# Глава 7. Хосты

## 7.1. Введение в понятие хостов

Хосты, также известные как «гипервизоры», — это физические серверы, на которых выполняются виртуальные машины. Полная виртуализация достигается за счёт использования загружаемого модуля ядра Linux, называемого Kernel-based Virtual Machine (KVM).

KVM может поддерживать одновременную работу многих виртуальных машин под управлением ОС Windows или ОС Linux. На машине хоста ВМ выполняются как отдельные процессы и потоки Linux и управляются удалённо виртуализированным ЦУ. К виртуализированному ЦУ присоединяется один или более хостов виртуализации.

Система виртуализации Red Hat поддерживает два способа установки хостов. Можно использовать источник установки хостов виртуализации (RHVH) или же установить на стандартный хост пакеты гипервизора.

ВНИМАНИЕ

Чтобы установить тип отдельного хоста в виртуализированном ЦУ, выберите имя хоста, чтобы перейти к подробному просмотру, а затем в разделе *Программное обеспечение* просмотрите пункт *Описание ОС*.

На хостах используются профили tuned , предоставляющие оптимизацию виртуализации. Сведения об этих профилях см. <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/Performance_Tuning_Guide/sect-Red_Hat_Enterprise_Linux-Performance_Tuning_Guide-Performance_Monitoring_Tools-tuned_and_tuned_adm.html>

На хостах виртуализации включены средства защиты. Система SELinux и межсетевой экран полностью настроены и активированы по умолчанию. Статус SELinux на выбранном хосте отображается в разделе **Режим SELinux** вкладки **Общие** подробного просмотра. При добавлении в окружение обычных хостов, виртуализированный ЦУ может открыть необходимые порты этих хостов.

Обычный хост — это физический 64-битный сервер с расширениями Intel VT или AMD-V под управлением ОС Red Hat Enterprise Linux 7 AMD64/Intel для 64 битных систем.

Физический хост платформы системы виртуализации Red Hat:

* Должен принадлежать только к одному кластеру в системе
* Должен иметь ЦП с поддержкой расширений аппаратной виртуализации AMD-V или Intel VT.
* Должен иметь процессор с поддержкой всех функций того типа виртуального ЦП, который был выбран при создании кластера
* Имеет минимум 2 Гбайт ОЗУ
* Обслуживается системным администратором с системными полномочиями

**7.2. Хосты виртуализации Red Hat**

Хост виртуализации red Hat устанавливается в виде специальной сборки ОС Red Hat Enterprise Linux, в которую входят только пакеты, необходимые для виртуальных машин. Во время установки используется интерфейс Anaconda, на базе этого же установщика, используемого для обычных хостов. ПО хостов виртуализации обновляется при участии виртуализированного ЦУ или с помощью yum. Использование yum является единственным способом установки дополнительных пакетов и сохранения их после обновлений.

Для наблюдения за ресурсами хоста и выполнения задач администрирования на хостах виртуализации используется веб-интерфейс Cockpit. Прямой доступ к хостам виртуализации с помощью SSH или консоли не поддерживается, поэтому веб-интерфейс Cockpit предоставляет графический интерфейс также и для задач, выполняемых перед тем, как хост будет добавлен в виртуализированный ЦУ, таких, как настройка сетевой конфигурации и установка виртуализированного ЦУ (диспетчера виртуализации). Кроме того, во вкладке **Терминал** веб-интерфейса можно выполнять консольные команды.

Доступ к веб-интерфейсу Cockpit осуществляется в веб-браузере по адресу https://*полное\_доменное\_имя\_хоста\_или\_IP*:9090. В составе Cockpit также есть панель мониторинга **Виртуализация**, где показывается состояние работоспособности хоста, ключ SSH хоста, статус виртуализированного ЦУ, виртуальные машины и их статистика.

Для сбора имеющей значение информации отладки на хостах виртуализации используется «инструмент автоматизированных отчётов об ошибках» (Automatic Bug Reporting Tool, ABRT).

ВНИМАНИЕ

Частные аргументы загрузки ядра на хостах виртуализации можно добавить с помощью утилиты grubby, вносящей постоянные изменения в файл grub.cfg. Для работы с командами grubby перейдите на вкладку *Терминал* веб-интерфейса Cockpit.

ПРЕДУПРЕЖДЕНИЕ

Настоятельно рекомендуется не создавать на хостах виртуализации недоверенных пользователей, поскольку это может привести к эксплуатации локальных уязвимостей.

# 7.3. Стандартные хосты Red Hat

Установленную на соответствующем требованиям аппаратном оборудовании ОС Red Hat Enterprise Linux 7 можно использовать в качестве хоста. Система виртуализации Red Hat поддерживает хосты под управлением Red Hat Enterprise Linux 7 Server AMD64/Intel для 64 битных систем с расширениями Intel VT или AMD-V.

Добавление хоста может занять некоторое время, по мере выполнения платформой следующих шагов: проверки виртуализации, установка пакетов и создание моста. После наладки соединения между хостом и системой управления используйте подробный просмотр для наблюдения за ходом всех процессов.

Опционально, для наблюдения за ресурсами хоста и выполнения административных задач можно установить веб-интерфейс Cockpit. Веб-интерфейс Cockpit предоставляет графический пользовательский интерфейс также и для задач, выполняемых перед тем, как хост будет добавлен в виртуализированный ЦУ, таких, как настройка сетевой конфигурации и установка виртуализированного ЦУ (диспетчера виртуализации). Кроме того, во вкладке **Терминал** веб-интерфейса можно выполнять консольные команды.

ВАЖНО

На обычных хостах Red Hat Enterprise Linux нельзя устанавливать сторонние модули наблюдения, поскольку они могут помешать фоновой работе модуля наблюдения, предоставляемого VDSM.

# 7.4. Хосты, предоставляемые поставщиком хостов системы Satellite

Хосты, предоставляемые поставщиком хостов Satellite, также могут использоваться виртуализированным ЦУ в качестве хостов виртуализации. После добавления Satellite в качестве поставщика в виртуализированный ЦУ, любые предоставляемые им хосты можно добавлять и использовать в системе виртуализации Red Hat точно так же, как и хосты виртуализации и обычные хосты.

# 7.5. Задачи при работе с хостами

### 7.5.1. Добавление в виртуализированный ЦУ стандартных хостов

Добавление хоста в систему виртуализации Red Hat может занять некоторое время, по мере выполнения платформой следующих шагов: проверки виртуализации, установка пакетов и создание моста.

ВАЖНО

При создании моста управления, использующего статический адрес IPv6, перед добавлением хоста отключите управление network manager в конфигурационном файле его интерфейсов (ifcfg). Подробности см. <https://access.redhat.com/solutions/3981311>

**Последовательность действий**

1. На портале администрирования нажмите **Вычисления → Хосты**.
2. Нажмите **Добавить**.
3. В выпадающем списке выберите **Дата-центр** и **Кластер хоста** для нового хоста.
4. Укажите **Имя** и **Адрес** нового хоста. В поле **Порт SSH** автоматически добавляется стандартный номер порта SSH, 22.
5. Выберите метод аутентификации, используемый диспетчером виртуализации для подключения к хосту:
   * При использовании аутентификации по паролю введите пароль root
   * Как вариант, скопируйте ключ из поля **Открытый ключ SSH** в файл **/root/.ssh/authorized\_keys** хоста, чтобы использовать аутентификацию по открытому ключу.
6. Опционально, нажмите на кнопку **Дополнительные параметры**, чтобы настроить следующие дополнительные параметры хоста:
   * Отключить автоматическую настройку межсетевого экрана
   * Добавить отпечаток SSH хоста для повышения уровня безопасности. Это можно сделать вручную или получить отпечаток автоматически.
7. Опционально, настройте управление питанием там, где у хоста есть поддерживаемая карта управления питанием.
8. Нажмите OK.

Новый хост появится в списке хостов со статусом **Устанавливается**, а проследить за процессом установки можно в разделе **События** в **Секции уведомлений** (). После некоторого ожидания статус хоста сменится на **Запущен**.

### 7.5.2. Добавление хоста, поставляемого поставщиком хостов системы Satellite

Процесс добавления хоста системы Satellite почти идентичен процессу добавления обычного хоста под управлением ОС Red Hat Enterprise Linux за исключением способа идентификации хоста в виртуализированном ЦУ. В нижеследующей шаговой последовательности описывается, как добавить хост, поставляемый поставщиком хостов системы Satellite.

**Добавление хоста Satellite**

1. Нажмите **Вычисления → Хосты**.
2. Нажмите **Добавить**.
3. В выпадающем списке выберите **Кластер хоста** для нового хоста.
4. Отметьте галочкой параметр **Foreman/Satellite** , чтобы увидеть параметры добавления поставщика хостов Satellite и выбрать поставщика добавляемого хоста.
5. Выберите либо **Обнаруженные хосты**, либо **Подготовленные хосты**.
   * **Обнаруженные хосты** (по умолчанию): в выпадающем списке выберите хост, группу хоста и вычислительные ресурсы.
   * **Подготовленные хосты**: выберите хост в выпадающем списке **Хосты поставщика**.

Все сведения о хосте, которые могут быть автоматически получены от внешнего поставщика, вводятся автоматически, и, при необходимости, могут быть отредактированы.

1. Укажите **Имя** и **Порт SSH** (только для хостов поставщиков) для нового хоста.
2. Выберите способ аутентификации, используемый на новом хосте.
   * При использовании аутентификации по паролю введите пароль root
   * Как вариант, скопируйте ключ из поля **Открытый ключ SSH** в файл **/root/.ssh/ authorized\_hosts** хоста, чтобы использовать аутентификацию по открытому ключу (только для хостов поставщиков).
3. На данном этапе все обязательные пункты по добавлению обычного хоста выполнены. Для просмотра дополнительных параметров хоста нажмите кнопку **Дополнительные параметры**.
   * Опционально, отключите автоматическую настройку межсетевого экрана.
   * Опционально, для повышения уровня безопасности, добавьте отпечаток SSH хоста. Его можно добавить вручную или получить автоматически .
4. Теперь, в соответствующих вкладках можно настроить **Управление питанием**, **SPM**, **Консоль** и **Поставщика сети**, но, поскольку эти шаги не являются основными при добавлении хостов, они здесь не описываются.
5. Нажмите **OK**, чтобы добавить хост и закрыть окно.

Новый хост будет показан в списке хостов со статусом **Устанавливается**, а в подробном просмотре можно пронаблюдать за продвижением процесса установки. После окончания установки статус хоста сменится на **Перезагрузка**. Чтобы статус сменился на **Запущен**, хост нужно активировать.

### 7.5.3. Настройка управления списком известных ошибок (Errata) системы Satellite для хоста

В системе виртуализации Red Hat можно настроить просмотр списка известных ошибок платформы Red Hat Satellite. Это даёт возможность администраторам хоста получать обновления о доступных списках ошибок и их важности, на той же панели управления, которая используется для работы с конфигурацией хоста.

Система виртуализации Red Hat 4.3. поддерживает управление списком ошибок системы Red Hat Satellite 6.5.

ВАЖНО

На сервере Satellite хосты идентифицируются по их полному доменному имени. Хосты, добавленные с использованием адреса IP, не смогут отправлять сообщения, содержащие Errata. Благодаря этому, для виртуализированного ЦУ отпадает необходимость управления идентификаторами хостов с внешним контентом.

Учётная запись Satellite, используемая для управления хостом, должна иметь полномочия администратора и настроенную организацию по умолчанию.

**Настройка управления списком известных ошибок (errata) платформы Satellite**

1. Добавьте сервер Satellite в качестве внешнего поставщика. Подробности см. в Разделе 11.2.1.
2. Привяжите нужный хост к серверу Satellite.

ВНИМАНИЕ

На хосте должен быть установлен пакет katello-agent и хост должен быть зарегистрирован на сервере Satellite.

* 1. Нажмите Вычисления → Хосты и выберите нужный хост.
  2. Нажмите **Изменить**.
  3. Отметьте галочкой параметр **Использовать** **Foreman/Satellite.**
  4. В выпадающем списке выберите нужный сервер Satellite
  5. Нажмите **OK**.

На панели управления хоста, используемой для работы с конфигурацией, теперь настроен показ доступных списков известных ошибок и их степень важности.

### 7.5.4. Объяснение параметров и элементов управления в окнах «Новый хост» и «Параметры хоста»

### 7.5.5. Объяснение общих параметров хоста

Эти параметры применяются во время изменения сведений о хосте или добавления обычных хостов под управлениям ОС Red Hat Enterprise Linux и хостов поставщика хостов системы Satellite

Таблица общих параметров содержит информацию, необходимую для указания во вкладке **Общие** окон **Новый хост** или **Параметры хоста**.

**Таблица 7.1.  Общие параметры**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Кластер хоста | Кластер и дата-центр, к которым принадлежит хост. |
| **Использовать Foreman/Satellite** | Поставьте или снимите галочку, чтобы просмотреть или скрыть параметры добавления хостов, поставляемых поставщиком хостов системы Satellite. Также доступны следующие возможности:  **Обнаруженные хосты**   * **Обнаруженные хосты**: выпадающий список, заполняемый именами хостов Satellite, обнаруженными диспетчером виртуализации * **Группы хостов**: выпадающий список доступных групп хостов * **Вычислительные ресурсы**: выпадающий список гипервизоров, предоставляющих вычислительные ресурсы.   **Подготовленные хосты**   * **Хосты поставщиков**: выпадающий список, заполняемый именами хостов, предоставляемых выбранным внешним поставщиком. Элементы списка фильтруются в соответствии с любыми поисковыми запросами, введёнными в **Поисковом фильтре поставщика**. * **Поисковый фильтр поставщиков**: текстовое поле для поиска хостов, предоставленных выбранным внешним поставщиком. Этот параметр зависит от поставщика; подробности создания поисковых запросов смотрите в документации поставщика. Для просмотра всех хостов оставьте это поле пустым. |
| Имя | Имя хоста. У этого текстового поля имеется ограничение в 40 символов, а введённое название должно быть уникальным сочетанием любых строчных или прописных букв, цифр, дефисов и знаков подчёркивания |
| Комментарий | Поле для добавления удобочитаемого комментария для хоста в простом текстовом формате. |
| Имя хоста | Адрес IP хоста или разрешаемое имя хоста. При использовании разрешаемого имени необходимо обеспечить совпадение разрешаемого имени хоста со всеми адресами IP (IPv4 и IPv6), используемыми в сети управления хоста. |
| Пароль | Пароль пользователя root. Можно указать только при добавлении хоста; после этого изменению не подлежит. |
| Открытый ключ SSH | Скопируйте содержимое текстового блока в файл **/root/.ssh/authorized\_hosts** хоста, чтобы при аутентификации на хосте использовать ключ SSH диспетчера виртуализации вместо пароля. |
| Автоматически настроить межсетевой экран хоста | При добавлении нового хоста виртуализированный ЦУ может открыть требуемые порты в конфигурации межсетевого экрана этого хоста. Это параметр включён по умолчанию и является **Дополнительным параметром**. |
| Отпечаток SSH | Возможность получить отпечаток SSH хоста и сопоставить его с ожидаемым отпечатком, проверив таким образом их соответствие. Это **Дополнительный параметр**. |

### 7.5.6. Объяснение параметров управления питанием хоста

Таблица параметров **Управления питанием** содержит информацию, которую необходимо указать во вкладке **Управление питанием** окон **Новый хост** или **Параметры хоста**.

