



Red Hat

Red Hat Virtualization 4.4

管理ガイド

Red Hat Virtualization の管理タスク

Red Hat Virtualization 4.4 管理ガイド

Red Hat Virtualization の管理タスク

Red Hat Virtualization Documentation Team

Red Hat Customer Content Services

rhev-docs@redhat.com

法律上の通知

Copyright © 2023 Red Hat, Inc.

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

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

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

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

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

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

Java® is a registered trademark of Oracle and/or its affiliates.

XFS® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

このドキュメントでは、Red Hat Virtualization の管理者に関する情報および手順を説明します。

目次

第1章 RED HAT VIRTUALIZATION 環境の管理と保守	4
1.1. グローバル設定	4
1.2. ダッシュボード	31
1.3. 検索	37
1.4. ブックマーク	55
1.5. タグ	56
第2章 リソースの管理	59
2.1. QOS (QUALITY OF SERVICE)	59
2.2. データセンター	64
2.3. クラスター	72
2.4. 論理ネットワーク	104
2.5. ホスト	146
2.6. ストレージ	188
2.7. プール	224
2.8. 仮想ディスク	240
2.9. 外部プロバイダー	257
第3章 環境の管理	274
3.1. セルフホスト型エンジンの管理	274
3.2. バックアップと移行	283
3.3. RED HAT SATELLITE を使用したエラータ表示の設定	338
3.4. 有効期限が切れる前の証明書更新	339
3.5. ANSIBLE を使用した設定タスクの自動化	341
3.6. ユーザーとロール	343
3.7. クォータとサービスレベル契約ポリシー	375
3.8. イベント通知	381
3.9. ユーティリティー	393
第4章 環境に関する情報の収集	410
4.1. 監視および可観測性	410
4.2. ログファイル	418
付録A VDSM サービスとフック	427
A.1. VDSM フックのインストール	427
A.2. サポートされている VDSM イベント	428
A.3. VDSM フック環境	430
A.4. VDSM フックドメイン XML オブジェクト	430
A.5. カスタムプロパティーの定義	431
A.6. 仮想マシンのカスタムプロパティーの設定	433
A.7. VDSM フックでの仮想マシンのカスタムプロパティーの評価	433
A.8. VDSM フックモジュールの使用	433
A.9. VDSM フックの実行	434
A.10. VDSM フックの戻りコード	435
A.11. VDSM フックの例	435
付録B カスタムネットワークプロパティー	438
B.1. BRIDGE_OPTS パラメーターの説明	438
B.2. RED HAT VIRTUALIZATION MANAGER を使用するように RED HAT VIRTUALIZATION MANAGER を設定する方法	440
B.3. FCOE を使用するように RED HAT VIRTUALIZATION MANAGER を設定する方法	441
付録C RED HAT VIRTUALIZATION ユーザーインターフェイスプラグイン	442

C.1. RED HAT VIRTUALIZATION ユーザーインターフェイスプラグインについて	442
C.2. RED HAT VIRTUALIZATION ユーザーインターフェイスプラグインのライフサイクル	442
C.3. ユーザーインターフェイスプラグイン関連のファイルとその場所	444
C.4. ユーザーインターフェイスプラグインのデプロイメント例	444
付録D RED HAT VIRTUALIZATION での FIPS の有効化	446
D.1. セルフホスト型エンジンでの FIPS の有効化	446
D.2. RHV ホストおよびスタンダロン MANAGER での FIPS の有効化	446
D.3. 関連情報	447
付録E RED HAT VIRTUALIZATION と暗号化された通信	448
E.1. RED HAT VIRTUALIZATION MANAGER CA 証明書の置き換え	448
E.2. MANAGER と LDAP サーバー間の暗号化通信の設定	451
E.3. FIPS の暗号化された VNC コンソールの有効化	453
付録F プロキシー	456
F.1. SPICE プロキシー	456
F.2. SQUID プロキシー	458
F.3. WEBSOCKET プロキシー	460
付録G ブランド化	461
G.1. ブランド化	461
付録H システムアカウント	464
H.1. RED HAT VIRTUALIZATION MANAGER のユーザー アカウント	464
H.2. RED HAT VIRTUALIZATION MANAGER グループ	464
H.3. 仮想化ホストのユーザー アカウント	464
H.4. 仮想化ホスト グループ	465
付録I 法的通知	466

第1章 RED HAT VIRTUALIZATION 環境の管理と保守

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

- ホストや仮想マシンなどの物理リソースおよび仮想リソースの管理。これには、ホストのアップグレードおよび追加、ドメインのインポート、外部ハイパーバイザーで作成された仮想マシンの変換、および仮想マシンプールの管理が含まれます。
- ホストのいずれかに対する極端な負荷や、メモリーまたはディスクの容量不足などの潜在的な問題に関連する全体的なシステムリソースの監視と、必要なアクション(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するなどのアクション)の実行。
- 仮想マシンの新しい要件への対応(オペレーティングシステムのアップグレードや、メモリー割り当ての増加など)。
- タグを使用したカスタムオブジェクトプロパティーの管理。
- [パブリックブックマーク](#) として保存された検索の管理。
- ユーザー設定の管理とパーミッションレベルの設定。
- システム機能全体の特定ユーザーまたは仮想マシンのトラブルシューティング。
- 汎用および特定レポートの生成。

1.1. グローバル設定

Administration → **Configure** をクリックしてアクセスします。**Configure** ウィンドウでは、ユーザー、ロール、システムパーミッション、スケジューリングポリシー、インスタンスタイプ、MAC アドレスプールなどの Red Hat Virtualization 環境のグローバルリソースを複数設定できます。このウィンドウでは、ユーザーが環境のリソースと対話する方法をカスタマイズし、複数のクラスターに適用できるオプションを設定する一元的な場所を提供します。

1.1.1. ロール

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

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

1.1.1.1. 新しいロールの作成

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

手順

1. Administration → Configure をクリックします。これにより、Configure ウィンドウが開きます。デフォルトでは Roles タブが選択されており、デフォルトの User ロールと Administrator ロール、およびカスタムロールのリストが表示されます。
2. New をクリックします。
3. 新規ロールの Name および Description を入力します。
4. Account Type で Admin または User のいずれかを選択します。
5. Expand All または Collapse All ボタンを使用して、Check Boxes to Allow Action リストに記載されているオブジェクトのパーミッション表示を展開、または折りたたみます。各オブジェクトのオプションも展開、または折りたたむことができます。
6. 各オブジェクトで、設定しているロールに対して許可または拒否するアクションを、それぞれ選択もしくは消去します。
7. OK をクリックして変更を適用します。ロールの一覧に新しいロールが表示されます。

1.1.1.2. ロールの編集またはコピー

作成したロールの設定は変更できますが、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、そのロールのクローンを作成し、要件に合わせて変更します。

手順

1. Administration → Configure をクリックします。Configure ウィンドウが表示され、デフォルトの User ロールと Administrator ロール、およびカスタムロールのリストが表示されます。
2. 変更するロールを選択します。
3. Edit または Copy をクリックします。Edit Role または Copy Role ウィンドウが開きます。
4. 必要に応じて、ロールの Name および Description を編集します。
5. Expand All または Collapse All ボタンを使用して、リストされているオブジェクトのパーミッション表示を展開、または折りたたみます。各オブジェクトのオプションも展開、または折りたたむことができます。
6. 各オブジェクトで、編集しているロールに対して許可または拒否するアクションを、それぞれ選択もしくは消去します。
7. OK をクリックして、変更を適用します。

1.1.1.3. ユーザーロールと承認の例

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

例1.1 クラスター権限

Sarah は、ある企業の経理部門のシステム管理者です。この部署の仮想リソースは、すべて Accounts という名前の Red Hat Virtualization クラスターの下に編成されています。Sarah には Accounts クラスターの ClusterAdmin ロールが割り当てられています。仮想マシンはクラスターの子オブジェクトであるため、Sarah はクラスター内のすべての仮想マシンを管理できます。仮想マシンの管理には、ディスクなどの仮想リソースの編集、追加、削除、およびスナップショットの作成

などが含まれます。このクラスターの外部にあるリソースを管理することはできません。ClusterAdmin は管理者ロールであるため、管理ポータルまたは VM ポータルを使用してこれらのリソースを管理できます。

例1.2 VM PowerUser パーミッション

John は、経理部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を構築し、テストしています。Sarah は、John に **johndesktop** という仮想デスクトップを作成しました。John は、**johndesktop** 仮想マシンで UserVmManager ロールが割り当てられています。これにより、VM ポータルを使用してこの単一仮想マシンにアクセスすることができます。John は UserVmManager のパーミッションを持っているため、仮想マシンを変更できます。UserVmManager はユーザーロールであるため、管理ポータルを使用できません。

例1.3 データセンターパワーユーザーロールパーミッション

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

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

これは、Penelope に **DataCenterAdmin** 権限を割り当てるることは違うことに注意してください。データセンターの PowerUser として、Penelope は VM ポータルにログインして、データセンター内の仮想マシン固有のアクションを実行できます。Penelope は、ホストまたはストレージをデータセンターに割り当てるなど、データセンターレベルの操作を実行できません。

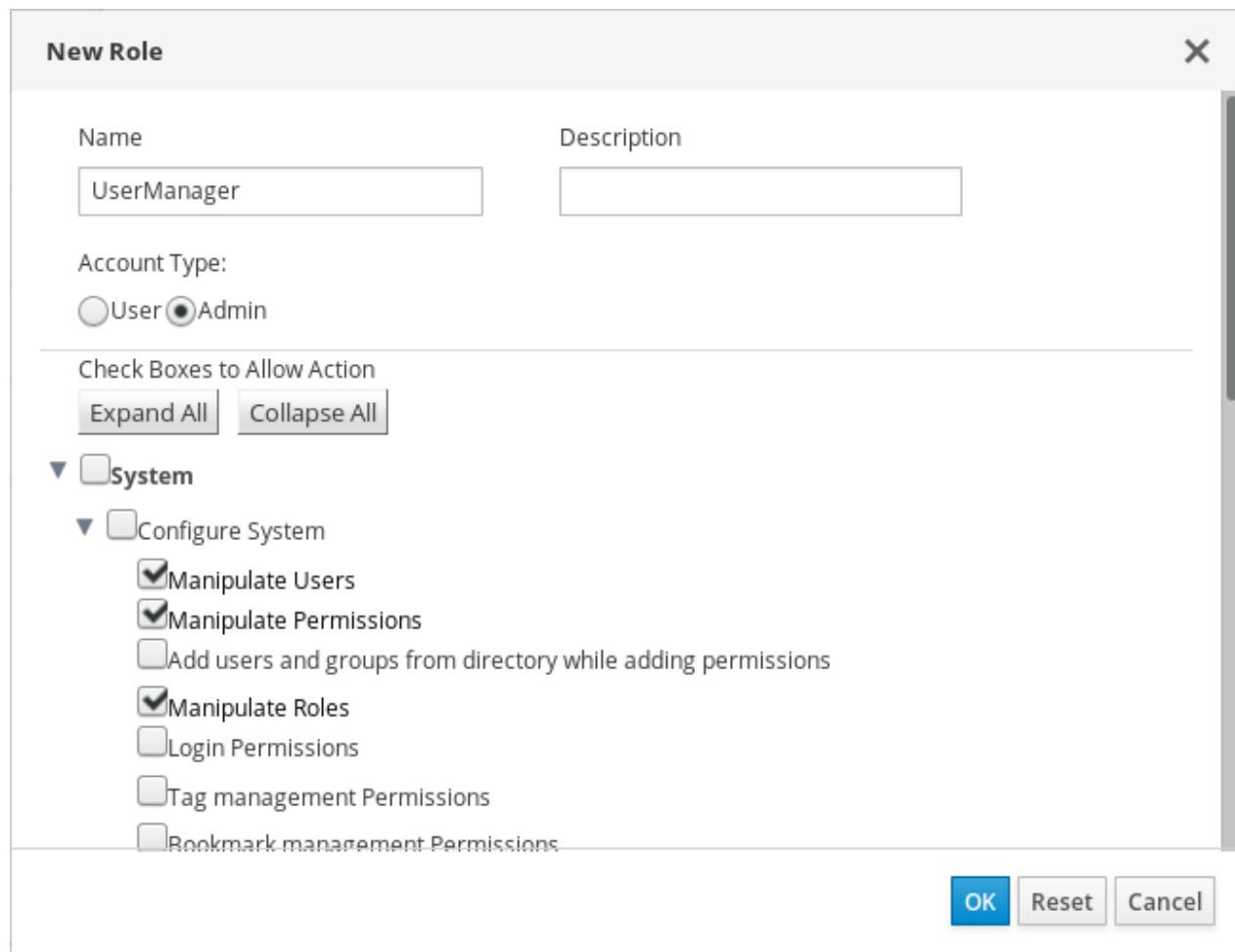
例1.4 ネットワーク管理者のパーミッション

Chris は、IT 部門のネットワーク管理者です。日常業務として、部内の Red Hat Virtualization 環境におけるネットワークの作成、操作、削除などを担当しています。担当業務を行うためには、リソースおよび各リソースのネットワークにおける管理者権限が必要です。たとえば、Chris が IT 部門のデータセンターの **NetworkAdmin** 権限を持っている場合、データセンター内のネットワークを追加および削除したり、データセンターに属するすべての仮想マシンのネットワークをアタッチおよびデタッチすることができます。

例1.5 カスタムロールパーミッション

Rachel は IT 部門に所属し、Red Hat Virtualization のユーザーアカウント管理を担当しています。担当業務を行うためには、ユーザー アカウントを追加し、適切なロールおよびパーミッションを割り当てるパーミッションが必要です。Rachel 自身は仮想マシンを使用せず、ホスト、仮想マシン、クラスター、データセンターの管理権限を付与するべきではありません。Rachel にこのような特定のパーミッションを付与できるビルトインのロールはありません。Rachel の担当業務に適したパーミッションセットを定義するために、カスタムロールを作成する必要があります。

図1.1 UserManager カスタムロール

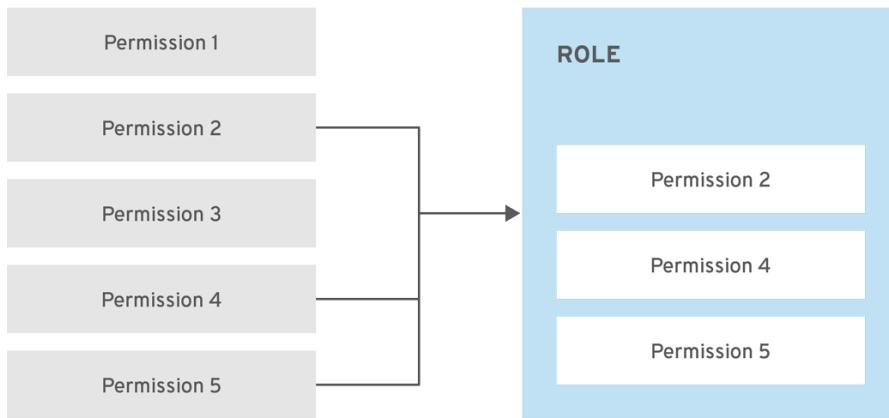


上記の **UserManager** のカスタムロールは、ユーザー、パーミッション、およびロールの操作を可能にします。これらのアクションは、[オブジェクト階層](#) に示される階層の最上位オブジェクトであるシステムの下に整理されています。これは、システム内のすべてのオブジェクトに適用されることを意味します。ロールの **Account Type** は **Admin** に設定されます。つまり、このロールが割り当てられると、Rachel は管理ポータルとかそマシンポータルの両方を使用できるようになります。

1.1.2. システムパーミッション

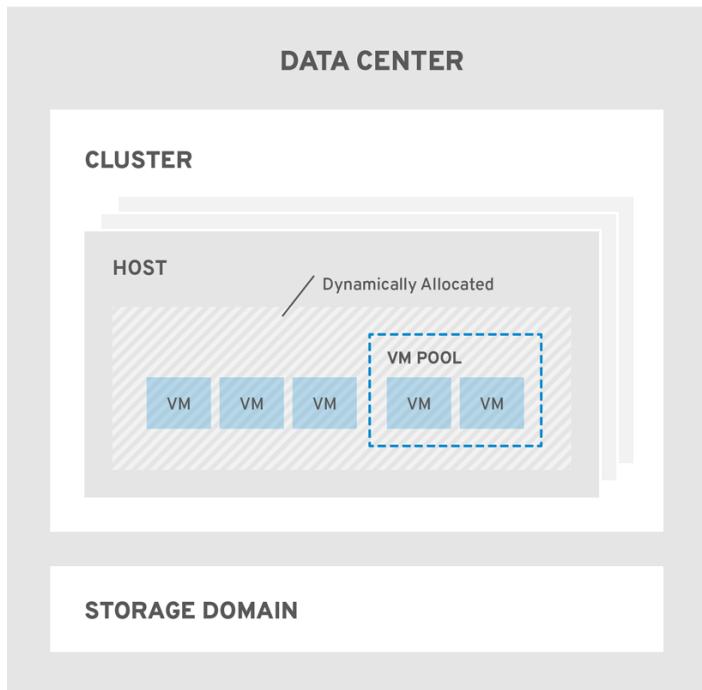
パーミッションにより、ユーザーはオブジェクトに対してアクションを実行できます。オブジェクトは個別オブジェクトまたはコンテナーオブジェクトのいずれかになります。コンテナーオブジェクトに適用されるパーミッションは、そのコンテナーのすべてのメンバーにも適用されます。

図1.2 パーミッションおよびロール



RHV_453537_0219

図1.3 Red Hat Virtualization オブジェクトの階層



RHV_453537_0219

1.1.2.1. ユーザープロパティ

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

1.1.2.2. ユーザーおよび管理者ロール

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

- 管理者ロール:** 物理リソースおよび仮想リソースを管理するための **管理ポータル**へのアクセスを許可します。管理者ロールは、VM ポータルで実行するアクションのパーミッションを付与しますが、ユーザーが VM ポータルで見ることができる内容には影響しません。
- ユーザーロール:** **VM ポータル**にアクセスして、仮想マシンおよびテンプレートを管理し、アクセスできるようにします。ユーザーロールは、ユーザーが VM ポータルで表示できる内容を決定します。管理者ロールを持つユーザーに付与されるパーミッションは、そのユーザーが VM ポータルで利用できるアクションに反映されます。

1.1.2.3. ユーザーロールの概要

以下の表は、VM ポータルで仮想マシンにアクセスして設定する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を説明しています。

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

ロール	権限	注記
UserRole	仮想マシンおよびプールへのアクセスと使用が可能。	VM ポータルへのログイン、割り当てられた仮想マシンやプールの使用、仮想マシンの状態や詳細の表示が可能。
PowerUserRole	仮想マシンおよびテンプレートの作成と管理が可能。	Configure ウィンドウで、このロールを環境全体のユーザー、または特定のデータセンターやクラスターのユーザーに適用します。たとえば、PowerUserRole がデータセンターレベルに適用されると、PowerUser はデータセンターで仮想マシンおよびテンプレートを作成できます。
UserVmManager	仮想マシンのシステム管理者。	仮想マシンの管理、スナップショットの作成と使用が可能。VM ポータルで仮想マシンを作成したユーザーには、そのマシンの UserVmManager ロールが自動的に割り当てられます。

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

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

ロール	権限	注記
UserTemplateBasedVm	テンプレートのみを使用できる限定的な権限。	テンプレートを使用して仮想マシンを作成できます。

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

1.1.2.4. 管理者ロールの概要

以下の表は、管理ポータルのリソースにアクセスして設定する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を説明しています。

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

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



重要

ディレクトリーサーバーの管理ユーザーを、Red Hat Virtualization の管理ユーザーとして使用しないでください。ディレクトリーサーバーに、Red Hat Virtualization の管理ユーザーとして使用するためのユーザーを作成してください。

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

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

ロール	権限	注記
TemplateAdmin	仮想マシンテンプレートの管理者。	テンプレートのストレージドメインやネットワークの詳細を作成、削除、設定したり、ドメイン間でテンプレートを移動したりできます。
StorageAdmin	ストレージ管理者。	割り当てられたストレージドメインを作成、削除、設定、および管理できます。
HostAdmin	ホスト管理者。	特定のホストをアタッチ、削除、設定、および管理できます。

ロール	権限	注記
NetworkAdmin	ネットワーク管理者。	特定のデータセンターまたはクラスターのネットワークを設定および管理できます。データセンターまたはクラスターのネットワーク管理者は、クラスター内の仮想プールのネットワークパーミッションを継承します。
VmPoolAdmin	仮想プールのシステム管理者。	仮想プールの作成、削除、および設定、仮想プールユーザーの割り当てと削除、プールの仮想マシンに対する基本操作を実行できます。
GlusterAdmin	Gluster Storage 管理者。	Gluster ストレージボリュームを作成、削除、設定、および管理できます。
VmImporterExporter	仮想マシン管理者のインポートおよびエクスポート。	仮想マシンをインポートおよびエクスポートできます。他のユーザーがエクスポートした仮想マシンおよびテンプレートをすべて表示できます。

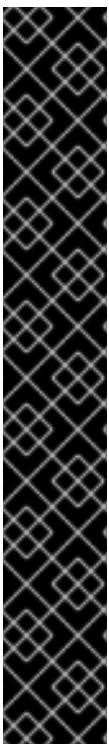
1.1.2.5. リソースへの管理者ロールまたはユーザーロールの割り当て

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

手順

- リソースの名前を見つけてクリックします。詳細ビューが開きます。
- Permissions タブをクリックして、割り当てられたユーザー、各ユーザーのロール、および選択したリソースの継承されたパーミッションを一覧表示します。
- Add をクリックします。
- Search テキストボックスに既存ユーザーの名前またはユーザー名を入力し、Go をクリックします。表示された候補の中からユーザーを選択します。
- Role to Assign ドロップダウンリストからロールを選択します。
- OK をクリックします。

ユーザーは、そのリソースに対して有効化されたロールに継承されたパーミッションを持つようになります。



重要

クラスターなどのリソースのグローバルパーミッションは、システム階層が下位のリソースにも自動的に継承されるため、一般ユーザーにグローバルパーミッションは割り当てないようにしてください。**UserRole** およびその他すべてのユーザーロールパーミッションは、仮想マシン、プール、(特に)仮想マシンプールなどの特定リソースに設定してください。

グローバルパーミッションを割り当てるとき、パーミッションの継承により、以下の2つの問題が発生する可能性があります。

- パーミッションを割り当てる管理者が意図していない場合でも、一般ユーザーに仮想マシンプールを制御するパーミッションが自動的に付与される可能性があります。
- プールを使用すると、仮想マシンポータルが予期せぬ動作をする可能性があります。

したがって、**UserRole** および他のすべてのユーザーロールパーミッションは、特定のリソース (特に仮想マシンプールのリソース) のみに設定し、他のリソースがパーミッションを継承するリソースには設定しないことを強く推奨します。

1.1.2.6. リソースからの管理者またはユーザーロールの削除

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

手順

1. リソースの名前を見つけてクリックします。詳細ビューが開きます。
2. **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースの継承されたパーミッションを一覧表示します。
3. リソースから削除するユーザーを選択します。
4. **Remove** をクリックします。
5. **OK** をクリックします。

1.1.2.7. データセンターのシステムパーミッションの管理

システム管理者は **SuperUser** として、管理ポータルをあらゆる面から管理します。他のユーザーに特定の管理ロールを割り当ることができます。このような制限付き管理者ロールは、特定のリソースに限定して管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対する権利者権限のみ (そのデータセンターのストレージを除く)を持ち、**ClusterAdmin** は割り当てられたクラスターに対する管理者権限のみを持ちます。

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

データセンターの管理者ロールでは、以下のアクションが許可されます。

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



注記

ロールやパーミッションは、既存のユーザーにのみ割り当てることができます。

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

1.1.2.8. データセンター管理者ロールの概要

データセンターのパーミッションロール

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

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

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

1.1.2.9. クラスターのシステムパーミッションの管理

システム管理者は **SuperUser** として、管理ポータルをあらゆる面から管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限付き管理者ロールは、特定のリソースに限定して管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対する権利者権限のみ（そのデータセンターのストレージを除く）を持ち、**ClusterAdmin** は割り当てられたクラスターに対する管理者権限のみを持ちます。

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

クラスター管理者ロールは以下のアクションを許可します。

- 関連付けられたクラスターの作成および削除。

- クラスターに関連付けられたホスト、仮想マシン、およびプールの追加および削除。
- クラスターに関連付けられた仮想マシンのユーザーパーミッションの編集。



注記

ロールやパーミッションは、既存のユーザーにのみ割り当てることができます。

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

1.1.2.10. クラスター管理者ロールの概要

クラスター権限ロール

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

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

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

1.1.2.11. ネットワークのシステムパーミッションの管理

システム管理者は **SuperUser** として、管理ポータルをあらゆる面から管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限付き管理者ロールは、特定のリソースに限定して管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対する権利者権限のみ(そのデータセンターのストレージを除く)を持ち、**ClusterAdmin** は割り当てられたクラスターに対する管理者権限のみを持ちます。

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

ネットワーク管理者ロールは以下のアクションを許可します。

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

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

1.1.2.12. ネットワーク管理者およびユーザーロールの概要

ネットワークパーミッションロール

以下の表は、ネットワークの管理に適用される管理者ロールとユーザーロール、および権限を説明しています。

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

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

1.1.2.13. ホストのシステムパーミッションの管理

システム管理者は **SuperUser** として、管理ポータルをあらゆる面から管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限付き管理者ロールは、特定のリソースに限定して管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、

割り当てられたデータセンターに対する権利者権限のみ(そのデータセンターのストレージを除く)を持ち、**ClusterAdmin** は割り当てられたクラスターに対する管理者権限のみを持ちます。

ホスト管理者は、特定のホストのみのシステム管理ロールです。これは、複数のホストを持つクラスターで、各ホストにシステム管理者が必要な場合に有効です。ヘッダーバーの **Configure** ボタンを使用して、環境内の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。

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

1.1.2.14. ホスト管理者ロールの概要

ホストパーミッションロール

以下の表は、ホスト管理に適用される管理者ロールおよび権限を説明しています。

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

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

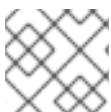
1.1.2.15. ストレージドメインのシステムパーミッションの管理

システム管理者は **SuperUser** として、管理ポータルをあらゆる面から管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限付き管理者ロールは、特定のリソースに限定して管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対する権利者権限のみ(そのデータセンターのストレージを除く)を持ち、**ClusterAdmin** は割り当てられたクラスターに対する管理者権限のみを持ちます。

ストレージ管理者は、特定のストレージドメインのみのシステム管理ロールです。これは、複数のストレージドメインを持つデータセンターで、各ストレージドメインにシステム管理者が必要な場合に有効です。ヘッダーバーの **Configure** ボタンを使用して、環境内のすべてのストレージドメインにストレージ管理者を割り当てます。

ストレージドメイン管理者ロールは、以下のアクションを許可します。

- ストレージドメインの設定の編集。
- ストレージドメインのメンテナンスモードへの切り替え。
- ストレージドメインの削除。



注記

ロールやパーミッションは、既存のユーザーにのみ割り当てることができます。

また、既存のシステム管理者を削除し、新しいシステム管理者を追加すると、ストレージドメインのシステム管理者を変更できます。

1.1.2.16. ストレージ管理者ロールの概要

ストレージドメインパーミッションロール

以下の表は、ストレージドメインの管理に適用される管理者ロールおよび権限を説明しています。

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

ロール	権限	注記
StorageAdmin	ストレージ管理者	特定のストレージドメインを作成、削除、設定、および管理できます。
GlusterAdmin	Gluster Storage 管理者	Gluster ストレージボリュームを作成、削除、設定、および管理できます。

1.1.2.17. 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、管理ポータルをあらゆる面から管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限付き管理者ロールは、特定のリソースに限定して管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対する権利者権限のみ（そのデータセンターのストレージを除く）を持ち、**ClusterAdmin** は割り当てられたクラスターに対する管理者権限のみを持ちます。

仮想マシンプールの管理者は、データセンター内の仮想マシンプールのシステム管理ロールです。このロールは、特定の仮想マシンプール、データセンター、または仮想化環境全体に適用できます。これは、異なるユーザーが特定の仮想マシンプールリソースを管理できるようにするのに役立ちます。

仮想マシンプールの管理者ロールは、以下のアクションを許可します。

- プールの作成、編集、および削除。
- プールからの仮想マシンの追加およびデタッチ。



注記

ロールやパーミッションは、既存のユーザーにのみ割り当てることができます。

1.1.2.18. 仮想マシンプール管理者ロールの概要

プールパーミッションロール

以下の表は、プール管理に適用される管理者ロールおよび権限を説明しています。

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

ロール	権限	注記
VmPoolAdmin	仮想プールのシステム管理者ロール。	仮想プールを作成、削除、および設定できます。仮想プールユーザーの割り当てと削除を行い、仮想マシン上で基本操作を実行できます。
ClusterAdmin	クラスター管理者	特定のクラスター内のすべての仮想マシンプールを使用、作成、削除、および管理できます。

1.1.2.19. 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、管理ポータルをあらゆる面から管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限付き管理者ロールは、特定のリソースに限定して管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、割り当てられたデータセンターに対する権利者権限のみ(そのデータセンターのストレージを除く)を持ち、**ClusterAdmin** は割り当てられたクラスターに対する管理者権限のみを持ちます。

Red Hat Virtualization Manager では、デフォルトの仮想ディスクユーザー ロールが 2 つ提供されますが、デフォルトの仮想ディスク管理者ロールはありません。ユーザー ロールの 1 つである **DiskCreator** ロールは、VM ポータルからの仮想ディスクの管理を可能にします。このロールは、特定の仮想マシン、データセンター、特定のストレージドメイン、または仮想化環境全体に適用することができます。これは、異なるユーザーが異なる仮想リソースを管理できるようにするために役立ちます。

仮想ディスク作成者ロールは、以下のアクションを許可します。

- 仮想マシンまたは他のリソースに関連付けられた仮想ディスクの作成、編集、および削除。
- 仮想ディスクのユーザーパーミッションの編集。



注記

ロールやパーミッションは、既存のユーザーにのみ割り当てることができます。

1.1.2.20. 仮想ディスクユーザー ロールの概要

仮想ディスクユーザー パーミッション ロール

以下の表は、VM ポータルでの仮想ディスクの使用および管理に適用されるユーザー ロールおよび権限を説明しています。

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

ロール	権限	注記
DiskOperator	仮想ディスクユーザー。	仮想ディスクの使用、表示、編集が可能です。仮想ディスクが接続されている仮想マシンを使用するパーミッションを継承します。

ロール	権限	注記
DiskCreator	割り当てられたクラスターまたはデータセンター内の仮想ディスクを作成、編集、管理、および削除できる。	このロールは特定の仮想ディスクには適用されません。Configure ウィンドウで環境全体のユーザーにこのロールを適用します。また、特定のデータセンター、クラスター、またはストレージドメインにこのロールを適用することもできます。

1.1.2.20.1. レガシー SPICE 暗号の設定

SPICE コンソールでは、デフォルトで FIPS 準拠の暗号化を行い、暗号文字列を使用します。デフォルトの SPICE 暗号文字列は **kECDHE+FIPS:kDHE+FIPS:kRSA+FIPS:leNULL:!aNULL** です。

通常、この文字列で十分です。ただし、古いオペレーティングシステムまたは SPICE クライアントの仮想マシンがあり、そのうちのいずれかが FIPS 準拠の暗号化に対応していない場合は、弱い暗号文字列を使用する必要があります。そうしないと、新規クラスターまたは新規ホストを既存のクラスターにインストールし、その仮想マシンへの接続を試みると、接続のセキュリティーエラーが発生します。

Ansible Playbook を使用して暗号文字列を変更できます。

暗号文字列の変更

- Manager マシンで、**/usr/share/ovirt-engine/playbooks** ディレクトリーにファイルを作成します。以下に例を示します。

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

- ファイルに以下を入力し、保存します。

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

- 作成したファイルを実行します。

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

または、変数 **host_deploy_spice_cipher_string** で **--extra-vars** オプションを使用して、Ansible Playbook **ovirt-host-deploy** でホストを再設定することもできます。

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

1.1.3. スケジューリングポリシー

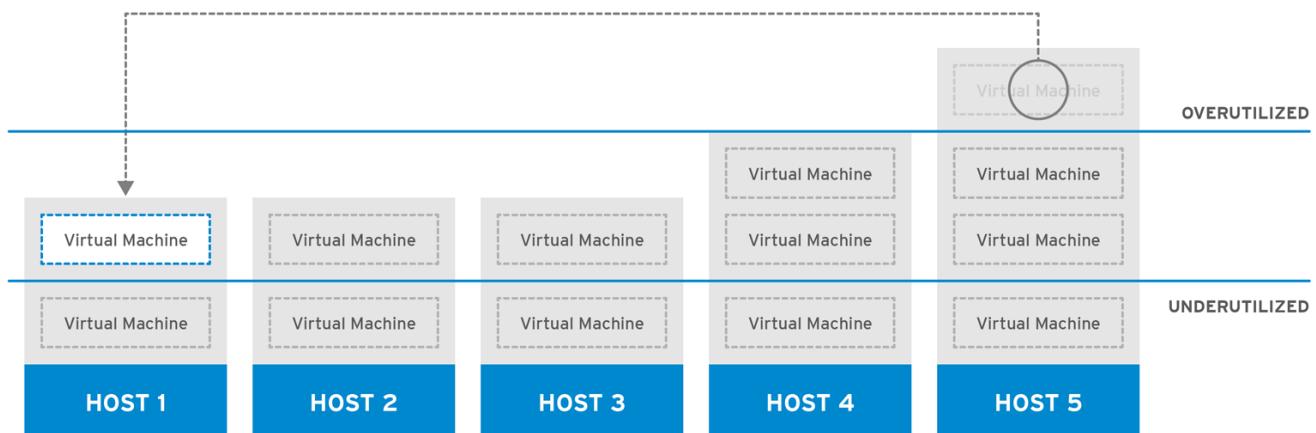
スケジューリングポリシーは、スケジューリングポリシーが適用されるクラスター内のホスト間で仮想マシンが分散されるロジックを定義するルールのセットです。スケジューリングポリシーは、フィルター、重み付け、および負荷分散ポリシーの組み合わせにより、このロジックを決定します。フィルターモジュールはハード強制を適用し、そのフィルターで指定された条件を満たさないホストを除外します。加重モジュールはソフト強制を適用し、仮想マシンが実行できるクラスター内のホストを決定する際に考慮される要因の相対優先度を制御するために使用されます。

Red Hat Virtualization Manager には 5 つのデフォルトスケジューリングポリシー

Evenly_Distributed、**Cluster_Maintenance**、**None**、**Power_Saving**、および **VM_Evenly_Distributed** があります。また、新しいスケジューリングポリシーを定義することで、仮想マシンの配布をきめ細かく制御することができます。スケジューリングポリシーに関わらず、CPU が過負荷状態のホストでは仮想マシンが起動しません。デフォルトでは、ホストの CPU が 5 分間 80% 以上の負荷がかかった場合に過負荷と判断されますが、この値はスケジューリングポリシーを使って変更できます。各スケジューリングポリシーのプロパティーの詳細は、管理ガイドの [スケジューリングポリシー](#) を参照してください。

スケジューリングポリシーの仕組みの詳細は、[How does cluster scheduling policy work?](#) を参照してください。

図1.4 Evenly Distributed スケジューリングポリシー

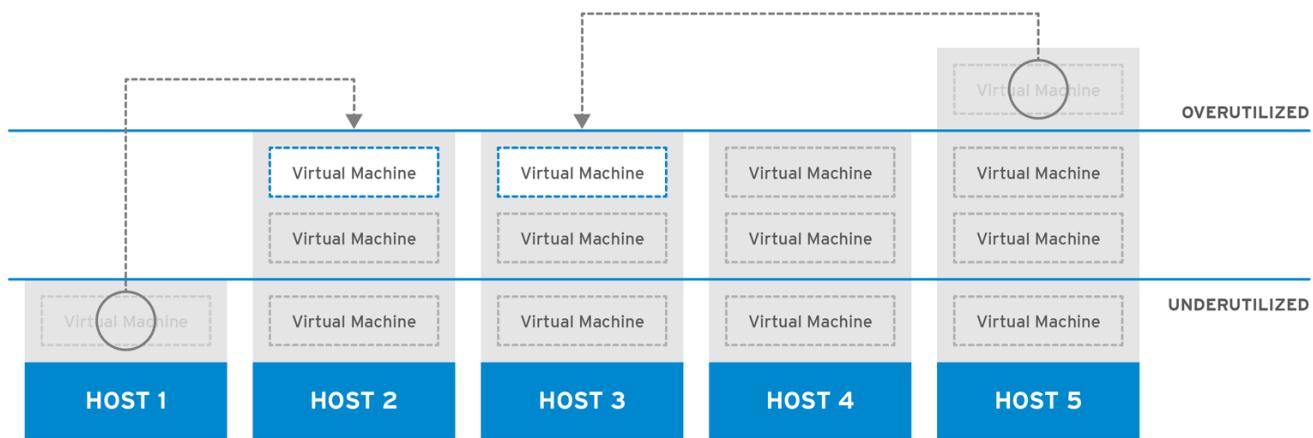


RHV_444396_0417

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

VM_Evenly_Distributed スケジューリングポリシーは、仮想マシンの数に応じて、ホスト間で仮想マシンを均等に配布します。**HighVmCount** よりも多くの仮想マシンを実行しているホストがあり、仮想マシン数が **MigrationThreshold** の範囲外であるホストが少なくとも 1 つ存在する場合、クラスターはアンバランスであると判断されます。

図1.5 Power Saving スケジューリングポリシー



RHV_444396_0417

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

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

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

Cluster_Maintenance スケジューリングポリシーは、メンテナンスタスク時にクラスター内のアクティビティーを制限します。**Cluster_Maintenance** ポリシーが設定されている場合、高可用性仮想マシンを除き、新しい仮想マシンを起動できません。ホストの障害が発生した場合、高可用性仮想マシンが正しく再起動し、どの仮想マシンも移行できます。

1.1.3.1. スケジューリングポリシーの作成

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

手順

1. Administration → Configure をクリックします。
2. Scheduling Policies タブをクリックします。
3. New をクリックします。
4. スケジュールポリシーの Name と Description を入力します。
5. フィルターモジュールを設定します。
 - a. Filter Modules セクションで、Disabled Filters セクションから Enabled Filters セクションに、優先するフィルターモジュールをドラッグアンドドロップしてスケジューリングポリシーに適用します。
 - b. また、特定のフィルターモジュールを First として設定して優先度を最も高くしたり、Last として設定して優先度を最も低くすることもできます。優先度を設定するには、フィル

ターモジュールを右クリックし、Positionにカーソルを合わせ、FirstまたはLastを選択します。

6. 加重モジュールを設定します。

- Weights Modulesセクションで、Disabled WeightsセクションからEnabled Weightsセクションに、優先する加重モジュールをドラッグアンドドロップしてスケジューリングポリシーに適用します。
- 有効な加重モジュールの左側にある+および-ボタンを使用して、これらのモジュールの重みを増減します。

7. ロードバランシングポリシーを指定します。

- Load Balancerセクションのドロップダウンメニューから、スケジューリングポリシーに適用する負荷分散ポリシーを選択します。
- Propertiesセクションのドロップダウンメニューから、スケジューリングポリシーに適用する負荷分散プロパティーを選択し、そのプロパティーの右側にあるtextフィールドを使用して値を指定します。
- +ボタンおよび-ボタンを使用して、プロパティーを追加または削除します。

8. OKをクリックします。

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

以下の表は、New Scheduling Policy および Edit Scheduling Policy ウィンドウで使用できるオプションの詳細を示しています。

表1.12 New Scheduling Policy および Edit Scheduling Policy の設定

フィールド名	説明
Name	スケジューリングポリシーの名前。これは、Red Hat Virtualization Manager のスケジューリングポリシーを参照するために使用される名前です。
Description	スケジューリングポリシーの説明。このフィールドは推奨されますが、必須ではありません。
Filter Modules	<p>クラスター内の仮想マシンが実行できるホストを制御するフィルターセット。フィルターを有効にすると、以下のように、フィルターで指定された条件を満たさないホストが除外されます。</p> <ul style="list-style-type: none"> ● ClusterInMaintenance: 高可用性に設定されていないホストで起動している仮想マシンは、そのホストを除外します。 ● CpuPinning: CPU ピニングの定義を満たさないホスト。 ● Migration: 同じホストへの移行をブロックします。 ● CPUOverloaded:

フィールド名	説明
	<p>OverCommitDurationMinutes で定義された間隔の CPU 使用率がしきい値 (HighUtilization) を超えているホスト。</p> <ul style="list-style-type: none"> ● PinToHost: 仮想マシンが固定されているホスト以外のホスト。 ● CPU-Level: 仮想マシンの CPU トポロジーを満たさないホスト。 ● VmAffinityGroups: 仮想マシンに定義されたアフィニティグループを満たさないホスト。 ● NUMA: リソースにおいて仮想マシン vNUMA ノードに対応できる NUMA ノードを持たないホスト。 ● InClusterUpgrade: 実行しているオペレーティングシステムが、現在仮想マシンが実行しているホストよりも前のバージョンのホスト。 ● MDevice: 必要な仲介デバイス (mDev) を提供しないホスト。 ● Memory: 仮想マシンを実行するために十分なメモリーを持たないホスト。 ● CPU: 仮想マシンに割り当てられた数よりも少ない CPU を持つホスト。 ● HostedEnginesSpares: 指定した数のセルフホスト型エンジンノードに Manager 仮想マシンの領域を確保します。 ● swap: しきい値内にスワップされていないホスト。 ● VM leases ready: ストレージのリースが設定された仮想マシンをサポートしないホスト。 ● VmToHostsAffinityGroups: アフィニティグループのメンバーである仮想マシンに対して指定した条件を満たさないホストのグループ。たとえば、アフィニティグループの仮想マシンは、グループ内のいずれかのホスト上で動作するか、グループから除外された別のホスト上で動作する必要がある、などの条件。 ● HostDevice: 仮想マシンに必要なホストデバイスに対応していないホスト。 ● HA: セルフホスト型エンジン環境内の Manager 用仮想マシンを強制し、正の高可用性スコアを持つホストでのみ実行するようになります。 ● Emulated-Machine: 適切なエミュレートされたマシンをサポートしていないホスト。

フィールド名	説明
	<ul style="list-style-type: none"> ● HugePages: 仮想マシンのメモリーに必要な Huge Page の数を満たさないホスト。 ● Migration-Tsc-Frequency: ホストが現在実行している仮想マシンと同じ TSC 周波数を持つ仮想マシンを持たないホスト。 ● Network: 仮想マシンのネットワークインターフェイスコントローラーで必要なネットワークがインストールされていないホスト、またはクラスターのディスプレイネットワークがインストールされていないホスト。 ● Label: 必要なアフィニティーラベルを持たないホスト。 ● Compatibility-Version: 正しいクラスター互換バージョンのサポートがないホスト。
Weights Modules	<p>仮想マシンを実行できるクラスター内のホストを決定する際に考慮される要因の相対優先度を制御する重みのセット。</p> <ul style="list-style-type: none"> ● VmAffinityGroups: 仮想マシンに定義されたアフィニティーグループに応じて、ホストを重み付けします。この加重モジュールは、あるアフィニティーグループの仮想マシンが、そのアフィニティーグループのパラメーターに応じて、同じホスト上で実行される可能性や、別々のホスト上で実行される可能性を決定します。 ● 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。この重みは、仮想マシンが現在実行されているホストと同じオペレーティングシステムを持つホストよりも前のオペレーティングシステムを持つホストにペナルティーを与えます。これにより、より新しいホストが常に優先されるようになります。 ● OptimalForCpuEvenDistribution: CPU 使用率に応じてホストを重み付けし、CPU 使用率が低いホストを優先します。 ● CPU for high performance VMs: 仮想マシンと同数以上のソケット、コア、スレッドを持つホストを優先します。 ● HA: 高可用性スコアに応じてホストを重み付けします。 ● OptimalForCpuPowerSaving: CPU 使用率に従ってホストを重み付けし、CPU 使用率が高いホストを優先します。 ● OptimalForMemoryPowerSaving: メモリーの使用量に応じてホストを重み付けし、利用可能なメモリーが少ないホストを優先します。

フィールド名	説明
	<ul style="list-style-type: none"> CPU and NUMA pinning compatibility: ピニングの互換性に応じてホストを重み付けします。仮想マシンの vNUMA とピニングの両方が定義されている場合、この重みモジュールは CPU ピニングが vNUMA ピニングと競合しないホストを優先します。 VmToHostsAffinityGroups: 仮想マシンに定義されたアフィニティーグループに応じて、ホストを重み付けします。この重みモジュールは、アフィニティーグループの仮想マシンが、グループ内のホストの1つ、またはグループから除外された別のホスト上で実行される可能性を決定します。 OptimalForEvenGuestDistribution: ホスト上で稼働している仮想マシンの数に応じて、ホストを重み付けします。 OptimalForHaReservation: 高可用性スコアに従ってホストを重み付けします。 OptimalForMemoryEvenDistribution : メモリーの使用量に応じてホストを重み付けし、利用可能なメモリーが多いホストを優先します。 Fit VM to single host NUMA node: 仮想マシンが1つの NUMA ノードに適合するかどうかに応じて、ホストを重み付けします。仮想マシンに vNUMA が定義されていない場合、この重みモジュールは、仮想マシンを単一の物理 NUMA に適合できるホストを優先します。 PreferredHosts: 仮想マシンのセットアップ時に優先的に使用するホストを指定します。
Load Balancer	このドロップダウンメニューでは、適用する負荷分散モジュールを選択できます。負荷分散モジュールは、使用率が高いホストから、使用率が低いホストに仮想マシンを移行するために使用されるロジックを決定します。
Properties	このドロップダウンメニューでは、負荷分散モジュールのプロパティーを追加または削除でき、スケジューリングポリシーに負荷分散モジュールを選択している場合にのみ利用できます。デフォルトではプロパティーは定義されておらず、利用可能なプロパティーは、選択された負荷分散モジュールに固有のプロパティーです。+ よび - ボタンを使用して、負荷分散モジュールにプロパティーを追加または削除します。

1.1.4. インスタンスタイプ

インスタンスタイプを使用して、仮想マシンのハードウェア設定を定義できます。仮想マシンの作成時

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



注記

インスタンスタイプのサポートは非推奨となり、今後のリリースで廃止される予定です。

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

表1.13 事前定義されたインスタンスタイプ

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

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

インスタンスタイプにバインドされる **New Virtual Machine** および **Edit Virtual Machine** ウィンドウのフィールドの横にチェーンリンクイメージ () があります。これらのフィールドの値の1つが変更されると、仮想マシンはインスタンスタイプから切り離され、**Custom** に変更され、チェーンが切れたよう見えます ()。しかし、値が元に戻されると、チェーンは再度リンクし、インスタンスタイプは選択されたものに戻ります。

1.1.4.1. インスタンスタイプの作成

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

手順

1. Administration → **Configure** をクリックします。
2. **Instance Types** タブをクリックします。
3. **New** をクリックします。
4. インスタンスタイプの **Name** および **Description** を入力します。
5. **Show Advanced Options** をクリックし、必要に応じてインスタンスタイプを設定します。New Instance Type ウィンドウに表示される設定は、New Virtual Machine ウィンドウの

設定と同じですが、関連するフィールドのみが表示されます。仮想マシン管理ガイドの [New Virtual Machine](#) および [Edit Virtual Machine](#) ウィンドウの設定の説明を参照してください。

6. **OK** をクリックします。

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

1.1.4.2. インスタンスタイプの編集

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

手順

1. **Administration** → **Configure** をクリックします。
2. **Instance Types** タブをクリックします。
3. 編集するインスタンスタイプを選択します。
4. **Edit** をクリックします。
5. 必要に応じて設定を変更します。
6. **OK** をクリックします。

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

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

1.1.4.3. インスタンスタイプの削除

手順

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

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

1.1.5. MAC アドレスプール

MAC アドレスプールは、各クラスターに割り当てられる MAC アドレスの範囲を定義します。各クラスターに MAC アドレスプールが指定されます。MAC アドレスプールを使用すると、Red Hat Virtualization は MAC アドレスを自動的に生成し、新しい仮想ネットワークデバイスに割り当てることができます。これは、MAC アドレスの重複を防ぐのに役立ちます。MAC アドレスプールは、クラスターに関連するすべての MAC アドレスが、割り当てられた MAC アドレスプールの範囲内にあると、メモリー効率が高くなります。

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



注記

複数の Red Hat Virtualization クラスターがネットワークを共有する場合は、デフォルトの MAC アドレスプールのみに依存しないでください。これは、各クラスターの仮想マシンが同じ範囲の MAC アドレスを使用しようとして競合が発生するためです。MAC アドレスの競合を回避するには、MAC アドレスプールの範囲をチェックして、各クラスターに一意の MAC アドレス範囲が割り当てられていることを確認します。

MAC アドレスプールでは、最後にプールに戻されたアドレスの次に利用可能な MAC アドレスが割り当てられます。範囲内に残されたアドレスがない場合は、範囲の先頭から検索を再開します。1つの MAC アドレスプールに、利用可能な MAC アドレスがある複数の MAC アドレス範囲が定義されている場合、利用可能な MAC アドレスが選択されるのと同じ方法で、受信したリクエストに対して範囲が順次対応します。

1.1.5.1. MAC アドレスプールの作成

新しい MAC アドレスプールを作成できます。

手順

1. Administration → Configure をクリックします。
2. MAC Address Pool タブをクリックします。
3. Add をクリックします。
4. 新しい MAC アドレスプールの Name および Description を入力します。
5. Allow Duplicates チェックボックスを選択し、MAC アドレスをプールで複数回使用できるようにします。MAC アドレスプールでは、重複した MAC アドレスを自動的に使用することはありませんが、duplicates オプションを有効にすると、ユーザーは手動で重複する MAC アドレスを使用できます。



注記

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

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

1.1.5.2. MAC アドレスプールの編集

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

手順

1. Administration → **Configure** をクリックします。
2. **MAC Address Pool** タブをクリックします。
3. 編集する MAC アドレスプールを選択します。
4. **Edit** をクリックします。
5. 必要に応じて **Name**、**Description**、**Allow Duplicates**、および **MAC Address Ranges** フィールドを変更します。



注記

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

6. **OK** をクリックします。

1.1.5.3. MAC アドレスプールのパーミッションの編集

MAC アドレスプールの作成後に、そのユーザーパーミッションを編集できます。ユーザーパーミッションにより、どのデータセンターが MAC アドレスプールを使用できるかが制御されます。新しいユーザーパーミッションを追加する方法については、[ロール](#) を参照してください。

手順

1. Administration → **Configure** をクリックします。
2. **MAC Address Pool** タブをクリックします。
3. 必要な MAC アドレスプールを選択します。
4. MAC アドレスプールのユーザーパーミッションを編集します。
 - ユーザーパーミッションを MAC アドレスプールに追加するには、以下を実行します。

- a. **Configure** ウィンドウの下にあるユーザー一覧ペインで **Add** をクリックします。
 - b. 必要なユーザーを検索して選択します。
 - c. **Role to Assign** ドロップダウンリストから必要なロールを選択します。
 - d. **OK** をクリックしてユーザー一覧ペインを追加します。
- ユーザー一覧ペインを MAC アドレスプールから削除するには、以下を実行します。
 - a. **Configure** ウィンドウの下にあるユーザー一覧ペインで、削除するユーザー一覧ペインを選択します。
 - b. ユーザー一覧ペインを削除するには、**Remove** をクリックします。

1.1.5.4. MAC アドレスプールの削除

作成した MAC アドレスプールがクラスターに関連付けられていない場合は削除できますが、デフォルトの MAC アドレスプールは削除できません。

手順

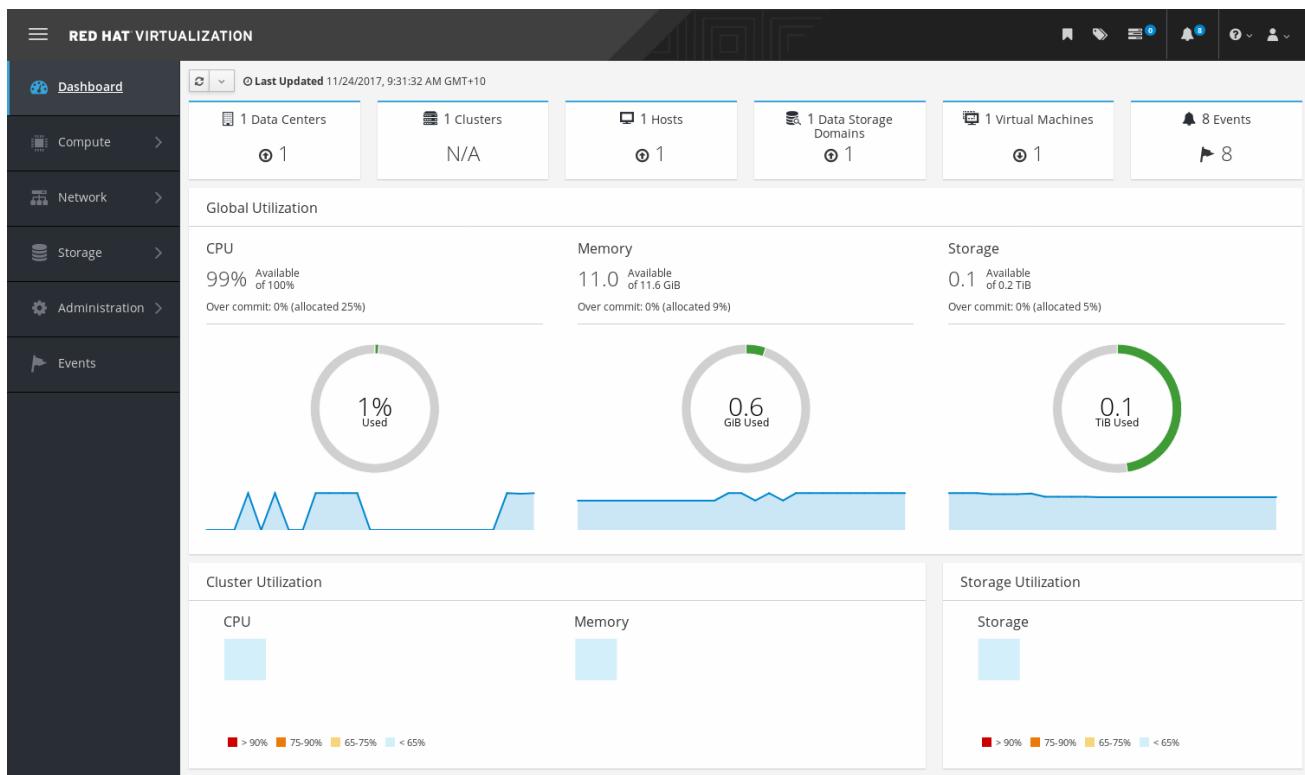
1. Administration → **Configure** をクリックします。
2. **MAC Address Pool** タブをクリックします。
3. 削除する MAC アドレスプールを選択します。
4. **Remove** をクリックします。
5. **OK** をクリックします。

1.2. ダッシュボード

ダッシュボードは、Red Hat Virtualization のリソースと使用率の概要を表示することで、Red Hat Virtualization のシステム状態の概要を提供します。この概要により、問題を警告することができ、問題領域を分析できます。

ダッシュボードの情報は、Data Warehouse からはデフォルトで 15 分ごと、Manager API からはデフォルトで 15 秒ごと、またはダッシュボードが更新されるたびに更新されます。ダッシュボードは、ユーザーが他のページから戻ったときや、手動でリフレッシュしたときに更新されます。ダッシュボードは自動的に更新されません。イベントリーカードの情報は Manager API から提供され、利用状況の情報は Data Warehouse から提供されます。ダッシュボードは、UI プラグインコンポーネントとして実装されており、Manager と一緒に自動的にインストールおよびアップグレードされます。

図1.6 ダッシュボード



1.2.1. 前提条件

ダッシュボードを使用するには、Data Warehouse がインストールされ、設定されている必要があります。Data Warehouse ガイドの [Data Warehouse のインストールおよび設定](#) を参照してください。

1.2.2. グローバルイベントトリー

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

図1.7 グローバルイベントトリー



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

表1.14 リソースの状況

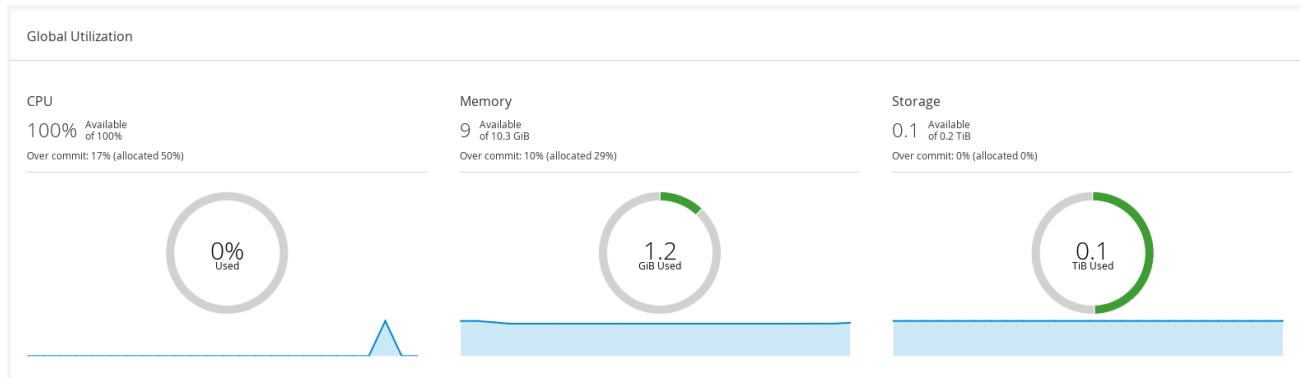
アイコン	状態
✓	Red Hat Virtualization に該当するリソースは追加されていません。

アイコン	状態
	<p>警告ステータスを持つリソースの数量を表示します。アイコンをクリックすると、該当ページに移動し、検索対象は警告状態のリソースに限定されます。検索の制限は、リソースごとに異なります。</p> <ul style="list-style-type: none"> ● Data Centers: 検索対象は、稼働していないデータセンターまたは応答していないデータセンターに限られます。 ● Gluster Volumes: 検索対象は、開始中、一時停止中、移行中、待機中、中断中、または停止中の Gluster ボリュームに限定されます。 ● Hosts: 検索対象は、未割り当て、メンテナنسモード、インストール中、再起動中、メンテナンスの準備中、承認待ち、または接続中のホストに限定されます。 ● Storage Domains: 検索対象となるのは、初期化されていない、アタッチされていない、非クティブでない、メンテナансモード、メンテナンスの準備中、デタッチ中、またはアクティベート中のストレージドメインに限られます。 ● Virtual Machines: 検索対象は、開始中、一時停止中、移行中、待機中、中断中、または停止中の仮想マシンに限定されます。 ● Events: 重大度が警告のイベントに限定して検索を行います。
	<p>up ステータスを持つリソースの番号を表示します。アイコンをクリックすると、該当ページに移動し、検索対象は up 状態のリソースに限定されます。</p>

アイコン	状態
	<p>down 状態のリソースの番号を表示します。アイコンをクリックすると、該当ページに移動し、検索対象は down 状態のリソースに限定されます。検索の制限は、リソースごとに異なります。</p> <ul style="list-style-type: none"> ● Data Centers: 検索対象は、初期化されていない、メンテナンスモード、または down ステータスのデータセンターに限られます。 ● Gluster Volumes: 検索対象は、デタッチされているまたは非アクティブな Gluster ボリュームに限られます。 ● Hosts: 検索対象は、反応しない、エラーが発生している、インストールエラーが発生している、動作していない、初期化中、または down 状態のホストに限られます。 ● Storage Domains: 検索対象は、デタッチされているまたは非アクティブなストレージドメインに限られます。 ● Virtual Machines: 検索対象は、down 状態、応答していない、または再起動中の仮想マシンに限られます。
images:images/Dashboard_Alert.png[title="Alert icon"]	アラートステータスを持つイベントの数を表示します。アイコンをクリックすると Events に移動しますが、検索対象は深刻度が警告のイベントに限定されます。
images:images/Dashboard_Error.png[title="Error icon"]	エラーステータスを持つイベントの数を表示します。アイコンをクリックすると Events に移動しますが、検索対象は深刻度がエラーのイベントに限定されます。

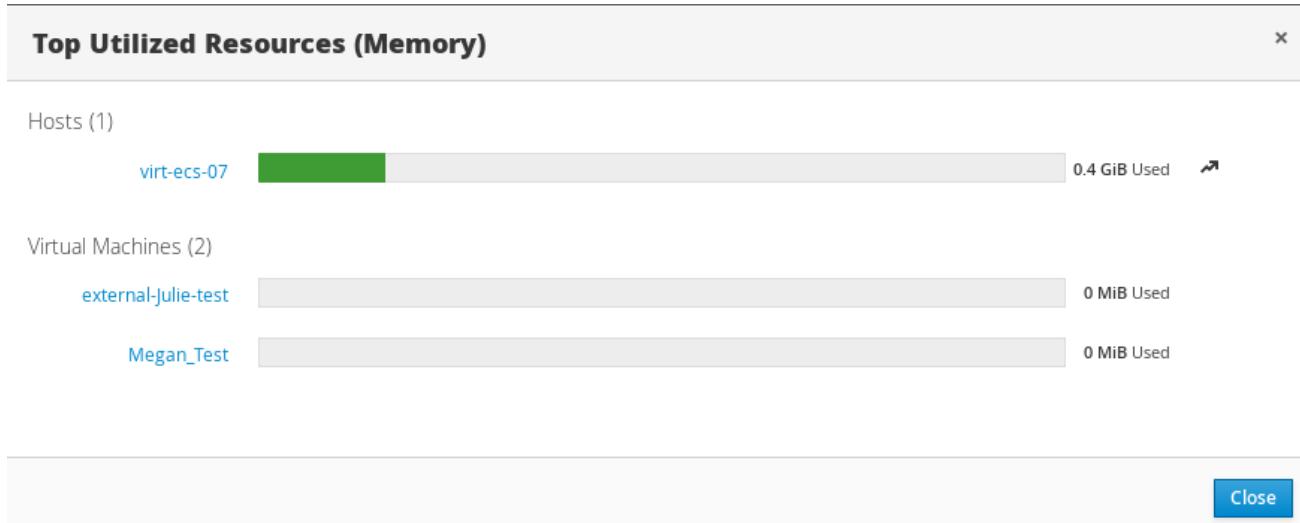
1.2.3. グローバルでの活用

Global Utilization セクションでは、CPU、Memory、Storage のシステム使用状態が表示されます。

図1.8 グローバルでの活用

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

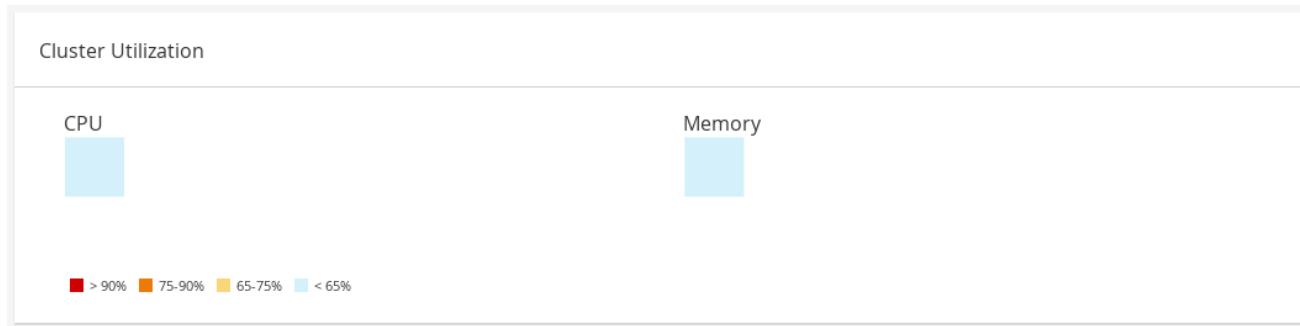
1.2.3.1. 最も使用されているリソース

図1.9 最も使用されているリソース(メモリー)

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

1.2.4. クラスターの活用

Cluster Utilizationセクションは、CPUとメモリーのクラスター使用率をヒートマップで表示します。

図1.10 クラスターの活用

1.2.4.1. CPU

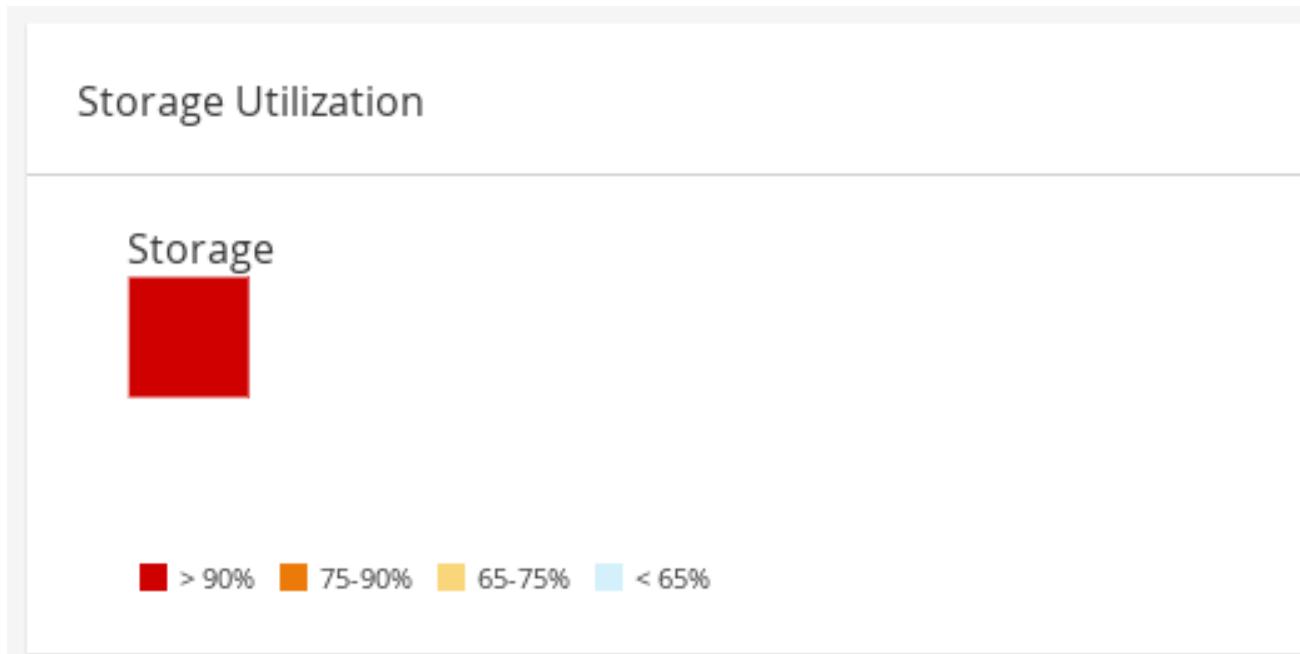
過去 24 時間の CPU 平均使用率を示す特定クラスターの CPU 使用率のヒートマップ。ヒートマップにカーソルを合わせると、クラスター名が表示されます。ヒートマップをクリックすると、Compute → Hosts に移動し、特定のクラスターの検索を CPU 使用率でソートした結果が表示されます。クラスターによる CPU の使用率を計算するために使用される式は、クラスターのホスト CPU 使用率の平均です。これは、クラスターによる CPU の合計平均使用率を出すために、過去 24 時間の各ホストの CPU 使用率の平均値を用いて算出されます。

1.2.4.2. メモリー

過去 24 時間のメモリー平均使用率を示す特定クラスターのメモリー使用率のヒートマップ。ヒートマップにカーソルを合わせると、クラスター名が表示されます。ヒートマップをクリックすると、Compute → Hosts に移動し、特定のクラスターの検索をメモリー使用率でソートした結果が表示されます。クラスターによるメモリー使用率を計算するために使用される式は、クラスターのメモリー使用率の合計 (GB 単位) です。これは、クラスターによるメモリー合計平均使用率を出すために、過去 24 時間の各ホストの平均メモリー使用率を用いて算出されます。

1.2.5. ストレージの活用

Storage Utilization セクションには、ヒートマップでストレージ使用率が表示されます。

図1.11 ストレージの活用

ヒートマップは、過去 24 時間のストレージ平均利用率を表します。クラスターによるストレージ使用

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

1.3. 検索

1.3.1. 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、何千ものリソースを管理することができます。検索を行うには、各リソースのメインページにある検索バーに、検索クエリー(フリーテキストまたは構文ベース)を入力します。検索条件をブックマークとして保存しておけば、検索結果を必要とするたびに検索条件を再入力する必要はありません。検索では大文字小文字の区別はありません。

1.3.2. 検索構文と例

Red Hat Virtualization リソースの検索クエリーの構文は以下のとおりです。

result type: {criteria} [sortby sort_spec]

構文の例

以下の例は、検索クエリーの使用方法と、Red Hat Virtualization が検索クエリーの構築を支援する方法を理解するのに役立ちます。

表1.15 検索クエリーの例

例	結果
Hosts: Vms.status = up page 2	稼働中の仮想マシンを実行しているすべてのホストのリストの 2 ページ目を表示します。
Vms: domain = qa.company.com	指定されたドメインで稼働しているすべての仮想マシンの一覧を表示します。
Vms: users.name = Mary	ユーザー名が Mary のユーザーに属する全仮想マシンの一覧を表示します。
Events: severity > normal sortby time	重大度が Normal よりも高いすべての Events の一覧を表示します。

1.3.3. 自動完了の検索

管理ポータルは、有効で強力な検索クエリーの作成に役立つ自動補完を提供します。検索クエリーの各部分を入力すると、検索の次の部分を選択するドロップダウンリストが、Search Bar の下に開きます。一覧から選択して検索の次の部分を入力/選択するか、オプションを無視して手動でクエリーを入力できます。

以下の表では、管理ポータルでクエリーを構築する際に自動補完がどのように機能するか、例を挙げて説明しています。

Hosts: Vms.status = down

表1.16 自動補完を使用した検索クエリーの例

入力	表示されるリスト項目	アクション
h	Hosts (1つのオプションのみ)	Hosts を選択、または Hosts を入力
Hosts:	すべてのホストプロパティー	vを入力
Hosts: v	vで始まるホストプロパティー	Vms を選択、または Vms を入力
Hosts: Vms	すべての仮想マシンプロパティー	sを入力
Hosts: Vms.s	sで始まるすべての仮想マシンプロパティー	status を選択、または status を入力
Hosts: Vms.status	=	=を選択/入力
	!=	
Hosts: Vms.status =	すべてのステータス値	downを選択/入力

1.3.4. 検索結果タイプのオプション

結果タイプを使用すると、以下のタイプのリソースを検索できます。

- **Vms**、仮想マシンのリスト。
- **Host**、ホストのリスト。
- **Pools**、プールのリスト。
- **Template**、テンプレートのリスト。
- **Events**、イベントのリスト。
- **Users**、ユーザーのリスト。
- **Cluster**、クラスターのリスト。
- **DataCenter**、データセンターのリスト。
- **Storage**、ストレージドメインのリスト。

各タイプのリソースには、一意のプロパティーセットと、関連付けられたその他のリソースタイプのセットがあるため、各検索タイプには、有効な構文の組み合わせがあります。自動補完機能を使用すると、有効なクエリーも簡単に作成できます。

1.3.5. 検索基準

クエリーのコロンの後に検索条件を指定できます。{criteria} の構文は以下のようになります。

<prop><operator><value>

または

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

例

以下の表は、構文の部分を示しています。

表1.17 検索基準の例

部分	説明	値	例	注記
prop	検索対象リソースのプロパティ。リソース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) にすることもできます。	検索対象を、特定のプロパティーを持つオブジェクトに制限します。たとえば、status プロパティーでオブジェクトを検索します。	Status	該当なし
obj-type	検索対象のリソースに関連付けることができるリソースタイプ。	データセンターや仮想マシンなどのシステムオブジェクトです。	Users	該当なし
operator	比較演算子。	= != (等しくない) > < >= <=	該当なし	値オプションはプロパティーによって異なります。

部分	説明	値	例	注記
Value	その式が何と比較されるか。	文字列 Integer Ranking Date (Regional Settings に応じた書式設定)	Jones 256 normal 	<ul style="list-style-type: none"> ワイルドカードは文字列内で使用できます。 "" (間にスペースがない 2つの引用符のセット) は、初期化されていない (空の) 文字列を表すために使用できます。 スペースが含まれる文字列または日付を二重引用符で囲む必要があります

1.3.6. 検索: 複数の基準およびワイルドカード

ワイルドカードは文字列の構文の **<value>** 部分で使用できます。たとえば、m で始まる全ユーザーを検索するには、**m*** を入力します。

ブール演算子の **AND** および **OR** を使用して、2つの基準を持つ検索を実行できます。以下に例を示します。

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

このクエリーは、名前が "m" で始まるユーザーに対して実行中の仮想マシンをすべて返します。

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

このクエリーは、名前が "m" で始まるユーザーに対して "paris-loc" でタグ付けされたすべての仮想マシンを返します。

AND または **OR** を使用せずに 2つの基準を指定した場合、**AND** が暗黙的に指定されます。**AND** は **OR** よりも優先され、**OR** は暗黙の **AND** よりも優先されます。

1.3.7. 検索: 検索順序の決定

返される情報の並び替え順序は、**sortby** を使用して決定できます。並べ替え方向 (昇順は **asc**、降順は **desc**) を含めることができます。

以下に例を示します。

events: severity > normal sortby time desc

このクエリーは、重大度が Normal よりも大きいすべての Events を時刻でソートして返します (降順)。

1.3.8. データセンターの検索

以下の表は、データセンターのすべての検索オプションを示しています。

表1.18 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の)	タイプ	説明 (参照)
Clusters.clusters-prop	プロパティータイプによります。	データセンターに関連付けられたクラスターのプロパティー。
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	List	データセンターの可用性。
sortby	List	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Datacenter: type = nfs and status != up

この例では、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の一覧を返します。

1.3.9. クラスターの検索

以下の表は、クラスターのすべての検索オプションを説明しています。

表1.19 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の)	タイプ	説明 (参照)
Datacenter.datacenter-prop	プロパティータイプによります。	クラスターに関連付けられたデータセンターのプロパティー。
Datacenter	文字列	クラスターが属するデータセンター。

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
name	文字列	ネットワーク上のクラスターを識別する一意の名前。
description	文字列	クラスターの説明。
initialized	文字列	クラスターのステータスを示す True または False。
sortby	List	返された結果をリソースプロパティの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Clusters: initialized = true or name = Default

この例では、初期化されたクラスターまたは Default という名前のクラスターの一覧を返します。

1.3.10. ホストの検索

以下の表は、ホストの全検索オプションを示しています。

表1.20 ホストの検索

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
Vms.Vms-prop	プロパティータイプによります。	ホストに関連付けられた仮想マシンのプロパティ。
Templates.templates-prop	プロパティータイプによります。	ホストに関連付けられたテンプレートのプロパティ。
Events.events-prop	プロパティータイプによります。	ホストに関連付けられたイベントのプロパティ。
Users.users-prop	プロパティータイプによります。	ホストに関連付けられたユーザーのプロパティ。
name	文字列	ホストの名前。
status	List	ホストの可用性。

プロパティ（リソースまたはリソースタイプの）	タイプ	説明（参照）
external_status	文字列	外部システムおよびプラグインによって報告されるホストのヘルステータス。
cluster	文字列	ホストが属するクラスター。
address	文字列	ネットワーク上のホストを識別する一意の名前。
cpu_usage	Integer	使用される処理能力の割合。
mem_usage	Integer	使用されるメモリーの割合。
network_usage	Integer	ネットワーク使用率の割合。
load	Integer	特定のタイムスライスで、プロセッサーごとに run-queue で実行されるのを待っているジョブ。
version	Integer	オペレーティングシステムのバージョン番号。
cpus	Integer	ホスト上の CPU 数。
memory	Integer	使用可能なメモリーの量。
cpu_speed	Integer	CPU の処理速度。
cpu_model	文字列	CPU のタイプ。
active_vms	Integer	現在実行中の仮想マシンの数。
migrating_vms	Integer	現在移行中の仮想マシンの数。
committed_mem	Integer	コミットされたメモリーの割合
tag	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。
sortby	List	返された結果をリソースプロパティの1つで並べ替えます。

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
page	Integer	表示する結果のページ番号。

例

Hosts: cluster = Default and Vms.os = rhel6

この例では、Default クラスターの一部であるホストの一覧と、Red Hat Enterprise Linux 6 オペレーティングシステムを実行するホスト仮想マシンを返します。

1.3.11. ネットワークの検索

以下の表は、ネットワークの全検索オプションを説明しています。

表1.21 ネットワークの検索

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
Cluster_network.clusternetwork-prop	プロパティータイプによります。	ネットワークに関連付けられたクラスターのプロパティ。
Host_Network.hostnetwork-prop	プロパティータイプによります。	ネットワークに関連付けられたホストのプロパティ。
name	文字列	ネットワークを識別するための人が判読可能な名前。
description	文字列	ネットワークを記述するキーワードまたはテキスト。オプションでネットワークの作成時に使用されます。
vlanid	Integer	ネットワークの VLAN ID。
stp	文字列	Spanning Tree Protocol (STP) がネットワークで有効か無効かを示します。
mtu	Integer	論理ネットワークの最大伝送単位。
vmnetwork	文字列	ネットワークが仮想マシントラフィックのみに使用されているかどうか。
datacenter	文字列	ネットワークが接続されているデータセンター。

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
sortby	List	返された結果をリソースプロパティの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Network: mtu > 1500 and vmnetwork = true

この例では、最大転送単位が 1500 バイトを超え、仮想マシンのみが使用するように設定されているネットワークの一覧を返します。

1.3.12. ストレージの検索

以下の表は、ストレージのすべての検索オプションを説明しています。

表1.22 ストレージの検索

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
Hosts.hosts-prop	プロパティタイプによります。	ストレージに関連付けられたホストのプロパティー。
Clusters.clusters-prop	プロパティタイプによります。	ストレージに関連付けられたクラスターのプロパティー。
name	文字列	ネットワーク上のストレージを識別する一意の名前。
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報告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。
type	文字列	ストレージのタイプ。
free-size	Integer	空きストレージのサイズ (GB)。
used-size	Integer	使用されるストレージの容量 (GB)。

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
total_size	Integer	利用可能なストレージの合計量 (GB)。
committed	Integer	コミットされたストレージの量 (GB)。
sortby	List	返された結果をリソースプロパティの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

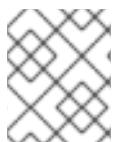
例

Storage: free_size > 6 GB and total_size < 20 GB

この例では、空き領域が 6 GB を超えるストレージの一覧または、合計ストレージ容量が 20 GB 未満のストレージの一覧を返します。

1.3.13. ディスクの検索

以下の表は、ディスクの全検索オプションを示しています。



注記

Disk Type および **Content Type** フィルターオプションを使用して、表示される仮想ディスクの数を減らすことができます。

表1.23 ディスクの検索

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
Datacenters.datacenters-prop	プロパティータイプによります。	ディスクに関連付けられたデータセンターのプロパティ。
Storages.storages-prop	プロパティータイプによります。	ディスクに関連付けられたストレージのプロパティ。
alias	文字列	ネットワーク上のストレージを識別する人が判読可能な名前。
description	文字列	ディスクを記述するキーワードまたはテキスト。オプションでディスクの作成時に使用されます。
provisioned_size	Integer	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の)	タイプ	説明(参照)
size	Integer	ディスクのサイズ。
actual_size	Integer	ディスクに割り当てられる実際のサイズ。
creation_date	Integer	ディスクが作成された日付。
bootable	文字列	ディスクを起動できるかどうか。有効な値は 0 、 1 、 yes 、 no のいずれかです。
shareable	文字列	ディスクを一度に複数の仮想マシンにアタッチできるかどうか。有効な値は 0 、 1 、 yes 、 no のいずれかです。
format	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	Integer	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	仮想ディスクで強制されるクォータの名前。
sortby	List	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Disk: format = cow and provisioned_size > 8

この例では、QCOW 形式の仮想ディスクの一覧と、8 GB を超える割り当て済みのディスクサイズを返します。

1.3.14. ボリュームの検索

以下の表は、ボリュームのすべての検索オプションを説明しています。

表1.24 ボリュームの検索

プロパティー(リソースまたはリソースタイプの)	タイプ	説明(参照)
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。
Cluster.cluster-prop	プロパティータイプ(例: name、description、comment、architecture)による	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。
name	文字列	ボリュームを識別する、人が判読可能な名前。
type	文字列	distribute、replicate、distributed_replicate、stripe、またはdistributed_stripe のいずれか。
transport_type	Integer	TCP または RDMA のいずれか。
replica_count	Integer	レプリカの数。
stripe_count	Integer	ストライプの数。
status	文字列	ボリュームのステータス。Up または Down のいずれかです。
sortby	List	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Volume: transport_type = rdma and stripe_count >= 2

この例では、トランSPORTタイプが RDMA に設定され、ストライプが 2 つ以上あるボリュームのリストを返します。

1.3.15. 仮想マシンの検索

以下の表は、仮想マシンのすべての検索オプションを説明しています。



注記

現時点では、Network Label、Custom Emulated Machine および Custom CPU Type プロパティはサポートされていない検索プロパティです。

表1.25 仮想マシンの検索

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
Hosts.hosts-prop	プロパティータイプによります。	仮想マシンに関連付けられたホストのプロパティ。
Templates.templates-prop	プロパティータイプによります。	仮想マシンに関連付けられたテンプレートのプロパティ。
Events.events-prop	プロパティータイプによります。	仮想マシンに関連付けられたイベントのプロパティ。
Users.users-prop	プロパティータイプによります。	仮想マシンに関連付けられたユーザーのプロパティ。
Storage.storage-prop	プロパティータイプによります。	仮想マシンに関連付けられたストレージデバイスのプロパティ。
Vnic.vnic-prop	プロパティータイプによります。	仮想マシンに関連付けられたvNIC のプロパティ。
name	文字列	仮想マシンの名前。
status	List	仮想マシンの可用性
ip	Integer	仮想マシンのIP アドレス。
uptime	Integer	仮想マシンが実行されている期間(分単位)。
domain	文字列	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されたオペレーティングシステム。
creationdate	Date	仮想マシンが作成された日付。
address	文字列	ネットワーク上の仮想マシンを識別する一意の名前。
cpu_usage	Integer	使用される処理能力の割合。

プロパティ（リソースまたはリソースタイプの）	タイプ	説明（参照）
mem_usage	Integer	使用されるメモリーの割合。
network_usage	Integer	使用されるネットワークの割合。
memory	Integer	定義された最大メモリー。
apps	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	List	仮想マシンが属するクラスター。
pool	List	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	List	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	List	仮想マシンタイプ（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オータの名前。
description	文字列	仮想マシンを記述するキーワードまたはテキスト。オプションとして、仮想マシンの作成時に使用されます。
sortby	List	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。
next_run_configuration_exists	Boolean	仮想マシンに保留中の設定変更があります。

例

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

この例では、ベーステンプレート名が **Win** で始まり、任意のユーザーに割り当てられている仮想マシンの一覧を返します。

例

Vms: cluster = Default and os = windows7

この例では、**Default** クラスターに属し、Windows 7 を実行している仮想マシンの一覧を返します。

1.3.16. プールの検索

以下の表は、プールの全検索オプションを示しています。

表1.26 プールの検索

プロパティー (リソースまたはリソースタイプの)	タイプ	説明 (参照)
name	文字列	プールの名前。
description	文字列	プールの説明。
type	List	プールのタイプ。
sortby	List	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Pools: type = automatic

この例では、タイプが **automatic** のプールの一覧を返します。

1.3.17. テンプレートの検索

以下の表は、テンプレートの全検索オプションを示しています。

表1.27 テンプレートの検索

プロパティー (リソースまたはリソースタイプの)	タイプ	説明 (参照)
Vms.Vms-prop	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。

プロパティ（リソースまたはリソースタイプの）	タイプ	説明（参照）
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。
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。
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	Integer	テンプレートが作成された日付。 日付の形式は mm/dd/yy です。
childcount	Integer	テンプレートから作成された仮想マシンの数。
mem	Integer	定義されたメモリー。
description	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	List	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

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

この例では、テンプレートから派生した仮想マシンで重大度が Normal 以上のイベントが発生し、かつ仮想マシンが引き続き実行されているテンプレートの一覧が返されます。

1.3.18. ユーザーの検索

以下の表は、ユーザーの全検索オプションを説明しています。

表1.28 ユーザーの検索

プロパティ（リソースまたはリソースタイプの）	タイプ	説明（参照）
Vms.Vms-prop	プロパティータイプによります。	ユーザーに関連付けられた仮想マシンのプロパティ。
Hosts.hosts-prop	プロパティータイプによります。	ユーザーに関連付けられたホストのプロパティ。
Templates.templates-prop	プロパティータイプによります。	ユーザーに関連付けられたテンプレートのプロパティ。
Events.events-prop	プロパティータイプによります。	ユーザーに関連するイベントのプロパティ。
name	文字列	ユーザーの名前。
lastname	文字列	ユーザーの名字。
username	文字列	ユーザーの一意の名前。
department	文字列	ユーザーが属する部門。
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	ユーザーの状態。
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	List	返された結果をリソースプロパティの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

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

この例では、仮想マシンで重大度が Normal よりも高いイベントが発生し、かつ仮想マシンがまだ稼働している場合や、ユーザーの仮想マシンが一時停止している場合のユーザーの一覧を返します。

1.3.19. イベントの検索

以下の表は、イベントの検索に使用できるすべての検索オプションを説明しています。自動補完は、必要に応じて多くのオプションに対して提供されます。

表1.29 イベントの検索

プロパティー(リソースまたはリソースタイプの)	タイプ	説明(参照)
Vms.Vms-prop	プロパティータイプによります。	イベントに関連付けられた仮想マシンのプロパティー。
Hosts.hosts-prop	プロパティータイプによります。	イベントに関連付けられたホストのプロパティー。
Templates.templates-prop	プロパティータイプによります。	イベントに関連付けられたテンプレートのプロパティー。
Users.users-prop	プロパティータイプによります。	イベントに関連付けられたユーザーのプロパティー。
Clusters.clusters-prop	プロパティータイプによります。	イベントに関連付けられたクラスターのプロパティー。
Volumes.Volumes-prop	プロパティータイプによります。	イベントに関連付けられたボリュームのプロパティー。
type	List	イベントのタイプ。
severity	List	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	List	イベントが発生した日。
username	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の)	タイプ	説明(参照)
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	Integer	イベントの識別番号。
sortby	List	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

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

この例では、ホスト **gonzo.example.com** で実行中の **testdesktop** という名前の仮想マシンで発生したイベントの一覧を返します。

1.4. ブックマーク

1.4.1. クエリー文字列をブックマークとして保存

ブックマークは、検索クエリーを記憶し、他のユーザーと共有するために使用できます。

手順

1. 検索バーに検索クエリーを入力し、検索を実行します。
2. 検索バーの右側にある星型の **Bookmark** ボタンをクリックします。これにより、**New Bookmark** ウィンドウが開きます。
3. ブックマークの **Name** を入力します。
4. 必要に応じて **Search string** フィールドを編集します。
5. **OK** をクリックします。

ヘッダーバーの **Bookmarks** アイコン()をクリックして、ブックマークを見つけて選択します。

1.4.2. ブックマークの編集

ブックマークの名前および検索文字列を変更できます。

手順

1. ヘッダーバーの **Bookmarks** アイコン () をクリックします。
2. ブックマークを選択し、**Edit** をクリックします。
3. 必要に応じて **Name** および **Search string** フィールドを変更します。
4. **OK** をクリックします。

1.4.3. ブックマークの削除

ブックマークが必要なくなったら、その設定を削除します。

手順

1. ヘッダーバーの **Bookmarks** アイコン () をクリックします。
2. ブックマークを選択し、**Remove** をクリックします。
3. **OK** をクリックします。

1.5. タグ

1.5.1. タグを使用して Red Hat Virtualization とのやり取りをカスタマイズ

Red Hat Virtualization プラットフォームをセットアップし、要件に合わせて設定したら、タグを使用してカスタマイズできます。タグを使用すると、システムリソースをグループまたはカテゴリーに分類できます。これは、仮想化環境に多くのオブジェクトが存在し、管理者が特定のオブジェクトセットに集中したい場合に便利です。

このセクションでは、タグの作成と編集、ホストまたは仮想マシンへの割り当て、タグを基準として使用した検索などの方法を説明します。タグは、企業のニーズに合わせて、構造に一致する階層に配置できます。

管理ポータルのタグを作成、変更、および削除するには、ヘッダーバーの **Tags** アイコン () をクリックします。

1.5.2. タグの作成

タグを作成し、そのタグを使用して検索結果を絞り込むことができます。

手順

1. ヘッダーバーの **Tags** アイコン () をクリックします。
2. **Add** をクリックして新規タグを作成するか、タグを選択して **New** をクリックし、子孫タグを作成します。

3. 新規タグの **Name** および **Description** を入力します。

4. **OK** をクリックします。

1.5.3. タグの変更

タグの名前と説明を編集できます。

タグの変更

1. ヘッダーバーの **Tags** アイコン () をクリックします。
2. 変更するタグを選択し、**Edit** をクリックします。
3. 必要に応じて **Name** および **Description** フィールドを変更します。
4. **OK** をクリックします。

1.5.4. タグの削除

タグが不要になったら、それを削除します。

手順

1. ヘッダーバーの **Tags** アイコン () をクリックします。
2. 削除するタグを選択し、**Remove** をクリックします。タグを削除すると、そのタグのすべての子孫も削除されることを警告するメッセージが表示されます。
3. **OK** をクリックします。

タグとその子孫をすべて削除しました。タグは、アタッチされたすべてのオブジェクトからも削除されます。

1.5.5. オブジェクトに対するタグの追加および削除

ホスト、仮想マシン、およびユーザーにタグを割り当てたり、削除したりできます。

手順

1. タグを割り当てる、または解除するオブジェクトを選択します。
2. **More Actions** () をクリックしてから **Assign Tags** をクリックします。
3. チェックボックスを選択してタグをオブジェクトに割り当てるか、選択を解除してオブジェクトからタグの割り当てを解除します。
4. **OK** をクリックします。

指定したタグが、選択したオブジェクトのカスタムプロパティーとして追加または削除されます。

1.5.6. タグを使用したオブジェクトの検索

tag プロパティーとしてタグを使用し、検索条件として目的の値または値のセットを使用して、検索クエリーを入力します。

指定された基準でタグ付けされたオブジェクトは結果リストに表示されます。



注記

tag をプロパティーとして使用し、不等式演算子 (!=、たとえば、**Host: Vms.tag!=server1**) を使用してオブジェクトを検索する場合、結果リストにタグなしオブジェクトは含まれません。

1.5.7. タグを使用したホストのカスタマイズ

タグを使用してホストに関する情報を保存できます。その後、タグに基づいてホストを検索できます。検索の詳細は、[検索](#) を参照してください。

手順

1. Compute → Hosts をクリックし、ホストを選択します。
2. More Actions (⋮) をクリックしてから Assign Tags をクリックします。
3. 該当するタグのチェックボックスを選択します。
4. OK をクリックします。

ホストに関する検索可能な追加情報がタグとして追加されます。

第2章 リソースの管理

2.1. QOS (QUALITY OF SERVICE)

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

2.1.1. ストレージ QoS

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

2.1.1.1. ストレージ QoS エントリーの作成

手順

1. Compute → Data Centers をクリックします。
2. データセンターの名前をクリックします。詳細ビューが開きます。
3. QoS タブをクリックします。
4. Storage で、New をクリックします。
5. QoS Name と QoS エントリーの Description を入力します。
6. 次のいずれかのラジオボタンをクリックして、Throughput Quality of Service を指定します。
 - None
 - Total - MB/s フィールドに最大許容合計スループットを入力します。
 - Read/Write - 左の MB/s フィールドに読み取り操作の最大許容スループットを入力し、右の MB/s フィールドに書き込み操作の最大許容スループットを入力します。
7. 次のいずれかのラジオボタンをクリックして、入出力 (IOps) の QoS を指定します。
 - None
 - Total - IOps フィールドに1秒あたりの入出力操作の最大許容数を入力します。
 - Read/Write - 左の IOps フィールドに1秒あたりの入力操作の最大許容数を入力し、右の IOps フィールドに1秒あたりの出力操作の最大許容数を入力します。
8. OK をクリックします。

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

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

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

手順

1. Compute → Data Centers をクリックします。
2. データセンターの名前をクリックします。 詳細ビューが開きます。
3. QoS タブをクリックします。
4. Storage でストレージの QoS エントリーを選択し、Remove をクリックします。
5. OK をクリックします。

そのエントリーに基づくディスクプロファイルが存在する場合、それらのプロファイルのストレージ QoS エントリーは自動的に [unlimited] に設定されます。

2.1.2. 仮想マシンのネットワーク QoS

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

2.1.2.1. 仮想マシンのネットワーク QoS エントリーの作成

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

仮想マシンのネットワーク QoS エントリーの作成

1. Compute → Data Centers をクリックします。
2. データセンターの名前をクリックします。 詳細ビューが開きます。
3. QoS タブをクリックします。
4. VM Network で、New をクリックします。
5. 仮想マシンネットワーク QoS (Quality of Service) エントリーの Name を入力します。
6. Inbound および Outbound ネットワークトラフィックの制限を入力します。
7. OK をクリックします。

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

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

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

表2.1仮想マシンネットワーク QoS 設定

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

Average、Peak、またはBurst フィールドで許可される最大値を変更するには、**engine-config** コマンドを使用して **MaxAverageNetworkQoSValue**、**MaxPeakNetworkQoSValue**、または**MaxBurstNetworkQoSValue** の設定キーの値を変更します。変更を反映するには、**ovirt-engine** サービスを再起動する必要があります。以下に例を示します。

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

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

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

手順

1. Compute → Data Centers をクリックします。
2. データセンターの名前をクリックします。詳細ビューが開きます。
3. QoS タブをクリックします。

4. VM Network で、仮想マシンネットワーク QoS (Quality of Service) エントリーを選択して Remove をクリックします。
5. OK をクリックします。

2.1.3. ホストネットワーク QoS

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

2.1.3.1. 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

1. Compute → Data Centers をクリックします。
2. データセンターの名前をクリックします。詳細ビューが開きます。
3. QoS タブをクリックします。
4. Host Network で、New をクリックします。
5. QoS Name と QoS エントリーの説明を入力します。
6. Weighted Share、Rate Limit [Mbps]、および Committed Rate [Mbps] に必要な値を入力します。
7. OK をクリックします。

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

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

表2.2 ホストネットワーク QoS 設定

フィールド名	説明
Data Center	ホストネットワーク QoS ポリシーを追加するデータセンター。このフィールドは、選択したデータセンターに応じて自動的に設定されます。
QoS Name	Manager 内のホストネットワーク QoS ポリシーを表す名前。
Description	ホストネットワーク QoS ポリシーの説明

フィールド名	説明
Outbound	<p>送信トラフィックに適用される設定。</p> <ul style="list-style-type: none"> ● Weight Share: 同じ論理リンクにアタッチされた他のネットワークと比較して、特定のネットワークに割り当てる必要がある論理リンクの容量を指定します。正確な共有は、そのリンクの全ネットワークの共有の合計によって異なります。デフォルトでは、この値は1-100の範囲の数字になります。 ● Rate Limit [Mbps]: ネットワークによって使用される最大帯域幅。 ● Committed Rate [Mbps]: ネットワークに必要な最小帯域幅。要求される Committed Rate は保証されず、ネットワークインフラストラクチャーおよび同じ論理リンクの他のネットワークによって要求される Committed Rate によって異なります。

Rate Limit [Mbps] または **Committed Rate [Mbps]** フィールドで許可される最大値を変更するには、**engine-config** コマンドを使用して **MaxAverageNetworkQoSValue** 設定キーの値を変更します。変更を反映するには、**ovirt-engine** サービスを再起動する必要があります。以下に例を示します。

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

2.1.3.3. 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

1. **Compute** → **Data Centers** をクリックします。
2. データセンターの名前をクリックします。詳細ビューが開きます。
3. **QoS** タブをクリックします。
4. **Host Network** で、ホストネットワーク QoS エントリーを選択して **Remove** をクリックします。
5. プロンプトが表示されたら **OK** をクリックします。

2.1.4. CPU QoS

CPU QoS は、仮想マシンが実行されているホスト上で仮想マシンがアクセスできる処理能力の最大量を定義します。これは、そのホストで使用可能な処理能力の合計に対する割合で表されます。CPU QoS を仮想マシンに割り当てるとき、クラスター内の1つの仮想マシンのワークロードが、そのクラスターの他の仮想マシンで利用できる処理リソースに影響を与えないようにすることができます。

2.1.4.1. 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

1. **Compute** → **Data Centers** をクリックします。
2. データセンターの名前をクリックします。詳細ビューが開きます。
3. **QoS** タブをクリックします。
4. **CPU** で **New** をクリックします。
5. **QoS Name** と QoS エントリーの **Description** を入力します。
6. QoS エントリーで許可される最大処理能力を **Limit (%)** フィールドに入力します。% 記号は含めないでください。
7. **OK** をクリックします。

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

2.1.4.2. 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

1. **Compute** → **Data Centers** をクリックします。
2. データセンターの名前をクリックします。詳細ビューが開きます。
3. **QoS** タブをクリックします。
4. **CPU** で CPU QoS エントリーを選択し、**Remove** をクリックします。
5. **OK** をクリックします。

そのエントリーに基づく CPU プロファイルが存在する場合、それらのプロファイルの CPU QoS エントリーは自動的に **[unlimited]** に設定されます。

2.2. データセンター

2.2.1. データセンターの概要

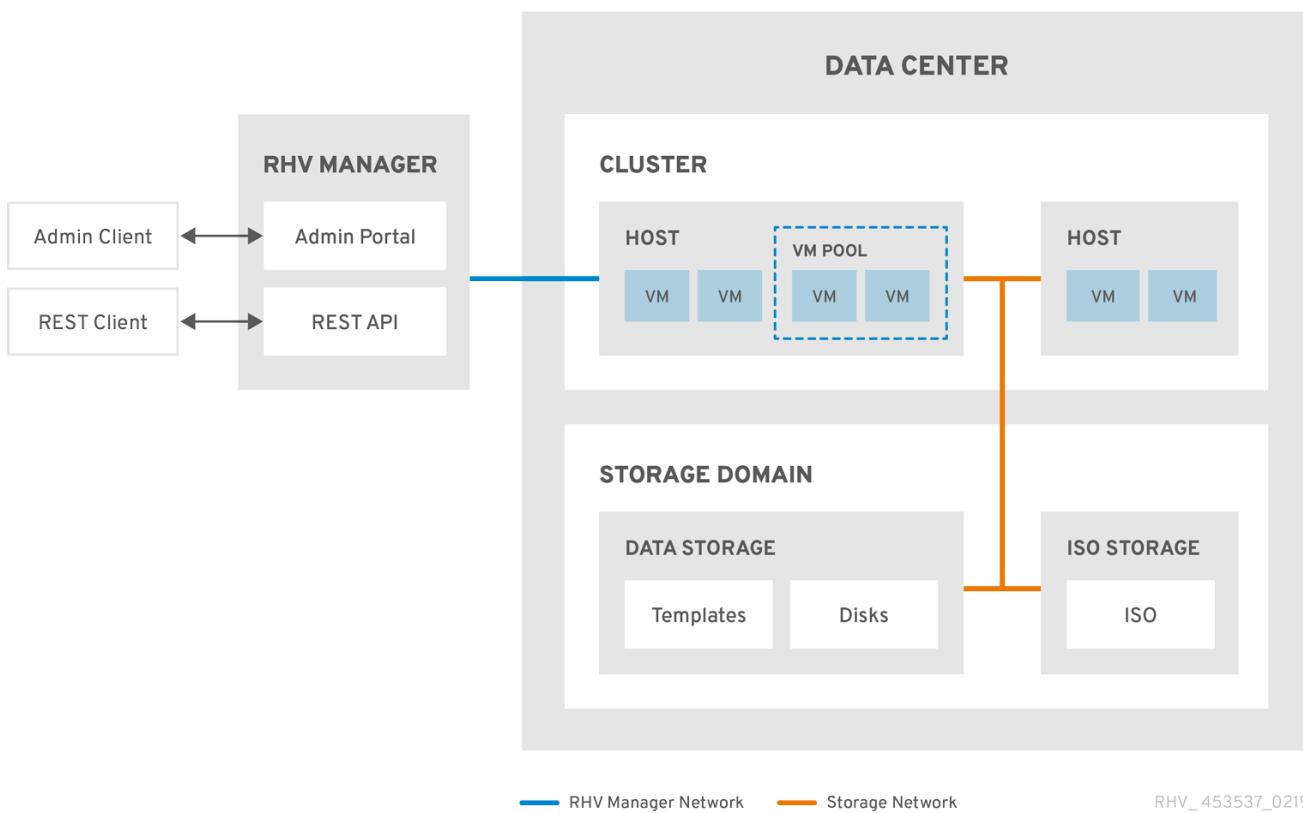
データセンターとは、特定の環境で使用するリソースのセットを定義する論理エンティティーです。データセンターは、コンテナリソース（クラスターとホストの形式の論理リソースで構成）、ネットワークリソース（論理ネットワークと物理 NIC の形式）、およびストレージリソース（ストレージドメインの形式）と見なされます。

データセンターには、複数のホストを含む複数のクラスターを含めることができます。複数のストレージドメインが関連付けられており、各ホスト上の複数の仮想マシンをサポートすることができます。Red Hat Virtualization 環境には複数のデータセンターを含めることができます。データセンターインフ

ラストラクチャーを使用すると、これらのセンターを分離した状態にすることができます。

すべてのデータセンターは、1つの管理ポータルから管理されます。

図2.1データセンター



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

2.2.2. ストレージプールマネージャー

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

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

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

2.2.3. SPM の優先度

SPM ロールは、ホストの利用可能なリソースの一部を使用します。ホストの SPM 優先度の設定によ

り、ホストが SPM ロールが割り当てられる可能性があります。SPM 優先度が高いホストには、SPM の優先度が低いホストの前に SPM ロールが割り当てられます。SPM 優先度が低いホストの重要な仮想マシンは、ホストリソースの SPM 操作と連動させる必要はありません。

Edit Host ウィンドウの SPM タブで、ホストの SPM タブの優先度を変更できます。

2.2.4. データセンタータスク

2.2.4.1. 新規データセンターの作成

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



注記

互換バージョン を設定したら、バージョン番号を低くすることはできません。バージョンリグレッショնはサポートされていません。

クラスターの MAC プール範囲を指定できます。MAC プール範囲の設定はサポートされなくなりました。

手順

1. Compute → Data Centers をクリックします。
2. New をクリックします。
3. データセンターの Name および Description を入力します。
4. ドロップダウンメニューから、データセンターの Storage Type、Compatibility Version、Quota Mode を選択します。
5. OK をクリックしてデータセンターを作成し、Data Center - Guide Me ウィンドウを開きます。
6. Guide Me ウィンドウには、データセンター用に設定する必要のあるエンティティーが一覧表示されます。これらのエンティティーを設定するか、Configure Later ボタンをクリックして設定を延期します。設定を再開するには、データセンターを選択し、More Actions (⋮) をクリックしてから Guide Me をクリックします。

新しいデータセンターは、クラスター、ホスト、およびストレージドメインが設定されるまで Uninitialized になります。Guide Me を使用してこれらのエンティティーを設定します。

2.2.4.2. New Data Center と Edit Data Center ウィンドウの設定の説明

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

表2.3 データセンターのプロパティー

フィールド	説明/アクション
-------	----------

フィールド	説明/アクション
Name	データセンターの名前。このテキストフィールドには 40 文字の制限があり、大文字、小文字、数字、ハイフン、およびアンダースコアの組み合わせが含まれる一意の名前である必要があります。
説明	データセンターの説明このフィールドは推奨されますが、必須ではありません。
Storage Type	<p>Shared または Local ストレージタイプを選択します。</p> <p>異なるタイプのストレージドメイン (iSCSI、NFS、FC、POSIX、および Gluster) を同じデータセンターに追加できます。ただし、ローカルドメインおよび共有ドメインを混在させることはできません。</p> <p>データセンターの初期化後にストレージタイプを変更できます。データセンターのストレージタイプの変更 を参照してください。</p>
Compatibility Version	<p>Red Hat Virtualization のバージョン。</p> <p>Red Hat Virtualization Manager をアップグレードした後も、ホスト、クラスター、およびデータセンターが以前のバージョンのままになっている可能性があります。データセンターの互換性レベルをアップグレードする前に、まずすべてのホスト、次にクラスターがアップグレードされていることを確認します。</p>
Quota Mode	<p>クォータは、Red Hat Virtualization で提供されるリソース制限ツールです。以下のいずれかを選択します。</p> <ul style="list-style-type: none"> ● Disabled: クォータを実装しない場合に選択します。 ● Audit: クォータ設定を編集する場合に選択します。 ● Enforced: クォータを実装する場合に選択します。
Comment	オプションで、データセンターに関するプレーンテキストコメントを追加します。

2.2.4.3. データセンターの再初期化: 復旧手順

この復旧手順は、データセンターの master データドメインを新しい master データドメインに置き換えます。データが破損している場合は、master データドメインを再初期化する必要があります。データセンターを再初期化すると、クラスター、ホスト、問題のないストレージドメインなど、データセン

ターに関連付けられた他のリソースをすべて復元できます。

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

手順

1. **Compute** → **Data Centers** をクリックし、データセンターを選択します。
2. データセンターに接続されたストレージドメインがメンテナンスモードにあることを確認します。
3. **More Actions** (⋮) をクリックしてから、**Re-Initialize Data Center** をクリックします。
4. **Data Center Re-Initialize** ウィンドウには、利用可能なすべての(割り当て解除あり、メンテナントモードの場合)ストレージドメインが一覧表示されます。データセンターに追加するストレージドメインのラジオボタンをクリックします。
5. **Approve operation** チェックボックスを選択します。
6. **OK** をクリックします。

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

2.2.4.4. データセンターの削除

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

手順

1. データセンターに接続されたストレージドメインがメンテナンスモードにあることを確認します。
2. **Compute** → **Data Centers** をクリックし、削除するデータセンターを選択します。
3. **Remove** をクリックします。
4. **OK** をクリックします。

2.2.4.5. データセンターの強制削除

アタッチされたストレージドメインが破損したり、ホストが **Non Responsive** になった場合、データセンターが **Non Responsive** になります。いずれの状況においても、データセンターを **Remove** できません。

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

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

手順

1. Compute → Data Centers をクリックし、削除するデータセンターを選択します。
2. More Actions (⋮) をクリックしてから、Force Remove をクリックします。
3. Approve operation チェックボックスを選択します。
4. OK をクリックします。

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

2.2.4.6. データセンターストレージタイプの変更

データセンターの初期化後に、データセンターのストレージタイプを変更できます。これは、仮想マシンまたはテンプレートの移動に使用されるデータドメインに役立ちます。

制限

- 共有からローカル - ホストおよびクラスターがそれぞれ1つしかないデータセンターの場合。
ローカルデータセンターではサポートされていません。
- ローカルから共有 - ローカルストレージドメインを含まないデータセンターの場合。

手順

1. Compute → Data Centers をクリックし、変更するデータセンターを選択します。
2. Edit をクリックします。
3. Storage Type を必要な値に変更します。
4. OK をクリックします。

2.2.4.7. データセンターの互換バージョンの変更

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

前提条件

- データセンターの互換レベルを変更するには、データセンター内のクラスターおよび仮想マシンの互換バージョンが、事前にすべて更新されている必要があります。

手順

1. 管理ポータルで Compute → Data Centers をクリックします。
2. 変更を行うデータセンターを選択し、Edit をクリックします。
3. Compatibility Version を必要な値に変更します。
4. OK をクリックします。Change Data Center Compatibility Version の確認ダイアログが開きます。
5. OK をクリックして確定します。

