Руководство администратора

Red Hat Virtualization 4.3

**Аннотация**

В данном руководстве содержатся сведения и инструкции для администраторов системы виртуализации Red Hat Virtualization.

# Часть I. Администрирование и обслуживание среды виртуализации Red Hat

Труд администратора является необходимым условием функционирования среды виртуализации. В обязанности администратора системы виртуализации Red Hat входят следующие задачи:

* Управление физическими и виртуальными ресурсами, такими, как хосты и виртуальные машины. Сюда входит добавление хостов и обновление версий ПО на хостах, импорт доменов, преобразование виртуальных машин, созданных на сторонних гипервизорах, а также управление пулами виртуальных машин.
* Мониторинг всех системных ресурсов на предмет потенциальных проблем, таких, как чрезмерная нагрузка на один из хостов, недостаток памяти или места на диске, а также выполнение любых необходимых задач (например, миграция ВМ на другие хосты для снижения нагрузки или высвобождение ресурсов путём выключения машин).
* Своевременное реагирование на изменяющиеся требования ВМ (например, обновление версии ОС или выделение большего объёма памяти).
* Управление изменёнными свойствами объектов с помощью тегов
* Работа с результатами поиска, сохранёнными как общедоступные закладки (<https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/introduction_to_the_administration_portal/index#chap-Bookmarks> )
* Управление параметрами пользователей и настройка уровней полномочий
* Диагностика и решение проблем конкретных пользователей или виртуальных машин в масштабе общих функциональных возможностей системы
* Создание общих и частных отчётов

# Глава 1. Настройка глобальных ресурсов

Окно **Параметры** можно открыть из меню Администрирование → Параметры. В этом окне можно настроить такие глобальные ресурсы среды виртуализации Red Hat, как пользователи, роли, системные полномочия, политики планирования задач, типы экземпляров и пулы адресов MAC. Кроме того, в этом окне можно настроить способы взаимодействия пользователей с ресурсами в окружении, также здесь располагается центральная локация для настройки параметров, которые можно применять к нескольким кластерам.

## Роли

Роли — это предварительно настроенный набор привилегий, настройку которых можно выполнить в виртуализированном центре управления. Роли предоставляют доступ и управленческие полномочия к разным уровням ресурсов в дата-центре, а также к конкретным физическим и виртуальным ресурсам.

В условиях многоуровневого администрирования любые полномочия, применяемые к контейнерному объекту, также применяются ко всем отдельным объектам в этом контейнере. Если, например, роль администратора хоста присвоена пользователю на конкретном хосте, то этот пользователь получает полномочия на выполнение любых доступных действий с хостом, но только на присвоенном хосте. Но если роль администратора хоста будет присвоена пользователю в дата-центре, то этот пользователь получает полномочия на выполнение действий для всех хостов в рамках кластера дата-центра.

### Создание новой роли

Если требуемая роль отсутствует в изначальном списке ролей системы виртуализации Red Hat, то можно создать новую роль и настроить её согласно целевому назначению.

**Добавление роли**

1. Чтобы открыть окно **Параметры**, нажмите Администрирование → Параметры. Вкладка **Роли** выбрана по умолчанию, и здесь показывается список изначальных ролей **Пользователя** и **Администратора**, а также все частные роли.
2. Нажмите **Добавить**.
3. Введите **Имя** и **Описание** новой роли.
4. Для параметра **Тип учётной записи** выберите **Администратор** или **Пользователь**.
5. С помощью кнопок **Развернуть всё** или **Свернуть всё** можно увидеть больше или меньше подробностей для полномочий объектов, присутствующих в списке **Чтобы разрешить действие, поставьте галочки**. Также можно развернуть или свернуть параметры для каждого объекта.
6. Для каждого объекта выберите или очистите действия, которые нужно разрешить или запретить в настраиваемой роли.
7. Для применения изменений нажмите **OK**. Новая роль будет показана в списке ролей.

### Изменение или копирование роли

Можно изменять параметры созданной администратором роли, но нельзя изменять роли по умолчанию. Чтобы изменить роль по умолчанию, клонируйте и измените копию роли согласно своим нуждам.

**Изменение или копирование роли**

1. Чтобы открыть окно **Параметры**, нажмите Администрирование → Параметры. В окне показывается список изначальных ролей **Пользователя** и **Администратора**, а также все частные роли.
2. Выберите роль, которую нужно изменить. Чтобы открыть окно **Параметры роли**, нажмите **Изменить**, или же, чтобы открыть окно **Копировать роль**, нажмите **Копировать**.
3. При необходимости, измените **Имя** и **Описание** роли.
4. С помощью кнопок **Развернуть всё** или **Свернуть всё** можно увидеть больше или меньше подробностей для полномочий объектов, присутствующих в списке. Также можно развернуть или свернуть параметры для каждого объекта.
5. Для каждого объекта выберите или очистите действия, которые нужно разрешить или запретить в настраиваемой роли.
6. Для применения внесённых изменений нажмите **OK**.

### Роль «Пользователь» и примеры авторизации

В примерах ниже демонстрируется применение контроля авторизации в различных сценариях с использованием различных возможностей системы авторизации, описываемой в данной главе.

**Пример 1.1. Полномочия для кластера**

Светлана – системный администратор отдела бухгалтерии в своей организации. Все виртуальные ресурсы её отдела организованы в кластер системы виртуализации Red Hat под названием Accounts. В кластере бухгалтерии Светлане присвоена роль **ClusterAdmin**. Это даёт ей возможность администрирования всех виртуальных машин в кластере, поскольку виртуальные машин являются дочерними объектами кластера. Администрирование ВМ включает в себя изменение, добавление или удаление таких виртуальных ресурсов, как диски, а также создание снимков. Её роль не позволяет администрировать никакие ресурсы за пределами кластера. Поскольку **ClusterAdmin** является ролью администратора, то Светлане позволено работать на «Портале администрирования» или на «Портале виртуализированного ЦУ» для управления этими ресурсами.

**Пример 1.2. Полномочия PowerUser на ВМ**

Иван — программист в отделе бухгалтерии. Для сборки и тестирования своих программ он использует виртуальные машины. Светлана создала для него виртуальный рабочий стол с названием ivandesktop. На ВМ со столом ivandesktop Ивану присвоена роль **UserVmManager**, дающая ему доступ с Портала виртуальных машин к этой единственной ВМ. Поскольку Иван обладает полномочиями **UserVmManager, то он может вносить изменения в параметры своей виртуальной машины. А поскольку UserVmManager** является ролью пользователя, то она не даёт ему возможности использовать Портал администрирования.

**Пример 1.3. Полномочия роли PowerUser дата-центра**

Дарья — руководитель отдела. В дополнение к её собственным обязанностям она время от времени помогает менеджеру по персоналу в задачах найма работников, планируя интервью и проверяя рекомендации. Согласно корпоративной политике, для задач найма персонала Дарья должна использовать определённое приложение.

Хотя у Дарьи есть своя собственная машина для задач управления отделом, ей нужно создать отдельную ВМ для работы с приложением по подбору персонала. Ей присвоены полномочия **PowerUserRole** для дата-центра, в котором будет располагаться её новая ВМ, потому что для создания новой виртуальной машины ей нужно внести изменения в некоторые компоненты в границах дата-центра, включая создание виртуального диска в домене хранилища.

Обратите внимание, что это не то же самое, что и присвоение Дарье привилегий **DataCenterAdmin**. В качестве пользователя PowerUser дата-центра, Дарья может входить на Портал ВМ и выполнять действия с виртуальными машинами в границах дата-центра. Но она не может выполнять такие действия на уровне дата-центра, как прикрепление к дата-центру хостов или хранилищ.

**Пример 1.4. Полномочия сетевого администратора**

Наташа работает сетевым администратором в отделе IT. В её ежедневные обязанности входит создание, управление и удаление сетей в окружении виртуализации Red Hat её отдела. Для её роли ей нужны административные привилегии на ресурсы и на сети каждого ресурса. Если, например, у Наташи будут привилегии **NetworkAdmin в дата-центре отдела IT**, то она сможет добавлять и удалять сети в дата-центре, а также присоединять и отсоединять сети для всех ВМ, принадлежащих дата-центру.

**Пример 1.5. Полномочия частной роли**

Раиса работает в отделе IT и отвечает за администрирование учётных записей пользователей в системе виртуализации Red Hat. Ей нужны полномочия для добавления учётных записей пользователей и для присвоения им соответствующих ролей и полномочий. Сама она не использует никаких виртуальных машин, и не должна иметь доступа к администрированию хостов, ВМ, кластеров или дата-центров. Такой встроенной роли, которая предоставляла бы ей этот конкретный набор полномочий, не существует. Для настройки набора полномочий, соответствующих рабочими обязанностям Раисы, нужно создать частную роль.

**Рисунок 1.1. Частная роль UserManager**

****

Частная роль **UserManager** на иллюстрации выше разрешает управление пользователями, полномочия и ролями. Эти действия собраны в разделе **Система**, являющимся самым верхним объектом иерархии, показанной на Рисунке 1.3, что означает, что эти действия применимы ко всем другим объектам в системе. **Тип учётной записи**, указанной для этой роли — **Администратор**, а это означает, что после присвоения ей этой роли, Раиса сможет использовать как Портал администрирования, так и Портал ВМ.

# 1.2. Системные полномочия

Полномочия дают пользователям возможность выполнять действия с объектами, где объекты — это либо отдельные объекты, либо контейнерные. Любые полномочия, применяющиеся к контейнерному объекту, также применимы ко всем членам этого контейнера.

**Рисунок 1.2. Полномочия и роли**

****

**Рисунок 1.3. Иерархия объектов системы виртуализации Red Hat**

****

### 1.2.1. Свойства пользователя

Роли и полномочия являются свойствами пользователя. Роли — это предварительно настроенные наборы привилегий, предоставляющих доступ к разным уровням физических и виртуальных ресурсов. Многоуровневое администрирование предоставляет тонко настроенную иерархию полномочий. У администратора дата-центра, например, есть полномочия на управление всеми объектами в дата-центре, в то время как у администратора хоста есть полномочия на управление одним физическим хостом. Один пользователь может иметь полномочия на использование одной ВМ и не иметь полномочий на внесение изменений в параметры ВМ, в то время как у другого пользователя могут иметься системные полномочия на ВМ.

### 1.2.2. Роли пользователей и администраторов

Система виртуализации Red Hat предоставляет широкий диапазон предварительно настроенных ролей, от администратора с системными полномочиями до конечного пользователя с доступом только к одной ВМ. Хотя роли по умолчанию нельзя изменять или удалять, их можно клонировать и редактировать, а также можно создавать новые роли согласно необходимым требованиям. Сущеcтвует два типа ролей:

* Роль **Администратор**: предоставляет доступ к **Порталу администрирования** для управления физическими и виртуальными ресурсами. Роль администратора присваивает права на выполнение действий на Портале ВМ; тем не менее, она никак не влияет на то, что доступно к просмотру для пользователя на Портале ВМ.
* Роль **Пользователь**: предоставляет доступ к Порталу ВМ для доступа к ВМ и шаблонами и для управления ими. Роль пользователя определяет, что доступно к просмотру для пользователя на Портале ВМ. Полномочия, выданные пользователю с ролью администратора, отражаются на том, какие действия доступны этому пользователю на Портале ВМ.

### 1.2.3. Объяснение ролей пользователей

В таблице ниже описываются базовые роли пользователей, предоставляющие полномочия на доступ к виртуальным машинам и их параметрам на Портале ВМ.

**Таблица 1.1. Базовые роли пользователей в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| UserRole | Доступ и использование ВМ и пулов | Может выполнять вход на Портал ВМ, использовать привязанные к нему виртуальные машины, просматривать статус ВМ и подробные сведения о неё. |
| PowerUserRole | Может создавать ВМ и шаблоны, а также управлять ими. | Присваивайте эту роль пользователю для доступа ко всему окружению в окне Параметры или для доступа к конкретным дата-центрам или кластерам. Если, например, роль PowerUserRole применяется на уровне дата-центра, то пользователь PowerUser может создавать ВМ и шаблоны в дата-центре. |
| UserVmManager | Системный администратор виртуальной машины | Может администрировать ВМ, а также создавать и использовать снимки. Пользователю, создавшему машину на Портале ВМ, автоматически присваивается роль UserVmManager на этой машине. |

В таблице ниже описываются продвинутые роли пользователей, позволяющие выполнять более тонкую настройку полномочий на ресурсы на Портале ВМ.

**Таблица 1.2. Продвинутые роли пользователей в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| UserTemplateBasedVm | **Привилегии, ограниченные только использованием шаблонов.** | **Может использовать шаблоны для создания виртуальных машин** |
| DiskOperator | **Пользователь виртуального диска** | **Может использовать, просматривать и изменять виртуальные диски. Наследует полномочия на использование ВМ, к которой присоединён виртуальный диск.** |
| VmCreator | **Может создавать виртуальные машины на Портале ВМ** | **Эта роль не применяется к конкретной ВМ; присваивайте эту роль пользователю в масштабах всего окружения в окне Параметры. Или же присваивайте эту роль в конкретных дата-центрах или кластерах. При присвоении роли в кластерах, также нужно присваивать роль** DiskCreator в масштабах всего дата-центра или конкретных доменов хранилищ. |
| TemplateCreator | **Может создавать, редактировать и удалять шаблоны ВМ в рамках присвоенных ресурсов.** | **Эта роль не присваивается к конкретному шаблону; присваивайте эту роль пользователю в масштабах всего окружения в окне Параметры. Или же присваивайте эту роль в конкретных дата-центрах, кластерах или доменах хранилищ.** |
| **DiskCreator** | **Может создавать, редактировать, управлять и удалять виртуальные диски рамках присвоенных кластеров или дата-центров** | **Эта роль не присваивается конкретному виртуальному диску; присваивайте эту роль пользователю в масштабах всего окружения в окне Параметры. Или же присваивайте эту роль в конкретных дата-центрах, кластерах или доменах хранилищ.** |
| TemplateOwner | **Может изменять и удалять шаблоны, присваивать и управлять полномочиями пользователей на шаблон.** | **Эта роль автоматически присваивается пользователю, создающему шаблон. Другие пользователи, не имеющие полномочий TemplateOwner для шаблона, не могут просматривать или использовать этот шаблон.** |
| VnicProfileUser | **Пользователь логических сетей и сетевых интерфейсов виртуальной машины и шаблона.** | **Может присоединять или отсоединять сетевые интерфейсы конкретных логических сетей.** |

### 1.2.4. Объяснение ролей администраторов

В таблице ниже описываются базовые административные роли, дающие полномочия на доступ и настройку ресурсов на Портале администрирования.

**Таблица 1.3. Базовые роли администраторов в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| SuperUser | **Системный администратор среды виртуализации red hat** | **Полные полномочия на все объекты и уровни, администрирует всеми объектами во всех дата-центрах** |
| ClusterAdmin | **Администратор кластера** | **Обладает административными полномочиями на все объекты в рамках конкретного кластера.** |
| DataCenterAdmin | Администратора дата-центра | **Обладает административными полномочиями на все объекты в рамках конкретного дата-центра, за исключением хранилища.** |

ВАЖНО

Не используйте пользователя-администратора сервера каталогов в качестве пользователя-администратора системы виртуализации red hat. Создайте на сервере каталогов пользователя специально для использования в качестве пользователя-администратора системы виртуализации.

В таблице ниже описываются продвинутые роли администраторов, позволяющие выполнять более тонкую настройку полномочий на ресурсы на Портале администрирования.

**Таблица 1.4. Продвинутые роли администраторов в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| TemplateAdmin | Администратор шаблона ВМ | Может создавать, удалять и настраивать домены хранилищ и сетевые параметры шаблонов, а также перемещать шаблоны между доменами. |
| StorageAdmin | Администратор хранилища | Может создавать, удалять, настраивать и управлять присвоенным доменом хранилища. |
| HostAdmin | Администратор хоста | Может присоединять, удалять, настраивать и управлять конкретным хостом. |
| NetworkAdmin | Сетевой администратор | Может настраивать и управлять сетью конкретного дата-центра или кластера. Сетевой администратор дата-центра или кластера наследует сетевые полномочия на виртуальные пулы в рамках кластера. |
| VmPoolAdmin | Системный администратор виртуального пула | Может создавать, удалять и настраивать виртуальный пул; присваивать и удалять пользователей виртуального пула; а также выполнять базовые операции на ВМ в пуле. |
| GlusterAdmin | Администратор хранилища Gluster | Может создавать, удалять, настраивать и управлять томами хранилища Gluster. |
| VmImporterExporter | Администратор импорта и экспорта виртуальных машин | Может импортировать и экспортировать ВМ. Имеет возможность посматривать все ВМ и шаблоны, экспортированные другими пользователями. |

### 1.2.5. Присвоение ресурсу роли администратора или пользователя

Присвоение роли администратора или пользователя ресурсу, чтобы дать возможность доступа или управления этим ресурсом.

**Присвоение роли ресурсу**

1. Найдите название нужного ресурса и нажмите на него, чтобы просмотреть детали.
2. Перейдите на вкладку **Полномочия**, чтобы указать присвоенных пользователей, роль пользователя и наследуемые полномочия для выбранного ресурса.
3. Нажмите **Добавить**.
4. Укажите имя или пользовательское имя существующего пользователя в поле **Поиск** и нажмите **Выполнить**. Из полученного списка возможных совпадений выберите пользователя.
5. В выпадающем списке **Присвоить роль** выберите нужную роль.
6. Нажмите **OK**.

Теперь на указанном ресурсе действуют наследуемые полномочия этой роли для указанного пользователя.

### 1.2.6. Удаление роли администратора или пользователя с ресурса

Удаление роли администратора или пользователя с ресурса; на этом ресурсе пользователь теряет наследуемые полномочия, связанные с ролью.

**Удаление роли с ресурса**

1. Найдите название нужного ресурса и нажмите на него, чтобы просмотреть детали.
2. Перейдите на вкладку **Полномочия**, чтобы указать присвоенных пользователей, роль пользователя и наследуемые полномочия для выбранного ресурса.
3. Выберите пользователя, удаляемого с ресурса.
4. Нажмите **Удалить**.
5. Нажмите **OK**.

### 1.2.7.  Администрирование системных полномочий в дата-центре

Являясь пользователем **SuperUser,** системный администратор управляет всеми аспектами Портала администрирования. Другим пользователям можно присваивать более конкретные административные роли. Эти узкоспециализированные административные роли удобны для присвоения пользователю административных привилегий, ограниченных конкретным ресурсом. У роли **DataCenterAdmin**, например, есть административные привилегии только для присвоенного дата-центра, за исключением хранилища этого дата-центра, а у роли **ClusterAdmin** есть административные привилегии только для назначенного кластера.

Администратор дата-центра — это роль системного администратора только для конкретного дата-центра. Она удобна в среде виртуализации с несколькими дата-центрами, где каждому дата-центру требуется администратор. Роль **DataCenterAdmin** является иерархической моделью; пользователь, которому назначена роль администратора дата-центра, может управлять всеми объектами в дата-центре за исключением хранилища этого дата-центра. С помощью кнопки **Параметры** на панели заголовков назначайте администраторов дата-центров для всех дата-центров в окружении.

Роль администратора дата-центра разрешает выполнять следующие действия:

* Создание и удаление кластеров, связанных с дата-центром.
* Добавление и удаление хостов, ВМ и пулов, связанных с дата-центром.
* Изменение пользовательских полномочий на виртуальных машинах, связанных с дата-центром.

ВНИМАНИЕ

Присваивать роли и полномочия можно только существующим пользователям.

Сменить администратора дата-центра можно, удалив существующего системного администратора и добавив нового.

### 1.2.8. Объяснение роли администратора дата-центра

**Роли с полномочиями в дата-центре**

В таблице ниже описываются административные роли и привилегии, применимые в администрировании дата-центров.

**Таблица 1.5. Административные роли в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| DataCenterAdmin | Администратор дата-центра | Может использовать, создавать, удалять и управлять всеми физическими и виртуальными ресурсами в рамках указанного дата-центра, за исключением хранилища, и включая кластеры, хосты, шаблоны и виртуальные машины. |
| NetworkAdmin | Администратор сети | Может настраивать и управлять сетью конкретного дата-центра. Сетевой администратор дата-центра также наследует сетевые полномочия на виртуальные машины в рамках дата-центра. |

### 1.2.9. Управление системными полномочиями в кластере

Являясь пользователем **SuperUser,** системный администратор управляет всеми аспектами Портала администрирования. Другим пользователям можно присваивать более конкретные административные роли. Эти узкоспециализированные административные роли удобны для присвоения пользователю административных привилегий, ограниченных конкретным ресурсом. У роли **DataCenterAdmin**, например, есть административные привилегии только для присвоенного дата-центра, за исключением хранилища этого дата-центра, а у роли **ClusterAdmin** есть административные привилегии только для назначенного кластера.

Администратор кластера — это роль системного администратора только для конкретного кластера. Она удобна в среде виртуализации с несколькими кластерами, где каждому кластеру требуется администратор. Роль **ClusterAdmin** является иерархической моделью; пользователь, которому назначена роль администратора кластера, может управлять всеми объектами в кластере. С помощью кнопки **Параметры** на панели заголовков назначайте администраторов кластеров для всех кластеров в окружении.

Роль администратора кластера разрешает выполнять следующие действия:

* Создание и удаление ассоциированных кластеров.
* Добавление и удаление хостов, ВМ и пулов, связанных с кластером.
* Изменение пользовательских полномочий на виртуальных машинах, связанных с кластером.

ВНИМАНИЕ

Присваивать роли и полномочия можно только существующим пользователям.

Также сменить администратора кластера можно, удалив существующего системного администратора и добавив нового.

### 1.2.10. Объяснение роли администратора кластера

**Роли с полномочиями в кластере**

В таблице ниже описываются административные роли и привилегии, применимые в администрировании кластеров.

**Таблица 1.6. Административные роли в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| ClusterAdmin | Администратор кластера | Может использовать, создавать и управлять всеми физическими и виртуальными ресурсами в конкретном кластере, включая хосты, шаблоны и виртуальные машины. Может настраивать свойства сети в рамках кластера, такие, как выделение сетей визуализации или назначение сети как требуемая или не требуемая.  Тем не менее, у **ClusterAdmin** нет полномочий на присоединение или отсоединение сетей от кластера, для этого требуются полномочия **NetworkAdmin.** |
| NetworkAdmin | Администратор сети | Может настраивать и управлять сетью конкретного кластера. Сетевой администратор кластера также наследует сетевые полномочия на виртуальные машины в рамках кластера. |

### 1.2.11. Управление сетевыми системными полномочиями

Являясь пользователем **SuperUser,** системный администратор управляет всеми аспектами Портала администрирования. Другим пользователям можно присваивать более конкретные административные роли. Эти узкоспециализированные административные роли удобны для присвоения пользователю административных привилегий, ограниченных конкретным ресурсом. У роли **DataCenterAdmin**, например, есть административные привилегии только для присвоенного дата-центра, за исключением хранилища этого дата-центра, а у роли **ClusterAdmin** есть административные привилегии только для назначенного кластера.

Сетевой администратор — это роль системного администратора, которую можно применить для конкретной сети или для всех сетей в дата-центре, кластере, хосте, виртуальной машине или шаблоне. Сетевой пользователь может исполнять ограниченные административные роли, такие, как просмотр и присоединение сетей на конкретной ВМ или конкретном шаблоне. Для назначения сетевого администратора всем сетям в окружении используйте кнопку **Параметры** на панели заголовков.

Роль сетевого администратора позволяет выполнять следующие действия:

* Создание, изменение и удаление сетей
* Редактирование параметров сети, включая настройку зеркалирования портов
* Подключение и отключение сетей от ресурсов, включая кластеры и виртуальные машины

Пользователю, создавшему сеть, автоматически присваиваются полномочия **NetworkAdmin** в созданной сети. Также сменить администратора сети можно, удалив существующего администратора и добавив нового.

### 1.2.12. Объяснение ролей сетевого администратора и сетевого пользователя

**Роли с сетевыми полномочиями**

В таблице ниже описываются роли администратора и пользователя, а также привилегии, используемые в сетевом администрировании.

**Таблица 1.7. Роли сетевого администратора и сетевого пользователя в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| NetworkAdmin | Сетевой администратор дата-центра, кластера, хоста, ВМ или шаблона. Пользователю, создавшему сеть, автоматически присваиваются полномочия **NetworkAdmin** для созданной сети. | Может настраивать и управлять сетью конкретного дата-центра, кластера, хоста, ВМ или шаблона. Сетевой администратор дата-центра или кластера наследует сетевые полномочия на виртуальные пулы в рамках кластера. Чтоб настроить зеркалирование портов в сети виртуальной машины, примените для сети роль **NetworkAdmin**, а на ВМ — роль **UserVmManager**. |
| VnicProfileUser | Пользователь логической сети и сетевого интерфейса виртуальной машины и шаблонов. | Может подключать или отключать сетевые интерфейсы для конкретных логических сетей. |

### 1.2.13. Управление системными полномочиями для хоста

Являясь пользователем **SuperUser,** системный администратор управляет всеми аспектами Портала администрирования. Другим пользователям можно присваивать более конкретные административные роли. Эти узкоспециализированные административные роли удобны для присвоения пользователю административных привилегий, ограниченных конкретным ресурсом. У роли **DataCenterAdmin**, например, есть административные привилегии только для присвоенного дата-центра, за исключением хранилища этого дата-центра, а у роли **ClusterAdmin** есть административные привилегии только для назначенного кластера.

Администратор хоста — это административная роль для одного конкретного хоста. Она удобна для кластеров с множеством хостов, где для каждого хоста нужен системный администратор. Используйте кнопку **Параметры** на панели заголовков для назначения администратора для всех хостов окружения.

Роль администратора хоста разрешает выполнять следующие действия:

* Настройка параметров хоста
* Настройка логических сетей
* Удаление хоста

Также сменить системного администратора хоста можно, удалив существующего системного администратора и добавив нового.

### 1.2.14. Объяснение роли администратора хоста

**Роли с полномочиями на хосте**

В таблице ниже описывается роль администратора, а также привилегии, применяемые для администрирования хостов.

**Таблица 1.8. Роли системного администратора в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| HostAdmin | Администратор хоста | Может настраивать, управлять и удалять конкретный хост. Также может выполнять действия, касающиеся сети на конкретном хосте. |

### 1.2.15. Управление системными полномочиями в домене хранилища

Являясь пользователем **SuperUser,** системный администратор управляет всеми аспектами Портала администрирования. Другим пользователям можно присваивать более конкретные административные роли. Эти узкоспециализированные административные роли удобны для присвоения пользователю административных привилегий, ограниченных конкретным ресурсом. У роли **DataCenterAdmin**, например, есть административные привилегии только для присвоенного дата-центра, за исключением хранилища этого дата-центра, а у роли **ClusterAdmin** есть административные привилегии только для назначенного кластера.

Администратор хранилища — это роль системного администрирования только для одного конкретного домена хранилища. Она удобна в дата-центрах с несколькими доменами хранилищ, где для каждого домена хранилища требуется свой системный администратор. Используйте кнопку **Параметры** на панели заголовков для назначения администратора хранилища для всех доменов хранилищ окружения.

Роль администратора домена хранилища позволяет выполнять следующие действия:

* Изменение конфигурации домена хранилища
* Перевод домена хранилища в режим обслуживания
* Удаление домена хранилища

ВНИМАНИЕ

Присваивать роли и полномочия можно только существующим пользователям.

Также сменить системного администратора домена хранилища можно, удалив существующего системного администратора и добавив нового.

### 1.2.16. Объяснение роли администратора хранилища

**Роли с полномочиями в домене хранилища**

В таблице ниже описывается роль администратора, а также привилегии, применяемые для администрирования доменов хранилищ.

**Таблица 1.9. Роли системного администратора в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| StorageAdmin | Администратор хранилища | Может создавать, удалять, настраивать и управлять конкретным доменом хранилища. |
| GlusterAdmin | Администратор хранилища Gluster | Может создавать, удалять, настраивать и управлять томами хранилища Gluster. |

### 1.2.17. Управление системными правами на пул виртуальных машин

Являясь пользователем **SuperUser,** системный администратор управляет всеми аспектами Портала администрирования. Другим пользователям можно присваивать более конкретные административные роли. Эти узкоспециализированные административные роли удобны для присвоения пользователю административных привилегий, ограниченных конкретным ресурсом. У роли **DataCenterAdmin**, например, есть административные привилегии только для присвоенного дата-центра, за исключением хранилища этого дата-центра, а у роли **ClusterAdmin** есть административные привилегии только для назначенного кластера.

Администратор пула ВМ — это роль системного администрирования пулов ВМ в дата-центре. Эту роль можно применить к конкретным пулам виртуальных машин, к дата-центру или ко всему виртуализованному окружению в целом; эта роль удобна для назначения различных пользователей на управление конкретными ресурсами пулов виртуальных машин.

Роль администратора пула ВМ позволяет выполнять следующие действия:

* Создание, изменение и удаление пулов
* Добавление и открепление ВМ от пулов.

ВНИМАНИЕ

Присваивать роли и полномочия можно только существующим пользователям.

### 1.2.18. Объяснение роли администратора пула виртуальных машин

**Роли с полномочиями в пуле**

В таблице ниже описывается роль администратора, а также привилегии, применяемые для администрирования пулов.

**Таблица 1.10. Роли системного администратора в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| VmPoolAdmin | Роль системного администратора виртуального пула. | Может создавать, удалять и настраивать виртуальный пул, присваивать и удалять пользователь виртуального пула, а также выполнять базовые операции на виртуальной машине. |
| ClusterAdmin | Администратор кластера | Может использовать, создавать, удалять и управлять всеми пулами ВМ в конкретном кластере. |

### 1.2.19. Управление системными полномочиями на виртуальные диски

Являясь пользователем **SuperUser,** системный администратор управляет всеми аспектами Портала администрирования. Другим пользователям можно присваивать более конкретные административные роли. Эти узкоспециализированные административные роли удобны для присвоения пользователю административных привилегий, ограниченных конкретным ресурсом. У роли **DataCenterAdmin**, например, есть административные привилегии только для присвоенного дата-центра, за исключением хранилища этого дата-центра, а у роли **ClusterAdmin** есть административные привилегии только для назначенного кластера.

Диспетчер виртуализации red hat предоставляет две изначальных роли пользователя виртуальных дисков, но не предоставляет изначальной роли администратора виртуальных дисков. Одна из этих пользовательских ролей, роль **DiskCreator** , предоставляет возможность администрирования виртуальных дисков на Портале ВМ. Эту роль можно применить к конкретным ВМ, к дата-центру, к конкретному домену хранилища или ко всему виртуализованному окружению в целом; эта роль удобна тем, что позволяет различным пользователям управлять различными виртуальными ресурсами.

