
TemplateAdmin	仮想マシンテンプレートの管理者	ストレージドメインやテンプレートのネットワーク詳細の作成/削除/設定やドメイン間のテンプレートの移動ができます。
StorageAdmin	ストレージの管理者	割り当て済みのストレージドメインを作成/削除/設定/管理できます。
HostAdmin	ホストの管理者	特定のホストをアタッチ/削除/設定/管理できます。
NetworkAdmin	ネットワークの管理者	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の設定と管理ができます。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に対するネットワークパーミッションも継承します。

ロール	権限	備考
VmPoolAdmin	仮想プールのシステム管理者	仮想プールの作成/削除/設定、仮想プールユーザーの割り当て/削除、およびプール内の仮想マシンに対する基本操作ができます。
GlusterAdmin	Gluster ストレージの管理者	Gluster ストレージボリュームを作成、削除、設定、管理することができます。
VmImporterExporter	仮想マシンのインポート/エクスポートに関する管理者	仮想マシンのインポートとエクスポートを実行することが可能です。また、他のユーザーによってエクスポートされた仮想マシンとテンプレートをすべて表示することができます。

1.2.5. リソースに対する管理者およびユーザーロールの割り当て

リソースに対して管理者またはユーザーのロールを割り当てると、ユーザーはそのリソースへのアクセスや管理ができるようになります。

リソースへのロール割り当て

1. リソースを特定し、その名前をクリックして詳細ビューを表示します。
2. **パーミッション** タブをクリックして、選択したリソースに割り当てられたユーザー、ユーザーのロール、継承されたパーミッションを一覧表示します。
3. **追加** をクリックします。
4. **検索** 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、**検索** をクリックします。結果一覧に表示される検索候補からユーザーを選択します。
5. **割り当てるロール** 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。

ユーザーは、対象のリソースに対して有効化されたロールのパーミッションを継承します。

1.2.6. リソースからの管理者またはユーザーロールの削除

リソースから管理者またはユーザーのロールを削除すると、そのリソースのロールに関連付けられたユーザーのパーミッションは継承されなくなります。

リソースからのロールの削除

1. リソースを特定し、その名前をクリックして詳細ビューを表示します。
2. **パーミッション** タブをクリックして、選択したリソースに割り当てられたユーザー、ユーザーのロール、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. **削除** をクリックします。

5. **OK** をクリックします。

1.2.7. データセンターに対する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全側面を管理する管理者です。他のユーザーには、より特定の管理者ロールを割り当てることができます。このような制限付きの管理者ロールは、特定のリソースに限定した特定の管理者権限をユーザーに付与する場合に有用です。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対してのみ (ただし、そのデータセンター用のストレージは例外)、**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があります。

データセンター管理者は、特定のデータセンターのみを対象とするシステム管理者ロールです。これは、複数のデータセンターがある仮想化環境で、各データセンターに管理者が必要な場合に有用です。**DataCenterAdmin** ロールは階層モデルで、特定のデータセンターを対象とする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内のストレージを除く全オブジェクトを管理することができます。仮想化環境内の全データセンターにデータセンター管理者を割り当てるには、ヘッダーバーの **設定** ボタンを使用してください。

データセンター管理者ロールは、以下のアクションを許可します。

- データセンターに関連付けられたクラスターの作成/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、プールの作成/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

ロールとパーミッションは、既存のユーザーにしか割り当てることができません。

また、既存のシステム管理者を削除して、新規システム管理者を追加することによって、データセンターのシステム管理者を変更することができます。

1.2.8. データセンター管理者ロール

データセンターに対するパーミッションがあるロール

以下の表には、データセンターの管理に適用可能な管理者のロールと権限についての説明をまとめています。

表1.5 Red Hat Virtualization のシステム管理者ロール

ロール	権限	備考
DataCenterAdmin	データセンター管理者	ストレージを除く、特定のデータセンター内の全物理/仮想リソース (クラスター、ホスト、テンプレート、仮想マシンを含む) を使用、作成、削除、管理することができます。

ロール	権限	備考
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、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に対するネットワークパーミッションも継承します。

1.2.9. クラスターに対する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を全側面を管理する管理者です。他のユーザーには、より特定の管理者ロールを割り当てることができます。このような制限付きの管理者ロールは、特定のリソースに限定した特定の管理者権限をユーザーに付与する場合に有用です。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対してのみ (ただし、そのデータセンター用のストレージは例外)、**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があります。

クラスター管理者は、特定のクラスターのみを対象とするシステム管理者ロールです。これは、複数のクラスターがあるデータセンターで、各クラスターにシステム管理者が必要な場合に有用です。**ClusterAdmin** ロールは階層モデルで、特定のクラスターを対象とするクラスター管理者ロールを割り当てられたユーザーは、そのクラスター内の全オブジェクトを管理することができます。環境内の全クラスターにクラスター管理者を割り当てするには、ヘッダーバーの **設定** ボタンを使用してください。

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/削除
- クラスターに関連付けられたホスト、仮想マシン、プールの作成/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ミッションの編集



注記

ロールとパーミッションは、既存のユーザーにしか割り当てることができません。

また、既存のシステム管理者を削除して、新規システム管理者を追加することによって、クラスターのシステム管理者を変更することもできます。

1.2.10. クラスター管理者ロール

クラスターに対するパーミッションがあるロール

以下の表には、クラスターの管理に適用可能な管理者ロールと権限についての説明をまとめています。

表1.6 Red Hat Virtualization のシステム管理者ロール

ロール	権限	備考
ClusterAdmin	クラスター管理者	<p>特定のクラスター内の全物理/仮想リソース (ホスト、テンプレート、仮想マシンを含む) を使用、作成、削除、管理することができます。クラスター内のネットワークプロパティを設定することができます (ディスプレイネットワークの指定、ネットワークを必須または任意にマークするなど)。</p> <p>ただし、ClusterAdmin には、クラスターにネットワークをアタッチ/デタッチするパーミッションはありません。この操作を行うには、NetworkAdmin パーミッションが必要です。</p>
NetworkAdmin	ネットワーク管理者	<p>特定のクラスターのネットワークを設定、管理できます。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マシンに対するネットワークパーミッションも継承します。</p>

1.2.11. ネットワークに対する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全側面を管理する管理者です。他のユーザーには、より特定の管理者ロールを割り当てることができます。このような制限付きの管理者ロールは、特定のリソースに限定した特定の管理者権限をユーザーに付与する場合に有用です。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対してのみ (ただし、そのデータセンター用のストレージは例外)、**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があります。

ネットワーク管理者は、特定のネットワークに対して適用したり、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上の全ネットワークに対して適用したりすることが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、特定の仮想マシンやテンプレート上のネットワークの表示やアタッチなどの限定された管理ロールを実行することができます。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するには、ヘッダーバーの **設定** ボタンを使用してください。

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/削除
- ポートミラーリングの設定などのネットワーク設定の編集
- クラスターおよび仮想マシンを含むリソースへのネットワークのアタッチ/デタッチ

ネットワークを作成したユーザーには、作成したネットワークに対する **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て、新規管理者を追加することによって、ネットワークの管理者を変更することもできます。

1.2.12. ネットワーク管理者およびユーザーロール

ネットワークに対するパーミッションがあるロール

以下の表には、ネットワークの管理に適用可能な管理者とユーザーのロールと権限についての説明をまとめています。

表1.7 Red Hat Virtualization のネットワーク管理者/ユーザーロール

ロール	権限	備考
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したユーザーには、作成したネットワークに対する 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管理することができます。 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、そのネットワークに対する NetworkAdmin ロールと、仮想マシンに対する 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ースのユーザー	特定の論理ネットワークにネットワークインターフェースをアタッチ/デタッチできます。

1.2.13. ホストに対する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を全側面を管理する管理者です。他のユーザーには、より特定の管理者ロールを割り当てることができます。このような制限付きの管理者ロールは、特定のリソースに限定した特定の管理者権限をユーザーに付与する場合に有用です。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対してのみ（ただし、そのデータセンター用のストレージは例外）、**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があります。

ホスト管理者は、特定のホストのみを対象とするシステム管理者ロールです。これは、複数のホストで構成されるクラスターで、各ホストにシステム管理者が必要な場合に有用です。環境内の全ホストにホスト管理者を割り当てするには、ヘッダーバーの **設定** ボタンを使用してください。

ホスト管理者ロールは、以下のアクションを許可します。

- ホストの設定の編集
- 論理ネットワークの設定
- ホストの削除

既存のシステム管理者を削除して新規システム管理者を追加することにより、ホストのシステム管理者を変更することも可能です。

1.2.14. ホスト管理者ロール

ホストに対するパーミッションがあるロール

以下の表には、ホストの管理に適用可能な管理者のロールと権限についての説明をまとめています。

表1.8 Red Hat Virtualization のシステム管理者ロール

ロール	権限	備考
HostAdmin	ホスト管理者	特定のホストの設定、管理、削除ができます。また、特定のホストに対するネットワーク関連の操作を行うこともできます。

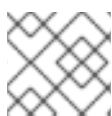
1.2.15. ストレージドメインに対するシステムパーミッションの管理

システム管理者は、**SuperUser** として管理ポータル全側面を管理する管理者です。他のユーザーには、より特定の管理者ロールを割り当てることができます。このような制限付きの管理者ロールは、特定のリソースに限定した特定の管理者権限をユーザーに付与する場合に有用です。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対してのみ (ただし、そのデータセンター用のストレージは例外)、**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があります。

ストレージ管理者は、特定のストレージドメインのみを対象とするシステム管理者ロールです。これは、複数のストレージドメインを使用するデータセンターで、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用です。環境内の全ストレージドメインにストレージ管理者を割り当てるには、ヘッダーバーの **設定** ボタンを使用してください。

ストレージ管理者ロールは、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

ロールとパーミッションは、既存のユーザーにしか割り当てることができません。

また、既存のシステム管理者を削除して、新規システム管理者を追加することによって、ストレージドメインのシステム管理者を変更することができます。

1.2.16. ストレージ管理者ロール

ストレージドメインに対するパーミッションがあるロール

以下の表には、ストレージドメインの管理に適用可能な管理者のロールと権限についての説明をまとめています。

表1.9 Red Hat Virtualization のシステム管理者ロール

ロール	権限	備考
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/管理できます。
GlusterAdmin	Gluster ストレージ管理者	Gluster ストレージボリュームを作成/削除/設定/管理できます。

1.2.17. 仮想マシンプールに対する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を全側面を管理する管理者です。他のユーザーには、より特定のな管理者ロールを割り当てることができます。このような制限付きの管理者ロールは、特定のリソースに限定した特定の管理者権限をユーザーに付与する場合に有用です。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対してのみ（ただし、そのデータセンター用のストレージは例外）、**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があります。

仮想マシンプール管理者は、データセンター内の仮想マシンプールの管理ロールです。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することができるので、異なるユーザーが特定の仮想マシンプールのリソースを管理する場合に有用です。

仮想マシンプール管理者ロールは、以下のアクションを許可します。

- プールの作成/編集/削除
- プールへの仮想マシン追加/プールからの仮想マシンのデタッチ



注記

ロールとパーミッションは、既存のユーザーにしか割り当てることができません。

1.2.18. 仮想マシンプールの管理者ロール

プールに対するパーミッションがあるロール

以下の表には、プールの管理に適用可能な管理者のロールと権限についての説明をまとめています。

表1.10 Red Hat Virtualization のシステム管理者ロール

ロール	権限	備考
VmPoolAdmin	仮想プールのシステム管理者ロール	仮想プールの作成/削除/設定、仮想プールユーザーの割り当て/削除、および仮想マシンに対する基本操作ができます。
ClusterAdmin	クラスター管理者	特定のクラスター内の全仮想マシンプールを作成、削除、管理することができます。

1.2.19. 仮想ディスクに対する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全側面を管理する管理者です。他のユーザーには、より特定のな管理者ロールを割り当てることができます。このような制限付きの管理者ロールは、特定のリソースに限定した特定の管理者権限をユーザーに付与する場合に有用です。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対してのみ (ただし、そのデータセンター用のストレージは例外)、**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があります。

Red Hat Virtualization Manager は、デフォルトの仮想ディスクユーザーロールを 2 タイプ提供していますが、デフォルトの仮想ディスク管理者ロールはありません。このユーザーロールの 1 つである **DiskCreator** ロールにより、VM ユーザーポータルから仮想ディスクの管理が行えるようになります。このロールは、特定の仮想マシン、データセンター、ストレージドメインだけでなく、仮想化環境全体に適用することができます。ユーザー別に異なる仮想リソースを管理できるようにするのに便利です。

仮想ディスクの作成者ロールは、以下のアクションを許可します。

- 仮想マシンや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/削除
- 仮想ディスクのユーザーパーミッションの編集



注記

ロールとパーミッションは、既存のユーザーにしか割り当てることができません。

1.2.20. 仮想ディスクユーザーロール

仮想ディスクに対するユーザーパーミッションがあるロール

以下の表には、VM ユーザーポータルで仮想ディスクを使用および管理するのに適用可能なユーザーロールや権限についての説明をまとめています。

表1.11 Red Hat Virtualization のシステム管理者ロール

ロール	権限	備考
DiskOperator	仮想ディスクのユーザー	仮想ディスクの使用/表示/編集ができます。仮想ディスクがアタッチされた仮想マシンを使用するための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で仮想ディスクの作成/編集/管理/削除ができます。	このロールは特定の仮想ディスクに適用するのではなく、 設定 ウィンドウを使用して環境全体でユーザーに適用するか、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適用します。

1.3. スケジューリングポリシー

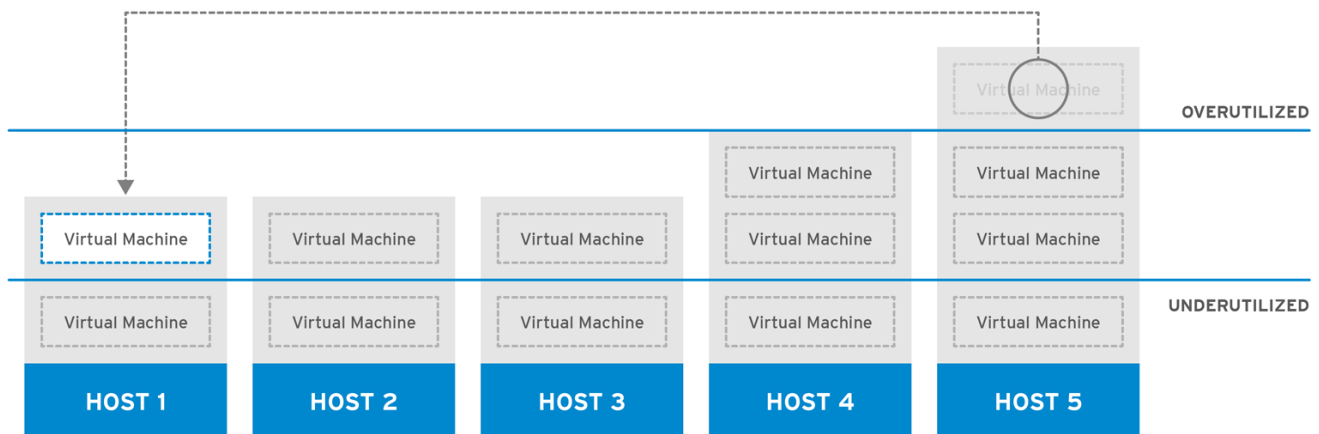
スケジューリングポリシーとは、そのスケジューリングポリシーが適用されるクラスター内のホスト間で仮想マシンを分散するロジックを定義する一式のルールです。スケジューリングポリシーは、フィルター、加重値、負荷分散ポリシーを組み合わせることでこのロジックを決定します。フィルターモジュールは

ハード強制を適用し、そのフィルターで指定した条件を満たさないホストを除外します。加重値モジュールはソフト強制を適用し、仮想マシンを実行することの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素の相対的な優先順位を制御するのに使用されます。

Red Hat Virtualization Manager はデフォルトで

evenly_distributed、**cluster_maintenance**、**none**、**power_saving**、および **vm_evenly_distributed** の5つのスケジューリングポリシーを提供しますが、より細かい粒度で仮想マシンの分散を制御することが可能な、新しいスケジューリングポリシーを定義することもできます。スケジューリングポリシーの設定にかかわらず、CPU が過負荷の状態にあるホストでは仮想マシンは起動しません。デフォルトでは、80% 以上の負荷が5分間続いた場合に、ホストのCPU が過負荷状態にあるとみなされます。ただし、これらの値はスケジューリングポリシーを使用して変更することができます。各スケジューリングポリシーのプロパティに関する詳細については、「[スケジューリングポリシーの設定](#)」を参照してください。

図1.4 均等分散スケジューリングポリシー



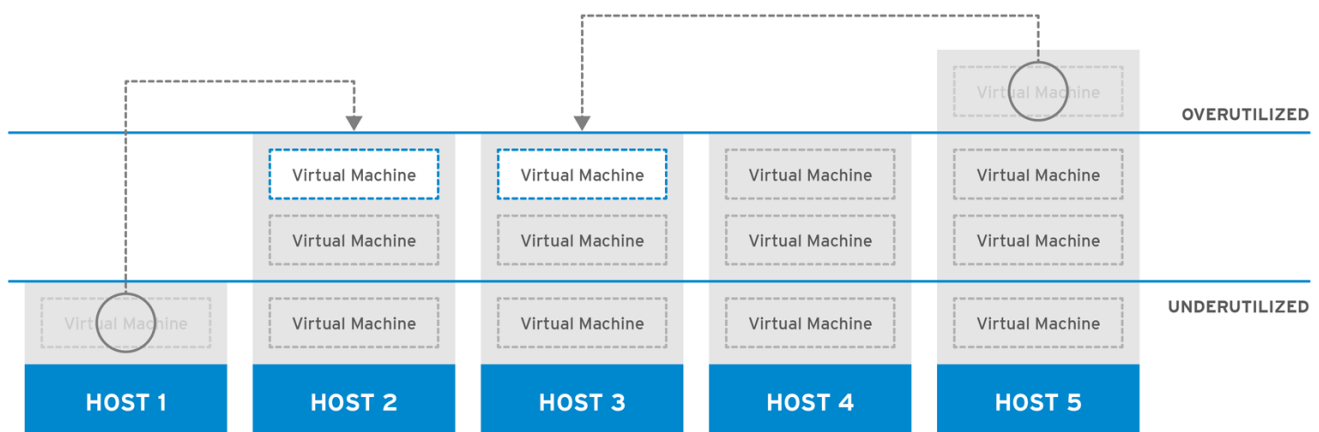
RHV_444396_0417

evenly_distributed スケジューリングポリシーでは、クラスター内の全ホストでメモリーおよび CPU 処理の負荷が均等に分散されます。ホストが定義された

CpuOverCommitDurationMinutes、**HighUtilization**、または **MaxFreeMemoryForOverUtilized** に達している場合には、仮想マシンをそのホストに追加でアタッチしてもそ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では、仮想マシンの数に基づいて仮想マシンがホスト間で均等に分散されます。**HighVmCount** を超える数の仮想マシンを実行しているホストがあり、かつ仮想マシンの数が **MigrationThreshold** から外れているホストが少なくとも1台ある場合に、そのクラスターはバランスが取れていない状態とみなされます。

図1.5 パワーセービング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では、使用可能なホストのサブセットでメモリーおよび CPU 処理の負荷を分散し、十分に活用されていないホストの電力消費を低減します。ホストの CPU 負荷が使用率の下限值以下の状態で所定の時間が経過すると、仮想マシンはすべて別のホストに移行され、電源をオフにできるようになります。ホストが定義された使用率の上限値に達している場合には、仮想マシンをそのホストに追加でアタッチしてもその仮想マシンは起動しません。

実行中の仮想マシンに関して、ホスト間で負荷の分散または電源の共有を行わない場合には、**none** ポリシーに設定します。これは、デフォルトのモードです。仮想マシンの起動時には、クラスター内のホスト間でメモリーと CPU 処理の負荷が均等に分散されます。ホストが定義された

CpuOverCommitDurationMinutes、**HighUtilization**、または **MaxFreeMemoryForOverUtilized** に達している場合には、仮想マシンをそのホストに追加でアタッチしてもその仮想マシンは起動しません。

cluster_maintenance スケジューリングポリシーでは、メンテナンス作業を実施中のクラスター内のアクティビティが制限されます。**cluster_maintenance** ポリシーが設定されると、高可用性の仮想マシンを除き新たな仮想マシンは起動しません。ホストで障害が発生すると、高可用性の仮想マシンは適切に再起動し、その他の仮想マシンも移行することができます。

1.3.1. スケジューリングポリシーの作成

新規スケジューリングポリシーを作成して、Red Hat Virtualization 環境内の特定のクラスターで仮想マシンを分散するロジックを制御することができます。

スケジューリングポリシーの作成

1. **管理** → **設定** をクリックします。
2. **スケジューリングポリシー** タブをクリックします。
3. **新規作成** をクリックします。
4. スケジューリングポリシーの **名前** と **説明** を入力します。
5. フィルターモジュールを設定します。
 - a. **フィルターモジュール** セクションで、スケジューリングポリシーに適用する対象のフィルターモジュールを **無効なフィルター** セクションから **有効なフィルター** セクションにドラッグアンドドロップします。
 - b. 基本的な最適化を行うために、特定のフィルターモジュールを **最初** に設定して優先順位を最も高くすることや、**最後** に設定して優先順位を最も低くすることも可能です。優先順位を設定するには、任意のフィルターモジュールを右クリックし、カーソルで **位置** をポイントして **最初** または **最後** を選択します。
6. 加重値モジュールを設定します。
 - a. **加重値モジュール** セクションで、スケジューリングポリシーに適用する対象の加重値モジュールを **無効な加重値** セクションから **有効な加重値と係数** セクションにドラッグアンドドロップします。
 - b. 有効な加重値モジュールの左側にある **+** または **-** ボタンを使用して、それらのモジュールの加重値を増減します。
7. 負荷分散ポリシーを指定します。
 - a. **ロードバランサー** セクションのドロップダウンメニューで、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. プロパティ セクションのドロップダウンメニューで、スケジューリングポリシーに適用する負荷分散のプロパティを選択し、そのプロパティの右側にあるテキストフィールドに値を指定します。

- c. + または - ボタンを使用して、プロパティを追加/削除します。

8. **OK** をクリックします。

1.3.2. 新規スケジューリングポリシーおよびスケジューリングポリシーの編集ウィンドウの設定

以下の表には、**新規スケジューリングポリシー** と **スケジューリングポリシーの編集** のウィンドウで使えるオプションについての説明をまとめています。

表1.12 新規スケジューリングポリシーおよびスケジューリングポリシーの編集の設定

フィールド名	説明
名前	スケジューリングポリシーの名前。ここで指定した名前は、Red Hat Virtualization Manager でスケジューリングポリシーを参照するのに使用されます。
説明	スケジューリングポリシーの説明。このフィールドへの入力推奨されますが、必須ではありません。
フィルターモジュール	<p>クラスター内の仮想マシンを実行することのできるホストを制御するためのフィルターのセット。フィルターを有効にすると、そのフィルターにより指定されている以下のような条件を満たさないホストは除外されます。</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: 同じホストへのマイグレーションを防ぎます。 ● 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 トポロジーに対応しないホスト ● CPU: 仮想マシンに割り当てられている数よりも CPU の少ないホスト ● Memory: 仮想マシンを実行するのに十分なメモリがないホスト ● VmAffinityGroups: アフィニティグループのメンバーとなっている仮想マシンに指定された条件を満たさないホスト。たとえば、1つのアフィニティグループ内の仮想マシンは、同じホストまたは別のホストで実行されるように指定されます。 ● VmToHostsAffinityGroups: アフィ

フィールド名	説明
	<p>ニティグループのメンバーとなっている仮想マシンに指定された条件を満たさないホストのグループ。たとえば、1つのアフィニティグループ内の仮想マシンは、グループ内のいずれかのホストまたはグループ外の別のホストで実行されるように指定されます。</p> <ul style="list-style-type: none"> ● InClusterUpgrade: 仮想マシンを実行しているホストよりも前のバージョンのオペレーティングシステムを使用しているホスト ● HostDevice: 仮想マシンが必要とするホストデバイスをサポートしていないホスト ● HA: セルフホストエンジン環境の Manager 用仮想マシンが、高可用性スコアがポジティブのホストでのみ実行されるように強制します。 ● Emulated-Machine: エミュレーションする仮想マシンタイプを正式にサポートしていないホスト ● Network: 仮想マシンのネットワークインターフェースコントローラーが必要とする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 ● HostedEnginesSpares: 指定した数のセルフホストエンジンノード上に、Manager 用仮想マシン用にディスク容量を確保します。 ● Label: 必要なアフィニティラベルのないホスト ● Compatibility-Version: 正しい互換バージョンがサポートされるホストでのみ仮想マシンを実行します。 ● CPUOverloaded: CPU が過負荷状態にあるホスト
加重値モジュール	<p>仮想マシンを実行することの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素の相対的な優先順位を制御するための加重値</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。重み付けにより、仮想マシンを実行しているホストよりも前のバージョンのオペレーティングシステムを使用しているホストには、同じバージョンのオペレーティングシステムを使用しているホストよりも大きなペナルティーが科されま

フィールド名	説明
	<p>す。したがって、より後のバージョンのオペレーティングシステムを使用しているホストが優先されます。</p> <ul style="list-style-type: none"> ● OptimalForHaReservation: 高可用性スコアに応じてホストに加重します。 ● None: 負荷均等配分のモジュールに応じてホストに加重します。 ● OptimalForEvenGuestDistribution: ホスト上で実行されている仮想マシンの数に応じてホストに加重します。 ● VmAffinityGroups: 仮想マシンに定義されているアフィニティグループに応じてホストに加重します。この加重値モジュールは、アフィニティグループのパラメーターに応じて、そのアフィニティグループ内の仮想マシンが同じホストまたは異なるホストで実行される可能性を決定します。 ● VmToHostsAffinityGroups: 仮想マシンに定義されているアフィニティグループに応じてホストに加重します。この加重値モジュールは、アフィニティグループ内の仮想マシンがグループ内のいずれかのホストまたはグループ外の別のホストで実行される可能性を決定します。 ● OptimalForCPUPowerSaving: CPU使用率に応じてホストに加重し、CPU使用率の高いホストを優先します。 ● OptimalForEvenCpuDistribution: CPU使用率に応じてホストに加重し、CPU使用率の低いホストを優先します。 ● HA: 高可用性スコアに応じてホストに加重します。 ● PreferredHosts: 優先ホストから先に、仮想マシンをセットアップして実行します。 ● OptimalForMemoryPowerSaving: メモリー使用率に応じてホストに加重し、利用可能なメモリーの少ないホストを優先します。 ● OptimalForMemoryEvenDistribution: メモリー使用率に応じてホストに加重し、利用可能なメモリーの多いホストを優先します。
ロードバランサー	<p>このドロップダウンメニューにより、適用する負荷分散モジュールを選択することができます。負荷分散モジュールは、高使用率から低使用率のホストへの仮想マシン移行に使用されるロジックを決定します。</p>

フィールド名	説明
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/削除することができます。このメニューは、スケジューリングポリシーで負荷分散モジュールを選択した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ず、提供されるプロパティーは選択した負荷分散モジュール固有です。+ または - 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/削除します。

1.4. インスタンスのタイプ



インスタンスタイプは、仮想マシンのハードウェア設定を定義するのに使用することができます。仮想マシンの作成/編集時にインスタンスタイプを選択すると、ハードウェア設定のフィールドが自動的に設定されます。これにより、ユーザーは手動で全フィールドを設定する必要なく、同じハードウェア設定の仮想マシンを複数作成することができます。

以下の表には、デフォルトで提供されている事前定義済みのインスタンスタイプをまとめています。

表1.13 事前定義済みのインスタンスタイプ

名前	メモリー	仮想 CPU
Tiny	512 MB	1
Small	2 GB	1
Medium	4 GB	2
Large	8 GB	2
XLarge	16 GB	4

管理者は、**設定** ウィンドウの **インスタンスタイプ** のタブでインスタンスタイプの作成、編集、削除を行うこともできます。

新規仮想マシン および **仮想マシンの編集** ウィンドウで、インスタンスタイプにバインドされたフィールドの横には鎖のリンクマークが表示されます ()。これらのフィールドの値が変更された場合には、仮想マシンはそのインスタンスタイプからデタッチされて、**カスタム** に変わり、鎖のリンクが解除されて表示されます ()。ただし、その値が元に戻された場合には、鎖のリンクが再度繋がり、選択したインスタンスタイプに戻ります。

1.4.1. インスタンスタイプの作成

管理者は、仮想マシンの作成または編集時にユーザーが選択できるように、新しいインスタンスタイプを作成することができます。

インスタンスタイプの作成

1. **管理** → **設定** をクリックします。
2. **インスタンスタイプ** タブをクリックします。
3. **新規作成** をクリックします。
4. インスタンスタイプの **名前** と **説明** を入力します。
5. **詳細オプションを表示** をクリックし、必要に応じて、インスタンスタイプの項目を設定します。**新規インスタンスタイプ** ウィンドウに表示される設定項目は、**新規仮想マシン** ウィンドウの設定項目と同じですが、関連するフィールドのみが表示されます。『**仮想マシン管理ガイド**』の「**新規仮想マシンおよび仮想マシンの編集ウィンドウの設定**」のセクション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が **設定** ウィンドウの **インスタンスタイプ** タブに表示され、仮想マシンの作成/編集時に **インスタンスタイプ** のドロップダウンリストから選択することができるようになりました。

1.4.2. インスタンスタイプの編集

管理者は、**設定** ウィンドウで既存のインスタンスタイプを編集することができます。

インスタンスタイプのプロパティの編集

1. **管理** → **設定** をクリックします。
2. **インスタンスタイプ** 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. **編集** をクリックします。
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をベースとする新規仮想マシンを作成する際に、またはこのインスタンスタイプをベースとする既存の仮想マシンを更新する際に、新しい設定が適用されます。

このインスタンスタイプをベースとする既存仮想マシンに表示される鎖のアイコンが付いたフィールドは、この変更を反映して更新されます。実行中の既存仮想マシンのインスタンスタイプを変更した場合は、仮想マシンの横にオレンジ色の「保留中の変更」アイコンが表示され、鎖のアイコンが付いたフィールドは次の再起動時に更新されます。

1.4.3. インスタンスタイプの削除

インスタンスタイプの削除

1. **管理** → **設定** をクリックします。
2. **インスタンスタイプ** 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. **削除** をクリックします。
5. いずれかの仮想マシンが削除するインスタンスタイプをベースとしている場合には、アタッチされている仮想マシンが一覧表示された警告のウィンドウが表示されます。このインスタンスタイプの削除を続行するには、**操作を承認** のチェックボックスを選択します。続行しない場合には **キャンセル** 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の一覧から対象のインスタンスタイプが削除され、新規仮想マシンの作成時には表示されなくなりました。削除したインスタンスタイプにアタッチされていた仮想マシンは **カスタム** (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、各クラスターで割り当てられる MAC アドレスの範囲を定義します。MAC アドレスプールは、各クラスターに指定されます。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生成して、新規仮想ネットワークデバイスに割り当てることができます。これは、MAC アドレスの重複を防ぐのに役立ちます。1 つのクラスターに関連するすべての MAC アドレスが、割り当て済みの MAC アドレスプールの範囲内にある場合に、MAC アドレスプールのメモリー効率がより高くなります。

同じ MAC アドレスプールを複数のクラスターで共有することができますが、各クラスターには単一の MAC アドレスプールが割り当てられます。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、他に MAC アドレスプールが割り当てられていない場合に使用されます。クラスターへの MAC アドレスプールの割り当てに関する詳しい情報は、[「新規クラスターの作成」](#) を参照してください。

MAC アドレスプールは、最後にプールに返されたアドレスの後に利用可能な MAC アドレスを割り当てます。この範囲内にそれ以降のアドレスが残っていない場合には、範囲の開始値から検索を開始します。単一の MAC アドレスプール内で複数の MAC アドレス範囲が定義されている場合には、それらの範囲は交互に使用され、利用可能な MAC アドレスが選択されるのと同じ方法で、受信した要求に対応します。

1.5.1. MAC アドレスプールの作成

新規 MAC アドレスプールを作成することができます。

MAC アドレスプールの作成

1. **管理** → **設定** をクリックします。
2. **MAC アドレスプール** タブをクリックします。
3. **追加** をクリックします。
4. 新規 MAC アドレスプールの **名前** と **説明** を入力します。
5. 1 つのプールで同じ MAC アドレスを複数回使用できるようにするには、**重複を許可する** チェックボックスを選択します。MAC アドレスプールは、重複した MAC アドレスを自動的に使用しませんが、重複のオプションを有効にすると、ユーザーは重複した MAC アドレスを手動で指定することができます。



注記

1 つの MAC アドレスプールで重複のオプションを無効にし、別の MAC アドレスプールで重複のオプションを有効にした場合には、重複が無効な MAC アドレスプールでは、各 MAC アドレスを 1 回しか使用できませんが、重複のオプションが有効なプールでは、MAC アドレスを複数回使用することができます。

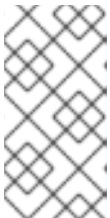
6. 必要な **MAC アドレスの範囲** を指定します。複数の範囲を入力するには、**開始アドレス** と **終了アドレス** のフィールドの横にある **プラス (+)** のボタンをクリックします。
7. **OK** をクリックします。

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、プール内で利用可能な MAC アドレスの範囲や、重複を許可するかどうかなどの詳細設定を変更することができます。

MAC アドレスプールのプロパティ編集

1. **管理** → **設定** をクリックします。
2. **MAC アドレスプール** 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. **編集** をクリックします。
5. 必要に応じて、**名前**、**説明**、**重複を許可する**、**MAC アドレスの範囲** のフィールドを変更します。



注記

MAC アドレス範囲の更新時に、既存の NIC の MAC アドレスは再割り当てされません。割り当て済みの MAC アドレスが、新しい MAC アドレスの範囲外となった場合には、ユーザー指定の MAC アドレスとして追加され、その MAC アドレスプールによって引き続きトラッキングされます。

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 アドレスプールを作成した後は、そのユーザーパーミッションを設定することができます。ユーザーパーミッションは、その MAC アドレスプールをどのデータセンターで 사용할 ことができるかを制御します。新規ユーザーパーミッションの追加については、「[ロール](#)」を参照してください。

MAC アドレスプールのパーミッションの編集

1. **管理** → **設定** をクリックします。
2. **MAC アドレスプール** タブをクリックします。
3. 対象の 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パーミッションを編集します。
 - MAC アドレスプールにユーザーパーミッションを追加するには、以下の手順を実行しま

す。

- a. **設定** ウィンドウの最下部にあるユーザーパーミッションペインで **追加** をクリックします。
 - b. 対象のユーザーを検索して選択します。
 - c. **割り当てるロール** 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** をクリックすると、ユーザーパーミッションが追加されます。
- MAC アドレスプールからユーザーパーミッションを削除するには、以下の手順を実行します。
 - a. **設定** ウィンドウの最下部にあるユーザーパーミッションペインで削除するユーザーパーミッションを選択します。
 - b. **削除** をクリックすると、ユーザーパーミッションが削除されます。

1.5.4. MAC アドレスプールの削除

作成した MAC アドレスプールがクラスターに関連付けられていない場合には、その MAC アドレスプールを削除することができます。ただし、デフォルトの MAC アドレスプールは削除できません。

MAC アドレスプールの削除

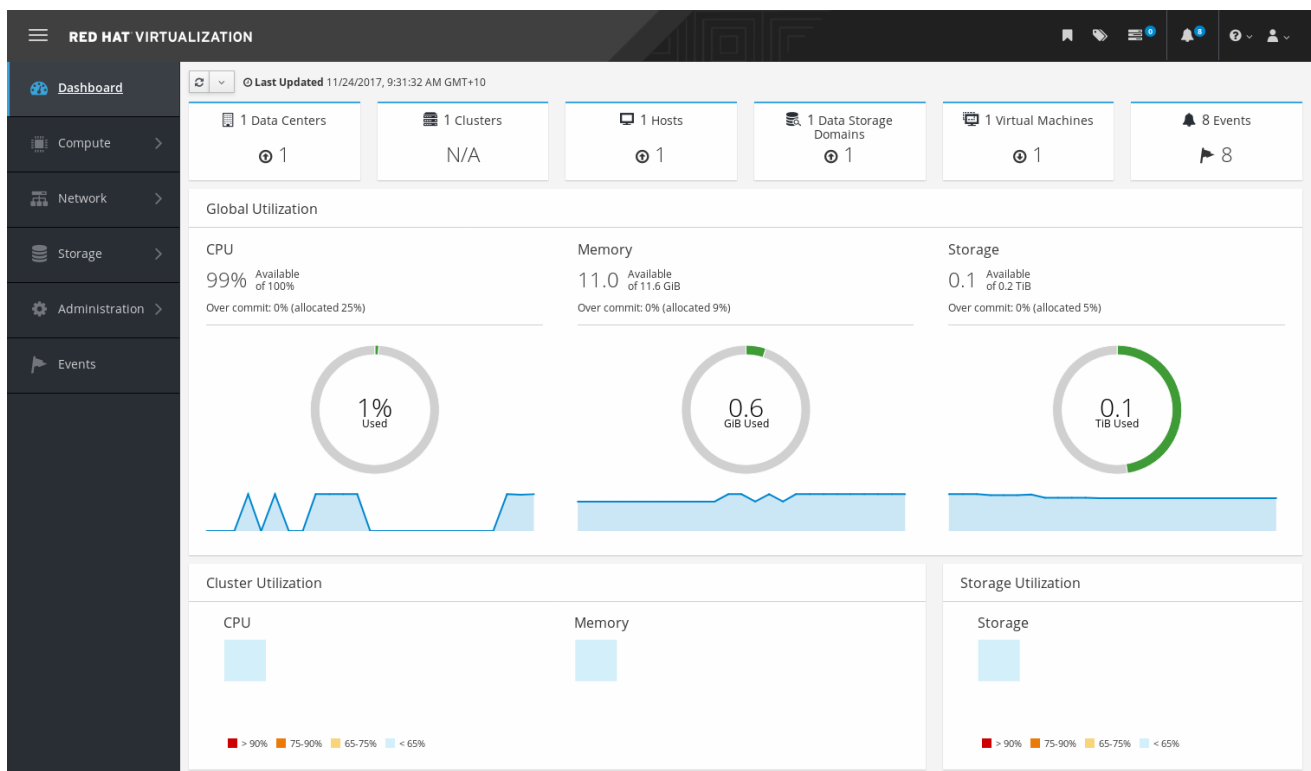
1. **管理** → **設定** をクリックします。
2. **MAC アドレスプール** タブをクリックします。
3. 削除する MAC アドレスプールを選択します。
4. **削除** をクリックします。
5. **OK** をクリックします。

第2章 ダッシュボード

ダッシュボードは、Red Hat Virtualization のリソースと使用状況のサマリーを表示して、Red Hat Virtualization システムのステータスに関する概要を提供します。このサマリーは問題を警告して、その問題の領域を分析することができるようにします。

ダッシュボードの情報は、Data Warehouse からはデフォルトで 15 分間隔で、Manager API によってデフォルトで 15 秒間隔で更新され、またダッシュボードがリフレッシュされるたびに更新されます。最新の情報は、別のページを表示していたユーザーがダッシュボードタブを再び開いた時と、リフレッシュを手動で実行した時にダッシュボードに反映されます。ダッシュボードは、自動ではリフレッシュされません。インベントリーカードの情報は、Manager API によって提供され、使用状況に関する情報は Data Warehouse によって提供されます。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、このコンポーネントは Manager と共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

ダッシュボードには、Data Warehouse をインストールおよび設定する必要があります。『[Data Warehouse Guide](#)』の「[Installing and Configuring Data Warehouse](#)」のセクションを参照してください。

2.2. グローバルインベントリー

ダッシュボードの最上部には、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ます。これには、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、イベントの項目が含まれます。アイコンは、各リソースのステータスを示し、数値は、そのステータスのリソースの数量を示します。




図2.2 グローバルインベントリー

22 Data Centers ▲ 10 ● 10 ● 8	25 Clusters N/A	125 Hosts ▲ 75 ● 63 ● 63	10 Storage Domains ▲ 9 ● 6 ● 4	95 Gluster Volumes ▲ 46 ● 13 ● 43	253 Virtual Machines ▲ 203 ● 33 ● 13	169 Events ▲ 93 ● 103 ▲ 10
----------------------------------	--------------------	-----------------------------	-----------------------------------	--------------------------------------	---	-------------------------------

タイトルには、特定のタイプのリソースの数が示され、その下には、それらの状態が示されます。リソースのタイトルをクリックすると、Red Hat Virtualization Manager 内の関連するページが開きます。クラスターのステータスは、常に「該当なし」と表示されます。

表2.1 リソースのステータス

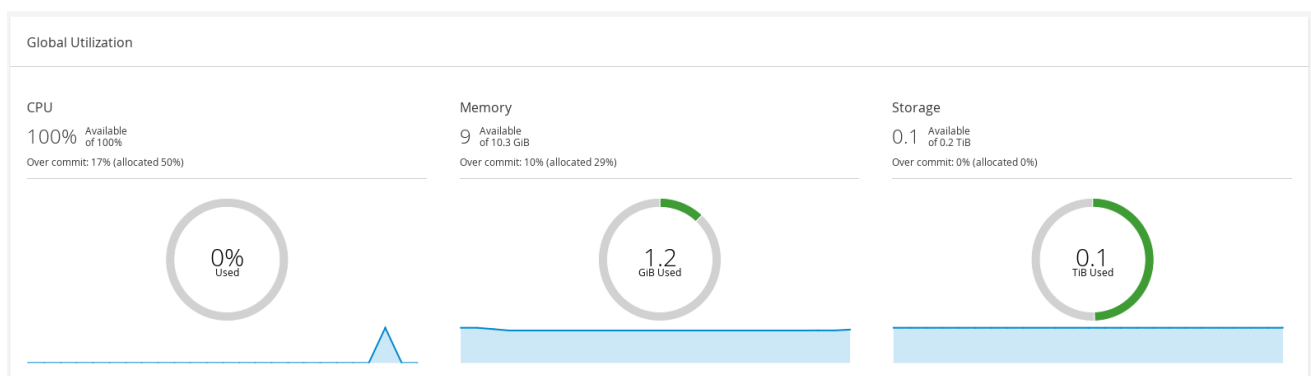
アイコン	ステータス
	そのリソースは、Red Hat Virtualization には 1 つも追加されていません。
	<p>警告のステータスのリソースの数を表示します。このアイコンをクリックすると、対象のページが開き、検索は警告のステータスのリソースに限定されます。検索の制限は、リソースによって異なります。</p> <ul style="list-style-type: none"> ● データセンター: 検索は、非稼働中または応答なしの状態のデータセンターに限定されます。 ● Gluster ボリューム: 検索は、電源投入中、一時停止中、移行中、待機中、サスペンド中、電源切断中のステータスの Gluster ボリュームに限定されます。 ● ホスト: 検索は、未割り当て、メンテナンスモード、インストール中、リブート中、メンテナンス準備中、承認待ち、接続中の状態のホストに限定されます。 ● ストレージドメイン: 検索は、未初期化、未アタッチ、非アクティブ、メンテナンスモード、メンテナンス準備中、デタッチ中、アクティブ化中のステータス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、電源投入中、一時停止中、移行中、待機中、サスペンド中、電源切断中のステータスの仮想マシンに限定されます。 ● イベント: 検索は、重大度が警告レベルのイベントに限定されます。
	稼働中のステータスのリソースの数を表示します。このアイコンをクリックすると、対象のページが開き、検索は稼働中のステータスのリソースに限定されます。

アイコン	ステータス
	<p>停止中の状態のリソースの数を表示します。このアイコンをクリックすると、対象のページが開き、検索は、停止中の状態のリソースに限定されます。検索の制限は、リソースによって異なります。</p> <ul style="list-style-type: none"> ● データセンター: 検索は、未初期化、メンテナンスモード、停止中の状態のデータセンターに限定されます。 ● Gluster ボリューム: 検索は、未アタッチまたは非アクティブの状態の Gluster ボリュームに限定されます。 ● ホスト: 検索は、応答なし、エラーおよびインストールエラーが発生したホスト、非稼働中、初期化中、停止中の状態のホストに限定されます。 ● ストレージドメイン: 検索は、未アタッチまたは非アクティブの状態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、停止中、応答なし、リブート中の状態の仮想マシンに限定されます。
	<p>ステータスが警告のイベントの数を表示します。アイコンをクリックすると、イベント のページが開き、検索は重大度が警告のイベントに限定されます。</p>
	<p>ステータスがエラーのイベントの数を表示します。アイコンをクリックすると、イベント のページが開き、検索は重大度がエラーのイベントに限定されます。</p>

2.3. システム全体の使用状況

システム全体の使用状況 のセクションには、システムの CPU、メモリー、ストレージの使用状況が表示されます。

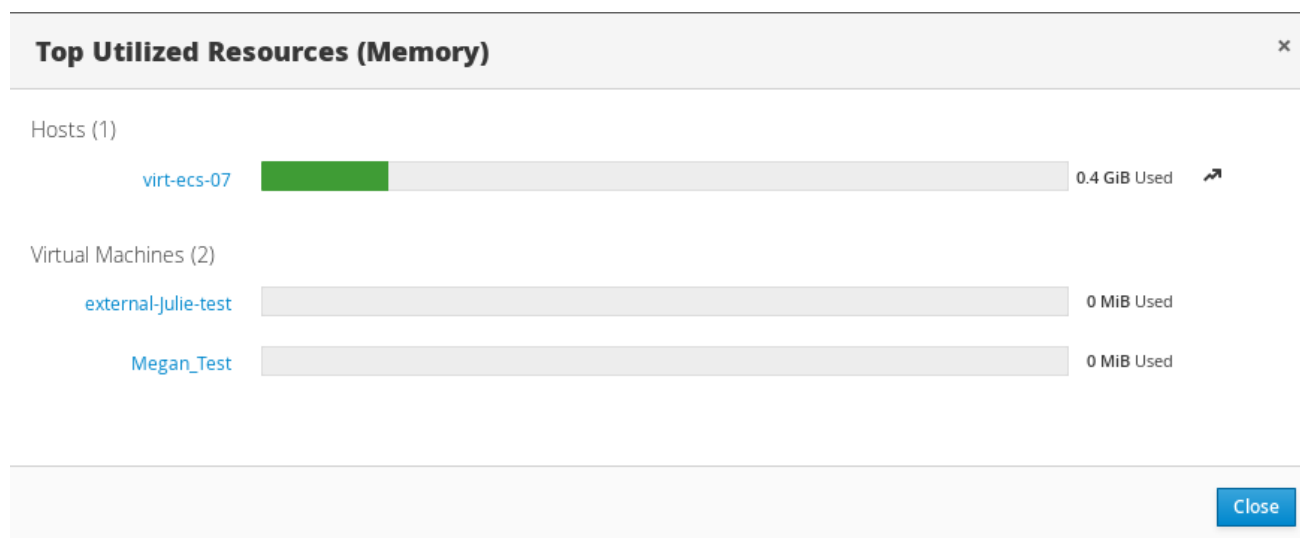
図2.3 システム全体の使用状況



- 最上部には、使用可能な CPU、メモリー、ストレージ、オーバーコミット比のパーセンテージが表示されます。たとえば、CPU のオーバーコミット比は、Data Warehouse の最新のデータに基づいて、仮想コア数を仮想マシンの実行に利用可能な物理コア数で除算した値です。
- ドーナツグラフには、CPU、メモリー、ストレージの使用状況がパーセンテージで表示されるとともに、過去 5 分間の平均的な使用状況に基づいた全ホストの平均使用率也表示されます。ドーナツグラフをポイントすると、選択したセクションの値が表示されます。
- 最下部の折れ線グラフには、過去 24 時間のトレンドが表示されます。各データポイントは、特定の時間の平均使用率を示します。グラフの特定の箇所をポイントすると、CPU のグラフでは時刻と使用率、メモリーとストレージのグラフでは時刻と使用量が表示されます。

2.3.1. 使用率の高いリソース

図2.4 使用率の高いリソース (メモリー)

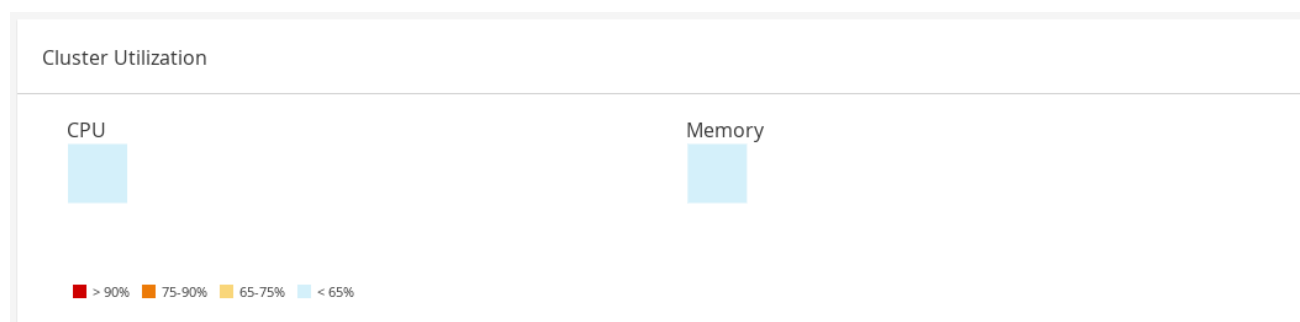


ダッシュボードのシステム全体の使用状況のセクションにあるドーナツグラフをクリックすると、CPU、メモリー、ストレージの使用率の高いリソースの一覧が表示されます。CPU とメモリーでは、ポップアップウィンドウに使用率の高い上位 10 位のホストと仮想マシンの一覧が表示されます。ストレージのポップアップウィンドウには、使用率の高い上位 10 位のストレージドメインと仮想マシンの一覧が表示されます。使用率バーの右側にある矢印で、過去 1 分間における対象リソースの使用状況の傾向が表示されます。

2.4. クラスター使用率

クラスター使用率 のセクションには、クラスターの CPU とメモリーの使用率がヒートマップで表示されます。

図2.5 クラスター使用率



2.4.1. CPU

特定のクラスターの CPU 使用率を示すヒートマップ。過去 24 時間の CPU 平均使用率を表示します。ヒートマップをポイントすると、クラスター名が表示されます。ヒートマップをクリックすると、**コンピュータ → ホスト** に移動し、特定のクラスターの検索結果が CPU 使用率順でソートされます。クラスターの CPU 使用率には、クラスター内の CPU の平均使用率の計算式が使用されます。クラスター別の CPU 使用率の全体平均を割り出すには、各ホストの過去 24 時間の平均 CPU 使用率を使用して算出します。

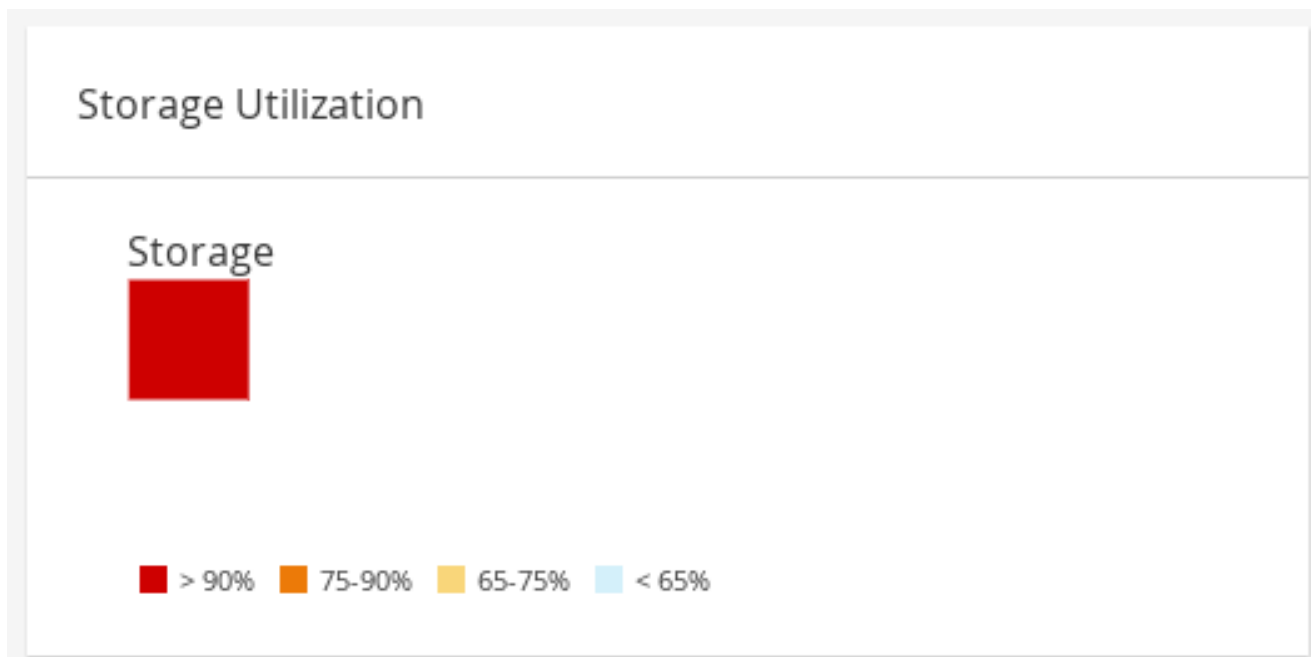
2.4.2. メモリー

特定のクラスターのメモリー使用率を示すヒートマップ。過去 24 時間のメモリー平均使用率を表示します。ヒートマップをポイントすると、クラスター名が表示されます。ヒートマップをクリックすると、**コンピュータ → ホスト** に移動し、特定のクラスターの検索結果がメモリー使用率順でソートされます。クラスターのメモリー使用率には、クラスター内のメモリーの合計使用率の計算式 (GB 単位) が使用されます。クラスター別のメモリー使用率の全体平均を割り出すには、各ホストの過去 24 時間の平均メモリー使用率を使用して算出します。

2.5. ストレージ使用率

ストレージ使用率 のセクションには、ストレージの使用率がヒートマップで表示されます。

図2.6 ストレージ使用率



このヒートマップは、過去 24 時間のストレージの平均使用率を示します。クラスターのストレージ使用率には、クラスター内のストレージの合計使用率の計算式 (GB 単位) が使用されます。クラスター別のストレージ使用率の全体平均を割り出すには、各ホストの過去 24 時間の平均ストレージ使用率を使用して算出します。ヒートマップをポイントすると、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、**ストレージ → ドメイン** に移動し、ストレージの使用率順にストレージドメインがソートされます。

パート II. リソースの管理

第3章 QOS (QUALITY OF SERVICE)

Red Hat Virtualization では、環境内のリソースがアクセス可能な入出力、処理、ネットワークの各機能のレベルに対する粒度の細かい制御を提供する QoS エントリーを定義することができます。QoS 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。このプロファイルは、作成元のクラスターおよびストレージドメイン内の個別のリソースに割り当てられます。

3.1. ストレージの QOS

ストレージの QoS 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。仮想ディスクにストレージの QoS を割り当てると、ストレージドメインのパフォーマンスが微調整されるとともに、特定の仮想ディスクに伴うストレージの操作により同じストレージドメイン内でホストされる他の仮想ディスクに提供されるストレージ機能に影響が及ば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 エントリーの作成

1. コンピュート → データセンター をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **QoS** タブをクリックします。
4. ストレージ セクションで **新規作成** をクリックします。
5. QoS エントリーの **QoS 名** と **説明** を入力します。
6. ラジオボタンのいずれかをクリックして、**スループット** の QoS を指定します。
 - なし
 - **合計: MB/s** のフィールドに総スループットの最大許容値を入力します。
 - **読み取り / 書き込み**: 左側の **MB/s** 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、右側の **MB/s** 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。
7. ラジオボタンのいずれかをクリックして、**入出力 (IOps)** の QoS を指定します。
 - なし
 - **合計: IOps** のフィールドに 1 秒あたりの入出力操作の最大許容数を入力します。
 - **読み取り / 書き込み**: 左側の **IOps** 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、右側の **IOps** 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。
8. **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ました。このエントリーをベースにして、そのデータセンターに属するデータストレージドメインにディスクプロファイルを作成することができます。

3.1.2. ストレージ QoS エントリーの削除

既存のストレージ QoS エントリーを削除します。

ストレージ QoS エントリーの削除

1. コンピュート → データセンター をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **QoS** タブをクリックします。
4. ストレージ セクションでストレージ QoS エントリーを選択し、**削除** をクリックします。
5. **OK** をクリックします。

いずれかのディスクプロファイルがこのエントリーをベースにしていた場合には、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 **[無制限]** に設定されます。

3.2. 仮想マシンネットワークの QoS

仮想マシンネットワークの QoS は、個別の仮想ネットワークインターフェースコントローラーの受信/送信トラフィックを制限するプロファイルの作成を可能にする機能です。この機能を使用すると、多数のレイヤーの帯域幅を制限して、ネットワークリソースの消費を制御することができます。

3.2.1. 仮想マシンネットワーク QoS エントリーの作成

仮想ネットワークインターフェースコントローラー (仮想 NIC) プロファイル (別称: 仮想マシンネットワークインターフェースのプロファイル) に適用してネットワークトラフィックを制御するための仮想マシンネットワーク QoS エントリーを作成します。

仮想マシンネットワーク QoS エントリーの作成

1. コンピュート → データセンター をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **QoS** タブをクリックします。
4. **仮想マシンネットワーク** セクションで **新規作成** をクリックします。
5. 仮想マシンネットワーク QoS エントリーの **名前** を入力します。
6. **受信** および **送信** ネットワークトラフィックの上限値を入力します。
7. **OK** をクリックします。

仮想ネットワークインターフェースコントローラーに使用することのできる仮想マシンネットワーク QoS エントリーの作成が完了しました。

3.2.2. 新規ネットワーク QoS およびネットワーク QoS の編集ウィンドウの設定

仮想マシンネットワーク QoS の設定により、3 つの特定のレベルにおける受信/送信トラフィックの帯域幅の制限を設定することができます。

表3.1 仮想マシンネットワーク QoS の設定

フィールド名	説明
データセンター	仮想マシンネットワーク 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、選択されているデータセンターによって自動的に設定されます。
名前	Manager 内で表示される仮想マシンネットワーク QoS ポリシーの名前
受信	<p>受信トラフィックに適用される設定。この設定を有効にするには 受信 チェックボックスにチェックを入れ、無効にするには外します。</p> <ul style="list-style-type: none"> ● 平均: 受信トラフィックの平均スピード ● 最大値: ピーク時の受信トラフィックのスピード ● バースト: バースト中の受信トラフィックのスピード
送信	<p>送信トラフィックに適用される設定。この設定を有効にするには 送信 チェックボックスにチェックを入れ、無効にするには外します。</p> <ul style="list-style-type: none"> ● 平均: 送信トラフィックの平均スピード ● 最大値: ピーク時の送信トラフィックのスピード ● バースト: バースト中の送信トラフィックのスピード

平均、最大値、または バースト フィールドの最大許容値を変更するには、**engine-config** コマンドを使用して **MaxAverageNetworkQoSValue**、**MaxPeakNetworkQoSValue**、または **MaxBurstNetworkQoSValue** 設定キーの値を変更します。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。以下に例を示します。

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

3.2.3. 仮想マシンネットワーク QoS エントリーの削除

既存の仮想マシンネットワーク QoS エントリーを削除します。

仮想マシンネットワーク QoS エントリーの削除

1. コンピュート → データセンター をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **QoS** タブをクリックします。

4. **仮想マシンネットワーク** セクションで仮想マシンネットワーク QoS エントリーを選択し、**削除** をクリックします。
5. **OK** をクリックします。

3.3. ホストネットワークの QoS

ホストネットワークの QoS は、1 台のホスト上の複数のネットワークを設定して、物理インターフェースを通過する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の QoS は、同一の物理ネットワークインターフェースコントローラー上におけるネットワークリソースの消費を制御することによって、ネットワークパフォーマンスを微調整することができます。これは、1 つのネットワークによって、同じ物理ネットワークインターフェー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機能しなくなる状態を防ぐのに役立ちます。ホストネットワークの QoS を設定することにより、輻輳の問題が発生することなく、それらのネットワークが同じ物理ネットワークインターフェースコントローラー上で正常に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 エントリーを作成します。

ホストネットワーク QoS エントリーの作成

1. **コンピュー**ト → **データセンター** をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **QoS** タブをクリックします。
4. **ホストネットワーク** セクションで **新規作成** をクリックします。
5. QoS エントリーの **QoS 名** と **説明** を入力します。
6. **加重シェア**、**速度の上限 [Mbps]**、および **コミット速度 [Mbps]** に適切な値を入力します。
7. **OK** をクリックします。

3.3.2. 新規ホストネットワーク QoS およびホストネットワーク QoS の編集ウィンドウの設定

ホストネットワーク QoS の設定で、送信トラフィックの帯域幅の上限を設定することができます。

表3.2 ホストネットワーク QoS の設定

フィールド名	説明
データセンター	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、選択されているデータセンターによって自動的に設定されます。
QoS 名	Manager 内で表示されるホストネットワーク QoS ポリシーの名前
説明	ホストネットワーク QoS ポリシーの説明

フィールド名	説明
送信	<p>送信トラフィックに適用される設定</p> <ul style="list-style-type: none"> ● 加重シェア: 特定のネットワークに割り当てる論理リンクのキャパシティを、同じ論理リンクにアタッチされた他のネットワークに対して相対的に示します。シェアの具体的な値は、そのリンク上の全ネットワークのシェアの和によって異なります。デフォルトでは、これは、1 - 100 の範囲内の数値です。 ● 速度の上限 [Mbps]: ネットワークが使用する最大帯域幅 ● コミット速度 [Mbps]: ネットワークに必要な最小の帯域幅。要求されるコミット速度は保証されず、ネットワークインフラストラクチャーや同じ論理リンク上の他のネットワークに要求されるコミット速度によって異なります。

速度の上限 [Mbps] または コミット速度 [Mbps] フィールドの最大許容値を変更するには、**engine-config** コマンドを使用して **MaxAverageNetworkQoSValue** 設定キーの値を変更します。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。以下に例を示します。

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

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 エントリーを削除します。

ホストネットワーク QoS エントリーの削除

1. コンピュート → データセンター をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **QoS** タブをクリックします。
4. **ホストネットワーク** セクションでホストネットワーク QoS エントリーを選択し、**削除** をクリックします。
5. プロンプトが表示されたら **OK** をクリックします。

3.4. CPU の QOS

CPU の QoS は、仮想マシンが、その仮想マシンを実行するホストで利用できる最大処理能力を定義します。この値は、そのホストで利用可能な総処理能力に対するパーセンテージで指定します。CPU の QoS を仮想マシンに割り当てると、クラスター内の 1 台の仮想マシンのワークロードが、同じクラスター内のその他の仮想マシンが利用可能な処理リソースに影響を及ぼすのを防ぐことができます。

3.4.1. CPU QoS エントリーの作成

CPU QoS エントリーを作成します。

CPU QoS エントリーの作成

1. **コンピュート** → **データセンター** をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **QoS** タブをクリックします。
4. **CPU** セクションで **新規作成** をクリックします。
5. QoS エントリーの **QoS 名** と **説明** を入力します。
6. **上限** フィールドには、QoS エントリーが許容する最大処理能力をパーセンテージで入力します。% のシンボルは入力しないでください。
7. **OK** をクリックします。

CPU QoS エントリーが作成されました。このエントリーをベースにして、そのデータセンターに属するクラスターで CPU プロファイルを作成することができます。

3.4.2. CPU QoS エントリーの削除

既存の CPU QoS エントリーを削除します。

CPU QoS エントリーの削除

1. **コンピュート** → **データセンター** をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **QoS** タブをクリックします。
4. **CPU** セクションで CPU QoS エントリーを選択し、**削除** をクリックします。
5. **OK** をクリックします。

いずれかの CPU プロファイルがこのエントリーをベースにしていた場合には、それらのプロファイルの CPU QoS エントリーは自動的に **[無制限]** に設定されます。

第4章 データセンター

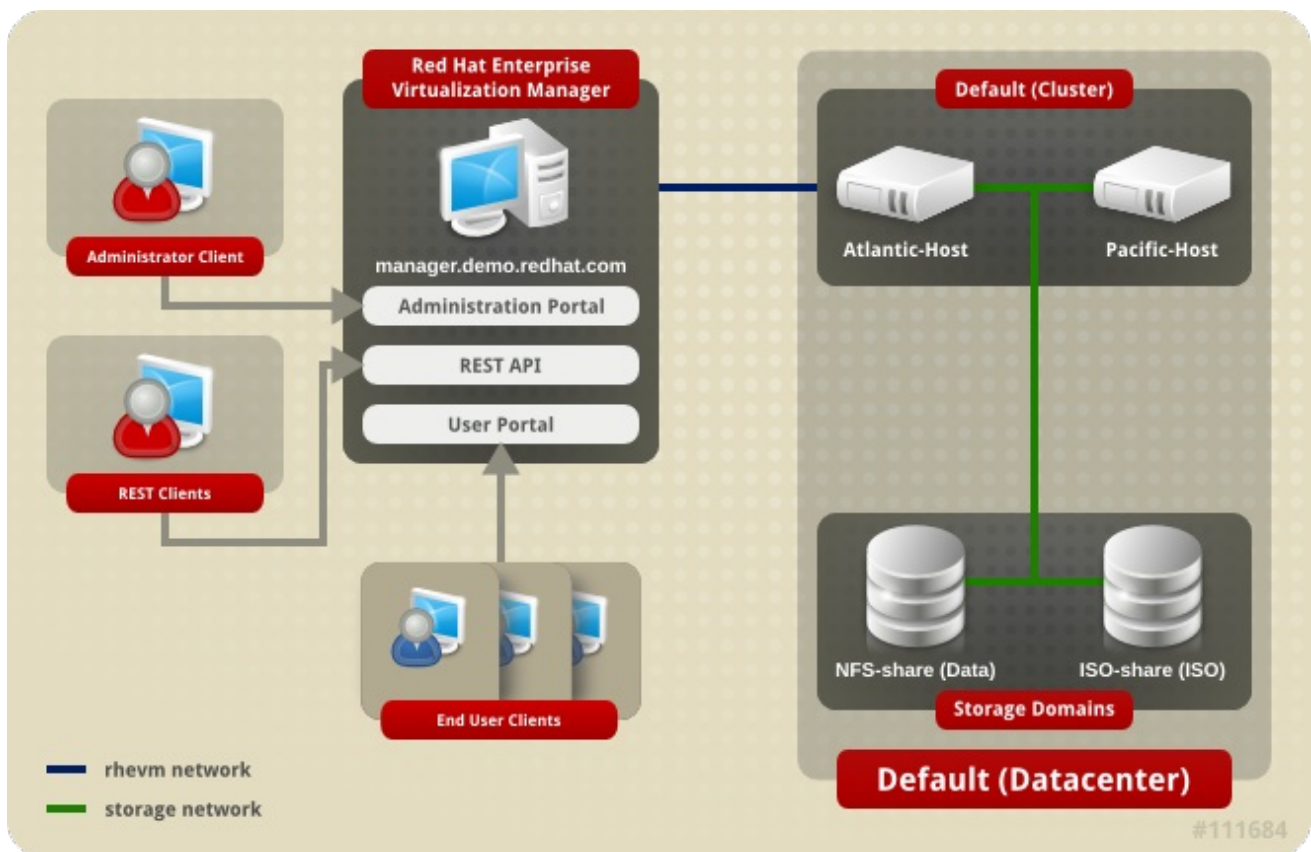
4.1. データセンターについて

データセンターとは、特定の環境で使用するリソースを定義する論理エンティティです。データセンターはコンテナリソースと考えられ、その中には、論理リソース (クラスター、ホストの形式) と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)、ストレージリソース (ストレージドメインの形式) が含まれています。

データセンターは、複数のクラスターで構成することができます。各クラスターには複数のホストを含めることが可能です。また、データセンターに複数のストレージドメインを関連付けたり、各ホスト上で複数の仮想マシンをサポートしたりすることもできます。Red Hat Virtualization 環境は、複数のデータセンターで構成することができます。データセンターのインフラストラクチャーにより、これらのセンターを別々に分けることが可能です。

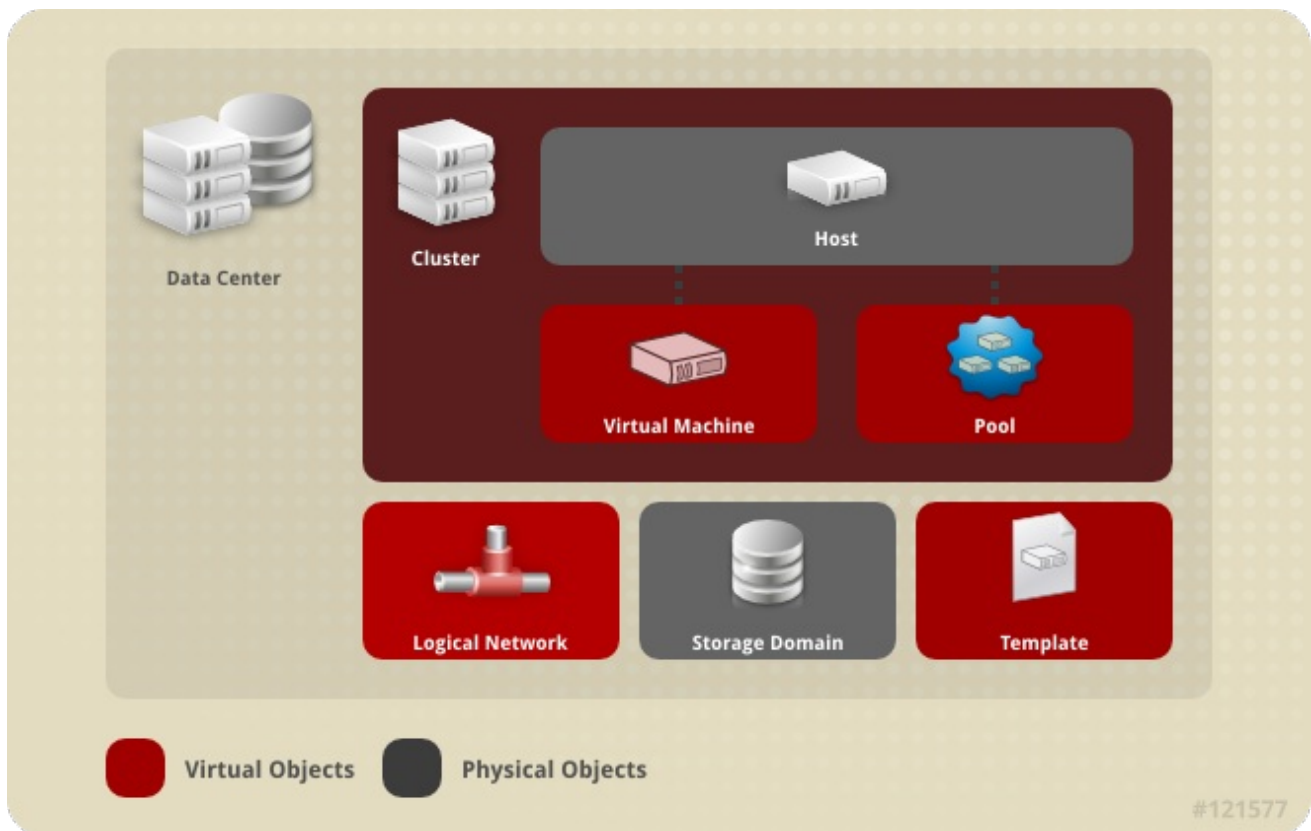
データセンターはすべて管理ポータルから一元管理されます。

図4.1 データセンター



Red Hat Virtualization はインストール中にデフォルトのデータセンターを作成します。このデフォルトのデータセンターを構成するか、適切な名前のデータセンターを新たに設定することが可能です。

