Red Hat Virtualization 4.0

管理ガイド

Red Hat Virtualization の管理タスク

Last Updated: 2018-10-24

Red Hat Virtualization 4.0 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

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

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のシステムリソース全体のモニタリングと必要措置の実施 (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ーの管理
- 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

管理ポータルのヘッダーバーから **設定** ボタンをクリックして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場所が提供されます。

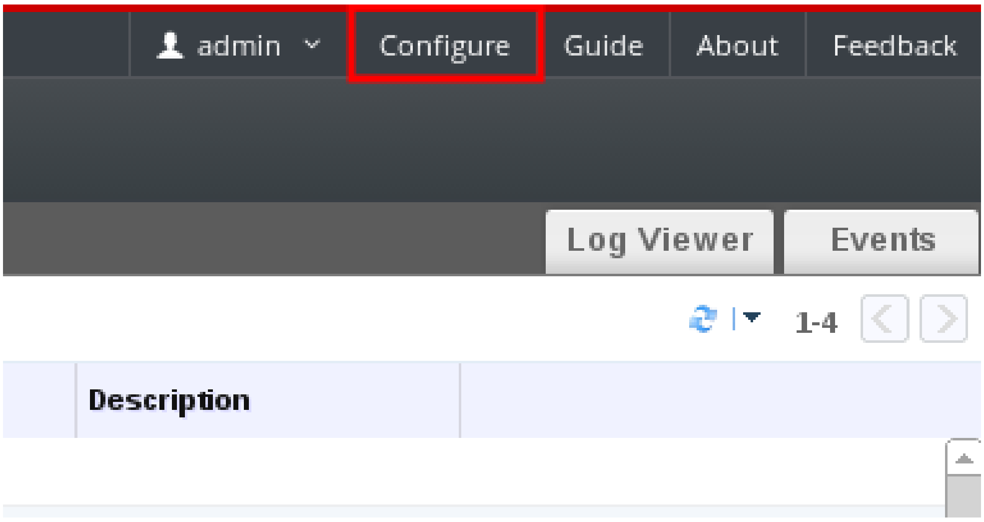


図1.1 設定ウィンドウへのアクセス

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、コンテナーオブジェクトに適用されるパーミッションは、そのコンテナー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、割り当てられたホストのみに対して、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。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。

手順1.1 新規ロールの作成

1. ヘッダーバーで **設定** ボタンをクリックすると **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. **新規作成** をクリックすると **新規ロール** のウィンドウが開きます。

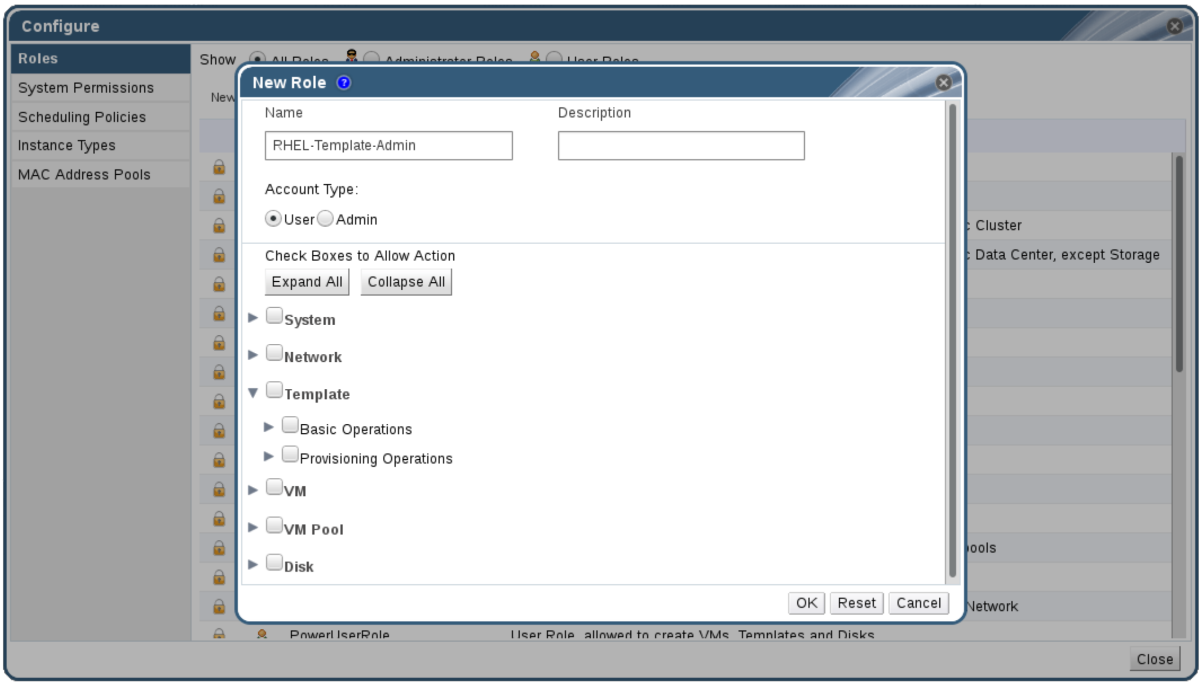


図1.2 新規ロールのウィンドウ

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。

手順1.2 ロールの編集とコピー

1. ヘッダーバーで **設定** ボタンをクリックすると **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** の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。

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、管理ポータルを使用してこれらのリソースを管理できますが、ユーザーポータルを介したアクセスは一切提供されません。

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、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したり、新規仮想ディスクなどのリソースを追加したり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際には、ストレージドメイン内での仮想マシンディスクイメージ作成など、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。

Chris は、この会社の仮想インフラストラクチャーのネットワークの管理に加えて、下級ネットワーク管理者の部下を 1 人監督しています。部下は、Pat という名前で、同社の社内研修部門用の小規模な仮想化環境を管理しています。Chris は、社内研修部門で使用する仮想マシンに対する **VnicProfileUser** パーミッションと **UserVmManager** パーミッションを Pat に付与しました。Pat はこれらのパーミッションを使用して、ユーザーポータル の **拡張** タブで、仮想マシンへのネットワークインターフェース追加など、簡単な管理タスクを実行することができますが、仮想マシンを実行しているホストのネットワークや、仮想マシンが属するデータセンターのネットワークを変更するパーミッションはありません。

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。

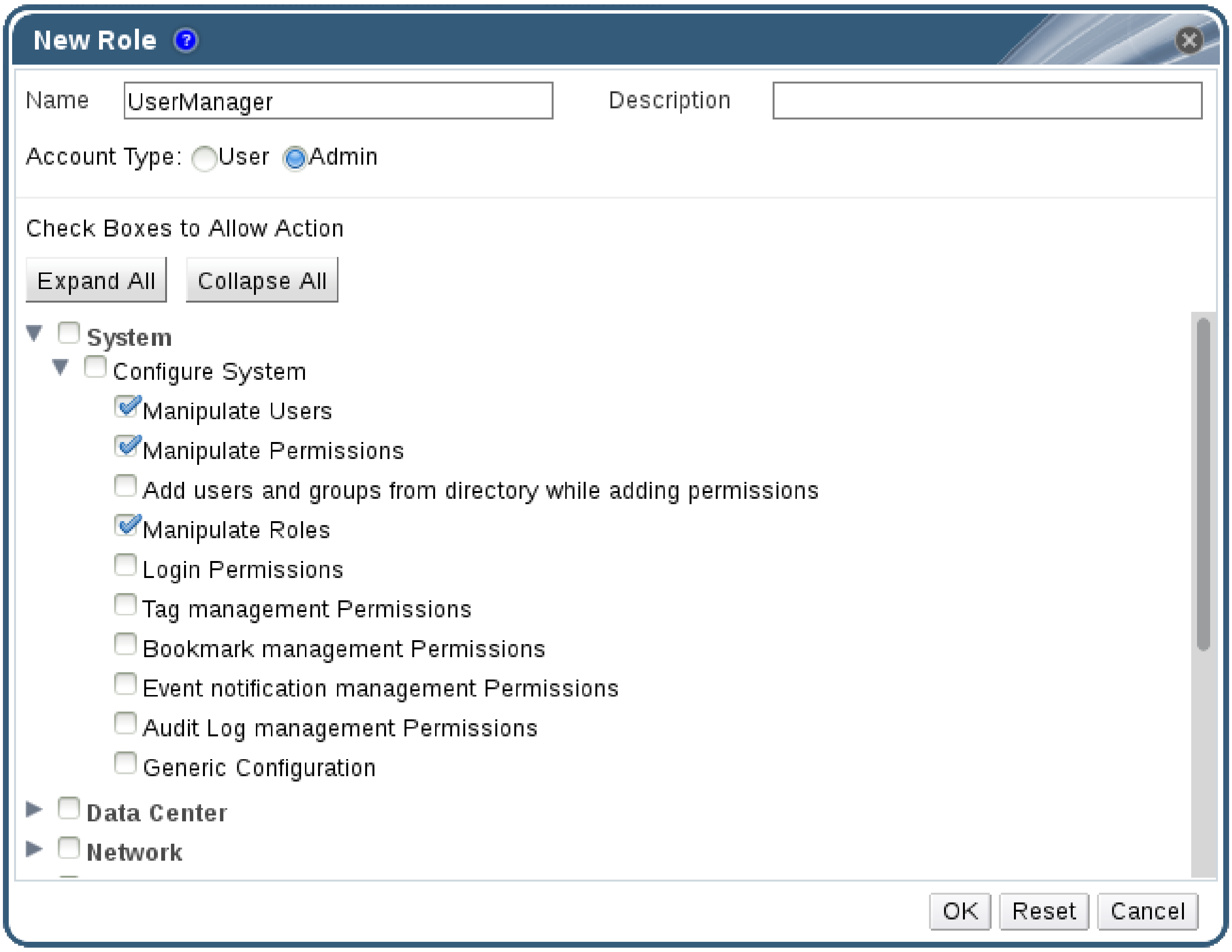


図1.3 UserManager のカスタムロール

> 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「UserManager のカスタムロール」 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、管理ポータルは使用できますが、ユーザーポータルは使用できないことになります。

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ーオブジェクトです。

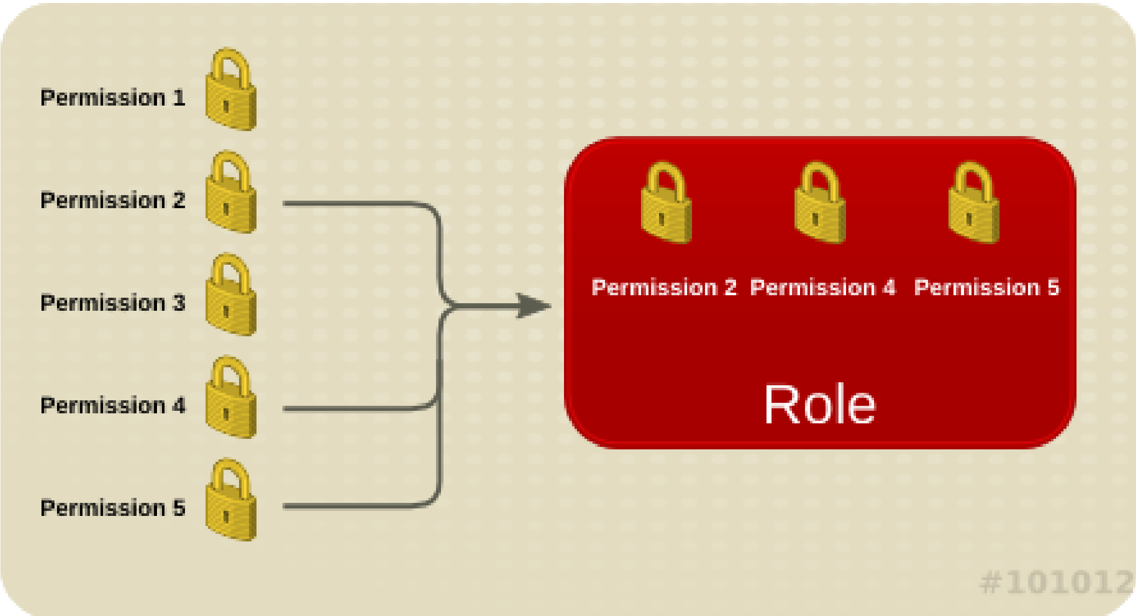


図1.4 パーミッッション & ロール

コンテナーオブジェクトに適用されるパーミッションは、そのコンテナーの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。

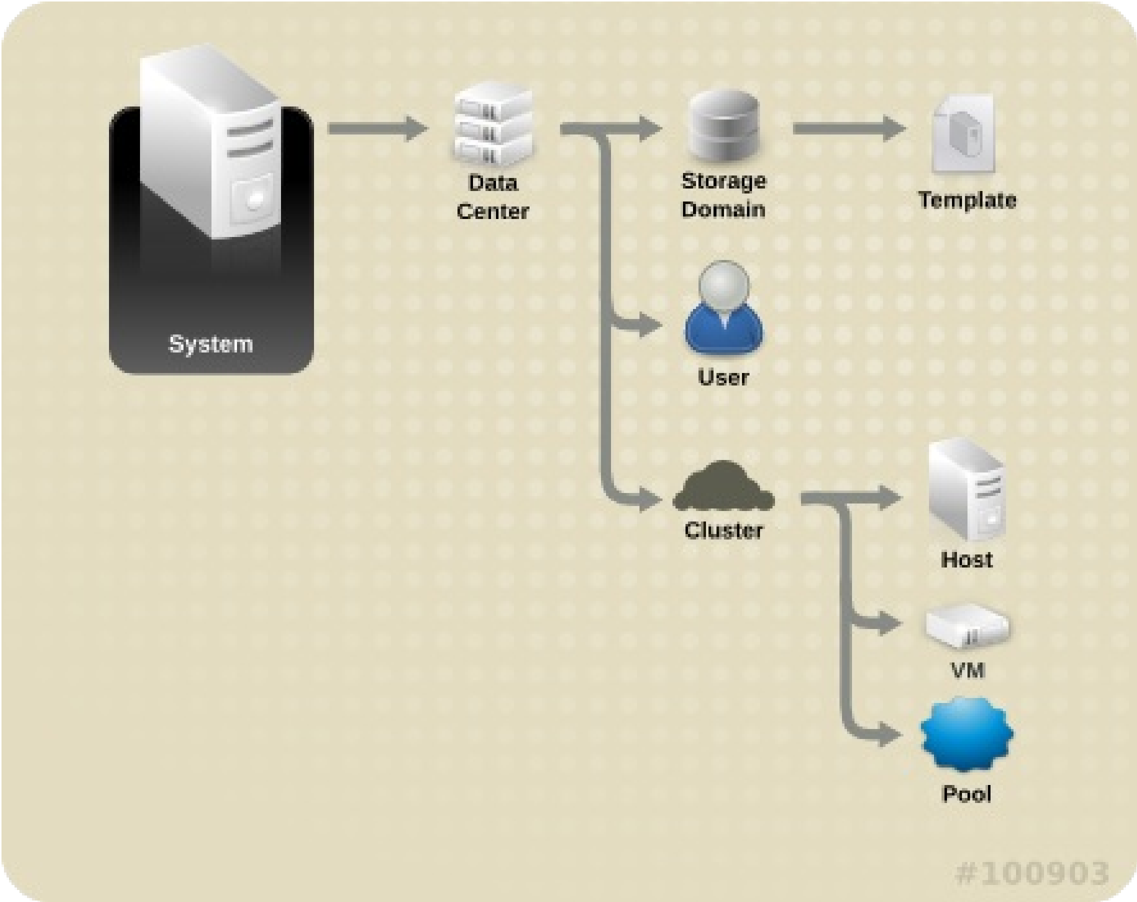


図1.5 Red Hat Virtualization のオブジェクト階層

1.2.1. ユーザーのプロパティー

ロールとパーミッションは、ユーザーのプロパティーです。ロールは、さまざまなレベルの物理/仮想リソースへ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、粒度の高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、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: **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、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、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。

たとえば、クラスターの **administrator** ロールが割り当てられている場合は、**管理ポータル** を使用してクラスター内の仮想マシンを管理することができますが、**ユーザーポータル** 内の仮想マシンには一切アクセスすることはできません。そのためには、**user** ロールが必要です。

1.2.3. ユーザーロール

以下の表には、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	特権	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。	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。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。このロールが割り当てられると、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	特権	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パーミッションは継承されます。

ロール	特権	備考
VmCreator	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** ウィンドウから全環境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に適用します。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。	このロールは個別のテンプレートに適用されません。**設定** ウィンドウを使用して、環境全体でこのロールをユーザーに適用します。または、特定のデータセンター、クラスター、ストレージドメインでこのロールを適用します。
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マシンディスクの作成/編集/管理/削除ができます。	このロールは個別の仮想ディスクに適用されません。環境全体で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ます。または、特定のデータセンター/ストレージドメインを対象にこのロールを適用します。
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に使用するユーザーを作成してください。

以下の表には、上級管理者ロールについての説明をまとめています。このロールが割り当てられると、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。

1.3. 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てこのロジックを決定します。Red Hat Virtualization Manager はデフォルトで **Evenly_Distributed**、**InClusterUpgrade**、**None**、**Power_Saving**、および **VM_Evenly_Distributed** の 5 つのポリシーを提供しますが、より高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。

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。

手順1.3 スケジューリングポリシーの作成

1. 管理ポータルのヘッダーバーで **設定** ボタンをクリックして **設定** ウィンドウを開きます。
2. **スケジューリングポリシー** をクリックしてスケジューリングポリシーのタブを表示します。
3. **新規作成** をクリックして **新規スケジューリングポリシー** ウィンドウを開きます。

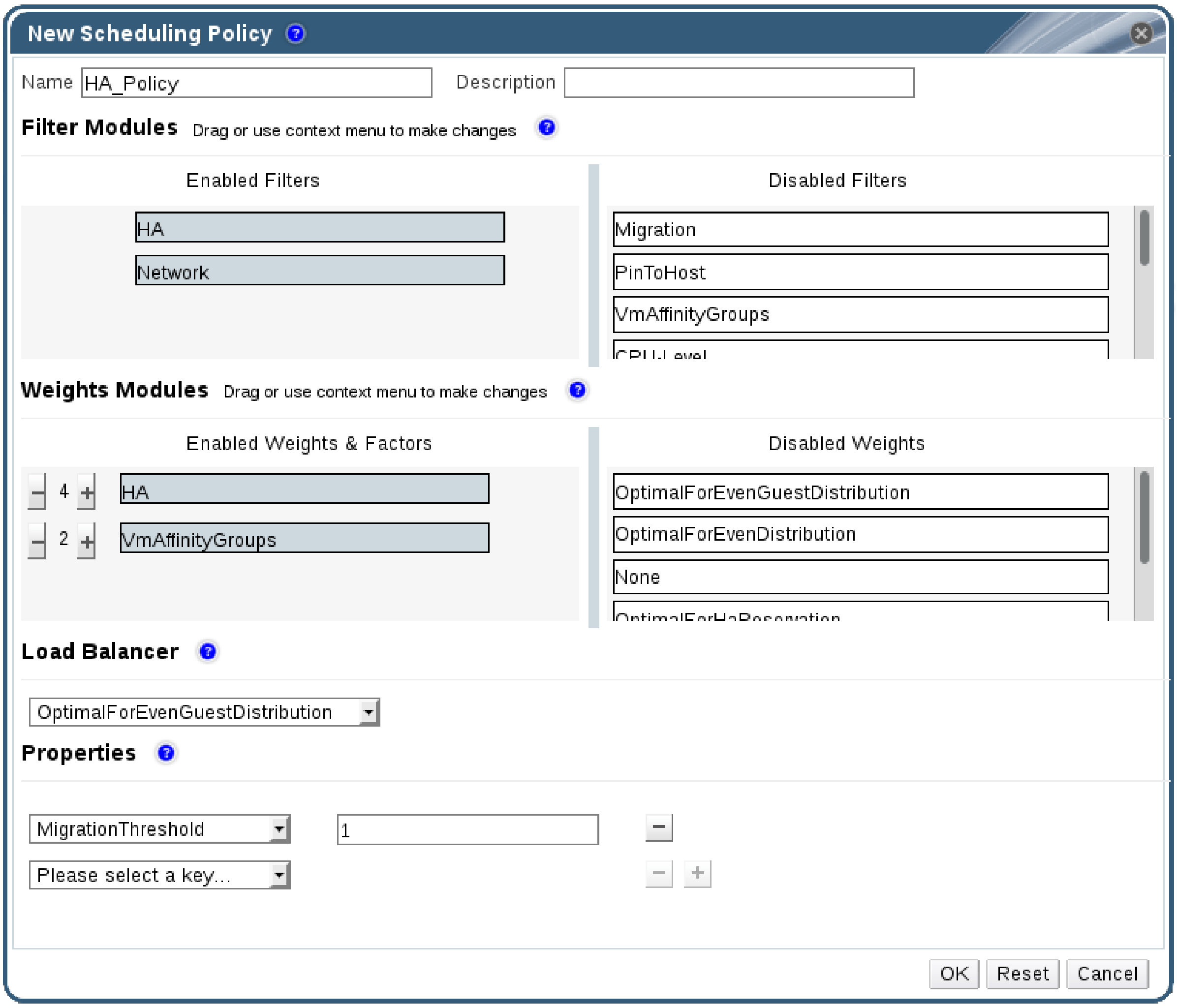


図1.6 新規スケジューリングポリシーウィンドウ

4. スケジューリングポリシーの **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＆ドロップします。

   b. 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して基本的な最適化を行うことも可能です。

      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＆ドロップします。

   b. 有効な加重値と係数の左側にある **+** 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のプロパティーを選択し、そのプロパティー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、プロパティーを追加/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** のウィンドウで使用できるオプションについての説明をまとめています。

表1.5 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は推奨されますが、必須ではありません。

<table>
<tr><th>フィールド名</th><th>説明</th></tr>
<tr><td>フィルターモジュール</td><td>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。
<code>CpuPinning</code>: CPU ピニングの定義を満たさないホスト
<code>Migration</code>: 同じホストへのマイグレーションを防ぎます。
<code>PinToHost</code>: 仮想マシンが固定されているホスト以外のホスト
<code>CPU-Level</code>: 仮想マシンの CPU トポロジーに対応しないホスト
<code>CPU</code>: 仮想マシンに割り当てられているよりも CPU 数が少ないホスト
<code>Memory</code>: 仮想マシンを実行するのに十分なメモリーがないホスト
<code>VmAffinityGroups</code>: アフィニティー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 つのアフィニティー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。
<code>InClusterUpgrade</code>: 仮想マシンを実行しているホストよりも古い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
<code>HostDevice</code>: 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
<code>HA</code>: ホストエンジンの仮想マシンが、高可用性スコアがポジティブのホストのみで実行されるように強制します。
<code>Emulated-Machine</code>: 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
<code>Network</code>: 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。
</td></tr>
</table>

フィールド名	説明
加重値モジュール	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 • **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古い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す。したがって、より新しい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。 • **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ー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、アフィニティーグループのパラメーターに応じて、アフィニティー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。 • **OptimalForPowerSaving**: 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。 • **OptimalForEvenDistribution**: 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。
ロードバランサー	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。

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に利用できます。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1.6 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。

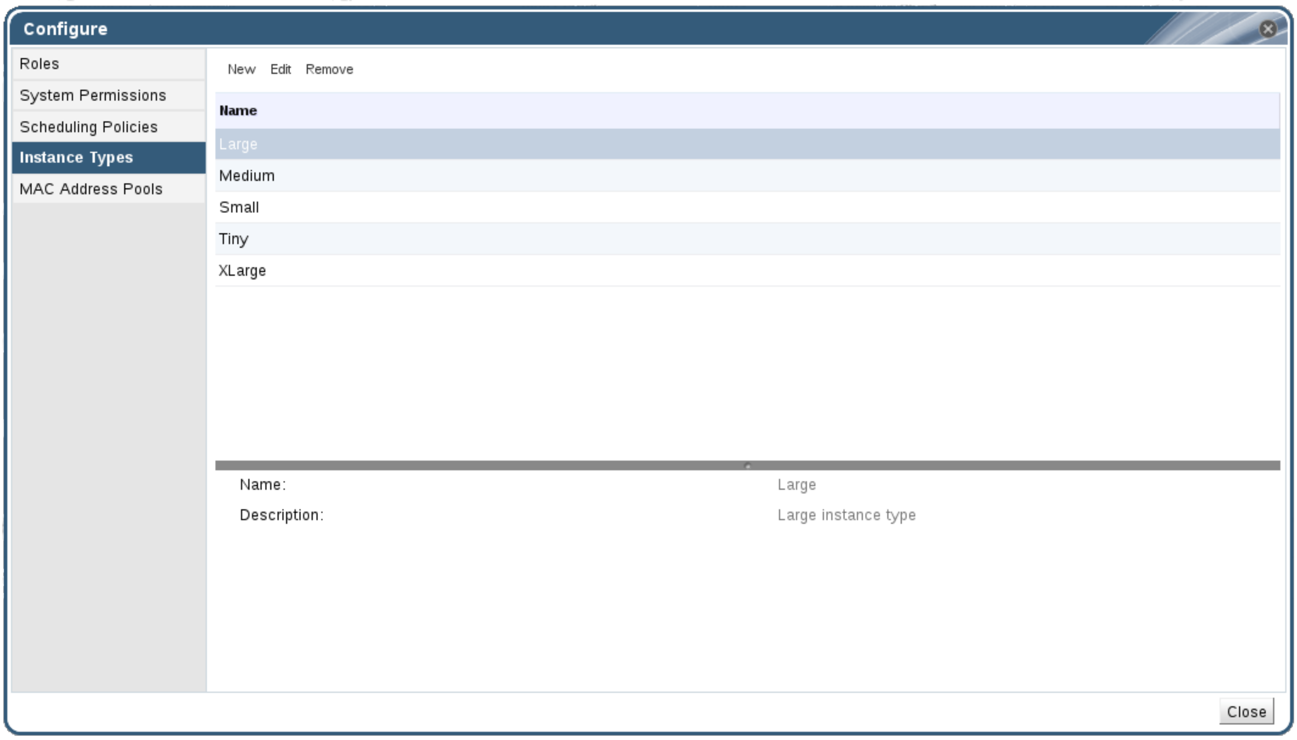


図1.7 インスタンスタイプのタブ

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。

手順1.4 インスタンスタイプの作成

1. ヘッダーバーで **設定** をクリックします。
2. **インスタンスタイプ** タブを開きます。
3. **新規** をクリックして、**新規インスタンスタイプ** ウィンドウを開きます。

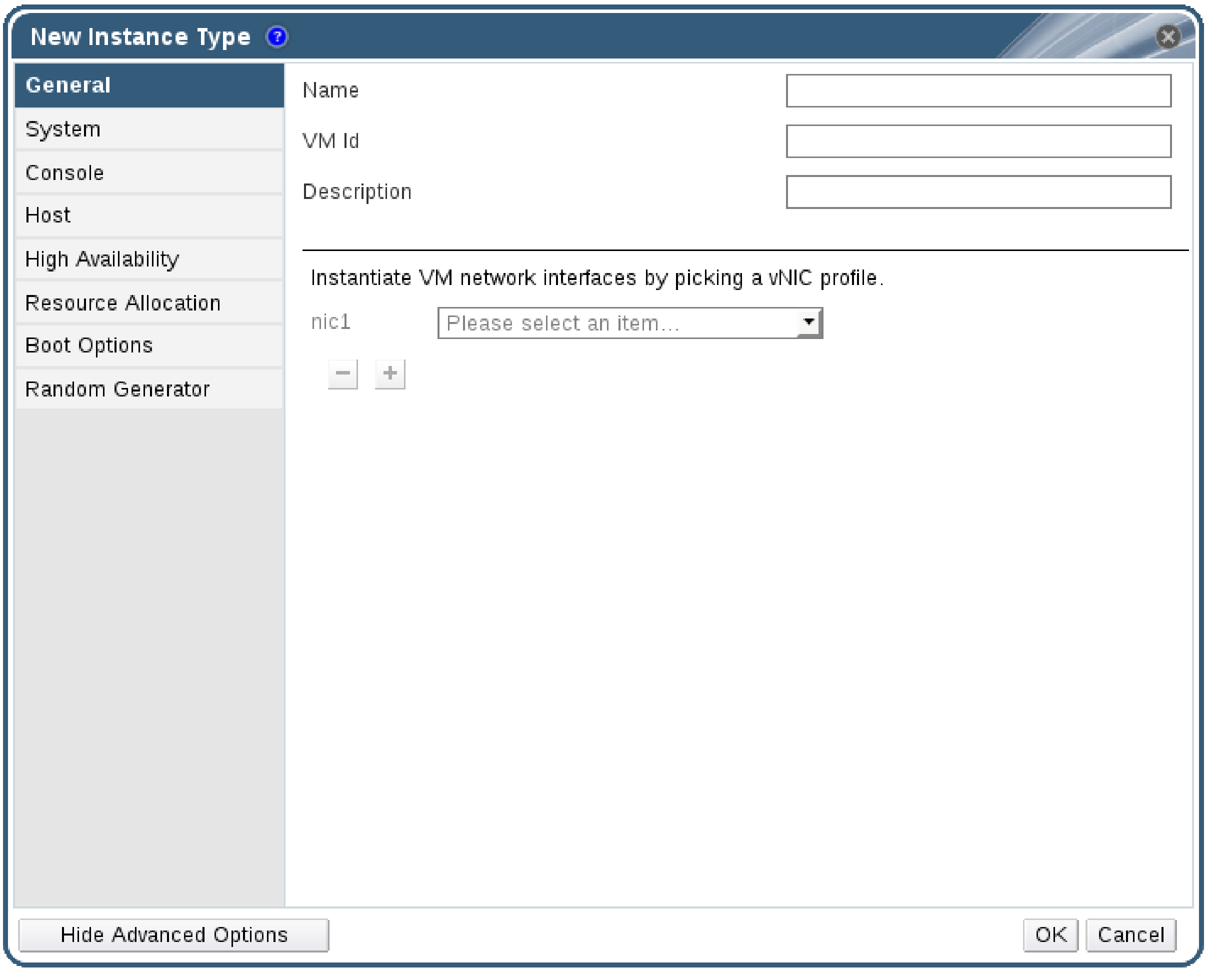


図1.8 新規インスタンスタイプのウィンドウ

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。

手順1.5 インスタンスタイプのプロパティーの編集

1. ヘッダーバーで **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** をクリックして **インスタンスタイプの編集** ウィンドウを開きます。

5. 必要に応じて設定を変更します。

6. **OK** をクリックします。

インスタンスタイプの設定が更新されます。このインスタンスタイプをベースとする新規仮想マシンと再起動された既存の仮想マシンが新規設定を使用するようになります。

1.4.3. インスタンスタイプの削除

手順1.6 インスタンスタイプの削除

1. ヘッダーバーで **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** をクリックして **インスタンスタイプの削除** ウィンドウを開きます。

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て OK をクリックします。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、MAC アドレスの範囲を定義します。MAC アドレスは、この範囲の中から各データセンターに割り当てられます。MAC アドレスプールは、各データセン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 つのデータセンターに関連するすべての MAC アドレスが、割り当て済みの 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データセンターで共有することができますが、各データセンターには単一の 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。データセンターへの MAC アドレスプールの割り当てに関する詳しい情報は、「新しいデータセンターの作成」を参照してください。

MAC アドレスプールは、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。

手順1.7 MAC アドレスプールの作成

1. ヘッダーバーで **設定** ボタンをクリックして **設定** ウィンドウを開きます。
2. **MAC アドレスプール** タブをクリックします。
3. **追加** ボタンをクリックして、**MAC アドレスプールの新規作成** ウィンドウを開きます。

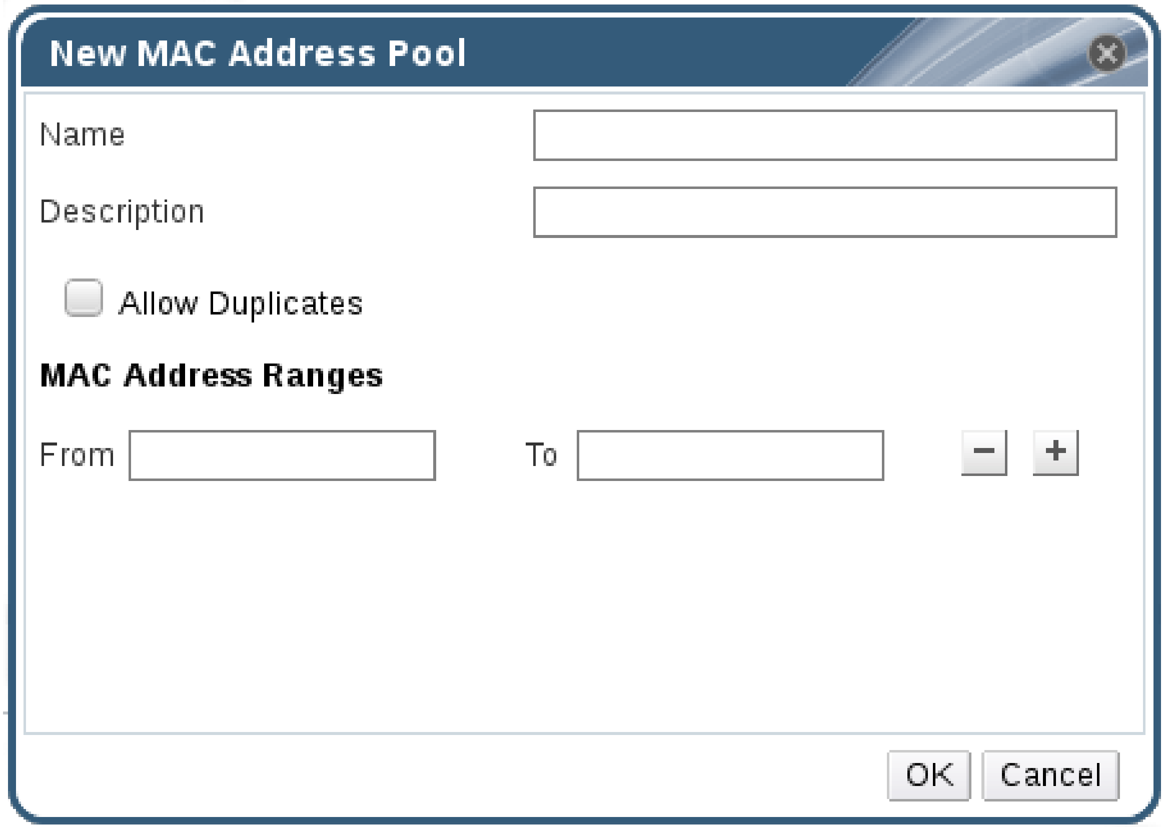


図1.9 MAC アドレスプールの新規作成ウィンドウ

4. 新規作成する 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は使用しませんが、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。

手順1.8 MAC アドレスプールのプロパティー

1. ヘッダーバーで **設定** ボタンをクリックして **設定** ウィンドウを開きます。
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** ボタンをクリックすると、**MAC アドレスプールの編集** ウィンドウが開きます。
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には、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使用する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。

手順1.9 MAC アドレスプールのパーミッションの編集

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

デフォルトの MAC アドレスプールは削除できませんが、作成した MAC アドレスプールは削除することができます。

手順1.10 MAC アドレスプールの削除

1. ヘッダーバーで **設定** ボタンをクリックして **設定** ウィンドウを開きます。
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** ボタンをクリックして、**MAC アドレスプールの削除** ウィンドウを開きます。
5. **OK** をクリックします。

第2章 DASHBOARD

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、ユーザーに問題を警告して、その問題のある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 によってはデフォルトで 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、別のタブ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。Dashboard 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。

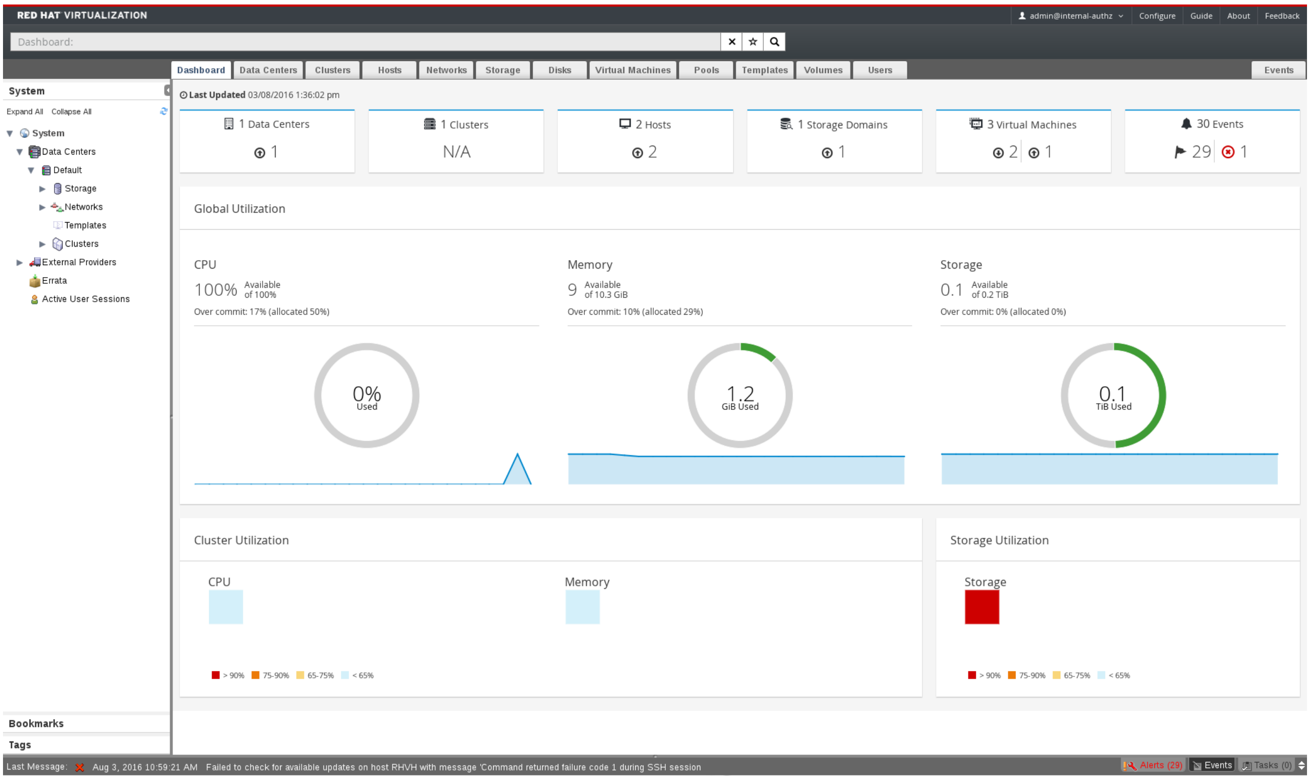


図2.1 ダッシュボード

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 のインストールと設定についての詳しい情報は、『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。

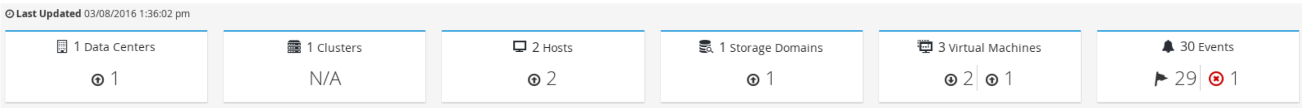


図2.2 グローバルインベントリー

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 内の関連するタブが開きます。**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。
	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、対象のタブが開き、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。 • **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。 • **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、対象のタブが開き、検索は稼働中のステータスのリソースに限定されます。
	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、対象のタブが開き、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。 • **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。 • **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。

アイコン	ステータス
	警告のステータス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** タブが開き、検索は重大度が警告のステータスのイベントに限定されます。
	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** タブが開き、検索は重大度がエラーのステータスのイベントに限定されます。

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。

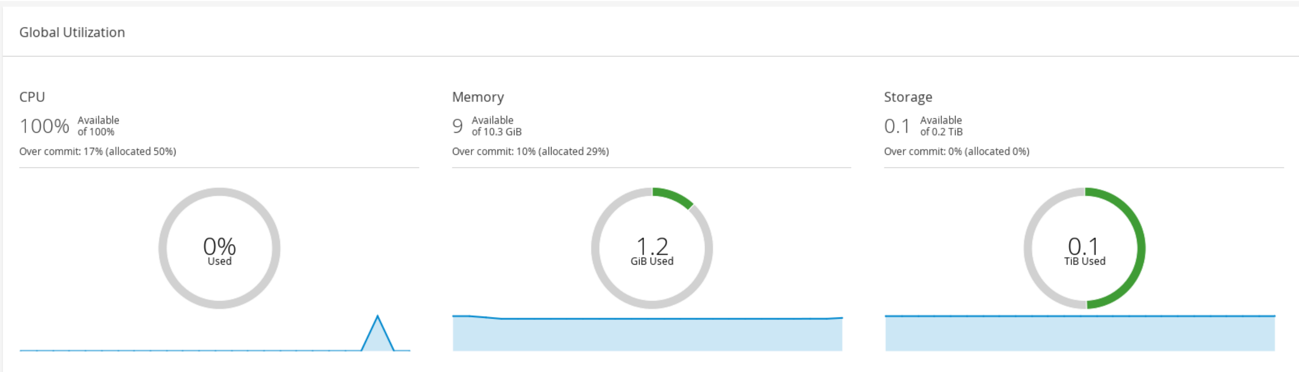


図2.3 システム全体の使用状況

- 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も表示されます。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

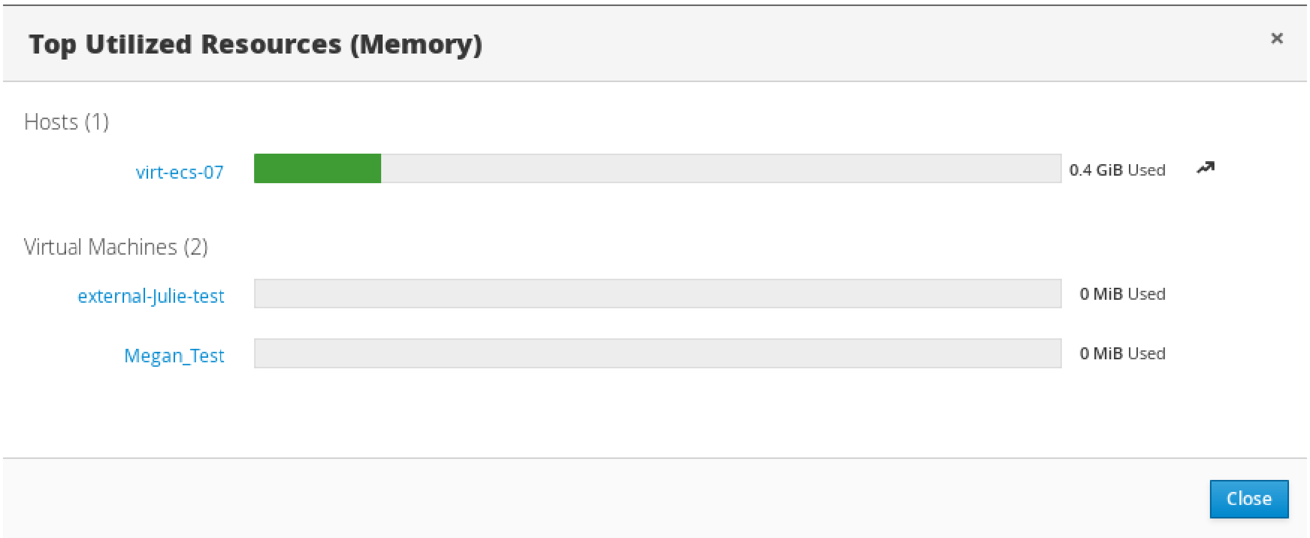


図2.4 使用率の高いリソース (メモリー)

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、ポップアップウイ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インドウには、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 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。

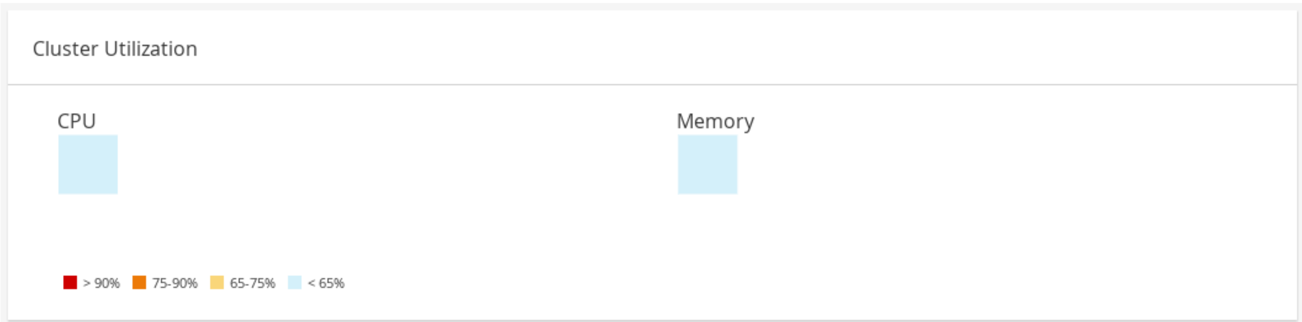


図2.5 クラスター使用率

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、**ホスト** タブが開き、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、**ホスト** タブが開き、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 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。

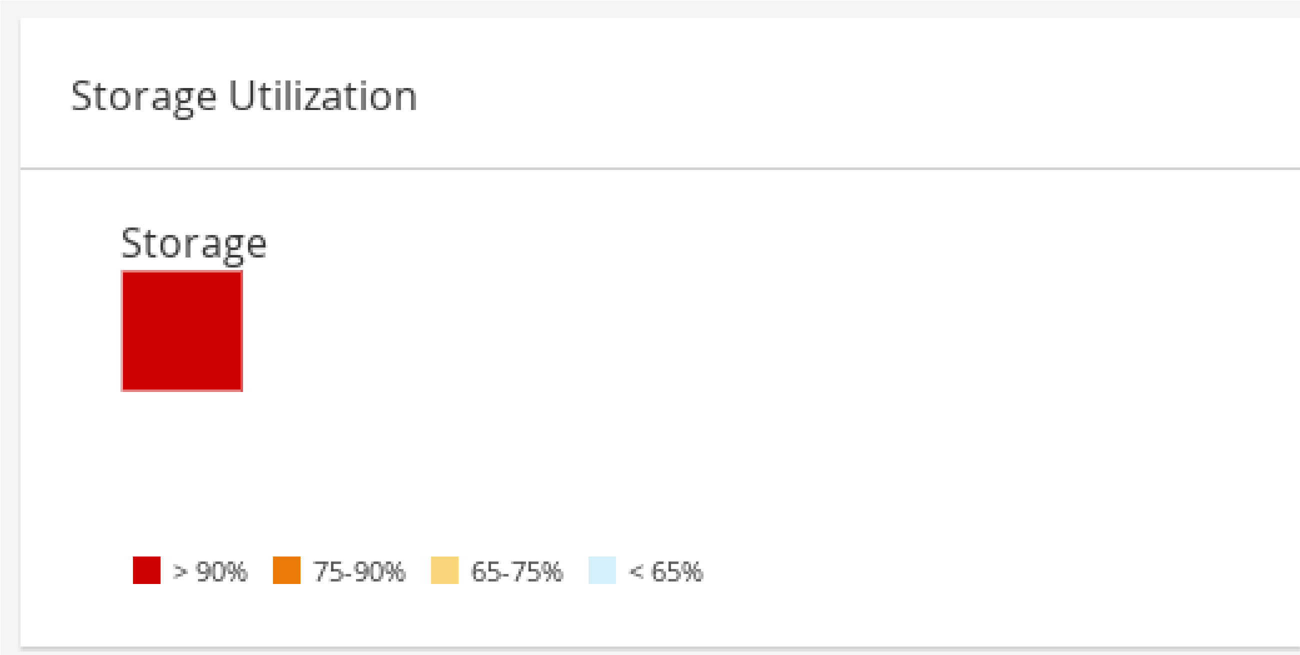


図2.6 ストレージ使用率

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** タブが開き、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高い制御を提供する 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 QOS

ストレージ 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 エントリーを作成します。

手順3.1 ストレージ QoS エントリーの作成

1. **データセンター** リソースタブをクリックして対象のデータセンターを選択します。
2. 詳細ペインで **QoS** タブをクリックします。
3. **ストレージ** をクリックします。
4. **新規作成** をクリックします。
5. **QoS 名** のフィールドに QoS エントリーの名前を入力します。
6. **説明** フィールドに QoS エントリーの説明を入力します。
7. スループットの QoS を指定します。
    a. **スループット** のチェックボックスを選択します。
    b. **合計** 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。
    c. **読み取り** フィールドに読み取り操作の最大許容スループットを入力します。
    d. **書き込み** フィールドに書き込み操作の最大許容スループットを入力します。
8. 入出力の QoS を指定します。
    a. **IOps** のチェックボックスを選択します。
    b. **合計** のフィールドに入出力操作の最大許容数を入力します。
    c. **読み取り** のフィールドに入力操作の最大許容数を入力します。
    d. **書き込み** のフィールドに出力操作の最大許容数を入力します。
9. **OK** をクリックします。

ストレージ QoS エントリーが作成されました。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。

手順3.2 ストレージ QoS エントリーの削除

1. **データセンター** リソースタブをクリックして対象のデータセンターを選択します。
2. 詳細ペインで **QoS** タブをクリックします。
3. **ストレージ** をクリックします。
4. 削除するストレージ QoS エントリーを選択します。
5. **削除** をクリックします。
6. プロンプトが表示されたら **OK** をクリックします。

ストレージ QoS エントリーが削除され、使用できなくなりました。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。

手順3.3 仮想マシンネットワーク QoS エントリーの作成

1. **データセンター** リソースタブをクリックして対象のデータセンターを選択します。
2. 詳細ペインの **QoS** タブをクリックします。
3. **仮想マシンネットワーク** をクリックします。
4. **新規作成** ボタンをクリックします。
5. **名前** のフィールドに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. 新規仮想マシンネットワーク QoS の設定および 仮想マシンネットワーク QoS の編集ウィンドウ

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	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。 • **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	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。 • **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

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。

手順3.4 仮想マシンネットワーク QoS エントリーの削除

1. **データセンター** リソースタブをクリックして対象のデータセンターを選択します。
2. 詳細ペインの **QoS** タブをクリックします。
3. **仮想マシンネットワーク** を選択します。
4. 削除する仮想マシンネットワーク QoS エントリーを選択します。

5. **削除** をクリックします。

6. プロンプトが表示されたら **OK** をクリックします。

仮想マシンネットワーク QoS エントリーの削除が完了し、そのエントリーは使用できなくなりました。

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。

手順3.5 ホストネットワーク QoS エントリーの作成

1. **データセンター** リソースタブをクリックして対象のデータセンターを選択します。

2. 詳細ペインで **QoS** タブをクリックします。

3. **ホストネットワーク** をクリックします。

4. **新規作成** をクリックします。

5. **QoS 名** のフィールドに QoS エントリーの名前を入力します。

6. **説明** フィールドに QoS エントリーの説明を入力します。

7. **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。

8. **OK** をクリックします。

3.3.2. 「新規ホストネットワーク QoS」と「ホストネットワーク QoS の編集」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。

フィールド名	説明
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
送信	送信トラフィックに適用される設定 • **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ーを、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。

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。

手順3.6 ホストネットワーク QoS エントリーの削除

1. **データセンター** リソースタブをクリックして対象のデータセンターを選択します。
2. 詳細ペインの **QoS** タブをクリックします。
3. **ホストネットワーク** をクリックします。
4. 削除するネットワーク QoS エントリーを選択します。
5. **削除** をクリックします。
6. プロンプトが表示されたら **OK** をクリックします。

3.4. CPU QOS

CPU 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 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。

手順3.7 CPU QoS エントリーの作成

1. **データセンター** リソースタブをクリックして対象のデータセンターを選択します。
2. 詳細ペインで **QoS** タブをクリックします。
3. **CPU** をクリックします。
4. **新規作成** をクリックします。
5. **QoS 名** のフィールドに QoS エントリーの名前を入力します。
6. **説明** フィールドに QoS エントリーの説明を入力します。
7. **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。
8. **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。

手順3.8 CPU QoS エントリーの削除

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

CPU QoS エントリーが削除され、使用できなくなりました。いずれかの CPU プロファイルがそ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ーです。データセンターはコンテナー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。

