Red Hat Virtualization 4.3

『Cockpit Web インターフェースを使用したセルフホストエンジンの Red Hat Virtualization のインストール』

Cockpit を使用した、Red Hat Virtualization Manager の管理するホストで実行している仮想マシンとして Red Hat Virtualization Manager をインストールするための推奨される方法

Last Updated: 2022-04-12

Red Hat Virtualization 4.3 『Cockpit Web インターフェースを使用したセルフホストエンジンの Red Hat Virtualization のインストール』

Cockpit を使用した、Red Hat Virtualization Manager の管理するホストで実行している仮想マシンとして Red Hat Virtualization Manager をインストールするための推奨される方法

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

本書では、自動インストールを設定および実行するために Cockpit Web インターフェースを使用して、セルフホストエンジン環境をインストールする方法について説明します。セルフホストエンジン環境とは、Red Hat Virtualization Manager (または「engine」) が、管理している環境と同じ環境内の特化したホスト上で実行される仮想マシン上にインストールされている環境のことです。これが希望する構成ではない場合には、『製品ガイド』の「その他のインストールオプション」を参照してください。

目次

前書き

セルフホストエンジンのインストールは、Ansible により自動化されています。最初のデプロイメントホスト上で Cockpit Web インターフェースのインストールウィザードを実行し、デプロイメントホスト上に作成される仮想マシンに Red Hat Virtualization Manager (または「engine」) をインストールおよび設定します。Manager および Data Warehouse データベースは Manager 用仮想マシンにインストールされますが、必要であればインストール後に別のサーバーに移行することができます。

Red Hat Virtualization Host では Cockpit がデフォルトで利用可能ですが、Red Hat Enterprise Linux ホストに Cockpit をインストールすることもできます。

Manager 用仮想マシンを実行することのできるホストは、セルフホストエンジンノードと呼ばれます。高可用性機能に対応するためには、少なくとも 2 台のセルフホストエンジンノードが必要です。

Manager 用仮想マシン専用のストレージドメインは、セルフホストエンジン用ストレージドメインと呼ばれます。このストレージドメインはインストールのスクリプトにより作成されるので、インストールの開始前にベースとなるストレージを準備する必要があります。

環境オプションおよび推奨される構成に関する情報は、『**Planning and Prerequisites Guide**』を参照してください。セルフホストエンジン環境に固有の設定については、「セルフホストエンジンの推奨事項」を参照してください。

表1 Red Hat Virtualization の主要コンポーネント

コンポーネント名	説明
Red Hat Virtualization Manager	環境内のリソースを管理するグラフィカルユーザーインターフェースと REST API を提供するサービス。Manager は、Red Hat Enterprise Linux を実行する物理マシンまたは仮想マシンにインストールされます。
ホスト	サポートされているホストには、Red Hat Enterprise Linux ホスト (RHEL ホスト) と Red Hat Virtualization Host (イメージベースのハイパーバイザー) の 2 つのタイプがあります。ホストは、Kernel-based Virtual Machine (KVM) テクノロジーを使用して、仮想マシンを実行するためのリソースを提供します。
共有ストレージ	仮想マシンに関連付けられたデータの保管に使用するストレージサービス
Data Warehouse	Manager から設定情報および統計データを収集するサービス

セルフホストエンジンのアーキテクチャー

Red Hat Virtualization Manager は、管理している環境と同じ環境内のセルフホストエンジンノード (特化したホスト) で仮想マシンとして実行されます。セルフホストエンジン環境に必要な物理サーバーは 1 台少なくなりますが、デプロイと管理を行うための管理オーバーヘッドがより高くなります。Manager は、外部の HA 管理を使用せずに高可用性になります。

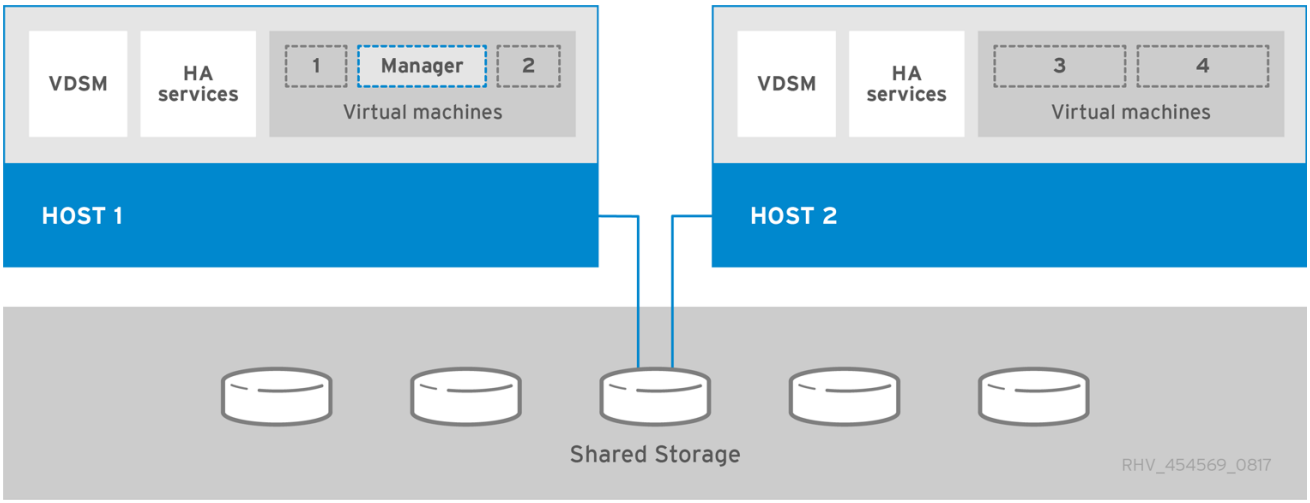
セルフホストエンジン環境の最小限のセットアップには、以下が含まれます。

- セルフホストエンジンノードでホストされている Red Hat Virtualization Manager 用仮想マシン 1 台。RHV-M Appliance は、Red Hat Enterprise Linux 7 仮想マシンのインストールと、その仮想マシンへの Manager のインストールを自動化するために使用されます。

- 仮想マシンの高可用性には、最小でセルフホストエンジンノード 2 台。Red Hat Enterprise Linux ホストまたは Red Hat Virtualization Host (RHVH) を使用することができます。VDSM (ホストエージェント) は全ホストで実行され、Red Hat Virtualization Manager との通信を円滑に行います。HA サービスは、すべてのセルフホストエンジンノードで実行され、Manager 用仮想マシンの高可用性を管理します。

- ストレージサービスを 1 つ。使用するストレージタイプに応じて、ローカルまたはリモートサーバーでホストすることができます。ストレージサービスは全ホストからアクセス可能である必要があります。

図1 セルフホストエンジンの Red Hat Virtualization アーキテクチャー



第1章 インストールの概要

セルフホストエンジンのインストールには Ansible および RHV-M Appliance (事前設定された Manager 用仮想マシンのイメージ) が使用され、以下のタスクを自動化しています。

- 最初のセルフホストエンジンノードの設定
- そのノードへの Red Hat Enterprise Linux 仮想マシンのインストール
- その仮想マシンへの Red Hat Virtualization Manager のインストールと設定
- セルフホストエンジン用ストレージドメインの設定

注記

RHV-M Appliance が使用されるのはインストール時だけです。Manager のアップグレードには使用されません。

セルフホストエンジン環境をインストールするステップは、以下のとおりです。

1. セルフホストエンジン用ストレージドメインおよび通常のストレージドメインに使用するストレージを準備します。以下のストレージタイプのいずれかを使用することができます。
   - NFS
   - iSCSI
   - ファイバーチャネル (FCP)
   - Red Hat Gluster Storage
2. インストールを実行するデプロイメントホストをインストールします。このホストが最初のセルフホストエンジンノードになります。以下のホストタイプのいずれかを使用することができます。
   - Red Hat Virtualization Host
   - Red Hat Enterprise Linux
     Red Hat Virtualization Host では Cockpit がデフォルトで利用可能ですが、Red Hat Enterprise Linux ホストに Cockpit をインストールすることもできます。
3. Red Hat Virtualization Manager をインストールおよび設定します。
   a. デプロイメントホストの Cockpit Web インターフェースを通じて、セルフホストエンジンをインストールします。
   b. Manager をコンテンツ配信ネットワークに登録し、Red Hat Virtualization Manager のリポジトリーを有効化する
   c. 管理ポータルに接続し、ホストおよびストレージドメインを追加する
4. Manager にさらにセルフホストエンジンノードおよび通常のホストを追加します。セルフホストエンジンノードは Manager 用仮想マシンおよびその他の仮想マシンを実行することができます。通常のホストは Manager 用仮想マシンを実行することはできませんが、その他すべての仮想マシンを実行することができます。
   a. 以下のホストタイプのいずれか、または両方を使用します。

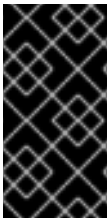
- Red Hat Virtualization Host
- Red Hat Enterprise Linux

b. Manager にセルフホストエンジンノードのホストを追加します。

c. Manager に通常のホストを追加します。

5. Manager にさらにストレージドメインを追加します。セルフホストエンジン用ストレージドメインは、Manager 用仮想マシンだけが使用することを推奨します。

6. データベースまたはサービスを Manager とは別のサーバーでホストする場合には、インストールの完了後にそれらを移行することができます。



重要

環境を最新の状態に維持してください。詳細は、https://access.redhat.com/articles/2974891 を参照してください。既知の問題に対するバグ修正は頻繁にリリースされるため、Red Hat は、スケジュールされたタスクを使用してホストと Manager を更新することを推奨します。

第2章 要件

2.1. RED HAT VIRTUALIZATION MANAGER の要件

2.1.1. ハードウェアの要件

以下に記載するハードウェアの最低要件および推奨要件は、一般的な中小規模のインストールをベースとしています。正確な要件は、デプロイメントの規模や負荷により異なります。

Red Hat Virtualization のハードウェア認定には、Red Hat Enterprise Linux のハードウェア認定が適用されます。詳細は、https://access.redhat.com/solutions/725243 を参照してください。特定のハードウェア項目が Red Hat Enterprise Linux での使用に認定されているかどうかを確認するには、https://access.redhat.com/ecosystem/#certifiedHardware を参照してください。

表2.1 Red Hat Virtualization Manager ハードウェアの要件

リソース	最低要件	推奨要件
CPU	デュアルコア CPU	クアッドコア CPU または複数のデュアルコア CPU
メモリー	利用可能なシステムメモリー 4 GB (Data Warehouse が未インストールで、かつ既存のプロセスによって消費されていないこと)	システムメモリー 16 GB
ハードディスク	ディスクの空き容量 25 GB (ローカルアクセス、書き込みが可能であること)	ディスクの空き容量 50 GB (ローカルアクセス、書き込みが可能であること) Manager 履歴データベースのサイズに適したディスク容量を算出するには、RHV Manager History Database Size Calculator ツールを使用できます。
ネットワークインターフェース	1 Gbps 以上の帯域幅のネットワークインターフェースカード (NIC) 1 基	1 Gbps 以上の帯域幅のネットワークインターフェースカード (NIC) 1 基

2.1.2. ブラウザーの要件

管理ポータルと VM ポータルには、以下のブラウザーバージョンとオペレーティングシステムを使用してアクセスすることができます。

ブラウザーのサポートは下記のように階層に分かれます。

- 階層 1: 全面的に検証済みで、完全にサポートされているブラウザーおよびオペレーティングシステムの組み合わせ。Red Hat Engineeringは、この層のブラウザーに関する問題の修正に取り組んでいます。

- 階層 2: 部分的に検証済みで、正常に機能する可能性の高いブラウザーとオペレーティングシステムの組み合わせ。この階層のサポートは限定されます。この階層のブラウザーで問題が発生した場合には、Red Hat のエンジニアリングチームが修正を試みます。
- 階層 3: 未検証ですが、正常に機能することが予想されるブラウザーとオペレーティングシステムの組み合わせ。この階層では、最小限のサポートが提供されます。この階層のブラウザーでは、Red Hat のエンジニアリングチームはマイナーな問題のみ修正を試みます。

表2.2 ブラウザーの要件

サポート階層	オペレーティングシステムファミリー	ブラウザー
階層 1	Red Hat Enterprise Linux	Mozilla Firefox 延長サポート版 (ESR) のバージョン
	任意	Google Chrome、Mozilla Firefox、または Microsoft Edge の最新バージョン
階層 2		
階層 3	任意	Google Chrome または Mozilla Firefox の旧バージョン
	任意	その他のブラウザー

2.1.3. クライアントの要件

仮想マシンコンソールは、Red Hat Enterprise Linux および Windows でサポートされている Remote Viewer (**virt-viewer**) クライアントを使用した場合にのみアクセスすることができます。**virt-viewer** をインストールするには、**『仮想マシン管理ガイド』の「クライアントマシンへのサポート コンポーネントのインストール」を** 参照してください。**virt-viewer** のインストールには管理者権限が必要です。

仮想マシンコンソールには、SPICE、VNC、または RDP（Windows のみ）プロトコルを介してアクセスされます。QXL グラフィカルドライバーは、ゲストオペレーティングシステムにインストールして、SPICE 機能を向上できます。SPICE が現在サポートしている最大解像度は 2560 x 1600 ピクセルです。

サポートされる QXL ドライバーは、Red Hat Enterprise Linux、Windows XP、および Windows 7 で利用できます。

SPICE のサポートは階層に分かれます。

- 階層 1: Remote Viewer が完全にテストされ、サポートされているオペレーティングシステム。
- 階層 2: Remote Viewer が部分的にテストされており、機能する可能性の高いオペレーティングシステム。この階層のサポートは限定されます。この階層の remote-viewer に関する問題を修正しようとします。

表2.3 クライアントオペレーティングシステムの SPICE サポート

サポート階層	オペレーティングシステム
階層 1	Red Hat Enterprise Linux 7.2 and later
	Microsoft Windows 7
階層 2	Microsoft Windows 8
	Microsoft Windows 10

2.1.4. オペレーティングシステムの要件

Red Hat Virtualization Manager は、最新のマイナーリリースに更新された Red Hat Enterprise Linux 7 のベースインストールにインストールする必要があります。

Manager に必要なパッケージのインストールを試みる際に、依存関係の問題が発生する可能性があるため、ベースのインストール後に他のパッケージをインストールしないでください。

Manager のインストールに必要なリポジトリー以外は有効にしないでください。

2.2. ホストの要件

Red Hat Virtualization のハードウェア認定には、Red Hat Enterprise Linux のハードウェア認定が適用されます。詳細は、https://access.redhat.com/solutions/725243 を参照してください。特定のハードウェア項目が Red Hat Enterprise Linux での使用に認定されているかどうかを確認するには、https://access.redhat.com/ecosystem/#certifiedHardware を参照してください。

ゲストに適用される要件および制限に関する詳しい情報は、「Red Hat Enterprise Linux テクノロジーの機能と制限」および「Red Hat Enterprise Virtualization における仮想化の制限」 を参照してください。

2.2.1. CPU の要件

すべての CPU が Intel® 64 または AMD64 CPU の拡張機能をサポートし、AMD-V™ または Intel VT® のハードウェア仮想化拡張機能が有効化されている必要があります。No eXecute flag (NX) のサポートも必要です。

以下の CPU モデルがサポートされています。

- AMD
  - Opteron G4
  - Opteron G5
  - EPYC
- Intel
  - Nehalem
  - Westmere

- SandyBridge
- Haswell
- Haswell-noTSX
- Broadwell
- Broadwell-noTSX
- Skylake（クライアント）
- Skylake（サーバー）

- IBM POWER8

2.2.1.1. プロセッサーが必要なフラグをサポートしているかどうかのチェック

BIOS で仮想化を有効にする必要があります。この設定を行った後には、ホストの電源をオフにしてから再起動して、変更が適用されるようにします。

1. Red Hat Enterprise Linux または Red Hat Virtualization Host の起動画面で任意のキーを押し、一覧から **Boot** か **Boot with serial console** のエントリーを選択します。
2. **Tab** を押して、選択したオプションのカーネルパラメーターを編集します。
3. 最後のカーネルパラメーターの後にスペースがあり、パラメーター **rescue** を追加します。
4. **Enter** を押して、レスキューモードで起動します。
5. プロンプトが表示されたら以下のコマンドを実行して、プロセッサーに必要な拡張機能があるかどうか、またそれらが有効になっているかどうかを確認します。

```
# grep -E 'svm|vmx' /proc/cpuinfo | grep nx
```

何らかの出力が表示されれば、プロセッサーはハードウェアの仮想化が可能です。出力が何も表示されない場合でも、プロセッサーがハードウェアの仮想化に対応している可能性があります。場合によっては、メーカーが BIOS で仮想化拡張機能を無効にしていることがあります。これに該当すると思われる場合には、メーカーが提供しているシステムの BIOS やマザーボードに関するマニュアルを参照してください。

2.2.2. メモリーの要件

必要最小限の RAM は 2 GB です。Red Hat Virtualization Host 上の仮想マシンでサポートされている RAM の最大値は、1 台あたり 4 TB です。

ただし、必要な RAM 容量は、ゲストオペレーティングシステムの要件、ゲストのアプリケーションの要件、ゲストのメモリーアクティビティーと使用状況によって異なります。KVM は、全ゲストがピークの負荷で同時に稼働しないことを前提として、仮想ゲストに対して物理 RAM をオーバーコミットして、物理的に存在する RAM を超える要件でゲストをプロビジョニングすることも可能です。KVM は、ゲストが必要とする RAM だけを割り当てて、使用率の低いゲストを swap に移動することによって、オーバーコミットします。

