Инструкция по применению обновления №1 от 18.08.2025

При отсутствии сетевого доступа к онлайн-репозиториям zVirt, можно настроить локальные репозитории в соответствии с инструкцией.

1. Обновление хостов

1.1. Настройка репозиториев

Порядок действий:

1. Подключитесь по SSH или через веб-консоль к хосту.
2. Убедитесь, что включены репозитории **zvirt-main** и **zvirt-extras**:

```bash
dnf repolist all
```

Ожидаемый вывод команды:

```bash
repo id                                    repo name
status
zvirt-extras                               zVirt extras mirror repository
enabled
zvirt-main                                 zVirt 4.4 main repository
enabled
```

Если указанные репозитории отключены, их можно включить следующей командой:

```bash
dnf config-manager --enable "*"
```

После использования команды убедитесь, что все репозитории zVirt включились.

3. Настройте доступ к репозиториям:

```bash
zvirt-credentials.py -u <имя_пользователя> -p <пароль>
```

Если утилита не найдена, переустановите её:

```
wget --user=<имя_пользователя> --password=<пароль> https://repo-zvirt.orionsoft.ru/repository/zvirt-4/4.4/packages/zvirt-credentials-0.1.1-1.190019.zvirt.el8.noarch.rpm ①
dnf install -y zvirt-credentials-0.1.1-1.190019.zvirt.el8.noarch.rpm
```

① <имя_пользователя> и <пароль> берутся из лицензионного сертификата, выданного при покупке продукта.

Настроить доступ к репозиториям необходимо на всех хостах, которые используются в среде zVirt.

1.2. Проверка наличия обновлений

Предварительные требования:

- Обновлен Менеджер управления.
- На хостах настроены и активированы репозитории.

Проверка обновления может выполняться вручную или автоматически.

Автоматическая проверка выполняется через заданный интервал времени. Значение для интервала задается с помощью ключа конфигурации `HostPackagesUpdateTimeInHours`. Значение по умолчанию - 24 часа.

Для проверки текущего интервала, подключитесь по SSH к Менеджеру управления и выполните следующую команду:

```
engine-config --get=HostPackagesUpdateTimeInHours
```

Для установки нового значения используйте следующую команду:

```
engine-config --set HostPackagesUpdateTimeInHours=10 ①
```

① В этом примере устанавливается частота проверки равная 10 часам

Для ручной проверки обновлений выполните следующие действия:

1. Авторизуйтесь на портале администрирования с достаточными правами.
2. Перейдите в **Ресурсы > Хосты**.
3. Выделите нужный хост и нажмите **Настройки > Проверить обновления**.
4. В окне подтверждения нажмите **[OK]**.

После окончания проверки, при наличии доступных обновлений, в строке соответствующего хоста, а также в подробном представлении появится значок  .

1.3. Ручное обновление

Предварительные требования:

- На обновляемом хосте настроены и активированы репозитории.

1. Переведите хост в режим обслуживания (**Управление > Обслуживание**).
2. Подключитесь по SSH или через веб-консоль к хосту.
3. Выполните удаление всех метаданных, кешированных пакетов и заголовков с помощью команды:

```
dnf clean all
```

4. Очистите все исключения блокировки пакетов с помощью команды:

```
dnf versionlock clear
```

5. Выполните обновление:

```
dnf update -y
```

6. Перезагрузите хост:

```
reboot
```

1.4. Автоматическое обновление

Предварительные требования:

- Обновлен Менеджер управления.
- На обновляемом хосте(ах) настроены и активированы репозитории.

Обновление может быть выполнено как для отдельных хостов, так и для всех хостов указанного кластера.

1.4.1. Обновление всех хостов в кластере

Перед обновлением кластера учтите следующие особенности и ограничения:

- Обновление необходимо производить по одному кластеру.
- Если в кластере включена миграция, виртуальные машины автоматически мигрируют на другой хост в кластере.

- В кластере должно быть достаточно памяти для миграции виртуальных машин. В противном случае миграция зависнет и завершится сбоем. Уменьшить использование памяти можно путем выключения виртуальных машин в кластере.
- Виртуальные машины, закрепленные за хостами, не могут мигрировать. Такие виртуальные машины могут быть выключены вручную или автоматически с помощью активации соответствующего параметра обновления (см. ниже).
- Виртуальная машина HostedEngine не может мигрировать на стандартные хосты, поэтому убедитесь, что в кластере с ВМ HostedEngine есть хотя бы один дополнительный хост с ролью HosteEngine.

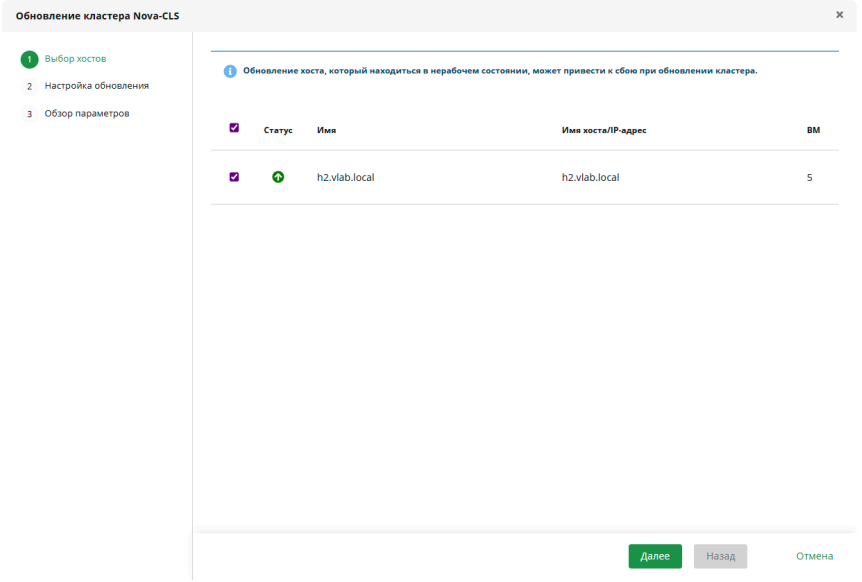
Порядок действий:

1. Авторизуйтесь на портале администрирования с правами, достаточными для обновления.
2. Перейдите в **Ресурсы** > **Кластеры**.

   Если была выполнена проверка наличия обновлений, то кластеры, для которых доступны обновления, отмечаются значком .

   Если проверка наличия обновлений не была выполнена, это можно сделать в визарде обновления с помощью активации соответствующего параметра обновления (см. ниже).
3. Выделите нужный кластер и нажмите **[Обновить]**.
4. В визарде обновления кластера:

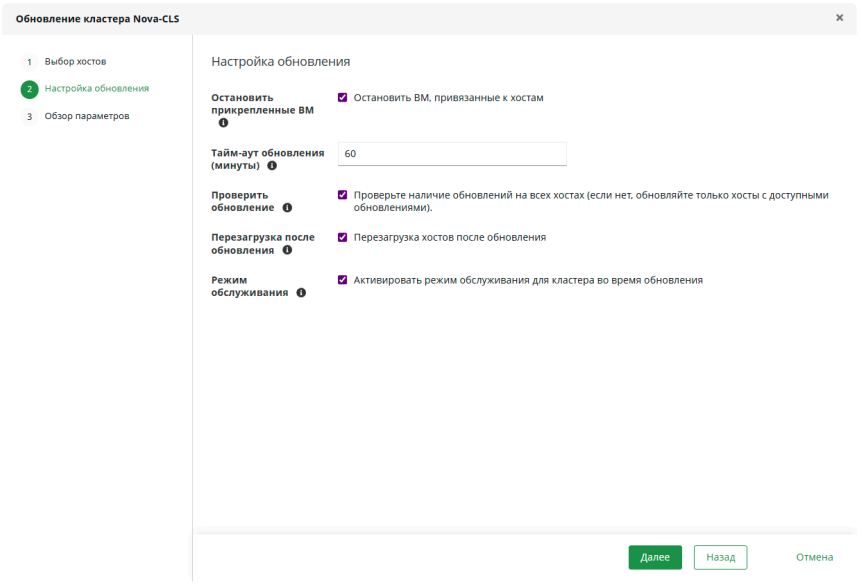
   a. Выберите хосты, для которых необходимо выполнить обновление и нажмите **[Далее]**.



   b. Укажите параметры обновления:

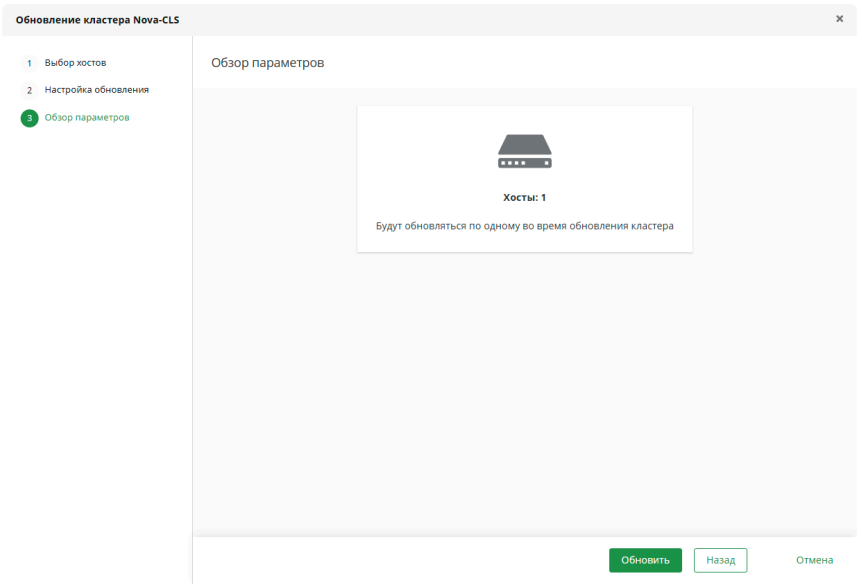
   - **Остановить прикрепленные ВМ**: при выборе останавливает все виртуальные машины, которые закреплены на хостах в кластере. Можно снять этот флажок, чтобы пропустить обновление хостов с закрепленными ВМ.

- **Тайм-аут обновления**: устанавливает время ожидания обновления отдельного хоста, прежде чем обновление кластера завершится сбоем. Значение по умолчанию — **60**. Таймаут можно увеличить для больших кластеров, где 60 минут может быть недостаточно, или уменьшить для небольших кластеров, где хосты обновляются быстро.
- **Проверить обновление**: проверяет каждый хост на наличие доступных обновлений перед запуском процесса обновления. Этот параметр можно активировать, чтобы убедиться, что для хостов имеются доступные обновления.
- **Перезагрузка после обновления**: перезагружает каждый хост после его обновления и выбран по умолчанию. Можно снять этот флажок, чтобы ускорить процесс, если вы уверены, что обновление не требует перезагрузки хоста.
- **Режим обслуживания**: устанавливает политику планирования `cluster_maintenance` на время обновления кластера. Она выбрана по умолчанию, поэтому активность ограничена, и виртуальные машины не могут запускаться, если они не являются высокодоступными. Вы можете снять этот флажок, если у вас есть настраиваемая политика планирования, которую вы хотите продолжать использовать во время обновления, но это может иметь неизвестные последствия.

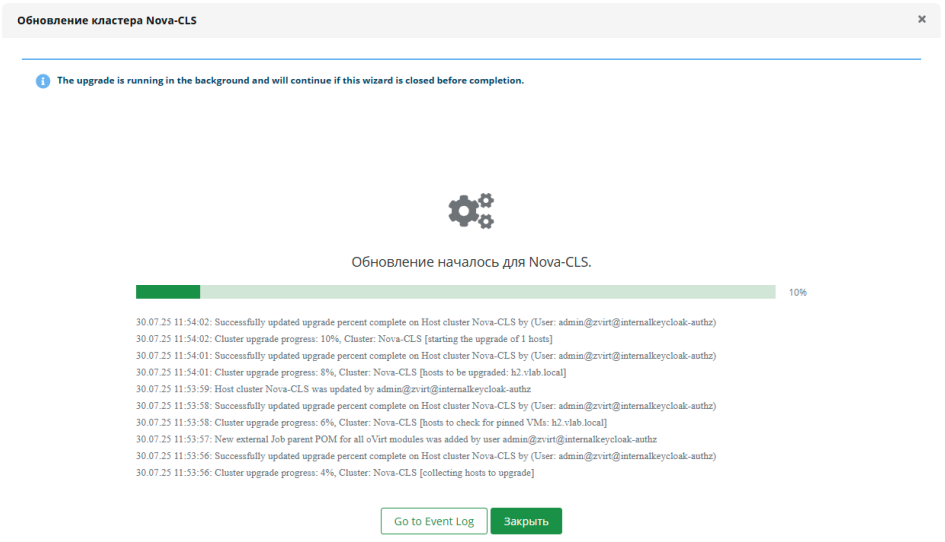


c. Нажмите **[Далее]**.

d. На странице обзора параметров проверьте количество обновляемых хостов и нажмите **[Обновить]**.



После начала обновления отображается экран статуса обновления кластера с индикатором выполнения и списком этапов, которые были завершены.



Вы можете нажать **[Go to Event Log]**, чтобы открыть записи журнала для обновления. Закрытие этого экрана не прерывает процесс обновления.

Процесс обновления можно наблюдать:

- На экране **Ресурсы > Кластеры** - в столбце **Доступность обновления** будет отображаться индикатор выполнения обновления.
- На экране **Ресурсы > Хосты** - обновляемые хосты будут иметь состояние **Installing** и помечены значком .
- В разделе **События** панели уведомлений.

1.4.2. Обновление отдельных хостов

Перед обновлением хостов учтите следующие особенности и ограничения:

- Если в кластере включена миграция, виртуальные машины автоматически мигрируют на другой хост в кластере.
- В кластере должно быть достаточно памяти для миграции виртуальных машин. В противном случае миграция зависнет и завершится сбоем. Уменьшить использование памяти можно путем выключения виртуальных машин в кластере.
- Виртуальные машины, закрепленные за хостами, не могут мигрировать. Такие виртуальные машины могут быть выключены вручную или автоматически с помощью активации соответствующего параметра обновления (см. ниже).
- Виртуальная машина HostedEngine не может мигрировать на стандартные хосты, поэтому убедитесь, что в кластере с ВМ HostedEngine есть хотя бы один дополнительный хост с ролью HosteEngine.

Порядок действий:

1. Авторизуйтесь на портале администрирования с правами, достаточными для обновления.
2. Перейдите в **Ресурсы > Хосты**.
3. Убедитесь, что хосты получили информацию о наличии обновлений. Хосты, для которых доступно обновление будут помечены значком .
4. Выделите нужный хост и нажмите **Настройки > Обновить**.
5. В окне подтверждения нажмите **[OK]**. Работающие виртуальные машины мигрируют на другие хосты кластера в соответствии с политикой миграции. Если миграция отключена для каких-либо виртуальных машин, вам будет предложено их выключить.

   В процессе обновления хост состояние хоста будет меняться в следующем порядке: **PreparingForMaintenance > Maintenance > Installing > Reboot > Up**.

   Если обновление не удалось, статус хоста изменится на **Install Failed**. В этом случае, изучив события и журналы, найдите и устраните причину ошибки и повторите процедуру обновления.
6. Повторите процедуру для остальных хостов кластера.

2. Обновление Менеджера управления

Порядок действий:

1. Если Менеджер управления развернут в режиме HostedEngine, активируйте режим глобального обслуживания:

   На хосте с **ВМ HostedEngine** режим глобального обслуживания кластера в веб-интерфейсе или выполнив, подключившись по SSH к хосту, следующие команды:

```
hosted-engine --set-maintenance --mode=global
hosted-engine --vm-status
```

Убедитесь, что включен режим глобального обслуживания - в выводе должна присутствовать надпись `!! Cluster is in GLOBAL MAINTENANCE mode !!`:

2. Подключитесь по SSH к Менеджеру управления и авторизуйтесь пользователем *root*.
3. Убедитесь, что включены репозитории **zvirt-main** и **zvirt-extras**:

```
dnf repolist all
```

Ожидаемый вывод команды:

```
repo id                                    repo name
status
zvirt-extras                               zVirt extras mirror repository
enabled
zvirt-main                                 zVirt 4.4 main repository
enabled
```

Если указанные репозитории отключены, их можно включить следующей командой:

```
dnf config-manager --enable "*"
```

После использования команды убедитесь, что все репозитории zVirt включились.

4. Настройте доступ к репозиториям:

```
zvirt-credentials.py -u <имя_пользователя> -p <пароль>
```

Если утилита не найдена, переустановите её:

```
wget --user=<имя_пользователя> --password=<пароль> https://repo-
zvirt.orionsoft.ru/repository/zvirt-4/4.4/packages/zvirt-credentials-0.1.1-
1.190019.zvirt.el8.noarch.rpm ①
dnf install -y zvirt-credentials-0.1.1-1.190019.zvirt.el8.noarch.rpm
```

① <имя_пользователя> и <пароль> берутся из лицензионного сертификата, выданного при покупке продукта.

5. Выполните удаление всех метаданных, кешированных пакетов и заголовков с помощью команды:

```
dnf clean all
```

6. Очистите все исключения блокировки пакетов с помощью команды:

```
dnf versionlock clear
```

7. Установите метапакет **zvirt-release-appliance**:

```
dnf install -y zvirt-release-appliance
```

8. Выполните обновление:

```
dnf update -y
```

9. Запустите реконфигурацию Менеджера управления:

```
engine-setup --offline
```

10. Перезапустите службы:

```
systemctl restart ovirt-engine zvirt-engine-backend
```

11. Если ранее был включен режим глобального обслуживания, отключите его:

```
hosted-engine --set-maintenance --mode=none
hosted-engine --vm-status
```

В выводе должно отсутствовать уведомление `!! Cluster is in GLOBAL MAINTENANCE mode !!`.

Управление кластерами

1. Введение в кластеры

Кластер - логическая группа хостов с общими доменами хранения и ЦП одного типа (Intel или AMD). Если модели ЦП хостов относятся к разным поколениям, то используются только те функции, которые присутствуют во всех моделях.

Каждый кластер в системе должен относиться к центру данных, а каждый хост в системе должен относиться к кластеру. Виртуальные машины динамически распределяются между хостами кластера и могут перемещаться между ними в соответствии с политиками, заданными в кластере, и настройками виртуальных машин. Кластер является самым высоким уровнем, на котором могут определяться политики электропитания и разделения нагрузки.

Количество хостов и количество виртуальных машин, относящихся к кластеру, отображаются в списке результатов поиска как **Количество хостов (Host Count)** и **Количество ВМ (VM Count)** соответственно.

В кластерах выполняются виртуальные машины или серверы хранения Gluster.

При развертывании гиперконвергентной среды эти функции могут быть включены для кластера одновременно.

Во время установки zVirt создает кластер `Default` в центре данных `Default`.

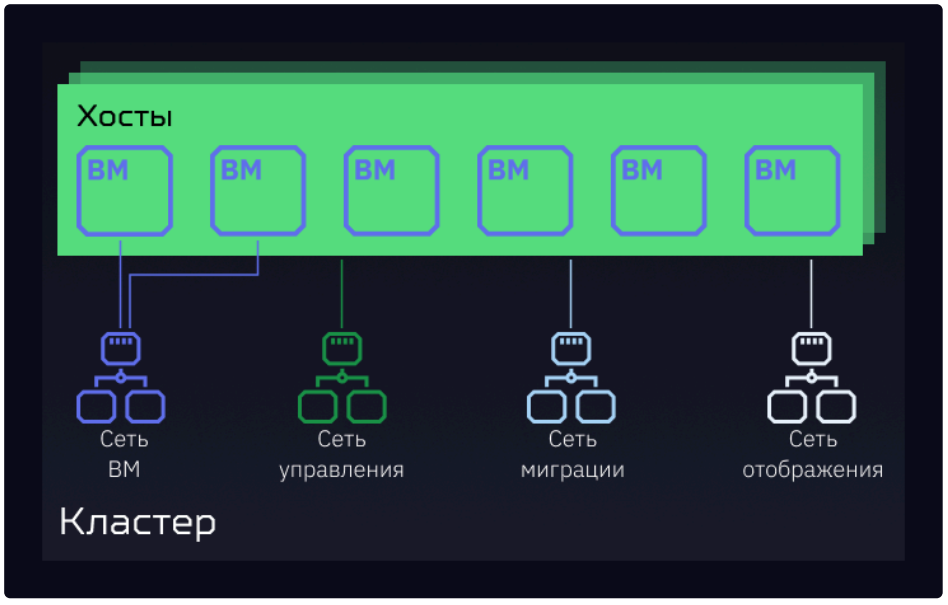


Рисунок 1. Кластер

2. Задачи, относящиеся к кластеру

Некоторые параметры кластеров не применимы к кластерам Gluster.

2.1. Создание нового кластера

Центр данных может содержать несколько кластеров, а кластер может содержать несколько хостов. Все хосты в кластере должны иметь одинаковую архитектуру ЦП. Чтобы оптимизировать типы ЦП, создавайте хосты до создания кластера. После создания кластера хосты можно сконфигурировать, нажав кнопку **[Помощник (Guide Me)]**.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Кластеры (Clusters)**.
2. Нажмите **[Новый (New)]**.
3. В выпадающем списке выберите **Центр данных (Data Center)**, к которому будет относиться кластер.
4. В поле **Имя (Name)** введите имя кластера.
5. В поля **Описание (Description)** и **Комментарий (Comment)** введите описание кластера и, при необходимости добавьте комментарий.
6. В выпадающем списке **Сеть управления (Management Network)** выберите сеть, чтобы назначить роль сети управления.
7. Выберите **Архитектура ЦП (CPU Architecture)**. При выборе `x86_64` становится доступным выбор **Тип чипсета/ПО (Chipset/Firmware Type)**.
8. В качестве **Типа ЦП (CPU Type)** выберите **самое старое семейство ЦП** среди хостов, которые войдут в кластер. Типы ЦП перечисляются от самого старого к самому новому.
9. В выпадающем списке выберите **Тип чипсета/ПО (Chipset/Firmware Type)** для создаваемых виртуальных машин и шаблонов в кластере.
10. Установите флажок **Изменить существующие ВМ/шаблоны с чипсетом I440fx на чипсет Q35 с BIOS (Change existing VMs/Templates from I440fx to Q35 Chipset with BIOS)** при необходимости.
11. В выпадающем списке выберите **Версию совместимости (Compatibility Version)** кластера.
12. В выпадающем списке выберите **Тип коммутатора (Switch Type)**.
13. Выберите **Тип межсетевого экрана (Firewall Type)** для хостов в кластере: **FirewallD** (по умолчанию) или **iptables**.
14. В выпадающем списке выберите **Провайдер сети по умолчанию (Default Network Provider)**

15. Установите **Максимальный порог памяти логирования (Maximum Log Memory Threshold)**
16. Установите флажок **Включить службу Virt (Enable Virt Service)** или **Включить службу Gluster (Enable Gluster Service)**, чтобы указать, будет ли кластер заполняться хостами с виртуальными машинами или узлами с включенной службой Gluster.
17. При желании можно установить флажок **Дополнительный источник генератора случайных чисел /dev/hwrng (Additional Random Number Generator source: /dev/hwrng source)**, чтобы указать аппаратный генератор случайных чисел, который будут использовать все хосты кластера. Устройство **/dev/urandom source** (предоставлено операционной системой Linux) включено по умолчанию.
18. Откройте вкладку **Оптимизация (Optimization)**, чтобы выбрать пороговое значение для совместного использования страницы памяти в кластере, а также при желании включите управление потоками ЦП, динамическое распределение памяти (memory ballooning), совместное использование памяти и выберите механизм её распределения на хостах кластера.
19. Откройте вкладку **Политика миграции (Migration Policy)**, чтобы определить политику миграции виртуальных машин в кластере.
20. Откройте вкладку **Политика планирования (Scheduling Policy)**, чтобы при желании настроить политику планирования и оптимизировать планировщик, включить доверенную службу для хостов кластера и резервирование высокой доступности (HA Reservation), а также выбрать политику серийных номеров.
21. Откройте вкладку **Консоль (Console)**, чтобы при желании переопределить глобальный SPICE-прокси (если он есть) и задать адрес SPICE-прокси для хостов кластера.
22. Откройте вкладку **Политика ограничения (Fencing policy)**, чтобы включить или выключить ограничение (изоляцию) в кластере, а также выберите опции, отвечающие за ограничение (изоляцию).
23. Откройте вкладку **Пул MAC-адресов (MAC Address Pool)**, чтобы указать пул MAC-адресов, отличный от заданного по умолчанию для кластера. Дополнительные сведения о способах создания, изменения или удаления пулов MAC-адресов см. в разделе Пулы MAC-адресов.
24. Нажмите **[OK]**, чтобы создать кластер и открыть окно **Помощник по созданию кластера (Cluster - Guide Me)**.
25. Окно **Помощник (Guide Me**) содержит список сущностей, которые нужно сконфигурировать для кластера. Сконфигурируйте эти сущности или отложите конфигурирование, нажав **Настроить позже (Configure Later)**. Чтобы возобновить конфигурирование, выберите кластер и нажмите **Дополнительные действия (More Actions) ⋮**, а затем нажмите **[Помощник (Guide Me)]**.

Хосты, у которых семейство ЦП старше указанного в поле **Тип ЦП (CPU Type)**, не могут стать частью этого кластера.

Добавлять хосты можно только к кластерам с типом межсетевого экрана **firewalld**.

2.2. Описание общих настроек кластера

В приведенной ниже таблице описаны настройки вкладки **Общее (General)** в окнах **Новый кластер (New Cluster)** и **Изменить кластер (Edit Cluster)**. При нажатии кнопки **[OK]** система подсвечивает некорректно введенные значения оранжевым цветом, не давая принять изменения. Кроме того, поля снабжены подсказками, которые указывают ожидаемые значения или диапазон значений.

Таблица 1. Общие настройки кластера

Поле	Описание/действие
Центр данных (Data Center)	Центр данных, в котором будет содержаться кластер. Центр данных должен быть создан до добавления кластера.
Имя (Name)	Имя кластера. В этом текстовом поле должно быть не больше 40 знаков. Имя должно быть уникальным и представлять собой любую комбинацию латинских букв в верхнем и нижнем регистре, цифр, дефисов и знаков подчеркивания.
Описание/комментарий (Description/Comment)	Описание кластера или дополнительные примечания. Эти поля являются рекомендованными, но не обязательными.
Сеть управления (Management Network)	Логическая сеть, которой будет назначена роль сети управления. По умолчанию - **ovirtmgmt**. Эта сеть также будет использоваться для миграции виртуальных машин, если сеть миграции не подключена к хосту-источнику или хосту-приемнику. В существующих кластерах сеть управления можно изменить, только нажав кнопку **Управление сетями (Manage Networks)** на вкладке **Логические сети (Logical Networks)** в подробном представлении.
Архитектура ЦП (CPU Architecture)	Архитектура ЦП кластера. Все хосты в кластере должны иметь указанную архитектуру. В зависимости от выбранной архитектуры ЦП доступны различные типы ЦП. • **не определено (undefined)**: все остальные типы ЦП. • **x86_64**: ЦП типа Intel и AMD.

Поле	Описание/действие
Тип ЦП (CPU Type)	Самое старое семейство ЦП в кластере. Список типов ЦП приведен в разделе Требования к ЦП в Руководстве по планированию и требованиям (Planning and Prerequisites Guide). Его изменение после создания кластера приведет к серьезному нарушению работы. Установите тип ЦП, ориентируясь на самую старую модель ЦП хоста в кластере. Использоваться могут только те функции, которые есть во всех моделях. Для ЦП типа Intel и AMD модели ЦП перечисляются в логическом порядке от самой старой к самой новой.
Версия совместимости (Compatibility Version)	Для zVirt 4.0 - 4.7. Нельзя выбрать более раннюю версию, чем та, что указана для центра данных.
Тип коммутатора (Switch Type)	Тип коммутатора, используемого кластером. • **Мост (Linux Bridge)** - стандартный коммутатор zVirt. • **Open vSwitch (OVS)**- обеспечивает поддержку сетевых функций Open vSwitch.
Тип межсетевого экрана (Firewall Type)	Указывает тип межсетевого экрана для хостов в кластере: **Firewalld** (по умолчанию) или **iptables**. Добавлять хосты можно только к кластерам с типом межсетевого экрана **firewalld**.
Провайдер сети по умолчанию (Default Network Provider)	Указывает внешнего поставщика сети по умолчанию, которого будет использовать кластер. Если выбрать **ovirt-provider-ovn**, то хосты, добавляемые в кластер, автоматически будут настраиваться на взаимодействие через поставщика OVN. Изменение поставщика сети по умолчанию потребует переустановки всех хостов в кластере для того, чтобы изменения вступили в силу.
Максимальный порог памяти логирования (Maximum Log Memory Threshold)	Задает пороговое значение максимального потребления памяти (в процентах или в виде абсолютной величины в МБ), факт достижения которого вносится в журнал. Сообщение вносится в журнал, если использование памяти хоста превышает это процентное значение или если объем доступной памяти хоста падает ниже абсолютного значения в МБ. Значение по умолчанию - 95%.
Включить службу Virt (Enable Virt Service)	При нажатии кнопки-переключателя хосты в этом кластере будут использоваться для запуска виртуальных машин.
Включить службу Gluster (Enable Gluster Service)	При нажатии кнопки-переключателя хосты в этом кластере будут использоваться в качестве узлов серверов хранения zVirt.

Поле	Описание/действие
Импорт существующей конфигурации Gluster (Import existing gluster configuration)	Этот флажок можно установить, только если отмечена кнопка-переключатель **Включить службу Gluster (Enable Gluster Service)**. Эта опция позволяет импортировать существующий кластер с поддержкой Gluster и все подключенные к нему хосты в менеджер управления. Следующие параметры необходимы для каждого хоста в импортируемом кластере: • **Адрес (Address)**: Введите IP-адрес или FQDN хост-сервера Gluster. • **Публичный ключ SSH хоста (Host ssh public key (PEM))**: позволяет обратиться к хосту без пароля и убедиться, что вы подключаетесь к правильному хосту. • **Пароль (Password)**: Введите root-пароль, необходимый для взаимодействия с хостом.
Дополнительный источник - генератор случайных чисел (Additional Random Number Generator source)	Если этот флажок установлен, то для всех хостов в кластере доступно дополнительное устройство - генератор случайных чисел. Это способствует распространению энтропии от генератора случайных чисел к виртуальным машинам.

2.3. Описание настроек оптимизации

Пояснения относительно памяти

Совместное использование страницы памяти позволяет виртуальным машинам использовать до 200% от выделенной им памяти благодаря использованию памяти, которая не используется в других виртуальных машинах. Этот процесс основан на том допущении, что виртуальные машины в среде zVirt не будут одновременно работать на полной мощности, а значит, неиспользуемую память можно временно выделить конкретной виртуальной машине.

Пояснения относительно ЦП

- Для процессов, не очень сильно загружающих ЦП, можно запускать виртуальные машины с общим количеством процессорных ядер, превышающим количество ядер хоста. Плюсы такого подхода следующие:
  - Можно запускать большее количество виртуальных машин, что снижает требования к оборудованию.
  - Это также позволяет конфигурировать виртуальные машины с топологиями ЦП, которые иначе были бы невозможны - например, когда количество виртуальных ядер находится в диапазоне между количеством ядер хоста и количеством потоков хоста.
- Для достижения наилучшей производительности и особенно для процессов, сильно загружающих ЦП, на виртуальной машине следует использовать ту же топологию,

что и на хосте, чтобы и для хоста, и для виртуальной машины ожидаемая работа кэша была одинаковой. Когда на хосте включена гиперпоточность, QEMU-процесс трактует гиперпотоки (hyperthreads) хоста как ядра, поэтому виртуальная машина не знает, что она работает на одном ядре с несколькими потоками. Такое поведение может повлиять на производительность виртуальной машины, поскольку виртуальное ядро, которое фактически соответствует гиперпотоку (hyperthread) в ядре хоста, может использовать один и тот же кэш вместе с другим гиперпотоком в том же ядре хоста, в то время как виртуальная машина трактует его как отдельное ядро.

В приведенной ниже таблице описаны настройки вкладки **Оптимизация (Optimization)** окон **Новый кластер (New Cluster)** и **Изменить кластер (Edit Cluster)**.

Таблица 2. Настройки оптимизации

Поле	Описание/действие
Оптимизация памяти (Memory Optimization)	• **Выключить перераспределение памяти (None - Disable memory overcommit)**: Отключает совместное использование страниц памяти. • **Для серверной нагрузки - разрешить перераспределение физической памяти на 150% от системной памяти на каждом хосте (For Server Load - Allow scheduling of 150% of physical memory)**: Устанавливает порог совместного использования страницы памяти в значение, равное 150% от объема системной памяти на каждом хосте. • **Для нагрузки рабочей станции - разрешить перераспределение физической памяти на 200% от системной памяти на каждом хосте (For Desktop Load - Allow scheduling of 200% of physical memory)**: Устанавливает порог совместного использования страницы памяти в значение, равное 200% от объема системной памяти на каждом хосте.
Симметричная многопоточность (Symmetric Multithreading)	Позволяет отключить использование гиперпоточности в ЦП (hyperhreading). При этом следующая опция **Потоки ЦП (CPU Threads)** становится недоступной
Потоки ЦП (CPU Threads)	Установка флажка **Считать потоки как ядра (Count Threads As Cores)** позволяет хостам обеспечить работу виртуальных машин с общим количеством процессорных ядер, превышающим количество ядер хоста. Если этот флажок установлен, открытые потоки хостов трактуются как ядра, которые виртуальные машины могут использовать. Например, 24-ядерная система с 2 потоками на ядро (всего 48 потоков) может запускать виртуальные машины, каждая из которых содержит до 48 ядер, а алгоритмы расчета загрузки ЦП хоста будут сравнивать нагрузку с удвоенным количеством потенциально используемых ядер.

Поле	Описание/действие
Динамическое выделение памяти (Memory Balloon)	Если установлен флажок **Включить оптимизацию динамического выделения памяти (Enable Memory Balloon Optimization)**, то на виртуальных машинах, работающих на хостах в этом кластере, становится возможным выделение памяти в объеме, превышающем физически доступный (memory overcommitment). Когда этот флажок установлен, **менеджер избыточного выделения памяти (Memory Overcommit Manager, MoM)** начинает применять динамическое выделение памяти во всех возможных ситуациях, при этом каждой виртуальной машине будет предоставлен как минимум тот гарантированный объем памяти, который был указан при её создании. Для динамического выделения памяти виртуальная машина должна иметь устройство balloon с соответствующими драйверами. Каждая виртуальная машина включает в себя такое устройство по умолчанию, если только оно не было удалено специально. Каждый хост в этом кластере получает обновление политики динамического выделения памяти, когда его статус меняется на **Включен (Up)**. При необходимости вы можете вручную обновить политику динамического выделения памяти на хосте, не меняя статус. Смотрите Обновление политики Менеджера избыточного выделения памяти (MoM) на хостах в кластере. Важно понимать, что в некоторых сценариях динамическое выделение памяти (ballooning) может вступать в конфликт с объединением одинаковых страниц памяти (KSM). В таких случаях Менеджер избыточного выделения памяти (MoM) будет пытаться скорректировать объем выделения памяти (ballooning), чтобы минимизировать конфликты. Кроме того, в ряде сценариев динамическое выделение памяти может привести к тому, что производительность для виртуальной машины будет неоптимальной. Администраторам рекомендуется с осторожностью использовать данную опцию в целях оптимизации.
Контроль KSM	Если выбрана опция **Включить KSM (Enable KSM)**, то MoM может запустить KSM, когда это необходимо и может дать экономию памяти, выгода от которой перевешивает затраты на ЦП.

2.4. Описание настроек политик миграции

Политика миграции определяет порядок миграции работающих виртуальных машин в случае сбоя хоста, в том числе время простоя виртуальной машины в процессе миграции, полосу пропускания сети и то, как виртуальным машинам присваивается приоритет.

Таблица 3. Описание настроек политик миграции

Политика	Описание
Значение по умолчанию для кластера - «Минимальный простой» (Minimal downtime)	Переопределение в vdsm.conf по-прежнему применимо. Гостевой хук-механизм выключен.

Политика	Описание
Минимальный простой (Minimal downtime)	Политика разрешает миграцию виртуальных машин в типичных ситуациях. У виртуальных машин не должно быть значительного простоя. Процесс миграции будет прерван, если синхронизация состояния памяти слишком затянулась (зависит от итераций QEMU, максимум 500 миллисекунд).
Миграция после копирования (Post-copy migration)	Когда применяется эта политика, она приостанавливает виртуальные ЦП мигрирующей виртуальной машины на хосте-источнике, переносит только минимальное количество страниц памяти, активирует виртуальные ЦП виртуальной машины на хосте-приемнике и переносит оставшиеся страницы памяти, пока виртуальная машина работает на хосте-приемнике. Политика миграции с пост-копированием сначала пытается провести предварительное копирование, чтобы убедиться, что синхронизация состояния памяти пройдет успешно. Миграция переключается в режим с пост-копированием, если при миграции виртуальной машины затянулась синхронизация состояния памяти. Так значительно сокращается время простоя мигрируемой виртуальной машины, а также гарантируется, что миграция завершится независимо от того, насколько быстро меняются страницы памяти виртуальной машины на хосте-источнике. Это оптимальный вариант для миграции виртуальных машин в условиях интенсивного непрерывного использования, когда их невозможно перенести стандартным способом с предварительным копированием. Недостаток этой политики заключается в том, что на этапе пост-копирования виртуальная машина может сильно замедлиться из-за переноса недостающих частей памяти между хостами. Если сетевое соединение прерывается до завершения процесса пост-копирования, то менеджер приостанавливает, а затем выключает работающую виртуальную машину. Не прибегайте к миграции с пост-копированием, если доступность виртуальной машины критически важна или если сеть миграции нестабильна.
Приостановка при необходимости (Suspend workload if needed)	Эта политика разрешает миграцию виртуальных машин в большинстве случаев, включая перенос виртуальных машин, на которых запущены ресурсоемкие процессы, но из-за этого могут происходить более длительные простои ВМ, чем при других настройках. Миграция, тем не менее, может быть прервана при экстремальных нагрузках.
Очень большие ВМ (Very large VMs)	Виртуальную машину нельзя перенести с помощью какой-либо другой политики, допускается рискованный механизм миграции, и миграцию не нужно шифровать. Виртуальная машина может испытывать значительные простои. Подробнее об этой политике см. в статье Миграция очень больших виртуальных машин.

В настройках полосы пропускания указывается максимальная пропускная способность исходящих и входящих миграций для каждого хоста.

Таблица 4. Описание полосы пропускания

Политика	Описание
Авто (Auto)	Полоса пропускания копируется из настройки **Ограничение скорости (Мбит/с) (Rate Limit (Mbps))** в политике QoS сети хоста (Host Network QoS) в центре данных. Если ограничение скорости не установлено, то оно рассчитывается как минимальное значение скорости соединения отправляющего и принимающего сетевых интерфейсов. Если ограничение скорости не установлено, а скорости каналов недоступны, то оно определяется локальной настройкой Менеджера виртуальных рабочих мест и серверов (VDSM) на отправляющем хосте.
Гипервизор (по умолчанию) (Hypervisor default)	Полоса пропускания контролируется локальной настройкой VDSM на хосте-источнике.
Пользовательский (Custom)	Задается пользователем (в Мбит/с). Это значение делится на количество одновременных миграций (по умолчанию 2, чтобы учесть входящие и исходящие миграции). Поэтому заданная пользователем полоса пропускания должна быть достаточно большой, чтобы вместить все одновременные миграции. Например, если **Пользовательская (Custom)** полоса пропускания задана в размере 600 Мбит/с, то максимальная полоса пропускания при миграции виртуальной машины на самом деле составляет 300 Мбит/с.