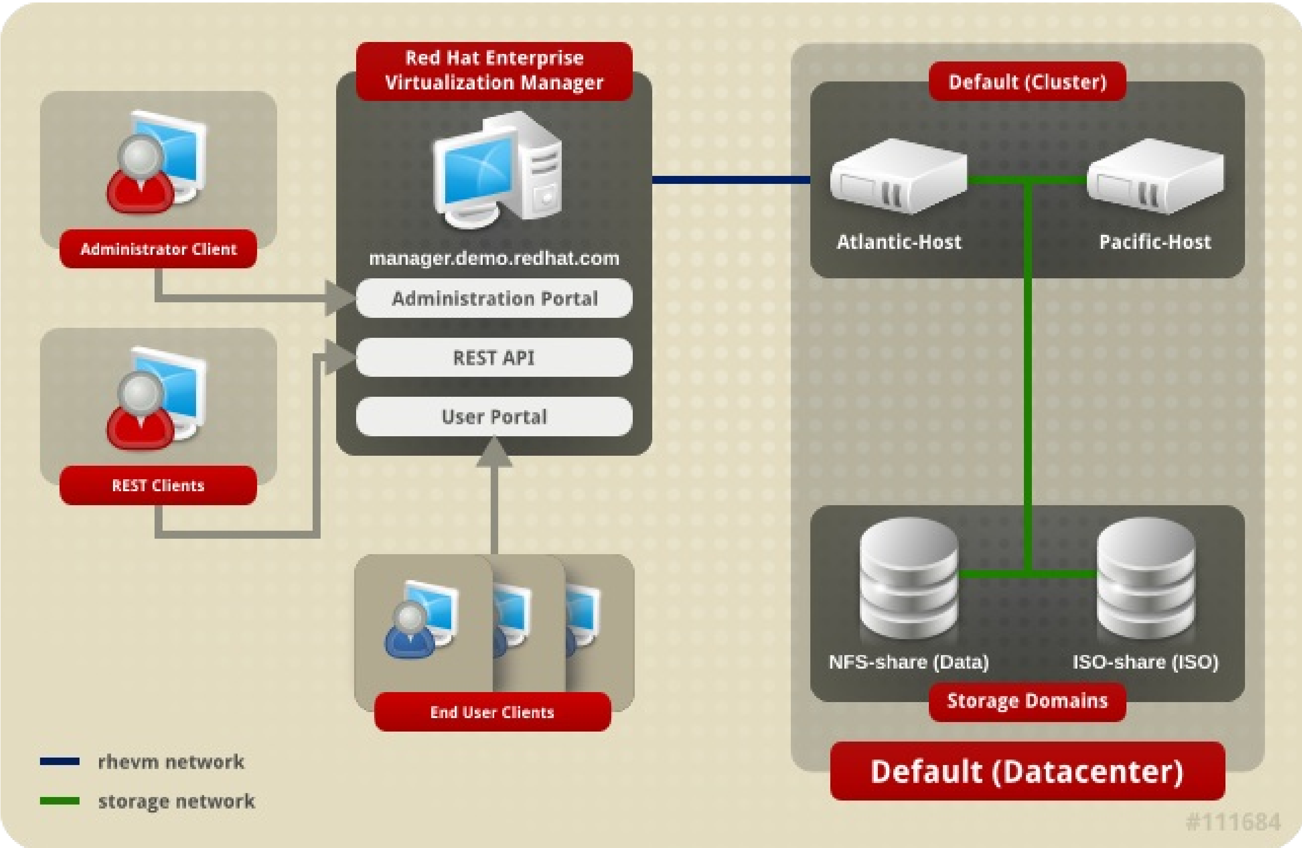


図4.1 データセンター

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。

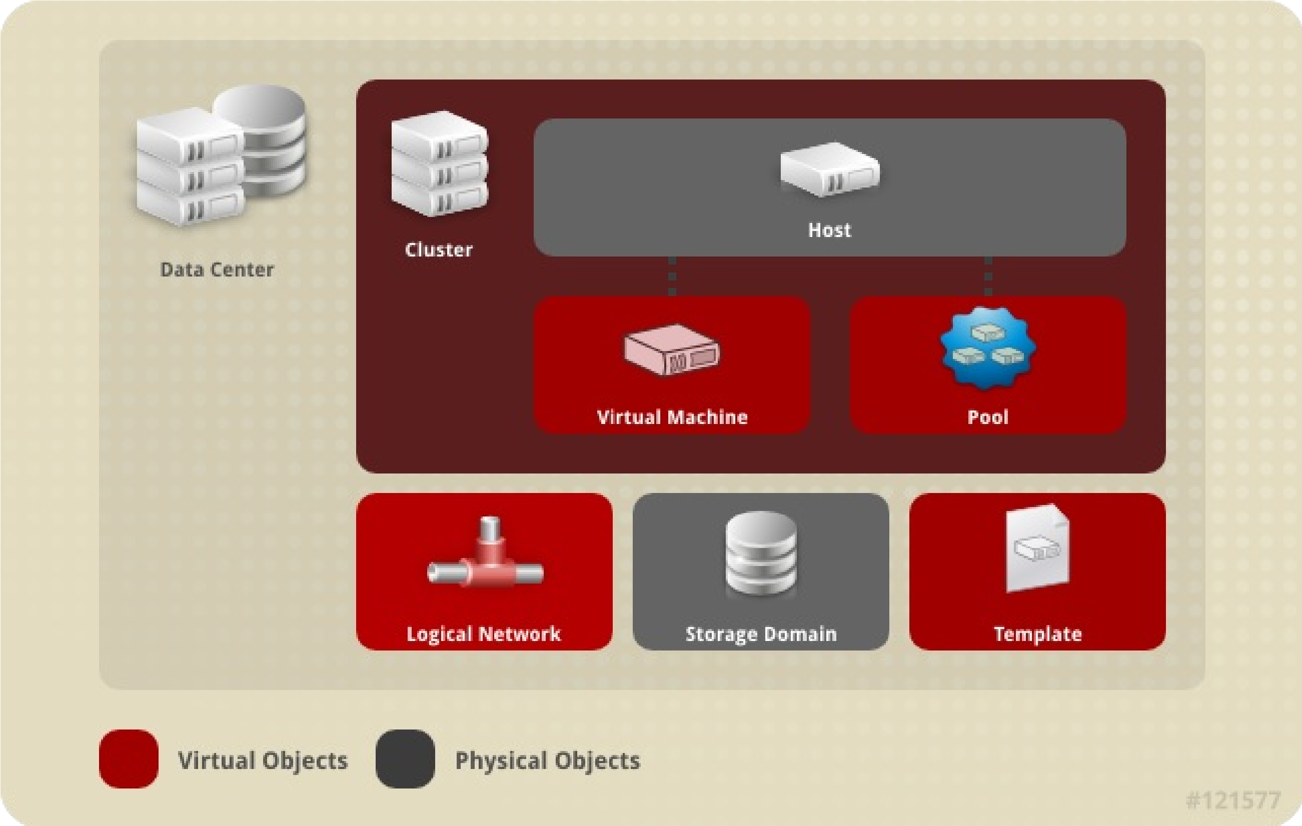


図4.2 データセンターのオブジェクト

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 優先度を変更するには、ホストを編集します。

4.4. データセンター内で問題のあるオブジェクトをイベントタブで特定する手順

データセンターの **イベント** タブは、データセンターに関連付けられたイベントをすべて表示します。イベントには監査、警告、エラーが含まれます。結果一覧に表示される情報から、Red Hat Virtualization 環境で問題のあるオブジェクトを特定することができます。

イベント の結果一覧には簡易表示と詳細表示の 2 つのビューがあります。簡易表示では、イベントアイコン、イベントの発生時刻、イベントの説明が表示されます。詳細表示では、上記の項目に加え、必要に応じてイベント ID、関連するユーザー、ホスト、仮想マシン、テンプレート、データセンター、ストレージ、クラスター、Gluster ボリューム、相関 ID などが表示されます。

4.5. データセンターのタスク

4.5.1. 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

ストレージの **タイプ** は、最初のストレージドメインがデータセンターに追加されるまで編集可能です。ストレージドメインが追加されると、ストレージの **タイプ** は変更できなくなります。

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。

手順4.1 新しいデータセンターの作成

1. **データセンター** リソースタブを選択すると、結果一覧にデータセンターがすべて表示されます。
2. 次に **新規作成** ボタンをクリックして、**新規データセンター** ウィンドウを開きます。
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の **タイプ**、**互換バージョン**、**クォータモード** を選びます。
5. オプションで、データセンター用の MAC アドレスプールを変更します。デフォルトの MAC アドレスプールは、デフォルトで事前に選択されます。MAC アドレスプールの作成についての詳しい説明は、「MAC アドレスプール」を参照してください。
    a. **MAC アドレスプール** タブをクリックします。
    b. **MAC アドレスプール** のドロップダウンリストから、必要な MAC アドレスを選択します。
6. **OK** をクリックしデータセンターを作成すると、**新規データセンター - ガイド** ウィンドウが開きます。
7. **新規データセンター - ガイド** ウィンドウでは、データセンターに設定する必要のあるエンティティーが表示されます。これらのエンティティーを設定するか、**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、**Guide Me** ボタンを押してください。

新しいデータセンターが仮想化環境に追加されました。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、ステータスは **Uninitialized** のままとなります。これらのエンティティーの設定には **Guide Me** を使用してください。

4.5.2. 新規データセンターウィンドウ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ー

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。
タイプ	ストレージのタイプ。以下のいずれかを選択します。 • **Shared** • **Local** データドメインのタイプによってデータセンターのタイプが決定し、作成後に変更すると大幅なサービスの中断を招きます。同じデータセンターに複数の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が、ローカルドメインと共有ドメインを混在させることはできません。
互換バージョン	Red Hat Virtualization のバージョン。以下のいずれかを選択します。 • **3.6** • **4.0** Red Hat Virtualization Manager のアップグレード後に、ホスト、クラスター、データセンターが旧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。

フィールド	説明/アクション
クォータモード	クォータは、Red Hat Virtualizaton 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。 • **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。
MAC アドレスプール	データセンターの MAC アドレスプール。他の MAC アドレスプールが割り当てられていない場合には、デフォルトの MAC アドレスプールが使用されます。MAC アドレスプールについての詳しい説明は、「MAC アドレスプール」を参照してください。

4.5.3. 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。リカバリー作業は、マスターデータドメインのデータが破損した際に必要です。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。

手順4.2 データセンターの再初期化

1. **データセンター** リソースタブをクリックして再初期化するデータセンターを選択します。
2. データセンターに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. データセンターを右クリックし、ドロップダウンメニューから **データセンターを再初期化** を選択して **データセンターの再初期化** ウィンドウを開きます。
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. ウィンドウを閉じてデータセンターを再初期化するには **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。

4.5.4. データセンターの削除

データセンターを削除するには、アクティブなホストが 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。

手順4.3 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. **データセンター** リソースタブをクリックし、削除するデータセンターを選択します。
3. **削除** をクリックすると **データセンターの削除** の確認ウィンドウが開きます。
4. **OK** をクリックします。

4.5.5. データセンターの強制削除

アタッチされ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 **Non Responsive** になります。いずれの状況でも、データセンターを **削除** することはできません。

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。

手順4.4 データセンターの強制削除

1. **データセンター** リソースタブをクリックし、削除するデータセンターを選択します。
2. **強制削除** をクリックすると、**データセンターの強制削除** の確認ウィンドウが開きます。
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。

4.5.6. データセンターの互換バージョンの変更

Red Hat Virtualization データセンターには、互換バージョンがあります。互換バージョンとは、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、最初に、変更後の互換性レベルをサポートするレベルまで、データセンター内の全クラスターを更新する必要があります。

手順4.5 データセンターの互換バージョンの変更

1. 管理ポータルで **データセンター** タブをクリックします。

2. 表示された一覧の中から、変更するデータセンターを選択します。

3. **編集** をクリックします。

4. **互換バージョン** を必要な値に変更します。

5. **OK** をクリックして、**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。

6. **OK** をクリックして確定します。

データセンターの互換バージョンが更新されました。

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。

4.6. データセンターとストレージドメイン

4.6.1. データセンターへの既存データドメインのアタッチ

Unattached のデータドメインはデータセンターにアタッチすることができます。複数のタイプ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。

手順4.6 データセンターへの既存データドメインのアタッチ

1. **データセンター** リソースタブをクリックして対象のデータセンターを選択します。

2. 詳細ペインの **ストレージ** タブを選択し、データセンターにすでにアタッチされているストレージドメインを表示します。

3. **データをアタッチ** をクリックし、**ストレージのアタッチ** ウィンドウを開きます。

4. データセンターにアタッチするデータドメインのチェックボックスを選択します。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。

5. **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。

4.6.2. データセンターへの既存 ISO ドメインのアタッチ

Unattached の ISO ドメインはデータセンターにアタッチすることができます。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。

手順4.7 データセンターへの既存 ISO ドメインのアタッチ

1. **データセンター** リソースタブをクリックして対象のデータセンターを選択します。

2. 詳細ペインの **ストレージ** タブを選択し、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。

3. **ISO のアタッチ** をクリックして、**ISO ライブラリーのアタッチ** ウィンドウを開きます。

4. 対象の ISO ドメインのラジオボタンをクリックします。

5. **OK** をクリックします。

ISO ドメイン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。

4.6.3. 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イメージ、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 **Unattached** のエクスポートドメインはデータセンターにアタッチすることができます。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。

手順4.8 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. **データセンター** リソースタブをクリックして対象のデータセンターを選択します。

2. 詳細ペインの **ストレージ** タブを選択し、データセンターにすでにアタッチされているストレージドメインを表示します。

3. **エクスポートをアタッチ** をクリックすると、**エクスポートドメインのアタッチ** ウィンドウが開きます。

4. 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。

5. **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。

4.6.4. 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。

手順4.9 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. **データセンター** リソースタブをクリックして対象のデータセンターを選択します。

2. 詳細ペインの **ストレージ** タブを選択し、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。

3. デタッチするストレージドメインを選択します。ストレージドメインが **アクティブ** である場合は、**メンテナンス** をクリックして、**ストレージドメインのメンテナンス** の確認ウィンドウを開きます。

4. **OK** をクリックしてメンテナンスモードを開始します。

5. **デタッチ** をクリックすると、**ストレージのデタッチ** の確認ウィンドウが開きます。

6. **OK** をクリックします。

データセンターからストレージドメインがデタッチされました。ストレージドメインが詳細ペインに表示されなくなるまでに数分かかる場合があります。

4.7. データセンターとパーミッション

4.7.1. データセンターのシステムパーミッション管理

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、より特定的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のみに対して (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のみに対して管理者権限があります。

データセンターの管理者は、特定のデータセンターのみ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、ある 1 つ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。

4.7.2. データセンターの管理者ロール

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4.2 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。
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。

4.7.3. 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。

手順4.10 リソースへのロール割り当て

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。
2. 詳細ペインの **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。

ユーザーにロールが割り当てられました。このユーザーは、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。

4.7.4. リソースからの管理者またはユーザーロールの削除

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。

手順4.11 リソースからのロール削除

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。

2. 詳細ペインの **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。パーミッションが削除されることを確認する **パーミッションの削除** ウィンドウが開きます。

5. **OK** をクリックします。

ユーザーロールおよび関連付けられたパーミッションが削除されました。

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** タブやランタイム中に設定ツールで定義したポリシーに従って、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。

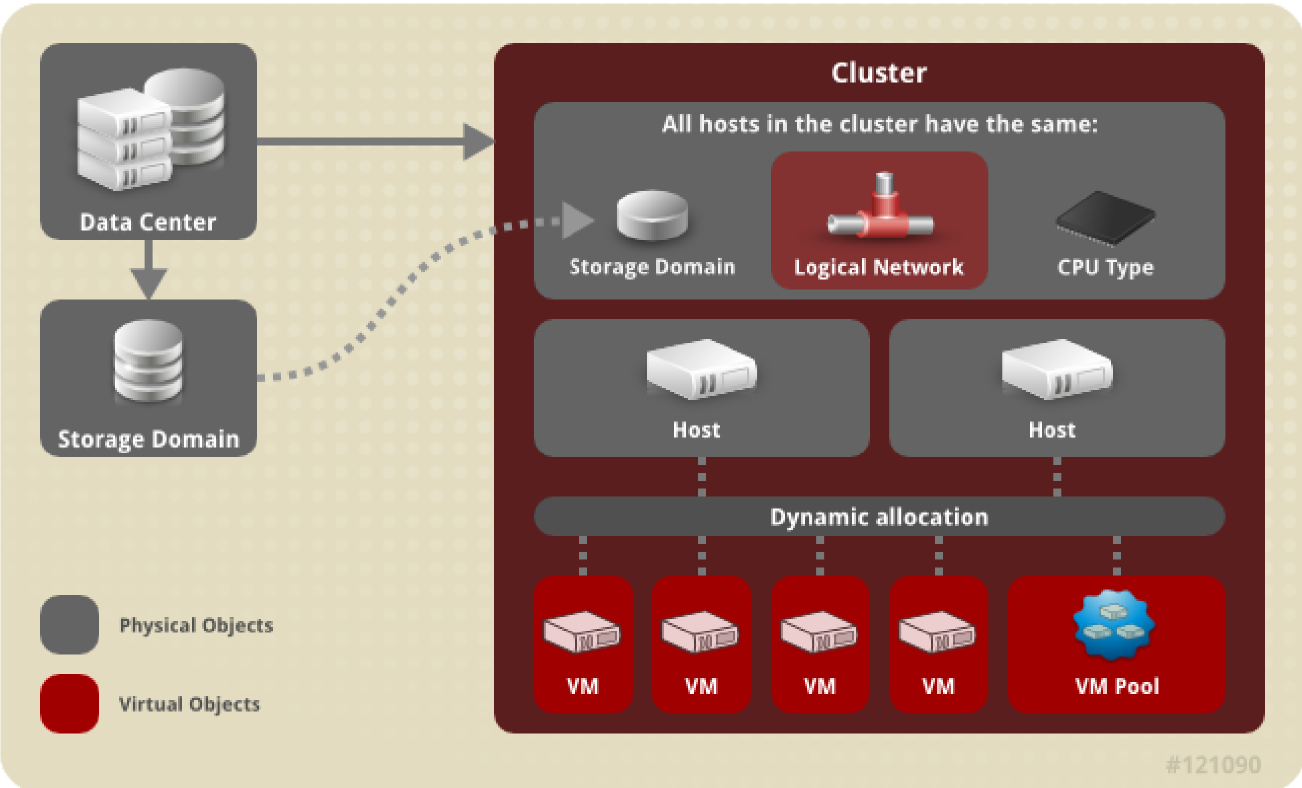


図5.1 クラスター

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。

手順5.1 新規クラスターの作成

1. **クラスター** リソースタブを選択します。
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 のプロセッサーファミリーが、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、https://access.redhat.com/ja/solutions/1358113 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. 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** のいずれかのラジオボタンを選択します。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。
9. 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、管理者によりメンテナンスの説明を提示できるようにします。
10. 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。
11. **/dev/random source** (Linux 提供のデバイス) または **/dev/hwrng source** (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して、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します。
12. **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ルーニングを有効化します。
13. 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。

14. **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。

15. オプションとして、グローバルの SPICE プロキシー (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 プロキシーのアドレスを指定します。

16. **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。

17. **OK** をクリックしてクラスターを作成すると、**新規クラスター - ガイド** ウィンドウが開きます。

18. **新規クラスター - ガイド** ウィンドウでは、データセンターに設定する必要のあるエンティティーが表示されます。これらのエンティティーを設定するか、**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、**Guide Me** ボタンを押してください。

新規クラスターが仮想化環境に追加されました。

5.2.2. 新規クラスターおよびクラスターの編集ウィンドウの設定とコントロール

5.2.2.1. クラスターの全般設定

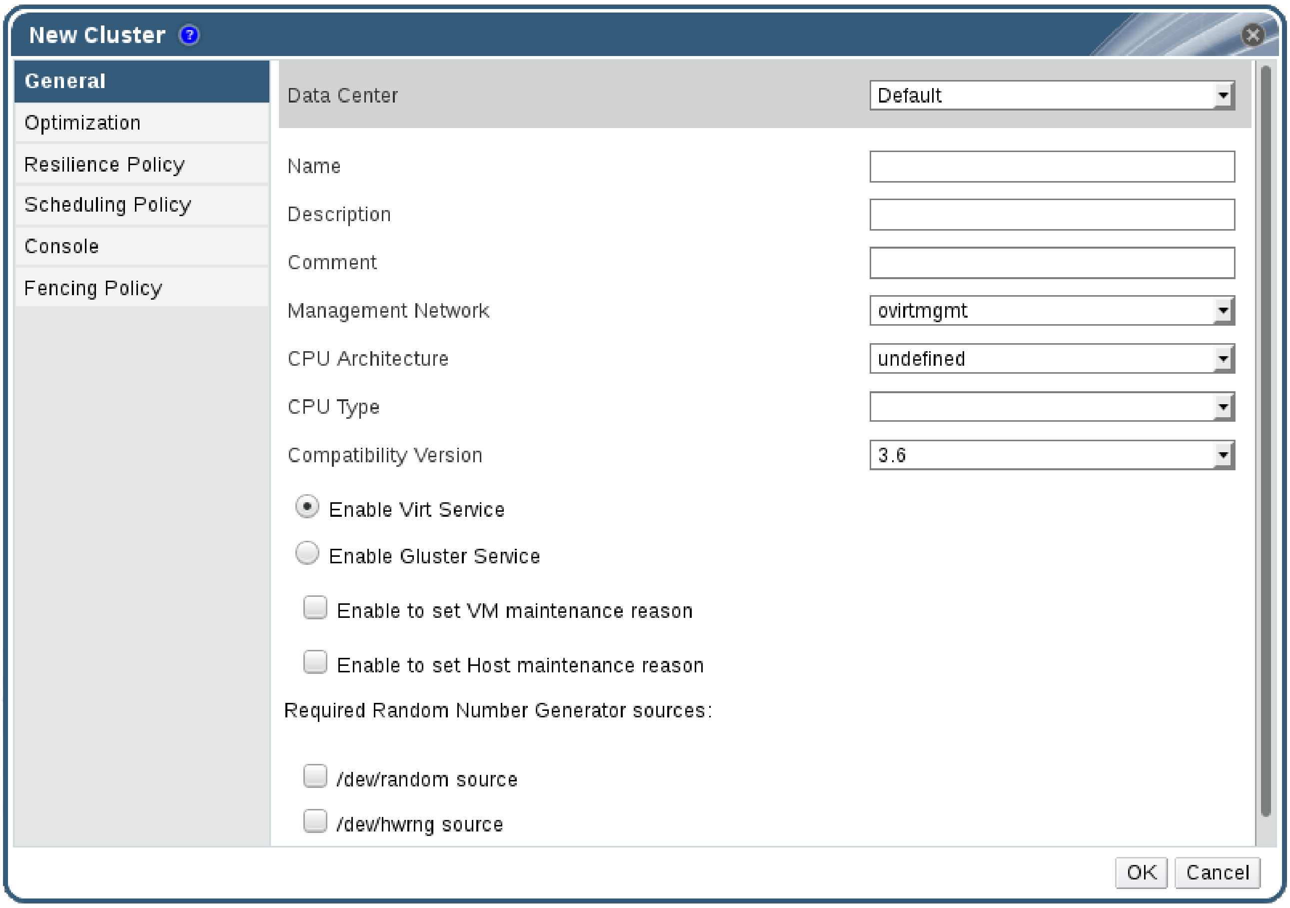


図5.2 新規クラスターウィンドウ

以下の表には、**新規クラスター** および **クラスターの編集** ウィンドウ内の **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 / 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は推奨されますが、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、詳細ペインの **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。
CPU アーキテクチャー	クラスターの CPU アーキテクチャー。選択する 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。 • **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。

<table>
<tr><th>フィールド</th><th>説明/アクション</th></tr>
<tr><td>CPU タイプ</td><td>クラスターの CPU タイプ。以下のいずれかを選択します。
Intel Conroe Family
Intel Penryn Family
Intel Nehalem Family
Intel Westmere Family
Intel SandyBridge Family
Intel Haswell
AMD Opteron G1
AMD Opteron G2
AMD Opteron G3
AMD Opteron G4
AMD Opteron G5
IBM POWER 8
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。</td></tr>
<tr><td>互換バージョン</td><td>Red Hat Virtualization のバージョン。以下のいずれかを選択します。
3.6
4.0
データセンターに指定されているバージョンよりも古いバージョンは選択できません。</td></tr>
<tr><td>Virt サービスを有効にする</td><td>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。</td></tr>
</table>

フィールド	説明/アクション
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	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。 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。 • **アドレス**: 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。 • **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。 • **root 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が選択されている場合には、Manager から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と、オプションの理由のフィールドが表示されます。これにより、メンテナンスの理由を入力することが可能となります。この理由は、ログに表示され、またホストを再度アクティブにすると表示されます。

フィールド	説明/アクション
必要な乱数ジェネレーターのソース:	以下のチェックボックスのいずれかを選択する場合は、クラスター内の全ホストでそのデバイスが利用可能である必要があります。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。 • **`/dev/random source`**: Linux により提供される乱数ジェネレーター • **`/dev/hwrng source`**: 外部ハードウェアのジェネレーター

5.2.2.2. 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ー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	• **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	**スレッドをコアとしてカウント** 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ーコア合計数の仮想マシンを実行することができます。 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。
メモリーバルーン	**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。 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。 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。
KSM コントロール	**KSM を有効化** 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リットが得られる場合に Kernel Same-page Merging (KSM) を実行します。

5.2.2.3. 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。**`vdsm.conf`** の設定内容がそのまま優先されて適用されます。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。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。
`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
`Auto`	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。
`Hypervisor default`	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。
`Custom`	ユーザーが定義します (Mbps)。

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 耐障害性ポリシー設定

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。

フィールド	説明/アクション
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。

追加のプロパティー 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

プロパティー	説明
移行の自動収束	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。 • 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。 • グローバル設定を上書き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。 • グローバル設定を上書きして、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。

プロパティー	説明
移行時の圧縮の有効化	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。 • 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。 • グローバル設定を上書き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。 • グローバル設定を上書きして、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。

5.2.2.4. 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。

既存のクラスターにスケジューリングポリシーを追加するには、**クラスター** タブで **編集** ボタンをクリックして、**スケジューリングポリシー** のタブを選択します。

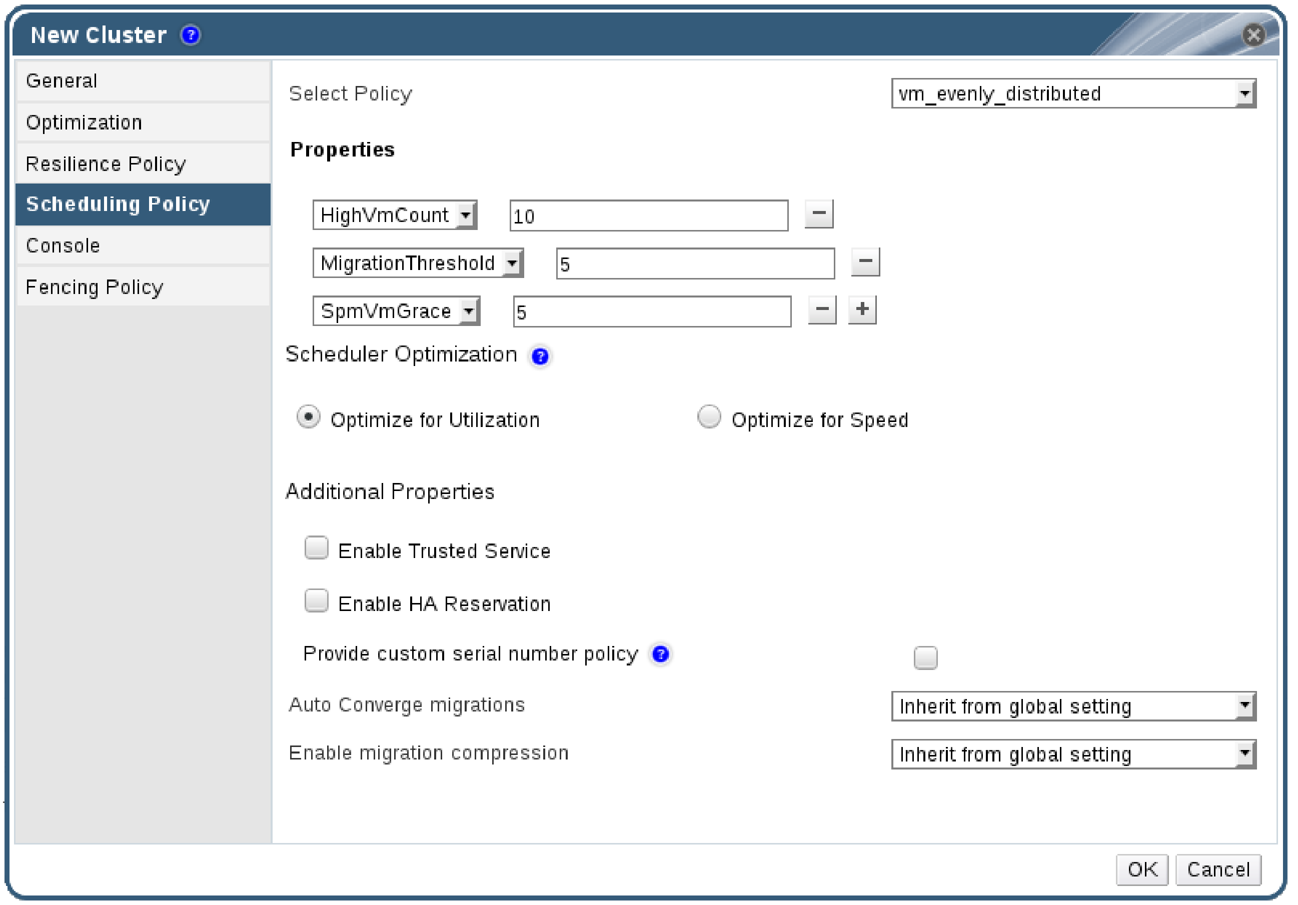


図5.3 スケジューリングポリシーの設定: vm_evenly_distributed

以下の表には、**スケジューリングポリシー** タブの設定についての説明をまとめています。

表5.7 スケジューリングポリシータブのプロパティー

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	ドロップダウンリストからポリシーを選択します。 • **None**: ポリシーの値を **None** に設定すると、ホスト間での負荷分散や電源共有は行われません。これはデフォルトのモードになります。 • **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。ホストが定義済みの上限閾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。 • **InClusterUpgrade**: ホストのオペレーティングシステムのバージョンに基づいて仮想マシンを分散します。仮想マシンを実行しているホストよりも新しい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優先されます。より新しいオペレーティングシステムのホストに移行した仮想マシンは、古いオペレーティングシステムのホストには戻りません。仮想マシンは、クラスター内の任意のホストで再起動することが可能です。このポリシーでは、クラスターで複数のオペレーティングシステムのバージョンの混在を許可することによって、クラスター内のホストをアップグレードすることができます。このポリシーを有効にする前に、前提条件を満たす必要があります。詳しくは、『アップグレードガイド』 を参照してください。 • **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値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。ホストが定義済みの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。ホストが **HighVmCount** を超える数の仮想マシンを実行しており、かつ仮想マシン数が **MigrationThreshold** を超えるホストが少なくとも 1 台ある場合には、そのクラスターはバランスが取れていない状態と見なされます。
プロパティー	以下のプロパティーは、選択したポリシーに応じて表示され、必要に応じて編集することができます。

フィールド	説明/アクション
	• **HighVmCount**: 各ホストで実行することができる仮想マシンの最大数を設定します。この制限を超えると、ホストは過負荷状態と見なされます。デフォルト値は **10** です。 • **MigrationThreshold**: 仮想マシンがホストから移行されるバッファーを定義します。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。ホストが上限値以上の CPU 使用率で稼働した状態で、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仮想マシンに移動します。デフォルト値は **80** です。 • **LowUtilization**: パーセンテージで指定します。CPU 使用率が下限値を下回っている状態でホストが稼働して、規定の時間が経過すると、Red Hat Virtualization Manager はクラスター内の他のホストに仮想マシンを移行します。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に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可能なオプションのプロパティーです。 • **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

フィールド	説明/アクション
	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ーです。 • **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ーです。デフォルト値は **true** です。 • **MaxFreeMemoryForOverUtilized**: 最小のサービスレベルに必要な空きメモリー容量を MB 単位で設定します。ホストのメモリー使用率がこの値以上で実行されると、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るまで、仮想マシンをクラスター内の他のホストに移行します。**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。これは、**power_saving** および **evenly_distributed** のポリシーに追加可能なオプションのプロパティーです。 • **MinFreeMemoryForUnderUtilized**: 最小の空きメモリー容量を MB 単位で設定します。この値を超えると、ホストは使用率が低いと見なされます。ホストのメモリー使用率がこの値以下で実行されると、Red Hat Virtualization Manager はクラスター内の別のホストに仮想マシンを移行してから、そのホストマシンの電源を自動的に切断し、負荷分散により要求された場合やクラスター内の利用可能なホストが足りない場合に再起動します。**MaxFreeMemoryForOverUtilized** と **MinFreeMemoryForUnderUtilized** を両方 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。これは、**power_saving** および **evenly_distributed** のポリシーに追加可能なオプションのプロパティーです。
スケジューラーの最適化	ホストの加重/順序のスケジューリングを最適化します。 • **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、最適の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。

フィールド	説明/アクション
信頼済みサービスを有効にする	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。
HA 予約を有効にする	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。
カスタムのシリアル番号ポリシーを指定する	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。 • **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。
移行の自動収束	このオプションは、クラスター内の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率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させることができます。QEMU は収束されていないことを自動検出し、仮想マシンで vCPU のスロットルを減らします。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。 • **engine-config** を使用して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。 • グローバル設定を上書きして、クラスター内の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。 • グローバル設定を上書きして、クラスター内の仮想マシンの自動収束をできないようにするには、**自動収束しない** を選択します。

フィールド	説明/アクション
移行時の圧縮の有効化	このオプションでは、クラスター内の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。 • **`engine-config`** を使用して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。 • グローバル設定を上書きして、クラスター内の仮想マシンの圧縮を可能にするには、**圧縮** を選択します。 • グローバル設定を上書きして、クラスター内の仮想マシンの圧縮をできないようにするには、**圧縮しない** を選択します。

ホストの空きメモリーが 20% 未満に下がると、**`mom.Controllers.Balloon - INFO Ballooning guest:half1 from 1096400 to 1991580`** のようなバ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。

5.2.2.5. クラスターのコンソール設定

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 プロキシーを定義	グローバル設定で定義されている SPICE プロキシー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: ユーザーポータルからの接続) に有用です。
SPICE プロキシーアドレスを上書き	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ー。このアドレスは、以下の形式で指定する必要があります。 `protocol://[host]:[port]`

5.2.2.6. 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。

5.2.3. リソースの編集

概要

リソースのプロパティーを編集します。

手順5.2 リソースの編集

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。
2. **編集** をクリックして **編集** ウィンドウを開きます。
3. 必要なプロパティーを変更して **OK** をクリックします。

結果

新規プロパティーがリソースに保存されました。プロパティーフィールドが無効の場合には、**編集** ウィンドウは閉じません。

5.2.4. クラスター内のホストに負荷および電源管理のポリシーを設定する手順

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

リーおよび 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。

手順5.3 ホストに負荷および電源管理のポリシーを設定する手順

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のクラスターを選択します。

2. **編集** クリックすると、**クラスターの編集** ウィンドウが表示されます。

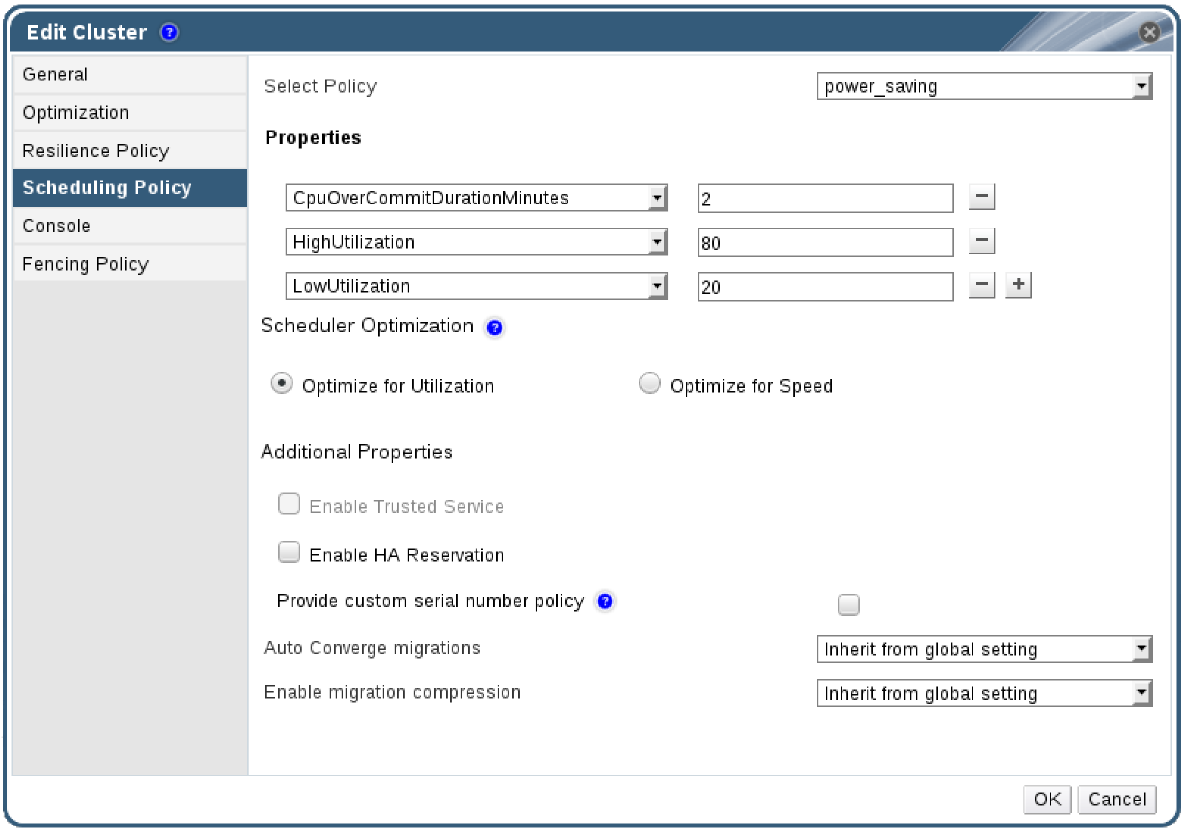


図5.4 スケジューリングポリシーの編集

3. 以下のポリシーのいずれかを選択します。

   - **none**

   - **vm_evenly_distributed**

     a. **HighVmCount** フィールドには、各ホストで実行可能な仮想マシンの最大数を設定します。

     b. **MigrationThreshold** フィールドには、使用率が最も高いホスト上の仮想マシン数と使用率が最も低いホスト上の仮想マシン数の差異を定義します。

     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。

   - **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、仮想マシンが他のホストへの移行を開始する、必要な空きメモリー容量の最小値を MB 単位でを入力します。

d. **MaxFreeMemoryForOverUtilized** には、仮想マシンが他のホストへの移行を開始する、必要な最大空きメモリー容量を MB 単位でを入力します。

- **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見なされる 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、仮想マシンが他のホストへの移行を開始する、必要な空きメモリー容量の最小値を MB 単位でを入力します。

e. **MaxFreeMemoryForOverUtilized** には、仮想マシンが他のホストへの移行を開始する、必要な最大空きメモリー容量を MB 単位でを入力します。

4. 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、最適の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。

5. **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。

6. 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ー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。

7. 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、**Host 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、**Vm 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。

8. **OK** をクリックします。

5.2.5. 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 の機能を処理します。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。

手順5.4 ホスト上での MOM ポリシーの同期

1. **クラスター** タブをクリックして、対象のホストが属するクラスターを選択します。
2. 詳細ペインの **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。
3. **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なく、ホスト上の MOM ポリシーが更新されます。

5.2.6. CPU プロファイル

CPU プロファイルは、クラスター内の仮想マシンが、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ので、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。

5.2.6.1. CPU プロファイルの作成

CPU プロファイルを作成します。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。

手順5.5 CPU プロファイルの作成

1. **クラスター** リソースタブをクリックしてクラスターを選択します。
2. 詳細ペインで **CPU プロファイル** のサブタブをクリックします。
3. **新規作成** をクリックします。
4. **名前** フィールドに CPU プロファイルの名前を入力します。
5. **説明** フィールドに CPU プロファイルの説明を入力します。
6. **QoS** 一覧から CPU プロファイルに適用する QoS を選択します。
7. **OK** をクリックします。

CPU プロファイルが作成されました。この CPU プロファイルは、そのクラスター内の仮想マシンに適用することができます。

5.2.6.2. CPU プロファイルの削除

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

手順5.6 CPU プロファイルの削除

1. **クラスター** リソースタブをクリックしてクラスターを選択します。
2. 詳細ペインで **CPU プロファイル** のサブタブをクリックします。
3. 削除する CPU プロファイルを選択します。
4. **削除** をクリックします。
5. **OK** をクリックします。

CPU プロファイルが削除され、その CPU プロファイルは使用できなくなりました。CPU プロファイルが仮想マシンに割り当てられていた場合は、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。

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

Red Hat Gluster Storage クラスターおよび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、インポートした後には、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。

手順5.7 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. **クラスター** リソースタブを選択すると、結果一覧に全クラスターが表示されます。
2. 次に **新規作成** ボタンをクリックして、**新規クラスター** ウィンドウを開きます。
3. ドロップダウンメニューからクラスターが属する **データセンター** を選択します。
4. クラスターの **名前** と **説明** を入力します。
5. **Gluster サービスを有効にする** のラジオボタンと **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** のラジオボタンを選択した場合のみに表示されます。
6. **アドレス** フィールドに、クラスター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 **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、**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 **root パスワード** を入力し、**OK** をクリックします。

8. **ホストの追加** ウィンドウが開き、クラスター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ました。既存の Red Hat Gluster Storage クラスターが Red Hat Virtualization Manager に正常にインポートされました。

5.2.8. 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 対応クラスター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、**新規クラスター** 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	クラスター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、**新規クラスター** ウィンドウで指定したホストの完全修飾ドメイン名または IP アドレスが自動的に入力されます。
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。

5.2.9. クラスターの削除

概要

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。

手順5.8 クラスターの削除

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象の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** をクリックすると **クラスターの削除** の確認ウィンドウが開きます。
4. **OK** をクリックします。

結果

クラスターが削除されました。

5.2.10. クラスターの互換バージョンの変更

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

注記

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

手順5.9 クラスターの互換バージョンの変更

1. 管理ポータルで **クラスター** タブをクリックします。
2. 表示された一覧の中から、変更するクラスターを選択します。
3. **編集** をクリックします。
4. **互換バージョン** を必要な値に変更します。
5. **OK** をクリックして、**クラス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。
6. **OK** をクリックして確定します。

クラスターの互換バージョンが更新されました。データセンター内の全クラスターの互換バージョンの更新が済むと、データセンター自体の互換バージョンも変更することができます。

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。

5.3. クラスターとパーミッション

5.3.1. 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、より特定的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のみに対して (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のみに対して管理者権限があります。

クラスターの管理者は、特定のクラスターのみの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、特定のクラスターのクラスター管理者ロールを割り当てられたユーザーは、そのクラスター内のオブジェクトをすべて管理することができます。ヘッダーバーの **設定** ボタンを使用すると、環境内の全クラスターのクラスター管理者を割り当てることができます。

クラスター管理者ロールは、以下のアクションを許可します。

- 関連付けられたクラスターの作成/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。

5.3.2. 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5.11 Red Hat Virtualization のシステム管理者ロール

ロール	権限	備考

ロール	権限	備考
ClusterAdmin	クラスター管理者	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ー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)。 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。
NetworkAdmin	ネットワーク管理者	特定のクラスターのネットワークを設定、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。

5.3.3. 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。

手順5.10 リソースへのロール割り当て

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。
2. 詳細ペインの **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。

ユーザーにロールが割り当てられました。このユーザーは、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。

5.3.4. リソースからの管理者またはユーザーロールの削除

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。

手順5.11 リソースからのロール削除

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。

2. 詳細ペインの **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。パーミッションが削除されることを確認する **パーミッションの削除** ウィンドウが開きます。

5. **OK** をクリックします。

ユーザーロールおよび関連付けられたパーミッションが削除されました。

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. ネットワークタブの使用

ネットワーク リソースタブは、ユーザーが論理ネットワーク関連の操作を行ったり、各ネットワークのプロパティーやその他のリソースとの関連付けに基づいて論理ネットワークの検索を行ったりする中央の場所です。

ネットワーク タブの結果一覧には、Red Hat Virtualization 環境内の全論理ネットワークが表示されます。**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、プロパティー変更、削除を行うことができます。

各ネットワーク名をクリックして、詳細ペインの **クラスター**、**ホスト**、**仮想マシン**、**テンプレート**、**パーミッション** 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

これらの機能は、各リソースタブ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。

手順6.1 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. **データセンター** または **クラスター** リソースタブをクリックして、結果一覧からデータセンターまたはクラスターを選択します。

2. 詳細ペインの **論理ネットワーク** タブをクリックして既存の論理ネットワークを表示します。

3.
    - **データセンター** の詳細ペインから **新規作成** をクリックし、**新規論理ネットワーク** ウィンドウを開きます。
    - **クラスター** の詳細ペインから **ネットワークを追加** をクリックし、**新規論理ネットワーク** ウィンドウを開きます。

4. 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。

5. オプションとして、**外部プロバイダー上に作成する** チェックボックスを選択します。ドロップダウンリストから **外部プロバイダー** を選択し、**物理ネットワーク** の IP アドレスを指定します。**外部プロバイダー** のドロップダウンリストには、読み取り専用モードの外部プロバイダーはリストされません。

   外部プロバイダー上に作成する を選択した場合には、**ネットワークラベル**、**仮想マシンネットワーク**、および **MTU** オプションは無効になります。

6. **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。

7. オプションで **VLAN タグ付けを有効にする** を選択します。

8. オプションで **仮想マシンネットワーク** を無効にします。

9. **MTU** 値を **デフォルト (1500)** または **カスタム** に設定します。

10. **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。

11. **外部プロバイダー上に作成する** 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。

12. 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。

13. **OK** をクリックします。

データセンター内のクラスターが必要とするリソースとして、論理ネットワークを定義しました。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

論理ネットワーク設定を編集します。

手順6.2 論理ネットワークの編集

重要

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。

1. **データセンター** リソースタブをクリックして、結果一覧内で論理ネットワークのデータセンターを選択します。
2. 詳細ペインの **論理ネットワーク** タブをクリックし、クラスター内の論理ネットワークを表示します。
3. 論理ネットワークを選択して **編集** をクリックし、**論理ネットワークの編集** ウィンドウを開きます。
4. 必要な設定を編集します。
5. **OK** をクリックして変更を保存します。

注記

マルチホストネットワーク設定により、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のみに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。**仮想マシンのネットワーク** 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 リソースタブまたは **データセンター** リソースタブ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。

手順6.3 論理ネットワークの削除

1. **データセンター** リソースタブをクリックして、結果一覧内で論理ネットワークのデータセンターを選択します。
2. 詳細ペインの **論理ネットワーク** タブをクリックし、クラスター内の論理ネットワークを表示します。
3. 論理ネットワークを選択して **削除** をクリックすると、**論理ネットワークの削除** ウィンドウが開きます。
4. 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ーアウトします。

5. **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. 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 台のホストで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。

手順6.4 論理ネットワークのゲートウェイの表示/編集

1. **ホスト** リソースタブをクリックして、対象のホストを選択します。

2. 詳細ペインにある **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。

3. **ホストネットワークを設定** ボタンをクリックすると **ホストネットワークの設定** ウィンドウが開きます。

4. 割り当てられた論理ネットワークの上にマウスを移動し、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。**Static** 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。

6.1.6. 新規ネットワークおよび論理ネットワークの編集ウィンドウの設定とコントロール

6.1.6.1. 論理ネットワークの全般設定

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

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は最長で 15 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	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
外部プロバイダー上に作成する	外部プロバイダーとして Manager に追加済みの OpenStack Networking Service 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。 **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。
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ー機能です。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。
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。

6.1.6.2. 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
クラスターに対するネットワークのアタッチ/デタッチ	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。 **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。 **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。 **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。

6.1.6.3. 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	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。 **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。 **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。

6.1.7. ネットワークの管理ウィンドウで論理ネットワークに特定のトラフィックタイプを指定する手順

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。

手順6.5 論理ネットワークのトラフィックタイプの指定

1. **クラスター** リソースタブをクリックして、結果一覧からクラスターを選択します。
2. 詳細ペインの **論理ネットワーク** タブをクリックし、クラスターに割り当てられた論理ネットワークを表示します。
3. **ネットワークを管理** をクリックし、**ネットワークの管理** ウィンドウを開きます。

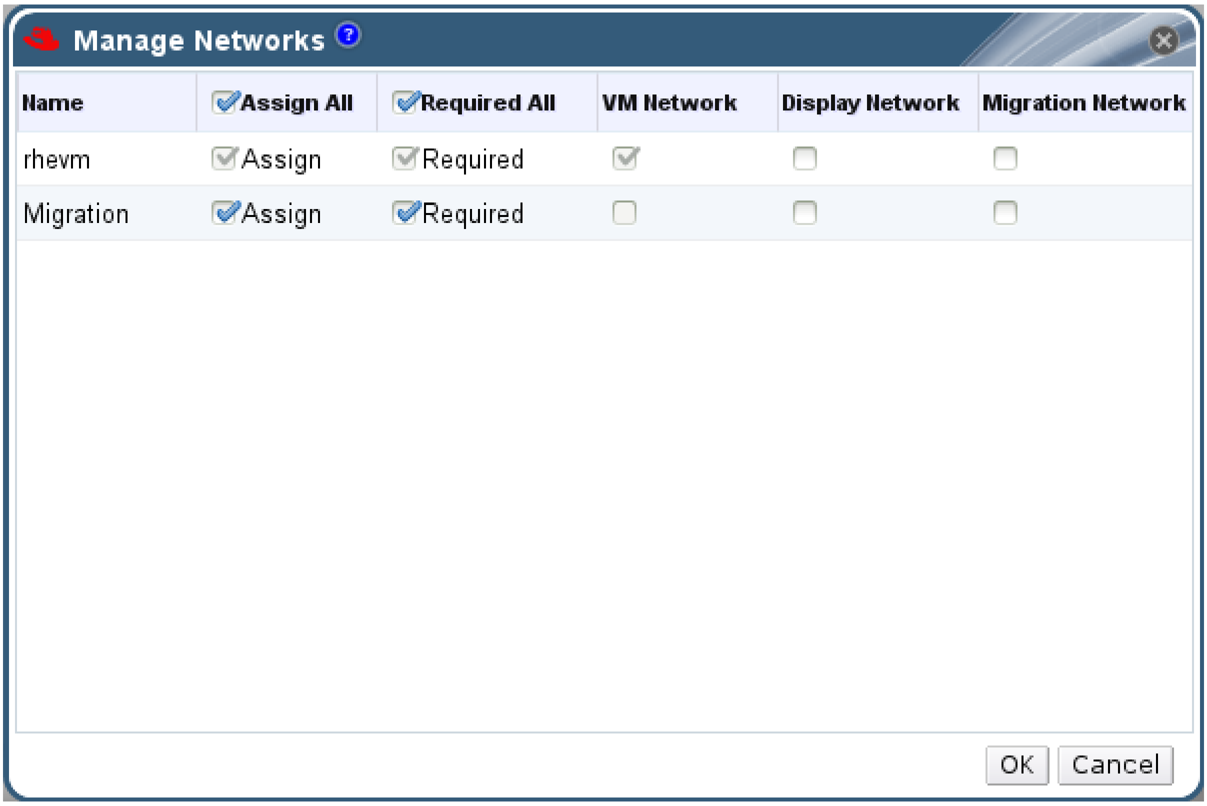


図6.1 ネットワークの管理

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

特定の論理ネットワークで特定のタイプのトラフィックが伝送されるように割り当てることにより、ネットワークトラフィックのフローを最適化しました。

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。

6.1.8. 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 ネットワーク設定の管理

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。

6.1.9. 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。

手順6.6 NIC の Virtual Function 設定の編集

1. SR-IOV 対応のホストを選択して、詳細ペインの **ネットワークインターフェース** タブをクリックします。

2. **ホストネットワークを設定** をクリックすると **ホストネットワークの設定** ウィンドウが開きます。

3.  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て、*NIC の* **VF（SR-IOV）設定の編集** ウィンドウを開きます。

4. 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。

5. **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が表示してから、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。

6. **OK** をクリックしてウィンドウを閉じます。**ホストネットワークの設定** ウィンドウで **OK** ボタンをクリックするまで設定の変更は有効にならない点に注意してください。

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

Virtual Network Interface (仮想 NIC) 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ーを追加/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。

手順6.7 仮想 NIC プロファイルの作成と編集

1. **ネットワーク** リソースタブをクリックし、結果一覧で論理ネットワークを選択します。

2. 詳細ペインで **仮想 NIC プロファイル** タブを選択します。ツリーモードで論理ネットワークを選択した場合には、ナビゲーションペインで **仮想 NIC プロファイル** タブを選択することができます。

3. **新規作成** または **編集** をクリックすると、**仮想マシンインターフェースのプロファイル** ウィンドウが表示されます。

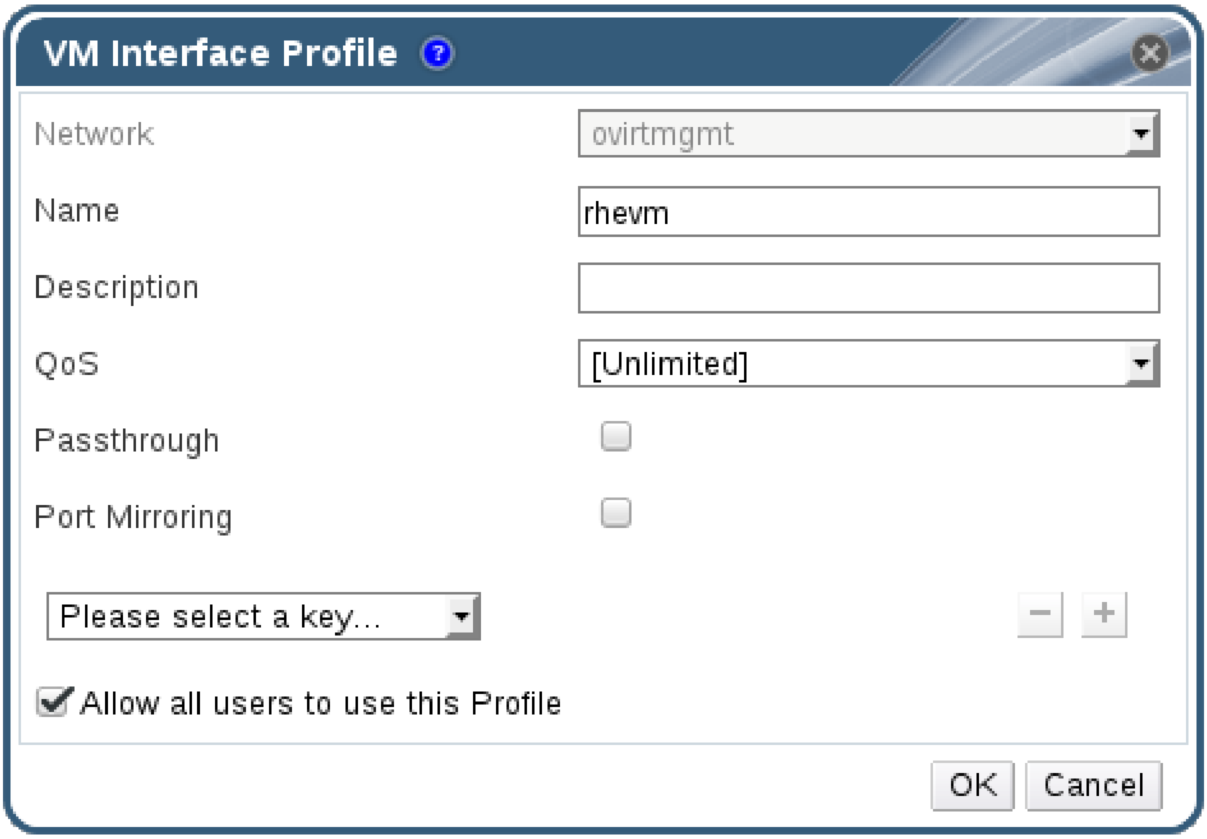


図6.2 仮想マシンインターフェースのプロファイルウィンドウ

4. プロファイルの **名前** と **説明** を入力します。

5. **QoS** 一覧から対象の QoS を選択します。

6. 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ーを有効にすると、QoS と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。

7. **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。

8. カスタムプロパティーの一覧からカスタムプロパティーを 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ーを追加または削除します。

9. **OK** をクリックします。

仮想 NIC プロファイルを作成しました。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る点に注意してください。

注記

ゲストオペレーティングシステムが、仮想 NIC のホットプラグとホットアンプラグをサポートする必要があります。

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利用可能なネットワークのドロップダウンメニュー
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メニュー。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。
パススルー	パススルーのプロパティー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ーは編集できません。 パススルーを有効にした場合には、QoS とポートミラーリングは仮想 NIC プロファイルで無効化されます。
ポートミラーリング	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。
デバイスのカスタムプロパティー	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ーを選択するためのドロップダウンメニュー。プロパティーを追加する場合は **+** ボタンを、削除する場合は **-** ボタンを使用します。
全ユーザーにこのプロファイルの使用を許可する	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。

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ーにより、SR-IOV を有効化した NIC の Virtual Function (VF) に仮想 NIC を直接接続することが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ー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 にパススルーが有効化されている場合には、そのプロファイルの QoS とポートミラーリングは無効になります。

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、『SR-IOV 実装に関するハードウェアの考慮事項』を参照してください。

手順6.8 パススルーの有効化

1. **ネットワーク** の結果一覧から論理ネットワークを選択してから詳細ペインの **仮想 NIC プロファイル** タブをクリックすると、その論理ネットワークの全仮想 NIC プロファイルが表示されます。

2. **新規作成** をクリックすると、**仮想マシンインターフェースのプロファイル** ウィンドウが表示されます。

3. プロファイルの **名前** と **説明** を入力します。

4. **パススルー** チェックボックスを選択します。これにより、**QoS** と **ポートミラーリング** が無効になります。

5. 必要な場合には、カスタムプロパティーの一覧からカスタムプロパティーを 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ーを追加または削除します。

6. **OK** をクリックしてプロファイルを保存し、ウィンドウを閉じます。

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。

手順6.9 仮想 NIC プロファイルの削除

1. **ネットワーク** リソースタブをクリックし、結果一覧で論理ネットワークを選択します。

2. 詳細ペインで **プロファイル** タブを選択すると、利用可能な仮想 NIC プロファイルが表示されます。ツリーモードで論理ネットワークを選択した場合には、ナビゲーションペインで **仮想 NIC プロファイル** タブを選択することができます。

