Red Hat Virtualization 4.4

プランニングおよび前提条件に関するガイド

Red Hat Virtualization 4.4 のインストールおよび設定のプランニング

Last Updated: 2024-08-29

Red Hat Virtualization 4.4 プランニングおよび前提条件に関するガイド

Red Hat Virtualization 4.4 のインストールおよび設定のプランニング

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

法律上の通知

概要

このドキュメントでは、Red Hat Virtualization 環境の要件、オプション、および推奨事項を説明します。

目次

はじめに

Red Hat Virtualization は、それぞれが環境で異なるロールを担う接続されたコンポーネントで構成されています。事前に要件を計画して準備することで、これらのコンポーネントが効率的に通信し、実行できるようになります。

このガイドでは、以下を説明します。

- ハードウェアおよびセキュリティー要件
- 各種コンポーネントで利用可能なオプション
- 環境の最適化に関する推奨事項

第1章 RED HAT VIRTUALIZATION のアーキテクチャー

Red Hat Virtualization はセルフホストエンジンとして、あるいはスタンドアロンの Manager としてデプロイすることができます。セルフホストエンジンが推奨されるデプロイメントのオプションです。

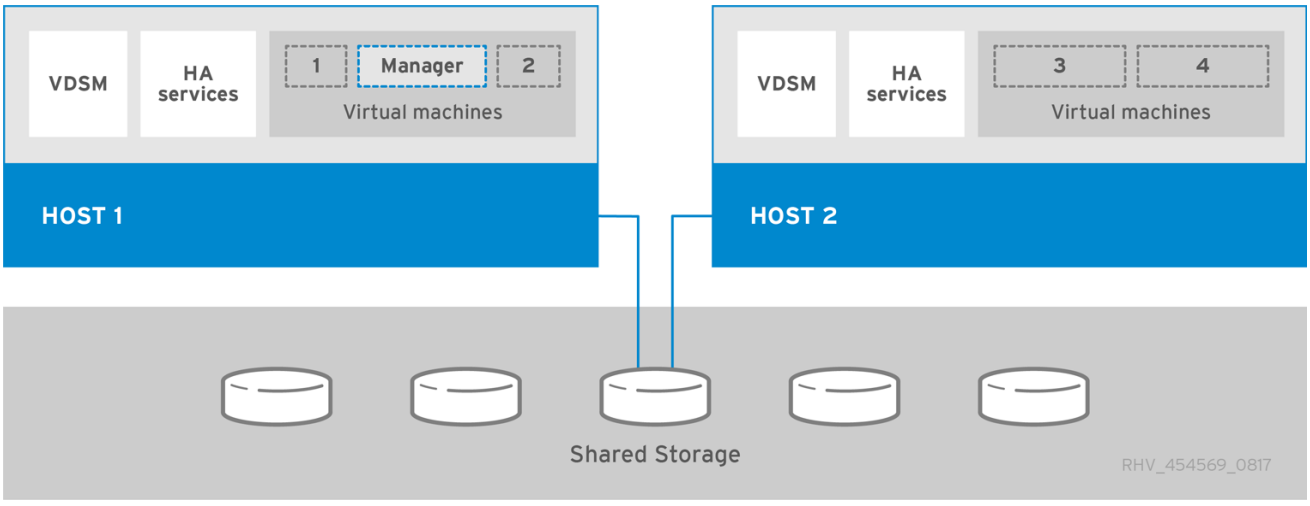
1.1. セルフホストエンジンのアーキテクチャー

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。Red Hat Enterprise Linux 8 仮想マシンのインストールおよび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、RHV-M Appliance が使用されます。
- 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できるようにする必要があります。

図1.1 セルフホストエンジンの Red Hat Virtualization アーキテクチャー



1.2. スタンドアロンの MANAGER のアーキテクチャー

Red Hat Virtualization Manager は物理サーバーか、別の仮想環境でホストされている仮想マシン上で実行されます。スタンドアロンの Manager は、デプロイと管理が簡単ですが、追加の物理サーバーが 1 台必要となります。Manager は、Red Hat の High Availability Add-On などの別製品を使用して外部から管理した場合にのみ高可用性になります。