Политика отказоустойчивости определяет приоритет виртуальных машин при миграции.

Таблица 5. Настройки политики отказоустойчивости

Поле	Описание/действие
Мигрировать ВМ (Migrate Virtual Machines)	Переносятся все виртуальные машины в заданном порядке приоритетности.
Мигрировать только ВМ в режиме высокой доступности (Migrate only Highly Available Virtual Machines)	Переносятся только виртуальные машины с признаком высокой доступности, чтобы предотвратить перегрузку других хостов.
Не мигрировать виртуальные машины (Do Not Migrate Virtual Machines)	Не дает переносить виртуальные машины.

Таблица 6. Дополнительные свойства

Поле	Описание/действие
Включить шифрование при миграции (Enable migration encryption)	Эта настройка позволяет включить/отключить шифрование виртуальной машины в процессе миграции. • **Значение по умолчанию (Не шифровать) (Default (Don’t encrypt))** • **Шифровать (Encrypt)** • **Не шифровать (Don’t encrypt)**
Параллельные миграции (Parallel Migrations)	Позволяет включить функцию параллельных соединений для миграции. Подробнее см. в статье Настройка параллельных соединений для миграции.
Количество соединений ВМ миграций (Количество соединений ВМ миграций)	Позволяет указать количество соединений для параллельных миграций. Активируется при выборе **Custom** в поле **Параллельные миграции (Parallel Migrations)**. Допустимые значения от 2 до 255

2.5. Описание настроек политик планирования

Политика планирования позволяет задать параметры использования и распределения виртуальных машин между доступными хостами. Задайте политику планирования, чтобы включить автоматическую балансировку нагрузки между хостами в кластере. Независимо от политики планирования, виртуальная машина не запустится на хосте с перегруженным ЦП. По умолчанию ЦП хоста считается перегруженным, если нагрузка на него превышает 80% в течение 5 минут, но эти значения можно изменить с помощью политик планирования. Дополнительные сведения см. в разделе Политики планирования в Руководстве по администрированию.

Таблица 7. Свойства на вкладке политики планирования

Поле	Описание/действие

Поле	Описание/действие
Выбор политики	Выберите политику из выпадающего списка. • **Не назначена (none)**: Балансировка нагрузки или распределение питания между хостами для уже работающих виртуальных машин выключены. Этот режим выбран по умолчанию. Когда виртуальная машина запущена, ресурсы памяти и загрузка ЦП равномерно распределяются между всеми хостами в кластере. Дополнительные виртуальные машины, подключенные к хосту, не запустятся, если параметры `CpuOverCommitDurationMinutes`, `HighUtilization` или `MaxFreeMemoryForOverUtilized` этого хоста достигли заданных значений. • **Равномерное распределение (evenly_distributed)**: Распределяет нагрузку на оперативную память и ЦП равномерно между всеми хостами в кластере. Дополнительные виртуальные машины, подключенные к хосту, не запустятся, если параметры `CpuOverCommitDurationMinutes`, `HighUtilization` или `MaxFreeMemoryForOverUtilized` этого хоста достигли заданных значений. • **Обслуживание кластера (cluster_maintenance)**: Ограничивает активность в кластере во время выполнения задач технического обслуживания. Нельзя запускать новые виртуальные машины, кроме виртуальных машин с признаком высокой доступности. В случае отказа хоста виртуальные машины с признаком высокой доступности перезапустятся в установленном порядке, и любая виртуальная машина сможет мигрировать. • **Энергосбережение (power_saving)**: Распределяет загрузку ОЗУ и ЦП по подмножеству доступных хостов, чтобы снизить энергопотребление на недогруженных хостах. Если на некоторых хостах загрузка ЦП находится ниже нижнего значения загрузки дольше заданного интервала времени, то, чтобы их питание можно было отключить, все виртуальные машины переносятся с них на другие хосты. Дополнительные виртуальные машины, подключенные к хосту, не запустятся, если загрузка этого хоста достигла заданного верхнего значения загрузки. • **Равномерное распределение ВМ (vm_evenly_distributed)**: Распределяет виртуальные машины равномерно между хостами, исходя из количества виртуальных машин. Кластер считается несбалансированным, если на любом из хостов запущено больше виртуальных машин, чем указано в параметре `HighVmCount`, и есть хотя бы один хост, количество виртуальных машин на котором выходит за предельное значение параметра `MigrationThreshold`.

Поле	Описание/действие
Свойства	В зависимости от выбранной политики доступны следующие ниже свойства. При необходимости их можно изменить: • **HighVmCount**: Устанавливает минимальное количество виртуальных машин, которые должны работать на одном хосте для активизации балансировки нагрузки. По умолчанию это 10 работающих виртуальных машин на хост. Балансировка нагрузки будет включена, если хотя бы на одном хосте в кластере будет достигнуто значение параметра `HighVmCount` по количеству работающих виртуальных машин. • **MigrationThreshold**: Определяет "буфер" перед переносом виртуальных машин с хоста. Это максимальная разница (включительно) между количеством виртуальных машин на наиболее загруженном и наименее загруженном хостах. Кластер сбалансирован, если для каждого хоста в кластере количество виртуальных машин не выходит за пределы диапазона миграции. Значение по умолчанию - 5. • **SpmVmGrace**: Определяет количество слотов для виртуальных машин, которые должны быть зарезервированы на хостах SPM. Загрузка на хосте SPM будет ниже, чем на других хостах, т.е. эта переменная определяет, насколько меньше виртуальных машин может работать на хосте SPM по сравнению с другими хостами. Значение по умолчанию - 5. • **CpuOverCommitDurationMinutes**: Задает время (в минутах), в течение которого хост может работать при загрузке ЦП, выходящей за заданные значения, прежде чем вступит в действие политика планирования. Этот интервал времени позволяет избежать активации политики планирования и ненужной миграции виртуальных машин при временных скачках загрузки ЦП. Максимум два знака. Значение по умолчанию - 2. • **HighUtilization**: Выражается в процентах. Если в течение заданного интервала времени хост загружает ЦП на уровне верхнего предела загрузки или выше, то Менеджер управления будет переносить виртуальные машины на другие хосты кластера до тех пор, пока загрузка ЦП этого хоста не опустится ниже максимального порога. Значение по умолчанию - 80. Значение не может быть меньше **50** или больше **99**. • **LowUtilization**: Выражается в процентах. Если в течение заданного интервала времени хост загружает ЦП на уровне ниже нижнего предела загрузки, то Менеджер управления будет переносить виртуальные машины на другие хосты кластера. Менеджер управления отключит питание на исходном хосте и перезапустит его снова, когда того потребует балансировка нагрузки или когда в кластере не будет достаточно свободных хостов. Значение по умолчанию - 20. Значение не может быть больше **49**. • **ScaleDown**: Уменьшает влияние весовой функции Резервирование высокой доступности (HA Reservation) методом деления оценки хоста на указанную величину. Это необязательное свойство, которое может быть добавлено в любую политику, включая политику Не назначена (`none`). • **HostsInReserve**: Указывает количество хостов, которые должны продолжать работать, даже если на них нет запущенных виртуальных машин. Это

Поле	Описание/действие
	необязательное свойство, которое может быть добавлено к политике **Энергосбережение (power_saving)**. • **EnableAutomaticHostPowerManagement**: Включает автоматическое управление питанием на всех хостах в кластере. Это необязательное свойство, которое может быть добавлено к политике Энергосбережение (power_saving). Значение по умолчанию - верно (true). • **MaxFreeMemoryForOverUtilized**: Указывает минимальный объем свободной оперативной памяти, обязательный для хоста, в МБ. Если объем свободной оперативной памяти на хосте меньше указанного, то Менеджер управления считает хост перегруженным. Например, если установить для этого свойства значение 1 000, то хост, у которого меньше 1 ГБ свободной оперативной памяти, будет перегружен. Подробнее о том, как это свойство работает с политиками **Энергосбережение (power_saving)** и **Равномерное распределение (evenly_distributed)**, см. в Разделе Свойства политики планирования в кластере MaxFreeMemoryForOverUtilized и MinFreeMemoryForUnderUtilized. Это свойство можно добавить к политикам **Энергосбережение (power_saving)** и **Равномерное распределение (evenly_distributed)**. Хотя оно появляется в списке свойств для политики **Равномерное распределение ВМ (vm_evenly_distributed)**, оно не применяется к ней. • **MinFreeMemoryForUnderUtilized**: Указывает максимальный объем свободной оперативной памяти в МБ, который будет у хоста. Если объем свободной оперативной памяти на хосте больше указанного, то Менеджер управления считает, что хост недогружен. Например, если для этого параметра установить значение `10 000`, то хост, у которого больше 10 ГБ свободной оперативной памяти, будет недогружен. Подробнее о том, как это свойство работает с политиками **Энергосбережение (power_saving)** и **Равномерное распределение (evenly_distributed**) см. в Разделе Свойства политики планирования в кластере MaxFreeMemoryForOverUtilized и MinFreeMemoryForUnderUtilized. Это свойство можно добавить к политикам **Энергосбережение (power_saving)** и **Равномерное распределение (evenly_distributed)**. Хотя оно появляется в списке свойств для политики **Равномерное распределение ВМ (vm_evenly_distributed)**, оно не применяется к ней. • **HeSparesCount**: Устанавливает количество дополнительных узлов с ролью **hosted engine**, которые должны зарезервировать достаточно свободной оперативной памяти для запуска виртуальной машины с Менеджером управления в случае ее переноса или выключения. Другим виртуальным машинам запрещено запускаться на узле с ролью **hosted engine**, если из-за этого не останется достаточно свободной оперативной памяти для виртуальной машины с Менеджером управления. Это необязательное свойство, которое может быть добавлено к политикам **Энергосбережение (power_saving)**, **Равномерное распределение ВМ (vm_evenly_distributed)** и **Равномерное распределение (evenly_distributed)** Значение по умолчанию - 0.

Поле	Описание/действие
	• **VCpuToPhysicalCpuRatio**: Устанавливает пороговое значение соотношения виртуальных ЦП к физическим. Когда этот параметр установлен, при планировании виртуальной машины предпочтение отдается хостам с меньшей загрузкой процессора. Допустимые значения от 0 до 2.99.
Оптимизация планировщика (Scheduler Optimization)	Оптимизируйте планирование для взвешивания/упорядочивания хостов. • **Оптимизировать для утилизации (Optimize for Utilization)**: Включает модули взвешивания в процесс планирования для обеспечения наилучшего выбора. • **Оптимизировать для скорости (Optimize for Speed)**: Пропускает взвешивание хостов в случаях, когда имеется более десяти ожидающих запросов.
Включить Trusted Service (Enable Trusted Service)	Активирует интеграцию с сервером OpenAttestation. Прежде чем ее можно будет включить, введите сведения о сервере OpenAttestation с помощью инструмента engine-config. Сервер OpenAttestation и технология Intel Trusted Execution Technology (Intel TXT) больше недоступны.
Включить резервирование ресурсов для высокодоступных ВМ (Enable HA Reservation)	Менеджер управления будет отслеживать ресурсы кластера для виртуальных машин с признаком высокой доступности. Менеджер обеспечивает наличие достаточных ресурсов в кластере для виртуальных машин, обозначенных как ВМ с признаком высокой доступности, чтобы перенести их в случае внезапного отказа текущего хоста.

Поле	Описание/действие

Политика серийных номеров (Serial Number Policy)	Конфигурация политики присвоения серийных номеров каждой новой виртуальной машине в кластере:
	
	• **Значение по умолчанию для системы (System Default)**: Использует общесистемные значения по умолчанию в базе данных Менеджера управления. Для конфигурирования этих значений по умолчанию, используйте инструмент конфигурации механизма, чтобы установить значения `DefaultSerialNumberPolicy` и DefaultCustomSerialNumber. Эти пары ключ-значение сохраняются в таблице vdc_options в базе данных Менеджера управления.
	
	Для политики ***`DefaultSerialNumberPolicy`***
	
	◦ Значение по умолчанию: HOST_ID
	
	◦ Возможные значения: HOST_ID, VM_ID, CUSTOM
	
	◦ Пример командной строки:
	
	`engine-config --set DefaultSerialNumberPolicy=VM_ID`
	
	Перезапустите Менеджер управления для применения настроек.
	
	Для ***`DefaultCustomSerialNumber`***
	
	◦ Значение по умолчанию: Фиктивный серийный номер. Возможные значения: Любая строка (ограничение: максимум 255 знаков)
	
	◦ Пример командной строки:
	
	`engine-config --set DefaultCustomSerialNumber="My very special string value"`
	
	Перезапустите Менеджер управления для применения настроек.
	
	• **Идентификатор хоста (Host ID)**: Устанавливает серийный номер каждой новой виртуальной машины в значение, соответствующее UUID хоста.
	
	• **Идентификатор ВМ (Vm ID)**: Устанавливает серийный номер каждой новой виртуальной машины в значение, соответствующее UUID виртуальной машины.
	
	• **Пользовательский серийный номер (Custom serial number)**: Устанавливает серийный номер каждой новой виртуальной машины в значение, которое вы задаете в параметре Пользовательский серийный номер (Custom Serial Number).

Пользовательский серийный номер (Custom serial number)	Задает пользовательский серийный номер, который будет применен к новым виртуальным машинам в кластере.

Когда свободная память хоста падает ниже 20%, в журнал **/var/log/vdsm/mom.log** записывается предупреждение:

```
mom.Controllers.Balloon - INFO Ballooning guest:half1 from 1096400 to 1991580
```

/Var/log/vdsm/mom.log - это файл журнала Менеджера избыточного выделения памяти.

2.6. Свойства политики планирования в кластере MaxFreeMemoryForOverUtilized и MinFreeMemoryForUnderUtilized

В составе планировщика есть фоновый процесс, который переносит виртуальные машины в соответствии с текущей политикой планирования кластера и ее параметрами. Основываясь на различных критериях и их относительных весах в политике, планировщик непрерывно классифицирует хосты как хосты-источники или хосты-приемники и переносит отдельные виртуальные машины с одних на другие.

Ниже описано, как политики планирования в кластере **Равномерное распределение (evenly_distributed)** и **Энергосбережение (power_saving)** взаимодействуют со свойствами `MaxFreeMemoryForOverUtilized` и `MinFreeMemoryForUnderUtilized`. Хотя обе политики учитывают загрузку ЦП и памяти, загрузка ЦП не имеет отношения к свойствам `MaxFreeMemoryForOverUtilized` и `MinFreeMemoryForUnderUtilized`.

Если вы зададите свойства `MaxFreeMemoryForOverUtilized` и `MinFreeMemoryForUnderUtilized` как часть политики **равномерного распределения (evenly_distributed)**:

- Хосты, которые имеют меньше свободной памяти, чем `MaxFreeMemoryForOverUtilized`, являются перегруженными и становятся хостами-источниками.
- Хосты, которые имеют больше свободной памяти, чем `MinFreeMemoryForUnderUtilized`, являются недогруженными и становятся хостами-приемниками.
- Если значение `MaxFreeMemoryForOverUtilized` не указано, то планировщик не переносит виртуальные машины, исходя из загрузки памяти. (Он продолжает переносить виртуальные машины, исходя из других критериев политики, таких как загрузка ЦП.)
- Если значение `MinFreeMemoryForUnderUtilized` не указано, то планировщик считает, что все хосты могут становиться хостами-приемниками.

Если вы зададите свойства `MaxFreeMemoryForOverUtilized` и `MinFreeMemoryForUnderUtilized` как часть политики **Энергосбережение (power_saving)**:

- Хосты, которые имеют меньше свободной памяти, чем `MaxFreeMemoryForOverUtilized`, являются перегруженными и становятся хостами-источниками.
- Хосты, которые имеют больше свободной памяти, чем `MinFreeMemoryForUnderUtilized`, являются недогруженными и становятся хостами-источниками.
- Хосты, которые имеют больше свободной памяти, чем `MaxFreeMemoryForOverUtilized`, не являются перегруженными и становятся хостами-приемниками.
- Хосты, которые имеют меньше свободной памяти, чем `MinFreeMemoryForUnderUtilized`, не являются недогруженными и становятся хостами-приемниками.
- Планировщик предпочитает переносить виртуальные машины на хосты, которые не являются ни перегруженными, ни недогруженными. Если таких хостов недостаточно, планировщик может переносить виртуальные машины на недогруженные хосты. Если недогруженные хосты для этой цели не нужны, планировщик может выключить их.
- Если значение MaxFreeMemoryForOverUtilized не задано, то никакие хосты не являются перегруженными. Поэтому хостами-источниками являются только недогруженные хосты, а хостами-приемниками - все хосты в кластере.
- Если значение MinFreeMemoryForUnderUtilized не задано, то хостами-источниками являются только перегруженные хосты, а хостами-приемниками - хосты, которые не являются перегруженными.

Дополнительные ресурсы

- Описание настроек политик планирования.

2.7. Описание настроек консоли кластера

В приведенной ниже таблице описаны настройки вкладки **Консоль (Console)** в окнах **Новый кластер (New Cluster)** и **Изменить кластер (Edit Cluster)**.

Таблица 8. Настройки консоли

Поле	Описание/действие
Перезаписать адрес SPICE-прокси (Overridden SPICE proxy address)	Поставьте флажок в это поле, чтобы переопределить SPICE-прокси, заданный в глобальной конфигурации. Эта функция полезна, когда пользователь (например, подключающийся через Пользовательский портал) располагается вне сети, в которой находятся гипервизоры.

Поле	Описание/действие
Задать адрес SPICE-прокси для кластера (Define SPICE Proxy for Cluster)	Прокси-сервер, посредством которого клиент SPICE соединяется с виртуальными машинами. Адрес должен быть задан в следующем формате: `protocol://[host]:[port]`

2.8. Описание настроек журналирования

В приведенной ниже таблице описаны настройки вкладки **Журналирование (Logging)** в окнах **Новый кластер (New Cluster)** и **Изменить кластер (Edit Cluster)**.

Таблица 9. Настройки журналирования

Поле	Описание/действие
Определить адрес Syslog-сервера	При активации позволяет указать адрес сервера сбора журналов. Подробнее см. в разделе Настройка централизованного журналирования.
Использовать TCP-соединение	При активации, для передачи файлов журналов используется протокол TCP вместо UDP. Активация возможна только при активной опции **Определить адрес Syslog-сервера**.
Включить шифрование	При активации обеспечивает безопасное взаимодействие с сервером Syslog. Активация возможна только при активных опциях **Определить адрес Syslog-сервера** и **Использовать TCP-соединение**. Подробнее см. в разделе Настройка использования шифрования.

2.9. Описание настроек политик ограничения

В приведенной ниже таблице описаны настройки вкладки **Политика ограничения (Fencing Policy)** в окнах **Новый кластер (New Cluster)** и **Изменить кластер (Edit Cluster)**.

Таблица 10. Настройки политик ограничения

Поле	Описание/действие

Поле	Описание/действие
Включить ограничения (Enable fencing)	Включает изоляцию в кластере. Изоляция включена по умолчанию, но при необходимости ее можно выключить: например, если возникают или ожидаются временные проблемы в работе сети, администраторы могут отключить изоляцию до завершения диагностики или обслуживания. Внимание! Если изоляция выключена, виртуальные машины с признаком высокой доступности, работающие на хостах, находящихся в состоянии "не отвечает", не будут перезапущены где-либо еще.
Пропустить ограничение, если хост имеет аренду на хранилище (Skip fencing if host has live lease on storage)	Если этот флажок установлен, то никакие хосты в кластере, которые находятся в состоянии "не отвечает" и все еще подключены к хранилищу, не будут изолироваться.
Пропустить ограничение при проблемах подключения кластера (Skip fencing on cluster connectivity issues)	Когда этот флажок установлен, изоляция будет временно выключена, если процент хостов в кластере, испытывающих проблемы со связью, больше или равен заданному значению **Threshold**. Значение **Threshold** выбирается из следующего выпадающего списка: **25**, **50**, **75** и **100**.
Пропустить ограничение, если блоки Gluster активны (Skip fencing if gluster bricks are up)	Эта опция доступна только при включенной функции Gluster Storage. Когда этот флажок установлен, изоляция пропускается, если брики работают и доступны с других узлов того же ранга.
Пропустить ограничение, если кворум Gluster не соблюден (Skip fencing if gluster quorum not met)	Эта опция доступна только при включенной функции Gluster Storage. Когда этот флажок установлен, изоляция пропускается, если брики работают и выключение хоста вызовет потерю кворума.

2.10. Задание политик управления загрузкой и питанием для хостов в кластере

Политики планирования **Равномерное распределение (evenly_distributed)** и **Энергосбережение (power_saving)** позволяют задавать приемлемые значения загрузки ОЗУ и ЦП, а также момент, в который виртуальные машины нужно переносить на хост или с хоста. Политика планирования **Равномерное распределение ВМ (vm_evenly_distributed)** распределяет виртуальные машины равномерно между хостами, исходя из количества виртуальных машин. Задайте политику планирования, чтобы включить автоматическую балансировку нагрузки между хостами в кластере. Подробное описание каждой из политик планирования см. в разделе Описание настроек политик планирования.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Кластеры (Clusters)** и выберите кластер.
2. Нажмите **[Изменить (Edit)]**.

3. Откройте вкладку **Политика планирования (Scheduling Policy)**.

4. Выберите одну из следующих политик:

   - **none**
   - **vm_evenly_distributed**

     a. Чтобы включить балансировку нагрузки, в поле **HighVmCount** укажите минимальное количество виртуальных машин, которое должно быть запущено хотя бы на одном хосте.

     b. В поле **MigrationThreshold** задайте максимальную допустимую разницу между количеством виртуальных машин на наиболее загруженном и наименее загруженном хостах.

     c. В поле **SpmVmGrace** укажите количество слотов для виртуальных машин, которое должно быть зарезервировано на хостах SPM.

     d. При желании в поле **HeSparesCount** введите количество дополнительных узлов с ролью **hosted engine**, на которых нужно зарезервировать достаточно свободной оперативной памяти для запуска виртуальной машины с Менеджером управления в случае ее переноса или выключения. Дополнительную информацию см. в разделе Настройка слотов памяти.

   - **evenly_distributed**

     a. В поле **CpuOverCommitDurationMinutes** укажите время (в минутах), в течение которого хост может работать при загрузке ЦП, выходящей за заданные значения, прежде чем вступит в действие политика планирования.

     b. В поле **HighUtilization** укажите процент загрузки ЦП, при котором начинается миграция виртуальных машин на другие хосты.

     c. При желании в поле **HeSparesCount** введите количество дополнительных узлов с ролью hosted engine, на которых нужно зарезервировать достаточно свободной оперативной памяти для запуска виртуальной машины с Менеджером управления в случае ее переноса или выключения. Дополнительную информацию см. в разделе Настройка слотов памяти.

     d. Чтобы предотвратить чрезмерное использование хостом всех физических процессоров, задайте соотношение виртуальных и физических процессоров - **VCpuToPhysicalCpuRatio** со значением от 0 до 2.9. Когда этот параметр установлен, при планировании виртуальной машины предпочтение отдается хостам с меньшей загрузкой процессора.

     Если при добавлении виртуальной машины соотношение превысит заданный предел, будут учитываться как **VCpuToPhysicalCpuRatio**, так и загрузка процессора.

В рабочей среде, если соотношение **VCpuToPhysicalCpuRatio** хоста превышает 2.5, некоторые виртуальные машины могут быть сбалансированы по нагрузке и перемещены на хосты с более низким соотношением **VCpuToPhysicalCpuRatio**.

- **power_saving**

  a. В поле **CpuOverCommitDurationMinutes** укажите время (в минутах), в течение которого хост может работать при загрузке ЦП, выходящей за заданные значения, прежде чем вступит в действие политика планирования.

  b. В поле **LowUtilization** укажите процент загрузки ЦП, ниже которого хост будет считаться недогруженным.

  c. В поле **HighUtilization** укажите процент загрузки ЦП, при котором начинается миграция виртуальных машин на другие хосты.

  d. При желании в поле **HeSparesCount** введите количество дополнительных узлов с ролью hosted engine, на которых нужно зарезервировать достаточно свободной оперативной памяти для запуска виртуальной машины с Менеджером управления в случае ее переноса или выключения. Дополнительную информацию см. в разделе Настройка слотов памяти.

5. В качестве **Оптимизации расписания (Scheduler Optimization)** выберите для кластера одно из следующих значений:
   - **Оптимизировать для утилизации (Optimize for Utilization)**, чтобы включить модули взвешивания в процесс планирования для обеспечения наилучшего выбора.
   - **Оптимизировать для скорости (Optimize for Speed)**, чтобы пропустить взвешивание хостов в случаях, когда имеется более десяти ожидающих запросов.
6. При желании установите флажок в поле **Включить резервирование ресурсов для высокодоступных ВМ (Enable HA Reservation)**, чтобы Менеджер управления отслеживал ресурсы кластера для виртуальных машин с признаком высокой доступности.
7. При желании выберите **Политику серийных номеров (Serial Number Policy)** для виртуальных машин в кластере:
   - **Значение по умолчанию (System Default)**: Используйте системные значения по умолчанию, которые настраиваются в базе данных Менеджера управления с помощью инструмента настройки узла **engine**, и имена ключей **DefaultSerialNumberPolicy** и **DefaultCustomSerialNumber**. Значение по умолчанию для **DefaultSerialNumberPolicy** - это использовать ID хоста (Host ID). Дополнительную информацию см. в разделе Политики планирования.
   - **Хост ID (Host ID)**: Установите серийный номер каждой виртуальной машины в значение, соответствующее UUID хоста.
   - **Код ВМ (Vm ID)**: Установите серийный номер каждой виртуальной машины в значение, соответствующее UUID виртуальной машины.

- **Настраиваемый серийный номер (Custom serial number)**: Установите серийный номер каждой виртуальной машины в значение, которое вы задаете в следующем параметре **Пользовательский серийный номер (Custom Serial Number)**.

8. Нажмите **[OK]**.

2.11. Обновление политики Менеджера избыточного выделения памяти (MoM) на хостах в кластере

Менеджер избыточного выделения памяти управляет функциями баллунинга памяти и KSM на хосте. Относящиеся к кластеру изменения в этих функциях передаются хостам при следующем переходе хоста в состояние **Включен (Up)** 🔺 после перезагрузки или после режима обслуживания. Однако при необходимости важные изменения можно применить к хосту немедленно, синхронизировав политику **MoM**, когда хост находится в состоянии **Включен (Up)** 🔺. Следующую процедуру нужно выполнить на каждом хосте по отдельности.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Кластеры (Clusters)**.
2. Нажмите на имя кластера. Откроется подробное представление.
3. Откройте вкладку **Хосты (Hosts)** и выберите хост, который требует обновленной политики MoM.
4. Нажмите **[Политика синхронизации MoM (Sync MoM Policy)]**.

Политика MoM на хосте обновляется без необходимости переводить хост в режим обслуживания и обратно в состояние **Включен (Up)** 🔺.

2.12. Создание профиля ЦП

Профили ЦП определяют максимальную вычислительную мощность, которую виртуальная машина в кластере может получить на хосте, на котором она работает, выраженную в процентах от общей вычислительной мощности, доступной этому хосту. Профили ЦП создаются на основе профилей ЦП, определенных в центрах данных, и не применяются автоматически ко всем виртуальным машинам в кластере - чтобы профиль вступил в силу, его нужно вручную назначить отдельным виртуальным машинам.

Эта процедура предполагает, что вы уже задали одну или несколько политик QoS ЦП в центре данных, к которому относится кластер.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Кластеры (Clusters)**.
2. Нажмите на имя кластера. Откроется подробное представление.

3. Откройте вкладку **Профили ЦП (CPU Profiles)**.
4. Нажмите **[Новый (New)]**.
5. В поля **Имя (Name)** и **Описание (Description)** введите имя и описание профиля ЦП.
6. Выберите политику QoS, которую следует применить к профилю ЦП, из списка **QoS**.
7. Нажмите **[OK]**.

2.13. Удаление профиля ЦП

Удалите существующий профиль ЦП из среды zVirt.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Кластеры (Clusters)**.
2. Нажмите на имя кластера. Откроется подробное представление.
3. Откройте вкладку **Профили ЦП (CPU Profiles)** и выберите профиль ЦП, который нужно удалить.
4. Нажмите **[Удалить (Remove)]**.
5. Нажмите **[OK]**.

Если этот профиль ЦП был назначен каким-либо виртуальным машинам, то этим виртуальным машинам будет автоматически назначен профиль ЦП **default**.

2.14. Импортирование существующего кластера хранения Gluster

Можно импортировать кластер хранения Gluster и все принадлежащие ему хосты в Менеджер управления.

После указания таких сведений, как IP-адрес или имя хоста и пароль какого-либо хоста в кластере, на этом хосте через SSH будет выполнена команда `gluster peer status`, которая выведет список входящих в кластер хостов. Необходимо вручную проверить SSH-ключи каждого хоста и указать для них пароли. Невозможно импортировать кластер, если один из хостов в нем не работает или недоступен. Поскольку на только что импортированных хостах не установлен VDSM, скрипт начальной загрузки устанавливает все необходимые пакеты VDSM на хосты после их импорта и перезагружает их.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Кластеры (Clusters)**.
2. Нажмите **[Новый (New)]**.
3. Выберите **Центр данных (Data Center)**, которому будет принадлежать кластер.

4. В поля **Имя (Name)** и **Описание (Description)** введите имя и описание кластера.
5. Установите флажки в полях **Включить службу Gluster (Enable Gluster Service)** и **Импорт существующей конфигурации gluster (Import existing gluster configuration)**.

   Поле **Импорт существующей конфигурации gluster (Import existing gluster configuration)** отображается только при установленном флажке **Импорт существующей конфигурации gluster (Import existing gluster configuration)**.
6. В поле **Имя хоста (Hostname)** введите имя хоста или IP-адрес любого сервера в кластере.

   Отображается **публичный ключ SSH хоста (Host ssh public key (PEM))**, чтобы можно было убедиться, что соединение устанавливается с правильным хостом. Если хост недоступен или возникла сетевая ошибка, то в поле **публичный ключ SSH хоста (Host ssh public key (PEM))** будет отображаться ошибка **Ошибка при получении открытого ключа SSH (Error in fetching ssh public key)**.
7. Введите **Пароль (Password)** для сервера и нажмите **[OK]**.
8. Откроется окно **Добавить хосты (Add Hosts)**, и будет выведен список хостов, которые являются частью кластера.
9. Для каждого хоста введите **Имя (Name)** и **Root-пароль (Root Password)**.
10. Если вы хотите использовать один и тот же пароль для всех хостов, то установите флажок **Использовать общий пароль (Use a Common Password)**, чтобы ввести пароль в соответствующее текстовое поле.

    Нажмите **[Применить (Apply)]**, чтобы установить введенный пароль для всех хостов.

    Убедитесь, что SSH ключи действительны, и примените изменения, нажав **[OK]**.

Скрипт начальной загрузки установит все необходимые пакеты VDSM на хосты после их импорта и перезагрузит их. Вы успешно импортировали существующий кластер хранения Gluster в Менеджер управления.

2.15. Описание настроек в окне "Добавить хосты (Add Hosts)"

В окне **Добавить хосты (Add Hosts)** можно указать подробные сведения о хостах, импортированных как часть кластера Gluster. Это окно появится после установки флажка в поле **Включить службу Gluster (Enable Gluster Service)** в окне Создать кластер (New Cluster) и указания необходимых сведений о хосте.

Таблица 11. Настройки в окне "Добавить хосты Gluster (Add Gluster Hosts)"

Поле	Описание

Поле	Описание
Использовать общий пароль (Use a common password)	Установите этот флажок, чтобы использовать один и тот же пароль для всех хостов, принадлежащих кластеру. Введите пароль в поле **Пароль (Password)**, затем нажмите **[Применить (Apply)]**, чтобы установить этот пароль для всех хостов.
Имя (Name)	Введите имя хоста.
Имя/IP-адрес хоста (Hostname/IP)	В это поле автоматически подставляется FQDN или IP-адрес хоста, который вы задали в окне **Создать кластер (New Cluster)**.
Root Password (Root-пароль)	Введите пароль в это поле, чтобы использовать разные root-пароли для каждого хоста. Это поле переопределяет общий пароль, указанный для всех хостов в кластере.
Отпечаток (Fingerprint)	Отображается отпечаток хоста, чтобы можно было убедиться, что соединение устанавливается с правильным хостом. В это поле автоматически подставляется отпечаток хоста, который вы задали в окне **Создать кластер (New Cluster)**.

2.16. Удаление кластера

Перенесите все хосты из кластера перед его удалением.

> Кластер **Default** удалить невозможно, так как он содержит **пустой (Blank)** шаблон. Однако кластер **Default** можно переименовать и добавить в новый Центр данных.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Кластеры (Clusters)** и выберите кластер.
2. Убедитесь в том, что в кластере нет хостов.
3. Нажмите **Дополнительные действия (More Actions)** ⋮, а затем **[Удалить (Remove)]**.
4. Нажмите **[OK]**

2.17. Оптимизация памяти

Чтобы увеличить количество виртуальных машин на хосте, можно использовать **избыточное выделение памяти (memory overcommitment)**, при котором объем памяти, назначаемый виртуальным машинам, превышает объем ОЗУ и определяется областью подкачки.

Однако избыточное выделение памяти влечет за собой потенциальные проблемы:

- Производительность подкачки - область подкачки работает медленнее и потребляет больше ресурсов ЦП, чем ОЗУ, что влияет на производительность виртуальных машин. Чрезмерно интенсивная подкачка может привести к перегрузке ЦП.

- Демон остановки процессов при нехватке памяти (Out-of-memory, или OOM killer) - если на хосте заканчивается пространство подкачки, то новые процессы не могут запуститься и демон ядра OOM killer начинает завершать активные процессы (такие как гостевые процессы виртуальных машин).

Для решения этих проблем можно:

- Ограничить избыточное выделение памяти, используя настройку **Оптимизация памяти (Memory Optimization)** и **Менеджер избыточного выделения памяти (Memory Overcommit Manager, MoM)**.
- Сделать область подкачки достаточно большой, чтобы удовлетворить максимально возможные потребности в виртуальной памяти с запасом.
- Уменьшить объем виртуальной памяти, включив **баллунинг памяти (memory ballooning)** и **Объединение одинаковых страниц памяти (Kernel Same-page Merging, KSM)**.

2.18. Оптимизация памяти и избыточное выделение памяти

Можно ограничить величину избыточного выделения памяти, установив настройку **Оптимизация памяти (Memory Optimization)** в одно из следующих значений:

- **Выключить перераспределение памяти (None) - 0%**
- **Для серверной нагрузки (For Server Load) - 150%**
- **Для нагрузки рабочей станции (For Desktop Load) - 200%**.

Каждое значение соответствует процентной доле от объема ОЗУ. Например, если хост имеет 64 ГБ ОЗУ, выбор значения **Для серверной нагрузки (For Server Load) (150%)** означает, что может быть выделено дополнительно 32 ГБ и, таким образом, общий объем виртуальной памяти станет равен 96 ГБ. Если хост использует 4 ГБ из этого общего объема, то оставшиеся 92 ГБ будут доступны. Их можно назначить виртуальным машинам (**Оперативная память (разделяемая) (Memory Size)** на вкладке **Система (System)**), но оставьте какую-то часть не назначенной - в качестве запаса.

Внезапные скачки потребности в виртуальной памяти могут снизить производительность, а MoM и механизмы баллунинга памяти и KSM могут не успеть повторно оптимизировать виртуальную память. Чтобы уменьшить это воздействие, выберите ограничение, подходящее для используемых типов приложений и процессов:

- В отношении процессов, для которых характерен скорее плавный рост потребности в памяти, выберите более высокий процент, например **Для нагрузки рабочей станции (For Desktop Load) (200%)** или **Для серверной нагрузки (For Server Load) (150%)**.
- В отношении более критичных приложений или процессов, для которых характерны скорее внезапные скачки потребности в памяти, выберите более низкий процент,

например **Для серверной нагрузки (For Server Load) (150%)** или **Выключить перераспределение памяти (None) (0%)**. Выбор значения **Выключить перераспределение памяти (None)** предотвращает избыточное выделение памяти, но позволяет MoM и механизмам баллунинга памяти и KSM продолжать оптимизировать виртуальную память.

Всегда подвергайте настройки **Оптимизации памяти (Memory Optimization)** стресс-тестированию в широком диапазоне условий, прежде чем развернуть конфигурацию в продуктивной среде.

Чтобы настроить **Оптимизацию памяти (Memory Optimization)**, откройте вкладку **Оптимизация (Optimization)** в окне **Новый кластер (New Cluster)** или **Изменить кластер (Edit Cluster)**. См. раздел Описание настроек оптимизации.

Дополнительные комментарии

- Фактическую доступную память нельзя определить в реальном времени, поскольку степень оптимизации памяти, обеспечиваемой механизмами KSM и баллунинга памяти, все время меняется.
- Если виртуальная машина достигла предела виртуальной памяти, в ней не смогут запуститься новые приложения.
- При планировании количества виртуальных машин, которые будут работать на хосте, используйте в качестве отправной точки максимальный объем виртуальной памяти (объем физической памяти и настройку **Оптимизация памяти (Memory Optimization)**). Не учитывайте небольшие объемы виртуальной памяти, достигаемые благодаря оптимизации памяти, такой как баллунинг памяти и KSM.

2.19. Область подкачки и избыточное выделение памяти

Оценивая общий размер виртуальной памяти, отталкивайтесь от объема физической памяти и настройки **Оптимизация памяти (Memory Optimization)**. Исключите любое уменьшение объема виртуальной памяти в результате оптимизации с помощью MoM, баллунинга памяти и KSM.

Для предотвращения состояния нехватки памяти (Out-of-memory), сделайте область подкачки достаточно большой, чтобы справиться с наихудшим сценарием и при этом иметь возможность её увеличения. Всегда подвергайте конфигурацию стресс-тестированию в широком диапазоне условий, прежде чем развернуть ее в продуктивной среде.

2.20. Менеджер избыточного выделения памяти (Memory Overcommit Manager, MoM)

Менеджер избыточного выделения памяти (Memory Overcommit Manager, MoM) решает две задачи:

- Ограничивает избыточное выделение, применяя настройку **Оптимизация памяти (Memory Optimization)** к хостам в кластере, как описано в предыдущем разделе.
- Оптимизирует память, управляя **баллунингом памяти (memory ballooning)** и **KSM**, как описано в следующих разделах.

Включать или выключать MoM не нужно.

Когда свободная память хоста падает ниже 20%, в журнал **/var/log/vdsm/mom.log** записывается предупреждение:

```
mom.Controllers.Balloon — INFO Ballooning guest:half1 from 1096400 to 1991580
```

/Var/log/vdsm/mom.log - это файл журнала Менеджера избыточного выделения памяти.

2.21. Баллунинг памяти (Memory Ballooning)

Виртуальные машины запускаются с полным объемом виртуальной памяти, который им выделен. Как только использование виртуальной памяти превысит объем ОЗУ, хост начинает больше полагаться на область подкачки. Если **баллунинг памяти (memory ballooning)** включен, он позволяет виртуальным машинам отдавать неиспользуемые части памяти. Освобожденная память может быть повторно использована другими процессами и виртуальными машинами на хосте. Уменьшение объема занимаемой памяти снижает вероятность подкачки и повышает производительность.

Пакет **virtio-balloon**, который устанавливает устройство баллунинга памяти и драйверы, поставляется как загружаемый модуль ядра (loadable kernel module, LKM). По умолчанию он сконфигурирован так, чтобы загружаться автоматически. Помещение модуля в черный список или его выгрузка выключает баллунинг памяти.