**Таблица 7.2. Параметры управления питанием**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| **Включить управление питанием** | Включает управление питанием на хосте. Отметьте галочкой этот параметр для активации остальных полей во вкладке **Управление питанием**. |
| **Интеграция kdump** | Предотвращает проведение операции блокады на хосте во время выполнения аварийного дампа ядра, чтобы не прерывать дамп. В ОС Red Hat Enterprise Linux 7.1 и более поздних утилита kdump доступна по умолчанию. Если kdump присутствует на хосте, но её конфигурация недействительна (невозможно запустить службу kdump), то включение параметра **Интеграция kdump приведёт к сбою установки (или переустановки). В этом случае обратитесь к Разделу 7.6.4.** |
| Отключить контроль управления питанием со стороны политики | Управление питанием контролируется **Политикой планирования** кластера хоста. При включённом управлении питанием и достижении указанного значения низкого потребления виртуализированный ЦУ выключит машину хоста и запустит её снова из расчёта балансировки нагрузки, или когда в кластере не будет достаточного числа свободных хостов. Поставьте здесь галочку, чтобы отключить контроль со стороны политики. |
| Агенты в последовательном порядке | Список агентов операции блокады. Агенты операции блокады могут быть последовательными, параллельными или совмещать и то и другое.   * Если агенты операции блокады используются последовательно, то сначала, для остановки или запуска хоста, используется первичный агент, а в случае его сбоя — вторичный. * Если агенты работают параллельно, то на команду остановки хоста должны отреагировать оба агента; если на команду запуска хоста отреагирует один агент, то хост начнёт работу.   По умолчанию, агенты операции блокады являются последовательными. Для смены последовательности, в которой используются агенты, используйте кнопки со стрелками вверх и вниз.  Чтобы сделать двух агентов операции блокады параллельными, выберите одного агента из выпадающего списка **Одновременно с:** рядом с другим агентом. Дополнительных агентов можно добавить в группу параллельно выполняющихся агентов, выбрав группу из выпадающего списка **Одновременно с:** рядом с дополнительным агентом**.** |
| Добавить агента операции блокады | Для добавления нового агента нажмите на кнопку со знаком **+**. Будет открыто окно **Параметры агента операции блокады**. Дополнительные сведения о параметрах в этом окне смотрите в таблице ниже. |
| Предпочитаемый прокси для управления питанием | По умолчанию указывает, что диспетчер виртуализации будет искать прокси операции блокады в рамках того же **кластера**, в состав которого входит хост, а в случае неудачного поиска — в том же дата-центре. Это поле находится в **Дополнительных параметрах**. |

В таблице ниже содержится информация, необходимая для заполнения полей в окне **Параметры агента операции блокады**.

**Таблица 7.3. Параметры агента операции блокады**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Адрес | Адрес для доступа к устройству управления питаниям хоста. Укажите разрешаемое имя хоста или адрес IP. |
| Имя пользователя | Учётная запись пользователя, которая будет получать доступ к устройству управления питанием. Для устройства можно настроить специального пользователя, или использовать пользователя по умолчанию. |
| Пароль | Пароль пользователя, получающего доступ к устройству управления питанием. |
| Тип | Тип устройства управления питанием на хосте. Выберите что-то одно из следующего:   * **apc** - коммутатор питания по сети APC MasterSwitch. Нельзя использовать с устройствами серии APC 5.x. * **apc\_snmp** - д**ля работы с коммутаторами питания серии** APC 5.x * **bladecenter** – удалённый супервизор-адаптер IBM Bladecenter. * **cisco\_ucs** - Cisco Unified Computing System. * **drac5** – контроллер удалённого доступа Dell для компьютеров Dell. * **drac7** - контроллер удалённого доступа Dell для компьютеров Dell. * **eps** - ePowerSwitch 8M+ коммутатор питания по сети. * **hpblade** - HP BladeSystem. * **ilo**, **ilo2**, **ilo3**, **ilo4** - HP Integrated Lights-Out. * **ipmilan** –устройства управления Intelligent Platform Management Interface и Sun Integrated Lights Out Management. * **rsa** - удалённый супервизор-адаптер IBM. * **rsb** – интерфейс управления Fujitsu-Siemens RSB. * **wti** - коммутатор питания по сети WTI.   Для дополнительной информации об устройствах управления питанием обратитесь к разделу **Управление питанием** Технического справочника. |
| Порт | Номер порта, используемого устройством управления питанием для связи с хостом. |
| Слот | Число для идентификации платы устройства управления питанием. |
| Профиль службы | Имя профиля устройства, используемое для идентификации платы устройства управления питанием. Это поле появляется вместо поля **Слот** при использовании типа cisco\_ucs. |
| Параметры | Параметры конкретного устройства управления питанием. Указывайте в виде «ключ=значение». Доступные параметры ищите в документации конкретного устройства.  При использовании cisco\_ucs на обычных хостах под управлением ОС Red Hat 7, в поле **Параметры** также необходимо добавлять ssl\_insecure=1. |
| Защищённое | Отметьте этот параметр галочкой для защищённого подключения к хосту с помощью ssh, ssl или других протоколов аутентификации, в зависимости от агента управления питанием. |

### 7.5.7. Объяснение параметров приоритетов SPM (диспетчер пула хранилища)

В таблице параметров **SPM** приводятся подробности о сведениях, необходимых для заполнения вкладки **SPM** окон **Новый хост** или **Параметры хоста**.

**Таблица 7.4. Параметры SPM**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Приоритет SPM | Определяет вероятность того, что хосту будет присвоена роль диспетчера пула хранилища (Storage Pool Manager, SPM). Можно выбрать **Низкий**, **Нормальный** и **Высокий** приоритеты. Низкий приоритет означает сниженную вероятность присвоения роли SPM, высокий — повышенную. Значение по умолчанию — «Нормальный». |

### 7.5.8. Объяснение параметров вкладки «Консоль»

В таблице «Параметры вкладки Консоль» приводятся подробности о сведениях, необходимых для указания во вкладке **Консоль** окон **Новый хост** и **Параметры хоста**.

**Таблица 7.5. Параметры вкладки «Консоль»**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Переназначить адрес экрана | Отметьте галочкой этот параметр, чтобы переназначить адрес экрана хоста. Этот параметр удобен в том случае, когда хосты определяются внутренним IP и находятся за межсетевым экраном NAT. При подключении пользователя к ВМ из-за пределов внутренней сети, вместо того, чтобы возвращать частный адрес хоста, на котором выполняется ВМ, машина будет возвращать открытый IP или FQDN (который во внешней сети разрешается на открытый IP). |
| Адрес экрана | Указанный здесь адрес экрана будет использоваться для всех ВМ, выполняющихся н этом хосте. Этот адрес должен указываться в формате полного доменного имени или IP. |

### 7.5.9. Объяснение параметров вкладки «Поставщик сети»

В таблице «Параметры вкладки «Поставщик сети» приводятся подробности о сведениях, необходимых для указания во вкладке **Поставщик сети** окон **Новый хост** и **Параметры хоста**.

**Таблица 7.6. Параметры вкладки «Поставщик сети»**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Поставщик внешней сети | В случае наличия поставщика внешней сети и необходимости того, чтобы сеть хоста предоставлялась внешним поставщиком, выберите поставщика из этого списка. |

### 7.5.10. Объяснение параметров ядра

В таблице «Параметры ядра» приводятся подробности о сведениях, необходимых для указания во вкладке «Ядро» окон **Новый хост** и **Параметры хоста**. Наиболее часто встречающиеся параметры загрузки ядра приводятся в виде флажков для удобства быстрого выбора.

Для более сложного редактирования и добавления любых необходимых дополнительных параметров используйте свободное текстовое поле с меткой **Командная строка ядра**. При изменении любых консольных параметров необходима переустановка хоста (Раздел 7.5.20).

ВАЖНО

Перед тем, как вносить изменения в параметры хостов, присоединённых к виртуализированному ЦУ, эти хосты необходимо перевести в режим обслуживания. Затем, для применения внесённых изменений, эти хосты необходимо переустановить (Раздел 7.5.20)

**Таблица 7.7. Параметры ядра**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| **Сквозной доступ к устройству хоста и SR-IOV** | Включает флаг IOMMU ядра для возможности использования виртуальной машиной устройства хоста, как устройства, напрямую подключённого к ВМ. Аппаратное и программное обеспечение также должно поддерживать IOMMU. Для аппаратного обеспечения должны быть включены расширения виртуализации и IOMMU. См. Раздел 7.5.14. В IBM POWER8 функционал IOMMU активирован по умолчанию.Р |
| **Вложенная виртуализация** | Активирует флаги vmx или svm для возможности запуска виртуальных машин внутри виртуальных машин. Этот параметр предназначается для задач оценки и не поддерживает эксплуатацию в условиях производства. На хосте должна быть установлена ловушка vdsm-hook-nestedvt. |
| **Небезопасные прерывания** | Этот параметр может быть включён в случаях сбоя сквозного доступа при активированном IOMMU. Обратите внимание, что этот параметр моет быть активирован только если ВМ хоста являются доверенными; активный параметр потенциально открывает хост для атак MSI со стороны виртуальных машин. Этот параметр рассматривается только как обходное решение при использовании несертифицированного аппаратного обеспечения для оценочных целей. |
| Перераспределение PCI | Если сетевая плата с поддержкой SR-IOV не может выделить виртуальный функционал в связи с проблемами памяти, попробуйте включить этот параметр. Аппаратное и программное обеспечение хоста также должно поддерживать перераспределение PCI. Этот параметр рассматривается только как обходное решение при использовании несертифицированного аппаратного обеспечения для оценочных целей. |
| **Командная строка ядра** | Это поле даёт возможность добавить дополнительные параметры ядра к параметрам по умолчанию. |

ВНИМАНИЕ

В случае, если параметры загрузки ядра отображаются серым цветом, нажмите на кнопку *Сбросить*, и параметры станут доступны.

### 7.5.11. Объяснение параметров виртуализированного ЦУ

В таблице «Параметры виртуализированного ЦУ» приводятся подробности о сведениях, необходимых для указания во вкладке «Виртуализированный ЦУ» окон **Новый хост** и **Параметры хоста**.

**Таблица 7.8. Параметры виртуализированного ЦУ**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| **Выберите действие по развёртыванию виртуализированного ЦУ** | Доступно три возможности:   * **Нет** — никаких действий не требуется * **Развернуть** — выберите это действие, чтобы развернуть хост в качестве узла виртуализированного ЦУ * **Свернуть** — этот параметр выбирается для узла виртуализированного ЦУ в случае необходимости свернуть установку хоста и удалить все конфигурации, относящиеся к виртуализированному ЦУ |

### 7.5.12. Настройка параметров управления питанием хоста

Настройте параметры устройства управления питанием хоста для выполнения операций жизненного цикла (останов, запуск, перезапуск) с портала администрирования.

Для того, чтобы использовать функционал высокой доступности хоста и высокой доступности ВМ, должно быть настроено управление питанием хоста. Подробные сведения об устройстве управления питанием щите в разделе **Управление питанием** Технического справочника.

**Настройка параметров управления питанием**

1. Нажмите **Вычисления → Хосты** и выберите хост.
2. Нажмите **Управление → Обслуживание** и нажмите **OK** для подтверждения.
3. После перевода хоста в режим обслуживания нажмите **Изменить**.
4. Перейдите на вкладку **Управление питанием**.
5. Отметьте галочкой параметр **Включить управление питанием**, чтобы активировать соответствующие поля.
6. Отметьте галочкой параметр **Интеграция kdump**, чтобы предотвратить проведение операции блокады хоста во время выполнения аварийного дампа ядра.

ВАЖНО

Если Интеграция kdump включается или отключается на существующем хосте, этот хост необходимо переустановить для настройки параметров kdump (Раздел 7.5.20).

1. Опционально, отметьте галочкой параметр **Отключить контроль управления питанием со стороны политики**, если управление питанием хоста не должно контролироваться **Политикой планирования** кластера хоста.
2. Для добавления нового устройства управления питаниям нажмите на кнопку со знаком плюс (**+**). Будет открыто окно **Параметры агента операции блокады**.
3. В соответствующих полях укажите **Имя пользователя** и **Пароль** для устройства управления питанием.
4. Выберите **Тип** устройства управления питанием в выпадающем списке.
5. В поле Адрес укажите адрес IP.
6. Укажите номер **Порта SSH**, используемого устройством управления питанием для связи с хостом.
7. Укажите номер **Слота**, используемого для идентификации платы устройства управления питанием.
8. Настройте **Параметры** устройства управления питанием в форме списка записей «ключ=значение», разделённых запятыми.
   * В случае использования как адресов IPv4, так и адресов IPv6 (по умолчанию), оставьте поле **Параметры** пустым.
   * При использовании только адресов IPv4, введите inet4\_only=1.
   * При использовании только адресов IPv6, введите inet6\_only=1.
9. Отметьте галочкой параметр **Защищённое**, чтобы включить защищённое соединение между устройством управления питанием и хостом.
10. Чтобы убедиться в том, что все значения корректны, нажмите кнопку **Проверка**. В случае успешной проверки будет показано сообщение **Проверка выполнена, статус хоста: запущен**.
11. Нажмите **OK**, чтобы закрыть окно **Параметры агента операции блокады**.
12. Во вкладке **Управление питанием** при желании разверните **Дополнительные параметры**, и с помощью кнопок со стрелками вверх и вниз настройте порядок, в котором виртуализированный ЦУ будет выполнять поиск прокси операции блокады в **кластере** хоста и в **дата-центре**.
13. Нажмите **OK**.

ВНИМАНИЕ

* + Поддерживается только статическая адресация IPv6
  + Адресация для двойного стека (IPv4 и IPv6) не поддерживается.

На портале администрации теперь доступно выпадающее меню Управление → Управление питанием

### 7.5.13. Настройка параметров управления пулом хранилища хоста

Диспетчер пула хранилища (SMP) — это роль управления, присваиваемая одному из хостов в дата-центре для контроля доступа к доменам хранилищ. Диспетчер пула хранилища должен быть всегда доступен, и в случае недоступности хоста SPM, эта роль будет присвоена другому хосту. Поскольку роль SPM использует некоторые из доступных ресурсов хоста, очень важно отдать приоритет тем хостам, которые могут выделить эти ресурсы.

Параметр приоритете SPM хоста изменяет вероятность присвоения роли SPM хосту: хосту с высоким приоритетом роль SPM будет присвоена раньше хоста с низким приоритетом.

**Настройка параметров SPM**

1. Нажмите **Вычисления → Хосты**
2. Нажмите **Изменить**.
3. Перейдите на вкладку **SPM**.
4. Отметьте галочкой соответствующий приоритет SPM хоста.
5. Нажмите **OK**.

### 7.5.14. Настройка на хосте сквозного доступа к PCI

ВНИМАНИЕ

Это один из нескольких разделов, в которых рассказывается, как установить и настроить технологию виртуализацию ввода-вывода с единым корнем (SR-IOV) в системе виртуализации Red Hat. Подробности смотрите в Разделе 6.4.10.

Включение технологии сквозного даёт возможность виртуальной машине использовать устройство хоста так, как если бы оно было напрямую подключено к ВМ. Чтобы включить функцию сквозного доступа к PCI, необходимо активировать расширения виртуализации и функционал IOMMU. В нижеследующей пошаговой инструкции требуется перезагрузка хоста. Если хост уже был присоединён к виртуализированному ЦУ, обязательно сначала переместите хост в режим облуживания.

**Предварительные условия**

* Убедитесь в том, что аппаратное обеспечение хоста отвечает требованиям сквозного доступа к PCI и его присвоения.

**Подготовка хоста для применения сквозного доступа к PCI**

1. Включите в BIOS расширения виртуализации и IOMMU.
2. Включите флаг IOMMU в ядре, отметив галочкой параметр **Сквозной доступ к устройству хоста и SR-IOV** при добавлении хоста в виртуализированный ЦУ или вручную отредактировав конфигурационный файл загрузчика **grub**.
   * Чтобы включить флаг IOMMU с помощью портала администрирования, обратитесь к разделам 7.5.1 и 7.5.10
   * Чтобы вручную изменить конфигурационный файл **grub**, обратитесь к разделу 7.5.12
3. Для активации сквозного доступа к GPU необходимо выполнить дополнительные шаги по настройке как на хосте так и в гостевой системе. Подробности см. <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. Включите IOMMU, отредактировав конфигурационный файл grub.

ВНИМАНИЕ

В случае использования аппаратного обеспечения IBM POWER8 этот шаг нужно пропустить, так как IOMMU активирован по умолчанию.

* + В случае Intel, загрузите машину и добавьте intel\_iommu=on в конце записи GRUB\_CMDLINE\_LINUX в конфигурационном файле **grub**.

# vi /etc/default/grub

...

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

...

* + В случае AMD, загрузите машину и добавьте amd\_iommu=on в конце записи GRUB\_CMDLINE\_LINUX в конфигурационном файле **grub**.

# vi /etc/default/grub

...

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

...

