<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 виртуализации Red Hat в качестве виртуализованного ЦУ

[1 Обзор процесса установки 6](#_Toc32932737)

[2 Требования 7](#_Toc32932738)

[2.1 Требования для работы виртуализированного ЦУ 7](#_Toc32932739)

[2.1.1 Требования к аппаратному обеспечению 7](#_Toc32932740)

[2.1.2 Требования к браузеру 8](#_Toc32932741)

[2.1.3 Требования к клиенту 9](#_Toc32932742)

[2.1.4 Требования к операционным системам 9](#_Toc32932743)

[2.2 Требования к хостам 10](#_Toc32932744)

[2.2.1 Требования к ЦП 10](#_Toc32932745)

[2.2.2 Требования к памяти 11](#_Toc32932746)

[2.2.3 Требования к хранилищу 11](#_Toc32932747)

[2.2.4 Требования к устройствам PCI 12](#_Toc32932748)

[2.2.5 Требования к выделяемым устройствам 12](#_Toc32932749)

[2.2.6 Требования к vGPU 13](#_Toc32932750)

[2.3 Требования к сетям 13](#_Toc32932751)

[2.3.1 Общие требования 13](#_Toc32932752)

[2.3.2 Требования к межсетевому экрану для DNS, NTP и операций блокады IPMI 14](#_Toc32932753)

[2.3.3 Требования к межсетевому экрану для виртуализированного ЦУ 15](#_Toc32932754)

[2.3.4 Требования к межсетевому экрану для хостов 17](#_Toc32932755)

[2.3.5 Требования к межсетевому экрану для баз данных 20](#_Toc32932756)

[3 Подготовка хранилища для системы виртуализации 22](#_Toc32932757)

[3.1 Подготовка хранилища NFS 22](#_Toc32932758)

[3.2 Подготовка хранилища iSCSI 23](#_Toc32932759)

[3.3 Подготовка хранилища FCP 24](#_Toc32932760)

[3.4 3.4. Preparing Red Hat Gluster Storage 25](#_Toc32932761)

[4 Установка хоста развёртывания виртуализированного ЦУ 25](#_Toc32932762)

[4.1 Установка хостов системы виртуализации 26](#_Toc32932763)

[4.1.1 Подключение репозиториев хоста виртуализации 27](#_Toc32932764)

[4.2 Установка хостов Red Hat Enterprise Linux 28](#_Toc32932765)

[4.2.1 Подключение репозиториев хостов Red Hat Enterprise Linux 28](#_Toc32932766)

[4.2.2 Установка Cockpit на хостах Red Hat Enterprise 29](#_Toc32932767)

[5 Установка диспетчера виртуализации 30](#_Toc32932768)

[5.1 Развёртывание виртуализированного ЦУ с помощью Cockpit 30](#_Toc32932769)

[5.2 Подключение к порталу администрирования 33](#_Toc32932770)

[6 Установка хостов для системы виртуализации 34](#_Toc32932771)

[6.1 Хосты виртуализации 35](#_Toc32932772)

[6.1.1 Установка хостов виртуализации 35](#_Toc32932773)

[6.1.2 Продвинутая установка 37](#_Toc32932774)

[6.2 Хосты Red Hat Enterprise Linux 41](#_Toc32932775)

[6.2.1 Установка хостов Red Hat Enterprise Linux 41](#_Toc32932776)

[6.2.2 Установка Cockpit на хостах Red Hat Enterprise Linux 42](#_Toc32932777)

[6.3 Практические рекомендации по настройке сетей хостов 42](#_Toc32932778)

[6.4 Добавление узлов виртуализированного ЦУ к диспетчеру виртуализации 44](#_Toc32932779)

[6.5 Добавление в виртуализированный ЦУ стандартных хостов. 45](#_Toc32932780)

[7 Добавление хранилищ в среду виртуализации 46](#_Toc32932781)

[7.1 Добавление хранилища NFS 47](#_Toc32932782)

[7.2 Добавление хранилища iSCSI 48](#_Toc32932783)

[7.3 Добавление хранилища FCP 50](#_Toc32932784)

[7.4 Добавление хранилища Gluster 51](#_Toc32932785)

[A. Нахождение и исправление проблем развёртывания виртуализированного ЦУ 52](#_Toc32932786)

[A.1 Нахождение и исправление проблем виртуальной машины с виртуализированным ЦУ 52](#_Toc32932787)

[A.2 Очистка после неудачного развёртывания виртуализированного ЦУ 55](#_Toc32932788)

[B. Перенос баз данных и служб на удалённый сервер 57](#_Toc32932789)

[B.1 Перенос базы данных виртуализированного ЦУ на удалённый сервер 57](#_Toc32932790)

[B.1.1 Процедура миграции базы данных виртуализированного ЦУ на удалённый сервер 57](#_Toc32932794)

[B.2 Перенос хранилища данных на отдельную машину 58](#_Toc32932798)

[7.4.1 B.2.1. Migrating the Data Warehouse Database to a Separate Machine 58](#_Toc32932799)

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 |

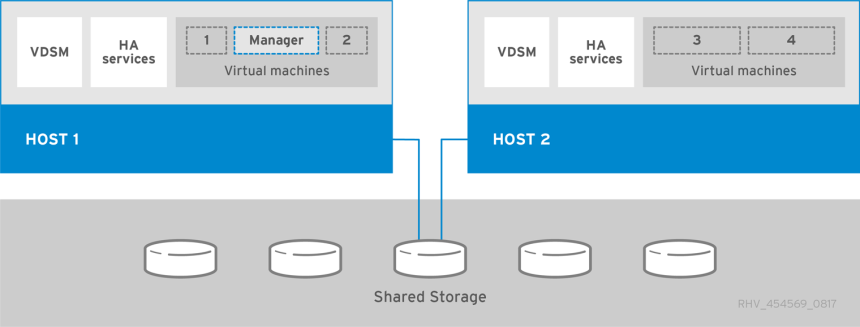
**Архитектура виртуализованного ЦУ**

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
   * Протокол оптоволоконного канала (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 для 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.