図4.2 データセンターのオブジェクト



4.2. STORAGE POOL MANAGER

Storage Pool Manager (SPM) はデータセンター内の 1 台のホストに割り当てられるロールで、そのホストは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なります。SPM エンティティーはデータセンターのどのホストでも実行できます。Red Hat Virtualization Manager はこのロールを 1 台のホストに割り当てます。SPM によって、ホストが標準の操作を実行できなくなるわけではありません。SPM として稼働しているホストは、引き続き仮想リソースをホストすることができます。

SPM エンティティーは、複数のストレージドメインにまたがるメタデータを調整し、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/操作や、スパースブロックデバイス (SAN 上) 用のストレージ割り当てが含まれます。このロールは排他的であり、1 つのデータセンター内で一度に 1 台のホストしか SPM となることができないため、メタデータの整合性が確保されます。

Red Hat Virtualization Manager は、SPM が常に稼働している状態を維持します。SPM がストレージにアクセスする際に問題が発生すると、Manager は SPM のロールを別のホストに移します。SPM の起動時には、Manager は、SPM ロールが付与されているのがそのホストのみとなるようにするので、ストレージセントリックリリースを取得します。このプロセスには多少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を使用します。ホストの SPM 優先度設定により、ホストが SPM ロールに割り当てられる可能性が変更されます。SPM 優先度の高いホストには、優先度の低いホストより先に SPM ロールが割り当てられます。SPM 優先度の低いホスト上にある重要な仮想マシンは、SPM の操作と、ホストのリソースを巡って争う必要はありません。

ホストの SPM 優先度は、**ホストの編集** ウィンドウの **SPM** タブで変更することができます。

4.4. データセンターのタスク

4.4.1. 新しいデータセンターの作成

仮想化環境でデータセンターを作成するには、以下の手順で行います。データセンターが稼働するには、正常に機能するクラスター、ホスト、ストレージドメインが必要です。



注記

互換バージョン は、一旦設定されると、後で低くすることはできません。下位バージョンへの変更はできないようになっています。

データセンターに **MAC プール範囲**を指定するオプションは無効になり、現在はクラスターレベルで指定するようになりました。

新しいデータセンターの作成

1. **コンピュータ** → **データセンター** をクリックします。
2. **新規作成** をクリックします。
3. データセンターの **名前** と **説明** 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**、**クォータモード** を選びます。
5. **OK** をクリックしデータセンターを作成すると、**データセンター - ガイド** ウィンドウが開きます。
6. **データセンター - ガイド** ウィンドウでは、データセンターに設定する必要があるエンティティが表示されます。これらのエンティティを設定するか、**後で設定** ボタンを押して後ほど設定を行います。設定を再開するにはデータセンターを選択し、**その他の操作** → **Guide Me** をクリックしてください。

クラスター、ホスト、ストレージドメインが設定されるまで、新しいデータセンターのステータスは **未初期化** のままとなります。これらのエンティティの設定には **Guide Me** を使用してください。

4.4.2. 新規データセンターおよびデータセンターの編集ウィンドウの設定

以下の表には、**新規データセンター** および **データセンターの編集** 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の説明をまとめています。**OK** をクリックすると、無効な値が入力されている箇所はオレンジ色の枠で囲まれ、そのままでは変更が確定されないようになっています。また、フィールドプロンプトには、期待値または期待値の範囲が表示されます。

表4.1 データセンタープロパティ

フィールド	説明/アクション
名前	データセンターの名前。このテキストフィールドは最長で 40 文字に制限されており、アルファベットの大文字/小文字、数字、ハイフン、アンダースコアを任意に組み合わせた一意名にする必要があります。
説明	データセンターの説明。このフィールドへの入力は推奨されますが、必須ではありません。

フィールド	説明/アクション
ストレージタイプ	<p>ストレージのタイプ。共有 または ローカル のいずれかを選択します。</p> <p>同じデータセンターに異なるタイプのストレージドメイン (iSCSI、NFS、FC、POSIX、Gluster) を追加することができます。ただし、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> <p>データセンターの動作開始後でも、ストレージタイプを変更することができます。「データセンターのストレージタイプの変更」を参照してください。</p>
互換バージョン	<p>Red Hat Virtualization のバージョン</p> <p>Red Hat Virtualization Manager のアップグレード後に、ホスト、クラスター、データセンターが前のバージョンのままになっている可能性があります。最初に全ホストをアップグレードし、次にクラスターをアップグレードしてから、データセンターの互換性レベルをアップグレードしてください。</p>
クォータモード	<p>クォータは、Red Hat Virtualization に搭載されてい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"> ● 無効: クォータを実装しない場合に選択します。 ● 監査: クォータの設定をテストする場合に選択します。 ● 有効: クォータを実装する場合に選択します。
コメント	<p>オプションとして、データセンターに関するプレーンテキスト形式のコメントを追加します。</p>

4.4.3. データセンターの再初期化: リカバリーの手順

このリカバリー手順を実行すると、データセンターのマスターデータドメインが新規のマスターデータドメインに置き換えられます。マスターデータドメインのデータが破損した場合には、その再初期化が必要です。データセンターを再初期化すると、データセンターに関連付けられたその他のリソースすべて (例: クラスター、ホスト、問題のないストレージドメインなど) を復元することができます。

バックアップまたはエクスポートした仮想マシン/テンプレートを新規のマスターデータドメインにインポートすることができます。

データセンターの再初期化

1. **コンピューター → データセンター** をクリックし、データセンターを選択します。

2. データセンターにアタッチされているストレージドメインがメンテナンスモードになっていることを確認してください。
3. その他の操作 → データセンターを再初期化 をクリックします。
4. データセンターの再初期化 ウィンドウでは使用可能な (デタッチされた状態で、メンテナンスモードに入っている) ストレージドメインをすべて表示します。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てください。
5. 操作を承認 のチェックボックスを選択します。
6. OK をクリックします。

ストレージドメインが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て、アクティブ化されました。バックアップまたはエクスポートした仮想マシン/テンプレートを新規の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。

4.4.4. 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 1 台必要です。データセンターを削除しても、そのデータセンターに関連付けられたリソースは削除されません。

データセンターの削除

1. データセンターにアタッチされているストレージドメインがメンテナンスモードになっていることを確認してください。
2. コンピュート → データセンター をクリックし、削除するデータセンターを選択します。
3. 削除 をクリックします。
4. OK をクリックします。

4.4.5. データセンターの強制削除

アタッチされているストレージドメインが破損した場合や、ホストが **Non Responsive** になった場合には、データセンターは **応答なし** 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。

強制削除 を実行するには、アクティブなホストは必要はありません。また、強制削除により、アタッチされているストレージドメインも完全に削除されます。

破損したストレージドメインを **破棄** してからデータセンターの **強制削除** を行う必要がある場合もあります。

データセンターの強制削除

1. コンピュート → データセンター をクリックし、削除するデータセンターを選択します。
2. その他の操作 → 強制削除 をクリックします。
3. 操作を承認 のチェックボックスを選択します。
4. OK をクリックします。

データセンターとアタッチされていたストレージドメインが Red Hat Virtualization 環境から完全に削除されました。

4.4.6. データセンターのストレージタイプの変更

データセンターの動作開始後でも、ストレージタイプを変更することができます。この機能は、仮想マシンまたはテンプレートを移動するのに使用されるデータドメインに有用です。

制約

- 共有からローカル: 複数のホストおよび複数のクラスターが含まれていないデータセンターの場合に変更可能 (ローカルのデータセンターでは複数のホストおよび複数のクラスターはサポートされていないため)。
- ローカルから共有: ローカルストレージドメインが含まれていないデータセンターの場合に変更可能。

データセンターのストレージタイプの変更

1. **コンピュー**ト → **データセンター** をクリックし、変更するデータセンターを選択します。
2. **編集** をクリックします。
3. **ストレージタイプ** を適切な値に変更します。
4. **OK** をクリックします。

4.4.7. 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。互換バージョンとは、データセンターと互換性のある Red Hat Virtualization のバージョンを指します。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します。



注記

データセンターの互換バージョンを変更するには、まず最初に、データセンター内の全クラスターを更新して、必要な互換性レベルをサポートするレベルにしておく必要があります。

データセンターの互換バージョンの変更

1. **コンピュー**ト → **データセンター** をクリックし、変更するデータセンターを選択します。
2. **編集** をクリックします。
3. **互換バージョン** を必要な値に変更します。
4. **OK** をクリックして、**データセンターの互換バージョンを変更** の確認ウィンドウを開きます。
5. **OK** をクリックして確定します。



重要

互換バージョンをアップグレードすると、そのデータセンターに属しているストレージドメインもすべてアップグレードされます。

4.5. データセンターとストレージドメイン

4.5.1. データセンターへの既存データドメインのアタッチ

ステータスが **未アタッチ** 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。複数のタイプの共有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することが可能です。

データセンターへの既存データドメインのアタッチ

1. **コンピュー**ト → **データセンター** をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **ストレージ** タブをクリックし、すでにデータセンターにアタッチされているストレージドメインを表示します。
4. **データをアタッチ** をクリックします。
5. 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。チェックボックスを複数選択して複数のデータドメインをアタッチすることが可能です。
6. **OK** をクリックします。

データドメインがデータセンターにアタッチされ、自動的にアクティブ化されます。

4.5.2. データセンターへの既存 **ISO** ドメインのアタッチ

ステータスが **未アタッチ** 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。この ISO ドメインは、データセンターと同じ **ストレージタイプ** でなければなりません。

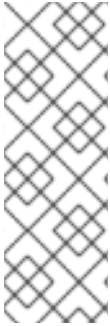
1 つのデータセンターにアタッチできる ISO ドメインは 1 つのみです。

データセンターへの既存 **ISO** ドメインのアタッチ

1. **コンピュー**ト → **データセンター** をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **ストレージ** タブをクリックし、すでにデータセンターにアタッチされているストレージドメインを表示します。
4. **ISO をアタッチ** をクリックします。
5. 対象の ISO ドメインのラジオボタンをクリックします。
6. **OK** をクリックします。

ISO ドメインがデータセンターにアタッチされ、自動的にアクティブ化されます。

4.5.3. データセンターへの既存エクスポートドメインのアタッチ



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。データストレージドメインは、データセンターからアタッチを解除して、同じ環境または異なる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、テンプレートは、インポートしたストレージドメインからアタッチされているデータセンターにアップロードすることができます。ストレージドメインのインポートに関する情報は、「[既存のストレージドメインのインポート](#)」の項を参照してください。

ステータスが **未アタッチ** 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。1つのデータセンターにアタッチできるエクスポートドメインは1つのみです。

データセンターへの既存エクスポートドメインのアタッチ

1. **コンピューター** → **データセンター** をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **ストレージ** タブをクリックし、すでにデータセンターにアタッチされているストレージドメインを表示します。
4. **エクスポートをアタッチ** をクリックします。
5. 対象の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。
6. **OK** をクリックします。

エクスポートドメインがデータセンターにアタッチされ、自動的にアクティブ化されます。

4.5.4. データセンターからのストレージドメインのデタッチ

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、そのデータセンターはストレージドメインに関連付けられなくなります。そのストレージドメインは、Red Hat Virtualization 環境からは削除されず、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、そのストレージドメインにアタッチされたままとなります。



注記

使用可能なストレージドメインがマスターストレージ以外に残っていない場合は、削除することはできません。

データセンターからのストレージドメインのデタッチ

1. **コンピューター** → **データセンター** をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **ストレージ** タブをクリックし、データセンターにアタッチされているストレージドメインを表示します。
4. 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 **アクティブ** である場合は、**メンテナンス** をクリックします。

5. **OK** をクリックしてメンテナンスモードを開始します。

6. **デタッチ** をクリックします。

7. **OK** をクリックします。

ストレージドメインが詳細ビューに表示されなくなるまでに数分かかる場合があります。

第5章 クラスター

5.1. クラスターについて

クラスターとは、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) を使用するホストの論理的な集合体です。ホストの各 CPU モデルの世代が違う場合には、すべてのモデルで提供されている機能のみを使用します。

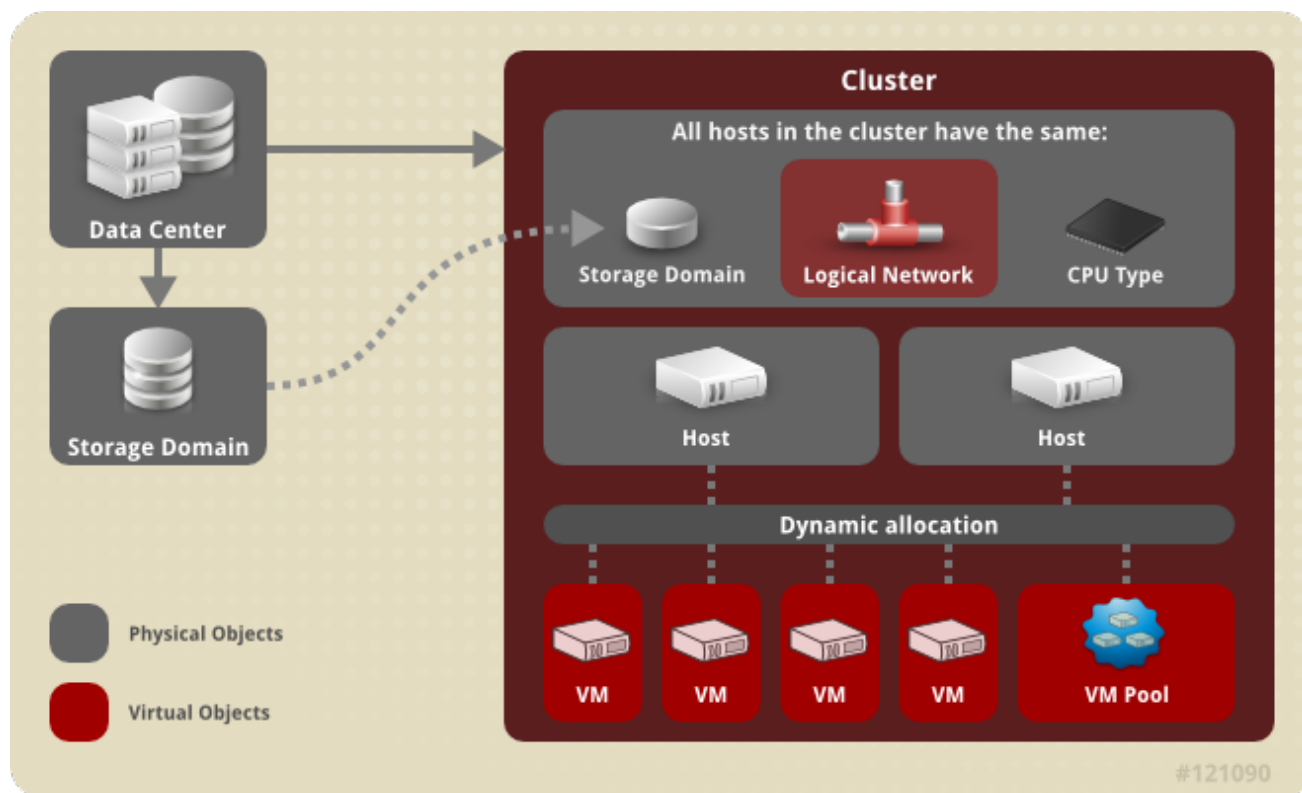
システム内のクラスターはすべて 1 つのデータセンターに属し、またシステム内のホストはすべて 1 つのクラスターに属する必要があります。仮想マシンは、クラスターに定義したポリシーや仮想マシンの設定に従って、クラスター内のいずれかのホストに動的に割り当てられ、ホスト間での移行が可能です。また、クラスターは、電源および負荷共有ポリシーを定義することができる最上位にあります。

クラスターに属するホストと仮想マシンの数はそれぞれ、結果一覧の **ホスト数** と **仮想マシン数** の欄に表示されます。

クラスターは、仮想マシンまたは Red Hat Gluster Storage Server のいずれかを実行します。これらの 2 つの用途は相互に排他的なので、1 つのクラスターで仮想化ホストとストレージホストを同時にサポートすることはできません。

Red Hat Virtualization では、インストール中にデフォルトのデータセンター内にデフォルトのクラスターが作成されます。

図5.1 クラスター



5.2. クラスターのタスク

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が属することができます。また、クラスターには複数のホストが属することが可能です。クラスター内のホストは同じ CPU タイプ (Intel あるいは AMD) である必要があります。CPU タイプを確実に最適化するには、クラスターを作成する前にホストを作成しておくこ

とをお勧めします。ただしホストの設定は、**Guide Me** ボタンを使用して後で行うことができます。

新規クラスターの作成

1. コンピュート → クラスター をクリックします。
2. **新規作成** 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 **データセンター** を選択します。
4. クラスターの **名前** と **説明** を入力します。
5. **管理ネットワーク** ドロップダウンリストでネットワークを選択して、管理ネットワークのロールを割り当てます。
6. ドロップダウンリストから **CPU アーキテクチャー** と **CPU タイプ** を選択します。CPU のプロセッサファミリーが、クラスターにアタッチするホストの最小限必要な CPU タイプに適合していることが重要です。この条件が満たされない場合には、ホストは稼働しません。



注記

Intel および AMD のいずれの CPU タイプでも、CPU モデルは最も古いものから最も新しいものに論理的な順序でリストされます。クラスターに異なる複数の CPU モデルが含まれている場合には、最も古い CPU モデルを選択してください。各 CPU モデルについての詳しい情報は、[「Which CPU family should a RHEV3 or RHV4 cluster be set to?」](#) を参照してください。

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. ドロップダウンリストから **スイッチのタイプ** を選択します。
9. クラスター内のホストの **ファイアウォールタイプ** として、**iptables** または **firewalld** のいずれかを選択します。
10. クラスターに仮想マシンホストまたは Gluster 対応ノードを事前設定するかどうかに応じて、**Virt サービスを有効にする** または **Gluster サービスを有効にする** のいずれかのチェックボックスを選択します。Gluster サービスを有効にしたクラスターには、Red Hat Virtualization Host (RHVH) を追加することはできない点に注意してください。
11. オプションで、**仮想マシンのメンテナンスを行う理由の設定を有効にする** のチェックボックスを選択して、Manager から仮想マシンをシャットダウンする際の理由フィールド (オプション) を有効にして、管理者がメンテナンスの説明を提示できるようにします。
12. オプションで、**ホストのメンテナンスを行う理由の設定を有効にする** のチェックボックスを選択して、Manager からホストをメンテナンスモードに切り替える際の理由フィールド (オプション) を有効にして、管理者がメンテナンスの説明を提示できるようにします。
13. オプションとして、**/dev/hwrng ソース** (外部のハードウェアデバイス) のチェックボックスを選択すると、クラスター内の全ホストが使用する乱数ジェネレーターデバイスを指定することができます。**/dev/urandom** ソース (Linux で提供されるデバイス) はデフォルトで有効化されます。
14. **最適化** タブをクリックし、クラスターのメモリーページ共有の閾値を選択します。またオプションで、クラスターのホストで CPU スレッド処理とメモリーバレーニングを有効化します。

15. クラスターに対して仮想マシンの移行ポリシーを定義するには **移行ポリシー** タブをクリックします。
16. **スケジューリングポリシー** タブをクリックして、そのクラスター内のホストのスケジューリングポリシーの設定、スケジューラーの最適化の設定、信頼済みサービスの有効化、HA 予約の有効化、カスタムのシリアル番号ポリシーの指定などをオプションで設定します。
17. オプションとして、グローバルの SPICE プロキシ (該当する場合) を上書きするには、**コンソール** タブをクリックして、そのクラスター内のホストの SPICE プロキシのアドレスを指定します。
18. **フェンシングポリシー** タブをクリックして、クラスター内のフェンシングを有効化/無効化して、フェンシングオプションを選択します。
19. クラスターのデフォルトのプール以外の MAC アドレスプールを指定するには、**MAC アドレスプール** タブをクリックします。MAC アドレスプールの作成、編集、削除のオプションに関する詳しい情報は、「[MAC アドレスプール](#)」を参照してください。
20. **OK** をクリックしてクラスターを作成すると、**クラスター - ガイド** ウィンドウが開きます。
21. **クラスター - ガイド** ウィンドウでは、クラスターに設定する必要があるエンティティが表示されます。これらのエンティティを設定するか、**後で設定** ボタンを押して後ほど設定を行います。設定を再開するにはクラスターを選択し、**その他の操作** → **Guide Me** をクリックしてください。

5.2.2. クラスターの全般の設定

以下の表には、**新規クラスター** および **クラスターの編集** ウィンドウの **全般** タブの設定についての説明をまとめています。**OK** をクリックすると、無効な値が入力されている箇所はオレンジ色の枠で囲まれ、そのままでは変更が確定されないようになっています。また、フィールドプロンプトには、期待値または期待値の範囲が表示されます。

表5.1 クラスターの全般の設定

フィールド	説明/アクション
データセンター	クラスターが所属するデータセンター。このデータセンターは、クラスターを追加する前に作成しておく必要があります。
名前	クラスターの名前。このテキストフィールドは最長で 40 文字に制限されており、アルファベットの大字/小文字、数字、ハイフン、アンダースコアを任意に組み合わせた一意名にする必要があります。
説明/コメント	クラスターの説明または補注。これらのフィールドへの入力推奨されますが、必須ではありません。
管理ネットワーク	管理ネットワークロールに割り当てられる論理ネットワーク。デフォルトでは ovirtmgmt です。既存のクラスターの管理ネットワークは、詳細ビューの 論理ネットワーク タブの ネットワークを管理 ボタンを押して変更するのが唯一の方法です。

フィールド	説明/アクション
CPU アーキテクチャー	<p>クラスターの CPU アーキテクチャー。選択する CPU アーキテクチャーによって、異なる CPU タイプが利用できます。</p> <ul style="list-style-type: none"> ● 未定義: すべての CPU タイプを利用できます。 ● x86_64: すべての Intel および AMD CPU タイプを利用できます。 ● ppc64: IBM POWER 8 のみを利用できます。
CPU タイプ	<p>クラスターの CPU タイプ。サポートされる CPU タイプの一覧については、『プランニングおよび前提条件ガイド』の「CPU の要件」を参照してください。クラスター内の全ホストが Intel、AMD、IBM POWER 8 のいずれかの CPU タイプを実行する必要があります。作成後に変更すると大幅なサービスの中断を招きます。CPU タイプは、クラスター内で最も古い CPU モデルに設定すべきです。全モデルで実装されている機能のみが使用可能です。Intel および AMD のいずれの CPU タイプでも、CPU モデルは最も古いものから最も新しいものに論理的な順序でリストされます。</p>
互換バージョン	<p>Red Hat Virtualization のバージョン。データセンターに指定されているバージョンよりも前のバージョンは選択できません。</p>
スイッチのタイプ	<p>クラスターで使用されるスイッチのタイプ。Linux Bridge が Red Hat Virtualization の標準スイッチです。OVS は Open vSwitch ネットワーク機能に対応します。</p>
ファイアウォールタイプ	<p>クラスター内のホストのファイアウォールタイプを、iptables または firewalld のどちらかに指定します。既存クラスターのファイアウォールタイプを変更した場合には、そのクラスター内のホストをすべて再インストールして (インストール → 再インストール をクリック) 変更を適用する必要があります。</p>
デフォルトのネットワークプロバイダー	<p>クラスターで使用されるデフォルトの外部ネットワークプロバイダーを指定します。Open Virtual Network (OVN) を選択すると、クラスターに追加されたホストは、OVN プロバイダーと通信するように自動的に設定されます。</p>

フィールド	説明/アクション
Virt サービスを有効にする	このラジオボタンを選択した場合に、そのクラスター内のホストは仮想マシンの実行に使用されます。
Gluster サービスを有効にする	このラジオボタンを選択した場合に、そのクラスター内のホストは Red Hat Gluster Storage Server のノードとして使用され、仮想マシンは実行しません。このオプションが有効化されているクラスターには、Red Hat Virtualization Host を追加することはできません。
既存の Gluster 設定をインポート	<p>このチェックボックスは、Gluster サービスを有効にする のラジオボタンが選択されている場合にのみ表示されます。このオプションにより、既存の Gluster 対応クラスターおよびそのクラスターにアタッチされた全ホストを Red Hat Virtualization Manager にインポートすることができます。</p> <p>次のオプションは、インポートするクラスター内の各ホストに必要となります。</p> <ul style="list-style-type: none"> ● ホスト名: Gluster ホストサーバーの IP アドレスまたは完全修飾ドメイン名を入力します。 ● SSH フィンガープリント: Red Hat Virtualization Manager がホストのフィンガープリントを取得し、正しいホストに接続していることを確認します。 ● パスワード: ホストとの通信に必要な root パスワードを入力します。
仮想マシンのメンテナンスを行う理由の設定を有効にする	このチェックボックスを選択した場合には、Manager を使用してクラスター内の仮想マシンをシャットダウンする際に、オプションの理由のフィールドが表示され、メンテナンスの理由を入力することができます。この理由は、ログに表示され、また仮想マシンの電源が再度オンになると表示されます。
ホストのメンテナンスを行う理由の設定を有効にする	このチェックボックスを選択した場合には、Manager を使用してクラスター内のホストをメンテナンスモードに切り替える際に、オプションの理由のフィールドが表示され、メンテナンスの理由を入力することができます。この理由は、ログに表示され、またホストが再度アクティブ化されると表示されます。

フィールド	説明/アクション
追加の乱数ジェネレーターのソース	このチェックボックスを選択した場合には、クラスター内の全ホストで追加の乱数ジェネレーターデバイスを利用できます。この設定により、乱数ジェネレーターデバイスからエントロピーを仮想マシンに渡すことができるようになります。

5.2.3. 最適化の設定

メモリーページ共有により、仮想マシンは他の仮想マシンで未使用のメモリーを活用することで、割り当てられたメモリーを最大 200% 利用することができます。このプロセスは、Red Hat Virtualization 環境にある仮想マシンが同時にフル稼働しておらず、未使用のメモリーを特定の仮想マシンに一時的に割り当てることができるという前提に基づいています。

CPU スレッド処理により、ホストは、そのホストのコア数を上回るプロセッサコア合計数で仮想マシンを実行することができます。この機能は、CPU を集中的に使用しないワークロードに有用で、より多くの仮想マシンを実行可能にすることにより、ハードウェア要件を軽減できます。またこれにより、特にゲストのコア数がホストのコアよりも多く、ホストのスレッド数よりも少ない場合に、この機能がなければ不可能な CPU トポロジーで仮想マシンを実行できます。

以下の表には、**新規クラスター** および **クラスターの編集** ウィンドウの **最適化** タブの設定についての説明をまとめています。

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"> ● なし - メモリーのオーバーコミットを無効にする: メモリーページの共有が無効になります。 ● サーバーの負荷 - 物理メモリーの 150% のスケジューリングを許可する: メモリーページ共有の閾値を各ホストのシステムメモリーの 150% に設定します。 ● デスクトップの負荷 - 物理メモリーの 200% のスケジューリングを許可する: メモリーページ共有の閾値を各ホストのシステムメモリーの 200% に設定します。

フィールド	説明/アクション
CPU スレッド	<p>スレッドをコアとしてカウントする のチェックボックスを選択すると、ホストのコア数を上回るプロセッサコア合計数の仮想マシンを実行することができます。</p> <p>公開されたホストのスレッドは、コアとして扱われ、仮想マシンに活用することができます。たとえば、1 コアあたり 2 スレッドの 24 コアシステム (合計 48 スレッド) は、それぞれ最大 48 コアの仮想マシンを実行することができ、ホスト CPU の負荷を算出するアルゴリズムは、2 倍の利用可能コアに対して負荷を比較します。</p>
メモリーバルーン	<p>メモリーバルーンの最適化を有効にする のチェックボックスを選択すると、このクラスター内のホストで実行されている仮想マシンのメモリーのオーバーコミットが有効になります。このオプションが設定されると、Memory Overcommit Manager (MOM) が可能な箇所で可能な場合にバルーニングを開始します。各仮想マシンに確保されているメモリーのサイズが上限となります。</p> <p>バルーンを稼働させるには、バルーンデバイスと適切なドライバーが必要です。バルーンデバイスは、特に削除していない限り、各仮想マシンに含まれます。このクラスター内の各ホストは、ステータスが Up に切り替わった時点でバルーンポリシーの更新を受信します。必要な場合には、ホスト上でステータスを変更せずにバルーンポリシーを手動で更新することができます。「クラスター内のホスト上での MOM ポリシーの更新」 を参照してください。</p> <p>シナリオによっては、バルーニングが KSM と競合する可能性があることを認識しておくことが重要です。そのような場合には、MOM がバルーンサイズの調整を試みて、競合を最小限に抑えます。また、一部のシナリオでは、バルーニングによって、仮想マシンでパフォーマンスが十分最適化されない可能性があります。バルーニングの最適化は、慎重に使用することを推奨します。</p>
KSM コントロール	<p>KSM を有効にする のチェックボックスを選択すると、MOM が有効になり、必要な場合に、CPU を犠牲にしてもメモリーを節約することでより高いメモリットが得られる場合に Kernel Same-page Merging (KSM) を実行します。</p>

5.2.4. 移行ポリシーの設定

移行ポリシーは、ホストに問題が発生した場合に、仮想マシンをライブマイグレーションする条件を定義します。これらの条件には、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、仮想マシンの優先順位付けなどが含まれます。

表5.3 移行ポリシー

ポリシー	説明
Legacy	バージョン 3.6 のレガシーの動作。デフォルトの動作に優先する vdsm.conf への設定変更が、そのまま適用されます。ゲストエージェントのフックメカニズムは無効になります。
Minimal downtime	一般的な状況での仮想マシンの移行が可能です。仮想マシンのダウンタイムは長時間にならないはずですが、仮想マシンが長時間経過した後に収束されない場合は移行が中断されます (最大 500 ミリ秒の QEMU の繰り返し回数により異なります)。ゲストエージェントのフックメカニズムは有効になります。
Post-copy migration	このポリシーは、テクノロジープレビュー機能です。最小ダウンタイムのポリシーと同様に、仮想マシンで大幅なダウンタイムが発生してはなりません。長時間経過しても仮想マシンの移行が収束しない場合には、マイグレーションはポストコピーに切り替わります。このポリシーの欠点は、ポストコピー段階に、メモリーの不足している部分がホスト間で転送されるために、仮想マシンの動作の速度が大幅に低減する可能性があることです。ポストコピー段階に、ホスト間のネットワーク障害などの何らかの問題が発生した場合には、実行中の仮想マシンインスタンスは損失します。そのため、ポストコピー段階には、マイグレーションを中止することはできません。ゲストエージェントのフックメカニズムは有効になります。
Suspend workload if needed	仮想マシンが高負荷のワークロードを実行している場合など、多くの状況で仮想マシンを移行できます。仮想マシンのダウンタイムはさらに長時間にわたる可能性があります。ワークロードが過剰な場合には、移行が中断されてしまう可能性があります。ゲストエージェントのフックメカニズムは有効になります。

帯域幅の設定では、ホスト毎の移行 (移行される場合も移行する場合も両方) の際の最大帯域幅を定義します。

表5.4 帯域幅

ポリシー	説明
------	----

ポリシー	説明
自動	帯域幅は、データセンターの ホストネットワーク QoS の 速度の上限 [Mbps] 設定からコピーされます。速度の上限が定義されていない場合には、ネットワークインターフェースの送受信の最低リンクスピードとして算出されます。速度の上限が定義されておらず、リンクスピードが取得できない場合には、送信ホストのローカル VDSM の設定により決まります。
ハイパーバイザーのデフォルト	帯域幅は、送信元のホストのローカル VDSM 設定で制御されます。
カスタム	<p>ユーザーが定義します (Mbps 単位)。この値が同時に発生する移行の数 (デフォルト値は 2 で、出と入の移行に対応します) で割られます。したがって、同時に発生するすべての移行に対応するために、ユーザー定義の帯域幅を十分に大きくする必要があります。</p> <p>たとえば、カスタム 帯域幅を 600 Mbps と定義した場合、仮想マシン移行の最大帯域幅は、実際には 300 Mbps になります。</p>

耐障害性ポリシーは、移行時に仮想マシンをどのように優先順位付けするかを定義します。

表5.5 耐障害性ポリシー

フィールド	説明/アクション
仮想マシンを移行する	定義した優先度の順に、すべての仮想マシンを移行します。
高可用性の仮想マシンのみを移行する	高可用性の仮想マシンのみ移行し、他のホストが過負荷状態になるのを防ぎます。
仮想マシンを移行しない	仮想マシンが移行されないようにします。

追加のプロパティ は、**Legacy** の移行ポリシーにのみ適用されます。

表5.6 追加のプロパティ

プロパティ	説明
-------	----

プロパティ	説明
移行の自動収束	<p>仮想マシンのライブマイグレーション中に自動収束を使用するかどうかを設定することができます。ワークロードが大きくサイズの大きい仮想マシンは、ライブマイグレーション中に到達する転送速度よりも早くメモリーをダーティーな状態にして、移行を収束できないようにする可能性があります。QEMU の自動収束機能は、仮想マシンの移行を強制的に収束することができます。収束されていない場合には、QEMU が自動的に検出して、仮想マシン上の vCPU の使用率を制限します。デフォルトでは、自動収束はグローバルレベルで無効化されています。</p> <ul style="list-style-type: none"> ● グローバルレベルで設定されている自動収束の設定を使用するには、グローバル設定から継承する 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。 ● グローバル設定を無効にして仮想マシンの自動収束を可能にするには、自動収束 を選択します。 ● グローバル設定を無効にして仮想マシンの自動収束を避けるには、自動収束しない を選択します。
移行時の圧縮の有効化	<p>仮想マシンのライブマイグレーション中に移行の圧縮を使用するかどうかを設定することができます。この機能は、Xor Binary Zero Run-Length-Encoding を使用して、仮想マシンのダウンタイム、およびメモリーの書き込みの多いワークロードを実行する仮想マシンやメモリー更新パターンがスパースなアプリケーションの合計ライブマイグレーション時間を減らします。デフォルトでは、移行の圧縮はグローバルレベルで無効化されています。</p> <ul style="list-style-type: none"> ● グローバルレベルで設定されている圧縮の設定を使用するには、グローバル設定から継承する 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。 ● グローバル設定を無効にして仮想マシンの圧縮を可能にするには、圧縮 を選択します。 ● グローバル設定を無効にして仮想マシンの圧縮を避けるには、圧縮しない を選択します。

5.2.5. スケジューリングポリシーの設定

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仮想マシンの使用率や配分を指定することが

できます。クラスター内のホスト間で、自動的に負荷を分散できるようにするには、スケジューリングポリシーを定義します。スケジューリングポリシーの設定にかかわらず、CPU が過負荷の状態にあるホストでは仮想マシンは起動しません。デフォルトでは、80% 以上の負荷が 5 分間続いた場合に、ホストの CPU が過負荷状態にあるとみなされます。ただし、これらの値はスケジューリングポリシーを使用して変更することができます。スケジューリングポリシーの詳細については、「[スケジューリングポリシー](#)」を参照してください。

表5.7 スケジューリングポリシータブのプロパティ

フィールド	説明/アクション
-------	----------

フィールド	説明/アクション
ポリシーを選択	<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: すでに実行中の仮想マシンに関して、ホスト間で負荷の分散または電源の共有を行わない場合には、ポリシー値を none に設定します。これは、デフォルトのモードです。仮想マシンの起動時には、クラスター内のホスト間でメモリーと CPU 処理の負荷が均等に分散されます。ホストが定義された CpuOverCommitDurationMinutes、HighUtilization、または MaxFreeMemoryForOverUtilized に達している場合には、仮想マシンをそのホストに追加でアタッチしてもその仮想マシンは起動しません。 ● evenly_distributed: クラスター内の全ホストでメモリーおよび CPU 処理の負荷が均等に分散されます。ホストが定義された CpuOverCommitDurationMinutes、HighUtilization、または MaxFreeMemoryForOverUtilized に達している場合には、仮想マシンをそのホストに追加でアタッチしてもその仮想マシンは起動しません。 ● cluster_maintenance: メンテナンス作業を実施中のクラスター内のアクティビティーが制限され、高可用性の仮想マシンを除き新たな仮想マシンは起動しません。ホストで障害が発生すると、高可用性の仮想マシンは適切に再起動し、その他の仮想マシンも移行することができます。 ● power_saving: 使用可能なホストのサブセットでメモリーおよび CPU 処理の負荷を分散し、十分に活用されていないホストの電力消費を低減します。ホストの CPU 負荷が使用率の下限值以下の状態で所定の時間が経過すると、仮想マシンはすべて別のホストに移行され、電源をオフにできるようになります。ホストが定義された使用率の上限値に達している場合には、仮想マシンをそのホストに追加でアタッチしてもその仮想マシンは起動しません。 ● vm_evenly_distributed: 仮想マシンの数に基づいて仮想マシンがホスト間で均等に分散されます。HighVmCount を超える数の仮想マシンを実行しているホストがあり、かつ仮想マシンの数が MigrationThreshold から外れているホストが少なくとも 1 台ある場合に、そのクラスターはバランスが取れていない状態とみなされます。
プロパティ	<p>以下のプロパティは、選択したポリシーに応じて表示され、必要に応じて編集することができます。</p>

フィールド	説明/アクション
	<ul style="list-style-type: none"> ● HighVmCount: 負荷分散を可能にするために、1台のホストで最低限実行しなければならない仮想マシンの数を設定します。デフォルト値は 10 です。HighVmCount で定義した数以上の仮想マシンを実行中のホストがクラスター内に最低でも 1 台なければ、負荷分散は有効になりません。 ● MigrationThreshold: 仮想マシンがホストから移行されない許容値を定義します。これは、稼働率の最も高いホストと最も低いホストの間での仮想マシン数の差異の最大値 (この値を含む) です。クラスター内の全ホストで仮想マシン数がこの移行閾値内に収まる場合は、そのクラスターはバランスが取れた状態ということになります。デフォルト値は 5 です。 ● SpmVmGrace: SPM ホスト上で仮想マシン用に確保されるスロット数に関する定義を行います。SPM ホストの負荷が他のホストよりも低くなるように、この変数で SPM ホストが他のホストよりもどれだけ少ない数の仮想マシンを実行するかを定義します。デフォルト値は 5 です。 ● CpuOverCommitDurationMinutes: スケジューリングポリシーが対応するまでに、ホストが所定の使用率外で CPU 負荷を実行できる時間 (分単位) を設定します。この時間を定義することにより、CPU 負荷の一時的な急上昇によりスケジューリングポリシーがアクティブ化されて仮想マシンの移行が不必要に行われるのを防ぐことができます。最大 2 桁までとします。デフォルト値は 2 です。 ● HighUtilization: パーセンテージで指定します。ホストの CPU 使用率が上限値を超えた状態で規定の時間が経過すると、Red Hat Virtualization Manager は、ホストの CPU 負荷が上限閾値を下回るまで、仮想マシンをクラスター内の別のホストに移行します。デフォルト値は 80 です。 ● LowUtilization: パーセンテージで指定します。ホストの CPU 使用率が下限値を下回る状態で規定の時間が経過すると、Red Hat Virtualization Manager は仮想マシンをクラスター内の別のホストに移行します。Manager は元のホストマシンの電源を遮断し、負荷分散で必要となった場合やクラスター内で使用可能なホストが十分でない場合にそのホストを再起動します。デフォルト値は 20 です。 ● ScaleDown: 指定した値でホストのスコアを除することにより、HA 予約 の加重関数による影響を軽減します。これは、none を含む任意のポリシーに追加することができるオプションのプロパティです。 ● HostsInReserve: 実行中の仮想マシンがなくても稼働を続けるホストの数を指定しま

フィールド	説明/アクション
	<p>す。これは、power_saving ポリシーに追加することができるオプションのプロパティです。</p> <ul style="list-style-type: none"> EnableAutomaticHostPowerManagement : クラスター内の全ホストの自動電源管理を有効にします。これは、power_saving ポリシーに追加することができるオプションのプロパティです。デフォルト値は true です。 MaxFreeMemoryForOverUtilized: 最低限のサービスレベルに必要な空きメモリー容量の最小値を MB 単位で設定します。ホストの空きメモリー容量がこの値以下になると、Red Hat Virtualization Manager は、ホストの空きメモリーが最小のサービス閾値を下回っている間は、仮想マシンをクラスター内の別のホストに移行します。MaxFreeMemoryForOverUtilized と MinFreeMemoryForUnderUtilized の両方を 0 MB に設定すると、メモリーベースの負荷分散は無効になります。 MaxFreeMemoryForOverUtilized を設定する場合は、予期せぬ挙動を避けるために MinFreeMemoryForUnderUtilized も設定する必要があります。これは、power_saving および evenly_distributed のポリシーに追加することができるオプションのプロパティです。 MinFreeMemoryForUnderUtilized: ホストを稼働するのに必要な空きメモリー容量の最大値を MB 単位で設定します。ホストの空きメモリー容量がこの値を超えると、ホストは使用率が低いとみなされます。その場合、Red Hat Virtualization Manager は仮想マシンをクラスター内の別のホストに移行します。Manager は元のホストマシンの電源を自動的に切断し、負荷分散で必要となった場合やクラスター内で使用可能なホストが十分でない場合にそのホストを再起動します。 MaxFreeMemoryForOverUtilized と MinFreeMemoryForUnderUtilized の両方を 0 MB に設定すると、メモリーベースの負荷分散は無効になります。 MinFreeMemoryForUnderUtilized を設定する場合は、予期せぬ挙動を避けるために MaxFreeMemoryForOverUtilized も設定する必要があります。これは、power_saving および evenly_distributed のポリシーに追加することができるオプションのプロパティです。 HeSparesCount: Manager 用仮想マシンが移行またはシャットダウンした際にその仮想マシンを起動するのに十分な空きメモリーを確保するための、追加セルフホストエンジンノードの数を設定します。セルフホストエンジンノードで他の仮想マシンを起動すると Manager 用仮想マシン用に十分

フィールド	説明/アクション
	<p>な空きメモリを確保できない場合には、説明/アクション上で他の仮想マシンを起動することができなくなります。これは、power_saving、vm_evenly_distributed、および evenly_distributed のポリシーに追加することができるオプションのプロパティです。デフォルト値は 0 です。</p>
スケジューラーの最適化	<p>ホストの加重/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"> ● 使用率で最適化: スケジューリングに加重モジュールが含まれ、最適な選択が可能となります。 ● スピードで最適化: 保留中の要求が 10 件以上ある場合には、ホストの重み付けをスキップします。
信頼済みサービスを有効にする	<p>OpenAttestation サーバーとの統合を有効にします。この設定を有効にする前に、engine-config ツールを使用して OpenAttestation サーバーの詳細を入力します。詳しくは、「信頼済みコンピュートプール」を参照してください。</p>
HA 予約を有効にする	<p>Manager による高可用性仮想マシン用のクラスターキャパシティーのモニタリングを有効にします。Manager は、既存のホストで予期しないエラーが発生した場合に、高可用性に指定されている仮想マシンを移行するための適切なキャパシティーをクラスター内で確保します。</p>
カスタムのシリアル番号ポリシーを指定する	<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することができます。以下のいずれかのオプションを選択してください。</p> <ul style="list-style-type: none"> ● ホストの ID: 仮想マシンのシリアル番号に、ホストの UUID を設定します。 ● 仮想マシンの ID: 仮想マシンのシリアル番号に、仮想マシンの UUID を設定します。 ● カスタムのシリアル番号: カスタムのシリアル番号を指定することができます。

ホストの空きメモリが 20% 未満に下がると、**mom.Controllers.Balloon - INFO Ballooning guest:half1 from 1096400 to 1991580** のようなブルーニングコマンドが **/var/log/vdsm/mom.log** にログ記録されます。**/var/log/vdsm/mom.log** は、Memory Overcommit Manager のログファイルです。

5.2.6. クラスターのコンソールの設定

以下の表には、新規クラスター および クラスターの編集 ウィンドウの コンソール タブの設定についての説明をまとめています。

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 プロキシを定義する	グローバル設定で定義されている SPICE プロキシの上書きを有効にするには、このチェックボックスを選択します。この機能は、ハイパーバイザーが属するネットワークの外部からユーザーが接続する場合 (例: VM ユーザーポータルからの接続) に有効です。
SPICE プロキシアドレスの上書き	SPICE クライアントが仮想マシンに接続するのに使用するプロキシ。このアドレスは、以下の形式で指定する必要があります。 <div style="border: 1px solid black; padding: 5px; width: fit-content;">protocol://[host]:[port]</div>

5.2.7. フェンシングポリシーの設定

以下の表には、新規クラスター および クラスターの編集 ウィンドウの フェンシングポリシー タブの設定についての説明をまとめています。

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
フェンシングを有効にする	クラスターで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化されていますが、必要に応じて無効にすることができます。たとえば、一時的なネットワークの問題が発生している場合、または発生することが予想される場合に、診断またはメンテナンスの作業が完了するまでの間、管理者はフェンシングを無効にすることができます。フェンシングが無効になると、応答なしの状態のホストで実行されている高可用性の仮想マシンは、別のホストでは再起動されなくなる点に注意してください。
ホストがストレージの有効なリースを持ってい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た場合には、ステータスが Non Responsive で、かつストレージにまだ接続されているクラスター内のホストはフェンシングされません。
クラスターの接続性に問題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すると、クラスター内で接続の問題が発生しているホストの割合が定義済みの 閾値 以上となった場合にフェンシングが一時的に無効となります。 閾値 の値はドロップダウンリストから選択します。設定可能な値は、 25、50、75、100 です。

フィールド	説明/アクション
Gluster ブリックが UP の場合はフェンシングをスキップ	このオプションは、Red Hat Gluster Storage の機能が有効な場合にのみ利用することができます。このチェックボックスを選択すると、ブリックが稼働中で他のピアから到達可能な場合には、フェンシングが一時的に無効となります。詳細については、『 Maintaining Red Hat Hyperconverged Infrastructure 』の「 Configure High Availability using Fencing Policies 」および「 Appendix A. Fencing Policies for Red Hat Gluster Storage 」を参照してください。
Gluster クォーラムが満たされない場合にはフェンシングをスキップ	このオプションは、Red Hat Gluster Storage の機能が有効な場合にのみ利用することができます。このチェックボックスを選択すると、ブリックが稼働中でそのホストをシャットダウンするとクォーラムが失われる場合には、フェンシングが一時的に無効となります。詳細については、『 Maintaining Red Hat Hyperconverged Infrastructure 』の「 Configure High Availability using Fencing Policies 」および「 Appendix A. Fencing Policies for Red Hat Gluster Storage 」を参照してください。

5.2.8. クラスター内のホストへの負荷および電源管理ポリシーの設定

evenly_distributed および **power_saving** のスケジューリングポリシーでは、許容可能なメモリおよび CPU 使用率の値と、どの時点で仮想マシンがホスト間で移行される必要があるかを指定することができます。**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配分します。クラスター内のホスト間における自動負荷分散を有効にするスケジューリングポリシーを定義します。各スケジューリングポリシーに関する詳しい説明は、「[スケジューリングポリシーの設定](#)」を参照してください。

ホストへの負荷および電源管理ポリシーの設定

1. **コンピュート** → **クラスター** をクリックし、クラスターを選択します。
2. **編集** をクリックします。
3. **スケジューリングポリシー** タブをクリックします。
4. 以下のポリシーのいずれかを選択します。
 - **none**
 - **vm_evenly_distributed**
 - a. **HighVmCount** フィールドには、負荷分散を可能にするために、少なくとも 1 台のホストで最低限実行しなければならない仮想マシンの数を設定します。
 - b. **MigrationThreshold** フィールドには、稼働率が最も高いホスト上の仮想マシン数と最も低いホスト上の仮想マシン数の差の最大許容値を定義します。

- c. **SpmVmGrace** フィールドで定義するスロット数により、SPM ホスト上で仮想マシン用に確保されるスロット数が他のホストよりもどれだけ少なくなるかを指定します。
 - d. オプションとして、**HeSparesCount** フィールドに、Manager 用仮想マシンが移行またはシャットダウンした際にその仮想マシンを起動するのに十分な空きメモリーを確保するための、追加セルフホストエンジンノードの数を入力します。詳細については、『セルフホストエンジンガイド』の「[追加ホスト上にセルフホストエンジン用として確保するメモリースロットの設定](#)」を参照してください。
- **evenly_distributed**
 - a. **CpuOverCommitDurationMinutes** フィールドには、スケジューリングポリシーが対応するまでに、ホストが所定の使用率外で CPU 負荷を実行できる時間 (分単位) を設定します。
 - b. **HighUtilization** フィールドには、他のホストへの仮想マシン移行を開始する CPU 使用率を入力します。
 - c. **MinFreeMemoryForUnderUtilized** には、ホストを稼働するのに必要な空きメモリー容量の最大値を MB 単位で入力します。この値を超えると、他のホストへの仮想マシン移行が開始されます。
 - d. **MaxFreeMemoryForOverUtilized** には、必要な空きメモリー容量の最小値を MB 単位で入力します。この値を下回ると、他のホストへの仮想マシン移行が開始されます。
 - e. オプションとして、**HeSparesCount** フィールドに、Manager 用仮想マシンが移行またはシャットダウンした際にその仮想マシンを起動するのに十分な空きメモリーを確保するための、追加セルフホストエンジンノードの数を入力します。詳細については、『セルフホストエンジンガイド』の「[追加ホスト上にセルフホストエンジン用として確保するメモリースロットの設定](#)」を参照してください。
 - **power_saving**
 - a. **CpuOverCommitDurationMinutes** フィールドには、スケジューリングポリシーが対応するまでに、ホストが所定の使用率外で CPU 負荷を実行できる時間 (分単位) を設定します。
 - b. **LowUtilization** フィールドには、ホストが十分に活用されていないとみなされる CPU 使用率の下限を入力します。
 - c. **HighUtilization** フィールドには、他のホストへの仮想マシン移行を開始する CPU 使用率を入力します。
 - d. **MinFreeMemoryForUnderUtilized** には、ホストを稼働するのに必要な空きメモリー容量の最大値を MB 単位で入力します。この値を超えると、他のホストへの仮想マシン移行が開始されます。
 - e. **MaxFreeMemoryForOverUtilized** には、必要な空きメモリー容量の最小値を MB 単位で入力します。この値を下回ると、他のホストへの仮想マシン移行が開始されます。
 - f. オプションとして、**HeSparesCount** フィールドに、Manager 用仮想マシンが移行またはシャットダウンした際にその仮想マシンを起動するのに十分な空きメモリーを確保するための、追加セルフホストエンジンノードの数を入力します。詳細については、『セルフホストエンジンガイド』の「[追加ホスト上にセルフホストエンジン用として確保するメモリースロットの設定](#)」を参照してください。
5. クラスターの **スケジューラーの最適化** には、以下のいずれかを選択します。

- **使用率で最適化** を選択すると、スケジューリングに加重モジュールが含まれ、最適な選択が可能となります。
 - **スピードで最適化** を選択すると、保留中の要求が 10 件以上ある場合には、ホストの重み付けをスキップします。
6. **engine-config** ツールを使用してサーバーの詳細を設定済みで、OpenAttestation サーバーを使用してホストを検証する場合は、**信頼済みサービスを有効にする** のチェックボックスを選択します。
 7. オプションとして、Manager による高可用性仮想マシン用のクラスターキャパシティのモニタリングを有効にするには、**HA 予約を有効にする** のチェックボックスにチェックを入れます。
 8. オプションとして、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するには、**カスタムのシリアル番号ポリシーを指定する** チェックボックスにチェックを入れて、以下のオプションのいずれかを選択します。
 - ホストの UUID を仮想マシンのシリアル番号として設定するには、**ホストの ID** を選択します。
 - 仮想マシンの UUID を仮想マシンのシリアル番号として設定するには、**仮想マシンの ID** を選択します。
 - カスタムのシリアル番号を指定するには、**カスタムのシリアル番号** を選択します。
 9. **OK** をクリックします。

5.2.9. クラスター内のホスト上での **MOM** ポリシーの更新

Memory Overcommit Manager は、ホストでメモリーバルーンと KSM の機能进行处理します。これらの機能をクラスターレベルで変更した場合には、その設定がホストに渡されるのは、ホストの再起動後か、ホストがメンテナンスモードから **Up** のステータスに切り替わった後のみです。ただし、必要な場合には、ホストが **Up** の状態の時に MOM ポリシーを同期することによって、重要な変更をホストに即時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。

ホスト上での **MOM** ポリシーの同期

1. **コンピューター** → **クラスター** をクリックします。
2. クラスター名をクリックして、詳細ビューを表示します。
3. **ホスト** タブをクリックして、MOM ポリシーを更新する必要のあるホストを選択します。
4. **MOM ポリシーを同期** をクリックします。

この操作を実行すると、ホストをメンテナンスモードに切り替えてから **Up** のステータスに戻す必要がなく、ホスト上の MOM ポリシーが更新されます。

5.2.10. CPU プロファイルの作成

CPU プロファイルは、クラスター内の仮想マシンが、その仮想マシンを実行するホストで利用できる最大処理能力を定義します。この値は、そのホストで利用可能な総処理能力に対するパーセンテージで指定します。CPU プロファイルは、データセンター下で定義されている CPU プロファイルに基づいて作成されますが、クラスター内の全仮想マシンには自動的に適用されないため、有効にするには個別の仮想マシンに手動で割り当てる必要があります。

以下の手順は、クラスターの属するデータセンター下で CPU QoS エントリーが 1 つ以上定義済みであることを前提としています。

CPU プロファイルの作成

1. コンピュート → クラスター をクリックします。
2. クラスター名をクリックして、詳細ビューを表示します。
3. **CPU プロファイル** タブをクリックします。
4. **新規作成** をクリックします。
5. CPU プロファイルの **名前** と **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 QoS を選択します。
7. **OK** をクリックします。

5.2.11. 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。

CPU プロファイルの削除

1. コンピュート → クラスター をクリックします。
2. クラスター名をクリックして、詳細ビューを表示します。
3. **CPU プロファイル** タブをクリックし、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 プロファイルが仮想マシンに割り当てられていた場合は、その仮想マシンには **default** CPU プロファイルが自動的に割り当てられます。

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

Red Hat Gluster Storage クラスターおよびそのクラスターに属する全ホストを Red Hat Virtualization Manager にインポートすることができます。

クラスター内のホストの IP アドレスやホスト名、パスワードなどの情報を提供する際には、SSH 経由で、そのホスト上で **gluster peer status** コマンドを実行すると、そのクラスターに属す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は手動で確認して、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しているか、または到達不可な時には、クラスターをインポートすることはできません。新たにインポートされたホストには、VDSM はインストールされていないので、インポートした後は、ブートストラップスクリプトにより必要な VDSM パッケージがすべてホストにインストールされ、ホストが再起動されます。

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

1. コンピュート → クラスター をクリックします。
2. **新規作成** をクリックします。

3. クラスタが属する **データセンター** を選択します。
4. クラスタの **名前** と **説明** を入力します。
5. **Gluster サービスを有効にする** のチェックボックスと **既存の Gluster 設定をインポート** のチェックボックスを選択します。
既存の Gluster 設定をインポート のフィールドは、**Gluster サービスを有効にする** を選択した場合にのみ表示されます。
6. **ホスト名** フィールドに、クラスタ内の任意のサーバーのホスト名または IP アドレスを入力します。
ホストの **SSH 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。ホストが到達不可の場合、またはネットワークエラーが発生している場合には、**SSH フィンガープリント** フィールドに「フィンガープリントの取得でエラーが発生しました」というエラーメッセージが表示されます。
7. サーバーの **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** ウィンドウが開き、クラスタに属するホストの一覧が表示されます。
9. 各ホストの **名前** と **root パスワード** を入力します。
10. 全ホストで同じパスワードを使用する場合は、**共通のパスワードを使用** のチェックボックスを選択し、表示されているテキストフィールドにパスワードを入力します。
適用 をクリックし、入力したパスワードを全ホストに設定します。

フィンガープリントが有効であることを確認した上で **OK** をクリックし、変更を送信します。

ホストをインポートした後に、ブートストラップスクリプトにより必要な VDSM パッケージがすべてホストにインストールされ、その後ホストが再起動されます。既存の Red Hat Gluster Storage クラスタが Red Hat Virtualization Manager に正常にインポートされました。

5.2.13. ホストの追加ウィンドウの設定

ホストの追加 ウィンドウでは、Gluster 対応クラスタの一部としてインポートするホストの詳細を指定することができます。このウィンドウは、**新規クラスタ** ウィンドウの **Gluster サービスを有効にする** のチェックボックスを選択して、必要なホストの詳細を指定した後に表示されます。

表5.10 Gluster ホスト追加の設定

フィールド	説明
共通のパスワードを使用	クラスタ内の全ホストに同じパスワードを使用するには、このチェックボックスにチェックを入れます。 パスワード フィールドにパスワードを入力して、 適用 ボタンをクリックすると、そのパスワードが全ホストに設定されます。
名前	ホスト名を入力します。
ホスト名/IP アドレス	このフィールドには、 新規クラスタ 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 アドレスが自動的に入力されます。

フィールド	説明
root パスワード	ホストごとに異なる root パスワードを使用する場合には、このフィールドにパスワードを入力します。このフィールドにより、クラスター内の全ホストに対して指定した共通パスワードが上書きされます。
フィンガープリント	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す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。

5.2.14. クラスターの削除

削除前にクラスターからすべてのホストを移動します。



注記

Default クラスターには **Blank** テンプレートが含まれているため削除することはできません。ただし、**Default** クラスターの名前を変更し、新規データセンターに追加することはできます。

クラスターの削除

1. **コンピューター** → **クラスター** をクリックし、クラスターを選択します。
2. クラスター内にホストがないことを確認します。
3. **削除** をクリックします。
4. **OK** をクリックします。

5.2.15. 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のバージョンに応じて設定されます。

『アップグレードガイド』の「[クラスターの互換バージョンの変更](#)」を参照してください。

第6章 論理ネットワーク

6.1. 論理ネットワークのタスク

6.1.1. ネットワークタスクの実行

ネットワーク → ネットワーク から、論理ネットワーク関連の操作や各ネットワークのプロパティまたはその他のリソースとの関連付けに基づいた論理ネットワークの検索など、あらゆるタスクを実行することができます。**新規作成**、**編集**、**削除** のボタンで、データセンター内の論理ネットワークの作成、プロパティ変更、削除を行うことができます。

それぞれのネットワーク名をクリックして、詳細ビューの各タブを使用すると、以下のような操作を実行することができます。

- クラスターおよびホストへのネットワークのアタッチ/デタッチ
- 仮想マシンおよびテンプレートからのネットワークインターフェースの削除
- ユーザーがネットワークにアクセスして管理するためのパーミッションの追加/削除

これらの機能には、各リソースからもアクセスすることができます。



警告

実行中のホストがある場合には、クラスターやデータセンター内のネットワークを変更しないでください。ホストが到達不能となるリスクがあります。

重要

Red Hat Virtualization ノードをサービスの提供に使用する予定がある場合には、Red Hat Virtualization 環境が稼働停止すると、そのサービスも停止してしまうことを念頭に置いてください。

これはすべてのサービスが対象となりますが、特に以下のサービスを Red Hat Virtualization で実行する場合の危険性を認識しておく必要があります。

- 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内での新規論理ネットワークの作成

データセンター内またはデータセンター内のクラスターに論理ネットワークを作成し、その用途を定義します。

データセンターまたはクラスター内での新規論理ネットワークの作成

1. コンピュート → データセンター または コンピュート → クラスター をクリックします。

2. データセンターまたはクラスターの名前をクリックして、詳細ビューを表示します。
3. **論理ネットワーク** タブをクリックします。
4. **新規論理ネットワーク** ウィンドウを開きます。
 - データセンターの詳細ビューからは、**新規作成** をクリックします。
 - クラスターの詳細ビューからは、**ネットワークを追加** をクリックします。
5. 論理ネットワークの **名前**、**説明**、および **コメント** を入力します。
6. オプションで **VLAN タグ付けを有効にする** を選択します。
7. オプションで **仮想マシンネットワーク** を無効にします。
8. オプションとして、**Create on external provider** チェックボックスを選択します。これにより、**ネットワークラベル**、**仮想マシンネットワーク**、および **MTU** オプションが無効になります。詳細については、「[11章 外部プロバイダー](#)」を参照してください。
9. **外部プロバイダー** を選択します。**外部プロバイダー** の一覧には、**読み取り専用** モードの外部プロバイダーは表示されません。
内部の独立したネットワークを作成するには、**外部プロバイダー** の一覧から **ovirt-provider-ovn** を選択し、**Connect to physical network** チェックボックスのチェックを外します。
10. **ネットワークラベル** のテキストフィールドには、その論理ネットワーク用に新規ラベルを入力するか、既存のラベルを選択します。
11. **MTU** 値を **デフォルト (1500)** または **カスタム** に設定します。
12. **クラスター** タブから、ネットワークを割り当てるクラスターを選択します。その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することができます。
13. **Create on external provider** を選択した場合には、**サブネット** タブが表示されます。この **サブネット** タブで **サブネットを作成** を選択して、その論理ネットワークが提供するサブネットの **名前**、**CIDR**、**ゲートウェイ アドレス** を入力し、**IP バージョン** を選択します。また、必要に応じて、DNS サーバーも追加することができます。
14. 必要に応じて、**仮想 NIC プロファイル** タブから、仮想 NIC プロファイルを論理ネットワークに追加します。
15. **OK** をクリックします。

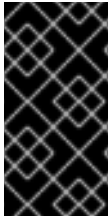
論理ネットワークにラベルを指定した場合には、論理ネットワークは、そのラベルがついた全ホストネットワークインターフェースに自動的に追加されます。



注記

新規論理ネットワークを作成する場合、または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を変更する場合には、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、そのネットワークを使用する実行中の仮想マシンを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



重要

論理ネットワークは、ホスト上のネットワーク設定と同期されていない場合には、編集したり、別のインターフェースに移動したりすることはできません。ネットワークの同期方法については、「[ホストネットワークインターフェー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。

論理ネットワークの編集

1. **コンピュータ** → **データセンター** をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **論理ネットワーク** タブをクリックし、論理ネットワークを選択します。
4. **編集** をクリックします。
5. 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を除き、仮想マシンを停止せずに新規または既存ネットワークの名前を編集することができます。

6. **OK** をクリックします。



注記

マルチホストネットワーク設定により、そのネットワークが割り当てられたデータセンター内の全ホストに、更新したネットワークの設定が自動的に適用されます。変更は、そのネットワークを使用する仮想マシンの停止時にのみ適用することができます。ホスト上ですでに設定済みの論理ネットワークの名前は変更できません。**仮想マシンネットワーク 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は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

ネットワーク → **ネットワーク** または **コンピュータ** → **データセンター** から、論理ネットワークを削除することができます。以下の手順には、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記載します。Red Hat Virtualization 環境が稼働するには、少なくとも 1 つの論理ネットワークを **ovirtmgmt** 管理ネットワークとして使用する必要があります。

論理ネットワークの削除

1. **コンピュータ** → **データセンター** をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **論理ネットワーク** タブをクリックし、データセンター内の論理ネットワークを表示します。
4. 論理ネットワークを選択し、**削除** をクリックします。
5. オプションで、ネットワークが外部プロバイダーから提供されている場合は **このネットワークを外部プロバイダーからも削除する** のチェックボックスにチェックを入れることで、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することができます。外部プロバイ

ダーが読み取り専用モードの場合には、このチェックボックスはグレイアウトします。

6. **OK** をクリックします。

Manager から論理ネットワークが削除され、利用できなくなりました。

6.1.5. デフォルトルートとしての非管理論理ネットワークの設定

クラスター内のホストが使用するデフォルトのルートは、管理ネットワーク (**ovirtmgmt**) 経由です。デフォルトのルートに非管理論理ネットワークを設定する手順を以下に示します。

前提条件:

- **default_route** カスタムプロパティを使用している場合は、アタッチされたすべてのホストからカスタムプロパティの設定を削除してから以下の手順を実施する必要があります。

デフォルトルートロールの設定

1. **ネットワーク** → **ネットワーク** をクリックします。
2. デフォルトルートに設定する非管理論理ネットワークの名前をクリックし、その詳細ビューを表示します。
3. **クラスター** タブをクリックします。
4. **ネットワークの管理** をクリックして **ネットワークを管理** ウィンドウを開きます。
5. 適切なクラスターの **デフォルトルート** チェックボックスを選択します。
6. **OK** をクリックします。

ネットワークがホストにアタッチされると、ホストのデフォルトルートがこのネットワークに設定されます。ホストをクラスターに追加する前に、デフォルトルートロールを設定することを推奨します。ホストがすでにクラスターに含まれている場合は、変更をこれらのホストに同期するまでホストは「非同期」の状態となります。

6.1.6. 論理ネットワークのゲートウェイの表示/編集

論理ネットワークのゲートウェイは、IP アドレスやサブネットマスクと同様にユーザーが定義することができます。これは、1 台のホストに複数のネットワークが存在する場合に、デフォルトのゲートウェイではなく、指定のネットワークを使用してトラフィックをルーティングする必要がある場合に不可欠です。

1 台の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のゲートウェイを使用してルーティングされ、目的の送信先に到達しない可能性があります。その場合には、ユーザーはホストを ping できなくなります。

Red Hat Virtualization は、インターフェースの状態が up または down に切り替わると、自動的に複数のゲートウェイに対応します。

論理ネットワークのゲートウェイの表示/編集

1. **コンピューター** → **ホスト** をクリックします。
2. ホスト名をクリックし、詳細ビューを表示します。

3. **ネットワークインターフェース** タブをクリックし、ホストにアタッチされたネットワークインターフェースおよびその設定を一覧表示します。
4. **ホストネットワークを設定** をクリックします。
5. カーソルで割り当て済み論理ネットワークをポイントし、鉛筆のアイコンをクリックすると、**管理ネットワークの編集** ウィンドウが開きます。

管理ネットワークの編集 ウィンドウには、ネットワーク名、ブートプロトコル、IP アドレス、サブネットマスク、およびゲートウェイのアドレスが表示されます。**静的** ブートプロトコルを選択すると、アドレス情報が手動で編集できる状態になります。

6.1.7. 論理ネットワークの全般の設定

以下の表には、**新規論理ネットワーク** および **論理ネットワークの編集** ウィンドウの **全般** タブの設定についての説明をまとめています。

表6.1 新規論理ネットワーク および 論理ネットワークの編集 の設定

フィールド名	説明
名前	論理ネットワークの名前。このテキストフィールドには、アルファベットの太文字/小文字、数字、ハイフン、アンダースコアを任意に組み合わせた一意名を設定する必要があります。
説明	論理ネットワークの説明。このテキストフィールドは、最長で 40 文字に制限されています。
コメント	論理ネットワークに関する、プレーンテキスト形式の人間が判読できるコメントを追加するためのフィールド
Create on external provider	<p>外部プロバイダーとして Manager に追加済みの OpenStack Networking サービスのインスタンスに論理ネットワークを作成することができます。</p> <p>外部プロバイダー: 論理ネットワークの作成先となる外部プロバイダーを選択することができます。</p>
VLAN タグ付けを有効にする	VLAN タグ付けは、論理ネットワーク上のネットワークトラフィックすべてに特定の特性を指定するセキュリティ機能です。VLAN タグが付いたトラフィックは、同じ特性を持つインターフェース以外で読み取ることはできません。論理ネットワークで VLAN を使用すると、1 つのネットワークインターフェースを異なる VLAN タグの付いた複数の論理ネットワークに関連付けることができます。VLAN タグ付けを有効にする場合は、テキスト入力フィールドに数値を入力してください。

フィールド名	説明
仮想マシンネットワーク	そのネットワークを仮想マシンのみが使用する場合には、このオプションを選択します。ネットワークが仮想マシンには関係のないトラフィック (例: ストレージ用の通信など) に使用される場合には、このチェックボックスは選択しないでください。
MTU	デフォルト を選択して論理ネットワークの最大転送単位 (MTU) を括弧内の値に設定するか、 カスタム を選択してカスタムの MTU を設定します。この設定を使用すると、新規論理ネットワークがサポートする MTU 値と、そのネットワークがインターフェース接続するハードウェアがサポートする MTU 値を適合させることができます。 カスタム を選択した場合は、テキスト入力フィールドに数値を入力してください。
ネットワークラベル	ネットワークの新規ラベルを指定したり、ホストネットワークインターフェースにすでにアタッチされている既存のラベルから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、論理ネットワークは、そのラベルが付いた全ホストネットワークインターフェースに自動的に割り当てられます。

6.1.8. 論理ネットワークのクラスターの設定

以下の表には、**新規論理ネットワーク** ウィンドウの **クラスター** タブの設定についての説明をまとめています。

表6.2 新規論理ネットワーク の設定

フィールド名	説明
--------	----

フィールド名	説明
クラスターに対するネットワークのアタッチ/デタッチ	<p>データセンター内のクラスターに論理ネットワークをアタッチ/デタッチして、その論理ネットワークが個別のクラスターの必須ネットワークとなるかどうかを指定することができます。</p> <p>名前: 設定を適用するクラスターの名前。この値は編集できません。</p> <p>すべてをアタッチ: データセンター内の全クラスターに論理ネットワークをアタッチ/デタッチすることができます。もしくは、各クラスター名の横にある アタッチ チェックボックスを選択または選択解除して、特定のクラスターに論理ネットワークをアタッチ/デタッチします。</p> <p>すべて必須: その論理ネットワークを全クラスター上の必須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。もしくは、各クラスター名の横にある 必須 チェックボックスを選択または選択解除して、特定のクラスターでその論理ネットワークを必須ネットワークとするかどうかを指定します。</p>

6.1.9. 論理ネットワークの仮想 NIC プロファイルの設定

以下の表には、**新規論理ネットワーク** ウィンドウの **仮想 NIC プロファイル** タブの設定についての説明をまとめています。

表6.3 新規論理ネットワーク の設定

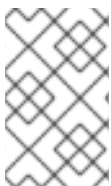
フィールド名	説明
仮想 NIC プロファイル	<p>対象の論理ネットワークに 1 つまたは複数の仮想 NIC プロファイルを指定することができます。仮想 NIC プロファイルの横にあるプラスまたはマイナスのボタンをクリックすると、論理ネットワークに仮想 NIC プロファイルを追加または削除することができます。最初のフィールドには、仮想 NIC プロファイルの名前を入力します。</p> <p>パブリック: 対象のプロファイルを全ユーザーが利用できるかどうかを指定することができます。</p> <p>QoS: ネットワークのサービス品質 (QoS) プロファイルを仮想 NIC プロファイルに指定することができます。</p>