2.2.3. ストレージの要件

ホストには、設定、ログ、カーネルダンプを格納し、swap 領域として使用するためのストレージが必

要です。ストレージはローカルまたはネットワークベースとすることができます。Red Hat Virtualization Host (RHVH) は、ネットワークストレージのデフォルト割り当ての 1 つ、一部、またはすべてを使用して起動することができます。ネットワークストレージから起動する場合、ネットワークの接続が失われるとフリーズする場合があります。ドロップインマルチパス設定ファイルを追加すると、ネットワーク接続の喪失に対処することができます。SAN ストレージから起動した RHVH がネットワーク接続を失うと、接続が回復するまでファイルは読み取り専用になります。ネットワークストレージを使用すると、パフォーマンスが低下する場合があります。

本セクションでは、RHVH の最低ストレージ要件について説明します。Red Hat Enterprise Linux ホストのストレージ要件は、既存の設定で使用されるディスク容量によって異なりますが、RHVH の要件よりも多くなるはずです。

ホストのインストールの最低ストレージ要件を以下に示します。ただし、Red Hat では、より多くのストレージ領域を使用するデフォルトの割り当てを使用することを推奨します。

- / (root): 6 GB
- /home: 1 GB
- /tmp: 1 GB
- /boot: 1 GB
- /var: 15 GB
- /var/crash: 10 GB
- /var/log: 8 GB
- /var/log/audit: 2 GB
- swap: 1 GB (推奨の swap サイズについては、「Red Hat Enterprise Linux で推奨される swap のサイズ」を参照してください)
- Anaconda では、将来のメタデータ拡張用に、ボリュームグループ内のシンプールサイズの 20% が確保されます。これは、通常の使用条件においてデフォルト設定でストレージを使い果たすのを防ぐためです。インストール中のシンプールのオーバープロビジョニングもサポートされていません。
- **最小合計： 55 GB**

セルフホストエンジンのインストールに RHV-M Appliance もインストールする場合には、**/var/tmp** は 5 GB 以上である必要があります。

メモリーのオーバーコミットを使用する場合には、すべての仮想マシンに仮想メモリーを提供するのに十分な swap 領域を追加してください。「 Memory Optimization 」を参照してください。

2.2.4. PCI デバイスの要件

ホストには、1 Gbps 以上の帯域幅のネットワークインターフェースが少なくとも 1 基搭載されている必要があります。Red Hat では、各ホストにネットワークインターフェースが 2 つあり、仮想マシンの移行など、ネットワーク集約型アクティビティーをサポートする専用インターフェースがあります。このように負荷の高い操作のパフォーマンスは、利用可能な帯域幅により制限されます。

Intel Q35 ベースの仮想マシンで PCI Express と従来の PCI デバイスを使用する方法に関する情報は、**「Using PCI Express and Conventional PCI Devices with the Q35 Virtual Machine」**を参照してください。

2.2.5. デバイス割り当ての要件

仮想マシンがホストから特定の PCIe デバイスを使用できるように、デバイス割り当ておよび PCI パススルーを実装する予定がある場合は、以下の要件を満たしていることを確認してください。

- CPU が IOMMU (例: VT-d または AMD-Vi) をサポートしていること。IBM POWER8 はデフォルトで IOMMU をサポートしています。
- ファームウェアが IOMMU をサポートしていること。
- 使用する CPU ルートポートが ACS または ACS と同等の機能をサポートしていること。
- PCIe デバイスが ACS または ACS と同等の機能をサポートしていること。
- Red Hat は、PCIe デバイスとルートポート間の PCIe スイッチおよびブリッジがすべて ACS をサポートすることを推奨します。たとえば、スイッチが ACS をサポートしていない場合には、そのスイッチの背後にあるデバイスはすべて同じ IOMMU グループを共有し、同じ仮想マシンにしか割り当てることができません。
- GPU のサポートについては、Red Hat Enterprise Linux 7 は、VGA 以外のグラフィックデバイスとして PCIe ベースの NVIDIA K シリーズ Quadro（モデル 2000 シリーズ以上）、GRID および Tesla の PCI デバイス割り当てをサポートします。現在、標準のエミュレーションされた VGA インターフェースの 1 つ以外に、仮想マシンには GPU を 2 つまでアタッチすることができます。エミュレーションされた VGA は、起動前やインストールに使用され、NVIDIA グラフィックドライバーが読み込まれると NVDIA GPU に引き継がれます。NVIDIA Quadro 2000 も、Quadro K420 カードもサポートされていない点にご注意ください。

ベンダーの仕様とデータシートをチェックして、お使いのハードウェアが要件を満たしていることを確認してください。**lspci -v** コマンドを使用すると、システムにインストールされている PCI デバイスの情報を表示できます。

2.2.6. vGPU の要件

ホスト上の仮想マシンが仮想 GPU を使用するためには、ホストが以下の要件を満たす必要があります。

- GPU が vGPU に対応していること
- ホストカーネルで GPU が有効であること
- 適切なドライバーと共に GPU がインストールされていること
- 事前定義の **mdev_type** が、デバイスのサポートする mdev タイプのいずれかに設定されていること
- クラスター内の各ホストに vGPU に対応したドライバーがインストールされていること
- vGPU ドライバーと共に vGPU に対応した仮想マシンのオペレーティングシステムがインストールされていること

2.3. ネットワークの要件

2.3.1. 一般要件

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 (または 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。

2.3.2. DNS、NTP、IPMI フェンシング、およびメトリクスストアのファイアウォール要件

以下のトピックに対するファイアウォールの要件は特殊なケースで、個別に検討する必要があります。

DNS および NTP

Red Hat Virtualization では DNS または NTP サーバーは作成されません。したがって、ファイアウォールには、着信トラフィックに対するオープンポートは必要ありません。

デフォルトでは、Red Hat Enterprise Linux は任意のアドレス上の DNS および NTP への送信トラフィックを許可します。発信トラフィックを無効にする場合には、DNS および NTP サーバーに送付されるリクエストに例外を定義します。

重要

- Red Hat Virtualization Manager およびすべてのホスト (Red Hat Virtualization Host および Red Hat Enterprise Linux ホスト) には、完全修飾ドメイン名と、全面的かつ完全な正引きおよび逆引きの名前解決が必要です。
- DNS サービスを Red Hat Virtualization 環境内の仮想マシンとして実行する方法はサポートされていません。Red Hat Virtualization 環境が使用する DNS サービスは、すべて環境の外部でホストする必要があります。
- Red Hat は、名前解決に **/etc/hosts** ファイルの代わりに DNS を使用することを強く推奨します。hosts ファイルを使用すると、より多くの作業が必要となり、誤設定の可能性がより高くなります。

IPMI およびその他のフェンシング機構 (オプション)

IPMI (Intelligent Platform Management Interface) およびその他のフェンシング機構については、ファイアウォールには、着信トラフィックに対するオープンポートは必要ありません。

デフォルトでは、Red Hat Enterprise Linux は任意のアドレス上のポートへの送信 IPMI トラフィックを許可します。発信トラフィックを無効にする場合には、IPMI またはフェンシングサーバーに送付されるリクエストに例外を設定します。

クラスター内の各 Red Hat Virtualization Host および Red Hat Enterprise Linux ホストは、クラスター内にある残りの全ホストのフェンシングデバイスに接続できる必要があります。クラスターホストにエラー (ネットワークエラー、ストレージエラーなど) が発生し、ホストとして機能できない場合は、データセンターの他のホストに接続できる必要があります。

具体的なポート番号は、使用するフェンスエージェントのタイプおよびその設定により異なります。

以降のセクションで説明するファイアウォール要件の表には、このオプションは含まれていません。

メトリクスストア、Kibana、および ElasticSearch

Metrics Store、Kibana、および ElasticSearch については、「Metric Store 仮想マシンのネットワーク設定」を参照してください。

2.3.3. Red Hat Virtualization Manager ファイアウォールの要件

Red Hat Virtualization Manager では、ネットワークトラフィックがシステムのファイアウォールを通過できるように複数のポートを開放しておく必要があります。

engine-setup スクリプトではファイアウォールを自動的に設定できますが、**iptables** を使用している場合は既存のファイアウォール設定が上書きされます。既存のファイアウォール設定を維持するには、Manager で必要なファイアウォールルールを手動で挿入する必要があります。**engine-setup** コマンドは、**/etc/ovirt-engine/ iptables.example** ファイルに必要な iptables ルールの一覧を保存します。**firewalld** を使用している場合、**engine-setup** は既存の設定を上書きしません。

本セクションに記載するファイアウォール設定は、デフォルトの設定を前提としています。

注記

これらのファイアウォール要件の模式図が、https://access.redhat.com/articles/3932211 に記載されています。表に書かれた ID を使用して、模式図内の接続を探すことができます。

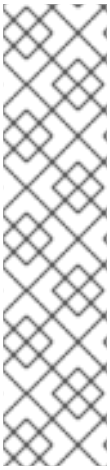
表2.4 Red Hat Virtualization Manager ファイアウォールの要件

ID	ポート	プロトコル	送信元	宛先	目的	デフォルトで暗号化
M1	-	ICMP	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Red Hat Virtualization Manager	オプション 診断に役立つ場合があります。	✗
M2	22	TCP	バックエンドの設定やソフトウェアのアップグレードなど、Manager のメンテナンスに使うシステム	Red Hat Virtualization Manager	Secure Shell (SSH) アクセス オプション	◯
M3	2222	TCP	仮想マシンのシリアルコンソールにアクセスするクライアント	Red Hat Virtualization Manager	仮想マシンのシリアルコンソールへの接続を可能にするための Secure Shell (SSH) アクセス。	◯

ID	ポート	プロトコル	送信元	宛先	目的	デフォルトで暗号化
M4	80、443	TCP	管理ポータルのクライアント VM ポータルのクライアント Red Hat Virtualization Host Red Hat Enterprise Linux ホスト REST API クライアント	Red Hat Virtualization Manager	Manager に HTTP (ポート 80、暗号化なし) および HTTPS (ポート 443、暗号化あり) のアクセスを提供します。HTTP は接続を HTTPS にリダイレクトします。	○
M5	6100	TCP	管理ポータルのクライアント VM ポータルのクライアント	Red Hat Virtualization Manager	Manager 上で WebSocket プロキシーを実行している場合に、Web ベースのコンソールクライアント (**noVNC**) に対する Websocket プロキシーアクセスを提供します。ただし、WebSocket プロキシーが別のホストで実行されている場合には、このポートは使用されません。	✗

ID	ポート	プロトコル	送信元	宛先	目的	デフォルトで暗号化
M6	7410	UDP	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Red Hat Virtualization Manager	ホストの Kdump が有効な場合には、Manager の fence_kdump リスナー用にこのポートを開きます。「fence_kdump Advanced Configuration」を参照してください。**fence_kdump** には、接続を暗号化する方法はありません。ただし、このポートは、適していないホストからのアクセスをブロックするように手動で設定できます。	✗
M7	54323	TCP	管理ポータルのクライアント	Red Hat Virtualization Manager (ImageIO Proxy サーバー)	ImageIO プロキシー (**ovirt-imageio-proxy**) との通信に必要です。	はい
M8	6442	TCP	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Open Virtual Network (OVN) southbound データベース	Open Virtual Network (OVN) データベースへの接続	◯
M9	9696	TCP	OVN 用外部ネットワークプロバイダーのクライアント	OVN 用外部ネットワークプロバイダー	OpenStack Networking API	◯ engine-setup によって生成された設定による暗号化。

ID	ポート	プロトコル	送信元	宛先	目的	デフォルトで暗号化
M10	35357	TCP	OVN 用外部ネットワークプロバイダーのクライアント	OVN 用外部ネットワークプロバイダー	OpenStack Identity API	◯ engine-setup によって生成された設定による暗号化。
M11	53	TCP、UDP	Red Hat Virtualization Manager	DNS サーバー	1023 より大きいポート番号からポート 53 への DNS ルックアップリクエストおよび応答。デフォルトで開いています。	✗
M12	123	UDP	Red Hat Virtualization Manager	NTP サーバー	1023 より大きいポート番号からポート 123 への NTP リクエストおよび応答。デフォルトで開いています。	不要



注記

- デフォルトの設定では、OVN northbound データベース (6641) のクライアントは **ovirt-provider-ovn** のみなので、OVN northbound データベースのポート (6641) は記載されていません。両者は同じホスト上で動作しているので、その通信はネットワークには現れません。
- デフォルトでは、Red Hat Enterprise Linux は任意のアドレス上の DNS および NTP への送信トラフィックを許可します。発信トラフィックを無効にする場合には、Manager がリクエストを DNS および NTP サーバーに送付するように例外を設定します。他のノードでも DNS および NTP が必要な場合があります。その際には、それらのノードの要件を確認し、適切にファイアウォールを設定してください。

2.3.4. ホストファイアウォールの要件

Red Hat Enterprise Linux ホストおよび Red Hat Virtualization Host (RHVH) では、ネットワークトラフィックがシステムのファイアウォールを通過できるように複数のポートを開放しておく必要があります。新たなホストを Manager に追加する際に、ファイアウォールルールがデフォルトで自動的に設定され、既存のファイアウォール設定はすべて上書きされます。

新規ホストの追加時のファイアウォール自動設定を無効にするには、**詳細パラメーター** の下の **ホストのファイアウォールを自動設定する** のチェックボックスからチェックを外します。

ホストのファイアウォールルールをカスタマイズするには、https://access.redhat.com/solutions/2772331 を参照してください。

注記

これらのファイアウォール要件の模式図が、https://access.redhat.com/articles/3932211 に記載されています。表に書かれた ID を使用して、模式図内の接続を探すことができます。

表2.5 仮想化ホストファイアウォールの要件

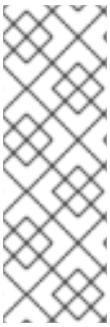
ID	ポート	プロトコル	送信元	宛先	目的	デフォルトで暗号化
H1	22	TCP	Red Hat Virtualization Manager	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Secure Shell (SSH) アクセス オプション	○
H2	2223	TCP	Red Hat Virtualization Manager	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	仮想マシンのシリアルコンソールへの接続を可能にするための Secure Shell (SSH) アクセス。	○
H3	161	UDP	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Red Hat Virtualization Manager	Simple Network Management Protocol (SNMP)。ホストから 1 つまたは複数の外部 SNMP マネージャーに Simple Network Management Protocol のトラップを送信する場合にのみ必要です。 オプション	✗

ID	ポート	プロトコル	送信元	宛先	目的	デフォルトで暗号化
H4	111	TCP	NFS ストレージサーバー	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	NFS 接続 オプション	✗
H5	5900 - 6923	TCP	管理ポータルのクライアント VM ポータルのクライアント	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	VNC および SPICE を介したリモートゲストのコンソールアクセス。クライアントが仮想マシンに容易にアクセスできるように、これらのポートは開放しておく必要があります。	◯ (オプション)

ID	ポート	プロトコル	送信元	宛先	目的	デフォルトで暗号化
H6	5989	TCP、UDP	Common Information Model Object Manager (CIMOM)	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Common Information Model Object Managers (CIMOM) がホスト上で実行中の仮想マシンをモニタリングするために使用します。このポートは、仮想化環境内の仮想マシンのモニタリングに CIMOM を使用する場合にのみ開放する必要があります。 オプション	✗
H7	9090	TCP	Red Hat Virtualization Manager クライアントマシン	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Cockpit がインストールされている場合には、Cockpit Web インターフェースにアクセスするために必要です。	○
H8	16514	TCP	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	**libvirt** を使った仮想マシンの移行	○

ID	ポート	プロトコル	送信元	宛先	目的	デフォルトで暗号化
H9	49152 - 49215	TCP	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	VDSM を使用した仮想マシンの移行とフェンシング。仮想マシンの自動および手動での移行を容易に実行できるように、これらのポートを開放しておく必要があります。	◯フェンスエージェントに応じて、libvirt を介して移行が行われます。
H10	54321	TCP	Red Hat Virtualization Manager Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	VDSM による Manager およびその他の仮想化ホストとの通信	◯
H11	54322	TCP	Red Hat Virtualization Manager (ImageIO Proxy サーバー)	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	ImageIO デーモン (**ovirt-imageio-daemon**) との通信に必要です。	◯

ID	ポート	プロトコル	送信元	宛先	目的	デフォルトで暗号化
H12	6081	UDP	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Open Virtual Network (OVN) をネットワークプロバイダーとして使用している場合に、OVN がホスト間にトンネルを作成するために必要です。	✗
H13	53	TCP、UDP	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	DNS サーバー	1023 より大きいポート番号からポート 53 への DNS ルックアップリクエストおよび応答。このポートは必須で、デフォルトで開いています。	✗



注記

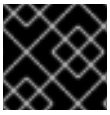
デフォルトでは、Red Hat Enterprise Linux は任意のアドレス上の DNS および NTP への送信トラフィックを許可します。発信トラフィックを無効にする場合には、Red Hat Virtualization Host に例外を設定します。

Red Hat Enterprise Linux ホストは DNS および NTP サーバーにリクエストを送付します。他のノードでも DNS および NTP が必要な場合があります。その際には、それらのノードの要件を確認し、適切にファイアウォールを設定してください。

2.3.5. データベースサーバーファイアウォールの要件

Red Hat Virtualization では、Manager データベース (**engine**) および Data Warehouse データベース (**ovirt-engine-history**) にリモートのデータベースサーバーの使用をサポートしています。リモートのデータベースサーバーを使用する予定の場合には、Manager および Data Warehouse サービス (Manager と分離することが可能) からの接続を許可する必要があります。

同様に、Red Hat CloudForms などの外部システムからローカルまたはリモートの Data Warehouse データベースにアクセスする予定の場合には、そのシステムからの接続が許可される必要があります。



重要

外部システムからの Manager データベースへのアクセスはサポートされていません。

注記

これらのファイアウォール要件の模式図が、https://access.redhat.com/articles/3932211 に記載されています。表に書かれた ID を使用して、模式図内の接続を探すことができます。

