<https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/installing_red_hat_virtualization_as_a_self-hosted_engine_using_the_cockpit_web_interface/index>

Использование веб-интерфейса Cockpit для установки системы Red Hat Virtualization в качестве виртуализованного ЦУ

[Использование веб-интерфейса Cockpit для установки системы Red Hat Virtualization в качестве виртуализованного ЦУ 1](#_Toc32334052)

[Использование Cockpit для установки диспетчера Red Hat Virtualization в виде виртуальной машины, выполняющейся на хостах под собственным управлением (виртуализованный центр управления). 2](#_Toc32334053)

[Необходимые условия и предпосылки 3](#_Toc32334054)

[Архитектура виртуализованного ЦУ 4](#_Toc32334055)

[Глава 1. Обзор процесса установки 5](#_Toc32334056)

[Глава 2. Требования 6](#_Toc32334057)

[2.1. Требования для работы виртуализированного ЦУ 6](#_Toc32334058)

[2.1.1. Требования к аппаратному обеспечению 7](#_Toc32334059)

[2.1.2. Требования к браузеру 7](#_Toc32334060)

[2.1.3. Требования к клиенту 8](#_Toc32334061)

[2.1.4. Требования к операционным системам 9](#_Toc32334062)

[2.2. Требования к хостам 9](#_Toc32334063)

[2.2.1. Требования к ЦП 9](#_Toc32334064)

[2.2.2. Требования к памяти 10](#_Toc32334065)

[2.2.3. Требования к хранилищу 10](#_Toc32334066)

[2.2.4. Требования к устройствам PCI 11](#_Toc32334067)

[2.2.5. Требования к выделяемым устройствам 12](#_Toc32334068)

[2.2.6. Требования к vGPU 13](#_Toc32334069)

[2.3. Требования к сетям 13](#_Toc32334070)

[2.3.1. Общие требования 13](#_Toc32334071)

[2.3.2. Требования к межсетевому экрану относительно DNS, NTP и операций блокады IPMI 13](#_Toc32334072)

[2.3.3. Требования к межсетевому экрану для виртуализированного ЦУ 14](#_Toc32334073)

[2.3.4. Требования к межсетевому экрану для хостов 16](#_Toc32334074)

[2.3.5. Требования к межсетевому экрану для баз данных 19](#_Toc32334075)

[Глава 3. Подготовка хранилища для системы виртуализации 21](#_Toc32334076)

[3.1. Подготовка хранилища NFS 22](#_Toc32334077)

[3.2. Подготовка хранилища iSCSI 22](#_Toc32334078)

[3.3. Подготовка хранилища FCP 23](#_Toc32334079)

[3.4. Preparing Red Hat Gluster Storage 24](#_Toc32334080)

[4. Установка хоста развёртывания виртуализированного ЦУ 25](#_Toc32334081)

[4.1. Установка хостов системы виртуализации 25](#_Toc32334082)

[4.1.1. Подключение репозиториев хоста виртуализации 27](#_Toc32334083)

[4.2. Установка хостов Red Hat Enterprise Linux 27](#_Toc32334084)

[4.2.1. Подключение репозиториев хостов Red Hat Enterprise Linux 28](#_Toc32334085)

[4.2.2. Установка Cockpit на хостах Red Hat Enterprise 29](#_Toc32334086)

[Глава 5. Установка диспетчера виртуализации 30](#_Toc32334087)

[5.1. Развёртывание виртуализированного ЦУ с помощью Cockpit 30](#_Toc32334088)

[5.2. Enabling the Red Hat Virtualization Manager Repositories 33](#_Toc32334089)

Red Hat Virtualization 4.3

Использование Cockpit для установки диспетчера Red Hat Virtualization в виде виртуальной машины, выполняющейся на хостах под собственным управлением (виртуализованный центр управления).

**Аннотация**

В данном документе описывается процесс установки среды Виртуализованного Центра управления, то есть диспетчера (он же «Центр управления») виртуализации, установленного на виртуальной машине, выполняющейся на адаптированных хостах в окружении под управлением этой же виртуальной машины. Установка выполняется с использованием веб-интерфейса Cockpit, с помощь которого настраивается и выполняется автоматизированная установка.

**Необходимые условия и предпосылки установки**

Автоматизация установки виртуализованного ЦУ выполняется с помощью системы Ansible. Мастер установки веб-интерфейса Cockpit запускается на хосте начального развёртывания, а Центр Управления виртуализацией устанавливается и настраивается на ВМ, создаваемой на хосте развёртывания. Базы данных ЦУ и хранилища данных устанавливаются на ВМ Центра управления, но, при необходимости, могут быть перенесены на отдельный сервер после завершения установки.

Cockpit по умолчанию присутствует в составе Red Hat Virtualization Hosts, также его можно установить на хостах Red Hat Enterprise Linux.

Хосты, на которых может выполняться виртуальная машина Центра управления, называются «узлы виртуализированного ЦУ». Для поддержки высокой доступности требуется минимум два таких узла.

Домен хранилища, выделенный для ВМ диспетчера, называется «домен хранилища виртуализированного ЦУ». Этот домен хранилища создаётся сценарием установки, поэтому перед началом установки необходимо подготовить базовую систему хранения.

Сведения о параметрах окружения и рекомендуемой конфигурации ищите в документе *Planning and Prerequisites Guide* . Сведения о параметрах, имеющих отношение непосредственно к окружению виртуализованного ЦУ, ищите в документе Self-Hosted Engine Recommendations .

**Таблица 1. Ключевые компоненты системы виртуализации Red Hat Virtualization**

|  |  |
| --- | --- |
| **Название компонента** | **Описание** |
| Центр управления системой виртуализации (диспетчер виртуализации) | Служба, предоставляющая графический интерфейс пользователя и REST API для управления ресурсами окружения. Диспетчер устанавливается на физической или виртуальной машине под управлением Red Hat Enterprise Linux. |
| Хосты | Хосты Red Hat Enterprise Linux (хосты RHEL) и хосты Red Hat Virtualization (гипервизоры на базе образов) — это два поддерживаемых типа хостов. На хостах используется технология Kernel-based Virtual Machine (KVM), и они предоставляют ресурсы, необходимые для работы виртуальных машин. |
| Разделяемое хранилище | Служба хранилищ, используемая для хранения данных, связанных с виртуальными машинами. |
| Хранилище данных | Служба, получающая информацию о параметрах и статистику из Центра управления |

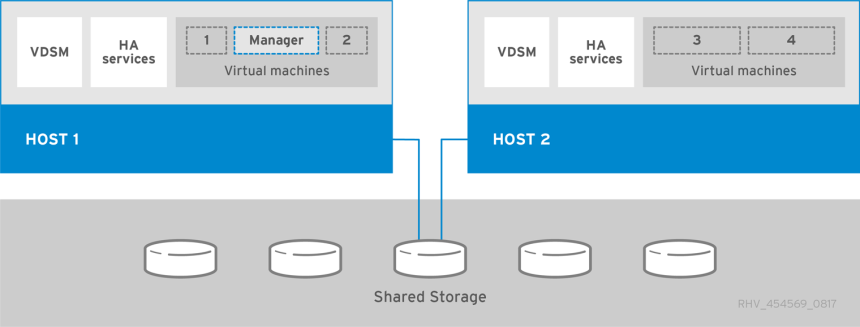
**Архитектура виртуализованного ЦУ**

Диспетчер виртуализации Red Hat Virtualization работает в виде виртуальной машины на узлах виртуализированного ЦУ (адаптированные хосты) в том же самом окружении, которым управляет данная ВМ. Окружение виртуализированного ЦУ требует на один физический сервер меньше, но взамен требует дополнительной работы от администратора для его разворачивания и управления. Диспетчер виртуализации является высоко доступным без дополнительного стороннего управления высокой доступностью.

Минимальный набор окружения виртуализированного ЦУ включает в себя:

* Одну виртуальную машину с диспетчером системы виртуализации Red Hat Virtualization, расположенную на узле виртуализированного ЦУ. Для автоматизации установки ВМ под управлением Red Hat Enterprise Linux 7 и диспетчера виртуализации на этой машине используются готовые образы RHV-M Appliance.
* Минимум два узла виртуализированного ЦУ для высокой доступности ВМ. Для этого можно использовать хосты Red Hat Enterprise Linux или хосты Red Hat Virtualization. Для облегчения обмена информацией с диспетчером виртуализации на всех хостах работает интерфейс VDSM (агент узлов). Задачами высокой доступности виртуальной машины с диспетчером управляют службы высокой доступности, запущенные на всех узлах виртуализированного ЦУ.
* Одна служба хранилищ, которая может размещаться локально или на удалённом сервере, в зависимости от используемого типа хранилища. К службе хранилища должны иметь доступ все хосты.

**Рисунок 1. Архитектура виртуализированного ЦУ системы виртуализации**



# Обзор процесса установки

В процессе установки виртуализированного ЦУ используется программа Ansible, а также RHV-M Appliance (предварительно настроенный образ ВМ диспетчера виртуализации) для автоматизации следующих задач:

* Настройка узла виртуализированного ЦУ
* Установка на этом узле ВМ под управлением Red Hat Enterprise Linux
* Установка и настройка на этой машине диспетчера системы виртуализации
* Настройка домена хранилища виртуализированного ЦУ

ВНИМАНИЕ

Образ RHV-M Appliance используется только во время установки. Для обновления диспетчера он не используется.

Процесс установки окружения виртуализированного ЦУ состоит из следующих этапов:

1. Подготовка хранилища для работы с доменом хранилища виртуализированного ЦУ и со стандартными домена хранилища. Можно использовать один из следующих типов хранилищ:
   * NFS
   * iSCSI
   * оптоволоконный канал (FCP)
   * хранилище Gluster
2. Установка хоста развёртывания для запуска на нём установки. Этот хост станет первым узлом виртуализированного ЦУ. Можно использовать любой тип хоста:
   * Red Hat Virtualization Host
   * Red Hat Enterprise Linux

Cockpit по умолчанию доступен в хостах системы виртуализации Red Hat, и доступен для установки на хостах Red Hat Enterprise Linux.