2.2.5. データセンターおよびストレージドメイン

2.2.5.1. 既存のデータドメインをデータセンターにアタッチ

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

手順

1. **Compute → Data Centers** をクリックします。
2. データセンターの名前をクリックします。詳細ビューが開きます。
3. **Storage** タブをクリックして、データセンターにすでにアタッチされているストレージドメインを一覧表示します。
4. **Attach Data** をクリックします。
5. データセンターにアタッチするデータドメインのチェックボックスを選択します。複数のデータドメインを割り当てる場合は、複数のチェックボックスを選択できます。
6. **OK** をクリックします。

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

2.2.5.2. 既存の ISO ドメインをデータセンターにアタッチ

Unattached ISO ドメインは、データセンターにアタッチすることができます。ISO ドメインは、データセンターと同じ **Storage Type** である必要があります。

データセンターに1つの ISO ドメインのみをアタッチできます。

手順

1. **Compute → Data Centers** をクリックします。
2. データセンターの名前をクリックします。詳細ビューが開きます。
3. **Storage** タブをクリックして、データセンターにすでにアタッチされているストレージドメインを一覧表示します。
4. **Attach ISO** をクリックします。
5. 適切な ISO ドメインのラジオボタンをクリックします。
6. **OK** をクリックします。

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

2.2.5.3. 既存のエクスポートドメインをデータセンターにアタッチ



注記

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

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

手順

1. **Compute → Data Centers** をクリックします。
2. データセンターの名前をクリックします。詳細ビューが開きます。
3. **Storage** タブをクリックして、データセンターにすでにアタッチされているストレージドメインを一覧表示します。
4. **Attach Export** をクリックします。
5. 適切なエクスポートドメインのラジオボタンをクリックします。
6. **OK** をクリックします。

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

2.2.5.4. データセンターからストレージドメインをデタッチ

データセンターからストレージドメインをデタッチすると、データセンターとそのストレージドメインの関連付けは解除されます。ストレージドメインは Red Hat Virtualization 環境から削除されず、別のデータセンターにアタッチすることができます。

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



警告

最後のマスターストレージドメインをデタッチすることは可能ですが、これはお勧めできません。

マスターストレージドメインがデタッチされている場合は、再初期化する必要があります。

ストレージドメインが再初期化されると、すべてのデータが失われ、ストレージドメインがディスクを再度検出できなくなる可能性があります。

手順

1. **Compute → Data Centers** をクリックします。

2. データセンターの名前をクリックします。詳細ビューが開きます。
3. **Storage** タブをクリックして、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一覧表示します。
4. デタッチするストレージドメインを選択します。ストレージドメインが **Active** の場合は、**Maintenance** をクリックします。
5. **OK** をクリックしてメンテナンスモードを開始します。
6. **Detach** をクリックします。
7. **OK** をクリックします。

ストレージドメインが詳細ビューから消えるまでに数分かかる場合があります。

2.3. クラスター

2.3.1. クラスターの概要

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

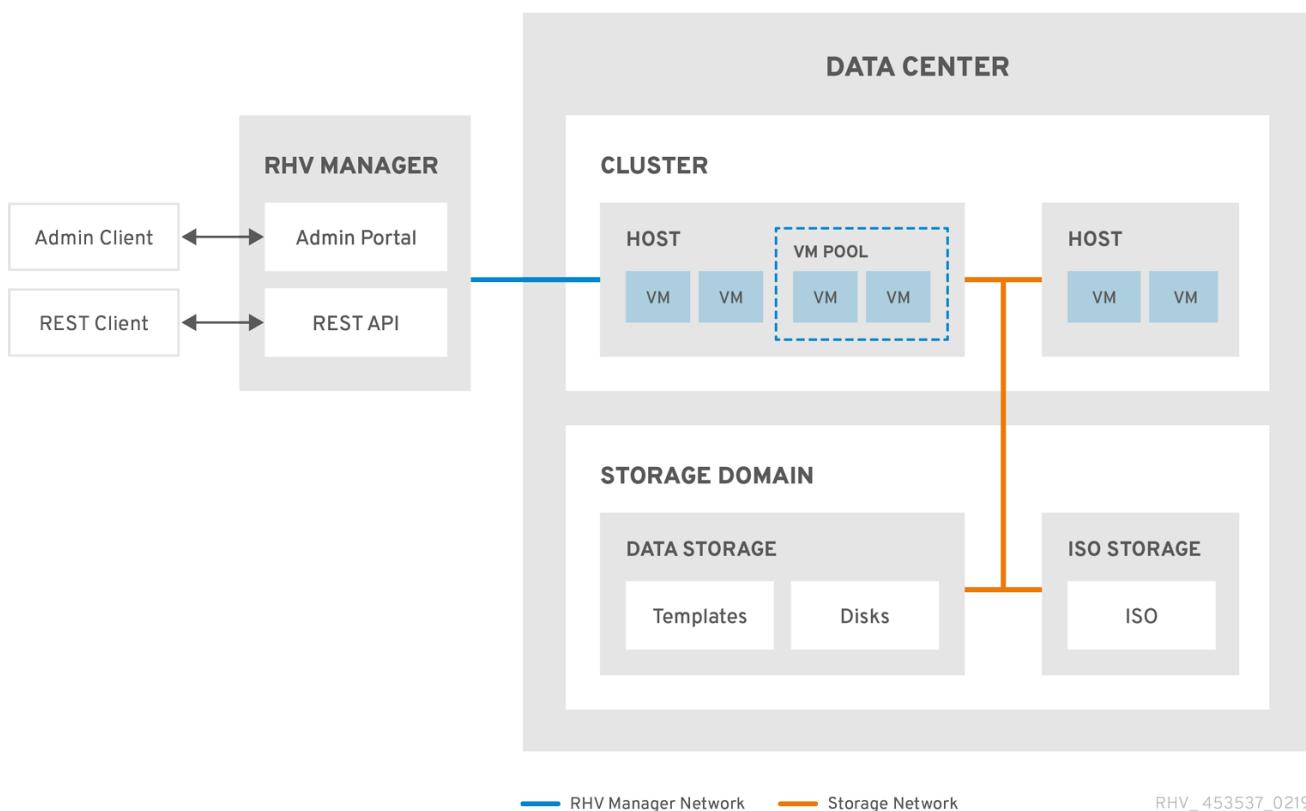
システム内の各クラスターはデータセンターに属し、システム内の各ホストはクラスターに属している必要があります。仮想マシンはクラスター内の任意のホストに動的に割り当てられ、仮想マシン上のクラスターおよび設定に合わせて、それらのホスト間で移行することができます。クラスターは、電源および負荷分散ポリシーを定義できる最上位です。

クラスターに属するホストおよび仮想マシンの数は、**Host Count** および **VM Count** の結果一覧にそれぞれ表示されます。

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

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

図2.2 クラスター



2.3.2. クラスター タスク



注記

一部のクラスターオプションは Gluster クラスターには適用されません。Red Hat Virtualization で Red Hat Gluster Storage を使用する方法の詳細は、[Red Hat Gluster Storage を使用した Red Hat Virtualization の設定](#) を参照してください。

2.3.2.1. 新規クラスターの作成

データセンターには複数のクラスターを含めることができます。クラスターには複数のホストを含めることができます。クラスター内のすべてのホストに同じ CPU アーキテクチャーがなければなりません。CPU タイプを最適化するには、クラスターを作成する前にホストを作成します。クラスターを作成したら、Guide Me ボタンを使用してホストを設定できます。

手順

1. Compute → Clusters をクリックします。
2. New をクリックします。
3. ドロップダウンリストからクラスターが所属する Data Center を選択します。
4. クラスターの Name および Description を入力します。
5. Management Network のドロップダウンリストからネットワークを選択して、管理ネットワーククロールを割り当てます。

6. CPU Architecture を選択します。
7. CPU Type には、このクラスターの一部であるホスト間で、最も古い CPU プロセッサーファミリーを選択します。CPU タイプは、最も古いものから最新の順に一覧表示されます。



重要

CPU プロセッサーファミリーが CPU Type で指定したホストよりも古いホストは、このクラスターの一部にすることはできません。詳細は、[RHEV3 または RHV4 クラスターをどの CPU ファミリーに設定する必要があるか](#) を参照してください。

8. ドロップダウンリストからクラスターの FIPS Mode を選択します。
9. ドロップダウンリストから、クラスターの Compatibility Version を選択します。
10. ドロップダウンリストから Switch Type を選択します。
11. クラスター内のホストの Firewall Type (Firewalld (デフォルト) または iptables) を選択します。



注記

iptables がサポートされるのは、互換バージョン 4.2 または 4.3 のクラスターの Red Hat Enterprise Linux 7 ホストのみです。Red Hat Enterprise Linux 8 ホストは、ファイアウォールタイプが firewalld のクラスターにのみ追加できます。

12. Enable Virt Service または Enable Gluster Service チェックボックスを選択して、クラスターが仮想マシンホストまたは Gluster 対応ノードと共に設定されるかどうかを定義します。
13. Enable to set VM maintenance reason チェックボックスを選択すると、仮想マシンを Manager からシャットダウンする際に任意の reason フィールドが有効になり、管理者はメンテナンスの説明を提供できます。
14. Enable to set Host maintenance reason チェックボックスを選択すると、ホストを Manager からメンテナンスマードにする時に任意の reason フィールドが有効になり、管理者はメンテナンスの説明を提供できます。
15. オプションで /dev/hwrng source (外部ハードウェアデバイス) のチェックボックスを選択し、クラスター内のすべてのホストが使用する乱数ジェネレーターデバイスを指定します。/dev/urandom source (Linux が提供するデバイス) はデフォルトで有効になっています。
16. Optimization タブをクリックしてクラスターのメモリーページ共有しきい値を選択し、必要に応じてクラスター内のホストで CPU スレッド処理とメモリーバルーンを有効にします。
17. Migration Policy タブをクリックして、クラスターの仮想マシン移行ポリシーを定義します。
18. Scheduling Policy (スケジューリングポリシー) タブをクリックして、スケジューリングポリシーの設定、スケジューラー最適化の設定、クラスター内のホストの信頼できるサービスの有効化、HA Reservation の有効化、シリアル番号ポリシーを選択します。
19. Console タブをクリックしてオプションでグローバル SPICE プロキシー (ある場合) を上書きし、クラスターに含まれるホストの SPICE プロキシーのアドレスを指定します。

20. **Fencing policy** タブをクリックして、クラスターでフェンシングを有効または無効にします。また、フェンシングオプションを選択します。
21. **MAC Address Pool** タブをクリックして、クラスターのデフォルトプール以外の MAC アドレスプールを指定します。MAC アドレスプールの作成、編集、削除に関するその他のオプションについては、[MAC アドレスプール](#) を参照してください。
22. **OK** をクリックしてクラスターを作成し、**Cluster - Guide Me** ウィンドウを開きます。
23. **Guide Me** ウィンドウには、クラスターに設定する必要のあるエンティティーが一覧表示されます。これらのエンティティーを設定するか、**Configure Later** ボタンをクリックして設定を延期します。設定を再開するには、クラスターを選択し、**More Actions** (⋮) をクリックしてから、**Guide Me** をクリックします。

2.3.2.2. 一般的なクラスター設定に関する説明

以下の表は、**New Cluster** および **Edit Cluster** ウィンドウの **General** タブの設定を説明しています。**OK** をクリックすると、無効なエントリーはオレンジ色で囲まれ、変更は承認されません。さらに、フィールドプロンプトには、予想される値または値の範囲が示されます。

表2.4 一般的なクラスター設定

フィールド	説明/アクション
Data Center	クラスターが含まれるデータセンター。クラスターを追加する前にデータセンターを作成する必要があります。
Name	クラスターの名前。このテキストフィールドには 40 文字の制限があり、大文字、小文字、数字、ハイフン、およびアンダースコアの組み合わせが含まれる一意の名前である必要があります。
Description / Comment	クラスターまたは追加のメモの説明。これらのフィールドは推奨されますが、必須ではありません。
Management Network	管理ネットワークロールを割り当てる論理ネットワーク。デフォルトは ovirtmgmt です。移行ネットワークが移行元または移行先ホストに正しくアタッチされていない場合、このネットワークが仮想マシンの移行にも使用されます。
	既存のクラスターでは、詳細ビューの Logical Networks タブにある Manage Networks ボタンを使用すると、管理ネットワークを変更できます。

フィールド	説明/アクション
CPU Architecture	<p>クラスターの CPU アーキテクチャー。クラスター内のすべてのホストは、指定したアーキテクチャーを実行する必要があります。選択した CPU アーキテクチャーに応じて、さまざまな CPU タイプを利用できます。</p> <ul style="list-style-type: none">● undefined: その他のすべての CPU タイプ。● x86_64: Intel および AMD CPU タイプ用● ppc64: IBM POWER CPU タイプ用
CPU Type	<p>クラスター内の最も古い CPU ファミリー。CPU タイプの一覧は、プランニングおよび前提条件に関するガイドの CPU の要件 を参照してください。作成したクラスターは、重大な中断が発生しない限り変更できません。CPU タイプをクラスター内の最も古い CPU モデルに設定します。すべてのモデルに存在する機能のみ使用できます。Intel タイプおよび AMD CPU タイプの両方の場合、リストされた CPU モデルは、最も古いものから最新の順に論理的に使用されます。</p>

フィールド	説明/アクション
Chipset/Firmware Type	<p>この設定は、クラスターの CPU Architecture が x86_64 に設定されている場合にのみ使用できます。この設定では、チップセットとファームウェアのタイプを指定します。オプションは以下のとおりです。</p> <ul style="list-style-type: none"> ● Auto Detect: この設定は、チップセットとファームウェアのタイプを自動的に検出します。Auto Detect が選択されている場合、チップセットとファームウェアは、クラスター内で最初に起動したホストによって決定されます。 ● I440FX Chipset with BIOS: BIOS のファームウェアタイプでチップセットを I440FX に指定します。 ● Q35 Chipset with BIOS: UEFI を使用しない BIOS ファームウェアタイプで Q35 チップセットを指定します(互換性バージョン 4.4 のクラスターのデフォルト)。 ● Q35 Chipset with UEFI: UEFI を使用する BIOS のファームウェアタイプで Q35 チップセットを指定します。(互換バージョン 4.7 のクラスターのデフォルト) ● Q35 Chipset with UEFI SecureBoot: ファームウェアタイプが UEFI with SecureBoot の Q35 チップセットを指定し、ブートローダーのデジタル署名を認証します。 <p>詳細は、管理ガイドの UEFI および Q35 チップセット を参照してください。</p>
Change Existing VMs/Templates from 1440fx to Q35 Chipset with Bios	クラスターのチップセットが I440FX から Q35 に変更された場合、既存のワークLOADを変更するには、このチェックボックスを選択します。

フィールド	説明/アクション
FIPS Mode	<p>クラスターが使用する FIPS モード。クラスター内のすべてのホストは、指定する FIPS モードを実行する必要があります。実行しないと、稼働しなくなります。</p> <ul style="list-style-type: none"> ● Auto Detect: この設定は、FIPS モードが有効または無効であるかどうかを自動的に検出します。Auto Detect を選択すると、FIPS モードはクラスター内の最初のホストによって決定されます。 ● Disabled: クラスターでの FIPS を無効にします。 ● Enabled: クラスターで FIPS を有効にします。
Compatibility Version	Red Hat Virtualization のバージョン。データセンターに指定したバージョンよりも前のバージョンは選択できません。
Switch Type	クラスターが使用するスイッチのタイプ。Linux Bridge は、標準の Red Hat Virtualization スイッチです。OVS は、Open vSwitch のネットワーク機能をサポートします。
Firewall Type	クラスター内のホストのファイアウォールタイプ (<code>firewalld</code> (デフォルト) または <code>iptables</code> のいずれか) を指定します。 <code>iptables</code> がサポートされるのは、互換バージョン 4.2 または 4.3 のクラスターの Red Hat Enterprise Linux 7 ホストのみです。Red Hat Enterprise Linux 8 ホストは、ファイアウォールタイプ <code>firewalld</code> のクラスターにのみ追加できます。既存のクラスターのファイアウォールタイプを変更する場合は、クラスターで すべてのホストを再インストール し、変更を適用する必要があります。
Default Network Provider	<p>クラスターが使用するデフォルトの外部ネットワークプロバイダーを指定します。Open Virtual Network (OVN) を選択する場合、クラスターに追加されたホストは OVN プロバイダーと通信するように自動的に設定されます。</p> <p>デフォルトのネットワークプロバイダーを変更する場合は、クラスターのすべてのホストを再インストール し、変更を適用する必要があります。</p>

フィールド	説明/アクション
Maximum Log Memory Threshold	最大メモリー消費のロギングしきい値を、パーセンテージまたは絶対値(MB単位)で指定します。ホストのメモリー使用量がパーセンテージ値を超えている場合や、ホストで利用可能なメモリーが絶対値(MB単位)を下回る場合にログに記録されます。デフォルトは 95% です。
Enable Virt Service	こ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は仮想マシンの実行に使用されます。
Enable Gluster Service	このチェックボックスを選択すると、このクラスターのホストはRed Hat Gluster Storage Serverノードとして使用され、仮想マシンの実行には使用されません。
Import existing gluster configuration	<p>このチェックボックスは、Enable Gluster Serviceラジオボタンが選択されている場合にのみ利用できます。このオプションを使用すると、既存のGluster対応クラスターおよびその割り当てられたすべてのホストをRed Hat Virtualization Managerにインポートできます。</p> <p>以下のオプションは、インポートされているクラスター内のホストごとに必要です。</p> <ul style="list-style-type: none"> ● Hostname: GlusterホストサーバーのIPまたは完全修飾ドメイン名を入力します。 ● Host ssh public key (PEM): Red Hat Virtualization ManagerはホストのSSH公開鍵を取得して、正しいホストに接続していることを確認します。 ● Password: ホストとの通信に必要なrootパスワードを入力します。
Additional Random Number Generator source	このチェックボックスを選択すると、クラスター内のすべてのホストで追加の乱数ジェネレーターデバイスを使用できます。これにより、乱数ジェネレーターデバイスから仮想マシンへのエントロピーのパススルーが可能になります。
Gluster Tuned Profile	このチェックボックスは、 Enable Gluster Service チェックボックスが選択されている場合にのみ利用できます。このオプションは、 virtual-host チューニングプロファイルを指定してダーティーメモリーページのさらに積極的なライトバックを有効にし、ホストのパフォーマンスを向上させます。

2.3.2.3. 最適化設定の説明

メモリーに関する考慮事項

メモリーページの共有により、仮想マシンは、他の仮想マシンで未使用的メモリーを利用することで、割り当てられたメモリーの最大 200% を使用できます。このプロセスは、Red Hat Virtualization 環境内のすべての仮想マシンが同時に全容量を使用して実行されるわけではなく、未使用的メモリーが一時的に特定の仮想マシンに割り当てられることを前提としています。

CPU の考慮事項

- **CPU 負荷が高くないワークロードの場合**、ホスト内のコア数よりも大きいプロセッサーコアの合計数で仮想マシンを実行できます（単一仮想マシンのプロセッサーコア数は、ホストのコア数を超えることができません）。以下の利点があります。
 - より多くの仮想マシンを実行することができます。これにより、ハードウェアの要件が減少します。
 - 仮想コア数がホストコア数とホストスレッド数の間にある場合など、それ以外の場合は不可能な CPU トポロジーで仮想マシンを設定できます。
- **最適なパフォーマンス、特に CPU 集約型のワークロードの場合**、ホストと同じトポロジーを仮想マシンで使用し、ホストと仮想マシンが同じキャッシュの使用を想定するようにします。ホストのハイパスレッディングが有効な場合、QEMU がホストのハイパスレッドをコアとして扱うため、仮想マシンは複数のスレッドを持つ単一のコアで実行されていることを認識しません。ホストコアのハイパスレッドに実際に対応する仮想コアは、仮想マシンのパフォーマンスに影響する可能性があります。これは、同じホストコアのハイパスレッドと単一のキャッシュを共有する可能性がありますが、仮想マシンは別のコアとして扱います。

以下の表は、New Cluster および Edit Cluster ウィンドウの Optimization タブの設定を説明しています。

表2.5 最適化の設定

フィールド	説明/アクション
Memory Optimization	<ul style="list-style-type: none"> ● None - Disable memory overcommit メモリーページ共有を無効にします。 ● Server Load - Allow scheduling of 150% of physical memory: 各ホストのシステムメモリーのメモリーページ共有しきい値を 150% に設定します。 ● For Desktop Load - Allow scheduling of 200% of physical memory: 各ホストのシステムメモリーのメモリーページ共有しきい値を 200% に設定します。

フィールド	説明/アクション
CPU Threads	<p>Count Threads As Cores チェックボックスをオンにすると、ホスト内のコア数よりも大きいプロセッサー核心の合計数で仮想マシンを実行できます(単一仮想マシンのプロセッサー核心数は、ホストのコア数を超えることができません)。</p> <p>このチェックボックスを選択すると、公開されるホストスレッドは仮想マシンが使用できるコアとして扱われます。たとえば、コアごとに2つのスレッドがある24コアのシステム(全部で48スレッド)では、最大48コアを持つ仮想マシンを実行できます。そして、ホストのCPU負荷を計算するアルゴリズムでは、潜在的に使用されるコアの2倍に対して負荷を比較します。</p>
Memory Balloon	<p>Enable Memory Balloon Optimization のチェックボックスを選択し、このクラスターのホストで実行している仮想マシンでメモリーのオーバーコミットを有効にします。このチェックボックスを選択すると、Memory Overcommit Manager (MoM) は、可能な限りバルーニングを開始し、すべての仮想マシンの保証メモリーサイズを制限します。</p> <p>バルーンを実行するには、仮想マシンに適切なドライバーを持つバルーンデバイスが必要です。各仮想マシンには、特に削除しない限り、バルーンデバイスが含まれます。このクラスター内の各ホストは、ステータスが Up に変わると、バルーンポリシーの更新を受け取ります。必要に応じて、ステータスを変更せずに、ホストのバルーンポリシーを手動で更新できます。クラスター内のホストにおける MoM ポリシーの更新 を参照してください。</p> <p>状況によっては、バルーニングが KSM と競合する可能性がある点を理解することが重要です。このような場合、MoM は競合の可能性を最小限に抑えるためにバルーンサイズの調整を試みます。また、バルーニングによって仮想マシンのパフォーマンスが最適化されない場合もあります。ルーニングの最適化に関して、管理者は慎重に使用することが推奨されます。</p>
KSM control	Enable KSM チェックボックスを選択すると、MoM は必要に応じて、CPUコストを上回るメモリー節約効果が得られる場合に、Kernel Same-page Merging (KSM) を実行できます。

2.3.2.4. 移行ポリシー設定の説明

移行ポリシーは、ホストに障害が発生した場合に仮想マシンをライフマイクレーションするための条件を定義します。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、および仮想マシンの優先順位が含まれます。

表2.6 移行ポリシーの説明

ポリシー	説明
Cluster default (Minimal downtime)	vdsm.conf のオーバーライドは引き続き適用されます。ゲストエージェントフックメカニズムが無効になっています。
Minimal downtime	仮想マシンを一般的な状況で移行できるようにするポリシー。仮想マシンで重大なダウンタイムは発生しません。移行は、長時間 (QEMU の反復により最大 500 ミリ秒) 経過しても仮想マシンの移行が収束されない場合に中止されます。ゲストエージェントフックメカニズムは有効化されています。

ポリシー	説明
Post-copy migration	<p>post-copy migration を使用すると、移行元のホスト上にある移行対象の仮想マシンの vCPU が一時停止され、最小限のメモリーページのみ転送されます。次に、移行先ホストにある仮想マシンの vCPU がアクティブ化され、移行先で仮想マシンが動作している間に残りのメモリーページが転送されます。</p> <p>post-copy ポリシーでは、まず pre-copy を実行して収束するか検証します。長時間経過しても仮想マシンの移行が収束しない場合、post-copy に切り替わります。</p> <p>これにより、移行先の仮想マシンのダウンタイムが大幅に短縮されるとともに、移行元の仮想マシンのメモリーページがどれだけ急激に変化しても、確実に移行が完了されます。標準的な pre-copy の移行では対応できない、連続使用率の高い仮想マシンの移行に最適です。</p> <p>このポリシーの欠点として、post-copy フェーズではメモリーの不足部分がホスト間で転送されるため、仮想マシンが大幅に遅くなる可能性があります。</p>



警告

post-copy プロセスの完了前にネットワーク接続が切斷されると、Manager は一時停止し、実行中の仮想マシンを強制終了します。仮想マシンの可用性が重要である場合や、移行ネットワークが不安定な場合は、post-copy migration を使用しないでください。

ポリシー	説明
Suspend workload if needed	負荷の高いワークロードを実行している仮想マシンを含め、ほとんどの状況で仮想マシンを移行できるポリシー。結果として、他の設定よりも重大なダウンタイムが仮想マシンで発生する場合があります。ワークロードが極端な場合、移行が中止される可能性があります。ゲストエージェントフックメカニズムは有効化されています。

帯域幅設定は、ホストごとの送信移行と受信移行の両方の最大帯域幅を定義します。

表2.7 帯域幅の説明

ポリシー	説明
Auto	帯域幅は、データセンターの Host Network QoS の Rate Limit [Mbps] 設定からコピーされます。レート制限が定義されていない場合は、ネットワークインターフェイスの送受信における最小リンク速度として計算されます。レート制限が設定されていない場合や、リンク速度が利用できない場合には、ホスト送信時にローカルの VDSM 設定により決定されます。
Hypervisor default	帯域幅は、ホスト送信時にローカルの VDSM 設定によって制御されます。
Custom	ユーザーにより定義されます (Mbps 単位)。この値は、同時移行の数 (デフォルトは ingoing と outgoing の移行を考慮して 2) で分割されます。したがって、ユーザー定義の帯域幅は、すべての同時移行に対応できる十分な大きさである必要があります。 たとえば、Custom 帯域幅が 600 Mbps として定義されている場合、仮想マシンの移行の最大帯域幅は実際には 300 Mbps になります。

耐障害性ポリシーは、移行での仮想マシンの優先順位を定義します。

表2.8 耐障害性ポリシーの設定

フィールド	説明/アクション
Migrate Virtual Machines	定義された優先順位で、すべての仮想マシンを移行します。
Migrate only Highly Available Virtual Machines	他のホストのオーバーロードを防ぐために、高可用性の仮想マシンのみを移行します。

フィールド	説明/アクション
Do Not Migrate Virtual Machines	仮想マシンを移行しないようにします。

表2.9 その他のプロパティー設定

フィールド	説明/アクション
Enable Migration Encryption	移行中に仮想マシンを暗号化できるようにします。 <ul style="list-style-type: none"> ● Cluster default ● Encrypt ● Don't encrypt
Parallel Migrations	使用する並列移行接続の有無と数を指定できます。 <ul style="list-style-type: none"> ● Disabled: 仮想マシンは、単一の非並列接続を使用して移行されます。 ● Auto: 並列接続の数は自動的に決定されます。この設定により、並列接続が自動的に無効になる可能性があります。 ● Auto Parallel: 並列接続の数は自動的に決定されます。 ● Custom: 並列接続の優先数を指定できます。実際の数はそれより少ない場合があります。
Number of VM Migration Connections	この設定は、Custom が選択されている場合にのみ利用できます。カスタム並列移行の推奨数は 2 から 255 です。

2.3.2.5. スケジューリングポリシー設定に関する説明

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

表2.10 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
Select Policy	<p>ドロップダウンリストからポリシーを選択します。</p> <ul style="list-style-type: none"> ● none: すでに実行中の仮想マシンに対して、ホスト間の負荷分散または省電力を無効にします。これはデフォルトのモードです。仮想マシンが起動すると、メモリーと CPU 処理の負荷がクラスター内の全ホストに均等に分散されます。ホストが定義された CpuOverCommitDurationMinutes、HighUtilization、または MaxFreeMemoryForOverUtilized に達した場合、ホストにアタッチされた追加の仮想マシンは起動しません。 ● evenly_distributed: メモリーおよび CPU 処理をクラスター内のすべてのホストで均等に分散します。ホストが定義された CpuOverCommitDurationMinutes、HighUtilization、VCpuToPhysicalCpuRatio、または MaxFreeMemoryForOverUtilized に達した場合、ホストにアタッチされた追加の仮想マシンは起動しません。 ● cluster_maintenance: メンテナンススク中のクラスターでアクティビティーを制限します。高可用性の仮想マシンを除き、新規の仮想マシンを起動することはできません。ホストの障害が発生した場合、高可用性仮想マシンが正しく再起動し、どの仮想マシンも移行できます。 ● power_saving: 使用率の低いホストの電力消費を減らすために、利用可能なホストのサブセットにメモリーおよび CPU 処理負荷を分散します。CPU 負荷が使用率の下限値を下回っている状態が定義された時間以上続いたホストは、すべての仮想マシンを他のホストに移行させ、電源を切れるようにします。ホストにアタッチされた追加の仮想マシンは、そのホストが定義された使用率の上限値に達した場合は起動しません。 ● vm_evenly_distributed: 仮想マシンの数に基づいて、仮想マシンをホスト間で均等に分散します。HighVmCount より多くの仮想マシンを実行しているホストがあり、仮想マシン数が MigrationThreshold の範囲外であるホストが少なくとも 1 つ存在する場合、クラスターはアンバランスであると判断されます。
Properties	<p>以下のプロパティは、選択したポリシーに応じて表示されます。必要に応じてこれを編集します。</p> <ul style="list-style-type: none"> ● HighVmCount: 負荷分散を有効にするためにホストごとに実行する必要のある仮想マシンの最小数を設定します。デフォルト値は 10 で、1 台のホストで 10 の仮想マシンが実行されます。負荷分散は、少なくとも HighVmCount が仮想マシンを実行するクラスターに 1 つ以上のホストがある場合にのみ有効になります。 ● MigrationThreshold: 仮想マシンがホストから移行される前にバッファーを定義します。これは、使用率が最も高いホストと使用率が最も低いホストの間の仮想マシン数の差の最大値です。クラスター内のすべてのホストの仮想マシン数が移行しきい値内に収まる場合、クラスターはバランスが取れています。デフォルト値は 5 です。 ● SpmVmGrace: SPM ホストで予約される仮想マシンのスロット数を定義します。SPM ホストの負荷は他のホストよりも低くなるため、この変数は、他のホストと比較して SPM ホストが実行できる仮想マシンの数がどれだけ少なくなるかを定義します。デフォルト値は 5 です。 ● CpuOverCommitDurationMinutes: スケジューリングポリシーの実行前に、定義された使用率の値を超えてホストが 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で、スケジューリング

フィールド	説明/アクション
	<p>グポリシーがアクティブ化して一時的なCPU負荷の急増から保護し、仮想マシンの移行を軽減します。文字数は最大2文字です。デフォルト値は2です。</p> <ul style="list-style-type: none"> ● HighUtilization: パーセンテージで表されます。定義された時間間隔において、ホストがCPU使用率の上限以上で実行されると、Red Hat Virtualization ManagerはホストのCPU負荷が最大サービスしきい値を下回るまで、仮想マシンをクラスター内の他のホストに移行します。デフォルト値は80です。 ● LowUtilization: パーセンテージで表されます。定義された時間間隔において、ホストがCPU使用率の下限を下回って実行されると、Red Hat Virtualization Managerは仮想マシンをクラスター内の他のホストに移行します。Managerは元のホストマシンの電源をオフにし、負荷分散が必要な場合、またはクラスターに空きホストが十分がない場合に再び再起動します。デフォルト値は20です。 ● ScaleDown: ホストのスコアを指定した数で除算して、HA Reservation機能の影響を減らします。これは、<code>none</code>を含む、任意のポリシーに追加できる任意のプロパティーです。 ● HostsInReserve: 実行中の仮想マシンがない場合でも、実行し続けるホストの数を指定します。これは、<code>power_saving</code>ポリシーに追加できる任意のプロパティーです。 ● EnableAutomaticHostPowerManagement: クラスター内のすべてのホストの自動電源管理を有効にします。これは、<code>power_saving</code>ポリシーに追加できる任意のプロパティーです。デフォルト値は<code>true</code>です。 ● MaxFreeMemoryForOverUtilized: ホストが持つ空きメモリーの最小量を指定します(MB単位)。ホストの空き容量がこれを下回る場合、RHV Managerはホストが過剰に使用されているとみなします。たとえば、このプロパティーを1000に設定すると、空きメモリーが1GB未満のホストが過剰使用とみなされます。 このプロパティーが<code>power_saving</code>および<code>evenly_distributed</code>ポリシーとどのように相互作用するかの詳細は、MaxFreeMemoryForOverUtilizedおよびMinFreeMemoryForUnderUtilizedクラスタースケジューリングポリシープロパティーを参照してください。 このプロパティーは、<code>power_saving</code>および<code>evenly_distributed</code>ポリシーに追加できます。<code>vm_evenly_distributed</code>ポリシーのプロパティーリストに表示されますが、このポリシーには適用されません。 ● MinFreeMemoryForUnderUtilized: ホストが持つべき空きメモリーの最大量を指定します(MB単位)。ホストが持つ空きメモリーがこの量を上回る場合、RHV Managerスケジューラーはホストの使用率が低いとみなします。たとえば、このパラメーターを10000に設定すると、空きメモリーが10 GBを超えるホストが十分に使用されていないとみなされます。 このプロパティーが<code>power_saving</code>および<code>evenly_distributed</code>ポリシーとどのように相互作用するかの詳細は、MaxFreeMemoryForOverUtilizedおよびMinFreeMemoryForUnderUtilizedクラスタースケジューリングポリシープロパティーを参照してください。 このプロパティーは、<code>power_saving</code>および<code>evenly_distributed</code>ポリシーに追加できます。<code>vm_evenly_distributed</code>ポリシーのプロパティーリストに表示されますが、このポリシーには適用されません。 ● HeSparesCount: Manager用仮想マシンを移行またはシャットダウンした場合に、そのマシンを起動するのに十分な空きメモリーを予約する必要があるセルフホスト型エンジンノードの数を設定します。Manager用仮想マシンに必要な空きメモリーが残らない場合、その他の仮想マシン

フィールド	説明/アクション
	はセルフホスト型エンジンノードで起動できなくなります。これ 説明/アクション: <code>power_saving</code> 、 <code>vm_evenly_distributed</code> 、 <code>evenly_distributed</code> ポリ シーに追加できる任意のプロパティーです。デフォルト値は 0 です。
Scheduler Optimization	<p>ホストの重み付け/順序のスケジューリングを最適化します。</p> <ul style="list-style-type: none"> ● Optimize for Utilization: スケジューリングに重みモジュールを追加し、最適な選択を可能にします。 ● Optimize for Speed: 保留中のリクエストの数が 10 個ある場合に、ホストの重み付けをスキップします。
Enable Trusted Service	OpenAttestation サーバーとのインテグレーションを有効にします。これを有効にする前に、 engine-config ツールを使用して OpenAttestation サーバーの詳細を入力します。 重要: OpenAttestation および Intel Trusted Execution Technology (Intel TXT) は利用できなくなりました。
Enable HA Reservation	Manager が高可用性仮想マシンのクラスター容量を監視できるようにします。Manager は、既存のホストに予期せぬ障害が発生した場合に移行するため、高可用性として指定された仮想マシンのクラスター内に適切な容量が存在することを確認します。

フィールド	説明/アクション
Serial Number Policy	<p>クラスター内の各新規仮想マシンにシリアル番号を割り当てるポリシーを設定します。</p> <ul style="list-style-type: none"> ● System Default: Manager データベースにシステム全体のデフォルトを使用します。これらのデフォルトを設定するには、エンジン設定ツールを使用して、DefaultSerialNumberPolicy および DefaultCustomSerialNumber の値を設定します。これらのキーと値のペアは、Manager データベースの vdc_options テーブルに保存されます。 <p>DefaultSerialNumberPolicy の場合:</p> <ul style="list-style-type: none"> ○ デフォルト値: HOST_ID ○ 使用できる値: HOST_ID、VM_ID、CUSTOM ○ コマンドラインの例: <code>engine-config --set DefaultSerialNumberPolicy=VM_ID</code> ○ 重要: Manager を再起動して設定を適用します。 <p>DefaultCustomSerialNumber:</p> <ul style="list-style-type: none"> ○ デフォルト値: Dummy シリアル番号 ○ 使用できる値: 任意の文字列 (最大長 255 文字) ○ コマンドラインの例: <code>engine-config --set DefaultCustomSerialNumber="My very special string value"</code> ○ 重要: Manager を再起動して設定を適用します。 <ul style="list-style-type: none"> ● Host ID: 新しい仮想マシンのシリアル番号を、ホストの UUID に設定します。 ● VM ID: 仮想マシンの UUID にそれぞれ新しい仮想マシンのシリアル番号を設定します。 ● Custom serial number: 以下の Custom Serial Number パラメーターで指定した値に、新しい仮想マシンのシリアル番号を設定します。
Custom Serial Number	クラスター内の新しい仮想マシンに適用するカスタムのシリアル番号を指定します。

ホストの空きメモリーが 20% 未満になると、**mom.Controllers.Balloon - INFO Ballooning guest:half1 from 1096400 to 1991580** が `/var/log/vdsdm/mom.log` に記録されます。`/var/log/vdsdm/mom.log` は、Memory Overcommit Manager のログファイルです。

2.3.2.6. MaxFreeMemoryForOverUtilized および MinFreeMemoryForUnderUtilized クラス タースケジューリングポリシーのプロパティ

スケジューラーには、現在のクラスタースケジューリングポリシーおよびそのパラメーターに従って仮想マシンを移行するバックグラウンドプロセスがあります。スケジューラーは、さまざまな基準と相対的な重みに基づいて、継続的にホストを 移行元ホスト または 移行先ホスト に分類し、個々の仮想マシンを移行元ホストから移行先ホストに移行します。

以下は、`evenly_distributed` および `power_saving` クラスタースケジューリングポリシーと、`MaxFreeMemoryForOverUtilized` および `MinFreeMemoryForUnderUtilized` プロパティーとの相互作用を説明しています。どちらのポリシーも CPU とメモリーの負荷を考慮しますが、CPU 負荷は `MaxFreeMemoryForOverUtilized` プロパティーおよび `MinFreeMemoryForUnderUtilized` プロパティーには関係ありません。

`MaxFreeMemoryForOverUtilized` プロパティーおよび `MinFreeMemoryForUnderUtilized` プロパティーを `evenly_distributed` ポリシーの一部として定義する場合:

- 空きメモリーが `MaxFreeMemoryForOverUtilized` より少ないホストが過剰使用とみなされ、移行元ホストになります。
- 空きメモリーが `MinFreeMemoryForUnderUtilized` よりも大きいホストが、十分に使用されていないとみなされ、移行先ホストになります。
- `MaxFreeMemoryForOverUtilized` が定義されていない場合、スケジューラーはメモリー負荷に基づいて仮想マシンを移行しません。(CPU 負荷など、ポリシーの他の基準に基づく仮想マシンの移行は継続されます。)
- `MinFreeMemoryForUnderUtilized` が定義されていない場合、スケジューラーはすべてのホストを移行先ホストとして適格であるとみなします。

`power_saving` ポリシーの一部として `MaxFreeMemoryForOverUtilized` および `MinFreeMemoryForUnderUtilized` プロパティーを定義する場合:

- 空きメモリーが `MaxFreeMemoryForOverUtilized` より少ないホストが過剰使用とみなされ、移行元ホストになります。
- 空きメモリーが `MinFreeMemoryForUnderUtilized` よりも大きいホストが過小使用とみなされ、移行元ホストになります。
- 空きメモリーが `MaxFreeMemoryForOverUtilized` よりも大きいホストが過剰使用ではないとみなされ、移行先ホストになります。
- 空きメモリーが `MinFreeMemoryForUnderUtilized` より少ないホストが過小使用ではないとみなされ、移行先ホストになります。
- スケジューラーは仮想マシンを移行する際に、過剰使用でも過小使用でもないホストへの移行を優先します。該当するホストが不足する場合、スケジューラーは仮想マシンを使用率の低いホストに移行できます。この目的で使用率の低いホストが必要ない場合は、スケジューラーはそのホストの電源を切ることができます。
- `MaxFreeMemoryForOverUtilized` が定義されていない場合は、ホストは過剰使用とみなされません。そのため、使用率の低いホストのみが移行元ホストとなり、クラスター内のすべてのホストが移行先ホストとみなされます。
- `MinFreeMemoryForUnderUtilized` が定義されていない場合は、使用率の低いホストのみが移行元ホストとなり、過剰使用されていないホストが移行先ホストになります。
- ホストによるすべての物理 CPU の過剰使用を防ぐには、仮想 CPU と物理 CPU の比率 (`VCpuToPhysicalCpuRatio`) を 0.1 - 2.9 の値で定義します。このパラメーターを設定すると、仮想マシンをスケジュールするときに CPU 使用率が低いホストが優先されます。仮想マシンを追加すると比率が制限を超える場合、`VCpuToPhysicalCpuRatio` と CPU 使用率の両方が考慮されます。

実行環境では、ホスト `VCpuToPhysicalCpuRatio` が 2.5 を超えると、一部の仮想マシンが負荷分散され、`VCpuToPhysicalCpuRatio` が低いホストに移動される可能性があります。

関連情報

- クラスタースケジューリングポリシーの設定

2.3.2.7. クラスターコンソール設定の説明

以下の表は、New Cluster および Edit Cluster ウィンドウの Console タブの設定を説明しています。

表2.11 コンソールの設定

フィールド	説明/アクション
Define SPICE Proxy for Cluster	このチェックボックスを選択すると、グローバル設定で定義された SPICE プロキシーのオーバーライドが有効になります。この機能は、ハイパーバイザーが存在するネットワークの外部にユーザー（たとえば、仮想マシンポータル経由で接続するユーザー）がいる場合に役に立ちます。
Overridden SPICE proxy address	SPICE クライアントが仮想マシンに接続するプロキシー。アドレスは以下の形式でなければなりません。 protocol://[host]:[port]

2.3.2.8. フェンシングポリシー設定の説明

以下の表は、New Cluster および Edit Cluster ウィンドウの Fencing Policy タブの設定を説明しています。

表2.12 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
Enable fencing	クラスターのフェンシングを有効にします。フェンシングはデフォルトで有効になっていますが、必要に応じて無効にできます。たとえば、一時的なネットワークの問題が発生したり、予想される場合に、管理者は診断またはメンテナンスアクティビティが完了するまでフェンシングを無効にできます。フェンシングが無効になっている場合、応答しないホストで実行している高可用性仮想マシンは、別の場所で再起動されないように注意してください。
Skip fencing if host has live lease on storage	このチェックボックスが選択されている場合、クラスター内でレスポンスがなく、引き続きストレージに接続されているホストはフェンスされません。

フィールド	説明/アクション
Skip fencing on cluster connectivity issues	このチェックボックスを選択すると、接続の問題が発生するクラスター内のホストのパーセンテージが、定義された Threshold 以上になると、フェンシングが一時的に無効になります。Threshold 値はドロップダウンリストから選択されます。利用可能な値は 25、50、75、および 100 です。
Skip fencing if gluster bricks are up	このオプションは、Red Hat Gluster Storage 機能が有効にされている場合にのみ利用できます。このチェックボックスを選択すると、ブリックが実行中で、他のピアから到達できる場合にフェンシングはスキップされます。 2章を参照してください。フェンシングポリシー を使用して高可用性を設定します。詳細は、 Red Hat ハイパーコンバージドインフラストラクチャーのメンテナンス の付録 A. Red Hat Gluster Storage のフェンシングポリシー を参照してください。
Skip fencing if gluster quorum not met	このオプションは、Red Hat Gluster Storage 機能が有効にされている場合にのみ利用できます。このチェックボックスが選択されている場合、ブリックが実行されているとフェンシングがスキップされ、ホストをシャットダウンするとクォーラムが失われます。 2章を参照してください。フェンシングポリシー を使用して高可用性を設定します。詳細は、 Red Hat ハイパーコンバージドインフラストラクチャーのメンテナンス の付録 A. Red Hat Gluster Storage のフェンシングポリシー を参照してください。

2.3.2.9. クラスター内のホストの負荷および電源管理ポリシーの設定

`evenly_distributed` および `power_saving` スケジューリングポリシーを使用すると、許容可能なメモリーおよび CPU 使用率の値と、仮想マシンとホスト間の移行が必要なポイント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布します。スケジューリングポリシーを定義して、クラスター内のホスト全体で自動負荷分散を有効にします。各スケジューリングポリシーの詳細は、[クラスター 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

1. Compute → Clusters をクリックし、クラスターを選択します。
2. Edit をクリックします。
3. Scheduling Policy タブをクリックします。
4. 以下のポリシーのいずれかを選択します。

- **none**
- **vm_evenly_distributed**
 - a. **HighVmCount** フィールドで、少なくとも1台のホストで実行されている必要がある仮想マシンの最小数を設定して、負荷分散を有効にします。
 - b. **MigrationThreshold** フィールドで、最も使用率の高いホスト上の仮想マシン数と、最も使用率の低いホスト上の仮想マシン数の、許容可能な最大差を定義します。
 - c. **SpmVmGrace** フィールドで、SPMホストで予約される仮想マシンのスロット数を定義します。
 - d. 必要に応じて **HeSparesCount** フィールドで、移行またはシャットダウンした場合に Manager用仮想マシンを起動できる十分な空きメモリーを確保する、追加のセルフホスト型エンジンノードの数を入力します。詳細は、[セルフホスト型エンジン用に予約されているメモリースロットの設定](#)を参照してください。
- **evenly_distributed**
 - a. **CpuOverCommitDurationMinutes** フィールドで、スケジューリングポリシーによりアクションが実行される前に、定義された使用率値の範囲外となるCPU負荷をホストで実行できる時間(分単位)を設定します。
 - b. **HighUtilization** フィールドに、仮想マシンが他のホストへの移行を開始するCPU使用率をパーセンテージで入力します。
 - c. 必要に応じて **HeSparesCount** フィールドで、移行またはシャットダウンした場合に Manager用仮想マシンを起動できる十分な空きメモリーを確保する、追加のセルフホスト型エンジンノードの数を入力します。詳細は、[セルフホスト型エンジン用に予約されているメモリースロットの設定](#)を参照してください。
 - d. ホストによるすべての物理CPUの過剰使用を防ぐには、仮想CPUと物理CPUの比率(**VCpuToPhysicalCpuRatio**)を0.1-2.9の値で定義します(オプション)。このパラメーターを設定すると、仮想マシンをスケジュールするときにCPU使用率が低いホストが優先されます。
仮想マシンを追加すると比率が制限を超える場合、**VCpuToPhysicalCpuRatio**とCPU使用率の両方が考慮されます。

実行環境では、ホスト **VCpuToPhysicalCpuRatio** が2.5を超えると、一部の仮想マシンが負荷分散され、**VCpuToPhysicalCpuRatio** が低いホストに移動される可能性があります。
- **power_saving**
 - a. **CpuOverCommitDurationMinutes** フィールドで、スケジューリングポリシーによりアクションが実行される前に、定義された使用率値の範囲外となるCPU負荷をホストで実行できる時間(分単位)を設定します。
 - b. **LowUtilization** フィールドに、その値を下回った場合に使用率が低すぎるとホストが判断するCPU使用率を入力します。
 - c. **HighUtilization** フィールドに、仮想マシンが他のホストへの移行を開始するCPU使用率をパーセンテージで入力します。
 - d. 必要に応じて **HeSparesCount** フィールドで、移行またはシャットダウンした場合に Manager用仮想マシンを起動できる十分な空きメモリーを確保する、追加のセルフホスト型エンジンノードの数を入力します。詳細は、[セルフホスト型エンジン用に予約されているメモリースロットの設定](#)を参照してください。

[されているメモリースロットの設定](#) を参照してください。

5. クラスターの **Scheduler Optimization** として、以下のいずれかを選択します。
 - **Optimize for Utilization**を選択すると、スケジューリングに重みモジュールが追加され、最適な選択が可能になります。
 - **Optimize for Speed**を選択すると、保留中のリクエスト数が 10 を上回る場合にホストの重み付けをスキップします。
6. OpenAttestation サーバーを使用してホストを確認し、**engine-config** ツールを使用してサーバーの詳細を設定している場合は、**Enable Trusted Service** チェックボックスを選択します。

OpenAttestation および Intel Trusted Execution Technology (Intel TXT) は利用できなくなりました。

1. 必要に応じて、**Enable HA Reservation** チェックボックスを選択し、Manager が高可用性仮想マシンのクラスター容量を監視できるようにします。
2. オプションで、クラスター内の仮想マシンの **Serial Number Policy** を選択します。
 - **System Default:** [エンジン設定ツール](#)、**DefaultSerialNumberPolicy**、**DefaultCustomSerialNumber** キー名を使用して Manager データベースに設定されたシステム全体のデフォルトを使用します。**DefaultSerialNumberPolicy** のデフォルト値は Host ID を使用します。詳細は、[管理ガイド](#) の [スケジューリングポリシー](#) を参照してください。
 - **Host ID:** 仮想マシンのシリアル番号を、ホストの UUID に設定します。
 - **VM ID:** 仮想マシンの UUID にそれぞれの仮想マシンのシリアル番号を設定します。
 - **Custom serial number:** 各仮想マシンのシリアル番号を、以下の **Custom Serial Number** パラメーターで指定した値に設定します。
3. **OK** をクリックします。

2.3.2.10. クラスター内のホストでの MoM ポリシーの更新

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

手順

1. **Compute** → **Clusters** をクリックします。
2. クラスターの名前をクリックします。詳細ビューが開きます。
3. **Hosts** タブをクリックして、更新後の MoM ポリシーが必要なホストを選択します。
4. **Sync MoM Policy** をクリックします。

ホストの MoM ポリシーが更新されます。その際に、ホストをメンテナンスマードに移行してから **Up** に戻す必要はありません。

2.3.2.11. CPU プロファイルの作成

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

この手順では、クラスターが属するデータセンター配下に1つ以上の CPU QoS エントリーがすでに定義されていることを前提としています。

手順

1. Compute → Clusters をクリックします。
2. クラスターの名前をクリックします。詳細ビューが開きます。
3. CPU Profiles タブをクリックします。
4. New をクリックします。
5. CPU プロファイルの Name および Description 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。

2.3.2.12. 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

1. Compute → Clusters をクリックします。
2. クラスターの名前をクリックします。詳細ビューが開きます。
3. CPU Profiles タブをクリックし、削除する CPU プロファイルを選択します。
4. Remove をクリックします。
5. OK をクリックします。

CPU プロファイルが仮想マシンに割り当てられている場合、それらの仮想マシンには default CPU プロファイルが自動的に割り当てられます。

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

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

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

手順

1. Compute → Clusters をクリックします。
2. New をクリックします。
3. クラスターが属する Data Center を選択します。
4. クラスターの Name および Description を入力します。
5. Enable Gluster Service チェックボックスを選択し、Import existing gluster configuration チェックボックスを選択します。
Import existing gluster configuration フィールドは、Enable Gluster Service が選択されている場合にのみ表示されます。
6. Hostname フィールドには、クラスター内のサーバーのホスト名または IP アドレスを入力します。
ホストの SSH Fingerprint が表示され、正しいホストに接続していることを確認します。ホストが到達不能な場合や、ネットワークエラーが発生した場合には、Error in fetching fingerprint のエラーが Fingerprint フィールドに表示されます。
7. サーバーの Password を入力し、OK をクリックします。
8. Add Hosts 画面が開き、クラスターに含まれるホストの一覧が表示されます。
9. 各ホストに Name と Root Password を入力します。
10. すべてのホストに同じパスワードを使用する場合は、Use a Common Password チェックボックスを選択して、指定したテキストフィールドにパスワードを入力します。
Apply をクリックして、すべてのホストに入力したパスワードを設定します。
Fingerprint が有効であることを確認し、OK をクリックして変更を送信します。

ブートストラップスクリプトは、インポート後にホストに必要な VDSM パッケージをすべてインストールして再起動します。これで、Red Hat Virtualization Manager に既存の Red Hat Gluster Storage クラスターが正常にインポートされました。

2.3.2.14. Add Hosts ウィンドウの設定の説明

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

表2.13 Gluster ホスト追加時の設定

フィールド	説明
Use a common password	このチェックボックスをオンになると、クラスターに属するすべてのホストに同じパスワードを使用します。Password フィールドにパスワードを入力し、Apply ボタンをクリックして全ホストにパスワードを設定します。
Name	ホストの名前を入力します。

フィールド	説明
Hostname/IP	このフィールドには、 New Cluster ウィンドウで指定したホストの完全修飾ドメイン名または IP が自動的に設定されます。
Root Password	各ホストに異なる root パスワードを使用するには、このフィールドにパスワードを入力します。このフィールドは、クラスター内のすべてのホストに提供される共通パスワードをオーバーライドします。
Fingerprint	ホストのフィンガープリントが表示され、正しいホストに接続していることを確認できます。このフィールドには、 New Cluster 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。

2.3.2.15. クラスターの削除

クラスターを削除する前に、すべてのホストをクラスターから移動します。



注記

Default クラスターは **Blank** テンプレートを保持するため、削除できません。ただし、**Default** クラスターの名前を変更し、新しいデータセンターに追加することは可能です。

手順

1. **Compute** → **Clusters** をクリックし、クラスターを選択します。
2. クラスターにホストがないことを確認します。
3. **Remove** をクリックします。
4. **OK** をクリックします。

2.3.2.16. メモリーの最適化

ホストの仮想マシン数を増やすには、**メモリーのオーバーコミット** を使用できます。その場合、仮想マシンに割り当てるメモリーは RAM を超え、スワップ領域に依存します。

ただし、メモリーのオーバーコミットには潜在的な問題があります。

- スワッピングパフォーマンス - スワップ領域が遅くなり、RAM よりも多くの CPU リソースを消費し、仮想マシンのパフォーマンスに影響を及ぼします。過度なスワッピングは、CPU のスラッシングにつながる可能性があります。
- OOM (Out-of-memory) killer: ホストがスワップ領域を使い果たすと、新規プロセスは開始できなくなり、カーネルの OOM killer デーモンは仮想マシンゲストなどのアクティブなプロセスのシャットダウンを開始します。

これらの欠点に対処するために、以下を実行できます。

- **Memory Optimization** 設定および **Memory Overcommit Manager (MoM)** を使用してメモリーのオーバーコミットを制限します。
- 仮想メモリーの潜在的な最大要求に対応できる大きな swap 領域を作成し、安全マージンを残します。
- **memory ballooning** および **Kernel Same-page Merging (KSM)** を有効にして、仮想メモリーサイズを縮小します。

2.3.2.17. メモリーの最適化とメモリーオーバーコミット

Memory Optimization 設定 (**None** (0%)、150%、または 200% のいずれか) を選択して、メモリーのオーバーコミット量を制限できます。

各設定は、RAM に対する割合を表します。たとえば RAM が 64 GB のホストの場合、150% を選択すると、32 GB をオーバーコミットでき、仮想メモリーは合計 96 GB となります。ホストが 4 GB を使用している場合、残りの 92 GB が利用可能になります。そのほとんどを仮想マシンに割り当てるることができます (**System** タブの **Memory Size**) が、安全マージンとして、その一部を割り当てずに残しておくことを検討してください。

仮想メモリーの要求が急増すると、MoM、メモリーバルーン、および KSM が仮想メモリーを再最適化するまで、パフォーマンスに影響が出る可能性があります。この影響を軽減するには、実行するアプリケーションおよびワークロードの種類に適した制限を選択します。

- 必要なメモリーの増分が大きいワークロードの場合は、200% または 150% などの高いパーセンテージを選択します。
- 必要なメモリーが急激に増加する重大なアプリケーションまたはワークロードの場合は、150% や **None** (0%) などの低いパーセンテージを選択します。**None** を選択するとメモリーのオーバーコミットを防ぎつつ、MoM、メモリーバルーンデバイス、および KSM における仮想メモリーの最適化を継続できます。



重要

設定を実稼働環境にデプロイする前に、さまざまな条件下で **Memory Optimization** の設定を必ずテストしてください。

Memory Optimization を設定するには、**New Cluster** または **Edit Cluster** ウィンドウの **Optimization** タブをクリックします。 [クラスター最適化設定の説明](#) を参照してください。

その他のコメント:

- [ホスト統計ビュー](#) には、オーバーコミットメント率のサイズを決定するための有用な履歴情報が表示されます。
- KSM とメモリーバルーニングにより得られるメモリー最適化のサイズは継続的に変化するため、実際に利用可能なメモリーをリアルタイムで決定することはできません。
- 仮想マシンが仮想メモリー制限に達すると、新しいアプリを開始できません。
- ホストで実行する仮想マシンの数を計画する際には、最大仮想メモリー (物理メモリーサイズと **Memory Optimization** 設定) から開始します。メモリーバルーニングや KSM などのメモリー最適化により実現される、より小さい仮想メモリーは考慮しないでください。

2.3.2.18. swap 領域とメモリーオーバーコミットメント

Red Hat は、[スワップ領域の設定に関する推奨事項](#) を提供しています。

これらの推奨事項を適用する場合は、ガイダンスに従い、ワーストケースシナリオにおける "最後のメモリー" としてスワップ領域のサイズを決定してください。物理メモリーのサイズと **Memory Optimization** 設定を、仮想メモリーサイズの合計を見積もるためのベースとして使用します。MoM、メモリーバルーニング、および KSM による最適化から仮想メモリーサイズの減少を除外してください。



重要

OOM 状態を回避するには、ワーストケースのシナリオを処理するのに十分な swap 領域を確保し、安全マージンを確保してください。実稼働環境にデプロイする前に、さまざまな条件で設定を常にテストしてください。

2.3.2.19. Memory Overcommit Manager(MoM)

Memory Overcommit Manager (MoM) は、以下の 2 つを行います。

- これは、前述のセクションで説明されているように、クラスターのホストに **Memory Optimization** 設定を適用してメモリーのオーバーコミットを制限します。
- 以下のセクションで説明されているように、**メモリーバルーニング** と **KSM** を管理することで、メモリーを最適化します。

MoM を有効または無効にする必要はありません。

ホストの空きメモリーが 20% 未満になると、**mom.Controllers.Balloon - INFO Ballooning guest:half1 from 1096400 to 1991580** が Memory Overcommit Manager ログファイル /var/log/vdsm/mom.log に記録されます。

2.3.2.20. メモリーバルーニング

仮想マシンは、割り当てた仮想メモリーの全量で開始されます。仮想メモリー使用量が RAM を超えると、スワップ領域へのホストの依存が大きくなります。メモリーバルーニングを有効にすると、仮想マシンはそのメモリーの未使用部分を解放できます。解放されたメモリーは、ホスト上の他のプロセスおよび仮想マシンで再利用できます。メモリーフットプリントが削減されると、スワッピングの可能性が低くなり、パフォーマンスが向上します。

メモリーバルーンデバイスとドライバーを提供する **virtio-balloon** パッケージは、ロードブルカーネルモジュール (LKM) として出荷されます。デフォルトでは、自動的にロードするように設定されています。モジュールを拒否リストに追加するかアンロードすると、バルーニングが無効になります。

メモリーバルーンデバイスは、相互に直接調整しません。MoM (ホストの Memory Overcommit Manager) プロセスに依存して、各仮想マシンのニーズを継続的に監視し、バルーンデバイスに仮想メモリーの増減を指示します。

パフォーマンスに関する考慮事項:

- Red Hat は、高パフォーマンスと低レイテンシーを継続的に必要とするワークロードには、メモリーバルーンおよびオーバーコミットを推奨しません。[高パフォーマンスの仮想マシンテンプレートおよびプールの設定](#) を参照してください。
- パフォーマンスよりも仮想マシンの密度 (経済性) を高めることが重要な場合は、メモリーバルーニングを使用します。

- メモリーバルーニングは CPU 使用率に大きな影響を及ぼしません。(KSM は一部の CPU リソースを消費しますが、負荷がかかっても消費量は変化しません。)

メモリーバルーニングを有効にするには、[New Cluster](#) または [Edit Cluster](#) ウィンドウの **Optimization** タブをクリックします。次に、**Enable Memory Balloon Optimization** チェックボックスを選択します。この設定により、このクラスターのホストで実行されている仮想マシンでメモリーのオーバーコミットが有効になります。このチェックボックスを選択すると、MoM はバルーニングを開始し、可能な場合はすべての仮想マシンのメモリーサイズが保証されます。[クラスター最適化設定の説明](#) を参照してください。

このクラスター内の各ホストは、ステータスが Up に変わったときにバルーンポリシーの更新を受け取ります。必要に応じて、ステータスを変更せずに、ホストのバルーンポリシーを手動で更新できます。[クラスター内のホストにおける MoM ポリシーの更新](#) を参照してください。

2.3.2.21. Kernel Same-page Merging (KSM)

仮想マシンの実行時には、一般的なライブラリーや使用頻度の高いデータといったアイテム向けに、重複したメモリーページが作成されることがあります。さらに、同じようなゲスト OS やアプリケーションを実行している仮想マシンでは、仮想メモリー内のメモリーページが重複してしまいます。

KSM (Kernel Sam-page Merging) を有効にすると、ホスト上の仮想メモリーを調査し、重複するメモリーページを排除して、残りのメモリーページを複数のアプリケーションや仮想マシンで共有できます。これらの共有メモリーページにはコピーオンライトのマークがついており、仮想マシンでページに変更を書き込む必要がある場合には、先にコピーを作成してからそのコピーに変更を書き込みます。

KSM が有効な間は、MoM が KSM を管理します。KSM を手動で設定制御する必要はありません。

KSM は、2つの方法で仮想メモリーのパフォーマンスを向上させます。共有メモリーのページは使用頻度が高いため、ホストはそのページをキャッシュやメインメモリーに格納する可能性が高くなり、メモリーアクセス速度が向上します。さらに、メモリーオーバーコミットを使用することで、KSM は仮想メモリーのフットプリントを減らし、スワッピング発生の可能性を軽減してパフォーマンスを向上させます。

KSM はメモリーバルーニングよりも多くの CPU リソースを消費します。KSM の CPU 消費量は、負荷をかけても変わりません。同一の仮想マシンやアプリケーションをホスト上で実行すると、KSM は異なる仮想マシンを実行する場合と比較して、メモリーページをマージする機会が多くなります。異なる仮想マシンやアプリケーションを多く実行している場合には、KSM を使用するための CPU コストにより利点が相殺されてしまう可能性があります。

パフォーマンスに関する考慮事項:

- KSM デーモンが大量のメモリーをマージした後に、カーネルメモリアカウンティング統計が最終的に矛盾することがあります。システムに大量の空きメモリーがある場合には、KSM を無効にするとパフォーマンスが向上することがあります。
- Red Hat は、パフォーマンスが高く、低レイテンシーを必要とするワークロードには KSM およびオーバーコミットを推奨しません。[高パフォーマンスの仮想マシンテンプレートおよびプロファイルの設定](#) を参照してください。
- パフォーマンスよりも仮想マシンの密度(経済性)を高めることが重要な場合は、KSM を使用します。

KSM を有効にするには、[New Cluster](#) または [Edit Cluster](#) ウィンドウの **Optimization** タブをクリックします。次に、**Enable KSM** のチェックボックスを選択します。この設定を使用すると、MoM は必要なときに KSM を実行でき、CPU コストを上回るメモリー節約のメリットが得られます。[クラスター最適化設定の説明](#) を参照してください。

2.3.2.22. UEFI と Q35 チップセット

新しい仮想マシンのデフォルトのチップセットであるインテル Q35 チップセットは、従来の BIOS に代わる UEFI (Unified Extensible Firmware Interface) に対応しています。

また、UEFI に対応していないレガシーの Intel i440fx チップセットを使用するように仮想マシンやクラスターを設定することもできます。

UEFI には、従来の BIOS に比べて以下のようなメリットがあります。

- 最新のブートローダー
- ブートローダーのデジタル署名を認証する SecureBoot
- 2TB 以上のディスクに対応した GUID パーティションテーブル (GPT)

仮想マシンで UEFI を使用するには、仮想マシンクラスターの互換性レベルを 4.4 以降に設定する必要があります。その後、既存の仮想マシンに UEFI を設定したり、クラスター内の新しい仮想マシンのデフォルト BIOS タイプに設定したりすることができます。以下のオプションを設定できます。

表2.14 利用可能な BIOS タイプ

BIOS タイプ	説明
Q35 チップセットとレガシー BIOS	UEFI 未対応のレガシー BIOS (互換性バージョン 4.4 のクラスターのデフォルト)
UEFI BIOS 対応の Q35 チップセット	UEFI 対応の BIOS
Q35 チップセット (SecureBoot 対応)	ブートローダーのデジタル署名を認証する SecureBoot に対応した UEFI
レガシー	レガシー BIOS 対応した i440fx チップセット

OS インストール前の BIOS タイプの設定

オペレーティングシステムをインストールする前に、Q35 チップセットと UEFI を使用するように仮想マシンを設定できます。オペレーティングシステムのインストール後に、仮想マシンのレガシー BIOS から UEFI への変換はサポートされていません。

2.3.2.23. Q35 チップセットと UEFI を使用するクラスターの設定

クラスターを Red Hat Virtualization 4.4 にアップグレードすると、クラスター内のすべての仮想マシンが VDSM の 4.4 バージョンを実行します。クラスターのデフォルトの BIOS タイプを設定すると、そのクラスターで作成する新しい仮想マシンのデフォルトの BIOS タイプが決定されます。必要に応じて、仮想マシンの作成時に異なる BIOS タイプを指定して、クラスターのデフォルトの BIOS タイプを上書きできます。

手順

1. 仮想マシンポータルまたは管理ポータルで、Compute → Clusters をクリックします。
2. クラスターを選択し、Edit をクリックします。

3. General をクリックします。
4. クラスター内の新しい仮想マシンのデフォルトの BIOS タイプを定義するには、BIOS Type ドロップダウンメニューをクリックし、以下のいずれかを選択します。
 - Legacy
 - Q35 Chipset with Legacy BIOS
 - Q35 Chipset with UEFI BIOS
 - Q35 チップセット (SecureBoot 対応)
5. Compatibility Version ドロップダウンメニューから 4.4 を選択します。Manager は、稼働中のすべてのホストが 4.4 と互換性があるかどうかを確認し、互換性がある場合は 4.4 の機能を使用します。
6. クラスター内の既存の仮想マシンが新しい BIOS タイプを使用する必要がある場合は、そのように設定します。BIOS タイプとして Cluster default を使用するように設定されたクラスター内の新しい仮想マシンは、選択した BIOS タイプを使用するようになりました。詳細は、[仮想マシンで Q35 チップセットと UEFI を使用するための設定](#) を参照してください。



注記

BIOS タイプの変更はオペレーティングシステムのインストール前にしかできないため、BIOS タイプとして Cluster default を使用するように設定されている既存の仮想マシンについては、BIOS タイプを以前のデフォルトクラスターの BIOS タイプに変更してください。そうしないと、仮想マシンが起動しないことがあります。また、仮想マシンの OS を再インストールする方法もあります。

2.3.2.24. 仮想マシンで Q35 チップセットと UEFI を使用するための設定

オペレーティングシステムをインストールする前に、Q35 チップセットと UEFI を使用するように仮想マシンを設定できます。仮想マシンをレガシー BIOS から UEFI に変換したり、UEFI からレガシー BIOS に変換したりすると、仮想マシンが起動しなくなることがあります。既存の仮想マシンの BIOS タイプを変更した場合は、OS を再インストールしてください。



警告

仮想マシンの BIOS タイプが Cluster default に設定されている場合、クラスターの BIOS タイプを変更すると、仮想マシンの BIOS タイプも変更されます。仮想マシンにオペレーティングシステムがインストールされている場合、クラスターの BIOS タイプを変更すると、仮想マシンの起動に失敗することがあります。

手順

Q35 チップセットと UEFI を使用するように仮想マシンを設定する方法:

1. 仮想マシンポータルまたは管理ポータルで Compute → Virtual Machines をクリックします。
2. 仮想マシンを選択し、Edit をクリックします。

3. General タブで Show Advanced Options をクリックします。
4. System → Advanced Parameters をクリックします。
5. BIOS Type ドロップダウンメニューから以下のいずれかを選択します。
 - Cluster default
 - Q35 Chipset with Legacy BIOS
 - Q35 Chipset with UEFI BIOS
 - Q35 チップセット (SecureBoot 対応)
6. OK をクリックします。
7. 仮想マシンポータルまたは管理ポータルから、仮想マシンの電源をオフにします。次に仮想マシンを起動すると、選択した新しい BIOS タイプで実行されます。

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

前提条件

- クラスターの互換レベルを変更するには、まず、クラスター内のすべてのホストを更新して、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る。更新が利用可能であることを示すアイコンがホストの横にあるかどうかを確認します。

制限

- クラスター互換性レベルを 4.6 にアップグレードすると、VirtIO NIC は別のデバイスとして列挙されます。そのため、NIC の再設定が必要になる場合があります。Red Hat は、仮想マシンをテストするために、クラスターをアップグレードする前に仮想マシンでクラスター互換性レベルを 4.6 に設定し、ネットワーク接続を確認することをお勧めします。
仮想マシンのネットワーク接続に失敗した場合は、クラスターをアップグレードする前に、現在のエミュレートされたマシンと一致するカスタムのエミュレートされたマシンを使用して、仮想マシンを設定します (例: 4.5 互換バージョンの場合は pc-q35-rhel8.3.0)。

手順

1. 管理ポータルで、Compute → Clusters をクリックします。
2. 変更を行うクラスターを選択し、Edit をクリックします。
3. General タブで Compatibility Version を必要な値に変更します。
4. OK をクリックします。Change Cluster Compatibility Version の確認ダイアログが開きます。
5. OK をクリックして確定します。



重要

一部の仮想マシンおよびテンプレートが不適切に設定されていることを警告するエラーメッセージが表示される場合があります。このエラーを修正するには、それぞれの仮想マシンを手動で編集します。Edit Virtual Machine ウィンドウには、修正が必要な項目を示す追加の検証および警告が表示されます。問題が自動的に修正され、仮想マシンの設定を再度保存するだけで十分な場合もあります。それぞれの仮想マシンを編集したら、クラスターの互換バージョンを変更することができます。

クラスターの互換バージョンを更新したら、実行中または一時停止中のすべての仮想マシンについてクラスターの互換バージョンを更新する必要があります。そのためには、管理ポータルから再起動するか、REST API を使用するか、ゲストオペレーティングシステム内から更新する必要があります。再起動が必要な仮想マシンには、変更が保留されていることを示すアイコン (⚠) が付きます。プレビュー段階の仮想マシンスナップショットの場合、クラスターの互換バージョンは変更できません。まずコミットするか、プレビューを取り消す必要があります。

セルフホスト型エンジン環境では、Manager 仮想マシンを再起動する必要はありません。

別途適切な時期に仮想マシンを再起動することもできますが、仮想マシンで最新の設定が使用されるように、直ちに再起動することを強く推奨します。更新されていない仮想マシンは古い設定で実行され、再起動前に仮想マシンに他の変更を加えた場合には新しい設定が上書きされてしまう可能性があります。

データセンター内のすべてのクラスターと仮想マシンの互換性バージョンを更新したら、データセンター自身の互換性バージョンを変更できます。

2.4. 論理ネットワーク

2.4.1. 論理ネットワークタスク

2.4.1.1. ネットワークタスクの実行

Network → Networks は、ユーザーが論理ネットワーク関連の操作を実行し、各ネットワークのプロパティーや他のリソースとの関連付けに基づいて論理ネットワークを検索するための中心的な場所を提供します。New、Edit、Remove ボタンで、データセンター内の論理ネットワークの作成、プロパティーの変更、削除ができます。

各ネットワーク名をクリックし、詳細表示のタブを使って以下の機能を実行します。

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

これらの機能は、それぞれのリソースからもアクセス可能です。



警告

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



重要

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

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

- ディレクトリーサービス
- DNS
- ストレージ

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

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

手順

1. Compute → Data Centers または Compute → Clusters をクリックします。
2. データセンターネームまたはクラスターネームをクリックします。Details ビューが開きます。
3. Logical Networks タブをクリックします。
4. New Logical Network ウィンドウを開きます。
 - データセンターの詳細表示から、New をクリックします。
 - クラスターの詳細表示で、Add Network をクリックします。
5. 論理ネットワークの Name、Description、および Comment を入力します。
6. オプション: Enable VLAN tagging を有効にします。
7. オプション: VM Network を無効にします。
8. オプション: Create on external provider チェックボックスを選択します。これにより、ネットワークラベルと VM ネットワークが無効になります。詳細は、[外部プロバイダー](#) を参照してください。
 - a. External Providerを選択します。外部プロバイダーのリストには、読み取り専用モードの外部プロバイダーは含まれません。

- b. 内部の分離されたネットワークを作成するには、External Provider リストで **ovirt-provider-ovn** を選択し、Connect to physical network はそのままオフにしておきます。
- 9. Network Label テキストフィールドに、論理ネットワークの新しいラベルを入力するか、既存のラベルを選択します。
- 10. MTU については、Default (1500) を選択するか、Custom を選択してカスタム値を指定します。



重要

外部のプロバイダーでネットワークを作成した後は、ネットワークの MTU 設定を変更できません。



重要

ネットワークの MTU 設定を変更する場合は、この変更をネットワーク上で実行中の仮想マシンに伝達する必要があります。それには、MTU 設定を適用する必要があるすべての仮想マシンの vNIC をホットアンプラグ/再プラグするか、仮想マシンを再起動します。そうしないと、仮想マシンが別のホストに移行すると、これらのインターフェイスが失敗します。詳細は、[After network MTU change, some VMs and bridges have the old MTU and seeing packet drops](#) と [BZ#1766414](#) を参照してください。

- 11. External Provider ドロップダウンリストから **ovirt-provider-ovn** を選択した場合は、ネットワークに **Security Groups** を実装するかどうかを定義します。詳細は、[論理ネットワークの一般設定の説明](#) を参照してください。
- 12. Cluster 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。また、論理ネットワークを必須ネットワークにするかどうかも指定できます。
- 13. Create on external provider チェックボックスが選択されている場合は、Subnet タブが表示されます。Subnet タブから Create subnet を選択し、Name、CIDR、Gateway アドレスを入力し、論理ネットワークが割り当てるサブネットの IP Version を選択します。必要に応じて DNS サーバーを追加することもできます。
- 14. vNIC Profiles タブで、必要に応じて vNIC プロファイルを論理ネットワークに追加します。
- 15. **OK** をクリックします。

論理ネットワークにラベルを入力した場合は、そのラベルが割り当てられたすべてのホストネットワークインターフェイスに自動的に追加されます。



注記

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

2.4.1.3. 論理ネットワークの編集



重要

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



重要

ディスプレイネットワークとして使用される既存論理ネットワークの **VM** ネットワークプロパティーを変更すると、すでに稼働マシンが実行されているホスト上で新しい仮想マシンを起動することはできません。**VM Network** プロパティーの変更後に仮想マシンが実行されていないホストのみ、新しい仮想マシンを起動できます。

手順

1. **Compute** → **Data Centers** をクリックします。
2. データセンターの名前をクリックします。詳細ビューが開きます。
3. **Logical Networks** タブをクリックして、論理ネットワークを選択します。
4. **Edit** をクリックします。
5. 必要な設定を編集します。



注記

デフォルトのネットワーク除き、新規または既存のネットワークの名前は、仮想マシンを停止しなくとも編集できます。

6. **OK** をクリックします。



注記

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

2.4.1.4. 論理ネットワークの削除

Network → **Networks** または **Compute** → **Data Centers** から論理ネットワークを削除できます。以下の手順では、データセンターに関連付けられた論理ネットワークを削除する方法を説明します。Red Hat Virtualization の環境では、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

1. **Compute** → **Data Centers** をクリックします。
2. データセンターの名前をクリックします。詳細ビューが開きます。

3. Logical Networks タブをクリックすると、データセンター内の論理ネットワークがリストアップされます。
4. 論理ネットワークを選択し、Remove をクリックします。
5. オプションで、ネットワークが外部のプロバイダーによって提供されている場合は、Remove external network (s) from the provider (s) as well チェックボックスを選択して、Manager と外部のプロバイダーの両方から論理ネットワークを削除してください。外部プロバイダーが読み取り専用モードの場合、チェックボックスはグレーアウトされます。
6. OK をクリックします。

論理ネットワークが Manager から削除され、利用できなくなります。

2.4.1.5. 非管理者用論理ネットワークのデフォルトルートとしての設定

クラスター内のホストが使用するデフォルトのルートは、管理ネットワーク (**ovirtmgmt**) を経由します。以下では、非管理者用の論理ネットワークをデフォルトルートとして設定する手順を説明します。

前提条件:

- **default_route** カスタムプロパティを使用している場合、接続しているすべてのホストからカスタムプロパティの設定を解除してから、この手順を実行する必要があります。

デフォルトルートロールの設定

1. Network → Networks をクリックします。
2. デフォルトルートとして設定する非管理用論理ネットワークの名前をクリックすると、その詳細が表示されます。
3. Clusters タブをクリックします。
4. Manage Network をクリックします。Manage Network ウィンドウが表示されます。
5. 該当するクラスターの Default Route チェックボックスを選択します。
6. OK をクリックします。

ホストにネットワークが接続されている場合、ホストのデフォルトルートは選択したネットワークに設定されます。クラスターにホストを追加する前に、デフォルトルートのロールを設定することをお勧めします。クラスターにすでにホストが含まれている場合は、変更内容をホストに同期するまで、ホストが同期しなくなる可能性があります。

IPv6 の重要な制限事項

- IPv6 の場合、Red Hat Virtualization でサポートされるのは静的アドレスのみです。
- 両方のネットワークが単一のゲートウェイを共有している(同じサブネット上にある)場合は、デフォルトルートのロールを管理ネットワーク (**ovirtmgmt**) から別の論理ネットワークに移動できます。
- ホストと Manager が同じサブネットにない場合には、IPv6 ゲートウェイが削除されているため、Manager はホストとの接続を失います。
- デフォルトのルートロールを非管理ネットワークに移動すると、ネットワークインターフェイスから IPv6 ゲートウェイが削除され、次の警告が表示されます: "On cluster **clusternname** the

'Default Route Role' network is no longer network ovirtmgmt.The IPv6 gateway is being removed from this network."

2.4.1.6. ホストでの静的ルートの追加

`nmstate` を使ってホストに静的ルートを追加できます。この方法では、Red Hat Virtualization Manager を使用せずにホストを直接設定する必要があります。

追加した静的ルートは、関連するルーティングブリッジ、インターフェイス、またはボンドが存在し、IP アドレスがある限り保存されます。そうでなければ、システムは静的ルートを削除します。



重要

ホストの静的ルートを追加または削除する場合を除き、クラスター内のホストのネットワーク設定は常に RHV Manager を使用して行います。詳細は、[Network Manager のステートフル設定 \(nmstate\)](#) を参照してください。



注記

カスタムの静的ルートは、そのインターフェイス/ボンドが存在し、IP アドレスが存在する限り、保存されます。それ以外の場合は削除されます。

その結果、VM ネットワークは、VM ネットワーク以外とは異なる動作をします。

- VM ネットワークは、ブリッジをベースにしています。ネットワークを別のインターフェイス/ボンドに移動しても、VM ネットワークのルートには影響しません。
- VM ネットワーク以外では、インターフェイスをベースにしています。ネットワークを別のインターフェイス/ボンドに移動すると、VM ネットワーク以外のネットワークと関連するルートが削除されます。

前提条件

この手順には `nmstate` が必要です。これは、環境で以下を使用する場合にのみ使用できます。

- Red Hat Virtualization Manager バージョン 4.4
- Red Hat Enterprise Linux 8 をベースにした Red Hat Enterprise Linux ホストおよび Red Hat Virtualization Hosts

手順

1. 設定するホストに接続します。
2. ホスト上に、以下の例の内容で `static_route.yml` ファイルを作成します。

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

3. 表示されている例の値は、ネットワークの実際の値に置き換えてください。

4. セカンダリーに追加されたネットワークにトラフィックをルーティングするには、**next-hop-interface** を使ってインターフェイスやネットワーク名を指定します。
 - 仮想マシン以外のネットワークを使用する場合は、**eth1** などのインターフェイスを指定します。
 - 仮想マシンのネットワークを使用するには、**net1** のようにブリッジ名でもあるネットワーク名を指定します。
5. このコマンドを実行します。

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

検証手順

- **static_route.yml** で設定した宛先パラメーターの値を指定して、IP ルートコマンドの **ip route** を実行します。これで目的のルートが表示されるはずです。たとえば、以下のコマンドを実行します。
- ```
$ ip route | grep 192.168.123.0`
```

## 関連情報

- [Network Manager Stateful Configuration \(nmstate\)](#)
- [ホストでの静的ルートの削除](#)

### 2.4.1.7. ホストでの静的ルートの削除

`nmstate` を使ってホストからスタティックルートを削除することができます。この方法では、Red Hat Virtualization Manager を使用せずにホストを直接設定する必要があります。



#### 重要

ホストの静的ルートを追加または削除する場合を除き、クラスター内のホストのネットワーク設定は常に RHV Manager を使用して行います。詳細は、[Network Manager のステートフル設定 \(nmstate\)](#) を参照してください。



#### 注記

カスタムの静的ルートは、そのインターフェイス/ボンドが存在し、IP アドレスが存在する限り、保存されます。それ以外の場合は削除されます。

その結果、VM ネットワークは、VM ネットワーク以外とは異なる動作をします。

- VM ネットワークは、ブリッジをベースにしています。ネットワークを別のインターフェイス/ボンドに移動しても、VM ネットワークのルートには影響しません。
- VM ネットワーク以外では、インターフェイスをベースにしています。ネットワークを別のインターフェイス/ボンドに移動すると、VM ネットワーク以外のネットワークと関連するルートが削除されます。

## 前提条件

この手順には nmstate が必要です。これは、環境で以下を使用する場合にのみ使用できます。

- Red Hat Virtualization Manager バージョン 4.4
- Red Hat Enterprise Linux 8 をベースにした Red Hat Enterprise Linux ホストおよび Red Hat Virtualization Hosts

## 手順

1. 再設定するホストに接続します。
2. ホストで、**static\_route.yml** ファイルを編集します。
3. 次の例のように、**state: absent** の行を挿入します。
4. **interfaces: []** のカッコの間に、**next-hop-interface** の値を追加します。結果は以下の例のようになります。

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

5. このコマンドを実行します。

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

## 検証手順

- **static\_route.yml** で設定した宛先パラメーターの値を指定して、IP ルートコマンドの **ip route** を実行します。これで目的のルートが表示されなくなるはずです。たとえば、以下のコマンドを実行します。

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

## 関連情報

- [Network Manager Stateful Configuration \(nmstate\)](#)
- [ホストでの静的ルートの追加](#)

### 2.4.1.8. 論理ネットワークのゲートウェイの表示と編集

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

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

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

## 手順

1. **Compute** → **Hosts** をクリックします。
2. ホストの名前をクリックします。詳細ビューが開きます。
3. **Network Interfaces** タブをクリックすると、ホストに接続されているネットワークインターフェイスとその設定内容が一覧表示されます。
4. **Setup Host Networks** をクリックします。
5. 割り当てられた論理ネットワークにカーソルを合わせ、鉛筆アイコンをクリックします。これにより、**Edit Management Network** ウィンドウが開きます。

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

### 2.4.1.9. 論理ネットワーク一般設定の説明

以下の表では、**New Logical Network** および **Edit Logical Network** ウィンドウの **General** タブの設定を説明しています。

表2.15 New Logical Network と Edit Logical Network の設定

| フィールド名  | 説明                                                                             |
|---------|--------------------------------------------------------------------------------|
| Name    | 論理ネットワークの名前。このテキストフィールドは、大文字、小文字、数字、ハイフン、およびアンダースコアの組み合わせが含まれる一意の名前である必要があります。 |
| 説明      | 論理ネットワークの説明。このテキストフィールドには 40 文字の制限があります。                                       |
| Comment | 論理ネットワークに関するプレーンテキストの、人間が判読できる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                                                                                                                                                                                                                                   |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create on external provider | <p>外部プロバイダーとして Manager に追加された OpenStack Networking インスタンスへの論理ネットワークを作成できます。</p> <p><b>External Provider</b> - 論理ネットワークを作成するための外部プロバイダーを選択できます。</p>                                                                                   |
| Enable VLAN tagging         | VLAN タグは、論理ネットワークで伝送されるすべてのネットワークトラフィックに特別な特性を与えるセキュリティー機能です。VLAN タグ付きのトラフィックは、その特性のないインターフェイスでは読み取れません。また、論理ネットワークに VLAN を使用すると、1つのネットワークインターフェイスに、複数の異なる VLAN タグ付き論理ネットワークを関連付けることができます。VLAN のタグ付けが有効な場合は、テキストエントリーフィールドに数値を入力します。 |
| VM Network                  | このネットワークを使用するのが仮想マシンのみの場合は、このオプションを選択します。ストレージの通信など、仮想マシンを介さないトラフィックにネットワークを使用する場合は、このチェックボックスを選択しないでください。                                                                                                                           |
| Port Isolation              | これが設定されている場合、同じホスト上の仮想マシンは、この論理ネットワーク上で相互に通信および認識できなくなります。このオプションを異なるハイパーバイザー上で動作させるためには、ハイパーバイザーに接続されているそれぞれのポート/VLAN に PVLAN/ポート分離を設定し、ヘアピン設定をしたフレームを反射させないようにする必要があります。                                                           |

| フィールド名          | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MTU             | <p><b>Default</b> または <b>Custom</b> を選択できます。 <b>Default</b> は最大伝送単位 (MTU) を括弧 () で指定された値に設定し、<b>Custom</b> は論理ネットワークのカスタム MTU を設定します。これをを利用して、新しい論理ネットワークでサポートされる MTU を、それがインターフェースで接続するハードウェアでサポートされる MTU に一致させることができます。<b>Custom</b> 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ます。重要: ネットワークの MTU 設定を変更する場合は、この変更をネットワーク上で実行中の仮想マシンに伝播する必要があります。それには、MTU 設定を適用する必要があるすべての仮想マシンの vNIC をホットアンプラグ/再プラグするか、仮想マシンを再起動します。そうしないと、仮想マシンが別のホストに移行すると、これらのインターフェイスが失敗します。詳細は、<a href="#">After network MTU change, some VMs and bridges have the old MTU and seeing packet drops</a> と <a href="#">BZ#1766414</a> を参照してください。</p> |
| Network Label   | <p>ネットワークの新しいラベルを指定したり、ホストネットワークインターフェイスに既にアタッチされている既存のラベルを選択したりすることができます。既存のラベルを選択した場合には、そのラベルが指定されたすべてのホストネットワークインターフェイスに論理ネットワークが自動的に割り当てられます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Security Groups | <p>この論理ネットワーク上のポート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。<b>Disabled</b> は、セキュリティーグループ機能を無効にします。<b>Enabled</b> は、この機能を有効にします。ポートを作成してこのネットワークに接続すると、ポートセキュリティーが有効な状態で定義されます。つまり、仮想マシンに対するアクセスには、現在プロビジョニングされているセキュリティーグループが適用されることになります。<b>Inherit from Configuration</b> では、すべてのネットワークで定義されている設定ファイルの動作をポートに継承させます。デフォルトでは、このファイルはセキュリティーグループを無効にします。詳細は、<a href="#">論理ネットワークへのセキュリティーグループの割り当て</a> を参照してください。</p>                                                                                                                                                                                                     |

#### 2.4.1.10. 論理ネットワーククラスター設定の説明

以下の表は、New Logical Network ウィンドウの Cluster タブの設定を説明しています。

表2.16 New Logical Network 設定

| フィールド名                                   | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Attach/Detach Network to/from Cluster(s) | <p>論理ネットワークをデータセンター内のクラスターにアタッチまたはデタッチでき、論理ネットワークを個々のクラスターに必要なネットワークとするかどうかを指定することができます。</p> <p><b>Name</b> - 設定が適用されるクラスターの名前。この値は編集できません</p> <p><b>Attach All</b> - データセンター内のすべてのクラスターとの間で、論理ネットワークをアタッチまたはデタッチできます。各クラスターの名前の横にある <b>Attach</b> チェックボックスを選択または選択解除して、論理ネットワークを特定のクラスターに接続したり、クラスターから分離したりすることもできます。</p> <p><b>Required All</b> - 論理ネットワークがすべてのクラスターで必須のネットワークであるかどうかを指定できます。各クラスターの名前の横にある <b>Required</b> チェックボックスを選択または選択解除して、論理ネットワークが特定のクラスターに必要なネットワークであるかどうかを指定することもできます。</p> |

#### 2.4.1.11. 論理ネットワークの vNIC プロファイル設定の説明

以下の表は、New Logical Network ウィンドウの vNIC Profiles タブの設定を説明しています。

表2.17 New Logical Network 設定

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

#### 2.4.1.12. Manage Networks ウィンドウを使用した論理ネットワークの特定トラフィックタイプの指定

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

## 手順

1. Compute → Clusters をクリックします。
2. クラスターの名前をクリックします。詳細ビューが開きます。
3. Logical Networks タブをクリックします。
4. Manage Networks をクリックします。
5. 適切なチェックボックスやラジオボタンを選択してください。
6. OK をクリックします。



### 注記

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

#### 2.4.1.13. ネットワーク管理画面での設定内容の説明

以下の表では、Manage Networks ウィンドウの設定を説明しています。

表2.18 Manage Networks 設定

| フィールド             | 説明/アクション                                                                                                                     |
|-------------------|------------------------------------------------------------------------------------------------------------------------------|
| Assign            | クラスター内の全ホストに論理ネットワークを割り当てます。                                                                                                 |
| Required          | "required" と表示されたネットワークに関連付けられたホストは、そのネットワークが常に稼働していないければ、正しく機能しません。必須ネットワークが機能しなくなると、そのネットワークに関連付けられたホストはすべて動作しなくなります。      |
| VM Network        | "VM Network" 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するネットワークトラフィックを伝送します。                                                          |
| Display Network   | "Display Network" とマークされた論理ネットワークは、SPICE と仮想ネットワークコントローラーに関するネットワークトラフィックを伝送します。                                             |
| Migration Network | "Migration Network" とマークされた論理ネットワークは、仮想マシンとストレージの移行トラフィックを伝送します。このネットワークに障害が発生した場合には、代わりに管理ネットワーク ovirtmgmt (デフォルト) が使用されます。 |

#### 2.4.1.14. NIC での仮想機能の設定



## 注記

これは、Red Hat Virtualization で SR-IOV を準備およびセットアップする方法を示す一連のトピックの1つです。詳細は、[SR-IOV のセットアップと設定](#) を参照してください。

Single Root I/O Virtualization (SR-IOV) を使用すると、物理機能 (PF) と仮想機能 (VF) を用いて、各 PCIe エンドポイントを複数の独立したデバイスとして使用できます。1枚の PCIe カードには、1~8個の PF が搭載されています。それぞれの PF には VF が多数含まれます。含めることのできる VF の数は、PCIe デバイスの種類によって異なります。

SR-IOV 対応のネットワークインターフェイスコントローラー (NIC) を設定するには、Red Hat Virtualization Manager を使用します。Red Hat Virtualization Manager では、各 NIC の VF の数を設定できます。

VF は、スタンドアロンの NIC と同じように、以下のように設定できます。

- VF に1つまたは複数の論理ネットワークを割り当てる。
- VF との連携インターフェイスを構築する。
- VF に vNIC を割り当てて、デバイスを直接パススルーする。

デフォルトでは、すべての仮想ネットワークが仮想機能にアクセスできます。このデフォルトを無効にして、どのネットワークが仮想機能にアクセスできるかを指定することができます。

## 前提条件

- vNIC を VF マスターに接続するためには、そのパススループロパティーを有効にする必要があります。詳細は、[Enabling\\_Passthrough\\_on\\_a\\_vNIC\\_Profile](#) を参照してください。

## 手順

1. **Compute** → **Hosts** をクリックします。
2. SR-IOV 対応ホストの名前をクリックします。詳細ビューが開きます。
3. **Network Interfaces** タブをクリックします。
4. **Setup Host Networks** をクリックします。
5. ( のマークが付いた) SR-IOV 対応の NIC を選択し、鉛筆アイコンをクリックします。
6. オプション: 仮想機能の数を変更するには、**Number of VFs setting** ドロップダウンボタンをクリックし、**Number of VFs** テキストフィールドを編集します。



## 重要

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

7. オプション: 仮想機能にアクセスできる仮想ネットワークを制限するには、**Specific networks** を選択します。

- a. VF にアクセスすべきネットワークを選択するか、Labels を使ってネットワークラベルに基づきネットワークを選択します。
8. **OK** をクリックします。
9. **Setup Host Networks** ウィンドウで **OK** をクリックします。

## 2.4.2. 仮想ネットワークインターフェイスカード (vNIC)

### 2.4.2.1. vNIC プロファイルの概要

バーチャルネットワークインターフェイスカード (vNIC) のプロファイルは、Manager 内の個々のバーチャルネットワークインターフェイスカードに適用できる設定の集まりです。vNIC プロファイルでは、ネットワーク QoS プロファイルの vNIC への適用、ポートミラーリングの有効化/無効化、カスタムプロパティーの追加/削除が可能です。また、vNIC プロファイルは、特定のユーザーに使用 (消費) のパーミッションを与えることができるという点で、管理上の柔軟性において、追加の切り口が提供されています。このようにして、異なるユーザーが特定のネットワークから受けるサービスの質を制御できます。

### 2.4.2.2. vNIC プロファイルの作成と編集

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



#### 注記

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

#### 手順

1. **Network → Networks** をクリックします。
2. 論理ネットワークの名前をクリックします。詳細ビューが開きます。
3. **vNIC Profiles** タブをクリックします。
4. **New** または **Edit** をクリックします。
5. プロファイルの **Name** および **Description** を入力します。
6. **QoS** リストから該当する Quality of Service ポリシーを選択します。
7. ドロップダウンリストから **Network Filter** を選択して、仮想マシンとの間のネットワークパケットのトラフィックを管理します。ネットワークフィルターの詳細は、[Red Hat Enterprise Linux Virtualization のデプロイメントおよび管理ガイド](#) の [ネットワークフィルターの適用](#) を参照してください。
8. vNIC のパススルーを有効にして、仮想機能のデバイスを直接割り当てるようには、**Passthrough** 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なると、QoS、ネットワークフィルタリング、ポートミラーリングに互換性がないため、これらが無効になります。パススルーの詳細は、[vNIC プロファイルでのパススルーの有効化](#) を参照してください。

9. **Passthrough**を選択した場合には、オプションで**Migratable**チェックボックスの選択を解除すると、このプロファイルを使用するvNICの移行が無効になります。このチェックボックスを選択したままにする場合は、[仮想マシン管理ガイドの SR-IOV が有効な vNICs を使用する仮想マシンの追加の前提条件](#)を参照してください。
10. **Port Mirroring**と**Allow all users to use this Profile**のチェックボックスを使って、これらのオプションを切り替えます。
11. カスタムプロパティーリストからカスタムプロパティーを選択すると、デフォルトで **Please select a key...** と表示されます。+ および - ボタンを使用して、カスタムプロパティーを追加または削除します。
12. **OK**をクリックします。

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

#### 2.4.2.3. VM Interface Profile ウィンドウの設定内容の説明

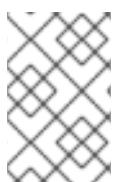
表2.19 VM Interface Profile ウィンドウ

| フィールド名         | 説明                                                                                                                     |
|----------------|------------------------------------------------------------------------------------------------------------------------|
| <b>Network</b> | vNIC プロファイルの適用先の利用可能なネットワークのドロップダウンリスト。                                                                                |
| <b>Name</b>    | vNIC プロファイルの名前。1から 50 文字までの大文字と小文字、数字、ハイフン、およびアンダースコアの組み合わせが含まれる一意の名前である必要があります。                                       |
| <b>説明</b>      | vNIC プロファイルの説明。このフィールドは推奨されますが、必須ではありません。                                                                              |
| <b>QoS</b>     | vNIC プロファイルに適用する、利用可能な Network Quality of Service ポリシーのドロップダウンリスト。QoS ポリシーは、vNIC のインバウンドおよびアウトバウンドのネットワークトラフィックを規制します。 |

| フィールド名         | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Filter | <p>vNIC プロファイルに適用するネットワークフィルターのドロップダウンリスト。ネットワークフィルターは、仮想マシンとの間で送信可能なパケットの種類をフィルタリングして、ネットワークセキュリティーを向上させます。デフォルトのフィルターは <b>vdsm-no-mac-spoofing</b> で、<b>no-mac-spoofing</b> と <b>no-arp-mac-spoofing</b> を組み合わせたもので、libvirt が提供するネットワークフィルターの詳細は、Red Hat Enterprise Linux Virtualization のデプロイメントおよび管理ガイドの <a href="#">既存のネットワークフィルター</a> セクションを参照してください。</p> <p>仮想マシンの VLAN やボンドには、<b>&lt;No Network Filter&gt;</b> を使用してください。信頼できる仮想マシンでネットワークフィルターを使用しない場合、パフォーマンスが向上します。</p>  <p><b>注記</b></p> <p>Red Hat では、<b>engine-config</b> ツールを使用して <b>EnableMACAntiSpoofingFilterRules</b> パラメーターを <b>false</b> に設定することでフィルターを無効化する方法をサポートしなくなりました。代わりに <b>&lt;No Network Filter&gt;</b> オプションを使用してください。</p> |
| Passthrough    | <p>パススルーのプロパティを切り替えるためのチェックボックス。パススルーでは、vNIC がホスト NIC の仮想機能に直接接続できるようになります。vNIC プロファイルが仮想マシンにアタッチされている場合、パススルーのプロパティは編集できません。</p> <p>パススルーを有効にすると、vNIC プロファイルでの QoS、ネットワークフィルター、ポートミラーリングが無効になります。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Migratable     | <p>このプロファイルを使用する vNIC が移行可能かどうかを切り替えるチェックボックスです。移行は、通常の vNIC プロファイルではデフォルトで有効になっています。その場合はチェックボックスが選択されており、変更できません。<b>Passthrough</b> チェックボックスが選択されていると <b>Migratable</b> が有効になり、必要に応じて選択を解除して、パススルー vNIC の移行を無効にできます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| フィールド名                              | 説明                                                                                                                                                                      |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Failover                            | フェイルオーバーデバイスとして機能する、利用可能な vNIC プロファイルを選択するためのドロップダウンメニューです。Passthrough と Migratable のチェックボックスがチェックされている場合のみ有効です。                                                        |
| Port Mirroring                      | ポートミラーリングを切り替えるためのチェックボックスです。ポートミラーリングは、論理ネットワーク上のレイヤー 3 のネットワークトラフィックを、仮想マシン上の仮想インターフェイスにコピーします。デフォルトでは選択されていません。詳細は、テクニカルリファレンスの <a href="#">ポートミラーリング</a> を参照してください。 |
| Device Custom Properties            | vNIC プロファイルに適用する利用可能なカスタムプロパティーを選択するためのドロップダウンメニューです。+ と - ボタンを使用してプロパティーをそれぞれ追加、削除します。                                                                                 |
| Allow all users to use this Profile | 環境内の全ユーザーがプロファイルを利用できるかどうかを切り替えるためのチェックボックスです。これはデフォルトで選択されます。                                                                                                          |

#### 2.4.2.4. vNIC プロファイルでのパススルーの有効化



##### 注記

これは、Red Hat Virtualization で SR-IOV を準備およびセットアップする方法を示す一連のトピックの1つです。詳細は、[SR-IOV のセットアップと設定](#) を参照してください。

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

vNIC プロファイルがすでに vNIC にアタッチされている場合、パススループロパティーは有效地できません。この手順では、これを避けるために新しいプロファイルを作成します。vNIC プロファイルでパススルーが有効になっている場合、QoS、ネットワークフィルター、およびポートミラーリングを同じプロファイルで有効にすることはできません。

SR-IOV、デバイスの直接割り当て、および Red Hat Virtualization へのこれらの実装に関するハードウェアの考慮事項は、[SR-IOV を実装するためのハードウェアの考慮事項](#) を参照してください。

##### 手順

1. Network → Networks をクリックします。
2. 論理ネットワークの名前をクリックします。詳細ビューが開きます。

3. vNIC Profiles タブをクリックすると、その論理ネットワークのすべての vNIC プロファイルが一覧表示されます。
4. New をクリックします。
5. プロファイルの Name および Description を入力します。
6. Passthrough チェックボックスを選択します。
7. オプション: このプロファイルを使用する vNIC の移行を無効にするには、Migratable チェックボックスの選択を解除します。このチェックボックスを選択したままにする場合は、仮想マシン管理ガイドの SR-IOV が有効な vNICs を使用する仮想マシンの追加の前提条件 を参照してください。
8. 必要に応じて、Please select a key... とデフォルトで表示されるカスタムプロパティーリストからカスタムプロパティーを選択します。+ および - ボタンを使用して、カスタムプロパティーを追加または削除します。
9. OK をクリックします。

vNIC プロファイルがパススルーに対応するようになりました。このプロファイルを使用して仮想マシンを NIC または PCI VF に直接アタッチするには、論理ネットワークを NIC にアタッチして、パススルー vNIC プロファイルを仮想マシン上に新しい PCI PassthroughvNIC を作成します。これらの手順の詳細は、仮想マシン管理ガイドの ホストネットワークインターフェイスの編集とホストへの論理ネットワークの割り当て および 新しいネットワークインターフェイスの追加 を参照してください。

#### 2.4.2.5. フェイルオーバーを伴う SR-IOV 移行用 vNIC プロファイルの有効化

フェイルオーバーでは、仮想マシンの移行時に VF のデタッチが必要になると、フェイルオーバーデバイスとして機能するプロファイルを選択できるため、中断を最小限に抑えて仮想マシンの通信を維持できます。



#### 注記

フェイルオーバーはテクノロジープレビュー機能としてのみ提供されます。テクノロジープレビュー機能は、Red Hat の実稼働環境のサービスレベルアグリーメント (SLA) ではサポートされず、機能的に完全ではないことがあるため、Red Hat では実稼働環境での使用を推奨していません。テクノロジープレビュー機能では、最新の製品機能をいち早く提供します。これにより、お客様は開発段階で機能をテストし、フィードバックを提供できます。詳細は、テクノロジープレビュー機能のサポート範囲 を参照してください。

#### 前提条件

- プロファイルの Passthrough と Migratable のチェックボックスが選択されている。
- フェイルオーバーネットワークがホストに接続されている。
- まずフェイルオーバーの参照を削除することで、フェイルオーバーとして機能する vNIC プロファイルの編集が可能になっている。
- フェイルオーバーとして機能する vNIC プロファイルは、パススルーとして選択されていないか、外部ネットワークに接続されていないプロファイルである。

#### 手順

1. 管理ポータルで Network → vNIC profiles に移動して vNIC プロファイルを選択し、Edit をクリックして、ドロップダウンリストから Failover vNIC profile を選択します。
2. OK をクリックすると、プロファイルの設定が保存されます。



#### 注記

同じフェイルオーバー vNIC プロファイルを参照する 2 つの vNIC プロファイルを同じ仮想マシンにアタッチすると、libvirt で失敗します。

#### 2.4.2.6. vNIC プロファイルの削除

vNIC プロファイルを削除すると、仮想化環境からも削除されます。

#### 手順

1. Network → Networks をクリックします。
2. 論理ネットワークの名前をクリックします。詳細ビューが開きます。
3. vNIC Profiles タブをクリックすると、利用可能な vNIC プロファイルが表示されます。
4. 1つまたは複数のプロファイルを選択し、Remove をクリックします。
5. OK をクリックします。

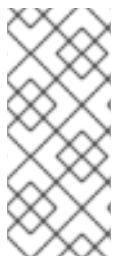
#### 2.4.2.7. vNIC プロファイルへのセキュリティーグループの割り当て



#### 注記

この機能は、ovirt-provider-ovn が外部ネットワークプロバイダーとして追加された場合にのみ使用できます。セキュリティーグループは Red Hat Virtualization Manager で作成できません。ovirt-provider-ovn で OpenStack Networking を使用してセキュリティーグループを作成する必要があります。詳細は、Red Hat OpenStack Platform ユーザおよびアイデンティティ管理ガイドの [プロジェクトのセキュリティ管理](#) を参照してください。

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



#### 注記

セキュリティーグループは、Open Virtual Network (OVN) 外部ネットワークプロバイダーに登録されているセキュリティーグループの ID で識別されます。OpenStack Networking API を使用して、特定テナントのセキュリティーグループの ID を把握することができます。OpenStack API リファレンスの [セキュリティーグループリスト](#) を参照してください。

#### 手順

1. Network → Networks をクリックします。

2. 論理ネットワークの名前をクリックします。詳細ビューが開きます。
3. vNIC Profiles タブをクリックします。
4. New をクリックするか、既存の vNIC プロファイルを選択して Edit をクリックします。
5. カスタムプロパティーのドロップダウンリストから、SecurityGroups を選択します。カスタムプロパティーのドロップダウンを空白のままにすると、デフォルトのセキュリティ設定が適用され、すべてのアウトバウンドトラフィックとの相互通信が許可されますが、デフォルトのセキュリティーグループ外からのインバウンドトラフィックはすべて拒否されます。後で SecurityGroups プロパティーを削除しても、適用されたセキュリティーグループには影響しません。
6. テキストフィールドに、vNIC プロファイルにアタッチするセキュリティーグループの ID を入力します。
7. OK をクリックします。

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

#### 2.4.2.8. vNIC プロファイルのユーザーパーミッション

ユーザーパーミッションを設定して、特定の vNIC プロファイルにユーザーを割り当てます。VnicProfileUser ロールをユーザーに割り当ててプロファイルの使用を可能にします。特定のプロファイルに対するパーミッションを削除して、ユーザーを制限できます。

##### vNIC プロファイルのユーザーパーミッション

1. Network → vNIC Profile をクリックします。
2. vNIC プロファイル名をクリックします。詳細ビューが開きます。
3. Permissions タブをクリックすると、そのプロファイルの現在のユーザーパーミッションが表示されます。
4. Add または Remove をクリックして、vNIC プロファイルのユーザーパーミッションを変更します。
5. Add Permissions to User ウィンドウで My Groups をクリックすると、ユーザーグループが表示されます。このオプションを使用して、グループ内の他のユーザーにパーミッションを付与できます。

vNIC プロファイルのユーザーパーミッションを設定しました。

#### 2.4.3. 外部プロバイダーネットワーク

##### 2.4.3.1. 外部プロバイダーからのネットワークのインポート

Open Virtual Network (OVN) のネットワークを利用するには、プロバイダーをマネージャーに登録する必要があります。詳細は、[外部ネットワークプロバイダーの追加](#) を参照してください。その後、以下の手順でプロバイダーが提供するネットワークを Manager にインポートし、仮想マシンがネットワークを使用できるようにします。

## 手順

1. Network → Networks をクリックします。
2. Import をクリックします。
3. Network Provider ドロップダウンリストから、外部のプロバイダーを選択します。そのプロバイダーが提供しているネットワークが自動的に検出され、Provider Networks リストに表示されます。
4. チェックボックスを使って、Provider Networks リストでインポートするネットワークを選択し、下矢印をクリックしてそのネットワークを Networks to Import リストに移動させます。
5. インポートするネットワークの名前をカスタマイズすることができます。名前をカスタマイズするには、Name 列でネットワークの名前をクリックして、テキストを変更します。
6. Data Center ドロップダウンリストから、ネットワーク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: 対象のネットワークをすべてのユーザーが利用できるようにするには、Allow All チェックボックスをオフにします。
8. Import をクリックします。

選択されたネットワークがターゲットデータセンターにインポートされ、仮想マシンにアタッチできるようになります。詳細は、仮想マシン管理ガイドの [新しいネットワークインターフェイスの追加](#) を参照してください。

### 2.4.3.2. 外部プロバイダーネットワークの使用に関する制限

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

- 外部プロバイダーが提供する論理ネットワークは、仮想マシンのネットワークとして使用する必要があり、ディスプレイネットワークとして使用できません。
- 同一の論理ネットワークを複数回インポートできますが、同じデータセンターにはインポートできません。
- 外部プロバイダーが提供する論理ネットワークを Manager で編集できません。外部プロバイダーが提供する論理ネットワークの詳細を編集するには、対象の論理ネットワークを提供している外部のプロバイダーから直接編集する必要があります。
- 外部プロバイダーが提供する論理ネットワークに接続された仮想ネットワークインターフェイスカードでは、ポートミラーリングは利用できません。
- 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、その論理ネットワークが仮想マシンで使用されている間は、そのプロバイダーを Manager から削除できません。
- 外部プロバイダーが提供するネットワークは必須ではありません。そのため、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、ホスト選択時にこれらの論理ネットワークは考慮されません。ユーザーは、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で、論理ネットワークの可用性を確保する必要があります。