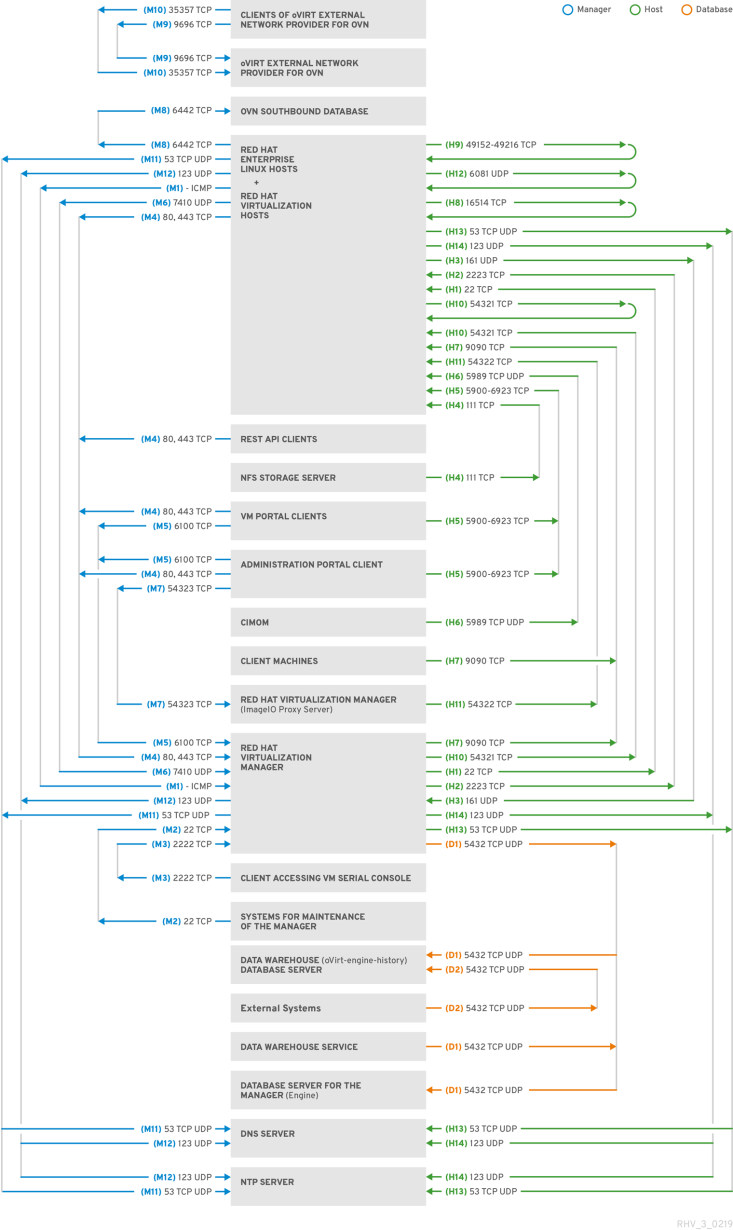
По умолчанию, в Red Hat Enterprise Linux разрешён исходящий трафик на DNS и NTP по любому адресу назначения. При запрете исходящего трафика сделайте исключения, чтобы диспетчер виртуализации мог посылать запросы на серверы DNS и NTP. Другим узлам тоже может понадобиться DNS и NTP, и в этих случаях получите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

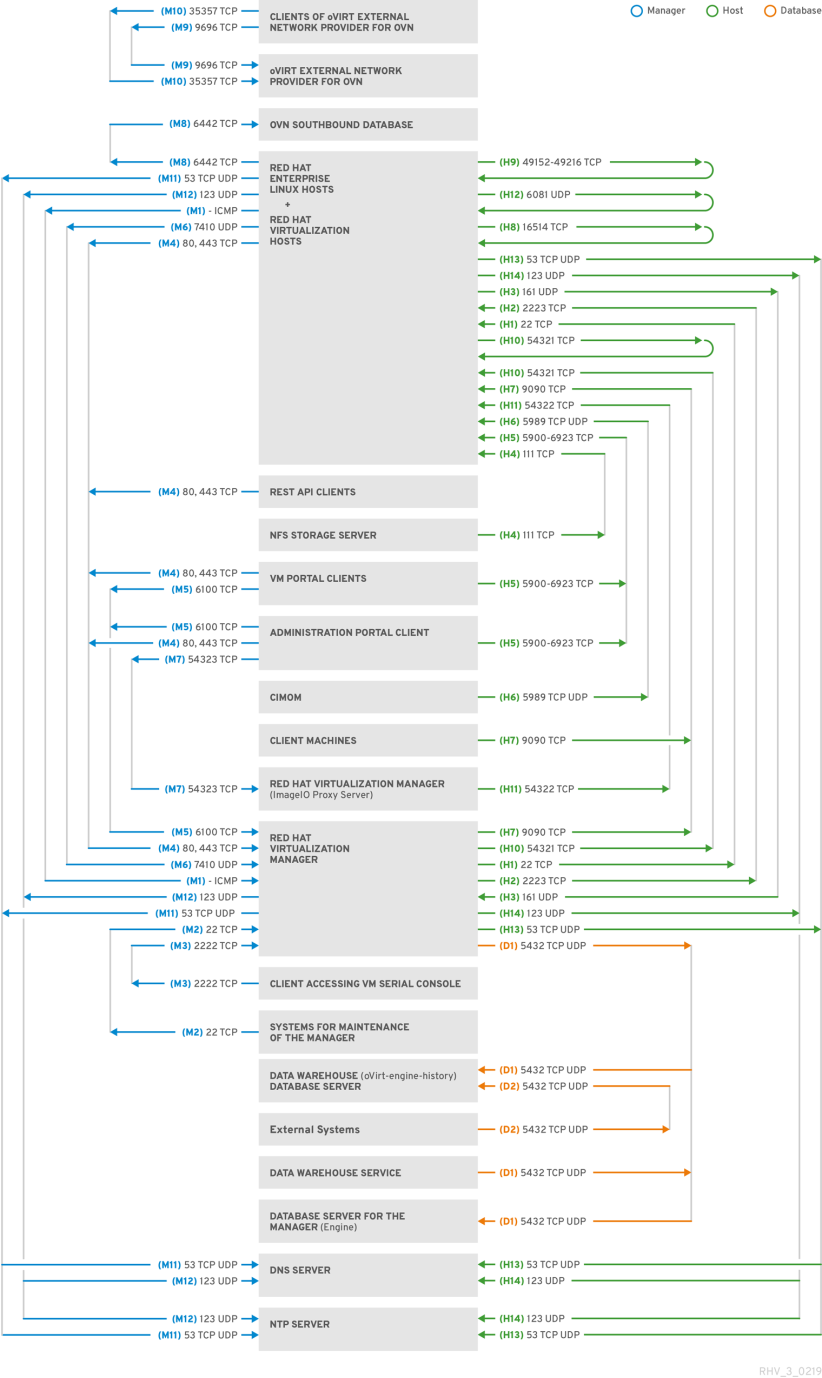
Система виртуализации Red Hat Virtualization поддерживает использование удалённого сервера баз данных с базой данных диспетчера виртуализации (engine) и базой данных хранилища данных (ovirt-engine-history). Если планируется использовать удалённый сервер баз данных, то он должен разрешать подключения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

### 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

Хост Red Hat Enterprise Linux базируется на стандартной 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.
* Придерживайтесь следующих соглашений 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 отключайте 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

Узлы виртуализированного ЦУ добавляются тем же самым способом, что и стандартные хосты, с дополнительным шагом в виде развёртывания хоста как узла виртуализированного ЦУ. Разделяемый домен хранилища определяется автоматически, и затем, при необходимости, узел может быть использован в виде отказоустойчивого хоста для размещения ВМ диспетчера виртуализации. К окружению виртуализированного ЦУ также можно присоединить и стандартные хосты, но на них нельзя будет разместить ВМ диспетчера. Мы рекомендуем иметь как минимум два узла виртуализированного ЦУ для обеспечения высокой доступности ВМ диспетчера виртуализации. Дополнительные хосты можно также добавлять с помощью REST API: <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/rest_api_guide/services#services-hosts>

**Предварительные условия и предпосылки**

* При использовании узла виртуализированного ЦУ, удалите существующую конфигурацию его виртуализированного ЦУ. <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/administration_guide/removing_a_host_from_a_self-hosted_engine_environment>

ВАЖНО

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

**Последовательность действий**

1. На портале администрирования нажмите **Вычисления → Хосты**
2. Нажмите **Добавить**.