スタンドアロンの Manager 環境の最小セットアップには、以下が含まれます。

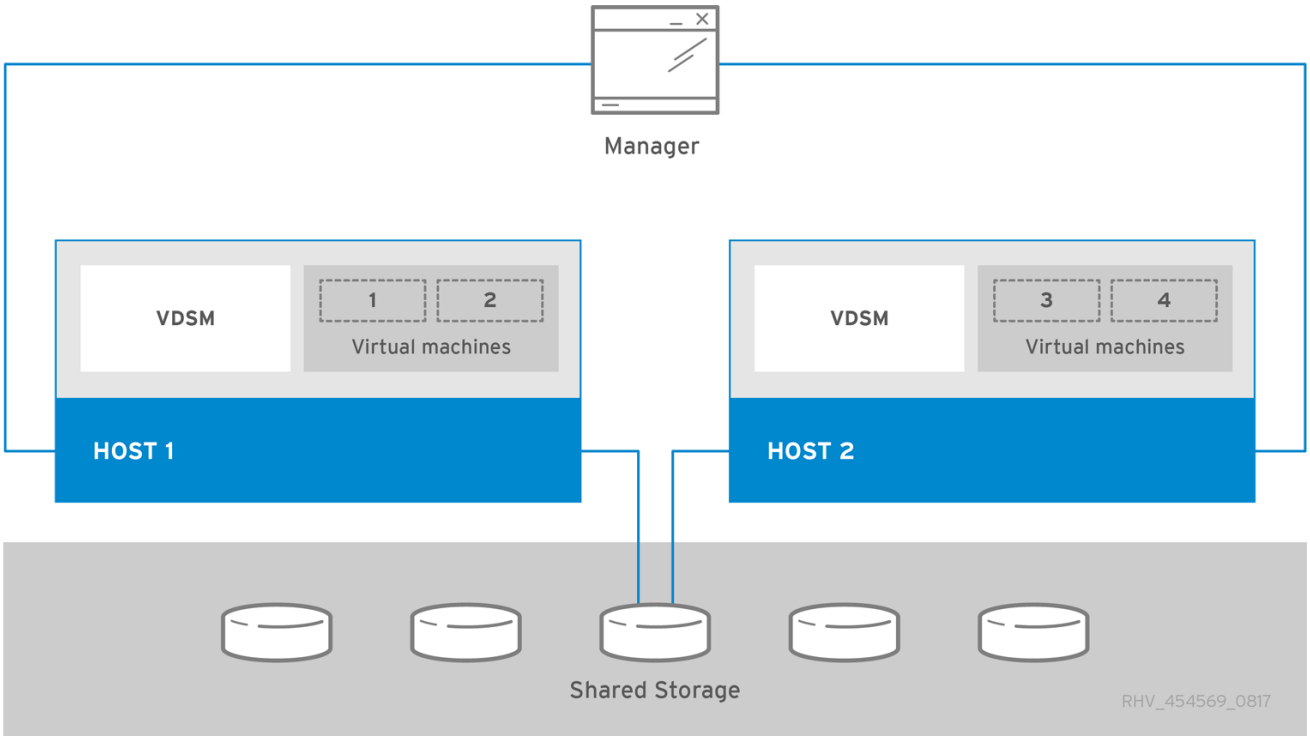
- Red Hat Virtualization Manager マシン 1 台。Manager は通常物理サーバーにデプロイされます。仮想マシン上にデプロイすることも可能ですが、その仮想マシンは別の環境でホストされ

ていなければなりません。Manager は Red Hat Enterprise Linux 8 上で実行する必要があります。

- 仮想マシンの高可用性には、最小でホストが 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。

- 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できるようにする必要があります。

図1.2 スタンドアロンの Manager の Red Hat Virtualization アーキテクチャー



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、Does Red Hat Virtualization also have hardware certification? 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、Red Hat 認定ハードウェア 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 x86_64 CPU	クアッドコア x86_64 CPU または複数のデュアルコア x86_64 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イス	1 Gbps 以上の帯域幅のネットワークインターフェイスカード (NIC) 1 基	1 Gbps 以上の帯域幅のネットワークインターフェイスカード (NIC) 1 基

2.1.2. ブラウザーの要件

管理ポータルと仮想マシンポータルには、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 のエンジニアリングチームは、この階層のブラウザーで問題が発生した場合には、必ず修正を行います。

- 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。Red Hat のエンジニアリングチームは、この階層のブラウザーで問題が発生した場合には、修正を試みます。
- 階層 3: 未検証だが、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。Red Hat のエンジニアリングチームは、この階層のブラウザー問題が発生した場合には、マイナーな問題に対して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

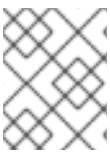
2.1.3. クライアントの要件

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) プロトコルを使用してアクセスできます。ゲストオペレーティングシステムに QXLDOD グラフィカルドライバーをインストールして、SPICE の機能を向上させることができます。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。

クライアントオペレーティングシステムの SPICE サポート

サポートされている QXLDOD ドライバーは、Red Hat Enterprise Linux 7.2 以降および Windows 10 で利用できます。



注記

SPICE は QXLDOD ドライバーを使用して Windows 8 または 8.1 で動作しますが、認定もテストもされていません。

2.1.4. オペレーティングシステムの要件

Red Hat Virtualization Manager は、Red Hat Enterprise Linux 8.6 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、Does Red Hat Virtualization also have hardware certification? 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、認定ソリューションの検索 を参照してください。

ゲストに適用される要件と制限の詳細は、Red Hat Enterprise Linux テクノロジーの機能と制限 および Supported Limits for Red Hat Virtualization 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
  - IvyBridge
  - Haswell
  - Broadwell
  - Skylake (クライアント)
  - Skylake (サーバー)
  - Cascadelake サーバー
- IBM
  - POWER8

- POWER9

CPU タイプ は、セキュリティー更新のある CPU モデルごとに、基本的なタイプと安全なタイプを一覧表示します。以下に例を示します。

- **Intel Cascadelake Server Family**
- **Secure Intel Cascadelake Server Family**

Secure CPU タイプには最新の更新が含まれます。詳細は、BZ#1731395 を参照してください。

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。

手順

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、リストから **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ることを確認し、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に対応しています。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。クラスターレベル 4.2 から 4.5 の場合、Red Hat Virtualization Host で仮想マシンごとにサポートされる最大 RAM は 6 TB です。クラスターレベル 4.6 から 4.7 の場合、Red Hat Virtualization Host で仮想マシンごとにサポートされる最大 RAM は 16 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。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た場合、KVM は仮想ゲストに対して物理 RAM をオーバーコミットし、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。