Роль создателя виртуальных дисков позволяет выполнять следующие действия:

* Создание, изменение и удаление виртуальных дисков, связанных с ВМ или другими ресурсами
* Изменение полномочий пользователей на виртуальные диски

ВНИМАНИЕ

Присваивать роли и полномочия можно только существующим пользователям.

### 1.2.20. Объяснение ролей пользователей виртуальных дисков

**Роли пользователя с полномочиями на виртуальные диски**

В таблице ниже описываются роли пользователей и привилегии, применимые для использования и администрирования виртуальных дисков на Портале ВМ.

**Таблица 1.11. Роли системного администратора в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| DiskOperator | **Пользователь виртуального диска** | Может использовать, просматривать и изменять виртуальные диски. Наследует полномочия на использование ВМ, к которой присоединён виртуальный диск. |
| DiskCreator | Может создавать, изменять, управлять и удалять виртуальные диски в рамках назначенных кластеров или дата-центров. | Эта роль не применяется к конкретному виртуальному диску; применяйте эту роль к пользователю в рамках всего окружения в окне **Параметры**. Как вариант, применяйте эту роль для конкретных дата-центров, кластеров или доменов хранилищ. |

### 1.2.21. 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” \

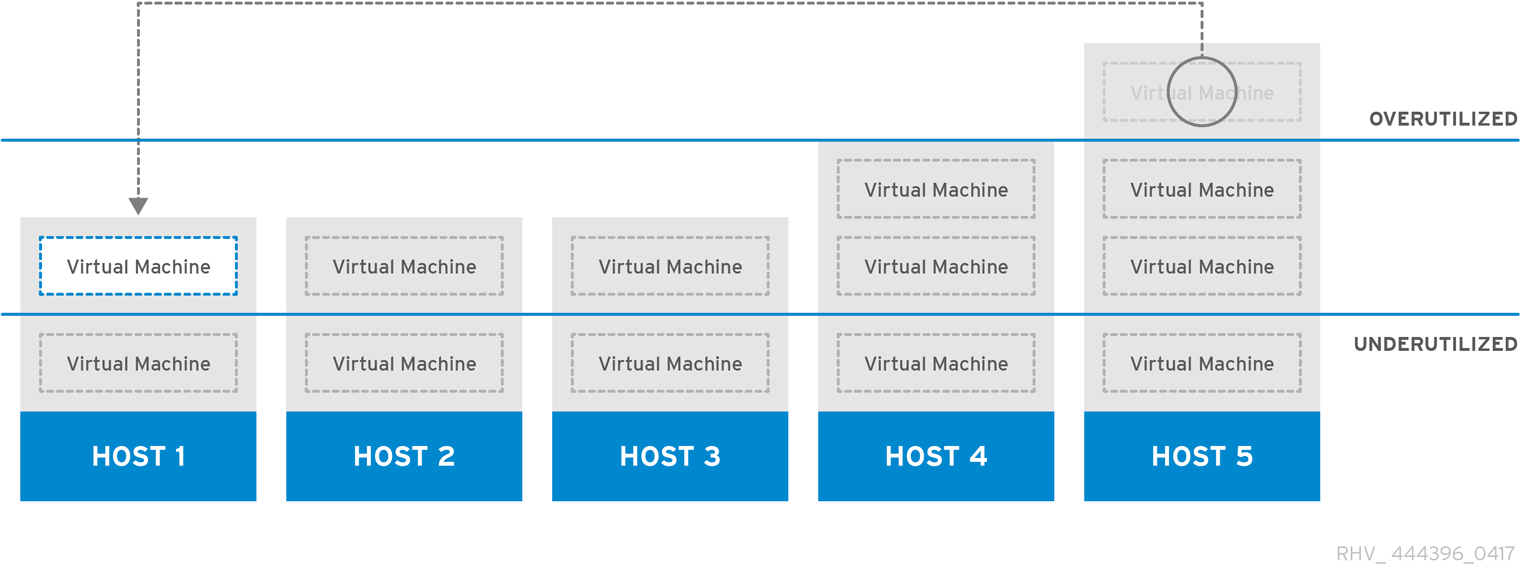
/usr/share/ovirt-engine/playbooks/ovirt-host-deploy.yml

# 1.3. Политики планирования

Политика планирования — это набор правил, определяющих логику, согласно которой виртуальные машины распределяются между хостами в кластере, к которому применяется данная политика. Политики планирования определяют эту логику с помощью сочетания фильтров, весов и политики балансировки нагрузки. Модули фильтров реализуют жёсткое применение политики и отфильтровывают хосты, не соответствующие указанным условиям. Модули веса применяют мягкое применение, и используются для контроля относительного приоритета факторов, принимаемых во внимание при определении тех хостов в кластере, на которых может выполняться виртуальная машина.

Диспетчер системы виртуализации Red Hat по умолчанию предоставляет пять политик планирования: **Evenly\_Distributed**, **Cluster\_Maintenance**, **None**, **Power\_Saving** и **VM\_Evenly\_Distributed**. Также можно настроить новые политики, предлагающие тонко настроенный контроль распределения виртуальных машин. Вне зависимости от политики планирования, виртуальная машина не станет начинать работу на хосте с перегруженным ЦП. По умолчанию, ЦП хоста считается перегруженным, если в течении 5 минут его загрузка составляет более 80%, но эти значения можно изменить с помощью политик планирования. Сведения о параметрах каждой политики планирования смотрите в Разделе 5.5.5, «Объяснение параметров политик планирования».

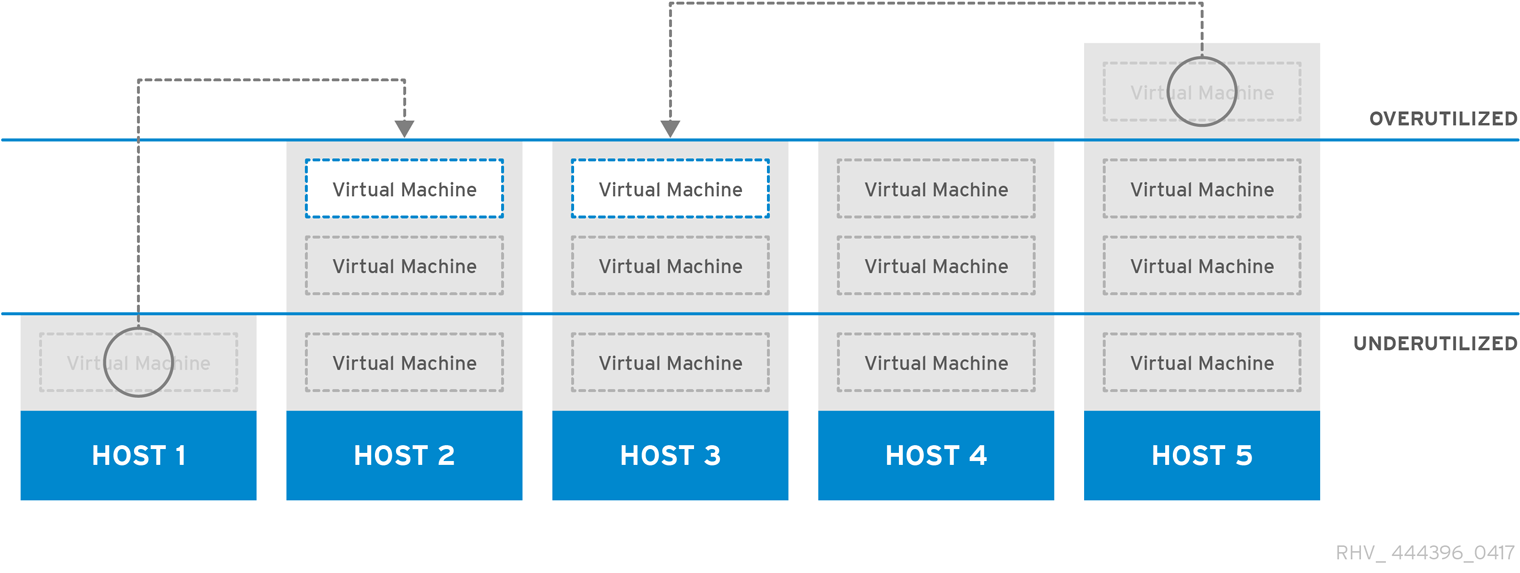
**Рисунок 1.4. Политика планирования равномерного распределения (Evenly Distributed)**



Политика планирования **Evenly\_Distributed** равномерно распределяет загрузку на память и вычисления ЦП между всеми хостами в кластере. Дополнительные ВМ, прикреплённые к хосту, не начнут работу, если хост достиг указанного значения параметров **CpuOverCommitDurationMinutes**, **HighUtilization** или **MaxFreeMemoryForOverUtilized**.

Политика планирования **VM\_Evenly\_Distributed** равномерно распределяет виртуальные машины между хостами на основе количества машин. Кластер считается несбалансированным, если на любом из хостов выполняется больше машин, чем указано в значении параметра **HighVmCount** , и если есть в наличии хоть один хост, число ВМ на котором выходит за пределы значения **MigrationThreshold**.

**Рисунок 1.5. Политика планирования энергосбережения (Power Saving)**



Политика планирования **Power\_Saving** распределяет память и вычислительные мощности ЦП между хостами в выборке доступных хостов для снижения потребления энергии на недозагруженных хостах. Виртуальные машины с хостов, имеющих нагрузку на ЦП ниже указанного значения слабой загрузки в течение интервала времени, превышающего указанный интервал, будут перенесены на другие хосты с тем, чтобы работу данного хоста можно было завершить. Дополнительные ВМ, прикреплённые к хосту, не начнут работу, если этот хост достиг указанного значения высокого коэффициента использования.

Укажите политику **None** чтобы нагрузка или использование энергии для выполняемых ВМ не разделялись между хостами. Это режим по умолчанию. При начале работы ВМ, память и загрузка на вычислительные мощности ЦП равномерно разделяются между всеми хостами кластера. Дополнительные ВМ, прикреплённые к хосту, не начнут работу, если этот хост достиг указанных значений **CpuOverCommitDurationMinutes**, **HighUtilization** или **MaxFreeMemoryForOverUtilized**.

Политика планирования **Cluster\_Maintenance** ограничивает активность в кластере во время выполнения задач обслуживания. При активной политике **Cluster\_Maintenance** никакие новые ВМ не могут начинать работу, за исключением ВМ с высокой доступностью. В случае отказа хоста, высокодоступные ВМ корректно возобновят работу, и любая ВМ сможет мигрировать.

### 1.3.1. Создание политик планирования

Для контролирования логики, согласно которой ВМ распределяются по указанному кластеру в окружении виртуализации red hat, можно создавать новые политики планирования.

**Создание политики планирования**

1. Нажмите Администрирование → Параметры.
2. Перейдите на вкладку **Политики планирования**.
3. Нажмите **Добавить**.
4. Укажите **Имя** и **Описание** политики планирования.
5. Настройте модули фильтров:
   1. В разделе **Модули фильтров** перетащите предпочитаемые модули фильтров из раздела **Отключённые фильтры** в раздел **Включённые фильтры**, для применения их в политике планирования.
   2. Конкретные модули фильтров также можно настроить как **Первый**, чтобы у него был наивысший приоритет, или **Последний**, чтобы он получил самый низкий приоритет, для базовой оптимизации. Чтобы установить приоритет, сделайте щелчок ПКМ по любому модулю фильтра, наведите курсор на пункт Местоположение и выберите **Первый** или **Последний**.
6. Настройте модули веса:
   1. В разделе **Модули весовых коэффициентов** перетащите предпочитаемые модули веса из области **Отключённые весовые коэффициенты** в область **Включённые весовые коэффициенты** , чтобы применить их к политике планирования.
   2. С помощью кнопок **+** и **–** слева от включённых модулей веса повышайте или уменьшайте вес этих модулей.
7. Укажите политику балансировки нагрузки:
   1. Из выпадающего списка в разделе **Балансировщик нагрузки** выберите политику балансировки нагрузки, которая будет применяться в политике планирования.
   2. В выпадающем списке в разделе **Параметры** выберите свойство балансировки нагрузки, которое нужно применить в политике планирования, и в текстовом поле справа от этого свойства укажите значение.
   3. С помощью кнопок **+** и **–** добавьте или удалите дополнительные свойства.
8. Нажмите **OK**.

### 1.3.2. Объяснение параметров в окнах «Новая политика планирования» и «Параметры политики планирования»

В таблице ниже приводятся подробности для параметров, доступных в окнах **Новая политика планирования** и **Параметры политики планирования**.

**Таблица 1.12. Окна «Новая политика планирования» и** «**Параметры политики планирования»**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| **Название** | Название политики планирования. Это название используется для наименования этой политики в виртуализированном ЦУ |
| **Описание** | Описание политики планирования. Это поле рекомендуется заполнить, но оно не обязательно. |
| **Модули фильтров** | Набор фильтров для контролирования хоста, на котором может выполняться ВМ из кластера. Включённый фильтр будет отсеивать хосты, не соответствующие условиям фильтра, а именно:   * CpuPinning: хосты, не отвечающие определению привязки задачи к процессору. * Migration: предотвращение миграции на один и тот же хост. * PinToHost: хосты, отличные от того хоста, за которым закреплена ВМ * CPU-Level: хосты, не соответствующие топологии ЦП виртуальной машины * CPU: хосты с меньшим числом ЦП, чем число, указанное для ВМ * Memory: хосты с недостаточным объёмом памяти для работы ВМ * VmAffinityGroups: хосты, не отвечающие условиям, указанным для ВМ-участницы группы схожести, например: ВМ в группе схожести должны работать на одном и том же хосте или на разных хостах. * VmToHostsAffinityGroups: группа хостов, не отвечающих условиям, указанным для ВМ-участницы группы схожести, например: виртуальные машины в группе схожести должны выполняться на хостах группы или на отельном хосте, не являющимся участником группы. * InClusterUpgrade: хосты, работающие под управлением ОС более ранней версии, чем версия ОС хоста, на котором на данный момент выполняется ВМ. * HostDevice: хосты, не поддерживающие хостовые устройства, требуемые для ВМ. * HA: принудительный запуск ВМ из окружения диспетчера виртуализации только на хостах с положительной оценкой высокой доступности * Emulated-Machine: хосты без должной поддержки эмулируемой машины * Network: хосты, на которых не установлены сети, требуемые контроллером сетевого интерфейса ВМ, или на которых не установлена сеть визуализации кластера. * HostedEnginesSpares: резервация места под ВМ диспетчера виртуализации на указанном числе узлов диспетчера виртуализации * Label: хосты без требуемых меток схожести * Compatibility-Version: запускает ВМ только на хостах с корректной версией совместимости * CPUOverloaded: хосты с перегруженными ЦП |
| Модули весовых коэффициентов | Набор весовых коэффициентов для настройки относительного приоритета факторов, учитываемых при определении в кластере хостов, на которых могут выполняться ВМ.   * InClusterUpgrade: определяет весовой коэффициент хоста в соответствии с версией их ОС. Вес сильнее «наказывает» хосты с более ранней версией ОС, чем хосты с версией ОС, аналогичной версии ОС того хоста, на котором в данный момент выполняется ВМ. Таким образом предпочтение всегда оказывается хостам со свежими версиями ОС. * OptimalForHaReservation: определяет весовой коэффициент хостов в соответствии с их оценкой высокой доступности. * None: определяет весовой коэффициент хостов согласно модулю равномерного распределения. * OptimalForEvenGuestDistribution: определяет весовой коэффициент хостов в соответствии с числом ВМ, выполняемых на этих хостах. * VmAffinityGroups: определяет весовой коэффициент хостов в соответствии с группой схожести, определённой для ВМ. В соответствии с параметрами этой группы схожести, модуль веса определяет вероятность того, будут ли ВМ в группе схожести выполняться на одном и том же хосте или на разных. * VmToHostsAffinityGroups: определяет весовой коэффициент хостов в соответствии с группами схожести, настроенными для машин. Весовой модуль определяет вероятность того, будут ли ВМ в группе схожести выполняться на одном из хостов-участников группы, или на отдельном хосте, не состоящем в группе. * OptimalForCPUPowerSaving: определяет весовой коэффициент хостов в соответствии с загрузкой их ЦП. Приоритет отдаётся хостам с наиболее высокой загрузкой. * OptimalForEvenCpuDistribution: определяет весовой коэффициент хостов в соответствии с загрузкой их ЦП. Приоритет отдаётся хостам с наиболее низкой загрузкой. * HA: определяет весовой коэффициент хостов в соответствии с оценкой их высокой доступности * PreferredHosts: во время настройки ВМ приоритет отдаётся предпочитаемым (preferred) хостам * OptimalForMemoryPowerSaving: определяет весовой коэффициент хостов в соответствии с их потреблением памяти. Приоритет отдаётся хостам с более низким объёмом доступной памяти. * OptimalForMemoryEvenDistribution: определяет весовой коэффициент хостов в соответствии с их потреблением памяти. Приоритет отдаётся хостам с более высоким объёмом доступной памяти. |
| Балансировщик нагрузки | В этом выпадающем меню можно выбрать применяемый модуль балансировки нагрузки. Модули балансировки нагрузки определяют логику, используемую во время миграции ВМ с хостов с текущей высокой нагрузкой на хосты с текущей низкой загрузкой. |
| Параметры | В этом выпадающем меню можно добавить или удалить параметры модулей балансировки нагрузки. Это меню доступно только в случае выбора модуля балансировки нагрузки для политики планирования. По умолчанию, настроенных параметров нет, а доступные параметры относятся к выбранному модулю. Используйте кнопки **+** и ­**–** для добавления или удаления дополнительных свойств модуля балансировки нагрузки. |

# 1.4. Типы экземпляров

Типы экземпляров можно использовать для настройки аппаратных составляющих ВМ. При выборе типа экземпляра при создании или редактировании ВМ, параметры аппаратных составляющих будут заполнены автоматически. Это даёт пользователям возможность создавать множество ВМ с одними и теми же аппаратными компонентами без необходимости ручного заполнения каждого пункта.

По умолчанию доступен набор предварительно настроенных типов экземпляров, показанных в таблице ниже:

**Таблица 1.13. Предварительно настроенные типы экземпляров**

|  |  |  |
| --- | --- | --- |
| **Название** | **Память** | **Виртуальных ЦП** |
| Tiny | 512 Мбайт | 1 |
| Small | 2 Гбайт | 1 |
| Medium | 4 Гбайт | 2 |
| Large | 8 Гбайт | 2 |
| XLarge | 16 Гбайт | 4 |

Администраторы также могут создавать, редактировать и удалять типы экземпляров из вкладки **Типы экземпляров** окна **Параметры**.

Рядом с текстовыми полями в окнах **Новая ВМ** и **Параметры виртуальной машины**, привязанными к типам экземпляров, располагаются значки звена цепочки (). При изменении значения в одном из этих полей, виртуальная машина будет откреплена от типа экземпляра, который сменится на **Пользовательский**, а значок сменится на значок разорванного звена ( ). Но если значение будет возвращено, звено цепочки вновь соединится, и снова будет указан выбранный тип экземпляра.

### 1.4.1. Создание типов экземпляров

Администраторы могут создавать новые типы экземпляров, которые затем выбираются пользователями при создании или редактировании ВМ.

**Создание типа экземпляра**

1. Нажмите **Администрирование** → **Параметры**
2. Перейдите на вкладку **Типы экземпляров**.
3. Нажмите **Добавить**.
4. Введите **Название** и **Описание** типа экземпляра.
5. Нажмите **Показать расширенные параметры** и настройте параметры типа экземпляра так, как это необходимо. Параметры, присутствующие в окне **Новый тип экземпляра**, идентичны параметрам в окне **Новая виртуальная машина**, но присутствуют только поля, имеющие отношение к типам экземпляров. См. Приложение A.1.
6. Нажмите **OK**.

Новый тип экземпляра появится во вкладке **Типы экземпляров** в окне **Параметры**, и может быть выбран в выпадающем списке **Тип экземпляра** при создании или изменении ВМ.

### 1.4.2. Изменение типов экземпляров

В окне **Параметры** администраторы могут изменять типы экземпляров.

**Изменение параметров типов экземпляров**

1. Нажмите **Администрирование** → **Параметры**.
2. Перейдите на вкладку **Типы экземпляров**.
3. Выберите изменяемый тип экземпляра.
4. Нажмите **Изменить**.
5. Измените параметры так, как это необходимо.
6. Нажмите **OK**.

Конфигурация типа экземпляра будет обновлена. При создании новой ВМ на базе этого типа экземпляра или же при изменении существующей ВМ, основанной на этом типе экземпляра, будет применяться эта новая конфигурация.

В параметрах существующих ВМ, основанных на этом типе экземпляра, будут показаны поля со значком цепи, и информация в этих полях будет обновлена. Если во время изменения типа экземпляра выполнялись ВМ, то рядом с такими ВМ появится оранжевый значок «Изменения, ожидающие применения», а информация в полях со значком цепи будет обновлена во время следующего перезапуска.

### 1.4.3. Удаление типов экземпляров

**Удаление типа экземпляра**

1. Нажмите **Администрирование** → **Параметры**.
2. Перейдите на вкладку **Типы экземпляров**.
3. Выберите удаляемый тип экземпляра.
4. Нажмите **Удалить**.
5. При наличии ВМ, созданных на основе этого типа экземпляра, появится предупреждающее окно со списком привязанных машин. Чтобы продолжить удаление типа экземпляра, отметьте галочкой пункт **Одобрить действие**. В противном случае нажмите **Отмена**.
6. Нажмите **OK**.

Тип экземпляра будет удалён из списка **Типы экземпляров** и его больше нельзя будет использовать во время создания новых ВМ. Все ВМ, ранее прикреплённые к этому типу экземпляра, теперь будут прикреплены к типу **Пользовательский** (то есть без типа экземпляра).

# 1.5. Пулы адресов MAC

Пулы адресов MAC определяют диапазон(ы) адресов MAC, выделенные для каждого кластера. Пул адресов MAC настраивается для каждого кластера. Используя пулы адресов MAC, система виртуализации Red Hat может автоматически создавать и присваивать адреса MAC новым устройствам в виртуальной сети, что помогает предотвратить дупликацию адресов. Пулы адресов MAC более продуктивно работают с памятью, если все адреса, относящиеся к кластеру, находятся в диапазоне присвоенного пула.

Несколько кластеров могут разделять один и тот же пул адресов MAC, но каждому кластеру присваивается один пул. Система виртуализации Red Hat создаёт изначальный пул адресов MAC, который используется в случае, если не будет присвоено ещё одного пула. Подробности о присвоении кластерам пулов адресов MAC смотрите в Разделе 5.2.1. «Создание нового кластера».

ВНИМАНИЕ

Если сеть разделяют более одного кластера системы виртуализации Red Hat, не полагаетесь только на изначальный пул адресов MAC, так как ВМ каждого кластера попытаются использовать один и тот же диапазон адресов, что приведёт к конфликтам. Для избежания конфликтов адресов MAC проверяйте диапазоны пулов, чтобы каждому кластеру был присвоен уникальный диапазон адресов MAC.

Пул адресов MAC присваивает следующий доступный адрес, следующий за последним адресов, возвращённым в пул. Если в диапазоне не осталось адресов, поиск начинается снова с начала диапазона. При наличии в одном пуле нескольких диапазонов адресов MAC с доступными адресами, диапазоны обслуживают входящие запросы в том же порядке, что и выбираются доступные адреса MAC.

### 1.5.1. Создание пулов адресов MAC

Можно создавать новые пулы адресов MAC.

**Создание пула адресов MAC**

1. Нажмите **Администрирование** → **Параметры**.
2. Перейдите на вкладку **Пулы адресов MAC**.
3. Нажмите **Добавить**.
4. Введите **Название** и **Описание** нового пула адресов MAC.
5. Отметьте галочкой пункт **Разрешить дубликаты**, чтобы разрешить использование в пуле одного и того адреса более одного раза. Пул не будет автоматически использовать дублирующий адрес MAC, но включение параметра, разрешающего дубликаты, означает, что пользователь может вручную использовать дублирующий адрес.

ВНИМАНИЕ

Если в одном пуле дубликаты разрешены, а в другом — нет, то каждый адрес MAC может один раз использоваться в пуле с запрещёнными дубликатами, и много раз – в пуле с разрешёнными.

1. Укажите требуемые **Диапазоны адресов MAC**. Для указания нескольких диапазонов нажмите кнопку с плюсом рядом с полями **От** и **До**.
2. Нажмите **OK**.

### 1.5.2. Изменение пулов адресов MAC

Администраторы могут изменять пулы адресов MAC, включая такие детали, как диапазон адресов, доступных в пуле, а также разрешение или запрещение дубликатов

**Изменение параметров пулов адресов MAC**

1. Нажмите **Администрирование** → **Параметры**.
2. Перейдите на вкладку **Пулы адресов MAC**.
3. Выберите изменяемый пул.
4. Нажмите **Изменить**.
5. Необходимым образом измените поля **Название**, **Описание**, **Разрешить дубликаты** и **Диапазоны адресов MAC**.

ВНИМАНИЕ

При обновлении диапазона адресов MAC, адреса существующих NIC повторно не присваиваются. Адреса MAC, уже присвоенные, но находящиеся вне нового диапазона, добавляются как адреса MAC, присвоенные пользователем, и по-прежнему отслеживаются этим пулом.

1. Нажмите **OK**.

### 1.5.3. Изменение полномочий на пулы адресов MAC

После создания пула адресов MAC можно изменить полномочия пользователей пула. Полномочия пользователей определяют, какие дата-центры могут использовать пул адресов MAC. Подробности о добавлении новых полномочий пользователям смотрите в Разделе 1.1. «Роли».

**Изменение полномочий на пул адресов MAC**

1. Нажмите **Администрирование** → **Параметры**.
2. Перейдите на вкладку **Пулы адресов MAC**.
3. Выберите нужный пул.
4. Измените полномочия пользователей для этого пула:
   * Чтобы добавить полномочия на пул адресов MAC:
     1. На панели полномочий пользователей в нижней части окна **Параметры** нажмите на кнопку **Добавить**.
     2. Найдите и выберите нужных пользователей.
     3. В выпадающем списке **Присвоить роль:** выберите нужную роль.
     4. Чтобы добавить полномочия пользователям, нажмите **OK**.
   * Чтобы удалить полномочия пользователей на пул адресов MAC:
     1. Выберите удаляемые полномочия на панели полномочий пользователей в нижней части окна **Параметры**.
     2. Чтобы удалить полномочия пользователей, нажмите **Удалить**.

### 1.5.4. Удаление пулов адресов MAC

Созданный пул адресов MAC, не связанный с кластером, можно удалить, но пул по умолчанию удалить нельзя.

**Удаление пула адресов MAC**

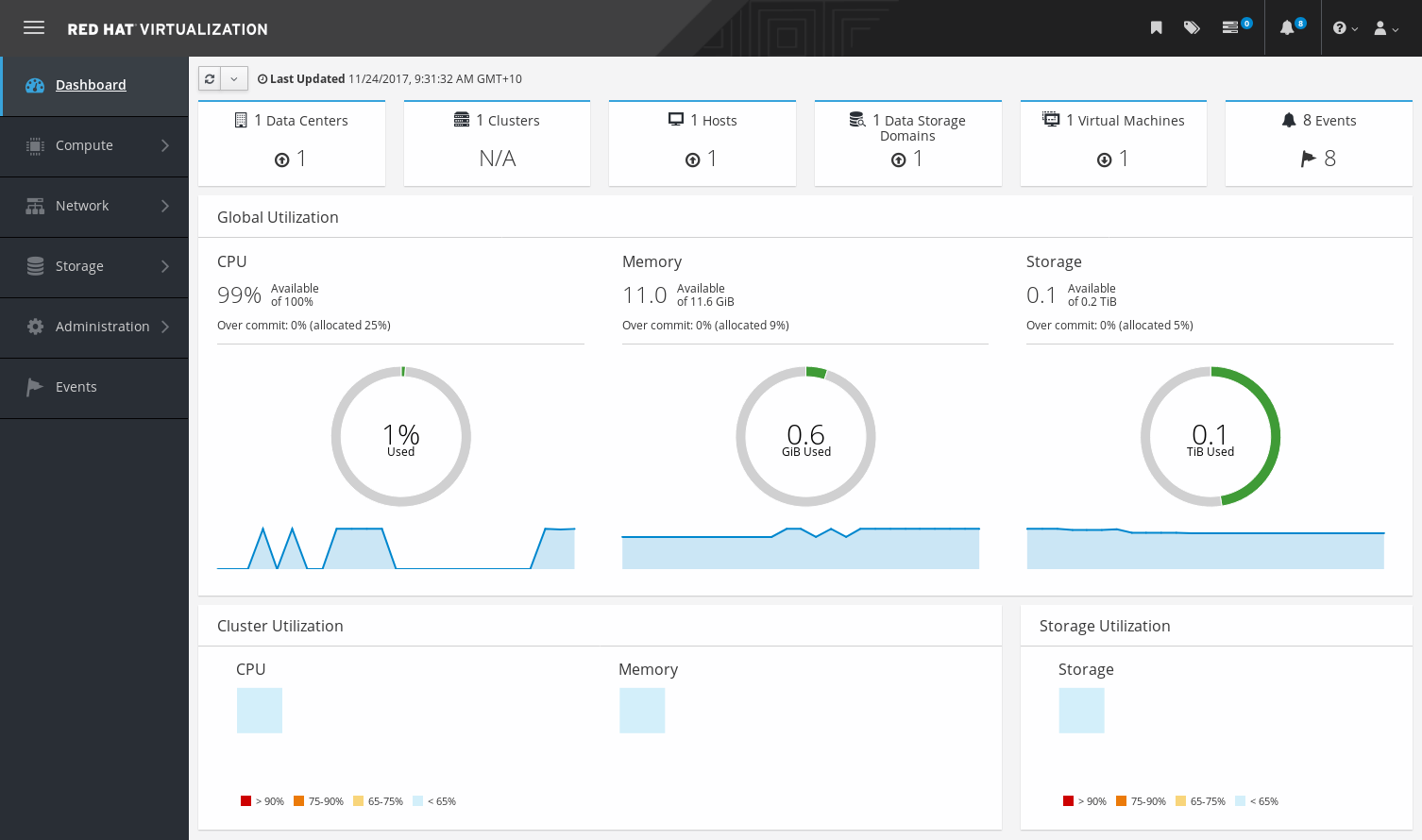
1. Нажмите **Администрирование** → **Параметры**.
2. Перейдите на вкладку **Пулы адресов MAC**.
3. Выберите удаляемый пул.
4. Нажмите **Удалить**.
5. Нажмите **OK**.