Сведения о дополнительных параметрах хоста смотрите в Руководстве по администрированию: <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/administration_guide/index#sect-Explanation_of_Settings_and_Controls_in_the_New_Host_and_Edit_Host_Windows>

1. В выпадающем списке выберите **Дата-центр** и **Кластер хоста** для нового хоста.
2. Укажите **Имя** и **Адрес** нового хоста. В поле **Порт SSH** автоматически указывается стандартный порт SSH, 22.
3. Выберите способ аутентификации, используемый диспетчером виртуализации при доступе к хосту.
   * Для использования аутентификации по паролю укажите пароль root.
   * Или же скопируйте ключ, показываемый в поле Открытый ключ SSH в файл **/root/.ssh/authorized\_keys** на хосте, чтобы использовать аутентификацию по открытому ключу.
4. При необходимости и при наличии у хоста поддерживаемой платы управления питанием, настройте управление питанием. Сведения о параметрах управления питанием: <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/administration_guide#Host_Power_Management_settings_explained>
5. Перейдите на вкладку **Виртуализированный ЦУ**.
6. Выберите **Установить**.
7. Нажмите **OK**.

## Добавление в виртуализированный ЦУ стандартных хостов.

Процесс добавления хоста в среду виртуализации может занять некоторое время, о мере выполнения платформой следующих шагов: проверки виртуализации, установка пакетов и создание моста.

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.

**Последовательность действий**

1. На портале администрирования нажмите **Вычисления →Хосты**.
2. Нажмите **Добавить**.
3. В выпадающем списке выберите **Дата-центр** и **Кластер хоста**.
4. Укажите **Имя** и **Адрес** нового хоста. В поле **Порт SSH** автоматически указывается стандартный порт SSH, 22.
5. Выберите способ аутентификации, используемый диспетчером виртуализации при доступе к хосту.
   * Для использования аутентификации по паролю укажите пароль root.
   * Или же скопируйте ключ, показываемый в поле Открытый ключ SSH в файл **/root/.ssh/authorized\_keys** на хосте, чтобы использовать аутентификацию по открытому ключу.
6. При необходимости, нажмите на кнопку **Дополнительные параметры** для изменения следующих дополнительных параметров хоста:
   * Отключите автоматическую конфигурацию межсетевого экрана
   * Для повышения безопасности добавьте метод идентификации SSH хоста. Его можно добавить вручную или получить автоматически.
7. При необходимости и при наличии у хоста поддерживаемой платы управления питанием, настройте управление питанием. Сведения о параметрах управления питанием: <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/administration_guide#Host_Power_Management_settings_explained>
8. Нажмите **OK**.

Новый хост будет показан в списке хостов со статусом Устанавливается, а прогресс установки можно наблюдать в разделе **События** секции уведомлений (). После короткой задержки статус хоста сменится на Запущен.

# Добавление хранилищ в среду виртуализации

Добавление хранилищ в качестве доменов данных в новое окружение. В среде виртуализации Red Hat должен присутствовать как минимум один домен данных, но рекомендуется добавить больше.

Добавление ранее подготовленного хранилища:

* NFS
* iSCSI
* Протокол оптоволоконного канала (FCP)
* Хранилище Gluster

ВАЖНО

При использовании хранилища iSCSI, новые домены данных не должны использовать ту же самую цель iSCSI, что и домен хранилища виртуализированного ЦУ.

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 не будет возможности добавить новые домены или удалить повреждённый; придётся разворачивать новый виртуализированный ЦУ.

## Добавление хранилища NFS

В данной инструкции рассказывается, как можно включить существующее хранилище NFS в окружение виртуализации в качестве домена данных.

При необходимости включить домен **ISO** или домен экспорта, используйте те же шаги, но в списке **Функция домена** выберите **ISO** или **Экспорт**.

**Последовательность действий**

1. На Портале администрирования нажмите **Хранилище → Домены**.
2. Нажмите **Добавить домен**.
3. Укажите **Имя** нового домена хранилища.
4. Примите параметры по умолчанию для **Дата-центра**, **Функции домена**, **Типа хранилища**, **Формата** и списков **Доменов**.
5. Укажите **Путь экспорта**, используемый для домена хранилища. Путь экспорта должен иметь формат 123.123.0.10:/data (для IPv4), [2001:0:0:0:0:0:0:5db1]:/data (для IPv6), или domain.example.com:/data.
6. При необходимости можно настроить дополнительные параметры:
   1. **Нажмите Дополнительные параметры**.
   2. Введите процентное значение в поле **Индикатор предупреждения о недостатке места**. Если объём свободного доступного места в домене хранилищ меньше этого процентного значения, то пользователю будет показано предупреждение и будет создана запись в журнале.
   3. Укажите значение в Гбайт в поле **Блокировщик действия при критической нехватке места. Если объём доступного свободного места в домене хранилищ меньше этого значения, то** пользователю будет показано предупреждение и будет создана запись в журнале, а любое новое действие добавления (даже временное), использующее место, будет заблокировано.
   4. Отметьте галочкой пункт **Забить нулями после удаления** для включения полного стирания данных после удаления диска. Этот параметр можно изменить после создания домена, но это изменение не затронет значение данного параметра для уже существующих дисков.
7. Нажмите **OK**.

Пока диск не будет подготовлен, домен данных NFS будет иметь статус Заблокировано. Затем домен данных будет автоматически присоединён к дата-центру.

## Добавление хранилища iSCSI

В данной инструкции рассказывается, как можно включить существующее хранилище iSCSI в окружение виртуализации в качестве домена данных.

**Последовательность действий**

1. Нажмите **Хранилище → Домены**.
2. Нажмите **Добавить домен**.
3. Укажите **Имя** нового домена хранилищ.
4. В выпадающем списке выберите **Дата-центр**.
5. Для **Функции домена** укажите **Данные**, а для **Типа хранилища** укажите **iSCSI.**
6. Выберите активный хост в качестве **Хоста**.

ВАЖНО

Данные в домен хранилищ поступают из выбранного хоста, а не напрямую из диспетчера виртуализации. Поэтому, ещё до настройки домена хранилища, все хосты должны получить доступ к устройству хранения.

1. Диспетчер виртуализации может отобразить цели iSCSI на номера LUN или номера LUN на цели iSCSI. При выборе типа хранилища iSCSI в окне **Новый домен** автоматически отображаются известные цели с неиспользованными LUN. Если цель, используемая для добавления хранилища, не отображается, для её нахождения можно запустить обнаружение цели; в противном случае переходите к следующему пункту.
   1. Для включения возможностей обнаружения целей нажмите **Обнаружение целей**. После обнаружения и загрузки целей, в окне Новый домен будут автоматически отображены цели с номерами LUN, не используемыми в окружении.

ВНИМАНИЕ

Внешние для среды виртуализации номера LUN также отображаются.

Параметр *Обнаружение целей* можно использовать для добавления номеров LUN к нескольким целям, или нескольких путей к одним и тем же LUN.

* 1. В поле **Адрес** укажите полное доменное имя или адрес IP хоста iSCSI.
  2. В поле **Порт** укажите номер порта, используемого для подключения к хосту во время обнаружения целей. Значение по умолчанию — 3260.
  3. Если для защиты хранилища используется CHAP, отметьте галочкой пункт **Аутентификация пользователя**. Укажите **Имя пользователя CHAP** и **Пароль CHAP**.

ВНИМАНИЕ

С помощью REST API можно настроить учётные данные цели iSCSI для конкретного хоста.

