



# Red Hat Virtualization 4.2

## プランニングおよび前提条件ガイド

Red Hat Virtualization 4.2 のインストールおよび設定のプランニング



# Red Hat Virtualization 4.2 プランニングおよび前提条件ガイド

---

Red Hat Virtualization 4.2 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](mailto:rhev-docs@redhat.com)

## 法律上の通知

Copyright © 2018 Red Hat, Inc.

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

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

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

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

## 概要

本ガイドには、Red Hat Virtualization 環境の要件、オプション、および推奨事項を記載しています。

## 目次

<b>第1章 はじめに</b>	<b>3</b>
1.1. 最小のアーキテクチャー	3
<b>第2章 要件</b>	<b>4</b>
2.1. RED HAT VIRTUALIZATION MANAGER の要件	4
2.1.1. ハードウェア要件	4
2.1.2. ブラウザーの要件	4
2.1.3. クライアント要件	5
2.1.4. オペレーティングシステムの要件	6
2.2. ホストの要件	6
2.2.1. CPU の要件	6
2.2.1.1. プロセッサ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	7
2.2.2. メモリーの要件	7
2.2.3. ストレージの要件	7
2.2.4. PCI デバイスの要件	8
2.2.5. デバイス割り当てのハードウェア要件	8
2.2.6. vGPU の要件	9
2.3. ネットワーク要件	9
2.3.1. DNS 要件	9
2.3.2. Red Hat Virtualization Manager のファイアウォール要件	9
2.3.3. ホストのファイアウォール要件	11
2.3.4. データベースサーバーのファイアウォール要件	14
<b>第3章 考慮事項</b>	<b>15</b>
3.1. ホストのタイプ	15
3.1.1. Red Hat Virtualization Host	15
3.1.2. Red Hat Enterprise Linux ホスト	15
3.2. ストレージタイプ	15
3.2.1. NFS	16
3.2.2. iSCSI	16
3.2.3. ファイバーチャネル	16
3.2.4. Fibre Channel over Ethernet	17
3.2.5. Red Hat Gluster Storage	17
3.2.6. Red Hat Hyperconverged Infrastructure	17
3.2.7. Red Hat Ceph File System	17
3.2.8. POSIX 準拠 FS	17
3.2.9. ローカルストレージ	18
3.3. ネットワークの考慮事項	18
3.4. ディレクトリーサーバーのサポート	19
3.5. インフラストラクチャーに関する考慮事項	19
3.5.1. ローカルまたはリモートのホスティング	20
3.5.2. リモートのホスティングのみ	20
<b>第4章 推奨事項</b>	<b>22</b>
4.1. 一般的な推奨事項	22
4.2. セキュリティーに関する推奨事項	23
4.3. ホストに関する推奨事項	23
4.4. ネットワークに関する推奨事項	23
4.5. セルフホストエンジンに関する推奨事項	24



## 第1章 はじめに

Red Hat Virtualization は、複数の接続されたコンポーネントで構成され、各コンポーネントは、環境内で異なる役割を果たします。それらの要件を事前に計画/準備しておく、コンポーネントの通信と実行を効率化するのに役立ちます。

本ガイドでは以下の内容について説明します。

- ハードウェアおよびセキュリティの要件
- さまざまなコンポーネント向けの利用可能なオプション
- 環境を最適化するための推奨事項

### 1.1. 最小のアーキテクチャー

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

- Red Hat Virtualization Manager マシン 1 台
- 仮想マシンの高可用性には最小 2 台のホスト
- ストレージサービスを 1 つ。全ホストにアクセス可能である必要があります。

セルフホストエンジン環境には、以下が含まれます。

- セルフホストエンジンノード上でホストされている Red Hat Virtualization Manager 用仮想マシン 1 台
- 仮想マシンの高可用性には、最小 2 台のセルフホストエンジンノード
- ストレージサービスを 1 つ。全ホストにアクセス可能である必要があります。