表2.6 データベースサーバーファイアウォールの要件

ID	ポート	プロトコル	送信元	宛先	目的	デフォルトで暗号化
D1	5432	TCP、UDP	Red Hat Virtualization Manager Data Warehouse サービス	Manager (**エンジン**) データベースサーバー Data Warehouse (**ovirt-engine-history**) データベースサーバー	PostgreSQL データベース接続のデフォルトポート	いいえ、有効化は可能です。
D2	5432	TCP、UDP	外部のシステム	Data Warehouse (**ovirt-engine-history**) データベースサーバー	PostgreSQL データベース接続のデフォルトポート	デフォルトでは無効です。いいえ、有効化は可能です。

第3章 RED HAT VIRTUALIZATION 用ストレージの準備

新しい環境のストレージドメインとして使用するストレージを準備します。Red Hat Virtualization 環境には少なくとも 1 つのデータストレージドメインが必要ですが、さらに追加することを推奨します。

データドメインには、データセンター内の仮想マシンおよびテンプレートの仮想ハードディスクと OVF ファイルを格納します。このドメインは、アクティブな間は複数のデータセンター間で共有することはできません (ただし、データセンター間で移行することは可能です)。複数のストレージタイプのデータドメインを同じデータセンターに追加することは可能ですが、それらはすべてローカルドメインではなく、全ホストがアクセス可能なドメインであることが条件となります。

セルフホストエンジンには、Manager 用仮想マシン専用の追加のデータドメインが必要です。このドメインはセルフホストエンジンのデプロイメント中に作成され、74 GiB 以上である必要があります。デプロイメントを開始する前に、このドメイン用のストレージを準備する必要があります。

以下のストレージタイプのいずれかを使用することができます。

- NFS
- iSCSI
- ファイバーチャネル (FCP)
- Red Hat Gluster Storage

重要

iSCSI ストレージを使用する場合には、セルフホストエンジン用ストレージドメインは独自の iSCSI ターゲットを使用する必要があります。追加のストレージドメインは、異なる iSCSI ターゲットを使用しなければなりません。

警告

セルフホストエンジン用ストレージドメインと同じデータセンター内に追加のデータストレージドメインを作成することを強く推奨します。セルフホストエンジンをデータセンター内にデプロイする際に、アクティブなデータストレージドメインを 1 つしか用意していない場合、そのストレージドメインが破損しても、新しいストレージドメインを追加したり、破損したストレージドメインを削除することはできません。セルフホストエンジンを再デプロイしなければなりません。

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 の準備と設定の詳細は、『**Red Hat Enterprise Linux 7 ストレージ管理ガイド**』の「ネットワークファイルシステム(NFS)」を参照してください。

「NFS」共有をエクスポートする方法は、「How to export 'NFS' share from NetApp Storage / EMC SAN in Red Hat Virtualization」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。

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 36
```

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

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

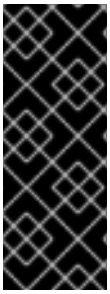
4. 所有者に読み取り/書き込みアクセスを許可し、グループおよびその他のユーザーに読み取り/実行アクセスを許可するように、ディレクトリーのモードを変更します。

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

3.2. 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 ストレージの準備および設定に関する詳細は、**『Red Hat Enterprise Linux 7 ストレージ管理ガイド』の「オン ラインストレージ管理」**を参照してください。

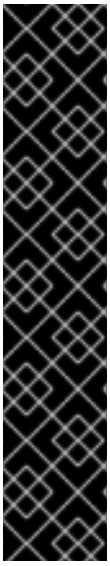


重要

ブロックストレージを使用する際、仮想マシンを Raw デバイスまたは直接 LUN にデプロイし、論理ボリュームマネージャーで管理する場合は、フィルターを作成してゲストの論理ボリュームを除外する必要があります。これにより、ホストの起動時にゲストの論理ボリュームがアクティブ化されるのを防ぐことができます。アクティブ化されると、論理ボリュームの内容が古くなり、データ破損が生じる可能性があります。詳細は、https://access.redhat.com/solutions/2662261 を参照してください。

重要

現状、Red Hat Virtualization はブロックサイズ 4K の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。

この状況を防ぐために、Red Hat は、ブート LUN 用に 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、接続がある場合はキューに置かれておくことを推奨します。

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

3.3. FCP ストレージの準備

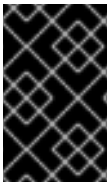
Red Hat Virtualization は、既存の LUN で構成されるボリュームグループからストレージドメインを作成する方法で、SAN ストレージをサポートしています。ボリュームグループおよび LUN は、いずれも同時に複数のストレージドメインにアタッチすることはできません。

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 **『Red Hat Enterprise Linux DM Multipath』**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。詳細は、https://access.redhat.com/solutions/2662261 を参照してください。



重要

現状、Red Hat Virtualization はブロックサイズ 4K の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。

この状況を防ぐために、Red Hat は、ブート LUN 用に 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、接続がある場合はキューに置かれておくことを推奨します。

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

3.4. RED HAT GLUSTER STORAGE の準備

Red Hat Gluster Storage のセットアップおよび設定に関する詳細は、『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 でサポートされる Red Hat Gluster Storage のバージョンについては、https://access.redhat.com/articles/2356261 を参照してください。

3.5. SAN ベンダーのマルチパス設定のカスタマイズ

マルチパス構成設定をカスタマイズする場合は、**/etc/multipath.conf** を変更しないでください。代わりに、**/etc/multipath.conf** を上書きする新しい設定ファイルを作成します。

警告

Virtual Desktop and Server Manager(VDSM)をアップグレードすると、**/etc/multipath.conf** ファイルが上書きされます。**multipath.conf** にカスタマイズが含まれている場合は、これを上書きするとストレージの問題が発生することがあります。

前提条件

- このトピックは、マルチパス接続ストレージドメインを使用するように設定されているシステムのみに適用されるため、**/etc/multipath.conf** ファイルがあります。
- **user_friendly_names** と **find_multipaths** の設定を上書きしないでください。詳細は、「ref-Recommended_Settings_for_Multipath.conf_SHE_cockpit_deploy」を参照してください。
- ストレージベンダーで必要な場合を除き、**no_path_retry** および **polling_interval** は上書きしないようにします。詳細は、「ref-Recommended_Settings_for_Multipath.conf_SHE_cockpit_deploy」を参照してください。

手順

1. **/etc/multipath.conf** の設定の値を上書きするには、**/etc/multipath/conf.d/** ディレクトリーに新しい設定ファイルを作成します。

注記

/etc/multipath/conf.d/ のファイルはアルファベット順で実行されます。名前の先頭に番号が付いたファイルの命名規則に従います。たとえば、**/etc/multipath/conf.d/90-myfile.conf** です。

2. **/etc/multipath.conf** から、**/etc/multipath/conf.d/** の新しい設定ファイルに、上書きする設定をコピーします。設定値を編集し、変更を保存します。

3. **systemctl reload multipathd** コマンドを入力して、新しい設定を適用します。

注記

multipathd サービスを再起動しないようにします。これにより、VDSM ログにエラーが生成されます。

検証手順

/etc/multipath.conf で VDSM が生成した設定を上書きする場合は、さまざまな障害シナリオで新しい設定が想定どおりに実行されていることを確認します。

たとえば、ストレージの接続をすべて無効にします。その後、一度に 1 つの接続を有効にし、これによりストレージドメインに到達可能であることを確認します。

トラブルシューティング

Red Hat Virtualization Host が共有ストレージにアクセスできない場合は、**/etc/multpath.conf** および **/etc/multipath/conf.d/** の下にあるファイルで SAN と互換性のない値を確認してください。

関連情報

- RHEL ドキュメントの『Red Hat Enterprise Linux DM Multipath』
- 『Administration Guide』 の 「 Configuring iSCSI Multipathing 」
- 「How do I customize /etc/multipath.conf on my RHV-H hypervisors?What values must not change and why? Red Hat カスタマーポータルの **multipath.conf** ファイルの例を示し、本トピックのベースとなっています。

3.6. MULTIPATH.CONF の推奨される設定

/etc/multipath.conf を上書きする場合は、以下の設定を上書きしないでください。

user_friendly_names no

この設定では、実際のデバイス名に加えて、ユーザーフレンドリーな名前がデバイスに割り当てられるかどうかを制御します。デバイスにアクセスするには、複数のホストが同じ名前を使用する必要があります。この設定を無効にすることで、ユーザーフレンドリーな名前がこの要件を妨げないようにします。

find_multipaths no

この設定は、パスが 1 つしかない場合でも、RHVH がマルチパスを介してすべてのデバイスにアクセスしようとするかどうかを制御します。この設定を無効にすることで、この設定が有効な場合に RHV が too-clever 動作を使用しないようにします。

ストレージシステムベンダーが必要としない限り、以下の設定を上書きしないようにします。

no_path_retry 4

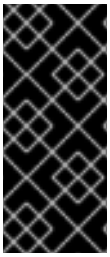
この設定では、利用可能なパスがない場合にポーリングを再試行する回数を制御します。RHV バージョン 4.2 より前は、パスが利用できない場合に QEMU の I/O キューに問題が生じていたため、**no_path_retry** の値は **fail** でした。**fail** 値により、仮想マシンはすぐに失敗し、一時停止していました。RHV バージョン 4.2 ではこの値が **4** に変更されました。これにより、multipathd は最後のパスが失敗したことを検知すると、すべてのパスをさらに 4 回確認します。ポーリングがデフォルトの 5 秒間隔で行われると仮定すると、パスの確認には 20 秒かかります。パスが起動しない場合、multipathd は、パスが復元されるまでキューを停止するようにカーネルに指示し、未処理および将来の I/O をすべて失敗させます。パスが復元されると、次にすべてのパスが失敗したときのために、20 秒間のパスの確認時間がリセットされます。詳細は、この設定を変更したコミット を参照してください。

polling_interval 5

この設定では、パスが開いているか、または失敗したかを検出するポーリングの試行間隔の秒数を決定します。ベンダーが値を増やす明確な理由を提供しない限り、VDSM が生成するデフォルト値を維持します。これにより、システムはパスの失敗に早めの対応することができます。

第4章 セルフホストエンジン用デプロイメントホストのインストール

セルフホストエンジンは、Red Hat Virtualization Host または Red Hat Enterprise Linux ホスト からデプロイすることができます。



重要

高可用性のためにボンドインターフェースを使用する、またはトラフィックをタイプごとに分離するために VLAN を使用する場合は (例: ストレージ用の接続と管理用の接続)、セルフホストエンジンのデプロイメント開始前にホストに設定する必要があります。『**Planning and Prerequisites Guide**』の「Networking Recommendations」を参照してください。

4.1. RED HAT VIRTUALIZATION HOST のインストール

Red Hat Virtualization Host (RHVH) は、Red Hat Virtualization 環境でハイパーバイザーとして機能する物理マシンの簡単な設定方法を提供するために設計された、Red Hat Enterprise Linux をベースとする最小構成のオペレーティングシステムです。この最小構成のオペレーティングシステムには、マシンがハイパーバイザーとして機能するのに必要なパッケージのみが含まれており、ホストの監視や管理タスクの実行用に Cockpit Web インターフェースが備えられています。最低限のブラウザー要件については、http://cockpit-project.org/running.html を参照してください。

RHVH は NIST SP 800-53 パーティショニングの要件をサポートし、より強固なセキュリティーを提供します。RHVH は、デフォルトで NIST 800-53 パーティションレイアウトを使用します。

ホストは最低限の ホスト要件 を満たしている必要があります。

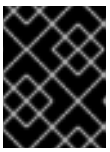
手順

1. カスタマーポータルから RHVH ISO イメージをダウンロードします。
   a. カスタマーポータル (https://access.redhat.com) にログインします。
   b. メニューバーの **ダウンロード** をクリックします。
   c. **Red Hat Virtualization** をクリックします。スクロールして **Download Latest** をクリックして、製品のダウンロードページにアクセスします。
   d. **RHV 4.3 の Hypervisor Image に移動し、今すぐダウンロード** をクリックします。
   e. ブート可能なメディアデバイスを作成します。詳細は、『**Red Hat Enterprise Linux インストールガイド**』の「メディアの作成」を参照してください。
2. RHVH のインストール先となるマシンを起動し、準備したインストールメディアから起動します。
3. 起動メニューから **Install RHVH 4.3 を** 選択し、**Enter** を押します。

注記

また、**Tab** キーを押してカーネルパラメーターを編集することもできます。カーネルパラメーターはスペースで区切る必要があります。また、指定したカーネルパラメーターを使用してシステムを起動するには、**Enter** キーを押します。**Esc** キーを押してカーネルパラメーターへの変更を消去し、起動メニューに戻ります。

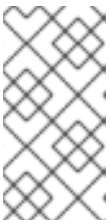
4. 言語を選択し、**Continue** をクリックします。
5. 日付と時刻 の画面から **タイムゾーンを** 選択し、完了 をクリックし **ます**。
6. キーボード画面からキーボードレイアウトを選択し 、 完了 をクリックし **ます**。
7. **インストール先** の画面から RHVH のインストール先のデバイスを選択します。オプションで暗号化を有効にします。**完了**をクリックします。



重要

Red Hat は、**自動構成のパーティション設定** オプションを使用することを強く推奨します。

8. **ネットワーク & ホスト名** の画面からネットワークを選択し、**設定** をクリックして接続の詳細を設定します。



注記

システムの起動するたびに接続を使用するには、**Automatically connect to this network when it is available** チェックボックスを選択します。詳細は、『 **Red Hat Enterprise Linux 7 インストールガイド**』 の「 ネットワーク接続の編集 」を参照してください。

ホスト名 フィールドにホスト名を **入力** し、完了 をクリックし **ます**。

9. オプションで **言語サポート**、**セキュリティーポリシー**、および Kdump を設定します。インストール **概要 画面の各セクションの詳細は、『Red Hat Enterprise Linux 7 インストールガイド』 の「Anaconda を使用** した Anaconda のインストール 」を参照してください。
10. **インストールの開始** をクリックします。
11. RHVH のインストールの際に root パスワードを設定して、オプションで追加のユーザーを作成します。

警告

ローカルのセキュリティー脆弱性が悪用される可能性があるため、Red Hat は RHVH に信頼できないユーザーを作成しないことを強く推奨します。

12. **再起動** をクリックしてインストールを完了します。

注記

RHVH の再起動時に、**nodectl check** はホストでヘルスチェックを実行し、コマンドラインへのログイン時に結果を表示します。**node status: OK** または **node status: DEGRADED** のメッセージはヘルスステータスを示します。**nodectl check** を実行して詳細情報を取得します。サービスはデフォルトで有効になっています。

4.1.1. Red Hat Virtualization Host のリポジトリーの有効化

更新を受け取るためにシステムを登録します。Red Hat Virtualization Host に必要なリポジトリーは 1 つだけです。本セクションでは、RHVH を コンテンツ配信ネットワーク または Red Hat Satellite 6 に登録する手順について説明します。

コンテンツ配信ネットワークへの RHVH の登録

1. **https://HostFQDNorIP:9090** で Cockpit Web インターフェースにログインします。
2. **サブスクリプション** に移動し、**システムの登録** をクリックして、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。**Red Hat Virtualization Host** のサブスクリプションが自動的にシステムにアタッチされます。
3. **Terminal** をクリックします。
4. **Red Hat Virtualization Host 7** リポジトリーを有効にして、Red Hat Virtualization Host に対する後続の更新を可能にします。

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

Red Hat Satellite 6 への RHVH の登録

1. **https://HostFQDNorIP:9090** で Cockpit Web インターフェースにログインします。
2. **Terminal** をクリックします。
3. RHVH を Red Hat Satellite 6 に登録します。

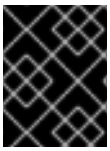
```
# rpm -Uvh http://satellite.example.com/pub/katello-ca-consumer-latest.noarch.rpm
# subscription-manager register --org="org_id"
# subscription-manager list --available
# subscription-manager attach --pool=pool_id
# subscription-manager repos \
  --disable='*' \
  --enable=rhel-7-server-rhvh-4-rpms
```

4.2. RED HAT ENTERPRISE LINUX ホストのインストール

Red Hat Enterprise Linux ホストは、**Red Hat Enterprise Linux Server** および **Red Hat Virtualization** サブスクリプションがアタッチされた、物理サーバーに Red Hat Enterprise Linux 7 の標準的な基本インストールをベースにしています。

詳細なインストール手順は『標準的な {enterprise-linux-shortname} インストールの実行』を参照してください。

ホストは最低限の ホスト要件 を満たしている必要があります。



重要

ホストの BIOS 設定で仮想化が有効になっている必要があります。ホストの BIOS 設定の変更に関する詳細は、そのホストのハードウェアのマニュアルを参照してください。

重要

VDSM が提供する watchdog デーモンを妨げる可能性があるため、サードパーティーのウォッチドッグを Red Hat Enterprise Linux ホストにインストールしないでください。

4.2.1. Red Hat Enterprise Linux ホストのリポジトリーの有効化

Red Hat Enterprise Linux マシンをホストとして使用するには、システムをコンテンツ配信ネットワークに登録し、**Red Hat Enterprise Linux Server** および **Red Hat Virtualization** サブスクリプションを割り当て、ホストのリポジトリー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
```

2. **Red Hat Enterprise Linux Server** および **Red Hat Virtualization** 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=poolid
```

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
```

有効なリポジトリーをすべて一覧表示するには、以下のコマンドを実行します。

```
# yum repolist
```

4. リポジトリーを設定します。

```
# subscription-manager repos \
    --disable='*' \
```

```
    --enable=rhel-7-server-rpms \
    --enable=rhel-7-server-rhv-4-mgmt-agent-rpms \
    --enable=rhel-7-server-ansible-2.9-rpms
```