<https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/rest_api_guide/services#services-storage_server_connection_extensions-methods-add>

* 1. Нажмите **Обнаружение**.
  2. В результатах обнаружения выберите одну или несколько целей и нажмите **Авторизоваться или, для нескольких целей, Авторизоваться на всех.**

ВАЖНО

Если требуется больше одного пути, необходимо обнаружить и авторизоваться на цели с использованием всех требуемых путей. Возможность изменения домена хранилища с целью добавления дополнительных путей на данный момент не поддерживается.

1. Нажмите на кнопку с крестиком (**+**) рядом с нужной целью. Элемент будет развёрнут, и будут показаны все неиспользуемые LUN, присоединённые к цели.
2. Отметьте галочкой каждый LUN, используемый для создания домена хранилища.
3. При необходимости можно настроить дополнительные параметры:
   1. Нажмите **Дополнительные параметры**.
   2. Введите процентное значение в поле **Индикатор предупреждения о недостатке места**. Если объём свободного доступного места в домене хранилищ меньше этого процентного значения, то пользователю будет показано предупреждение и будет создана запись в журнале.
   3. Укажите значение в Гбайт в поле **Блокировщик действия при критической нехватке места. Если объём доступного свободного места в домене хранилищ меньше этого значения, то** пользователю будет показано предупреждение и будет создана запись в журнале, а любое новое действие добавления (даже временное), использующее место, будет заблокировано.
   4. Отметьте галочкой пункт **Забить нулями после удаления** для включения полного стирания данных после удаления диска. Этот параметр можно изменить после создания домена, но это изменение не затронет значение данного параметра для уже существующих дисков.
   5. Отметьте галочкой пункт **Освободить блоки перед удалением для включения функции выполнения команды** blkdiscard на логическом томе непосредственно перед его удалением. После создания домена этот параметр можно изменить. Этот параметр доступен только для доменов блочных хранилищ.
4. Нажмите **OK**.

Если для одной и той же цели было настроено несколько путей, то для завершения настройки связки iSCSI нужно выполнить последовательность действий по настройке iSCSI с несколькими путями:

<https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/administration_guide/sect-preparing_and_adding_block_storage#Configuring_iSCSI_Multipathing>

Если необходимо выполнить миграцию текущей сети хранилища на связку iSCSI, смотрите последовательность действий Миграция логической сети на связку iSCSI:

<https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/administration_guide/sect-preparing_and_adding_block_storage#Migrating_a_logical_network_to_an_iscsi_bond>

## Добавление хранилища FCP

В данной инструкции рассказывается, как можно включить существующее хранилище FCP в окружение виртуализации в качестве домена данных.

**Последовательность действий**

1. Нажмите **Хранилище → Домены**.
2. Нажмите **Добавить домен**.
3. Укажите **Имя** нового домена хранилищ.
4. В выпадающем списке выберите **Дата-центр FCP**.

Если подходящего дата-центра FCP ещё не существует, выберите (нет).

1. В выпадающем списке выберите **Функцию домена** и **Тип хранилища**. Типы доменов хранилищ, несовместимые с выбранным дата-центром, не будут доступны.
2. Выберите активный хост в поле **Хост**. Если это не первый домен данных в дата-центре, необходимо выбрать хост-диспетчер пула хранилища (SPM).

ВАЖНО

Данные в домен хранилищ поступают из выбранного хоста, а не напрямую из диспетчера виртуализации. В системе должен существовать как минимум один активный хост, присоединённый к выбранному дата-центру. Ещё до настройки домена хранилища все хосты должны получить доступ к устройству хранения.

1. При выборе типа хранилища **Оптоволокно**, в окне **Новый домен** будут автоматически показаны известные цели с не используемыми LUN. Отметьте галочкой параметр **Идентификатор LUN** для выбора всех доступных LUN.
2. При необходимости можно настроить дополнительные параметры:
   1. Нажмите **Дополнительные параметры**.
   2. Введите процентное значение в поле **Индикатор предупреждения о недостатке места**. Если объём свободного доступного места в домене хранилищ меньше этого процентного значения, то пользователю будет показано предупреждение и будет создана запись в журнале.
   3. Укажите значение в Гбайт в поле **Блокировщик действия при критической нехватке места. Если объём доступного свободного места в домене хранилищ меньше этого значения, то** пользователю будет показано предупреждение и будет создана запись в журнале, а любое новое действие добавления (даже временное), использующее место, будет заблокировано.
   4. Отметьте галочкой пункт **Забить нулями после удаления** для включения полного стирания данных после удаления диска. Этот параметр можно изменить после создания домена, но это изменение не затронет значение данного параметра для уже существующих дисков.
   5. Отметьте галочкой пункт **Освободить блоки перед удалением для включения функции выполнения команды** blkdiscard на логическом томе непосредственно перед его удалением. После создания домена этот параметр можно изменить. Этот параметр доступен только для доменов блочных хранилищ.
3. Нажмите **OK**.

Во время подготовки к использованию статус нового домена FCP будет показан как Заблокировано. Как только домен будет готов, он автоматически будет присоединён к дата-центру.

## Добавление хранилища Gluster

Информацию об использовании хранилищ Gluster со средой виртуализации ищите в документации.

<https://access.redhat.com/documentation/en-us/red_hat_gluster_storage/3.4/html/configuring_red_hat_virtualization_with_red_hat_gluster_storage/index>

Версии Gluster, поддерживаемые системой виртуализации Red Hat:

<https://access.redhat.com/articles/2356261>.

# Нахождение и исправление проблем развёртывания виртуализированного ЦУ

Чтобы проверить, был ли установлен виртуализированный ЦУ, выполните команду hosted-engine --check-deployed. Ошибка выводится только в случае, если виртуализированный ЦУ не был установлен.

## Нахождение и исправление проблем виртуальной машины с виртуализированным ЦУ

Чтобы проверить статус виртуальной машины виртуализированного ЦУ, выполните hosted-engine --vm-status.

ВНИМАНИЕ

Все изменения, вносимые в параметры ВМ виртуализированного ЦУ, отображаются в выводе команды состояния с задержкой примерно в 20 секунд.

В зависимости от содержимого записи Engine status в выводе, ниже ищите информацию о нахождении или исправлении ошибки.

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

1. Если ВМ диспетчера виртуализации запущена и работает без отклонений от нормы, вывод будет следующим:

--== Host 1 status ==--

Status up-to-date : True

Hostname : hypervisor.example.com

Host ID : 1

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

Score : 3400

stopped : False

Local maintenance : False

crc32 : 99e57eba

Host timestamp : 248542

1. Если вывод не отличается от нормы, но к диспетчеру виртуализации невозможно подключиться, проверьте сетевое подключение.

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

1. Если health имеет значение bad, а vm имеет значение up, то службы высокой доступности попробуют перезапустить ВМ диспетчера виртуализации, чтобы возобновить работу диспетчера. Если в течение нескольких минут этого добиться не удалось, активируйте в консоли режим глобального обслуживания, чтобы хосты больше не управлялись службами высокой доступности.