このセクションでは、RHVH の最低ストレージ要件を説明します。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、より多くのストレージ領域を利用できるデフォルトの割り当てを使用してください。

- / (root): 6 GB
- /home: 1 GB
- /tmp: 1 GB
- /boot: 1 GB
- /var: 5 GB
- /var/crash: 10 GB
- /var/log: 8 GB
- /var/log/audit: 2 GB
- /var/tmp: 10 GB
- スワップ - 1 GB詳細は、What is the recommended swap size for Red Hat platforms? 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。
- **最少の合計: 64 GiB**

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 10 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。メモリーの最適化 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イスが少なくとも 1 基搭載されている必要があります。各ホストに 2 つのネットワークインターフェイスを搭載し、そのうちの 1 つは仮想マシンの移行などネットワークへの負荷が高い作業専用にする必要があります。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。
- PCIe デバイスとルートポート間の PCIe スイッチとブリッジはすべて、ACS をサポートしていること。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 8 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 シリーズ以降)、GRID、Tesla の PCI デバイス割り当てをサポートしていること。現在、標準のエミュレーションされた VGA インターフェイスの 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 NVIDIA 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。
- 仮想マシンの **Administration Portal** の **Host Devices** タブにある **Manage vGPU** ダイアログを使用して、この仮想マシンで使用する vGPU のタイプとインスタンスの数を選択します。
- 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 を実行している物理または仮想マシンで IPv6 を有効にしたままにしておく必要があります。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. セルフホストエンジンデプロイメントのネットワーク範囲

セルフホストエンジンのデプロイメントプロセスは、**192.168** 下の **/24** ネットワークアドレスを一時的に使用します。デフォルトは **192.168.222.0/24** で、このアドレスが使用されている場合は、使用されていないアドレスが見つかるまで、**192.168** 下にある他の **/24** アドレスを試します。この範囲で未使用のネットワークアドレスが見つからない場合は、デプロイメントに失敗します。

コマンドラインを使用してセルフホストエンジンをインストールする場合は、オプション **--ansible-extra-vars=he_ipv4_subnet_prefix=PREFIX** を使用して、別の **/24** ネットワーク範囲を使用するようにデプロイメントスクリプトを設定できます。**PREFIX** はデフォルト範囲の接頭辞に置き換えます。以下に例を示します。

```
# hosted-engine --deploy --ansible-extra-vars=he_ipv4_subnet_prefix=192.168.222
```

注記

コマンドラインで Red Hat Virtualization をセルフホストエンジンとしてインストールすることでのみ、別の範囲を設定することができます。

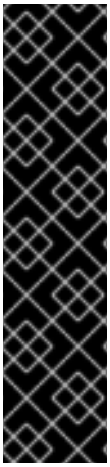
2.3.3. DNS、NTP、および IPMI フェンシングに対するファイアウォールの要件

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、受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。出力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。
- 名前解決には、**/etc/hosts** ファイルの代わりに DNS を使用します。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、受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。

2.3.4. 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 スクリプトは、ファイアウォールを自動的に設定できます。

この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、模式図内の接続を検索できます。

表2.3 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	送信先	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。	いいえ
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	はい

ID	ポート	プロトコル	送信元	送信先	目的	デフォルトで暗号化
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。	はい
M4	80、443	TCP	管理ポータルのクライアント 仮想マシン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。	はい
M5	6100	TCP	管理ポータルのクライアント 仮想マシン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。	いいえ

ID	ポート	プロトコル	送信元	送信先	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 の高度な設定 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。	いいえ
M7	54323	TCP	管理ポータルのクライアント	Red Hat Virtualization Manager (**ovirt-imageio** サービス)	**ovirt-imageo** サービスとの通信に必要です。	はい
M8	6642	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	はい
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	はい。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	送信先	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	はい。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。	いいえ
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。	いいえ

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。出力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 サーバーに送信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。

2.3.5. 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、**Advanced Parameters** の下の **Automatically configure host firewall** 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、RHV: How to customize the Host's firewall rules? 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図は、Red Hat Virtualization: Firewall Requirements Diagram で入手できます。表に書かれた ID を使用して、模式図内の接続を検索できます。

表2.4 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	送信先	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	はい
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。	はい
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	いいえ

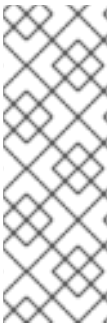
ID	ポート	プロトコル	送信元	送信先	目的	デフォルトで暗号化
H4	111	TCP	NFS ストレージサーバー	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	NFS 接続 オプション	いいえ
H5	5900 - 6923	TCP	管理ポータルのクライアント 仮想マシンポータルのクライアント	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	VNC および SPICE を介したリモートゲストのコンソールアクセス。クライアントが仮想マシンに容易にアクセスできるよ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

ID	ポート	プロトコル	送信元	送信先	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	いいえ
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 インターフェイスにアクセスするために必要です。	はい
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** を使用した仮想マシンの移行	はい