6.1.10. ネットワークの管理ウィンドウでの論理ネットワークへの特定トラフィックタイプの指定

論理ネットワークのトラフィックタイプを指定して、ネットワークトラフィックのフローを最適化します。

論理ネットワークのトラフィックタイプの指定

1. コンピュート → クラスター をクリックします。
2. クラスター名をクリックして、詳細ビューを表示します。
3. 論理ネットワーク タブをクリックします。
4. ネットワークを管理 をクリックします。
5. 該当するチェックボックスおよびラジオボタンを選択します。
6. OK をクリックします。



注記

外部プロバイダーが提供する論理ネットワークは、仮想マシンネットワークとして使用する必要があり、ディスプレイや移行などの特別なクラスターロールを割り当てることはできません。

6.1.11. ネットワークの管理ウィンドウの設定

以下の表には、ネットワークの管理 ウィンドウの設定についての説明をまとめています。

表6.4 ネットワークの管理の設定

フィールド	説明/アクション
割り当て	論理ネットワークをクラスター内の全ホストに割り当てます。
必須	関連付けられているホストが正常に機能するためには、「必須」とマークされているネットワークは稼働状態を維持する必要があります。必須ネットワークが機能を停止すると、そのネットワークに関連付けられたホストはいずれも非稼働状態となります。
仮想マシンネットワーク	「仮想マシンネットワーク」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」とマークされている論理ネットワークは、SPICE および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	「移行ネットワーク」とマークされている論理ネットワークは、仮想マシンおよびストレージの移行トラフィックを伝送します。

6.1.12. NIC の Virtual Function 設定の編集

Single Root I/O Virtualization (SR-IOV) により、単一の PCIe エンドポイントを複数の別個のデバイスとして使用できるようになります。これは、Physical Function (PF) と Virtual Function (VF) の 2 つの PCIe 機能を導入することによって実現します。1 つの PCIe カードには 1 から 8 までの PF を使用することができますが、各 PF は、それよりもはるかに多くの VF をサポートすることが可能です (デバイスによって異なります)。

各 NIC 上の VF 数や VF にアクセス可能な仮想ネットワークの指定などを含む SR-IOV 対応のネットワークインターフェースコントローラー (NIC) の設定は、Red Hat Virtualization Manager で編集することが可能です。


VF の作成が完了したら、各 VF をスタンドアロンの NIC と同様に扱うことができます。これには、1 つまたは複数の論理ネットワークを VF に割り当てたり、VF でボンディングされたインターフェースを作成したり、仮想 NIC を直接割り当てて直接のデバイスパススルーを可能にしたりするなどが含まれます。

仮想 NIC を VF に直接アタッチするには、仮想 NIC でパススルーを有効化する必要があります。「[仮想 NIC 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。

NIC の Virtual Function 設定の編集

1. コンピュート → ホスト をクリックします。
2. SR-IOV 対応ホストの名前をクリックして、詳細ビューを表示します。
3. ネットワークインターフェース タブをクリックします。
4. ホストネットワークを設定 をクリックします。



5.  のマークが付いた SR-IOV 対応の NIC を選択し、鉛筆アイコンをクリックします。
6. Virtual Function の数を編集するには、**VF 設定数** のドロップダウンボタンをクリックして、**VF 数** 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、新規 VF が作成される前にそのネットワークインターフェース上の以前の VF は削除されます。これには、仮想マシンが直接アタッチされていた VF も含まれます。

7. 全ネットワーク チェックボックスはデフォルトで選択され、全ネットワークが Virtual Function にアクセスすることができます。Virtual Function にアクセス可能な仮想ネットワークを指定するには、**特定のネットワーク** ラジオボタンを選択して、全ネットワークの一覧を表示してから、指定するネットワークのチェックボックスを選択するか、**ラベル** テキストフィールドを使用して 1 つまたは複数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します。
8. **OK** をクリックします。
9. ホストのネットワーク設定 ウィンドウで **OK** をクリックします。

6.2. 仮想ネットワークインターフェースカード

6.2.1. 仮想 NIC プロファイルの概要

仮想ネットワークインターフェースカード (仮想 NIC) のプロファイルは、Manager 内の個別の仮想マシンネットワークインターフェースに適用することができる設定値の集合体です。仮想 NIC プロファイルにより、ネットワーク QoS プロファイルを 仮想 NIC に適用して、ポートミラーリングを有効化/無効化したり、カスタムプロパティを追加/削除したりできます。また、仮想 NIC プロファイルにより、管理における柔軟性が向上します。プロファイルを使用 (消費) するためのパーミッションを特定のユーザーに付与することができるので、特定のネットワークから異なるユーザーに提供されるサービス品質を制御することができます。

6.2.2. 仮想 NIC プロファイルの作成と編集

ユーザーおよびグループ用のネットワーク帯域幅を制御するための仮想ネットワークインターフェースコントローラー (仮想 NIC) プロファイルを作成/編集します。



注記

ポートミラーリングを有効化/無効化する場合には、変更する前に、関連付けられたプロファイルを使用している仮想マシンをすべて停止状態にする必要があります。

仮想 NIC プロファイルの作成と編集

1. **ネットワーク** → **ネットワーク** をクリックします。
2. 論理ネットワーク名をクリックし、詳細ビューを表示します。
3. **仮想 NIC プロファイル** タブをクリックします。
4. **新規作成** または **編集** をクリックします。
5. プロファイルの **名前** と **説明** を入力します。
6. **QoS** 一覧から対象の QoS を選択します。
7. 仮想マシンとの間で送受信するネットワークパケットのトラフィックを管理するには、ドロップダウンリストから **ネットワークフィルター** を選択します。ネットワークフィルターに関する詳しい情報は、『**Red Hat Enterprise Linux 仮想化の導入および管理ガイド**』の「**ネットワークフィルター機能の適用**」を参照してください。
8. 仮想 NIC でパススルーを有効化して Virtual Function のデバイスの直接割り当てができるようにするには、**パススルー** チェックボックスを選択します。パススルーのプロパティを有効にすると、QoS、ネットワークフィルター、およびポートミラーリングは互換性がないため無効になります。パススルーに関する詳しい説明は、「**仮想 NIC 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。
9. **パススルー** を選択した場合は、オプションとして **移行可能** チェックボックスのチェックを外し、このプロファイルを使用する仮想 NIC の移行を無効にします。このチェックボックスを選択したままにする場合は、『**仮想マシン管理ガイド**』の「**SR-IOV 対応 vNIC を持つ仮想マシンに対する追加の前提条件**」を参照してください。
10. **ポートミラーリング** および **全ユーザーにこのプロファイルの使用を許可する** の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。
11. カスタムプロパティの一覧からカスタムプロパティを 1 つ選択します。このフィールドには、デフォルトで **キーを選択してください** と表示されます。+ および - のボタンを使用して、カスタムプロパティを追加または削除します。
12. **OK** をクリックします。

このプロファイルをユーザーおよびグループに適用して、ネットワーク帯域幅を制御してください。仮想 NIC プロファイルを編集した場合には、仮想マシンを再起動するか、仮想 NIC をホットアンプラグしてからホットプラグする必要があります (ゲストオペレーティングシステムが仮想 NIC のホットプラグ/ホットアンプラグに対応している場合)。

6.2.3. 仮想マシンインターフェースのプロファイルウィンドウの設定

表6.5 仮想マシンインターフェースの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	仮想 NIC プロファイルを適用することができるネットワークのドロップダウンリスト
名前	仮想 NIC プロファイルの名前。1 - 50 文字のアルファベットの大文字/小文字、数字、ハイフン、アンダースコアを任意に組み合わせた一意名にする必要があります。
説明	仮想 NIC プロファイルの説明。このフィールドは、必須ではありませんが、記入することを推奨します。
QoS	仮想 NIC プロファイルに適用する利用可能なネットワーク QoS ポリシーのドロップダウンリスト。QoS ポリシーは仮想 NIC の受信/送信トラフィックを制御します。
ネットワークフィルター	<p>仮想 NIC プロファイルに適用可能なネットワークフィルターのドロップダウンリスト。ネットワークフィルターは、仮想マシンとの間で送受信できるパケットのタイプをフィルタリングすることにより、ネットワークのセキュリティを強化します。デフォルトのフィルターは vdsm-no-mac-spoofing です。これは、no-mac-spoofing と no-arp-mac-spoofing を組み合わせたフィルターです。libvirt によって提供されるネットワークフィルターについての詳しい情報は、『Red Hat Enterprise Linux 仮想化の導入および管理ガイド』の「既存のネットワークフィルター」のセクションを参照してください。</p> <p>仮想マシンの VLAN およびボンディングには <ネットワークフィルターなし> を使用すべきです。信頼されている仮想マシンでは、ネットワークフィルターを使用しないと、パフォーマンスを向上させることができます。</p>

フィールド名	説明
パススルー	<p>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。パススルーにより、仮想 NIC をホストの Virtual Function に直接接続することができます。仮想 NIC 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、パススループロパティは編集できません。</p> <p>パススルーを有効化した場合には、仮想 NIC 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化されます。</p>
移行可能	<p>このプロファイルを使用する仮想 NIC の移行を許可するかどうかを切り替えるチェックボックス。通常の仮想 NIC プロファイルの場合、移行はデフォルトで有効になっています (このチェックボックスが選択され、変更することはできません)。パススルーのチェックボックスを選択すると 移行可能 のチェックボックスが使用可能になり、必要に応じてチェックを外してパススルー仮想 NIC の移行を無効にすることができます。</p>
ポートミラーリング	<p>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。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 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ースにコピーします。デフォルトでは選択されません。詳しくは、『テクニカルリファレンス』の「ポートミラーリング」のセクションを参照してください。</p>
カスタムプロパティ	<p>仮想 NIC 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を選択するためのドロップダウンメニュー。プロパティを追加する場合は + ボタンを、削除する場合は - ボタンを使用します。</p>
全ユーザーにこのプロファイルの使用を許可する	<p>環境内の全ユーザーがこのプロファイルを利用できるかどうかの設定を切り替えるためのチェックボックス。デフォルトで選択されます。</p>

6.2.4. 仮想 NIC プロファイルでのパススルーの有効化

仮想 NIC のパススループロパティにより、SR-IOV を有効化した NIC の Virtual Function (VF) に仮想 NIC を直接接続できるようになります。これにより仮想 NIC はソフトウェアのネットワーク仮想化を迂回して VF に直接接続され、デバイスの直接割り当てが可能になります。

仮想 NIC プロファイルがすでに仮想 NIC にアタッチされている場合には、パススループロパティは有効化できません。以下の手順では、この問題を回避するために新規プロファイルを作成します。仮想 NIC プロファイルでパススルーが有効化されている場合には、同じプロファイルの QoS、ネットワークフィルター、およびポートミラーリングを有効にすることはできません。

SR-IOV、デバイスの直接割り当て、およびそれらを Red Hat Virtualization に実装するにあたってハードウェアの考慮事項に関する詳しい情報は、『[Hardware Considerations for Implementing SR-IOV](#)』を参照してください。

パススルーの有効化

1. **ネットワーク** → **ネットワーク** をクリックします。
2. 論理ネットワーク名をクリックし、詳細ビューを表示します。
3. **仮想 NIC プロファイル** タブをクリックし、その論理ネットワークの全 NIC プロファイルを表示します。
4. **新規作成** をクリックします。
5. プロファイルの **名前** と **説明** を入力します。
6. **パススルー** のチェックボックスを選択します。
7. オプションとして **移行可能** チェックボックスのチェックを外し、このプロファイルを使用する仮想 NIC の移行を無効にします。このチェックボックスを選択したままにする場合は、『[仮想マシン管理ガイド](#)』の「[SR-IOV 対応 vNIC を持つ仮想マシンに対する追加の前提条件](#)」を参照してください。
8. 必要に応じて、カスタムプロパティの一覧からカスタムプロパティを 1 つ選択します。このフィールドには、デフォルトで **キーを選択してください** と表示されます。**+** および **-** のボタンを使用して、カスタムプロパティを追加または削除します。
9. **OK** をクリックします。

仮想 NIC プロファイルがパススルー対応になりました。このプロファイルを使用して仮想マシンを直接 NIC または PCI VF にアタッチするには、その論理ネットワークを NIC にアタッチしてから、パススルーの仮想 NIC プロファイルを使用する任意の仮想マシン上で **PCI** パススルー 対応の新規仮想 NIC を作成します。これらの手順については、それぞれ「[ホストネットワークインターフェースの編集とホストへの論理ネットワークの割り当て](#)」と『[仮想マシン管理ガイド](#)』の「[新規ネットワークインターフェースの追加](#)」のセクションを参照してください。

6.2.5. 仮想 NIC プロファイルの削除

仮想化環境から、仮想 NIC プロファイルを削除します。

仮想 NIC プロファイルの削除

1. **ネットワーク** → **ネットワーク** をクリックします。
2. 論理ネットワーク名をクリックし、詳細ビューを表示します。
3. **仮想 NIC プロファイル** タブをクリックすると、利用可能な仮想 NIC プロファイルが表示されます。
4. プロファイルを 1 つまたは複数選択して **削除** をクリックします。
5. **OK** をクリックします。

6.2.6. 仮想 NIC 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、外部ネットワークプロバイダーとして OpenStack Networking (Neutron) を追加した場合にのみ利用することができます。Red Hat Virtualization Manager からセキュリティグループを作成することはできません。セキュリティグループは、OpenStack から作成する必要があります。詳しくは、『[Red Hat OpenStack Platform ユーザーおよびアイデンティティ管理ガイド](#)』の「[プロジェクトのセキュリティ管理](#)」を参照してください。

OpenStack Networking インスタンスからインポートした、Open vSwitch プラグインを使用するネットワークの仮想 NIC プロファイルにセキュリティグループを割り当てることができます。セキュリティグループとは、厳格に実行されるルールのコレクションで、ユーザーがネットワークインターフェース上で送受信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、セキュリティグループを仮想 NIC プロファイルにアタッチする方法を説明します。



注記

セキュリティグループは、OpenStack Networking インスタンスに登録されたのと同じセキュリティグループの 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グループ ID を確認するには、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
```

仮想 NIC プロファイルへのセキュリティグループの割り当て

1. ネットワーク → ネットワーク をクリックします。
2. 論理ネットワーク名をクリックし、詳細ビューを表示します。
3. **仮想 NIC プロファイル** タブをクリックします。
4. **新規作成** をクリックするか、既存の仮想 NIC プロファイルを選択して **編集** をクリックします。
5. カスタムプロパティ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のドロップダウンを空欄のままにした場合には、デフォルトのセキュリティグループが適用されます。デフォルトのセキュリティ設定は、すべての送信トラフィックと内部通信を許可しますが、デフォルトのセキュリティグループ外からの受信トラフィックはすべて拒否します。後で **SecurityGroups** プロパティを削除しても、適用済みのセキュリティグループには影響を及ぼしません。
6. テキストフィールドに仮想 NIC プロファイルにアタッチするセキュリティグループの ID を入力します。
7. **OK** をクリックします。

セキュリティグループが仮想 NIC プロファイルにアタッチされました。そのプロファイルがアタッチされている論理ネットワークを通過するトラフィックはすべて、そのセキュリティグループで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. 仮想 NIC プロファイルのユーザーパーミッション

ユーザーを特定の仮想 NIC プロファイルに割り当てるためのユーザーパーミッションを設定します。プロファイルを使用できるようにするには、**VnicProfileUser** ロールをユーザーに割り当てます。ユー

ザーが特定のプロファイルを使用できないように制限するには、そのプロファイルからユーザーのパーミッションを削除します。

仮想 NIC プロファイルのユーザーパーミッション

1. ネットワーク → 仮想 NIC プロファイル をクリックします。
2. 仮想 NIC プロファイルの名前をクリックし、詳細ビューを表示します。
3. パーミッション タブをクリックすると、そのプロファイルに対する現在のユーザーパーミッションが表示されます。
4. 追加 または 削除 をクリックして、その仮想 NIC 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. ユーザーへのパーミッション追加 ウィンドウで 自分のグループ をクリックし、自分の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パーミッションを付与することができます。

仮想 NIC プロファイルのユーザーパーミッションの設定が完了しました。

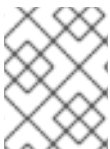
6.2.8. UCS 統合のための仮想 NIC プロファイルの設定

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機能の管理に使用されます。

vdsm-hook-vmfex-dev フックにより、仮想 NIC プロファイルを設定して、仮想マシンは Cisco の UCS で定義されたポートプロファイルに接続することができます。UCS で定義されたポートプロファイルには、UCS 内で仮想インターフェースを設定するのに使用するプロパティと設定が含まれます。**vdsm-hook-vmfex-dev** フックは、VDSM でデフォルトでインストールされます。詳しくは、「[付録A VDSM とフック](#)」を参照してください。

仮想 NIC を使用する仮想マシンを作成する際には、Cisco の仮想 NIC を使用します。

UCS 統合のための仮想 NIC プロファイルの設定手順では、カスタムデバイスプロパティを最初に設定する必要があります。カスタムデバイスプロパティの設定時には、既存の設定値はいずれも上書きされます。新規のカスタムプロパティと既存のカスタムプロパティを組み合わせる場合には、キー値の設定に使用するコマンドにすべてのカスタムプロパティを含めてください。カスタムプロパティを複数指定する場合には、セミコロンで区切ります。



注記

UCS ポートプロファイルは、仮想 NIC プロファイルを設定する前に、Cisco UCS で設定しておく必要があります。

カスタムデバイスプロパティの設定

1. Red Hat Virtualization Manager 上で、**vmfex** のカスタムプロパティを設定し、**--cver** を使用してクラスターの互換レベルを指定します。

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

2. **vmfex** のカスタムプロパティが追加されたことを確認します。


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

3. **ovirt-engine** サービスを再起動します。

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

設定する仮想 NIC プロファイルは、新規または既存の論理ネットワークに属することができます。新規論理ネットワークの設定手順については、「[データセンターまたはクラスター内での新規論理ネットワークの作成](#)」を参照してください。

UCS 統合のための仮想 NIC プロファイルの設定

1. **ネットワーク** → **ネットワーク** をクリックします。
2. 論理ネットワーク名をクリックし、詳細ビューを表示します。
3. **仮想 NIC プロファイル** タブをクリックします。
4. **新規作成** をクリックするか、仮想 NIC プロファイルを選択して **編集** をクリックします。
5. プロファイルの **名前** と **説明** を入力します。
6. カスタムプロパティの一覧から **vmfex** のカスタムプロパティを選択して、UCS ポートプロファイル名を入力します。
7. **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) を使用するには、そのプロバイダーを Manager に登録します。詳しくは、「[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](#)」を参照してから、以下の手順に従って、そのプロバイダーによって提供されているネットワークを Manager にインポートし、仮想マシンがそのネットワークを使用できるようにします。

外部プロバイダーからのネットワークのインポート

1. **ネットワーク** → **ネットワーク** をクリックします。
2. **インポート** をクリックします。
3. **ネットワークプロバイダー** の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。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** 一覧に表示されます。
4. チェックボックスを使用して、**プロバイダーネットワーク** 一覧からインポートするネットワークを選択し、下向きの矢印をクリックしてそのネットワークを **インポートするネットワーク** 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は、カスタマイズすることが可能です。名前をカスタマイズするには、**名前** のコラムでそのネットワークの名前をクリックして編集します。

6. **データセンター** ドロップダウンリストから、ネットワークのインポート先となるデータセンターを選択します。
7. オプションとして、ネットワークの使用が全ユーザーに許可されないようにするには、**全ユーザーに許可** チェックボックスのチェックを外します。
8. **インポート** をクリックします。

選択したネットワークは、ターゲットの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。詳しくは、『[仮想マシン管理ガイド](#)』の「[新規ネットワークインターフェースの追加](#)」のセクション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おける制限事項

以下の制限事項は、Red Hat Virtualization 環境内の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の使用に適用されます。

- 外部プロバイダーから提供される論理ネットワークは、仮想マシンネットワークとして使用する必要があり、ディスプレイネットワークとしては使用できません。
- 同じ論理ネットワークを複数回インポートすることが可能ですが、インポート先が異なるデータセンターの場合のみです。
- 外部プロバイダーによって提供される論理ネットワークは、Manager 内で編集することはできません。外部プロバイダーによって提供される論理ネットワークの情報を編集するには、その論理ネットワークを提供する外部プロバイダーから直接、論理ネットワークを編集する必要があります。
- ポートミラーリングは、外部プロバイダーによって提供され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ースカードには使用できません。
- 外部プロバイダーが提供する論理ネットワークを仮想マシンが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により使用されている間は、Manager からそのプロバイダーを削除することはできません。
- 外部プロバイダーによって提供されるネットワークは、必須ではありません。このため、そのような論理ネットワークがインポートされたクラスターのスケジューリングでは、ホストの選択中にそれらの論理ネットワークは考慮されません。また、そのような論理ネットワークがインポートされたクラスター内のホスト上の論理ネットワークの可用性を確保するのは、ユーザーの責任となります。

6.3.3. 外部プロバイダーの論理ネットワーク上のサブネット設定

外部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に 1 つ以上のサブネットが定義されていないと、仮想マシンに IP アドレスを割り当てることができません。サブネットが定義されていない場合は、仮想マシンには IP アドレスが割り当てられません。またサブネットが 1 つの場合は、そのサブネットから仮想マシンに IP アドレスが割り当てられ、サブネットが複数ある場合は、使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。論理ネットワークをホストす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る役割を果たします。

Red Hat Virtualization Manager では、インポートされた論理ネットワーク上で事前定義されているサブネットが自動的に検出されますが、Manager 内で論理ネットワークにサブネットを追加したり、サブネットを削除したりすることも可能です。

6.3.4. 外部プロバイダーの論理ネットワークへのサブネット追加

外部プロバイダーが提供する論理ネットワークにサブネットを作成します。

外部プロバイダーの論理ネットワークへのサブネット追加

1. **ネットワーク** → **ネットワーク** をクリックします。
2. 論理ネットワーク名をクリックし、詳細ビューを表示します。
3. **サブネット** タブをクリックします。
4. **新規作成** をクリックします。
5. 新規サブネットの **名前** と **CIDR** を入力します。
6. **IP バージョン** のドロップダウンリストから、**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。

6.3.5. 外部プロバイダーの論理ネットワークからのサブネット削除

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。

外部プロバイダーの論理ネットワークからのサブネット削除

1. **ネットワーク** → **ネットワーク** をクリックします。
2. 論理ネットワーク名をクリックし、詳細ビューを表示します。
3. **サブネット** タブをクリックします。
4. サブネットを選択し、**削除** をクリックします。
5. **OK** をクリックします。

6.4. ホストとネットワーク

6.4.1. ホストの機能のリフレッシュ

ホストにネットワークインターフェースカードを追加した場合は、Manager でそのネットワークインターフェースカードを表示するには、そのホストの機能をリフレッシュする必要があります。

ホストの機能のリフレッシュ

1. **コンピュー**ト → **ホスト** をクリックし、ホストを選択します。
2. **管理** → **機能をリフレッシュ** をクリックします。

選択したホストの **ネットワークインターフェース** タブのネットワークインターフェースカードの一覧が更新され、Manager で新しいネットワークインターフェースカードを使用できるようになりました。

6.4.2. ホストネットワークインターフェースの編集とホストへの論理ネットワークの割り当て

物理ホストのネットワークインターフェースの設定を変更して、物理ホストのネットワークインターフェース間で管理ネットワークを移動し、物理ホストのネットワークインターフェースに論理ネット

ワークを割り当てることができます。ブリッジおよび `ethtool` のカスタムプロパティーもサポートされています。



警告

Red Hat Virtualization でホストの IP アドレスを変更するには、ホストを削除してから、再度追加するのが唯一の方法です。

ホストの VLAN 設定を変更するには、そのホストを Manager から削除し、再設定してから、Manager に再度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、ホストをメンテナンスモードに切り替えて、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 を介して到達できるようになります。次に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 が変更されると、以下のような警告が表示されます。

管理ネットワークの特定のプロパティー（例：VLAN、MTU）を変更すると、配下のネットワークインフラストラクチャーがそのような変更に対応するように設定されていない場合には、データセンター内のホストへの接続が切断される可能性があります。操作を続行してもよろしいですか？

続行すると、データセンター内の全ホストが Manager に接続できなくなり、新規管理ネットワークへのホストの移行は失敗します。管理ネットワークは「非同期」と報告されます。



重要

外部プロバイダーによって提供されてい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ースには割り当てられません。そのようなネットワークは、仮想マシンの要求に応じて、ホストに動的に割り当てられます。



注記

Link Layer Discovery Protocol (LLDP) 情報を提供するようにスイッチが設定されている場合、カーソルで物理ネットワークインターフェースをポイントして、スイッチポートの現在の設定を表示することができます。この機能は、誤設定を防止するのに役立ちます。Red Hat では、論理ネットワークを割り当てる前に以下の情報を確認することを推奨します。

- **port description (TLV タイプ 4)** および **system name (TLV タイプ 5)** は、ホストのインターフェースがパッチされるポート/スイッチを把握するのに役立ちます。
- **Port VLAN ID** には、タグ付けされていないイーサネットフレームのスイッチポートに設定されたネイティブ VLAN ID が表示されます。スイッチポートに設定されたすべての VLAN が、**VLAN Name** と **VLAN ID** の組み合わせで表示されます。

ホストネットワークインターフェースの編集とホストへの論理ネットワークの割り当て

1. コンピュート → ホスト をクリックします。
2. ホスト名をクリックし、詳細ビューを表示します。
3. ネットワークインターフェース タブをクリックします。
4. ホストネットワークを設定 をクリックします。
5. オプションとして、カーソルでホストネットワークインターフェースをポイントして、スイッチから提供される設定情報を表示します。
6. 論理ネットワークを物理ホストに割り当てるには、その論理ネットワークを選択して、その物理ホストのネットワークインターフェースの横にある **割り当て済み論理ネットワーク** のエリアにドラッグします。
もしくは、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ースを選択します。
7. 論理ネットワークを設定します。
 - a. カーソルで割り当て済み論理ネットワークをポイントし、鉛筆のアイコンをクリックすると、**管理ネットワークの編集** ウィンドウが開きます。
 - b. **IPv4** タブで、**ブートプロトコル** になし、**DHCP**、**静的** のいずれかを選択します。**静的** を選択した場合には、**IP アドレス**、**ネットマスク / ルーティングプレフィックス**、および **ゲートウェイ** を入力してください。



注記

各論理ネットワークには、管理ネットワークゲートウェイで定義されている別のゲートウェイを使用することができます。これにより、論理ネットワークに到着したトラフィックは、管理ネットワークが使用するデフォルトの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ので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のネットワーク QoS を上書きします。**QoS** を上書きを選択して、以下のフィールドに必要な値を入力します。
 - **加重シェア**: 特定のネットワークに割り当てる論理リンクのキャパシティを、同じ論理リンクにアタッチされた他のネットワークに対して相対的に示します。シェアの具体的な値は、そのリンク上の全ネットワークのシェアの和によって異なります。デフォルトでは、これは、1 - 100 の範囲内の数値です。
 - **速度の上限 [Mbps]**: ネットワークが使用する最大帯域幅
 - **コミット速度 [Mbps]**: ネットワークに必要な最小の帯域幅。要求されるコミット速度は保証されず、ネットワークインフラストラクチャーや同じ論理リンク上の他のネットワークに要求されるコミット速度によって異なります。
- d. ネットワークブリッジを設定するには、**カスタムプロパティ** タブをクリックして、ドロップダウンリストから **bridge_opts** を選択します。有効なキーと値を **key=value** の構文

で入力します。エントリーが複数ある場合は、空白文字で区切ります。以下のキーが有効です (値は例として提示しています)。これらのパラメーターに関する詳しい説明は、[「bridge_opts パラメーター」](#)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. イーサネットのプロパティを設定するには、**カスタムプロパティ** タブをクリックして、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を使用して有効な値を入力します。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
```

このフィールドではワイルドカードを使用することができます。たとえば、このネットワークの全インターフェースに同じオプションを適用するには、以下のように指定します。

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

ethtool_opts オプションはデフォルトでは利用できないので、engine 設定ツールを使用して追加する必要があります。詳しくは、[「Red Hat Virtualization Manager で Ethtool を使用するための設定方法」](#)を参照してください。ethtool のプロパティに関する詳しい情報は、コマンドラインで **man ethtool** と入力して 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、**カスタムプロパティ** タブをクリックして、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。少なくとも **enable=yes** が必要です。**dcb=** と **auto_vlan=[yes|no]** を追加することもできます。エントリーが複数の場合には空白文字で区切ってください。**fcoe** のオプションはデフォルトでは利用できないので、engine 設定ツールを使用して追加する必要があります。詳しくは、[「Red Hat Virtualization Manager で FCoE を使用するための設定方法」](#)を参照してください。



注記

FCoE には、別の専用論理ネットワークを使用することを推奨します。

- g. ホストが使用するデフォルトネットワークを管理ネットワーク (ovirtmgmt) から非管理ネットワークに変更するには、非管理ネットワークのデフォルトルートを設定します。詳細については、「[デフォルトルートとしての非管理論理ネットワークの設定](#)」を参照してください。
- h. 論理ネットワークの定義がホスト上のネットワーク設定と同期されていない場合には、**ネットワークを同期** のチェックボックスを選択します。論理ネットワークが同期されるまでは、その論理ネットワークを編集したり、他のインターフェースに移動したりすることはできません。



注記

以下のいずれかの条件が該当する場合には、ネットワークは同期されていると見なされません。

- **仮想マシンネットワーク** が物理ホストのネットワークと異なる場合。
- **VLAN ID** が物理ホストのネットワークと異なる場合。
- **カスタム** の **MTU** が論理ネットワークで設定済みで、かつ物理ホストのネットワークと異なる場合。

- 8. ネットワーク接続をチェックするには、**ホストと Engine 間の接続を検証** のチェックボックスを選択します。この操作は、ホストがメンテナンスモードに入っている場合にのみ機能します。
- 9. 環境をリブートした時に変更が維持されるようにするには、**ネットワーク設定を保存** のチェックボックスを選択します。
- 10. **OK** をクリックします。

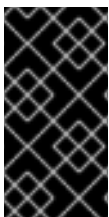


注記

ホストの全ネットワークインターフェースカードが表示されない場合には、**管理 → 機能をリフレッシュ** 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ースカードの一覧を更新します。

6.4.3. 論理ネットワークを使用した単一ネットワークインターフェースへの複数の VLAN 追加

単一のネットワークインターフェースに複数の VLAN を追加することにより、1 台のホスト上のトラフィックを分離することができます。



重要

そのためには、あらかじめ複数の論理ネットワークを作成しておく必要があります。それらの論理ネットワークにはすべて、**新規論理ネットワーク** または **論理ネットワークの編集** のウィンドウで **VLAN タグ付けを有効にする** のチェックボックスにチェックを入れてください。

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ースへの複数の VLAN 追加

1. **コンピューター → ホスト** をクリックします。

2. ホスト名をクリックし、詳細ビューを表示します。
3. ネットワークインターフェース タブをクリックします。
4. ホストネットワークを設定 をクリックします。
5. VLAN タグの付いた論理ネットワークを物理ネットワークインターフェースの横にある **割り当て済み論理ネットワーク** のエリアにドラッグします。VLAN タグ付けにより、物理ネットワークインターフェースに複数の論理ネットワークを割り当てることができます。
6. 論理ネットワークを編集します。
 - a. カーソルで割り当て済み論理ネットワークをポイントし、鉛筆のアイコンをクリックします。
 - b. 論理ネットワークの定義がホスト上のネットワーク設定と同期されていない場合には、**ネットワークを同期** のチェックボックスを選択します。
 - c. 次のいずれかの **ブートプロトコル** を選択します。
 - なし
 - DHCP
 - 静的
 - d. **IP アドレス と ネットマスク / ルーティングプレフィックス** を入力します。
 - e. **OK** をクリックします。
7. ネットワークのチェックを実行するには、**ホストと Engine 間の接続を検証** のチェックボックスを選択します。この検証は、ホストがメンテナンスモードに入っている場合にのみ機能します。
8. **ネットワーク設定を保存** チェックボックスを選択します。
9. **OK** をクリックします。

クラスター内のホストの NIC を編集して、各ホストに論理ネットワークを追加します。この作業が完了すると、ネットワークが稼働するようになります。

この手順を繰り返して、各ホストで同じネットワークインターフェースを選択/編集し、単一のネットワークインターフェースに異なる VLAN タグの付いた論理ネットワークを各ホストに追加することができます。

6.4.4. 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、初回の設定では IP アドレスが1つのみで作成されます。このため、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でも、ホストネットワークに割り当てられるのは最初にリストされている IP アドレスのみとなります。ストレージへの接続や、同じ NIC を使用する別のプライベートサブネット上のサーバーへの接続に、追加の IP アドレスが必要となる場合があります。

vdsm-hook-extra-ipv4-addrs フックにより、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。フックに関する詳しい情報は、「[付録A VDSM とフック](#)」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。

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。このパッケージは、Red Hat Virtualization Host ではデフォルトで利用可能ですが、Red Hat Enterprise Linux ホストにはインストールする必要があります。

```
# yum install vdsd-hook-extra-ipv4-addr
```

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 **コンピュータ** → **ホスト** をクリックします。
5. ホスト名をクリックし、詳細ビューを表示します。
6. **ネットワークインターフェース** タブをクリックして、**ホストネットワークを設定** をクリックします。
7. カーソルで割り当て済み論理ネットワークをポイントして鉛筆のアイコンをクリックし、ホストのネットワークインターフェースを編集します。
8. **カスタムプロパティ** のドロップダウンリストから **ipv4_addr** を選択して追加の IP アドレスとプレフィックス (例: 5.5.5.5/24) を指定します。IP アドレスを複数指定する場合にはコンマで区切る必要があります。
9. **OK** をクリックします。
10. **ネットワーク設定を保存** チェックボックスを選択します。
11. **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** コマンドを実行すると、追加されているかどうかを確認できます。

6.4.5. ホストネットワークインターフェー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ことによって、ホストネットワークインターフェースへの論理ネットワーク割り当てに伴う管理ワークロードを大幅に簡素化することができます。



注記

ローカルネットワーク (例: 移行ネットワークやディスプレイネットワークなど) にラベルを設定すると、そのネットワークが全ホストに一括でデプロイされます。このようなネットワークの一括追加は、DHCP を使用して処理されます。この方法による一括デプロイは、静的アドレスを入力する方法よりも優先されます。これは、多数の静的 IP アドレスを入力する作業が性質上スケーラブルでないことが理由です。

ホストネットワークインターフェースへのネットワークラベルの追加

1. **コンピュータ** → **ホスト** をクリックします。
2. ホスト名をクリックし、詳細ビューを表示します。
3. **ネットワークインターフェース** タブをクリックします。
4. **ホストネットワークを設定** をクリックします。
5. **ラベル** をクリックして **[新規ラベル]** を右クリックします。ラベルを付ける物理ネットワークインターフェースを選択します。
6. **ラベル** のテキストフィールドにネットワークラベル名を入力します。
7. **OK** をクリックします。

ホストネットワークインターフェースにネットワークラベルが追加されました。同じラベルで新規作成される論理ネットワークはいずれも、そのラベルが付いたホストネットワークインターフェー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、その論理ネットワークは、そのラベルが付いた全ホストネットワークインターフェースから自動的に削除されます。

6.4.6. Red Hat Virtualization におけるボンディングロジック

Red Hat Virtualization Manager 管理ポータルでは、グラフィカルインターフェースを使用してボンディングデバイスを作成することができます。ボンディング作成には複数の異なるシナリオがあり、それぞれに独自のロジックが適用されます。

ボンディングロジックに影響を及ぼす 2 つの要因:

- いずれかのデバイスが論理ネットワークをすでに伝送しているかどうか。
- デバイスは、互換性のある論理ネットワークを伝送しているかどうか。

表6.6 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
NIC + NIC	<p>新規ボンディングの作成 ウィンドウが表示され、新規ボンディングデバイスを設定することができます。</p> <p>ネットワークインターフェースが互換性のない論理ネットワークを伝送している場合には、新規ボンディングを形成するデバイスから互換性のない論理ネットワークをデタッチするまで、ボンディング操作は失敗します。</p>

ボンディングシナリオ	結果
NIC + Bond	<p>NIC がボンディングデバイスに追加されます。NIC とボンディングデバイスが伝送する各論理ネットワークに互換性がある場合には、それらの論理ネットワークはすべて、この操作で作成されるボンディングデバイスに追加されます。</p> <p>ボンディングデバイスが互換性のない論理ネットワークを伝送している場合には、新規ボンディングを形成するデバイスから互換性のない論理ネットワークをデタッチするまで、ボンディング操作は失敗します。</p>
Bond + Bond	<p>ボンディングデバイスが論理ネットワークにアタッチされていない場合、または互換性のある論理ネットワークにアタッチされている場合には、新規ボンディング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ースが含まれ、ボンディングを構成するデバイスの全論理ネットワークを伝送します。新規ボンディングの作成 ウィンドウが表示され、新規ボンディングの設定を行うことができます。</p> <p>ボンディングデバイスが互換性のない論理ネットワークを伝送している場合には、新規ボンディングを形成するデバイスから互換性のない論理ネットワークをデタッチするまで、ボンディング操作は失敗します。</p>

6.4.7. ボンディングモード

ボンディングとは、複数のネットワークインターフェースをソフトウェアで定義したデバイス 1 つに集約することです。ボンディングされたネットワークインターフェースは、ボンディングに含まれているネットワークインターフェースカード (NIC) の伝送機能を統合して、1 つのネットワークインターフェースとして機能するため、単一の NIC よりも伝送速度が早くなります。また、ボンディング内の NIC すべてに障害が発生しない限り、ボンディング自体には障害が発生しないため、ボンディングすることでフォールトトレランスが向上します。ただし、一点制約があり、ボンディング内のすべてのネットワークインターフェースカードが同じオプションやモードをサポートするように、ネットワークインターフェースをボンディングする NIC は、必ず同じメーカーおよびモデルでなければなりません。

ボンディングのパケット分散アルゴリズムは、使用するボンディングモードによって決定されます。



重要

モード 1、2、3、4 は、仮想マシン (ブリッジ) および物理マシン (ブリッジなし) のネットワークタイプをサポートします。モード 0、5、6 は、物理マシン (ブリッジなし) のネットワークのみをサポートします。

Red Hat Virtualization は、デフォルトでモード 4 を使用しますが、以下にあげる一般的なボンディングモードに対応しています。

モード 0 (round-robin ポリシー)

このモードは、ネットワークインターフェースカードを順番に使用してパケットを送信します。パケットの送信は、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ースカードから、最後に利用可能なネットワークインターフェースカードまでループで使用をくり返します。それ以降のループでもすべて、最初に利用可能なネットワークインターフェースカードから使用されます。モード 0 では、ネットワークに対して耐障害性や負荷分散が提供されていますが、ブリッジと併用できないため、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)

このモードは、すべてのネットワークインターフェースカードをバックアップ状態に設定して、1 つだけアクティブなカードを残します。アクティブなネットワークインターフェースカードで障害が発生すると、バックアップに設定されていたネットワークインターフェースカードの 1 つが、障害の発生したインターフェースに代わって、ボンディング内で唯一のアクティブインターフェースになります。1 つ以上のポートでアドレスが表示されていると、有効なネットワークインターフェースカードの MAC アドレスを反映するためにボンディングの MAC アドレスが変更された場合に混乱が生じる可能性があり、このような混乱を避ける目的で、モード 1 のボンディングの MAC アドレスは、1 つのポートだけで表示されます。モード 1 は耐障害性を提供し、Red Hat Virtualization でサポートされています。

モード 2 (XOR ポリシー)

このモードは、送信元と送信先の MAC アドレスの XOR (排他的理論和) をネットワークインターフェースカードのスレーブ数で除算した剰余に基づいて、パケット送信に用いるネットワークインターフェースカードを選択します。この計算により、各送信先の MAC アドレスに必ず同じネットワークインターフェースカードが選択されるようにします。モード 2 は耐障害性と負荷分散を提供し、Red Hat Virtualization でサポートされています。

モード 3 (broadcast ポリシー)

このモードは、全パケットをすべてのネットワークインターフェースカードに送信します。モード 3 は耐障害性を提供し、Red Hat Virtualization でサポートされています。

モード 4 (IEEE 802.3ad ポリシー)

このモードは、任意の集約グループを作成し、このグループ内のインターフェースが速度およびデュプレックスの設定を共有します。モード 4 は、IEEE 802.3ad 仕様に従ってアクティブな集約グループ内のネットワークインターフェースカードをすべて使用します。このモードも、Red Hat Virtualization でサポートされています。

モード 5 (adaptive transmit load balancing ポリシー)

このモードは、ボンディング内の各ネットワークインターフェースカードの負荷に応じて発信トラフィックが分散され、現在のネットワークインターフェースカードが全着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ているネットワークインターフェースカードに障害が発生した場合には、着信トラフィックの受信ロールは別のネットワークインターフェースカードに割り当てられます。モード 5 はブリッジと併用できないため、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 6 (adaptive load balancing ポリシー)

このモードは、モード 5 (adaptive transmit load balancing ポリシー) に IPv4 トラフィックの受信負荷分散を組み合わせたポリシーで、特別なスイッチ要件はありません。ARP ネゴシエーションを使用して受信負荷の分散を行います。モード 6 はブリッジと併用できないため、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。

6.4.8. 管理ポータルを使用したボンディングデバイスの作成

互換性のある複数のネットワークデバイスをボンディングしてまとめることができます。このタイプの設定を使用することで帯域幅と信頼度が高まります。ボンディングは、複数のネットワークインターフェース、既存のボンディングデバイス、この 2 つを組み合わせたものに対して適用することができます。ボンディングは VLAN タグ付きのトラフィックと、VLAN タグなしのトラフィックの両方を伝送することができます。



注記

Link Layer Discovery Protocol (LLDP) 情報を提供するようにスイッチが設定されている場合、カーソルで物理ネットワークインターフェースをポイントして、スイッチポートの現在の集約設定を表示することができます。Red Hat では、ボンディングデバイスを作成する前に設定を確認することを推奨します。

管理ポータルを使用したボンディングデバイスの作成

1. **コンピュータ** → **ホスト** をクリックします。
2. ホスト名をクリックし、詳細ビューを表示します。
3. **ネットワークインターフェース** タブをクリックし、ホストにアタッチされた物理ネットワークインターフェースを一覧表示します。
4. **ホストネットワークを設定** をクリックします。
5. オプションとして、カーソルでホストネットワークインターフェースをポイントして、スイッチから提供される設定情報を表示します。
6. 一方のデバイスを選択して、他方のデバイスの上にドラッグアンドドロップすると、**新規ボンディングの作成** ウィンドウが開きます。または、一方のデバイスを右クリックして、他方のデバイスをドロップダウンメニューから選択します。
デバイスに互換性がない場合には、ボンディングの操作は失敗して、互換性問題の解決方法を示したメッセージが表示されます。
7. ドロップダウンメニューから **ボンディング名** および **ボンディングモード** を選択します。
ボンディングモード 1、2、4、5 を選択することができます。その他のモードを設定するには、**カスタム** オプションを使用します。
8. **OK** をクリックしてボンディングを作成し、**新規ボンディングの作成** ウィンドウを閉じます。
9. 新規作成したボンディングデバイスに論理ネットワークを割り当てます。
10. オプションとして、**ホストと Engine 間の接続を検証** および **ネットワーク設定を保存** を選択することができます。
11. **OK** をクリックします。

複数のネットワークデバイスが1つのボンディングデバイスにリンクされ、単一のインターフェースとして編集できるようになりました。このボンディングデバイスは、選択したホストの **ネットワークインターフェース** タブに表示されます。

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化する手順は、スイッチによって若干異なります。ボンディング有効化に関する詳しい情報は、そのスイッチのメーカーが提供しているマニュアルを参照してください。



注記

モード 4 のボンディングの場合には、スイッチで全スレーブを正しく設定する必要があります。スイッチで正しく設定されているスレーブが1つもない場合には、**ad_partner_mac** は 00:00:00:00:00:00 として報告されます。Manager は **ネットワークインターフェース** タブのボンディングに感嘆符のアイコンで警告を表示します。いずれかのスレーブが稼働している場合には警告は表示されません。

6.4.9. ホストインターフェースのカスタムボンディングオプションの使用例

新規ボンディングの作成 ウィンドウで **ボンディングモード** から **カスタム** を選択すると、カスタマイズされたボンディングデバイスを作成することができます。以下の例は、必要に応じて適用してください。ボンディングオプションとその説明をまとめた包括的なリストは、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、多数の異なる IP アドレス間のトラフィックが大半の場合には、IP アドレス別に負荷分散するようにポリシーを設定することができます。この負荷分散ポリシーを設定するには、**カスタム** ボンディングモードを選択して、テキストフィールドに以下の値を入力します。

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

例6.2 ARP モニタリング

ARP モニターは、ethtool を介して適切にリンク状態を報告できない、もしくは報告しないシステムに有用です。ホストのボンディングデバイスに **arp_interval** を設定するには、**カスタム** ボンディングモードを選択して、テキストフィールドに以下の値を入力します。

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

例6.3 プライマリー

ボンディングデバイス内のプライマリーインターフェースとして、特定の NIC により高いスループットを指定する必要がある場合があります。プライマリーとなる NIC を指定するには、**カスタム** ボンディングモードを選択して、テキストフィールドに以下の値を入力します。

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

6.4.10. ホストの完全修飾ドメイン名の変更

ホストの完全修飾ドメイン名を変更するには、以下の手順に従ってください。

ホストの完全修飾ドメイン名の更新

1. ホストをメンテナンスモードに切り替えて、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。詳しい説明は、『[ホストのメンテナンスモードへの切り替え](#)』を参照してください。または、全仮想マシンを手動でシャットダウンして、別のホストに移行します。詳しくは、『[仮想マシン管理ガイド](#)』の『[手動での仮想マシン移行](#)』のセクションを参照してください。
2. **削除** をクリックしてから **OK** をクリックし、管理ポータルからホストを削除します。
3. ホスト名を更新するには、**hostnamectl** ツールを使用します。その他のオプションについては、『[Red Hat Enterprise Linux 7 ネットワークガイド](#)』の『[ホスト名の設定](#)』の章を参照してください。

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

4. ホストをリブートします。
5. Manager でホストを再登録します。詳しい情報は「[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. ホストについて

ホストとは、仮想マシンを実行する物理サーバーで、ハイパーバイザーとしても知られています。Kernel-based Virtual Machine (KVM) と呼ばれる読み込み可能な Linux カーネルモジュールを使用することにより、完全仮想化が提供されます。

KVM は、Windows または Linux 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実行することができます。仮想マシンは、ホストマシン上で個別の Linux プロセスおよび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 環境には、単一または複数のホストをアタッチすることができます。

Red Hat Virtualization はホストのインストールで 2 つのメソッドをサポートしており、Red Hat Virtualization Host (RHVH) インストールメディアを使用する方法または標準の Red Hat Enterprise Linux の環境にハイパーバイザーのパッケージをインストールする方法のいずれかを使用することができます。



注記

Red Hat Virtualization Manager では、個々のホストのホストタイプを特定することができます。ホスト名を選択して詳細ビューを表示し、ソフトウェアセクションの **OS の説明** を確認してください。

ホストは、**tuned** プロファイルを使用して仮想化を最適化します。**tuned** に関する詳しい情報は、[『Red Hat Enterprise Linux 7 パフォーマンスチューニングガイド』](#)を参照してください。

Red Hat Virtualization Host ではセキュリティ機能が有効化されています。Security Enhanced Linux (SELinux) およびファイアウォールがデフォルトで完全に設定済みで、有効な状態となっています。選択したホストの SELinux ステータスは、詳細ビューにある **全般** タブの **SELinux モード** に表示されます。Manager が Red Hat Enterprise Linux ホストを環境に追加する際には、そのホスト上の必要なポートを開くことができます。

ホストは、Red Hat Enterprise Linux 7 (AMD64/Intel 64 バージョン) を実行する Intel VT または AMD-V 拡張機能搭載の 64 ビットの物理サーバーです。

Red Hat Virtualization プラットフォームの物理ホストの要件は次のとおりです。

- システム内の単一のクラスターにのみ属していること。
- AMD-V または Intel VT ハードウェア仮想化拡張機能をサポートする CPU が搭載されていること。
- クラスター作成時に選択した仮想 CPU タイプで公開される全機能をサポートする CPU が搭載されていること。
- 最小で 2 GB の RAM が搭載されていること。
- システムパーミッションを持つシステム管理者を 1 名指定可能であること。

管理者は、Red Hat Virtualization のウォッチリスト (rhev-watch-list) から最新のセキュリティアドバイザリーを受信することができます。Red Hat Virtualization 製品に関するセキュリティアドバイザリーをメールで受信するには、Red Hat Virtualization ウォッチリストをサブスクライブします。以下のフォームで登録してください。

[RHSA-announce -- Security announcements for all Red Hat products and services.](#)

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で構成される 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。RHVH は、Red Hat Enterprise Linux ホストに使用される **Anaconda** のインストールインターフェースを使用し、Red Hat Virtualization Manager または **yum** で更新が可能です。追加のパッケージをインストールして、アップグレード後にもそれらが永続されるようにするには、**yum** コマンドを使用するのが唯一の方法です。

RHVH には、ホストのリソースのモニタリングと管理タスク実行のためのユーザーインターフェースである Cockpit の機能があります。SSH またはコンソールを使用した RHVH への直接のアクセスはサポートされていないので、Cockpit のユーザーインターフェースは、Red Hat Virtualization Manager にホストを追加する前のタスク (例: ネットワークの設定、セルフホストエンジンのデプロイなど) のためのグラフィカルユーザーインターフェースを提供します。また、Cockpit のユーザーインターフェースを使用して、**端末** のサブタブからターミナルコマンドを実行することもできます。

Web ブラウザーで、<https://HostFQDNorIP:9090> を開いて、Cockpit ユーザーインターフェー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、カスタムの **Virtualization** ダッシュボードが搭載されています。

RHVH では、アプリケーションのクラッシュに関する有用なデバッグ情報を収集するために、自動バグ報告ツール (ABRT) が使われています。詳細については、『[Red Hat Enterprise Linux システム管理者のガイド](#)』を参照してください。



注記

grubby ツールを使用して、カスタムのブートカーネル引数を Red Hat Virtualization Host に追加することが可能です。**grubby** ツールは、**grub.cfg** ファイルに永続的な変更を加えます。**grubby** コマンドを使用するには、ホストの Cockpit ユーザーインターフェースで **端末** サブタブにナビゲートします。詳しくは、『[Red Hat Enterprise Linux システム管理者のガイド](#)』を参照してください。



警告

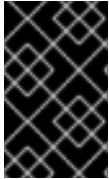
ローカルのセキュリティ脆弱性が攻撃される可能性があるため、Red Hat は RHVH に信頼できないユーザーを作成することは推奨しません。

7.3. RED HAT ENTERPRISE LINUX ホスト

Red Hat Enterprise Linux 7 を対応するハードウェアにインストールして、ホストとして使用することができます。Red Hat Virtualization は、Intel VT または AMD-V 拡張機能搭載の AMD64/Intel 64 バージョン Red Hat Enterprise Linux 7 サーバーを実行するホストをサポートしています。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** エンタイトルメントをアタッチする必要もあります。

ホストを追加するには、プラットフォームにより、仮想化の確認、パッケージのインストール、ブリッジの作成などのタスクが実行されるため、多少時間がかかる場合があります。ホストと管理システムが接続を確立する際のプロセスをモニタリングするには、詳細ビューを使用してください。

オプションとして、ホストのリソースのモニタリングと管理タスク実行のために Cockpit のユーザーインターフェースをインストールすることができます。Cockpit のユーザーインターフェースは、Red Hat Virtualization Manager にホストを追加する前のタスク (例: ネットワークの設定、セルフホストエンジンのデプロイなど) のためのグラフィカルユーザーインターフェースを提供します。また、Cockpit のユーザーインターフェースを使用して、**端末** のサブタブからターミナルコマンドを実行することもできます。



重要

サードパーティ製のウォッチドッグは、VDSM によって提供される watchdog デモンを妨げる可能性があるため、Red Hat Enterprise Linux ホストにはインストールすべきではありません。

7.4. SATELLITE ホストプロバイダーのホスト

Red Hat Virtualization Manager では、Satellite ホストプロバイダーによって提供されるホストを仮想化ホストとして使用することができます。Satellite ホストプロバイダーが外部プロバイダーとして Manager に追加された後には、その Satellite ホストプロバイダーが提供するホストはすべて、Red Hat Virtualization に追加して Red Hat Virtualization Host (RHVH) や Red Hat Enterprise Linux ホストと同じように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、およびブリッジの作成の各ステップをプラットフォームで完了する必要があるため、多少時間がかかります。ホストと Manager 間での接続確立の進行状況は、詳細ビューで確認してください。

Red Hat Virtualization Manager へのホストの追加

1. **コンピューター** → **ホスト** をクリックします。
2. **新規作成** をクリックします。
3. ドロップダウンリストを使用して、新規ホスト用の **データセンター** および **ホストクラスター** を選択します。
4. 新規ホストの **名前** と **ホスト名** を入力します。**SSH ポート** フィールドには、標準の SSH ポートであるポート 22 が自動入力されます。
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 公開鍵** フィールドに表示される鍵をホスト上の `/root/.ssh/authorized_keys` にコピーして、公開鍵認証を使用します。
6. **詳細パラメーター** ボタンをクリックして、ホストの詳細設定を展開します。
 - a. オプションとして、ファイアウォールの自動設定を無効にすることができます。
 - b. オプションとして、ホストの SSH フィンガープリントを追加し、セキュリティを強化することができます。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**、**カーネル** を設定します。詳しくは、「[新規ホストおよびホストの編集ウィンドウの設定とコントロール](#)」を参照してください。**セルフホストエンジン** は、セルフホストエンジンのデプロイまたはアンデプロイ時に使用します。

8. **OK** をクリックします。

新規ホストが **Installing** のステータスでホスト一覧に表示され、詳細ビューでインストールの進捗状況を確認することができます。しばらくすると、ホストのステータスが **Up** に変わります。



重要

環境を最新の状態に維持してください。詳細については、「[How do I update my Red Hat Virtualization system?](#)」を参照してください。既知の問題に対するバグ修正が頻繁にリリースされることから、Red Hat ではホストおよび Manager の更新タスクをスケジュール化することを推奨します。

7.5.2. Satellite ホストプロバイダーのホストの追加

Satellite ホストプロバイダーのホストを追加する手順は、Manager でホストを特定する方法を除いては、Red Hat Enterprise Linux ホストを追加する手順とほぼ同じです。以下の手順では、Satellite ホストプロバイダーによって提供されるホストを追加する方法について説明します。

Satellite ホストプロバイダーのホストの追加

1. **コンピューター → ホスト** をクリックします。
2. **新規作成** をクリックします。
3. ドロップダウンメニューで、新規ホスト用の **ホストクラスター** を選択します。
4. **Foreman/Satellite を使用する** のチェックボックスを選択して、Satellite ホストプロバイダーを追加するための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. **検出されたホスト** または **プロビジョン済みホスト** のいずれかを選択します。
 - **検出されたホスト** (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、コンピュートリソースを選択します。
 - **プロビジョン済みホスト**: **プロバイダーのホスト** のドロップダウンリストからホストを1つ選択します。
外部プロバイダーから取得可能なホストに関する情報は、自動的に設定され、必要に応じて編集することができます。
6. 新規ホストの **名前** および **SSH ポート** (プロビジョン済みホストのみ) を入力します。
7. ホストに使用する認証の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。
 - 公開鍵認証を使用するには、**SSH 公開鍵** フィールドに表示される鍵をホスト上の `/root/.ssh/authorized_hosts` にコピーします (プロビジョン済みホストのみ)。
8. 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。次に、**詳細パラメーター** の展開ボタンをクリックして、ホストの詳細設定を表示します。
 - a. オプションとして、ファイアウォールの自動設定を無効にすることができます。

- b. オプションとして、ホストの SSH フィンガープリントを追加し、セキュリティを強化することができます。手動での追加または自動取得が可能です。
9. 該当するタブで **電源管理**、**SPM**、**コンソール**、および **ネットワークプロバイダー** を設定することができる状態になりました。ただし、これらの設定は、Red Hat Enterprise Linux ホストの追加に必須ではないため、このセクションでは説明していません。
10. **OK** をクリックしてホストを追加し、ウィンドウを閉じます。

新規ホストが **Installing** のステータスでホスト一覧に表示され、詳細ビューでインストールの進捗状況を確認することができます。インストールが完了するとステータスは **Reboot** になります。ステータスを **Up** に変えるには、ホストをアクティブ化する必要があります。

7.5.3. ホストを対象とする **Satellite** のエラータ管理の設定

Red Hat Virtualization では、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、ホストの管理者は、ホストの設定の管理に使用すると同じ画面で、利用可能なエラータの更新とそれらの重大度についての情報を受信することができます。Red Hat Satellite に関する詳しい情報は、『[Red Hat Satellite User Guide](#)』を参照してください。

Red Hat Virtualization 4.2 では、Red Hat Satellite 6.1 を使用したエラータ管理をサポートしています。



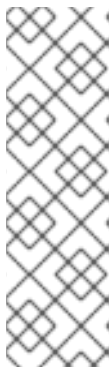
重要

Satellite サーバー内では、ホストは FQDN で識別されます。IP アドレスを使用して追加されたホストは、エラータを報告できません。このため、外部コンテンツホストの ID を Red Hat Virtualization で維持管理する必要があります。

ホストの管理に使用する Satellite のアカウントには、管理者の権限とデフォルトの組織を設定する必要があります。

ホストを対象とする **Satellite** のエラータ管理の設定

1. Satellite サーバーを外部プロバイダーとして追加します。詳しい説明は、『[ホスト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. 対象のホストを Satellite サーバーに関連付けます。



注記

ホストは、Satellite サーバーにコンテンツホストとして登録し、**katello-agent** パッケージをインストールする必要があります。

ホスト登録の設定方法についての詳しい情報は、『[Red Hat Satellite User Guide](#)』の『[Configuring a Host for Registration](#)』のセクションを参照してください。また、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に関する詳しい情報は、『[Red Hat Satellite User Guide](#)』の『[Registration](#)』のセクションを参照してください。

- a. **コンピュータ** → **ホスト** をクリックし、ホストを選択します。
- b. **編集** をクリックします。
- c. **Foreman/Satellite** を使用する チェックボックスを選択します。

d. ドロップダウンリストから対象の Satellite サーバーを選択します。

e. **OK** をクリックします。

ホストの設定が完了し、ホストの設定を管理するのと同じ画面で、利用可能なエラータとその重大度が表示されるようになりました。

7.5.4. 新規ホストおよびホストの編集ウィンドウの設定とコントロール

7.5.5. ホストの全般の設定

以下の設定は、ホストの詳細を編集したり、Red Hat Enterprise Linux ホストおよび Satellite ホストプロバイダーのホストを新規追加したりする際に適用されます。

全般 の設定の表には、**新規ホスト** または **ホストの編集** ウィンドウの **全般** タブに必要な情報をまとめています。

表7.1 全般 の設定

フィールド名	説明
ホストクラスター	ホストが属するクラスターおよびデータセンター

フィールド名	説明
Foreman/Satellite を使用する	<p>Satellite ホストプロバイダーによって提供されるホストを追加するためのオプションを表示/非表示にするには、このチェックボックスを選択/選択解除します。以下のオプションを設定することができます。</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: engine によって検出された Satellite ホストの名前が含まれるドロップダウンリスト ● 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 ● コンピュータリソース: コンピュータ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 <p>プロビジョン済みホスト</p> <ul style="list-style-type: none"> ● プロバイダーのホスト: 選択した外部プロバイダーによって提供されるホストの名前が記載されたドロップダウンリスト。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 のフィールドに入力した検索クエリーに応じてフィルターされます。 ● 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によって提供されるホストを検索することができ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形成に関する詳しい情報は、そのプロバイダーのマニュアルを参照してください。利用可能なホストをすべて表示するには、このフィールドは空欄のままにします。
名前	ホストの名前。このテキストフィールドは最長で 40 文字に制限されており、アルファベットの大文字/小文字、数字、ハイフン、アンダースコアを任意に組み合わせた一意名にする必要があります。
コメント	ホストに関する、プレーンテキスト形式の人間が判読できるコメントを追加するためのフィールド
ホスト名	ホストの IP アドレス、または解決可能なホスト名
パスワード	ホストの root ユーザーのパスワード。ホストを追加する時にのみ指定することができ、それ以降は編集できません。

フィールド名	説明
SSH 公開鍵	ホストとの認証で、パスワードを使用する代わりに Manager の SSH キーを使用する場合には、テキストボックスの内容をホストの <code>/root/.ssh/authorized_hosts</code> ファイルにコピーします。
ホストのファイアウォールを自動設定する	新規ホストを追加する際には、Manager がホストのファイアウォール上の必要なポートを開くことができます。この設定はデフォルトで有効化されています。これは 詳細パラメーター です。
SSH フィンガープリント	ホストの SSH フィンガープリントを 取得 して、ホストが返すはずのフィンガープリントと比較し、それらが一致しているかどうかを確認することができます。これは 詳細パラメーター です。

7.5.6. ホストの電源管理の設定

電源管理 の設定の表には、**新規ホスト** または **ホストの編集** ウィンドウの **電源管理** タブに必要な情報をまとめています。電源管理は、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設定できます。

表7.2 電源管理 の設定

フィールド名	説明
電源管理を有効にする	ホストで電源管理を有効にします。このチェックボックスを選択して、 電源管理 タブの残りのフィールドを有効にします。
kdump 統合	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 以降のバージョンでは、kdump はデフォルトで利用可能です。ホストで kdump が利用可能であっても、設定が有効でない (kdump サービスが起動できない) 場合には、 kdump 統合 を有効にすると、ホストのインストールが失敗します。このようなエラーが発生した場合には、 「fence_kdump の詳細設定」 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 で設定されている スケジューリングポリシー によって制御されます。電源管理を有効にすると、ホストの使用率が定義済みの下限値に達した場合、Manager はそのホストマシンの電源を遮断し、負荷分散で必要となった場合やクラスター内で使用可能なホストが十分でない場合にそのホストを再起動します。ポリシー制御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
<p>順次に使用するエージェント</p>	<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は、順次、同時、またはそれらの両方を組み合わせて使用することができます。</p> <ul style="list-style-type: none"> フェンスエージェントが順次に使用される場合には、ホストの停止/起動にまず 1 番目のエージェントが使用され、失敗すると 2 番目のエージェントが使用されます。 フェンスエージェントが同時に使用される場合、ホストが停止するには、両方のエージェントが停止のコマンドに応答する必要があります。1 つのエージェントが起動のコマンドに応答すると、ホストが起動します。 <p>デフォルトでは、フェンスエージェントは順次に使用されます。フェンスエージェントの使用順序を変更するには、上向き/下向きのボタンを使用してください。</p> <p>2 つのフェンスエージェントを同時に使用するには、一方のフェンスエージェントの横にある 同時に使用するフェンスエージェント のドロップダウンリストからもう一方のフェンスエージェントを選択します。同時に使用するフェンスエージェントのグループにフェンスエージェントをさらに追加するには、その追加のフェンスエージェントの横にある 同時に使用するフェンスエージェント ドロップダウンリストから対象のグループを選択して設定することができます。</p>
<p>フェンスエージェントの追加</p>	<p>+ のボタンをクリックして、新規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 ウィンドウが開きます。以下の表には、このウィンドウのフィールドについての詳しい説明をまとめています。</p>

フィールド名	説明
電源管理プロキシの設定	デフォルトでは、Manager がホストと同じ cluster 内のフェンシングプロキシを検索するように指定されます。フェンシングプロキシが見つからない場合には、Manager は同じ dc (データセンター) 内を検索します。これらのリソースの使用順序を変更するには、上向き/下向きのボタンを使用します。このフィールドは、 詳細パラメーター の下にありません。

以下の表には、フェンスエージェントの**編集** ウィンドウに必要な情報をまとめています。

表7.3 フェンスエージェントの編集 の設定

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を入力します。
ユーザー名	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てください。
パスワード	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

フィールド名	説明
タイプ	<p>ホストの電源管理デバイスのタイプ。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には使用できません。 • apc_snmp: APC 5.x 電源スイッチデバイスに使用 • bladecenter: IBM Bladecenter 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: HP BladeSystem • 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 Adapter • rsb: Fujitsu-Siemens RSB 管理インターフェース • wti: WTI Network Power Switch <p>電源管理デバイスの詳細については、『テクニカルリファレンス』の「電源管理」を参照してください。</p>
SSH 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
スロット	電源管理デバイスのブレードの特定に使用する番号
サービスプロファイル	電源管理デバイスのブレードの特定に使用するサービスプロファイル名。このフィールドは、デバイスタイプが cisco_ucs の場合に スロット フィールドの代わりに表示されます。

フィールド名	説明
オプション	<p>電源管理デバイス固有のオプション。「key=value」として指定します。使用可能なオプションについては、ホストの電源管理デバイスのマニュアルを参照してください。</p> <p>Red Hat Enterprise Linux 7 ホストで、電源管理デバイスに <code>cisco_ucs</code> を使用する場合には、オプション フィールドに <code>ssl_insecure=1</code> を追記する必要があります。</p>
セキュリティー保護	<p>電源管理デバイスがホストにセキュアに接続できるようにするには、このチェックボックスを選択します。この接続には、電源管理エージェントに応じて、ssh、ssl、またはその他の認証プロトコルを使用することができます。</p>

7.5.7. SPM 優先度の設定

SPM の設定の表には、**新規ホスト** または **ホストの編集** ウィンドウの **SPM** タブに必要な情報をまとめています。

表7.4 SPM の設定

フィールド名	説明
SPM 優先度	<p>ホストに Storage Pool Manager (SPM) のロールが割り当てられる優先度を定義します。優先度のオプションは、低、標準、高 です。優先度が低の場合は、そのホストに SPM のロールが割り当てられる確率が低くなり、高の場合は確率が高くなります。デフォルト設定は標準です。</p>

7.5.8. ホストのコンソールの設定

コンソール の設定の表には、**新規ホスト** または **ホストの編集** ウィンドウの **コンソール** タブに必要な情報をまとめています。

表7.5 コンソール の設定

フィールド名	説明
--------	----

フィールド名	説明
表示アドレスを上書き	ホストの表示アドレスを上書きするには、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 アドレスで定義され、かつ 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すると、仮想マシンを実行しているホストのプライベートアドレスの代わりに、パブリック IP アドレスまたは FQDN (外部ネットワークでパブリック IP アドレスに解決される) がそのマシンによって返されます。
表示アドレス	このフィールドに指定する表示アドレスは、そのホスト上で実行する全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 アドレスの形式にする必要があります。

7.5.9. ネットワークプロバイダーの設定

ネットワークプロバイダー の設定の表には、**新規ホスト** または **ホストの編集** ウィンドウの **ネットワークプロバイダー** タブに必要な情報をまとめています。

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済みで、その外部ネットワークプロバイダーでホストのネットワークをプロビジョニングする場合は、該当するプロバイダーを一覧から選択します。

7.5.10. カーネルの設定

カーネル の設定の表には、**新規ホスト** または **ホストの編集** ウィンドウの **カーネル** タブに必要な情報をまとめています。一般的なカーネルブートパラメーターのオプションは、チェックボックスとしてリストされるので簡単に選択できます。より複雑な変更の場合は、**カーネルコマンドライン** の自由形式のテキスト入力欄を使用して必要なパラメーターを追加します。



重要

ホストが Manager にすでにアタッチ済みの場合には、変更を適用する前に、そのホストをメンテナンスモードに必ず切り替えてください。**インストール** → **再インストール** をクリックしてホストを再インストールする必要があります。再インストールが完了したら、ホストを再起動して変更を有効にしてください。

表7.7 カーネル の設定

フィールド名	説明
--------	----

フィールド名	説明
ホストデバイスパススルー & SR-IOV	カーネルで IOMMU フラグを有効にすると、ホストのデバイスは、仮想マシン自体に直接アタッチされているかのような状態で、仮想マシンが使用できるようになります。これには、ホストのハードウェアとファームウェアも IOMMU をサポートしている必要があります。また、仮想化拡張機能と IOMMU 拡張機能をハードウェアで有効にする必要があります。『インストールガイド』の「 PCI パススルーを有効にするためのホストの設定 」を参照してください。IBM POWER8 では IOMMU はデフォルトで有効化されています。
ネストされた仮想化	vmx または svm フラグを有効にすると、仮想マシン内で仮想マシンを実行できるようになります。このオプションは、評価目的でのみ提供されており、実稼働目的ではサポートされていません。これには、ホストに vdsm-hook-nestedvt フックをインストールしておく必要があります。
安全でない割り込み	ハードウェアが再マッピングの割り込みをサポートしていないことが原因で IOMMU が有効化されているのにも拘らず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してみてください。このオプションは、ホスト上の仮想マシンが信頼されている場合にのみ有効にすべきである点に注意してください。このオプションを有効にすることによって、仮想マシンからホストが MSI 攻撃に晒される可能性があります。このオプションは、認定されていないハードウェアを評価目的で使用する場合に、回避策として使用することのみを目的としています。
PCI 再割り当て	メモリーの問題が原因で SR-IOV NIC が Virtual Function を割り当てることができない場合には、このオプションを有効化することを検討してください。ホストのハードウェアとファームウェアも PCI の再割り当てをサポートしている必要があります。このオプションは、認定されていないハードウェアを評価目的で使用する場合に、回避策として使用することのみ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、デフォルトのカーネルパラメーターに追加のパラメータを追記することができます。



注記

カーネルのブートパラメーターがグレイアウトしている場合には、**リセット** ボタンをクリックするとこのオプションが利用できるようになります。

7.5.11. セルフホストエンジンの設定

セルフホストエンジン の設定の表には、**新規ホスト** または **ホストの編集** ウィンドウの **セルフホストエンジン** タブに必要な情報をまとめています。

表7.8 セルフホストエンジン の設定

フィールド名	説明
セルフホストエンジンのデプロイメントアクションの選択	<p>以下の 3 つのオプションがあります。</p> <ul style="list-style-type: none"> ● NONE: アクションは必要ありません。 ● DEPLOY: セルフホストエンジンノードとしてホストをデプロイするには、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には、このオプションを選択してホストをアンデプロイし、セルフホストエンジンに関連した設定を削除することができます。

7.5.12. ホストの電源管理設定の定義

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) を行うには、ホストの電源管理デバイス設定値を設定します。

ホストおよび仮想マシンの高可用性を活用するには、ホストの電源管理設定を行う必要があります。電源管理デバイスの詳細については、『[テクニカルリファレンス](#)』の「[電源管理](#)」を参照してください。

電源管理設定の定義

1. **コンピュー**ト → **ホスト** をクリックし、ホストを選択します。
2. **管理** → **メンテナンス** をクリックし、**OK** をクリックして確定します。
3. ホストがメンテナンスモードに切り替わったら、**編集** をクリックします。
4. **電源管理** タブをクリックします。
5. **電源管理を有効にする** のチェックボックスを選択し、フィールドを有効にします。
6. **kdump 統合** 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** を有効にする場合には、kdump を設定するためにその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。