詳しくは、『製品ガイド』の「[アーキテクチャー](#)」を参照してください。

## 第2章 要件

### 2.1. RED HAT VIRTUALIZATION MANAGER の要件

#### 2.1.1. ハードウェア要件

以下に記載するハードウェアの最小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。詳しくは、<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 のハードウェア要件

リソース	最小	推奨
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、 <a href="#">RHV Manager History Database Size Calculator</a> ツールを使用することができます。
ネットワークインターフェース	最小帯域幅 1 Gbps のネットワークインターフェースカード (NIC) 1 基	最小帯域幅 1 Gbps 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 ユーザーポータルには、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とオペレーティングシステムの組み合わせ。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に取り組みます。



- 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: 未検証ですが、正常に機能することが予想されるブラウザとオペレーティングシステムの組み合わせ。この階層には、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にはマイナーな問題のみの修正を試みます。

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
階層 1	Red Hat Enterprise Linux	Mozilla Firefox 延長サポート版 (ESR) のバージョン
階層 2	Windows	Internet Explorer 11 以降
	任意	Google Chrome または Mozilla Firefox の最新バージョン
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

### 2.1.3. クライアント要件

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リモートビューアー (**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補助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は、SPICE プロトコルを使用してアクセスされます。ゲストのオペレーティングシステムに QXL グラフィカルドライバーをインストールすると、SPICE の機能を向上/強化させることができます。

サポートされている 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 のサポートは下記のように階層に分かれます。

- 階層 1: Remote Viewer が全面的に検証済みで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 が部分的に検証済みで、正常に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。Red Hat のエンジニアリングチームは、この階層の remote-viewer で問題が発生した場合には、修正を試みます。

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 以降
	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済みの Red Hat Enterprise Linux 7 のベースインストール上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。

『インストールガイド』に記載されている以外の追加のレポジトリは有効化しないでください。

## 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。詳しくは、<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。

### 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 G1
  - Opteron G2
  - Opteron G3
  - Opteron G4
  - Opteron G5
- Intel
  - Conroe
  - Penryn

- Nehalem
- Westmere
- Sandybridge
- Haswell
- Haswell-noTSX
- Skylake (クライアント)
- Skylake (サーバー)
- IBM POWER8

#### 2.2.1.1. プロセッサ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 1 つ空いていることを確認して、**rescue** パラメーターを追記します。
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、プロセッサに必要な拡張があるか確認してください。また、次のコマンドを実行して、仮想化拡張機能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、プロセッサがハードウェア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。サポートされている RAM の最大値は 2 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、ゲストの RAM を必要に応じてのみ割り当てて、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ローカルストレージが必要です。本セクションでは、Red Hat Virtualization Host のストレージの最小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、Red Hat Virtualization Host の要件よりも多くなるはずです。

ホストのインストールには、最小限のストレージ要件があります。Red Hat 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ています。

**表2.4 Red Hat Virtualization Host の最小ストレージ要件**

パーティション	最小サイズ
/	6 GB
/home	1 GB
/tmp	1 GB
/boot	1 GB
/var	15 GB
/var/log	8 GB
/var/log/audit	2 GB
swap	1 GB
最小の合計	35 GB



#### 重要

セルフホストエンジンのシステム環境に RHV-M Virtual Appliance をインストールする場合には、**/var/tmp** は 5 GB 以上でなければなりません。

推奨の swap サイズについては、<https://access.redhat.com/ja/solutions/108483> 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、最小帯域幅が 1 Gbps のネットワークインターフェースを少なくとも 1 基搭載している必要があります。Red Hat は、各ホストには 2 つのネットワークインターフェースを搭載し、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ことを推奨します。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の PCI Express と従来の PCI デバイスの使用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ハードウェア要件

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 ルートポートは、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 では、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を推奨しています。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 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 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` コマンドで、システムにインストール済みの PCI デバイスの情報を表示することができます。

『インストールガイド』の「[PCI パススルーを有効にするためのホストの設定](#)」を参照してください。

## 2.2.6. vGPU の要件

vGPU を使用するためのホストと仮想マシンの設定に関する情報は、『[仮想マシン管理ガイド](#)』の「[仮想マシンへの vGPU のインストール](#)」を参照してください。