1. Установка и настройка диспетчера виртуализации:
2. Установка виртуализированного ЦУ с помощью веб-интерфейса Cockpit, доступного на хосте развёртывания
3. Регистрация диспетчера в сети доставки данных и активация репозиториев диспетчера системы виртуализации
4. Подключение к порталу администрирования для добавления хостов и доменов хранилищ
5. Добавление в диспетчер узлов виртуализированного ЦУ и стандартных хостов. На узлах виртуализированного ЦУ может работать как ВМ диспетчера, так и другие ВМ. На стандартных хостах могут все другие ВМ, кроме ВМ диспетчера. Используйте либо один из типов хостов, либо оба:
   * + Red Hat Virtualization Host
     + Red Hat Enterprise Linux
   * Добавьте хосты в виртуализированный ЦУ в виде узлов виртуализированного ЦУ .
   * Добавьте хосты в ЦУ в виде стандартных хостов.
6. Добавьте дополнительные домены хранилищ в ЦУ. Домен хранилища виртуализированного ЦУ рекомендуется для работы только ВМ диспетчера, и ни для чего другого.
7. При желании разметить какие-либо базы данных или хосты на сервере отдельно от диспетчера виртуализации, то можно провести их миграцию после завершения процесса установки.

**ВАЖНО**

Регулярно обновляйте версии ПО окружения. Поскольку обновления с исправлениями ошибок кода выходят довольно часто, мы рекомендуем внести операции по обновлению ПО хостов и диспетчера виртуализации в список периодических заданий.

# Требования

## Требования для работы виртуализированного ЦУ

### Требования к аппаратному обеспечению

Указанные здесь минимальные и рекомендованные аппаратные конфигурации основаны на типичных случаях установок от небольших и средних размеров. Точные требования отличаются в зависимости от требований размеров и нагрузки.

**Таблица 2.1. Требования к аппаратному обеспечению для диспетчера системы виртуализации**

|  |  |  |
| --- | --- | --- |
| **Ресурс** | **Минимум** | **Рекомендуется** |
| ЦП | Двухъядерный процессор | Четырёхядерный процессор или несколько двухъядерных. |
| ОЗУ | 4Гбайт доступной системной памяти при условии, что хранилище данных не установлено, и если память не потребляется существующими процессами. | 16Гбайт системной памяти |
| Жёсткий диск | 25Гбайт локально доступного места на диске с возможностью для записи | 50Гбайт локально доступного места на диске с возможностью для записи |
| Сетевой интерфейс | Одна сетевая карта (NIC) с минимальной пропускной способностью в 1 Гб/сек | Одна сетевая карта (NIC) с минимальной пропускной способностью в 1 Гб/сек |

### Требования к браузеру

Для доступа к порталу администрирования и порталу ВМ можно использовать следующие версии браузеров и операционных систем.

Поддержка браузеров разделена на категории:

* Категория 1: полностью протестированное и полностью поддерживаемое сочетание браузера и ОС. Для браузеров этой категории выполняется исправление ошибок, возникающих при работе виртуализированного ЦУ с этими браузерами.
* Категория 2: частично протестированное сочетание браузера и ОС, которое скорее всего будет работать. Для этой категории предоставляется ограниченная поддержка. Инженеры Red Hat постараются исправить ошибки при работе с браузерами этой категории.
* Категория 3: не протестированное сочетание браузера и ОС, которое, возможно, заработает. Для этой категории предоставляется минимальная поддержка. Инженеры Red Hat постараются исправить только незначительные ошибки при работе с браузерами этой категории.

**Таблица 2.2. Требования к браузеру**

|  |  |  |
| --- | --- | --- |
| Категория поддержки | Семья операционных систем | Браузер |
| Категория 1 | Red Hat Enterprise Linux | Mozilla Firefox с расширенной поддержкой (Mozilla Firefox Extended Support Release, ESR) |
|  | Любая | Самая свежая версия браузеров Google Chrome, Mozilla Firefox или Microsoft Edge |
| Категория 2 |  |  |
| Категория 3 | Любая | Более ранние версии браузеров Google Chrome или Mozilla Firefox |
|  | Любая | Другие браузеры |

### Требования к клиенту

Доступ к консолям ВМ возможен только при использовании клиентов программы удалённого просмотра Remote Viewer (virt-viewer) в ОС Red Hat Enterprise Linux и Windows. Установка virt-viewer требует администраторских привилегий.

Получить доступ к консолям ВМ можно только с помощью протоколов SPICE, VNC или RDP (только для ОС Windows). Для улучшенной/расширенной функциональности SPICE в гостевую ОС можно установить графический драйвер QXL. Максимальное разрешение, поддерживаемое на данный момент SPICE, составляет 2560x1600 пикселей.

Поддерживаемые драйверы QXL доступны в ОС Red Hat Enterprise Linux, Windows XP и Windows 7.

Поддержка SPICE разделена на категории:

* Категория 1: операционные системы, в которых было произведено полное тестирование Remote Viewer и имеется его поддержка.
* Категория 2: операционные системы, в которых было произведено частичное тестирование Remote Viewer, и он, скорей всего, заработает. Для этой категории предоставляется ограниченная поддержка. Инженеры Red Hat постараются исправить ошибки работы удалённого просмотра в этой категории.

**Таблица 2.3. Поддержка SPICE в клиентских ОС**

|  |  |
| --- | --- |
| **Категория поддержки** | **Операционная система** |
| Категория 1 | Red Hat Enterprise Linux 7.2 и более поздние |
|  | Microsoft Windows 7 |
| Категория 2 | Microsoft Windows 8 |
|  | Microsoft Windows 10 |

### Требования к операционным системам

Диспетчер системы виртуализации должен быть установлен в базовой системе Red Hat Enterprise Linux 7 с программным обеспечением, обновлённым до последней минорной версии.

Не устанавливайте никаких дополнительных пакетов после базовой установки, поскольку это может повлечь за собой проблемы пакетных зависимостей во время установки пакетов, необходимых для работы виртуализированного ЦУ.

Не подключайте никаких дополнительных репозиториев, кроме тех, которые нужны для установки виртуализированного ЦУ .

## Требования к хостам

### Требования к ЦП

Все процессоры должны поддерживать расширения Intel® 64 или AMD64, с включённым расширением аппаратной виртуализации AMD-V™ или Intel VT®. Также необходима поддержка флага No eXecute (NX).

Поддерживаются следующие модели ЦП:

* AMD
  + Opteron G4
  + Opteron G5
  + EPYC
* Intel
  + Nehalem
  + Westmere
  + Sandybridge
  + Haswell
  + Haswell-noTSX
  + Broadwell
  + Broadwell-noTSX
  + Skylake (клиент)
  + Skylake (сервер)
* IBM POWER8

#### Проверка поддержки процессором требуемых флагов

В BIOS должна быть включена поддержка виртуализации. Отключите и перезагрузите хост после её включения, чтобы убедиться в том, что изменения вступили в силу.

1. Находясь в загрузочном экране хоста Red Hat Enterprise Linux или Red Hat Virtualization, нажмите любу клавишу и выберите в списке элемент **Загрузка** или **Загрузка в последовательную консоль**.
2. Нажмите клавишу Tab для редактирования параметров ядра для выбранной опции.
3. Убедитесь в том, что после последнего указанного параметра ядра есть пробел, и добавьте параметр rescue.
4. Нажмите клавишу Ввод чтобы загрузиться в режиме восстановления
5. В приглашении командной строки с помощью следующей команды узнайте, имеет ли процессор нужные расширения, и активированы ли они:

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

Если будет показан хоть какой-то вывод, то ЦП поддерживает аппаратную виртуализацию. Если никакого вывода не будет, ЦП всё ещё может иметь поддержку; в некоторых случаях производители отключают расширения виртуализации в BIOS. Если, по вашему мнению, это ваш случай, обратитесь к руководствам по BIOS и материнской плате машины.

### Требования к памяти

Минимальный требуемый объём памяти — 2Гб. Максимальный поддерживаемый объём памяти на одну виртуальную машину на хостах Red Hat Virtualization — 4Тб.

Тем не менее, требуемый объём ОЗУ зависит от требований к гостевой ОС, требованиям к гостевым приложениям, а также от активности и использования памяти гостем. Кроме того, KVM может также выделить слишком много физической памяти виртуальным гостям, так что объём, требуемый гостям, может превышать физически доступный объём, исходя из предположения, что не все гостевые ОС работают параллельно на пиковой загрузке. При этом KVM выделяет ОЗУ гостям по требованию, и перемещает мало используемые гостевые ОС на работу с подкачкой.

### Требования к хранилищу

Для хранения параметров, файлов журналов, дампа ядра и для использования файла подкачки хостам нужно хранилище. Хост Red Hat Virtualization может загружаться, имея одно, несколько или все свои размещения по умолчанию в сетевом хранилище. В случае сбоя сети, загрузка из сетевого хранилища может привести к зависанию. Добавление замещающего конфигурационного файла с несколькими путями может помочь в разрешении проблемы потери сетевой связи. Если загружающийся из хранилища SAN хост системы виртуализации потеряет связь, то все файлы станут доступны только для чтения, пока не будет восстановлена сеть. Использование сетевого хранилища может привести к снижению производительности.

В данном разделе приводятся минимальные требования к хранилищам для хостов системы виртуализации. Требования к хранилищам для хостов Red Hat Enterprise Linux изменяются в зависимости от объёма дискового пространства, используемого текущей конфигурацией, но, как правило, их объёмы больше, чем объёмы хранилища для хостов системы виртуализации.

Ниже приводятся минимальные требования к размерам хранилищ для установки хоста, но мы рекомендуем использовать значения по умолчанию.

* / (root) - 6 Гбайт
* /home - 1 Гбайт
* /tmp - 1 Гбайт
* /boot - 1 Гбайт
* /var - 15 Гбайт
* /var/crash - 10 Гбайт
* /var/log - 8 Гбайт
* /var/log/audit - 2 Гбайт
* подкачка - 1 Гбайт
* Программа установки Anaconda резервирует 20% от размера тонкого пула в рамках группы томов для будущего наращивания метаданных. Это делается для того, чтобы исключить ситуацию нехватки места в нормальных условиях эксплуатации при использовании конфигурации по умолчанию. Избыточное выделение пулов разреженных (тонких) томов во время установки также не поддерживается.
* **Минимальный общий объём — 55 Гбайт**

Если для дальнейшей установки виртуализированного ЦУ также планируется установка образа RHV-M Appliance, то размер /var/tmp должен быть не меньше 5 Гбайт.

Если планируется использовать превышенное выделение памяти, то размер подкачки должен быть достаточным для того, чтобы предоставлять виртуальную память для всех ВМ. Смотрите раздел «Оптимизация памяти».

### Требования к устройствам PCI

У хостов должен быть как минимум один сетевой интерфейс с минимальной пропускной способностью в 1Гб/сек. Мы рекомендуем для каждого хоста настроить два сетевых интерфейса, один из которых должен предназначаться для поддержки активно использующих сеть процессов, таких, как миграция виртуальных машин. Производительность таких операций ограничивается доступной пропускной способностью.