Устройства баллунинга памяти не координируются напрямую друг с другом; они полагаются на процесс **Memory Overcommit Manager (MoM)** хоста, постоянно отслеживающий потребности каждой виртуальной машины и указывающий устройству баллунинга памяти увеличить или уменьшить виртуальную память.

Пояснения относительно производительности:

- Не рекомендуется использовать баллунинг памяти и избыточное выделение памяти для процессов, требующих стабильно высокой производительности и низкой задержки. См. Настройка высокопроизводительных виртуальных машин.
- Используйте баллунинг памяти, когда увеличение плотности виртуальных машин (экономичность) важнее производительности.

- Баллунинг памяти не сильно влияет на загрузку ЦП. (KSM потребляет часть ресурсов ЦП, но это потребление остается постоянным под нагрузкой).

Чтобы включить баллунинг памяти, откройте вкладку **Оптимизация (Optimization)** в окне **Новый кластер (New Cluster)** или **Изменить кластер (Edit Cluster)**. Затем установите флажок в поле **Включить оптимизацию динамического выделения памяти (Enable Memory Balloon Optimization)**. Эта настройка включает избыточное выделение памяти на виртуальных машинах, работающих на узлах в этом кластере. Когда этот флажок поставлен, MoM начинает применять баллунинг памяти во всех возможных ситуациях с ограничением гарантированного объема памяти для каждой виртуальной машины. См. раздел Описание настроек оптимизации.

Каждый хост в этом кластере получает обновление политики баллунинга памяти, когда его статус меняется на **Включен (Up)** ▲. При необходимости вы можете вручную обновить политику баллунинга памяти на хосте, не меняя статус. См. раздел Обновление политики Менеджера избыточного выделения памяти на хостах в кластере.

2.22. Объединение одинаковых страниц памяти (Kernel Same-page Merging, KSM)

Когда виртуальная машина работает, она часто создает дублирующиеся страницы памяти для таких элементов, как общие библиотеки и часто используемые данные. Более того, виртуальные машины, на которых работают похожие гостевые ОС и приложения, создают дублирующиеся страницы памяти в виртуальной памяти.

Включенная функция **Объединения одинаковых страниц памяти (Kernel Same-page Merging, KSM)** проверяет виртуальную память на хосте, устраняет дублирующиеся страницы памяти и распределяет оставшиеся страницы памяти между несколькими приложениями и виртуальными машинами. Эти общие страницы памяти помечаются как копируемые при записи, и если виртуальной машине необходимо записать изменения на страницу, она сначала создает копию и только потом записывает свои изменения в копию.

Когда функция KSM включена, ей управляет MoM. Настраивать или управлять функцией KSM вручную не нужно.

KSM повышает производительность виртуальной памяти двумя способами. Поскольку страница общей памяти используется чаще, хост с большей вероятностью будет хранить ее в кэше или основной памяти, что повышает скорость доступа к памяти. Кроме того, при избыточном выделении памяти KSM уменьшает объем используемой виртуальной памяти, снижая вероятность подкачки и повышая производительность.

KSM потребляет больше ресурсов ЦП, чем баллунинг памяти, и это потребление остается постоянным под нагрузкой. Запуск идентичных виртуальных машин и приложений на хосте дает KSM больше возможностей для объединения страниц памяти, чем запуск разнородных.

Если запускаются в основном разнородные виртуальные машины и приложения, то затраты на ЦП, связанные с использованием функции KSM, могут свести на нет ее преимущества.

Пояснения относительно производительности:

- После того, как демон KSM объединит большие объемы памяти, статистика учета памяти ядра может в конечном итоге стать противоречивой. Если в системе много свободной памяти, ее производительность можно повысить, выключив KSM.
- Не рекомендуется использовать KSM и избыточное выделение памяти для процессов, требующих стабильно высокой производительности и низкой задержки. См. Настройка высокопроизводительных виртуальных машин.
- Используйте KSM, когда увеличение плотности виртуальных машин (экономичность) важнее производительности.

Чтобы включить KSM, откройте вкладку **Оптимизация (Optimization)** в окне **Новый кластер (New Cluster)** или **Изменить кластер (Edit Cluster)**. Затем установите флажок в поле **Включить KSM (Enable KSM)**. Этот флажок позволяет **Менеджеру избыточного выделения памяти** запускать KSM, когда это необходимо и может дать экономию памяти, выгода от которой перевешивает затраты на ЦП. См. раздел Описание настроек оптимизации.

2.23. UEFI и чипсет Q35

Чипсет Q35 с UEFI и SecureBoot - это предварительные версии технологий, представленные для оценки (Technology Preview). Такие технологии не поддерживаются соглашениями об уровне обслуживания (SLA) продуктивной среды и могут быть функционально неполными. Не рекомендуется использовать их в продуктивной среде. Тем не менее они дают возможность раннего доступа к будущим функциям продукта, позволяя заказчикам тестировать функциональность и оставлять отзывы в процессе разработки.

Чипсет Intel Q35, используемый по умолчанию для новых виртуальных машин, включает в себя поддержку **Unified Extensible Firmware Interface (UEFI)**, который заменяет устаревший **BIOS**.

Либо можно настроить виртуальную машину или кластер для использования устаревшего чипсета Intel i440fx, который не поддерживает UEFI.

UEFI имеет ряд преимуществ по сравнению с устаревшей BIOS, а именно:

- Современный загрузчик.
- Функцию **SecureBoot**, которая проверяет подлинность цифровых подписей загрузчика.
- Таблицу разделов GUID (GPT), позволяющую использовать диски размером более 2 ТБ.

Можно установить UEFI для любой существующей виртуальной машины или задать его как **Тип чипсета/ПО** по умолчанию для новых виртуальных машин в кластере. Доступны следующие опции:

Таблица 12. Доступные типы BIOS

Тип BIOS	Описание
Чипсет Q35 с BIOS (Q35 Chipset with BIOS)	BIOS
Чипсет Q35 с UEFI (Q35 Chipset with UEFI)	UEFI
Чипсет Q35 с UEFI SecureBoot (Q35 Chipset with UEFI SecureBoot)	UEFI с функцией SecureBoot, которая проверяет подлинность цифровых подписей загрузчика
I440FX Chipset with BIOS	Чипсет i440fx с устаревшей BIOS

Задание типа BIOS до установки ОС

Настроить виртуальную машину для использования чипсета Q35 и UEFI можно перед установкой ОС. Преобразование виртуальной машины из устаревшей BIOS в UEFI после установки ОС не поддерживается.

2.24. Настройка кластера для использования чипсета Q35 и UEFI

Можно настроить тип чипсета/ПО по умолчанию для кластера, который определяет тип чипсета/ПО по умолчанию для любых новых виртуальных машин, создаваемых в кластере. При необходимости можно переопределить тип чипсета/ПО по умолчанию для кластера, указав другой тип при создании виртуальной машины.

Чипсет Q35 с UEFI и SecureBoot - это предварительные версии технологий, представленные для оценки (Technology Preview). Такие технологии не поддерживаются соглашениями об уровне обслуживания (SLA) продуктивной среды и могут быть функционально неполными. Не рекомендуется использовать их в продуктивной среде. Тем не менее они дают возможность раннего доступа к будущим функциям продукта, позволяя заказчикам тестировать функциональность и оставлять отзывы в процессе разработки

Порядок действий:

1. На **Пользовательском портале** или **Портале администрирования** нажмите **Ресурсы (Compute) > Кластеры (Clusters)**.
2. Выберите кластер и нажмите **[Изменить (Edit)]**.
3. Нажмите **Общие (General)**.

4. Определите тип чипсета/ПО по умолчанию для новых виртуальных машин в кластере, нажав на выпадающее меню **Тип чипсета/ПО (Chipset/Firmware Type)** и выбрав один из следующих вариантов:
    - **I440FX Chipset with BIOS**
    - **Чипсет Q35 с BIOS (Q35 Chipset with BIOS)**
    - **Чипсет Q35 с UEFI (Q35 Chipset with UEFI)**
    - **Чипсет Q35 с UEFI SecureBoot (Q35 Chipset with UEFI SecureBoot)**
5. Если какие-либо из существующих виртуальных машин в кластере должны использовать новый тип чипсета/ПО, настройте их соответствующим образом. Дополнительную информацию см. в разделе Настройка виртуальной машины для использования чипсета Q35 с UEFI.

Поскольку изменить тип чипсета/ПО можно только перед установкой ОС, для всех существующих виртуальных машин, настроенных на использование BIOS типа Заданный для кластера по умолчанию (Cluster default), измените тип чипсета/ПО в значение, соответствующее предыдущему типу, заданному для кластера по умолчанию. В противном случае виртуальная машина может не загрузиться. Либо, как вариант, можно переустановить ОС виртуальной машины.

2.25. Настройка виртуальной машины для использования чипсета Q35 с UEFI

Чипсет Q35 с UEFI и SecureBoot - это предварительные версии технологий, представленные для оценки (Technology Preview). Такие технологии не поддерживаются соглашениями об уровне обслуживания (SLA) продуктивной среды и могут быть функционально неполными. Не рекомендуется использовать их в продуктивной среде. Тем не менее они дают возможность раннего доступа к будущим функциям продукта, позволяя заказчикам тестировать функциональность и оставлять отзывы в процессе разработки

Настроить виртуальную машину для использования чипсета Q35 и UEFI можно перед установкой ОС. Преобразование виртуальной машины из устаревшей BIOS в UEFI или из UEFI в устаревший BIOS может помешать загрузке виртуальной машины. Если вы меняете тип BIOS существующей виртуальной машины, переустановите ОС.

Если тип чипсета/ПО виртуальной машины установлен в значение Заданный для кластера по умолчанию (Cluster default), изменение тип чипсета/ПО кластера приводит к изменению тип чипсета/ПО виртуальной машины. Если на виртуальной машине установлена ОС, изменение тип чипсета/ПО кластера может привести к сбою загрузки виртуальной машины.

Порядок действий:

1. На **Пользовательском портале** или **Портале администрирования** нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)**.

2. Выберите виртуальную машину и нажмите **[Изменить (Edit)]**.
3. На вкладке **Общие (General)** нажмите **Показать расширенные настройки (Show Advanced Options)**.
4. Нажмите **Система (System)**.
5. В выпадающем меню **Тип BIOS (Chipset/Firmware Type)** выберите одно из следующих значений:
    - **I440FX Chipset with BIOS**
    - **Чипсет Q35 с BIOS (Q35 Chipset with BIOS)**
    - **Чипсет Q35 с UEFI (Q35 Chipset with UEFI)**
    - **Чипсет Q35 с UEFI SecureBoot (Q35 Chipset with UEFI SecureBoot)**
6. Нажмите **[OK]**.
7. На **Пользовательском портале** или **Портале администрирования** выключите виртуальную машину. При следующем запуске виртуальной машины она будет работать с выбранным новым типом чипсета/ПО.

Управление центрами данных

1. Введение в центры данных

Центр данных - это логическая сущность, определяющая набор ресурсов, используемых в конкретной среде. Центр данных рассматривается как контейнер ресурсов в том смысле, что он состоит из **логических ресурсов** (в форме кластеров и хостов), **сетевых ресурсов** (в форме логических сетей и физических сетевых карт) и **ресурсов хранилища** (в форме доменов хранения).

Центр данных может содержать несколько кластеров, которые, в свою очередь, могут содержать несколько хостов; с ним может быть ассоциировано несколько доменов хранения; он может поддерживать несколько виртуальных машин на каждом из своих хостов. Среда zVirt может содержать несколько центров данных; инфраструктура центров данных позволяет поддерживать их раздельную работу.

Управление всеми центрами данных осуществляется через единый **Портал администрирования**.

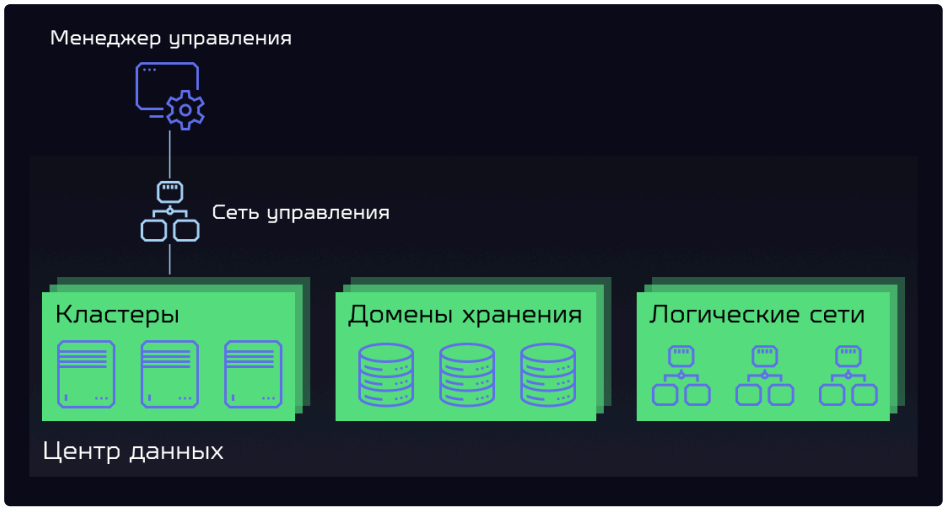


Рисунок 1. Центр данных

Во время установки zVirt создается центр данных по умолчанию **Default**. Можно сконфигурировать этот центр данных по умолчанию либо настроить новые центры данных с соответствующими именами.

2. Менеджер пула хранения (SPM)

Менеджер пула хранения (Storage Pool Manager, SPM) - роль, назначаемая одному из хостов центра данных для управления доменами хранения центра данных. **SPM** может

выполняться на любом хосте центра данных, которому менеджер управления назначит эту роль. **SPM** не мешает стандартной работе хоста: на хосте, работающем как **SPM**, по-прежнему могут размещаться виртуальные ресурсы.

SPM управляет доступом к хранилищу, согласовывая метаданные между доменами хранения. Сюда входит создание, удаление и управление виртуальными дисками (образами), моментальными снимками и шаблонами, а также выделение ресурсов хранилища для динамически расширяемых блочных устройств (в сетях SAN). Это эксклюзивная задача: чтобы обеспечить целостность метаданных, только один хост может в отдельный момент времени выполнять роль **SPM** в центре данных.

Менеджер управления обеспечивает, чтобы **SPM** всегда был доступен. Если у хоста **SPM** возникают проблемы с доступом к хранилищу, то Менеджер управления передает роль **SPM** другому хосту. Когда **SPM** запускается, он убеждается, что является единственным хостом, которому назначена эта роль.

3. Приоритет SPM

Роль SPM использует часть доступных ресурсов хоста. Установка приоритета SPM для хоста изменяет вероятность того, что хосту будет назначена роль SPM: сначала роль SPM будет назначена хосту с высоким приоритетом SPM и лишь затем - хосту с низким приоритетом SPM. Критически важным виртуальным машинам на хостах с низким приоритетом SPM не придется бороться с операциями SPM за ресурсы хоста.

Для изменения приоритета SPM выполните следующие действия:

Порядок действий:

1. На Портале администрирования выберите **Ресурсы (Compute) > Хосты (Hosts)**.
2. Выберите нужный хост и нажмите **[Изменить (Edit)]**.
3. Перейдите на вкладку **SPM**.
4. Выберите нужный приоритет.
5. Нажмите **[OK]**

4. Задачи, относящиеся к центрам данных

4.1. Создание нового центра данных

С помощью этой процедуры в среде виртуализации создается новый центр данных. Для работы центру данных требуется функционирующий кластер, хост и домен хранения.

После установки **Версии совместимости (Compatibility Version)** вы не сможете уменьшить номер версии. Возврат к более старым версиям не поддерживается.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)**.
2. Нажмите **[Новый (New)]**.
3. Введите **Имя (Name)** и **Описание (Description)** центра данных.
4. В выпадающих меню выберите **Тип хранилища (Storage Type)**, **Версия совместимости (Compatibility Version)** и **Режим квотирования (Quota Mode)** для центра данных.
5. Нажмите **[OK]**, чтобы создать центр данных
6. При необходимости воспользуйтесь **Помощником по созданию Центра данных (Data Center - Guide Me)**.

   Окно **Помощник по созданию Центра данных(Data Center - Guide Me)** содержит список сущностей, которые нужно сконфигурировать для центра данных. Сконфигурируйте эти сущности или отложите конфигурирование, нажав **Настроить позже (Configure Later)**. Чтобы возобновить конфигурирование, выберите центр данных и нажмите **Дополнительные действия (More Actions)** (⋮), а затем нажмите **[Помощник (Guide Me)]**.

Новый центр данных останется в состоянии **Неинициализированный (Uninitialized)**, пока для него не будут сконфигурированы кластер, хост и домен хранения. Чтобы сконфигурировать их, используйте **[Помощник (Guide Me)]**.

4.2. Описание настроек в окнах "Новый центр данных (New Data Center)" и "Изменить центр данных (Edit Data Center)"

В приведенной ниже таблице описаны настройки центра данных, отображаемые в окнах **Новый центр данных (New Data Center)** и **Изменить центр данных (Edit Data Center)**. При нажатии кнопки **[OK]** система подсвечивает некорректно введенные значения оранжевым цветом, не давая принять изменения. Кроме того, поля снабжены подсказками, которые указывают ожидаемые значения или диапазон значений.

Таблица 1. Свойства центра данных

Поле	Описание (действие)
Имя (Name)	Имя центра данных. В этом текстовом поле должно быть не больше 40 знаков. Имя должно быть уникальным и представлять собой любую комбинацию **латинских букв** в верхнем и нижнем регистре, цифр, дефисов и знаков подчеркивания.

Поле	Описание (действие)
Описание (Description)	Описание центра данных. Это поле является рекомендованным, но не обязательным.
Тип хранилища (Storage Type)	Выберите тип хранилища: **Общий (Shared)** или **Локальный (Local)**. К одному центру данных можно добавлять домены хранения разных типов (iSCSI, NFS, FC, POSIX и Gluster), однако локальные и общие домены нельзя смешивать. После инициализации центра данных тип хранилища можно изменить, подробнее смотри в Изменение типа хранилища центра данных.
Версия совместимости (Compatibility Version)	Версия zVirt. После обновления версии менеджера управления можно оставить прежние версии хостов, кластеров и центров данных. Перед тем как обновлять уровень совместимости (Compatibility Level) центра данных, убедитесь, что обновлены все хосты и затем кластеры.
Режим квотирования (Quota Mode)	**Квота** - это инструмент ограничения ресурсов, предоставляемый Менеджером управления. Выберите один из следующих вариантов: • **Выключено (Disabled)**: Выберите, чтобы отключить квоту • **Аудит (Audit)**: Выберите, чтобы изменить настройки квоты • **Принудительно (Enforced)**: Выберите, чтобы включить квоту
Комментарий (Comment)	Необязательный комментарий о центре данных в виде неформатированного текста.

4.3. Повторная инициализация центра данных: Процедура восстановления

Эта процедура восстановления заменяет основной домен данных (мастер) центра данных новым основным доменом данных. Необходимо повторно инициализировать основной домен данных (мастер), если данные в нем повреждены. Повторная инициализация центра данных позволяет восстановить все остальные ресурсы, ассоциированные с центром данных, в том числе кластеры, хосты и исправные домены хранения.

Можно импортировать любые резервные или экспортированные виртуальные машины или шаблоны в новый основной домен данных (мастер).

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)** и выберите центр данных.
2. Убедитесь, что все домены хранения, подключенные к центру данных, находятся в режиме обслуживания.
3. Нажмите **Дополнительные действия (More Actions)** ⋮, затем нажмите **[Переинициализировать центр данных (Re-Initialize Data Center)]**.

4. В окне **Переинициализировать центр данных (Data Center Re-Initialize)** перечислены все доступные (отключенные, находящиеся в режиме обслуживания) домены хранения. С помощью кнопки-переключателя выберите домен хранения, который нужно добавить к центру данных.
5. Установите флажок в поле **Подтвердить операцию (Approve operation)**.
6. Нажмите **[OK]**.

Домен хранения подключен к центру данных как основной домен данных (мастер) и активирован. Теперь можно импортировать любые резервные или экспортированные виртуальные машины или шаблоны в новый основной домен данных (мастер).

4.4. Удаление центра данных

Для удаления центра данных требуется активный хост. Удаление центра данных не влечет за собой удаления ассоциированных ресурсов.

Порядок действий:

1. Убедитесь, что домены хранения, подключенные к центру данных, находятся в режиме обслуживания.
2. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)** и выберите центр данных, который нужно удалить.
3. Нажмите **[Удалить (Remove)]**.
4. Нажмите **[OK]**.

4.5. Принудительное удаление центра данных

Центр данных перейдет в состояние **Не отвечает (Non Responsive)**, если будет поврежден подключенный домен хранения или если хост перейдет в состояние **Не отвечает (Non Responsive)**. В обоих случаях удалить центр данных действием **[Удалить (Remove)]** будет невозможно.

Для выполнения действия **Удалить принудительно (Force Remove)** активный хост не требуется. При этом навсегда удаляется и подключенный домен хранения.

Перед **принудительным удалением (Force Remove)** центра данных может потребоваться **уничтожить (Destroy)** поврежденный домен хранения (см. Уничтожение домена хранения)

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)** и выберите центр данных, который нужно удалить.
2. Нажмите **Дополнительные действия (More Actions)** ⋮, затем - **[Удалить принудительно (Force Remove)]**.

3. Установите флажок в поле **Подтвердить операцию (Approve operation)**.
4. Нажмите **[OK]**.

Центр данных и подключенный домен хранения навсегда удалены из среды zVirt.

4.6. Изменение типа хранилища центра данных

После инициализации центра данных тип его хранилища можно изменить. Это рекомендуется делать для доменов данных, которые используются для перемещения виртуальных машин или шаблонов.

Ограничения:

- Тип хранилища можно изменить из **общего** в **локальный** (**Shared** to **Local**) только для центра данных, который содержит один кластер с одним хостом.
- Нельзя изменить тип хранилища из **локального** в **общий** (**Local** to **Shared**) для центра данных, который не содержит локального домена хранения.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)** и выберите центр данных, который нужно изменить.
2. Нажмите **[Изменить (Edit)]**.
3. Измените значение **Тип хранилища (Storage Type)** на необходимое.
4. Нажмите **[OK]**.

4.7. Изменение версии совместимости центра данных

У центров данных zVirt есть версия совместимости (например, для zVirt 4.0 - будет версия 4.7). Все кластеры в таком центре данных должны поддерживать требуемый уровень совместимости.

Предварительные условия:

- Чтобы изменить уровень совместимости центра данных, сначала нужно обновить версию совместимости всех кластеров и виртуальных машин в центре данных.

Порядок действий:

1. На портале администрирования нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)**.
2. Выберите центр данных, который нужно изменить, и нажмите **[Изменить (Edit)]**.
3. Измените значение **Версия совместимости (Compatibility Version)** на необходимое.
4. Нажмите **[OK]**. Откроется диалог подтверждения **Изменить версию совместимости центра данных (Change Data Center Compatibility Version)**.

5. Нажмите **[OK]** для подтверждения.

5. Центры данных и домены хранения

5.1. Подключение существующего домена данных к центру данных

Откреплённые (Unattached) домены данных можно подключить к центру данных. К одному центру данных можно добавлять общие домены хранения разных типов (iSCSI, NFS, FC, POSIX и Gluster).

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.
3. Откройте вкладку **Хранилище (Storage)**, чтобы увидеть список доменов хранения, уже подключенные к центру данных.
4. Нажмите **[Прикрепить домен данных (Attach Data)]**.
5. Установите флажок для домена данных, который нужно подключить к центру данных. Можно установить несколько флажков, чтобы подключить несколько доменов данных.
6. Нажмите **[OK]**.

Домен данных подключен к центру данных и автоматически активирован.

5.2. Подключение существующего домена экспорта к центру данных

Сущность "экспорт-домен" считается устаревшей. Экспорт-домен можно отключить от центра данных и импортировать в другой центр данных в той же или другой среде. Затем виртуальные машины, "плавающие" виртуальные диски и шаблоны можно выгрузить из импортированного домена хранения в подключенный центр данных. Информацию об импорте доменов хранения см. в разделе Импортирование существующих доменов хранения.

Откреплённый (Unattached) домен экспорта можно подключить к центру данных. К центру данных можно подключить только один домен экспорта.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.

3. Откройте вкладку **Хранилище (Storage)**, чтобы увидеть список доменов хранения, уже подключенных к центру данных.
4. Нажмите **[Прикрепить экспорт-домен (Attach Export)]**.
5. Выберите соответствующий домен экспорта кнопкой-переключателем.
6. Нажмите **[OK]**.

Домен экспорта подключается к центру данных и автоматически активируется.

5.3. Отключение домена хранения от центра данных

Отключение домена хранения от центра данных разрывает ассоциацию центра данных с этим доменом хранения. Этот домен хранения не удаляется из среды zVirt и может быть подключен к другому центру данных.

Данные (такие как виртуальные машины и шаблоны) остаются подключенными к домену хранения.

Основной домен данных (мастер) (если он является последним доступным доменом хранения) нельзя удалить.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.
3. Откройте вкладку **Хранилище (Storage)**, чтобы увидеть список доменов хранения, подключенных к центру данных.
4. Выберите домен хранения, который нужно отключить. Если домен хранения **Активен (Active)**, нажмите **[Обслуживание (Maintenance)]**.
5. Нажмите **[OK]**, чтобы перейти в режим обслуживания.
6. Нажмите **[Отсоединить (Detach)]**.
7. Нажмите **[OK]**.

Прежде чем этот домен хранения исчезнет из подробного представления, может пройти несколько минут.

Управление внешними провайдерами

1. Общая информация о внешних провайдерах в zVirt

Помимо ресурсов, управляемых Менеджером управления, в zVirt могут использоваться ресурсы, которые управляются из внешних источников. Провайдеры этих ресурсов, известные как внешние провайдеры, могут предоставлять хосты виртуализации, образы виртуальных машин и сети.

Сейчас в zVirt поддерживаются следующие внешние провайдеры:

KubeVirt/Openshift Virtualization

Openshift Virtualization (ранее контейнерная виртуализация или "CNV") позволяет внедрять виртуальные машины (ВМ) в контейнерные рабочие процессы, чтобы можно было разрабатывать, управлять и разворачивать виртуальные машины рядом с контейнерами и бессерверными средами. Для получения дополнительной информации см. раздел Добавление KubeVirt/Openshift Virtualization в качестве внешнего провайдера.

Служба OpenStack Image Service (Glance) для управления образами

Служба **OpenStack Image Service** предоставляет каталог образов виртуальных машин. В zVirt эти образы можно импортировать в Менеджер управления и использовать в качестве плавающих дисков или подключить к виртуальным машинам и преобразовать в шаблоны. После добавления службы **OpenStack Image Service** в Менеджер управления она отображается как домен хранения, не подключенный ни к одному из центров данных. Виртуальные диски в среде zVirt также можно экспортировать в службу **OpenStack Image Service** как виртуальные диски.

VMware для выделения виртуальных машин

Виртуальные машины, созданные в VMware, можно преобразовать, используя **V2V** (**virt-v2v**), и импортировать в среду zVirt. После добавления провайдера VMware в Менеджер управления можно импортировать виртуальные машины, которые он предоставляет. Преобразование V2V выполняется на указанном прокси-хосте в рамках импортирования.

KVM для выделения виртуальных машин

Виртуальные машины, созданные в KVM, можно импортировать в среду zVirt. После добавления хоста KVM в Менеджер управления можно импортировать виртуальные машины, которые он предоставляет.

Open Virtual Network (OVN) для выделения сетей

Open Virtual Network (OVN) - расширение Open vSwitch (OVS), предоставляющее программно-определяемые сети. После добавления OVN в Менеджер управления можно импортировать существующие сети OVN и создать новые сети OVN из Менеджера управления. Можно также автоматически установить OVN на Менеджер управления, используя `engine-setup`.

2. Добавление внешних провайдеров

2.1. Добавление экземпляра OpenStack Image (Glance) для управления образами

Добавьте экземпляр **OpenStack Image (Glance)** в Менеджер управления для управления образами.

Порядок действий:

1. Нажмите **Управление (Administration)** > **Провайдеры (Providers)**.
2. Нажмите **[Добавить (Add)]** и введите подробности на вкладке **Общие (General Settings)**. Дополнительные сведения об этих полях см. в разделе Описание общих настроек при добавлении провайдера.
3. Введите **Имя (Name)** и **Описание (Description)**.
4. Из выпадающего списка **Тип (Type)** выберите `OpenStack Image`.
5. В текстовом поле **URL провайдера (Provider URL)** введите URL или FQDN машины, на которой установлен экземпляр OpenStack Image.
6. При желании установите флажок **Требуется авторизация (Requires Authentication)** и введите **Имя пользователя (Username)** и **Пароль (Password)** для пользователя экземпляра OpenStack Image, зарегистрированного в Keystone. Нужно также задать URL-адрес аутентификации сервера Keystone, задав **Протокол (Protocol)** (должен быть HTTP), **Имя хоста (Hostname)** и **Порт API (API Port)**.

   Укажите **Доменное имя пользователя (User Domain Name)**, **Название проекта (Project Name)** и **Доменное имя проекта (Project Domain Name)** для экземпляра OpenStack Image.
7. Проверка учетных данных:
   a. Нажмите **[Тестировать (Test)]**, чтобы проверить, удается ли выполнить успешную аутентификацию на экземпляре OpenStack Image с использованием предоставленных учетных данных.

b. Если в экземпляре OpenStack Image используется SSL, то откроется окно Импортировать сертификаты провайдера. Нажмите **[OK]**, чтобы импортировать сертификат, предоставленный экземпляром OpenStack Image, чтобы гарантировать, что Менеджер управления сможет взаимодействовать с экземпляром.

8. Нажмите **[OK]**.

2.2. Добавление KubeVirt/Openshift Virtualization в качестве внешнего провайдера

Для запуска виртуальных машин в контейнере на платформе **OpenShift Container Platform**, добавьте OpenShift в качестве внешнего провайдера в zVirt.

Эта функция называется OpenShift Virtualization.

Предварительные условия:

- На платформе OpenShift Container Platform ваш кластер конфигурируется для OpenShift Virtualization.

Порядок действий:

1. На Портале администрирования выберите **Управление (Administration) > Провайдеры (Providers)** и нажмите **[Добавить (Add)]**.
2. В окне **Добавить провайдер (Add Provider)** выберите значение `Виртуализация KubeVirt/Openshift` (`KubeVirt/Openshift Virtualization`) для параметра **Тип (Type)**.
3. Введите требуемые **URL провайдера (Provider URL)** и **Токен (Token)**.
4. Дополнительно: Задайте значения таких **Дополнительных параметров (Advanced parameters)**, как **Центр сертификации (Certificate Authority)**, **URL-адрес Prometheus** и **Центр сертификации Prometheus (Prometheus Certificate Authority)**.
5. Нажмите **[Тестировать (Test)]** для проверки подключения к новому провайдеру.
6. Нажмите **[OK]** для завершения добавления этого нового провайдера.

Действия по проверке:

1. На Портале администрирования нажмите **Ресурсы (Compute) > Кластеры (Clusters)**.
2. Нажмите на имя нового только что созданного кластера. Это имя кластера, например, **kubevirt** имеет в основе имя провайдера. Откроется подробное представление кластера.
3. Откройте вкладку **Хосты (Hosts)**, чтобы убедиться, что рабочие узлы OpenShift Container Platform имеют статус **Включен (up)** ▲. NOTE: Статус узлов панели управления будет **Выключен (down)**, даже если они работают, так как они не могут разместить виртуальные машины.

4. Выберите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)**, чтобы развернуть виртуальную машину в новом кластере.
5. На веб-консоли OpenShift Container Platform, в представлении Администратор (Administrator) выберите **Процессы (Workloads)** → **Виртуальные машины (Virtual Machines)** для просмотра развернутой виртуальной машины.

   Дополнительные ресурсы

   - Описание общих настроек при добавлении провайдера/

2.3. Добавление экземпляра VMware в качестве провайдера виртуальных машин

Добавьте экземпляр VMware vCenter, чтобы импортировать виртуальные машины из VMware в Менеджер управления.

zVirt использует **V2V**, чтобы перед импортированием преобразовать виртуальные машины VMware в корректный формат. Пакет **virt-v2v** должен быть установлен хотя бы на одном хосте. Пакет **virt-v2v** доступен по умолчанию на хостах с zVirt Node и устанавливается на хостах как VDSM-зависимость при добавлении в среду zVirt.

Порядок действий:

1. Нажмите **Управление (Administration)** > **Провайдеры (Providers)**.
2. Нажмите **[Добавить (Add)]**.
3. Введите **Имя (Name)** и **Описание (Description)**.
4. Выберите `VMware` в выпадающем списке **Тип (Type)**.
5. Выберите **Центр данных (Data Center)**, в который будут импортироваться виртуальные машины VMware, либо `Любой центр данных (Any Data Center)`, чтобы указывать центр данных, являющийся приемником, во время каждой отдельной операции импорта.
6. Введите IP-адрес или FQDN экземпляра VMware vCenter в поле **vCenter**.
7. Введите IP-адрес или FQDN хоста, из которого будут импортироваться виртуальные машины, в поле **ESXi**.
8. Введите имя центра данных, в котором находится указанный хост ESXi, в поле **Центр данных (Data Center)**.
9. Если вы обменивались SSL-сертификатом между хостом ESXi и Менеджером управления, то оставьте флажок **Проверка SSL-сертификата сервера (Verify server's SSL certificate)** установленным, чтобы проверять сертификат хоста ESXi. В противном случае снимите этот флажок.
10. Выберите хост в выбранном центре данных с установленным пакетом **virt-v2v**, который будет служить **Прокси-хостом (Proxy Host)** во время операций импорта виртуальных машин. Этот хост также должен быть способен подключаться к сети внешнего

провайдера VMware vCenter. Если выше вы выбрали **Любой центр данных (Any Data Center)**, то вы не можете выбирать здесь хост, но зато можете указывать хост для конкретной операции импорта.

11. Введите **Имя пользователя (Username)** и **Пароль (Password)** для экземпляра VMware vCenter. Пользователь должен иметь доступ к центру данных VMware и хосту ESXi, на котором находятся виртуальные машины.
12. Проверьте учетные данные:
    a. Нажмите **[Тестировать (Test)]**, чтобы проверить, удается ли выполнить успешную аутентификацию на экземпляре VMware vCenter с использованием предоставленных учетных данных.
    b. Если экземпляр VMware vCenter использует SSL, откроется окно **Импортировать сертификаты провайдера (Import provider certificates)**. Нажмите **[OK]**, чтобы импортировать сертификат, предоставленный экземпляром VMware vCenter, чтобы гарантировать, что Менеджер управления сможет взаимодействовать с экземпляром.
13. Нажмите **[OK]**.

Чтобы импортировать виртуальные машины из внешнего провайдера VMware, см. раздел Импортирование виртуальной машины из провайдера VMware в руководстве пользователя.

2.4. Добавление хоста KVM в качестве провайдера виртуальных машин

Добавьте хост KVM, чтобы импортировать виртуальные машины из KVM в Менеджер управления.

Порядок действий:

1. Включите аутентификацию с открытым ключом между прокси-хостом и хостом KVM:
    a. Авторизуйтесь на прокси-хосте и сгенерируйте SSH-ключи для пользователя **vdsm**.

```
sudo -u vdsm ssh-keygen
```

    b. Скопируйте открытый ключ пользователя **vdsm** на хост KVM. Файл **known_hosts** на прокси-хосте также обновится и включит в себя хост-ключ хоста KVM.

```
sudo -u vdsm ssh-copy-id root@_kvmhost.example.com_
```

    c. Авторизуйтесь на хосте KVM, чтобы убедиться, что все работает правильно.

```
sudo -u vdsm ssh root@_kvmhost.example.com_
```

2. Нажмите **Управление (Administration)** > **Провайдеры (Providers)**.
3. Нажмите **[Добавить (Add)]**.
4. Введите **Имя (Name)** и **Описание (Description)**.
5. Выберите `KVM` в выпадающем списке **Тип (Type)**.
6. Выберите **Центр данных (Data Center)**, в который будут импортироваться виртуальные машины KVM, либо `Любой центр данных (Any Data Center)`, чтобы указывать центр данных, являющийся приемником, во время каждой отдельной операции импорта.
7. В поле **URI** укажите URI хоста KVM. Например:

```
qemu+ssh://root@host.example.com/system
```

8. Выберите хост в выбранном центре данных, который будет служить **Прокси-хостом (Proxy Host)** во время операций импорта виртуальных машин. Этот хост также должен быть способен подключаться к сети внешнего провайдера KVM. Если выше вы выбрали `Любой центр данных (Any Data Center)` в поле **Центр данных (Data Center)**, то вы не сможете выбрать хост здесь. Это поле неактивно, и в нем отображается `Любой хост в центре данных (Any Host in Data Center)`. Вместо этого вы можете указать хост во время отдельных операций импорта.
9. При желании установите флажок **Требуется авторизация (Requires Authentication)** и введите **Имя пользователя (Username)** и **Пароль (Password)** для хоста KVM. Пользователь должен иметь доступ к хосту KVM, на котором находятся виртуальные машины.
10. Нажмите **[Тестировать (Test)]**, чтобы проверить, удается ли выполнить успешную аутентификацию на хосте KVM с использованием предоставленных учетных данных.
11. Нажмите **[OK]**.

Чтобы импортировать виртуальные машины из внешнего провайдера KVM, см. раздел Импортирование виртуальной машины из хоста KVM в руководстве по управлению виртуальными машинами.

2.5. Добавление Open Virtual Network (OVN) в качестве внешнего провайдера сети

Вы можете использовать **Open Virtual Network (OVN)** для создания оверлейных виртуальных сетей, которые обеспечивают связь между виртуальными машинами без добавления VLAN или изменения инфраструктуры. OVN - это расширение Open vSwitch (OVS), которое обеспечивает встроенную поддержку виртуальных оверлейных сетей L2 и L3.

Вы можете установить новый провайдер сети OVN или добавить существующий.

Вы также можете подключить сеть OVN к собственной сети zVirt. Дополнительную информацию см. в разделе Подключение сети OVN к физической сети.

Данная возможность доступна только как предварительная версия технологии, представленная для оценки (Technology Preview).

ovirt-provider-ovn предоставляет REST API для работы в сети OpenStack. Его можно использовать для создания сетей, подсетей, портов и маршрутизаторов. Подробности см. в документе OpenStack Networking API v2.0.

2.6. Установка нового провайдера сети OVN

При установке OVN с использованием `engine-setup` выполняются следующие шаги:

- Установка центрального сервера OVN на машину с Менеджером управления.
- Добавление OVN к zVirt в качестве внешнего провайдера сети.
- Установка **Провайдер сети по умолчанию (Default Network Provider)** в значение ovirt-provider-ovn (только в кластере по умолчанию).

- Установка OVN меняет настройку Провайдер сети по умолчанию (Default Network Provider) только в кластере по умолчанию, но не в других кластерах.
- Изменение настройки Провайдер сети по умолчанию (Default Network Provider) не обновляет хосты в этом кластере так, чтобы они использовали Провайдера сети по умолчанию (Default Network Provider).
- Чтобы хосты и виртуальные машины смогли использовать OVN, выполните дополнительные действия, описанные в подразделе "Дальнейшие шаги" в конце этого раздела.