IBM POWER8 ハードウェアに Red Hat Enterprise Linux 7 ホスト（リトルエンディアン）の場合：

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

IBM POWER9（リトルエンディアン）ハードウェアに Red Hat Enterprise Linux 7 ホストをインストールする場合：

```
# subscription-manager repos \
    --disable='*' \
    --enable=rhel-7-server-rhv-4-mgmt-agent-for-power-9-rpms \
    --enable=rhel-7-for-power-9-rpms
```

5. 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。

```
# yum update
```

6. マシンを再起動します。

4.2.2. Red Hat Enterprise Linux ホストへの Cockpit のインストール

ホストのリソースの監視および管理タスクの実施のために、Cockpit をインストールすることができます。

手順

1. dashboard パッケージをインストールします。

```
# yum install cockpit-ovirt-dashboard
```

2. **cockpit.socket** サービスを有効にして起動します。

```
# systemctl enable cockpit.socket
# systemctl start cockpit.socket
```

3. ファイアウォールで Cockpit がアクティブなサービスかどうかを確認します。

```
# firewall-cmd --list-services
```

cockpit のリストが表示されるはずです。表示されない場合には、root 権限で以下のコマンドを入力し、**cockpit** をサービスとしてファイアウォールに追加します。

```
# firewall-cmd --permanent --add-service=cockpit
```

--permanent オプションは、再起動後も **cockpit** サービスをアクティブな状態を維持します。

https://HostFQDNorIP:9090 で Cockpit Web インターフェースにログインできます。

第5章 RED HAT VIRTUALIZATION MANAGER のインストール

デプロイメントプロセス中に RHV-M Appliance がインストールされている。ただし、必要な場合は、インストールを開始する前にデプロイメントホストにインストールすることができます。

```
# yum install rhvm-appliance
```

Manager 用仮想マシンの手動インストールはサポートされていません。

5.1. COCKPIT を使用したセルフホストエンジンのデプロイ

Cockpit を使用してご自分の環境の情報を収集して、セルフホストエンジンをデプロイします。これは推奨される方法です。Red Hat Virtualization Host では Cockpit がデフォルトで有効化されていますが、Red Hat Enterprise Linux ホストに Cockpit をインストールすることもできます。

前提条件

- Manager およびデプロイメントホスト用の完全修飾ドメイン名が準備されています。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。

手順

1. **https://HostIPorFQDN:9090** で Cockpit にログインし、**Virtualization → Hosted Engine** をクリックします。
2. **Hosted Engine** オプションの下の **Start** をクリックします。
3. Manager 用仮想マシンに関する情報を入力します。
    a. **Engine VM FQDN** を入力します。これはベースホストではなく、Manager 用仮想マシンの FQDN になります。
    b. Manager 用仮想マシンの **MAC アドレス** を入力します。あるいは、無作為に生成される MAC アドレスを適用します。
    c. **Network Configuration** のドロップダウンリストから、**DHCP** または **Static** のいずれかを選択します。

注記

IPv6 については、Red Hat Virtualization でサポートされるのは静的なアドレスだけです。

- **DHCP** を選択した場合には、ホスト名が DHCP から受け取るアドレスに解決されるように、Manager 用仮想マシンの DHCP 予約がなければなりません。その MAC アドレスを **MAC Address** フィールドで指定します。
- **Static** を選択した場合には、以下の情報を入力します。
    - **VM IP Address**: 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。

- **Gateway Address**: ゲートウェイの IP アドレス
- **DNS Servers**: DNS サーバーの IP アドレス

d. **Bridge Interface** のドロップダウンリストから、ブリッジインターフェースを選択します。

e. **Root Password** に仮想マシンの root パスワードを入力し、それを確認します。

f. **Root SSH Access** で、root に SSH アクセスを許可するかどうかを指定します。

g. **Number of Virtual CPUs** に、仮想マシンの CPU 数を入力します。

h. **Memory Size (MiB)** に、メモリーのサイズを入力します。使用可能なメモリー容量が入力フィールドの横に表示されます。

4. オプションとして、**Advanced** フィールドを展開します。

a. **Root SSH Public Key** に、root ユーザーが Manager 用仮想マシンにアクセスする際に使用する公開鍵を入力します。

b. **Edit Hosts File** のチェックボックスを選択/選択解除して、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。

c. **Bridge Name** で管理ブリッジの名前を変更します。あるいは、デフォルトの **ovirtmgmt** を適用します。

d. **Gateway Address** に、管理ブリッジのゲートウェイ IP アドレスを入力します。

e. **Host FQDN** に、Manager に追加する第 1 ホストの FQDN を入力します。これは、デプロイメントを実行しているベースホストの FQDN です。

5. **Next** をクリックします。

6. **Admin Portal Password** に、**admin@internal** ユーザーのパスワードを入力し、それを確認します。

7. イベント通知を設定します。

a. **Server Name** および **Server Port Number** に、SMTP サーバーの名前およびポート番号を入力します。

b. **Sender E-Mail Address** に、送信元のメールアドレスを入力します。

c. **Recipient E-Mail Addresses** に、受け取り先のメールアドレスを入力します。

8. **Next** をクリックします。

9. Manager およびその仮想マシンの設定を見直します。情報が正しければ、**Prepare VM** をクリックします。

10. 仮想マシンのインストールが完了したら、**Next** をクリックします。

11. **Storage Type** のドロップダウンリストからストレージのタイプを選択し、セルフホストエンジン用ストレージドメインの情報を入力します。

- NFS の場合:

a. **Storage Connection** フィールドに、完全なアドレスおよびストレージへのパスを入力します。

b. 必要に応じて、**Mount Options** にマウントオプションを入力します。

c. **Disk Size (GiB)** にディスクのサイズを入力します。

d. **NFS Version** のドロップダウンリストから、NFS のバージョンを選択します。

e. **Storage Domain Name** にストレージのドメイン名を入力します。

- iSCSI の場合:

a. **Portal IP Address**、**Portal Port**、**Portal Username**、および **Portal Password** に、ポータルの IP アドレス、ポート、ユーザー名、およびパスワードを入力します。

b. **Retrieve Target List** をクリックしてターゲットを選択します。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することができます。

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 Multipath』 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。

c. **Disk Size (GiB)** にディスクのサイズを入力します。

d. **Discovery Username** および **Discovery Password** に、ターゲット自動検出時のユーザー名およびそのパスワードを入力します。

- ファイバーチャネルの場合:

a. **LUN ID** を入力します。ホストのバスアダプターが設定、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、『**Administration Guide**』 の 「 Reusing LUNs 」 を参照してください。

b. **Disk Size (GiB)** にディスクのサイズを入力します。

- Red Hat Gluster Storage の場合:

a. **Storage Connection** フィールドに、完全なアドレスおよびストレージへのパスを入力します。

b. 必要に応じて、**Mount Options** にマウントオプションを入力します。

c. **Disk Size (GiB)** にディスクのサイズを入力します。

12. **Next** をクリックします。

13. ストレージの設定を見直します。情報が正しければ、**Finish Deployment** をクリックします。

14. デプロイメントが完了したら、**Close** をクリックします。

1 つのデータセンター、クラスター、ホスト、ストレージドメイン、および Manager 用仮想マシンがすでに稼働しているはずです。管理ポータルにログインして、さらにリソースを追加することができます。

15. オプションとして、**ovirt-engine-extension-aaa-ldap-setup** インタラクティブセットアップスクリプトを使用してディレクトリーサーバーを追加して、環境にユーザーを追加することができます。詳細は、『**Administration Guide**』の「Configuring an External LDAP Provider」を参照してください。

セルフホストエンジンのステータスが Cockpit の **Virtualization → Hosted Engine** タブに表示されます。管理ポータルで、Manager 用仮想マシン、仮想マシンを実行しているホスト、およびセルフホストエンジン用ストレージドメインに金色の王冠のフラグが付けられます。

Red Hat Virtualization Manager リポジトリーを有効にすることは、自動インストールの一部ではありません。Manager 用仮想マシンにログインして、コンテンツ配信ネットワークに登録します。

5.2. RED HAT VIRTUALIZATION MANAGER リポジトリーの有効化

システムを Red Hat Subscription Manager に登録し、**Red Hat Virtualization Manager** のサブスクリプションをアタッチして Manager のリポジトリーを有効にします。

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
```

有効なリポジトリーをすべて一覧表示するには、以下のコマンドを実行します。

```
# yum repolist
```

4. リポジトリーを設定します。

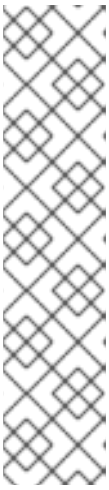
```
# subscription-manager repos \
    --disable='*' \
    --enable=rhel-7-server-rpms \
    --enable=rhel-7-server-supplementary-rpms \
    --enable=rhel-7-server-rhv-4.3-manager-rpms \
    --enable=rhel-7-server-rhv-4-manager-tools-rpms \
    --enable=rhel-7-server-ansible-2.9-rpms \
    --enable=jb-eap-7.2-for-rhel-7-server-rpms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

次に管理ポータルにログインします。ここで、環境にホストおよびストレージを追加することができます。

5.3. 管理ポータルへの接続

Web ブラウザーを使って管理ポータルへアクセスします。

1. Web ブラウザーで、**https://manager-fqdn/ovirt-engine** に移動します。**manager-fqdn** は、インストール時に指定した FQDN に置き換えます。



注記

別のホスト名または IP アドレスを使用して、管理ポータルにアクセスすることができます。これには、**/etc/ovirt-engine/engine.conf.d/** に設定ファイルを追加する必要があります。たとえば、以下のような構成です。

```
# vi /etc/ovirt-engine/engine.conf.d/99-custom-sso-setup.conf
SSO_ALTERNATE_ENGINE_FQDNS="alias1.example.com
alias2.example.com"
```

代替ホスト名の一覧は、スペースで区切る必要があります。また、Manager の IP アドレスを一覧に追加することもできますが、DNS で解決可能なホスト名の代わりに IP アドレスを使用することは推奨していません。

2. **管理ポータル** をクリックすると、SSO ログインページが表示されます。SSO ログインにより、管理ポータルと VM ポータルに同時にログインすることができます。

3. **ユーザー名** と **パスワード** を入力します。初回ログインの場合は、ユーザー名 **admin** とインストール時に指定したパスワードを使用してください。

4. 認証する **プロファイル** を選択します。内部の **admin** ユーザー名を使用してログインする場合は、プロファイルに **internal** を選択します。

5. **ログイン** をクリックします。

6. 管理ポータルは複数の言語で表示することができます。デフォルトの選択は、お使いの Web ブラウザーのロケール設定をベースに決定されます。デフォルト以外の言語で管理ポータルを表示する場合は、ウェルカムページのドロップダウンリストから任意の言語を選択してください。

Red Hat Virtualization 管理ポータルからログアウトするには、ヘッダーバーでユーザー名をクリックして、**サインアウト** をクリックします。すべてのポータルからログアウトされ、Manager のウェルカム画面が表示されます。

第6章 RED HAT VIRTUALIZATION 用ホストのインストール

Red Hat Virtualization は、Red Hat Virtualization Hosts (RHVH) および Red Hat Enterprise Linux ホスト の 2 つのタイプのホストをサポートしています。環境に応じて、1 タイプのみまたは両方のタイプを使用することができます。移行や高可用性などの機能を利用するには、少なくとも 2 台のホストが必要です。

ネットワーク設定に関する情報は、「ホストネットワーク設定の推奨プラクティス」 を参照してください。

重要

SELinux は インストール時に enforcing モードに設定されます。確認するには、**getenforce** を実行します。Red Hat Virtualization 環境をサポートするには、すべてのホストと Manager で SELinux を enforcing モードに設定する必要があります。

表6.1 ホストタイプ

ホストタイプ	別名	説明
Red Hat Virtualization Host	RHVH、シンホスト	Red Hat Enterprise Linux をベースとする最小限のオペレーティングシステム。カスタマーポータルから ISO ファイルとして配布され、マシンがホストとして機能するためのパッケージのみが含まれています。
Red Hat Enterprise Linux ホスト	RHEL ホスト、シックホスト	適切なサブスクリプションがアタッチされた Red Hat Enterprise Linux システムは、ホストとして使用することができます。

ホストの互換性

新規データセンターの作成時に、互換バージョンを設定することができます。データセンター内の全ホストに適した互換バージョンを選択します。一旦設定されると、それよりも古いバージョンに変更することはできません。Red Hat Virtualization を新規インストールした場合には、最新の互換バージョンが Default データセンターと Default クラスターに設定されるので、それ以前の互換バージョンを使用するには、追加でデータセンターおよびクラスターを作成する必要があります。互換バージョンに関する詳細は、Red Hat Virtualization のライフサイクル の **Red Hat Virtualization Manager の互換性** を参照してください。

6.1. RED HAT VIRTUALIZATION HOST

6.1.1. Red Hat Virtualization Host のインストール

Red Hat Virtualization Host (RHVH) は、Red Hat Virtualization 環境でハイパーバイザーとして機能する物理マシンの簡単な設定方法を提供するために設計された、Red Hat Enterprise Linux をベースとする最小構成のオペレーティングシステムです。この最小構成のオペレーティングシステムには、マシン

がハイパーバイザーとして機能するのに必要なパッケージのみが含まれており、ホストの監視や管理タスクの実行用に Cockpit Web インターフェースが備えられています。最低限のブラウザー要件については、http://cockpit-project.org/running.html を参照してください。

RHVH は NIST SP 800-53 パーティショニングの要件をサポートし、より強固なセキュリティーを提供します。RHVH は、デフォルトで NIST 800-53 パーティションレイアウトを使用します。

ホストは最低限の ホスト要件 を満たしている必要があります。

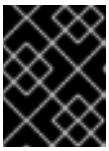
手順

1. カスタマーポータルから RHVH ISO イメージをダウンロードします。
   a. カスタマーポータル (https://access.redhat.com) にログインします。
   b. メニューバーの **ダウンロード** をクリックします。
   c. **Red Hat Virtualization** をクリックします。スクロールして **Download Latest** をクリックして、製品のダウンロードページにアクセスします。
   d. **RHV 4.3 の Hypervisor Image に移動し、今すぐダウンロード** をクリックします。
   e. ブート可能なメディアデバイスを作成します。詳細は、『**Red Hat Enterprise Linux インストールガイド**』 の「メディアの作成」を参照してください。
2. RHVH のインストール先となるマシンを起動し、準備したインストールメディアから起動します。
3. 起動メニューから **Install RHVH 4.3 を** 選択し、**Enter** を押します。

注記

また、**Tab** キーを押してカーネルパラメーターを編集することもできます。カーネルパラメーターはスペースで区切る必要があります。また、指定したカーネルパラメーターを使用してシステムを起動するには、**Enter** キーを押します。**Esc** キーを押してカーネルパラメーターへの変更を消去し、起動メニューに戻ります。

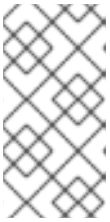
4. 言語を選択し、**Continue** をクリックします。
5. 日付と時刻 の画面から **タイムゾーンを** 選択し、完了 をクリックし **ます**。
6. キーボード画面からキーボードレイアウトを選択し 、 完了 をクリックし **ます**。
7. **インストール先** の画面から RHVH のインストール先のデバイスを選択します。オプションで暗号化を有効にします。**完了**をクリックします。



重要

Red Hat は、**自動構成のパーティション設定** オプションを使用することを強く推奨します。

8. **ネットワーク & ホスト名** の画面からネットワークを選択し、**設定** をクリックして接続の詳細を設定します。



注記

システムの起動するたびに接続を使用するには、**Automatically connect to this network when it is available** チェックボックスを選択します。詳細は、『**Red Hat Enterprise Linux 7 インストールガイド**』の「ネットワーク接続の編集」を参照してください。

ホスト名 フィールドにホスト名を **入力** し、完了 をクリックし **ます**。

9. オプションで **言語サポート**、**セキュリティーポリシー**、および Kdump を設定します。インストール **概要 画面の各セクションの詳細は、『Red Hat Enterprise Linux 7 インストールガイド』 の「Anaconda を使用** した Anaconda のインストール」を参照してください。

10. **インストールの開始** をクリックします。

11. RHVH のインストールの際に root パスワードを設定して、オプションで追加のユーザーを作成します。

警告

ローカルのセキュリティー脆弱性が悪用される可能性があるため、Red Hat は RHVH に信頼できないユーザーを作成しないことを強く推奨します。

12. **再起動** をクリックしてインストールを完了します。

注記

RHVH の再起動時に、**nodectl check** はホストでヘルスチェックを実行し、コマンドラインへのログイン時に結果を表示します。**node status: OK** または **node status: DEGRADED** のメッセージはヘルスステータスを示します。**nodectl check** を実行して詳細情報を取得します。サービスはデフォルトで有効になっています。

6.1.2. Red Hat Virtualization Host のリポジトリーの有効化

更新を受け取るためにシステムを登録します。Red Hat Virtualization Host に必要なリポジトリーは 1 つだけです。本セクションでは、RHVH を コンテンツ配信ネットワーク または Red Hat Satellite 6 に登録する手順について説明します。

コンテンツ配信ネットワークへの RHVH の登録

1. **https://HostFQDNorIP:9090** で Cockpit Web インターフェースにログインします。

2. **サブスクリプション** に移動し、**システムの登録** をクリックして、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。**Red Hat Virtualization Host** のサブスクリプションが自動的にシステムにアタッチされます。

3. **Terminal** をクリックします。

4. **Red Hat Virtualization Host 7** リポジトリーを有効にして、Red Hat Virtualization Host に対する後続の更新を可能にします。