## 2.3. ネットワーク要件

### 2.3.1. DNS 要件

Manager およびホストにはすべて、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。Red Hat は DNS を使用することを推奨しています。名前解決に `/etc/hosts` ファイルを使用すると、より多くの作業が必要となり、エラーが発生する可能性がより高くなります。

Red Hat Virtualization 環境では DNS が幅広く使用されるため、環境の DNS サービスを同じ環境でホストされている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 環境が名前解決に使用する全 DNS サービスは、環境の外部でホストする必要があります。

### 2.3.2. Red Hat Virtualization Manager のファイアウォール要件

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` スクリプトにより、ファイアウォールを自動設定することができますが、`iptables` を使用している場合には、既存のファイアウォール設定はすべて上書きされます。既存のファイアウォール

ル設定を維持する場合には、Manager が必要とする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、必要な **iptables** ルールを **/etc/ovirt-engine/iptables.example** ファイルに保存します。**firewalld** を使用している場合には、**engine-setup** によって既存の設定は上書きされません。

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。

表2.5 Red Hat Virtualization Manager のファイアウォール要件

ポート	プロトコル	送信元	宛先	目的
-	ICMP	Red Hat Virtualization Host  Red Hat Enterprise Linux ホスト	Red Hat Virtualization Manager	任意  診断に役立つ場合があります。
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 アクセス  任意
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 アクセス
80、443	TCP	管理ポータルクライアント  VM ユーザーポータルクライアント  Red Hat Virtualization Host  Red Hat Enterprise Linux ホスト  REST API クライアント	Red Hat Virtualization Manager	HTTP および HTTPS 経由で Manager にアクセスできるようにします。

ポート	プロトコル	送信元	宛先	目的
6100	TCP	管理ポータル のクライアント  VM ユーザー ポータル のクライアント	Red Hat Virtualization Manager	Manager 上で Websocket プロ キシを実行して 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 プロキシアクセ スを提供します 。ただし、Web socket 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。
7410	UDP	Red Hat Virtualization Host  Red Hat Enter prise Linux ホスト	Red Hat Virtualization Manager	Kdump が有効 化されている 場合には、Ma nager が kdump の通知を受信 するためにこ のポートを開 放する必要が あります。
54323	TCP	管理ポータル のクライアント	Red Hat Virtualization Manager (Ima geIO Proxy サーバー)	ImageIO Proxy (ovirt-imageio -proxy) との通 信に必要です

### 2.3.3. ホストのファイアウォール要件

Red Hat Enterprise Linux ホストおよび Red Hat Virtualization Host (RHVH) には、システムのファイアウォールで複数のポートを開放する必要があります。ホストを Manager に追加する際には、ファイアウォールルールは、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。

表2.6 仮想化ホストのファイアウォール要件

ポート	プロトコル	送信元	宛先	目的
-----	-------	-----	----	----

ポート	プロトコル	送信元	宛先	目的
22	TCP	Red Hat Virtualization Manager	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Secure Shell アクセス 任意
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 アクセス
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 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。 任意
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 任意
5900 - 6923	TCP	管理ポータルクライアント VM ユーザー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。



ポート	プロトコル	送信元	宛先	目的
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のに使用します。このポートは、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。  任意
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、そのユーザーインターフェースにアクセスするために必要です。
16514	TCP	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	Red Hat Virtualization Host Red Hat Enterprise Linux ホスト	<b>libvirt</b> を使った仮想マシンの移行
49152 - 49216	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。
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

ポート	プロトコル	送信元	宛先	目的
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 ( <b>ovirt-imageio-daemon</b> ) との通信に必要です。
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。

### 2.3.4. データベースサーバーのファイアウォール要件

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アクセスをデータベースで許可する必要があります。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。

表2.7 データベースサーバーのファイアウォール要件

ポート	プロトコル	送信元	宛先	目的
5432	TCP、UDP	Red Hat Virtualization Manager Data Warehouse サービス 外部のシステム	Manager ( <b>engine</b> ) データベースサーバー Data Warehouse ( <b>ovirt-engine-history</b> ) 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