### Требования к выделяемым устройствам

Если планируется реализация присвоения устройств и сквозной доступ к PCI в целях использования виртуальной машиной конкретного устройства PCI хоста, убедитесь в том, что соблюдаются следующие условия:

* ЦП должен поддерживать IOMMU (например, VT-d или AMD-Vi). IBM POWER8 поддерживает IOMMU по умолчанию.
* Встроенные программы должны поддерживать IOMMU.
* Корневые порты ЦП должны иметь поддержку ACS или возможностей, эквивалентных ACS
* Устройства PCIe должны иметь поддержку ACS или возможностей, эквивалентных ACS
* Рекомендуется, чтобы у всех коммутаторов PCIe и мостов между устройствами PCIe и корневыми портами имелась поддержка ACS
* Что касается поддержки GPU, то в качестве графических устройств, не использующих подключение VGA, система Red Hat Enterprise Linux 7 поддерживает присвоение устройств PCI для NVIDIA K-Series Quadro на базе PCI (модели серии 2000 или выше), GRID и Tesla. В настоящее время, в дополнение к стандартным эмулируемым интерфейсам VGA, к ВМ можно подключить до двух GPU. Эмулируемый VGA используется для предзагрузочных операций и установки, а затем, после загрузки графических драйверов, управление берёт на себя NVIDIA GPU. Обратите внимание, что карты NVIDIA Quadro 2000 и Quadro K420 не поддерживаются.

Чтобы получить сведения о том, отвечает ли аппаратное обеспечение этим требованиям, обратитесь к соответствующим спецификациям и паспортам на изделия. Для просмотра сведения об устройствах PCI, уже установленных в систему, используйте команду lspci –v.

### Требования к vGPU

Чтобы виртуальная машина могла использовать vGPU, хост должен отвечать следующим критериям:

* GPU, совместимый с vGPU
* ядро хоста с включённой поддержкой GPU
* установленный GPU с корректными драйверами
* Предварительно настроенный **mdev\_type**, соответствующий типам mdev, поддерживаемым устройством
* драйвера с поддержкой vGPU, установленные на каждом хосте кластера
* ОС виртуальной машины, поддерживаемая данным vGPU, с установленными драйверами vGPU

## Требования к сетям

### Общие требования

Для системы виртуализации необходимо, чтобы на компьютере или ВМ, где работает виртуализированный ЦУ (такая ВМ называется также «машина диспетчера»), поддержка IPv6 оставалась включённой. Не отключайте поддержку IPv6 на машине диспетчера, даже если в вашей системе этот протокол не используется.

### Требования к межсетевому экрану относительно DNS, NTP и операций блокады IPMI

Требования к межсетевому экрану для всех подразделов ниже являются особыми случаями, которые требуют индивидуального рассмотрения.

**DNS и NTP**

Система виртуализации Red Hat Virtualization не создаёт серверов DNS или NTP, поэтому в межсетевом экране не нужны открытые порты для входящего трафика.

По умолчанию, в Red Hat Enterprise Linux разрешён исходящий трафик DNS и NTP по любому адресу назначения. При запрете исходящего трафика настраивайте исключения для запросов, посылаемых на адреса серверов DNS и NTP.

ВАЖНО

Диспетчер виртуализации и все хосты (как хосты виртуализации, так и обычные хосты) должны иметь полное доменное имя, а также отлично выравненное прямое и обратное разрешение имён.

Система виртуализации Red Hat Virtualization не поддерживает запуск службы DNS в виде виртуальной машины в среде виртуализации. Все службы DNS, используемые в среде виртуализации Red Hat Virtualization, должны размещаться за пределами окружения.

Для разрешения имён настоятельно рекомендуется использование DNS, а не файл /etc/hosts. Использование файла hosts обычно требует повышенных трудозатрат и повышает шансы возникновения ошибок.

**IPMI и другие механизмы операций блокады (по желанию)**

Для работы IPMI (интеллектуальный интерфейс управления платформой) и других механизмов операции блокады не требуются открытые порты на входящий трафик.

В Red Hat Enterprise Linux о умолчанию разрешён исходящий трафик IPMI на порты любых адресов назначения. При запрете исходящего трафика настраивайте исключения для запросов, посылаемых на ваши серверы IPMI.

Каждый хост виртуализации и каждый обычный хост в кластере должны иметь возможность связаться с устройствами операций блокады на всех хостах кластера. Если хосты кластера получают ошибки (ошибки сетевого подключения, ошибки хранилища и т.п.) и не могут выполнять свои функции, то они должны иметь возможность связаться с другими хостами в дата-центре.

Конкретные номера портов зависят от типа используемого агента операции блокады и его параметров.

Таблицы с требованиями к межсетевому экрану в разделах ниже не отражают этот параметр.

### Требования к межсетевому экрану для виртуализированного ЦУ

Виртуализированному ЦУ требуются несколько открытых портов для разрешения пропуска трафика сквозь системный межсетевой экран.

Сценарий engine-setup может автоматически настроить межсетевой экран, но, в случае с использованием **iptables**, все ранее настроенные параметры будут перезаписаны. При желании сохранить существующую конфигурацию межсетевого экрана, необходимо будет вручную указать нужные правила. Команда engine-setup сохраняет список правил iptables в файле **/etc/ovirt-engine/iptables.example**. В случае использования **firewalld, сценарий** engine-setup не перезаписывает текущие параметры.

Приводимые здесь параметры межсетевого экрана предполагают конфигурацию по умолчанию.

**Таблица 2.4. Требования к межсетевому экрану для виртуализированного ЦУ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Порт | Протокол | Исходная точка | Конечная точка | Назначение | Шифрование по умолчанию |
| M1 | - | ICMP | Хосты системы виртуализации  Обычные хосты | Диспетчер виртуализации | По желанию. Может помочь в диагностике | Нет |
| M2 | 22 | TCP | Системы, используемые для обслуживания диспетчера, включая параметры серверной части и обновления ПО | Диспетчер виртуализации | Доступ по протоколу Secure Shell (SSH)  По желанию. | Да |
| M3 | 2222 | TCP | Доступ клиентов к последовательным консолям ВМ | Диспетчер виртуализации | Доступ по протоколу Secure Shell (SSH) для возможности подключения к последовательным консолям ВМ | Да |
| M4 | 80, 443 | TCP | Клиенты портала администрирования  Клиенты портала виртуальных машин  Обычные хосты  Клиенты REST API | Диспетчер виртуализации | Предоставляет доступ по протоколам HTTP (порт 80, соединение не зашифровано) и HTTPS (порт 443, соединение зашифровано) к диспетчеру виртуализации. HTTP перенаправляет соединения на HTTPS | Да |
| M5 | 6100 | TCP | Клиенты портала администрирования  Клиенты портала виртуальных машин | Диспетчер виртуализации | Предоставляет доступ websocket прокси для консольного веб-клиента, noVNC, когда websocket прокси работает на хосте диспетчера виртуализации. Но если websocket прокси работает на другом хосте, этот порт не используется. | Нет |
| M6 | 7410 | UDP | Хосты виртуализации  Обычные хосты | Диспетчер виртуализации | Если на хостах активен Kdump, откройте этот порт для слушающего fence\_kdump на диспетчере. fence\_kdump не предоставляет способа шифрования соединения, но этот порт можно вручную настроить на блокирование доступа с ненадлежащих хостов. |  |
| M7 | 54323 | TCP | Клиенты портала администрации | Диспетчер виртуализации  (сервер ImageIO Proxy) | Требуется для обмена информацией с ImageIO Proxy (ovirt-imageio-proxy). | Да |
| M8 | 6442 | TCP | Хосты виртуализации  Обычные хосты | База данных Open Virtual Network (OVN) южного направления | Подключение к базе данных Open Virtual Network (OVN) | Да |
| M9 | 9696 | TCP | Клиенты внешнего сетевого поставщика для OVN | Внешний сетевой поставщик для OVN | OpenStack Networking API | Да  Конфигурация создаётся сценарием engine-setup |
| M10 | 35357 | TCP | Клиенты внешнего сетевого поставщика для OVN | Внешний сетевой поставщик для OVN | OpenStack Identity API | Да  Конфигурация создаётся сценарием engine-setup |
| M11 | 53 | TCP, UDP | Диспетчер виртуализации | Сервер DNS | Запросы DNS-поиска из портов больше 1023 на порт 53, и ответы. По умолчанию открыты. | Нет |
| M12 | 123 | UDP |  | Сервер NTP | Запросы NTP из портов больше 1023 на порт 123, и ответы. По умолчанию открыты. | Нет |

ВНИМАНИЕ

В таблице не указывается порт для базы данных OVN северного направления (6641), так как в конфигурации по умолчанию единственным клиентом для базы данных OVN северного направления является ovirt-provider-ovn. Поскольку они оба работают на одном и том же хосте, то обмен информацией между ними не виден в сети.