3. プロファイルを 1 つまたは複数選択して **削除** をクリックすると、**仮想マシンインターフェースのプロファイルの削除** ウィンドウが開きます。

4. **OK** をクリックしてプロファイルを削除し、ウィンドウを閉じます。

6.2.6. 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、OpenStack Neutron を統合する場合のみに利用することができます。Red Hat Virtualization Manager ではセキュリティーグループを作成できません。セキュリティーグループは、OpenStack 内で作成する必要があります。詳しくは、『Red Hat OpenStack Platform Users and Identity Management Guide』の https://access.redhat.com/documentation/en/red-hat-openstack-platform/9/single/users-and-identity-management-guide#project-security 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ーグループを割り当てることができます。セキュリティーグループとは、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、セキュリティーグループを仮想 NIC プロファイルにアタッチする方法を説明します。

注記

セキュリティーグループは、OpenStack Networking インスタンスに登録されたのと同じセキュリティーグループの ID を使用して識別されます。特定のテナントのセキュリティーグループ ID を確認するには、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
```

手順6.10 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

1. **ネットワーク** タブをクリックし、結果一覧で論理ネットワークを選択します。

2. 詳細ペインで **仮想 NIC プロファイル** タブをクリックします。

3. **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** をクリックすると、**仮想マシンインターフェースのプロファイル** ウィンドウが開きます。

4. カスタムプロパティーのドロップダウンリストから **SecurityGroups** を選択します。カスタムプロパティーのドロップダウンを空欄のままにした場合には、デフォルトのセキュリティーグループが適用されます。デフォルトのセキュリティー設定は、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ー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** プロパティーを削除しても、適用済みのセキュリティーグループには影響を及ぼしません。

5. 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ーグループの ID を入力します。

6. **OK** をクリックします。

セキュリティーグループが仮想 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、そのセキュリティー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。

手順6.11 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** タブをクリックし、結果一覧で論理ネットワークを選択します。
2. **仮想 NIC プロファイル** のリソースタブを選択すると仮想 NIC プロファイルが表示されます。
3. 詳細ペインで **パーミッション** タブを選択すると、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** ボタンをクリックして **ユーザーへのシステム権限の追加** ウィンドウを開くか、**削除** ボタンをクリックして **パーミッションの削除** ウィンドウを開いて、仮想 NIC プロファイルに対するユーザーパーミッションの追加または削除を行います。

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の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ー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ー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ーの設定時には、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ーと既存のカスタムプロパティー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ーを含めてください。カスタムプロパティー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。

手順6.12 カスタムデバイスプロパティーの設定

1. Red Hat Virtualization Manager 上で、**vmfex** のカスタムプロパティーを設定し、**--cver** を使用してクラスターの互換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ーが追加されたことを確認します。

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

3. engine を再起動します。

```
# service ovirt-engine restart
```

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。

手順6.13 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** リソースタブをクリックし、結果一覧で論理ネットワークを選択します。
2. 詳細ペインで **仮想 NIC プロファイル** タブを選択します。ツリーモードで論理ネットワークを選択すると、ナビゲーションペインで **仮想 NIC プロファイル** タブを選択することができます。
3. **新規作成** または **編集** をクリックして、**仮想マシンインターフェースのプロファイル** ウィンドウを開きます。
4. プロファイルの **名前** と **説明** を入力します。
5. カスタムプロパティーの一覧から **vmfex** のカスタムプロパティーを選択して、UCS ポートプロファイル名を入力します。
6. **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のための OpenStack Networking Service (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。

手順6.14 外部プロバイダーからのネットワークのインポート

1. **ネットワーク** タブをクリックします。
2. **インポート** ボタンをクリックすると **ネットワークのインポート** ウィンドウが開きます。

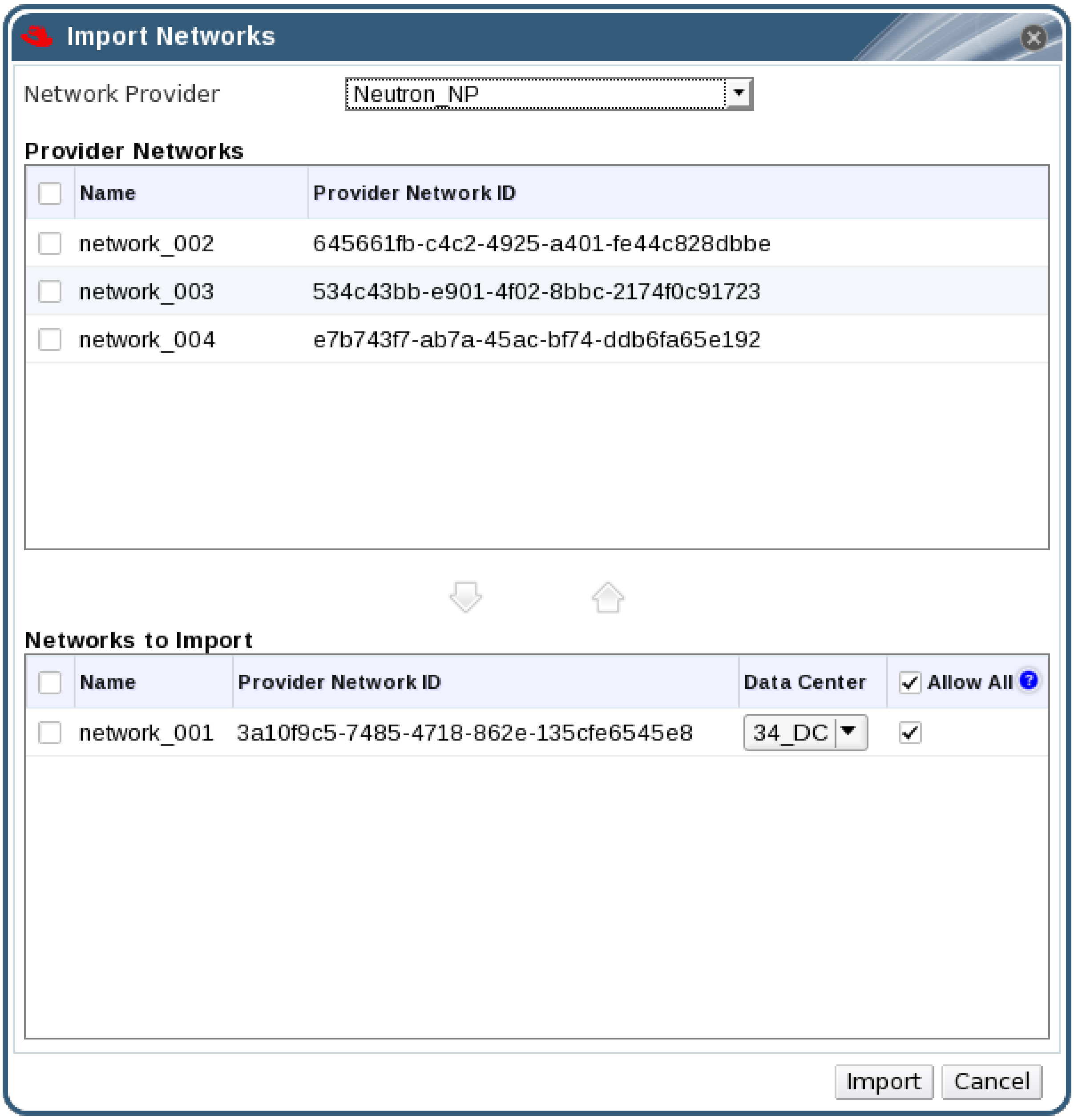


図6.3 ネットワークのインポートウィンドウ

3. **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、**インポートするネットワーク** リストのネットワークの **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** ボタンをクリックします。

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。

重要

外部プロバイダーからインポートされた論理ネットワークは、Red Hat Enterprise Linux ホスト以外とは互換性がないため、RHVH で実行されている仮想マシンには割り当てることはできません。

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

6.3.3.1. 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。

6.3.3.2. 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。

手順6.15 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** タブをクリックします。
2. 外部プロバイダーにより提供される論理ネットワークのうち、サブネットを追加する論理ネットワークをクリックします。
3. 詳細ペインの **サブネット** タブをクリックします。
4. **新規作成** ボタンをクリックし、**新規外部サブネット** ウィンドウを開きます。

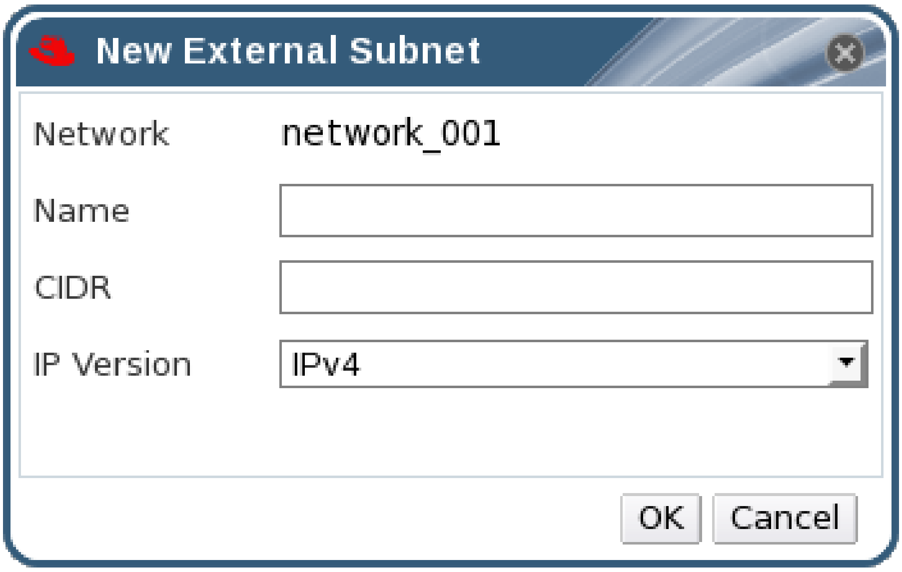


図6.4 新規外部サブネットウィンドウ

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** のドロップダウンメニューから、**IPv4** または **IPv6** のいずれかを選択します。
7. **OK** をクリックします。

6.3.3.3. 外部プロバイダー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。

手順6.16 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** タブをクリックします。
2. 外部プロバイダーにより提供される論理ネットワークのうち、サブネットを削除する論理ネットワークをクリックします。
3. 詳細ペインの **サブネット** タブをクリックします。
4. 削除するサブネットをクリックします。
5. **削除** をクリックし、プロンプトが表示されたら **OK** をクリックします。

6.4. 論理ネットワークおよびパーミッション

6.4.1. 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、より特定的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のみに対して (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のみに対して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。ヘッダーバーの **設定** ボタンをクリックすると、環境内の全ネットワークにネットワーク管理者を割り当てることができます。

ネットワーク管理者ロールは、以下のアクションを許可します。

- ネットワークの作成/編集/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。

6.4.2. ネットワークの管理者およびユーザーのロール

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

ロール	特権	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。

ロール	特権	備考
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。

6.4.3. 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。

手順6.17 リソースへのロール割り当て

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。
2. 詳細ペインの **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。

ユーザーにロールが割り当てられました。このユーザーは、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。

6.4.4. リソースからの管理者またはユーザーロールの削除

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。

手順6.18 リソースからのロール削除

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。
2. 詳細ペインの **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。パーミッションが削除されることを確認する **パーミッションの削除** ウィンドウが開きます。
5. **OK** をクリックします。

ユーザーロールおよび関連付けられたパーミッションが削除されました。

6.5. ホストとネットワーク

6.5.1. 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。

手順6.19 ホストの機能をリフレッシュする手順

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のホストを選択します。

2. **機能をリフレッシュ** ボタンをクリックします。

選択したホストの詳細ペインの **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。

6.5.2. 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。

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ることはできません。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。

手順6.20 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. **ホスト** リソースタブをクリックして、対象のホストを選択します。

2. 詳細ペインにある **ネットワークインターフェース** タブをクリックします。

3. **ホストネットワークを設定** ボタンをクリックすると **ホストネットワークの設定** ウィンドウが開きます。

4. 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。

5. 論理ネットワークを設定します。

   a. 割り当てられた論理ネットワークの上にマウスを移動し、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. **None**、**DHCP**、**Static** の中から **ブートプロトコル** を選択します。**Static** を選択した場合には、**IP**、**ネットマスク / ルーティングプレフィックス**、**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。

c. デフォルトのホストネットワーク QoS を上書きするには、**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ーを、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。

ホストネットワーク QoS の設定に関する詳しい情報は、「ホストネットワークの QoS」を参照してください。

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ー** のドロップダウンメニューをクリックして **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. ethtool のプロパティーを設定するには、**カスタムプロパティー** のドロップダウンメニューをクリックして **ethtool_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。**ethtool_opts** オプションはデフォルトでは使用できないので、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 のプロパティーに関する詳しい情報は、 man ページを参照してください。

f. 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。

6. 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のみに機能します。

7. 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。

8. **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、**機能をリフレッシュ** ボタンをクリックして、そのホストで利用可能なネットワークインターフェースカードの一覧を更新します。

6.5.3. 論理ネットワークを使用した単一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。

手順6.21 論理ネットワークを使用した、ネットワークインターフェースへの複数の VLAN 追加

1. **ホスト** リソースタブをクリックして、VLAN タグ付きの論理ネットワークが割り当てられたクラスターに関連付けられているホストを結果一覧から選択します。

2. 詳細ペインにある **ネットワークインターフェース** タブをクリックし、データセンター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。

3. **ホストネットワークを設定** をクリックすると **ホストネットワークの設定** ウィンドウが開きます。

4. 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。

5. 割り当て済み論理ネットワークの上にマウスを移動し、鉛筆のアイコンをクリックすると、**ネットワークの編集** ウィンドウが開きます。

   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。

   次のいずれかの **ブートプロトコル** を選択します。

   - **None**

   - **DHCP**

   - **Static**

     IP アドレス と **サブネットマスク** を入力します。

   OK をクリックします。

6. 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のみに機能します。

7. **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。

8. **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。

単一のインターフェースに VLAN タグの付いた論理ネットワークを複数追加しました。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追加することができます。

6.5.4. 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。

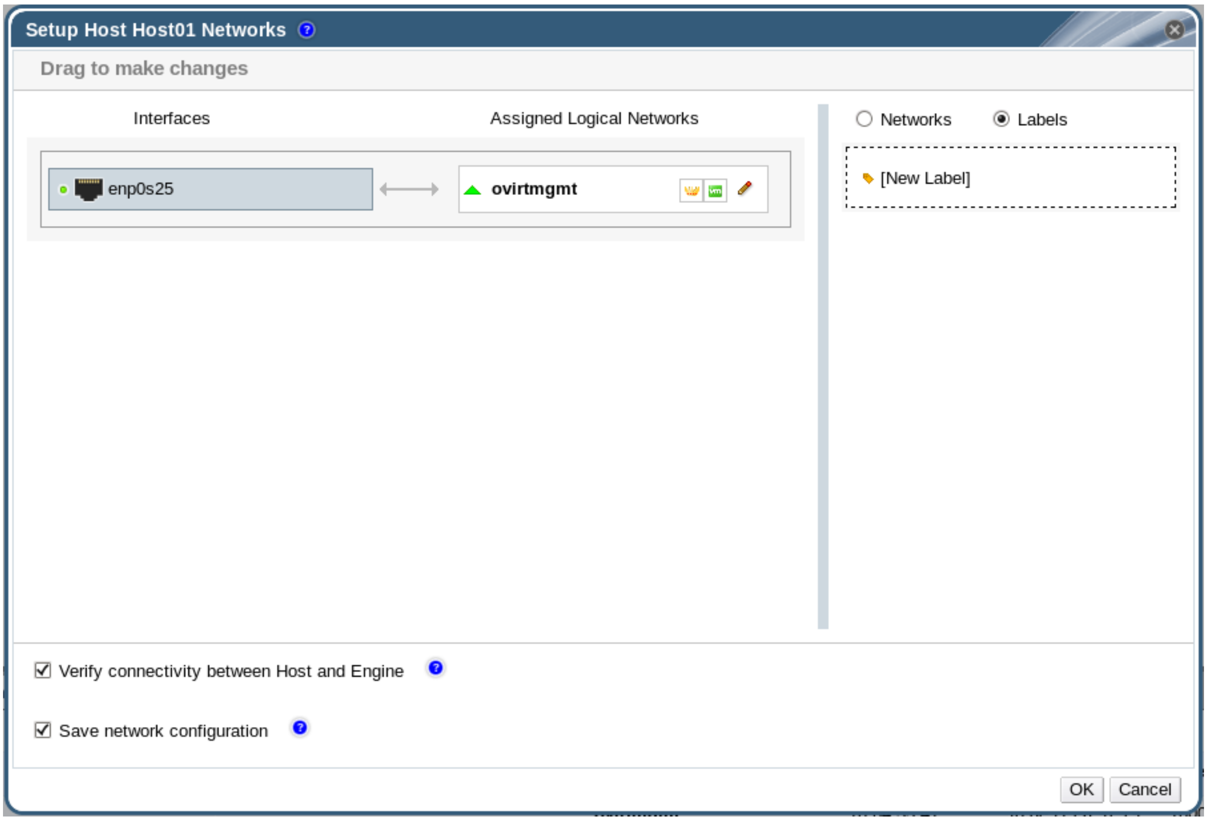
手順6.22 ホストネットワークインターフェースへのネットワークラベルの追加

1. **ホスト** リソースタブをクリックして、VLAN タグ付きの論理ネットワークが割り当てられたクラスターに関連付けられているホストを結果一覧から選択します。

2. 詳細ペインにある **ネットワークインターフェース** タブをクリックし、データセンター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。

3. **ホストネットワークを設定** をクリックすると **ホストネットワークの設定** ウィンドウが開きます。

4. **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。



5. **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。

6. **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。

6.5.5. ボンディング

6.5.5.1. 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6.7 ボンディングシナリオとその結果

ボンディングシナリオ	結果
NIC + NIC	**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。 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。
NIC + Bond	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。 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。
Bond + Bond	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。 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。

6.5.5.2. ボンディング

*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、ボンディングで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。

ボンディングモード
Red Hat Virtualization は、デフォルトでモード 4 を使用しますが、以下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。

6.5.5.3. 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。

手順6.23 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. **ホスト** リソースタブをクリックして、結果一覧でホストを選択します。

2. 詳細ペインにある **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。

3. **ホストネットワークを設定** をクリックすると **ホストネットワークの設定** ウィンドウが開きます。

4. 一方のデバイスを選択して、他方のデバイスの上にドラ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。

5. 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。

6. **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。

7. 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。

8. 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。

9. **OK** をクリックして変更を受け入れ、**ホストネットワークの設定** ウィンドウを閉じます。

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、選択したホストの詳細ペインにある **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は、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。

6.5.5.4. 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
```

6.5.6. 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。

手順6.24 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。

6.5.7. ホストの IP アドレスの変更

手順6.25

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. **admin** ユーザーとしてホストにログインします。

4. **F2** を押して **OK** を選択し、**Enter** を押してレスキューシェルに入ります。

5. **/etc/sysconfig/network-scripts/ifcfg-ovirtmgmt** ファイルを編集して、IP アドレスを変更します。以下に例を示します。

   ```
   # vi /etc/sysconfig/network-scripts/ifcfg-ovirtmgmt
   ...
   BOOTPROTO=none
   IPADDR=10.x.x.x
   PREFIX=24
   ...
   ```

6. ネットワークサービスを再起動して、IP アドレスが更新されたことを確認します。

   ```
   # systemctl restart network.service
   ```

   ```
   # ip addr show ovirtmgmt
   ```

7. **exit** と入力してレスキューシェルを終了し、テキストユーザーインターフェースに戻ります。

8. 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。ホストを選択して、詳細ペインの **全般** タブの下の **ソフトウェア** をクリックして、**OS の説明** を確認します。

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 にはセキュリティー機能が有効化されています。Security Enhanced Linux (SELinux) および iptables 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、詳細ペインにある **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のみに属していること。
- 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ー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ー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.

> **警告**
>
> 現在、NetworkManager (**nmcli**、**nmtui**、Cockpit ユーザーインターフェースを含む) を使用したネットワークの設定はサポートされていません。Manager にホストを追加する前に追加のネットワーク設定が必要な場合は、**ifcfg** ファイルに手動で記述する必要があります。詳しい情報は『Red Hat Enterprise Linux ネットワークガイド』 を参照してください。

7.2. RED HAT VIRTUALIZATION HOST

Red Hat Virtualization Host (RHVH) は、仮想マシンをホストするのに必要なパッケージのみで構成される 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。ただし、追加のパッケージのインストールは現在サポートされていません。追加のパッケージをインストールした場合には、RHVH が更新されるたびに毎回再インストールする必要があります。

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。SHH 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: 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、**Tools** > **Terminal** のサブタブからコマンドを実行するのに使用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。

> **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 **Tools** > **Terminal** 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。

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があります。

ホストを追加する際には、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、ホストの再起動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、詳細ペインを使用してください。

重要

サードパーティー製のウォッチドッグは、VDSM によって提供される watchdog デーモンを妨げる可能性あるので、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、ブリッジの作成、ホストの再起動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、詳細ペインで確認してください。

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

1. 管理ポータルで、**ホスト** リソースタブをクリックします。
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 **アドレス** 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、公開鍵認証に使用します。
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、JSON プロトコルの使用を無効にすることができます。
    c. 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、セキュリティー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、ホストが電源管理カードをサポートしている場合には、電源管理を設定するこ

とができます。電源管理の設定に関する情報は、「ホストの電源管理の設定」のセクションを参照してください。

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、詳細ペイン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。

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。

手順7.2 Satellite ホストプロバイダーのホストの追加

1. **ホスト** リソースタブをクリックすると、結果一覧にホストが一覧表示されます。
2. **新規作成** をクリックすると、**新規ホスト** ウィンドウが表示されます。
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** 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**、**アドレス**、**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、JSON プロトコルの使用を無効にすることができます。
   c. 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、セキュリティー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. 対象のタブで **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、詳細ペイン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。ステータスが **Up** に変わるには、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のと同じ画面で、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 4.0 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せん。

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。

手順7.3 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. **ホスト** タブをクリックして、結果一覧でホストを選択します。

   b. **編集** をクリックし、**ホストの編集** ウィンドウを開きます。

   c. **Foreman/Satellite を使用する** チェックボックスにチェックを付けます。

   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

7.5.4.1. ホストの全般設定

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 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
データセンター	ホストが属するデータセンター。Red Hat Virtualization Host (RHVH) は、Gluster が有効化されたクラスターには追加できません。
ホストクラスター	ホストが属するクラスター

フィールド名	説明
`Foreman/Satellite` を使用する	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。 **検出されたホスト** • **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た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 • **コンピュートリソース**: コンピュートリソースを提供するハイパーバイザーのドロップダウンリスト **プロビジョン済みホスト** • **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	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
アドレス	ホストの IP アドレス、または解決可能なホスト名
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 **/root/.ssh/authorized_hosts** 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	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。
JSON プロトコルを使用する	このチェックボックスはデフォルトで有効化されます。これは、**詳細パラメーター** の設定です。
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 **フェッチ** して、ホストが返す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。

7.5.4.2. ホストの電源管理の設定

電源管理 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。

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。新しい 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には、Manager が、そのホストマシンの電源を切断し、また負荷分散でそのホストが必要となった場合や、クラスター内で空いているホストが不足した場合には、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
順次に使用するエージェント	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。 • 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。 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。 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。
フェンスエージェントの追加	プラス (**+**) 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、このウィンドウ内のフィールドについての詳しい説明をまとめています。
電源管理プロキシーの設定	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ーを検索するように指定されます。フェンシングプロキシー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** の下にあります。

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

フィールド名	説明
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
タイプ	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。 • **`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
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

フィールド名	説明
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。
オプション	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。 Red Hat Enterprise Linux 7 ホストで、電源管理デバイスに cisco_ucs を使用する場合には、**オプション** フィールドに **ssl_insecure=1** を追記する必要もあります。
セキュリティー保護	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。

7.5.4.3. SPM 優先度の設定

SPM 設定の表には、**新規ホスト** や **ホストの編集** ウィンドウの **SPM** タブで必要な情報を詳しく記載しています。

表7.4 SPM 設定

フィールド名	説明
SPM 優先度	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。

7.5.4.4. ホストコンソールの設定

コンソール の設定表には、**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詳しく記載しています。

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用です。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。

7.5.5. ホストの電源管理設定値の設定

管理ポータルからホストのライフサイクル操作 (停止、開始、再起動) を行うには、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。

重要

電源管理設定を行う前には、そのホストが **Maintenance** モードに入っていることを確認します。このモードに入っていない場合には、そのホストで実行されている仮想マシン、ホストの再起動時にすべて強制終了され、実稼働環境が停止してしまうことになります。ホストが **Maintenance** モードに正しく設定されていない場合は、警告のメッセージが表示されます。

手順7.4 電源管理設定値の設定

1. **ホスト** タブをクリックして、結果一覧でホストを選択します。
2. **編集** をクリックし、**ホストの編集** ウィンドウを開きます。
3. **電源管理** タブをクリックし、電源管理設定を表示します。
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

   既存のホストに **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、ホストの **クラスター** の **スケジューリングポリシー** によってホストの電源管理が制御され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. 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。

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** を適切なフィールドに入力します。

9. ドロップダウンリストから、電源管理デバイスの **タイプ** を選択します。

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** 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。

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 がホストの **cluster** および **dc** (データセンター) でフェンシングプロキシーを探す順序を指定します。

17. **OK** をクリックします。

管理ポータルで、**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。

7.5.6. ホストの Storage Pool Manager の設定

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、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。

手順7.5 SPM 設定値の設定

1. **ホスト** リソースタブをクリックして、結果一覧でホストを選択します。

2. **編集** をクリックし、**ホストの編集** ウィンドウを開きます。

3. **SPM** タブをクリックすると、**SPM 優先度** の設定画面が表示されます。

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** をクリックして設定を保存し、ウィンドウを閉じます。

ホストの SPM 優先度設定が完了しました。

7.5.7. リソースの編集

リソースのプロパティーを編集します。

手順7.6 リソースの編集

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。

2. **編集** をクリックして **編集** ウィンドウを開きます。

3. 必要なプロパティーを変更して **OK** をクリックします。

新規プロパティーがリソースに保存されました。プロパティーフィールドが無効の場合には、**編集** ウィンドウは閉じません。

7.5.8. 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。

手順7.7 ホストをメンテナンスモードに切り替える手順

1. **ホスト** リソースタブをクリックして、対象のホストを選択します。

2. **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、**ホストのメンテナンス** 確認ウィンドウで、ホストをメンテナンスモードに切り替える **理由** を入力して、メンテナンスモードに切り替える理由を指定することができます。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、「クラスターの全般設定」を参照してください。

4. **OK** をクリックしてメンテナンスモードを開始します。

稼働中の仮想マシンはすべて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、ホストの **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、その仮想マシンの **移行をキャンセル** をクリックし、移行を停止します。

7.5.9. 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。

手順7.8 メンテナンスモードのホストのアクティブ化

1. **ホスト** リソースタブをクリックして、ホストを選択します。

2. **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。

7.5.10. ホストの削除

仮想化環境からホストを削除します。

手順7.9 ホストの削除

1. 管理ポータルで、**ホスト** リソースタブをクリックして、結果一覧でホストを選択します。

2. ホストをメンテナンスモードに切り替えます。

3. **削除** をクリックすると **ホストの削除** の確認ウィンドウが開きます。

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。

環境からホストが削除され、**ホスト** タブに表示されなくなりました。

7.5.11. 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と持つためにマイナーリリースの更新を行う方法は、『アップグレードガイド』の https://access.redhat.com/documentation/en/red-hat-virtualization/4.0/single/upgrade-guide/#chap-Updates_between_Minor_Releases の項を参照してください。

7.5.12. 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。ハイパーバイザーの ISO イメージから現在インストール済みの RHVH と同じバージョンのハイパーバイザーをインストールする場合には、以下の手順に従ってください。この手

順では、Red Hat Enterprise Linux ホストに VDSM が再インストールされます。これには、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と、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。

手順7.10 Red Hat Virtualization Host および Red Hat Enterprise Linux ホストの再インストール

1. **ホスト** リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のホストを選択します。
2. **メンテナンス** ボタンをクリックします。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. **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。**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。

7.5.13. 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と、そのタグを基に検索を行うことができます。

手順7.11 タグを使用したホストのカスタマイズ

1. **ホスト** リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のホストを選択します。
2. **タグを割り当て** をクリックすると、**タグの割り当て** ウィンドウが開きます。

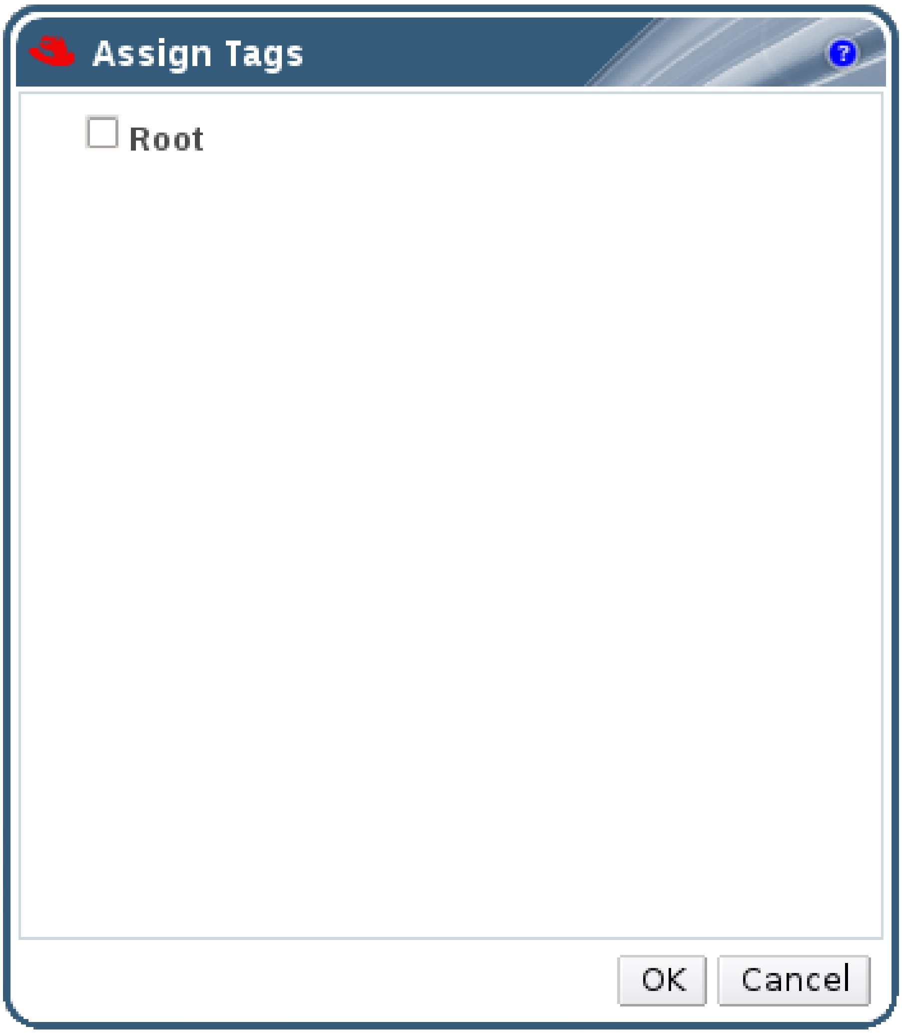


図7.1 タグの割り当てのウィンドウ

3. **タグの割り当て** のウィンドウには、使用可能なタグがすべて一覧表示されます。対象のタグのチェックボックスを選択します。

4. **OK** をクリックしてタグを割り当て、ウィンドウを閉じます。

ホストに関する、検索可能な補足情報がタグとして追加されます。

7.5.14. 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には、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。

手順7.12 ホストのエラータの表示

1. **ホスト** リソースタブをクリックして、結果一覧でホストを選択します。

2. 詳細ペインで **全般** タブをクリックします。

3. **全般** タブ内の **エラータ** サブタブをクリックします。

7.5.15. 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、管理者が設定して、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
- **Info**: 
- **Warning**: 
- **Error**: 
- **Failure**: 

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、ホストを選択してから **イベント** サブ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。

7.5.16. ホストデバイスの表示

詳細ペインで、各ホストのホストデバイスを表示することができます。ホストでデバイスを直接割り当てるために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。

デバイスの直接割り当てに関する詳しい情報は、『Red Hat Virtualization SR-IOV 実装に関するハードウェアの考慮事項』の「デバイス割り当てを使用するための追加のハードウェア考慮事項」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。

手順7.13 ホストデバイスの表示

1. **ホスト** リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のホストを選択します。
2. 詳細ペインの **ホストデバイス** タブをクリックします。

詳細ペインに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。

7.5.17. 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。また、変更を有効にするには、両マシンを再起動する必要もあります。

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、『インストールガイド』の「PCI デバイスの要件」のセクションを参照してください。

手順7.14 GPU パススルーを使用するためのホストの準備

1. ホストサーバーにログインして、デバイスの *vendor ID:product ID* 見つけます。以下の例では ID は **10de:13ba** と **10de:0fbc** です。

    ```
    # lspci -nn
    ...
    01:00.0 VGA compatible controller [0300]: NVIDIA Corporation GM107GL
    [Quadro K2200] [10de:13ba] (rev a2)
    01:00.1 Audio device [0403]: NVIDIA Corporation Device [10de:0fbc]
    (rev a1)
    ...
    ```

2. grub 設定ファイルを編集して、**GRUB_CMDLINE_LINUX** の行の末尾に *pci-stub.ids=xxxx:xxxx* を追記します。

    ```
    # vi /etc/default/grub
    ...
    GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... pci-
    stub.ids=10de:13ba,10de:0fbc"
    ...
    ```

    ホスト上で対応するドライバーをブラックリストします。以下の例では、**GRUB_CMDLINE_LINUX** の行に追記して、nVidia の nouveau ドライバーをブラックリストしています。

    ```
    # vi /etc/default/grub
    ...
    GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... pci-
    stub.ids=10de:13ba,10de:0fbc rdblacklist=nouveau"
    ...
    ```

    grub 設定ファイルを保存します。

3. **grub.cfg** ファイルをリフレッシュしてからサーバーを再起動し、変更を有効にします。

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

    ```
    # reboot
    ```

4. **lspci** コマンドを実行して、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
...
```

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。

手順7.15 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

  a. 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"
  ...
  ```

  b. 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)
  ```

  c. **/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
  ```

  d. 仮想マシンを再起動します。

- Windows の場合

  a. デバイスに対応するドライバーをダウンロードして、インストールします。たとえば、Nvidia ドライバーの場合は、NVIDIA Driver Downloads のページにアクセスします。

  b. 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、『Red Hat Virtualization 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。

7.5.18. 管理ポータルからの Cockpit へのアクセス

Cockpit UI プラグインは、Red Hat Virtualization 環境にインストール可能なオプションの機能で、このプラグインを利用すると、ホストリソースの監視や管理に使用する Cockpit ユーザーインターフェースに管理ポータルからアクセスすることができます。ホストに Cockpit がインストールされている場合は、**Cockpit** サブタブをクリックすると、管理ポータルの詳細ペインに Cockpit ユーザーインターフェースが直接表示されます。または、メインの **ホスト** メニューの **Cockpit** ボタンをクリックすると、Cockpit ユーザーインターフェースが新しいブラウザータブに表示されます。

デフォルトでは Cockpit ユーザーインターフェースは Red Hat Virtualization Host (RHVH) で利用可能ですが、Red Hat Enterprise Linux ホストでは現在サポートされていません。

手順7.16 管理ポータルからの Cockpit へのアクセス

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

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

2. **ovirt-engine** サービスを再起動します。

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

3. 管理ポータルで **ホスト** タブをクリックして、ホストを選択します。

4. 新規タブで Cockpit ユーザーインターフェースを開くか、管理ポータルから Cockpit インターフェースを直接表示します。

   - ホストを右クリックして **Cockpit** を選択し、新規ブラウザータブに Cockpit ユーザーインターフェースを開きます。

   - **Cockpit** サブタブをクリックして、**ホスト** タブの詳細ペインに Cockpit ユーザーインターフェースを表示します。

注記

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

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。

電源管理デバイスを使用するホストが Manager と通信できなくなった場合には、そのホストを管理ポータルからフェンス (リブート) することができます。そのホスト上で実行されている仮想マシンはすべて停止され、高可用性の仮想マシンが別のホストで起動されます。

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。

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る上、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。

電源管理のパラメーターを使用すると、ホストを自動的にフェンス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。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。

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

7.6.2. Red Hat Virtualization 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** フィールドを使用します。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。

手順7.17 ホスト上でのフェンシングパラメーターの設定

1. **ホスト** リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のホストを選択します。
2. **編集** をクリックし、**ホストの編集** ウィンドウを開きます。
3. **電源管理** タブをクリックします。

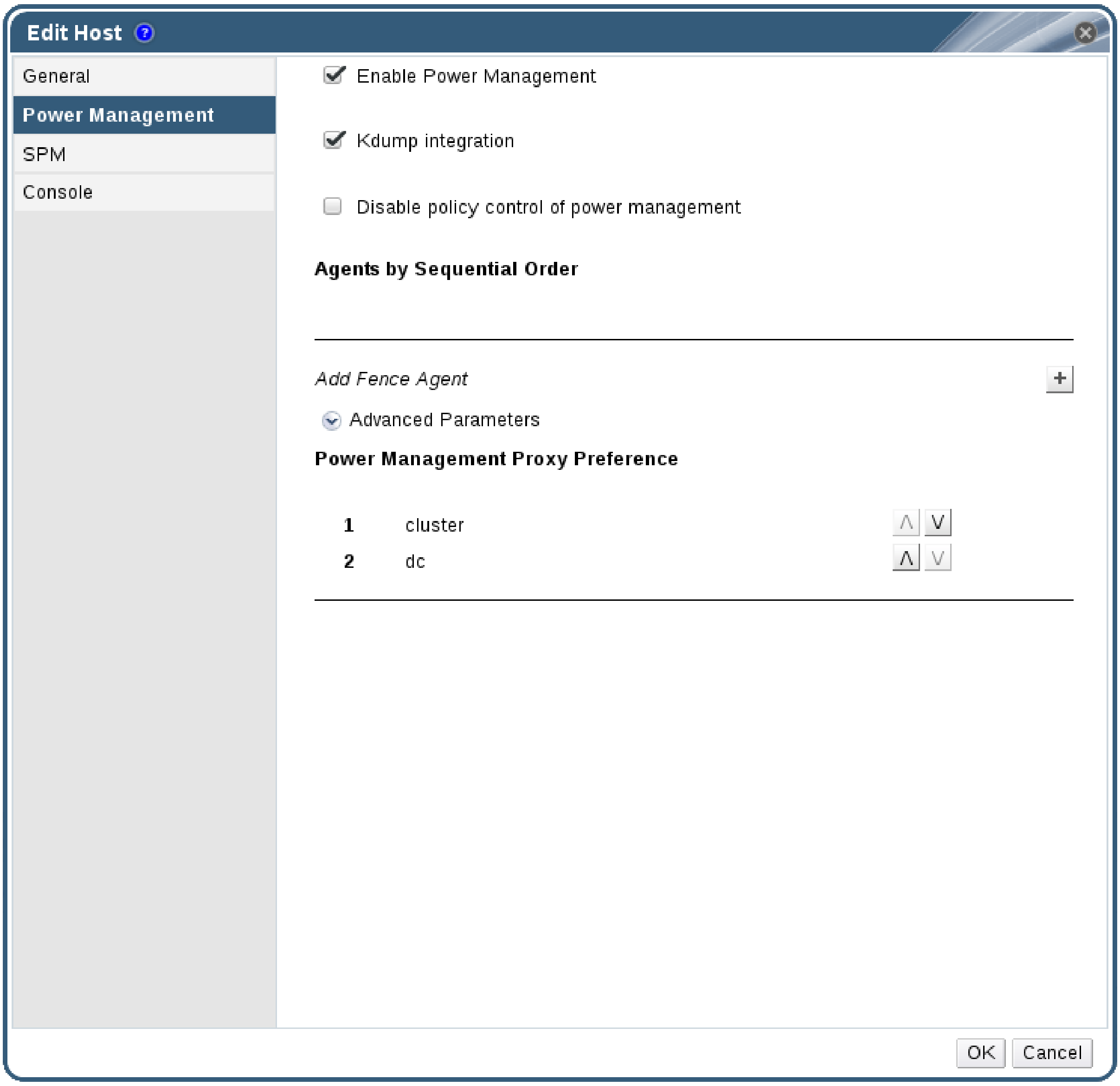


図7.2 電源管理の設定

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

既存のホストに **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。

7. 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。

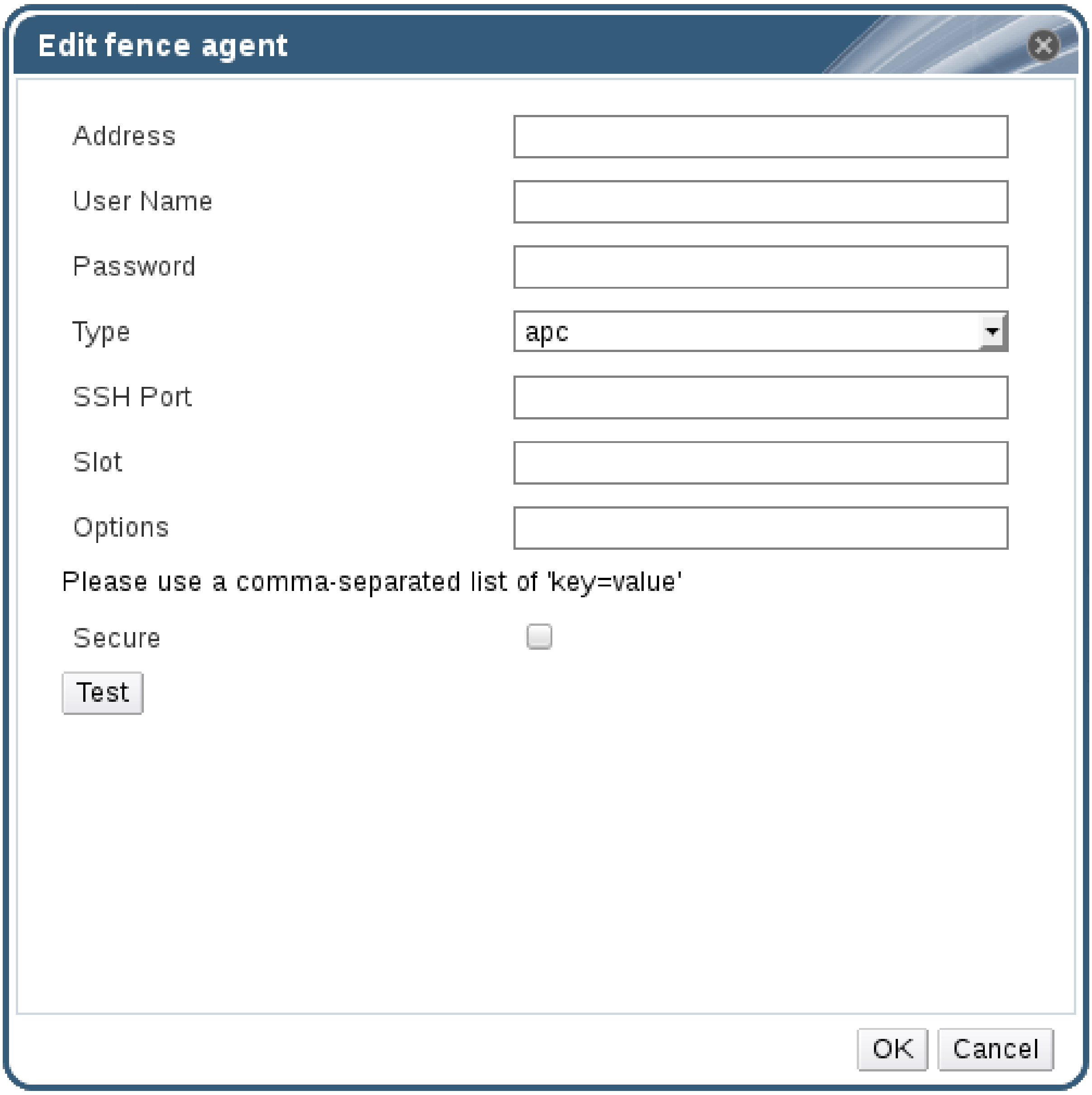


図7.3 フェンスエージェントの編集

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

9. ドロップダウンリストから、電源管理デバイスの **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、https://access.redhat.com/articles/1238743 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を無視した場合や、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 がホストの **cluster** および **dc** (データセンター) でフェンシングプロキシーを探す順序を指定します。

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

ホストを選択して、詳細ペインの **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、旧バージョンの 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、パッケージ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。

手順7.18 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。

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

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7.6 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。

変数	説明	デフォルト	注記
LISTENER_PORT	fence_kdump メッセージを受信するポートを定義します。	7410	このパラメーターの値を変更する場合には、**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
```

手順7.19 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。

```
# service ovirt-engine restart
```

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7.7 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。
FenceKdumpMessageInterval	fence_kdump の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。

変数	説明	デフォルト	注記
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ーホスト (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) が存在している必要があります。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。この時間を決定する計算式は、TimeoutToResetVdsInSeconds (デフォルトは 60 秒) + [DelayResetPerVmInSeconds (デフォルトは 0.5 秒)]*(ホスト上で実行中の仮想マシン数) + [DelayResetForSpmInSeconds (デフォルトは 20 秒)] * 1 (ホストが SPM として稼働している場合) または 0 (ホストが SPM としては稼働していない場合) の設定値によって設定されます。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) で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 **`vdsm restart`** が実行されます。

4. **vdsm 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

概要

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することが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。

手順7.20 ホストの電源管理機能の使用方法

1. **ホスト** リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のホストを選択します。

2. **電源管理** ドロップダウンメニューをクリックします。

3. 以下のオプションのいずれかを選択します。

    - **再起動**: このオプションはホストを停止させて、ホストのステータスが **Down** に変わるのを待ちます。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、クラスターに追加します。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。

    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。

4. 上記のいずれかのオプションを選択すると、確認のウィンドウが表示されます。**OK** をクリックして確定し、続行します。

結果

選択したアクションが実行されます。

7.6.7. 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

概要

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。

手順7.21 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. **ホスト** タブでホストを選択します。ステータスは **Non Responsive** と表示されるはずです。
2. ホストを手動で再起動します。これは、物理的にラボに入って、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、ホストエントリーを右クリックし、**ホストがリブートされていることを確認**のボタンを選択します。
4. ホストがシャットダウンまたは再起動されていることを確認するメッセージが表示されます。**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。

結果

ホストを手動でリブートして、高可用性の仮想マシンがアクティブなホストで起動できるようになりました。管理ポータルで手動によるフェンシング操作を確認し、ホストがオンライン状態となりました。

7.7. ホストとパーミッション

7.7.1. 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、より特定的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のみに対して (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のみに対して管理者権限があります。

ホスト管理者は、特定のホストのみのシステム管理者ロールです。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 1 人ずつ必要な場合に有用です。ヘッダーバーの **設定** ボタンを使用して、環境内の全ホストにホスト管理者を割り当てることができます。

ホスト管理者ロールは、以下のアクションを許可します。

- ホストの設定の編集
- 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。

7.7.2. 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7.8 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。

7.7.3. 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。

手順7.22 リソースへのロール割り当て

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。
2. 詳細ペインの **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。

ユーザーにロールが割り当てられました。このユーザーは、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。

7.7.4. リソースからの管理者またはユーザーロールの削除

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。

手順7.23 リソースからのロール削除

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。

2. 詳細ペインの **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。パーミッションが削除されることを確認する **パーミッションの削除** ウィンドウが開きます。

5. **OK** をクリックします。

ユーザーロールおよび関連付けられたパーミッションが削除されました。

第8章 ストレージ

Red Hat Virtualization では、仮想マシンのディスクイメージ、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
- 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初期化できないため、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ので、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。

Red Hat Virtualization では、管理ポータルの **ストレージ** タブを使用して、ストレージの割り当てと管理を行うことができます。**ストレージ** の結果一覧には、すべてのストレージドメインが表示されます。詳細ペインには、ドメインに関する全般情報が表示されます。

ストレージドメインを追加するには、管理ポータルに正常にアクセスすることが可能で、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必要なくなります。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ーです。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イメージ、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 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ーに集約された後に、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の管理』ガイド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 6 サーバー上でデータドメインおよびエクスポート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。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G システムアカウント」を参照してください。

注記

以下の手順には、非推奨になったエクスポートストレージドメインの設定のステップが含まれます。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イメージ、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。

1. NFS ツールを提供する nfs-utils パッケージをインストールします。

```
# yum install nfs-utils
```

2. ブートスクリプトを設定して、システムのブート時に毎回共有が使用できるようにします。

```
# chkconfig --add rpcbind
# chkconfig --add nfs
# chkconfig rpcbind on
# chkconfig nfs on
```

3. rpcbind サービスおよび nfs サービスを起動します。

```
# service rpcbind start
# service nfs start
```

4. data および export の各ディレクトリーを作成します。

```
# mkdir -p /exports/data
# mkdir -p /exports/export
```

5. 新規作成したディレクトリーを **/etc/exports** ファイルに追加します。**/etc/exports** に以下の内容を追記してください。

```
/exports/data *(rw)
/exports/export *(rw)
```

6. ストレージドメインをエクスポートします。

```
# exportfs -r
```

7. NFS サービスを再読み込みします。

```
# service nfs reload
```

8. **kvm** というグループを作成します。

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

9. 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
```

10. 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。これにより、Manager はこれらのエクスポートされたディレクトリーによって表示されるストレージドメイン内にデータを保管することができるようになります。