Порядок действий:

1. Дополнительно: Если вы используете заранее сконфигурированный файл ответов для `engine-setup`, добавьте следующую запись, чтобы установить OVN:

```
OVESETUP_OVN/ovirtProviderOvn=bool:True
```

2. Запустите `engine-setup` на машине с Менеджером управления.
3. Если вы не используете заранее сконфигурированный файл ответов, ответьте `Yes`, когда `engine-setup` спросит:

```
Configuring ovirt-provider-ovn also sets the Default cluster's default
network provider to ovirt-provider-ovn.
Non-Default clusters may be configured with an OVN after installation.
Configure ovirt-provider-ovn (Yes, No) [Yes]
```

4. Ответьте на следующий вопрос:

```
Use default credentials (admin@internal) for ovirt-provider-ovn (Yes, No)
[Yes]?:
```

Если `Yes`, то `engine-setup` использует имя и пароль пользователя engine, указанные ранее в процессе настройки в качестве значений по умолчанию. Эта опция доступна только во время новой установки.

```
oVirt OVN provider user[admin]:
oVirt OVN provider password[empty]:
```

Можно использовать значения по умолчанию или указать имя пользователя и пароль провайдера oVirt OVN.

Чтобы изменить метод аутентификации позже, можно внести правки в файл **/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf** или создать новый файл **/etc/ovirt-provider-ovn/conf.d/20_engine_setup.conf**. Перезапустите службу `ovirt-provider-ovn`, чтобы изменение вступило в силу. Подробности об аутентификации OVN см. по ссылке.

Дальнейшие действия:

Прежде чем вы сможете создавать виртуальные машины, использующие только что установленную сеть OVN, выполните следующие дополнительные действия:

1. Добавьте сеть в кластер Default.
    a. Для этого установите флажок **Создать на внешнем провайдере (Create on external provider)**. Будет создана сеть на базе ovirt-provider-ovn.
    b. Дополнительно: Чтобы подключить сеть OVN к физической сети, установите флажок **Подключение к физической сети (Connect to physical network)** и укажите сеть zVirt, которую нужно использовать.
    c. Дополнительно: Если сеть должна использовать группы безопасности, убедитесь, что в выпадающем списке **Безопасность сетевого порта (Network Port Security)** установлено значение **Включен (Enabled)**. Дополнительную информацию о доступных опциях см. в разделе Описание общих настроек логической сети.
2. Добавьте хосты к кластеру **Default** или переустановите хосты на нем, чтобы они использовали нового **Провайдера сети по умолчанию (Default Network Provider)** кластера - `ovirt-provider-ovn`.
3. Дополнительно: Измените кластеры, не являющиеся кластерами по умолчанию, и установите параметр **Провайдер сети по умолчанию (Default Network Provider)** в значение `ovirt-provider-ovn`.
    a. Дополнительно: Переустановите хосты на каждом кластере, не являющемся кластером по умолчанию, чтобы они использовали нового Провайдера сети по умолчанию (Default Network Provider) кластера - `ovirt-provider-ovn`.

Дополнительные ресурсы

- Сведения о том, как настроить хосты на использование существующей сети, не являющейся сетью по умолчанию, см. в разделе Настройка хостов для сети туннелей OVN.

2.7. Добавление существующего провайдера сети OVN

Добавление существующего центрального сервера OVN в качестве внешнего провайдера сети в zVirt включает в себя следующие ключевые шаги:

- Установите провайдер OVN, прокси, используемый Менеджером управления для взаимодействия с OVN. Провайдер OVN можно установить на любой машине, но он должен иметь возможность связываться с центральным сервером OVN и Менеджером управления.
- Добавьте провайдера OVN в zVirt в качестве внешнего провайдера сети.
- Создайте новый кластер, использующий OVN в качестве провайдера сети по умолчанию. Хосты, добавленные в этот кластер, автоматически настраиваются на связь с OVN.

Порядок действий:

1. Установите и настройте провайдер OVN.
   a. Установите провайдер на машине провайдера:

   ```
   dnf install ovirt-provider-ovn
   ```

   b. Если вы не устанавливаете провайдер на одну машину с Менеджером управления, то добавьте следующую запись в файл **/etc/ovirt-provider-ovn/conf.d/10_engine_set-up.conf** (создайте этот файл, если он еще не существует):

   ```
   [OVIRT]
   ovirt-host=https://<Manager_host_name>
   ```

   Это нужно для аутентификации, если она включена.

   c. Если вы не устанавливаете провайдер на одну машину с центральным сервером OVN, то добавьте следующую запись в файл **/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf** (создайте этот файл, если он еще не существует):

   ```
   [OVN REMOTE]
   ovn-remote=tcp:<OVN_central_server_IP>:6641
   ```

   d. Откройте порты `9696`, `6641` и `6642` в межсетевом экране, чтобы разрешить взаимодействие между провайдером OVN, центральным сервером OVN и

Менеджером управления. Это можно сделать либо вручную, либо добавив службы ovirt-provider-ovn и ovirt-provider-ovn-central в соответствующую зону:

```
firewall-cmd --zone=<ZoneName> --add-service=ovirt-provider-ovn --
permanent
firewall-cmd --zone=<ZoneName> --add-service=ovirt-provider-ovn-central
--permanent
firewall-cmd --reload
```

e. Запустите и включите службу:

```
systemctl start ovirt-provider-ovn
systemctl enable ovirt-provider-ovn
```

f. Настройте центральный сервер OVN на прослушивание запросов с портов `6642` и `6641`:

```
ovn-sbctl set-connection ptcp:6642
ovn-nbctl set-connection ptcp:6641
```

2. На Портале администрирования нажмите **Управление (Administration)** > **Провайдеры (Providers)**.
3. Нажмите **[Добавить (Add)]** и введите подробные сведения на вкладке **Общее (General Settings)**. Дополнительную информацию об этих полях см. в разделе Описание общих настроек при добавлении провайдера.
4. Введите **Имя (Name)** и **Описание (Description)**.
5. В списке **Тип (Type)** выберите **Внешний провайдер сети (External Network Provider)**.
6. Нажмите на текстовое поле **Сетевой модуль (Networking Plugin)** и выберите **Провайдер сети oVirt для OVN (oVirt Network Provider for OVN)** в выпадающем меню.
7. При желании установите флажок **Автоматическая синхронизация (Automatic Synchronization)**. Это включает автоматическую синхронизацию внешнего провайдера сети с существующими сетями.

Автоматическая синхронизация включена по умолчанию на провайдере сети ovirt-provider-ovn, созданном инструментом engine-setup.

8. Введите URL-адрес или FQDN провайдера OVN в текстовое поле **URL провайдера (Provider URL)** и далее номер порта. Если провайдер OVN и центральный сервер OVN находятся на разных машинах, то это URL-адрес машины провайдера, а не центрального сервера. Если провайдер OVN находится на той же машине, что и Менеджер управления, можно оставить URL-адрес, заданный по умолчанию: `http://localhost:9696`.

9. Снимите флажок **Только для чтения (Read-Only)**, чтобы разрешить создание новых сетей OVN из Менеджера управления.
10. При желании установите флажок **Требуется авторизация (Requires Authentication)** и введите **Имя пользователя (Username)** и **Пароль (Password)** для пользователя внешнего провайдера сети, зарегистрированного в Keystone. Необходимо также указать аутентификационный URL-адрес сервера Keystone, задав **Протокол (Protocol)**, **Имя хоста (Hostname)** и **Порт API (API Port)**.

    Метод аутентификации должен быть настроен в файле **/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf** (создайте этот файл, если он еще не существует). Перезапустите службу `ovirt-provider-ovn`, чтобы изменение вступило в силу. Подробности об аутентификации OVN см. по ссылке.
11. Проверьте учетные данные:
    a. Нажмите **[Тестировать (Test)]**, чтобы проверить, удается ли выполнить успешную аутентификацию в OVN с использованием предоставленных учетных данных.
    b. Если экземпляр OVN использует SSL, откроется окно **Импортировать сертификаты провайдера (Import provider certificates)**. Нажмите **[OK]**, чтобы импортировать сертификат, предоставленный экземпляром OVN, чтобы гарантировать, что Менеджер управления сможет взаимодействовать с экземпляром.
12. Нажмите **[OK]**.
13. Создайте новый кластер, использующий OVN в качестве провайдера сети по умолчанию. См. раздел Создание нового кластера и выберите провайдера сети OVN в выпадающем списке **Провайдер сети по умолчанию (Default Network Provider)**.
14. Добавьте хосты к кластеру. Хосты, добавленные в этот кластер, автоматически настраиваются на связь с OVN. Чтобы добавить новые хосты, см. раздел Добавление стандартных хостов в Менеджер управления.
15. Импортируйте или добавьте сети OVN к новому кластеру. Чтобы импортировать сети, см. раздел Импортирование сетей из внешних провайдеров. Чтобы создать новые сети с использованием OVN, см. раздел Создание новой логической сети в центре данных или кластере и установите флажок **Создать на внешнем провайдере (Create on external provider)**. По умолчанию выбрано значение `ovirt-provider-ovn`.

    Сведения о том, как настроить хосты на использование существующей сети, не являющейся сетью по умолчанию, см. в разделе Настройка хостов для сети туннелей OVN.

    Чтобы подключить сеть OVN к собственной сети zVirt, установите флажок **Подключить к физической сети (Connect to physical network)** и укажите сеть zVirt, которую нужно использовать. Дополнительную информацию и предварительные требования см. в разделе Подключение сети OVN к физической сети.

Теперь можно создавать виртуальные машины, использующие сети OVN.

2.8. Использование Ansible-playbook для изменения сети туннелей OVN

Можно применить Ansible-playbook **ovirt-provider-ovn-driver**, чтобы использовать длинные имена для модификации сети туннелей для контроллеров OVN.

Использование Ansible-playbook для модификации сети туннелей OVN

```
ansible-playbook \
    --key-file <path_to_key_file> \
    -i <path_to_inventory> \
    --extra-vars "cluster_name=<cluster_name> ovn_central=
<ovn_central_ip_address> ovirt_network=<ovirt network name>
ovn_tunneling_interface=<vdsm_network_name>" \
    ovirt-provider-ovn-driver.yml
```

Параметры

- `key-file` - Файл ключа для авторизации на хосте. Файл ключа по умолчанию обычно находится в каталоге **/etc/pki/ovirt-engine/keys**.
- `inventory` - Список виртуальных машин oVirt. Чтобы определить значение списка, используйте данный скрипт: **/usr/share/ovirt-engine-metrics/bin/ovirt-engine-hosts-ansible-inventory**.
- `cluster_name` - Имя кластера, на которое нужно заменить имя
- `ovn_central` - IP-адрес центрального сервера OVN. Этот IP-адрес должен быть доступен для всех хостов.
- `ovirt_network` - Имя сети oVirt.
- `ovn_tunneling_interface` - Имя сети VDSM.

Ansible-playbook **ovirt-provider-ovn-driver** поддерживает использование либо параметра `ovirt_network`, либо параметра `ovn_tunneling_interface`. Если в одном playbook присутствуют оба параметра, то этот playbook не работает.

Пример 1. Playbook с параметром ovirt_network

```
ansible-playbook \
  --key-file /etc/pki/ovirt-engine/keys/engine_id_rsa \
  -i /usr/share/ovirt-engine-metrics/bin/ovirt-engine-hosts-ansible-inventory
\
  --extra-vars " cluster_name=test-cluster ovn_central=192.168.200.2
```

```
ovirt_network="Long_Network_Name_with_Ascii_character"" \
  ovirt-provider-ovn-driver.yml
```

Пример 2. Playbook с параметром ovn_tunneling_interface

```
ansible-playbook \
  --key-file /etc/pki/ovirt-engine/keys/engine_id_rsa \
  -i /usr/share/ovirt-engine-metrics/bin/ovirt-engine-hosts-ansible-inventory
\
  --extra-vars " cluster_name=test-cluster ovn_central=192.168.200.2
ovn_tunneling_interface=on703ea21ddbc34" \
  ovirt-provider-ovn-driver.yml
```

На машине с Менеджером управления перейдите в каталог **/usr/share/ovirt-engine/play-books**, чтобы запускать Ansible-playbook.

2.9. Настройка хостов для сети туннелей OVN

Можно настроить свои хосты на использование существующей сети, отличной от сети по умолчанию ovirtmgmt, с помощью Ansible-playbook **ovirt-provider-ovn-driver**. Сеть должна быть доступна для всех хостов в кластере.

Ansible-playbook **ovirt-provider-ovn-driver** обновляет существующие хосты. При добавлении новых хостов в кластер необходимо снова запустить playbook.

Порядок действий:

1. На машине с Менеджером управления перейдите в каталог **playbooks**:

   ```
   cd /usr/share/ovirt-engine/playbooks
   ```

2. Выполните команду `ansible-playbook` со следующими параметрами:

   ```
   ansible-playbook \
       --private-key=/etc/pki/ovirt-engine/keys/engine_id_rsa \
       -i /usr/share/ovirt-engine-metrics/bin/ovirt-engine-hosts-ansible-
   inventory \
       --extra-vars " cluster_name=Cluster_Name ovn_central=OVN_Central_IP
   ovn_tunneling_interface=VDSM_Network_Name" \
       ovirt-provider-ovn-driver.yml
   ```

   Пример 3. Настройка хоста для сети туннелей OVN

   ```
   ansible-playbook \
    --private-key=/etc/pki/ovirt-engine/keys/engine_id_rsa \
   ```

```
 -i /usr/share/ovirt-engine-metrics/bin/ovirt-engine-hosts-ansible-
inventory \
 --extra-vars " cluster_name=MyCluster ovn_central=192.168.0.1
ovn_tunneling_interface=MyNetwork" \
 ovirt-provider-ovn-driver.yml
```

OVN_Central_IP может находиться в новой сети, но это не обязательно. OVN_Central_IP должен быть доступен для всех хостов.

Длина VDSM_Network_Name ограничена 15 знаками. Если вы задали имя логической сети, длина которого превышает 15 знаков или содержит знаки, отличные от ASCII, то будет автоматически создано 15-значное имя. Указания по визуализации сопоставления этих имен см. в разделе Инструмент сопоставления VDSM с именем сети.

Обновление сети туннелей OVN на одном хосте

Обновить сеть туннелей OVN на одном хосте можно с помощью vdsm-tool:

```
vdsm-tool ovn-config _OVN_Central_IP_ _Tunneling_IP_or_Network_Name_
```

Пример 4. Обновление хоста с помощью vdsm-tool

```
vdsm-tool ovn-config 192.168.0.1 MyNetwork
```

2.10. Подключение сети OVN к физической сети

Можно создать сеть на внешнем провайдере, наложенную на собственную сеть zVirt, чтобы виртуальные машины в каждой из них выглядели использующими одну и ту же подсеть.

Если вы создали подсеть для сети OVN, то виртуальная машина, использующая эту сеть, получит IP-адрес оттуда. Если нужно, чтобы IP-адрес выделяла физическая сеть, не создавайте подсеть для сети OVN.

Предварительные условия:

- В качестве **Типа коммутатора (Switch Type)** в кластере должно быть выбрано `Open vSwitch`. Хосты, добавляемые в этот кластер, не должны иметь уже настроенных сетей zVirt, таких как **мост (bridge) ovirtmgmt**.
- На хостах должна быть доступна физическая сеть. Это можно обеспечить, настроив физическую сеть в соответствии с требованиями кластера (в окне **Управление сетями (Manage Networks)** или на вкладке **Кластер (Cluster)** окна **Новая логическая сеть (New Logical Network)**).

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Кластеры (Clusters)**.
2. Нажмите на имя кластера, Откроется подробное представление.
3. Откройте вкладку **Логические сети (Logical Networks)** и нажмите **[Добавить сеть (Add Network)]**.
4. Введите **Имя (Name)** для сети.
5. Установите флажок **Создать на внешнем провайдере (Create on external provider)**. По умолчанию выбрано `ovirt-provider-ovn`.
6. Установите флажок **Подключение к физической сети (Connect to physical network)**, если он не установлен по умолчанию.
7. Выберите физическую сеть, к которой будет подключаться новая сеть:
   - Нажмите кнопку-переключатель **Сеть центра данных (Data Center Network)** и выберите физическую сеть в выпадающем списке. Это - рекомендуемый параметр.
   - Нажмите кнопку-переключатель **Пользовательские (Custom)** и введите имя физической сети. Если в физической сети включено тегирование VLAN, то необходимо также установить флажок **Включить тегирование VLAN (Enable VLAN tagging)** и ввести VLAN-тег физической сети.

> Имя физической сети не должно быть длиннее 15 знаков и не должно содержать специальных знаков.

8. Нажмите **[OK]**.

2.11. Добавление внешнего провайдера сети

В zVirt можно добавить любого провайдера сети, реализующего REST API для работы в сети OpenStack. Драйвер виртуального интерфейса должен быть предоставлен разработчиком внешнего провайдера сети.

Порядок действий:

1. Нажмите **Управление (Administration)** > **Провайдеры (Providers)**.
2. Нажмите **[Добавить (Add)]** и введите подробные сведения на вкладке **Общее (General Settings)**. Дополнительную информацию об этих полях см. в разделе Описание общих настроек при добавлении провайдера.
3. Введите **Имя (Name)** и **Описание (Description)**.
4. Выберите **Внешнего провайдера сети (External Network Provider)** в выпадающем списке **Тип (Type)**.
5. При желании нажмите на текстовое поле **Сетевой модуль (Networking Plugin)** и выберите соответствующий драйвер в выпадающем меню.

6. При желании установите флажок **Автоматическая синхронизация (Automatic Synchronization)**. Это включает автоматическую синхронизацию внешнего провайдера сети с существующими сетями. При добавлении внешних провайдеров сети эта возможность по умолчанию отключена.

> Автоматическая синхронизация включена по умолчанию на провайдере сети ovirt-provider-ovn, созданном инструментом engine-setup.

7. Введите URL-адрес или FQDN машины с установленным внешним провайдером сети в текстовое поле **URL провайдера (Provider URL)** и далее номер порта. По умолчанию установлен флажок **Только для чтения (Read-Only)**. Это не позволит пользователям внести изменения в провайдер внешней сети.
8. При желании установите флажок **Требуется авторизация (Requires Authentication)** и введите **Имя пользователя (Username)** и **Пароль (Password)** для пользователя внешнего провайдера сети, зарегистрированного в Keystone. Необходимо также указать аутентификационный URL-адрес сервера Keystone, задав **Протокол (Protocol)**, **Имя хоста (Hostname)** и **Порт API (API Port)**.
9. Проверьте учетные данные:
    a. Нажмите **[Тестировать (Test)]**, чтобы проверить, удается ли выполнить успешную аутентификацию на провайдере внешней сети с использованием предоставленных учетных данных.
    b. Если провайдер внешней сети использует SSL, откроется окно **Импортировать сертификаты провайдера (Import provider certificates)**. Нажмите **[OK]**, чтобы импортировать сертификат, предоставленный внешним провайдером сети, чтобы гарантировать, что Менеджер управления сможет взаимодействовать с экземпляром.
10. Нажмите **[OK]**.

Прежде чем можно будет использовать сети от этого провайдера, нужно установить драйвер виртуального интерфейса на хосты и импортировать сети. Чтобы импортировать сети, см. раздел Импортирование сетей из внешних провайдеров.

2.12. Описание общих настроек при добавлении провайдера

На вкладке **Общее (General)** в окне **Добавить провайдера (Add Provider)** можно регистрировать основные сведения о внешнем провайдере.

Таблица 1. Добавление провайдера: общие настройки

Параметр	Пояснение

Параметр	Пояснение
Имя (Name)	Имя, под которым провайдер представляется в Менеджере управления.
Описание (Description)	Удобочитаемое описание провайдера в виде неформатированного текста.

Параметр	Пояснение
Тип (Type)	Тип внешнего провайдера. Изменение этой настройки изменяет поля, доступные для конфигурирования провайдера. **Внешний провайдер сети (External Network Provider)** • **Сетевой модуль (Networking Plugin)**: Определяет, какая реализация драйвера будет использоваться на хосте для организации работы сетевой карты. Если внешний провайдер сети с плагином oVirt Network Provider for OVN добавляется в качестве провайдера сети по умолчанию для кластера, то этот параметр также определяет, какой драйвер будет устанавливаться на хостах, добавляемых к кластеру. • **Автоматическая синхронизация (Automatic Synchronization)**: Позволяет указать, будет ли провайдер автоматически синхронизироваться с существующими сетями. • **URL провайдера (Provider URL)**: URL-адрес или FQDN машины, на которой размещен внешний провайдер сети. В конец URL-адреса или FQDN необходимо добавить номер порта для внешнего провайдера сети. Номер порта по умолчанию - 9696. • **Только для чтения (Read Only)**: Позволяет указать, можно ли изменять внешний провайдер сети с Портала администрирования. • **Требуется авторизация (Requires Authentication)**: Позволяет указать, требуется ли аутентификация для доступа к внешнему провайдеру сети. • **Имя пользователя (Username)**: Имя пользователя для подключения к внешнему провайдеру сети. Если для аутентификации используется Active Directory, то имя пользователя должно иметь формат `имя_пользователя@домен@профиль_авторизации` вместо формата, используемого по умолчанию: `имя_пользователя@домен`. • **Пароль (Password)**: Пароль, по которому будет выполняться аутентификация пользователя с вышеуказанным именем. • **Протокол (Protocol)**: Протокол, используемый для взаимодействия с сервером Keystone. Значение по умолчанию - `HTTPS`. • **Имя хоста (Hostname)**: IP-адрес или имя хоста сервера Keystone. • **Порт API (API port)**: Номер порта API сервера Keystone. • **Версия API (API Version)**: Версия сервера Keystone. Значение равно v2.0, и это поле неактивно. • **Наименование арендатора (Tenant Name)**: Необязательно. Имя арендатора, членом которого является внешний провайдер сети. **KubeVirt/OpenShift Virtualization** • **URL провайдера (Provider URL)**: URL-адрес или FQDN и номер порта API-интерфейса контейнерной платформы OpenShift. Номер порта по умолчанию - 6443.

Параметр	Пояснение
	• **Токен (Token)**: Токен доступа OAuth для аутентификации этого подключения к API-интерфейсу. • **Центр сертификации (Certificate Authority)**: Сертификат ЦС, которому следует доверять при выполнении https-запросов. • **URL-адрес Prometheus (Prometheus URL)**: URL-адрес службы prometheus кластера OpenShift. Если не указать этот URL-адрес, программа попытается автоматически определить его. • **Центр сертификации Prometheus (Prometheus Certificate Authority)**: Сертификат X509 для prometheus. Если не указать этот Центр сертификации, провайдер использует вместо него KubeVirt. **OpenStack Image** • **URL провайдера (Provider URL)**: URL-адрес или FQDN машины, на которой размещена служба OpenStack Image. В конец URL-адреса или FQDN необходимо добавить номер порта для службы OpenStack Image. Номер порта по умолчанию - 9292. • **Требуется аутентификация (Requires Authentication)**: Позволяет указать, требуется ли аутентификация для доступа к службе OpenStack Image. • **Имя пользователя (Username)**: Имя пользователя для подключения к серверу Keystone. Это имя пользователя должно представлять собой имя пользователя для службы OpenStack Image, зарегистрированное в экземпляре Keystone, членом которого является служба OpenStack Image. • **Пароль (Password)**: Пароль, по которому будет выполняться аутентификация пользователя с вышеуказанным именем. Этот пароль должен представлять собой пароль для службы OpenStack Image, зарегистрированный в экземпляре Keystone, членом которого является служба OpenStack Image. • **Протокол (Protocol)**: Протокол, используемый для взаимодействия с сервером Keystone. Необходимо задать значение HTTP. • **Имя хоста (Hostname)**: IP-адрес или имя хоста сервера Keystone. • **Порт API (API Port)**: Номер порта API сервера Keystone. • **Версия API (API Version)**: Версия службы Keystone. Значение равно v2.0, и это поле неактивно. • **Наименование арендатора (Tenant Name)**: Необязательно. Имя арендатора, членом которого является внешний провайдер сети. **OpenStack Networking** • **Сетевой модуль (Networking Plugin)**: Сетевой плагин для подключения к серверу OpenStack Networking. Для OpenStack Networking единственным параметром является **Open vSwitch**, и он выбран по умолчанию.

Параметр	Пояснение
	• **Автоматическая синхронизация (Automatic Synchronization)**: Позволяет указать, будет ли провайдер автоматически синхронизироваться с существующими сетями. • **URL провайдера (Provider URL)**: URL-адрес или FQDN машины, на которой размещен экземпляр OpenStack Networking. В конец URL-адреса или FQDN необходимо добавить номер порта для экземпляра OpenStack Networking. Номер порта по умолчанию - 9696. • **Только для чтения (Read Only)**: Позволяет указать, можно ли изменять экземпляр OpenStack Networking с Портала администрирования. • **Требуется авторизация (Requires Authentication)**: Позволяет указать, требуется ли аутентификация для доступа к службе OpenStack Networking. • **Имя пользователя (Username)**: Имя пользователя для подключения к экземпляру OpenStack Networking. Это имя пользователя должно представлять собой имя пользователя для OpenStack Networking, зарегистрированное в экземпляре Keystone, членом которого является экземпляр OpenStack Networking. • **Пароль (Password)**: Пароль, по которому будет выполняться аутентификация пользователя с вышеуказанным именем. Этот пароль должен представлять собой пароль для OpenStack Networking, зарегистрированный в экземпляре Keystone, членом которого является экземпляр OpenStack Networking. • **Протокол (Protocol)**: Протокол, используемый для взаимодействия с сервером Keystone. Значение по умолчанию - `HTTPS`. • **Имя хоста (Hostname)**: IP-адрес или имя хоста сервера Keystone. • **Порт API (API Port)**: Номер порта API сервера Keystone. • **Версия API (API Version)**: Версия сервера Keystone. Она отображается в URL-адресе. Если отобразится v2.0, выберите `v2.0`. Если отобразится `v3`, выберите `v3`. ***Если в поле Версия API (API Version) выбрать v3, появляются следующие поля*** ◦ **Имя доменного пользователя (User Domain Name)**: Имя пользователя, определенного в домене. При использовании версии v3 API-интерфейса Keystone домены используются для определения административных границ служебных объектов в OpenStack. Домены позволяют объединять пользователей в группы для различных целей, например для настройки конфигурации конкретного домена или параметров безопасности. ◦ **Имя проекта (Project Name)**: Определяет имя проекта для версии v3 API-интерфейса службы OpenStack Identity.

Параметр	Пояснение
	◦ **Доменное имя проекта (Project Domain Name)**: Определяет имя домена проекта для версии v3 API-интерфейса службы OpenStack Identity. ***Если в поле Версия API (API Version) выбрать `v2.0`, появляется следующее поле*** ◦ **Наименование арендатора (Tenant Name)**: Появляется только, когда в поле **Версия API (API Version)** выбрано `v2.0`. Имя арендатора OpenStack, членом которого является экземпляр OpenStack Networking. **OpenStack_Volume** • **Центр данных (Data Center)**: Центр данных, к которому будут подключены тома хранилища OpenStack Volume. • **URL провайдера (Provider URL)**: URL-адрес или FQDN машины, на которой размещен экземпляр OpenStack Volume. В конец URL-адреса или FQDN необходимо добавить номер порта для экземпляра OpenStack Volume. Номер порта по умолчанию - 8776. • **Требуется авторизация (Requires Authentication)**: Позволяет указать, требуется ли аутентификация для доступа к службе OpenStack Volume. • **Имя пользователя (Username)**: Имя пользователя для подключения к серверу Keystone. Это имя пользователя должно представлять собой имя пользователя для OpenStack Volume, зарегистрированное в экземпляре Keystone, членом которого является экземпляр OpenStack Volume. • **Пароль (Password)**: Пароль, по которому будет выполняться аутентификация пользователя с вышеуказанным именем. Этот пароль должен представлять собой пароль для OpenStack Volume, зарегистрированный в экземпляре Keystone, членом которого является экземпляр OpenStack Volume. • **Протокол (Protocol)**: Протокол, используемый для взаимодействия с сервером Keystone. Необходимо задать значение HTTP. • **Имя хоста (Hostname)**: IP-адрес или имя хоста сервера Keystone. • **Порт API (API Port)**: Номер порта API сервера Keystone. • **Версия API (API Version)**: Версия сервера Keystone. Значение равно `v2.0`, и это поле неактивно. • **Наименование арендатора (Tenant Name)**: Имя арендатора OpenStack, членом которого является экземпляр OpenStack Volume. **VMware** • **Центр данных (Data Center)**: Укажите **Центр данных (Data Center)**, в который будут импортироваться виртуальные машины VMware, либо выберите `Любой центр данных (Any Data Center)`, чтобы указывать центр данных, являющийся приемником, во время каждой отдельной операции импорта (используя функцию

Параметр	Пояснение
	[Импортировать (Import)] на вкладке **Виртуальные машины (Virtual Machines)**). • **vCenter**: IP-адрес или FQDN экземпляра VMware vCenter. • **ESXi**: IP-адрес или FQDN хоста, из которого будут импортироваться виртуальные машины. • **Центр данных (Data Center)**: Имя центра данных, в котором находится указанный хост ESXi. • **Кластер (Cluster)**: Имя кластера, в котором находится указанный хост ESXi. • **Проверять SSL-сертификат сервера (Verify server's SSL certificate)**: Укажите, будет ли сертификат хоста ESXi проверяться при подключении. • **Хост прокси (Proxy Host)**: Выберите хост в выбранном центре данных с установленным пакетом virt-v2v, который будет служить хостом во время операций импорта виртуальных машин. Этот хост также должен быть способен подключаться к сети внешнего провайдера VMware vCenter. Если вы выбрали `Любой центр данных (Any Data Center)`, то вы не сможете выбрать хост здесь, но сможете указывать хост во время конкретных операций импорта (используя функцию **[Импортировать (Import)]** на вкладке **Виртуальные машины (Virtual Machines)**. • **Имя пользователя (Username)**: Имя пользователя для подключения к экземпляру VMware vCenter. Пользователь должен иметь доступ к центру данных VMware и хосту ESXi, на котором находятся виртуальные машины. • **Пароль (Password)**: Пароль, по которому будет выполняться аутентификация пользователя с вышеуказанным именем. **KVM** • **Центр данных (Data Center)**: Укажите центр данных, в который будут импортироваться виртуальные машины KVM, либо выберите `Любой центр данных (Any Data Center)`, чтобы указывать центр данных, являющийся приемником, во время каждой отдельной операции импорта (используя функцию **[Импортировать (Import)]** на вкладке **Виртуальные машины (Virtual Machines)**). • **URI**: URI хоста KVM. • **Хост прокси (Proxy Host)**: Выберите хост в выбранном центре данных, который будет служить хостом во время операций импорта виртуальных машин. Этот хост также должен быть способен подключаться к сети внешнего провайдера KVM. Если вы выбрали `Любой центр данных (Any Data Center)`, то вы не сможете выбрать хост здесь, но зато сможете указывать хост во время конкретных операций импорта (используя функцию **[Импортировать (Import)]** на вкладке **Виртуальные машины (Virtual Machines)**).

Параметр	Пояснение
	• **Требуется авторизация (Requires Authentication)**: Позволяет указать, требуется ли аутентификация для доступа к хосту KVM. • **Имя пользователя (Username)**: Имя пользователя для подключения к хосту KVM. • **Пароль (Password)**: Пароль, по которому будет выполняться аутентификация пользователя с вышеуказанным именем.
Тестирование (Test)	Позволяет пользователям проверить указанные учетные данные. Эта кнопка доступна для провайдеров всех типов.

3. Изменение внешнего провайдера

Порядок действий:

1. Нажмите **Управление (Administration)** > **Провайдеры (Providers)** и выберите внешнего провайдера, который нужно изменить.
2. Нажмите **[Изменить (Edit)]**.
3. Измените текущие значения параметров провайдера на желаемые.
4. Нажмите **[OK]**.

4. Удаление внешнего провайдера

Порядок действий:

1. Нажмите **Управление (Administration)** > **Провайдеры (Providers)** и выберите внешнего провайдера, который нужно удалить.
2. Нажмите **[Удалить (Remove)]**.
3. Нажмите **[OK]**.

Управление хостами

1. Общие сведения о хостах

Хосты, также именуемые **гипервизорами** - это физические серверы, на которых работают виртуальные машины. Полная виртуализация обеспечивается благодаря использованию загружаемого модуля ядра Linux, который носит название Kernel-based Virtual Machine (KVM).

KVM позволяет одновременно запускать несколько виртуальных машин под управлением Windows или Linux. Виртуальные машины работают как отдельные Linux процессы и потоки на хост-машине, а дистанционное управление ими осуществляет Менеджер управления. К среде zVirt подключены один или несколько хостов.

Для установки хостов zVirt используйте установочный носитель zVirt Node.

Тип отдельного хоста можно узнать в Менеджере управления, выбрав имя нужного хоста. Откроется подробное представление. Затем посмотрите **Описание ОС (OS Description)** в разделе **Программное обеспечение (Software)**.

Хосты используют профили `tuned`, обеспечивающие оптимизацию виртуализации.

В среде исполнения zVirt включены функции безопасности. Security Enhanced Linux (SELinux) и межсетевой экран полностью настроены и включены по умолчанию. Состояние SELinux на выбранном хосте отображается под заголовком **Режим SELinux (SELinux mode)** на вкладке **Общие (General)** в подробном представлении. Менеджер управления может открывать необходимые порты на хостах, когда он добавляет их в среду.

Хост - это физический 64-разрядный сервер с расширениями AMD-V™ или Intel VT®, на котором работает соответствующая версия ОС.

Физический хост на платформе zVirt:

- Должен принадлежать только одному кластеру в системе.
- Должен иметь ЦП, которые поддерживают расширения для виртуализации аппаратного обеспечения AMD-V™ или Intel VT®.
- Должен иметь ЦП, поддерживающие всю функциональность, предоставляемую типом виртуального процессора, который был выбран при создании кластера.
- Должен иметь объем ОЗУ не менее 4 ГБ.
- Может иметь назначенного системного администратора с системными разрешениями.

2. Среда исполнения zVirt Node

Среда исполнения zVirt Node устанавливается с помощью специальной сборки, содержащей только те пакеты, которые необходимы для хостинга виртуальных машин. Она использует интерфейс установки **Anaconda** и может обновляться с помощью Менеджера управления или команды `dnf`. Использование команды `dnf` - это единственный способ установить дополнительные пакеты.

zVirt Node имеет веб-интерфейс Cockpit для мониторинга ресурсов хоста и выполнения административных задач. Веб-интерфейс Cockpit предлагает графический пользовательский интерфейс для задач, которые выполняются до добавления хоста в Менеджер управления, таких как настройка сети или выполнение терминальных команд на вкладке **Терминал (Terminal)**.

Для доступа к веб-интерфейсу Cockpit в веб-браузере введите `https://<HostFQDNorIP>:9090`. В Cockpit для zVirt Node есть настраиваемый дашборд **Virtualization**, отображающий состояние хоста, SSH ключ хоста, статус **hosted engine**, виртуальные машины и статистику виртуальных машин.

zVirt Node использует инструмент автоматического создания отчетов об ошибках (ABRT) для сбора значимой отладочной информации о сбоях приложений.

Пользовательские аргументы ядра загрузки можно добавить в zVirt Node с помощью инструмента **grubby**. Инструмент **grubby** вносит постоянные изменения в файл **grub.cfg**. Перейдите на вложенную вкладку **Терминал (Terminal)** в веб-интерфейсе хоста Cockpit для использования команд `grubby`.

Не следует добавлять непроверенных пользователей к zVirt Node, так как это может создать условия для эксплуатации локальных уязвимостей в системе защиты.

3. Задачи в отношении хоста

3.1. Добавление стандартных хостов в Менеджер управления

Всегда используйте Менеджер управления для изменения сетевой конфигурации хостов в кластерах. В противном случае можно создать неподдерживаемую конфигурацию. Дополнительные сведения см. в разделе Менеджер сетевой конфигурации с отслеживанием состояния (nmstate).

Добавление хоста в среду zVirt может занять некоторое время, так как платформа выполняет следующие шаги: **проверка поддержки виртуализации**, **установка пакетов** и **создание моста**.

Порядок действий:

1. На Портале администрирования выберите **Ресурсы (Compute) > Хосты (Hosts)**.
2. Нажмите **[Новый (New)]**.
3. В выпадающем списке **Хост кластера (Host Cluster)** выберите Центр данных (Data Center) и Кластер для нового хоста.
4. Введите имя и адрес нового хоста в поля **Имя (Name)** и **FQDN/IP**. Стандартный для SSH порт 22 автоматически вводится в поле **Порт SSH (SSH Port)**.
5. Выберите способ аутентификации, который Менеджер управления будет использовать для доступа к хосту:
    - Укажите пароль root-пользователя, чтобы использовать аутентификацию по паролю.
    - Либо скопируйте ключ, отображаемый в поле **Публичный ключ SSH (SSH PublicKey)**, в **/root/.ssh/authorized_keys** на хосте, чтобы использовать аутентификацию по открытому ключу.
6. При желании можно нажать **Дополнительные параметры (Advanced Parameters)**, чтобы изменить следующие дополнительные настройки хоста:
    - Отключить **автоматическую настройку межсетевого экрана**.
    - Добавить **Публичный ключ SSH хоста**, чтобы повысить безопасность. Его можно добавить вручную или подтянуть автоматически.
7. При необходимости настройте управление питанием, если хост имеет поддерживаемую карту с управлением питания. Информацию о настройках параметров управления питанием см. в разделе Описание настроек управления питанием хоста.
8. Нажмите **[OK]**.

Новый хост отображается в списке хостов со статусом **Установка (Installing)** ; за ходом установки можно следить в разделе **События (Events)** на **Панели уведомлений (Notification Drawer)**. После небольшой задержки статус хоста изменится на **Включен (Up)** .

3.2. Настройка хоста для сквозного доступа PCI

Включение сквозного доступа PCI позволяет виртуальной машине использовать устройство хоста, как если бы оно было напрямую подключено к виртуальной машине. Чтобы включить сквозной доступ PCI, необходимо включить расширения виртуализации и функцию IOMMU.

Следующая процедура требует перезагрузки хоста. Если хост уже подключен к Менеджеру управления, сначала убедитесь, что хост переведен в режим обслуживания.

Предварительные условия:

- Убедитесь, что аппаратное обеспечение хоста отвечает требованиям сквозного доступа и назначения PCI-устройств. Дополнительную информацию см. в разделе Требования к проброску устройств Руководства по предварительному планированию инфраструктуры.

Настройка хоста для сквозного доступа PCI

Порядок действий:

1. Включите расширение виртуализации и расширение IOMMU в BIOS.
2. Включите флаг IOMMU в ядре, установив флажок **Passthrough устройств хоста и SR-IOV (Hostdev Passthrough & SR-IOV)** при добавлении хоста в Менеджер управления или изменив конфигурационный файл grub вручную.
    - Чтобы включить флаг IOMMU на Портале администрирования, см. разделы Добавление стандартных хостов в Менеджер управления и Описание настроек ядра.
    - Чтобы изменить конфигурационный файл grub вручную, см. **Включение IOMMU вручную**.
3. Для включения сквозного доступа к графическому процессору нужно выполнить дополнительные действия по настройке как на хосте, так и в гостевой системе. Дополнительную информацию см. в документе NVIDIA vGPU

Включение IOMMU вручную

Порядок действий:

1. Включите IOMMU, изменив конфигурационный файл grub.
    - Если используется Intel, загрузите машину и добавьте `intel_iommu=on` в конец строки `GRUB_CMDLINE_LINUX` в конфигурационном файле **grub**.

```
vi /etc/default/grub
...
GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... intel_iommu=on
...
```

    - Если используется AMD, загрузите машину и добавьте amd_iommu=on в конец строки GRUB_CMDLINE_LINUX в конфигурационном файле grub.

```
vi /etc/default/grub
...
GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... amd_iommu=on
...
```

В случае обнаружения `intel_iommu=on` или `amd_iommu=on` можно попытаться добавить `iommu=pt`. Опция `pt` включает IOMMU только для устройств в сквозном доступе и обеспечивает более высокую производительность хоста. Однако эта опция поддерживается не на всем оборудовании. Если опция `pt` для вашего хоста не работает, вернитесь к предыдущей опции.