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

1. Подключитесь к консоли. Получив приглашение командной строки, введите пароль root операционной системы. Дополнительные параметры консоли смотрите по ссылке <https://access.redhat.com/solutions/2221461>

# hosted-engine --console

1. Авторизуйтесь в ОС виртуальной машины диспетчера виртуализации, чтобы убедиться в том, что эта ОС работает.
2. Проверьте статус службы ovirt-engine:

# systemctl status -l ovirt-engine

# journalctl -u ovirt-engine

1. Просмотрите следующие файлы журналов: **/var/log/messages**, **/var/log/ovirt-engine/engine.log** и **/var/log/ovirt-engine/server.log**.
2. Исправив проблему, вручную перезагрузите ВМ диспетчера виртуализации с одного из узлов виртуализированного ЦУ:

# hosted-engine --vm-shutdown

# hosted-engine --vm-start

ВНИМАНИЕ

Когда узлы виртуализированного ЦУ находятся в глобальном режиме обслуживания, виртуальную машину виртуализированного ЦУ необходимо перезапускать вручную. При попытке перезагрузки ВМ с помощью консольной команды *reboot*, виртуальная машина диспетчера виртуализации останется в отключённом состоянии. Такое поведение запланировано специально.

1. Убедитесь в том, что служба ovirt-engine на виртуальной машине диспетчера виртуализации активна и выполняется:

# systemctl status ovirt-engine.service

1. Убедившись в том, что ВМ диспетчера виртуализации включена и работает, закройте сеанс консоли и отключите режим обслуживания, чтобы снова включить работу служб высокой доступности:

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

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

1. Если в окружении больше одного хоста, убедитесь в том, что ни один другой хост не пытается перезапустить ВМ диспетчера виртуализации в данную минуту.
2. Убедитесь, что режим глобального обслуживания отключён.
3. Просмотрите файл журналов **ovirt-ha-agent** в **/var/log/ovirt-hosted-engine-ha/agent.log**.
4. Попробуйте вручную перезапустить ВМ диспетчера виртуализации с одного из узлов виртуализированного ЦУ:

# hosted-engine --vm-shutdown

# hosted-engine --vm-start

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

Это означает, что ovirt-ha-agent не смог получить сведения о ВМ от службы VDSM.

1. Просмотрите файл журнала VDSM в **/var/log/vdsm/vdsm.log**.
2. Просмотрите файл журнала **ovirt-ha-agent** в **/var/log/ovirt-hosted-engine-ha/agent.log**.

**Engine status: The self-hosted engine’s configuration has not been retrieved from shared storage**

Если был получен статус The hosted engine configuration has not been retrieved from shared storage. Please ensure that ovirt-ha-agent is running and the storage server is reachable, то это означает проблемы либо со службой ovirt-ha-agent, либо с хранилищем, либо с ними обоими.

1. Проверьте статус ovirt-ha-agent на хосте:

# systemctl status -l ovirt-ha-agent

# journalctl -u ovirt-ha-agent

1. Если ovirt-ha-agent не запущена, запустите её:

# systemctl start ovirt-ha-agent

1. Просмотрите файл журнала ovirt-ha-agent в **/var/log/ovirt-hosted-engine-ha/agent.log**.
2. Проверьте доступность разделяемого хранилища с помощью команды ping.
3. Убедитесь, что разделяемое хранилище смонтировано.

**Дополнительные команды для нахождения и решения проблем**

ВАЖНО

Свяжитесь со службой поддержки, если вы считаете, что вам необходимо выполнить одну из этих команд для нахождения проблем в окружении виртуализированного ЦУ.

* hosted-engine --reinitialize-lockspace: эта команда используется при неправильной работе зарезервированного пространства sanlock. Перед повторной инициализацией зарезервированных пространств sanlock убедитесь в том, что режим глобального облуживания был запущен, и что ВМ диспетчера виртуализации была остановлена.
* hosted-engine --clean-metadata: удаление метаданных агента хоста из глобальной базы данных состояний, после чего все остальные хосты забудут об этом хосте. Убедитесь в том, что целевой хост не работает, и что был активирован глобальный режим обслуживания.
* hosted-engine --check-liveliness: эта команда проверяет страницу liveliness службы ovirt-engine. Также эту проверку можно выполнить, зайдя на страницу https://полное\_доменное\_имя\_диспетчера/ovirt-engine/services/health/в веб-браузере.
* hosted-engine --connect-storage: по этой команде VDSM подготавливает все подключения хранилища, необходимые для хоста и ВМ диспетчера виртуализации. Как правило, эта команда выполняется на серверной части во время развёртывания диспетчера виртуализации. Если эта команда нужна для диагностики проблем с хранилищем, убедитесь в том, что перед её запуском был включён глобальный режим обслуживания.

## Очистка после неудачного развёртывания виртуализированного ЦУ

В случае, если установка виртуализированного ЦУ была прервана, все последующие развёртывания закончатся неудачно с сообщением об ошибке. Эта ошибка меняется в зависимости от стадии, на которой произошёл сбой развёртывания.

В случае получения сообщения об ошибке, можно запустить сценарий очистки на хосте развёртывания, чтобы очистить остатки от неудачного развёртывания. Тем не менее, лучшим выбором будет переустановить базовую ОС и начать развёртывание сначала.

ВНИМАНИЕ

У сценария очистки имеются следующие ограничения:

Обрыв сетевого соединения во время выполнения сценария может привести к тому, что сценарий не сможет удалить мост администрирования или воссоздать рабочую сетевую конфигурацию

Сценарий не рассчитан на очистку устройств разделяемых хранилищ, использованных во время неудачной попытки развёртывания. Устройство разделяемого хранилища необходимо очистить заранее, до того, как оно будет повторно использовано в последующем развёртывании.

**Последовательность действий**

1. Запустите /usr/sbin/ovirt-hosted-engine-cleanup и выберите y, чтобы очистить любые оставшиеся следы предудыщей сбойной установки виртуализированного ЦУ.

# /usr/sbin/ovirt-hosted-engine-cleanup

This will de-configure the host to run ovirt-hosted-engine-setup from scratch.

Caution, this operation should be used with care.

Are you sure you want to proceed? [y/n]

1. Укажите, нужно ли устанавливать на то же устройство разделяемого хранилища, или нужно выбрать другое устройство разделяемого хранилища.
   * Чтобы развернуть установку в том же домене хранилища, очистите домен, выполнив следующую команду в соответствующем каталоге на сервере, для доменов хранилища NFS, Gluster, PosixFS или локальных:

# rm -rf местоположение\_хранилища/\*

* + В случае хранилищ iSCSI или протокола FCP обратитесь к документу <https://access.redhat.com/solutions/2121581> , чтобы получить сведения о том, как очистить хранилище.
  + Или выберите другой тип хранилища.

1. Выполните повторное развёртывание виртуализированного ЦУ.

# Перенос баз данных и служб на удалённый сервер

Хотя во время автоматизированной установки нельяз настраивать службы и базы данных, после установки их можно перенести на удалённый сервер.

## Перенос базы данных виртуализированного ЦУ на удалённый сервер

You can migrate the engine database of a self-hosted engine to a remote database server after the Red Hat Virtualization Manager has been initially configured. Use engine-backup to create a database backup and restore it on the new database server.

После начальной конфигурации диспетчера виртуализации, базу данных engine виртуализированного ЦУ можно перенести на удалённый сервер баз данных. Для создания резервной копии базы данных и восстановления её на новом сервере баз данных используйте команду engine-backup.

На новом сервере базы данных должна быть установлена ОС Red Hat Enterprise Linux 7 с подключёнными репозиториями.