ID	ポート	プロトコル	送信元	送信先	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。	はい。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	はい
H11	54322	TCP	Red Hat Virtualization Manager **ovirt-imageio** サービス	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	**ovirt-imageo** サービスとの通信に必要です。	はい

ID	ポート	プロトコル	送信元	送信先	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。	いいえ
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。	いいえ
H14	123	UDP	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	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。このポートは必須で、デフォルトで開いています。	
H15	4500	TCP、UDP	Red Hat Virtualization Host	Red Hat Virtualization Host	インターネットセキュリティープロトコル (IPSec)	はい

ID	ポート	プロトコル	送信元	送信先	目的	デフォルトで暗号化
H16	500	UDP	Red Hat Virtualization Host	Red Hat Virtualization Host	インターネットセキュリティープロトコル (IPSec)	はい
H17	-	AH、ESP	Red Hat Virtualization Host	Red Hat Virtualization Host	インターネットセキュリティープロトコル (IPSec)	はい



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。出力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信します。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。

2.3.6. 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**) でのリモートデータベースサーバーの使用をサポートしています。リモートデータベースサーバーを使用する予定がある場合は、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、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がある場合は、そのシステムからのアクセスをデータベースで許可する必要があります。

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、模式図内の接続を検索できます。

表2.5 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	送信先	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 (**engine**) 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	無効ですが、有効にできます。
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。無効ですが、有効にできます。

2.3.7. 最大伝送単位の要件

デプロイメント中のホストで推奨される最大伝送単位 (MTU) の設定は 1500 です。環境が別の MTU に設定された後で、この設定を更新することができます。MTU 設定の変更に関する詳細は、How to change the Hosted Engine VM network MTU を参照してください。

第3章 留意事項

この章では、さまざまな Red Hat Virtualization コンポーネントの利点、制限、および利用可能なオプションを説明します。

3.1. ホストタイプ

実際の環境に最も適したホストタイプを使用してください。必要に応じて、同じクラスターで両方のタイプのホストを使用することもできます。

クラスター内のすべてのマネージドホストには同じ CPU タイプが必要です。Intel と AMD CPU は同じクラスター内で共存できません。

Red Hat Virtualization Manager がサポートできるホストの最大数などの、サポートされる最大値と制限に関する情報は、Supported Limits for Red Hat Virtualization を参照してください。

3.1.1. Red Hat Virtualization Host

Red Hat Virtualization Host (RHVH) には、Red Hat Enterprise Linux ホストと比較して、以下の利点があります。

- RHVH は Red Hat Virtualization のサブスクリプションに含まれています。Red Hat Enterprise Linux ホストには、追加のサブスクリプションが必要になる場合があります。
- RHVH は単一のイメージとしてデプロイされます。これにより、更新プロセスが簡素化されます。個別に更新されるパッケージとは異なり、イメージ全体がひとまとまりで更新されます。
- 仮想マシンをホストし、ホスト自体を管理するのに必要なパッケージとサービスのみが含まれます。これにより、操作が簡素化されれ、全体的な攻撃ベクトルが削減されます。不要なパッケージやサービスはデプロイされないため、悪用できません。
- Cockpit Web インターフェイスがデフォルトで利用でき、仮想マシンモニタリングツールやセルフホストエンジンの GUI インストーラーなど、Red Hat Virtualization 固有の拡張機能が含まれます。Cockpit は Red Hat Enterprise Linux ホストでサポートされますが、手動でインストールする必要があります。

3.1.2. Red Hat Enterprise Linux ホスト

Red Hat Enterprise Linux ホストには、Red Hat Virtualization Host と比較して、以下の利点があります。

- Red Hat Enterprise Linux ホストは高度なカスタマイズが可能なため、たとえばホストに特定のファイルシステムのレイアウトが必要な場合に適します。
- Red Hat Enterprise Linux ホストは、頻繁に更新される場合に適しています (特に追加パッケージがインストールされる場合)。イメージ全体ではなく、個別のパッケージを更新することができます。

3.2. ストレージタイプ

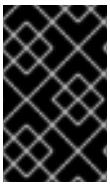
各データセンターには、少なくとも 1 つのデータストレージドメインが必要です。データセンターごとに 1 つの ISO ストレージドメインも推奨されます。ストレージドメインのエクスポートは非推奨となっていますが、必要に応じて引き続き作成できます。

ストレージドメインは、ブロックデバイス (iSCSI またはファイバーチャネル) またはファイルシステムのいずれかで構成できます。

デフォルトでは、GlusterFS ドメインとローカルストレージドメインは 4K ブロックサイズをサポートします。4K ブロックサイズを使用すると、特に大きなファイルを使用する場合などに、パフォーマンスが向上します。また、VDO などの 4K 互換性を必要とするツールを使用する場合にも必要です。

注記

GlusterFS Storage は非推奨になり、将来のリリースではサポートされなくなります。



重要

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

以下のセクションで説明するストレージタイプは、データストレージドメインとしての使用がサポートされます。ISO およびエクスポートストレージドメインは、ファイルベースのストレージタイプのみをサポートしています。ISO ドメインは、ローカルストレージ用のデータセンター内で使用される場合にローカルストレージをサポートします。

参照:

- **Administration Guide**の Storage
- **Red Hat Enterprise Linux Storage Administration Guide**