Если сквозной доступ включить не удастся из-за того, что оборудование не поддерживает переназначение прерываний, можно попробовать включить опцию `allow_unsafe_interrupts`, если виртуальные машины являются доверенными. По умолчанию опция `allow_unsafe_interrupts` выключена, поскольку включить ее - значит потенциально подвергнуть хост MSI-атакам со стороны виртуальных машин. Чтобы включить ее, выполните:

```
vi /etc/modprobe.d
options vfio_iommu_type1 allow_unsafe_interrupts=1
```

2. Обновите файл **grub.cfg** и перезагрузите хост, чтобы эти изменения вступили в силу:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
reboot
```

3.3. Включение вложенной виртуализации

3.3.1. Включение вложенной виртуализации для всех виртуальных машин

Вложенная виртуализация позволяет одним виртуальным машинам осуществлять хостинг других виртуальных машин. Для ясности назовем их родительскими виртуальными машинами (parent virtual machines) и вложенными виртуальными машинами (nested virtual machines).

Вложенные виртуальные машины видимы и управляются только пользователями, имеющими доступ к родительской виртуальной машине. Они невидимы для администраторов zVirt.

По умолчанию вложенная виртуализация в zVirt выключена. Чтобы включить вложенную виртуализацию, установите хук VDSM `vdsm-hook-nestedvt` на все хосты в кластере. Затем все виртуальные машины, работающие на этих хостах, смогут работать как родительские.

Запускать родительские виртуальные машины следует только на хостах, поддерживающих вложенную виртуализацию. Если родительскую виртуальную машину перенести на хост, не поддерживающий вложенную виртуализацию, то ее вложенные виртуальные машины перестанут работать. Чтобы этого не произошло, настройте все хосты в кластере на

поддержку вложенной виртуализации. Либо запретите миграцию родительских виртуальных машин на хосты, не поддерживающие вложенную виртуализацию.

Не забудьте запретить миграцию родительских виртуальных машин на хосты, не поддерживающие вложенную виртуализацию.

Порядок действий:

1. На Портале администрирования нажмите **Ресурсы (Compute) > Хосты (Hosts)**.
2. Выберите хост в кластере, где хотите включить вложенную виртуализацию, и нажмите **[Управление (Management)]** → **[Обслуживание (Maintenance)]** и затем **[OK]**.
3. Выберите хост снова, нажмите **[Консоль хоста (Host Console)]** и авторизуйтесь на консоли хоста.
4. Установите хук VDSM:

   ```
   dnf install vdsm-hook-nestedvt
   ```

5. Перезагрузите хост.
6. Снова авторизуйтесь на консоли хоста и убедитесь, что вложенная виртуализация включена:

   ```
   $ cat /sys/module/kvm*/parameters/nested
   ```

   Если эта команда вернет `Y` или `1`, то вложенная виртуализация включена.

7. Повторите эту процедуру для всех хостов в кластере.

   Дополнительные ресурсы

   - Хуки VDSM.

3.3.2. Включение вложенной виртуализации для отдельных виртуальных машин

Вложенная виртуализация позволяет одним виртуальным машинам осуществлять хостинг других виртуальных машин. Для ясности назовем их родительскими виртуальными машинами (parent virtual machines) и вложенными виртуальными машинами (nested virtual machines).

Вложенные виртуальные машины видимы и управляются только пользователями, имеющими доступ к родительской виртуальной машине. Они невидимы для администраторов zVirt (RHV).

Чтобы включить вложенную виртуализацию не на всех, а лишь на некоторых виртуальных машинах, настройте хост или хосты на поддержку вложенной виртуализации. Затем настройте виртуальную машину или виртуальные машины на запуск на этих конкретных

хостах и включите **Сквозной доступ ЦП хоста (Pass-Through Host CPU)**. Эта опция позволяет виртуальным машинам использовать настройки вложенной виртуализации, которые вы только что задали на хосте. Эта опция также указывает, на каких хостах могут работать виртуальные машины, и требует ручной миграции.

В остальном, чтобы включить вложенную виртуализацию для всех виртуальных машин в кластере, см. раздел Включение вложенной виртуализации для всех виртуальных машин.

Запускайте родительские виртуальные машины только на хостах, поддерживающих вложенную виртуализацию. Если родительскую виртуальную машину перенести на хост, не поддерживающий вложенную виртуализацию, то ее вложенные виртуальные машины перестанут работать.

Не переносите родительские виртуальные машины на хосты, не поддерживающие вложенную виртуализацию.

Старайтесь не переносить "на лету" родительские виртуальные машины, на которых работают вложенные виртуальные машины. Даже если хост-источник и хост-приемник идентичны и поддерживают вложенную виртуализацию, миграция "на лету" может привести к сбою вложенных виртуальных машин. Вместо этого выключайте виртуальные машины, прежде чем переносить их.

Настройка хостов на поддержку вложенной виртуализации

Порядок действий:

1. На Портале администрирования нажмите **Ресурсы (Compute) > Хосты (Hosts)**.
2. Выберите хост в кластере, где хотите включить вложенную виртуализацию, и нажмите **[Управление (Management)]→ [Обслуживание (Maintenance)]** и затем **[OK]**.
3. Выберите хост снова, нажмите **[Консоль хоста (Host Console)]** и авторизуйтесь на консоли хоста.
4. В окне **Изменить хост (Edit Host)** выберите вкладку **Ядро (Kernel)**.
5. Если в блоке **Параметры загрузки ядра (Kernel boot parameters)** флажки неактивны, нажмите **[Сброс (RESET)]**.
6. Выберите **Вложенная виртуализация (Nested Virtualization)** и нажмите **[OK]**.

   Это действие выведет параметр `kvm-<architecture>.nested=1` в **Командной строке ядра (Kernel command line)**. Выполнение следующих действий добавит этот параметр в **Текущую cmdline ядра (Current kernel CMD line)**.
7. Нажмите **[Настройки (Installation)] → [Переустановить (Reinstall)]**.
8. Когда хост вернется в состояние **Включен (Up)** , нажмите **[Управление (Management)] → [Перезапустить (Restart)*]**в блоке **Управление питанием (Power Management)** или **Управление SSH (SSH Management)**.

9. Убедитесь, что вложенная виртуализация включена. Авторизуйтесь на консоли хоста и введите:

   ```
   $ cat /sys/module/kvm*/parameters/nested
   ```

   Если эта команда вернет `Y` или `1`, то вложенная виртуализация включена.

10. Повторите эту процедуру для всех хостов, на которых нужно запускать родительские виртуальные машины.

Включение вложенной виртуализации на отдельных виртуальных машинах

Порядок действий:

1. На Портале администрирования нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)**.
2. Выберите виртуальную машину и нажмите **[Изменить (Edit)]**.
3. В окне **Изменить виртуальную машину (Edit Vitual Machine)** нажмите **[Показать расширенные настройки (Show Advanced Options)]** и выберите вкладку **Хост (Host)**.
4. В блоке **Запустить на (Start Running On)** нажмите **Указанном хосте (Specific Host)** и выберите хост или хосты, которые вы настроили на поддержку вложенной виртуализации.
5. В блоке **Параметры ЦП (CPU Options)** выберите **Passthrough ЦП хоста (Pass-Through Host CPU)**. Это действие автоматически установит **Режим миграции (Migration mode)** в значение **Разрешить только ручную миграцию (Allow manual migration only).**

3.4. Перевод хоста в режим обслуживания

Многие распространенные задачи обслуживания, включая настройку сети и развертывание обновлений ПО, требуют перевода хостов в режим обслуживания. Хосты нужно переводить в режим обслуживания перед любым событием (например, перезагрузкой), которое может нарушить правильную работу VDSM или привести к проблемам с сетью или хранилищем.

Когда хост переводится в режим обслуживания, Менеджер управления пытается перенести все работающие виртуальные машины на альтернативные хосты. Для миграции "на лету" применимы стандартные предварительные условия, в частности, в кластере должен быть хотя бы один активный хост, способный запускать перенесенные виртуальные машины.

Виртуальные машины, которые закреплены за хостом и не могут быть перенесены, выключаются. Чтобы выяснить, какие виртуальные машины закреплены за хостом, нажмите **[Прикреплён к текущему хосту (Pinned to Host)]** на вкладке **Виртуальные машины (Virtual Machines)** в подробном представлении хоста.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)** и выберите нужный хост.
2. Нажмите **[Управление (Management)]** → **[Обслуживание (Maintenance)]**. Откроется окно подтверждения **Обслуживание хоста (Maintenance Host(s))**.
3. Если нужно, укажите **Причину (Reason)** перевода хоста в режим обслуживания, которая будет отображаться в журналах и при повторной активации хоста. Затем нажмите **[OK]**
4. Если нужно, установите необходимые флажки для хостов, поддерживающих Gluster.

   Установите флажок в поле **Игнорировать кворум Gluster и проверки в целях самовосстановления (Ignore Gluster Quorum and Self-Heal Validations)**, чтобы избежать выполняемых по умолчанию проверок. По умолчанию Менеджер управления проверяет, не потеряется ли кворум Gluster при переводе хоста в режим обслуживания. Менеджер управления также проверяет, не выполняется ли операция самовосстановления, которую может затронуть перевод хоста в режим обслуживания. Если будет потерян кворум Gluster или затронута операция самовосстановления, Менеджер управления не позволит перевести хост в режим обслуживания. Устанавливайте этот флажок только в том случае, если нет другого способа перевести хост в режим обслуживания.

   Установите флажок в поле **Остановить службу Gluster (Stop Gluster Service)**, чтобы остановить все службы Gluster при переводе хоста в режим обслуживания.

   > Эти поля будут отображаться в окне обслуживания хоста, только если выбранный хост поддерживает Gluster.

5. Нажмите **[OK]**, чтобы перейти в режим обслуживания.

Все работающие виртуальные машины переносятся на альтернативные хосты. Если хост выполняет роль **Менеджера пула хранения (SPM)**, то эта роль переносится на другой хост. Поле **Статус (Status)** хоста меняется на **Подготовка к обслуживанию (Preparing for Maintenance)** 🔧 и наконец на **[Обслуживание (Maintenance)]** 🔧, когда операция успешно завершается. VDSM не останавливается, пока хост находится в режиме обслуживания.

> Если миграция какой-либо виртуальной машины заканчивается неудачей, нажмите **[Управление (Management)]** → **[Включить (Activate)]** на хосте, чтобы остановить операцию перевода в режим обслуживания, затем нажмите **Отменить миграцию (Cancel Migration)** на виртуальной машине, чтобы остановить миграцию.

3.5. Активация хоста из режима обслуживания

Хост, переведенный в режим обслуживания или недавно добавленный в среду, должен быть активирован, прежде чем его можно будет использовать. Активация может завершиться неудачно, если хост не готов - перед активацией хоста убедитесь, что все задачи завершены.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)** и выберите хост.
2. Нажмите **[Управление (Management)]** → **[Включить (Activate)]**.

Статус хоста меняется на **Unassigned** 🔻 и наконец на **Включен (Up)** 🔺, когда операция завершается. Теперь на хосте могут работать виртуальные машины. Виртуальные машины, которые были перенесены с хоста при его переводе в режим обслуживания, не переносятся автоматически обратно на хост при его активации, но их можно перенести вручную. Если перед переводом в режим обслуживания хост выполнял роль **Менеджера пула хранения**, эта роль не возвращается автоматически при активации хоста.

3.6. Настройка правил межсетевого экрана для хостов

С помощью Ansible можно настроить правила межсетевого экрана для хостов, чтобы они были постоянными. Кластер должен быть сконфигурирован для использования firewalld.

ℹ️ Изменение зоны firewalld не поддерживается.

Порядок действий:

1. Чтобы добавить пользовательский порт межсетевого экрана, в машине Менеджера управления измените **ovirt-host-deploy-post-tasks.yml.example**:

```
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
```

2. Сохраните файл под именем **ovirt-host-deploy-post-tasks.yml**.

Новые или переустановленные хосты настраиваются с помощью обновленных правил межсетевого экрана.

Существующие хосты нужно переустановить, нажав **[Настройки (Installation)]** → **[Переустановить (Reinstall)]** и выбрав **Автоматически настроить межсетевой экран хоста (Automatically configure host firewall)**.

3.7. Удаление хоста

Иногда бывает нужно удалить хост из среды виртуализации zVirt, например, если его нужно переустановить.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)** и выберите хост.
2. Нажмите **[Управление (Management)]** → **[Обслуживание (Maintenance)]**.
3. Как только хост перейдет в режим обслуживания, нажмите **[Удалить (Remove)]**. Откроется окно с запросом на подтверждение удаления хостов **Удалить хост(ы) (Remove Host(s))**.
4. Если хост является частью кластера Gluster Storage и на нем находятся брики томов либо если хост не реагирует на запросы (**non-responsive**), то установите флажок **Принудительно удалить (Force Remove)**.
5. Нажмите **[OK]**.

3.8. Обновление хостов

Процедура обновления зависит от текущей версии zVirt и от режима развертывания (Hosted-Engine, StandAlone или StandAlone-All-in-One).

Для выполнения обновления хостов обратитесь к соответствующим процедурам, описанным в инструкциях Руководства по обновлению

3.9. Переустановка хостов

Переустановите хосты с zVirt Node с Портала администрирования. Процедура включает в себя остановку и перезапуск хоста.

Предварительные условия:

- Если в кластере включена миграция, то виртуальные машины могут автоматически мигрировать на другой хост в кластере. Поэтому переустанавливайте хост, пока уровень его использования относительно невысок.
- Убедитесь, что в кластере достаточно памяти для хостов, чтобы можно было проводить обслуживание. Если в кластере недостаточно памяти, то миграция виртуальных машин зависнет, а затем завершится сбоем. Прежде чем переводить хост на техническое

обслуживание, выключите некоторые или все виртуальные машины, чтобы уменьшить использование ресурсов памяти.

- Перед выполнением переустановки убедитесь, что кластер содержит более одного хоста. Не пытайтесь переустановить все хосты одновременно. Один хост должен оставаться доступным для выполнения задач **Менеджера пула хранения (SPM)**.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)** и выберите хост.
2. Нажмите **[Управление (Management)]** → **[Обслуживание (Maintenance)]** и **[OK]**.
3. Нажмите **[Настройки (Installation)]** → **[Переустановить (Reinstall)]**. Откроется окно **Настройка хоста (Install Host)**.
4. Нажмите **[OK]**, чтобы переустановить хост.

После переустановки хоста и возвращения его статуса к значению **Включен (Up)** ▲ можно перенести виртуальные машины обратно на хост.

> После регистрации хоста с zVirt Node в Менеджере управления и его переустановки Портал администрирования может ошибочно отобразить его статус как **Install Failed**. Нажмите **[Управление (Management)]** → **[Включить (Activate)]**, затем хост перейдет в состояние **Включен (Up)** и будет готов к использованию.

3.10. Просмотр состояния хоста

Кроме обычного Статуса (Status), у хостов есть внешний статус состояния. О внешнем статусе состояния сообщают подключаемые модули или внешние системы, его может задать администратор, и он отображается слева от **Имени (Name)** хоста в виде одного из следующих значков:

- OK: Без значка
- Информация (Info): 
- Предупреждение (Warning): 
- Ошибка (Error): 
- Отказ (Failure): 

Чтобы просмотреть дополнительные сведения о статусе состояния хоста, нажмите его имя, Откроется подробное представление, далее выберите вкладку **События (Events)**.

Статус состояние хоста также можно посмотреть через REST API. Запрос GET на хост будет включать в себя элемент `external_status`, который содержит статус состояния.

Можно установить статус состояния хоста в REST API через набор `events`. Дополнительные сведения см. в разделе Добавление событий в Руководстве по REST API.

3.11. Просмотр устройств хоста

Устройства по каждому хосту можно посмотреть на вкладке **Устройства хоста (Host Devices)** в подробном представлении. Если хост настроен на прямое назначение устройств, то устройства могут быть напрямую подключены к виртуальным машинам для повышения производительности.

Дополнительную информацию о том, как настраивать хосты для прямого назначения устройств см. в разделе Настройка хоста для сквозного доступа PCI.

Дополнительные сведения о подключении устройств хоста к виртуальным машинам см. в разделе Устройства хоста в Руководстве по управлению виртуальными машинами.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Хосты (Hosts)**.
2. Нажмите на имя хоста. Откроется подробное представление.
3. Откройте вкладку **Устройства хоста (Host Devices)**.

На этой вкладке отображаются сведения об устройствах хоста, включая информацию о том, подключено ли устройство к виртуальной машине и используется ли оно ею в данный момент.

3.12. Доступ к Cockpit с Портала администрирования

Cockpit доступен по умолчанию на хостах с zVirt Node. Доступ к веб-интерфейсу Cockpit можно получить, набрав адрес в браузере, или через Портал администрирования.

Порядок действий:

1. На Портале администрирования нажмите **Ресурсы (Compute) > Хосты (Hosts)** и выберите хост.
2. Нажмите **[Консоль хоста (Host Console)]**.

В новом окне браузера откроется страница авторизации Cockpit.

3.13. Настройка устаревшего шифра SPICE

По умолчанию консоли SPICE используют FIPS-совместимое шифрование и строку шифра. По умолчанию используется следующая строка шифра SPICE:
`kECDHE+FIPS:kDHE+FIPS:kRSA+FIPS:!eNULL:!aNULL`

Этой строки обычно бывает достаточно. Однако для виртуальной машины с более старой ОС или более старым клиентом SPICE, где ОС или клиент не поддерживает FIPS-совместимое шифрование, следует использовать более слабую строку шифра. В противном

случае может возникнуть ошибка безопасности подключения, если установить новый кластер или новый хост в существующем кластере и попытаться подключиться к этой виртуальной машине.

Можно изменить строку шифра, используя Ansible-playbook.

Порядок действий::

1. На машине с Менеджером управления перейдите в каталог **/usr/share/ovirt-engine/ansible-runner-service-project/**

   ```
   cd /usr/share/ovirt-engine/ansible-runner-service-project/
   ```

2. В подкаталоге **project/** создайте файл playbook. Например:

   ```
   vim project/change-spice-cipher.yml
   ```

3. Введите в файл следующие данные и сохраните его:

   ```
   - 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
   ```

   где, `<hostname>` - имя хоста или группы хостов, на котором нужно внести изменения.

4. Запустите только что созданный файл с указанием инвентарного файла:

   ```
   ansible-playbook ansible-playbook project/change-spice.yml -i
   inventory/hosts
   ```

Либо можно переконфигурировать хост Ansible-playbook `ovirt-host-deploy`, используя опцию `--extra-vars` с переменной `host_deploy_spice_cipher_string`:

Следующая команда, для сокращения путей, предполагает запуск из каталога **/usr/share/ovirt-engine/ansible-runner-service-project/**

```
ansible-playbook -l _hostname_ \
  --extra-vars host_deploy_spice_cipher_string="DEFAULT:-RC4:-3DES:-DES" \
  -i inventory/hosts \
  project/ovirt-host-deploy.yml
```

3.14. Настройка параметров управления питанием хоста

Параметры устройства управления питанием хоста необходимо настроить для выполнения операций жизненного цикла хоста (остановка, запуск, перезапуск) с Портала администрирования.

Настроить управление питанием хоста необходимо, чтобы использовать высокую доступность хоста и высокую доступность виртуальной машины. Дополнительные сведения об устройствах управления питанием см. в разделе Управление питанием в Техническом справочнике.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)** и выберите хост.
2. Нажмите **[Управление (Management)]** → **[Обслуживание (Maintenance)]**, нажмите **[OK]** для подтверждения.
3. Как только хост перейдет в режим обслуживания, нажмите **[Изменить (Edit)]**.
4. Откройте вкладку **Управление питанием (Power Management)**.
5. Отметьте флажком **Включить управление питанием (Enable Power Management)**, чтобы поля стали активными.
6. Отметьте флажком **Интеграция Kdump (Kdump integration)**, чтобы предотвратить изоляцию хоста, пока создается аварийный дамп ядра.

   > ! После включения или выключения Интеграции Kdump (Kdump integration) на существующем хосте необходимо переустановить хост, чтобы можно было сконфигурировать kdump.

7. При желании можно установить флажок **Выключить политику управления питанием (Disable policy control of power management)**, и тогда питание хоста не будет контролироваться **Политикой планирования (Scheduling Policy)** кластера, к которому относится этот хост.
8. Нажмите **+**, чтобы добавить новое устройство управления питанием. Откроется окно **Изменить fence-агента (Edit fence agent)**.
9. Заполните поля **Имя пользователя (User Name)** и **Пароль (Password)** устройства управления питанием.
10. В выпадающем списке выберите **Тип (Type)** устройства управления питанием.
11. Введите IP-адрес в поле **Адрес (Address)**.
12. Введите номер **Порта (Port)**, который устройство управления питанием использует для связи с хостом.
13. Введите номер **Слота (Slot)**, который используется для идентификации блейда устройства управления питанием.

14. Укажите **Настройки (Options)** устройства управления питанием. Используйте список записей в формате `key=значение`, разделенных запятыми.
    - Если можно использовать и IPv4-адреса, и IPv6-адреса (по умолчанию), то оставьте поле **Настройки (Options)** пустым.
    - Если можно использовать только IPv4-адреса, то введите `inet4_only=1`.
    - Если можно использовать только IPv6-адреса, то введите `inet6_only=1`.
15. Поставьте флажок **Безопасность (Secure)**, чтобы позволить устройству управления питанием безопасно соединяться с хостом.
16. Нажмите **[Тестировать (Test)]**, чтобы убедиться в правильности настроек. После успешной проверки появится сообщение `Test Succeeded, Host Status is: on`.
17. Нажмите **[OK]**, чтобы закрыть окно **Изменить fence-агента (Edit fence agent)**.
18. На вкладке **Управление питанием (Power Management)** можно при желании развернуть блок **Дополнительные параметры (Advanced Parameters)** и кнопками "вверх" ↑ и "вниз" ↓ задать порядок, в котором Менеджер управления будет искать изолирующий прокси в кластере и центре данных хоста.
19. Нажмите **[OK]**.

- zVirt поддерживает только статическую адресацию для IPv6.
- Одновременная адресация (IPv4 и IPv6) не поддерживается.

Выпадающий список в разделе **[Управление (Management)]** → **Управление питанием (Power Management)** теперь стал активным на Портале администрирования.

3.15. Настройка параметров для Менеджера пула хранения хоста

Менеджер пула хранения (SPM) - это управленческая роль, присваиваемая одному из хостов в центре данных для управления доступом к доменам хранения. SPM должен быть постоянно доступен; если хост SPM становится недоступен, роль SPM назначается другому хосту. Поскольку при выполнении роли SPM используется часть доступных ресурсов хоста, важно установить приоритетный порядок для хостов, которые могут выделять эти ресурсы.

Настройка приоритета SPM для хоста изменяет вероятность назначения хосту роли SPM: хост с высоким приоритетом SPM будет назначен на роль SPM раньше, чем хост с низким приоритетом SPM.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)** и выберите хост.
2. Нажмите **[Изменить (Edit)]**.

3. Откройте вкладку **SPM**.
4. С помощью кнопок-переключателей выберите для хоста подходящий приоритет SPM.
5. Нажмите **[OK]**.

3.16. Перенос хостов с ролью hosted engine на другой кластер

Хост с ролью **hosted engine** можно перенести только в центр данных и кластер, в котором работает виртуальная машина с ролью **hosted engine**. Все хосты с ролью **hosted engine** должны находиться в одном и том же центре данных и кластере.

Для переноса хоста с ролью **hosted engine** в центр данных и/или кластер, в котором не выполняется ВМ **HostedEngine** необходимо забрать у хоста роль **hosted engine**, удалив конфигурацию **hosted engine** с хоста.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)** и выберите хост.
2. Нажмите **[Управление (Management)]** → **[Обслуживание (Maintenance)]**. Статус хоста изменится на **[Обслуживание (Maintenance)]** 🔧.
3. Нажмите **[Настройки (Installation)]** → **[Переустановить (Reinstall)]**. Откроется окно **Настройка хоста (Install Host)**.
4. На вкладке **Hosted Engine** в выпадающем меню **Настроить хост для размещения на нём ВМ HostedEngine (Choose hosted engine deployment action)** выберите `UNDEPLOY`.
5. Нажмите **[OK]**.

   Кроме того, можно воспользоваться параметром REST API `undeploy_hosted_engine`.

6. После окончания процедуры переустановки и перехода хоста в состояние **Включен (UP)** снова переведите его в режим обслуживания и нажмите **[Изменить (Edit)]**.
7. Выберите целевой центр данных и кластер.
8. Нажмите **[OK]**.
9. Нажмите **[Управление (Management)]** → **[Включить (Activate)]**.

Дополнительные ресурсы

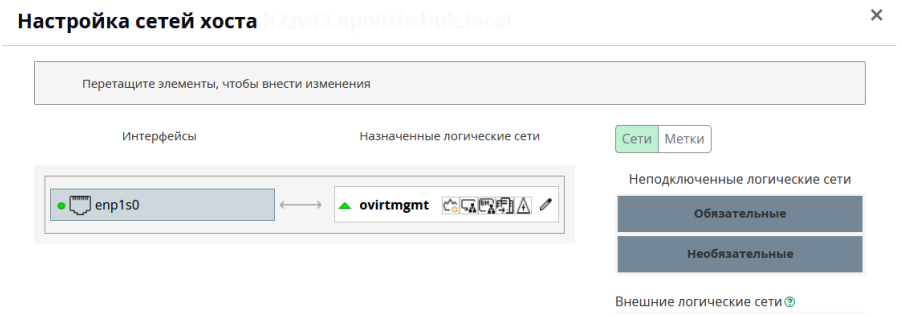
- Перевод хоста в режим обслуживания.
- Активация хоста из режима обслуживания.

3.17. Перенос хостов в кластер с типом коммутатора Open vSwitch

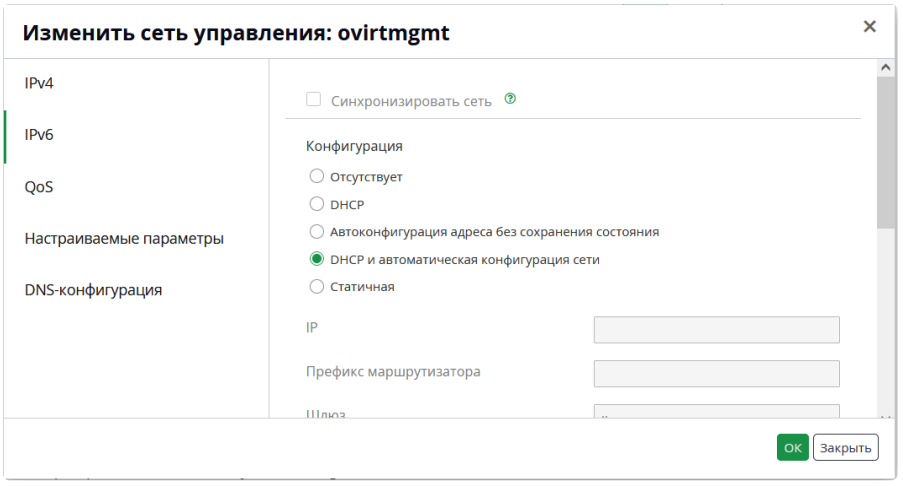
У хоста на момент переноса должна быть только сеть **ovirtmgmt**.

Порядок действий:

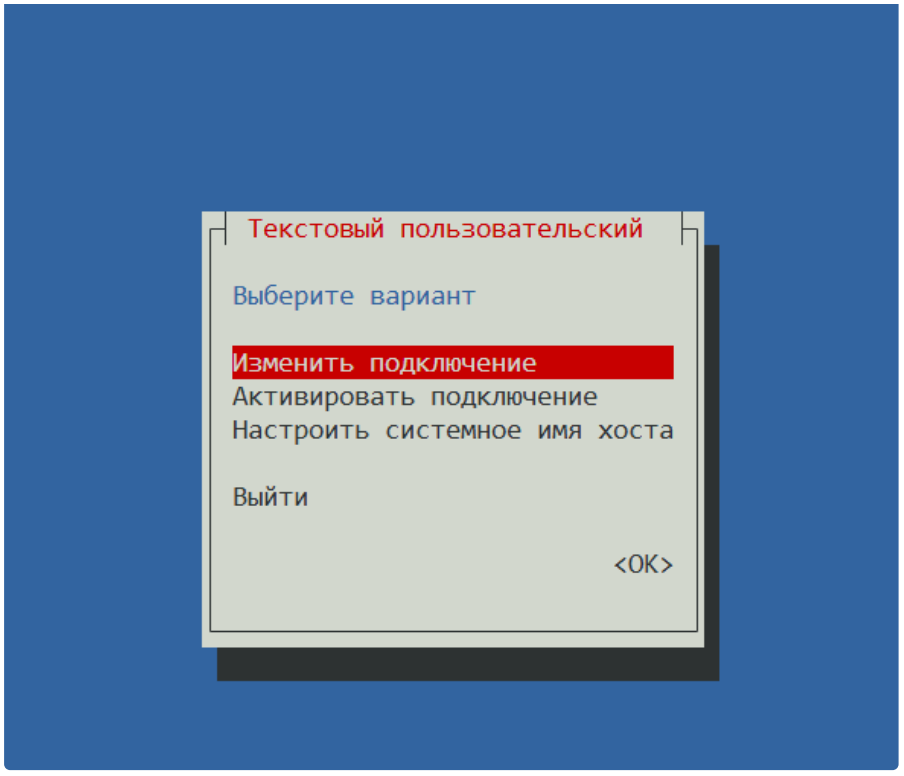
1. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)** и выберите хост.
2. Нажмите **[Управление (Management)]** → **[Обслуживание (Maintenance)]**. Статус хоста изменится на **[Обслуживание (Maintenance)]** 🔧.
3. Перейти в подробное представление хоста. Открыть вкладку **Сетевые интерфейсы** → нажать кнопку **[Настройка сетей хоста]**.
4. В окне **Настройка сетей хоста** отключите все логические сети от интерфейсов хоста кроме сети **ovirtmgmt**.
5. Напротив сети **ovirtmgmt** нажмите кнопку **[✎]**.



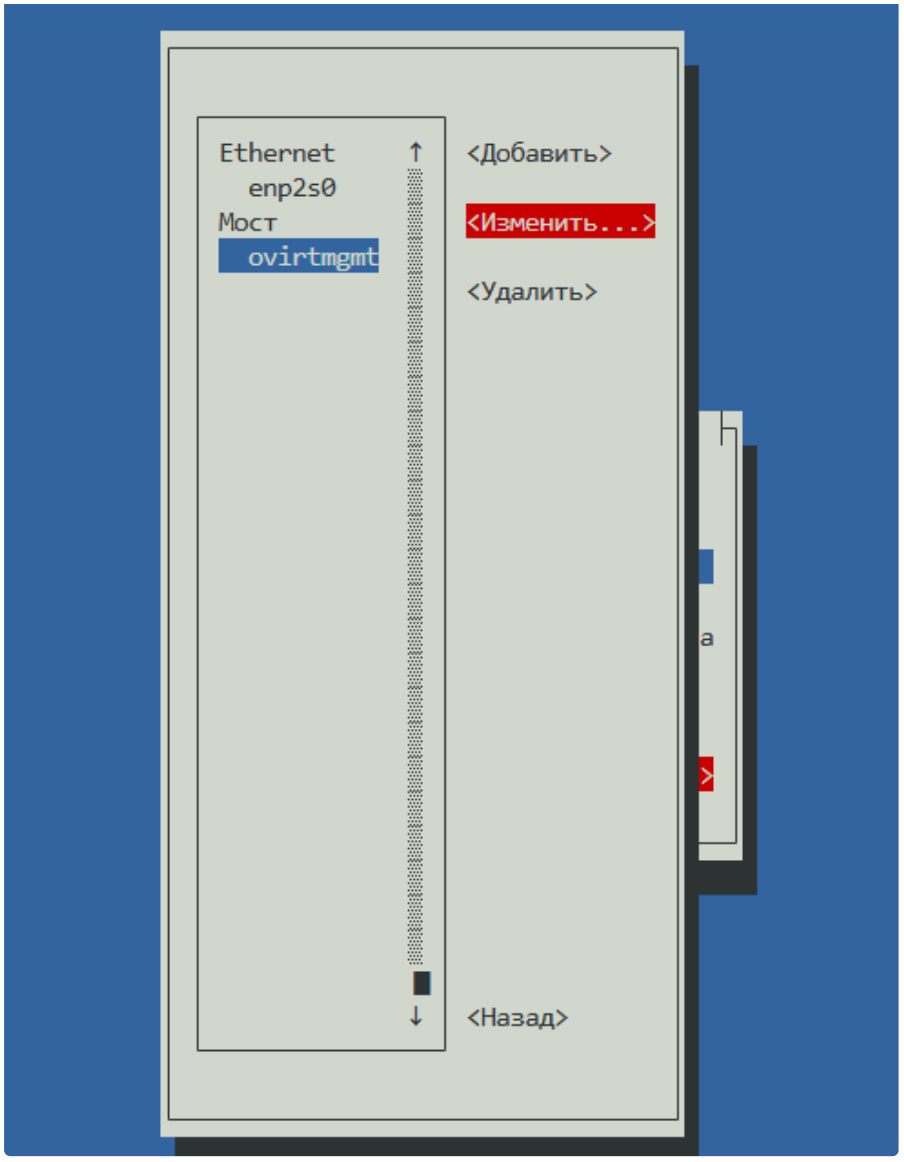
6. В окне **Изменить сеть управления:ovirtmgmt** перейти на вкладку **IPv6** и в параметре **Конфигурация** выбрать значение **DHCP и автоматическая конфигурация сети**.



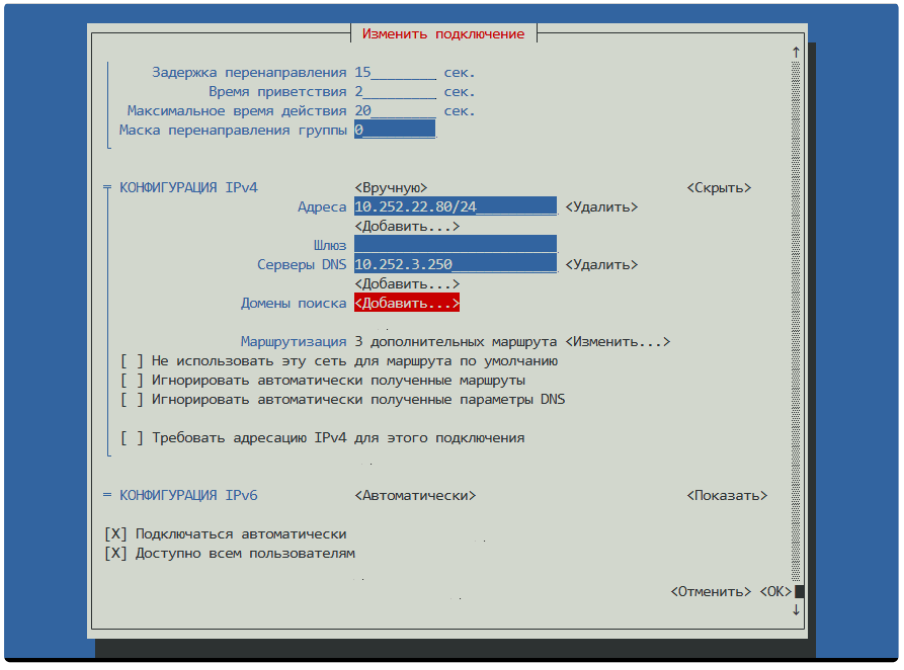
7. Нажмите **[OK]**.
8. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)** и выберите хост.
9. В верхнем меню нажмите на кнопку **Консоль хоста**.
10. В открывшейся вкладке, войдите в систему с помощью своей учётной записи пользователя сервера.
11. В боковом меню перейдите во вкладку **Терминал** и выполните команду `nmtui`.



12. В открывшемся окне перейдите во вкладку **Редактировать соединение(Edit connection)** и выберите сетевое соединение типа **Мост(Bridge)** с именем **ovirtmgmt**. Нажмите **[Изменить]**.



13. В окне настроек соединения удалите значения в параметре **Домены поиска(Domain Search)**.



14. В консоли хоста выполните команды для перезагрузки сетевого интерфейса:

```
nmcli con reload
nmcli con down ovirtmgmt && nmcli con up ovirtmgmt
```

15. Отключитесь от консоли хоста.
16. Вернитесь в **Ресурсы (Compute) > Хосты (Hosts)** и выберите хост.
17. Нажмите **[Изменить]**.Откроется окно **Изменить хост**.
18. Во вкладке **Общее** в параметре **Хост кластера** выберите кластер с типом коммутатора **Open vSwitch**.
19. Нажмите **[OK]**.
20. Вернитесь в **Ресурсы (Compute) > Хосты (Hosts)** и выберите хост.
21. Нажмите **[Настройки (Installation)] → [Переустановить (Reinstall)]**. Откроется окно **Настройка хоста (Install Host)**.
22. Нажмите **[OK]**.

После переустановки хоста и возвращения его статуса к значению **Включен (Up)** 🔺 хост готов к использованию.

3.18. Конфигурация хостов для использования больших страниц

Включение динамического выделения больших страниц

1. Отключите фильтр **Большие страницы (HugePages)** в планировщике: **Управление (Administration) > Настройка (Configure) > Политика планирования (Scheduling Polices)**
2. В разделе `[performance]` в `/etc/vdsm/vdsm.conf` установите следующее:

```
use_dynamic_hugepages = true
```

Конфигурация хостов для статических больших страниц

1. Нажмите **Ресурсы (Compute) > Хосты (Hosts)** и выберите хост.
2. Нажмите **[Изменить (Edit)]**.
3. На вкладке **Ядро** в поле **Командная строка ядра** впишите через пробел необходимые значения параметров (см. таблицу ниже).
4. Нажмите **[OK]**.
5. Переустановите, а затем перезагрузите хост.

Таблица 1. Параметры ядра для больших страниц

Параметр	Описание	Значение по умолчанию

Параметр	Описание	Значение по умолчанию
`hugepages`	Определяет количество больших страниц, настроенных в ядре во время загрузки. В системе NUMA большие страницы, для которых определен этот параметр, делятся поровну между узлами.	0
`hugepagesz`	Определяет размер больших страниц, настроенных в ядре во время загрузки.	Допустимые значения: `2M` и `1G`. Значение по умолчанию: `2M`.
`default_hugepagesz`	Определяет размер по умолчанию больших страниц, настроенных в ядре во время загрузки.	Допустимые значения: `2M` и `1G`. Значение по умолчанию: `2M`.

Сравнение динамических и статических больших страниц

В таблице ниже описаны преимущества и недостатки динамических и статических больших страниц.

Таблица 2. Динамические и статические большие страницы

Параметр	Преимущества	Недостатки	Рекомендации
Динамические большие страницы"	Требуют меньше конфигурирования Меньше памяти тратится впустую (например, свободные большие страницы на хосте ожидают возможных входящих миграций)	Нельзя выделять из-за фрагментации	Используйте большие страницы размером 2 МБ
Статические большие страницы	Предсказуемые результаты	Требуется изменение в командной строке ядра в конфигурации "Изменить хост (Edit Host)" на Портале администрирования.Требуется перезагрузка хоста.	

Применяются следующие ограничения:

- Горячее подключение/отключение памяти выключено
- Ресурсы памяти хоста ограничены

4. Описание настроек и средств управления в окнах "Новый хост" и "Изменить хост"

4.1. Описание общих настроек хоста

В таблице **Общие настройки** содержится информация, которая должна быть указана на вкладке **Общие (General)** окон **Новый хост (New Host)** или **Изменить хост (Edit Host)**.

Таблица 3. Общие настройки

Имя поля	Описание
Хост кластера (Host Cluster)	Кластер и центр данных, к которым относится хост.
Имя (Name)	Имя хоста. Длина этого текстового поля ограничена 40 знаками. Имя должно быть уникальным и представлять собой любую комбинацию латинских букв в верхнем или нижнем регистре, цифр, дефисов или знаков подчеркивания.
Комментарий (Comment)	Поле для добавления обычного текста в читаемой человеком форме - комментариев, относящихся к хосту.
FQDN/IP (Hostname/IP)	IP-адрес или разрешимое имя хоста. Если используется разрешимое имя хоста, то необходимо убедиться, что все адреса, по которым разрешается имя хоста, соответствуют IPv4- и IPv6-адресам, используемым сетью управления хоста.
Порт SSH (SSH port)	Порт для подключения к хосту по протоколу SSH. По умолчанию `22`. Если на хосте изменён стандартный порт, укажите в этом поле актуальное значение.
Пароль (Password)	Пароль root-пользователя хоста. Установите пароль при добавлении хоста. После этого пароль нельзя изменить.
Включить хост после установки (Activate host after install)	Установите этот флажок, чтобы активировать хост после успешной установки. Этот параметр включен по умолчанию и необходим для успешной активации гипервизоров. Можно снять этот флажок, чтобы после успешной установки переключить статус хоста в режим **Обслуживание (Maintenance)**. Это позволит администратору выполнять дополнительные задачи по настройке гипервизоров.

Имя поля	Описание
Перезагрузить хост после установки (Reboot host after install)	Установите этот флажок, чтобы перезагрузить хост после установки. Флажок стоит по умолчанию. Изменение параметров командной строки ядра хоста или изменение типа межсетевого экрана кластера также требует перезагрузки хоста.
Публичный ключ SSH (SSH Public Key)	Скопируйте содержимое текстового поля в файл **/root/.ssh/authorized_hosts** на хосте, чтобы использовать для аутентификации на хосте SSH-ключ Менеджера управления, а не пароль.
Автоматически настроить межсетевой экран хоста (Automatically configure host firewall)	При добавлении нового хоста Менеджер управления может открывать требуемые порты на межсетевом экране хоста. Флажок стоит по умолчанию. Это - **Дополнительный параметр (Advanced Parameter)**.
Публичный ключ SSH хоста (Host ssh public key (PEM))	Можно **получить (fetch)** публичный ключ SSH хоста и сравнить его с ключом, который ожидается от хоста, чтобы убедиться, что они совпадают. Это - **Дополнительный параметр (Advanced Parameter)**.

4.2. Описание настроек управления питанием хоста

В таблице **Настройки Управления питанием** содержится информация, которая должна быть указана на вкладке **Управление питанием (Power Management)** окон **Новый хост (New Host)** или **Изменить хост (Edit Host)**. Управление питанием можно настроить, если у хоста есть поддерживаемая карта управления питанием.

Таблица 4. Настройки Управления питанием

Имя поля	Описание
Включить управление питанием (Enable Power Management)	Включает управление питанием на хосте. Установите этот флажок, чтобы сделать активными остальные поля на вкладке **Управление питанием (Power Management)**.
Интеграция Kdump (Kdump integration)	Предотвращает изоляцию хоста во время создания аварийного дампа ядра, чтобы процесс не прерывался. Если kdump доступен на хосте, но его конфигурация недействительна (служба kdump не может быть запущена), включение **Интеграции Kdump (Kdump integration)** приведет тому, что (повторная) установка хоста завершится ошибкой. В этом случае см. раздел Расширенная конфигурация fence_kdump.

Имя поля	Описание
Выключить политику управления питанием (Disable policy control of power management)	Управление питанием контролируется **Политикой планирования (Scheduling Policy)** кластера хоста. Если управление питанием включено и заданный нижний порог загрузки достигнут, то Менеджер управления отключит питание на хосте и перезапустит его снова, когда потребуется балансировка нагрузки или в кластере не будет достаточно свободных хостов. Поставьте флажок, чтобы отключить контроль со стороны этой политики.
Агенты в последовательном порядке (Agents by Sequential Order)	Выдает список агентов изоляции хоста. Агенты изоляции могут быть последовательными, параллельными или сочетать оба варианта. • Если агенты изоляции используются последовательно, то для остановки или запуска хоста сначала используется первый агент, а если это не срабатывает, то используется второй агент. • Если агенты изоляции используются параллельно, то оба агента изоляции должны отреагировать на команду Stop, чтобы остановить хост. Если один агент отреагирует на команду Start, то хост запустится. По умолчанию агенты изоляции работают последовательно. Чтобы изменить порядок использования агентов изоляции, воспользуйтесь кнопками ↑ и ↓. Чтобы два агента изоляции работали параллельно, выберите один агент изоляции из выпадающего списка **Параллельно с (Concurrent with)** рядом с другим агентом изоляции. К группе параллельных агентов изоляции можно добавить дополнительных агентов изоляции, выбрав группу из выпадающего списка **Параллельно с (Concurrent with)** рядом с дополнительным агентом изоляции.
Добавить агент управления питанием (Add Fence Agent)	Нажмите +, чтобы добавить нового агента изоляции. Откроется окно **Изменить fence-агента (Edit fence agent)**. Более подробная информация о полях этого окна приведена в таблице ниже.
Предпочтения прокси управления питанием (Power Management Proxy Preference)	По умолчанию указано, что Менеджер управления будет искать изолирующий прокси в том же **кластере**, к которому относится хост, а если изолирующий прокси не найден, то Менеджер управления будет искать его в том же **центре данных**. Чтобы изменить порядок использования этих ресурсов, воспользуйтесь кнопками ↑ и ↓. Это поле доступно в разделе **Дополнительные параметры (Advanced Parameters)**.

В таблице ниже приведена информация, необходимая в окне **Изменить fence-агента (Edit fence agent)**

Таблица 5. Настройки окна Изменить fence-агента (Edit fence agent)

Имя поля	Описание

Имя поля	Описание
Адрес (Address)	Адрес для доступа к устройству управления питанием хоста. Укажите разрешимое имя хоста или IP-адрес.
Имя пользователя (User Name)	Учётная запись пользователя, используемая для доступа к устройству управления питанием. Можно задать пользователя на устройстве или использовать пользователя по умолчанию.
Пароль (Password)	Пароль для пользователя, получающего доступ к устройству управления питанием.
Тип (Type)	Тип устройства управления питанием на хосте. Выберите один из следующих вариантов: • `apc` - сетевой переключатель питания APC MasterSwitch. Не подходит для использования с устройствами коммутации питания APC 5.x. • `apc_snmp` - используется с устройствами коммутации питания APC 5.x. • `bladecenter` - IBM Bladecenter Remote Supervisor Adapter. • `cisco_ucs` - Cisco Unified Computing System. • `drac5` - Dell Remote Access Controller для компьютеров Dell. • `drac7` - Dell Remote Access Controller для компьютеров Dell. • `eps` - сетевой переключатель питания ePowerSwitch 8M+. • `hpblade` - HP BladeSystem. • `ilo`, `ilo2`, `ilo3`, `ilo4`, `ilo_ssh` - HP Integrated Lights-Out. • `ipmilan` - Intelligent Platform Management Interface и устройства управления Sun Integrated Lights Out. • `redfish` - спецификация и открытый индустриальный стандарт, который пришёл на смену устаревшему IPMI. Он используется для управления серверным оборудованием посредством RESTful интерфейса. • `rsa` - IBM Remote Supervisor Adapter. • `rsb` - интерфейс управления Fujitsu-Siemens RSB. • `wti` - сетевой переключатель питания WTI. Дополнительные сведения об устройствах управления питанием см. в разделе Управление питанием в Техническом справочнике.
Порт (Port)	Номер порта, который устройство управления питанием использует для связи с хостом.
Слот (Slot)	Номер, который используется для идентификации блейда устройства управления питанием.
Профиль службы (Service Profile)	Имя профиля службы, которое используется для идентификации блейда устройства управления питанием. Это поле появляется вместо поля **Слот (Slot)**, когда тип устройства - `cisco_ucs`.

Имя поля	Описание
Настройки (Options)	Специальные опции устройства управления питанием. Указываются в формате `key=значение`. См. доступные опции в документации на устройство управления питанием хоста.
Безопасность (Secure)	Поставьте этот флажок, чтобы разрешить устройству управления питанием безопасно соединяться с хостом. Для этого можно использовать ssh, ssl или другие протоколы аутентификации в зависимости от агента управления питанием.

4.3. Описание настроек приоритета SPM

В таблице **Настройки SPM** содержится информация, которая должна быть указана на вкладке SPM окон **Новый хост (New Host)** или **Изменить хост (Edit Host)**.

Таблица 6. Настройки SPM

Имя поля	Описание
Приоритет SPM (SPM Priority)	Определяет вероятность того, что хосту будет назначена роль SPM. Возможные варианты выбора приоритета: • `Никогда (Never)` • `Низкий (Low)` • `Нормальный (Normal)` • `Высокий (High)` `Низкий` означает низкую вероятность того, что хосту будет назначена роль SPM, а `Высокий` означает высокую вероятность. По умолчанию выбирается вариант `Нормальный`.

4.4. Описание настроек консоли хоста

В таблице **Настройки консоли (Console settings)** содержится информация, которая должна быть указана на вкладке **Консоль (Console)** окон **Новый хост (New Host)** или **Изменить хост (Edit Host)**.

Таблица 7. Настройки консоли (Console settings)

Имя поля	Описание

Имя поля	Описание
Переопределить отображаемый адрес (Override display address)	Поставьте этот флажок, чтобы переопределить отображаемый адрес хоста. Это полезная опция, если хосты определяются внутренним IP-адресом и располагаются за межсетевым экраном NAT. Когда пользователь подключается к виртуальной машине не из внутренней сети, виртуальная машина возвращает не частный адрес хоста, на котором она работает, а публичный IP-адрес или FQDN (который разрешается во внешней сети в публичный IP-адрес).
Отображаемый адрес (Display address)	Указанный здесь адрес будет использоваться для всех виртуальных машин, работающих на данном хосте. Адрес должен иметь формат FQDN или IP-адреса.
Размещение vGPU(vGPU Placement)	Указывает предпочтительное размещение vGPU: • **Объединённый (Consolidated)**: Выберите этот параметр, если вы предпочитаете использовать больше vGPU на доступных физических картах. • **Разделённый (Separated)**: Выберите этот параметр, если вы предпочитаете запускать каждый vGPU на отдельной физической карте.

4.5. Описание настроек журналирования

В приведенной ниже таблице описаны настройки вкладки **Журналирование (Logging)** в окнах **Новый хост (New Host)** или **Изменить хост (Edit Host)**.

Таблица 8. Настройки журналирования

Поле	Описание/действие
Определить адрес Syslog-сервера	При активации позволяет указать адрес сервера сбора журналов. При активации и указании адреса сервера, переопределяет параметры, заданные на уровне кластера этого хоста. Подробнее см. в разделе Настройка централизованного журналирования.
Использовать TCP-соединение	При активации, для передачи файлов журналов используется протокол TCP вместо UDP. Активация возможна только при активной опции **Определить адрес Syslog-сервера**. При активации, переопределяет параметры, заданные на уровне кластера этого хоста.

Поле	Описание/действие
Включить шифрование	При активации обеспечивает безопасное взаимодействие с сервером Syslog. Активация возможна только при активных опциях **Определить адрес Syslog-сервера** и **Использовать TCP-соединение**. При активации, переопределяет параметры, заданные на уровне кластера этого хоста. Подробнее см. в разделе Настройка использования шифрования.

4.6. Описание настроек ядра

В таблице **Настройки ядра** описана информация, которая должна быть указана на вкладке **Ядро (Kernel)** окон **Новый хост (New Host)** или **Изменить хост (Edit Host)**. Общие загрузочные параметры ядра перечислены в виде флажков, с которыми легко работать.

Если нужно внести более сложные изменения, используйте текстовое поле для ввода текста в свободной форме рядом с **Командной строкой ядра (Kernel command line)**, чтобы добавить любые необходимые параметры. После изменения любых параметров командной строки ядра переустановите хост.

Если хост уже подключен к Менеджеру управления, то перед внесением изменений переведите хост в режим обслуживания. После внесения изменений переустановите хост, чтобы изменения вступили в силу.

Таблица 9. Настройки ядра

Имя поля	Описание
Passthrough устройств хоста и SR-IOV (Hostdev Passthrough & SR-IOV)	Включает флаг IOMMU в ядре, чтобы виртуальная машина могла использовать устройство хоста, как если бы оно было подключено непосредственно к виртуальной машине. Аппаратное и микропрограммное обеспечение хоста также должны поддерживать IOMMU. На оборудовании должны быть включены расширение виртуализации и расширение IOMMU. См. раздел Настройка хоста для сквозного доступа PCI.
Вложенная виртуализация (Nested Virtualization)	Включает флаг vmx или svm, позволяющий виртуальным машинам работать внутри виртуальных машин. Вложенная виртуализация - это предварительная версия технологии, представленная для оценки (Technology Preview): Она предназначена только для оценки и не поддерживается в продуктивных средах. Чтобы использовать эту настройку, установите хук `vdsm-hook-nestedvt` на хосте. Дополнительную информацию см. в разделе Включение вложенной виртуализации.

Имя поля	Описание
Небезопасные прерывания (Unsafe Interrupts)	Если IOMMU включен, но сквозной доступ не работает из-за того, что оборудование не поддерживает переназначение прерываний, можно попробовать установить этот флажок. Имейте в виду, что эту опцию следует включать только в том случае, если виртуальные машины на хосте являются доверенными, так как она потенциально подвергает хост MSI-атакам со стороны виртуальных машин. Выбирайте эту опцию только в качестве обходного решения при использовании несертифицированного оборудования в ознакомительных целях.
Перераспределение PCI (PCI Reallocation)	Если сетевая карта SR-IOV не может назначить виртуальные функции из-за проблем с памятью, попробуйте включить эту опцию. Аппаратное и микропрограммное обеспечение хоста также должны поддерживать переназначение PCI-устройств. Выбирайте эту опцию только в качестве обходного решения при использовании несертифицированного оборудования в ознакомительных целях.
Заблокировать Nouveau (Blacklist Nouveau)	Блокирует драйвер **nouveau**. **Nouveau** - это неофициальный драйвер для графических процессоров NVIDIA, который конфликтует с вендорскими драйверами. Драйвер **nouveau** следует блокировать, когда приоритет отдается вендорским драйверам.
Отключить SMT (SMT Disabled)	Отключает одновременную многопоточность (SMT). Отключение SMT может ослабить уязвимости, такие как L1TF или MDS.
Командная строка ядра (Kernel command line)	Это поле позволяет добавить дополнительные параметры ядра к параметрам по умолчанию.

Если поля загрузочных параметров ядра неактивны, нажмите **[сброс (reset)]**, и они активируются.

4.7. Описание настроек Hosted Engine

В таблице **Настройки Hosted Engine** описана информация, которая должна быть указана на вкладке **Hosted Engine** окон **Новый хост (New Host)** или **Изменить хост (Edit Host)**.

Таблица 10. Настройки Hosted Engine

Имя поля	Описание
Настроить хост для размещения на нём ВМ HostedEngine (Choose hosted engine deployment action)	Доступны три варианта: • `Нет (None)` - никакие действия не требуются. • `Да (Deploy)` - выберите эту опцию, чтобы развернуть хост как узел с ролью hosted engine.

Выбор опции **Настроить хост для размещения на нём ВМ HostedEngine (Choose hosted engine deployment action)** влияет на роль **Hosted Engine** только для новых хостов. Для изменения роли **Hosted Engine** для уже добавленных хостов, используйте вкладку **Hosted Engine** в окне **Настройка хоста**, появляющееся в процессе переустановки хоста.

5. Устойчивость хоста

5.1. Высокая доступность хоста

Менеджер управления использует изоляцию, чтобы поддерживать хосты в кластере в состоянии "responsive" (т.е. когда они реагируют на запросы). Хост, не реагирующий на запросы (**Non Responsive**) - это не то же самое, что неработоспособный (**Non Operational**) хост. Неработоспособные (**Non Operational**) хосты имеют неверную конфигурацию (например, у них отсутствует логическая сеть), но Менеджер управления может связаться с ними. С хостами, не реагирующими на запросы (**Non Responsive**), Менеджер управления связаться не может.

Изоляция позволяет кластеру реагировать на неожиданные отказы хоста и принудительно применять политики энергосбережения, балансировки нагрузки и обеспечения доступности виртуальных машин. Следует настроить параметры изоляции для устройства управления питанием хоста и время от времени проверять их корректность. При выполнении операции изоляции хост, находящийся в состоянии **non-responsive**, перезагружается, и, если он не вернется в активное состояние в течение заданного времени, то останется в состоянии **non-responsive** до ручного вмешательства и устранения неполадок.

Для автоматической проверки параметров изоляции можно настроить параметры engine-config: `PMHealthCheckEnabled` (по умолчанию - `false`) и `PMHealthCheckIntervalInSec` (по умолчанию - `3600` секунд).

Если установить параметр `PMHealthCheckEnabled` в значение `true`, то он будет проверять все агенты хоста с периодичностью, указанной в параметре `PMHealthCheckIntervalInSec`, и выдавать предупреждения при обнаружении проблем. Дополнительную информацию о настройке параметров engine-config см. в разделе Синтаксис команды engine-config.

Операции управления питанием могут выполняться Менеджером управления после его перезагрузки, прокси-хостом или вручную на Портале администрирования. Все виртуальные машины, работающие на хосте, который не реагирует на запросы, останавливаются, а виртуальные машины с признаком высокой доступности запускаются на другом хосте. Для операций управления питанием требуется хотя бы два хоста.

После запуска Менеджера управления он - по истечении времени ожидания (по умолчанию - 5 минут) - автоматически пытается изолировать не реагирующие на запросы хосты, для

которых включено управление питанием. Время ожидания можно настроить, изменив значение параметра engine-config `DisableFenceAtStartupInSec`.

> Параметр engine-config `DisableFenceAtStartupInSec` позволяет избежать ситуации, в которой Менеджер управления попытался бы изолировать хосты, пока они загружаются. А такая ситуация может возникнуть после сбоя в работе центра данных, поскольку хост обычно загружается дольше, чем Менеджер управления.

Хосты могут изолироваться автоматически прокси-хостом (с использованием параметров управления питанием) или вручную (нажатием правой кнопки мыши на хосте и выбором соответствующих опций меню).

> Если на хосте работают виртуальные машины с признаком высокой доступности, необходимо включить и настроить управление питанием.

5.2. Управление питанием с прокси в zVirt

Менеджер управления не связывается с агентами изоляции напрямую. Вместо этого он использует прокси для отправки команд управления питанием на устройство управления питанием хоста. Менеджер управления использует VDSM для выполнения действий над устройством управления питанием, поэтому другой хост в среде используется в качестве изолирующего прокси.

Варианты выбора:

- Любой хост в том же кластере, что и хост, который нужно изолировать.
- Любой хост в том же центре данных, что и хост, который нужно изолировать.

Работоспособный изолирующий прокси-хост имеет статус либо **Включен (UP)** ▲, либо **Обслуживание (Maintenance)** 🔧.

5.3. Установка параметров изоляции на хосте

Параметры изоляции хостов устанавливаются с помощью полей **Управление питанием (Power Management)** окон **Новый хост (New Host)** или **Изменить хост (Edit Host)**. Управление питанием позволяет системе изолировать проблемный хост, используя дополнительный интерфейс, такой как карта удаленного доступа (RAC).

Все операции управления питанием выполняются с использованием прокси-хоста, а не напрямую с помощью Менеджера управления. Для операций управления питанием требуется хотя бы два хоста.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)** и выберите хост.
2. Нажмите **[Изменить (Edit)]**.
3. Откройте вкладку **Управление питанием (Power Management)**.
4. Установите флажок в поле **Включить управление питанием (Enable Power Management)**, чтобы активировать поля.
5. Установите флажок **Интеграция kdump (Kdump integration)**, чтобы предотвратить изолирование хоста, пока создается аварийный дамп ядра.

   После установки или снятия флажка **Интеграция kdump (Kdump integration)** на имеющемся хосте необходимо переустановить хост.

6. При желании можно установить флажок **Выключить политику управления питанием (Disable policy control of power management)**, и тогда питание хоста не будет контролироваться **Политикой планирования (Scheduling Policy)** кластера, к которому относится этот хост.
7. Нажмите **+**, чтобы добавить новое устройство управления питанием. Откроется окно **Изменить fence-агента (Edit fence agent)**.
8. Введите **Адрес (Address)**, **Имя пользователя (User Name)** и **Пароль (Password)** устройства управления питанием.
9. В выпадающем списке выберите **Тип (Type)** устройства управления питанием.
10. Введите номер **Порта (Port)**, который устройство управления питанием использует для связи с хостом.
11. Введите номер **Слота (Slot)**, используемый для идентификации блейда устройства управления питанием.
12. Введите **Настройки (Options)** для устройства управления питанием. Используйте список записей в формате `key=значение`, разделенных запятыми.
13. Поставьте флажок **Безопасность (Secure)**, чтобы позволить устройству управления питанием безопасно соединяться с хостом.
14. Нажмите **[Тестировать (Test)]**, чтобы убедиться в правильности настроек. После успешной проверки появится сообщение `Проверка прошла успешно, Статус хоста: включен (Test Succeeded, Host Status is: on)`.

    Параметры управления питанием (идентификатор пользователя, пароль, опции и т.д.) проверяются Менеджером управления только во время установки, а затем - вручную. Если вы проигнорируете предупреждения о некорректных параметрах или параметры оборудования управления питанием будут изменены без соответствующего изменения в Менеджере управления, то изоляция скорее всего даст сбой в самый нужный момент.

15. Нажмите **[OK]**, чтобы закрыть окно **Изменить fence-агента (Edit fence agent)**.

16. На вкладке **Управление питанием (Power Management)** при желании можно развернуть блок **Дополнительные параметры (Advanced Parameters)** и кнопками ↑ и ↓ задать порядок, в котором Менеджер управления будет искать изолирующий прокси в кластере и центре данных хоста.
17. Нажмите **[OK]**.

Произойдет возврат к списку хостов. Обратите внимание, что восклицательный знак ❗ рядом с именем хоста теперь исчез, а значит, управление питанием настроено успешно.

5.4. Расширенная конфигурация fence_kdump

kdump

Нажмите на имя хоста, чтобы увидеть статус службы kdump на вкладке **Общие (General)** подробного представления:

- **Включено (Enabled)**: служба kdump настроена правильно и работает.
- **Выключено (Disabled)**: служба kdump не работает (в этом случае интеграция kdump не будет работать должным образом).
- **Неизвестно (Unknown)**: так бывает только у хостов с более ранней версией VDSM, которая не сообщает статус kdump.

fence_kdump

Включение **Интеграции kdump (Kdump integration)** на вкладке **Управление питанием (Power Management)** окон **Новый хост (New Host)** или **Изменить хост (Edit Host)** формирует стандартную конфигурацию **fence_kdump**. Если сетевая конфигурация среды проста, а FQDN Менеджера управления разрешимо на всех хостах, то для использования достаточно стандартных настроек **fence_kdump**.

Однако бывает и так, что нужна расширенная конфигурация **fence_kdump**. В средах с более сложной организацией сети, возможно, потребуется вручную изменить конфигурацию Менеджера управления, прослушивающего процесса **fence_kdump** либо того и другого. Например, если FQDN Менеджера управления не разрешимо на всех хостах с включенной опцией **Интеграция kdump (Kdump integration)**, можно указать нужное имя или IP-адрес хоста с помощью `engine-config` :

```
engine-config -s FenceKdumpDestinationAddress=_A.B.C.D_
```

Ниже приведены еще примеры, когда может потребоваться изменение конфигурации:

- Менеджер управления имеет две сетевых карты, одна из которых служит для связи с публичным сегментом, а другая - для приема сообщений **fence_kdump**.

- Нужно запустить прослушивающий процесс **fence_kdump** на другом IP-адресе или порту.
- Нужно задать свой интервал для сообщений **fence_kdump**, чтобы предотвратить возможную потерю пакетов.

Только опытным пользователям рекомендуется задавать свои настройки обнаружения **fence_kdump**, поскольку изменения конфигурации по умолчанию необходимы лишь в случаях более сложной организации сети.

5.5. Конфигурация прослушивающего процесса fence_kdump

Измените конфигурацию прослушивающего процесса **fence_kdump**. Это необходимо только тогда, когда конфигурации по умолчанию недостаточно.

Порядок действий:

1. Создайте новый файл (например, **my-fence-kdump.conf**) в **/etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/**.
2. Введите свои параметры, используя синтаксис `OPTION=значение`, и сохраните файл.

   Отредактированные значения нужно также изменить в engine-config, как указано в таблице Параметры конфигурации kdump в разделе **Настройка fence_kdump в Менеджере управления**.

3. Перезапустите прослушивающий процесс fence_kdump:

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

При необходимости можно изменить следующие параметры:

Таблица 11. Параметры конфигурации прослушивающего процесса fence_kdump**

Переменная	Описание	Значение по умолчанию	Примечание
`LISTENER_ADDRESS`	Определяет IP-адрес, на который будут приниматься сообщения fence_kdump.	`0.0.0.0`	Если значение этого параметра будет изменено, то оно должно соответствовать значению параметра `FenceKdumpDestinationAddress` в engine-config.

Переменная	Описание	Значение по умолчанию	Примечание
`LISTENER_PORT`	Определяет порт, на который будут приниматься сообщения fence_kdump.	`7410`	Если значение этого параметра будет изменено, то оно должно соответствовать значению параметра `FenceKdumpDestinationPort` в engine-config.
`HEARTBEAT_INTERVAL`	Определяет интервал (в секундах) между сигналами работоспособности прослушивающего процесса.	`30`	Если значение этого параметра будет изменено, то оно должно быть как минимум в два раза меньше значения параметра `FenceKdumpListenerTimeout` в engine-config.
`SESSION_SYNC_INTERVAL`	Определяет интервал (в секундах) синхронизации сеансов, во время которых в памяти прослушивающий процесс создает дамп ядра хоста, с базой данных.	`5`	Если значение этого параметра будет изменено, то оно должно быть как минимум в два раза меньше значения параметра `KdumpStartedTimeout` в engine-config.
`REOPEN_DB_CONNECTION_INTERVAL`	Определяет интервал (в секундах) до следующей попытки установить соединение с базой данных, которая до этого была недоступна.	`30`	-

Переменная	Описание	Значение по умолчанию	Примечание
`KDUMP_FINISHED_TIMEOUT`	Определяет максимальное время ожидания (в секундах) после получения последнего сообщения от хостов, создающих дамп ядра, после чего поток kdump хоста помечается как **Завершенный (FINISHED)**.	`60`	Если значение этого параметра будет изменено, то оно должно быть как минимум в два раза больше значения параметра `FenceKdumpMessageInterval` в engine-config.

5.6. Настройка fence_kdump в Менеджере управления

Измените конфигурацию kdump Менеджера управления. Это необходимо только тогда, когда конфигурации по умолчанию недостаточно. Текущие значения параметров конфигурации можно узнать командой:

```
engine-config -g OPTION
```

Порядок действий:

1. Измените конфигурацию kdump командой `engine-config`:

   ```
   engine-config -s OPTION=value
   ```

   Отредактированные значения нужно также изменить в файле конфигурации прослушивающего процесса fence_kdump, как указано в таблице Параметры конфигурации прослушивающего процесса fence_kdump в разделе **Конфигурация прослушивающего процесса fence_kdump**.

2. Перезапустите службу **ovirt-engine**:

   ```
   systemctl restart ovirt-engine.service
   ```

3. Если необходимо, переустановите все хосты с включенной **Интеграцией kdump (Kdump integration)** (см. таблицу ниже).

Следующие параметры можно настроить с помощью engine-config:

Таблица 12. Параметры конфигурации kdump

Переменная	Описание	Значение по умолчанию	Примечание
`FenceKdumpDestinationAddress`	Определяет имя (имена) или IP-адрес (адреса) хоста (хостов), куда будут отправляться сообщения fence_k-dump. Пустое поле означает, что используется FQDN Менеджера управления.	Пустая строка (используется FQDN Менеджера управления)	Если значение этого параметра будет изменено, то оно должно соответствовать значению параметра `LISTENER_ADDRESS` в файле конфигурации прослушивающего процесса fence_kdump, а все хосты с включенной **Интеграцией kdump (Kdump integration)** должны быть переустановлены.
`FenceKdumpDestinationPort`	Определяет порт, на который будут отправляться сообщения fence_kdump.	`7410`	Если значение этого параметра будет изменено, то оно должно соответствовать значению параметра `LISTENER_PORT` в файле конфигурации прослушивающего процесса fence_kdump, а все хосты с включенной **Интеграцией kdump (Kdump integration)** должны быть переустановлены.
`FenceKdumpMessageInterval`	Определяет интервал (в секундах) между сообщениями, которые отправляет fence_kdump.	`5`	Если значение этого параметра будет изменено, то оно должно быть как минимум в два раза меньше значения параметра `KDUMP_FINISHED_TIMEOUT` в файле конфигурации прослушивающего процесса fence_kdump, а все хосты с включенной **Интеграцией kdump (Kdump integration)** должны быть переустановлены.

Переменная	Описание	Значение по умолчанию	Примечание
`FenceKdumpListenerTimeout`	Определяет максимальное время ожидания (в секундах) с момента последнего сигнала работоспособности, в течение которого прослушивающий процесс fence_k-dump считается работоспособным.	`90`	Если значение этого параметра будет изменено, то оно должно быть как минимум в два раза больше значения параметра `HEARTBEAT_INTERVAL` в файле конфигурации прослушивающего процесса fence_kdump.
`KdumpStartedTimeout`	Определяет максимальное время ожидания (в секундах) до получения первого сообщения от хоста, создающего дамп ядра (чтобы определить, что поток kdump хоста запущен).	`30`	Если значение этого параметра будет изменено, то оно должно быть как минимум в два раза больше значения параметра `SESSION_SYNC_INTERVAL` в файле конфигурации прослушивающего процесса fence_kdump и параметра `FenceKdumpMessageInterval`.

5.7. 2.5.5.7. Программная изоляция хостов

Иногда хосты могут перестать реагировать на запросы из-за неожиданно возникшей проблемы, и хотя VDSM не может отвечать на запросы, виртуальные машины, зависящие от VDSM, остаются активными и доступными. В таких случаях перезапуск VDSM-службы возвращает её в рабочее состояние и устраняет проблему.

SSH Soft Fencing - это процесс, когда Менеджер управления пытается по SSH перезапустить VDSM на хостах, не реагирующих на запросы. Если Менеджеру управления не удается перезапустить VDSM по SSH, то задача изоляции возлагается на внешний агент изоляции, если он настроен.

Программная изоляция по SSH работает следующим образом. На хосте должна быть настроена и включена изоляция, и должен существовать допустимый прокси-хост (второй хост в состоянии **UP (включен)** ▲ в центре данных). Когда время ожидания для соединения между Менеджером управления и хостом истекает, происходит следующее:

1. При первом сбое сети статус хоста меняется на **Подключается (connecting)**.

2. Затем Менеджер управления делает три попытки запросить статус у VDSM или ждет в течение интервала, определяемого нагрузкой на хост. Формула определения длительности интервала задается параметрами конфигурации **TimeoutToResetVdsInSeconds** (по умолчанию - 60 секунд) + [**DelayResetPerVmInSeconds** (по умолчанию - 0,5 секунд)] * (**количество работающих виртуальных машин на хосте**) + [**DelayResetForSpmInSeconds** (по умолчанию - 20 секунд)] * **1** (если хост работает как SPM) или **0** (если хост не работает как SPM). Чтобы дать VDSM максимальное время для ответа, Менеджер управления выбирает более продолжительный из двух вышеупомянутых вариантов (три попытки получить статус VDSM или интервал, определяемый вышеприведенной формулой).
3. Если хост не реагирует и после истечения этого интервала, то по SSH производится попытка перезапуска службы **vdsmd**.
4. Если перезапуск службы **vdsmd** не помогает восстановить соединение между хостом и Менеджером управления, то статус хоста меняется на Не отвечает (**Non Responsive**) и, если управление питанием настроено, задача изоляции передается внешнему агенту изоляции.

Программную изоляцию по SSH можно выполнять на хостах, на которых не настроено управление питанием. Она отличается от просто изоляции, которая может выполняться только на хостах, на которых настроено управление питанием.

5.8. Использование функций управления питанием хоста

Когда для хоста управление питанием настроено, можно получить доступ к ряду параметров через интерфейс Портала администрирования. Хотя каждое устройство управления питанием имеет собственные настраиваемые параметры, все они поддерживают базовые параметры запуска, остановки и перезапуска хоста.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)** и выберите хост.
2. Откройте выпадающее меню **[Управление (Management)]** и выберите один из следующих вариантов Управления питанием (Power Management):
   - **[Перезапустить (Restart)]**: этот вариант предусматривает остановку хоста и ожидание изменения статуса хоста на **Выключен (Down)** 🔻. Когда агент убедился, что хост выключен, виртуальные машины с признаком высокой доступности перезапускаются на другом хосте в кластере. Затем агент перезапускает этот хост. Когда хост готов к использованию, его статус отображается как **Включен (Up)** 🔺.
   - **[Запустить (Start)]**: этот вариант предусматривает запуск хоста и его присоединение к кластеру. Когда он готов к использованию, его статус

отображается как **Включен (Up)** ▲.

- **[Остановить (Stop)]**: в этом варианте предусматривается выключение хоста. Прежде чем выбрать этот вариант, убедитесь, что виртуальные машины, работающие на хосте, перенесены на другие хосты в кластере. В противном случае произойдет сбой в работе виртуальных машин, и лишь виртуальные машины с признаком высокой доступности будут перезапущены на другом хосте. Когда хост остановлен, его статус отображается как Неработоспособный (**Non-Operational**).

Если **Управление питанием (Power Management)** не включено, то для перезапуска или остановки хоста выберите его в выпадающем меню **[Управление (Management)]**, затем в категории **Управление SSH (SSH Management)** выберите **[Перезапустить (Restart)]** или **[Остановить (Stop)]**.

Если на хосте определены два агента изоляции, их можно использовать параллельно или последовательно. При параллельном использовании оба агента должны отреагировать на команду `Stop`, чтобы остановить хост. Если один агент отреагирует на команду `Start`, то хост запустится. В случае последовательно работающих агентов для запуска или остановки хоста сначала используется первый агент, а в случае его отказа - второй агент.

3. Нажмите **[OK]**.

5.9. Изолирование хоста, не реагирующего на запросы, вручную

Если хост неожиданно перестает отвечать на запросы, например, из-за аппаратного сбоя, это может существенно повлиять на производительность среды. Если устройство управления питанием отсутствует или неправильно настроено, то можно перезагрузить хост вручную.

Не выбирайте **Подтвердить 'Хост был перезагружен' (Confirm 'Host has been Rebooted')**, если не перезагружали его вручную. Использование этой опции во время работы хоста может вызвать повреждение образа виртуальной машины.

Порядок действий:

1. На Портале администрирования нажмите **Ресурсы (Compute) > Хосты (Hosts)** и убедитесь, что хост имеет статус Не отвечает (**Non Responsive**).
2. Вручную перезагрузите хост. Это может потребовать физического входа в серверную и перезагрузки хоста.
3. На Портале администрирования выберите хост и нажмите **Дополнительные действия (More Actions)** ⋮, затем нажмите
[Подтвердить 'Хост был перезагружен' (Confirm 'Host has been Rebooted')].

4. Установите флажок в поле **Подтвердить операцию (Approve operation)** и нажмите **[OK]**.
5. Если хосты загружаются необычно долго, можно задать параметр `ServerRebootTimeout`, чтобы указать, через сколько секунд следует считать, что хост Не отвечает (**Non Responsive**):