### 2.4.3.3. 外部プロバイダーの論理ネットワークでのサブネット設定

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

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

外部ネットワークプロバイダーとして Open Virtual Network (OVN) (ovirt-provider-ovn) を追加すると、複数のサブネットをルーターで接続できます。これらのルーターを管理するには、[OpenStack Networking API v2.0](#) を使用できます。ただし、ovirt-provider-ovn には制限がありますのでご注意ください。ソース NAT (OpenStack API の enable\_snat) は実装されていません。

#### 2.4.3.4. 外部プロバイダー論理ネットワークへのサブネットの追加

外部プロバイダーが提供する論理ネットワーク上に、サブネットを作成します。

##### 手順

1. Network → Networks をクリックします。
2. 論理ネットワークの名前をクリックします。詳細ビューが開きます。
3. Subnets タブをクリックします。
4. New をクリックします。
5. 新しいサブネットの Name と CIDR を入力します。
6. IP Version ドロップダウンリストから、IPv4 または IPv6 のいずれかを選択します。
7. OK をクリックします。



##### 注記

IPv6 の場合、Red Hat Virtualization でサポートされるのは静的アドレスのみです。

#### 2.4.3.5. 外部プロバイダー論理ネットワークからのサブネットの削除

外部プロバイダーが提供する論理ネットワークからサブネットを削除します。

##### 手順

1. Network → Networks をクリックします。
2. 論理ネットワークの名前をクリックします。詳細ビューが開きます。
3. Subnets タブをクリックします。
4. サブネットを選択し、Remove をクリックします。
5. OK をクリックします。

### 2.4.3.6. 論理ネットワークとポート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、Open Virtual Network (OVN) を外部ネットワークプロバイダー (`ovirt-provider-ovn`) として追加した場合にのみ使用できます。セキュリティーグループは Red Hat Virtualization Manager で作成できません。セキュリティーグループの作成は、OpenStack Networking API v2.0 または Ansible で行う必要があります。

セキュリティーグループとは、厳密に適用されるルールの集合体であり、ネットワーク上のインバウンドおよびアウトバウンドのトラフィックをフィルタリングすることができます。また、セキュリティーグループを使って、ポートレベルでトラフィックをフィルタリングすることもできます。

Red Hat Virtualization 4.2.7 では、セキュリティーグループはデフォルトで無効になっています。

#### 手順

1. Compute → Clusters をクリックします。
2. クラスターの名前をクリックします。詳細ビューが開きます。
3. Logical Networks タブをクリックします。
4. Add Network をクリックしてプロパティーを定義し、External Providers ドロップダウンリストから `ovirt-provider-ovn` が選択されていることを確認します。詳細は、データセンターまたはクラスターでの新しい論理ネットワークの作成 を参照してください。
5. Security Group ドロップダウンリストから Enabled を選択します。詳細は、論理ネットワークの一般設定の説明 を参照してください。
6. OK をクリックします。
7. OpenStack Networking API v2.0 または Ansible を使用して、セキュリティーグループを作成します。
8. OpenStack Networking API v2.0 または Ansible を使用して、セキュリティーグループのルールを作成します。
9. OpenStack Networking API v2.0 または Ansible を使用して定義したセキュリティーグループでポートを更新します。
10. オプションセキュリティ機能をポートレベルで有効にするかどうかを定義します。現在のところ、これは OpenStack Networking API でのみ可能です。`port_security_enabled` 属性が設定されていない場合は、所属するネットワークで指定された値がデフォルトとなります。

### 2.4.4. ホストとネットワーキング

#### 2.4.4.1. Network Manager Stateful Configuration (nmstate)

Red Hat Virtualization (RHV) のバージョン 4.4 は、Network Manager Stateful Configuration (`nmstate`) を使用して RHEL 8 ベースの RHV ホストのネットワークを設定します。RHV バージョン 4.3 以前のバージョンでは、ホストのネットワーク管理にインターフェイス設定 (`ifcfg`) のネットワークスクリプトを使用しています。

`nmstate` を使用するには、[RHV アップグレードガイド](#) に記載されている方法で Red Hat Virtualization Manager とホストをアップグレードします。

管理者は、`nmstate` のインストールや設定を行う必要はありません。デフォルトで有効になっており、バックグラウンドで動作します。



### 重要

クラスター内のホストのネットワーク設定を変更するには、必ず RHV Manager を使用します。使用しない場合は、サポート対象外の設定が作成される可能性があります。

`nmstate` への変更はほぼ透過的に行われます。以下のように、ホストネットワークの設定方法のみ変更されます。

- クラスターにホストを追加した後は、必ず RHV Manager を使用してホストのネットワークを変更してください。
- Manager を使用せずにホストネットワークを変更すると、サポートされていない設定になってしまることがあります。
- サポートされていない設定を修正するには、Manager を使用してホストネットワークを同期させ、サポート対象の設定に置き換えます。詳細は、[ホストネットワークの同期](#) を参照してください。
- Manager の外部でホストネットワークを変更するのは、ホストで静的ルートを設定する場合のみです。詳細は、[ホストへの静的ルートの追加](#) を参照してください。

`nmstate` を変更することで、ホストを Manager に追加する前に Cockpit および Anaconda で行った設定変更を RHV Manager が適用する方法が改善されます。これにより、[BZ#1680970 Static IPv6 Address is lost on host deploy if NM manages the interface](#) などの問題が修正されました。



### 重要

`dnf` または `yum` を使用して `nmstate` パッケージを手動で更新した場合は、ホスト上の `vdsmd` および `supervdsmd` を再起動してください。以下に例を示します。

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



### 重要

`dnf` または `yum` を使用して Network Manager パッケージを手動で更新した場合は、ホスト上で `NetworkManager` を再起動します。以下に例を示します。

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

#### 2.4.4.2. ホスト機能のリフレッシュ

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

### 手順

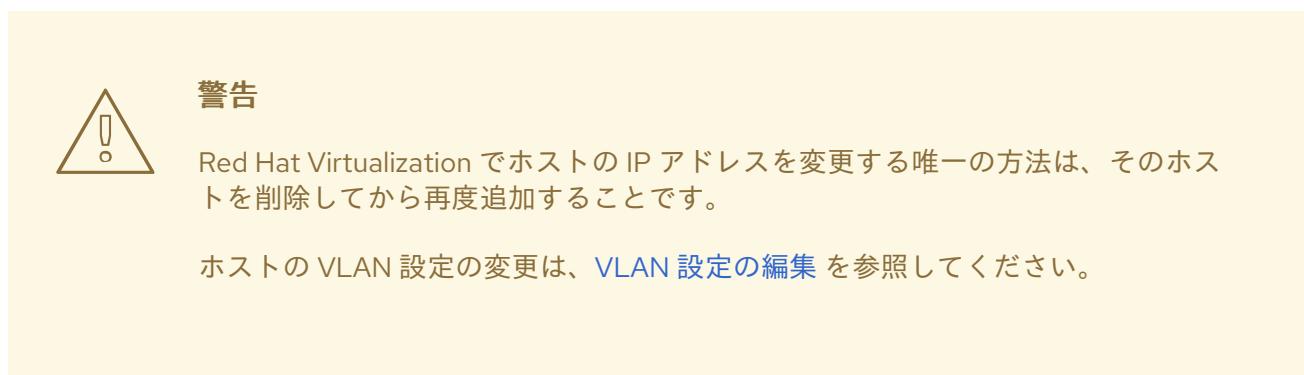
1. Compute → Hosts をクリックし、ホストを選択します。

2. Management → Refresh Capabilities をクリックします。

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

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

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



#### 重要

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



#### 注記

スイッチが LLDP (Link Layer Discovery Protocol) 情報を提供するように設定されている場合は、物理ネットワークインターフェイスにカーソルを合わせると、そのスイッチポートの現在の設定が表示されます。これにより、誤った設定を防ぐことができます。論理ネットワークを割り当てる前に、以下の情報を確認してください。

- Port Description (TLV type 4) と System Name (TLV type 5) は、ホストのどのポート、そしてどのスイッチにパッチが当てられているかを検出するのに役立ちます。
- Port VLAN ID は、タグなしイーサネットフレーム用にスイッチポートに設定されたネイティブ VLAN ID を表示します。スイッチポートに設定されているすべての VLAN が、VLAN Name と VLAN ID の組み合わせで表示されます。

#### 手順

1. Compute → Hosts をクリックします。
2. ホストの名前をクリックします。詳細ビューが開きます。
3. Network Interfaces タブをクリックします。

4. **Setup Host Networks** をクリックします。
5. 必要に応じて、ホストネットワークインターフェイスにカーソルを合わせ、スイッチが提供する設定情報を表示します。
6. 論理ネットワークを選択して、物理ホストネットワークインターフェイスの横にある**Assigned Logical Networks** 領域にドラッグして、論理ネットワークを物理ホストネットワークインターフェイスにアタッチします。



### 注記

1つの NIC が複数の論理ネットワークに接続されている場合には、そのうちの1つのネットワークのみを VLAN 以外にすることができます。他のすべての論理ネットワークは、一意の VLAN でなければなりません。

## 7. 論理ネットワークの設定

- a. 割り当てられた論理ネットワークにカーソルを合わせ、鉛筆アイコンをクリックします。これにより、**Edit Management Network** ウィンドウが開きます。
- b. IPv4 タブの **Boot Protocol** で **None**、**DHCP** または **Static** を選択します。**Static** を選択した場合は、**IP**、**Netmask/Routing Prefix**、**Gateway** を入力します。



### 注記

IPv6 は、静的 IPv6 アドレスにのみ対応しています。論理ネットワークを設定するには、**IPv6** タブを選択し、次のように入力します。

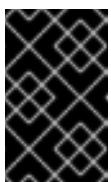
- **Boot Protocol** を **Static** に設定します。
- **Routing Prefix** には、スラッシュと小数点を使って、接頭辞の **長さ** を入力します。例: **/48**
- **IP:** ホストのネットワークインターフェイスの完全な IPv6 アドレス。例: **2001:db8::1:0:0:6**
- **Gateway:** 送信元ルーターの IPv6 アドレス。例: **2001:db8::1:0:0:1**



### 注記

ホストの管理ネットワークの IP アドレスを変更した場合には、新しい IP アドレスの設定に、[ホストを再インストール](#) する必要があります。

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



### 重要

クラスター内のすべてのホストが、管理ネットワークに同じ IP スタック (IPv4 または IPv6 のみ) を使用するように設定します。デュアルスタックには対応していません。

- c. QoS タブでは、デフォルトのホストネットワークのサービス品質を上書きします。Override QoS を選択し、以下のフィールドに必要な値を入力します。
- **Weight Share:** 同じ論理リンクにアタッチされた他のネットワークと比較して、特定のネットワークに割り当てる必要がある論理リンクの容量を指定します。正確な共有は、そのリンクの全ネットワークの共有の合計によって異なります。デフォルトでは、この値は 1-100 の範囲の数字になります。
  - **Rate Limit [Mbps]:** ネットワークによって使用される最大帯域幅。
  - **Committed Rate [Mbps]:** ネットワークに必要な最小帯域幅。要求される Committed Rate は保証されず、ネットワークインフラストラクチャーおよび同じ論理リンクの他のネットワークによって要求される Committed Rate によって異なります。
- d. ネットワークブリッジを設定するには、Custom Properties タブをクリックし、ドロップダウンリストから **bridge\_opts** を選択します。有効なキーと値を次の構文で入力してください: **key=value** 複数の項目を空白文字で区切ります。以下のキーが有効で、値は例として示されています。これらのパラメーターの詳細は、[bridge\\_opts パラメーターの説明](#) を参照してください。

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

- e. イーサネットのプロパティーを設定するには、Custom Properties タブをクリックし、ドロップダウンリストから **ethtool\_opts** を選択します。ethtool のコマンドライン引数の形式で、有効な値を入力してください。たとえば、以下のようになります。

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

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

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

**ethtool\_opts** オプションはデフォルトでは使用できないので、エンジン設定ツールで追加する必要があります。詳細は [Ethtool を使用するための Manager の設定方法](#) を参照してください。ethtool プロパティーの詳細は、コマンドラインで **man ethtool** と入力し、man ページを参照してください。

- f. Fibre Channel over Ethernet (FCoE) を設定するには、Custom Properties タブをクリックし、ドロップダウンリストから **fcoe** を選択します。有効なキーと値を次の構文で入力してください: **key=value**少なくとも **enable=yes** が必要です。**dcb = [yes|no]** および **`auto\_vlan= [yes|no]** を追加することもできます。複数の項目を空白文字で区切れます。**fcoe** オプションはデフォルトでは利用できないので、エンジン設定ツールを使って追加する必要があります。詳細は、[FCoE を使用するための Manager の設定方法](#) を参照してください。



#### 注記

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

- g. ホストが使用するデフォルトネットワークを管理ネットワーク (ovirtmgmt) から非管理ネットワークに変更するには、非管理ネットワークのデフォルトルートを設定します。詳細は、[デフォルトルートの設定](#) を参照してください。
- h. 論理ネットワークの定義がホストのネットワーク設定と同期していない場合は、**Sync network** チェックボックスを選択します。同期されていないホストとそれらを同期する方法の詳細は、[ホストネットワークの同期](#) を参照してください。
8. **Verify connectivity between Host and Engine** チェックボックスを選択し、ネットワークの接続性を確認します。このアクションは、ホストがメンテナンスモードの場合にのみ機能します。
9. **OK** をクリックします。



#### 注記

ホストのすべてのネットワークインターフェイスカードが表示されていない場合は、**Management → Refresh Capabilities** をクリックして、そのホストで利用可能なネットワークインターフェイスカードのリストを更新します。

### トラブルシューティング

場合によっては、**Setup Host Networks** ウィンドウまたは **setupNetwork** コマンドを使用してホストネットワーク設定を複数同時に変更すると、イベントログで **Operation failed: [Cannot setup Networks].Another Setup Networks or Host Refresh process in progress on the host. Please try later.]** のエラーが発生して失敗することがあります。このエラーは、変更内容の一部がホストで設定されていないことを示しています。これは、設定の状態を維持するために、ネットワークの設定コマンドは一度に1つしか処理できないためです。他の同時進行の設定コマンドは、最大 20 秒 (デフォルトのタイムアウト)、待ちキューに入ります。上記の失敗を防ぐために、**engine-config** コマンドを使用して、**SetupNetworksWaitTimeoutSeconds** のタイムアウト時間を 20 秒より長くしてください。以下に例を示します。

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

### 関連情報

- [engine-config コマンドの構文](#)
- [setupnetworks POST](#)

#### 2.4.4.4. ホストネットワークの同期

ホスト上のインターフェイスの定義が Manager が記憶している定義と異なる場合は、Manager はネットワークインターフェイスを **out-of-sync** と定義します。

同期していないネットワークは、ホストの Network Interfaces タブの Out-of-sync アイコン (  ) と、Setup Host Networks ウィンドウのこのアイコン  とともに表示されます。

ホストのネットワークが同期していない場合、Setup Host Networks ウィンドウで同期していないネットワークに対して実行できるアクティビティーは、ネットワークインターフェイスからの論理ネットワークの切り離しが、ネットワークの同期のみです。

## ホストが同期しなくなる仕組み

次のような場合には、ホストは非同期の状態になります。

- Edit Logical Networks ウィンドウなどを使わずに、ホスト上で設定を変更した場合。
  - 物理ホスト上の VLAN 識別子を変更した場合。
  - 物理ホストの Custom MTU を変更した場合。
- ネットワーク名は同じだが、値やパラメーターが異なる別のデータセンターにホストを移動した場合。
- ホストから手動でブリッジを削除してネットワークの VM Network プロパティーを変更した場合。



### 重要

ネットワークの MTU 設定を変更する場合は、この変更をネットワーク上で実行中の仮想マシンに伝達する必要があります。それには、MTU 設定を適用する必要があるすべての仮想マシンの vNIC をホットアンプラグ/再プラグするか、仮想マシンを再起動します。そうしないと、仮想マシンが別のホストに移行すると、これらのインターフェイスが失敗します。詳細は、[After network MTU change, some VMs and bridges have the old MTU and seeing packet drops](#) と [BZ#1766414](#) を参照してください。

## ホストの非同期化の回避

以下のベストプラクティスに従うことで、ホストの非同期化を回避できます。

1. ホストのローカルで変更するのではなく、管理ポータルで変更します。
2. [Editing VLAN Settings](#) の手順に従って VLAN 設定を編集します。

## ホストの同期

ホストのネットワークインターフェイスの定義を同期させるには、Manager からの定義を使用してホストに適用します。これらの定義が必要でない場合は、同期後に管理ポータルからホストの定義を更新してください。ホストのネットワークを 3 つのレベルで同期させることができます。

- 論理ネットワーク別
- ホスト別
- クラスター別

## 論理ネットワークレベルでのホストネットワークの同期

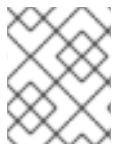
1. Compute → Hosts をクリックします。
2. ホストの名前をクリックします。詳細ビューが開きます。
3. Network Interfaces タブをクリックします。
4. Setup Host Networks をクリックします。
5. 同期していないネットワークにカーソルを置き、鉛筆アイコンをクリックします。Edit Network ウィンドウが開きます。
6. Sync network チェックボックスを選択します。
7. OK をクリックすると、ネットワークの変更が保存されます。
8. OK をクリックして Setup Host Networks ウィンドウを閉じます。

#### ホストレベルでのホストネットワークの同期

- ホストの Network Interfaces タブにある Sync All Networks ボタンをクリックすると、ホストで同期していないネットワークインターフェイスがすべて同期されます。

#### クラスターレベルでのホストネットワークの同期

- クラスターの Logical Networks タブの Sync All Networks ボタンをクリックして、クラスター全体の同期されていない論理ネットワーク定義をすべて同期します。



#### 注記

REST API 経由でホストのネットワークを同期することもできます。REST API ガイドの [syncallnetworks](#) を参照してください。

#### 2.4.4.5. ホストの VLAN 設定の編集

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

ネットワークを同期させるためには、以下を実行します。

1. ホストをメンテナンスモードにします。
2. 管理ネットワークを手動でホストから外します。これにより、ホストは新しい VLAN 上で到達可能になります。
3. ホストをクラスターに追加します。管理ネットワークに直接接続されていない仮想マシンは、ホスト間で安全に移行できます。

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

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

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



## 重要

管理ネットワークの VLAN ID を変更した場合は、[ホストを再インストール](#)して新しい VLAN ID を適用する必要があります。

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

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



## 重要

複数の論理ネットワークを作成している場合、すべての論理ネットワークで **New Logical Network** または **Edit Logical Network** ウィンドウの **Enable VLAN tagging** チェックボックスをチェックしておく必要があります。

## 手順

1. **Compute** → **Hosts** をクリックします。
2. ホストの名前をクリックします。詳細ビューが開きます。
3. **Network Interfaces** タブをクリックします。
4. **Setup Host Networks** をクリックします。
5. VLAN タグ付きの論理ネットワークを、物理ネットワークインターフェイスの横にある **Assigned Logical Networks** エリアにドラッグします。物理ネットワークインターフェイスには、VLAN タグがあるため、複数の論理ネットワークを割り当てることができます。
6. 論理ネットワークを設定します。
  - a. 割り当てられた論理ネットワークにカーソルを合わせ、鉛筆アイコンをクリックします。
  - b. 論理ネットワークの定義がホストのネットワーク設定と同期していない場合は、**Sync network** チェックボックスを選択します。
  - c. **Boot Protocol** を選択します。
    - **None**
    - **DHCP**
    - **Static**
  - d. **IP** と **Subnet Mask** を入力します。
  - e. **OK** をクリックします。
7. **Verify connectivity between Host and Engine** チェックボックスを選択すると、ネットワークチェックが実行されますが、これはホストがメンテナンスモードの場合にのみ機能します。
8. **OK** をクリックします。

クラスター内の各ホストの NIC を編集して、論理ネットワークをクラスター内の各ホストに追加します。これが完了すると、ネットワークの運用が開始されます。

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

#### 2.4.4.6.1. ホストネットワークのコピー

時間を節約するために、ソースホストのネットワーク設定を同じクラスター内のターゲットホストにコピーできます。

ネットワーク設定のコピーには以下が含まれます。

- ホストに接続された論理ネットワーク (**ovirtmgmt** 管理ネットワークを除く)
- インターフェイスに割り当てられたボンディング

#### 制限

- 静的 IP アドレスを含むネットワーク設定はコピーしないでください。コピーすると、ターゲットホストのブートプロトコルが **none** に設定されます。
- コピー元のホストと同じインターフェイス名で、物理ネットワーク接続が異なるターゲットホストに設定をコピーすると、誤った設定になります。
- ターゲットホストには、ソースホストと同等以上の数のインターフェイスが必要です。そうでない場合、操作は失敗します。
- **QoS**、**DNS**、**custom\_properties** のコピーはサポートされていません。
- ネットワークインターフェイスのラベルはコピーされません。



#### 警告

ホストのネットワークをコピーすると、対象となるホストのネットワーク設定が、**ovirtmgmt** 管理ネットワークへの接続以外、すべて置き換えられます。

#### 前提条件

- ターゲットホストの NIC 数は、ソースホストの NIC 数と同等以上である。そうでない場合、操作は失敗します。
- ホストは同じクラスター内にある。

#### 手順

1. 管理ポータルで **Compute → Hosts** をクリックします。
2. 設定をコピーするホストを選択します。
3. **Copy Host Networks** をクリックします。**Copy Host Networks** ウィンドウが表示されます。

4. Target Host を使用して、設定を受信するホストを選択します。このリストには、同じクラス ター内にあるホストのみが表示されます。
5. **Copy Host Networks** をクリックします。
6. ターゲットホストのネットワーク設定を確認します。

## ヒント

- 複数のホストを選択すると、**Copy Host Networks** ボタンとコンテキストメニューが無効になります。
- **Copy Host Networks** ボタンを使用する代わりに、ホストを右クリックし、コンテキストメニューから **Copy Host Networks** を選択できます。
- **Copy Host Networks** ボタンは、すべてのホストの詳細表示でも利用できます。

### 2.4.4.7. ホストネットワークへの追加の IPv4 アドレスの割り当て

**ovirtmgmt** 管理ネットワークなどのホストネットワークは、最初にセットアップされたときに1つのIPアドレスのみで作成されます。つまり、NICの設定ファイルに複数のIPアドレスが設定されている場合、最初にリストアップされたIPアドレスのみがホストネットワークに割り当てられることになります。ストレージに接続する場合や、同じNICを使って別のプライベートサブネット上のサーバーに接続する場合は、追加のIPアドレスが必要になることがあります。

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

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

## 手順

1. 追加のIPv4アドレスを設定したいホストに、VDSMのフックパッケージをインストールします。パッケージは、Red Hat Enterprise LinuxホストおよびRed Hat Virtualization Hostに手動でインストールする必要があります。

```
dnf install vdsm-hook-extra-ipv4-addrs
```

2. Managerで以下のコマンドを実行してキーを追加します。

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

3. **ovirt-engine** サービスを再起動します。

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

4. 管理ポータルで **Compute → Hosts** をクリックします。

5. ホストの名前をクリックします。詳細ビューが開きます。

6. **Network Interfaces** タブをクリックし、**Setup Host Networks** をクリックします。

7. 割り当てられた論理ネットワークの上にカーソルを置き、鉛筆アイコンをクリックして、ホストネットワークインターフェイスを編集します。

8. **Custom Properties** のドロップダウンリストから **ipv4\_addr** を選択し、IP アドレスと接頭辞を追加します (5.5.5.5/24 など)。複数の IP アドレスはコンマで区切る必要があります。
9. **OK** をクリックして、**Edit Network** ウィンドウを閉じます。
10. **OK** をクリックして **Setup Host Networks** ウィンドウを閉じます。

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

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

ネットワークラベルを使用すると、ホストネットワークインターフェイスへの論理ネットワークの割り当てに関連する管理ワークフローを大幅に簡素化できます。ロールネットワーク (たとえば、移行ネットワークやディスプレイネットワーク) にラベルを設定すると、そのネットワークがすべてのホストに大量に展開されます。このようなネットワークの大量追加は、DHCP を使って実現しています。多くの静的 IP アドレスを入力するタスクのスケーラブルでない性質のため、この大量展開の方法は、静的アドレスを入力する方法よりも選択されました。

ホストネットワークインターフェイスにラベルを追加するには 2 つの方法があります。

- 管理ポータルで手動で実行する
- LLDP Labeler サービスで自動で実行する

#### 手順

1. **Compute** → **Hosts** をクリックします。
2. ホストの名前をクリックします。詳細ビューが開きます。
3. **Network Interfaces** タブをクリックします。
4. **Setup Host Networks** をクリックします。
5. **Labels** をクリックし、**[New Label]** を右クリックします。ラベルを追加する物理ネットワークインターフェイスを選択します。
6. **Label** テキストフィールドに、ネットワークラベルの名前を入力します。
7. **OK** をクリックします。

#### 手順

LLDP Labeler サービスを使用すると、設定済みのクラスターリスト内のホストネットワークインターフェイスにラベルを割り当てるプロセスを自動化できます。

#### 2.4.4.8.1. LLDP ラベルセレクターの設定

デフォルトでは、LLDP Labeler は 1 時間ごとのサービスとして動作します。このオプションは、ハードウェアを変更する場合 (NIC、スイッチ、ケーブルなど)、またはスイッチ設定を変更する場合に役立ちます。

#### 前提条件

- インターフェイスは、ジュニパー製スイッチに接続されている。

- ジュニパーのスイッチは、LLDP を使って **Port VLAN** を提供するように設定されている。

## 手順

1. `/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf` で **username** および **password** を設定します。
  - **username**: Manager 管理者のユーザー名。デフォルトは `admin@internal` です。
  - **password**: Manager 管理者のパスワード。デフォルトは `123456` です。
2. `etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf` で以下の値を更新して、LLDP Labeler サービスを設定します。
  - **clusters**: サービスが実行されるクラスターのコンマ区切りリスト。ワイルドカードはサポートされます。たとえば、**Cluster\*** は、**Cluster** という単語から始まるすべてのクラスターで実行する LLDP ラクターを定義します。データセンター内のすべてのクラスターでサービスを実行するには、\* と入力します。デフォルトは **Def\*** です。
  - **api\_url**: Manager の API の完全な URL。デフォルトは `https://Manager_FQDN/ovirt-engine/api` です。
  - **ca\_file**: カスタム CA 証明書ファイルへのパス。カスタム証明書を使用しない場合は、この値を空欄のままにします。デフォルトは空です。
  - **auto\_bonding**: LLDP ラベラーのボンディング機能を有効にします。デフォルトは `true` です。
  - **auto\_labeling**: LLDP ラベラーのラベリング機能を有効にします。デフォルトは `true` です。
3. 必要に応じて、`etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer` の **OnUnitActiveSec** の値を変更することで、別の時間間隔でサービスを実行するように設定できます。デフォルトは `1h` です。
4. 以下のコマンドを入力して、現在およびシステムの起動時にサービスが開始するように設定します。

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

手動でサービスを呼び出すには、以下のコマンドを入力します。

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

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

### 2.4.4.9. ホストの FQDN の変更

以下の手順で、ホストの完全修飾ドメイン名を変更します。

## 手順

1. ホストをメンテナンスモードにして、仮想マシンが別のホストにライブマイグレーションされ

るようになります。詳細は、[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。あるいは、すべての仮想マシンを手動でシャットダウンするか、別のホストに移行してください。詳細は、[仮想マシン管理ガイド](#) の [仮想マシンの手動移行](#) を参照してください。

2. Remove をクリックし、OK をクリックすると、管理ポータルからホストが削除されます。
3. **hostnamectl** ツールを使用して、ホスト名を更新します。その他のオプションは、[Red Hat Enterprise Linux 7 ネットワークガイド](#) の [ホスト名の設定](#) を参照してください。

```
hostnamectl set-hostname NEW_FQDN
```

4. ホストを再起動します。
5. ホストをマネージャーに再登録する。詳細は、[マネージャーへの標準ホストの追加](#) を参照してください。

#### 2.4.4.9.1. IPv6 ネットワーキングサポート

Red Hat Virtualization は、ほとんどのコンテキストで静的 IPv6 ネットワーキングをサポートします。



#### 注記

Red Hat Virtualization では、Manager を実行しているコンピューターまたは仮想マシン（もしくは "Manager マシン"）で、引き続き IPv6 を有効にする必要があります。お使いのシステムが IPv6 を使用しない場合でも、Manager マシンで [IPv6 を無効にしないでください](#)。

#### IPv6 の制限事項

- スタティックな IPv6 アドレッシングにのみ対応しています。DHCP や Stateless Address Autoconfiguration による動的な IPv6 アドレスの設定はサポートしていません。
- デュアルスタックアドレッシング、IPv4 および IPv6 はサポートされていません。
- OVN のネットワークは、IPv4 または IPv6 のみで使用できます。
- クラスターの IPv4 から IPv6 への切り替えはサポートされていません。
- IPv6 では、ホストごとに1つのゲートウェイしか設定できません。
- 両方のネットワークが単一のゲートウェイを共有している（同じサブネット上にある）場合は、デフォルトルートのロールを管理ネットワーク（ovirtmgmt）から別の論理ネットワークに移動できます。ホストと Manager は同じ IPv6 ゲートウェイを持つ必要があります。ホストと Manager が同じサブネット上にない場合、IPv6 ゲートウェイが削除されたために Manager がホストとの接続を失う可能性があります。
- IPv6 アドレスの gluster サーバーでの glusterfs ストレージドメインの使用はサポートされていません。

#### 2.4.4.9.2. SR-IOV のセットアップと設定

このトピックでは、SR-IOV のセットアップと設定の手順をまとめ、各手順の詳細を説明するトピックへのリンクを掲載しています。

#### 前提条件

SR-IOV を実装するためのハードウェアの考慮事項 に従ってハードウェアをセットアップする。

## 手順

SR-IOV をセットアップして設定するには、以下のタスクを実行します。

1. PCI パススルーを有効にするためのホストの設定
2. NIC の仮想機能設定の編集
3. vNIC プロファイルでのパススルーの有効化
4. 移行中のネットワーク停止を減らすための SR-IOV 対応 vNIC を使用した仮想マシンの設定

## 注記

- パススルーの vNIC の数は、ホスト上で利用可能な仮想機能 (VF) の数によって異なります。たとえば、3つの SR-IOV カード (vNIC) で仮想マシン (VM) を実行するには、ホストで 3つ以上の VF が有効になっている必要があります。
- ホットプラグとアンプラグに対応しています。
- ライブマイグレーションにも対応しています。
- 仮想マシンを移行するためには、移行先のホストにも VM を受け入れるのに十分な空き VF が必要です。マイグレーションの際、仮想マシンはソースホスト上のいくつかの VF を解放し、宛先ホスト上で同じ数の VF を占有します。
- ホストには、他のインターフェイスと同様に、デバイス、リンク、または ifcae が表示されます。そのデバイスは、仮想マシンに接続すると消え、切り離すと再び表示されます。
- SR-IOV 機能では、ホストデバイスを仮想マシンに直接接続することは避けてください。
- 複数の VLAN を持つトランクポートとして VF を使用し、ゲスト内で VLAN を設定するには、[Cannot configure VLAN on SR-IOV VF interfaces inside the Virtual Machine](#) を参照してください。

ここでは、インターフェイスの libvirt XML がどのように見えるかの例を示します。

```

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

```

## トラブルシューティング

以下の例は、インターフェイスにアタッチされている VF に関する診断情報を取得する方法を示しています。

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

```

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

```

#### 2.4.4.9.2.1. 関連情報

- [How to configure SR-IOV passthrough for RHV VM?](#)
- [How to configure bonding with SR-IOV VF\(Virtual Function\) in RHV](#)
- [How to enable host device passthrough and SR-IOV to allow assigning dedicated virtual NICs to virtual machines in RHV](#)

### 2.4.5. ネットワークボンディング

#### 2.4.5.1. ボンディングメソッド

ネットワークボンディングは、複数の NIC を1つのボンドデバイスにまとめるもので、以下のようなメリットがあります。

- ボンディングされた NIC の伝送速度は、シングル NIC の伝送速度よりも高速です。
- ネットワークボンディングは、その NIC のすべてで障害が発生しない限り障害が発生することはないため、フォールトトレランスを提供します。

同じメーカー、同じモデルの NIC を使用することで、同じボンディングオプションやモードをサポートすることができます。



#### 重要

Red Hat Virtualization のデフォルトのボンディングモードである (**Mode 4) Dynamic Link Aggregation** には、802.3ad をサポートするスイッチが必要です。

ボンディングの論理的なネットワークには互換性がなければなりません。ボンディングは、非 VLAN 論理ネットワークを1つだけサポートできます。残りの論理ネットワークには、固有の VLAN ID を設定する必要があります。

スイッチのポートでボンディングを有効にする必要があります。具体的な方法は、スイッチのベンダーが提供するマニュアルを参照してください。

ネットワークボンドデバイスは、以下のいずれかの方法で作成することができます。

- [管理ポータル](#) で、特定のホストに対して手動で作成する方法
- クラスターやデータセンター内の全ホストのボンディングされていない NIC に対して、[LLDP Labeler](#) を用いて自動的に作成する方法

ご使用の環境で iSCSI ストレージを使用していて、冗長性を実装する場合は、iSCSI マルチパスを設定するための手順に従ってください。

#### 2.4.5.2. 管理ポータルでのボンドデバイスの作成

管理ポータルで特定のホストにボンドデバイスを作成することができます。ボンドデバイスは、VLAN タグ付きのトラフィックと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

1. Compute → Hosts をクリックします。
2. ホストの名前をクリックします。詳細ビューが開きます。
3. Network Interfaces タブをクリックすると、ホストに接続されている物理的なネットワークインターフェイスが一覧表示されます。
4. Setup Host Networks をクリックします。
5. スイッチの設定を確認してください。スイッチが LLDP (Link Layer Discovery Protocol) 情報を提供するように設定されている場合は、物理的な NIC の上にカーソルを置くと、スイッチポートのアグリゲーション設定が表示されます。
6. NIC を他の NIC やボンドにドラッグアンドドロップします。



##### 注記

2枚の NIC が新しいボンドを形成します。NIC とボンドは、既存のボンドに NIC を追加します。

論理ネットワークに [互換性がない](#) 場合、ボンディング操作はロックされます。

7. ドロップダウンメニューから Bond Name および Bonding Mode を選択します。詳細は、[ボンディングモード](#) を参照してください。  
Custom ボンディングモードを選択した場合、次の例のように、テキストフィールドにボンディングオプションを入力できます。
  - ご使用の環境で **ethtool** を使用してもリンク状態が報告されない場合は、**mode=1arp\_interval=1arp\_ip\_target=192.168.0.2** を入力して ARP モニタリングを設定できます。
  - **mode=1 primary=eth0** を入力すると、スループットの高い NIC をプライマリーインターフェイスとして指定できます。  
ボンディングオプションとその説明のリストについては、Kernel.org の [Linux Ethernet Bonding Driver HOWTO](#) を参照してください。
8. OK をクリックします。
9. 新しいボンドに論理ネットワークをアタッチして設定します。手順は [ホストネットワークインターフェイスの編集](#) および [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。



## 注記

論理ネットワークをボンド内の個々の NIC に直接アタッチすることはできません。

10. オプション: ホストがメンテナスマードの場合は、Verify connectivity between Host and Engine を選択できます。

11. OK をクリックします。

### 2.4.5.3. LLDP Labeler Service によるボンドデバイスの作成

LLDP Labeler サービスを利用すると、1つ以上のクラスターまたはデータセンター全体のすべてのホストに対して、すべてのアンボンド NIC で自動的にボンドデバイスを作成することができます。ボンディングモードは (Mode 4) Dynamic Link Aggregation(802.3ad) です。

互換性のない論理ネットワークを持つ NIC は結合できません。

#### 2.4.5.3.1. LLDP ラベルセレクターの設定

デフォルトでは、LLDP Labeler は1時間ごとのサービスとして動作します。このオプションは、ハードウェアを変更する場合(NIC、スイッチ、ケーブルなど)、またはスイッチ設定を変更する場合に役立ちます。

#### 前提条件

- インターフェイスは、ジュニパー製スイッチに接続されている。
- ジュニパースイッチは、LLDP を使用してリンクアグリゲーション制御プロトコル (LACP) 用に設定する必要があります。

#### 手順

- /etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf で **username** および **password** を設定します。
  - username**: Manager 管理者のユーザー名。デフォルトは **admin@internal** です。
  - password**: Manager 管理者のパスワード。デフォルトは **123456** です。
- etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf で以下の値を更新して、LLDP Labeler サービスを設定します。
  - clusters**: サービスが実行されるクラスターのコンマ区切りリスト。ワイルドカードはサポートされます。たとえば、**Cluster\*** は、**Cluster** という単語から始まるすべてのクラスターで実行する LLDP ラクターを定義します。データセンター内のすべてのクラスターでサービスを実行するには、\*と入力します。デフォルトは **Def\*** です。
  - api\_url**: Manager の API の完全な URL。デフォルトは **https://Manager\_FQDN/ovirt-engine/api** です。
  - ca\_file**: カスタム CA 証明書ファイルへのパス。カスタム証明書を使用しない場合は、この値を空欄のままにします。デフォルトは空です。
  - auto\_bonding**: LLDP ラベラーのボンディング機能を有効にします。デフォルトは **true** です。

- **auto\_labeling**: LLDP ラベラーのラベリング機能を有効にします。デフォルトは **true** です。
- 必要に応じて、**etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer** の **OnUnitActiveSec** の値を変更することで、別の時間間隔でサービスを実行するように設定できます。デフォルトは **1h** です。
  - 以下のコマンドを入力して、現在およびシステムの起動時にサービスが開始するように設定します。

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

手動でサービスを呼び出すには、以下のコマンドを入力します。

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

- 新しいボンドに論理ネットワークをアタッチして設定します。手順は [ホストネットワークインターフェイスの編集および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。



#### 注記

論理ネットワークをボンド内の個々の NIC に直接アタッチすることはできません。

#### 2.4.5.4. ボンディングモード

パケット分散アルゴリズムは、ボンディングモードによって決定されます。(詳細は [Linux Ethernet Bonding Driver HOWTO](#) を参照してください)。Red Hat Virtualization のデフォルトのボンディングモードは **(Mode 4)Dynamic Link Aggregation(802.3ad)** です。

Red Hat Virtualization は、仮想マシン(ブリッジ)ネットワークで使用できるため、以下のボンディングモードをサポートしています。

##### **(Mode 1) Active-Backup**

1つの NIC がアクティブです。アクティブな NIC が故障した場合、バックアップ NIC の1つが、ボンド内の唯一のアクティブな NIC としてその NIC を置き換えます。このボンドの MAC アドレスは、ネットワークアダプターのポートにのみ表示されます。これにより、ボンドの MAC アドレスが変更されても、新しいアクティブな NIC の MAC アドレスが反映されるため、MAC アドレスの混乱を防ぐことができます。

##### **(Mode 2) Load Balance (balance-xor)**

パケットを送信する NIC は、送信元 MAC アドレスと宛先 MAC アドレスに対して XOR 演算を実行し、NIC の総数の **modulo** を乗算して選択されます。このアルゴリズムでは、各宛先 MAC アドレスに対して同じ NIC が選択されるようになっています。

##### **(Mode 3) Broadcast**

パケットはすべての NIC に送信されます。

##### **(Mode 4) Dynamic Link Aggregation(802.3ad) (デフォルト)**

NIC は、同じ速度とデュプレックス設定を共有するグループに集約されます。アクティブなアグリゲーショングループのすべての NIC が使用されます。

## 注記

**(Mode 4) Dynamic Link Aggregation(802.3ad)** には 802.3ad 対応のスイッチが必要です。

ボンディングされた NIC は、同じアグリゲーター ID を持つ必要があります。それ以外の場合、Manager は Network Interfaces タブのボンドに警告として感嘆符アイコンを表示し、ボンドの **ad\_partner\_mac** 値は **00:00:00:00:00:00** として報告されます。以下のコマンドを入力することで、アグリゲーター ID を確認できます。

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

[Which bonding modes work when used with a bridge that virtual machine guests or containers connect to?](#) を参照してください。

以下のボンディングモードは、仮想マシンの論理ネットワークとは互換性がないため、これらのモードを使用してボンディングに接続できるのは非仮想マシンの論理ネットワークのみです。

### (Mode 0) Round-Robin

NIC は、パケットを順番に送信します。パケットは、ボンド内の利用可能な最初の NIC から始まり、ボンド内の利用可能な最後の NIC で終わるループで送信されます。後続のループは、最初に利用可能な NIC から始まります。

### (Mode 5) Balance-TLB (Transmit Load-Balance とも呼ばれる)

送信トラフィックは、負荷に応じて、ボンド内のすべての NIC に分散されます。受信トラフィックは、アクティブな NIC で受信されます。受信トラフィックを受信する NIC が故障した場合、別の NIC が割り当てられます。

### (Mode 6) Balance-ALB (Adaptive Load-Balance とも呼ばれる)

(Mode 5) Balance-TLB は、IPv4 トラフィックの受信負荷分散と組み合わせます。ARP ネゴシエーションは、受信負荷のバランスをとるために使用されます。

## 2.5. ホスト

### 2.5.1. ホストの概要

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

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

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



## 注記

Red Hat Virtualization Manager で個々のホストのホストタイプを識別するには、ホストの名前を選択します。詳細ビューが開きます。次に、Software の OS Description を確認します。

ホストは、仮想化の最適化を提供する **tuned** プロファイルを使用します。**tuned** の詳細は、Red Hat Enterprise Linux システムのステータスとパフォーマンスの監視と管理 の [TuneD プロファイル](#) を参照してください。

Red Hat Virtualization Host では、セキュリティ機能が有効になっています。SELinux (Security Enhanced Linux) とファイアウォールは完全に設定されており、デフォルトでオンになっています。選択したホストの SELinux の状態は、詳細ビューの General タブの SELinux mode で報告されます。Manager は、Red Hat Enterprise Linux ホストを環境に追加する際に、必要なポートを開くことができます。

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

Red Hat Virtualization プラットフォーム上の物理的なホストは、以下を満たす必要があります。

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

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

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

### 2.5.2. Red Hat Virtualization Host

Red Hat Virtualization Host (RHVH) は、仮想マシンをホストするために必要なパッケージのみを搭載した、Red Hat Enterprise Linux の特別なビルドを使用してインストールされます。Red Hat Enterprise Linux ホストで使用されているものをベースにした **Anaconda** インストールインターフェイスを使用しており、Red Hat Virtualization Manager または **yum** を通じて更新することができます。追加のパッケージをインストールして、アップグレード後もそれを維持するには、**yum** コマンドを使う必要があります、それ以外の方法はありません。

RHVH には、ホストのリソースを監視し、管理作業を行うための Cockpit Web インターフェイスがあります。SSH やコンソールを介した RHVH への直接アクセスはサポートされていません。そのため、Cockpit Web インターフェイスは、ネットワークの設定や、Terminal サブタブ経由でのターミナルコマンドの実行など、ホストが Red Hat Virtualization Manager に追加される前に実行されるタスクのためのグラフィカルユーザーインターフェイスを提供します。

Web ブラウザーで Cockpit Web インターフェイス (<https://HostFQDNorIP:9090>) にアクセスします。Cockpit for RHVH には、ホストのヘルスステータス、SSH ホストキー、セルフホスト型エンジンのス

データス、仮想マシン、および仮想マシンの統計情報を表示するカスタム Virtualization ダッシュボードが含まれています。

Red Hat Virtualization バージョン 4.4 SP1 以降、RHVH は **systemd-coredump** を使用してコアダンプを収集、保存、および処理します。詳細は、[core dump storage configuration files](#) および [systemd-coredump service](#) のドキュメントを参照してください。

Red Hat Virtualization 4.4 以前では、RHVH は自動バグ報告ツール (ABRT) を使用して、アプリケーションのクラッシュに関する有意義なデバッグ情報を収集します。詳細は [Red Hat Enterprise Linux System 管理者ガイド](#) を参照してください。



### 注記

カスタムブートカーネル引数は、**grubby** ツールを使用して Red Hat Virtualization Host に追加することができます。**grubby** ツールは、**grub.cfg** ファイルに永続的な変更を加えます。ホストの Cockpit Web インターフェイスの Terminal サブタブに移動し、**grubby** コマンドを使用します。詳細は [Red Hat Enterprise Linux System 管理者ガイド](#) を参照してください。



### 警告

ローカルのセキュリティ脆弱性が悪用される可能性があるので、RHVH には信頼できないユーザーを作成しないでください。

## 2.5.3. Red Hat Enterprise Linux ホスト

対応するハードウェアにインストールされた Red Hat Enterprise Linux 7 をホストとして使用することができます。Red Hat Virtualization は、Red Hat Enterprise Linux 7 Server AMD64/Intel 64 版の Intel VT または AMD-V 拡張を実行するホストをサポートします。Red Hat Enterprise Linux マシンをホストとして使用するには、**Red Hat Enterprise Linux Server** および **Red Hat Virtualization** のサブスクリプションもアタッチする必要があります。

ホストを追加するには、仮想化のチェック、パッケージのインストール、およびブリッジ作成の各ステップをプラットフォームで完了する必要があるため、多少時間がかかります。詳細ビューを使用して、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監視します。

オプションで、ホストのリソースを監視し、管理タスクを実行するために、Cockpit をインストールできます。Cockpit Web インターフェイスは、ネットワークの設定や、Terminal サブタブ経由でのターミナルコマンドの実行など、ホストが Red Hat Virtualization Manager に追加される前に実行されるタスクのためのグラフィカルユーザーインターフェイスを提供します。



### 重要

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

## 2.5.4. Satellite ホストプロバイダーのホスト

Satellite ホストプロバイダーによって提供されたホストは、Red Hat Virtualization Manager によって仮

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

## 2.5.5. ホストのタスク

### 2.5.5.1. Red Hat Virtualization Manager への通常ホストの追加



#### 重要

クラスター内のホストのネットワーク設定を変更するには、必ず RHV Manager を使用します。使用しない場合は、サポート対象外の設定が作成される可能性があります。詳細は、[Network Manager のステートフル設定 \(nmstate\)](#) を参照してください。

Red Hat Virtualization 環境にホストを追加するには、仮想化のチェック、パッケージのインストール、およびブリッジ作成の各ステップをプラットフォームで完了する必要があるため、多少時間がかかります。

#### 手順

1. 管理ポータルから **Compute → Hosts** をクリックします。
2. **New** をクリックします。
3. ドロップダウンリストを使用して、新規ホスト用の **Data Center** および **Host Cluster** を選択します。
4. 新規ホストの **Name** と **Address** を入力します。SSH Port 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 PublicKey フィールドに表示される鍵をホスト上の `/root/.ssh/authorized_keys` にコピーして、公開鍵認証を使用します。
6. オプションで、Advanced Parameters ボタンをクリックして、以下に示すホストの詳細設定を変更します。
  - ファイアウォールの自動設定を無効にします。
  - 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します。手動での追加または自動取得が可能です。
7. ホストにサポート対象の電源管理カードが搭載されている場合は、オプションとして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詳細は、[管理ガイド の ホスト電源管理の設定の説明](#) 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、通知トレイ (🔔) のイベントセクションでインストールの進捗状況を確認できます。しばらくすると、ホストのステータスが **Up** になります。

### 2.5.5.2. 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プロセスは、マネージャーでホストを識別する方法を除いて、Red Hat Enterprise Linux のホストを追加するプロセスとほぼ同じです。以下の手順では、Satellite ホストプロバイダーが提供するホストの追加方法を説明します。

#### 手順

1. Compute → Hosts をクリックします。
2. New をクリックします。
3. ドロップダウンメニューを使って、新しいホストの Host Cluster を選択します。
4. Foreman/Satellite チェックボックスを選択すると、Satellite ホストプロバイダーのホストを追加するためのオプションが表示され、ホストを追加するプロバイダーを選択できます。
5. Discovered Hosts または Provisioned Hosts のいずれかを選択します。
  - Discovered Hosts (デフォルトオプション): ドロップダウンリストから、ホスト、ホストグループ、コンピュートリソースを選択します。
  - Provisioned Hosts: Providers Hosts ドロップダウンリストからホストを選択します。外部プロバイダーから取得できるホストの詳細は自動的に設定され、必要に応じて編集できます。
6. 新しいホストの Name と SSH Port (プロビジョニング済みホストのみ) を入力します。
7. ホストで使用する認証方法を選択します。
  - パスワード認証を使用するには、root ユーザーのパスワードを入力します。
  - SSH PublicKey フィールドに表示される鍵をホスト上の /root/.ssh/authorized\_keys にコピーして、公開鍵認証を使用します (プロビジョニング済みホストのみ)。
8. これで、Red Hat Enterprise Linux ホストを追加するための必須手順が完了しました。Advanced Parameters ドロップダウンボタンをクリックすると、ホストの詳細設定が表示されます。
  - a. オプションで、ファイアウォールの自動設定を無効にします。
  - b. 必要に応じてホストの SSH フィンガープリントを追加し、セキュリティーを強化します。手動での追加または自動取得が可能です。
9. 現在、適切なタブを使用して Power Management、SPM、Console、Network Provider を設定できますが、これらは Red Hat Enterprise Linux ホストを追加するための基本ではないため、この手順では説明しません。
10. OK をクリックすると、ホストが追加され、ウィンドウが閉じます。

新規ホストが **Installing** のステータスでホスト一覧に表示され、詳細ビューでインストールの進捗を表示できます。インストールが完了すると、ステータスが **Reboot** に更新されます。ホストがアクティブでなければ、ステータスは **Up** に変わりません。

### 2.5.5.3. ホストでの Satellite エラーダ表示の設定

管理ポータルでは、Red Hat Satellite からエラーランクを表示するようにホストを設定できます。ホストを Red Hat Satellite プロバイダーと関連付けた後、ホスト設定ダッシュボードで利用可能なエラーランクとその重要性に関する更新情報を受け取り、現実的な更新適用時期を決定できます。

Red Hat Virtualization 4.4 は、Red Hat Satellite 6.6 でのエラーランクの表示をサポートします。

## 前提条件

- Satellite サーバーが外部プロバイダーとして追加されている。
- Manager と、エラーランクの表示先であるホストが、それぞれの FQDN で Satellite サーバーに登録されている。これにより、外部コンテンツホスト ID を Red Hat Virtualization で維持する必要がなくなります。



### 重要

IP アドレスを使用して追加されたホストは、エラーランクを報告できません。

- ホストを管理する Satellite アカウントは、Administrator パーミッションを持ち、デフォルトの組織が設定されている必要があります。
- ホストを Satellite Server に登録しておく必要があります。
- Red Hat Satellite のリモート実行を使用して、ホスト上のパッケージを管理する。



### 注記

Katello エージェントは非推奨で、今後の Satellite のバージョンで削除されます。プロセスを移行し、リモート実行機能を使用してクライアントをリモートで更新してください。

## 手順

1. Compute → Hosts をクリックし、ホストを選択します。
2. Edit をクリックします。
3. Use Foreman/Satellite チェックボックスを選択します。
4. ドロップダウンリストから、必要な Satellite サーバーを選択します。
5. OK をクリックします。

これで、ホスト設定の管理に使用されるダッシュボードに、利用可能なエラーランクとその重要性が表示されるようになりました。

## 関連情報

- ホストのプロビジョニングに使用する Red Hat Satellite インスタンスの追加
- Red Hat Satellite ドキュメントの [ホスト管理](#) に記載されている [Goferd と Katello Agent を使用しないホスト管理](#)

### 2.5.5.3.1. PCI パススルー用ホストの設定



## 注記

これは、Red Hat Virtualization で SR-IOV を準備およびセットアップする方法を示す一連のトピックの1つです。詳細は、[SR-IOV のセットアップと設定](#) を参照してください。

PCI パススルーを有効化すると、デバイスが仮想マシンに直接アタッチされているかのように、ホストのデバイスを仮想マシンで使用できます。PCI パススルー機能を有効化するには、仮想化拡張機能および IOMMU 機能を有効化する必要があります。以下の手順では、ホストを再起動する必要があります。すでにホストが Manager にアタッチされている場合は、最初にホストがメンテナンスマードに設定されていることを確認してください。

## 前提条件

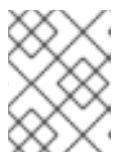
- ホストハードウェアが PCI デバイスパススルーおよび割り当ての要件を満たしていることを確認する。詳細は、[PCI デバイスの要件](#) を参照してください。

## PCI パススルー用ホストの設定

- BIOS の仮想化拡張機能および IOMMU 拡張機能を有効にします。詳細は、[Red Hat Enterprise Linux 仮想化の導入および管理ガイド](#) の [BIOS での Intel VT-X と AMD-V の仮想化ハードウェア拡張の有効化](#) を参照してください。
- ホストを Manager に追加する際に Hostdev Passthrough & SR-IOV のチェックボックスを選択するか、手動で grub 設定ファイルを編集して、カーネルの IOMMU フラグを有効化します。
  - 管理ポータルから IOMMU フラグを有効化する方法については、[Red Hat Virtualization Manager への通常ホストの追加](#) および [カーネル設定の説明](#) を参照してください。
  - 手動で grub 設定ファイルを編集する方法については、[IOMMU の手動での有効化](#) を参照してください。
- GPU パススルーを有効にするには、ホストとゲストシステムの両方で追加の設定手順を実行する必要があります。詳細は、[Red Hat Virtualization での仮想マシン用 NVIDIA GPU のセットアップ](#) の [GPU デバイスパススルー: 単一の仮想マシンへのホスト GPU の割り当て](#) を参照してください。

## IOMMU の手動での有効化

- grub 設定ファイルを編集して IOMMU を有効化します。



## 注記

IBM POWER8 ハードウェアを使用している場合は、デフォルトで IOMMU が有効になっているため、この手順は省略してください。

- Intel の場合は、マシンを起動し、grub 設定ファイルの `GRUB_CMDLINE_LINUX` 行の末尾に `intel_iommu=on` を追加します。

```
vi /etc/default/grub
...
GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... intel_iommu=on
..."
```

- AMD の場合は、マシンを起動し、grub 設定ファイルの **GRUB\_CMDLINE\_LINUX** 行の末尾に **amd\_iommu=on** を追加します。

```
vi /etc/default/grub
...
GRUB_CMDLINE_LINUX="nofb splash=splash console=tty0 ... amd_iommu=on
..."
```

## 注記

**intel\_iommu=on** または AMD IOMMU が検出される場合は、**iommu=pt** を追加してみてください。**pt** オプションでは、パススルーで使用するデバイスの IOMMU のみが有効化され、ホストのパフォーマンスが向上します。ただし、このオプションはすべてのハードウェアでサポートされているわけではありません。**pt** オプションがお使いのホストで機能しない場合は、以前のオプションに戻してください。

ハードウェアが割り込みの再マッピングをサポートしていないためにパススルーが失敗する場合、仮想マシンが信頼できるのであれば **allow\_unsafe\_interrupts** オプションを有効化することも検討してください。**allow\_unsafe\_interrupts** を有効化すると、ホストが仮想マシンからの MSI 攻撃にさらされる可能性があるため、このオプションはデフォルトで有効化されていません。オプションを有効化するには、以下のとおり設定してください。

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

- grub.cfg ファイルをリフレッシュしてからホストを再起動し、変更を有効にします。

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

### 2.5.5.3.2. すべての仮想マシンでネストされた仮想化を有効化

#### 重要

フックを使用してネストされた仮想化を有効にする機能は、テクノロジープレビュー機能です。テクノロジープレビュー機能は、Red Hat の実稼働環境のサービスレベルアグリーメント (SLA) ではサポートされず、機能的に完全ではないことがあるため、Red Hat では実稼働環境での使用を推奨していません。テクノロジープレビュー機能では、最新の製品機能をいち早く提供します。これにより、お客様は開発段階で機能をテストし、フィードバックを提供できます。詳細は、[テクノロジープレビュー機能のサポート範囲](#) を参照してください。

仮想マシンが他の仮想マシンをホストすることができるネスト型の仮想化。わかりやすくするために、これらを **親仮想マシン** と **ネストされた仮想マシン** と呼ぶことにします。

子仮想マシンを表示および管理できるのは、親仮想マシンへのアクセス権を持つユーザーだけです。Red Hat Virtualization (RHV) の管理者には見えません。

デフォルトでは、RHV ではネストされた仮想化は有効になっていません。ネストされた仮想化を有効にするには、クラスター内のすべてのホストに VDSM フック **vdsmd-hook-nestedv**t をインストールします。これらのホスト上で動作するすべての仮想マシンは、親仮想マシンとして機能できます。

親仮想マシンは、ネストされた仮想化をサポートするホスト上でのみ実行する必要があります。親仮想マシンがネストされた仮想化をサポートしていないホストに移行した場合、その子仮想マシンが失敗するという問題がありました。これを防ぐためには、クラスター内のすべてのホストがネストされた仮想化をサポートするように設定します。それ以外の場合は、親仮想マシンがネストされた仮想化をサポートしていないホストへの移行を制限します。

### 警告



親仮想マシンが、ネストされた仮想化をサポートしていないホストに移行しないよう注意してください。

### 手順

1. 管理ポータルで **Compute** → **Hosts** をクリックします。
2. ネストされた仮想化を有効にするクラスターでホストを選択し、**Management** → **Maintenance** および **OK** をクリックします。
3. 再度、ホストを選択し、**Host Console** をクリックして、ホストコンソールにログインします。
4. VDSM フックを取り付けます。

```
dnf install vdsmd-hook-nestedv
```

5. ホストを再起動します。
6. ホストのコンソールに再度ログインし、ネストされた仮想化が有効になっていることを確認します。

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

このコマンドが **Y** または **1** を返す場合、この機能は有効になっています。

7. この手順をクラスター内のすべてのホストに繰り返します。

### 関連情報

- [VDSM フック](#)

#### 2.5.5.3.3. 個々の仮想マシンでネストされた仮想化を有効化



## 重要

ネストされた仮想化はテクノロジープレビュー機能です。テクノロジープレビュー機能は、Red Hat の実稼働環境のサービスレベルアグリーメント (SLA) ではサポートされず、機能的に完全ではないことがあるため、Red Hat では実稼働環境での使用を推奨していません。テクノロジープレビュー機能では、最新の製品機能をいち早く提供します。これにより、お客様は開発段階で機能をテストし、フィードバックを提供できます。詳細は、[テクノロジープレビュー機能のサポート範囲](#) を参照してください。

仮想マシンが他の仮想マシンをホストすることができるネスト型の仮想化。わかりやすくするために、これらを **親仮想マシン** と **ネストされた仮想マシン** と呼ぶことにします。

子仮想マシンを表示および管理できるのは、親仮想マシンへのアクセス権を持つユーザーだけです。Red Hat Virtualization (RHV) の管理者には見えません。

すべての仮想マシンではなく、**特定の仮想マシン** でネストされた仮想化を有効にするには、ネストされた仮想化をサポートするようにホストを設定します。その後、その特定のホスト上で動作する仮想マシンを設定し、**Pass-Through Host CPU** を有効にします。このオプションにより、仮想マシンは、ホストで設定したネストされた仮想化の設定を使用できます。このオプションでは、仮想マシンを実行できるホストが制限され、手動での移行が必要になります。

それ以外の場合で、クラスター内の **すべての仮想マシン** に対してネストされた仮想化を有効にするには、[すべての仮想マシンに対してネストされた仮想化を有効にする](#) を参照してください。

親仮想マシンは、ネストされた仮想化をサポートするホスト上でのみ実行してください。親仮想マシンをネストされた仮想化をサポートしていないホストに移行すると、その子仮想マシンが故障します。



## 警告

親の仮想マシンは、ネストされた仮想化をサポートしていないホストに移行しないでください。

子仮想マシンを実行している親仮想マシンのライブマイグレーションは避けてください。移行元と移行先のホストが同一で、ネストされた仮想化をサポートしていても、ライブマイグレーションによって子仮想マシンが故障することがあります。代わりに、移行前に仮想マシンをシャットダウンしてください。

## 手順

ネストされた仮想化をサポートするようにホストを設定します。

1. 管理ポータルで **Compute → Hosts** をクリックします。
2. ネストされた仮想化を有効にするクラスターでホストを選択し、**Management → Maintenance** および **OK** をクリックします。
3. 再度、ホストを選択し、**Host Console** をクリックして、ホストコンソールにログインします。
4. **Edit Host** ウィンドウで、**Kernel** タブを選択します。
5. **Kernel boot parameters** で、チェックボックスがグレーアウトしている場合は、**RESET** をクリックします。

6. Nested Virtualization を選択し、OK をクリックします。
- カーネルコマンドラインに **kvm-<architecture>.nested=1** パラメーターを表示します。以下の手順では、このパラメーターを Current kernel CMD line に追加します。
7. Installation → Reinstall をクリックします。
8. ホストのステータスが Up に戻ったら、Power Management または SSH Management の下にある Management → Restart をクリックします。
9. ネストされた仮想化が有効になっていることを確認します。ホストのコンソールにログインし、入力します。

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

このコマンドが Y または 1 を返す場合、この機能は有効になっています。

10. この手順を、親仮想マシンを実行する必要があるすべてのホストに対して繰り返します。

特定の仮想マシンでネストされた仮想化を有効化するには、以下を実行します。

1. 管理ポータルで Compute → Virtual Machines をクリックします。
2. 仮想マシンを選択し、Edit をクリックします。
3. Edit Virtual Machine ウィンドウで Show Advanced Options をクリックし、Host タブを選択します。
4. Start Running On で Specific Host をクリックし、ネストされた仮想化をサポートするように設定したホストを選択します。
5. CPU Options で Pass-Through Host CPU を選択します。このアクションは、自動的に Migration mode を Allow manual migration only に設定します。



### 注記

RHV バージョン 4.2 では、Do not allow migration が選択されている場合に限り、Pass-Through Host CPU を有効にできます。

## 関連情報

- [VDSM フック](#)
- RHEL ドキュメントの [ネストされた仮想マシンの作成](#)。

### 2.5.5.4. ホストのメンテナンスマードへの切り替え

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

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



## 注記

ホストに固定されていて移行できない仮想マシンはシャットダウンされます。どの仮想マシンがホストに固定されているかは、ホストの詳細ビューの **Virtual Machines** タブで **Pinned to Host** をクリックすると確認できます。

## ホストのメンテナンスマードへの配置

1. **Compute** → **Hosts** をクリックし、任意のホストを選択します。
2. **Management** → **Maintenance** をクリックします。 **Maintenance Host** の確認画面が表示されます。
3. オプションで、ホストをメンテナンスマードに切り替える理由を **Reason** に入力します。これは、ログに表示され、ホストが再びアクティブになったときに表示されます。 **OK** をクリックします。



## 注記

ホストメンテナンスの **Reason** フィールドは、クラスター設定で有効になっていない場合にのみ表示されます。 詳細は、[クラスターの一般設定の説明](#) を参照してください。

4. オプションで、Gluster をサポートするホストに必要なオプションを選択します。

デフォルトのチェックを回避するには、**Ignore Gluster Quorum and Self-Heal Validations** オプションを選択します。デフォルトでは、ホストがメンテナンスマードに切り替わったときに、Gluster クオーラムが失われていないか Manager が確認します。Manager は、ホストをメンテナンスマードに切り替えることで影響を受ける自己修復アクティビティーがないことを確認します。Gluster のクオーラムが失われる場合や、自己修復活動が影響を受ける場合、Manager はホストがメンテナンスマードになるのを防ぎます。このオプションは、他の方法でホストをメンテナンスマードに切り替えることができない場合にのみ使用してください。

ホストをメンテナンスマードに切り替える際にすべての Gluster サービスを停止するには、**Stop Gluster Service** オプションを選択します。



## 注記

これらのフィールドは、選択したホストが Gluster に対応している場合にのみ、ホストのメンテナスウィンドウに表示されます。 詳細は、[Red Hat Hyperconverged Infrastructure のメンテナンス の プライマリー Gluster Storage ノードの交換](#) を参照してください。

5. **OK** をクリックしてメンテナンスマードを開始します。

稼働中の仮想マシンはすべて代替ホストに移行されます。ホストが Storage Pool Manager (SPM) の場合、SPM のロールは別のホストに移行されます。ホストの **Status** フィールドが **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。ホストがメンテナンスマードになっても、VDSM は停止しません。



## 注記

いずれかの仮想マシンで移行が失敗した場合は、ホストで **Management** → **Activate** をクリックして操作を停止し、メンテナンスマードにしてから、仮想マシンで **Cancel Migration** をクリックして移行を停止します。

### 2.5.5.5. メンテナンスマードのホストのアクティブ化

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

#### 手順

1. Compute → Hosts をクリックし、ホストを選択します。
2. Management → Activate をクリックします。

操作が完了すると、ホストの状態は **Unassigned** に変わり、最後に **Up** となります。これで仮想マシンがホスト上で動作するようになりました。メンテナンスマード時にホストから移行された仮想マシンは、ホストが起動しても自動的には戻ってきませんが、手動で移行することができます。メンテナンスマードに移行する前にホストがストレージプールマネージャー (SPM) であった場合、ホストがアクティブになっても SPM のロールは自動的には戻りません。

#### 2.5.5.5.1. ホストファイアウォールルールの設定

ホストのファイアウォールルールは、Ansible を使用して永続的になるように設定することができます。firewalld を使用するようにクラスターが設定されている必要があります。



#### 注記

firewalld ゾーンの変更はサポートされていません。

#### ホストのファイアウォールルールの設定

1. Manager マシン上で、ovirt-host-deploy-post-tasks.yml.example を編集し、カスタムファイアウォールポートを追加します。

```
vi /etc/ovirt-engine/ansible/ovirt-host-deploy-post-tasks.yml.example

#
Any additional tasks required to be executing during host deploy process can
be added below
#
- name: Enable additional port on firewalld
 firewalld:
 port: "12345/tcp"
 permanent: yes
 immediate: yes
 state: enabled
```

2. ファイルを別の場所に ovirt-host-deploy-post-tasks.yml として保存します。

新規ホストまたは再インストールされたホストは、更新されたファイアウォールルールで設定されます。

Installation → Reinstall をクリックし、Automatically configure host firewall を選択して、既存のホストを再インストールする必要があります。

#### 2.5.5.5.2. ホストの削除

ホストの再インストール時など、Red Hat Virtualization 環境からホストを削除する必要がある場合があります。

## 手順

1. Compute → Hosts をクリックし、ホストを選択します。
2. Management → Maintenance をクリックします。
3. ホストがメンテナンスマードになったら、Remove をクリックします。Remove Host(s) の確認ウィンドウが開きます。
4. ホストが Red Hat Gluster Storage クラスターに含まれており、ボリュームブリックがある場合や、ホストが応答していない場合は、Force Remove 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。

### 2.5.5.3. マイナーリリース間でのホストの更新

クラスター内のすべてのホスト を更新したり、個別のホスト を更新したりできます。

#### 2.5.5.3.1. クラスター内の全ホストの更新

ホストを個別に更新するのではなく、クラスター内の全ホストを更新することができます。この手法は、Red Hat Virtualization を新しいバージョンにアップグレードする際に特に役立ちます。更新の自動化に使用する Ansible ロールの詳細は、[oVirt クラスターアップグレード](#) を参照してください。

クラスターは一度に1つずつ更新します。

## 制限

- RHVH を更新すると、/etc および /var ディレクトリー内の変更されたコンテンツのみ保持されます。他のパスに含まれる変更されたデータは、更新時に上書きされます。
- クラスターの移行が有効な場合、仮想マシンはそのクラスター内の別のホストに自動的に移行されます。
- セルフホスト型エンジン環境では、Manager 用仮想マシンは同一クラスター内のセルフホスト型エンジンノード間でのみ移行が可能です。通常のホストに移行することはできません。
- 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。確保されていないと、仮想マシンの移行がハングして失敗してしまいます。ホストを更新す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、ホスト更新によるメモリー使用量を減らすことができます。
- ホストに固定された仮想マシン (vGPU を使用している仮想マシンなど) を別のホストに移行することはできません。ホストをスキップするよう選択した場合を除き、更新中は固定された仮想マシンはシャットダウンされます。

## 手順

1. 管理ポータルで Compute → Clusters をクリックし、クラスターを選択します。Upgrade status 列には、クラスターの任意のホストでアップグレードが利用可能かどうかが表示されます。
2. Upgrade をクリックします。

3. 更新するホストを選択し、次に **Next** をクリックします。
4. オプションを設定します。
  - **Stop Pinned VMs:** クラスター内のホストに固定された仮想マシンをシャットダウンします。このオプションは、デフォルトで選択されています。このチェックボックスの選択を解除すると、固定された仮想マシンが動作を続けられるように、それらのホストの更新をスキップすることができます（固定された仮想マシンが重要なサービスまたはプロセスを実行中で、更新中の予期せぬ時にシャットダウンされるのを避けたい場合など）。
  - **Upgrade Timeout (Minutes):** このオプションで設定した時間内に個々のホストの更新が完了しない場合、クラスターのアップグレードはタイムアウトで失敗します。デフォルトは **60** です。60 分では不十分と思われる大規模なクラスターの場合は、時間を延長することができます。また、ホストの更新が短時間で完了する小規模なクラスターは、短縮することができます。
  - **Check Upgrade:** アップグレードプロセスを実行する前に、それぞれのホストで更新が利用可能かどうかを確認します。このオプションは、デフォルトでは選択されていません。ただし、Manager がホストの更新を確認する頻度をデフォルトより低く設定している状況などで、最新の更新を確実に含める必要がある場合は、このオプションを選択することができます。
  - **Reboot After Upgrade:** ホストの更新後に、それぞれのホストを再起動します。このオプションは、デフォルトで選択されています。ホストを再起動する必要のある保留中の更新がないことが明らかであれば、このチェックボックスの選択を解除してプロセスを迅速化することができます。
  - **Use Maintenance Policy:** 更新時にクラスターのスケジューリングポリシーを [cluster maintenance](#) に設定します。このオプションはデフォルトで選択されています。したがって、許可される動作は限定的で、仮想マシンは高可用性でない限り起動できません。更新中も使用を続けたいカスタムのスケジューリングポリシーがある場合は、このチェックボックスの選択を解除できます。ただし、解除することで想定外の結果が生じる可能性があります。このオプションを無効にする前に、カスタムのポリシーがクラスターのアップグレード操作に対応していることを確認してください。

5. **Next** をクリックします。
6. 影響を受けるホストと仮想マシンの概要を確認します。
7. **Upgrade** をクリックします。
8. クラスターのアップグレードステータス画面が表示され、完了の割合を示す進行状況バーと、完了したアップグレードプロセスの手順のリストが表示されます。[Go to Event Log](#) をクリックして、アップグレードのログエントリーを開くことができます。この画面を閉じても、アップグレードプロセスは中断されません。

以下で、ホスト更新の進捗状況を追跡できます。

- **Compute → Clusters** ビュー (**Upgrade Status** 列に完了率を示す進捗バーが表示されます)
- **Compute → Hosts** ビュー
- **Notification Drawer** の **Events** セクション (

仮想マシン移行の進捗を、**Compute → Virtual Machines** ビューの **Status** 列で個々に追跡できます。大規模な環境では、特定の仮想マシングループの結果を表示するために、結果を絞り込まなければならぬ場合があります。

### 2.5.5.3.2. 個々のホストの更新

ホストのアップグレードマネージャーを使用して、管理ポータルから直接個々のホストを更新します。



#### 注記

アップグレードマネージャーが確認するのは、ステータスが **Up** または **Non-operational** のホストだけです。ステータスが **Maintenance** のホストは確認されません。

#### 制限

- RHVH を更新すると、**/etc** および **/var** ディレクトリー内の変更されたコンテンツのみ保持されます。他のパスに含まれる変更されたデータは、更新時に上書きされます。
- クラスターの移行が有効な場合、仮想マシンはそのクラスター内の別のホストに自動的に移行されます。使用率が比較的に低い時間帯にホストを更新してください。
- セルフホスト型エンジン環境では、Manager 用仮想マシンは同一クラスター内のセルフホスト型エンジンノード間でのみ移行が可能です。通常のホストに移行することはできません。
- 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。確保されていないと、仮想マシンの移行がハングして失敗してしまいます。ホストを更新す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、ホスト更新によるメモリー使用量を減らすことができます。
- ホストに固定された仮想マシン (vGPU を使用している仮想マシンなど) を別のホストに移行することはできません。ホストを更新する前に、固定された仮想マシンをシャットダウンする必要があります。

#### 手順

- 適切なリポジトリが有効であることを確認します。現在有効なリポジトリの一覧を表示するには、**dnf repolist** を実行します。

- Red Hat Virtualization Host の場合:

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

- Red Hat Enterprise Linux ホストの場合:

```
subscription-manager repos \
--enable=rhel-8-for-x86_64-baseos-eus-rpms \
--enable=rhel-8-for-x86_64-appstream-eus-rpms \
--enable=rhv-4-mgmt-agent-for-rhel-8-x86_64-rpms \
--enable=advanced-virt-for-rhel-8-x86_64-rpms \
--enable=fast-datapath-for-rhel-8-x86_64-rpms
```

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

- 管理ポータルで **Compute → Hosts** をクリックし、更新するホストを選択します。
- Installation → Check for Upgrade** をクリックしてから **OK** をクリックします。  
Notification Drawer ( ) を開き、Events セクションを展開して結果を表示します。

4. 更新が利用可能であれば、**Installation → Upgrade** をクリックします。
5. **OK** をクリックしてホストを更新します。実行中の仮想マシンは、その移行ポリシーに従って移行されます。いずれかの仮想マシンの移行が無効になっている場合は、シャットダウンするよう求められます。  
**Compute → Hosts** にホストの情報が更新され、ステータスが以下の順序で変わります。

Maintenance > Installing > Reboot > Up



#### 注記

更新が失敗すると、ホストのステータスは **Install Failed** に変わります。**Install Failed** のステータスから **Installation → Upgrade** を再度クリックすることができます。

Red Hat Virtualization 環境内のホストごとに同じ手順を繰り返してください。



#### 注記

管理ポータルからホストを更新する必要があります。ただし、管理ポータルの代わりに **dnf upgrade** を使用してホストを更新することもできます。

### 2.5.5.3.3. ホストの手動更新

#### 注意

これは、ホストの手動更新 (Red Hat によるサポートの対象外) を実行する必要がある上級システム管理者向けの情報です。証明書の更新などの重要な手順については熟知していると想定し、このトピックでは説明していません。Red Hat は、管理ポータルを使用したホストの更新をサポートします。詳細は、[管理ガイド](#) の [個々のホストの更新](#) または [クラスター内の全ホストの更新](#) を参照してください。

**dnf** コマンドを使用して、ホストを更新できます。セキュリティーやバグに関する修正がタイムリーに適用されるように、システムを定期的に更新してください。

#### 制限

- RHVH を更新すると、**/etc** および **/var** ディレクトリー内の変更されたコンテンツのみ保持されます。他のパスに含まれる変更されたデータは、更新時に上書きされます。
- クラスターの移行が有効な場合、仮想マシンはそのクラスター内の別のホストに自動的に移行されます。使用率が比較的に低い時間帯にホストを更新してください。
- セルフホスト型エンジン環境では、Manager 用仮想マシンは同一クラスター内のセルフホスト型エンジンノード間でのみ移行が可能です。通常のホストに移行することはできません。
- 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。確保されていないと、仮想マシンの移行がハングして失敗してしまいます。ホストを更新す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、ホスト更新によるメモリー使用量を減らすことができます。
- ホストに固定された仮想マシン (vGPU を使用している仮想マシンなど) を別のホストに移行することはできません。ホストを更新する前に、固定された仮想マシンをシャットダウンする必要があります。

## 手順

- 適切なリポジトリが有効であることを確認します。**dnf repolist** を実行して、現在有効なリポジトリを確認できます。

- Red Hat Virtualization Host の場合:

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

- Red Hat Enterprise Linux ホストの場合:

```
subscription-manager repos \
--enable=rhel-8-for-x86_64-baseos-eus-rpms \
--enable=rhel-8-for-x86_64-appstream-eus-rpms \
--enable=rhv-4-mgmt-agent-for-rhel-8-x86_64-rpms \
--enable=advanced-virt-for-rhel-8-x86_64-rpms \
--enable=fast-datapath-for-rhel-8-x86_64-rpms
```

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

- 管理ポータルで **Compute → Hosts** をクリックし、更新するホストを選択します。

- Management → Maintenance** をクリックしてから **OK** をクリックします。

- Red Hat Enterprise Linux ホストの場合:

- Red Hat Enterprise Linux の現行バージョンを特定します。

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

- redhat-release パッケージの利用可能なバージョンを確認します。

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

このコマンドは、利用可能な更新をすべて表示します。たとえば、Red Hat Enterprise Linux 8.2.z から 8.3 にアップグレードする場合は、パッケージのバージョンを、現在インストールされているバージョンと比較します。

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

## 注意

通常、Red Hat Enterprise Linux Advanced Virtualization モジュールは、Red Hat Enterprise Linux y-stream よりも遅れてリリースされます。新しい Advanced Virtualization モジュールがまだ利用できない場合や、有効化した際にエラーが発生した場合は、ここで停止してアップグレードを取り消します。取り消さない場合は、ホストが破損するリスクがあります。

- Red Hat Enterprise Linux 8.3 以降の Advanced Virtualization ストリームが利用できる場合は、**virt** モジュールをリセットします。

```
dnf module reset virt
```



### 注記

Advanced Virtualization ストリームでこのモジュールがすでに有効になっている場合は、このステップは必要なく、マイナス要因となることもあります。

以下を入力してストリームの値を確認できます。

```
dnf module list virt
```

- d. 以下のコマンドを使用して、Advanced Virtualization ストリームで **virt** モジュールを有効にします。

- RHV 4.4.2 の場合:

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

- RHV 4.4.3 から 4.4.5 に対応しています。

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

- RHV 4.4.6 - 4.4.10 の場合:

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

- RHV 4.4 以降の場合:

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



### 注記

RHEL 8.6 以降、Advanced Virtualization パッケージは標準の **virt:rhel** モジュールを使用します。RHEL 8.4 および 8.5 では、1つの Advanced Virtualization ストリーム **rhel:av** のみが使用されます。

5. **nodejs** モジュールのバージョン 14 を有効にします。

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

6. ホストを更新します。

```
dnf upgrade --nobest
```

7. すべての更新が正常に適用されるように、ホストを再起動します。



## 注記

`imgbased` ログを確認して、Red Hat Virtualization Host 向けの追加パッケージの更新に失敗したものがないかを確認します。更新後に一部のパッケージの再インストールに失敗した場合は、そのパッケージが `/var/imgbased/persisted-rpms` に記載されていることを確認します。足りないパッケージを追加してから `rpm -Uvh /var/imgbased/persisted-rpms/*` を実行します。

Red Hat Virtualization 環境内のホストごとに同じ手順を繰り返してください。

### 2.5.5.4. ホストの再インストール

管理ポータルから Red Hat Virtualization Host (RHVH) および Red Hat Enterprise Linux ホストを再インストールします。この手順には、ホストの停止および再起動が含まれます。



#### 警告

ホストのオペレーティングシステムのインストールまたは再インストールを行う場合、Red Hat では、ホストにアタッチされている既存の OS 以外のストレージを最初にデタッチすることを強く推奨しています。これは、ディスクを誤って初期化してデータが失われる可能性を避けるためです。

#### 前提条件

- クラスターの移行が有効化されている場合、仮想マシンはそのクラスター内の別のホストに自動的に移行できます。したがって、使用量が比較的低い間にホストを再インストールします。
- ホストによるメンテナンスの実行に必要なメモリーがクラスターにあることを確認します。クラスターにメモリーがない場合、仮想マシンの移行はハングして失敗します。メモリー使用量を減らすには、ホストをメンテナンスに移行する前に、一部またはすべての仮想マシンをシャットダウンします。
- 再インストールを実行する前に、クラスターに複数のホストが含まれていることを確認してください。すべてのホストを同時に再インストールしようとしないでください。Storage Pool Manager (SPM) タスクを実行するには、1台のホストは使用可能な状態でなければなりません。

#### 手順

- Compute → Hosts をクリックし、ホストを選択します。
- Management → Maintenance をクリックしてから OK をクリックします。
- Installation → Reinstall をクリックします。Install Host ウィンドウが表示されます。
- OK をクリックして、ホストを再インストールします。

ホストを再インストールし、そのステータスが Up に戻れば、仮想マシンをホストに戻すことができます。



## 重要

Red Hat Virtualization Host を Red Hat Virtualization Manager に登録し、これを再インストールした後、管理ポータルでそのステータスが誤って **Install Failed** と表示される場合があります。Management → Activate をクリックすると、ホストのステータスが **Up** に変わり、使用できるようになります。

### 2.5.5.6. ホストのエラーダの表示

Red Hat Satellite サーバーからエラーダ情報を受信するようにホストを設定すると、各ホストのエラーダが表示されます。エラーダ情報を受け取るようホストを設定する方法は、[ホストの Satellite エラーダ管理の設定](#) を参照してください。

## 手順

1. Compute → Hosts をクリックします。
2. ホストの名前をクリックします。詳細ビューが開きます。
3. Errata タブをクリックします。

### 2.5.5.7. ホストのヘルスステータスの表示

ホストには、通常の **Status** に加えて、外部ヘルスステータスがあります。外部ヘルスステータスは、プラグインや外部システムから報告されたり、管理者が設定したりするもので、ホストの **Name** の左側に以下のいずれかのアイコンとして表示されます。

- OK: アイコンなし
- Info:
- Warning:
- Error:
- Failure:

ホストのヘルスステータスの詳細を表示するには、ホストの名前をクリックします。詳細ビューが開きます。ここで **Events** タブをクリックします。

REST API を使ってホストのヘルスステータスを確認することもできます。ホストの **GET** リクエストには、ヘルスステータスを含む **external\_status** 要素が含まれます。

REST API では、**events** コレクションを介してホストのヘルスステータスを設定できます。詳細は、[REST API ガイドの イベントの追加](#) を参照してください。

### 2.5.5.8. ホストデバイスの表示

各ホストのホストデバイスは、詳細ビューの **Host Devices** タブで確認できます。ホストにデバイスの直接割り当てが設定されている場合、これらのデバイスを仮想マシンに直接接続してパフォーマンスを高めることができます。

デバイスの直接割り当てに関するハードウェア要件の詳細は、[SR-IOV を実装するための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の考慮事項](#) を参照してください。

直接デバイスの割り当て用にホストを設定する方法は、[PCI パススルーのホストタスク用のホストの設定](#) を参照してください。

仮想マシンにホストデバイスを割り当てる方法の詳細は、[仮想マシン管理ガイド](#) の [ホストデバイス](#) を参照してください。

## 手順

1. Compute → Hosts をクリックします。
2. ホストの名前をクリックします。 詳細ビューが開きます。
3. Host Devices タブをクリックします。

このタブでは、仮想マシンに接続されているかどうか、その仮想マシンで現在使用されているかどうかなど、ホストデバイスの詳細が表示されます。

### 2.5.5.9. 管理ポータルから Cockpit へのアクセス

Cockpit は、デフォルトで Red Hat Virtualization Hosts (RHVH) および Red Hat Enterprise Linux ホストで利用できます。Cockpit の Web インターフェイスには、ブラウザーにアドレスを入力するか、管理ポータルからアクセスできます。

## 手順

1. 管理ポータルで Compute → Hosts をクリックし、ホストを選択します。
2. Host Console をクリックします。

Cockpit のログインページが新しいブラウザーウィンドウで開きます。

### 2.5.5.9.1. レガシー SPICE 暗号の設定

SPICE コンソールでは、デフォルトで FIPS 準拠の暗号化を行い、暗号文字列を使用します。デフォルトの SPICE 暗号文字列は **kECDHE+FIPS:kDHE+FIPS:kRSA+FIPS:!eNULL:!aNULL** です。

通常、この文字列で十分です。ただし、古いオペレーティングシステムまたは SPICE クライアントの仮想マシンがあり、そのうちのいずれかが FIPS 準拠の暗号化に対応していない場合は、弱い暗号文字列を使用する必要があります。そうしないと、新規クラスターまたは新規ホストを既存のクラスターにインストールし、その仮想マシンへの接続を試みると、接続のセキュリティーエラーが発生します。

Ansible Playbook を使用して暗号文字列を変更できます。

#### 暗号文字列の変更

1. Manager マシンで、**/usr/share/ovirt-engine/playbooks** ディレクトリーにファイルを作成します。以下に例を示します。

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

2. ファイルに以下を入力し、保存します。

```
name: oVirt - setup weaker SPICE encryption for old clients
hosts: hostname
vars:
```

```

host_deploy_spice_cipher_string: 'DEFAULT:-RC4:-3DES:-DES'
roles:
 - ovirt-host-deploy-spice-encryption

```

3. 作成したファイルを実行します。

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

または、変数 **host\_deploy\_spice\_cipher\_string** で **--extra-vars** オプションを使用して、Ansible Playbook **ovirt-host-deploy** でホストを再設定することもできます。

```

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

```

#### 2.5.5.10. ホストの電源管理の設定

管理ポータルからホストのライフサイクル操作(停止、開始、再起動)を行うために、ホストの電源管理デバイスを設定します。

ホストの高可用性や仮想マシンの高可用性を利用するためには、ホストの電源管理を設定する必要があります。電源管理デバイスの詳細は、テクニカルリファレンスの [電源管理](#) を参照してください。

#### 手順

1. **Compute** → **Hosts** をクリックし、ホストを選択します。
2. **Management** → **Maintenance** をクリックし、**OK** をクリックして確定します。
3. ホストがメンテナンスマードになったら、**Remove** をクリックします。
4. **Power Management** タブをクリックします。
5. **Enable Power Management** チェックボックスを選択し、フィールドを有効にします。
6. **Kdump integration** チェックボックスを選択すると、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するのを防ぐことができます。



#### 重要

既存のホストで **Kdump integration** を有効または無効にした場合、kdump を設定するには [ホストを再インストール](#) する必要があります。

7. オプションとして、ホストの電源管理をホストの **クラスターのスケジューリングポリシー** で制御たくない場合は、**Disable policy control of power management** チェックボックスを選択します。
8. プラス (+) ボタンをクリックして、新しい電源管理デバイスを追加します。**Edit fence agent** ウィンドウが開きます。
9. 電源管理デバイスの **User Name** と **Password** を適切なフィールドに入力します。
10. ドロップダウンリストから電源管理デバイスの **Type** を選択します。

11. **Address** フィールドに IP アドレスを入力します。
12. 電源管理デバイスがホストとの通信に使用する **SSH Port** の番号を入力します。
13. 電源管理デバイスのブレードを識別するための **Slot** 番号を入力します。
14. 電源管理デバイスの **Options** を入力します。key=value ペアのコンマ区切りリストを使用します。
  - IPv4 と IPv6 の両方の IP アドレスを使用できる場合 (デフォルト) は、**Options** フィールドを空白にします。
  - IPv4 の IP アドレスのみを使用する場合は、**inet4\_only=1** を入力します。
  - IPv6 の IP アドレスのみを使用する場合は、**inet6\_only=1** を入力します。
15. 電源管理デバイスがホストに安全に接続できるようにするには、**Secure** チェックボックスを選択します。
16. **Test** をクリックして、設定が正しいことを確認します。検証に成功すると **Test Succeeded, Host Status is: on** と表示されます。
17. **OK** をクリックして、**Edit fence agent** ウィンドウを閉じます。
18. **Power Management** タブで、オプションで **Advanced Parameters** を展開し、上下のボタンを使用して、Manager がホストの クラスターと DC (データセンター) でフェンシングプロキシーを検索する順序を指定します。
19. **OK** をクリックします。



### 注記

- IPv6 の場合、Red Hat Virtualization でサポートされるのは静的アドレスのみです。
- IPv4 と IPv6 のデュアルスタックアドレッシングはサポートされていません。

**Management** → **Power Management** ドロップダウンメニューは、管理者ポータルで有効化されています。

#### 2.5.5.11. ホストの Storage Pool Manager の設定

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

ホストの SPM (Storage Pool Manager) 優先度の設定により、ホストに SPM ロールが割り当てられる可能性があります。SPM 優先度が高いホストには、SPM の優先度が低いホストよりも先に SPM ロールが割り当てられます。

### 手順

1. **Compute** → **Hosts** をクリックします。

2. **Edit** をクリックします。
3. **SPM** タブをクリックします。
4. ラジオボタンで、ホストに適した SPM の優先順位を選択します。
5. **OK** をクリックします。

#### 2.5.5.11.1. セルフホスト型エンジンホストの別のクラスターへの移行

セルフホスト型エンジンホストとして設定されているホストを、セルフホスト型エンジンの仮想マシンが稼働しているデータセンターやクラスター以外のデータセンターやクラスターに移行することはできません。すべてのセルフホスト型エンジンのホストは、同じデータセンターとクラスター内にある必要があります。

ホストからセルフホスト型エンジン設定をアンデプロイすることで、ホストをセルフホスト型エンジンのホストとして無効にする必要があります。

#### 手順

1. **Compute** → **Hosts** をクリックし、ホストを選択します。
2. **Management** → **Maintenance** をクリックします。ホストのステータスが **Maintenance** に変わります。
3. **Reinstall** で、**Hosted Engine UNDEPLOY** を選択します。
4. **Reinstall** をクリックします。

#### ヒント

また、REST API の **undeploy\_hosted\_engine** パラメーターを使用することもできます。

5. **Edit** をクリックします。
6. 対象となるデータセンターとクラスターを選択します。
7. **OK** をクリックします。
8. **Management** → **Activate** をクリックします。

#### 関連情報

- ホストのメンテナンスマードへの切り替え
- メンテナンスマードのホストのアクティビ化

#### 2.5.6. New Host および Edit Host ウィンドウの設定とコントロールの説明

##### 2.5.6.1. ホストの一般設定の説明

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

General 設定の表には、New Host または Edit Host ウィンドウの General タブで必要な情報が含まれています。

表2.20 General 設定

フィールド名	説明
Host Cluster	ホストが属するクラスターとデータセンター。
Use Foreman/Satellite	このチェックボックスを選択またはクリアすると、Satellite ホストプロバイダーが提供するホストを追加するためのオプションが表示または非表示になります。以下のオプションを利用できます。
	<p><b>Discovered Hosts</b></p> <ul style="list-style-type: none"> <li>● <b>Discovered Hosts</b> - エンジンによって発見された Satellite ホストの名前が入力されたドロップダウンリスト。</li> <li>● <b>Host Groups</b> - 利用可能なホストグループのドロップダウンリスト。</li> <li>● <b>Compute Resources</b> - コンピュートリソースを提供するハイパーバイザのドロップダウンリスト。</li> </ul> <p><b>Provisioned Hosts</b></p> <ul style="list-style-type: none"> <li>● <b>Providers Hosts</b> - 選択された外部プロバイダーが提供するホストの名前が表示されるドロップダウンリスト。このリストのエンターは、<b>Provider search filter</b> に入力された検索クエリーに応じてフィルタリングされます。</li> <li>● <b>Provider search filter</b> - 選択された外部プロバイダーが提供するホストを検索するためのテキストフィールド。プロバイダー固有のオプションです。特定プロバイダーの検索クエリーを作成する際の詳細は、プロバイダーのドキュメントを参照してください。利用可能なすべてのホストを表示するには、このフィールドを空白にします。</li> </ul>
Name	ホストの名前。このテキストフィールドには 40 文字の制限があり、大文字、小文字、数字、ハイフン、およびアンダースコアの組み合わせが含まれる一意の名前である必要があります。
Comment	ホストに関するプレーンテキストで人間が判読できる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
ホスト名	ホストの IP アドレスまたは解決可能なホスト名。解決可能なホスト名を使用する場合は、ホスト名が解決されたすべてのアドレスが、ホストの管理ネットワークで使用されている IP アドレス (IPv4 および IPv6) と一致していることを確認する必要があります。
Password	ホストの root ユーザーのパスワード。ホストの追加時にパスワードを設定します。パスワードを後から編集することはできません。
Activate host after install	<p>インストールが成功した後、ホストをアクティブにするには、このチェックボックスを選択します。これはデフォルトで有効になっており、ハイパーバイザーを正常にアクティブ化するために必要です。</p> <p>インストールに成功した後、このチェックボックスをクリアすると、ホストの状態がメンテナンスに切り替わります。これにより、管理者はハイパーバイザー上で追加の設定作業を行うことができます。</p>
Reboot host after install	このチェックボックスを選択すると、インストール後にホストを再起動します。これはデフォルトで有効になっています。
SSH Public Key	 <p>注記</p> <p>また、ホストのカーネルコマンドラインパラメーターの変更や、クラスターのファイアウォールタイプの変更には、ホストの再起動が必要です。</p>
Automatically configure host firewall	新しいホストを追加する際に、Manager はホストのファイアウォールで必要なポートを開くことができます。これはデフォルトで有効になっています。これは Advanced Parameter です。
SSH Fingerprint	ホストの SSH フィンガープリントを取得し、ホストが返すと予想されるフィンガープリントと比較して、両者が一致することを確認できます。これは Advanced Parameter です。

## 2.5.6.2. ホストの Power Management 設定の説明

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

表2.21 Power Management 設定

フィールド名	説明
<b>Enable Power Management</b>	ホストの電源管理を有効にします。このチェックボックスを選択すると、 <b>Power Management</b> タブの残りのフィールドが有効になります。
<b>Kdump integration</b>	カーネルのクラッシュダンプの実行中にホストがフェンシングするのを防ぎ、クラッシュダンプが中断されないようにします。Red Hat Enterprise Linux 7.1以降では、デフォルトで kdump が利用できます。kdump がホスト上で利用可能であっても、その設定が有効でない (kdump サービスが開始できない) 場合、 <b>Kdump integration</b> を有効にすると、ホストの(再)インストールが失敗します。既存のホストで <b>Kdump integration</b> を有効または無効にした場合、 <a href="#">ホストを再インストール</a> する必要があります。
<b>Disable policy control of power management</b>	電源管理は、ホストの <b>クラスターのスケジューリングポリシー</b> によって制御されます。電源管理が有効で、定義された低使用率の値に達した場合、マネージャーはホストマシンをパワーダウンさせ、ロードバランスが必要な場合や、クラスター内に十分な空きホストがない場合には、再びホストマシンを再起動させます。ポリシーコントロールを無効にする場合は、このチェックボックスを選択します。

フィールド名	説明
Agents by Sequential Order	<p>ホストのフェンスエージェントを一覧表示します。フェンスエージェントには、シーケンシャル(順次使用)、コンカレント(同時使用)、またはその両方の組み合わせがあります。</p> <ul style="list-style-type: none"> <li>フェンスエージェントが順次使用される場合、ホストの停止または起動にはまずプライマリーエージェントが使用され、それが失敗した場合にはセカンダリーエージェントが使用されます。</li> <li>フェンスエージェントを同時に使用する場合、両方のフェンスエージェントが Stop コマンドに反応しなければホストは停止しませんが、一方のエージェントが Start コマンドに反応すればホストは起動します。</li> </ul> <p>フェンスエージェントはデフォルトではシーケンシャルです。上下のボタンでフェンスエージェントの使用順序を変更できます。</p> <p>2つのフェンスエージェントをコンカレントにするには、一方のフェンスエージェントをもう一方のフェンスエージェントの隣にある <b>Concurrent with</b> ドロップダウンリストから選択します。コンカレントフェンスエージェントのグループに別のフェンスエージェントを追加するには、追加するフェンスエージェントの横にある <b>Concurrent with</b> ドロップダウンリストからグループを選択します。</p>
Add Fence Agent	+ ボタンをクリックして、新しい接続を追加します。Edit fence agent ウィンドウが開きます。このウィンドウのフィールドの詳細は、以下の表を参照してください。
Power Management Proxy Preference	デフォルトでは、Manager がホストと同じ クラスター内のフェンシングプロキシーを検索し、フェンシングプロキシーが見つからない場合は、同じ DC(データセンター) 内を検索するよう指定されます。上下のボタンで、これらのリソースの使用順序を変更できます。このフィールドは、Advanced Parameters で利用できます。

次の表は、Edit fence agent ウィンドウで必要な情報です。

表2.22 Edit fence agent の設定

フィールド名	説明
Address	ホストの電源管理デバイスにアクセスするためのアドレス。解決可能なホスト名または IP アドレスのいずれか。

フィールド名	説明
User Name	電源管理デバイスにアクセスするユーザー アカウント。デバイスにユーザーを設定するか、デフォルトのユーザーを使用します。
Password	電源管理デバイスにアクセスするユーザーのパスワード。
Type	<p>ホストの電源管理デバイスのタイプ。以下のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>● <b>apc</b> - 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では使用しないでください。</li> <li>● <b>apc_snmp</b> - APC 5.x 電源スイッチデバイスでは使用しないでください。</li> <li>● <b>bladecenter</b> - IBM BladeCenter リモートスーパーバイザアダプター。</li> <li>● <b>cisco_ucs</b> - Cisco Unified Computing System.</li> <li>● <b>drac5</b> - Dell コンピューター用の Dell Remote Access Controller。</li> <li>● <b>drac7</b> - Dell コンピューター用の Dell Remote Access Controller。</li> <li>● <b>eps</b> - ePower Switch 8M+ ネットワークパワースイッチ。</li> <li>● <b>hpblade</b> - HP BladeSystem.</li> <li>● <b>ILO</b>、<b>ILO2</b>、<b>ILO3</b>、<b>ILO4</b> - HP Integrated Lights-Out。</li> <li>● <b>ipmilan</b> - Intelligent Platform Management Interface と Sun Integrated Lights Out Management デバイス。</li> <li>● <b>rsa</b> - IBM リモートスーパーバイザアダプター。</li> <li>● <b>rsb</b> - 富士通シーメンスの RSB 管理インターフェイス。</li> <li>● <b>wti</b> - WTI ネットワークパワースイッチ。</li> </ul> <p>電源管理デバイスの詳細は、<a href="#">テクニカルリファレンス</a>の<a href="#">電源管理</a>を参照してください。</p>
Port	電源管理デバイスがホストとの通信に使用するポート番号。
Slot	電源管理デバイスのブレードを識別するための番号。

フィールド名	説明
Service Profile	電源管理デバイスのブレードを識別するために使用されるサービスプロファイル名。デバイスタイプが <b>cisco_ucs</b> の場合、Slot の代わりにこのフィールドが表示されます。
Options	電源管理デバイス固有のオプション。これらを 'key=value' として入力します。利用可能なオプションについては、お使いのホストの電源管理デバイスのドキュメントを参照してください。  Red Hat Enterprise Linux 7 ホストで、電源管理デバイスとして cisco_ucs を使用している場合は、Options フィールドに <b>ssl_insecure=1</b> を追加する必要があります。
Secure	電源管理デバイスがホストに安全に接続できるようにするには、このチェックボックスを選択します。これは、電源管理エージェントに応じて、ssh、ssl、または他の認証プロトコルを介して行うことができます。

### 2.5.6.3. SPM Priority 設定の説明

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

表2.23 SPM の設定

フィールド名	説明
SPM Priority	ホストに Storage Pool Manager (SPM) のロールが与えられる可能性を定義します。オプションは、Low、Normal、High の 3 つです。優先度が低いと、ホストに SPM のロールが割り当てられる可能性が低いことを意味し、優先度が高いと、その可能性が高いことを意味します。デフォルト設定は Normal です。

### 2.5.6.4. ホストの Console 設定の説明

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

表2.24 Console の設定

フィールド名	説明
Override display address	ホストの表示アドレスを上書きする場合は、このチェックボックスを選択します。この機能は、ホストが内部 IP で定義されており、NAT ファイアウォールの内側にある場合に有効です。ユーザーが内部ネットワークの外から仮想マシンに接続した場合、仮想マシンが動作しているホストのプライベートアドレスを返すのではなく、パブリック IP または FQDN (外部ネットワークではパブリック IP に解決される) を返します。
Display address	ここで指定した表示アドレスは、このホスト上で動作するすべての仮想マシンに使用されます。アドレスは、完全修飾ドメイン名または IP の形式でなければなりません。
vGPU Placement	<p>優先される vGPU 配置を指定します。</p> <ul style="list-style-type: none"> <li>● <b>Consolidated</b> - 利用可能な物理カードで vGPU をさらに実行する場合は、このオプションを選択します。</li> <li>● <b>Separated</b> - 各仮想 GPU を別の物理カードで実行する場合は、このオプションを選択します。</li> </ul>

### 2.5.6.5. Network Provider 設定の説明

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

表2.25 Network Provider 設定

フィールド名	説明
External Network Provider	外部ネットワークプロバイダーを追加し、ホストのネットワークをその外部ネットワークプロバイダーを使用してプロビジョニングする場合は、リストから選択します。

### 2.5.6.6. Kernel 設定の説明

Kernel 設定の表には、New Host または Edit Host ウィンドウの Kernel タブに必要な情報の詳細が記載されています。一般的なカーネルブートパラメーターのオプションはチェックボックスで表示されるため、簡単に選択できます。

より複雑な変更を行う場合は、Kernel command line の横にあるフリーテキスト入力フィールドを使用して、必要な追加パラメーターを追加します。カーネルのコマンドラインパラメーターを変更した場合は、[ホストを再インストール](#) する必要があります。



## 重要

ホストが Manager に接続されている場合、変更する前にホストをメンテナンスマードにする必要があります。変更後に、[ホストを再インストールして](#) 変更を適用します。

表2.26 Kernel 設定

フィールド名	説明
Hostdev Passthrough & SR-IOV	カーネルの IOMMU フラグを有効にすることで、仮想マシンがホストデバイスを仮想マシンに直接接続されているかのように使用できるようになります。また、ホストのハードウェアとファームウェアも IOMMU に対応している必要があります。ハードウェア上で仮想化拡張機能と IOMMU 拡張機能が有効になっている必要があります。 <a href="#">PCI パススルー用ホストの設定</a> を参照してください。IBM POWER8 では、デフォルトで IOMMU が有効になっています。
Nested Virtualization	<b>vmx</b> または <b>svm</b> フラグを有効にして、仮想マシンが仮想マシン内で実行できるようにします。このオプションは、テクノロジープレビュー機能です。評価目的でのみご利用いただけます。これは実稼働環境ではサポートされません。この設定を使用するには、ホストに <b>vdsmd-hook-nestedvt</b> フックをインストールする必要があります。詳細は、 <a href="#">すべての仮想マシンでネストされた仮想化を有効化</a> および <a href="#">個々の仮想マシンでネストされた仮想化を有効化</a> を参照してください。
Unsafe Interrupts	IOMMU が有効になっているが、ハードウェアが割り込みの再マッピングをサポートしていないためにパススルーが失敗する場合は、このオプションを有効にすることを検討してください。このオプションは、ホスト上の仮想マシンが信頼できる場合にのみ有効にしてください。このオプションを有効にすると、仮想マシンからの MSI 攻撃を受ける可能性があります。このオプションは、評価目的で認定されていないハードウェアを使用する場合に限定して、回避策として使用することを目的としています。
PCI Reallocation	メモリーの問題で SR-IOV NIC が仮想機能を割り当てられない場合は、このオプションを有効にすることを検討してください。また、ホストのハードウェアとファームウェアが PCI の再配置をサポートしている必要があります。このオプションは、評価目的で認定されていないハードウェアを使用する場合に限定して、回避策として使用することを目的としています。

フィールド名	説明
Blacklist Nouveau	nouveau ドライバーをブロックします。nouveau は、NVIDIA GPU 用のコミュニティードライバーで、ベンダーが提供するドライバーと競合します。ベンダードライバーが優先される場合は、nouveau ドライバーをブロックする必要があります。
SMT Disabled	同時マルチスレッド (SMT) を無効にします。SMT を無効にすると、L1TF や MDS などのセキュリティー脆弱性を軽減できます。
FIPS mode	FIPS モードを有効にします。詳細は、 <a href="#">マネージャーを使用した FIPS の有効化</a> を参照してください。
Kernel command line	このフィールドでは、デフォルトのパラメーターにさらにカーネルパラメーターを追加することができます。



### 注記

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

#### 2.5.6.7. Host Engine 設定の説明

Hosted Engine 設定の表は、New Host または Edit Host ウィンドウの Hosted Engine タブで必要な情報の詳細を示します。

表2.27 Hosted Engine 設定

フィールド名	説明
Choose hosted engine deployment action	<p>利用可能な 3 つのオプションは以下のとおりです。</p> <ul style="list-style-type: none"> <li>● <b>None</b> - 必要なアクションはありません。</li> <li>● <b>Deploy</b> - ホストをセルフホスト型のエンジンノードとしてデプロイする場合は、このオプションを選択します。</li> <li>● <b>Undeploy</b> - セルフホスト型エンジンノードの場合、このオプションを選択すると、ホストがアンデプロイされ、セルフホスト型エンジン関連の設定が削除されます。</li> </ul>

#### 2.5.7. ホストの耐障害性

##### 2.5.7.1. 高可用性

Red Hat Virtualization Manager は、クラスター内のホストの応答性を維持するためにフェンシングを使用します。Non Responsive ホストは、Non Operational ホストとは異なります。Non Operational ホストは、Manager から通信可能ですが、論理ネットワークがないなど、設定が正しくない場合があります。Non Responsive ホストは、Manager から通信できません。

フェンシングにより、クラスターは予期せぬホストの障害に対応し、省電力、ロードバランシング、仮想マシンの可用性のポリシーを適用できます。ホストの電源管理デバイスにフェンシングのパラメーターを設定し、時々その正確性をテストする必要があります。フェンシング操作では、応答のないホストが再起動されます。所定の時間内にアクティブな状態に戻らない場合は、手動での介入やトラブルシューティングが行われるまで、応答しない状態が続きます。



### 注記

フェンシングパラメーターを自動的にチェックするには、**PMHealthCheckEnabled** (デフォルトでは false) と **PMHealthCheckIntervalInSec** (デフォルトでは 3600 秒) の engine-config オプションを設定できます。

#### **PMHealthCheckEnabled** が true に設定されている場合

は、**PMHealthCheckIntervalInSec** で指定された間隔で全てのホストエージェントをチェックし、問題を検出した場合は警告を発します。engine-config オプションの設定に関する詳細は、[engine-config コマンドの構文](#) を参照してください。

電源管理操作は、Red Hat Virtualization Manager が再起動した後、プロキシホストによって、または管理ポータルで手動で実行できます。応答のないホスト上で稼働しているすべての仮想マシンを停止し、高可用性を持つ仮想マシンを別のホスト上で起動します。電源管理操作には、少なくとも 2 台のホストが必要です。

Manager の起動後、電源管理が有効になっている応答のないホストに対して、待機時間 (デフォルトでは 5 分) が経過した後、自動的にフェンスを試みます。**DisableFenceAtStartupInSec** エンジン設定オプションを更新することで、待機時間を設定できます。



### 注記

**DisableFenceAtStartupInSec** engine-config オプションは、ホストの起動時に Manager がフェンスを試みてしまうシナリオを防ぐのに役立ちます。通常、ホストのブートプロセスは Manager のブートプロセスよりも長いため、データセンターが停止した後にこのような事態が発生する可能性があります。

ホストのフェンスは、プロキシホストが電源管理パラメーターを使って自動的に実行するか、ホストを右クリックしてメニューのオプションを使って手動で実行できます。



### 重要

ホストが高可用性を持つ仮想マシンを実行する場合、パワーマネージメントを有効にして設定する必要があります。

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

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

以下のいずれかを選択できます。

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

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

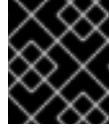
### 2.5.7.3. ホストでのフェンシングパラメーターの設定

ホストフェンシングのパラメーターは、**New Host** または **Edit Host** ウィンドウの **Power Management** フィールドで設定します。電源管理を行うことで、RAC (Remote Access Card) などの追加インターフェイスを使って、システムがトラブルのあるホストをフェンスできます。

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

#### 手順

1. **Compute** → **Hosts** をクリックし、ホストを選択します。
2. **Edit** をクリックします。
3. **Power Management** タブをクリックします。
4. **Enable Power Management** 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 integration** チェックボックスを選択すると、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するのを防ぐことができます。



#### 重要

既存のホストで **Kdump integration** を有効または無効にした場合、[ホストを再インストール](#) する必要があります。

6. オプション: ホストの電源管理をホストのクラスターの **スケジューリングポリシー** で制御しない場合は、**Disable policy control of power management** チェックボックスを選択します。
7. + ボタンをクリックして、新しい電源管理デバイスを追加します。**Edit fence agent** ウィンドウが開きます。
8. 電源管理デバイスの **Address**、**User Name**、**Password** 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 **Type** 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 Port** の番号を入力します。
11. 電源管理デバイスのブレードを識別するための **Slot** 番号を入力します。
12. 電源管理デバイスの **Options** を入力します。**key=value** ペアのコンマ区切りリストを使用します。
13. 電源管理デバイスがホストに安全に接続できるようにするには、**Secure** チェックボックスを選択します。
14. **Test** ボタンをクリックして、設定が正しいことを確認します。検証に成功すると **Test Succeeded, Host Status is: on** と表示されます。