## 第3章 考慮事項

本章では、Red Hat Virtualization のさまざまなコンポーネントの利点、制限事項、および利用可能なオプションについて説明します。

### 3.1. ホストのタイプ

環境に最も適したホストタイプを使用します。必要な場合には、両方のホストタイプを同じクラスター内で使用することも可能です。

#### 3.1.1. Red Hat Virtualization Host

Red Hat Virtualization Host (RHVH) は、Red Hat Enterprise Linux ホストと比較した場合に、以下のような利点があります。

- 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な場合があります。
- 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、更新プロセスが効率化され、パッケージごとに個別に更新されるのではなく、イメージ全体がまとめて更新されます。
- 仮想マシンのホスティングやホスト自体の管理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、不要なパッケージとサービスはデプロイされず、悪用することができないため、操作が効率化され、全体的な攻撃ベクトルが少なくなります。
- Cockpit のユーザーインターフェースは、デフォルトで利用可能で、仮想マシンのモニタリングツール、セルフホストエンジン用の GUI インストーラーなど、Red Hat Virtualization 固有の拡張機能が含まれています。Cockpit は Red Hat Enterprise Linux ホストでサポートされていますが、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

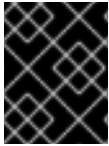
Red Hat Enterprise Linux ホストは、Red Hat Virtualization Host と比較した場合に、以下のような利点があります。

- Red Hat Enterprise Linux ホストは、高度なカスタマイズが可能なので、たとえば、ホストに特定のファイルシステムレイアウトが必要な場合などにはより望ましいでしょう。
- Red Hat Enterprise Linux ホストは、特に追加のパッケージをインストールする場合、頻繁な更新により適しています。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可能です。

### 3.2. ストレージタイプ

ストレージドメインは、ブロックデバイス (iSCSI または Fibre Channel) もしくはファイルシステムで構成されます。

以下の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にサポートされています。ISO とエクスポートドメインは、ファイルベースのストレージ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データセンターで使用する場合にローカルストレージをサポートします。



## 重要

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

### 参考資料

- 『管理ガイド』の「[ストレージ](#)」
- 『Red Hat Enterprise Linux ストレージ管理ガイド』

### 3.2.1. NFS

NFS バージョン 3 および 4 は Red Hat Virtualization 4 でサポートされています。NFS を ISO ストレージドメインとしてのみ使用する場合以外は、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 を 10GbE 上にデプロイし、VLAN で分離して、個々のサービスが特定のポートを使用するように設定すると、高速かつセキュアとなります。

NFS エクスポートは、ストレージのより多くのニーズに対応するようになっているため、Red Hat Virtualization は大型のデータストアをただちに認識します。ホスト上または Red Hat Virtualization 内からは追加の設定は必要ありません。このため、NFS はスケーリングと運用の面でブロックストレージを上回ります。

### 参考資料

- 『Red Hat Enterprise Linux ストレージ管理ガイド』の「[NFS \(Network File System\)](#)」
- 『管理ガイド』の「[NFS ストレージの準備と追加](#)」

### 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 を 10GbE 上にデプロイし、VLAN で分離して、CHAP 認証を利用すると、高速かつセキュアとなります。

iSCSI ではマルチパスを使用して高可用性を向上させることも可能です。

### 参考資料

- 『Red Hat Enterprise Linux ストレージ管理ガイド』の「[オンラインストレージ管理](#)」
- 『管理ガイド』の「[iSCSI ストレージの追加](#)」

### 3.2.3. ファイバーチャネル

ファイバーチャネルは、高速かつセキュアなので、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、活用すべきです。また、iSCSI と NFS に比べて CPU オーバーヘッドが低いという利点もあります。

ファイバーチャネルではマルチパスを使用して高可用性を向上させることも可能です。

### 参考資料

- 『Red Hat Enterprise Linux ストレージ管理ガイド』の「[オンラインストレージ管理](#)」
- 『管理ガイド』の「[FCP ストレージの追加](#)」