7. オプションで、ホストの **クラスター のスケジューリングポリシー** がホストの電源管理を制御しないようにするには、**電源管理のポリシー制御を無効にする** のチェックボックスを選択します。
8. プラス (+) のボタンをクリックして、新規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** ウィンドウが開きます。
9. 電源管理デバイスの **ユーザー名** および **パスワード** を該当するフィールドに入力します。
10. ドロップダウンリストで電源管理デバイスの **タイプ** を選択します。
11. **アドレス** フィールドに IP アドレスを入力します。
12. 電源管理デバイスがホストとの通信に使用する **SSH ポート** 番号を入力します。
13. 電源管理デバイスのブレードの特定に使用する **スロット** 番号を入力します。
14. 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てください。
 - IPv4 および IPv6 IP アドレスの両方を使用することができる場合は (デフォルト)、**オプション** フィールドを空欄のままにしてください。
 - IPv4 の IP アドレスしか使用することができない場合は、**inet4_only=1** と入力します。
 - IPv6 の IP アドレスしか使用することができない場合は、**inet6_only=1** と入力します。
15. 電源管理デバイスからホストへのセキュアな接続を有効にするには、**セキュリティー保護** のチェックボックスを選択します。
16. **テスト** をクリックして、設定が正しいことを確認します。検証が正常に完了すると、「**Test Succeeded, Host Status is: on**」というメッセージが表示されます。
17. **OK** をクリックして **フェンスエージェントの編集** ウィンドウを閉じます。
18. **電源管理** タブでは、オプションとして **詳細パラメーター** の箇所を展開し、上下に移動するボタンを使用して Manager がフェンシングプロキシを探す際に使用するリソース (**cluster** および **dc** (データセンター)) の順序を指定します。
19. **OK** をクリックします。

管理ポータルで、**管理** → **電源管理** のドロップダウンメニューが有効になりました。

7.5.13. ホストの **Storage Pool Manager** 設定の定義

Storage Pool Manager (SPM) とは、ストレージドメインに対するアクセス制御を維持管理するためにデータセンター内のホストに割り当てられる管理ロールです。SPM は常に稼働状態である必要があります。SPM ホストが使用不可となった場合には、SPM ロールは別のホストに割り当てられます。SPM ロールは、そのホストの使用可能なリソースを一部使用するので、リソースに余裕のあるホストの優先度を高く設定することが重要となります。

ホストの Storage Pool Manager (SPM) 優先度設定により、SPM ロールが割り当てられる可能性を変更することができます。SPM 優先度の高いホストには、SPM 優先度の低いホストよりも先に SPM ロールが割り当てられます。

SPM 設定の定義

1. **コンピューター** → **ホスト** をクリックします。
2. **編集** をクリックします。
3. **SPM** タブをクリックします。
4. ラジオボタンで、そのホストに適切な SPM 優先度を選択します。
5. **OK** をクリックします。

7.5.14. ホストのメンテナンスモードへの切り替え

ネットワーク設定やソフトウェアアップデートのデプロイメントなど、多くの一般的なメンテナンスタスクを行う際には、ホストをメンテナンスモードに切り替える必要があります。再起動や、ネットワークまたはストレージの問題で、VDSM が正しく機能しなくなる事態が発生する前に、ホストをメンテナンスモードに切り替える必要があります。

ホストをメンテナンスモードに切り替えると、Red Hat Virtualization Manager は稼働中の全仮想マシンを別のホストに移行しようと試みます。この場合には、ライブマイグレーションの標準の前提条件が適用されます。特に、クラスター内には、移行された仮想マシンを実行するキャパシティーのあるアクティブなホストが少なくとも 1 台必要です。



注記

ホストに固定されていて移行することのできない仮想マシンは、シャットダウンされます。どの仮想マシンがホストに固定されているかを確認するには、ホストの詳細ビューの **仮想マシン** タブで **ホストに固定済み** をクリックしてください。

ホストのメンテナンスモードへの切り替え

1. **コンピューター** → **ホスト** をクリックし、対象のホストを選択します。
2. **管理** → **メンテナンス** をクリックすると **ホストのメンテナンス** の確認ウィンドウが開きます。
3. オプションとして、ホストをメンテナンスモードに切り替える **理由** を入力します。この理由は、ログとホストの再アクティブ化時に表示されます。



注記

ホストのメンテナンスの **理由** フィールドは、クラスターの設定で有効化されている場合にのみ表示されます。詳しくは、[「クラスターの全般の設定」](#)を参照してください。

4. オプションとして、Gluster をサポートするホストに必要なオプションを選択します。
デフォルトの確認を避けるには、**Gluster クォーラムと自己修復の検証を無視する** のオプションを選択します。デフォルトでは、ホストがメンテナンスモードに切り替わる際に、Manager は Gluster クォーラムが失われないことを確認します。Manager は、ホストをメンテナンスモードに切り替えることで影響を受ける自己修復作業がないことも確認します。Gluster クォー

ラムの喪失や影響を受ける自己修復作業がある場合、Manager はホストをメンテナンスモードに切り替えません。このオプションは、これ以外にホストをメンテナンスモードに切り替える手段がない場合にしか使用しないでください。

ホストをメンテナンスモードに切り替える間すべての Gluster サービスを停止するには、**Gluster サービスを停止する** のオプションを選択します。



注記

これらのフィールドは、選択したホストが Gluster をサポートする場合に限り、ホストのメンテナンス ウィンドウに表示されます。詳細については、『**Maintaining Red Hat Hyperconverged Infrastructure**』の「[Replacing the Primary Gluster Storage Node](#)」を参照してください。

5. **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別のホストに移行されます。ホストが Storage Pool Manager (SPM) の場合には、SPM ロールは別のホストに移ります。**ステータス** フィールドが **Preparing for Maintenance** に変わり、操作が正常に完了すると最終的に **Maintenance** となります。VDSM は、ホストのメンテナンスモード中には停止しません。



注記

いずれかの仮想マシンの移行が失敗した場合には、ホストで **管理** → **アクティブ化** をクリックしてメンテナンスモードへの切り替えの操作を停止してから、その仮想マシンで **移行をキャンセル** をクリックし、移行を停止します。

7.5.15. メンテナンスモードのホストのアクティブ化

メンテナンスモードに入っているホストまたは最近環境に追加されたホストを使用するには、アクティブ化する必要があります。ホストの準備が整っていない場合には、アクティブ化が失敗する可能性があります。ホストのアクティブ化を試みる前には、全タスクが完了していることを確認してください。

メンテナンスモードのホストのアクティブ化

1. **コンピュー**ト → **ホスト** をクリックして、ホストを選択します。
2. **管理** → **アクティブ化** をクリックします。

ホストのステータスが **Unassigned** に切り替わり、操作が完了すると最終的には **Up** となります。これで仮想マシンをこのホスト上で実行できるようになりました。このホストをメンテナンスモードに切り替えた際に別のホストに移行されていた仮想マシンは、ホストのアクティブ化時に自動的にこのホストには戻されませんが、手動で移行することができます。メンテナンスモードに切り替える前にホストが Storage Pool Manager (SPM) だった場合には、ホストがアクティブ化されても、SPM ロールは自動的に元には戻りません。

7.5.16. ホストの削除

仮想化環境からホストを削除します。

ホストの削除

1. **コンピュー**ト → **ホスト** をクリックし、ホストを選択します。
2. **管理** → **メンテナンス** をクリックします。

3. ホストがメンテナンスモードに切り替わったら、**削除** をクリックして **ホストの削除** の確認ウィンドウを開きます。
4. ホストが Red Hat Gluster Storage クラスターに属し、ボリュームブリックがある場合、もしくはホストが応答していない場合には、**強制削除** のチェックボックスを選択します。
5. **OK** をクリックします。

7.5.17. マイナーリリース間のホストの更新

ホストを最新の状態に保つためにマイナーリリースの更新を行う方法については、『[アップグレードガイド](#)』の「[ホストの更新](#)」を参照してください。

7.5.18. 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、再起動の操作が含まれます。クラスターレベルでマイグレーションが有効化されている場合には、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ので、ホストの再インストールは、ホストの使用率が比較的に低いときに行うことを推奨します。

ホストが属するクラスターには、ホストがメンテナンスを実行するのに十分なメモリーが確保されている必要があります。メモリーが十分に確保されていないクラスターで稼働中の仮想マシンがあるホストをメンテナンスに切り替えると、仮想マシンの移行の操作がハングして、失敗してしまいます。ホストをメンテナンスに切り替える前に、一部またはすべての仮想マシンをシャットダウンしておく、この操作のメモリー使用量を削減することができます。



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ます。全ホストを同時に再インストールしないようにしてください。Storage Pool Manager (SPM) のタスクを実行するために、ホストが 1 台使用可能である必要があります。

Red Hat Virtualization Host および Red Hat Enterprise Linux ホストの再インストール

1. **コンピュー**ト → **ホスト** をクリックし、ホストを選択します。
2. **管理** → **メンテナンス** をクリックします。クラスターレベルでマイグレーションが有効化されている場合には、このホストで実行中の仮想マシンは別のホストに移行されます。ホストが SPM の場合には、SPM 機能も別のホストに移動します。ホストがメンテナンスモードに入るとステータスが変わります。
3. **インストール** → **再インストール** をクリックすると、**ホストのインストール** ウィンドウが開きます。
4. **OK** をクリックしてホストを再インストールします。

再インストールが正常に完了すると、ホストは **Up** のステータスで表示されます。別のホストに移行された仮想マシンは、この時点で、元のホストに戻すことができます。



重要

Red Hat Virtualization Host が Red Hat Virtualization Manager に正常に登録され、再インストールされた後に、管理ポータルに **Install Failed** のステータスで誤って表示される場合があります。管理 → アクティブ化 をクリックすると、そのホストのステータスは **Up** に変わり、使用できる状態となります。

7.5.19. 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ついての情報を保存しておく、そのタグを基に検索を行うことができます。

タグを使用したホストのカスタマイズ

1. コンピュート → ホスト をクリックし、ホストを選択します。
2. その他の操作 → タグを割り当て をクリックします。
3. 対象のタグのチェックボックスを選択します。
4. OK をクリックします。

ホストに関する、検索可能な補足情報がタグとして追加されます。

7.5.20. ホストのエラータの表示

ホストが Red Hat Satellite サーバーからエラータ情報を受信するように設定した後は、各ホストのエラータを表示することができます。エラータ情報を受信するための設定方法に関する詳しい説明は、「[ホストを対象とする Satellite のエラータ管理の設定](#)」を参照してください。

ホストのエラータの表示

1. コンピュート → ホスト をクリックします。
2. ホスト名をクリックし、詳細ビューを表示します。
3. エラータ タブをクリックします。

7.5.21. ホストのヘルスステータスの確認

ホストには、通常のステータスに加えて外部のヘルスステータスがあります。外部のヘルスステータスはプラグインまたは外部のシステムによってレポートされるか、管理者によって設定され、ホストの名前の左側に以下のアイコンのいずれかが表示されます。

- OK: アイコンなし
- 情報:
- 警告:
- エラー:
- 異常:

ホストのヘルスステータスについての更に詳しい情報を確認するには、ホスト名をクリックして詳細ビューを表示し、イベント タブをクリックしてください。

ホストのヘルスステータスは、REST API を使用して確認することも可能です。ホストに対する **GET** 要求には、ヘルスステータスが記載された **external_status** 要素が含まれます。

events コレクションで REST API 内のホストのヘルスステータスを設定することができます。『**REST API Guide**』の「[Events - add](#)」のセクションを参照してください。

7.5.22. ホストデバイスの表示

詳細ビューの **ホストデバイス** タブで、各ホストのホストデバイスを表示することができます。ホストでデバイスの直接割り当てが設定されている場合には、それらのデバイスを仮想マシンに直接アタッチしてパフォーマンスを向上させることができます。

デバイスを直接割り当てるためのハードウェア要件に関する詳しい情報は、『**Hardware Considerations for Implementing SR-IOV**』の「[Additional Hardware Considerations for Using Device Assignment](#)」を参照してください。

デバイスを直接割り当てるためのホストの設定に関する詳しい情報は、『**インストールガイド**』の「[PCI パススルーを有効にするためのホストの設定](#)」のセクションを参照してください。

ホストデバイスを仮想マシンにアタッチする操作に関する詳しい情報は、『**仮想マシン管理ガイド**』の「[ホストデバイス](#)」のセクションを参照してください。

ホストデバイスの表示

1. **コンピュータ** → **ホスト** をクリックします。
2. ホスト名をクリックし、詳細ビューを表示します。
3. **ホストデバイス** タブをクリックします。

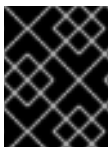
このタブにホストデバイスの詳細が表示され、デバイスが仮想マシンにアタッチされているかどうかや現在その仮想マシンによって使用されているかどうかなどの情報を確認することができます。

7.5.23. GPU パススルーを使用するためのホストおよびゲストシステムの準備

ホストの Graphics Processing Unit (GPU) デバイスを仮想マシンに直接割り当てることが可能です。この操作を実行する前には、ホストと仮想マシンの両方で **grub** 設定ファイルに必要な変更を加える必要があります。ホストの **grub** 設定ファイルは、管理ポータルで **カーネルコマンドライン** の自由形式のテキスト入力欄を使用して編集することができます。変更を有効にするには、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。

以下の手順は、x86_64 または ppc64le アーキテクチャーのホストに適した方法です。

デバイスを直接割り当てるためのハードウェア要件に関する詳しい情報は、『**プランニングおよび前提条件ガイド**』の「[PCI デバイスの要件](#)」のセクションを参照してください。



重要

ホストが Manager にすでにアタッチ済みの場合には、変更を適用する前に、そのホストをメンテナンスモードに必ず切り替えてください。

GPU パススルーを使用するためのホストの準備

1. 管理ポータルで **コンピュータ** → **ホスト** をクリックします。

2. ホスト名をクリックし、詳細ビューを表示します。
3. **全般** タブをクリックして、**ハードウェア** をクリックします。GPU デバイスの **ベンダー ID:製品 ID** を特定します。この例では、ID は **10de:13ba** と **10de:0fbc** です。
4. ホストを右クリックして、**編集** を選択します。**カーネル** タブをクリックします。
5. **カーネルコマンドライン** の自由形式のテキスト入力欄に、前のステップで特定した ID を入力します。

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

6. ホスト上の対応するドライバーをブラックリストします。たとえば、nVidia の nouveau ドライバーをブラックリストするには、**pci-stub.ids=xxxx:xxxx** の後に **rdblacklist=nouveau** と入力します。

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

7. **OK** をクリックします。
8. **インストール** → **再インストール** をクリックして、ホストへの変更をコミットします。
9. 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:0fbc] (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加える方法については、バージョン 3.6 の『[管理ガイド](#)』の「[GPU パススルーに向けたホストおよびゲストシステムの準備](#)」を参照してください。

次の手順に進み、ゲストシステム側で GPU パススルーを設定します。

GPU パススルーを使用するためのゲスト仮想マシンの準備

Linux の場合

1. プロプライエタリーの GPU ドライバーのみがサポートされています。対応するオープンソースのドライバーは、**grub** 設定ファイルでブラックリストしてください。以下に例を示します。

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

- GPU BusID を特定します。以下の例では、BusID は **00:09.0** です。

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

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

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

- 仮想マシンを再起動します。

Windows の場合

- 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」](#) のページにアクセスします。
- 仮想マシンを再起動します。

これで、準備した仮想マシンにホストの GPU を直接割り当てることができるようになりました。ホストデバイスを仮想マシンに割り当てる操作に関する詳しい情報は、『[仮想マシン管理ガイド](#)』の「[ホストデバイス](#)」のセクションを参照してください。

7.5.24. 管理ポータルからの Cockpit へのアクセス

Cockpit は、デフォルトで Red Hat Virtualization Host (RHVH) および Red Hat Enterprise Linux ホストで利用可能です。ブラウザーにアドレスを入力して Cockpit ユーザーインターフェースにアクセスできますが、管理ポータルからアクセスすることも可能です。

管理ポータルからの Cockpit へのアクセス

- 管理ポータルで **コンピュータ** → **ホスト** をクリックして、ホストを選択します。
- ホストコンソール** をクリックします。

新しいブラウザーウィンドウに Cockpit のログインページが開きます。

7.6. ホストの耐障害性

7.6.1. ホストの高可用性

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を応答可能な状態に維

持します。**Non Responsive** のホストは、**Non Operational** のホストとは異なります。Manager は **Non Operational** のホストとは通信することができますが、ホストの設定は正しくありません (例: 論理ネットワークが見つからないなど)。Manager は、**Non Responsive** のホストとは通信できません。

フェンシングにより、クラスターは予期せぬホスト障害に対応可能となり、パワーセービング、負荷分散、および仮想マシンの可用性の各ポリシーが強化されます。ホストの電源管理デバイスにはフェンシングパラメーターを設定し、その正確性を時々テストすることを推奨します。フェンシングの操作では、応答なしのホストがリブートされて、所定時間内にアクティブな状態に戻らない場合には、手動による介入とトラブルシューティングが行われるまで、応答なしの状態が続きます。



注記

engine-config の **PMHealthCheckEnabled** (デフォルト: false) および **PMHealthCheckIntervalInSec** (デフォルト: 3600 秒) オプションを設定して、フェンシングパラメーターを自動的に確認することができます。

PMHealthCheckEnabled を true に設定すると、**PMHealthCheckIntervalInSec** で指定した間隔ですべてのホストエージェントが確認され、問題が検出されると警告が出されます。engine-config オプション設定の詳細については、[「engine-config コマンドの構文」](#)を参照してください。

電源管理の操作は、再起動後の Red Hat Virtualization Manager、プロキシーホスト、または管理ポータルでの手動操作により実施することができます。応答なしのホスト上で実行されている仮想マシンはすべて停止し、高可用性の仮想マシンが別のホストで起動します。電源管理の操作には、少なくとも 2 台のホストが必要です。

Manager の起動後、沈黙時間 (デフォルトでは 5 分) が経過しても電源管理が設定されたホストが応答なしの場合には、自動的にフェンシングを試みます。沈黙時間は、engine-config の **DisableFenceAtStartupInSec** オプションを更新して設定することができます。



注記

engine-config の **DisableFenceAtStartupInSec** オプションにより、Manager が起動中のホストをフェンシングしようとするのを防ぐことができます。通常、ホストの起動プロセスは Manager より長いので、データセンターの障害が発生した後にこのような状況となる可能性があります。

電源管理のパラメーターを使用すると、プロキシーホストによりホストを自動的にフェンシングすることができます。手動で行うには、ホストを右クリックすると表示されるメニューのオプションを使用します。



重要

高可用性の仮想マシンを実行するホストでは、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 におけるプロキシーを使用した電源管理

Red Hat Virtualization Manager はフェンスエージェントとは直接通信を行いません。その代わりに、Manager はプロキシーを使用して電源管理のコマンドをホストの電源管理デバイスに送ります。Manager は VDSM を利用して電源管理デバイスの操作を実行し、環境内の別のホストがフェンシングプロキシーとして使用されます。

以下のいずれかを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にある任意のホスト
- フェンシングが必要なホストと同じデータセンター内にある任意のホスト

有効なフェンシングプロキシーホストのステータスは **Up** または **Maintenance** です。

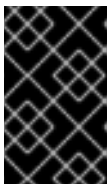
7.6.3. ホスト上でのフェンシングパラメーターの設定

ホストのフェンシング用のパラメーターを編集するには、**新規ホスト** または **ホストの編集** ウィンドウの **電源管理** タブを使用します。電源管理により、システムは Remote Access Card (RAC) などの追加のインターフェースを使用して、問題のあるホストをフェンシングすることができるようになります。

電源管理操作はすべて、Red Hat Virtualization Manager が直接行うのではなく、プロキシーホストを使用して実行します。電源管理の操作には、少なくとも 2 台のホストが必要です。

ホスト上でのフェンシングパラメーターの設定

1. **コンピューター** → **ホスト** をクリックし、ホストを選択します。
2. **編集** をクリックします。
3. **電源管理** タブをクリックします。
4. **電源管理を有効にする** のチェックボックスを選択し、フィールドを有効にします。
5. **kdump 統合** 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** を有効にする場合には、kdump を設定するためにその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、ホストが属するクラスターの **スケジューリングポリシー** がホストの電源管理を制御しないようにするには、**電源管理のポリシー制御を無効にする** のチェックボックスを選択します。
7. **+** のボタンをクリックして、新規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** ウィンドウが開きます。
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 **タイプ** 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については、[「How to set up a custom fence agent for power management in RHEV 3.5」](#) の記事を参照してください。

10. 電源管理デバイスがホストとの通信に使用する **SSH ポート** 番号を入力します。
11. 電源管理デバイスのブレードの特定に使用する **スロット** 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てください。
13. 電源管理デバイスからホストへのセキュアな接続を有効にするには、**セキュリティー保護** の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。検証が正常に完了すると、「**Test Succeeded, Host Status is: on**」というメッセージが表示されます。



警告

Red Hat Virtualization Manager によって電源管理のパラメーター (ユーザー ID、パスワード、オプションなど) がテストされるのは、セットアップ時のみで、それ以降は手動で実行します。パラメーターが正しくないことを警告するアラートが無視した場合や、電源管理デバイスで変更されたパラメーターが Red Hat Virtualization Manager では同じように変更されていない場合には、フェンシングを最も必要とする時に失敗してしまう可能性があります。

15. **OK** をクリックして **フェンスエージェントの編集** ウィンドウを閉じます。
16. **電源管理** タブでは、オプションとして **詳細パラメーター** の箇所を展開し、上下に移動するボタンを使用して Manager がフェンシングプロキシを探す際に使用するリソース (**cluster** および **dc** (データセンター)) の順序を指定します。
17. **OK** をクリックします。

ホストの一覧に戻ります。ホスト名に横の感嘆符が表示されなくなった点に注意してください。これは、電源管理の設定が適切に完了したことを意味します。

7.6.4. fence_kdump の詳細設定

kdump

ホスト名をクリックして、詳細ビューの **全般** タブで kdump サービスのステータスを確認します。

- **有効**: kdump が適切に設定されており、kdump サービスが実行中です。
- **無効**: kdump サービスは実行されていません (その場合には、kdump 統合は適切に機能しません)。
- **不明**: kdump ステータスを報告しない、以前のバージョンの VDSM を使用しているホストでのみ発生します。

kdump のインストールおよび使用方法に関する詳しい情報は、『Red Hat Enterprise Linux 7 カーネル管理ガイド』の「**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

新規ホスト または ホストの編集 ウィンドウの **電源管理** タブで **kdump 統合** を有効にすると、標準的な fence_kdump 構成が設定されます。環境のネットワーク設定が単純で、かつ Manager の FQDN が全ホストで解決可能な場合に使用するには、デフォルトの fence_kdump 設定で十分です。

ただし、fence_kdump の詳細設定が必要となる場合があります。より複雑なネットワークには、Manager と fence_kdump リスナーのいずれか一方または両方の設定を手動で変更する必要がある可能性があります。たとえば、**kdump 統合** を有効にした全ホストで Manager の FQDN が解決できない場合には、**engine-config** を使用して、適切なホスト名または IP アドレスを設定することができます。

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

以下の例のような場合には、設定の変更も必要となる可能性があります。

- Manager に 2 つの NIC があり、一方がパブリックで、他方が fence_kdump メッセージの指定送信先の場合。
- 異なる IP またはポートで fence_kdump リスナーを実行する必要がある場合。
- fence_kdump 通知メッセージの間隔をカスタム設定して、パケットの損失を防ぐ必要がある場合。

デフォルト設定の変更は、ネットワーク設定がより複雑な場合にのみ必要となるので、カスタマイズされた fence_kdump 検出設定は上級ユーザーのみが使用することを推奨します。fence_kdump リスナーの設定オプションについては、「[fence_kdump リスナーの設定](#)」を参照してください。Manager 上での kdump の設定については、「[Manager 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。この手順は、デフォルトの設定が十分でない場合にのみ必要です。

fence_kdump リスナーの手動設定

1. `/etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/` に新規ファイルを作成します (例: `my-fence-kdump.conf`)。
2. **OPTION=value** の構文でカスタマイズの設定を入力し、ファイルを保存します。



重要

編集した値は、「[Manager での fence_kdump の設定](#)」の fence_kdump リスナーの設定オプションの表に記載したように、**engine-config** でも変更する必要があります。

3. 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 fence_kdump リスナーの設定オプション

変数	説明	デフォルト	注記
LISTENER_ADDRESS	fence_kdump メッセージを取得する 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には、 engine-config の FenceKdumpDestinationAddress の値と一致する必要があります。
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には、 engine-config の FenceKdumpDestinationPort の値と一致する必要があります。
HEARTBEAT_INTERVAL	リスナーの Heartbeat の更新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には、 engine-config の FenceKdumpListenerTimeout の値の半分以下にする必要があります。
SESSION_SYNC_INTERVAL	リスナーのホストのメモリー内の kdump セッションをデータベースと同期す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には、 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	kdump を実行するホストからメッセージを最後に受信した後に、ホストの kdump フローが FINISHED とマークされるまでのタイムアウトの最大値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には、 engine-config の FenceKdumpMessageInterval の値の 2 倍以上にする必要があります。

7.6.4.2. Manager での fence_kdump の設定

Manager の kdump 設定を編集します。この手順は、デフォルトの設定が十分でない場合にのみ必要です。現在の設定値は、以下のコマンドを実行すると確認できます。

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

engine-config を使用した 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** の設定オプション の表に記載した fence_kdump リスナーの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. 必要な場合には、**kdump 統合** が有効化されている全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** を使用して設定することができます。

表7.10 Kdump の設定オプション

変数	説明	デフォルト	注記
FenceKdumpDestinationAddress	fence_kdump メッセージの送信先のホスト名または IP アドレスを定義します。この値が指定されていない場合には、Manager の FQDN が使用されます。	空の文字列 (Manager の 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には、fence_kdump リスナー設定ファイルの LISTENER_ADDRESS の値と一致しなければなりません。また、 kdump 統合 が有効化された全ホストを再インストールする必要があります。
FenceKdumpDestinationPort	fence_kdump メッセージを送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には、fence_kdump リスナー設定ファイルの LISTENER_PORT の値と一致しなければなりません。また、 kdump 統合 が有効化された全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
FenceKdumpMessageInterval	fence_kdump メッセージの送信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には、fence_kdump リスナー設定ファイルの KDUMP_FINISHED_TIMEOUT の値の半分以下にする必要があります。また、 kdump 統合 が有効化された全ホストを再インストールする必要があります。
FenceKdumpListenerTimeout	最後の Heartbeat の後に、fence_kdump リスナーが実行中と見なされなくなるまでのタイムアウトの最大値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には、fence_kdump リスナー設定ファイルの HEARTBEAT_INTERVAL の値の 2 倍以上にする必要があります。
KdumpStartedTimeout	kdump を実行する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 フローが開始したことを検知するまで) の待ち時間のタイムアウトの最大値を定義します。	30	このパラメーターの値を変更する場合には、fence_kdump リスナー設定ファイルの SESSION_SYNC_INTERVAL および FenceKdumpMessageInterval の値の 2 倍以上にする必要があります。

7.6.5. ホストのソフトフェンシング

ホストは、予期しない問題が原因となって応答なしの状態になる場合があります。VDSM は要求に応答できませんが、VDSM に依存している仮想マシンは稼働を続け、アクセス可能な状態のままとなります。このような状況が発生した場合には、VDSM を再起動すると、VDSM が応答可能な状態に戻り、問題は解決します。

「SSH を介したソフトフェンシング」は、Manager が SSH を使用して、応答しない状態のホストで VDSM の再起動を試みるプロセスです。Manager が SSH を使用した VDSM の再起動に失敗した場合には、フェンシングは外部のフェンスエージェントの責任となります (外部のフェンスエージェントが設定されている場合)。

SSH ソフトフェンシングが機能するためには、ホストでフェンシングが設定および有効化されており、かつ有効なプロキシホスト (同じデータセンター内にある、ステータスが Up の第 2 のホスト) が存在する必要があります。Manager とホスト間の接続がタイムアウトになると、次のような状態となります

1. 初回のネットワーク障害発生時には、ホストのステータスが「connecting」に変わります。
2. Manager は次に VDSM に対してステータス確認を 3 回試みるか、ホストの負荷によって決定

される時間が経過するのを待ちます。この時間は、 $[\text{TimeoutToResetVdsInSeconds (デフォルトは 60 秒)}] + [\text{DelayResetPerVmInSeconds (デフォルトは 0.5 秒)}] * [\text{ホスト上で実行中の仮想マシン数}] + [\text{DelayResetForSpmInSeconds (デフォルトは 20 秒)}] * [1 (\text{ホストが SPM として稼働している場合}) \text{ または } 0 (\text{ホストが SPM としては稼働していない場合})]$ の計算式で決定されます。VDSM が応答する時間を最大限にするために、Manager は上記のオプション (VDSM のステータス確認を 3 回試みる、または上記の計算式で決定される時間の経過を待つ) のいずれか長い方を選択します。

3. この時間が経過してもホストが応答しない場合には、SSH を介して **vdsd restart** が実行されます。
4. **vdsd restart** を実行しても、ホストと Manager 間の接続が再度確立されない場合には、ホストのステータスが **Non Responsive** に変わります。電源管理が設定されている場合には、フェンシングは外部のフェンスエージェントによって引き継がれます。



注記

SSH を介したソフトフェンシングは、電源管理を設定していないホストに対しても実行することが可能です。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たホストでしか実行することはできません。

7.6.6. ホストの電源管理機能の使用方法

ホストに電源管理の設定を行うと、管理ポータルから数多くのオプションにアクセスできるようになります。電源管理デバイスには、それぞれカスタマイズ可能なオプションがありますが、ホストを起動、停止、再起動する基本的なオプションは全デバイスでサポートされます。

ホストの電源管理機能の使用方法

1. **コンピュータ** → **ホスト** をクリックし、ホストを選択します。
2. **管理** → **電源管理** をクリックし、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させて、ホストのステータスが **Down** になるのを待ちます。ホストが **Down** の状態となったことをエージェントが確認すると、高可用性の仮想マシンが同じクラスター内の別のホスト上で再起動します。次にエージェントは、このホストを再起動させて、ホストの準備が整うと、ステータスが **Up** に変わります。
 - **起動**: このオプションは、ホストを起動させて、クラスターにアタッチします。使用する準備が整うと、ステータスが **Up** に変わります。
 - **停止**: このオプションは、ホストの電源を切断します。このオプションを使用する前には、そのホスト上で実行中の仮想マシンが同じクラスター内の別のホストに移行済みであることを確認してください。そうでない場合には、仮想マシンがクラッシュし、高可用性のマシンのみが別のホストで再起動します。ホストが停止すると、ステータスは **Non Operational** に変わります。



注記

電源管理が有効ではないホストを再起動または停止するには、そのホストを選択して **管理** ドロップダウンメニューをクリックし、**再起動** または **停止** を選択します。



重要

1 台のホストに 2 つのフェンスエージェントを定義すると、それらのエージェントは同時もしくは順次に使用することができます。同時エージェントの場合に、ホストを停止させるには、両方のエージェントが停止のコマンドに応答する必要があります。また、一方のエージェントが起動のコマンドに応答すると、ホストが起動します。順次エージェントの場合に、ホストを起動または停止させるには、プライマリーエージェントが最初に使用され、それが失敗するとセカンダリーエージェントが使用されます。

3. **OK** をクリックします。

7.6.7. 応答なしのホストの手動によるフェンシングまたは分離

ハードウェア障害などが原因で、ホストが予期せず応答なしの状態となった場合には、環境のパフォーマンスに多大な影響を及ぼす可能性があります。電源管理デバイスを使用していない場合や、正しく設定されていない場合は、ホストを手動でリブートすることができます。



警告

ホストを手動でリブートした場合以外は、**ホストがリブートされていることを確認**のオプションは使用しないでください。ホストの稼働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してしまう場合があります。

応答なしのホストの手動によるフェンシングまたは分離

1. 管理ポータルで **コンピュート** → **ホスト** をクリックし、ホストのステータスが **Non Responsive** であることを確認します。
2. ホストを手動で再起動します。これは、物理マシンの電源ボタンを押してホストをリブートすることを意味します。
3. 管理ポータルでホストを選択し、**その他の操作** → **ホストがリブートされていることを確認** をクリックします。
4. **操作を承認** チェックボックスにチェックを入れて、**OK** をクリックします。
5. ホストの起動に通常より長い時間がかかる場合は、**ServerRebootTimeout** を設定してホストを **Non Responsive** とみなすまでの時間を指定することができます (秒単位)。

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

第8章 ストレージ

Red Hat Virtualization では、仮想ディスク、ISO ファイル、スナップショット用に一元化された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クは、以下のストレージタイプを使用して実装することができます。

- Network File System (NFS)
- GlusterFS エクスポート
- CephFS
- その他の POSIX 準拠のファイルシステム
- Internet Small Computer System Interface (iSCSI)
- 仮想化ホストに直接アタッチされたローカルストレージ
- Fibre Channel Protocol (FCP)
- Parallel NFS (pNFS)

データセンターは、ストレージドメインがアタッチされ、アクティブ化された状態でなければ使用できないため、ストレージの設定は新規データセンターの重要な前提条件となります。

Red Hat Virtualization システム管理者は、仮想化エンタープライズのストレージの作成、設定、アタッチ、メンテナンスを行う必要があるため、ストレージのタイプと使用方法に精通している必要があります。ストレージアレイのベンダーの説明書をお読みください。ストレージの概念、プロトコル、要件、一般的な使用方法についての詳しい説明は、『[Red Hat Enterprise Linux ストレージ管理ガイド](#)』を参照してください。

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することが可能で、かつ、少なくとも 1 台のホストが **Up** のステータスで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。

- **データドメイン:** データドメインには、データセンター内にある全仮想マシンの仮想ハードディスクおよび OVF ファイル、ならびにテンプレートが保管されます。また、仮想マシンのスナップショットもデータドメインに格納されます。
データドメインは、複数のデータセンター間で共有することができません。ドメインがローカルのドメインではなく全ホストからアクセス可能なドメインの場合は、複数のタイプのデータドメイン (iSCSI、NFS、FC、POSIX、Gluster) を同じデータセンターに追加することができます。

データドメイン以外のタイプのドメインをデータセンターにアタッチするには、先にデータドメインをデータセンターにアタッチしておく必要があります。

- **ISO ドメイン:** ISO ドメインには、仮想マシンのオペレーティングシステムとアプリケーションのインストールおよび起動に使用する ISO ファイル (または論理 CD) が保管されます。ISO ドメインにより、データセンターには物理メディアが不要になります。ISO ドメインは異なるデータセンター間で共有することができます。ISO ドメインは NFS ベースのみで、1 つのデータセンターに 1 つしか追加できません。
- **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 環境間でのイメージのコピーや移動に使用する一時的なストレージリポジトリです。また、仮想マシンのバックアップにも使用できます。エクスポートドメインは、複数のデータセンター

間で移動させることができますが、一度に1つのデータセンターでしかアクティブにすることはできません。エクスポートドメインは、NFS ベースのみで、1つのデータセンターに1つしか追加できません。



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。データストレージドメインは、データセンターからアタッチを解除して、同じ環境または異なる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、テンプレートは、インポートしたストレージドメインからアタッチされているデータセンターにアップロードすることができます。ストレージドメインのインポートに関する情報は、「[既存のストレージドメインのインポート](#)」の項を参照してください。



重要

Red Hat Virtualization 環境に対するストレージの設定およびアタッチは、使用しているデータセンターのストレージ要件を決定してから、開始するようにしてください。

8.1. ストレージドメインについての知識

ストレージドメインとは、共通のストレージドインターフェースを使用するイメージの集合体です。ストレージドメインには、テンプレートおよび仮想マシン (スナップショットを含む) の完全なイメージまたは ISO ファイルが格納されます。ストレージドメインには、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 準拠ファイルシステム) を使用することができます。

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、仮想ディスク、テンプレート、スナップショットはそれぞれが1つの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単一の論理エンティティに集約された後に、仮想ハードディスクとして使用するように、LVM (論理ボリュームマネージャー) によって分割されます。LVM に関する詳しい情報は『[Red Hat Enterprise Linux 論理ボリュームマネージャーの管理](#)』を参照してください。

仮想ディスクには2つの形式 (QCOW2 または RAW) のいずれかを使用することができます。ストレージのタイプは、スパース割り当てまたは事前割り当てのいずれかに指定することができます。スナップショットは常にスパースですが、いずれの形式のディスクのスナップショットも作成することができます。

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 サーバー上でデータドメインとして機能する NFS 共有を設定します。Red Hat Virtualization Manager のインストールの工程で ISO ドメインを作成済みの場合には、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。データストレージドメインは、データセンターからアタッチを解除して、同じ環境または異なる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、テンプレートは、インポートしたストレージドメインからアタッチされているデータセンターにアップロードすることができます。ストレージドメインのインポートに関する情報は、「[既存のストレージドメインのインポート](#)」の項を参照してください。

Red Hat Enterprise Linux における NFS の設定および構成についての説明は、『[Red Hat Enterprise Linux 6 ストレージ管理ガイド](#)』の「[NFS \(Network File System\)](#)」または『[Red Hat Enterprise Linux 7 ストレージ管理ガイド](#)』の「[NFS \(Network File System\)](#)」を参照してください。

エクスポートされたディレクトリーにより表されるストレージドメインに Manager がデータを保管するには、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。

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** というグループを作成します。

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

2. ユーザー **vdsm** を作成してグループ **kvm** に追加します。

```
# useradd vdsm -u 36 -g 36
```

3. エクスポートディレクトリーの所有権を 36:36 に設定すると、vdsm:kvm に所有権が付与されます。

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

4. 所有者に読み取り/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/実行アクセスを許可す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についての詳しい情報は、「[付録F 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アタッチします。このストレージドメインは、仮想ディスクおよび ISO 起動メディア用のストレージを提供します。以下の手順は、エクスポート共有がすでに用意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しておく必要があります。エクスポートドメインの作成にも同じ手順を使用しますが、その場合は、**ドメイン機能 / ストレージタイプ** の一覧で **エクスポート / NFS** を選択します。

1. 管理ポータルで **ストレージ → ドメイン** をクリックします。

2. **新規ドメイン** をクリックします。
3. ストレージドメインの **名前** 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、形式、および使用するホスト** の一覧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 **エクスポートパス** を入力します。エクスポートパスは、**192.168.0.10:/data** または **domain.example.com:/data** の形式にする必要があります。
6. オプションで、詳細パラメーターを設定することが可能です。
 - a. **詳細パラメーター** をクリックします。
 - b. **容量不足の警告** のフィールドに、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、ユーザーに警告のメッセージが表示され、ログに記録されます。
 - c. **アクションをブロックする深刻な容量不足** のフィールドに GB 単位で値を入力します。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. 削除後にワイプするオプションを有効にするには、**削除後にワイプ** 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るディスクの「削除後にワイプ」プロパティは変更されません。
7. **OK** をクリックします。

ディスクの準備が完了するまで新規 NFS データドメインのステータスは **ロック** と表示され、その後データセンターに自動的にアタッチされます。

8.2.3. NFS ストレージの拡張

NFS ストレージの容量を拡張するには、新規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 サーバー上の使用可能な空き容量を増やします。最初のオプションについては、[「NFS ストレージのアタッチ」](#)を参照してください。以下の手順は、既存の NFS サーバーで使用可能な空き容量を増やす方法について説明します。

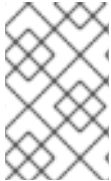
既存の NFS ストレージドメインの拡張

1. **ストレージ → ドメイン** をクリックします。
2. NFS ストレージドメインの名前をクリックし、詳細ビューを表示します。
3. **データセンター** タブをクリックし、**メンテナンス** 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切り替えます。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となります。
4. NFS サーバーで、ストレージをリサイズします。Red Hat Enterprise Linux 6 システムの場合は、[『Red Hat Enterprise Linux 6 ストレージ管理ガイド』](#)を参照してください。Red Hat Enterprise Linux 7 システムの場合は、[『Red Hat Enterprise Linux 7 ストレージ管理ガイド』](#)を参照してください。
5. 詳細ビューで **データセンター** タブをクリックし、**アクティブ化** 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。ホストがローカルストレージを使用するように設定すると、そのホストは、他のホストを追加することができない新規データセンターとクラスターに自動的に追加されます。複数のホストで構成されるクラスターの場合は、全ホストが全ストレージドメインにアクセス可能である必要があり、ローカルストレージでは対応不可能です。単一ホストのクラスター内で作成された仮想マシンは、移行、フェンシング、スケジューリングはできません。必要なシステムユーザーとグループについての詳しい情報は、「[付録F 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維持する方法は、『[Red Hat Virtualization 4.0 Upgrade Guide](#)』の「[Upgrading to RHVH While Preserving Local Storage](#)」を参照してください。



重要

Red Hat Virtualization Host (RHVH) の場合は、必ず / (ルート) とは異なるファイルシステム上にローカルストレージを定義すべきです。Red Hat では、アップグレード中のデータ喪失を防ぐために、別の論理ボリュームまたはディスクを使用することを推奨しています。

ローカルストレージの準備 (Red Hat Enterprise Linux ホスト向け)

1. ホストで、ローカルストレージとして使用するディレクトリを作成します。

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

2. **vdsm** ユーザー (UID 36) と **kvm** グループ (GID 36) がそのディレクトリに読み取り/書き込みアクセスできるように、パーミッションを設定します。

```
# 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。

ローカルストレージの準備 (Red Hat Virtualization Host 向け)

Red Hat では、以下のように論理ボリューム上に論理ストレージを作成することを推奨します。

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

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

以下に説明する方法でホストをローカルストレージに追加すると、ホストが新規のデータセンターと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。

ローカルストレージの追加

1. **コンピュー**ト → **ホスト** をクリックし、ホストを選択します。
2. **管理** → **メンテナンス** をクリックし、**OK** をクリックします。
3. **管理** → **ローカルストレージを設定** をクリックします。
4. **データセンター**、**クラスター**、**ストレージ** フィールドの横にある **編集** ボタンをクリックし、ローカルのストレージドメインを設定して名前を付けます。
5. 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。
6. 該当する場合には、**最適化** タブをクリックして新規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。
7. **OK** をクリックします。

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

8.4.1. POSIX 準拠ファイルシステムストレージのアタッチ

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する POSIX 準拠のファイルシステムは、Global File System 2 (GFS2) 等のクラスター化したファイルシステムで、かつスパースファイルおよびダイレクト I/O をサポートしている必要があります。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 準拠ファイルシステムの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。必ず、NFS ストレージドメインを作成してください。

POSIX 準拠ファイルシステムストレージのアタッチ

1. **ストレージ** → **ドメイン** をクリックします。
2. **新規ドメイン** をクリックします。
3. ストレージドメインの **名前** を入力します。
4. このストレージドメインと関連づける **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 準拠 FS)** でなければなりません。または、**(none)** を選択します。

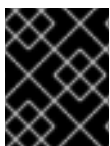
5. **ドメイン機能** ドロップダウンリストから **データ** を、**ストレージタイプ** ドロップダウンリストから **POSIX 準拠 FS** を、それぞれ選択します。
該当する場合には、ドロップダウンメニューから **形式** を選択します。
6. **使用するホスト** のドロップダウンリストからホストを選択します。
7. 通常 **mount** コマンドで指定するように、POSIX ファイルシステムへの **パス** を入力します。
8. 通常 **-t** 引数を使用して **mount** コマンドで指定するように、**VFS タイプ** を入力します。有効な VFS タイプの一覧については、**man mount** で確認してください。
9. 通常 **-o** 引数を使用して **mount** コマンドで指定するように、追加の **マウントオプション** を入力します。このマウントオプションはコンマ区切りで提示してください。有効なマウントオプションの一覧については、**man mount** で確認してください。
10. オプションで、詳細パラメーターを設定することが可能です。
 - a. **詳細パラメーター** をクリックします。
 - b. **容量不足の警告** のフィールドに、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、ユーザーに警告のメッセージが表示され、ログに記録されます。
 - c. **アクションをブロックする深刻な容量不足** のフィールドに GB 単位で値を入力します。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. 削除後にワイプするオプションを有効にするには、**削除後にワイプ** 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るディスクの「削除後にワイプ」プロパティは変更されません。
11. **OK** をクリックします。

8.5. ブロックストレージの追加



重要

ブロックストレージを使用する際、仮想マシンを Raw デバイスまたは直接 LUN にデプロイし、論理ボリュームマネージャーで管理する場合は、フィルターを作成してゲストの論理ボリュームを除外する必要があります。これにより、ホストの起動時にゲストの論理ボリュームがアクティブ化されるのを防ぐことができます。アクティブ化されると、論理ボリュームと論理ボリュームマネージャーのメタデータが同期しなくなり、データ破損が生じる可能性があります。詳細については、[「RHV: Hosts boot with Guest LVs activated」](#) を参照してください。



重要

現状、Red Hat Virtualization はブロックサイズ 4K のストレージはサポートしていません。ブロックストレージはレガシー (512b ブロック) モードで設定する必要があります。

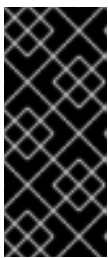
8.5.1. iSCSI ストレージの追加

Red Hat Virtualization は、既存の LUN で構成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方法で、iSCSI ストレージをサポートしています。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はアタッチできません。

Red Hat Enterprise Linux における iSCSI の設定方法については、『Red Hat Enterprise Linux 6 ストレージ管理ガイド』の「[iSCSI ターゲットの設定](#)」または『Red Hat Enterprise Linux 7 ストレージ管理ガイド』の「[オンラインストレージ管理](#)」を参照してください。

iSCSI ストレージの追加

1. **ストレージ → ドメイン** をクリックします。
2. **新規ドメイン** をクリックします。
3. 新規ストレージドメインの **名前** を入力します。
4. ドロップダウンリストから **データセンター** を選択します。
5. ドロップダウンリストから **ドメイン機能** および **ストレージタイプ** 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選択できません。
6. **使用するホスト** のフィールドでアクティブなホストを 1 台選択します。データセンターで初めて作成するデータドメインでなければ、そのデータセンターの 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あればなりません。

7. Red Hat Virtualization Manager でマッピングが可能なのは、iSCSI ターゲットから LUN へのマッピング、または LUN から iSCSI ターゲットへのマッピングのいずれかです。**新規ドメイン** ウィンドウで、ストレージタイプに iSCSI を選択した場合は、未使用の LUN が割り当てられた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元のターゲットが表示されない場合には、「ターゲットを検出」を使用して検索することができます。表示されている場合には、次の手順に進んでください。
 - a. **ターゲットを検出** をクリックし、ターゲットの検出オプションを有効にします。Manager がターゲットを検出してログインすると、**新規ドメイン** ウィンドウに、その環境では未使用の 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。

ターゲットを検出 のオプションを使用すると、多数のターゲットに 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。

- b. **アドレス** 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。
- c. **ポート** フィールドには、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。

- d. ストレージのセキュリティ保護に Challenge Handshake Authentication Protocol (CHAP) を使用している場合は、**ユーザー認証** のチェックボックスを選択します。**CHAP** のユーザー名と **CHAP** のパスワードを入力してください。



注記

REST API を使用して、ホスト毎の iSCSI ターゲットに特定の認証情報を定義することができるようになりました。詳しくは、『**REST API Guide**』の「[StorageServerConnectionExtensions - add](#)」のセクションを参照してください。

- e. **検出** をクリックします。
- f. 検出結果から使用するターゲットを選択して **ログイン** ボタンをクリックします。もしくは、**全ターゲットにログイン** をクリックして、検出された全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を通して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さらに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表示されている **+** ボタンをクリックします。エントリが展開され、ターゲットにアタッチ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にチェックを入れます。
10. オプションで、詳細パラメーターを設定することが可能です。
 - a. **詳細パラメーター** をクリックします。
 - b. **容量不足の警告** のフィールドに、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、ユーザーに警告のメッセージが表示され、ログに記録されます。
 - c. **アクションをブロックする深刻な容量不足** のフィールドに GB 単位で値を入力します。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. 削除後にワイプするオプションを有効にするには、**削除後にワイプ** 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るディスクの「削除後にワイプ」プロパティは変更されません。
 - e. **削除後に破棄** チェックボックスを選択して、削除後に破棄のオプションを有効化します。このオプションは、ドメインの作成後に編集できます。また、このオプションを利用できるのは、ブロックストレージドメインのみです。
11. **OK** をクリックします。

同じターゲットに対して複数のストレージ接続パスを設定している場合には、[「iSCSI マルチパス機能の設定」](#)の手順に従ってください。

8.5.2. iSCSI マルチパス機能の設定

iSCSI マルチパス により、論理ネットワークおよび iSCSI ストレージ接続のグループを作成/管理することができます。ネットワークパスのエラーによるホストのダウンタイムを防ぐには、ホストと iSCSI ストレージ間に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 はデータセンター内の各ホストを、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、ボンディングされた各ターゲットに接続します。ホストがデフォルトのネットワークを使用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可能です。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アタッチされた後にのみ、管理ポータルで指定することができます。

前提条件

- iSCSI ストレージドメインの作成が完了していること。また、iSCSI ターゲットへの全パスを検出済みで、ログインしていること。
- iSCSI ストレージの接続とボンディングするための **任意** の論理ネットワークが作成済みであること。複数の論理ネットワークまたはボンディングネットワークを設定すると、ネットワークのフェイルオーバーを可能にすることができます。

iSCSI マルチパス機能の設定

1. **コンピューター** → **データセンター** をクリックします。
2. データセンターの名前をクリックして、詳細ビューを表示します。
3. **iSCSI マルチパス** タブをクリックします。
4. **追加** をクリックします。
5. **iSCSI ボンディングの追加** ウィンドウでボンディングの **名前** と **説明** を入力します。
6. **論理ネットワーク** の一覧から、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、**任意** の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 **必須** プロパティを **任意** に変更するには、管理ポータルでそのネットワークを選択し、**クラスター** タブをクリックして **ネットワークの管理** ボタンをクリックし、**必須** チェックボックスのチェックを外します。

7. **ストレージターゲット** の一覧から、指定したネットワークを介して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パスをすべて選択するようにしてください。
8. **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 で構成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方法で、SAN ストレージをサポートしています。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はアタッチできません。

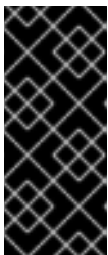
Red Hat Virtualization システムの管理者には Storage Area Networks (SAN) の概念に関する作業知識が必要になります。SAN は通常、ホストと外部の共有ストレージ間のトラフィックに Fibre Channel Protocol (FCP) を使用します。このため、SAN は FCP ストレージとも呼ばれています。

Red Hat Enterprise Linux での FCP またはマルチパスの設定/構成に関する情報については、『[ストレージ管理ガイド](#)』および『[DM Multipath](#)』を参照してください。

以下の手順は、既存の FCP ストレージを Red Hat Virtualization 環境にデータドメインとしてアタッチする方法について説明します。サポートされているストレージタイプについての詳しい情報は、『[8 章 ストレージ](#)』を参照してください。

FCP ストレージの追加

1. **ストレージ** → **ドメイン** をクリックします。
2. **新規ドメイン** をクリックします。
3. ストレージドメインの **名前** を入力します。
4. ドロップダウンリストから **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. ドロップダウンリストから **ドメイン機能** および **ストレージタイプ** 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. **使用するホスト** のフィールドでアクティブなホストを 1 台選択します。データセンターで初めて作成するデータドメインでなければ、そのデータセンターの 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. **新規ドメイン** ウィンドウで、ストレージタイプに **ファイバーチャネル** を選択した場合は、未使用の LUN が割り当てられた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、使用可能な LUN をすべて選択します。
8. オプションで、詳細パラメーターを設定することが可能です。
 - a. **詳細パラメーター** をクリックします。
 - b. **容量不足の警告** のフィールドに、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、ユーザーに警告のメッセージが表示され、ログに記録されます。
 - c. **アクションをブロックする深刻な容量不足** のフィールドに GB 単位で値を入力します。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. 削除後にワイプするオプションを有効にするには、**削除後にワイプ** 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るディスクの「削除後にワイプ」プロパティは変更されません。

- e. **削除後に破棄** チェックボックスを選択して、削除後に破棄のオプションを有効化します。このオプションは、ドメインの作成後に編集できます。また、このオプションを利用できるのは、ブロックストレージドメインのみです。

9. **OK** をクリックします。

使用準備中、新規 FCP データドメインは **ロック** のステータスとなります。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 ストレージの拡張

iSCSI または FCP ストレージのサイズを拡張するには、いくつかの方法があります。

- 既存の LUN を、現在のストレージドメインに追加する
- 新しい LUN で新規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 (「[iSCSI ストレージの追加](#)」を参照)
- 下層の LUN をリサイズして、ストレージドメインを拡張する

Red Hat Enterprise Linux 7 システムで iSCSI ストレージを作成、設定、リサイズする方法についての説明は、[『Red Hat Enterprise Linux 7 ストレージ管理ガイド』](#)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規 LUN を追加して、Storage Area Network (SAN) ストレージを拡張する方法について説明します。

前提条件

- ストレージドメインのステータスは **Up** でなければなりません。
- LUN は、ステータスが **Up** であるすべてのホストからアクセス可能でなければなりません。この条件が満たされないと、操作は失敗して LUN はドメインに追加されません。ただし、ホスト自体には影響を及ぼしません。新たに追加したホストまたはメンテナンス (もしくは **Non Operational**) の状態から回復したホストが LUN にアクセスすることができない場合、ホストのステータスは **Non Operational** となります。

既存の iSCSI または FCP ストレージドメインの拡張

1. **ストレージ → ドメイン** をクリックして、iSCSI または FCP ドメインを選択します。
2. **ドメインを管理** をクリックします。
3. **ターゲット > LUN** をクリックして、**ターゲットを検出** の展開ボタンをクリックします。
4. ストレージサーバーへの接続情報を入力し、**検出** をクリックして接続を開始します。
5. **LUN > ターゲット** をクリックし、新しく利用可能となった LUN のチェックボックスを選択します。
6. **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、ストレージドメインは、追加した LUN のサイズ分拡張されます。

下層の LUN をリサイズしてストレージドメインを拡張する場合には、管理ポータルで LUN をリフレッシュする必要もあります。

LUN サイズのリフレッシュ

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格納されているすべての仮想マシンとテンプレートにアクセスすることができます。ストレージドメインをインポートした後は、仮想マシン、フローティングディスクのイメージ、テンプレートを手動でターゲットのデータセンターに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に格納されている仮想マシンと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プロセスと似ていますが、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ので、データ復旧やデータセンター/環境間での大規模な仮想マシンの移行の場合には、データストレージドメインをインポートすることをお勧めします。



重要

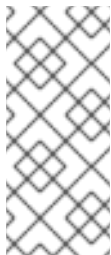
互換性レベルが 3.5 以上のデータセンターにアタッチされていた既存のデータストレージドメインをインポートすることができます。

ISO

既存の ISO ストレージドメインをインポートすると、その ISO ストレージドメインに格納されているすべての ISO ファイルと仮想フロッピーにアクセスすることができます。ストレージドメインをインポートした後は、リソースへのアクセスに追加の操作は不要なので、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。

エクスポート

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、そのエクスポートストレージドメインに格納されているすべての仮想マシンとテンプレートにアクセスすることができます。エクスポートストレージドメインは、仮想マシンイメージとテンプレートのエクスポート/インポート用に設計されているので、同じ環境内または異なる環境間で少数の仮想マシンとテンプレートを移行する場合には、エクスポートストレージドメインをインポートする方法を推奨します。エクスポートドメインを使用した仮想マシンとテンプレートのエクスポート/インポートについての情報は、『**仮想マシン管理ガイド**』の「**仮想マシンとテンプレートのエクスポート/インポート**」のセクション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。データストレージドメインは、データセンターからアタッチを解除して、同じ環境または異なる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、テンプレートは、インポートしたストレージドメインからアタッチされているデータセンターにアップロードすることができます。

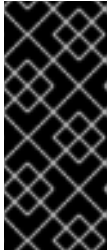
8.6.2. ストレージドメインのインポート

同じ環境または異なる環境のデータセンターに以前アタッチされていたストレージドメインをインポートします。以下の手順では、データの破損を回避するために、ストレージドメインがどの環境のデータセンターにもアタッチされていない状態である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データセンターにインポートするには、インポート先のデータセンターが動作開始済みである必要があります。

ストレージドメインのインポート

1. ストレージ → ドメイン をクリックします。
2. ドメインをインポート をクリックします。

3. ストレージドメインのインポート先となる **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. ドロップダウンリストから **ドメイン機能** および **ストレージタイプ** を選択します。
6. **使用するホスト** の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

ストレージドメインの詳細を指定するフィールドは、**ドメイン機能** および **ストレージタイプ** の一覧で選択した値に応じて異なります。これらのフィールドは、新規ストレージドメインの追加で表示される項目と同じです。

8. **データセンター内のドメインを有効化する** のチェックボックスにチェックを入れると、選択したデータセンターにストレージドメインがアタッチされた後にそのドメインがアクティブ化されます。
9. **OK** をクリックします。

これで、ストレージドメインからデータセンターに仮想マシンとテンプレートをインポートできるようになりました。

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 環境内のデータセンター間でストレージドメインを移行すると、移行先のデータセンターで、そのストレージドメインに格納されているデータにアクセスすることができます。以下の手順では、移行元のデータセンターからストレージドメインをデタッチしてから、別のデータセンターにアタッチするステップを伴います。

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. 対象のストレージドメインで実行中の仮想マシンをすべて停止します。
2. **ストレージ → ドメイン** をクリックします。
3. ストレージドメインの名前をクリックし、詳細ビューを表示します。
4. **データセンター** タブをクリックします。
5. **メンテナンス** をクリックして、**OK** をクリックします。
6. **デタッチ** をクリックして、**OK** をクリックします。
7. **アタッチ** をクリックします。

8. 移行先のデータセンターを選択して **OK** をクリックします。

移行先のデータセンターにストレージドメインがアタッチされ、自動的にアクティブ化されます。これで、ストレージドメインから仮想マシンおよびテンプレートを移行先のデータセンターにインポートすることができます。

8.6.4. 異なる環境のデータセンター間でのストレージドメインの移行

異なる Red Hat Virtualization 環境間でストレージドメインを移行すると、移行先の環境で、そのストレージドメインに格納されているデータにアクセスすることができます。以下の手順は、1 つの Red Hat Virtualization 環境からストレージドメインを削除して、別の環境にインポートするステップを伴います。既存のデータストレージドメインをインポートして Red Hat Virtualization のデータセンターにアタッチするには、ストレージドメインの移行元のデータセンターの互換レベルが 3.5 以上である必要があります。

異なる環境のデータセンター間でのストレージドメインの移行

1. 移行元の環境の管理ポータルにログインします。
2. 対象のストレージドメインで実行中の仮想マシンをすべて停止します。
3. **ストレージ → ドメイン** をクリックします。
4. ストレージドメインの名前をクリックし、詳細ビューを表示します。
5. **データセンター** タブをクリックします。
6. **メンテナンス** をクリックして、**OK** をクリックします。
7. **デタッチ** をクリックして、**OK** をクリックします。
8. **削除** をクリックします。
9. **ストレージの削除** ウィンドウで **ドメインをフォーマット** します。**ストレージの中身が失われます。** のチェックボックスが選択されていないことを確認します。このステップにより、ストレージドメイン内のデータが保持され、後で使用することができます。
10. **OK** をクリックすると、移行元の環境からストレージドメインが削除されます。
11. 移行先の環境の管理ポータルにログインします。
12. **ストレージ → ドメイン** をクリックします。
13. **ドメインをインポート** をクリックします。
14. **データセンター** のドロップダウンリストから、移行先のデータセンターを選択します。
15. ストレージドメインの名前を入力します。
16. 該当するドロップダウンリストから **ドメイン機能** および **ストレージタイプ** を選択します。
17. **使用するホスト** のドロップダウンリストからホストを選択します。
18. ストレージドメインの詳細を入力します。



注記

ストレージドメインの詳細を指定するフィールドは、**ストレージタイプ** のドロップダウンリストで選択した値に応じて異なります。これらのフィールドは、新規ストレージドメインの追加で表示される項目と同じです。

19. **データセンター内のドメインを有効化する** のチェックボックスを選択すると、ストレージドメインがアタッチされた時に自動的にアクティブ化されます。

20. **OK** をクリックします。

新しい Red Hat Virtualization 環境にある移行先のデータセンターにストレージドメインがアタッチされ、自動的にアクティブ化されます。これで、ストレージドメインから仮想マシンおよびテンプレートを移行先のデータセンターにインポートすることができます。

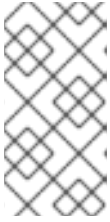
8.6.5. インポートされたデータストレージドメインからの仮想マシンのインポート

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 1 つまたは複数のクラスターにインポートします。以下の手順は、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アタッチ済みで、かつアクティブ化されていることを前提としています。

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. **ストレージ → ドメイン** をクリックします。
2. インポートしたストレージドメインの名前をクリックし、詳細ビューを表示します。
3. **仮想マシンのインポート** タブをクリックします。
4. インポートする仮想マシンを 1 台または複数選択します。
5. **インポート** をクリックします。
6. **仮想マシンのインポート** ウィンドウの各仮想マシンに、**クラスター** リストで正しいターゲットのクラスターが選択されていることを確認します。
7. 外部の仮想マシンの仮想 NIC プロファイルをターゲットのクラスター上のプロファイルにマッピングします。
 - a. **仮想 NIC プロファイルのマッピング** をクリックします。
 - b. 使用する仮想 NIC プロファイルを **ターゲットの仮想 NIC プロファイル** のドロップダウンリストから選択します。
 - c. **仮想マシンのインポート** ウィンドウで複数のターゲットクラスターが選択されている場合には、**ターゲットのクラスター** のドロップダウンリストで各ターゲットクラスターを選択して、正しくマッピングされるようにします。
 - d. **OK** をクリックします。
8. MAC アドレスの競合が検出された場合には、仮想マシン名の横に感嘆符が表示されます。このアイコンの上にマウスを移動するとヒントが表示され、発生したエラーのタイプを確認することができます。

無効な MAC を再割り当て のチェックボックスを選択して、問題のあるすべての仮想マシンに新しい MAC アドレスを再割り当てします。仮想マシンごとに **再割り当て** のチェックボックスを選択することができます。



注記

割り当てに利用可能なアドレスがない場合には、インポートの操作は失敗しますが、クラスターの MAC アドレスプール範囲外の MAC アドレスの場合には、新規 MAC アドレスを再割り当てせずに仮想マシンをインポートすることができます。

9. **OK** をクリックします。

インポートした仮想マシンは、**仮想マシンのインポート** タブの一覧には表示されなくなります。

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。以下の手順は、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アタッチ済みで、かつアクティブ化されていることを前提としています。

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. **ストレージ → ドメイン** をクリックします。
2. インポートしたストレージドメインの名前をクリックし、詳細ビューを表示します。
3. **テンプレートのインポート** タブをクリックします。
4. インポートするテンプレートを 1 つまたは複数選択します。
5. **インポート** をクリックします。
6. **テンプレートのインポート** ウィンドウの各テンプレートに、**クラスター** リストで正しいターゲットのクラスターが選択されていることを確認します。
7. 外部の仮想マシンの仮想 NIC プロファイルをターゲットのクラスター上のプロファイルにマッピングします。
 - a. **仮想 NIC プロファイルのマッピング** をクリックします。
 - b. 使用する仮想 NIC プロファイルを **ターゲットの仮想 NIC プロファイル** のドロップダウンリストから選択します。
 - c. **テンプレートのインポート** ウィンドウで複数のターゲットクラスターが選択されている場合には、**ターゲットのクラスター** のドロップダウンリストで各ターゲットクラスターを選択して、正しくマッピングされるようにします。
 - d. **OK** をクリックします。
8. **OK** をクリックします。

インポートしたテンプレートは、**テンプレートのインポート** タブの一覧には表示されなくなります。

8.7. ストレージのタスク

8.7.1. ISO ストレージドメインへのイメージのアップロード

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、仮想マシンの起動用 ISO イメージを格納します。

ISO アップローダーツールにより、正しいユーザー権限で適切なディレクトリーにイメージをアップロードすることができます。詳細については、「[ISO アップローダーツール](#)」を参照してください。

物理メディアから ISO イメージを作成する方法については本ガイドでは触れていません。ご使用の環境に必要なイメージがお手元にあることを前提としています。

ISO ストレージドメインへのイメージのアップロード

1. root 権限で Manager マシンにログインします。
2. Manager マシンの一時ディレクトリーに、ISO イメージをコピーします。
3. **engine-iso-uploader** コマンドを実行します。