## 警告

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

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

ホストのリストに戻ります。ホスト名の横にあった感嘆符が消えていることに注意してください。これは、電源管理の設定に成功したことを示しています。

### 2.5.7.4. fence\_kdump の高度な設定

#### kdump

ホスト名をクリックすると、詳細表示の General タブに kdump サービスの状態が表示されます。

- **Enabled:** kdump が正しく設定され、kdump サービスが実行されています。
- **Disable:** kdump サービスは実行されていません(この場合、kdump の統合は正しく動作しません)。
- **Unknown:** kdump の状態を報告しない以前の VDSM のバージョンを持つホストでのみ発生します。

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

#### fence\_kdump

New Host または Edit Host ウィンドウの Power Management タブで Kdump の統合 を有効にすると、標準的な fence\_kdump の設定が行われます。環境のネットワーク設定が単純で、Manager の FQDN がすべてのホストで解決可能な場合は、デフォルトの fence\_kdump 設定を使用できます。

ただし、fence\_kdump の高度な設定が必要な場合もあります。ネットワークが複雑な環境では、Manager、fence\_kdump リスナー、またはその両方の設定を手動で変更する必要がある場合があります。例えば、Kdump integration が有効になっているすべてのホストで Manager の FQDN が解決できない場合、engine-config を使って適切なホスト名や 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
```

以下の例の場合も、設定変更が必要な場合があります。

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

デフォルトの設定を変更する必要があるのは、より複雑なネットワーク設定の場合に限られるため、カスタマイズされた fence\_kdump 検出設定は、上級ユーザーのみに推奨されます。

#### 2.5.7.5. fence\_kdump リスナーの設定

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

##### 手順

- etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/ に新しいファイル(例えば、my-fence-kdump.conf)を作成します。
- カスタマイズした内容を `OPTION=value` の構文で入力し、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](#) の表で説明されているように、[engine-config](#) で変更する必要があります。

- fence\_kdump リスナーを再起動します。

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

以下のオプションは、必要に応じてカスタマイズすることができます。

表2.28 追加のリスナー設定オプション

変数	説明	デフォルト	注記
LISTENER_ADDRESS	fence_kdump メッセージを受信するための IP アドレスを定義します。	0.0.0.0	このパラメーターの値を変更する場合は、 <a href="#">engine-config</a> の <b>FenceKdumpDestinationAddress</b> の値と一致させる必要があります。
LISTENER_PORT	fence_kdump メッセージを受信するポートを定義します。	7410	このパラメーターの値を変更する場合は、 <a href="#">engine-config</a> の <b>FenceKdumpDestinationPort</b> の値と一致させる必要があります。

変数	説明	デフォルト	注記
HEARTBEAT_INTERVAL	リスナーのハートビート更新の間隔を秒単位で定義します。	30	このパラメーターの値を変更する場合は、 <b>engine-config</b> の <b>FenceKdumpListenेrTimeout</b> の値の半分以下にしなければなりません。
SESSION_SYNC_INTERVAL	リスナーのメモリー上のホストの kdumping セッションをデータベースに同期させる間隔を秒単位で定義します。	5	このパラメーターの値を変更する場合は、 <b>engine-config</b> の <b>KdumpStartedTimеout</b> の値の半分以下にしなければなりません。
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	kdumpping ホストからのメッセージを最後に受信してから、ホストの kdump フローが FINISHED とマークされるまでの最大タイムアウトを秒単位で定義します。	60	このパラメーターの値を変更する場合は、 <b>engine-config</b> の <b>FenceKdumpMessageInterval</b> 値の 2 倍以上でなければなりません。

### 2.5.7.6. Manager での fence\_kdump の設定

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

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

#### 手順

1. **engine-config** コマンドで kdump の設定を編集します。

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



#### 重要

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

2. **ovirt-engine** サービスを再起動します。

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

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

**engine-config** では以下のオプションが設定できます。

表2.29 Kdump 設定オプション

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

変数	説明	デフォルト	注記
FenceKdumpListenerTimout	最後のハートビート以降、fence_kdump リスナーが有効であると見なす最大タイムアウトを秒単位で定義します。	90	このパラメーターの値を変更する場合は、fence_kdump リスナー設定ファイルの <b>HEARTBEAT_INTERVAL</b> の値の 2 倍以上でなければなりません。
KdumpStartedTimeout	kdumping ホストからの最初のメッセージを受信するまで(ホストの kdump フローが開始されたことを検出するまで)の最大タイムアウトを秒単位で定義します。	30	このパラメーターの値を変更する場合は、fence_kdump リスナー設定ファイルの <b>SESSION_SYNC_INTERVAL</b> および <b>FenceKdumpMessageInterval</b> 値の 2 倍以上でなければなりません。

### 2.5.7.7. ソフトフェンシングホスト

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

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

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

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



## 注記

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

### 2.5.7.8. ホストの電源管理機能の利用

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

#### 手順

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



## 注記

電源管理が有効になっていない場合は、Management ドロップダウンメニューをクリックし、SSH Management オプションで Restart または Stop を選択することで、ホストを再起動または停止できます。



## 重要

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

3. OK をクリックします。

#### 関連情報

- [統合フェンスデバイスで使用する ACPI の設定](#)

### 2.5.7.9. 応答しないホストを手動でフェンシングまたは隔離する方法

ハードウェアの故障などにより、ホストが予期せず非応答状態になると、環境のパフォーマンスに大きな影響を与えます。電源管理デバイスがない場合や、設定が間違っている場合は、手動でホストを再起動することができます。



#### 警告

ホストを手動で再起動した場合を除き、**Confirm 'Host has been Rebooted'**は選択しないでください。ホストの実行中にこのオプションを使用すると、仮想マシンのイメージが破損する可能性があります。

#### 手順

1. 管理ポータルで **Compute → Hosts** をクリックし、ホストのステータスが **Non Responsive** になっていることを確認します。
2. システムを手動で再起動します。これは物理的にラボに入り、ホストを再起動することを意味します。
3. 管理ポータルでホストを選択し、**More Actions (■)** をクリックしてから、**Confirm 'Host has been Rebooted'** をクリックします。
4. **Approve Operation** チェックボックスを選択し、**OK** をクリックします。
5. ホストの起動に異常に長い時間がかかる場合は、**ServerRebootTimeout** を設定して、ホストが **Non Responsive** と判断するまで待機する秒数を指定できます。

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

## 2.6. ストレージ

### 2.6.1. Red Hat Virtualization ストレージについて

Red Hat Virtualization では、仮想ディスク、ISO ファイル、スナップショットのための集中型ストレージシステムを使用しています。ストレージネットワーキングは、以下を使用して実装できます。

- Network File System (NFS)
- その他 POSIX 準拠ファイルシステム
- Internet Small Computer System Interface (iSCSI)
- 仮想化ホストに直接接続されたローカルストレージ
- ファイバーチャネルプロトコル (FCP)
- Parallel NFS (pNFS)

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

Red Hat Virtualization システム管理者は、仮想化されたエンタープライズ用のストレージを作成、設定、接続、および維持します。そのためには、ストレージの種類と使い方に対する理解が必要です。ストレージの概念、プロトコル、要件、および一般的な使用方法の詳細は、ストレージアレイベンダーのガイドと、[Red Hat Enterprise Linux ストレージデバイスの管理](#) を参照してください。

ストレージドメインを追加するには、管理ポータルに正常にアクセスできなければなりません。また、Up のステータスで接続されているホストが少なくとも1台必要です。

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

- **Data Domain:** データドメインは、データセンター内のすべての仮想マシンとテンプレートの仮想ハードディスクおよび OVF ファイルを保持します。さらに、仮想マシンのスナップショットもデータドメインに保存されます。  
データドメインは、データセンター間で共有することはできません。複数のタイプ (iSCSI、NFS、FC、POSIX、および Gluster) のデータドメインは、ローカルドメインではなくすべて共有されていることを条件として、同じデータセンターに追加できます。
- **ISO Domain:** ISO ドメインは、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される ISO ファイル (または論理 CD) を格納します。ISO ドメインを使用することで、データセンターは物理的なメディアを必要としなくなります。ISO ドメインは、異なるデータセンターで共有することができます。ISO ドメインは NFS ベースに限定されます。データセンターに1つの ISO ドメインのみをアタッチできます。
- **Export Domain:** エクスポートドメインは、データセンターと Red Hat Virtualization 環境の間でイメージをコピーおよび移動するために使用される一時的なストレージリポジトリです。エクスポートドメインは、仮想マシンのバックアップに使用できます。エクスポートドメインは、データセンター間で移動できますが、同時に1つのデータセンターでしか有効にすることできません。エクスポートドメインは、NFS ベースに限定されます。データセンターに追加できるエクスポートドメインは1つだけです。



### 注記

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



### 重要

Red Hat Virtualization 環境へのストレージの設定と接続は、データセンターにおけるストレージの必要性が明確になってから開始してください。

## 2.6.2. ストレージドメインについて

ストレージドメインとは、共通のストレージインターフェイスを持つイメージの集合体です。ストレージドメインには、テンプレートや仮想マシンの完全なイメージ (スナップショットを含む)、または ISO ファイルが格納されています。ストレージドメインは、ブロックデバイス (SAN - iSCSI または FCP) ま

たはファイルシステム (NAS - NFS、GlusterFS、またはその他の POSIX 準拠ファイルシステム) で構成できます。

デフォルトでは、GlusterFS ドメインとローカルストレージドメインは 4K ブロックサイズをサポートします。4K ブロックサイズを使用すると、特に大きなファイルを使用する場合などに、パフォーマンスが向上します。また、VDO などの 4K 互換性を必要とするツールを使用する場合にも必要です。



## 注記

GlusterFS Storage は非推奨になり、将来のリリースではサポートされなくなります。

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

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

仮想ディスクの形式は、QCOW2 または raw のいずれかになります。ストレージのタイプは、スパースまたは事前割り当て型のいずれかになります。スナップショットは常にスパースですが、どちらの形式のディスクでも取得できます。

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

### 2.6.3. NFS ストレージの準備と追加

#### 2.6.3.1. NFS ストレージの準備

ファイルストレージまたはリモートサーバーで NFS 共有を設定し、Red Hat Enterprise Virtualization Host システムのストレージドメインとして機能するようにします。リモートストレージで共有をエクスポートし、Red Hat Virtualization Manager で共有を設定すると、共有は Red Hat Virtualization Host に自動的にインポートされます。

NFS の準備、設定、マウント、およびエクスポートに関する詳細は、[Red Hat Enterprise Linux 8 のファイルシステムの管理](#) を参照してください。

Red Hat Virtualization には、特定のシステムユーザー アカウントおよびシステムユーザーグループが必要です。これにより、Manager はストレージドメイン (エクスポートしたディレクトリー) にデータを保管することができます。以下の手順では、1つのディレクトリーのパーミッションを設定しています。Red Hat Virtualization のストレージドメインとして使用するすべてのディレクトリーについて、**chown** および **chmod** のステップを繰り返す必要があります。

#### 前提条件

1. NFS **utils** パッケージをインストールする。

```
dnf install nfs-utils -y
```

2. 有効なバージョンを確認するには、以下のコマンドを実行します。

```
cat /proc/fs/nfsd/versions
```

3. 以下のサービスを有効にします。

```
systemctl enable nfs-server
systemctl enable rpcbind
```

## 手順

1. **kvm** グループを作成します。

```
groupadd kvm -g 36
```

2. **kvm** グループに **vdsm** ユーザーを作成します。

```
useradd vdsm -u 36 -g kvm
```

3. **storage** ディレクトリーを作成し、アクセス権を変更します。

```
mkdir /storage
chmod 0755 /storage
chown 36:36 /storage/
```

4. **storage** ディレクトリーを、適切なパーミッションで **/etc(exports** に追加します。

```
vi /etc(exports
cat /etc(exports
/storage *(rw)
```

5. 以下のサービスを再起動します。

```
systemctl restart rpcbind
systemctl restart nfs-server
```

6. 特定の IP アドレスで利用可能なエクスポートを確認するには、以下のコマンドを実行します。

```
exportfs
/nfs_server/srv
10.46.11.3/24
/nfs_server <world>
```



## 注記

サービス起動後に **/etc(exports** を変更した場合は、**exportfs -ra** コマンドを使用してその変更を再読み込みできます。上記のすべての手順を実行すると、**exports** ディレクトリーの準備が整い、別のホストで利用可能かどうかをテストできます。

### 2.6.3.2. NFS ストレージの追加

ここでは、既存の NFS ストレージをデータ ドメインとして Red Hat Virtualization 環境にアタッチする手順を説明します。

ISO またはエクスポート ドメインが必要な場合も、この手順を使用します。ただし、Domain Function の一覧では ISO または Export を選択します。

## 手順

1. 管理ポータルで **Storage → Domains** をクリックします。
2. **New Domain** をクリックします。
3. ストレージドメインの **Name** を入力します。
4. **Data Center**、**Domain Function**、**Storage Type**、**Format**、および **Host** のリストのデフォルト値をそのまま使用します。
5. ストレージドメインに使用する **Export Path** を入力します。エクスポートパスは、123.123.0.10:/data (IPv4 の場合)、[2001:0:0:0:0:0:5db1]:/data (IPv6 の場合)、または domain.example.com:/data の形式で指定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できます。
  - a. **Advanced Parameters** をクリックします。
  - b. **Warning Low Space Indicator** フィールドに、パーセンテージ値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーに警告メッセージが表示され、ログに記録されます。
  - c. **Critical Space Action Blocker** 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、**Wipe After Delete** チェックボックスを選択します。このオプションは、ドメインの作成後に編集できますが、その場合はすでに存在している wipe after delete プロパティは変更されません。
7. **OK** をクリックします。

新しい NFS データドメインのステータスは、ディスクの準備ができるまで **Locked** になります。その後、データドメインはデータセンターに自動的にアタッチされます。

### 2.6.3.3. NFS ストレージの増設

NFS ストレージの容量を増やすには、新しいストレージドメインを作成して既存のデータセンターに追加するか、NFS サーバーの利用可能な空き容量を増やします。新しく作成する場合の詳細は、[NFS ストレージの追加](#) を参照してください。以下の手順では、既存の NFS サーバーの利用可能な空き容量を増やす方法を説明しています。

#### 手順

1. **Storage → Domains** をクリックします。
2. NFS ストレージドメインの名前をクリックします。詳細ビューが開きます。
3. **Data Center** タブをクリックし、**Maintenance** をクリックして、ストレージドメインをメンテナンスマードにします。これにより、既存の共有がアンマウントされ、ストレージドメインのサイズ変更が可能になります。
4. NFS サーバー上で、ストレージのサイズを変更します。Red Hat Enterprise Linux 6 システムについては、[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 システムについては、[Red Hat Enterprise Linux 7 Storage Administration Guide](#) を参照してください。Red Hat Enterprise Linux 8 システムについては、[パーティションのサイズ変更](#) を参照してください。

- 詳細ビューで、Data Center タブをクリックし、Activate をクリックしてストレージドメインをマウントします。

## 2.6.4. ローカルストレージの準備と追加

仮想マシンのディスクが、仮想マシンのホストに物理的に設置されているストレージデバイスを使用している場合、ローカルストレージデバイスと呼ばれます。

ストレージデバイスは、ストレージドメインの一部である必要があります。ローカルストレージのストレージドメインタイプは、ローカルストレージドメインと呼ばれます。

ローカルストレージを使用するようにホストを設定すると、他のホストが追加できない新しいローカルストレージドメイン、データセンター、およびクラスターが自動的に作成され、そこにホストが追加されます。複数のホストで設定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、スケジューリングできません。

### 2.6.4.1. ローカルストレージの準備

Red Hat Virtualization Host (RHVH) の場合は、必ず / (root) とは異なるファイルシステム上にローカルストレージを定義する必要があります。アップグレード中にデータが失われる可能性を防ぐために、別の論理ボリュームまたはディスクを使用します。

#### Red Hat Enterprise Linux ホストの場合

- ホスト上に、ローカルストレージで使用するディレクトリーを作成します。

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

- vdsd ユーザー (UID 36) および kvm グループ (GID 36) がそのディレクトリーにアクセスして読み取り/書き込みできるように、パーミッションを設定します。

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

#### Red Hat Virtualization ホストの場合

論理ボリュームにローカルストレージを作成します。

- ローカルストレージディレクトリーを作成します。

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

- 新しいローカルストレージをマウントします。

```
mount -a
```

- vdsd ユーザー (UID 36) および kvm グループ (GID 36) がそのディレクトリーにアクセスして読み取り/書き込みできるように、パーミッションを設定します。

```
chown 36:36 /data/rhv-data
chmod 0755 /data/rhv-data
```

### 2.6.4.2. ローカルストレージドメインの追加

ローカルストレージドメインをホストに追加する際、ローカルストレージディレクトリーへのパスを設定すると、自動的にローカルデータセンター、ローカルクラスター、ローカルストレージドメインが作成され、ホストが配置されます。

#### 手順

1. Compute → Hosts をクリックし、ホストを選択します。
2. Management → Maintenance をクリックしてから **OK** をクリックします。ホストのステータスが Maintenance に変わります。
3. Management → Configure Local Storage をクリックします。
4. Data Center、Cluster、および Storage フィールドの横にある Edit ボタンをクリックし、ローカルのストレージドメインを設定して名前を付けます。
5. 文字入力フィールドにローカルストレージへのパスを設定します。
6. 該当する場合は、Optimization タブをクリックして新規ローカルストレージクラスターのメモリー最適化ポリシーを設定します。
7. **OK** をクリックします。

Manager は、ローカルクラスター、ローカルストレージドメインを使用してローカルデータセンターをセットアップします。ホストのステータスも Up に変更します。

#### 検証

1. Storage → Domains をクリックします。
2. 追加したローカルストレージドメインを探します。

ドメインのステータスは Active (  ) である必要があります。また、Storage Type 列の値は Local on Host である必要があります。

これで、新しいローカルストレージドメインにディスクイメージをアップロードできます。

### 2.6.5. POSIX 準拠ファイルシステムストレージの準備

#### 2.6.5.1. POSIX 準拠ファイルシステムストレージの準備

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用してファイルシステムをマウントできます。この機能は、NFS、iSCSI、または FCP 以外を使用してマウントするストレージへのアクセスを可能にすることを目的としています。

Red Hat Virtualization でストレージドメインとして使用する POSIX 準拠のファイルシステムは、Global File System 2 (GFS2) 等のクラスター化したファイルシステムでなければなりません。また、スペ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ため、Red Hat Virtualization との互換性はありません。

POSIX 準拠ファイルシステムストレージの準備および設定に関する情報は、[Red Hat Enterprise Linux Global File System 2](#) を参照してください。



## 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。

### 2.6.5.2. POSIX 準拠ファイルシステムストレージの追加

ここでは、既存の POSIX 準拠ファイルシステムストレージをデータドメインとして Red Hat Virtualization 環境にアタッチする手順を説明します。

#### 手順

1. Storage → Domains をクリックします。
2. New Domain をクリックします。
3. ストレージドメインの Name を入力します。
4. このストレージドメインと関連付ける Data Center を選択します。選択したデータセンターのタイプは、POSIX (POSIX compliant FS) でなければなりません。または、(none) 選択します。
5. Domain Function ドロップダウンリストから Data を選択し、Storage Type ドロップダウンリストから **POSIX compliant FS** を選択します。  
該当する場合は、ドロップダウンメニューから Format を選択します。
6. Host のドロップダウンリストからホストを選択します。
7. 通常は **mount** コマンドで指定するように、POSIX ファイルシステムへの Path を入力します。
8. 通常は -t 引数を使用して **mount** コマンドで指定するように、VFS Type を入力します。有効な VFS タイプの一覧は、**man mount** で確認してください。
9. 通常は **mount** コマンドに -o 引数を指定して指定するように、追加の Mount Options を入力します。このマウントオプションはコンマ区切りリストで提示してください。有効なマウントオプションの一覧は、**man mount** 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できます。
  - a. Advanced Parameters をクリックします。
  - b. Warning Low Space Indicator フィールドに、パーセンテージ値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーに警告メッセージが表示され、ログに記録されます。
  - c. Critical Space Action Blocker フィールドに GB 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、**Wipe After Delete** チェックボックスを選択します。このオプションは、ドメインの作成後に編集できますが、その場合はすでに存在している wipe after delete プロパティーは変更されません。

11. **OK** をクリックします。

## 2.6.6. ブロックストレージの準備と追加

### 2.6.6.1. iSCSI ストレージの準備

Red Hat Virtualization は、LUN で構成されるボリュームグループから作成されるストレージドメインである iSCSI ストレージをサポートします。ボリュームグループおよび LUN は、いずれも同時に複数のストレージドメインにアタッチすることはできません。

iSCSI ストレージのセットアップおよび設定に関する詳細は、Red Hat Enterprise Linux 8 の [ストレージデバイスの管理](#) で、[iSCSI ターゲットの設定](#) を参照してください。



#### 重要

ブロックストレージを使用する際、仮想マシンを Raw デバイスまたは直接 LUN にデプロイし、論理ボリュームマネージャー (LVM) で管理する場合は、フィルターを作成してゲストの論理ボリュームを除外する必要があります。これにより、ホストの起動時にゲストの論理ボリュームがアクティブ化されるのを防ぐことができます。アクティブ化されると、論理ボリュームの内容が古くなり、データ破損が生じる可能性があります。**vdsm-tool config-lvm-filter** コマンドを使用して、LVM のフィルターを作成します。



#### 重要

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



#### 重要

SAN ストレージから起動したホストがストレージへの接続を失うと、ストレージファイルシステムは読み取り専用になり、接続が回復した後もその状態が続きます。

この状態を回避するには、ブート LUN の SAN のルートファイルシステムにドロップインマルチパス設定ファイルを追加し、接続可能な場合にキューに置かれるようにしてください。

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

### 2.6.6.2. iSCSI ストレージの追加

ここでは、既存の iSCSI ストレージをデータドメインとして Red Hat Virtualization 環境にアタッチする手順を説明します。

## 手順

1. Storage → Domains をクリックします。
2. New Domain をクリックします。
3. 新規ストレージドメインの Name を入力します。
4. ドロップダウンリストから Data Center を選択します。
5. Domain Function として Data を、Storage Type として iSCSI を、それぞれ選択します。
6. Host としてアクティブな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、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。したがって、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. Manager は iSCSI ターゲットを LUN に、または LUN を iSCSI ターゲットにマッピングすることができます。New Domain ウィンドウでストレージタイプに iSCSI を選択すると、未使用的 LUN が割り当てられた既知のターゲットが自動的に表示されます。ストレージの追加に使用するターゲットが表示されない場合は、ターゲットの検出機能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は、次の手順に進んでください。
  - a. Discover Targets 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、New Domain ウィンドウに、その環境では未使用的 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

環境外で使用されている LUN も表示されます。

Discover Targets のオプションを使用すると、多数のターゲットの 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。



### 重要

REST API メソッド **discoveriscsi** を使用して、iSCSI ターゲットを検出する場合には、FQDN または IP アドレスを使用できますが、REST API メソッド **iscsilogin** を使用してログインするには、検出された iSCSI ターゲットの詳細を使用する必要があります。詳細は、REST API ガイドの [discoveriscsi](#) を参照してください。

- b. Address フィールドに iSCSI ホストの FQDN または IP アドレスを入力します。
- c. Port フィールドには、ターゲットを参照する際にホストに接続するポートを入力します。デフォルトは **3260** です。
- d. ストレージのセキュリティー保護に CHAP を使用している場合は、User Authentication チェックボックスを選択します。CHAP user name と CHAP password を入力してください。



## 注記

REST API を使用して、特定ホストの iSCSI ターゲットに認証情報を定義することができます。詳細は、[REST API ガイド](#) の [StorageServerConnectionExtensions: add](#) を参照してください。

- e. **Discover** をクリックします。
- f. 検出結果から1つまたは複数のターゲットを選択し、1つのターゲットの場合は **Login** をクリックします。複数のターゲットの場合は **Login All** をクリックします。



## 重要

複数のパスのアクセスが必要な場合は、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必要があります。ストレージドメインを変更してパスを追加する方法は、現在サポートされていません。



## 重要

REST API メソッド **iscsilogin** を使用してログインする場合は、**discoveriscsi** メソッドで検出された iSCSI ターゲットの詳細を使用する必要があります。詳細は、[REST API ガイド](#) の [iscsilogin](#) を参照してください。

- 8. 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。エントリーがデプロイされ、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できます。
  - a. **Advanced Parameters** をクリックします。
  - b. **Warning Low Space Indicator** フィールドに、パーセンテージ値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーに警告メッセージが表示され、ログに記録されます。
  - c. **Critical Space Action Blocker** 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、**Wipe After Delete** チェックボックスを選択します。このオプションは、ドメインの作成後に編集できますが、その場合はすでに存在している wipe after delete プロパティは変更されません。
  - e. **Discard After Delete** のチェックボックスを選択して、削除後に破棄のオプションを有効化します。このオプションは、ドメインの作成後に編集できます。また、このオプションを利用できるのは、ブロックストレージドメインのみです。
- 11. **OK** をクリックします。

同じターゲットに対して複数のストレージ接続パスを設定している場合は、[iSCSI マルチパスの設定](#) に記載されている手順に従い、iSCSI のボンディング設定を完了してください。

現在のストレージネットワークを iSCSI ボンディングに移行するには、[ロジカルネットワークへの iSCSI ボンドの移行](#) を参照してください。

### 2.6.6.3. iSCSI マルチパスの設定

iSCSI マルチパスでは、論理ネットワークと iSCSI ストレージ接続のグループを作成し、管理できます。ホストと iSCSI ストレージの間に複数のネットワークパスがあるので、ネットワークパスの障害によるホストのダウンタイムを防ぎます。

Manager は、iSCSI ボンドの論理ネットワークに割り当てられた NIC または VLAN を使用して、データセンター内の各ホストを各ターゲットに接続します。

複数のターゲットと論理ネットワークを持つ iSCSI ボンドを作成し、冗長性を持たせることができます。

#### 前提条件

- 1つまたは複数の [iSCSI ターゲット](#)
- 以下の要件を満たす1つまたは複数の [論理ネットワーク](#)。
  - [必須](#) または [VM ネットワーク](#) として定義されていない。
  - [ホストインターフェイス](#) に割り当てられている。
  - iSCSI ボンド内の他の論理ネットワークと同じ VLAN およびサブネット内の [スタティック IP アドレス](#) が割り当てられている。



#### 注記

マルチパスはセルフホストエンジンのデプロイメントではサポートされていません。

#### 手順

1. Compute → Data Centers をクリックします。
2. データセンター名をクリックします。詳細ビューが開きます。
3. iSCSI Multipathing タブで Add をクリックします。
4. Add iSCSI Bond ウィンドウで、Name と Description を入力します。
5. Logical Networks から論理ネットワークを、Storage Targets からストレージドメインを選択します。同じターゲットへのすべてのパスを選択する必要があります。
6. OK をクリックします。

データセンター内のホストは、iSCSI ボンドの論理ネットワークを介して iSCSI ターゲットに接続されています。

### 2.6.6.4. ロジカルネットワークを iSCSI ボンドに移行

iSCSI トラフィック用に作成した論理ネットワークがあり、既存の [ネットワークボンド](#) の上に設定されている場合は、中断やダウンタイムなしに同じサブネット上の iSCSI ボンドに移行することができます。

## 手順

1. 現在の論理ネットワークを **Required** ではなくなるように変更します。
  - a. **Compute** → **Clusters** をクリックします。
  - b. クラスターの名前をクリックします。詳細ビューが開きます。
  - c. **Logical Networks** タブで、現在の論理ネットワーク (**net-1**) を選択し、**Manage Networks** をクリックします。
  - d. **Require** チェックボックスをオフにして、**OK** をクリックします。
2. **Required** ではなく、**VM network** でもない新しい論理ネットワークを作成します。
  - a. **Add Network** をクリックします。**New Logical Network** ウィンドウが表示されます。
  - b. **General** タブで、**Name (net-2)** を入力し、**VM network** のチェックボックスをオフにします。
  - c. **Cluster** タブで **Require** のチェックボックスをオフにして **OK** をクリックします。
3. 現在のネットワークボンドを削除し、論理ネットワークを再割り当てます。
  - a. **Compute** → **Hosts** をクリックします。
  - b. ホスト名をクリックします。詳細ビューが開きます。
  - c. **Network Interfaces** タブで **Setup Host Networks** をクリックします。
  - d. **net-1** を右にドラッグすると、割り当てが解除されます。
  - e. 現在のボンドを右にドラッグすると、ボンドが削除されます。
  - f. **net-1** と **net-2** を左にドラッグして、物理インターフェイスに割り当てます。
  - g. **net-2** の鉛筆アイコンをクリックします。**Edit Network** ウィンドウが開きます。
  - h. **IPV4** タブで、**Static** を選択します。
  - i. サブネットの IP と Netmask/Routing Prefix を入力し、**OK** をクリックします。
4. iSCSI ボンドを作成します。
  - a. **Compute** → **Data Centers** をクリックします。
  - b. データセンター名をクリックします。詳細ビューが開きます。
  - c. **iSCSI Multipathing** タブで **Add** をクリックします。
  - d. **Add iSCSI Bond** ウィンドウで、Name を入力し、ネットワーク **net-1** と **net-2** を選択して、**OK** をクリックします。

データセンターには、古い論理ネットワークと新しい論理ネットワークを含む iSCSI ボンドがあります。

### 2.6.6.5. FCP ストレージの準備

Red Hat Virtualization は、既存の LUN で構成されるボリュームグループからストレージドメインを作成することで、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アタッチすることはできません。

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

Red Hat Enterprise Linux での FCP またはマルチパスの準備および設定に関する情報は、[ストレージ管理ガイド](#) および [DM Multipath ガイド](#) を参照してください。



### 重要

ブロックストレージを使用する際、仮想マシンを Raw デバイスまたは直接 LUN にデプロイし、論理ボリュームマネージャー (LVM) で管理する場合は、フィルターを作成してゲストの論理ボリュームを除外する必要があります。これにより、ホストの起動時にゲストの論理ボリュームがアクティブ化されるのを防ぐことができます。アクティブ化されると、論理ボリュームの内容が古くなり、データ破損が生じる可能性があります。**vdsm-tool config-lvm-filter** コマンドを使用して、LVM のフィルターを作成します。



### 重要

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



### 重要

SAN ストレージから起動したホストがストレージへの接続を失うと、ストレージファイルシステムは読み取り専用になり、接続が回復した後もその状態が続きます。

この状態を回避するには、ブート LUN の SAN のルートファイルシステムにドロップインマルチパス設定ファイルを追加し、接続可能な場合にキューに置かれるようにしてください。

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

## 2.6.6.6. FCP ストレージの追加

ここは、既存の FCP ストレージをデータドメインとして Red Hat Virtualization 環境にアタッチする手順を説明します。

### 手順

1. Storage → Domains をクリックします。
2. New Domain をクリックします。

3. ストレージドメインの **Name** を入力します。
4. ドロップダウンリストから **FCP Data Center** を選択します。  
適切な FCP データセンターがない場合は (**none**) を選択します。
5. ドロップダウンリストから **Domain Function** および **Storage Type** を選択します。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. **Host** 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はない場合、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。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、ストレージドメインは設定できません。

7. **New Domain** ウィンドウで、ストレージタイプとして **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できます。
  - a. **Advanced Parameters** をクリックします。
  - b. **Warning Low Space Indicator** フィールドに、パーセンテージ値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーに警告メッセージが表示され、ログに記録されます。
  - c. **Critical Space Action Blocker** 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、**Wipe After Delete** チェックボックスを選択します。このオプションは、ドメインの作成後に編集できますが、その場合はすでに存在している wipe after delete プロパティーは変更されません。
  - e. **Discard After Delete** のチェックボックスを選択して、削除後に破棄のオプションを有効化します。このオプションは、ドメインの作成後に編集できます。また、このオプションを利用できるのは、ブロックストレージドメインのみです。
9. **OK** をクリックします。

使用準備中は、新規 FCP データドメインのステータスは **Locked** になります。準備が整った時点で、自動的にデータセンターにアタッチされます。

#### 2.6.6.7. iSCSI または FCP ストレージの増設

iSCSI や FCP のストレージサイズを大きくするにはいくつかの方法があります。

- 既存の LUN を現在のストレージドメインに追加します。

- 新しい LUN を持つ新しいストレージドメインを作成し、既存のデータセンターに追加します。[iSCSI ストレージの追加](#) を参照してください。
- 基盤となる LUN のサイズを変更することで、ストレージドメインを拡張します。

FCP ストレージの設定またはサイズ変更については、Red Hat Enterprise Linux 8 の [ストレージデバイスの管理](#) で、[ファイバーチャネルデバイスの使用](#) を参照してください。

以下の手順では、既存のストレージドメインに新しい LUN を追加して、SAN (Storage Area Network) ストレージを拡張する方法を説明します。

### 前提条件

- ストレージドメインのステータスは **UP** である。
- LUN は、ステータスが **UP** のすべてのホストにアクセスできる。アクセスできない場合、操作は失敗し、LUN はドメインに追加されません。ただし、ホストには影響はありません。新しく追加されたホスト、またはメンテナンスか **Non Operational** のステータスから遷移するホストが LUN にアクセスできない場合、ホストの状態は **Non Operational** になります。

### 既存の iSCSI または FCP ストレージドメインの拡張

- Storage → Domains** をクリックして、iSCSI または FCP ドメインを選択します。
- Manage Domain** をクリックします。
- Targets → LUNs** をクリックし、**Discover Targets** 拡張ボタンをクリックします。
- ストレージサーバーの接続情報を入力し、**Discover** をクリックして接続を開始します。
- LUNs → Targets** をクリックして、新しく利用可能になった LUN のチェックボックスを選択します。
- OK** をクリックして、選択したストレージドメインに LUN を追加します。

これにより、追加した LUN のサイズでストレージドメインが増えます。

基礎となる LUN のサイズを変更してストレージドメインを拡張する場合は、管理ポータルで LUN も更新する必要があります。

### LUN サイズの更新

- Storage → Domains** をクリックして、iSCSI または FCP ドメインを選択します。
- Manage Domain** をクリックします。
- LUNs → Targets** をクリックします。
- Additional Size** の列で、LUN の **Add Additional\_Storage\_Size** ボタンをクリックして更新します。
- OK** をクリックして LUN を更新し、新規のストレージサイズを示します。

### 2.6.6.8. LUN の再利用

LUN をそのまま再利用して、ストレージドメインまたは仮想ディスクを作成することはできません。LUN を再利用しようとすると、管理ポータルに以下のエラーメッセージが表示されます。

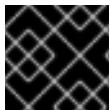


Physical device initialization failed. Please check that the device is empty and accessible by the host.

セルフホスト型エンジンでは、インストール時に以下のエラーが表示されます。

```
[ERROR] Error creating Volume Group: Failed to initialize physical device: ("[u'/dev/mapper/00000000000000000000000000000000']",)
[ERROR] Failed to execute stage 'Misc configuration': Failed to initialize physical device: ("[u'/dev/mapper/00000000000000000000000000000000']",)
```

LUN を再利用できるようにするには、古いパーティションテーブルをクリアする必要があります。



## 手順

誤ってデータを破棄しないように、正しい LUN でこの手順を実行する必要があります。

1. <LUN\_ID> でパーティションマッピングを削除します。

```
kpartx -dv /dev/mapper/<LUN_ID>
```

2. <LUN\_ID> の filesystem または raid 署名を削除します。

```
wipefs -a /dev/mapper/<LUN ID>
```

3. <LUN\_ID> でのパーティションテーブルの変更について、オペレーティングシステムに通知します。

partprobe

#### 2.6.6.9. 古い LUN の削除

ストレージドメインが削除されると、古くなった LUN リンクがストレージサーバーに残ることがあります。これにより、マルチパススキャンが遅くなったり、ログファイルが乱雑になったり、LUN ID の競合が発生したりします。

Red Hat Virtualization は iSCSI サーバーを管理しないため、ストレージドメインが削除されても LUN を自動的に削除することはできません。管理者は、[remove\\_stale\\_lun.yml](#) Ansible ロールを使用して、古くなった LUN リンクを手動で削除することができます。このロールは、指定されたデータセンターに属するすべてのホストから、古くなった LUN リンクを削除します。このロールとその変数の詳細は、[oVirt Ansible コレクションの古い LUN ロールの削除](#) を参照してください。



注記

すでにエンジンの ssh キーがすべてのホストに追加されているため、エンジンマシンから `remove_stale_lun.yml` を実行していることが想定されます。Playbook がエンジンマシン上で実行されていない場合は、データセンターに属するすべてのホストにユーザーの SSH キーを追加するか、ユーザーが適切なインベントリーファイルを提供する必要があります。

手順

1. Storage → Domains をクリックします。
  2. ストレージドメインの名前をクリックします。 詳細ビューが開きます。

3. Data Center タブをクリックします。
4. Maintenance をクリックしてから OK をクリックします。
5. Detach をクリックしてから OK をクリックします。
6. Remove をクリックします。
7. OK をクリックすると、ソース環境からストレージドメインが削除されます。
8. ストレージサーバーから LUN を取り外します。
9. Ansible を使用して、ホストから古い LUN を削除します。

```
ansible-playbook --extra-vars "lun=<LUN>"
/usr/share/ansible/collections/ansible_collections/ovirt/ovirt/roles/remove_stale_lun/examples/re
move_stale_lun.yml
```

ここでの LUN は、上記の手順でストレージサーバーから削除された LUN です。



### 注記

ストレージサーバーから LUN を最初に削除せずに、Ansible を使用してホストから古い LUN を削除すると、次回 VDSM が iSCSI の再スキャンを実行したときに、古い LUN がホスト上に再び現れます。

#### 2.6.6.10. LVM フィルターの作成

LVM フィルターとは、`/etc/lvm/lvm.conf` で設定できる機能で、正規表現のクエリーに基づいてボリュームのリストにデバイスを受け入れたり、ボリュームのリストからデバイスを拒否したりします。例えば、`/dev/cdrom` を無視するには、`filter=[^r|^/dev/cdrom$]"` を使用するか、`lvm config devices{filter=[^r|cdrom|"]}'` パラメーターを追加します。

これにより、ホストが直接必要としていない論理ボリュームをスキャンしてアクティブにすることを簡単に防ぐことができます。具体的には、RHV が管理する共有ストレージ上の論理ボリュームや、RHV の raw ボリュームにゲストが作成した論理ボリュームに対応しています。他の論理ボリュームをスキャンしてアクティブにすると、データの破損や起動の遅延などの問題が発生する可能性があるため、このソリューションが必要です。

解決策としては、各ホストに LVM フィルターを設定することで、ホスト上の LVM が、ホストが必要とする論理ボリュームのみをスキャンできます。

`vdsm-tool config-lvm-filter` コマンドを使用すると、現在の LVM 設定を分析し、フィルターを設定する必要があるかどうかを判断することができます。

LVM フィルターがまだ設定されていない場合、このコマンドはホスト用の LVM フィルターオプションを生成し、そのオプションを LVM の設定に追加します。

#### シナリオ 1: 未設定のホスト

まだ設定されていないホストでは、ユーザーが操作を確認すると、このコマンドが自動的に LVM を設定します。

```
vdsm-tool config-lvm-filter
```

```
Analyzing host...
```

```
Found these mounted logical volumes on this host:
```

```
logical volume: /dev/mapper/vg0-lv_home
mountpoint: /home
devices: /dev/vda2
```

```
logical volume: /dev/mapper/vg0-lv_root
mountpoint: /
devices: /dev/vda2
```

```
logical volume: /dev/mapper/vg0-lv_swap
mountpoint: [SWAP]
devices: /dev/vda2
```

```
This is the recommended LVM filter for this host:
```

```
filter = ["a|^/dev/vda2$", "r|.*|"]
```

```
This filter will allow LVM to access the local devices used by the
hypervisor, but not shared storage owned by VDSM. If you add a new
device to the volume group, you will need to edit the filter manually.
```

```
Configure LVM filter? [yes,NO] ? [NO/yes] yes
Configuration completed successfully!
```

```
Please reboot to verify the LVM configuration.
```

## シナリオ 2: 設定済みのホスト

ホストがすでに設定されている場合、このコマンドは単に LVM フィルターがすでに設定されていることをユーザーに知らせます。

```
vdsm-tool config-lvm-filter
```

```
Analyzing host...
```

```
LVM filter is already configured for Vdsm
```

## シナリオ 3: 手動設定が必要

ホストの設定が VDSM で要求される設定と一致しない場合は、LVM フィルターを手動で設定する必要があります。

```
vdsm-tool config-lvm-filter
```

```
Analyzing host...
```

```
Found these mounted logical volumes on this host:
```

```
logical volume: /dev/mapper/vg0-lv_home
mountpoint: /home
devices: /dev/vda2
```

```
logical volume: /dev/mapper/vg0-lv_root
mountpoint: /
devices: /dev/vda2
```

```
logical volume: /dev/mapper/vg0-lv_swap
mountpoint: [SWAP]
devices: /dev/vda2
```

This is the recommended LVM filter for this host:

```
filter = ["a|^/dev/vda2$", "r|.*|"]
```

This filter will allow LVM to access the local devices used by the hypervisor, but not shared storage owned by VDSM. If you add a new device to the volume group, you will need to edit the filter manually.

This is the current LVM filter:

```
filter = ["a|^/dev/vda2$", "a|^/dev/vdb1$", "r|.*|"]
```

WARNING: The current LVM filter does not match the recommended filter, Vdsm cannot configure the filter automatically.

Please edit /etc/lvm/lvm.conf and set the 'filter' option in the 'devices' section to the recommended value.

It is recommended to reboot after changing LVM filter.

## 2.6.7. Red Hat Gluster Storage の準備と追加

### 2.6.7.1. Red Hat Gluster Storage の準備

Red Hat Gluster Storage の準備および設定に関する情報は、[Red Hat Gluster Storage インストールガイド](#) を参照してください。

Red Hat Virtualization でサポートされている Red Hat Gluster Storage のバージョンは、[Red Hat Gluster Storage のバージョン互換性とサポート](#) を参照してください。

### 2.6.7.2. Red Hat Gluster Storage の追加

Red Hat Virtualization で Red Hat Gluster Storage を使用するには、[Red Hat Virtualization で Red Hat Gluster Storage を使用する場合の設定](#) を参照してください。

Red Hat Virtualization でサポートされている Red Hat Gluster Storage のバージョンは、[Red Hat Gluster Storage のバージョン互換性とサポート](#) を参照してください。

## 2.6.8. 既存ストレージドメインのインポート

### 2.6.8.1. 既存ストレージドメインのインポートの概要

データを含まない新しいストレージドメインを追加するだけでなく、既存のストレージドメインをインポートして、その中のデータにアクセスできます。ストレージドメインをインポートすることで、Manager データベースに障害が発生してもデータを復旧し、データセンター間でデータを移行できます。

以下は、各ストレージドメインタイプのインポートの概要です。

#### Data

既存のデータストレージドメインをインポートすると、そのデータストレージドメインに含まれるすべての仮想マシンやテンプレートにアクセスできるようになります。ストレージドメインをインポートした後、仮想マシン、フローティングディスクイメージ、テンプレートを宛先データセンターに手動でインポートする必要があります。データストレージドメインに含まれる仮想マシンやテンプレートをインポートするプロセスは、エクスポートストレージドメインの場合と同様です。ただし、データストレージドメインには、特定のデータセンター内のすべての仮想マシンとテンプレートが含まれているため、データ復旧や、データセンター間または環境間での仮想マシンの大規模な移行を行う場合は、データストレージドメインのインポートを推奨します。



#### 重要

サポートされている正しい互換性レベルを持つデータセンターに接続された既存のデータストレージドメインをインポートすることができます。詳細は、[Supportability and constraints regarding importing Storage Domains and Virtual Machines from older RHV versions](#) を参照してください。

#### 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含まれるすべての ISO ファイルや仮想ディスクケットにアクセスできるようになります。これらのリソースにアクセスするために、ストレージドメインをインポートした後に追加の操作をする必要はなく、必要に応じて仮想マシンにアタッチすることができます。

#### Export

既存のエクスポートストレージドメインをインポートすると、エクスポートストレージドメインに含まれるすべての仮想マシンイメージとテンプレートにアクセスできるようになります。エクスポートドメインは仮想マシンのイメージとテンプレートをエクスポートおよびインポートするように設計されているため、環境内または環境間で少数の仮想マシンとテンプレートを移行するには、エクスポートストレージドメインをインポートすることが推奨されます。エクスポートストレージドメイン間で仮想マシンとテンプレートをエクスポートおよびインポートする方法については、[Virtual Machine Management Guide](#) の [仮想マシンとテンプレートのエクスポートおよびインポート](#) を参照してください。



#### 注記

エクスポートストレージドメインは非推奨になりました。ストレージデータドメインはデータセンターからデタッチし、同じ環境または別の環境にある別のデータセンターにインポートすることができます。仮想マシン、フローティング仮想ディスク、およびテンプレートは、インポートされたストレージドメインからアタッチされたデータセンターにアップロードできます。



### 警告

ストレージドメインを宛先データセンターに接続すると、新しいストレージドメイン形式にアップグレードされ、ソースデータセンターに再接続されない場合があります。これにより、エクスポートドメインの代わりとしてのデータドメインを使用できなくなります。

#### 2.6.8.2. ストレージドメインのインポート

以前に同じ環境または別の環境のデータセンターに接続されていたストレージドメインをインポートします。この手順では、データの破損を防ぐために、ストレージドメインがどの環境のどのデータセンターにも接続されていないことを前提としています。既存のデータストレージドメインをインポートしてデータセンターに接続するには、ターゲットデータセンターを初期化する必要があります。

#### 手順

1. Storage → Domains をクリックします。
2. Import Domain をクリックします。
3. ストレージドメインをインポートする Data Center を選択します。
4. ストレージドメインの Name を入力します。
5. ドロップダウンリストから Domain Function および Storage Type を選択します。
6. Host 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。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、ストレージドメインは設定できません。

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ためのフィールドは、Domain Function リストと Storage Type リストで選択した値によって異なります。これらのフィールドは、新しいストレージドメインを追加するために使用できるフィールドと同じです。

8. 選択したデータセンターに接続した後にストレージドメインをアクティブ化するには、Activate Domain in Data Center チェックボックスをオンにします。
9. OK をクリックします。

これで、仮想マシンとテンプレートをストレージドメインからデータセンターにインポートできます。



### 警告

ストレージドメインを宛先データセンターに接続すると、新しいストレージドメイン形式にアップグレードされ、ソースデータセンターに再接続されない場合があります。これにより、エクスポートドメインの代わりとしてのデータドメインを使用できなくなります。

### 関連情報

- データドメインからの仮想マシンのインポート
- 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

#### 2.6.8.3. 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 環境内にあるデータセンターから別のデータセンターにストレージドメインを移行して、宛先データセンターがストレージドメインに含まれるデータにアクセスできるようにします。この手順では、ストレージドメインをデータセンターから切り離し、別のデータセンターに接続します。



### 警告

データストレージドメインを元のデータセンターよりも互換性の高いデータセンターに移行すると、ストレージドメインのストレージ形式のバージョンがアップグレードされます。

仮想マシンを新しいデータセンターに移行するなどの理由でストレージドメインを元のデータセンターに戻す場合は、上位バージョンではデータストレージドメインを元のデータセンターに再接続できないことに注意してください。

管理ポータルでは、ストレージドメイン形式を(たとえば V3 から V5 に)更新するか確認されます。また、DC レベルが低い古いデータセンターには再アタッチできないことが警告されます。

この問題を回避するには、ソースデータセンターと同じ互換性バージョンを持つターゲットデータセンターを作成します。互換性の低いバージョンを維持する必要がなくなった場合は、ターゲットデータセンターの互換性バージョンを引き上げることができます。

詳細は、[Supportability and constraints regarding importing Storage Domains and Virtual Machines from older RHV versions](#) を参照してください。

### 手順

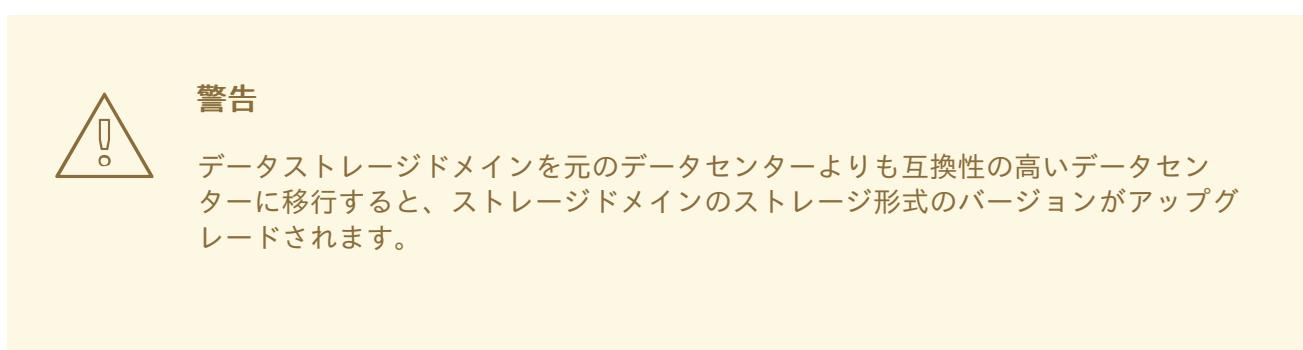
1. 目的のストレージドメインで実行されているすべての仮想マシンをシャットダウンします。

2. Storage → Domains をクリックします。
3. ストレージドメインの名前をクリックします。詳細ビューが開きます。
4. Data Center タブをクリックします。
5. Maintenance をクリックしてから OK をクリックします。
6. Detach をクリックしてから OK をクリックします。
7. Attach をクリックします。
8. 宛先データセンターを選択し、OK をクリックします。

ストレージドメインは宛先データセンターにアタッチされ、自動的にアクティブになります。これで、仮想マシンとテンプレートをストレージドメインから宛先データセンターにインポートできます。

#### 2.6.8.4. 異なる環境内のデータセンター間でのストレージドメインの移行

ストレージドメインを、ある Red Hat Virtualization 環境から別の環境に移行して、移行先環境がストレージドメインに含まれるデータにアクセスできるようにします。この手順では、1つの Red Hat Virtualization 環境からストレージドメインを削除し、それを別の環境にインポートします。既存のデータストレージドメインをインポートして Red Hat Virtualization データセンターに接続するには、ストレージドメインのソースデータセンターに、サポートされている正しい互換性レベルが必要です。



仮想マシンを新しいデータセンターに移行するなどの理由でストレージドメインを元のデータセンターに戻す場合は、上位バージョンではデータストレージドメインを元のデータセンターに再接続できないことに注意してください。

管理ポータルでは、ストレージドメイン形式を(たとえば V3 から V5 に)更新するか確認されます。また、DC レベルが低い古いデータセンターには再アタッチできないことが警告されます。

この問題を回避するには、ソースデータセンターと同じ互換性バージョンを持つターゲットデータセンターを作成します。互換性の低いバージョンを維持する必要がなくなった場合は、ターゲットデータセンターの互換性バージョンを引き上げることができます。

詳細は、[Supportability and constraints regarding importing Storage Domains and Virtual Machines from older RHV versions](#) を参照してください。

#### 手順

1. ソース環境の管理ポータルにログインします。
2. 目的のストレージドメインで実行されているすべての仮想マシンをシャットダウンします。

3. Storage → Domains をクリックします。
4. ストレージドメインの名前をクリックします。詳細ビューが開きます。
5. Data Center タブをクリックします。
6. Maintenance をクリックしてから OK をクリックします。
7. Detach をクリックしてから OK をクリックします。
8. Remove をクリックします。
9. Remove Storage(s) ウィンドウで、Format Domain, i.e. Storage Content will be lost! チェックボックスが選択されていません。この手順では、後で使用できるようにデータをストレージドメインに保存します。
10. OK をクリックすると、ソース環境からストレージドメインが削除されます。
11. 宛先環境の管理ポータルにログインします。
12. Storage → Domains をクリックします。
13. Import Domain をクリックします。
14. Data Center ドロップダウンリストから宛先データセンターを選択します。
15. ストレージドメインの名前を入力します。
16. 適切なドロップダウンリストから Domain Function および Storage Type を選択します。
17. Host のドロップダウンリストからホストを選択します。
18. ストレージドメインの詳細を入力します。



#### 注記

ストレージドメインの詳細を指定するためのフィールドは、Storage Type ドロップダウンリストで選択した値により異なります。これらのフィールドは、新しいストレージドメインを追加するために使用できるフィールドと同じです。

19. ストレージドメインが接続されたときに自動的にアクティブ化するには、Activate Domain in Data Center チェックボックスをオンにします。
20. OK をクリックします。

ストレージドメインは、新しい Red Hat Virtualization 環境の宛先データセンターに接続され、自動的にアクティブ化されます。これで、インポートしたストレージドメインから宛先データセンターに、仮想マシンおよびテンプレートをインポートできます。



## 警告

ストレージドメインを宛先データセンターに接続すると、新しいストレージドメイン形式にアップグレードされ、ソースデータセンターに再接続されない場合があります。これにより、エクスポートドメインの代わりとしてのデータドメインを使用できなくなります。

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

Red Hat Virtualization 環境にインポートしたデータストレージドメインからテンプレートをインポートします。この手順は、インポートされたデータストレージドメインがデータセンターに接続され、アクティブ化されていることを前提としています。

#### 手順

1. Storage → Domains をクリックします。
2. インポートされたストレージドメインの名前をクリックします。詳細ビューが開きます。
3. Template Import 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つ以上選択します。
5. Import をクリックします。
6. Import Templates(s) ウィンドウの各テンプレートについて、Cluster リストで正しいターゲットクラスターが選択されていることを確認します。
7. 外部仮想マシンの vNIC プロファイルを、ターゲットクラスターに存在するプロファイルにマッピングします。
  - a. vNic Profiles Mapping をクリックします。
  - b. Target vNic Profile ドロップダウンリストから、使用する vNIC プロファイルを選択します。
  - c. Import Templates ウィンドウで複数のターゲットクラスターを選択した場合、Target Cluster のドロップダウンリストで各ターゲットクラスターを選択し、マッピングが正しいことを確認します。
  - d. OK をクリックします。
8. OK をクリックします。

インポートされたテンプレートは、Template Import タブの下のリストに表示されなくなります。

### 2.6.9. ストレージタスク

#### 2.6.9.1. データストレージドメインへのイメージのアップロード

管理ポータルまたは REST API を使用して、仮想ディスクイメージと ISO イメージをデータストレージ ドメインにアップロードできます。



## 注記

REST API でイメージをアップロードするには、REST API ガイドの [IMAGETRANSFERS](#) および [IMAGETRANSFER](#) を参照してください。

QEMU 互換の仮想ディスクを仮想マシンに接続できます。仮想ディスクのタイプは、QCOW2 または raw のいずれかである必要があります。QCOW2 仮想ディスクから作成されたディスクは共有できません。また、QCOW2 仮想ディスクファイルにバックティングファイルを含めることはできません。

ISO イメージは、CDROM として仮想マシンに添付することも、仮想マシンの起動に使用することもできます。

## 前提条件

アップロード機能は HTML 5 API を使用するため、使用する環境には以下が必要です。

- 管理ポータルへのアクセスに使用される Web ブラウザーにインポートされた認証局。  
認証局をインポートするには、[https://engine\\_address/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA](https://engine_address/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA) にアクセスし、すべての信頼設定を有効にします。Firefox、Internet Explorer、または Google Chrome に認証局をインストールする手順を参照してください。
- Firefox 35、Internet Explorer 10、Chrome13 またはそれ以降などの HTML5 をサポートするブラウザー。

## 手順

1. Storage → Disks をクリックします。
2. Upload メニューから Start を選択します。
3. Choose File をクリックして、アップロードするイメージを選択します。
4. Disk Options フィールドに入力します。関連するフィールドについては、[新しい仮想ディスク ウィンドウの設定の説明](#) を参照してください。
5. OK をクリックします。  
進捗バーは、アップロードのステータスを示します。Upload メニューから、アップロードを一時停止、キャンセル、または再開できます。

## ヒント

アップロードが Reason: timeout due to transfer inactivity メッセージでタイムアウトした場合、タイムアウト値を増やして、ovirt-engine サービスを再起動します。

```
engine-config -s TransferImageClientInactivityTimeoutInSeconds=6000
systemctl restart ovirt-engine
```

### 2.6.9.2. VirtIO イメージファイルのストレージ ドメインへのアップロード

パフォーマンスと使いやすさの向上を目的として、virtio-win\_version.iso イメージには Windows 仮想マシン用に以下が含まれています。

- VirtIO ドライバー
- ゲストエージェントのインストーラー
- ドライバーのインストーラー

最新版の **virtio-win\_version.iso** をインストールしアップロードするには、以下を行います。

1. Manager マシンにイメージファイルをインストールします。

```
dnf -y install virtio-win
```

Manager マシンにインストールすると、イメージファイルは **/usr/share/virtio-win/virtio-win\_version.iso** になります。

2. インストール中にローカルで作成されなかったデータストレージドメインにイメージファイルをアップロードします。詳細は、[管理ガイド の データストレージドメインへのイメージのアップロード](#) を参照してください。
3. イメージファイルを仮想マシンに接続します。

これで、仮想マシンは virtio ドライバーとエージェントを使用できるようになります。

イメージファイルを仮想マシンにアタッチする方法の詳細は、[仮想マシン管理ガイド の Windows への ゲストエージェント、ツール、およびドライバーのインストール](#) を参照してください。

### 2.6.9.3. ISO ドメインへのイメージのアップロード



#### 注記

ISO ドメインは、非推奨のストレージドメインタイプです。ISO Uploader ツールである **ovirt-iso-uploader** は、Red Hat Virtualization 4.4 で削除されました。管理ポータルまたは REST API を使用して ISO イメージをデータドメインにアップロードする必要があります。詳細は、[データストレージドメインへのイメージのアップロード](#) を参照してください。

ISO ドメインは非推奨ですが、ISO ドメインを使用する必要がある場合に備え、この情報が提供されています。

ISO イメージを ISO ストレージドメインにアップロードして、Manager 内から使用できるようにするには、次の手順に従います。

#### 手順

1. ISO ストレージドメインが存在するデータセンターに属するホストに root としてログインします。
2. **/rhev/data-center** のディレクトリツリーを取得します。

```
tree /rhev/data-center
.
|-- 80dfacc7-52dd-4d75-ab82-4f9b8423dc8b
| |-- 76d1ecba-b61d-45a4-8eb5-89ab710a6275 -> /rhev/data-
| | center/mnt/10.10.10.10:_rhevnfssd/76d1ecba-b61d-45a4-8eb5-89ab710a6275
| | |-- b835cd1c-111c-468d-ba70-fec5346af227 -> /rhev/data-
```

```

center/mnt/10.10.10.10:_rhevisosd/b835cd1c-111c-468d-ba70-fec5346af227
| |-- mastersd → 76d1ecba-b61d-45a4-8eb5-89ab710a6275
| |-- tasks → mastersd/master/tasks
| '-- vms → mastersd/master/vms
|-- hsm-tasks
`-- mnt
 '-- 10.10.10.10:_rhevisosd
 | |-- b835cd1c-111c-468d-ba70-fec5346af227
 | | |-- dom_md
 | | | |-- ids
 | | | |-- inbox
 | | | |-- leases
 | | | |-- metadata
 | | | '-- outbox
 | | '-- images
 | | '-- 11111111-1111-1111-1111-111111111111
 | '-- lost+found [error opening dir]

(output trimmed)

```

- ソースの場所から **11111111-1111-1111-1111-111111111111** の完全パスにイメージを安全にコピーします。

```

scp root@isosource:/isos/example.iso /rhev/data-
center/mnt/10.96.4.50:_rhevisosd/b835cd1c-111c-468d-ba70-
fec5346af227/images/11111111-1111-1111-111111111111

```

- 新しくコピーされた ISO イメージのファイルパーミッションは 36:36 (vdsm:kvm) である必要があります。そうでない場合は、ISO ファイルのユーザーおよびグループの所有権を 36:36 (vdsm のユーザーおよびグループ) に変更します。

```

cd /rhev/data-center/mnt/10.96.4.50:_rhevisosd/b835cd1c-111c-468d-ba70-
fec5346af227/images/11111111-1111-1111-111111111111
chown 36.36 example.iso

```

これで、ISO イメージがデータセンターの ISO ドメインで利用できるようになります。

#### 2.6.9.4. ストレージドメインのメンテナンスモードへの移行

ストレージドメインを切り離して削除する前に、ストレージドメインをメンテナンスモードにする必要があります。これは、別のデータドメインを **master** データドメインとして再指定するために必要です。



#### 重要

仮想マシンにストレージドメインのリースがある場合、ストレージドメインをメンテナンスモードに移行することはできません。最初に仮想マシンをシャットダウンするか、リースを削除するか、別のストレージドメインに移動する必要があります。仮想マシンのリースに関する詳細は、[仮想マシン管理ガイド](#) を参照してください。

LUN を追加して iSCSI ドメインを拡張できるのは、ドメインがアクティブな場合のみです。

#### 手順

1. ストレージドメインで実行しているすべての仮想マシンをシャットダウンします。
2. Storage → Domains をクリックします。
3. ストレージドメインの名前をクリックします。詳細ビューが開きます。
4. Data Center タブをクリックします。
5. Maintenance をクリックします。



#### 注記

**Ignore OVF update failure** チェックボックスをオンにすると、OVF 更新が失敗した場合でも、ストレージドメインをメンテナンスマードにすることができます。

6. OK をクリックします。

ストレージドメインは非アクティブ化され、結果リストに **Inactive** ステータスが表示されます。これで、データセンターから非アクティブなストレージドメインを編集、デタッチ、削除、または再アクティブ化できます。



#### 注記

また、関連付けられているデータセンターの詳細ビューのストレージタブを使用して、ドメインをアクティブ化し、デタッチし、メンテナンスマードにすることもできます。

### 2.6.9.5. ストレージドメインの編集

管理ポータルからストレージドメインパラメーターを編集できます。ストレージドメインの状態(アクティブまたは非アクティブ)に応じて、さまざまなフィールドを編集できます。Data Center、Domain Function、Storage Type、および Format などのフィールドを変更することはできません。

- **Active:** ストレージドメインがアクティブ状態の場合、Name、Description、Comment、Warning Low Space Indicator (%)、Critical Space Action Blocker (GB)、Wipe After Delete、および Discard After Delete フィールドを編集できます。Name フィールドは、ストレージドメインがアクティブな場合にのみ編集できます。他のすべてのフィールドは、ストレージドメインが非アクティブの場合も編集できます。
- **Inactive:** ストレージドメインがメンテナンスマードにあるかアタッチされていないため非アクティブ状態になっている場合、Name、Data Center、Domain Function、Storage Type、および Format を除くすべてのフィールドを編集できます。ストレージ接続、マウントオプション、およびその他の高度なパラメーターを編集するには、ストレージドメインを非アクティブにする必要があります。これは、NFS、POSIX、およびローカルストレージタイプでのみサポートされます。



#### 注記

iSCSI ストレージ接続は、管理ポータルを介して編集することはできませんが、REST API を介して編集することができます。REST API ガイドの [ストレージ接続の更新](#) を参照してください。

#### アクティブなストレージドメインの編集\*

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

2. **Manage Domain** をクリックします。
3. 必要に応じて、使用可能なフィールドを編集します。
4. **OK** をクリックします。

#### 非アクティブなストレージドメインの編集

1. **Storage → Domains** をクリックします。
2. ストレージドメインがアクティブな場合は、メンテナンスモードに移行します。
  - a. ストレージドメインの名前をクリックします。詳細ビューが開きます。
  - b. **Data Center** タブをクリックします。
  - c. **Maintenance** をクリックします。
  - d. **OK** をクリックします。
3. **Manage Domain** をクリックします。
4. 必要に応じて、ストレージパスおよびその他の詳細を編集します。新しい接続の詳細は、元の接続と同じストレージタイプである必要があります。
5. **OK** をクリックします。
6. ストレージドメインをアクティブ化します。
  - a. ストレージドメインの名前をクリックします。詳細ビューが開きます。
  - b. **Data Center** タブをクリックします。
  - c. **Activate** をクリックします。

#### 2.6.9.6. OVF の更新

デフォルトでは、OVF は 60 分ごとに更新されます。ただし、重要な仮想マシンをインポートした場合、または重要な更新を行った場合は、OVF を手動で更新できます。

#### 手順

1. **Storage → Domains** をクリックします。
2. ストレージドメインを選択し、**More Actions** (⋮) をクリックしてから、**Update OVFs** をクリックします。  
OVF が更新され、メッセージが **Events** に表示されます。

#### 2.6.9.7. メンテナンスモードからのストレージドメインのアクティブ化

データセンターのストレージに変更を加えている場合は、ストレージドメインをメンテナンスモードにする必要があります。ストレージドメインをアクティブ化して、使用を再開します。

1. **Storage → Domains** をクリックします。
2. 非アクティブなストレージドメインの名前をクリックします。詳細ビューが開きます。

3. Data Centers タブをクリックします。

4. Activate をクリックします。



### 重要

データドメインをアクティブ化する前に ISO ドメインをアクティブ化しようとすると、エラーメッセージが表示され、ドメインはアクティブ化されません。

#### 2.6.9.8. データセンターからストレージドメインをデタッチ

ある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、別のデータセンターに移行します。

##### 手順

1. Storage → Domains をクリックします。
2. ストレージドメインの名前をクリックします。詳細ビューが開きます。
3. Data Center タブをクリックします。
4. Maintenance をクリックします。
5. OK をクリックしてメンテナンスモードを開始します。
6. Detach をクリックします。
7. OK をクリックして、ストレージドメインを切り離します。

ストレージドメインがデータセンターから切り離され、別のデータセンターに接続できるようになります。

#### 2.6.9.9. ストレージドメインのデータセンターへのアタッチ

ストレージドメインをデータセンターにアタッチします。

##### 手順

1. Storage → Domains をクリックします。
2. ストレージドメインの名前をクリックします。詳細ビューが開きます。
3. Data Center タブをクリックします。
4. Attach をクリックします。
5. 適切なデータセンターを選択します。
6. OK をクリックします。

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

#### 2.6.9.10. ストレージドメインの削除

データセンターに、仮想化環境から削除するストレージドメインがあります。

## 手順

1. Storage → Domains をクリックします。
2. ストレージドメインをメンテナンスモードに移動し、デタッチします。
  - a. ストレージドメインの名前をクリックします。詳細ビューが開きます。
  - b. Data Center タブをクリックします。
  - c. Maintenance をクリックしてから OK をクリックします。
  - d. Detach をクリックしてから OK をクリックします。
3. Remove をクリックします。
4. オプションで Format Domain, i.e. Storage Content will be lost! チェックボックスを選択して、ドメインのコンテンツを消去します。
5. OK をクリックします。

ストレージドメインが環境から完全に削除されます。

### 2.6.9.11. ストレージドメインの破棄

エラーが発生したストレージドメインは、通常の手順では削除できない場合があります。ストレージドメインを破棄すると、仮想化環境からストレージドメインが強制的に削除されます。

## 手順

1. Storage → Domains をクリックします。
2. ストレージドメインを選択し、More Actions (⋮) をクリックしてから Destroy をクリックします。
3. Approve operation チェックボックスを選択します。
4. OK をクリックします。

### 2.6.9.12. ディスクプロファイルの作成

ディスクプロファイルは、ストレージドメイン内における仮想ディスクのスループットの最大レベルと入出力操作の最大レベルを定義します。ディスクプロファイルは、データセンターで定義されたストレージプロファイルに基づいて作成され、プロファイルを有効にするには、個々の仮想ディスクに手動で割り当てる必要があります。

この手順は、ストレージドメインが属するデータセンターの下に1つ以上のストレージサービス品質エンタリーやすでに定義されていることを前提としています。

## 手順

1. Storage → Domains をクリックします。
2. データストレージドメインの名前をクリックします。詳細ビューが開きます。
3. Disk Profiles タブをクリックします。

4. **New** をクリックします。
5. ディスクプロファイルの **Name** と **Description** 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 (Quality of Service) を選択します。
7. **OK** をクリックします。

#### 2.6.9.13. 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

1. Storage → Domains をクリックします。
2. データストレージドメインの名前をクリックします。詳細ビューが開きます。
3. Disk Profiles タブをクリックします。
4. 削除するディスクプロファイルを選択します。
5. Remove をクリックします。
6. **OK** をクリックします。

ディスクプロファイルがいずれかの仮想ディスクに割り当てられている場合、ディスクプロファイルはそれらの仮想ディスクから削除されます。

#### 2.6.9.14. ストレージドメインのヘルスステータスの表示

ストレージドメインには、通常の **Status** に加えて、外部ヘルスステータスがあります。外部ヘルスステータスは、プラグインや外部システムから報告されたり、管理者が設定したりするもので、ストレージドメインの **Name** の左側に以下のいずれかのアイコンで表示されます。

- 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の詳細を表示するには、ストレージドメインの名前をクリックします。詳細ビューが開きます。ここで Events タブをクリックします。

ストレージドメインのヘルスステータスは、REST API を使用して表示することもできます。ストレージドメインでの **GET** リクエストには、ヘルスステータスを含む **external\_status** 要素が含まれます。

**events** コレクションを介して、REST API でストレージドメインのヘルスステータスを設定できます。詳細は、REST API ガイドの [イベントの追加](#) を参照してください。

#### 2.6.9.15. ストレージドメインの Discard After Delete の設定

**Discard After Delete** チェックボックスがオンになっている場合は、論理ボリュームが削除されると **blkdiscard** コマンドが呼び出され、ブロックが解放されたことが基盤となるストレージに通知されます。ストレージアレイは、解放されたスペースを使用して、要求に応じて割り当てることができます。**Discard After Delete** は、ブロックストレージでのみ機能します。このフラグは、NFS などのファイルストレージ用の Red Hat Virtualization Manager では使用できません。

#### 制限:

- **Discard After Delete** は、iSCSI やファイバーチャネルなどのブロックストレージドメインでのみ使用できます。
- 基盤となるストレージは **Discard** をサポートする必要があります。

**Discard After Delete** は、ブロックストレージドメインを作成するとき、またはブロックストレージドメインを編集するときに有効にできます。[ブロック・ストレージの準備と追加](#) および [ストレージドメインの編集](#) を参照してください。

#### 2.6.9.16. 250 を超えるホストがある環境での 4K サポートの有効化

デフォルトでは、GlusterFS ドメインとローカルストレージドメインは、最大 250 のホストを備えた Red Hat Virtualization 環境で 4K ブロックサイズをサポートします。4K ブロックサイズを使用すると、特に大きなファイルを使用する場合などに、パフォーマンスが向上します。また、VDO などの 4K 互換性を必要とするツールを使用する場合にも必要です。



#### 注記

GlusterFS Storage は非推奨になり、将来のリリースではサポートされなくなります。

ホストの最大数がデフォルトの 250 の場合、Sanlock が割り当てるロックスペース領域は 1MB です。4K ストレージを使用するときにホストの最大数を増やすと、ロックスペース領域が大きくなります。たとえば、2000 のホストを使用する場合、ロックスペース領域は最大 8MB になる可能性があります。

エンジン設定パラメーター **MaxNumberOfHostsInStoragePool** を設定することにより、250 を超えるホストがある環境で 4K ブロックのサポートを有効にできます。

#### 手順

1. Manager マシンで、必要な最大数のホストを有効にします。

```
engine-config -s MaxNumberOfHostsInStoragePool=NUMBER_OF_HOSTS
```

2. JBoss Application Server を再起動します。

```
service jboss-as restart
```

たとえば、300 のホストを持つクラスターがある場合は、次のように入力します。

```
engine-config -s MaxNumberOfHostsInStoragePool=300
service jboss-as restart
```

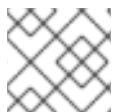
#### 検証

Manager で **MaxNumberOfHostsInStoragePool** パラメーターの値を表示します。

```
engine-config --get=MaxNumberOfHostsInStoragePool
MaxNumberOfHostsInStoragePool: 250 version: general
```

### 2.6.9.17. 4K サポートの無効化

デフォルトでは、GlusterFS ドメインとローカルストレージドメインは 4K ブロックサイズをサポートします。4K ブロックサイズを使用すると、特に大きなファイルを使用する場合などに、パフォーマンスが向上します。また、VDO などの 4K 互換性を必要とするツールを使用する場合にも必要です。



#### 注記

GlusterFS Storage は非推奨になり、将来のリリースではサポートされなくなります。

4K ブロックのサポートを無効にすることができます。

#### 手順

1. 4K ブロックのサポートが有効になっていることを確認してください。

```
$ vdsm-client Host getCapabilities
...
{
 "GLUSTERFS": [
 0,
 0,
 512,
 4096,
]
 ...
}
```

2. `/etc/vdsm/vdsm.conf.d/gluster.conf` を編集し、`enable_4k_storage` を `false` に設定します。  
以下に例を示します。

```
$ vi /etc/vdsm/vdsm.conf.d/gluster.conf

[gluster]
Use to disable 4k support
if needed.
enable_4k_storage = false
```

### 2.6.9.18. ストレージドメインの使用可能なスペースの監視

ストレージドメインの使用可能なスペースを監視し、ストレージドメインが容量に近づいたときに警告するアラートを作成できます。ドメインがシャットダウンする重大なしきい値を定義することもできます。

Virtual Data Optimizer (VDO) とシンプールのサポートにより、物理的に使用可能なスペースよりも多くの使用可能なスペースが表示される場合があります。VDO の場合はこの動作が予想されますが、Manager は実際に書き込むことができるデータの量を予測できません。Warning Low Confirmed Space Indicator パラメーターは、ドメインが物理スペース容量に近づいたときに通知し、確認済みスペースの残りの量を示します。確認済みスペースとは、データの書き込みに使用できる実際のスペースを指します。

#### 手順

1. 管理ポータルで **Storage → Storage Domain** をクリックし、ストレージドメインの名前をクリックします。
2. **Manage Domain** をクリックします。 **Manage Domains** ダイアログボックスが開きます。
3. **Advanced Parameters** を展開します。
4. **Warning Low Space Indicator (%)** には、パーセンテージ値を入力します。ストレージドメインの使用可能なスペースがこの値に達すると、Manager はドメインが容量に近づいていることを警告します。
5. **Critical Space Action Blocker (GB)** の場合は、ギガバイト単位で値を入力します。ストレージドメインの使用可能なスペースがこの値に達すると、Manager はシャットダウンします。
6. **Warning Low Confirmed Space Indicator (%)** には、パーセンテージ値を入力します。ストレージドメインの使用可能なスペースがこの値に達すると、Manager はデータの書き込みに使用できる実際のスペースが容量に近づいていることを警告します。

## 2.7. プール

### 2.7.1. 仮想マシンプールの概要

仮想マシンプールは、すべて同じテンプレートのクローンであり、特定のグループ内の任意のユーザーがオンデマンドで使用できる仮想マシンのグループです。仮想マシンプールを使用すると、管理者はユーザー向けに一連の一般化された仮想マシンを迅速に設定できます。

ユーザーは、プールから仮想マシンを取得することにより、仮想マシンプールにアクセスします。ユーザーがプールから仮想マシンを取得すると、プール内の仮想マシン(使用可能な場合)のいずれかが提供されます。その仮想マシンは、プールのベースとなったテンプレートと同じオペレーティングシステムと設定を持ちますが、ユーザーが仮想マシンを使用するたびにプールの同じメンバーを受け取るとは限りません。ユーザーは、プールの設定に応じて、同じ仮想マシンプールから複数の仮想マシンを取得することもできます。

仮想マシンプールはデフォルトでステートレスです。つまり、仮想マシンのデータと設定の変更は再起動後も永続的ではありません。ただし、プールはステートフルになるように設定できるため、前のユーザーが行った変更を保持できます。ただし、ユーザーが仮想マシンプールから取得した仮想マシンのコンソールオプションを設定する場合、それらのオプションは、その仮想マシンプールのそのユーザーのデフォルトとして設定されます。



#### 注記

管理ポータルからアクセスした場合、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める必要があるためです。

原則として、プール内の仮想マシンは、ユーザーが取得すると起動し、ユーザーが終了するとシャットダウンされます。ただし、仮想マシンプールには、事前に起動した仮想マシンを含めることができます。事前に起動した仮想マシンは稼働状態に保たれ、ユーザーが使用するまでアイドル状態のままになります。これにより、ユーザーはそのような仮想マシンの使用をすぐに開始できますが、これらの仮想マシンは、アイドル状態のために使用されていないときでもシステムリソースを消費します。

### 2.7.2. 仮想マシンプールの作成

共通のテンプレートに基づいて、複数の仮想マシンを含む仮想マシンプールを作成できます。仮想マシンのシーリングおよびテンプレートの作成の詳細は、[仮想マシン管理ガイド](#) の [テンプレート](#) を参照してください。

## Windows 仮想マシンの Sysprep ファイル設定オプション

要件に応じて、いくつかの **sysprep** ファイル設定オプションを使用できます。

プールがドメインに参加する必要がない場合は、`/usr/share/ovirt-engine/conf/sysprep/` にあるデフォルトの **sysprep** ファイルを使用できます。

プールをドメインに参加させる必要がある場合は、Windows オペレーティングシステムごとにカスタム **sysprep** を作成できます。

- 各オペレーティングシステムに関連するセクションを `/usr/share/ovirt-engine/conf/osinfo-defaults.properties` から新しいファイルにコピーし、`99-defaults.properties` として保存します。

- 99-defaults.properties** で、Windows 製品のアクティベーションキーと新しいカスタム **sysprep** ファイルのパスを指定します。

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

- ドメイン、ドメインパスワード、およびドメイン管理者を指定して、新しい **sysprep** ファイルを作成します。

```
<Credentials>
 <Domain>__AD_Domain__</Domain>
 <Password>__Domain_Password__</Password>
 <Username>__Domain_Administrator__</Username>
</Credentials>
```

Windows 仮想マシンのさまざまなプール用に異なる **sysprep** 設定が必要な場合は、管理ポータルにカスタムの **sysprep** ファイルを作成することができます（以下の [仮想マシンプールの作成](#) を参照）。詳細は、[仮想マシンガイド](#) の [sysprep を使用した仮想マシン設定の自動化](#) を参照してください。

## 手順

- Compute** → **Pools** をクリックします。
- New** をクリックします。
- ドロップダウンリストから **Cluster** を選択します。
- ドロップダウンメニューから **Template** とバージョンを選択します。テンプレートは、プール内のすべての仮想マシンの標準設定を指定します。
- ドロップダウンリストから **Operating System** を選択します。
- Optimized for** を使用して、**Desktop** または **Server** の仮想マシンを最適化します。



## 注記

高性能仮想マシンは単一のホストと具体的なリソースに固定されているため、**High Performance** 最適化はプールには推奨されません。このような設定の仮想マシンが複数含まれるプールは、適切に実行されません。

7. **Name** を入力し、オプションで **Description** と **Comment** を入力します。

プールの **Name** は、数値の接尾辞を付けて、プール内の各仮想マシンに適用されます。仮想マシンの番号付けは、プレースホルダーとして **?** を使用してカスタマイズできます。

### 例2.1 プール名と仮想マシンの番号付けの例

- プール: **MyPool**  
仮想マシン: **MyPool-1**、**MyPool-2**、... **MyPool-10**
- プール: **MyPool-???**  
仮想マシン: **MyPool-001**、**MyPool-002**、... **MyPool-010**

8. プールの **Number of VMs** を入力します。

9. **Prestarted** フィールドに、事前起動する仮想マシンの数を入力します。

10. 1人のユーザーがセッションで実行できる **Maximum number of VMs per user** を選択します。最小値は 1 です。

11. 削除からの保護を有効にするには、**Delete Protection** チェックボックスをオンにします。

12. Windows 以外の仮想マシンのプールを作成している場合、またはデフォルトの **sysprep** を使用している場合、この手順をスキップしてください。Windows 仮想マシンのプール用のカスタム **sysprep** ファイルを作成する場合:

- a. **Show Advanced Options** ボタンをクリックします。
- b. **Initial Run** タブをクリックし、**Use Cloud-Init/Sysprep** チェックボックスを選択します。
- c. **Authentication** 矢印をクリックして **User Name** と **Password** を入力するか、**Use already configured password** を選択します。



## 注記

この **User Name** は、ローカル管理者の名前です。この値は、**Authentication** セクションまたはカスタム **sysprep** ファイルでデフォルト値 (**user**) 以外の値に変更できます。

- d. **Custom Script** の矢印をクリックして、**/usr/share/ovirt-engine/conf/sysprep/** にあるデフォルトの **sysprep** ファイルの内容をテキストボックスに貼り付けます。
- e. **sysprep** ファイルの次の値を変更できます。
  - **Key**。事前定義された Windows アクティベーションプロダクトキーを使用しない場合は、**<![CDATA[\$ProductKey\$]]>** を有効なプロダクトキーに置き換えてください。

```
<ProductKey>
 <Key><![CDATA[$ProductKey$]]></Key>
</ProductKey>
```

### 例2.2 Windows のプロダクトキーの例

```
<ProductKey>
 <Key>0000-000-000-000</Key>
</ProductKey>
```

- Windows 仮想マシンが参加する **Domain**、ドメインの **Password**、およびドメイン管理者の **Username**:

```
<Credentials>
 <Domain>_AD_Domain_</Domain>
 <Password>_Domain_Password_</Password>
 <Username>_Domain_Administrator_</Username>
</Credentials>
```

### 例2.3 ドメイン認証情報の例

```
<Credentials>
 <Domain>addomain.local</Domain>
 <Password>12345678</Password>
 <Username>Sarah_Smith</Username>
</Credentials>
```

#### 注記

ドメインに参加するには、**Domain**、**Password**、および **Username** が必要です。**Key** はアクティベーション用です。必ずしも両方が必要なわけではありません。

ドメインと認証情報は、Initial Run タブでは変更できません。

- ローカル管理者の **FullName**:

```
<UserData>
...
 <FullName>_Local_Administrator_</FullName>
...
</UserData>
```

- DisplayName** とローカル管理者の **Name**:

```
<LocalAccounts>
 <LocalAccount wcm:action="add">
 <Password>
 <Value><![CDATA[$AdminPassword$]]></Value>
 <PlainText>true</PlainText>
```

```
</Password>
<DisplayName>__Local_Administrator__</DisplayName>
<Group>administrators</Group>
<Name>__Local_Administrator__</Name>
</LocalAccount>
</LocalAccounts>
```

**sysprep** ファイルの残りの変数は、Initial Run タブで入力できます。

13. オプションPool Type を設定します。

- a. Type タブをクリックして、Pool Type を選択します。
  - Manual - 管理者は、仮想マシンをプールに明示的に戻す責任があります。
  - Automatic - 仮想マシンは自動的に仮想マシンプールに戻されます。
- b. 仮想マシンがスタートフルモードで開始されるようにするには、Stateful Pool チェックボックスをオンにします。これにより、前のユーザーが行った変更が仮想マシンに保持されます。
- c. OK をクリックします。

14. オプションSPICE プロキシーをオーバーライドします。

- a. Console タブで、Override SPICE Proxy チェックボックスをオンにします。
- b. Overridden SPICE proxy address テキストフィールドで、グローバル SPICE プロキシーをオーバーライドする SPICE プロキシーのアドレスを指定します。
- c. OK をクリックします。

15. Windows 仮想マシンのプールの場合は、Compute → Virtual Machines をクリックして、プールから各仮想マシンを選択し、Run → Run Once をクリックします。



## 注記

仮想マシンが起動せず、Info [windeploy.exe] Found no unattend file が %WINDIR%\panther\UnattendGC\setupact.log に表示されない場合は、作成に使用された Windows 仮想マシンのレジストリーに UnattendFile キーを追加して、プールのテンプレートを作成します。

1. Windows 仮想マシンに、A:\Unattend.xml などの無人ファイルを含むセカンドドライブ CD-ROM デバイスが接続されていることを確認します。
2. 仮想マシンを選択し、Run → Run once をクリックします。
3. ブートオプションで、Attach Windows guest tools CD をオンにします。
4. Start、Run の順にクリックし、Open テキストボックスに regedit を入力して OK をクリックします。
5. 左側のペインで、HKEY\_LOCAL\_MACHINE → SYSTEM → Setup に移動します。
6. 右ペインを右クリックして、New → String Value を選択します。
7. キー名として UnattendFile を入力します。
8. 新しいキーをダブルクリックし、キーの値として unattend ファイルの名前とパス (A:\Unattend.xml など) を入力します。
9. レジストリーを保存し、Windows 仮想マシンをシールして新しいテンプレートを作成します。詳細は、仮想マシン管理ガイドの [テンプレート](#) を参照してください。

指定した数の同一の仮想マシンを使用して仮想マシンプールを作成および設定しました。これらの仮想マシンは、Compute → Virtual Machines で表示するか、プールの名前をクリックして詳細ビューを開くことで表示できます。プール内の仮想マシンは、アイコンにより独立した仮想マシンと区別されます。

### 2.7.3. New Pool と Edit Pool ウィンドウの設定およびコントロール

#### 2.7.3.1. New Pool と Edit Pool の一般設定の説明

次の表に、仮想マシンプールに固有の New Pool ウィンドウと Edit Pool ウィンドウの General タブに必要な情報の詳細を示します。他のすべての設定は、New Virtual Machine ウィンドウの設定と同じです。

表2.30 General 設定

フィールド名	説明
--------	----

フィールド名	説明
Template	仮想マシンプールのベースとなるテンプレートおよびテンプレートサブバージョン。テンプレートの <b>latest</b> サブバージョンに基づいてプールを作成する場合、プール内のすべての仮想マシンは、再起動すると、最新のテンプレートバージョンを自動的に受け取ります。仮想マシンのテンプレートの設定に関する詳細は、仮想マシン管理ガイドの <a href="#">仮想マシンの General の設定に関する説明</a> および <a href="#">New Template</a> および <a href="#">Edit Template</a> ウィンドウの設定に関する説明を参照してください。
説明	仮想マシンに関する分かりやすい説明。
Comment	仮想マシンプールについて、人間が判読可能なコメントをプレーンテキストで追加するフィールド。
Prestarted VMs	ユーザーによって取得される前に開始され、その状態に維持される、仮想マシンプール内の仮想マシンの数を指定できます。このフィールドの値は、0 から仮想マシンプール内の仮想マシン総数の間でなければなりません。
Number of VMs/Increase number of VMs in pool by	作成して仮想マシンプールで使用できるようにする仮想マシンの数を指定できます。編集ウィンドウでは、仮想マシンプール内の仮想マシンの数を指定された数だけ増やすことができます。デフォルトでは、プールに作成できる仮想マシンの最大数は 1000 です。この値は、 <a href="#">engine-config</a> コマンドの <b>MaxVmsInPool</b> キーを使用して設定できます。
Maximum number of VMs per user	1人のユーザーが一度に仮想マシンプールから取得できる仮想マシンの最大数を指定できます。このフィールドの値は、1 から 32,767 の間でなければなりません。
Delete Protection	プール内の仮想マシンが削除されないようにすることができます。
Sealed	テンプレートからのマシン固有の設定が、テンプレートからプロビジョニングされた仮想マシンで再現されないようにします。シールプロセスの詳細は、 <a href="#">テンプレートとしてデプロイするための Windows 仮想マシンのシール</a> を参照してください。

### 2.7.3.2. New Pool と Edit Pool の Type 設定

次の表に、New Pool ウィンドウと Edit Pool ウィンドウの Type タブに必要な情報の詳細を示します。

表2.31 Type 設定

フィールド名	説明
Pool Type	<p>このドロップダウンメニューでは、仮想マシンプールのタイプを指定できます。以下のオプションを設定できます。</p> <ul style="list-style-type: none"> <li>● <b>Automatic:</b> ユーザーが仮想マシンプールから取得した仮想マシンの使用を終了すると、その仮想マシンは自動的に仮想マシンプールに戻されます。</li> <li>● <b>Manual:</b> ユーザーが仮想マシンプールから取得した仮想マシンの使用を終了した後、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。</li> </ul>
Stateful Pool	<p>仮想マシンが別のユーザーに渡されたときに、プール内の仮想マシンの状態を保持するかどうかを指定します。これは、前のユーザーが行った変更が仮想マシンに保持されることを意味します。</p>

### 2.7.3.3. New Pool と Edit Pool の Console 設定

次の表に、仮想マシンプールに固有の **New Pool** または **Edit Pool** ウィンドウの **Console** タブに必要な情報の詳細を示します。他のすべての設定は、**New Virtual Machine** ウィンドウと **Edit Virtual Machine** ウィンドウの設定と同じです。

表2.32 Console の設定

フィールド名	説明
Override SPICE proxy	<p>このチェックボックスを選択すると、グローバル設定で定義された SPICE プロキシーのオーバーライドが有効になります。この機能は、ホストが存在するネットワーク外にユーザー(たとえば、仮想マシンポータル経由で接続する)がある場合に役に立ちます。</p>
Overridden SPICE proxy address	<p>SPICE クライアントが仮想マシンに接続するプロキシー。このプロキシーは、Red Hat Virtualization 環境用に定義されたグローバル SPICE プロキシーと、仮想マシンプールが属するクラスター用に定義された SPICE プロキシー(存在する場合)の両方をオーバーライドします。アドレスは以下の形式でなければなりません。</p> <p style="text-align: center;"><code>protocol://host:port</code></p>

### 2.7.3.4. 仮想マシンプールの Host 設定

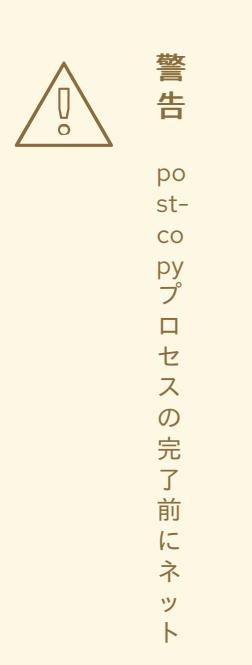
次の表に、New Pool ウィンドウおよび Edit Pool ウィンドウの Host タブで使用できるオプションの詳細を示します。

表2.33 仮想マシンプール: Host 設定

フィールド名	サブ要素	説明
Start Running On		<p>仮想マシンを実行する優先ホストを定義します。以下のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>● <b>Any Host in Cluster</b> - 仮想マシンは、クラスター内の利用可能な任意のホストで起動し、実行できます。</li> <li>● <b>Specific Host(s)</b> - 仮想マシンはクラスター内の特定のホストで実行を開始します。ただし、Manager または管理者は、仮想マシンの移行および高可用性設定に応じて、仮想マシンをクラスター内の別のホストに移行することができます。利用可能なホスト一覧から、特定のホストまたはホストのグループを選択します。</li> </ul>
CPU options	<p>Pass-Through Host CPU</p> <p>Migrate only to hosts with the same TSC frequency</p>	<p>選択すると、仮想マシンがホストのCPU フラグを使用できるようになります。これを選択すると、Migration Options が Allow manual migration only に設定されます。</p> <p>選択した場合、仮想マシンは同じ TSC 周波数のホストにしか移行できません。このオプションは、高性能仮想マシンにのみ有効です。</p>

フィールド名	サブ要素	説明
Migration Options	Migration mode	<p>仮想マシンの実行および移行オプションを定義します。このオプションを使用しない場合、仮想マシンはそのクラスターのポリシーに従って実行または移行されます。</p> <ul style="list-style-type: none"> <li>● <b>Allow manual and automatic migration</b> - 環境のステータスに応じて自動的に、または管理者により手動で、仮想マシンをホストから別のホストに移行することができます。</li> <li>● <b>Allow manual migration only</b> - 仮想マシンは、管理者が手動で移行する場合にのみ、ホストから別のホストに移行できます。</li> <li>● <b>Do not allow migration</b> - 自動と手動のいずれの場合も、仮想マシンは移行できません。</li> </ul>
	Migration policy	<p>移行収束ポリシーを定義します。チェックボックスをオフのままになると、ホストがポリシーを決定します。</p> <ul style="list-style-type: none"> <li>● <b>Cluster default (Minimal downtime)</b> - <b>vds.conf</b> のオーバーライドは引き続き適用されます。ゲストエージェントフックメカニズムが無効になっています。</li> <li>● <b>Minimal downtime</b> - 一般的な状況において、仮想マシンを移行できます。仮想マシンで重大なダウンタイムは発生しません。移行は、長時間 (QEMU の反復により最大 500 ミリ秒) が経過しても仮想マシンの移行が収束されない場合に中止されます。ゲストエージェントフックメカニズムは有効化されています。</li> </ul>

フィールド名	サブ要素	説明
		<ul style="list-style-type: none"> <li>Post-copy migration - コピー後の移行を使用すると、ソースホスト上にある、移行予定の仮想マシンの vCPU を一時停止し、最小限のメモリーページのみを転送します。次に、移行先ホストにある仮想マシンの vCPU をアクティブにし、移行先で仮想マシンが動作中に残りのメモリーページを転送します。</li> </ul> <p>post-copy ポリシーでは、まず pre-copy を実行して収束するか検証します。長時間経過しても仮想マシンの移行が収束しない場合、post-copy に切り替わります。</p> <p>これにより、移行先の仮想マシンのダウンタイムが大幅に短縮されるとともに、移行元の仮想マシンのメモリーページがどれだけ急激に変化しても、確実に移行が完了されます。標準的な pre-copy の移行では対応できない、連続使用率の高い仮想マシンの移行に最適です。</p> <p>このポリシーの欠点として、post-copy フェーズではメモリーの不足部分がホスト間で転送されるため、仮想マシンが大幅に遅くなる可能性があります。</p>



フィールド名	サブ要素	説明
		ワーク接続が切断されると、Managerは一時停止し、実行中の仮想マシンを強制終了します。仮想マシンの可用性が重要な場合や、移行ネット

フィールド名	サブ要素	説明
		<p>ワークが不安定な場合は、post-copy migrationを使用しないでください。</p>
	<b>Enable migration encryption</b>	<ul style="list-style-type: none"> <li>● <b>Suspend workload if needed</b> - 仮想マシンが負荷の高いワークロードを実行している場合も含め、ほとんどの状況で仮想マシンを移行できます。そのため、仮想マシンで他の設定よりも大きなダウントIMEが生じる場合があります。ワークロードが極端な場合、移行が中止される可能性があります。ゲストエージェントフックメカニズムは有効化されています。</li> </ul> <p>移行中に仮想マシンを暗号化できるようにします。</p> <ul style="list-style-type: none"> <li>● Cluster default</li> <li>● Encrypt</li> <li>● Don't encrypt</li> </ul>

フィールド名	サブ要素	説明
	Parallel Migrations	<p>使用する並列移行接続の有無と数を指定できます。</p> <ul style="list-style-type: none"> <li>● <b>Cluster default:</b> 並列移行接続は、クラスターのデフォルトによって決定されます。</li> <li>● <b>Disabled:</b> 仮想マシンは、単一の非並列接続を使用して移行されます。</li> <li>● <b>Auto:</b> 並列接続の数は自動的に決定されます。この設定により、並列接続が自動的に無効になる可能性があります。</li> <li>● <b>Auto Parallel:</b> 並列接続の数は自動的に決定されます。</li> <li>● <b>Custom:</b> 並列接続の優先数を指定できます。実際の数はそれより少ない場合があります。</li> </ul>
	Number of VM Migration Connections	<p>この設定は、Custom が選択されている場合にのみ利用できます。カスタム並列移行の推奨数は 2 から 255 です。</p>
Configure NUMA	NUMA Node Count	仮想マシンに割り当てることができるホストで利用可能な仮想 NUMA ノードの数。

フィールド名	サブ要素	説明
	NUMA Pinning	<p>NUMA Topology ウィンドウを開きます。このウィンドウには、ホストの合計 CPU、メモリー、NUMA ノード、および仮想マシンの仮想 NUMA ノードが表示されます。右側のボックスから左側の NUMA ノードに各 vNUMA をクリックアンドドラッグすることで、仮想 NUMA ノードを手動でホストの NUMA ノードに固定することができます。</p> <p>メモリー割り当てに <b>Tune Mode</b> を設定することもできます。</p> <p><b>Strict</b> - メモリーをターゲットノードに割り当たることができない場合は、メモリーの割り当てに失敗します。</p> <p><b>Preferred</b> - メモリーは、1つの優先ノードから割り当てられます。十分なメモリーが利用できない場合は、他のノードからメモリーを割り当てることができます。</p> <p><b>Interleave</b> - メモリーはラウンドロビンアルゴリズムで全ノードに割り当てられます。</p> <p>NUMA ピニングを定義する場合、<b>Migration Options</b> は <b>Allow manual migration only</b> に設定されます。</p>

#### 2.7.3.5. New Pool と Edit Pool の Resource Allocation 設定

次の表に、仮想マシンプールに固有の New Pool ウィンドウと Edit Pool ウィンドウの Resource Allocation タブに必要な情報の詳細を示します。他のすべての設定は、New Virtual Machine ウィンドウの設定と同じです。詳細は、仮想マシン管理ガイドの [仮想マシンの Resource Allocation 設定に関する説明](#) を参照してください。

表2.34 Resource Allocation の設定

フィールド名	サブ要素	説明
Disk Allocation	Auto select target	このチェックボックスをオンになると、空き容量が最も多いストレージドメインが自動的に選択されます。Target フィールドと Disk Profile フィールドは無効になっています。

フィールド名	サブ要素	説明
	Format	このフィールドは読み取り専用で、常に QCOW2 を表示します。

#### 2.7.3.6. 仮想マシンプールの編集

作成した仮想マシンプールのプロパティーを編集できます。仮想マシンプールの編集時に使用できるプロパティーは、新しい仮想マシンプールの作成時に使用できるプロパティーと同じですが、**Number of VMs** プロパティーが **Increase number of VMs in pool by** に置き換えられている点が異なります。



注記

仮想マシンプールを編集する場合、導入された変更は新しい仮想マシンにのみ影響します。導入された変更の時点ですでに存在していた仮想マシンは影響を受けません。

手順

1. Compute → Pools をクリックして、仮想マシンプールを選択します。
  2. Edit をクリックします。
  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。

### 2.7.3.7. プール内の仮想マシンの事前起動

仮想マシンプール内の仮想マシンは、デフォルトで電源がオフになっています。ユーザーがプールから仮想マシンを要求すると、マシンの電源がオンになり、ユーザーに割り当てられます。一方で、事前に起動した仮想マシンはすでに稼働しており、ユーザーへの割り当てを待機しているため、ユーザーがマシンにアクセスできるようになるまで待機する時間が短縮されます。事前に起動した仮想マシンがシャットダウンすると、プールに戻され、元の状態に復元されます。事前に起動した仮想マシンの最大数は、プール内の仮想マシンの数です。

事前に起動した仮想マシンは、ユーザーが特に割り当てられていない仮想マシンにすぐにアクセスする必要がある環境に適しています。自動プールのみが仮想マシンを事前に起動できます。

手順

1. Compute → Pools をクリックして、仮想マシンプールを選択します。
  2. Edit をクリックします。
  3. Prestarted VMs フィールドに、事前起動する仮想マシンの数を入力します。
  4. Type タブをクリックします。Pool Type が Automatic に設定されていることを確認します。
  5. OK をクリックします。

### 2.7.3.8. 仮想マシンプールへの仮想マシンの追加

仮想マシンプールで最初にプロビジョニングされた数よりも多くの仮想マシンが必要な場合は、プールにマシンを追加します。

## 手順

1. **Compute → Pools** をクリックして、仮想マシンプールを選択します。
2. **Edit** をクリックします。
3. **Increase number of VMs in pool by** フィールドに、追加の仮想マシンの数を入力します。
4. **OK** をクリックします。

### 2.7.3.9. 仮想マシンプールからの仮想マシンのデタッチ

仮想マシンを仮想マシンプールからデタッチできます。仮想マシンを切り離すと、その仮想マシンがプールから削除され、独立した仮想マシンになります。

## 手順

1. **Compute → Pools** をクリックします。
2. プールの名前をクリックします。詳細ビューが開きます。
3. **Virtual Machines** タブをクリックして、プール内の仮想マシンを一覧表示します。
4. 仮想マシンのステータスが **Down** であることを確認します。実行中の仮想マシンをデタッチすることはできません。
5. 1つ以上の仮想マシンを選択し、**Detach** をクリックします。
6. **OK** をクリックします。



## 注記

仮想マシンは環境内に存在したままで、**Compute → Virtual Machines** から表示およびアクセスできます。アイコンが変化して、デタッチされた仮想マシンが独立した仮想マシンであることを示すことに注意してください。

### 2.7.3.10. 仮想マシンプールの削除

データセンターから仮想マシンプールを削除できます。最初に、プール内のすべての仮想マシンを削除またはデタッチする必要があります。プールから仮想マシンを切り離すと、それらは独立した仮想マシンとして保持されます。

## 手順

1. **Compute → Pools** をクリックして、仮想マシンプールを選択します。
2. **Remove** をクリックします。
3. **OK** をクリックします。

## 2.8. 仮想ディスク

## 2.8.1. 仮想マシンストレージについて

Red Hat Virtualization は、NFS、iSCSI、FCP の 3 つのストレージタイプをサポートしています。

それぞれのタイプで、Storage Pool Manager (SPM) と呼ばれるホストが、ホストとストレージ間のアクセスを管理します。SPM ホストは、ストレージプール内でフルアクセスできる唯一のノードです。SPM は、ストレージドメインのメタデータとプールのメタデータを変更できます。他のすべてのホストは、仮想マシンのハードディスクイメージデータにのみアクセスできます。

NFS、ローカル、または POSIX 準拠のデータセンターの場合、SPM はデフォルトで、ファイルシステム内のファイルとしてシンプロビジョニングされた形式を使用して仮想ディスクを作成します。

iSCSI およびその他のブロックベースのデータセンターの場合、SPM は、提供された論理ユニット番号 (LUN) の上にボリュームグループを作成し、仮想ディスクとして使用する論理ボリュームを作成します。ブロックベースのストレージ上の仮想ディスクは、デフォルトで事前に割り当てられています。

仮想ディスクが事前に割り当てられている場合は、GB 単位で指定されたサイズの論理ボリュームが作成されます。仮想マシンは、**kpartx**、**vgscan**、**vgchange**、または **mount** を使用して Red Hat Enterprise Linux サーバーにマウントし、仮想マシンのプロセスまたは問題を調査できます。

仮想ディスクがシンプロビジョニングされる場合は、1GB の論理ボリュームが作成されます。論理ボリュームは、仮想マシンが実行しているホストによって継続的に監視されます。使用量がしきい値に近づくとすぐに、ホストは SPM に通知し、SPM は論理ボリュームを 1GB 拡張します。ホストは、論理ボリュームが拡張された後、仮想マシンを再開する責任があります。仮想マシンが一時停止状態になる場合は、SPM が時間内にディスクを拡張できなかったことを意味します。これは、SPM がビジー状態であるか、十分なストレージスペースがない場合に発生します。

事前に割り当てられた (raw) 形式の仮想ディスクの書き込み速度は、シンプロビジョニング (QCOW2) 形式の仮想ディスクの書き込み速度を大幅に上回ります。シンプロビジョニングでは、仮想ディスクの作成にかかる時間が大幅に短縮されます。シンプロビジョニング形式は、I/O を多用しない仮想マシンに適しています。I/O 書き込みが多い仮想マシンには、事前に割り当てられた形式が推奨されます。仮想マシンが 4 秒ごとに 1GB を超える書き込みを実行できる場合は、可能であれば事前に割り当てられたディスクを使用してください。

## 2.8.2. 仮想ディスクの概要

Red Hat Virtualization のストレージオプションには、事前割り当て (シックプロビジョニング) とスペース (シンプロビジョニング) があります。

- 事前割り当て

事前割り当ての仮想ディスクは、仮想マシンに必要なすべてのストレージを事前に割り当てます。たとえば、仮想マシンのデータパーティション用に事前に割り当てられた 20 GB の論理ボリュームは、作成直後に 20GB のストレージスペースを占有します。

- スペース

スペース割り当てを使用すると、管理者は仮想マシンに割り当てるストレージの合計を定義できますが、ストレージは必要な場合にのみ割り当てられます。

たとえば、20 GB のシンプロビジョニングされた論理ボリュームは、最初に作成されたときに 0 GB のストレージスペースを占有します。オペレーティングシステムがインストールされると、インストールされたファイルのサイズを占める可能性があり、最大 20 GB まで追加されるにつれて大きくなり続けます。

**Storage → Disks** で仮想ディスクの ID を表示できます。ID は、デバイス名 (たとえば、/dev/vda0) が変更されてディスクが破損する可能性があるため、仮想ディスクを識別するために使用されます。/dev/disk/by-id で仮想ディスクの ID を表示することもできます。

ディスクの **Virtual Size** は、Storage → Disks と、ストレージドメイン、仮想マシン、およびテンプレートの詳細ビューの Disks タブで確認できます。Virtual Size は、仮想マシンが使用できるディスク容量の合計量です。これは、仮想ディスクを作成または編集するときに Size(GB) フィールドに入力する数値です。

ディスクの **Actual Size** は、ストレージドメインとテンプレートの詳細ビューの Disks タブで確認できます。これは、これまでに仮想マシンに割り当てられたディスク容量です。事前に割り当てられたディスクは、Virtual Size と Actual Size が同じになります。スパースディスクは、割り当てられているディスク容量に応じて、異なる値を表示する場合があります。

次の表に、ストレージのタイプとフォーマットの可能な組み合わせを示します。

表2.35 許可されたストレージの組み合わせ

ストレージ	フォーマット	タイプ	注記
NFS	Raw	事前割り当て	仮想ディスクに定義されたストレージの量に等しい、フォーマットされていない初期サイズのファイル。
NFS	Raw	スパース	初期サイズがゼロに近く、フォーマットされていないファイル。
NFS	QCOW2	スパース	初期サイズがゼロに近く、QCOW2 フォーマットのファイル。後続のリヤーは QCOW2 フォーマットになります。
SAN	Raw	事前割り当て	仮想ディスクに定義されたストレージの量に等しい、フォーマットされていない初期サイズのブロックデバイス。
SAN	QCOW2	スパース	初期サイズが仮想ディスクに定義されたサイズ（現在は 1 GB）よりもるかに小さく、必要に応じてスペースが割り当てられる QCOW2 フォーマット（現在は 1 GB 刻み）のブロックデバイス。

### 2.8.3. 削除後に仮想ディスクをワイプするための設定

管理ポータルで **Wipe After Delete** チェックボックスとして表示される **wipe\_after\_delete** フラグは、仮想ディスクが削除されると使用済みデータをゼロに置き換えます。デフォルトの **false** に設定されて

いる場合、ディスクを削除すると、それらのブロックが再利用できるようになりますが、データは消去されません。その場合、ブロックがゼロに戻されていないため、このデータが復元される可能性があります。

**wipe\_after\_delete** フラグは、ブロックストレージでのみ機能します。NFSなどのファイルストレージでは、ファイルシステムがデータが存在しないことを確認するため、このオプションによる影響はありません。

仮想ディスクに対して **wipe\_after\_delete** を有効にするとさらにセキュアになるため、仮想ディスクに機密データが含まれている場合に推奨されます。これはより負荷の高い操作であり、パフォーマンスの低下と削除時間の延長が発生する可能性があります。



### 注記

Wipe After Delete 機能はセキュアな削除とは異なります。同じストレージ上に作成された新しいディスクが古いディスクからのデータを公開しないだけで、ストレージからのデータの削除は保証されません。

**wipe\_after\_delete** フラグのデフォルトは、セットアップ時に `true` に変更できます ([Red Hat Virtualization Manager の設定](#) を参照)。または、Red Hat Virtualization Manager で `engine-config` ツールを使用して変更できます。設定の変更を有効にするには、`ovirt-engine` サービスを再起動します。



### 注記

**wipe\_after\_delete** フラグのデフォルト設定を変更しても、既存のディスクの Wipe After Delete プロパティーには影響しません。

## エンジン設定ツールを使用して SANWipeAfterDelete をデフォルトの True に設定

1. `--set` アクションを指定して `engine-config` ツールを実行します。