ВНИМАНИЕ

Если параметры intel\_iommu=on или amd\_iommu=on являются рабочими, можно попробовать добавить iommu=pt или amd\_iommu=pt. Параметр pt активирует IOMMU только для устройств, используемых в сквозном доступе и улучшает производительность хоста. Но этот параметр может поддерживаться не всеми аппаратными составляющими. Откатитесь к предыдущему параметру, если pt не сработает на конкретном хосте.

Если сквозной доступ будет неудачным по причине отсутствия поддержки переназначения прерываний аппаратными составляющими, то, в случае доверенных ВМ, можно попробовать параметр allow\_unsafe\_interrupts . Этот параметр не включается по умолчанию, поскольку его активация потенциально может открыть хост атакам MSI со стороны ВМ. чтобы включить параметр:

# vi /etc/modprobe.d

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

1. Обновите информацию в файле **grub.cfg** и перезагрузите хост для применения изменений:

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

# reboot

Чтобы включить SR-IOV и назначить предназначенные для этого сетевые карты виртуальным машинам, см. <https://access.redhat.com/articles/2335291>.

### 7.5.15. Перевод хоста в режим обслуживания

Многие задачи обслуживания, включая настройку сетевой конфигурации и разворачивание обновлений ПО, требует помещения хостов в режим обслуживания. Хосты должны помещаться в режим обслуживания до того, как могут произойти события, которые потенциально могут нарушить корректную работу VDSM, такие, как перезагрузка или сбои в работе сети или хранилищ.

При помещении хоста в режим обслуживания, виртуализированный ЦУ попытается перенести все работающие ВМ на альтернативные хосты. Здесь применяются стандартные предварительные условия динамической миграции. В частности, в кластере должен присутствовать минимум один хост с ресурсами, достаточными для выполнения переносимых ВМ.

ВНИМАНИЕ

Виртуальные машины, привязанные к хосту и не подлежащие миграции, выключаются. Проверить, какие машины привязаны к хосту, можно, нажав на кнопку Привязано к хосту на вкладке Виртуальные машины в подробном просмотре хоста.

**Перемещение хоста в режим обслуживания**

1. Нажмите **Вычисления → Хосты** и выберите хост.
2. Нажмите Управление → Обслуживание, чтобы открыть окно подтверждения **Хосты на обслуживании**.
3. Опционально, укажите **Причину** перемещения хоста в режим облуживания, которая появится в журнале и при повторной активации хоста.

ВНИМАНИЕ

Поле *Причина* переведения хоста в режим обслуживания появится, только если эта возможность была включена в параметрах кластера. Смотрите Раздел 5.2.2.

1. Опционально, выберите нужные параметры для хостов с поддержкой Gluster.

Выберите параметр **Игнорировать кворум Gluster и проверки самовосстановления** для избежания проверок по умолчанию. По умолчанию, во время помещения хоста в режим обслуживания, виртуализированный ЦУ проверяет, не был ли потерян кворум Gluster. ЦУ также проверяет хост на наличие задач по самовосстановлению, на которые может повлиять перевод хоста в режим обслуживания. Если кворум будет потерян, или если выполняются действия по самовосстановлению, которые могут быть затронуты, виртуализированный ЦУ не разрешит поместить хост в режим обслуживания. Используйте этот параметр, только если нет никаких других способов поместить хост в режим облуживания.

Выберите **Остановить службу Gluster**, чтобы остановить выполнение всех служб Gluster во время перемещения хоста в режим облуживания.

ВНИМАНИЕ

Эти поля появляются в окне обслуживания хоста, если выбранный хост поддерживает Gluster.

1. Нажмите **OK** для запуска режима обслуживания.

Все выполняющиеся ВМ мигрируют на другие хосты. Если хосту была присвоена роль диспетчера пула хранилища, то эта роль переходит к другому хосту. В поле **Статус** хоста сначала указывается Подготовка к облуживанию, а затем, после успешного окончания подготовки, Обслуживание. Когда хосты находятся в режиме обслуживания, VDSM не прекращает свою работу.

ВНИМАНИЕ

При сбое миграции какой-либо ВМ, нажмите на хосте *Управление → Активировать* для остановки действий по помещению этого хоста в режим обслуживания, затем на виртуальной машине нажмите *Прервать миграцию*, для остановки миграции.

### 7.5.16. Активация хоста из режима обслуживания

Перед использованием хоста, помещённого ранее в режим обслуживания или недавно добавленного в окружение, его необходимо активировать. Если хост не готов, его активация может закончиться неудачей; перед тем, как попытаться активировать хост, убедитесь в том, что выполнение всех задач завершено.

**Активация хоста из режима обслуживания**

1. Нажмите **Вычисления → Хосты** и выберите хост.
2. Нажмите **Управление → Активировать**.

Статус хоста изменится на Не присвоено, а затем, после завершения операции, на Запущен. Теперь на хосте могут выполняться виртуальные машины. ВМ, мигрировавшие с хоста при помещении его в режим обслуживания, не возвращаются автоматически, но их можно вернуть вручную. Если до помещения в режим обслуживания хост выполнял роль диспетчера пула хранилища (SPM), эта роль не возвращается автоматически при активации хоста.

### 7.5.17. Настройка правил межсетевого экрана хоста

С помощью утилиты Ansible можно настроить перманентную конфигурацию правил межсетевого экрана. Кластер должен быть настроен на работу с firewalld, а не с iptables.

ВНИМАНИЕ

iptables является устаревшим.

**Настройка правил межсетевого экрана для хостов**

1. На машине диспетчера виртуализации отредактируйте файл **ovirt-host-deploy-post-tasks.yml.example** для добавления частного порта межсетевого экрана:

# vi /etc/ovirt-engine/ansible/ovirt-host-deploy-post-tasks.yml.example

---

#

# Any additional tasks required to be executing during host deploy process can

# be added below

#

- name: Enable additional port on firewalld

firewalld:

port: "12345/tcp"

permanent: yes

immediate: yes

state: enabled

1. Сохраните файл по другому пути как **ovirt-host-deploy-post-tasks.yml**.

Новые или повторно установленные хосты настраиваются с обновлёнными правилами межсетевого экрана.

Существующие хосты необходимо переустановить, с помощью пунктов меню **Установка → Переустановить** и с выбранным параметром **Автоматически настроить межсетевой экран хоста**.

### 7.5.18. Удаление хоста

Удалите хост из окружения виртуализации.

**Удаление хоста**

1. Нажмите **Вычисления → Хосты** и выберите хост.
2. Нажмите **Управление → Обслуживание**
3. После помещения хоста в режим обслуживания нажмите **Удалить**, чтобы открыть окно подтверждения **Удалить хост(ы)**.
4. Если хост является частью кластера хранилища Gluster и на хосте имеются кирпичи тома, или же если хост не отвечает — отметьте галочкой параметр **Принудительное удаление**.
5. Нажмите **OK**.

### 7.5.19. Обновление ПО хоста до следующего минорного выпуска

Можно обновить все хосты в кластере (7.5.19.1) или отдельные хосты (7.5.19.2).

#### 7.5.19.1. Обновление всех хостов в кластере

Вместо обновления ПО на отдельных хостах, можно обновить сразу все хосты в кластере. Это особенно удобно при переходе на новые версии системы виртуализации Red Hat. Сведения о роли Ansible, используемой для автоматизации процесса обновления до новой версии, смотрите по ссылке <https://github.com/oVirt/ovirt-ansible-cluster-upgrade/blob/master/README.md>

Мы рекомендуем обновлять только один кластер за раз.

**Ограничения**

* На хостах виртуализации при обновлении сохраняется только изменённое содержимое каталогов /etc и /var. Изменённое содержимое других каталогов при обновлении перезаписывается.
* Если миграция включена на уровне кластера, ВМ автоматически мигрируют на другой хост в кластере.
* В окружении виртуализированного ЦУ виртуальная машина ЦУ может мигрировать только на узлы виртуализированного ЦУ в рамках одного кластера, и не может мигрировать на стандартные хосты.
* В кластере должен иметься резерв памяти, достаточный для выполнения обслуживания хостов в составе этого кластера. В противном случае миграция ВМ зависнет и закончится неудачно. Снизить потребление памяти во время обновления ПО хостов можно, выключив некоторые из ВМ до начала процесса обновления хостов.
* Прикреплённые к хосту ВМ (такие, как ВМ, использующие виртуальные GPU) не могут мигрировать на другие хосты. Во время обновления такие машины выключаются, или же такие хосты можно не обновлять.

**Последовательность действий**

1. На портале администрирования нажмите **Вычисления → Кластеры** и выберите кластер.
2. Нажмите **Обновить**.
3. Выберите хосты для обновления и нажмите **Далее**.
4. Настройте параметры:
   * **Остановить работу прикреплённых ВМ выключает любые ВМ, прикреплённые к хосту в кластере; по умолчанию этот параметр отмечен. Можно снять галочку с этого параметра, чтобы пропустить обновление этих хостов, для продолжения работы прикреплённых ВМ, если на этих ВМ выполняются важные службы или процессы, которые нежелательно останавливать на неопределённое время во время обновления ПО.**
   * **Время ожидания обновления (мин.)** устанавливает время ожидания обновления отдельного хоста перед тем, как обновление кластера будет считаться неудачным. Значение по умолчанию — 60. Для больших кластеров, где 60 минут может не хватить, значение можно увеличить, а для маленьких кластеров с быстро обновляющимися хостами — снизить.
   * **Проверить обновления** проверяет доступные обновления ПО для каждого хоста перед запуском процесса обновления. Этот параметр не выбран по умолчанию, но его можно выбрать, если есть необходимость убедиться в том, что будут включены все самые свежие обновления в тех случаях, когда виртуализированный ЦУ настроен на проверку обновлений не так часто, как устанавливается значением проверок по умолчанию.
   * **Перезагрузить после обновления перезагружает каждый хост после применения обновлений; параметр выбран по умолчанию. Эту галочку можно снять, если есть необходимость ускорить процесс в тех случаях, когда администратор уверен, что применённые обновления не требуют перезагрузок.**
   * **Использовать политику обслуживания устанавливает значение** cluster\_maintenance **для политики планирования кластера на время применения обновлений. Параметр выбран по умолчанию, поэтому активность будет ограничена, а ВМ не смогут начать работу, если только они не являются высокодоступными. Эту галочку можно снять при наличии частной политики планирования, которую необходимо выполнять и во время обновлений, но последствия таких действий неизвестны. Перед отключениям этого параметра убедитесь в том, что такая частная политика совместима с действиями обновления ПО в кластере.**
5. Нажмите **Далее**.
6. Просмотрите сводку о хостах и ВМ, которые будут затронуты процессом обновления ПО.
7. Нажмите **Обновить**.

Проследить за прогрессом обновления ПО на хостах можно в меню **Вычисления → Хосты**, а также в разделе **События** в **Секции уведомлений** ().

Проследить за процессом миграции отдельных ВМ можно в столбце **Статус** меню **Вычисления → Виртуальные машины**. В обширных окружениях может понадобиться отфильтровать результаты для показа конкретной группы ВМ.

#### 7.5.19.2. Обновление отдельных хостов

Для обновления ПО на конкретных хостах используйте диспетчер обновления хостов на портале администрирования.

ВНИМАНИЕ

Диспетчер обновлений проверят только хосты со статусом *Запущен* или *В нерабочем состоянии*, но не со статусом *Обслуживание*.

**Ограничения**

* На хостах виртуализации при обновлении сохраняется только изменённое содержимое каталогов /etc и /var. Изменённое содержимое других каталогов при обновлении перезаписывается.
* Если миграция включена на уровне кластера, ВМ будут автоматически мигрировать на другой хост в кластере. Обновляйте ПО на хосте при низкой его загруженности.
* В окружении виртуализированного ЦУ виртуальная машина ЦУ может мигрировать только на узлы виртуализированного ЦУ в рамках одного кластера, и не может мигрировать на стандартные хосты.
* В кластере должен иметься резерв памяти, достаточный для выполнения обслуживания хостов в составе этого кластера. В противном случае миграция ВМ зависнет и закончится неудачно. Снизить потребление памяти во время обновления ПО хостов можно, выключив некоторые из ВМ до начала процесса обновления хостов.
* Не обновляйте ПО на всех хостах одновременно, один из хостов должен быть доступен для выполнения задач роли диспетчера пула хранилища (SPM).
* Прикреплённые к хосту ВМ (такие, как ВМ, использующие виртуальные GPU) не могут мигрировать на другие хосты. Во время обновления такие машины выключаются, или же такие хосты можно не обновлять.

**Последовательность действий**

1. Убедитесь в том, что подключены соответствующие репозитории. Чтобы просмотреть список текущих подключённых репозиториев, выполните yum repolist.
2. На портале администрирования нажмите **Вычисления → Хосты** и выберите обновляемый хост.
3. Нажмите **Установка → Проверить наличие обновлений** и нажмите **OK**. Для просмотра результатов откройте **Секцию уведомлений** () и разверните раздел **События**.
4. При наличии обновлений нажмите **Установка → Обновить**.
5. Чтобы применить обновления нажмите OK. Выполняющиеся ВМ будут мигрировать согласно их политике миграции. Если для какой-либо ВМ миграция отключена, будет предложена возможность их выключить.

Подробные сведения о хосте обновляются в разделе **Вычисления → Хост**, а статус будет меняться в следующей последовательности:

**Обслуживание > Идёт установка > Перезагрузка > Запущен**

ВНИМАНИЕ

В случае сбоя процесса обновления, статус хоста сменится на *Сбой установки*. После этого можно снова нажать *Установка → Обновление*.

Повторите эти шаги для каждого хоста в окружении виртуализации.

Рекомендуется обновлять хосты с портала администрирования. Тем не менее, обновить хосты можно и вручную с помощью yum update:

#### 7.5.19.3. Обновление ПО на хостах вручную

Для обновления ПО на хостах используется программа yum. Обновляйте системы регулярно для своевременного применения исправлений ошибок безопасности и ошибок кода.

**Ограничения**

* На хостах виртуализации при обновлении сохраняется только изменённое содержимое каталогов /etc и /var. Изменённое содержимое других каталогов при обновлении перезаписывается.
* Если миграция включена на уровне кластера, ВМ будут автоматически мигрировать на другой хост в кластере. Обновляйте ПО на хосте при низкой его загруженности.
* В окружении виртуализированного ЦУ виртуальная машина ЦУ может мигрировать только на узлы виртуализированного ЦУ в рамках одного кластера, и не может мигрировать на стандартные хосты.
* В кластере должен иметься резерв памяти, достаточный для выполнения обслуживания хостов в составе этого кластера. В противном случае миграция ВМ зависнет и закончится неудачно. Снизить потребление памяти во время обновления ПО хостов можно, выключив некоторые из ВМ до начала процесса обновления хостов.
* Не обновляйте ПО на всех хостах одновременно, один из хостов должен быть доступен для выполнения задач роли диспетчера пула хранилища (SPM).
* Прикреплённые к хосту ВМ (такие, как ВМ, использующие виртуальные GPU) не могут мигрировать на другие хосты. Во время обновления такие машины выключаются, или же такие хосты можно не обновлять.

**Последовательность действий**

1. Убедитесь в том, что подключены соответствующие репозитории. Чтобы просмотреть список текущих подключённых репозиториев, выполните yum repolist.
2. На портале администрирования нажмите **Вычисления → Хосты** и выберите обновляемый хост.
3. Нажмите **Управление → Обслуживание**.
4. Обновите ПО на хосте:

# yum update

1. Перезагрузите хост для корректного применения всех обновлений.

ВНИМАНИЕ

Проверьте файлы журнала imgbased, чтобы узнать о возможных сбоях обновлений дополнительных пакетов на хостах виртуализации. Если какие-либо пакеты не были переустановлены успешно после обновления, проверьте, перечислены ли эти пакеты в файле **/var/imgbased/persisted-rpms**. Добавьте отсутствующие пакеты и затем выполните rpm -Uvh /var/imgbased/persisted-rpms/\*.

Повторите эти шаги для каждого из хостов в окружении виртуализации Red Hat.

### 7.5.20. Повторная установка хостов

Переустановите хосты виртуализации и стандартные хосты с помощью портала администрирования. В последовательность действий включается останов и перезапуск хостов.