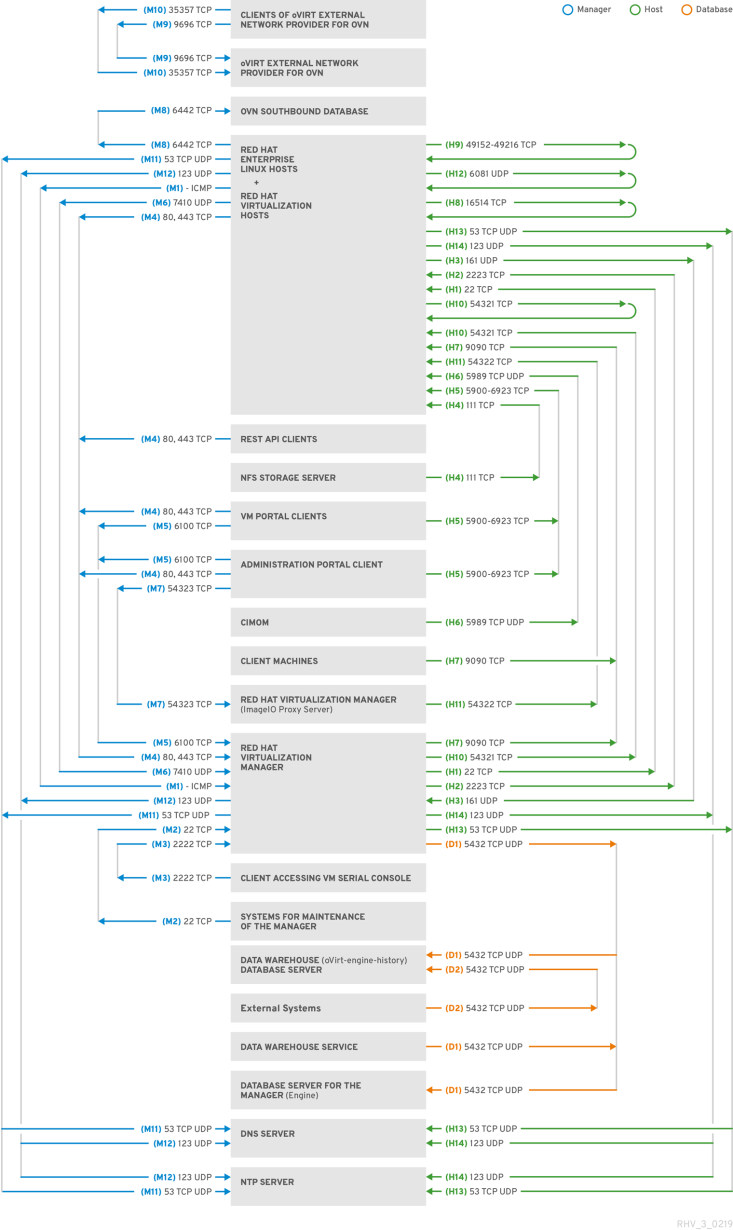
По умолчанию, в Red Hat Enterprise Linux разрешён исходящий трафик на DNS и NTP по любому адресу назначения. При запрете исходящего трафика сделайте исключения, чтобы диспетчер виртуализации мог посылать запросы на серверы DNS и NTP. Другим узлам тоже может понадобиться DNS и NTP, и в этих случаях получите сведения о требованиях для этих узлов и настройте межсетевой экран соответствующим образом.

### Требования к межсетевому экрану для хостов

Как хостам виртуализации, так и обычным хостам требуется некоторое число открытых портов с разрешённым сетевым трафиком. Правила межсетевого экрана автоматически настраиваются по умолчанию во время добавления нового хоста в виртуализированный ЦУ, при этом ранее существовавшие параметры межсетевого экрана будут перезаписаны.

Чтобы отключить автоматическую настройку межсетевого экрана при добавлении нового хоста, снимите галочку с параметра **Автоматически настраивать межсетевой экран хоста** в разделе **Дополнительные параметры**.

Просмотрите диаграмму с указанными в таблице выше требованиями к межсетевому экрану. Подключения в диаграмме можно найти по идентификаторам, указанным в таблице.



**Таблица 2.5. Требования к межсетевому экрану для хостов виртуализации**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Порты** | **Протокол** | **Исходная точка** | **Конечная точка** | **Назначение** | **Шифрование по умолчанию** |
| H1 | 22 | TCP | Диспетчер виртуализации | Хосты виртуализации  Обычные хосты | Доступ по протоколу Secure Shell (SSH)  По желанию | Да |
| H2 | 2223 | TCP | Диспетчер виртуализации | Хосты виртуализации  Обычные хосты | Доступ по протоколу Secure Shell (SSH) для возможности подключения к последовательным консолям ВМ | Да |
| H3 | 161 | UDP | Хосты виртуализации  Обычные хосты | Диспетчер виртуализации | Протокол Simple network management (SNMP). Нужен, только если требуется, чтобы ловушки SNMP посылались с хоста на один или несколько диспетчеров SNMP.  По желанию. | Нет |
| H4 | 111 | TCP | Сервер хранилища NFS | Хосты виртуализации  Обычные хосты | Подключения NFS.  По желанию. | Нет |
| H5 | 5900 - 6923 | TCP | Клиенты Портала администрирования  Клиенты портала виртуальных машин | Хосты виртуализации  Обычные хосты | Консольный доступ с использованием VNC и SPICE. Эти порты должны быть открыты для облегчения клиентского доступа к виртуальным машинам. | Да (по желанию) |
| H6 | 5989 | TCP, UDP | Диспетчер объектов CIM (CIMOM) | Хосты виртуализации  Обычные хосты | Используется диспетчерами объектов CIM (CIMOM) для мониторинга ВМ, выполняющихся на хосте. Нужно только в случае необходимости мониторинга ВМ в конкретной среде виртуализации. По желанию. | Нет |
| H7 | 9090 | TCP | Диспетчер виртуализации  Клиентские машины | Хосты виртуализации  Обычные хосты | Нужен для получения доступа к веб-интерфейсу Cockpit, если он установлен. | Да |
| H8 | 16514 | TCP | Хосты виртуализации  Обычные хосты | Хосты виртуализации  Обычные хосты | Миграция виртуальных машин с использованием **libvirt**. | Да |
| H9 | 49152 - 49215 | TCP | Хосты виртуализации  Обычные хосты | Хосты виртуализации  Обычные хосты | Миграция и блокада ВМ с помощью VDSM. Эти порты должны быть открыты для облегчения как автоматического, так и ручного переноса виртуальных машин. | Да.  В зависимости от агента операции блокады; миграция выполняется с использованием **libvirt**. |
| H10 | 54321 | TCP | Диспетчер виртуализации  Хосты виртуализации  Обычные хосты | Хосты виртуализации  Обычные хосты | Обмен данными VDSM с диспетчером виртуализации и другими хостами виртуализации | Да |
| H11 | 54322 | TCP | Диспетчер виртуализации  (сервер ImageIO Proxy) | Хосты виртуализации  Обычные хосты | Требуется для обмена данными с демоном ImageIO (ovirt-imageio-daemon). | Да |
| H12 | 6081 | UDP | Хосты виртуализации  Обычные хосты | Хосты виртуализации  Обычные хосты | Требуется в случае, если в качестве поставщика сети используется Open Virtual Network (OVN), чтобы дать OVN возможность создавать тоннели между хостами. | Нет |
| H13 | 53 | TCP, UDP | Хосты виртуализации  Обычные хосты | Сервер DNS | Запросы DNS-поиска с портов больше 1023 на порт 53, и ответы. Этот порт нужен и по умолчанию открыт. | Нет |

### Требования к межсетевому экрану для баз данных

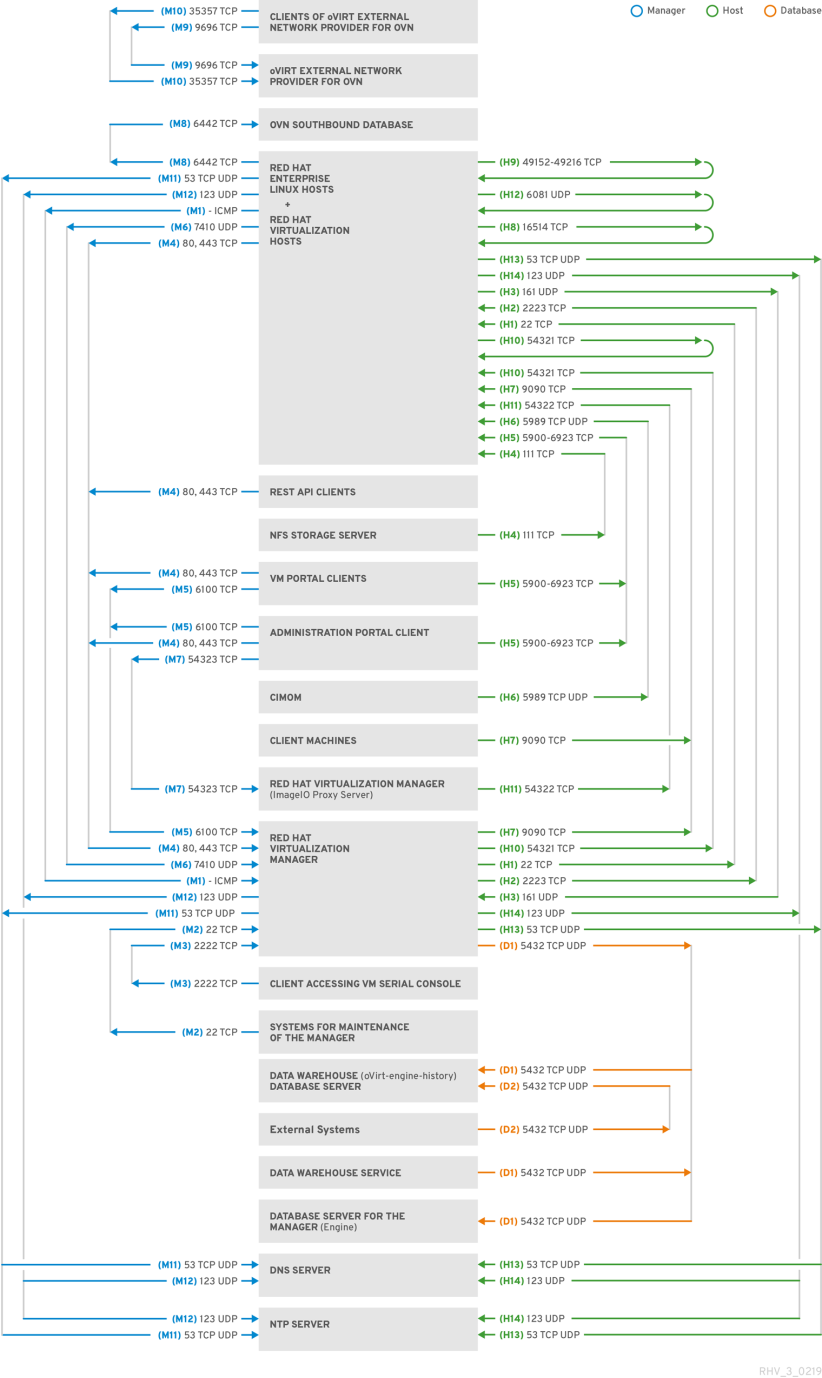
Система виртуализации Red Hat Virtualization поддерживает использование удалённого сервера баз данных с базой данных диспетчера виртуализации (engine) и базой данных хранилища данных (ovirt-engine-history). Если планируется использовать удалённый сервер баз данных, то он должен разрешать подключения от диспетчера виртуализации и службы хранилища баз данных (которая может быть отдельной от диспетчера).

По аналогии, если планируется доступ к локальной или удалённой базе данных хранилища данных из внешней системы, такой, как Red Hat CloudForms, то база данных должна разрешать подключения от этой системы.

ВАЖНО

Доступ к базе данных диспетчера виртуализации из внешних систем не поддерживается.