```
# engine-iso-uploader --iso-domain=ISO_domain upload file.iso
```



注記

管理ユーザーのユーザー名およびパスワードの入力が求められます。ユーザー名の形式は **username@domain.com** です。

イメージのサイズや使用可能な帯域幅によっては、このアクションに時間がかかる場合があります。

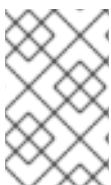
ISO イメージがアップロードされ、ISO ストレージドメイン内に表示されます。このストレージドメインがアタッチされたデータセンター内で仮想マシンを作成する際に、使用できるブートメディアの一覧に表示され、CD/DVD-ROM として仮想マシンにアタッチすることもできます。

8.7.2. データストレージドメインへのイメージのアップロード

仮想ディスクイメージおよび ISO イメージを、データストレージドメインにアップロードすることができます。

QEMU との互換性がある仮想ディスクは、仮想マシンにアタッチすることができます。仮想ディスクのタイプは、QCOW2 または Raw でなければなりません。QCOW2 仮想ディスクから作成したディスクは共有できません。QCOW2 仮想ディスクファイルには、バックアップファイルが含まれないようにしてください。

ISO ディスクイメージは、CD/DVD-ROM として仮想マシンにアタッチすることができます。



注記

REST API を使用して仮想ディスクイメージおよび ISO イメージをアップロードする場合は、『[REST API Guide](#)』の「[ImageTransfers](#)」および「[ImageTransfer](#)」を参照してください。

前提条件

- **engine-setup** を使用して設定されたイメージ I/O プロキシ (**ovirt-imageio-proxy**)。詳細については、『[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。
- 必須の認証局の証明書を、管理ポータルへのアクセスに使用する Web ブラウザーにインポートする必要があります。

認証局の証明書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 に進み、信頼設定をすべて有効にします。認証局の証明書のインストール方法については、「[How do I add the RHEV-M CA to Firefox so that I can use https to access the WebAdmin Portal or the UserPortal?](#)」、「[How do I add the RHEV-M CA to Internet Explorer to access the Admin Portal or the UserPortal via https?](#)」、「[How do I add the RHV-M CA Certificate to Google Chrome?](#)」のいずれかを参照してください。

- Internet Explorer 10、Firefox 35、または Chrome 13 以降のバージョンのブラウザ。これ以前のバージョンのブラウザでは、必須の HTML5 API がサポートされません。

データストレージドメインへのイメージのアップロード

1. **ストレージ → ディスク** をクリックします。
2. **アップロード** メニューから **開始** を選択します。
3. **ファイルを選択** をクリックし、アップロードするイメージを選択します。
4. **ディスクのオプション** のフィールドに入力します。各フィールドの説明については、「[新規仮想ディスクウィンドウの設定](#)」を参照してください。
5. **OK** をクリックします。
プログレスバーにアップロードのステータスが表示されます。**アップロード** メニューからアップロードを一時停止、キャンセル、再開することができます。
6. アップロードがタイムアウトし「**Reason: timeout due to transfer inactivity**」というメッセージが表示された場合には、タイムアウトの値を増やします。

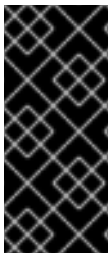
```
# engine-config -s
TransferImageClientInactivityTimeoutInSeconds=6000
```

7. **ovirt-engine** サービスを再起動します。

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

8.7.3. 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をデタッチして削除するには、メンテナンスモードに切り替えておく必要があります。これは、他のデータドメインをマスターデータドメインに指定し直すために必要です。



重要

仮想マシンがストレージドメインのリースを保持している場合には、そのストレージドメインはメンテナンスモードに切り替えることはできません。仮想マシンをシャットダウンするか、リースを削除または他のストレージドメインに移動する必要があります。仮想マシンのリースについての説明は、「[仮想マシン管理ガイド](#)」を参照してください。

ドメインがアクティブな場合のみ、LUN をさらに追加して iSCSI ドメインを拡張することができます。

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

1. ストレージドメインで実行中の仮想マシンをすべて停止します。

2. ストレージ → ドメイン をクリックします。
3. ストレージドメインの名前をクリックし、詳細ビューを表示します。
4. データセンター タブをクリックします。
5. メンテナンス をクリックします。



注記

OVF の更新失敗を無視する チェックボックスにより、OVF の更新に失敗した場合でもストレージドメインをメンテナンスモードに切り替えることができます。

6. **OK** をクリックします。

ストレージドメインがアクティブではなくなり、結果一覧に **非アクティブ** のステータスで表示されます。これで、非アクティブなストレージドメインの編集、再アクティブ化、データセンターからのデタッチ、削除を行うことができるようになりました。



注記

ドメインのアクティブ化、デタッチ、メンテナンスモードへの切り替えを行うには、ドメインが関連付けられたデータセンターの詳細ビューにある **ストレージ** タブを使用することもできます。

8.7.4. ストレージドメインの編集

管理ポータルを使用して、ストレージドメインのパラメーターを編集することができます。ストレージドメインの状態がアクティブか非アクティブかによって、編集可能なフィールドが異なります。**データセンター**、**ドメイン機能**、**ストレージタイプ**、および **形式** 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な状態の時には、**名前**、**説明**、**コメント**、**容量不足の警告 (%)**、**アクションをブロックする深刻な容量不足 (GB)**、**削除後にワイプ**、および **削除後に破棄** のフィールドを編集することが可能です。**名前** のフィールドを編集できるのは、ストレージドメインがアクティブな間のみです。他のフィールドはすべて、ストレージドメインが非アクティブでも編集することができます。
- **非アクティブ**: ストレージドメインがメンテナンスモードまたは未アタッチ (したがって非アクティブの状態) の場合には、**名前**、**データセンター**、**ドメイン機能**、**ストレージタイプ**、**形式** 以外の全フィールドを編集することができます。ストレージ接続、マウントオプション、その他の詳細パラメーターを編集するには、ストレージドメインが非アクティブである必要があります。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ています。



注記

iSCSI ストレージの接続は、管理ポータルを使用しては編集できませんが、REST API で編集可能です。**『REST API Guide』** の [「StorageServerConnectionExtension - update」](#) を参照してください。

アクティブなストレージドメインの編集

1. ストレージ → ドメイン をクリックして、ストレージドメインを選択します。

2. **ドメインを管理** をクリックします。
3. 必要に応じて、編集可能なフィールドを編集します。
4. **OK** をクリックします。

非アクティブなストレージドメインの編集

1. **ストレージ → ドメイン** をクリックします。
2. ストレージドメインがアクティブな場合には、メンテナンスモードに切り替えます。
 - a. ストレージドメインの名前をクリックし、詳細ビューを表示します。
 - b. **データセンター** タブをクリックします。
 - c. **メンテナンス** をクリックします。
 - d. **OK** をクリックします。
3. **ドメインを管理** をクリックします。
4. ストレージパスおよびその他の情報を編集します。新しい接続情報は、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. ストレージドメインをアクティブ化します。
 - a. ストレージドメインの名前をクリックし、詳細ビューを表示します。
 - b. **データセンター** タブをクリックします。
 - c. **アクティブ化** をクリックします。

8.7.5. OVF の更新

デフォルトでは、OVF は 60 分ごとに更新されます。ただし、重要な仮想マシンをインポートした場合や重要な更新を実施した場合には、OVF を手動で更新することができます。

OVF の更新

1. **ストレージ → ドメイン** をクリックします。
2. ストレージドメインを選択し、**その他の操作 → OVF を更新** をクリックします。
OVF が更新され、メッセージが **イベント** に表示されます。

8.7.6. メンテナンスモード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る場合は、ストレージドメインをメンテナンスモードに切り替える必要があります。使用を再開するには、ストレージドメインをアクティブ化します。

1. **ストレージ → ドメイン** をクリックします。
2. 非アクティブなストレージドメインの名前をクリックし、詳細ビューを表示します。
3. **データセンター** タブをクリックします。

4. アクティブ化 をクリックします。



重要

データドメインよりも先に ISO ドメインをアクティブ化しようとする、エラーメッセージが表示され、そのドメインはアクティブ化されません。

8.7.7. データセンターからのストレージドメインのデタッチ

ストレージドメインをあるデータセンターからデタッチして、別のデータセンターに移行します。

データセンターからのストレージドメインのデタッチ

1. ストレージ → ドメイン をクリックします。
2. ストレージドメインの名前をクリックし、詳細ビューを表示します。
3. データセンター タブをクリックします。
4. メンテナンス をクリックします。
5. **OK** をクリックしてメンテナンスモードを開始します。
6. **デタッチ** をクリックします。
7. **OK** をクリックしてストレージドメインをデタッチします。

ストレージドメインがデータセンターからデタッチされ、別のデータセンターをアタッチする準備ができました。

8.7.8. データセンターへのストレージドメインのアタッチ

データセンターにストレージドメインをアタッチします。

データセンターへのストレージドメインのアタッチ

1. ストレージ → ドメイン をクリックします。
2. ストレージドメインの名前をクリックし、詳細ビューを表示します。
3. データセンター タブをクリックします。
4. **アタッチ** をクリックします。
5. 対象のデータセンターを選択します。
6. **OK** をクリックします。

ストレージドメインがデータセンターにアタッチされ、自動的にアクティブ化されます。

8.7.9. ストレージドメインの削除

データセンター内のストレージドメインを仮想化環境から削除します。

ストレージドメインの削除

1. **ストレージ → ドメイン** をクリックします。
2. ストレージドメインをメンテナンスモードに切り替えて、デタッチします。
 - a. ストレージドメインの名前をクリックし、詳細ビューを表示します。
 - b. **データセンター** タブをクリックします。
 - c. **メンテナンス** をクリックして、**OK** をクリックします。
 - d. **デタッチ** をクリックして、**OK** をクリックします。
3. **削除** をクリックします。
4. オプションとして、**ドメインをフォーマットします。ストレージの中身が失われます。** のチェックボックスを選択して、ドメインの中身を消去します。
5. **OK** をクリックします。

ストレージドメインが環境から完全に削除されました。

8.7.10. 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、通常の手順で削除することができません。ストレージドメインを強制的に破棄することによって、そのストレージドメインは仮想化環境から削除されます。

ストレージドメインの破棄

1. **ストレージ → ドメイン** をクリックします。
2. ストレージドメインを選択し、**その他の操作 → 破棄** をクリックします。
3. **操作を承認** のチェックボックスを選択します。
4. **OK** をクリックします。

8.7.11. ディスクプロファイルの作成

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、データセンター下で定義されているストレージプロファイルをベースに作成されますが、プロファイルを有効にするには、個別の仮想ディスクに手動で割り当てる必要があります。

以下の手順は、ストレージドメインの属するデータセンター下でストレージ QoS エントリーが 1 つ以上定義済みであることを前提としています。

ディスクプロファイルの作成

1. **ストレージ → ドメイン** をクリックします。
2. データストレージドメインの名前をクリックして、詳細ビューを表示します。
3. **ディスクプロファイル** タブをクリックします。
4. **新規作成** をクリックします。
5. ディスクプロファイルの **名前** と **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 QoS を選択します。

7. **OK** をクリックします。

8.7.12. 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。





ディスクプロファイルの削除

1. **ストレージ → ドメイン** をクリックします。
2. データストレージドメインの名前をクリックして、詳細ビューを表示します。
3. **ディスクプロファイル** タブをクリックします。
4. 削除するディスクプロファイルを選択します。
5. **削除** をクリックします。
6. **OK** をクリックします。

そのディスクプロファイルが仮想ディスクに割り当てられていた場合は、それらの仮想ディスクからディスクプロファイルが削除されます。

8.7.13. ストレージドメインのヘルスステータスの確認

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ステータスがあります。外部のヘルスステータスはプラグインまたは外部のシステムによってレポートされるか、管理者によって設定され、ストレージドメインの **名前** の左側に以下のアイコンのいずれかが表示されます。

- **OK:** アイコンなし
- **情報:** 
- **警告:** 
- **エラー:** 
- **異常:** 

ストレージドメインのヘルスステータスについての更に詳しい情報を確認するには、ストレージドメイン名をクリックして詳細ビューを表示し、**イベント** タブをクリックしてください。

ストレージドメインのヘルスステータスは、REST API を使用して確認することも可能です。ストレージドメインに対する **GET** 要求には、ヘルスステータスが記載された **external_status** 要素が含まれます。

events コレクションで REST API 内のストレージドメインのヘルスステータスを設定することができます。『**REST API Guide**』の「[Events - add](#)」のセクションを参照してください。

8.7.14. ストレージドメインの削除後に破棄の設定

削除後に破棄 のチェックボックスを選択すると、ストレージの削除時に論理ボリューム上で **blkdiscard** コマンドが呼び出され、下層のストレージにはブロックが解放されたことが通知されま

す。ストレージアレイは解放された領域を使用して、要求に応じて割り当てを行います。**削除後に破棄**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の場合には、Red Hat Virtualization Manager ではこのフラグを使用できません。

制限事項:

- **削除後に破棄** は iSCSI、ファイバーチャネルなどのブロックストレージドメインでのみ利用可能です。
- 下層のストレージが **Discard** をサポートしている必要があります。

削除後に破棄 はブロックストレージドメインの作成時や編集時に有効化することができます。「[ブロックストレージの追加](#)」および「[ストレージドメインの編集](#)」を参照してください。

第9章 プール

9.1. 仮想マシンプールについて

仮想マシンプールは、すべて同じテンプレートからクローン作成した仮想マシンのグループです。グループ内のいずれのユーザーも、プール内の仮想マシンをオンデマンドで使用することができます。仮想マシンプールにより、管理者は、一般化された仮想マシンのセットをユーザー向けに迅速に設定することができます。

ユーザーは、仮想マシンプールから仮想マシンを取得することによって、その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、プール内に利用可能な仮想マシンがある場合には、その中の1つが提供されます。その仮想マシンには、プールのベースとなっているテンプレートと同じオペレーティングシステムと設定が適用されますが、ユーザーが仮想マシンを取得する度に同じ仮想マシンは割り当てられません。仮想マシンプールの設定によっては、ユーザーが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可能です。

デフォルトでは仮想マシンプールはステートレスであるため、再起動後には仮想マシンのデータは維持されませんが、プールをステートフルに設定することができ、この場合には、以前のユーザーが加えた変更が維持されます。ただし、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ユーザーが設定すると、それらのオプションはその仮想マシンプールでそのユーザーのデフォルトオプションとして設定されます。



注記

管理ポータルからアクセスした場合には、プールから取得した仮想マシンは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むことができるようにする必要があるためです。

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時点で起動し、ユーザーが使用を終了した時点でシャットダウンされますが、仮想マシンプールには、事前起動済みの仮想マシンを用意することもできます。事前起動済みの仮想マシンは、Up のステータスで維持され、ユーザーが取得するまではアイドル状態となります。これによりユーザーは、その仮想マシンを即時に使用開始することができますが、これらの仮想マシンは、アイドル時にもシステムリソースを消費します。

9.2. 仮想マシンプールの作成

仮想マシンプールを作成し、共通のテンプレートをベースにした複数の仮想マシンを含めることができます。仮想マシンのシーリングおよびテンプレートの作成については、『[仮想マシン管理ガイド](#)』の「[テンプレート](#)」を参照してください。

Windows 仮想マシンにおける Sysprep ファイルの設定オプション

必要に応じて、**sysprep** ファイルのさまざまな設定オプションを利用することができます。

プールをドメインにアタッチする必要がなければ、`/usr/share/ovirt-engine/conf/sysprep/`にあるデフォルトの **sysprep** ファイルを使用することができます。

プールをドメインにアタッチする必要がある場合は、それぞれの Windows オペレーティングシステム用のカスタム **sysprep** を作成することができます。

1. それぞれのオペレーティングシステムの該当部分を `/usr/share/ovirt-engine/conf/osinfo-defaults.properties` から新しいファイルにコピーし、**99-defaults.properties** として保存します。

2. **99-defaults.properties** において、Windows アクティベーション用プロダクトキーおよび新しいカスタム **sysprep** ファイルのパスを指定します。

```
os.operating_system.productKey.value=Windows_product_activation_key
...
os.operating_system.sysprepPath.value =
${ENGINE_USR}/conf/sysprep/sysprep.operating_system
```

3. 新しい **sysprep** ファイルを作成し、ドメイン、ドメインのパスワード、およびドメインの管理者を指定します。

```
<Credentials>
  <Domain>AD_Domain</Domain>
  <Password>Domain_Password</Password>
  <Username>Domain_Administrator</Username>
</Credentials>
```

Windows 仮想マシンのさまざまなプールに対応するために、さまざまな **sysprep** 設定を定義する必要がある場合には、管理ポータルでカスタム **sysprep** ファイルを作成することができます (以下に示す「[仮想マシンプールの作成](#)」を参照してください)。詳細については、『[仮想マシン管理ガイド](#)』の「[Sysprep を使用した仮想マシンの設定の自動化](#)」を参照してください。

仮想マシンプールの作成

1. コンピュート → プール をクリックします。
2. **新規作成** 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** を選択します。
4. ドロップダウンメニューから **テンプレート** およびバージョンを選択します。テンプレートはプール内の全仮想マシンの標準設定を提供します。
5. ドロップダウンリストから **オペレーティングシステム** を選択します。
6. **最適化オプション** のドロップダウンリストを使用して、仮想マシンを **デスクトップ** 用または **サーバー** 用に最適化します。



注記

ハイパフォーマンス仮想マシンは単一のホストおよび特定のリソースに固定されるので、プールの最適化オプションに **ハイパフォーマンス** を設定することは推奨されません。そのような設定の仮想マシンが複数含まれるプールは、正しく機能しません。

7. **名前** ならびにオプションとして **説明** および **コメント** を入力します。
プール内の各仮想マシンには、数字の接尾辞と共にこのプールの **名前** が適用されます。**?** をプレースホルダーとして、仮想マシンの番号付けをカスタマイズすることができます。

例9.1 プール名と仮想マシンの番号付けの例

- プール: **MyPool1**
仮想マシン: **MyPool1-1**、**MyPool1-2**、... **MyPool1-10**

- プール: **MyPool-???**
仮想マシン: **MyPool-001**、**MyPool-002**、... **MyPool-010**

8. プール内の **仮想マシン数** を入力します。
9. **事前起動済みの仮想マシン** 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。
10. **最大仮想マシン数/ユーザー** で、1 ユーザーが 1 セッションで実行できる仮想マシンの最大数を指定します。最小値は 1 です。
11. **削除防止** のチェックボックスを選択して、削除防止の設定を有効にします。
12. Windows 以外の仮想マシンのプールを作成する場合、またはデフォルトの **sysprep** を使用する場合には、このステップを省略してください。Windows 仮想マシンのプール用にカスタム **sysprep** ファイルを作成する場合は、以下の手順を実施してください。
 - a. **詳細オプションを表示** ボタンをクリックします。
 - b. **初期起動** タブをクリックし、**Cloud-Init/Sysprep を使用** のチェックボックスを選択します。
 - c. **認証** の矢印をクリックし、**ユーザー名** と **パスワード** を入力するか、**設定済みのパスワードを使用** を選択します。



注記

この **ユーザー名** は、ローカルの管理者名です。この **認証** セクションまたはカスタム **sysprep** ファイルで、その値をデフォルト値 (**user**) から変更することができます。

- d. **カスタムスクリプト** の矢印をクリックし、テキストボックスに **/usr/share/ovirt-engine/conf/sysprep/** にあるデフォルトの **sysprep** ファイルの内容を貼り付けます。
- e. **sysprep** ファイルの以下の値を変更することができます。
 - **Key**. 事前定義の Windows アクティベーション用プロダクトキーを使用しない場合は、`<![CDATA[$ProductKey$]]>` を有効なプロダクトキーに置き換えます。

```
<ProductKey>
  <Key><![CDATA[$ProductKey$]]></Key>
</ProductKey>
```

例9.2 Windows プロダクトキーの例

```
<ProductKey>
  <Key>0000-0000-0000-0000</Key>
</ProductKey>
```

- Windows 仮想マシンをアタッチする **Domain**、ドメインの **Password**、およびドメイン管理者の **Username**:

```
<Credentials>
  <Domain>AD_Domain</Domain>
  <Password>Domain_Password</Password>
  <Username>Domain_Administrator</Username>
</Credentials>
```

例9.3 ドメイン認証情報の例

```
<Credentials>
  <Domain>addomain.local</Domain>
  <Password>12345678</Password>
  <Username>Sarah_Smith</Username>
</Credentials>
```



注記

Domain、**Password**、および **Username** はドメインへのアタッチに必要です。**Key** はアクティベーション用です。両方は必要ありません。

ドメインおよび認証情報を **初期起動** タブで変更することはできません。

- ローカルの管理者の **FullName**:

```
<UserData>
  ...
  <FullName>Local_Administrator</FullName>
  ...
</UserData>
```

- ローカルの管理者の **DisplayName** および **Name**:

```
<LocalAccounts>
  <LocalAccount wcm:action="add">
    <Password>
      <Value><![CDATA[$AdminPassword$]]></Value>
      <PlainText>true</PlainText>
    </Password>
    <DisplayName>Local_Administrator</DisplayName>
    <Group>administrators</Group>
    <Name>Local_Administrator</Name>
  </LocalAccount>
</LocalAccounts>
```

sysprepファイルの残りの変数は、**初期起動** タブで入力することができます。

13. オプションとして、**プールタイプ** を設定します。

a. **タイプ** タブをクリックして **プールタイプ** を選択します。

- 手動**: 管理者は、仮想マシンをプールに明示的に返却する責任があります。

- **自動:** 仮想マシンは自動的に仮想マシンプールに返却されます。
 - b. 仮想マシンを必ずステートフルモードで起動するには、**ステートフルプール** のチェックボックスを選択します。これにより、前のユーザーが仮想マシンに加えた変更が維持されます。
 - c. **OK** をクリックします。
14. オプションとして、SPICE プロキシを上書きします。
- a. **コンソール タブで SPICE プロキシを上書きする** のチェックボックスを選択します。
 - b. **SPICE プロキシアドレスの上書き** のテキストフィールドで、グローバルの SPICE プロキシを上書きする SPICE プロキシのアドレスを指定します。
 - c. **OK** をクリックします。
15. Windows 仮想マシンのプールの場合は、**コンピューター → 仮想マシン** をクリックし、プールからそれぞれの仮想マシンを選択して **実行 → 1 回実行** をクリックします。

注記

仮想マシンが起動せず、`%WINDIR%\panther\UnattendGC\setupact.log` に「**Info [windeploy.exe] Found no unattend file**」と表示される場合は、プールのテンプレートを作成するために使用した Windows 仮想マシンのレジストリーに、**UnattendFile** キーを追加します。

1. Windows 仮想マシンに unattend ファイルが入ったフロッピーデバイスがアタッチされていることを確認します (例: `A:\Unattend.xml`)。
2. **スタート** をクリックして **実行** をクリックし、**開く** テキストボックスに `regedit` と入力して **OK** をクリックします。
3. 左側のペインで **HKEY_LOCAL_MACHINE → SYSTEM → Setup** の順に移動します。
4. 右側のペインで右クリックし、**新規 → 文字列値** を選択します。
5. キー名に **UnattendFile** と入力します。
6. 新しいキーをダブルクリックし、キーの値として **unattend** ファイルの名前およびパスを入力します (例: `A:\Unattend.xml`)。
7. レジストリーを保存し、Windows 仮想マシンをシーリングして新規テンプレートを作成します。詳細については、『[仮想マシン管理ガイド](#)』の「[テンプレート](#)」を参照してください。

指定した数の同一の仮想マシンが入った仮想マシンプールの作成と設定が完了しました。これらの仮想マシンは、**コンピューター → 仮想マシン** で、またはプールの名前をクリックして表示される詳細ビューで確認することができます。仮想マシンプール内の仮想マシンと独立した仮想マシンは、アイコンで見分けることができます。

9.3. 新規プールおよびプールの編集ウィンドウの設定とコントロール

9.3.1. 新規プールおよびプールの編集における全般の設定

以下の表には、**新規プール** および **プールの編集** ウィンドウの **全般** タブに必要な、仮想マシンプール固有の情報をまとめています。その他の設定は、**新規仮想マシン** ウィンドウと全く同じです。

表9.1 全般 の設定

フィールド名	説明
テンプレート	仮想マシンプールのベースとなっているテンプレートおよびテンプレートのサブバージョン。テンプレートの 最新 サブバージョンをベースに仮想マシンプールを作成する場合、そのプール内の全仮想マシンはリブート時に最新のテンプレートバージョンを自動的に受け取ります。仮想マシンのテンプレートの設定に関する詳しい情報は、『 仮想マシン管理ガイド 』の「 仮想マシンの全般の設定 」および「 新規テンプレートウィンドウの設定 」を参照してください。
説明	仮想マシンプールのわかりやすい説明
コメント	仮想マシンプールに関する、人間が判読できるプレーンテキスト形式のコメントを追加するためのフィールド
事前起動済みの仮想マシン	ユーザーが取得する前に起動され、取得するまでその状態で維持される、仮想マシンプール内の仮想マシンの数を指定することができます。このフィールドの値は、 0 以上で、仮想マシンプール内の仮想マシンの合計数以下とする必要があります。
仮想マシン数/プールに追加する仮想マシンの数	仮想マシンプール内に作成され、使用可能となる仮想マシンの数を指定することができます。編集のウィンドウでは、数を指定して仮想マシンプール内の仮想マシン数を増やすことができます。デフォルトでは、1 プール内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 キーで設定することができます。
最大仮想マシン数/ユーザー	1 ユーザーが仮想マシンプールから 1 回に取得できる仮想マシンの最大数を指定することができます。このフィールドの値は、 1 から 32,767 までの範囲内とする必要があります。
削除防止	プール内の仮想マシンが削除されるのを防ぐことができます。

9.3.2. 新規プールおよびプールの編集におけるタイプの設定

以下の表には、**新規プール** および **プールの編集** ウィンドウの **タイプ** タブに必要な情報をまとめています。

表9.2 タイプ の設定

フィールド名	説明
プールタイプ	<p>このドロップダウンメニューで、仮想マシンプールのタイプを指定することができます。以下のオプションが利用可能です。</p> <ul style="list-style-type: none"> ● 自動: 仮想マシンプールから取得した仮想マシンをユーザーが使い終わった後に、その仮想マシンは自動的に仮想マシンプールに返却されます。 ● 手動: 仮想マシンプールから取得した仮想マシンをユーザーが使い終わった後に、管理者が手動で仮想マシンを返却した場合にのみ、その仮想マシンは仮想マシンプールに返却されます。
ステートフルプール	<p>プール内の仮想マシンが別のユーザーに渡された時に、仮想マシンの状態が維持されるかどうかを指定します。選択すると、前のユーザーが仮想マシンに加えた変更が維持されます。</p>

9.3.3. 新規プールおよびプールの編集におけるコンソールの設定

以下の表には、**新規プール** または **プールの編集** ウィンドウの **コンソール** タブに必要な、仮想マシンプール固有の情報をまとめています。その他の設定は、**新規仮想マシン** および **仮想マシンの編集** ウィンドウと全く同じです。

表9.3 コンソール の設定

フィールド名	説明
SPICE プロキシを上書きする	<p>グローバル設定で定義されている SPICE プロキシの上書きを有効にするには、このチェックボックスを選択します。この機能は、ホストが属するネットワークの外部からユーザーが接続する場合 (例: VM ユーザーポータルからの接続) に有用です。</p>
SPICE プロキシアドレスの上書き	<p>SPICE クライアントが仮想マシンに接続するのに使用するプロキシ。このプロキシは、Red Hat Virtualization 環境で定義されているグローバル SPICE プロキシと、仮想マシンプールが属する (該当する場合) クラスターの SPICE プロキシの両方を上書きします。アドレスは以下の形式にする必要があります。</p> <p>protocol://host:port</p>

9.3.4. 仮想マシンプールのホストの設定

以下の表には、**新規プール** および **プールの編集** ウィンドウの **ホスト** タブで使用可能なオプションについての説明をまとめています。

表9.4 仮想マシンプールのホストの設定

フィールド名	サブ要素	説明
実行を開始するホスト		<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てください。</p> <ul style="list-style-type: none"> ● クラスター内の任意のホスト: 仮想マシンはクラスター内の使用可能な任意のホストで起動、実行できます。 ● 特定のホスト: 仮想マシンは、クラスター内の特定のホストで起動します。ただし、Manager または管理者は、仮想マシンの移行/高可用性の設定に応じて、クラスター内の別のホストに仮想マシンを移行することが可能です。使用可能なホストの一覧から、特定のホストまたはホストのグループを選択します。
移行のオプション	移行モード	<p>仮想マシンの実行/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には、仮想マシンはクラスターのポリシーに従って実行/移行されます。</p> <ul style="list-style-type: none"> ● 手動および自動の移行を許可する: 仮想マシンは、環境のステータスに応じてホスト間で自動移行されるか、管理者が手動で移行することができます。 ● 手動の移行のみを許可する: 仮想マシンは、管理者による手動のホスト間移行のみが可能です。 ● 移行を許可しない: 仮想マシンは、自動または手動のいずれでも移行することはできません。

フィールド名	サブ要素	説明
	カスタム移行ポリシーを使用する	<p>移行収束のポリシーを定義します。チェックボックスにチェックが入っていない場合は、ホストがポリシーを決定します。</p> <ul style="list-style-type: none"> Legacy: バージョン 3.6 のレガシーの動作。デフォルトの動作に優先する vdsm.conf への設定変更が、そのまま適用されます。ゲストエージェントのフックメカニズムは無効になります。 Minimal downtime: 一般的な状況での仮想マシンの移行が可能です。仮想マシンのダウンタイムは長時間にならないはずです。長時間経過した後に仮想マシンの移行が収束しない場合は、移行が中断されます (QEMU の繰り返し回数によりますが、最大でも 500 ミリ秒)。ゲストエージェントのフックメカニズムは有効になります。 Suspend workload if needed: 仮想マシンが大きなワークロードを実行している場合を含め、多くの状況で仮想マシンを移行できます。仮想マシンのダウンタイムはさらに長時間にわたる可能性があります。極端に大きなワークロードの場合には、移行が中断されてしまう可能性があります。ゲストエージェントのフックメカニズムは有効になります。
	カスタム移行ダウンタイムを使用	<p>このチェックボックスにより、ライブマイグレーション中の仮想マシンの最長ダウンタイムをミリ秒単位で指定することができます。各仮想マシンのワークロードと SLA の要件に応じて、異なる最長ダウンタイムを設定してください。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
	移行の自動収束	<p>移行ポリシーが Legacy の場合にのみ有効です。このオプションでは、仮想マシンのライブマイグレーション中に自動収束を使用するかどうかを設定することができます。ワークロードが大きくサイズの大きい仮想マシンは、ライブマイグレーション中に到達する転送速度よりも早くメモリーをダーティーな状態にして、移行を収束できないようにする可能性があります。QEMU の自動収束機能は、仮想マシンの移行を強制的に収束することができます。移行が収束されていない場合には、QEMU が自動的に検出して、仮想マシンの vCPU の使用率を制限します。デフォルトでは、自動収束はグローバルレベルで無効化されています。</p> <ul style="list-style-type: none">● クラスター設定から継承する を選択して、クラスターレベルで設定されている自動収束設定を使用します。このオプションは、デフォルトで選択されています。● クラスター設定またはグローバル設定を無効にして仮想マシンの自動収束を可能にするには、自動収束 を選択します。● クラスター設定またはグローバル設定を無効にして仮想マシンの自動収束を避けるには、自動収束しない を選択します。

フィールド名	サブ要素	説明
	移行時の圧縮の有効化	<p>移行ポリシーが Legacy の場合にのみ有効です。このオプションでは、仮想マシンのライブマイグレーション中に移行の圧縮を使用するかどうかを設定することができます。この機能は、Xor Binary Zero Run-Length-Encoding を使用して、仮想マシンのダウンタイム、およびメモリーの書き込みの多いワークロードを実行する仮想マシンやメモリー更新パターンがスパースなアプリケーションの合計ライブマイグレーション時間を減らします。デフォルトでは、移行の圧縮はグローバルレベルで無効化されています。</p> <ul style="list-style-type: none"> ● クラスター設定から継承する を選択して、クラスターレベルで設定されている圧縮設定を使用します。このオプションは、デフォルトで選択されています。 ● クラスター設定またはグローバル設定を無効にして仮想マシンの圧縮を可能にするには、圧縮 を選択します。 ● クラスター設定またはグローバル設定を無効にして仮想マシンの圧縮を避けるには、圧縮しない を選択します。
	ホストの CPU をパススルーする	<p>このチェックボックスにより、仮想マシンはその仮想マシンが配置されているホストの物理 CPU の機能を活用することができます。このオプションは、移行を許可しない が選択されている場合のみ有効にすることができます。</p>
NUMA の設定	NUMA ノード数	<p>仮想マシンに割り当てる仮想 NUMA ノードの数。チューニングモード が 優先 に指定されている場合には、この値は 1 に設定する必要があります。</p>

フィールド名	サブ要素	説明
	チューニングモード	<p>メモリーの割り当てに使用する方 法</p> <ul style="list-style-type: none"> ● 厳格: ターゲットノード でメモリーを割り当てる ことができない場合には メモリーの割り当ては失 敗します。 ● 優先: 単一の優先ノード からのみメモリーの割り 当てが行われます。十分 なメモリーが使用できな い場合には、他のノード からメモリーを割り当て ることができます。 ● インターリーブ: 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 固定	<p>NUMA トポロジー ウィンドウが 開きます。このウィンドウでは、 ホストの合計 CPU、メモリー、 NUMA ノード、仮想マシンの仮想 NUMA ノードが表示されます。右 側のボックスから各仮想 NUMA をクリックし、左側の NUMA ノードにドラッグして、仮想 NUMA ノードをホストの NUMA ノードに固定します。</p>

9.3.5. 新規プールおよびプールの編集におけるリソースの割り当ての設定

以下の表には、**新規プール** および **プールの編集** ウィンドウの **リソースの割り当て** タブに必要な、仮想マシンプール固有の情報をまとめています。その他の設定は、**新規仮想マシン** ウィンドウと全く同じです。詳細については、『**仮想マシン管理ガイド**』の「**仮想マシンにおけるリソースの割り当ての設定**」を参照してください。

表9.5 リソースの割り当て の設定

フィールド名	サブ要素	説明
ディスクの割り当て	ターゲットを自動選択	<p>空き容量が最も大きいストレージ ドメインを自動的に選択するに は、このチェックボックスを選択 します。ターゲット および ディ スクプロファイル フィールドは 無効になります。</p>

フィールド名	サブ要素	説明
	形式	このフィールドは読み取り専用で、ストレージドメインのタイプに OpenStack Volume (Cinder) を設定しない限り常に QCOW2 と表示されます。OpenStack Volume の場合、形式は Raw となります。

9.4. 仮想マシンプールの編集

仮想マシンプールの作成後にそのプロパティを編集することができます。仮想マシンプールの編集時に指定できるプロパティは、**仮想マシン数** プロパティが **プールに追加する仮想マシンの数** に置き換えられる以外は、新規仮想マシンプールの作成時に指定できるプロパティと全く同じです。



注記

仮想マシンプールを編集すると、加えた変更は新しい仮想マシンだけに適用されます。変更を加えた時にすでに存在する仮想マシンには、変更は適用されません。

仮想マシンプールの編集

1. **コンピュート** → **プール** をクリックして、仮想マシンプールを選択します。
2. **編集** をクリックします。
3. 仮想マシンプールのプロパティを編集します。
4. **OK** をクリックします。

9.5. プール内の仮想マシンの事前起動

仮想マシンプール内では、各マシンはデフォルトで電源がオフの状態となっています。ユーザーがプールから仮想マシンを要求すると、マシンの電源が投入され、ユーザーに割り当てられます。一方、事前起動済みの仮想マシンはすでに起動しており、ユーザーを割り当てられるのを待機している状態なので、ユーザーがマシンにアクセスするまでの待機時間が短縮されます。事前起動済みの仮想マシンがシャットダウンされると、プールに戻り、元の状態に復元されます。事前起動済みの仮想マシンの最大数は、プール内の仮想マシンの数です。

事前起動済みの仮想マシンは、ユーザーが特にユーザー割り当てがさ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。自動プールのみが事前起動済みの仮想マシンに対応しています。

プール内の仮想マシンの事前起動

1. **コンピュート** → **プール** をクリックして、仮想マシンプールを選択します。
2. **編集** をクリックします。
3. **事前起動済みの仮想マシン** 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. **タイプ** タブをクリックし、**プールタイプ** が **自動** 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。

9.6. 仮想マシンプールへの仮想マシン追加

仮想マシンプールで最初にプロビジョニングされた数以上の仮想マシンが必要な場合には、そのプールにマシンを追加します。

仮想マシンプールへの仮想マシン追加

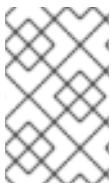
1. **コンピュー**ト → **プール** をクリックして、仮想マシンプールを選択します。
2. **編集** をクリックします。
3. **プールに追加する仮想マシンの数** フィールドに、追加する仮想マシンの数を入力します。
4. **OK** をクリックします。

9.7. 仮想マシンプールからの仮想マシンのデタッチ

仮想マシンプールから仮想マシンをデタッチします。プールから仮想マシンをデタッチすると、独立した仮想マシンとなります。

仮想マシンプールからの仮想マシンのデタッチ

1. **コンピュー**ト → **プール** をクリックします。
2. プール名をクリックし、詳細ビューを表示します。
3. **仮想マシン** タブをクリックすると、プール内の仮想マシンが一覧表示されます。
4. 実行中の仮想マシンはデタッチできないので、その仮想マシンのステータスが **Down** であることを確認してください。
5. 仮想マシンを1つまたは複数選択して、**デタッチ** をクリックします。
6. **OK** をクリックします。



注記

仮想マシンはまだ環境に存在しており、**コンピュー**ト → **仮想マシン** で表示およびアクセスすることができます。アイコンが変わり、仮想マシンがデタッチされて独立した仮想マシンになったことがわかる点に注意してください。

9.8. 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することができます。そのプール内の仮想マシンはすべて、あらかじめ削除またはデタッチしておく必要があります。仮想マシンをプールからデタッチすると、独立した仮想マシンとして保持されます。

仮想マシンプールの削除

1. **コンピュー**ト → **プール** をクリックして、仮想マシンプールを選択します。

2. **削除** をクリックします。

3. **OK** をクリックします。

9.9. 信頼済みコンピュートプール

信頼済みのコンピュートプールは、Intel Trusted Execution Technology (Intel TXT) をベースとするセキュアなクラスターです。信頼済みクラスターは、Intel の OpenAttestation で検証済みのホストのみを許可します。OpenAttestation は、ホストのハードウェアとソフトウェアをホワイトリストデータベースと比較して整合性を評価します。信頼済みのホストと、そのホスト上で実行される仮想マシンには、セキュリティ要件の高いタスクを割り当てることができます。Intel TXT、信頼済みシステム、およびアテステーション (証明) についての詳しい情報は、『[Intel® Trusted Execution Technology \(Intel® TXT\) Enabling Guide](#)』を参照してください。

信頼済みのコンピュートプールを作成するには、以下のステップを実行します。

- Manager が OpenAttestation サーバーと通信するように設定します。
- 信頼済みのホストのみを実行することが可能な信頼済みクラスターを作成します。
- 信頼済みホストを信頼済みクラスターに追加します。OpenAttestation サーバーがホストを検証するには、そのホストが 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、ホスト上での OpenAttestation エージェントのインストール、およびホワイトリストデータベースの作成方法についての説明は、<https://github.com/OpenAttestation/OpenAttestation/wiki> を参照してください。

9.9.1. OpenAttestation サーバーを Manager に接続する方法

信頼済み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 サーバーの完全修飾ドメイン名または IP アドレスを追加します。

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

必要な場合には、以下の設定も変更することができます。

表9.6 engine-config の OpenAttestation 設定

オプション	デフォルト値	説明
AttestationServer	oat-server	OpenAttestation サーバーの完全修飾ドメイン名または IP アドレス。これは、Manager が OpenAttestation サーバーと通信するために設定する必要があります。
AttestationPort	8443	OpenAttestation サーバーが Manager と通信するために使用するポート

オプション	デフォルト値	説明
AttestationTruststore	TrustStore.jks	OpenAttestation サーバーとの通信をセキュリティー保護するために使用するトラストストア
AttestationTruststorePass	password	トラストストアへのアクセスに使用するパスワード
AttestationFirstStageSize	10	簡易初期化に使用します。適切な理由がない場合には、この値は変更しないことを推奨します。
SecureConnectionWithOATServers	true	OpenAttestation サーバーとのセキュアな通信を有効化または無効化します。
PollUri	AttestationService/resources/PollHosts	OpenAttestation サービスへのアクセスに使用する URI

9.9.2. 信頼済みクラスターの作成

信頼済みクラスターは、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。ホストが信頼済みクラスターに追加されると、OpenAttestation サーバーは、ホストのハードウェアおよびソフトウェアをホワイトリストデータベースと比較します。仮想マシンは、信頼済みクラスター内の信頼済みホストの間で移行できるので、セキュアな環境で高可用性を得ることができます。

信頼済みクラスターの作成

1. **コンピュート → クラスター** をクリックします。
2. **新規作成** をクリックします。
3. クラスターの **名前** を入力します。
4. **Virt サービスを有効にする** のチェックボックスを選択します。
5. **スケジューリングポリシー** タブをクリックし、**信頼済みサービスを有効にする** のチェックボックスを選択します。
6. **OK** をクリックします。

9.9.3. 信頼済みホストの作成

Red Hat Enterprise Linux ホストを信頼済みクラスターに追加して、OpenAttestationサーバーのホワイトリストデータベースと比較することができます。ホストが OpenAttestation サーバーに信頼されるには、以下の要件を満たす必要があります。

- BIOS で Intel TXT が有効化されていること。
- OpenAttestation エージェントがインストール済みで実行中であること。

- ホスト上で実行中のソフトウェアが OpenAttestation サーバーのホワイトリストデータベースと一致していること。

信頼済みホストの作成

1. コンピュート → ホスト をクリックします。
2. 新規作成 をクリックします。
3. ホストクラスター のドロップダウンリストから、信頼済みの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 ホスト名 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。

ホストが信頼済みクラスターに追加された後には、OpenAttestation サーバーによって評価されます。ホストが OpenAttestation サーバーに信頼されなかった場合には、ステータスが **Non Operational** となり、信頼済みクラスターから削除する必要があります。

第10章 仮想ディスク

10.1. 仮想マシンストレージについての知識

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。

各タイプでは、Storage Pool Manager (SPM) という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で唯一フルアクセスのあるノードです。SPM はストレージドメインのメタデータおよびプールのメタデータを変更することができます。それ以外のホストはすべて、仮想マシンのハードディスクのメタデータにしかアクセスできません。

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の場合に、SPM は仮想ディスクをシンプロビジョニング形式でファイルシステム内のファイルとして作成します。

iSCSI およびその他のブロックベースのデータセンターの場合には、SPM は提供される論理ユニット番号 (LUN) の最上位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。ブロックベースストレージ上の仮想ディスクは、デフォルトで事前割り当てられます。

事前割り当て済みの仮想ディスクの場合には、指定したサイズ (GB 単位) の論理ボリュームが作成されます。**kpartx**、**vgscan**、**vgchange**、**mount** のいずれかを使用して仮想マシンを Red Hat Enterprise Linux サーバーにマウントし、その仮想マシンのプロセスや問題を調べることができます。

シンプロビジョニングされた仮想ディスクの場合には、1 GB の論理ボリュームが作成されます。この論理ボリュームは、仮想マシンを実行しているホストによって継続的に監視されます。使用率が閾値に近づくと、ホストは SPM に通知し、SPM は論理ボリュームを 1 GB 単位で拡張します。ホストは、論理ボリュームの拡張後に仮想マシンを再開する役割を果たします。仮想マシンが一時停止状態になると、SPM は予定どおりにディスクの拡張ができないことになります。このような問題は、SPM が過度にビジー状態の場合や、十分なストレージ容量がない場合に発生します。

事前割り当て済み (Raw) の仮想ディスクの書き込み速度は、シンプロビジョニング (QCOW2) 形式の仮想ディスクよりもはるかに高速です。シンプロビジョニングの場合には、仮想ディスク作成の所要時間は大幅に短くなります。シンプロビジョニング形式は I/O を集中的に使用しない仮想マシンに適しています。I/O 書き込みの高速な仮想マシンには、事前割り当て済みのフォーマットを推奨します。4 秒あたり 1 GB 以上の書き込みが可能な仮想マシンの場合には、可能であれば事前割り当て済みのディスクを使用してください。

10.2. 仮想ディスクについての知識

Red Hat Virtualization は、**事前割り当て済み** (シックプロビジョニング) および **スパース** (シンプロビジョニング) のストレージオプションを特長としています。

- **事前割り当て済み**
事前割り当て済みの仮想ディスクは、仮想マシンに必要なすべてのストレージを前もって割り当てます。たとえば、仮想マシンのデータパーティション用に作成した 20 GB の事前割り当て済み論理ボリュームは、作成直後に 20 GB のストレージ領域を占有します。
- **スパース**
スパース割り当てでは、管理者は仮想マシンに割り当てる全ストレージを定義することができますが、そのストレージが割り当てられるのは必要時のみです。

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が作成時に占有するストレージ領域は 0 GB ですが、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分が占有され、データが追加されるにしたがって、最大 20 GB まで拡大します。

仮想ディスクの **ID** は、**ストレージ → ディスク** に表示されます。仮想ディスクのデバイス名 (例: `/dev/vda0`) は変わる場合があります。ディスクの破損を招く恐れがあるので、仮想ディスクの識別には **ID** が使用されます。仮想ディスクの ID は `/dev/disk/by-id` でも確認することができます。

ディスクの **仮想サイズ** は、**ストレージ → ディスク**、ならびにストレージドメイン、仮想マシン、およびテンプレートの詳細ビューの **ディスク** タブに表示されます。**仮想サイズ** は、仮想マシンが使用可能なディスク容量の合計です。これは、仮想ディスクの作成または編集時に **サイズ (GB)** フィールドに入力した値です。

ディスクの **実サイズ** は、ストレージドメインおよびテンプレートの詳細ビューの **ディスク** タブに表示されます。これは、それまでに仮想マシンに割り当て済みのディスク容量です。事前割り当て済みディスクの場合、**仮想サイズ** と **実サイズ** には同じ値が表示されます。スパースディスクの場合には、割り当て済みのディスク容量に応じて、異なる値が表示される場合があります。



注記

Cinder 仮想ディスクを作成する際には、そのディスクの形式とタイプは Cinder によって内部で処理され、Red Hat Virtualization では管理されません。

以下の表には、ストレージのタイプと形式の可能な組み合わせについての説明をまとめています。

表10.1 許可されているストレージの組み合わせ

ストレージ	形式	タイプ	注記
NFS	RAW	事前割り当て済み	仮想ディスク用に定義されたストレージの容量と等しい初期サイズのファイル。フォーマットはなし。
NFS	RAW	スパース	初期サイズがゼロに近いファイル。フォーマットなし。
NFS	QCOW2	スパース	初期サイズがゼロに近いファイル。QCOW2 フォーマット。後続のレイヤーは QCOW2 フォーマット。
SAN	RAW	事前割り当て済み	仮想ディスク用に定義されたストレージの容量と等しい初期サイズのブロックデバイス。フォーマットなし。

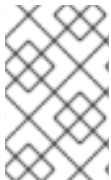
ストレージ	形式	タイプ	注記
SAN	QCOW2	スパース	仮想ディスク用に定義されたサイズ (現在は 1 GB) よりもはるかに小さな初期サイズのブロックデバイス。QCOW2 フォーマットで、必要に応じてスペースが割り当てられる (現在は 1 GB 単位)。

10.3. 削除後に仮想ディスクをワイプする設定

管理ポータルで **削除後にワイプ** のチェックボックスとして表示される **wipe_after_delete** フラグは、仮想ディスクの削除時に使用済みデータをゼロに置き換えます。デフォルトの False に設定した場合には、ディスクを削除するとそれらのブロックが解放されて再利用できるようになりますが、データがワイプされるわけではないので、ブロックはゼロ処理されないため、そのデータは復元可能です。

wipe_after_delete フラグはブロックストレージでのみ機能します。ファイルストレージでは、たとえば NFS の場合はファイルシステムがデータを残さないようにするため、このオプションでは何の操作も実行されません。

仮想ディスクで **wipe_after_delete** を有効にすると、セキュリティが向上します。したがって、仮想ディスクに機密データが含まれている場合には、このオプションを有効にすることを推奨します。この操作は負荷が高い処理なので、パフォーマンスが低下し、削除に長時間を要する可能性があります。



注記

「削除後にワイプ」の機能は、セキュアな削除と同じではないので、ストレージからデータが削除されることは保証できません。これは、同じストレージで作成された新規ディスクが古いディスクのデータを公開しないということです。

wipe_after_delete フラグのデフォルト設定は、セットアッププロセス中 (『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 上で engine 設定ツールを使用して **true** に変更することができます。設定変更を有効にするには、engine を再起動してください。



注記

wipe_after_delete フラグを変更しても、すでに存在しているディスクの **削除後にワイプ** プロパティは変更されません。

engine 設定ツールを使用した **SANWipeAfterDelete** のデフォルトから **True** への設定

1. **--set** アクションで、engine 設定ツールを実行します。

```
# engine-config --set SANWipeAfterDelete=true
```

2. engine を再起動して、変更を有効にします。

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

ホスト上にある `/var/log/vdsm/vdsm.log` ファイルをチェックすると、仮想ディスクが正常にワイプおよび削除されたことを確認することができます。

ワイプが正常に実行された場合には、ログファイルに「**storage_domain_id/volume_id was zeroed and will be deleted**」というエントリが追加されます。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
```

削除が正常に実行された場合には、ログファイルに「**finished with VG:storage_domain_id LVs: list_of_volume_ids, img: image_id**」というエントリが追加されます。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
```

ワイプに失敗した場合には、「**zeroing storage_domain_id/volume_id failed. Zero and remove this volume manually**」というログメッセージが表示され、削除に失敗した場合には「**Remove failed for some of VG: storage_domain_id zeroed volumes: list_of_volume_ids**」というメッセージが表示されます。

10.4. RED HAT VIRTUALIZATION の共有可能ディスク

アプリケーションによっては、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 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、これらのディスクを仮想マシンにアタッチすることができます。この方法により、1 つの仮想ディスクを複数のクラスター対応ゲストで使うことが可能となります。

共有ディスクは、すべての状況で使えるわけではありません。共有ディスクは、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アタッチすると、ディスクの読み取り/書き込みが連携されないため、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は作成できません。また、スナップショットを作成した仮想ディスクは、後で共有可能とマークすることはできません。

ディスクは、作成時または後で編集して共有可能とマークすることができます。

10.5. RED HAT VIRTUALIZATION における読み取り専用ディスク

アプリケーションによっては、管理者はデータを読み取り専用として共有する必要があります。これは、仮想マシンにアタッチされるディスクの作成/編集時に、仮想マシンの詳細ビューの **ディスク タブ** で **読み取り専用** のチェックボックスを選択することによって可能となります。**読み取り専用** および **共有可能** に設定すると、管理者は書き込み権限を維持しつつ、複数のクラスター対応ゲストが単一のディスクを共有して読み取ることができます。

仮想マシンの実行中には、ディスクの読み取り専用ステータスは変更できません。



重要

ジャーナリングファイルシステムのマウントには、読み取りおよび書き込みのアクセスが必要です。このようなファイルシステム (例: **EXT3**、**EXT4**、または **XFS**) が含まれている仮想ディスクに **読み取り専用** オプションを使用するのは適切ではありません。

10.6. 仮想ディスクのタスク

10.6.1. 仮想ディスクの作成

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。直接 **LUN** ディスクには、すでに存在する、外部で準備されたターゲットが必要です。**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 に追加された OpenStack Volume のインスタンスへのアクセスが必要です。詳しくは、「[ストレージ管理用の OpenStack Block Storage \(Cinder\) インスタンスの追加](#)」を参照してください。

特定の仮想マシンにアタッチする仮想ディスクを作成することができます。「[新規仮想ディスクウィンドウの設定](#)」で説明するように、アタッチする仮想ディスクを作成する際に追加のオプションを利用することができます。

仮想マシンにアタッチする仮想ディスクの作成

1. **コンピュー**ト → **仮想マシン** をクリックします。
2. 仮想マシンの名前をクリックし、詳細ビューを表示します。
3. **ディスク** タブをクリックします。
4. **新規作成** をクリックします。
5. 適切なボタンをクリックして、仮想ディスクを **イメージ**、**直接 LUN**、または **Cinder** ディスクのいずれかに指定します。
6. 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、選択したディスクのタイプによって異なります。各オプションとディスクタイプについての詳しい説明は、「[新規仮想ディスクウィンドウの設定](#)」を参照してください。
7. **OK** をクリックします。

どの仮想マシンにも属さないフローティング仮想ディスクを作成することもできます。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には複数の仮想マシンにアタッチしたりすることができます。「[新規仮想ディスクウィンドウの設定](#)」で説明するように、仮想ディスクの作成時に利用することができないオプションもあります。

フローティング仮想ディスクの作成



重要

フローティング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。これらの機能は、近々発表予定の製品機能をリリースに先駆けてご提供することにより、お客様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。

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、[「テクノロジープレビュー機能のサポート範囲」](#)を参照してください。

1. **ストレージ → ディスク** をクリックします。
2. **新規作成** をクリックします。
3. 適切なボタンをクリックして、仮想ディスクを **イメージ**、**直接 LUN**、または **Cinder ディスク** のいずれかに指定します。
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、選択したディスクのタイプによって異なります。各オプションとディスクタイプについての詳しい説明は、[「新規仮想ディスクウィンドウの設定」](#)を参照してください。
5. **OK** をクリックします。

10.6.2. 新規仮想ディスクウィンドウの設定

フローティング仮想ディスクを作成する場合とアタッチする仮想ディスクを作成する場合で、新規仮想ディスク ウィンドウはほとんど同一なので、これらの設定を 1 つのセクションで説明します。

表10.2 新規仮想ディスクおよび仮想ディスクの編集の設定: イメージ

フィールド名	説明
サイズ (GB)	新規仮想ディスクのサイズ (GB 単位)
エイリアス	仮想ディスク名。最大長は 40 文字。
説明	仮想ディスクの説明。このフィールドへの入力推奨されますが、必須ではありません。

フィールド名	説明
インターフェース	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>ディスクが仮想マシンに対して提示する仮想インターフェース。VirtIO はより高速ですが、ドライバーが必要です。このドライバーは、Red Hat Enterprise Linux 5 以降のバージョンには搭載されています。Windows にはこのドライバーは搭載されていませんが、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することができます。IDE デバイスには特別なドライバーは必要ありません。</p> <p>インターフェースのタイプは、そのディスクがアタッチされている仮想マシンすべてを停止した後に更新が可能となります。</p>
データセンター	<p>このフィールドは、フローティングディスクを作成する場合にのみ表示されます。</p> <p>仮想ディスクを使用できるデータセンター</p>
ストレージドメイン	<p>仮想ディスクが格納されるストレージドメイン。ドロップダウンリストには、対象のデータセンターで利用できる全ストレージドメインが表示されます。また、ストレージドメインの全容量と現在の空き容量も表示されます。</p>

フィールド名	説明
割り当てポリシー	<p>新規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"> ● 事前割り当て済み を指定すると、仮想ディスク作成時にストレージドメイン上の全ディスクサイズが割り当てられます。事前割り当て済みディスクの仮想サイズと実サイズは同じです。事前割り当て済みの仮想ディスクは、シンプロビジョニングの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/書き込みのパフォーマンスがより優れています。サーバーやその他の I/O を集中的に行う仮想マシンには、事前割り当て済みの仮想ディスクが推奨されます。4 秒あたり 1 GB 以上の書き込みが可能な仮想マシンの場合には、可能であれば事前割り当て済みのディスクを使用してください。 ● シンプロビジョニング を指定すると、仮想ディスク作成時に 1 GB が割り当てられ、ディスクサイズ拡張の上限が設定されます。ディスクの仮想サイズが上限です。実サイズは、それまでに割り当て済みの容量です。シンプロビジョニングのディスクは、事前割り当て済みのディスクよりも作成が高速で、ストレージのオーバーコミットメントが可能です。シンプロビジョニングの仮想ディスクはデスクトップに推奨されます。
ディスクプロファイル	<p>仮想ディスクに割り当てる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最大スループットと入出力操作数の最大レベルを定義します。ディスクプロファイルは、データセンターに対して作成されたストレージ QoS 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。</p>
ディスクのアクティブ化	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>仮想ディスクの作成直後にアクティブ化します。</p>
削除後にワイプ	<p>仮想ディスクの削除時に、機密性の高い情報を削除するセキュリティ強化を有効にすることができます。</p>
ブート可能	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>仮想ディスクにブート可能のフラグを設定することができます。</p>

フィールド名	説明
共有可能	仮想ディスクを複数の仮想マシンに同時にアタッチすることができます。
読み取り専用	このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。 ディスクを読み取り専用に設定することができます。同じディスクを1つの仮想マシンには読み取り専用として、もう1つの仮想マシンには再書き込み可能としてアタッチすることが可能です。
Trim 処理の省略	このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。 仮想マシンの実行中にシンプロビジョニングされたディスクを圧縮できます。ブロックストレージの場合は、下層のストレージデバイスが呼び出しの破棄をサポートしている必要があり、このオプションは、下層のストレージが discard_zeroes_data プロパティをサポートしない限り 削除後にワイプ と併用できません。ファイルストレージの場合は、下層のファイルシステムやブロックデバイスが呼び出しの破棄をサポートしている必要があります。すべての要件が満たされている場合には、ゲスト仮想マシンから実行した SCSI UNMAP コマンドは、QEMU により下層のストレージに渡され、未使用の領域を開放します。

直接 LUN の設定は、**ターゲット > LUN** または **LUN > ターゲット** のいずれかのタブで表示することができます。**ターゲット > LUN** には、検出先のホストで利用可能な LUN の一覧が、**LUN > ターゲット** には 全 LUN の一覧がそれぞれ表示されます。

ターゲットを検出 セクションの各フィールドに必要事項を入力し、**検出** をクリックしてターゲットのサーバーを検出します。次に **全ターゲットにログイン** ボタンをクリックして、そのターゲットサーバー上の利用可能な LUN を一覧表示し、各 LUN の横にあるラジオボタンで追加する LUN を選択することができます。

仮想マシンのハードディスクイメージとして LUN を直接使用すると、仮想マシンと仮想マシンのデータの間の抽象化層が削除されます。

直接 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際には、以下の点に注意してください。

- 直接 LUN の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。
- 直接 LUN ディスクは、仮想マシンエクスポートには含まれません。
- 直接 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ません。

表10.3 新規仮想ディスクおよび仮想ディスクの編集の設定: 直接 LUN

フィールド名	説明
エイリアス	仮想ディスク名。最大長は 40 文字。
説明	<p>仮想ディスクの説明。このフィールドへの入力推奨されますが、必須ではありません。デフォルトでは、このフィールドに LUN ID の最後の 4 文字が挿入されています。</p> <p>デフォルトの動作は、engine-config コマンドで PopulateDirectLUNDiskDescriptionWithLUNId の設定キーに適切な値を指定して設定することができます。完全な LUN ID を使用するには設定キーに -1 を、この機能を見捨てるには 0 を指定します。正の整数を指定すると、その文字数分だけ LUN ID が説明フィールドに挿入されます。</p>
インターフェース	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>ディスクが仮想マシンに対して提示する仮想インターフェース。VirtIO はより高速ですが、ドライバーが必要です。このドライバーは、Red Hat Enterprise Linux 5 以降のバージョンには搭載されています。Windows にはこのドライバーは搭載されていませんが、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することができます。IDE デバイスには特別なドライバーは必要ありません。</p> <p>インターフェースのタイプは、そのディスクがアタッチされている仮想マシンすべてを停止した後に更新が可能となります。</p>
データセンター	<p>このフィールドは、フローティングディスクを作成する場合にのみ表示されます。</p> <p>仮想ディスクを使用できるデータセンター</p>
使用するホスト	LUN のマウント先のホスト。データセンター内の任意のホストを選択できます。
ストレージタイプ	追加する外部 LUN のタイプ。 iSCSI または ファイバーチャネル から選択可能です。

フィールド名	説明
ターゲットを検出	<p>このセクションは、iSCSI の外部 LUN を使用する場合に、「ターゲット > LUN」のタブを選択すると拡張されます。</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。ユーザー認証 フィールドは、iSCSI の外部 LUN を使用する場合に表示されます。</p> <p>CHAP のユーザー名: LUN にログインするパーミッションのあるユーザーのユーザー名。このフィールドは、ユーザー認証 チェックボックスが選択されている場合に編集が可能です。</p> <p>CHAP のパスワード: LUN にログインするパーミッションのあるユーザーのパスワード。このフィールドは、ユーザー認証 チェックボックスが選択されている場合に編集が可能です。</p>
ディスクのアクティブ化	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>仮想ディスクの作成直後にアクティブ化します。</p>
ブート可能	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>仮想ディスクにブート可能のフラグを設定することができます。</p>
共有可能	<p>仮想ディスクを複数の仮想マシンに同時にアタッチすることができます。</p>
読み取り専用	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>ディスクを読み取り専用を設定することができます。同じディスクを 1 つの仮想マシンには読み取り専用として、もう 1 つの仮想マシンには再書き込み可能としてアタッチすることが可能です。</p>

フィールド名	説明
Trim 処理の省略	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>仮想マシンの実行中にシンプロビジョニングされたディスクを圧縮できます。このオプションが有効な場合は、ゲスト仮想マシンから実行した SCSI UNMAP コマンドは、QEMU により下層のストレージに渡され、未使用の領域を開放します。</p>
SCSI パススルーを有効にする	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>インターフェース が VirtIO-SCSI に設定されている場合に利用可能。このチェックボックスを選択すると、物理 SCSI デバイスから仮想ディスクへのパススルーが有効になります。VirtIO-SCSI インターフェースに SCSI パススルーを有効にすると、SCSI discard のサポートが自動的に含まれます。このチェックボックスが選択されている場合は、読み取り専用 はサポートされません。</p> <p>このチェックボックスが選択されていない場合は、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。エミュレートされた VirtIO-SCSI ディスクでは、読み取り専用 がサポートされます。</p>
特権のある SCSI I/O を許可	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>SCSI パススルーを有効にする のチェックボックスを選択すると設定可能となります。このチェックボックスを選択すると、フィルター処理なしの SCSI 汎用 I/O (SG_IO) アクセスが可能となり、ディスク上で特権のある SG_IO コマンドを実行できるようになります。永続的な予約にはこの設定が必要です。</p>
SCSI 予約を使用	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>SCSI パススルーを有効にする および 特権のある SCSI I/O を許可 のチェックボックスが選択されている場合に利用できます。このチェックボックスを選択すると、SCSI 予約を使用する仮想マシンからこのディスクへのアクセスが失われないように、このディスクを使用した仮想マシンの移行が無効になります。</p>

適切なデータセンターへのディスク作成のパーミッションがある OpenStack Volume ストレージドメインを利用できない場合には **Cinder** 設定フォームは無効になります。**Cinder** ディスクでは、**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 Volume のインスタンスにアクセスできる状態でなければなりません。詳しい情報は、[「ストレージ管理用の OpenStack Block Storage \(Cinder\) インスタンスの追加」](#) を参照してください。

表10.4 新規仮想ディスクおよび仮想ディスクの編集の設定: Cinder

フィールド名	説明
サイズ (GB)	新規仮想ディスクのサイズ (GB 単位)
エイリアス	仮想ディスク名。最大長は 40 文字。
説明	仮想ディスクの説明。このフィールドへの入力推奨されますが、必須ではありません。
インターフェース	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>ディスクが仮想マシンに対して提示する仮想インターフェース。VirtIO はより高速ですが、ドライバーが必要です。このドライバーは、Red Hat Enterprise Linux 5 以降のバージョンには搭載されています。Windows にはこのドライバーは搭載されていませんが、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することができます。IDE デバイスには特別なドライバーは必要ありません。</p> <p>インターフェースのタイプは、そのディスクがアタッチされている仮想マシンすべてを停止した後に更新が可能となります。</p>
データセンター	<p>このフィールドは、フローティングディスクを作成する場合にのみ表示されます。</p> <p>仮想ディスクを使用できるデータセンター</p>
ストレージドメイン	仮想ディスクが格納されるストレージドメイン。ドロップダウンリストには、対象のデータセンターで利用できる全ストレージドメインが表示されます。また、ストレージドメインの全容量と現在の空き容量も表示されます。
ボリュームタイプ	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、利用可能なボリュームのタイプがすべて表示されます。ボリュームのタイプは、OpenStack Cinder で管理/設定されます。
ディスクのアクティブ化	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>仮想ディスクの作成直後にアクティブ化します。</p>

フィールド名	説明
ブート可能	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>仮想ディスクにブート可能のフラグを設定することができます。</p>
共有可能	<p>仮想ディスクを複数の仮想マシンに同時にアタッチすることができます。</p>
読み取り専用	<p>このフィールドは、アタッチするディスクを作成する場合にのみ表示されます。</p> <p>ディスクを読み取り専用に設定することができます。同じディスクを 1 つの仮想マシンには読み取り専用として、もう 1 つの仮想マシンには再書き込み可能としてアタッチすることが可能です。</p>



重要

ジャーナリングファイルシステムのマウントには、読み取りおよび書き込みのアクセスが必要です。このようなファイルシステム (例: **EXT3**、**EXT4**、または **XFS**) が含まれている仮想ディスクに **読み取り専用** オプションを使用するのは適切ではありません。

10.6.3. ライブストレージマイグレーションの概要

アタッチ先の仮想マシンが稼働している状態で、仮想ディスクをストレージドメイン間で移行することが可能です。この機能は、ライブストレージマイグレーションと呼ばれています。実行中の仮想マシンにアタッチされたディスクを移行する際には、移行元のストレージドメインで、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作成されて、移行先のストレージドメインにイメージチェーン全体が複製されるので、移行元と移行先の両方のストレージドメインに、ディスクイメージチェーンとスナップショットをホストするのに十分なストレージ容量があることを確認してください。新規スナップショットは、ライブストレージマイグレーションを試みる度に作成されます。これは、マイグレーションが失敗した場合も変わりません。

ライブストレージマイグレーション機能を使用する際には、以下の点を考慮してください。

- 一度に複数のディスクのライブマイグレーションを行うことが可能です。
- 同じ仮想マシンの複数のディスクを複数のストレージドメインに分散して配置することができますが、各ディスクのイメージチェーンは 1 つのストレージドメインに保管する必要があります。
- 同じデータセンター内の任意のストレージドメイン間でディスクのライブマイグレーションを行うことができます。
- 直接 LUN のハードディスクイメージまたは共有可能とマークされたディスクはライブマイグレーションすることはできません。

10.6.4. 仮想ディスクの移動

仮想マシンにアタッチされた仮想ディスク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

スクをストレージドメイン間で移動することができます。実行中の仮想マシンにアタッチされた仮想ディスクを移動することが可能です。この機能は、ライブストレージマイグレーションと呼ばれています。もしくは、操作を続行する前に、仮想マシンをシャットダウンしてください。

ディスクを移動する際には、以下の点を考慮してください。

- 複数のディスクを同時に移行することが可能です。
- 同じデータセンター内の任意のストレージドメイン間でディスクを移行することができます。
- テンプレートをベースに作成された仮想ディスクが、ストレージ割り当てのシンプロビジョニングオプションを使用した仮想マシンにアタッチされている場合は、仮想マシンのベースとなったテンプレート用のディスクを、仮想ディスクと同じストレージドメインにコピーする必要があります。

仮想ディスクの移動

1. **ストレージ → ディスク** をクリックし、移動する仮想ディスクを1つまたは複数選択します。
2. **移動** をクリックします。
3. **ターゲット** の一覧から、仮想ディスクの移動先となるストレージドメインを選択します。
4. 該当する場合には、**ディスクプロファイル** の一覧から、ディスクのプロファイルを選択します。
5. **OK** をクリックします。

仮想ディスクは、ターゲットのストレージドメインに移動されます。移動中には、**ステータス** コラムに **ロック** というステータスと、移動操作の進捗状況を示すプログレスバーが表示されます。

10.6.5. ディスクのインターフェースタイプの変更

ディスクを作成した後に、そのディスクのインターフェースタイプを変更することができます。これにより、異なるインターフェースタイプが必要な仮想マシンに既存のディスクをアタッチすることが可能となります。たとえば、**VirtIO-SCSI** または **IDE** のインターフェースが必要な仮想マシンには **VirtIO** インターフェースを使用するディスクをアタッチすることができます。これにより、バックアップ、復元、障害復旧を目的としてディスクを移行するための柔軟性が提供されます。共有可能なディスク用のインターフェースも仮想マシンごとに更新可能です。これは、共有ディスクを使用する各仮想マシンで異なるインターフェースタイプを使用できることを意味します。

ディスクのインターフェースタイプを更新するには、そのディスクを使用している仮想マシンをすべて停止する必要があります。

ディスクのインターフェースタイプの変更

1. **コンピューター → 仮想マシン** をクリックして、該当する仮想マシンを停止します。
2. 仮想マシンの名前をクリックし、詳細ビューを表示します。
3. **ディスク** タブをクリックし、ディスクを選択します。
4. **編集** をクリックします。
5. **インターフェース** の一覧から、新しいインターフェースタイプを選択して **OK** をクリックします。

異なるインターフェースタイプを必要とする別の仮想マシンにディスクをアタッチすることができます。

異なるインターフェースタイプを使用する別の仮想マシンへのディスクのアタッチ

1. **コンピュータ** → **仮想マシン** をクリックして、該当する仮想マシンを停止します。
2. 仮想マシンの名前をクリックし、詳細ビューを表示します。
3. **ディスク** タブをクリックし、ディスクを選択します。
4. **削除** をクリックして、**OK** をクリックします。
5. **仮想マシン** に戻り、ディスクのアタッチ先となる新しい仮想マシンの名前をクリックします。
6. **ディスク** タブをクリックして、**アタッチ** をクリックします。
7. **仮想ディスクのアタッチ** ウィンドウでディスクを選択して、**インターフェース** ドロップダウンから適切なインターフェースを選択します。
8. **OK** をクリックします。

10.6.6. 仮想ディスクのコピー

ストレージドメイン間で仮想ディスクをコピーすることができます。コピーされたディスクは、仮想マシンにアタッチすることが可能です。

仮想ディスクのコピー

1. **ストレージ** → **ディスク** をクリックし、仮想ディスクを選択します。
2. **コピー** をクリックします。
3. オプションで、**エイリアス** フィールドに新しい名前を入力します。
4. **ターゲット** の一覧から、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。
5. 該当する場合には、**ディスクプロファイル** の一覧から、ディスクのプロファイルを選択します。
6. **OK** をクリックします。

コピー中、仮想ディスクのステータスは **ロック** になります。

10.6.7. 仮想ディスクのアップロード

[「データストレージドメインへのイメージのアップロード」](#) を参照してください。

10.6.8. 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

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 にインポートすることができるのは、QEMU との互換性があるディスクだけです。

ディスクイメージのインポート

1. ストレージ → ドメイン をクリックします。
2. インポートしたストレージドメインの名前をクリックし、詳細ビューを表示します。
3. **ディスクのインポート** タブをクリックします。
4. ディスクを 1 つまたは複数選択し、**インポート** をクリックします。
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** をクリックします。

10.6.9. インポートされたストレージドメインからの未登録ディスクイメージのインポート

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 環境以外で作成されたフローティングディスクは、Manager には登録されていません。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 にインポートすることができるのは、QEMU との互換性があるディスクだけです。

ディスクイメージのインポート

1. ストレージ → ドメイン をクリックします。
2. ストレージドメインの名前をクリックし、詳細ビューを表示します。
3. Manager が未登録のディスクを特定できるように、**その他の操作 → ディスクをスキャン** をクリックします。
4. **ディスクのインポート** タブをクリックします。
5. ディスクイメージを 1 つまたは複数選択し、**インポート** をクリックします。
6. 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。
7. **OK** をクリックします。

10.6.10. OpenStack Image サービスからの仮想ディスクのインポート

OpenStack Image サービスが外部プロバイダーとして Red Hat Virtualization Manager に追加されている場合には、OpenStack Image サービスによって管理される仮想ディスクを Manager にインポートすることが可能です。

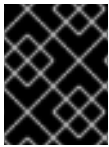
1. ストレージ → ドメイン をクリックします。
2. OpenStack Image サービスドメインの名前をクリックし、詳細ビューを表示します。
3. **イメージ** タブをクリックし、イメージを選択します。
4. **インポート** をクリックします。

5. イメージのインポート先となる **データセンター** を選択します。
6. **ドメイン名** ドロップダウンリストから、イメージの保管先となるストレージドメインを選択します。
7. オプションで、**クォータ** ドロップダウンリストから、イメージに適用するクォータを選択します。
8. **OK** をクリックします。

これで、ディスクが仮想マシンにアタッチすることのできる状態になりました。

10.6.11. OpenStack Image サービスへの仮想ディスクのエクスポート

外部プロバイダーとして Manager に追加済みの OpenStack Image サービスに仮想ディスクをエクスポートすることができます。



重要

複数のボリュームが含まれず、シンプロビジョニングされておらず、かつスナップショットが含まれていない場合に限り、仮想ディスクのエクスポートが可能です。

1. **ストレージ → ディスク** をクリックし、エクスポートするディスクを選択します。
2. **その他の操作 → エクスポート** をクリックします。
3. **ドメイン名** 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 サービスを選択します。
4. クォータを適用する場合には、**クォータ** ドロップダウンリストから、そのディスクのクォータを選択します。
5. **OK** をクリックします。

10.6.12. 仮想ディスクの領域解放

シンプロビジョニングを使用する仮想ディスクは、それらのディスクからファイルを削除しても自動的に縮小されません。たとえば、実際のディスクサイズが 100 GB で 50 GB のファイルを削除した場合に、割り当て済みのディスクサイズは 100 GB から変わらず、残りの 50 GB はホストに返されないの、他の仮想マシンがその領域を使用することができません。この未使用のディスク領域は、ホストで仮想ディスクに対してスパース化の操作を実行することによって解放することができます。これにより、ディスクから空き領域がホストに転送されます。複数の仮想ディスクを並行してスパース化することができます。

Red Hat では、仮想マシンのクローン作成、仮想マシンをベースとするテンプレートの作成、ストレージドメインのディスク領域のクリーンアップなどを行う前にこの操作を実行しておくことを推奨します。

制約

- NFS ストレージドメインでは NFS バージョン 4.2 以降を使用する必要があります。
- 直接 LUN または Cinder を使用するディスクはスパース化できません。
- 事前割り当て済みの割り当てポリシーを使用するディスクはスパース化できません。テンプレートから仮想マシンを作成する場合には、**ストレージの割り当て** フィールドから **シンプロビ**

ジョニングを選択する必要があります。また クローン を選択する場合には、シンプロビジョニングが選択されている仮想マシンをベースにしたテンプレートであることを確認してください。

- スパース化できるのは、アクティブなスナップショットのみです。

ディスクのスパース化

1. コンピュート → 仮想マシン をクリックし、対象の仮想マシンをシャットダウンします。
2. 仮想マシンの名前をクリックし、詳細ビューを表示します。
3. ディスク タブをクリックします。ディスクのステータスが **OK** であることを確認します。
4. その他の操作 → スパース化 をクリックします。
5. **OK** をクリックします。

スパース化操作の実行中には、イベント タブに **Started to sparsify** というイベントが表示され、ディスクのステータスは **ロック** と表示されます。操作が完了すると、イベント タブに **Sparsified successfully** というイベントが表示され、ディスクのステータスは **OK** と表示されます。未使用のディスク領域はホストに返還され、他の仮想マシンが使用できるようになります。

第11章 外部プロバイダー

11.1. RED HAT VIRTUALIZATION の外部プロバイダーについて

Red Hat Virtualization では、Red Hat Virtualization Manager 自体によって管理されるリソースに加えて、外部のソースによって管理されるリソースを活用することも可能です。このようなリソースのプロバイダーは、外部プロバイダーとして知られ、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することができます。

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。

Red Hat Satellite (ホストのプロビジョニング)

Satellite は、物理/仮想ホストの両方のライフサイクルの全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することができます。Satellite のインスタンスを Manager に追加すると、その Satellite インスタンスによって管理されるホストは、新規ホストの追加時に、その Satellite インスタンスで利用可能なホストを検索して追加することができます。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しい情報は、『[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。

OpenStack Image サービス (Glance) (イメージ管理)

OpenStack Image サービスは、仮想マシンイメージのカatalog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、仮想マシンにアタッチしてテンプレートに変換したりすることができます。OpenStack Image サービスを Manager に追加すると、どのデータセンターにもアタッチされていないストレージドメインとして表示されます。また、Red Hat Virtualization 環境内の仮想ディスクを OpenStack Image サービスにエクスポートすることも可能です。

OpenStack Networking (Neutron) (ネットワークプロビジョニング)

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 によって提供されるネットワークを Red Hat Virtualization Manager にインポートして、全タイプ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することができます。OpenStack Networking を Manager に追加すると、OpenStack Networking によって提供されるネットワークを手動でインポートしてアクセスすることができます。

OpenStack Volume (Cinder) (ストレージ管理)

OpenStack Volume は、仮想ハードドライブ用の永続ブロックストレージの管理を提供します。OpenStack Cinder ボリュームは、Ceph Storage によってプロビジョニングされます。Red Hat Virtualization では、フローティングディスクとして使用するためのディスクや、仮想マシンにアタッチするディスクを OpenStack Volume ストレージ上に作成することができます。OpenStack Volume を Manager に追加すると、OpenStack Volume によって提供されるストレージ上にディスクを作成することが可能となります。

VMware (仮想マシンのプロビジョニング)

VMware で作成された仮想マシンは、V2V (**virt-v2v**) を使用して変換してから Red Hat Virtualization 環境にインポートすることができます。VMware プロバイダーを Manager に追加すると、そのプロバイダーが提供する仮想マシンをインポートすることができます。V2V の変換は、指定したプロキシホストで、インポート操作の一貫として実行されます。

Xen (仮想マシンのプロビジョニング)

Xen で作成された仮想マシンは、V2V (**virt-v2v**) を使用して変換してから Red Hat Virtualization 環境にインポートすることができます。Xen ホストを Manager に追加すると、そのプロバイダーが提供する仮想マシンをインポートすることができます。V2V の変換は、指定したプロキシホストで、インポート操作の一貫として実行されます。

KVM (仮想マシンのプロビジョニング)

KVM で作成された仮想マシンは、Red Hat Virtualization 環境にインポートすることができます。KVM ホストを Manager に追加すると、そのプロバイダーが提供する仮想マシンをインポートすることができます。

Open Virtual Network (OVN) (ネットワークプロビジョニング)

Open Virtual Network (OVN) は、ソフトウェア定義ネットワークを提供する Open vSwitch (OVS) の論理拡張です。OVN を Manager に追加すると、既存の OVN ネットワークをインポートし、Manager から新規 OVN ネットワークを作成することができます。**engine-setup** を使用して、自動的に OVN を Manager にインストールすることもできます。

外部ネットワークプロバイダー (ネットワークプロビジョニング)

サポートされている外部のソフトウェア定義ネットワークプロバイダーには、OpenStack Neutron REST API を実装する任意の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ースドライバの実装としては使用されません。その代わりに、仮想インターフェースドライバは外部ネットワークプロバイダーの実装者によって提供される必要があります。

外部のリソースプロバイダーはすべて、ユーザーの入力に対応した単一のウィンドウを使用して追加します。リソースプロバイダーの提供するリソースを Red Hat Virtualization の環境で使用するには、そのリソースプロバイダーを追加する必要があります。

11.2. 外部プロバイダーの追加

11.2.1. ホストプロビジョニング用の Red Hat Satellite インスタンスの追加

ホストのプロビジョニング用に Satellite インスタンスを Red Hat Virtualization Manager に追加します。Red Hat Virtualization 4.2 は Red Hat Satellite 6.1 でサポートされています。

ホストプロビジョニング用の Satellite インスタンスの追加

1. **管理** → **プロバイダー** をクリックします。
2. **追加** をクリックします。
3. **名前** と **説明** を入力します。
4. **タイプ** のドロップダウンリストから **Foreman/Satellite** を選択します。
5. **プロバイダーの URL** のテキストフィールドに Satellite インスタンスがインストールされたマシンの URL または完全修飾ドメイン名を入力します。ポート番号を指定する必要はありません。



重要

Satellite インスタンスの追加に IP アドレスは使用できません。

6. **認証が必要** のチェックボックスを選択します。
7. Satellite インスタンス用の **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ユーザー名とパスワード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. **テスト** をクリックし、入力した認証情報を使用して Satellite インスタンスと正しく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 を使用している場合には **プロバイダー証明書のインポート** ウィンドウが開きます。**OK** をクリックして Satellite インスタンスの提供する証明書をインポートして、Manager がそのインスタンスと通信できるようにします。

9. **OK** をクリックします。

11.2.2. イメージ管理用の **OpenStack Image (Glance)** インスタンスの追加

イメージ管理用に OpenStack Image (Glance) インスタンスを Red Hat Virtualization Manager に追加します。

イメージ管理用の **OpenStack Image (Glance)** インスタンスの追加

1. **管理** → **プロバイダー** をクリックします。
2. **追加** をクリックします。
3. **名前** と **説明** を入力します。
4. **タイプ** のドロップダウンリストから **OpenStack Image** を選択します。
5. **プロバイダーの URL** のテキストフィールドに OpenStack Image インスタンスがインストールされたマシンの URL または完全修飾ドメイン名を入力します。
6. オプションとして、**認証が必要** のチェックボックスを選択して 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。これには、Keystone に登録されている OpenStack Image ユーザーのユーザー名およびパスワード、OpenStack Image インスタンスがメンバーになっているテナント、ならびに Keystone サーバーの URL および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. **テスト** をクリックし、入力した認証情報を使用して OpenStack Image インスタンスと正しく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には **プロバイダー証明書のインポート** ウィンドウが開きます。**OK** をクリックして OpenStack Image インスタンスの提供する証明書をインポートして、Manager がそのインスタンスと通信できるようにします。
8. **OK** をクリックします。

11.2.3. 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に OpenStack Networking (Neutron) インスタンスを Red Hat Virtualization Manager に追加します。OpenStack Neutron REST API を実装する別のサードパーティーの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、Red Hat OpenStack Platform バージョン 8、9、10、11、および 12 を外部ネットワークプロバイダーとしてサポートしています。

Neutron ネットワークを使用するには、ホストに Neutron エージェントを設定する必要があります。

ネットワークノードをホストとして Manager に追加する前に、手動でエージェントを設定するか、Red Hat OpenStack Platform director を使用して Networker ロールをデプロイすることができます。director の使用を推奨します。新規ホスト ウィンドウの **ネットワークプロバイダー** タブを使用した Neutron エージェントの自動デプロイはサポートされません。

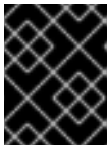
ネットワークノードと通常のホストを同じクラスター内で使用することはできますが、Neutron ネットワークを使用する仮想マシンはネットワークノードでしか実行することができません。

ホストとしてのネットワークノードの追加

1. Red Hat OpenStack Platform director を使用して、ネットワークノードに Networker ロールをデプロイします。『**Red Hat OpenStack Platform** オーククラウドの高度なカスタマイズ』の「**新規ロールの作成**」および「**Networker**」を参照してください。
2. Red Hat Virtualization のリポジトリを有効にします。『インストールガイド』の「**必要なエントタイトルメントのサブスクリプション**」を参照してください。
3. Openstack Networking フックをインストールします。

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

4. Manager にホストとしてネットワークノードを追加します。「**Red Hat Virtualization Manager へのホストの追加**」を参照してください。



重要

ネットワークプロバイダー タブから OpenStack Networking プロバイダーを選択しないでください。現在、このオプションはサポートされていません。

5. ICMP トラフィックを拒否するファイアウォールルールを削除します。