**Предварительные условия**

* Если миграция включена на уровне кластера, ВМ будут автоматически мигрировать на другой хост в кластере. Рекомендуется обновлять ПО на хосте при относительно низкой его загруженности.
* В кластере должен иметься резерв памяти, достаточный для выполнения обслуживания хостов в составе этого кластера. В противном случае миграция ВМ зависнет и закончится неудачно. Снизить потребление памяти во время обновления ПО хостов можно, выключив некоторые из ВМ до начала перевода хостов в режим обслуживания.
* Перед началом повторной установки убедитесь, что кластер содержит более одного хоста. Не обновляйте ПО на всех хостах одновременно, один из хостов должен быть доступен для выполнения задач роли диспетчера пула хранилища (SPM).

**Последовательность действий**

1. Нажмите **Вычисления → Хосты** и выберите хост.
2. Нажмите **Управление → Обслуживание**.
3. Нажмите **Установка → Повторная установка**, откроется окно **Установка хоста**.
4. Нажмите **OK** для повторной установки хоста.

После успешной переустановки хоста будет иметь статус **Запущен**. Все ВМ, мигрировавшие с хоста, теперь могут вернуться.

ВАЖНО

После успешной регистрации хоста виртуализации в виртуализированном ЦУ и последующей переустановки, на портале администрирования этот хост может получить ошибочный статус *Сбой установки*. Нажмите *Управление → Активировать*, статус хоста сменится на *Запущен*, и хост будет готов к работе.

### 7.5.21. Индивидуализация хостов с помощью меток

Метки можно использовать для хранения информации о хостах, а затем выполнять поиск на основе этих меток. Подробности о поиске см. <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/introduction_to_the_administration_portal/index#Searching_for_hosts>

**Индивидуальная настройка хостов с помощью меток**

1. Нажмите **Вычисления → Хосты** и выберите хост.
2. Нажмите **Больше действий** (), затем **Назначить теги**.
3. Отметьте галочками применимые метки.
4. Нажмите **OK**.

Мы добавили дополнительную, доступную для поиска информацию о хостах в виде меток.

### 7.5.22. Просмотр списка известных ошибок (errata) для хоста

Список известных ошибок для каждого хоста можно просмотреть после того, как на хосте было настроено получение информации с сервера Red Hat Satellite. Подробности о настройке получения хостом информации о списке известных ошибок см. Раздел 7.5.3.

**Просмотр списка известных ошибок (errata) для хоста**

1. Нажмите **Вычисления → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Errata**.

### 7.5.23. Просмотр статуса работоспособности хоста

В дополнение к обычному **Статусу**, у хостов есть внешний статус работоспособности. Информация о внешнем статусе работоспособности доставляется расширениями или внешними системами, или же настраивается администратором. Просмотреть её можно слева от имени хоста в виде следующих значков:

* **OK**: без значка
* **Информация**: 
* **Предупреждение**: 
* **Ошибка**: 
* **Сбой**: 

Чтобы узнать дополнительные подробности о работоспособности хоста нажмите на имя хоста, чтобы перейти к подробному просмотру , и перейдите на вкладку **События**.

Статус работоспособности хоста также можно узнать с помощью REST API. В запрос GET будет включён элемент external\_status , содержащий этот статус.

Указать статус работоспособности хоста в REST API можно с помощью набора events. Подробности см. <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/rest_api_guide/services#services-events-methods-add>

### 7.5.24. Просмотр устройств хоста

Устройства каждого хоста можно увидеть на вкладке Устройства хоста в подробном просмотре. Если на хосте можно настроить прямое присвоение устройств, то эти устройства можно напрямую подключить к ВМ, для улучшения производительности.

Подробности о настройке прямого присвоения устройств на хосте смотрите в Разделе 7.5.14.

**Просмотр устройств хоста**

1. Нажмите **Вычисления → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Устройства хоста**.

В этой вкладке приводится подробный список устройств хоста, включая информацию о том, подключено ли устройство к ВМ и используется ли этой ВМ в данный момент.

### 7.5.25. Доступ к веб-интерфейсу Cockpit с портала админиcтрирования.

По умолчанию, Cockpit доступен как на хостах виртуализации, так и на стандартных хостах. Доступ к нему можно получить, введя адрес в адресную строку браузера, или через портал администрирования.

**Доступ к Cockpit с портала администрирования**

1. На портале администрирования нажмите **Вычисления → Хосты** и выберите хост.
2. Нажмите **Консоль хоста**.

В новом окне браузера будет открыта страница авторизации Cockpit.

### 7.5.26. Настройка шифра для старых версий SPICE

По умолчанию, в консолях SPICE используется совместимое с FIPS шифрование, со строкой шифра. Строка шифра для SPICE по умолчанию: kECDHE+FIPS:kDHE+FIPS:kRSA+FIPS:!eNULL:!aNULL

Обычно этой строки хватает. Тем не менее, при наличии ВМ с более старой ОС или старым клиентом SPICE, где один из них не поддерживает совместимое с FIPS шифрование, необходимо будет использовать более слабую строку. В противном случае, при установке нового кластера или нового хоста в уже существующий кластер и попытке подключения к этой виртуальной машине может возникнуть ошибка безопасности соединения.

Изменить строку шифра можно с помощью файла сценариев Ansible (Ansible playbook).

**Изменение строки шифра**

1. На машине диспетчера виртуализации создайте файл в каталоге /usr/share/ovirt-engine/playbooks. Например:

# vim /usr/share/ovirt-engine/playbooks/change-spice-cipher.yml

1. Вставьте в файл следующее содержимое и сохраните файл:

name: oVirt - setup weaker SPICE encryption for old clients

hosts: hostname

vars:

host\_deploy\_spice\_cipher\_string: 'DEFAULT:-RC4:-3DES:-DES'

roles:

- ovirt-host-deploy-spice-encryption

1. Запустите только что созданный файл:

# ansible-playbook -l hostname /usr/share/ovirt-engine/playbooks/change-spice-cipher.yml

Как вариант, можно изменить параметры хоста с помощью Ansible playbook ovirt-host-deploy с параметром --extra-vars и переменной host\_deploy\_spice\_cipher\_string следующим образом:

# ansible-playbook -l hostname \

--extra-vars host\_deploy\_spice\_cipher\_string=”DEFAULT:-RC4:-3DES:-DES” \

/usr/share/ovirt-engine/playbooks/ovirt-host-deploy.yml

# 7.6. Отказоустойчивость хостов

### 7.6.1. Высокая доступность хостов

Для поддержания отзывчивости хостов в кластере, диспетчер виртуализации использует операции блокады («огораживание»). Хост со статусом **Не отвечает** отличается от хоста со статусом **В нерабочем состоянии**. Нерабочие хосты могут обмениваться информацией с диспетчером виртуализации, но имеют некорректную конфигурацию, например, отсутствие локальной сети. Не отвечающие хосты не могут поддерживать связь с диспетчером виртуализации.

Огораживание позволяет кластеру среагировать на неожиданный сбой хоста и принудительно применить доступные политики экономии питания, балансировки нагрузки и доступности ВМ. Параметры операции блокады устройства управления питанием хоста должны быть настроены, и их корректность необходимо время от времени тестировать. Во время операции огораживания неотвечающий хост перезагружается, и если он не вернётся к активному состоянию в течение указанного времени, он останется неотвечающим в ожидании ручного вмешательства и решения проблем.

ВНИМАНИЕ

Для автоматической проверки параметров операции блокады можно настроить параметры engine-config: PMHealthCheckEnabled (по умолчанию false) и PMHealthCheckIntervalInSec (3600 сек по умолчанию).

При значении true, PMHealthCheckEnabled будет проверять всех агентов хоста согласно временному интервалу, указанному параметром PMHealthCheckIntervalInSec, и в случае обнаружения проблем выдаст предупреждение. Подробности о настройке параметров engine-config смотрите в Разделе 19.2.2.

После перезагрузки, действия по управлению питанием могут быть выполнены виртуализированным ЦУ, хостом прокси или вручную на портале администрирования. Все ВМ, выполняющиеся на неотвечающих хостах, будут остановлены, а высокодоступные ВМ будут запущены на другом хосте. Для действий по управлению питанием необходимо минимум два хоста.

После запуска диспетчера виртуализации, после окончания времени молчания (5 минут по умолчанию), он автоматически попытается огородить не отвечающие хосты, на которых включено управление питанием. Время молчания можно настроить с помощью параметра DisableFenceAtStartupInSec для engine-config.

ВНИМАНИЕ

Параметр engine-config DisableFenceAtStartupInSec помогает предотвратить ситуации, когда диспетчер виртуализации пытается выполнить операцию блокады для загружающихся хостов. Это может случиться после перебоя в работе дата-центра, так как процесс загрузки хоста занимает больше времени, чем процесс загрузки диспетчера виртуализации.

Хосты могут быть огорожены автоматически с помощью хоста прокси, использующего параметры управления питанием, или же вручную, сделав щелчок ПКМ по хосту и выбрав необходимые пункты меню.

ВАЖНО

На хосте, где выполняются высокодоступные ВМ, управление питанием должно быть включено и настроено.

### 7.6.2. Управление питанием с помощью прокси в системе виртуализации Red Hat

Виртуализированный ЦУ не связывается напрямую с агентами операции блокады. Для обмена командами с устройством управления питанием хоста виртуализированный ЦУ использует прокси. Для выполнения действий устройства управления питанием, виртуализированный ЦУ использует VDSM, поэтому другой хост в окружении играет роль прокси для операции блокады.

Можно выбрать:

* Любой хост в том же кластере, что и огораживаемый хост
* Любой хост в том же дата-центре, что и огораживаемый хост

Хост, пригодный для роли прокси огораживания, имеет статус либо **Запущен**, либо **Обслуживание**.

### 7.6.3. Настройка параметров операции блокады («огораживание») на хосте

Параметры огораживания хостов настраиваются в области **Управление питанием** окон **Новый хост** или **Параметры хоста**. Управление питанием даёт возможность системе огородить проблемный хост, используя такие дополнительные интерфейсы, как карта удалённого доступа (Remote Access Card, RAC).

Все действия по управлению питанием выполняются через хост-прокси, а не напрямую виртуализированным ЦУ. Для действий управления питанием необходимо как минимум два хоста.

**Настройка параметров операции блокады («огораживания») на хосте**

1. Нажмите **Вычисления → Хосты** и выберите хост.
2. Нажмите **Изменить**.
3. Перейдите на вкладку **Управление питанием**.
4. Отметьте галочкой параметр **Включить управление питанием**, чтобы активировать поля ввода.
5. Отметьте галочкой параметр **Интеграция kdump**, чтобы предотвратить огораживание хоста во время выполнения аварийного дампа ядра.

ВАЖНО

При активации или деактивации *Интеграции kdump* на существующем хосте, этот хост необходимо затем переустановить (Раздел 7.5.20).

1. Опционально, отметьте галочкой параметр **Отключить контроль управления питанием со стороны политик**, если управление питанием хоста не должно контролироваться **Политикой планирования** кластера, в который входит хост.
2. Нажмите на кнопку **+**, чтобы добавить новое устройство управления питанием. Будет открыто окно **Параметры агента операции блокады**.
3. Укажите **Адрес**, **Имя пользователя** и **Пароль** для устройства управления питанием.
4. В выпадающем списке выберите **Тип** устройства управления питанием.
5. Укажите номер **Порта SSH**, используемый устройством управления питанием для связи с хостом.
6. Укажите номер **Слота**, используемого для идентификации платы устройства управления питанием.
7. Настройте **Параметры** устройства управления питанием в форме списка записей «ключ=значение», разделённых запятыми.
8. Отметьте галочкой параметр **Защищённое**, чтобы включить защищённое соединение между устройством управления питанием и хостом.
9. Чтобы убедиться в том, что все значения корректны, нажмите кнопку **Проверка**. В случае успешной проверки будет показано сообщение **Проверка выполнена, статус хоста: запущен**.

ПРЕДУПРЕЖДЕНИЕ

Параметры управления питанием (идентификатор пользователя, пароль, параметры и др) тестируются виртуализированным ЦУ только во время настройки, а после этого вручную. При выборе игнорирования предупреждений о некорректных параметрах, или же если параметры изменяются на аппаратных компонентах устройств управления питанием без внесения соответствующих изменений в виртуализированном ЦУ, в самый ответственный момент может случиться сбой операции блокады.

1. Нажмите **OK** для закрытия окна **Параметры агента операции блокады**.
2. Опционально, во вкладке **Управление питанием** разверните Дополнительные параметры, и с помощью кнопок со стрелками вверх и вниз укажите порядок, в котором виртуализированный ЦУ будет вести поиск прокси для операции блокады в **кластере** и **дата-центре**.
3. Нажмите **OK**.

Мы вернулись к списку хостов. Обратите внимание, что восклицательный знак рядом с именем хоста исчез, что означает успешную настройку управления питанием.

### 7.6.4. Дополнительные параметры fence\_kdump

**kdump**

Чтобы просмотреть статус службы kdump, нажмите на имя хоста во вкладке **Общие** подробного просмотра:

* **Включено**: kdump настроен соответствующим образом, а служба kdump выполняется.
* **Отключено**: служба kdump не выполняется (в этом случае интеграция kdump не будет работать должным образом).
* **Неизвестно**: случается только на хостах с более ранними версиями VDSM, не сообщающими о статусе kdump.

**fence\_kdump**

Включение параметра **Интеграция kdump** во вкладке **Управление питанием** окон **Новый хост** или **Параметры хоста** создаёт стандартную конфигурацию агента fence\_kdump. Если сетевая конфигурация окружения не слишком сложна, а полное доменное имя диспетчера виртуализации разрешается на всех хостах, то исходных параметров fence\_kdump будет достаточно для его использования.

Но существуют случаи, когда бывает необходима продвинутая конфигурация fence\_kdump. В окружениях с более сложными сетевыми параметрами может понадобиться вручную настроить виртуализированный ЦУ, слушатель fence\_kdump или их обоих. Если, например, полное доменное имя виртуализированного ЦУ разрешается не на всех хостах с активированной **Интеграцией kdump**, то настроить правильное имя хоста или адрес IP можно с помощью engine-config:

engine-config -s FenceKdumpDestinationAddress=A.B.C.D

Примеры случаев, когда также могут понадобиться изменения конфигурации:

* Виртуализированный ЦУ с двумя сетевыми картами, одна из которых общедоступна, а вторая предназначена для сообщений fence\_kdump
* Необходимость запуска слушателя fence\_kdump по другому адресу IP или на другом порту.
* Необходимость настроить частный интервал для уведомлений fence\_kdump в целях предотвращения возможных потерь пакетов.

Частные параметры обнаружения fence\_kdump рекомендуются только для продвинутых пользователей, поскольку внесение изменений в изначальную конфигурацию необходимо только в усложнённых сетевых конфигурациях. Доступные параметры слушателя fence\_kdump ищите в Разделе 7.6.4.1. Как настроить kdump в виртуализированном ЦУ — Раздел 7.6.4.2.

#### 7.6.4.1. Настройка слушателя fence\_kdump

Измените параметры слушателя fence\_kdump. Это необходимо только в тех случаях, когда конфигурации по умолчанию бывает недостаточно.

**Ручная настройка слушателя fence\_kdump**

1. Создайте новый файл (например, **my-fence-kdump.conf**) в каталоге **/etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/**.
2. Укажите частные параметры согласно синтаксису ПАРАМЕТР=значение и сохраните файл.