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

11. 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
```

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、仮想化ゲストイメージおよび 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 **`Export / NFS`** を選択します。

1. Red Hat Virtualization Manager 管理ポータルで **ストレージ** リソースタブをクリックします。

2. **新規ドメイン** をクリックします。

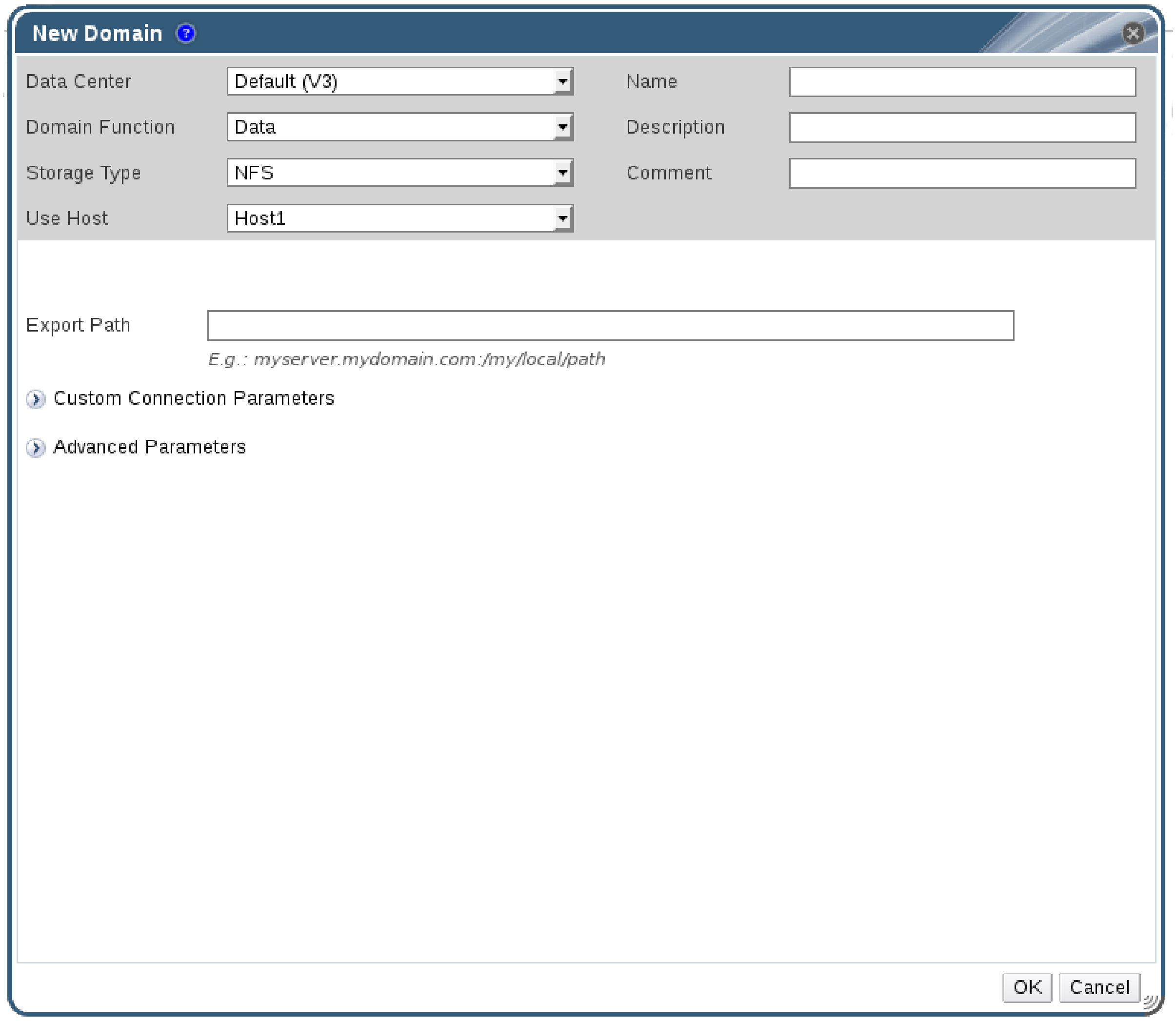


図8.1 新規ドメインウィンドウ

3. ストレージドメインの **名前** を入力します。

4. **データーセンター**、**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たディスクの「削除後にワイプ」プロパティーは変更されません。

7. **OK** をクリックします。

   新規 NFS データドメインが **ストレージ** タブに表示されます。ディスクの準備が完了するまでステータスが **Locked** と表示され、その後には自動的にデータセンター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。

手順8.1 既存の NFS ストレージドメインの拡張

1. **ストレージ** リソースタブをクリックして、NFS ストレージドメインを選択します。

2. 詳細ペインで **データセンター** タブをクリックし、**メンテナンス** ボタンをクリックしてストレージドメインをメンテナンス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。

3. 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。

4. 詳細ペインで **データセンター** タブをクリックし、**アクティブ化** ボタンをクリックしてストレージドメインをマウントします。

8.3. ローカルストレージの準備と追加

8.3.1. ローカルストレージの準備

ホスト上にローカルストレージドメインをセットアップすることができます。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G システムアカウント」を参照してください。

重要

Red Hat Virtualization Host (RHVH) で、ローカルストレージに使用するパスは /var ディレクトリー内にある必要があります。以下の手順では、/var 内にストレージディレクトリーを作成します。

手順8.2 ローカルストレージの準備

1. ホストで、ローカルストレージとして使用するディレクトリーを作成します。

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

2. **vdsm** ユーザー (UID 36) と **kvm** グループ (GID 36) がそのディレクトリーに読み取り/書き込みアクセスが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。

注記

ホストマシンに外部のストレージをマウントして、ローカルストレージドメインとして使用することも可能です。ストレージのマウントについての詳しい情報は、Red Hat Enterprise Linux 『ストレージ管理ガイド』を参照してください。

8.3.2. ローカルストレージの追加

ホストのローカルストレージの準備が完了したので、次に Manager を使用してそのストレージをホストに追加します。

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。

手順8.3 ローカルストレージの追加

1. **ホスト** リソースタブをクリックして、結果一覧でホストを選択します。
2. **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. **OK** をクリックしてメンテナンスモードを開始します。
4. **ローカルストレージを設定** をクリックすると、**ローカルストレージの設定** ウィンドウが開きます。

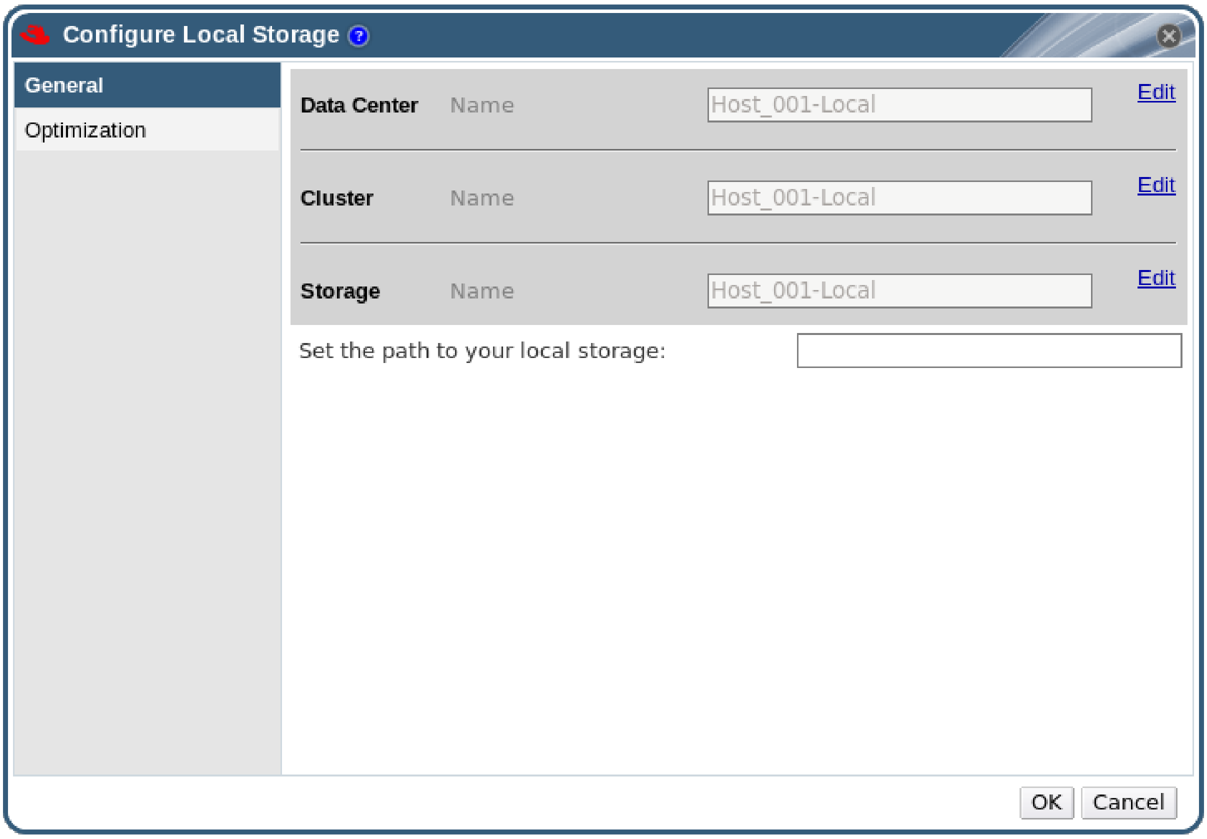


図8.2 ローカルストレージの設定ウィンドウ

5. **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。

6. 文字入力フィールドにローカルストレージへのパスを設定します。

7. **最適化** タブを選択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。

8. **OK** をクリックして設定を保存し、ウィンドウを閉じます。

ホストのデータセンター内でオンライン表示されます。

8.4. POSIX 準拠ファイルシステムストレージの準備と追加

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

Red Hat Virtualization でストレージドメインとして使用する POSIX 準拠のファイルシステムは、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。

8.4.1. POSIX 準拠ファイルシステムストレージのアタッチ

NFS、iSCSI、または FCP 以外を使用してマウントする POSIX 準拠のファイルシステムをストレージドメインとして使用します。

手順8.4 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** リソースタブをクリックすると、結果一覧に既存のストレージドメインが表示されます。

2. **新規ドメイン** をクリックすると、**新規ドメイン** ウィンドウが開きます。

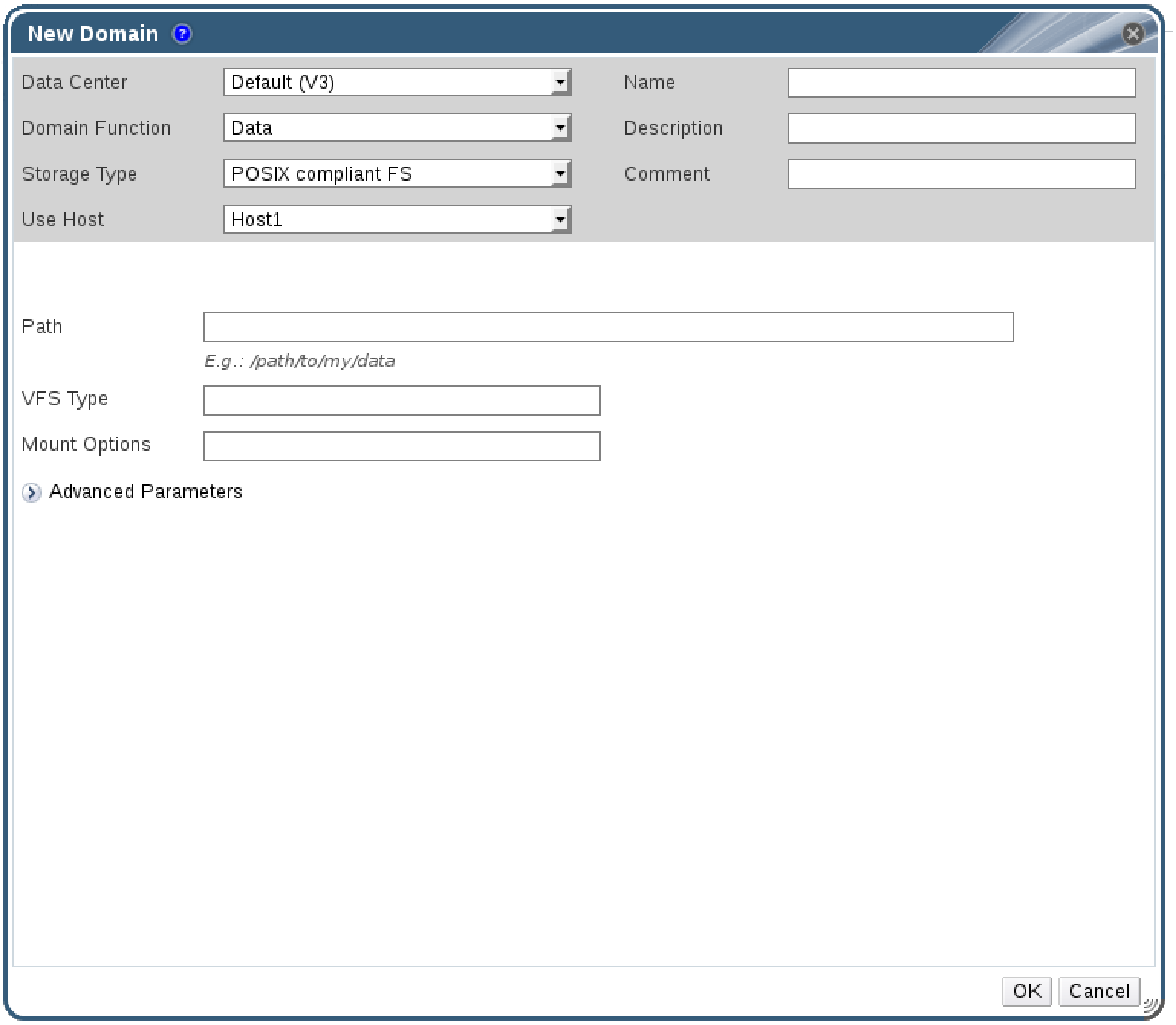


図8.3 POSIX ストレージ

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 compliant 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/ストレージタイプ** のドロップダウンメニューから **`Data / POSIX compliant FS`** を選択します。

   該当する場合には、ドロップダウンメニューから **フォーマット** を選択します。

6. **使用するホスト** のドロップダウンメニューからホストを選択します。選択したデータセンターの中にあるホストのみが表示されます。選択したホストを使って、ストレージドメインに接続します。

7. 通常 **`mount`** コマンドに渡すように、POSIX ファイルシステムへの **パス** を入力します。

8. 通常、***`-t`*** 引数を使用して **`mount`** コマンドに渡すときのように、**`VFS Type`** を入力します。有効な VFS 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`** コマンドに渡すときのように、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たディスクの「削除後にワイプ」プロパティーは変更されません。

11. **`OK`** をクリックすると新規ストレージドメインがアタッチされ、ウィンドウが閉じます。

8.5. ブロックストレージの準備と追加

8.5.1. iSCSI ストレージの準備

Red Hat Enterprise Linux 6 を実行するサーバーから iSCSI ストレージデバイスをエクスポートして、Red Hat Virtualization でストレージドメインとして使用するには、以下の手順に従ってください。

手順8.5 iSCSI ストレージの準備

1. ストレージサーバーで root として **`yum`** コマンドを実行して、**scsi-target-utils** パッケージをインストールします。

   ```
   # yum install -y scsi-target-utils
   ```

2. エクスポートするデバイスまたはファイルを **`/etc/tgt/targets.conf`** ファイルに追加します。**`targets.conf`** ファイルへの追記の一般的な例は以下のとおりです。

   ```
   <target iqn.YEAR-MONTH.com.EXAMPLE:SERVER.targetX>
             backing-store /PATH/TO/DEVICE1 # Becomes LUN 1
             backing-store /PATH/TO/DEVICE2 # Becomes LUN 2
             backing-store /PATH/TO/DEVICE3 # Becomes LUN 3
   </target>
   ```

- ターゲットは通常、作成年月、サーバーが属するドメインを後ろから順に記載した FQDN、サーバー名、ターゲット番号で定義します。

3. **tgtd** サービスを起動します。

```
# service tgtd start
```

4. 再起動後も **tgtd** が起動するように永続的に設定します。

```
# chkconfig tgtd on
```

5. iptables のファイアウォールポートを開き、クライアントが iSCSI エクスポートにアクセスするのを許可します。デフォルトでは、iSCSI はポート 3260 を使用します。以下の例では、ファイアウォールルールを INPUT テーブルのポジション 6 に挿入します。

```
# iptables -I INPUT 6 -p tcp --dport 3260 -j ACCEPT
```

6. 作成した iptables ルールを保存します。

```
# service iptables save
```

基本的な iSCSI エクスポートを作成しました。このエクスポートは iSCSI データドメインとして使用することができます。

8.5.2. iSCSI 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、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 ストレージ管理ガイド』の「オンラインストレージ管理」のセクションを参照してください。

手順8.6 iSCSI ストレージの追加

1. **ストレージ** リソースタブをクリックすると、結果一覧に既存のストレージドメインが表示されます。

2. **新規ドメイン** ボタンをクリックし、**新規ドメイン** ウィンドウを開きます。

3. 新規ストレージドメインの **名前** を入力します。

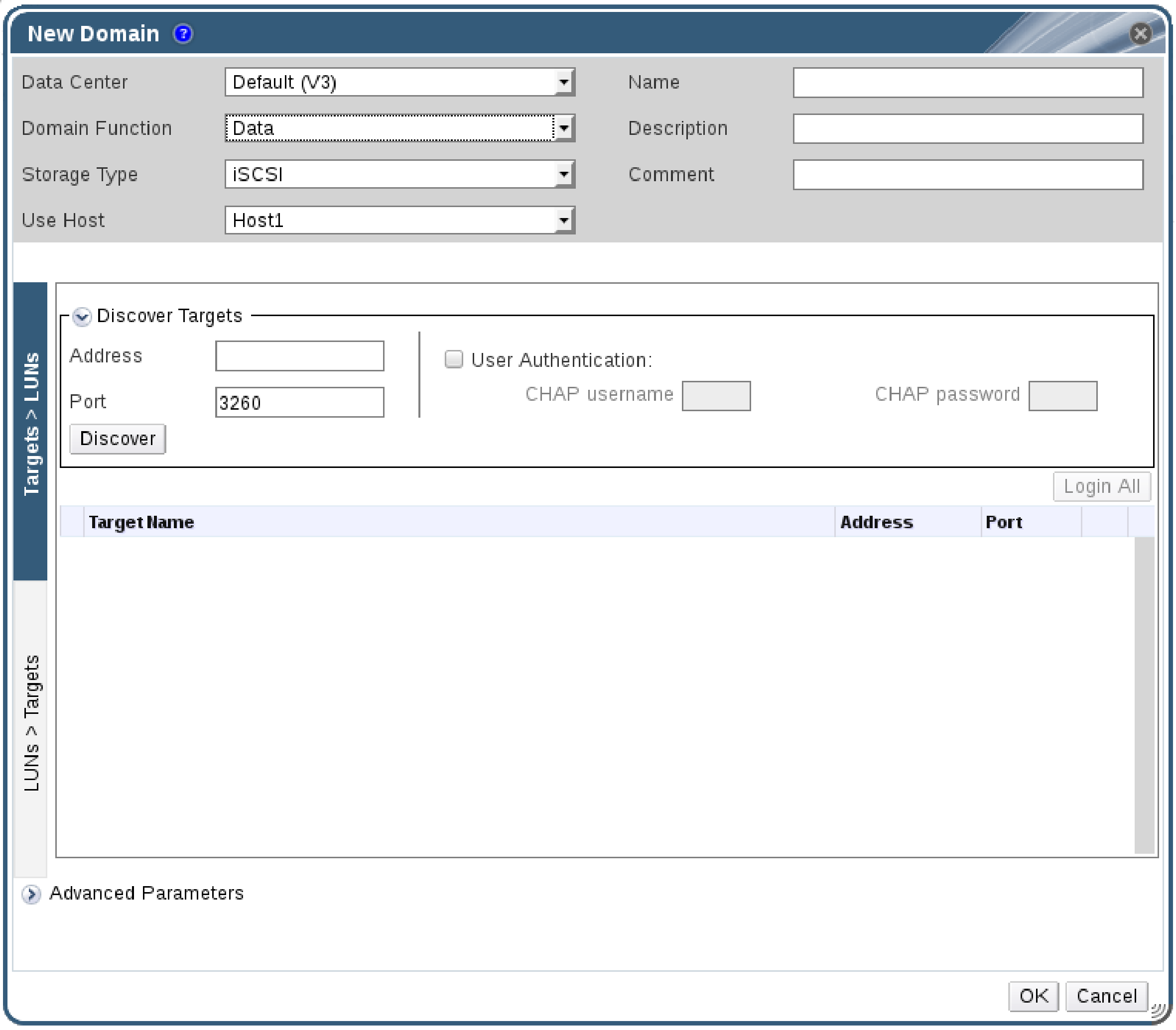


図8.4 新規 iSCSI ドメイン

4. **データセンター** のドロップダウンメニューでデータセンターを選択します。

5. ドロップダウンメニューで **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なければなりません。

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。iSCSI をストレージタイプに選択すると、**新規ドメイン** ダイアログには未使用の LUN を持つ既知のターゲットが自動的に表示されます。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。

iSCSI ターゲット検出

1. **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。

2. **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。

3. **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。

4. ストレージのセキュリティー保護に 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 ユーザー名`** と **`CHAP 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。

5. **検出** ボタンをクリックします。

6. 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。エントリーが展開され、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たディスクの「削除後にワイプ」プロパティーは変更されません。

11. **OK** をクリックするとストレージドメインが作成され、ウィンドウが閉じます。

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。

8.5.3. 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。

手順8.7 iSCSI マルチパス機能の設定

1. **データセンター** タブをクリックして、結果一覧からデータセンターを選択します。
2. 詳細ペインで **iSCSI マルチパス** タブをクリックします。
3. **追加** をクリックします。
4. **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。
5. **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** 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** プロパティーを変更するには、管理ポータルでそのネットワークを選択し、ネットワーク名をクリックして詳細ビューを表示し、**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。

6. **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。

7. **OK** をクリックします。

データセンター内の全ホストは、選択した論理ネットワークを介して、選択した iSCSI ターゲットに接続されます。

8.5.4. 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/構成に関する情報は、『ストレージ管理ガイド』 および 『DM Multipath ガイド』を参照してください。

以下の手順は、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。

手順8.8 FCP ストレージの追加

1. **ストレージ** リソースタブをクリックして、全ストレージドメインを一覧表示します。

2. **新規ドメイン** をクリックすると、**新規ドメイン** ウィンドウが開きます。

3. ストレージドメインの **名前** を入力します。

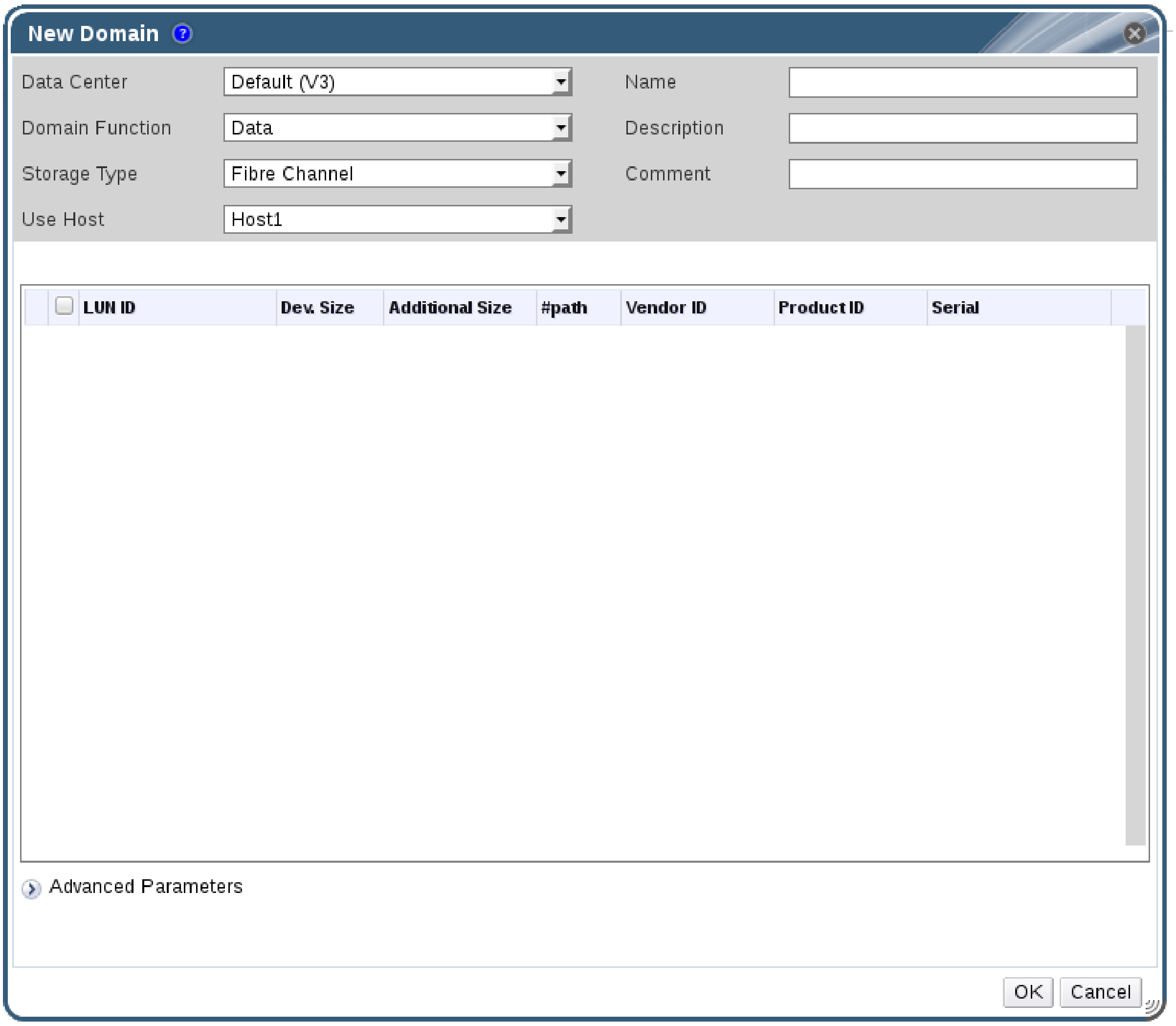


図8.5 FCP ストレージの追加

4. **データセンター** ドロップダウンメニューで FCP データセンターを選択します。

   適切な FCP データセンターがない場合には **(None)** を選択します。

5. ドロップダウンメニューで **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 **Data / Fibre Channel** 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たディスクの「削除後にワイプ」プロパティーは変更されません。

9. **OK** をクリックするとストレージドメインが作成され、ウィンドウが閉じます。

ストレージ タブに新規 FCP データドメインが表示されます。使用準備中には、**Locked** 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。

8.5.5. 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、複数の方法があります。

- 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)

- 新しい LUN を作成して、既存のストレージドメインに追加する

- 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 6 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 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。

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。

手順8.9 既存の iSCSI または FCP ストレージドメインの拡張

1. SAN 上に新規 LUN を作成します。

2. **ストレージ** リソースタブをクリックして、iSCSI または FCP ドメインを選択します。

3. **編集** ボタンをクリックします。

4. **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。

5. ストレージサーバーへの接続情報を入力し、**検出** ボタンをクリックして、接続を開始します。

6. **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。

7. **OK** をクリックして、選択したストレージドメインに LUN を追加します。

これにより、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、Red Hat Virtualization 管理ポータルで LUN をリフレッシュする必要もあります。

手順8.10 LUN サイズのリフレッシュ

1. **ストレージ** リソースタブをクリックして、iSCSI または FCP ドメインを選択します。
2. **編集** ボタンをクリックします。
3. **LUN > ターゲット** をクリックします。
4. **追加するサイズ** のコラムで、LUN の ***Additional_Storage_Size*** **追加** ボタンをクリックしてリフレッシュします。
5. **OK** をクリックして、LUN をリフレッシュすると、新しいストレージのサイズが表示されます。

8.5.6. Red Hat Virtualization で使用できない LUN

場合によっては、Red Hat Virtualization で LUN を使用してストレージドメインや仮想マシンのハードディスクを作成することができません。

- すでに、現在の Red Hat Virtualization 環境の一部となっている LUN は、使用されないように自動設定されます。

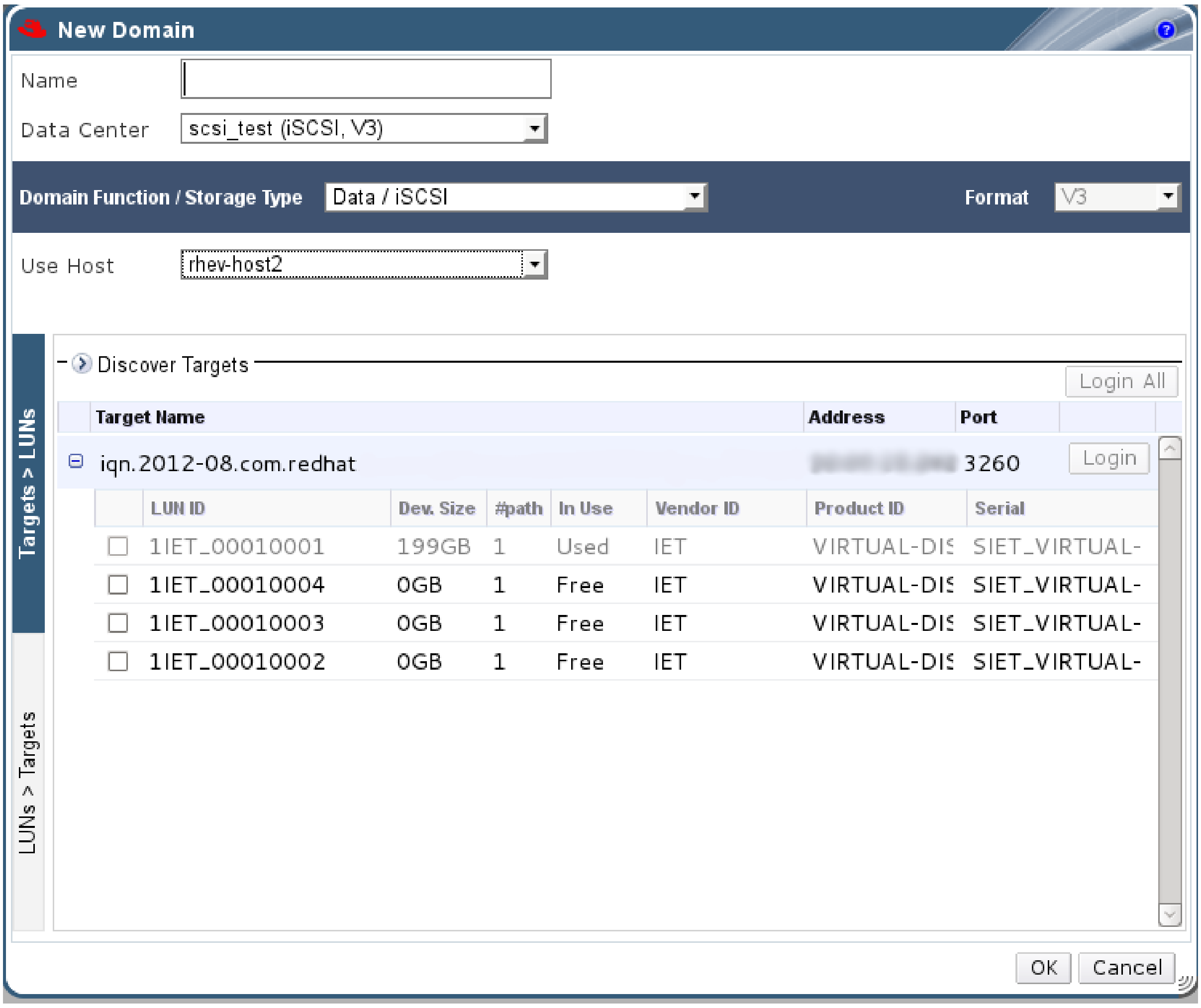


図8.6 Red Hat Virtualization 管理ポータルで使用できない LUN

- SPM ホストがすでに使用している LUN も使用中と表示されます。これらの LUN の内容を強制的に上書きするよう選択することも可能ですが、この上書きの操作が正常に行われる保証はありません。

8.6. 既存のストレージドメインのインポート

8.6.1. 既存のストレージドメインのインポートについての概要

データが一切格納されていない新規ストレージドメインを追加するだけでなく、既存のストレージドメインをインポートして、その中に格納されているデータにアクセスすることも可能です。ストレージドメインのインポート機能により、Manager データベースでエラーが発生した際にデータを復旧して、そのデータをデータセンター間または環境間で移行することができます。

ストレージドメインタイプ別のインポートについての概要は以下のとおりです。

データ

既存のデータストレージドメインをインポートすると、そのデータストレージドメインに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には、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たすべての 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た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、同じの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イメージ、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初期化済みである必要があります。

手順8.11 ストレージドメインのインポート

1. **ストレージ** リソースタブをクリックします。
2. **ドメインをインポート** をクリックします。

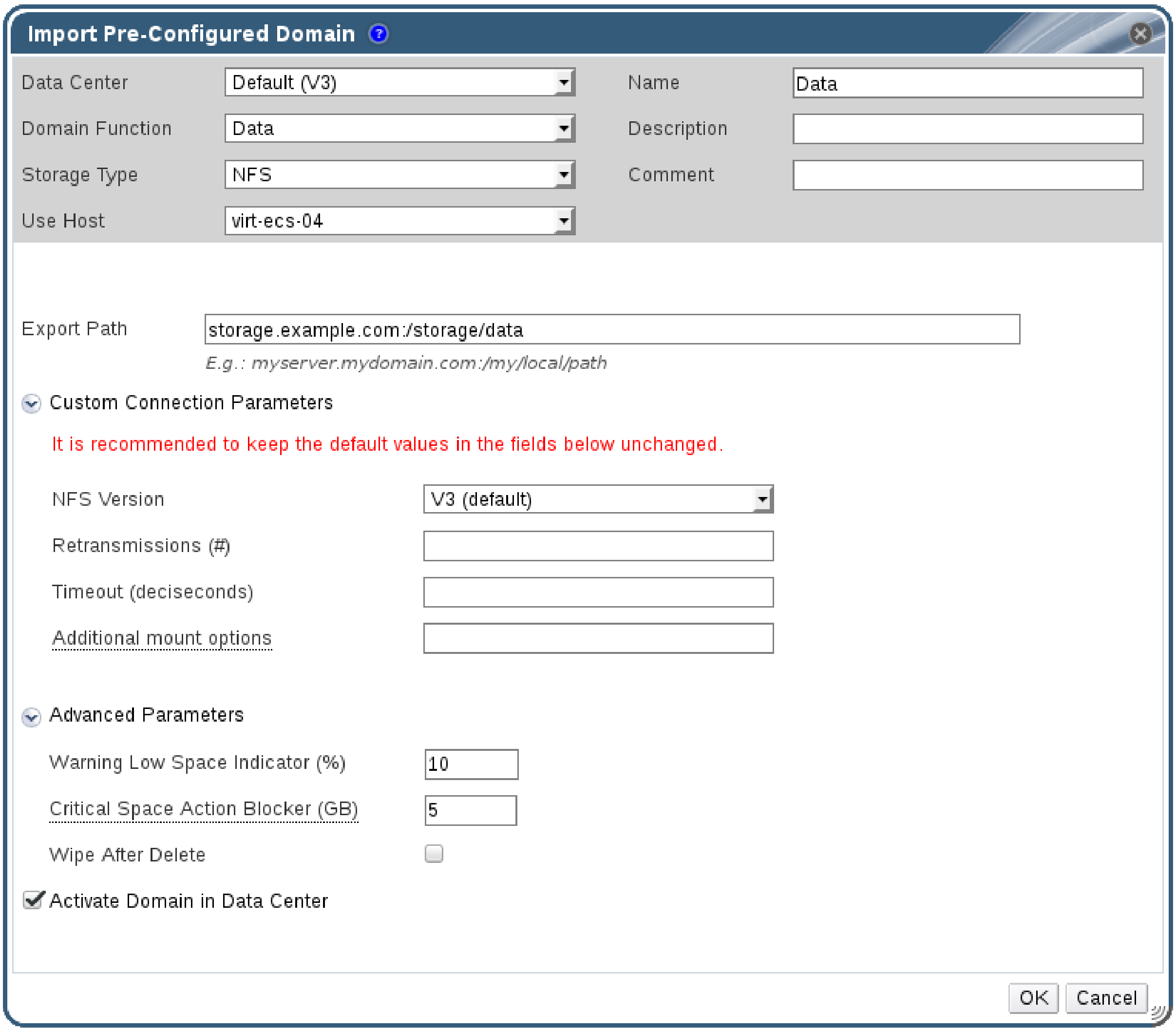


図8.7 事前設定済みドメインのインポートのウィンドウ

3. **データセンター** のドロップダウンリストから、ストレージドメインをアタッチするデータセンターを選択します。

4. ストレージドメインの名前を入力します。

5. **ドメイン機能** と **ストレージタイプ** のドロップダウンリストから適切な項目を選択します。

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/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。これらのオプションは、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。オプションについての詳しい情報は 「ストレージドメインについての知識」を参照してください。

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。

ストレージドメインがインポートされ、**ストレージ** タブに表示されます。これで、インポートしたストレージドメインから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。

手順8.12 同じ環境内のデータセンター間でのストレージドメインの移行

1. 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** リソースタブをクリックして、結果一覧からストレージドメインを選択します。

3. 詳細ペインで **データセンター** タブをクリックします。

4. **メンテナンス** をクリックしてから **OK** をクリックすると、ストレージドメインがメンテナンスモードに切り替わります。

5. **デタッチ** をクリックしてから **OK** をクリックすると、移行元のデータセンターからストレージドメインがデタッチされます。

6. **アタッチ** をクリックします。

7. 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。

手順8.13 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** リソースタブをクリックして、結果一覧からストレージドメインを選択します。
4. 詳細ペインで **データセンター** タブをクリックします。
5. **メンテナンス** をクリックしてから **OK** をクリックすると、ストレージドメインがメンテナンスモードに切り替わります。
6. **デタッチ** をクリックしてから **OK** をクリックすると、移行元のデータセンターからストレージドメインがデタッチされます。
7. **削除** をクリックします。
8. **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。
9. **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。
10. 移行先の環境の管理ポータルにログインします。
11. **ストレージ** リソースタブをクリックします。
12. **ドメインをインポート** をクリックします。

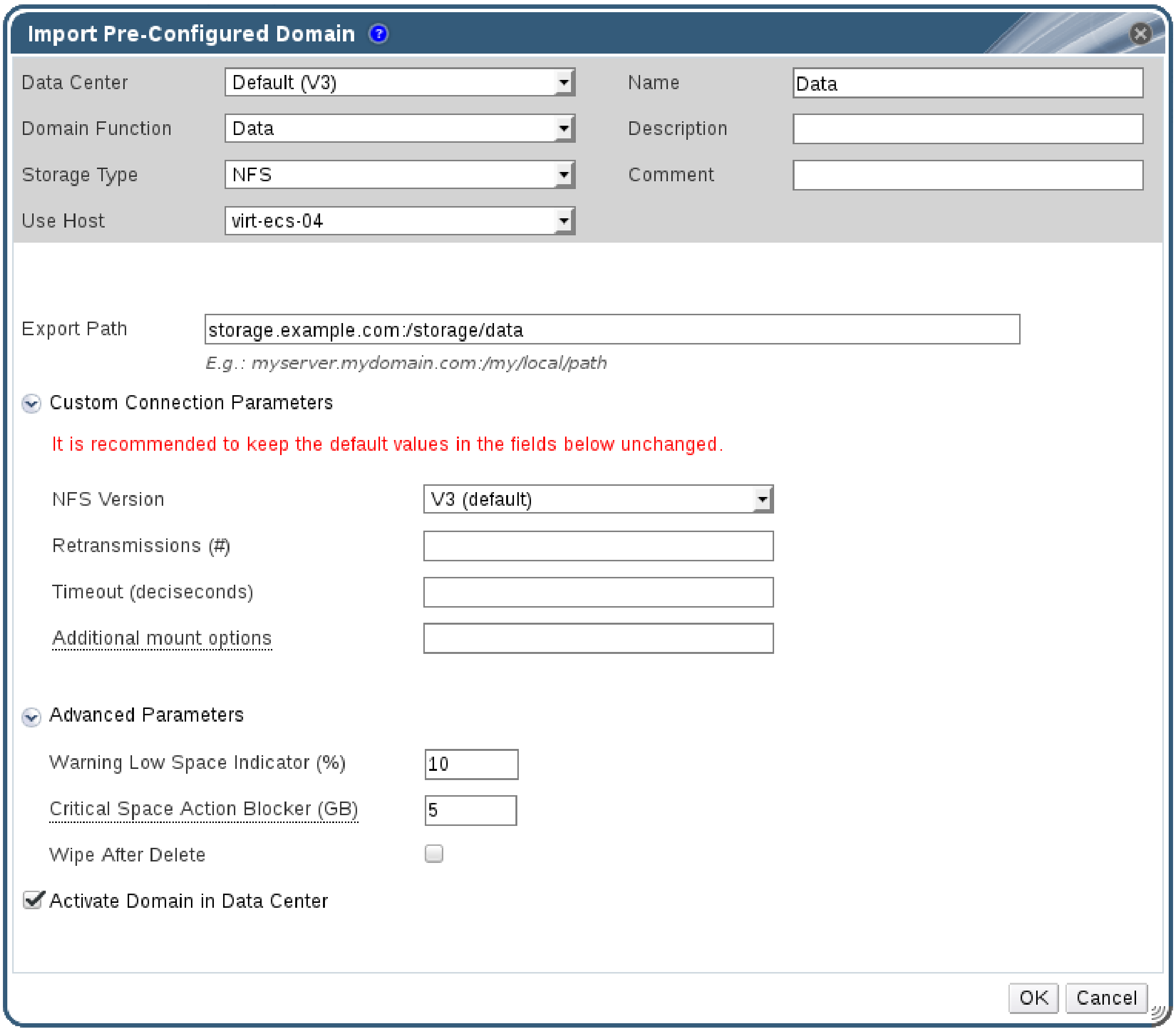


図8.8 事前設定済みドメインのインポートのウィンドウ

13. **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。

14. ストレージドメインの名前を入力します。

15. **ドメイン機能** と **ストレージタイプ** のドロップダウンリストから適切な項目を選択します。

16. **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。

17. 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。これらのオプションは、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。オプションについての詳しい情報は 「ストレージドメインについての知識」を参照してください。

18. Select the **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。

19. **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。

手順8.14 インポートされたデータストレージドメインからの仮想マシンのインポート

1. **ストレージ** リソースタブをクリックします。
2. インポートしたデータストレージドメインをクリックします。
3. 詳細ペインで **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. **クラスター** の一覧から、仮想マシンのインポート先となるクラスターを選択します
7. **OK** をクリックします。

環境に仮想マシンがインポートされます。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。

手順8.15 インポートされたデータストレージドメインからのテンプレートのインポート

1. **ストレージ** リソースタブをクリックします。
2. インポートしたデータストレージドメインをクリックします。
3. 詳細ペインで **テンプレートのインポート** の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. **クラスター** の一覧から、テンプレートのインポート先となるクラスターを選択します
7. **OK** をクリックします。

環境にテンプレートがインポートされます。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。

8.6.7. インポートされたストレージドメインからのディスクイメージのインポート

詳細ペインの **ディスクのインポート** タブを使用して、インポートされたストレージドメインからフローティング仮想ディスクをインポートします。

注記

Manager にインポート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。

手順8.16 ディスクイメージのインポート

1. データセンターにインポートしたストレージドメインを選択します。
2. 詳細ペインで **ディスクのインポート** をクリックします。
3. インポートする仮想マシンを 1 台または複数選択して **インポート** をクリックすると、**ディスクのインポート** ウィンドウが開きます。
4. 各ディスクに適切な **ディスクプロファイル** を選択します。
5. **OK** をクリックすると選択したディスクがインポートされます。

8.6.8. インポートされたストレージドメインからの未登録ディスクイメージのインポート

詳細ペインの **ディスクのインポート** タブを使用して、ストレージドメインからフローティング仮想ディスクをインポートします。Red Hat Virtualization 環境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、インポート予定で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。

手順8.17 ディスクイメージのインポート

1. データセンターにインポートしたストレージドメインを選択します。
2. ストレージドメインを右クリックして、Manager が未登録のディスクを特定できるように **ディスクのスキャン** を選択します。
3. 詳細ペインで **ディスクのインポート** 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て **インポート** をクリックすると、**ディスクのインポート** ウィンドウが開きます。
5. 各ディスクに適切な **ディスクプロファイル** を選択します。
6. **OK** をクリックすると選択したディスクがインポートされます。

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データ読み込み

ISO ストレージドメインは、データセンターにアタッチして、ISO イメージをアップロードする必要があります。Red Hat Virtualization は、イメージを正しいパスに正しいユーザーパーミッションでアップロードするための ISO アップローダーツールを提供しています。

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。

手順8.18 ISO ストレージドメインへのデータ読み込み

1. Red Hat Virtualization Manager を実行しているシステムの一時ディレクトリーに、対象の ISO イメージをコピーします。

2. Red Hat Virtualization Manager を実行しているシステムに **root** ユーザーでログインします。

3. **engine-iso-uploader** コマンドを使用して ISO イメージをアップロードします。この操作には多少時間がかかり、アップロードするイメージのサイズや使用可能なネットワークの帯域幅によって所要時間が異なります。

   > **例8.1 ISO アップローダーの使用例**
   >
   > 以下の例では、**RHEL6.iso** の ISO イメージを **ISODomain** という名前の ISO ドメインに NFS でアップロードしています。コマンドでは、管理者のユーザー名およびパスワードの入力が求められます。ユーザー名は *username@domain* の形式で入力する必要があります。
   >
   > ```
   > # engine-iso-uploader --iso-domain=ISODomain upload RHEL6.iso
   > ```

ISO イメージがアップロードされ、指定した 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は、使用できる起動メディアの一覧にも表示されます。

8.7.2. 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たり、削除したりするには、メンテナンスモードに切り替え、別のデータドメインをマスターのデータドメインとして再度指定できるようにする必要があります。

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。

手順8.19 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** リソースタブをクリックして、ストレージドメインを選択します。

3. 詳細ペインの **データセンター** タブをクリックします。

4. **メンテナンス** をクリックすると、**ストレージドメインのメンテナンス** の確認ウィンドウが開きます。

5. **OK** をクリックすると、メンテナンスモードが開始します。ストレージドメインが非アクティブ化され、結果一覧のステータスが **Inactive** に変わります。

これで、非アクティブなストレージドメインの編集、データセンターからのデタッチ、削除、再アクティブ化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ペインにあるストレージタブを使用することもできます。

8.7.3. ストレージドメインの編集

管理ポータルを使用して、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。

- **Active**: 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** 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。

- **Inactive**: ストレージドメインがメンテナンスモードまたはアタッチされていない状態で、非アクティブの場合には、**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。

手順8.20 アクティブなストレージドメインの編集

1. **ストレージ** タブをクリックして、ストレージドメインを選択します。
2. **編集** をクリックします。
3. 必要に応じて、利用可能なフィールドを編集します。
4. **OK** をクリックします。

手順8.21 非アクティブなストレージドメインの編集

1. **ストレージ** タブをクリックして、ストレージドメインを選択します。
2. ストレージドメインがアクティブな場合には、詳細ペインで **データセンター** タブをクリックして、**メンテナンス** をクリックします。
3. **編集** 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. **データセンター** タブをクリックして、詳細ペインで **アクティブ化** をクリックします。

8.7.4. 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** リソースタブをクリックして、結果一覧から非アクティブなストレージドメインを選択します。

2. 詳細ペインの **データセンター** タブをクリックします。

3. 対象のストレージドメインを選択し、**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と、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。

8.7.5. 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。

手順8.22 ストレージドメインの削除

1. **ストレージ** リソースタブをクリックして、結果一覧から対象のストレージドメインを選択します。

2. ドメインをメンテナンスモードに切り替えて、非アクティブにします。

3. データセンターからドメインをデタッチします

4. **削除** をクリックすると、**プールの削除** の確認ウィンドウが開きます。

5. 一覧からホストを選択します。

6. **OK** をクリックするとストレージドメインが削除され、ウィンドウが閉じます。

ストレージドメインが環境から完全に削除されました。

8.7.6. ストレージドメインの破棄

エラーが発生したストレージドメインは、通常の手順で削除することができません。ストレージドメインを破棄することによって、そのストレージドメインは、エクスポートディレクトリーへの参照なしに、仮想化環境から強制的に削除されます。

ストレージドメインを破棄した場合に、そのストレージドメインのエクスポートディレクトリーを再度使用できるようにするには、手動で修正する必要があります。

手順8.23 ストレージドメインの破棄

1. **ストレージ** 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対象のストレージドメインを選択します。

2. ストレージドメインを右クリックして **破棄** を選択すると、**ストレージドメインの破棄** の確認ウィンドウが開きます。

3. **操作を承認** のチェックボックスを選択して **OK** をクリックすると、ストレージドメインが破棄されてウィンドウが閉じます。

ストレージドメインが破棄されました。エクスポートディレクトリーを手動で消去してストレージドメインがそのエクスポートディレクトリーをリサイクルできるようにしてください。

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

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、仮想マシンとテンプレートを別のデータセンターに移行します。

手順8.24 データセンターからのストレージドメインのデタッチ

1. **ストレージ** リソースタブをクリックして、結果一覧からストレージドメインを選択します。

2. 詳細ペインの **データセンター** タブをクリックして、ストレージドメインを選択します。

3. **メンテナンス** をクリックすると、**メンテナンスストレージドメイン** の確認ウィンドウが開きます。

4. **OK** をクリックしてメンテナンスモードを開始します。

5. **デタッチ** をクリックすると、**ストレージのデタッチ** の確認ウィンドウが開きます。

6. **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。

手順8.25 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** リソースタブをクリックして、結果一覧からストレージドメインを選択します。

2. 詳細ペインの **データセンター** タブをクリックします。

3. 次に **アタッチ** ボタンをクリックして、**データセンターへのアタッチ** のウィンドウを開きます。

4. 対象のデータセンターのラジオボタンを選択します。

5. **OK** をクリックしてストレージドメインをアタッチします。

ストレージドメイン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. ディスクプロファイル

ディスクプロファイルは、ストレージドメイン内の仮想ディスクのスループットの最大レベルと入出力操作の最大レベルを定義します。ディスクプロファイルは、データセンター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。

8.7.9.1. ディスクプロファイルの作成

ディスクプロファイルを作成します。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。

手順8.26 ディスクプロファイルの作成

1. **ストレージ** リソースタブをクリックして、データストレージドメインを選択します。
2. 詳細ペインで **ディスクプロファイル** サブタブをクリックします。
3. **新規作成** をクリックします。
4. **名前** フィールドにディスクプロファイルの名前を入力します。
5. **説明** フィールドにディスクプロファイルの説明を入力します。
6. **QoS** 一覧からディスクプロファイルに適用する QoS を選択します。
7. **OK** をクリックします。

ディスクプロファイルが作成されました。このディスクプロファイルは、そのデータストレージドメイン内でホストされる新規仮想ディスクに適用することができます。

8.7.9.2. ディスクプロファイルの削除

Red Hat Virtualization 環境から既存のディスクプロファイルを削除します。

手順8.27 ディスクプロファイルの削除

1. **ストレージ** リソースタブをクリックして、データストレージドメインを選択します。
2. 詳細ペインで **Disk Profiles** サブタブをクリックします。
3. 削除するディスクプロファイルを選択します。
4. **削除** をクリックします。
5. **OK** をクリックします。

ディスクプロファイルが削除されて使用できなくなりました。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。

8.7.10. 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、管理者が設定して、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
- **Info**: 

- **Warning**:
- **Error**:
- **Failure**:

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を選択してから **イベント** サブ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。

8.8. ストレージとパーミッション

8.8.1. ストレージドメインのシステムパーミッションの管理

システム管理者は、**SuperUser** として管理ポータルの全側面を管理する管理者です。他のユーザーには、より特定的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のみに対して (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のみに対して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のシステム管理者ロールです。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 1 人ずつ必要な場合に有用です。ヘッダーバーの **設定** ボタンを使用して、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ます。

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。

8.8.2. 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特権についての説明をまとめています。

表8.1 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。

8.8.3. 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。

手順8.28 リソースへのロール割り当て

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。
2. 詳細ペインの **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。

ユーザーにロールが割り当てられました。このユーザーは、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。

8.8.4. リソースからの管理者またはユーザーロールの削除

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。

手順8.29 リソースからのロール削除

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。
2. 詳細ペインの **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。パーミッションが削除されることを確認する **パーミッションの削除** ウィンドウが開きます。
5. **OK** をクリックします。

ユーザーロールおよび関連付けられたパーミッションが削除されました。

第9章 RED HAT GLUSTER STORAGE を使用した作業

9.1. RED HAT GLUSTER STORAGE ノード

9.1.1. Red Hat Gluster Storage ノードの追加

Gluster 対応クラスターに Red Hat Gluster Storage ノードを追加し、Red Hat Virtualization 環境に GlusterFS ボリュームとブリックを取り入れます。

以下の手順は、適切な **互換バージョン** の Gluster 対応クラスターが存在し、Red Hat Gluster Storage がすでに設定済みであることを前提としています。Red Hat Gluster Storage ノードの設定については、『Red Hat Gluster Storage Installation Guide』を参照してください。互換性マトリックスについては、『Red Hat Gluster Storage Version Compatibility and Support』を参照してください。

手順9.1 Red Hat Gluster Storage ノードの追加

1. **ホスト** リソースタブをクリックすると、結果一覧にホストが一覧表示されます。
2. **新規作成** をクリックすると、**新規ホスト** ウィンドウが表示されます。
3. ドロップダウンメニューを使用して、Red Hat Gluster Storage ノード用の **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. Red Hat Gluster Storage ノードの **名前**、**アドレス**、および **SSH ポート** を入力します。
5. Red Hat Gluster Storage ノードで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。
   - 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 Red Hat Gluster Storage ノードの **/root/.ssh/authorized_keys** にコピーします。
6. **OK** をクリックしてノードを追加し、ウィンドウを閉じます。

Red Hat Gluster Storage ノードが Red Hat Virtualization 環境に追加され、ボリュームとブリックのリソースを使用できるようになりました。

9.1.2. Red Hat Gluster Storage ノードの削除

Red Hat Gluster Storage ノードを Red Hat Virtualization 環境から削除します。

手順9.2 Red Hat Gluster Storage ノードの削除

1. **ホスト**リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象の Red Hat Gluster Storage ノードを選択します。
2. **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. **OK** をクリックして、ホストをメンテナンスモードに切り替えます。
4. **削除** をクリックすると、**ホストの削除** の確認ウィンドウが開きます。
5. ノードにボリュームブリックがある場合、またはノードが応答していない状態の場合には、**強制削除** のチェックボックスを選択します。

6. **OK** をクリックするとノードが削除され、ウィンドウが閉じます。

Red Hat Gluster Storage ノードが環境から削除され、**ホスト** タブに表示されなくなりました。

9.2. RED HAT GLUSTER STORAGE をストレージドメインとして使用する方法

9.2.1. Red Hat Gluster Storage (GlusterFS) ボリュームについて

Red Hat Gluster Storage ボリュームは、複数の Red Hat Gluster Storage サーバーのストレージを単一グローバル名前空間に統合します。ボリュームはブリックの集合で、各ブリックは、Trusted Storage Pool 内の Red Hat Gluster Storage Server 上のマウントポイントまたはディレクトリーです。

Red Hat Gluster Storage の管理操作の大半は、ボリュームに対して行われます。

管理ポータルを使用して、新規ボリュームの作成と起動を行うことができます。また、Red Hat Gluster Storage クラスター内のボリュームは、**ボリューム** タブでモニタリングすることができます。

ボリュームの作成と管理は、管理ポータルから行うことができますが、管理ポータルを使用してブリックを追加するには、個別の Red Hat Gluster Storage ノードであらかじめ作成しておく必要があります。

9.2.2. Gluster ストレージの用語

表9.1 データセンタープロパティー

用語	定義
ブリック	ブリックとは、GlusterFS ストレージの基本単位のことで、Trusted Storage Pool のサーバー上にあるエクスポートディレクトリーで表わされます。ブリックは、サーバーとエクスポートディレクトリーを合わせて以下のような形式で表現されます。 **`SERVER:EXPORT`** 例: **`myhostname:/exports/myexportdir/`**
ブロックストレージ	システムがブロック形式でデータを移動する際に使うブロックスペシャルファイルまたはブロックデバイス。これらのデバイスノードは、ハードディスク、CD-ROM ドライブ、メモリー領域などのアドレス可能なデバイスを表します。Red Hat Gluster Storage は、拡張属性で XFS ファイルシステムに対応しています。

用語	定義
クラスター	リンクされたコンピューターの信頼されたプール。これらのコンピューターは密に連携するため、多くの点で 1 つのコンピューターを形成しているようになります。Red Hat Gluster Storage の用語では、クラスターは Trusted Storage Pool と呼ばれています。
クライアント	ボリュームをマウントするマシン (サーバーの場合もあり)
分散ファイルシステム	Trusted Storage Pool 内の複数のサーバー/ブリック全体に散在するデータへ複数のクライアントが同時にアクセスすることができるファイルシステム。複数ロケーション間のデータ共有は、すべての分散ファイルシステムに必須です。
ジオレプリケーション	ジオレプリケーションは、ローカルエリアネットワーク (LAN)、ワイドエリアネットワーク (WAN)、インターネット経由でサイト間の継続、非同期、ならびに増分レプリケーションサービスを提供します。
glusterd	Trusted Storage Pool 内の全サーバー上で実行する必要のある Gluster 管理デーモン
メタデータ	メタデータとは、1 つまたは複数の他のデータに関する情報を提供するデータです。
N-way レプリケーション	通常キャンパスまたは Amazon Web Services Availability Zones 全体にデプロイされる同期データのローカルレプリケーション
名前空間	名前空間とは、一意識別子やシンボルの論理グループを格納するために作成される抽象的なコンテナーまたは環境のことです。Red Hat Gluster Storage の Trusted Storage Pool はそれぞれ、その Trusted Storage Pool 内の全ファイルを格納する POSIX マウントポイントとして、単一の名前空間を公開します。
POSIX	Portable Operating System Interface (Unix 用) とは、IEEE が規定する関連規格群の総称です。UNIX オペレーティングシステムのさまざまなバージョンと互換性のあるソフトウェアのシェルやユーティリティーのインターフェースとともに、アプリケーションプログラミングインターフェース (API) を定義します。Red Hat Gluster Storage は、POSIX と完全に互換性のあるファイルシステムをエクスポートします。

用語	定義
RAID	Redundant Array of Inexpensive Disks (RAID) とは、複数の低コスト、かつ信頼性が低いディスクドライブコンポーネントを論理ユニットに組み合わせ冗長化することでストレージの信頼性を高める技術です。この論理ユニットにあるアレイ内のドライブはそれぞれ独立しています。
RRDNS	Round Robin Domain Name Service (RRDNS) とは、アプリケーションサーバー全体で負荷を分散する方法です。RRDNS は、DNS サーバーのゾーンファイルに、同名で別の IP アドレスを持つ A レコードを複数作成することで実装します。
サーバー	データを格納する実際のファイルシステムをホストするマシン (仮想またはベアメタル)
スケールアップ型ストレージ	ストレージデバイスの容量を 1 つのディメンションのみで増やします。一例を挙げると、Trusted Storage Pool 内にあるコンピューターを 1 台に追加のディスク容量を増やすなどです。
スケールアウト型ストレージ	ストレージデバイスの容量を複数のディメンションで増やします。一例を挙げると、Trusted Storage Pool にサーバーを追加して、CPU、ディスク容量、Trusted Storage Pool の処理量を増やすなどです。
サブボリューム	サブボリュームとは、最低でも 1 つのトランスレーターが処理を行ったブリックです。
トランスレーター	トランスレーターは、1 つまたは複数のサブボリュームに接続して処理を行い、サブボリューム接続を提供します。
Trusted Storage Pool	ストレージプールとは、ストレージサーバーの信頼されたネットワークです。最初のサーバーを起動すると、ストレージプールはそのサーバーだけで構成されます。
ユーザースペース	ユーザースペースで実行中のアプリケーションは、ハードウェアと直接やりとりを行わず、カーネルを使用して、アクセスを管理します。一般的にユーザースペースのアプリケーションは、カーネルスペースのアプリケーションより移植性が高くなっています。Gluster はユーザースペースアプリケーションです。
仮想ファイルシステム (VFS)	VFS とは、標準の Linux ファイルシステムに関連したシステムコールをすべて処理するカーネルソフトウェア層で、数種類のファイルシステムに接続するための共通のインターフェースを提供します。

用語	定義
ボリュームファイル	ボリュームファイルとは、GlusterFS プロセスが使用する設定ファイルです。ボリュームファイルは、通常 **/var/lib/glusterd/vols/VOLNAME** にあります。
ボリューム	ボリュームとは、ブリックの論理的な集合です。Gluster 管理操作の多くがボリューム上で行われます。

9.2.3. Red Hat Gluster Storage ボリュームをストレージドメインとしてアタッチする方法

ストレージドメインとして直接使用するための Red Hat Gluster Storage ボリュームを Red Hat Virtualization Manager に追加します。これは、Red Hat Virtualization Manager からボリュームとブリックに対する制御を可能にする Red Hat Storage Gluster ノードを追加する方法とは異なり、Gluster 対応のクラスターは必要ありません。

ボリュームをマウントするには、ホストに glusterfs、glusterfs-fuse、および glusterfs-cli のパッケージをインストールする必要があります。glusterfs-cli パッケージはカスタマーポータルの **rh-common-rpms** チャンネルから提供されています。

Red Hat Gluster Storage ノードの設定については、『Red Hat Gluster Storage Installation Guide』を参照してください。Red Hat Storage Gluster ボリュームとして使用するホストの準備についての説明は、『Configuring Red Hat Virtualization with Red Hat Gluster Storage Guide』を参照してください。また互換性のマトリックスについては、『Configuring Red Hat Virtualization with Red Hat Storage Guide』を参照してください。

手順9.3 Red Hat Gluster Storage ボリュームをストレージドメインとして追加する方法

1. **ストレージ** リソースタブをクリックすると、結果一覧に既存のストレージドメインが表示されます。

2. **新規ドメイン** をクリックし、**新規ドメイン** ウィンドウを開きます。

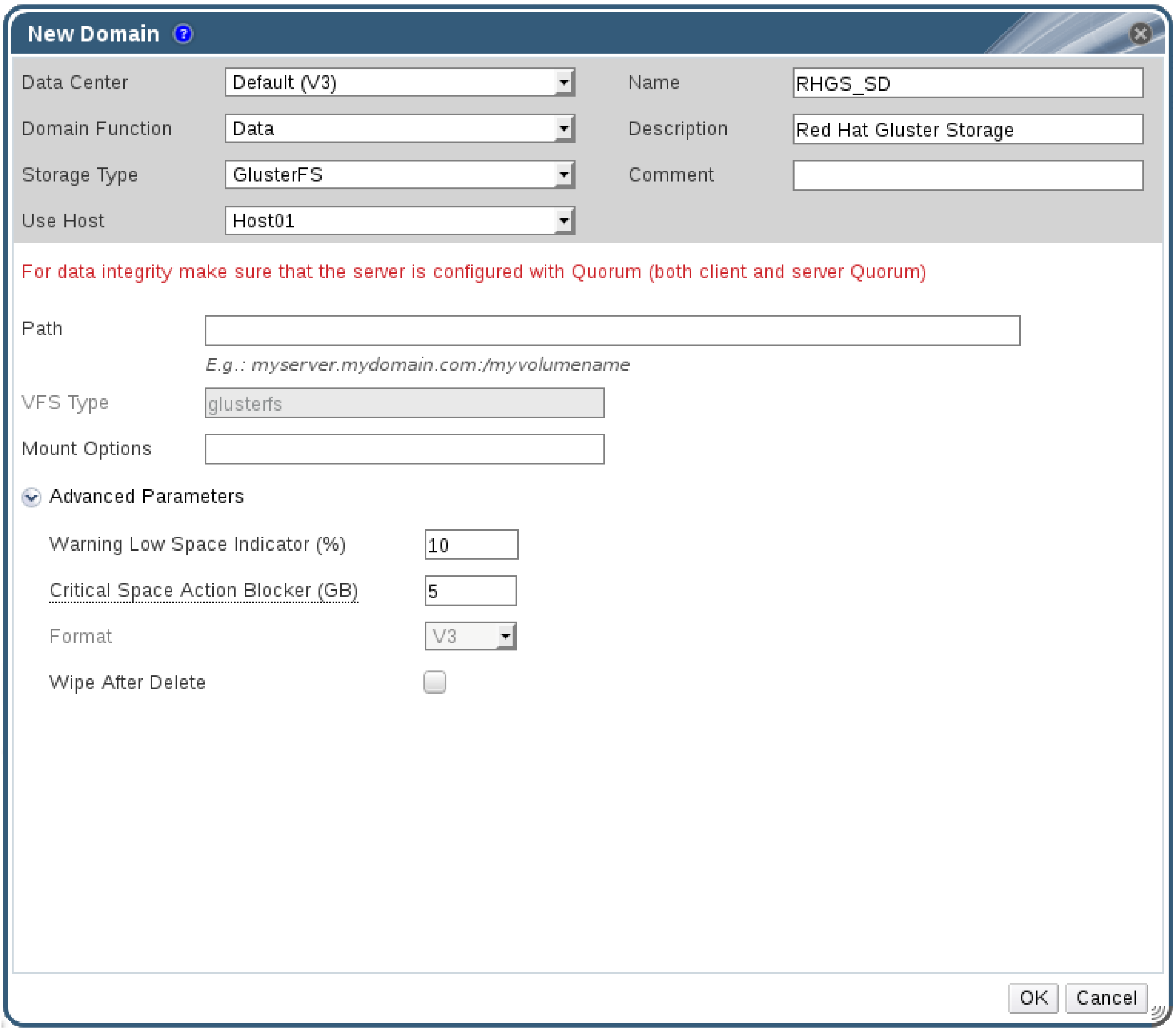


図9.1 Red Hat Gluster Storage

3. ストレージドメインの **名前** を入力します。

4. ストレージドメインに関連付ける **データセンター** を選択します。

5. **ドメインの機能** のドロップダウンリストから **`Data`** を選択します。

6. **ストレージタイプ** のドロップダウンリストから **`GlusterFS`** を選択します。

7. **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。ボリュームをマウントするには、選択したホストに glusterfs と glusterfs-fuse のパッケージをインストールする必要があります。

8. **パス** のフィールドで、Red Hat Gluster Storage サーバーの IP アドレスまたは完全修飾ドメイン名とボリューム名をコロンで区切って入力します。

9. 通常、***`-o`*** 引数を使用して **`mount`** コマンドに渡すときのように、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リストで指定してください。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たディスクの「削除後にワイプ」プロパティーは変更されません。

11. **OK** をクリックするとボリュームがストレージドメインとしてマウントされ、ウィンドウが閉じます。

9.2.4. ストレージボリュームの作成

管理ポータルを使用して、新しいボリュームを作成することができます。新規ボリュームを作成する際には、ボリュームを構成するブリックを指定して、そのボリュームが分散/複製/ストライプ化されるかを設定する必要があります。

ブリックをボリュームに追加する前には、ブリックのディレクトリーまたはマウントポイントを作成しておく必要があります。

重要

ブリックが異なるホストからエクスポートされて統合される、複製ボリュームを使用することをお勧めします。複製ボリュームは、ボリューム内の複数のブリックにまたがるファイルのコピーを作成し、ホストがフェンスされた場合のデータ損失を防ぎます。

手順9.4 ストレージボリュームの作成

1. **ボリューム** リソースタブをクリックすると、結果一覧に既存のボリュームがリストされます。

2. **新規作成** をクリックして、**新規ボリューム** ウィンドウを開きます。

3. ドロップダウンメニューで **データセンター** と **ボリュームクラスター** を選択します。

4. ボリュームの **名前** を入力します。

5. ドロップダウンメニューを使用して、ボリュームの **タイプ** を選択します。

6. アクティブな場合には、適切な **トランスポートタイプ** のチェックボックスを選択します。

7. **ブリックの追加** ボタンをクリックして、ボリュームに追加するブリックを選択します。ブリックは、外部の Red Hat Gluster Storage ノードで作成する必要があります。

8. アクティブな場合には、**Gluster**、**NFS**、および **CIFS** のチェックボックスを使用して、そのボリュームに使用する適切なアクセスプロトコルを選択します。

9. **アクセスを許可するホスト** のフィールドには、ボリュームのアクセス制御を IP アドレスまたはホスト名のコンマ区切りリストで入力します。

   アスタリスク (*) をワイルドカードとして使用して、IP アドレスまたはホスト名を範囲で指定することができます。

10. 仮想マシンストレージ用にボリュームを最適化するパラメーターを指定するには、**仮想ストア用に最適化** オプションを選択しします。ボリュームをストレージドメインとして使用する場合には、このオプションを選択してください。

11. **OK** をクリックしてボリュームを作成します。新規ボリュームが追加され、**ボリューム** タブに表示されます。

Red Hat Gluster Storage ボリュームを追加し、ストレージとして使用することができるようになりました。

9.2.5. ボリュームへのブリックの追加

概要

新しいブリックを追加することにより、ボリュームを拡張することができます。ストレージ容量を拡張する場合は、分散ボリュームには少なくともブリックを 1 つ、レプリケーションボリュームには 2 の倍数のブリック、ストライプボリュームには 4 の倍数のブリックを追加する必要があります。

手順9.5 ボリュームへのブリックの追加

1. ナビゲーションペインの **ボリューム** タブで、ブリックを追加するボリュームを選択します。
2. 詳細ペインの **ブリック** タブをクリックします。
3. **ブリックの追加** をクリックすると、**ブリックの追加** ウィンドウが開きます。
4. **サーバー** のドロップダウンメニューで、ブリックの追加先となるサーバーを選択します。
5. **ブリックディレクトリー** のパスを入力します。このディレクトリーがすでに存在している必要があります。
6. **追加** をクリックします。ボリュームのブリック一覧にそのブリックがサーバーアドレスとブリックディレクトリー名とともに表示されます。
7. **OK** をクリックします。

結果

新しいブリックがボリュームに追加され、そのブリックがボリュームの **ブリック** タブに表示されます。

9.2.6. ブリックの追加ウィンドウの設定

表9.2 ブリックの追加タブのプロパティー

フィールド名	説明
ボリュームのタイプ	ボリュームの種類を表示します。このフィールドはボリュームの作成時に設定済みで変更はできません。
サーバー	ブリックがホストされるサーバー
ブリックディレクトリー	ブリックのディレクトリーまたはマウントポイント

9.2.7. 仮想マシンイメージを保管するための Red Hat Gluster Storage ボリュームの最適化

管理ポータルを使用して、仮想マシンイメージを保管する Red Hat Gluster Storage ボリュームを最適化します。

仮想マシンを保管するボリュームを最適化するために、Manager はそのボリュームに複数の仮想化固有パラメーターを設定します。

仮想マシンを保管するためのボリュームは、作成時に **仮想ストア用に最適化** のチェックボックスを選択するか、**ボリューム** リソースタブの **仮想ストア用に最適化** ボタンを使用して、最適化することができます。

重要

3 つ以上のノードにまたがってボリュームが複製される場合には、そのボリュームが仮想ストレージ用に最適化されていることを確認して、ノード間におけるデータの不整合を回避します。

もう 1 つの方法として、Red Hat Gluster Storage ノードの 1 つにアクセスしてボリュームグループを **virt** に設定することができます。この方法では **cluster.quorum-type** パラメーターは **auto** に、**cluster.server-quorum-type** パラメーターは **server** に設定されます。