```
# iptables -D INPUT -j REJECT --reject-with icmp-host-prohibited
```

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. **管理** → **プロバイダー** をクリックします。
2. **追加** をクリックします。
3. **名前** と **説明** を入力します。
4. **タイプ** のドロップダウンリストから **OpenStack Networking** を選択します。
5. **ネットワークプラグイン** 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. **プロバイダーの URL** のテキストフィールドに OpenStack Networking インスタンスがインストールされたマシンの URL または完全修飾ドメイン名を入力し、後ろにポート番号を指定します。**読み取り専用** のチェックボックスは、デフォルトで選択されています。これは、ユーザーが OpenStack Networking インスタンスを変更するのを防ぎます。



重要

Red Hat のサポートを受けるには、**読み取り専用** のチェックボックスを選択したままにする必要があります。

7. オプションとして、**認証が必要** のチェックボックスを選択して 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。これには、Keystone 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、OpenStack Networking インスタンスがメンバーになっているテナント、ならびに Keystone サーバーの URL および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. **テスト** をクリックし、入力した認証情報を使用して OpenStack Networking インスタンスと正しく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には **プロバイダー証明書のインポート** ウィンドウが開きます。**OK** をクリックして OpenStack Networking インスタンスの提供する証明書をインポートして、Manager がそのインスタンスと通信できるようにします。
9. **エージェントの設定** タブをクリックします。



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しています。Red Hat Virtualization は、事前設定済みの Neutron ホストしかサポートしていません。

10. **インターフェースマッピング** フィールドに、Open vSwitch エージェントのインターフェースマッピングのコンマ区切りリストを入力します。
11. **ブローカータイプ** の一覧から、OpenStack Networking インスタンスが使用するメッセージブローカーのタイプを選択します。
12. **ホスト** フィールドに、メッセージブローカーをホスティングするホストの 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 **ポート** を入力します。デフォルトではこのポート番号は、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 5762、SSL を使用するように設定されている場合は 5761 です。
14. メッセージブローカーインスタンスに登録済みの OpenStack Networking ユーザーの **ユーザー名** と **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。このインスタンスが提供するネットワークは、使用する前に 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。

11.2.4. ストレージ管理用の **OpenStack Block Storage (Cinder)** インスタンスの追加

重要

ストレージ管理用の OpenStack Block Storage (Cinder) インスタンスの使用は、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。これらの機能は、近々発表予定の製品機能をリリースに先駆けてご提供することにより、お客様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。

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、[「テクノロジープレビュー機能のサポート範囲」](#)を参照してください。

ストレージ管理用に OpenStack Block Storage (Cinder) インスタンスを Red Hat Virtualization Manager に追加します。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。

ストレージ管理用の OpenStack Block Storage (Cinder) インスタンスの追加

1. **管理** → **プロバイダー** をクリックします。
2. **追加** をクリックします。
3. **名前** と **説明** を入力します。
4. **タイプ** のドロップダウンリストから **OpenStack Block Storage** を選択します。
5. OpenStack Block Storage ボリュームをアタッチする **データセンター** を選択します。
6. **プロバイダーの URL** のテキストフィールドに OpenStack Block Storage インスタンスがインストールされたマシンの URL または完全修飾ドメイン名を入力し、後ろにポート番号を指定します。
7. オプションとして、**認証が必要** のチェックボックスを選択して OpenStack Block Storage 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。これには、Keystone に登録されている OpenStack Block Storage ユーザーのユーザー名およびパスワード、OpenStack Block Storage インスタンスがメンバーになっているテナント、ならびに 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. **テスト** をクリックし、入力した認証情報を使用して OpenStack Block Storage インスタンスと正しく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. クライアントの Ceph 認証 (**cephx**) が有効化されている場合には、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化されます。
 - 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** についての詳しい情報は、『Red Hat Ceph Storage Configuration Guide』の「[Cephx Configuration Reference](#)」を参照してください。また、新規ユーザー用のキー作成についての詳しい説明は、『Red Hat Ceph Storage Administration Guide』の「[Managing Users](#)」を参照してください。**client.cinder** ユーザー用のキーがすでに存在している場合には、同じコマンドを使用して取得してください。
 - b. 管理ポータルで、**プロバイダー** 一覧から、新規作成した Cinder 外部プロバイダーを選択します。
 - c. **認証キー** タブをクリックします。

- d. **新規作成** をクリックします。
- e. **値** のフィールドに秘密鍵を入力します。
- f. 自動生成された **UUID** をテキストフィールドにコピーするか、既存の UUID を入力します。
- g. Cinder サーバーで、前のステップでコピー/入力した 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 Block Storage (Cinder) ディスクの作成については、「[仮想ディスクの作成](#)」を参照してください。

11.2.5. 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、VMware から Red Hat Virtualization Manager に仮想マシンをインポートします。

Red Hat Virtualization では、VMware の仮想マシンをインポートする前に V2V を使用して正しい形式に変換します。少なくとも 1 台のホストに **virt-v2v** パッケージをインストールする必要があります。**virt-v2v** パッケージは Red Hat Virtualization Host (RHVH) ではデフォルトで提供されます。Red Hat Enterprise Linux ホストの場合は、Red Hat Virtualization 環境に追加する際に VDSM の依存関係としてインストールされます。Red Hat Enterprise Linux ホストのバージョンは Red Hat Enterprise Linux 7.2 以降でなければなりません。



注記

ppc64le アーキテクチャーでは **virt-v2v** パッケージを利用することができません。したがって、これらのホストをプロキシホストとして使用することはできません。

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. **管理** → **プロバイダー** をクリックします。
2. **追加** をクリックします。
3. **名前** と **説明** を入力します。
4. **タイプ** のドロップダウンリストから **VMware** を選択します。
5. VMware 仮想マシンのインポート先となる **データセンター** を選択するか、**任意のデータセンター** を選択して個々のインポート操作中にインポート先のデータセンターを指定するようにします。
6. **vCenter** フィールドには、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. **ESXi** フィールドには、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入力します。
8. **データセンター** フィールドには、指定した ESXi ホストが属するデータセンターの名前を入力します。

9. ESXi および Manager の間で SSL 証明書を交換した場合には、ESXi ホストの証明書が検証されるように **サーバーの SSL 証明書を確認** のチェックボックスを選択した状態にしてください。交換していない場合は、このチェックボックスのチェックを外してください。
10. 選択したデータセンター内の **virt-v2v** をインストールしたホストを選択します。このホストは、仮想マシンのインポート操作中に **プロキシホスト** として機能します。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可能である必要があります。上記のステップで **任意のデータセンター** を選択した場合は、ここでホストを指定することはできませんが、個々のインポート操作中にホストを指定することが可能です。
11. VMware vCenter インスタンスの **ユーザー名** と **パスワード** を入力します。ユーザーは、VMware データセンターと仮想マシンが属する ESXi ホストへのアクセスが可能である必要があります。
12. 認証情報をテストします。
 - a. **テスト** をクリックし、入力した認証情報を使用して VMware vCenter インスタンスと正しく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 を使用している場合には **プロバイダー証明書のインポート** ウィンドウが開きます。**OK** をクリックして VMware vCenter インスタンスの提供する証明書をインポートして、Manager がそのインスタンスと通信できるようにします。
13. **OK** をクリックします。

VMware 外部プロバイダーから仮想マシンをインポートする手順については、『**仮想マシン管理ガイド**』の「**VMware プロバイダーからの仮想マシンのインポート**」を参照してください。

11.2.6. 仮想マシンプロバイダーとしての Xen ホストの追加

Xen ホストを追加して、Xen から Red Hat Virtualization Manager に仮想マシンをインポートします。

Red Hat Virtualization では、Xen の仮想マシンをインポートする前に V2V を使用して正しい形式に変換します。少なくとも 1 台のホストに **virt-v2v** パッケージをインストールする必要があります。**virt-v2v** パッケージは Red Hat Virtualization Host (RHVH) ではデフォルトで提供されます。Red Hat Enterprise Linux ホストの場合は、Red Hat Virtualization 環境に追加する際に VDSM の依存関係としてインストールされます。Red Hat Enterprise Linux ホストのバージョンは Red Hat Enterprise Linux 7.2 以降でなければなりません。



注記

ppc64le アーキテクチャーでは **virt-v2v** パッケージを利用することができません。したがって、これらのホストをプロキシホストとして使用することはできません。

仮想マシンプロバイダーとしての Xen インスタンスの追加

1. プロキシホストと Xen ホスト間の公開鍵認証を有効化します。
 - a. プロキシホストにログインして **vds**m ユーザーの SSH キーを生成します。


```
# sudo -u vds m ssh-keygen
```
 - b. **vds**m ユーザーの公開鍵を Xen ホストにコピーします。これによりプロキシホストの **known_hosts** ファイルも更新され、Xen ホストのホストキーを含むようになります。

```
# sudo -u vdsd ssh-copy-id root@xenhost.example.com
```

c. Xen ホストにログインし、ログインが正常に機能していることを確認します。

```
# sudo -u vdsd ssh root@xenhost.example.com
```

2. **管理** → **プロバイダー** をクリックします。
3. **追加** をクリックします。
4. **名前** と **説明** を入力します。
5. **タイプ** のドロップダウンリストから **XEN** を選択します。
6. Xen 仮想マシンのインポート先となる **データセンター** を選択するか、**任意のデータセンター** を選択して個々のインポート操作中にインポート先のデータセンターを指定するようにします。
7. **URI** のフィールドに Xen ホストの URI を入力します。
8. 選択したデータセンター内の **virt-v2v** をインストールしたホストを選択します。このホストは、仮想マシンのインポート操作中に **プロキシホスト** として機能します。このホストは、Xen 外部プロバイダーのネットワークに接続可能である必要もあります。上記のステップで **任意のデータセンター** を選択した場合は、ここでホストを指定することはできませんが、個々のインポート操作中にホストを指定することが可能です。
9. **テスト** をクリックし、Xen ホストと正しく認証できるかどうかをテストします。
10. **OK** をクリックします。

Xen 外部プロバイダーから仮想マシンをインポートする手順については、『**仮想マシン管理ガイド**』の「**Xen ホストからの仮想マシンのインポート**」を参照してください。

11.2.7. 仮想マシンプロバイダーとしての KVM ホストの追加

KVM ホストを追加して、KVM から Red Hat Virtualization Manager に仮想マシンをインポートします。

仮想マシンプロバイダーとしての KVM ホストの追加

1. プロキシホストと KVM ホスト間の公開鍵認証を有効化します。
 - a. プロキシホストにログインして **vdsd** ユーザーの SSH キーを生成します。


```
# sudo -u vdsd ssh-keygen
```
 - b. **vdsd** ユーザーの公開鍵を KVM ホストにコピーします。これによりプロキシホストの **known_hosts** ファイルも更新され、KVM ホストのホストキーを含むようになります。


```
# sudo -u vdsd ssh-copy-id root@kvmhost.example.com
```
 - c. KVM ホストにログインし、ログインが正常に機能していることを確認します。

```
# sudo -u vdsd ssh root@kvmhost.example.com
```

2. **管理** → **プロバイダー** をクリックします。
3. **追加** をクリックします。
4. **名前** と **説明** を入力します。
5. **タイプ** のドロップダウンリストから **KVM** を選択します。
6. KVM 仮想マシンのインポート先となる **データセンター** を選択するか、**任意のデータセンター** を選択して個々のインポート操作中にインポート先のデータセンターを指定するようにします。
7. **URI** のフィールドに KVM ホストの URI を入力します。
8. 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、仮想マシンのインポート操作中に **プロキシホスト** として機能します。このホストは、KVM 外部プロバイダーのネットワークに接続可能である必要もあります。上記の **データセンター** フィールドで **任意のデータセンター** を選択した場合は、ここでホストを指定することはできません。フィールドが無効になり、**データセンター内の任意のホスト** と表示されます。ただし、個々のインポート操作中にホストを指定することが可能です。
9. オプションとして、**認証が必要** のチェックボックスを選択して KVM ホストの **ユーザー名** および **パスワード** を入力します。ユーザーは、仮想マシンが属する KVM ホストへのアクセスが可能である必要があります。
10. **テスト** をクリックし、入力した認証情報を使用して KVM ホストと正しく認証できるかどうかをテストします。
11. **OK** をクリックします。

KVM 外部プロバイダーから仮想マシンをインポートする手順については、『[仮想マシン管理ガイド](#)』の「[KVM ホストからの仮想マシンのインポート](#)」を参照してください。

11.2.8. 外部ネットワークプロバイダーとしての **Open Virtual Network (OVN)** の追加

Open Virtual Network (OVN) を使用すると、VLAN の追加やインフラストラクチャーの変更を行わずにネットワークを作成することができます。OVN は Open vSwitch (OVS) の論理拡張で、仮想 L2 および L3 オーバーレイに対するネイティブ OVS サポートを追加して、仮想ネットワークのサポートを可能にします。

[新規 OVN ネットワークプロバイダーをインストールする](#) か [既存の OVN ネットワークプロバイダーを追加する](#) ことができます。

OVN ネットワークをネイティブの Red Hat Virtualization ネットワークに接続することもできます。詳細については、「[物理ネットワークへの OVN ネットワークの接続](#)」を参照してください。この機能は、テクノロジープレビューとしてのみ利用可能です。

Neutron のような REST API が **ovirt-provider-ovn** により公開され、ネットワーク、サブネット、ポート、およびルーターを作成することができます (詳細については、『[OpenStack Networking API v2.0](#)』を参照してください)。これらのオーバーレイネットワークにより、仮想マシン同士の通信が可能になります。



注記

CloudForms では、OpenStack (Neutron) API を使用して OVN を外部プロバイダーとしてサポートします。詳細については、『**Red Hat CloudForms プロバイダーの管理**』の「**ネットワークマネージャー**」を参照してください。

OVS および OVN の詳細については、<http://docs.openvswitch.org/en/latest/> および <http://openvswitch.org/support/dist-docs/> で OVS のドキュメントを参照してください。

11.2.8.1. 新規 OVN ネットワークプロバイダーのインストール



警告

バージョン 1:2.6.1 (バージョン 2.6.1 エポック 1) の **openvswitch** パッケージがすでにインストールされている場合は、最新の **openvswitch** パッケージをインストールする際に OVN のインストールに失敗します。詳細および回避策については、[BZ#1505398](#) の「Doc Text」を参照してください。

engine-setup を使用して OVN をインストールする場合は、以下の手順が自動的に実行されます。

- Manager マシンに OVN 集中サーバーをセットアップする
- OVN を外部ネットワークプロバイダーとして Red Hat Virtualization に追加する
- デフォルト クラスターのデフォルトネットワークプロバイダーを **ovirt-provider-ovn** に設定する
- クラスターに追加されたホストが OVN と通信するように設定する

engine-setup の実行時に事前に定義された応答ファイルを使用する場合は、以下のエントリーを追加して OVN をインストールすることができます。

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

新規 OVN ネットワークプロバイダーのインストール

1. **engine-setup** を使用して Manager に OVN をインストールします。インストール中、**engine-setup** から以下の質問を尋ねられます。

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

- **Yes** と回答すると、**engine-setup** により **ovirt-provider-ovn** がインストールされます。**engine-setup** によるシステム更新の場合は、これまでに **ovirt-provider-ovn** がインストールされていない場合にのみこの質問が表示されます。
- **No** と回答すると、次回 **engine-setup** の実行時にはこの質問は表示されなくなります。このオプションを表示するには、**engine-setup --reconfigure-optional-components** を実行します。


```
# Use default credentials (admin@internal) for ovirt-provider-
ovn(Yes, No) [Yes]?:
```

Yes と回答すると、**engine-setup** はセットアッププロセスの初期に指定したデフォルトの engine ユーザーおよびパスワードを使用します。このオプションは、新規インストール時にのみ利用することができます。

```
# oVirt OVN provider user[admin]:
# oVirt OVN provider password[empty]:
```

デフォルト値を使用するか、oVirt OVN プロバイダーのユーザーおよびパスワードを指定することができます。



注記

後で認証方法を変更するには、`/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf` ファイルを編集するか、新たに `/etc/ovirt-provider-ovn/conf.d/20_engine_setup.conf` ファイルを作成します。**ovirt-provider-ovn** サービスを再起動して、変更を有効にします。OVN の認証に関する詳細については、[「oVirt external network provider for OVN」](#) を参照してください。

- ホストを **デフォルト** のクラスターに追加します。このクラスターに追加されたホストは、OVN と通信するように自動的に設定されます。新規ホストの追加方法については、[「Red Hat Virtualization Manager へのホストの追加」](#) を参照してください。
既存のデフォルトではないネットワークを使用するようにホストを設定する場合は、[「OVN トンネルネットワーク用のホスト設定」](#) を参照してください。
- ネットワークを **デフォルト** のクラスターに追加します。[「データセンターまたはクラスター内での新規論理ネットワークの作成」](#) を参照し、**Create on external provider** のチェックボックスを選択します。**ovirt-provider-ovn** がデフォルトで選択されています。
OVN ネットワークをネイティブの Red Hat Virtualization ネットワークに接続するには、**Connect to physical network** のチェックボックスを選択し、使用する Red Hat Virtualization ネットワークを指定します。詳細および前提条件については、[「物理ネットワークへの OVN ネットワークの接続」](#) を参照してください。

これで、OVN ネットワークを使用する仮想マシンを作成することができます。

11.2.8.2. 既存 OVN ネットワークプロバイダーの追加

外部ネットワークプロバイダーとして既存の OVN 集中サーバーを Red Hat Virtualization に追加する手順は、以下の主要なステップで構成されます。

- OVN プロバイダー (Manager が OVN と通信するのに使用するプロキシ) をインストールする。OVN プロバイダーは任意のマシンにインストールできますが、OVN 集中サーバーおよび Manager と通信できなければなりません。
- 外部ネットワークプロバイダーとして OVN プロバイダーを Red Hat Virtualization に追加する。
- OVN をデフォルトネットワークプロバイダーとして使用する新規クラスターを作成する。このクラスターに追加されたホストは、OVN と通信するように自動的に設定されます。

前提条件

OVN プロバイダーには以下のパッケージが必要なので、プロバイダーマシンで利用可能な状態でなければなりません。

- openvswitch-ovn-central
- openvswitch
- openvswitch-ovn-common
- python-openvswitch

これらのパッケージがプロバイダーマシンで有効化済みのリポジトリから利用することができない場合は、OVS Web サイト <http://openvswitch.org/download/> からダウンロードすることができます。

既存 OVN ネットワークプロバイダーの追加

1. OVN プロバイダーをインストールして設定します。

a. プロバイダーマシンにプロバイダーをインストールします。

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

b. Manager とは別のマシンにプロバイダーをインストールする場合は、以下のエントリーを `/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf` ファイルに追加します (このファイルが存在しない場合は作成します)。

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

認証が有効な場合に、このエントリーが認証のために使用されます。

c. OVN 集中サーバー とは別のマシンにプロバイダーをインストールする場合は、以下のエントリーを `/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf` ファイルに追加します (このファイルが存在しない場合は作成します)。

```
[OVN_REMOTE]
ovn-remote=tcp:OVN_central_server_IP:6641
```

d. ファイアウォールのポート 9696、6641、および 6642 を開放し、OVN プロバイダー、OVN 集中サーバー、および Manager 間の通信を許可します。手動でこの設定を行うか、適切なゾーンに `ovirt-provider-ovn` および `ovirt-provider-ovn-central` サービスを追加して設定することができます。

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

e. サービスを起動し、さらに有効にします。

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


- f. ポート 6642 および 6641 からリクエストをリスンするように OVN 集中サーバーを設定します。

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

2. 管理ポータルで **管理** → **プロバイダー** をクリックします。
3. **追加** をクリックします。
4. **名前** と **説明** を入力します。
5. **タイプ** の一覧から **外部ネットワークプロバイダー** を選択します。
6. **ネットワークプラグイン** のテキストボックスをクリックし、ドロップダウンメニューから **OVN 向けの oVirt ネットワークプロバイダー** を選択します。
7. **プロバイダーの URL** のテキストフィールドに OVN プロバイダーの URL または完全修飾ドメイン名を入力し、後ろにポート番号を指定します。OVN プロバイダーと OVN 集中サーバーが別のマシンにある場合、これは集中サーバーではなくプロバイダーマシンの URL になります。OVN プロバイダーが Manager と同じマシンにある場合は、URL をデフォルトの <http://localhost:9696> から変更する必要はありません。
8. **読み取り専用** のチェックボックスからチェックを外し、Red Hat Virtualization Manager から新規 OVN ネットワークを作成するのを許可します。
9. オプションとして、**認証が必要** のチェックボックスを選択して OVN 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。
認証方法を `/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf` ファイルで設定する必要があります (このファイルが存在しない場合は作成します)。**ovirt-provider-ovn** サービスを再起動して、変更を有効にします。OVN の認証に関する詳細については、[「oVirt external network provider for OVN」](#) を参照してください。
10. 認証情報をテストします。
 - a. **テスト** をクリックし、入力した認証情報を使用して OVN と正しく認証できるかどうかをテストします。
 - b. OVN インスタンスが SSL を使用している場合には **プロバイダー証明書のインポート** ウィンドウが開きます。**OK** をクリックして OVN インスタンスの提供する証明書をインポートして、Manager がそのインスタンスと通信できるようにします。
11. **OK** をクリックします。
12. OVN をデフォルトネットワークプロバイダーとして使用する新規クラスターを作成します。[「新規クラスターの作成」](#) を参照して、**デフォルトのネットワークプロバイダー** ドロップダウンリストから OVN ネットワークプロバイダーを選択します。
13. ホストをクラスターに追加します。このクラスターに追加されたホストは、OVN と通信するように自動的に設定されます。新規ホストの追加方法については、[「Red Hat Virtualization Manager へのホストの追加」](#) を参照してください。
14. OVN ネットワークを新規クラスターにインポートまたは追加します。ネットワークのインポート方法については、[「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。OVN を使用する新規ネットワークの作成方法については、[「データセンターまたはクラスター内での新規論理ネットワークの作成」](#) を参照し、**Create on external provider** のチェックボックスを選択します。**ovirt-provider-ovn** がデフォルトで選択されています。

既存のデフォルトではないネットワークを使用するようにホストを設定する場合は、「[OVN トンネルネットワーク用のホスト設定](#)」を参照してください。

OVN ネットワークをネイティブの Red Hat Virtualization ネットワークに接続するには、**Connect to physical network** のチェックボックスを選択し、使用する Red Hat Virtualization ネットワークを指定します。詳細および前提条件については、「[物理ネットワークへの OVN ネットワークの接続](#)」を参照してください。

これで、OVN ネットワークを使用する仮想マシンを作成することができます。

11.2.8.3. OVN トンネルネットワーク用のホスト設定

ovirt-provider-ovn-driver Ansible Playbook を使用して、デフォルトの **ovirtmgmt** ネットワーク以外の既存ネットワークを使用するように、ホストを設定することができます。クラスター内の全ホストがネットワークにアクセスできる必要があります。



注記

ovirt-provider-ovn-driver Ansible Playbook は、既存のホストを更新します。新規ホストをクラスターに追加した場合には、Playbook を再度実行する必要があります。

OVN トンネルネットワーク用のホスト設定

1. Manager マシンで **playbooks** ディレクトリーに移動します。

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

2. 以下のパラメーターで **ansible-playbook** コマンドを実行します。

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

例11.1 ansible-playbook を使用したホストの更新

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



注記

OVN_Central_IP を新規ネットワーク上に置くことができますが、これは必須の要求ではありません。すべてのホストが **OVN_Central_IP** にアクセスできる必要があります。

VDSM_Network_Name は最長 15 文字です。

単一ホスト上の OVN トンネルネットワークの更新

vdsm-tool を使用して、単一ホスト上の OVN トンネルネットワークを更新することができます。

```
# vds
```

m-tool ovn-config **OVN_Central_IP Tunneling_IP_or_Network_Name**

例11.2 vds

m-tool を使用したホストの更新

```
# vds
```

m-tool ovn-config 192.168.0.1 MyNetwork

11.2.8.4. 物理ネットワークへの OVN ネットワークの接続

重要

この機能は Open vSwitch のサポートに依存しており、Red Hat Virtualization のテクノロジープレビュー機能としてのみ利用可能です。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。これらの機能は、近々発表予定の製品機能をリリースに先駆けてご提供することにより、お客様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。

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、[「テクノロジープレビュー機能のサポート範囲」](#)を参照してください。

ネイティブの Red Hat Virtualization ネットワークを覆う外部プロバイダーネットワークを作成することができます。これにより、各ネットワーク上の仮想マシンは同じサブネットを共有しているように見えます。

重要

OVN ネットワークにサブネットを作成した場合、そのネットワークを使用する仮想マシンはそこから IP アドレスを受け取ります。物理ネットワークから IP アドレスを割り当てる必要がある場合には、OVN ネットワークにサブネットを作成しないでください。

前提条件

- クラスターの **スイッチのタイプ** には、**OVS** を選択する必要があります。また、このクラスターに追加するホストには、既存の Red Hat Virtualization ネットワーク (**ovirtmgmt** ブリッジ等) が設定されていないこと。
- ホストで物理ネットワークが利用可能でなければなりません。そのためには、必要に応じてクラスターに物理ネットワークを設定します (**ネットワークの管理** ウィンドウまたは **新規論理ネットワーク** ウィンドウの **クラスター** タブを使用)。

物理ネットワークに接続された新規外部ネットワークの作成

1. **コンピュータ** → **クラスター** をクリックします。
2. クラスター名をクリックして、詳細ビューを表示します。
3. **論理ネットワーク** タブをクリックし、**ネットワークを追加** をクリックします。
4. ネットワークの **名前** を入力します。

5. **Create on external provider** のチェックボックスを選択します。**ovirt-provider-ovn** がデフォルトで選択されています。
6. デフォルトで **Connect to physical network** のチェックボックスが選択されていない場合は、チェックボックスを選択します。
7. 新規ネットワークを接続する物理ネットワークを選択します。
 - **Data Center Network** のラジオボタンをクリックし、ドロップダウンリストから物理ネットワークを選択します。これが推奨されるオプションです。
 - **Custom** のラジオボタンをクリックし、物理ネットワークの名前を入力します。物理ネットワークの VLAN タグ付けが有効な場合は、**VLAN タグ付けを有効にする** のチェックボックスを選択し、物理ネットワークの VLAN タグも入力する必要があります。



重要

物理ネットワークの名前は 15 文字以下で、特殊文字を含んでいないこと。

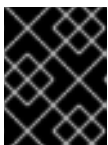
8. **OK** をクリックします。

11.2.9. 外部ネットワークプロバイダーの追加

Red Hat Virtualization には、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実装することが可能です。仮想インターフェースドライバーは、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と仮想インターフェースドライバーの参照実装は、<https://github.com/mmirecki/ovirt-provider-mock> および https://github.com/mmirecki/ovirt-provider-mock/blob/master/docs/driver_installation で入手することができます。

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の追加

1. **管理** → **プロバイダー** をクリックします。
2. **追加** をクリックします。
3. **名前** と **説明** を入力します。
4. **タイプ** のドロップダウンリストから **外部ネットワークプロバイダー** を選択します。
5. オプションとして、**ネットワークプラグイン** のテキストボックスをクリックし、ドロップダウンメニューから適切なドライバーを選択します。
6. **プロバイダーの URL** のテキストフィールドに外部ネットワークプロバイダーがインストールされたマシンの URL または完全修飾ドメイン名を入力し、後ろにポート番号を指定します。**読み取り専用** のチェックボックスは、デフォルトで選択されています。これは、ユーザーが外部ネットワークプロバイダーを変更するのを防ぎます。



重要

Red Hat のサポートを受けるには、**読み取り専用** のチェックボックスを選択したままにする必要があります。

7. オプションとして、**認証が必要** のチェックボックスを選択して、外部ネットワークプロバイダーの **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。

8. オプションとして、**Automatic Synchronization** のチェックボックスを選択します。これにより、外部ネットワークプロバイダーと既存ネットワークの自動同期が有効になります。外部ネットワークプロバイダーを追加する際のデフォルトでは、この機能は無効になっています。



注記

engine-setup ツールにより作成された **ovirt-provider-ovn** ネットワークプロバイダーでは、自動同期はデフォルトで有効になっています。

9. 認証情報をテストします。
- テスト** をクリックし、入力した認証情報を使用して外部ネットワークプロバイダーと正しく認証できるかどうかをテストします。
 - 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には **プロバイダー証明書のインポート** 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の提供する証明書をインポートして、Manager がそのインスタンスと通信できるようにします。
10. **OK** をクリックします。

このプロバイダーが提供するネットワークを使用する前には、ホストに仮想インターフェースドライバをインストールして、ネットワークをインポートする必要があります。ネットワークのインポート方法については、「[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。

11.2.10. プロバイダーの追加における全般の設定

プロバイダーの追加 ウィンドウの **全般** タブでは、外部プロバイダーの主要な情報を登録することができます。

表11.1 プロバイダーの追加: 全般の設定

設定	説明
名前	Manager で表示されるプロバイダーの名前
説明	プレーンテキスト形式の人間が判読できるプロバイダーの説明
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、プロバイダー設定で表示されるフィールドが変わります。</p> <p>Foreman/Satellite</p> <ul style="list-style-type: none"> プロバイダーの 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付ける必要はありません。 認証が必要: そのプロバイダーに認証が必要かどうかを指定することができます。Foreman/Satellite が選択されている場合には、認証は必須です。 Automatic Synchronization: プロバイダー

設定	説明
	<p>と既存のネットワークを自動的に同期させるかどうかを指定することができます。外部ネットワークプロバイダーを追加する際のデフォルトでは、この機能は無効になっています。</p> <ul style="list-style-type: none"> ● ユーザー名: Satellite インスタンスへ接続するためのユーザー名。このユーザー名は、Satellite インスタンス上のプロビジョニングポータルへのログインに使用するユーザー名である必要があります。デフォルトでは、このユーザー名は admin です。 ● パスワード: 上記のユーザーを認証するパスワード。このパスワードは、Satellite インスタンス上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ある必要があります。 <p>OpenStack Image</p> <ul style="list-style-type: none"> ● プロバイダーの URL: OpenStack Image サービ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 OpenStack Image サービスのポート番号を付ける必要があります。デフォルトでは、このポート番号は 9292 です。 ● 認証が必要: OpenStack Image サービスへのアクセスに認証が必要かどうかを指定することができます。 ● 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 サービスがメンバーとなっている Keystone インスタンスに登録済みの OpenStack Image サービスのユーザー名である必要があります。デフォルトでは、このユーザー名は glance です。 ● パスワード: 上記のユーザーを認証するパスワード。このパスワードは、OpenStack Image サービスがメンバーとなっている Keystone インスタンスに登録済みの OpenStack Image サービスのパスワードである必要があります。 ● テナント名: OpenStack Image サービスがメンバーとなっている OpenStack テナント。デフォルトでは、services です。 ● 認証 URL: OpenStack Image サービスが認証を行う Keystone サーバーの URL とポート <p>OpenStack Networking</p> <ul style="list-style-type: none"> ● ネットワークプラグイン: OpenStack Networking サーバーに接続するネットワークプラグイン。OpenStack Networking の場合、オプションは Open vSwitch のみで、デフォルトで選択されます。

設定	説明
	<ul style="list-style-type: none"> ● プロバイダーの URL: OpenStack Networking 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。この URL または完全修飾ドメイン名の末尾には OpenStack Networking インスタンスのポート番号を付ける必要があります。デフォルトでは、このポート番号は 9696 です。 ● 読み取り専用: 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することができます。 ● 認証が必要: OpenStack Networking サービスへのアクセスに認証が必要かどうかを指定することができます。 ● 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 インスタンスがメンバーとなっている Keystone インスタンスに登録済みの OpenStack Networking のユーザー名である必要があります。デフォルトでは、このユーザー名は neutron です。 ● パスワード: 上記のユーザーを認証するパスワード。このパスワードは、OpenStack Networking インスタンスがメンバーとなっている Keystone インスタンスに登録済みの OpenStack Networking のパスワードである必要があります。 ● テナント名: OpenStack Networking インスタンスがメンバーとなっている OpenStack テナント。デフォルトでは、services となります。 ● 認証 URL: OpenStack Networking インスタンスが認証を行う Keystone サーバーの URL とポート <p>OpenStack Volume</p> <ul style="list-style-type: none"> ● データセンター: OpenStack Volume ストレージボリュームがアタッチされるデータセンター ● プロバイダーの URL: OpenStack Volume 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。この URL または完全修飾ドメイン名の末尾には OpenStack Volume インスタンスのポート番号を付ける必要があります。デフォルトでは、このポート番号は 8776 です。 ● 認証が必要: OpenStack Volume サービスへのアクセスに認証が必要かどうかを指定することができます。 ● 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 インスタンスがメンバーとなっている Keystone インスタンスに登録済みの OpenStack Volume の

設定	説明
	<p>ユーザー名である必要があります。デフォルトでは、このユーザー名は cinder です。</p> <ul style="list-style-type: none"> ● パスワード: 上記のユーザーを認証するパスワード。このパスワードは、OpenStack Volume インスタンスがメンバーとなっている Keystone インスタンスに登録済みの OpenStack Volume のパスワードである必要があります。 ● テナント名: OpenStack Volume インスタンスがメンバーとなっている OpenStack テナント。デフォルトでは、services です。 ● 認証 URL: OpenStack Volume インスタンスが認証を行う Keystone サーバーの URL とポート <p>VMware</p> <ul style="list-style-type: none"> ● データセンター: VMware 仮想マシンのインポート先となるデータセンターを指定するか、任意のデータセンター を選択して個々のインポート操作中にインポート先のデータセンターを指定するようにします (仮想マシン タブの インポート 機能を使用)。 ● 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 ● データセンター: 指定した ESXi ホストが属するデータセンターの名前 ● クラスター: 指定した ESXi ホストが属するクラスターの名前 ● サーバーの SSL 証明書を確認: ESXi ホストの証明書を接続時に確認するかどうかを指定します。 ● プロキシホスト: 選択したデータセンターで、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、virt-v2v をインストール済みのホストを指定します。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可能である必要があります。任意のデータセンター を選択した場合は、ここでホストを指定することはできませんが、個々のインポート操作中にホストを指定することが可能です (仮想マシン タブの インポート 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、VMware データセンターと仮想マシンが属する ESXi ホストへのアクセスが可能です。必要があります。

設定	説明
	<ul style="list-style-type: none"> ● パスワード: 上記のユーザーを認証するパスワード <p>XEN</p> <ul style="list-style-type: none"> ● データセンター: Xen 仮想マシンのインポート先となるデータセンターを指定するか、任意のデータセンター を選択して個々のインポート操作中にインポート先のデータセンターを指定するようにします (仮想マシン タブの インポート 機能を使用)。 ● URI: Xen ホストの URI ● プロキシホスト: 選択したデータセンターで、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、virt-v2v をインストール済みのホストを指定します。このホストは、Xen 外部プロバイダーのネットワークに接続可能である必要もあります。任意のデータセンター を選択した場合は、ここでホストを指定することはできませんが、個々のインポート操作中にホストを指定することが可能です (仮想マシン タブの インポート 機能を使用)。 <p>KVM</p> <ul style="list-style-type: none"> ● データセンター: KVM 仮想マシンのインポート先となるデータセンターを指定するか、任意のデータセンター を選択して個々のインポート操作中にインポート先のデータセンターを指定するようにします (仮想マシン タブの インポート 機能を使用)。 ● URI: KVM ホストの URI ● プロキシホスト: 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、選択したデータセンター内のホストを指定します。このホストは、KVM 外部プロバイダーのネットワークに接続可能である必要もあります。任意のデータセンター を選択した場合は、ここでホストを指定することはできませんが、個々のインポート操作中にホストを指定することが可能です (仮想マシン タブの インポート 機能を使用)。 ● 認証が必要: KVM ホストへのアクセスに認証が必要かどうかを指定することができます。 ● ユーザー名: KVM ホストに接続するためのユーザー名 ● パスワード: 上記のユーザーを認証するパスワード <p>外部ネットワークプロバイダー</p> <ul style="list-style-type: none"> ● ネットワークプラグイン: NIC の操作を処理するために、ホスト上でどのドライバーの実装を使用するかを定義します。Open

設定	説明
	<p>Virtual Network (OVN) がデフォルトネットワークプロバイダーとしてクラスターに追加される場合には、クラスターに追加されたホストにどのドライバーがインストールされるかも定義します。</p> <ul style="list-style-type: none"> ● プロバイダーの URL: 外部ネットワークプロバイダーの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外部ネットワークプロバイダーのポート番号を付ける必要があります。デフォルトでは、このポート番号は 9696 です。 ● 読み取り専用: 外部ネットワークプロバイダーを管理ポータルから変更できるかどうかを指定することができます。 ● 認証が必要: 外部ネットワークプロバイダーへのアクセスに認証が必要かどうかを指定することができます。 ● 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。Active Directory を使用した認証の場合、ユーザー名の形式は、デフォルトの username@domain ではなく、username@domain@auth_profile となります。 ● パスワード: 上記のユーザーを認証するパスワード ● 認証 URL: 外部ネットワークプロバイダーが認証を行う認証サーバーの URL とポート
テスト	指定した認証情報をテストすることができます。このボタンは、全プロバイダータイプで利用することができます。

11.2.11. プロバイダーの追加における「エージェントの設定」の設定

プロバイダーの追加 ウィンドウの **エージェントの設定** タブでは、ネットワークプラグインに関する詳細を登録することができます。このタブは、**OpenStack Networking** プロバイダータイプでのみ使用することができます。

表11.2 プロバイダーの追加: 「エージェントの設定」の設定

設定	説明
インターフェースマッピング	label:interface 形式のマッピングのコンマ区切りリスト

設定	説明
ブローカータイプ	OpenStack Networking インスタンスが使用するメッセージブローカーのタイプ。 RabbitMQ または Qpid を選択します。
ホスト	メッセージブ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
SSH ポート	上記のホストと接続するリモートポート。このポートはデフォルトでは、ホストで SSL が有効化されていない場合には 5762、有効化されている場合には 5761 です。
ユーザー名	OpenStack Networking インスタンスを上記のメッセージブローカーで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。
パスワード	上記のユーザーを認証するパスワード

11.3. 外部プロバイダーの編集

外部プロバイダーの編集

1. 管理 → プロバイダー をクリックし、編集する外部プロバイダーを選択します。
2. 編集 をクリックします。
3. そのプロバイダーの現在の値を希望する値に変更します。
4. OK をクリックします。

11.4. 外部プロバイダーの削除

外部プロバイダーの削除

1. 管理 → プロバイダー をクリックし、削除する外部プロバイダーを選択します。
2. 削除 をクリックします。
3. OK をクリックします。

パート III. 環境の管理

第12章 バックアップと移行

12.1. RED HAT VIRTUALIZATION MANAGER のバックアップと復元

12.1.1. Red Hat Virtualization Manager のバックアップ

engine-backup ツールを使用して、Red Hat Virtualization Manager を定期的にバックアップします。このツールは、**ovirt-engine** サービスを中断せずに、engine 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することができます。

12.1.2. engine-backup コマンドの構文

engine-backup コマンドは、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、バックアップのスコープや engine データベースの異なる認証情報を指定することができる一連のパラメーターにより、さらに拡張されます。パラメーターとその機能の完全な一覧については、**engine-backup --help** を実行します。

基本オプション

--mode

コマンドがバックアップ操作と復元操作のどちらを実行するかを指定します。**backup** と **restore** の2つのオプションが利用可能です。これは必須のパラメーターです。

--file

バックアップモードでは、バックアップ対象ファイルのパスと名前を指定します。リストアモードでは、バックアップデータの読み取り先ファイルのパスと名前を指定します。これは、バックアップモードとリストア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の書き込み先ファイルのパスと名前を指定します。このパラメーターはバックアップモードとリストアモードの両方で必須のパラメーターです。

--scope

バックアップおよび復元操作のスコープを指定します。**all** (全データベースと設定データをバックアップ/復元)、**files** (システム上のファイルのみをバックアップ/復元)、**db** (Manager データベースのみをバックアップ/復元)、**dwhdb** (Data Warehouse データベースのみをバックアップ/復元) の4つのオプションがあります。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することができます。

Manager データベースのオプション

以下のオプションは、**engine-backup** コマンドを **restore** モードで使用する場合にのみ利用可能です。以下に示したオプションの構文は、Manager データベースの復元に適用します。Data Warehouse データベースの復元では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

Manager データベースのバックアップをリストアする先の PostgreSQL データベースを作成します。リモートホストの場合や新規インストールをして PostgreSQL データベースがまだ設定されていない場合にバックアップを復元する時に、このパラメーターは必要です。

--change-db-credentials

バックアップ自体に保管されている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することができます。このパラメーターに必要なその他のパラメーターについては、**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パーミッションを復元します (--no-restore-permissions の場合は復元させません)。バックアップの復元の際には、いずれかのパラメーターが必要です。



注記

追加のデータベースユーザーのアクセス許可がバックアップに含まれている場合には、**--restore-permissions** および **--provision-db** (または **--provision-dwh-db**) のオプションを指定してそのバックアップを復元すると、追加のユーザーが作成され、無作為なパスワードが設定されます。復元したシステムに追加のユーザーがアクセスする必要がある場合には、これらのパスワードを変更する必要があります。「[How to grant access to an extra database user after restoring Red Hat Virtualization from a backup](#)」の記事を参照してください。

12.1.3. 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、**engine-backup** コマンドを使用して Manager がアクティブな状態の時にバックアップすることができます。**--scope** に以下のオプションのいずれかを追加して、実行するバックアップを指定します。

- **all**: Manager 上の全データベースと設定ファイルの完全なバックアップ
- **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**: Data Warehouse データベースのみのバックアップ



重要

Red Hat Virtualization Manager の新規インストールにデータベースを復元するには、データベースのバックアップだけでは不十分です。Manager は設定ファイルにもアクセスする必要があります。デフォルトの **all** 以外の範囲を指定するバックアップは、**files** の範囲または filesystem バックアップと共に復元する必要があります。

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12.1 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12.2 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
```

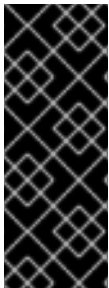
Data Warehouse データベースまたは Reports データベースをバックアップするには、**db** オプションを **dwhdb** に置き換えます。

指定したパスとファイル名で、バックアップが含まれた **tar** ファイルが作成されます。

バックアップが含まれた **tar** ファイルを環境の復元に使用できるようになりました。

12.1.4. engine-backup コマンドを使用したバックアップの復元

engine-backup コマンドを使用したバックアップの復元では、復元先によっては、バックアップの作成以外のステップも必要となります。たとえば、**engine-backup** コマンドを使用して、ローカルまたはリモートのデータベースを使用する既存の Red Hat Virtualization インストール上に、Red Hat Virtualization の新規インストールを復元することが可能です。



重要

バックアップは、そのバックアップと同じメジャーリリースの環境に対してのみ復元することが可能です。たとえば、Red Hat Virtualization バージョン 4.2 環境のバックアップは、別の Red Hat Virtualization バージョン 4.2 環境に対してのみ復元することができます。バックアップファイルに格納されている Red Hat Virtualization のバージョンを確認するには、そのバックアップファイルを展開し、そのファイルの root ディレクトリーにある **version** ファイルの値を読み取ってください。

12.1.5. 新規インストールへのバックアップ復元

engine-backup コマンドを使用して、Red Hat Virtualization Manager の新規インストールにバックアップを復元することができます。以下の手順は、ベースオペレーティングシステムと Red Hat Virtualization Manager の必須パッケージがインストール済みで、かつ **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バックアップファイル (単一または複数) にアクセスできることを前提としています。

新規インストールへのバックアップ復元

1. Manager マシンにログインします。engine データベースをリモートのホストに復元する場合には、そのホストにログオンして、適切な操作を実行する必要があります。また同様に、Data Warehouse をリモートホストに復元する場合には、そのホストにログインして、適切な操作を行う必要があります。
2. 完全な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。
 - 完全なバックアップを復元する場合:

```
# engine-backup --mode=restore --file=file_name --
log=log_file_name --provision-db --restore-permissions
```

Data Warehouse も全バックアップの一部として復元する場合には、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
```

- データベースのみのバックアップを復元する場合 (設定ファイルとデータベースのバックアップを復元):

```
# 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が復元されます。

```
# 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が復元されます。

正常に終了すると、以下のような出力が表示されます。

```
You should now run engine-setup.
Done.
```

3. 以下のコマンドを実行してプロンプトに従い、Manager を復元します。

```
# engine-setup
```

Red Hat Virtualization Manager がバックアップに保存されていた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-engine-rename ツール](#)」を参照してください。

12.1.6. バックアップの復元による既存インストールの上書き

engine-backup コマンドで Red Hat Virtualization Manager がすでにインストール/設定されているマシンにバックアップを復元することができます。この方法は、インストールのバックアップを取得済みで、そのインストールに対して変更を加えた後にバックアップからインストールを復元する場合に有効です。

重要

バックアップを復元して既存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インストールをクリーンアップしておく必要があります。**engine-cleanup** コマンドは、engine データベースをクリーンアップするのみで、データベースをドロップしたり、データベースを所有するユーザーを削除したりはしません。このため、ユーザーとデータベースはすでに存在しているので、新規データベース作成やデータベース認証情報の指定は必要ありません。

バックアップの復元による既存インストールの上書き

1. Red Hat Virtualization Manager マシンにログインします。
2. 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
```

3. 完全な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。
4. 完全なバックアップを復元する場合:

```
# engine-backup --mode=restore --file=file_name --log=log_file_name
--restore-permissions
```

5. データベースのみのバックアップを復元する場合 (設定ファイルとデータベースのバックアップを復元):

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

上記の例は、Manager データベースのバックアップを復元します。必要な場合には、Data Warehouse の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
```

正常に終了すると、以下のような出力が表示されます。

```
You should now run engine-setup.
Done.
```

6. 以下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て、**ovirt-engine** サービスを正しく設定します。

```
# engine-setup
```

12.1.7. 異なる認証情報を使用したバックアップの復元

バックアップ内のデータベースの認証情報がバックアップの復元先となるマシンのデータベースの認証情報と異なる場合でも、**engine-backup** コマンドを使用して、Red Hat Virtualization Manager がすでにインストール/設定済みのマシンにバックアップを復元することができます。この方法は、インストールのバックアップを作成済みで、そのインストールをバックアップから別のシステムに復元する必要がある場合に有効です。



重要

バックアップを復元して既存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インストールをクリーンアップしておく必要があります。**engine-cleanup** コマンドは、engine データベースをクリーンアップするのみで、データベースをドロップしたり、データベースを所有するユーザーを削除したりはしません。このため、ユーザーとデータベースはすでに存在しているので、新規データベース作成やデータベース認証情報の指定は必要ありません。ただし、engine データベースの所有者の認証情報が不明の場合には、バックアップを復元する前に変更しておく必要があります。

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 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 の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
```

3. **engine** データベースの所有者の認証情報が不明の場合には、そのユーザーのパスワードを変更します。

- a. postgresql のコマンドラインに入ります。

```
# su - postgres -c 'scl enable rh-postgresql95 -- psql'
```

- b. 以下のコマンドを実行して、**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';
```

必要な場合には、**ovirt_engine_dwh** のデータベースを所有するユーザーにも上記のコマンドを実行します。

4. **--change-db-credentials** パラメーターを使用して新しいデータベースの認証情報を渡し、完全な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。Manager のローカルに設定されているデータベースの **database_location** は **localhost** です。



注記

以下の例では、パスワードは指定せずに、各データベースに **--*password** オプションを使用するため、このコマンドを実行すると、データベースごとにパスワードを入力するように要求されます。コマンド内でこれらのオプションにパスワードを指定することも可能ですが、パスワードが shell の履歴に保存されてしまうため推奨しません。別の方法として、各データベースに **--*passfile=password_file** オプションを使用して、対話型プロンプトの必要なくパスワードをセキュアに **engine-backup** ツールに渡すことができます。

- 完全なバックアップを復元する場合:

```
# 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 も全バックアップの一部として復元する場合には、追加のデータベースの変更後の認証情報を含めるようにしてください。

```
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
```

- データベースのみのバックアップを復元する場合 (設定ファイルとデータベースのバックアップを復元):

```
# 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が復元されます。

```
# 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が復元されます。

正常に終了すると、以下のような出力が表示されます。

```
You should now run engine-setup.
Done.
```

5. 以下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て、**ovirt-engine** サービスを正しく設定します。

```
# engine-setup
```

12.1.8. リモートサーバーデータベースへの **engine** データベースの移行

Red Hat Virtualization Manager の初期設定の後に、**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することができます。データベースのバックアップの作成や、新規データベースサーバーへのバックアップの復元には、**engine-backup** を使用します。以下の手順は、新規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ており、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「[必要なエンタイトルメントのサブスクリプション](#)」を参照してください。

データベースの移行

1. Red Hat Virtualization Manager のマシンにログインし、engine のバックアップと干渉しないように **ovirt-engine** サービスを停止します。

```
# 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. 新規データベースにログインして **engine-backup** をインストールします。

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

5. 新規データベースサーバーに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に置き換えてください。

```
# 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** サービスを起動します。

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

12.2. バックアップ/リストア API を使用した仮想マシンのバックアップと復元

12.2.1. バックアップ/リストア API

バックアップ/リストア API は、全体またはファイルレベルでの仮想マシンのバックアップと復元を可能にする機能のコレクションです。この API は、ライブスナップショットや REST API などの Red Hat Virtualization の複数のコンポーネントを組み合わせ、独立系のソフトウェアプロバイダーの提供するバックアップソフトウェアが実装された仮想マシンにアタッチできる一時ボリュームを作成/操作します。

サポート対象のサードパーティーバックアップベンダーについては、[「The Red Hat Ecosystem」](#) をご確認ください。

12.2.2. 仮想マシンのバックアップ

バックアップ/リストア API を使用して仮想マシンをバックアップします。以下の手順は、バックアップ用の仮想マシンと、バックアップを管理するソフトウェアのインストール先となる仮想マシンの合計 2 台が用意されていることを前提とします。

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、スナップショット作成時点の仮想マシンの設定データのコピーは、そのスナップショット下の **initialization** 内の **configuration** 属性の **data** 属性に保管されます。



重要

共有可能とマークされたディスクまたは直接 LUN ディスクをベースとするディスクのスナップショットは作成できません。

- スナップショット下の **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 とスナップショット 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
```

- バックアップ用仮想マシンにスナップショットをアタッチします。その際、正しいインターフェースタイプ (例: **virtio_scsi**) を設定してアクティブなディスクとしてアタッチします。

```
POST /api/vms/22222222-2222-2222-2222-222222222222/diskattachments/
HTTP/1.1
Accept: application/xml
Content-type: application/xml

<disk_attachment>
  <active>true</active>
  <interface>_virtio_scsi</interface>
  <disk id="11111111-1111-1111-1111-111111111111">
    <snapshot id="11111111-1111-1111-1111-111111111111"/>
  </disk>
</disk_attachment>
```

- バックアップ用仮想マシンでバックアップソフトウェアを使用して、スナップショット上のデータをバックアップします。

6. バックアップ用仮想マシンからスナップショットディスクのアタッチを解除します。

```
DELETE /api/vms/22222222-2222-2222-2222-222222222222/diskattachments/11111111-1111-1111-1111-111111111111 HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

7. オプションとして、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したバックアップソフトウェアを使用して、一定時点の仮想マシンがバックアップされました。

12.2.3. 仮想マシンの復元

バックアップ/リストア API を使用してバックアップした仮想マシンを復元します。以下の手順は、以前のバックアップの管理に使用するソフトウェアがインストール済みの仮想マシン 1 台が用意されていることを前提とします。

仮想マシンの復元

1. 管理ポータルで、バックアップを復元するためのフローティングディスクを作成します。フローティングディスクの作成方法についての説明は「[仮想ディスクの作成](#)」を参照してください。
2. バックアップ用仮想マシンにディスクをアタッチします。

```
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>
```

3. バックアップソフトウェアを使用して、ディスクにバックアップを復元します。
4. バックアップ用仮想マシンからディスクをデタッチします。

```
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>
```

5. 復元する仮想マシンの設定データを使用して、新規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. 新規仮想マシンにディスクをアタッチします。

```
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/リストア API を使用して作成したバックアップで、仮想マシンを復元しました。

第13章 RED HAT SATELLITE によるエラータ管理

Red Hat Virtualization では、Red Hat Satellite からエラータを Red Hat Virtualization Manager で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、それらを対象とする利用可能なエラータの更新とそれらの重大度についての情報を受信できるようになります。受信した更新は、管理者が選択して、対象のホスト、仮想マシン、または Manager で実行して、適用することができます。Red Hat Satellite についての詳しい情報は、『[Red Hat Satellite User Guide](#)』を参照してください。

Red Hat Virtualization 4.2 では、Red Hat Satellite 6.1 を使用したエラータ管理をサポートしています。



重要

Satellite サーバー内では、Manager、ホスト、および仮想マシンは FQDN で識別されます。このため、外部コンテンツホストの ID を Red Hat Virtualization で維持管理する必要はありません。

Manager、ホスト、および仮想マシンの管理に使用する Satellite のアカウントには、管理者の権限とデフォルトの組織を設定する必要があります。

Red Hat Virtualization エラータの設定

Manager、ホスト、仮想マシンを Red Hat Satellite プロバイダーと関連付けるには、最初に Manager をプロバイダーと関連付ける必要があります。次に、ホストを同じプロバイダーに関連付け設定します。最後に仮想マシンを同じプロバイダーに関連付けて設定します。

1. Manager を関連付けるには、Satellite サーバーを外部プロバイダーとして追加します。詳しい説明は、『[ホスト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、Satellite サーバーにコンテンツホストとして登録し、katello-agent パッケージをインストールする必要があります。

ホスト登録の設定方法についての詳しい情報は、『[Red Hat Satellite User Guide](#)』の『[Configuring a Host for Registration](#)』のセクションを参照してください。また、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に関する詳しい情報は、『[Red Hat Satellite User Guide](#)』の『[Registration](#)』のセクションを参照してください。

2. オプションで、必要なホストがエラータを表示するように設定します。詳しくは、『[ホストを対象とする Satellite のエラータ管理の設定](#)』を参照してください。
3. オプションで、必要な仮想マシンが利用可能なエラータを表示するように設定します。その仮想マシンを設定する前に、関連付けられたホストを設定しておく必要があります。詳しくは、『[仮想マシン管理ガイド](#)』の『[仮想マシンの Red Hat Satellite エラータ管理の設定](#)』のセクションを参照してください。

Red Hat Virtualization Manager エラータの表示

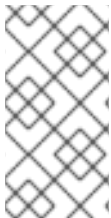
1. **管理** → **エラータ** をクリックします。
2. **セキュリティ**、**バグ**、または **機能拡張** のチェックボックスを選択すると、そのタイプのエラータのみが表示されます。

ホストに利用可能なエラータの表示方法に関する詳しい説明は、「[ホストのエラータの表示](#)」および『[仮想マシン管理ガイド](#)』の「[仮想マシンの Red Hat Satellite エラータの表示](#)」のセクションを参照してください。

第14章 ANSIBLE を使用した設定作業の自動化

Ansible は、システムの設定、ソフトウェアのデプロイ、およびローリングアップデートの実行に使用する自動化ツールです。Ansible には Red Hat Virtualization のサポートが含まれ、Ansible のモジュールを使用してインストール後の作業 (データセンターのセットアップおよび設定、ユーザーの管理、または仮想マシンの操作) を自動化することができます。

REST API および SDK を用いた場合と比較して、Ansible による Red Hat Virtualization 設定の自動化は容易で、他の Ansible モジュールと統合することができます。Red Hat Virtualization に利用可能な Ansible モジュールの詳細については、Ansible のドキュメントの [Ovirt modules](#) を参照してください。



注記

Ansible Tower は、Ansible の Web インターフェースおよび REST API エンドポイントからアクセスできるグラフィック対応のフレームワークです。Ansible Tower に対するサポートを受けるには、Ansible Tower のライセンスが必要です (Red Hat Virtualization のサブスクリプションには含まれていません)。

Ansible は Red Hat Virtualization に同梱されています。Ansible をインストールするには、必要なりポジトリを有効にする必要があります。『インストールガイド』の「[必要なエンタイトルメントのサブスクリプト](#)」を参照し、以下のコマンドを実行してください。

```
# yum install ansible
```

その他のインストール手順および Ansible の使用方法については、[Ansible のドキュメント](#) を参照してください。

14.1. ANSIBLE ロール

Red Hat Virtualization インフラストラクチャーのさまざまな要素の設定および管理に役立つ Ansible ロールが、複数用意されています。Ansible ロールにより、大規模な Playbook を他のユーザーと共有できる小規模で再利用可能なファイルに分割して、Ansible コードをモジュール化することができます。

Red Hat Virtualization で利用可能な Ansible ロールは、さまざまなインフラストラクチャーコンポーネントごとにカテゴリー分けされます。Ansible ロールの詳細については、「[oVirt Ansible Roles](#)」のドキュメントを参照してください。Ansible ロールと共にインストールされるドキュメントについては、「[Ansible ロールのインストール](#)」を参照してください。

14.1.1. Ansible ロールのインストール

Red Hat Virtualization 用の Ansible ロールは、「rhel-7-server-rhv-4.2-manager-rpms」リポジトリからインストールすることができます。詳細については、『インストールガイド』の「[必要なエンタイトルメントのサブスクリプト](#)」を参照してください。

以下のコマンドを使用して Ansible ロールをインストールします。

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

デフォルトでは、ロールは **/usr/share/ansible/roles** にインストールされます。**ovirt-ansible-roles** パッケージの構成は以下のとおりです。

- **/usr/share/ansible/roles**: ロールを保管

- `/usr/share/doc/ovirt-ansible-roles/`: サンプル、基本概要、およびライセンスを保管
- `/usr/share/doc/ansible/roles/role_name`: ロールに固有のドキュメントを保管

14.1.2. Ansible ロールを使用した Red Hat Virtualization の設定

以下の手順で、Ansible ロールを使用した Playbook の作成/実行から Red Hat Virtualization 設定までの一連のプロセスを説明します。以下の例では、Ansible を使用してローカルマシン上の Manager に接続し、新規データセンターを作成します。

前提条件

- `/etc/ansible/ansible.cfg` の `roles_path` オプションが Ansible ロールの場所 (`/usr/share/ansible/roles`) をポイントしていること。
- Playbook を実行するマシンに Python SDK がインストールされていること。

Ansible ロールを使用した Red Hat Virtualization の設定

1. 作業ディレクトリーに、Red Hat Virtualization Manager のユーザーパスワードを保管するためのファイルを作成します。

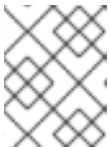
```
# cat passwords.yml
---
engine_password: youruserpassword
```

2. ユーザーパスワードを暗号化します。Vault パスワードが要求されます。

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

3. URL、証明書の場合、ユーザー等の Manager に関する情報を保管するファイルを作成します。

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



注記

これらの変数は、ファイルに保管せずに直接 Playbook に追加することもできます。

4. Playbook を作成します。この手順を簡素化する場合には、`/usr/share/doc/ovirt-ansible-roles/examples` のサンプルをコピーしてそれを変更することができます。

```
# cat rhv_infra.yml
---
- name: RHV infrastructure
  hosts: localhost
  connection: local
  gather_facts: false
```

```

vars_files:
  # Contains variables to connect to the Manager
  - engine_vars.yml
  # Contains encrypted engine_password variable using ansible-
vault
  - passwords.yml

pre_tasks:
  - name: Login to RHV
    ovirt_auth:
      url: "{{ engine_url }}"
      username: "{{ engine_user }}"
      password: "{{ engine_password }}"
      ca_file: "{{ engine_cafile | default(omit) }}"
      insecure: "{{ engine_insecure | default(true) }}"
    tags:
      - always

vars:
  data_center_name: mydatacenter
  data_center_description: mydatacenter
  data_center_local: false
  compatibility_version: 4.1

roles:
  - ovirt-datacenters

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

```

5. Playbook を実行します。

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

ovirt-datacenters Ansible ロールを使用して、**mydatacenter** という名前のデータセンターを正しく作成することができました。

第15章 ユーザーとロール

15.1. ユーザーについて

Red Hat Virtualization では、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。デフォルトのローカルドメインは **internal** ドメインと呼ばれ、Manager のインストールプロセス中に **admin** というデフォルトユーザーが作成されます。

ovirt-aaa-jdbc-tool を使用して、**internal** に追加のユーザーを作成することができます。ローカルドメイン上で作成されるユーザーアカウントはローカルユーザーと呼ばれます。また、Red Hat Directory Server、Active Directory、OpenLDAP、その他多数のサポートされているオプションの外部ディレクトリーサーバーを Rerprise Virtualization 環境にアタッチして、外部ドメインとして使用することができます。ユーザーアカウントはディレクトリーユーザーと呼ばれます。

ローカルユーザーおよびディレクトリーユーザーが環境内で正常に機能するためには、いずれのユーザーに対しても、管理ポータルから適切なロールとパーミッションを割り当てる必要があります。ユーザーロールには主に、エンドユーザーと管理者の 2 タイプがあります。エンドユーザーロールは、VM 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管理します。ロールは、仮想マシンやホストなどの個別のリソースを対象としたり、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を対象としたりすることができます。

15.2. ディレクトリーサーバーの概要

Red Hat Virtualization Manager は、インストール中に **internal** ドメイン上に **admin** ユーザーを作成します。このユーザーの別名は、**admin@internal** です。このアカウントは、環境の初期設定と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。外部のディレクトリーサーバーをアタッチし、ディレクトリーユーザーを追加してからそれらのユーザーに適切なロールとパーミッションを割り当てた後には、必要がなければ **admin@internal** ユーザーを無効にすることができます。サポートされるディレクトリーサーバーは以下のとおりです。

- 389ds
- 389ds RFC-2307 スキーマ
- Active Directory
- IBM Security Directory Server
- IBM Security Directory Server RFC-2307 スキーマ
- FreeIPA
- iDM
- Novell eDirectory RFC-2307 スキーマ
- OpenLDAP RFC-2307 スキーマ
- OpenLDAP Standard スキーマ
- 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 スキーマ
- iPlanet



重要

Red Hat Virtualization Manager (**rhev**m) と IdM (**ipa-server**) は同じシステム上にはインストールできません。IdM には、Red Hat Virtualization Manager に必要とされる **mod_ssl** パッケージとの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ており、テンプレートおよび仮想マシンの作成で **sysprep** を使用する場合には、Red Hat Virtualization 管理者ユーザーにドメインの制御を委任して、以下のような操作を行えるようにする必要があります。

- コンピューターをドメインにアタッチする
- グループのメンバーシップを変更する

Active Directory のユーザーアカウントの作成に関する情報は「[Create a New User Account](#)」を参照してください。

Active Directory の制御の委任に関する情報は「[Delegate Control of an Organizational Unit](#)」を参照してください。

15.3. 外部の LDAP プロバイダーの設定

15.3.1. 外部の LDAP プロバイダーの設定 (対話式の設定)

ovirt-engine-extension-aaa-ldap 拡張機能により、ユーザーは外部ディレクトリーの設定を容易にカスタマイズすることができます。**ovirt-engine-extension-aaa-ldap** 拡張機能は多数の異なる LDAP サーバータイプをサポートし、大半の LDAP タイプの設定に役立つ対話型の設定スクリプトが提供されます。

対話型の設定スクリプトに LDAP サーバータイプがリストされていない場合や、さらにカスタマイズする必要がある場合には、設定ファイルを手動で編集することができます。詳しい情報は、「[外部の LDAP プロバイダーの設定 \(手動の設定\)](#)」を参照してください。

Active Directory の例は、「[Active Directory のアタッチ](#)」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る必要があります。
- LDAP サーバーと Manager の間でセキュアな接続を設定するには、PEM エンコードされた CA 証明書が準備されている必要があります。
- LDAP サーバーに対して検索およびログインのクエリーを実行する準備の整っているアカウント名とパスワードのセットを少なくとも 1 つ用意してください。

外部の LDAP プロバイダーの設定

1. Red Hat Virtualization Manager に LDAP 拡張機能の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、対話式の設定を開始します。

```
# ovirt-engine-extension-aaa-ldap-setup
```

3. 対応する番号を入力して LDAP タイプを選択します。お使いの LDAP サーバーのスキーマがどれかわからない場合には、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 の場合には、「[Active Directory のアタッチ](#)」の手順に従ってください。

```
Available LDAP implementations:
 1 - 389ds
 2 - 389ds RFC-2307 Schema
 3 - Active Directory
 4 - IBM Security Directory Server
 5 - IBM Security Directory Server RFC-2307 Schema
 6 - IPA
 7 - Novell eDirectory RFC-2307 Schema
 8 - OpenLDAP RFC-2307 Schema
 9 - OpenLDAP Standard Schema
10 - Oracle Unified Directory RFC-2307 Schema
11 - RFC-2307 Schema (Generic)
12 - RHDS
13 - RHDS RFC-2307 Schema
14 - iPlanet
Please select:
```

4. **Enter** を押して、デフォルト値を受け入れ、お使いの 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]:
```

5. DNS ポリシーメソッドを選択します。

- オプション 1 の場合は、**/etc/resolv.conf** にリストされている DNS サーバーが IP アドレス解決に使用されます。**/etc/resolv.conf** ファイルが最新の状態で、正しい DNS サーバーの情報が記載されていることを確認してください。
- オプション 2 の場合は、LDAP サーバーの完全修飾ドメイン名 (FQDN) または IP アドレスを入力します。**dig** コマンドで SRV レコードを使用してドメイン名を確認することができます。SRV レコードは、**_service._protocol.domain name** の形式を取ります。たとえば、**dig _ldap._tcp.redhat.com SRV** のようになります。
- オプション 3 の場合は、LDAP サーバーのスペース区切り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 サーバー間のロードバランシングを指定します。クエリーは、ラウンドロビンアルゴリズムに従って、全 LDAP サーバー間で分散されます。
- オプション 4 の場合は、LDAP サーバーのスペース区切り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。最初のサーバーが利用できない場合には、クエリーはこのリストで次に記載されている LDAP サーバーに割り当てられます。

```
1 - Single server
2 - DNS domain LDAP SRV record
3 - Round-robin between multiple hosts
4 - Failover between multiple hosts
Please select:
```

6. お使いの LDAP サーバーがサポートするセキュアな接続メソッドを選択し、PEM エンコードされた CA 証明書の取得にそのメソッドを指定します。

- **File** の場合は、証明書へのフルパスを指定することができます。
- **URL** の場合は、証明書の URL を指定することができます。
- **Inline** の場合は、証明書の内容をターミナルにペーストすることができます。
- **System** の場合は、全 CA ファイルのデフォルトの場所を指定することができます。
- **Insecure** の場合は証明書の検証はスキップされますが、接続は引き続き TLS で暗号化されます。

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 ldaps protocol.