ВАЖНО

Изменённые значения также должны быть согласованы с параметрами engine-config, согласно таблице параметров настройки слушателя fence\_kdump в Разделе 7.6.4.2

1. Перезапустите слушатель fence\_kdump:

# systemctl restart ovirt-fence-kdump-listener.service

При необходимости, также можно изменить следующие параметры:

**Таблица 7.9. Параметры настройки слушателя fence\_kdump**

|  |  |  |  |
| --- | --- | --- | --- |
| **Переменная** | **Описание** | **По умолчанию** | **Примечание** |
| LISTENER\_ADDRESS | Адрес IP, на который будут приходить сообщения fence\_kdump | 0.0.0.0 | При изменении значения этого параметра, он должен соответствовать значению параметра FenceKdumpDestinationAddress в engine-config. |
| LISTENER\_PORT | Указывает порт, на который будут приходить сообщения fence\_kdump | 7410 | При изменении значения этого параметра, он должен соответствовать значению параметра FenceKdumpDestinationPort в engine-config. |
| HEARTBEAT\_INTERVAL | Указывает интервал (в сек.) обновлений периодического сигнала слушателя. | 30 | При изменении значения этого параметра, он должен быть равен (или быть меньше) половинному значению параметра FenceKdumpListenerTimeout в engine-config. |
| SESSION\_SYNC\_INTERVAL | Указывает интервал (в сек.) синхронизации сеансов kdump в памяти хоста слушателя с базой данных. | 5 | При изменении значения этого параметра, он должен быть равен (или быть меньше) половинному значению параметра KdumpStartedTimeout в engine-config. |
| REOPEN\_DB\_CONNECTION\_INTERVAL | Указывает интервал (в сек.) для повторного открытия соединения к базе данных, которая ранее была недоступна. | 30 | - |
| KDUMP\_FINISHED\_TIMEOUT | Определяет максимальный период ожидания (в сек.) после последнего полученного сообщения от хостов, на которых выполняется kdump, по истечению которого поток kdump хоста будет помечен как ЗАВЕРШЕНО. | 60 | При изменении значения этого параметра, он должен быть равен (или быть больше) двойному значению параметра FenceKdumpMessageInterval в engine-config. |

#### 7.6.4.2. Настройка fence\_kdump в виртуализированном ЦУ

Отредактируйте конфигурацию kdump в виртуализированном ЦУ. Это необходимо только для случаев, когда конфигурации по умолчанию недостаточно. Текущие параметры можно узнать с помощью команды:

# engine-config -g ПАРАМЕТР

**Ручная настройка Kdump с помощью engine-config**

1. Отредактируйте конфигурацию kdump с помощью команды engine-config:

# engine-config -s ПАРАМЕТР=значение

ВАЖНО

Параметры файла конфигурации слушателя fence\_kdump должны быть согласованы с изменёнными параметрами, согласно таблице «Параметры конфигурации kdump», см. Раздел 7.6.4.1.

1. Перезапустите службу ovirt-engine:

# systemctl restart ovirt-engine.service

1. Переустановите все хосты, при необходимости активировав параметр **Интеграция** **Kdump** (см. таблицу ниже).

С помощью engine-config можно настроить следующие параметры:

**Таблица 7.10. Параметры конфигурации Kdump**

|  |  |  |  |
| --- | --- | --- | --- |
| **Переменная** | **Описание** | **По умолчанию** | **Примечание** |
| FenceKdumpDestinationAddress | Имена хостов или адреса IP, на которые будут посылаться сообщения fence\_kdump. Если значение отсутствует, используется FQDN диспетчера виртуализации. | Пустая строка (используется FQDN диспетчера виртуализации ) | При изменении значения этого параметра, оно должно соответствовать значению параметра LISTENER\_ADDRESS в конфигурации слушателя fence\_kdump, а все хосты с включённой **Интеграцией kdump** должны быть переустановлены. |
| FenceKdumpDestinationPort | Указывает порт, на который необходимо посылать сообщения fence\_kdump. | 7410 | При изменении значения этого параметра, оно должно соответствовать значению параметра LISTENER\_PORT в конфигурации слушателя fence\_kdump, а все хосты с включённой **Интеграцией kdump** должны быть переустановлены. |
| FenceKdumpMessageInterval | Указывает временной интервал (в сек.) между сообщениями, посылаемыми fence\_kdump. | 5 | При изменении значения этого параметра, он должен быть равен (или быть меньше) половинному значению параметра KDUMP\_FINISHED\_TIMEOUT в файле конфигурации слушателя fence\_kdump, а все хосты с включённой **Интеграцией kdump** должны быть переустановлены. |
| FenceKdumpListenerTimeout | Определяет максимальный период ожидания (в сек.) после последнего периодического сигнала, в течение которого слушатель fence\_kdump ещё считается работающим. | 90 | При изменении значения этого параметра, он должен быть равен (или быть больше) половинному значению параметра HEARTBEAT\_INTERVAL в файле конфигурации слушателя fence\_kdump. |
| KdumpStartedTimeout | Определяет максимальный период ожидания (в сек.) до первого получения сообщения от хоста, выполняющего kdump (для определения того, что процедуры kdump начали выполняться). | 30 | При изменении значения этого параметра, он должен быть равен (или быть больше) двойному значению параметра SESSION\_SYNC\_INTERVAL в файле конфигурации слушателя fence\_kdump и параметра FenceKdumpMessageInterval. |

### 7.6.5. Мягкая блокада хостов

Иногда, в связи с неожиданными проблемами, хосты могут перестать отвечать, но, несмотря на то, что VDSM бывает не в состоянии ответить на запрос, виртуальная машина, зависящая от VDSM, остаётся работающий и доступной. В таких ситуациях перезапуск VDSM возвращает ему возможность отвечать на запросы и разрешает проблему.

Мягкая блокада (огораживание) с использованием SSH — это процесс, во время которого диспетчер виртуализации пытается перезапустить VDSM на не отвечающем хосте с помощью протокола SSH. В случае неудачи ответственность за проведение операции блокады падает на внешнего агента огораживания, если он ранее был настроен.

Мягкое огораживание с помощью SSH выполняется следующим образом: на хосте должна быть настроена и включена возможность проведения операции блокады, а также должен существовать действительный хост-прокси (второй хост, имеющий статус «запущен», в том же дата-центре). При истечении времени ожидания подключения между диспетчером виртуализации и хостом происходит следующее:

1. При первом сбое сети статус хоста меняется на «идёт подключение».
2. Далее диспетчер виртуализации выполняет три попытки запросить у VDSM его статус или же ждёт в течение временнòго интервала, определённого загрузкой хоста. Формула определения этого интервала настраивается с помощью значений TimeoutToResetVdsInSeconds (по умолчанию 60 сек.) + [DelayResetPerVmInSeconds (по умолчанию 0.5 сек.)]x(число выполняющихся на хосте ВМ) + [DelayResetForSpmInSeconds (по умолчанию 20 сек.)] x 1 (если хост выполняет роль SPM) или 0 (если хост не выполняет роль SPM). Чтобы дать VDSM максимальное время на ответ, диспетчер виртуализации выбирает наибольший из двух вышеупомянутых параметров (три попытки определить статус VDSM или же интервал, рассчитанный по формуле выше).
3. Если по истечении интервала хост по-прежнему не отвечает, с использованием протокола SSH выполняется команда vdsm restart.
4. Если команда vdsm restart не сможет восстановить соединение между хостом и диспетчером виртуализации, то статус хоста меняется на «не отвечает» и, в случае, если было настроено управление питанием, выполнение операции блокады передаётся внешнему агенту.

ВНИМАНИЕ

Мягкое огораживание с помощью SSH может выполняться для хостов без настроенного управления питанием. Эта операция отличается от обычного огораживания, которое может выполняться только для хостов с настроенным управлением питанием.

### 7.6.6. Использование возможностей хоста по управлению питанием

При настроенном на хосте управлении питанием, получить доступ к некоторому числу параметров управления питанием можно через интерфейс портала администрирования. Хотя каждое устройство управления питанием обладает своими настраиваемыми параметрами, все они поддерживают базовые возможности запуска, останова и перезапуска хоста.

**Использование возможностей хоста по управлению питанием**

1. Нажмите **Вычисления → Хосты** и выберите хост.
2. Раскройте выпадающее меню и выберите одну из следующих возможностей **Управления питанием**:
   * **Перезапустить**: этот параметр останавливает работу хоста, пока статус хоста не сменится на Не запущен. После того, как агент удостоверился в том, что хост не запущен, высокодоступные ВМ перезапускаются на другом хосте в кластере. Затем агент перезапускает хост. Статус готового к использованию хоста затем изменяется на Запущен.
   * **Запустить**: этот параметр запускает хост и даёт ему присоединиться к кластеру. Статус готового к использованию хоста затем изменяется на Запущен.
   * **Остановить**: этот параметр выключает питание хоста. Перед тем, как использовать этот параметр, убедитесь в том, что ВМ, выполняющиеся на хосте, уже мигрировали на другие хосты в кластере. В противном случае случится аварийное прерывание работы этих ВМ, и на другом хосте будут перезапущены только высокодоступные ВМ. После остановки хоста, его статус изменяется на В нерабочем состоянии.

ВНИМАНИЕ

Если управление питанием не включено, перезапустить или остановить работу хоста можно выбрав хост, раскрыв выпадающее меню *Управление* и выбрав пункт *Управление SSH*, *Перезапустить* или *Остановить*.

ВАЖНО

Если на хосте было настроено два агента операции блокады, их можно использовать по очереди или параллельно. В случае параллельных агентов, для остановки хоста нужно, чтобы оба агента ответили на команду *Остановить*; а когда один из агентов ответит на команду *Запустить*, хост начнёт работу. В случае последовательных агентов, для остановка или запуска хоста сначала используется первичный агент; в случае его сбоя используется вторичный агент.

1. Нажмите **OK**.

### 7.6.7. Ручное огораживание или изолирование неотвечающего хоста

В случае, если хост внезапно перестанет отвечать, например, по причине аппаратного сбоя, то это может значительно повлиять на производительность окружения. В случае отсутствия устройства управления питанием или в случае некорректной настройки такого устройства, хост можно перезапустить вручную.

ПРЕДУПРЕЖДЕНИЕ

Используйте параметр *Подтвердить, что хост был перезагружен* только в случае, если хост был перезагружен вручную. Использование этого параметра во время работы хоста может привести к повреждению образа ВМ.

**Ручное огораживание или изолирование неотвечающего хоста**

1. На портале администрирования нажмите Вычисления → Хосты и убедитесь в том, что хост действительно имеет статус Не отвечает.
2. Перезагрузите хост вручную. Это может означать физическое взаимодействие с аппаратурой непосредственно в серверной.
3. На портале администрирования выберите хост и нажмите **Больше действий** (), а затем — **Подтвердить, что хост был перезагружен**.
4. Отметьте галочкой пункт **Одобрить действие** и нажмите **OK**.
5. Если перезагрузка хоста занимает необычно много времени, можно настроить параметр ServerRebootTimeout, чтобы указать, сколько секунд должно длиться ожидание перед тем, как хост получит статус Не отвечает:

# engine-config --set ServerRebootTimeout=целое\_число

# Глава 8. Хранилища

Система виртуализации Red Hat использует централизованную систему хранилищ для виртуальных дисков, файлов ISO и снимков. Реализовать сеть хранения можно с помощью:

* Сетевой файловой системы NFS
* Экспортов GlusterFS
* Других POSIX-совместимых ФС
* Интерфейса iSCSI
* Локальных хранилищ, присоединённых непосредственно к хостам виртуализации
* Протокола Fibre Channel (FCP)
* Параллельного доступа с помощью pNFS

Настроенное хранилище является предварительным условием для создания дата-центра, поскольку дата-центр невозможно инициализировать до тех пор, пока не будут присоединены и активированы домены хранилищ.

В обязанности администраторов систем виртуализации Red Hat входит создание, настройка, присоединение и поддержка хранилищ виртуализированных предприятий. Необходимо иметь представление о типах хранилищ и случаях их использования.

Для добавления доменов хранилищ необходим рабочий доступ на портал администрирования, а также как минимум один подключённый хост со статусом **Запущен**.

В системе виртуализации Red Hat есть три типа доменов хранилищ:

* **Домен данных**: в доменах данных хранятся виртуальные жёсткие диски и файлы OVF всех ВМ и шаблонов в дата-центре. Кроме того, в доменах данных хранятся снимки ВМ.

Домены данных не могут быть общими для разных дата-центров. Домены данных нескольких типов (iSCSI, NFS, FC, POSIX и Gluster) могут быть добавлены в один дата-центр при условии, что они являются разделяемыми, а не локальными.

Домен данных необходимо присоединить к дата-центру перед тем, как присоединять к дата-центру домены других типов.

* **Домен ISO:** в доменах ISO хранятся файлы образов ISO (или логические носители CD), используемые для установки и загрузки операционных систем и приложений виртуальных машин. Наличие домена ISO отменяет необходимость физических носителей для дата-центров. Домен ISO может быть общим для разных дата-центров. Домены ISO могут создаваться только на базе NFS. К дата-центру может быть присоединён только один домен ISO.
* **Домен экспорта:** домены экспорта — это временные репозитории хранения, используемые для копирования и перемещения образов между дата-центрами и окружениями виртуализации Red Hat. Домен экспорта можно использовать для создания резервных копий ВМ. Домен экспорта можно перемещать между дата-центрами, но он может быть активным одновременно только в одном из дата-центров. Домены экспорта можно создавать только на базе NFS. К дата-центру может быть присоединён только один домен экспорта.

ВНИМАНИЕ

Домены хранилищ экспорта являются устаревшими. Домены хранилищ данных можно отсоединить от дата-центра и импортировать в другие дата-центры в том же или в другом окружении. Затем, виртуальные машины, «плавающие» виртуальные диски и шаблоны можно загрузить из домена хранения в прикреплённый дата-центр. Сведения об импорте доменов хранилищ смотрите в Разделе 8.7.

ВАЖНО

Начинайте настройку и присоединение хранилищ к окружению виртуализации Red Hat только после того, как были определены требования к хранилищам со стороны дата-центров.

## 8.1. Что такое домены хранилищ

Домен хранилищ — это собрание образов, имеющих общий интерфейс хранения. Домен хранилищ содержит полные образы шаблонов и ВМ (включая снимки), или файлов ISO. Домен хранилища может быть создан на базе блочных устройств (SAN - iSCSI или FCP) или файловых систем (NAS - NFS, GlusterFS, или других POSIX-совместимых ФС).

В NFS все виртуальные диски, шаблоны и снимки являются файлами.

В SAN (iSCSI/FCP) каждый виртуальный диск, шаблон или снимок является логическим томом. Блочные устройства собираются в логическую сущность, называемую «группой томов», а затем разделяются диспетчером логических томов (Logical Volume Manager, LVM) на логические тома для использования их в качестве виртуальных жёстких дисков.

Виртуальные диски могут иметь два формата: QCOW2 или RAW. Тип хранилища может быть разреженный (тонкое резервирование) или предварительно выделенный. Снимки всегда имеют разреженный тип, но могут быть сделаны для дисков любого формата из двух форматов.

ВМ, разделяющие один и тот же домен хранилища, могут мигрировать между хостами в одном кластере.

# 8.2. Подготовка и добавление хранилища NFS

### 8.2.1. Подготовка хранилища NFS

Создайте общие ресурсы NFS в хранилище файлов или на удалённом сервере в качестве доменов хранилищ в системах хостов виртуализации Red Hat. После экспорта этих общих ресурсов в удалённое хранилище и настройки их конфигурации в виртуализированном ЦУ, они будут автоматически импортированы на хосты виртуализации.

Сведения о настройке NFS <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/Storage_Administration_Guide/index.html#ch-nfs>

Сведения об экспорте общих ресурсов NFS <https://access.redhat.com/solutions/113593>

Для того, чтобы виртуализированный ЦУ мог хранить данные в доменах хранилищ, представленных экспортированными каталогами, необходимы специальные системные учётные записи пользователей и системные группы пользователей. В нижеследующей последовательности действий описывается настройка прав доступа для одного каталога. Шаги с использованием chown и chmod необходимо повторить для каждого каталога, который планируется использовать в качестве доменов хранилищ в системе виртуализации Red Hat.

**Последовательность действий**

1. Создайте группу kvm:

# groupadd kvm -g 36

1. Создайте пользователя vdsm в группе kvm:

# useradd vdsm -u 36 -g 36

1. Укажите 36:36, что даст владельцев vdsm:kvm для экспортированного каталога:

# chown -R 36:36 /exports/data

1. Измените режим доступа к каталогу так, чтобы владелец имел доступ на чтение и запись, а группа и другие пользователи имели доступ на чтение и выполнение:

# chmod 0755 /exports/data

### 8.2.2. Добавление хранилища NFS

В данной последовательности шагов показывается, как присоединить существующее хранилище NFS к окружению виртуализации Red Hat в качестве домена данных.

При необходимости использовать домен экспорта или домен ISO, используйте эти же действия, но в списке **Функция домена** выбирайте **ISO** или **Экспорт**.