```
# gluster volume set VOLUME_NAME group virt
```

ボリュームの情報を一覧表示してボリュームのステータスを確認します。

```
# gluster volume info VOLUME_NAME
```

9.2.8. ボリュームの起動

概要

ボリュームを作成した後や既存ボリュームを停止した後には、そのボリュームを起動して使用できるようにする必要があります。

手順9.6 ボリュームの起動

1. **ボリューム** タブで起動するボリュームを選択します。

   Shift キーまたは **Ctrl** キーを使用すると、起動するボリュームを複数選択することができます。

2. **起動** ボタンをクリックします。

ボリュームのステータスが **Up** に変わります。

結果

仮想マシンのストレージにボリュームを使用できるようになりました。

9.2.9. ボリュームのチューニング

概要

ボリュームをチューニングすることにより、パフォーマンスを調整することができます。ボリュームのチューニングを行うには、オプションを追加します。

手順9.7 ボリュームのチューニング

1. **ボリューム** タブをクリックします。

   ボリュームの一覧が表示されます。

2. チューニングをするボリュームを選択し、詳細ペインから **ボリュームオプション** タブを選択します。

   ボリュームオプション タブに、そのボリューム用のオプションセットの一覧が表示されます。

3. **追加** をクリックしてオプションを設定します。**オプションの追加** ウィンドウが表示されます。ドロップダウンメニューからオプションキーを選択し、オプション値を入力します。

4. **OK** をクリックします。

   オプションが設定され、**ボリュームオプション** タブに表示されます。

結果

ストレージボリュームのオプションが調整されました。

9.2.10. ボリュームオプションの編集

概要

オプションを追加してボリュームのチューニングを行いました。このストレージボリュームのオプションは、変更することが可能です。

手順9.8 ボリュームオプションの編集

1. **ボリューム** タブをクリックします。

   ボリュームの一覧が表示されます。

2. 編集するボリュームを選択し、詳細ペインの **ボリュームオプション** タブをクリックします。

   ボリュームオプション タブに、そのボリューム用のオプションセットの一覧が表示されます。

3. 編集するオプションを選択し、**編集** をクリックします。**オプションの編集** ウィンドウが表示されます。新たなオプション値を入力してください。

4. **OK** をクリックします。

   編集したオプションが **ボリュームオプション** タブに表示されます。

結果

ボリュームのオプションの変更が完了しました。

9.2.11. ボリュームオプションのリセット

概要

オプションをリセットしてデフォルト値に戻すことができます。

1. **ボリューム** タブをクリックします。

   ボリュームの一覧が表示されます。

2. ボリュームを選択し、詳細ペインから **ボリュームオプション** タブを選択します。

   ボリュームオプション タブに、そのボリューム用のオプションセットの一覧が表示されます。

3. リセットするオプションを選択して **リセット** をクリックします。オプションのリセットを確認するウィンドウが表示されます。

4. **OK** をクリックします。

   選択したオプションがリセットされます。

注記

すべてのボリュームオプションをリセットするには **すべてをリセット** ボタンをクリックします。オプションのリセットを確認するウィンドウが表示されます。**OK** をクリックします。選択したボリュームの全オプションがリセットされます。

結果

ボリュームのオプションがデフォルトの状態にリセットされました。

9.2.12. ボリュームからのブリックの削除

概要

クラスターがオンラインで使用可能な状態の時に、必要に応じてボリュームを縮小することができます。たとえば、ハードウェアやネットワークの障害が原因でアクセス不可能となったブリックを削除する必要がある場合などです。

手順9.9 ボリュームからのブリックの削除

1. ナビゲーションペインの **ボリューム** タブで、ブリックを削除するボリュームを選択します。

2. 詳細ペインの **ブリック** タブをクリックします。

3. 削除するブリックを選択して、**ブリックを削除** をクリックします。

4. 削除の確認を求めるウィンドウが開きます。**OK** をクリックして確定します。

結果

ボリュームからブリックが削除されました。

9.2.13. Red Hat Gluster Storage ボリュームの停止

ボリュームを起動した後には、そのボリュームを停止することができます。

手順9.10 ボリュームの停止

1. **ボリューム** タブで、停止するボリュームを選択します。

Shift キーまたは **Ctrl** キーを使用すると、停止するボリュームを複数選択することができます。

2. **停止** をクリックします。

9.2.14. Red Hat Gluster Storage ボリュームの削除

クラスターから単一または複数のボリュームを削除することができます。

1. **ボリューム** タブで削除するボリュームを選択します。

2. **削除** をクリックします。ウィンドウが開き、削除の実行を確認するように要求されます。**OK** をクリックします。

9.2.15. ボリュームのリバランス

概要

ブリックを追加または削除することによってボリュームが拡張または縮小された場合には、そのボリューム上のデータをサーバー間でリバランスする必要があります。

手順9.11 ボリュームのリバランス

1. **ボリューム** タブをクリックします。

   ボリュームの一覧が表示されます。

2. リバランスするボリュームを選択します。

3. **リバランス** をクリックします。

結果

選択したボリュームがリバランスされます。

9.3. クラスターと GLUSTER フック

9.3.1. Gluster フックの管理

Gluster フックは、ボリュームライフサイクルの拡張機能です。Gluster フックは Manager から管理することができます。フックのコンテンツタイプが **Text** の場合はフックのコンテンツを表示することができます。

Manager からは以下の操作を行うことができます。

- ホストで使用可能なフックの一覧表示
- フックのコンテンツとステータスの表示
- フックの有効化/無効化
- フックの競合の解決

9.3.2. フックの一覧表示

概要

環境内の Gluster フックを一覧表示します。

手順9.12 フックの一覧表示

1. **クラスター** 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対象のクラスターを選択します。
2. **`Gluster フック`** サブタブを選択して、詳細ペインにフックを一覧表示します。

結果

お使いの環境内の Gluster フックが一覧表示されました。

9.3.3. フックのコンテンツの表示

概要

お使いの環境の Gluster フックのコンテンツを表示します。

手順9.13 フックのコンテンツの表示

1. **クラスター** 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対象のクラスターを選択します。
2. **`Gluster フック`** サブタブを選択して、詳細ペインにフックを一覧表示します。
3. コンテンツタイプが **テキスト** のフックを 1 つ選択して **コンテンツを表示** のボタンをクリックすると、**フックのコンテンツ** ウィンドウが開きます。

結果

お使いの環境内にあるフックのコンテンツが表示されました。

9.3.4. フックの有効化/無効化

概要

Gluster フックを有効化または無効化して、動作を切り替えます。

手順9.14 フックの有効化/無効化

1. **クラスター** 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対象のクラスターを選択します。
2. **`Gluster フック`** サブタブを選択して、詳細ペインにフックを一覧表示します。
3. フックを 1 つ選択して **有効化** または **無効化** のボタンをクリックします。クラスター内の全ノードでフックが有効化または無効化されます。

結果

お使いの環境内にある Gluster フックの動作を切り替えました。

9.3.5. フックのリフレッシュ

概要

デフォルトでは、Manager は、1 時間ごとに定期処理ジョブを実行して、クラスター内の全サーバーにインストールされているフックのステータスをチェックし、新規フックを検出します。**同期** ボタンをクリックすると、手動でフックをリフレッシュすることができます。

手順9.15 フックのリフレッシュ

1. **クラスター** 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対象のクラスターを選択します。

2. **`Gluster フック`** サブタブを選択して、詳細ペインにフックを一覧表示します。

3. **同期** ボタンをクリックします。

結果

フックが同期され、詳細ペインで更新されます。

9.3.6. 競合の解決

フックは、**クラスター** タブの **`Gluster フック`**サブタブに表示されます。競合の原因となっているフックには感嘆符が表示されます。これは、クラスター内のサーバー間において、フックのコンテンツまたはステータスで競合が発生しているか、フックのスクリプトが見つからないことを意味します。このような競合は、Manager で解決することができます。サーバー内のフックは、engine データベースと定期的に同期され、フックでは次のような競合が発生する場合があります。

- コンテンツの競合: フックのコンテンツがサーバー間で異なる
- 不明のフックの競合: クラスター内の 1 台または複数サーバーで、フックが存在しない
- ステータスの競合: フックのステータスがサーバー間で異なる
- 複数の競合: 1 つのフックで上記の競合が複数発生する

9.3.7. コンテンツの競合解決

概要

全サーバーと engine 上で一致していないフックには、競合のフラグが付けられます。この競合を解決するには、全サーバーと engine にコピーするフックのバージョンを選択する必要があります。

手順9.16 コンテンツの競合解決

1. **クラスター** 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対象のクラスターを選択します。

2. **`Gluster フック`** サブタブを選択して、詳細ペインにフックを一覧表示します。

3. 競合しているフックを選択して **競合を解決** ボタンをクリックすると、**競合の解決** ウィンドウが開きます。

4. フックのコンテンツを表示するソースの一覧から engine またはサーバーを選択して、フックのバージョンを確定します。

注記

すべてのサーバーと engine でフックのコンテンツが上書きされます。

5. **使用するコンテンツのソース** ドロップダウンメニューで対象のサーバーまたは engine を選択します。

6. **OK** をクリックすると競合が解決し、ウィンドウが閉じます。

結果

選択したサーバーのフックが全サーバーと engine にコピーされ、環境全体で一貫性が保たれます。

9.3.8. 不明のフックの競合解決

概要

全サーバーと engine 上で存在していないフックは、競合が発生しているとフラグされます。この競合を解決するには、全サーバーにわたってコピーするフックのバージョンを選択するか、不明のフックを全面的に削除します。

手順9.17 不明のフックの競合解決

1. **クラスター** 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対象のクラスターを選択します。

2. **Gluster フック** サブタブを選択して、詳細ペインにフックを一覧表示します。

3. 競合しているフックを選択して **競合を解決** ボタンをクリックすると、**競合の解決** ウィンドウが開きます。

4. フックのコンテンツを表示するには、ステータスが **有効** となっている任意のソースを選択します。

5. 適切なラジオボタン (**全サーバーにフックをコピー** または **見つからないフックを削除**) を選択します。後者を選択すると、そのフックは engine と全サーバーから削除されます。

6. **OK** をクリックすると競合が解決し、ウィンドウが閉じます。

結果

選択した解決方法に応じて、フックが環境から全面的に削除されるか、全サーバーと engine にコピーされて環境全体で一貫性が保たれます。

9.3.9. ステータスの競合の解決

概要

サーバーと engine 全体でステータスが一致していないフックには、競合のフラグが付けられます。この競合を解決するには、環境内の全サーバーに適用するステータスを選択します。

手順9.18 ステータスの競合解決

1. **クラスター** 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対象のクラスターを選択します。

2. **Gluster フック** サブタブを選択して、詳細ペインにフックを一覧表示します。

3. 競合しているフックを選択して **競合を解決** ボタンをクリックすると、**競合の解決** ウィンドウが開きます。

4. フックの **ステータス** を **有効** または **無効** に設定します。

5. **OK** をクリックすると競合が解決し、ウィンドウが閉じます。

結果

選択したフックのステータスが engine および全サーバーに適用され、環境全体で一貫性が保たれます。

9.3.10. 複数の競合の解決

概要

1 つのフックで複数の競合が併せて発生する場合があります。このような競合は、**競合の解決** ウィンドウですべてを同時に解決するか、個別に解決することができます。以下の手順では、環境内の engine と全サーバーでフックの一貫性が保たれるように、全競合を解決します。

手順9.19 複数の競合の解決

1. **クラスター** 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対象のクラスターを選択します。

2. **Gluster フック** サブタブを選択して、詳細ペインにフックを一覧表示します。

3. 競合しているフックを選択して **競合を解決** ボタンをクリックすると、**競合の解決** ウィンドウが開きます。

4. 影響を及ぼしている各競合に対して、解決方法を選択します。

5. **OK** をクリックすると競合が解決し、ウィンドウが閉じます。

結果

すべての競合が解決し、engine と全サーバーにわたってフックの一貫性が維持されました。

9.3.11. Gluster 同期の管理

Gluster 同期機能は、GlusterFS から最新のクラスター設定を定期的に取得して、engine DB と同期します。このプロセスは、Manager から実行することができます。クラスターを選択すると、ホストをインポートしたり既存のホストをデタッチしたりするオプションが表示されます。クラスター内にホストが存在する場合に Gluster 同期を実行することが可能です。

注記

Manager は、ストレージクラスターへのホストの追加と削除を継続的に監視します。ホストの追加または削除が検知されると、そのクラスターの **全般** タブにアクション項目が表示されます。ここでそのホストを **インポート** するか、クラスターから **デタッチ** するかを選択することができます。

第10章 プール

10.1. 仮想マシンプールについて

仮想マシンプールは、同じテンプレートからすべて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。

仮想マシンプール内の仮想マシンはステートレスであるため、再起動後にはデータは維持されませんが、仮想マシンプールから取得した仮想マシンのコンソールオプションを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。

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。

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。

10.2. 仮想マシンプールのタスク

10.2.1. 仮想マシンプールの作成

共通のテンプレートを 1 つ使用して、複数の仮想マシンが入った仮想マシンプールを作成することができます。

手順10.1 仮想マシンプールの作成

1. **プール** タブをクリックします。
2. **新規作成** ボタンをクリックし、**新規プール** ウィンドウを開きます。
3. ドロップダウンリストで **クラスター** を選択するか、選択されているデフォルトを使用します。
4. **テンプレート** のドロップダウンメニューを使用して必要なテンプレートとバージョンを選択するか、デフォルトで選択されている値を使用します。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. **オペレーティングシステム** のドロップダウンリストを使用して **オペレーティングシステム** を選択するか、テンプレートによって提供されるデフォルト値を使用します。

6. **最適化オプション** のドロップダウンリストで仮想マシンを **デスクトップ** 用または **サーバー** 用に最適化するかを選択します。

7. プールの **名前**、**説明**、**コメント**、およびプール内の **仮想マシン数** を入力します。

8. **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。

9. **1 ユーザーあたりの最大仮想マシン数** 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。最小で 1 にする必要があります。

10. **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。

11. オプションとして、**詳細オプションを表示** ボタンをクリックして、以下の設定を行うことができます。

    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。仮想マシンは、プールに返却されると、オリジナルのベースイメージに戻ります。

       - **自動**: 仮想マシンはシャットダウン時に自動的にベースイメージに戻り、仮想マシンプールに返却されます。

    b. **コンソール** タブを選択します。このタブのウィンドウ最下部で **SPICE プロキシーアドレスを上書き** のチェックボックスを選択して **SPICE プロキシーアドレスを上書き** のテキストフィールドが有効化します。グローバルの SPICE プロキシーを上書きする SPICE プロキシーのアドレスを指定します。

12. **OK** をクリックします。

指定した数の同一の仮想マシン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、**仮想マシン** のリソースタブまたは **プール** の詳細ペイン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。

10.2.2. 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

10.2.2.1. 新規プールおよびプールの編集の全般設定

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10.1 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るテンプレート
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

フィールド名	説明
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。
1 ユーザーあたりの最大仮想マシン数	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。

10.2.2.2. 新規プールおよびプールの編集のタイプ設定

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** タブに必要な詳しい情報をまとめています。

表10.2 タイプ の設定

フィールド名	説明
プールタイプ	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。 • **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、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。

10.2.2.3. 新規プールおよびプールの編集のコンソール設定

以下の表には、**新規プール** ウィンドウまたは **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** ウィンドウおよび **仮想マシンの編集** ウィンドウと全く同じです。

表10.3 コンソール の設定

フィールド名	説明
SPICE プロキシーを上書き	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、ホストが所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: ユーザーポータルから接続) に有用です。
SPICE プロキシーアドレスを上書き	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ー。このプロキシーは、Red Hat Virtualization 環境で定義されているグローバル SPICE プロキシーと、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 プロキシー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。 `protocol://[host]:[port]`

10.2.2.4. 仮想マシンプールのホスト設定

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** タブで利用可能なオプションについて詳しい情報をまとめています。

表10.4 仮想マシンプール: ホスト設定

フィールド名	サブ要素	説明

フィールド名	サブ要素	説明
実行を開始するホスト		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。 • **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ホストで起動、実行できます。 • **特定**: 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**	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。 • **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
	カスタムマイグレーションポリシーを使用	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。 • **`Legacy`**: バージョン 3.6 のレガシーの動作。**`vdsm.conf`** の設定内容がそのまま優先されて適用されます。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。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。 • **`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。
	カスタム移行ダウンタイムを使用	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。

フィールド名	サブ要素	説明
	移行の自動収束	マイグレーションポリシーが **Legacy** の場合にのみ有効です。このオプションは、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率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させることができます。QEMU は収束されていないことを自動検出し、仮想マシンで vCPU のスロットルを減らします。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。 • **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	マイグレーションポリシーが **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。 • **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	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、または **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。
NUMA の設定	**NUMA ノード数**	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。

フィールド名	サブ要素	説明
	チューニングモード	メモリーの割り当てに使用する方法 • **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**: 単一の優先メモリーノードからのみメモリーの割り当てが行なわれます。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	**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 をクリックして、左側にドラッグして、仮想 NUMA ノードをホストの NUMA ノードに固定します。

10.2.3. 仮想マシンプールの編集

10.2.3.1. 仮想マシンプールの編集

仮想マシンプールの作成後にそのプロパティー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ーは、**仮想マシン数** プロパティーが **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、新規仮想マシンの作成時に指定できるプロパティーと全く同じです。

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。

手順10.2 仮想マシンプールの編集

1. **プール** リソースタブをクリックして、結果一覧から仮想マシンプールを選択します。

2. **編集** をクリックすると、**プールの編集** ウィンドウが開きます。

3. 仮想マシンプールのプロパティーを編集します。

4. **OK** をクリックします。

10.2.3.2. プール内の仮想マシンの事前起動

仮想マシンプール内では、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。

手順10.3 プール内の仮想マシンの事前起動

1. **プール** 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対象の仮想マシンプールを選択します。

2. **編集** をクリックすると、**プールの編集** ウィンドウが開きます。

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. **プール** タブを選択して、**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。

プール内の事前起動済み仮想マシンの数を設定しました。事前起動済みのマシンは稼働中で使用できる状態です。

10.2.3.3. 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。

手順10.4 仮想マシンプールへの仮想マシン追加

1. **プール** 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対象の仮想マシンプールを選択します。

2. **編集** をクリックすると、**プールの編集** ウィンドウが開きます。

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。

仮想マシンプールに仮想マシンが追加されました。

10.2.3.4. 仮想マシンプールからの仮想マシンのデタッチ

仮想マシン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。

手順10.5 仮想マシンプールからの仮想マシンのデタッチ

1. **プール** 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対象の仮想マシンプールを選択します。

2. 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。

   詳細ペインの **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。

3. 仮想マシンを 1 つまたは複数選択して、**デタッチ** をクリックすると **仮想マシンのデタッチ** の確認ウィンドウが開きます。

4. **OK** をクリックすると、仮想マシンがプールからデタッチされます。

注記

仮想マシンはまだ環境に存在しており、**仮想マシン** リソースタブ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。

仮想マシンプールから仮想マシンがデタッチされました。

10.2.4. 仮想マシンプールの削除

データセンターから仮想マシンプールを削除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。

手順10.6 仮想マシンプールの削除

1. **プール** 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対象の仮想マシンプールを選択します。

2. **削除** をクリックすると、**プールの削除** の確認ウィンドウが開きます。

3. **OK** をクリックしてプールを削除します。

データセンターからプールが削除されました。

10.3. プールとパーミッション

10.3.1. 仮想マシンプールのシステムパーミッションの管理

システム管理者は、**SuperUser** として管理ポータルの全側面を管理する管理者です。他のユーザーには、より特定的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のみに対して (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のみに対して管理者権限があります。

仮想マシンプールの管理者は、データセンター内の仮想マシンプールの管理ロールです。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を管理する場合に有用です。

仮想マシンプールの管理者ロールは、以下のアクションを許可します。

- プールの作成/編集/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。

10.3.2. 仮想マシンプール管理者ロール

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10.5 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。

10.3.3. 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。

手順10.7 リソースへのロール割り当て

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。
2. 詳細ペインの **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。

ユーザーにロールが割り当てられました。このユーザーは、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。

10.3.4. リソースからの管理者またはユーザーロールの削除

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。

手順10.8 リソースからのロール削除

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。

2. 詳細ペインの **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。パーミッションが削除されることを確認する **パーミッションの削除** ウィンドウが開きます。

5. **OK** をクリックします。

ユーザーロールおよび関連付けられたパーミッションが削除されました。

10.4. 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、セキュリティー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、https://software.intel.com/en-us/articles/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。OpenAttestatoin 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。

10.4.1. 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10.6 engine-config の OpenAttestation 設定

オプション	デフォルト値	説明
AttestationServer	oat-server	OpenAttestation サーバーの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
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信頼ストア
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

10.4.2. 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が可能となります。

手順10.9 信頼済みクラスターの作成

1. **クラスター** タブを選択します。
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** のラジオボタンを選択します。
5. **スケジューリングポリシー** タブで **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。

10.4.3. 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。

手順10.10 信頼済みホストの作成

1. **ホスト** タブを選択します。
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 **アドレス** 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11章 仮想マシンのディスク

11.1. 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、仮想マシン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マシンディスクは、デフォルトで事前割り当てされます。

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。仮想マシンが 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。

11.2. 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。

ディスクのサイズは、各仮想マシンおよびテンプレートの **ディスク** サブタブに表示されます。ディスクの **仮想サイズ** は、仮想マシンが使用可能なディスク容量の合計です。これは、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、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には、両方のフィールドに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、**仮想サイズ** に表示されるのとは異なる値が **実サイズ** フィールドに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11.1 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	注意
NFS または iSCSI/FCP	**RAW または QCOW2**	**スパースまたは事前割り当て済み**	
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	注意
NFS または iSCSI/FCP	**RAW または QCOW2**	**スパースまたは事前割り当て済み**	
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)。

11.3. 削除後に仮想ディスクをワイプする設定

管理ポータルでは **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。

仮想ディスクの **`wipe_after_delete`** を有効にするのは、よりセキュアなオプションなので、仮想ディスクに機密データが含まれている場合に推奨されます。この操作は、負荷が高いため、パフォーマンスが低下したり、削除に長時間かか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。設定を有効にするには、engine を再起動してください。

手順11.1 engine 設定ツールを使用して SANWipeAfterDelete を Default から True に設定する方法

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。