```
engine-config --set ServerRebootTimeout=integer
```

Управление традиционными логическими сетями

1. Задачи, касающиеся логических сетей

1.1. Выполнение задач, касающихся логических сетей

Нажав **Сеть (Network)** > **Сети (Networks)**, пользователь попадает в центр выполнения операций с логическими сетями и поиска логических сетей по свойствам каждой сети или ее ассоциации с другими ресурсами. Кнопки **[Новая (New)]**, **[Изменить (Edit)]** и **[Удалить (Remove)]** позволяют создавать, менять свойства и удалять логические сети в центрах данных.

Нажмите на имя сети и используйте вкладки в подробном представлении для выполнения следующих функций:

- Подключение сетей к кластерам и хостам или отключение сетей от них
- Удаление сетевых интерфейсов из виртуальных машин и шаблонов
- Добавление и удаление разрешений для пользователей на доступ к сетям и управление ими

Эти функции также доступны через каждый отдельный ресурс.

Если вы планируете использовать узлы zVirt для предоставления каких-либо служб, то помните, что службы остановятся, если среда zVirt перестанет работать.

Это относится ко всем службам, однако особое внимание следует уделять рискам, связанным с работой в zVirt следующих сущностей:

- Службы каталогов
- DNS
- Хранилище

1.2. Создание новой логической сети в центре данных или кластере

Создайте логическую сеть и определите ее использование в центре данных или в кластерах центра данных.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Центры данных (Data Centers)** или **Ресурсы (Compute) > Кластеры (Clusters)**.
2. Нажмите на имя центра данных или кластера. Откроется подробное представление.
3. Откройте вкладку **Логические сети (Logical Networks)**.
4. Откройте окно Новая логическая сеть (New Logical Network):
    - В подробном представлении центра данных нажмите **[Новая (New)]**.
    - В подробном представлении кластера нажмите **[Добавить сеть (Add Network)]**.
5. В полях **Имя (Name)**, **Описание (Description)** и **Комментарий (Comment)** укажите значения для логической сети.
6. Дополнительно: Установите флажок **Включить тегирование VLAN (Enable VLAN tagging)**.
7. Дополнительно: Снимите флажок **Сеть ВМ (VM Network)**.
8. Дополнительно: Установите флажок в поле **Создать на внешнем провайдере (Create on external provider)**. Это выключает параметры "Метка сети" и "Сеть ВМ". Подробности см. в статье Внешние провайдеры.
    - Выберите **Внешний провайдер (External Provider)**. Список **Внешних провайдеров (External Provider)** не включает в себя внешних провайдеров, находящихся в режиме "только чтение".
    - Чтобы создать внутреннюю изолированную сеть, выберите **ovirt-provider-ovn** в списке **Внешних провайдеров (External Provider)** и не ставьте флажок в поле **Подключаться к физической сети (Connect to physical network)**.
9. В текстовом поле **Метка сети (Network Label)** введите новую или выберите существующую метку для логической сети.
10. В качестве **Максимального размера передаваемого блока данных (MTU)** либо выберите **Значение по умолчанию (1500) (Default (1500))**, либо выберите **Пользовательский (Custom)** и укажите само это значение.

    После создания сети на внешнем провайдере изменить ее настройки MTU невозможно.

    В случае изменения настроек MTU сети необходимо распространить это изменение на работающие виртуальные машины в сети: Выполните горячее выключение и повторное включение каждой виртуальной сетевой карты виртуальной машины, к которой нужно применить эту настройку MTU, или перезапустите виртуальные машины. В противном случае эти интерфейсы перестанут работать при переносе виртуальной машины на другой хост.
11. В случае выбора **ovirt-provider-ovn** в выпадающем списке **Внешний провайдер (External Provider)** укажите, должна ли сеть использовать Группы безопасности (опция

Безопасность сетевого порта (Network Port Security)). Подробности см. в Разделе Описание общих настроек логической сети.

12. На вкладке **Кластер (Cluster)** выберите кластеры, которым будет назначена эта сеть (опция **Подключить (Attach)**). Можно также указать, будет ли логическая сеть обязательной сетью (опция **Обязательная (Require)**).
13. Если поставлен флажок **Создать на внешнем провайдере (Create on external provider)**, то будет видна вкладка **Подсеть (Subnet)**. На вкладке **Подсеть (Subnet)** выберите **Создать подсеть (Create subnet)**, введите **Имя (Name)**, **CIDR** и адрес **Шлюза (Gateway)** и выберите **Версию IP (IP Version)** для подсети, которую будет предоставлять логическая сеть. Можно также добавить **серверы DNS**, если необходимо.
14. На вкладке **Профили vNIC (vNIC Profiles)** добавьте vNIC-профили к логической сети, если необходимо.
15. Нажмите **[OK]**.

Если вы указали метку для логической сети, то она будет автоматически добавляться ко всем сетевым интерфейсам хоста с этой меткой.

При создании новой логической сети или внесении изменений в существующую логическую сеть, которая используется как сеть отображения, все работающие виртуальные машины, использующие эту сеть, должны быть перезагружены, прежде чем сеть станет доступной или будут применены изменения.

1.3. Изменение логической сети

Логическую сеть нельзя изменить или переместить на другой интерфейс, если она не синхронизирована с конфигурацией сети на хосте. Узнать о том, как синхронизировать сети, можно в разделе Изменение сетевых интерфейсов хоста и назначение логических сетей хостам.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.
3. Откройте вкладку **Логические сети (Logical Networks)** и выберите логическую сеть.
4. Нажмите **[Изменить (Edit)]**.
5. Измените необходимые настройки.

   Не останавливая виртуальные машины, можно изменить имя новой или существующей сети, за исключением сети по умолчанию.

6. Нажмите **[OK]**.

В сети с несколькими хостами обновленные сетевые настройки автоматически применяются ко всем хостам в центре данных, которому назначена сеть. Изменения можно применить только тогда, когда виртуальные машины, использующие сеть, выключены. Логическую сеть, уже настроенную на хосте, невозможно переименовать. Невозможно выключить опцию **Сеть ВМ (VM Network)**, пока работают виртуальные машины или шаблоны, использующие эту сеть.

1.4. Удаление логической сети

Для удаления логической сети нажмите **Сеть (Network) > Сети (Networks)** или **Ресурсы (Compute) > Центры данных (Data Centers)**. Далее показано, как удалить логические сети, ассоциированные с центром данных. Для работающей среды zVirt должна быть хотя бы одна логическая сеть, используемая в качестве сети управления **ovirtmgmt**.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.
3. Откройте вкладку **Логические сети (Logical Networks)**, чтобы вывести список логических сетей центра данных.
4. Выберите логическую сеть и нажмите **[Удалить (Remove)]**.
5. Если сеть предоставлена внешним провайдером, то при желании для удаления логической сети сразу из Менеджера управления и внешнего провайдера поставьте флажок **Удалить сеть(и) внешнего(их) провайдера(ов) (Remove external network(s) from the provider(s) as well)**. Поле для флажка неактивно, если внешний провайдер находится в режиме "только чтение".
6. Нажмите **[OK]**.

Логическая сеть удалена из Менеджера управления и более не доступна.

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

Маршрут по умолчанию, используемый узлами в кластере, проходит через сеть управления (**ovirtmgmt**). Далее показано, как настроить логическую сеть, не являющуюся сетью управления, в качестве маршрута по умолчанию.

Предварительные условия:

- Если используется пользовательское свойство **default_route**, то уберите флажок напротив этого свойства во всех подключенных хостах и далее следуйте описанной ниже процедуре.

Порядок действий:

1. Нажмите **Сеть (Network) > Сети (Networks)**.
2. Нажмите на имя логической сети, не являющейся сетью управления, чтобы открыть сведения о ней и настроить ее в качестве маршрута по умолчанию.
3. Откройте вкладку **Кластеры (Clusters)**.
4. Нажмите **[Управление сетью (Manage Network)]**. Откроется окно **Управление сетью (Manage Network)**.
5. Установите флажок **Маршрут по умолчанию (Default Route)** для соответствующих кластеров.
6. Нажмите **[OK]**.

Когда сети подключены к хосту, выбранная сеть будет задана для хоста в качестве маршрута по умолчанию. Рекомендуется настроить маршрут по умолчанию прежде, чем добавлять хосты в кластер. Если в кластере уже есть хосты, они могут стать несинхронизированными, пока изменения не будут синхронизированы с ними.

Важные ограничения при использовании IPv6

- zVirt поддерживает только статическую адресацию для IPv6.
- Если обе сети используют один шлюз (находятся в одной подсети), то можно передать роль маршрута по умолчанию от **сети управления (ovirtmgmt)** другой логической сети.
- Если хост и Менеджер управления находятся в разных подсетях, то Менеджер управления теряет связь с хостом, поскольку шлюз IPv6 был удален.
- При переносе маршрута по умолчанию в сеть, не являющуюся сетью управления, шлюз IPv6 удаляется из сетевого интерфейса и генерируется предупреждение: `В кластере имя кластера (clustername) у сети ovirtmgmt больше нет роли "маршрут по умолчанию". Шлюз IPv6 удаляется из этой сети`.

1.6. Добавление статического маршрута на хосте

Для добавления статических маршрутов к хостам можно использовать nmstate. Для этого метода необходимо настраивать хосты напрямую, без использования Менеджера управления.

Добавляемые статические маршруты сохраняются до тех пор, пока соответствующий мост маршрутизации, интерфейс или bond-интерфейс существует и имеет IP-адрес. В противном случае система удалит статический маршрут.

Кроме случаев добавления или удаления статического маршрута на хосте, всегда используйте Менеджер управления для настройки сети хоста в кластере.

Пользовательский статический маршрут сохраняется до тех пор, пока его интерфейс или bond-интерфейс существует и имеет IP-адрес. В противном случае он удаляется.

В результате **сети ВМ** ведут себя не так, как **сети без ВМ**:

- В основе сетей ВМ лежит мост (bridge). Перенос сети с одного интерфейса или bond-интерфейса на другой не влияет на маршрут в сети ВМ.
- В основе сетей без ВМ лежит интерфейс. Перенос сети с одного интерфейса или bond-интерфейса на другой удаляет маршрут, связанный с сетью без ВМ.

Предварительные условия:

- Для этой процедуры требуется инструмент `nmstate`

Порядок действий:

1. Подключитесь к хосту, который вы хотите настроить.
2. На хосте создайте файл **static_route.yml** со следующим содержимым (пример):

```yaml
routes:
config:
- destination: 192.168.123.0/24
    next-hop-address: 192.168.178.1
    next-hop-interface: eth1
```

3. Замените приведенные в качестве примера значения реальными значениями для вашей сети.
4. Чтобы маршрутизировать трафик в сеть, добавленную в качестве вторичной, используйте `next-hop-interface` для указания интерфейса или имени сети.
    - Чтобы использовать сеть без ВМ, укажите интерфейс, например, **eth1**.
    - Чтобы использовать сеть ВМ, укажите имя сети, которое является и именем моста, например, **net1**.
5. Выполните команду:

```
$ nmstatectl set static_route.yml
```

Действия по проверке:

- Выполните команду `ip route` со значением параметра приемника, установленным в **static_route.yml**. Должен отобразиться желаемый маршрут. Например, выполните следующую команду:

```
$ ip route | grep 192.168.123.0
```

Дополнительные ресурсы

- Удаление статического маршрута на хосте

1.7. Удаление статического маршрута на хосте

Для удаления статических маршрутов с хостов можно использовать `nmstate`. Для этого метода необходимо настраивать хосты напрямую, без использования Менеджера управления.

Кроме случаев добавления или удаления статического маршрута на хосте, всегда используйте Менеджер управления для настройки сети хоста в кластере.

Пользовательский статический маршрут сохраняется до тех пор, пока его интерфейс или bond-интерфейс существует и имеет IP-адрес. В противном случае он удаляется.

В результате **сети ВМ** ведут себя не так, как **сети без ВМ**:

- В основе сетей ВМ лежит мост (bridge). Перенос сети с одного интерфейса или bond-интерфейса на другой не влияет на маршрут в сети ВМ.
- В основе сетей без ВМ лежит интерфейс. Перенос сети с одного интерфейса или bond-интерфейса на другой удаляет маршрут, связанный с сетью без ВМ.

Предварительные условия:

- Для этой процедуры требуется инструмент `nmstate`

Порядок действий:

1. Подключитесь к хосту, который хотите перенастроить.
2. На хосте измените файл **static_route.yml**.
3. Вставьте строку `state: absent`, как показано в следующем примере.
4. Вставьте значение `next-hop-interface` между квадратными скобками конструкции `interfaces: []`. Результат должен быть похож на показанный в следующем примере.

```
routes:
config:
- destination: 192.168.123.0/24
    next-hop-address: 192.168.178.
    next-hop-interface: eth1
    state: absent
interfaces: [{"name": eth1}]
```

5. Выполните команду:

```
$ nmstatectl set static_route.yml
```

Действия по проверке:

- Выполните команду `ip route` со значением параметра приемника, установленным в **static_route.yml**. Желаемый маршрут больше не должен отображаться. Например, выполните следующую команду:

  ```
  $ ip route | grep 192.168.123.0
  ```

  Дополнительные ресурсы

- Добавление статического маршрута на хосте.

1.8. Просмотр или изменение шлюза для логической сети

Администратор может задать шлюз вместе с IP-адресом и маской подсети для логической сети. Это необходимо, когда на хосте существует несколько сетей и трафик должен маршрутизироваться через указанную сеть, а не через шлюз по умолчанию.

Если на хосте существует несколько сетей, а шлюзы не заданы, то обратный трафик будет маршрутизироваться через шлюз по умолчанию и может не достичь приемника. В результате пользователи не смогут проверить хост ping-запросом.

Менеджер автоматически управляет несколькими шлюзами при каждом включении или отключении интерфейса.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Хосты (Hosts)**.
2. Нажмите на имя хоста. Откроется подробное представление.
3. Откройте вкладку **Сетевые интерфейсы (Network Interfaces)**, чтобы вывести список сетевых интерфейсов, подключенных к хосту, и их конфигурации.
4. Нажмите **[Настройка сетей хоста (Setup Host Networks)]**.
5. Наведите указатель мыши на назначенную логическую сеть и нажмите на значок карандаша . Откроется окно **Изменить сеть управления (Edit Management Network)**.

В окне **Изменить сеть управления (Edit Management Network)** отображается имя сети, способ конфигурации (boot protocol), IP-адрес, маска подсети и адреса шлюзов. Сведения об адресах можно изменить вручную, выбрав **Статичную (Static)** конфигурацию.

1.9. Описание общих настроек логической сети

В приведенной ниже таблице описаны настройки вкладки **Общие (General)** окон **Новая логическая сеть (New Logical Network)** и **Изменить логическую сеть (Edit Logical Network)**.

Таблица 1. Настройки окон "Новая логическая сеть (New Logical Network)" и "Изменить логическую сеть (Edit Logical Network)"

Имя поля	Описание
Имя (Name)	Имя логической сети. В этом текстовом поле должно быть уникальное имя, представляющее собой любую комбинацию латинских букв в верхнем и нижнем регистре, цифр, дефисов и знаков подчеркивания. Имейте в виду, что хотя имя логической сети может быть длиннее 15 знаков и может содержать знаки, отличные от ASCII, идентификатор на хосте (vdsm_name) будет отличаться от заданного имени. Указания по отображению сопоставления этих имен см. в разделе Инструмент сопоставления VDSM с именем сети.
Описание (Description)	Описание логической сети. Это текстовое поле имеет ограничение по длине (40 знаков).
Комментарий (Comment)	Поле для добавления обычного текста в читаемой человеком форме - комментариев, относящихся к логической сети.
Создать на внешнем провайдере (Create on external provider)	Позволяет создать логическую сеть к экземпляру OpenStack Networking, добавленному в Менеджер управления в качестве внешнего провайдера. **Внешний провайдер (External Provider)** - позволяет выбрать внешнего провайдера, на котором будет создана логическая сеть.
Включить тегирование VLAN (Enable VLAN tagging)	Тегирование VLAN - это функция безопасности, которая присваивает специальную характеристику всему сетевому трафику, проходящему через логическую сеть. Трафик с тегированием VLAN не может быть считан интерфейсами, которые не обладают этой же характеристикой. Используя VLAN в логических сетях, также можно ассоциировать один сетевой интерфейс с несколькими логическим сетям с различным тегированием VLAN. Если тегирование VLAN включено, то укажите числовое значение в поле ввода текста.
Сеть ВМ (VM Network)	Выберите эту опцию, если эту сеть используют только виртуальные машины. Если сеть используется для трафика, который не охватывает виртуальные машины (например, для связи с хранилищами), то не устанавливайте этот флажок.
Изоляция портов (Port Isolation)	Если этот флажок установлен, виртуальные машины на одном хосте не могут обмениваться данными и видеть друг друга в этой логической сети. Чтобы эта опция работала на разных гипервизорах, на коммутаторах должна быть настроена PVLAN/изоляция портов на соответствующих портах/VLAN, подключенных к гипервизорам, и не должны использоваться какие-либо настройки возврата кадров (например, Hairpin NAT).

Имя поля	Описание
Максимальный размер передаваемого блока данных (MTU)	Выберите либо значение **По умолчанию (Default)**, тем самым установив максимальный размер передаваемого блока данных (MTU) в значение, указанное в круглых скобках (), либо **Пользовательский (Custom)** MTU и задайте его для логической сети. Это можно использовать, чтобы привести MTU, поддерживаемый вашей новой логической сетью, в соответствие MTU, поддерживаемому оборудованием, с которым взаимодействует эта сеть. Если выбрано значение **Пользовательский (Custom)**, то укажите числовое значение в поле ввода текста. В случае изменения настроек MTU сети необходимо распространить это изменение на работающие виртуальные машины в сети: Выполните горячее выключение и повторное включение каждой виртуальной сетевой карты виртуальной машины, к которой нужно применить эту настройку MTU, или перезапустите виртуальные машины. В противном случае эти интерфейсы перестанут работать при переносе виртуальной машины на другой хост.
Метка сети (Network Label)	Позволяет задать для сети новую метку или выбрать одну из существующих меток, уже прикрепленных к сетевым интерфейсам хоста. Если выбирается существующая метка, логическая сеть будет автоматически назначена всем сетевым интерфейсам хоста с этой меткой.
Безопасность сетевого порта (Network Port Security)	Позволяет назначать группы безопасности портам в этой логической сети. **Выключен (Disabled)** отключает функцию групп безопасности. **Включен (Enabled)** включает эту функцию. Когда порт создается и подключается к этой сети, функция безопасности будет включена. Это означает, что доступ к виртуальным машинам и от них будет зависеть от групп безопасности, которые в настоящее время предоставляются. **Неопределён (Undefined)** разрешает портам наследовать поведение из файла конфигурации, заданного для всех сетей. По умолчанию этот файл выключает группы безопасности. Подробности см. в разделе Назначение групп безопасности логическим сетям и портам.

1.10. Описание настроек кластера логической сети

В приведенной ниже таблице описаны настройки вкладки **Кластер (Cluster)** окна **Новая логическая сеть (New Logical Network)**.

Таблица 2. Настройки в окне "Новая логическая сеть (New Logical Network)"

Имя поля	Описание

Имя поля	Описание
Управление сетями кластера (Attach/Detach Network to/from Cluster(s))	Позволяет подключать логическую сеть к кластерам или отключать ее от кластеров в центре данных и указывать, будет ли логическая сеть обязательной сетью для отдельных кластеров. **Имя (Name)** - имя кластера, к которому будут применяться настройки. Это неизменяемое значение. **Выбрать все (Attach All)** - позволяет подключить логическую сеть ко всем кластерам в центре данных или отключить ее от них. Либо поставьте или снимите флажок **Подключить (Attach)** рядом с именем каждого кластера, чтобы подключить логическую сеть к данному кластеру или отключить ее от него. **Выбрать все (Required All)** - позволяет указать, является ли логическая сеть обязательной сетью на всех кластерах. Либо поставьте или снимите флажок **Обязательная (Required)** рядом с именем каждого кластера, чтобы указать, является ли логическая сеть обязательной сетью для конкретного кластера.

1.11. Описание настроек vNIC-профилей логической сети

В приведенной ниже таблице описаны настройки вкладки профили vNIC (vNIC Profiles) окна **Новая логическая сеть (New Logical Network)**.

Таблица 3. Настройки окна Новая логическая сеть (New Logical Network)

Имя поля	Описание
Профили vNIC (vNIC Profiles)	Эта опция позволяет задать один или несколько профилей vNIC для логической сети. Можно добавить/удалить профиль vNIC для/из логической сети, нажав кнопку + или — рядом с профилем. Первое поле предназначено для указания имени профиля vNIC. **Публичный (Public)** - позволяет указать, будет ли профиль доступен для всех пользователей. **QoS** - позволяет указать профиль QoS сети для профиля vNIC.

1.12. Назначение определённого типа трафика для логической сети

Тип трафика для логической сети необходимо указать в целях оптимизации потока сетевого трафика.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Кластеры (Clusters)**.
2. Нажмите имя кластера. Откроется подробное представление.
3. Выберите вкладку **Логические сети (Logical Networks)**.
4. Нажмите **[Управление сетями (Manage Networks)]**.
5. Установите необходимые флажки и кнопки-переключатели.
6. Нажмите **[OK]**.

Логические сети от внешних поставщиков должны использоваться как сети виртуальных машин; им нельзя назначать специальные роли кластера, такие как отображение или миграция.

1.13. Описание настроек в окне "Управление сетями (Manage Networks)"

В приведенной ниже таблице описаны настройки окна **Управление сетями (Manage Networks)**.

Таблица 4. Настройки окна "Управление сетями (Manage Networks)"

Поле	Описание/действие
Подключить (Assign)	Назначает логическую сеть всем хостам в кластере.
Обязательная (Require)	Сеть, отмеченная как "Обязательная (Require)", должна сохранять работоспособность для надлежащего функционирования ассоциированных с нею хостов. Если обязательная сеть перестаёт функционировать, все ассоциированные с нею хосты становятся неработоспособными.
Сеть ВМ (VM Network)	Логическая сеть, отмеченная как "Сеть ВМ (VM Network)", обслуживает сетевой трафик, относящийся к сети виртуальных машин.
Сеть отображения (Display Network)	Логическая сеть, обозначенная как "Сеть отображения (Display Network)", обслуживает сетевой трафик, относящийся к SPICE и VNC.
Сеть миграции (Migration Network)	Логическая сеть, обозначенная как "Сеть миграции (Migration Network)", обслуживает трафик миграции виртуальных машин и хранилищ. Если в этой сети произойдет отключение питания, то вместо нее будет использоваться сеть управления (**ovirtmgmt**).

1.14. Настройка виртуальных функций на сетевой карте

Это один из вопросов на тему, как настроить и сконфигурировать SR-IOV в zVirt. Дополнительные сведения см. в разделе Установка и настройка SR-IOV.

Виртуализация ввода-вывода (технология SR-IOV) позволяет с помощью физических и виртуальных функций использовать каждое оконечное устройство PCIe как несколько отдельных устройств. PCIe-карта может иметь от одной до восьми физических функций. Каждая физическая функция может иметь множество виртуальных функций. Количество возможных виртуальных функций зависит от конкретного типа PCIe-устройства.

Для настройки сетевых карт с поддержкой технологии SR-IOV используется Менеджер управления, в котором можно настроить количество виртуальных функций на каждой сетевой карте.

Виртуальные функции можно настроить так же, как и отдельную сетевую карту, в том числе:

- Назначить одну или несколько логических сетей для виртуальной функции;
- Создать бондинг интерфейсов с виртуальными функциями;
- Назначить виртуальные сетевые карты (vNIC) виртуальным функциям для сквозного доступа к устройствам.

По умолчанию у всех виртуальных сетей есть доступ к виртуальным функциям. Можно выключить эту возможность по умолчанию и указать, у каких сетей будет доступ к виртуальной функции.

Предварительное условие:

- Для того чтобы vNIC была подключена к виртуальной функции, ее свойство сквозного доступа должно быть включено. Подробнее см. в разделе Включение сквозного доступа на профиле vNIC.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Хосты (Hosts)**.
2. Нажмите на имя хоста с поддержкой технологии SR-IOV. Откроется подробное представление.
3. Откройте вкладку **Сетевые интерфейсы (Network Interfaces)**.
4. Выберите **[Настройка сетей хоста (Setup Host Networks)]**.
5. Выберите сетевую карту с поддержкой SR-IOV, отмеченную знаком 

, и нажмите на значок карандаша .
6. Дополнительно: Чтобы изменить количество виртуальных функций, нажмите кнопку с выпадающим списком **Настройка количества виртуальных функций (Number of VFs setting)** и измените значение в текстовом поле **Количество виртуальных функций (Number of VFs)**.

Если изменить количество виртуальных функций, то будут удалены все предыдущие виртуальные функции, существовавшие в интерфейсе сети до создания новых виртуальных функций. В том числе все виртуальные функции, которые были напрямую подключены к виртуальным машинам.

7. Дополнительно: Чтобы установить ограничение для виртуальных сетей на доступ к виртуальным функциям, выберите **Особые сети (Specific networks)**.
    - Выберите те сети, которым будет разрешен доступ к виртуальным функциям, или с помощью **Меток (Labels)** выберите сети с соответствующими сетевыми метками.
8. Нажмите **[OK]**.
9. В окне **Настройка сетей хоста (Setup Host Networks)** нажмите **[OK]**.

2. Виртуальные сетевые карты (vNICs)

2.1. Обзор профилей vNIC

Профиль виртуальной сетевой карты (профиль vNIC) - это набор параметров, которые можно применить к отдельным виртуальным сетевым картам в Менеджере управления. Профиль vNIC позволяет применять профили QoS сети к vNIC, включать или выключать зеркалирование портов, добавлять или удалять пользовательские свойства. Профиль vNIC также дает дополнительную гибкость управления, поскольку разрешение на использование (потребление) этих профилей может быть предоставлено определенным пользователям. Таким образом, можно регулировать качество обслуживания (QoS) различных пользователей в определенной сети.

2.2. Создание или изменение профилей vNIC

Создание или изменение профилей vNIC нужно, чтобы регулировать полосу пропускания сети виртуальных машин.

Если включить или отключить зеркалирование портов, то все виртуальные машины, использующие ассоциированный профиль, должны находиться в выключенном состоянии до внесения в них изменений.

Порядок действий:

1. Нажмите **Сеть (Network)** > **Сети (Networks)**.
2. Нажмите на имя логической сети. Откроется подробное представление.
3. Выберите вкладку **Профили vNIC (vNIC Profiles)**.
4. Нажмите **[Новый (New)]** или **[Изменить (Edit)]**.

5. Введите имя и описание профиля в поля **Имя (Name)** и **Описание (Description)**.
6. Выберите подходящую политику QoS из списка **QoS**.
7. Выберите **Сетевой фильтр (Network Filter)** из выпадающего списка, чтобы настроить трафик сетевых пакетов к виртуальным машинам и от них.
8. Установите флажок в поле **Passthrough**, чтобы включить сквозной доступ на vNIC и разрешить прямое назначение устройства виртуальной функции. Если включить свойство сквозного доступа, то по причине несовместимости будут выключены политика QoS, сетевая фильтрация и зеркалирование портов. Дополнительные сведения о сквозном доступе см. в разделе Включение сквозного доступа на профиле vNIC.
9. Если выбран **Сквозной доступ (Passthrough)**, то при желании можно снять флажок **Мигрируемый (Migratable)**, чтобы выключить возможность миграции для vNIC, которые используют этот профиль. Если оставляете флажок в этом поле, то см. Настройка виртуальных машин с виртуальными сетевыми картами с включенным SR-IOV в Руководстве по управлению виртуальными машинами.
10. Используйте флажки в полях **Зеркалирование портов (Port Mirroring)** и **Разрешить всем пользователям доступ к этому профилю (Allow all users to use this Profile)**, чтобы включать и выключать эти опции.
11. Выберите пользовательское свойство из списка **пользовательских свойств**, где по умолчанию отображается `Выберите ключ… (Please select a key…)`. Нажимая кнопки + и —, добавляйте или удаляйте пользовательские свойства.
12. Нажмите **[OK]**.

Применение этого профиля к сетевым картам виртуальных машин регулирует их полосу пропускания сети. После изменения профиля vNIC необходимо либо перезапустить виртуальную машину, либо, если гостевая операционная система это позволяет, выполнить горячее выключение и затем горячее включение карты vNIC.

2.3. Описание настроек в окне "Профиль интерфейса (Interface Profile)"

Таблица 5. Окно "Профиль интерфейса (Interface Profile)"

Имя поля	Описание
Сеть (Network)	Выпадающий список доступных сетей, к которым можно применить профиль vNIC.
Имя (Name)	Имя профиля vNIC. Это должно быть уникальное имя длинной от 1 до 50 знаков, представляющее собой любую комбинацию латинских букв в верхнем и нижнем регистре, цифр, дефисов и знаков подчеркивания.

Имя поля	Описание
Описание (Description)	Описание профиля vNIC. Это поле является рекомендованным, но необязательным.
QoS	Выпадающий список доступных политик QoS сети для применения к профилю vNIC. Политики QoS регулируют входящий и исходящий сетевой трафик vNIC.
Сетевой фильтр (Network Filter)	Выпадающий список доступных сетевых фильтров, который можно применить к профилю vNIC. Сетевые фильтры повышают безопасность сети за счет фильтрации типов пакетов, которые могут быть отправлены на виртуальные машины и от них. По умолчанию установлен фильтр vdsm-no-mac-spoofing, который представляет собой комбинацию no-mac-spoofing и no-arp-mac-spoofing. Используйте параметр `Нет сетевого фильтра (No Network Filter)` для сетей VLAN и bond-интерфейсов виртуальных машин. Отключение сетевого фильтра на доверенных виртуальных машинах может повысить производительность.
Passthrough	Отметить флажком, чтобы включить свойство сквозного доступа. Сквозной доступ позволяет карте vNIC напрямую подключаться к виртуальной функции сетевой карты хоста. Свойство сквозного доступа нельзя изменять, если профиль vNIC подключен к виртуальной машине. При включенном сквозном доступе политика QoS, сетевые фильтры и зеркалирование портов в профиле vNIC выключены.
Мигрируемый (Migratable)	Флажок в этом поле определяет, можно ли переносить карты vNIC, использующие этот профиль, или нет. Миграция включена по умолчанию для обычных профилей vNIC: флажок в поле стоит, и снять его нельзя. Когда стоит флажок в поле **Passthrough**, свойство **Мигрируемый (Migratable)** становится доступным, и при необходимости флажок можно снять, чтобы выключить возможность миграции карт vNIC сквозного доступа.
Профиль отказоустойчивости vNIC (Failover)	Выпадающий список для выбора доступных профилей vNIC, действующих в качестве устройств аварийного переключения. Доступно только, когда стоят флажки в полях **Passthrough** и **Мигрируемый (Migratable)**.
Зеркалирование портов (Port Mirroring)	Поставить/снять флажок, чтобы включить/отключить зеркалирование портов. При зеркалировании портов сетевой трафик третьего уровня копируется с логической сети на виртуальный интерфейс виртуальной машины. По умолчанию флажок в этом поле снят. Дополнительные сведения см. в разделе Зеркалирование портов (Port Mirroring) в Техническом справочнике.
Пользовательские свойства (Custom Properties)	Выпадающий список, в котором можно выбрать доступные пользовательские свойства, которые можно применить к профилю vNIC. Нажимая кнопки + и —, добавляйте или удаляйте соответствующие свойства.

Имя поля	Описание
Разрешить всем пользователям доступ к этому профилю (Allow all users to use this Profile)	Отметить флажком, чтобы сделать профиль доступным для всех пользователей. По умолчанию флажок стоит.

2.3.1. Описание сетевых фильтров

Целью сетевой фильтрации является предоставление администраторам виртуализированной системы возможности настраивать и применять правила фильтрации сетевого трафика на виртуальных машинах, а также управлять параметрами сетевого трафика, который виртуальным машинам разрешено отправлять или получать. Правила фильтрации сетевого трафика применяются на хосте при запуске виртуальной машины. Поскольку правила фильтрации невозможно обойти изнутри виртуальной машины, это делает их обязательными с точки зрения пользователя виртуальной машины.

Ниже приведен список некоторых базовых сетевых фильтров, которые доступны при настройке профилей vNic.

Таблица 6. Базовые сетевые фильтры

Имя	Описание
vdsm-no-mac-spoofing	Представляет собой комбинацию no-mac-spoofing и no-arp-mac-spoofing
allow-arp	Разрешает ARP-трафик в обоих направлениях
allow-dhcp	Разрешает виртуальной машине запрашивать IP-адрес через DHCP (с любого DHCP-сервера).
allow-in-coming-ipv4	Разрешает входящий трафик IPv4
allow-ipv4	Разрешает трафик IPv4 в обоих направлениях
clean-traffic	Предотвращает подмену MAC, IP и ARP. Этот фильтр ссылается на несколько других фильтров.
no-arp-spoofing	Предотвращает подмену ARP-трафика виртуальной машиной; этот фильтр разрешает только сообщения ARP-запроса и ARP-ответа и обеспечивает, чтобы эти пакеты содержали MAC- и IP-адреса виртуальной машины.
no-ip-multicast	Запрещает виртуальной машине отправлять многоадресные IP-пакеты.
no-ip-spoofing	Запрещает виртуальной машине отправлять пакеты IPv4 с исходящим IP-адресом, отличным от адреса в пакете.

Имя	Описание
no-mac-broadcast	Запрещает виртуальной машине отправлять широковещательные кадры (mac-адрес назначения `ff:ff:ff:ff:ff:ff`)
no-mac-spoofing	Предотвращает подмену mac-адреса виртуальной машиной

Следует отметить, что в таблице представлены не все доступные фильтры. В большинстве случаев фильтр представляет собой комбинацию других фильтров что обеспечивает необходимый набор правил фильтрации сетевого трафика.

Например, фильтр clean-traffic может быть объединен с фильтром no-ip-multicast для предотвращения отправки виртуальными машинами многоадресного IP-трафика в дополнение к предотвращению подмены пакетов.

Для получения подробной информации о соответствующем фильтре изучите XML-файл этого фильтра. Это можно сделать на любом гипервизоре в среде zVirt.

Пример 1. Получение информации о фильтре

```
cat /etc/libvirt/nwfilter/no-arp-ip-spoofing.xml

...