# Глава 2. Панель мониторинга

Панель мониторинга предлагает общий обзор состояния системы виртуализации Red Hat с помощью сводки сведений о её ресурсах и общем коэффициенте использования. Эта сводка может предупредить о проблеме и даёт возможность проанализировать проблемную область.

Новая информация поступает на панель каждые 15 минут (по умолчанию) из хранилища данных, и каждые 15 секунд (по умолчанию) из API диспетчера виртуализации, или же при обновлении информации на панели. Информация на панели обновляется во время перехода пользователя на панель с другой страницы или же при ручном обновлении. Информация на панели мониторинга не обновляется автоматически. Информация инвентарной карточки поступает от API диспетчера виртуализации, а сведения об загруженности ресурсов — из хранилища данных. Панель мониторинга реализована в виде расширения для графического интерфейса, которое автоматически устанавливается и обновляется вместе с диспетчером.

**Рисунок 2.1. Панель мониторинга**

****

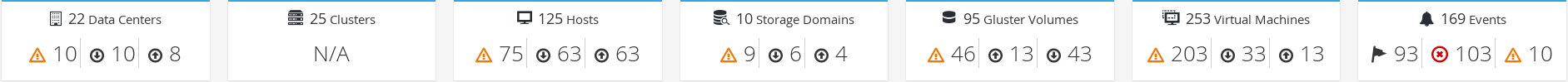
## 2.1. Предварительные условия для установки

Для панели мониторинга необходимо установленное и настроенное хранилище данных. Смотрите <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.0/html-single/data_warehouse_guide/index#chap-Installing_and_Configuring_Data_Warehouse>

**2.2. Общий перечень**

Самый верхний раздел панели мониторинга предлагает общий перечень ресурсов системы виртуализации Red Hat, в который входят разделы для дата-центров, кластеров, хостов, доменов хранилищ, виртуальных машин и событий. Значки показывают состояние каждого ресурса, а числа — количество ресурсов с этим статусом.

**Рисунок 2.2. Общий перечень**



Заголовок показывает номер типа ресурса, а его статус показывается под заголовком. Нажав на ресурс, можно перейти на соответствующую страницу диспетчера виртуализации. Статус кластеров всегда показывается как «Недоступно».

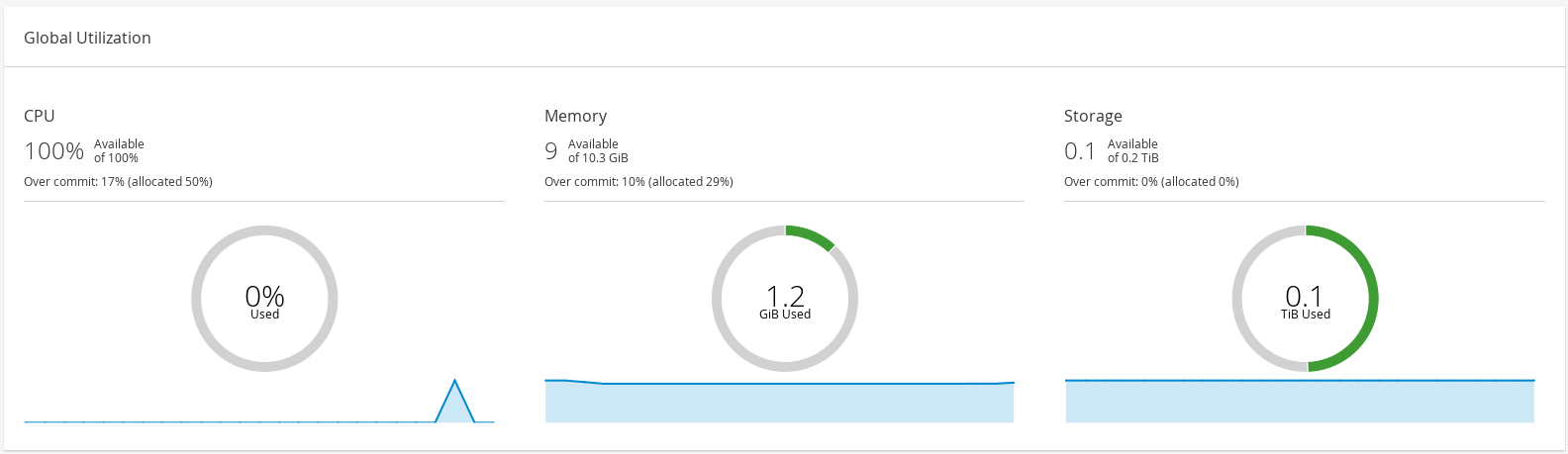
**Таблица 2.1. Статусы ресурсов**

|  |  |
| --- | --- |
| **Значок** | **Статус** |
|  | Ни один из этих ресурсов не был добавлен в систему виртуализации Red Hat. |
|  | Показывает число ресурсов с статусом предупреждения. Нажатие на значок переносит на соответствующую страницу с поиском, ограниченным только данным ресурсом со статусом предупреждения. У каждого поиска по ресурсу имеются свои ограничения:   * **Дата-центры**: поиск ограничен дата-центрами со статусами *в нерабочем состоянии* и *не отвечает*. * **Тома Gluster**: поиск ограничен томами gluster со статусами *идёт запуск*, *работа приостановлена*, *идёт миграция*, *ожидание*, *заморожено* или *идёт выключение*. * **Хосты**: поиск ограничен хостами со статусами *не назначен*, *в режиме обслуживания*, *идёт установка*, *идёт перезагрузка*, *подготовка к обслуживанию*, *ожидает утверждения* или *идёт подключение*. * **Домены хранилищ**: поиск ограничен доменами хранилищ со статусами *не инициализирован*, *не присоединён*, *неактивен*, *в режиме обслуживания*, *подготовка к обслуживанию*, *отсоединение* или *активация*. * **Виртуальные машины**: поиск ограничен машинами со статусом *идёт запуск*, *работа приостановлена*, *идёт миграция*, *ожидание*, *заморожена* или *идёт выключение*. * **События**: поиск ограничен сеьёзностью предупреждения. |
|  | Показывает число ресурсов со статусом *запущен*. Нажатие на значок переносит на соответствующую страницу с поиском, ограниченным запущенными ресурсами. |
|  | Показывает число ресурсов со статусом «не запущен». Нажатие на значок переносит на соответствующую страницу с поиском, ограниченным только данным ресурсом со статусом «не запущен». У каждого поиска по ресурсу имеются свои ограничения:   * **Дата-центры**: поиск ограничен дата-центрами без инициализации, в режиме обслуживания или незапущенными. * **Тома Gluster**: поиск ограничен неактивными или отсоединёнными томами * **Хосты**: поиск ограничен хостами не отвечающими, с ошибкой, с ошибкой инсталляции, в нерабочем состоянии, в процессе инициализации или не запущенными. * **Домены хранилищ**: поиск ограничен отсоединёнными или неактивными доменами хранилищ * **Виртуальные машины**: поиск ограничен машинами незапущенными, не отвечающими или в перезагрузке. |
|  | Показывает число событий с оповещениями о состоянии. Нажатие на значок переносит на страницу **События** с поиском, ограниченным серьёзностью оповещения. |
|  | Показывает количество событий с ошибкой. Нажатие на значок переносит на страницу **События** с поиском, ограниченным серьёзностью ошибки |

# 2.3. Общий коэффициент использования

Раздел **Общее использование** показывает коэффициент использования ЦП, памяти и хранилища.

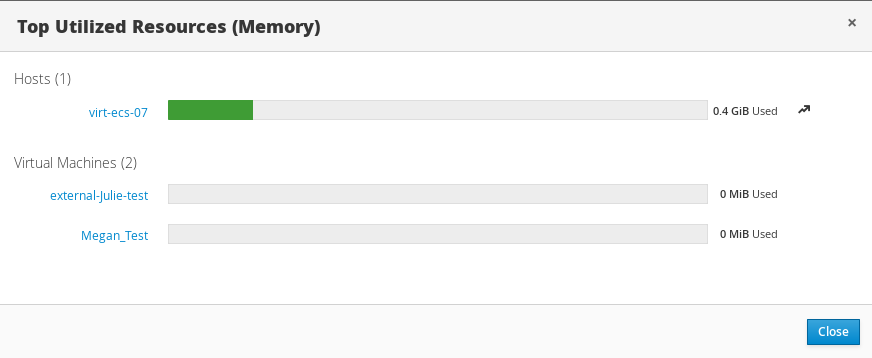
**Рисунок 2.3. Общее использование**



* В верхнем разделе показывается процент доступных ресурсов ЦП, памяти или хранилища, а также процент превышенного выделения ресурсов. Процент превышенного выделения ресурсов ЦП, например, рассчитывается при помощи деления числа виртуальных ядер на число физических ядер, доступных для выполняющихся ВМ, на основании самых свежих данных в хранилище данных.
* На круговых графиках отображаются процентные значения использования ЦП, памяти или хранилища, а также среднее потребление для всех хостов на основе среднего потребления за последние 5 минут. Наведение курсора мыши на сегмент кругового графика покажет значение выделенного сегмента.
* Линейный график в нижней части отображает тенденции за последние 24 часа. Каждая точка данных показывает среднее потребление за указанный час. Наведение курсора на точку графика покажет время и процентное использование для графика ЦП и объём использования для графиков памяти и хранилища.

### 2.3.1. Наиболее используемые ресурсы

**Рисунок 2.4. Наиболее используемые ресурсы (память)**

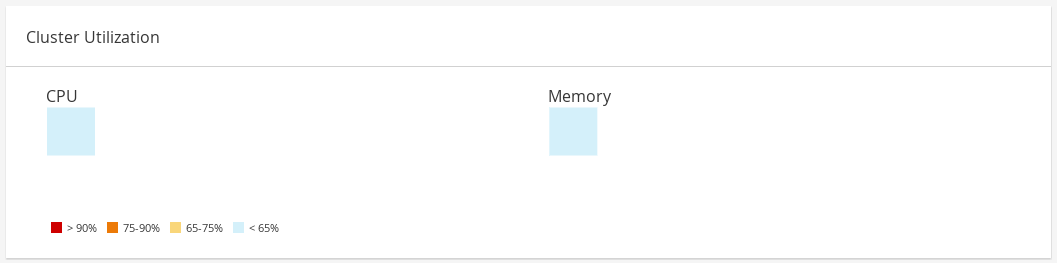


Нажатие на круговой график в разделе общего использования панели мониторинга покажет список наиболее используемых ресурсов ЦП, памяти или хранилища. Для ЦП и памяти всплывающий список показывает десять хостов и ВМ с наиболее высоким потреблением. Для хранилища всплывающий список покажет десять наиболее используемых доменов хранилищ и ВМ. Стрелка справа от панели использования показывает тенденции потребления этого ресурса за последнюю минуту.

# 2.4. Использование кластера

В разделе **Использование кластера** на тепловой карте отображается использование ЦП и памяти.

**Рисунок 2.5. Использование кластера**



### 2.4.1. ЦП

Тепловая карта использования ЦП конкретного кластера, показывающая средний процент использования ЦП за последние 24 часа. Наведение курсора на тепловую карту показывает название кластера. Нажатие на тепловую карту переносит в меню **Вычисления → Хосты** с результатами поиска по конкретному кластеру с фильтром использования ЦП. Расчёты для нахождения общего среднего использования ЦП на кластер делаются с использованием среднего процента нагрузки ЦП для каждого хоста за последние 24 часа.

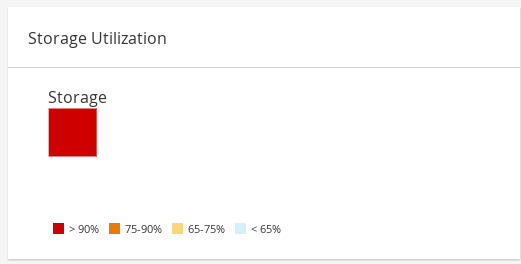
### 2.4.2. Память

Тепловая карта использования памяти конкретного кластера, показывающая средний процент использования памяти за последние 24 часа. Наведение курсора на тепловую карту показывает название кластера. Нажатие на тепловую карту переносит в меню **Вычисления → Хосты** с результатами поиска по конкретному кластеру с фильтром использования памяти. Расчёты для нахождения общего среднего использования памяти на кластер в Гбайт делаются с использованием среднего процента нагрузки памяти для каждого хоста за последние 24 часа.

# 2.5. Использование хранилища

В разделе **Использование хранилища** на тепловой карте показывается процент использования хранилища.

**Рисунок 2.6. Использование хранилища**



Тепловая карта показывает средний процент использования хранилища за последние 24 часа. Формула, используемая для расчёта использования хранилища — общее использование хранилища в кластере. Расчёты для нахождения общего среднего использования хранилища кластером делаются с использованием среднего процента использования хранилища для каждого хоста за последние 24 часа. Наведение курсора на тепловую карту показывает название домена хранилища. Нажатие на тепловую карту переносит в меню **Хранилище → Домены** с доменами хранилищ, отсортированными по проценту.

# Часть II. Администрирование ресурсов

# Глава 3. Качество обслуживания

Система виртуализации Red Hat даёт возможность создать записи качества обслуживания, предоставляющие тонкую настройку контроля уровня входа и выхода, обработки данных и возможностей сети, к которым получают доступ ресурсы окружения. Записи качества обслуживания определяются на уровне дата-центра и присваиваются профилям, созданным в кластерах и доменах хранилищ. Профили далее присваиваются конкретным ресурсам в кластерах и доменах хранилищ, в которых эти профили были созданы.

## 3.1. Качество обслуживания хранилищ

Качество обслуживания хранилища определяет максимальный уровень скорости обработки информации и максимальный уровень операций ввода и вывода для виртуального диска в домене хранилища. Присвоение качества обслуживания хранилища диску даёт возможность тонкой настройки производительности доменов хранилищ и а также возможность предотвратить влияние операций, связанных с одним виртуальным диском, на доступность возможностей хранилища для других виртуальных дисков, размещённых в том же домене хранилища.

### 3.1.1. Создание записи о качестве обслуживания хранилища

**Создание записи о качестве обслуживания в хранилище**

1. Нажмите **Вычисления** **→ Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра
3. Перейдите на вкладку **QoS**.
4. В разделе **Хранилище** нажмите **Добавить**.
5. Укажите **Название QoS** и **Описание** для записи качества обслуживания.
6. Укажите **Пропускную способность** качества обслуживания, отметив один из переключателей:
   * **Нет**
   * **Общая** – укажите максимально разрешённую общую пропускную способность в поле **Мбит/сек**.
   * **Чтение/запись** — укажите максимально разрешённую общую пропускную способность для операций чтения в левом поле **Мбит/сек**, и максимально разрешённую общую пропускную способность для операций записи в правом поле **Мбит/сек**.
7. Укажите качество обслуживания ввода и вывода (**IOps**), отметив один из переключателей:
   * **Нет**
   * **Всего** — укажите максимальное разрешённое число операций ввода и вывода в секунду в поле **IOps**
   * **Чтение/запись** — укажите максимальное разрешённое число операций ввода в секунду в левом поле **IOps**, и максимальное разрешённое число операций вывода в секунду в правом поле **IOps**
8. Нажмите **OK**.

Мы создали запись качества обслуживания для хранилища и на основе этой записи можем теперь создавать профили дисков в доменах хранилища данных, принадлежащих этому дата-центру.

### 3.1.2. Удаление записи о качестве обслуживания хранилища

Удалите существующую запись QoS хранилища.

**Удаление записи качества обслуживания для хранилища**

1. Нажмите **Вычисления** **→ Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS**.
4. В разделе **Хранилище** выберите запись качества обслуживания этого хранилища и нажмите **Удалить**.
5. Нажмите **OK**.

Если на основе этой записи были ранее созданы какие-либо профили дисков, то для этих профилей автоматически устанавливается запись QoS [unlimited].

# 3.2. Качество обслуживания сети виртуальной машины

Качество обслуживания сети ВМ это возможность, позволяющая создавать профили ка для ограничения входящего, так и для ограничения исходящего трафика отдельного контроллера сетевого интерфейса. С помощью той возможности можно ограничивать пропускную способность на нескольких уровнях, контролируя потребление сетевых ресурсов.

### 3.2.1. Создание записи о качестве обслуживания сети ВМ

Создание записи о качестве обслуживания сети ВМ для регулирования сетевого трафика при применении профиля контроллера виртуального сетевого интерфейса (vNIC), также известного как профиль интерфейса сети виртуальной машины.

**Создание записи о качестве обслуживания сети ВМ**

1. Нажмите **Вычисления** **→ Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS**.
4. В разделе **Сеть ВМ** нажмите **Добавить**.
5. Введите **Название** записи QoS сети ВМ.
6. Укажите лимиты для **Входящего** и **Исходящего** сетевого трафика.
7. Нажмите **OK**.

Мы создали записи QoS сети ВМ, которую может использовать контроллер сетевого интерфейса виртуальной сети.

### 3.2.2. Объяснение параметров в окнах «Добавить QoS для сети ВМ» и «Изменить QoS для сети ВМ»

Параметры качества обслуживания сети ВМ дают возможность настроить лимиты пропускной полосы как для входящего, так и для исходящего трафика на трёх разных уровнях.

**Таблица 3.1. Параметры QoS сети виртуальной машины**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата-центр | Дата-центр, в который будет добавлена политика QoS сети ВМ. Это поле настраивается автоматически согласно выбранному дата-центру. |
| Название QoS | Название, представляющее политику QoS сети виртуальной машины в виртуализированном ЦУ. |
| Входящий | Параметры, применяемые ко входящему трафику. Поставьте или снимите галочку с поля **Входящий** для включения или отключения этих параметров.   * **Средняя**: средняя скорость входящего трафика. * **Пиковая**: скорость входящего трафика в период пиковой нагрузки. * **Пиковый всплеск**: скорость входящего трафика во время пиковых всплесков. |
| Исходящий | Параметры, применяемые ко исходящему трафику. Поставьте или снимите галочку с поля **Исходящий** для включения или отключения этих параметров.   * **Средняя**: средняя скорость исходящего трафика. * **Пиковая**: скорость исходящего трафика в период пиковой нагрузки. * **Пиковый всплеск**: скорость исходящего трафика во время пиковых всплесков. |

Чтобы сменить максимальное значение, разрешаемое в полях **Средняя**, **Пиковая** или **Пиковый всплеск**, используйте команду engine-config для изменения ключей конфигурации MaxAverageNetworkQoSValue, MaxPeakNetworkQoSValue или MaxBurstNetworkQoSValue. Для применения внесённых изменений необходимо перезапустить службу **ovirt-engine**. Например:

# engine-config -s MaxAverageNetworkQoSValue=2048

# systemctl restart ovirt-engine

### 3.2.3. Удаление записи о качестве обслуживания сети ВМ

Удалите существующую запись QoS сети виртуальной машины.

**Удаление записи о качестве обслуживания сети ВМ**

1. Нажмите **Вычисления** **→ Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS**.
4. В разделе **Сеть ВМ** выберите запись QoS сети виртуальной машины и нажмите **Удалить**.
5. Нажмите **OK**.

# 3.3. Качество обслуживания сетей хоста

Качество обслуживания сетей хоста реализует контроль сетевого трафика на физических интерфейсах сетей хоста. Качество обслуживания сети хоста позволяет тонкую настройку производительности сети, контролируя потребление сетевых ресурсов на физическом сетевом контроллере. Таким образом можно предотвратить ситуации, когда из-за загруженности трафика какой-то одной сети, другие сети на том же физическом сетевом интерфейсе не могут функционировать. При настроенном качестве обслуживания сетей хоста эти сети смогут функционировать на одном и том же физическом сетевом контроллере без проблем, вызываемых перегрузкой.

### 3.3.1. Создание записи о качестве обслуживания для сетей хоста

Создайте запись о качестве обслуживания для сетей хоста.

**Создание записи о качестве обслуживания для сетей хоста**

1. Нажмите **Вычисления** **→ Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS**.
4. В разделе **Сеть хоста** нажмите **Добавить**.
5. Введите **Название** **QoS** и описание для записи о качестве обслуживания.
6. Укажите нужные значения **Взвешенной доли**, **Предела скорости [Мбит/с]** и **Гарантированной скорости [МБ/с]**.
7. Нажмите **OK**.

### 3.3.2. Объяснение параметров в окнах «Добавить QoS для сетей хоста» и «Изменить QoS для сетей хоста »

Параметры QoS сетей хоста дают возможность настроить лимиты пропускной способности для исходящего трафика.

**Таблица 3.2. Параметры QoS сетей хоста**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата-центр | Дата-центр, в который будет добавлена политика QoS сетей хоста. Это поле настраивается автоматически согласно выбранному дата-центру. |
| Название QoS | Название, представляющее политику QoS в виртуализированном ЦУ. |
| Описание | Описание политики QoS сетей хоста. |
| Исходящий | Параметры, которые будут применяться к исходящему трафику.   * **Взвешенная доля**: определяет, какую долю пропускной способности логического канала нужно выделить для конкретной сети относительно других сетей, привязанных к тому же логическому каналу. Точная доля зависит от суммы долей всех сетей на этом канале. По умолчанию, это число в диапазоне от 1 до 100. * **Предел скорости [Мбит/с]**: максимальная пропускная способность, используемая сетью. * **Гарантированная скорость [МБ/с]**: минимальная пропускная способность, требуемая для сети. Запрошенная скорость не является гарантированной и будет меняться в зависимости от сетевой инфраструктуры и гарантированных скоростей, запрошенных другими сетями на том же логическом канале. |

Чтобы сменить максимальное значение, разрешённое в полях **Предел скорости [Мбит/с]** и **Гарантированная скорость [МБ/с]**, измените значение ключа конфигурации MaxAverageNetworkQoSValue с помощью команды engine-config. Для применения внесённых изменений необходимо перезапустить службу **ovirt-engine**. Например:

# engine-config -s MaxAverageNetworkQoSValue=2048

# systemctl restart ovirt-engine

### 3.3.3. Удаление записи о качестве обслуживания для сетей хоста

Удалите существующую запись QoS сети.

**Удаление записи о качестве обслуживания сетей хоста**

1. Нажмите **Вычисления** **→ Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS**.
4. В разделе **Сеть хоста** выберите запись о качестве обслуживания и нажмите **Удалит**ь.
5. По запросу нажмите **OK**.

# 3.4. Качество обслуживания ЦП

Качество обслуживания центрального процессора определяет максимальный объём вычислительной мощности хоста, к которому может получить доступ выполняющаяся на хосте ВМ, выраженный в проценте от общей вычислительной мощности, доступной на этом хосте. Присвоение QoS для ЦП виртуальной машине даёт возможность предотвратить влияние загруженности одной ВМ в кластере на вычислительные мощности, доступные другим ВМ в этом кластере.

### 3.4.1. Создание записи качества обслуживания для ЦП

Создайте запись QoS для центрального процессора.

**Создание записи о качестве обслуживания для центрального процессора**

1. Нажмите **Вычисления** **→ Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS**.
4. В разделе **ЦП** нажмите **Добавить**.
5. Введите **Название** **QoS** и описание для записи о качестве обслуживания.
6. В поле **Ограничение (%)** введите максимальную вычислительную возможность, разрешаемую записью QoS. Не указывайте символ %.
7. Нажмите **OK**.

Мы создали запись о качестве обслуживания для ЦП и теперь можем на основе этой записи создавать профили ЦП в кластерах, принадлежащих этому дата-центру.

### 3.4.2. Удаление записи качества обслуживания для ЦП

Удалите существующую запись QoS для ЦП.

**Удаление записи QoS для центрального процессора**

1. Нажмите **Вычисления** **→ Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS**.
4. В разделе **ЦП** выберите нужную запись QoS для ЦП и нажмите **Удалить**.
5. Нажмите **OK**.

Если на основе этой записи были ранее созданы какие-либо профили ЦП, то для этих профилей автоматически устанавливается запись [unlimited].

# Глава 4. Дата-центры

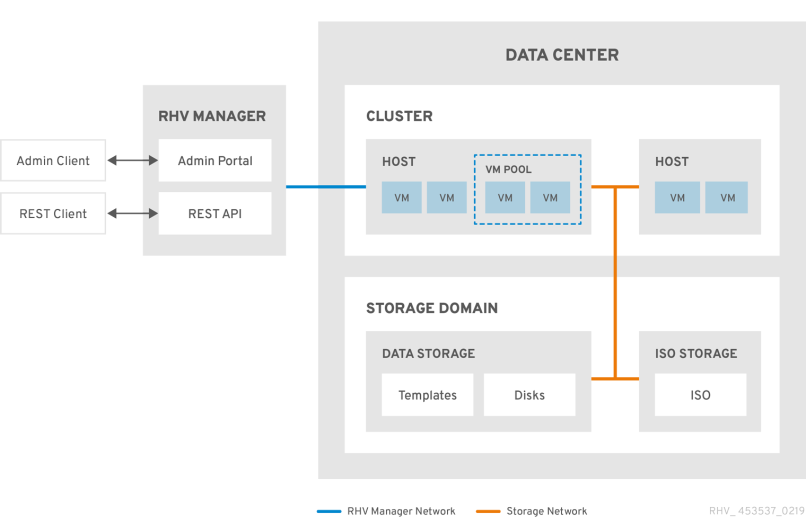
## 4.1. Введение в понятие дата-центров

Дата-центр – это логический объект, определяющий набор ресурсов, используемых в конкретном окружении. Дата-центр считается контейнерным ресурсом, состоящим из логических ресурсов в виде кластеров и хостов; сетевых ресурсов в виде логических сетей и физических сетевых контроллеров; а также ресурсов хранения в виде доменов хранилищ.

Дата-центр может содержать несколько кластеров, каждый их которых может содержать несколько хостов; у дата-центров может быть несколько связанных с ним доменов хранилищ; а также он может поддерживать несколько виртуальных машин на каждом из свих хостов. В окружении системы виртуализации Red Hat может находиться несколько дата-центров; инфраструктура дата-центров даёт возможность управлять ими отдельно друг от друга.

Все дата-центры управляются из одного Портала администрирования.

**Рисунок 4.1. Дата-центры**



Во время установки система виртуализации Red Hat создаёт дата-центр по умолчанию. Можно настроить дата-центр по умолчанию или же создать новые дата-центры с подходящими названиями.

# 4.2. Диспетчер пула хранилища (SMP)

Диспетчер пула хранилища (Storage Pool Manager, SPM) — это роль с возможностью управления доменами хранилищ в дата-центре, выделяемая одному из хостов дата-центра. Объект SPM может работать на любом хосте дата-центра; виртуализированный ЦУ присваивает эту роль одному из хостов. Роль SPM не исключает выполнения хостом стандартных операций; на хосте, выполняющем роль диспетчера пула хранилища, по-прежнему могут располагаться виртуальные ресурсы.

Объект диспетчера пула хранилища контролирует доступ к хранилищу, координируя метаданные со всех доменов хранилищ. Это включает в себя создание, удаление и выполнение действий с виртуальными дисками (образами), снимками и шаблонами, а также выделение хранилища для разреженных блочных устройств (в сети хранения данных). Это исключительная ответственность: для обеспечения целостности метаданных только один хост может быть диспетчером пула хранилища в текущий момент времени.

Виртуализированный ЦУ обеспечивает постоянную доступность диспетчера пула хранилища. В случае, если у хоста SPM возникнут проблемы с доступом к хранилищу, виртуализированный ЦУ передаёт роль SPM другому хосту. При запуске диспетчера пула хранилища виртуализированный ЦУ гарантирует, что этот хост будет единственным, выполняющим эту роль; соответственно, он получит хранилище-ориентированную аренду. Этот процесс может занять некоторое время.

↑ therefore it will acquire a storage-centric lease

# 4.3. Приоритет диспетчера пула хранилища (SMP)

Роль диспетчера пула хранилища использует некоторые доступные ресурсы хоста. Параметр приоритета SPM для хоста изменяет возможность присвоения хосту роли SPM: хосту с высоким приоритетом SPM эта роль будет присвоена ранее хоста с низким приоритетом SPM. Критически важные виртуальные машины на хостах с низким приоритетом SPM не будут вынуждены конкурировать за ресурсы хоста с операциями диспетчера пула хранилища.

Приоритет SPM для хоста можно изменить на вкладке **SPM** в окне **Параметры хоста**.

# 4.4. Задачи при работе с дата-центрами

### 4.4.1. Создание нового дата-центра

Данная процедура создаёт дата-центр в окружении системы виртуализации. Для работы дата-центра нужен функционирующий кластер, хост и домен хранилища.

ВНИМАНИЕ

*Версию совместимости* нельзя будет понизить после её указания; регрессия версий не разрешается.

Возможность указать диапазон адресов MAC для дата-центра была отключена, теперь это выполняется на уровне кластера.

**Создание нового дата-центра**

1. Нажмите **Вычисления** **→ Дата-центры**.
2. Нажмите **Добавить**.
3. Укажите **Название** и **Описание** дата-центра.
4. В выпадающих меню выберите **Тип хранилища**, **Версию совместимости** и **Режим квоты** дата-центра.
5. Для создания дата-центра нажмите **OK** и перейдите в окно **Дата-центр — пошаговый помощник**.
6. В окне пошагового помощника присутствует список объектов дата-центра, которые необходимо настроить. Настройте их или отложите настройку, нажав на кнопку **Настроить позже**. Возобновить процесс настройки можно, выбрав дата-центр и перейдя по пунктам меню значка **Больше действий** () → **Пошаговый помощник**.

Новый дата-центр будет иметь статус **Не инициализирован** до тех пор, пока для него не будут настроены кластер, хост и домен хранилища; для настройки этих объектов используйте **Пошаговый помощник**.

### 4.4.2. Объяснение параметров в окнах «Новый дата-центр» и «Параметры дата-центра».

В таблице ниже описываются параметры дата-центра, присутствующие в окнах **Новый дата-центр** и **Параметры дата-центра**. При попытке нажать **OK** недействительные элементы обводятся оранжевым, запрещая применение изменений. Кроме того, в полях ввода указываются ожидаемые значения или диапазон значений.