3.2.1. NFS

NFS バージョン 3 および 4 が、Red Hat Virtualization 4 でサポートされます。NFS が ISO ストレージドメインとしてしか使用されない限り、実稼働環境のワークロードには、エンタープライズレベルの NFS サーバーが必要です。エンタープライズ NFS が 10GbE でデプロイされ、VLAN で分離され、個別のサービスが特定のポートを使用するように設定される場合、高速かつセキュアになります。

NFS エクスポートはより多くのストレージニーズに対応して拡張されるため、Red Hat Virtualization はより大きなデータストアをすぐに認識します。ホスト上で、または Red Hat Virtualization 内から、追加の設定は必要ありません。これにより、スケーリングおよび運用上の面から、NFS にブロックストレージより若干の優位性がもたらされます。

参照:

- **Red Hat Enterprise Linux Storage Administration Guide**の Network File System (NFS)
- **Administration Guide**の Preparing and Adding NFS Storage

3.2.2. iSCSI

実稼働環境のワークロードには、エンタープライズレベルの iSCSI サーバーが必要です。エンタープライズ iSCSI が 10GbE でデプロイされ、VLAN で分離され、CHAP 認証が利用される場合、高速かつセキュアになります。また、iSCSI はマルチパスを使用して高可用性を改善することができます。

Red Hat Virtualization は、ブロックベースのストレージドメインごとに 1500 の論理ボリュームをサポートします。300 以下の LUN が許可されます。

参照:

- **Red Hat Enterprise Linux Storage Administration Guide**の Online Storage Management
- **Administration Guide**の Adding iSCSI Storage

3.2.3. ファイバーチャネル

ファイバーチャンネルは高速かつセキュアで、ターゲットのデータセンターですでに使用されている場合には活用する必要があります。また、iSCSI および NFS と比較して、CPU のオーバーヘッドが低くなるという利点があります。また、ファイバーチャンネルはマルチパスを使用して高可用性を改善することができます。

Red Hat Virtualization は、ブロックベースのストレージドメインごとに 1500 の論理ボリュームをサポートします。300 以下の LUN が許可されます。

参照:

- **Red Hat Enterprise Linux Storage Administration Guide**の Online Storage Management
- **Administration Guide**の Adding FCP Storage

3.2.4. Fibre Channel over Ethernet

Red Hat Virtualization で Fibre Channel over Ethernet (FCoE) を使用するには、Manager で **fcoe** キーを有効にし、ホスト上に **vdsm-hook-fcoe** パッケージをインストールする必要があります。

Red Hat Virtualization は、ブロックベースのストレージドメインごとに 1500 の論理ボリュームをサポートします。300 以下の LUN が許可されます。

参照:

- **Red Hat Enterprise Linux Storage Administration Guide**の Online Storage Management
- **Administration Guide**の How to Set Up Red Hat Virtualization Manager to Use FCoE

3.2.5. Red Hat Hyperconverged Infrastructure

Red Hat Hyperconverged Infrastructure (RHHI) は、Red Hat Virtualization をリモート Red Hat Gluster Storage サーバーに接続するのではなく、同じインフラストラクチャーに Red Hat Virtualization と Red Hat Gluster Storage を組み合わせます。このコンパクトオプションにより、運用費用やオーバーヘッドを削減します。

参照:

- **Deploying Red Hat Hyperconverged Infrastructure for Virtualization**
- **Deploying Red Hat Hyperconverged Infrastructure for Virtualization On A Single Node**
- **Automating RHHI for Virtualization Deployment**

3.2.6. POSIX 準拠 FS

Red Hat Global File System 2 (GFS2) 等のクラスター化したファイルシステムで、かつスパースファイルおよびダイレクト I/O をサポートしている限り、他の POSIX 準拠のファイルシステムを Red Hat Virtualization のストレージドメインとして使用することができます。たとえば、Common Internet File

System (CIFS) は、ダイレクト I/O をサポートしていないため、Red Hat Virtualization との互換性はありません。

参照:

- **Red Hat Enterprise Linux Global File System 2**
- **Administration Guide**の Adding POSIX Compliant File System Storage

3.2.7. ローカルストレージ

ローカルストレージは、ホスト独自のリソースを使用して個々のホスト上に設定されます。ホストがローカルストレージを使用するように設定すると、他のホストを追加することができない新規データセンターとクラスターに自動的に追加されます。単一ホストのクラスター内で作成された仮想マシンは、移行、フェンシング、スケジューリングできません。

Red Hat Virtualization Host の場合は、必ず / (ルート) とは異なるファイルシステム上にローカルストレージを定義する必要があります。別の論理ボリュームまたはディスクを使用します。

Administration Guideの Preparing and Adding Local Storage を参照してください。

3.3. ネットワークの留意事項

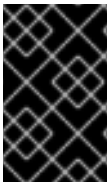
Red Hat Virtualization 環境でネットワークのプランニングや設定を行う場合、ネットワーク概念やその使用についてよく理解しておくことが強く推奨されます。ネットワーク管理の詳細は、ネットワークハードウェアベンダーのガイドを確認してください。

論理ネットワークは、NIC などの物理デバイス、またはネットワークボンディングなどの論理デバイスを使用してサポートされる場合があります。ボンディング自体が機能しなくなるには、ボンディング内のすべてのネットワークインターフェイスカードに障害が発生する必要があるので、ボンディングにより高可用性が改善され、対障害性が向上します。ボンディングモード 1、2、3、および 4 は、仮想マシンおよび非仮想マシンのネットワークタイプの両方をサポートします。モード 0、5、および 6 は、非仮想マシンのネットワークのみをサポートします。Red Hat Virtualization は、デフォルトでモード 4 を使用します。