```
# service ovirt-engine restart
```

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**」というエントリーが追加されます。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***」というエントリーが追加されます。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。

11.4. 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用することが可能となります。

共有ディスクは、すべての状況で使用でき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。

11.5. 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/編集中に、仮想マシンの詳細ペインの **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マシンディスクに **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。

11.6. 仮想ディスクのタスク

11.6.1. フローティング仮想ディスクの作成

どの仮想マシンにも属さない仮想ディスクを作成して、単一の仮想マシンにアタッチすることができます。また、ディスクが共有可能の場合には、複数の仮想マシンにアタッチすることが可能です。

イメージ ディスクの作成は、Manager によって完全に管理されます。**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、「ストレージ管理のための OpenStack Volume (Cinder) インスタンスの追加」を参照してください。

手順11.2 フローティング仮想ディスクの作成

1. **ディスク** リソースタブを選択します。
2. **新規作成** をクリックします。

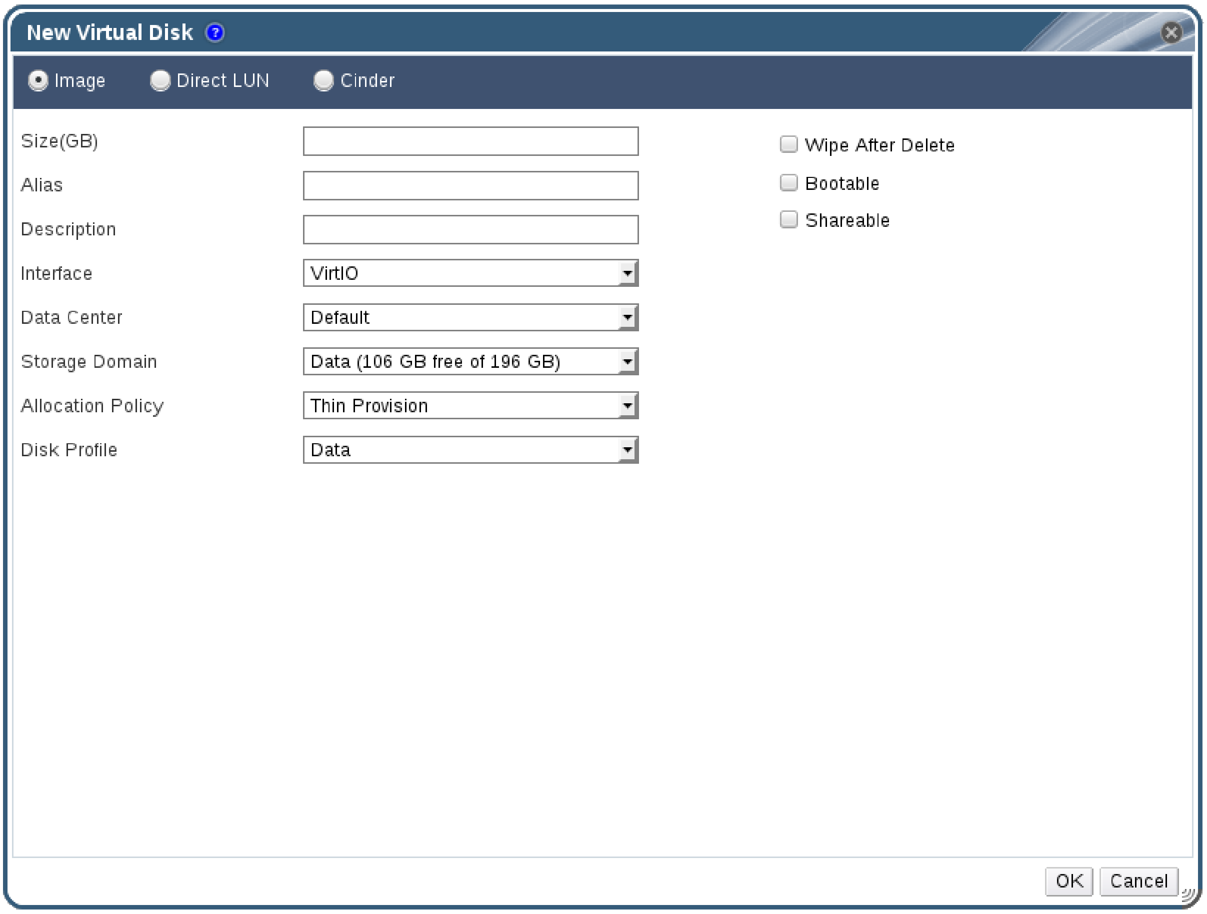


図11.1 仮想ディスクの追加ウィンドウ

3. ラジオボタンで、仮想ディスクを **イメージ**、**直接 LUN**、**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。

11.6.2. 新規仮想ディスクウィンドウの設定

表11.2 新規仮想ディスクの設定: 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は推奨されますが、必須ではありません。
インターフェース	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。
データセンター	仮想ディスクを使用できるデータセンター
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使用できる全ストレージドメインと、ストレージドメインの全容量と現在の空き容量が表示されます。

フィールド名	説明
割り当てポリシー	新規仮想ディスクのプロビジョニングポリシー • **Preallocated** を選択すると、仮想ディスクの作成時に、ストレージドメイン上のディスクの全サイズが割り当てられます。Preallocated ディスクの仮想サイズおよび実サイズは同じです。 Preallocated の仮想ディスクは、Thin Provision 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。Preallocated の仮想ディスクはサーバーや、その他の I/O を集中的に行う仮想マシンに推奨します。仮想マシンが 4 秒につき 1 GB の書き込みを行うことができる場合には、可能であれば Preallocated のディスクを使用してください。 • **Thin Provision** を選択すると、仮想ディスクの作成時に 1 GB の容量が割り当てられ、ディスクが拡張可能な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。Thin Provision ディスクは、Prealocated 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。Thin Provision の仮想ディスクはデスクトップに推奨します。
Disk Profile	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。
削除後にワイプ	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ー強化を有効にすることができます。
ブート可能	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。
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。

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、**LUN > ターゲット** には 全 LUN の一覧が表示されます。

表11.3 新規仮想ディスクの設定: 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	仮想ディスクの説明。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。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。 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、この機能を無視するには **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。詳しくは、「engine-config コマンドの構文」を参照してください。
インターフェース	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。
データセンター	仮想ディスクを使用できるデータセンター
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 **Fibre Channel** から選択可能です。

フィールド名	説明
ターゲットを検出	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。 **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 **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。 **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。 **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名前。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。 **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。
ブート可能	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。
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。
SCSI パススルーを有効にする	**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を選択しなかった場合には、仮想ディスクは、エミュレーションされた SCSI デバイスを使用します。
特権のある SCSI I/O を許可	**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。

ターゲットを検出 セクションで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。

対象のデータセンターでディスクを作成するパーミッションのある OpenStack のボリュームストレージドメインが利用できない場合には、**Cinder** の設定のフォームは無効になります。**Cinder** ディスクには、**外部プロバイダー** のウィンドウで Red Hat Virtualization 環境に追加された OpenStack ボリュームのインスタンスへのアクセスが必要です。詳しくは、「ストレージ管理のための OpenStack Volume (Cinder) インスタンスの追加」を参照してください。

表11.4 新規仮想ディスクの設定: 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は推奨されますが、必須ではありません。
インターフェース	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。
データセンター	仮想ディスクを使用できるデータセンター
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使用できる全ストレージドメインと、ストレージドメインの全容量と現在の空き容量が表示されます。
ボリュームのタイプ	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。
ブート可能	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。
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。

11.6.3. 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、仮想マシン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が移行される際には、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。

11.6.4. 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。

手順11.3 仮想ディスクの移動

1. **ディスク** タブを選択します。
2. 移動する仮想ディスクを 1 つまたは複数選択します。
3. **移動** をクリックして **ディスクの移動** ウィンドウを開きます。
4. **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。
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。

仮想ディスクがターゲットのストレージドメインに移動され、移動中にはステータス **Locked** となります。

11.6.5. 仮想ディスクのコピー

概要

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。

手順11.4 仮想ディスクのコピー

1. **ディスク** タブを選択します。
2. コピーする仮想ディスクを選択します。
3. **コピー** ボタンをクリックし、**ディスクのコピー** ウィンドウを開きます。
4. オプションで、**エイリアス** テキストフィールドにエイリアスを入力します。
5. **ターゲット** のドロップダウンメニューを使用して、仮想ディスクのコピー先となるストレージドメインを選択します。
6. **OK** をクリックします。

結果

仮想ディスクがターゲットのストレージドメインにコピーされ、コピー中にはステータス **Locked** となります。

11.6.6. ストレージドメインへのディスクイメージのアップロード

QEMU 互換のある仮想マシンのディスクイメージは、ローカルマシンから Red Hat Virtualization ストレージドメインにアップロードすることも、仮想マシンにアタッチすることもできます。

仮想マシンのディスクイメージタイプは、QCOW2 または Raw でなければなりません。QCOW2 ディスクイメージから作成したディスクは共有できません。QCOW2 ディスクイメージファイルにはバッキングファイルが含まれないようにしてください。

前提条件:

- **engine-setup** の実行時にイメージ I/O プロキシーを設定する必要があります。詳しい情報は、『インストールガイド』の「Red Hat Virtualization Manager の設定」を参照してください。
- 管理ポータルへのアクセスに使用する必須の認証局を Web ブラウザーにインポートする必要があります。
- このアップロード手順を実行するには、Internet Explorer 10、Firefox 35 または Chrome 13 以降が必要です。これ以前のバージョンは、必須の HTML5 API がサポートされません。

注記

認証局のインポートは、https://*engine_address*/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA に移動して、トラストの設定をすべて選択します。

手順11.5 ストレージドメインへのディスクイメージのアップロード

1. イメージのアップロード画面を開きます。

    - **ディスク** タブの **アップロード** のドロップダウンリストから **起動** を選択します。

    - または、**ストレージ** タブからストレージドメインを選択して、次に **ディスク** サブタブを選択し、**アップロード** のドロップダウンリストから **起動** を選んでください。

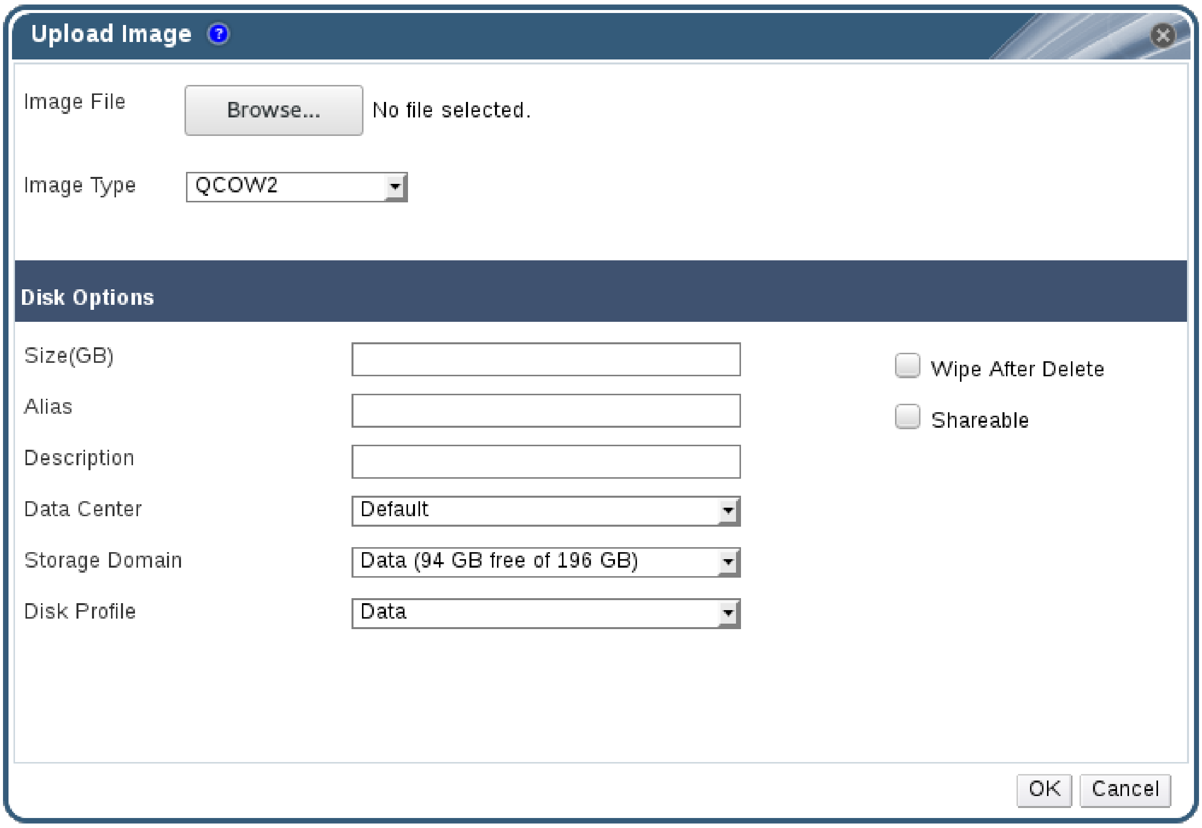


図11.2 イメージのアップロード画面

2. **イメージのアップロード** 画面で、**ファイルを選択** をクリックしてローカルディスクのイメージを選択します。

3. **イメージタイプ** を **QCOW2** または **Raw** に設定します。

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。

プログレスバーで、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** のドロップダウンリスト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。

11.6.7. インポートされたストレージドメインからのディスクイメージのインポート

詳細ペインの **ディスクのインポート** タブを使用して、インポートされたストレージドメインからフローティング仮想ディスクをインポートします。

注記

Manager にインポート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。

手順11.6 ディスクイメージのインポート

1. データセンターにインポートしたストレージドメインを選択します。
2. 詳細ペインで **ディスクのインポート** をクリックします。
3. インポートする仮想マシンを 1 台または複数選択して **インポート** をクリックすると、**ディスクのインポート** ウィンドウが開きます。
4. 各ディスクに適切な **ディスクプロファイル** を選択します。
5. **OK** をクリックすると選択したディスクがインポートされます。

11.6.8. インポートされたストレージドメインからの未登録ディスクイメージのインポート

詳細ペインの **ディスクのインポート** タブを使用して、ストレージドメインからフローティング仮想ディスクをインポートします。Red Hat Virtualization 環境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、インポート予定で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。

手順11.7 ディスクイメージのインポート

1. データセンターにインポートしたストレージドメインを選択します。
2. ストレージドメインを右クリックして、Manager が未登録のディスクを特定できるように **ディスクのスキャン** を選択します。
3. 詳細ペインで **ディスクのインポート** 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て **インポート** をクリックすると、**ディスクのインポート** ウィンドウが開きます。
5. 各ディスクに適切な **ディスクプロファイル** を選択します。
6. **OK** をクリックすると選択したディスクがインポートされます。

11.6.9. OpenStack Image Service からの仮想ディスクイメージのインポート

概要

OpenStack Image Service 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 Service によって管理される仮想ディスクイメージを Manager にインポートすることが可能です。

1. **ストレージ** リソースタブをクリックして、結果一覧から OpenStack Image Service ドメインを選択します。

2. 詳細ペインの **イメージ** タブでインポートするイメージを選択します。

3. **インポート** をクリックすると **イメージのインポート** ウィンドウが開きます。

4. **データセンター** ドロップダウンメニューから、仮想ディスク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。

5. **ドメイン名** ドロップダウンメニューから、仮想ディスク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。

6. オプションで、**クォータ** ドロップダウンメニューから、仮想ディスクイメージに適用するクォータを選択します。

7. **OK** をクリックしてイメージをインポートします。

結果

イメージがフローティングディスクとしてインポートされて、**ディスク** リソースタブの結果一覧に表示されます。これで仮想マシンにアタッチできる状態となりました。

11.6.10. OpenStack Image Service への仮想マシンディスクのエクスポート

概要

外部プロバイダーとして Manager に追加済みの OpenStack Image Service に仮想マシンディスクをエクスポートすることができます。

1. **ディスク** リソースタブをクリックします。

2. エクスポートするディスクを選択します。

3. **エクスポート** ボタンをクリックすると、**イメージのエクスポート** ウィンドウが開きます。

4. **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 Service を選択します。

5. 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。

6. **OK** をクリックします。

結果

仮想マシンディスクが指定した OpenStack Image Service にエクスポートされて、仮想マシンのディスクイメージとして管理されるようになりました。

重要

仮想マシンディスクは、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ていない場合にのみエクスポートが可能です。

11.7. 仮想ディスクとパーミッション

11.7.1. 仮想ディスクのシステムパーミッションの管理

システム管理者は、**SuperUser** として管理ポータルの全側面を管理する管理者です。他のユーザーには、より特定的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のみに対して (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のみに対して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、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 Creator ロールは以下のアクションが可能です。

- 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。

11.7.2. 仮想ディスクのユーザーロール

仮想ディスクのユーザーパーミッションロール

以下の表には、ユーザーポータルで仮想マシン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説明をまとめています。

表11.5 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マシンディスクの作成/編集/管理/削除ができます。	このロールは個別の仮想ディスクには適用されません。このロールは、**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で適用します。

11.7.3. 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。

手順11.8 リソースへのロール割り当て

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。

2. 詳細ペインの **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。

ユーザーにロールが割り当てられました。このユーザーは、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。

11.7.4. リソースからの管理者またはユーザーロールの削除

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。

手順11.9 リソースからのロール削除

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧に表示された候補の中から対象のリソースを選択します。

2. 詳細ペインの **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。パーミッションが削除されることを確認する **パーミッションの削除** ウィンドウが開きます。

5. **OK** をクリックします。

ユーザーロールおよび関連付けられたパーミッションが削除されました。

第12章 外部プロバイダー

12.1. 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 を使用した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 に追加した後には、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、『Installation Guide』および『Host Configuration Guide』を参照してください。

OpenStack Image Service (Glance) によるイメージ管理

OpenStack Image Service は、仮想マシンイメージのカタログを提供します。Red Hat Virtualization では、これらのイメージを Red Hat Virtualization Manager にインポートして、フローティングディスクとして使用したり、仮想マシンに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 Service を Manager に追加した後には、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 環境内の仮想マシンディスクを仮想マシンディスクイメージとして OpenStack Image Service にエクスポートすることも可能です。

OpenStack Networking (Neutron) インスタンスによるネットワークプロビジョニング

OpenStack Network 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 に追加した後には、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) によるストレージ管理

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 に追加した後には、OpenStack Volume によって提供されるストレージを作成することが可能となります。

VMware による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 に追加した後に、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、指定したプロキシーホストで、インポート操作の一貫として実行されます。

ネットワークプロビジョニング向けの外部ネットワークプロバイダー

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ー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ー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。

12.2. 外部プロバイダーの追加

12.2.1. 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の Satellite インスタンスを Red Hat Virtualization Manager に追加します。Red Hat Satellite 6.1 では、Red Hat Virtualization 4.0 がサポートされています。

手順12.1 ホストプロビジョニング用の Satellite インスタンスの追加

1. ツリーペインから **外部プロバイダー** を選択します。
2. **追加** をクリックして **プロバイダーの追加** ウィンドウを開きます。

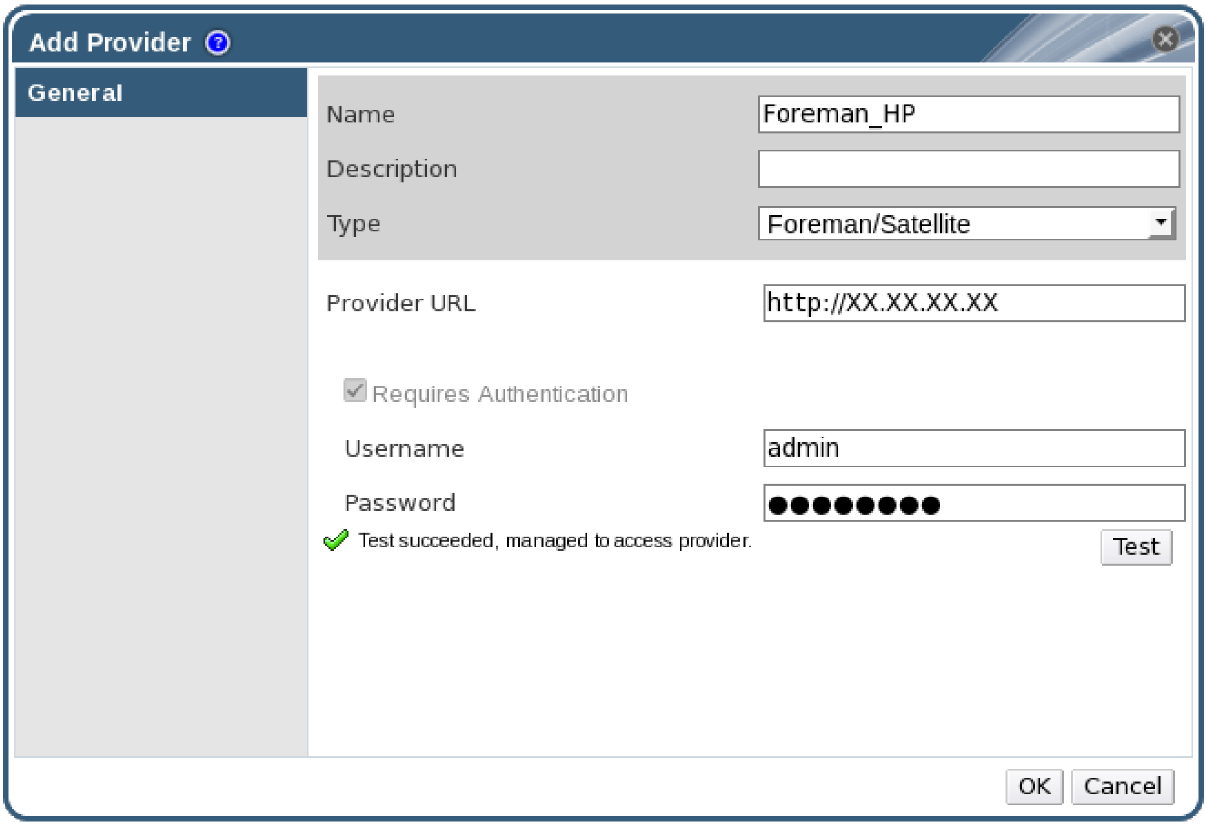


図12.1 プロバイダーの追加ウィンドウ

3. **名前** と **説明** を入力します。
4. **タイプ** の一覧で **`Foreman/Satellie`** が選択されていることを確認します。

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. 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。

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 Satellite インスタンスで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ます。

        重要

        Manager が Satellite インスタンスと通信できるようにするには、そのインスタンスが提供する証明書をインポートする必要があります。

8. **OK** をクリックします。

Satellite インスタンスを Red Hat Virtualization Manager に追加し、そのインスタンスが提供するホストを使用して作業ができるようになりました。

12.2.2. イメージ管理のための OpenStack Image (Glance) インスタンスの追加

OpenStack Image (Glance) インスタンスをイメージ管理用に Red Hat Virtualization Manager に追加します。

手順12.2 イメージ管理のための OpenStack Image (Glance) インスタンスの追加

1. ツリーペインから **外部プロバイダー** を選択します。

2. **追加** をクリックして **プロバイダーの追加** ウィンドウを開きます。

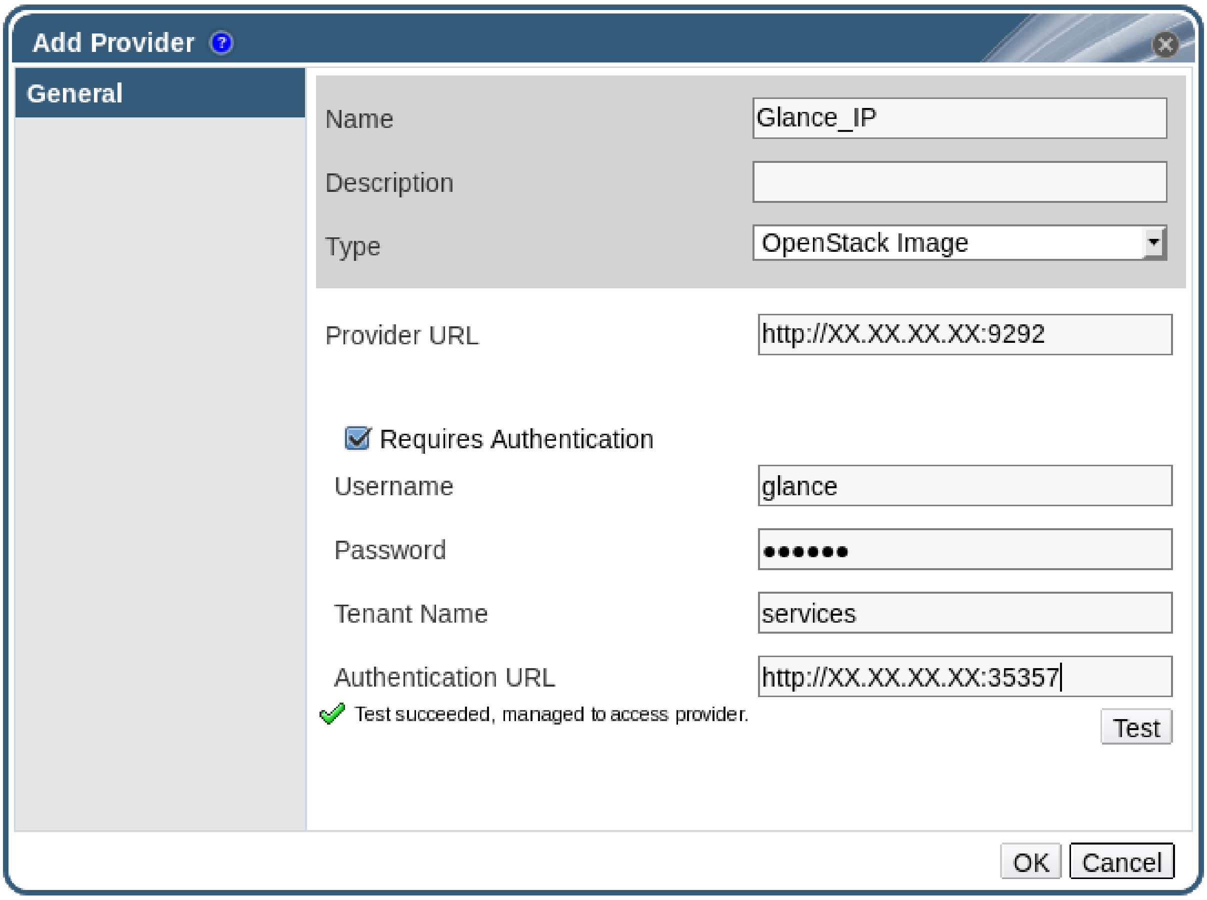


図12.2 プロバイダーの追加ウィンドウ

3. **名前** と **説明** を入力します。

4. **タイプ** の一覧から **`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**、および **テナント名** と **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と、OpenStack Image インスタンスがメンバーになっているテナン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** をクリックして、提供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ます。

   重要

   Manager が OpenStack Image インスタンスと通信できるようにするには、そのインスタンスが提供する証明書をインポートする必要があります。

8. **OK** をクリックします。

OpenStack Image インスタンスを Red Hat Virtualization Manager に追加し、そのインスタンスが提供するイメージを使用して作業ができるようになりました。

12.2.3. ネットワークプロビジョニングのための OpenStack Networking Service (Neutron) インスタンスの追加

OpenStack Networking Service (Neutron) インスタンスをネットワークプロビジョニング用に 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。

手順12.3 ネットワークプロビジョニングのための OpenStack Networking Service (Neutron) インスタンスの追加

1. ツリーペインから **外部プロバイダー** を選択します。
2. **追加** をクリックして **プロバイダーの追加** ウィンドウを開きます。

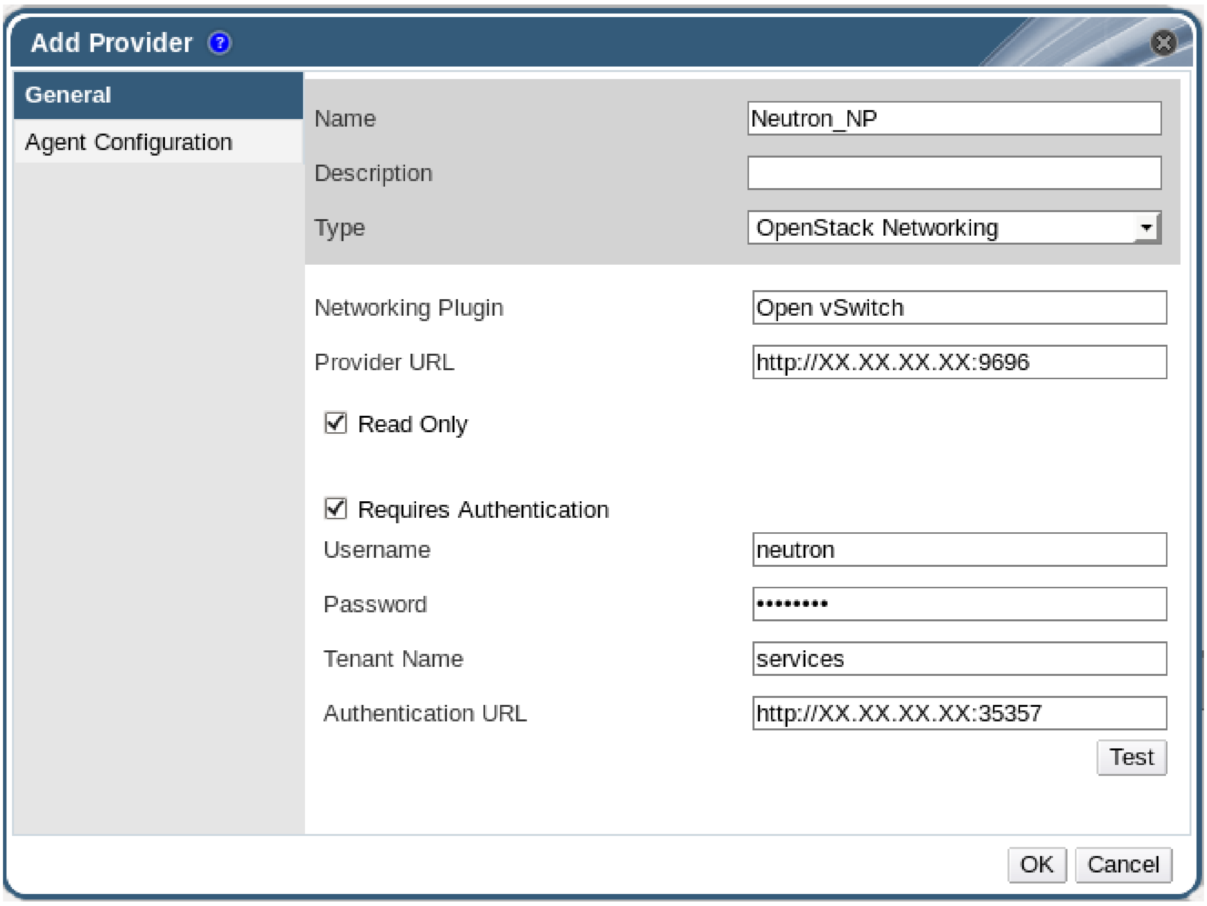


図12.3 プロバイダーの追加ウィンドウ

3. **名前** と **説明** を入力します。
4. **タイプ** の一覧から **`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 **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。**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**、および **テナント名** と **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と、OpenStack Networking インスタンスがメンバーになっているテナン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、提供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ます。

重要

Manager が OpenStack Networking インスタンスと通信できるようにするには、そのインスタンスが提供する証明書をインポートする必要があります。

9. **エージェントの設定** タブをクリックします。

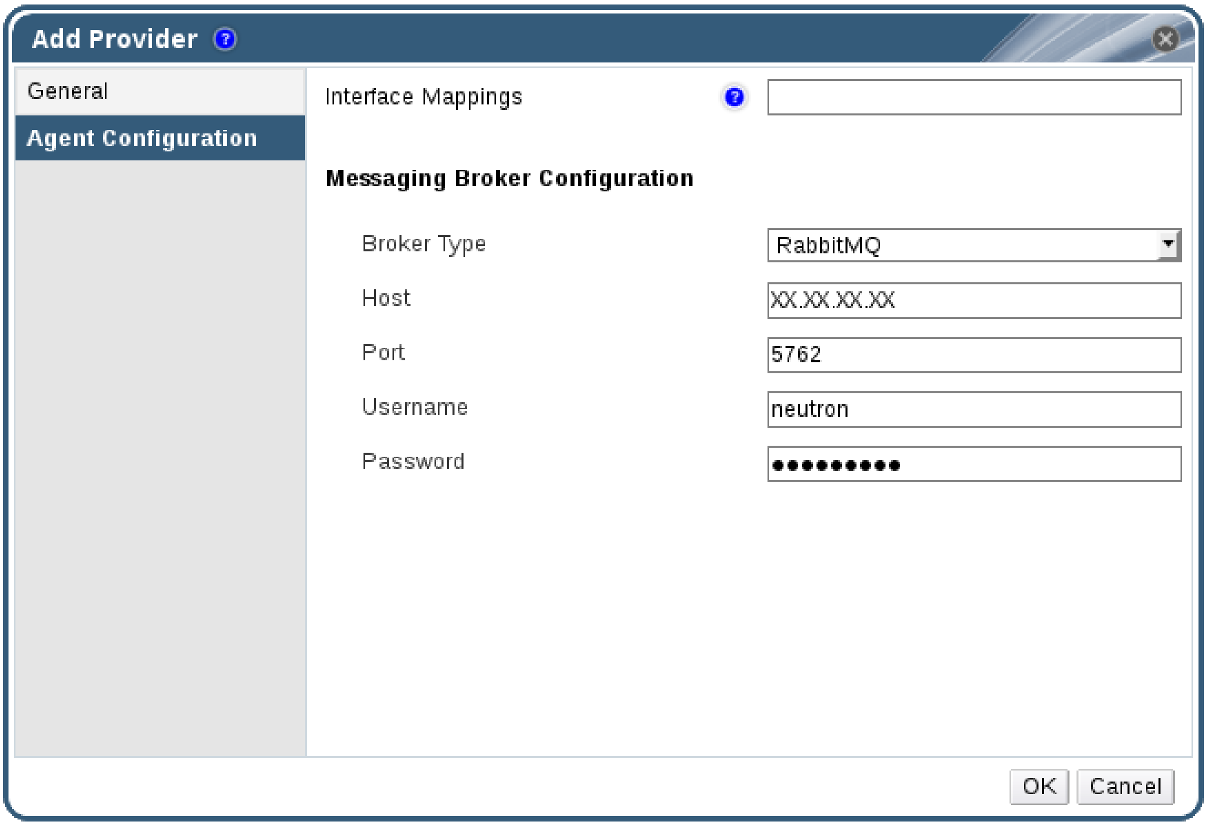


図12.4 エージェントの設定タブ

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。

12.2.4. ストレージ管理のための **OpenStack Volume (Cinder)** インスタンスの追加

Red Hat Virtualization Manager に、ストレージ管理のための OpenStack Volume (Cinder) インスタンスを追加します。OpenStack Cinder ボリュームは、Ceph Storage によりプロビジョニングされます。

手順12.4 ストレージ管理のための OpenStack Volume (Cinder) インスタンスの追加

1. ツリーペインから **外部プロバイダー** を選択します。

2. **追加** をクリックして **プロバイダーの追加** ウィンドウを開きます。

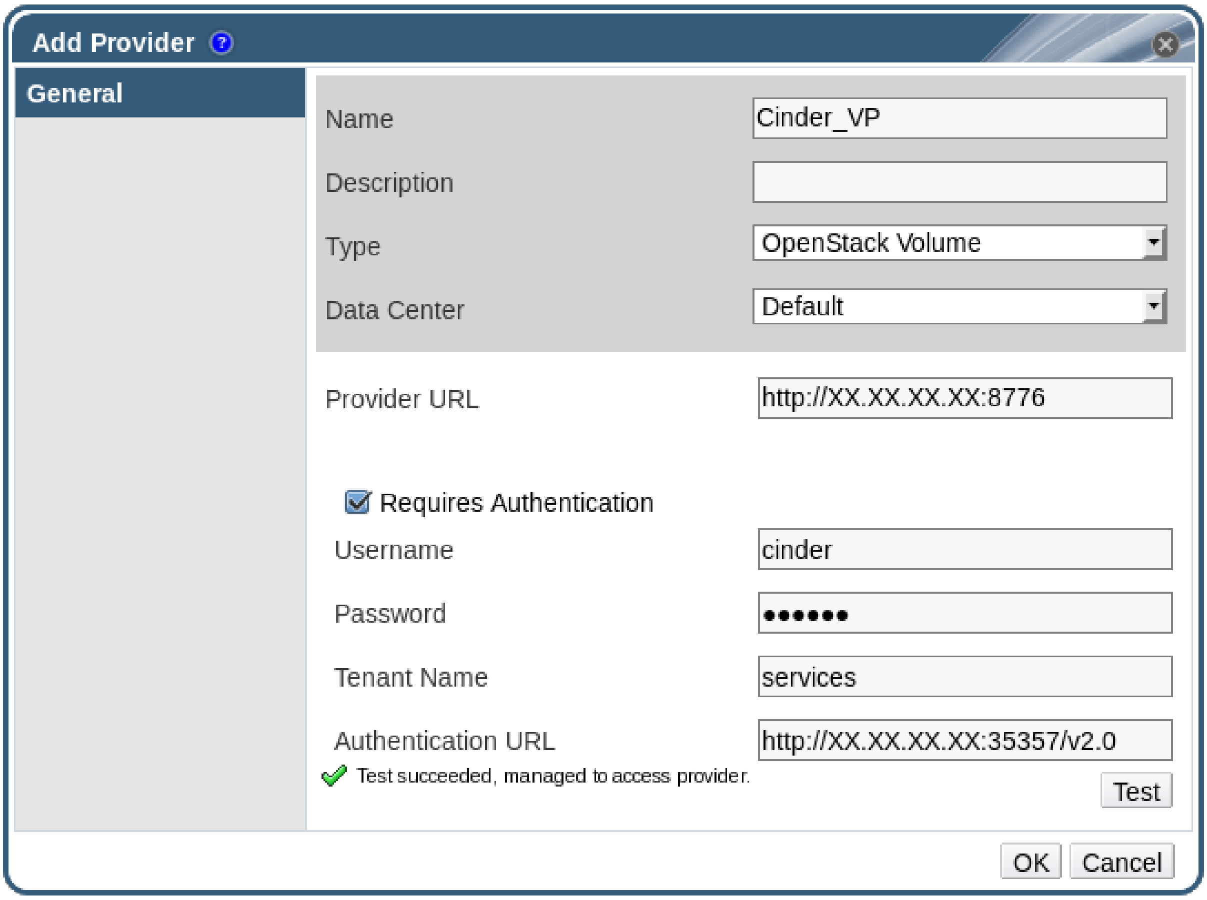


図12.5 プロバイダーの追加ウィンドウ

3. **名前** と **説明** を入力します。

4. **タイプ** の一覧から **`OpenStack Volume`** を選択します。

5. OpenStack Volume のストレージ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 Volume 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 Volume インスタンスの **ユーザー名**、**パスワード**、および **テナント名** と **認証 URL** を入力します。これには、Keystone に登録されている OpenStack Volume ユーザーのユーザー名およびパスワードと、OpenStack Volume インスタンスがメンバーになっているテナントと、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** をクリックして、提供した認証情報を使用して OpenStack Volume 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「Cephx Config 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「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** のサブ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** または既存の UUID をテキストフィールドにコピーします。

g. Cinder サーバーで、前のステップでコピーした 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 Volume インスタンスを Red Hat Virtualization Manager に追加して、そのインスタンスが提供するストレージボリュームを使用できるようになりました。OpenStack Volume (Cinder) ディスクの作成については、「フローティング仮想ディスクの作成」を参照してください。

12.2.5. VMware インスタンスを仮想マシンプロバイダーとして追加する方法

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 は V2V を使用して、VMware の仮想マシンをインポートする前に正しい形式に変換します。少なくとも 1 台の Red Hat Enterprise Linux 7.2 以降のバージョンのホストに virt-v2v パッケージをインストールする必要があります。このパッケージは、ベースの **rhel-7-server-rpms** リポジトリーで利用可能です。

手順12.5 VMware vCenter インスタンスを仮想マシンプロバイダーとして追加する方法

1. ツリーペインから **外部プロバイダー** を選択します。

2. **追加** をクリックして **プロバイダーの追加** ウィンドウを開きます。

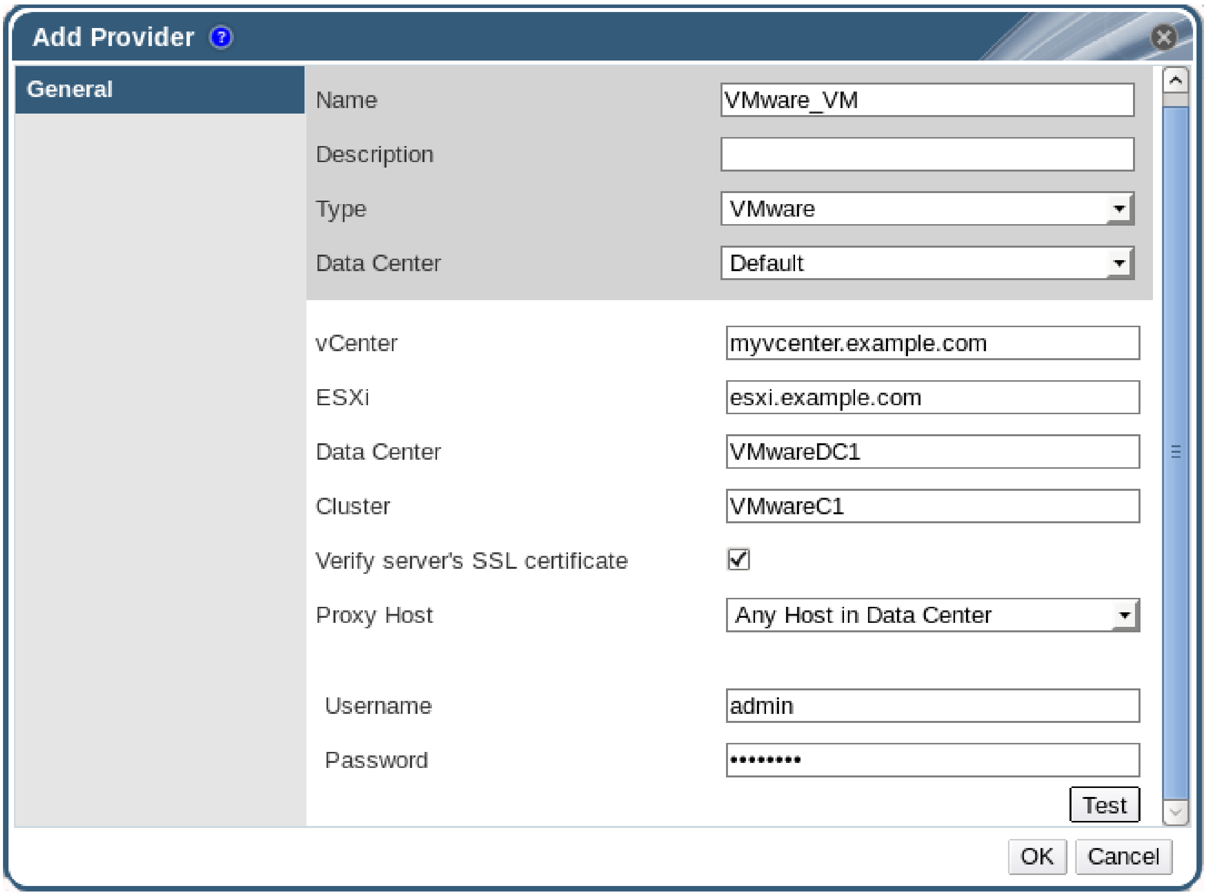


図12.6 プロバイダーの追加ウィンドウ

3. **名前** と **説明** を入力します。

4. **タイプ** の一覧から、**VMware** を選択します。

5. VMware 仮想マシン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 (**仮想マシン** タブの **インポート** 機能を使用します)。

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 **SSL 検証** をチェックした状態にしてください。交換していない場合は、このオプション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で、仮想マシンのインポート操作中に、**プロキシーホスト** 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 (**仮想マシン** タブの **インポート** 機能を使用します)。

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** をクリックして、提供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ます。

    重要

    Manager が VMware vCenter インスタンスと通信できるようにするには、そのインスタンスが提供する証明書をインポートする必要があります。

13. **OK** をクリックします。

Red Hat Virtualization Manager に VMware vCenter インスタンスを追加して、そのインスタンスが提供する仮想マシンをインポートできるようになりました。詳しくは、『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。

12.2.6. 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_instalation で入手することができます。

手順12.6 ネットワークプロビジョニング向けの外部ネットワークプロバイダーの追加

1. ツリーペインから **外部プロバイダー** を選択します。

2. **追加** をクリックします。

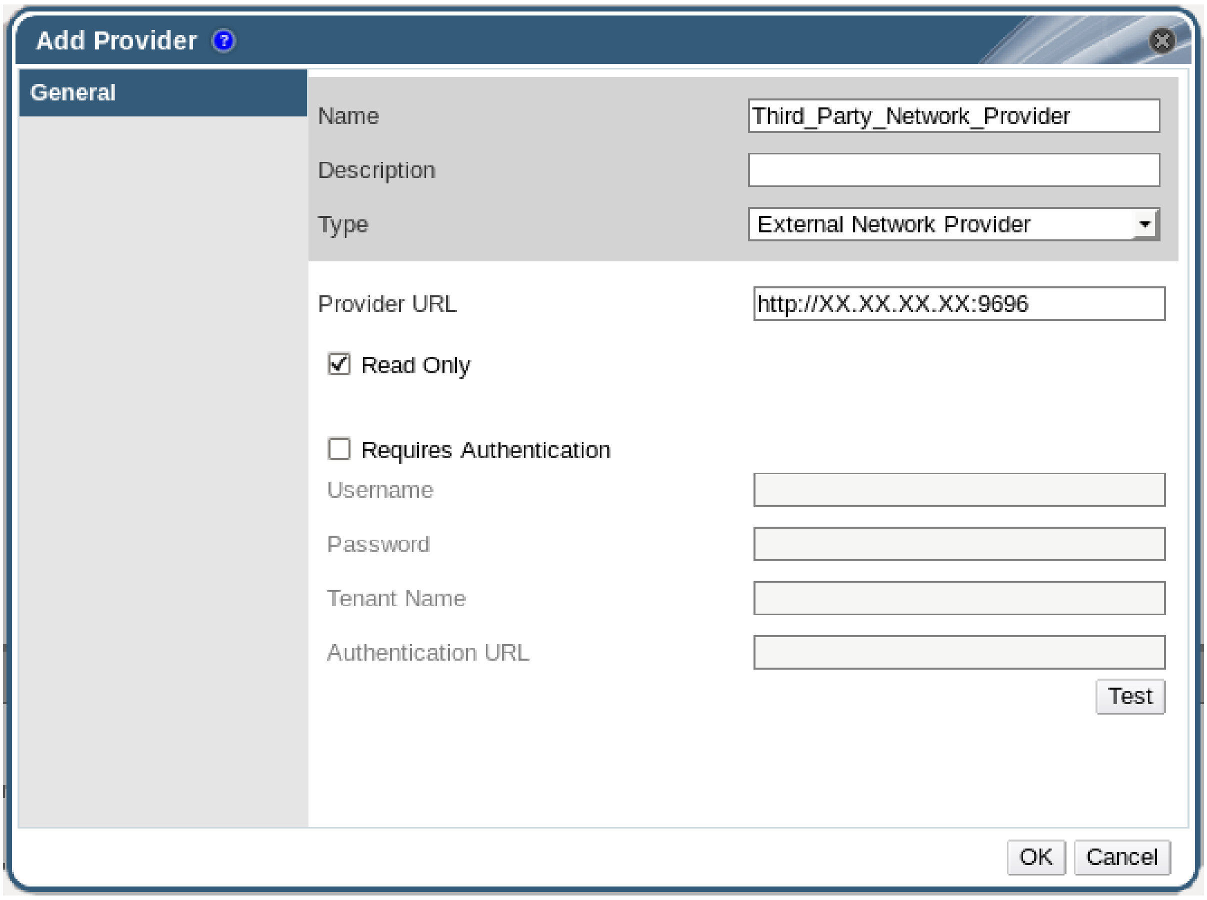


図12.7 プロバイダーの追加ウィンドウ

3. **名前** と **説明** を入力します。

4. **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。

5. **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。

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、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**、**認証 URL** を入力します。

7. 認証情報をテストします。

   a. **テスト** をクリックし、提供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。

   b. 外部ネットワークプロバイダーが SSL を使用している場合には **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を通信できるようにします。

外部ネットワークプロバイダーが Red Hat Virtualization Manager に追加されました。そ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ーをインス

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の方法については、「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。

12.2.7. プロバイダーの追加の全般設定

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12.1 プロバイダーの追加: 全般設定

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	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。 **`Foreman/Satellite`** • **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。 • **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。 **`OpenStack Image`** • **プロバイダーの URL**: OpenStack Image Service 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 Service 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。

<table>
<tr><th>設定</th><th>説明</th></tr>
<tr><td></td><td>

認証が必要: OpenStack Image Service 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 Service に接続するためのユーザー名。このユーザー名は、OpenStack Image Service 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 Service 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 <code>glance</code> 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 Service 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 Service のパスワードである必要があります。
テナント名: OpenStack Image Service がメンバーとなっている OpenStack テナント。デフォルトでは、<code>services</code> です。
認証 URL: OpenStack Image Service が認証を行う Keystone サーバーの URL とポート

<code>OpenStack Networking</code>

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。オプションは <code>Open vSwitch</code> のみで、デフォルトで選択されます。
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 Service 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 <code>neutron</code> 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

</td></tr>
</table>

設定	説明
	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 **`OpenStack Volume`** • **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。 • **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 **`VMware`** • **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

設定	説明
	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 • **SSL 認証**: 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。 • **プロキシーホスト**: 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)。 • **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ある必要があります。 • **パスワード**: 上記のユーザーを認証するパスワード **外部ネットワークプロバイダー** • **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

設定	説明
	• **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。

12.2.8. プロバイダーエージェント設定の設定値

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、ユーザー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12.2 プロバイダーの追加: 全般設定

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
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
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

12.3. 外部プロバイダーの編集

12.3.1. 外部プロバイダーの編集

手順12.7 外部プロバイダーの編集

1. ツリーペインから **外部プロバイダー** を選択します。
2. 編集する外部プロバイダーを選択します。

3. **編集** ボタンをクリックすると、**プロバイダーの編集** ウィンドウが表示されます。

4. 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。

5. **OK** をクリックします。

12.4. 外部プロバイダーの削除

12.4.1. 外部プロバイダーの削除

手順12.8 外部プロバイダーの削除

1. ツリーペインから **外部プロバイダー** を選択します。

2. 削除する外部プロバイダーを選択します。

3. **削除** をクリックします。

4. **プロバイダーの削除** ウィンドウで **OK** をクリックして、このプロバイダーの削除を確定します。

パート III. 環境の管理

第13章 バックアップと移行

13.1. RED HAT VIRTUALIZATION MANAGER のバックアップと復元

13.1.1. 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。

13.1.2. 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

データベースの初期設定後に作成した追加のデータベースユーザーは、新しいデータベースには移行されません。新規データベースのある復元後の環境に、バックアップ済みのパーミッションを指定してデータベースユーザーを追加するには、データベースとユーザーを手動で作成してから、***--restore-permissions*** パラメーターでバックアップを復元する必要があります。PostgreSQL データベースを手動で作成する方法は、『インストールガイド』のhttps://access.redhat.com/documentation/en/red-hat-virtualization/4.0/single/installation-guide/#appe-Preparing_a_Remote_PostgreSQL_Database_for_Use_with_the_Red_Hat_Enterp 参照してください。

13.1.3. engine-backup コマンドを使用したバックアップの作成

Red Hat Virtualization Manager は、**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。

手順13.1 engine-backup コマンドの使用例

1. Red Hat Virtualization Manager を実行しているマシンにログインします。

2. バックアップを作成します。

   例13.1 完全バックアップの作成

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

   例13.2 Manager データベースのバックアップの作成

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

   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。

13.1.4. engine-backup コマンドを使用したバックアップの復元

engine-backup コマンドを使用し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 version 4.0 環境のバックアップは、別の Red Hat Virtualization version 4.0 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。

13.1.5. 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。

手順13.2 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 --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 --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 --provision-db --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 --provision-dwh-db --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.
   ```

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。

13.1.6. 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用です。

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。

手順13.3 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。

   - 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
     ```

   - 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.
   ```

4. 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
   ```

13.1.7. 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用です。

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。

手順13.4 異なる認証情報を使用したバックアップの復元

1. Red Hat Virtualization Manager がインストールされているマシンにログインします。

2. 以下のコマンドを実行し、プロンプトに従って Manager 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。

    1. postgresql のコマンドラインに入ります。

    ```
    # su postgres
    $ psql
    ```

    2. 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規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、パスワードを指定せずにデータベースごとに **--*password** オプションを使用しており、データベースごとにパスワードが要求されます。これらのオプションに対して、コマンド自体で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、この方法は推奨していません。代わりに、各データベースに対して **--*passfile=***password_file* オプションを使用すると、対話型プロンプトなしで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、**ovirt-engine** サービスを正しく設定します。

```
# engine-setup
```

13.1.8. engine データベースをリモートサーバーのデータベースへ移行する手順

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リストアは、**engine-backup** を使用します。以下の手順では、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が前提となっています。『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ライブ」を参照してください。

手順13.5 データベースの移行

1. Red Hat Virtualization Manager のマシンにログインし、engine のバックアップを干渉しないように **ovirt-engine** サービスを停止します。

```
# service ovirt-engine stop
```

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リストアします。*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。

```
# service ovirt-engine start
```

13.2. 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

13.2.1. 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て、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。

注記

REST API の操作方法についての情報は、『REST API Guide』の「The Backup and Restore API」のセクションを参照してください。

13.2.2. 仮想マシンのバックアップ

バックアップ/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。

手順13.6 仮想マシンのバックアップ

1. REST API を使用して、バックアップ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。

2. 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
```

3. 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
```

4. 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てディスクをアクティブ化します。

```
POST /api/vms/22222222-2222-2222-2222-222222222222/disks/ HTTP/1.1
Accept: application/xml
Content-type: application/xml

<disk id="11111111-1111-1111-1111-111111111111">
```

```
    <snapshot id="11111111-1111-1111-1111-111111111111"/>
    <active>true</active>
</disk>
```

5. 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の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>
```

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。

13.2.3. 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。

手順13.7 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 「フローティング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14章 RED HAT SATELLITE によるエラータ管理

Red Hat Virtualization では、Red Hat Satellite からのエラータを 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された後に、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 4.0 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。

手順14.1 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。

手順14.2 Red Hat Virtualization Manager エラータの表示

1. ツリーペインで **エラータ** のエントリーを選択します。

2. **セキュリティー**、**バグ**、または **機能拡張** のチェックボックスをクリックすると、選択した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、『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、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
- FreeIPA
- Red Hat Identity Management (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 (rhevm) と IdM (idm-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参加させる**
- **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 http://technet.microsoft.com/en-us/library/cc732336.aspx を参照してください。

Active Directory の制御の委任に関する情報は http://technet.microsoft.com/en-us/library/cc732524.aspx 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。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、ディレクトリーサーバー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できる必要があります。検索ユーザーの識別名をメモします。ディレクトリーサーバーの管理ユーザーは使用しないでください。
- 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。

手順15.1 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. 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。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
```

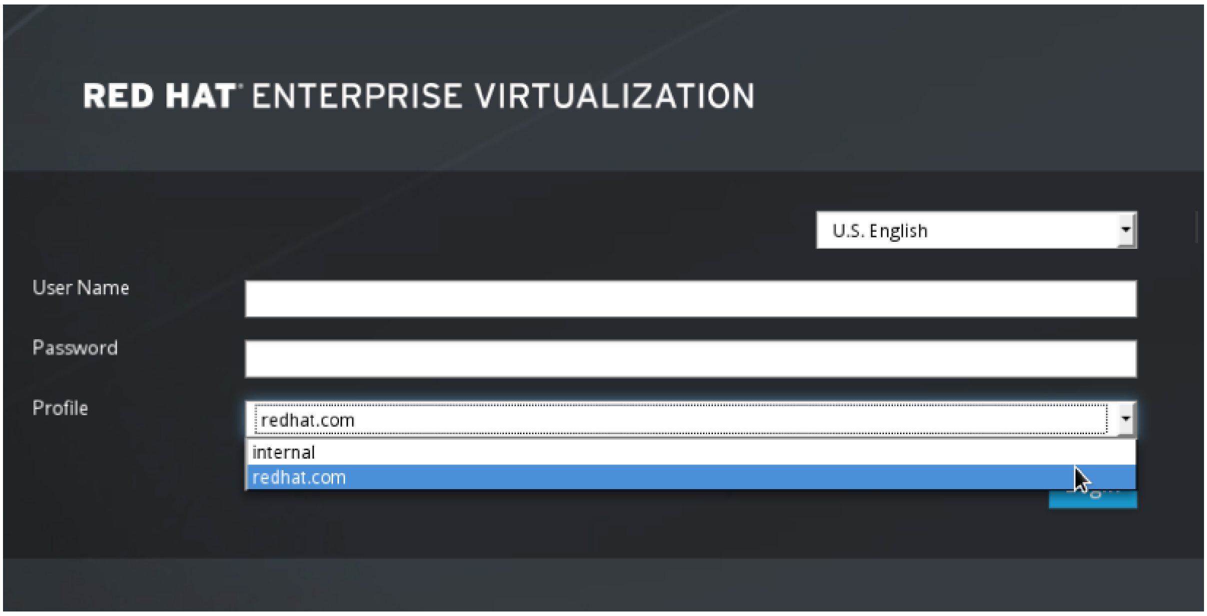


図15.1 管理者ポータルのログインページ

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、ブラウザーのクッキーに保管され、次回のユーザーログインでは事前に選択されます。

4. 対応する番号を入力して LDAP タイプを選択します。お使いの LDAP サーバーのスキーマがどれだ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 - IPA
5 - Novell eDirectory RFC-2307 Schema
6 - OpenLDAP RFC-2307 Schema
7 - OpenLDAP Standard Schema
8 - Oracle Unified Directory RFC-2307 Schema
9 - RFC-2307 Schema (Generic)
10 - RHDS
11 - RHDS RFC-2307 Schema
12 - iPlanet
Please select: 10
```

5. **Enter** を押して、デフォルト値を受け入れ、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]:
```

6. 対応する番号を入力して DNS ポリシーメソッドを選択します。

```
1 - Single server
2 - DNS domain LDAP SRV record
3 - Round-robin between multiple hosts
4 - Failover between multiple hosts
Please select:
```

   - オプション 1 の場合は、**/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。

     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 2 には、DNS サーバーのドメイン名を入力します。SRV レコードをルックアップして LDAP サーバーのドメイン名を見つけるための DNS 検索が実行されます。

   - オプション 3 には、LDAP サーバーのスペース区切り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 には、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。

7. 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 ファイルのデフォルトの場所を指定することができます。Insecure モードを選択すると、接続が TLS で暗号化されることは変わりませんが、証明書の検証はスキップされます。

```
NOTE:
It is highly recommended to use secure protocol to access the LDAP
server.
Protocol startTLS is the standard recommended method to do so.
Only in cases in which the startTLS is not supported, fallback to
non standard 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。

8. 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:
```

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.
Perform at least one Login sequence and one Search sequence.
Select test sequence to execute (Done, Abort, Login, Search)
[Abort]: Login
Enter search user name: testuser1
Enter search user password:
[ INFO  ] Executing login sequence...
...
Select test sequence to execute (Done, Abort, Login, Search)
```

```
[Abort]: Search
Select entity to search (Principal, Group) [Principal]:
Term to search, trailing '*' is allowed: testuser1
Resolve Groups (Yes, No) [No]:
[ INFO  ] Executing login sequence...
...
Select test sequence to execute (Done, Abort, Login, Search)
[Abort]: Done
[ INFO  ] Stage: Transaction setup
[ INFO  ] Stage: Misc configuration
[ INFO  ] Stage: Package installation
[ INFO  ] Stage: Misc configuration
[ INFO  ] Stage: Transaction commit
[ INFO  ] Stage: Closing up
          CONFIGURATION SUMMARY
          Profile name is: redhat.com
          The following files were created:
              /etc/ovirt-engine/aaa/redhat.com.properties
              /etc/ovirt-engine/extensions.d/redhat.com-
authz.properties
              /etc/ovirt-engine/extensions.d/redhat.com-
authn.properties
[ INFO  ] Stage: Clean up
          Log file is available at /tmp/ovirt-engine-extension-aaa-
ldap-setup-20160114064955-1yar9i.log:
[ INFO  ] Stage: Pre-termination
[ INFO  ] Stage: Termination
```

10. 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: 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。

```
# service ovirt-engine restart
```

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。

- 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できる必要があります。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。

手順15.2 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. 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
```

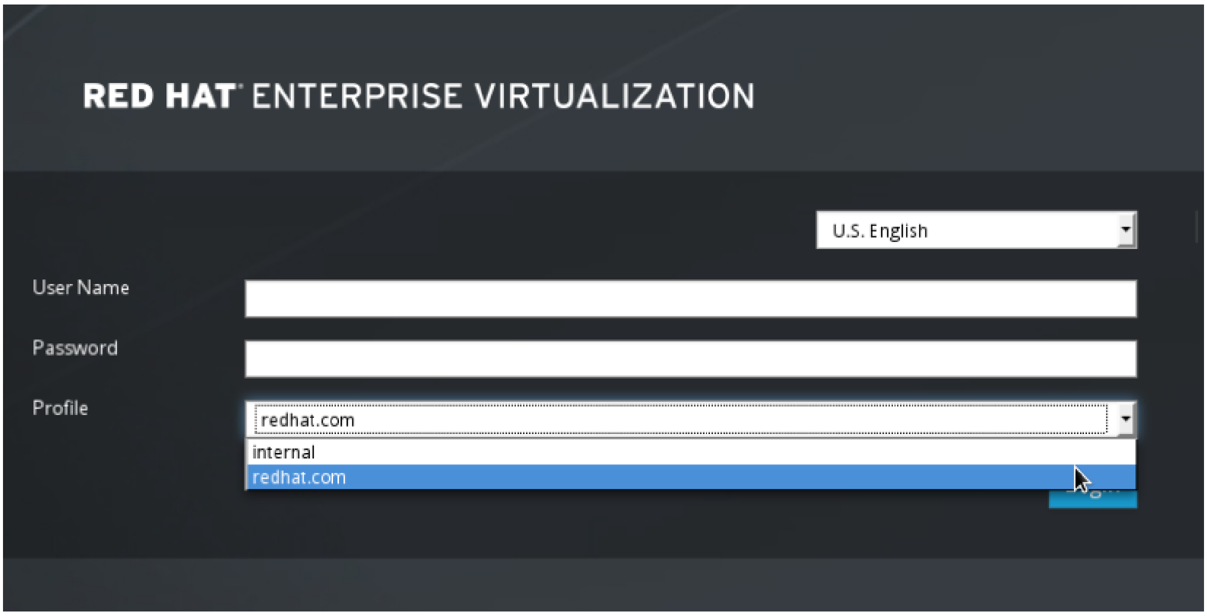


図15.2 管理者ポータルのログインページ

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、ブラウザーのクッキーに保管され、次回のユーザーログインでは事前に選択されます。

4. 対応する番号を入力して、LDAP タイプを選択します。この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 - IPA
5 - Novell eDirectory RFC-2307 Schema
6 - OpenLDAP RFC-2307 Schema
7 - OpenLDAP Standard Schema
8 - Oracle Unified Directory RFC-2307 Schema
9 - RFC-2307 Schema (Generic)
10 - RHDS
11 - RHDS RFC-2307 Schema
12 - iPlanet
Please select: 3
```

5. 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
```

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 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使用することができます。

```
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。

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 (empty for anonymous):
uid=user1,ou=Users,dc=test,dc=redhat,dc=com
Enter search user password:
```

8. 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.
Perform at least one Login sequence and one Search sequence.
Select test sequence to execute (Done, Abort, Login, Search)
[Abort]: Login
Enter search user name: testuser1
Enter search user password:
[ INFO  ] Executing login sequence...
...
Select test sequence to execute (Done, Abort, Login, Search)
[Abort]: Search
Select entity to search (Principal, Group) [Principal]:
Term to search, trailing '*' is allowed: testuser1
Resolve Groups (Yes, No) [No]:
[ INFO  ] Executing login sequence...
...
Select test sequence to execute (Done, Abort, Login, Search)
[Abort]: Done
[ INFO  ] Stage: Transaction setup
[ INFO  ] Stage: Misc configuration
[ INFO  ] Stage: Package installation
[ INFO  ] Stage: Misc configuration
[ INFO  ] Stage: Transaction commit
[ INFO  ] Stage: Closing up
          CONFIGURATION SUMMARY
          Profile name is: redhat.com
          The following files were created:
              /etc/ovirt-engine/aaa/redhat.com.properties
              /etc/ovirt-engine/extensions.d/redhat.com-
authz.properties
              /etc/ovirt-engine/extensions.d/redhat.com-
authn.properties
[ INFO  ] Stage: Clean up
          Log file is available at /tmp/ovirt-engine-extension-aaa-
ldap-setup-20160114064955-1yar9i.log:
[ INFO  ] Stage: Pre-termination
[ INFO  ] Stage: Termination
```

9. 作成したプロファイルが管理ポータルと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: 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。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の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。

手順15.3 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**) に提供されています。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 プロパティー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。プロファイル名は、管理ポータルおよびユーザーポータルのログインページで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。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。全フィールド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。

```
# service ovirt-engine restart
```

9. 作成した *example* プロファイルが管理ポータルと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: 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。

15.4. 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、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 1 つ (**mod_auth_kerb**) 設定する必要があります。Keberos 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

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。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、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。

手順15.4 Apache サービス用の Kerberos の設定

1. KDC サーバーで、**kadmin** ユーティリティーを使用して 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** ファイルが共有秘密鍵を保管します。

```
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
```

手順15.5 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_kerb** 認証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_kerb
```

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-sso**) およびその他のディレクトリータイプ用 (**simple-sso**) に提供されています。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-
sso/. /etc/ovirt-engine
```

4. Apache が SSO 設定ファイルを使用するために、**/etc/httpd/conf.d** ディレクトリーのシンボリックリンクを作成します。

```
# ln -s /etc/ovirt-engine/aaa/ovirt-sso.conf /etc/httpd/conf.d
```

5. Apache が Kerberos を認証に使用するように、認証メソッドファイルを編集します。

```
# vi /etc/ovirt-engine/aaa/ovirt-sso.conf
```

例15.5 認証メソッドファイルの例

```
<LocationMatch ^(/ovirt-engine/(webadmin|userportal|api)|/api)>
    RewriteEngine on
    RewriteCond %{LA-U:REMOTE_USER} ^(.*)$
    RewriteRule ^(.*)$ - [L,P,E=REMOTE_USER:%1]
    RequestHeader set X-Remote-User %{REMOTE_USER}s

    AuthType Kerberos
    AuthName "Kerberos Login"
    Krb5Keytab /etc/httpd/http.keytab
```

```
    KrbAuthRealms REALM.COM
    Require valid-user
</LocationMatch>
```

6. 管理ポータルおよびユーザーポータルのログインページで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
```

7. LDAP プロパティー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。プロファイル名は、管理ポータルおよびユーザーポータルのログインページで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。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。全フィールド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 =
org.ovirt.engine-extensions.aaa.misc
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-http
ovirt.engine.aaa.authn.authz.plugin = example-authz
ovirt.engine.aaa.authn.mapping.plugin = example-http-mapping
config.artifact.name = HEADER
config.artifact.arg = X-Remote-User
```

9. 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15.9 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
```

10. 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
```

11. Apache サービスと engine サービスを再起動します。

```
# service httpd restart
```

```
# service ovirt-engine restart
```

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。この関係を簡単に図にまとめると以下のようになります。

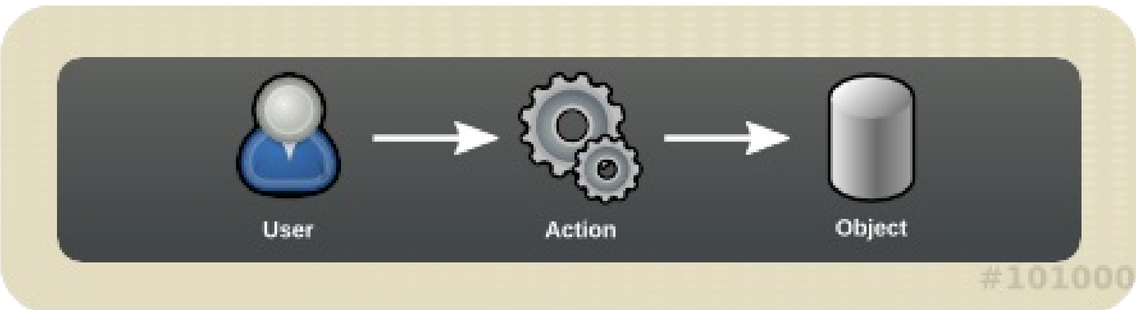


図15.3 アクション

重要

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。

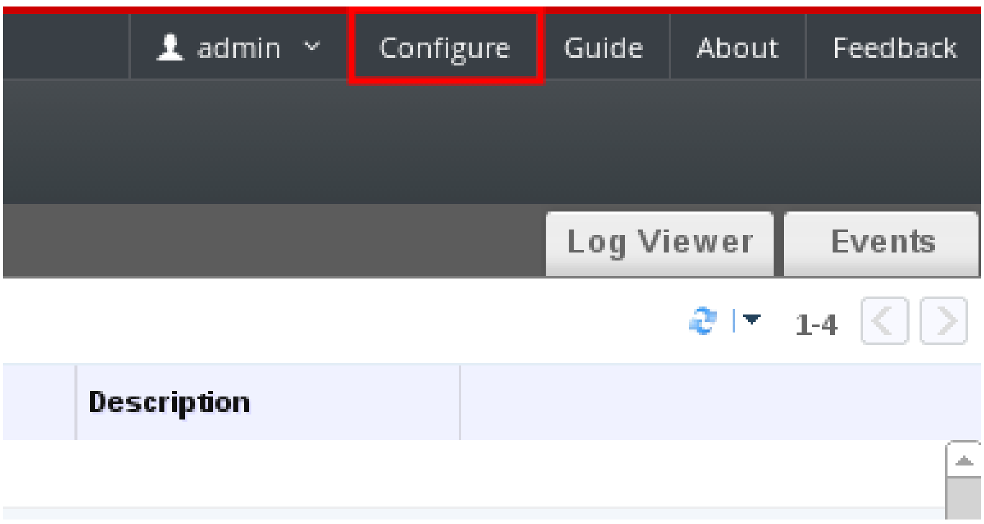
15.6. 管理ポータルからのユーザー管理タスク

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。

手順15.6 ユーザーの追加およびユーザーポータルパーミッションの割り当て

1. ヘッダーバーで **設定** をクリックして **設定** ウィンドウを開きます。**システム権限** をクリックします。



2. **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。

3. **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。

4. 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。

5. **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。

6. **OK** をクリックします。

ユーザーポータルにログインして、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

各ユーザーの詳細情報は、**ユーザー** タブで確認できます。

手順15.7 ユーザー情報の確認

1. **ユーザー** タブをクリックし、認証済みのユーザー一覧を表示します。
2. ユーザーを選択するか、結果一覧に表示されない場合は検索を行います。
3. 選択したユーザーの詳細ペインには、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を表示する **全般** タブがあります。
4. 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。

手順15.8 リソースに対するユーザーパーミッションの表示

1. リソースタブをクリックして、結果一覧からリソースを選択します。
2. 詳細ペインの **パーミッション** タブをクリックし、割り当てられたユーザー、ユーザーのロール、選択したリソースに対して継承したパーミッションを表示します。

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。

手順15.9 ユーザーの削除

1. **ユーザー** タブ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** ボタンをクリックします。削除の確認を求めるメッセージが表示されます。**OK** をクリックします。

ユーザーが 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

現在ログイン中のユーザー、セッション時間、およびその他の情報を確認することができます。ツリーペインから **アクティブなユーザーセッション** のエントリーをクリックすると、各ログインユーザーのセッションの情報が表示されます。

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。

手順15.10 ユーザーセッションの終了

1. ツリーペインで **アクティブなユーザーセッション** のエントリーをクリックします。
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

15.7.1. ユーザーの管理

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。

手順15.11 ユーザーの作成

以下の手順では、ユーザーを作成してパスワードを設定し、Red Hat Virtualization 環境に追加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. 新規ユーザーアカウントを作成します。オプションで **--attribute** を使用してアカウントの詳細を指定します。オプションの全リストは、**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
```

3. パスワードを設定します。**--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。以下の例では **-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。

4. 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ます。詳しい説明は、「ユーザーの追加およびユーザーポータルパーミッションの割り当て」を参照してください。

手順15.12 ユーザー情報の確認

以下の手順は、ユーザーアカウントの情報を表示する方法について説明します。管理ポータルの **ユーザー** タブよりもさらに詳しい情報を確認することができます。

1. Red Hat Virtualization Manager がインストールされているマシンにログインします。
2. 以下のコマンドを実行します。

```
# ovirt-aaa-jdbc-tool user show test1
```

手順15.13 ユーザー情報の編集

以下の手順では、ユーザーアカウント情報を更新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. 以下のコマンドを実行して、ユーザー情報を編集します。次の例では、メールアドレスを更新します。

```
# ovirt-aaa-jdbc-tool user edit test1 --
attribute=email=jdoe@example.com
```

手順15.14 ユーザーの削除

以下の手順では、ユーザーアカウントの削除の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. ユーザーを削除します。

```
# ovirt-aaa-jdbc-tool user delete test1
```

3. 管理ポータルからユーザーを削除します。詳しい説明は、「ユーザーの削除」を参照してください。

15.7.2. 内部管理ユーザーのパスワード変更

内部管理ユーザー (**admin@internal**) のパスワードをリセットするには、**ovirt-aaa-jdbc-tool** ツールを使用します。パスワードの変更を有効にするために **ovirt-engine** サービスを再起動する必要はありません。