**Таблица 4.1. Свойства дата-центра**

|  |  |
| --- | --- |
| **Поле** | **Описание/действие** |
| Название | Название дата-центра. 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. |
| Описание | Описание дата-центра. Заполнение этого поле рекомендуется, но не обязательно. |
| Тип хранилища | Выберите **Разделяемый** или **Локальный** тип хранилища.  В один и тот же дата-центр можно добавить различные типы доменов хранилищ (iSCSI, NFS, FC, POSIX, Gluster). Тем не менее, локальные и разделяемые домены нельзя смешивать.  Изменить тип хранилища можно после инициализации дата-центра. Смотрите Раздел 4.4.6. |
| Версия совместимости | Версия системы виртуализации Red Hat  После обновления виртуализированного ЦУ до новой версии, хосты, кластеры и дата-центры по-прежнему могут иметь более раннюю версию. Перед обновлением до новой версии **Уровня совместимости** дата-центра убедитесь в том, что были обновлены версии всех хостов, а затем кластеров. |
| Режим квоты | Quota — это инструмент ограничения использования ресурсов в составе системы виртуализации Red Hat. Выберите одно из следующего:   * **Отключено**: выберите, если не нужно использовать квоты * **Аудит**: выберите, если нужно изменить параметры квоты * **Принудительно**: выберите для применения квоты |
| Комментарий | По желанию добавьте комментарий о дата-центре в простом текстовом формате. |

### 4.4.3. Повторная инициализация дата-центра: процедура восстановления

Данная процедура восстановления заменяет домен мастер-данных дата-центра новым доменом мастер-данных. Если данные домена мастер-данных повреждены, то его надо инициализировать повторно. Повторная инициализация дата-центра даст возможность восстановить все другие ресурсы, связанные с дата-центром, включая кластеры, хосты и не проблемные домены хранилищ.

В новый домен мастер-данных можно импортировать ВМ или шаблоны из резервных копий или экспортированные ВМ и шаблоны.

**Повторная инициализация дата-центра**

1. Нажмите **Вычисления** → **Дата-центры** и выберите нужный дата-центр.
2. Убедитесь в том, что любые домены хранилищ, присоединённые к дата-центру, находятся в режиме обслуживания.
3. Нажмите значок **Больше действий** (), затем пункт **Повторно инициализировать дата-центр**.
4. В окне **Повторная инициализация дата-центра** располагается список всех доступных (отсоединённых; в режиме обслуживания) доменов хранилищ. Поставьте отметку для домена хранилища, добавляемого в дата-центр.
5. Отметьте галочкой пункт **Подтвердить операцию**.
6. Нажмите **OK**.

Домен хранилища присоединён к дата-центру в качестве домена мастер-данных и активирован. Теперь в новый домен мастер-данных можно импортировать любые экспортированные ВМ или шаблоны, а также ВМ и шаблоны из резервных копий.

### 4.4.4. Удаление дата-центра

Для удаления дата-центра требуется активный хост. Удаление дата-центра не удалит связанные ресурсы.

**Удаление дата-центра**

1. Убедитесь в том, что домены хранилищ, присоединённые к дата-центру, находятся в режиме обслуживания.
2. Нажмите **Вычисления** → **Дата-центры** и выберите дата-центр, который нужно удалить.
3. Нажмите **Удалить**.
4. Нажмите **OK**.

### 4.4.5. Принудительное удаление дата-центра

Статус Не отвечает присваивается дата-центру, если присоединённый домен хранилища повреждён, или если хост получает статус Не отвечает. В любых других ситуациях **Удалить** дата-центр невозможно.

**Принудительное удаление** не требует активного хоста. Оно также навсегда удаляет присоединённый домен хранилища.

Перед **Принудительным удалением** дата-центра может понадобиться **Уничтожить** повреждённый домен хранилища.

**Принудительное удаление дата-центра**

1. Нажмите **Вычисления** → **Дата-центры** и выберите дата-центр, который нужно удалить.
2. Нажмите на значок **Больше действий** () и далее **Принудительно удалить**.
3. Отметьте галочкой параметр **Одобрить операцию**.
4. Нажмите **OK**

Дата-центр и присоединённый домен хранилища навсегда будут удалены из окружения виртуализации Red Hat.

### 4.4.6. Изменение типа хранилища дата-центра

Сменить тип хранилища дата-центра можно после его инициализации. Это удобно в доменах данных, используемых для перемещения виртуальных машин или шаблонов.

**Ограничения**

* Разделяемый на локальный — для дата-центра, который содержит не более одного хоста и одного кластера, поскольку локальный дата-центр это не поддерживает.
* Локальный на разделяемый — для дата-центра, который не содержит домена локального хранилища.

**Изменение типа хранилища дата-центра**

1. Нажмите **Вычисления** → **Дата-центры** и выберите дата-центр, который нужно изменить.
2. Нажмите **Изменить**.
3. Измените **Тип хранилища** на желаемый тип.
4. Нажмите **OK**.

### 4.4.7. Изменение версии совместимости дата-центра

Дата-центры системы виртуализации Red Hat имеют версию совместимости. Версия совместимости указывает на версию системы виртуализации Red Hat, с которой должен быть совместим дата-центр. Все кластеры в дата-центре должны поддерживать желаемый уровень совместимости.

ВАЖНО

Чтобы сменить версию совместимости дата-центра, нужно сначала обновить версию совместимости всех кластеров и ВМ в дата-центре.

**Последовательность действий**

1. На портале администрирования нажмите **Вычисления** → **Дата-центры**.
2. Выберите изменяемый дата-центр и нажмите **Изменить**.
3. Укажите необходимую **Версию совместимости**.
4. Нажмите **OK**. Будет открыт диалог подтверждения **Изменить версию совместимости дата-центра**.
5. Нажмите **OK** для подтверждения.

# 4.5. Дата-центры и домены хранилищ

### 4.5.1. Присоединение к дата-центру существующего домена данных

Домены данных со статусом **Не присоединён** можно присоединять к дата-центру. Разделяемые домены хранилищ множественных типов (iSCSI, NFS, FC, POSIX и Gluster) можно присоединять к одному и тому же дата-центру.

**Добавление существующего домена данных к дата-центру**

1. Нажмите **Вычисления** → **Дата-центры**
2. Нажмите на название дата-центра чтобы открыть подробные сведения.
3. Перейдите на вкладку **Хранилище**, чтобы просмотреть список доменов, уже присоединённых к дата-центру.
4. Нажмите **Присоединить данные**.
5. Отметьте галочкой домен данных, который нужно присоединить к дата-центру. Можно выбрать несколько доменов данных.
6. Нажмите **OK**.

Домен данных будет присоединён к дата-центру и автоматически активирован.

### 4.5.2. Присоединение к дата-центру существующего домена ISO

Домены ISO со статусом **Не присоединён** можно присоединять к дата-центру. Домен ISO должен иметь тот же **Тип хранилища**, что и дата-центр.

К дата-центру можно присоединить только один домен ISO.

**Добавление существующего домена ISO к дата-центру**

1. Нажмите **Вычисления** → **Дата-центры**.
2. Нажмите на название дата-центра, чтобы открыть подробные сведения.
3. Перейдите на вкладку **Хранилище**, чтобы просмотреть список доменов, уже присоединённых к дата-центру.
4. Нажмите **Присоединить ISO**.
5. Поставьте отметку напротив нужного домена ISO
6. Нажмите **OK**.

Домен ISO будет присоединён к дата-центру и автоматически активирован.

### 4.5.3. Присоединение к дата-центру существующего домена экспорта

ВНИМАНИЕ

Домены экспорта являются устаревшими. Домены хранилищ данных можно отсоединять от дата-центра и импортировать в другой дата-центр в том же или в другом окружении. После этого виртуальные машины, плавающие виртуальные диски и шаблоны можно загрузить из импортированного домена хранилища в присоединённый дата-центр. Сведения об импорте доменов хранилищ смотрите в Разделе 8.7.

Домен экспорта со статусом **Не присоединён** можно присоединять к дата-центру. К дата-центру можно присоединить только один домен экспорта.

**Присоединение существующего домена экспорта к дата-центру**

1. Нажмите **Вычисления** → **Дата-центры**.
2. Нажмите на название дата-центра, чтобы открыть подробные сведения.
3. Перейдите на вкладку **Хранилище**, чтобы просмотреть список доменов, уже присоединённых к дата-центру.
4. Нажмите **Присоединить экспорт**.
5. Поставьте отметку рядом с нужным доменом экспорта.
6. Нажмите **OK**.

Домен экспорта будет присоединён к дата-центру и автоматически активирован.

### 4.5.4. Отсоединение доменов хранилищ от дата-центра

Отсоединение домена хранилища от дата-центра отменяет привязку дата-центра к этому домену. Домен хранилища не удаляется из окружения виртуализации Red Hat; его можно будет присоединить к другому дата-центру.

Данные, такие, как виртуальные машины и шаблоны, остаются присоединёнными к домену хранилища.

ВНИМАНИЕ

Главное хранилище, если это единственный доступный домен хранилища, удалить нельзя.

**Отсоединение домена хранилища от дата-центра**

1. Нажмите **Вычисления** → **Дата-центры**.
2. Нажмите на название дата-центра, чтобы открыть подробные сведения.
3. Перейдите на вкладку **Хранилище**, чтобы просмотреть список доменов, уже присоединённых к дата-центру.
4. Выберите домен хранилища, который надо отсоединить. Если домен Активен, нажмите **Обслуживание**.
5. Нажмите **OK** для запуска режима обслуживания.
6. Нажмите **Отсоединить**.
7. Нажмите **OK**.

Прежде чем домен хранилища исчезнет из отображения подробных сведений, может пройти несколько минут.

# Глава 5. Кластеры

## 5.1. Введение в понятие кластеров

Кластер — это логическое объединение хостов, разделяющих один и тот же домен хранилища и имеющих один и тот же тип ЦП (либо Intel, либо AMD). Если на хостах присутствуют разные поколения моделей ЦП, то в работе используются только возможности, общие для всех моделей.

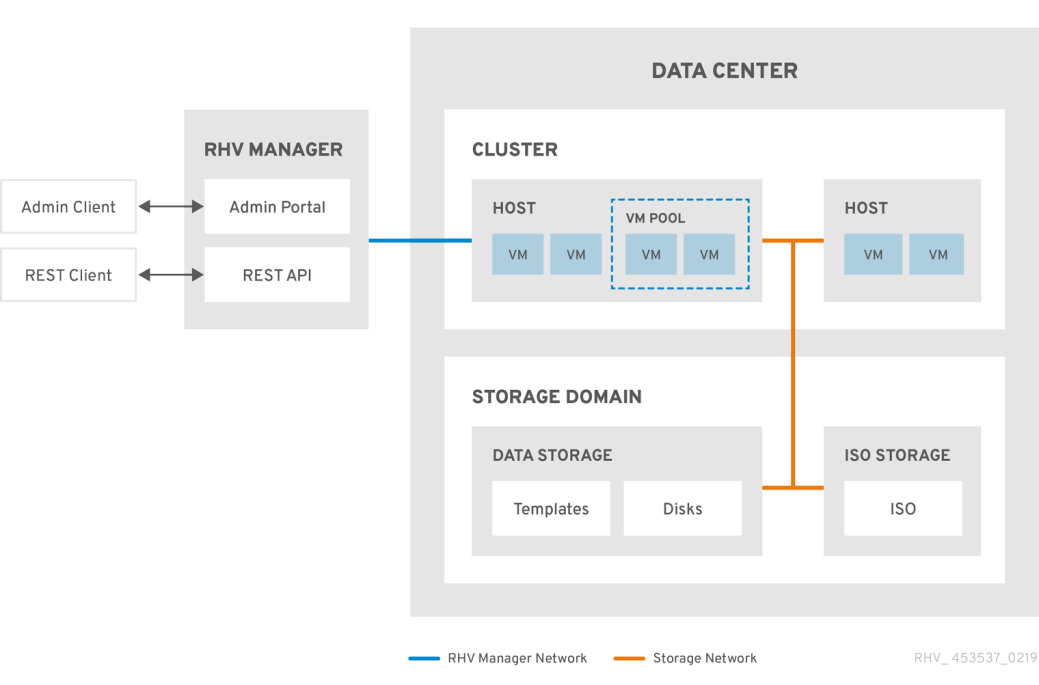
Каждый кластер в системе должен принадлежать дата-центру, а каждый хост в системе должен принадлежать кластеру. Виртуальные машины динамически выделяются каждому хосту в кластере и могут переноситься между ними, согласно политикам, определённым в кластере, и параметрам ВМ. Кластер — это самый высокий из возможных уровней, на которых должны быть настроены политики энергосбережения и распределения нагрузки.

Число хостов и число ВМ, принадлежащих кластеру, отображаются в списках **Число хостов** и **Число ВМ**, соответственно.

На кластерах выполняются виртуальные машины или серверы хранилищ Gluster. Эти два назначения являются взаимоисключающими: один кластер не может поддерживать и виртуализацию и хосты хранилищ.

Во время установки система виртуализации Red Hat создаёт кластер по умолчанию в дата-центре по умолчанию.

**Рисунок 5.1. Кластер**



# 5.2. Задачи при работе с кластерами

ВНИМАНИЕ

Некоторые параметры кластера не применимы к кластерам Gluster. Подробности об использовании хранилищ Gluster смотрите здесь: <https://access.redhat.com/documentation/en-us/red_hat_gluster_storage/3.3/html/configuring_red_hat_virtualization_with_red_hat_gluster_storage/index>

### 5.2.1. Создание нового кластера

В дата-центре может присутствовать несколько кластеров, а кластер может содержать несколько хостов. Все хосты в кластере должны иметь один и тот же тип ЦП (Intel или AMD). Для обеспечения оптимизации типа ЦП рекомендуется создавать хосты до того, как будет создаваться кластер. Тем не менее, хосты можно настроить и позже, с помощью кнопки **Пошаговый помощник**.

**Создание нового кластера**

1. Нажмите **Вычисления → Кластеры**.
2. Нажмите **Добавить**.
3. В выпадающем списке выберите **Дата-центр**, к которому будет принадлежать кластер.
4. Укажите **Название** и **Описание** кластера.
5. В выпадающем списке **Сеть управления** выберите сеть, которой нужно присвоить роль сети управления.
6. В выпадающих списках выберите **Архитектуру ЦП** и **Тип ЦП**. Важно, чтобы семья процессора совпадала с минимальным типом процессора хостов, к которым предполагается присоединить кластер, в противном случае хост будет нерабочим.

ВНИМАНИЕ

Как для типа Intel, так и для типа AMD, указанные в списке модели идут в логическом порядке от самых старых к самым новым. Если в кластер включены хосты с разными моделями ЦП, выбирайте в списке самую старую модель. Подробности о каждой из моделей ЦП смотрите: <https://access.redhat.com/solutions/634853>. +

1. В выпадающем списке выберите **Версию совместимости** кластера.
2. Выберите Тип коммутатора в выпадающем списке
3. Для хостов в кластере выберите **Тип межсетевого экрана**: **iptables** или **firewalld**

ВНИМАНИЕ

iptables является устаревшим типом межсетевого экрана.

1. Отметьте параметр **Включить службу Virt** или **Включить службу Gluster**, чтобы определить, будет ли кластер населён виртуальными машинами или узлами с поддержкой Gluster.
2. При необходимости, отметьте галочкой параметр **Включите, чтобы указать причину обслуживания ВМ**, чтобы администратор мог указывать причину обслуживания ВМ в дополнительном поле во время отключения машины от диспетчера виртуализации.
3. При необходимости, отметьте галочкой параметр **Включите, чтобы указать причину обслуживания хоста**, чтобы администратор мог указывать причину перевода хоста в режим обслуживания в дополнительном поле во время отключения хоста от диспетчера виртуализации.
4. При необходимости, отметьте галочкой параметр **Источник /dev/hwrng (внешнее аппаратное устройство), чтобы указать устройство для создания случайных чисел, которое будут использовать все хосты в кластере. Источник /dev/urandom (устройство Linux) отмечено по умолчанию.**
5. Перейдите на вкладку **Оптимизация** для выбора порога разделяемых страниц памяти в кластере, а также, при необходимости, включите обработку потоков ЦП и вытеснение памяти на хостах в кластере.
6. Перейдите на вкладку **Политика миграции** для настройки политики миграции машин в кластере.
7. Перейдите на вкладку **Политика планирования**, чтобы, при необходимости, настроить политику планирования, указать параметры оптимизации планировщика, включить доверенную службу для хостов в кластере, включить резервирование высокой доступности и добавить частную политику порядковых номеров.
8. Перейдите на вкладку **Консоль**, чтобы, при необходимости, переопределить глобальные параметры прокси SPICE для хостов в кластере.
9. Перейдите на вкладку **Политика операций блокады**, чтобы включить или отключить возможность проведения операций блокады в кластере и выбрать параметры блокады.
10. Нажмите **Пул адресов MAC**, чтобы указать пул, отличный от пула адресов MAC по умолчанию. Подробности о создании, редактировании или удалении пулов адресов MAC смотрите в Разделе 1.5.
11. Нажмите **OK** чтобы создать кластер и запустить окно **Кластер — пошаговый помощник**.
12. В окне **Пошаговый помощник** указан список объектов, для которых необходимо настроить взаимодействие с кластером. Настройте эти объекты или отложите настройку, нажав на кнопку **Настроить позже**. Процесс настройки можно возобновить позднее, выбрав кластер, нажав на значок **Больше действий** () и затем выбрав **Пошаговый помощник**.

### 5.2.2. Объяснение общих параметров кластера

В таблице ниже описываются параметры вкладки Общее в окнах **Новый кластер** и **Параметры кластера**. При попытке нажать **OK** недействительные элементы обводятся оранжевым, запрещая применение изменений. Кроме того, в полях ввода указываются ожидаемые значения или диапазон значений.

**Таблица 5.1. Общие параметры кластера**

|  |  |
| --- | --- |
| **Поле** | **Описание/действие** |
| **Дата-центр** | **Дата-центр, в котором будет располагаться кластер. Дата-центр должен быть создан до создания кластера.** |
| **Название** | Название кластера. 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. |
| **Описание/комментарий** | Описание кластера или дополнительные заметки. Заполнение этих полей рекомендуется, но не обязательно. |
| **Сеть управления** | **Логическая сеть, которой будет присвоена роль сети управления. Значение по умолчанию — ovirtmgmt. Эта сеть также будет использоваться для миграции ВМ, если сеть миграции не присоединена корректным образом к хостам-источникам или целевым хостам.**  **Изменить сеть управления в существующих кластерах можно, только нажав на кнопку Управление сетями на вкладке Логическая сеть в детальном просмотре.** |
| **Архитектура ЦПУ** | Архитектура ЦП в кластере. Типы ЦП показываются в зависимости от выбранной архитектуры.   * **Не определено**: доступны все типы ЦП * **x86\_64**: доступны все типы ЦП Intel и AMD. * **ppc64**: доступен только IBM POWER 8. |
| **Тип ЦП** | Тип ЦП в кластере. Список поддерживаемых моделей ЦП:   * **AMD**    + Opteron G4   + Opteron G5   + EPYC * **Intel**    + Nehalem   + Westmere   + Sandybridge   + Haswell   + Haswell-noTSX   + Broadwell   + Broadwell-noTSX   + Skylake (client)   + Skylake (server) * **IBM POWER8**   **Все хосты в кластере должны иметь тип** Intel, AMD, или IBM POWER 8; после создания кластера тип нельзя изменить без значительных повреждений кластера. Тип ЦП должен быть настроен согласно самой старой модели ЦП в кластере. Будут использоваться только возможности, присутствующие во всех моделях. Как для типов Intel, так и для типов AMD модели указываются в логическом порядке от самых старых к самым новым. |
| **Версия совместимости** | Версия системы виртуализации Red Hat. Нельзя выбрать версию, более раннюю, чем версия, указанная для дата-центра. |
| **Тип коммутатора** | Тип коммутатора, используемый в кластере. Стандартным виртуальным коммутатором в системе виртуализации Red Hat является **Linux Bridge. OVS предлагает поддержку для сетевых возможностей** Open vSwitch. |
| **Тип межсетевого экрана** | **Указывает тип межсетевого экрана для хостов в кластере, это iptables** или **firewalld**.  **ВНИМАНИЕ:** iptables является устаревшим типом.  После смены типа межсетевого экрана в существующем кластере, для применения изменений необходимо переустановить (раздел 7.5.20) все хосты в кластере. |
| **Поставщик сети по умолчанию** | Указывает поставщика внешней сети по умолчанию, который будет использоваться в кластере. При выборе Open Virtual Network (OVN) на хостах, добавленных в кластер, автоматически настраивается обмен данными с поставщиком OVN.  При смене поставщика сети по умолчанию, для применения изменений необходимо переустановить (раздел 7.5.20) все хосты в кластере. |
| **Максимальный порог журналирования потребления памяти** | Указывает порог журналирования для максимального потребления памяти в процентном или абсолютном значении в Мбайт. Сообщение записывается в журнал, если потребление памяти на хосте превышает процентное значение, или если объём доступной на хосте памяти падает ниже абсолютного значения в Мбайт. Значение по умолчанию — 95%. |
| **Включить службу Virt** | Если этот переключатель активирован, то хосты в данном кластере будут использоваться для работы виртуальных машин. |
| **Включить службу Gluster** | Если этот переключатель активирован, то хосты в данном кластере будут использоваться в качестве узлов сервера хранилища Gluster, а не для работы виртуальных машин. |
| **Импортировать существующую конфигурацию Gluster** | Этот флажок появляется только при активации переключателя **Включить службу Gluster. Этот параметр позволяет импортировать в виртуализированный ЦУ уже существующий кластер с поддержкой Gluster и все его присоединённые хосты.**  Каждый из хостов импортируемого кластера должен соответствовать следующим требованиям:   * **Адрес**: укажите IP или полное доменное имя хоста сервера Gluster. * **Отпечаток**: виртуализированный ЦУ получает отпечаток (fingerprint) хоста для гарантии того, что подключение было выполнено к правильному хосту. * **Пароль root**: укажите пароль root, необходимый для обмена информацией с хостом. |
| Включите, чтобы указать причину обслуживания ВМ | Если этот параметр отмечен галочкой, то во время отключения ВМ кластера от виртуализированного ЦУ появится дополнительное поле для указания причины отключения. Это возможность предоставить объяснение причины, по которой выполняется обслуживание. Объяснение будет записано в журнал, а также будет показано после того, как ВМ снова будет включена. |
| Включите, чтобы указать причину обслуживания хоста | Если этот параметр отмечен галочкой, то во время перемещения хоста кластера в режим обслуживания из виртуализированного ЦУ появится дополнительное поле для указания причины. Это возможность предоставить объяснение причины, по которой выполняется обслуживание. Объяснение будет записано в журнал, а также будет показано после того, как хост снова будет активирован. |
| **Дополнительный источник для генератора случайных чисел** | Если этот параметр отмечен галочкой, то для всех хостов в кластере станет доступно дополнительное устройство для генерации случайных чисел. Этот параметр включает сквозную энтропию от устройства, создающего случайные числа, к виртуальным машинам. |

### 5.2.3. Объяснение параметров оптимизации

**Критерии для памяти**

Разделение страниц памяти даёт возможность ВМ использовать до 200% выделенной им памяти, используя свободную память других ВМ. Этот процесс базируется на предположении, что ВМ в окружении системы виртуализации Red Hat не будут работать на полную мощность все одновременно, что даёт возможность временно выделять неиспользуемую память какой-то одной ВМ.

**Критерии для ЦП**

* **Для рабочей нагрузки без серьёзного потребления ресурсов ЦП** виртуальные машины могут работать, имея общее число ядер процессора, превышающее число ядер на хосте. Таким образом активируются следующие возможности:
  + Можно запускать большее число ВМ, что снижает требования к аппаратным составляющим.
  + Можно настраивать ВМ с топологией ЦП, которая в противном случае не была бы возможной, например, когда значение количества виртуальных ядер находится между числом ядер хоста и числом потоков хоста.
* **Для лучшей производительности, и особенно для рабочей нагрузки с серьёзным потреблением ресурсов ЦП для ВМ необходимо использовать ту же топологию, что и на хосте, чтобы и ВМ и хост рассчитывали на одинаковое использование кэша. При включённой на хосте гиперпоточности,** QEMU обрабатывает гиперпотоки хоста как ядра, так что ВМ не знает о том что она выполняется на одном ядре с несколькими потоками. Такое поведение может повлиять на производительность ВМ, поскольку виртуальное ядро, на самом деле соответствующее гиперпотоку ядра хоста, может разделять один и тот же кэш с другим гиперпотоком на том же ядре хоста, в то время как ВМ считает его отдельным ядром.

В таблице ниже описываются параметры вкладки **Оптимизация** в окнах **Новый кластер** и **Параметры кластера**.

**Таблица 5.2. Параметры оптимизации**

|  |  |
| --- | --- |
| **Поле** | **Описание/действие** |
| Оптимизация памяти | * **Отсутствует: отключить превышенное выделение памяти**: отключает общие страницы памяти * **Для нагрузки сервера — разрешить запланировать 150% физической памяти**: устанавливает порог разделения страниц памяти на 150% от системной памяти на каждом хосте. * **Для нагрузки рабочего стола — разрешить запланировать 200% физической памяти**: устанавливает порог разделения страниц памяти на 200% от системной памяти на каждом хосте. |
| Потоки ЦП | Флажок **Считать потоки ядрами** даёт хостам возможность запускать ВМ с общим числом ядер процессора, превышающим число ядер на хосте.  Если этот флажок установлен, то предоставляемые потоки хоста считаются ядрами, которые может использовать ВМ. Например, в системе с 24 ядрами и 2 потоками на ядро (всего 48 потоков) могут выполняться ВМ с числом ядер вплоть до 48, а алгоритмы для расчёта загрузки ЦП хоста будут сопоставлять нагрузку с двойным числом потенциально используемых ядер. |
| Вытеснение памяти (baloon) | Установка флажка **Включить оптимизацию вытеснения памяти** включает превышенное выделение памяти для ВМ, работающих на хостах в этом кластере. Если этот параметр отмечен, то диспетчер превышенного выделения памяти (Memory Overcommit Manager, MoM) начинает вытеснение памяти где и когда это только возможно. Ограничением служит гарантированный размер памяти каждой ВМ.  Чтобы выполнять вытеснение памяти, виртуальной машине требуется устройство вытеснения памяти с соответствующими драйверами. Каждая ВМ включает в себя такое устройство, если только оно не было удалено специально. При смене статуса на «Запущен», каждый хост в этом кластере получает обновление политики вытеснения памяти. Если нужно, политику вытеснения памяти на хосте можно обновить вручную, без необходимости смены статуса. Смотрите раздел 5.2.9.  Очень важно понимать, что в некоторых сценариях вытеснение памяти может конфликтовать с функцией объединения одинаковых страниц памяти ядром (KSM). В таких случаях MoM постарается перенастроить размер вытесняемой памяти для минимизации конфликта. Кроме того, в некоторых сценариях вытеснение памяти может привести к производительности ВМ ниже оптимальной. Администраторам следует прибегать к оптимизации вытеснения памяти с осторожностью. |
| Контроль KSM | Галочка **Включить KSM** даёт возможность MoM выполнять объединение одинаковых страниц памяти при необходимости и тогда, когда выгода от экономии памяти перевешивает вычислительные затраты ЦП. |

### 5.2.4. Объяснение параметров политик миграции

Политика миграции определяет условия для динамической миграции ВМ в случае сбоев работы хоста. Эти условия включают в себя простой ВМ во время миграции, пропускную способность сети и то, каким образом выставляются приоритеты виртуальных машин.

**Таблица 5.3. Объяснение политик миграции**

|  |  |
| --- | --- |
| **Политика** | **Описание** |
| Устаревшая | Устаревшее поведение версий 3.6. Переназначение параметров vdsm.conf ещё применяется. Механизм ловушек гостевого агента отключён. |
| Минимальный простой | Политика, разрешающая миграцию ВМ в типичных ситуациях. ВМ не должны испытывать значительный простой. Миграция будет прервана, если после долгого промежутка времени ВМ не достигнет состояния целостности (в зависимости от итераций QEMU, с максимальным интервалов в 500 миллисекунд). Механизм ловушек гостевого агента включён. |
| **Миграция пост-копирования** | По аналогии с политикой минимального простоя, ВМ не должны испытывать значительный простой. Политика пост-копирования сначала пытается выполнить пред-копирование для проверки возможности конфликтов. Если ВМ не достигает состояния целостности после долгого промежутка времени, то происходит переключение на пост-копирование. Недостаток этой политики в том, что во время фазы пост-копирования по мере перемещения недостающих фрагментов памяти между хостами машина может значительно замедлиться.  Если во время фазы пост-копирования что-то пойдёт не так, например, случится сбой сети между хостами, то тогда процесс миграции приведёт к утрате целостности, приостановке работы ВМ и к дальнейшей потере ВМ. Соответственно, прерывание миграции во время фазы пост-копирования невозможно.  ПРЕДУПРЕЖДЕНИЕ  Если сетевое соединение оборвётся до завершения процесса пост-копирования, то виртуализированный ЦУ приостановит и затем убьёт выполняющуюсь ВМ. Не используйте миграцию пост-копирования при критической доступности ВМ или в нестабильной сети миграции. |
| **Приостановить рабочую нагрузку при необходимости** | Политика, дающая возможность миграции ВМ в большинстве ситуаций, включая серьёзную рабочую нагрузку на ВМ. В связи с этим машины под серьёзной рабочей нагрузкой могут простаивать в течение гораздо более долгого времени, чем с параметрами других политик. При экстремальных рабочих нагрузках миграция всё ещё может быть прервана. Механизм ловушек гостевого агента включён. |

Параметры пропускной способности определяют максимальную пропускную способность как входящих так и исходящих миграций на каждый отдельный хост.

**Таблица 5.4. Объяснение параметров пропускной способности**

|  |  |
| --- | --- |
| **Политика** | **Описание** |
| Авто | Значение пропускной способности копируется из параметра **Предел скорости [Мбит/с]** конфигурации **QoS сети хоста** дата-центра. Если предел скорости не был назначен, он рассчитывается как минимальная из скоростей канала на получающих и отправляющих сетевых интерфейсах. Если предел скорости не был назначен, а скорости канала неизвестны, значение определяется, исходя из локального параметра VDSM на посылающем хосте. |
| Гипервизор (по умолчанию) | Пропускная способность контролируется локальным параметром VDSM на отправляющем хосте. |
| Частная | Настраивается пользователем (в Мбит/сек). Это значение разделяется на число одновременных миграций (по умолчанию — 2, для учёта и входящей и исходящей миграции). Соответственно, пропускная способность, настроенная пользователем, должна быть достаточно высокой для вмещения всех одновременных миграций.  Если, например, Частная пропускная способность указана как 600 Мбит/сек, то максимальная пропускная способность при миграции ВМ фактически составит 300 Мбит/сек. |

Политика устойчивости определяет параметры приоритетов ВМ во время миграции.