Просмотрите диаграмму с указанными в таблице выше требованиями к межсетевому экрану. Подключения в диаграмме можно найти по идентификаторам, указанным в таблице.



**Таблица 2.6. Требования к межсетевому экрану для сервера баз данных**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Порты** | **Протокол** | **Исходная точка** | **Конечная точка** | **Назначение** | **Шифрование по умолчанию** |
| D1 | 5432 | TCP, UDP | **Диспетчер виртуализации**  **Служба хранилища данных** | **Сервер базы данных диспетчера виртуализации** (engine)  Сервер базы данных хранилища данных (ovirt-engine-history) | **Порт по умолчанию для подключений базы данных** PostgreSQL | **Нет, но можно включить** |
| D2 | 5432 | TCP, UDP | **Внешние системы** | Сервер базы данных хранилища данных (ovirt-engine-history) | **Порт по умолчанию для подключений базы данных** PostgreSQL | **Нет, но можно включить** |

# Подготовка хранилища для системы виртуализации

Подготовьте хранилище, которое будет использоваться для доменов хранилищ в новом окружении. Окружение виртуализации Red Hat Virtualization должно иметь как минимум один домен хранилища данных, но рекомендуется добавить больше.

Домен хранилища содержит виртуальные жёсткие диски и файлы OVF всех ВМ и шаблонов дата-центра, и его нельзя сделать общим для всех дата-центров, пока он активен (но можно выполнять его миграцию между дата-центрами). В один и тот же дата-центр можно добавлять домены данных с несколькими типами хранилищ, при условии, что это разделяемые домены, а не локальные.

Виртуализированные центры управления должны иметь дополнительный домен данных, преднахзначнный для ВМ диспетчера виртуализации. Этот домен создаётся во время развёртывания виртуализированного ЦУ и должен иметь как минимум 74Гбайт. Перед началом установки необходимо подготовить хранилище для этого домена.

Можно использовать один из следующих типов хранилища:

* NFS
* iSCSI
* Fibre Channel (FCP)
* Red Hat Gluster Storage

ВАЖНО

При использовании хранилища iSCSI, домен хранилища виртуализированного ЦУ должен использовать свою собственную цель iSCSI. Цель iSCSI каждого дополнительного домена хранилища должна быть отличной от других.

ВНИМАНИЕ

Крайне рекомендуется создание дополнительных доменов хранилищ данных в том же самом дата-центре, в котором размещается и домен хранилищ виртуализированного ЦУ. Если развернуть виртуализированный ЦУ в дата-центре только с одним доменом хранилища данных, и этот домен будет повреждён, то у вас будет возможности добавить новые домены или удалить повреждённый; придётся разворачивать новый виртуализированный ЦУ.

## Подготовка хранилища NFS

Настройте общие ресурсы NFS в файловом хранилище или на удалённом сервере для использования их в качестве доменов хранилищ в системах виртуализации Red Hat. После экспорта общих ресурсов в удалённое хранилище и настройки их в диспетчере виртуализации, эти общие ресурсы будут автоматически импортированы на хосты виртуализации.

Для системы виртуализации требуются специальные системные учётные записи пользователей и системные группы пользователей, чтобы диспетчер виртуализации мог хранить данные в доменах хранилища, представленных экспортированные каталогами. Права доступа к одному каталогу настраиваются с помощью нижеследующей процедуры. Шаги chown и chmod необходимо повторить для каждого из каталогов, который предназначен для использования в качестве доменов хранилищ в системе виртуализации.

**Последовательность действий**

1. Создайте группу kvm:

# groupadd kvm -g 36

1. Создайте пользователя vdsm в группе kvm:

# useradd vdsm -u 36 -g 36

1. Настройте права владения экспортированного каталога на 36:36, что даст права владения vdsm:kvm:

# chown -R 36:36 /exports/data

1. Измените режим каталога так, чтобы у владельца были права на чтение и запись, а у группы и у других пользователей были права на чтение и запуск:

# chmod 0755 /exports/data

## Подготовка хранилища iSCSI

Система виртуализации поддерживает хранилища iSCSI, являющиеся доменом хранилища, созданный на базе группы тома, состоящей из номеров LUN. Группы томов и LUN могут быть присоединены только к одному домену хранилищ одновременно.

ВАЖНО

Если при использовании блочного хранилища планируется разворачивать ВМ на raw-устройствах или прямых LUN и администрировать их с помощью диспетчера логических томов, то необходимо создать фильтр для скрытия гостевых логических томов. Это предотвратит активацию гостевых томов при загрузке хоста, что могло бы привести к устареванию логических томов и повреждению данных.

ВАЖНО

Система виртуализации на данный момент не поддерживает хранилища с размером блока в 4Кбайт. Блочное хранилище необходимо настраивать в старом режиме (блоки размером в 512Б).

ВАЖНО

Если хост, загружаемый из хранилища SAN, теряет связь с хранилищем, то файловые системы хранилища переходят в режим только для чтения и остаются в нём после восстановления связи.

Для предотвращения такой ситуации мы рекомендуем добавление в корневую файловую систему SAN замещающего файла конфигурации с несколькими путями, чтобы обеспечить поставку в очередь загрузки LUN при восстановлении связи:

# cat /etc/multipath/conf.d/host.conf

multipaths {

multipath {

wwid boot\_LUN\_wwid

no\_path\_retry queue

}

## Подготовка хранилища FCP

Система виртуализации поддерживает хранилища SAN созданием домена хранилищ из группы томов, созданной из уже существующих LUN. Ни группы томов, ни LUN нельзя присоединить к более, чем одному домену хранилищ одновременно.

Администраторы системы виртуализации должны иметь практические знания о принципах работы с сетями хранения данных (SAN). Для обмена трафиком между хостами и общим внешним хранилищем в SAN обычно используется протокол FCP (Fibre Channel Protocol, протокол оптоволоконных каналов). По этой причине SAN иногда называют хранилищем FCP.

ВАЖНО

Если при использовании блочного хранилища планируется разворачивать ВМ на raw-устройствах или прямых LUN и администрировать их с помощью диспетчера логических томов, то необходимо создать фильтр для скрытия гостевых логических томов. Это предотвратит активацию гостевых томов при загрузке хоста, что могло бы привести к устареванию логических томов и повреждению данных.

ВАЖНО

Система виртуализации на данный момент не поддерживает хранилища с размером блока в 4Кбайт. Блочное хранилище необходимо настраивать в старом режиме (блоки размером в 512Б).

ВАЖНО

Если хост, загружаемый из хранилища SAN, теряет связь с хранилищем, то файловые системы хранилища переходят в режим только для чтения и остаются в нём после восстановления связи.

Для предотвращения такой ситуации мы рекомендуем добавление в корневую файловую систему SAN замещающего файла конфигурации с несколькими путями, чтобы обеспечить поставку в очередь загрузки LUN при восстановлении связи:

# cat /etc/multipath/conf.d/host.conf

multipaths {

multipath {

wwid boot\_LUN\_wwid

no\_path\_retry queue

}

## 3.4. Preparing Red Hat Gluster Storage

For information on setting up and configuring Red Hat Gluster Storage, see the [Red Hat Gluster Storage Installation Guide](https://access.redhat.com/documentation/en-us/red_hat_gluster_storage/3.4/html/installation_guide/).

For the Red Hat Gluster Storage versions that are supported with Red Hat Virtualization, see <https://access.redhat.com/articles/2356261>.

# Установка хоста развёртывания виртуализированного ЦУ

Виртуализированный ЦУ можно развернуть с хоста виртуализации или с обычного хоста.

ВАЖНО

Если для разделения различных типов трафика планируется использовать объединённые интерфейсы в конфигурации высокой доступности или в виртуальных LAN (например, для хранилищ или административных связей), то их следует настраивать на хосте перед началом установки виртуализированного ЦУ.

## Установка хостов системы виртуализации

Хост системы виртуализации — это минимальная ОС на базе Red Hat Enterprise Linux, разработанная для того, чтобы предоставить простой способ настройки физической машины для выполнения роли гипервизора в окружении системы виртуализации. Минимальная ОС содержит только пакеты, нужные машине для роли гипервизора, а также предлагает веб-интерфейс Cockpit для наблюдений за хостом и выполнения задач администрирования.

В целях повышения контроля безопасности, хосты виртуализации поддерживают разбиение на разделы по стандарту NIST 800-53, эта схема разделов применяется по умолчанию.

Минимальные требования для хостов.

**Последовательность действий**

1. Загрузите образ RHVH ISO:
   1. Выполните вход на портал <https://access.redhat.com>.
   2. Нажмите **Загрузки** на панели меню.
   3. Нажмите **Виртуализация**. Прокрутите вверх и нажмите Загрузить последние версии, чтобы получить доступ к странице загрузке продуктов.
   4. Перейдите к ссылке **Образ гипервизора для** и нажмите **Скачать**.
   5. Создайте загрузочный носитель.
2. Загрузите машину, на которую будет установлен хост виртуализации, с подготовленного загрузочного носителя.
3. В меню загрузки выберите **Установить** **RHVH 4.3** и нажмите Ввод.

ВНИМАНИЕ

Для доступа к редактированию параметров ядра можно также нажать Tab. Параметры ядра должны разделяться пробелом, а загрузить ядро с указанными параметрами можно нажатием клавиши Ввод. Для очистки любых внесённых изменений нажмите клавишу Esc и возвращайтесь в меню загрузки.

1. Выберите язык, затем нажмите **Продолжить**.
2. На экране **Дата и время** выберите часовой пояс и нажмите **Готово**.
3. На экране **Клавиатура** выберите раскладку и нажмите **Готово**.
4. На экране **Целевое устройство установки** выберите устройство, на которое нужно установить хост. По желанию включите шифрование. Нажмите **Готово**.

ВАЖНО

Мы настоятельно рекомендуем использовать параметр Настроить разделы автоматически.

1. На экране **Сеть и имя хоста** выберите сеть и нажмите **Настроить…**, чтобы настроить параметры соединения.

ВНИМАНИЕ

Чтобы использовать это соединение каждый раз при загрузке системы, отметьте галочкой параметр Автоматически подключаться к этой сети, когда она доступна.

В поле **Имя хоста** укажите имя хоста и нажмите **Готово**.

1. При необходимости, настройте **Языковую поддержку**, **Политику безопасности** и **Kdump**.
2. Нажмите **Начать установку**.
3. Пока устанавливается хост, настройте пароль root и, по желанию, создайте дополнительного пользователя.

ПРЕДУПРЕЖДЕНИЕ

Мы настоятельно рекомендуем не создавать недоверенных пользователей на хосте виртуализации, поскольку это может привести к эксплуатации местных уязвимостей защиты.