### Процедура миграции базы данных виртуализированного ЦУ на удалённый сервер

1. Авторизуйтесь на узле виртуализированного ЦУ и переведите среду в глобальный режим обслуживания. Это действие отключает агентов высокой доступности и предотвращает миграцию ВМ виртуализированного ЦУ во время миграции БД:

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

1. Авторизуйтесь на машине виртуализированного ЦУ и остановите службу ovirt-engine, чтобы её работа не пересекалась с созданием резервной копии виртуализированного ЦУ:

# systemctl stop ovirt-engine.service

1. Создайте резервную копию базы данных engine:

# engine-backup --scope=files --scope=db --mode=backup --file=имя\_файла --log=имя\_журнала\_резервной\_копии

1. Скопируйте файл с резервной копией на новый сервер баз данных:

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

1. Авторизуйтесь на новом сервере баз данных и установите engine-backup:

# yum install ovirt-engine-tools-backup

1. Восстановите базу данных из резервной копии на новом сервере базы данных. имя\_файла — это файл с резервной копией, скопированный из виртуализированного ЦУ.

# engine-backup --mode=restore --scope=files --scope=db --file=имя\_файла --log=название\_журнала\_восстановления --provision-db --no-restore-permissions

1. После успешной миграции базы данных запустите службу ovirt-engine:

# systemctl start ovirt-engine.service

1. Log in to a self-hosted engine node and turn off maintenance mode, enabling the High Availability agents Авторизуйтесь на узле виртуализированного ЦУ и отключите режим обслуживания, при этом активируются агенты высокой доступности:

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



## Перенос хранилища данных на отдельную машину

В данном разделе описывается процесс миграции службы и базы данных хранилища из виртуализированного ЦУ на отдельную машину. Размещение службы хранилища данных на отдельной машине снижает нагрузку на каждую отдельную машину, а также даёт возможность каждой службе избежать потенциальных конфликтов из-за ресурсов ЦП и памяти, разделяемых с другими процессами.

Можно перенести службу хранилища данных и подключить её к уже существующей базе данных (ovirt\_engine\_history), или же можно перенести всю базу данных хранилища на отдельную машину перед операцией миграции службы хранилища данных. Если база данных хранилища размещается в виртуализированном ЦУ, то миграция базы данных в дополнение к миграции службы исключит возможную будущую борьбу за ресурсы на ВМ диспетчера. Базу данных можно перенести на ту же машину, на которую будет перенесена и служба хранилища данных, или же на машину, отдельную как от машины диспетчера, так и от машины службы хранилища данных.



### Миграция базы данных хранилища данных на отдельную машину

Перед началом миграции службы хранилища данных выполните миграцию базы данных хранилища данных (ovirt\_engine\_history). Создайте резервную копию с помощью engine-backup и восстановите её на новой машине базы данных. Чтобы получить дополнительные сведения о команде engine-backup, выполните engine-backup --help. Чтобы выполнить миграцию только службы, обратитесь к разделу B 2.2 Миграция службы хранилища данных на отдельную машину.

На новом сервере базы данных должна быть установлена ОС Red Hat Enterprise Linux 7 с подключёнными репозиториями.

#### Миграция базы данных хранилища данных на отдельную машину

1. Создайте резервную копию хранилища данных и файлов конфигурации на виртуализированном ЦУ:

# engine-backup --mode=backup --scope=dwhdb --scope=files --file=имя\_файла --log=название\_журнала\_восстановления

1. Скопируйте файл резервной копии с виртуализированного ЦУ на новую машину:

# scp /tmp/имя\_файла root@new.dwh.server.com:/tmp

1. Установите engine-backup на новой машине:

# yum install ovirt-engine-tools-backup

1. Установите пакет сервера PostgreSQL:

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

1. Инициализируйте базу данных PostgreSQL, запустите службу postgresql и убедитесь в том, что эта служба стартует при загрузке:

# scl enable rh-postgresql10 -- postgresql-setup --initdb

# systemctl enable rh-postgresql10-postgresql

# systemctl start rh-postgresql10-postgresql

1. Восстановите базу данных хранилища данных из резервной копии на новой машине. имя\_файла — это файл с резервной копией, скопированный из виртуализированного ЦУ

# engine-backup --mode=restore --scope=files --scope=dwhdb --file= имя\_файла --log=название\_журнала\_восстановления --provision-dwh-db --no-restore-permissions

База данных хранилища данных теперь размещается на машине, отдельной от машины, на которой размещается диспетчер виртуализации . После успешного восстановления базы данных из резервной копии, будет выведено сообщение о том, что нужно запустить команду engine-setup. Перед выполнением этой команды выполните миграцию службы хранилища данных.

### Миграция службы хранилища данных на отдельную машину

Службу хранилища данных, установленную и настроенную на виртуализированном ЦУ, можно перенести на отдельную машину. Размещение службы хранилища данных на отдельной машине снижает нагрузку на машину диспетчера виртуализации. Обратите внимание, что во время данной процедуры происходит миграция только службы. Сведения о том, как перенести базу данных хранилища данных (ovirt\_engine\_history) до начала переноса службы смотрите в разделе B 2.1.

**Предварительные условия и предпосылки**

* Виртуализированный ЦУ и хранилища данных должны быть установлены и настроены на одной и той же машине.
* Обязательные условия, необходимые для настройки новой машины для хранилища данных:
  + Пароль из файла диспетчера виртуализации **/etc/ovirt-engine/engine.conf.d/10-setup-database.conf**.
  + Разрешённый доступ из машины хранилища данных к порту 5432 TCP машины базы данных диспетчера виртуализации.
  + Имя пользователя и пароль для хранилища данных из файла диспетчера виртуализации **/etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-database.conf**. Если база данных ovirt\_engine\_history была перенесена по инструкции из раздела B 2.1, то в резервной копии содержатся учётные данные, настроенные во время процесса конфигурации базы данных на этой машине.

Установка по данному сценарию состоит из четырёх шагов:

1. Подготовка новой машины хранилища данных
2. Останов службы хранилища данных на машине диспетчера виртуализации
3. Настройка конфигурации новой машины хранилища данных
4. Отключение пакета хранилища данных на машине диспетчера виртуализации

#### Подготовка новой машины хранилища данных

1. Подключите репозитории и установите пакет настройки хранилища данных на машине под управлением ОС Red Hat Enterprise Linux 7.
2. Обновите версии текущих установленных пакетов:

# yum update

1. Установите пакет ovirt-engine-dwh-setup:

# yum install ovirt-engine-dwh-setup

#### Останов службы хранилища данных на машине диспетчера виртуализации

1. Остановите выполнение службы хранилища данных:

# systemctl stop ovirt-engine-dwhd.service

1. Если база данных размещается на удалённой машине, необходимо вручную предоставить доступ, отредактировав файл postgres.conf. Измените файл /var/opt/rh/rh-postgresql10/lib/pgsql/data/postgresql.conf так, чтобы строка listen\_addresses соответствовала следующей:

listen\_addresses = '\*'

Если эта строка не существует или была закомментирована, добавьте её вручную.

Если база данных размещается на машине диспетчера виртуализации и была настроена во время чистой установки диспетчера, то доступ будет разрешён по умолчанию.

Дополнительные сведения о том, как настраивать и переносить базу данных хранилища данных, смотрите в разделе B 2.1.

1. Перезапустите службу postgresql:

# systemctl restart rh-postgresql10-postgresql

#### Настройка конфигурации новой машины хранилища данных

Порядок вопросов, показанных на этом шаге, может отличаться, в зависимости от конкретного окружения.