**Таблица 5.5. Параметры политики устойчивости**

|  |  |
| --- | --- |
| **Поле** | **Описание/действие** |
| **Переносить виртуальные машины** | Все виртуальные машины переносятся в порядке их настроенного приоритета. |
| **Переносить только ВМ с высокой доступностью** | Переносятся только высокодоступные машины для предотвращения перегрузки других хостов. |
| **Не переносить ВМ** | **Запрещает миграцию виртуальных машин.** |

**Дополнительные параметры** применяются только к **Устаревшей** политике миграции.

**Таблица 5.6. Объяснение дополнительных параметров**

|  |  |
| --- | --- |
| **Параметр** | **Описание** |
| Автоматическое приведение в состояние целостности | Даёт возможность указать, будет ли использоваться автоматическое приведение в состояние целостности во время динамических миграций ВМ. Во время динамических миграций крупноразмерные ВМ с высокой рабочей нагрузкой могут загрязнять память быстрее, чем будет достигнута скорость переноса, и тем самым могут воспрепятствовать достижению состояния целостности. Функции автоматического приведения в состояние целостности QEMU дают возможность принудительно привести ВМ в состояние целостности. QEMU автоматически определяет отсутствие целостности и «затормаживает» виртуальные ЦП на машине. По умолчанию, автоматическое приведение в состояние целостности отключено глобально.   * Выберите пункт **Наследовать из глобального параметра**, чтобы использовать глобальную конфигурацию автоматического приведения в состояние целостности. Этот пункт выбран по умолчанию. * Выберите **Автоматическое приведение в состояние целостности** для перезаписи глобальной конфигурации и разрешения автоматического приведения ВМ в состояние целостности. * Выберите **Не применять автоматическое приведение в состояние целостности** для перезаписи глобальной конфигурации и запрещения автоматического приведения ВМ в состояние целостности. |
| Включить сжатие при миграции | Даёт возможность указать, будет ли использоваться сжатие во время динамических миграций виртуальных машин. При этом используется сжатие по алгоритму Xor Binary Zero Run-Length-Encoding для сокращения времени простоя ВМ и общего времени динамических миграций для ВМ с рабочей нагрузкой с интенсивной записью в память, а также для любого приложения, как правило, редко обновляющего память. По умолчанию, сжатие во время миграции отключено глобально.   * Выберите пункт **Наследовать из глобального параметра**, чтобы использовать глобальную конфигурацию сжатия. Этот пункт выбран по умолчанию * Выберите **Сжимать**, чтобы переопределить глобальный параметр и разрешить сжатие ВМ. * Выберите **Не сжимать**, чтобы переопределить глобальный параметр и запретить сжатие ВМ. |

### 5.2.5. Объяснение политик планирования

Политики планирования дают возможность указать использование и распределение виртуальных машин между доступными хостами. Настройте политику планирования, чтобы включить автоматическую балансировку нагрузки для всех хостов в кластере. Вне зависимости от политики планирования, ВМ не начнёт работу на хосте с перегруженным ЦП. По умолчанию, ЦП хоста считается перегруженным, если в течение более 5 минут нагрузка на его ЦП превышает 80%, но эти значения можно изменить с помощью политик планирования. Подробности о политиках планирования смотрите в Разделе 1.3.

**Таблица 5.7. Параметры вкладки политик планирования**

|  |  |
| --- | --- |
| **Поле** | **Описание/действие** |
| Выберите политику | Выберите политику в выпадающем списке.   * **None (отсутствует)**: без балансировки нагрузки или разделения энергосбережения между хостами уже работающих ВМ. Это режим по умолчанию. При запуске ВМ нагрузка на память и вычислительные ресурсы ЦП равномерно распределяются между всеми хостами в кластере. Дополнительные ВМ не начнут работу, если нагрузка хоста достигла ранее настроенных значенийCpuOverCommitDurationMinutes, HighUtilization или MaxFreeMemoryForOverUtilized * **evenly\_distributed (равномерное распределение)**: равномерно распределяет память и вычислительные ресурсы ЦП между всеми хостами в кластере. Дополнительные ВМ, присоединённые к хосту, не начнут работу, если нагрузка хоста достигла ранее настроенных значений CpuOverCommitDurationMinutes, HighUtilizationили MaxFreeMemoryForOverUtilized. * **cluster\_maintenance (обслуживание кластера)**: ограничивает активность в кластере во время выполнения задач обслуживания. Нельзя запускать никакие ВМ, включая высокодоступные. В случае сбоя хоста, высокодоступные ВМ будут корректно перезапущены, а также можно выполнять миграцию любых ВМ. * **power\_saving (энергосбережение)**: распределение памяти и нагрузки на вычислительные мощности ЦП внутри группы доступных хостов для снижения потребления энергии на недозагруженных хостах. Хосты с нагрузкой на ЦП ниже значения низкого использования в течение большего промежутка времени, чем указанный промежуток, выполнят миграцию всех ВМ на другие хосты с тем, чтобы можно было произвести отключение этого хоста. Дополнительные ВМ, присоединённые к этому хосту, не начнут работу, если хост достиг указанного значения высокой загрузки. * **vm\_evenly\_distributed (равномерное распределение ВМ)**: ВМ равномерно распределяются между хостами, основываясь на количестве машин. Кластер считается несбалансированным, если на каком-то из хостов выполняется больше ВМ, чем указано в значении HighVmCount, и если существует минимум один хост, число выполняемых ВМ на котором выходит за значение MigrationThreshold. |
| Параметры | В зависимости от выбранной политики появляются следующие, доступные к редактированию, параметры:   * **HighVmCount**: указывает минимальное число ВМ, выполняемых на хосте, для включения балансировки нагрузки. Значение по умолчанию — 10 работающих ВМ на хосте. Балансировка нагрузки включается только тогда, когда в кластере присутствует минимум один хост с числом работающих машин, как минимум равным значению HighVmCount. * **MigrationThreshold**: настраивает буфер до того, как ВМ будут перенесены с хоста. Это значение представляет собой максимальную инклюзивную разницу числа ВМ между самым высокозагруженным хостом и самым низкозагруженным хостом. Кластер считается сбалансированным, когда число ВМ на каждом хосте не выходит за значение порога миграции. Значение по умолчанию — 5. * **SpmVmGrace**: определяет число слотов ВМ, зарезервированных на хостах SPM. У хостов SPM более низкая нагрузка, чем у обычных хостов, поэтому эта прееменная опредляет, насколько меньше ВМ будут выпоняться на хосте SPM, по сравнению с друими хостами. Значение по умолчанию — 5. * **CpuOverCommitDurationMinutes**: указывает промежуток времени (в минутах**)**, в течение которого нагрузка на ЦП хоста может превышать настроенные значения до того, как будет применена политика планирования. Указанный временной интервал защищает от активации политик планирования по причине кратковременных пиков нагрузки на ЦП и последующих нежелательных миграций ВМ. Допускается максимум два знака. Значение по умолчанию — 2. * **HighUtilization**: выражается в процентном значении. Если нагрузка на ЦП хоста равна или превышает значение высокой нагрузки в теченпе указанного промежутка времени, то виртуализированный ЦУ выполняет миграцию ВМ на дтугие хосты в кластере до тех пор, пока нагрузка на ЦП хоста не будет превышать максимальный порог обслуживания. Значение по умолчанию — 80. * **LowUtilization**: выражается в процентном значении. Если нагрузка на ЦП хоста ниже значения низкой нагрузки в течение указанного промежутка времени, то виртуализированный ЦУ выполняет миграцию ВМ на другие хосты в кластере. Виртуализированный ЦУ выключит машину с исходным хостом, и включит её только тогда, когда это будет необходимо из соображений балансировки нагрузки, или если в кластере будет недостаточно свободных хостов. Значение по умолчанию — 20. * **ScaleDown**: снижает влияние весовой функции **HA Reservation**, путём деления значения оценки степени высокой готовности хоста на указанное число. Это дополнительный параметр, который можно добавлять к любой политике, включая политику **none**. * **HostsInReserve**: указывает число хостов, которые всегда должны работать, даже если на них отсутствуют ВМ. Это дополнительный параметр, который можно добавить к политике **power\_saving**. * **EnableAutomaticHostPowerManagement**: включает автоматическое управление энергосбережением на всех хостах кластера. Это дополнительный параметр, который можно добавить к политике **power\_saving**. Значение по умолчанию — **верно**. * **MaxFreeMemoryForOverUtilized**: указывает минимальный размер свободной памяти (в Мбайт), требуемый для минимального уровня обслуживания. Если объём доступной памяти хоста будет равен или ниже этого значения, то виртуализированный ЦУ будет переносить ВМ на другие хосты этого кластера в течение всего того времени, когда объём доступной памяти хоста будет находиться ниже значения порога минимального уровня обслуживания. Значения 0 для параметров **MaxFreeMemoryForOverUtilized** и **MinFreeMemoryForUnderUtilized** отключает балансировку памяти. Для избежания непредсказуемого поведения, при указании значения для параметра **MaxFreeMemoryForOverUtilized** необходимо также указывать значение и для параметра **MinFreeMemoryForUnderUtilized**. Это дополнительный параметр, который можно указать для политик **power\_saving** и **evenly\_distributed**. * **MinFreeMemoryForUnderUtilized**: указывает минимальный размер свободной памяти (в Мбайт), требуемый для того, чтобы хост считался низкозагруженным. Если объём доступной памяти хоста будет иметь значение ниже указанного в этом параметре, то виртуализированный ЦУ перенесёт ВМ на другие хосты в кластере и автоматически отключит машину хоста. Машина будет включена снова по соображениям балансировки нагрузки, или если в кластере будет недостаточно свободных хостов. Значение 0 для параметров **MaxFreeMemoryForOverUtilized** и **MinFreeMemoryForUnderUtilized** отключает балансировку памяти. Для избежания непредсказуемого поведения, при указании значения для параметра **MaxFreeMemoryForOverUtilized** необходимо также указывать значение и для параметра **MinFreeMemoryForUnderUtilized**. Это дополнительный параметр, который можно указать для политик **power\_saving** и **evenly\_distributed**. * **HeSparesCount**: указывает число дополнительных узлов виртуализированного ЦУ, на которых должна быть зарезервирована память в объёме, достаточном для запуска виртуальной машины виртуализированного ЦУ на случай её миграции или отключения. Если запуск других машин на узле виртуализированного ЦУ не оставит достаточного объёма свободной памяти для ВМ виртуализированного ЦУ, то эти машины не начнут работу. Это дополнительный параметр, который можно добавить к политикам **power\_saving**, **vm\_evenly\_distributed**, and **evenly\_distributed**. Значение по умочанию — 0. |
| Оптимизация планировщика | Оптимизация планировщика для определения весового коэффициента/распределения хостов.   * **Оптимизация для нагрузки**: в планирование включаются весовые модули для наилучшего выбора. * **Оптимизация для скорости**: определение весового коэффициента хоста пропускается в тех случаях, когда в очереди находится больше десяти запросов. |
| Включить доверенную службу | Включить интеграцию с сервером OpenAttestation. Чтобы включить возможность этого параметра, используйте утилиту engine-config для указания сведений о сервере OpenAttestation. Подробности смотрите в Разделе 9.9. |
| Включить резервирование высокой доступности | Разрешить виртуализированному ЦУ выполнять наблюдения за доступными мощностями кластера для отказоустойчивых ВМ. Виртуализированный ЦУ обеспечивает наличие в кластере необходимых ресурсов для миграции высокодоступных ВМ в случае внезапного отказа их текущего хоста. |
| **Укажите политику нумерации** | Этот параметр даёт возможность указать политику порядковых номеров для ВМ в кластере. Выберите одну из следующих возможностей:   * **ID хоста**: в качестве порядкового номера ВМ указывается UUID хоста. * **ID ВМ**: в качестве порядкового номера ВМ указывается её UUID. * **Частный порядковый номер**: даёт возможность указать частный порядковый номер. |

Если объём свободной памяти хоста падает ниже значения 20%, такие команды вытеснения памяти, как mom.Controllers.Balloon - INFO Ballooning guest:half1 from 1096400 to 1991580 журналируются в **/var/log/vdsm/mom.log**. Файл **/var/log/vdsm/mom.log** является файлом журнала диспетчера превышенного выделения памяти MoM.

### 5.2.6. Объяснения параметров консоли кластера

В таблице ниже описываются параметры вкладки **Консоль** в окнах **Новый кластер** и **Параметры кластера**.

**Таблица 5.8. Параметры консоли**

|  |  |
| --- | --- |
| **Поле** | **Описание/действие** |
| **Укажите прокси SPICE для кластера** | Отметьте галочкой этот параметр, чтобы включить переопределение прокси SPICE, указанное в глобальной конфигурации. Этот параметр бывает полезен в тех случаях, когда пользователь (подключающийся, например, с помощью Портала ВМ) находится за пределами сети расположения гипервизоров. |
| **Переопределённый адрес прокси SPICE** | Прокси, с помощью которого клиент SPICE подключается к виртуальным машинам. Адрес должен указываться в следующем формате:  протокол://[хост]:[порт] |

### 5.2.7. Объяснение параметров политики операций блокады

В таблице ниже описываются параметры вкладки **Политика операций блокады** в окнах **Новый кластер** и **Параметры кластера**.

**Таблица 5.9. Параметры политик операций блокады**

|  |  |
| --- | --- |
| **Поле** | **Описание/действие** |
| Включить возможность операций блокады | Разрешает проведений операций блокады в кластере. По умолчанию эта возможность присутствует, но при необходимости её можно отключить; если, например, возникают или ожидаются временные проблемы с сетью, то администратор может отключить возможность проведения операций блокады до завершения действий по диагностики или обслуживания. Обратите внимание, что при отключённой возможности проведения операций блокады, высокодоступные ВМ, выполняемые на неотвечающих хостах, не будут перезапущены в другом месте. |
| Пропустить операцию блокады, если у хоста имеется динамическая аренда в хранилище | Если этот параметр отмечен галочкой, операции блокады не будут выполняться на любых хостах со статусом «не отвечает», по-прежнему подключённых к хранилищу. |
| Пропустить операцию блокады, если у кластера есть проблемы с соединением | Если этот параметр отмечен галочкой, операции блокады временно не будут выполняться, если процентное значение хостов в кластере, испытывающих проблемы с соединением, равен или больше указанного значения **Порога**. Значение **Порога** выбирается в выпадающем списке; доступные значения: **25**, **50**, **75** и **100**. |
| **Пропустить операцию блокады, если имеются работающие элементы (кирпичи) Gluster** | Этот параметр доступен только при включённых возможностях хранилища Gluster. При выбранном параметре операция блокады будет пропускаться, если присутствуют работающие элементы (кирпичи), к которым есть доступ с других одноранговых узлов. |
| **Пропустить операцию блокады, если не выполнены требования кворума Gluster.** | Этот параметр доступен только при включённых возможностях хранилища Gluster. Если этот параметр включён, операция блокады будет пропускаться при работающих элементах (кирпичах), а выключение хоста приведёт к потере кворума. |

### 5.2.8. Настройка политик управления нагрузкой и энергосбережением на хосте

Политики планирования **evenly\_distributed** (равномерное распределение) и **power\_saving** (энергосбережение) дают возможность указать приемлемые значения потребления ресурсов памяти и ЦП, а также порог значений, после превышения которого виртуальные машины должны мигрировать с хоста или на хост. Политика планирования **vm\_evenly\_distributed** (равномерное распределение ВМ) равномерно распределяет ВМ между хостами, руководствуясь количеством машин. Для включения автоматической балансировки нагрузки хостов в кластере настройте политику планирования. Подробное объяснение каждой политики планирования смотрите в Разделе 5.2.5.

**Настройка политик управления нагрузкой и энергосбережением хостов**

1. Нажмите Вычисления → Кластеры и выберите кластер.
2. Нажмите **Изменить**.
3. Перейдите на вкладку **Политика планирования**.
4. Выберите одну из следующих политик:
   * **нет**
   * **vm\_evenly\_distributed**
     1. В поле **HighVmCount** укажите минимальное число ВМ, выполняющихся как минимум на одном хосте, для включения балансировки нагрузки.
     2. В поле **MigrationThreshold** укажите максимальную приемлемую разницу между числом ВМ на самом загруженном хосте и числом ВМ на самом незагруженном хосте.
     3. В поле **SpmVmGrace** укажите число слотов для ВМ, которое должно быть зарезервировано на хостах SPM.
     4. По желанию, в поле **HeSparesCount** укажите число дополнительных узлов виртуализированного ЦУ, на которых нужно зарезервировать объём свободной памяти, достаточный для запуска ВМ виртуализированного ЦУ в случае её миграции или выключения. Подробности смотрите в Разделе 12.3.
   * **evenly\_distributed**
     1. В поле **CpuOverCommitDurationMinutes** укажите время (в минутах), в течение которого нагрузка на ЦП хоста может превышать настроенные значения нагрузки перед тем, как будет применена политика планирования.
     2. В поле **HighUtilization** укажите процентное значение нагрузки на ЦП, при котором ВМ будут начинать миграцию на другие хосты.
     3. В поле **MinFreeMemoryForUnderUtilized укажите минимальный объём свободной памяти в Мбайт, при превышении которого ВМ начнут мигрировать на другие хосты.**
     4. В поле **MaxFreeMemoryForOverUtilized** укажите максимальный требуемый объём свободной памяти, ниже которого ВМ начнут миграцию на другие хосты.
     5. По желанию, в поле **HeSparesCount** укажите число дополнительных узлов виртуализированного ЦУ, на которых нужно зарезервировать объём свободной памяти, достаточный для запуска ВМ виртуализированного ЦУ в случае её миграции или выключения. Подробности смотрите в Разделе 12.3.
   * **power\_saving**
     1. В поле **CpuOverCommitDurationMinutes** укажите время (в минутах), в течение которого нагрузка на ЦП хоста может превышать настроенные значения нагрузки перед тем, как будет применена политика планирования.
     2. В поле **LowUtilization** укажите процент загруженности ЦП, ниже которого хост будет сичтаться недохзагруженным.
     3. В поле **HighUtilization** укажите процентное значение нагрухки на ЦП, при октором ВМ начунт миграцуию на другие хосты.
     4. В поле **MinFreeMemoryForUnderUtilized укажите минимальный объём свободной памяти в Мбайт, при превышении которого ВМ начнут мигрировать на другие хосты.**
     5. В поле **MaxFreeMemoryForOverUtilized** укажите максимальный требуемый объём свободной памяти, ниже которого ВМ начнут миграцию на другие хосты.
     6. По желанию, в поле **HeSparesCount** укажите число дополнительных узлов виртуализированного ЦУ, на которых нужно зарезервировать объём свободной памяти, достаточный для запуска ВМ виртуализированного ЦУ в случае её миграции или выключения. Подробности смотрите в Разделе 12.3.
5. Выберите одно из значений для **Оптимизации планировщика** кластера:
   * Выберите **Оптимизировать на использование**, чтобы включить в планировку весовые модули для лучшего выбора.
   * Выберите **Оптимизировать на скорость**, чтобы пропускать измерение веса хоста в тех случаях, когда в очереди находится более 10 запросов.
6. Если для верификации хостов используется сервер OpenAttestation, и его конфигурация была настроена с помощью утилиты engine-config, то отметьте галочкой параметр **Включить доверенную службу**.
7. При желании отметьте параметр **Включить резервирование высокой доступности**, чтобы виртуализированный ЦУ мог обеспечивать доступность ресурсов в кластере для отказоустойчивых ВМ.
8. При желании отметьте параметр **Предоставить пользовательскую политику нумерации**, чтобы указать политику порядковых номеров для ВМ в кластере, а затем выберите одну из следующих возможностей:
   * Выберите **ID хоста**, чтобы в качестве порядкового номера ВМ указывался UUID хоста.
   * Выберите **ID ВМ,** чтобы в качестве порядкового номера ВМ указывался UUID машины.
   * Выберите **Частный порядковый номер** и затем укажите его в текстовом поле.
9. Нажмите **OK**.

### 5.2.9. Обновление информации о политике MoM на хостах в кластере

Диспетчер превышенного выделения памяти (Memory Overcommit Manager, MoM) хоста отвечает за обработку возможностей вытеснения памяти и объединения одинаковых страниц памяти ядром (KSM). Изменения параметров этих функций на уровне кластера передаются хостам только после того, как хост вновь получит статус «Запущен» после перезагрузки или после снятия режима обслуживания. Тем не менее, при необходимости, применить важные изменения можно немедленно, выполнив синхронизацию политики превышенного выделения памяти для хостов, ещё имеющих статус «Запущен». Нижеследующая последовательность действий должна выполняться на каждом из хостов индивидуально.

**Синхронизация политики превышенного выделения памяти на хосте**

1. Нажмите **Вычисления → Кластеры**.
2. Нажмите на название кластера, чтобы открыть подробный просмотр.
3. Перейдите на вкладку **Хосты** и выберите хост, для которого нужно обновить политику MoM.
4. Нажмите **Синхронизировать политику MoM**.

Информация о политике MoM на хосте будет обновлена без необходимости перемещать хост в режим обслуживания и после этого обратно в состояние «Запущен».

### 5.2.10. Создание профиля ЦП

Профили ЦП определяют максимальный объём вычислительных возможностей хоста, к которому может получить доступ выполняемая на этом хосте ВМ в составе кластера, выраженный в процентном соотношении к общей вычислительной мощности, доступной для этого хоста. Профили ЦП создаются на базе профилей ЦП, настроенных в дата-центрах, и не применяются автоматически ко всем ВМ в кластере; чтобы профили вступили в силу, их необходимо вручную присваивать виртуальным машинам индивидуально.

В данной последовательности действий подразумевается, что на дата-центре, которому принадлежит кластер, ранее были настроены одна или более записей о качестве обслуживания для ЦП.

**Создание профиля ЦП**

1. Нажмите **Вычисления → Кластеры**
2. Нажмите на название кластера, чтобы открыть подробный просмотр.
3. Перейдите на вкладку **Профили ЦП**.
4. Нажмите **Добавить**.
5. Укажите **Название** и **Описание** профиля ЦП.
6. Из списка **QoS** выберите запись о качестве обслуживания, которую необходимо применить к профилю ЦП.
7. Нажмите **OK**.

### 5.2.11. Удаление профиля ЦП

Удалите существующий профиль ЦП из окружения виртуализации Red Hat.

**Удаление профиля ЦП**

1. Нажмите **Вычисления → Кластеры**.
2. Нажмите на название кластера, чтобы открыть подробный просмотр.
3. Перейдите на вкладку **Профили ЦП** и выберите удаляемый профиль ЦП.
4. Нажмите **Удалить**.
5. Нажмите **OK**.

Если этот профиль был присвоен какой-либо ВМ, то этим машинам автоматически будет присвоен профиль ЦП по умолчанию.

### 5.2.12. Импортирование существующего кластера хранилища Gluster.

В виртуализированный ЦУ можно импортировать кластер хранилища Gluster и все принадлежащие к нему хосты.

При указании таких параметров любого хоста в кластере, как адрес IP или имя и пароль хоста, на этом хосте с помощью протокола SSH выполняется команда gluster peer status , а затем выводится список хостов, принадлежащих кластеру. Необходимо вручную заверить отпечаток каждого хоста и указать для них пароли. Если один из хостов в кластере не запущен или недоступен, то выполнить импортирование кластера будет невозможно. Поскольку на свежеимпортированных хостах не установлен VDSM, то после завершения импорта сценарий самозагрузки установит на хостах все необходимые пакеты VDSM и перезагрузит их.

**Импортирование существующего хранилища Gluster в виртуализированный ЦУ**

1. Нажмите **Вычисления → Кластеры**.
2. Нажмите **Добавить**.
3. Выберите **Дата-центр**, к которому будет принадлежать кластер.
4. Укажите **Название** и **Описание** кластера.
5. Отметьте галочками параметры **Включить службу Gluster** и **Импортировать существующую конфигурацию Gluster**.

Поле **Импортировать существующую конфигурацию Gluster** будет показано только при выбранном параметре **Включить службу Gluster**.

1. В поле **Имя хоста** укажите имя хоста или адрес IP любого сервера в кластере.

Будет показан **Отпечаток SSH** для подтверждения того, что выполняется подключение к нужному хосту. Если хост недоступен или появилась ошибка сети, то в поле **Отпечаток** будет выведена **Ошибка получения отпечатка**.

1. Укажите **Пароль сервера** и нажмите **OK**.
2. Будет показано окно **Добавить хосты** и список хостов в составе кластера.
3. Для каждого хоста укажите **Название** и **Пароль root**.
4. В случае использования одного и того же пароля для всех хостов, отметьте галочкой параметр **Использовать общий пароль**, чтобы указать этот пароль в текстовом поле.

Нажмите **Применить**, чтобы установить введённый пароль для всех хостов.

Проверьте подлинность всех отпечатков и внесите изменения, нажав **OK**.

После импорта хостов, сценарий самозагрузки установит на хостах необходимые пакеты VDSM и перезагрузит хосты. Существующий кластер хранилища Gluster был успешно импортирован в виртуализированный ЦУ.

### 5.2.13. Объяснение параметров в окне «Добавить хосты».

В окне **Добавить хосты** можно указать подробные сведения о хостах, импортируемых в составе кластера с поддержкой Gluster. Это окно появляется после того, как в окне **Новый кластер** была поставлена галочка рядом с параметром **Включить службу Gluster** и указаны все необходимые сведения о хосте.

**Таблица 5.10. Добавление параметров Gluster**

|  |  |
| --- | --- |
| **Поле** | **Описание** |
| Использовать общий пароль | Поставьте галочку, чтобы для всех хостов в кластере использовался один и тот же пароль. Введите пароль в поле **Пароль**, затем нажмите на кнопку **Применить**, чтобы установить пароль для всех хостов. |
| Название | Укажите название хоста. |
| Имя хоста/IP | Это поле заполняется автоматически на основании данных о полном доменном имени или адресе IP, указанных в окне **Новый кластер**. |
| Пароль root | Чтобы использовать различные пароли root для каждого хоста, введите пароль в этом поле. Данные в этом поле переопределяют общий пароль, указанный для всех хостов в кластере. |
| Отпечаток | Для подтверждения того, что выполняется подключение к нужному хосту, здесь будет показан его отпечаток. Это поле заполняется автоматически на базе данных об отпечатке хоста, указанных в окне **Новый кластер**. |

### 5.2.14. Удаление кластеров

Перед удалением кластера переместите из него все хосты.

ВНИМАНИЕ

Удалить кластер по умолчанию нельзя, поскольку в нём хранится пустой шаблон. Тем не менее, кластер по умолчанию можно переименовать и добавить его в новый дата-центр.

**Удаление кластера**

1. Нажмите **Вычисления → Кластеры** и выберите кластер.
2. Убедитесь в том, что в кластере нет хостов.
3. Нажмите **Удалить**.
4. Нажмите **OK**

### 5.2.15. Оптимизация памяти

Для увеличения числа виртуальных машин на хосте можно использовать *превышенное выделение памяти*, при котором объём памяти, выделяемый машине, превышает объём ОЗУ и обуславливается файлом подкачки.

Тем не менее, существует ряд потенциальных проблем, связанных с превышенным выделением памяти:

* Производительность подкачки — файл подкачки работает медленнее и потребляет больше ресурсов ЦП, чем ОЗУ, что влияет на производительность ВМ. Чрезмерное использование подкачки может привести к «пробуксовке» ЦП.
* Уничтожитель перерасхода памяти (OOM) — если на хосте заканчивается место в файле подкачки и новые процессы не могут начать работу, то фоновая программа ядра, уничтожитель OOM, начинает выключать активные процессы, такие, как гостевые ОС.

Чтобы исправить эти недостатки, можно сделать следующее:

* Ограничить превышенное выделение памяти с помощью параметра **Оптимизация памяти** и *диспетчера превышенного выделения памяти (MoM)*.
* Создать раздел подкачки, достаточно объёмный для того, чтобы потенциально обеспечить максимальный запрос на виртуальную память и одновременно не выходить за пределы безопасности.
* Уменьшить размер виртуальной памяти, включив *вытеснение памяти* (ballooning) и *объединение одинаковых страниц памяти ядром* (KSM).

#### 5.2.15.1. Оптимизация памяти и превышенное выделение памяти

Ограничить объём превышенного выделения памяти можно с помощью одного из параметров **Оптимизации памяти**: **Нет** (0%), **150%**, or **200%**.

Каждый параметр представляет процентное значение ОЗУ. Для хоста с 64 Гбайт ОЗУ, например, выбор значения в 150% означает, что превысить выделение памяти можно на дополнительные 32 Гбайт, получив всего 96 Гбайт виртуальной памяти. Если хост использует 4 Гбайт от этого общего объёма, то будут доступны оставшиеся 92 Гбайт. Большую часть от этого объёма можно выделить виртуальной машине (пункт **Размер памяти** на вкладке **Система**), но также рекомендуется оставить какой-то резерв в качестве запаса прочности.

Внезапные пиковые скачки запросов на виртуальную память могут повлиять на производительность до того, как механизмы MoM, вытеснения памяти и KSM успеют повторно оптимизировать виртуальную память. Для снижения этого влияния выберите лимит, соответствующий типам выполняемых приложений и рабочих нагрузок:

* Для рабочих нагрузок, создающих наиболее значимый постепенный прирост запросов памяти, выберите более высокий процент, например **200%** или **150%**.
* Для более критически важных приложений или рабочих нагрузок, создающих внезапные скачки запросов памяти, выберите более низкое процентное значение, например **150%** или **Нет**. Выбор значения **Нет** помогает предотвратить превышенное выделение памяти, но одновременно даёт возможность MoM, устройствам вытеснения памяти и KSM продолжать работу по оптимизации виртуальной памяти.

ВАЖНО

Перед развёртыванием конфигурации *Оптимизации памяти* в рабочей среде, всегда сначала проводите стресс-тестирование с широким диапазоном условий.

Чтобы настроить параметры **Оптимизации памяти** перейдите на вкладку **Оптимизация** в окнах **Новый кластер** или **Параметры кластера**. Смотрите Раздел 5.2.3.