1. Нажмите **Перезагрузить** для завершения установки.

ВНИМАНИЕ

При перезагрузке виртуального хоста служба nodectl check выполняет проверку работоспособности хоста и выводит результат при авторизации пользователя в консоли. Сообщение node status: OK или node status: DEGRADED сообщает о результате проверки. Для получения подробностей выполните nodectl check. Эта служба включена по умолчанию.

### 4.1.1. Подключение репозиториев хоста виртуализации

Register the system to receive updates. Red Hat Virtualization Host only requires one repository. This section provides instructions for registering RHVH with the [Content Delivery Network](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/installing_red_hat_virtualization_as_a_self-hosted_engine_using_the_cockpit_web_interface/Installing_the_self-hosted_engine_deployment_host_SHE_cockpit_deploy#RHVH_CDN_register_SHE_deployment_host), or with [Red Hat Satellite 6](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/installing_red_hat_virtualization_as_a_self-hosted_engine_using_the_cockpit_web_interface/Installing_the_self-hosted_engine_deployment_host_SHE_cockpit_deploy#RHVH_Sat6_register_SHE_deployment_host).

## Установка хостов Red Hat Enterprise Linux

Хосты Red Hat Enterprise Linux представляют собой стандартную базовую установку Red Hat Enterprise Linux 7 на физическом сервере с подключёнными подписками Red Hat Enterprise Linux Server and Red Hat Virtualization.

Хост должен отвечать следующим минимальным требованиям:

ВАЖНО

В параметрах BIOS хоста должна быть включена поддержка виртуализации. Сведения об изменении параметров BIOS хоста ищите в документации к используемому аппаратному обеспечению.

ВАЖНО

На хостах Red Hat Enterprise Linux не должны устанавливаться сторонние модули наблюдения за безопасностью, так как они могут помешать работе демона модуля наблюдения, предоставляемого VDSM.

### Подключение репозиториев хостов Red Hat Enterprise Linux

Чтобы получить возможность использовать машину под управлением Red Hat Enterprise Linux в качестве хоста, необходимо зарегистрировать систему в сети Content Delivery Network, привязать подписки Red Hat Enterprise Linux Server и Red Hat Virtualization и активировать репозитории хоста.

**Procedure**

1. Register your system with the Content Delivery Network, entering your Customer Portal user name and password when prompted:

# subscription-manager register

1. Find the Red Hat Enterprise Linux Server and Red Hat Virtualization subscription pools and record the pool IDs:

# subscription-manager list --available

1. Use the pool IDs to attach the subscriptions to the system:

# subscription-manager attach --pool=id\_пула

Note

To view currently attached subscriptions:

# subscription-manager list --consumed

To list all enabled repositories:

# yum repolist

1. Configure the repositories:
2. # subscription-manager repos \
3. --disable='\*' \
4. --enable=rhel-7-server-rpms \
5. --enable=rhel-7-server-rhv-4-mgmt-agent-rpms \

--enable=rhel-7-server-ansible-2-rpms

For Red Hat Enterprise Linux 7 hosts, little endian, on IBM POWER8 hardware:

# subscription-manager repos \

--disable='\*' \

--enable=rhel-7-server-rhv-4-mgmt-agent-for-power-le-rpms \

--enable=rhel-7-for-power-le-rpms

For Red Hat Enterprise Linux 7 hosts, little endian, on IBM POWER9 hardware:

# subscription-manager repos \

--disable='\*' \

--enable=rhel-7-server-rhv-4-mgmt-agent-for-power-9-rpms \

--enable=rhel-7-for-power-9-rpms

1. Ensure that all packages currently installed are up to date:

# yum update

1. Reboot the machine.

### Установка Cockpit на хостах Red Hat Enterprise

Для наблюдения за ресурсами хоста и выполнения задач администрирования можно установить программу Cockpit.

**Последовательность действий**

1. Установите пакеты панели наблюдения:

# yum install cockpit-ovirt-dashboard

1. Активируйте и запустите службу cockpit.socket:

# systemctl enable cockpit.socket

# systemctl start cockpit.socket

1. Проверьте, является ли Cockpit активной службой в межсетевом экране:

# firewall-cmd --list-services

В списке должен присутствовать элемент cockpit. Если он отсутствует, выполните следующую команду с правами root для добавления cockpit в качестве службы в межсетевой экран:

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

Параметр --permanent поддерживает активность службы cockpit после перезагрузки.

Получить доступ к веб-интерфейсу Cockpit можно по адресу https://*полное\_доменное\_имя\_хоста\_или\_IP*:9090.

# Установка диспетчера виртуализации

Во время процесса развёртывания выполняется установка образа RHV-M Appliance; но, при необходимости, его можно установить на хосте развёртывания до начала установки:

# yum install rhvm-appliance

Ручная установка виртуальной машины диспетчера не поддерживается.

## Развёртывание виртуализированного ЦУ с помощью Cockpit

Разверните виртуализированный ЦУ с помощью веб-интерфейса Cockpit для сбора информации об окружении. Это рекомендованный метод. По умолчанию, Cockpit включается в хосты виртуализации, и его также можно установить на обычных хостах.

**Предпосылки и требования установки**

* Для диспетчера виртуализации и хоста развёртывания должны быть подготовлены полные доменные имена (FQDN). В DNS должны быть настроены записи как прямого, так и обратного просмотра.

**Последовательность действий**

1. Выполните вход в Cockpit по адресу https:// *полное\_доменное\_имя\_хоста\_или\_IP*:9090 и нажмите кнопки меню **Виртуализация** → **Виртуализированный ЦУ**.
2. Под параметром **Виртуализированный ЦУ** нажмите кнопку **Запустить**
3. Укажите сведения о виртуальной машине виртуализированного ЦУ:
   1. Укажите **Полное доменное имя ВМ диспетчера**. Это доменное имя виртуальной машины, а не базового хоста.
   2. Укажите **Адрес MAC** виртуальной машины диспетчера или примите случайно созданное значение.
   3. В выпадающем списке **Параметры сети** выберите значение **DHCP** или **Статичный**.

ВНИМАНИЕ

Для протокола IPv6 система виртуализации Red Hat Virtualization поддерживает только статичную адресацию.

* + - Если был выбран параметр **DHCP**, то для ВМ диспетчера должна существовать резервация DHCP, чтобы имя его хоста разрешалось на адрес, полученный от DHCP. Укажите его адрес MAC в соответствующем поле.
    - При выборе параметра **Статичный** введите следующую информацию:
      * **Адрес IP виртуальной машины** —адрес IP должен принадлежать той же подсети, к которой принадлежит и хост. Если, например, хост принадлежит подсети 10.1.1.0/24, то адрес IP машины диспетчера должен находиться в том же диапазоне (10.1.1.1-254/24).
      * Адрес шлюза
      * **Серверы DNS**
  1. В выпадающем списке выберите **Интерфейс моста**
  2. Введите и подтвердите **Пароль root** виртуальной машины
  3. Укажите, нужно ли разрешить **Доступ root по SSH**.
  4. Укажите **Число виртуальных ЦП** этой ВМ
  5. Укажите **Объём памяти (Мбайт)**. Доступный объём памяти отображается рядом с полем ввода.

1. При желании, разверните поля **Дополнительно**:
   1. Укажите **Открытый ключ SSH для root** для доступа root к ВМ виртуализированного ЦУ.
   2. Поставьте или снимите галочку с параметра **Изменение файла hosts**, чтобы указать, нужно ли добавлять записи ВМ диспетчера и базового хоста в файл /etc/hosts виртуальной машины. Убедитесь в том, что имена хостов разрешаются.
   3. Измените **Имя моста для администрирования** или примите значение по умолчанию ovirtmgmt.
   4. Укажите **Адрес шлюза** моста для администрирования
   5. Укажите **Полное доменное имя** первого хост, добавляемого в виртуализированный ЦУ. Это полное доменное имя базового хоста, на котором выполняется развёртывание.
2. Нажмите **Далее**.
3. Введите и подтвердите **Пароль администратора портала** для пользователя admin@internal .
4. Настройте уведомления о событиях:
   1. Укажите **Имя сервера** и **Номер порта сервера** для сервера SMTP.
   2. Укажите **Почтовый адрес отправителя**
   3. Укажите **Почтовый адрес получателя**
5. Нажмите **Далее**.
6. Просмотрите конфигурацию диспетчера и его ВМ. Если всё правильно, нажмите **Подготовить ВМ**.
7. По завершении установки ВМ нажмите **Далее**.
8. В выпадающем списке выберите **Тип хранилища** и укажите сведения о домене хранилища виртуализированного ЦУ:
   1. Для NFS:
      1. В поле **Подключение к хранилищу** укажите полный и путь до хранилища.
      2. При необходимости, укажите **Параметры монтирования**
      3. Укажите **Размер диска (Гбайт)**.
      4. В выпадающем списке выберите **Версию NFS**.
      5. Укажите **Доменное имя хранилища**.
   2. Для iSCSI:
      * Укажите **Адрес IP портала**, **Порт портала**, **Имя пользователя портала** и **Пароль портала**.
   3. Нажмите **Получить список целей** и выберите цель. Во время развёртывания можно выбрать только одну цель iSCSI, но для подключения всех порталов из одной и той же группы порталов есть поддержка механизма доступа по нескольким путям.

ВНИМАНИЕ

Чтобы иметь возможность указать более одной цели iSCSI, необходимо перед началом развёртывания виртуализированного ЦУ активировать механизм доступа по нескольким путям. Подробности ищите в документации к DM Multipath. Существует также утилита Multipath Helper, создающая сценарий для установки и настройки доступа по нескольким путям с разными параметрами.

* 1. Укажите **Размер диска (Гбайт)**.
  2. Укажите **Имя пользователя обнаружения** и **Пароль обнаружения**.
  3. Для оптоволоконного канала:
     + Укажите **Идентификатор** **LUN**. Хост-адаптеры шины должны быть настроены и подключены, а LUN не должны содержать никаких существующих данных.
     + Укажите **Размер диска (Гбайт)**.
  4. Для хранилища Gluster:
     + В поле **Подключение хранилища** укажите полный адрес и путь до хранилища.
     + При необходимости, укажите **Параметры монтирования**.
     + Укажите **Размер диска (Гбайт)**.

1. Нажмите **Далее**.
2. Просмотрите конфигурацию хранилища. Если вся информация верна, нажмите **Завершить развёртывание**.
3. По завершении процесса развёртывания нажмите **Закрыть**.