仮想 LAN (VLAN) タグ付けを使用してネットワークトラフィックを分離することで、複数の論理ネットワークが 1 つのデバイスを共有できるので、論理ネットワークごとに 1 つのデバイスを設定する必要はありません。この機能を使用するには、スイッチレベルでも VLAN タグ付けをサポートする必要があります。

Red Hat Virtualization 環境で定義する論理ネットワークの数に適用される制限は、以下のとおりです。

- ホストに接続される論理ネットワークの数は、利用可能なネットワークデバイスの数と仮想 LAN (VLAN) の最大数 (4096) の組み合わせに制限されます。
- 1 回の操作でホストにアタッチできるネットワークの数は、現在 50 に制限されます。
- ネットワーク設定はクラスター内のすべてのホストで同じでなければならないので、クラスター内の論理ネットワークの数は、ホストに接続可能な論理ネットワークの数に制限されます。
- データセンター内の論理ネットワーク数は、データセンター内のクラスターの数とクラスターごとに許容される論理ネットワークの数の組み合わせによってのみ制限されます。



重要

管理ネットワーク (**ovirtmgmt**) のプロパティーを変更する場合には、細心の注意を払ってください。**ovirtmgmt** ネットワークのプロパティーの変更が間違っていると、ホストに到達できなくなる可能性があります。

重要

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

Red Hat Virtualization は Cisco Application Centric Infrastructure (ACI) と完全に統合されています。これにより、包括的なネットワーク管理機能が提供され、Red Hat Virtualization ネットワークインフラストラクチャーを手動で設定する必要性が低減されます。インテグレーションは、Cisco のドキュメントに従って、Cisco の Application Policy Infrastructure Controller (APIC) バージョン 3.1(1) 以降に Red Hat Virtualization を設定して実施されます。

3.4. ディレクトリーサーバーのサポート

インストール時に、Red Hat Virtualization Manager は、デフォルトの **internal** ドメインにデフォルトの **admin** ユーザーを作成します。このアカウントは、環境の初期設定およびトラブルシューティングに使用することを目的としています。**ovirt-aaa-jdbc-tool** を使用して、**internal** ドメインに追加のユーザーを作成できます。ローカルドメインに作成されたユーザーアカウントは、ローカルユーザーとして知られています。**Administration Guide**の Administering User Tasks From the Command Line を参照してください。

外部ディレクトリーサーバーを Red Hat Virtualization 環境にアタッチし、外部ドメインとして使用することもできます。外部ドメインに作成されたユーザーアカウントは、ディレクトリーユーザーとして知られています。複数のディレクトリーサーバーの Manager への割り当てもサポートされます。

以下のディレクトリーサーバーは、Red Hat Virtualization との使用がサポートされます。サポート対象のディレクトリーサーバーのインストールおよび設定の詳細は、ベンダーのドキュメントを参照してください。

- Microsoft Active Directory
- Red Hat Enterprise Linux Identity Management
- Red Hat Directory Server
- OpenLDAP
- IBM Security (Tivoli) Directory Server

重要

Red Hat Virtualization の管理ユーザーとして使用するため、すべてのユーザーおよびグループを読み取るパーミッションを持つユーザーをディレクトリーサーバーに作成する必要があります。ディレクトリーサーバーの管理ユーザーを、Red Hat Virtualization の管理ユーザーとして **使用しないでください**。

Administration Guideの Users and Roles を参照してください。

3.5. インフラストラクチャーに関する留意事項

3.5.1. ローカルまたはリモートホスト

以下のコンポーネントは、Manager またはリモートマシンのいずれかでホストされます。Manager マシンにすべてのコンポーネントを維持することが、より簡単で、メンテナンスが少なくなります。したがって、パフォーマンスが問題ではない場合には推奨されます。コンポーネントをリモートマシンに移動するにはより多くの保守が必要になりますが、Manager と Data Warehouse の両方のパフォーマンスを向上させることができます。

Data Warehouse データベースおよびサービス

Manager で Data Warehouse をホストするには、**engine-setup** でプロンプトが表示されたら **Yes** を選択します。
リモートマシンで Data Warehouse をホストするには、**engine-setup** でプロンプトが表示されたら **No** を選択し、**Installing Red Hat Virtualization as a standalone Manager with remote databases**の Installing and Configuring Data Warehouse on a Separate Machine を参照してください。

インストール後に Data Warehouse を移行するには、**Data Warehouse Guide**の Migrating Data Warehouse to a Separate Machine を参照してください。

また、Data Warehouse サービスと Data Warehouse データベースを、相互に分離してホストすることもできます。

Manager データベース

Manager で Manager データベースをホストするには、**engine-setup** でプロンプトが表示されたら **Local** を選択します。
Manager データベースをリモートマシンでホストするには、Manager で **engine-setup** を実行する前に、**Installing Red Hat Virtualization as a standalone Manager with remote databases**の Preparing a Remote PostgreSQL Database を参照してください。