Дополнительные комментарии:

* Фактический объём доступной памяти невозможно определить в реальном времени, поскольку объём оптимизации памяти, достигаемый KSM, и объём вытеснения памяти постоянно меняются.
* После достижения виртуальными машинами лимита виртуальной памяти невозможен запуск новых приложений.
* При планировании числа выполняемых на хосте ВМ в качестве точки отсчёта используйте максимальный объём виртуальной памяти (размер физической памяти и параметр **Оптимизация памяти**). Не используйте в расчётах более низкий объём памяти, достигаемый за счёт оптимизации с помощью вытеснения памяти и KSM.

#### 5.2.15.2.  Раздел подкачки и превышенное выделение памяти

При настройке раздела подкачки мы советуем придерживаться следующих рекомендаций:

**Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Red Hat Enterprise Open Stack Platform 3 and Red Hat Enterprise Open Stack Platform 4**

|  |  |  |
| --- | --- | --- |
| **Объём установленной ОЗУ** | **Рекомендуемый размер раздела подкачки** | **Рекомендуемый размер раздела подкачки если разрешается гибернации** |
| 2 Гбайт или меньше | Двойной объём установленной ОЗУ | Тройной объём установленной ОЗУ |
| 2 Гбайт - 8 Гбайт | Объём, равный объёму ОЗУ | Двойной объём ОЗУ |
| 8 Гбайт - 64 Гбайт | Минимум 4 Гбайт | Полуторный объём ОЗУ |
| 64 Гбайт или больше | Минимум 4 Гбайт | Гибернация не рекомендуется |

ВНИМАНИЕ

Для систем с числом логических процессоров, превышающим 140, или с объёмом ОЗУ более 3 Тбайт рекомендованный размер раздела подкачки составляет не менее 100 Гбайт.

* Следующие моменты также влияют на принятие решения о выделяемом размере раздела подкачки:
  + **Есть ли конкретные требования со стороны приложений? Приложение могло создаваться с учётом конкретного размера раздела подкачки. В таких случаях размер раздела должен соответствовать рекомендациям поставщика приложения.**
  + **Есть ли другие требования? Рабочие станции и ноутбуки могут использовать возможности гибернации, когда содержимое ОЗУ сохраняется в области подкачки. В таких случаях, чтобы иметь возможность выполнять гибернацию, размер области подкачки должен быть равен или больше объёма установленной в системе ОЗУ**
  + **Выделение подкачки в качестве памяти «последней возможности»**. Хотя блочные устройства, на которых размещается подкачка, в целом гораздо медленнее ОЗУ, бывает удобно иметь подкачку в качестве дополнительного слоя памяти при необходимости. В случае приложений с высоким потреблением памяти, подкачка даёт возможность выгрузить память на диск для отсрочки или предотвращения прерывания работы приложения программой-уничтожителем OOM.
* Виртуальные гости: к виртуальным гостям применяются те же самые условия, что и к физическим системам. Кроме того, использование дополнительного небольшого объёма подкачки может повлиять на возрастающие число обращений к памяти этим процессом, что в итоге сначала приведёт к замедлению его работы (что даёт администратору время вручную исправить ситуацию), а затем к исчерпанию ресурсов подкачки и окончательному прерыванию работы процесса программой-уничтожителем OOM. Если объём памяти, в который пишет этот процесс, не превышает объём доступной подкачки, то система просто испытает временное замедление работы.

Применяя данные рекомендации, следуйте совету по установке размера раздела подкачки в качестве «последней возможности» для наихудшего возможного сценария. Используйте размер физической памяти и параметр **Оптимизация памяти** в качестве базы для расчёта общего объёма виртуальной памяти. Не включайте в эти расчёты сокращение памяти с помощью оптимизации диспетчером превышенного выделения памяти (MoM), вытеснения памяти и объединения одинаковых страниц памяти ядром (KSM).

ВАЖНО

Чтобы повысить шансы предотвращения состояния нехватки памяти, создавайте раздел подкачки достаточно большим из расчёта на наихудший возможный сценарий плюс резерв запаса прочности. Перед развёртыванием конфигурации в рабочей среде обязательно выполняйте стресс-тестирование при самых разных условиях.

#### 5.2.15.3. Диспетчер превышенного выделения памяти (MoM)

*Диспетчер превышенного выделения памяти* (Memory Overcommit Manager, MoM) выполняет две функции:

* Он ограничивает превышенное выделение памяти путём применения описанного выше параметра **Оптимизация памяти** к хостам в кластере.
* Он оптимизирует память, управляя процессами *вытеснения памяти* (ballooning) и *объединения одинаковых страниц памяти ядром* (KSM), что описывается в разделах ниже.

Диспетчер MoM не нуждается во включении или отключении.

Если объём доступной свободной памяти хоста падает ниже 20%, такие команды вытеснения памяти, как mom.Controllers.Balloon - INFO Ballooning guest:half1 from 1096400 to 1991580 записываются в файл журнала **/var/log/vdsm/mom.log**, являющегося файлом журнала диспетчера MoM.

#### 5.2.15.4. Вытеснение памяти

Виртуальные машины начинают работу, располагая полным объёмом выделенной им виртуальной памяти. По мере того, как потребление виртуальной памяти превышает объём ОЗУ, хост всё более и более начинает полагаться на подкачку. Механизм *вытеснения памяти*, в случае, если он активен, заставляет ВМ отдать неиспользуемую часть этой памяти. Освобождённая память может быть повторно использована другими процессами и другими ВМ на хосте. По причине сокращения объёма используемой памяти сокращается и число обращений к подкачке, а также улучшается производительность.

Пакет virtio-balloon , содержащий устройство вытеснения памяти и его драйверы, представляет собой модуль ядра (LKM). По умолчанию, он настроен на автоматическую загрузку. Внесение модуля в чёрный список или его выгрузка отключает механизм вытеснения памяти.

Устройства вытеснения памяти не координируются напрямую друг с другом; они зависят от диспетчера превышенного выделения памяти хоста (MoM), постоянно наблюдающего за нуждами каждой ВМ и инструктирующего устройство вытеснения памяти увеличить или уменьшить объём виртуальной памяти.

Факторы производительности:

* Мы не рекомендуем применять вытеснение памяти и превышенное выделение памяти для рабочих нагрузок, требующих постоянной высокой производительности и низких значений задержки.
* Мы рекомендуем применять вытеснение памяти там, где увеличение численности ВМ (экономия) играет бòльшую роль, чем производительность.
* Вытеснение памяти не имеет значительного влияния на загруженность ЦП. (KSM потребляет некоторые количество ресурсов ЦП, но в стрессовых условиях объём этого потребления не изменяется.)

Чтобы включить механизм вытеснения памяти, перейдите на вкладку **Оптимизация** в окне **Новый кластер** или **Параметры кластера**. Затем отметьте галочкой параметр **Включить оптимизацию памяти balloon**. Этот параметр включает механизм вытеснения памяти на виртуальных машинах, выполняющихся на хостах в данном кластере. При отмеченном параметре, MoM начинает вытеснение памяти где и когда только возможно, ограничением служит только размер гарантированной памяти каждой ВМ. Смотрите Раздел 5.2.3.

Каждый хост в данном кластере получает обновление политики вытеснения памяти при смене статуса этого хоста на «запущен». При необходимости, обновить информацию о политике вытеснения памяти на хосте можно без смены статуса. Смотрите Раздел 5.2.9.

#### 5.2.15.5. Объединение одинаковых страниц памяти ядром (KSM)

Во время своей работы виртуальная машина часто копирует страницы памяти для таких элементов, как общие библиотеки и часто используемые данные. Кроме того, виртуальные машины, на которых выполняются одинаковые гостевые ОС и приложения, создают дубликаты страниц памяти в виртуальной памяти.

*Процесс объединения одинаковых страниц памяти ядром* (KSM) проверяет виртуальную память на хосте, избавляется от дубликатов страниц памяти и разделяет оставшиеся страницы памяти между несколькими приложениями и виртуальными машинами. Эти общие страницы памяти помечены как «копирование при записи»; если ВМ требуется записать в эту страницу каике-то изменения, то она сначала делает копию, а потом записывает изменения в эту копию.

Пока механизм KSM остаётся включённым, им управляет диспетчер превышенного выделения памяти (MoM). Ручная настройка или управление KSM не требуется.

KSM улучшает производительность виртуальной памяти двумя способами. Поскольку разделяемая страница памяти используется более часто, то скорей всего хост именно её сохранит в кэше или главной памяти, ч то повышает скорость доступа к памяти. Кроме того, при превышенном выделении памяти, KSM уменьшает загруженность виртуальной памяти, снижая вероятность использования подкачки и повышая производительность.

KSM потребляет больше ресурсов ЦП, чем механизм вытеснение памяти. Объём потребляемых KSM ресурсов остаётся неизменным и в критических условиях. Выполнение одинаковых ВМ и приложений на хосте даёт KSM больше возможностей для объединения страниц памяти, чем выполнение отличающихся друг от друга ВМ. Если отличающиеся друг от друга ВМ и приложения составляют бòльшую часть выполняемых ВМ и приложений, то соображения нагрузки на ЦП при использовании KSM могут перевесить преимущества этого использования.

Факторы производительности:

* После того, как KSM объединит большой объём памяти, статистика подсчёта памяти, собираемая ядром, может в итоге не отражать реальной картины. Если в системе присутствует большой объём свободной памяти, отключение KSM может улучшить производительность.
* Мы не рекомендуем применять механизмы объединения одинаковых страниц памяти ядром и превышенного выделения памяти для рабочих нагрузок, требующих постоянной высокой производительности и низких значений задержки.
* Мы рекомендуем применять механизм объединения одинаковых страниц памяти ядром там, где увеличение численности ВМ (из соображений экономии) играет бòльшую роль, чем производительность.

Чтобы включить механизм объединения одинаковых страниц памяти ядром, перейдите на вкладку **Оптимизация** в окне **Новый кластер** или **Параметры кластера**. Затем отметьте галочкой параметр **Включить KSM**. Этот параметр заставляет диспетчер превышенного выделения памяти MoM запускать KSM, когда это необходимо, и когда преимущества экономии памяти при объединении одинаковых страниц памяти перевешивают затраты ЦП на работу KSM. Смотрите Раздел 5.2.3.

### 5.2.16. Изменение версии совместимости кластера

Кластеры в системе виртуализации Red Hat имеют версию совместимости. Версия совместимости кластера указывает на возможности системы виртуализации, поддерживаемые всеми хостами в кластере. Совместимость кластеров настраивается согласно версии ОС хоста в кластере, имеющей наименьшие возможности.

ВАЖНО

Чтобы сменить версию совместимости кластера, сначала нужно обновить версию всех хостов в кластере до уровня, поддерживающего желаемый уровень совместимости. Проверьте наличие рядом с хостом значка, обозначающего возможность обновления версии.

**Последовательность действий**

1. На портале администрирования нажмите Вычисления → Кластеры.
2. Выберите кластер и нажмите **Параметры**.
3. На вкладке **Общее** смените **Версию совместимости** на желаемое значение.
4. Нажмите OK. Будет показан диалог подтверждения **Изменить версию совместимости кластера**.
5. Нажмите OK для подтверждения.

ВАЖНО

Существует вероятность появления сообщения, предупреждающего о некорректной конфигурации некоторых ВМ и шаблонов. Чтобы исправить эту ошибку, отредактируйте параметры каждой ВМ вручную. В окне *Параметры ВМ* есть дополнительные предупреждения и пункты соответствия, указывающие на то, что именно необходимо скорректировать. Иногда проблема исправляется автоматически, и конфигурацию ВМ просто нужно ещё раз сохранить. После изменения параметров каждой ВМ можно будет сменить версию совместимости кластера.

После обновления версии совместимости кластера необходимо обновить версию совместимости всех работающих или приостановленных ВМ, перезапустив их с помощью Портала администрирования или с помощью REST API, а не из гостевых ОС. Машины, которым нужна перезагрузка, отмечены значком изменений, ждущих применения (). Нельзя изменить версию совместимости снимка виртуальной машины, находящегося в предпросмотре. Сначала необходимо зафиксировать изменения или отменить предварительный просмотр.

В окружении виртуализированного ЦУ виртуальная машина ЦУ не нуждается в перезагрузке.

Хотя можно отложить перезагрузку машин до более удобного момента, крайне рекомендуется перезагрузить ВМ немедленно, чтобы машины использовали самую последнюю конфигурацию. ВМ, не получившие обновлений, работают со старой конфигурацией, а новые конфигурации могут быть перезаписаны, если до перезагрузки в параметры ВМ будут внесены другие изменения.

Как только версия совместимости всех кластеров и ВМ в дата-центре будет обновлена, можно изменять версию совместимости самого дата-центра.

# Глава 6. Логические сети

## 6.1. Задачи при работе с логическими сетями

### 6.1.1. Выполнение сетевых задач

Меню Сеть → Сети предоставляет пользователю централизованную локацию для выполнения действий, связанных с логическими сетями, а также для поиска логических сетей на основе свойств сетей или связи с другими ресурсами. С помощью кнопок **Добавить**, **Параметры** и **Удалить** можно создавать, изменять свойства и удалять логические сети в рамках дата-центра.

Нажмите на имя каждой из сети и, переходя по вкладкам в подробном просмотре, выполняйте действия, включающие в себя:

* Присоединение или отсоединение сетей от кластеров или хостов
* Удаление сетевых интерфейсов ВМ и шаблонов
* Добавление и удаление полномочий пользователей на доступ и управление сетями

Доступ к этому функционалу также возможен для каждого индивидуального ресурса.

ПРЕДУПРЕЖДЕНИЕ

Не изменяйте сетевые параметры в дата-центре или в кластере при работающих хостах, так как существует риск того, что хосты станут недоступными.

ВАЖНО

Если узлы системы виртуализации Red Hat планируется использовать для предоставления каких-либо служб, помните, что службы остановятся, если окружение виртуализации прекратит работать

Это касается всех служб, но особенно чётко нужно понимать риски выполнения в окружении виртуализации следующих служб:

Службы каталогов

DNS

Хранилище

### 6.1.2. Создание новой логической сети в дата-центре или кластере

Создайте логическую сеть и настройте её использование в дата-центре или в кластерах дата-центра.

**Создание новой логической сети в дата-центре или в кластере**

1. Нажмите **Вычисления → Дата-центры** или **Вычисления → Кластеры**.
2. Нажмите на название дата-центра или кластера, чтобы открыть подробный просмотр.
3. Перейдите на вкладку **Логические сети**.
4. Откройте окно **Новая логическая сеть**:
   * В подробном просмотре дата-центра нажмите **Добавить**.
   * В подробном просмотре кластера нажмите **Добавить сеть**.
5. Укажите Название, Описание и Комментарий для логической сети.
6. Опционально, включите параметр **Включить добавление тегов для VLAN**.
7. Опционально, отключите **Сеть ВМ**.
8. Опционально, отметьте галочкой параметр **Создать на внешнем поставщике**. Таким образом будут отключены параметры **Метка сети**, **Сеть ВМ** и **MTU**. Смотрите Главу 11 «Внешние поставщики».
9. Выберите **Внешнего поставщика**. В список **Внешний поставщик** не включены внешние поставщики с режимом read-only.

Чтобы создать внутреннюю изолированную сеть, выберите в списке **Внешний поставщик** пункт **ovirt-provider-ovn** и не отмечайте параметр **Подключиться к физической сети**.

1. В поле **Метка сети** введите новую метку логической сети или выберите уже существующую.
2. Укажите значение **MTU**: **По умолчанию (1500)** или **Пользовательское**.
3. При выборе в списке **Внешний поставщик** пункта **ovirt-provider-ovn, укажите, необходимо ли в сети применять Группы безопасности. Подробности смотрите в Разделе 6.1.7.**
4. Во вкладке **Кластер** выберите кластеры, которым будет присвоена сеть. Также можно указать, будет ли эта логическая сеть требуемой сетью.
5. При выборе пункта **Создать внешнего поставщика** станет видимой вкладка **Подсеть**. Укажите в этой вкладке **Название**, **CIDR** и **Шлюз**. При необходимости, можно добавить серверы DNS.
6. Во вкладке **Профили vNIC** добавьте профили требуемых виртуальных NIC к логической сети.
7. Нажмите **OK**.

Если для логической сети была указана метка, то сеть будет автоматически добавлена ко всем сетевым интерфейсам с этой меткой.

ВНИМАНИЕ

При создании новых логических сетей или внесение изменений в существующие логические сети, используемые в качестве сетей визуализации, то для того, чтобы новые сети стали доступы или для применения внесённых изменений необходимо перезапустить любые выполняющиеся ВМ, использующие эти сети.

### 6.1.3. Изменение параметров логических сетей

ВАЖНО

Логическую сеть нельзя редактировать или переместить на другой интерфейс, если она не синхронизирована с сетевой конфигурацией на хосте. Информацию о том, как синхронизировать сети, смотрите в Разделе 6.4.2.

**Изменение параметров логической сети**

1. Нажмите **Вычисления → Дата-центры**.
2. Нажмите на название дата-центра, чтобы открыть подробный просмотр.
3. Перейдите на вкладку **Логические сети** и выберите логическую сеть.
4. Нажмите **Параметры**.
5. Внесите необходимые изменения параметров.

ВНИМАНИЕ

Изменить название новой или существующей сети без остановки работы ВМ можно для всех сетей, кроме сети по умолчанию.

1. Нажмите **OK**.

ВНИМАНИЕ

В сетевой конфигурации с поддержкой нескольких хостов обновлённые сетевые параметры применяются автоматически ко всем хостам в дата-центре, которому присвоена эта сеть. Применения могут применяться только если ВМ, использующие эту сеть, не запущены. Нельзя переименовать логическую сеть, уже настроенную на хосте. Нельзя отключить параметр Сеть ВМ, пока выполняются виртуальные машины или шаблоны, использующие эту сеть.

### 6.1.4. Удаление логической сети

Удаление логической сети выполняется из меню **Сеть → Сети** или **Вычисления → Дата-центры**. В нижеследующей пошаговой последовательности показывается, как удалить логические сети, связанные с дата-центром. Для окружения виртуализации Red Hat необходима как минимум одна логическая сеть, используемая в качестве сети управления **ovirtmgmt**.

**Удаление логических сетей**

1. Нажмите **Вычисления → Дата-центры**.
2. Нажмите на название дата-центра, чтобы открыть подробный просмотр.
3. Перейдите на вкладку **Логические сети**, чтобы просмотреть список логических сетей в дата-центре.
4. Выберите логическую сеть и нажмите **Удалить**.
5. Опционально, отметьте параметр **Также удалить внешние сети из поставщика**, чтобы удалить логическую сеть как из виртуализированного ЦУ, так и с внешнего поставщика. Если внешний поставщик имеет режим только для чтения, то отметка для этого параметра будет неактивной.
6. Нажмите **OK**.

Логическая сеть будет удалена из виртуализированного ЦУ и больше не будет доступна.

### 6.1.5. Настройка логической сети, не являющейся сетью управления, в качестве маршрута по умолчанию.

Маршрут по умолчанию, используемый хостами в кластере, пролагается через сеть управления (ovirtmgmt). В нижеследующей пошаговой инструкции показано, как настроить логическую сеть, не являющуюся сетью управления, качестве маршрута по умолчанию.

**Предварительное условие:**

* Если используется частный параметр default\_route , то перед выполнением данной инструкции необходимо будет сначала удалить пользовательское значение на всех прикреплённых хостах.

Настройка роли маршрута по умолчанию

1. Нажмите **Сеть → Сети**.
2. Нажмите на название логической сети без функции управления, которая будет настраиваться в качестве маршрута по умолчанию, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Кластеры**.
4. Нажмите **Управление сетью**, чтобы открыть окно **Управление сетью**.
5. Отметьте галочкой параметр Маршрут по умолчанию соответствующего кластера.
6. Нажмите **OK**.

Когда сети будут присоединяться к хостам, маршрут по умолчанию хоста будет настроен на выбранную сеть. Рекомендуется настраивать роль маршрута по умолчанию перед тем, как хосты будут добавляться в кластер. Если в кластере уже есть хосты, то они могут выбиться из синхронизации до тех пор, пока администратор не синхронизирует с ними все изменения.

**Важные ограничения, связанные с IPv6**

* Для IPv6 поддерживается только статическая адресация.
* Если обе сети разделяют один и тот же шлюз (принадлежат одной и той же подсети), то роль маршрута по умолчанию можно перенести из сети управления (ovirtmgmt) в другую логическую сеть.
* Если хост и виртуализированный ЦУ располагаются в разных подсетях, то из-за удаления шлюза IPv6 виртуализированный ЦУ потеряет связь с хостом.
* При перемещении роли маршрута по умолчанию в сеть, не являющуюся сетью управления, шлюз IPv6 удаляется с сетевого интерфейса, а также выводится предупреждение: «В кластере *имя\_кластера* роль «маршрут по умолчанию» более не принадлежит сети ovirtmgmt. Шлюз IPv6 удаляется из этой сети.»

### 6.1.6. Просмотр или редактирование параметров шлюза логической сети

Для логической сети можно настроить шлюз, адрес IP и маску подсети. Это необходимо, когда на хосте существует несколько сетей, и трафик должен направляться по маршруту в конкретной сети, а не по маршруту по умолчанию.

Если на хосте существует несколько сетей, а шлюзы не настроены, обратный трафик будет направляться по маршруту по умолчанию, который может и не доходить до необходимой точки назначения. Это может повлечь за собой невозможность для пользователей получить ответ от хоста при использовании команды ping.

Система виртуализации Red Hat автоматически обрабатывает несколько шлюзов всякий раз, когда интерфейс начинает или завершает работу.

**Просмотр или редактирование параметров шлюза логической сети**

1. Нажмите **Вычисления → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру
3. Прейдите на вкладку **Сетевые интерфейсы**, чтобы увидеть список и параметры сетевых интерфейсов, подключённых к хосту.
4. Нажмите кнопку **Настроить сети хоста**.
5. Наведите курсор на присвоенную логическую сеть и нажмите на значок карандаша, чтобы открыть окно **Изменить сеть управления**.

В окне **Изменить сеть управления** показывается имя сети, протокол загрузки, а также адреса IP, маски подсети и шлюза. Сведения об адресах можно изменить вручную, выбрав **Статический** протокол загрузки.

### 6.1.7. Объяснение общих параметров логической сети

В таблице ниже описываются параметры вкладки **Общие** в окнах **Новая логическая сеть** и **Параметры логической сети**.

**Таблица 6.1. Параметры в окнах Новая логическая сеть и Параметры логической сети**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Название | Название логической сети. Это текстовое поле должно содержать уникальное название, состоящее из любого сочетания строчных и прописных букв, чисел, тире и символ нижнего подчёркивания.  Обратите внимание, что, хотя в названии логической сети может быть больше 15 символов, и оно может содержать символы, не входящие в таблицу ASCII, идентификатор на хосте (vdsm\_name) будет отличаться от указанного названия. См. <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/administration_guide/sect-The_VDSM_To_Network_Name_Tool#Vdsm_To_Network_Mapping_Tool> |
| Описание | Описание логической сети. Предел для этого текстового поля: 40 символов. |
| Комментарий | Поле для добавления удобочитаемого комментария для логической сети в простом текстовом формате. |
| Создать на внешнем поставщике | Даёт возможность создать логическую сеть до экземпляра OpenStack Networking, добавленного в виртуализированный ЦУ в качестве внешнего поставщика.  **Внешний поставщик** — даёт возможность выбрать внешнего поставщика, на котором будет создана логическая сеть. |
| Включить добавление тегов для VLAN | Добавление тегов для VLAN — это средство защиты, выдающее всему сетевому трафику, передающемуся по логической сети, особые характеристики. Трафик с тегами VLAN не может быть прочитан интерфейсами, не имеющими таких же характеристик. Использование виртуальных LAN в логических сетях также даёт возможность одному сетевому интерфейсу быть связанным с несколькими логическими сетями, имеющими разные метки VLAN. Если метки VLAN включены, введите числовое значение в данное текстовое поле. |
| Сеть ВМ | Отметьте этот параметр, если эту сеть используют только ВМ. Если трафик, для передачи которого используется эта сеть, создаётся не виртуальными машинами (например, обмен информацией между хранилищами), не отмечайте этот параметр. |
| **MTU** | Выберите либо параметр **По умолчанию**, который устанавливает максимальный размер пакета согласно значению, указанному в скобках (), либо **Пользовательское**, чтобы указать частное значение MTU для логической сети. Этот параметр можно использовать, чтобы сравнять значение MTU, поддерживаемое логической сетью, со значением MTU, поддерживаемым аппаратными составляющими интерфейса. Укажите **Пользовательское** числовое значение в текстовом поле. |
| Метка сети | Даёт возможность указать новую метку сети или выбрать метку из существующих, уже присвоенных сетевым интерфейсам хоста. При выборе существующей метки логическая сеть будет автоматически присвоена всем сетевым интерфейсам хоста с этой меткой. |
| Группы безопасности | Даёт возможность присвоить группы безопасности портам в этой логической сети. Параметр **Отключено** отключает группы безопасности, **Включено** — включает. При создании и подключении порта к этой сети, порт создаётся с активированной безопасностью. Это означает, что доступ к ВМ или от ВМ выполняется согласно настроенным на данный момент группам безопасности. Параметр **Наследовать из конфигурации** означает, что порты наследуют поведение, указанное в файле конфигурации, общем для всех сетей. Подробности смотрите в Разделе 6.3.3. |

### 6.1.8. Объяснение параметров кластеров при настройке логических сетей

В таблице ниже описываются параметры вкладки **Кластер** окна **Новая логическая сеть**.

**Таблица 6.2. Параметры новой логической сети**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Присоединить сеть к/отсоединить сеть от кластеров | Позволяет присоединить логическую сеть к кластеру или отсоединить сеть от кластера в дата-центре, а также указать, будет ли логическая сеть требуемой сетью для отдельных кластеров.  **Название** — название кластера, к которому применяются параметры. Это значение нельзя изменить.  **Присоединить все** — даёт возможность присоединить логическую сеть ко всем кластерам или отсоединить логическую сеть ото всех кластеров в дата-центре. Как вариант, можно выставить или убрать галочки напротив параметра **Присоединить** рядом с названием каждого кластера.  **Требуемые: все** — даёт возможность указать, является ли логическая сеть требуемой сетью на всех кластерах. Как вариант, можно выставить или убрать галочки напротив параметра **Требуемая** рядом с названием каждого кластера. |

### 6.1.9. Объяснение параметров профилей vNIC при настройке логических сетей

В таблице ниже описываются параметры вкладки **Профили vNIC** окна **Новая логическая сеть**.

**Таблица 6.3. Параметры новой логической сети**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Профили **vNIC** | Даёт возможность указать один или более профилей vNIC логической сети. Чтобы добавить или удалить профиль логической сети, нажмите значок плюса или минуса рядом с профилем vNIC. Первое поле служит для указания имени профиля.  **Открытый** — будет ли профиль доступен всем пользователям.  **QoS** — Профиль качества обслуживания сети, назначенный профилю vNIC. |

### 6.1.10. Настройка конкретного типа трафика для логической сети в окне «Управление сетями».

Укажите тип трафика в логической сети для оптимизации потока сетевого трафика.

**Настройка типов трафика для логических сетей**

1. Нажмите **Вычисления → Кластеры**.
2. Нажмите на имя кластера, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Логические сети**.
4. Нажмите **Управление сетями**.
5. Проставьте нужные галочки и настройте переключатели.
6. Нажмите **OK**.

ВНИМАНИЕ

Логические сети, предоставленные внешними поставщиками, должны использоваться как сети виртуальных машин; им нельзя присвоить специальные кластерные роли, такие, как сеть визуализации или сеть миграции.

### 6.1.11. Объяснение параметров в окне «Управление сетями»

В таблице ниже описываются параметры окна **Управление сетями**.

**Таблица 6.4. Параметры окна «Управление сетями»**

|  |  |
| --- | --- |
| **Поле** | **Описание/действие** |
| Присвоить | Присваивает логическую сеть всем хостам в кластере. |
| Требуемая | Сеть, обозначенная как «требуемая», должна оставаться в рабочем состоянии для обеспечения корректной работы связанных с ней хостов. Если требуемая сеть перестаёт функционировать, любые связанные с ней хосты становятся нерабочими. |
| Сеть ВМ | Логическая сеть, обозначенная как «сеть ВМ», переносит сетевой трафик виртуальных машин. |
| Сеть визуализации | Логическая сеть, обозначенная как «сеть визуализации», переносит сетевой трафик SPICE и контроллера виртуальной сети. |
| Сеть миграции | Логическая сеть, обозначенная как «сеть миграции», переносит трафик миграции ВМ и хранилищ. Если в этой сети произойдёт сбой, то вместо неё будет использована сеть управления (по умолчанию, **ovirtmgmt**). |

### 6.1.12. Изменение конфигурации виртуальной функции сетевой платы

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.

Технология виртуализации ввода-вывода с единым корнем (SR-IOV) даёт возможность использовать одно устройство PCIe в качестве нескольких отдельных устройств. Это достигается добавлением двух функций PCIe: физических функций (PF) и виртуальных функций (VF). Одна карта PCIe может иметь от одной до восьми физических функций, но каждая из этих физических функций может поддерживать ещё большее число виртуальных функций (в зависимости от устройства).

В виртуализированном ЦУ можно изменить конфигурацию сетевых плат с поддержкой SR-IOV, включая количество виртуальных функций на каждой плате, а также указать виртуальные сети, которым разрешён доступ к этим виртуальным функциям.

После того, как виртуальные функции были созданы, каждая из них может функционировать как отдельная сетевая плата, включая присвоение им одной или более логических сетей, создание сетевых связок с их участием, а также прямое присвоение им виртуальных NIC для сквозного доступа.

Для возможности прямого подключения vNIC к виртуальной функции, в профиле vNIC необходимо активировать возможность сквозного доступа. Смотрите Раздел 6.2.4 «Активация возможности сквозного доступа в профиле vNIC».

**Редактирование конфигурации виртуальной функции сетевой платы**

1. Нажмите **Вычисления → Хосты**.
2. Нажмите на название хоста с поддержкой SR-IOV, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**.
4. Нажмите кнопку **Настроить сети хоста**.
5. Выберите сетевую карту с поддержкой SR-IOV (отмечается значком ) и нажмите на значок карандаша.
6. Чтобы изменить число виртуальных функций, нажмите на разворачивающуюся кнопку **Параметр числа виртуальных функций** и измените значение в поле **Число виртуальных функций**.

ВАЖНО

Изменение числа VF удалит все предыдущие виртуальные функции на этом сетевом интерфейсе перед созданием новых, включая любые VF, к которым напрямую присоединены виртуальные машины.