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

Red Hat Satellite 6 への RHVH の登録

1. **https://HostFQDNorIP:9090** で Cockpit Web インターフェースにログインします。
2. **Terminal** をクリックします。
3. RHVH を Red Hat Satellite 6 に登録します。

```
# rpm -Uvh http://satellite.example.com/pub/katello-ca-consumer-latest.noarch.rpm
# subscription-manager register --org="org_id"
# subscription-manager list --available
# subscription-manager attach --pool=pool_id
# subscription-manager repos \
  --disable='*' \
  --enable=rhel-7-server-rhvh-4-rpms
```

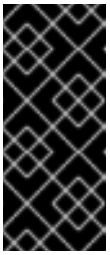
6.1.3. 高度なインストール

6.1.3.1. カスタムパーティション設定

Red Hat Virtualization Host (RHVH) でのカスタムパーティション設定は推奨されません。Red Hat は、**インストール先 画面** で **Automatically configure partitioning** オプションを使用することを強く推奨します。

インストールでカスタムのパーティション設定が必要な場合は、インストール時に **I will configure partitioning** オプションを選択します。ただし、以下の制限が適用される点に注意してください。

- **手動パーティション設定** ウィンドウで、デフォルトの **LVM シンプロビジョニング** オプションを選択する必要があります。
- 以下のディレクトリーが必要で、シンプロビジョニングされた論理ボリューム上になければなりません。
  - root (/)
  - **/home**
  - **/tmp**
  - **/var**
  - **/var/crash/**
  - **/var/log**
  - **/var/log/audit**



重要

/usr 用に別のパーティションを作成しないでください。別のパーティションを作成すると、インストールに失敗します。

/usr は、RHVH と共にバージョンを変更できる論理ボリューム上になければなりません。したがって、root (/) 上に残す必要があります。

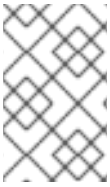
各パーティションに必要なストレージのサイズについては、「ストレージの要件」 を参照してください。

- **/boot** ディレクトリーは、標準のパーティションとして定義する必要があります。
- **/var** ディレクトリーは、別のボリュームまたはディスク上になければなりません。
- XFS または Ext4 ファイルシステムのみがサポートされます。

キックスタートファイルでの手動パーティション設定の定義

以下の例では、キックスタートファイルでパーティションを手動設定する方法を説明します。

```
clearpart --all
part /boot --fstype xfs --size=1000 --ondisk=sda
part pv.01 --size=42000 --grow
volgroup HostVG pv.01 --reserved-percent=20
logvol swap --vgname=HostVG --name=swap --fstype=swap --recommended
logvol none --vgname=HostVG --name=HostPool --thinpool --size=40000 --grow
logvol / --vgname=HostVG --name=root --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=6000 --grow
logvol /var --vgname=HostVG --name=var --thin --fstype=ext4 --poolname=HostPool
--fsoptions="defaults,discard" --size=15000
logvol /var/crash --vgname=HostVG --name=var_crash --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=10000
logvol /var/log --vgname=HostVG --name=var_log --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=8000
logvol /var/log/audit --vgname=HostVG --name=var_audit --thin --fstype=ext4 --poolname=HostPool -
-fsoptions="defaults,discard" --size=2000
logvol /home --vgname=HostVG --name=home --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=1000
logvol /tmp --vgname=HostVG --name=tmp --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=1000
```



注記

logvol --thinpool --grow を使用する場合は、シンプールを拡張するために、**volgroup --reserved-space** または **volgroup --reserved-percent** のボリュームグループに領域を確保する必要があります。

6.1.3.2. Red Hat Virtualization Host デプロイメントの自動化

物理メディアデバイスなしに Red Hat Virtualization Host (RHVH) をインストールすることができます。そのためには、インストールの質問に対する回答が含まれたキックスタートファイルを使用し、ネットワーク経由で PXE サーバーから起動します。

RHVH は Red Hat Enterprise Linux とほぼ同じ方法でインストールされるので、キックスタートファイ

ルを使用して PXE サーバーからインストールする手順の概要については、『Red Hat Enterprise Linux インストールガイド』の **「キックスタートを使ったインストール」** を参照してください。RHVH に固有の手順 (Red Hat Satellite を使用した RHVH のデプロイメントを例として使用) については、この後に説明します。

RHVH の自動デプロイメントは、以下の 3 つのステージで構成されます。

- 「インストール環境の準備」
- 「PXE サーバーおよびブートローダーの設定」
- 「キックスタートファイルの作成および実行」

6.1.3.2.1. インストール環境の準備

1. カスタマーポータル にログインします。
2. メニューバーの **ダウンロード** をクリックします。
3. **Red Hat Virtualization** をクリックします。スクロールして **Download Latest** をクリックして、製品のダウンロードページにアクセスします。
4. **RHV 4.3 の Hypervisor Image に移動し、今すぐダウンロード** をクリックします。
5. RHVH ISO イメージをネットワーク経由で提供できるようにします。**『Red Hat Enterprise Linux インストールガイド』** の 「インストールソース - ネットワーク」 を参照してください。
6. RHVH ISO から **squashfs.img** ハイパーバイザーイメージファイルを抽出します。

```
# mount -o loop /path/to/RHVH-ISO /mnt/rhvh
# cp /mnt/rhvh/Packages/redhat-virtualization-host-image-update* /tmp
# cd /tmp
# rpm2cpio redhat-virtualization-host-image-update* | cpio -idmv
```

注記

/tmp/usr/share/redhat-virtualization-host/image/ ディレクトリーにある **squashfs.img** ファイルの名前は **redhat-virtualization-host-version_number_version.squashfs.img** です。物理マシンにインストールするためのハイパーバイザーイメージが含まれます。これは、Anaconda **inst.stage2** オプションで使用される **/LiveOS/squashfs.img** ファイルと混同しないでください。

6.1.3.2.2. PXE サーバーおよびブートローダーの設定

1. PXE サーバーを設定します。**『Red Hat Enterprise Linux インストールガイド』** の 「ネットワークからのインストールの準備」 を参照してください。
2. RHVH 起動イメージを **/tftpboot** ディレクトリーにコピーします。

```
# cp mnt/rhvh/images/pxeboot/{vmlinuz,initrd.img} /var/lib/tftpboot/pxelinux/
```

3. ブートローダー設定で RHVH 起動イメージを指定して、**rhvh** ラベルを作成します。

```
LABEL rhvh
```

```
MENU LABEL Install Red Hat Virtualization Host
KERNEL /var/lib/tftpboot/pxelinux/vmlinuz
APPEND initrd=/var/lib/tftpboot/pxelinux/initrd.img inst.stage2=URL/to/RHVH-ISO
```

Red Hat Satellite 用 RHVH ブートローダーの設定例

Red Hat Satellite からの情報を使用してホストをプロビジョニングする場合には、グローバルまたはホストグループレベルのパラメーターを作成し (ここでは **rhvh_image**)、ISO をマウントまたは抽出するディレクトリーの URL を定義する必要があります。

```
<%#
kind: PXELinux
name: RHVH PXELinux
%>
# Created for booting new hosts
#

DEFAULT rhvh

LABEL rhvh
KERNEL <%= @kernel %>
APPEND initrd=<%= @initrd %> inst.ks=<%= foreman_url("provision") %> inst.stage2=<%=
@host.params["rhvh_image"] %> intel_iommu=on console=tty0 console=ttyS1,115200n8
ssh_pwauth=1 local_boot_trigger=<%= foreman_url("built") %>
IPAPPEND 2
```

4. RHVH ISO の内容をローカルで利用可能な状態にし、たとえば HTTPD サーバーを使用して、ネットワークにエクスポートします。

```
# cp -a /mnt/rhvh/ /var/www/html/rhvh-install
# curl URL/to/RHVH-ISO/rhvh-install
```

6.1.3.2.3. キックスタートファイルの作成および実行

1. キックスタートファイルを作成し、ネットワーク経由で提供できるようにします。『**Red Hat Enterprise Linux インストールガイド**』の「キックスタートを使ったインストール」を参照してください。

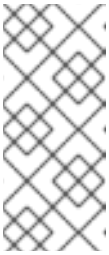
2. キックスタートファイルは以下に示す RHV 固有の要件を満たす必要があります。

   - RHVH には **%packages** セクションは必要ありません。代わりに、**liveimg** オプションを使用して、RHVH ISO イメージからの **redhat-virtualization-host-version_number_version.squashfs.img** ファイルを指定します。

     ```
     liveimg --url=example.com/tmp/usr/share/redhat-virtualization-host/image/redhat-virtualization-host-version_number_version.squashfs.img
     ```

   - 自動パーティション設定を強く推奨します。

     ```
     autopart --type=thinp
     ```



注記

自動パーティション設定では、シンプロビジョニングを使用する必要があります。

/**home** は必須のディレクトリーであるため、RHVH では **--no-home** オプションは機能しません。

インストールで手動パーティション設定が必要な場合は、「カスタムパーティション設定」 でパーティション設定に適用される制限の一覧およびキックスタートファイルでの手動パーティション設定の例を確認してください。

- **nodectl init** コマンドを呼び出す **%post** セクションが必要です。

```
%post
nodectl init
%end
```

RHVH を Own にデプロイするキックスタートの例

このキックスタートの例では、RHVH のデプロイ方法を示しています。必要に応じて、コマンドとオプションをさらに追加してください。

```
liveimg --url=http://FQDN/tmp/usr/share/redhat-virtualization-host/image/redhat-virtualization-host-version_number_version.squashfs.img
clearpart --all
autopart --type=thinp
rootpw --plaintext ovirt
timezone --utc America/Phoenix
zerombr
text

reboot

%post --erroronfail
nodectl init
%end
```

Satellite からの登録およびネットワーク設定を使用した RHVH のデプロイのキックスタート例

このキックスタートの例では、Red Hat Satellite からの情報を使用してホストネットワークを設定し、ホストを Satellite サーバーに登録します。グローバルまたはホストグループレベルのパラメーターを作成し (ここでは **rhvh_image**)、**squashfs.img** ファイルを格納するディレクトリーの URL を定義する必要があります。**ntp_server1** もグローバルまたはホストグループレベルの変数です。

```
<%#
kind: provision
name: RHVH Kickstart default
oses:
- RHVH
%>
install
liveimg --url=<%= @host.params['rhvh_image'] %>squashfs.img
```

```
network --bootproto static --ip=<%= @host.ip %> --netmask=<%= @host.subnet.mask
%> --gateway=<%= @host.subnet.gateway %> --nameserver=<%=
@host.subnet.dns_primary %> --hostname <%= @host.name %>

zerombr
clearpart --all
autopart --type=thinp

rootpw --iscrypted <%= root_pass %>

# installation answers
lang en_US.UTF-8
timezone <%= @host.params['time-zone'] || 'UTC' %>
keyboard us
firewall --service=ssh
services --enabled=sshd

text
reboot

%post --log=/root/ks.post.log --erroronfail
nodectl init
<%= snippet 'subscription_manager_registration' %>
<%= snippet 'kickstart_networking_setup' %>
/usr/sbin/ntpdate -sub <%= @host.params['ntp_server1'] || '0.fedora.pool.ntp.org' %>
/usr/sbin/hwclock --systohc

/usr/bin/curl <%= foreman_url('built') %>

sync
systemctl reboot
%end
```

3. キックスタートファイルの場所を、PXE サーバーのブートローダー設定ファイルに追加します。

```
APPEND initrd=/var/tftpboot/pxelinux/initrd.img inst.stage2=URL/to/RHVH-ISO
inst.ks=URL/to/RHVH-ks.cfg
```

4. **『Red Hat Enterprise Linux インストールガイド』**の「PXE を使ったネットワークからの起動」に記載された手順に従って、RHVH をインストールします。

6.2. RED HAT ENTERPRISE LINUX ホスト

6.2.1. Red Hat Enterprise Linux ホストのインストール

Red Hat Enterprise Linux ホストは、**Red Hat Enterprise Linux Server** および **Red Hat Virtualization** サブスクリプションがアタッチされた、物理サーバーに Red Hat Enterprise Linux 7 の標準的な基本インストールをベースにしています。

詳細なインストール手順は『**標準的な {enterprise-linux-shortname} インストールの実行**』を参照してください。

ホストは最低限の ホスト要件 を満たしている必要があります。

重要

ホストの BIOS 設定で仮想化が有効になっている必要があります。ホストの BIOS 設定の変更に関する詳細は、そのホストのハードウェアのマニュアルを参照してください。

重要

VDSM が提供する watchdog デーモンを妨げる可能性があるため、サードパーティーのウォッチドッグを Red Hat Enterprise Linux ホストにインストールしないでください。

6.2.2. Red Hat Enterprise Linux ホストのリポジトリーの有効化

Red Hat Enterprise Linux マシンをホストとして使用するには、システムをコンテンツ配信ネットワークに登録し、**Red Hat Enterprise Linux Server** および **Red Hat Virtualization** サブスクリプションを割り当て、ホストのリポジトリー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
```

2. **Red Hat Enterprise Linux Server** および **Red Hat Virtualization** 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=poolid
```

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
```

有効なリポジトリーをすべて一覧表示するには、以下のコマンドを実行します。

```
# yum repolist
```

4. リポジトリーを設定します。

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

```
    --enable=rhel-7-server-rhv-4-mgmt-agent-rpms \
    --enable=rhel-7-server-ansible-2.9-rpms
```

IBM POWER8 ハードウェアに Red Hat Enterprise Linux 7 ホスト（リトルエンディアン）の場合：

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

IBM POWER9（リトルエンディアン）ハードウェアに Red Hat Enterprise Linux 7 ホストをインストールする場合：

```
# subscription-manager repos \
    --disable='*' \
    --enable=rhel-7-server-rhv-4-mgmt-agent-for-power-9-rpms \
    --enable=rhel-7-for-power-9-rpms
```

5. 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。

```
# yum update
```

6. マシンを再起動します。

6.2.3. Red Hat Enterprise Linux ホストへの Cockpit のインストール

ホストのリソースの監視および管理タスクの実施のために、Cockpit をインストールすることができます。

手順

1. dashboard パッケージをインストールします。

```
# yum install cockpit-ovirt-dashboard
```

2. **cockpit.socket** サービスを有効にして起動します。

```
# systemctl enable cockpit.socket
# systemctl start cockpit.socket
```

3. ファイアウォールで Cockpit がアクティブなサービスかどうかを確認します。

```
# firewall-cmd --list-services
```

cockpit のリストが表示されるはずです。表示されない場合には、root 権限で以下のコマンドを入力し、**cockpit** をサービスとしてファイアウォールに追加します。

```
# firewall-cmd --permanent --add-service=cockpit
```

--permanent オプションは、再起動後も **cockpit** サービスをアクティブな状態を維持します。

https://HostFQDNorIP:9090 で Cockpit Web インターフェースにログインできます。

6.3. ホストネットワーク設定の推奨プラクティス

お使いのネットワーク環境が複雑な場合には、ホストを Red Hat Virtualization Manager に追加する前に、ホストネットワークを手動で設定しなければならない場合があります。

Red Hatでは、以下に示すホストネットワーク設定のプラクティスを推奨しています。

- Cockpit を使用してネットワークを設定する。**nmtui** または **nmcli** を使用することもできます。
- セルフホストエンジンのデプロイメントまたは Manager へのホスト追加にネットワークが必要ない場合には、ホストを Manager に追加した後に、管理ポータルでネットワークを設定する。『 Creating a New Logical Network in a Data Center or Cluster 』を参照してください。
- 以下の命名規則を使用する。
  - VLAN デバイス: **VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD**
  - VLAN インターフェース: **physical_device.VLAN_ID** (例: **eth0.23**, **eth1.128**, **enp3s0.50**)
  - ボンディングインターフェース: **bondnumber** (例: **bond0**, **bond1**)
  - ボンディングインテリアの VLAN: **bondnumber.VLAN_ID** (例: **bond0.50**, **bond1.128**)
- ネットワークボンディング を使用する。ネットワークチーミングは Red Hat Virtualization でサポートされておらず、ホストを使用してセルフホストエンジンをデプロイするか、Manager に追加されるとエラーが発生します。
- 推奨されるボンディングモードを使用する。
  - 仮想マシンが **ovirtmgmt** ネットワークを使用しない場合には、ネットワークではサポートされるいずれかのボンディングモードが使用されます。
  - 仮想マシンが **ovirtmgmt** ネットワークを使用する場合には、**「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。
  - 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** です。お使いのスイッチがリンクアグリゲーション制御プロトコル (LACP) に対応していない場合には、**(Mode 1) Active-Backup** を使用してください。詳細は、「ボンドモード」を参照してください。
- 以下の例に示すように、物理 NIC 上に VLAN を設定する (以下の例では **nmcli** を使用していますが、任意のツールを使用することができます)。

```
# nmcli connection add type vlan con-name vlan50 ifname eth0.50 dev eth0 id 50
# nmcli con mod vlan50 +ipv4.dns 8.8.8.8 +ipv4.addresses 123.123.0.1/24 +ivp4.gateway
123.123.0.254
```

- 以下の例に示すように、ボンディング上に VLAN を設定する (以下の例では **nmcli** を使用していますが、任意のツールを使用することができます)。

```
# nmcli connection add type bond con-name bond0 ifname bond0 bond.options
"mode=active-backup,miimon=100" ipv4.method disabled ipv6.method ignore
# nmcli connection add type ethernet con-name eth0 ifname eth0 master bond0 slave-type
bond
# nmcli connection add type ethernet con-name eth1 ifname eth1 master bond0 slave-type
```