インストール後に Manager データベースを移行するには、**Administration Guide**の Migrating the Engine Database to a Remote Server Database を参照してください。

Websocket プロキシー

Manager で Websocket プロキシーをホストするには、**engine-setup** でプロンプトが表示されたら **Yes** を選択します。

重要

セルフホストエンジン環境では、アプライアンスを使用して Manager 用仮想マシンのインストールおよび設定を行います。したがって、Data Warehouse、Manager データベース、および Websocket プロキシーは、インストール後にのみ外部にすることができます。

3.5.2. リモートホストのみ

以下のコンポーネントは、リモートマシンでホストされる必要があります。

DNS

Red Hat Virtualization 環境では DNS を過度に使用するため、環境でホストされる仮想マシンとして環境の DNS サービスを実行することはサポートされません。

ストレージ

ローカルストレージ を除き、ストレージサービスは Manager またはいずれかのホストと同じマシン上に配置しないでください。

Identity Management

IdM (**ipa-server**) は、Manager で必要な **mod_ssl** パッケージと互換性がありません。

第4章 推奨事項

この章では、厳密には必須ではないが、環境のパフォーマンスまたは安定性を向上させる可能性がある設定を説明します。

4.1. 一般的な推奨事項

- デプロイメントが完了したらすぐに完全バックアップを作成し、別の場所に保存します。その後は、定期的にバックアップを作成します。**Administration Guide**の Backups and Migration を参照してください。

- Red Hat Virtualization が依存するサービスを同じ環境内の仮想マシンとして実行することは避けてください。そうする場合には、そのサービスが含まれる仮想マシンにダウンタイムが生じた場合に、ダウンタイムを最小限に抑えるように慎重に計画する必要があります。

- Red Hat Virtualization Manager がインストールされるベアメタルホストまたは仮想マシンに、十分なエントロピーがあることを確認します。200 未満の値の場合、Manager のセットアップが失敗する可能性があります。エントロピー値を確認するには、**cat /proc/sys/kernel/random/entropy_avail** を実行します。エントロピーを増やすには、**rng-tools** パッケージをインストールし、How can I customize rngd service startup? の手順に従います。.

- PXE、キックスタート、Satellite、CloudForms、Ansible を使用して、またはこれらを組み合わせて、ホストと仮想マシンのデプロイメントを自動化できます。ただし、PXE を使用したセルフホストエンジンのインストールはサポートされていません。参照:

  - Automating Red Hat Virtualization Host Deployment (PXE およびキックスタートを使用した RHVH の自動デプロイメントに関する追加要件)

  - **Performing a Standard RHEL Installation**の Preparing for your installation

  - **Performing an Advanced RHEL Installation**の Performing an Automated Installation Using Kickstart

  - **Red Hat Satellite 6.2 Provisioning Guide**

  - **Red Hat CloudForms 5.0 Provisioning Virtual Machines and Hosts**

  - **Administration Guide**の Automating Configuration Tasks using Ansible

- デプロイメント内のすべてのマシンのシステムタイムゾーンを UTC に設定します。これにより、サマータイムなど、ローカルのタイムゾーンのバリエーションでデータ収集と接続が中断されないようにします。

- 時刻を同期するために、環境内のすべてのホストおよび仮想マシンで Network Time Protocol (NTP) を使用します。認証と証明書は、特に時刻のずれに敏感です。以前は、NTP は **chrony** (**chronyd**) または **ntp** (**ntpd**) を使用して実装できましたが、Red Hat Enterprise Linux 8 では **chrony** のみがサポートされています。
  ntp から **chrony** への移行に関する情報は、**chrony** への移行 を参照してください。

  chrony の詳細は、Chrony スイートを使用した NTP の設定 を参照してください。

- 環境で操作を行うユーザーが誰でも現在の状態と必要な手順を理解するように、すべてを文書化します。

4.2. セキュリティーに関する推奨事項

- ホストまたは仮想マシンで、セキュリティー機能 (HTTPS、SELinux、ファイアウォールなど) を無効にしないでください。
- 最新のセキュリティー更新とエラータを受け取るために、すべてのホストと Red Hat Enterprise Linux 仮想マシンを Red Hat コンテンツ配信ネットワークまたは Red Hat Satellite のいずれかに登録します。
- アクティビティーを適切に追跡するために、多くのユーザーにデフォルトの **admin** アカウントの使用を許可するのではなく、個別の管理者アカウントを作成します。
- ホストへのアクセスを制限し、別のログインを作成します。すべてのユーザーが使用する 1 つの **root** ログインを作成しないでください。ユーザー、グループ、および root パーミッションの管理に関する詳細は、Configuring Basic System Settings を参照してください。
- ホストに信頼できないユーザーを作成しないでください。
- Red Hat Enterprise Linux ホストをデプロイする場合、仮想化、パフォーマンス、セキュリティー、およびモニタリング要件を満たすのに必要なパッケージおよびサービスのみをインストールします。実稼働ホストには、解析ツール、コンパイラー等の追加のパッケージ、または不要なセキュリティーリスクを追加するその他のコンポーネントを含めないでください。