1. Галочка **Все сети** проставлена по умолчанию, разрешая возможность доступа к виртуальным функциям для всех сетей. Чтобы указать отдельные виртуальные сети, которым разрешён доступ к виртуальным функциям, выберите переключатель **Конкретные сети**, чтобы увидеть список всех сетей. Затем можно либо отметить нужные сети, либо с помощью текстового поля **Метки** автоматически выбрать все сети с нужными сетевыми метками.
2. Нажмите **OK**.
3. В окне **Настроить сети хоста** нажмите на кнопку **OK**.

# 6.2. Виртуальные сетевые платы (vNIC)

### 6.2.1. Обзор профиля vNIC

Профиль виртуальной сетевой платы (vNIC) представляет собой набор параметров, который можно применить к отдельным картам сетевых интерфейсов в виртуализированном ЦУ. Профиль vNIC даёт возможность применить профили QoS сетей к vNIC, включить или отключить зеркалирование портов, а также добавлять или удалять частные свойства. Профиль vNIC также добавляет дополнительный слой для гибкого администрирования, где полномочия использовать эти профили можно выдать конкретным пользователям. Таким образом можно контролировать качество обслуживания, получаемое различными пользователями, использующими данную сеть.

### 6.2.2. Создание или изменение профиля vNIC

Создавайте или изменяйте профиль виртуальной сетевой платы для регулирования пропускной способности сети на уровне пользователей и групп.

ВНИМАНИЕ

При включении или отключении зеркалирования портов все ВМ, использующие связанный профиль, должны быть отключены до внесения изменений.

**Создание или редактирование профиля vNIC**

1. Нажмите **Сеть → Сети**.
2. Нажмите на имя логической сети, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Профили vNIC**.
4. Нажмите **Добавить** или **Изменить**.
5. Введите **Название** и **Описание** профиля.
6. В списке **QoS** выберите соответствующую политику качества обслуживания.
7. В выпадающем списке выберите **Сетевой фильтр** для управления исходящим и входящим трафиком сетевых пакетов виртуальных машин. Подробности о сетевых фильтрах смотрите <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/Virtualization_Deployment_and_Administration_Guide/index.html#sect-Virtual_Networking-Applying_network_filtering>
8. Отметьте галочкой параметр **Сквозной доступ**, чтобы включить возможность сквозного доступа для vNIC и разрешить прямое присвоение виртуальной функции устройствам. Включение сквозного доступа отключит QoS, сетевую фильтрацию и зеркалирование портов, так как эти возможности несовместимы со сквозным доступом. Подробные сведения о сквозном доступе смотрите в Разделе 6.2.4.
9. При выбранном параметре **Сквозной доступ** также опционально снимите отметку с параметра **С возможностью миграции**, чтобы отключить возможность миграции для vNIC, использующих этот профиль. Оставляя этот параметр отмеченным, дополнительно обратитесь к информации <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/virtual_machine_management_guide/#Live_migration_prerequisites>
10. Установите переключатели **Зеркалирование портов** и **Разрешить всем пользователям использовать этот профиль** в нужное положение.
11. Выберите частное свойство из списка свойств. По умолчанию здесь показывается пункт **Выберите ключ…**. Добавьте или удалите частные свойства с помощью кнопок **+** и **-**.
12. Нажмите **OK**.

Применяйте этот профиль к пользователям и группам для регулирования пропускной способности их сетей. После редактирования профиля vNIC необходимо либо перезапустить ВМ, либо выполнить горячее отключение и затем подключение vNIC.

### 6.2.3. Объяснение параметров в окне «Профиль сетевого адаптера ВМ»

**Таблица 6.5. Окно «Профиль сетевого адаптера ВМ»**

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Сеть | Выпадающий список доступных сетей, к которым можно применить профиль vNIC. |
| Название | Название профиля vNIC. Это должно быть уникальное имя, состоящее из любого сочетания прописных и строчных букв, чисел, тире и знаков подчёркивания между 1 и 50 символами. |
| Описание | Описание профиля vNIC. Заполнение этого поля рекомендуется, но не обязательно. |
| QoS | Выпадающий список доступных политик качества обслуживания сетей, которые можно применить к профилю vNIC. Политики QoS регулируют входящий и исходящий трафик vNIC. |
| Сетевой фильтр | Выпадающий список доступных сетевых фильтров, которые можно применить к профилю vNIC. Сетевые фильтры повышают безопасность сети, фильтруя типы пакетов, которые могут быть посланы с ВМ или на ВМ. Фильтр по умолчанию — vdsm-no-mac-spoofing, являющийся комбинацией no-mac-spoofing и no-arp-mac-spoofing. Дополнительные сведения о фильтрах, предоставляемых библиотекой libvirt, смотрите по ссылке <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/Virtualization_Deployment_and_Administration_Guide/sect-Virtual_Networking-Applying_network_filtering.html#sect-Applying_network_filtering-Advanced_Filter_Configuration_Topics>  Для виртуальных LAN и сетевых связок ВМ используйте <No Network Filter>. На доверенных ВМ отказ от использования сетевого фильтра может улучшить производительность.  ВНИМАНИЕ  Red Hat больше не поддерживает отключение сетевых фильтров с помощью указания значения false для параметра EnableMACAntiSpoofingFilterRules с использованием утилиты engine-config . Используйте для этого параметр <No Network Filter>. |
| Сквозной доступ | «Галочка» для переключения свойства сквозного доступа. Сквозной доступ позволяет vNIC напрямую подключаться к виртуальной функции сетевой карты хоста. Свойство сквозного доступа нельзя редактировать, если профиль vNIC присоединён к ВМ.  При включении сквозного доступа в профиле vNIC отключаются QoS, сетевые фильтры и зеркалирование портов. |
| С возможностью миграции | «Галочка» для переключения возможности миграции vNIC, использующей этот профиль. В обычных профилях vNIC миграция включена по умолчанию; галочка выставлена и её нельзя изменить. При отмеченном параметре **Сквозной доступ** становится доступным параметр **С возможностью миграции**. При необходимости, его можно отключить, чтобы запретить миграцию vNIC со сквозным доступом. |
| Зеркалирование портов | «Галочка» для переключения зеркалирования портов. Зеркалирование портов копирует сетевой трафик третьего уровня из логической сети на виртуальный интерфейс на виртуальной машине. По умолчанию этот параметр не выбран. Подробности см. по ссылке <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/technical_reference/#Port_Mirroring> |
| Частные свойства устройства | Выпадающее меню для выбора доступных частных свойств, применимых к профилю vNIC. Для добавления и удаления свойств используйте кнопки **+** и **–**, соответственно. |
| Разрешить всем пользователям использовать этот профиль | «Галочка» для переключения доступности профиля для всех пользователей в окружении. Параметр отмечен по умолчанию. |

### 6.2.4. Включение сквозного доступа в профиле vNIC

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.

Технология сквозного доступа в профиле vNIC даёт возможность прямого подключения vNIC к виртуальным функциям (VF) на сетевых платах с поддержкой SR-IOV. После этого vNIC будет обходить программную виртуализацию сети и подключаться напрямую к VF для прямого присвоения устройства.

Сквозной доступ нельзя включить, если профиль vNIC уже присоединён к vNIC; для избежания этой ситуации, во время данной пошаговой инструкции создаётся новый профиль. Если в профиле vNIC включается сквозной доступ, то в этом же профиле нельзя будет включить QoS, сетевые фильтры и зеркалирование портов.

Дополнительные сведения о SR-IOV, прямом присвоении устройств и аппаратном обеспечении для реализации всего вышеуказанного в системах виртуализации Red Hat смотрите по ссылке <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/hardware_considerations_for_implementing_sr-iov/index>

**Включение сквозного доступа**

1. Нажмите **Сеть → Сети**.
2. Нажмите на имя логической сети, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Профили vNIC**, чтобы увидеть список всех профилей vNIC для этой логической сети.
4. Нажмите **Добавить**.
5. Укажите **Название** и **Описание** профиля.
6. Отметьте галочкой параметр **Сквозной доступ**.
7. Опционально, отключите параметр С возможностью миграции для отключения миграции vNIC, использующих этот профиль. Если необходимо оставить этот параметр включённым, дополнительно обратитесь к <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/virtual_machine_management_guide/#Live_migration_prerequisites>
8. Выберите частное свойство из списка свойств. По умолчанию здесь показывается пункт **Выберите ключ…**. Добавьте или удалите частные свойства с помощью кнопок **+** и **-**.
9. Нажмите **OK**.

Профиль vNIC теперь поддерживает технологию сквозного доступа. Чтобы напрямую присоединить ВМ к сетевой плате или виртуальной функции PCI, подключите логическую сеть к сетевой плате и создайте на нужной ВМ, использующей профиль vNIC с поддержкой сквозного доступа, новую vNIC со **Сквозным доступом к PCI**. Подробные сведения об этих пошаговых действиях смотрите в Разделе 6.4.2 и по ссылке <https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/virtual_machine_management_guide/#Adding_a_Network_Interface>, соответственно.

### 6.2.5. Удаление профиля vNIC

Удалите профиль vNIC из окружения виртуализации.

**Удаление профиля vNIC**

1. Нажмите **Сеть → Сети**.
2. Нажмите на имя логической сети, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Профили vNIC**, чтобы увидеть список всех профилей vNIC.
4. Выберите один или более профилей и нажмите **Удалить**.
5. Нажмите **OK**.

### 6.2.6. Присвоение групп безопасности профилям vNIC

ВНИМАНИЕ

Эта возможность доступна только при конфигурации внешнего поставщика OpenStack Networking (neutron). Группы безопасности нельзя создать средствами виртуализированного ЦУ, их необходимо создавать при помощи OpenStack. Подробности смотрите по ссылке <https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/10/html-single/users_and_identity_management_guide/#project-security> .

Группы безопасности можно присваивать профилям vNIC тех сетей, которые были импортированы из экземпляра OpenStack Networking, и в которых используется расширение Open vSwitch. Группа безопасности – это набор принудительно применяемых правил, позволяющих фильтровать входящий и исходящий трафик на сетевом интерфейсе. В пошаговой инструкции ниже показывается, как группа безопасности присваивается профилю vNIC.

ВНИМАНИЕ

Группа безопасности опознаётся с помощью идентификатора этой группы, зарегистрированном в экземпляре OpenStack Networking. Найти идентификаторы групп безопасности указанного участника можно, выполнив следующую команду в системе с установленным комплексом OpenStack Networking:

# neutron security-group-list

**Присвоение групп безопасности профилям vNIC**

1. Нажмите **Сеть → Сети**.
2. Нажмите на имя логической сети, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Профили vNIC**.
4. Нажмите **Добавить** или выберите уже существующий профиль vNIC и нажмите **Изменить**.
5. В выпадающем списке частных свойств выберите **SecurityGroups. Пустое поле частного свойства означает применение параметров безопасности по умолчанию, которые разрешают исходящий трафик и обмен информацией, но запрещают весь входящий трафик извне изначальной группы безопасности. Обратите внимание, что если свойство SecurityGroups в дальнейшем будет удалено, это не повлияет на выбранную группу безопасности.**
6. Введите ID группы безопасности в текстовое поле, чтобы присвоить её профилю vNIC.
7. Нажмите **OK**.

Группа безопасности была присоединена к профилю vNIC. Весь трафик, проходящий через логическую сеть, к которой присоединён данный профиль, будет фильтроваться согласно правилам, определённым для этой группы безопасности.

### 6.2.7. Полномочия пользователей на профили vNIC

Настройте полномочия пользователей, чтобы привязать пользователей к определённым профилям vNIC. Присвойте роль **VnicProfileUser** пользователю, чтобы пользователь получил возможность использовать этот профиль. Запретите пользователям доступ к определённым профилям, удалив их полномочия на этот профиль.

**Пользовательские полномочия на профиль vNIC**

1. Нажмите **Сеть → Профиль vNIC**.
2. Нажмите на профиль vNIC, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Полномочия**, чтобы просмотреть текущие полномочия пользователя для этого профиля.
4. Чтобы изменить полномочия пользователя на профиль vNIC, нажмите **Добавить** или **Удалить**.
5. В окне **Добавить полномочия пользователю** нажмите **Мои группы**, чтобы отобразить группы пользователя. Этот параметр можно использовать для добавления полномочий другим пользователям в этих группах.

Полномочия пользователя на профиль vNIC были настроены.

### 6.2.8. Настройка профилей vNIC для интеграции с UCS

Системы Cisco’s Unified Computing System (UCS) используются для управлениями такими аспектами работы дата- центра, как вычислительные и сетевые ресурсы, а также ресурсы хранилищ.

С помощью профилей vNIC ловушка vdsm-hook-vmfex-dev даёт возможность ВМ подключаться к профилям портов, настроенным системой UCS,. Профили портов, настроенных системой UCS, содержат свойства и параметры, используемые в UCS для настройки виртуальных интерфейсов. Ловушка vdsm-hook-vmfex-dev устанавливается по умолчанию в составе VDSM. Подробности смотрите в Приложении A.

При создании машины, использующей профиль vNIC, эта машина будет использовать Cisco vNIC.

В последовательность действий по подготовке профиля vNIC к интеграции в UCS в качестве первого шага входит настройка частного свойства устройства. Во время настройки этого частного свойства любое существующее значение будет переопределено. При сочетании новых и уже существующих частных свойств, указывайте все частные свойства в команде, с помощью которой настраивается значение ключей. Указываемые свойства разделяются точкой с запятой.

ВНИМАНИЕ

Профиль порта UCS должен быть настроен в системе Cisco UCS до настройки профиля vNIC.

**Настройка частного свойства устройства**

1. Настройте честное свойство vmfex в виртуализированном ЦУ, и с помощью --cver укажите уровень совместимости кластера.

# engine-config -s CustomDeviceProperties='{type=interface;prop={vmfex=^[a-zA-Z0-9\_.-]{2,32}$}}' --cver=3.6

1. Убедитесь в том, что частное свойство vmfex было добавлено.

# engine-config -g CustomDeviceProperties

1. Перезапустите службу ovirt-engine.

# systemctl restart ovirt-engine.service

Настраиваемый профиль vNIC может принадлежать к новой или ужt существующей логичеcкой сети. Инструкцию по настройке новой логической сети смотрите в Разделе 6.1.2.

**Настройка профиля vNIC для интеграции в UCS**

1. Нажмите **Сеть → Сети**.
2. Нажмите на имя логической сети, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Профили vNIC**.
4. Нажмите **Добавить** или выберите уже существующий профиль vNIC и нажмите **Изменить**.
5. Укажите **Название** и **Описание** профиля
6. В списке частных свойств выберите свойство vmfex и введите название профиля порта UCS.
7. Нажмите **OK**.

# 6.3. Сети внешних поставщиков

### 6.3.1. Импортирование сетей из внешних поставщиков

Чтобы иметь возможность использовать сети от внешнего поставщика (OpenStack Networking или любой другой сторонний поставщик с реализацией OpenStack Neutron REST API), зарегистрируйте поставщика в виртуализированном ЦУ. Подробности смотрите в Разделе 11.2.3. Затем выполните следующую последовательность действий чтобы импортировать сети этого поставщика в виртуализированный ЦУ для возможности их использования виртуальными машинами.

**Импортирование сетей внешнего поставщика**

1. Нажмите **Сеть → Сети**.
2. Нажмите **Импорт**.
3. В выпадающем списке **Поставщик сетей** выберите внешнего поставщика. Сети, предоставляемые этим поставщиком, обнаруживаются автоматически и указываются в списке **Сети поставщика**.
4. В списке **Сети поставщика** отметьте галочками сети, которые нужно импортировать, и нажмите значок «стрелочка вниз», чтобы переместить эти сети в список **Сети для импорта**.
5. Имя импортируемой сети можно настроить. Для этого нажмите на имя сети в столбце **Название** и измените текст.
6. В выпадающем списке **Дата-центр** выберите дата-центр, в который будут импортированы сети.
7. Опционально, снимите галочку с пункта **Разрешить всем**, чтобы сеть не была доступна всем пользователям.
8. Нажмите **Импортировать**.

Выбранные сети будут импортированы в целевой дата-центр, и их можно будет присоединять к ВМ.

### 6.3.2. Ограничения при использовании сетей внешних поставщиков

Существуют следующие ограничения при использовании логических сетей, импортированных с внешнего поставщика, в системе виртуализации Red Hat.

* Логические сети, предлагаемые внешними поставщиками, должны использоваться как сети ВМ, и не могут быть использованы в качестве сетей визуализации
* Одну и ту же логическую сеть можно импортировать несколько раз, но только в разные дата-центры.
* В виртуализированном ЦУ невозможно редактировать параметры логических сетей, предоставляемых внешними поставщиками. Чтобы изменить параметры такой логической сети, их нужно редактировать напрямую во внешнем поставщике, предоставляющем эту логическую сеть.
* Для виртуальных сетевых карт, подключённых к логическим сетям внешних поставщиков, недоступно зеркалирование портов.
* Если ВМ использует логическую сеть внешнего поставщика, то этого поставщика невозможно удалить из виртуализированного ЦУ, пока логическая сеть используется виртуальными машинами.
* Сети, предоставляемые внешними поставщиками, не являются требуемыми сетями. В связи с этим, планирование для кластеров, в которые были импортированы подобные сети, не будет учитывать их во время выбора хостов. Кроме того, обеспечение доступности логических сетей на тех хостах в кластере, на которые эти сети были импортированы, входит в обязанности пользователей.

### 6.3.3. Настройка подсетей в логических сетях внешних поставщиков

Логическая сеть внешнего поставщика может присваивать адреса IP виртуальным машинам только в том случае, если в этой логической сети была настроена одна или более подсетей. Если подсети не были настроены, виртуальным машинам не будут присвоены адреса IP. При наличии одной подсети, виртуальным машинам будут присвоены адреса из этой подсети, а при наличии нескольких подсетей, машинам будут присвоены адреса из одной из доступных подсетей. За присвоение адресов IP отвечает служба DHCP, предоставляемая внешним поставщиком сети, в которой располагается логическая сеть.

Хотя виртуализированный ЦУ выполняет автоматическое обнаружение предварительно настроенных подсетей в импортированных логических сетях, добавить или удалить подсети логических сетей также можно вручную с помощью интерфейса виртуализированного ЦУ.

Если в качестве внешнего поставщика был добавлен Open Virtual Network (OVN) (ovirt-provider-ovn), то несколько подсетей можно соединить между собой с помощью роутеров. Для управления этими роутерами можно использовать [OpenStack Networking API v2.0](https://developer.openstack.org/api-ref/network/v2/?expanded=list-routers-detail,create-router-detail#routers-routers). Тем не менее, обратите внимание, что у ovirt-provider-ovn есть свои ограничения: отсутствует реализация Source NAT (enable\_snat в OpenStack API).

### 6.3.4. Добавление подсетей в логических сетях внешних поставщиков

Создайте подсеть в логической сети, предоставленной внешним поставщиком.

**Добавление подсетей в логических сетях внешних поставщиков**

1. Нажмите **Сеть → Сети**.
2. Нажмите на имя логической сети, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Подсети**.
4. Нажмите **Добавить**.
5. Укажите **Название** и **CIDR** новой подсети.
6. В выпадающем списке **Версия IP** выберите **IPv4** или **IPv6**.
7. Нажмите **OK**.

ВНИМАНИЕ

Для IPv6 поддерживается только статическая адресация.

### 6.3.5. Удаление подсетей из логических сетей внешних поставщиков

Удалите подсеть из логической сети внешнего поставщика.

**Удаление подсетей из логических сетей внешних поставщиков**

1. Нажмите **Сеть → Сети**.
2. Нажмите на имя логической сети, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Подсети**.
4. Выберите подсеть и нажмите **Удалить**.
5. Нажмите **OK**.

### 6.3.6. Присвоение групп безопасности логическим сетям и портам

ВНИМАНИЕ

Эта возможность доступна, только если в качестве внешнего поставщика сетей выбран Open Virtual Network (OVN) (в виде ovirt-provider-ovn). В виртуализированном ЦУ нельзя создавать группы безопасности. Группы безопасности необходимо создавать с помощью OpenStack Networking API v2.0 или Ansible.

Группа безопасности — это набор принудительно применяемых правил, позволяющих фильтровать входящий и исходящий трафик в сети. Группы безопасности можно также применять для фильтрации трафика на уровне портов.

В системе виртуализации Red Hat 4.2.7 группы безопасности по умолчанию отключены.

**Добавление групп безопасности в логические сети**

1. Нажмите **Вычисления → Кластеры**.
2. Нажмите на имя кластера, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Логические сети**.
4. Нажмите **Добавить сеть** и настройте её свойства: не забудьте выбрать в выпадающем списке **Внешний поставщик** пункт ovirt-provider-ovn . Подробности смотрите в Разделе 6.1.2.
5. В выпадающем списке **Группа безопасности** выберите **Включено**. Подробности смотрите в Разделе 6.1.7.
6. Нажмите OK.
7. Создайте группы безопасности с помощью [OpenStack Networking API v2.0](https://developer.openstack.org/api-ref/network/v2/#security-groups-security-groups) или [Ansible](https://docs.ansible.com/ansible/2.7/modules/os_security_group_module.html).
8. Создайте правила групп безопасности с помощью либо [OpenStack Networking API v2.0](https://developer.openstack.org/api-ref/network/v2/#security-groups-security-groups) либо [Ansible](https://docs.ansible.com/ansible/2.7/modules/os_security_group_module.html).
9. Обновите информацию о настроенных группах безопасности на портах.
10. Опционально: укажите, будет ли этот функционал безопасности включён на уровне портов. На данный момент это возможно только с помощью [OpenStack Networking API](https://developer.openstack.org/api-ref/network/v2/?expanded=update-port-detail#ports). Если атрибут port\_security\_enabled не был указан, то его значение по умолчанию будет совпадать со значением в сети, которой он принадлежит.

# 6.4. Хосты и организация сетей

### 6.4.1. Обновление сведений о характеристиках хоста

При добавлении хосту карты сетевого интерфейса, сведения о характеристиках хоста должны быть обновлены, чтобы карта отобразилась в виртуализированном ЦУ.

**Обновление сведений о характеристиках хоста**

1. Нажмите **Вычисления → Хосты** и выберите хост.
2. Нажмите **Управление → Обновить сведения о характеристиках хоста**.

Список сетевых карт выбранного хоста во вкладке **Сетевые интерфейсы** будет обновлён. Теперь в виртуализированном ЦУ можно использовать любые добавленные сетевые карты.

### 6.4.2. Изменение параметров сетевых интерфейсов и присвоение логических сетей хостам.

Администратор может изменять параметры физических сетевых интерфейсов, переносить сеть управления с одного физического интерфейса хоста на другой, а также присваивать логические сети физическим сетевых интерфейсам хоста. Также поддерживаются частные свойства «мост» и «ethtool».

ПРЕДУПРЕЖДЕНИЕ

Единственным способом изменить адрес IP хоста в системе виртуализации Red Hat является удаление хоста и повторное его добавление.

Сведения о том, как изменить параметры VLAN хоста, читайте в Разделе 6.4.4.

ВАЖНО

Логические сети внешних поставщиков невозможно присвоить физическим сетевым интерфейсам хоста; такие сети присваиваются хостам динамически по мере требований виртуальных машин.

ВНИМАНИЕ

Если коммутатор был настроен на предоставление сведений о протоколе LLDP, то, чтобы просмотреть текущую конфигурацию порта коммутатора, наведите курсор на физический сетевой интерфейс. Это может помочь в предотвращении создания неправильных конфигураций. Перед присвоением логических сетей мы рекомендуем проверить следующую информацию:

* ***Описание порта (TLV тип 4)* **и** *Системное имя (TLV тип 5)* **помогают определить, на какие порты и на какой коммутатор накладываются интерфейсы хоста.****
* ***Идентификатор VLAN порта* **показывает встроенный идентификатор VLAN, настроенный на порте коммутатора для кадров Ethernet без меток. Все виртуальные LAN, настроенные на порте коммутатора, показываются в виде сочетаний** *VLAN название* **и** *VLAN идентификатор***.****

**Изменение параметров сетевых интерфейсов хоста и присвоение хостам логических сетей**

1. Нажмите **Вычисления → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**.
4. Нажмите **Настроить сети хоста**.
5. При необходимости, наведите курсор на сетевой интерфейс хоста, чтобы просмотреть сведения о конфигурации, предоставляемой коммутатором.
6. Подключите логическую сеть к физическому сетевому интерфейсу хоста, выбрав и перетащив логическую сеть в область **Присвоенные логические сети** рядом с физическим сетевым интерфейсом хоста.

ВНИМАНИЕ

Если сетевая плата подключена более чем к одной логической сети, то только одна сеть может не быть VLAN. Все остальные логические сети должны быть уникальными VLAN.

1. Настройте локальную сеть:
   1. Наведите курсор на присвоенную логическую сеть и нажмите на значок карандаша, чтобы открыть окно **Изменить сеть управления**.
   2. Во вкладке **IPv4** выберите протокол загрузки: **Нет**, **DHCP или Статический. При выборе статического протокола укажите IP, Префикс сетевой маски/маршрутизации и Шлюз.**

ВНИМАНИЕ

Для протокола IPv6 поддерживаются только статическая адресация. Для настройки логической сети перейдите на вкладку **IPv6 **и создайте следующие записи:****

* + - Укажите *Статический протокол загрузки*.
    - Укажите *длину* *Префикса маршрутизации* с помощью прямой косой черты и десятичного числа. Например: /48
    - ***IP*:** полный адрес IPv6 сетевого интерфейса хоста. Например: 2001:db8::1:0:0:6
    - ***Шлюз*:** адрес IPv6 маршрутизатора источника. Например: 2001:db8::1:0:0:1

ВНИМАНИЕ

При смене адреса IP сети управления хоста, хост необходимо переустановить (Раздел 7.5.20), чтобы настроить адрес IP.

Каждая логическая сеть может иметь отдельный шлюз на базе шлюза сети управления. Это обеспечивает перенаправление трафика, приходящего в логическую сеть, через шлюз логической сети, а не через шлюз по умолчанию, используемый сетью управления.

ВАЖНО

Настройте все хосты в кластере на использование одного и того же стека IP в сети управления этих хостов; либо только IPv4, либо только IPv6. Двойной стек не поддерживается.

* 1. Используйте параметры во вкладке **QoS** для переопределения качества обслуживания сети по умолчанию. Выберите **Переопределить QoS** и укажите нужные значения в следующих полях:
     + **Взвешенная доля**: означает, какую долю пропускной способности логического канала нужно выделить конкретной сети, относительно других сетей, прикреплённых к этому же логическому каналу. Точная доля зависит от суммы долей всех сетей на этом канале. По умолчанию, это число в диапазоне от 1 до 100.
     + **Предел скорости [Мбит/сек]**: максимальная пропускная способность сети.
     + **Гарантированная скорость [Мбит/сек]**: минимальная пропускная способность, требуемая для сети. Гарантированная скорость на деле не гарантируется, и будет изменяться в зависимости от сетевой инфраструктуры и гарантированной скорости, запрашиваемой другими сетями на этом же логическом канале.
  2. Для настройки сетевого моста перейдите на вкладку **Задаваемые пользователем параметры** и в выпадающем списке выберите **bridge\_opts**. Введите действительный ключ и значение, придерживаясь следующего синтаксиса: *ключ=значение*. Несколько записей разделяются символом пробела. Действительными являются следующие ключи, с примерными значениями. Подробности об этих параметрах смотрите в Разделе B.1.

forward\_delay=1500

gc\_timer=3765

group\_addr=1:80:c2:0:0:0

group\_fwd\_mask=0x0

hash\_elasticity=4

hash\_max=512

hello\_time=200

hello\_timer=70

max\_age=2000

multicast\_last\_member\_count=2

multicast\_last\_member\_interval=100

multicast\_membership\_interval=26000

multicast\_querier=0

multicast\_querier\_interval=25500

multicast\_query\_interval=13000

multicast\_query\_response\_interval=1000

multicast\_query\_use\_ifaddr=0

multicast\_router=1

multicast\_snooping=1

multicast\_startup\_query\_count=2

multicast\_startup\_query\_interval=3125

* 1. Чтобы настроить свойства Ethernet, перейдите на вкладку **Задаваемые пользователем параметры** и в выпадающем списке выберите параметр **ethtool\_opts**. Укажите действительное значение, используя формат командных аргументов ethtool. Например:

--coalesce em1 rx-usecs 14 sample-interval 3 --offload em2 rx on lro on tso off --change em1 speed 1000 duplex half

В этом поле допускаются символы подстановки. Чтобы, например, применить один и тот же параметр ко всем интерфейсам этой сети, используйте:

--coalesce \* rx-usecs 14 sample-interval 3

Параметр **ethtool\_opts** по умолчанию недоступен; его необходимо добавить с помощью утилиты настройки виртуализированного ЦУ. Смотрите Раздел B.2. Дополнительную информацию о свойствах ethtool можно найти на странице руководства, введя в консоли команду man ethtool .

* 1. Для настройки протокола FCoE перейдите на вкладку **Задаваемые пользователем параметры** и выпадающем списке выберите параметр **fcoe**. Введите действительный ключ и значение, придерживаясь следующего синтаксиса: *ключ=значение*. Минимальное требуемое значение: enable=yes. Также можно добавить dcb= and auto\_vlan=[yes|no]. Отделяйте записи символом пробела. Параметр **fcoe** по умолчанию недоступен; его необходимо добавить с помощью утилиты настройки виртуализированного ЦУ. Смотрите Раздел B.3.

ВНИМАНИЕ

Для использования FCoE рекомендуется отдельная выделенная логическая сеть.

* 1. Чтобы сменить сеть хоста по умолчанию с сети управления (ovirtmgmt) на сеть, не являющуюся сетью управления, настройте маршрут этой сети по умолчанию. Подробности смотрите в Разделе 6.1.5.
  2. Если определение логической сети не синхронизировано с сетевой конфигурацией на хосте, отметьте галочкой параметр **Синхронизировать сеть**. Подробности о хостах без синхронизации и об их синхронизации смотрите в Разделе 6.4.3.

1. Отметьте параметр **Проверить доступность соединения между хостом и ЦУ**, чтобы проверить сетевое соединение. Это действие эффективно только для хостов, находящихся в режиме обслуживания.
2. Нажмите **OK**.

ВНИМАНИЕ

Если не все карты сетевых интерфейсов хоста отображаются в ЦУ, выберите меню *Управление → Обновить сведения о характеристиках хоста*, чтобы обновить список карт сетевых интерфейсов, доступных для этого хоста.