デフォルトでは、内部ドメイン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。

手順15.15 内部管理ユーザーのパスワードの再設定

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. 対話モードでパスワードを変更するには、以下のコマンドを実行します。**--password-valid-to** 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。以下の例では **Z** は UTC 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 admin --password-valid-to="2025-08-01 12:00:00Z"
```

15.7.3. 内部管理ユーザーのパスワードの無効化

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。

手順15.16 内部管理ユーザーのパスワードの無効化

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。

15.7.4. 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。

手順15.17 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ユーザーポータルパーミッションの割り当て」を参照してください。

手順15.18 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ユーザーポータルパーミッションの割り当て」を参照してください。

15.7.5. ユーザー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。

手順15.19 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. - すべての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
     ```

   - 全グループアカウントの情報を一覧表示します。

     ```
     # ovirt-aaa-jdbc-tool query --what=group
     ```

手順15.20 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. - 「j」の文字で始まる名前の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"
     ```

15.7.6. アカウント設定の管理

デフォルトアカウントの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。

手順15.21 アカウント設定の更新

以下の手順では、デフォルトアカウントの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** 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のみに設定可能です。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のみに計算されます。
>
> 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が、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モードの有効化/変更

このセクションでは、データセンターのクォータモードの有効化と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。

手順16.1 データセンターのクォータの有効化/変更

1. ナビゲーションペインの **データセンター** タブをクリックします。
2. ナビゲーションペインに表示されたデータセンター一覧から、編集するクォータポリシーが設定されたデータセンターを選択します。
3. ナビゲーションペインの左上にある **編集** をクリックします。

   データセンターの編集 ウィンドウが開きます。
4. **クォータモード** ドロップダウンメニューで、クォータモードを **有効** に変更します。
5. **OK** をクリックします。

データセンターレベルでクォータモードが有効になりました。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モードを有効にしました。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。

手順16.2 新規クォータポリシーの作成

1. ツリーモードでデータセンターをクリックすると、ナビゲーションペインに **クォータ** タブが表示されます。
2. ナビゲーションペインで **クォータ** タブをクリックします。

3. ナビゲーションペインで **追加** をクリックすると、**新規クォータ** ウィンドウが開きます。

4. **名前** フィールドに分かりやすい名前を入力します。

   説明 フィールドに分かりやすい説明を入力します。

5. **新規クォータ** ウィンドウの **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. **新規クォータ** ウィンドウの **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** のラジオボタンを選択します。**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** ボタンをクリックすると、**クォータの編集** ウィンドウが表示されます。

9. **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単位で入力します。

10. **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、このクォータの CPU 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、**vCPU** フィールドに vCPU の数量を入力します。

11. **クォータの編集** ウィンドウで **OK** をクリックします。

12. **新規クォータ** ウィンドウの **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。

13. **新規クォータ** ウィンドウの **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。

14. **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** のラジオボタンを選択します。**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。

15. **編集** ボタンをクリックすると、**クォータの編集** ウィンドウが表示されます。

16. **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の上限を設定します。**上限** ラジオボタンを選択した場合は、ストレージクォータを **GB** フィールドにギガバイト単位 (GB) で入力します。

17. **クォータの編集** ウィンドウで **OK** をクリックします。**新規クォータ** ウィンドウに戻ります。

18. **新規クォータ** ウィンドウで **OK** をクリックします。

結果

新しいクォータポリシーが作成されました。

16.6. クォータの閾値設定

表16.3 クォータの閾値設定と猶予

設定	定義
クラスターの閾値	データセンターあたりで使用可能なクラスターリソースの容量
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の容量
ストレージの閾値	1 データセンターあたりで使用可能なストレージリソース容量
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

概要

以下の手順では、仮想マシンをクォータに関連付けする方法について説明します。

手順16.3 仮想マシンへのクォータ割り当て

1. ナビゲーションペインでクォータを追加する仮想マシンを選択します。
2. **編集** をクリックすると、**仮想マシンの編集**ウィンドウが表示されます。
3. **クォータ** のドロップダウンメニューで、その仮想マシンに使用するクォータを選択します。
4. **OK** をクリックします。

結果

選択した仮想マシンのクォータが指定されました。

概要

以下の手順では、仮想マシンディスクをクォータに関連付ける方法について説明します。

手順16.4 仮想ディスクへのクォータ割り当て

1. ナビゲーションペインで、クォータを追加する仮想マシン (複数可) を選択します。
2. 詳細ペインでクォータに関連付けるディスクを選択します。
3. **編集** をクリックすると、**仮想ディスクの編集** ウィンドウが開きます。
4. 仮想ディスクに使用するクォータを選択します。

5. **OK** をクリックします。

結果

選択した仮想ディスクのクォータが指定されました。

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を関連付けし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

概要

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。

手順16.5 クォータへのユーザー割り当て

1. ツリーモードで、ユーザーと関連付けるクォータが設定されているデータセンターをクリックします。
2. ナビゲーションペインで **クォータ** タブをクリックします。
3. ナビゲーションペインの一覧から対象のクォータを選択します。
4. 詳細ペインの **コンシューマー** タブをクリックします。
5. 詳細ペインの最上部の **追加** をクリックします。
6. **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。
7. **検索** をクリックします。
8. 対象のユーザーの名前が表示された行の左側にあるチェックボックスを選択します。
9. **クォータへのユーザー/グループ割り当て** ウィンドウの右下の **OK** をクリックします。

結果

しばらくすると、詳細ペインの **コンシューマー** タブにユーザーが表示されます。

16.9. クォータの編集

概要

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。

手順16.6 クォータの編集

1. ツリーペインで、編集するクォータのあるデータセンターをクリックします。

2. ナビゲーションペインの **クォータ** タブをクリックします。

3. 編集するクォータをクリックします。

4. ナビゲーションペインで **編集** ボタンをクリックします。

5. **クォータの編集** ウィンドウが開きます。必要な場合には、**名前** フィールドに、わかりやすい名前を入力します。

6. 必要な場合には、**説明** フィールドに、わかりやすい説明を入力します。

7. **すべてのクラスター** ラジオボタンまたは **特定のクラスター** ラジオボタンのいずれかを選択します。**メモリー & CPU** のスライダーで **クラスターの閾値** と **クラスターの猶予** のつまみを必要な位置に動かします。

8. **すべてのストレージドメイン** ラジオボタンまたは **特定のストレージドメイン** ラジオボタンのいずれかを選択します。**ストレージ** のスライダーで **ストレージの閾値** と **ストレージの猶予** のつまみを必要な位置に動かします。

9. **クォータの編集** ウィンドウで **OK** をクリックし、新規設定を確定します。

結果

既存のクォータが変更されました。

16.10. クォータの削除

概要

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。

手順16.7 クォータの削除

1. ツリーペインで、編集するクォータのあるデータセンターをクリックします。

2. ナビゲーションペインの **クォータ** タブをクリックします。

3. 削除するクォータの名前をクリックします。

4. タブの列の下にあるナビゲーションペイン上部の **削除** をクリックします。

5. **クォータの削除** ウィンドウで **OK** をクリックし、このクォータの削除を確定します。

結果

クォータが削除されました。

16.11. SERVICE LEVEL AGREEMENT ポリシーの有効化

概要

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。

手順16.8 service level agreement CPU ポリシーの有効化

1. ナビゲーションペインで、**新規仮想マシン** をクリックします。

2. **詳細オプションを表示** をクリックします。

3. **リソースの割り当て** タブを選択します。

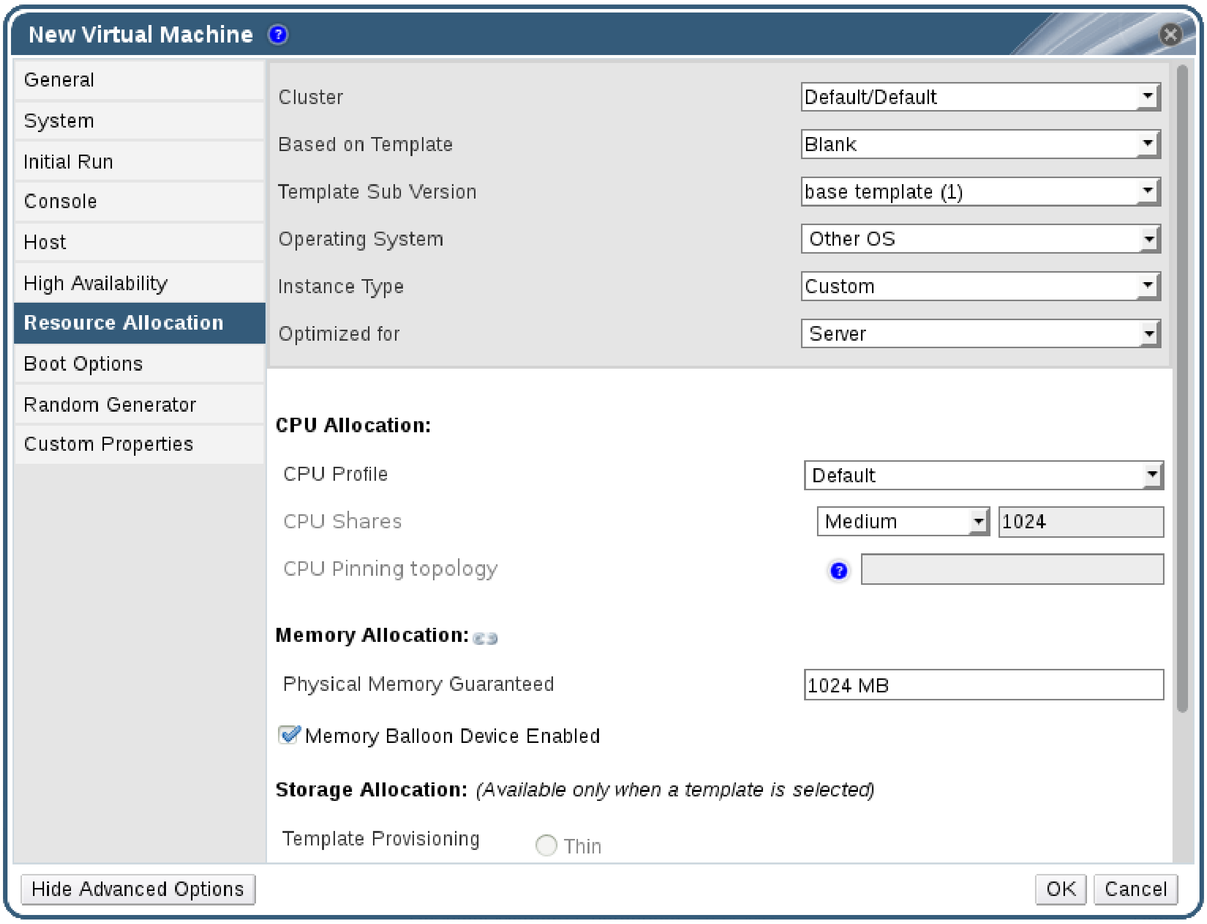


図16.1 service level agreement ポリシーの有効化 - CPU 割り当てのメニュー

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。

結果

service level agreement CPU ポリシーを設定しました。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

概要

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。

手順17.1 イベント通知の設定

1. 適切な変数を使用してメール転送エージェントを設定します。
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. 詳細ペインの **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** をクリックすると、**イベント通知の追加** ウィンドウが開きます。

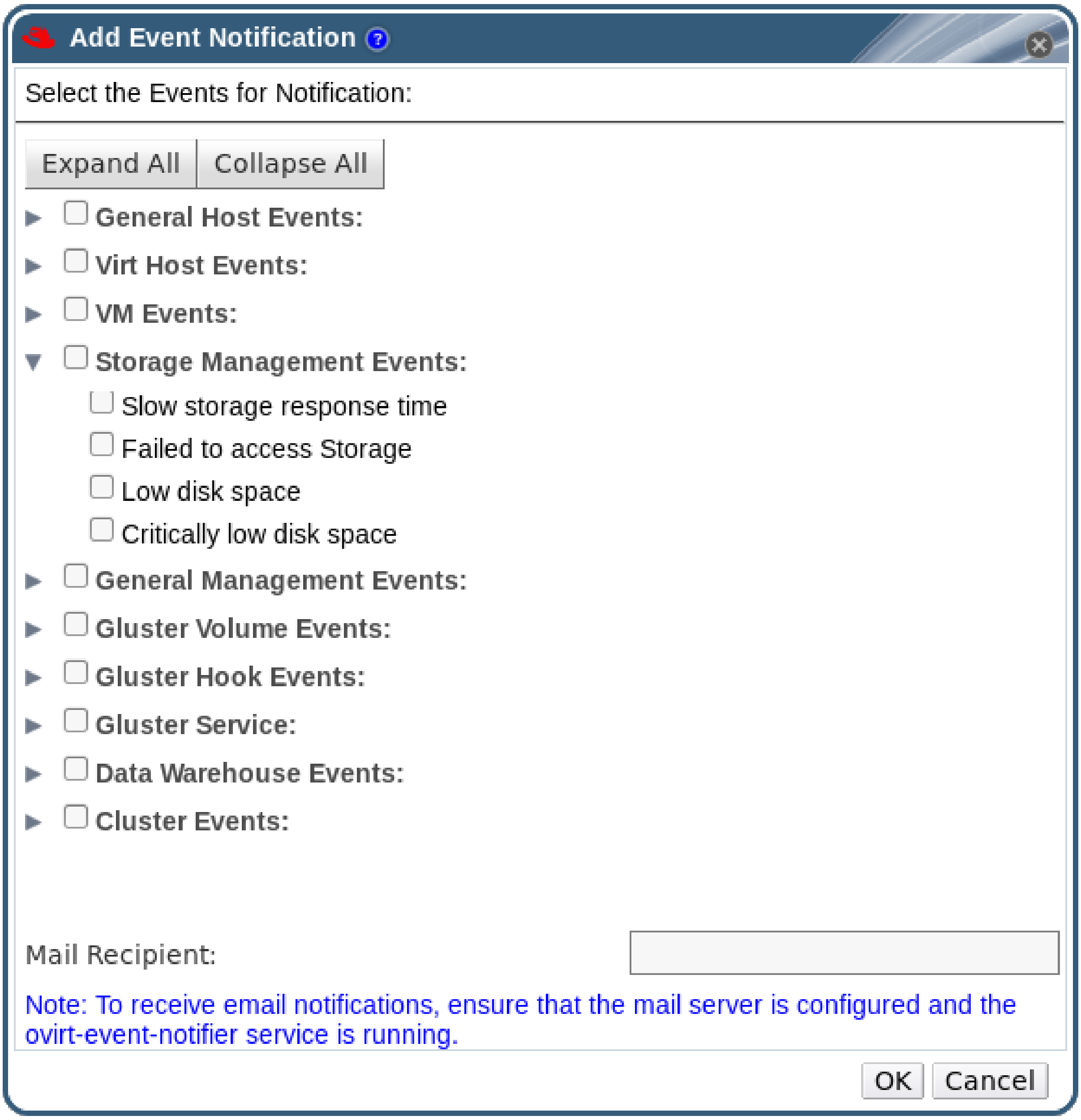


図17.1 イベント通知の追加のウィンドウ

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** をクリックして変更を保存し、ウィンドウを閉じます。

9. Red Hat Virtualization Manager で **ovirt-engine-notifier** サービスを追加して起動すると、変更した内容が有効になります。

```
# chkconfig --add ovirt-engine-notifier
# chkconfig ovirt-engine-notifier on
# service ovirt-engine-notifier restart
```

結果

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

概要

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。

手順17.2 イベント通知のキャンセル

1. **ユーザー** タブでユーザーまたはユーザーグループを選択します。
2. 詳細ペインの **イベント通知機能** タブを選択すると、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。
3. **イベントを管理** をクリックすると、**イベント通知の追加** ウィンドウが開きます。
4. **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。
5. 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。
6. **OK** をクリックして変更を保存し、ウィンドウを閉じます。

結果

不要なイベント通知がキャンセルされました。

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	/usr/share/jbossas	Manager が使用する JBoss application server の場所
ENGINE_ETC	/etc/ovirt-engine	Manager が使用する **etc** ディレクトリーの場所
ENGINE_LOG	/var/log/ovirt-engine	Manager が使用する **logs** ディレクトリーの場所
ENGINE_USR	/usr/share/ovirt-engine	Manager が使用する **usr** ディレクトリーの場所
ENGINE_JAVA_MODULEPATH	${ENGINE_USR}/modules	JBoss モジュールを追加するファイルパス

変数名	デフォルト	備考
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)
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。

変数名	デフォルト	備考
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。
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 設定コネクターが使用するプロトコル
SSL_IGNORE_CERTIFICATE_ERRORS	false	JBoss がセキュアなモードで実行され、SSL エラーが無視されようにする場合には、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ようにする場合には、この値は **`true`** に設定する必要があります。

変数名	デフォルト	備考
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 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決定します。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、同じコミュニティー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。

手順17.3 Manager で SNMP トラップを設定します

手順17.3 Manager で SNMP トラップを設定します。

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* 以外は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。

```
# service ovirt-engine-notifier start
# chkconfig ovirt-engine-notifier on
```

■

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

SNMP_MANAGERS、**MAIL_SERVER**、または両方を **/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf** または上書き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/imageuploader.conf.d/10-engine-setup.conf
- /etc/ovirt-engine/isouploader.conf.d/10-engine-setup.conf
- /etc/ovirt-engine/logcollector.conf.d/10-engine-setup.conf
- /etc/pki/ovirt-engine/cert.conf
- /etc/pki/ovirt-engine/cert.template
- /etc/pki/ovirt-engine/certs/apache.cer
- /etc/pki/ovirt-engine/keys/apache.key.nopass
- /etc/pki/ovirt-engine/keys/apache.p12

警告

ovirt-engine-rename コマンドは、Manager 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、engine の証明書や認証局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 ツールの使用方法

概要

ovirt-engine-rename コマンドを使用して、Manager の完全修飾ドメイン名の記録を更新することができます。

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。

手順18.1 Red Hat Virtualization Manager の名前変更

1. 新しい完全修飾ドメイン名用に、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. 次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]
```

結果

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。

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ーです。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 サービスを再起動して、変更を有効にします。

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。

```
# service ovirt-engine restart
```

18.3. イメージアップローダーツール

18.3.1. イメージアップローダーツール

注記

エクスポートストレージドメインは非推奨になりました。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イメージ、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。

engine-image-uploader コマンドで、エクスポートストレージドメインを一覧表示し、エクスポートドメインに仮想マシンイメージを OVF または OVA 形式でアップロードして、Red Hat Virtualization Manager で自動認識させることができます。

OVA とは、OVF ファイルの **tar** アーカイブです。

注記

イメージアップローダーは、Red Hat Virtualization によって作成された gzip 圧縮済みの OVF または OVA ファイルのみをサポートしています。

OVF アーカイブには、以下の形式のイメージとマスターディレクトリーが含まれます。

```
|-- images
|    |-- [Image Group UUID]
|         |--- [Image UUID (this is the disk image)]
|         |--- [Image UUID (this is the disk image)].meta
|-- master
|    |---vms
|         |--- [UUID]
|              |--- [UUID].ovf
```

18.3.2. engine-image-uploader コマンドの構文

イメージアップローダーコマンドの基本構文は以下の形式です。

–

```
engine-image-uploader [options] list
engine-image-uploader [options] upload [file].[file]...[file]
```

イメージアップローダーのコマンドは、***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、イメージをアップロードすることができるエクスポートストレージドメインを一覧表示します。
- ***upload*** アクションは、指定したエクスポートストレージドメインにイメージをアップロードします。

イメージアップローダー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-image-uploader コマンドをさらに詳しく指定する複数のパラメーターがあります。これらのパラメーターのデフォルト値は、**/etc/ovirt-engine/imageuploader.conf** ファイルで設定することができます。

一般的なオプション

-h、--help

イメージアップローダーコマンドの使用方法に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の *[PATH]* を設定します。デフォルトは、**etc/ovirt-engine/imageuploader.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の *[PATH]* を設定します。デフォルトは **/var/log/ovirt-engine/ovirt-image-uploader/ovirt-image-uploader-*[date]*.log** です。

--cert-file=[PATH]

engine を検証するための証明書の *[PATH]* を設定します。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。

--quiet

コンソールの出力を最小限に抑える Quiet モードに設定します。

-v、--verbose

より詳しいコンソール出力を表示する詳細モードに設定します。

-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、アップロード先のエクスポート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。

エクスポート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エクスポートドメインを指定します。これらのオプションは、同時に使用することはできません。***-e*** または ***-n*** のいずれかを使用する必要があります。

-e [EXPORT_DOMAIN]*, *--export-domain=[EXPORT_DOMAIN]

ストレージドメイン *EXPORT_DOMAIN* をアップロード先に設定します。

-n [NFSSERVER]*, *--nfs-server=[NFSSERVER]

NFS path *[NFSSERVER]* をアップロード先に設定します。

インポートオプション

以下のオプションを使用すると、イメージをエクスポートドメインにアップロードする際に含まれる、アップロード対象イメージの属性をカスタマイズすることができます。

-i*, *--ovf-id

イメージの UUID が更新されないように指定します。デフォルトでは、コマンドにより、アップロードするイメージの新規 UUID が生成されます。これにより、アップロードされるイメージと、環境内にすでに存在するイメージの間で ID の競合が発生するのを防ぎます。

-d*, *--disk-instance-id

イメージ内の各ディスクの ID の名前が変更されないように指定します。デフォルトでは、コマンドによりアップロードされるイメージ内のディスクの新規 UUID が生成されます。これにより、アップロードされるイメージ上のディスクと、環境内にすでに存在するディスクの間で競合が発生するのを防ぎます。

-m*, *--mac-address

イメージ内のネットワークコンポーネントがイメージから削除されないように指定します。デフォルトでは、コマンドにより、アップロードされるイメージからネットワークカードが削除されます。これにより、環境内にすでに存在する他の仮想マシンのネットワークカードとの競合を防ぎます。このオプションを使用しなかった場合には、管理ポータルを使用して、新たにインポートしたイメージにネットワークインターフェースカードを追加すると、Manager は MAC アドレスで競合が発生しないようにします。

-N [NEW_IMAGE_NAME]*, *--name=[NEW_IMAGE_NAME]

アップロードされるイメージの新しい名前を指定します。

18.3.3. イメージアップローダーと互換性のある OVF アーカイブの作成

概要

engine-image-uploader ツールを使用して、アップロード可能なファイルを作成することができます。

手順18.2 イメージアップローダーと互換性のある OVF アーカイブの作成

1. Manager を使用して、空のエクスポートドメインを作成します。空のエクスポートドメインがあると、仮想マシンがどのディレクトリーに含まれているか簡単に確認することができます。

2. 作成した空のエクスポートドメインに仮想マシンをエクスポートします。

3. エクスポートドメインとして機能するストレージサーバーにログインし、NFS 共有の root を探し、そのマウントポイント下のサブディレクトリーに移動します。新規エクスポートドメインを作成するところから開始したので、エクスポートしたディレクトリーの配下にはディレクトリーが 1 つしかありません。このディレクトリーには、**images/** と **master/** のディレクトリーが含まれています。

4. **tar -zcvf my.ovf images/ master/** コマンドを実行して tar/gzip OVF アーカイブを作成します。

5. 作成した OVF ファイル (上記の例では **my.ovf**) を受け取ると、誰でも **engine-image-uploader** コマンドを使用して Red Hat Virtualization Manager にそのファイルをインポートすることができます。

結果

配布可能な OVF イメージの圧縮ファイルを作成しました。このファイルを受け取ると、誰でも **engine-image-uploader** を使用して、イメージを Red Hat Virtualization 環境にアップロードすることができます。

18.3.4. engine-image-uploader の基本的な使用例

以下は、engine アップローダーコマンドを使用してエクスポートストレージドメインを一覧表示する方法の例です。

例18.1 イメージアップローダーを使用したエクスポートストレージドメインの一覧表示

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

以下は、Open Virtualization Format (OVF) ファイルをアップロードする方法の例です。

例18.2 イメージアップローダーを使用したファイルのアップロード

```
# engine-image-uploader -e myexportdom upload myrhel6.ovf
Please provide the REST API password for the admin@internal oVirt Engine
user (CTRL+D to abort):
```

18.4. USB FILTER EDITOR

18.4.1. 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 の以下の場所に保管されます。

/etc/ovirt-engine/usbfilter.txt

USB フィルターポリシーへの変更は、次回に Red Hat Virtualization Manager サーバー上で **ovirt-engine** サービスが再起動されるまでは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。

手順18.3 USB Filter Editor のインストール

1. Windows マシンで、コンテンツ配信ネットワークから取得した **USBFilterEditor.msi** インストーラーを起動します。

2. インストールウィザードの手順に従ってインストールを行います。USB Filter Editor のインスト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 (http://winscp.net) です。

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。

18.4.2. 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。

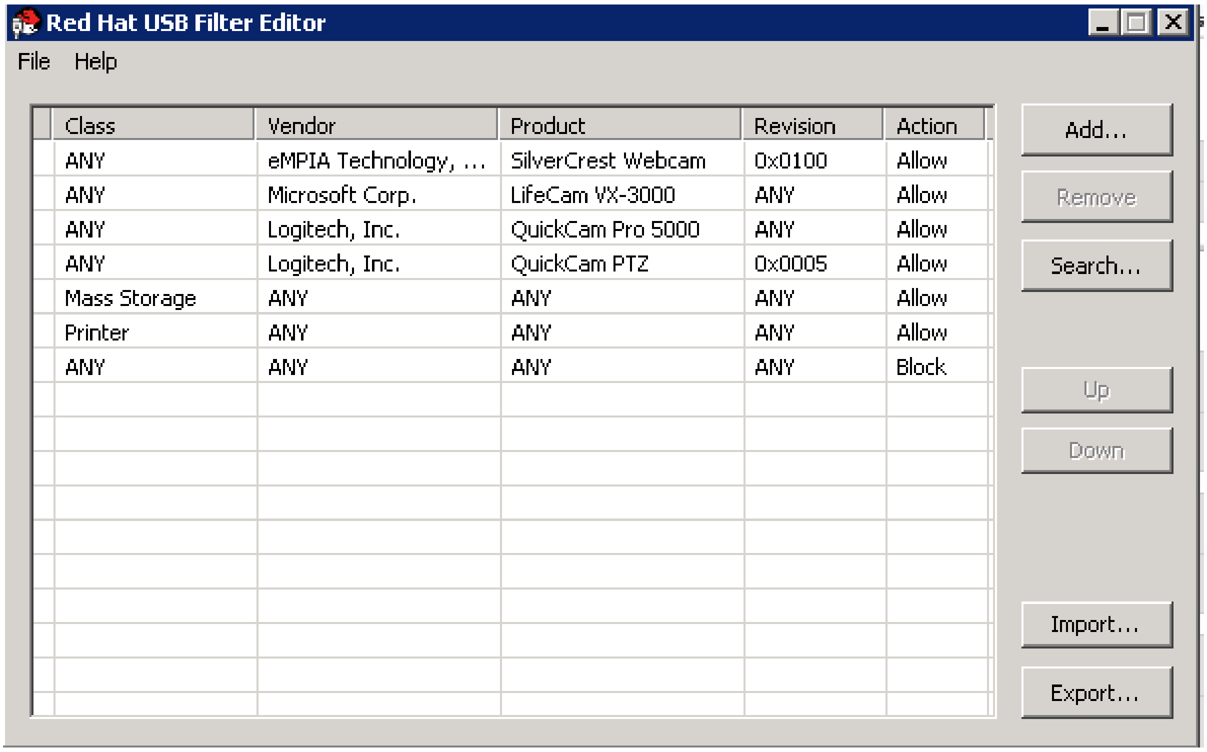


図18.1 Red Hat USB Filter Editor

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 デバイスが **Allow** に、許可されていないデバイスが **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、大容量記憶域コントローラー)
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、ルールの順序を上下に移動させて並べ替えることができます。ユニバーサルの **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。

18.4.3. USB ポリシーの追加

概要

USB Filter Editor に USB ポリシーを追加します。

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。

手順18.4 USB ポリシーの追加

1. **Add** ボタンをクリックします。**Edit USB Criteria** ウィンドウが開きます。

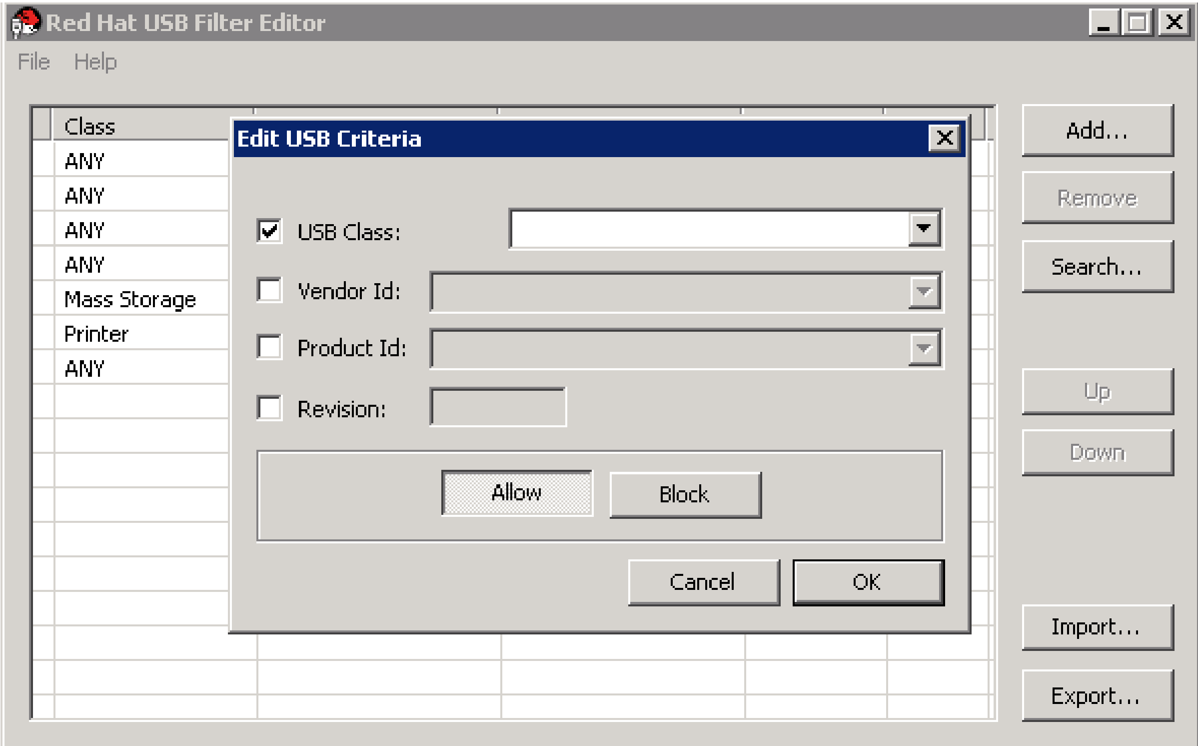


図18.2 USB Criteria の編集

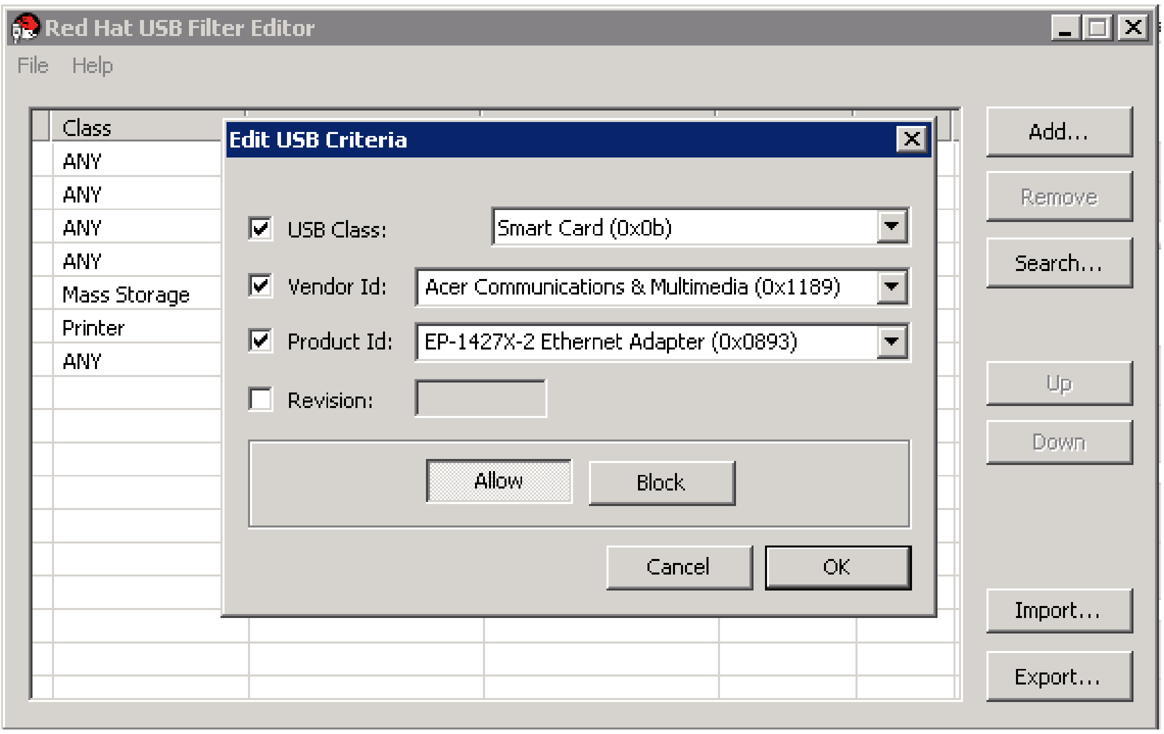
2. **USB Class**、**Vendor ID**、**Product ID**、および **Revision** のチェックボックスと一覧を使用して、デバイスを指定します。

   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18.3 デバイスの追加

   以下は、USB Class **Smartcard**、**Acer Communications & Multimedia** 社製造のデバイス **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。

結果

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。

18.4.4. USB ポリシーの削除

概要

USB Filter Editor から USB ポリシーを削除します。

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。

手順18.5 USB ポリシーの削除

1. 削除するポリシーを選択します。

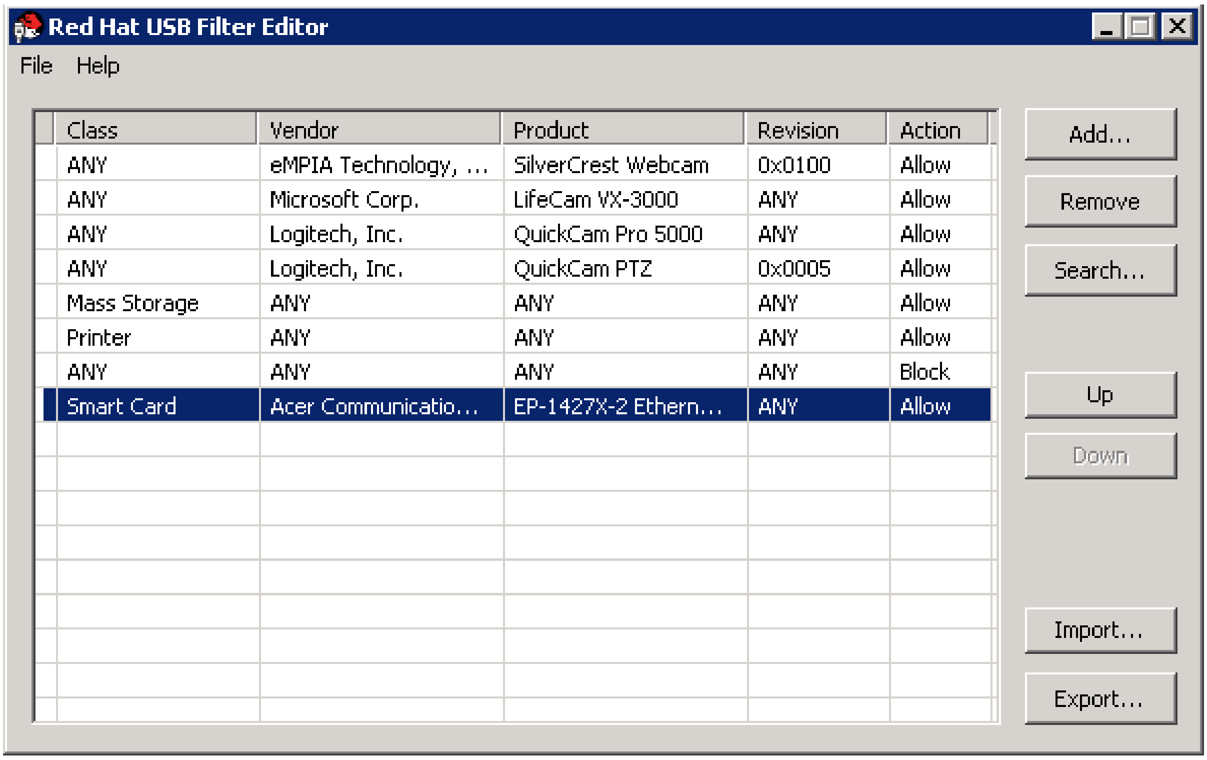


図18.3 USB ポリシーの選択

2. **Remove** ボタンをクリックします。メッセージが表示され、ポリシーの削除を確認します。

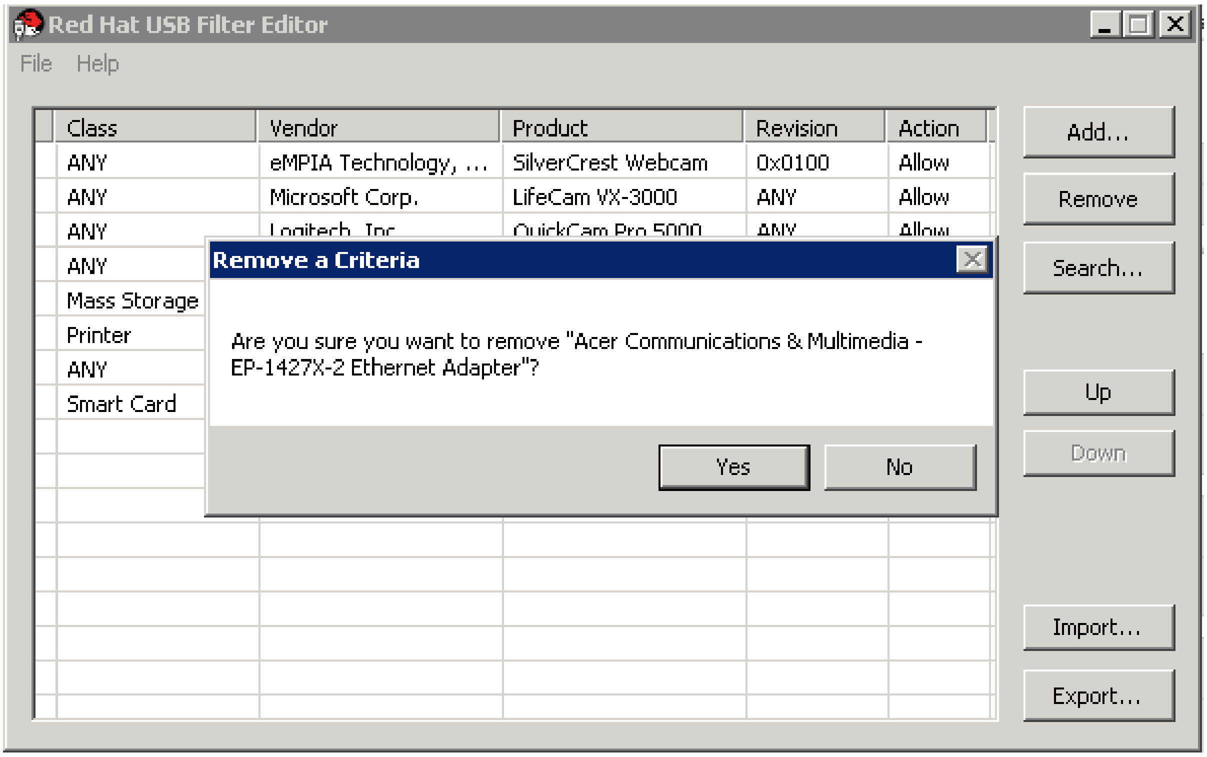


図18.4 USB Criteria の編集

3. **Yes** ボタンをクリックして、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。

結果

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。

18.4.5. USB デバイスポリシーの検索

概要

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。

手順18.6 USB デバイスポリシーの検索

1. **Search** ボタンをクリックします。**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。

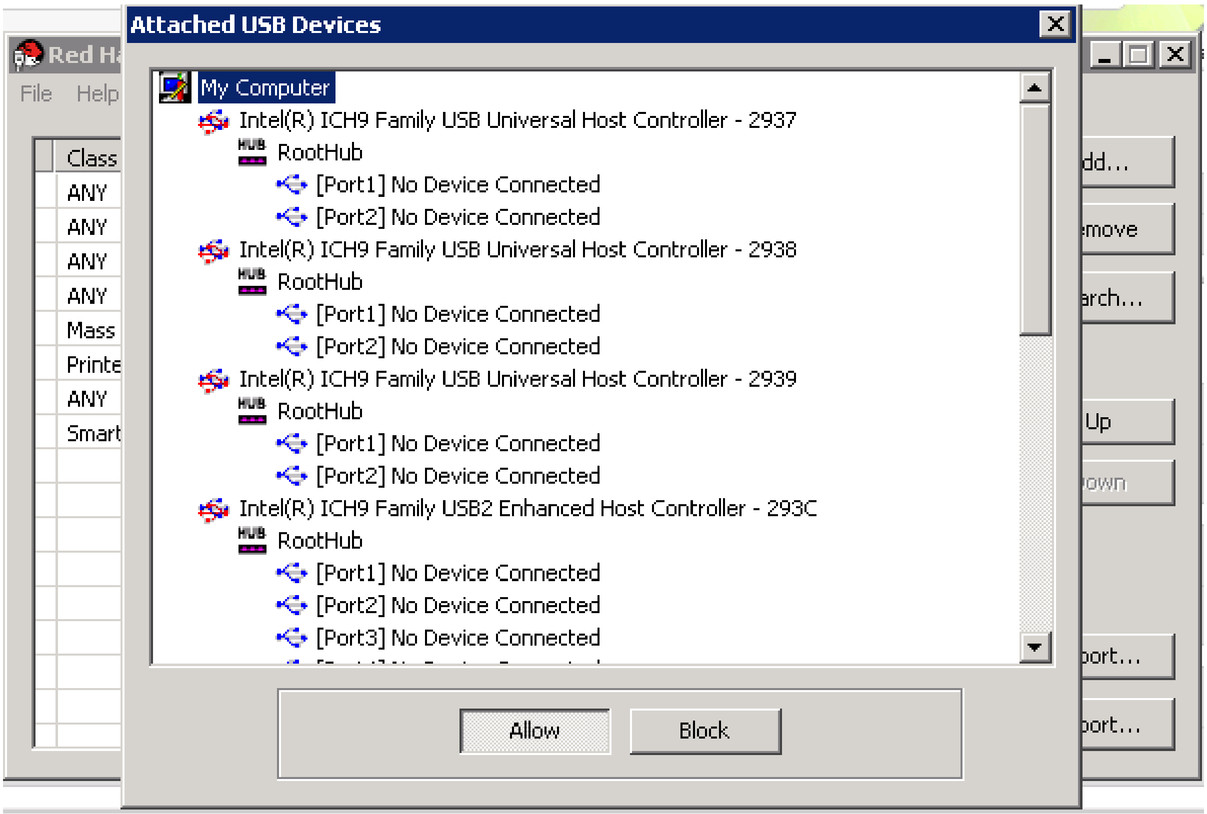


図18.5 アタッチされた USB デバイス

2. デバイスを選択し、必要に応じて **Allow** または **Block** のボタンをクリックします。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。

結果

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。

18.4.6. USB ポリシーのエクスポート

概要

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。

手順18.7 USB ポリシーのエクスポート

1. **Export** をクリックすると、**Save As** ウィンドウが開きます。
2. **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 を実行するサーバーに **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以下のディレクトリーに配置する必要があります。

   /etc/ovirt-engine/

4. Red Hat Virtualization Manager を稼働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。

```
# service ovirt-engine restart
```

結果

Red Hat Virtualization 環境内で実行されている仮想マシンに USB デバイスポリシーが実装されました。

18.4.7. USB ポリシーのインポート

概要

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。

手順18.8 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 を実行するサーバーに **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以下のディレクトリーに配置する必要があります。

   /etc/ovirt-engine/

2. デスクトップ上の 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。

結果

USB デバイスポリシーを USB Filter Editor で編集することができるようになりました。

18.5. ログ収集ツール

18.5.1. 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** の有効なコマンド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. 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
: *PATH* には、ツールが使用する設定ファイルを指定します。

--local-tmp=PATH
: *PATH* には、ログを保存するディレクトリーを指定します。デフォルトのディレクトリーは **/tmp/logcollector** です。

--ticket-number=TICKET

TICKET には、SOS レポートに関連付けるチケットまたはケース番号を指定します。

--upload=FTP_SERVER

FTP_SERVER には、FTP を使用して送信される取得済みログの送信先を指定します。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

PATH には、このコマンドがログ出力に使用するファイル名を指定します。

--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。

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** ホストのみに制限します。

--no-hypervisors

ログ収集から仮想化ホストを除外します。

-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 が認識している必要があります。

-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。

SOS レポートのオプション

ログコレクターは JBoss SOS プラグインを使用します。以下のオプションを使用して、JMX コンソールからのデータ収集をアクティブ化します。

--jboss-home=JBOSS_HOME

JBoss インストールのディレクトリーパス。デフォルトは **/var/lib/jbossas** です。

--java-home=JAVA_HOME

Java インストールのディレクトリーパス。デフォルトは **/usr/lib/jvm/java** です。

--jboss-profile=JBOSS_PROFILE

サーバープロファイルを、引用符で囲まれたスペース区切りの一覧で表示します。これにより、ログ収集が特定のプロファイルに限定されます。デフォルトは ***rhevm-slimmed*** です。

--enable-jmx

Red Hat Virtualization の JBoss JMX インターフェースからのランタイムメトリックの収集を有効にします。

--jboss-user=JBOSS_USER

JBoss JMX を呼び出すパーミッションを持つユーザー。デフォルトは ***admin*** です。

--jboss-logsize=LOG_SIZE

取得したログファイルの最大サイズ (MB 単位)

--jboss-stdjar=STATE

JBoss 標準 JAR の JAR 統計の収集を指定します。*STATE* の箇所は **on** または **off** に置き換えます。デフォルトは **on** です。

--jboss-servjar=STATE

任意のサーバー設定ディレクトリーからの JAR 統計収集を設定します。*STATE* の箇所は **on** または **off** に置き換えます。デフォルトは **on** です。

--jboss-twiddle=STATE

Twiddle データの収集を on または off に設定します。Twiddle は JMX の呼び出し元からデータを収集するために使用する JBoss のツールです。*STATE* の箇所は **on** または **off** に置き換えます。デフォルトは **on** です。

--jboss-appxml=XML_LIST

XML 記述を取得するアプリケーションを、引用符で囲まれたスペース区切りの一覧で表示します。デフォルトは **all** です。

SSH の設定

--ssh-port=PORT

PORT には、仮想化ホストとの SSH 接続に使用するポートを指定します。

-k KEYFILE*、*--key-file=KEYFILE

KEYFILE には、仮想化ホストへのアクセスに使用する SSH 公開鍵を指定します。

--max-connections=MAX_CONNECTIONS

MAX_CONNECTIONS には、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

USER には、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設定します。デフォルトは **postgres** です。

--pg-dbname=DBNAME

DBNAME には、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指定します。デフォルトは **rhevm** です。

--pg-dbhost=DBHOST

DBHOST には、データベースサーバーのホスト名を指定します。デフォルトは **localhost** です。

--pg-host-key=KEYFILE

KEYFILE には、データベースサーバーの公開 ID ファイル (秘密鍵) を指定します。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。

18.5.3. 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18.4 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
```

18.6. ISO アップローダーツール

18.6.1. ISO アップローダーツール

ISO アップローダーは、ISO イメージを ISO ストレージドメインにアップロードするためのツールです。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。このコマンドを実行するには、必ず **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*** の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。

18.6.2. 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、複数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の *[PATH]* を設定します。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の *[PATH]* を設定します。デフォルトは **/var/log/ovirt-engine/ovirt-iso-uploader/ovirt-iso-uploader*[date]*.log** です。

--cert-file=[PATH]

engine を検証するための証明書の *[PATH]* を設定します。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

コンソールの出力を最小限に抑える Quiet モードに設定します。

-v**、*****--verbose***

より詳しいコンソール出力を表示する詳細モードに設定します。

-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]

ストレージドメイン *[ISODOMAIN]* には、アップロード先を指定します。

-n, --nfs-server=[NFSSERVER]

NFS パス *[NFSSERVER]* には、アップロード先を指定します。

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]

[USER] には、アップロード時に使用する SSH ユーザー名を指定します。デフォルトは **root** です。

--ssh-port=[PORT]

[PORT] には、SSH 接続時に使用するポートを指定します。

-k [KEYFILE], --key-file=[KEYFILE]

[KEYFILE] には、SSH 認証に使用する公開鍵を指定します。鍵が指定されていない場合は、***--ssh-user=[USER]*** で指定したユーザーのパスワード入力が求められます。

18.6.3. NSF サーバーの指定

例18.5 NFS サーバーへのアップロード

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

18.6.4. 基本的な ISO アップローダーの使用法

以下は、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18.6 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):
```

18.6.5. VirtIO およびゲストツールのイメージファイルの ISO ストレージドメインへのアップロード

以下の例は、**virtio-win.iso**、**virtio-win_x86.vfd**、**virtio-win_amd64.vfd**、**rhev-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18.7 VirtIO およびゲストツールのイメージファイルのアップロード

```
# engine-iso-uploader --iso-domain=[ISODomain] upload
/usr/share/virtio-win/virtio-win.iso /usr/share/virtio-win/virtio-
win_x86.vfd /usr/share/virtio-win/virtio-win_amd64.vfd /usr/share/rhev-
guest-tools-iso/rhev-tools-setup.iso
```

18.6.6. VirtIO およびゲストツールのイメージファイル

Windows 仮想マシン用の 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 rhev-tools-setup ISO は、ドメインのインストールおよび設定時に ISO ストレージドメインにコピーされます。

これらのイメージファイル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ーを向上させることができます。最新の virtio-win と rhev-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/rhev-guest-tools-iso/rhev-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。

パート IV. 環境に関する情報の収集

第19章 ログファイル

19.1. RED HAT VIRTUALIZATION MANAGER 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
/var/log/ovirt-engine/engine-cleanup_*yyyy_mm_dd_hh_mm_ss*.log	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。
/var/log/ovirt-engine/engine-db-install-*yyyy_mm_dd_hh_mm_ss*.log	**engine-setup** コマンドからのログ。**rhevm** データベースの作成、設定が詳しく記録されます。
/var/log/ovirt-engine/ovirt-engine-dwh-setup-*yyyy_mm_dd_hh_mm_ss*.log	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。
/var/log/ovirt-engine/setup/ovirt-engine-setup-*yyyymmddhhmmss*.log	**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ー

ログファイル	説明
/var/log/ovirt-engine/engine.log	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
/var/log/ovirt-engine/host-deploy	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
/var/lib/ovirt-engine/setup-history.txt	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

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	/var/log/libvirt/qemu/(guest_name).log	ゲストを起動する前に、ホスト/ハイパーバイザーで **export SPICE_DEBUG_LEVEL=5** のコマンドを実行します。

19.3.2. ゲストマシンのSPICE ログ

表19.4 ゲストマシンのSPICE ログ

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	/var/log/spice-vdagent.log	**/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。

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. ログを表示するには、**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、**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. **debug-helper.exe** ファイルをダウンロードして、**remote-viewer.exe** ファイルと同じディレクトリー(例: **C:\Users*[user name]*\AppData\Local\virt-viewer\bin**) に移動します。

2. **debug-helper.exe** ファイルを実行して、GNU Debugger (GDB) をインストールします。

3. **debug-helper.exe** ファイルを実行して、SPICE デバッグを有効にします。

```
debug-helper.exe remote-viewer.exe --spice-controller
```

4. 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. RED HAT VIRTUALIZATION ホストのログファイル

表19.5

ログファイル	説明
/var/log/vdsm/libvirt.log	**libvirt** のログファイル
/var/log/vdsm/spm-lock.log	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。
/var/log/vdsm/vdsm.log	仮想化ホスト上の Manager のエージェントである VDSM のログファイル
/tmp/ovirt-host-deploy-*@DATE@*.log	ホスト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、/var/log/ovirt-engine/host-deploy/ovirt-*@DATE@*-*@HOST@*-*@CORRELATION_ID@*.log として engine にコピーされます。

19.5. 仮想化ホストのロギングサーバーの設定

ホストは、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。

手順19.1 仮想化ホストのロギングサーバー設定

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。

   ```
   # service rsyslog restart
   ```

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 プロキシー

20.1. SPICE プロキシー

20.1.1. SPICE プロキシーの概要

SPICE プロキシーは、SPICE クライアントがハイパーバイザーを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 プロキシーを設定するには、マシンに **Squid** をインストールして、プロキシートラフィックがファイアウォールを通過できるようにするための **iptables** 設定を行います。SPICE プロキシーを有効にするには、Manager で **engine-config** を使用して `SpiceProxyDefault` のキーをプロキシーの名前とポートで構成される値に設定します。SPICE プロキシーをオフにするには、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 プロキシーは、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、SPICE HTML5 または 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 プロキシーのマシン設定

以下の手順では、SPICE プロキシーとしてマシンを設定する方法について説明します。SPICE プロキシーにより、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、プロキシーサービスに **Squid** を使用します。

手順20.1 Red Hat Enterprise Linux への Squid のインストール

1. プロキシーマシンに **Squid** をインストールします。

```
# yum install squid
```

2. `/etc/squid/squid.conf` を開いて、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. プロキシーを起動します。

```
# service squid start
```

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 プロキシー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 プロキシーを有効にしてください。

20.1.3. SPICE プロキシーの有効化

以下の手順では、SPICE プロキシーを有効 (オン) にする方法を説明します。

手順20.2 SPICE プロキシーの有効化

1. Manager で engine-config ツールを使用してプロキシーを設定します。

   ```
   # engine-config -s SpiceProxyDefault=someProxy
   ```

2. **ovirt-engine** サービスを再起動します。

   ```
   # service ovirt-engine restart
   ```

   プロキシーは以下の形式を使用するようにします。

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

   注記

   HTTPS プロキシー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。これらのバージョンよりも古いクライアントは、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ー設定を無視して、ホストに直接接続を試みます。

SPICE プロキシーが有効 (オン) になりました。SPICE プロキシーを使用して Red Hat Virtualization 環境に接続することができます。

20.1.4. SPICE プロキシーの無効化

以下の手順では、SPICE プロキシーを無効 (オフ) にする方法を説明します。

手順20.3 SPICE プロキシーの無効化

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 プロキシーを削除します。

   ```
   # engine-config -s SpiceProxyDefault=""
   ```

3. Manager を再起動します。

```
# service ovirt-engine restart
```

SPICE プロキシーが無効 (オフ) になりました。SPICE プロキシーを使用しても Red Hat Virtualization 環境に接続できなくなりました。

20.2. SQUID プロキシー

20.2.1. Squid プロキシーのインストールと設定

概要

本セクションでは、ユーザーポータルへの Squid プロキシーのインストールと設定方法を説明します。Squid プロキシーサーバーは、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。

手順20.4 Squid プロキシーの設定

1. Squid プロキシーの 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。プロキシー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. プロキシーのホスト名を選択し、次にプロキシー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、プロキシーの証明書の完全な識別名を作成します。

   ```
   /C=US/O=Example Inc./CN=proxy.example.com
   ```

3. プロキシーマシンにログインして、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、プロキシー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、特別な保護は必要ありません。

4. 署名済みの証明書を生成するには、プロキシーのマシンから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/.
```

5. 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。

6. 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** という名前がついているはずです。プロキシーマシンで、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 .
```

7. **proxy.key** と **proxy.cer** の両ファイルがプロキシー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
```

8. プロキシーマシンに Squid プロキシーサーバーパッケージをインストールします。

```
# yum install squid
```

9. 秘密鍵と署名済みの証明書をプロキシーがアクセスできる場所 (例: **/etc/squid** ディレクトリー) に移動します。

```
# cp proxy.key proxy.cer /etc/squid/.
```

10. **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.*
```

11. Squid プロキシーは 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ー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** ユーザーがこれら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 プロキシーサーバーを再起動します。

    ```
    # service squid restart
    ```

16. 以下のような完全な URL でユーザーポータルに接続します。

    ```
    https://proxy.example.com/UserPortal/org.ovirt.engine.ui.userportal.
    UserPortal/UserPortal.html
    ```

    注記

    https://*proxy.example.com*/UserPortal などの短縮 URL は機能しません。このような短縮 URL は、302 レスポンスコードとロケーションヘッダーを使用して、アプリケーションサーバーによって長い URL にリダイレクトされます。Red Hat Enterprise Linux および Fedora の **Squid** は、これらのヘッダーの書き換えはサポートしていません。

注記

デフォルトでは、Squid プロキシーはアイドル状態が 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 プロキシー

20.3.1. Websocket プロキシーの概要

websocket プロキシーにより、ユーザーは、 noVNC および SPICE HTML5 コンソールを介して仮想マシンに接続することができるようになります。以前は、websocket プロキシーは Red Hat Virtualization Manager マシンでしか実行できませんでしたが、現在このプロキシーは、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 プロキシーは、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』「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 プロキシーのインストール」のセクションを参照してください)。

websocket プロキシーは 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 プロキシーの移行」を参照してください。

注記

SPICE HTML5 のサポートはテクノロジープレビュー機能です。テクノロジープレビュー機能は、Red Hat サービスレベルアグリーメント (SLA) では完全にサポートされていません。これらは、機能的に完全でない可能性があり、実稼働環境での使用を目的とはしていませんが、近々発表予定のプロダクトイノベーションをリリースに先駆けてご提供することにより、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。

20.3.2. 別のマシンへの Websocket プロキシーの移行

セキュリティー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 プロキシー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 プロキシーを移行する手順では、Manager のマシンから Websocket プロキシーの設定を削除してから、別のマシンにプロキシーをインストールする必要があります。

Manager マシンから websocket プロキシーを削除するには、**engine-cleanup** コマンドを使用することができます。

手順20.5 別のマシンへの Websocket プロキシーの移行

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. websocke 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ー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 プロキシーのインストール」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ー** 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ー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

名前	説明
after_nic_hotunplug	NIC が仮想マシンからホットアンプラグされた後
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ーをサポートするデバイスを作成する前
after_device_create	カスタムプロパティーをサポートするデバイスを作成した後
before_update_device	カスタムプロパティーをサポートするデバイスを更新する前
after_update_device	カスタムプロパティーをサポートするデバイスを更新した後
before_device_destroy	カスタムプロパティーをサポートするデバイスを破棄する前
after_device_destroy	カスタムプロパティーをサポートするデバイスを破棄した後
before_device_migrate_destination	デバイスの移行の前に、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

名前	説明
after_device_migrate_source	デバイスの移行の後に、移行元のホストで実行

A.5. VDSM フックの環境

大半のフックスクリプトは、**vdsm** ユーザーとして実行され、VDSM プロセスの環境を継承します。例外となるのは、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 ドメイン内の対象の仮想マシンの XML 表現へのパスが含まれます。このルールでは、以下のようなフックが例外となります。
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、http://libvirt.org/formatdomain.html 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 **vmId** としても提供されます。

A.7. カスタムプロパティーの定義

Red Hat Virtualization Manager によって受け入れられ、カスタムフックに渡されるカスタムプロパティーは、**engine-config** コマンドを使用して定義します。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ー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ー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ーは、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ー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には、**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*** は既に定義済みです。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。

   ```
   # service ovirt-engine restart
   ```

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ーは、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** サブプロパティーの値は 0 から 99999 までの範囲に設定し、**duplex** サブプロパティーの値には **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ー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。

```
# service ovirt-engine restart
```

A.8. 仮想マシンのカスタムプロパティーの設定

Red Hat Virtualization Manager でカスタムプロパティーを定義した後には、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ーは、管理ポータルの **新規仮想マシン** および **仮想マシンの編集** ウィンドウの **カスタムプロパティー** 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ー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ーは、その仮想マシンが次回シャットダウンされるまでの間のみに適用されます。

カスタムプロパティー タブは、定義済みのカスタムプロパティー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ーキーを選択すると追加のフィールドが表示され、そのキーの値を入力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ーの評価

仮想マシンの **カスタムプロパティー** 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ー** 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する必要があります。