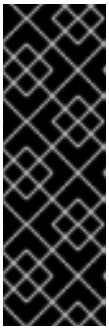
4.3. ホストの推奨事項

- 同じクラスター内のホストを標準化します。これには、一貫性のあるハードウェアモデルとファームウェアのバージョンが含まれます。同じクラスター内で異なるサーバーハードウェアを混在させると、ホスト間でパフォーマンスが一定しない可能性があります。
- 同じクラスターで Red Hat Enterprise Linux ホストと Red Hat Virtualization Host の両方を使用することができますが、この設定は特定のビジネスまたは技術要件に対応する場合に限り使用してください。
- デプロイ時にフェンシングデバイスを設定します。高可用性には、フェンシングデバイスが必要です。
- フェンシングトラフィックには、別のハードウェアスイッチを使用します。同じスイッチで監視とフェンシングが行われると、そのスイッチは、高可用性の対して単一障害点になります。

4.4. ネットワークの推奨事項

- 特に実稼働ホストでは、ネットワークインターフェイスをボンディングします。ボンディングにより、サービスの全体的な可用性と、ネットワークの帯域幅が向上します。**Administration Guide**の Network Bonding を参照してください。
- DNS および DHCP レコードで設定された安定したネットワークインフラストラクチャー。
- ボンディングを他のネットワークトラフィックと共有する場合には、ストレージおよび他のネットワークトラフィック用に適切な Quality of Service (QoS) が必要です。
- 最適なパフォーマンスと簡素化されたトラブルシューティングを行うには、VLAN を使用して異なるトラフィック種別を分離し、10 GbE ネットワークまたは 40 GbE ネットワークを最大限活用します。
- 基礎となるスイッチがジャンボフレームをサポートする場合は、基礎となるスイッチが対応する最大サイズ (例: **9000**) に MTU を設定します。この設定により、ほとんどのアプリケーション

に対して、帯域幅が高くなり、CPU 使用率が削減され、最適なスループットが得られます。デフォルトの MTU は、基礎となるスイッチでサポートされる最小サイズで決定されます。LLDP が有効化されている場合には、**Setup Host Networks** ウィンドウの NIC のツールチップで各ホストのピアが対応する MTU が表示されます。

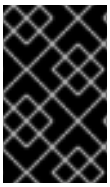


重要

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

- 1 GbE ネットワークは、管理トラフィックにのみ使用してください。仮想マシンおよびイーサネットベースのストレージには、10 GbE または 40 GbE を使用します。
- ストレージ用に追加の物理インターフェイスをホストに追加する場合は、**仮想マシンネットワーク** をクリアし、VLAN が物理インターフェイスに直接割り当てられるようにします。

ホストネットワーク設定の推奨プラクティス



重要

クラスター内のホストのネットワーク設定を変更するには、必ず RHV Manager を使用します。使用しない場合は、サポート対象外の設定が作成される可能性があります。詳細は、Network Manager のステートフル設定 (nmstate) を参照してください。

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。

以下に示すホストネットワーク設定のプラクティスを検討してください。

- Cockpit を使用してネットワークを設定。**nmtui** または **nmcli** を使用することも可能。
- 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します。データセンターまたはクラスターでの新しい論理ネットワークの作成 を参照。
- 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 インターフェイス: **physical_device.VLAN_ID** (例: **eth0.23**, **eth1.128**, **enp3s0.50**)
  - ボンディングインターフェイス: **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。Red Hat Virtualization ではネットワークチーミングはサポートされておらず、セルフホストエンジンのデプロイメントにホストが使用されたりホストが Manager に追加されたりすると、エラーが発生する原因となります。
- 推奨されるボンディングモードを使用。

- 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る。
- 仮想マシンが **ovirtmgmt** ネットワークを使用する場合には、**仮想マシンのゲストが接続するブリッジで使用される場合にどのボンディングモードが有効ですか?** を参照。
- 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、ボンディングモード 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 を設定します (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 +ipv4.gateway
123.123.0.254
```

- 以下の例に示すように、ボンディング上に VLAN を設定すします (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 +ipv4.gateway
123.123.0.254
```

- **firewalld** は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します。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。

4.5. セルフホストエンジンの推奨事項

- Red Hat Virtualization Manager およびその他のインフラストラクチャーレベルのサービス用に、別のデータセンターおよびクラスターを作成します (環境が十分大きく、それが可能な場合)。Manager 用仮想マシンは通常のクラスター内のホストで実行できますが、実稼働仮想マシンから分離することで、バックアップスケジュールが容易になり、パフォーマンス、可用性、およびセキュリティーが向上します。
- 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のデプロイメント時に作成されます。他の仮想マシンにはこのストレージドメインを使用しないでください。
- ストレージ負荷が大きいと予想される場合は、移行、管理、およびストレージネットワークを切り離し、Manager 用仮想マシンの健全性への影響を低減します。
- クラスターごとのホスト数には技術的にはハード制限はありませんが、セルフホストエンジンノードをクラスターごとに 7 ノードに制限します。(ラックを変えるなど) 耐障害性を強化する方法でサーバーを配置します。

- Manager 用仮想マシンがホスト間で安全に移行できるように、セルフホストエンジンノードはすべて同じ CPU ファミリーを持つようにします。さまざまなファミリーがある場合は、最も性能の低いものでインストールを開始します。

- Manager 用仮想マシンのシャットダウンまたは移行が必要な場合、Manager 用仮想マシンを再起動または移行できるだけの十分なメモリーがセルフホスト型エンジンノードに必要です。

付録A 法的通知