### 6.4.3. Синхронизация сетей хостов

Виртуализированный ЦУ помечает сетевой интерфейс статусом «вне синхронизации», когда определение интерфейса на хосте отличается от определений, хранящихся в ЦУ. Во вкладке **Сетевые интерфейсы** сети вне синхронизации помечаются значком , а в окне **Настроить сети хоста** — значком .

Когда сеть хоста находится вне синхронизации, то единственные действия, которые возможно выполнить с такими сетями в окне **Настроить сети хоста** — это отсоединение логической сети от сетевого интерфейса или её синхронизация.

**Каким образом хост может оказаться вне синхронизации**

Хост может получить статус «вне синхронизации», если:

* Изменения конфигурации были сделаны на хосте, а не в окне **Настроить логические сети**. Примеры изменения конфигураций:
  + Изменение идентификатора VLAN на физическом хосте
  + Изменение **Пользовательского MTU** на физическом хосте
* Хост был перемещён в другой дата-центр с тем же сетевым именем, но с другими значениями/параметрами.
* Свойство сети **Сеть ВМ** было изменено при помощи удаления моста вручную с хоста.

**Как предотвратить рассинхронизацию хостов**

Использование следующих лучших практических решений может предотвратить рассинхронизацию хостов:

1. Вносите изменения на Портале администрирования, а не локально на хосте.
2. Изменяйте параметры VLAN согласно инструкциям в Разделе 6.4.4.

**Синхронизация хостов**

Синхронизация определений сетевых интерфейсов хоста включает в себя применение используемых определений виртуализированного ЦУ на хосте. Если эти определения не являются требуемыми определениями, то после синхронизации хостов, обновите их определения с помощью интерфейса на Портале администрирования. Сети хостов можно синхронизировать на трёх уровнях:

* На уровне каждой логической сети
* На уровне каждого хоста
* На уровне каждого кластера

**Синхронизация сетей хоста на уровне логической сети**

1. Нажмите **Вычисления → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**.
4. Нажмите **Настроить сети хоста**.
5. Наведите курсор на сеть вне синхронизации и нажмите на значок карандаша, чтобы открыть окно **Свойства сети**.
6. Отметьте галочкой параметр **Синхронизировать сеть**.
7. Нажмите **OK** для сохранения изменений.
8. Нажмите **OK,** чтобы закрыть окно **Настроить сети хоста**.

**Синхронизация сетей хоста на уровне хоста**

* Нажмите на кнопку **Синхронизировать все сети** во вкладке **Сетевые интерфейсы** хоста, чтобы синхронизировать все интерфейсы хоста находящиеся вне синхронизации.

**Синхронизация сетей хоста на уровне кластера**

* Нажмите на кнопку **Синхронизировать все сети** во вкладке **Логические сети** кластера, чтобы синхронизировать все определения логических сетей кластера, находящиеся вне синхронизации.

ВНИМАНИЕ

Синхронизировать сети хоста можно также с помощью REST API. Смотрите [syncallnetworks](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/rest_api_guide/services#services-host-methods-sync_all_networks).

### 6.4.4. Изменение параметров VLAN хоста

Для смены параметров VLAN хоста необходимо удалить хост из виртуализированного ЦУ, изменить его параметры, и затем повторно добавить его в ЦУ.

Чтобы сохранить синхронизацию сетей, выполните следующие шаги:

1. Переместите хост в режим обслуживания.
2. Вручную удалите сеть управления с хоста. В результате хост станет доступен для подключений из новой VLAN.
3. Добавьте хост в кластер. ВМ, не подключённые напрямую к сети управления, могут безопасно выполнять миграцию между хостами.

При смене VLAN ID сети управления появляется следующее предупреждение:

Изменение некоторых параметров сети управления (напр., VLAN, MTU) может привести к потере связи с хостами дата-центра, если базовая сетевая инфраструктура не настроена на адаптацию к таким изменениям. Продолжить?

При продолжении, все хосты в дата-центре потеряют связь с виртуализированным ЦУ, и процесс миграции хостов в новую сеть управления завершится неудачей. Сеть управления получит статус «вне синхронизации».

ВАЖНО

При смене VLAN ID сети управления, для применения нового значения VLAN ID необходимо переустановить хост. См. Раздел 7.5.20.

### 6.4.5. Добавление нескольких виртуальных LAN на один сетевой интерфейс с помощью логических сетей

Для разделения трафика в рамках одного хоста, на один сетевой интерфейс можно добавить несколько VLAN.

ВАЖНО

Предварительно должно быть создано более одной логической сети, при этом для всех этих сетей в окнах *Новая логическая сеть* и *Параметры логической сети* должен быть отмечен параметр *Включить метки VLAN*.

**Добавление нескольких VLAN на один сетевой интерфейс с помощью логических сетей**

1. Нажмите **Вычисления → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**.
4. Нажмите **Настроить сети хоста**.
5. Перетащите логические сети с метками VLAN в область **Присвоенные логические сети** рядом с физическим сетевым интерфейсом. Благодаря меткам VLAN, физическому сетевому интерфейсу можно присвоить несколько логических сетей.
6. Измените параметры логических сетей:
   1. Наведите курсор на присвоенную логическую сеть и нажмите на значок карандаша.
   2. Если определение логической сети не синхронизировано с сетевой конфигурацией на хосте, отметьте галочкой параметр **Синхронизировать сеть**.
   3. Выберите **Протокол загрузки**:
      * **Нет**
      * **DHCP**
      * **Статический**
   4. Укажите **IP** и **Маску подсети**.
   5. Нажмите **OK**.
7. Отметьте галочкой параметр **Проверить доступность соединения между хостом и ЦУ**, чтобы выполнить проверку сети; это может быть сделано только для хостов, находящихся в режиме обслуживания.
8. Нажмите **OK**.

Добавьте логическую сеть к каждому хосту в кластере, отредактировав параметры сетевой платы на каждом хосте в кластере. После этого сеть будет готова к эксплуатации.

Эту процедуру можно повторять неоднократно, каждый раз выбирая и изменяя один и тот же сетевой интерфейс на хостах, чтобы добавить логические сети с разными тегами VLAN на один сетевой интерфейс.

### 6.4.6. Присвоение дополнительных адресов IPv4 сетям хостов

Сети хоста, такие, как сеть управления **ovirtmgmt, изначально создаются только с одним адресом IP. Это означает, что если в файле конфигурации сетевой платы (например, /etc/sysconfig/network-scripts/ifcfg-eth01) настроено несколько адресов IP, то сети хоста будет присвоен только первый указанный IP. Остальные адреса могут потребоваться при подключении к хранилищу или к серверу в отдельной частной подсети, использующей ту же самую сетевую плату.**

Ловушка vdsm-hook-extra-ipv4-addrs даёт возможность настроить дополнительные адреса IPv4 для сетей хоста. Более подробные сведения ловушках смотрите в Приложении A, VDSM и ловушки.

В нижеследующей пошаговой инструкции задачи, относящиеся к хосту, должны выполняться на каждом хосте, для которого необходимо настроить дополнительные адреса IP.

**Присвоение дополнительных адресов IPv4 сетям хоста**

1. На хосте, для которого необходимо настроить дополнительно адреса IPv4, установите пакет ловушки VDSM. Этот пакет по умолчанию доступен на хостах виртуализации, но на простых хостах его необходимо устанавливать дополнительно.

# yum install vdsm-hook-extra-ipv4-addrs

1. В виртуализированном ЦУ выполните следующую команду для добавления ключа:

# engine-config -s 'UserDefinedNetworkCustomProperties=ipv4\_addrs=.\*'

1. Перезапустите службу ovirt-engine:

# systemctl restart ovirt-engine.service

1. На Портале администрирования нажмите **Вычисления → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы** и нажмите **Настроить сети хоста**.
4. Наведите курсор на присвоенную логическую сеть и нажмите на значок карандаша.
5. В выпадающем списке **Задаваемые пользователем параметры** выберите пункт **ipv4\_addr** и добавьте дополнительный адрес IP и префикс (например 5.5.5.5/24). Несколько адресов IP должны разделяться запятой
6. Чтобы закрыть окно **Параметры сети**, нажмите **OK**.
7. Чтобы закрыть окно **Настроить сети хоста**, нажмите **OK**.

Дополнительные адреса IP не будут показаны в виртуализированном ЦУ, но для проверки того, что адреса были добавлены, можно выполнить команду ip addr show на хосте.

### 6.4.7. Добавление сетевых меток сетевым интерфейсам хоста

Использование сетевых меток сильно упрощает выполнение административных задач, связанных с присвоением логических сетей сетевым интерфейсам хоста. Присвоение метки ролевой сети (например, сети миграции, или сети визуализации) ведёт к массовому развёртыванию этой сети на всех хостах. Такое массовое добавление сетей реализуется с помощью протокола DHCP. Этот способ массового развёртывания был выбран вместо способа указывания статических адресов потому, что задачу многократного вписывания статических адресов IP невозможно масштабировать.

Существует два способа добавления меток сетевому интерфейсу хоста:

* Вручную, на портале администрирования
* Автоматически, с помощью службы меток LLDP

**Добавление сетевых меток на портале администрирования**

1. Нажмите **Вычисления → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**.
4. Нажмите **Настроить сети хоста**.
5. Нажмите **Метки** и сделайте щелчок ПКМ по кнопке **[Новая метка]**. Выберите физический сетевой интерфейс, которому нужно назначить метку.
6. В поле **Метка** введите имя сетевой метки.
7. Нажмите **OK**.

**Добавление сетевых меток с помощью службы меток LLDP**

С помощью службы меток LLDP можно автоматизировать процесс присвоения меток сетевым интерфейсам хоста в настроенном списке кластеров.

По умолчанию, служба меток LLDP запускается раз в час. Это удобно при замене аппаратных составляющих (сетевых карт, коммутаторов или кабелей) или изменении конфигураций коммутаторов.

**Предварительные условия**

* Интерфейс должен быть подключён к коммутатору Juniper
* Коммутатор Juniper должен предоставлять Port VLAN с помощью LLDP.

**Последовательность действий**

1. Настройте параметры username и password в файле /etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf:
   * username - имя пользователя администратора виртуализированного ЦУ, значение по умолчанию: admin@internal.
   * password - пароль администратора виртуализированного ЦУ, значение по умолчанию: 123456.
2. Настройте службу меток LLDP, обновив следующие значения в файле etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf:
   * clusters — список кластеров, через запятую, на которых должна выполняться служба. Cluster\*, например, означает, что служба меток будет выполняться в кластерах, название которых начинается со слова Cluster. Чтобы служба меток выполнялась во всех кластерах в дата-центре, введите \*. Значение по умолчанию — Def\*.
   * api\_url – полный URL-адрес API виртуализированного ЦУ. Значение по умолчанию: https://*полное\_доменное\_имя\_ЦУ*/ovirt-engine/api
   * ca\_file — путь до частного файла сертификата центра сертификации. Если сертификат не используется, оставьте пустое поле. Значение по умолчанию — пустое поле.
   * auto\_bonding — включает возможности службы меток LLDP по созданию сетевых агрегаций. Значение по умолчанию: true.
   * auto\_labeling — включает возможности службы меток LLDP по созданию меток. Значение по умолчанию: true.
3. При желании, можно настроить выполнение службы с другими интервалами, для этого измените значение параметра OnUnitActiveSec в файле etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer. Значение по умолчанию: 1h (1 час).
4. Настройте запуск службы «сейчас» и при загрузке, введя следующую команду:

# systemctl enable --now ovirt-lldp-labeler

Чтобы запустить службу вручную, введите:

# /usr/bin/python /usr/share/ovirt-lldp-labeler/ovirt\_lldp\_labeler\_cli.py

Мы присвоили сетевую метку сетевому интерфейсу хоста. Новые логические сети с такой же меткой будут автоматически присваиваться всем сетевым интерфейсам хоста, имеющим ту же метку. Удаление метки логической сети автоматически удалит эту сеть со всех сетевых интерфейсов хоста с такой же меткой.

### 6.4.8. Изменение полного доменного имени хоста

Для смены полного доменного имени хоста выполните следующие шаги.

**Обновление полного доменного имени (FQDN) хоста**

1. Переведите хост в режим обслуживания, при котором выполняется динамическая миграция ВМ на другой хост. Подробности смотрите в Разделе 7.5.15. Как вариант, вручную включите или перенесите все ВМ на другой хост.
2. Нажмите **Удалить**, а затем нажмите **OK**, чтобы удалить хост с портала администрирования.
3. Укажите новое имя хоста с помощью утилиты hostnamectl. Дополнительные параметры смотрите: <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/Networking_Guide/ch-Configure_Host_Names.html>

# hostnamectl set-hostname новое\_полное\_доменное\_имя

1. Перезагрузите хост.
2. Повторно зарегистрируйте хост в виртуализированном ЦУ. Подробности смотрите в Разделе 7.5.1.

### 6.4.9. Поддержка организации сетей с помощью IPv6

В большинстве контекстов система виртуализации Red Hat поддерживает статические сети IPv6.

ВНИМАНИЕ

Системе виртуализации Red Hat необходима включённая поддержка протокола IPv6 на тех компьютерах или ВМ, где работает виртуализированный ЦУ. Не отключайте поддержку IPv6 на этих компьютерах или ВМ, даже если в системе он не используется.

**Ограничения, связанные с IPv6**

* Поддерживается только статическая адресация IPv6. Динамическая адресация с помощью **DHCP** или **автоматическая настройка адресов без сохранения состояния** не поддерживаются.
* Адресация для двойного стека (IPv4 и IPv6) не поддерживается.
* Сетевые конфигурации OVN могут использовать только IPv4 или IPv6.
* Перевод кластеров с использования IPv4 на использование IPv6 не поддерживается.
* Для IPv6 можно настроить только один шлюз на хост.
* Если две сети разделяют один шлюз (находятся в одной подсети), то можно перенести роль маршрута по умолчанию из сети управления (ovirtmgmt) в другую логическую сеть. Хост и виртуализированный ЦУ должны иметь один и тот же шлюз IPv6. Если хост и виртуализированный ЦУ находятся в разных подсетях, ЦУ может потерять связь с хостом из-за потенциального удаления шлюза IPv6.
* Использование домена хранилищ на базе glusterfs, где сервер gluster использует адресацию IPv6, не поддерживается.

### 6.4.10. Установка и настройка технологии виртуализации ввода-вывода с единым корнем (SR-IOV)

Раздел полностью состоит только из ссылок на внешние документы.

# 6.5. Объединение сетевых интерфейсов

Network bonding combines multiple NICs into a bond device, with the following advantages:

Объединение сетевых интерфейсов (агрегирование каналов) — это объединение нескольких сетевых плат в единое устройство, имеющее следующие преимущества:

* Скорость передачи нескольких агрегированных интерфейсов выше, чем у одного отдельного интерфейса.
* Устойчивость к отказам, так как устройство связки не откажет до тех пор, пока не откажут все интерфейсы в его составе.

Использование физических сетевых интерфейсов одной марки и одной модели обеспечивает поддержку одних и тех же параметров и режимов связок.

ВАЖНО

Режим агрегации по умолчанию в системе виртуализации Red Hat, (Режим 4) Динамическое агрегирование каналов, требует коммутатора с поддержкой стандарта 802.3ad.

Логические сети одной связки должны быть совместимы друг с другом. Связка может поддерживать только одну логическую сеть, не являющуюся виртуальной LAN. Остальные логические сети должны иметь уникальные идентификаторы VLAN.

На портах коммутатора должна быть включена возможность агрегации. Конкретные инструкции ищите в документации производителей оборудования.

Создать устройство связки можно одним из следующих способов:

* Вручную на портале администрирования, для конкретного хоста
* Автоматически, с помощью службы меток LLDP (см. Раздел 6.5.2), для неагрегированных сетевых карт всех хостов кластера или дата-центра.

Если в окружении используется хранилище iSCSI и есть необходимость резервирования (избыточности), следуйте инструкциям для настройки механизма доступа iSCSI по нескольким путям (раздел 8.5.3).

### 6.5.1. Создание устройства связки на портале администрирования

Создать устройство связки на конкретном хосте можно на портале администрирования. Устройство связки может передавать трафик как с метками VLAN, так и без меток.

**Последовательность действий**

1. Нажмите **Вычисления → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**, чтобы увидеть список физических сетевых интерфейсов, присоединённых к хосту.
4. Нажмите **Настроить сети хоста**.
5. Проверьте параметры коммутатора. Если на коммутаторе было настроено предоставление информации о протоколе обнаружения топологии канального уровня (LLDP), наведите курсор на область физического интерфейса, чтобы просмотреть конфигурацию агрегирования портов коммутатора.
6. Перетащите сетевую карту на другую карту или в связку.

ВНИМАНИЕ

Две сетевые карты формируют новую связку. Связка и сетевая карта — добавление карты в уже существующую связку.

Если сетевые карты являются несовместимыми, то операция агрегирования будет заблокирована.

1. В выпадающих списках **Имя связки** и **Режим связки** выберите соответствующие пункты. Подробности смотрите в Разделе 6.5.3.

При выборе **Пользовательского** режима связки нужно ввести параметры связки в текстовое поле, смотрите примеры ниже:

* + Если существующее окружение не сообщает о состоянии каналов с помощью ethtool, то наблюдение за протоколом разрешения адресов (ARP) можно настроить, введя mode=1 arp\_interval=1 arp\_ip\_target=192.168.0.2.
  + Назначить карту с самой высокой пропускной способностью в качестве первичного интерфейса можно, введя mode=1 primary=eth0.

Исчерпывающий список параметров агрегирования и их описание можно посмотреть на Kernel.org по ссылке [Linux Ethernet Bonding Driver HOWTO](https://www.kernel.org/doc/Documentation/networking/bonding.txt) (Англ).

1. Нажмите **OK**.
2. Присоедините к новой связке логическую сеть и настройте её. Пошаговую инструкцию смотрите в Разделе 6.4.2.

ВНИМАНИЕ

Логическую сеть невозможно присоединить напрямую к отдельной сетевой карте в связке.

1. При желании, если хост находится в режиме обслуживания, можно выбрать пункт **Проверить доступность соединения между хостом и ЦУ**.
2. Нажмите **OK**.

### 6.5.2. Создание устройства сетевой связки с помощью службы меток LLDP

Служба меток LLDP даёт возможность автоматического создания устройства связки с использованием всех несвязанных сетевых плат для всех хостов в одном или более кластерах или в дата-центре. Режим агрегирования — [(режим 4) динамическое агрегирование каналов(802.3ad)](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html/administration_guide/sect-Network_Bonding#Bonding_Modes)(Раздел 6.5.3) .

Сетевые платы с несовместимыми логическими сетями нельзя агрегировать.

По умолчанию, служба меток LLDP запускается раз в час. Это удобно в ситуациях замены аппаратных составляющих (например, сетевые карты, коммутаторы или кабели) или изменений в конфигурации коммутатора.

**Предварительные условия**

* Интерфейс должен быть подключён к коммутатору Juniper
* Протокол управления агрегированием каналов на коммутаторе Juniper должен быть настроен с использованием LLDP.

**Последовательность действий**

1. Настройте параметры username и password в файле /etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf:
   * username - имя пользователя администратора виртуализированного ЦУ, значение по умолчанию: admin@internal.
   * password - пароль администратора виртуализированного ЦУ, значение по умолчанию: 123456.
2. Настройте службу меток LLDP, обновив следующие значения в файле etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf:
   * clusters — список кластеров, через запятую, на которых должна выполняться служба. Cluster\*, например, означает, что служба меток будет выполняться в кластерах, название которых начинается со слова Cluster. Чтобы служба меток выполнялась во всех кластерах в дата-центре, введите \*. Значение по умолчанию — Def\*.
   * api\_url – полный URL-адрес API виртуализированного ЦУ. Значение по умолчанию: https://*полное\_доменное\_имя\_ЦУ*/ovirt-engine/api
   * ca\_file — путь до частного файла сертификата центра сертификации. Если сертификат не используется, оставьте пустое поле. Значение по умолчанию — пустое поле.
   * auto\_bonding — включает возможности службы меток LLDP по созданию сетевых агрегаций. Значение по умолчанию: true.
   * auto\_labeling — включает возможности службы меток LLDP по созданию меток. Значение по умолчанию: true.
3. При желании, можно настроить выполнение службы с другими интервалами, для этого измените значение параметра OnUnitActiveSec в файле etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer. Значение по умолчанию: 1h (1 час).
4. Настройте запуск службы «сейчас» и при загрузке, введя следующую команду:

# systemctl enable --now ovirt-lldp-labeler

Чтобы запустить службу вручную, введите:

# /usr/bin/python /usr/share/ovirt-lldp-labeler/ovirt\_lldp\_labeler\_cli.py

1. Присоедините логическую сеть к новой связке и настройте её. Пошаговые инструкции ищите в Разделе 6.4.2.

ВНИМАНИЕ

Логическую сеть нельзя присоединять напрямую к отдельной сетевой плате в связке.

### 6.5.3. Режимы агрегирования

Алгоритм рассеивания пакетов определяется режимом агрегирования. (Подробности смотрите в руководстве [Linux Ethernet Bonding Driver HOWTO](https://www.kernel.org/doc/Documentation/networking/bonding.txt) (Англ.). режим агрегирования по умолчанию в системе виртуализации Red Hat — (Режим 4) динамическое агрегирование каналов(802.3ad).

Система виртуализации Red Hat поддерживает следующие режимы агрегирования каналов, поскольку они могут использоваться в сетях виртуальных машин (мостовые сети):

(Режим 1) Active-Backup

Остаётся активной только одна сетевая карта. При сбое активной карты её заменяет одна из запасных. Адрес MAC этой связки виден только на порте сетевого адаптера, что предотвращает путаницу, которая может случиться в случае смены адреса MAC связки, в соответствии с адресом MAC новой активной сетевой карты.

(Режим 2) Load Balance (balance-xor)

Сетевая карта, передающая пакеты, выбирается с помощью выполнения операции XOR для исходного и целевого адресов MAC, умноженных на фактор modulo общего числа сетевых карт. Этот алгоритм обеспечивает выбор одной и той же сетевой карты для каждого из целевых адресов MAC.

(Режим 3) Broadcast

Пакеты передаются на все сетевые карты.

(Mode 4) Dynamic Link Aggregation(802.3ad) (По умолчанию)

Сетевые карты объединяются в группы, разделяющие одни и те же параметры скорости и дуплекса. В активной группе связки используются все сетевые карты.

ВНИМАНИЕ

(Режим 4) Dynamic Link Aggregation(802.3ad) требует коммутатора с поддержкой протокола 802.3ad.

Физические интерфейсы в связке должны иметь одни и те же идентификаторы агрегатора. В противном случае во вкладке **Сетевые интерфейсы** виртуализированный ЦУ пометит связку значком восклицательного знака , и укажет значение 00:00:00:00:00:00 для параметра связки ad\_partner\_mac. Просмотреть идентификаторы агрегатора можно с помощью следующей команды:

# cat /proc/net/bonding/bond0

See <https://access.redhat.com/solutions/67546>.

Система виртуализации Red Hat не поддерживает следующие режимы агрегации, так как их нельзя использовать в мостовых сетях, и поэтому они несовместимы с логическими сетями виртуальных машин:

(Режим 0) Round-Robin

Сетевые карты передают пакеты в последовательном порядке. Пакеты передаются в петле, которая начинается с первой доступной сетевой платы в связке и заканчивается в последней доступной плате. Последующие петли начинаются с первой доступной сетевой платы.

(Mode 5) Balance-TLB, также называемый Transmit Load-Balance

В зависимости от нагрузки, исходящий трафик распределяется по всем сетевым картам в связке. Входящий трафик получает активная сетевая карта. В случае сбоя карты, получающей трафик, выделяется другая сетевая карта.

(Режим 6) Balance-ALB, также называемый Adaptive Load-Balance

(Режим 5) Balance-TLB комбинируется с балансировкой нагрузки по принятию пакетов трафика IPv4. Для балансировки входящей нагрузки используется согласование ARP.

# 6.6. Наблюдение и анализ сетевой активности

### 6.6.1. Общий обзор анализатора Skydive

Skydive можно использовать для мониторинга логических сетей, включая сети Open Virtual Networks (OVN), которые были настроены в качестве внешнего поставщика сетей (Раздел 11.2.8). Skydive предоставляет динамический обзор сетевой топологии, зависимостей и уязвимых мест, создаёт отчёты и выполняет аудит конфигураций.

Данные, предоставляемые Skydive, можно использовать для:

* Обнаружения потерь пакетов
* Проверки корректности установки системы с помощью захвата сетевой топологии кластеров, включая мосты и интерфейсы
* Проверки правильности применения ожидаемых параметров MTU
* Захвата сетевого трафика между виртуальными машинами или между ВМ и хостами

Подробную информацию о возможностях Skydive смотрите по ссылке <http://skydive.network>.

ВНИМАНИЕ

Skydive является экспериментальной функцией. Экспериментальные возможности не поддерживаются соглашениями об уровне обслуживания, могут иметь неполный функционал и не рекомендуются к использовании на производстве. Эти возможности предоставляют ранний доступ к будущим возможностям продукта, давая клиентам возможность протестировать функциональность и предоставлять отзывы, полезные для разработчиков.

### 6.6.2. Установка Skydive

**Последовательность действий**

1. Установите **skydive-ansible** на машине диспетчера виртуализации:

# yum --disablerepo="\*" --enablerepo="rhel-7-server-rpms,rhel-7-server-extras-rpms,rhel-7-server-rh-common-rpms,rhel-7-server-openstack-14-rpms" install skydive-ansible

1. Скопируйте файл/usr/share/ovirt-engine/playbooks/install-skydive.inventory.sample в текущий каталог и переименуйте его в inventory.
2. Измените файл inventory/01\_hosts следующим образом (полное содержимое смотрите ниже):
   1. Измените значение параметра **skydive\_os\_auth\_url**, указав полное доменное имя диспетчера виртуализации. Оно необходимо системе OVN, использующей то же полное доменное имя, что и диспетчер виртуализации.
   2. Измените значение **ovn\_provider\_username** , указав имя пользователя, используемое для поставщика OVN. Значение по уомлчанию указыавется в /etc/ovirt-provider-ovn/ovirt-provider-ovn.conf.
   3. Обновите **ovn\_provider\_password**.
   4. В разделе **[agents:children] <host\_group>** укажите сведения о хостах, кластерах или дата-центре, в которых устанавливаются агенты Skydive.

Просмотреть список действительных групп можно с помощью команды

/usr/share/ovirt-engine-metrics/bin/ovirt-engine-hosts-ansible-inventory | python -m json.tool

ВНИМАНИЕ

Нет необходимости явно указывать каждый хост. Чтобы установить программу-агент на всех хостах в кластере, добавьте **ovirt\_cluster\_Default**. Или, чтобы установить агента на всех хостах в дата-центре, добавьте **ovirt\_datacenter\_Default**.

**Пример файла Inventory**

[agents]

[analyzers]

[skydive:children]

analyzers

agents

[skydive:vars]

skydive\_listen\_ip=0.0.0.0

skydive\_deployment\_mode=package

skydive\_extra\_config={'agent.topology.probes': ['ovsdb', 'neutron'], 'agent.topology.neutron.ssl\_insecure': true}

skydive\_fabric\_default\_interface=ovirtmgmt

skydive\_os\_auth\_url=https://MANAGERS\_FQDN:35357/v2.0

skydive\_os\_service\_username=ovn\_provider\_username

skydive\_os\_service\_password=ovn\_provider\_password

skydive\_os\_service\_tenant\_name=service

skydive\_os\_service\_domain\_name=Default

skydive\_os\_service\_region\_name=RegionOne

[agents:vars]

ansible\_ssh\_private\_key\_file=/etc/pki/ovirt-engine/keys/engine\_id\_rsa

[agents:children]

host\_group

[analyzers]

localhost ansible\_connection=local

1. Запустите playbook:

# ansible-playbook -i inventory /usr/share/ovirt-engine/playbooks/install-skydive.yml /usr/share/skydive-ansible/playbook.yml.sample

1. Проверьте, распознаёт ли Skydive порт ВМ: перейдите по адресу http:// FQDN\_диспетчера\_виртуализации:8082, выберите ВМ и проверьте следующие поля в разделе **Метаданные** вкладки **Захват**:
   1. Manager: Neutron
   2. NetworkName: имя\_сети
   3. IPV4: *адрес*\_IP, если используется подсеть.

В Разделе 6.6.3 можно просмотреть пример использования Skydive для захвата сетевой активности.

### 6.6.3. Использование Skydive для тестирования сетевых подключений

В данном примере тестируется соединение между двумя хостами, имеющими сетевые карты с адресами IPv4. Сетевые карты подключены к логической сети с меткой VLAN 4. Сведения о присвоении адреса IP логической сети смотрите в Разделе 6.4.2.

**Последовательность действий**

1. Установите Skydive (Раздел 6.6.2)
2. Откройте Skydive по адресу **http://** FQDN\_диспетчера\_виртуализации**:8082**.
3. На карте сети откройте network\_4 хоста rhv-host1.
4. Во вкладке **Capture** нажмите **Create** и затем **Start**.
5. Повторите предыдущие шаги для network\_4 на хосте rhv-host0.
6. Перейдите на вкладку **Generate**.
7. Выберите eth0 на хосте rhv-host0 в качестве **Source** и eth0 на хосте rhv-host1 в качестве **Destination**.
8. В выпадающем списке **Type** выберите **ICMPv4/Echo Request**.
9. Нажмите **Inject** , чтобы внедрить пакет.
10. Перейдите на вкладку **Flows**. Результаты команды ping показываются в таблице. Если ping был удачным, будет показана строка с **ICMPv4** и исходный и целевой адреса IP. Если навести курсор на эту строку, то на карте сети жёлтым кружком будет выделена сеть network\_4.

Подробности работы со Skydive смотрите в документации <http://skydive.network/documentation/> (Англ.)

# 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. Обычные 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 об errata. Благодаря этому, This ensures that an external content host ID does not need to be maintained in Red Hat Virtualization

Учётная запись Satellite, используемая для управления хостом, должна иметь полномочия администратора и default organization set.

**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 работу 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 совершения событий, которые потенциально могут нарушить корректную работу VDSM, таких, как перезагрузки, или же проблем с сетью или хранилищем.

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 хоста, 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 VDSM о его статусе или же ждёт в течение временного 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 системе 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 access to storage not exposed using NFS, iSCSI, or 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 4Kбайт. Блочные хранилища необходимо настраивать в старом режиме (512Б 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. Несколько сетевых путей между хостом и хранилищем iSCSI предохраняет хост от простоя во время сбоя сетевого пути.