1. Если миграция базы данных ovirt\_engine\_history и службы хранилища данных выполняется на **одну и ту же** машину, выполните следующую команду. В противном случае переходите к следующему шагу.

# sed -i '/^ENGINE\_DB\_/d' \

/etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-database.conf

# sed -i \

-e 's;^\(OVESETUP\_ENGINE\_CORE/enable=bool\):True;\1:False;' \

-e '/^OVESETUP\_CONFIG\/fqdn/d' \

/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf

1. Чтобы начать процесс конфигурирования хранилища данных на машине, запустите команду engine-setup:

# engine-setup

1. Нажмите Ввод для настройки хранилища данных:

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

1. **Чтобы принять имя хоста, обнаруженное автоматически, нажмите Ввод. В противном случае, укажите другое имя хоста и нажмите Ввод**:

Host fully qualified DNS name of this server [обнаруженное имя хоста]:

1. Для автоматической настройки межсетевого экрана нажмите Ввод, или же, для сохранения существующих параметров, введите No и нажмите клавишу Ввод:

Setup can automatically configure the firewall on this system.

Note: automatic configuration of the firewall may overwrite current settings.

Do you want Setup to configure the firewall? (Yes, No) [Yes]:

Если будет выбрана автоматическая настройка межсетевого экрана, и ни один из диспетчеров межсетевого экрана не является активным, будет выведено сообщение о выборе текущего диспетчера из списка поддерживаемых диспетчеров межсетевого экрана. Введите название диспетчера и нажмите Ввод. Это касается также и тех случаев, когда список поддерживаемых диспетчеров состоит только из одного элемента.

1. Укажите полное доменное имя и пароль виртуализированного ЦУ. Нажмите **Ввод** для принятия значений по умолчанию во всех других полях:

Host fully qualified DNS name of the engine server []: engine-fqdn

Setup needs to do some actions on the remote engine server. Either automatically, using ssh as root to access it, or you will be prompted to manually perform each such action.

Please choose one of the following:

1 - Access remote engine server using ssh as root

2 - Perform each action manually, use files to copy content around

(1, 2) [1]:

ssh port on remote engine server [22]:

root password on remote engine server engine-fqdn: password

1. Укажите полное доменное имя и пароль для виртуальной машины базы данных виртуализированного ЦУ. Нажмите Ввод для принятия значений по умолчанию во всех других полях:

Engine database host []: manager-db-fqdn

Engine database port [5432]:

Engine database secured connection (Yes, No) [No]:

Engine database name [engine]:

Engine database user [engine]:

Engine database password: password

1. Подтвердите параметры установки:

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

Теперь служба хранилища данных на удалённой машине настроена. Далее переходите к шагам, необходимым для отключения службы хранилища данных на машине диспетчера виртуализации.

#### Отключение службы хранилища данных на машине диспетчера виртуализации

1. Перезапустите диспетчер виртуализации на машине диспетчера:

# service ovirt-engine restart

1. Отключите службу хранилища данных:

# systemctl disable ovirt-engine-dwhd.service

1. Удалите файлы хранилища данных:

# rm -f /etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/\* .conf /var/lib/ovirt-engine-dwh/backups/\*

Теперь служба хранилища данных размещается на машине, отдельной от виртуализированного ЦУ.

## Перенос на отдельную машину сервера прокси, использующего протокол Websocket

ВАЖНО

Возможности noVNC и прокси с протоколом websocket являются исключительно экспериментальными. Экспериментальные возможности не поддерживаются соглашениями Red Hat об уровне обслуживания и могут иметь функциональные недоработки. Мы не рекомендуем использование этих возможностей в среде промышленной эксплуатации.

Из соображений безопасности или производительности, websocket proxy может работать на отдельной машине, на которой не функционирует виртуализированный ЦУ. Действия по переносу прокси с протоколом websocket с машины диспетчера виртуализации на отдельную машину включают в себя удаление конфигурации прокси с протоколом websocket с машины виртуализированного ЦУ, а затем установку прокси на отдельной машине.

Для удаления прокси с протоколом websocket с машины виртуализированного ЦУ используйте команду engine-cleanup:

#### Удаление прокси с протоколом websocket с машины диспетчера виртуализации

1. Для удаления нужной конфигурации выполните на машине диспетчера виртуализации команду engine-cleanup.

# engine-cleanup

1. На запрос о том, нужно ли удалить все компоненты, введите No и нажмите Ввод.

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

1. На запрос о том, нужно ли удалить виртуализированный ЦУ, введите No и нажмите Ввод.

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

1. На запрос о том, нужно ли удалить прокси с протоколом websocket, введите Yes и нажмите Ввод.

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

В случае вывода запроса на удаление любых других компонентов введите No.

#### Установка прокси с протоколом websocket на отдельную машину

ВАЖНО

Возможности *noVNC* и *прокси с протоколом websocket* являются исключительно экспериментальными. Экспериментальные возможности не поддерживаются соглашениями Red Hat об уровне обслуживания и могут иметь функциональные недоработки. Мы не рекомендуем использование этих возможностей в среде промышленной эксплуатации.

Прокси с протоколом websocket предоставляет возможность подключения пользователей к ВМ с использованием консоли noVNC. Клиент noVNC использует вебсокеты для передачи данных VNC. Но сервер VNC в QEMU не имеет поддержки websocket, поэтому между клиентом и сервером VNC нужно разместить сервер прокси, использующий протокол websocket . Этот прокси может работать на любой машине, имеющей сетевой доступ, включая машину виртуализированного ЦУ.

Из соображений безопасности или производительности пользователи могут настроить прокси с протоколом websocket на отдельной машине.

**Последовательность действий**

1. Установите прокси с протоколом websocket :

# yum install ovirt-engine-websocket-proxy

1. Выполните конфигурацию прокси с протоколом websocket, запустив команду engine-setup.

# engine-setup

ВНИМАНИЕ

Если ранее также был установлен пакет rhvm, то на запрос о том, нужно ли настроить виртуализированный ЦУ (Engine) на этом хосте, выберите No.

1. Разрешите команде engine-setup настроить сервер прокси с протоколом websocket, нажав клавишу Ввод.

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

1. **Чтобы принять имя хоста, обнаруженное автоматически, нажмите** Ввод**. В противном случае укажите другое имя хоста и нажмите** Ввод**. Обратите внимание, что в случае использования виртуальных хостов, автоматически обнаруженное имя хоста может быть неправильным:**

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

1. Разрешите команде engine-setup настроить межсетевой экран и открыть порты, необходимые для внешних связей. В случае, если вы не хотите дать это разрешение, откройте нужные порты вручную.

Setup can automatically configure the firewall on this system.

Note: automatic configuration of the firewall may overwrite current settings.

Do you want Setup to configure the firewall? (Yes, No) [Yes]:

1. Укажите полное доменное имя машины виртуализированного ЦУ и нажмите Ввод.

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

1. Разрешите engine-setup выполнять действия на машине виртуализированного ЦУ, нажав Ввод, или введите 2, чтобы выполнить действия вручную.

Setup will need to do some actions on the remote engine server. Either automatically, using ssh as root to access it, or you will be prompted to manually perform each such action.

Please choose one of the following:

1 - Access remote engine server using ssh as root

2 - Perform each action manually, use files to copy content around

(1, 2) [1]:

* 1. Для принятия номера порта SSH по умолчанию нажмите Ввод, или же введите номер порта машины диспетчера виртуализации:

ssh port on remote engine server [22]:

* 1. Укажите пароль root для авторизации на машине диспетчера виртуализации и нажмите Ввод.

root password on remote engine server *engine\_host.example.com*:

1. Выберите, нужно ли просмотреть созданные правила iptables на случай, если они отличаются от текущих.