```
engine-config --set SANWipeAfterDelete=true
```

2. 変更を反映するには、`ovirt-engine` サービスを再起動します。

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

ホストにある `/var/log/vdsm/vdsm.log` ファイルをチェックして、仮想ディスクが正常に消去および削除されたことを確認できます。

正常にワイプされると、ログファイルには `storage_domain_id/volume_id was zeroed and will be deleted` が記録されます。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
```

正常に削除されると、ログファイルには `finished with VG:storage_domain_id LVs:  
list_of_volume_ids, img: image_id` が記録されます。以下に例を示します。

```
finished with VG:a9cb0625-d5dc-49ab-8ad1-72722e82b0bf LVs: {'a49351a7-15d8-4932-8d67-
512a369f9d61': ImgPar(imgs=['11f8b3be-fa96-4f6a-bb83-14c9b12b6e0d'], parent='00000000-0000-
0000-0000-000000000000'), img: 11f8b3be-fa96-4f6a-bb83-14c9b12b6e0d}
```

ワイプに失敗すると、**zeroing storage\_domain\_id/volume\_id failedZero and remove this volume manually** のログメッセージが表示され、削除に失敗すると **Remove failed for some of VG: storage\_domain\_id zeroed volumes: list\_of\_volume\_ids** が表示されます。

## 2.8.4. Red Hat Virtualization の共有可能ディスク

一部のアプリケーションでは、サーバー間でストレージを共有する必要があります。Red Hat Virtualization を使用すると、仮想マシンのハードディスクを **Shareable** としてマークし、それらのディスクを仮想マシンにアタッチできます。このようにして、単一の仮想ディスクを複数のクラスター対応ゲストが使用できます。

共有ディスクは、すべての状況で使用されるわけではありません。クラスター化されたデータベースサーバーやその他の高可用性サービスなどのアプリケーションには、共有ディスクが適しています。クラスターに対応していない複数のゲストに共有ディスクをアタッチすると、ディスクへの読み取りと書き込みが調整されていないため、データが破損する可能性があります。

共有ディスクのスナップショットは取得できません。スナップショットを取得した場合、その仮想ディスクは後で共有可能としてマークできません。

ディスクを作成するとき、または後でディスクを編集することで、ディスクを共有可能としてマークできます。



### 重要

RAW 形式のディスクのみ共有可能にできます。

## 2.8.5. Red Hat Virtualization の読み取り専用ディスク

一部のアプリケーションでは、管理者が読み取り専用の権限でデータを共有する必要があります。これは、仮想マシンにアタッチされたディスクを作成または編集する際に、仮想マシンの詳細ビューにある **Disks** タブで **Read Only** チェックボックスをオンにすることで実行できます。これにより、管理者の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による同一ディスクの読み取りを可能にできます。

仮想マシンの実行中は、ディスクの読み取り専用ステータスを変更することはできません。



### 重要

ジャーナルファイルシステムをマウントするには、読み取り/書き込みアクセスが必要です。 **Read Only** オプションの使用は、そのようなファイルシステム (EXT3、EXT4、XFS など) を含む仮想ディスクには適していません。

## 2.8.6. 仮想ディスクタスク

### 2.8.6.1. 仮想ディスクの作成

**Image** ディスクの作成は、すべて Manager が管理します。 **Direct LUN** ディスクには、外部で準備された、既存のターゲットが必要です。

特定の仮想マシンに接続された仮想ディスクを作成できます。 [New Virtual Disk ウィンドウの設定](#) で指定されているように、接続された仮想ディスクを作成するときに追加のオプションを使用できます。

#### 仮想マシンに接続された仮想ディスクの作成

1. Compute → Virtual Machines をクリックします。
2. 仮想マシンの名前をクリックします。詳細ビューが開きます。
3. Disks タブをクリックします。
4. New をクリックします。
5. 適切なボタンをクリックして、仮想ディスクを Image ディスクにするか Direct LUN ディスクにするかを指定します。
6. 仮想ディスクに必要なオプションを選択します。オプションは、選択したディスクタイプにより異なります。各ディスクタイプの各オプションの詳細は、[New Virtual Disk ウィンドウの設定](#) を参照してください。
7. OK をクリックします。

どの仮想マシンにも属さないフローティング仮想ディスクを作成することもできます。このディスクは、単一の仮想マシンに接続することも、ディスクが共有可能な場合は複数の仮想マシンに接続することもできます。[New Virtual Disk ウィンドウの設定](#) で指定されているように、仮想ディスクの作成時に一部のオプションを使用できません。

#### フローティング仮想ディスクの作成

1. Storage → Disks をクリックします。
2. New をクリックします。
3. 適切なボタンをクリックして、仮想ディスクを Image ディスクにするか Direct LUN ディスクにするかを指定します。
4. 仮想ディスクに必要なオプションを選択します。オプションは、選択したディスクタイプにより異なります。各ディスクタイプの各オプションの詳細は、[New Virtual Disk 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。

#### 2.8.6.2. New Virtual Disk ウィンドウの設定

フローティング仮想ディスクと接続仮想ディスクを作成する際に使用する New Virtual Disk ウィンドウは非常に似ているため、両ウィンドウの設定については1つのセクションでまとめて説明しています。

表2.36 New Virtual Disk 設定と Edit Virtual Disk 設定

フィールド名	説明
Size(GB)	新しい仮想ディスクのサイズ(GB 単位)。
Alias	仮想ディスクの名前。最大で 40 文字に制限されています。
Description	仮想ディスクの説明。このフィールドは推奨されますが、必須ではありません。

フィールド名	説明
Interface	<p>このフィールドは、接続されたディスクの作成時にのみ表示されます。</p> <p>ディスクが仮想マシンに提示する仮想インターフェイス。VirtIO はより高速ですが、ドライバーが必要です。Red Hat Enterprise Linux 5 以降にはこれらのドライバーが含まれています。これらのドライバーは Windows には含まれていませんが、virtio-win ISO イメージからインストールできます。IDE および SATA デバイスは特別なドライバーを必要としません。</p> <p>インターフェイスタイプは、ディスクが接続されているすべての仮想マシンを停止した後に更新できます。</p>
Data Center	<p>このフィールドは、フローティングディスクの作成時にのみ表示されます。</p> <p>仮想ディスクが利用できるデータセンター。</p>
Storage Domain	<p>仮想ディスクが保存されるストレージドメイン。ドロップダウンリストには、特定のデータセンターで使用可能なすべてのストレージドメインが表示され、ストレージドメインで使用可能な合計容量と現在使用可能な容量も表示されます。</p>
Allocation Policy	<p>新しい仮想ディスクのプロビジョニングポリシー。</p> <ul style="list-style-type: none"> <li>● <b>Preallocated</b> は、仮想ディスクの作成時に、ディスクのサイズ全体をストレージドメインに割り当てます。事前に割り当てられたディスクの仮想サイズと実際のサイズは同じです。事前に割り当てられた仮想ディスクは、シンプロビジョニングされた仮想ディスクよりも作成に時間がかかりますが、読み取りと書き込みのパフォーマンスは向上します。サーバーやその他の I/O を多用する仮想マシンには、事前に割り当てられた仮想ディスクをお勧めします。仮想マシンが 4 秒ごとに 1GB を超える書き込みを実行できる場合は、可能であれば事前に割り当てられたディスクを使用してください。</li> <li>● <b>Thin Provision</b> は、仮想ディスクの作成時に 1GB を割り当て、ディスクを拡張できるサイズの最大制限を設定します。ディスクの仮想サイズが上限です。ディスクの実際のサイズは、これまでに割り当てられたスペースです。シンプロビジョニングされたディスクは、事前に割り当てられたディスクよりも短時間で作成でき、ストレージのオーバーコミットが可能です。デスクトップには、シンプロビジョニングされた仮想ディスクが推奨されます。</li> </ul>

フィールド名	説明
Disk Profile	仮想ディスクに割り当てられたディスクプロファイル。ディスクプロファイルは、ストレージドメイン内の仮想ディスクのスループットの最大量と入出力操作の最大レベルを定義します。ディスクプロファイルは、データセンター用に作成されたストレージの Quality of Service エントリーに基づき、ストレージドメインレベルで定義されます。
Activate Disk(s)	このフィールドは、接続されたディスクの作成時にのみ表示されます。  作成後すぐに仮想ディスクをアクティブ化します。
Wipe After Delete	仮想ディスクが削除されたときに機密資料を削除するための強化されたセキュリティーを有効にできます。
Bootable	このフィールドは、接続されたディスクの作成時にのみ表示されます。  仮想ディスクで起動可能フラグを有効にできます。
Shareable	一度に複数の仮想マシンに仮想ディスクを接続できます。
Read-Only	このフィールドは、接続されたディスクの作成時にのみ表示されます。  ディスクを読み取り専用として設定できます。同じディスクを読み取り専用として1つの仮想マシンに接続したり、別の仮想マシンに再書き込み可能として接続したりできます。
Enable Incremental Backup	仮想ディスクの増分バックアップを有効にします。増分バックアップでは、ディスクを RAW 形式ではなく QCOW2 形式でフォーマットする必要があります。 <a href="#">増分バックアップと復元</a> を参照してください。

フィールド名	説明
Enable Discard	<p>このフィールドは、接続されたディスクの作成時にのみ表示されます。</p> <p>仮想マシンが稼働しているときに、シンプロビジョニングされたディスクを縮小できます。ブロックストレージの場合、基盤となるストレージデバイスは破棄呼び出しをサポートする必要があります。基盤となるストレージが <code>discard_zeroes_data</code> プロパティーをサポートしない限り、このオプションを <b>Wipe After Delete</b> で使用することはできません。ファイルストレージの場合、基盤となるファイルシステムおよびブロックデバイスは破棄呼び出しをサポートする必要があります。すべての要件が満たされている場合、ゲスト仮想マシンから発行された SCSI UNMAP コマンドは、QEMU によって基盤となるストレージに渡され、未使用のスペースが解放されます。</p>

Direct LUN 設定は、Targets > LUNs または LUNs > Targets のいずれかに表示できます。Targets > LUNs は、検出されたホストに従って使用可能な LUN をソートしますが、LUNs > Targets は LUN の単一のリストを表示します。

Discover Targets セクションのフィールドに入力し、Discover をクリックしてターゲットサーバーを検出します。次に、Login All ボタンをクリックして、ターゲットサーバーで使用可能な LUN を一覧表示し、各 LUN の横にあるラジオボタンを使用して、追加する LUN を選択します。

LUN を仮想マシンのハードディスクイメージとして直接使用すると、仮想マシンとそのデータの間の抽象化レイヤーが削除されます。

ダイレクト LUN を仮想マシンのハードディスクイメージとして使用する場合は、次の考慮事項を考慮する必要があります。

- ダイレクト LUN ハードディスクイメージのライブストレージ移行はサポートされていません。
- ダイレクト LUN ディスクは、仮想マシンのエクスポートには含まれません。
- ダイレクト LUN ディスクは、仮想マシンのスナップショットには含まれません。

表2.37 New Virtual Disk および Edit Virtual Disk の設定 Direct LUN

フィールド名	説明
Alias	仮想ディスクの名前。最大で 40 文字に制限されています。

フィールド名	説明
説明	<p>仮想ディスクの説明。このフィールドは推奨されますが、必須ではありません。デフォルトでは、LUN ID の最後の 4 文字がフィールドに挿入されます。</p> <p>デフォルトの動作は、<b>engine-config</b> コマンドを使用して  <b>PopulateDirectLUNDiskDescriptionWithLUNId</b> 設定キーを適切な値に設定することで設定できます。完全な LUN ID を使用する場合は設定キーを <b>-1</b> に設定し、この機能を無視する場合は <b>0</b> に設定します。正の整数は、説明に LUN ID の対応する文字数を入力します。</p>
Interface	<p>このフィールドは、接続されたディスクの作成時にのみ表示されます。</p> <p>ディスクが仮想マシンに提示する仮想インターフェイス。<b>VirtIO</b> はより高速ですが、ドライバーが必要です。Red Hat Enterprise Linux 5 以降にはこれらのドライバーが含まれています。これらのドライバーは Windows には含まれていませんが、<b>virtio-win</b> ISO からインストールできます。IDE および SATA デバイスは特別なドライバーを必要としません。</p> <p>インターフェイスタイプは、ディスクが接続されているすべての仮想マシンを停止した後に更新できます。</p>
Data Center	<p>このフィールドは、フローティングディスクの作成時にのみ表示されます。</p> <p>仮想ディスクが利用できるデータセンター。</p>
Host	LUN がマウントされるホスト。データセンター内の任意のホストを選択できます。
Storage Type	追加する外部 LUN のタイプ。 <b>iSCSI</b> または <b>Fibre Channel</b> を選択できます。

フィールド名	説明
Discover Targets	<p>iSCSI 外部 LUN を使用しており、Targets &gt; LUNs が選択されている場合、このセクションを展開できます。</p> <p><b>Address</b> - ターゲットサーバーのホスト名または IP アドレス。</p> <p><b>Port</b> - ターゲットサーバーへの接続を試みるためのポート。デフォルトポートは 3260 です。</p> <p><b>User Authentication</b> - iSCSI サーバーにはユーザー認証が必要です。iSCSI 外部 LUN を使用している場合は、User Authentication フィールドが表示されます。</p> <p><b>CHAP user name</b> - LUN にログインするパーミッションを持つユーザーのユーザー名。このフィールドには、User Authentication チェックボックスがオンになっている場合にアクセスできます。</p> <p><b>CHAP password</b> - LUN にログインするパーミッションを持つユーザーのパスワード。このフィールドには、User Authentication チェックボックスがオンになっている場合にアクセスできます。</p>
Activate Disk(s)	<p>このフィールドは、接続されたディスクの作成時にのみ表示されます。</p> <p>作成後すぐに仮想ディスクをアクティブ化します。</p>
Bootable	<p>このフィールドは、接続されたディスクの作成時にのみ表示されます。</p> <p>仮想ディスクで起動可能フラグを有効にできます。</p>
Shareable	一度に複数の仮想マシンに仮想ディスクを接続できます。
Read-Only	<p>このフィールドは、接続されたディスクの作成時にのみ表示されます。</p> <p>ディスクを読み取り専用として設定できます。同じディスクを読み取り専用として1つの仮想マシンに接続したり、別の仮想マシンに再書き込み可能として接続したりできます。</p>

フィールド名	説明
Enable Discard	<p>このフィールドは、接続されたディスクの作成時にのみ表示されます。</p> <p>仮想マシンが稼働しているときに、シンプロビジョニングされたディスクを縮小できます。このオプションを有効にすると、ゲスト仮想マシンから発行された SCSI UNMAP コマンドは、QEMU によって基盤となるストレージに渡され、未使用のスペースが解放されます。</p>
Enable SCSI Pass-Through	<p>このフィールドは、接続されたディスクの作成時にのみ表示されます。</p> <p><b>Interface</b> が <b>VirtIO-SCSI</b> に設定されている場合に使用できます。このチェックボックスをオンにすると、物理 SCSI デバイスを仮想ディスクにパススルーできます。SCSI パススルーハードウェアが有効になっている <b>VirtIO-SCSI</b> インターフェイスでは、自動的に SCSI 廃棄がサポートされます。このチェックボックスが選択されている場合、<b>Read-Only</b> はサポートされません。</p> <p>このチェックボックスが選択されていない場合、仮想ディスクはエミュレートされた SCSI デバイスを使用します。<b>Read-Only</b> は、エミュレートされた <b>VirtIO-SCSI</b> ディスクでサポートされています。</p>
Allow Privileged SCSI I/O	<p>このフィールドは、接続されたディスクの作成時にのみ表示されます。</p> <p><b>Enable SCSI Pass-Through</b> チェックボックスがオンになっている場合に使用できます。このチェックボックスをオンにすると、フィルタリングされていない SCSI Generic I/O (SG_IO) アクセスが有効になり、ディスク上で特権的な SG_IO コマンドが許可されます。これは永続的な予約に必要です。</p>
Using SCSI Reservation	<p>このフィールドは、接続されたディスクの作成時にのみ表示されます。</p> <p><b>Enable SCSI Pass-Through</b> および <b>Allow Privileged SCSI I/O</b> チェックボックスがオンになっている場合に使用できます。このチェックボックスをオンにすると、このディスクを使用する仮想マシンの移行が無効になり、SCSI 予約を使用する仮想マシンがディスクにアクセスできなくなるのを防ぐことができます。</p>



## 重要

ジャーナルファイルシステムをマウントするには、読み取り/書き込みアクセスが必要です。Read Only オプションの使用は、そのようなファイルシステム (EXT3、EXT4、XFS など) を含む仮想ディスクには適していません。

### 2.8.6.3. ライブストレージ移行の概要

仮想ディスクは、それらが接続されている仮想マシンの実行中に、あるストレージドメインから別のストレージドメインに移行できます。これは、ライブストレージ移行と呼ばれます。実行中の仮想マシンに接続されているディスクが移行されると、そのディスクのイメージチェーンのスナップショットがソースストレージドメインに作成され、イメージチェーン全体が宛先ストレージドメインに複製されます。そのため、ソースストレージドメインと宛先ストレージドメインの両方に、ディスクイメージチェーンとスナップショットの両方をホストするのに十分なストレージスペースがあることを確認する必要があります。移行が失敗した場合でも、ライブストレージの移行が試行されるたびに新しいスナップショットが作成されます。

ライブストレージ移行を使用する場合は、次の点を考慮してください。

- 一度に複数のディスクをライブマイグレーションできます。
- 同じ仮想マシンの複数のディスクは複数のストレージドメインにまたがって存在できますが、各ディスクのイメージチェーンは単一のストレージドメインに存在する必要があります。
- 同じデータセンター内の任意の 2 つのストレージドメイン間でディスクをライブマイグレーションできます。
- ダイレクト LUN ハードディスクイメージまたは共有可能としてマークされたディスクをライブマイグレーションすることはできません。

### 2.8.6.4. 仮想ディスクの移動

仮想マシンに接続されている、またはフローティング仮想ディスクとして機能する仮想ディスクを、あるストレージドメインから別のストレージドメインに移動します。実行中の仮想マシンに接続されている仮想ディスクを移動できます。これは、ライブストレージ移行と呼ばれます。別の方針として、続行する前に仮想マシンをシャットダウンします。

ディスクを移動するときは、次の点を考慮してください。

- 複数のディスクを同時に移動できます。
- 同じデータセンター内の任意の 2 つのストレージドメイン間でディスクを移動できます。
- テンプレートに基づいて作成され、シンプロビジョンングストレージ割り当てオプションを使用した仮想マシンに仮想ディスクが接続されている場合は、仮想マシンのベースとなったテンプレートのディスクを、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

1. Storage → Disks をクリックして、移動する 1 つ以上の仮想ディスクを選択します。
2. Move をクリックします。
3. Target リストから、仮想ディスクの移動先のストレージドメインを選択します。

4. 必要に応じて、Disk Profile リストからディスクのプロファイルを選択します。

5. OK をクリックします。

仮想ディスクは、対象のストレージドメインに移動します。移動の手順の中で、Status 列には **Locked** が表示され、移動操作の進捗を示す進捗バーが表示されます。

#### 2.8.6.5. ディスクインターフェイスタイプの変更

ユーザーは、ディスク作成後にディスクのインターフェイスタイプを変更できます。これにより、既存のディスクを、異なるインターフェイスタイプを必要とする仮想マシンに接続できます。たとえば、**VirtIO** インターフェイスを使用するディスクは、**VirtIO-SCSI** または **IDE** インターフェイスを必要とする仮想マシンに接続できます。これにより、バックアップと復元、または障害復旧の目的でディスクを移行する柔軟性が提供されます。共有可能ディスクのディスクインターフェイスは、仮想マシンごとに更新することもできます。これは、共有ディスクを使用する各仮想マシンが異なるインターフェイスタイプを使用できることを意味します。

ディスクインターフェイスタイプを更新するには、最初にディスクを使用するすべての仮想マシンを停止する必要があります。

##### ディスクインターフェイスタイプの変更\*

1. Compute → Virtual Machines をクリックして、該当する仮想マシンを停止します。
2. 仮想マシンの名前をクリックします。詳細ビューが開きます。
3. Disks タブをクリックして、ディスクを選択します。
4. Edit をクリックします。
5. Interface リストから、新しいインターフェイスタイプを選択し、OK をクリックします。

別のインターフェイスタイプを必要とする別の仮想マシンにディスクを接続できます。

##### 別のインターフェイスタイプを使用して別の仮想マシンにディスクを接続

1. Compute → Virtual Machines をクリックして、該当する仮想マシンを停止します。
2. 仮想マシンの名前をクリックします。詳細ビューが開きます。
3. Disks タブをクリックして、ディスクを選択します。
4. Remove をクリックしてから OK をクリックします。
5. Virtual Machines に戻り、ディスクが割り当てられる新しい仮想マシンの名前をクリックします。
6. Disks タブをクリックしてから Attach をクリックします。
7. Attach Virtual Disks ウィンドウでディスクを選択し、Interface ドロップダウンから適切なインターフェイスを選択します。
8. OK をクリックします。

#### 2.8.6.6. 仮想ディスクのコピー

あるストレージドメインから別のストレージドメインに仮想ディスクをコピーできます。コピーしたディスクは仮想マシンに接続できます。

## 手順

1. Storage → Disks をクリックして、仮想ディスクを選択します。
2. Copy をクリックします。
3. 必要に応じて、Alias フィールドに新しい名前を入力します。
4. Target リストから、仮想ディスクのコピー先のストレージドメインを選択します。
5. 必要に応じて、Disk Profile リストからディスクのプロファイルを選択します。
6. OK をクリックします。

コピー中の仮想ディスクのステータスは **Locked** です。

### 2.8.6.7. ディスクパフォーマンスの向上

管理ポータルの仮想マシンの Resource Allocation タブで、デフォルトの I/O Threads Enabled 設定がオン(有効)になっており、スレッド数は 1 です。

仮想マシンに VirtIO コントローラーを備えた複数のディスクがあり、そのワークロードがそれらのコントローラーを大幅に利用しているとします。その場合、I/O スレッドの数を増やすことで、パフォーマンスが向上します。

ただし、I/O スレッドの数を増やすと、仮想マシンのスレッドプールが減少することも考慮してください。ワークロードが VirtIO コントローラーとそれに割り当てたスレッドを使用しない場合は、I/O スレッドの数を増やすと全体的なパフォーマンスが低下する可能性があります。

最適なスレッド数を見つけるには、スレッド数を調整する前後に、ワークロードを実行している仮想マシンのパフォーマンスをベンチマークします。

## 手順

1. Compute → Virtual Machines で、仮想マシンの 電源をオフ にします。
2. 仮想マシンの名前をクリックします。
3. 詳細ペインで、Vm Devices タブをクリックします。
4. Type が **virtio** または **virtio-scsi** であるコントローラーの数を数えます。
5. Edit をクリックします。
6. Edit Virtual Machine ウィンドウで、Resource Allocation タブをクリックします。
7. I/O Threads Enabled がチェックされている(有効になっている)ことを確認します。
8. I/O Threads Enabled の右側で、スレッドの数を増やしますが、タイプが **virtio** または **virtio-scsi** であるコントローラーの数を超えないようにします。
9. OK をクリックします。
10. 詳細ペインで、Disks タブをクリックします。

11. ディスクごとに、More Actions (⋮) を使用して、ディスクを 非アクティブ化 および アクティブ化 します。このアクションにより、ディスクがコントローラーに再マップされます。
12. Run をクリックして、仮想マシンを起動します。

## 検証手順

- どのコントローラーに I/O スレッドがあるかを確認するには、詳細ペインで Vm Devices をクリックし、Spec Params 列で **ioThreadid=** を探します。
- ディスクからコントローラへのマッピングを確認するには、ホストマシンにログインして、次のコマンドを入力します。

```
virsh -r dumpxml virtual_machine_name
```

## 関連情報

- 高パフォーマンスの仮想マシンテンプレートおよびプールの設定
- 仮想マシンのリソース割り当て設定に関する説明

### 2.8.6.8. データストレージドメインへのイメージのアップロード

管理ポータルまたは REST API を使用して、仮想ディスクイメージと ISO イメージをデータストレージドメインにアップロードできます。詳細は、[データストレージドメインへのイメージのアップロード](#) を参照してください。

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

インポートされたストレージドメインからフローティング仮想ディスクをインポートできます。



#### 注記

Manager にインポートできるのは QEMU 互換ディスクのみです。

## 手順

1. Storage → Domains をクリックします。
2. インポートされたストレージドメインの名前をクリックします。詳細ビューが開きます。
3. Disk Import タブをクリックします。
4. 1つ以上のディスクを選択し、Import をクリックします。
5. 各ディスクに適切な Disk Profile を選択します。
6. OK をクリックします。

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

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できます。Red Hat Virtualization 環境の外部で作成されたフローティングディスクは、Manager には登録されません。ストレージドメインをスキャンして、インポートする未登録のフローティングディスクを特定します。



## 注記

Manager にインポートできるのは QEMU 互換ディスクのみです。

## 手順

1. Storage → Domains をクリックします。
2. ストレージドメインの名前をクリックします。詳細ビューが開きます。
3. More Actions (⋮) をクリックしてから、Manager が未登録のディスクを特定できるよう に、Scan Disks ディスクをクリックします。
4. Disk Import タブをクリックします。
5. 1つ以上のディスクリメージを選択し、Import をクリックします。
6. 各ディスクに適切な Disk Profile を選択します。
7. OK をクリックします。

### 2.8.6.11. OpenStack Image Service からの仮想ディスクのインポート

OpenStack Image サービスが外部プロバイダーとして Manager に追加されている場合は、その OpenStack Image サービスが管理する仮想ディスクを Red Hat Virtualization Manager にインポートすることができます。

1. Storage → Domains をクリックします。
2. OpenStack Image Service ドメインの名前をクリックします。詳細ビューが開きます。
3. Images タブをクリックして、イメージを選択します。
4. Import をクリックします。
5. イメージをインポートする データセンター を選択します。
6. Domain Name ドロップダウンリストから、イメージが保存されるストレージドメインを選択します。
7. 必要に応じて、Quota ドロップダウンリストからイメージに適用するクオータを選択します。
8. OK をクリックします。

これで、ディスクを仮想マシンに接続できます。

### 2.8.6.12. OpenStack Image Service への仮想ディスクのエクスポート

仮想ディスクは、外部プロバイダーとして Manager に追加された OpenStack Image Service にエクスポートできます。



## 重要

仮想ディスクは、複数のボリュームがなく、シンプロビジョンングされておらず、スナップショットがない場合にのみエクスポートできます。

1. Storage → Disks をクリックして、エクスポートするディスクを選択します。
2. More Actions (⋮) をクリックしてから、Export をクリックします。
3. Domain Name ドロップダウンリストから、ディスクのエクスポート先となる OpenStack Image Service を選択します。
4. クオータを適用する場合は、Quota ドロップダウンリストからディスクのクオータを選択します。
5. OK をクリックします。

#### 2.8.6.13. 仮想ディスクスペースの回収

シンプロビジョニングを使用する仮想ディスクは、ファイルを削除した後、自動的に縮小しません。たとえば、実際のディスクサイズが 100 GB で、50 GB のファイルを削除した場合、割り当てられたディスクサイズは 100GB のままであり、残りの 50 GB はホストに返されないため、他の仮想マシンで使用できません。この未使用的ディスク領域は、仮想マシンのディスクでスペース操作を実行することにより、ホストによって再利用できます。これにより、空き領域がディスクイメージからホストに転送されます。複数の仮想ディスクを並行してスペース化できます。

この操作は、仮想マシンのクローンを作成する前、仮想マシンに基づいてテンプレートを作成する前、またはストレージドメインのディスク領域をクリーンアップする前に実行してください。

#### 制限

- NFS ストレージドメインは、NFS バージョン 4.2 以降を使用する必要があります。
- ダイレクト LUN を使用するディスクをスペース化することはできません。
- 事前に割り当てられた割り当てポリシーを使用するディスクをスペース化することはできません。テンプレートから仮想マシンを作成する場合は、Storage Allocation フィールドから Thin を選択する必要があります。Clone を選択する場合は、テンプレートがシンプロビジョニングのある仮想マシンに基づいていることを確認してください。
- アクティブなスナップショットのみをスペースできます。

#### ディスクのスペース化

1. Compute → Virtual Machines をクリックして、必要な仮想マシンをシャットダウンします。
2. 仮想マシンの名前をクリックします。詳細ビューが開きます。
3. Disks タブをクリックします。ディスクのステータスが OK であることを確認します。
4. More Actions (⋮) をクリックしてから、Sparsify をクリックします。
5. OK をクリックします。

**Started to sparsify** イベントは、スペース化操作中に Events タブに表示され、ディスクのステータスは Locked と表示されます。操作が完了すると、**Sparsified successfully** イベントが Events タブに表示され、ディスクのステータスが OK と表示されます。これで未使用的ディスク領域はホストに戻され、他の仮想マシンで使用できるようになりました。

## 2.9. 外部プロバイダー

## 2.9.1. Red Hat Virtualization における外部プロバイダーの紹介

Red Hat Virtualization は、Red Hat Virtualization Manager が管理するリソースに加え、外部ソースが管理するリソースも利用できます。外部プロバイダーと呼ばれるこれらのリソースのプロバイダーは、仮想化ホスト、仮想マシンイメージ、ネットワークなどのリソースを提供できます。

Red Hat Virtualization は現在、以下の外部プロバイダーをサポートしています。

### ホストプロビジョニング用の Red Hat Satellite

Satellite は、物理ホストと仮想ホストのライフサイクルのあらゆる側面を管理するためのツールです。Red Hat Virtualization では、Satellite によって管理されるホストを、Red Hat Virtualization Manager に仮想化ホストとして追加して使用できます。Manager に Satellite インスタンスを追加した後、新しいホストを追加するときにその Satellite インスタンスで使用可能なホストを検索することにより、Satellite インスタンスが管理するホストを追加できます。Red Hat Satellite のインストールおよび Red Hat Satellite を使用したホストの管理に関する詳細は、[Red Hat Satellite クイックスタートガイド](#) および [Red Hat Satellite ホストの管理](#) を参照してください。

### KubeVirt/OpenShift Virtualization

OpenShift Virtualization (以前のコンテナーネイティブ仮想化または "CNV") を使用すると、仮想マシン (VM) をコンテナー化されたワークフローに組み込むことができるため、仮想マシンをコンテナーおよびサーバーレスと並行して開発、管理、およびデプロイできます。RHV Manager で、このプロバイダーを追加することは、OpenShift Virtualization を使用するための要件の1つです。詳細は、[KubeVirt/OpenShift Virtualization を外部プロバイダーとして追加](#) を参照してください。

### イメージ管理用の OpenStack Image Service (Glance)

OpenStack Image Service は、仮想マシンイメージのカタログを提供します。Red Hat Virtualization では、これらのイメージを Red Hat Virtualization Manager にインポートして、フローティングディスクとして使用したり、仮想マシンに接続してテンプレートに変換したりできます。OpenStack Image Service を Manager に追加すると、どのデータセンターにも接続されていないストレージドメインとして表示されます。Red Hat Virtualization 環境の仮想ディスクは、仮想ディスクとして OpenStack Image Service にエクスポートすることもできます。



#### 注記

OpenStack Glance のサポートは非推奨になりました。この機能は今後のリリースで削除されます。

### 仮想マシンプロビジョニング用の VMware

VMware で作成された仮想マシンは、V2V (**virt-v2v**) を使用して変換し、Red Hat Virtualization 環境にインポートできます。VMware プロバイダーを Manager に追加した後、それが提供する仮想マシンをインポートできます。V2V 変換は、インポート操作の一部として、指定されたプロキシーホストで実行されます。

### 仮想マシンプロビジョニング用の RHEL 5 Xen

RHEL 5 Xen で作成された仮想マシンは、V2V (**virt-v2v**) を使用して変換し、Red Hat Virtualization 環境にインポートできます。RHEL 5 Xen ホストを Manager に追加した後、それが提供する仮想マシンをインポートできます。V2V 変換は、インポート操作の一部として、指定されたプロキシーホストで実行されます。

### 仮想マシンプロビジョニング用の KVM

KVM で作成された仮想マシンは、Red Hat Virtualization 環境にインポートできます。KVM ホストを Manager に追加した後、KVM ホストが提供する仮想マシンをインポートできます。

### ネットワークプロビジョニング用の Open Virtual Network (OVN)

Open Virtual Network (OVN) は、ソフトウェア定義のネットワークを提供する Open vSwitch (OVS) 拡張機能です。Manager に OVN を追加した後、既存の OVN ネットワークをインポートし、

Manager から新しい OVN ネットワークを作成できます。**engine-setup** を使用して、Manager に OVN を自動的にインストールすることもできます。

## 2.9.2. 外部プロバイダーの追加

### 2.9.2.1. ホストのプロビジョニングに使用する Red Hat Satellite インスタンスの追加

ホストプロビジョニング用の Satellite インスタンスを Red Hat Virtualization Manager に追加します。Red Hat Virtualization 4.2 は、Red Hat Satellite 6.1 でサポートされています。

#### 手順

1. Administration → Providers をクリックします。
2. Add をクリックします。
3. Name および Description を入力します。
4. Type ドロップダウンリストから Foreman/Satellite を選択します。
5. Satellite インスタンスがインストールされているマシンの URL または完全修飾ドメイン名を Provider URL テキストフィールドに入力します。ポート番号を指定する必要はありません。



#### 重要

IP アドレスを使用して Satellite インスタンスを追加することはできません。

6. Requires Authentication チェックボックスをオンにします。
7. Satellite インスタンスの Username と Password を入力します。Satellite プロビジョニングポータルへのログインに使用するのと同じユーザー名とパスワードを使用する必要があります。
8. 認証情報をテストします。
  - a. Test をクリックし、提供された認証情報を使用して Satellite インスタンスで正常に認証できるかどうかをテストします。
  - b. Satellite インスタンスが SSL を使用している場合は、Import provider certificates ウィンドウが開きます。OK をクリックして、Satellite インスタンスが提供する証明書をインポートし、Manager がインスタンスと通信できるようにします。
9. OK をクリックします。

### 2.9.2.2. イメージ管理用の OpenStack Image (Glance) インスタンスの追加



#### 注記

OpenStack Glance のサポートは非推奨になりました。この機能は今後のリリースで削除されます。

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

## 手順

1. Administration → Providers をクリックします。
2. Add をクリックし、General Settings タブに詳細を入力します。これらのフィールドの詳細は、[Add Provider の General 設定に関する説明](#) を参照してください。
3. Name および Description を入力します。
4. Type ドロップダウンリストから OpenStack Image を選択します。
5. OpenStack Image インスタンスがインストールされているマシンの URL または完全修飾ドメイン名を Provider URL テキストフィールドに入力します。
6. 必要に応じて、Requires Authentication チェックボックスを選択し、Keystone に登録されている OpenStack Image インスタンスユーザーの Username 名と Password を入力します。Protocol (HTTP である必要があります)、Hostname、および API Port. を定義して Keystone サーバーの認証 URL を定義する必要があります。OpenStack Image インスタンスの Tenant を入力します。
7. 認証情報をテストします。
  - a. Test をクリックし、提供された認証情報を使用して OpenStack Image インスタンスで正常に認証できるかどうかをテストします。
  - b. OpenStack Image インスタンスが SSL を使用している場合、Import provider certificates ウィンドウが開きます。OK をクリックして、OpenStack Image インスタンスが提供する証明書をインポートし、Manager がインスタンスと通信できるようにします。
8. OK をクリックします。

### 2.9.2.3. KubeVirt/OpenShift Virtualization を外部プロバイダーとして追加

OpenShift Container Platform のコンテナーで仮想マシンを実行するには、Red Hat Virtualization の外部プロバイダーとして OpenShift を追加します。



#### 注記

この機能は、OpenShift Virtualization として知られています。

## 前提条件

- OpenShift Container Platform でクラスターが OpenShift Virtualization 用に設定されている。

## 手順

1. RHV 管理ポータルで、Administration → Providers に移動し、New をクリックします。
2. Add Provider で、Type を KubeVirt/OpenShift Virtualization に設定します。
3. 必要な Provider URL と Token を入力します。
4. オプション: Certificate Authority、Prometheus URL、Prometheus Certificate Authority などの Advanced parameters の値を入力します。
5. Test をクリックして、新しいプロバイダーへの接続を確認します。

6. **OK** をクリックして、この新しいプロバイダーの追加を終了します。

## 検証手順

1. RHV 管理ポータルで、Compute → Clusters をクリックします。
2. 作成した新しいクラスターの名前をクリックします。このクラスターネーム(たとえば、**kubevirt**)は、プロバイダーの名前に基づいています。このアクションにより、クラスターの詳細ビューが開きます。
3. **Hosts** タブをクリックして、OpenShift Container Platform ワーカーノードのステータスが **up** となっていることを確認します。



### 注記

コントロールプレーンノードのステータスは、仮想マシンをホストできないため、実行中であっても **down** となっています。

4. Compute → Virtual Machines を使用して、仮想マシンを新しいクラスターにデプロイします。
5. OpenShift Container Platform Web コンソールの Administrator パースペクティブで、Workloads → Virtual Machines を使用して、デプロイした仮想マシンを表示します。

## 関連情報

- [OpenShift Virtualization について](#)
- [Add Provider の General 設定に関する説明](#)

### 2.9.2.4. VMware インスタンスを仮想マシンプロバイダーとして追加

VMware vCenter インスタンスを追加して、仮想マシンを VMware から Red Hat Virtualization Manager にインポートします。

Red Hat Virtualization は、V2V を使用して、VMware 仮想マシンをインポートする前に正しい形式に変換します。**virt-v2v** パッケージが、1つ以上のホストにインストールされている必要があります。Red Hat Virtualization Host (RHVH) では、**virt-v2v** パッケージがデフォルトで利用でき、Red Hat Virtualization 環境に追加されると、Red Hat Enterprise Linux ホストに VDSM の依存関係としてインストールされます。Red Hat Enterprise Linux ホストが、Red Hat Enterprise Linux 7.2 以降を使用している。



### 注記

ppc64le アーキテクチャーで **virt-v2v** パッケージは使用できません。これらのホストはプロキシーホストとして使用できません。

## 手順

1. Administration → Providers をクリックします。
2. Add をクリックします。
3. Name および Description を入力します。

4. **Type** ドロップダウンリストから **VMware** を選択します。
5. **VMware** 仮想マシンをインポートする **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宛先データセンターを指定します。
6. **vCenter** フィールドに VMware vCenter インスタンスの IP アドレスまたは完全修飾ドメイン名を入力します。
7. **ESXi** フィールドに仮想マシンをインポートするホストの IP アドレスまたは完全修飾ドメイン名を入力します。
8. 指定した ESXi ホストが存在するデータセンターの名前を **Data Center** フィールドに入力します。
9. ESXi ホストと Manager との間で SSL 証明書を交換した場合は、**Verify server's SSL certificate** チェックボックスを選択したままにして、ESXi ホストの証明書を確認します。交換していない場合は、チェックボックスの選択を解除します。
10. 仮想マシンのインポート操作中に **Proxy Host** として機能するように、**virt-v2v** がインストールされている、選択したデータセンター内のホストを選択します。このホストは、VMware vCenter 外部プロバイダーのネットワークに接続できる必要があります。上記の **Any Data Center** を選択した場合、ここでホストは選択できませんが、代わりに、個別のインポート操作時にホストを指定できます。
11. VMware vCenter インスタンスの **Username** および **Password** を入力します。ユーザーは、仮想マシンが置かれている VMware データセンターおよび ESXi ホストにアクセスできる必要があります。
12. 認証情報をテストします。
  - a. **Test** をクリックし、提供された認証情報を使用して VMware vCenter インスタンスで正常に認証できるかどうかをテストします。
  - b. VMware vCenter インスタンスが SSL を使用している場合は、**Import provider certificates** ウィンドウが開きます。**OK** をクリックして、VMware vCenter インスタンスが提供する証明書をインポートし、Manager がインスタンスと通信できるようにします。
13. **OK** をクリックします。

VMware 外部プロバイダーから仮想マシンをインポートするには、**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。

### 2.9.2.5. RHEL 5 Xen ホストを仮想マシンプロバイダーとして追加

RHEL 5 Xen ホストを追加して、仮想マシンを Xen から Red Hat Virtualization にインポートします。

Red Hat Virtualization は、V2V を使用して、RHEL 5 Xen 仮想マシンをインポートする前に正しい形式に変換します。**virt-v2v** パッケージが、1つ以上のホストにインストールされている必要があります。Red Hat Virtualization Host (RHVH) では、**virt-v2v** パッケージがデフォルトで利用でき、Red Hat Virtualization 環境に追加されると、Red Hat Enterprise Linux ホストに VDSM の依存関係としてインストールされます。Red Hat Enterprise Linux ホストが、Red Hat Enterprise Linux 7.2 以降を使用している。



#### 注記

ppc64le アーキテクチャーで **virt-v2v** パッケージは使用できません。これらのホストはプロキシホストとして使用できません。

## 手順

1. プロキシホストと RHEL 5 ホスト間の公開鍵認証を有効にします。

- a. プロキシホストにログインし、`vdsdm` ユーザーの SSH キーを生成します。

```
sudo -u vdsdm ssh-keygen
```

- b. `vdsdm` ユーザーの公開鍵を RHEL 5 Xen ホストにコピーします。プロキシホストの `known_hosts` ファイルも更新され、RHEL 5 Xen ホストのホストキーが追加されます。

```
sudo -u vdsdm ssh-copy-id root@xenhost.example.com
```

- c. RHEL 5 Xen ホストにログインして、ログインが正常に機能していることを確認します。

```
sudo -u vdsdm ssh root@xenhost.example.com
```

2. Administration → Providers をクリックします。

3. Add をクリックします。

4. Name および Description を入力します。

5. Type ドロップダウンリストから XEN を選択します。

6. Xen 仮想マシンをインポートする 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宛先データセンターを指定します。

7. URI フィールドに RHEL 5 Xen ホストの URI を入力します。

8. 仮想マシンのインポート操作中に Proxy Host として機能するように、virt-v2v がインストールされている、選択したデータセンター内のホストを選択します。このホストは、RHEL 5 Xen 外部プロバイダーのネットワークにも接続できる必要があります。上記の Any Data Center を選択した場合、ここでホストは選択できませんが、代わりに、個別のインポート操作時にホストを指定できます。

9. Test をクリックして、RHEL 5 Xen ホストで正常に認証できるかどうかをテストします。

10. OK をクリックします。

RHEL 5 Xen 外部プロバイダーから仮想マシンをインポートするには、仮想マシン管理ガイドの [RHEL 5 Xen ホストからの仮想マシンのインポート](#) を参照してください。

### 2.9.2.6. KVM ホストを仮想マシンプロバイダーとして追加

KVM ホストを追加して、仮想マシンを KVM から Red Hat Virtualization Manager にインポートします。

## 手順

1. プロキシホストと KVM ホスト間の公開鍵認証を有効にします。

- a. プロキシホストにログインし、`vdsdm` ユーザーの SSH キーを生成します。

```
sudo -u vdsdm ssh-keygen
```

- b. **vdsm** ユーザーの公開鍵を KVM ホストにコピーします。プロキシホストの `known_hosts` ファイルも更新され、KVM ホストのホストキーが追加されます。

```
sudo -u vdsm ssh-copy-id root@kvmhost.example.com
```

- c. KVM ホストにログインして、ログインが正常に機能していることを確認します。

```
sudo -u vdsm ssh root@kvmhost.example.com
```

2. Administration → Providers をクリックします。

3. Add をクリックします。

4. Name および Description を入力します。

5. Type ドロップダウンリストから KVM を選択します。

6. KVM 仮想マシンをインポートする 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宛先データセンターを指定します。

7. URI フィールドに KVM ホストの URI を入力します。

```
qemu+ssh://root@host.example.com/system
```

8. 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 プロキシホスト として機能するホストを選択します。このホストは、KVM 外部プロバイダーのネットワークにも接続できる必要があります。上記の Data Center フィールドで Any Data Center を選択した場合、ここでホストを選択することはできません。フィールドはグレー表示され、Any Host in Data Center が表示されます。代わりに、個別のインポート操作中にホストを指定できます。

9. 必要に応じて、Requires Authentication チェックボックスを選択し、KVM ホストの Username 名と Password を入力します。ユーザーは、仮想マシンが存在する KVM ホストにアクセスできる必要があります。

10. Test をクリックし、提供された認証情報を使用して、KVM ホストで正常に認証できるかどうかをテストします。

11. OK をクリックします。

KVM 外部プロバイダーから仮想マシンをインポートするには、仮想マシン管理ガイドの [KVM ホストからの仮想マシンのインポート](#) を参照してください。

### 2.9.2.7. オープン仮想ネットワーク (OVN) を外部ネットワークプロバイダーとして追加

Open Virtual Network (OVN) を使用して、VLAN を追加したりインフラストラクチャーを変更したりすることなく、仮想マシン間の通信を可能にするオーバーレイ仮想ネットワークを作成できます。OVN は、Open vSwitch (OVS) の拡張機能であり、仮想 L2 および L3 オーバーレイのネイティブサポートを提供します。

OVN ネットワークをネイティブの Red Hat Virtualization ネットワークに接続することもできます。詳細は、[OVN ネットワークの物理ネットワークに接続](#) を参照してください。この機能は、テクノロジープレビューとしてのみ利用できます。

**ovirt-provider-ovn** は、OpenStack Networking REST API を公開します。この API を使用して、ネットワーク、サブネット、ポート、およびルーターを作成できます。詳細は、[OpenStack Networking API v2.0](#) を参照してください。

詳細は、[Open vSwitch のドキュメント](#) および [Open vSwitch Manpages](#) を参照してください。

### 2.9.2.7.1. 新しい OVN ネットワークプロバイダーのインストール

**engine-setup** を使用して OVN をインストールすると、次の手順が実行されます。

- Manager マシンに OVN 中央サーバーをセットアップします。
- 外部ネットワークプロバイダーとして OVN を Red Hat Virtualization に追加します。
- デフォルトクラスターの場合のみ、Default Network Provider を **ovirt-provider-ovn** に設定します。



#### 重要

- OVN をインストールすると、デフォルトクラスターの Default Network Provider 設定が変更され、他のクラスターでは変更されません。
- Default Network Provider 設定を変更しても、そのクラスター内のホストは デフォルトネットワークプロバイダーを使用するように更新されません。
- ホストと仮想マシンで OVN を使用するには、このトピックの最後にある "次の手順" で説明されている追加タスクを実行します。

#### 手順

- オプション: **engine-setup** で事前設定されたアンサーファイルを使用する場合は、次のエントリーを追加して OVN をインストールします。

OVESETUP\_OVN/ovirtProviderOvn=bool:True

- Manager マシンで **engine-setup** を実行します。

- 事前設定されたアンサーファイルを使用しない場合は、**engine-setup** が次のように要求したときに **Yes** と答えます。

Configuring ovirt-provider-ovn also sets the Default cluster's default network provider to ovirt-provider-ovn.

Non-Default clusters may be configured with an OVN after installation.

Configure ovirt-provider-ovn (Yes, No) [Yes]:

- 以下の質問に答えてください。

Use default credentials (admin@internal) for ovirt-provider-ovn (Yes, No) [Yes]?:

**Yes** の場合、**engine-setup** は、セットアッププロセスの前半で指定されたデフォルトのエンジニアユーザーとパスワードを使用します。このオプションは、新規インストール時にのみ使用できます。

oVirt OVN provider user[admin]:

oVirt OVN provider password[empty]:

デフォルト値を使用するか、oVirt OVN プロバイダーのユーザーとパスワードを指定できます。



## 注記

後で認証方法を変更するには、`/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf` ファイルを編集するか、新しい `/etc/ovirt-provider-ovn/conf.d/20_engine_setup.conf` ファイルを作成します。変更を有効にするには、**ovirt-provider-ovn** サービスを再起動します。OVN 認証の詳細は [oVirt external network provider for OVN](#) を参照してください。

## 次のステップ

新しくインストールされた OVN ネットワークを使用する仮想マシンを作成する前に、次の追加手順を実行してください。

1. **Default** クラスターにネットワークを追加します。
  - a. その際、**Create on external provider** をオンにします。これにより、**ovirt-provider-ovn** に基づくネットワークが作成されます。
  - b. オプション: [OVN ネットワークを物理ネットワークに接続](#) するには、**Connect to physical network** チェックボックスをオンにして、使用する Red Hat Virtualization ネットワークを指定します。
  - c. オプション: ネットワークでセキュリティグループを使用するかどうかを決定し、**Security Groups** ドロップダウンからセキュリティグループを選択します。使用可能なオプションの詳細は、[論理ネットワークの一般設定の説明](#) を参照してください。
2. デフォルトクラスターに [ホストを追加する](#) か、[ホストを再インストール](#) して、クラスターの新しい [デフォルトネットワークプロバイダー](#) である **ovirt-provider-ovn** を使用するようにします。
3. オプション: デフォルト以外のクラスターを編集し、[デフォルトネットワークプロバイダー](#) を **ovirt-provider-ovn** に設定します。
  - a. オプション: デフォルト以外の各クラスターにホストを再インストールして、クラスターの新しい [デフォルトネットワークプロバイダー](#) である **ovirt-provider-ovn** を使用するようにします。

## 関連情報

- デフォルト以外の既存のネットワークを使用するようにホストを設定するには、[OVN トンネルネットワークのホストの設定](#) を参照してください。

### 2.9.2.7.2. 単一ホスト上の OVN トンネルネットワークの更新

**vdsm-tool** を使用して、単一のホスト上の OVN トンネルネットワークを更新できます。

```
vdsm-tool ovn-config OVN_Central_IP Tunneling_IP_or_Network_Name Host_FQDN
```



## 注記

Host\_FQDN は、このホストのエンジンで指定されている FQDN と一致する必要があります。

### 例2.4 vdsm-tool を使用したホストの更新

```
vdsm-tool ovn-config 192.168.0.1 MyNetwork MyFQDN
```

#### 2.9.2.7.3. OVN ネットワークを物理ネットワークに接続



## 重要

この機能は、Red Hat Virtualization のテクノロジープレビューとしてのみ利用可能な Open vSwitch サポートに依存しています。テクノロジープレビュー機能は、実稼働環境での Red Hat サービスレベルアグリーメント (SLA) ではサポートされておらず、機能的に完全ではない可能性があるため、Red Hat では実稼働環境での使用を推奨していません。テクノロジープレビュー機能では、最新の製品機能をいち早く提供します。これにより、お客様は開発段階で機能をテストし、フィードバックを提供できます。

Red Hat のテクノロジープレビュー機能のサポートの詳細は、[テクノロジープレビュー機能のサポート範囲](#) を参照してください。

ネイティブの Red Hat Virtualization ネットワークをオーバーレイする外部プロバイダーネットワークを作成して、それぞれの仮想マシンが同じサブネットを共有しているように見せることができます。



## 重要

OVN ネットワークのサブネットを作成した場合、そのネットワークを使用する仮想マシンはそこから IP アドレスを受け取ります。物理ネットワークに IP アドレスを割り当てる場合は、OVN ネットワークのサブネットを作成しないでください。

#### 前提条件

- クラスターで、**Switch Type** として **OVS** が選択されている。このクラスターに追加されたホストには、**ovirtmgmt** ブリッジなどの既存の Red Hat Virtualization ネットワークを設定ではありません。
- ホストで物理ネットワークを使用できる。そのためには、(Manage Networks ウィンドウ、または New Logical Network ウィンドウの Cluster タブで) クラスターに必要な物理ネットワークを設定します。

#### 手順

- Compute → Clusters をクリックします。
- クラスターの名前をクリックします。詳細ビューが開きます。
- Logical Networks タブをクリックし、Add Network をクリックします。
- ネットワークの Name を入力します。

5. **Create on external provider** チェックボックスをオンにします。デフォルトでは、**ovirt-provider-ovn** が選択されています。
6. デフォルトで選択されていない場合は、**Connect to physical network** チェックボックスをオンにします。
7. 新しいネットワークを接続する物理ネットワークを選択します。
  - **Data Center Network** ラジオボタンをクリックし、ドロップダウンリストから物理ネットワークを選択します。これは推奨されるオプションです。
  - **Custom** ラジオボタンをクリックして、物理ネットワークの名前を入力します。物理ネットワークで VLAN タギングが有効になっている場合は、**Enable VLAN tagging** チェックボックスをオンにして、物理ネットワークの VLAN タグも入力する必要があります。



### 重要

物理ネットワークの名前は 15 文字以下とし、特殊文字は使用できません。

8. **OK** をクリックします。

```
////Removing for BZ2006228
include::topics/Adding_an_External_Network_Provider.adoc[leveloffset=+2]
```

#### 2.9.2.8. Add Provider の General 設定に関する説明

Add Provider ウィンドウの **General** タブでは、外部プロバイダーのコアの詳細を登録できます。

表2.38 Add Provider: General 設定

設定	説明
Name	Manager でプロバイダーを表す名前。
Description	人間が判読可能なプレーンテキストで記述されたプロバイダーの説明。
Type	<p>外部プロバイダーのタイプ。この設定を変更すると、プロバイダーの設定に使用できるフィールドが変更されます。</p> <p><b>External Network Provider</b></p> <ul style="list-style-type: none"> <li>● <b>Networking Plugin:</b> NIC 操作を処理するのにホストで使用されるドライバーの実装を決定します。<b>oVirt Network Provider for OVN</b> プラグインを備えた外部ネットワークプロバイダーがクラスターのデフォルトネットワークプロバイダーとして追加されると、それに応じて、クラスターに追加されたホストにインストールされるドライバーも決まります。</li> <li>● <b>Automatic Synchronization:</b> プロバイダーが既存のネットワークと自動的に同期されるかどうかを指定できます。</li> </ul>

設定	説明
	<ul style="list-style-type: none"> <li>● <b>Provider URL:</b> 外部ネットワークプロバイダーがホストされるマシンの URL または完全修飾ドメイン名。外部ネットワークプロバイダーのポート番号を URL または完全修飾ドメイン名の末尾に追加する必要があります。デフォルトでは、このポート番号は 9696 です。</li> <li>● <b>Read Only:</b> 管理ポータルから外部ネットワークプロバイダーを変更できるかどうかを指定します。</li> <li>● <b>Requires Authentication:</b> 外部ネットワークプロバイダーにアクセスするために認証が必要であるかどうかを指定できます。</li> <li>● <b>Username:</b> 外部ネットワークプロバイダーに接続するためのユーザー名。Active Directory で認証する場合は、ユーザー名の形式は、デフォルトの <code>username@domain</code> ではなく、<code>username@domain@auth_profile</code> の形式にする必要があります。</li> <li>● <b>Password:</b> 上記のユーザー名が認証されるパスワード。</li> <li>● <b>Protocol:</b> Keystone サーバーと通信するために使用するプロトコル。デフォルトは <b>HTTPS</b> です。</li> <li>● <b>Hostname:</b> Keystone サーバーの IP アドレスまたはホスト名。</li> <li>● <b>API port:</b> Keystone サーバーの API ポート番号。</li> <li>● <b>API Version:</b> Keystone サーバーのバージョン。値は <b>v2.0</b> で、フィールドは無効になっています。</li> <li>● <b>Tenant Name:</b> 任意。外部ネットワークプロバイダーがメンバーになっているテナントの名前。</li> </ul> <p><b>Foreman/Satellite</b></p> <ul style="list-style-type: none"> <li>● <b>Provider URL:</b> Satellite インスタンスをホストするマシンの URL または完全修飾ドメイン名。URL または完全修飾ドメイン名の末尾にポート番号を追加する必要はありません。</li> <li>● <b>Requires Authentication:</b> プロバイダーに認証が必要かどうかを指定できます。<b>Foreman/Satellite</b> が選択されている場合、認証は必須です。</li> <li>● <b>Username:</b> Satellite インスタンスに接続するためのユーザー名。このユーザー名は、Satellite インスタンスのプロビジョニングポータルへのログインに使用されるユーザー名でなければなりません。</li> <li>● <b>Password:</b> 上記のユーザー名が認証される</li> </ul>

設定	説明
	<p>パスワード。このパスワードは、Satellite インスタンスのプロビジョニングポータルへのログインに使用するパスワードでなければなりません。</p>
	<h4>KubeVirt/OpenShift Virtualization</h4> <ul style="list-style-type: none"> <li>● <b>Provider URL:</b> OpenShift Container Platform API の URL または完全修飾ドメイン名、およびポート番号。デフォルトでは、このポート番号は 6443 です。</li> <li>● <b>Token:</b> API に対するこの接続を認証するための <a href="#">OAuth アクセストークン</a>。</li> <li>● <b>Certificate Authority:</b> https 要求の実行時に信頼される CA 証明書。</li> <li>● <b>Prometheus URL:</b> OpenShift クラスターの prometheus サービスの URL。この URL を指定しない場合、ソフトウェアはこの URL を自動的に検出しようとします。</li> <li>● <b>Prometheus Certificate Authority:</b> prometheus 用の X509 証明書この CA を指定しない場合、プロバイダーは代わりに KubeVirt CA を使用します。</li> </ul>
	<h4>OpenStack Image</h4> <ul style="list-style-type: none"> <li>● <b>Provider URL:</b> OpenStack Image Service がホストされているマシンの URL または完全修飾ドメイン名。OpenStack Image Service のポート番号を URL または完全修飾ドメイン名の末尾に追加する必要があります。デフォルトでは、このポート番号は 9292 です。</li> <li>● <b>Requires Authentication:</b> OpenStack Image サービスにアクセスするために認証が必要であるかどうかを指定できます。</li> <li>● <b>Username:</b> Keystone サーバーに接続するためのユーザー名このユーザー名は、OpenStack Image サービスが所属する Keystone インスタンスに登録されている OpenStack Image サービスのユーザー名でなければなりません。</li> <li>● <b>Password:</b> 上記のユーザー名が認証されるパスワード。このパスワードは、OpenStack Image サービスが所属する Keystone インスタンスに登録されている OpenStack Image サービスのパスワードでなければなりません。</li> <li>● <b>Protocol:</b> Keystone サーバーと通信するために使用するプロトコル。HTTP に設定する必要があります。</li> <li>● <b>Hostname:</b> Keystone サーバーの IP アドレスまたはホスト名。</li> <li>● <b>API port:</b> Keystone サーバーの API ポート番号。</li> </ul>

設定	説明
	<ul style="list-style-type: none"> <li>● <b>API Version:</b> Keystone サービスのバージョン。値は <b>v2.0</b> で、フィールドは無効になっています。</li> <li>● <b>Tenant Name:</b> OpenStack Image サービスが所属する OpenStack テナントの名前。</li> </ul>
	<h4>OpenStack Volume</h4> <ul style="list-style-type: none"> <li>● <b>Data Center:</b> OpenStack ボリュームのストレージボリュームが接続されるデータセンター。</li> <li>● <b>Provider URL:</b> OpenStack Volume インスタンスがホストされるマシンの URL または完全修飾ドメイン名。OpenStack Volume インスタンスのポート番号を、URL または完全修飾ドメイン名の末尾に追加する必要があります。デフォルトでは、このポート番号は 8776 です。</li> <li>● <b>Requires Authentication:</b> OpenStack ボリュームサービスへのアクセスに認証が必要であるかどうかを指定できます。</li> <li>● <b>Username:</b> Keystone サーバーに接続するためのユーザー名このユーザー名は、OpenStack Volume インスタンスが所属する Keystone インスタンスに登録されている OpenStack Volume のユーザー名でなければなりません。</li> <li>● <b>Password:</b> 上記のユーザー名が認証されるパスワード。このパスワードは、OpenStack Volume インスタンスが所属する Keystone インスタンスに登録されている OpenStack Volume のパスワードでなければなりません。</li> <li>● <b>Protocol:</b> Keystone サーバーと通信するために使用するプロトコル。<b>HTTP</b> に設定する必要があります。</li> <li>● <b>Hostname:</b> Keystone サーバーの IP アドレスまたはホスト名。</li> <li>● <b>API port:</b> Keystone サーバーの API ポート番号。</li> <li>● <b>API Version:</b> Keystone サーバーのバージョン。値は <b>v2.0</b> で、フィールドは無効になっています。</li> <li>● <b>テナント名:</b> OpenStack Volume インスタンスがメンバーになっている OpenStack テナントの名前。</li> </ul>
	<h4>VMware</h4> <ul style="list-style-type: none"> <li>● <b>Data Center:</b> VMware 仮想マシンがインポートされるデータセンターを指定するか、<b>Any Data Center</b> を選択して、(Virtual Machines タブの Import 機能を使用して) 個々のインポート操作中に宛先データセンターを指定します。</li> </ul>

設定	説明
	<ul style="list-style-type: none"> <li>● <b>vCenter:</b> 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。</li> <li>● <b>ESXi:</b> 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。</li> <li>● <b>Data Center:</b> 指定された ESXi ホストが存在するデータセンターの名前。</li> <li>● <b>Cluster:</b> 指定された ESXi ホストが存在するクラスターの名前。</li> <li>● <b>Verify server's SSL certificate:</b> 接続時に ESXi ホストの証明書を確認するかどうかを指定します。</li> <li>● <b>Proxy Host</b> 仮想マシンのインポート操作中にホストとして機能するように、選択したデータセンターの <b>virt-v2v</b> をインストールしたホストを選択します。このホストは、VMware vCenter 外部プロバイダーのネットワークに接続できる必要があります。Any Data Center を選択した場合は、ここでホストを選択することはできませんが、個別のインポート操作時にホストを指定できます (<b>Virtual Machines</b> タブの <b>Import</b> 機能を使用)。</li> <li>● <b>ユーザー名:</b> VMware vCenter インスタンスに接続するためのユーザー名。ユーザーは、仮想マシンが置かれている VMware データセンターおよび ESXi ホストにアクセスできる必要があります。</li> <li>● <b>Password:</b> 上記のユーザー名が認証されるパスワード。</li> </ul>
RHEL 5 Xen	<ul style="list-style-type: none"> <li>● <b>Data Center:</b> Xen 仮想マシンがインポートされるデータセンターを指定するか、Any Data Center を選択して、(<b>Virtual Machines</b> タブの <b>Import</b> 機能を使用して) 個々のインポート操作中に宛先データセンターを指定します。</li> <li>● <b>URI:</b> RHEL 5 Xen ホストの URI を入力します。</li> <li>● <b>Proxy Host</b> 仮想マシンのインポート操作中にホストとして機能するように、選択したデータセンターの <b>virt-v2v</b> をインストールしたホストを選択します。このホストは、RHEL 5 Xen 外部プロバイダーのネットワークにも接続できる必要があります。Any Data Center を選択した場合は、ここでホストを選択することはできませんが、代わりに、個別のインポート操作時にホストを指定できます (<b>Virtual Machines</b> タブの <b>Import</b> 機能を使用)。</li> </ul>
KVM	<ul style="list-style-type: none"> <li>● <b>Data Center:</b> KVM 仮想マシンがインポート</li> </ul>

設定	説明
	<p>されるデータセンターを指定するか、Any Data Center を選択して、(Virtual Machines タブの Import 機能を使用して) 個々のインポート操作中に宛先データセンターを指定します。</p> <ul style="list-style-type: none"> <li>● <b>URI</b>: KVM ホストの URI。</li> <li>● <b>Proxy Host</b> 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ホストを選択します。このホストは、KVM 外部プロバイダーのネットワークにも接続できる必要があります。Any Data Center を選択した場合は、ここでホストを選択することはできませんが、代わりに、個別のインポート操作時にホストを指定できます (Virtual Machines タブの Import 機能を使用)。</li> <li>● <b>Requires Authentication</b>: KVM ホストにアクセスするために認証が必要かどうかを指定できます。</li> <li>● <b>Username</b>: KVM ホストに接続するためのユーザー名</li> <li>● <b>Password</b>: 上記のユーザー名が認証されるパスワード。</li> </ul>
Test	ユーザーが指定の認証情報をテストすることを許可します。このボタンは、すべてのプロバイダータイプで使用できます。

### 2.9.3. 外部プロバイダーの編集

#### 手順

1. Administration → Providers をクリックし、編集する外部プロバイダーを選択します。
2. Edit をクリックします。
3. プロバイダーの現在の値を推奨値に変更します。
4. OK をクリックします。

### 2.9.4. 外部プロバイダーの削除

#### 手順

1. Administration → Providers をクリックし、削除する外部プロバイダーを選択します。
2. Remove をクリックします。
3. OK をクリックします。

## 第3章 環境の管理

### 3.1. セルフホスト型エンジンの管理

#### 3.1.1. セルフホスト型エンジンの保守

##### 3.1.1.1. セルフホスト型エンジンメンテナンスモードの説明

メンテナンスモードを使用すると、高可用性エージェントからの干渉を受けずに Manager 仮想マシンを起動、停止、変更したり、Manager に干渉することなく環境内のセルフホスト型エンジンノードを再起動および変更したりできます。

3つのメンテナンスモードがあります。

- **global** - クラスター内のすべての高可用性エージェントは、Manager 仮想マシンの状態を監視できなくなります。グローバルメンテナンスモードは、Red Hat Virtualization の新しいバージョンへのアップグレードなど、**ovirt-engine** サービスの停止を必要とするセットアップまたはアップグレード操作に適用する必要があります。
- **local** - コマンドを発行しているノードの高可用性エージェントは、Manager 仮想マシンの状態を監視できません。ローカルメンテナンスモードでは、ノードは Manager 仮想マシンのホスティングを免除されます。このモードに設定されたときに Manager 仮想マシンをホストしている場合、使用可能なノードがあれば、Manager は別のノードに移行します。セルフホスト型エンジンノードにシステムの変更または更新を適用する場合は、ローカルメンテナンスモードをお勧めします。
- **none** - メンテナンスモードを無効にして、高可用性エージェントが動作していることを確認します。

##### 3.1.1.2. ローカルメンテナンスモードの設定

ローカルメンテナンスモードを有効にすると、単一のセルフホスト型エンジンノードで高可用性エージェントが停止します。

##### 管理ポータルからのローカルメンテナンスモードの設定

1. セルフホスト型エンジンノードをローカルメンテナンスモードにします。
  - a. 管理ポータルで、Compute → Hosts をクリックし、セルフホスト型エンジンノードを選択します。
  - b. Management → Maintenance をクリックしてから OK をクリックします。そのノードに対してローカルメンテナンスモードが自動的にトリガーされます。
2. メンテナンスタスクを完了したら、メンテナンスモードを無効にします。
  - a. 管理ポータルで Compute → Hosts をクリックし、セルフホスト型エンジンノードを選択します。
  - b. Management → Activate をクリックします。

##### コマンドラインからローカルメンテナンスモードを設定

1. セルフホスト型エンジンノードにログインし、ローカルメンテナンスモードにします。

```
hosted-engine --set-maintenance --mode=local
```

- メンテナンスタスクを完了したら、メンテナスモードを無効にします。

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

### 3.1.1.3. グローバルメンテナスモードの設定

グローバルメンテナスモードを有効にすると、クラスター内のすべてのセルフホスト型エンジンノードで高可用性エージェントが停止します。

#### 管理ポータルからグローバルメンテナスモードを設定

- すべてのセルフホスト型エンジンノードをグローバルメンテナスモードにします。
  - 管理ポータルで **Compute → Hosts** をクリックし、セルフホスト型エンジンノードを選択します。
  - More Actions (⋮)** をクリックしてから、**Enable Global HA Maintenance** をクリックします。
- メンテナンスタスクを完了したら、メンテナスモードを無効にします。
  - 管理ポータルで **Compute → Hosts** をクリックし、セルフホスト型エンジンノードを選択します。
  - More Actions (⋮)** をクリックしてから、**Disable Global HA Maintenance** をクリックします。

#### コマンドラインからグローバルメンテナスモードを設定

- セルフホスト型エンジンノードにログインし、グローバルメンテナスモードにします。

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

- メンテナンスタスクを完了したら、メンテナスモードを無効にします。

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

### 3.1.2. Manager 仮想マシンの管理

**hosted-engine** ユーティリティーは、Manager 仮想マシンの管理に役立つ多くのコマンドを提供します。**hosted-engine** は、任意のセルフホスト型エンジンノードで実行できます。利用可能なコマンドをすべて表示するには、**hosted-engine --help** を実行します。特定のコマンドの詳細は、**hosted-engine --command --help** を実行してください。

#### 3.1.2.1. セルフホスト型エンジン設定の更新

セルフホスト型エンジン設定を更新するには、**hosted-engine --set-shared-config** コマンドを使用します。このコマンドは、初期デプロイ後に共有ストレージドメインのセルフホスト型エンジン設定を更新します。

現在の設定値を表示するには、**hosted-engine --get-shared-config** コマンドを使用します。

利用可能なすべての設定キーの一覧とそれに対応するタイプを表示するには、以下のコマンドを入力します。

```
hosted-engine --set-shared-config key --type=type --help
```

**type** は次のいずれかです。

<b>he_local</b>	ローカルホストの <b>/etc/ovirt-hosted-engine/hosted-engine.conf</b> のローカルインスタンスに値を設定し、そのホストのみが新しい値を使用するようにします。新しい値を有効にするには、ovirt-ha-agent サービスおよび ovirt-ha-broker サービスを再起動します。
<b>he_shared</b>	共有ストレージの <b>/etc/ovirt-hosted-engine/hosted-engine.conf</b> に値を設定するため、設定の変更後にデプロイされるすべてのホストがこれらの値を使用します。ホストで新しい値を有効にするには、そのホストを再デプロイします。
<b>ha</b>	ローカルストレージの <b>/var/lib/ovirt-hosted-engine-ha/ha.conf</b> に値を設定します。新しい設定はすぐに有効になります。
<b>broker</b>	ローカルストレージの <b>/var/lib/ovirt-hosted-engine-ha/broker.conf</b> に値を設定します。ovirt-ha-broker サービスを再起動して、新しい設定を有効にします。

### 3.1.2.2. メール通知の設定

セルフホスト型エンジンノードの HA 状態遷移に対して、SMTP を使用して電子メール通知を設定できます。更新できるキーには、**smtp-server**、**smtp-port**、**source-email**、**destination-emails**、および **state\_transition** が含まれます。

電子メール通知の設定:

- セルフホスト型エンジンノードで、**smtp-server** キーを目的の SMTP サーバーアドレスに設定します。

```
hosted-engine --set-shared-config smtp-server smtp.example.com --type=broker
```



#### 注記

セルフホスト型エンジン設定ファイルが更新されたことを確認するには、次のコマンドを実行します。

```
hosted-engine --get-shared-config smtp-server --type=broker
broker : smtp.example.com, type : broker
```

- デフォルトの SMTP ポート (ポート 25) が設定されていることを確認します。

```
hosted-engine --get-shared-config smtp-port --type=broker
broker : 25, type : broker
```

- SMTP サーバーが電子メール通知の送信に使用する電子メールアドレスを指定します。指定できるアドレスは1つだけです。

```
hosted-engine --set-shared-config source-email source@example.com --type=broker
```

4. 電子メール通知を受け取る宛先電子メールアドレスを指定します。複数のメールアドレスを指定するには、各アドレスをコンマで区切れます。

```
hosted-engine --set-shared-config destination-emails
destination1@example.com,destination2@example.com --type=broker
```

SMTP がセルフホスト型エンジン環境用に適切に設定されていることを確認するには、セルフホスト型エンジンノードの HA 状態を変更し、電子メール通知が送信されたかどうかを確認します。たとえば、HA エージェントをメンテナンスマードにすることで、HA の状態を変更できます。詳細は、[セルフホスト型エンジンの更新](#) を参照してください。

### 3.1.3. 追加ホスト上のセルフホスト型エンジン用に予約されたメモリースロットの設定

Manager 用仮想マシンのシャットダウンまたは移行が必要な場合、Manager 用仮想マシンを再起動または移行できるだけの十分なメモリーがセルフホスト型エンジンノードに必要です。このメモリーは、スケジューリングポリシーを使用して、複数のセルフホスト型エンジンノードで予約できます。スケジューリングポリシーは、仮想マシンを起動または移行する前に、Manager 仮想マシンを起動するのに十分なメモリーが指定された数の追加のセルフホスト型エンジンノードに残っているかどうかを確認します。スケジューリングポリシーの詳細は、[管理ガイド の スケジューリングポリシーの作成](#) を参照してください。

Red Hat Virtualization Manager へのセルフホストエンジンノードを追加するには、[Manager へのセルフホスト型エンジンノードの追加](#) を参照してください。

#### 追加ホスト上のセルフホスト型エンジン用に予約されたメモリースロットの設定

1. クラスターの **Compute → Clusters** をクリックして、セルフホスト型エンジンノードを含むクラスターを選択します。
2. **Edit** をクリックします。
3. **Scheduling Policy** タブをクリックします。
4. **+** をクリックして、**HeSparesCount** を選択します。
5. Manager 仮想マシンを起動するのに十分な空きメモリーを予約する追加のセルフホスト型エンジンノードの数を入力します。
6. **OK** をクリックします。

### 3.1.4. Red Hat Virtualization Manager へのセルフホスト型エンジンノードの追加

セルフホスト型エンジンノードは、通常のホストと同じ方法で追加しますが、セルフホスト型エンジンノードとしてホストをデプロイするという追加のステップが必要です。共有ストレージドメインは自動的に検出され、ノードは必要に応じて Manager 用仮想マシンをホストするフェイルオーバー用ホストとして使用できます。セルフホスト型エンジン環境に通常のホストをアタッチできますが、Manager 用仮想マシンはホストできません。Manager 用仮想マシンの高可用性を確保するためには、セルフホスト型エンジンノードを最低でも 2 つ用意します。追加のホストは、REST API を使用して追加することもできます。[REST API ガイド の ホスト](#) を参照してください。

#### 前提条件

- セルフホスト型エンジンノードはすべて、同じクラスター内になければなりません。

- セルフホスト型エンジンノードを再利用する場合は、既存のセルフホスト型エンジン設定を削除する。[セルフホスト型エンジン環境からのホストの削除](#) を参照してください。

## 手順

- 管理ポータルで **Compute → Hosts** をクリックします。
- New** をクリックします。  
ホストの追加設定に関する情報は、[管理ガイド の New Host および Edit Host ウィンドウの設定とコントロールの説明](#) を参照してください。
- ドロップダウンリストを使用して、新規ホスト用の **Data Center** および **Host Cluster** を選択します。
- 新規ホストの **Name** と **Address** を入力します。SSH Port 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。
- Manager がホストにアクセスするために使用する認証メソッドを選択します。
  - パスワード認証を使用するには、root ユーザーのパスワードを入力します。
  - または、SSH PublicKey フィールドに表示される鍵をホスト上の `/root/.ssh/authorized_keys` にコピーして、公開鍵認証を使用します。
- ホストにサポート対象の電源管理カードが搭載されている場合は、オプションとして電源管理を設定できます。電源管理の設定に関する詳細は、[管理ガイド の ホスト電源管理の設定の説明](#) を参照してください。
- Hosted Engine** タブをクリックします。
- Deploy** を選択します。
- OK** をクリックします。

### 3.1.5. 既存ホストをセルフホスト型エンジンノードとして再インストール

セルフホスト型エンジン環境内の既存の標準ホストは、Manager 仮想マシンをホストするセルフホスト型エンジンノードに変換できます。



#### 警告

ホストのオペレーティングシステムのインストールまたは再インストールを行う場合、Red Hat では、ホストにアタッチされている既存の OS 以外のストレージを最初にデタッチすることを強く推奨しています。これは、ディスクを誤って初期化してデータが失われる可能性を避けるためです。

## 手順

- Compute → Hosts** をクリックし、ホストを選択します。
- Management → Maintenance** をクリックしてから **OK** をクリックします。

3. Installation → Reinstall をクリックします。
4. Hosted Engine タブをクリックし、ドロップダウンリストから DEPLOY を選択します。
5. OK をクリックします。

ホストは、セルフホスト型エンジンの設定で再インストールされ、管理ポータルで王冠アイコンのフラグが付加されます。

### 3.1.6. Manager 仮想マシンをレスキュー モードで起動

このトピックでは、Manager 仮想マシンが起動しないときにレスキュー モードで起動する方法を説明します。詳細は、Red Hat Enterprise Linux System 管理者ガイドの [レスキュー モードでの起動](#) を参照してください。

1. ホストエンジンノードの1つに接続します。

```
$ ssh root@host_address
```

2. セルフホスト型エンジンをグローバルメンテナンスモードにします。

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

3. Manager 仮想マシンの実行中のインスタンスがすでに存在するか確認します。

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

Manager 仮想マシンインスタンスが実行されている場合は、そのホストに接続します。

```
ssh root@host_address
```

4. 仮想マシンをシャットダウンします。

```
hosted-engine --vm-shutdown
```



#### 注記

仮想マシンがシャットダウンしない場合は、次のコマンドを実行します。

```
hosted-engine --vm-poweroff
```

5. Manager 仮想マシンを一時停止モードで起動します。

```
hosted-engine --vm-start-paused
```

6. 一時的な VNC パスワードを設定します。

```
hosted-engine --add-console-password
```

このコマンドは、VNC を使用して Manger 仮想マシンにログインするために必要な情報を出力します。

7. VNC で Manager 用仮想マシンにログインします。Manager 仮想マシンはまだ一時停止しているため、フリーズしているように見えます。
8. ホストで次のコマンドを使用して、Manager 仮想マシンを再開します。



### 警告

次のコマンドを実行すると、ブートローダーメニューが表示されます。  
ブートローダーが通常のブートプロセスを続行する前に、レスキューモードに入る必要があります。このコマンドを続行する前に、レスキューモードへの遷移に関する次の手順を読んでください。

```
/usr/bin/virsh -c qemu:///system?authfile=/etc/ovirt-hosted-engine/virsh_auth.conf resume HostedEngine
```

9. Manager 仮想マシンをレスキューモードで起動します。
10. グローバルメンテナンスマードを無効にします。

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

これで、Manager 仮想マシンでレスキュータスクを実行できます。

### 3.1.7. セルフホスト型エンジン環境からのホストの削除

セルフホスト型エンジンノードを環境から削除するには、ノードをメンテナンスマードにし、アンデプロイし、オプションでそれを削除します。HA サービスが停止し、セルフホスト型エンジン設定ファイルが削除された後は、そのノードを通常のホストとして管理できます。

#### 手順

1. 管理ポータルで **Compute → Hosts** をクリックし、セルフホスト型エンジンノードを選択します。
2. **Management → Maintenance** をクリックしてから **OK** をクリックします。
3. **Installation → Reinstall** をクリックします。
4. **Hosted Engine** タブをクリックし、ドロップダウンリストから **UNDEPLOY** を選択します。このアクションにより、**ovirt-ha-agent** および **ovirt-ha-broker** サービスが停止し、セルフホスト型エンジン設定ファイルが削除されます。
5. **OK** をクリックします。
6. 必要に応じて、**Remove** をクリックします。これにより、**Remove Host(s)** 確認ウィンドウが開きます。
7. **OK** をクリックします。

### 3.1.8. セルフホスト型エンジンの更新

セルフホスト型エンジンを現在お使いのバージョンから最新のバージョンに更新するには、環境をグローバルメンテナンスモードに切り替え、続いてマイナーバージョン間の標準更新手順に従う必要があります。

#### グローバルメンテナンスモードの有効化

Manager 用仮想マシンの設定またはアップグレード作業を実施する前に、セルフホスト型エンジン環境をグローバルメンテナンスモードに切り替える必要があります。

#### 手順

- セルフホスト型エンジンノードのいずれかにログインして、グローバルメンテナンスモードを有効にします。

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

- 作業を進める前に、環境がグローバルメンテナンスモードにあることを確認します。

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

クラスターがグローバルメンテナンスモードにあることを示すメッセージが表示されるはずです。

#### Red Hat Virtualization Manager の更新

#### 手順

- Manager マシンで、更新されたパッケージが利用可能かどうかを確認します。

```
engine-upgrade-check
```

- setup パッケージを更新します。

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

- engine-setup** スクリプトで Red Hat Virtualization Manager を更新します。**engine-setup** スクリプトにより、設定に関する質問への回答が求められます。その後、**ovirt-engine** サービスの停止、更新パッケージのダウンロード/インストール、データベースのバックアップ/更新、インストール後設定の実施を経てから、**ovirt-engine** サービスが起動します。

```
engine-setup
```

スクリプトが正常に完了すると、以下のメッセージが表示されます。

```
Execution of setup completed successfully
```



## 注記

**engine-setup** スクリプトは、Red Hat Virtualization Manager のインストールプロセス中にも使用され、指定した設定値が保存されます。更新時に、設定をプレビューすると保存された値が表示されますが、インストール後に **engine-config** を使用して設定を更新した場合、この値は最新ではない可能性があります。たとえば、インストール後に **engine-config** を使用して **SANWipeAfterDelete** を **true** に更新した場合、**engine-setup** は設定プレビューに "Default SAN wipe after delete: False" を出力します。ただし、更新された値が **engine-setup** によって上書きされることはありません。



## 重要

更新プロセスに時間がかかる場合があります。完了するまでプロセスを停止しないでください。

- Manager にインストールされているベースオペレーティングシステムと、オプションパッケージを更新します。

```
yum update --nobest
```



## 重要

更新中に必要な Ansible パッケージの競合が発生した場合は、[RHV Manager で yum update を実行できない \(ansible の競合\)](#) を参照してください。



## 重要

カーネルパッケージが更新された場合は、以下を実行します。

- グローバルメンテナンスマードを無効にします。
- マシンを再起動して更新を完了します。

## 関連情報

[グローバルメンテナンスマードの無効化](#)

[グローバルメンテナンスマードの無効化](#)

## 手順

- Manager 用仮想マシンにログインし、シャットダウンします。
- セルフホスト型エンジンノードのいずれかにログインして、グローバルメンテナンスマードを無効にします。

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

グローバルメンテナンスマードを終了すると、ovirt-ha-agent が Manager 用仮想マシンを起動し、続いて Manager が自動的に起動します。Manager が起動するまでに最大で 10 分程度かかる場合があります。

- 環境が動作していることを確認します。

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

情報の一覧に、**Engine Status** が含まれます。**Engine status** の値は、以下のようになるはずです。

```
{"health": "good", "vm": "up", "detail": "Up"}
```



### 注記

仮想マシンが起動中で Manager がまだ動作していない場合、**Engine status** は以下のようになります。

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

このような場合は、数分間待ってからやり直してください。

## 3.1.9. セルフホスト型エンジンで Manager の FQDN を変更

**ovirt-engine-rename** コマンドを使用して、Manager の完全修飾ドメイン名 (FQDN) のレコードを更新できます。

詳細は、[Ovirt Engine Rename Tool を使用した Manager の名前変更](#) を参照してください。

## 3.2. バックアップと移行

### 3.2.1. Red Hat Virtualization Manager のバックアップと復元

#### 3.2.1.1. Red Hat Virtualization Manager のバックアップ - 概要

**engine-backup** ツールを使用して、定期的に Red Hat Virtualization Manager のバックアップを作成します。このツールを使用すると、エンジンデータベースおよび設定ファイルが1つのファイルにバックアップされ、**ovirt-engine** サービスを中断することなく実行できます。

#### 3.2.1.2. engine-backup コマンドの構文

**engine-backup** コマンドは、次の2つの基本モードのいずれかで機能します。

```
engine-backup --mode=backup
```

```
engine-backup --mode=restore
```

これらの2つのモードは、バックアップの範囲とエンジンデータベースのさまざまな認証情報を指定できる一連のオプションによってさらに拡張されます。オプションとその機能の完全なリストについては、**engine-backup --help** を実行してください。

#### 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指定します。使用可能なオプションは、**backup** (デフォルトで設定)、**restore**、および **verify** です。**verify** または **restore** 操作の **mode** オプションを定義する必要があります。

**--file**

バックアップモードでバックアップが保存され、リストアモードでバックアップデータとして読み取られるファイルのパスと名前(たとえば、`file_name.backup`)を指定します。パスはデフォルトで`/var/lib/ovirt-engine-backup/`と定義されます。

**--log**

バックアップまたは復元操作のログが書き込まれるファイルのパスと名前(たとえば、`log_file_name`)を指定します。パスはデフォルトで`/var/log/ovirt-engine-backup/`と定義されます。

**--scope**

バックアップまたは復元操作の範囲を指定します。4つのオプションがあります。**all** は、すべてのデータベースおよび設定データをバックアップまたは復元します(デフォルトで設定)。**files** は、システム上のファイルのみをバックアップまたは復元します。**db** は、Manager データベースのみをバックアップまたは復元します。**dwhdb** は、Data Warehouse データベースのみをバックアップまたは復元します。

**--scope** オプションは、同じ **engine-backup** コマンドで複数回指定できます。

**Manager データベースのオプション**

次のオプションは、**restore** モードで **engine-backup** コマンドを使用する場合にのみ使用できます。以下のオプション構文は、Manager データベースの復元に適用されます。Data Warehouse データベースを復元するための同じオプションがあります。Data Warehouse オプションの構文は、**engine-backup --help** を参照してください。

**--provision-db**

復元先の Manager データベースバックアップ用の PostgreSQL データベースを作成します。これは、PostgreSQL データベースがまだ設定されていないリモートホストまたは新規インストールで、バックアップを復元する場合に必要なオプションです。このオプションを復元モードで使用すると、**--restore-permissions** オプションがデフォルトで追加されます。

**--provision-all-databases**

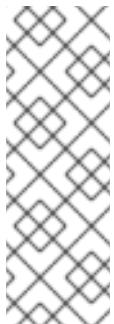
アーカイブに含まれるすべてのメモリーダンプのデータベースを作成します。有効にすると、これがデフォルトになります。

**--change-db-credentials**

バックアップ自体に保存されている認証情報以外の認証情報を使用して、Manager データベースを復元するための代替認証情報を指定できます。このオプションで必要な追加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 --noRestore-permissions**

データベースユーザーのパーミッションを復元したり、復元しなかったりします。バックアップを復元する場合は、これらのオプションのいずれかが必要です。復元モードで **--provision-\*** オプションを使用すると、デフォルトで **--restore-permissions** が適用されます。

**注記**

バックアップに追加のデータベースユーザーの許可が含まれている場合、**--restore-permissions** および **--provision-db**(または **--provision-dwh-db**) オプションを使用してバックアップを復元すると、ランダムなパスワードを持つ追加のユーザーが作成されます。追加のユーザーが復元したシステムにアクセスする必要がある場合は、これらのパスワードを手動で変更する必要があります。 [バックアップから Red Hat Virtualization を復元した後に追加のデータベースユーザーにアクセス権を付与する方法](#) を参照してください。

### 3.2.1.3. engine-backup コマンドを使用してバックアップを作成

Manager がアクティブなときに、**engine-backup** コマンドを使用して Red Hat Virtualization Manager をバックアップできます。次のいずれかの値を **--scope** オプションに追加して、バックアップする対象を指定します。

#### **all**

Manager 上のすべてのデータベースおよび設定ファイルの完全バックアップ。これは **--scope** オプションのデフォルト設定です。

#### **files**

システム上のファイルのみのバックアップ

#### **db**

Manager データベースのみのバックアップ

#### **dwhdb**

データウェアハウスデータベースのみのバックアップ

#### **cinderlibdb**

Cinderlib データベースのみのバックアップ

#### **grafanadb**

Grafana データベースのみのバックアップ

**--scope** オプションは複数回指定できます。

追加のファイルをバックアップするように **engine-backup** コマンドを設定することもできます。バックアップしたものすべてを復元します。



#### 重要

データベースを Red Hat Virtualization Manager の新規インストールに復元するには、データベースのバックアップだけでは不十分です。Manager には、設定ファイルへのアクセスも必要です。**all** 以外のスコープを指定する場合は、**--scope=files** も含めるか、ファイルシステムをバックアップする必要があります。

**engine-backup** コマンドの詳細は、Manager マシンで **engine-backup --help** と入力してください。

#### 手順

1. Manager マシンにログインします。
2. バックアップを作成します。

```
engine-backup
```

次の設定がデフォルトで適用されます。

#### **--scope=all**

#### **--mode=backup**

このコマンドは、**/var/lib/ovirt-engine-backup/file\_name.backup** にバックアップを生成し、**/var/log/ovirt-engine-backup/log\_file\_name** にログファイルを生成します。

**file\_name.tar** を使用して、環境を復元します。

次の例は、いくつかの異なるバックアップシナリオを示しています。

#### 例3.1 完全バックアップ

```
engine-backup
```

#### 例3.2 Manager データベースのバックアップ

```
engine-backup --scope=files --scope=db
```

#### 例3.3 データウェアハウスデータベースのバックアップ

```
engine-backup --scope=files --scope=dwhdb
```

#### 例3.4 バックアップに特定ファイルを追加

1. **engine-backup** コマンドの設定のカスタマイズを保存するディレクトリーを作成します。

```
mkdir -p /etc/ovirt-engine-backup/engine-backup-config.d
```

2. **ntp-chrony.sh** という名前の新しいディレクトリーに次の内容のテキストファイルを作成します。

```
BACKUP_PATHS="${BACKUP_PATHS}
/etc/chrony.conf
/etc/ntp.conf
/etc/ovirt-engine-backup"
```

3. **engine-backup** コマンドを実行するときは、**--scope=files** を使用します。バックアップと復元には、**/etc/chrony.conf**、**/etc/ntp.conf**、および**/etc/ovirt-engine-backup** が含まれます。

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

**engine-backup** コマンドを使用してバックアップを復元する場合、復元先によっては、バックアップを作成するよりも多くの手順が必要です。たとえば、Red Hat Virtualization の既存のインストールの他に、ローカルまたはリモートのデータベースを使用して Red Hat Virtualization の新規インストールにバックアップを復元するために、**engine-backup** コマンドを使用できます。



## 重要

バックアップの復元に使用される Red Hat Virtualization Manager のバージョン (4.4.8 など) は、バックアップの作成に使用される Red Hat Virtualization Manager のバージョン (4.4.7 など) 以降である必要があります。Red Hat Virtualization 4.4.7 以降、このポリシーは engine-backup コマンドによって厳密に適用されます。バックアップファイルに含まれている Red Hat Virtualization のバージョンを表示するには、バックアップファイルを解凍し、解凍されたファイルのルートディレクトリーにある **version** ファイルの値を読み取ります。

### 3.2.1.5. バックアップを新規インストールに復元

**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 に必要なパッケージがインストールされていて、**engine-setup** コマンドがまだ実行されていないマシンで実行する必要があります。この手順は、バックアップを復元するマシンから 1つまたは複数のバックアップファイルにアクセスできることを前提としています。

#### 手順

- Manager マシンにログインします。エンジンデータベースをリモートホストに復元する場合は、そのホストにログオンして、関連するアクションを実行する必要があります。同様に、Data Warehouse をリモートホストにも復元する場合は、そのホストにログオンして、関連するアクションを実行する必要があります。
- 完全バックアップまたはデータベースのみのバックアップを復元します。
  - 完全バックアップを復元します。

```
engine-backup --mode=restore --file=file_name --log=log_file_name --provision-db
```

復元モードで **--provision-\*** オプションを使用すると、デフォルトで **--restore-permissions** が適用されます。

完全バックアップの一部として Data Warehouse も復元される場合は、追加のデータベースをプロビジョニングします。

```
engine-backup --mode=restore --file=file_name --log=log_file_name --provision-db --provision-dwh-db
```

- 設定ファイルとデータベースバックアップを復元して、データベースのみのバックアップを復元します。

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

上記の例では、Manager データベースのバックアップを復元します。

```
engine-backup --mode=restore --scope=files --scope=dwhdb --file=file_name --log=log_file_name --provision-dwh-db
```

上記の例では、Data Warehouse データベースのバックアップを復元します。

成功すると、次の出力が表示されます。

You should now run engine-setup.  
Done.

- 次のコマンドを実行し、プロンプトに従って復元された Manager を設定します。

```
engine-setup
```

Red Hat Virtualization Manager は、バックアップに保存されているバージョンに復元されました。新しい Red Hat Virtualization システムの完全修飾ドメイン名を変更するには、[oVirt Engine Rename Tool](#) を参照してください。

### 3.2.1.6. バックアップを復元して既存のインストールを上書き

**engine-backup** コマンドを使用すると、Red Hat Virtualization Manager がすでにインストールおよび設定されているマシンに、バックアップを復元できます。これは、環境のバックアップを作成し、その環境に変更を加えた後、バックアップから環境を復元して変更を元に戻したい場合に役立ちます。

バックアップ作成後に環境に加えられた、ホストの追加や削除などの変更は、復元された環境には表示されません。そのような変更はやり直す必要があります。

#### 手順

- Manager マシンにログインします。
- 設定ファイルを削除し、Manager に関連付けられているデータベースをクリーンアップします。

```
engine-cleanup
```

**engine-cleanup** コマンドは、Manager データベースのみを削除します。データベースを削除したり、そのデータベースを所有しているユーザーを削除したりすることはありません。

- 完全バックアップまたはデータベースのみのバックアップを復元します。ユーザーとデータベースがすでに存在しているので、新規のデータベースを作成したり、データベースの認証情報を見つける必要はありません。

- 完全バックアップを復元します。

```
engine-backup --mode=restore --file=file_name --log=log_file_name --restore-permissions
```

- 設定ファイルおよびデータベースバックアップを復元して、データベースのみのバックアップを復元します。

```
engine-backup --mode=restore --scope=files --scope=db --scope=dwhdb --file=file_name --log=log_file_name --restore-permissions
```



#### 注記

Manager データベースのみを復元するには(たとえば、Data Warehouse データベースが別のマシンにある場合)、**-scope=dwhdb** パラメーターを省略できます。

成功すると、次の出力が表示されます。

You should now run engine-setup.  
Done.