```
bond
# nmcli connection add type vlan con-name vlan50 ifname bond0.50 dev bond0 id 50
# nmcli con mod vlan50 +ipv4.dns 8.8.8.8 +ipv4.addresses 123.123.0.1/24 +ivp4.gateway
123.123.0.254
```

- **firewalld** を無効にしないでください。
- ホストを Manager に追加した後に、管理ポータルでファイアウォールルールをカスタマイズする。「 ホストファイアウォールルールの 設定」を参照してください。

重要

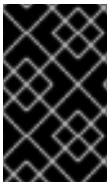
静的 IPv6 アドレスを使用する管理ブリッジを作成する場合は、ホストを追加する前にインターフェース設定(ifcfg)ファイルでネットワークマネージャーの制御を無効にします。詳細は、https://access.redhat.com/solutions/3981311 を参照してください。

6.4. RED HAT VIRTUALIZATION MANAGER へのセルフホストエンジンノードの追加

セルフホストエンジンノードは、通常のホストと同じ方法で追加することができますが、セルフホストエンジンノードとしてホストをデプロイする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することができます。セルフホストエンジン環境に通常のホストをアタッチすることもできますが、Manager 用仮想マシンをホストすることはできません。Red Hat では、Manager 用仮想マシンが高可用性を確保するために、セルフホストエンジンノードを少なくとも 2 つ用意することを推奨します。追加ホストは、REST API を使用して追加することもできます。『**REST API Guide**』の 「 Hosts 」 を参照してください。

前提条件

- セルフホスト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エンジン設定を削除してください。「 セルフホストエンジン環境からのホストの削除」を参照してください。



重要

静的 IPv6 アドレスを使用する管理ブリッジを作成する場合は、ホストを追加する前にインターフェース設定(ifcfg)ファイルでネットワークマネージャーの制御を無効にします。詳細は、https://access.redhat.com/solutions/3981311 を参照してください。

手順

1. 管理ポータルで **コンピュート → ホスト** をクリックします。
2. **新規作成** をクリックします。
   ホストの追加設定の詳細は、『**Administration Guide**』 の 「 Explanation of Settings and Controls in the New Host and Edit Host Windows 」 を参照してください。
3. ドロップダウンリストを使用して、新規ホスト用の **データセンター** および **ホストクラスター** を選択します。
4. 新規ホストの **名前** と **アドレス** を入力します。**SSH ポート** フィールドには、標準の SSH ポートであるポート 22 が自動入力されます。
5. Manager がホストにアクセスするために使用する認証メソッドを選択します。

- パスワード認証を使用するには、root ユーザーのパスワードを入力します。
- または、**SSH 公開鍵** フィールドに表示される鍵をホスト上の **/root/.ssh/authorized_keys** にコピーして、公開鍵認証を使用します。

6. ホストにサポート対象の電源管理カードが搭載されている場合には、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、『**Administration Guide**』の「Host Power Management Settings Explained」を参照してください。
7. **ホストエンジン** タブをクリックします。
8. **デプロイ** を選択します。
9. **OK** をクリックします。

6.5. RED HAT VIRTUALIZATION MANAGER への通常のホストの追加

Red Hat Virtualization 環境にホストを追加するには、仮想化のチェック、パッケージのインストール、およびブリッジの作成の各ステップをプラットフォームで完了する必要があるため、多少時間がかかります。

重要

静的 IPv6 アドレスを使用する管理ブリッジを作成する場合は、ホストを追加する前にインターフェース設定(ifcfg)ファイルでネットワークマネージャーの制御を無効にします。詳細は、https://access.redhat.com/solutions/3981311 を参照してください。

手順

1. 管理ポータルから **コンピュート → ホスト** をクリックします。
2. **新規作成** をクリックします。
3. ドロップダウンリストを使用して、新規ホスト用の **データセンター** および **ホストクラスター** を選択します。
4. 新規ホストの **名前** と **アドレス** を入力します。**SSH ポート** フィールドには、標準の SSH ポートであるポート 22 が自動入力されます。
5. Manager がホストにアクセスするために使用する認証メソッドを選択します。
   - パスワード認証を使用するには、root ユーザーのパスワードを入力します。
   - または、**SSH 公開鍵** フィールドに表示される鍵をホスト上の **/root/.ssh/authorized_keys** にコピーして、公開鍵認証を使用します。
6. オプションとして、**詳細パラメーター** 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する。
   - ホストの SSH フィンガープリントを追加し、セキュリティーを強化する。手動での追加または自動取得が可能です。

7. ホストにサポート対象の電源管理カードが搭載されている場合には、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、『 **Administration Guide** 』の 「 Host Power Management Settings Explained 」 を参照してください。

8. **OK** をクリックします。

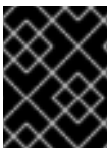
新規ホストが **Installing** のステータスでホスト一覧に表示され、**通知トレイ** () の **イベント** セクションでインストールの進捗状況を確認できます。しばらくすると、ホストのステータスが **Up** に変わります。

第7章 RED HAT VIRTUALIZATION 用ストレージの追加

新たな環境にデータドメインとしてストレージを追加します。Red Hat Virtualization 環境には少なくとも 1 つのデータドメインが必要ですが、さらに追加することを推奨します。

前の手順で準備したストレージを追加します。

- NFS
- iSCSI
- ファイバーチャネル (FCP)
- Red Hat Gluster Storage



重要

iSCSI ストレージを使用する場合には、新しいデータドメインはセルフホストエンジン用ストレージドメインと同じ iSCSI ターゲットを使用することはできません。

警告

セルフホストエンジン用ストレージドメインと同じデータセンター内に追加のデータドメインを作成することを強く推奨します。セルフホストエンジンをデータセンター内にデプロイする際に、アクティブなデータストレージドメインを 1 つしか用意していない場合、そのストレージドメインが破損しても、新しいストレージドメインを追加したり、破損したストレージドメインを削除することはできません。セルフホストエンジンを再デプロイしなければなりません。

7.1. NFS ストレージの追加

この手順では、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方法について説明します。

ISO またはエクスポートドメインが必要な場合にも、この手順を使用します。ただし、**ドメイン機能** の一覧から **ISO** または **Export** を選択します。

手順

1. 管理ポータルで **ストレージ → ドメイン** をクリックします。
2. **新規ドメイン** をクリックします。
3. ストレージドメインの **名前** を入力します。
4. **データセンター**、**ドメイン機能**、**ストレージタイプ**、**形式**、および **ホスト** 一覧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 **エクスポートパス** を入力します。エクスポートパスは、**123.123.0.10:/data** (IPv4 の場合)、**[2001:0:0:0:0:0:0:5db1]:/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することが可能です。

   a. **詳細パラメーター** をクリックします。

   b. **容量不足の警告** のフィールドに、パーセンテージ値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーに警告メッセージが表示され、ログに記録されます。

   c. **アクションをブロックする深刻な容量不足** のフィールドに GB 単位で値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーにエラーメッセージが表示され、ログに記録されます。容量を消費する新規アクションは、一時的であってもすべてブロックされます。

   d. 削除後にワイプするオプションを有効にするには、**削除後にワイプ** のチェックボックスを選択します。このオプションは、ドメインの作成後に編集することが可能ですが、その場合にはすでに存在していたディスクの「削除後にワイプ」プロパティーは変更されません。

7. **OK** をクリックします。

新しい NFS データドメインのステータスは、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。

7.2. ISCSI ストレージの追加

この手順では、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方法について説明します。

手順

1. **ストレージ → ドメイン** をクリックします。

2. **新規ドメイン** をクリックします。

3. 新規ストレージドメインの **名前** を入力します。

4. ドロップダウンリストから **データセンター** を選択します。

5. **ドメイン機能** に**データ** を、**ストレージタイプ** に **iSCSI** を、それぞれ選択します。

6. **ホスト** にアクティブなホストを選択します。

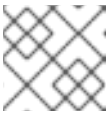
重要

ストレージドメインへの通信は、直接 Manager からではなく、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。**新規ドメイン** ウィンドウでストレージタイプに iSCSI を選択すると、未使用の LUN が割り当てられた既知のターゲットが自動的に表示されます。ストレージの追加に使用す

るターゲットが表示されない場合には、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には、次の手順に進んでください。

a. **ターゲットを検出** をクリックし、ターゲットの検出オプションを有効にします。Manager がターゲットを検出してログインすると、**新規ドメイン** ウィンドウに、その環境では未使用の LUN が割り当てられたターゲットが自動的に表示されます。



注記

環境の外部で使用されている LUN も表示されます。

ターゲットを検出 のオプションを使用すると、多数のターゲットの 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。

b. **アドレス** 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. **ポート** フィールドには、ターゲットを参照する際にホストに接続するポートを入力します。デフォルトは **3260** です。

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

注記

REST API を使用して、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 Guide**』の「StorageServerConnectionExtensions: add」を参照してください。

e. **検出** をクリックします。

f. 検出結果から 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 **ログイン** をクリックします。複数のターゲットの場合は **全ターゲットにログイン** 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には、すべての必要なパスを通してターゲットを検出してログインする必要があります。ストレージドメインを変更してさらにパスを追加する方法は、現在サポートされていません。

8. 対象のターゲットの横に表示されている + ボタンをクリックします。エントリーが展開され、ターゲットにアタッチされている未使用の LUN がすべて表示されます。

9. ストレージドメインの作成に使用する各 LUN のチェックボックスにチェックを入れます。

10. オプションで、詳細パラメーターを設定することが可能です。

a. **詳細パラメーター** をクリックします。

b. **容量不足の警告** のフィールドに、パーセンテージ値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーに警告メッセージが表示され、ログに記録されます。

c. **アクションをブロックする深刻な容量不足** のフィールドに GB 単位で値を入力します。ス

トレージドメインの空き容量がこの値を下回ると、ユーザーにエラーメッセージが表示され、ログに記録されます。容量を消費する新規アクションは、一時的であってもすべてブロックされます。

d. 削除後にワイプするオプションを有効にするには、**削除後にワイプ** のチェックボックスを選択します。このオプションは、ドメインの作成後に編集することが可能ですが、その場合にはすでに存在していたディスクの「削除後にワイプ」プロパティーは変更されません。

e. **削除後に破棄** 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、「 Configuring iSCSI Multipathing 」の手順に従い、iSCSI ボンディングを完了します。

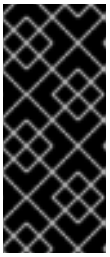
現在のストレージネットワークを iSCSI ボンディングに移行する場合は、「 Migrating a Logical Network to an iSCSI Bond 」を参照してください。

7.3. FCP ストレージの追加

この手順では、既存の FCP ストレージをデータドメインとして Red Hat Virtualization 環境にアタッチする方法について説明します。

手順

1. **ストレージ → ドメイン** をクリックします。
2. **新規ドメイン** をクリックします。
3. ストレージドメインの **名前** を入力します。
4. ドロップダウンリストから FCP **データセンター** を選択します。
適切な FCP データセンターがない場合には **(none)** を選択します。
5. ドロップダウンリストから **ドメイン機能** および **ストレージタイプ** を選択します。選択したデータセンターとの互換性がないストレージドメインタイプは選択できません。
6. **ホスト** のフィールドでアクティブなホストを 1 台選択します。データセンターで初めて作成するデータドメインでなければ、そのデータセンターの SPM ホストを選択する必要があります。



重要

ストレージドメインへの通信はすべて、Red Hat Virtualization Manager から直接ではなく、選択したホストを介して行われます。システムには、アクティブなホストが少なくとも 1 台存在し、選択したデータセンターにアタッチされている必要があります。ストレージドメインを設定する前には、全ホストがストレージデバイスにアクセスできる状態でなければなりません。

7. **新規ドメイン** ウィンドウで、ストレージタイプに **ファイバーチャネル** を選択した場合は、未使用の LUN が割り当てられた既知のターゲットが自動的に表示されます。**LUN ID** のチェックボックスを選択し、使用可能な LUN をすべて選択します。

8. オプションで、詳細パラメーターを設定することが可能です。

    a. **詳細パラメーター** をクリックします。

    b. **容量不足の警告** のフィールドに、パーセンテージ値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーに警告メッセージが表示され、ログに記録されます。

    c. **アクションをブロックする深刻な容量不足** のフィールドに GB 単位で値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーにエラーメッセージが表示され、ログに記録されます。容量を消費する新規アクションは、一時的であってもすべてブロックされます。

    d. 削除後にワイプするオプションを有効にするには、**削除後にワイプ** のチェックボックスを選択します。このオプションは、ドメインの作成後に編集することが可能ですが、その場合にはすでに存在していたディスクの「削除後にワイプ」プロパティーは変更されません。

    e. **削除後に破棄** 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。

7.4. RED HAT GLUSTER STORAGE の追加

Red Hat Virtualization で Red Hat Gluster Storage を使用するには、**『Configuring Red Hat Virtualization with Red Hat Gluster Storage』** を参照してください。

Red Hat Virtualization でサポートされる Red Hat Gluster Storage のバージョンについては、https://access.redhat.com/articles/2356261 を参照してください。

付録A セルフホストエンジンのデプロイメントのトラブルシューティング

セルフホストエンジンがすでにデプロイされているかどうかを確認するには、**hosted-engine --check-deployed** を実行します。セルフホストエンジンがデプロイされていない場合にだけ、エラーが表示されます。

A.1. MANAGER 用仮想マシンのトラブルシューティング

hosted-engine --vm-status を実行して Manager 用仮想マシンのステータスを確認します。

注記

Manager 用仮想マシンに加えた変更がステータスコマンドの出力に反映されるには、20 秒ほどかかります。

出力の **Engine status** ごとに、問題を特定または解決するためのアドバイスを以下に示します。

Engine status: "health": "good", "vm": "up" "detail": "up"

1. Manager 用仮想マシンが通常通りに稼働中の場合には、以下のような出力が表示されます。

```
--== Host 1 status ==--

Status up-to-date              : True
Hostname                       : hypervisor.example.com
Host ID                        : 1
Engine status                  : {"health": "good", "vm": "up", "detail": "up"}
Score                          : 3400
stopped                        : False
Local maintenance              : False
crc32                          : 99e57eba
Host timestamp                 : 248542
```

2. 出力は正常だが Manager に接続することができない場合は、ネットワーク接続を確認してください。

Engine status: "reason": "failed liveliness check", "health": "bad", "vm": "up", "detail": "up"

1. **health** が **bad** で **vm** が **up** の場合、HA サービスは Manager 用仮想マシンを再起動して Manager の復旧を試みます。数分以内に復旧しない場合は、コマンドラインからグローバルメンテナンスモードを有効にして、ホストを HA サービスの管理対象外にします。

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

2. コンソールに接続します。プロンプトが表示されたら、オペレーティングシステムの root パスワードを入力します。コンソールのオプションに関する詳細は、https://access.redhat.com/solutions/2221461 を参照してください。

```
# hosted-engine --console
```

3. Manager 用仮想マシンにログインして、オペレーティングシステムが動作していることを確認します。

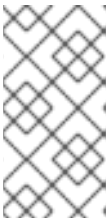
4. **ovirt-engine** サービスのステータスを確認します。

```
# systemctl status -l ovirt-engine
# journalctl -u ovirt-engine
```

5. **/var/log/messages**、**/var/log/ovirt-engine/engine.log**、および **/var/log/ovirt-engine/server.log** のログを確認します。

6. 問題を解決したら、セルフホストエンジンノードのいずれかから、手動で Manager 用仮想マシンを再起動します。

```
# hosted-engine --vm-shutdown
# hosted-engine --vm-start
```



注記

セルフホストエンジンノードがグローバルメンテナンスモードにある場合は、Manager 用仮想マシンを手動で再起動する必要があります。コマンドラインから **reboot** コマンドを送信して Manager 用仮想マシンを再起動しようとしても、Manager 用仮想マシンは電源オフのままです。設計上、このようになります。

7. Manager 用仮想マシンで **ovirt-engine** サービスが稼働中であることを確認します。

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

8. Manager 用仮想マシンが稼働中であることを確認した後は、コンソールセッションを終了して、メンテナンスモードを無効にし、HA サービスを再び有効にします。

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

Engine status: "vm": "down", "health": "bad", "detail": "unknown", "reason": "vm not running on this host"

1. 環境内に複数のホストがある場合は、現在別のホストが Manager 用仮想マシンの再起動を試みていないことを確認します。

2. グローバルメンテナンスモードにないことを確認します。

3. **/var/log/ovirt-hosted-engine-ha/agent.log** で、**ovirt-ha-agent** のログを確認します。

4. セルフホストエンジンノードのいずれかから、手動で Manager 用仮想マシンの再起動を試みます。

```
# hosted-engine --vm-shutdown
# hosted-engine --vm-start
```

Engine status: "vm": "unknown", "health": "unknown", "detail": "unknown", "reason": "failed to getVmStats"

このステータスは、**ovirt-ha-agent** が VDSM から仮想マシンの詳細を取得できなかったことを意味しています。

1. **/var/log/vdsm/vdsm.log** で VDSM のログを確認します。

2. **/var/log/ovirt-hosted-engine-ha/agent.log** で、**ovirt-ha-agent** のログを確認します。

Engine status: セルフホストエンジンの設定が共有ストレージから取得されていない
ステータス **が表示されると、共有ストレージからセルフホストエンジン設定は取得されていません。ovirt-ha-agent が実行されており、ストレージサーバーにアクセスできることを確認してくださいovirt-ha-agent** サービス、ストレージ、またはその両方に問題があります。

1. ホストで **ovirt-ha-agent** のステータスを確認します。

```
# systemctl status -l ovirt-ha-agent
# journalctl -u ovirt-ha-agent
```

2. **ovirt-ha-agent** がダウンしている場合は、再起動します。