**Последовательность действий**

1. На портале администрирования выберите **Хранилище → Домены**.
2. Нажмите **Добавить домен**.
3. Укажите **Название** домена хранилища.
4. Примите значения по умолчанию для списков **Дата-центр**, **Функции домена**, **Тип хранилища**, **Формат** и **Хосты**.
5. Введите **Путь экспорта**, используемый для домена хранилища. Путь 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. Опционально, можно настроить следующие параметры:
   1. Нажмите **Дополнительные параметры**.
   2. В поле **Индикатор предупреждения о недостатке места** введите процентное значение. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупредительное сообщение, и событие будет занесено в журнал.
   3. В поле **Блокировщик действия при критической нехватке места** введите значение в Гбайт. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого значения, пользователю будет показано сообщение об ошибке, событие будет занесено в журнал, а любое новое действие, которому необходимо дисковое пространство, даже временное, будет блокировано.
   4. Отметьте галочкой пункт **Очистить после удаления**. Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя.
7. Нажмите **OK**.

Новый домен данных NFS будет иметь статус **Заблокировано** до тех пор, пока не будет подготовлен диск. Затем домен будет автоматически подключён к дата-центру.

### 8.2.3. Увеличение объёма хранилища NFS

Для увеличения объёма хранилища NFS можно либо создать новый домен хранилища и добавить его в существующий дата-центр, либо увеличить доступный объём на сервере NFS. Информацию для первого варианта можно найти в Разделе 8.2.2, а в последовательности действий, описанной ниже, указывается, как увеличить доступное место на существующем сервере NFS.

**Увеличение существующего домена хранилища NFS**

1. Нажмите Хранилище → Домены.
2. Нажмите на название существующего домена NFS, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Дата-центр** и нажмите **Обслуживание**, чтобы перевести домен хранилищ в режим обслуживания. Это действие отмонтирует существующий общий ресурс и даст возможность изменить размер домена хранилища.
4. Измените размер хранилища на сервере NSF. Для Red Hat Enterprise Linux 7 см. <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/Storage_Administration_Guide/index.html#s2-disk-storage-parted-resize-part>
5. В подробном просмотре перейдите на вкладку **Дата-центр** и нажмите **Активировать** для того, чтобы смонтировать домен хранилища.

# 8.3. Подготовка и добавление локального хранилища

### 8.3.1. Подготовка локального хранилища

Локальный домен хранилища можно настроить на хосте. При настройке локального хранилища на хосте, хост автоматически добавляется в новый дата-центр и кластер, состоящий из одного хоста. Кластеры, состоящие из множества хостов, требуют, чтобы у каждого хоста имелся доступ ко всем доменам хранилищ, что невозможно в случае локального хранилища. Виртуальные машины, созданные в однохостовом кластере, не могут мигрировать, их нельзя огородить или добавить в планирование.

ВАЖНО

На хостах виртуализации локальные хранилища всегда должны настраиваться на файловой системе, отделённой от / (root). Для предотвращения потенциальных потерь данных во время обновления версий ПО, рекомендуется использовать отдельный логический том.

**Подготовка локального хранилища на стандартных хостах**

1. Создайте каталог, который будет использоваться как локальное хранилище:

# mkdir -p /data/images

1. Убедитесь в том, что пользователь **vdsm** (UID 36) и группа **kvm** (GID 36) имеют права на чтение/запись: в этом каталоге:

# chown 36:36 /data /data/images

# chmod 0755 /data /data/images

**Подготовка локального хранилища на хостах виртуализации**

Рекомендуется создать локальное хранилище на логическом томе следующим образом:

1. Создайте каталог локального хранилища:

# mkdir /data

# lvcreate -L $SIZE rhvh -n data

# mkfs.ext4 /dev/mapper/rhvh-data

# echo "/dev/mapper/rhvh-data /data ext4 defaults,discard 1 2" >> /etc/fstab

# mount /data

1. Смонтируйте новое локальное хранилище и затем измените права доступа и владельца:

# mount -a

# chown 36:36 /data /rhvh-data

# chmod 0755 /data /rhvh-data

### 8.3.2. Добавление локального хранилища

Добавление локального хранилища помещает хост в новый дата-центр и кластер. В окне параметров локального хранилища в одной последовательности действий соединено создание дата-центра, кластера и хранилища.

**Последовательность действий**

1. Нажмите Вычисления → Хосты и выберите хост.
2. Нажмите Управление → Обслуживание и нажмите OK.
3. Нажмите Управление → Настроить локальное хранилище.
4. Нажмите на кнопки **Изменить** рядом с полями **Дата-центр**, **Кластер** и **Хранилище**, чтобы именовать и настроить домен локального хранилища.
5. В текстовом поле укажите путь до локального хранилища.
6. Там где это применимо, перейдите на вкладку **Оптимизация** для настройки политики оптимизации памяти для нового кластера локального хранилища.
7. Нажмите **OK**.

Хост присоединится к сети в своём собственном дата-центре.

# 8.4. Подготовка и добавление хранилища на базе совместимой с POSIX файловой системы

### 8.4.1. Подготовка хранилища на базе совместимой с POSIX файловой системы

Поддержка файловой системы стандарта POSIX даёт возможность монтировать файловые системы с теми же самыми параметрами монтирования, которые обычно применяются при ручном монтировании из командной строки. Назначение этой возможности — возможность доступа к хранилищам, не подверженного потенциальным угрозам, возникающим при использовании NFS, iSCSI или FCP.

Любая совместимая с POSIX файловая система, используемая в качестве домена хранилища в системе виртуализации Red Hat, должна быть кластерной, например, Global File System 2 (GFS2), а также должна поддерживать разреженные файлы и прямой ввод-вывод. К примеру, файловая система CIFS (Common Internet File System) не поддерживает механизм прямого ввода-вывода, что делает её несовместимой с системой виртуализации Red Hat.

Сведения о том, как установить и настроить хранилище на базе ФС, совместимой со стандартом POSIX, см. <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/Global_File_System_2/index.html>

ВАЖНО

*Не монтируйте* хранилище NFS, создавая домен хранилища на базе POSIX-совместимой ФС. Всегда создавайте для этого домен хранилища NFS.

### 8.4.2. Добавление хранилища на базе файловой системы, совместимой с POSIX

В данной процедуре описывается, как присоединить существующее хранилище на базе POSIX-совместимой ФС к среде виртуализации Red Hat в качестве домена данных.

**Последовательность действий**

1. Нажмите Хранилище → Домены.
2. Нажмите **Добавить домен**.
3. Введите **Название домена** хранилища.
4. Выберите **Дата-центр**, связанный с доменом хранилища. Выбранный ДЦ должен иметь тип **POSIX (POSIX-совместимая ФС)**. Как вариант, выберите (нет).
5. В выпадающем списке **Функция домена** выберите Данные, а в списке **Тип хранилища** выберите POSIX-совместимая ФС.

Там, где применимо, в выпадающем списке выберите **Форматировать**.

1. В выпадающем списке выберите **Хост**.
2. Укажите **Путь** до POSIX-совместимой ФС так, как обычно он указывается при выполнении команды mount.
3. Укажите **Тип VFS** так, как обычно он указывается при выполнении команды mount с аргументом –t. Список действительных типов VFS смотрите в выводе man mount.
4. Укажите дополнительные **Параметры mount** так, как обычно он указывается при выполнении команды mount с аргументом –o. Параметры монтирования должны указываться в виде списка, разделённого запятыми. Список действительных параметров смотрите в выводе man mount.
5. Опционально, можно настроить дополнительные параметры.
   1. Нажмите **Дополнительные параметры**.
   2. В поле **Индикатор предупреждения о недостатке места** введите процентное значение. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупредительное сообщение, и событие будет занесено в журнал.
   3. В поле **Блокировщик действия при критической нехватке места** введите значение в Гбайт. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого значения, пользователю будет показано сообщение об ошибке, событие будет занесено в журнал, а любое новое действие, которому необходимо дисковое пространство, даже временное, будет блокировано.
   4. Отметьте галочкой пункт **Очистить после удаления**. Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя.
6. Нажмите **OK**.

# 8.5. Подготовка и добавление блочного хранилища

### 8.5.1. Подготовка хранилища iSCSI

Система виртуализации Red Hat поддерживает хранилища iSCSI, который представляет собой домен хранилища из группы томов на базе LUN. Группы томов и номера LUN нельзя присоединить более чем к одному домену хранилищ одновременно.

Сведения об установке и настройке хранилища iSCSI см. <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/storage_administration_guide/#online-storage-management>

ВАЖНО

При использовании блочного хранилища и планировании размещения ВМ на устройствах raw или прямых LUN под управлением диспетчера логических томов, необходимо создать фильтр для скрытия гостевых логических томов. Это предотвратит активацию гостевых томов при загрузке хоста, что может привести к устареванию данных томов и далее к повреждению данных. Подробности: <https://access.redhat.com/solutions/2662261>

ВАЖНО

Система виртуализации Red Hat на данный момент не поддерживает хранилища с размером блоков в 4Мбайт. Блочные хранилища необходимо настраивать в старом режиме (512Кбайт на блок).

ВАЖНО

В ситуации, когда хост загружается из хранилища SAN и теряет связь с хранилищем, файловые системы хранилища становятся доступны только для чтения и остаются в этом состоянии после восстановления связи.

Для предотвращения этой ситуации мы рекомендуем добавить в корневую ФС SAN замещающий конфигурационный файл доступа по нескольким путям к загрузочным LUN, для обеспечения постановки их в очередь при наличии соединения:

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

multipaths {

multipath {

wwid wwid\_загрузочного\_LUN

no\_path\_retry queue

}

### 8.5.2. Добавление хранилища iSCSI

С помощью этих действий существующее хранилище iSCSI присоединяется к среде виртуализации в качестве домена данных.

**Последовательность действий**

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

ВАЖНО

Подключение к домену хранилища идёт от выбранного хоста, а не напрямую из виртуализированного ЦУ, поэтому до того, как можно будет настроить домен хранилищ, у всех хостов должен иметься доступ к устройству хранения.

1. Виртуализированный ЦУ может отобразить цели iSCSI на номера LUN или номера LUN на цели iSCSI. В окне **Новый домен** при выборе типа хранилища iSCSI автоматически отображаются известные цели с неиспользуемыми LUN. Если цель, используемая для добавления хранилища, отсутствует, её можно найти с помощью обнаружения целей; в противном случае переходите к следующему шагу.
   1. Для активации возможности обнаружения целей нажмите **Обнаружить цели**. После обнаружения целей и авторизации на них, в окне **Новый домен** автоматически будут показаны цели с неиспользуемыми в окружении LUN.

ВНИМАНИЕ

Также показываются LUN, используемые вне окружения.

Параметр **Обнаружить цели** можно использовать для добавления LUN ко многим целям или нескольких путей к одним и тем же LUN.

* 1. В поле **Адрес** введите полное доменное имя или адрес IP хоста iSCSI.
  2. В поле **Порт** укажите номер порта, к которому будет подключаться хост при просмотре целей. Значение по умолчанию — 3260.
  3. Если для защиты хранилища используется CHAP, отметьте галочкой пункт **Аутентификация пользователей**. Введите **Имя пользователя CHAP** и **Пароль CHAP**.

ВНИМАНИЕ

Настроить учётные записи цели iSCSI для конкретного хоста можно с помощью REST API. Подробности смотрите в [Руководстве для REST API](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/rest_api_guide/services#services-storage_server_connection_extensions-methods-add) (Англ.)

* 1. Нажмите **Обнаружить**.
  2. Выберите одну или более целей из результатов обнаружения и нажмите **Авторизация** для одной цели или **Авторизоваться на всех** для нескольких целей.

ВАЖНО

Если для доступа требуется более одного пути, необходимо обнаружить и провести авторизацию на цели с использованием всех путей. Изменение домена хранилища для добавления дополнительных путей на данный момент не поддерживается.

1. Нажмите на кнопку **+** рядом с нужной целью. Элемент раскроется и будут показаны все неиспользуемые LUN, присоединённые к цели.
2. Отметьте галочкой каждый LUN, используемый для создания домена хранилища.
3. Опционально, можно настроить дополнительные параметры.
   1. Нажмите **Дополнительные параметры**.
   2. В поле **Индикатор предупреждения о недостатке места** введите процентное значение. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупредительное сообщение, и событие будет занесено в журнал.
   3. В поле **Блокировщик действия при критической нехватке места** введите значение в Гбайт. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого значения, пользователю будет показано сообщение об ошибке, событие будет занесено в журнал, а любое новое действие, которому необходимо дисковое пространство, даже временное, будет блокировано.
   4. Отметьте галочкой пункт **Очистить после удаления**. Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя
4. Нажмите **OK**.

Если к одной цели было настроено несколько соединений из хранилищ, то для завершения создания связки iSCSI следуйте пошаговой инструкции в Разделе 8.5.3.

Если текущая сеть хранилища должна мигрировать в связку iSCSI, смотрите Раздел 8.5.4.

### 8.5.3. Настройка доступа к iSCSI по нескольким путям

Доступ к iSCSI по нескольким путям даёт возможность создания и управления группами логических сетей и подключений к хранилищу iSCSI. Конфигурация нескольких сетевых путей от хоста до хранилища iSCSI предохраняет хост от простоя во время потенциального сбоя сетевого пути.

С помощью сетевых карт или виртуальных LAN, присвоенных логическим путям в связке iSCSI, виртуализированный ЦУ подключает каждый хост в дата-центре к каждой из целей.

В целях избыточности, связку iSCSI можно создать с помощью нескольких целей и логических сетей.

**Предварительные условия**

* Одна или более целей iSCSI (Раздел 8.5.2)
* Одна или более логических сетей (Раздел 6.1.2), отвечающих следующим требованиям:
  + Не является требуемой сетью или сетью виртуальной машины (Раздел 8.5.4)
  + Сеть присвоена интерфейсу хоста (Раздел 6.4.2)
  + Сети присвоен статический адрес IP в той же VLAN и подсети, в которой размещаются другие логические сети в связке iSCSI. (Раздел 6.4.2)

**Последовательность действий**

1. Нажмите Вычисления → Дата-центры
2. Нажмите на имя дата-центра, чтобы перейти к подробному просмотру.
3. На вкладке **Доступ к iSCSI по нескольким путям** нажмите **Добавить**.
4. В окне **Добавить связку iSCSI** укажите **Название** и **Описание**.
5. Выберите логическую сеть из списка **Логические сети** и домен хранилища из **Таргеты хранилища**. Все пути до одной и той же цели должны быть выбраны.
6. Нажмите **OK**.

Хосты в дата-центре подключены к целям iSCSI с помощью логических сетей в связке iSCSI.

### 8.5.4. Миграция логической сети в связку iSCSI

При наличии логической сети, созданной для передачи трафика iSCSI и настроенной поверх существующей сетевой связки (Раздел 6.5), её можно перенести в связку iSCSI в той же подсети с нулевым временем простоя и без сбоев.

**Последовательность действий**

1. Измените текущую логическую сеть так, чтобы она не была **Требуемой**:
   1. Нажмите Вычисления → Кластеры.
   2. Нажмите на название кластера, чтобы перейти к подробному просмотру.
   3. Во вкладке Логические сети выберите текущую логическую сеть (net-1) и нажмите **Управление сетями**.
   4. Снимите галочку с пункта **Требуется** и нажмите **OK**.
2. Создайте новую логическую сеть, не являющуюся **Требуемой** и не являющуюся **Сетью ВМ**:
   1. Нажмите Добавить сеть, чтобы открыть окно **Новая логическая сеть**.
   2. Во вкладке **Общие** введите **Название** (net-2) и снимите отметку с пункта **Сеть ВМ**.
   3. Во вкладке **Кластер** снимите галочку с пункта **Требовать** и нажмите **OK**.
3. Удалите текущую сетевую связку и заново присвойте логические сети:
   1. Нажмите Вычисления → Хосты.
   2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
   3. Во вкладке **Сетевые интерфейсы** нажмите **Настроить сети хоста**.
   4. Перетащите сеть net-1 вправо, чтобы заново её присвоить.
   5. Перетащите текущую связку вправо, чтобы удалить её.
   6. Перетащите сети net-1 и net-2 влево, чтобы присвоить их физическим интерфейсам.
   7. Нажмите на значок карандаша рядом с сетью net-2, чтобы открыть окно **Свойства сети**.
   8. Во вкладке **IPV4** выберите **Статический**.
   9. Укажите **IP** и **Сетевую маску/префикс маршрутизации** подсети и нажмите **OK**.
4. Создайте связку iSCSI:
   1. Нажмите Вычисления → Дата-центры .
   2. Нажмите на имя дата-центра, чтобы перейти к подробному просмотру.
   3. Во вкладке **Доступ к iSCSI по нескольким путям** нажмите **Добавить**.
   4. В окне **Добавить связку iSCSI** укажите **Название**, выберите сети, net-1 и net-2, и нажмите **OK**.