例A.3 カスタムプロパティーの編集

以下の例は、カスタムプロパティー ***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ー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ー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込み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られます。
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、**vdsm** 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

この例では、**vdsm** 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。

```
vdsm ALL=(ALL) NOPASSWD: /bin/chown
```

これは、**vdsm** 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定されます。

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ー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
multicast_query_interval	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 multicast_query_interval 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 multicast_query_interval 内に送信されている場合には、再送信されません。
multicast_query_response_interval	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)。multicast_query_interval の値以下である必要があります。
multicast_router	マルチキャストルーター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。
multicast_snooping	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。
multicast_startup_query_count	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。
multicast_startup_query_interval	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の ethtool 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。

手順B.1 Manager への ethtool_opts キーの追加

1. Manager で以下のコマンドを実行し、キーを追加します。

   ```
   # engine-config -s
   UserDefinedNetworkCustomProperties=ethtool_opts=.* --cver=3.6
   ```

2. **`ovirt-engine`** サービスを再起動します。

   ```
   # service ovirt-engine restart
   ```

3. Ethtool のプロパティーを設定するホストに VDSM フックパッケージをインストールします。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 vdsm-hook-ethtool-options
   ```

ethtool_opts キーが管理ポータルで利用できるようになりました。ethtool プロパティーを論理ネットワークに適用する方法については、「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。

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。

1. プラグインの検出
2. プラグインの読み込み
3. プラグイン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-plugins** 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ものと想定されていますが、プラグイン記述子には JSON 形式の仕様に加えて、Java/C++ 形式のコメント (/* と // の両変数) 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-plugins** に保管されており、デフォルトのマッピングは oVirt Engine のローカル設定ファイルで定義されている **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ものと想定されます。

注記

プラグインユーザー設定ファイルは、通常、以下の **<descriptorFileName>-config.json** 命名規則にしたがいます。

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の 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。

手順C.1 プラグインブートストラップシーケンス

1. 指定されたプラグインの pluginApi インスタンスの取得
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)	**/usr/share/ovirt-engine/ui-plugins/my-plugin.json**	
プラグインのユーザー設定ファイル	**/etc/ovirt-engine/ui-plugins/my-plugin-config.json**	
プラグインのリソースファイル	**/usr/share/ovirt-enging/ui-plugins/<resourcePath>/PluginHostPage.html**	**<resourcePath>** 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。

手順C.2 Hello World! プラグインのデプロイ

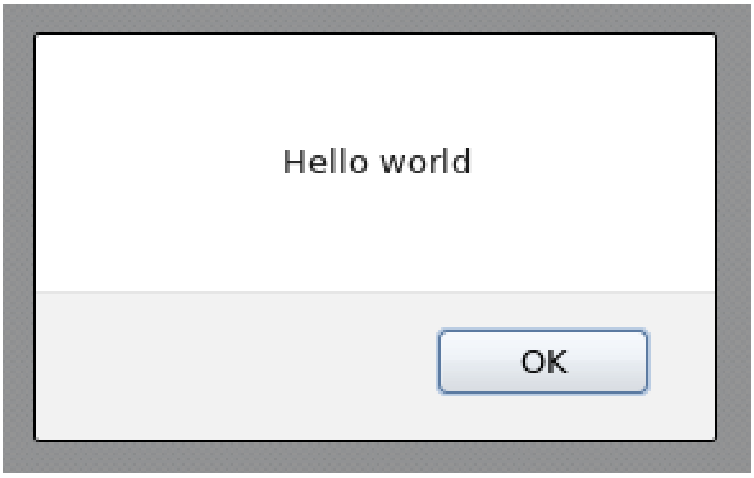
1. Manager の **/usr/share/ovirt-engine/ui-plugins/helloWorld.json** に以下のファイルを作成して、プラグイン記述子を作成します。

```
{
    "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。



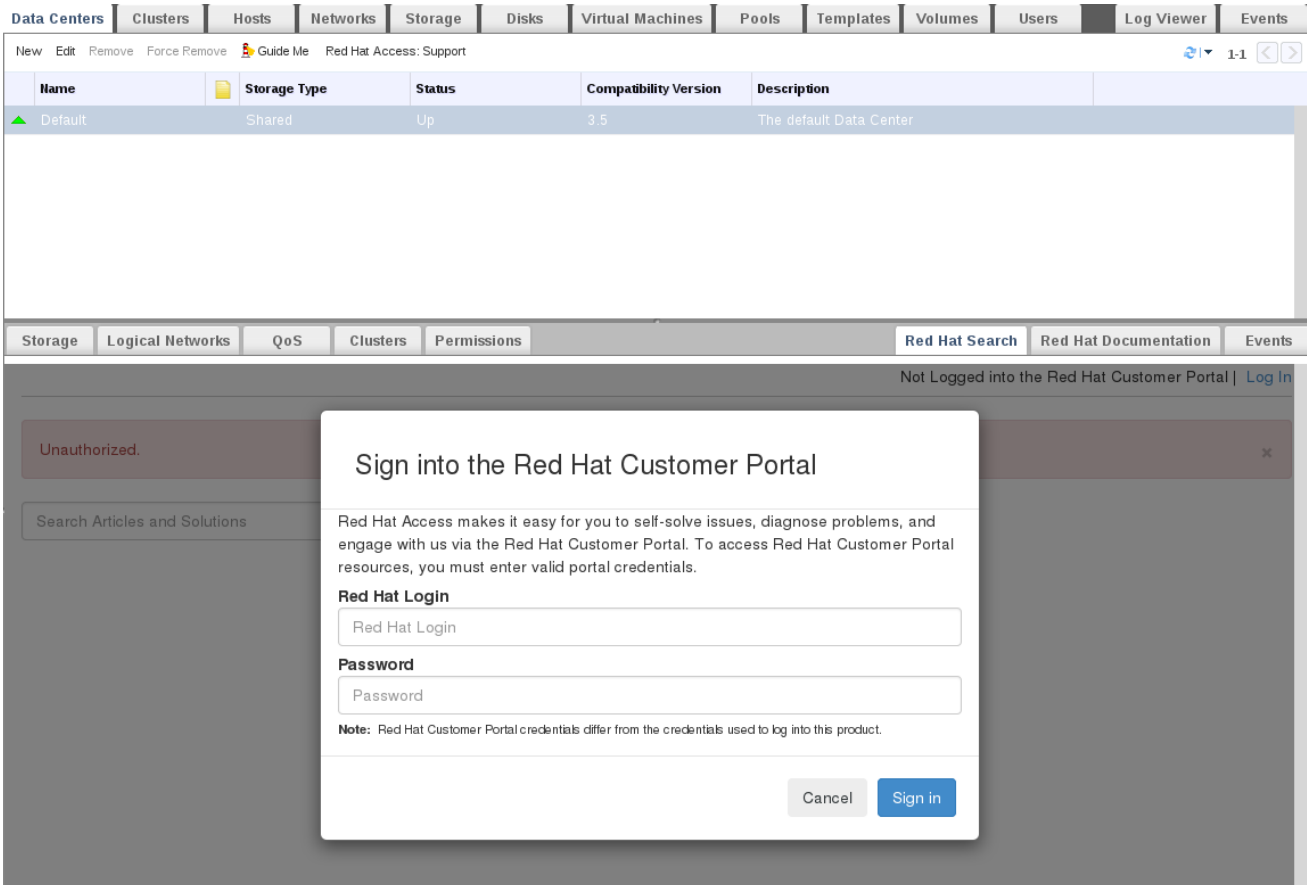
図C.1 Hello World! プラグインの実装完了

C.5. RED HAT SUPPORT プラグインの使用

Red Hat Access プラグインにより、Red Hat Virtualization 管理ポータルから Red Hat Access サービスを利用することができます。Red Hat のログイン認証情報を使用してログインする必要があります。Red Hat Access プラグインにより、ユーザーのログイン状態が検出され、ログインしていない場合には、ログインウィンドウが開きます。

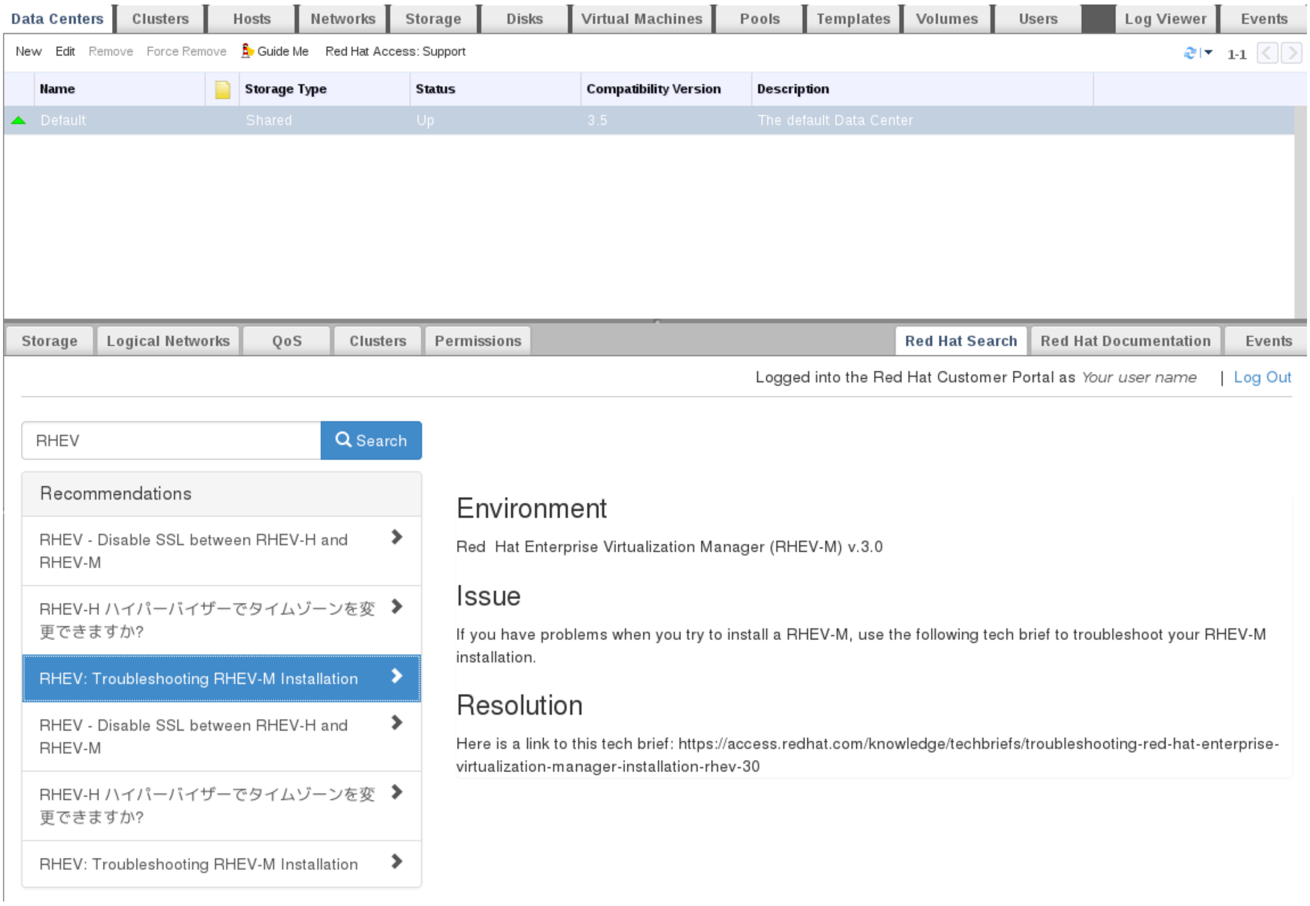
注記

Red Hat Virtualization 管理ポータルの認証情報は、ユーザーの Red Hat ログインとは同じではありません。



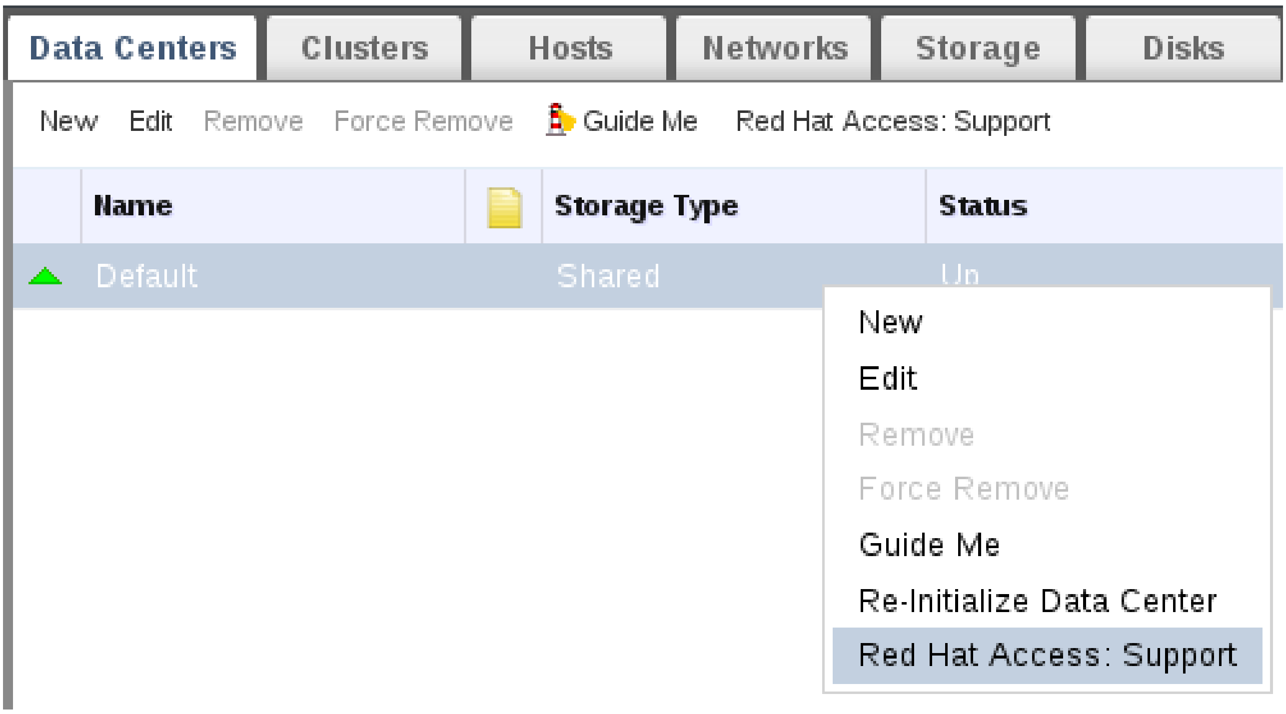
図C.2 Red Hat Support プラグイン - ログインウィンドウ

ログインすると、Red Hat カスタマーポータルにアクセスできるようになります。Red Hat Support プラグインは、Red Hat Virtualization 管理ポータルの詳細ペインまたは一部のコンテキストメニューで利用することができます。Red Hat Access のデータベースを検索するには、検索バーを使用します。検索結果は、詳細ペインの左側にあるナビゲーションリストに表示されます。



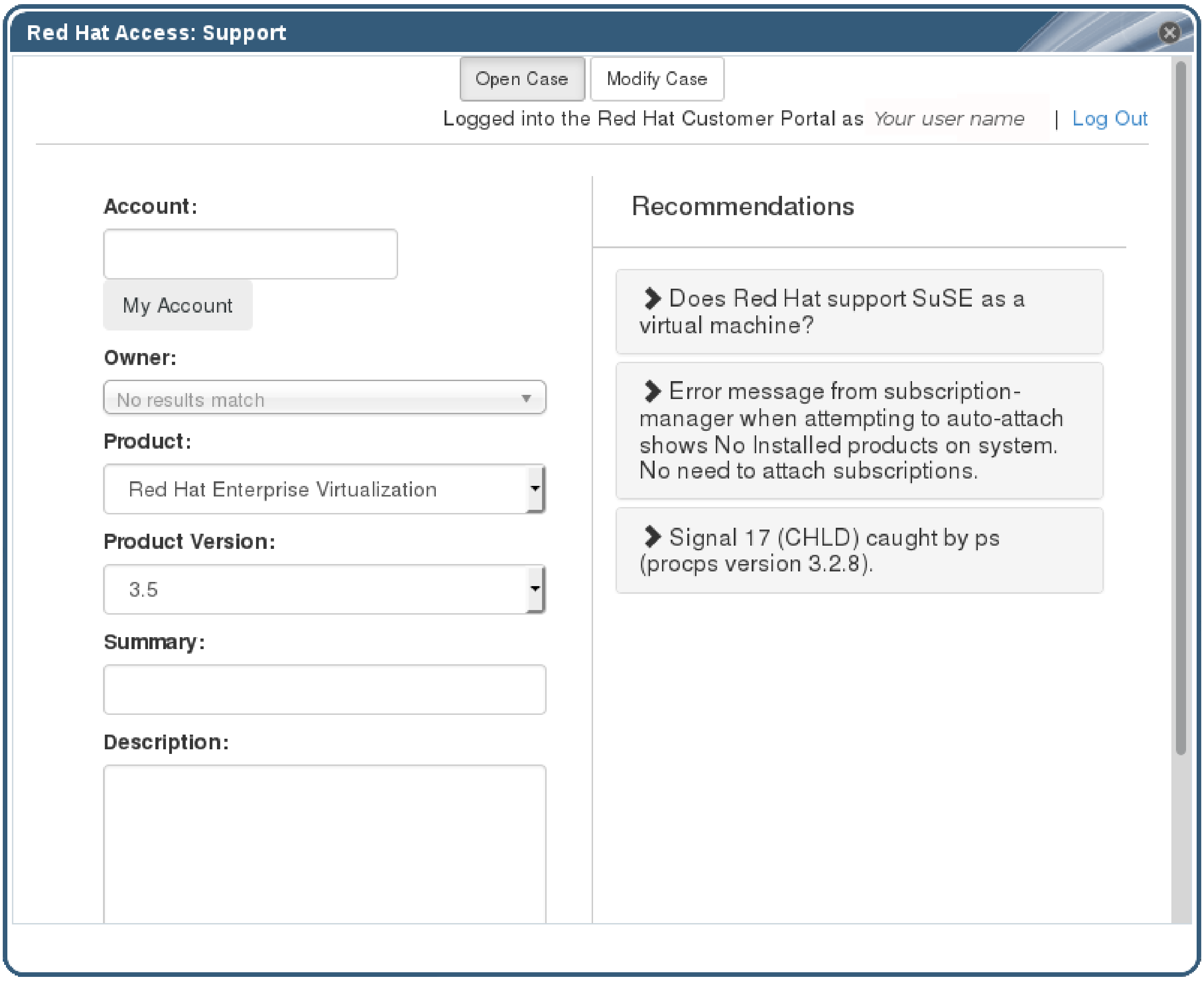
図C.3 Red Hat Support プラグイン - 左側のナビゲーションリストに表示される検索結果

Red Hat Virtualization 管理ポータルのコンテキストメニューを右クリックして Red Hat Support プラグインにアクセスします。



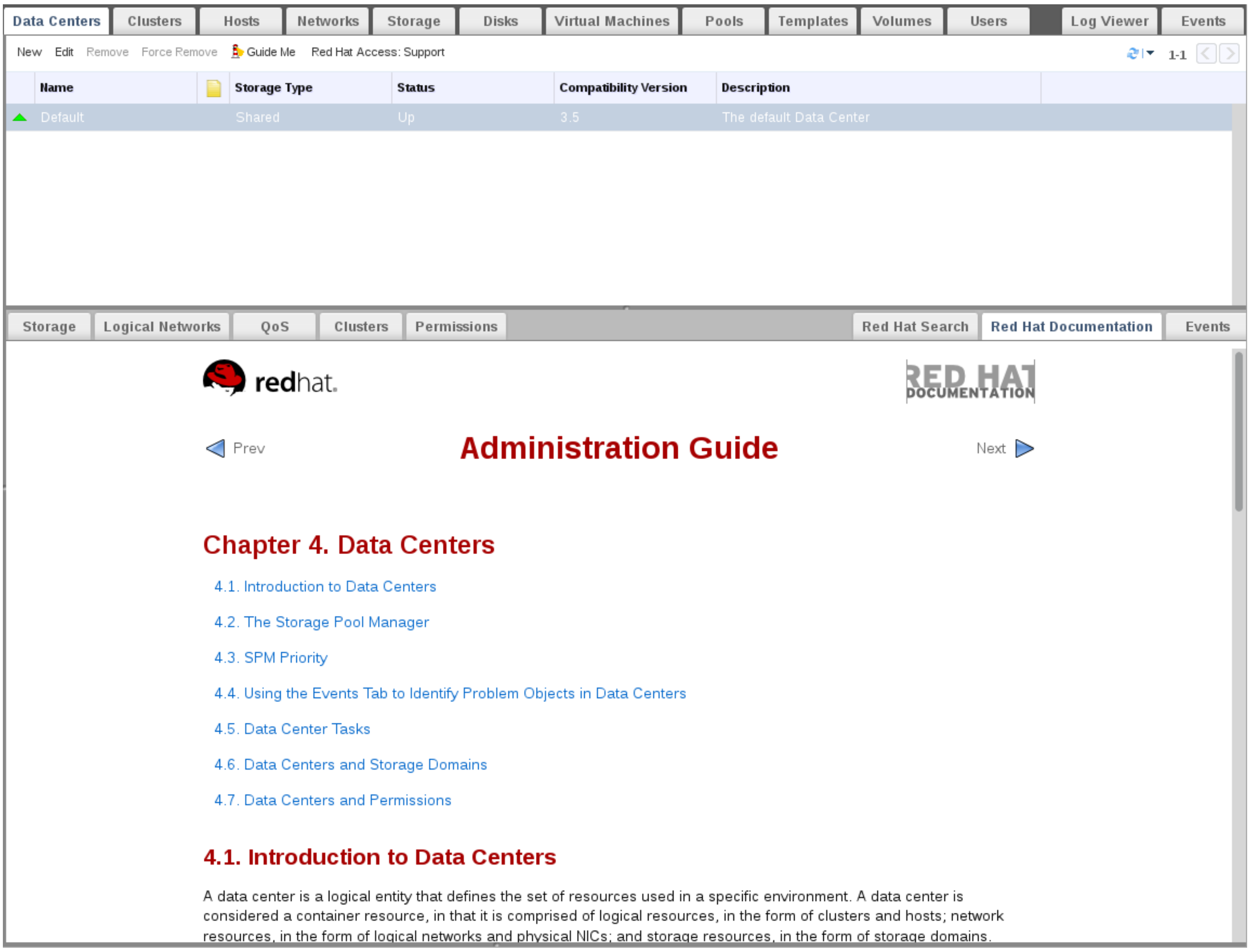
図C.4 コンテキストメニューの右クリックによる Red Hat Support プラグインへのアクセス

新規サポートケースを開く場合は **`Open New Support Case`** のボタンを、既存のケースを変更する場合は **`Modify Existing Case`** のボタンを選択します。



図C.5 Red Hat Support プラグイン - 新規サポートケースの作成

`Red Hat Documentation` タブを選択すると、現在管理ポータルの画面で表示されている箇所に関連したドキュメントが開きます。



図C.6 Red Hat Support プラグイン - ドキュメントへのアクセス

付録D RED HAT VIRTUALIZATION と SSL

D.1. RED HAT VIRTUALIZATION MANAGER の SSL 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。

自分の組織の商用署名入り証明書を使用し、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します。

注記

商用に発行された https 接続用の証明書を使用しても、Manager とホスト間の認証に使用している証明書には影響を及ぼすことなく、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。

要件

この手順には、商用証明書の発行機関から取得した PEM 形式の証明書、**.nokey** ファイル、および **.cer** ファイルが必要です。**.nokey** ファイルおよび **.cer** ファイルは、証明書と鍵のバンドルとして、P12 形式で配布されている場合があります。

本手順は、**P12** 形式の証明書/鍵バンドルがあることを前提としています。

手順D.1 Red Hat Virtualization Manager Apache SSL 証明書の置き換え

1. Manager は、**/etc/pki/ovirt-engine/ca.pem** にシンボリックリンクされた **/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
```

2. 商用に発行された証明書を **/etc/pki/ovirt-engine/apache-ca.pem** として保存します。証明書チェーンは、ルート証明書まで完了する必要があります。チェーンの順序は重要で、最新の中間証明書、ルート証明書の順にする必要があります。

```
mv YOUR-3RD-PARTY-CERT.pem /etc/pki/ovirt-engine/apache-ca.pem
```

3. **P12** バンドルを **/etc/pki/ovirt-engine/keys/apache.p12** に移動します。

4. バンドルから鍵を抽出します。

```
# openssl pkcs12 -in  /etc/pki/ovirt-engine/keys/apache.p12 -nocerts
-nodes > /etc/pki/ovirt-engine/keys/apache.key.nopass
```

5. バンドルから証明書を抽出します。

```
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nokeys >
/etc/pki/ovirt-engine/certs/apache.cer
```

6. Apache サーバーを再起動します。

```
# service httpd restart
```

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、ポータルに接続できるようになりました。

重要

証明書を置き換えると、https://access.redhat.com/solutions/458713 に記載されているように、ログコレクターでエラーが発生する場合があります。このようなエラーを回避するには、ログコレクターの設定を以下のように編集してください。

1. CA サーバーから CA 証明書をエクスポートして、Red Hat Virtualization Manager サーバーにコピーします。
2. **/etc/ovirt-engine/logcollector.conf** に以下の行を追加して、ログコレクターを新規ロケーションにポイントします。

```
cert-file=/path/to/new/CA/file
```

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 エンコードされたファイルの作成および証明書の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*** で README ファイルの「**X.509 CERTIFICATE TRUST STORE**」セクションを参照してください。

手順D.2 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。証明書の場所とパスワードを書き留めてください。対話型の設定を使用する場合に必要な情報がこれがすべてです。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

${local:_basedir}** は LDAP プロパティー設定ファイルの場所で、**/etc/ovirt-engine/aaa** ディレクトリーをポイントします。PEM エンコードされた CA 証明書を別のディレクトリーに作成した場合には、**${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 (対話式の設定)」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 検索、ブックマーク、タグの使用

E.1. 検索

E.1.1. Red Hat Virtualization での検索

管理ポータルでは、仮想マシン、ホスト、ユーザーなど、数千におよぶリソースの管理ができます。検索を行うには、検索クエリー (フリーテキストまたは構文ベース) を検索バーに入力します。特定の検索結果が必要な場合に検索クエリーを毎回入力しなくても済むように、検索クエリーをブックマークとして保存しておいて、後で使用することができます。検索では、大文字と小文字が区別されます。

E.1.2. 検索構文および例

Red Hat Virtualization リソースの検索クエリーの構文は、以下のとおりです。

`result type: {criteria} [sortby sort_spec]`

構文の例

以下の表には、検索クエリーの使用例を記載しています。これにより、Red Hat Virtualization での検索クエリーの構築方法を理解することができます。

表E.1 検索クエリーの例

例	結果
Hosts: Vms.status = up	稼働中の仮想マシンを実行している全ホストの一覧を表示
Vms: domain = qa.company.com	指定したドメインで稼働中の全仮想マシンの一覧を表示
Vms: users.name = Mary	ユーザー名が Mary のユーザーに属する全仮想マシンの一覧を表示
Events: severity > normal sortby time	重大度が Normal を超える全イベントの一覧を時間順に表示

E.1.3. 検索のオートコンプリート機能

管理ポータルは、正しく有効な検索クエリーの作成に役立つオートコンプリート機能を提供しています。検索クエリーの一部を入力すると、検索バーの下に、後に続く箇所の選択肢がドロップダウンリストに表示されます。このリストから選択して入力/選択を続けることができます。また、オプションを無視して手動でクエリーの入力を続けることも可能です。

以下の表には、管理ポータルでクエリー構築にオートコンプリート機能を活用する方法の例をまとめています。

```
Hosts: Vms.status = down
```

表E.2 オートコンプリートを使用した検索クエリーの例

入力	表示される一覧項目	アクション
h	**Hosts** (オプションは 1 つのみ)	**Hosts** を選択もしくは **Hosts** と入力
Hosts:	ホストの全プロパティー	**v** と入力
Hosts: v	**v** で始まるホストのプロパティー	**Vms** を選択もしくは **Vms** と入力
Hosts: Vms	仮想マシンの全プロパティー	**s** と入力
Hosts: Vms.s	**s** で始まる仮想マシンの全プロパティー	**status** を選択もしくは **status** と入力
Hosts: Vms.status	**=** **!=**	**=** を選択または入力
Hosts: Vms.status =	すべてのステータス値	**down** を選択または入力

E.1.4. 検索結果タイプのオプション

結果タイプを指定して、以下のいずれかのタイプのリソースを検索することができます。

- **Vms**: 仮想マシンの一覧
- **Host**: ホストの一覧
- **Pools**: プールの一覧
- **Template**: テンプレートの一覧
- **Event**: イベントの一覧
- **Users**: ユーザーの一覧
- **Cluster**: クラスターの一覧
- **Datacenter**: データセンターの一覧
- **Storage**: ストレージドメインの一覧

各リソースタイプには、固有のプロパティーセットと、それが関連付けられたその他のリソースタイプのセットがあります。また、各検索タイプには、一式の有効な構文の組み合わせがあります。オートコンプリート機能を使用すると、正しいクエリーを容易に作成することができます。

E.1.5. 検索条件

クエリーのコロンの後に、検索条件を指定することができます。**{criteria}** の構文は以下のとおりです。

<prop><operator><value>

または

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

例

以下の表には、構文の各要素についての説明をまとめています。

表E.3 検索条件の例

要素	説明	値	例	注記
prop	検索対象となるリソースのプロパティー。リソースタイプのプロパティー (**obj-type** を参照) または **tag** (カスタムタグ) を指定することも可能。	検索対象を特定のプロパティーのオブジェクトに限定 (例: **status** プロパティーのオブジェクトの検索)	Status	該当なし
obj-type	検索対象となるリソースに関連付けできるリソースタイプ	データセンターや仮想マシンなどのシステムオブジェクト	Users	該当なし
operator	比較演算子	= != (not equal) > < >= <=	該当なし	プロパティーによって、値のオプションが異なる

要素	説明	値	例	注記
value	式の比較対象	文字列 整数 ランキング 日付 (地域設定に応じた形式)	Jones 256 normal	• 文字列内にワイルドカードを使用することが可能 • 初期化されていない (空の) 文字列を示すには、"" (一組の二重引用符。間にはスペースなし) を使用することが可能 • 空白を含む文字列や日付は、二重引用符で囲む

E.1.6. 検索: 複数の基準とワイルドカード

ワイルドカードは、文字列の構文の **<value>** の部分に使用することができます。たとえば、**m** で始まる全ユーザーを検索するには、**m*** と入力します。

AND や **OR** などのブール演算子を使うと、2 つの基準で検索を行うことができます。例:

```
Vms: users.name = m* AND status = Up
```

上記のクエリーは、ユーザー名が "m" で始まるユーザーの実行中の仮想マシンをすべて返します。

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

上記のクエリーは、ユーザー名が "m" で始まるユーザーの "paris-loc" とタグ付けされた仮想マシンをすべて返します。

AND または **OR** を使わずに 2 つの基準を指定すると、**AND** が暗黙的に指定されます。**AND** は **OR** より優先され、また **OR** は、暗黙的な **AND** より優先されます。

E.1.7. 検索: 検索結果のソート順の特定

sortby を使用することにより、返される情報のソート順を特定することができます。また、ソート方向を指定することも可能です (昇順の場合は **asc**、降順の場合は **desc**)。

例

```
events: severity > normal sortby time desc
```

このクエリーは、重大度が Normal を超える全イベントを時間順で返します (降順)。

E.1.8. データセンターの検索

以下の表には、データセンターの全検索オプションをまとめています。

表E.4 データセンターの検索

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Clusters.*clusters-prop*	プロパティータイプによって異なる	データセンターに関連付けられたクラスターのプロパティー
name	文字列	データセンターの名前
description	文字列	データセンターの説明
type	文字列	データセンターのタイプ
status	一覧	データセンターの稼働状況
sortby	一覧	リソースプロパティー別に検索結果を並べ替え
page	整数	表示する結果のページ番号

例

```
Datacenter: type = nfs and status != up
```

以下の条件に一致するデータセンターの一覧を返します。

- ストレージタイプが NFS で、ステータスが UP 以外のデータセンター

E.1.9. クラスターの検索

以下の表には、クラスターの全検索オプションをまとめています。

表E.5 クラスターの検索

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Datacenter.*datacenter-prop*	プロパティータイプによって異なる	クラスターに関連付けられたデータセンターのプロパティー

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Datacenter	文字列	クラスターが属するデータセンター
name	文字列	ネットワーク上でクラスターを識別する一意名
description	文字列	クラスターの説明
initialized	文字列	True または False でクラスターのステータスを表示
sortby	一覧	リソースプロパティー別に検索結果を並べ替え
page	整数	表示する結果のページ番号

例

`Clusters: initialized = true or name = Default`

以下の条件に一致するクラスターの一覧を返します。

- 初期化されたクラスター
- Default と名前の付いたクラスター

E.1.10. ホストの検索

以下の表には、ホストの全検索オプションをまとめています。

表E.6 ホストの検索

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Vms.*Vms-prop*	プロパティータイプによって異なる	ホストに関連付けられた仮想マシンのプロパティー
Templates.*templates-prop*	プロパティータイプによって異なる	ホストに関連付けられたテンプレートのプロパティー
Events.*events-prop*	プロパティータイプによって異なる	ホストに関連付けられたイベントのプロパティー
Users.*users-prop*	プロパティータイプによって異なる	ホストに関連付けられたユーザーのプロパティー

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
name	文字列	ホスト名
status	一覧	ホストの稼働状況
external_status	文字列	外部システムおよびプラグインによってレポートされるホストのヘルスステータス
cluster	文字列	ホストが属するクラスター
address	文字列	ネットワーク上でホストを識別する一意名
cpu_usage	整数	処理能力の使用率
mem_usage	整数	メモリー使用率
network_usage	整数	ネットワークの使用率
load	整数	任意のタイムスライスにおいて、各プロセッサーの **run-queue** で実行を待機中のジョブ
version	整数	オペレーティングシステムのバージョン番号
cpus	整数	ホスト上の CPU 数
memory	整数	使用可能なメモリー容量
cpu_speed	整数	CPU の処理速度
cpu_model	文字列	CPU のタイプ
active_vms	整数	現在実行中の仮想マシン数
migrating_vms	整数	現在移行中の仮想マシン数
committed_mem	整数	メモリーのコミット率
tag	文字列	ホストに割り当てられたタグ
type	文字列	ホストのタイプ
datacenter	文字列	ホストが属するデータセンター

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
sortby	一覧	リソースプロパティー別に検索結果を並べ替え
page	整数	表示する結果のページ番号

例

```
Hosts: cluster = Default and Vms.os = rhel6
```

以下の条件に一致するホストの一覧を返します。

- Default のクラスターに属し、Red Hat Enterprise Linux 6 オペレーティングシステムを実行する仮想マシンをホストしている

E.1.11. ネットワークの検索

以下の表には、ネットワークの全検索オプションをまとめています。

表E.7 ネットワークの検索

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Cluster_network.*clusternetwork-prop*	プロパティータイプによって異なる	ネットワークに関連付けられたクラスターのプロパティー
Host_Network.*hostnetwork-prop*	プロパティータイプによって異なる	ネットワークに関連付けられたホストのプロパティー
name	文字列	ネットワークを識別する、人間が判読可能な名前
description	文字列	ネットワークを説明するキーワードまたはテキスト。ネットワークの作成時にオプションで使用することができます。
vlanid	整数	ネットワークの VLAN ID
stp	文字列	そのネットワークで Spanning Tree Protocol (STP) が有効かどうか。
mtu	整数	論理ネットワークの最大転送単位
vmnetwork	文字列	そのネットワークを仮想マシントラフィック専用に使用するかどうか。

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
datacenter	文字列	ネットワークがアタッチされたデータセンター
sortby	一覧	リソースプロパティー別に検索結果を並べ替え
page	整数	表示する結果のページ番号

例

```
Network: mtu > 1500 and vmnetwork = true
```

以下の条件に一致するネットワークの一覧を返します。

- 最大転送単位が 1500 バイトを上回る
- 仮想マシン専用に設定されている

E.1.12. ストレージの検索

以下の表には、ストレージの全検索オプションをまとめています。

表E.8 ストレージの検索

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Hosts.*hosts-prop*	プロパティータイプによって異なる	ストレージに関連付けられたホストのプロパティー
Clusters.*clusters-prop*	プロパティータイプによって異なる	ストレージに関連付けられたクラスターのプロパティー
name	文字列	ネットワークでストレージを識別する一意名
status	文字列	ストレージドメインのステータス
external_status	文字列	外部システムおよびプラグインによってレポートされるストレージドメインのヘルスステータス
datacenter	文字列	ストレージが属するデータセンター

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
type	文字列	ストレージのタイプ
size	整数	ストレージのサイズ
used	整数	使用済みストレージ容量
committed	整数	コミット済みストレージ容量
sortby	一覧	リソースプロパティー別に検索結果を並べ替え
page	整数	表示する結果のページ番号

例

```
Storage: size > 200 or used < 50
```

以下の条件に一致するストレージの一覧を返します。

- ストレージ領域が合計で 200 GB を超えるストレージ
- 使用済みのストレージ領域が 50 GB 未満のストレージ

E.1.13. ディスクの検索

以下の表には、ディスクの全検索オプションをまとめています。

表E.9 ディスクの検索

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Datacenters.*datacenters-prop*	プロパティータイプによって異なる	ディスクに関連付けられたデータセンターのプロパティー
Storages.*storages-prop*	プロパティータイプによって異なる	ディスクに関連付けられたストレージのプロパティー
alias	文字列	ネットワーク上のストレージを識別する、人間が判読可能な名前
description	文字列	ディスクを説明するキーワードまたはテキスト。ディスクの作成時にオプションで使用することができます。
provisioned_size	整数	ディスクの仮想サイズ

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
size	整数	ディスクのサイズ
actual_size	整数	ディスクに割り当てられる実サイズ
creation_date	整数	ディスクの作成日
bootable	文字列	ディスクがブート可能であるかどうか。有効な値は **0**、**1**、**yes**、**no** のいずれかです。
shareable	文字列	ディスクを複数の仮想マシンに同時にアタッチできるかどうか。有効な値は **0**、**1**、**yes**、**no** のいずれかです。
format	文字列	ディスクの形式。**unused**、**unassigned**、**cow**、**raw** のいずれかです。
status	文字列	ディスクのステータス。**unassigned**、**ok**、**locked**、**invalid**、**illegal** のいずれかです。
disk_type	文字列	ディスクのタイプ。**image** または **lun** のいずれかです。
number_of_vms	整数	ディスクがアタッチされている仮想マシンの数
vm_names	文字列	ディスクがアタッチされている仮想マシンの名前
quota	文字列	仮想ディスクに有効化されているクォータの名前
sortby	一覧	リソースプロパティー別に検索結果を並べ替え
page	整数	表示する結果のページ番号

例

```
Disks: format = cow and provisioned_size > 8
```

この例は、以下の条件に一致する仮想ディスクの一覧を返します。

- QCOW (別称: シンプロビジョニング) 形式
- 割り当てられたディスクサイズが 8 GB 以上

E.1.14. ボリュームの検索

以下の表には、ボリュームの全検索オプションをまとめています。

表E.10 ボリュームの検索

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Cluster.*cluster-prop*	プロパティーのタイプによって異なる	ボリュームに関連付けられたクラスターのプロパティー
Cluster	文字列	ボリュームに関連付けられたクラスターの名前
name	文字列	ボリュームを識別する、人間が判読可能な名前
type	文字列	distribute、replicate、distributed_replicate、stripe、distributed_stripe のいずれかを指定することができます。
transport_type	整数	TCP または RDMA のいずれかを指定することができます。
replica_count	整数	レプリカの数
stripe_count	整数	ストライプの数
status	文字列	ボリュームのステータス。Up または Down のいずれか。
sortby	一覧	リソースプロパティー別に検索結果を並べ替え
page	整数	表示する結果のページ番号

例

```
Volume: transport_type = rdma and stripe_count >= 2
```

この例は、以下の条件に一致するボリュームの一覧を返します。

- トランスポートタイプが RDMA に設定されている
- ストライプ数が 2 以上

E.1.15. 仮想マシンの検索

以下の表には、仮想マシンの全検索オプションをまとめています。

表E.11 仮想マシンの検索

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Hosts.*hosts-prop*	プロパティータイプによって異なる	仮想マシンに関連付けられたホストのプロパティー
Templates.*templates-prop*	プロパティータイプによって異なる	仮想マシンに関連付けられたテンプレートのプロパティー
Events.*events-prop*	プロパティータイプによって異なる	仮想マシンに関連付けられたイベントのプロパティー
Users.*users-prop*	プロパティータイプによって異なる	仮想マシンに関連付けられたユーザーのプロパティー
Storage.*storage-prop*	プロパティータイプによって異なる	仮想マシンに関連付けられたストレージデバイスのプロパティー
Vnic.*vnic-prop*	プロパティータイプによって異なる	仮想マシンに関連付けられた仮想 NIC のプロパティー
name	文字列	仮想マシンの名前
status	一覧	仮想マシンの稼働状況
ip	整数	仮想マシンの IP アドレス
uptime	整数	仮想マシンの実行時間 (分単位)
domain	文字列	これらのマシンをグループ化するドメイン (通常は、Active Directory ドメイン)
os	文字列	仮想マシンの作成時に選択したオペレーティングシステム
creationdate	日付	仮想マシンの作成日
address	文字列	ネットワーク上で仮想マシンを識別する一意名
cpu_usage	整数	処理能力の使用率
mem_usage	整数	メモリー使用率

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
network_usage	整数	ネットワーク使用率
memory	整数	定義済みの最大メモリー
apps	文字列	仮想マシンに現在インストールされているアプリケーション
cluster	一覧	仮想マシンが属するクラスター
pool	一覧	仮想マシンが属する仮想マシンプール
loggedinuser	文字列	仮想マシンに現在ログインしているユーザーの名前
tag	一覧	仮想マシンが属するタグ
datacenter	文字列	仮想マシンが属するデータセンター
type	一覧	仮想マシンのタイプ (サーバーまたはデスクトップ)
quota	文字列	仮想マシンに関連付けられたクォータの名前
description	文字列	仮想マシンを説明するキーワードまたはテキスト。仮想マシンの作成時にオプションで使用することができます。
sortby	一覧	リソースプロパティー別に検索結果を並べ替え
page	整数	表示する結果のページ番号

例

```
Vms: template.name = Win* and user.name = ""
```

この例は、以下の条件に一致する仮想マシンの一覧を返します。

- ベーステンプレート名が Win で始まり、いずれかのユーザーに割り当てられている仮想マシン

例

```
Vms: cluster = Default and os = windows7
```

この例は、以下の条件に一致する仮想マシンの一覧を返します。

- 属するクラスター名が Default で、Windows 7 オペレーティングシステムを実行している仮想マシン

E.1.16. プールの検索

以下の表には、プールの全検索オプションをまとめています。

表E.12 プールの検索

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
name	文字列	プールの名前
description	文字列	プールの説明
type	一覧	プールのタイプ
sortby	一覧	リソースプロパティー別に検索結果を並べ替え
page	整数	表示する結果のページ番号

例

`Pools: type = automatic`

以下の条件に一致するプールの一覧を返します。

- タイプが automatic

E.1.17. テンプレートの検索

以下の表には、テンプレートの全検索オプションをまとめています。

表E.13 テンプレートの検索

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Vms.*Vms-prop*	文字列	テンプレートに関連付けられた仮想マシンのプロパティー
Hosts.*hosts-prop*	文字列	テンプレートに関連付けられたホストのプロパティー
Events.*events-prop*	文字列	テンプレートに関連付けられたイベントのプロパティー

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Users.*users-prop*	文字列	テンプレートに関連付けられたユーザーのプロパティー
name	文字列	テンプレートの名前
domain	文字列	テンプレートのドメイン
os	文字列	オペレーティングシステムのタイプ
creationdate	整数	テンプレートの作成日 日付の形式 **mm/dd/yy**
childcount	整数	テンプレートから作成された仮想マシンの数
mem	整数	定義されたメモリー
description	文字列	テンプレートの説明
status	文字列	テンプレートのステータス
cluster	文字列	テンプレートに関連付けられたクラスター
datacenter	文字列	テンプレートに関連付けられたデータセンター
quota	文字列	テンプレートに関連付けられたクォータ
sortby	一覧	リソースプロパティー別に検索結果を並べ替え
page	整数	表示する結果のページ番号

例

```
Template: Events.severity >= normal and Vms.uptime > 0
```

以下の条件に一致するテンプレートの一覧を返します。

- テンプレートを使用して作成した仮想マシンで、重大度が normal 以上のイベントが発生し、その仮想マシンがまだ実行中である

E.1.18. ユーザーの検索

以下の表には、ユーザーの全検索オプションをまとめています。

表E.14 ユーザーの検索

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Vms.*Vms-prop*	プロパティータイプによって異なる	ユーザーに関連付けられた仮想マシンのプロパティー
Hosts.*hosts-prop*	プロパティータイプによって異なる	ユーザーに関連付けられたホストのプロパティー
Templates.*templates-prop*	プロパティータイプによって異なる	ユーザーに関連付けられたテンプレートのプロパティー
Events.*events-prop*	プロパティータイプによって異なる	ユーザーに関連付けられたイベントのプロパティー
name	文字列	ユーザー名
lastname	文字列	ユーザーの姓
usrname	文字列	ユーザーの一意名
department	文字列	ユーザーが属する部署
group	文字列	ユーザーが属するグループ
title	文字列	ユーザーのタイトル
status	文字列	ユーザーのステータス
role	文字列	ユーザーのロール
tag	文字列	ユーザーが属するタグ
pool	文字列	ユーザーが属するプール
sortby	一覧	リソースプロパティー別に検索結果を並べ替え
page	整数	表示する結果のページ番号

例

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

以下のいずれかの条件に一致するユーザーの一覧を返します。

- そのユーザーの仮想マシンで重大度が中レベルを超えるイベントが発生し、かつその仮想マシンが現在も稼働している
- そのユーザーの仮想マシンが一時停止されている

E.1.19. イベントの検索

以下の表には、イベントの検索に使用できる全検索オプションをまとめています。オートコンプリート機能により、数多くのオプションが適宜表示されます。

表E.15 イベントの検索

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
Vms.*Vms-prop*	プロパティータイプによって異なる	イベントに関連付けられた仮想マシンのプロパティー
Hosts.*hosts-prop*	プロパティータイプによって異なる	イベントに関連付けられたホストのプロパティー
Templates.*templates-prop*	プロパティータイプによって異なる	イベントに関連付けられたテンプレートのプロパティー
Users.*users-prop*	プロパティータイプによって異なる	イベントに関連付けられたユーザーのプロパティー
Clusters.*clusters-prop*	プロパティータイプによって異なる	イベントに関連付けられたクラスターのプロパティー
Volumes.*Volumes-prop*	プロパティータイプによって異なる	イベントに関連付けられたボリュームのプロパティー
type	一覧	イベントのタイプ
severity	一覧	イベントの重大度: Warning/Error/Normal
message	文字列	イベントタイプの説明
time	一覧	イベントの発生日
usrname	文字列	イベントに関連付けられたユーザー名
event_host	文字列	イベントに関連付けられたホスト
event_vm	文字列	イベントに関連付けられた仮想マシン

プロパティー (リソースまたはリソースタイプ)	タイプ	説明
event_template	文字列	イベントに関連付けられたテンプレート
event_storage	文字列	イベントに関連付けられたストレージ
event_datacenter	文字列	イベントに関連付けられたデータセンター
event_volume	文字列	イベントに関連付けられたボリューム
correlation_id	整数	イベントの識別番号
sortby	一覧	リソースプロパティー別に検索結果を並べ替え
page	整数	表示する結果のページ番号

例

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

以下の条件に一致するイベントの一覧を返します。

- **gonzo.example.com** というホストで実行していた **testdesktop** という名前の仮想マシンで発生したイベント

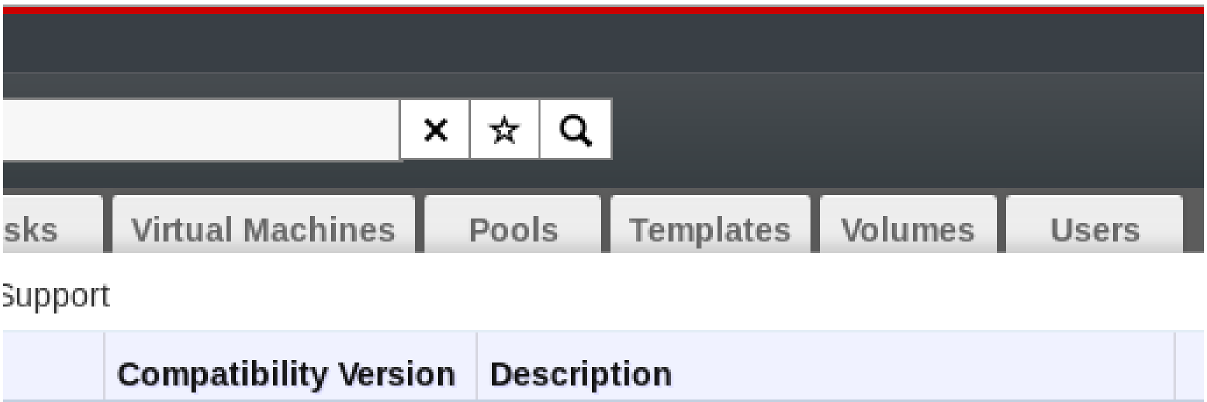
E.2. ブックマーク

E.2.1. ブックマークとしてクエリー文字列を保存する手順

ブックマークを使用すると、検索クエリーを保存したり、他のユーザーと共有したりすることができます。

手順E.1 ブックマークとしてクエリー文字列を保存する手順

1. 検索バーに必要な検索クエリーを入力し、検索を行います。
2. 検索バーの右側にある、星型の **ブックマーク** ボタンをクリックし、**新規ブックマーク** を開きます。



図E.1 ブックマークのアイコン

3. ブックマークの **名前** を入力します。
4. **検索文字列** フィールドを編集します (該当する場合)。
5. **OK** をクリックしてクエリーをブックマークとして保存し、ウィンドウを閉じます。
6. 検索クエリーが保存され、**ブックマーク** ペインに表示されます。

今後再使用できるようブックマークとして検索クエリーを保存しました。ブックマークを検索/選択するには、**ブックマーク** ペインを使用してください。

E.2.2. ブックマークの編集

ブックマークの名前および検索文字列を変更することができます。

手順E.2 ブックマークの編集

1. 画面の左端にある **ブックマーク** タブをクリックします。
2. 編集するブックマークを選択します。
3. **編集** ボタンをクリックすると **ブックマークの編集** ウィンドウが開きます。
4. 必要に応じて **名前** と **検索文字列** のフィールドを変更します。
5. **OK** をクリックして編集したブックマークを保存します。

検索クエリーのブックマークが編集されました。

E.2.3. ブックマークの削除

ブックマークが不要となった場合には削除してください。

手順E.3 ブックマークの削除

1. 画面の左端にある **ブックマーク** タブをクリックします。
2. 削除するブックマークを選択します。
3. **削除** ボタンをクリックすると **ブックマークの削除** ウィンドウが開きます。
4. **OK** をクリックして、選択したブックマークを削除します。

検索クエリーのブックマークが削除されました。

E.3. タグ

E.3.1. タグを使用した、Red Hat Virtualization との対話のカスタマイズ

Red Hat Virtualization プラットフォームをセットアップして、要件に応じた設定を完了したら、タグを使用して作業に適したカスタマイズを行うことができます。タグがシステム管理者にもたらす重要な利点は、システムリソースのグループ分け/カテゴリー分けが可能となることです。これは、仮想化環境に多数のオブジェクトが存在し、それらの中の特定のセットを対象に管理者が集中的に作業を行う場合に役立ちます。

このセクションでは、タグの作成と編集、ホストまたは仮想マシンへのタグ割り当て、タグを基準とした検索の方法について説明します。タグは、一定の構造に合わせて階層化し、エンタープライズ環境のニーズに対応することができます。

管理ポータルのタグは、**タグ** ペインで作成/変更/削除することができます。

E.3.2. タグの作成

タグを使用して検索結果をフィルタリングすることができるようにタグを作成します。

手順E.4 タグの作成

1. 画面の左端にある **タグ** タブをクリックします。
2. タグを作成するノードを選択します。たとえば、最上位でタグを作成するには、**`root`** ノードをクリックします。
3. **新規作成** ボタンをクリックすると **新規タグ** ウィンドウが開きます。
4. 新規作成するタグの **名前** と **説明** を入力します。
5. **OK** をクリックすると、タグが作成されます。

新規タグが作成され、**タグ** タブに表示されます。

E.3.3. タグの変更

タグの名前と説明を編集することができます。

手順E.5 タグの変更

1. 画面の左端にある **タグ** タブをクリックします。
2. 変更するタグを選択します。
3. **編集** をクリックすると **タグの編集** ウィンドウが開きます。
4. 必要に応じて **名前** と **説明** のフィールドを変更します。
5. **OK** をクリックして編集したタグを保存します。

タグのプロパティーが変更されました。

E.3.4. タグの削除

タグが不要となった場合には削除してください。

手順E.6 タグの削除

1. 画面の左端にある **タグ** タブをクリックします。
2. 削除するタグを選択します。
3. **削除** をクリックすると **タグの削除** ウィンドウが開きます。タグを削除すると、そのタグの子要素もすべて削除されることを警告するメッセージが表示されます。
4. **OK** をクリックすると選択したタグが削除されます。

タグとその子要素がすべて削除されました。このタグがアタッチされていたオブジェクトからも削除されます。

E.3.5. オブジェクトへのタグの追加と削除

ホスト、仮想マシン、ユーザーにタグを割り当てたり、削除したりすることができます。

手順E.7 オブジェクトへのタグの追加と削除

1. リソースタブをクリックして、タグ付けまたはタグ付け解除するオブジェクトを選択します。
2. **タグを割り当て** をクリックすると **タグの割り当て** ウィンドウが開きます。
3. オブジェクトにタグを割り当てるには、チェックボックスを選択します。オブジェクトからタグを解除するには、チェックボックスからチェックを外します。
4. **OK** をクリックします。

指定したタグが選択したオブジェクトのカスタムプロパティーとして追加または削除されます。

E.3.6. タグを使用したオブジェクトの検索

- **タグ** をプロパティーとして、必要な値/値セットを検索条件として使用して、検索クエリーを入力します。

  指定した条件でタグ付けされたオブジェクトが結果一覧に表示されます。

付録F ブランディング

F.1. ブランディング

F.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ー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。

F.1.2. ログイン画面

ログイン画面は、管理ポータルとユーザーポータルの両方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。

F.1.3. 管理ポータルの画面

管理ポータルの画面は、管理ポータルにログインする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。

F.1.4. ユーザーポータルの画面

ユーザーポータルの画面は、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。ユーザー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
- 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

ユーザーポータルの画面のクラスは **user_portal.css** にあります。

F.1.5. ポップアップウィンドウ

ポップアップウィドウは、ホストや仮想マシンなどのエンティティーを作成/編集/更新することができる、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。

F.1.6. タブ

ユーザーポータルのタブ要素には、「基本」ビューと「拡張」ビューを切り替えるためのメインのタブと、「拡張」ビューが選択されている場合に表示される左側のタブの 2 つのタイプがあります。また、管理ポータルのポップアップウィンドウの多くにもタブが含まれます。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。

F.1.7. Welcome ページ

Welcome ページは、Manager のホームページにアクセスする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。

F.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G システムアカウント

G.1. システムアカウント

G.1.1. Red Hat Virtualization Manager のユーザーアカウント

rhevm パッケージ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。

G.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

G.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。

G.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。