```
# systemctl start ovirt-ha-agent
```

3. **/var/log/ovirt-hosted-engine-ha/agent.log** で、**ovirt-ha-agent** のログを確認します。
4. 共有ストレージに ping を送信できることを確認します。
5. 共有ストレージがマウントされているかどうかを確認します。

その他のトラブルシューティング用コマンド

重要

以下のコマンドのいずれかを実行してセルフホストエンジン環境のトラブルシューティングを行う必要がある場合には、Red Hat サポートまでご連絡ください。

- **hosted-engine --reinitialize-lockspace**: このコマンドは、sanlock ロックスペースが壊れている場合に使用します。sanlock ロックスペースを再初期化する前に、グローバルメンテナンスモードが有効で Manager 用仮想マシンが停止していることを確認してください。
- **hosted-engine --clean-metadata**: ホストのエージェントのメタデータをグローバルステータスデータベースから削除します。これにより、他のホストではすべて、このホストについての情報はなくなります。ターゲットのホストが停止状態でグローバルメンテナンスモードが有効であることを確認してください。
- **hosted-engine --check-liveliness**: このコマンドは、ovirt-engine サービスの liveliness ページを確認します。Web ブラウザーで **https://engine-fqdn/ovirt-engine/services/health/** に接続して確認することもできます。
- **hosted-engine --connect-storage**: このコマンドは、ホストと Manager 用仮想マシンに必要なすべてのストレージ接続の準備をするように VDSM に指示します。これは通常、セルフホストエンジンのデプロイ中にバックエンドで実行します。このコマンドを実行してストレージの問題のトラブルシューティングを行う必要がある場合には、グローバルメンテナンスモードを必ず有効にしてください。

A.2. 失敗したセルフホストエンジンのデプロイメントのクリーンアップ

セルフホストエンジンのデプロイメントが中断された場合には、その後のデプロイメントは失敗して、エラーメッセージが表示されます。このエラーはデプロイメントが失敗した段階によって異なります。

エラーメッセージが表示される場合には、デプロイメントホストでクリーンアップスクリプトを実行して、失敗したデプロイメントをクリーンアップすることができます。ただし、最良の手段は、ベースのオペレーティングシステムを再インストールして、デプロイメントを最初からやり直すことです。

注記

クリーンアップスクリプトには、以下の制約があります。

- スクリプトの実行中にネットワークの接続が中断すると、スクリプトによる管理ブリッジの削除や作業用ネットワーク設定の再作成に失敗する場合がある。
- スクリプトでは、失敗したデプロイメント中に使用された共有ストレージデバイスをクリーンアップすることができない。以降のデプロイメントで再使用するには、共有ストレージデバイスをクリーンアップする必要があります。

手順

1. **/usr/sbin/ovirt-hosted-engine-cleanup** を実行して **y** を選択し、失敗したセルフホストエンジンのデプロイメントで残されたものを削除します。

```
# /usr/sbin/ovirt-hosted-engine-cleanup
This will de-configure the host to run ovirt-hosted-engine-setup from scratch.
Caution, this operation should be used with care.
Are you sure you want to proceed? [y/n]
```

2. 同じ共有ストレージデバイスに再インストールするか、別の共有ストレージデバイスを選択するかを定義します。
   - 同じストレージドメインにインストール環境をデプロイする場合は、NFS、Gluster、PosixFS またはローカルストレージドメインのサーバーの適切なディレクトリーで以下のコマンドを実行し、そのストレージドメインをクリーンアップします。

     ```
     # rm -rf storage_location/*
     ```

   - iSCSI またはファイバーチャネルプロトコル (FCP) のストレージの場合は、https://access.redhat.com/solutions/2121581 で、ストレージのクリーンアップ方法を参照してください。
   - または、別の共有ストレージデバイスを選択します。
3. セルフホストエンジンを再デプロイします。

付録B リモートサーバーへのデータベースおよびサービスの移行

自動化されたインストール中にリモートデータベースおよびサービスを設定することはできませんが、インストール後にリモートサーバーに移行することができます。

B.1. リモートサーバーへのセルフホストエンジンデータベースの移行

Red Hat Virtualization Manager の初期設定後に、セルフホストエンジンのエンジンデータベースをリモートのデータベースサーバーに移行することができます。**engine-backup を使用してデータベースのバックアップを作成し、新しいデータベースサーバーに復元します。**

新しいデータベースサーバーで Red Hat Enterprise Linux 7 がインストールされ、必要なリポジトリーが有効になっている必要があります。

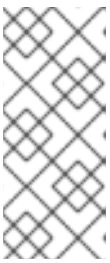
Red Hat Virtualization Manager リポジトリーの有効化

システムを Red Hat Subscription Manager に登録し、Red Hat Virtualization Manager のサブスクリプションをアタッチして Manager のリポジトリーを有効にします。

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
```

有効なリポジトリーをすべて一覧表示するには、以下のコマンドを実行します。

```
# yum repolist
```

4. リポジトリーを設定します。

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

リモートサーバーへのセルフホストエンジンデータベースの移行

1. セルフホストエンジンノードにログインし、環境を グローバル メンテナンスモードに配置します。これにより、高可用性エージェントを無効化して、この手順の実行中に **Manager** 用仮想マシンが移行されないようにします。

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

2. **Red Hat Virtualization Manager** マシンにログインして、**ovirt-engine** サービスを停止して、エンジンのバックアップに干渉しないようにします。

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

3. エンジン データベースのバックアップを作成します。

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

4. バックアップファイルを新規データベースサーバーにコピーします。

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

5. 新しいデータベースサーバーにログインし、**engine-backup** をインストールします。

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

6. 新しいデータベースサーバーでデータベースを復元します。**file_name** は、**Manager** からコピーされたバックアップファイルです。

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

7. データベースが移行されたので、**ovirt-engine** サービスを起動します。

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

8. セルフホストエンジンノードにログインし、メンテナンスモードをオフにして、高可用性エージェントを有効にします。

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

B.2. 別のマシンへの DATA WAREHOUSE の移行

本セクションでは、**Data Warehouse** データベースおよびサービスを **Red Hat Virtualization Manager** 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、各サービスは、**CPU** および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を回避することができます。

Data Warehouse サービスを移行して既存の **Data Warehouse** データベース(ovirt_engine_history)に接続するか、**Data Warehouse** サービスを移行する前に **Data Warehouse** データベースを別のマシンに移行することができます。**Data Warehouse** データベースを **Manager** でホストされる場合、**Data Warehouse** サービスに加えてデータベースを移行すると、**Manager** マシンのリソースの計算がさらに削減されます。データベースを、**Data Warehouse** サービスを移行するマシンと同じマシンに移行するか、**Manager** マシンと新しい **Data Warehouse** サービスマシンの両方とは別のマシンに移行することができます。

B.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 を実行してください。

Data Warehouse サービスのみを移行する場合は、「別のマシンへの Data Warehouse サービスの移行」 を参照してください。

新しいデータベースサーバーに Red Hat Enterprise Linux 7 がインストールされ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ーを有効にします。

Red Hat Virtualization Manager リポジトリーの有効化

システムを Red Hat Subscription Manager に登録し、Red Hat Virtualization Manager のサブスクリプションをアタッチして Manager のリポジトリーを有効にします。

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
```

有効なリポジトリーをすべて一覧表示するには、以下のコマンドを実行します。

```
# yum repolist
```

4. リポジトリーを設定します。

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

別のマシンへの Data Warehouse データベースの移行

1. **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=dwhdb --scope=files --file=file_name --
log=log_file_name
```

2. 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
```

3. **engine-backup** を新しいマシンにインストールします。

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

4. **PostgreSQL サーバーパッケージをインストールします。**

```
# yum install rh-postgresql10 rh-postgresql10-postgresql-contrib
```

5. **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。**

```
# scl enable rh-postgresql10 -- postgresql-setup --initdb
# systemctl enable rh-postgresql10-postgresql
# systemctl start rh-postgresql10-postgresql
```

6. **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=dwhdb --file=file_name --
log=log_file_name --provision-dwh-db --no-restore-permissions
```

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。

B.2.2. 別のマシンへの Data Warehouse サービスの移行

Red Hat Virtualization Manager マシンにインストールおよび設定した Data Warehouse サービスを、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) を移行する場合は、「別のマシンへの Data Warehouse データベースの移行」 を参照してください。

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必要があります。**

- 新たな Data Warehouse マシンを設定するには、以下の項目が必要です。
  - Manager /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。「別のマシンへの Data Warehouse データベースの移行」 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、そのマシンでデータベースの設定中に定義した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 サービスの無効化

B.2.2.1. 新たな Data Warehouse マシンの準備

Red Hat Virtualization のリポジトリーを有効にし、Red Hat Enterprise Linux 7 マシンに Data Warehouse 設定パッケージをインストールします。

1. 必要なリポジトリーを有効にします。
   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
```

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. **リポジトリーを設定します。**

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

2. **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。**

```
# yum update
```

3. **ovirt-engine-dwh-setup パッケージをインストールします。**

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

B.2.2.2. Manager マシンでの Data Warehouse サービスの停止

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には、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/opt/rh/rh-**

postgresql10/lib/pgsql/data/postgresql.conf ファイルを編集し、以下に一致するように listen_addresses 行を変更します。

```
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には、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には、デフォルトでアクセス権限が付与されます。

Data Warehouse データベースの設定および移行方法に関する詳細情報は、「別のマシンへの Data Warehouse データベースの移行」 を参照してください。

3. **postgresql サービスを再起動します。**

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

B.2.2.3. 新たな Data Warehouse マシンの設定

本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_CONFIG\/fqdn/d' \
    /etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

2. **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
```

3. **Enter を押して Data Warehouse を設定します。**

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

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 と入力して Enter キーを押し、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。

B.2.2.4. Manager マシンでの Data Warehouse サービスの無効化

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
```

3. **Data Warehouse サービスを無効にします。**

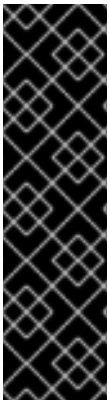
```
# systemctl disable ovirt-engine-dwhd.service
```

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。

B.3. 別のマシンへの WEBSOCKET プロキシーの移行



重要

Websocket プロキシーおよび noVNC は、テクノロジープレビュー機能としてのみ提供されています。テクノロジープレビューの機能は、Red Hat の本番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。これらの機能は、近々発表予定の製品機能をリリースに先駆けてご提供することにより、開発プロセスの中でお客様に機能性のテストとフィードバックをしていただくことを目的としています。詳しい情報は、「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。

セキュリティーまたはパフォーマンスの理由から、websocket プロキシーは Red Hat Virtualization Manager を実行しない別のマシンで実行できます。Manager マシンから別のマシンに Websocket プロキシーを移行する手順では、Manager マシンから Websocket プロキシー設定を削除してから、別のマシンにプロキシーをインストールする必要があります。

engine-cleanup コマンドを使用して、Manager マシンから websocket プロキシーを削除できます。

Manager マシンからの Websocket プロキシーの削除

1. **Manager マシンで engine-cleanup を実行して必要な設定を削除します。**

```
# engine-cleanup
```

2. **すべてのコンポーネントの削除を要求したら、No と 入力 し、Enter を押します。**

```
Do you want to remove all components? (Yes, No) [Yes]: No
```

3. **エンジンの削除を要求されたら No と 入力 し、Enter を押します。**

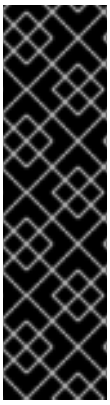
```
Do you want to remove the engine? (Yes, No) [Yes]: No
```

4. **Websocket プロキシーを削除するように要求されたら Yes と 入力 し、Enter を押します。**

```
Do you want to remove the WebSocket proxy? (Yes, No) [No]: Yes
```

他のコンポーネントを削除するように要求されたら No を選択します。

別のマシンへの Websocket プロキシーのインストール



重要

Websocket プロキシーおよび noVNC は、テクノロジープレビュー機能としてのみ提供されています。テクノロジープレビューの機能は、Red Hat の本番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。これらの機能は、近々発表予定の製品機能をリリースに先駆けてご提供することにより、開発プロセスの中でお客様に機能性のテストとフィードバックをしていただくことを目的としています。詳しい情報は、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。

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することができます。noVNC クライアントは Websocket を使用して VNC データを渡します。ただし、QEMU の VNC サーバーには Websocket サポートがないため、Websocket プロキシーはクライアントと VNC サーバーの間に配置する必要があります。Websocket プロキシーは、ネットワークへのアクセスがあるすべてのマシン (Manager マシンを含む) で実行可能です。

セキュリティーおよびパフォーマンスの理由から、ユーザーには別のマシンで Websocket プロキシーを設定することを推奨します。

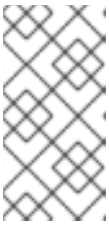
手順

1. Websocket プロキシーをインストールします。

```
# yum install ovirt-engine-websocket-proxy
```

2. engine-setup コマンドを実行して Websocket プロキシーを設定します。

```
# engine-setup
```



注記

rhvm パッケージもインストールされている場合は、このホストで Manager(Engine)を設定するか尋ねられた場合は No を選択します。

3. Enter を押して、engine-setup がマシンに Websocket プロキシーサーバーを設定できるようにします。

```
Configure WebSocket Proxy on this machine? (Yes, No) [Yes]:
```

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。仮想化ホストを使用している場合には、自動的に検出されたホスト名が間違っている可能性がある点に注意してください。**

```
Host fully qualified DNS name of this server [host.example.com]:
```

5. **Enter を押して engine-setup でファイアウォールを設定し、外部通信に必要なポートを開きます。engine-setup によるファイアウォール設定の変更を許可しない場合には、必要なポートを手動で開放する必要があります。**

```
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]:
```

6. **Manager マシンの FQDN を入力して、Enter を押します。**

```
Host fully qualified DNS name of the engine server []: manager.example.com
```

7. **Enter を押して、engine-setup が Manager マシンでアクションを実行することを許可するか、2 を押して手動でアクションを実行します。**

```
Setup will need to do some actions on the remote engine server. Either automatically, using
ssh as root to access it, or you will be prompted to manually perform each such action.
Please choose one of the following:
1 - Access remote engine server using ssh as root
2 - Perform each action manually, use files to copy content around
(1, 2) [1]:
```

a. **Enter を押してデフォルトの SSH ポート番号をそのまま使用するか、Manager マシンのポート番号を入力します。**

```
ssh port on remote engine server [22]:
```

b. **Manager マシンにログインするための root パスワードを入力して Enter キーを押します。**

```
root password on remote engine server engine_host.example.com:
```

8. **iptables ルールを現在の設定と異なる場合にそれらを確認するかどうかを選択します。**

```
Generated iptables rules are different from current ones.
Do you want to review them? (Yes, No) [No]:
```

9. **Enter を押して構成設定を確定します。**

```
--== CONFIGURATION PREVIEW ==--

Firewall manager                    : iptables
Update Firewall                     : True
Host FQDN                           : host.example.com
Configure WebSocket Proxy           : True
Engine Host FQDN                    : engine_host.example.com

Please confirm installation settings (OK, Cancel) [OK]:
```

Manager マシンが設定済みの Websocket プロキシーを使用するように設定するための説明が表示されます。

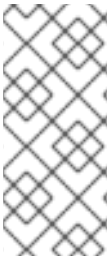
```
Manual actions are required on the engine host
in order to enroll certs for this host and configure the engine about it.

Please execute this command on the engine host:
   engine-config -s WebSocketProxy=host.example.com:6100
and than restart the engine service to make it effective
```

10. **Manager マシンへログインして、表示された説明に沿って操作を行います。**

```
# engine-config -s WebSocketProxy=host.example.com:6100
# systemctl restart ovirt-engine.service
```

付録C PCI パススルーを有効にするためのホストの設定



注記

これは、Red Hat Virtualization で SR-IOV を準備および設定する方法を示す一連のトピックの 1 つです。詳細は、「Setting Up and Configuring SR-IOV」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することができます。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には、最初にホストがメンテナンスモ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してください。詳細は、「PCI Device Requirements 」を参照してください。

PCI パススルーを有効にするためのホストの設定

1. BIOS の仮想化拡張機能および IOMMU 拡張機能を有効化してください。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。

2. ホストを Manager に追加する際に ホストデバイスパススルー & 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 フラグを有効にするには、「 Adding Standard Hosts to the Red Hat Virtualization Manager 」および「 Kernel Settings Explained 」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。

3. 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、『 Setting up an NVIDIA GPU for a virtual machine in Red

Hat Virtualization 』の「GPU device passthrough: Assigning a host GPU to a single virtual machine」を参照してください。

IOMMU の手動での有効化

1. grub 設定ファイルを編集して IOMMU を有効化します。

注記

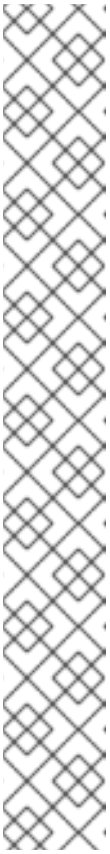
IBM POWER8 ハードウェアを使用している場合は、IOMMU がデフォルトで有効化されているので、この手順は飛ばしてください。

- 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=quiet console=tty0 ... amd_iommu=on
...
```



注記

intel_iommu=on または amd_iommu=on が機能する場合は、iommu=pt または amd_iommu=pt を追加できます。pt オプションでは、パススルーで使用するデバイスの IOMMU のみが有効化されて、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は、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、ホストは仮想マシンからの MSI 攻撃に晒されることになるため、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、以下のように設定してください。

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

2. **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。**

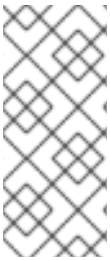
```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

```
# reboot
```

SR-IOV を有効にして専用の仮想 NIC を仮想マシンに割り当てるには、https://access.redhat.com/articles/2335291 を参照してください。

付録D RED HAT VIRTUALIZATION MANAGER の削除

engine-cleanup コマンドを使用して、**Red Hat Virtualization Manager** の特定のコンポーネントまたはすべてのコンポーネントを削除できます。