В дата-центре теперь есть связка iSCSI, включающая в себя и старую и новую логические сети.

### 8.5.5. Подготовка хранилища FCP

Система виртуализации Red Hat поддерживает хранилище SAN путём создания домена хранилища из группы томов, созданной из ранее существовавших LUN. Ни группы томов, ни номера LUN нельзя присоединить более чем к одному домену хранилища одновременно.

Администраторы системы виртуализации Red Hat должны иметь практические знания о теории и принципах работы сетей хранения данных (SAN). Как правило, для переноса трафика между хостом и общим внешним хранилищем SAN используют протокол FCP. В связи с этим SAN иногда называют «хранилища FCP».

ВАЖНО

При использовании блочного хранилища и планировании размещения ВМ на устройствах raw или прямых LUN под управлением диспетчера логических томов, необходимо создать фильтр для скрытия гостевых логических томов. Это предотвратит активацию гостевых томов при загрузке хоста, что может привести к устареванию данных томов и далее к повреждению данных. Подробности: <https://access.redhat.com/solutions/2662261>

ВАЖНО

Система виртуализации Red Hat на данный момент не поддерживает хранилища с размером блоков в 4Мбайт. Блочные хранилища необходимо настраивать в старом режиме (512Кбайт на блок).

ВАЖНО

В ситуации, когда хост загружается из хранилища SAN и теряет связь с хранилищем, файловые системы хранилища становятся доступны только для чтения и остаются в этом состоянии после восстановления связи.

Для предотвращения этой ситуации мы рекомендуем добавить в корневую ФС SAN замещающий конфигурационный файл доступа по нескольким путям к загрузочным LUN, для обеспечения постановки их в очередь при наличии соединения:

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

multipaths {

multipath {

wwid wwid\_загрузочного\_LUN

no\_path\_retry queue

}

### 8.5.6. Добавление хранилища FCP

В данной последовательности действий показывается, как присоединить существующее хранилище FCP к середе виртуализации Red Hat в виде домена данных.

**Последовательность действий**

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

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

1. В выпадающих списках выберите **Функцию домена** и **Тип хранилища**. Типы доменов хранилища, несовместимые с выбранным дата-центром, не будут доступны.
2. В поле **Хост** выберите активный хост. Если этот домен данных не первый в этом дата-центре, необходимо выбрать хост-SPM дата-центра.

ВАЖНО

Подключение к домену хранилища идёт через выбранный хост, а не напрямую из виртуализированного ЦУ. В системе должен существовать как минимум один активный хост, присоединённый к выбранному дата-центру. До начала настройки домена хранилища у всех хостов должен быть доступ к устройству хранения.

1. При выборе типа хранилища **Оптоволокно**, в окне **Новый домен** автоматически показываются известные цели с неиспользуемыми LUN. Отметьте галочкой пункт **LUN ID**, чтобы выбрать все доступные LUN.
2. Опционально, можно настроить дополнительные параметры.
   1. Нажмите **Дополнительные параметры**.
   2. В поле **Индикатор предупреждения о недостатке места** введите процентное значение. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупредительное сообщение, и событие будет занесено в журнал.
   3. В поле **Блокировщик действия при критической нехватке места** введите значение в Гбайт. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого значения, пользователю будет показано сообщение об ошибке, событие будет занесено в журнал, а любое новое действие, которому необходимо дисковое пространство, даже временное, будет блокировано.
   4. Отметьте галочкой пункт **Очистить после удаления**. Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя
3. Нажмите **OK**.

Во время подготовки к использованию, домен данных FCP будет иметь статус Заблокировано. Когда домен будет готов, он автоматически присоединится к дата-центру.

### 8.5.7. Увеличение размера хранилища iSCSI или FCP

Есть несколько способов увеличения объёма хранилища iSCSI или FCP:

* Добавление в текущий домен хранения существующего LUN.
* Создать новый домен с новыми LUN, и добавить его в существующий дата-центр. Смотрите Раздел 8.5.2.
* Расширить домен хранения, изменив размер базовых LUN.

В нижеследующей последовательности шагов объясняется, как расширить хранилище сети хранения данных (SAN) при помощи добавления нового номера LUN в существующий домен хранения.

**Предварительные условия**

* Домен хранилища должен иметь статус Запущен.
* Все хосты со статусом Запущен должны иметь доступ к LUN, в противном случае действие закончится неудачей, и LUN не будет добавлен в домен. Хосты, тем не менее, не будут затронуты. Если недавно добавленный хост, или хост, выходящий из режима обслуживания или из статуса В нерабочем состоянии, не будет иметь доступа к LUN, то такой хост получит статус В нерабочем состоянии.

**Увеличение размера существующего хранилища iSCSI или FCP**

1. Нажмите Хранилище → Домены и выберите домен iSCSI or FCP
2. Нажмите **Управление доменом**.
3. Нажмите **Таргеты > LUN** и нажмите на кнопку расширения **Обнаружить таргеты**.
4. Укажите сведения о подключении для сервера хранилища и нажмите **Обнаружить** для инициации подключения.
5. Нажмите **Таргеты > LUN** и отметьте галочкой новый доступный LUN.
6. Нажмите OK, чтобы добавить LUN в выбранный домен хранилищ.

Данное действие увеличит домен хранения на размер добавленного LUN.

При расширении домена хранилищ с помощью изменения размера базовых LUN, информация об этих LUN также должна быть обновлена на портале администрирования.

**Обновление информации о размере LUN**

1. Нажмите Хранилище → Домены и выберите домен iSCSI или FCP
2. Нажмите **Управление доменами**.
3. Нажмите **LUN > Таргеты**.
4. В столбце **Дополнительный размер** нажмите на кнопку **Добавить** *дополнительный\_размер\_хранилища* для обновления информации о LUN.
5. Нажмите **OK** чтобы LUN отображал новый размер хранилища.

### 8.5.8. Повторное использование LUN

Для создания домена хранилища или виртуального диска номера LUN не могут быть повторно использованы в их текущем состоянии. При попытке повторно использовать LUN, портал администрирования выведет следующее сообщение об ошибке:

Сбой инициализации физического устройства. Убедитесь, что устройство пусто и у хоста есть к нему доступ.

Виртуализированный ЦУ покажет следующую ошибку во время установки:

[ ERROR ] Error creating Volume Group: Failed to initialize physical device: ("[u'/dev/mapper/000000000000000000000000000000000']",)

[ ERROR ] Failed to execute stage 'Misc configuration': Failed to initialize physical device: ("[u'/dev/mapper/000000000000000000000000000000000']",)

Перед повторным использованием LUN необходимо очистить старую таблицу разделов.

**Очистка таблицы разделов от LUN**

ВАЖНО

Это действие необходимо выполнить для корректного LUN во избежание непреднамеренного повреждения данных.

Выполните команду dd с указанием идентификатора LUN, который необходимо использовать повторно, максимального числа байтов для одновременного чтения и записи и число копируемых входных блоков:

# dd if=/dev/zero of=/dev/mapper/LUN\_ID bs=1M count=200 oflag=direct

# 8.6. Подготовка и добавление хранилища Gluster

### 8.6.1. Подготовка хранилища Gluster

Раздел полностью состоит из ссылок на внешние документы.

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>.

### 8.6.2. Добавление хранилища Gluster

To use Red Hat Gluster Storage with Red Hat Virtualization, see [Configuring Red Hat Virtualization with Red Hat Gluster Storage](https://access.redhat.com/documentation/en-us/red_hat_gluster_storage/3.4/html/configuring_red_hat_virtualization_with_red_hat_gluster_storage/).

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

# 8.7. Импорт существующих доменов хранилищ

### 8.7.1. Общий обзор процесса импорта существующих доменов хранилищ

Кроме добавления новых доменов хранилищ, не содержащих данных, можно импортировать уже существующие и получать доступ к хранящимся в них данным. С помощью импорта домена хранилища можно восстанавливать данные после сбоев в базе данных виртуализированного ЦУ, а также переносить данные из одного дата-центра или окружения в другое.

Ниже приводится общий обзор процесса импорта каждого из типов доменов хранилищ:

**Данные**

Импорт существующего домена хранения данных даёт доступ ко всем ВМ и шаблонам, хранящимся в этом домене. После импорта домена необходимо вручную импортировать ВМ, образы плавающих дисков и шаблоны в целевой дата-центр. Процесс импорта ВМ и шаблонов, хранящихся в домене хранения данных, аналогичен процессу экспорта домена хранилищ. Но, поскольку домены хранения данных содержат все ВМ и шаблоны указанного дата-центра, импорт доменов хранения данных рекомендуется в целях восстановления данных или при масштабных миграциях ВМ между дата-центрами или окружениями.

ВАЖНО

Импорт существующих доменов хранения данных, присоединённых к дата-центрам, возможен при корректном поддерживаемом уровне совместимости. Подробности см. <https://access.redhat.com/solutions/4303801>

**ISO**

Импорт существующего домена хранения ISO даёт доступ ко всем файлам ISO и виртуальным дискетам, хранящимся в этом домене. После завершения процесса импорта, для доступа к этим ресурсам не требуется дополнительных действий; их можно присоединять к виртуальным машинам по требованию.

**Экспорт**

Импорт существующего домена хранения экспорта даёт доступ ко всем образам ВМ и шаблонам, хранящимся в домене. Поскольку домены экспорта созданы для экспорта и импорта образов ВМ и шаблонов, импорт доменов хранения экспорта рекомендуется при небольших миграциях ВМ и шаблонов внутри окружения или между окружениями. Сведения об экспорте и импорте ВМ и шаблонов в и из доменов хранения экспорта см. <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/virtual_machine_management_guide/#sect-Exporting_and_Importing_Virtual_Machines_and_Templates>

ВНИМАНИЕ

Домены хранилищ экспорта являются устаревшими. Домены хранилищ данных можно отсоединить от дата-центра и импортировать в другие дата-центры в том же или в другом окружении. Затем, виртуальные машины, «плавающие» виртуальные диски и шаблоны можно загрузить из домена хранения в прикреплённый дата-центр.

ПРЕДУПРЕЖДЕНИЕ

После прикрепления домена хранилищ к целевому дата-центру, домен может быть обновлён до нового формата, после чего повторное прикрепление к исходному дата-центру может быть невозможным. Это может нарушить процесс использования доменов данных в качестве замены доменам экспорта.

### 8.7.2. Импорт доменов хранилищ

Импортируйте домен хранилищ, ранее прикреплённый к дата-центру в том же или в другом окружении. Для предотвращения возможного повреждения данных, действие подразумевает, что домен хранения уже не прикреплён ни к одному из дата-центров в любом окружении. Для импорта и прикрепления существующего домена хранилищ к дата-центру, целевой дата-центр должен быть инициализирован.

**Последовательность действий**

1. Нажмите Хранилище → Домены.
2. Нажмите **Импортировать домен**.
3. Выберите **Дата-центр**, в который нужно импортировать домен хранения.
4. Укажите **Название** домена хранения.
5. В выпадающих списках выберите **Функцию домена** и **Тип хранилища**.
6. В выпадающем списке выберите **Хост**.

ВАЖНО

Подключение к домену хранилища идёт через выбранный хост, а не напрямую из виртуализированного ЦУ. В системе должен существовать как минимум один активный хост, присоединённый к выбранному дата-центру. До начала настройки домена хранилища у всех хостов должен быть доступ к устройству хранения.

1. Укажите сведения о домене хранения.

ВНИМАНИЕ

Поля для вода сведений о домене хранилищ изменяются в зависимости от значений, выбранных в списках *Функция домена* и *Тип хранилища*. Эти поля аналогичны полям при добавлении нового домена хранилищ.

1. Отметьте галочкой пункт **Активировать домен в дата-центре**, чтобы активировать домен хранения после присоединения его к выбранному дата-центру.
2. Нажмите **OK**.

Теперь из домена хранения в дата-центр можно импортировать ВМ и шаблоны.

ПРЕДУПРЕЖДЕНИЕ

После прикрепления домена хранилищ к целевому дата-центру домен может быть обновлён до нового формата, после чего повторное прикрепление к исходному дата-центру может быть невозможным. Это может нарушить процесс использования доменов данных в качестве замены доменам экспорта.

**Сопутствующая информация**

* Раздел 8.7.5. Импортирование виртуальных машин из импортированных доменов хранения данных
* Раздел 8.7.6. Импортирование шаблонов из импортированных доменов хранения данных

### 8.7.3. Миграция доменов хранилищ между дата-центрами в одном окружении

Перенесите домен хранилищ из одного дата-центра в другой в рамках окружения виртуализации Red Hat, чтобы целевые дата-центры получили доступ к данным, хранящимся в домене. В действия входит открепление домена хранилища от одного дата-центра и прикрепление к другому дата-центру.

**Последовательность действий**

1. Выключите все ВМ, выполняющиеся в нужном домене хранения.
2. Нажмите Хранилище → Домены.
3. Нажмите на название домена, чтобы перейти к подробному просмотру.
4. Перейдите на вкладку **Дата-центр**.
5. Нажмите **Обслуживание**, а затем нажмите **OK**.
6. Нажмите **Открепить** и затем нажмите **OK**.
7. Нажмите **Прикрепить**.
8. Выберите целевой дата-центр и нажмите **OK**.

Домен хранения прикреплён целевому дата-центру и автоматически активируется. Теперь можно импортировать ВМ и шаблоны из домена хранения в целевой дата-центр.

ПРЕДУПРЕЖДЕНИЕ

После прикрепления домена хранилищ к целевому дата-центру домен может быть обновлён до нового формата, после чего повторное прикрепление к исходному дата-центру может быть невозможным. Это может нарушить процесс использования доменов данных в качестве замены доменам экспорта.

### 8.7.4. Миграция доменов хранилищ между дата-центрами в разных окружениях

Перенесите домен хранилища из одного окружения виртуализации в другое, чтобы целевое окружение получило доступ к данным, хранящимся в домене хранилищ. В данную процедуру входит удаление домена хранилища из одного окружения виртуализации Red Hat и импорт его в другое окружение. Для импорта и присоединения существующего домена хранения данных к дата-центру виртуализации Red Hat , исходный дата-центр домена хранения должен иметь корректный поддерживаемый уровень совместимости. Подробности см. <https://access.redhat.com/solutions/4303801>

**Последовательность действий**

1. Авторизуйтесь на портале администрирования в исходном окружении.
2. Выключите все ВМ, выполняемые в требуемом домене хранения.
3. Нажмите Хранилище → Домены.
4. Нажмите на имя домена хранилища, чтобы перейти к подробному просмотру.
5. Перейдите на вкладку **Дата-центр**.
6. Нажмите **Облуживание**, затем **OK**.
7. Нажмите **Открепить**, затем **OK**.
8. Нажмите **Удалить**.
9. В окне **Удалить хранилище** убедитесь в том, что пункт **Форматировать домен, т.е. содержимое хранилища будет потеряно** не отмечен. Таким образом данные в домене сохраняются для последующего использования.
10. Нажмите OK для удаления домена хранилища из исходного окружения.
11. Авторизуйтесь на портале администрирования целевого окружения.
12. Нажмите Хранилище → Домены.
13. Нажмите **Импортировать домен**.
14. В выпадающем списке **Дата-центр** выберите целевой дата-центр.
15. Введите имя домена хранения.
16. В соответствующих выпадающих списках выберите **Функцию домена** и **Тип хранилища**.
17. Выберите хост в выпадающем списке **Хост**.
18. Укажите сведения о домене хранилища.

ВНИМАНИЕ

Поля для вода сведений о домене хранилищ изменяются в зависимости от значения, выбранного в выпадающем списке *Тип хранилища*. Эти поля аналогичны полям при добавлении нового домена хранилищ.

1. Отметьте галочкой пункт **Активировать домен в дата-центре**, чтобы домен хранилища был активирован автоматически при присоединении.
2. Нажмите **OK**.

Домен хранения присоединён к целевому дата-центру в новом окружении виртуализации Red Hat и активирован автоматически. Теперь из импортированного домена можно импортировать ВМ и шаблоны в целевой дата-центр.