- Manager を再設定します。

```
engine-setup
```

### 3.2.1.7. 異なる認証情報を使用したバックアップの復元

**engine-backup** コマンドは、Red Hat Virtualization Manager がすでにインストールされセットアップされているマシンにバックアップを復元できますが、バックアップ内のデータベースの認証情報は、バックアップを復元するマシン上のデータベースの認証情報とは異なります。これは、インストールのバックアップを取り、バックアップから別のシステムにインストールを復元する場合に役立ちます。



#### 重要

バックアップを復元して既存のインストールを上書きする場合は、**engine-backup** コマンドを使用する前に、**engine-cleanup** コマンドを実行して既存のインストールをクリーンアップする必要があります。**engine-cleanup** コマンドは、エンジンデータベースをクリーンアップするだけで、データベースを削除したり、そのデータベースを所有しているユーザーを削除したりすることはありません。したがって、新規のデータベースを作成したり、データベースの認証情報を指定する必要はありません。ただし、エンジンデータベースの所有者の認証情報がわからない場合は、バックアップを復元する前に認証情報を変更する必要があります。

#### 手順

- Red Hat Virtualization Manager マシンにログインします。
- 次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 のデータベースをクリーンアップします。

```
engine-cleanup
```

- engine** データベースの所有者のパスワードがわからない場合は、そのユーザーのパスワードを変更します。

- postgresql コマンドラインを入力します。

```
su - postgres -c 'psql'
```

- engine** データベースを所有するユーザーのパスワードを変更します。

```
postgres=# alter role user_name encrypted password 'new_password';
```

必要に応じて、**ovirt\_engine\_history** データベースを所有するユーザーに対してこれを繰り返します。

- change-db-credentials** パラメーターを使用して完全バックアップまたはデータベースのみのバックアップを復元し、新しいデータベースの認証情報を渡します。Manager に対してローカルなデータベースの **database\_location** は **localhost** です。



## 注記

次の例では、パスワードを指定せずにデータベースごとに `--*password` オプションを使用します。これにより、データベースごとにパスワードの入力を求められます。別の方法として、データベースごとに `--*passfile=password_file` オプションを使用して、対話型プロンプトを必要とせずに、パスワードを `engine-backup` ツールに安全に渡すことができます。

- 完全バックアップを復元します。

```
engine-backup --mode=restore --file=file_name --log=log_file_name --change-db-credentials --db-host=database_location --db-name=database_name --db-user=engine --db-password --no-restore-permissions
```

Data Warehouse も完全バックアップの一部として復元される場合は、追加のデータベースの改訂された認証情報を含めます。

```
engine-backup --mode=restore --file=file_name --log=log_file_name --change-db-credentials --db-host=database_location --db-name=database_name --db-user=engine --db-password --change-dwh-db-credentials --dwh-db-host=database_location --dwh-db-name=database_name --dwh-db-user=ovirt_engine_history --dwh-db-password --no-restore-permissions
```

- 設定ファイルおよびデータベースバックアップを復元して、データベースのみのバックアップを復元します。

```
engine-backup --mode=restore --scope=files --scope=db --file=file_name --log=log_file_name --change-db-credentials --db-host=database_location --db-name=database_name --db-user=engine --db-password --no-restore-permissions
```

上記の例では、Manager データベースのバックアップを復元します。

```
engine-backup --mode=restore --scope=files --scope=dwhdb --file=file_name --log=log_file_name --change-dwh-db-credentials --dwh-db-host=database_location --dwh-db-name=database_name --dwh-db-user=ovirt_engine_history --dwh-db-password --no-restore-permissions
```

上記の例では、Data Warehouse データベースのバックアップを復元します。

成功すると、次の出力が表示されます。

```
You should now run engine-setup.
Done.
```

- 次のコマンドを実行し、プロンプトに従ってファイアウォールを再設定し、`ovirt-engine` サービスが正しく設定されていることを確認します。

```
engine-setup
```

### 3.2.1.8. セルフホスト型エンジンのバックアップおよび復元

セルフホスト型エンジンをバックアップして、新しいセルフホスト環境に復元できます。この手順は、環境を別のストレージタイプの新しいセルフホスト型エンジンストレージドメインに移行するなどのタスクに使用します。

デプロイメント中にバックアップファイルを指定すると、バックアップは、新しいセルフホスト型エンジンストレージドメインを使用して、新しいManager仮想マシンに復元されます。古いManagerが削除されます。また、古いセルフホスト型エンジンストレージドメインの名前が変更され、新しい環境が正しく機能していることが確認された後で、これを手動で削除できます。新規ホストにデプロイすることを強く推奨します。デプロイメントに使用されたホストがバックアップ環境に存在している場合、新しい環境で競合を回避するために、復元されたデータベースから削除されます。新しいホストにデプロイする場合は、ホストに一意の名前を割り当てる必要があります。バックアップに含まれる既存ホストの名前を再利用すると、新しい環境で競合が発生する可能性があります。

バックアップと復元の操作には、次の主要なアクションが含まれます。

1. [engine-backup](#) ツールを使用して元の Manager をバックアップします。
2. 新しいセルフホスト型エンジンをデプロイしてバックアップを復元します。
3. 新しい Manager 用仮想マシンで Manager のリポジトリを有効化します。
4. セルフホスト型エンジンノードを再インストールして設定を更新します。
5. 古いセルフホスト型エンジンストレージドメインを削除します。

この手順の前提として、移行元の Manager に対するアクセス権があり、変更を加えることできる必要があります。

## 前提条件

- Manager とホスト用に用意された完全修飾ドメイン名。正引き(フォワードルックアップ)と逆引き(リバースルックアップ)の記録は、両方とも DNS で設定する必要があります。新しい Manager は、元の Manager と同じ完全修飾ドメイン名を持っている必要があります。
- 元の Manager を最新のマイナーバージョンに更新する。バックアップの復元に使用される Red Hat Virtualization Manager のバージョン(4.4.8など)は、バックアップの作成に使用される Red Hat Virtualization Manager のバージョン(4.4.7など)以降である必要があります。Red Hat Virtualization 4.4.7 以降、このポリシーは [engine-backup](#) コマンドによって厳密に適用されます。アップグレードガイドの [Red Hat Virtualization Manager の更新](#) を参照してください。



## 注記

バックアップを復元する必要があるが、新しいアプライアンスがない場合、復元プロセスを一時停止し、SSH 経由で一時的な Manager マシンにログインしてチャンネルの登録、サブスクリプション、設定を適宜行い、Manager パッケージをアップグレードしてから復元プロセスを再開できます。

- 更新されたストレージバージョンとの互換性を確保するために、データセンターの互換性レベルを最新バージョンに設定する必要があります。
- 環境内に少なくとも 1 つの標準ホストが存在する必要があります。このホスト(およびその他の通常のホスト)は、SPM ロールおよび実行中の仮想マシンをホストするためにアクティブなままになります。標準ホストがまだ SPM ではない場合、標準ホストを選択し、Management → Select as SPM をクリックして、SPM のロールを移動してからバックアップを作成します。標準ホストが利用できない場合に 1 つを追加する方法は 2 つあります。

- セルフホスト型エンジン設定をノードから削除します(ただし、環境からノードは削除しないでください)。[セルフホスト型エンジン環境からのホストの削除](#) を参照してください。
- 新しい標準ホストを追加します。[Manager ホストタスクへの標準ホストの追加](#) を参照してください。

### 3.2.1.8.1. 元の Manager のバックアップ

**engine-backup** コマンドを使用して元の Manager をバックアップし、バックアップファイルを別の場所にコピーして、処理中にいつでもアクセスできるようにします。

**engine-backup --mode=backup** オプションの詳細は、[管理ガイド](#) の [Red Hat Virtualization Manager のバックアップと復元](#) を参照してください。

#### 手順

- セルフホスト型エンジンノードの1つにログインし、環境をグローバルメンテナンスモードに移行します。

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

- 元の Manager にログインし、**ovirt-engine** サービスを停止します。

```
systemctl stop ovirt-engine
systemctl disable ovirt-engine
```



#### 注記

元の Manager の実行を停止することは必須ではありませんが、バックアップの作成後に環境を変更しないように推奨しています。さらに、元の Manager と新しい Manager が既存リソースを同時に管理しないようにします。

- 作成するバックアップファイルの名前と、バックアップログを保存するログファイルの名前を指定して、**engine-backup** コマンドを実行します。

```
engine-backup --mode=backup --file=file_name --log=log_file_name
```

- ファイルを外部サーバーにコピーします。以下の例の **storage.example.com** は、必要になるまでバックアップを保存するネットワークストレージサーバーの完全修飾ドメイン名です。**/backup/** は指定のフォルダーまたはパスです。

```
scp -p file_name log_file_name storage.example.com:/backup/
```

- Manager マシンを他の目的で必要としない場合は、Red Hat Subscription Manager から登録を解除します。

```
subscription-manager unregister
```

- セルフホスト型エンジンノードの1つにログインし、元の Manager 仮想マシンをシャットダウンします。

```
hosted-engine --vm-shutdown
```

Manager のバックアップ後に、新しいセルフホスト型エンジンをデプロイし、新しい仮想マシンにバックアップを復元します。

### 3.2.1.8.2. 新しいセルフホスト型エンジンでのバックアップの復元

**hosted-engine** スクリプトを新規ホストで実行し、デプロイメント中に **--restore-from-file=path/to/file name** オプションを使用して Manager バックアップを復元します。



重要

iSCSI ストレージを使用し、イニシエーターの ACL に従い iSCSI ターゲット フィルターを使用して接続を フィルタリングすると、デプロイメントは

**STORAGE\_DOMAIN\_UNREACHABLE** エラーで失敗する可能性があります。これを回避するには、セルフホストエンジンのデプロイメントを開始する前に iSCSI 設定を更新する必要があります。

- 既存のホストに再デプロイする場合は、`/etc/iscsi/initiatorname.iscsi` でホストの iSCSI イニシエーター設定を更新する必要があります。イニシエーター IQN は、iSCSI ターゲットで以前にマッピングされていたものと同じか、必要に応じて新しい IQN に更新する必要があります。
  - 新規ホストにデプロイする場合は、iSCSI ターゲット設定を更新して、ホストからの接続を受け入れる必要があります。

IQN はホスト側 (iSCSI イニシエーター) またはストレージ側 (iSCSI ターゲット) で更新できることに注意してください。

手順

1. バックアップファイルを新規ホストにコピーします。以下の例では、`host.example.com` はホストの FQDN、`/backup/` は指定されたフォルダーまたはパスです。

```
scp -p file name host.example.com:/backup/
```

- 新しいホストにログインします。
  - Red Hat Virtualization Host にデプロイする場合、**ovirt-hosted-engine-setup** はすでにインストールされているため、この手順を省略します。Red Hat Enterprise Linux にデプロイする場合は、**ovirt-hosted-engine-setup** パッケージをインストールします。

```
dnf install ovirt-hosted-engine-setup
```

4. ネットワークやターミナルが切断された場合などにセッションが失われないように、**tmux** ウィンドウマネージャーを使用してスクリプトを実行します。  
**tmux** をインストールし、実行します。

```
dnf -y install tmux
tmux
```

5. バックアップファイルへのパスを指定して `hosted-engine` スクリプトを実行します。

```
hosted-engine --deploy --restore-from-file=backup/file name
```

仕事のタイミングでスクリプトをエグエーノするには、**CTRL+D** を使用してアノロイメントを中止します。

6. **Yes** を選択してデプロイメントを開始します。
7. ネットワークを設定します。スクリプトにより、環境の管理ブリッジとして使用する NIC 候補が検出されます。
8. 仮想マシンのインストールにカスタムアプライアンスを使用する場合は、OVA アーカイブへのパスを入力します。使用しない場合は、このフィールドを空欄のままにして RHV-M Appliance を使用します。
9. Manager の root パスワードを入力します。
10. root ユーザーとして Manager にログインできる SSH 公開鍵を入力し、root ユーザーの SSH アクセスを有効にするかどうかを指定します。
11. 仮想マシンの CPU およびメモリー設定を入力します。
12. Manager 用仮想マシンの MAC アドレスを入力するか、無作為に生成される MAC アドレスを適用します。Manager 用仮想マシンへの IP アドレス割り当てに DHCP を使用する場合は、この MAC アドレスに有効な DHCP 予約があることを確認してください。デプロイメントスクリプトは、DHCP サーバーの設定は行いません。
13. 仮想マシンのネットワーク情報を入力します。Static を指定する場合は、Manager の IP アドレスを入力します。



### 重要

静的 IP アドレスは、ホストと同じサブネットに属している必要があります。たとえばホストが 10.1.1.0/24 内にある場合、Manager 用仮想マシンの IP は同じサブネット範囲 (10.1.1.1-254/24) になければなりません。

14. Manager 用仮想マシンおよびベースホストのエントリーを、仮想マシンの **/etc/hosts** ファイルに追加するかどうかを指定します。ホスト名は解決可能でなければなりません。
15. SMTP サーバーの名前と TCP ポート番号、メール通知を送信するメールアドレス、メール通知を受信するメールアドレス（複数ある場合はコンマ区切りリスト）を指定します。
16. 管理ポータルにアクセスする際に使用する **admin@internal** ユーザーのパスワードを入力します。  
スクリプトにより仮想マシンが作成されます。RHV-M Appliance をインストールする必要がある場合は、時間がかかることがあります。

## 注記

必要なネットワークがないなどの理由でホストが動作しなくなると、デプロイが一時停止し、次のようなメッセージが表示されます。

```
[INFO] You can now connect to https://<host name>:6900/ovirt-engine/ and
check the status of this host and eventually remediate it, please continue only
when the host is listed as 'up'
[INFO] TASK [ovirt.ovirt.hosted_engine_setup : include_tasks]
[INFO] ok: [localhost]
[INFO] TASK [ovirt.ovirt.hosted_engine_setup : Create temporary lock file]
[INFO] changed: [localhost]
[INFO] TASK [ovirt.ovirt.hosted_engine_setup : Pause execution until
/ttmp/ansible.<random>_he_setup_lock is removed, delete it once ready to
proceed]
```

プロセスを一時停止すると、以下が可能になります。

- 提供された URL を使用して管理ポータルに接続します。
- 状況を評価し、ホストが動作していない理由を調べ、必要に応じて修正します。たとえば、このデプロイメントがバックアップから復元され、ホストクラスターに **必要なネットワーク** がバックアップに含まれている場合は、ネットワークを設定し、関連するホスト NIC をこれらのネットワークに接続します。
- すべてが正常に見え、ホストのステータスが **Up** になったら、上記のメッセージに表示されているロックファイルを削除します。デプロイメントは続行されます。

### 17. 使用するストレージのタイプを選択します。

- NFS の場合は、バージョン、完全なアドレス、ストレージへのパスおよびマウントオプションを入力します。

#### 警告



仮想マシンのデータが失われるリスクがあるため、古いセルフホスト型エンジンストレージドメインのマウントポイントを新しいストレージドメインに使用しないでください。

- iSCSI の場合は、ポータルの詳細を入力し、自動検出された一覧からターゲットおよび LUN を選択します。デプロイメント時に選択できる iSCSI ターゲットは1つだけですが、マルチパスがサポートされているので、同じポータルグループのポータルをすべて接続できます。



## 注記

複数の iSCSI ターゲットを指定するには、セルフホスト型エンジンをデプロイする前にマルチパスを有効にする必要があります。詳細は、[Red Hat Enterprise Linux DM マルチパス](#) を参照してください。[Multipath Helper](#) ツールを使用して、さまざまなオプションでマルチパスをインストールおよび設定するスクリプトを生成することもできます。

- Gluster ストレージの場合は、完全なアドレスおよびストレージへのパスならびにマウントオプションを入力します。



## 警告

仮想マシンのデータが失われるリスクがあるため、古いセルフホスト型エンジンストレージドメインのマウントポイントを新しいストレージドメインに使用しないでください。



## 重要

レプリカ 1 およびレプリカ 3 Gluster ストレージのみがサポートされます。必ず以下のようにボリュームを設定します。

```
gluster volume set VOLUME_NAME group virt
gluster volume set VOLUME_NAME performance.strict-o-direct on
gluster volume set VOLUME_NAME network.remote-dio off
gluster volume set VOLUME_NAME storage.owner-uid 36
gluster volume set VOLUME_NAME storage.owner-gid 36
gluster volume set VOLUME_NAME network.ping-timeout 30
```

- ファイバーチャネルの場合は、自動検出されたリストから LUN を選択します。ホストのバスアダプターが設定および接続されている必要があります。また、LUN には既存のデータが含まれないようにする必要があります。既存の LUN を再利用するには、[管理ガイドの LUN の再利用](#) を参照してください。
18. Manager のディスクサイズを入力します。  
スクリプトはデプロイメントが完了するまで続行されます。
19. デプロイメントプロセスでは Manager の SSH キーが変更されます。クライアントマシンが SSH エラーなしで新規の Manager にアクセスできるようにするには、元の Manager にアクセスするクライアントマシンの **.ssh/known\_hosts** ファイルから元の Manager のエントリーを削除します。

デプロイメントが完了したら、新しい Manager 仮想マシンにログインし、必要なリポジトリを有効にします。

### 3.2.1.8.3. Red Hat Virtualization Manager リポジトリの有効化

ログインして、Red Hat Subscription Manager で Manager マシンを登録し、**Red Hat Virtualization Manager** のサブスクリプションをアタッチして Manager のリポジトリを有効にする必要があります。

## 手順

1. コンテンツ配信ネットワークにシステムを登録します。プロンプトが表示されたら、カスタマーポータルのユーザー名とパスワードを入力します。

```
subscription-manager register
```



### 注記

IPv6 ネットワークを使用している場合は、IPv6 移行メカニズムを使用して、コンテンツ配信ネットワークおよびサブスクリプションマネージャーにアクセスします。

2. **Red Hat Virtualization Manager** のサブスクリプションプールを見つけ、プール ID を記録します。

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

3. 上記のプール ID を使用して、サブスクリプションをシステムにアタッチします。

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



### 注記

現在アタッチされているサブスクリプションを表示するには、以下のコマンドを実行します。

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

有効なリポジトリをすべてリスト表示するには、以下のコマンドを実行します。

```
dnf repolist
```

4. リポジトリを設定します。

```
subscription-manager repos \
--disable='*' \
--enable=rhel-8-for-x86_64-baseos-eus-rpms \
--enable=rhel-8-for-x86_64-appstream-eus-rpms \
--enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
--enable=fast-datapath-for-rhel-8-x86_64-rpms \
--enable=jb-eap-7.4-for-rhel-8-x86_64-rpms \
--enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
--enable=rhceph-4-tools-for-rhel-8-x86_64-rpms
```

5. RHEL のバージョンを 8.6 に設定します。

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

6. **pki-deps** モジュールを有効にします。

```
dnf module -y enable pki-deps
```

7. **postgresql** モジュールのバージョン 12 を有効にします。

```
dnf module -y enable postgresql:12
```

8. **nodejs** モジュールのバージョン 14 を有効にします。

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

9. インストール済みパッケージを同期して、利用可能な最新バージョンに更新します。

```
dnf distro-sync --nobest
```

## 関連情報

モジュールおよびモジュールストリームの詳細は、[ユーザー空間コンポーネントのインストール、管理、および削除](#) の以下のセクションを参照してください。

- [モジュールストリーム](#)
- [パッケージインストールの前のストリーム選択](#)
- [モジュールストリームのリセット](#)
- [後のストリームへの切り替え](#)

Manager とそのリソースは、新しいセルフホスト環境で実行されています。セルフホスト型エンジンノードは、セルフホスト型エンジン設定を更新するために Manager に再インストールする必要があります。標準ホストは影響を受けません。セルフホスト型エンジンノードごとに次の手順を実行します。

### 3.2.1.8.4. ホストの再インストール

管理ポータルから Red Hat Virtualization Host (RHVH) および Red Hat Enterprise Linux ホストを再インストールします。この手順には、ホストの停止および再起動が含まれます。

#### 警告



ホストのオペレーティングシステムのインストールまたは再インストールを行う場合、Red Hat では、ホストにアタッチされている既存の OS 以外のストレージを最初にデタッチすることを強く推奨しています。これは、ディスクを誤って初期化してデータが失われる可能性を避けるためです。

## 前提条件

- クラスターの移行が有効化されている場合、仮想マシンはそのクラスター内の別のホストに自動的に移行できます。したがって、使用量が比較的低い間にホストを再インストールします。
- ホストによるメンテナンスの実行に必要なメモリーがクラスターにあることを確認します。クラスターにメモリーがない場合、仮想マシンの移行はハングして失敗します。メモリー使用量を減らすには、ホストをメンテナンスに移行する前に、一部またはすべての仮想マシンをシャットダウンします。
- 再インストールを実行する前に、クラスターに複数のホストが含まれていることを確認してください。すべてのホストを同時に再インストールしようとしないでください。Storage Pool Manager (SPM) タスクを実行するには、1台のホストは使用可能な状態でなければなりません。

## 手順

1. Compute → Hosts をクリックし、ホストを選択します。
2. Management → Maintenance をクリックしてから OK をクリックします。
3. Installation → Reinstall をクリックします。Install Host ウィンドウが表示されます。
4. Hosted Engine タブをクリックし、ドロップダウンリストから DEPLOY を選択します。
5. OK をクリックして、ホストを再インストールします。

ホストを再インストールし、そのステータスが Up に戻れば、仮想マシンをホストに戻すことができます。



## 重要

Red Hat Virtualization Host を Red Hat Virtualization Manager に登録し、これを再インストールした後、管理ポータルでそのステータスが誤って Install Failed と表示される場合があります。Management → Activate をクリックすると、ホストのステータスが Up に変わり、使用できるようになります。

セルフホスト型エンジンノードを再インストールした後に、いずれかのノードで以下のコマンドを実行して、新しい環境のステータスを確認できます。

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

復元中に、古いセルフホスト型エンジンのストレージドメインの名前が変更されたが、復元に問題があった場合に備えて、新しい環境からは削除されませんでした。環境が正常に実行されていることを確認したら、古いセルフホスト型エンジンストレージドメインを削除できます。

### 3.2.1.8.5. ストレージドメインの削除

データセンターに、仮想化環境から削除するストレージドメインがあります。

## 手順

1. Storage → Domains をクリックします。
2. ストレージドメインをメンテナンスモードに移動し、デタッチします。
  - a. ストレージドメインの名前をクリックします。詳細ビューが開きます。

- b. Data Center タブをクリックします。
- c. Maintenance をクリックしてから **OK** をクリックします。
- d. Detach をクリックしてから **OK** をクリックします。
3. Remove をクリックします。
4. オプションで **Format Domain, i.e. Storage Content will be lost!** チェックボックスを選択して、ドメインのコンテンツを消去します。
5. **OK** をクリックします。

ストレージドメインが環境から完全に削除されます。

### 3.2.1.9. 既存のバックアップからのセルフホスト型エンジンの復元

修復できない問題が原因でセルフホスト型エンジンが使用できない場合は、問題が発生する前に作成したバックアップを使用して、新しいセルフホスト環境でエンジンを復元できます（使用可能な場合）。

デプロイメント中にバックアップファイルを指定すると、バックアップは、新しいセルフホスト型エンジンストレージドメインを使用して、新しい Manager 仮想マシンに復元されます。古い Manager が削除されます。また、古いセルフホスト型エンジンストレージドメインの名前が変更され、新しい環境が正しく機能していることが確認された後で、これを手動で削除できます。新規ホストにデプロイすることを強く推奨します。デプロイメントに使用されたホストがバックアップ環境に存在している場合、新しい環境で競合を回避するために、復元されたデータベースから削除されます。新しいホストにデプロイする場合は、ホストに一意の名前を割り当てる必要があります。バックアップに含まれる既存ホストの名前を再利用すると、新しい環境で競合が発生する可能性があります。

セルフホスト型エンジンの復元には、次の主要なアクションが含まれます。

1. 新しいセルフホスト型エンジンをデプロイしてバックアップを復元します。
2. 新しい Manager 用仮想マシンで Manager のリポジトリを有効化します。
3. セルフホスト型エンジンノードを再インストールして設定を更新します。
4. 古いセルフホスト型エンジンストレージドメインを削除します。

この手順は、元の Manager にアクセスできず、新しいホストがバックアップファイルにアクセスできることを前提としています。

#### 前提条件

- Manager とホスト用に用意された完全修飾ドメイン名。正引き（フォワードルックアップ）と逆引き（リバースルックアップ）の記録は、両方とも DNS で設定する必要があります。新しい Manager は、元の Manager と同じ完全修飾ドメイン名を持っている必要があります。

#### 3.2.1.9.1. 新しいセルフホスト型エンジンでのバックアップの復元

**hosted-engine** スクリプトを新規ホストで実行し、デプロイメント中に **--restore-from-file=path/to/file\_name** オプションを使用して Manager バックアップを復元します。



## 重要

iSCSIストレージを使用し、イニシエーターのACLに従いiSCSIターゲットフィルターを使用して接続をフィルタリングすると、デプロイメントは**STORAGE\_DOMAIN\_UNREACHABLE**エラーで失敗する可能性があります。これを回避するには、セルフホストエンジンのデプロイメントを開始する前にiSCSI設定を更新する必要があります。

- 既存のホストに再デプロイする場合は、`/etc/iscsi/initiatorname.iscsi`でホストのiSCSIイニシエーター設定を更新する必要があります。イニシエーターIQNは、iSCSIターゲットで以前にマッピングされていたものと同じか、必要に応じて新しいIQNに更新する必要があります。
- 新規ホストにデプロイする場合は、iSCSIターゲット設定を更新して、ホストからの接続を受け入れる必要があります。

IQNはホスト側(iSCSIイニシエーター)またはストレージ側(iSCSIターゲット)で更新できることに注意してください。

## 手順

- バックアップファイルを新規ホストにコピーします。以下の例では、**host.example.com**はホストのFQDN、`/backup/`は指定されたフォルダーまたはパスです。

```
scp -p file_name host.example.com:/backup/
```

- 新しいホストにログインします。
- Red Hat Virtualization Hostにデプロイする場合、**ovirt-hosted-engine-setup**はすでにインストールされているため、この手順を省略します。Red Hat Enterprise Linuxにデプロイする場合は、**ovirt-hosted-engine-setup**パッケージをインストールします。

```
dnf install ovirt-hosted-engine-setup
```

- ネットワークやターミナルが切断された場合などにセッションが失われないように、**tmux**ウィンドウマネージャーを使用してスクリプトを実行します。**tmux**をインストールし、実行します。

```
dnf -y install tmux
tmux
```

- バックアップファイルへのパスを指定して**hosted-engine**スクリプトを実行します。

```
hosted-engine --deploy --restore-from-file=backup/file_name
```

任意のタイミングでスクリプトをエスケープするには、**CTRL+D**を使用してデプロイメントを中止します。

- Yes**を選択してデプロイメントを開始します。
- ネットワークを設定します。スクリプトにより、環境の管理ブリッジとして使用するNIC候補が検出されます。

8. 仮想マシンのインストールにカスタムノンフィールドを使用する場合は、OVA フォルダへのパスを入力します。使用しない場合は、このフィールドを空欄のままにして RHV-M Appliance を使用します。
9. Manager の root パスワードを入力します。
10. root ユーザーとして Manager にログインできる SSH 公開鍵を入力し、root ユーザーの SSH アクセスを有効にするかどうかを指定します。
11. 仮想マシンの CPU およびメモリー設定を入力します。
12. Manager 用仮想マシンの MAC アドレスを入力するか、無作為に生成される MAC アドレスを適用します。Manager 用仮想マシンへの IP アドレス割り当てに DHCP を使用する場合は、この MAC アドレスに有効な DHCP 予約があることを確認してください。デプロイメントスクリプトは、DHCP サーバーの設定は行いません。
13. 仮想マシンのネットワーク情報を入力します。Static を指定する場合は、Manager の IP アドレスを入力します。



### 重要

静的 IP アドレスは、ホストと同じサブネットに属している必要があります。たとえばホストが 10.1.1.0/24 内にある場合、Manager 用仮想マシンの IP は同じサブネット範囲 (10.1.1.1-254/24) になければなりません。

14. Manager 用仮想マシンおよびベースホストのエントリーを仮想マシンの **/etc/hosts** ファイルに追加するかどうかを指定します。ホスト名は解決可能でなければなりません。
15. SMTP サーバーの名前と TCP ポート番号、メール通知を送信するメールアドレス、メール通知を受信するメールアドレス（複数ある場合はコンマ区切りリスト）を指定します。
16. 管理ポータルにアクセスする際に使用する **admin@internal** ユーザーのパスワードを入力します。  
スクリプトにより仮想マシンが作成されます。RHV-M Appliance をインストールする必要がある場合は、時間がかかることがあります。

## 注記

必要なネットワークがないなどの理由でホストが動作しなくなると、デプロイが一時停止し、次のようなメッセージが表示されます。

```
[INFO] You can now connect to https://<host name>:6900/ovirt-engine/ and
check the status of this host and eventually remediate it, please continue only
when the host is listed as 'up'
[INFO] TASK [ovirt.ovirt.hosted_engine_setup : include_tasks]
[INFO] ok: [localhost]
[INFO] TASK [ovirt.ovirt.hosted_engine_setup : Create temporary lock file]
[INFO] changed: [localhost]
[INFO] TASK [ovirt.ovirt.hosted_engine_setup : Pause execution until
/ttmp/ansible.<random>_he_setup_lock is removed, delete it once ready to
proceed]
```

プロセスを一時停止すると、以下が可能になります。

- 提供された URL を使用して管理ポータルに接続します。
- 状況を評価し、ホストが動作していない理由を調べ、必要に応じて修正します。たとえば、このデプロイメントがバックアップから復元され、ホストクラスターに **必要なネットワーク** がバックアップに含まれている場合は、ネットワークを設定し、関連するホスト NIC をこれらのネットワークに接続します。
- すべてが正常に見え、ホストのステータスが **Up** になったら、上記のメッセージに表示されているロックファイルを削除します。デプロイメントは続行されます。

### 17. 使用するストレージのタイプを選択します。

- NFS の場合は、バージョン、完全なアドレス、ストレージへのパスおよびマウントオプションを入力します。

#### 警告



仮想マシンのデータが失われるリスクがあるため、古いセルフホスト型エンジンストレージドメインのマウントポイントを新しいストレージドメインに使用しないでください。

- iSCSI の場合は、ポータルの詳細を入力し、自動検出された一覧からターゲットおよび LUN を選択します。デプロイメント時に選択できる iSCSI ターゲットは1つだけですが、マルチパスがサポートされているので、同じポータルグループのポータルをすべて接続できます。



## 注記

複数の iSCSI ターゲットを指定するには、セルフホスト型エンジンをデプロイする前にマルチパスを有効にする必要があります。詳細は、[Red Hat Enterprise Linux DM マルチパス](#) を参照してください。[Multipath Helper](#) ツールを使用して、さまざまなオプションでマルチパスをインストールおよび設定するスクリプトを生成することもできます。

- Gluster ストレージの場合は、完全なアドレスおよびストレージへのパスならびにマウントオプションを入力します。



## 警告

仮想マシンのデータが失われるリスクがあるため、古いセルフホスト型エンジンストレージドメインのマウントポイントを新しいストレージドメインに使用しないでください。



## 重要

レプリカ 1 およびレプリカ 3 Gluster ストレージのみがサポートされます。必ず以下のようにボリュームを設定します。

```
gluster volume set VOLUME_NAME group virt
gluster volume set VOLUME_NAME performance.strict-o-direct on
gluster volume set VOLUME_NAME network.remote-dio off
gluster volume set VOLUME_NAME storage.owner-uid 36
gluster volume set VOLUME_NAME storage.owner-gid 36
gluster volume set VOLUME_NAME network.ping-timeout 30
```

- ファイバーチャネルの場合は、自動検出されたリストから LUN を選択します。ホストのバスアダプターが設定および接続されている必要があります。また、LUN には既存のデータが含まれないようにする必要があります。既存の LUN を再利用するには、[管理ガイドの LUN の再利用](#) を参照してください。
- Manager のディスクサイズを入力します。  
スクリプトはデプロイメントが完了するまで続行されます。
  - デプロイメントプロセスでは Manager の SSH キーが変更されます。クライアントマシンが SSH エラーなしで新規の Manager にアクセスできるようにするには、元の Manager にアクセスするクライアントマシンの **.ssh/known\_hosts** ファイルから元の Manager のエントリーを削除します。

デプロイメントが完了したら、新しい Manager 仮想マシンにログインし、必要なリポジトリを有効にします。

### 3.2.1.9.2. Red Hat Virtualization Manager リポジトリの有効化

ログインして、Red Hat Subscription Manager で Manager マシンを登録し、**Red Hat Virtualization Manager** のサブスクリプションをアタッチして Manager のリポジトリを有効にする必要があります。

## 手順

1. コンテンツ配信ネットワークにシステムを登録します。プロンプトが表示されたら、カスタマーポータルのユーザー名とパスワードを入力します。

```
subscription-manager register
```



### 注記

IPv6 ネットワークを使用している場合は、IPv6 移行メカニズムを使用して、コンテンツ配信ネットワークおよびサブスクリプションマネージャーにアクセスします。

2. **Red Hat Virtualization Manager** のサブスクリプションプールを見つけ、プール ID を記録します。

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

3. 上記のプール ID を使用して、サブスクリプションをシステムにアタッチします。

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



### 注記

現在アタッチされているサブスクリプションを表示するには、以下のコマンドを実行します。

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

有効なリポジトリをすべてリスト表示するには、以下のコマンドを実行します。

```
dnf repolist
```

4. リポジトリを設定します。

```
subscription-manager repos \
--disable='*' \
--enable=rhel-8-for-x86_64-baseos-eus-rpms \
--enable=rhel-8-for-x86_64-appstream-eus-rpms \
--enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
--enable=fast-datapath-for-rhel-8-x86_64-rpms \
--enable=jb-eap-7.4-for-rhel-8-x86_64-rpms \
--enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
--enable=rhceph-4-tools-for-rhel-8-x86_64-rpms
```

5. RHEL のバージョンを 8.6 に設定します。

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

6. **pki-deps** モジュールを有効にします。

```
dnf module -y enable pki-deps
```

7. **postgresql** モジュールのバージョン 12 を有効にします。

```
dnf module -y enable postgresql:12
```

8. **nodejs** モジュールのバージョン 14 を有効にします。

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

9. インストール済みパッケージを同期して、利用可能な最新バージョンに更新します。

```
dnf distro-sync --nobest
```

## 関連情報

モジュールおよびモジュールストリームの詳細は、[ユーザー空間コンポーネントのインストール、管理、および削除](#) の以下のセクションを参照してください。

- [モジュールストリーム](#)
- [パッケージインストールの前のストリーム選択](#)
- [モジュールストリームのリセット](#)
- [後のストリームへの切り替え](#)

Manager とそのリソースは、新しいセルフホスト環境で実行されています。セルフホスト型エンジンノードは、セルフホスト型エンジン設定を更新するために Manager に再インストールする必要があります。標準ホストは影響を受けません。セルフホスト型エンジンノードごとに次の手順を実行します。

### 3.2.1.9.3. ホストの再インストール

管理ポータルから Red Hat Virtualization Host (RHVH) および Red Hat Enterprise Linux ホストを再インストールします。この手順には、ホストの停止および再起動が含まれます。

#### 警告



ホストのオペレーティングシステムのインストールまたは再インストールを行う場合、Red Hat では、ホストにアタッチされている既存の OS 以外のストレージを最初にデタッチすることを強く推奨しています。これは、ディスクを誤って初期化してデータが失われる可能性を避けるためです。

## 前提条件

- クラスターの移行が有効化されている場合、仮想マシンはそのクラスター内の別のホストに自動的に移行できます。したがって、使用量が比較的低い間にホストを再インストールします。
- ホストによるメンテナンスの実行に必要なメモリーがクラスターにあることを確認します。クラスターにメモリーがない場合、仮想マシンの移行はハングして失敗します。メモリー使用量を減らすには、ホストをメンテナンスに移行する前に、一部またはすべての仮想マシンをシャットダウンします。
- 再インストールを実行する前に、クラスターに複数のホストが含まれていることを確認してください。すべてのホストを同時に再インストールしようとしないでください。Storage Pool Manager (SPM) タスクを実行するには、1台のホストは使用可能な状態でなければなりません。

## 手順

1. Compute → Hosts をクリックし、ホストを選択します。
2. Management → Maintenance をクリックしてから OK をクリックします。
3. Installation → Reinstall をクリックします。Install Host ウィンドウが表示されます。
4. Hosted Engine タブをクリックし、ドロップダウンリストから DEPLOY を選択します。
5. OK をクリックして、ホストを再インストールします。

ホストを再インストールし、そのステータスが Up に戻れば、仮想マシンをホストに戻すことができます。



### 重要

Red Hat Virtualization Host を Red Hat Virtualization Manager に登録し、これを再インストールした後、管理ポータルでそのステータスが誤って Install Failed と表示される場合があります。Management → Activate をクリックすると、ホストのステータスが Up に変わり、使用できるようになります。

セルフホスト型エンジンノードを再インストールした後に、いずれかのノードで以下のコマンドを実行して、新しい環境のステータスを確認できます。

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

復元中に、古いセルフホスト型エンジンのストレージドメインの名前が変更されたが、復元に問題があった場合に備えて、新しい環境からは削除されませんでした。環境が正常に実行されていることを確認したら、古いセルフホスト型エンジンストレージドメインを削除できます。

### 3.2.1.9.4. ストレージドメインの削除

データセンターに、仮想化環境から削除するストレージドメインがあります。

## 手順

1. Storage → Domains をクリックします。
2. ストレージドメインをメンテナンスモードに移動し、デタッチします。
  - a. ストレージドメインの名前をクリックします。詳細ビューが開きます。

- b. Data Center タブをクリックします。
  - c. Maintenance をクリックしてから **OK** をクリックします。
  - d. Detach をクリックしてから **OK** をクリックします。
3. Remove をクリックします。
4. オプションで Format Domain, i.e. Storage Content will be lost! チェックボックスを選択して、ドメインのコンテンツを消去します。
5. **OK** をクリックします。

ストレージドメインが環境から完全に削除されます。

### 3.2.1.10. 既存のバックアップからのセルフホスト型エンジンの上書き

セルフホスト型エンジンにアクセスできるが、データベースの破損や設定エラーなどロールバックが難しい問題が発生した場合、問題が発生する前に取ったバックアップがあれば、それを使用して以前の状態に環境を復元することができます。

セルフホスト型エンジンを以前の状態に復元するには、次の手順が必要です。

1. 環境をグローバルメンテナンスモードに切り替えます。
2. Manager 仮想マシンでバックアップを復元します。
3. グローバルメンテナンスモードを無効化します。

**engine-backup --mode=restore** オプションの詳細は、[Manager のバックアップおよび復元](#) を参照してください。

#### 3.2.1.10.1. グローバルメンテナンスモードの有効化

Manager 用仮想マシンの設定またはアップグレード作業を実施する前に、セルフホスト型エンジン環境をグローバルメンテナンスモードに切り替える必要があります。

##### 手順

1. セルフホスト型エンジンノードのいずれかにログインして、グローバルメンテナンスモードを有効にします。

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

2. 作業を進める前に、環境がグローバルメンテナンスモードにあることを確認します。

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

クラスターがグローバルメンテナンスモードにあることを示すメッセージが表示されるはずです。

#### 3.2.1.10.2. バックアップを復元して既存のインストールを上書き

**engine-backup** コマンドを使用すると、Red Hat Virtualization Manager がすでにインストールおよび設定されているマシンに、バックアップを復元できます。これは、環境のバックアップを作成し、その環境に変更を加えた後、バックアップから環境を復元して変更を元に戻したい場合に役立ちます。

バックアップ作成後に環境に加えられた、ホストの追加や削除などの変更は、復元された環境には表示されません。そのような変更はやり直す必要があります。

## 手順

1. 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
```

**engine-cleanup** コマンドは、Manager データベースのみを削除します。データベースを削除したり、そのデータベースを所有しているユーザーを削除したりすることはありません。

3. 完全バックアップまたはデータベースのみのバックアップを復元します。ユーザーとデータベースがすでに存在しているので、新規のデータベースを作成したり、データベースの認証情報を見つける必要はありません。
- 完全バックアップを復元します。

```
engine-backup --mode=restore --file=file_name --log=log_file_name --restore-permissions
```

- 設定ファイルおよびデータベースバックアップを復元して、データベースのみのバックアップを復元します。

```
engine-backup --mode=restore --scope=files --scope=db --scope=dwhdb --file=file_name --log=log_file_name --restore-permissions
```



### 注記

Manager データベースのみを復元するには(たとえば、Data Warehouse データベースが別のマシンにある場合)、**-scope=dwhdb** パラメーターを省略できます。

成功すると、次の出力が表示されます。

```
You should now run engine-setup.
Done.
```

4. Manager を再設定します。

```
engine-setup
```

### 3.2.1.10.3. グローバルメンテナンスモードの無効化

## 手順

- Manager 用仮想マシンにログインし、シャットダウンします。
- セルフホスト型エンジンノードのいずれかにログインして、グローバルメンテナンスモードを無効にします。

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

グローバルメンテナンスモードを終了すると、ovirt-ha-agent が Manager 用仮想マシンを起動し、続いて Manager が自動的に起動します。Manager が起動するまでに最大で 10 分程度かかる場合があります。

- 環境が動作していることを確認します。

**# hosted-engine --vm-status**

情報の一覧に、**Engine Status** が含まれます。**Engine status** の値は、以下のようになるはずです。

**{"health": "good", "vm": "up", "detail": "Up"}**



#### 注記

仮想マシンが起動中で Manager がまだ動作していない場合、**Engine status** は以下のようになります。

**{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}**

このような場合は、数分間待ってからやり直してください。

環境が再び実行している場合は、停止した仮想マシンを起動して、環境内のリソースが期待どおりに動作していることを確認できます。

### 3.2.2. データウェアハウスを別のマシンに移行

このセクションでは、Data Warehouse データベースおよびサービスを Red Hat Virtualization Manager マシンから別のマシンに移行する方法を説明します。Data Warehouse サービスを別のマシンでホストすると、各個別マシンの負荷が削減され、CPU やメモリーリソースを他のプロセスと共有することで競合が生じる可能性を回避できます。



#### 注記

Data Warehouse データベース、Data Warehouse サービス、Grafana はそれぞれ別々のマシンにインストールできますが、Red Hat はこれらの各コンポーネントをすべて同じマシンにインストールする場合のみサポートします。

以下の移行オプションがあります。

- Manager マシンから Data Warehouse サービスを移行し、既存の Data Warehouse データベース (**ovirt\_engine\_history**) に接続できます。
- Manager マシンから Data Warehouse データベースを移行してから、Data Warehouse サービスを移行することができます。

### 3.2.2.1. 別のマシンへの Data Warehouse データベースの移行

Data Warehouse サービスを移行する前に、Data Warehouse データベース (**ovirt\_engine\_history**) を移行します。**engine-backup** を使用してデータベースのバックアップを作成し、それを新規データベースマシンで復元します。**engine-backup** の詳細は、**engine-backup --help** を実行して確認してください。



#### 注記

Data Warehouse データベース、Data Warehouse サービス、Grafana はそれぞれ別々のマシンにインストールできますが、Red Hat はこれらの各コンポーネントをすべて同じマシンにインストールする場合のみサポートします。

新規データベースサーバーに Red Hat Enterprise Linux 8 がインストールされている必要があります。

新規データベースサーバーで必要なリポジトリを有効にします。

### 3.2.2.1.1. Red Hat Virtualization Manager リポジトリの有効化

ログインして、Red Hat Subscription Manager で Data Warehouse マシンを登録し、**Red Hat Virtualization Manager** のサブスクリプションをアタッチして Manager のリポジトリを有効にする必要があります。

#### 手順

1. コンテンツ配信ネットワークにシステムを登録します。プロンプトが表示されたら、カスタマーポータルのユーザー名とパスワードを入力します。

```
subscription-manager register
```



#### 注記

IPv6 ネットワークを使用している場合は、IPv6 移行メカニズムを使用して、コンテンツ配信ネットワークおよびサブスクリプションマネージャーにアクセスします。

2. **Red Hat Virtualization Manager** のサブスクリプションプールを見つけ、プール ID を記録します。

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

3. 上記のプール ID を使用して、サブスクリプションをシステムにアタッチします。

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



## 注記

現在アタッチされているサブスクリプションを表示するには、以下のコマンドを実行します。

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

有効なリポジトリをすべてリスト表示するには、以下のコマンドを実行します。

```
dnf repolist
```

4. リポジトリを設定します。

```
subscription-manager repos \
--disable='*' \
--enable=rhel-8-for-x86_64-baseos-eus-rpms \
--enable=rhel-8-for-x86_64-appstream-eus-rpms \
--enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
--enable=fast-datapath-for-rhel-8-x86_64-rpms \
--enable=jb-eap-7.4-for-rhel-8-x86_64-rpms \
--enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
--enable=rhceph-4-tools-for-rhel-8-x86_64-rpms
```

5. RHEL のバージョンを 8.6 に設定します。

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

6. **postgresql** モジュールのバージョン 12 を有効にします。

```
dnf module -y enable postgresql:12
```

7. **nodejs** モジュールのバージョン 14 を有効にします。

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

8. インストール済みパッケージを同期して、利用可能な最新バージョンに更新します。

```
dnf distro-sync --nobest
```

## 関連情報

モジュールおよびモジュールストリームの詳細は、**ユーザー空間コンポーネントのインストール、管理、および削除** の以下のセクションを参照してください。

- [モジュールストリーム](#)
- [パッケージインストールの前のストリーム選択](#)
- [モジュールストリームのリセット](#)
- [後のストリームへの切り替え](#)

### 3.2.2.1.2. 別のマシンへの Data Warehouse データベースの移行

#### 手順

- Manager で Data Warehouse データベースおよび設定ファイルのバックアップを作成します。

```
engine-backup --mode=backup --scope=grafanadb --scope=dwhdb --scope=files --
file=file_name --log=log_file_name
```

- そのバックアップファイルを Manager マシンから新たなマシンにコピーします。

```
scp /tmp/file_name root@new.dwh.server.com:/tmp
```

- engine-backup** を新しいマシンにインストールします。

```
dnf install ovirt-engine-tools-backup
```

- PostgreSQL サーバーパッケージをインストールします。

```
dnf install postgresql-server postgresql-contrib
```

- PostgreSQL データベースを初期化し、**postgresql** サービスを開始して、このサービスが起動時に開始されることを確認します。

```
su - postgres -c 'initdb'
systemctl enable postgresql
systemctl start postgresql
```

- 新しいマシンで Data Warehouse データベースを復元します。file\_name は、Manager からコピーされたバックアップファイルです。

```
engine-backup --mode=restore --scope=files --scope=grafanadb --scope=dwhdb --
file=file_name --log=log_file_name --provision-dwh-db
```

復元モードで **--provision-\*** オプションを使用すると、デフォルトで **--restore-permissions** が適用されます。

これで、Manager がホストされるマシンとは別のマシンで、Data Warehouse データベースがホストされるようになりました。Data Warehouse データベースを正常に復元したら、**engine-setup** コマンドの実行を指示するプロンプトが表示されます。このコマンドを実行する前に、Data Warehouse サービスを移行します。

### 3.2.2.2. 別のマシンへの Data Warehouse サービスの移行

Red Hat Virtualization Manager にインストールおよび設定した Data Warehouse サービスは、別のマシンに移行することができます。Data Warehouse サービスを別のマシンでホストすることは、Manager マシンの負荷を削減する上で役立ちます。

この手順では、Data Warehouse サービスのみを移行することに注意してください。

Data Warehouse サービスを移行する前に Data Warehouse データベース (**ovirt\_engine\_history**) を移行するには、[Data Warehouse のデータセットの別のマシンへの移行](#) を参照してください。



## 注記

Data Warehouse データベース、Data Warehouse サービス、Grafana はそれぞれ別々のマシンにインストールできますが、Red Hat はこれらの各コンポーネントをすべて同じマシンにインストールする場合のみサポートします。

## 前提条件

- Manager と Data Warehouse が同じマシン上にインストールおよび設定されている。
- 新たな Data Warehouse マシンを設定するには、以下を満たしている必要があります。
  - Manager の `/etc/ovirt-engine/engine.conf.d/10-setup-database.conf` ファイルからのパスワード。
  - Data Warehouse マシンから Manager データベースマシンの TCP ポート 5432 へのアクセス許可。
  - Manager の `/etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-database.conf` ファイルからの Data Warehouse データベースのユーザー名とパスワード。

[Data Warehouse データセットの別のマシンへの移行](#) で説明されている手順を使用して `ovirt_engine_history` データベースを移行した場合、バックアップには、そのマシンでのデータベースのセットアップ中に定義したこれらの認証情報が含まれます。

このシナリオのインストールでは、以下の 4 つのステップを実施する必要があります。

1. 新たな Data Warehouse マシンの準備
2. Manager マシンでの Data Warehouse サービスの停止
3. 新たな Data Warehouse マシンの設定
4. Manager マシンでの Data Warehouse パッケージの無効化

### 3.2.2.2.1. 新たな Data Warehouse マシンの準備

Red Hat Virtualization のリポジトリを有効にし、Red Hat Enterprise Linux 8 マシンに Data Warehouse セットアップパッケージをインストールします。

1. 必要なリポジトリを有効にします。
  - a. コンテンツ配信ネットワークにシステムを登録します。プロンプトが表示されたら、カスタマーportalのユーザー名とパスワードを入力します。
 

```
subscription-manager register
```
  - b. **Red Hat Virtualization Manager** のサブスクリプションプールを見つけ、プール ID を記録します。
 

```
subscription-manager list --available
```
  - c. 上記のプール ID を使用して、サブスクリプションをシステムにアタッチします。
 

```
subscription-manager attach --pool=pool_id
```
  - d. リポジトリを設定します。

```
subscription-manager repos \
--disable='*' \
--enable=rhel-8-for-x86_64-baseos-eus-rpms \
--enable=rhel-8-for-x86_64-appstream-eus-rpms \
--enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
--enable=fast-datapath-for-rhel-8-x86_64-rpms \
--enable=jb-eap-7.4-for-rhel-8-x86_64-rpms

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

2. **pki-deps** モジュールを有効にします。

```
dnf module -y enable pki-deps
```

3. 現在インストールされている全パッケージを最新の状態にします。

```
dnf upgrade --nobest
```

4. **ovirt-engine-dwh-setup** パッケージをインストールします。

```
dnf install ovirt-engine-dwh-setup
```

### 3.2.2.2. Manager マシンでの Data Warehouse サービスの停止

#### 手順

1. Data Warehouse サービスを停止します。

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

2. データベースがリモートマシンでホストされる場合は、**postgres.conf** ファイルを編集して手動でアクセス権限を付与する必要があります。**/var/lib/pgsql/data/postgresql.conf** ファイルを編集し、**listen\_addresses** 行を変更して以下と一致するようにします。

```
listen_addresses = '*'
```

その行が存在しない、またはコメントアウトされている場合は、手動で追加します。

Manager マシンでデータベースがホストされていて、そのデータベースが Red Hat Virtualization Manager のクリーンセットアップ中に設定された場合は、デフォルトでアクセス権限が付与されます。

3. **postgresql** サービスを再起動します。

```
systemctl restart postgresql
```

### 3.2.2.3. 新たな Data Warehouse マシンの設定

このセクションで示すオプションまたは設定の順序は、お使いの環境によって異なる場合があります。

1. **ovirt\_engine\_history** データベースと Data Warehouse サービスの両方を 同じ マシンに移行する場合は、以下のコマンドを実行します。移行しない場合は、次のステップに進みます。

-

```
sed -i '/^ENGINE_DB_/d' \
/etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-database.conf

sed -i \
-e 's;^(OVESETUP_ENGINE_CORE/enable=bool):True;\1:False;' \
-e '/^OVESETUP_CONFIGVfqdn/d' \
/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

2. apache/grafana PKI ファイルを削除して、**engine-setup** によって正しい値で再生成されるようにします。

```
rm -f \
/etc/pki/ovirt-engine/certs/apache.cer \
/etc/pki/ovirt-engine/certs/apache-grafana.cer \
/etc/pki/ovirt-engine/keys/apache.key.nopass \
/etc/pki/ovirt-engine/keys/apache-grafana.key.nopass \
/etc/pki/ovirt-engine/apache-ca.pem \
/etc/pki/ovirt-engine/apache-grafana-ca.pem
```

3. **engine-setup** コマンドを実行し、マシンでの Data Warehouse の設定を開始します。

```
engine-setup
```

4. **Enter** キーを押して自動検出されたホスト名をそのまま使用するか、別のホスト名を入力して **Enter** キーを押します。

Host fully qualified DNS name of this server [**autodetected host name**]:

5. **Enter** キーを押して、ファイアウォールを自動設定するか、**No** と入力し、**Enter** キーを押して、既存の設定を維持します。

Setup can automatically configure the firewall on this system.

Note: automatic configuration of the firewall may overwrite current settings.

Do you want Setup to configure the firewall? (Yes, No) [Yes]:

ファイアウォールの自動設定を選択した場合に、ファイアウォール管理機能がアクティブ化されていなければ、サポートされているオプション一覧から、選択したファイアウォール管理機能を指定するように要求されます。ファイアウォール管理機能の名前を入力して、**Enter** キーを押してください。この操作は、オプションが1つしかリストされていない場合でも必要です。

6. Manager の完全修飾ドメイン名およびパスワードを入力します。その他のフィールドについては、**Enter** キーを押してそれぞれのデフォルト値をそのまま使用します。

Host fully qualified DNS name of the engine server []: **engine-fqdn**

Setup needs to do some actions on the remote engine server. Either automatically, using ssh as root to access it, or you will be prompted to manually perform each such action.

Please choose one of the following:

1 - Access remote engine server using ssh as root

2 - Perform each action manually, use files to copy content around

(1, 2) [1]:

ssh port on remote engine server [22]:

root password on remote engine server **engine-fqdn**: **password**

7. Manager データベースマシンの完全修飾ドメイン名 (FQDN) およびパスワードを入力します。その他のフィールドについては、**Enter** キーを押してそれぞれのデフォルト値をそのまま使用します。

```
Engine database host []: manager-db-fqdn
Engine database port [5432]:
Engine database secured connection (Yes, No) [No]:
Engine database name [engine]:
Engine database user [engine]:
Engine database password: password
```

8. インストールの設定を確認します。

```
Please confirm installation settings (OK, Cancel) [OK]:
```

これで、Data Warehouse サービスがリモートマシンに設定されました。次は、Manager マシンの Data Warehouse サービスを無効にします。

### 3.2.2.2.4. Manager マシンでの Data Warehouse サービスの無効化

#### 前提条件

- Manager マシンの Grafana サービスが無効になっている。

```
systemctl disable --now grafana-server.service
```

#### 手順

1. Manager マシンで Manager を再起動します。

```
service ovirt-engine restart
```

2. 以下のコマンドを実行して `/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf` ファイルを変更し、オプションを **False** に設定します。

```
sed -i \
-e 's;^(OVESETUP_DWH_CORE/enable=bool):True;\1:False;' \
-e 's;^(OVESETUP_DWH_CONFIG/remoteEngineConfigured=bool):True;\1:False;' \
/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf

sed -i \
-e 's;^(OVESETUP_GRAFANA_CORE/enable=bool):True;\1:False;' \
/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

3. Data Warehouse サービスを無効にします。

```
systemctl disable ovirt-engine-dwhd.service
```

4. Data Warehouse に関するファイルを削除します。

```
rm -f /etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/*.conf /var/lib/ovirt-engine-dwh/backups/*
```

これで、Data Warehouse サービスが Manager とは別のマシンでホストされるようになりました。

### 3.2.3. バックアップストレージドメインを使用した仮想マシンのバックアップと復元

#### 3.2.3.1. バックアップストレージドメインの説明

バックアップストレージドメインは、災害復旧、移行、その他のバックアップ/復旧使用モデルにおけるバックアップと復元を目的として、仮想マシンおよび仮想マシンテンプレートの保存と移行に特化して使用できます。バックアップドメインは、バックアップドメイン上のすべての仮想マシンがパワーダウン状態にあるという点で、非バックアップドメインとは異なります。仮想マシンはバックアップドメインで実行できません。

任意のデータストレージドメインをバックアップドメインとして設定できます。Manage Domain ダイアログボックスのチェックボックスを選択または選択解除することで、この設定を有効または無効にできます。この設定を有効にできるのは、そのストレージドメイン上のすべての仮想マシンが停止した後でのみです。

バックアップドメインに保存されている仮想マシンを起動することはできません。Manager は、これと、バックアップを無効にする可能性のあるその他の操作をブロックします。ただし、仮想マシンのディスクがバックアップドメインの一部でない場合は、バックアップドメインに保存されているテンプレートに基づいて仮想マシンを実行できます。

他のタイプのストレージドメインと同様に、バックアップドメインをデータセンターに接続したり、データセンターから切り離したりできます。そのため、バックアップの保存に加え、バックアップドメインを使用してデータセンター間で仮想マシンを移行できます。

#### メリット

エクスポートドメインではなくバックアップドメインを使用するいくつかの理由を以下に示します。

- データセンターで、エクスポートドメインを1つだけ持つのではなく、複数のバックアップストレージドメインを持つことができます。
- バックアップストレージドメインをバックアップと障害復旧専用として使用できます。
- 仮想マシン、テンプレート、またはスナップショットのバックアップをバックアップストレージドメインに転送できます。
- 多数の仮想マシン、テンプレート、または OVF ファイルの移行は、エクスポートドメインよりもバックアップドメインの方が圧倒的に高速に行えます。
- バックアップドメインは、エクスポートドメインよりも効率的にディスクスペースを使用します。
- バックアップドメインは、ファイルストレージ (NFS、Gluster) とブロックストレージ (ファイバーチャネルと iSCSI) の両方をサポートします。これは、ファイルストレージのみをサポートするエクスポートドメインとは対照的です。
- 制限を考慮して、ストレージドメインのバックアップ設定を動的に有効または無効にできます。

#### 制約

- \_backup ドメイン上のすべての仮想マシンまたはテンプレートは、同じドメイン上にすべてのディスクを持っている必要があります。

- ストレージドメインをバックアップドメインとして設定する前に、ストレージドメイン上のすべての仮想マシンの電源を切る必要があります。
- バックアップドメインに保存されている仮想マシンは実行できません。実行すると、ディスクのデータが操作される可能性があるためです。
- メモリーボリュームはアクティブな仮想マシンでのみサポートされているため、バックアップドメインをメモリーボリュームのターゲットにできません。
- バックアップドメインでは仮想マシンをプレビューできません。
- 仮想マシンはバックアップドメインにライブ移行できません。
- バックアップドメインは **master** ドメインとして設定できません。
- セルフホスト型エンジンのドメインはバックアップドメインとして設定できません。
- デフォルトのストレージドメインをバックアップドメインとして使用しないでください。

### 3.2.3.2. データストレージドメインをバックアップドメインに設定

#### 前提条件

- ストレージドメイン上の仮想マシンまたはテンプレートに属するすべてのディスクは、同じドメイン上にある必要があります。
- ドメイン上のすべての仮想マシンの電源を切る必要があります。

#### 手順

- 管理ポータルで、Storage → Domains を選択します。
- 新しいストレージドメインを作成するか、既存のストレージドメインを選択して、Manage Domain をクリックします。ドメインの管理ダイアログボックスが開きます。
- Advanced Parameters で、Backup チェックボックスを選択します。

これで、ドメインはバックアップドメインになります。

### 3.2.3.3. バックアップドメインを使用した仮想マシンおよびスナップショットのバックアップと復元

電源がオフになっている仮想マシンまたはスナップショットをバックアップできます。その後、バックアップを同じデータセンターに保存して必要に応じて復元したり、別のデータセンターに移行したりできます。

#### 手順: 仮想マシンのバックアップ

- バックアップドメインを作成します。[ストレージドメインをバックアップドメインとして設定する](#) を参照してください。
- バックアップする仮想マシンをベースに、新しい仮想マシンを作成します。
  - スナップショットをバックアップするには、最初にスナップショットから仮想マシンを作成します。[Virtual Machine Management Guide](#) の [Creating a Virtual Machine from a Snapshot](#) を参照してください。

- 仮想マシンをバックアップするには、最初に仮想マシンのクローンを作成します。仮想マシン管理ガイドの[仮想マシンのクローン作成](#)を参照してください。続行する前に、クローンの電源がオフになっていることを確認してください。
3. 新しい仮想マシンをバックアップドメインにエクスポートします。仮想マシン管理ガイドの[データドメインへの仮想マシンのエクスポート](#)を参照してください。

#### 手順: 仮想マシンの復元

1. 仮想マシンのバックアップを保存するバックアップストレージドメインがデータセンターに接続されていることを確認してください。
2. バックアップドメインから仮想マシンをインポートします。[データドメインからの仮想マシンのインポート](#)を参照してください。

#### 関連情報

- [ストレージドメインのインポート](#)
- [同じ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](#)

### 3.2.4. バックアップおよびリストア API を使用した仮想マシンのバックアップおよび復元

#### 3.2.4.1. バックアップおよびリストア API

バックアップおよびリストア API は、仮想マシンのフルバックアップまたはファイルレベルのバックアップと復元を実行可能にする機能のコレクションです。API は、ライブスナップショットや REST API などの Red Hat Virtualization コンポーネントをいくつか組み合わせて、独立したソフトウェアプロバイダーが提供するバックアップソフトウェアが含まれる仮想マシンに接続できる一時ボリュームを作成して操作します。

サポートされているサードパーティのバックアップベンダーについては、[Red Hat Virtualization Ecosystem](#) を参照してください。

#### 3.2.4.2. 仮想マシンのバックアップ

バックアップおよびリストア API を使用して、仮想マシンをバックアップします。この手順では、バックアップを作成する仮想マシンと、バックアップを管理するためのソフトウェアがインストールされている仮想マシンの 2 つの仮想マシンがあることを前提としています。

#### 手順

1. REST API を使用して、バックアップを作成する仮想マシンのスナップショットを作成します。

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

<snapshot>
 <description>BACKUP</description>
</snapshot>
```



## 注記

- ここで、**{vm:id}** を、スナップショットを作成している仮想マシンの VM ID に置き換えます。この ID は、**管理ポータル** および **VM ポータル** の **New Virtual Machine** ウィンドウと **Edit Virtual Machine** ウィンドウの **General** タブから利用できます。
- 仮想マシンのスナップショットを作成すると、スナップショットの下の **initialization** にある **configuration** 属性の **data** 属性に現在の設定データが格納されます。



## 重要

共有可能としてマークされたディスク、または直接 LUN ディスクに基づくディスクのスナップショットを作成することはできません。

- スナップショットの下の **data** 属性から仮想マシンの設定データを取得します。

```
GET /api/vms/{vm:id}/snapshots/{snapshot:id} HTTP/1.1
All-Content: true
Accept: application/xml
Content-type: application/xml
```



## 注記

- ここで、**{vm:id}** を、以前にスナップショットを作成した仮想マシンの ID に置き換えます。**{snapshot:id}** をスナップショット ID に置き換えます。
- All-Content: true** ヘッダーを追加して、応答内の追加の OVF データを取得します。XML 応答の OVF データは、VM 設定要素 **<initialization>** **<configuration>** 内にあります。その後、このデータを使用して仮想マシンを復元します。

- スナップショット ID を取得します。

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

- スナップショットのディスク ID を特定します。

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

- スナップショットを、正しいインターフェイスタイプ(例: **virtio\_scsi**)を使用して、アクティブディスクアタッチメントとしてバックアップ仮想マシンにアタッチします。

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

<disk_attachment>
```

```
<active>true</active>
<interface>_virtio_scsi_</interface>
<disk id="{disk:id}">
<snapshot id="{snapshot:id}">/>
</disk>
</disk_attachment>
```



### 注記

ここで、**{vm:id}** を、以前にスナップショットを作成した仮想マシンではなく、バックアップ仮想マシンの ID に置き換えます。**{disk:id}** をディスク ID に置き換えます。**{snapshot:id}** をスナップショット ID に置き換えます。

6. バックアップ仮想マシンのバックアップソフトウェアを使用して、スナップショットディスク上のデータをバックアップします。
7. バックアップ仮想マシンからスナップショットディスクアタッチメントを削除します。

```
DELETE /api/vms/{vm:id}/diskattachments/{snapshot:id} HTTP/1.1
```

Accept: application/xml

Content-type: application/xml



### 注記

ここで、**{vm:id}** を、以前にスナップショットを作成した仮想マシンではなく、バックアップ仮想マシンの ID に置き換えます。**{snapshot:id}** をスナップショット ID に置き換えます。

8. 必要に応じて、スナップショットを削除します。

```
DELETE /api/vms/{vm:id}/snapshots/{snapshot:id} HTTP/1.1
```

Accept: application/xml

Content-type: application/xml



### 注記

ここで、**{vm:id}** を、以前にスナップショットを作成した仮想マシンの ID に置き換えます。**{snapshot:id}** をスナップショット ID に置き換えます。

これで、別の仮想マシンにインストールされたバックアップソフトウェアを使用して、特定の時点における仮想マシンの状態をバックアップしました。

### 3.2.4.3. 仮想マシンの復元

バックアップおよびリストア API を使用してバックアップされた仮想マシンを復元します。この手順は、前のバックアップの管理に使用されたソフトウェアがインストールされているバックアップ仮想マシンがあることを前提としています。

#### 手順

1. 管理ポータルで、バックアップを復元するフローティングディスクを作成します。フローティングディスクの作成方法の詳細は、[仮想ディスクの作成](#) を参照してください。

2. ディスクをバックアップ仮想マシンに接続します。

```
POST /api/vms/{vm:id}/disks/ HTTP/1.1
```

Accept: application/xml

Content-type: application/xml

```
<disk id="{disk:id}">
</disk>
```



#### 注記

ここで、**{vm:id}** を、以前にスナップショットを作成した仮想マシンではなく、このバックアップ仮想マシンの ID に置き換えます。**{disk:id}** を、仮想マシンのバックアップ時に取得したディスク ID に置き換えます。

3. バックアップソフトウェアを使用して、バックアップをディスクに復元します。

4. バックアップ仮想マシンからディスクの割り当てを解除します。

```
DELETE /api/vms/{vm:id}/disks/{disk:id} HTTP/1.1
```

Accept: application/xml

Content-type: application/xml

```
<action>
 <detach>true</detach>
</action>
```



#### 注記

ここで、**{vm:id}** を、以前にスナップショットを作成した仮想マシンではなく、このバックアップ仮想マシンの ID に置き換えます。**{disk:id}** をディスク ID に置き換えます。

5. 復元される仮想マシンの設定データを使用して、新しい仮想マシンを作成します。

```
POST /api/vms/ HTTP/1.1
```

Accept: application/xml

Content-type: application/xml

```
<vm>
 <cluster>
 <name>cluster_name</name>
 </cluster>
 <name>_NAME_</name>
 <initialization>
 <configuration>
 <data>
 <!-- omitting long ovf data -->
 </data>
 <type>ovf</type>
 </configuration>
```

```
</initialization>
...
</vm>
```

**注記**

仮想マシンの作成時に ovf の任意の値を上書きするには、**initialization** 要素の前または後に要素を再定義します。initialization 要素内では定義しません。

## 6. ディスクを新規の仮想マシンにアタッチします。

```
POST /api/vms/{vm:id}/disks/ HTTP/1.1
```

Accept: application/xml

Content-type: application/xml

```
<disk id="{disk:id}">
</disk>
```

**注記**

ここで、**{vm:id}** を、以前にスナップショットを作成した仮想マシンではなく、新しい仮想マシンの ID に置き換えます。**{disk:id}** をディスク ID に置き換えます。

バックアップおよびリストア API を使用して作成されたバックアップを使用して、仮想マシンを復元しました。

### 3.2.5. 増分バックアップおよびリストア API を使用した仮想マシンのバックアップと復元

#### 3.2.5.1. 増分バックアップおよび復元 API

Red Hat Virtualization は、QCOW2 または RAW 仮想ディスクの完全バックアップ、もしくは QCOW2 仮想ディスクの増分バックアップに、一時的なスナップショットなしで使用できる増分バックアップ API を提供します。バックアップされる仮想ディスクが QCOW2 であるか RAW であるかに関係なく、データは RAW 形式でバックアップされます。RAW ゲストデータ、および RAW または QCOW2 ディスクのいずれかを復元できます。増分バックアップ API は、RHV REST API の一部です。実行中または実行されていない仮想マシンをバックアップできます。

開発者は、API を使用してバックアップアプリケーションを開発できます。

#### 機能

バックアップは、バックアップと復元 API を使用する場合よりも簡単、高速、堅牢です。増分バックアップ API は、バックアップアプリケーションとの統合を改善し、基盤となるディスクフォーマットに関係なく RAW ゲストデータのバックアップと復元を新たにサポートします。

無効なビットマップが原因でバックアップが失敗した場合は、バックアップチェーン内の特定のチェックポイントを削除できます。完全バックアップを実行する必要はありません。

#### 制限事項:

- RAW 形式のディスクではなく、QCOW2 形式のディスクのみを増分バックアップできます。バックアッププロセスでは、バックアップされたデータが RAW 形式で保存されます。
- 復元できるのは、RAW 形式でバックアップされたデータのみです。
- 増分リストアは、バックアップ時に存在していたスナップショットの復元をサポートしていません。増分リストアは、バックアップ時に存在していたスナップショット内のボリュームまたはイメージの構造ではなく、データのみを復元します。この制限は、他のシステムのバックアップソリューションでは一般的です。
- バックアップソリューションの場合と同様に、増分リストアではデータのみが復元され、バックアップ時に存在していたスナップショットのボリュームやイメージの構造は復元されません。
- 原因が何であれ、仮想マシンのクリーンでないシャットダウンは、ディスク上のビットマップを無効にし、バックアップチェーン全体を無効にする可能性があります。無効なビットマップを使用して増分バックアップを復元すると、仮想マシンのデータが破損します。バックアップを開始する以外に、無効なビットマップを検出する方法はありません。ディスクに無効なビットマップが含まれていると、操作は失敗します。

次の表に、増分バックアップをサポートするディスク設定を示します。



### 注記

管理ポータルを使用してディスクを作成するときは、ストレージタイプ、プロジェクトニングタイプ、および増分バックアップを有効にするか無効にするかを設定します。これらの設定に基づいて、Manager は仮想ディスクの形式を決定します。

表3.1 増分バックアップでサポートされているディスク設定

ストレージタイプ	プロジェクトニングタイプ	増分バックアップの場合	仮想ディスクの形式
block	thin	enabled	qcow2
block	preallocated	enabled	qcow2 (preallocated)
file	thin	enabled	qcow2
file	preallocated	enabled	qcow2 (preallocated)
block	thin	disabled	qcow2
block	preallocated	disabled	raw (preallocated)
file	thin	disabled	raw (sparse)
file	preallocated	disabled	raw (preallocated)
network	該当なし	disabled	raw
lun	該当なし	disabled	raw

### 3.2.5.1.1. 増分バックアップのフロー

増分バックアップ API を使用するバックアップアプリケーションは、次の順序に従って、増分バックアップがすでに有効になっている仮想マシンディスクをバックアップする必要があります。

1. バックアップアプリケーションは、REST API を使用して、バックアップに含める必要のある [仮想マシンディスクを検索](#) します。QCOW2 形式のディスクのみが含まれています。
2. バックアップアプリケーションは、[完全バックアップ](#) または [増分バックアップ](#) を開始します。API呼び出しは、仮想マシン ID、オプションの以前のチェックポイント ID、およびバックアップするディスクのリストを指定します。API呼び出しで以前のチェックポイント ID が指定されていない場合は、各ディスクの現在の状態に基づいて、指定されたディスク内のすべてのデータを含む完全バックアップが開始されます。
3. エンジンは、バックアップ用に仮想マシンを準備します。仮想マシンは、バックアップ中も実行を継続できます。
4. バックアップアプリケーションは、バックアップを開始する準備ができたことをエンジンが報告するまで、バックアップステータスについてエンジンをポーリングします。
5. バックアップを開始する準備ができると、バックアップアプリケーションは、バックアップに含まれるすべてのディスクに対して [イメージ転送オブジェクトを作成](#) します。
6. バックアップアプリケーションは、[イメージ転送ごとに ovirt-imageio から変更されたブロックのリストを取得](#) します。変更リストが利用できない場合、バックアップアプリケーションはエラーになります。
7. バックアップアプリケーションは、[変更されたブロックを RAW 形式で ovirt-imageio からダウンロードし、バックアップメディアに保存](#) します。変更されたブロックのリストが利用できない場合、バックアップアプリケーションはディスク全体のコピーにフォールバックできます。
8. バックアップアプリケーションは、すべてのイメージ転送を完了します。
9. バックアップアプリケーションは、[REST API を使用してバックアップを完了](#) します。

### 3.2.5.1.2. 増分リストアのフロー

増分バックアップ API を使用するバックアップアプリケーションは、次の手順に従って、バックアップされた仮想マシンディスクを復元する必要があります。

1. ユーザーは、バックアップアプリケーションを使用して、使用可能なバックアップに基づき復元ポイントを選択します。
2. バックアップアプリケーションは、復元されたデータを保持するために、新しいディスク、または既存のディスクを持つスナップショットを作成します。
3. バックアップアプリケーションは、[format が raw であることを指定して、ディスクごとにアップロードイメージの転送を開始](#) します。これにより、RAW データを QCOW2 ディスクにアップロードするときにフォーマット変換が可能になります。
4. バックアップアプリケーションは、[API を使用してこの復元ポイントに含まれるデータを imageio に転送](#) します。
5. バックアップアプリケーションは、イメージ転送を完了します。

### 3.2.5.1.3. 増分バックアップおよびリストア API タスク

増分バックアップおよび復元 API は、[Red Hat Virtualization REST API ガイド](#) に記載されています。バックアップおよび復元のフローには、以下のアクションが必要です。

- 新規または既存の仮想ディスクで増分バックアップを有効にします。
  - [新規ディスク \(管理ポータルを使用\)](#)
  - [既存ディスク \(管理ポータルを使用\)](#)
  - [新規または既存のディスク \(API呼び出しを使用\)](#)
- 増分バックアップが有効になっているディスクの検索
- フルバックアップの開始
- 増分バックアップの開始
- バックアップのファイナライズ
- バックアップに関する情報の取得
- バックアップ内のディスクに関する情報を取得
- 仮想マシンのすべてのチェックポイントを一覧表示
- 特定の仮想マシンチェックポイントのリスト情報
- 特定の仮想マシンのチェックポイントを削除
- バックアップをアーカイブするためのイメージ転送オブジェクトのダウンロード
- バックアップを復元するためのイメージ転送オブジェクトのアップロード
- 変更されたロックの一覧表示
- 変更されたロックのダウンロードとアップロード

#### 3.2.5.1.4. 新しい仮想ディスクでの増分バックアップの有効化

仮想ディスクの増分バックアップを有効にして、仮想ディスクを増分バックアップに含まれるものとしてマークします。ディスクを追加する場合は、REST API または管理ポータルを使用して、すべてのディスクの増分バックアップを有効にできます。フルバックアップを使用するか、以前と同じ方法を適用して、増分バックアップが有効にならない既存のディスクをバックアップできます。



#### 注記

Manager では、ディスクを増分バックアップに含めるためにディスクを有効にする必要はありませんが、有効になっているディスクを追跡するために有効にすることができます。

増分バックアップではディスクを QCOW2 でフォーマットする必要があるため、RAW 形式ではなく QCOW2 形式を使用してください。

#### 手順

1. 新しい仮想ディスクを追加します。詳細は、[仮想ディスクの作成](#) を参照してください。

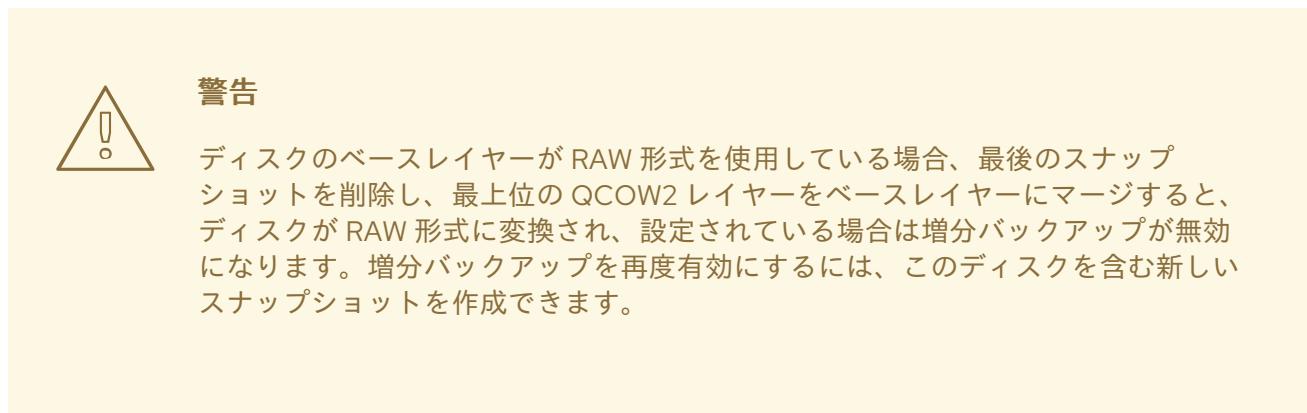
2. ディスクを設定するときは、**Enable Incremental Backup** チェックボックスをオンにします。

## 関連情報

- API を使用したディスクの増分バックアップの有効化

### 3.2.5.1.5. 既存の RAW 仮想ディスクでの増分バックアップの有効化

増分バックアップは RAW 形式のディスクではサポートされていないため、増分バックアップを使用するには、すべての RAW 形式のディスクの上に QCOW2 形式のレイヤーが存在する必要があります。スナップショットを作成すると、QCOW2 レイヤーが生成され、スナップショットが作成された時点から、スナップショットに含まれるすべてのディスクで増分バックアップが有効になります。



## 手順

1. 管理ポータルで **Compute → Virtual Machines** をクリックします。
2. 仮想マシンを選択し、**Disks** タブをクリックします。
3. **Edit** ボタンをクリックします。**Edit Disk** ダイアログボックスが開きます。
4. **Enable Incremental Backup** チェックボックスを選択します。

## 関連情報

- API を使用したディスクの増分バックアップの有効化

### 3.2.5.1.6. 増分バックアップの有効化

REST API リクエストを使用して、仮想マシンのディスクの増分バックアップを有効にできます。

## 手順

- 新しいディスクの増分バックアップを有効にします。たとえば、ID **123** の仮想マシンの新規ディスクでは、以下の要求を送信します。

POST /ovirt-engine/api/vms/123/diskattachments

要求の本文には、次のように、**disk** オブジェクトの一部として **incremental** に設定された **backup** を含める必要があります。

<disk\_attachment>

```

...
<disk>
...
<backup>incremental</backup>
...
</disk>
</disk_attachment>
```

応答は次のとおりです。

```

<disk_attachment>
...
<disk href="/ovirt-engine/api/disks/456" id="456"/>
...
</disk_attachment>
```

## 関連情報

- RHV 用 REST API ガイドの [DiskBackup 列挙型](#)

### 3.2.5.1.7. 増分バックアップが有効になっているディスクの検索

指定した仮想マシンについて、増分バックアップが有効になっているディスクを、バックアッププロパティに従ってフィルタリングして一覧表示できます。

## 手順

- 仮想マシンに接続されているディスクを一覧表示します。たとえば、ID **123** の仮想マシンの場合、以下の要求を送信します。

```
GET /ovirt-engine/api/vms/123/diskattachments
```

応答にはすべての **disk\_attachment** オブジェクトが含まれ、各オブジェクトには1つ以上の **disk** オブジェクトが含まれます。以下に例を示します。

```

<disk_attachments>
 <disk_attachment>
 ...
 <disk href="/ovirt-engine/api/disks/456" id="456"/>
 ...
 </disk_attachment>
 ...
</disk_attachments>
```

- disk** サービスを使用して、前の手順のディスクプロパティーを表示します。たとえば、ID **456** のディスクの場合は、以下の要求を送信します。

```
GET /ovirt-engine/api/disks/456
```

応答には、ディスクのすべてのプロパティーが含まれます。**backup** は **none** または **incremental** に設定されています。以下に例を示します。

```
<disk href="/ovirt-engine/api/disks/456" id="456">
```

```

...
<backup>incremental</backup>
...
</disk>
```

## 関連情報

- [Disk 構造体の backup 属性](#)
- [DiskBackup 列挙型](#)

### 3.2.5.1.8. フルバックアップの開始

フルバックアップの後、作成されたチェックポイント ID を次の増分バックアップの開始点として使用できます。

実行中の仮想マシンのバックアップを作成する場合、プロセスは、バックアップされるディスクと同じストレージドメインにスクラッチディスクを作成します。バックアッププロセスではこのディスクを作成して、バックアップ中に実行中の仮想マシンに新しいデータを書き込めるようにします。このスクラッチディスクは、バックアップ中に管理ポータルで確認できます。バックアップが終了すると自動的に削除されます。

フルバックアップを開始するには、本文を使用した要求呼び出しが必要であり、応答が含まれます。

## 手順

1. バックアップを作成する仮想マシンを指定する要求を送信します。たとえば、以下のように ID **123** の仮想マシンを指定します。

```
POST /ovirt-engine/api/vms/123/backups
```

2. 要求の本文で、バックアップを作成するディスクを指定します。たとえば、ID **456** のディスクのフルバックアップを開始するには、以下の要求本文を送信します。

```

<backup>
 <disks>
 <disk id="456" />
 ...
 </disks>
</backup>
```

応答本文は以下のようになります。

```

<backup id="789">
 <disks>
 <disk id="456" />
 ...
 </disks>
 <status>initializing</status>
 <creation_date>
</backup>
```

応答には以下が含まれます。

- バックアップ ID
  - バックアップのステータス。バックアップが初期化中であることを示します。
3. ステータスが **ready** になるまでバックアップをポーリングします。応答には、**to\_checkpoint\_id** が含まれます。この ID をメモし、次の増分バックアップで **from\_checkpoint\_id** に使用します。

## 関連情報

- RHV の REST API ガイドにおける [VmBackups サービスの add メソッド](#)

### 3.2.5.1.9. 増分バックアップの開始

特定の仮想ディスクのフルバックアップが完了すると、そのディスクの後続の増分バックアップには、最後のバックアップ以降の変更のみが含まれます。最新のバックアップの **to\_checkpoint\_id** の値を、要求本文の **from\_checkpoint\_id** の値として使用します。

実行中の仮想マシンのバックアップを作成する場合、プロセスは、バックアップされるディスクと同じストレージドメインにスクラッチディスクを作成します。バックアッププロセスではこのディスクを作成して、バックアップ中に実行中の仮想マシンに新しいデータを書き込めるようにします。このスクラッチディスクは、バックアップ中に管理ポータルで確認できます。バックアップが終了すると自動的に削除されます。

増分バックアップまたは混合バックアップを開始するには、本文を使用した要求呼び出しが必要であり、応答が含まれます。

## 手順

1. バックアップを作成する仮想マシンを指定する要求を送信します。たとえば、以下のように ID **123** の仮想マシンを指定します。

```
POST /ovirt-engine/api/vms/123/backups
```

2. 要求の本文で、バックアップを作成するディスクを指定します。たとえば、ID **456** のディスクの増分バックアップを開始するには、以下の要求本文を送信します。

```
<backup>
 <from_checkpoint_id>previous-checkpoint-uuid</from_checkpoint_id>
 <disks>
 <disk id="456" />
 ...
 </disks>
</backup>
```



## 注記

要求本文に、前のチェックポイントに含まれていないディスクを含めると、要求はこのディスクの完全バックアップも実行します。たとえば、ID **789** のディスクはまだバックアップされていません。上記の要求本文に **789** のフルバックアップを追加するには、次のような要求本文を送信します。

```
<backup>
 <from_checkpoint_id>previous-checkpoint-uuid</from_checkpoint_id>
 <disks>
 <disk id="456" />
 <disk id="789" />
 ...
 </disks>
</backup>
```

応答本文は以下のようになります。

```
<backup id="101112">
<from_checkpoint_id>previous-checkpoint-uuid</from_checkpoint_id>
<to_checkpoint_id>new-checkpoint-uuid</to_checkpoint_id>
<disks>
 <disk id="456" />
 <disk id="789" />
 ...
 ...
</disks>
<status>initializing</status>
<creation_date>
</backup>
```

応答には以下が含まれます。

- バックアップ ID
- バックアップに含まれていたディスクの ID。
- バックアップが初期化中であることを示すステータス。

3. ステータスが **ready** になるまでバックアップをポーリングします。応答には、**to\_checkpoint\_id** が含まれます。この ID をメモし、次の増分バックアップで **from\_checkpoint\_id** に使用します。

## 関連情報

- RHV の REST API ガイドにおける [VmBackups サービスの add メソッド](#)

### 3.2.5.1.10. バックアップに関する情報の取得

新しい増分バックアップを開始するために使用できるバックアップに関する情報を取得できます。

VmBackups サービスの **list** メソッドは、バックアップに関する次の情報を返します。

- バックアップされた各ディスクの ID

- バックアップの開始チェックポイントおよび終了チェックポイントの ID
  - バックアップに含まれる各ディスクの、バックアップディスクイメージの ID。
  - バックアップのステータス
  - バックアップが作成された日付

<status> の値が **ready** になると、応答には <to\_checkpoint\_id> が含まれます。これは次の増分バックアップで <from\_checkpoint\_id> として使用され、仮想マシンストレージのバックアップにディスクのダウンロードを開始できます。

手順

- ID 123 の仮想マシンの ID 456 のバックアップに関する情報を取得するには、以下のような要求を送信します。

GET /ovirt-engine/api/vms/456/backups/123

応答には、ID 456 のバックアップ (<from\_checkpoint\_id> 999 と <to\_checkpoint\_id> 666) が含まれます。バックアップに含まれるディスクは、<link> 要素で参照されます。

```
<backup id="456">
 <from_checkpoint_id>999</from_checkpoint_id>
 <to_checkpoint_id>666</to_checkpoint_id>
 <link href="/ovirt-engine/api/vms/456/backups/123/disks" rel="disks"/>
 <status>ready</status>
 <creation_date>
</backup>
```

関連情報

- VmBackups サービスの `list` メソッド

### 3.2.5.1.11. バックアップ内のディスクに関する情報を取得

バックアップの各ディスクに使用されたバックアップモードなど、バックアップの一部であるディスクに関する情報を取得できます。これは、バックアップのダウンロードに使用するモードを決定するのに役立ちます。

`VmBackupDisks` サービスの `list` メソッドは、バックアップに関する次の情報を返します。

- バックアップされた各ディスクの ID および名前。
  - バックアップに含まれる各ディスクの、バックアップディスクイメージの ID。
  - ディスクのフォーマット。
  - ディスクでサポートされているバックアップ動作。
  - ディスク用に作成されたバックアップタイプ(フル/増分)。

手順

- ID 123 の仮想マシンの ID 456 のバックアップに関する情報を取得するには、以下のような要求を送信します。

■ GET /ovirt-engine/api/vms/456/backups/123/disks

応答には ID 789 のディスクが含まれ、ディスクイメージの ID は 555 です。

```
<disks>
 <disk id="789">
 <name>vm1_Disk1</name>
 <actual_size>671744</actual_size>
 <backup>incremental</backup>
 <backup_mode>full</backup_mode>
 <format>cow</format>
 <image_id>555</image_id>
 <qcow_version>qcow2_v3</qcow_version>
 <status>locked</status>
 <storage_type>image</storage_type>
 <total_size>0</total_size>
 </disk>
</disks>
```

## 関連情報

- [VmBackupDisks サービスの list メソッド](#)

### 3.2.5.1.12. バックアップのファイナライズ

バックアップをファイナライズすると、バックアップが終了し、リソースのロックが解除され、クリーンアップが実行されます。バックアップサービスの **finalize** 方法を使用する

## 手順

- ID が **123** の仮想マシンで ID が **456** のディスクのバックアップをファイナライズするには、次のような要求を送信します。

■ POST /vms/123/backups/456/finalize

## 関連情報

- [REST API ガイドで POST をファイナライズ](#) します。

### 3.2.5.1.13. 増分バックアップ用のイメージ転送オブジェクトの作成

バックアップをダウンロードする準備ができたら、バックアップアプリケーションは **imagetransfer** オブジェクトを作成する必要があります。これにより、増分バックアップの転送が開始されます。

イメージ転送オブジェクトを作成するには、本文を使用した要求呼び出しが必要です。

## 手順

1. 次のような要求を送信します。

■ POST /ovirt-engine/api/imagetransfers

2. 要求本文で、次のパラメーターを指定します。

- ディスク ID
- バックアップ ID
- **download** するディスクセットの方向
- **raw** に設定されたディスクのフォーマット

たとえば、ディスクの ID が **123** で、バックアップの ID が **456** であるディスクのバックアップを転送するには、次の要求本文を送信します。

```
<image_transfer>
 <disk id="123"/>
 <backup id="456"/>
 <direction>download</direction>
 <format>raw</format>
</image_transfer>
```

## 関連情報

- RHV の REST API ガイドの [imagetransfer オブジェクトを作成するための add メソッド](#)。

### 3.2.5.1.14. 増分リストア用のイメージ転送オブジェクトの作成

増分バックアップ API を使用してバックアップされた raw データを QCOW2 フォーマットのディスクに復元できるようにするには、バックアップアプリケーションで **imagetransfer** オブジェクトを作成する必要があります。

転送フォーマットが **raw** で、基礎となるディスクフォーマットが QCOW2 の場合、アップロードされたデータは、ストレージへの書き込み時にオンザフライで QCOW2 フォーマットに変換されます。QCOW2 ディスクから RAW ディスクへのデータのアップロードはサポートされていません。

イメージ転送オブジェクトを作成するには、本文を使用した要求呼び出しが必要です。

## 手順

1. 次のような要求を送信します。

```
POST /ovirt-engine/api/imagetransfers
```

2. 要求本文で、次のパラメーターを指定します。

- ディスク ID またはスナップショット ID
- **upload** を行うディスクセットの方向
- **raw** に設定されたディスクのフォーマット

たとえば、ディスクの ID が **123** であるディスクのバックアップを転送するには、次の要求本文を送信します。

```
<image_transfer>
```

```
<disk id="123"/>
<direction>upload</direction>
<format>raw</format>
</image_transfer>
```

## 関連情報

- RHV の REST API ガイドの [imagetransfer オブジェクトを作成するための add メソッド](#)。

### 3.2.5.1.15. 仮想マシンのチェックポイントの一覧表示

要求呼び出しを送信することにより、各チェックポイントの情報を含む、仮想マシンのすべてのチェックポイントを一覧表示できます。

## 手順

- 仮想マシンを指定する要求を送信します。たとえば、以下のように ID **123** の仮想マシンを指定します。

```
GET /vms/123/checkpoints/
```

応答には、すべての仮想マシンのチェックポイントが含まれます。各チェックポイントには、次の情報が含まれています。

- チェックポイントのディスク
- 親チェックポイントの ID
- チェックポイントの作成日
- 所属する仮想マシン

以下に例を示します。

```
<parent_id>, <creation_date> and the virtual machine it belongs to <vm>:
<checkpoints>
 <checkpoint id="456">
 <link href="/ovirt-engine/api/vms/vm-uuid/checkpoints/456/disks" rel="disks"/>
 <parent_id>parent-checkpoint-uuid</parent_id>
 <creation_date>xxx</creation_date>
 <vm href="/ovirt-engine/api/vms/123" id="123"/>
 </checkpoint>
</checkpoints>
```

## 関連情報

- RHV の REST API ガイドの [仮想マシンチェックポイントを一覧表示する list メソッド](#)

### 3.2.5.1.16. 仮想マシンの特定チェックポイントの一覧表示

要求呼び出しを送信することにより、仮想マシンの特定チェックポイントの情報を一覧表示できます。

## 手順

- 仮想マシンを指定する要求を送信します。たとえば、以下のように ID **123** の仮想マシンと ID **456** のチェックポイントを指定します。

```
GET /vms/123/checkpoints/456
```

応答には、チェックポイントに関する次の情報が含まれます。

- チェックポイントのディスク
- 親チェックポイントの ID
- チェックポイントの作成日
- 所属する仮想マシン

以下に例を示します。

```
<checkpoint id="456">
 <link href="/ovirt-engine/api/vms/vm-uuid/checkpoints/456/disks" rel="disks"/>
 <parent_id>parent-checkpoint-uuid</parent_id>
 <creation_date>xxx</creation_date>
 <vm href="/ovirt-engine/api/vms/123" id="123"/>
</checkpoint>
```

## 関連情報

- RHV の REST API ガイドの [仮想マシンチェックポイントを一覧表示する list メソッド](#)

### 3.2.5.1.17. チェックポイントの削除

DELETE 要求を送信して、仮想マシンのチェックポイントを削除できます。仮想マシンが実行しているかどうかに関係なく、仮想マシン上のチェックポイントを削除できます。

## 手順

- 仮想マシンおよびチェックポイントを指定してリクエストを送信します。たとえば、以下のように ID **123** の仮想マシンと、ID **456** のチェックポイントを指定します。

```
DELETE /vms/123/checkpoints/456/
```

## 関連情報

- [VmCheckpoint の remove メソッド](#)

### 3.2.5.1.18. imageio API を使用したバックアップデータの転送

イメージ転送 API は、イメージ転送を開始および停止します。結果は転送 URL です。

imageio API を使用して、転送 URL から実際にデータを転送します。

imageio API の使用方法に関する詳細は、[ovirt-imageio Images API リファレンス](#) を参照してください。

表3.2 増分バックアップと復元で使用される imageio Image API メソッド

API 要求	説明	imageio Image API リファレンスセクション
<b>OPTIONS /images/{ticket-id}</b> HTTP/1.1	サーバーオプションを取得して、サーバーがサポートする機能を確認します。	OPTIONS を参照してください。
<b>GET /images/{ticket-id}/extents</b>	ディスクイメージのコンテンツと割り当て、または増分バックアップ中に変更されたブロックに関する情報を取得します。この情報は、エクステント情報として知られています。	EXTENTS を参照してください。
<b>GET /images/{ticket-id}/extent?context=dirty</b>	イメージ転送を行うプログラムは、バックアップから変更をダウンロードする必要があります。これらの変更は、ダーティエクステントとして知られています。変更をダウンロードするには、次のようなリクエストを送信します。	EXTENTS→Examples→Request dirty extents を参照してください。
<b>PUT /images/{ticket-id}</b>	バックアップアプリケーションは、復元されたデータを保持するために、新しいディスク、または既存のディスクを持つスナップショットを作成します。	PUT を参照してください。

## 関連情報

Red Hat Virtualization Python SDK には、バックアップの転送を開始するために使用できるいくつかの実装例が含まれています。

- [ovirt-imageio Images API リファレンス](#)
- [ディスクの作成](#)
- [imagetransfer.create\\_transfer\(\) の呼び出し](#)
- [転送の作成を簡素化するヘルパー](#)
- [Red Hat Virtualization Python SDK の使用](#)

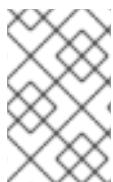
## 3.3. RED HAT SATELLITE を使用したエラータ表示の設定

管理ポータルでは、Red Hat Virtualization Manager で Red Hat Satellite からエラータを表示するように Red Hat Virtualization を設定できます。ホスト、仮想マシン、および Manager を Red Hat Satellite プロバイダーに関連付けた後、利用可能なエラータとその重要性に関する最新情報を受け取り、それらをいつ適用するかを決定できます。Red Hat Satellite の詳細は、[Red Hat Satellite ドキュメント](#) を参照してください。

Red Hat Virtualization 4.4 は、Red Hat Satellite 6.6 でのエラータの表示をサポートします。

## 前提条件

- Satellite サーバーが外部プロバイダーとして追加されている。
- Manager、ホスト、および仮想マシンはすべて、それぞれの FQDN によって Satellite サーバーに登録されている。これにより、外部コンテンツホスト ID を Red Hat Virtualization で維持する必要がなくなります。
- Manager、ホスト、および仮想マシンを管理する Satellite アカウントに、管理者パーミッションとデフォルトの組織セットがある。



### 注記

Katello エージェントは非推奨で、今後の Satellite のバージョンで削除されます。プロセスを移行し、リモート実行機能を使用してクライアントをリモートで更新してください。

## Red Hat Virtualization エラータの設定

Manager、ホスト、および仮想マシンを Red Hat Satellite プロバイダーに関連付けるには、以下のタスクを実行します。

1. 必要な Satellite サーバーを外部プロバイダーとして Manager に追加します。
2. 使用可能なエラータを表示するように必要なホストを設定します。
3. 使用可能なエラータを表示するように必要な仮想マシンを設定します。

## Red Hat Virtualization Manager エラータの表示

1. Administration → Errata をクリックします。
2. これらのエラータタイプのみを表示するには、Security、Bugs、または Enhancements チェックボックスをオンにします。

## 関連情報

- ホストの Satellite エラータ管理の設定
- Red Hat Enterprise Linux 仮想マシンの [仮想マシン管理ガイド](#) の [Linux でのゲストエージェント、ツール、ドライバーのインストール](#)
- Windows 仮想マシンの [仮想マシン管理ガイド](#) の [Windows でのゲストエージェント、ツール、ドライバーのインストール](#)
- ホストのエラータの表示
- 詳細は、[仮想マシン管理ガイド](#) の [仮想マシンの Satellite エラータ表示の設定](#) を参照してください。
- [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](#)。

## 3.4. 有効期限が切れる前の証明書更新

バージョン 4.4 SP1 より前の Red Hat Virtualization では、すべての証明書の有効期間は 398 日でした。Red Hat Virtualization バージョン 4.4 SP1 以降、ハイパーテナントと Manager 間の自己署名内部

証明書の有効期間は 5 年間です。Web ブラウザーに表示される証明書は、引き続き標準の 398 日の有効期間に従い、年に 1 回更新する必要があります。



### 警告

証明書を期限切れにしないでください。証明書が期限切れになると、ホストと Manager は応答を停止し、リカバリーはエラーが発生しやすく、時間のかかるプロセスになります。

## 手順

1. ホスト証明書を更新します。
  - a. 管理ポータルで **Compute → Hosts** をクリックします。
  - b. **Management → Maintenance** をクリックし、**OK** をクリックします。仮想マシンは、ホストから自動的に移行されます。固定されているか、移行できない場合は、シャットダウンする必要があります。
  - c. ホストがメンテナンスマードで、このホストに仮想マシンが残っていない場合は、**Installation → Enroll Certificate** をクリックします。
  - d. 登録が完了したら、**Management → Activate** をクリックします。
2. Manager 証明書を更新します。
  - a. セルフホストエンジンのみ: ホストにログインし、グローバルメンテナンスマードにします。
 

```
hosted-engine --set-maintenance --mode=global
```
  - b. セルフホストエンジンとスタンドアロンマネージャー: Manager にログインして **engine-setup** を実行します。
 

```
engine-setup --offline
```

**engine-setup** スクリプトにより、設定に関する質問が表示されます。必要に応じて質問に答えるか、回答ファイルを使用します。
  - c. 次の **engine-setup** プロンプトの後に **Yes** と入力します。
 

```
Renew certificates? (Yes, No) [Yes]:
```
  - d. セルフホストエンジンのみ: ホストにログインし、グローバルメンテナンスマードを無効にします。
 

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

## 関連情報

- [How to manually renew RHV host SSL certificate if expired?](#)

## 3.5. ANSIBLE を使用した設定タスクの自動化

Ansible は、システムの設定、ソフトウェアのデプロイ、ローリング更新の実行に使用する自動化ツールです。Red Hat Virtualization には、データセンターのセットアップと設定、ユーザーの管理、仮想マシンの操作など、RHV のインストール後のタスクを自動化するための限定バージョンの Ansible が含まれています。

Ansible は、REST API や SDK と比較して、Red Hat Virtualization 設定を自動化する簡単な方法を提供し、他の Ansible モジュールと統合できます。Red Hat Virtualization で利用可能な Ansible モジュールの詳細は、Red Hat Ansible Automation Hub ドキュメントの [oVirt Ansible Collection](#) を参照してください。



### 注記

Ansible Tower は、Ansible の Web インターフェイスと REST API を介してアクセスできるグラフィカルに有効化されたフレームワークです。Ansible Tower のサポートが必要な場合は、Red Hat Virtualization サブスクリプションの一部ではない Ansible Tower ライセンスが必要です。

他のインストール手順、および Ansible の使用に関する情報は、[Ansible のドキュメント](#) を参照してください。

### 3.5.1. oVirt Ansible Collection

**oVirt Ansible コレクション** は、Red Hat Virtualization インフラストラクチャーのさまざまな部分を管理するためのモジュール、ロール、およびプラグインを提供します。モジュールは、Ansible と Red Hat Virtualization Manager 間の通信に使用されます。Ansible のロールは、大きな Playbook を他のユーザーと共有できる小さな再利用可能なファイルに分割することで、Ansible コードをモジュール化する方法を提供します。**oVirt Ansible Collection** の詳細は、[Automation Hub のドキュメント](#) を参照してください。

#### 3.5.1.1. RPM パッケージからの oVirt Ansible Collection のインストール

**oVirt Ansible Collection for Red Hat Virtualization** は、Red Hat Virtualization Manager のリポジトリからインストールできます。

#### 前提条件

**oVirt Ansible Collection** をインストールするには、次のサブスクリプションチャネルのいずれかにサブスクライブする必要があります。

- Red Hat Virtualization サブスクリプションを使用する場合 - **rhv-4.4-manager-for-rhel-8-x86\_64-rpms**
- 任意の Red Hat Enterprise Linux サブスクリプションを使用する場合 - **rhv-4-tools-for-rhel-8-x86\_64-rpms**

#### 手順

1. 次のコマンドを実行して、Manager マシンに **oVirt Ansible Collection** をインストールします。

```
dnf install ovirt-ansible-collection
```

- デフォルトでは、コレクションは次の場所にインストールされます。

/usr/share/ansible/collections/ansible\_collections/redhat/rhv

**ovirt-ansible-collection** パッケージの構造は次のとおりです。

```
/usr/share/ansible/collections/ansible_collections/redhat/rhv/usr/share/doc/ovirt-ansible-collection/
```

### 3.5.1.2. Automation Hub からの oVirt Ansible Collection のインストール

Automation Hub は、**oVirt Ansible Collection** のインストールに使用できる新しい場所です。環境を設定するには、[oVirt Ansible Collection ドキュメント](#) の指示に従います。

#### 手順

- コレクションをインストールします。

```
ansible-galaxy collection install redhat.rhv
```

- Automation Hub は現在、RPM 依存関係をインストールしていません。Playbook を実行するホストに次のパッケージがあることを確認してください。

- python3-ovirt-engine-sdk4**
- python3-netaddr**
- python3-jmespath**
- python3-passlib**

### 3.5.1.3. oVirt Ansible コレクションを使用した Red Hat Virtualization の設定

次の手順では、**oVirt Ansible Collection** を使用して Red Hat Virtualization を設定する Playbook を作成および実行する方法を説明します。この例では、Ansible を使用してローカルマシンのマネージャーに接続し、新しいデータセンターを作成します。

#### 前提条件

- Playbook を実行しているマシンに Python SDK がインストールされていることを確認する。

#### 手順

- Playbook を作成します。

```
- name: RHV infrastructure
 hosts: localhost
 connection: local
 gather_facts: false

 vars_files:
 # Contains variables to connect to the Manager
 - engine_vars.yml
```

```

Contains encrypted engine_password variable using ansible-vault
- passwords.yml

pre_tasks:
 # The use of redhat.rhv before ovirt_auth is to check if oVirt Ansible Collection is correctly
 loaded
 - name: Login to RHV
 redhat.rhv.ovirt_auth:
 hostname: "{{ engine_fqdn }}"
 username: "{{ engine_user }}"
 password: "{{ engine_password }}"
 ca_file: "{{ engine_cafile | default(omit) }}"
 insecure: "{{ engine_insecure | default(true) }}"
 tags:
 - always

vars:
 data_center_name: mydatacenter
 data_center_description: mydatacenter
 data_center_local: false
 compatibility_version: 4.4

roles:
 - infra
collections:
 - redhat.rhv
post_tasks:
 - name: Logout from RHV
 ovirt_auth:
 state: absent
 ovirt_auth: "{{ ovirt_auth }}"
 tags:
 - always

```

これで、oVirt Ansible Collection の Ansible ロール `infra` を使用して、`mydatacenter` という名前のデータセンターが作成されました。

## 3.6. ユーザーとロール

### 3.6.1. ユーザーの概要

Red Hat Virtualization には、ローカルドメインと外部ドメインの 2 種類のユーザードメインがあります。Manager のインストールプロセス中に、**内部** ドメインと呼ばれるデフォルトのローカルドメインとデフォルトユーザーである `admin` が作成されます。

`ovirt-aaa-jdbc-tool` を使用して、**内部** ドメインに追加のユーザーを作成できます。ローカルドメインに作成されたユーザー アカウントは、ローカルユーザーと呼ばれます。また、Red Hat Directory Server、Active Directory、OpenLDAP、その他多くのサポート対象オプションなどの外部 Directory Server を Red Hat Virtualization 環境にアタッチし、外部ドメインとして使用することも可能です。外部ドメインに作成されたユーザー アカウントは、ディレクトリユーザーと呼ばれます。

ローカルユーザーとディレクトリユーザーが環境内で機能するには、管理ポータルを介して両方のユーザーに適切なロールおよび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 つのタイプがあります。エンドユーザーのロールは、VM ポータルからの仮想リソースを使用および管理します。管理者のロールは、管理ポータルを使用してシステムインフ

ラストラクチャーを維持します。ロールは、仮想マシンやホストなどの個々のリソースのユーザーに割り当てることも、クラスターやデータセンターなどのオブジェクトの階層に割り当てることもできます。

### 3.6.2. Directory Server の概要

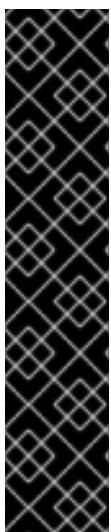
インストール中に、Red Hat Virtualization Manager は内部ドメインに **admin** ユーザーを作成します。このユーザーは、**admin@internal** とも呼ばれます。このアカウントは、環境の初期設定およびトラブルシューティングに使用することを目的としています。外部 Directory Server を接続し、ディレクトリユーザーを追加して適切なロールとパーミッションを割り当てた後、必要がない場合は **admin@internal** ユーザーを無効にできます。サポート対象の Directory Server は次のとおりです。

- 389ds
- 389ds RFC-2307 Schema
- Active Directory
- IBM Security Directory Server
- IBM Security Directory Server RFC-2307 Schema
- FreeIPA
- iDM
- Novell eDirectory RFC-2307 Schema
- OpenLDAP RFC-2307 Schema
- OpenLDAP Standard Schema
- Oracle Unified Directory RFC-2307 Schema
- RFC-2307 Schema (汎用)
- Red Hat Directory Server (RHDS)
- Red Hat Directory Server (RHDS) RFC-2307 Schema
- iPlanet



#### 重要

Red Hat Virtualization Manager (**rhev-m**) と IdM (**ipa-server**) は同じシステムにインストールできません。IdM は、Red Hat Virtualization Manager で必要な **mod\_ssl** パッケージと互換性がありません。



## 重要

ディレクトリーサーバーとして Active Directory を使用していて、テンプレートと仮想マシンの作成に **sysprep** を使用する場合は、Red Hat Virtualization の管理ユーザーに以下を実行するためのドメイン制御をを委任する必要があります。

- コンピューターをドメインに参加させる
- グループのメンバーシップを変更する

Active Directory でのユーザー アカウントの作成については、[新規ユーザー アカウントの作成](#) を参照してください。

Active Directory での制御の委任については、[組織単位での制御の委任](#) を参照してください。

### 3.6.3. 外部 LDAP プロバイダーの設定

#### 3.6.3.1. 外部 LDAP プロバイダーの設定 (対話型セットアップ)



## 注記

**ovirt-engine-extension-aaa-ldap** は非推奨になりました。新規インストールの場合は、Red Hat Single Sign On を使用します。詳細は、[管理ガイド の Red Hat Single Sign-On のインストールおよび設定](#) を参照してください。

**ovirt-engine-extension-aaa-ldap** 拡張機能を使用すると、ユーザーは外部ディレクトリーの設定を簡単にカスタマイズできます。**ovirt-engine-extension-aaa-ldap** 拡張機能では多くの異なる LDAP サーバータイプがサポートされており、ほとんどの LDAP タイプのセットアップを支援する対話型セットアップスクリプトが提供されています。

LDAP サーバーの種類が対話型セットアップスクリプトにリストされていない場合、またはさらにカスタマイズしたい場合は、設定ファイルを手動で編集できます。詳細は、[外部 LDAP プロバイダーの設定](#) を参照してください。

Active Directory の例については、[Active Directory の接続](#) を参照してください。

## 前提条件

- DNS または LDAP サーバーのドメイン名を把握している。
- LDAP サーバーとマネージャーの間に安全な接続を設定するために、PEM でエンコードされた CA 証明書が準備されていることを確認する。
- LDAP サーバーへの検索およびログインクエリーを実行するために、少なくとも 1 セットのアカウント名とパスワードを用意する。

## 手順

1. Red Hat Virtualization Manager で、LDAP 拡張パッケージをインストールします。

```
dnf install ovirt-engine-extension-aaa-ldap-setup
```

2. **ovirt-engine-extension-aaa-ldap-setup** を実行して、対話型セットアップを開始します。

```
ovirt-engine-extension-aaa-ldap-setup
```

3. 対応する番号を入力して、LDAP タイプを選択します。LDAP サーバーのスキーマが不明な場合は、LDAP サーバータイプの標準スキーマを選択してください。Active Directory の場合は、[Attaching\\_an\\_Active\\_Directory](#) の手順に従います。

Available LDAP implementations:

- 1 - 389ds
- 2 - 389ds RFC-2307 Schema
- 3 - Active Directory
- 4 - IBM Security Directory Server
- 5 - IBM Security Directory Server RFC-2307 Schema
- 6 - IPA
- 7 - Novell eDirectory RFC-2307 Schema
- 8 - OpenLDAP RFC-2307 Schema
- 9 - OpenLDAP Standard Schema
- 10 - Oracle Unified Directory RFC-2307 Schema
- 11 - RFC-2307 Schema (Generic)
- 12 - RHDS
- 13 - RHDS RFC-2307 Schema
- 14 - iPlanet

Please select:

4. **Enter** を押してデフォルトを許可し、LDAP サーバー名のドメイン名解決を設定します。

It is highly recommended to use DNS resolution for LDAP server.

If for some reason you intend to use hosts or plain address disable DNS usage.

Use DNS (Yes, No) [Yes]:

5. DNS ポリシー方式を選択します。

- オプション 1 の場合、`/etc/resolv.conf` にリストされている DNS サーバーを使用して IP アドレスを解決します。`/etc/resolv.conf` ファイルが正しい DNS サーバーで更新されていることを確認します。
- オプション 2 には、完全修飾ドメイン名 (FQDN) または LDAP サーバーの IP アドレスを入力します。SRV レコードで **dig** コマンドを使用して、ドメイン名を見つけることができます。SRV レコードの形式は次のとおりです。

**\_service.\_protocol.domain\_name**

例: **dig \_ldap.\_tcp.redhat.com SRV**。

- オプション 3 には、LDAP サーバーのスペース区切りのリストを入力します。サーバーの FQDN または IP アドレスのいずれかを使用します。このポリシーは、LDAP サーバー間の負荷分散を提供します。クエリーは、ラウンドロビンアルゴリズムに従ってすべての LDAP サーバーに分散されます。
- オプション 4 には、スペースで区切られた LDAP サーバーのリストを入力します。サーバーの FQDN または IP アドレスのいずれかを使用します。このポリシーは、クエリーに応答するデフォルトの LDAP サーバーとなる最初の LDAP サーバーを定義します。最初のサーバーが使用できない場合、クエリーはリストの次の LDAP サーバーに移動します。

1 - Single server

2 - DNS domain LDAP SRV record

3 - Round-robin between multiple hosts  
 4 - Failover between multiple hosts  
 Please select:

6. LDAP サーバーがサポートする安全な接続方法を選択し、PEM でエンコードされた CA 証明書を取得する方法を指定します。

- **File** を使用すると、証明書へのフルパスを指定できます。
- **URL** を使用すると、証明書の URL を指定できます。
- **Inline** を使用すると、証明書の内容を端末に貼り付けることができます。
- **System** では、すべての CA ファイルのデフォルトの場所を指定できます。
- **Insecure** は証明書の検証をスキップしますが、接続は引き続き TLS を使用して暗号化されます。

**NOTE:**

It is highly recommended to use secure protocol to access the LDAP server.

Protocol startTLS is the standard recommended method to do so.

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

Use plain for test environments only.

Please select protocol to use (startTLS, ldaps, plain) [startTLS]: **startTLS**

Please select method to obtain PEM encoded CA certificate (File, URL, Inline, System, Insecure):

Please enter the password:



### 注記

LDAPS は、Lightweight Directory Access Protocol Over Secure Socket Links の略です。SSL 接続の場合は、**ldaps** オプションを選択します。

7. 検索ユーザーの識別名 (DN) を入力します。ユーザーには、Directory Server 上のすべてのユーザーとグループを参照するための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は、入力せずに **Enter** を押します。

Enter search user DN (for example uid=username,dc=example,dc=com or leave empty for anonymous): **uid=user1,ou=Users,ou=department-1,dc=example,dc=com**  
 Enter search user password:

8. ベース DN を入力します。

Please enter base DN (dc=redhat,dc=com) [dc=redhat,dc=com]: **ou=department-1,dc=redhat,dc=com**

9. 仮想マシン用に Single Sign-On を設定する場合は、**Yes** を選択します。この機能は、管理ポータル機能に対する Single Sign-On では使用できないことに注意してください。スクリプトにより、プロファイル名とドメイン名が一致する必要があることが通知されます。この場合も、[仮想マシン管理ガイド](#)の[仮想マシンのシングルサインオンの設定](#)に記載された手順に従う必要があります。

Are you going to use Single Sign-On for Virtual Machines (Yes, No) [Yes]:

10. プロファイル名を指定します。プロファイル名は、ログインページでユーザーに表示されます。この例では、**redhat.com** を使用しています。



#### 注記

ドメインの設定後にプロファイル名を変更するには、`/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。変更を反映するには、**ovirt-engine** サービスを再起動します。

Please specify profile name that will be visible to users: **redhat.com**

図3.1 管理ポータルのログインページ



#### 注記

ユーザーは、初めてログインするときにドロップダウンリストからプロファイルを選択する必要があります。情報はブラウザーの Cookie に保存され、ユーザーが次にログインしたときに事前に選択されます。

11. ログイン機能をテストして、LDAP サーバーが Red Hat Virtualization 環境に正しく接続されていることを確認します。ログインクエリーには、**user name** および **password** を入力します。

#### NOTE:

It is highly recommended to test drive the configuration before applying it into engine. Login sequence is executed automatically, but it is recommended to also execute Search sequence manually after successful Login sequence.

Please provide credentials to test login flow:

Enter user name:

Enter user password:

```
[INFO] Executing login sequence...
...
[INFO] Login sequence executed successfully
```

12. ユーザーの詳細が正しいことを確認してください。ユーザーの詳細が正しくない場合は、**Abort** を選択します。

```
Please make sure that user details are correct and group membership meets expectations
(search for PrincipalRecord and GroupRecord titles).
Abort if output is incorrect.
```

Select test sequence to execute (Done, Abort, Login, Search) [Abort]:

13. 検索機能を手動でテストすることが推奨されます。検索クエリーで、ユーザーアカウントの場合は **Principal**、グループアカウントの場合は **Group** を選択します。ユーザーアカウントのグループアカウント情報を返す場合は、**Resolve Groups** で **Yes** を選択します。3つの設定ファイルが作成され、画面出力に表示されます。

```
Select test sequence to execute (Done, Abort, Login, Search) [Search]: Search
Select entity to search (Principal, Group) [Principal]:
Term to search, trailing '*' is allowed: testuser1
Resolve Groups (Yes, No) [No]:
```

14. **Done** を選択してセットアップを完了します。

```
Select test sequence to execute (Done, Abort, Login, Search) [Abort]: Done
[INFO] Stage: Transaction setup
[INFO] Stage: Misc configuration
[INFO] Stage: Package installation
[INFO] Stage: Misc configuration
[INFO] Stage: Transaction commit
[INFO] Stage: Closing up
CONFIGURATION SUMMARY
Profile name is: redhat.com
The following files were created:
/etc/ovirt-engine/aaa/redhat.com.properties
/etc/ovirt-engine/extensions.d/redhat.com.properties
/etc/ovirt-engine/extensions.d/redhat.com-authn.properties
[INFO] Stage: Clean up
Log file is available at /tmp/ovirt-engine-extension-aaa-ldap-setup-20171004101225-
mmneib.log:
[INFO] Stage: Pre-termination
[INFO] Stage: Termination
```

15. **ovirt-engine** サービスを再起動します。作成したプロファイルは、管理ポータルおよび VM ポータルのログインページで利用できるようになります。たとえば VM ポータルにログインするためには、LDAP サーバー上のユーザーアカウントに適切なロールとパーミッションを割り当てる場合は、[Manager ユーザーのタスク](#) を参照してください。

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



## 注記

詳細は、[/usr/share/doc/ovirt-engine-extension-aaa-ldap-version](#) の LDAP 認証および承認拡張 README ファイルを参照してください。

### 3.6.3.2. Active Directory の接続



#### 注記

**ovirt-engine-extension-aaa-ldap** は非推奨になりました。新規インストールの場合は、Red Hat Single Sign On を使用します。詳細は、[管理ガイド の Red Hat Single Sign-On のインストールおよび設定](#) を参照してください。

#### 前提条件

- Active Directory フォレスト名を知っている。フォレスト名は、ルートドメイン名とも呼ばれています。



#### 注記

`ovirt-engine-extension-aaa-ldap-setup` ツールで設定できない、最も一般的な Active Directory の設定例は [/usr/share/ovirt-engine-extension-aaa-ldap/examples/README.md](#) に記載されています。

- Active Directory フォレスト名を解決できる DNS サーバーを Manager の `/etc/resolv.conf` ファイルに追加するか、Active Directory DNS サーバーを書き留めて、対話型セットアップスクリプトのプロンプトが表示されたら入力する。
- LDAP サーバーと Manager の間に安全な接続を設定するために、PEM でエンコードされた CA 証明書が準備されていることを確認する。詳細は、[Manager と LDAP サーバー間で SSL または TLS 接続の設定](#) を参照してください。
- 匿名検索がサポートされていない場合、検索ユーザーとして使用できる、すべてのユーザーとグループを参照するパーミッションを持つユーザーが Active Directory で利用可能である。検索ユーザーの識別名 (DN) を書き留めます。Active Directory の管理ユーザーは使用しないでください。
- Active Directory への検索およびログインクエリーを実行するには、アカウント名とパスワードを少なくとも 1つ用意しておく。
- Active Directory のデプロイメントが複数のドメインにまたがる場合は、`/usr/share/ovirt-engine-extension-aaa-ldap/profiles/ad.properties` ファイルに記載されている制限に注意する。

#### 手順

- Red Hat Virtualization Manager で、LDAP 拡張パッケージをインストールします。

```
dnf install ovirt-engine-extension-aaa-ldap-setup
```

- ovirt-engine-extension-aaa-ldap-setup** を実行して、対話型セットアップを開始します。

```
ovirt-engine-extension-aaa-ldap-setup
```

- 対応する番号を入力して、LDAP タイプを選択します。この手順の後の LDAP 関連の質問は、LDAP タイプにより異なります。

```
Available LDAP implementations:
1 - 389ds
```

2 - 389ds RFC-2307 Schema  
 3 - Active Directory  
 4 - IBM Security Directory Server  
 5 - IBM Security Directory Server RFC-2307 Schema  
 6 - IPA  
 7 - Novell eDirectory RFC-2307 Schema  
 8 - OpenLDAP RFC-2307 Schema  
 9 - OpenLDAP Standard Schema  
 10 - Oracle Unified Directory RFC-2307 Schema  
 11 - RFC-2307 Schema (Generic)  
 12 - RHDS  
 13 - RHDS RFC-2307 Schema  
 14 - iPlanet  
 Please select: 3

- Active Directory フォレスト名を入力します。フォレスト名が Manager の DNS で解決できない場合、スクリプトは、スペースで区切られた Active Directory サーバー名のリストを入力するように求めます。

Please enter Active Directory Forest name: **ad-example.redhat.com**  
 [ INFO ] Resolving Global Catalog SRV record for **ad-example.redhat.com**  
 [ INFO ] Resolving LDAP SRV record for **ad-example.redhat.com**

- LDAP サーバーがサポートする安全な接続方法を選択し、PEM でエンコードされた CA 証明書を取得する方法を指定します。ファイルオプションを使用すると、証明書へのフルパスを指定できます。URL オプションを使用すると、証明書への URL を指定できます。インラインオプションを使用して、証明書の内容をターミナルに貼り付けます。システムオプションを使用すると、すべての CA ファイルの場所を指定できます。セキュアでないオプションを使用すると、startTLS をセキュアでないモードで使用できます。

**NOTE:**

It is highly recommended to use secure protocol to access the LDAP server.

Protocol startTLS is the standard recommended method to do so.

Only in cases in which the startTLS is not supported, fallback to non standard ldaps protocol.  
Use plain for test environments only.