注記

Manager データベースのバックアップおよび **PKI** キーや設定の圧縮アーカイブは常に自動で作成されます。これらのファイルは **/var/lib/ovirt-engine/backups/** に保存され、ファイル名に **date** と **engine- pki-** を含めます。

手順

1. **Manager** マシンで以下のコマンドを実行します。

```
# engine-cleanup
```

2. **Red Hat Virtualization Manager** コンポーネントをすべて削除するかどうかを確認するプロンプトが表示されます。

- **Yes** と 入力 し、**Enter** を押してすべてのコンポーネントを削除します。

```
Do you want to remove all components? (Yes, No) [Yes]:
```

- **No** と 入力 して、**Enter** を押して削除するコンポーネントを選択します。各コンポーネントについて保持するか削除するかを個別に選択することができます。

```
Do you want to remove Engine database content? All data will be lost (Yes, No) [No]:
Do you want to remove PKI keys? (Yes, No) [No]:
Do you want to remove PKI configuration? (Yes, No) [No]:
Do you want to remove Apache SSL configuration? (Yes, No) [No]:
```

3. この段階でも **Red Hat Virtualization Manager** の削除を中止することができます。続行する場合は、**ovirt-engine** サービスが停止し、選択したオプションに従ってお使いの環境の設定が削除されます。

```
During execution engine service will be stopped (OK, Cancel) [OK]:
ovirt-engine is about to be removed, data will be lost (OK, Cancel) [Cancel]:OK
```

4. **Red Hat Virtualization パッケージを削除します。**

```
# yum remove rhvm* vdsm-bootstrap
```

付録E RED HAT VIRTUALIZATION のセキュリティー保護

このトピックには、Red Hat Virtualization のセキュリティー保護に関する限定的な情報が記載されています。この情報は今後増えていく予定です。

この情報は Red Hat Virtualization に特化したものです。以下に関連する基本のセキュリティープラクティスは対象としていません。

- 不要なサービスの無効化
- 認証
- 認可
- アカウンティング
- RHV 以外のサービスの侵入テストおよび耐性
- 機密アプリケーションデータの暗号化

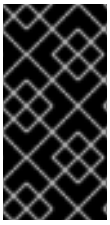
前提条件

- お客様は所属する組織のセキュリティー標準およびプラクティスを熟知している必要があります。可能な場合は、所属する組織のセキュリティー担当者にお問い合わせください。
- RHEL ホストをデプロイする前に 『セキュリティーガイド』 を参照してください。

E.1. DISA STIG FOR RED HAT LINUX 7

国防情報システム局 (DISA: Defense Information Systems Agency) は、さまざまなプラットフォームおよびオペレーティングシステム向けにセキュリティー技術導入ガイド (STIG: Security Technical Implementation Guide) を配布しています。

Red Hat Virtualization Host (RHVH) のインストールに際して、利用可能なセキュリティーポリシーの 1 つに DISA STIG for Red Hat Linux 7 プロファイルがあります。インストール時にこのプロファイルをセキュリティーポリシーとして有効にすると、SSH キー、SSL 証明書を再生成する必要がなくなります。有効にしない場合は、デプロイメントプロセスでホストを再生成する必要があります。



重要

DISA STIG セキュリティーポリシーは、Red Hat が正式にテストおよび認定する唯一のセキュリティーポリシーです。

「DISA STIG は、DOD IA および IA 対応デバイス/システムの構成標準です。DISA は 1998 年以降、セキュリティー技術導入ガイド (STIG: Security Technical Implementation Guide) を提供することで、国防総省 (DoD: Department of Defense) のセキュリティーシステムの Security Posture を強化する上で重大な役割を果たしてきました。STIG には、悪意あるコンピューター攻撃に対して脆弱である可能性のある情報システム/ソフトウェアを 'ロックダウン' するテクニカルガイダンスが含まれています。」

これらの STIG は、米国標準技術局 (NIST: National Institute of Standards and Technology) Special Publication 800-53 (NIST SP 800-53) がまとめた要件に基づくものです。NIST SP 800-53 とは、国家安全保障に関わるもの以外のすべての米連邦政府情報システムに関するセキュリティー管理のガイドラインです。

さまざまなプロファイルの中から重複するものを判断するため、Red Hat では、Cloud Security Alliance の Cloud Controls Matrix (CCM) を参照しています。この CCM は、クラウド固有のセキュリティー制御の包括的なセットを指定し、主要な標準、ベストプラクティス、および規制の要件にそれぞれをマッピングします。

Red Hat では、セキュリティーポリシーの検証をサポートするため、RHEL や RHV を含むさまざまな Red Hat プラットフォームに OpenSCAP ツールおよびセキュリティー設定共通化手順 (SCAP: Security Content Automation Protocol) プロファイルを提供しています。

Red Hat の OpenSCAP プロジェクトは、SCAP ベースラインを評価、査定、および実施するために、管理者および監査担当者にオープンソースツールを提供します。OpenSCAP は 2014 年に、NIST の SCAP 1.2 で認証されるようになりました。

NIST は SCAP 標準を保守します。SCAP 準拠のプロファイルは、オペレーティングシステムおよびアプリケーションのセキュリティー設定に関するローレベルの詳細なガイダンスを提供します。

Red Hat は、さまざまな製品およびプラットフォームの SCAP ベースラインを以下に公開していま

す。

- NIST National Checklist Program (NCP): 公開されているセキュリティーチェックリスト (またはベンチマーク) の米政府のリポジトリー
- 国防総省 (DoD: Department of Defense) Cyber Exchange

関連情報

- NIST National Checklist Program Repository for Red Hat
- Unix/Linux 関連の STIG の DoD Cyber Exchange ダウンロードページ
- NIST Special Publication 800-53 Rev. 4
- NIST Special Publication 800-53 Rev. 5 (DRAFT)
- OpenSCAP プロジェクト
- Cloud Security Alliance: Cloud Controls Matrix

E.2. DISA STIG FOR RED HAT LINUX 7 プロファイルの適用

このトピックでは、Red Hat Virtualization (RHV) Manager (Manager)、Red Hat Virtualization Host (RHVH)、および Red Hat Enterprise Linux ホストのインストールに際して、DISA STIG for Red Hat Linux 7 のセキュリティープロファイルを有効にする方法を説明します。

DISA STIG for Red Hat Linux 7 を RHVH 用に有効化

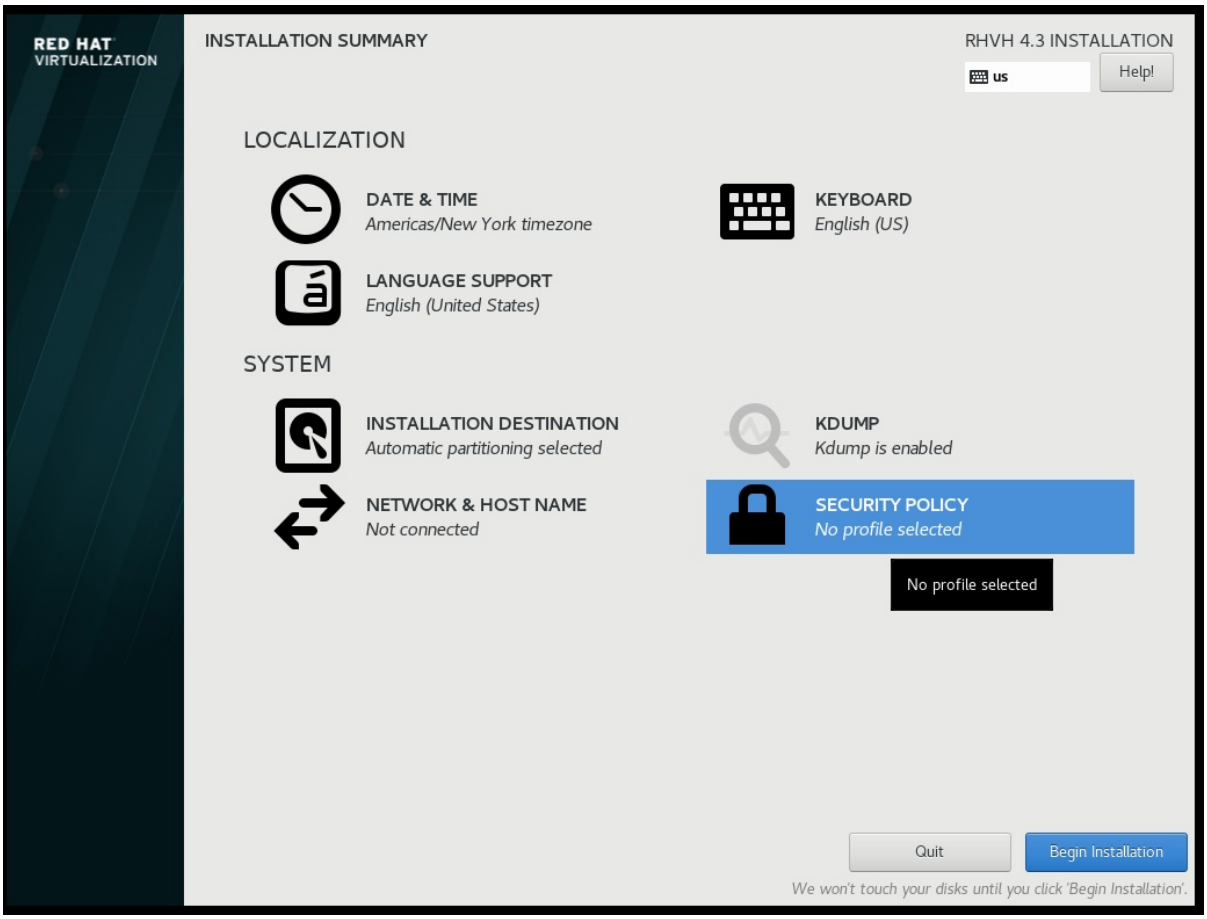
以下に示す 2 つの使用目的で Red Hat Virtualization Host (RHVH) をインストールする場合に、以下の手順が適用されます。

- Manager をセルフホストエンジンとしてデプロイする際に、RHVH を Manager 用仮想マシンのホストとして使用する。

- RHVH を RHV クラスター内で通常のホストとして使用する。

Anaconda インストーラーを使用して RHVH をインストールする場合は、以下の手順を実行します。

1. インストールの概要 画面で、セキュリティーポリシー を選択します。



2. セキュリティーポリシー 画面を開いたら、セキュリティーポリシーの適用 設定を On に切り替えます。

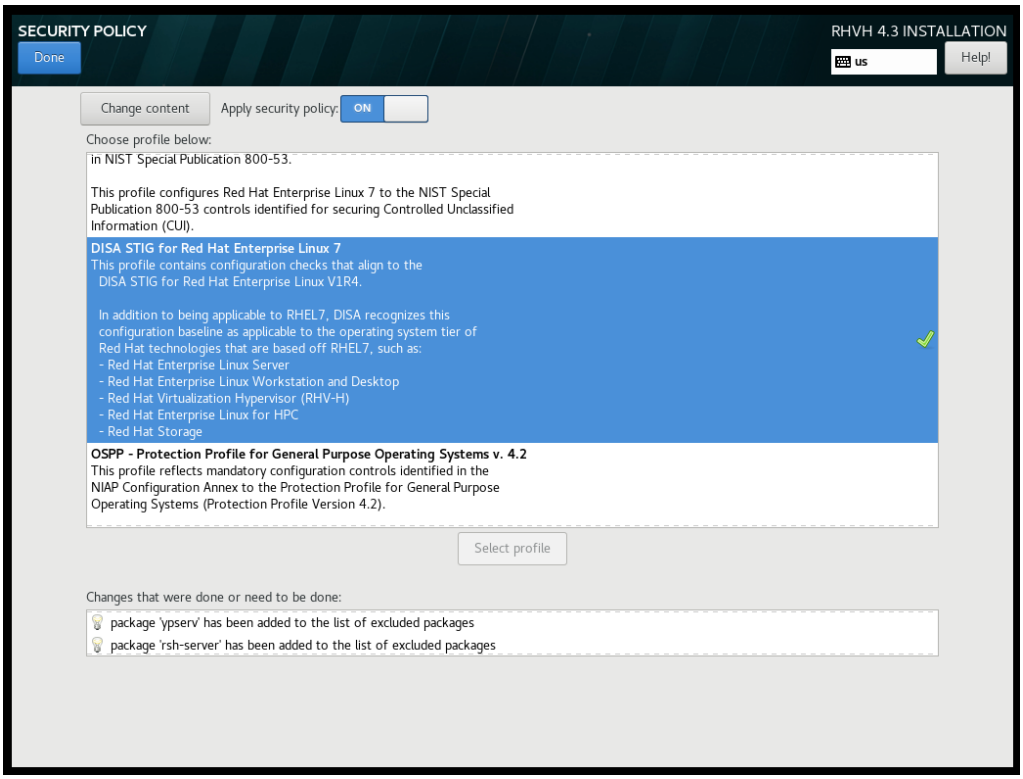
3. プロファイルのリストをスクロールダウンし、DISA STIG for Red Hat Linux 7 を選択します。

4. プロファイルの選択 ボタンをクリックします。クリックすることで、プロファイルの横に緑色のチェックマークが追加され、パッケージを 完了済みまたは完了する必要のある変更 の一

覧に追加します。

注記

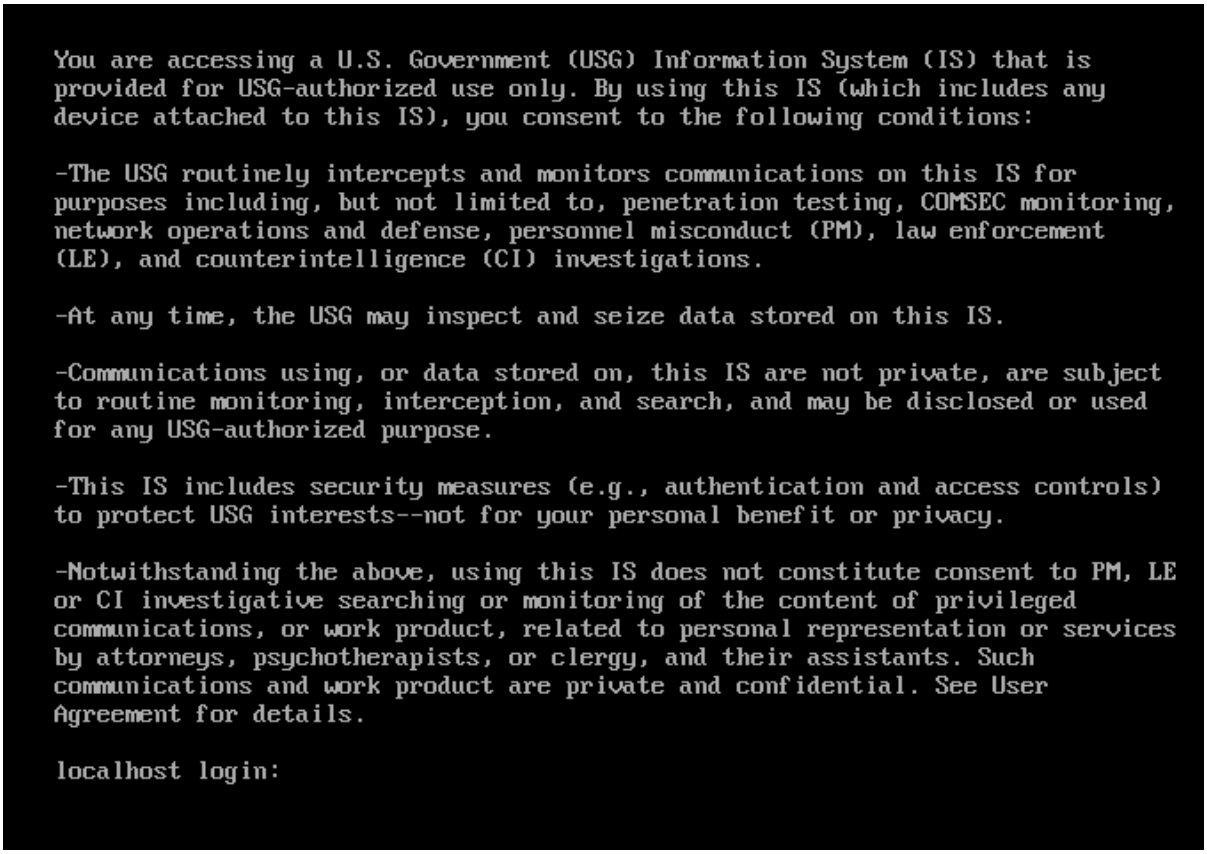
これらのパッケージは RHVH イメージにすでに含まれています。RHVH は単一のシステムイメージとして出荷されます。RHVH イメージの一部ではない他の選択されたセキュリティープロファイルで必要なパッケージのインストールができない場合があります。含まれるパッケージの一覧は、RHVH の『Package Manifest』を参照してください。

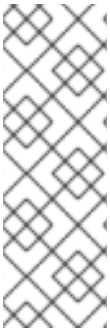


5. 完了 をクリックします。

6. インストールの概要 画面で、セキュリティーポリシー のステータスが 問題なし であることを確認します。

7. 後ほど RHVH にログインすると、コマンドラインに以下の情報が表示されます。





注記

コマンドラインを使用して RHV をセルフホストエンジンとしてデプロイする場合、ovirt- hosted-engine-setup の入力後に一連のプロンプトが表示されると、コマンドラインで デフォルトの OpenSCAP セキュリティープロファイルを適用するかどうかを尋ねられますか？Yes と入力して手順にしたがって DISA STIG for Red Hat Linux 7 プロファイルを選択します。

関連情報

- 「Configuring and Applying SCAP Policies During Installation」