Один дата-центр, кластер, хост, домен хранилища и ВМ диспетчера виртуализации на этот момент уже работают. Можно выполнить вход на Портал администрирования и добавить дополнительные ресурсы.

1. При необходимости, добавьте сервер каталогов с помощью интерактивного сценария настройки ovirt-engine-extension-aaa-ldap-setup и добавьте дополнительных пользователей в окружение.

Статус виртуализированного ЦУ показывается в меню Cockpit **Виртуализация** → вкладка **Виртуализированный ЦУ**. На Портале администрирования ВМ диспетчера виртуализации, хост, на котором она выполняется, и домен хранилища диспетчера отмечены значками с золотой короной.

## Подключение к порталу администрирования

Получите доступ к порталу администрирования с помощью веб-браузера.

1. В веб-браузере перейдите по адресу https://*полное\_доменное\_имя\_диспетчера\_виртуализации*/ovirt-engine, где полное\_доменное\_имя\_диспетчера\_виртуализации является полным доменным именем, указанным во время установки.

ВНИМАНИЕ

Получить доступ к Порталу администрирования можно также с использованием альтернативных имён хостов или адресов IP. Для этого нужно добавить и настроить файл конфигурации в каталоге /etc/ovirt-engine/engine.conf.d/. Например:

# vi /etc/ovirt-engine/engine.conf.d/99-custom-sso-setup.conf

SSO\_ALTERNATE\_ENGINE\_FQDNS="*alias1.example.com alias2.example.com*"

Список альтернативных имён хостов должен разделяться пробелами. Также можно добавить в список адрес IP диспетчера виртуализации, но использование адресов IP вместо разрешаемых в DNS имён хостов не рекомендуется.

1. Нажмите **Портал администрирования**. Будет показана страница единого входа (SSO). Единый вход даёт возможность одновременной авторизации как на портале администрирования, так и на портале виртуальных машин.
2. Введите **Имя пользователя** и **Пароль**. Если это первый вход на портал, используйте имя пользователя **admin** вместе с паролем, указанным во время установки.
3. Выберите **Домен**, на котором нужно выполнить аутентификацию. Если вход выполняется с внутренним именем пользователя **admin**, выберите **внутренний** домен.
4. Нажмите **Выполнить вход**.
5. Портал администрирования доступен на многих языках. Выбор по умолчанию делается на основе параметров локали используемого веб-браузера. При необходимости работать с языком, отличным от языка по умолчанию, выберите нужный язык в выпадающем списке на странице приветствия.

Чтобы выполнить выход из портала администрирования системы виртуализации, нажмите на имя своего пользователя в заголовке и далее на **Выход из системы**. Будет выполнен выход из всех порталов и страницы приветствия диспетчера виртуализации .

# Установка хостов для системы виртуализации

Система виртуализации поддерживает два типа хостов: хосты системы виртуализации и хосты под управлением Red Hat Enterprise Linux. В зависимости от окружения, может использоваться либо какой-то один тип, либо оба. Для таких возможностей, как миграция и высокая доступность требуется как минимум два хоста.

Сведения о сети смотрите в разделе 6.3 «Рекомендации для настройки сетей хостов».

ВАЖНО

После установки SELinux находится в принудительном режиме. Чтобы это проверить, выполните команду getenforce. Для поддержки окружения виртуализации, SELinux должен иметь принудительный режим на всех хостах и диспетчерах виртуализации.

**Таблица 6.1. Типы хостов**

|  |  |  |
| --- | --- | --- |
| **Тип хоста** | **Другие названия** | **Описание** |
| Хост системы виртуализации Red Hat | Тонкий хост | Минимальная ОС на основе Red Hat Enterprise Linux. Она распространяется в виде файла образа ISO и содержит только пакеты, нужные для того, чтобы машина выполняла роль хоста. |
| Хост Red Hat Enterprise Linux | Толстый хост | Системы Red Hat Enterprise Linux с подключёнными репозиториями могут использоваться в виде хостов. |

**Совместимость хостов**

При создании нового дата-центра можно указать версию совместимости. Выберите версию совместимости, подходящую ко всем хостам в дата-центре. После установки, возврат к ранним версиям будет уже невозможен. Для новой установки системы виртуализации для дата-центра по умолчанию и для хоста по умолчанию настроена самая свежие версия совместимости; для использования более ранней версии совместимости необходимо создать дополнительные дата-центры и кластеры.

## Хосты виртуализации

### Установка хостов виртуализации

Хост виртуализации — это минимальная ОС на базе Red Hat Enterprise Linux, созданная для предоставляения простого способа настройка физической машины как гипервоизора в окружении виртуализации. Эта минимальная ОС содержит только пакеты, требуемые для функционала гипервизора, и представляет веб-интерфейс Cockpit для наблюдений за хостом и выполнения задач админитсрирования.

В целях повышения контроля безопасности, хосты виртуализации поддерживают разбиение на разделы по стандарту NIST 800-53, эта схема разделов применяется по умолчанию.

Хост должен соответствовать минимальным требованиям для хоста.

<https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/planning_and_prerequisites_guide/rhv_requirements#host-requirements>

**Последовательность действий**

1. Загрузите образ RHVH ISO:
   1. Выполните вход на портал <https://access.redhat.com>.
   2. Нажмите **Загрузки** на панели меню.
   3. Нажмите **Виртуализация**. Прокрутите вверх и нажмите Загрузить последние версии, чтобы получить доступ к странице загрузке продуктов.
   4. Перейдите к ссылке **Образ гипервизора для** и нажмите **Скачать**.
   5. Создайте загрузочный носитель.
2. Загрузите машину, на которую будет установлен хост виртуализации, с подготовленного загрузочного носителя.
3. В меню загрузки выберите **Установить** **RHVH 4.3** и нажмите Ввод.

ВНИМАНИЕ

Для доступа к редактированию параметров ядра можно также нажать Tab. Параметры ядра должны разделяться пробелом, а загрузить ядро с указанными параметрами можно нажатием клавиши Ввод. Для очистки любых внесённых изменений нажмите клавишу Esc и возвращайтесь в меню загрузки.

1. Выберите язык, затем нажмите **Продолжить**.
2. На экране **Дата и время** выберите часовой пояс и нажмите **Готово**.
3. На экране **Клавиатура** выберите раскладку и нажмите **Готово**.
4. На экране **Целевое устройство установки** выберите устройство, на которое нужно установить хост. По желанию включите шифрование. Нажмите **Готово**.

ВАЖНО

Мы настоятельно рекомендуем использовать параметр «Настроить разделы автоматически».

1. На экране **Сеть и имя хоста** выберите сеть и нажмите **Настроить…**, чтобы настроить параметры соединения.

ВНИМАНИЕ

Чтобы использовать это соединение каждый раз при загрузке системы, отметьте галочкой параметр «Автоматически подключаться к этой сети, когда она доступна».

В поле **Имя хоста** укажите имя хоста и нажмите **Готово**.

1. При необходимости, настройте **Языковую поддержку**, **Политику безопасности** и **Kdump**.
2. Нажмите **Начать установку**.
3. Пока устанавливается хост, настройте пароль root и, по желанию, создайте дополнительного пользователя.

ПРЕДУПРЕЖДЕНИЕ

Мы настоятельно рекомендуем не создавать недоверенных пользователей на хосте виртуализации, поскольку это может привести к эксплуатации местных уязвимостей защиты.

1. Нажмите **Перезагрузить** для завершения установки.

ВНИМАНИЕ

При перезагрузке виртуального хоста служба nodectl check выполняет проверку работоспособности хоста и выводит результат при авторизации пользователя в консоли. Сообщение node status: OK или node status: DEGRADED сообщает о результате проверки. Для получения подробностей выполните nodectl check. Эта служба включена по умолчанию.

### Продвинутая установка

#### Ручное разбиение на разделы

Ручное разбиение на разделы на хосте виртуализации не рекомендуется. Мы настоятельно советуем использовать параметр **Настроить разделы автоматически** в окне **Целевое устройство установки**.

Если же для конкретной установки требуется ручное разбиение на разделы, выберите параметр **Настроить разбиение на разделы самостоятельно**, и учитывайте следующие требования:

* Убедитесь в том, что в окне **Ручное разбиение на разделы** выбран параметр **Тонкое резервирование LVM**.
* The following directories are required and must be on thin provisioned logical volumes Логические тома с тонким резервированием обязательно должны содержать следующие каталоги:
  + root (/)
  + /home
  + /tmp
  + /var
  + /var/crash
  + /var/log
  + /var/log/audit

ВАЖНО

Не создавайте отдельный раздел для каталога /usr. В противном случае установка не будет выполнена.

/usr должен располагаться на логическом томе, который может изменять версии параллельно с хостами виртуализации, и поэтому должен оставаться в корне (/).

Сведения о требуемых размерах хранилищ смотрите в разделе «Требования к хранилищам»

* Каталог /boot должен быть определён как стандартный раздел.
* Каталог /var должен располагаться на отдельном томе или диске.
* Поддерживаются только файловые системы XFS или Ext4.

**Настройка ручной разбивки на разделы в файле Kickstart**

В следующем примере показывается, как настроить ручное разбиение на разделы в файле Kickstart.

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

ВНИМАНИЕ

При использовании logvol --thinpool –grow также необходимо включать volgroup --reserved-space или volgroup --reserved-percent , для резервирования места в группе томов под будущее увеличение тонкого пула.

#### Автоматизация развёртывания хостов виртуализации

Существует возможность установить хост виртуализации без физического загрузочного носителя, используя сетевую загрузку с сервера PXE и файл Kickstart, в котором содержатся ответы на вопросы установки.

Общие указания для установки с сервера PXE с помощью файла Kickstart доступны в руководстве по установке Red Hat Ent Linux, поскольку хосты виртуализации устанавливаются почти также, как и ОС Red Hat Enterprise Linux. Указания, имеющие отношения непосредственно к развёртыванию хостов виртуализации с использованием Red Hat Satellite, приводятся ниже.