### 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** キーを有効化して、ホストに **vdsm-hook-fcoe** パッケージをインストールする必要があります。

参考資料

- 『Red Hat Enterprise Linux ストレージ管理ガイド』の「オンラインストレージ管理」
- 『管理ガイド』の「Red Hat Virtualization Manager で FCoE を使用するための設定方法」

### 3.2.5. Red Hat Gluster Storage

Red Hat Gluster Storage (RHGS) は POSIX 準拠のオープンソースファイルシステムです。Red Hat Gluster Storage のクラスターは、Network Attached Storage (NAS) アプライアンスや Storage Area Network (SAN) アレイの代わりに 3 台以上のサーバーで構成されます。

Red Hat Gluster Storage は 10GbE 上にデプロイし、VLAN で分離すべきです。

Red Hat Virtualization で RHGS を使用する前には、<https://access.redhat.com/articles/2356261> で互換性マトリックスを確認してください。

参考資料

- [Red Hat Gluster Storage](#)
- 『Configuring Red Hat Virtualization with Red Hat Gluster Storage』

### 3.2.6. Red Hat Hyperconverged Infrastructure

Red Hat Hyperconverged Infrastructure (RHHI) は、Red Hat Virtualization をリモートの Red Hat Gluster Storage サーバーに接続する代わりに、Red Hat Virtualization と Red Hat Gluster Storage を同じインフラストラクチャーに統合します。このコンパクトなオプションにより、運用の費用とオーバーヘッドが削減されます。

参考資料

- 『Red Hat Hyperconverged Infrastructure のデプロイ』
- 『Maintaining Red Hat Hyperconverged Infrastructure』

### 3.2.7. Red Hat Ceph File System

Red Hat Ceph File System (CephFS) は POSIX 標準と互換性のあるファイルシステムで、Ceph Storage Cluster を使用してデータを保管します。CephFS をストレージドメインとして追加する際には、Red Hat Virtualization 側で特別な設定は必要なく、他の POSIX 互換 FS ストレージを追加するのと同じ方法で追加します。

『Ceph File System Guide』を参照してください。

### 3.2.8. POSIX 準拠 FS

その他の POSIX 準拠ファイルシステムは、Red Hat Global File System 2 (GFS2) などのクラスター化されたファイルシステムで、スパーファイルと直接 I/O をサポートしている限りは、Red Hat Virtualization で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、直接 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。

参考資料

- [『Red Hat Enterprise Linux Global File System 2』](#)
- [『管理ガイド』の「POSIX 準拠ファイルシステムストレージの追加」](#)

### 3.2.9. ローカルストレージ

ローカルストレージは、ホスト自体のリソースを使用して、個別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、新しいデータセンターとクラスターに自動的に追加され、そこには他のホストは追加できません。単一のホストで構成されるクラスター内で作成された仮想マシンは、移行、フェンシング、スケジューリングはできません。

Red Hat Virtualization Host の場合は、/ (root) とは異なるファイルシステム上でローカルストレージを常に定義すべきです。Red Hat では、別の論理ボリュームまたはディスクを使用することを推奨しています。

[『管理ガイド』の「ローカルストレージの準備と追加」](#)を参照してください。

## 3.3. ネットワークの考慮事項

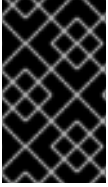
Red Hat Virtualization 環境におけるネットワークの計画と設定を行うにあたっては、ネットワークの概念と使用方法を十分に理解しておくことを強く推奨します。ネットワークの管理に関する詳しい情報は、ネットワークのハードウェアベンダーのガイドを参照してください。

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することができます。ボンディングを使用する場合は、そのボンディング内の全ネットワークカードでエラーが発生しなければボンディング自体は失敗しないため、高可用性が向上し、フォールトトレランスが高まります。ボンディングモード 1、2、3、4 は仮想マシン用またはそれ以外の用途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、6 は仮想マシン以外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) タグを使用してネットワークトラフィックを分離すると、複数の論理ネットワークで単一のデバイスを共有できるので、論理ネットワーク毎に 1 デバイスを使用する必要はありません。この機能を使用するには、VLAN タグがスイッチレベルでもサポートされている必要があります。