Please select protocol to use (startTLS, ldaps, plain) [startTLS]: **startTLS**

Please select method to obtain PEM encoded CA certificate (File, URL, Inline, System, Insecure): **File**

Please enter the password:



### 注記

LDAPS は、Lightweight Directory Access Protocol Over Secure Socket Links の略です。SSL 接続の場合は、**ldaps** オプションを選択します。

PEM でエンコードされた CA 証明書の作成の詳細は、[Manager と LDAP サーバー間の SSL または TLS 接続のセットアップ](#) を参照してください。

- 検索ユーザーの識別名 (DN) を入力します。ユーザーには、Directory Server 上のすべてのユーザーとグループを参照するためのパーミッションが必要です。検索ユーザーは LDAP アノテーションである必要があります。匿名検索が許可されている場合は、入力せずに **Enter** を押します。

Enter search user DN (empty for anonymous):  
**cn=user1,ou=Users,dc=test,dc=redhat,dc=com**  
 Enter search user password:

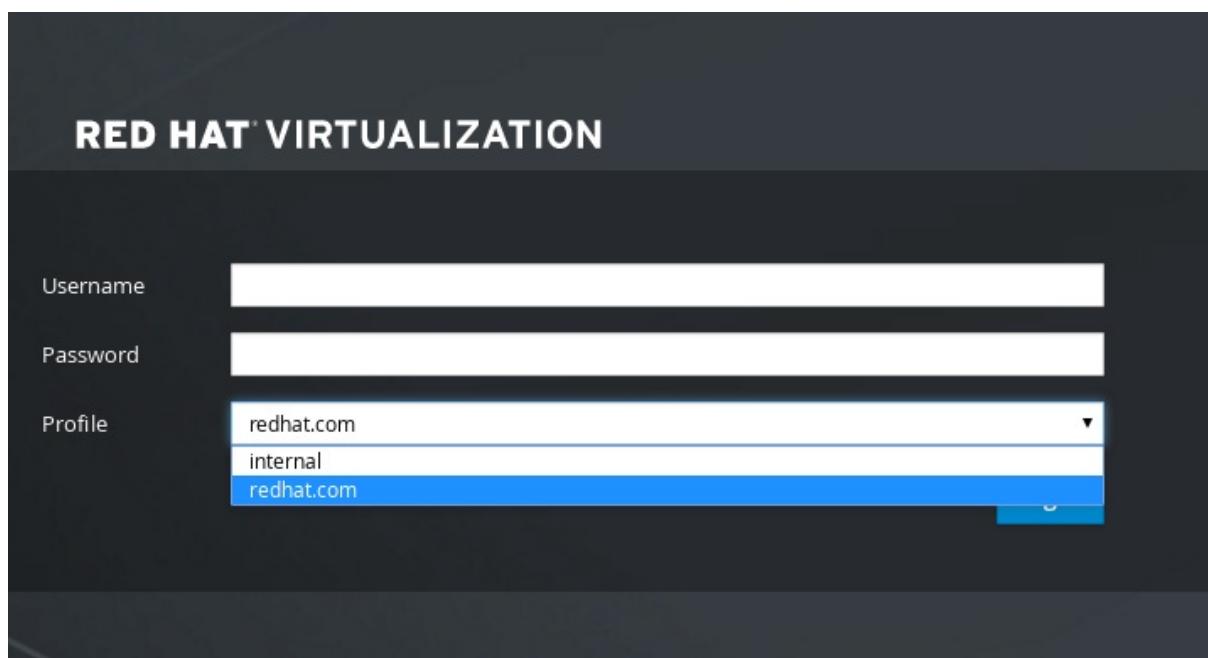
7. 仮想マシンにシングルサインオンを使用するかどうかを指定します。この機能はデフォルトで有効になっていますが、管理ポータルへのシングルサインオンが有効になっている場合は使用できません。スクリプトにより、プロファイル名とドメイン名が一致する必要があることが通知されます。この場合も、[仮想マシン管理ガイド](#)の[仮想マシンのシングルサインオンの設定](#)に記載された手順に従う必要があります。

Are you going to use Single Sign-On for Virtual Machines (Yes, No) [Yes]:

8. プロファイル名を指定します。プロファイル名は、ログインページでユーザーに表示されます。この例では、**redhat.com** を使用しています。

Please specify profile name that will be visible to users:**redhat.com**

図3.2 管理ポータルのログインページ



### 注記

ユーザーは、初めてログインするときに、ドロップダウンリストから目的のプロファイルを選択する必要があります。その後、情報はブラウザーのCookieに保存され、ユーザーが次にログインしたときに事前に選択されます。

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 環境に正しく接続されていることを確認します。ログインクエリーには、アカウント名とパスワードを入力します。検索クエリーで、ユーザー アカウントの場合は **Principal** を選択し、グループ アカウントの場合は **Group** を選択します。ユーザー アカウントのグループ アカウント情報を返す場合は、**Resolve Groups** に **Yes** を入力します。**Done** を選択してセットアップを完了します。3つの設定ファイルが作成され、画面出力に表示されます。

#### NOTE:

It is highly recommended to test drive the configuration before applying it into engine.  
 Login sequence is executed automatically, but it is recommended to also execute Search

```

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

```

- 作成したプロファイルは、管理ポータルおよびVMポータルのログインページで利用できるようになります。たとえばVMポータルにログインするために、LDAPサーバー上のユーザーアカウントに適切なロールとパーミッションを割り当てる場合は、[Managerユーザーのタスク](#)を参照してください。



### 注記

詳細は、[/usr/share/doc/ovirt-engine-extension-aaa-ldap-version](#) の LDAP 認証および承認拡張 README ファイルを参照してください。

#### 3.6.3.3. 外部 LDAP プロバイダーの設定 (手動)



### 注記

**ovirt-engine-extension-aaa-ldap** は非推奨になりました。新規インストールの場合は、Red Hat Single Sign On を使用します。詳細は、[管理ガイド](#) の [Red Hat Single Sign-On のインストールおよび設定](#) を参照してください。

**ovirt-engine-extension-aaa-ldap** 拡張機能は、LDAP プロトコルを使用してディレクトリサーバーにアクセスし、完全にカスタマイズ可能です。仮想マシンポータルまたは管理ポータル機能への Single Sign-On を有効にする場合を除いて、Kerberos 認証は必要ありません。

前のセクションの対話型セットアップ方法でユースケースがカバーされていない場合は、設定ファイルを手動で変更して LDAP サーバーを接続できます。次の手順では、一般的な詳細を使用します。具体的な値は、設定により異なります。

## 手順

- Red Hat Virtualization Manager で、LDAP 拡張パッケージをインストールします。

```
dnf install ovirt-engine-extension-aaa-ldap
```

- LDAP 設定テンプレートファイルを /etc/ovirt-engine ディレクトリーにコピーします。テンプレートファイルは、アクティブなディレクトリー (ad) およびその他のディレクトリータイプ (simple) で使用できます。この例では、単純な設定テンプレートを使用しています。

```
cp -r /usr/share/ovirt-engine-extension-aaa-ldap/examples/simple/. /etc/ovirt-engine
```

- 管理ポータルおよび仮想マシンポータルのログインページでユーザーに表示するプロファイル名と一致するように、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
```

- LDAP サーバーの種類のコメントを解除し、ドメインとパスワードのフィールドを更新して、LDAP プロパティー設定ファイルを編集します。

```
vi /etc/ovirt-engine/aaa/example.properties
```

### 例3.5 プロファイルの例: LDAP サーバーセクション

```
Select one
#
include = <openldap.properties>
#include = <389ds.properties>
#include = <rhds.properties>
#include = <ipa.properties>
#include = <iplanet.properties>
#include = <rfc2307-389ds.properties>
#include = <rfc2307-rhds.properties>
#include = <rfc2307-openldap.properties>
#include = <rfc2307-edir.properties>
#include = <rfc2307-generic.properties>

Server
#
vars.server = ldap1.company.com

Search user and its password.
#
vars.user = uid=search,cn=users,cn=accounts,dc=company,dc=com
vars.password = 123456
```

```
pool.default.serverset.single.server = ${global:vars.server}
pool.default.auth.simple.bindDN = ${global:vars.user}
pool.default.auth.simple.password = ${global:vars.password}
```

TLS または SSL プロトコルを使用して LDAP サーバーと対話するには、LDAP サーバーのルート CA 証明書を取得し、それを使用して公開 keystore ファイルを作成します。次の行のコメントを解除し、公開 keystore ファイルへのフルパスとファイルにアクセスするためのパスワードを指定します。



### 注記

公開 keystore ファイルの作成の詳細は、[Manager と LDAP サーバー間の SSL または TLS 接続の設定](#) を参照してください。

#### 例3.6 プロファイルの例: keystore セクション

```
Create keystore, import certificate chain and uncomment
if using tls.
pool.default.ssl.startTLS = true
pool.default.ssl.truststore.file = /full/path/to/myrootca.jks
pool.default.ssl.truststore.password = password
```

5. 認証設定ファイルを確認します。管理ポータルおよび仮想マシン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` によって定義されます。設定プロファイルの場所は、LDAP 設定ファイルの場所と一致する必要があります。すべてのフィールドをデフォルトのままにできます。

```
vi /etc/ovirt-engine/extensions.d/example-authn.properties
```

#### 例3.7 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.extension.aaa.ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.ldap.AuthnExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authn
ovirt.engine.aaa.authn.profile.name = example
ovirt.engine.aaa.authn.authz.plugin = example-authz
config.profile.file.1 = ../aaa/example.properties
```

6. 許可設定ファイルを確認してください。設定プロファイルの場所は、LDAP 設定ファイルの場所と一致する必要があります。すべてのフィールドをデフォルトのままにできます。

```
vi /etc/ovirt-engine/extensions.d/example-authz.properties
```

#### 例3.8 許可設定ファイルの例

```
ovirt.engine.extension.name = example-authz
```

```

ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.ldap.AuthzExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authz
config.profile.file.1 = ../aaa/example.properties

```

7. 設定プロファイルの所有権およびパーミッションが適切であることを確認してください。

```

chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties
chmod 600 /etc/ovirt-engine/aaa/example.properties

```

8. エンジンサービスを再起動します。

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

9. 作成した **example** プロファイルは、管理ポータルおよび仮想マシンポータルのログインページで利用できるようになります。たとえば VM ポータルにログインするために、LDAP サーバー上のユーザー アカウントに適切なパーミッションを割り当てる場合は、[Manager ユーザーのタスク](#) を参照してください。



### 注記

詳細は、[/usr/share/doc/ovirt-engine-extension-aaa-ldap-version](#) の LDAP 認証および承認拡張 README ファイルを参照してください。

#### 3.6.3.4. 外部 LDAP プロバイダーの削除

この手順では、外部で設定された LDAP プロバイダーとそのユーザーを削除する方法を示します。

##### 手順

1. LDAP プロバイダー設定ファイルを削除し、デフォルト名 **profile1** を置き換えます。

```

rm /etc/ovirt-engine/extensions.d/profile1-authn.properties
rm /etc/ovirt-engine/extensions.d/profile1-authz.properties
rm /etc/ovirt-engine/aaa/profile1.properties

```

2. **ovirt-engine** サービスを再起動します。

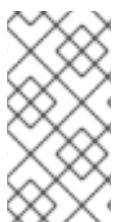
```
systemctl restart ovirt-engine
```

3. 管理ポータルの **Users** リソースタブで、このプロバイダーのユーザー (**Authorization provider** が **profile1-authz** であるユーザー) を選択し、**Remove** をクリックします。

#### 3.6.4. シングルサインオン用の LDAP および Kerberos の設定

シングルサインオンを使用すると、ユーザーはパスワードを再入力せずに VM ポータルまたは管理ポータルにログインできます。認証情報は Kerberos サーバーから取得します。管理ポータルと VM ポータルへのシングルサインオンを設定するには、**ovirt-engine-extension-aaa-misc** および **ovirt-engine-**

`extension-aaa-ldap` の 2 つの拡張機能と、2 つの Apache モジュール `mod_auth_gssapi` および `mod_session` を設定する必要があります。Kerberos を含まないシングルサインオンを設定できますが、これはこのドキュメントの範囲外です。



### 注記

VM 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、仮想マシンにはシングルサインオンできません。VM 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には、VM ポータルはパスワードを受け入れる必要がないので、パスワードを委任して仮想マシンにサインインすることはできません。

この例では、以下を前提としています。

- 既存の Key Distribution Center (KDC) サーバーは、MIT バージョンの Kerberos 5 を使用します。
- KDC サーバーに対する管理者権限があります。
- Kerberos クライアントは、Red Hat Virtualization Manager とユーザーマシンにインストールされます。
- **kadmin** ユーティリティーは、Kerberos サービスプリンシパルと **keytab** ファイルを作成するために使用されます。

この手順には、次のコンポーネントが含まれます。

- **On the KDC server**
  - Red Hat Virtualization Manager 上で 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 の場合**
  - 認証および許可拡張パッケージと Apache Kerberos 認証モジュールをインストールします。
  - 拡張ファイルを設定します。

#### 3.6.4.1. 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 で Apache サービスのサービスプリンシパルを作成します。サービスプリンシパルは、Apache サービスの KDC への参照 ID です。

```
kadmin
kadmin> addprinc -randkey HTTP/fqdn-of-rhevm@REALM.COM
```

2. Apache サービスの **keytab** ファイルを生成します。**keytab** ファイルには、共有秘密鍵が格納されています。



### 注記

`engine-backup` コマンドには、バックアップおよび復元時にファイル `/etc/httpd/http.keytab` が含まれます。**keytab** ファイルに別の名前を使用する場合は、必ずバックアップして復元してください。

```
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
```

== 仮想マシン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

4. Red Hat Virtualization Manager で、keytab の所有権とパーミッションが適切であることを確認します。

```
chown apache /etc/httpd/http.keytab
chmod 400 /etc/httpd/http.keytab
```

5. 認証拡張パッケージ、LDAP 拡張パッケージ、および **mod\_auth\_gssapi** および **mod\_sessionApache** モジュールをインストールします。

```
dnf install ovirt-engine-extension-aaa-misc ovirt-engine-extension-aaa-ldap
mod_auth_gssapi mod_session
```



### 注記

**ovirt-engine-extension-aaa-ldap** は非推奨になりました。新規インストールの場合は、Red Hat Single Sign On を使用します。詳細は、[管理ガイド の Red Hat Single Sign-On のインストールおよび設定](#) を参照してください。

6. SSO 設定テンプレートファイルを /etc/ovirt-engine ディレクトリーにコピーします。テンプレートファイルは、Active Directory (ad-sso) およびその他のディレクトリータイプ (simple-sso) で使用できます。この例では、単純な SSO 設定テンプレートを使用しています。

```
cp -r /usr/share/ovirt-engine-extension-aaa-ldap/examples/simple-sso/. /etc/ovirt-engine
```

7. **ovirt-sso.conf** を Apache 設定ディレクトリーに移動します。



### 注記

**engine-backup** コマンドは、バックアップと復元の際に、**/etc/httpd/conf.d/ovirt-sso.conf** ファイルを含めます。このファイルに別の名前を使用する場合は、必ずバックアップして復元してください。

```
mv /etc/ovirt-engine/aaa/ovirt-sso.conf /etc/httpd/conf.d
```

8. 認証方法ファイルを確認します。レルムは keytab ファイルから自動的に取得されるため、このファイルを編集する必要はありません。

```
vi /etc/httpd/conf.d/ovirt-sso.conf
```

### 例3.9 認証方法ファイルの例

```
<LocationMatch ^/ovirt-engine/sso/(interactive-login-negotiate|oauth/token-htt-
```

```

auth)|^/ovirt-engine/api>
<If "req('Authorization') !~ /^(Bearer|Basic)/i">
 RewriteEngine on
 RewriteCond %{LA-U:REMOTE_USER} ^(.*)$
 RewriteRule ^(.*)$ - [L,NS,P,E=REMOTE_USER:%1]
 RequestHeader set X-Remote-User %{REMOTE_USER}s

 AuthType GSSAPI
 AuthName "Kerberos Login"

 # Modify to match installation
 GssapiCredStore keytab:/etc/httpd/http.keytab
 GssapiUseSessions On
 Session On
 SessionCookieName ovirt_gssapi_session path=/private;httponly;secure;

 Require valid-user
 ErrorDocument 401 "<html><meta http-equiv=\"refresh\" content=\"0; url=/ovirt-engine/sso/login-unauthorized\"/><body>Here</body></html>"
</If>
</LocationMatch>

```

9. 管理ポータルおよび仮想マシンポータルのログインページでユーザーに表示するプロファイル名と一致するように、設定ファイルの名前を変更します。

```

mv /etc/ovirt-engine/aaa/profile1.properties /etc/ovirt-engine/aaa/example.properties

mv /etc/ovirt-engine/extensions.d/profile1-http-authn.properties /etc/ovirt-engine/extensions.d/example-http-authn.properties

mv /etc/ovirt-engine/extensions.d/profile1-http-mapping.properties /etc/ovirt-engine/extensions.d/example-http-mapping.properties

mv /etc/ovirt-engine/extensions.d/profile1-authz.properties /etc/ovirt-engine/extensions.d/example-authz.properties

```

10. LDAP サーバーの種類のコメントを解除し、ドメインとパスワードのフィールドを更新して、LDAP プロパティー設定ファイルを編集します。

```
vi /etc/ovirt-engine/aaa/example.properties
```

#### 例3.10 プロファイルの例: LDAP サーバーセクション

```

Select one
include = <openldap.properties>
#include = <389ds.properties>
#include = <rhds.properties>
#include = <ipa.properties>
#include = <iplanet.properties>
#include = <rfc2307-389ds.properties>
#include = <rfc2307-rhds.properties>

```

```
#include = <rfc2307-openldap.properties>
#include = <rfc2307-edir.properties>
#include = <rfc2307-generic.properties>

Server
#
vars.server = ldap1.company.com

Search user and its password.
#
vars.user = uid=search,cn=users,cn=accounts,dc=company,dc=com
vars.password = 123456

pool.default.serverset.single.server = ${global:vars.server}
pool.default.auth.simple.bindDN = ${global:vars.user}
pool.default.auth.simple.password = ${global:vars.password}
```

TLS または SSL プロトコルを使用して LDAP サーバーと対話するには、LDAP サーバーのルート CA 証明書を取得し、それを使用して公開 keystore ファイルを作成します。次の行のコメントを解除し、公開 keystore ファイルへのフルパスとファイルにアクセスするためのパスワードを指定します。



### 注記

公開 keystore ファイルの作成の詳細は、[Manager と LDAP サーバー間の SSL または TLS 接続の設定](#) を参照してください。

### 例3.11 プロファイルの例: keystore 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
```

- 認証設定ファイルを確認します。管理ポータルおよび仮想マシン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` によって定義されます。設定プロファイルの場所は、LDAP 設定ファイルの場所と一致する必要があります。すべてのフィールドをデフォルトのままにできます。

```
vi /etc/ovirt-engine/extensions.d/example-http-authn.properties
```

### 例3.12 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.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.http.AuthnExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authn
ovirt.engine.aaa.authn.profile.name = example-http
```

```
ovirt.engine.aaa.authn.authz.plugin = example-authz
ovirt.engine.aaa.authn.mapping.plugin = example-http-mapping
config.artifact.name = HEADER
config.artifact.arg = X-Remote-User
```

12. 許可設定ファイルを確認してください。設定プロファイルの場所は、LDAP 設定ファイルの場所と一致する必要があります。すべてのフィールドをデフォルトのままにできます。

```
vi /etc/ovirt-engine/extensions.d/example-authz.properties
```

### 例3.13 許可設定ファイルの例

```
ovirt.engine.extension.name = example-authz
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.ldap.AuthzExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authz
config.profile.file.1 = ../aaa/example.properties
```

13. 認証マッピング設定ファイルを確認します。設定プロファイルの場所は、LDAP 設定ファイルの場所と一致する必要があります。設定プロファイルの拡張名は、認証設定ファイルの **ovirt.engine.aaa.authn.mapping.plugin** 値と一致させる必要があります。すべてのフィールドをデフォルトのままにできます。

```
vi /etc/ovirt-engine/extensions.d/example-http-mapping.properties
```

#### 例3.14 認証マッピング設定ファイルの例

```
ovirt.engine.extension.name = example-http-mapping
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.mapping.MappingExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Mapping
config.mapAuthRecord.type = regex
config.mapAuthRecord.regex.mustMatch = true
config.mapAuthRecord.regex.pattern = ^(?<user>.*?)(@|\\|(?<at>@)(?<suffix>.*?)@.*|)(?<realm>@.*$)
config.mapAuthRecord.regex.replacement = ${user}${at}${suffix}
```

14. 設定ファイルの所有権およびパーミッションが適切であることを確認してください。

```
chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties
```

```
chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-http-authn.properties
```

```
chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-http-mapping.properties
```

```
chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-authz.properties
chmod 600 /etc/ovirt-engine/aaa/example.properties
chmod 640 /etc/ovirt-engine/extensions.d/example-http-authn.properties
chmod 640 /etc/ovirt-engine/extensions.d/example-http-mapping.properties
chmod 640 /etc/ovirt-engine/extensions.d/example-authz.properties
```

15. Apache サービスおよび **ovirt-engine** サービスを再起動します。

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

### 3.6.5. Red Hat Single Sign-On のインストールおよび設定

認証方法として Red Hat Single Sign-On を使用するには、以下を行う必要があります。

- Red Hat SSO をインストールします。
- LDAP グループマッパーを設定します。
- Manager で Apache を設定します。
- OVN プロバイダーの認証情報を設定します。
- モニタリングポータル (Grafana) を設定します。



#### 注記

Red Hat SSO が設定されている場合、一度に使用できる認証プロトコルは 1 つだけであるため、以前の LDAP サインオンは機能しません。

#### 3.6.5.1. Red Hat SSO のインストール

Red Hat Single Sign-On をインストールするには、ZIP ファイルをダウンロードして解凍するか、RPM ファイルを使用します。

[Red Hat SSO のインストール](#) に記載されたインストール手順に従います

次の情報を準備します。

- **Open ID Connect** サーバーのパス/場所。
- 正しいリポジトリのサブスクリプションチャネル。
- 有効な Red Hat サブスクリプションのログイン認証情報。

#### 3.6.5.2. LDAP グループマッパーの設定

#### 手順

1. 以下の情報を使用して LDAP グループマッパーを追加します。
  - **Name:** ldapgroups
  - **Mapper Type:** group-ldap-mapper
  - **LDAP Groups DN:** ou=groups,dc=example,dc=com
  - **Group Object Classes:** groupofuniqueNames (LDAP サーバーの設定に応じてこのクラスを適合させます)
  - **Membership LDAP Attribute:** uniquemember (LDAP サーバーの設定に応じてこのクラスを適合させます)
2. **Save** をクリックします。
3. **Sync LDAP Groups to Keycloak** をクリックします。
4. **User Federation Provider** ページの下部で、**Synchronize all users** をクリックします。
5. **Clients** タブの **Add Client** で、**Client ID** に **ovirt-engine** を追加し、**Root URL** にエンジンの URL を入力します。
6. **Client Protocol** を **openid-connect** に変更し、**Access Type** を **confidential** に変更します。
7. **Clients** タブの **Ovirt-engine > Advanced Settings** で、**Access Token Lifespan** の有効期間を延長します。
8. **https://rhvm.example.com:443/\*** を有効なリダイレクト URI として追加します。
9. クライアントシークレットが生成されます。これは、認証情報タブで確認できます。
10. **Create Mapper Protocol** の下の **Clients** タブで、以下の設定でマッパーを作成します。
  - **Name:** groups
  - **Mapper Type:** Group Membership
  - **Token Claim Name:** groups
  - **Full group path:** ON
  - **Add to ID token:** ON
  - **Add to access token:** ON
  - **Add to userinfo:** ON
11. **username** に **Builtin Protocol Mapper** を追加します。
12. **ovirt-engine**、**ovirt-app-api**、**ovirt-app-admin**、および **ovirt-ext-auth:sequence-priority=~** で必要なスコープを作成します。
13. 前の手順で作成したスコープを使用して、ovirt-engine クライアントのオプションのクライアントスコープを設定します。

### 3.6.5.3. Manager での Apache の設定

1. **mod\_auth\_openidc** モジュールを有効にします。

```
dnf module enable mod_auth_openidc:2.3 -y
```

2. Manager で Apache を設定します。

```
dnf install mod_auth_openidc
```

3. `/etc/httpd/conf.d/` に、以下の内容で新しい **httpd** 設定ファイル **ovirt-openidc.conf** を作成します。

```
LoadModule auth_openidc_module modules/mod_auth_openidc.so

OIDCProviderMetadataURL https://SSO.example.com/auth/realms/master/.well-known/openid-configuration
OIDCSSLValidateServer Off

OIDCClientID ovirt-engine
OIDCClientSecret <client_SSO_generated_key>
OIDCRedirectURI https://rhvm.example.com/ovirt-engine/callback
OIDCDefaultURL https://rhvm.example.com/ovirt-engine/login?scope=ovirt-app-admin+ovirt-app-portal+ovirt-ext%3Dauth%3Asequence-priority%3D%7E

maps the prefered_username claim to the REMOTE_USER environment variable:

OIDCRemoteUserClaim <preferred_username>
OIDCCryptoPassphrase <random1234>

<LocationMatch ^/ovirt-engine/sso/(interactive-login-negotiate|oauth/token-http-auth)|^/ovirt-engine/callback>
<If "req('Authorization') !~ /^(Bearer|Basic)/i">
 Require valid-user
 AuthType openid-connect

 ErrorDocument 401 "<html><meta http-equiv=\"refresh\" content=\"0; url=/ovirt-engine/sso/login-unauthorized\"/><body>Here</body></html>"
</If>
</LocationMatch>

OIDCOAuthIntrospectionEndpoint
https://SSO.example.com/auth/realms/master/protocol/openid-connect/token/introspect
OIDCOAuthSSLValidateServer Off
OIDCOAuthIntrospectionEndpointParams token_type_hint=access_token
OIDCOAuthClientID ovirt-engine
OIDCOAuthClientSecret <client_SSO_generated_key>
OIDCOAuthRemoteUserClaim sub

<LocationMatch ^/ovirt-engine/(api$|api/)>
 AuthType oauth20
 Require valid-user
</LocationMatch>
```

4. 設定変更を保存するには、**httpd** および **ovirt-engine** を再起動します。

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

5. 以下の内容で、`/etc/ovirt-engine/extensions.d/` に **openidc-authn.properties** ファイルを作成します。

```
ovirt.engine.extension.name = openidc-authn
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.http.AuthnExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authn
ovirt.engine.aaa.authn.profile.name = openidchttp
ovirt.engine.aaa.authn.authz.plugin = openidc-authz
ovirt.engine.aaa.authn.mapping.plugin = openidc-http-mapping
config.artifact.name = HEADER
config.artifact.arg = OIDC_CLAIM_preferred_username
```

6. 以下の内容で、`/etc/ovirt-engine/extensions.d/` に **openidc-http-mapping.properties** ファイルを作成します。

```
ovirt.engine.extension.name = openidc-http-mapping
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.mapping.MappingExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Mapping
config.mapAuthRecord.type = regex
config.mapAuthRecord.regex.mustMatch = false
config.mapAuthRecord.regex.pattern = ^(?<user>.*?)(@|\\|(?<at>@)(?<suffix>.*?)@.*|(?<realm>@.*$)
config.mapAuthRecord.regex.replacement = ${user}${at}${suffix}
```

7. 以下の内容で、`/etc/ovirt-engine/extensions.d/` に **openidc-authz.properties** ファイルを作成します。

```
ovirt.engine.extension.name = openidc-authz
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.http.AuthzExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authz
config.artifact.name.arg = OIDC_CLAIM_preferred_username
config.artifact.groups.arg = OIDC_CLAIM_groups
```

8. 以下の内容で、`/etc/ovirt-engine/engine.conf.d/` に **99-enable-external-auth.conf** ファイルを作成します。

```
ENGINE_SSO_ENABLE_EXTERNAL_SSO=true
ENGINE_SSO_EXTERNAL_SSO_LOGOUT_URI="${ENGINE_URI}/callback"
EXTERNAL_OIDC_USER_INFO_END_POINT=https://SSO.example.com/auth/realms/master
/protocol/openid-connect/userinfo
EXTERNAL_OIDC_TOKEN_END_POINT=https://SSO.example.com/auth/realms/master/prot
ocol/openid-connect/token
```

```
EXTERNAL_OIDC_LOGOUT_END_POINT=https://SSO.example.com/auth/realms/master/protocol/openid-connect/logout
EXTERNAL_OIDC_CLIENT_ID=ovirt-engine
EXTERNAL_OIDC_CLIENT_SECRET=<client_SSO_generated_key>
EXTERNAL_OIDC_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
EXTERNAL_OIDC_HTTPS_PKI_TRUST_STORE_PASSWORD=""
EXTERNAL_OIDC_SSL_VERIFY_CHAIN=false
EXTERNAL_OIDC_SSL_VERIFY_HOST=false
```

### 3.6.5.4. OVN の設定

Manager で **ovirt-ovn-provider** を設定した場合は、OVN プロバイダーの認証情報を設定する必要があります。

#### 手順

- 以下の内容で **/etc/ovirt-provider-ovn/conf.d/** に **20-setup-ovirt-provider-ovn.conf** ファイルを作成します。ここでの **user1** は LDAP グループ **ovirt-administrator** に属し、**openidchttp** は **aaa-ldap-misc** 用に設定されたプロファイルです。

```
[OVIRT]
ovirt-admin-user-name=user1@openidchttp
```

- ovirt-provider-ovn** を再起動します。

```
systemctl restart ovirt-provider-ovn
```

- 管理ポータルにログインして **Administration** → **Providers** に移動し、**ovirt-provider-ovn** を選択し、**Edit** をクリックして ovn プロバイダーのパスワードを更新します。

### 3.6.5.5. モニタリングポータル (Grafana) の設定

#### 手順

- クライアントの有効なリダイレクト URL を設定します。
  - 前の手順で設定したクライアントを選択します (例: **ovirt-engine**)。
  - モニタリングポータル (Grafana) 用に有効なリダイレクト URI を追加します。有効なリダイレクト URI: **https://rhvm.example.com:443/ovirt-engine-grafana/login/generic\_oauth/**
  - Mappers** タブを選択します。
  - Create** をクリックして、新しい Mapper を作成し、以下のフィールドに入力します。
    - Name: **realm role**
    - Mapper Type: **User Realm Role**
    - Token Claim Name: **realm\_access.roles**
    - Claim JSON Type: String
- Grafana 固有のロールを設定します。

- a. メインメニューから **Roles** を選択します。
- b. **admin**、**editor**、**viewer** のロールを追加します。
3. 目的のグループに Grafana 固有のロールを割り当てます。
  - a. メインメニューから **Groups** を選択し、目的のグループを選択します。
  - b. **Role Mappings** を選択します。
  - c. 目的のロールを **Available Roles** から **Assigned Roles** に移動します。
4. Grafana の設定 - **/etc/grafana/grafana.ini** の **auth.generic\_oauth** セクションを次のように変更します。必要に応じて、山括弧 (< >) 内の値を置き換えてください。

```
(...)
#####
[auth.generic_oauth]
name = oVirt Engine Auth
enabled = true
allow_sign_up = true
client_id = ovirt-engine
client_secret = <client-secret-of-RH-SSO>
scopes = openid,ovirt-app-admin,ovirt-app-portal,ovirt-ext=auth:sequence-priority=~email_attribute_name = email:primary
role_attribute_path = "contains(realm_access.roles['*'], 'admin') && 'Admin' ||
contains(realm_access.roles['*'], 'editor') && 'Editor' || 'Viewer'"
auth_url = https://<rh-sso-hostname>/auth/realms/<RH-SSO-REALM>/protocol/openid-connect/auth
token_url = https://<rh-sso-hostname>/auth/realms/<RH-SSO-REALM>/protocol/openid-connect/token
api_url = https://<rh-sso-hostname>/auth/realms/<RH-SSO-REALM>/protocol/openid-connect/userinfo
team_ids =
allowed_organizations =
tls_skip_verify_insecure = false
tls_client_cert =
tls_client_key =
tls_client_ca = /etc/pki/ovirt-engine/apache-ca.pem
send_client_credentials_via_post = false
(...)
```

### 3.6.6. ユーザーの承認

#### 3.6.6.1. ユーザー認証モデル

Red Hat Virtualization は、次の 3 つのコンポーネントの組み合わせに基づいて承認制御を適用します。

- アクションを実行するユーザー
- 実行されているアクションのタイプ
- アクションが実行されているオブジェクト

#### 3.6.6.2. ユーザーアクション

アクションを正常に実行するには、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 を ユーザー が、持っている必要があります。各アクションの種類には、対応する パーミッション があります。

いくつかのアクションは、複数のオブジェクトに対して実行されます。たとえば、テンプレートを別のストレージドメインにコピーすると、テンプレートと宛先ストレージドメインの両方に影響します。アクションを実行するユーザーは、アクションが影響を与えるすべてのオブジェクトに対して適切なパーミッションを持っている必要があります。

### 3.6.7. 管理ポータルからのユーザータスクの管理

#### 3.6.7.1. Account Settings ウィンドウ

Administration → Account Settings ウィンドウでは、次の管理ポータルユーザー設定を表示または編集できます。

- General タブ

- User Name - 読み取り専用。
- E-mail - 読み取り専用。
- Home Page:  
Default - #dashboard-main.

Custom home page - ハッシュマーク (#) を含む URL の最後の部分のみを入力します。例: #vms-snapshots;name-testVM。

- Serial Console

User's Public Key - シリアルコンソールを使用して Manager にアクセスするために使用される SSH 公開鍵を入力します。

- Tables

Persist grid settings - グリッド列の設定をサーバーに保存します。

- Confirmations タブ:

Show confirmation dialog on Suspend VM - 仮想マシンが一時停止された場合の確認ダイアログを有効にします。

#### 3.6.7.2. ユーザーの追加と VM ポータルパーミッションの割り当て

ユーザーを追加してロールおよびパーミッションを割り当てる前に、ユーザーを作成しておく必要があります。この手順で割り当てられたロールとパーミッションにより、ユーザーは VM ポータルにログインして仮想マシンの作成を開始できます。この手順は、グループアカウントにも適用されます。

#### 手順

1. ヘッダーバーで、Administration → Configure をクリックします。これにより、Configure ウィンドウが開きます。
2. System Permissions をクリックします。
3. Add をクリックします。Add System Permission to User ウィンドウが開きます。



4. **Search** でプロファイルを選択します。プロファイルは、検索するドメインです。検索テキスト フィールドに名前または名前の一部を入力し、**GO** をクリックします。または、**GO** をクリックして、すべてのユーザーとグループのリストを表示します。
5. 適切なユーザーまたはグループのチェックボックスを選択します。
6. **Role to Assign** で、割り当てる適切なロールを選択します。**UserRole** ロールは、VM ポータルにログインするためのアクセス許可をユーザー アカウントに付与します。
7. **OK** をクリックします。

VM ポータルにログインして、ユーザー アカウントにログインするパーミッションがあることを確認します。

### 3.6.7.3. ユーザー情報の表示

#### 手順

1. **Administration** → **Users** をクリックして、承認されたユーザーの一覧を表示します。
2. ユーザーの名前をクリックします。詳細ビューが開き、通常は **General** タブにドメイン名、電子メール、ユーザーのステータスなどの一般情報が表示されます。
3. 他のタブでは、ユーザーのグループ、パーミッション、割り当て、およびイベントを表示できます。

たとえば、ユーザーが属するグループを表示するには、**Directory Groups** タブをクリックします。

### 3.6.7.4. リソースでのユーザー パーミッションの表示

ユーザーには、特定のリソースまたはリソース階層のパーミッションを割り当てることができます。各リソースに割り当てられたユーザーとそのパーミッションを表示できます。

#### 手順

1. リソースの名前を見つけてクリックします。詳細ビューが開きます。
2. **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースの継承されたパーミッションを一覧表示します。

### 3.6.7.5. ユーザーの削除

不要になったユーザー アカウントは、Red Hat Virtualization から削除します。

#### 手順

1. **Administration** → **Users** をクリックして、承認されたユーザーの一覧を表示します。
2. 削除するユーザーを選択します。ユーザーが仮想マシンを実行していないことを確認します。
3. **Remove** をクリックしてから **OK** をクリックします。

ユーザーは Red Hat Virtualization から削除されますが、外部ディレクトリーからは削除されません。

### 3.6.7.6. ログインしたユーザーの表示

現在ログインしているユーザーを、セッション時間やその他の詳細とともに表示できます。Administration → Active User Sessions をクリックして、ログインしている各ユーザーの Session DB ID、User Name、Authorization provider、User id、Source IP、Session Start Time、および Session Last Active Time を表示します。

### 3.6.7.7. ユーザーセッションの終了

現在ログインしているユーザーのセッションを終了できます。

#### ユーザー SESSION の終了

1. Administration → Active User Sessions をクリックします。
2. 終了するユーザー SESSION を選択します。
3. Terminate Session をクリックします。
4. OK をクリックします。

### 3.6.8. コマンドラインからのユーザータスクの管理

**ovirt-aaa-jdbc-tool** ツールを使用して、内部ドメインのユーザーアカウントを管理できます。このツールを使用して行った変更はすぐに反映され、**ovirt-engine** サービスを再起動する必要はありません。ユーザー オプションの完全なリストを確認するには、**ovirt-aaa-jdbc-tool user --help** を実行してください。このセクションでは、一般的な例を示します。



#### 重要

Manager マシンにログインする必要があります。

#### 3.6.8.1. 新しいユーザーの作成

新しいユーザーアカウントを作成できます。オプションの **--attribute** コマンドは、アカウントの詳細を指定します。オプションの完全なリストについては、**ovirt-aaa-jdbc-tool user add --help** を実行してください。

```
ovirt-aaa-jdbc-tool user add test1 --attribute=firstName=John --attribute=lastName=Doe
adding user test1...
user added successfully
```

管理ポータルで新しく作成されたユーザーを追加し、ユーザーに適切なロールとパーミッションを割り当てることができます。詳細は、[ユーザーの追加](#) を参照してください。

#### 3.6.8.2. ユーザーパスワードの設定

パスワードを作成できます。**--password-valid-to** の値を設定する必要があります。設定しないと、パスワードの有効期限はデフォルトで現在の時刻になります。

+ 日付形式は **yyyy-MM-dd HH:mm:ssX** です。ここで、**X** は UTC からのタイムゾーンオフセットになります。この例では、**-0800** は GMT から 8 時間を引いたものを表します。ゼロオフセットの場合は、値 **Z** を使用します。

+ その他のオプションについては、**ovirt-aaa-jdbc-tool user password-reset --help** を実行してください。

```
ovirt-aaa-jdbc-tool user password-reset test1 --password-valid-to="2025-08-01 12:00:00-0800"
Password:
updating user test1...
user updated successfully
```



### 注記

デフォルトでは、内部ドメインのユーザーアカウントのパスワードポリシーには次の制限があります。

- 6 文字以上。
- パスワード変更中は、過去に使用した 3 つのパスワードを再度設定できません。

パスワードポリシーおよびその他のデフォルト設定の詳細は、**ovirt-aaa-jdbc-tool settings show** を実行してください。

管理者パスワードが更新されたら、変更を手動で **ovirt-provider-ovn** に送信する必要があります。そうしないと、Red Hat Virtualization Manager が引き続き古いパスワードを使用して **ovirt-provider-ovn** からのネットワークを同期するため、admin ユーザーがロックされます。新しいパスワードを **ovirt-provider-ovn** に送信するには、次の手順を実行します。

1. 管理ポータルで、Administration → Providers をクリックします。
2. **ovirt-provider-ovn** を選択します。
3. Edit をクリックして、Password フィールドに新しいパスワードを入力します。
4. Test をクリックして、指定した認証情報で認証が成功するかどうかをテストします。
5. 認証テストが成功したら、OK をクリックします。

#### 3.6.8.3. ユーザータイムアウトの設定

ユーザータイムアウト期間を設定できます。

```
engine-config --set UserSessionTimeOutInterval=integer
```

#### 3.6.8.4. ユーザーパスワードの事前暗号化

**ovirt-engine-crypto-tool** スクリプトを使用して、事前に暗号化されたユーザーパスワードを作成できます。このオプションは、スクリプトを使用してデータベースにユーザーとパスワードを追加する場合に役立ちます。



### 注記

パスワードは、暗号化された形式で Manager データベースに保存されます。すべてのパスワードを同じアルゴリズムで暗号化する必要があるため、**ovirt-engine-crypto-tool** スクリプトが使用されます。

パスワードがあらかじめ暗号化されている場合、パスワードの有効性テストは行えません。パスワードは、パスワード検証ポリシーに準拠していなくても受け入れられます。

1. 以下のコマンドを実行します。

```
/usr/share/ovirt-engine/bin/ovirt-engine-crypto-tool.sh pbe-encode
```

スクリプトは、パスワードの入力を促します。

また、**--password=file:file** オプションを使用すると、ファイルの先頭行として表示される1つのパスワードを暗号化することができます。このオプションは自動化に役立ちます。次の例では、**file** は暗号化用の単一のパスワードを含むテキストファイルです。

```
/usr/share/ovirt-engine/bin/ovirt-engine-crypto-tool.sh pbe-encode --password=file:file
```

2. **ovirt-aaa-jdbc-tool** スクリプトで、**--encrypted** オプションを使用して新しいパスワードを設定します。

```
ovirt-aaa-jdbc-tool user password-reset test1 --password-valid-to="2025-08-01 12:00:00-0800" --encrypted
```

3. 暗号化されたパスワードを入力して確認します。

```
Password:
Reenter password:
updating user test1...
user updated successfully
```

### 3.6.8.5. ユーザー情報の表示

詳細なユーザーアカウント情報を表示できます。

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

このコマンドにより、管理ポータルのAdministration → Users 画面により多くの情報が表示されます。

### 3.6.8.6. ユーザー情報の編集

メールアドレスなどのユーザー情報を更新できます。

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

### 3.6.8.7. ユーザーの削除

ユーザーアカウントを削除できます。

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

管理ポータルからユーザーを削除します。詳細は、[ユーザーの削除](#) を参照してください。

### 3.6.8.8. 内部管理ユーザーの無効化

**engine-setup** 中に作成された `admin@internal` ユーザーを含む、ローカルドメインのユーザーを無効にすることができます。デフォルトの `admin` ユーザーを無効にする前に、完全な管理者パーミッションを持つ環境に少なくとも1人のユーザーがいることを確認してください。

## 手順

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 ロールを持つ別のユーザーが環境に追加されていることを確認してください。詳細は、[ユーザーの追加](#) 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

無効になっているユーザーを有効にするには、**ovirt-aaa-jdbc-tool user edit username -flag=-disabled** を実行します。

## 3.6.8.9. グループの管理

**ovirt-aaa-jdbc-tool** ツールを使用して、内部ドメインのグループアカウントを管理できます。グループアカウントの管理は、ユーザーアカウントの管理に似ています。グループオプションの全リストは、**ovirt-aaa-jdbc-tool group --help** を実行してください。このセクションでは、一般的な例を示します。

### グループの作成

この手順では、グループアカウントを作成し、ユーザーをグループに追加し、グループの詳細を表示する方法を示します。

1. Red Hat Virtualization Manager がインストールされているマシンにログインします。
2. 新規グループを作成します。

```
ovirt-aaa-jdbc-tool group add group1
```

3. ユーザーをグループに追加します。ユーザーが作成されている必要があります。

```
ovirt-aaa-jdbc-tool group-manage useradd group1 --user=test1
```



### 注記

group-manage オプションの全リストは、**ovirt-aaa-jdbc-tool group-manage --help** を実行してください。

4. グループアカウントの詳細を表示します。

```
ovirt-aaa-jdbc-tool group show group1
```

5. 新しく作成したグループを管理ポータルに追加し、グループに適切なロールとパーミッションを割り当てます。グループ内のユーザーは、グループのロールおよびパーミッションを継承します。詳細は、[ユーザーの追加](#) を参照してください。

### ネストされたグループの作成

この手順では、グループ内にグループを作成する方法を示します。

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. 最初のグループを作成します。

```
ovirt-aaa-jdbc-tool group add group1
```

3. 2番目のグループを作成します。

```
ovirt-aaa-jdbc-tool group add group1-1
```

4. 2番目のグループを最初のグループに追加します。

```
ovirt-aaa-jdbc-tool group-manage groupadd group1 --group=group1-1
```

5. 管理ポータルに最初のグループを追加し、グループに適切なロールおよびパーミッションを割り当てます。詳細は、[ユーザーの追加](#) を参照してください。

### 3.6.8.10. ユーザーおよびグループのクエリー

**query** モジュールを使用すると、ユーザーおよびグループの情報をクエリーできます。オプションの完全なリストについては、**ovirt-aaa-jdbc-tool query --help** を実行してください。

#### すべてのユーザーまたはグループアカウントの詳細の一覧表示

この手順では、すべてのアカウント情報を一覧表示する方法を示します。

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

2. アカウントの詳細を一覧表示します。

- すべてのユーザーアカウントの詳細:

```
ovirt-aaa-jdbc-tool query --what=user
```

- すべてのグループアカウントの詳細:

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

#### フィルタリングされたアカウントの詳細の一覧表示

この手順では、アカウント情報を一覧表示するときにフィルターを適用する方法を示します。

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

2. **--pattern** パラメーターを使用して、アカウントの詳細をフィルタリングします。

- 文字 j で始まる名前でユーザーアカウントの詳細を一覧表示します。

```
ovirt-aaa-jdbc-tool query --what=user --pattern="name=j*"
```

- 部門属性が **marketing** に設定されているグループを一覧表示します。

```
ovirt-aaa-jdbc-tool query --what=group --pattern="department=marketing"
```

### 3.6.8.11. アカウント設定の管理

デフォルトのアカウント設定を変更するには、**ovirt-aaa-jdbc-tool settings** モジュールを使用します。

#### アカウント設定の更新

この手順では、デフォルトのアカウント設定を更新する方法を示します。

- 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。

- 次のコマンドを実行して、使用可能なすべての設定を表示します。

```
ovirt-aaa-jdbc-tool settings show
```

- 必要な設定を変更します。

- この例では、すべてのユーザーアカウントのデフォルトのログインセッション時間を 60 分に更新します。デフォルト値は 10080 分です。

```
ovirt-aaa-jdbc-tool settings set --name=MAX_LOGIN_MINUTES --value=60
```

- この例では、ユーザーアカウントがロックされる前に、ユーザーが実行できるログイン試行の失敗回数を更新します。デフォルト値は 5 です。

```
ovirt-aaa-jdbc-tool settings set --name=MAX_FAILURES_SINCE_SUCCESS --value=3
```



#### 注記

ロックされたユーザーアカウントを解除するには、**ovirt-aaa-jdbc-tool user unlock test1** を実行します。

### 3.6.9. 追加のローカルドメインの設定

デフォルトの内部ドメインに加え、追加のローカルドメインの作成もサポートされています。これは、**ovirt-engine-extension-aaa-jdbc** 拡張機能を使用して実行でき、外部のディレクトリーサーバーを接続せずに複数のドメインを作成できますが、エンタープライズ環境ではこのユースケースは一般的ではないでしょう。

追加で作成されたローカルドメインは、標準の Red Hat Virtualization アップグレード中に自動的にアップグレードされることはなく、将来のリリースごとに手動でアップグレードする必要があります。追加のローカルドメインの作成と、ドメインのアップグレード方法に関する詳細は、*/usr/share/doc/ovirt-engine-extension-aaa-jdbc-version/README.admin* の README ファイルを参照してください。



#### 注記

**ovirt-engine-extension-aaa-jdbc** 拡張機能は非推奨になりました。新規インストールの場合は、Red Hat Single Sign On を使用します。詳細は、[管理ガイドの Red Hat Single Sign-On のインストールおよび設定](#) を参照してください。

## 3.7. クォータとサービスレベル契約ポリシー

### 3.7.1. クォータの概要

クオータは、Red Hat Virtualization で提供されるリソース制限ツールです。クオータは、ユーザー・パーティションによって設定された制限レイヤーの上にある制限レイヤーと考えることができます。

クオータはデータセンター・オブジェクトです。

クオータを使用すると、Red Hat Virtualization 環境の管理者は、メモリー、CPU、およびストレージへのユーザー・アクセスを制限できます。クオータは、管理者がユーザーに割り当てることができるメモリーリソースとストレージリソースを定義します。その結果、ユーザーは自分に割り当てられたリソースのみを利用できます。クオータリソースを上限まで使用すると、Red Hat Virtualization はそれ以上のユーザー・アクションを許可しません。

クオータには 2 種類あります。

表3.3 2種類のクオータ

クオータタイプ	定義
実行時クオータ	このクオータは、CPU やメモリーなどのランタイムリソースの消費を制限するものです。
ストレージクオータ	このクオータは、利用可能なストレージの量を制限します。

SELinux などのクオータには 3 つのモードがあります。

表3.4 クオータモード

クオータモード	機能
Enforced	監査モードで設定したクオータが有効になり、クオータの影響を受けるグループまたはユーザーにリソースが制限されます。
Audit	ユーザーをブロックせずにクオータ違反をログに記録します。クオータのテストに使用できます。Audit モードでは、ランタイムクオータの量と、影響を受けるユーザーが利用できるストレージクオータの量を増減できます。
Disabled	クオータによって定義されたランタイムとストレージの制限をオフにします。

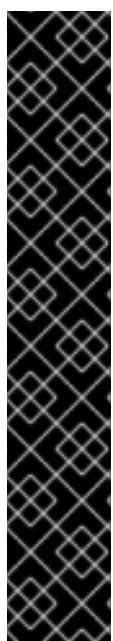
ユーザーが仮想マシンを実行しようとすると、仮想マシンの仕様と、該当するクオータに設定されているストレージ許容量およびランタイム許容量が比較されます。

仮想マシンを起動することで、クオータの対象となる実行中のすべての仮想マシンの集約リソースがクオータで定義された許容量を超える場合、Manager は仮想マシンの実行を拒否します。

ユーザーが新しいディスクを作成すると、要求されたディスクサイズが、該当するクオータでカバーされる他のすべてのディスクの合計ディスク使用量に追加されます。新しいディスクが、クオータで許可されている量を超える合計ディスク使用量を取得した場合、ディスクの作成は失敗します。

クオータでは、同じハードウェアのリソース共有が可能です。ハードとソフトのしきい値をサポートし

ます。管理者は、クオータを使用してリソースにしきい値を設定できます。ユーザーから見た場合、これらのしきい値はリソース使用率 100% として表示されます。ユーザーが予期せずしきい値を超えた場合に障害が発生することを防ぐために、インターフェイスでは一時的にしきい値を超えることができる "猶予量" をサポートしています。しきい値を超えると警告が送信されます。



### 重要

クオータは、仮想マシンの実行時に制限をいくつか課します。これらの制限を無視すると、仮想マシンと仮想ディスクを使用できない状況が発生する可能性があります。

クオータが強制モードで実行している場合、クオータが割り当てられていない仮想マシンとディスクは使用できません。

仮想マシンの電源をオンにするには、その仮想マシンにクオータを割り当てる必要があります。

仮想マシンのスナップショットを作成するには、仮想マシンに関連付けられているディスクにクオータが割り当てられている必要があります。

仮想マシンからテンプレートを作成する場合、テンプレートで使用するクオータを選択するように求められます。これにより、テンプレート (およびテンプレートから作成される将来のすべてのマシン) が、テンプレートの生成元の仮想マシンおよびディスクとは異なるクオータを消費するように設定できます。

### 3.7.2. 共有クオータおよび個別定義されたクオータ

SuperUser パーミッションを持つユーザーは、個々のユーザーのクオータまたはグループのクオータを作成できます。

Active Directory ユーザーに対してグループクオータを設定できます。ユーザー数が 10 人のグループに 1TB のストレージのクオータが割り当てられている場合、10 人のユーザーのうち 1人が 1TB をすべて使用すると、グループ全体がクオータを超過したことになります。10 人のユーザーのうち誰も自分のグループに関連するストレージを使用できなくなります。

個人ユーザーのクオータは、個人に対してのみ設定されます。個々のユーザーが自分のストレージまたはランタイムクオータをすべて使い切ると、ユーザーはクオータを超過し、ユーザーは自分のクオータに関連付けられたストレージを使用できなくなります。

### 3.7.3. クオータの計算

クオータがコンシューマーまたはリソースに割り当てられると、そのコンシューマーによる各アクションや、ストレージ、vCPU、メモリーに関連するリソースに対する各アクションにより、クオータの消費または解放が発生します。

クオータは、ユーザーによるリソースへのアクセスを制限する際の上限として機能するため、クオータの計算は、ユーザーによる現在の使用状況とは異なる場合があります。クオータは、現在の使用量ではなく、使用できる上限が計算されます。

#### 例3.15 計算例

ユーザーが、1つの vCPU と 1024 MB のメモリーを備えた仮想マシンを実行したとします。このアクションは、そのユーザーに割り当てられた 1つの vCPU と 1024 MB のクオータを消費します。仮想マシンが停止すると、1つの vCPU と 1024 MB の RAM が解放され、そのユーザーに割り当てられたクオータに戻ります。実行時のクオータ消費は、実際にコンシューマーが実行している間だけ計算に反映されます。

あるユーザーが 10 GB の仮想シンプロビジョンディスクを作成したとします。実際のディスク使用量としては、そのディスクが持つ 10 GB のうち 3 GB のみと表示されるかもしれません。しかし、クオータ消費量はそのディスクで使用できる上限であるため、10 GB になります。

### 3.7.4. データセンターにおけるクオータモードの有効化および変更

この手順では、データセンターのクオータモードを有効または変更します。クオータを定義する前に、クオータモードを選択する必要があります。この手順を実行するには、管理ポータルにログインする必要があります。

**Audit** モードを使用して、クオータをテストし、期待通りに動作することを確認します。クオータを作成または変更するために、クオータを **Audit** モードにする必要はありません。

#### 手順

1. データセンターの **Compute → Data Centers** をクリックして、データセンターを選択します。
2. **Edit** をクリックします。
3. **Quota Mode** ドロップダウンリストで、クオータモードを **Enforced** に変更します。
4. **OK** をクリックします。

テスト中にクオータモードを **Audit** に設定した場合、クオータ設定を有効にするには、クオータモードを **Enforced** に変更する必要があります。

### 3.7.5. 新しいクオータポリシーの作成

**Audit** モードまたは **Enforcing** モードのいずれかでクオータモードを有効にしました。データセンターのリソース使用量を管理するためのクオータポリシーを定義する必要があります。

#### 手順

1. **Administration → Quota** をクリックします。
2. **Add** をクリックします。
3. **Name** フィールドおよび **Description** フィールドに入力します。
4. **Data Center** を選択します。
5. **Memory & CPU** セクションで、緑のスライダーを使用して **Cluster Threshold** を設定します。
6. **Memory & CPU** セクションで、青のスライダーを使用して **Cluster Grace** を設定します。
7. **All Clusters** または **Specific Clusters** ラジオボタンをクリックします。**Specific Clusters** を選択した場合は、クオータポリシーを追加するクラスターのチェックボックスをオンにします。
8. **Edit** をクリックします。これにより、**Edit Quota** ウィンドウが開きます。
  - a. **Memory** フィールドで、**Unlimited** ラジオボタン（クラスター内のメモリーリソースを無制限に使用できるようにする）を選択するか、**limit to** ラジオボタンを選択して、このクオータで設定されるメモリーの量を設定します。**limit to** ラジオボタンを選択した場合は、**MB** フィールドにメモリークオータをメガバイト (MB) 単位で入力します。

- b. CPU フィールドで、Unlimited ラジオボタンまたは limit to ラジオボタンのいずれかを選択して、このクォータで設定される CPU の量を設定します。limit to ラジオボタンを選択した場合は、vCpus フィールドに vCPU の数を入力します。
  - c. Edit Quota ウィンドウで OK をクリックします。
9. Storage セクションで、緑色のスライダーを使用して Storage Threshold を設定します。
10. Storage セクションで、青のスライダーを使用して Storage Grace を設定します。
11. All Storage Domains または Specific Storage Domains ラジオボタンをクリックします。Specific Storage Domains を選択した場合は、クォータポリシーを追加するストレージドメインのチェックボックスをオンにします。
12. Edit をクリックします。これにより、Edit Quota ウィンドウが開きます。
- a. Storage Quota フィールドで、Unlimited ラジオボタン(ストレージを無制限に使用できるようにする)または limit to ラジオボタンを選択して、クォータがユーザーを制限するストレージの量を設定します。limit to ラジオボタンを選択した場合は、GB フィールドにストレージクォータのサイズをギガバイト(GB)で入力します。
  - b. Edit Quota ウィンドウで OK をクリックします。
13. New Quota ウィンドウで OK をクリックします。

### 3.7.6. クォータしきい値の設定の説明

表3.5 クォータしきい値と猶予

設定	定義
Cluster Threshold	データセンターごとに利用可能なクラスターリソースの量。
Cluster Grace	データセンターのクラスターしきい値を上限まで使用した後、データセンターで使用可能なクラスターの量。
Storage Threshold	データセンターごとに利用可能なストレージリソースの量。
Storage Grace	データセンターのストレージしきい値を上限まで使用した後、データセンターで使用可能なストレージの量。

クォータが 100 GB で、その猶予(Grace)が 20% に設定されている場合、使用者は 120 GB のストレージを使用した後、ストレージの使用をブロックされます。同じクォータのしきい値(Threshold)が 70% に設定されている場合、使用者は 70 GB のストレージ消費量を超えると警告を受け取ります(ただし、120 GB のストレージ消費量に達するまでストレージを消費できます)。“しきい値”および“猶予”的両方は、クォータを基準にして設定されます。“しきい値”は“ソフト制限”と考えることができます、それを超えると警告が生成されます。“猶予”は“ハード制限”として考えられ、それを超えると、これ以上ストレージリソースを消費できなくなります。

### 3.7.7. オブジェクトへのクオータの割り当て

#### 仮想マシンへのクオータの割り当て

1. Compute → Virtual Machines をクリックし、仮想マシンを選択します。
2. Edit をクリックします。
3. Quota ドロップダウンリストから、仮想マシンが消費するクオータを選択します。
4. OK をクリックします。

#### ディスクへのクオータの割り当て

1. Compute → Virtual Machines をクリックします。
2. 仮想マシンの名前をクリックします。詳細ビューが開きます。
3. Disks タブをクリックし、クオータに関連付ける予定のディスクを選択します。
4. Edit をクリックします。
5. Quota ドロップダウンリストから、仮想ディスクが消費するクオータを選択します。
6. OK をクリックします。



#### 重要

仮想マシンを機能させるには、仮想マシンに関連付けられているすべてのオブジェクトに対してクオータを選択する必要があります。仮想マシンに関連付けられているオブジェクトのクオータを選択しないと、仮想マシンは機能しません。この状況で Manager が出力するエラーは一般的なものであり、仮想マシンに関連付けられているすべてのオブジェクトにクオータを関連付けていないため、エラーが出力されたかどうかを判断することは困難です。クオータが割り当てられていない仮想マシンのスナップショットを作成することはできません。仮想ディスクにクオータが割り当てられていない仮想マシンのテンプレートを作成することはできません。

### 3.7.8. クオータを使用してユーザーごとにリソースを制限

この手順では、クオータを使用して、ユーザーがアクセスできるリソースを制限する方法を説明します。

#### 手順

1. Administration → Quota をクリックします。
2. ターゲットクオータの名前をクリックします。詳細ビューが開きます。
3. Consumers タブをクリックします。
4. Add をクリックします。
5. Search フィールドに、クオータに関連付けるユーザーの名前を入力します。
6. GO をクリックします。

7. ユーザー名の横にあるチェックボックスを選択します。

8. **OK** をクリックします。

しばらくすると、ユーザーが詳細ビューの **Consumers** タブに表示されます。

### 3.7.9. クオータの編集

この手順では、既存のクオータを変更する方法を説明します。

#### 手順

1. Administration → Quota をクリックして、クオータを選択します。
2. Edit をクリックします。
3. 必要に応じてフィールドを編集します。
4. **OK** をクリックします。

### 3.7.10. クオータの削除

この手順では、クオータを削除する方法を説明します。

#### 手順

1. Administration → Quota をクリックして、クオータを選択します。
2. Remove をクリックします。
3. **OK** をクリックします。

### 3.7.11. サービスレベルアグリーメントポリシーの実施

この手順では、サービスレベルアグリーメントの CPU 機能を設定する方法を説明します。

#### 手順

1. Compute → Virtual Machines をクリックします。
2. New をクリックするか、仮想マシンを選択して Edit をクリックします。
3. Resource Allocation タブをクリックします。
4. CPU Shares を指定します。使用できるオプションは、Low、Medium、High、Custom、および Disabled です。High に設定された仮想マシンは、Medium の 2 倍の共有を受け取り、Medium に設定された仮想マシンは、Low に設定された仮想マシンの 2 倍の共有を受け取ります。Disabled は、VDSM が共有の払い出しを決定するために古いアルゴリズムを使用するように指示します。通常、この条件で払い出される共有数は 1020 です。

ユーザーの CPU 消費は、設定したポリシーで制御されるようになりました。

## 3.8. イベント通知

### 3.8.1. 管理ポータルでのイベント通知の設定

Red Hat Virtualization Manager は、Red Hat Virtualization Manager が管理する環境で特定のイベントが発生したときに、指定されたユーザーに電子メールで通知できます。この機能を使用するには、メッセージを配信するようにメール転送エージェントを設定する必要があります。管理ポータルから設定できるのは、メール通知のみです。SNMP トラップは Manager マシンで設定する必要があります。

#### 手順

1. Manager からの自動メッセージを受け入れ、それらを配布リストに配信できる電子メールサーバーにアクセスできることを確認してください。
2. Administration → Users をクリックして、ユーザーを選択します。
3. ユーザーの **ユーザー名** をクリックすると、詳細ページが表示されます。
4. Event Notifier タブで、Manage Events をクリックします。
5. イベントを表示するには、Expand All ボタン、または件名別の展開ボタンを使用します。
6. 適切なチェックボックスを選択します。
7. Mail Recipient フィールドにメールアドレスを入力します。



#### 注記

電子メールアドレスは、テキストメッセージの電子メールアドレス(たとえば、**1234567890@carrierdomainname.com**)、または電子メールアドレスとテキストメッセージの電子メールアドレスを含む電子メールグループアドレスにすることができます。

8. OK をクリックします。
  9. Manager マシンで、**ovirt-engine-notifier.conf** を **90-email-notify.conf** という名前の新しいファイルにコピーします。
- ```
# cp /usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf /etc/ovirt-engine/notifier/notifier.conf.d/90-email-notify.conf
```
10. **90-email-notify.conf** を編集し、**EMAIL Notifications** セクション以外を削除します。
 11. 次の例のように、正しい電子メール変数を入力します。このファイルは、元の **ovirt-engine-notifier.conf** ファイルの値を上書きします。

```
#-----#
# EMAIL Notifications #
#-----#
# The SMTP mail server address. Required.
MAIL_SERVER=myemailserver.example.com

# The SMTP port (usually 25 for plain SMTP, 465 for SMTP with SSL, 587 for SMTP with TLS)
MAIL_PORT=25
```

```

# Required if SSL or TLS enabled to authenticate the user. Used also to specify 'from' user
address if mail server
# supports, when MAIL_FROM is not set. Address is in RFC822 format
MAIL_USER=

# Required to authenticate the user if mail server requires authentication or if SSL or TLS is
enabled
SENSITIVE_KEYS="${SENSITIVE_KEYS},MAIL_PASSWORD"
MAIL_PASSWORD=

# Indicates type of encryption (none, ssl or tls) should be used to communicate with mail
server.
MAIL_SMTP_ENCRYPTION=none

# If set to true, sends a message in HTML format.
HTML_MESSAGE_FORMAT=false

# Specifies 'from' address on sent mail in RFC822 format, if supported by mail server.
MAIL_FROM=rhev2017@example.com

# Specifies 'reply-to' address on sent mail in RFC822 format.
MAIL_REPLY_TO=

# Interval to send smtp messages per # of IDLE_INTERVAL
MAIL_SEND_INTERVAL=1

# Amount of times to attempt sending an email before failing.
MAIL_RETRIES=4

```



注記

その他のオプションについては、[/etc/ovirt-engine/notifier/notifier.conf.d/README](#) を参照してください。

12. **ovirt-engine-notifier** サービスを有効にして再起動し、行った変更をアクティブにします。

```

# systemctl daemon-reload
# systemctl enable ovirt-engine-notifier.service
# systemctl restart ovirt-engine-notifier.service

```

これで、指定されたユーザーは、Red Hat Virtualization 環境のイベントに基づいて電子メールを受信するようになりました。選択されたイベントは、そのユーザーの **Event Notifier** タブに表示されます。

3.8.2. 管理ポータルでのイベント通知のキャンセル

設定していた不要な電子メール通知をキャンセルします。

手順

1. Administration → Users をクリックします。
2. ユーザーの User Name をクリックします。 詳細ビューが開きます。

3. Event Notifier タブをクリックして、ユーザーが電子メール通知を受け取るイベントを一覧表示します。
4. Manage Events をクリックします。
5. イベントを表示するには、Expand All ボタン、または件名別の展開ボタンを使用します。
6. 該当するチェックボックスをオフにすると、そのイベントの通知が解除されます。
7. OK をクリックします。

3.8.3. ovirt-engine-notifier.conf のイベント通知のパラメーター

イベント通知機能の設定ファイルは、/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf にあります。

表3.6 ovirt-engine-notifier.conf 変数

| 変数名 | デフォルト | 備考 |
|------------------------|--------------------------------------|---|
| SENSITIVE_KEYS | none | ログに記録されないキーのコンマ区切りリスト。 |
| JBOSS_HOME | /opt/rh/eap7/root/usr/share/wildfly/ | Manager が使用する JBoss アプリケーションサーバーの場所。 |
| ENGINE_ETC | /etc/ovirt-engine | Manager が使用する etc ディレクトリーの場所。 |
| ENGINE_LOG | /var/log/ovirt-engine | Manager が使用する logs ディレクトリーの場所。 |
| ENGINE_USR | /usr/share/ovirt-engine | Manager が使用する usr ディレクトリーの場所。 |
| ENGINE_JAVA_MODULEPATH | \${ENGINE_USR}/modules | JBoss モジュールが追加されるファイルパス。 |
| NOTIFIER_DEBUG_ADDRESS | none | 通知機能が使用する Java 仮想マシンのリモートデバッグを実行するために使用できるマシンのアドレス。 |
| NOTIFIER_STOP_TIME | 30 | サービスがタイムアウトするまでの時間(秒)。 |
| NOTIFIER_STOP_INTERVAL | 1 | タイムアウトカウンターをインクリメントする時間(秒)。 |
| INTERVAL_IN_SECONDS | 120 | サブスクリーバーにメッセージをディスパッチするインスタンス間の間隔(秒)。 |

| 変数名 | デフォルト | 備考 |
|--|-----------|---|
| IDLE_INTERVAL | 30 | 低優先度タスクが実行される間隔(秒単位)。 |
| DAYS_TO_KEEP_HISTORY | 0 | ディスパッチされたイベントが履歴テーブルに保持される日数を設定します。この変数が設定されていない場合、イベントは履歴テーブルに無期限に残ります。 |
| FAILED_QUERIES_NOTIFICATION_THRESHOLD | 30 | 通知メールが送信された後に失敗したクエリーの数。最初に通知の取得に失敗した後、この変数で指定された失敗数に到達するたびに通知メールが1回送信されます。 0 または 1 を指定した場合は、失敗するたびに電子メールが送信されます。 |
| FAILED_QUERIES_NOTIFICATION_RECIPIENTS | none | 通知メールの送信先となる受信者のメールアドレス。メールアドレスはコンマで区切る必要があります。この項目は、 FILTER 変数によって非推奨とされました。 |
| DAYSTOSENDONSTARTUP | 0 | 通知機能の開始時に処理および送信される古いイベントの日数。値が0で、サービス停止後しばらくしてから起動すると、サービス停止とサービス開始の間のすべての通知が失われます。サービスの停止時刻と開始時刻の間に発生したイベントに関する通知を取得する場合は、この値を1に設定してください。 |
| FILTER | exclude:* | 電子メール通知のトリガーと受信者を決定するために使用されるアルゴリズム。この変数の値は、 include または exclude 、 event 、および recipient の組み合わせで構成されます。たとえば、 include:VDC_START(smt p:mail@example.com) \${FILTER} のようになります。 |
| MAIL_SERVER | none | SMTP メールサーバーアドレス。必須。 |

| 変数名 | デフォルト | 備考 |
|----------------------|----------------------------------|---|
| MAIL_PORT | 25 | 通信に使用されるポート。プレーンSMTPの場合は 25 、SSLを使用したSMTPの場合は 465 、TLSを使用したSMTPの場合は 587 を値として使用できます。 |
| MAIL_USER | none | ユーザー認証のためにSSLが有効な場合は、この変数を設定する必要があります。この変数は、MAIL_FROM変数が設定されていない場合に"from"のユーザーアドレスを指定するためにも使用されます。一部のメールサーバーでは、この機能をサポートしていません。アドレスはRFC822形式です。 |
| SENSITIVE_KEYS | \${SENSITIVE_KEYS},MAIL_PASSWORD | メールサーバーで認証が必要な場合、もしくはSSLまたはTLSが有効になっている場合は、ユーザーを認証するために必要です。 |
| MAIL_PASSWORD | none | メールサーバーで認証が必要な場合、もしくはSSLまたはTLSが有効になっている場合は、ユーザーを認証するために必要です。 |
| MAIL_SMTP_ENCRYPTION | none | 通信に使用する暗号の種類を指定します。可能な値は none 、 ssl 、 tls です。 |
| HTML_MESSAGE_FORMAT | false | この変数が true に設定されている場合、メールサーバーはHTMLフォーマットでメッセージを送信します。 |
| MAIL_FROM | none | メールサーバーでサポートされている場合、RFC822形式で送信者アドレスを指定します。 |
| MAIL_REPLY_TO | none | メールサーバーでサポートされている場合、送信メールの返信先アドレスをRFC822形式で指定します。 |
| MAIL_SEND_INTERVAL | 1 | IDLE_INTERVALごとに送信されるSMTPメッセージの数 |

| 変数名 | デフォルト | 備考 |
|--------------------|-------------------------|---|
| MAIL_RETRYES | 4 | 失敗する前に電子メールの送信を試行する回数。 |
| SNMP_MANAGERS | none | SNMP マネージャーとして機能するマシンの IP アドレスまたは完全修飾ドメイン名。エントリーはスペースで区切る必要があり、ポート番号を含めることができます。たとえば、 manager1.example.com manager2.example.com:164 です。 |
| SNMP_COMMUNITY | public | (SNMP バージョン 2 のみ) SNMP コミュニティー。 |
| SNMP_OID | 1.3.6.1.4.1.2312.13.1.1 | アラートのデフォルトのトラップオブジェクト識別子。この OID が定義されると、すべてのトラップタイプがイベント情報とともに SNMP マネージャーに送信されます。デフォルトのトラップを変更すると、生成されたトラップが Manager の管理情報ベースに準拠できなくなることに注意してください。 |
| SNMP_VERSION | 2 | 使用する SNMP のバージョンを定義します。SNMP バージョン 2 およびバージョン 3 トラップがサポートされています。可能な値: 2 または 3 。 |
| SNMP_ENGINE_ID | none | (SNMPv3) SNMPv3 トラップに使用されるマネージャー ID。この ID は、SNMP で接続された機器に固有の識別子です。 |
| SNMP_USERNAME | none | (SNMPv3) SNMPv3 トラップに使用されるユーザー名。 |
| SNMP_AUTH_PROTOCOL | none | (SNMPv3) SNMPv3 認可プロトコル。可能な値: MD5 、 SHA |

| 変数名 | デフォルト | 備考 |
|----------------------------|-------|--|
| SNMP_AUTH_PASSPHRASE | none | (SNMPv3)
SNMP_SECURITY_LEVEL が AUTH_NOPRIV および AUTH_PRIV に設定されている場合に使用されるパスフレーズ。 |
| SNMP_PRIVACY_PROTOCOL | none | (SNMPv3) SNMPv3 プライバシー プロトコル。可能な値:
AES128、AES192、AES256 |
| | |  重要
AES192 および AES256 は RFC3826 で定義されていないため、SNMP サーバーがこれらのプロトコルをサポートしていることを確認してから有効にしてください。 |
| SNMP_PRIVACY_PASSPHRASE | none | SNMP_SECURITY_LEVEL が AUTH_PRIV に設定されている場合に使用される SNMPv3 プライバシーパスフレーズ。 |
| SNMP_SECURITY_LEVEL | 1 | (SNMPv3) SNMPv3 のセキュリティーレベル。可能な値: *1 - NOAUTH_NOPRIV *2 - AUTH_NOPRIV *3 - AUTH_PRIV |
| ENGINE_INTERVAL_IN_SECONDS | 300 | Manager がインストールされているマシンを監視する間隔(秒)。この間隔は、監視が完了した時点から測定されます。 |
| ENGINE_MONITOR_RETRIES | 3 | 通知機能が、障害が発生した後、Manager がインストールされているマシンのステータスを指定された間隔で監視しようとする回数。 |
| ENGINE_TIMEOUT_IN_SECONDS | 30 | 通知機能が、障害が発生した後、Manager がインストールされているマシンのステータスを指定された間隔で監視するまで待機する時間(秒)。 |

| 変数名 | デフォルト | 備考 |
|------------------------------------|--|---|
| IS_HTTPS_PROTOCOL | false | JBoss がセキュアモードで実行されている場合、このエントリーは true に設定する必要があります。 |
| SSL_PROTOCOL | TLS | SSL が有効な場合に JBoss Configuration コネクターが使用するプロトコル。 |
| SSL_IGNORE_CERTIFICATE_ERRORS | false | JBoss がセキュアモードで実行されており、SSL エラーを無視する場合は、この値を true に設定する必要があります。 |
| SSL_IGNORE_HOST_VERIFICATION | false | JBoss がセキュアモードで実行されており、ホスト名の検証が無視される場合は、この値を true に設定する必要があります。 |
| REPEAT_NON_RESPONSIVE_NOTIFICATION | false | この変数は、Manager がインストールされているマシンが応答しない場合に、繰り返し失敗メッセージをサブスクリーバーに送信するかどうかを指定します。 |
| ENGINE_PID | /var/lib/ovirt-engine/ovirt-engine.pid | Manager の PID のパスとファイル名。 |

3.8.4. SNMP トラップを送信するための Red Hat Virtualization Manager 設定

Simple Network Management Protocol (SNMP) トラップを1つ以上の外部 SNMP マネージャーに送信するように Red Hat Virtualization Manager を設定します。SNMP トラップには、システムイベント情報が含まれています。これらは、Red Hat Virtualization 環境を監視するのに使用されます。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 内で定義できます。

Red Hat Virtualization は、SNMP バージョン 2 およびバージョン 3 をサポートします。SNMP バージョン 3 は、以下のセキュリティレベルをサポートしています。

NoAuthNoPriv

SNMP トラップは、許可やプライバシーなしで送信されます。

AuthNoPriv

SNMP トラップはパスワード認証で送信されますが、プライバシーは送信されません。

AuthPriv

SNMP トラップは、パスワード認証とプライバシーを使用して送信されます。

前提条件

- 1つ以上の外部 SNMP マネージャーがトラップを受け取るように設定されている。

- SNMP マネージャーとして機能するマシンの IP アドレスまたは完全修飾ドメイン名。必要に応じて、Manager がトラップ通知を受け取るポートを決定します。デフォルトは UDP ポート 162 です。
- SNMP コミュニティー (SNMP バージョン 2 のみ)。複数の SNMP マネージャーが単一のコミュニティーに属することができます。管理システムとエージェントは、同じコミュニティー内にある場合にのみ通信できます。デフォルトのコミュニティーは **public** です。
- アラートのトラップオブジェクト識別子。Red Hat Virtualization Manager は、デフォルトの OID 1.3.6.1.4.1.2312.13.1.1 を提供します。この OID が定義されると、すべてのトラップタイプがイベント情報とともに SNMP マネージャーに送信されます。デフォルトのトラップを変更すると、生成されたトラップが Manager の管理情報ベースに準拠できなくなることに注意してください。
- SNMP バージョン 3、セキュリティーレベル 1、2、3 の SNMP ユーザー名。
- SNMP バージョン 3、セキュリティーレベル 2 および 3 の SNMP パスフレーズ。
- SNMP バージョン 3、セキュリティーレベル 3 の SNMP プライベートパスフレーズ。



注記

Red Hat Virtualization Manager は、**/usr/share/doc/ovirt-engine/mibs/OVIRT-MIB.txt** および **/usr/share/doc/ovirt-engine/mibs/REDHAT-MIB.txt** に管理情報ベースを提供します。SNMP マネージャーに MIB をロードしてから作業を進めます。

デフォルトの SNMP 設定値は、Manager のイベント通知デーモン設定ファイル **/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf** にあります。次の手順で概説する値は、このファイルで提供されているデフォルト値またはサンプル値に基づいています。アップグレードなどのシステム変更により、このファイルに加えた変更が削除される可能性があるため、このファイルを直接編集しないでください。代わりに、このファイルを **/etc/ovirt-engine/notifier/notifier.conf.d/<integer>-snmp.conf** にコピーします。ここで **<integer>** は、ファイルを実行する優先順位を示す数値です。

手順

- Manager で、ファイル名 **<integer>-snmp.conf** を使用して SNMP 設定ファイルを作成します。ここで **<integer>** は、ファイルが処理される順序を示す整数です。以下に例を示します。

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

ヒント

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** からデフォルトの SNMP 設定をコピーします。このファイルには、すべての設定のインラインコメントが含まれています。

- 次の例の形式で、SNMP マネージャー、SNMP コミュニティー (SNMP バージョン 2 のみ)、および OID を指定します。

```
SNMP_MANAGER="manager1.example.com manager2.example.com:162"
SNMP_COMMUNITY=public
SNMP_OID=1.3.6.1.4.1.2312.13.1.1
```

3. SNMP バージョン 2(デフォルト) または 3 のいずれを使用するかを定義します。

```
SNMP_VERSION=3
```

4. SNMP_ENGINE_ID の値を指定します。以下に例を示します。

```
SNMP_ENGINE_ID="80:00:00:00:01:02:05:05"
```

5. SNMP バージョン 3 では、SNMP トラップのセキュリティーレベルを指定します。

セキュリティーレベル 1、NoAuthNoPriv トラップの場合。

```
SNMP_USERNAME=NoAuthNoPriv
SNMP_SECURITY_LEVEL=1
```

セキュリティーレベル 2、AuthNoPriv トラップ、ユーザー **ovirtengine** として、SNMP Auth パスフレーズ **authpass** を使用する場合。

```
SNMP_USERNAME=ovirtengine
SNMP_AUTH_PROTOCOL=MD5
SNMP_AUTH_PASSPHRASE=authpass
SNMP_SECURITY_LEVEL=2
```

セキュリティーレベル 3、AuthPriv トラップ、ユーザー **ovirtengine** として、SNMP Auth パスフレーズ **authpass** および SNMP Priv パスフレーズ **privpass** を使用する場合。以下に例を示します。

```
SNMP_USERNAME=ovirtengine
SNMP_AUTH_PROTOCOL=MD5
SNMP_AUTH_PASSPHRASE=authpass
SNMP_PRIVACY_PROTOCOL=AES128
SNMP_PRIVACY_PASSPHRASE=privpass
SNMP_SECURITY_LEVEL=3
```

6. SNMP マネージャーに送信するイベントを定義します。

例3.16 イベントの例

すべてのイベントをデフォルトの SNMP プロファイルに送信します。

```
FILTER="include:*(snmp:) ${FILTER}"
```

重大度が **ERROR** または **ALERT** のすべてのイベントをデフォルトの SNMP プロファイルに送信します。

```
FILTER="include:*:ERROR(snmp:) ${FILTER}"
```

```
FILTER="include:*:ALERT(snmp:) ${FILTER}"
```

VDC_START のイベントを指定された電子メールアドレスに送信します。

```
FILTER="include:VDC_START(snmp:mail@example.com) ${FILTER}"
```

VDC_START 以外のすべてのイベントをデフォルトの SNMP プロファイルに送信します。

```
FILTER="exclude:VDC_START include:*(snmp:) ${FILTER}"
```

これは、**ovirt-engine-notifier.conf** で定義されているデフォルトのフィルターです。このフィルターを無効にしない場合、またはオーバーライドフィルターを適用しない場合、通知は送信されません。

```
FILTER="exclude:*
```

VDC_START は、使用可能な監査ログメッセージの例です。監査ログメッセージの完全なリストは、**/usr/share/doc/ovirt-engine/AuditLogMessages.properties** にあります。または、SNMP マネージャー内で結果をフィルター処理します。

7. ファイルを保存します。
8. **ovirt-engine-notifier** サービスを開始し、このサービスが起動時に開始することを確認します。

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

SNMP マネージャーをチェックして、トラップを受け取っていることを確認します。



注記

通知サービスを実行するには、**SNMP_MANAGER**、**MAIL_SERVER**、またはその両方を、**/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf** またはオーバーライドファイルで適切に定義する必要があります。

サンプル SNMP 設定ファイル

このサンプル設定ファイルは、**ovirt-engine-notifier.conf** の設定に基づくものです。このような専用の SNMP 設定ファイルは、**ovirt-engine-notifier.conf** の設定より優先されます。

ヒント

デフォルトの SNMP 設定を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** から **/etc/ovirt-engine/notifier/notifier.conf.d/<_integer_>-snmp.conf** にコピーします。ここでの **<_integer_>** は、ファイルを実行する優先順位を示す数値です。このファイルには、すべての設定のインラインコメントが含まれています。

/etc/ovirt-engine/notifier/notifier.conf.d/20-snmp.conf

```
SNMP_MANAGER="manager1.example.com manager2.example.com:162" ①
SNMP_COMMUNITY=public ②
SNMP_OID=1.3.6.1.4.1.2312.13.1.1 ③
FILTER="include:*(snmp:)" ④
SNMP_VERSION=3 ⑤
SNMP_ENGINE_ID="80:00:00:00:01:02:05:05" ⑥
SNMP_USERNAME=<username> ⑦
SNMP_AUTH_PROTOCOL=MD5 ⑧
SNMP_AUTH_PASSPHRASE=<authpass> ⑨
```

SNMP_PRIVACY_PROTOCOL=AES128 ⑩
 SNMP_PRIVACY_PASSPHRASE=<privpass> ⑪
 SNMP_SECURITY_LEVEL=3 ⑫

- ① 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、ポート番号を含めることができます。たとえば、`manager1.example.com manager2.example.com:164` です。
- ② (SNMP バージョン 2 のみ) デフォルトの SNMP コミュニティー文字列です。
- ③ 送信通知用の SNMP トラップオブジェクト識別子 iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) redhat(2312) ovirt(13) engine(1) notifier(1) です。



注記

デフォルトを変更すると、生成されたトラップが OVIRT-MIB.txt に準拠しなくなります。

- ④ SNMP 通知のトリガーと受信者を決定するために使用されるアルゴリズム。
- ⑤ SNMP バージョン。SNMP バージョン 2 およびバージョン 3 トラップがサポートされています。
2 = SNMPv2、3 = SNMPv3。
- ⑥ (SNMP バージョン 3 のみ) SNMP トラップに使用されるエンジン ID。
- ⑦ (SNMP バージョン 3 のみ) SNMP トラップに使用されるユーザー名。
- ⑧ (SNMP バージョン 3 のみ) SNMP 認証プロトコル。サポートされている値は MD5 と SHA です。**SNMP_SECURITY_LEVEL** が 2 (**AUTH_NOPRIV**) または 3 (**AUTH_PRIV**) に設定されている場合に必要です。
- ⑨ (SNMP バージョン 3 のみ) SNMP 認証パスフレーズ。**SNMP_SECURITY_LEVEL** が 2 (**AUTH_NOPRIV**) または 3 (**AUTH_PRIV**) に設定されている場合に必要です。
- ⑩ (SNMP バージョン 3 のみ) SNMP プライバシープロトコル。サポートされている値は、AES128、AES192、および AES256 です。AES192 および AES256 は RFC3826 で定義されていないことに注意してください。したがって、SNMP サーバーがこれらのプロトコルをサポートしていることを確認してから、それらを有効にしてください。**SNMP_SECURITY_LEVEL** が 3 (**AUTH_PRIV**) に設定されている場合に必要です。
- ⑪ (SNMP バージョン 3 のみ) SNMP プライバシーパスフレーズです。**SNMP_SECURITY_LEVEL** が 3 (**AUTH_PRIV**) に設定されている場合に必要です。
- ⑫ (SNMP バージョン 3 のみ) SNMP セキュリティーレベル。1 = **NOAUTH_NOPRIV**、2 = **AUTH_NOPRIV**、3 = **AUTH_PRIV**。

3.9. ユーティリティー

3.9.1. oVirt エンジンの名前変更ツール

3.9.1.1. oVirt エンジンの名前変更ツール

`engine-setup` コマンドをクリーンな環境で実行すると、セットアッププロセス中に提供された

Manager の完全修飾ドメイン名を使用する多数の証明書およびキーが生成されます。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(たとえば、Manager をホストしているマシンを別のドメインに移行したため)、完全修飾ドメイン名のレコードを更新して、新しい名前を反映する必要があります。**ovirt-engine-rename** コマンドは、この作業を自動化します。

ovirt-engine-rename コマンドは、次の場所にある Manager の完全修飾ドメイン名のレコードを更新します。

- /etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
- /etc/ovirt-engine/isouploader.conf.d/10-engine-setup.conf
- /etc/ovirt-engine/logcollector.conf.d/10-engine-setup.conf
- /etc/pki/ovirt-engine/cert.conf
- /etc/pki/ovirt-engine/cert.template
- /etc/pki/ovirt-engine/certs/apache.cer
- /etc/pki/ovirt-engine/keys/apache.key.nopass
- /etc/pki/ovirt-engine/keys/apache.p12

注記

本当に必要な場合に限り、以下を実行してください。

バージョン 4.0.4 以降、Manager Web インターフェイスにアクセスするための名前をさらに追加できるようになりました。

1. 関連するレコードを DNS サーバーまたは **/etc/hosts** に追加して、選択した名前が Manager マシンの IP アドレスに対して解決できることを確認します(**ping enginenename** または **getent hosts enginenename** を使用して確認します)。
2. 以下のコマンドを実行します。

```
----  
# echo 'SSO_ALTERNATE_ENGINE_FQDN="alias1.example.com  
alias2.example.com"' \  
> /etc/ovirt-engine/engine.conf.d/99-custom-sso-setup.conf  
# systemctl restart ovirt-engine.service  
----  
. List the alternate names separated by spaces.
```

Manager マシンの IP アドレスを追加することもできます。ただし、DNS 名の代わりに IP アドレスを使用することは適切ではありません。



警告

ovirt-engine-rename コマンドは、Manager が実行している Web サーバーの新しい証明書を作成しますが、Manager または認証局の証明書には影響しません。このため、特に Red Hat Enterprise Virtualization 3.2 以前からアップグレードされた環境では、**ovirt-engine-rename** コマンドの使用に伴うリスクがあります。したがって、可能な場合は、**engine-cleanup** および **engine-setup** を実行して、Manager の完全修飾ドメイン名を変更することが推奨されます。



警告

アップグレードプロセス中、古いホスト名は解決可能である必要があります。oVirt Engine Rename Tool が失敗して [ERROR] Host name is not valid: <OLD FQDN> did not resolve into an IP address が発生した場合は、古いホスト名を **/etc/hosts** ファイルに追加し、oVirt Engine Rename Tool を使用します。次に、**/etc/hosts** ファイルから古いホスト名を削除します。

3.9.1.2. oVirt Engine Rename コマンドの構文

ovirt-engine-rename コマンドの基本的な構文は次のとおりです。

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

このコマンドは、次のオプションも受け入れます。

--newname=[new name]

ユーザーの操作なしで、Manager の新しい完全修飾ドメイン名を指定できます。

--log=[file]

名前変更操作のログが書き込まれるファイルのパスおよび名前を指定できます。

--config=[file]

名前変更操作にロードする設定ファイルのパスおよびファイル名を指定できます。

--config-append=[file]

名前変更操作に追加する設定ファイルのパスおよびファイル名を指定できます。このオプションを使用して、既存の応答ファイルのパスおよびファイル名を指定し、名前変更操作を自動化できます。

--generate-answer=[file]

回答と **ovirt-engine-rename** コマンドで変更された値が記録されるファイルのパスおよびファイル名を指定できます。

3.9.1.3. oVirt Engine Rename Tool を使って Manager の名前を変更

ovirt-engine-rename コマンドを使用して、Manager の完全修飾ドメイン名 (FQDN) のレコードを更新できます。

このツールは、Manager がローカル ISO またはデータストレージドメインを提供しているか確認します。提供している場合、操作を続行する前に、ストレージに接続されている仮想マシンまたはストレージドメインをイジェクト、シャットダウン、またはメンテナンスマードにするように、ツールからユーザーに対してプロンプトが表示されます。これにより、仮想マシンが仮想ディスクとの接続を失うことなくなり、名前の変更プロセス中に ISO ストレージドメインが接続を失うことを防げます。

手順

1. 新しい FQDN のすべての DNS およびその他の関連レコードを準備します。
2. DHCP を使用している場合は、DHCP サーバーの設定を更新します。
3. Manager のホスト名を更新します。
4. 以下のコマンドを実行します。

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

5. プロンプトが表示されたら、**Enter** キーを押してエンジンサービスを停止してください。

```
During execution engine service will be stopped (OK, Cancel) [OK]:
```

6. プロンプトが表示されたら、マネージャーの新しい FQDN を入力します。

```
New fully qualified server name:new_engine_fqdn
```

ovirt-engine-rename コマンドは、Manager の FQDN のレコードを更新します。

セルフホスト型エンジンで実行する追加の手順:

1. 既存のすべてのセルフホスト型エンジンノードで次のコマンドを実行します。

```
# hosted-engine --set-shared-config fqdn new_engine_fqdn --type=he_local
```

このコマンドは、各セルフホストエンジンノードのローカルコピー **/etc/ovirt-hosted-engine-ha/hosted-engine.conf** の FQDN を変更します

2. セルフホスト型エンジンノードの1つで次のコマンドを実行します。

```
# hosted-engine --set-shared-config fqdn new_engine_fqdn --type=he_shared
```

このコマンドは、共有ストレージドメインの **/etc/ovirt-hosted-engine-ha/hosted-engine.conf** のメインコピーの FQDN を変更します。

現在、すべての新規および既存のセルフホスト型エンジンノードは新しい FQDN を使用します。



注記

oVirt Engine Rename Tool は、ローカルマシンでのみ機能するように設計されています。Manager 名を変更しても、リモート Data Warehouse マシンの名前は自動的に更新されません。リモート DWH マシンの名前を変更するには、手動で実行する必要があります。

リモート Data Warehouse のデプロイメントの場合に (Manager マシン上ではなく) リモートマシン上で実行する手順:

- 以下の PKI ファイルを削除します。

```
/etc/pki/ovirt-engine/apache-ca.pem/etc/pki/ovirt-engine/apache-grafana-
ca.pem/etc/pki/ovirt-engine/certs/*etc/pki/ovirt-engine/keys/*
```

- 以下のファイルで、Manager の fqdn を新しい名前 (例: **vm-new-name.local_lab_server.redhat.com**) に更新します。

```
/etc/grafana/grafana.ini/etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-
database.conf/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

- offline スイッチを指定して engine-setup を実行し、この時点で更新を防ぎます。

```
# engine-setup --offline
```

3.9.2. エンジン設定ツール

3.9.2.1. エンジン設定ツール

エンジン設定ツールは、Red Hat Virtualization 環境のグローバル設定を設定するためのコマンドラインユーティリティーです。このツールは、エンジンデータベースに格納されているキーと値のマッピングのリストと対話し、個々のキーの値を取得して設定し、使用可能なすべての設定キーおよび値のリストを取得できるようにします。さらに、Red Hat Virtualization 環境の設定レベルごとに異なる値を保管できます。



注記

Red Hat Virtualization Manager と Red Hat JBoss Enterprise Application Platform を実行しているなくても、設定キーの値を取得または設定できます。設定キー値とキーのマッピングはエンジンデータベースに保存されるため、**postgresql** サービスの実行中に更新できます。その後、**ovirt-engine** サービスが再起動されたときに変更が適用されます。

3.9.2.2. engine-config コマンドの構文

Red Hat Virtualization Manager がインストールされているマシンからエンジン設定ツールを実行できます。使用方法の詳細は、そのコマンドのヘルプ出力を印刷してください。

```
# engine-config --help
```

一般的なタスク:

- 使用可能な設定キーを一覧表示します。

```
# engine-config --list
```

- 使用可能な設定値を一覧表示します。

```
# engine-config --all
```

- 設定キーの値を取得します。

```
# engine-config --get KEY_NAME
```

KEY_NAME を優先するキーの名前に置き換えて、与えられたバージョンのキーの値を取得します。取得する値の設定バージョンを指定する場合は、**-cver** パラメーターを使用します。バージョンを指定しない場合は、すべての既存バージョンの値が返されます。

- 設定キーの値を設定します。

```
# engine-config --set KEY_NAME=KEY_VALUE --cver=VERSION
```

KEY_NAME は設定するキーの名前に、**KEY_VALUE** は設定する値に置き換えます。複数の設定バージョンがある環境では、**VERSION** を指定する必要があります。

- 変更を読み込むために ovirt-engine サービスを再起動します。
変更を有効にするには、ovirt-engine サービスを再起動する必要があります。

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

3.9.3. USB フィルターエディター

3.9.3.1. USB Filter Editor のインストール

USB Filter Editor は、ポリシーファイル `usbfilter.txt` を設定するために使用する Windows ツールです。このファイルで定義されたポリシールールは、クライアントマシンから Red Hat Virtualization Manager を使用して管理される仮想マシンへの特定の USB デバイスの自動パススルーを許可または拒否します。ポリシーファイルは、Red Hat Virtualization Manager 上の `/etc/ovirt-engine/usbfilter.txt` に存在します。USB フィルターポリシーの変更は、Red Hat Virtualization Manager 上の ovirt-engine サービスが再起動されない限り、有効にはなりません。

[Installers and Images for Red Hat Virtualization Manager](#) のトピックから USB Filter Editor インストーラーをダウンロードします。

手順

1. Windows マシンの場合、`.zip` ファイルから `.msi` インストーラーを解凍し、`.msi` インストーラーを実行します。
2. インストールウィザードの手順に従います。特に指定がない限り、USB フィルターエディターは、Windows のバージョンに応じて、デフォルトで `C:\Program Files\RedHat\USB Filter Editor` または `C:\Program Files(x86)\RedHat\USB Filter Editor` のいずれかにインストールされます。
3. デスクトップに USB フィルターエディターのショートカットアイコンが作成されます。



重要

[WinSCP](#) などのセキュアコピー (SCP) クライアントを使用して、Red Hat Virtualization Manager からフィルターポリシーをインポートおよびエクスポートします。

デフォルトの USB デバイスピリシーは、仮想マシンに USB デバイスへの基本的なアクセスを提供します。ポリシーを更新して、追加の USB デバイスの使用を許可します。

3.9.3.2. USB Filter Editor インターフェイス

デスクトップの USB Filter Editor ショートカットアイコンをダブルクリックします。

Red Hat USB Filter Editor インターフェイスには、各 USB デバイスの Class、Vendor、Product、Revision、および Action が表示されます。許可された USB デバイスは、Action 列で Allow に設定されています。禁止されているデバイスは Block に設定されています。

表3.7 USB エディターフィールド

| 名前 | 説明 |
|----------|--|
| クラス | USB デバイスのタイプ(プリンター、大容量ストレージコントローラーなど)。 |
| Vendor | 選択したタイプの製造元。 |
| Product | 特定の USB デバイスモデル。 |
| Revision | 製品の改訂。 |
| Action | 指定されたデバイスを許可またはブロックします。 |

USB デバイスピリシールールは、リストされている順序で処理されます。Up ボタンと Down ボタンを使用して、ルールをリストの上下に移動します。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るようにするには、ユニバーサルな ブロック ルールを最下位のエントリーとして残す必要があります。

3.9.3.3. USB ポリシーの追加

デスクトップの USB Filter Editor ショートカットアイコンをダブルクリックします。これにより、エディターが開きます。

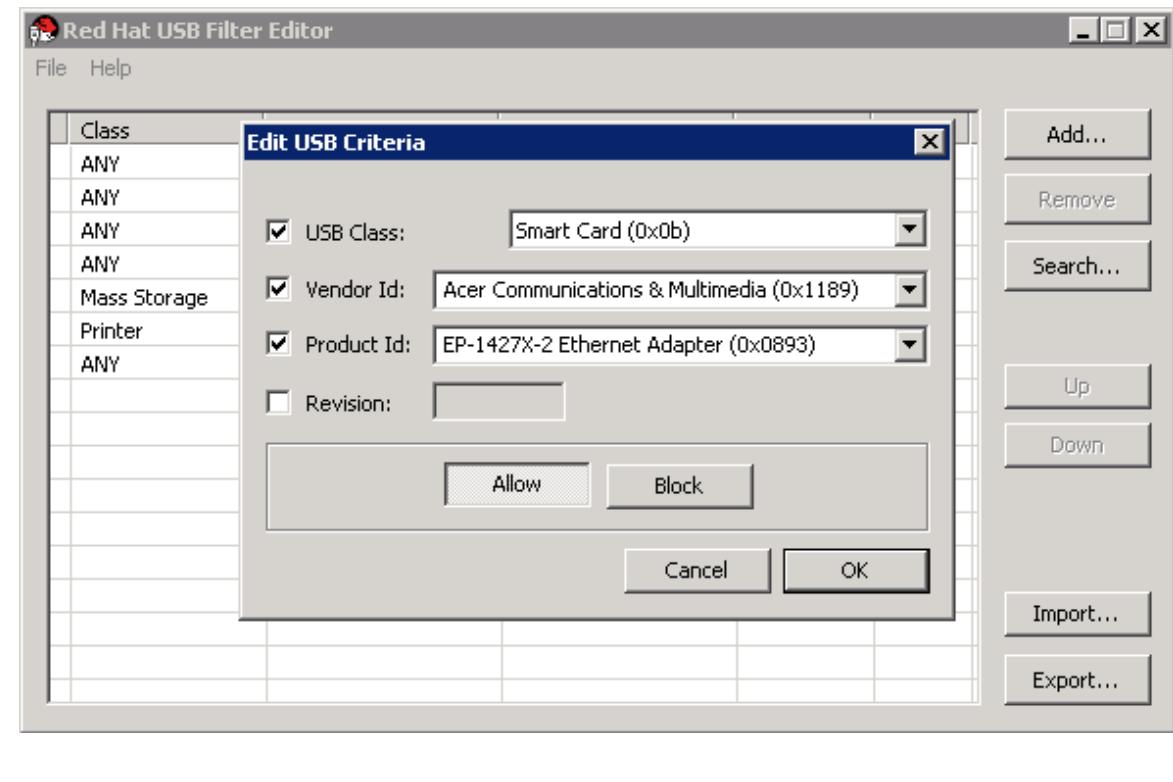
手順

1. Add をクリックします。
2. USB Class、Vendor ID、Product ID、および Revision チェックボックスおよびリストを使用して、デバイスを指定します。
Allow ボタンをクリックして、仮想マシンによる USB デバイスの使用を許可します。Block ボタンをクリックして、仮想マシンの USB デバイスを禁止します。

OK をクリックすると、選択したフィルタールールがリストに追加され、ウィンドウが閉じます。

例3.17 デバイスの追加

以下は、メーカーの Acer Communications & Multimedia から許可されたデバイスのリストに、USB クラス Smartcard、デバイス EP-1427X-2 Ethernet Adapter を追加する方法の例です。



- File → Save をクリックして、変更を保存します。

USB Filter Editor に USB ポリシーが追加されました。USB フィルター ポリシーを有効にするには、USB フィルター ポリシーを Red Hat Virtualization Manager にエクスポートする必要があります。

関連情報

- [USB ポリシーのエクスポート](#)

3.9.3.4. USB ポリシーの削除

デスクトップの USB Filter Editor ショートカットアイコンをダブルクリックします。これにより、エディターが開きます。

手順

- 削除するポリシーを選択します。
- Remove をクリックします。ポリシーを削除することを確認するメッセージが表示されます。
- Yes をクリックして、ポリシーを削除することを確認します。
- File → Save をクリックして、変更を保存します。

これで、USB フィルターエディターから USB ポリシーが削除されました。USB フィルター ポリシーを有効にするには、USB フィルター ポリシーを Red Hat Virtualization Manager にエクスポートする必要があります。

関連情報

- [USB ポリシーのエクスポート](#)

3.9.3.5. USB デバイスピリシーの検索

接続されている USB デバイスを検索して、USB フィルターエディターで許可またはブロックします。

デスクトップの USB Filter Editor ショートカットアイコンをダブルクリックします。これにより、エディターが開きます。

手順

1. **Search** をクリックします。Attached USB Devices ウィンドウには、接続されているすべてのデバイスのリストが表示されます。
2. デバイスを選択し、必要に応じて **Allow** または **Block** をクリックします。選択したデバイスをダブルクリックして、ウィンドウを閉じます。デバイスのポリシールールがリストに追加されます。
3. **Up** ボタンと **Down** ボタンを使用して、リスト内の新しいポリシールールの位置を変更します。
4. **File → Save** をクリックして、変更を保存します。

接続されている USB デバイスを検索しました。USB フィルターポリシーを有効にするには、Red Hat Virtualization Manager にエクスポートする必要があります。

3.9.3.6. USB ポリシーのエクスポート

更新されたポリシーを有効にするには、USB デバイスピリシーの変更をエクスポートして Red Hat Virtualization Manager にアップロードする必要があります。ポリシーをアップロードし、ovirt-engine サービスを再起動します。

デスクトップの USB Filter Editor ショートカットアイコンをダブルクリックします。これにより、エディターが開きます。

手順

1. **Export** をクリックします。Save As ウィンドウが開きます。
2. ファイル名を **usbfilter.txt** として保存してください。
3. WinSCP などのセキュアコピークライアントを使用して、**usbfilter.txt** ファイルを Red Hat Virtualization Manager を実行しているサーバーにアップロードします。ファイルは、サーバー上の /etc/ovirt-engine/ ディレクトリーに配置する必要があります。
4. Red Hat Virtualization Manager を実行しているサーバーで **root** ユーザーとして、ovirt-engine サービスを再起動します。

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

3.9.3.7. USB ポリシーのインポート

編集する前に、既存の USB デバイスピリシーをダウンロードして USB フィルターエディターにインポートする必要があります。

手順

1. WinSCP などの Secure Copy クライアントを使用して、Red Hat Virtualization Manager を実行しているサーバーから `usbfilter.txt` ファイルをダウンロードします。このファイルは、サーバー上の `/etc/ovirt-engine/` ディレクトリーにあります。
2. デスクトップの USB Filter Editor ショートカットアイコンをダブルクリックします。これにより、エディターが開きます。
3. Import をクリックします。これにより、Open 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。

3.9.4. イメージ不一致ツール

3.9.4.1. イメージ不一致ツールを使用したスナップショットの状態の監視

RHV Image Discrepancies ツールは、ストレージドメインと RHV データベースのイメージデータを分析します。ボリュームとボリューム属性に不一致が見つかった場合は警告しますが、それらの不一致は修正されません。このツールは、次のようなさまざまなシナリオで使用します。

- バージョンをアップグレードする前に、壊れたボリュームまたはチェーンを新しいバージョンに引き継がないようにします。
- ストレージ操作に失敗した後、不良状態のボリュームまたは属性を検出します。
- バックアップから RHV データベースまたはストレージを復元した後に使用します。
- 定期的に、問題が悪化する前に潜在的な問題を検出します。
- スナップショットまたはライブストレージの移行に関連する問題を分析し、これらのタイプの問題を修正した後、システムの状態を確認します。

前提条件

- 必要なバージョン。このツールは、`rhv-log-collector-analyzer-0.2.15-0.el7ev` の RHV バージョン 4.3.8 で導入されました。
- データ収集は異なる場所で同時に実行され、アトミックではないため、ストレージドメインを変更する可能性のある環境内のすべてのアクティビティーを停止する。つまり、スナップショットの作成や削除、ディスクの編集、移動、作成、削除は行わないでください。行った場合、不一致の誤検出が発生する可能性があります。プロセス中、仮想マシンは正常に動作し続けることができます。

手順

1. ツールを実行するには、RHV Manager で次のコマンドを入力します。


```
# rhv-image-discrepancies
```
2. ツールが不一致を検出したら、再実行して結果を確認します。ツールの実行中に一部の操作が実行された可能性がある場合、特に注意が必要です。



注記

このツールには Export および ISO ストレージドメインが含まれており、そのストレージドメインの不一致が報告される可能性があります。報告された場合、これらのストレージドメインは RHV データベースにはこれらのストレージドメインのイメージエントリーがないため、無視できます。

結果について

このツールは以下を報告します。

- ストレージに表示されているがデータベースにはないボリュームがある場合、またはデータベースに表示されているがストレージにはないボリュームがある場合
- 一部のボリューム属性がストレージとデータベースで異なる場合

出力サンプル

```
Checking storage domain c277ad93-0973-43d9-a0ca-22199bc8e801
Looking for missing images...
No missing images found
Checking discrepancies between SD/DB attributes...
image ef325650-4b39-43cf-9e00-62b9f7659020 has a different attribute capacity on
storage(2696984576) and on DB(2696986624)
image 852613ce-79ee-4adc-a56a-ea650dc4cfa has a different attribute capacity on
storage(5424252928) and on DB(5424254976)

Checking storage domain c64637b4-f0e8-408c-b8af-6a52946113e2
Looking for missing images...
No missing images found
Checking discrepancies between SD/DB attributes...
No discrepancies found
```

3.9.5. ログコレクターツール

3.9.5.1. ログコレクター

ログ収集ツールは、Red Hat Virtualization Manager に含まれています。サポートを要求する際に、このツールを使用して Red Hat Virtualization 環境全体から関連するログを簡単に収集できます。

ログ収集コマンドは、**ovirt-log-collector** です。root ユーザーとしてログインし、Red Hat Virtualization 環境の管理認証情報を提供する必要があります。**ovirt-log-collector -h** コマンドは、**ovirt-log-collector** コマンドのすべての有効オプションが記載されたリストを含む、使用状況に関する情報を表示します。

3.9.5.2. ovirt-log-collector コマンドの構文

ログコレクターコマンドの基本構文は以下の通りです。

```
# ovirt-log-collector options list all|clusters|datacenters
# ovirt-log-collector options collect
```

サポートされている 2 つの操作モードは、**list** と **collect** です。

- **list** パラメーターは、Red Hat Virtualization Manager に接続されているホスト、クラスター、またはデータセンターのいずれかをリストします。リストされたオブジェクトに基づいてログコレクションをフィルタリングできます。
- **collect** パラメーターは、Red Hat Virtualization Manager からのログを収集します。収集されたログは、/tmp/logcollector ディレクトリーの下のアーカイブファイルに配置されます。**ovirt-log-collector** コマンドは、各ログに特定のファイル名を割り当てます。

別のパラメーターが指定されていない限り、使用可能なホストを、それらが属するデータセンターおよびクラスターと一緒にリストすることがデフォルトのアクションとなります。特定のログを取得するために、ユーザー名とパスワードを入力するように求められます。

ovirt-log-collector コマンドをさらに改良するための多数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、プロンプトに戻ります。

-h、--help

コマンドの使用情報を表示し、プロンプトに戻ります。

--conf-file=PATH

ツールが使用する設定ファイルとして PATH を設定します。

--local-tmp=PATH

ログを保存するディレクトリーとして PATH を設定します。デフォルトのディレクトリーは /tmp/logcollector です。

--ticket-number=TICKET

SOS レポートに関連付けるチケット、またはケース番号として TICKET を設定します。

--upload=FTP_SERVER

取得したログを FTP で送信する際の送信先を FTP_SERVER に設定します。

Red Hat のサポート担当者から特に指示がない限り、このオプションは使用しないでください。

--log-file=PATH

コマンドがログ出力に使用する特定のファイル名として PATH を設定します。

--quiet

quiet モードを設定し、コンソール出力を最小限に抑えます。デフォルトでは、quiet モードはオフになっています。

-v、--verbose

verbose モードを設定し、より多くのコンソール出力を提供します。デフォルトでは、verbose モードはオフになっています。

--time-only

完全な SOS レポートを生成せずに、ホスト間の時差に関する情報のみを表示します。

Red Hat Virtualization Manager のオプション

ログコレクションをフィルタリングし、Red Hat Virtualization Manager の認証の詳細を指定するオプションです。

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 として指定し、ログコレクションをクラスター A および B の SalesHost ホストのみ

に制限します。

--no-hypervisors

ログコレクションから仮想化ホストを除外します。

--one-hypervisor-per-cluster

各クラスターから1台のホスト(存在する場合はSPM)のログを収集します。

-u USER、--user=USER

ログイン用のユーザー名を設定します。USERは、`user@domain`の形式で指定されます。ここで`user`はユーザー名で、`domain`は使用中のディレクトリーサービスドメインです。ユーザーはディレクトリーサービスに存在し、Red Hat Virtualization Managerに認識されている必要があります。

-r FQDN、--rhevm=FQDN

ログの収集元となるRed Hat Virtualization Managerの完全修飾ドメイン名を設定します。FQDNは、Managerの完全修飾ドメイン名に置き換えられます。ログコレクターは、Red Hat Virtualization Managerと同じローカルホストで実行していると想定されています。デフォルト値は`localhost`です。

-c CLUSTER、--cluster=CLUSTER

Red Hat Virtualization Managerからのログに加え、指定されたCLUSTER内の仮想化ホストからログを収集します。含めるクラスターは、クラスター名または一致パターンのコンマ区切りリストで指定する必要があります。

-d DATACENTER、--data-center=DATACENTER

Red Hat Virtualization Managerからのログに加え、指定されたDATACENTERの仮想化ホストからログを収集します。含めるデータセンターは、データセンター名または一致パターンのコンマ区切りリストで指定する必要があります。

-H HOSTS_LIST、--hosts=HOSTS_LIST

Red Hat Virtualization Managerからのログに加え、指定されたHOSTS_LIST内の仮想化ホストからログを収集します。含めるホストは、ホスト名、完全修飾ドメイン名、またはIPアドレスのコンマ区切りリストで指定する必要があります。一致パターンも有効です。

SSH 設定

--ssh-port=PORT

PORTを、仮想化ホストでのSSH接続に使用するポートとして設定します。

-k KEYFILE、--key-file=KEYFILE

仮想ホストへのアクセスに使用される公開SSHキーとしてKEYFILEを設定します。

--max-connections=MAX_CONNECTIONS

仮想化ホストからのログに対する最大同時SSH接続としてMAX_CONNECTIONSを設定します。デフォルトは10です。

PostgreSQL データベースのオプション

デフォルト値から変更されているデータベースユーザー名とデータベース名は、`pg-user`と`dbname`パラメーターを使用して指定する必要があります。

データベースがローカルホスト上にない場合は、`pg-dbhost`パラメーターを使用します。オプションの`pg-host-key`パラメーターを使用して、リモートログを収集します。リモートログ収集を成功させるには、PostgreSQL SOSプラグインをデータベースサーバーにインストールする必要があります。

--no-postgresql

データベースのコレクションを無効にします。--no-postgresql パラメーターが指定されていない限り、ログコレクターは Red Hat Virtualization Manager PostgreSQL データベースに接続し、データをログレポートに含めます。

--pg-user=USER

データベースサーバーとの接続に使用するユーザー名として USER を設定します。デフォルトは postgres です。

--pg-database=DBNAME

データベースサーバーへの接続に使用するデータベース名として DBNAME を設定します。デフォルトは rhevm です。

--pg-dbhost=DBHOST

データベースサーバーのホスト名として DBHOST を設定します。デフォルトは localhost です。

--pg-host-key=KEYFILE

データベースサーバーの公開 ID ファイル (秘密鍵) として、KEYFILE を設定します。この値はデフォルトでは設定されていません。データベースがローカルホストに存在しない場合にのみ必要です。

3.9.5.3. ログコレクターの基本的な使用法

追加のパラメーターを指定せずに **ovirt-log-collector** コマンドを実行すると、デフォルトの動作では、Red Hat Virtualization Manager とそれに接続されているホストからすべてのログが収集されます。また、--no-postgresql パラメーターを追加しない限り、データベースのログも収集します。次の例では、ログコレクターを実行して、Red Hat Virtualization Manager に接続されている 3 つのホストからすべてのログを収集します。

例3.18 ログコレクターの使用法