ПРЕДУПРЕЖДЕНИЕ

После прикрепления домена хранилищ к целевому дата-центру домен может быть обновлён до нового формата, после чего повторное прикрепление к исходному дата-центру может быть невозможным. Это может нарушить процесс использования доменов данных в качестве замены доменам экспорта.

### 8.7.5. Импорт виртуальных машин из импортированных доменов хранилищ данных

Импортируйте ВМ в один или более кластеров из домена хранения данных, ранее импортированного в виртуализированное окружение Red Hat. В данной процедуре предполагается, что импортированный домен хранилища данных ранее был прикреплён к дата-центру и был активирован.

**Последовательность действий**

1. Нажмите Хранилище → Домены.
2. Нажмите на имя импортированного домена, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Импорт ВМ**.
4. Выберите одну или более ВМ для импортирования.
5. Нажмите **Импортировать**.
6. Убедитесь, что для каждой ВМ в окне **Импорт ВМ** выбран корректный целевой кластер из списка **Кластер**.
7. Отобразите внешние профили vNIC ВМ на профили, присутствующие в целевом кластере:
   1. Нажмите **Отображение профилей vNIC**.
   2. Выберите используемый профиль vNIC в выпадающем списке **Целевой профиль vNIC**.
   3. Если в окне **Импорт ВМ** было выбрано несколько целевых кластеров, выберите каждый целевой кластер в выпадающем списке **Целевой кластер** и убедитесь в том, что отображения корректны.
   4. Нажмите **OK**.
8. При обнаружении конфликта адресов MAC, рядом с именем ВМ появится восклицательный знак. Наведите курсор на это значок, чтобы просмотреть всплывающую подсказку с возникшей ошибкой.

Отметьте галочкой пункт **Повторно присвоить неправильные MAC**, чтобы повторно присвоить конфликтующие адреса MAC всем проблемным ВМ. Как вариант, можно отметить пункт **Присвоить повторно** для каждой ВМ.

ВНИМАНИЕ

В случае отсутствия доступных адресов для присвоения, операция импорта закончится неудачей. Тем не менее, в случае адресов MAC, расположенных вне диапазона пула адресов MAC кластера, возможен импорт ВМ без присвоения им нового адреса.

1. Нажмите **OK**.

Импортированные ВМ больше не присутствуют в списке во вкладке **Импорт ВМ**.

### 8.7.6. Импорт шаблонов из импортированных доменов хранилищ данных

Импортируйте шаблон из домена хранения данных, ранее импортированного в виртуализированное окружение Red Hat. В данной процедуре предполагается, что импортированный домен хранилища данных ранее был прикреплён к дата-центру и был активирован.

**Последовательность действий**

1. Нажмите Хранилище → Домены.
2. Нажмите на имя импортированного домена, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Импорт шаблонов**.
4. Выберите один или больше шаблонов для импорта.
5. Нажмите **Импортировать**.
6. Убедитесь, что для каждого шаблона в окне **Импорт шаблонов** выбран корректный целевой кластер из списка **Кластер**.
7. Отобразите внешние профили vNIC ВМ на профили, присутствующие в целевом кластере:
   1. Нажмите **Отображение профилей vNIC**.
   2. Выберите используемый профиль vNIC в выпадающем списке **Целевой профиль vNIC**.
   3. Если в окне **Импорт Шаблонов** было выбрано несколько целевых кластеров, выберите каждый целевой кластер в выпадающем списке **Целевой кластер** и убедитесь в том, что отображения корректны.
   4. Нажмите **OK**.
8. Нажмите **OK**.

Импортированные шаблоны больше не присутствуют в списке во вкладке **Импорт шаблонов**.

# 8.8. Задачи при работе с хранилищами

### 8.8.1. Размещение образов в доменах хранения данных

Загрузить образы виртуальных дисков и образы ISO в домен хранения данных можно с помощью портала администрирования или REST API.

ВНИМАНИЕ

Информацию о загрузке образов в домен с помощью REST API ищите в разделах [IMAGETRANSFERS](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/rest_api_guide/#services-image_transfers) и [IMAGETRANSFER](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/rest_api_guide/#services-image_transfer) руководства по REST API (Англ.).

Виртуальные диски, совместимые с QEMU, можно присоединять к виртуальным машинам. Диски должны иметь тип raw или QCOW2. Диски, созданные на базе виртуального диска с типом QCOW2, нельзя сделать общими, а файл виртуального диска с типом QCOW2 не должен иметь резервной копии.

Образы ISO можно присоединять к ВМ в качестве дисков CDROM или использовать для загрузки ВМ.

**Предварительные условия**

Функция отправки в домен использует HTML 5 API, для чего в окружении необходимо иметь следующие компоненты:

* Прокси ввода-вывода изображений (ovirt-imageio-proxy), настроенный с помощью engine-setup.
* Центр сертификации, импортированный в веб-браузер, с помощью которого осуществляется доступ на портал администрирования.

Для импортирования центра сертификации перейдите по адресу https://*адрес\_диспетчера*\_виртуализации/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA и включите все параметры доверия.

* Браузер с поддержкой HTML5, например, Firefox 35, Internet Explorer 10, Chrome 13 и более поздние версии.

**Размещение образа в домене хранения данных**

1. Нажмите Хранилище → Диски.
2. Из меню **Отправить** выберите **Начать**.
3. Нажмите кнопку **Выбрать** **файл** и выберите образ для отправки.
4. Заполните поля **Параметры диска**. Описание соответствующих полей смотрите в Разделе 10.6.2.
5. Нажмите **OK**.

Статус отправки отображается с помощью индикатора выполнения. В меню **Отправка** можно приостановить, отменить или возобновить отправку файлов.

**Увеличение значения времени ожидания отправки**

1. В случае превышения времени ожидания окончания отправки и появлении сообщения **Причина: превышение времени ожидания в связи с неактивностью передачи**, увеличьте значение времени ожидания:

# engine-config -s TransferImageClientInactivityTimeoutInSeconds=6000

1. Перезапустите службу ovirt-engine:

# systemctl restart ovirt-engine

### 8.8.2. Помещение доменов хранения в режим обслуживания

Перед откреплением и удалением доменов хранения их необходимо поместить в режим обслуживания. Это необходимо для присвоения другого домена данных в качестве домена мастер-данных.

ВАЖНО

Домен хранения нельзя переместить в режим обслуживания, если у ВМ имеется аренда в домене. ВМ сначала необходимо выключить, удалить аренду или переместить аренду в другой домен хранения.

Расширение доменов iSCSI с помощью добавления дополнительных LUN можно выполнять только при активном домене.

**Перемещение доменов хранения в режим обслуживания**

1. Выключите все ВМ, выполняющиеся в домене хранилищ.
2. Нажмите Хранилище → Домены.
3. Нажмите на имя домена, чтобы перейти к подробному просмотру.
4. Перейдите на вкладку **Дата-центр**.
5. Нажмите **Обслуживание**.

ВНИМАНИЕ

Пункт Игнорировать сбой обновления OVF даёт возможность перемещать домен хранения в режим обслуживания даже при сбое обновления OVF.

1. Нажмите **OK**.

Домен хранения деактивируется и в списке результатов получает статус Неактивен. Теперь неактивные домены хранения можно изменять, отключать, удалять или активировать повторно в дата-центре.

ВНИМАНИЕ

Активировать, отсоединять и помещать домены в режим обслуживания можно также во вкладке *Хранилище* в подробном просмотре дата-центра, с которым ассоциированы эти домены.

### 8.8.3. Изменение параметров доменов хранилищ

Параметры доменов хранения можно изменять с помощью портала администрирования. В зависимости от статуса домена хранилищ («активен» или «неактивен»), для изменения будут доступны разные поля. Поля **Дата-центр**, **Функция** **домена**, **Тип хранилища** и **Форматировать** нельзя изменить.

* **Активен**: для домена с активным статусом можно изменить значение следующих полей: **Название**, **Описание**, **Комментарий**, **Индикатор** **предупреждения о недостатке места (%)**,**Блокировщик действия при критической нехватке места**, **Очистить после удаления** и **Освободить блоки перед удалением**. Поле **Название** можно изменять только для активного домена хранилища. Все другие поля также можно изменять при неактивном домене.
* **Неактивен**: для домена, находящегося в режиме обслуживания или неприсоединённого, и, следовательно, неактивного, можно редактировать все поля, за исключением полей **Название**, **Дата-центр**, **Функция** **домена**, **Тип хранилища** и **Форматировать**. Изменять параметры сетевых соединений, монтирования, а также другие дополнительных параметры можно только для неактивного домена. Эти параметры поддерживаются только для типов доменов NFS, POSIX и локальных.

ВНИМАНИЕ

Сетевые соединения хранилищ iSCSI нельзя редактировать на портале администрирования, но можно редактировать с помощью REST API. Смотрите раздел [Updating Storage Connections](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/rest_api_guide/services#services-storage_server_connection_extension-methods-update) (Англ.) в руководстве для REST API.

**Изменение параметров активного домена хранения**

1. Нажмите Хранилище → Домены и выберите домен хранения.
2. Нажмите **Управление доменами**.
3. Измените значения доступных полей так, как необходимо.
4. Нажмите **OK**.

**Изменение параметров неактивного домена хранения**

1. Нажмите Хранилище → Домены.
2. Если домен хранения активен, переместите его в режим обслуживания:
   1. Нажмите на имя домена, чтобы перейти к подробному просмотру.
   2. Перейдите на вкладку **Дата-центр**.
   3. Нажмите **Обслуживание**.
   4. Нажмите **OK**.
3. Нажмите **Управление доменом**.
4. Измените путь к хранилищу и другие необходимые сведения. Сведения о новых сетевых соединениях должны иметь тот де тип хранилища, что и исходное соединение.
5. Нажмите **OK**.
6. Активируйте домен хранения :
   1. Нажмите на имя домена хранения, чтобы перейти к подробному просмотру.
   2. Перейдите на вкладку **Дата-центр**.
   3. Нажмите **Активировать**.

### 8.8.4. Обновление файлов OVF

По умолчанию, файлы OVF обновляются каждые 60 минут. Но после импорта важной ВМ или критически важного обновления ПО, файлы OVF можно обновить вручную.

**Обновление файлов OVF**

1. Нажмите Хранилище → Домены.
2. Выберите домен хранилища и нажмите **Больше действий** (), а затем нажмите **Обновить файлы OVF**.

Информация в файлах OVF будет обновлена, и в разделе **События** появится сообщение.

### 8.8.5. Активация доменов хранения из режима обслуживания

Если в параметры хранилища дата-центра ранее вносились изменения, то домены хранилища необходимо поместить в режим обслуживания. Для возобновления использования домена хранилища, активируйте его.

1. Нажмите Хранилище → Домены.
2. Нажмите на имя неактивного домена, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Дата-центры**.
4. Нажмите **Активировать**.

ВАЖНО

При попытке активации домена ISO до активации домена данных будет показано сообщение об ошибке, и домен не будет активирован.

### 8.8.6. Отсоединение домена хранения от дата-центра

Отсоедините домен хранения от одного дата-центра, чтобы выполнить его миграцию в другой дата-центр.

**Отсоединение домена хранения от дата-центра**

1. Нажмите Хранилище → Домены.
2. Нажмите на имя домена, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Дата-центры**.
4. Нажмите **Обслуживание**.
5. Нажмите **OK** для инициации режима обслуживания.
6. Нажмите **Отсоединить**.
7. Нажмите **OK**, чтобы отсоединить домен хранения .

Домен хранения был отсоединён от дата-центра и готов для присоединения к другому дата-центру.

### 8.8.7. Присоединение домена хранения к дата-центру

Присоедините домен хранения к дата-центру.

**Присоединение домена хранения к дата-центру**

1. Нажмите Хранилище → Домены.
2. Нажмите на имя домена, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Дата-центр**.
4. Нажмите **Присоединить**.
5. Выберите соответствующий дата-центр.
6. Нажмите **OK**.

Домен хранения присоединён к дата-центру и активируется автоматически.

### 8.8.8. Удаление домена хранилищ

В дата-центр есть домен хранения, который нужно удалить из виртуализированного окружения.

**Последовательность действий**

1. Нажмите Хранилище → Домены.
2. Переместите домен хранения в режим обслуживания и отсоедините его:
   1. Нажмите на имя домена, чтобы перейти к подробному просмотру.
   2. Перейдите на вкладку **Дата-центр**.
   3. Нажмите **Обслуживание**, затем нажмите **OK**.
   4. Нажмите **Отсоединить**, затем нажмите **OK**.
3. Нажмите **Удалить**.
4. Опционально, отметьте галочкой пункт **Форматировать домен, т.е. содержимое хранилища будет потеряно**, чтобы стереть содержимое домена.
5. Нажмите **OK**.

Домен хранения навсегда удаляется из окружения.

### 8.8.9. Разрушение домена хранения

Домен хранения, содержащий ошибки, не всегда возможно удалить посредством стандартной процедуры. Разрушение домена хранения принудительно удаляет его из виртуализированного окружения.

**Разрушение домена хранения**

1. Нажмите Хранилище → Домены.
2. Выберите домен хранилища и нажмите **Больше действий** (), затем нажмите **Разрушить**.
3. Отметьте галочкой пункт **Одобрить действие**.
4. Нажмите **OK**.

### 8.8.10. Создание профилей дисков

Профили дисков определяют максимальный уровень пропускной способности и максимальный уровень операций ввода и вывода виртуальных дисков в домене хранения. Профили дисков создаются на базе профилей хранилищ, настроенных в дата-центрах. Чтобы профили вступили в силу, они должны вручную назначаться каждому виртуальному диску.

Действие подразумевает, что ранее в дата-центре, к которому принадлежит домен хранения, уже была настроена одна или более запись о качестве обслуживания хранилищ.

**Создание профиля диска**

1. Нажмите Хранилище → Домены.
2. Нажмите на имя домена, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Профили дисков**.
4. Нажмите **Добавить**.
5. Введите **Название** и **Описание** профиля диска.
6. В списке **QoS** выберите запись о качестве обслуживания, которую нужно применить к профилю диска.
7. Нажмите **OK**.

### 8.8.11. Удаление профилей дисков

Удалите существующий профиль диска из окружения виртуализации Red Hat.

**Удаление профиля диска**

1. Нажмите Хранилище → Домены.
2. Нажмите на имя домена хранения данных, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Профили дисков**.
4. Выберите удаляемый профиль диска.
5. Нажмите **Удалить**.
6. Нажмите **OK**.

Если профиль был присвоен одному из виртуальных дисков, этот профиль будет удалён из списка этих дисков.

### 8.8.12. Просмотр состояния работоспособности домена хранилищ

В дополнение к обычному **Статусу**, у доменов хранилищ есть внешний статус работоспособности. Информация о внешнем статусе работоспособности доставляется расширениями или внешними системами, или же настраивается администратором. Просмотреть её можно слева от **Имени** домена в виде следующих значков:

* **OK**: без значка
* **Информация**: 
* **Предупреждение**: 
* **Ошибка**: 
* **Сбой**: 

Чтобы узнать дополнительные подробности о работоспособности домена хранения, нажмите на его имя, чтобы перейти к подробному просмотру, и далее перейдите на вкладку **События**.

Статус работоспособности домена хранилища также можно узнать с помощью REST API. В запрос GET будет включён элемент external\_status , содержащий этот статус.

Указать статус работоспособности домена хранилища в REST API можно с помощью набора events. Подробности см. <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/rest_api_guide/services#services-events-methods-add>

### 8.8.13. Параметр домена хранилища «Освободить блоки перед удалением»

Если пункт **Освободить блоки перед удалением** отмечен, при удалении логического тома вызывается команда blkdiscard , и базовое хранилище оповещается о том, что блоки свободны. Затем массив хранилища может использовать освобождённое пространство и выделять его по запросу. Возможность **Освободить блоки перед удалением** эффективна только для блочных хранилищ. В виртуализированном ЦУ для файловых хранилищ, таких, как NFS, этот флаг недоступен.

**Ограничения:**

* **Возможность Освободить блоки перед удалением доступна только для доменов блочных хранилищ, таких, как iSCSI или** оптоволокно.
* Базовое хранилище должно поддерживать Discard.

Параметр **Освободить блоки перед удалением можно включить как при создании домена блочного хранилища, так и при изменении параметров домена блочного хранилища. Смотрите Разделы 8.5 и 8.8.3.**