Red Hat Virtualization 環境で定義可能な論理ネットワーク数に適用される上限

- ホストにアタッチした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と仮想 LAN (VLAN) の最大数 (4096) を合わせた数が上限となっています。
- 1 回の操作でホストにアタッチできるネットワーク数は、現在 50 が上限となっています。
- ネットワークはクラスター内の全ホストで同じでなければならないため、クラスター内の論理ネットワークの数は、ホストにアタッチ可能な論理ネットワーク数が上限となっています。
- データセンター内の論理ネットワーク数は、そのデータセンター内のクラスター数に 1 クラスターで許可される論理ネットワーク数を掛け合わせた値のみが上限となります。

**重要**

管理ネットワーク (**ovirtmgmt**) のプロパティを変更する際には、最新の注意を払うようにしてください。ネットワークのプロパティを誤って変更すると、**ovirtmgmt** ネットワークによりホストへの接続ができなくなる可能性があります。

**重要**

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

### 3.4. ディレクトリーサーバーのサポート

インストール中には、Red Hat Virtualization Manager がデフォルトの **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、環境の初期設定時およびトラブルシューティング用に使用することを目的としています。**ovirt-aaa-jdbc-tool** を使用すると、**internal** ドメインに追加のユーザーを作成することができます。ローカルドメインに作成される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。『管理ガイド』の「[コマンドラインからのユーザー管理タスク](#)」を参照してください。

また、外部のディレクトリーサーバーを Red Hat Virtualization 環境に接続して、外部ドメインとして使用することができます。外部ドメインで作成される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。Manager への複数のディレクトリーサーバーのアタッチもサポートされています。

Red Hat Virtualization では以下のディレクトリーサーバーがサポートされています。サポートされているディレクトリーサーバーのインストールおよび設定に関する詳しい説明は、そのベンダーのドキュメントを参照してください。

#### Active Directory

<https://docs.microsoft.com/en-us/windows-server/identity/identity-and-access>

#### Identity Management (IPA をベースとする IdM)

[https://access.redhat.com/documentation/ja-JP/Red\\_Hat\\_Enterprise\\_Linux/7/html/Linux\\_Domain\\_Identity\\_Authentication\\_and\\_Policy\\_Guide/index.h](https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html)

#### Red Hat Directory Server 9 (389DS をベースとする RHDS 9)

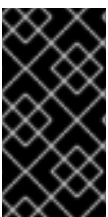
<https://access.redhat.com/documentation/en/red-hat-directory-server/>

#### OpenLDAP

<http://www.openldap.org/doc/>

#### IBM Security (Tivoli) Directory Server

[https://www.ibm.com/support/knowledgecenter/SSVJJU\\_6.4.0/com.ibm.IBMDS.doc\\_6.4/welcome.html](https://www.ibm.com/support/knowledgecenter/SSVJJU_6.4.0/com.ibm.IBMDS.doc_6.4/welcome.html)

**重要**

Red Hat Virtualization の管理ユーザーとして専用で使用する、全ユーザーとグループを参照するパーミッションを持つユーザーをディレクトリーサーバーに1つ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者ユーザーは、Red Hat Virtualization の管理ユーザーとしては使用しないでください。

『管理ガイド』の「[ユーザーとロール](#)」の章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考慮事項

### 3.5.1. ローカルまたはリモートのホスティング

以下のコンポーネントは、Manager またはリモートマシンでホストすることができます。全コンポーネントを Manage のマシンで保持する方がより簡単で、メンテナンスの手間が少なく済みます。したがって、これはパフォーマンスが問題とならない場合に望ましいオプションです。コンポーネントをリモートマシンに移動するとより多くのメンテナンスが必要となりますが、Manager と Data Warehouse のパフォーマンスはいずれも向上します。

#### Data Warehouse

Data Warehouse を Manager でホストするには、**engine-setup** のプロンプトで **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** のプロンプトで **No** を選択します。『**Data Warehouse Guide**』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。