Use plain for test environments only.

Please select protocol to use (startTLS, ldaps, plain)

[startTLS]: **startTLS**

Please select method to obtain PEM encoded CA certificate (File, URL, Inline, System, Insecure):

Please enter the password:



注記

LDAPS とは、Lightweight Directory Access Protocol Over Secure Socket Link の略語です。SSL 接続の場合には、**ldaps** オプションを選択してください。

7. 検索ユーザーの識別名を入力します。このユーザーには、ディレクトリーサーバー上の全ユーザーとグループを参照するパーミッションが必要です。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には、入力なしで **Enter** を押してください。

```
Enter search user DN (for example uid=username,dc=example,dc=com or
leave empty for anonymous): uid=user1,ou=Users,ou=department-
1,dc=example,dc=com
```

```
Enter search user password:
```

8. ベース DN を入力します。

Please enter base DN (dc=redhat,dc=com) [dc=redhat,dc=com]:
ou=department-1,dc=redhat,dc=com

9. 仮想マシンにシングルサインオンを設定する予定の場合には **Yes** を選択してください。この機能は、管理ポータルにシングルサインオンする機能と共には使用できない点に注意してください。スクリプトにより、プロファイル名がドメイン名と一致する必要があることを注意するメッセージが表示されます。『仮想マシン管理ガイド』の「[仮想マシンへのシングルサインオン \(SSO\) 設定](#)」に記載の手順を実行する必要があります。

Are you going to use Single Sign-On for Virtual Machines (Yes, No)
 [Yes]:

10. 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。以下の例では **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。`ovirt-engine` サービスを再起動して、変更を有効にします。

Please specify profile name that will be visible to users:
redhat.com

図15.1 管理者ポータルのログインページ



注記

ユーザーは、初回ログイン時にドロップダウンリストからプロファイルを選択する必要があります。この情報は、ブラウザのクッキーに保管され、次のユーザーログインでは事前に選択されます。

11. ログイン機能をテストして、LDAP サーバーが Red Hat Virtualization 環境に適切に接続されていることを確認します。ログインクエリーのために、**ユーザー名** と **パスワード** を入力します。

NOTE:

It is highly recommended to test drive the configuration before applying it into engine.

Login sequence is executed automatically, but it is recommended to also execute Search sequence manually after successful Login sequence.

Please provide credentials to test login flow:

Enter user name:

Enter user password:

[INFO] Executing login sequence...

...

[INFO] Login sequence executed successfully

12. ユーザー情報が正しいことを確認します。ユーザー情報が間違っている場合は、**Abort** を選択します。

Please make sure that user details are correct and group membership meets expectations (search for PrincipalRecord and GroupRecord titles).

Abort if output is incorrect.

Select test sequence to execute (Done, Abort, Login, Search)

[Abort]:

13. 手動で検索機能をテストすることを推奨します。検索クエリーでは、ユーザーアカウントの場合は **Principal** を、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情報が返されるようにするには、**Resolve Groups** で **Yes** を選択します。3 つの設定ファイルが作成され、画面の出力に表示されます。

Select test sequence to execute (Done, Abort, Login, Search)

[Search]: **Search**

Select entity to search (Principal, Group) [Principal]:

Term to search, trailing '*' is allowed: **testuser1**

Resolve Groups (Yes, No) [No]:

14. 設定を完了するには、**Done** を選択します。

Select test sequence to execute (Done, Abort, Login, Search)

[Abort]: **Done**

[INFO] Stage: Transaction setup

[INFO] Stage: Misc configuration

[INFO] Stage: Package installation

[INFO] Stage: Misc configuration

[INFO] Stage: Transaction commit

[INFO] Stage: Closing up

CONFIGURATION SUMMARY

Profile name is: redhat.com

The following files were created:

/etc/ovirt-engine/aaa/redhat.com.properties

/etc/ovirt-engine/extensions.d/redhat.com.properties

/etc/ovirt-engine/extensions.d/redhat.com-authn.properties

```
[ INFO ] Stage: Clean up
Log file is available at /tmp/ovirt-engine-extension-aaa-ldap-setup-
20171004101225-mmneib.log:
[ INFO ] Stage: Pre-termination
[ INFO ] Stage: Termination
```

15. **ovirt-engine** サービスを再起動します。作成したプロファイルが管理ポータルと VM ユーザーポータルのログインページで選択できるようになりました。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 (例: VM ユーザーポータルへのログイン) を割り当てるには、「[管理ポータルからのユーザー管理タスク](#)」を参照してください。

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



注記

詳しい情報は、`/usr/share/doc/ovirt-engine-extension-aaa-ldap-version` にある LDAP の認証/承認の拡張機能の README ファイルを参照してください。

15.3.2. Active Directory のアタッチ

前提条件:

- Active Directory の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。



注記

ovirt-engine-extension-aaa-ldap-setup ツールを使って設定することのできない、最も一般的な Active Directory 設定の例が、`/usr/share/ovirt-engine-extension-aaa-ldap/examples/README.md` に記載されています。

- Manager の `/etc/resolv.conf` ファイルに、Active Directory のフォレスト名を解決できる DNS サーバーを追加するか、Active Directory DNS サーバーを書き留めておいて、対話型のセットアップスクリプトで要求された時に入力します。
- LDAP サーバーと Manager の間でセキュアな接続を設定するには、PEM エンコードされた CA 証明書が準備されている必要があります。詳しくは、「[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。
- 匿名の検索がサポートされていない限りは、Active Directory 上で全ユーザーおよびグループを参照するパーミッションのあるユーザーを検索ユーザーとして使用する必要があります。検索ユーザーの識別名をメモします。Active Directory の管理ユーザーは使用しないでください。
- Active Directory に対して検索およびログインのクエリーを実行する準備の整っているアカウント名とパスワードのセットを少なくとも 1 つ用意してください。

外部の LDAP プロバイダーの設定

1. Red Hat Virtualization Manager に LDAP 拡張機能の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、対話式の設定を開始します。

■

```
# ovirt-engine-extension-aaa-ldap-setup
```

3. 対応する番号を入力して、LDAP タイプを選択します。このステップの後に表示される 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 - IBM Security Directory Server
5 - IBM Security Directory Server RFC-2307 Schema
6 - IPA
7 - Novell eDirectory RFC-2307 Schema
8 - OpenLDAP RFC-2307 Schema
9 - OpenLDAP Standard Schema
10 - Oracle Unified Directory RFC-2307 Schema
11 - RFC-2307 Schema (Generic)
12 - RHDS
13 - RHDS RFC-2307 Schema
14 - iPlanet
Please select: 3
```

4. Active Directory のフォレスト名を入力します。Manager の DNS でそのフォレスト名が解決できない場合には、スクリプトによりプロンプトが表示され、Active Directory DNS サーバー名をスペース区切りリストで入力するように要求されます。

```
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
```

5. お使いの LDAP サーバーがサポートするセキュアな接続メソッドを選択し、PEM エンコードされた CA 証明書の取得にそのメソッドを指定します。File オプションを選択すると、証明書へのフルパスを指定することができます。URL オプションを選択すると、証明書の URL を指定することができます。証明書の内容をターミナルにペーストするには、Inline オプションを選択します。System オプションを選択すると、全 CA ファイルの場所を指定することができます。Insecure オプションを選択すると、startTLS を非セキュアモードで 사용할 ことができます。

```
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 とは、Lightweight Directory Access Protocol Over Secure Socket Link の略語です。SSL 接続の場合には、**ldaps** オプションを選択してください。

PEM エンコードされた CA 証明書の作成に関する詳しい説明は、[「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を入力します。このユーザーには、ディレクトリーサーバー上の全ユーザーとグループを参照するパーミッションが必要です。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には、入力なしで **Enter** を押してください。

```
Enter search user DN (empty for anonymous):
uid=user1,ou=Users,dc=test,dc=redhat,dc=com
Enter search user password:
```

- 仮想マシンにシングルサインオンを使用するかどうかを指定します。この機能はデフォルトで有効になっていますが、管理ポータルへのシングルサインオンが有効な場合には使用することができません。スクリプトにより、プロファイル名がドメイン名と一致する必要があることを注意するメッセージが表示されます。『[仮想マシン管理ガイド](#)』の「[仮想マシンへのシングルサインオン \(SSO\) 設定](#)」に記載の手順を実行する必要があります。

```
Are you going to use Single Sign-On for Virtual Machines (Yes, No)
[Yes]:
```

- 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。以下の例では **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 管理者ポータルのログインページ



注記

ユーザーは、初回ログイン時にドロップダウンリストから希望のプロファイルを選択する必要があります。この情報は、ブラウザのクッキーに保管され、次のユーザーログインでは事前に選択されます。

9. 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 環境に適切に接続されていることを確認します。ログインクエリーでは、アカウント名とパスワードを入力します。検索クエリーでは、ユーザーアカウントの場合は **Principal** を、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情報が返されるようにするには、**Resolve Groups** に **Yes** と入力します。設定を完了するには、**Done** を選択します。3 つの設定ファイルが作成され、画面の出力に表示されます。

NOTE:

It is highly recommended to test drive the configuration before applying it into engine.

Login sequence is executed automatically, but it is recommended to also execute Search sequence manually after successful Login sequence.

Select test sequence to execute (Done, Abort, Login, Search)

[Abort]: Login

Enter search user name: **testuser1**

Enter search user password:

[INFO] Executing login sequence...

...

Select test sequence to execute (Done, Abort, Login, Search)

[Abort]: Search

Select entity to search (Principal, Group) [Principal]:

Term to search, trailing '*' is allowed: **testuser1**

Resolve Groups (Yes, No) [No]:

[INFO] Executing login sequence...

...

Select test sequence to execute (Done, Abort, Login, Search)

[Abort]: Done

[INFO] Stage: Transaction setup

[INFO] Stage: Misc configuration

[INFO] Stage: Package installation

[INFO] Stage: Misc configuration

[INFO] Stage: Transaction commit

[INFO] Stage: Closing up

CONFIGURATION SUMMARY

Profile name is: **redhat.com**

The following files were created:

/etc/ovirt-engine/aaa/**redhat.com**.properties

/etc/ovirt-engine/extensions.d/**redhat.com**-

authz.properties

/etc/ovirt-engine/extensions.d/**redhat.com**-

authn.properties

[INFO] Stage: Clean up

Log file is available at /tmp/ovirt-engine-extension-aaa-

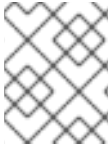
ldap-setup-20160114064955-1yar9i.log:

[INFO] Stage: Pre-termination

[INFO] Stage: Termination

10. 作成したプロファイルが管理ポータルと VM ユーザーポータルのログインページで選択できる

ようになりました。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 (例: VM ユーザーポータルへのログイン) を割り当てるには、「[管理ポータルからのユーザー管理タスク](#)」を参照してください。



注記

詳しい情報は、`/usr/share/doc/ovirt-engine-extension-aaa-ldap-version` にある LDAP の認証/承認の拡張機能の README ファイルを参照してください。

15.3.3. 外部の LDAP プロバイダーの設定 (手動の設定)

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ーサーバーにアクセスし、完全にカスタマイズ可能です。VM ユーザーポータルまたは管理ポータルの機能でシングルサインオンを有効にしない限りは、Kerberos 認証は必要ありません。

前のセクションに記載した対話式的設定メソッドではユースケースの要件を十分に満たさない場合には、手動で設定ファイルを編集して、LDAP サーバーをアタッチすることができます。以下の手順は、一般的な例を示しています。実際の値は、お使いの環境に応じて異なります。

外部の LDAP プロバイダーの手動設定

1. Red Hat Virtualization Manager に LDAP 拡張機能の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、Active Directory 用 (**ad**) およびその他のディレクトリータイプ用 (**simple**) が用意されています。以下の例では、シンプル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 VM ユーザーポータルのログインページで表示されるプロファイル名と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 プロパティ設定ファイルを編集して、LDAP サーバーのタイプの箇所をコメント解除し、ドメインとパスワードのフィールドを更新します。

```
# vi /etc/ovirt-engine/aaa/example.properties
```

例15.1 プロファイル例: LDAP サーバーのセクション

```
# 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、その証明書を使用して公開鍵のキーストアファイルを作成します。以下の行をコメント解除して、公開鍵のキーストアファイルへの完全パスとその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

公開鍵のキーストアファイルについての詳しい情報は、[「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 プロファイル例: キーストアのセクション

```
# 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 VM ユーザーポータル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** で定義されます。プロファイルの設定ファイルの場所は、LDAP 設定ファイルの場所と一致する必要があります。全フィールドの値をデフォルトのままにすることも可能です。

```
# 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. 承認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。

```
# vi /etc/ovirt-engine/extensions.d/example-authz.properties
```

例15.4 承認設定ファイルの例

```
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
```

7. 設定プロファイルの所有権とパーミッションを適切に設定します。

```
# chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties
# chmod 600 /etc/ovirt-engine/aaa/example.properties
```

8. engine サービスを再起動します。

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

9. 作成した **example** プロファイルが管理ポータルと VM ユーザーポータルのログインページで選択できるようになりました。LDAP サーバー上のユーザーアカウントに適切なパーミッション (例: VM ユーザーポータルへのログイン) を付与するには、[「管理ポータルからのユーザー管理タスク」](#)を参照してください。



注記

詳しい情報は、`/usr/share/doc/ovirt-engine-extension-aaa-ldap-version`にあるLDAPの認証/承認の拡張機能のREADMEファイルを参照してください。

15.3.4. 外部の LDAP プロバイダーの削除

以下の手順では、設定した外部の LDAP プロバイダーおよびそのユーザーを削除する方法について説明します。

外部の LDAP プロバイダーの削除

1. LDAP プロバイダーの設定ファイルを削除します (デフォルトのプロファイル名 **profile1** を実際のプロファイル名に置き換えてください)。

```
# rm /etc/ovirt-engine/extensions.d/profile1-authn.properties
# rm /etc/ovirt-engine/extensions.d/profile1-authz.properties
# rm /etc/ovirt-engine/aaa/profile1.properties
```

2. **ovirt-engine** サービスを再起動します。

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

3. 管理ポータルユーザー リソースタブにおいて、このプロバイダーのユーザー (認証プロバイダーに **profile1-authz** と表示されているユーザー) を選択して **削除** をクリックします。

15.4. シングルサインオンのための LDAP と 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する必要なく、VM ユーザーポータルまたは管理ポータルにログインすることができます。認証情報は Kerberos サーバーから取得します。管理ポータルと VM ユーザーポータルにシングルサインオンを設定するには、拡張機能を 2 つ (**ovirt-engine-extension-aaa-misc** および **ovirt-engine-extension-aaa-ldap**) と、Apache モジュールを 2 つ (**mod_auth_gssapi** および **mod_session**) 設定する必要があります。Kerberos を必要としないシングルサインオンを設定することは可能ですが、本ガイドの対象範囲外となっています。



注記

VM ユーザーポータルへのシングルサインオンが有効になっている場合は、仮想マシンへのシングルサインオンは使用できません。VM ユーザーポータルへのシングルサインオンが有効な状態では、VM ユーザーポータルによるパスワードの確認が必要ないため、このパスワードが渡されず、仮想マシンにサインインできません。

この例は、以下を前提としています。

- 既存のキー配布センター (KDC) サーバーは Kerberos 5 の MIT バージョンを使用すること。
- KDC サーバーの管理者権限があること。
- Red Hat Virtualization Manager およびユーザーのマシンに Kerberos クライアントがインストール済みであること。
- Kerberos のサービスプリンシパルおよび **keytab** ファイルの作成に **kadmin** ユーティリティーが使用されること。

この手順には以下のコンポーネントが必要となります。

KDC サーバー

- Red Hat Virtualization Manager 上の Apache サービス用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

- 認証および承認拡張機能のパッケージと 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。

Apache サービス用の Kerberos の設定

1. KDC サーバーで、**kadmin** ユーティリティを使用して Red Hat Virtualization Manager 上の Apache サービス用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とは、Apache サービス用の KDC に対するリファレンス ID です。

```
# kadmin
kadmin> addprinc -randkey HTTP/fqdn-of-rhevm@REALM.COM
```

2. Apache サービス用に **keytab** ファイルを作成します。**keytab** ファイルに共有秘密鍵が保管されます。

```
kadmin> ktadd -k /tmp/http.keytab HTTP/fqdn-of-rhevm@REALM.COM
kadmin> quit
```

3. 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
```

VM ユーザーポータルまたは管理ポータルへのシングルサインオンの設定

1. Red Hat Virtualization Manager で、keytab の所有権とパーミッションを適切に設定します。

```
# chown apache /etc/httpd/http.keytab
# chmod 400 /etc/httpd/http.keytab
```

2. 認証拡張機能のパッケージ、LDAP 拡張機能のパッケージ、および **mod_auth_gssapi** と **mod_session** の Apache 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
```

3. 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 用 (**ad-ssso**) およびその他のディレクトリータイプ用 (**simple-ssso**) が用意されています。以下の例では、シンプル 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-ssso/. /etc/ovirt-engine
```

4. **ovirt-ssso.conf** を Apache の設定ディレクトリーに移動します。

```
# mv /etc/ovirt-engine/aaa/ovirt-ssso.conf /etc/httpd/conf.d
```

5. 認証メソッドファイルを確認します。レルムは自動的に **keytab** ファイルから取得されるので、このファイルは編集する必要はありません。

```
# vi /etc/httpd/conf.d/ovirt-ssso.conf
```

例15.5 認証メソッドファイルの例

■

```
<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 VM ユーザーポータルのログインページで表示されるプロフィール名と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 プロパティ設定ファイルを編集して、LDAP サーバーのタイプの箇所をコメント解除し、ドメインとパスワードのフィールドを更新します。

```
# vi /etc/ovirt-engine/aaa/example.properties
```

例15.6 プロファイル例: LDAP サーバーのセクション

```
# 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、その証明書を使用して公開鍵のキーストアファイルを作成します。以下の行をコメント解除して、公開鍵のキーストアファイルへの完全パスとその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

公開鍵のキーストアファイルについての詳しい情報は、[「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 プロファイル例: キーストアのセクション

```
# 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 VM ユーザーポータル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** で定義されます。プロファイルの設定ファイルの場所は、LDAP 設定ファイルの場所と一致する必要があります。全フィールドの値をデフォルトのままにすることも可能です。

```
# 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 =
```


11. 設定ファイルの所有権とパーミッションを適切に設定します。

```
# chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties

# chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-http-
authn.properties

# chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-http-
mapping.properties

# chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-
authz.properties

# chmod 600 /etc/ovirt-engine/aaa/example.properties

# chmod 640 /etc/ovirt-engine/extensions.d/example-http-
authn.properties

# chmod 640 /etc/ovirt-engine/extensions.d/example-http-
mapping.properties

# chmod 640 /etc/ovirt-engine/extensions.d/example-authz.properties
```

12. Apache サービスと **ovirt-engine** サービスを再起動します。

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

15.5. ユーザー認証

15.5.1. ユーザー承認モデル

Red Hat Virtualization は、以下にあげる 3 つの要素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
- 実行するアクションのタイプ
- アクションの対象となるオブジェクト

15.5.2. ユーザーアクション

ユーザー が確実にアクションを実行するには、そのアクションの対象となる オブジェクト に対する適切な パーミッション が必要です。アクションのタイプには、それぞれ対応する パーミッション が存在します。

一部のアクションは、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、テンプレートとコピー先のストレージドメインの両方に影響を及ぼします。アクションを実行するユーザーには、そのアクションが影響を及ぼすすべてのオブジェクトに対する適切なパーミッションが必要です。

15.6. 管理ポータルからのユーザー管理タスク

15.6.1. ユーザーの追加および VM ユーザーポータルパーミッションの割り当て

ユーザーにロールとパーミッションを割り当てる前には、そのユーザーを予め作成しておく必要があります。以下の手順で割り当てるロールとパーミッションにより、ユーザーは VM ユーザーポータルにログインして仮想マシンを作成することができ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することができます。

ユーザーの追加および VM ユーザーポータルパーミッションの割り当て

1. ヘッダーバーで **管理** → **設定** をクリックして **設定** ウィンドウを開きます。
2. **システム権限** をクリックします。
3. **追加** をクリックすると、**ユーザーへのシステム権限の追加** ウィンドウが開きます。
4. **検索** 下のプロファイルを選択します。このプロファイルが検索対象のドメインです。検索テキストフィールドに名前またはその一部を入力して **検索** をクリックします。もしくは、**検索** をクリックして、全ユーザーとグループの一覧を表示します。
5. 対象となるユーザーまたはグループのチェックボックスにチェックを入れます。
6. **割り当てるロール** から割り当てる適切なロールを選択します。**UserRole** ロールは VM ユーザーポータルにログインするためのパーミッションをアカウントに付与します。
7. **OK** をクリックします。

VM ユーザーポータルにログインして、そのユーザーアカウントにログインのパーミッションが付与されていることを確認します。

15.6.2. ユーザー情報の確認

ユーザー情報の確認

1. **管理** → **ユーザー** をクリックし、認証済みのユーザー一覧を表示します。
2. ユーザー名をクリックして詳細ビューを表示します。通常、そのユーザーのドメイン名、メールアドレス、ステータスなどの全般情報が表示される **全般** タブが選択されます。
3. その他のタブでは、ユーザーのグループやパーミッション、クォータ、イベントを表示することができます。

たとえば、ユーザーが属するグループを表示するには、**ディレクトリーグループ** タブをクリックします。

15.6.3. リソースに対する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に対するパーミッションを割り当てることができます。各リソースに対するパーミッションが割り当てられたユーザーを表示することができます。

リソースに対するユーザーパーミッションの表示

1. リソースを特定し、その名前をクリックして詳細ビューを表示します。

2. パーミッション タブをクリックして、選択したリソースに割り当てられたユーザー、ユーザーのロール、継承されたパーミッションを一覧表示します。

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場合には、Red Hat Virtualization から削除してください。

ユーザーの削除

1. **管理** → **ユーザー** をクリックし、認証済みのユーザー一覧を表示します。
2. 削除するユーザーを選択します。その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。
3. **削除** をクリックして、**OK** をクリックします。

ユーザーが Red Hat Virtualization から削除されましたが、外部のディレクトリーからは削除されていません。

15.6.5. ログイン中のユーザーの確認

セッション時間およびその他の情報と共に、現在ログイン中のユーザーを確認することができます。**管理** → **アクティブなユーザーセッション** をクリックすると、ログイン中の各ユーザーの **セッション DB ID**、**ユーザー名**、**認証プロバイダー**、**ユーザー ID**、**ソース IP アドレス**、**セッション開始時刻**、および最後にセッションがアクティブだった時刻が表示されます。

15.6.6. ユーザーセッションの終了

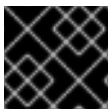
ログイン中のユーザーのセッションを終了することができます。

ユーザーセッションの終了

1. **管理** → **アクティブなユーザーセッション** をクリックします。
2. 終了するユーザーセッションを選択します。
3. **セッションの終了** をクリックします。
4. **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管理タスク

内部ドメイン上のユーザーアカウントを管理するには、**ovirt-aaa-jdbc-tool** ツールを使用することができます。このツールを使用して変更を加えると、その内容は直ちに有効になり、**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全リストは、**ovirt-aaa-jdbc-tool user --help** コマンドを実行すると確認できます。本セクションには、一般的な例を記載します。



重要

Manager マシンにログインしている必要があります。

15.7.1. 新規ユーザーの作成

新規ユーザーアカウントを作成することができます。オプションの **--attribute** コマンドを使用してアカウントの詳細を指定します。オプションの全リストは、**ovirt-aaa-jdbc-tool user add --help** のコマンドを実行すると表示されます。

```
# ovirt-aaa-jdbc-tool user add test1 --attribute=firstName=John --
attribute=lastName=Doe
adding user test1...
user added successfully
```

新規作成したユーザーを管理ポータルに追加し、そのユーザーに適切なロールとパーミッションを割り当てることができます。詳しい説明は、[「ユーザーの追加および VM 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。

15.7.2. ユーザーパスワードの設定

パスワードを作成することができます。**--password-valid-to** を設定する必要があります。設定しなかった場合には、パスワードの有効期限がデフォルトで現在の時刻に設定されてしまいます。日付/時刻の形式は **yyyy-MM-dd HH:mm:ssX** です。以下の例の **-0800** は GMT マイナス 8 時間を意味します。その他のオプションを確認するには、**ovirt-aaa-jdbc-tool user password-reset --help** コマンド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、内部ドメイン上のユーザーアカウント用のパスワードポリシーには、以下のような制限があります。

- 最小 6 文字
- パスワード変更時には、3 回前までに使用したパスワードは使用できません。

パスワードポリシーおよびその他のデフォルト設定に関する詳しい情報は、**ovirt-aaa-jdbc-tool settings show** のコマンドを実行すると確認できます。

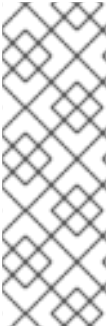
15.7.3. ユーザータイムアウトの設定

ユーザーセッションがタイムアウトになる期限を設定することができます。

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

15.7.4. ユーザーパスワードの事前暗号化

ovirt-engine-crypto-tool スクリプトを使用して、予め暗号化されたユーザーパスワードを作成することができます。このオプションは、スクリプトを使用してデータベースにユーザーおよびパスワードを追加する際に役立ちます。



注記

パスワードは、暗号化された状態で Manager データベースに保管されます。すべてのパスワードを同じアルゴリズムで暗号化するため、**ovirt-engine-crypto-tool** スクリプトが使用されます。

パスワードが予め暗号化されている場合は、パスワードの妥当性テストを実施することができません。パスワードの妥当性ポリシーを満たしていなくても、パスワードは受け入れられます。

1. 以下のコマンドを実行します。

```
# /usr/share/ovirt-engine/bin/ovirt-engine-crypto-tool.sh pbe-encode
```

スクリプトによりパスワードの入力が求められます。

あるいは、**--password-file=[file]** オプションを使用して、このオプションで指定するファイルの最初の行に表示されるパスワードだけを暗号化することができます。

```
# /usr/share/ovirt-engine/bin/ovirt-engine-crypto-tool.sh pbe-encode  
--password=file:file
```

2. **--encrypted** オプションと共に **ovirt-aaa-jdbc-tool** スクリプトを使用して、新しいパスワードを設定します。

```
# ovirt-aaa-jdbc-tool user password-reset test1 --password-valid-  
to="2025-08-01 12:00:00-0800" --encrypted
```

3. 暗号化されたパスワードを入力し、確認します。

```
Password:  
Reenter password:  
updating user test1...  
user updated successfully
```

15.7.5. ユーザー情報の確認

詳細なユーザーアカウント情報を確認することができます。

```
# ovirt-aaa-jdbc-tool user show test1
```

このコマンドにより、管理ポータルで **管理** → **ユーザー** 画面よりも詳しい情報が表示されます。

15.7.6. ユーザー情報の編集

メールアドレス等のユーザー情報を更新することができます。

```
# ovirt-aaa-jdbc-tool user edit test1 --attribute=email=jdoe@example.com
```

15.7.7. ユーザーの削除

ユーザーアカウントを削除することができます。

```
# ovirt-aaa-jdbc-tool user delete test1
```

管理ポータルからユーザーを削除します。詳しい説明は、[「ユーザーの削除」](#)を参照してください。

15.7.8. 内部管理ユーザーの無効化

engine-setup 実行中に作成された **admin@internal** ユーザーを含むローカルドメイン上のユーザーを無効にすることができます。デフォルトの **admin** ユーザーを無効にする前には、完全な管理権限を持つユーザーが環境内に少なくとも 1 人いることを確認してください。

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** ロールが割り当てられたユーザーが、環境にもう 1 人追加されていることを確認します。詳しい説明は、[「ユーザーの追加および VM 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。
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** のコマンドを実行します。

15.7.9. グループの管理

内部ドメイン上のグループアカウントを管理するには、**ovirt-aaa-jdbc-tool** ツールを使用することができます。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と似ています。グループのオプションの全一覧は、**ovirt-aaa-jdbc-tool group --help** のコマンドを実行すると確認できます。本セクションには、一般的な例を記載します。

グループの作成

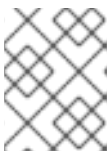
以下の手順では、グループアカウントを作成して、ユーザーをそのグループに追加し、そのグループの情報を表示する方法について説明します。

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. 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。ユーザーは予め作成しておく必要があります。

```
# ovirt-aaa-jdbc-tool group-manage useradd group1 --user=test1
```



注記

group-manage オプションの全一覧は、**ovirt-aaa-jdbc-tool group-manage --help** コマンドを実行すると確認できます。

4. グループアカウントの情報を表示します。

```
# ovirt-aaa-jdbc-tool group show group1
```

5. 新規作成したグループを管理ポータルで追加し、そのグループに適切なロールとパーミッションを割り当てます。このグループのユーザーは、グループのロールとパーミッションを継承します。詳しい説明は、[「ユーザーの追加および VM 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。

ネストされたグループの作成

以下の手順では、グループ内にグループを作成する方法について説明します。

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. 第 1 のグループを作成します。

```
# ovirt-aaa-jdbc-tool group add group1
```

3. 第 2 のグループを作成します。

```
# ovirt-aaa-jdbc-tool group add group1-1
```

4. 第 2 のグループを第 1 のグループに追加します。

```
# ovirt-aaa-jdbc-tool group-manage groupadd group1 --group=group1-1
```

5. 第 1 のグループを管理ポータルに追加し、そのグループに適切なロールとパーミッションを割り当てます。詳しい説明は、[「ユーザーの追加および VM 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。

15.7.10. ユーザーとグループのクエリー

query モジュールにより、ユーザーおよびグループの情報を照会することができます。オプションの全リストは、**ovirt-aaa-jdbc-tool query --help** のコマンドを実行すると確認できます。

全ユーザー/グループアカウント情報の一覧表示

以下の手順では、全アカウント情報を一覧表示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. アカウントの情報を一覧表示します。

- 全ユーザーアカウントの情報:

```
# ovirt-aaa-jdbc-tool query --what=user
```

- 全グループアカウントの情報:

```
# ovirt-aaa-jdbc-tool query --what=group
```

フィルタリングしたアカウント情報の一覧表示

以下の手順は、アカウント情報を一覧表示する際にフィルターを適用する方法について説明します。

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. **--pattern** パラメーターを使用して、アカウント情報を絞り込みます。

- 名前が「j」で始まるユーザーアカウントの情報を一覧表示します。

```
# ovirt-aaa-jdbc-tool query --what=user --pattern="name=j*"
```

- 部署の属性が **marketing** に設定されたグループを一覧表示します。

```
# ovirt-aaa-jdbc-tool query --what=group --
pattern="department=marketing"
```

15.7.11. 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** の **settings** モジュールを使用します。

アカウント設定の更新

以下の手順では、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、利用可能な全設定を確認します。

```
# ovirt-aaa-jdbc-tool setting show
```

3. 必要な設定を変更します。

- 以下の例は、全ユーザー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
```

- 以下の例では、ユーザーが実行可能なログインの最大試行回数を更新します。失敗回数がこの値を超えた場合には、ユーザーアカウントがロックされます。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

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** コマンドを実行してください。

15.8. 追加のローカルドメインの設定

デフォルトの **internal** ドメイン以外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することが可能で、外部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することができます。ただし、このユースケースは、エンタープライズ環境では一般的ではないかもしれません。

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は自動的にアップグレードされないため、今後リリースがある度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そのドメインをアップグレードする方法についての詳しい説明は、**/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 クォータと SERVICE LEVEL AGREEMENT のポリシー

16.1. クォータについて

クォータとは、Red Hat Virtualization の提供するリソース制限ツールです。クォータは、ユーザーパーミッションによって設定される制限層の上部にある制限層と考えることができます。

クォータはデータセンターのオブジェクトです。

クォータにより、Red Hat Virtualization 環境の管理者はメモリー、CPU、ストレージへのユーザーアクセスを制限できます。クォータは、管理者がユーザーに割り当て可能なメモリーリソースやストレージリソースを定義します。これにより、ユーザーは、割り当てられたリソースのみ使用することができます。ユーザーがクォータリソースを使い切ると、Red Hat Virtualization Manager はそれ以降のユーザーアクションを拒否します。

クォータには 2 種類あります。

表16.1 異なる 2 種類のクォータ

クォータタイプ	定義
ランタイムクォータ	このクォータは、CPU や メモリーなどのランタイムリソースの消費を制限します。
ストレージクォータ	このクォータは、使用可能なストレージ容量を制限します。

クォータには、SELinux と同様に 3 つのモードがあります。

表16.2 クォータのモード

クォータのモード	機能
有効	このモードは、監査モードでテストしたクォータを有効にし、クォータの影響を受けるグループまたはユーザーに対するリソースを制限します。
監査	このモードでは、クォータ違反があった場合にそれをログに記録しますが、実際にユーザーアクションが拒否されることはなく、クォータのテストに使用することができます。監査モードでは、クォータの影響を受けるユーザーに割り当てられるランタイムクォータの量やストレージクォータの量を増減することができます。
無効	このモードは、クォータにより定義されたランタイムおよびストレージの制限を無効にします。

ユーザーが仮想マシンの実行を試みると、その仮想マシンの仕様は、該当するクォータで設定されているストレージ上限およびランタイム上限と比較されます。

仮想マシンを起動することによって、クォータが適用される実行中の全仮想マシンのリソースの総計がクォータで定義されている上限を超えてしまう場合には、Manager が仮想マシンの実行を拒否します。

ユーザーが新規ディスクを作成すると、適用されるクォータの対象となるその他の全ディスクのディスク使用量総計に要求されたディスクサイズが追加されます。新規ディスクに、クォータで許可されている容量を超えるディスク使用量総計が必要な場合には、ディスクの作成が失敗します。

クォータにより、同じハードウェアのリソースを共有することができます。クォータはハードおよびソフトの閾値をサポートしています。管理者は、クォータを使用してリソースの閾値を設定することができます。これらの閾値は、ユーザー側から見ると、そのリソースの 100% の使用率として表示されます。この閾値を不意に超過して障害が発生しないようにするために、インターフェースは「猶予」の容量をサポートしており、閾値を多少超過できるようになっています。閾値を超過するとそのユーザーに警告が送信されます。

重要

クォータは、仮想マシンの実行に制限を課します。これらの制限を無視すると、仮想マシンや仮想ディスクが使えなくなってしまうような事態が発生する可能性があります。

クォータが有効モードで実行されている場合には、クォータが割り当てられていない仮想マシンおよびディスクは使用することができません。

仮想マシンの電源を入れるには、その仮想マシンにクォータが割り当てられている必要があります。

仮想マシンのスナップショットを作成するには、その仮想マシンに関連付けられた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。

テンプレートの作成時には、テンプレートが使用するクォータを選択するように要求されます。これにより、テンプレート (およびそのテンプレートから将来作成されるすべての仮想マシン) が、テンプレートの元となっている仮想マシンおよびディスクとは異なるクォータを使用するように設定することができます。

16.2. 共有クォータおよび個別に定義されたクォータ

SuperUser のパーミッションを持つユーザーは、個別のユーザー用のクォータまたはグループ用のクォータを作成することができます。

グループクォータは Active Directory のユーザーに設定することができます。10 人のユーザーで構成されるグループに 1 TB のクォータが割り当てられて、その 10 人のユーザーの 1 人がその 1 TB をすべて使い切った場合には、グループ全体がクォータ超過となり、そのグループに関連付けられたストレージは 10 人のユーザーのどれも使用できなくなります。

個別のユーザー用のクォータは個人にのみ設定可能です。個人ユーザーが割り当てられた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、そのユーザーはクォータ超過となり、自分のクォータに関連付けられている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

コンシューマーまたはリソースにクォータが割り当てられると、そのコンシューマーによるアクションまたはストレージ/vCPU/メモリーに関連したリソースに対するアクションを実行するたびに、クォータの消費またはクォータの解放が生じます。

クォータは、ユーザーによるリソースへのアクセスの上限の役割を果たすので、クォータの計算は、ユーザーによる現在の実使用量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、拡張可能な最大容量を算出します。

例16.1 アカウンティングの例

ユーザーは vCPU が 1 基、メモリーが 1024 MB の仮想マシンを実行しています。そのアクションにより、ユーザーに割り当てられた vCPU 1 基と 1024 MB のクォータが消費されます。仮想マシンが停止すると、vCPU 1 基と 1024 MB の RAM が解放されて、ユーザーに割り当てられたクォータに戻ります。ランタイムのクォータ消費は、コンシューマーの実際のランタイム中にのみ計算されません。

ユーザーが 10 GB のシンプロビジョニング仮想ディスクを作成します。ディスクの実使用量には、そのディスクの 3 GB のみが実際に使用中と表示される可能性があります。クォータの消費は、そのディスクが拡張可能な最大容量である 10 GB となります。

16.4. データセンターのクォータの有効化/モードの変更

このセクションでは、データセンターのクォータの有効化とモード変更の手順について説明します。クォータを定義するには、クォータモードを選択しておく必要があります。以下の手順に従って作業を実行するには、管理ポータルにログインしてください。

設定したクォータをテストして予想どおりに機能していることを確認するには、**監査** モードを使用します。クォータの作成/変更時は、クォータを **監査** モードにする必要はありません。

データセンターのクォータの有効化/モードの変更

1. **コンピュー**ト → **データセンター** をクリックし、データセンターを選択します。
2. **編集** をクリックします。
3. **クォータモード** ドロップダウンリストで、クォータモードを **有効** に変更します。
4. **OK** をクリックします。

テスト中にクォータモードを **監査** に設定した場合には、**有効** に変更して、クォータの設定を有効にする必要があります。

16.5. 新規クォータポリシーの作成

監査または有効モードでクォータを有効にしました。次にクォータポリシーを定義してデータセンターのリソース使用率を管理します。

新規クォータポリシーの作成

1. **管理** → **クォータ** をクリックします。
2. **追加** をクリックします。
3. **名前** と **説明** フィールドに値を入力します。
4. **データセンター** を選択します。
5. **メモリー & CPU** セクションにある緑のスライダーを使用して、**クラスターの閾値** を設定します。

6. **メモリー & CPU** セクションにある青のスライダーを使用して、**クラスターの猶予** を設定します。
7. **すべてのクラスター** または **特定のクラスター** のラジオボタンをクリックします。**特定のクラスター** を選択した場合には、クォータポリシーを適用するクラスターのチェックボックスを選択してください。
8. **編集** をクリックすると、**クォータの編集** ウィンドウが開きます。
 - a. **メモリー** フィールドの **無制限** ラジオボタン (クラスター内でメモリーリソースを無制限に使用可能にする) を選択するか、**上限** ラジオボタンを選択してこのクォータで設定するメモリー容量を指定します。**上限** ラジオボタンを選択した場合には、**MB** フィールドにメモリークォータをメガバイト (MB) 単位で入力します。
 - b. **CPU** フィールドの **無制限** ラジオボタンを選択するか、**上限** ラジオボタンを選択してこのクォータで設定する CPU の数を指定します。**上限** ラジオボタンを選択した場合には、**vCPU** フィールドに仮想 CPU の数を入力します。
 - c. **クォータの編集** ウィンドウで **OK** をクリックします。
9. **ストレージ** セクションにある緑のスライダーを使用して、**ストレージの閾値** を設定します。
10. **ストレージ** セクションにある青のスライダーを使用して、**ストレージの猶予** を設定します。
11. **すべてのストレージドメイン** または **特定のストレージドメイン** のラジオボタンをクリックします。**特定のストレージドメイン** を選択した場合には、クォータポリシーを適用するストレージドメインのチェックボックスを選択してください。
12. **編集** をクリックすると、**クォータの編集** ウィンドウが開きます。
 - a. **ストレージクォータ** フィールドの **無制限** ラジオボタン (ストレージを無制限に使用可能にする) を選択するか、**上限** ラジオボタンを選択してクォータがユーザーに制限を課すストレージ容量を設定します。**上限** ラジオボタンを選択した場合には、**GB** フィールドにストレージクォータをギガバイト (GB) 単位で入力します。
 - b. **クォータの編集** ウィンドウで **OK** をクリックします。
13. **新規クォータ** ウィンドウで **OK** をクリックします。

16.6. クォータの閾値設定

表16.3 クォータの閾値と猶予の設定

設定	定義
クラスターの閾値	1 つのデータセンターで使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閾値を超えた後にデータセンターが使用可能なクラスターリソースの量
ストレージの閾値	1 つのデータセンターで使用可能なストレージリソースの容量

設定	定義
ストレージの猶予	データセンターのストレージ閾値を超えた後にデータセンターが使用可能なストレージの容量

クォータが 100 GB、猶予 20% と設定されている場合には、ストレージ消費量が 120 GB に達すると、コンシューマーはそのストレージを使用できなくなります。同じクォータに 70% の閾値が設定されている場合には、ストレージの消費量が 70 GB を超えると、コンシューマーは警告を受け取ります (ただし、ストレージ消費量が 120 GB になるまでそのままストレージを使用することができます)。「閾値」は、その値を超えると警告が出される「ソフトリミット」、「猶予」は、その値を超えるとそれ以上ストレージリソースを消費できない「ハードリミット」と考えることができます。

16.7. オブジェクトへのクォータ割り当て

仮想マシンへのクォータ割り当て

1. **コンピュー**ト → **仮想マシン** をクリックして仮想マシンを選択します。
2. **編集** をクリックします。
3. **クォータ** のドロップダウンリストから、その仮想マシンが消費するクォータを選択します。
4. **OK** をクリックします。

仮想ディスクへのクォータ割り当て

1. **コンピュー**ト → **仮想マシン** をクリックします。
2. 仮想マシンの名前をクリックし、詳細ビューを表示します。
3. **ディスク** タブをクリックし、クォータに関連付けるディスクを選択します。
4. **編集** をクリックします。
5. **クォータ** のドロップダウンリストから、その仮想ディスクが消費するクォータを選択します。
6. **OK** をクリックします。



重要

仮想マシンが正常に機能するためには、仮想マシンに関連付けられた全オブジェクトにクォ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たオブジェクトにクォータを選択しなかった場合には、仮想マシンは正常に機能しません。このような場合に表示されるエラーは一般的な内容であるため、仮想マシンに関連付けられた全オブジェクトにクォータに関連付けなかったことが原因でエラーメッセージが表示されたと判断するのは困難となります。クォ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は作成できません。また、仮想ディスクにクォータが割り当てられていない仮想マシンからテンプレートを作成することも不可能です。

16.8. クォータを使用したユーザー別のリソース制限

以下の手順は、クォータを使用してユーザーがアクセス可能なリソースを制限する方法を説明します。

クォータへのユーザー割り当て

1. **管理** → **クォータ** をクリックします。
2. 対象のクォータの名前をクリックし、詳細ビューを表示します。
3. **コンシューマー** タブをクリックします。
4. **追加** をクリックします。
5. **検索** フィールドで、クォータに関連付けるユーザー名を入力します。
6. **検索** をクリックします。
7. ユーザー名の横にあるチェックボックスを選択します。
8. **OK** をクリックします。

しばらくすると、詳細ビューの **コンシューマー** のタブにユーザーが表示されます。

16.9. クォータの編集

以下の手順では、既存のクォータを変更する方法について説明します。

クォータの編集

1. **管理** → **クォータ** をクリックし、クォータを選択します。
2. **編集** をクリックします。
3. 必要に応じて、フィールドを編集します。
4. **OK** をクリックします。

16.10. クォータの削除

以下の手順では、クォータを削除する方法について説明します。

クォータの削除

1. **管理** → **クォータ** をクリックし、クォータを選択します。
2. **削除** をクリックします。
3. **OK** をクリックします。

16.11. SERVICE LEVEL AGREEMENT ポリシーの有効化

この手順では、service level agreement CPU ポリシー機能の設定方法について説明します。

service level agreement CPU ポリシーの設定

1. **コンピュー**ト → **仮想マシン** をクリックします。
2. **新規作成** をクリックするか、仮想マシンを選択して **編集** をクリックします。
3. **リソースの割り当て** タブをクリックします。

4. **CPU シェア** を指定します。設定可能なオプションには、**低**、**中**、**高**、**カスタム**、および **無効** があります。**高** に設定された仮想マシンへの割り当ては、**中** に設定された仮想マシンの 2 倍となります。また、**中** に設定された仮想マシンへの割り当ては、**低** に設定された仮想マシンの 2 倍となります。**無効** を指定すると、VDSM がシェアの割り当てを決定する旧アルゴリズムを使用するように指示します。このような条件下において割り当てられるシェア数は通常 1020 です。

ユーザーの CPU 消費が、設定したポリシーによって管理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

Red Hat Virtualization Manager が管理する環境内で特定のイベントが発生した場合には、Red Hat Virtualization Manager は指定したユーザーにメールで通知することができます。この機能を使用するには、メール転送エージェントを設定する必要があります。管理ポータルで設定できるのは、メール通知のみです。Manager のマシンで、SNMP トラップを設定する必要があります。

イベント通知の設定

1. RHVM から自動メッセージを受け取りそれを配信リストに配信することのできるメールサーバーにアクセスする必要があります。
2. **ユーザー** リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から、イベント通知の送信先となるユーザーを選択します。
3. **イベント通知機能** タブをクリックすると、ユーザーが通知を受けるイベントが表示されます。そのユーザーにイベント通知を設定していない場合には、この一覧は空欄となります。
4. **イベントを管理** をクリックします。
5. **すべてを展開** ボタンまたはカテゴリー別の展開ボタンを使用してイベントを表示します。
6. 該当するチェックボックスを選択します。
7. **メール受信者** のフィールドに電子メールアドレスを入力します。
8. **OK** をクリックします。
9. Manager マシンにおいて、**ovirt-engine-notifier.conf** をコピーし **90-email-notify.conf** という名前の新規ファイルとして保存します。

```
# cp /usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf /etc/ovirt-engine/notifier/notifier.conf.d/90-email-notify.conf
```

10. **90-email-notify.conf** を編集し、**EMAIL Notifications** セクション以外はすべて削除します。
11. 以下に示す例のように、正しい電子メールの変数を入力します。このファイルは、もとの **ovirt-engine-notifier.conf** ファイルの値に優先します。

```
-----
# EMAIL Notifications #
-----

# The SMTP mail server address. Required.
MAIL_SERVER=myemailserver.example.com

# The SMTP port (usually 25 for plain SMTP, 465 for SMTP with SSL,
587 for SMTP with TLS)
MAIL_PORT=25

# Required if SSL or TLS enabled to authenticate the user. Used also
```

```

to specify 'from' user address if mail server
# supports, when MAIL_FROM is not set. Address is in RFC822 format
MAIL_USER=

# Required to authenticate the user if mail server requires
authentication or if SSL or TLS is enabled
SENSITIVE_KEYS="${SENSITIVE_KEYS},MAIL_PASSWORD"
MAIL_PASSWORD=

# Indicates type of encryption (none, ssl or tls) should be used to
communicate with mail server.
MAIL_SMTP_ENCRYPTION=none

# If set to true, sends a message in HTML format.
HTML_MESSAGE_FORMAT=false

# Specifies 'from' address on sent mail in RFC822 format, if
supported by mail server.
MAIL_FROM=rhev2017@example.com

# Specifies 'reply-to' address on sent mail in RFC822 format.
MAIL_REPLY_TO=

# Interval to send smtp messages per # of IDLE_INTERVAL
MAIL_SEND_INTERVAL=1

# Amount of times to attempt sending an email before failing.
MAIL_RETRIES=4

```



注記

他のオプションについては、`/etc/ovirt-engine/notifier/notifier.conf.d/README` を参照してください。

12. **ovirt-engine-notifier** サービスを有効化および再起動すると、変更した内容が有効になります。

```

# systemctl daemon-reload
# systemctl enable ovirt-engine-notifier.service
# systemctl restart ovirt-engine-notifier.service

```

Red Hat Virtualization 環境のイベントに基づいて、指定したユーザーに電子メールが送信され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 **イベント通知機能** 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

ユーザーに不要なメール通知が設定されている場合には、その通知をキャンセルすることができます。

イベント通知のキャンセル

1. **管理** → **ユーザー** をクリックします。
2. ユーザーの **ユーザー名** をクリックし、詳細ビューを表示します。

3. **イベント通知機能** タブをクリックすると、ユーザーがメール通知を受けるイベントが表示されます。
4. **イベントを管理** をクリックします。
5. **すべてを展開** ボタンまたはカテゴリー別の展開ボタンを使用してイベントを表示します。
6. イベント通知を削除するには、該当するチェックボックスのチェックを外します。
7. **OK** をクリックします。

17.3. OVIRT-ENGINE-NOTIFIER.CONF 内のイベント通知パラメーター

イベント通知機能の設定ファイルは `/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf` に配置されています。

表17.1 ovirt-engine-notifier.conf の変数

変数名	デフォルト	備考
SENSITIVE_KEYS	なし	ログ記録されないキーのコンマ区切りリスト
JBOSS_HOME	<code>/opt/rh/eap7/root/usr/share/wildfly</code>	Manager が使用する JBoss application server の場所
ENGINE_ETC	<code>/etc/ovirt-engine</code>	Manager が使用する etc ディレクトリーの場所
ENGINE_LOG	<code>/var/log/ovirt-engine</code>	Manager が使用する logs ディレクトリーの場所
ENGINE_USR	<code>/usr/share/ovirt-engine</code>	Manager が使用する usr ディレクトリーの場所
ENGINE_JAVA_MODULEPATH	<code>\${ENGINE_USR}/modules</code>	JBoss モジュールを追加するファイルパス
NOTIFIER_DEBUG_ADDRESS	なし	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の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になる時間 (秒単位)
NOTIFIER_STOP_INTERVAL	1	タイムアウトカウンターがインクリメントされる時間 (秒単位)
INTERVAL_IN_SECONDS	120	サブスクライバーにメッセージをディスパッチするインスタンスの間隔 (秒単位)

変数名	デフォルト	備考
IDLE_INTERVAL	30	優先度の低いタスクが実行される間隔 (秒単位)
DAYS_TO_KEEP_HISTORY	0	ディスパッチされたイベントが履歴テーブルに保管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には、イベントは履歴テーブルに無期限に保持されます。
FAILED_QUERIES_NOTIFICATION_THRESHOLD	30	通知メールが送信されるまでの失敗クエリーの数。通知メールは、最初の失敗の後に送信されて通知をフェッチした後、この変数によって指定した失敗の回数に達するごとに 1 回送信されます。値を 0 または 1 に指定すると、失敗のたびにメールが送信されるようになります。
FAILED_QUERIES_NOTIFICATION_RECIPIENTS	なし	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。このエントリーは、 FILTER の変数によって非推奨となりました。
DAYS_TO_SEND_ON_STARTUP	0	通知機能の起動時に、この日数内の旧イベントが処理/送信されます。
FILTER	exclude:*	メール通知のトリガーと受信者を決定するのに使用されるアルゴリズム。この変数の値は、 include/exclude 、イベント、および受信者で構成されます (例: include:VDC_START(smtp:mail@example.com)\${FILTER})。
MAIL_SERVER	なし	SMTP メールサーバーのアドレス。必須。
MAIL_PORT	25	通信に使用するポート。設定可能な値には、プレーンの SMTP 用の 25 、SSL を使用した SMTP 用の 465 、および TLS を使用した SMTP 用の 587 が含まれます。

変数名	デフォルト	備考
MAIL_USER	なし	ユーザー認証のために SSL が有効化されている場合は、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「送信元」ユーザーのアドレスを指定するのにも使用します。一部のメールサーバーはこの機能をサポートしていません。アドレスは RFC822 の形式です。
SENSITIVE_KEYS	\${SENSITIVE_KEYS},MAIL_PASSWORD	メールサーバーで認証が必要な場合には、もしくは SSL または TLS が有効化されている場合にユーザーの認証に必要です。
MAIL_PASSWORD	なし	メールサーバーで認証が必要な場合には、もしくは SSL または TLS が有効化されている場合にユーザーの認証に必要です。
MAIL_SMTP_ENCRYPTION	なし	通信に使用する暗号化のタイプ。設定可能な値は 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には、メールサーバーはメッセージを HTML 形式で送信します。
MAIL_FROM	なし	この変数は、送信者のアドレスを RFC822 形式で指定します (メールサーバーが対応している場合)。
MAIL_REPLY_TO	なし	この変数は、送信されたメールに対する返信先アドレスを RFC822 形式で指定します (メールサーバーが対応している場合)。
MAIL_SEND_INTERVAL	1	各 IDLE_INTERVAL に送信される SMTP メッセージの数
MAIL_RETRIES	4	メール送信の試行回数。この数を超えるとエラーとなります。

変数名	デフォルト	備考
SNMP_MANAGER	なし	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、ポート番号を入れることが可能です (例: manager1.example.com manager2.example.com:164)。
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	アラート用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、全トラップタイプが送信され、イベント情報とともに SNMP マネージャーに追記されます。デフォルトのトラップを変更すると、生成されるトラップが Manager の管理情報ベースに準拠しなくなる点に注意してください。
ENGINE_INTERVAL_IN_SECONDS	300	Manager がインストールされているマシンのモニタリング間隔。この間隔は、モニタリングが完了した時点から計測されます。
ENGINE_MONITOR_RETRIES	3	エラー発生後に通知機能が所定の間隔で Manager がインストールされているマシンのステータスのモニタリングを試みる回数
ENGINE_TIMEOUT_IN_SECONDS	30	エラー発生後に通知機能が所定の間隔で Manager がインストールされているマシンのステータスのモニタリングを試みるまでの待ち時間 (秒単位)
IS_HTTPS_PROTOCOL	false	JBoss がセキュアなモードで実行されている場合には、この値は true に設定する必要があります。
SSL_PROTOCOL	TLS	SSL が有効化されている場合に JBoss 設定コネクタが使用するプロトコル

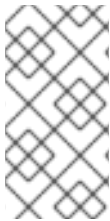
変数名	デフォルト	備考
SSL_IGNORE_CERTIFICATE_ERRORS	false	JBoss がセキュアなモードで実行され、SSL エラーが無視される場合には、この値は true に設定する必要があります。
SSL_IGNORE_HOST_VERIFICATION	false	JBoss がセキュアなモードで実行され、ホスト名の検証が無視される場合には、この値は true に設定する必要があります。
REPEAT_NON_RESPONSIVE_NOTIFICATION	false	この変数は、Manager がインストールされたマシンが応答しない状態となった場合に、サブスクライバーに対してエラーメッセージを繰り返し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. RED HAT VIRTUALIZATION MANAGER が SNMP トラップを送信するための設定

Red Hat Virtualization Manager が Simple Network Management Protocol (SNMP) トラップを単一または複数の外部 SNMP マネージャーに送信するように設定します。SNMP トラップには、システムイベント情報が含まれ、Red Hat Virtualization 環境のモニタリングに使用されます。SNMP マネージャーに送信されるトラップの数とタイプは、Red Hat Virtualization Manager 内で定義することができます。

以下の手順は、トラップを受信する外部 SNMP マネージャーが 1 つまたは複数設定済みで、かつ以下の情報が手元に用意されてい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。オプションとして、マネージャーがトラップ通知を受信するポートを定義します。デフォルトでは、UDP ポート 162 が使用されます。
- SNMP コミュニティー。1 つのコミュニティーには複数の SNMP マネージャーが属することができます。管理システムおよびエージェントは、同じコミュニティ内にある場合にのみ通信することが可能です。デフォルトのコミュニティーは **public** です。
- アラート用のトラップオブジェクト識別子。Red Hat Virtualization Manager はデフォルトで「1.3.6.1.4.1.2312.13.1.1」という OID を指定します。この OID が定義されると、全トラップタイプが送信され、イベント情報とともに SNMP マネージャーに追記されます。デフォルトのトラップを変更すると、生成されるトラップが Manager の管理情報ベースに準拠しなくなる点に注意してください。



注記

Red Hat Virtualization Manager は管理情報ベースを `/usr/share/doc/ovirt-engine/mibs/OVIRT-MIB.txt` および `/usr/share/doc/ovirt-engine/mibs/REDHAT-MIB.txt` で提供します。作業を開始する前に SNMP マネージャーの MIB (管理情報ベース) を読み込んでください。

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` 内に存在します。以下の手順で示す値は、このファイルに記載されているデフォルト値または例をベースとしています。アップグレード等のシステム変更後にも設定オプションを永続的に適用するには、**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することをお勧めします。

Manager での SNMP トラップの設定

1. 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
```

2. 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_MANAGERS="manager1.example.com manager2.example.com:162"
SNMP_COMMUNITY=public
SNMP_OID=1.3.6.1.4.1.2312.13.1.1
```

3. 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

デフォルトの SNMP プロファイルに全イベントを送信します。

```
FILTER="include:*(snmp:) ${FILTER}"
```

重大度が **ERROR** または **ALERT** のイベントをすべてデフォルトの 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 のイベントを指定のメールアドレスに送信します。

```
FILTER="include:VDC_START(snmp:mail@example.com) ${FILTER}"
```

VDC_START 以外のイベントを、すべてデフォルトの SNMP プロファイルに送信します。

```
FILTER="exclude:VDC_START include:*(snmp:) ${FILTER}"
```

ovirt-engine-notifier.conf で定義されるデフォルトフィルターは、以下のとおりです。このフィルターを無効にしない場合、またはこれに優先するフィルターを適用しない場合には、通知は一切送信されません。

```
FILTER="exclude:*"
```

VDC_START は、利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一覧は、**/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てください。

4. ファイルを保存します。

5. **ovirt-engine-notifier** サービスを起動します。さらに、このサービスがブート時に起動するように設定します。

```
# 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、トラップを受信し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_MANAGERS** と **MAIL_SERVER** のいずれか一方、もしくは両方を **/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-ENGINE-RENAME ツール

18.1.1. ovirt-engine-rename ツール

クリーンな環境で **engine-setup** コマンドを実行すると、設定プロセス中に指定した Manager の完全修飾ドメイン名を使用する複数の証明書と鍵が作成されます。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 (例: Manager をホストするマシンを異なるドメインに移行する場合など) には、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させる必要があります。**ovirt-engine-rename** コマンドにより、このタスクが自動化されます。

ovirt-engine-rename コマンドにより、以下の場所にある Manager の完全修飾ドメイン名のレコードが更新されます。

- /etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
- /etc/ovirt-engine/isouploader.conf.d/10-engine-setup.conf
- /etc/ovirt-engine/logcollector.conf.d/10-engine-setup.conf
- /etc/pki/ovirt-engine/cert.conf
- /etc/pki/ovirt-engine/cert.template
- /etc/pki/ovirt-engine/certs/apache.cer
- /etc/pki/ovirt-engine/keys/apache.key.nopass
- /etc/pki/ovirt-engine/keys/apache.p12



警告

ovirt-engine-rename コマンドは、Manager を実行している Web サーバー用の新規証明書を作成しますが、Manager や認証局の証明書には影響がありません。このため、**ovirt-engine-rename** コマンドを使用するにあたっては、多少リスクがあり、Red Hat Enterprise Virtualization 3.2 以前のバージョンからアップグレードした環境で特に顕著となります。したがって、可能な場合には、**engine-cleanup** および **engine-setup** を実行して Manager の完全修飾名を変更する方法が推奨されます。

18.1.2. ovirt-engine-rename コマンドの構文

ovirt-engine-rename コマンドの基本構文は以下の形式です。

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

このコマンドには、以下のオプションを指定することも可能です。

--newname=[new name]

ユーザー操作なしで Manager の新しい完全修飾ドメイン名を指定することができます。

--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と名前を指定することができます。

--config=[file]

名前変更操作で、ロードする設定ファイルのパスと名前を指定することができます。

--config-append=[file]

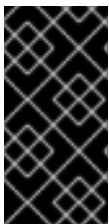
名前変更操作に追加する設定ファイルのパスと名前を指定することができます。このオプションは、応答ファイルのパスと名前の指定に使用可能です。

--generate-answer=[file]

応答および **ovirt-engine-rename** コマンドで変更した値が記録されるファイルのパスと名前を指定することができます。

18.1.3. ovirt-engine-rename ツールを使用した Manager の名前変更

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することができます。



重要

ovirt-engine-rename コマンドは **imageio-proxy** または **websocket-proxy** 等の SSL 証明書を更新しません。これらの証明書は、**ovirt-engine-rename** を実行した後、手動で更新する必要があります。この後に説明する「[SSL 証明書の更新](#)」を参照してください。

このツールは、Manager がローカルの ISO ストレージドメイン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チェックします。提供している場合には、操作を続行する前に、ツールはその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にアタッチされた ISO イメージを取り出し、シャットダウン、またはメンテナンスモードに切り替えるように、ユーザーに要求します。これにより、仮想マシンは、仮想ディスクとの接続を失わないようになり、名前変更の処理中に ISO ストレージドメインの接続が失われるのを防ぎます。

ovirt-engine-rename ツールの使用

1. 新しい完全修飾ドメイン名用に、全 DNS およびその他の関連するレコードを準備します。
2. DHCP を使用している場合には、DHCP サーバーの設定を更新します。
3. Manager で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 engine 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_
```

■

ovirt-engine-rename コマンドで Manager の完全修飾ドメイン名のレコードを更新しました。

SSL 証明書の更新

ovirt-engine-rename コマンドの後に以下のコマンドを実行して、SSL 証明書を更新します。

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

2. # subject="$(\
  openssl x509 \
  -in /etc/pki/ovirt-engine/certs/apache.cer \
  -noout \
  -subject | \
  sed \
    's;subject= \(.*\); \1;'
)"

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

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

18.2. ENGINE 設定ツール

18.2.1. engine 設定ツール

engine 設定ツールは、Red Hat Virtualization 環境のグローバル設定値を設定するためのコマンドラインユーティリティです。このツールは、engine データベースに保管されているキーと値のマッピングの一覧と対話して、個々のキーの値を取得したり、使用可能な設定キーと値の全一覧を取得したりすることができます。また、Red Hat Virtualization 環境の設定レベルごとに異なる値を保管することができます。



注記

設定キーの値を取得または設定するにあたって、Red Hat Virtualization Manager と Red Hat JBoss Enterprise Application Platform が実行中である必要はありません。その設定キーの値とキーのマッピングは、engine データベースに保管されているので、**postgresql** サービスの実行中に更新することができます。変更は、**ovirt-engine** サービスの再起動時に適用されます。

18.2.2. engine-config コマンドの構文

engine 設定ツールは、Red Hat Virtualization Manager がインストールされたマシンから実行することができます。使用方法についての詳細情報は、コマンドのヘルプ出力を参照してください。

■

```
# engine-config --help
```

一般的なタスク:

- 使用可能な設定キーの一覧表示

```
# engine-config --list
```

- 使用可能な設定値の一覧表示

```
# engine-config --all
```

- 設定キー値の取得

```
# engine-config --get KEY_NAME
```

特定のバージョンのキーの値を取得するには、**KEY_NAME** を対象のキー名に置き換えます。取得する値の設定バージョンを指定するには、**--cver** パラメーターを使用します。バージョンを指定しなかった場合には、全既存バージョンの値が返されます。

- 設定キー値の設定

```
# engine-config --set KEY_NAME=KEY_VALUE --cver=VERSION
```

KEY_NAME の箇所は設定する特定のキーの名前に、**KEY_VALUE** の箇所は設定する値に置き換えてください。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。

- ovirt-engine サービスの再起動による変更の有効化
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. USB FILTER EDITOR

18.3.1. USB Filter Editor のインストール

USB Filter Editor とは、**usbfilter.txt** という名前のポリシーファイルの設定に使用する Windows 用ツールです。このファイルで定義されたポリシールールにより、クライアントから 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が許可または拒否されます。ポリシーファイルは、Red Hat Virtualization Manager の **/etc/ovirt-engine/usbfilter.txt** に保管されます。USB フィルターポリシーへの変更は、Red Hat Virtualization Manager サーバーで次回 **ovirt-engine** サービスが再起動されるまで有効にはなりません。

コンテンツ配信ネットワーク (<https://rhn.redhat.com/rhn/software/channel/downloads/Download.do?cid=20703>) から **USBFilterEditor.msi** ファイルをダウンロードします。

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ってインストールを行います。USB Filter Editor のインス

ツール先を指定しなかった場合には、デフォルトでは使用している Windows のバージョンに応じて **C:\Program Files\RedHat\USB Filter Editor** または **C:\Program Files(x86)\RedHat\USB Filter Editor** にインストールされます。

3. デスクトップに USB Filter Editor のショートカットアイコンが作成されます。



重要

Secure Copy (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またはエクスポートします。Windows マシン用の Secure Copy ツールは WinSCP です (「[WinSCPとは](#)」を参照してください)。

デフォルトの USB デバイスポリシーにより、仮想マシンから USB デバイスへの基本的なアクセスが可能となります。追加の USB デバイスを使用するには、ポリシーを更新してください。

18.3.2. USB Filter Editor のインターフェース

デスクトップ上の USB Filter Editor のショートカットアイコンをダブルクリックします。

Red Hat USB Filter Editor インターフェースには、USB デバイスごとに **Class**、**Vendor**、**Product**、**Revision**、および **Action** が表示されます。**Action** コラムで、許可されている USB デバイスは **Allow** に、許可されていないデバイスは **Block** に設定されます。

表18.1 USB Editor のフィールド

名前	説明
Class	USB デバイスのタイプ (例: プリンター、大容量ストレージコントローラー)
Vendor	選択したタイプのデバイスの製造元
Product	具体的な USB デバイスモデル
Revision	製品のリビジョン
Action	指定したデバイスの許可またはブロック

USB デバイスポリシールールは、一覧に記載された順序で処理されます。**Up** および **Down** のボタンを使用すると、ルールを一覧内で上下に移動させることができます。ユニバーサル **Block** ルールは最下部に位置する必要があります。これにより、USB Filter Editor で明示的に許可されていない限り、すべての USB デバイスが拒否されます。

18.3.3. USB ポリシーの追加

デスクトップ上の USB Filter Editor の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。

USB ポリシーの追加

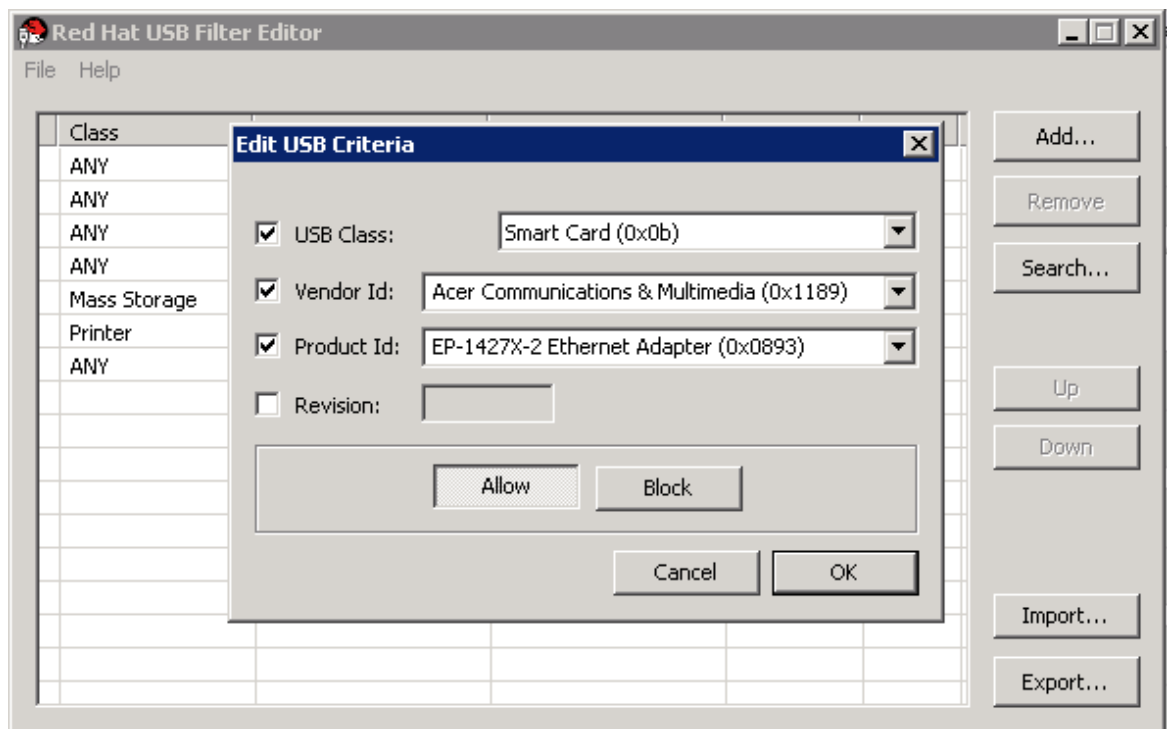
1. **追加** をクリックします。

2. **USB Class**、**Vendor Id**、**Product Id**、および **Revision** のチェックボックスと一覧を使用し、デバイスを指定します。
仮想マシンが USB デバイスを使用できるようにするには、**Allow** ボタンをクリックします。また、仮想マシンが USB デバイスを使用できないようにブロックするには **Block** ボタンをクリックします。

OK をクリックして、選択したフィルタールールを一覧に追加し、ウィンドウを閉じます。

例18.1 デバイスの追加

以下は、USB Class が **Smart Card** の **Acer Communications & Multimedia** 社製デバイス **EP-1427X-2 Ethernet Adapter** を許可済みデバイスの一覧に追加する方法の例です。



3. **File** → **Save** をクリックして、変更を保存します。

USB ポリシーが USB Filter Editor に追加されました。USB フィルターポリシーを適用するには、Red Hat Virtualization Manager にエクスポートする必要があります。

18.3.4. USB ポリシーの削除

デスクトップ上の USB Filter Editor の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。