Автоматическое развёртывание хоста виртуализации состоит из трёх фаз:

* Раздел 6.1.2.2.1, «Подготовка среды установка»
* Раздел 6.1.2.2.2, «Настройка сервера PXE и загрузчика»
* Раздел 6.1.2.2.3, «Создание и запуск файла Kickstart»

##### Подготовка среды установка

1. Выполните вход на портал https://access.redhat.com/.
2. Нажмите **Downloads** на панели меню.
3. Нажмите **Red Hat Virtualization**. Нажмите **Download Latest** в верхней части страницы чтобы получить доступ к странице загрузок.
4. Найдите **Hypervisor Image for RHV 4.3** и нажмите **Download Now**.
5. Сделайте образ RHVH ISO доступным по сети.
6. Извлеките файл образа гипервизора **squashfs.img** из образа RHVH ISO:

# 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

ВНИМАНИЕ

Файл **squashfs.img**, расположенный в каталоге /tmp/usr/share/redhat-virtualization-host/image/ , называется **redhat-virtualization-host-**номер\_версии**\_version.squashfs.img**. Не путайте его с файлом **/LiveOS/squashfs.img** , используемым с параметром inst.stage2 в установщике Anaconda.

##### Настройка сервера PXE и загрузчика

1. Настройте сервер PXE (обратитесь к разделу сетевой установки общего руководства по установке RHEL).
2. Скопируйте загрузочный образ хоста виртуализации в каталог/tftpboot:

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

1. Создайте метку rhvh в конфигурации загрузчика, указывающую на загрузочные образы хоста виртуализации:

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

##### Создание и запуск файла Kickstart

1. Создайте файл Kickstart и сделайте его доступным в сети.
2. Убедитесь в том, что файл Kickstart соответствует следующим требованиям для хостов виртуализации:
   * Хостам виртуализации не требуется раздел %packages. Вместо него используйте параметр liveimg и укажите файл **redhat-virtualization-host-номер\_версии\_version.squashfs.img** из образа хоста:

liveimg --url=example.com/tmp/usr/share/redhat-virtualization-host/image/redhat-virtualization-host-номер\_версии\_version.squashfs.img

* + Крайне рекомендуется автоматическое создание разделов:

autopart --type=thinp

ВНИМАНИЕ

Тонкое резервирование должно использоваться с автоматическим созданием разделов.

Параметр --no-home не имеет никакого эффекта для хостов виртуализации, так как /home — обязательный каталог.

Если установка требует ручной разбивки на разделы, обратитесь к разделу «6.1.2.1 Ручное разбиение на разделы», содержащему список ограничений, применяемых при создании разделов, и пример ручного разбиения в файле Kickstart.

* + Необходим раздел %post, вызывающий команду nodectl init:

%post

nodectl init

%end

**Пример Kickstart для самостоятельного развёртывания хоста виртуализации**

Данный пример Kickstart демонстрирует развёртывание хоста виртуализации. При необходимости, администраторы могут добавлять сюда команды и параметры.

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

1. Добавьте местоположение файла Kickstart в файл конфигурации загрузчика на сервере PXE:

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

1. Установите хост виртуализации, следуя общим инструкциям по сетевой установке с использованием PXE.

## Хосты Red Hat Enterprise Linux

### Установка хостов Red Hat Enterprise Linux

A Red Hat Enterprise Linux host is based on a standard basic installation of Red Hat Enterprise Linux 7 on a physical server, with the Red Hat Enterprise Linux Server and Red Hat Virtualization subscriptions attached.

Хост Red Hat Enterprise Linux базируется на станлатной установке ОС Red Hat Enterprise Linux 7 на физическом сервере.

Хост должен соответствовать минимальным требованиям.

<https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/planning_and_prerequisites_guide/rhv_requirements#host-requirements>

ВАЖНО

В параметрах BIOS хоста должна быть включена поддержка виртуализации. Сведения об изменении параметров BIOS хоста ищите в документации к используемому аппаратному обеспечению.

ВАЖНО

На хостах Red Hat Enterprise Linux не должны устанавливаться сторонние модули наблюдения за безопасностью, так как они могут помешать работе демона модуля наблюдения, предоставляемого VDSM.

### Установка Cockpit на хостах Red Hat Enterprise Linux

Для наблюдения за ресурсами хоста и выполнения задач администрирования можно установить программу Cockpit.

**Последовательность действий**

1. Установите пакеты панели наблюдения:

# yum install cockpit-ovirt-dashboard

1. Активируйте и запустите службу cockpit.socket:

# systemctl enable cockpit.socket

# systemctl start cockpit.socket

1. Проверьте, является ли Cockpit активной службой в межсетевом экране:

# firewall-cmd --list-services

В списке должен присутствовать элемент cockpit. Если он отсутствует, выполните следующую команду с правами root для добавления cockpit в качестве службы в межсетевой экран:

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

Параметр --permanent поддерживает активность службы cockpit после перезагрузки.

Получить доступ к веб-интерфейсу Cockpit можно по адресу https://*полное\_доменное\_имя\_хоста\_или\_IP*:9090.

## Практические рекомендации по настройке сетей хостов

Перед добавлением хоста в виртуализированный ЦУ в сложном сетевом окружении может понадобиться ручная настройка сети хоста.

Мы предлагаем следующие практические рекомендации по настройке параметров сети хоста:

* Настройте сеть с помощью Cockpit. Как вариант, можно использовать nmtui or nmcli.
* Если для развёртывания виртуализированного ЦУ или для добавления в ЦУ хоста сеть не требуется, то настройте сеть на портале администрирования после добавления хоста в ЦУ.
* Используйте следующие соглашения об именованиях:
  + Устройства VLAN: VLAN\_ИМЯ\_ТИП\_RAW\_PLUS\_VID\_NO\_PAD
  + Интерфейсы VLAN: физическое\_устройство.VLAN\_ID (например, eth0.23, eth1.128, enp3s0.50)
  + Интерфейсы связок: bondномер (например, bond0, bond1)
  + VLAN на интерфейсах связок: bondномер.VLAN\_ID (например, bond0.50, bond1.128)
* Используйте сетевые связки (bonding). В системе виртуализации не поддерживается объединение сетей teaming, и его использование может привести к ошибкам, если хост используется для развёртывания виртуализированного ЦУ или добавлен в ЦУ.
* Используйте рекомендованные режимы связок::
  + Если сеть ovirtmgmt не используется виртуальными машинами, то в сети может использоваться любой поддерживаемый режим связок.
  + If the ovirtmgmt network is used by virtual machines, see [Which bonding modes work when used with a bridge that virtual machine guests or containers connect to?](https://access.redhat.com/solutions/67546).
  + В системе виртуализации по умолчанию используется 4 политика — агрегирование каналов. Если свитч не поддерживает протокол LACP, используйте политику 1 — активный-резервный.
* Настройте VLAN на физической сетевой карте так, как показано в примере ниже (здесь используется nmcli, но можно использовать любой другой инструмент):

# 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

* Настройте VLAN на связке так, как показано в примере ниже (здесь используется nmcli, но можно использовать любой другой инструмент):

# 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

* Не выключайте firewalld.
* После добавления хоста в виртуализированный ЦУ, настройте правила межсетевого экрана.

ВАЖНО

При создании моста администрирования, использующего статический адрес IPv6, перед добавлением хоста отключите контроль network manager в конфигурации его интерфейса (ifcfg).

See <https://access.redhat.com/solutions/3981311> for more information.

## Добавление узлов виртуализированного ЦУ к диспетчеру виртуализации

Self-hosted engine nodes are added in the same way as a standard host, with an additional step to deploy the host as a self-hosted engine node. The shared storage domain is automatically detected and the node can be used as a failover host to host the Manager virtual machine when required. You can also attach standard hosts to a self-hosted engine environment, but they cannot host the Manager virtual machine. Red Hat recommends having at least two self-hosted engine nodes to ensure the Manager virtual machine is highly available. Additional hosts can also be added using the REST API. See [Hosts](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/rest_api_guide/services#services-hosts) in the REST API Guide.

**Prerequisites**

* If you are reusing a self-hosted engine node, remove its existing self-hosted engine configuration. See [Removing a Host from a Self-Hosted Engine Environment](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/administration_guide/removing_a_host_from_a_self-hosted_engine_environment).

Important

When creating a management bridge that uses a static IPv6 address, disable network manager control in its interface configuration (ifcfg) file before adding a host. See <https://access.redhat.com/solutions/3981311> for more information.

**Procedure**

1. In the Administration Portal, click Compute → Hosts.
2. Click New.

For information on additional host settings, see [Explanation of Settings and Controls in the New Host and Edit Host Windows](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/administration_guide#sect-Explanation_of_Settings_and_Controls_in_the_New_Host_and_Edit_Host_Windows) in the Administration Guide.

1. Use the drop-down list to select the **Data Center** and **Host Cluster** for the new host.
2. Enter the **Name** and the **Address** of the new host. The standard SSH port, port 22, is auto-filled in the **SSH Port** field.
3. Select an authentication method to use for the Manager to access the host.
   * Enter the root user’s password to use password authentication.
   * Alternatively, copy the key displayed in the **SSH PublicKey** field to **/root/.ssh/authorized\_keys** on the host to use public key authentication.
4. Optionally, configure power management, where the host has a supported power management card. For information on power management configuration, see [Host Power Management Settings Explained](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/administration_guide#Host_Power_Management_settings_explained) in the Administration Guide.
5. Click the **Hosted Engine** tab.
6. Select **Deploy**.
7. Click OK.

## 6.5. Adding Standard Hosts to the Red Hat Virtualization Manager

Adding a host to your Red Hat Virtualization environment can take some time, as the following steps are completed by the platform: virtualization checks, installation of packages, and creation of a bridge.

Important

When creating a management bridge that uses a static IPv6 address, disable network manager control in its interface configuration (ifcfg) file before adding a host. See <https://access.redhat.com/solutions/3981311> for more information.

**Procedure**

1. From the Administration Portal, click Compute → Hosts.
2. Click New.
3. Use the drop-down list to select the **Data Center** and **Host Cluster** for the new host.
4. Enter the **Name** and the **Address** of the new host. The standard SSH port, port 22, is auto-filled in the **SSH Port** field.
5. Select an authentication method to use for the Manager to access the host.
   * Enter the root user’s password to use password authentication.
   * Alternatively, copy the key displayed in the **SSH PublicKey** field to **/root/.ssh/authorized\_keys** on the host to use public key authentication.
6. Optionally, click the **Advanced Parameters** button to change the following advanced host settings:
   * Disable automatic firewall configuration.
   * Add a host SSH fingerprint to increase security. You can add it manually, or fetch it automatically.
7. Optionally configure power management, where the host has a supported power management card. For information on power management configuration, see [Host Power Management Settings Explained](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/administration_guide/#Host_Power_Management_settings_explained) in the Administration Guide.
8. Click OK.

The new host displays in the list of hosts with a status of Installing, and you can view the progress of the installation in the **Events** section of the **Notification Drawer** ( ). After a brief delay the host status changes to Up.