#### Manager のデータベース

Manager データベースを Manager 上でホストするには、**engine-setup** のプロンプトで **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『**インストールガイド**』の「[リモートの PostgreSQL データベースの準備](#)」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、『**管理ガイド**』の「[リモートサーバー データベースへの engine データベースの移行](#)」を参照してください。

#### Websocket プロキシ

Websocket プロキシ を Manager でホストするには、**engine-setup** のプロンプトで **Yes** を選択します。

Websocket プロキシをリモートマシンでホストするには、**engine-setup** のプロンプトで **No** を選択します。『**インストールガイド**』の「[別のマシンへの Websocket プロキシのインストール](#)」を参照してください。

インストール後に Websocket プロキシを移行するには、『**管理ガイド**』の「[別のマシンへの Websocket プロキシの移行](#)」を参照してください。



#### 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と設定を行います。Data Warehouse、Manager データベース、Websocket プロキシはインストール後に外部でのみ設定することができます。

### 3.5.2. リモートのホスティングのみ

以下のコンポーネントは、リモートマシン上でホストする必要があります。

#### DNS

Red Hat Virtualization 環境では DNS が幅広く使用されるため、環境の DNS サービスを同じ環境でホストされている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。

#### ストレージ



---

[ローカルストレージ](#) と [Red Hat Hyperconverged Infrastructure](#) 以外の場合は、ストレージサービスは、Manager またはホストと同じマシン上に配置することはできません。

#### アイデンティティ管理

IdM (**ipa-server**) は、Manager が必要とする **mod\_ssl** パッケージとの互換性がありません。

## 第4章 推奨事項

本章では、環境のパフォーマンスや安定性を向上させることのできる (必須ではない) 設定について説明します。

### 4.1. 一般的な推奨事項

- デプロイメントが完了次第、完全なバックアップを取って、別の場所に保管します。それ以降は、定期的にバックアップを取ります。『[管理ガイド](#)』の「[バックアップと移行](#)」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のは避けてください。そのように設定する場合は、そのサービスを実行する仮想マシンでダウンタイムが発生する場合にその時間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 をインストールす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てください。値が 200 の場合には、Manager のセットアップが失敗する可能性があります。エントロピーの値を確認するには、`cat /proc/sys/kernel/random/entropy_avail` コマンドを実行してください。エントロピーの値を増やすには、`rng-tools` パッケージをインストールして、<https://access.redhat.com/solutions/1395493> に記載の手順に従ってください。
- PXE、キックスタート、Satellite、CloudForms、Ansible のいずれか、もしくはそれらを組み合わせて、ホストおよび仮想マシンのデプロイメントを自動化することができます。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。以下のリンクを参照してください。
  - PXE またはキックスタートを使用した RHVH の自動デプロイの追加の要件に関する情報: 『[インストールガイド](#)』の「[Red Hat Virtualization Host デプロイメントの自動化](#)」
  - 「[Red Hat Enterprise Linux 7 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](#)」
  - 「[Red Hat Enterprise Linux 7 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](#)」
  - 『[Red Hat Satellite 6.2 プロビジョニングガイド](#)』
  - 「[Red Hat CloudForms 4.5 仮想マシンとホストのプロビジョニング](#)」
  - 『[管理ガイド](#)』の「[Ansible を使用した設定作業の自動化](#)」
- デプロイ環境内の全マシンのタイムゾーンを UTC に設定します。このように設定すると、夏時間などのローカルタイムゾーンのばらつきによってデータ収集や接続が中断されることがなくなります。
- 時刻を同期するには、環境内の全ホストと仮想マシンで Network Time Protocol (NTP) を使用します。認証および証明書は、特に時間のずれの影響を受けます。`ntpd` で `chronyd` を使用することを推奨します。『[Red Hat Enterprise Linux 7 システム管理者のガイド](#)』の以下のセクションを参照してください。
  - 「[chrony スイートを使用した NTP 設定](#)」
  - 「[システムクロックのリモートサーバーとの同期](#)」