```
# ovirt-log-collector
INFO: Gathering oVirt Engine information...
INFO: Gathering PostgreSQL the oVirt Engine database and log files from localhost...
Please provide REST API password for the admin@internal oVirt Engine user (CTRL+D to abort):
About to collect information from 3 hypervisors. Continue? (Y/n):
INFO: Gathering information from selected hypervisors...
INFO: collecting information from 192.168.122.250
INFO: collecting information from 192.168.122.251
INFO: collecting information from 192.168.122.252
INFO: finished collecting information from 192.168.122.250
INFO: finished collecting information from 192.168.122.251
INFO: finished collecting information from 192.168.122.252
Creating compressed archive...
INFO Log files have been collected and placed in /tmp/logcollector/sosreport-rhn-account-20110804121320-ce2a.tar.xz.
The MD5 for this file is 6d741b78925998caff29020df2b2ce2a and its size is 26.7M
```

3.9.6. Engine Vacuum ツール

3.9.6.1. Engine Vacuum ツール

Engine Vacuum ツールを使用すると、テーブルを更新してデッド行を削除することで PostgreSQL データベースを維持し、ディスクスペースを再利用できます。VACUUM コマンドとそのパラメーターに関する詳細は、[PostgreSQL のドキュメント](#) を参照してください。

Engine Vacuum コマンドは **engine-vacuum** です。root ユーザーとしてログインし、Red Hat Virtualization 環境の管理認証情報を指定する必要があります。

また、**engine-setup** コマンドを使用しながら Engine Vacuum ツールを実行することで、既存のインストールをカスタマイズすることも可能です。

```
$ engine-setup
...
[ INFO ] Stage: Environment customization
...
Perform full vacuum on the engine database engine@localhost?
This operation may take a while depending on this setup health and the
configuration of the db vacuum process.
See https://www.postgresql.org/docs/12/static/sql-vacuum.html
(Yes, No) [No]:
```

Yes オプションは、Engine Vacuum ツールを Full Vacuum 詳細モードで実行します。

3.9.6.2. Engine Vacuum のモード

Engine Vacuum には 2 つのモードがあります。

標準バキューム

標準バキュームを頻繁に実行することをお勧めします。

標準バキュームは、テーブルとインデックスの不要な行バージョンを削除し、将来の再利用のためにスペースをマークします。頻繁に更新されるテーブルは、定期的にバキュームする必要があります。しかし、標準バキュームでは、そのスペースを OS に戻すことはできません。

標準バキュームにはパラメーターがなく、その時点でデータベース内にあるすべてのテーブルを処理します。

フルバキューム

フルバキュームの日常的な使用はお勧めしませんが、テーブル内から大量のスペースを再利用する必要がある場合にのみ実行する必要があります。

フルバキュームでは、デッドスペースのないテーブルファイルの新しいコピーを書き込むことでテーブルが圧縮され、オペレーティングシステムがスペースを再利用できるようになります。フルバキュームには時間がかかる場合があります。

フルバキュームでは、操作が完了して古いコピーが削除されるまで、テーブルの新しいコピー用に追加のディスクスペースが必要です。フルバキュームにはテーブルの排他的ロックが必要なため、テーブルの他の使用と並行して実行することはできません。

3.9.6.3. engine-vacuum コマンドの構文

engine-vacuum コマンドの基本構文は以下の通りです。

```
# engine-vacuum
# engine-vacuum option
```

engine-vacuum コマンドをオプションなしで実行すると、標準バキュームが実行されます。

engine-vacuum コマンドをさらに精緻化するためのいくつかのパラメーターがあります。

一般的なオプション

-h --help

engine-vacuum コマンドの使用方法に関する情報を表示します。

-a

標準バキュームを実行し、データベースを分析して、オプティマイザーの統計を更新します。

-A

バキューム処理を行わずに、データベースを解析し、オプティマイザーの統計情報を更新します。

-f

フルバキュームを実行します。

-v

詳細モードで実行して、より多くのコンソール出力を提供します。

-t table_name

特定の1つテーブルまたは複数のテーブルをバキュームします。

```
# engine-vacuum -f -v -t vm_dynamic -t vds_dynamic
```

3.9.7. VDSM からネットワーク名へのマッピングツール

3.9.7.1. VDSM 名を論理ネットワーク名にマッピング

論理ネットワークの名前が15文字を超えるか、非 ASCII 文字が含まれる場合、システムはホスト上の識別子 (`vds_name`) の名前を自動的に生成します。これは、`on` の文字とネットワークの一意の識別子における最初の13文字(例: `ona1b2c3d4e5f6g`)で構成されます。ホストのログファイルには、この名前が表示されます。論理ネットワーク名とその自動生成ネットワーク名の一覧を表示するには、`/usr/share/ovirt-engine/bin/` にある VDSM-to-Network-Name マッピングツールを使用します。

手順

- ツールを初めて実行するときは、PASSWORD 環境変数を定義します。これは、Manager データベースへの読み取り権限を持つデータベースユーザーのパスワードです。たとえば、以下を実行します。

```
# export PASSWORD=DatabaseUserPassword
```

- VDSM-to-Network-Name マッピングツールを実行します。

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

ここでの `USER` は、Manager データベースの読み取り権限を持つデータベースユーザーであり、そのパスワードは `PASSWORD` 環境変数に割り当てられています。

このツールは、同等のホスト上の識別子にマップされている論理ネットワーク名のリストを表示します。

その他のフラグ

以下のフラグを指定してツールを実行できます。

--host は、データベースサーバーのホスト名/IP アドレスです。デフォルト値は `localhost` です。

--port はデータベースサーバーのポート番号です。デフォルト値は **5432** です。--**database** はデータベースの名前です。デフォルト値は **engine** で、これは Manager データベースです。

--secure は、データベースとのセキュアな接続を有効にします。デフォルトでは、セキュアな接続なしでツールが実行されます。

第4章 環境に関する情報の収集

4.1. 監視および可観測性

この章では、Red Hat Virtualization システムからメトリクスとログを監視および取得するためのいくつかの方法を説明します。その方法には以下が含まれます。

- データウェアハウスと Grafana を使用して RHV を監視
- Elasticsearch のリモートインスタンスにメトリクスを送信
- Red Hat Virtualization Manager で Insight をデプロイ

4.1.1. データウェアハウスと Grafana を使用して RHV を監視

4.1.1.1. Grafana の概要

Grafana は、データベース名 **ovirt_engine_history** で oVirt Data Warehouse PostgreSQL データベースから収集されたデータに基づいてレポートを表示するのに使用される Web ベースの UI ツールです。使用可能なレポートダッシュボードの詳細は、[Grafana ダッシュボード](#) および [Grafana Web サイト - ダッシュボード](#) を参照してください。

Manager からのデータは毎分収集され、1時間ごとおよび1日ごとに集計されます。データは、エンジンセットアップ中にデータウェアハウス設定で定義されたスケール設定に従って保持されます（基本またはフルスケール）。

- **Basic** (デフォルト) : サンプルデータは 24 時間、毎時データは 1 カ月間保存します。日次データは保存されません。
- **Full** (推奨) - サンプルデータは 24 時間、毎時データは 2 カ月間、日次集計は 5 年間保持されます。

Full サンプルスケーリングの場合、別の仮想マシンへの Data Warehouse の移行が必要となる場合があります。

- Data Warehouse のスケーリングの手順については、[Data Warehouse サンプリングスケールの変更](#) を参照してください。
- Data Warehouse を別のマシンに移行するか、または別のマシンにインストールする手順については、[別のマシンへの Data Warehouse の移行](#) および [別のマシンへの Data Warehouse のインストールおよび設定](#) を参照してください。



注記

Data Warehouse データベース、Data Warehouse サービス、Grafana はそれぞれ別々のマシンにインストールできますが、Red Hat はこれらの各コンポーネントをすべて同じマシンにインストールする場合のみサポートします。

4.1.1.2. インストール

スタンドアロンマネージャーのインストールおよびセルフホスト型エンジンのインストールで Red Hat Virtualization Manager の **engine-setup** を実行すると、Grafana 統合がデフォルトで有効になり、インストールされます。



注記

Grafana はデフォルトではインストールされないため、以前のバージョンの RHV からのアップグレードの実行、バックアップの復元、Data Warehouse の別のマシンへの移行など、一部のシナリオでは手動でインストールする必要があります。

Grafana 統合を手動で有効にするには、以下を実行します。

1. 環境をグローバルメンテナンスモードに切り替えます。

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

2. Grafana をインストールするマシンにログインします。このマシンは、データウェアハウスが設定されているマシンと同じである必要があります（通常は Manager マシン）。

3. 次のように **engine-setup** コマンドを実行します。

```
# engine-setup --reconfigure-optional-components
```

4. **Yes** と回答して、このマシンに Grafana をインストールします。

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

5. グローバルメンテナンスモードを無効にします。

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

Grafana ダッシュボードにアクセスするには、以下を行います。

- <https://<engine FQDN or IP address>/ovirt-engine-grafana> にアクセスします。

または

- 管理ポータル の Web 管理ウェルカムページで **Monitoring Portal** をクリックします。

4.1.1.2.1. シングルサインオン用の Grafana の設定

Manager の engine-setup は、Manager の既存ユーザーが管理ポータルから SSO を使用してログインできるように Grafana を自動的に設定しますが、ユーザーを自動的に作成することはありません。新しいユーザーを作成（Grafana UI で **Invite**）し、新しいユーザーを確認すると、そのユーザーはログインできます。

1. まだ定義されていない場合は、Manager でユーザーの電子メールアドレスを設定します。
2. 既存の管理者ユーザー（最初に設定された管理者）で Grafana にログインします。
3. Configuration → Users に移動し、**Invite** を選択します。
4. メールアドレスおよび名前を入力し、Role を選択します。
5. 次のいずれかのオプションを使用して招待状を送信します。

- **Send invite mail** を選択し、**Submit** をクリックします。このオプションでは、Grafana マシンで設定された運用可能なローカルメールサーバーが必要です。

または

- **Pending Invites** を選択します。
 - 必要なエントリーを見つけます
 - **Copy invite** を選択します
 - このリンクをコピーして使用し、アカウントをブラウザーのアドレスバーに直接貼り付けるか、別のユーザーに送信してアカウントを作成します。

Pending Invites オプションを使用すると、電子メールは送信されません。つまり、実際にその電子メールアドレスが存在する必要はありません。Manager ユーザーの電子メールアドレスとして設定されている限り、有効なアドレスが機能します。

このアカウントでログインするには、以下を行います。

1. この電子メールアドレスを持つアカウントを使用して、Red Hat Virtualization Web 管理のウェルカムページにログインします。
2. **Monitoring Portal** を選択して、Grafana ダッシュボードを開きます。
3. **Sign in with oVirt Engine Auth** を選択します。

4.1.1.3. ビルトイン Grafana ダッシュボード

Grafana の初期設定では、データセンター、クラスター、ホスト、および仮想マシンのデータをレポートするために、次のダッシュボードを使用できます。

表4.1 ビルトイン Grafana ダッシュボード

| ダッシュボードタイプ | コンテンツ |
|------------|-------|
|------------|-------|

| ダッシュボードタイプ | コンテンツ |
|-------------------|--|
| Executive ダッシュボード | <ul style="list-style-type: none"> System ダッシュボード - 最新の設定に応じた、システム内のホストおよびストレージドメインのリソース使用量と稼働時間。 Data Center ダッシュボード - 最新の設定に応じた、選択したデータセンター内のクラスター、ホスト、およびストレージドメインのリソース使用量、ピーク、および稼働時間。 Cluster ダッシュボード - 最新の設定に応じた、選択したクラスター内のホストおよび仮想マシンのリソース使用量、ピーク、オーバーコミット、および稼働時間。 Host ダッシュボード - 選択した期間における選択したホストの最新および履歴の設定の詳細およびリソース使用状況のメトリクス。 Virtual Machine ダッシュボード - 選択した期間における選択した仮想マシンの最新および履歴の設定の詳細およびリソース使用状況のメトリクス。 Executive ダッシュボード - 選択した期間における、選択したデータセンター内のホストおよび仮想マシンのユーザーリソースの使用状況およびオペレーティングシステムの数。 |
| Inventory ダッシュボード | <ul style="list-style-type: none"> Inventory ダッシュボード - 最新の設定に応じた、選択したデータセンターのホスト、仮想マシン、実行中の仮想マシンの数、リソース使用量、オーバーコミット率。 Hosts Inventory ダッシュボード - 最新の設定に応じた FQDN、VDSM バージョン、オペレーティングシステム、CPU モデル、CPU コア、メモリーサイズ、作成日、削除日、および選択したホストのハードウェアの詳細。 Storage Domains Inventory ダッシュボード - 選択した期間における選択したストレージドメインのドメインタイプ、ストレージタイプ、使用可能なディスクサイズ、使用済みディスクサイズ、合計ディスクサイズ、作成日、および削除日。 Virtual Machines Inventory ダッシュボード - 最新の設定に従って、選択した仮想マシンのテンプレート名、オペレーティングシステム、CPU コア、メモリーサイズ、作成日、および削除日。 |

| ダッシュボードタイプ | コンテンツ |
|-----------------------|---|
| Service Level ダッシュボード | <ul style="list-style-type: none"> ● Uptime ダッシュボード - 選択した期間内の選択したクラスター内のすべての仮想マシンのホスト、高可用性仮想マシンの計画的ダウンタイム、計画外ダウンタイム、および合計時間。 ● Hosts Uptime ダッシュボード - 選択したホストの選択した期間における稼働時間、計画的ダウンタイム、および計画外ダウンタイム。 ● Virtual Machines Uptime ダッシュボード - 選択した期間における選択した仮想マシンの稼働時間、計画的なダウンタイム、および計画外のダウンタイム。 ● クラスターのサービス品質 <ul style="list-style-type: none"> ○ Hosts ダッシュボード - 選択したホストが、選択した期間に CPU およびメモリーのしきい値の上下で実行した時間。 ○ Virtual Machines ダッシュボード - 選択した仮想マシンが、選択した期間に CPU およびメモリーのしきい値の上下で実行した時間。 |
| Trend ダッシュボード | <ul style="list-style-type: none"> ● Trend ダッシュボード - 選択した期間における、選択したクラスター内のメモリーおよび CPU ごとの 5 つの最も使用率の高い仮想マシンおよび最も使用率の低い仮想マシンおよびホストの使用率。 ● Hosts Trend ダッシュボード - 選択した期間における選択したホストのリソース使用量(仮想マシン、CPU、メモリー、およびネットワーク Tx/Rx の数)。 ● Virtual Machines Trend ダッシュボード - 選択した期間における選択した仮想マシンのリソース使用量(CPU、メモリー、ネットワーク Tx/Rx、ディスク I/O)。 ● Hosts Resource Usage ダッシュボード - 選択した期間における選択したホストの日次および時間ごとのリソース使用量(仮想マシン、CPU、メモリー、ネットワーク Tx/Rx の数)。 ● Virtual Machines Resource Usage ダッシュボード - 選択した期間における選択した仮想マシンの日次および時間ごとのリソース使用量(CPU、メモリー、ネットワーク Tx/Rx、ディスク I/O)。 |



注記

Grafana ダッシュボードには、Red Hat Virtualization 管理ポータルへの直接リンクが含まれており、クラスター、ホスト、および仮想マシンの追加の詳細をすばやく表示できます。

4.1.1.4. カスタマイズされた Grafana ダッシュボード

レポートニーズに応じて、カスタマイズされたダッシュボードを作成したり、既存のダッシュボードをコピーして変更したりできます。



注記

ビルトインダッシュボードはカスタマイズできません。

4.1.2. Elasticsearch のリモートインスタンスにメトリックとログを送信



注記

Red Hat は Elasticsearch を所有または維持していません。このオプションをデプロイするには、Elasticsearch のセットアップとメンテナンスに精通している必要があります。

メトリクスデータおよびログを既存の Elasticsearch インスタンスに送信するように Red Hat Virtualization Manager およびホストを設定できます。

これを行うには、Manager とすべてのホストで **collectd** および **rsyslog** を設定する Ansible ロールを実行し、**engine.log**、**vdsd.log**、および **collectd** メトリックを収集して、それらを Elasticsearch インスタンスに送信します。

利用可能なメトリクススキーマに関する説明が記載された完全なリストを含め、詳細は [リモート Elasticsearch インスタンスへの RHV 監視データの送信](#) を参照してください。

4.1.2.1. collectd と rsyslog のインストール

collectd と **rsyslog** をホストにデプロイして、ログおよびメトリクスを収集します。



注記

新しいホストに対してこの手順を繰り返す必要はありません。追加されるすべての新しいホストは、ホストのデプロイ中に Elasticsearch にデータを送信するように、Manager により自動的に設定されます。

手順

1. SSH を使用して Manager マシンにログインします。
2. **/etc/ovirt-engine-metrics/config.yml.example** をコピーして **/etc/ovirt-engine-metrics/config.yml.d/config.yml** を作成します。

```
# cp /etc/ovirt-engine-metrics/config.yml.example /etc/ovirt-engine-metrics/config.yml.d/config.yml
```

3. **config.yml** の **ovirt_env_name** パラメーターと **elasticsearch_host** パラメーターを編集し、ファイルを保存します。次の追加パラメーターをファイルに追加できます。

```
use_omelasticsearch_cert: false
rsyslog_elasticsearch_usehttps_metrics: !!str off
rsyslog_elasticsearch_usehttps_logs: !!str off
```

- 証明書を使用する場合は、**use_omelasticsearch_cert** を **true** に設定します。
- ログまたはメトリクスを無効にするには、**rsyslog_elasticsearch_usehttps_metrics** と **rsyslog_elasticsearch_usehttps_logs** のいずれか1つ、または両方のパラメーターを使用します。

4. **collectd** と **rsyslog** をホストにデプロイします。

```
# /usr/share/ovirt-engine-metrics/setup/ansible/configure_ovirt_machines_for_metrics.sh
```

configure_ovirt_machines_for_metrics.sh スクリプトは、**linux-system-roles** ([Administration and configuration tasks using System Roles in RHEL](#) を参照) を含む Ansible ロールを実行し、これを使用してホストに **rsyslog** をデプロイおよび設定します。**rsyslog** は、**collectd** からメトリクスを収集し、Elasticsearch に送信します。

4.1.2.2. スキーマのログ記録およびログの分析

RHV から収集したデータをインタラクティブに探索できる Discover ページを使用します。収集された結果の各セットは、ドキュメントと呼ばれます。ドキュメントは、以下のログファイルから収集されます。

- engine.log** - すべての oVirt Engine UI のクラッシュ、Active Directory ルックアップ、データベースの問題、およびその他のイベントが含まれます。
- vdsd.log** - 仮想化ホスト上の Manager のエージェントである VDSM のログファイルであり、ホスト関連のイベントが含まれています。

次のフィールドを使用できます。

| パラメーター | description |
|----------|---|
| _id | ドキュメントの一意の ID |
| _index | ドキュメントが属するインデックスの ID。接頭辞として project.ovirt-logs が付いたインデックスは、Discover ページで関連する唯一のインデックスです。 |
| hostname | engine.log の場合、これは Manager のホスト名です。vdsd.log の場合、これはホストのホスト名です。 |
| level | ログレコードの重大度: TRACE、DEBUG、INFO、WARN、ERROR、FATAL。 |
| message | ドキュメントメッセージの本文。 |

| パラメーター | description |
|---------------------|---|
| ovirt.class | このログを生成した Java クラスの名前。 |
| ovirt.correlationid | engine.log の場合のみ。この ID は、Manager によって実行される単一のタスクの複数の部分を相互に関連付けるために使用されます。 |
| ovirt.thread | ログレコードが生成された Java スレッドの名前。 |
| tag | データのフィルタリングに使用できる事前定義されたメタデータのセット。 |
| @timestamp | レコードが発行された [time] (Troubleshooting#information-is-missing-from-kibana)。 |
| _score | 該当なし |
| _type | 該当なし |
| ipaddr4 | マシンの IP アドレス。 |
| ovirt.cluster_name | vdslog の場合のみ。ホストが所属するクラスターの名前。 |
| ovirt.engine_fqdn | マネージャーの FQDN。 |
| ovirt.module_lineno | ovirt.class で定義されたコマンドを実行したファイル内のファイルと行番号。 |

4.1.3. Insights のデプロイ

Red Hat Virtualization Manager がインストールされている既存の Red Hat Enterprise Linux (RHEL) システムに Red Hat Insights をデプロイするには、以下のタスクを実行します。

- Red Hat Insights アプリケーションにシステムを登録します。
- Red Hat Virtualization 環境からのデータ収集を有効にします。

4.1.3.1. システムを Red Hat Insights に登録します。

Red Hat Insights サービスと通信し、Red Hat Insights コンソールに表示される結果を表示するには、システムを登録します。

```
[root@server ~]# insights-client --register
```

4.1.3.2. Red Hat Virtualization 環境からのデータ収集を有効にする

`/etc/ovirt-engine/rhv-log-collector-analyzer/rhv-log-collector-analyzer.conf` ファイルを変更して、次の行を含めます。

```
upload-json=True
```

4.1.3.3. Insights の結果を Insights コンソールで確認

システムおよびインフラストラクチャーの結果は、[Insights コンソール](#) で確認できます。Overview タブには、インフラストラクチャーに対する現在のリスクのダッシュボードビューが表示されます。この開始点から、特定のルールがシステムにどのように影響しているかを調査したり、システムベースのアプローチを使用して、システムにリスクをもたらすすべてのルールの一覧を表示したりできます。

手順

1. Rule hits by severity を選択し、インフラストラクチャーにもたらす Total Risk でルールを表示します (Critical、Important、Moderate、または Low)。
または、以下を実行します。
 2. Rule hits by category を選択し、インフラストラクチャーにもたらすリスクの種類を表示します (Availability、Stability、Performance、または Security)。
 3. 特定のルールを名前で検索したり、ルールの一覧をスクロールして、Ansible Playbook のリスク、システム公開、および可用性に関するハイレベルな情報を確認して修正を自動化します。
 4. ルールをクリックして、ルールの説明を表示し、関連するナレッジベースの記事から詳細を確認し、影響を受けるシステムのリストを表示します。
 5. システムをクリックして、検出された問題に関する特定の情報と問題を解決するための手順を確認します。

4.2. ログファイル

4.2.1. Manager のインストールログファイル

表4.2 インストール

| ログファイル | 説明 |
|--|---|
| <code>/var/log/ovirt-engine/engine-cleanup-yyyy_mm_dd_ss.log</code> | engine-cleanup コマンドからログに記録します。これは、Red Hat Virtualization Manager のインストールをリセットするために使用されるコマンドです。コマンドが実行されるたびにログが生成されます。実行の日付と時刻は、複数のログの存在を許可するためにファイル名で使用されます。 |
| <code>/var/log/ovirt-engine/engine-db-install-yyyy_mm_dd_ss.log</code> | engine-setup コマンドから、engine データベースの作成および設定の詳細をログに記録します。 |

| ログファイル | 説明 |
|--|---|
| /var/log/ovirt-engine/ovirt-engine-dwh-setup-yyyy_mm_dd_hh_mm_ss.log | ovirt-engine-dwh-setup コマンドからログに記録します。これは、レポート用の ovirt_engine_history データベースを作成するのに使用されるコマンドです。コマンドが実行されるたびにログが生成されます。実行の日付と時刻は、複数のログが同時に存在できるようにするためにファイル名で使用されます。 |
| /var/log/ovirt-engine/setup/ovirt-engine-setup-yyyymmddhhmmss.log | engine-setup コマンドからログに記録します。コマンドが実行されるたびにログが生成されます。実行の日付と時刻は、複数のログが同時に存在できるようにするためにファイル名で使用されます。 |

4.2.2. Red Hat Virtualization Manager ログファイル

表4.3 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 | すべての Red Hat Virtualization Manager GUI クラッシュ、Active Directory ルックアップ、データベースの問題、およびその他のイベントを反映します。 |
| /var/log/ovirt-engine/host-deploy | Red Hat Virtualization Manager からデプロイされたホストのログファイル。 |
| /var/lib/ovirt-engine/setup-history.txt | Red Hat Virtualization Manager に関連付けられているパッケージのインストールおよびアップグレードを追跡します。 |
| /var/log/httpd/ovirt-requests-log | HTTPS 経由で Red Hat Virtualization Manager に行われたリクエストのログファイルで、各リクエストにかかった時間などが記録されています。

Correlation-Id ヘッダーが含まれているため、ログファイルを /var/log/ovirt-engine/engine.log と比較するときにリクエストを比較できます。 |
| /var/log/ovn-provider/ovirt-provider-ovn.log | OVN プロバイダーのアクティビティーをログに記録します。Open vSwitch のログに関する情報は、 Open vSwitch のドキュメント を参照してください。 |

4.2.3. SPICE ログファイル

SPICE のログファイルは、SPICE の接続に関する問題をトラブルシューティングする際に有用です。SPICE デバッグを開始するには、ログレベルを **debugging** に変更します。次に、ログの場所を特定します。

ゲストマシンへのアクセスに使用されるクライアントと、ゲストマシンに、SPICE ログファイルがあります。クライアント側のログにおいて、`console.vv` ファイルがダウンロードされているネイティブクライアントを使用して SPICE クライアントを起動した場合は、`remote-viewer` コマンドを使用してデバッグを有効にし、ログ出力を生成します。

4.2.3.1. ハイパーバイザー SPICE サーバーの SPICE ログ

表4.4 ハイパーバイザー SPICE サーバーの SPICE ログ

| ログタイプ | ログの場所 | ログレベルを変更する際の操作 |
|-------------------------|--|--|
| 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 <code>export SPICE_DEBUG_LEVEL=5</code> を実行します。この変数は QEMU によって解析され、システム全体で実行すると、システム上のすべての仮想マシンのデバッグ情報が出力されます。このコマンドは、クラスター内の各ホストで実行する必要があります。このコマンドは、各クラスターではなく、各ホスト/ハイパーバイザーにのみ機能します。 |

4.2.3.2. ゲストマシンの SPICE ログ

表4.5 ゲストマシンの `spice-vdagent` ログ

| ログタイプ | ログの場所 | ログレベルを変更する際の操作 |
|-------------|--|----------------|
| Windows ゲスト | C:\Windows\Temp\vdagent.log
C:\Windows\Temp\vdservice.log | 該当なし |

| ログタイプ | ログの場所 | ログレベルを変更する際の操作 |
|------------------------------|------------------------------------|---|
| Red Hat Enterprise Linux ゲスト | journalctl を root ユーザーとして使用 | <p>spice-vdagentd サービスをデバッグモードで実行するには、root ユーザーとして、SPICE_VDAGENTD_EXTRA_ARGS="-d -d" のエントリーで /etc/sysconfig/spice-vdagentd ファイルを作成します。</p> <p>デバッグモードで spice-vdagent を実行するには、コマンドラインで以下を実行します。</p> <pre>\$ killall - u \$USER spice-vdagent \$ spice-vdagent -x -d [-d] [& tee spice-vdagent.log]</pre> |

4.2.3.3. console.vv ファイルを使用して起動された SPICE クライアントの SPICE ログ

Linux クライアントマシンの場合:

1. **--spice-debug** オプションを指定して **remote-viewer** コマンドを実行し、SPICE デバッグを有効にします。プロンプトが表示されたら、接続 URL を入力します(例: `spice://virtual_machine_IP:port`)。

```
# remote-viewer --spice-debug
```

2. デバッグパラメーターを指定して SPICE クライアントを実行し、それに .vv ファイルを渡すには、**console.vv** ファイルをダウンロードし、**--spice-debug** オプションを指定して **remote-viewer** コマンドを実行し、**console.vv** ファイルへのフルパスを指定します。

```
# remote-viewer --spice-debug /path/to/console.vv
```

Windows クライアントマシンの場合:

1. **virt-viewer** 2.0-11.el7ev 以降のバージョンでは、**virt-viewer.msi** は **virt-viewer** と **debug-viewer.exe** をインストールします。
2. **spice-debug** 引数を指定して **remote-viewer** コマンドを実行し、コマンドをコンソールへのパスに送信します。

```
remote-viewer --spice-debug path\to\console.vv
```

3. ログを表示するには、仮想マシンに接続します。GDB を実行しているコマンドプロンプトが表示され、**remote-viewer** の標準出力および標準エラーが出力されます。

4.2.4. ホストログファイル

| ログファイル | 説明 |
|---|---|
| /var/log/messages | libvirt によって使用されるログファイル。 journalctl を使用してログを表示します。ログを表示するには、adm、systemd-journal、またはwheel グループのメンバーである必要があります。 |
| /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の詳細を示すログファイル。ホストがリースを取得、解放、更新、または更新に失敗したときのログの詳細。 |
| /var/log/vdsm/vdsm.log | 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 Manager にコピーされるホストデプロイメントログ。 |
| /var/log/vdsm/import/import-UUID-Date.log | KVM ホスト、VMWare プロバイダー、または RHEL 5 Xen ホストからの仮想マシンのインポートの詳細を示すログファイル(インポートの失敗情報を含む)。UUID は、インポートされた仮想マシンの UUID であり、Date はインポートが開始された日時です。 |
| /var/log/vdsm/supervdsm.log | スーパーユーザーパーミッションで実行された VDSM タスクをログに記録します。 |
| /var/log/vdsm/upgrade.log | VDSM は、ホストのアップグレード時にこのログファイルを使用して、設定の変更を記録します。 |
| /var/log/vdsm/mom.log | VDSM のメモリーオーバーコミットメントマネージャーのアクティビティーをログに記録します。 |

4.2.5. Red Hat Virtualization サービスのデバッグレベルのログの設定



注記

ロギングをデバッグレベルに設定すると、パスワードや内部 VM データなどの機密情報が公開される可能性があります。信頼できないユーザーまたは承認されていないユーザーがデバッグログにアクセスできることを確認してください。

各サービスの **sysconfig** ファイルを変更することにより、以下の Red Hat Virtualization (RHV) サービスのログをデバッグレベルに設定できます。

表4.6 RHV サービスと sysconfig ファイルパス

| サービス | ファイルパス |
|---|--|
| ovirt-engine.service | /etc/sysconfig/ovirt-engine |
| ovirt-engine-dwhd.service | /etc/sysconfig/ovirt-engine-dwhd |
| ovirt-fence-kdump-listener.service | /etc/sysconfig/ovirt-fence-kdump-listener |
| ovirt-websocket-proxy.service | /etc/sysconfig/ovirt-websocket-proxy |

この変更は、メインのサービスプロセスではなく、Python ラッパーによって実行されるロギングに影響します。

ロギングをデバッグレベルに設定すると、起動に関連する問題をデバッグするのに役立ちます。たとえば、Java ランタイムまたはライブラリーが見つからない、または正しくないためにメインプロセスを起動できない場合などです。

前提条件

- 変更する **sysconfig** ファイルが存在することを確認する。必要があれば作成します。

手順

- サービスの **sysconfig** ファイルに以下を追加します。

```
OVIRT_SERVICE_DEBUG=1
```

- サービスを再起動します。

```
# systemctl restart <service>
```

これで、サービスの **sysconfig** ログファイルがデバッグレベルに設定されました。

この設定によって発生したログはシステムログに記録されるため、生成されるログは、サービス固有のログファイルではなく、**/var/log/messages** にあるか、**journalctl** コマンドを使用して見つけることができます。

4.2.6. Red Hat Virtualization サービスの主な設定ファイル

sysconfig ファイルに加えて、これらの各 Red Hat Virtualization (RHV) サービスには、より頻繁に使用される別の設定ファイルがあります。

表4.7 RHV サービスと設定ファイル

| サービス | sysconfig ファイルパス | 主要な設定ファイル |
|-----------------------------|------------------------------------|---|
| ovirt-engine.service | /etc/sysconfig/ovirt-engine | /etc/ovirt-engine/engine.conf.d/*.conf |

| サービス | sysconfig ファイルパス | 主要な設定ファイル |
|---|--|---|
| <code>ovirt-engine-dwhd.service</code> | <code>/etc/sysconfig/ovirt-engine-dwhd</code> | <code>/etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/*.conf</code> |
| <code>ovirt-fence-kdump-listener.service</code> | <code>/etc/sysconfig/ovirt-fence-kdump-listener</code> | <code>/etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/*.conf</code> |
| <code>ovirt-websocket-proxy.service</code> | <code>/etc/sysconfig/ovirt-websocket-proxy</code> | <code>/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/*.conf</code> |

4.2.7. ホストロギングサーバーのセットアップ

ホストはログファイルを生成および更新し、その動作や問題点を記録しています。これらのログファイルを一元的に収集すると、デバッグが簡素化されます。

この手順は、集中ログサーバーで使用する必要があります。別のロギングサーバーを使用するか、この手順を使用して Red Hat Virtualization Manager でホストロギングを有効にできます。

手順

1. ファイアウォールが **UDP 514** ポートでのトラフィックを許可し、**syslog** サービストラフィックに対してオーブンであるかどうかを確認します。

```
# firewall-cmd --query-service=syslog
```

出力が **no** の場合は、**UDP 514** ポートで次のトラフィックを許可します。

```
# firewall-cmd --add-service=syslog --permanent
# firewall-cmd --reload
```

2. **syslog** サーバーに新しい **.conf** ファイル (例: `/etc/rsyslog.d/from_remote.conf`) を作成し、次の行を追加します。

```
template(name="DynFile" type="string"
        string="/var/log/%HOSTNAME%/%PROGRAMNAME%.log")
RuleSet(name="RemoteMachine"){ action(type="omfile" dynaFile="DynFile") }
Module(load="imudp")
Input(type="imudp" port="514" ruleset="RemoteMachine")
```

3. **rsyslog** サービスを再起動します。

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

4. ハイパーバイザにログインし、`/etc/rsyslog.conf` に以下の行を追加します。

```
*.info;mail.none;authpriv.none;cron.none @<syslog-FQDN>:514
```

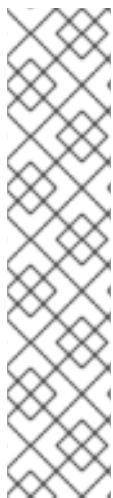
5. ハイパーバイザで **rsyslog** サービスを再起動します。

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

これで、集中ログサーバーは、仮想化ホストから `messages` ログおよび `secure` ログを受け取って保存するように設定されました。

4.2.8. SyslogHandler で RHV Manager ログをリモート syslog サーバーに渡すための設定

この実装では、JBoss EAP SyslogHandler ログマネージャーを使用し、`engine.log` および `server.log` から syslog サーバーにログレコードを渡すことができます。



注記

RHV 4.4.10 より前の RHV バージョンは、**ovirt-engine-extension-logger-log4j** により提供される同様の機能を備えていました。そのパッケージは RHV 4.4.10 で削除され、JBoss EAP SyslogHandler ログマネージャーを使用した新しい実装に置き換えられました。以前の RHV バージョンで **ovirt-engine-extension-logger-log4j** を使用していた場合は、RHV 4.4.10 にアップグレードした後、次の手順を実行します。

- この章に記載されているガイドラインを使用して、リモート syslog サーバーへのログレコードの送信を手動で設定します。
- **ovirt-engine-extension-logger-log4j** 設定ファイルを手動で削除します (`/etc/ovirt-engine/extensions.d/Log4jLogger.properties` 設定ファイルを削除します)。

中央の syslog ログサーバーでこの手順を使用します。別のログサーバーを使用するか、この手順を使用して、`engine.log` ファイルと `server.log` ファイルを Manager から syslog サーバーに渡すことができます。設定方法については、[ホストロギングサーバーの設定](#) も参照してください。

SyslogHandler 実装の設定

1. `/etc/ovirt-engine/engine.conf.d` ディレクトリーに設定ファイル **90-syslog.conf** を作成し、次のコンテンツを追加します。

```
SYSLOG_HANDLER_ENABLED=true
SYSLOG_HANDLER_SERVER_HOSTNAME=localhost
SYSLOG_HANDLER_FACILITY=USER_LEVEL
```

2. **rsyslog** をインストールして設定します。

```
# dnf install rsyslog
```

3. **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
```

4. 設定ファイル `/etc/rsyslog.d/rhvm.conf` を作成し、次のコンテンツを追加します。

```
user.* /var/log/jboss.log
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")
```

5. rsyslog サービスを再起動します。

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

6. ファイアウォールが有効でアクティブな場合は、次のコマンドを実行して、**Firewalld** で **rsyslog** ポートを開くために必要なルールを追加します。

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

7. Red Hat Virtualization Manager を再起動します。

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

これで、syslog サーバーは **engine.log** ファイルを受け取って保存できるようになります。

付録A VDSM サービスとフック

VDSM サービスは、Red Hat Virtualization Hosts (RHVH) および Red Hat Enterprise Linux ホストを管理するために Red Hat Virtualization Manager が使用します。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を管理および監視します。また、仮想マシンの作成、統計収集、ログ収集、およびその他のホスト管理タスクを調整します。VDSM は、Red Hat Virtualization Manager により管理される各ホスト上でデーモンとして実行されます。クライアントからの XML-RPC 呼び出しに応答します。Red Hat Virtualization Manager は VDSM クライアントとして機能します。

VDSM はフックを介して拡張可能です。フックは、重要なイベントが発生したときにホスト上で実行されるスクリプトです。サポートされ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/` にある実行可能フックスクリプトを英数字順に実行します。慣例により、各フックスクリプトには、ファイル名の前に含まれる 2 衔の番号が割り当てられ、スクリプトが実行される順序が明確になります。任意のプログラミング言語でフックスクリプトを作成できますが、この章に含まれる例では Python が使用されます。

イベントのホストで定義されたすべてのスクリプトが実行されることに注意してください。特定のフックをホスト上で実行される仮想マシンのサブセットに対してのみ実行する必要がある場合は、仮想マシンに関連付けられた **カスタムプロパティー** を評価することにより、フックスクリプト自体がこの要件を処理することを確認する必要があります。



警告

VDSM フックは Red Hat Virtualization の動作に干渉する可能性があります。VDSM フックのバグは、仮想マシンのクラッシュやデータの損失を引き起こす可能性があります。VDSM フックは注意して実装し、厳密にテストする必要があります。Hooks API は新しく、将来大幅に変更される可能性があります。

イベント駆動型フックを使用して VDSM を拡張できます。フックを使用して VDSM を拡張することは実験的な技術であり、この章は経験豊富な開発者を対象としています。

仮想マシンにカスタムプロパティーを設定することで、フックスクリプトに仮想マシン固有のパラメーターを追加で渡すことができます。

A.1. VDSM フックのインストール

デフォルトでは、VDSM フックはインストールされていません。特定のフックが必要な場合は、手動でインストールする必要があります。

前提条件

- ホストリポジトリを有効にします。
- root パーミッションでホストにログインしている。

手順

- 利用可能なフックのリストを取得します。

```
# dnf list vdsml*hook\*
```

-
- 2. ホストをメンテナンスモードにします。
- 3. 目的の VDSM フックパッケージをホストにインストールします。

```
# dnf install <vdsm-hook-name>
```

たとえば、**vdsm-hook-vhostmd** パッケージをホストにインストールするには、次のように入力します。

```
# dnf install vdsm-hook-vhostmd
```

- 4. ホストを再起動します。

関連情報

- [Red Hat Virtualization Host のリポジトリの有効化](#)
- [Red Hat Enterprise Linux ホストのリポジトリの有効化](#)

A.2. 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 | 仮想マシンの起動前。 |
| after_vm_start | 仮想マシンの起動後。 |
| before_vm_cont | 仮想マシンが続行する前。 |
| after_vm_cont | 仮想マシンが続行した後。 |
| before_vm_pause | 仮想マシンが一時停止する前。 |
| after_vm_pause | 仮想マシンが一時停止した後。 |
| before_vm_hibernate | 仮想マシンが休止状態になる前。 |
| after_vm_hibernate | 仮想マシンが休止状態になった後。 |
| before_vm_dehibernate | 仮想マシンが休止状態でなくなる前。 |
| after_vm_dehibernate | 仮想マシンが休止状態ではなくなった後。 |
| before_vm_migrate_source | 仮想マシンを移行する前に、移行が行われている移行元ホストで実行します。 |

| 名前 | 説明 |
|-------------------------------|---|
| after_vm_migrate_source | 仮想マシンの移行後、移行が行われている移行元ホストで実行します。 |
| before_vm_migrate_destination | 仮想マシンを移行する前に、移行が行われている移行先ホストで実行します。 |
| after_vm_migrate_destination | 仮想マシンの移行後、移行が行われている移行先ホストで実行します。 |
| after_vm_destroy | 仮想マシンの破棄後。 |
| before_vdsm_start | VDSM がホストで開始される前。 before_vdsm_start フックはユーザー root として実行され、VDSM プロセスの環境を継承しません。 |
| after_vdsm_stop | VDSM がホストで停止した後。 after_vdsm_stop フックはユーザー root として実行され、VDSM プロセスの環境を継承しません。 |
| before_nic_hotplug | NIC が仮想マシンにホットプラグされる前。 |
| after_nic_hotplug | NIC が仮想マシンにホットプラグされた後。 |
| before_nic_hotunplug | NIC が仮想マシンからホットアンプラグされる前。 |
| after_nic_hotunplug | NIC が仮想マシンからホットアンプラグされた後。 |
| 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 | NIC が仮想マシンからの 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。 |

| 名前 | 説明 |
|-----------------------------------|------------------------------------|
| after_disk_hotunplug_fail | 仮想マシンからのディスクのほっと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 | デバイスを移行する前に、移行が行われている宛先ホストで実行します。 |
| after_device_migrate_destination | デバイスの移行後、移行が行われている移行先ホストで実行します。 |
| before_device_migrate_source | デバイスを移行する前に、移行が行われている移行元ホストで実行します。 |
| after_device_migrate_source | デバイスの移行後、移行が行われている移行元ホストで実行します。 |
| after_network_setup | ホストマシンの起動時にネットワークを設定した後。 |
| before_network_setup | ホストマシンを起動するときにネットワークを設定する前。 |

A.3. VDSM フック環境

ほとんどのフックスクリプトは `vdsm` ユーザーとして実行され、VDSM プロセスの環境を継承します。例外は、`before_vdsm_start` イベントと `after_vdsm_stop` イベントによってトリガーされるフックスクリプトです。これらのイベントによってトリガーされるフックスクリプトは `root` ユーザーとして実行され、VDSM プロセスの環境を継承しません。

A.4. VDSM フックドメイン XML オブジェクト

VDSM は [libvirt domain XML format](#) を使用して仮想マシンを定義します。仮想マシンの UUID は、ドメイン XML から推測できますが、環境変数 **vmlid** としても使用できます。

フックスクリプトが開始されると、**_hook_domxml** 変数が環境に追加されます。この変数には、関連する仮想マシンの libvirt ドメイン XML 表現のパスが含まれています。

一部のフックは、この規則の例外です。次のフックには、仮想マシンではなく、NIC の XML 表現が含まれています。

- ***_nic_hotplug_***
- ***_nic_hotunplug_***
- **_update_device**
- **_device_create**
- ***_device_migrate_***



重要

before_migration_destination および **before_dehibernation** フックは現在、ソースホストからドメイン XML を受信しています。宛先のドメイン XML は異なります。

A.5. カスタムプロパティーの定義

Red Hat Virtualization Manager によって受け入れられ(次にカスタムフックに渡される)カスタムプロパティーは、**engine-config** コマンドを使用して定義されます。このコマンドは、Red Hat Virtualization Manager がインストールされているホストで **root** ユーザーとして実行します。

UserDefinedVMProperties および **CustomDeviceProperties** 設定キーは、サポートされているカスタムプロパティーの名前を格納するために使用されます。名前付きの各カスタムプロパティーの有効な値を定義する正規表現も、これらの設定キーに含まれています。

複数のカスタムプロパティーはセミコロンで区切られます。設定キーを設定すると、そこに含まれている既存の値が上書きされることに注意してください。新規および既存のカスタムプロパティーを組み合わせる場合は、キーの値を設定するために使用されるコマンドのすべてのカスタムプロパティーを含める必要があります。

設定キーが更新されたら、新しい値を有効にするために **ovirt-engine** サービスを再起動する必要があります。

例A.1 仮想マシンのプロパティー -smartcard カスタムプロパティーの定義

1. 次のコマンドを使用して、**UserDefinedVMProperties** 設定キーによって定義された既存のカスタムプロパティーを確認します。

```
# engine-config -g UserDefinedVMProperties
```

以下の出力が示すように、カスタムプロパティー **memory** が既に定義されています。正規表現 **^[0-9]+\$** は、カスタムプロパティーに数字のみが含まれるようにします。

```
# engine-config -g UserDefinedVMProperties
UserDefinedVMProperties: version: 4.3
UserDefinedVMProperties: version: 4.4
```

```
UserDefinedVMProperties : memory=^[0-9]+$ version: 4.4
```

2. **memory** カスタムプロパティーは **UserDefinedVMProperties** 設定キーすでに定義されているため、新しいカスタムプロパティーを追加する必要があります。追加のカスタムプロパティーである **smartcard** が、設定キーの値に追加されます。新しいカスタムプロパティーは、**true** または **false** の値を保持できます。

```
# engine-config -s UserDefinedVMProperties='memory=^[0-9]+$;smartcard=^(true|false)$' --cver=4.4
```

3. **UserDefinedVMProperties** 設定キーで定義されたカスタムプロパティーが正しく更新されていることを確認します。

```
# engine-config -g UserDefinedVMProperties
UserDefinedVMProperties: version: 4.3
UserDefinedVMProperties: version: 4.4
UserDefinedVMProperties : memory=^[0-9]+$;smartcard=^(true|false)$ version: 4.4
```

4. 最後に、設定の変更を有効にするには、**ovirt-engine** サービスを再起動する必要があります。

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

例A.2 デバイスプロパティー - **interface** カスタムプロパティーの定義

1. 次のコマンドを使用して、**CustomDeviceProperties** 設定キーで定義されている既存のカスタムプロパティーを確認します。

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

以下の出力に示されるように、カスタムプロパティーはまだ定義されていません。

```
# engine-config -g CustomDeviceProperties
CustomDeviceProperties: version: 4.3
CustomDeviceProperties: version: 4.4
```

2. **interface** カスタムプロパティーはまだ存在しないため、そのまま追加できます。この例では、**speed** サブプロパティーの値は 0 - 99999 の範囲に設定され、**duplex** サブプロパティーの値は **full** または **half** のいずれかに設定されます。

```
# engine-config -s CustomDeviceProperties="{type=interface;prop={speed=^([0-9]{1,5});duplex=^(full|half)}}" --cver=4.4
```

3. **CustomDeviceProperties** 設定キーで定義されたカスタムプロパティーが正しく更新されていることを確認します。

```
# engine-config -g CustomDeviceProperties
UserDefinedVMProperties: version: 4.3
UserDefinedVMProperties: version: 4.4
UserDefinedVMProperties : {type=interface;prop={speed=^([0-9]{1,5});duplex=^(full|half)}} version: 4.4
```

4. 最後に、設定の変更を有効にするには、`ovirt-engine` サービスを再起動する必要があります。

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

A.6. 仮想マシンのカスタムプロパティーの設定

Red Hat Virtualization Manager でカスタムプロパティーを定義したら、仮想マシンでの設定を開始できます。カスタムプロパティーは、管理ポータルの **New Virtual Machine** ウィンドウおよび**Edit Virtual Machine** ウィンドウの **Custom Properties** タブで設定されます。

Run Virtual Machine(s) ダイアログボックスからカスタムプロパティーを設定することもできます。**Run Virtual Machine(s)** ダイアログボックスから設定されたカスタムプロパティーは、次にシャットダウンされるまで仮想マシンにのみ適用されます。

Custom Properties タブには、定義済みのカスタムプロパティーのリストから選択するための機能があります。カスタムプロパティーキーを選択すると、追加のフィールドが表示され、そのキーの値を入力できます。+ ボタンをクリックしてキーと値のペアを追加し、- ボタンをクリックしてそれらを削除します。

A.7. VDSM フックでの仮想マシンのカスタムプロパティーの評価

仮想マシンの **Custom Properties** フィールドに設定された各キーは、フックスクリプトを呼び出すときに環境変数として追加されます。**Custom Properties** フィールドの検証に使用される正規表現を使用することである程度保護されますが、期待どおりに入力されているかをスクリプトで検証する必要もあります。

例A.3 カスタムプロパティーの評価

この短い Python の例は、カスタムプロパティー **key1** の存在を確認します。カスタムプロパティーが設定されている場合は、その値が標準エラーに出力されます。カスタムプロパティーが設定されていないと、アクションは実行されません。

```
#!/usr/bin/python

import os
import sys

if os.environ.has_key('key1'):
    sys.stderr.write('key1 value was : %s\n' % os.environ['key1'])
else:
    sys.exit(0)
```

A.8. VDSM フックモジュールの使用

VDSM には Python フックモジュールが付属しており、VDSM フックスクリプトのヘルパー関数を提供します。このモジュールは例として提供されており、Python で記述された VDSM フックにのみ関連しています。

フックモジュールは、仮想マシンの libvirt XML の DOM オブジェクトへの読み込みをサポートします。フックスクリプトは、Python のビルトイン [xml.dom ライブラリー](#) を使用してオブジェクトを操作できます。

変更されたオブジェクトは、フックモジュールを使用して libvirt XML に保存できます。フックモジュールは、フック開発をサポートするために次の機能を提供します。

表A.2 フックモジュール機能

| 名前 | 引数 | 説明 |
|---------------------|------------|--|
| tobool | 文字列 | 文字列 "true" または "false" 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込みます |
| write_domxml | DOM オブジェクト | DOM オブジェクトから仮想マシンの libvirt XML を書き込みます |

A.9. VDSM フックの実行

`before_vm_start` スクリプトは、ドメイン XML を編集して、仮想マシンが libvirt に到達する前に仮想マシンの VDSM 定義を変更できます。その際には注意が必要です。フックスクリプトは VDSM の動作を混乱させる可能性があり、バグのあるスクリプトは Red Hat Virtualization 環境の停止につながる可能性があります。特に、ドメインの UUID は変更しないでください。また、十分な背景知識がない限り、ドメインからデバイスを削除しないでください。

`before_vds_start` と `after_vds_stop` の両方のフックスクリプトが `root` ユーザーとして実行されます。システムへの `root` アクセスを必要とする他のフックスクリプトは、権限昇格に `sudo` コマンドを使用するように作成する必要があります。これをサポートするには、`/etc/sudoers` を更新して、`vds` ユーザーがパスワードを再入力せずに `sudo` を使用できるようにする必要があります。これは、フックスクリプトが非対話的に実行されるために必要です。

例A.4 VDSM フックの sudo の設定

この例では、`sudo` コマンドは、`vds` ユーザーが `root` として `/bin/chown` コマンドを実行できるように設定されます。

1. `root` として仮想化ホストにログインします。
2. テキストエディターで `/etc/sudoers` ファイルを開きます。
3. 次の行をファイルに追加します。

```
vds ALL=(ALL) NOPASSWD: /bin/chown
```

これは、`vds` 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ことを指定します。`NOPASSWD` パラメーターは、ユーザーが `sudo` を呼び出すときにパスワードの入力を求められないことを示しています。

この設定変更が行われると、VDSM フックは `sudo` コマンドを使用して `/bin/chown` を `root` として実行できるようになります。この Python コードは、`sudo` を使用して、ファイル `/my_file` の `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ストリームは、VDSM のログに収集されます。この情報は、フックスクリプトをデバッグするのに使用されます。

A.10. VDSM フックの戻りコード

フックスクリプトは、[フックリターンコード](#) に示すリターンコードのいずれかを返す必要があります。戻りコードは、さらにフックスクリプトが VDSM によって処理されるかどうかを判別します。

表A.3 フックリターンコード

| コード | 説明 |
|-----|--------------------------------------|
| 0 | フックスクリプトは正常に終了しました |
| 1 | フックスクリプトが失敗しました。他のフックを処理する必要があります |
| 2 | フックスクリプトが失敗しました。これ以上フックを処理する必要はありません |
| >2 | 予約済み |

A.11. VDSM フックの例

このセクションで提供されているフックスクリプトの例は、Red Hat では厳密にはサポートされていません。ソースにかかわらず、システムにインストールするすべてのフックスクリプトは、環境に対して徹底的にテストされているか確認する必要があります。

例A.5 NUMA ノードのチューニング

目的:

このフックスクリプトを使用すると、**numaset** カスタムプロパティに基づいて NUMA ホストのメモリー割り当てを調整できます。カスタムプロパティーが設定されていない場合、アクションは実行されません。

設定文字列:

```
numaset=^(interleave|strict|preferred):[^]?\\d+(-\\d+)?(,[^]?\\d+(-\\d+)?)*$
```

使用される正規表現により、特定の仮想マシンの **numaset** カスタムプロパティーで、割り当てモード (**interleave**、**strict**、**preferred**) と使用するノードの両方を指定できます。2つの値はコロン (:) で区切られます。正規表現を使用すると、**nodeset** を次のように指定できます。

- 特定のノード (**numaset=strict:1** はノード 1のみの使用を指定)、または
- 使用するノードの範囲 (**numaset=strict:1-4** はノード 1から 4 の使用を指定)、または

- 使用しない特定のノード (**numaset = strict: ^ 3** はノード 3 を使用しないことを指定)、または
- 上記の組み合わせをコンマ区切りで指定 (**numaset=strict:1-4,6** はノード 1 から 4、および 6 の使用を指定)。

スクリプト:

```
/usr/libexec/vdsd/hooks/before_vm_start/50_numa
```

```
#!/usr/bin/python

import os
import sys
import hooking
import traceback

"""
numa hook
=====
add numa support for domain xml:

<numatune>
  <memory mode="strict" nodeset="1-4,^3" />
</numatune>

memory=interleave|strict|preferred

numaset="1" (use one NUMA node)
numaset="1-4" (use 1-4 NUMA nodes)
numaset="^3" (don't use NUMA node 3)
numaset="1-4,^3,6" (or combinations)

syntax:
  numa=strict:1-4
  """

if os.environ.has_key('numa'):
    try:
        mode, nodeset = os.environ['numa'].split(':')

        domxml = hooking.read_domxml()

        domain = domxml.getElementsByTagName('domain')[0]
        numas = domxml.getElementsByTagName('numatune')

        if not len(numas) > 0:
            numatune = domxml.createElement('numatune')
            domain.appendChild(numatune)

            memory = domxml.createElement('memory')
            memory.setAttribute('mode', mode)
            memory.setAttribute('nodeset', nodeset)
            numatune.appendChild(memory)

        hooking.write_domxml(domxml)
```

```
else:  
    sys.stderr.write('numa: numa already exists in domain xml')  
    sys.exit(2)  
except:  
    sys.stderr.write('numa: [unexpected error]: %s\n' % traceback.format_exc())  
    sys.exit(2)
```

付録B カスタムネットワークプロパティー

B.1. BRIDGE_OPTS パラメーターの説明

表B.1 bridge_opts パラメーター

| パラメーター | 説明 |
|--------------------------------|---|
| forward_delay | ブリッジがリスニング状態とラーニング状態で費やす時間をデシ秒単位で設定します。この時点でスイッチングループが検出されない場合、ブリッジは転送状態になります。これにより、通常のネットワーク操作の前に、ネットワークのトラフィックおよびレイアウトを検査する時間ができます。 |
| group_addr | 一般的な問い合わせを行う場合は、この値をゼロに設定します。グループ固有およびグループおよびソース固有のクエリーを送信するには、この値を IP アドレスではなく 6 バイトの MAC アドレスに設定します。許可される値は、 01:80:C2:00:00:0x (01:80:C2:00:00:01 、 01:80:C2:00:00:02 、 01:80:C2:00:00:03 を除く) です。 |
| group_fwd_mask | ブリッジがリンクローカルグループアドレスを転送できるようにします。この値をデフォルトから変更すると、非標準のブリッジ動作が可能になります。 |
| hash_max | ハッシュテーブルのバケット数の最大値。これはすぐに有効になり、現在のマルチキャストグループエントリーの数より少ない値に設定することはできません。値は 2 の累乗でなければなりません。 |
| hello_time | 'hello' メッセージを送信してからネットワークトポロジー内のブリッジの位置を通知するまでの時間間隔をデシ秒単位で設定します。このブリッジが Spanning Tree ルートブリッジである場合にのみ適用されます。 |
| max_age | 他のルートブリッジから 'hello' メッセージを受け取ってから、そのブリッジがデッドとなったとみなされ、引き継ぎが開始されるまでの最大時間をデシ秒単位で設定します。 |
| multicast_last_member_count | ホストから 'leave group' メッセージを受け取った後、マルチキャストグループに送信する 'last member' クエリーの回数を設定します。 |
| multicast_last_member_interval | 'last member' クエリーの間隔をデシ秒単位で設定します。 |

| パラメーター | 説明 |
|-------------------------------|---|
| multicast_membership_interval | ブリッジがホストへのマルチキャストトラフィックの送信を停止する前に、ブリッジがマルチキャストグループのメンバーからの応答を待機する時間をデシ秒単位で設定します。 |
| multicast_querier | ブリッジがマルチキャストクエリーをアクティブに実行するかどうかを設定します。ブリッジが他のネットワークホストから'マルチキャストホストメンバーシップクエリー'を受信すると、そのホストはクエリーを受け取った時刻にマルチキャストクエリー間隔を加えた時間に基づいて追跡されます。ブリッジが後でそのマルチキャストメンバーシップのトラフィックを転送しようとした場合、またはクエリーを実行しているマルチキャストルーターと通信している場合は、このタイマーはクエリーアの有効性を確認します。有効な場合、マルチキャストトラフィックは、ブリッジの既存のマルチキャストメンバーシップテーブルを介して配信されます。有効でなくなると、トラフィックはすべてのブリッジポートを介して送信されます。マルチキャストメンバーシップを持つ、またはマルチキャストメンバーシップを期待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させるために少なくとも1つのマルチキャストクエリーアを実行する必要があります。 |
| multicast_querier_interval | ホストから受け取った最後の'マルチキャストホストメンバーシップ'クエリー間の最大間隔をデシ秒単位で設定して、それがまだ有効であることを確認します。 |
| multicast_query_use_ifaddr | ブール値。デフォルトは'0'です。この場合、クエリーアはIPv4メッセージの送信元アドレスとして0.0.0.0を使用します。これを変更すると、ブリッジIPが送信元アドレスとして設定されます。 |
| multicast_query_interval | マルチキャストメンバーシップの有効性を確保するために、ブリッジによって送信されるクエリーメッセージ間の時間をデシ秒単位で設定します。このとき、またはブリッジがそのメンバーシップのマルチキャストクエリーを送信するように要求された場合、ブリッジは、チェックが要求された時間とmulticast_query_intervalに基づいて、自身のマルチキャストクエリーアの状態をチェックします。このメンバーシップのマルチキャストクエリーが最後のmulticast_query_interval内に送信された場合、それは再度送信されません。 |

| パラメーター | 説明 |
|-----------------------------------|--|
| multicast_query_response_interval | 送信されたクエリーにホストが応答できる時間の長さ(デシ秒)。multicast_query_interval の値以下である必要があります。 |
| multicast_router | マルチキャストルーターが接続されているポートの有効/無効を設定します。1つ以上のマルチキャストルーターを備えたポートは、すべてのマルチキャストトラフィックを受信します。値0は完全に無効になり、値1はシステムがクエリーに基づいてルーターの存在を自動的に検出できるようにし、値2はポートが常にすべてのマルチキャストトラフィックを受信できるようにします。 |
| multicast_snooping | スヌーピングの有効/無効を切り替えます。スヌーピングを使用すると、ブリッジはルーターとホスト間のネットワークトラフィックをリッスンして、適切なリンクへのマルチキャストトラフィックをフィルタリングするためのマップを維持できます。このオプションを使用すると、ユーザーは、ハッシュの競合によって自動的に無効になった場合にスヌーピングを再度有効にできます。ハッシュの競合が解決されていない場合は、再度有効にしないでください。 |
| multicast_startup_query_count | メンバーシップ情報を決定するために起動時に送信されるクエリーの数を設定します。 |
| multicast_startup_query_interval | メンバーシップ情報を決定するために起動時に送信されるクエリー間の時間をデシ秒単位で設定します。 |

B.2. RED HAT VIRTUALIZATION MANAGER を使用するように RED HAT VIRTUALIZATION MANAGER を設定する方法

管理ポータルから、ホストネットワークインターフェイスカードの ethtool プロパティーを設定できます。`ethtool_opts` キーはデフォルトでは使用できないため、エンジン設定ツールを使用して Manager に追加する必要があります。ホストに必要な VDSM フックパッケージもインストールする必要があります。

ethtool_opts キーの Manager への追加

- Manager で以下のコマンドを実行してキーを追加します。

```
# engine-config -s UserDefinedNetworkCustomProperties=ethtool_opts=.* --cver=4.4
```

2. **ovirt-engine** サービスを再起動します。

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

3. ethtool プロパティーを設定するホストに、VDSM フックパッケージをインストールします。Red Hat Virtualization Host ではこのパッケージがデフォルトで利用可能ですが、Red Hat Enterprise Linux ホストにインストールする必要があります。

```
# dnf install vdsm-hook-ethtool-options
```

`ethtool_opts` キーが管理ポータルで利用できるようになりました。ethtool プロパティーを論理ネットワークに適用するには、[ホストネットワークインターフェイスの編集、およびホストへの論理ネットワークの割り当て](#) を参照してください。

B.3. FCOE を使用するように RED HAT VIRTUALIZATION MANAGER を設定する方法

管理ポータルから、ホストネットワークインターフェイスカードの Fibre Channel over Ethernet (FCoE) プロパティーを設定できます。`fcoe` キーはデフォルトでは使用できないため、エンジン設定ツールを使用して Manager に追加する必要があります。次のコマンドを実行して、`fcoe` がすでに有効になっているかどうかを確認できます。

```
# engine-config -g UserDefinedNetworkCustomProperties
```

ホストに必要な VDSM フックパッケージもインストールする必要があります。ホストの FCoE カードによっては、特別な設定が必要になる場合もあります。[Red Hat Enterprise Linux ストレージデバイスの管理](#) の [Fibre Channel over Ethernet の設定](#) を参照してください。

手順

1. Manager で以下のコマンドを実行してキーを追加します。

```
# engine-config -s UserDefinedNetworkCustomProperties='fcoe=^((enable|dcb|auto_vlan)=(yes|no),?)*$'
```

2. `ovirt-engine` サービスを再起動します。

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

3. FCoE プロパティーを設定する各 Red Hat Enterprise Linux ホストに VDSM フックパッケージをインストールします。Red Hat Virtualization Host (RHVH) では、デフォルトでパッケージが利用可能です。

```
# dnf install vdsm-hook-fcoe
```

`fcoe` キーが管理ポータルで使用できるようになりました。FCoE プロパティーを論理ネットワークに適用するには、[ホストネットワークインターフェイスの編集、およびホストへの論理ネットワークの割り当て](#) を参照してください。

付録C RED HAT VIRTUALIZATION ユーザーインターフェイスプラグイン

C.1. RED HAT VIRTUALIZATION ユーザーインターフェイスプラグインについて

Red Hat Virtualization は、非標準の機能を公開するプラグインをサポートしています。これにより、Red Hat Virtualization 管理ポータルを使用して他のシステムと統合することが容易になります。各インターフェイスプラグインは、Red Hat Virtualization で使用するためにパッケージ化および配布できるユーザーインターフェイス拡張機能のセットを表します。

Red Hat Virtualization のユーザーインターフェイスプラグインは、JavaScript プログラミング言語を使用して、クライアント上で直接管理ポータルと統合されます。プラグインは管理ポータルにより呼び出され、Web ブラウザーの JavaScript ランタイムで実行されます。ユーザーインターフェイスプラグインは、JavaScript 言語とそのライブラリーを使用できます。

実行時の主要なイベントで、管理ポータルは、管理ポータルからプラグインへの通信を表すイベントハンドラー関数を介して個々のプラグインを呼び出します。管理ポータルは複数のイベントハンドラー関数をサポートしていますが、プラグインはその実装に関係する関数のみを宣言します。各プラグインは、プラグインを管理ポータルで使用する前に、関連するイベントハンドラー関数をプラグインブートストラップシーケンスの一部として登録する必要があります。

ユーザーインターフェイス拡張機能を駆動するプラグインから管理ポータルへの通信を容易にするために、管理ポータルはプラグイン API を個々のプラグインが使用できるグローバル（トップレベル）の pluginApi JavaScript オブジェクトとして公開します。各プラグインは個別の pluginApi インスタンスを取得し、管理ポータルがプラグインのライフサイクルに関して各プラグインのプラグイン API 関数の呼び出しを制御できるようにします。

C.2. RED HAT VIRTUALIZATION ユーザーインターフェイスプラグインのライフサイクル

ユーザーインターフェイスプラグインの基本的なライフサイクルは、3つのステージに分けられます。

- プラグインの検出。
- プラグインの読み込み。
- プラグインのブートストラップ。

C.2.1. Red Hat Virtualization ユーザーインターフェイスプラグインの検出

プラグイン記述子の作成は、プラグイン検出プロセスの最初のステップです。プラグイン記述子には、重要なプラグインメタデータと、オプションでデフォルトのプラグイン固有の設定が含まれています。

管理ポータルの HTML ページ要求 (**HTTP GET**) の処理の一部として、ユーザーインターフェイスプラグインインフラストラクチャーは、ローカルファイルシステムからプラグイン記述子を検出してロードしようとします。インフラストラクチャーは、プラグイン記述子ごとにデフォルトプラグイン固有の設定（存在する場合）をオーバーライドし、それに対応する、プラグイン実行時の動作を微調整するために使用されるプラグインユーザー設定もロードしようとします。プラグインのユーザー設定は任意です。記述子と対応するユーザー設定ファイルをロードした後、oVirt Engine はユーザーインターフェイスプラグインデータを集約し、ランタイム評価のために管理ポータルの HTML ページに埋め込みます。

デフォルトでは、プラグイン記述子は \$ENGINEUSR/ui-plug-ins にあり、oVirt Engine ローカル設定

で定義されている `ENGINE_USR=/usr/share/ovirt-engine` のデフォルトマッピングがあります。プラグイン記述子は JSON 形式の仕様に準拠することが期待されていますが、プラグイン記述子では、JSON 形式の仕様に加えて (* と // の両方の) Java/C++ スタイルのコメントを使用できます。

デフォルトでは、プラグインユーザー設定ファイルは `$ENGINE_ETC/ui-plug-ins` にあり、oVirt Engine ローカル設定で定義されている `ENGINE_ETC=/etc/ovirt-engine` のデフォルトマッピングがあります。プラグインのユーザー設定ファイルは、プラグイン記述子と同じコンテンツ形式の規則に準拠する必要があります。



注記

プラグインのユーザー設定ファイルは、通常、`<descriptorFileName>-config.json` の命名規則に従います。

C.2.2. Red Hat Virtualization ユーザインターフェイスプラグインのロード

プラグインが検出され、そのデータが管理ポータルの HTML ページに埋め込まれた後、管理ポータルは、アプリケーションの起動の一部としてプラグインを読み込もうとします（アプリケーションの起動の一部として読み込まれないように設定した場合を除く）。

検出されたプラグインごとに、管理ポータルはホストページの読み込みに使用される HTML iframe 要素を作成します。プラグインホストページは、プラグインブートストラッププロセスを開始するために必要です。このプロセス（ブートストラッププロセス）は、プラグインの iframe 要素のコンテキストでプラグインコードを評価するために使用されます。ユーザーインターフェイスプラグインインフラストラクチャーは、ローカルファイルシステムからのプラグインリソースファイル（プラグインホストページなど）の提供をサポートします。プラグインホストページが iframe 要素に読み込まれ、プラグインコードが評価されます。プラグインコードが評価された後、プラグインはプラグイン API を使用して管理ポータルと通信します。

C.2.3. Red Hat Virtualization ユーザインターフェイスプラグインのブートストラップ

一般的なプラグインブートストラップシーケンスは、次の手順で構成されます。

プラグインブートストラップシーケンス

1. 指定されたプラグインの `pluginApi` インスタンスを取得します。
2. ランタイムプラグイン設定オブジェクトを取得します（オプション）。
3. 関連するイベントハンドラー関数を登録します。
4. UI プラグインインフラストラクチャーにプラグインの初期化を進めるよう通知します。

次のコードスニペットは、上記の手順を実際に示しています。

```
// 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({
    // UilInit event handler function.
    UilInit: function() {
        // Handle UilInit event.
        window.alert('Favorite music band is ' + config.band);
    }
});

// Notify UI plug-in infrastructure to proceed with plug-in initialization.
api.ready();

```

C.3. ユーザーインターフェイスプラグイン関連のファイルとその場所

表C.1 UI プラグイン関連のファイルとその場所

| ファイル | 場所 | 備考 |
|---------------------|---|--|
| プラグイン記述子ファイル（メタデータ） | /usr/share/ovirt-engine/ui-plugins/my-plugin.json | |
| プラグインユーザー設定ファイル | /etc/ovirt-engine/ui-plugins/my-plugin-config.json | |
| プラグインリソースファイル | /usr/share/ovirt-engine/ui-plugins/<resourcePath>/PluginHostPage.html | <resourcePath>は、プラグイン記述子の対応する属性によって定義されます。 |

C.4. ユーザーインターフェイスプラグインのデプロイメント例

次の手順に従って、Hello World! を実行するユーザーインターフェイスプラグインを作成します。Red Hat Virtualization Manager 管理ポータルにサインインするときにプログラムします。

Hello World! プラグインのデプロイ

- Manager の /usr/share/ovirt-engine/ui-plugins/helloWorld.json で次のファイルを作成し、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"
}
```

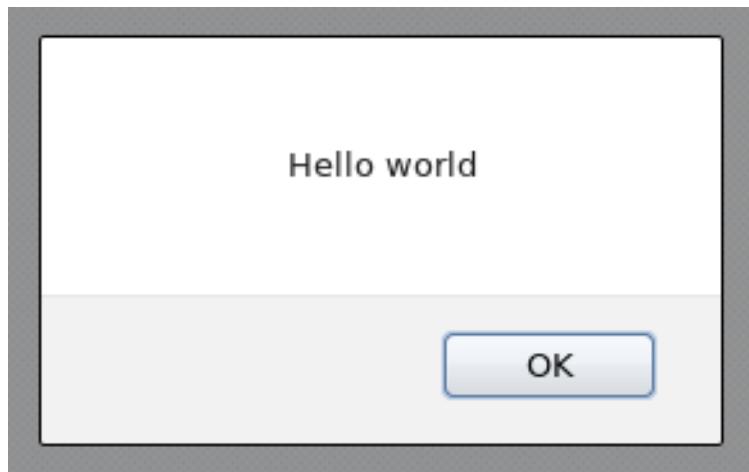
- Manager の /usr/share/ovirt-engine/ui-plugins/hello-files/start.html で次のファイルを作成し、プラグインホストページを作成します。

```
<!DOCTYPE html><html><head>
<script>
```

```
var api = parent.pluginApi('HelloWorld');
api.register({
  Uilnit: function() { window.alert('Hello world'); }
});
api.ready();
</script>
</head><body></body></html>
```

Hello World! プラグインが正常に実装されている場合は、管理ポータルにログインすると、この画面が表示されます。

図C.1 Hello World! の実装の成功プラグイン



付録D RED HAT VIRTUALIZATION での FIPS の有効化

連邦情報処理標準 (FIPS)、特に FIPS140-2 に準拠するように Red Hat Virtualization を設定できます。組織の FIPS コンプライアンス要件に基づいて、特定の仮想マシン、ベアメタルマシン、または環境全体で FIPS モードを選択的に有効にできます。

FIPS モードのオペレーティングシステムをインストールするか、またはオペレーティングシステムのインストール後にシステムを FIPS モードに切り替えることで、FIPS 対応のベアメタルマシンを RHV 4.4 で作成できます。ただし、システムの競合が発生しないように、Red Hat Virtualization をインストールして設定する前に FIPS モードに切り替える必要があります。



重要

Red Hat は、後で FIPS モードを有効にするのではなく、FIPS モードを有効にして RHEL 8 をインストールすることを推奨しています。インストール時に FIPS モードを有効にすると、システムは FIPS で承認されるアルゴリズムと継続的な監視テストですべてのキーを生成するようになります。

FIPS は、まず各ベアメタルマシン上で有効にし、次に Manager で有効にします。

- [セルフホスト型エンジンでの FIPS の有効化](#)
- [RHEL ホストとスタンドアロン Manager での FIPS の有効化](#)

D.1. セルフホスト型エンジンでの FIPS の有効化

コマンドラインを使用すると、デプロイ中にセルフホスト型エンジンで FIPS を有効にできます。

手順

1. セルフホスト型エンジンのデプロイメントスクリプトを開始します。コマンドラインを使用してセルフホスト型エンジンとして Red Hat Virtualization をインストール を参照してください。
2. デプロイメントスクリプトで **Do you want to enable FIPS?** と尋ねられた場合は、**Yes** と入力します。

検証

ホストでコマンド **fips-mode-setup --check** を入力して、FIPS が有効になっていることを確認します。コマンドは、**FIPS mode is enabled** を返すはずです。

```
# fips-mode-setup --check
FIPS mode is enabled.
```

D.2. RHV ホストおよびスタンドアロン MANAGER での FIPS の有効化

Red Hat Enterprise Linux (RHEL) ホストまたは Red Hat Virtualization Host (RHVH) のインストール時に、FIPS モードを有効にできます。詳細は、Red Hat Enterprise Linux 8 の [セキュリティー強化 ガイド](#) の [FIPS モードを有効化して RHEL 8 をインストール](#) を参照してください。Red Hat は、プロビジョニングされたホストまたは Manager マシンの FIPS モードへの切り替えをサポートしていません。

検証

ホストでコマンド **fips-mode-setup --check** を入力して、FIPS が有効になっていることを確認します。コマンドは、**FIPS mode is enabled** を返すはずです。

```
# fips-mode-setup --check  
FIPS mode is enabled.
```

D.3. 関連情報

- Red Hat Virtualization ホストのインストール
- Configuring and Applying SCAP Policies During Installation
- Installers and Images for Red Hat Virtualization Manager (v.4.4 for x86_64)
- Security policies available in the SCAP Security Guide
- Red Hat Enterprise Linux 8 の [セキュリティー強化](#)

付録E RED HAT VIRTUALIZATION と暗号化された通信

E.1. RED HAT VIRTUALIZATION MANAGER CA 証明書の置き換え

HTTPS 経由で Red Hat Virtualization Manager に接続するユーザーを認証するように、組織のサードパーティ CA 証明書を設定できます。

Manager とホスト間の認証、または [ディスク転送 URL](#) には、サードパーティの CA 証明書は使用されません。これらの HTTPS 接続は、Manager によって生成された自己署名証明書を使用します。



重要

カスタム HTTPS 証明書に切り替える場合は、独自の CA 証明書ディストリビューションを使用して、その証明書をクライアントで利用可能にする必要があります。

Red Hat Satellite と統合する場合は、正しい証明書を Satellite に手動でインポートする必要があります。

CA から秘密鍵と証明書を P12 ファイルで受け取った場合は、次の手順を使用してそれらを抽出します。他のファイル形式については、CA にお問い合わせください。秘密鍵と証明書を抽出した後、[Red Hat Virtualization Manager Apache CA 証明書の置き換え](#) に進みます。

E.1.1. P12 バンドルからの証明書および秘密鍵の抽出

内部 CA は、内部で生成されたキーおよび証明書を `/etc/pki/ovirt-engine/keys/apache.p12` の P12 ファイルに保存します。新しいファイルを同じ場所に保存します。以下の手順では、新しい P12 ファイルが `/tmp/apache.p12` にあると仮定しています。



警告

`/etc/pki` ディレクトリーまたはサブディレクトリーのパーミッションと所有権を変更しないでください。`/etc/pki` および `/etc/pki/ovirt-engine` ディレクトリーのパーミッションは、デフォルトの **755** のままにする必要があります。

手順

- 現在の `apache.p12` ファイルをバックアップします。

```
# cp -p /etc/pki/ovirt-engine/keys/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12.bck
```

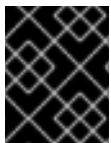
- 現在のファイルを新しいファイルに置き換えます。

```
# cp /tmp/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

- 秘密鍵と証明書を必要な場所に抽出します。

```
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nocerts -nodes >
/tmp/apache.key
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nokeys > /tmp/apache.cer
```

ファイルがパスワードで保護されている場合は、コマンドに **-passin pass: password** を追加し、**password** を必要なパスワードに置き換えます。



重要

Red Hat Virtualization の新規インストールでは、この手順のすべてのステップを完了する必要があります。

E.1.2. Red Hat Virtualization Manager の Apache CA 証明書の置き換え

HTTPS 経由で管理ポータルおよび VM ポータルに接続するユーザーを認証するように、組織のサードパーティ CA 証明書を設定します。



警告

/etc/pki ディレクトリーまたはサブディレクトリーのパーミッションと所有権を変更しないでください。**/etc/pki** および **/etc/pki/ovirt-engine** ディレクトリーのパーミッションは、デフォルトの **755** のままにする必要があります。

前提条件

- サードパーティの CA (認証局) 証明書。PEM ファイルとして提供されます。証明書チェーンは、ルート証明書まで完全である必要があります。チェーンの順序は重要であり、最後の中間証明書からルート証明書まででなければなりません。この手順は、サードパーティの CA 証明書が **/tmp/3rd-party-ca-cert.pem** で提供されていることを前提としています。
- Apache httpd に使用する秘密鍵。パスワードを含めることはできません。この手順では、**/tmp/apache.key** にあることを前提としています。
- CA によって発行された証明書。この手順では、**/tmp/apache.cer** にあることを前提としています。

手順

- セルフホスト型エンジンを使用している場合は、環境をグローバルメンテナンスモードにします。

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

詳細は、[セルフホスト型エンジンの更新](#) を参照してください。

- CA 証明書をホスト全体のトラストストアに追加します。

```
# cp /tmp/3rd-party-ca-cert.pem /etc/pki/ca-trust/source/anchors
# update-ca-trust
```

3. Manager は、**/etc/pki/ovirt-engine/ca.pem** にシンボリックリンクされている **/etc/pki/ovirt-engine/apache-ca.pem** を使用するように設定されています。シンボリックリンクを削除します。

```
# rm /etc/pki/ovirt-engine/apache-ca.pem
```

4. CA 証明書を **/etc/pki/ovirt-engine/apache-ca.pem** として保存します。

```
# cp /tmp/3rd-party-ca-cert.pem /etc/pki/ovirt-engine/apache-ca.pem
```

5. 既存の秘密鍵と証明書をバックアップします。

```
# cp /etc/pki/ovirt-engine/keys/apache.key.nopass /etc/pki/ovirt-engine/keys/apache.key.nopass.bck  
# cp /etc/pki/ovirt-engine/certs/apache.cer /etc/pki/ovirt-engine/certs/apache.cer.bck
```

6. 秘密鍵を必要な場所にコピーします。

```
# cp /tmp/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
```

7. 秘密鍵の所有者を root に設定し、パーミッションを **0640** に設定します。

```
# chown root:ovirt /etc/pki/ovirt-engine/keys/apache.key.nopass  
# chmod 640 /etc/pki/ovirt-engine/keys/apache.key.nopass
```

8. 証明書を必要な場所にコピーします。

```
# cp /tmp/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

9. 証明書の所有者を root に設定し、パーミッションを **0644** に設定します。

```
# chown root:ovirt /etc/pki/ovirt-engine/certs/apache.cer  
# chmod 644 /etc/pki/ovirt-engine/certs/apache.cer
```

10. Apache サーバーを再起動します。

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

11. 次のパラメーターを使用して、新しいトラストストア設定ファイル **/etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf** を作成します。

```
ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"  
ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

12. **/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf** ファイルをコピーし、10 より大きいインデックス番号 (たとえば、**99-setup.conf**) に名前を変更します。新しいファイルに以下のパラメーターを追加します。

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/certs/apache.cer  
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```

13. **websocket-proxy** サービスを再起動します。

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

14. **/etc/ovirt-provider-ovn/conf.d/10-setup-ovirt-provider-ovn.conf** ファイルを手動で変更した場合、または古いインストールの設定ファイルを使用している場合は、Manager がまだ、**/etc/pki/ovirt-engine/apache-ca.pem** を証明書ソースとして使用するように設定されていることを確認してください。

15. **/etc/ovirt-engine-backup/engine-backup-config.d** ディレクトリーを作成します。

```
# mkdir -p /etc/ovirt-engine-backup/engine-backup-config.d
```

16. 以下の内容で **/etc/ovirt-engine-backup/engine-backup-config.d/update-system-wide-pki.sh** ファイルを作成します。これにより、**ovirt-engine-backup** が復元時にシステムを自動的に更新できるようになります。

```
BACKUP_PATHS="${BACKUP_PATHS}
/etc/ovirt-engine-backup"
cp -f /etc/pki/ovirt-engine/apache-ca.pem \
/etc/pki/ca-trust/source/anchors/3rd-party-ca-cert.pem
update-ca-trust
```

17. **ovirt-provider-ovn** サービスを再起動します。

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

18. **ovirt-imageio** サービスを再起動します。

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

19. **ovirt-engine** サービスを再起動します。

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

20. セルフホスト型エンジンを使用している場合は、グローバルメンテナンスマードをオフにします。

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

ユーザーは、証明書の警告を表示することなく、管理ポータルと VM ポータルに接続できるようになりました。

E.2. MANAGER と LDAP サーバー間の暗号化通信の設定

Red Hat Virtualization Manager と LDAP サーバー間の暗号化された通信をセットアップするには、LDAP サーバーのルート CA 証明書を取得し、ルート CA 証明書を Manager にコピーして、PEM でエンコードされた CA 証明書を作成します。キーストアタイプは、Java でサポートされている任意のタイプになります。以下の手順では、Java KeyStore (JKS) 形式を使用します。



注記

PEM でエンコードされた CA 証明書の作成および証明書のインポートに関する詳細は、`/usr/share/doc/ovirt-engine-extension-aaa-ldap-<version>` にある README ファイルの **X.509 CERTIFICATE TRUST STORE** セクションを参照してください。



注記

ovirt-engine-extension-aaa-ldap は非推奨になりました。新規インストールの場合は、Red Hat Single Sign On を使用します。詳細は、[管理ガイド の Red Hat Single Sign-On のインストールおよび設定](#) を参照してください。

手順

- Red Hat Virtualization Manager で、LDAP サーバーの root CA 証明書を `/tmp` ディレクトリーにコピーし、**keytool** を使用して root CA 証明書をインポートして、PEM でエンコードされた CA 証明書を作成します。以下のコマンドは、`/tmp/myrootca.pem` の root CA 証明書をインポートし、`/etc/ovirt-engine/aaa/` の下に PEM でエンコードされた CA 証明書 `myrootca.jks` を作成します。証明書の場所とパスワードを書き留めます。インターラクティブセットアップツールを使用している場合は、これが必要なすべての情報です。LDAP サーバーを手動で設定している場合は、残りの手順に従って設定ファイルを更新してください。

```
$ keytool -importcert -noprompt -trustcacerts -alias myrootca -file /tmp/myrootca.pem -keystore /etc/ovirt-engine/aaa/myrootca.jks -storepass password
```

- `/etc/ovirt-engine/aaa/profile1.properties` ファイルを証明書情報で更新します。



注記

`${local:_basedir}` は、LDAP プロパティー設定ファイルが存在するディレクトリーであり、`/etc/ovirt-engine/aaa` ディレクトリーを指します。PEM でエンコードされた CA 証明書を別のディレクトリーに作成した場合は、 `${local:_basedir}` を証明書へのフルパスに置き換えます。

- startTLS (推奨) を使用するには、以下を行います。

```
# Create keystore, import certificate chain and uncomment
pool.default.ssl.startTLS = true
pool.default.ssl.truststore.file = ${local:_basedir}/myrootca.jks
pool.default.ssl.truststore.password = password
```

- SSL を使用するには、以下を行います。

```
# Create keystore, import certificate chain and uncomment
pool.default.serverset.single.port = 636
pool.default.ssl.enable = true
pool.default.ssl.truststore.file = ${local:_basedir}/myrootca.jks
pool.default.ssl.truststore.password = password
```

外部 LDAP プロバイダーの設定を続行するには、[外部 LDAP プロバイダーの設定](#) を参照してください。シングルサインオン用に LDAP および Kerberos の設定を続行するには、[シングルサインオン用の LDAP および Kerberos の設定](#) を参照してください。

E.3. FIPS の暗号化された VNC コンソールの有効化

暗号化された VNC コンソールをセットアップして、Red Hat Virtualization (RHV) Manager、および FIPS が有効になっているホストと連携することができます。

暗号化された VNC コンソールを設定するには、以下の手順を実行します。

- RHV での FIPS の有効化
- VNC 暗号化を有効化するためのクラスター設定
- 各ホストでの VNC SASL Ansible Playbook の実行
- Manager の CA 証明書を信頼するためのリモートビューアー設定

E.3.1. VNC 暗号化を有効化するためのクラスター設定

前提条件

- クラスターで FIPS が有効化されている。

手順

1. 管理ポータルで、Compute → Clusters をクリックします。
2. VNC 暗号化を有効にする予定のクラスターを選択し、Edit をクリックします。Edit Cluster ウィンドウが開きます。
3. Console タブを選択します。
4. Enable VNC Encryption チェックボックスを選択し、OK をクリックします。

E.3.2. ホストごとの VNC SASL Ansible Playbook の実行

手順

1. 管理ポータルで、FIPS 対応のホストをメンテナンスマードにします。
 - a. Compute → Hosts をクリックします。
 - b. Virtual Machines 列で、各ホストの仮想マシンがゼロであることを確認します。
必要に応じて、ライブマイグレーションを実行してホストから仮想マシンを削除します。[ホスト間での仮想マシンの移行](#) を参照してください。
 - c. 各ホストを選択し、Management → Maintenance および OK をクリックします。
2. Manager が実行されているマシンのコマンドラインに接続します。
 - スタンドアロン Manager の場合:


```
# ssh root@rhvm
```
 - セルフホスト型エンジンの場合: Compute → Virtual Machines の順にクリックし、デフォルトの名前が **HostedEngine** のセルフホスト型エンジンの仮想マシンを選択して、Console をクリックします。

- ホストごとに VNC SASL Ansible Playbook を実行します。

```
# cd /usr/share/ovirt-engine/ansible-runner-service-project/project/
# ansible-playbook --ask-pass --inventory=<hostname> ovirt-vnc-sasl.yml <1>
```

Compute → Hosts に表示される ホスト名 を指定します。

- ホストを選択し、Installation → Reinstall をクリックします。
- 再インストールしたら、ホストを選択し、Management → Restart をクリックします。
- 再起動したら、ホストを選択し、Management → Activate をクリックします。

VNC SASL Ansible Playbook エラーメッセージ

VNC SASL Ansible Playbook を実行すると、タスクが以下のエラーメッセージを表示して失敗する可能性があります。

Using a SSH password instead of a key is not possible because Host Key checking is enabled and sshpass does not support this. Please add this host's fingerprint to your known_hosts file to manage this host.

この問題を解決するには、次のいずれかを実行してホストキー検査を無効にします。

- /etc/ansible/ansible.cfg の次の行のコメントを解除して、ホストキー検査を永続的に無効にします。

```
#host_key_checking = False
```

- 以下のコマンドを実行して、ホストキーの確認を一時的に無効にします。

```
export ANSIBLE_HOST_KEY_CHECKING=False
```

関連情報

- [Configuring and Applying SCAP Policies During Installation](#)
- [Installers and Images for Red Hat Virtualization Manager \(v.4.3 for x86_64\)](#)

E.3.3. Manager の CA 証明書を信頼するためのリモートビューアーの設定

RHV Manager の認証局 (CA) を信頼するように、クライアントマシン **virt-viewer** または **remote-viewer** でリモートビューアーコンソールを設定します。

手順

- https://<engine_address>/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA に移動します。
- すべての信頼設定を有効にします。
- VNC コンソールを実行する予定のクライアントマシンで、証明書ファイルのディレクトリーを作成します。

```
$ mkdir ~/.pki/CA
```

警告



この手順で **mkdir: cannot create directory**

'/home/example_user/.pki/CA': File existsなどのエラーを生成する場合は、次の手順で **~/.pki/CA/cacert.pem** が上書きされないように予防措置を取ります。たとえば、ファイル名に現在の日付を含めます。

4. 証明書をダウンロードします。

```
$ curl -k -o ~/.pki/CA/cacert-<today's date>.pem \"https://<engine_address>/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA"
```

5. ブラウザーに認証局をインストールします。

- [Firefox](#)
- [Internet Explorer](#)
- [Google Chrome](#)

6. クライアントマシンに SASL SCRAM ライブラリーをインストールします。

```
$ sudo dnf install cyrus-sasl-scram
```

検証手順

1. 作成した FIPS 対応のホストのいずれかで仮想マシンを実行します。
2. VNC コンソールを使用して仮想マシンに接続します。

関連情報

- [コンソールコンポーネントのインストール](#)
- [Manager CA 証明書の置き換え](#)

付録F プロキシー

F.1. SPICE プロキシー

F.1.1. SPICE プロキシーの概要

SPICE プロキシーは、SPICE クライアントがハイパーバイザーを接続するネットワークの外部にある場合に SPICE クライアントを仮想マシンに接続するために使用されるツールです。SPICE プロキシーを設定するには、マシンに **Squid** をインストールし、プロキシートラフィックを許可するようにファイアウォールを構成します。SPICE プロキシーをオンにするには、Manager で **engine-config** を使用して、**SpiceProxyDefault** キーをプロキシーの名前および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** キーが構成されている値を削除します。



重要

SPICE プロキシーは、スタンドアロン SPICE クライアントと組み合わせた場合にのみ使用でき、noVNC を使用して仮想マシンに接続するためには使用できません。

F.1.2. SPICE プロキシーマシンの設定

この手順では、マシンを SPICE プロキシーとして設定する方法を説明します。SPICE プロキシーを使用すると、ネットワークの外部から Red Hat Virtualization ネットワークに接続できます。この手順で **Squid** を使用してプロキシーサービスを提供します。

手順

1. プロキシーマシンに **Squid** をインストールします。

```
# dnf install squid
```

2. `/etc/squid/squid.conf` を開きます。以下を、

```
http_access deny CONNECT !SSL_ports
```

次のように変更します。

```
http_access deny CONNECT !Safe_ports
```

3. squid サービスを起動し、再起動後に自動的に実行されるようにします。

```
# systemctl enable squid.service --now
```

4. デフォルトの firewalld ゾーンで squid サービスへの着信リクエストを有効にします。

```
# firewall-cmd --permanent --add-service=squid
```

5. このファイアウォールルールをランタイム設定で永続化します。

```
# firewall-cmd --reload
```

- ファイアウォールのサービス一覧に squid サービスが表示されていることを確認します。

```
# firewall-cmd --list-services
ssh dhcpcv6-client squid
```

これで、マシンを SPICE プロキシーとして設定できました。ネットワークの外部から Red Hat Virtualization ネットワークに接続する前に、SPICE プロキシーをアクティブ化します。

F.1.3. SPICE プロキシーをオンに設定

この手順では、SPICE プロキシーをアクティブ化（またはオン）する方法を説明します。

手順

- Manager で engine-config ツールを使用してプロキシーを設定します。

```
# engine-config -s SpiceProxyDefault=someProxy
```

- ovirt-engine** サービスを再起動します。

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

プロキシーの形式は以下のとおりとします。

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



注記

HTTPS プロキシーは、Red Hat Enterprise Linux 6.7、Red Hat Enterprise Linux 7.2 以降に同梱されている SPICE クライアントでのみサポートされています。それより前のクライアントでは、HTTP のみサポートされています。前のクライアントで HTTPS が指定されている場合、クライアントはプロキシー設定を無視し、ホストへの直接接続を試みます。

これで SPICE Proxy がアクティブ（オン）になりました。SPICE プロキシーを介した Red Hat Virtualization ネットワークへの接続が可能になりました。

F.1.4. SPICE プロキシーをオフに設定

この手順では、SPICE プロキシーをオフに（非アクティブ化）する方法を説明します。

手順

- Manager にログインします。

```
$ ssh root@[IP of Manager]
```

- 以下のコマンドを実行し、SPICE プロキシーをクリアします。

```
# engine-config -s SpiceProxyDefault=""
```

- Manager を再起動します。

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

これで SPICE プロキシーが非アクティブ（オフ）になりました。SPICE プロキシーを介して Red Hat Virtualization ネットワークに接続できなくなりました。

F.2. SQUID プロキシー

F.2.1. Squid プロキシーのインストールおよび設定

このセクションでは、VM ポータルに Squid プロキシーをインストールして設定する方法を説明します。Squid プロキシーサーバーは、コンテンツアクセラレーターとして使用されます。頻繁に表示されたコンテンツをキャッシュし、帯域幅を削減し、応答時間を改善します。

手順

1. Squid プロキシーサーバーの HTTPS ポートのキーペアと証明書を取得します。このキーペアは、別の SSL/TLS サービスのキーペアを取得するのと同じ方法で取得できます。キーペアは、秘密鍵と署名付き証明書を含む 2 つの PEM ファイルの形式です。この手順では、`proxy.key` および `proxy.cer` という名前が付けられていることを前提としています。



注記

キーペアと証明書は、エンジンの認証局を使用して生成することもできます。プロキシーの秘密鍵および証明書がすでにあり、エンジン認証局でそれを生成したくない場合は、次の手順にスキップしてください。

2. プロキシーのホスト名を選択します。次に、プロキシーの証明書の識別名の他のコンポーネントを選択します。



注記

エンジン自体が使用するのと同じ国と同じ組織名を使用することが推奨されます。Manager がインストールされているマシンにログインし、次のコマンドを実行して、この情報を見つけます。

```
openssl x509 -in /etc/pki/ovirt-engine/ca.pem -noout -text | grep DirName
```

このコマンドは以下を出力します。

```
subject= /C=US/O=Example Inc./CN=engine.example.com.81108
```

ここでは `/C=US/O=Example Inc.` に注目します。これを用いて、プロキシーの証明書の完全な識別名を作成します。

```
/C=US/O=Example Inc./CN=proxy.example.com
```

3. プロキシーマシンにログインし、証明書署名要求を生成します。

```
# openssl req -newkey rsa:2048 -subj '/C=US/O=Example Inc./CN=proxy.example.com' -nodes -keyout proxy.key -out proxy.req
```



重要

証明書の識別名の前後にある引用符も含める必要があります。-nodes オプションは、秘密鍵を暗号化しないためのものです。つまり、プロキシーサーバーを起動するため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 および 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に保管してください。proxy.req は証明書署名要求です。proxy.req に特別な保護は必要ありません。

- 署名付き証明書を生成するには、証明書署名要求ファイルをプロキシーマシンからマネージャーマシンにコピーします。

```
# scp proxy.req engine.example.com:/etc/pki/ovirt-engine/requests/.
```

- Manager マシンにログインし、証明書に署名します。

```
# /usr/share/ovirt-engine/bin/pki-enroll-request.sh --name=proxy --days=3650 --subject='C=US/O=Example Inc./CN=proxy.example.com'
```

証明書が署名され、10 年間 (3650 日) 有効になります。必要に応じて、証明書の有効期限を短く設定します。

- 生成された証明書ファイルは /etc/pki/ovirt-engine/certs ディレクトリーで利用可能で、名前は proxy.cer です。プロキシーマシンで、このファイルを Manager マシンから現在のディレクトリーにコピーします。

```
# scp engine.example.com:/etc/pki/ovirt-engine/certs/proxy.cer .
```

- proxy.key と proxy.cer の両方がプロキシーマシンに存在することを確認します。

```
# ls -l proxy.key proxy.cer
```

- Squid プロキシーサーバーパッケージをプロキシーマシンにインストールします。

```
# dnf install squid
```

- 秘密鍵と署名済み証明書を、プロキシーがアクセスできる場所 (例: /etc/squid ディレクトリー) に移動します。

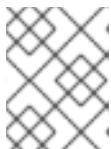
```
# cp proxy.key proxy.cer /etc/squid/.
```

- squid ユーザーが、これらのファイルを読み取れるようにパーミッションを設定します。

```
# chgrp squid /etc/squid/proxy.*  
# chmod 640 /etc/squid/proxy.*
```

- Squid プロキシーは、エンジンが使用する証明書を検証する必要があります。Manager 証明書をプロキシーマシンにコピーします。この例では、ファイルパス /etc/squid を使用します。

```
# scp engine.example.com:/etc/pki/ovirt-engine/ca.pem /etc/squid/.
```



注記

デフォルトの CA 証明書は、Manager マシンの `/etc/pki/ovirt-engine/ca.pem` にあります。

12. **squid** ユーザーが、証明書ファイルを読み取れるようにパーミッションを設定します。

```
# chgrp squid /etc/squid/ca.pem
# chmod 640 /etc/squid/ca.pem
```

13. SELinux が Enforcing モードの場合は、**semanage** ツールを使用して、ポート 443 のコンテキストを変更し、Squid がポート 443 を使用できるようにします。

```
# dnf install policycoreutils-python
# semanage port -m -p tcp -t http_cache_port_t 443
```

14. 既存の Squid 設定ファイルを以下に置き換えます。

```
https_port 443 key=/etc/squid/proxy.key cert=/etc/squid/proxy.cer ssl-bump
defaultsite=engine.example.com
cache_peer engine.example.com parent 443 0 no-query originserver ssl
sslcafile=/etc/squid/ca.pem name=engine login=PASSTHRU
cache_peer_access engine allow all
ssl_bump allow all
http_access allow all
```

15. Squid プロキシサーバーを再起動します。

```
# systemctl restart squid.service
```



注記

デフォルト設定の Squid プロキシーは、15 分のアイドル時間後に接続を終了します。Squid Proxy がアイドル状態の接続を終了するまでの時間を増やすには、`squid.conf` の **read_timeout** オプションを調整します (例: `read_timeout 10 hours`)。

F.3. WEBSOCKET プロキシー

F.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 コンソールを介して仮想マシンに接続できます。

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および設定できます ([Configuring the Red Hat Virtualization Manager](#) を参照)。

付録G ブランド化

G.1. ブランド化

G.1.1. Manager の再ブランド化

ポップアップウィンドウで使用されるアイコンや表示されるテキスト、Welcome ページに表示されるリンクなど、Red Hat Virtualization Manager のさまざまな側面をカスタマイズできます。これにより、Manager のブランドを変更し、管理者およびユーザーに表示される最終的なルックアンドフィールを細かく制御できます。

Manager のカスタマイズに必要なファイルは、Manager がインストールされているシステムの `/etc/ovirt-engine/branding/` ディレクトリーにあります。ファイルは、グラフィカルユーザーインターフェイスのさまざまな側面のスタイルを設定するために使用されるカスケードスタイルシートファイルのセットと、Manager のさまざまなコンポーネントに組み込まれるメッセージとリンクを含むプロパティーファイルのセットで構成されています。

コンポーネントをカスタマイズするには、そのコンポーネントのファイルを編集して変更を保存します。次にそのコンポーネントを開いたり更新したりすると、変更が適用されます。

G.1.2. ログイン画面

ログイン画面は、管理ポータルと VM ポータルの両方が使用するログイン画面です。カスタマイズできるログイン画面の要素は次のとおりです。

- ボーダー
- 左側のヘッダーイメージ
- 右側のヘッダーイメージ
- ヘッダーテキスト

ログイン画面のクラスは `common.css` にあります。

G.1.3. 管理ポータルの画面

管理ポータルの画面は、管理ポータルにログインする際に表示されるメイン画面です。カスタマイズできる管理ポータル画面の要素は、以下のとおりです。

- ロゴ
- 左側のバックグラウンドイメージ
- センターのバックグラウンドイメージ
- 右側のバックグラウンドイメージ
- ロゴの右側にあるテキスト

管理ポータル画面のクラスは `web_admin.css` にあります。

G.1.4. VM ポータル画面

VM ポータル画面は、VM ポータルにログインする際に表示される画面です。カスタマイズが可能な VM ポータル画面の要素は、以下のとおりです。

- 口ゴ
- センターのバックグラウンドイメージ
- 右側のバックグラウンドイメージ
- メイングリッド周辺の境界線
- `Logged in user` ラベルの上のテキスト

VM ポータル画面のクラスは `user_portal.css` にあります。

G.1.5. ポップアップウィンドウ

ポップアップウィンドウとは、ホストまたは仮想マシンなどのエンティティーの作成、編集、または更新を可能にする Manager のすべてのウィンドウです。カスタマイズできるポップアップウィンドウの要素は次のとおりです。

- ボーダー
- 左側のヘッダーイメージ
- ヘッダーセンターアイメージ(繰り返し)

ポップアップウィンドウのクラスは `common.css` にあります。

G.1.6. タブ

管理ポータルの多くのポップアップウィンドウにはタブが含まれています。カスタマイズ可能なこれらのタブの要素は次のとおりです。

- 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。

G.1.7. Welcome ページ

Welcome ページは、Manager のホームページにアクセスする際に最初に表示されるページです。全体的なルックアンドフィールをカスタマイズするだけでなく、テンプレートファイルを編集して、追加のドキュメントや内部 Web サイトのページへのリンクを追加するなどの変更を加えることもできます。カスタマイズできる Welcome ページの要素は次のとおりです。

- ページタイトル
- ヘッダー(左、中央、右)
- エラーメッセージ
- 転送するリンクおよびそのリンクに関連するメッセージ
- メッセージバーまたはプリアンブルの追加

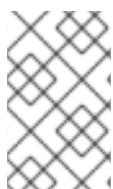
Welcome ページのクラスは **welcome_style.css** にあります。

テンプレートファイル

Welcome Page のテンプレートファイルは、**HTML**、**HEAD**、または **BODY** のタグが含まれない通常の HTML ファイルで、名前は **welcome_page.template** です。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。そのため、このファイルを編集して、新しいリンクを追加したり、コンテンツ自体を変更したりする必要があります。テンプレートファイルのもう 1 つの特長として、Welcome ページの処理時に **messages.properties** ファイル内の対応するテキストに置き換えられるプレースホルダーテキスト (例: **{user_portal}**) が含まれていることが挙げられます。

プリアンブル

バナーテキストを含む **preamble.template** とバナーサイズを定義する **preamble.css** ファイルを追加し、**branding.properties** ファイルでリンクすることにより、Welcome ページにカスタムメッセージバーを追加できます。サンプルファイルは、[sample preamble template](#) で利用できます。



注記

エンジンをアップグレードしても、カスタムメッセージバーはそのまま残り、問題なく機能します。エンジンのバックアップと復元の後、エンジンの復元中にカスタムメッセージバーを手動で復元して確認する必要があります。

G.1.8. Page Not Found ページ

Page Not Found ページは、Red Hat Virtualization Manager で見つからないページへのリンクを開くと表示されるページです。カスタマイズできる Page Not Found ページの要素は以下のとおりです。

- ページタイトル
- ヘッダー (左、中央、右)
- エラーメッセージ
- 転送するリンクおよびそのリンクに関連するメッセージ

Page Not Found ページのクラスは **welcome_style.css** にあります。

付録H システムアカウント

H.1. RED HAT VIRTUALIZATION MANAGER のユーザー アカウント

rhevm パッケージがインストールされると、Red Hat Virtualization をサポートするために多数のシステムユーザー アカウントが作成されます。各システムユーザーには、デフォルトのユーザー ID (UID) があります。作成されるシステムユーザー アカウントは、以下のとおりです。

- **vdsdm** ユーザー (UID **36**)。NFS ストレージドメインをマウントおよびアクセスするサポートツールに必要です。
- **ovirt** ユーザー (UID **108**)。**ovirt-engine** Red Hat JBoss Enterprise Application Platform インスタンスの所有者です。
- **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。

H.2. RED HAT VIRTUALIZATION MANAGER グループ

rhevm パッケージがインストールされると、Red Hat Virtualization をサポートするために多数のシステムユーザー グループが作成されます。各システムユーザー グループには、デフォルトのグループ ID (GID) があります。作成されるシステムユーザー グループは、以下のとおりです。

- **kvm** グループ (GID **36**)。グループメンバーには以下が含まれます。
- **vdsdm** ユーザー。
- **ovirt** グループ (GID **108**)。グループメンバーには以下が含まれます。
- **ovirt** ユーザー。
- **ovirt-vmconsole** グループ (GID **498**)。グループメンバーには以下が含まれます。
- **ovirt-vmconsole** ユーザー。

H.3. 仮想化ホストのユーザー アカウント

vdsdm および **qemu-kvm-rhev** パッケージがインストールされると、仮想化ホスト上に多数のシステムユーザー アカウントが作成されます。各システムユーザーには、デフォルトのユーザー ID (UID) があります。作成されるシステムユーザー アカウントは、以下のとおりです。

- **vdsdm** 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 ID (UID) およびグループ ID (GID) は、システムによって異なる場合があります。`vdsm` ユーザーの UID は **36** に固定され、`kvm` グループの GID は **36** に固定されます。

UID **36** または GID **36** がシステムの別のアカウントで既に使用されている場合は、`vdsm` および `qemu-kvm-rhev` パッケージのインストール時に競合が発生します。

H.4. 仮想化ホストグループ

`vdsm` および `qemu-kvm-rhev` パッケージがインストールされると、仮想化ホスト上に多数のシステムユーザーグループが作成されます。各システムユーザーグループには、デフォルトのグループ ID (GID) があります。作成されるシステムユーザーグループは、以下のとおりです。

- `kvm` グループ (GID **36**)。グループメンバーには以下が含まれます。
 - `qemu` ユーザー。
 - `sanlock` ユーザー。
- `qemu` グループ (GID **107**)。グループメンバーには以下が含まれます。
 - `vdsm` ユーザー。
 - `sanlock` ユーザー。
- `ovirt-vmconsole` グループ (GID **498**)。グループメンバーには以下が含まれます。
 - `ovirt-vmconsole` ユーザー。



重要

割り当てられるユーザー ID (UID) およびグループ ID (GID) は、システムによって異なる場合があります。`vdsm` ユーザーの UID は **36** に固定され、`kvm` グループの GID は **36** に固定されます。

UID **36** または GID **36** がシステムの別のアカウントで既に使用されている場合は、`vdsm` および `qemu-kvm-rhev` パッケージのインストール時に競合が発生します。

付録I 法的通知

Copyright © 2022 Red Hat, Inc.

Licensed under the ([Creative Commons Attribution-ShareAlike 4.0 International License](#)). Derived from documentation for the ([oVirt Project](#)). If you distribute this document or an adaptation of it, you must provide the URL for the original version.

Modified versions must remove all Red Hat trademarks.

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

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

Java® is a registered trademark of Oracle and/or its affiliates.

XFS® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.