Generated iptables rules are different from current ones.

Do you want to review them? (Yes, No) [No]:

1. Нажмите Ввод для подтверждения параметров конфигурации.

--== CONFIGURATION PREVIEW ==--

Firewall manager : iptables

Update Firewall : True

Host FQDN : host.example.com

Configure WebSocket Proxy : True

Engine Host FQDN : engine\_host.example.com

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

Для подготовки машины диспетчера виртуализации к использованию настроенного прокси с протоколом websocket предлагается инструкция.

Manual actions are required on the engine host

in order to enroll certs for this host and configure the engine about it.

Please execute this command on the engine host:

engine-config -s WebSocketProxy=host.example.com:6100

and than restart the engine service to make it effective

1. Авторизуйтесь на машине диспетчера виртуализации и выполните предложенную инструкцию.

# engine-config -s WebSocketProxy=host.example.com:6100

# systemctl restart ovirt-engine.service

# Настройка на хосте сквозного доступа к устройствам PCI

Включение сквозного доступа к устройствам PCI даёт виртуальной машине возможность использовать устройство хоста так, как если бы это устройство было напрямую подключено к ВМ. Чтобы включить возможность сквозного доступа к PCI, нужно активировать расширения виртуализации и функцию IOMMU. В инструкции ниже потребуется перезагрузка хоста. Если хост уже был присоединён к виртуализированному ЦУ, не забудьте сначала перевести хост в режим обслуживания.

**Предварительные условия и предпосылки**

* Убедитесь в том, что аппаратная часть хоста соответствует требованиям для присвоения и сквозного доступа к PCI. Подробности смотрите по ссылке <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/planning_and_prerequisites_guide/rhv_requirements#PCI_Device_Requirements_RHV_planning>

**Подготовка хоста к настройке сквозного доступа к устройствам PCI**

1. Включите в BIOS расширения виртуализации и IOMMU. Подробности смотрите в руководстве по ссылке <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/Virtualization_Deployment_and_Administration_Guide/sect-Troubleshooting-Enabling_Intel_VT_x_and_AMD_V_virtualization_hardware_extensions_in_BIOS.html>
2. Активируйте флаг IOMMU в ядре, отметив галочкой параметр **Hostdev Passthrough & SR-IOV** во время добавления хоста в виртуализированный ЦУ или вручную отредактировав конфигурационный файл **grub**.
   * Чтобы активировать флаг через Портал администрирования, просмотрите руководства [Adding Standard Hosts to the Red Hat Virtualization Manager](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/administration_guide#Adding_standard_hosts_to_the_Manager) and [Kernel Settings Explained](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/administration_guide#Kernel_Settings_Explained)
   * О том, как вручную редактировать файл конфигурации **grub**, читайте в [Enabling IOMMU Manually](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/Configuring_a_Host_for_PCI_Passthrough_SHE_cockpit_deploy#Enabling_IOMMU_Manually).
3. Для настройки сквозного доступа к GPU необходимо выполнить ряд дополнительных шагов как на стороне хоста, так и на стороне гостевой системы. Смотрите [GPU device passthrough: Assigning a host GPU to a single virtual machine](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/setting_up_an_nvidia_gpu_for_a_virtual_machine_in_red_hat_virtualization/proc_nvidia_gpu_passthrough_nvidia_gpu_passthrough) .

**Ручная активация IOMMU**

1. Включение IOMMU путём редактирования файла конфигурации grub.

ВНИМАНИЕ

В случае использования аппаратного обеспечения IBM POWER8 этот шаг можно пропустить, так как в этом аппаратном обеспечении IOMMU активирован по умолчанию.

* + Для Intel: загрузите машину и добавьте параметр intel\_iommu=on в конец строки GRUB\_CMDLINE\_LINUX конфигурационного файла **grub**.

# vi /etc/default/grub

...

GRUB\_CMDLINE\_LINUX="nofb splash=quiet console=tty0 ... intel\_iommu=on

...

* + Для AMD: загрузите машину и добавьте параметр amd\_iommu=on в конец строки GRUB\_CMDLINE\_LINUX конфигурационного файла **grub**.

# vi /etc/default/grub

...

GRUB\_CMDLINE\_LINUX="nofb splash=quiet console=tty0 ... amd\_iommu=on

...

ВНИМАНИЕ

Если параметр intel\_iommu=on или amd\_iommu=on дают желаемый эффект, то можно затем попробовать добавить iommu=pt или amd\_iommu=pt. Параметр pt активирует IOMMU только для устройств, используемых в сквозном доступе, что даёт лучшую производительность хоста, но не все аппаратные средства его поддерживают. Если для конкретного хоста параметр pt не работает, откатитесь к начальному параметру.

В случае неудачной реализации сквозного доступа из-за того, что аппаратное обеспечение не поддерживает переназначение прерываний, попробуйте включить на доверенных машинах параметр allow\_unsafe\_interrupts. По умолчанию, параметр allow\_unsafe\_interrupts не включён, поскольку его активация открывает хост для потенциальных атак MSI с виртуальных машин. Включить этот параметр можно следующим образом:

**# vi /etc/modprobe.d**

**options vfio\_iommu\_type1 allow\_unsafe\_interrupts=1**

1. Обновите содержимое файла **grub.cfg** и перезагрузите хост, чтобы изменения вступили в силу:

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

# reboot

Чтобы включить SR-IOV и присвоить соответствующие виртуальные NIC виртуальным машинам, смотрите руководство <https://access.redhat.com/articles/2335291>.

# Удаление виртуализированного ЦУ

Для удаления всех или отдельных компонентов диспетчера виртуализации используйте команду engine-cleanup.

ВНИМАНИЕ

Резервная копия базы данных виртуализированного ЦУ и сжатый архив ключей и параметров PKI всегда создаётся автоматически. Эти файлы сохраняются в каталоге /var/lib/ovirt-engine/backups/, а в имена этих файлов добавляется дата и префиксы engine- и engine-pki-, соответственно.

**Последовательность действий**

1. Запустите следующую команду на машине виртуализированного ЦУ :

# engine-cleanup

1. Будет выведен запрос об удалении всех компонентов диспетчера виртуализации :
   * Введите Yes и нажмите Ввод, чтобы удалить все компоненты:

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

* + Введите No и нажмите Ввод, чтобы выбрать компоненты для удаления. Для каждого отдельного компоненты можно указать, оставить его или удалить:

Do you want to remove Engine database content? All data will be lost (Yes, No) [No]:

Do you want to remove PKI keys? (Yes, No) [No]:

Do you want to remove PKI configuration? (Yes, No) [No]:

Do you want to remove Apache SSL configuration? (Yes, No) [No]:

1. Будет дана ещё одна возможность передумать и отменить удаление диспетчера виртуализации. При выборе продолжать работа службы ovirt-engine будет остановлена, а конфигурация окружения будет удалена в соответствии с выбранными параметрами.

During execution engine service will be stopped (OK, Cancel) [OK]:

ovirt-engine is about to be removed, data will be lost (OK, Cancel) [Cancel]:OK

1. Удалите пакеты среды виртуализации:

# yum remove rhvm\* vdsm-bootstrap