- 環境で作業する全ユーザーが、現在の状態と必要な手順を認識するための情報をすべて文書化してください。

## 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上のセキュリティー機能 (HTTPS、SELinux、ファイアウォールなど) は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信するには、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 に登録してください。
- 複数のユーザーがデフォルトの **admin** アカountを使用するのではなく、個別の管理者アカウントを作成して、アクティビティーを適切にトラッキングできるようにしてください。
- ホストへのアクセスは制限し、別個のログインを作成してください。全ユーザーに使用する単一の **root** ログインは作成しないでください。『Red Hat Enterprise Linux 7 システム管理者のガイド』の「[ユーザーとグループの管理](#)」を参照してください。
- 信頼されないユーザーをホスト上に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には、仮想化、パフォーマンス、セキュリティー、モニタリングの要件を満たすのに必要なパッケージとサービスのみをインストールしてください。実稼働環境のホストには、アナライザー、コンパイラーなどの不必要なセキュリティーリスクをもたらす追加のパッケージはインストールすべきではありません。

## 4.3. ホストに関する推奨事項

- 同じクラスター内のホストは統一してください。これには、ハードウェアの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の一貫性を保てなくなる可能性があります。
- Red Hat は、同じクラスター内における RHEL ホストと RHVH の両方の使用をサポートしていますが、この構成は、特定のビジネスまたは技術的な要件に対応する場合にのみ使用すべきです。
- デプロイ時にフェンシングデバイスを設定します。フェンシングデバイスは、高可用性に必要です。
- フェンシングのトラフィック用には、別のハードウェアスイッチを使用してください。モニタリングとフェンシングを同じスイッチ上で実行すると、そのスイッチは高可用性の単一障害点となってしまいます。

## 4.4. ネットワークに関する推奨事項

- 実稼働環境のホストでは特にネットワークインターフェースをボンディングしてください。ボンディングにより、全体的なサービスの可用性とネットワーク帯域幅が向上します。『[管理ガイド](#)』の「[Red Hat Virtualization におけるボンディングロジック](#)」を参照してください。
- パフォーマンスを最適化し、トラブルシューティングを簡素化するには、VLAN を使用して異なるトラフィックタイプを分離して、10GbE または 40GbE のネットワークを有効に活用してください。
- 1GbE ネットワークは、管理トラフィックのみに使用すべきです。10GbE と 40GbE は、仮想マシンとイーサネットベースのストレージに使用してください。

- ストレージに使用するために物理インターフェースをホストに追加する場合には、**VM ネットワーク** のチェックを外して、VLAN が物理インターフェースに直接割り当てられるようにしてください。
- Red Hat OpenStack Platform がすでにデプロイ済みの場合には、Red Hat Virtualization を OpenStack Networking (neutron) と統合して、Open vSwitch の機能を追加することができます。

## 4.5. セルフホストエンジンに関する推奨事項

- 環境が十分なサイズで可能な場合には、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とクラスターを作成します。Manager 用仮想マシンは、通常のクラスター内のホスト上で実行することが可能ですが、実稼働環境の仮想マシンと分離すると、バックアップスケジュール、パフォーマンス、可用性、セキュリティを向上させるのに役立ちます。
- Manager 用の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中に作成されます。このストレージドメインは、他の仮想マシンには一切使用しないでください。
- ストレージワークロードが高くなることが予想される場合には、移行、管理、ストレージのネットワークを分離して、Manager 用仮想マシンの正常性への影響を軽減してください。
- 1 クラスターあたりのホスト数には厳密にはハードリミットがありませんが、Red Hat では、セルフホストエンジンノードの数は、1 クラスターあたり 7 ノードを上限とすることを推奨しています。サーバーは、レジリエンスを向上させることのできる方法で分散してください (例: 複数のラックに分散するなど)。
- セルフホストエンジンノードはすべて、同じ CPU ファミリーに統一して、それらの間で Manager 用仮想マシンを安全に移行できるようにすべきです。異なる CPU ファミリーを使用する場合には、最も機能性の低いものからインストールを開始してください。
- Manager 用仮想マシンがシャットダウンされ、移行する必要がある場合には、セルフホストエンジンノードにその Manager 用仮想マシンを再起動または移行するために十分なメモリーが必要です。