USB ポリシーの削除

1. 削除するポリシーを選択します。
2. **Remove** をクリックします。ポリシーの削除を確認するメッセージが表示されます。
3. **Yes** をクリックして、ポリシーの削除を確定します。
4. **File** → **Save** をクリックして、変更を保存します。

USB ポリシーが USB Filter Editor から削除されました。USB フィルターポリシーを適用するには、Red Hat Virtualization Manager にエクスポートする必要があります。

18.3.5. USB デバイスポリシーの検索

アタッチされた USB デバイス を検索して、USB Filter Editor 内で許可またはブロックします。

デスクトップ上の USB Filter Editor の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。

USB デバイスポリシーの検索

1. **Search** をクリックします。 **Attached USB Devices** ウィンドウに、アタッチされている全デバイスの一覧が表示されます。
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、ウィンドウを閉じます。そのデバイスに対するポリシールールが一覧に追加されます。
3. 一覧内で新規ポリシールールの位置を変更するには、**Up** と **Down** のボタンを使用してください。
4. **File** → **Save** をクリックして、変更を保存します。

アタッチされている USB デバイスが検索されました。USB フィルターポリシーを適用するには、Red Hat Virtualization Manager にエクスポートする必要があります。

18.3.6. USB ポリシーのエクスポート

更新された USB デバイスポリシーを反映するには、変更を Red Hat Virtualization Manager にエクスポートして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て、**ovirt-engine** サービスを再起動します。

デスクトップ上の USB Filter Editor の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。

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. **usbfilter.txt** というファイル名でファイルを保存します。
3. WinSCP などの Secure Copy クライアントを使用して Red Hat Virtualization Manager を実行しているサーバーに **usbfilter.txt** ファイルをアップロードします。ファイルはサーバー上の **/etc/ovirt-engine/** ディレクトリーに配置する必要があります。
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
```

18.3.7. USB ポリシーのインポート

既存の USB デバイスポリシーを編集するには、ダウンロードして USB Filter Editor にインポートする必要があります。

USB ポリシーのインポート

1. WinSCP などの Secure Copy クライアントを使用して Red Hat Virtualization Manager を実行しているサーバーから **usbfilter.txt** ファイルをダウンロードします。ファイルはサーバー上の **/etc/ovirt-engine/** ディレクトリーに格納されています。
2. デスクトップ上の USB Filter Editor の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** をクリックすると **Open** のウィンドウが開きます。
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。

18.4. ログ収集ツール

18.4.1. ログコレクター

Red Hat Virtualization Manager には、ログ収集ツールが含まれています。これにより、サポートをリクエストする際には、Red Hat Virtualization 環境全体にわたる関連ログを簡単に収集することができます。

ログ収集のコマンドは、**ovirt-log-collector** です。**root** ユーザーとしてログインして、コマンドライン上で Red Hat Virtualization 環境の管理者の認証情報を入力する必要があります。**ovirt-log-collector -h** コマンドを実行すると、**ovirt-log-collector** コマンドの有効なオプションの全一覧など、使用方法に関する詳しい説明を表示することができます。

18.4.2. 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形式です。

```
# ovirt-log-collector options list all|clusters|datacenters
# ovirt-log-collector options collect
```

list および **collect** の 2 つの操作モードに対応しています。

- **list** パラメーターは、Red Hat Virtualization Manager にアタッチされているホスト、クラスター、データセンターのいずれかを一覧表示します。一覧表示されたオブジェクトをベースとして、ログ収集をフィルタリングできます。
- **collect** パラメーターは、Red Hat Virtualization Manager からログを収集します。収集されたログは、**/tmp/logcollector** ディレクトリーの配下にあるアーカイブファイルに配置されます。**ovirt-log-collector** コマンドは、ログごと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設定されていない限りは、デフォルトで、使用可能なホストならびにそれらが属するデータセンターとクラスターが一覧表示されます。特定のログを取得するためのユーザー名とパスワードを入力するプロンプトが表示されます。

ovirt-log-collector コマンドをさらに詳しく指定する数多くのパラメーターがあります。

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た後に、元のプロンプトに戻ります。

-h, --help

コマンドの使用方法についての情報を表示した後に、元の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を **PATH** で指定します。

--local-tmp=PATH

ログを保存するディレクトリーを **PATH** で指定します。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を **TICKET** で指定します。

--upload=FTP_SERVER

FTP を使用して送信される取得済みログの送信先を **FTP_SERVER** で指定します。Red Hat のサポート担当者のアドバイスなしには、このオプションは使用しないでください。

--log-file=PATH

このコマンドがログ出力に使用するファイル名を **PATH** で指定します。

--quiet

Quiet モードに設定し、コンソールの出力を最小限に抑えます。Quiet モードはデフォルトではオフになっています。

-v、--verbose

詳細モードに設定し、より詳しいコンソール出力を提供します。詳細モードは、デフォルトではオフになっています。

--time-only

完全な SOS レポートを生成せずに、ホスト間の時間差に関する情報だけを表示します。

Red Hat Virtualization Manager のオプション

以下のオプションは、ログ収集をフィルタリングして、Red Hat Virtualization Manager に対する認証の詳細を指定します。

これらのパラメーターは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** と指定して、ログ収集を **A** および **B** のクラスター内の **SalesHost** ホストだけに制限します。

--no-hypervisors

ログ収集から仮想化ホストを除外します。

--one-hypervisor-per-cluster

それぞれのクラスターから、1 台のホスト (もしあれば SPM) のログを収集します。

-u USER、--user=USER

ログインするユーザー名を設定します。**USER** は **user@domain** の形式で指定します。**user** はユーザー名、**domain** は使用している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内に存在し、かつ Red Hat Virtualization Manager が認識する必要があります。

-r FQDN、--rhevm=FQDN

ログを収集する 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** の箇所は Manager の完全修飾ドメイン名に置き換えてください。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されることを前提としています。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** の仮想化ホストからのログも収集します。対象となるクラスターは、クラスター名またはマッチ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のログも収集します。対象となるデータセンターは、データセンター名またはマッチ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** の仮想化ホストからのログも収集します。対象となるホストは、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。マッチパターンも有効です。

SSH の設定

--ssh-port=PORT

仮想化ホストとの SSH 接続に使用するポートを **PORT** で指定します。

-k KEYFILE、--key-file=KEYFILE

仮想化ホストへのアクセスに使用する SSH 公開鍵を **KEYFILE** で指定します。

--max-connections=MAX_CONNECTIONS

仮想化ホストからのログを収集する際の最大同時 SSH 接続数を **MAX_CONNECTIONS** で指定します。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およびデータベース名がデフォルト値から変更されている場合には、**pg-user** と **dbname** の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には、**pg-dbhost** パラメーターを設定します。オプションの **pg-host-key** パラメーターを使用すると、リモートログを収集します。適切にリモートログ収集を行うには、PostgreSQL SOS プラグインがデータベースサーバー上にインストールされている必要があります。

--no-postgresql

データベースの収集を無効にします。**--no-postgresql** パラメーターが指定されていない場合には、ログコレクターが Red Hat Virtualization Manager PostgreSQL データベースに接続して、ログレポートにデータを追加します。

--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を **USER** で指定します。デフォルトは **postgres** です。

--pg-database=DATABASE

データベースサーバーとの接続に使用するデータベース名を **DATABASE** で指定します。デフォルトは **rhevm** です。

--pg-dbhost=DBHOST

データベースサーバーのホスト名を **DBHOST** で指定します。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) を **KEYFILE** で指定します。この値は、ローカルホスト上にデータベースが存在しない場合にのみ必要なため、デフォルトでは設定されていません。

18.4.3. ログコレクターの基本的な使用例

追加のパラメーターを指定せずに **ovirt-log-collector** コマンドを実行した場合には、デフォルトの動作は、Red Hat Virtualization Manager および Manager にアタッチされたホストからのログをすべて収集します。また、**--no-postgresql** パラメーターが指定されていない限り、データベースのログも収集します。以下の例では、ログコレクターのコマンドを実行して、Red Hat Virtualization Manager とアタッチされたホスト 3 台からのログをすべて収集します。

例18.2 ログコレクターの使用例

```
# 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
```

18.5. ISO アップローダーツール

18.5.1. 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ためのツールです。このツールは Red Hat Virtualization Manager の一部としてインストールされます。

ISO アップローダーのコマンドは、**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て、Red Hat Virtualization 環境の管理者の認証情報を入力する必要があります。**engine-iso-uploader -h** コマンドを実行すると、**engine-iso-uploader** コマンドの有効なオプションの全一覧など、使用方法に関する詳しい説明を表示することができます。

18.5.2. engine-iso-uploader コマンドの構文

ISO アップローダーコマンドの基本構文は以下の形式です。

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

ISO アップローダーのコマンドは、**list** と **upload** の 2 つのアクションをサポートしています。

- **list** アクションは、ISO ファイルをアップロード可能な 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たマシン上にこの一覧を作成します。
- **upload** アクションは、1 つの ISO ファイルまたはスペースで区切った複数の ISO ファイルを、指定した 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 アップローダーのコマンドを使用する際には、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。また、**upload** アクションを使用するには、ローカルファイルを少なくとも 1 つ指定する必要があります。

engine-iso-uploader コマンドをさらに詳しく指定する数多くのパラメーターがあります。

一般的なオプション

--version

ISO アップローダーコマンドのバージョンを表示します。

-h, --help

ISO アップローダーコマンドの使用方法についての情報を表示します。

--conf-file=PATH

コマンドが使用する設定ファイルを **PATH** で指定します。デフォルトは **/etc/ovirt-engine/isouploader.conf** です。

--log-file=PATH

コマンドがログ出力を書き込むのに使用する特定のファイル名を **PATH** で指定します。デフォルトは **/var/log/ovirt-engine/ovirt-iso-uploader/ovirt-iso-uploader_date.log** です。

--cert-file=PATH

engine を検証するための証明書を **PATH** で指定します。デフォルトは **/etc/pki/ovirt-engine/ca.pem** です。

--insecure

engine の検証を試行しないように指定します。

--nossl

engine への接続で SSL が使用されないように指定します。

--quiet

Quiet モードに設定し、コンソールの出力を最小限に抑えます。

-v, --verbose

詳細モードに設定し、より詳しいコンソール出力を提供します。

-f, --force

強制モードは、アップロードされるソースファイルが、アップロード先の ISO ドメインの既存ファイルと同じ名前の場合に使用する必要があります。このオプションは、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

コマンドの実行に使用する認証情報のユーザーを指定します。**USER** は、**username@domain** の形式で指定してください。指定するユーザーは、指定したドメインに存在し、かつ Red Hat Virtualization Manager が認識し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元となる 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ることを前提としています。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

以下のオプションは、イメージのアップロード先となる ISO ドメインを指定します。これらのオプションは、同時に使用することはできません。-i または -n のいずれかを使用する必要があります。

-i、--iso-domain=ISODOMAIN

アップロード先としてストレージドメイン **ISODOMAIN** を指定します。

-n、--nfs-server=NFSSERVER

アップロード先として NFS パス **NFSSERVER** を指定します。

接続オプション

デフォルトでは、ISO アップローダーは NFS を使用してファイルをアップロードします。代わりに、以下のオプションは SSH ファイル転送を指定します。

--ssh-user=USER

アップロード時に使用する SSH ユーザー名を **USER** で指定します。デフォルトは **root** です。

--ssh-port=PORT

SSH 接続時に使用するポートを **PORT** で指定します。

-k KEYFILE、--key-file=KEYFILE

SSH 認証に使用する公開鍵を **KEYFILE** で指定します。鍵を指定しないと、**--ssh-user=USER** で指定したユーザーのパスワード入力が必要です。

18.5.3. NSF サーバーの指定**例18.3 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
```

18.5.4. 基本的な ISO アップローダーの使用法

以下は、ISO アップローダーと list パラメーターの使用例です。最初のコマンドは、使用可能な ISO ストレージドメインを表示します。コマンドでユーザー名を指定していなかったため、**admin@internal** が使用されます。2 番目のコマンドは、NFS 経由で指定の ISO ドメインに ISO ファイルをアップロードします。

例18.4 ドメインの一覧表示と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):
```

18.5.5. 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

Windows 仮想マシン用の VirtIO ドライバーを含む **virtio-win** ISO イメージと Virtual Floppy Drive (VFD) イメージ、Windows 仮想マシン用の Red Hat Virtualization ゲストツールを含む **rhv-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で提供されるソフトウェアを仮想マシンにインストールすると、パフォーマンスやユーザビリティを向上させることができます。最新の **virtio-win** と **rhv-tools-setup** の各イメージは、Red Hat Virtualization Manager のファイルシステム上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/rhv-guest-tools-iso/rhv-tools-setup.iso**

インストールプロセスで ISO ストレージドメインがローカルに作成されなかった場合には、これらのイメージファイルを手動でアップロードする必要があります。ISO ストレージドメインにこれらのファイルをアップロードするには **engine-iso-uploader** コマンドを使用します。イメージファイルのアップロードが完了すると、仮想マシンにアタッチして使用できるようになります。

以下の例は、**virtio-win.iso**、**virtio-win_x86.vfd**、**virtio-win_amd64.vfd**、**rhv-tools-setup.iso** の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18.5 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/rhv-guest-tools-
iso/rhv-tools-setup.iso
```

18.6. ENGINE-VACUUM ツール

18.6.1. engine-vacuum ツール

engine-vacuum ツールにより、PostgreSQL データベースのメンテナンスが行われます。テーブルを更新して実行されない行を削除することで、ディスク領域を再使用することができます。**VACUUM** コマンドおよびそのパラメーターについては、[「PostgreSQL 9.5.14 Documentation」](#) を参照してください。

engine の vacuum 操作に関するコマンドは、**engine-vacuum** です。**root** ユーザーとしてログインして、Red Hat Virtualization 環境の管理者の認証情報を入力する必要があります。

あるいは、**engine-setup** コマンドを使用する際に engine-vacuum ツールを実行して、既存のシステムをカスタマイズすることができます。

```
$ 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/9.5/static/sql-vacuum.html
(Yes, No) [No]:
```

Yes を選択すると、engine-vacuum ツールは詳細モードで完全 vacuum 操作を実施します。

18.6.2. engine の vacuum 操作モード

engine の vacuum 操作には 2 つのモードがあります。

標準 vacuum 操作

定期的に標準 vacuum 操作を実施することを推奨します。

標準 vacuum 操作はテーブル内の実行されない行のバージョンを削除し、その領域をインデックス化して今後再使用可能として識別します。頻繁に更新されるテーブルでは、定期的に vacuum 操作を実施する必要があります。ただし、標準 vacuum 操作ではこれらの領域はオペレーティングシステムに返還されません。

パラメーターを指定せずに標準 vacuum 操作を実施すると、現在のデータベースの全テーブルが処理されます。

完全 vacuum 操作

完全 vacuum 操作を定期的に実施することは推奨されません。テーブル内から相当量の領域を確保する必要がある場合にのみ実行してください。

完全 vacuum 操作でテーブルを圧縮する場合、書き込まれるテーブルファイルの新しいコピーには使用されない領域が含まれません。したがって、オペレーティングシステムは領域を再取得することができます。完全 vacuum 操作には時間がかかる場合があります。

完全 vacuum 操作には、処理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容量が必要です。完全 vacuum 操作を行うためにはテーブルを完全にロックする必要がありますので、テーブルを使用するその他の操作と並行して実施することはできません。

18.6.3. engine-vacuum コマンドの構文

engine-vacuum コマンドの基本構文は以下の形式です。

```
# 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 vacuum 操作が実施されます。

engine-vacuum コマンドをさらに詳しく指定する数多く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ついての情報を表示します。

-a

標準 vacuum 操作を実施し、データベースを分析し、最適化ツールの統計値を更新します。

-A

データベースを分析して最適化ツールの統計値を更新しますが、vacuum 操作は実施しません。

-f

完全 vacuum 操作を実施します。

-v

より詳しいコンソール出力を表示する詳細モードで実施します。

-t table_name

特定のテーブルの vacuum 操作を実施します。

```
# 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. MANAGER インストールのログファイル

表19.1 インストール

ログファイル	説明
<code>/var/log/ovirt-engine/engine-cleanup_yyyy_mm_dd_hh_mm_ss.log</code>	Red Hat Virtualization Manager のインストールをリセットするのに使用される engine-cleanup コマンドからのログ。このコマンドを実行すると、毎回ログが生成されます。ファイル名に実行日時が使用されるので、同時に複数のログが存在可能です。
<code>/var/log/ovirt-engine/engine-db-install_yyyy_mm_dd_hh_mm_ss.log</code>	engine-setup コマンドからのログ。 engine データベースの作成、設定が詳しく記録されます。
<code>/var/log/ovirt-engine/ovirt-engine-dwh-setup_yyyy_mm_dd_hh_mm_ss.log</code>	レポート用に ovirt_engine_history データベースを作成するのに使用される ovirt-engine-dwh-setup コマンドからのログ。このコマンドを実行すると、毎回ログが生成されます。ファイル名に実行日時が使用されるので、同時に複数のログが存在可能です。
<code>/var/log/ovirt-engine/setup/ovirt-engine-setup-yyyymmddhhmmss.log</code>	engine-setup コマンドからのログ。このコマンドを実行すると、毎回ログが生成されます。ファイル名に実行日時が使用されるので、同時に複数のログが存在可能です。

19.2. RED HAT VIRTUALIZATION MANAGER のログファイル

表19.2 サービスアクティビティ

ログファイル	説明
<code>/var/log/ovirt-engine/engine.log</code>	Red Hat Virtualization Manager の GUI のクラッシュ、Active Directory のルックアップ、データベースの問題、その他のイベントすべてを反映
<code>/var/log/ovirt-engine/host-deploy</code>	Red Hat Virtualization Manager からデプロイされたホストが出力するログファイル
<code>/var/lib/ovirt-engine/setup-history.txt</code>	Red Hat Virtualization Manager に関連したパッケージのインストールとアップグレードをトラッキング

ログファイル	説明
<code>/var/log/httpd/ovirt-requests-log</code>	<p>HTTPS を介して Red Hat Virtualization Manager に送信された要求は、ファイルにログ記録されます。これには、各要求にかかった時間も含まれます。</p> <p>Correlation-Id ヘッダーが含まれているので、ログファイルを <code>/var/log/ovirt-engine/engine.log</code> と対比する際に要求を比較することができます。</p>

19.3. SPICE のログファイル

SPICE のログファイルは、SPICE の接続問題のトラブルシューティングを行う際に役立ちます。SPICE デバッグを開始するには、ログレベルを **debugging** に変更してからログの場所を確認します。

ゲストマシンへのアクセスに使用するクライアントと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では、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には **console.vv** ファイルがダウンロードされ、**remote-viewer** コマンドを使用してデバッグを有効化し、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	ログレベルの変更手順
ホスト/ハイパーバイザー SPICE サーバー	<code>/var/log/libvirt/qemu/(guest_name).log</code>	<p>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した場合には、そのシステム上の全仮想マシンのデバッグ情報を出力します。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、ホスト/ハイパーバイザー単位でのみ機能し、クラスター単位では機能しません。</p>

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	ログレベルの変更手順
-------	-------	------------

ログタイプ	ログの場所	ログレベルの変更手順
Windows ゲスト	C:\Windows\Temp\vdagent.log C:\Windows\Temp\vdservice.log	該当なし
Red Hat Enterprise Linux ゲスト	root ユーザーとして journalctl を使用します。	<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 /etc/sysconfig/spice-vdagentd ファイルを作成して、SPICE_VDAGENTD_EXTRA_ARGS="-d -d" のエントリーを記述します。</p> <p>spice-vdagent をデバッグモードで実行するには、コマンドラインで以下のコマンドを実行します。</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した 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. **remote-viewer** コマンドに **--spice-debug** オプションを使用して実行し、SPICE の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 (例: `spice://virtual_machine_IP:port`) を入力します。

```
# remote-viewer --spice-debug
```

2. デバッグパラメーターを指定して SPICE クライアントを実行して .vv ファイルを渡すには、**console.vv** ファイルをダウンロードし、**remote-viewer** コマンドに **--spice-debug** オプションを使用して実行して、**console.vv** ファイルへの完全パスを指定します。

```
# 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** により **virt-viewer** と **debug-viewer.exe** がインストールされます。
2. **remote-viewer** コマンドに **spice-debug** の引数を指定して実行し、コマンドをコンソールへのパスでダイレクトします。

```
remote-viewer --spice-debug path\to\console.vv
```

3. ログを確認するには、仮想マシンに接続します。GDB を実行中のコマンドプロンプトで、**remote-viewer** の標準出力と標準エラーが表示されます。

19.4. ホストのログファイル

ログファイル	説明
<code>/var/log/vdsm/libvirt.log</code>	libvirt のログファイル
<code>/var/log/vdsm/spm-lock.log</code>	Storage Pool Manager ロールでリースを取得するホストの機能について詳細に記述したログファイル。ホストがリースを取得、解放、更新した時、または更新に失敗した時のログの詳細です。
<code>/var/log/vdsm/vdsm.log</code>	ホスト上の Manager のエージェントである VDSM のログファイル
<code>/tmp/ovirt-host-deploy-Date.log</code>	ホストのデプロイメントログ。ホストが正常にデプロイされた後、 <code>/var/log/ovirt-engine/host-deploy/ovirt-Date-Host-Correlation_ID.log</code> として Manager にコピーされます。
<code>/var/log/vdsm/import/import-UUID-Date.log</code>	KVM ホスト、VMWare プロバイダー、または Xen ホストからの仮想マシンのインポートに関する詳細を記載したログ。これには、インポートの失敗についての情報も含まれます。 UUID はインポートされた仮想マシンの UUID です。 Date はインポートが開始された日時です。

19.5. ホストのロギングサーバーの設定

ホストは、ホストのアクションや問題を記録するログファイルを生成、更新します。ログファイルを一元的に収集することにより、デバッグが確実に簡素化されます。

この手順には、集中ログサーバーを使用することを推奨しますが、別のロギングサーバーを使用することも可能です。また、この手順を使用して Red Hat Virtualization Manager でホストのロギングを有効にすることも可能です。

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` を編集して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
```

以下の行のコメントを解除します。

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

3. **rsyslog** サービスを再起動します。

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

仮想化ホストから **messages** および **secure** ログを受信して保管するように、集中ログサーバーを設定しました。

第20章 プロキシ

20.1. SPICE プロキシ

20.1.1. SPICE プロキシの概要

SPICE プロキシは、SPICE クライアントがハイパーバイザーを繋げてい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のに使用するツールです。SPICE プロキシを設定するには、マシンに **Squid** をインストールして、プロキシトラフィックを許可するようにファイアウォールを設定します。SPICE プロキシを有効にするには、Manager で **engine-config** を使用して **SpiceProxyDefault** のキーをプロキシの名前とポートで構成される値に設定します。SPICE プロキシをオフにするには、Manager で **engine-config** を使用して **SpiceProxyDefault** に設定されている値を削除します。



重要

SPICE プロキシは、スタンドアロンの SPICE クライアントと併用する場合にのみ使用可能で、noVNC を使用する仮想マシンへの接続には使用できません。

20.1.2. SPICE プロキシのマシン設定

以下の手順では、SPICE プロキシとしてマシンを設定する方法について説明します。SPICE プロキシにより、外部から Red Hat Virtualization ネットワークに接続することが可能になります。この手順では、プロキシサービスに **Squid** を使用します。

Red Hat Enterprise Linux への Squid のインストール

1. プロキシマシンに **Squid** をインストールします。

```
# yum install squid
```

2. **/etc/squid/squid.conf** を開いて、以下の箇所を見つけます。

```
http_access deny CONNECT !SSL_ports
```

これを以下のように編集します。

```
http_access deny CONNECT !Safe_ports
```

3. プロキシを起動します。

```
# 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 ルールを保存します。

```
# service iptables save
```

マシンが SPICE プロキシとして設定されました。Red Hat Virtualization ネットワークに外部から接続する前に SPICE プロキシを有効にしてください。

20.1.3. SPICE プロキシの有効化

以下の手順では、SPICE プロキシを有効 (オン) にする方法を説明します。

SPICE プロキシの有効化

1. Manager で engine-config ツールを使用してプロキシを設定します。

```
# engine-config -s SpiceProxyDefault=someProxy
```

2. **ovirt-engine** サービスを再起動します。

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

プロキシは以下の形式を使用するようにします。

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



注記

HTTPS プロキシをサポートしているのは、Red Hat Enterprise Linux 6.7、Red Hat Enterprise Linux 7.2、またはそれ以降のバージョンに同梱された SPICE クライアントのみです。それ以前のバージョンのクライアントは、HTTP しかサポートしません。以前のクライアントに対して HTTPS を指定すると、そのクライアントはプロキシ設定を無視して、ホストに直接接続を試みます。

SPICE プロキシが有効 (オン) になりました。SPICE プロキシを使用して Red Hat Virtualization 環境に接続することができます。

20.1.4. SPICE プロキシの無効化

以下の手順では、SPICE プロキシを無効 (オフ) にする方法を説明します。

SPICE プロキシの無効化

1. Manager にログインします。

```
$ ssh root@[IP of Manager]
```

2. 以下のコマンドを実行して SPICE プロキシを削除します。

```
# engine-config -s SpiceProxyDefault=""
```

3. Manager を再起動します。

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

SPICE プロキシが無効 (オフ) になりました。SPICE プロキシを使用しても Red Hat Virtualization 環境に接続できなくなりました。

20.2. SQUID プロキシ

20.2.1. Squid プロキシのインストールと設定

本セクションでは、VM ユーザーポータルへの Squid プロキシのインストールと設定方法を説明します。Squid プロキシサーバーは、頻繁に閲覧されるコンテンツをキャッシュして帯域幅を削減し、応答時間を向上させるコンテンツアクセラレーターとして使用されます。

Squid プロキシの設定

1. Squid プロキシの HTTPS ポート用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 サービス用のキーペアを取得するのと同じ方法で取得することができます。キーペアは 2 つの PEM ファイルの形式となっており、これらのファイルには秘密鍵と署名済み証明書が含まれています。この手順では、これらのファイル名を **proxy.key** および **proxy.cer** と仮定します。



注記

キーペアと証明書は、engine の認証局を使用して生成することもできます。プロキシに秘密鍵と証明書が設定されており、engine の認証局で生成しない場合は、次の手順は省略してください。

2. プロキシのホスト名を選択し、次にプロキシ用の証明書の識別名のその他のコンポーネントを選択します。



注記

engine 自体が使用しているのと同じ国や組織名を使用するのが適切なプラクティスです。Manager がインストールされているマシンにログインして以下のコマンドを実行すると、この情報を確認することができます。

```
# openssl x509 -in /etc/pki/ovirt-engine/ca.pem -noout -subject
```

このコマンドは以下のような出力を表示します。

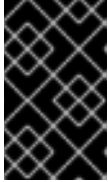
```
subject= /C=US/O=Example Inc./CN=engine.example.com.81108
```

対象となる箇所は **/C=US/O=Example Inc.** です。これを使用して、プロキシ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. プロキシマシンにログインして、証明書署名要求 (CSR) 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

証明書の識別名は引用符で囲む必要があります。-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、プロキシサーバーの起動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。このファイルは安全な場所に保管するようにしてください。**proxy.req** は証明書署名要求です。**proxy.req** には、特別な保護はありません。

- 署名済みの証明書を生成するには、プロキシのマシンからManagerのマシンに証明書署名要求ファイルをコピーします。

```
# scp proxy.req engine.example.com:/etc/pki/ovirt-engine/requests/.
```

- Managerのマシンにログインして、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'
```

このコマンドにより、証明書が署名され、10年間(3650日)有効になります。証明書の失効期限を短く設定することもできます。

- 生成し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** という名前が付いているはずです。プロキシマシンで、Managerのマシンから、現在のディレクトリーにこのファイルをコピーします。

```
# scp engine.example.com:/etc/pki/ovirt-engine/certs/proxy.cer .
```

- proxy.key** と **proxy.cer** の両ファイルがプロキシマシン上に存在していることを確認します。

```
# ls -l proxy.key proxy.cer
```

- プロキシマシンに Squid プロキシサーバーパッケージをインストールします。

```
# yum install squid
```

- 秘密鍵と署名済みの証明書をプロキシ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込むことができ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 プロキシは engine が使用する証明書を検証する必要があります。Manager の証明書をプロキシマシンにコピーします。以下の例では、ファイルパスに **/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 のマシンの `/etc/pki/ovirt-engine/ca.pem` にあります。

12. **squid** ユーザーがこの証明書ファイルを読み込むことができ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ます。これにより、Squid がポート 443 を使用できるようになります。

```
# 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のように置き換えます。

```
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
```



注記

デフォルトでは、Squid プロキシはアイドル状態が 15 分経過すると接続を終了します。アイドル状態の接続を切断するまでの時間を延長するには、**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

20.3.1. Websocket プロキシの概要

Websocket プロキシにより、ユーザーは、noVNC コンソールを介して仮想マシンに接続することができます。以前は、Websocket プロキシは Red Hat Virtualization Manager マシンでしか実行できませんでしたが、現在このプロキシは、ネットワークへのアクセスが可能な任意のマシンで実行することができます。

Websocket プロキシは、初期設定中に Red Hat Virtualization Manager マシンにインストール/設定することができます (『インストールガイド』の「[Red Hat Virtualization Manager の設定](#)」のセクションを参照してください)。または、Manager 以外のマシンにインストール/設定することも可能です (『インストールガイド』の「[別のマシンへの Websocket プロキシのインストール](#)」のセクションを参照してください)。

Websocket プロキシは Manager のマシンから別のマシンに移行することもできます。[「別のマシンへの Websocket プロキシの移行」](#)を参照してください。

20.3.2. 別のマシンへの Websocket プロキシの移行

セキュリティまたはパフォーマンス上の理由で、Red Hat Virtualization Manager を実行しているものとは別のマシンで Websocket プロキシを実行することが可能です。Manager のマシンから別のマシンに Websocket プロキシを移行する手順では、Manager のマシンから Websocket プロキシの設定を削除してから、別のマシンにプロキシをインストールする必要があります。

Manager マシンから Websocket プロキシを削除するには、**engine-cleanup** コマンドを使用することができます。

別のマシンへの Websocket プロキシの移行

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. 全コンポーネントを削除するかどうかを尋ねられたら、**No** と入力して **Enter** を押します。

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

3. engine を削除するかどうかを尋ねられたら、**No** と入力して **Enter** を押します。

```
Do you want to remove the engine? (Yes, No) [Yes]: No
```

4. Websocket プロキシを削除するかどうかを尋ねられたら、**Yes** と入力して **Enter** を押します。

```
Do you want to remove the WebSocket proxy? (Yes, No) [No]: Yes
```

その他のコンポーネントを削除するかどうかを尋ねられたら、**No** を選択します。

5. 別のマシンにプロキシをインストールして設定します。その手順は、『[インストールガイド](#)』の『[別のマシンへの Websocket プロキシのインストール](#)』のセクションを参照してください。

付録A VDSM とフック

A.1. VDSM

VDSM サービスは、Red Hat Virtualization Manager が Red Hat Virtualization Host (RHVH) および Red Hat Enterprise Linux ホストの管理に使用します。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の管理とモニタリングを行います。また、仮想マシンの作成、統計の収集、ログの収集、その他のホスト管理タスクの調整も行います。VDSM は、Red Hat Virtualization Manager によって管理されている各ハイパーバイザーホストでデーモンとして実行されます。また、クライアントからの XML-RPC コールに応答します。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、フックにより拡張可能です。フックは、重要なイベントが発生した際にホスト上で実行されるスクリプトです。サポートされてい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。規則により、各フックスクリプトには 2 桁の番号が割り当てられています。この番号は、スクリプトの実行順序が明確となるように、ファイル名の最初に付いています。フックスクリプトは、任意のプログラミング言語で作成することができますが、本章の例には、Python を使用しています。

ホスト上でイベントに対して定義されている全スクリプトが実行される点に注意してください。特定のフックが、ホスト上で稼働する仮想マシンのサブセットに対してのみ実行されるようにする必要がある場合には、仮想マシンに関連付けられた **カスタムプロパティ** を評価して、フックスクリプト自体がこの要件に対応するようにしなければなりません。



警告

VDSM フックは、Red Hat Virtualization の操作を妨げる可能性があります。VDSM フックのバグにより、仮想マシンがクラッシュしたり、データが損失したりする可能性があります。VDSM フックは、慎重かつ厳格にテストを行った上で実装する必要があります。フック API は新しいため、今後大幅に変更される可能性があります。

A.3. フックを使用した VDSM の拡張

本章では、イベント駆動型フックを使用した VDSM の拡張方法について説明します。フックを使用した VDSM の拡張は、実験的技術です。本章は熟練の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を設定することにより、特定の仮想マシン固有の追加パラメーターをフックスクリプトに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

名前	説明
before_vm_start	仮想マシンが起動する前
after_vm_start	仮想マシンが起動した後
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	仮想マシンを休止状態にする前
after_vm_hibernate	仮想マシンを休止状態にした後
before_vm_dehibernate	仮想マシンの休止状態を解除する前
after_vm_dehibernate	仮想マシンの休止状態を解除した後
before_vm_migrate_source	仮想マシンの移行の前に、移行元のホストで実行
after_vm_migrate_source	仮想マシンの移行の後に、移行元のホストで実行
before_vm_migrate_destination	仮想マシンの移行の前に、移行先のホストで実行
after_vm_migrate_destination	仮想マシンの移行の後に、移行先のホストで実行
after_vm_destroy	仮想マシンを破棄した後
before_vdsm_start	ホストで VDSM が起動する前。 before_vdsm_start フックは root ユーザーとして実行され、VDSM プロセスの環境は継承しない。
after_vdsm_stop	ホストで VDSM が停止した後。 after_vdsm_stop フックは root ユーザーとして実行され、VDSM プロセスの環境は継承しない。
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アンプラグされる前
after_nic_hotunplug	NIC が仮想マシンからホットアンプラグされた後

名前	説明
after_nic_hotplug_fail	仮想マシンへの NIC のホットプラグが失敗した後
after_nic_hotunplug_fail	仮想マシンからの NIC のホットアンプラグが失敗した後
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ホットアンプラグされる前
after_disk_hotunplug	ディスクが仮想マシンからホットアンプラグされた後
after_disk_hotplug_fail	仮想マシンへのディスクのホットプラグが失敗した後
after_disk_hotunplug_fail	仮想マシンからのディスクのホットアンプラグが失敗した後
before_device_create	カスタムプロパティ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	デバイスの移行の前に、移行先のホストで実行
after_device_migrate_destination	デバイスの移行の後に、移行先のホストで実行
before_device_migrate_source	デバイスの移行の前に、移行元のホストで実行
after_device_migrate_source	デバイスの移行の後に、移行元のホストで実行

名前	説明
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	ホストマシンの起動時にネットワークを設定する前

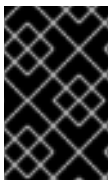
A.5. VDSM フックの環境

大半のフックスクリプトは、**vdsd** 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。例外となるのは、フックスクリプトが **before_vdsm_start** および **after_vdsm_stop** のイベントによってトリガーされた場合です。これらのイベントによってトリガーされたフックスクリプトは、**root** ユーザーとして実行され、VDSM プロセスの環境は継承しません。

A.6. VDSM フックドメインの XML オブジェクト

フックスクリプトが起動すると、`_hook_domxml` 変数が環境に追加されます。この変数には、libvirt ドメイン内の仮想マシンの XML 表現へのパスが含まれます。ただしこのルールには、以下に示すようにいくつかの例外があります。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

現在、**before_migration_destination** と **before_dehibernation** のフックは、移行元のホストからドメインの XML を受信します。移行先のドメインの XML には、さまざまな相違点が生じます。

VDSM は libvirt ドメイン XML 形式を使用して仮想マシンを定義します。libvirt ドメイン XML 形式についての詳細は、「[Domain XML format](#)」に記載されています。仮想マシンの UUID は、ドメイン XML から推定することができますが、環境変数 `vmld` としても提供されます。

A.7. カスタムプロパティの定義

Red Hat Virtualization Manager によって受け入れられ、カスタムフックに渡されるカスタムプロパティは、**engine-config** コマンドを使用して定義します。Red Hat Virtualization Manager がインストールされているホストで、**root** ユーザーとしてこのコマンドを実行してください。

UserDefinedVMProperties および **CustomDeviceProperties** の設定キーは、サポートされているカスタムプロパティの名前を保管するのに使用します。これら設定キーには、名付けられた各カスタムプロパティの有効な値を定義する正規表現も含まれます。

複数のカスタムプロパティは、セミコロンで区切ります。設定キーの設定時には、そのキーに含まれている既存の値が上書きされる点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を組み

合わせる場合には、キーの値を設定するのに使用するコマンドにすべてのカスタムプロパティーを入れる必要があります。

設定キーを更新した後は、**ovirt-engine** サービスを再起動して変更を有効にする必要があります。

例A.1 仮想マシンプロパティー: **smartcard** カスタムプロパティーの定義

1. 以下のコマンドを使用して、**UserDefinedVMProperties** 設定キーによって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 UserDefinedVMProperties
```

以下の出力に示されているように、カスタムプロパティー **memory** はすでに定義済みです。正規表現 **^[0-9]+\$** により、カスタムプロパティーに数字のみが含まれるようになっています。

```
# 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** 設定キーですすでに定義済みなので、そこに新規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 **smartcard** は、設定キーの値に追加します。新規カスタムプロパティーには、**true** または **false** の値を適用することができます。

```
# engine-config -s UserDefinedVMProperties='memory=^[0-9]+$;smartcard=^(true|false)$' --cver=4.0
```

3. **UserDefinedVMProperties** 設定キーで定義されているカスタムプロパティーが正しく更新されたかどうかを確認します。

```
# 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、**ovirt-engine** サービスを再起動して、変更を有効にします。

```
# 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

1. 以下のコマンドを使用して、**CustomDeviceProperties** 設定キーによって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ているように、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
```

2. **interface** カスタムプロパティは、まだ存在していないので、そのまま追加することができます。以下の例では、**speed** サブプロパティの値は 0 から 99999 までの範囲に設定し、**duplex** サブプロパティの値には **full** または **half** のいずれかを選択して設定します。

```
# engine-config -s CustomDeviceProperties="{type=interface;prop={speed=^[0-9]{1,5}};$duplex=^(full|half)$}" --cver=4.0
```

3. **CustomDeviceProperties** 設定キーで定義されているカスタムプロパティが正しく更新されたかどうかを確認します。

```
# 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
```

4. 最後に、**ovirt-engine** サービスを再起動して、変更を有効にします。

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

A.8. 仮想マシンのカスタムプロパティの設定

Red Hat Virtualization Manager でカスタムプロパティを定義した後は、それらを仮想マシンで設定することができます。カスタムプロパティは、管理ポータル **新規仮想マシン** および **仮想マシンの編集** ウィンドウの **カスタムプロパティ** タブで設定します。

また、**仮想マシンの実行** ウィンドウでカスタムプロパティを設定することも可能です。**仮想マシンの実行** ウィンドウで設定するカスタムプロパティは、その仮想マシンが次回シャットダウンされるまでの間にしか適用されません。

カスタムプロパティ タブは、定義済みのカスタムプロパティ一覧から選択する機能を提供します。カスタムプロパティ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することができます。キー/値のペアを追加するには **+** ボタンをクリックします。また削除する場合には **-** ボタンをクリックします。

A.9. VDSM フックの仮想マシンカスタムプロパティの評価

仮想マシンの **カスタムプロパティ** フィールドに設定される各キーは、フックスクリプトを呼び出す際の環境変数として追加されます。**カスタムプロパティ** フィールドの検証に使用される正規表現は、ある程度の保護を提供しますが、スクリプトによって、提供されている入力が適切であることを確認するようにはする必要があります。

例A.3 カスタムプロパティの評価

以下の例は、カスタムプロパティ **key1** の有無を確認するための短い Python スクリプトです。このカスタムプロパティが設定されている場合には、標準エラーにその値が出力されます。このカスタムプロパティが設定されていない場合は、何も起こりません。

```
#!/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 フッキングモジュールの使用方法

VDSM は Python フッキングモジュールと共に出荷され、VDSM フックスクリプトのヘルパー機能を提供します。このモジュールは、一例として提供されているもので、Python で書かれた VDSM フックにのみ適切です。

フッキングモジュールは、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ています。これにより、フックスクリプトが Python の組み込み **xml.dom** ライブラリー (<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することができます。

変更されたオブジェクトは、フッキングモジュールを使用して再度 libvirt XML に保存することができます。フッキングモジュールは、以下のような関数を提供して、フック開発をサポートします。

表A.2 フッキングモジュールの関数

名前	引数	説明
tobool	文字列	「true」または「false」の文字列をブール値に変換します。
read_domxml	-	仮想マシンの libvirt XML を DOM オブジェクトに読み取ります。
write_domxml	DOM オブジェクト	仮想マシンの libvirt XML を DOM オブジェクトから書き込みます。

A.11. VDSM フックの実行

before_vm_start スクリプトは、libvirt に達する前に、ドメイン XML を編集して仮想マシンの VDSM の定義を変更することができます。これを実行する際には、注意を払う必要があります。フックスクリプトは、VDSM の操作を妨げる可能性があり、スクリプトにバグがある場合には、Red Hat Virtualization 環境が停止してしまう可能性があります。特に、ドメインの UUID は決して変更しないでください。また、十分な予備知識なしには、ドメインからのデバイスの削除を試みないでください。

before_vdsm_start と **after_vdsm_stop** のフックスクリプトは、**root** ユーザーとして実行されます。システムへの **root** アクセスが必要なその他のフックスクリプトは、**sudo** コマンドで root 権限が使用

できるように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、**vds****m** 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。フックスクリプトは非対話的に実行されるため、このように設定しなければなりません。

例A.4 VDSM フックの **sudo** 設定

以下の例では、**vds****m** ユーザーが **root** として **/bin/chown** コマンドを実行できるように **sudo** コマンドを設定します。

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. ファイルに以下の行を追加します。

```
vds m ALL=(ALL) NOPASSWD: /bin/chown
```

これは、**vds****m** ユーザーが **root** ユーザーとして **/bin/chown** コマンドを実行できるように指定しています。また、**NOPASSWD** パラメーターは、**sudo** を呼び出す際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。

この設定ファイルが変更された後には、VDSM フックは **sudo** コマンドを使用して **root** として **/bin/chown** を実行することができるようになります。以下の Python コードは、**sudo** を使用して、**/my_file** ファイル上で **root** として **/bin/chown** を実行します。

```
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、フックスクリプトのデバッグに使用されます。

A.12. VDSM フックのリターンコード

フックスクリプトは、表A.3「フックのリターンコード」に記載したリターンコードのいずれか 1 つを返す必要があります。このリターンコードによって、VDSM がさらなるフックスクリプトを処理するかどうかが決まります。

表A.3 フックのリターンコード

コード	説明
0	フックスクリプトが正常に終了しました。
1	フックスクリプトが失敗し、他のフックを処理する必要があります。
2	フックスクリプトが失敗し、他のフックを処理する必要はありません。
>2	予備

A.13. VDSM フックの例

Red Hat は、このセクションに記載したフックスクリプトの例を厳密にはサポートしていません。システムにインストールするフックスクリプトは、ソースを問わず、いずれもご使用の環境で徹底的にテスト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は、**numaset** カスタムプロパティーに基づいた NUMA ホスト上におけるメモリ割り当ての調整を可能にします。カスタムプロパティーが設定されていない場合には、何も起こりません。

設定の文字列:

```
numaset=^(interleave|strict|preferred):[\^]?d+(-d+)?(,[\^]?d+(-d+)?)*$
```

正規表現を使用して、特定の仮想マシンの **numaset** カスタムプロパティーで割り当てモード (**interleave**、**strict**、**preferred**) と使用するノードの両方を指定することができます。2つの値は、コロン(:)で区切ります。正規表現により、**nodeset** を以下のように指定することができます。

- 特定のノード (**numaset=strict:1** で、ノード 1 のみを使用するように指定)
- 使用するノードの範囲 (**numaset=strict:1-4** で、ノード 1 から 4 までを使用するように指定)
- 特定のノードを使用しない (**numaset=strict:^3** で、ノード 3 を使用しないように指定)
- コンマ区切りで記述した、上記のいずれかの組み合わせ (**numaset=strict:1-4,6** で、ノード 1 から 4 までと、6 を使用するように指定)

スクリプト:

/usr/libexec/vdsm/hooks/before_vm_start/50_numa

```
#!/usr/bin/python

import os
import sys
import hooking
import traceback

...

numa hook
=====
add numa support for domain xml:

<numatune>
    <memory mode="strict" nodeset="1-4,^3" />
</numatune>

memory=interleave|strict|preferred
```

```
numaset="1" (use one NUMA node)
numaset="1-4" (use 1-4 NUMA nodes)
numaset="^3" (don't use NUMA node 3)
numaset="1-4,^3,6" (or combinations)

syntax:
    numa=strict:1-4
    ...

if os.environ.has_key('numa'):
    try:
        mode, nodeset = os.environ['numa'].split(':')

        domxml = hooking.read_domxml()

        domain = domxml.getElementsByTagName('domain')[0]
        numas = domxml.getElementsByTagName('numatune')

        if not len(numas) > 0:
            numatune = domxml.createElement('numatune')
            domain.appendChild(numatune)

            memory = domxml.createElement('memory')
            memory.setAttribute('mode', mode)
            memory.setAttribute('nodeset', nodeset)
            numatune.appendChild(memory)

            hooking.write_domxml(domxml)
        else:
            sys.stderr.write('numa: numa already exists in domain xml')
            sys.exit(2)
    except:
        sys.stderr.write('numa: [unexpected error]: %s\n' %
            traceback.format_exc())
        sys.exit(2)
```

付録B カスタムのネットワークプロパティー

B.1. BRIDGE_OPTS パラメーター

表B.1 bridge_opts パラメーター

パラメーター	説明
forward_delay	ブリッジがリッスンして状態を学習するのに費やす時間をデシ秒単位で設定します。この時間内にスイッチンググループが見つからなかった場合には、ブリッジは転送状態に入ります。これにより、通常のネットワーク操作を行う前にトラフィックと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時間をデシ秒単位で設定します。この時間が経過すると、転送のデータベースがチェックされ、タイムアウトのエントリーが消去されます。
group_addr	一般的なクエリーの送信時にゼロに設定されます。グループ固有またはグループおよびソース固有のクエリーの送信時には、IP マルチキャストアドレスに設定されます。
group_fwd_mask	転送リンクのローカルグループアドレスへのブリッジを有効にします。この値をデフォルトから変更すると、ブリッジングの動作が通常とは異なるようになります。
hash_elasticity	ハッシュテーブルで許容されるチェーンの最大長。次の新規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。リハッシュ後にこの条件が満たされないと、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	ハッシュテーブル内のバケットの最大量。この設定は直ちに有効になり、現在のマルチキャストグループエントリー数よりも少ない値には設定できません。値は2の累乗である必要があります。
hello_time	ネットワークトポロジー内のブリッジの位置をアナウンスする「hello」メッセージを送信する間隔をデシ秒単位で設定します。このブリッジが Spanning Tree ルートブリッジの場合にのみ適用します。
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	「hello」メッセージを別のルートブリッジから受信する最大時間をデシ秒単位で設定します。この時間を超えると、ブリッジは動作していないと見なされ、引き継ぎが開始します。
multicast_last_member_count	ホストから「leave group」メッセージを受信した後にマルチキャストグループに送信される「last member」クエリーの数を設定します。
multicast_last_member_interval	「last member」クエリーの間隔時間をデシ秒単位で設定します。
multicast_membership_interval	ブリッジが、マルチキャストグループのメンバーからの通信を待つ時間をデシ秒単位で設定します。この時間が経過すると、ホストに対するマルチキャストトラフィックの送信を停止します。
multicast_querier	ブリッジがマルチキャストクエリア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「multicast host membership」のクエリーを受信すると、クエリーの受信時間とマルチキャストクエリーの間隔時間に基づいてホストがトラッキングされます。ブリッジが後でそのマルチキャストメンバーシップ向けのトラフィックの送信を試みる場合や、クエリーマルチキャストルーターと通信している場合には、このタイマーによりそのクエリアーが有効であることを確認します。有効な場合には、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を使用して配信されます。有効でない場合には、トラフィックは全ブリッジポートから送信されます。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、またはマルチキャストメンバーシップを予定しているブロードキャストドメインは、パフォーマンス向上のためにはマルチキャストクエリアーを少なくとも1つ実行すべきです。
multicast_querier_interval	ホストから「multicast host membership」クエリーを最後に受信して、それが有効であることを確認した後の最大時間をデシ秒単位で設定します。
multicast_query_use_ifaddr	ブール値。デフォルトでは「0」に設定され、その場合にはクエリアーが0.0.0.0をIPv4メッセージのソースアドレスとして使用します。この設定を変更すると、ブリッジのIPがソースアドレスとして設定されます。

パラメーター	説明
<code>multicast_query_interval</code>	ブリッジが送信するクエリーの間隔をデシ秒単位で設定し、マルチキャストメンバーシップの有効性を確保します。この時点またはブリッジがメンバーシップについてのマルチキャストクエリーを送信するように要求されている場合には、チェックが要求された時間に加えて <code>multicast_query_interval</code> に基づいてブリッジは自分のマルチキャストクエリアーをチェックします。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 <code>multicast_query_interval</code> 内に送信されている場合には、再送信されません。
<code>multicast_query_response_interval</code>	クエリーが送信されてからホストが応答するまでの時間 (デシ秒単位)。 <code>multicast_query_interval</code> の値以下である必要があります。
<code>multicast_router</code>	マルチキャストルーターにアタッチするポートを有効化/無効化することができます。1 つ以上のマルチキャストルーターがアタッチされたポートは、全マルチキャストトラフィックを受信します。値を 0 に指定すると完全に無効化され、1 に指定するとシステムはクエリーに基づいてルーターの有無を検知することができるようになります。また、値を 2 に指定すると、全マルチキャストトラフィックを常に受信できるようになります。
<code>multicast_snooping</code>	スヌーピングの有効化/無効化を切り替えます。スヌーピングにより、ブリッジがルーターとホスト間のトラフィックをリッスンして、適切なリンクにマルチキャストトラフィックをフィルタリングするマップを維持します。このオプションにより、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スヌーピングを再度有効化することができます。ただし、そのハッシュの競合が解決されていない場合には再度有効化されません。
<code>multicast_startup_query_count</code>	起動時にメンバーシップ情報を確認するために送信されるクエリーの件数を設定します。
<code>multicast_startup_query_interval</code>	起動時にメンバーシップ情報を確認するために送信されるクエリーの間隔時間をデシ秒単位で設定します。

B.2. RED HAT VIRTUALIZATION MANAGER で ETHTOOL を使用するための設定方法

管理ポータルから、ホストのネットワークインターフェースカードに `ethtool` のプロパティーを設定することができます。**`ethtool_opts`** キーはデフォルトでは利用できないので、`engine` 設定ツールを使用して Manager に追加する必要があります。ホストには、必須の 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。

Manager への `ethtool_opts` キーの追加

1. 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
```

2. `ovirt-engine` サービスを再起動します。

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

3. Ethtool のプロパティ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。このパッケージは、Red Hat Virtualization Host ではデフォルトで利用可能ですが、Red Hat Enterprise Linux ホストにはインストールする必要があります。

```
# yum install vds-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` のプロパティを論理ネットワークに適用するには、「[ホストネットワークインターフェー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. RED HAT VIRTUALIZATION MANAGER で FCOE を使用するための設定方法

管理ポータルから、ホストのネットワークインターフェースカードの Fibre Channel over Ethernet (FCoE) プロパティを設定することができます。`fcoe` キーはデフォルトでは利用できないので、`engine` 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すると、`fcoe` がすでに有効化されているかどうかを確認することができます。

```
# engine-config -g UserDefinedNetworkCustomProperties
```

必須の VDSM フックパッケージをホストにインストールする必要があります。ホストの FCoE カードに応じて、特別な設定が必要となる場合もあります。『[Red Hat Enterprise Linux ストレージ管理ガイド](#)』の「[ファイバーチャネルオーバーイーサネットインターフェースの設定](#)」を参照してください。

Manager への `fcoe` キーの追加

1. 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),?)*$'
```

2. `ovirt-engine` サービスを再起動します。

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

3. FCoE のプロパティを設定する各 Red Hat Enterprise Linux ホストに VDSM フックのパッケージをインストールします。このパッケージは、Red Hat Virtualization Host (RHVH) ではデフォルトで提供されます。

```
# yum install vds-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 のプロパティを論理ネットワークに適用するには、「[ホストネットワークインターフェー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 のユーザーインターフェース プラグイン

C.1. RED HAT VIRTUALIZATION のユーザーインターフェースプラグイン

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、他のシステムと容易に統合することができます。各インターフェースプラグインは、管理ポータルを介して Red Hat Virtualization で使用するためにパッケージおよび配布することができるユーザーインターフェース拡張機能セットを提供します。

Red Hat Virtualization のユーザーインターフェースプラグインは、JavaScript プログラミング言語を使用して、クライアント上で直接管理ポータルに統合します。プラグインは、管理ポータルによって呼び出され、Web ブラウザーの JavaScript ランタイムで実行されます。ユーザーインターフェースプラグインは、JavaScript 言語とそのライブラリーを使用することができます。

ランタイム中のキーイベントにおいて、管理ポータルは、管理ポータル/プラグイン間の通信を提供するイベントハンドラー関数を使用して個別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、その実装に関連した関数のみを宣言します。管理ポータルでプラグインを使用する前に、各プラグインは、関連するイベントハンドラー関数をプラグインの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ースの拡張機能を駆動する、プラグイン/管理ポータル間の通信を円滑化するために、管理ポータルはプラグインの API をグローバル (最上位) の pluginApi JavaScript オブジェクトとして公開し、個々のプラグインが使用できるようにします。各プラグインは、別個の pluginApi インスタンスを取得するので、管理ポータルは、プラグインのライフサイクルに応じて、各プラグインのプラグイン API 関数の呼び出しを制御することができます。

C.2. RED HAT VIRTUALIZATION ユーザーインターフェースプラグインの ライフサイクル

C.2.1. Red Hat Virtualization ユーザーインターフェースプラグインのライフサイクル

ユーザーインターフェースプラグインの基本ライフサイクルは次の 3 つの段階に分かれます。

- プラグインの検出
- プラグインの読み込み
- プラグインのブートストラッピング

C.2.2. Red Hat Virtualization ユーザーインターフェースプラグインの検出

プラグインの検出プロセスの第 1 ステップは、プラグイン記述子の作成です。プラグイン記述子には重要なプラグインメタデータとオプションのデフォルトプラグイン固有の設定が含まれます。

管理ポータルの HTML ページ要求 (HTTP GET) 処理の一環として、ユーザーインターフェースプラグインの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の検出と読み込みを試みます。各プラグイン記述子に対して、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設定 (存在する場合) を上書きして、プラグインのランタイムの振る舞いを修正するのに使用される、対応するプラグインユーザー設定の読み込みも試みます。プラグインユーザー設定はオプションです。記述子および対応するユーザー設定ファイルを読み込んだ後には、oVirt Engine がユーザーインターフェースプラグインのデータを集約し、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、プラグインの記述子は `$ENGINE_USR/ui-plug-ins` に保管されており、デフォルトマッピングは oVirt Engine のローカル設定で定義されている `ENGINE_USR=/usr/share/ovirt-engine` です。プラグイン記述子は JSON 形式の仕様に準拠する必要がありますが、これに加えて、Java/C++ 形式のコメント (`/*` と `//` の両種) も可能です。

デフォルトでは、プラグインユーザー設定ファイルは `$ENGINE_ETC/ui-plug-ins` に保管されており、デフォルトのマッピングは oVirt Engine のローカル設定で定義されている `ENGINE_ETC=/etc/ovirt-engine` です。プラグイン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ルールを順守する必要があります。



注記

プラグイン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 ユーザーインターフェースプラグインの読み込み

プラグインが検出され、そのデータが管理ポータル HTML ページに埋め込まれた後に、管理ポータルはアプリケーション起動の一環としてそのプラグインの読み込みを試みます (アプリケーションの起動の一環として読み込まないように設定している場合を除く)。

管理ポータルは、検出されたプラグインごとに、そのホストページを読み込むのに使用する HTML `iframe` 要素を作成します。プラグインのホストページは、プラグインのブートストラッププロセスを開始するのに不可欠です。ブートストラッププロセスは、プラグインの `iframe` 要素に照らしてプラグインコードを評価するのに使用されます。ユーザーインターフェースプラグインのインフラストラクチャーは、ローカルシステムからサービスを提供するプラグインリソースファイル (例: プラグインのホストページ) をサポートします。プラグインのホストページは `iframe` 要素の中に読み込まれ、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を行います。

C.2.4. Red Hat Virtualization ユーザーインターフェースプラグインのブートストラッピング

標準的なプラグインブートストラップシーケンスは以下のような手順で構成されます。

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` インスタンスの取得
2. ランタイムプラグイン設定オブジェクトの取得 (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 の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開始するように通知

以下のコードスニペットは、上述の手順を実例として示しています。

```
// 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({
    // UiInit event handler function.
    UiInit: function() {
        // Handle UiInit 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ースプラグイン関連のファイルおよびその場所

表C.1 UI プラグイン関連のファイルおよびその場所

ファイル	場所	備考
プラグインの記述子ファイル (メタデータ)	<code>/usr/share/ovirt-engine/ui-plugins/my-plugin.json</code>	
プラグインのユーザー設定ファイル	<code>/etc/ovirt-engine/ui-plugins/my-plugin-config.json</code>	
プラグインのリソースファイル	<code>/usr/share/ovirt-enging/ui-plugins/<resourcePath>/PluginHostPage.html</code>	<code><resourcePath></code> は、プラグイン記述子内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ー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ースプラグインを作成します。

Hello World! プラグインのデプロイ

1. Manager の `/usr/share/ovirt-engine/ui-plugins/helloWorld.json` に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"
}

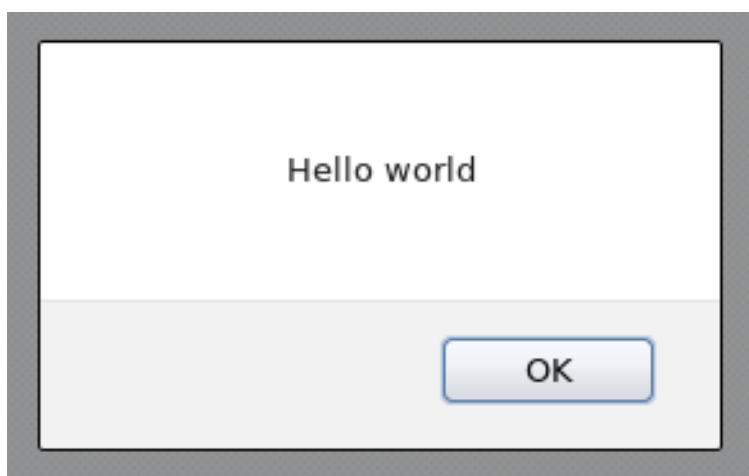
```

2. Manager の `/usr/share/ovirt-engine/ui-plugins/hello-files/start.html` に以下のファイルを作成して、プラグインのホストページを作成します。

```
<!DOCTYPE html><html><head>
<script>
  var api = parent.pluginApi('HelloWorld');
  api.register({
    UiInit: function() { window.alert('Hello world'); }
  });
  api.ready();
</script>
</head><body></body></html>
```

Hello World! プラグインの実装が正常に完了すると、管理ポータルへのサインイン時には以下のメッセージが画面が表示されます。

図C.1 Hello World! プラグインの実装完了



付録D RED HAT VIRTUALIZATION と SSL

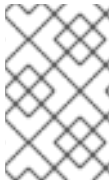
D.1. RED HAT VIRTUALIZATION MANAGER の SSL/TLS 証明書の変更



警告

/etc/pki ディレクトリーおよびサブディレクトリーのパーミッションと所有権は変更しないでください。**/etc/pki** ディレクトリーおよび **/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。

自分の組織のサードパーティー CA 証明書を使用し、HTTPS を介して Red Hat Virtualization Manager に接続するユーザーに対して Manager が信頼できるサイトであることを証明する場合には、以下の手順を使用します。



注記

HTTPS 接続用にサードパーティー CA 証明書を使用しても、Manager とホスト間の認証に使用される証明書は影響を受けません。Manager によって生成された自己署名証明書が引き続き使用されます。

前提条件

- サードパーティー 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、**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なければなりません。チェーンの順序は重要で、直近の中間証明書からルート証明書まで続いている必要があります。以下の手順では、サードパーティー CA 証明書が **/tmp/3rd-party-ca-cert.pem** として提供されているものとします。
- Apache httpd に使用する秘密鍵 (パスワードが設定されていないこと)。以下の手順では、**/tmp/apache.key** として保管されているものとします。
- CA の発行した証明書。以下の手順では、**/tmp/apache.cer** として保管されているものとします。

CA から秘密鍵と証明書を P12 ファイルで受け取っている場合は、以下の手順を使用して抽出します。その他のファイル形式については、CA に問い合わせてください。秘密鍵と証明書を抽出したら、「[Red Hat Virtualization Manager Apache SSL 証明書の置き換え](#)」に進みます。

P12 バンドルからの証明書と秘密鍵の抽出

内部 CA では、内部で生成した鍵および証明書が **P12** ファイルとして **/etc/pki/ovirt-engine/keys/apache.p12** に保管されます。Red Hat では、新しいファイルを同じ場所に保管することを推奨します。以下の手順では、新しい **P12** ファイルを **/tmp/apache.p12** と仮定しています。

1. 現在の **apache.p12** ファイルのバックアップを作成します。

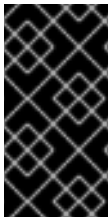
```
# cp -p /etc/pki/ovirt-engine/keys/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12.bck
```

2. 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. 秘密鍵および証明書を所定の場所に抽出します。ファイルがパスワードで保護されている場合は、**-passin pass:_password_** を追加する必要があります (**password** を実際のパスワードに置き換えてください)。

```
# 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の場合には、以下の手順の全ステップを完了する必要があります。商用署名入り証明書が設定された Red Hat Enterprise Virtualization 3.6 環境からアップグレードした場合は、ステップ 1、8、9 を実行する必要があります。

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** へのシンボリックリンクである **/etc/pki/ovirt-engine/apache-ca.pem** を使用するように設定されているので、この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. 既存の秘密鍵および証明書のバックアップを作成します。

```
# 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. 秘密鍵を所定の場所にコピーします。

```
# cp /tmp/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
```

6. 証明書を所定の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の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. `/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf` ファイルを編集します。

```
# vi /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf
```

以下に示す変更を加えてファイルを保存します。

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/apache-ca.pem
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```

10. `ovirt-engine` サービスを再起動します。

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

HTTPS トラフィックの暗号化に使用する証明書の信頼性についての警告が表示されることなく、管理ポータルおよび VM 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 Virtualization Manager と LDAP サーバーの間でセキュアな接続を設定するには、LDAP サーバーのルート CA 証明書を取得して、そのルート CA 証明書を Manager にコピーしてから、PEM エンコードされた CA 証明書を作成します。キーストアタイプには、任意の Java 対応タイプを使用することができます。以下の手順では、Java KeyStore (JKS) 形式を使用しています。



注記

PEM エンコードされた CA 証明書の作成およびインポートについての詳しい説明は、`/usr/share/doc/ovirt-engine-extension-aaa-ldap-version` にある 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。

PEM エンコード CA 証明書の作成

1. 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` を使用してそのルート CA 証明書をインポートし、PEM 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` にあるルート CA 証明書をインポートして PEM エンコードされた `myrootca.jks` という CA 証明書を `/etc/ovirt-engine/aaa/` 下に作成します。証明書の場合とパスワードを書き留めてください。対話型の設定ツールを使用する場合に必要な情報はこれですべてです。LDAP サーバーを手動で設定する場合には、残りの手順を実行して、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. 証明書の情報を使用して `/etc/ovirt-engine/aaa/profile1.properties` ファイルを更新します。



注記

`${local:_basedir}` は LDAP プロパティ設定ファイルの場所で、`/etc/ovirt-engine/aaa` ディレクトリーをポイントします。PEM エンコードされた CA 証明書を別のディレクトリーに作成した場合には、`${local:_basedir}` を証明書のフルパスに置き換えてください。

- startTLS を使用する場合 (推奨):

```
# 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 を使用する場合:

```
# 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、「[外部の LDAP プロバイダーの設定 \(対話式的設定\)](#)」を参照してください。シングルサインオンのための LDAP と Kerberos の設定を続行するには、「[シングルサインオンのための LDAP と Kerberos の設定](#)」を参照してください。

付録E ブランディング

E.1. ブランディング

E.1.1. Manager のブランド変更

Red Hat Virtualization Manager では、使用するアイコン、ポップアップウィンドウに表示されるテキスト、Welcome ページに表示されるリンクなどのさまざまな側面をカスタマイズすることが可能です。この機能により、Manager のブランドを変更して、管理者とユーザーに最終的に表示される外観をきめ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。このファイルは、グラフィカルユーザーインターフェースのスタイルを設定するのに使用する一式のカスケードスタイルシートと、Manager のさまざまなコンポーネントに取り入れられるメッセージやリンクが含まれたプロパティファイルの一式で構成されます。

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用のファイルを編集して変更を保存します。次回にそのコンポーネントを開いた時、またはリフレッシュした時に、変更が適用されます。

E.1.2. ログイン画面

ログイン画面は、管理ポータルと VM ユーザーポータルの両方で使用するログイン画面です。ログイン画面でカスタマイズが可能な要素は以下のとおりです。

- 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。

E.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と表示されるメインの画面です。管理ポータルの画面でカスタマイズが可能な要素は以下のとおりです。

- ロゴ
- 左側の背景画像
- 中央の背景画像
- 右側の背景画像
- ロゴの右側のテキスト

管理ポータルの画面のクラスは **web_admin.css** にあります。

E.1.4. VM ユーザーポータルの画面

VM ユーザーポータル画面は、VM ユーザーポータルにログインすると表示される画面です。VM ユーザーポータル画面でカスタマイズが可能な要素は以下のとおりです。

- ロゴ
- 中央の背景画像
- 右側の背景画像
- メイングリッドのボーダー
- ログインユーザー のラベルの上に表示されるテキスト

VM ユーザーポータル画面のクラスは **user_portal.css** にあります。

E.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、ホストや仮想マシンなどのエンティティを作成/編集/更新することができ、Manager 内の全ウィンドウです。ポップアップウィンドウでカスタマイズが可能な要素は以下のとおりです。

- ボーダー
- 左側のヘッダーイメージ
- 中央のヘッダーイメージ (反復)

ポップアップウィンドウのクラスは **common.css** にあります。

E.1.6. タブ

管理ポータルのポップアップウィンドウの多くにはタブが含まれます。これらのタブでカスタマイズが可能な要素は以下のとおりです。

- アクティブ
- 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。

E.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と最初に表示されるページです。テンプレートファイルを編集することによって、全体の外観をカスタマイズできる他、他のドキュメントや内部の Web サイトのリンクを追加することが可能です。Welcome ページでカスタマイズが可能な要素は以下のとおりです。

- ページのタイトル
- ヘッダー (左、中央、右)
- エラーメッセージ
- 転送先リンクとそのリンクに関するメッセージ

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 ページ用のテンプレートファイルは、**welcome_page.template** という名前の通常の HTML ファイルで、**HTML**、**HEAD**、**BODY** のタグは含まれていません。このファイルは、Welcome ページに直接挿入され、Welcome 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。このため、新規リンクを追加したり、コンテンツ自体を変更する場合には、このファイルを編集する必要があります。テンプレートファイルのもう 1 つの機能に、プレースホルダー (例: **{user_portal}**) があります。プレースホルダーは、Welcome ページが処理される際に **messages.properties** ファイル内の対応するテキストに置き換えられます。

E.1.8. 「ページが見つかりません」のページ

Red Hat Virtualization Manager で見つからないページへのリンクを開くと、「ページが見つかりません」のページが表示されます。「ページが見つかりません」のページでカスタマイズが可能な要素は以下のとおりです。

- ページのタイトル
- ヘッダー (左、中央、右)
- エラーメッセージ
- 転送先リンクとそのリンクに関するメッセージ

「ページが見つかりません」のページのクラスは、**welcome_style.css** にあります。

付録F システムアカウント

F.1. システムアカウント

F.1.1. Red Hat Virtualization Manager のユーザーアカウント

rhevm パッケージのインストール時には、Red Hat Virtualization をサポートするための複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。以下のシステムユーザーアカウントが作成されます。

- **vdsm** ユーザー (UID **36**)。NFS ストレージドメインのマウントやアクセスを行う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 **498**)。ゲストのシリアルコンソールに必要です。

F.1.2. Red Hat Virtualization Manager のグループ

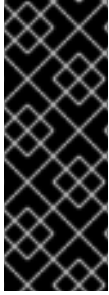
rhevm パッケージのインストール時には、Red Hat Virtualization をサポートするための複数のシステムユーザーグループが作成されます。各システムユーザーグループにはデフォルトのグループ ID (GID) があります。以下のシステムユーザーグループが作成されます。

- **kvm** グループ (GID **36**)。グループメンバーは以下のとおりです。
- **vdsm** ユーザー
- **ovirt** グループ (GID **108**)。グループメンバーは以下のとおりです。
- **ovirt** ユーザー
- **ovirt-vmconsole** グループ (GID **498**)。グループメンバーは以下のとおりです。
- **ovirt-vmconsole** ユーザー

F.1.3. 仮想化ホストのユーザーアカウント

vdsm および **qemu-kvm-rhev** パッケージのインストール時には、仮想化ホスト上に複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。以下のシステムユーザーアカウントが作成されます。

- **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 **498**)



重要

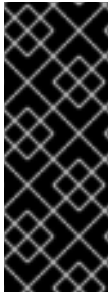
割り当てられるユーザー識別子 (UID) とグループ識別子 (GID) はシステムによって異なります。**vdsm** ユーザーの UID は **36** に、**kvm** グループの GID は **36** にそれぞれ固定されます。

システム上の別のアカウントで UID **36** または GID **36** をすでに使用している場合は、**vdsm** および **qemu-kvm-rhev** パッケージのインストール中に競合が発生します。

F.1.4. 仮想化ホストのグループ

vdsm および **qemu-kvm-rhev** パッケージのインストール時には、仮想化ホスト上に複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。以下のシステムユーザーグループが作成されます。

- **kvm** グループ (GID **36**)。グループメンバーは以下のとおりです。
- **qemu** ユーザー
- **sanlock** ユーザー
- **qemu** グループ (GID **107**)。グループメンバーは以下のとおりです。
- **vdsm** ユーザー
- **sanlock** ユーザー
- **ovirt-vmconsole** グループ (GID **498**)。グループメンバーは以下のとおりです。
- **ovirt-vmconsole** ユーザー



重要

割り当てられるユーザー識別子 (UID) とグループ識別子 (GID) はシステムによって異なります。**vdsm** ユーザーの UID は **36** に、**kvm** グループの GID は **36** にそれぞれ固定されます。

システム上の別のアカウントで UID **36** または GID **36** をすでに使用している場合は、**vdsm** および **qemu-kvm-rhev** パッケージのインストール中に競合が発生します。