<filter name='no-arp-ip-spoofing' chain='arp-ip' priority='-510'>
  <uuid>ced3eb5b-6e82-4120-a6d3-4fcff18577cd</uuid>
  <rule action='return' direction='out' priority='400'>
    <arp arpsrcipaddr='$IP'/>
  </rule>
  <rule action='drop' direction='out' priority='1000'/>
</filter>
```

Дополнительные ресурсы

- Сетевые фильтры

2.4. Включение сквозного доступа на профиле vNIC

Это один из вопросов на тему, как настроить и сконфигурировать SR-IOV в zVirt. Дополнительные сведения см. в разделе Установка и настройка SR-IOV.

Свойство сквозного доступа на профиле vNIC позволяет карте vNIC напрямую подключаться к виртуальной функции сетевой карты с включенной технологией SR-IOV. В

этом случае карта vNIC будет обходить программную виртуализацию сети и подключаться непосредственно к виртуальной функции для прямого назначения устройства.

Если профиль vNIC уже подключен к vNIC-карте, то включить свойство сквозного доступа нельзя; чтобы обойти это ограничение, создается новый профиль. Если в профиле vNIC включено свойство сквозного доступа, то политику QoS, сетевые фильтры и зеркалирование портов нельзя включить в том же профиле.

Порядок действий:

1. Нажмите **Сеть (Network)** > **Сети (Networks)**.
2. Выберите имя логической сети. Откроется подробное представление.
3. Выберите вкладку **Профили vNIC (vNIC Profiles)**, на которой отобразится список всех профилей vNIC для этой логической сети.
4. Нажмите **[Новый (New)]**.
5. Введите имя и описание профиля в поля **Имя (Name)** и **Описание (Description)**.
6. Поставьте флажок в поле **Passthrough**.
7. При желании можно снять флажок **Мигрируемый (Migratable)**, чтобы выключить возможность миграции для vNIC, которые используют этот профиль. Если флажок в этом поле остается, то см. Настройка виртуальных машин с виртуальными сетевыми картами с включенным SR-IOV в Руководстве по управлению виртуальными машинами.
8. При необходимости выберите пользовательское свойство из списка **пользовательских свойств**, где по умолчанию отображается `Выберите ключ… (Please select a key…)`. Нажимая кнопки **+** и **—**, добавляйте или удаляйте пользовательские свойства.
9. Нажмите **[OK]**.

Теперь возможность сквозного доступа активирована в профиле vNIC. Чтобы использовать этот профиль для прямого подключения виртуальной машины к сетевой карте или виртуальной функции PCI, подключите логическую сеть к сетевой карте и создайте новую виртуальную сетевую карту Сквозного доступа PCI (PCI Passthrough) на нужной виртуальной машине, которая использует профиль vNIC со сквозным доступом. Более подробную информацию об этих процедурах см. в разделе Изменение сетевых интерфейсов хоста и назначение логических сетей хостам руководства администратора и Добавление нового сетевого интерфейса в Руководстве по управлению виртуальными машинами.

2.5. Удаление профиля vNIC

Удаление профиля vNIC из среды виртуализации.

Порядок действий:

1. Нажмите **Сеть (Network)** > **Сети (Networks)**.

2. Выберите имя логической сети. Откроется подробное представление.
3. Откройте вкладку **Профили vNIC (vNIC Profiles)**, чтобы увидеть доступные профили vNIC.
4. Выберите один или сразу несколько профилей и нажмите **[Удалить (Remove)]**.
5. Нажмите **[OK]**.

2.6. Назначение профилям vNIC групп безопасности

Эта функция доступна только при добавлении ovirt-provider-ovn в качестве внешнего провайдера сети. Невозможно создать группы безопасности через Менеджер управления. Их необходимо создать через OpenStack Networking на ovirt-provider-ovn.

Группы безопасности можно назначить профилю vNIC тех сетей, которые были импортированы из экземпляра OpenStack Networking и используют плагин Open vSwitch. Группа безопасности - это свод строгих правил, которые позволяют фильтровать входящий и исходящий трафик, проходящий через сетевой интерфейс. В процедуре ниже описано, как подключить группу безопасности к профилю vNIC.

Группам безопасности присваивается идентификатор, зарегистрированный в системе Open Virtual Network (OVN) Внешнего провайдера сети. Идентификаторы групп безопасности для данного арендатора можно найти с помощью OpenStack Networking API, см. раздел Списки групп безопасности в справочнике OpenStack API Reference.

Порядок действий:

1. Нажмите **Сеть (Network) > Сети (Networks)**.
2. Выберите имя логической сети. Откроется подробное представление.
3. Выберите вкладку **Профили vNIC (vNIC Profiles)**.
4. Нажмите **[Новый (New)]** или выберите существующий профиль vNIC и нажмите **[Изменить (Edit)]**.
5. В выпадающем списке пользовательских свойств выберите **SecurityGroups**. Если оставить выпадающий список пользовательских свойств незаполненным, то будут применены настройки безопасности по умолчанию, которые разрешают весь исходящий и внутренний трафики, но запрещают весь входящий трафик, поступающий извне группы безопасности по умолчанию. Обратите внимание, что последующее удаление свойства **SecurityGroups** не повлияет на применяемую группу безопасности.
6. В текстовом поле введите идентификатор группы безопасности, которую нужно подключить к профилю vNIC.
7. Нажмите **[OK]**.

Группа безопасности успешно подключена к профилю vNIC. Весь трафик через логическую сеть, к которой подключен этот профиль, будет фильтроваться в соответствии с правилами, определенными для этой группы безопасности.

2.7. Разрешения пользователей для профилей vNIC

Настройте разрешения пользователей, чтобы назначить пользователей на определенные профили vNIC. Назначьте пользователю роль **VnicProfileUser**, чтобы он мог использовать профиль. Ограничьте доступ пользователей к определенным профилям, удалив у них разрешение на этот профиль.

Порядок действий:

1. Нажмите **Сеть (Network) > Профили vNIC (vNIC Profiles)**.
2. Выберите имя профиля vNIC. Откроется подробное представление.
3. Откройте вкладку **Разрешения (Permissions)**, чтобы увидеть текущие разрешения пользователей для профиля.
4. Нажмите **[Добавить (Add)]** или **[Удалить (Remove)]**, чтобы изменить разрешения пользователя для профиля vNIC.
5. В окне **Добавить разрешение для пользователя (Add Permissions to User)** нажмите **[Мои группы (My Groups)]**, чтобы увидеть группы пользователей. Эту опцию можно использовать для предоставления разрешений другим пользователям в ваших группах.

Разрешения пользователей для профиля vNIC успешно настроены.

3. Сети внешнего провайдера

3.1. Импортирование сетей из внешних провайдеров

Для использования сетей из Открытой виртуальной сети (OVN) зарегистрируйте провайдера с помощью Менеджера управления. Дополнительные сведения см. в разделе Добавление внешнего провайдера сети. Затем выполните следующие действия для импорта сетей, предоставленных этим провайдером, в Менеджер управления, чтобы виртуальные машины смогли их использовать.

Порядок действий:

1. Нажмите **Сеть (Network) > Сети (Networks)**.
2. Нажмите **[Импортировать (Import)]**.
3. Из выпадающего списка **Провайдер сети (Network Provider)** выберите внешнего провайдера. Система автоматически обнаруживает сети, предложенные этим провайдером, и отображает их в виде списка **Провайдер сетей (Provider Networks)**.

4. Устанавливая флажки в соответствующие поля, выберите сети для импорта из списка **Провайдер сетей (Provider Networks)** и нажмите стрелку вниз ⬇, чтобы переместить эти сети в список **Сети для импорта (Networks to Import)**.
5. Имя импортируемой сети можно изменить. Чтобы изменить имя, нажмите на имя сети в столбце **Имя (Name)** и измените текст.
6. Из выпадающего списка **Центр данных (Data Center)** выберите центр данных, в который будут импортированы сети.
7. Дополнительно: Уберите флажок из поля **Разрешить всем (Allow All)**, чтобы эта сеть не была доступна всем пользователям.
8. Нажмите **[Импортировать (Import)]**.

Выбранные сети импортируются в целевой центр данных и могут быть подключены к виртуальным машинам. Дополнительные сведения см. в разделе Добавление нового сетевого интерфейса в Руководстве по управлению виртуальными машинами.

3.2. Ограничения относительно использования сетей внешнего провайдера

Следующие ограничения применимы к использованию логических сетей, импортированных из внешнего провайдера, в среде zVirt.

- Логические сети, предложенные внешними провайдерами, должны использоваться в качестве сетей виртуальных машин, а не сетей отображения.
- Одну и ту же логическую сеть можно импортировать несколько раз, но только в разные центры данных.
- Логические сети, предложенные внешними провайдерами, нельзя изменять в Менеджере управления. Чтобы изменить сведения о логической сети, предложенной внешним провайдером, измените ее напрямую из соответствующего внешнего провайдера.
- Зеркалирование портов недоступно для виртуальных сетевых карт, которые подключены к логическим сетям, предложенным внешними провайдерами.
- Если виртуальная машина использует логическую сеть, предложенную внешним провайдером, то, пока это происходит, такого провайдера нельзя удалить из Менеджера управления.
- Сети, предлагаемые внешними провайдерами, не относятся к обязательным. Поэтому при выполнении планирования для кластеров, в которые эти логические сети были импортированы, эти логические сети не будут учитываться во время выбора хоста. Кроме того, пользователь отвечает за обеспечение доступности логической сети на хостах в кластерах, в которые эти логические сети были импортированы.

3.3. Настройка подсетей в логических сетях внешнего провайдера

Логическая сеть, предоставленная внешним провайдером, может назначать IP-адреса виртуальным машинам, если только в этой логической сети заданы одна или несколько подсетей. Если подсети не заданы, то виртуальным машинам IP-адреса не назначаются. При наличии одной подсети виртуальным машинам будут назначаться IP-адреса из этой подсети, а при наличии нескольких подсетей виртуальным машинам будут назначаться IP-адреса из любых доступных подсетей. Служба DHCP, предоставленная внешним провайдером сети, на котором размещена логическая сеть, отвечает за назначение этих IP-адресов.

Хотя Менеджер управления автоматически обнаруживает предопределенные подсети в импортированных логических сетях, с его помощью можно также добавлять или удалять подсети в логических сетях.

При добавлении **Открытой виртуальной сети (OVN) (ovirt-provider-ovn)** в качестве внешнего провайдера сети, несколько подсетей могут быть присоединены друг к другу через маршрутизаторы. Для управления этими маршрутизаторами можно использовать OpenStack Networking API v2.0. Обратите внимание, что у ovirt-provider-ovn есть ограничение: Source NAT не реализован.

3.4. Добавление подсетей в логические сети внешнего провайдера

Создайте подсеть в логической сети, предоставленной внешним провайдером.

Порядок действий:

1. Нажмите **Сеть (Network)** > **Сети (Networks)**.
2. Нажмите на имя логической сети. Откроется подробное представление.
3. Откройте вкладку **Подсети (Subnets)**.
4. Нажмите **[Новая (New)]**.
5. Введите **Имя (Name)** и бесклассовую междоменную маршрутизацию (**CIDR**) для новой подсети.
6. Из выпадающего списка **Версия IP (IP Version)** выберите или `IPv4`, или `IPv6`.
7. Нажмите **[OK]**.

В версии IPv6 zVirt поддерживает только статическую адресацию.

3.5. Удаление подсетей из логических сетей внешнего провайдера

Удалите подсеть из логической сети, предоставленной внешним провайдером.

Порядок действий:

1. Нажмите **Сеть (Network) > Сети (Networks)**.
2. Нажмите на имя логической сети. Откроется подробное представление.
3. Откройте вкладку **Подсети (Subnets)**.
4. Выберите подсеть и нажмите **[Удалить (Remove)]**.
5. Нажмите **[OK]**.

3.6. Назначение групп безопасности логическим сетям и портам

Функция доступна, когда Открытая виртуальная сеть (OVN) добавлена как внешний провайдер сети (ovirt-provider-ovn). Группы безопасности нельзя создать с помощью Менеджера управления. Они создаются через OpenStack Networking API v2.0 или Ansible.

Группа безопасности - совокупность строгих правил, позволяющих фильтровать входящий и исходящий трафик в сети. Можно также использовать группы безопасности для фильтрации трафика на уровне порта.

В zVirt группы безопасности выключены по умолчанию.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Кластеры (Clusters)**.
2. Нажмите на имя кластера. Откроется подробное представление.
3. Выберите вкладку **Логические сети (Logical Networks)**.
4. Нажмите **[Добавить сеть (Add Network)]** и задайте свойства, убедившись при этом, что выбираете `ovirt-provider-ovn` из выпадающего списка **Внешний провайдер (External Provider)**. Дополнительные сведения см. в разделе Создание новой логической сети в центре данных или кластере.
5. Из выпадающего списка **Безопасность сетевого порта (Network Port Security)** выберите Включен (Enabled). Дополнительные сведения см. в разделе Описание общих настроек логической сети.
6. Нажмите **[OK]**.
7. Создайте группы безопасности с помощью **OpenStack Networking API v2.0** или **Ansible**.

8. Создайте правила групп безопасности с помощью **OpenStack Networking API v2.0** или **Ansible**.
9. Обновите порты с группами безопасности, заданные с помощью **OpenStack Networking API v2.0** или **Ansible**.
10. Дополнительно. Задайте, будет ли включен функционал безопасности на уровне порта. Сейчас это возможно только с помощью **OpenStack Networking API**. Если не выставлен атрибут `port_security_enabled`, то по умолчанию будет задано значение, указанное в сети, которой он принадлежит.

4. Хосты и сетевое взаимодействие

4.1. Менеджер сетевой конфигурации с отслеживанием состояния (nmstate)

В zVirt используется Менеджер сетевой конфигурации с отслеживанием состояния (**nm-state**), чтобы настраивать сети для хостов zVirt

Администратору не нужно устанавливать или конфигурировать **nmstate**, который включен по умолчанию и работает в фоновом режиме.

Обязательно используйте Менеджер управления для модификации сетевой конфигурации хостов в кластерах, иначе может быть создана неподдерживаемая конфигурация.

Изменение в **nmstate** почти незаметно. Оно лишь меняет то, как вы настраиваете сетевое взаимодействие хостов, а именно:

- После добавления хоста в кластер обязательно используйте Менеджер управления для модификации сети хостов.
- При модификации сети хостов без использования Менеджера управления может быть создана неподдерживаемая конфигурация.
- Для исправления неподдерживаемой конфигурации замените ее на поддерживаемую, используя Менеджер управления для синхронизации сети хостов. Подробнее см. в разделе Синхронизация сетей хостов.
- Сети хостов модифицируются за пределами Менеджера управления только при настройке статического маршрута на хосте. Подробнее см. в разделе Добавление статического маршрута на хосте.

Изменение в nmstate позволяют Менеджеру управления эффективнее применять изменения, сделанные в Cockpit и Anaconda до того, как хост был добавлен в Менеджер управления.

4.2. Обновление конфигурации ресурсов хоста

При добавлении сетевой карты на хост нужно обновить конфигурацию ресурсов хоста, чтобы сетевая карта появилась в Менеджере управления.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)** и выберите хост.
2. Нажмите **[Управление (Management)]** → **[Обновить возможности (Refresh Capabilities)]**.

Список сетевых карт во вкладке **Сетевые интерфейсы (Network Interfaces)** для выбранного хоста обновлен. Теперь любая новая сетевая карта может использоваться Менеджером управления.

4.3. Изменение сетевых интерфейсов хоста и назначение логических сетей хостам

Можно изменять настройки физических сетевых интерфейсов хостов, переносить сеть управления с одного физического сетевого интерфейса хоста на другой, назначать логические сети физическим сетевым интерфейсам хостов. Пользовательские свойства **bridge** и **ethtool** также поддерживаются.

Изменить IP-адрес хоста в zVirt можно, только удалив хост и затем добавив его снова.

Чтобы изменить настройки VLAN хоста, см. раздел Изменение настроек VLAN хоста.

Невозможно назначать логические сети, предлагаемые внешними провайдерами, физическим сетевым интерфейсам хоста - такие сети динамически назначаются хостам, когда они требуются виртуальным машинам.

Если коммутатор был сконфигурирован для предоставления информации по протоколу **Link Layer Discovery Protocol (LLDP)**, наведите указатель мыши на физический сетевой интерфейс для просмотра текущей конфигурации порта коммутатора. Так можно избежать использования неправильной конфигурации. Проверьте следующую информацию перед назначением логических сетей:

- **Port Description** (TLV type 4) (описание порта) и **System Name** (TLV type 5) (системное имя) помогают определить, к каким портам и на каком коммутаторе коммутированы интерфейсы хоста.
- **Port VLAN ID** отображает ID сети VLAN, сконфигурированной на порте коммутатора для нетегированных кадров ethernet (Native VLAN). Все сети VLAN, сконфигурированные на порте коммутатора отображаются в виде комбинаций **VLAN Name** и **VLAN ID**.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Хосты (Hosts)**.
2. Нажмите на имя хоста. Откроется подробное представление.
3. Откройте вкладку **Сетевые интерфейсы (Network Interfaces)**.
4. Нажмите **[Настройка сетей хоста (Setup Host Networks)]**.
5. Дополнительно наведите указатель мыши на сетевой интерфейс хоста для просмотра информации о конфигурации, предоставленной коммутатором.
6. Подключите логическую сеть к физическому сетевому интерфейсу хоста, выбрав и перетащив логическую сеть в область **Назначенные логические сети (Assigned Logical Networks)** рядом с физическим сетевым интерфейсом хоста.

> Если сетевая карта подключена к нескольким логическим сетям, только одна из сетей может быть не VLAN. Все остальные логические сети должны быть уникальными сетями VLAN.

7. Сконфигурируйте логическую сеть:
   a. Наведите указатель мыши на назначенную логическую сеть и нажмите значок карандаша ✎. Откроется окно Изменить сеть управления (Edit Management Network).
   b. На вкладке IPv4 выберите **Конфигурацию (Boot Protocol)** из вариантов `Отсутствует (None)`, `DHCP` или `Статичная (Static)`. Если выбран вариант `Статичная (Static)`, то введите **IP-адрес (IP)**, **Маска подсети/префикс (Netmask/Routing Prefix)** и **Шлюз (Gateway)**.

> Для IPv6 поддерживается только статическая адресация. Для конфигурации логической сети выберите вкладку IPv6 и введите следующие входные данные:
>
> - Установите вариант `Статичная (Static)` для **Конфигурации (Boot Protocol)**.
> - В поле **Префикс маршрутизатора (Routing Prefix)** введите длину префикса, используя прямую косую черту и число в десятичной системе счисления. Например: `/48`
> - **IP**: Полный IPv6-адрес сетевого интерфейса хоста. Например: `2001:db8::1:0:0:6`
> - **Шлюз (Gateway)**: IPv6-адрес исходного маршрутизатора. Например: `2001:db8::1:0:0:1`

> Если вы изменяете IP-адреса сети управления хоста, необходимо переустановить хост, чтобы новый IP-адрес был настроен.
>
> У каждой логической сети может быть отдельный шлюз, отличный от шлюза сети управления. В результате трафик, поступающий в логическую сеть, пойдет через шлюз логической сети, а не через шлюз по умолчанию, используемый сетью управления.

Настройте все хосты в кластере, чтобы их сети управления использовали один и тот же IP-стек: или IPv4, или IPv6. Одновременное использование обоих стеков не поддерживается.

c. Чтобы переопределить политику QoS сети хоста по умолчанию, откройте вкладку QoS. Выберите **Перезаписать QoS (Override QoS)** и введите желаемые значения в следующие поля:

- **Общие веса (Weighted Share)**: Означает, какая часть пропускной способности логического канала связи должна быть выделена для конкретной сети относительно других сетей, подключенных к тому же логическому каналу связи. Точная доля зависит от суммарного количества долей всех сетей на этом канале связи. По умолчанию это число в диапазоне 1-100.
- **Ограничение скорости [Mbps] (Rate Limit [Mbps])**: Максимальная полоса пропускания для использования сетью.
- **Подтверждённая скорость [Мб/с] (Committed Rate [Mbps])**: Минимальная полоса пропускания, требуемая для сети. Требуемая **Подтверждённая скорость** не гарантируется и будет варьироваться в зависимости от сетевой инфраструктуры и **Подтверждённой скорости**, требуемой для других сетей на том же логическом канале связи.

d. Для конфигурирования сетевого моста откройте вкладку **Настраиваемые параметры (Custom Properties)** и из выпадающего списка выберите параметр `bridge_opts`. Введите корректный ключ и значение в следующем формате: `key=значение`. Разделите несколько записей знаком пробела. Следующие ключи корректны, а значения приведены в качестве примера. Для получения дополнительной информации об этих параметрах см. раздел Описание параметров bridge_opts.

```
forward_delay=1500
group_addr=1:80:c2:0:0:0
group_fwd_mask=0x0
hash_max=512
hello_time=200
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
```

e. Для конфигурирования ethernet-свойств откройте вкладку **Настраиваемые параметры (Custom Properties)** и из выпадающего списка выберите параметр `ethtool_opts`. Введите корректное значение, используя формат аргументов командной строки `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 можно использовать шаблоны подстановки. Например, для применения одного и того же параметра ко всем интерфейсам этой сети, используйте:

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

Параметр `ethtool_opts` не доступен по умолчанию; его нужно добавить, используя инструмент конфигурации **engine**. Для получения дополнительной информации см. раздел Как настроить Менеджер управления для использования ethtool. Для получения дополнительной информации о свойствах ethtool откройте соответствующую страницу руководства, введя `man ethtool` в командной строке.

f. Для конфигурирования **Fibre Channel over Ethernet (FCoE)** откройте вкладку **Настраиваемые параметры (Custom Properties)** и из выпадающего списка выберите параметр `fcoe`. Введите корректный ключ и значение в следующем формате: `key=значение`. Требуется указать хотя бы `enable=yes`. Можно также добавить `dcb=[yes|no]` и `auto_vlan=[yes|no]`. Разделите несколько записей знаком пробела. Параметр `fcoe` не доступен по умолчанию; его нужно добавить, используя инструмент конфигурации **engine**. Для получения дополнительной информации см. раздел Как настроить Менеджер управления для использования FCoE.

Использовать FCoE рекомендуется вместе с отдельной выделенной логической сетью.

g. Чтобы изменить сеть, используемую хостом по умолчанию, с сети управления (**ovirt-mgmt**) на сеть, не отвечающую за управление, сконфигурируйте маршрут сети, не отвечающей за управление, как используемый по умолчанию. Для получения дополнительной информации см. раздел Настройка логической сети, не являющейся сетью управления, в качестве маршрута по умолчанию.

h. Если ваше определение настроек логической сети не синхронизировано с конфигурацией сети на хосте, то поставьте флажок **Синхронизировать сеть (Sync network)**. Для получения дополнительной информации о несинхронизированных хостах и о том, как их синхронизировать см. раздел Синхронизация сетей хостов.

8. Установите флажок **Проверить соединение между хостом и Engine (Verify connectivity between Host and Engine)** для проверки сетевого подключения. Это действие возможно, только если хост находится в режиме обслуживания.
9. Нажмите **[OK]**.

Если для хоста отображаются не все сетевые карты, то нажмите **[Управление (Management)]** → **[Обновить возможности (Refresh Capabilities)]**, чтобы обновить список сетевых карт, доступных для этого хоста.

Поиск и устранение неполадок

Иногда внесение нескольких изменений одновременно в конфигурацию сети хостов с помощью окна **Настройка сетей хоста (Setup Host Networks)** или задачи `setupNetwork` завершается ошибкой `Сбой операции (Operation failed): [Cannot setup Networks]. Another Setup Networks or Host Refresh process in progress on the host. Please try later.`. Эта ошибка свидетельствует о том, что некоторые изменения не были сконфигурированы на хосте. Это происходит из-за того, что для сохранения целостности состояния конфигурации единовременно может обрабатываться только одна сетевая задача. Другие одновременные задачи конфигурирования ставятся в очередь с 20-секундным интервалом по умолчанию. Для предотвращения вышеуказанного сбоя используйте команду `engine-config`, чтобы задать интервал `SetupNetworksWaitTimeoutSeconds` больше **20** секунд. Например:

```
engine-config --set SetupNetworksWaitTimeoutSeconds=40
```

Дополнительные ресурсы

- Синтаксис команды engine-config
- Метод setupnetworks

4.4. Пользовательские свойства сети

4.4.1. Описание параметров bridge_opts

Таблица 7. Параметры bridge_opts**

Параметр	Описание
`forward_delay`	Задает время (в десятых долях секунды), которое мост будет проводить в состояниях прослушивания и обучения. Если за это время цикл коммутации не будет обнаружен, мост перейдет в состояние перенаправления. Это позволяет успеть проверить трафик и конфигурацию сети перед нормальной эксплуатацией.

Параметр	Описание
`group_addr`	Для отправки общего запроса установите это значение в 0. Для отправки запросов, относящихся к конкретной группе и к конкретным группе и источнику, задайте в качестве этого значения 6-байтовый MAC-адрес, а не IP-адрес. Допустимые значения: 01:80:C2:00:00:0x, за исключением 01:80:C2:00:00:01, 01:80:C2:00:00:02 и 01:80:C2:00:00:03.
`group_fwd_mask`	Включает мост для передачи адресов локальной группы по каналу. Изменение этого заданного по умолчанию значения позволит задать нестандартное поведение моста (bridge).
`hash_max`	Максимальное количество бакетов в хэш-таблице. Этот параметр вступает в силу немедленно и не может быть установлен в значение меньше текущего количества записей в мультивещательной группе. Значение должно быть степенью двойки.
`hello_time`	Задает интервал времени (в десятых долях секунды) между отправкой приветственных сообщений, анонсирующих позицию моста в топологии сети. Применяется, только если этот мост является корневым мостом связующего дерева (Spanning Tree).
`max_age`	Задает максимальное время (в десятых долях секунды) для получения приветственного сообщения от другого корневого моста, прежде чем этот мост будет сочтен неработающим и начнется процесс переключения.
`multicast_last_member_count`	Задает количество запросов "последнего члена", отправляемых в мультивещательную группу после получения от хоста сообщения "покинуть группу".
`multicast_last_member_interval`	Задает время (в десятых долях секунды) между запросами "последнего члена".
`multicast_membership_interval`	Задает время (в десятых долях секунды), в течение которого мост будет ждать ответа от члена мультивещательной группы, прежде чем прекратит отправку мультивещательного трафика на хост.

Параметр	Описание
`multicast_querier`	Указывает, будет ли мост активно запускать формирователь мультивещательных запросов. Когда мост получает запрос "членства на мультивещательном хосте" от другого хоста сети, этот хост отслеживается, исходя из времени получения запроса и длительности интервала мультивещательного запроса. Если позже мост попытается перенаправить трафик для этой мультивещательной группы или обменивается данными с запрашивающим мультивещательным маршрутизатором, то этот таймер подтверждает корректность формирователя запросов. Если корректность подтверждена, мультивещательный трафик доставляется через имеющуюся на мосте таблицу членства в мультивещательной группе, в противном случае трафик отправляется через все порты моста.Широковещательные домены с членством в мультивещательной группе (или ожидающие такого членства) должны иметь по крайней мере один работающий формирователь мультивещательных запросов для повышения производительности.
`multicast_querier_interval`	Задает максимальное время (в десятых долях секунды) между последним запросом "членства на мультивещательном хосте", полученным от хоста, чтобы убедиться в его корректности.
`multicast_query_use_ifaddr`	Логическое выражение. Значение по умолчанию равно нулю, и в этом случае формирователь запросов использует 0.0.0.0 в качестве адреса-источника для сообщений IPv4. Изменение этого значения задает IP-адрес моста в качестве адреса-источника.
`multicast_query_interval`	Задает время (в десятых долях секунды) между запросами-сообщениями, отправляемыми мостом для проверки действительности членства в мультивещательной группе. В это время (или если от моста запросят отправить мультивещательный запрос на такое членство) мост проверяет состояние своего собственного формирователя мультивещательных запросов, исходя из времени, когда была запрошена проверка, плюс `multicast_query_interval`. Если мультивещательный запрос на такое членство был отправлен в течение последнего интервала `multicast_query_interval`, то он не отправляется повторно.
`multicast_query_response_interval`	Время (в десятых долях секунды), в течение которого хосту разрешено отвечать на запрос после его отправки.Не должно превышать значения `multicast_query_interval`.

Параметр	Описание
`multicast_router`	Позволяет включать или выключать порты при подключении мультивещательных маршрутизаторов. Порт с одним или несколькими мультивещательными маршрутизаторами будет получать весь мультивещательный трафик. Значение 0 полностью отключает, 1 позволяет системе автоматически определять наличие маршрутизаторов, основываясь на запросах, а 2 позволяет портам всегда получать весь мультивещательный трафик.
`multicast_snooping`	Включает/выключает слежение. Слежение позволяет мосту прослушивать сетевой трафик между маршрутизаторами и хостами, чтобы поддерживать карту для фильтрации мультивещательного трафика по соответствующим каналам.Этот параметр позволяет пользователю повторно включить слежение, если оно было автоматически выключено из-за конфликта хэширования, однако слежение невозможно повторно включить, если конфликт хэширования не был разрешен.
`multicast_startup_query_count`	Задает количество запросов, отправляемых при запуске для определения информации о членстве.
`multicast_startup_query_interval`	Задает время (в десятых долях секунды) между запросами, отправляемыми при запуске для определения информации о членстве.

4.4.2. Как настроить Менеджер управления для использования ethtool

Свойства **ethtool** для сетевых карт хоста можно настроить на Портале администрирования. Ключ `ethtool_opts` недоступен по умолчанию - его нужно добавить в Менеджер управления, используя инструмент настройки **engine**. Кроме того, необходимо установить на хосты соответствующий пакет хуков VDSM.

Добавление ключа `ethtool_opts` в Менеджер управления

1. Чтобы добавить ключ, в Менеджере управления запустите следующую команду:

```
engine-config -s UserDefinedNetworkCustomProperties=ethtool_opts=.* --
cver=4.4
```

2. Перезапустите службу **ovirt-engine**:

```
systemctl restart ovirt-engine.service
```

3. На хостах, где необходимо настроить свойства **ethtool**, установите пакет хуков VDSM.

```
dnf install vdsm-hook-ethtool-options
```

Теперь ключ `ethtool_opts` доступен на Портале администрирования. Узнать о том, как применять свойства `ethtool` к логическим сетям, можно в разделе Изменение сетевых интерфейсов хоста и назначение логических сетей хостам.

4.4.3. Как настроить Менеджер управления для использования FCoE

Свойства **Fibre Channel over Ethernet (FCoE)** для сетевых карт хоста можно настроить на Портале администрирования. Ключ `fcoe` недоступен по умолчанию - его нужно добавить в Менеджер управления, используя инструмент настройки **engine**. Чтобы выяснить, не включен ли уже ключ `fcoe`, выполните следующую команду:

```
engine-config -g UserDefinedNetworkCustomProperties
```

Кроме того, необходимо установить на хосты соответствующий пакет хуков VDSM. В зависимости от карты FCoE на хостах может также потребоваться специальная конфигурация.

Порядок действий:

1. Чтобы добавить ключ, в Менеджере управления запустите следующую команду:

   ```
   engine-config -s
   UserDefinedNetworkCustomProperties='fcoe=^((enable|dcb|auto_vlan)=
   (yes|no),?)*$'
   ```

2. Перезапустите службу **ovirt-engine**:

   ```
   systemctl restart ovirt-engine.service
   ```

3. Установите пакет хуков VDSM на каждый хост, на котором необходимо настроить свойства FCoE. Пакет доступен по умолчанию на хостах с zVirt Node.

   ```
   dnf install vdsm-hook-fcoe
   ```

Теперь ключ `fcoe` доступен на Портале администрирования. Узнать о том, как применять свойства FCoE к логическим сетям, можно в разделе Изменение сетевых интерфейсов хоста и назначение логических сетей хостам.

4.5. Синхронизация сетей хостов

Менеджер управления определяет сетевой интерфейс как несинхронизированный (out-of-sync), когда определение настроек интерфейса на хосте отличается от определения настроек, которое хранит Менеджер управления.

Несинхронизированные сети обозначаются значком на вкладке Сетевые интерфейсы (Network Interfaces) и значком в окне **Настройка сетей хоста (Setup Host Networks)**.

Когда сеть хоста не синхронизирована, единственное, что можно сделать с несинхронизированной сетью в окне **Настройка сетей хоста (Setup Host Networks)** - это отключить логическую сеть от сетевого интерфейса или выполнить синхронизацию сети.

Причины, по которым хост становится несинхронизированным

Хост может стать несинхронизированным, если:

- Внести изменения в конфигурацию на хосте, а не в окне **Изменить логическую сеть (Edit Logical Networks)**, например:
  - изменить идентификатор VLAN на физическом хосте
  - изменить Пользовательское значение MTU (Custom MTU) на физическом хосте
- Переместить хост в другой центр данных с тем же именем сети, но с другими значениями/параметрами.
- Изменить свойство сети **Сеть ВМ (VM Network)**, вручную удалив мост (bridge) с хоста.

> В случае изменения настроек MTU сети необходимо распространить это изменение на работающие виртуальные машины в сети: Выполните горячее выключение и повторное включение каждой виртуальной сетевой карты виртуальной машины, к которой нужно применить эту настройку MTU, или перезапустите виртуальные машины. В противном случае эти интерфейсы перестанут работать при переносе виртуальной машины на другой хост.

Предотвращение рассинхронизации хоста

Следование этим рекомендациям предотвратит рассинхронизацию хоста:

1. Вносите изменения через **Портал администрирования**, а не локально на хосте.
2. Изменяйте настройки VLAN в соответствии с инструкциями в разделе Изменение настроек VLAN хоста.

Синхронизация хостов

Синхронизация определения настроек сетевых интерфейсов хоста подразумевает использование определения настроек из Менеджера управления и его применение к хосту. Если это не то определение настроек, которое вам нужно, после синхронизации хостов обновите их определение настроек с Портала администрирования.
Синхронизировать сети хоста можно на трех уровнях:

- логической сети

- хоста
- кластера

Синхронизация сетей хостов на уровне логической сети

1. Нажмите **Ресурсы (Compute) > Хосты (Hosts)**.
2. Нажмите на имя хоста. Откроется подробное представление.
3. Откройте вкладку **Сетевые интерфейсы (Network Interfaces)**.
4. Нажмите **[Настройка сетей хоста (Setup Host Networks)]**.
5. Наведите указатель мыши на несинхронизированную сеть и нажмите на значок карандаша . Откроется окно **Изменить сеть (Edit Network)**.
6. Поставьте флажок **Синхронизировать сеть (Sync network)**.
7. Нажмите **[OK]**, чтобы сохранить изменение сети.
8. Нажмите **[OK]**, чтобы закрыть окно **Настройка сетей хоста (Setup Host Networks)**.

Синхронизация сетей хоста на уровне хоста

- Нажмите **Синхронизировать все сети (Sync All Networks)** на вкладке **Сетевые интерфейсы (Network Interfaces)** хоста, чтобы синхронизировать все несинхронизированные сетевые интерфейсы хоста.

Синхронизация сетей хоста на уровне кластера

- Нажмите **Синхронизация всех сетей (Sync All Networks)** на вкладке **Логические сети (Logical Networks)** кластера, чтобы синхронизировать все несинхронизированные определения настроек логических сетей для всего кластера.

Сети хоста также можно синхронизировать через REST API. См. syncallnetworks в руководстве по REST API.

4.6. Изменение настроек VLAN хоста

Чтобы изменить настройки VLAN хоста, нужно удалить хост из Менеджера управления, переконфигурировать его и снова добавить в Менеджер управления.

Чтобы сохранить синхронизацию сетей, сделайте следующее:

1. Переведите хост в режим обслуживания.
2. Вручную удалите сеть управления из хоста. Это сделает хост доступным через новый VLAN.
3. Добавьте хост к кластеру. Виртуальные машины, которые не подключены напрямую к сети управления, можно безопасно переносить между хостами.

При изменении VLAN ID сети управления появляется следующее предупреждение:

```
Изменение определенных свойств (например, VLAN или MTU) сети управления
может привести к потере связи с хостами в центре данных, если конфигурация
его базовой сетевой инфраструктуры не учитывает эти изменения. Вы уверены,
что хотите продолжить?

(Changing certain properties (e.g. VLAN, MTU) of the management network could
lead to loss of connectivity to hosts in the data center, if its underlying
network infrastructure isn't configured to accommodate the changes.
Are you sure you want to proceed?)
```

В результате все хосты в центре данных потеряют связь с Менеджером управления, а миграция хостов в новую сеть управления завершится ошибкой. Будет выдано сообщение о том, что сеть управления не синхронизирована.

В случае изменения VLAN ID сети управления необходимо переустановить хост, чтобы применить новый VLAN ID.

4.7. Добавление нескольких VLAN к одному сетевому интерфейсу с помощью логических сетей

К одному сетевому интерфейсу можно добавить несколько VLAN для разделения трафика на одном хосте.

Для этого необходимо заранее создать несколько логических сетей и для каждой из них установить флажок **Включить тегирование VLAN (Enable VLAN tagging)** в окнах **Новая логическая сеть (New Logical Network)** или **Изменить логическую сеть (Edit Logical Network)**.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Хосты (Hosts)**.
2. Нажмите на имя хоста. Откроется подробное представление.
3. Откройте вкладку **Сетевые интерфейсы (Network Interfaces)**.
4. Нажмите **[Настройка сетей хоста (Setup Host Networks)]**.
5. Перетащите логические сети с тегами VLAN в область **Назначенные логические сети (Assigned Logical Networks)** рядом с физическим сетевым интерфейсом. Физическому сетевому интерфейсу может быть назначено несколько логических сетей благодаря назначению тегов VLAN.
6. Измените логические сети:
    a. Наведите указатель мыши на назначенную логическую сеть и нажмите на значок карандаша ✎.

b. Если определение настроек логической сети не синхронизировано с конфигурацией сети на хосте, то поставьте флажок **Синхронизировать сеть (Sync network)**.

c. Выберите **Конфигурацию (Boot Protocol)**:

- Отсутствует (None)
- DHCP
- Статичная (Static)

d. Укажите **IP-адрес (IP)** и **Маску подсети (Subnet Mask)**.

e. Нажмите **[OK]**.

7. Поставьте флажок **Проверить соединение между хостом и Engine (Verify connectivity between Host and Engine)**, чтобы запустить проверку сети. Это действие будет выполнено, только если хост находится в режиме обслуживания.
8. Нажмите **[OK]**.

Добавьте логическую сеть к каждому хосту в кластере, изменив сетевую карту на каждом хосте в кластере. После этого сеть станет работоспособной.

Этот процесс можно повторять многократно, каждый раз выбирая и изменяя один и тот же сетевой интерфейс на каждом хосте, чтобы добавлять логические сети с разными тегами VLAN к одному сетевому интерфейсу.

4.7.1. Копирование сетей хостов

Чтобы сэкономить время, можно скопировать конфигурацию сети исходного хоста на целевой хост в том же кластере.

Копирование конфигурации сети включает в себя:

- Логические сети, подключенные к хосту, кроме сети управления ovirtmgmt.
- Bond-интерфейсы, подключенные к интерфейсам

Ограничения:

- Не копируйте конфигурации сетей, содержащие статические IP-адреса. В этом случае **Конфигурация (Boot protocol)** на целевом хосте будет установлен в значение `Отсутствует (None)`.
- Копирование конфигурации на целевой хост с теми же именами интерфейсов, что и у исходного хоста, но с другими физическими сетевыми подключениями, приводит к неправильной конфигурации.
- Целевой хост должен иметь как минимум столько же интерфейсов, что и исходный хост. В противном случае операция будет неудачной.
- Копирование QoS, DNS и Настраиваемых параметров (custom_properties) не поддерживается.

- Метки сетевых интерфейсов не копируются.

Копирование сетей хоста заменяет все сетевые настройки на целевом хосте, кроме его подключения к сети управления **ovirtmgmt**.

Предварительные условия:

- Целевой хост должен иметь как минимум столько же сетевых карт, что и исходный хост. В противном случае операция будет неудачной.
- Хосты должны находиться в одном кластере.

Порядок действий:

1. На Портале администрирования нажмите **Ресурсы (Compute) > Хосты (Hosts)**.
2. Выберите исходный хост, чью конфигурацию хотите скопировать.
3. Нажмите **[Копирование сетей хоста (Copy Host Networks)]**. Откроется окно **Копирование сетей хоста (Copy Host Networks)**.
4. Используйте параметр **Целевой хост (Target Host)**, чтобы выбрать хост, который должен принять эту конфигурацию. В списке перечислены только те хосты, которые находятся в том же кластере.
5. Нажмите **[Копирование сетей хоста (Copy Host Networks)]**.
6. Проверьте сетевые настройки целевого хоста

- Выбор нескольких хостов деактивирует кнопку **[Копирование сетей хоста (Copy Host Networks)]** и контекстное меню.
- Вместо кнопки **[Копирование сетей хоста (Copy Host Networks)]** можно нажать правой кнопкой мыши на хост и выбрать **[Копирование сетей хоста (Copy Host Networks)]** в контекстном меню.
- Кнопка **[Копирование сетей хоста (Copy Host Networks)]** доступна также в подробном представлении каждого хоста.

4.8. Назначение дополнительных IPv4-адресов сети хоста

При начальной настройке сеть хоста (такая как сеть управления **ovirtmgmt**) создается с единственным IP-адресом. Это означает, что если конфигурационный файл сетевой карты содержит несколько IP-адресов, только первый указанный IP-адрес будет назначен сети хоста. Дополнительные IP-адреса могут потребоваться при подключении к хранилищу или к серверу в отдельной частной подсети с использованием той же сетевой карты.

Хук **vdsm-hook-extra-ipv4-addrs** позволяет настроить дополнительные IPv4-адреса для сетей хоста. Дополнительные сведения о хуках см. в VDSM и хуки.

В следующей процедуре специфичные для хоста задачи должны быть выполнены на каждом хосте, для которого вы хотите настроить дополнительные IP-адреса.

Порядок действий:

1. На хосте, для которого вы хотите настроить дополнительные IPv4-адреса, установите пакет хука VDSM.

```
dnf install vdsm-hook-extra-ipv4-addrs
```

2. В Менеджере управления запустите следующую команду, чтобы добавить ключ:

```
engine-config -s 'UserDefinedNetworkCustomProperties=ipv4_addrs=.*'
```

3. Перезапустите службу **ovirt-engine**:

```
systemctl restart ovirt-engine.service
```

4. На Портале администрирования нажмите **Ресурсы (Compute) > Хосты (Hosts)**.
5. Нажмите на имя хоста. Откроется подробное представление.
6. Откройте вкладку **Сетевые интерфейсы (Network Interfaces)** и нажмите **[Настройка сетей хоста (Setup Host Networks)]**.
7. Отредактируйте сетевой интерфейс хоста, наведя указатель мыши на назначенную логическую сеть и нажав на значок карандаша ✎.
8. Выберите ipv4_addr из выпадающего меню **Настраиваемые параметры (Custom Properties)** и добавьте дополнительный **IP-адрес** и **префикс** (например, `5.5.5.5/24`). Если IP-адресов несколько, их надо разделять запятой.
9. Нажмите **[OK]**, чтобы закрыть окно **Изменить сеть (Edit Network)**.
10. Нажмите **[OK]**, чтобы закрыть окно **Настройка сетей хоста (Setup Host Networks)**.

Дополнительные IP-адреса не будут отображаться в Менеджере управления, но можно выполнить команду `ip addr show` на хосте, чтобы убедиться, что они были добавлены.

4.9. Добавление меток сети к сетевым интерфейсам хостов

Использование меток сети значительно снижает административную нагрузку, связанную с назначением логических сетей сетевым интерфейсам хостов. Присвоение метки сети, выполняющей ту или иную роль (например, сети миграции или сети отображения) приводит к массовому развертыванию этой сети на всех хостах. Такое массовое добавление сетей достигается путем использования DHCP. Так как задача ввода множества статических IP-

адресов не масштабируется, был выбран именно этот метод массового развертывания, а не метод ввода статических адресов.

Существует два способа добавления меток к сетевому интерфейсу хоста:

- Вручную на Портале администрирования
- Автоматически с использованием службы LLDP Labeler

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Хосты (Hosts)**.
2. Нажмите на имя хоста. Откроется подробное представление.
3. Откройте вкладку Сетевые интерфейсы (Network Interfaces).
4. Нажмите **[Настройка сетей хоста (Setup Host Networks)]**.
5. Нажмите **Метки (Labels)**, после чего нажмите правой кнопкой мыши **[Новая метка] ([New Label])**. Выберите физический сетевой интерфейс, которому нужно присвоить метку.
6. Введите имя метки сети в текстовое поле **Метка (Label)**.
7. Нажмите **[OK]**.

Можно автоматизировать процесс присвоения меток сетевым интерфейсам хоста в настроенном списке кластеров с помощью службы LLDP Labeler.

4.10. Настройка службы LLDP Labeler

По умолчанию служба **LLDP Labeler** запускается раз в час. Этот вариант полезен, если вы меняете оборудование (например, сетевые карты, коммутаторы или кабели) или конфигурацию коммутаторов.

Предварительные условия:

- Интерфейсы должны быть подключены к коммутатору Juniper.
- Коммутатор Juniper должен быть настроен на предоставление Port VLAN с помощью LLDP.

Порядок действий:

1. Задайте `username` и `password` в **/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf**:
   - `username` - имя администратора Менеджера управления. Значение по умолчанию - `admin@internal`.
   - `password` - пароль администратора Менеджера управления. Значение по умолчанию = `123456`.

2. Настройте службу **LLDP Labeler**, обновив следующие значения в **/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf**:
    - `clusters` - разделенный запятыми список кластеров, на которых должна работать служба. Поддерживаются шаблоны подстановки. Например, значение `Cluster*` предпишет службе LLDP Labeler запуститься на всех кластерах, имя которых начинается со слова `Cluster`. Для запуска службы на всех кластерах в центре данных введите `. **Значение по умолчанию -** `Def`.
    - `api_url` - полный URL-адрес API-интерфейса Менеджера управления. Значение по умолчанию - `https://<Manager_FQDN>/ovirt-engine/api`
    - `ca_file` - путь к файлу сертификата, выданного альтернативным Центром сертификации. Если альтернативные сертификаты не используются, оставьте это значение `empty`. По умолчанию - `empty`.
    - `auto_bonding` - включает функции бондинга, имеющиеся у службы LLDP Labeler. Значение по умолчанию - `true`.
    - `auto_labeling` - включает функции присвоения меток, имеющиеся у службы LLDP Labeler. Значение по умолчанию - `true`.
3. При желании можно настроить службу на запуск с другой периодичностью, изменив значение `OnUnitActiveSec` в **/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer**. Значение по умолчанию - `1h`.
4. Настройте службу на запуск прямо сейчас и при загрузке, введя следующую команду:

    ```
    systemctl enable --now ovirt-lldp-labeler
    ```

    Чтобы вызвать службу вручную, введите следующую команду:

    ```
    /usr/bin/python /usr/share/ovirt-lldp-labeler/ovirt_lldp_labeler_cli.py
    ```

Сетевая метка будет добавлена к сетевому интерфейсу хоста. Вновь созданные логические сети с одной и той же меткой автоматически назначаются всем сетевым интерфейсам хоста с этой меткой. Удаление метки с логической сети автоматически удаляет эту логическую сеть из всех сетевых интерфейсов хоста с этой меткой.

4.11. Изменение полного доменного имени (FQDN) хоста

Используйте следующую процедуру, чтобы изменить полное доменное имя хостов.

Порядок действий:

1. Переведите хост в режим обслуживания, чтобы виртуальные машины "на лету" перенеслись на другой хост. Дополнительную информацию см. в разделе Перевод хоста

в режим обслуживания. Либо вручную выключите все виртуальные машины или перенесите их на другой хост. Дополнительную информацию см. в разделе Ручная миграция виртуальных машин руководства по управлению виртуальными машинами.

2. Нажмите **[Удалить (Remove)]** и затем **[OK]**, чтобы удалить хост из Портала администрирования.
3. Для обновления имени хоста воспользуйтесь инструментом `hostnamectl`.

```
hostnamectl set-hostname _NEW_FQDN_
```

4. Перезагрузите хост.
5. Заново зарегистрируйте хост в Менеджере управления. Дополнительную информацию см. в разделе Добавление стандартных хостов в Менеджер управления.

4.11.1. Поддержка работы в сетях IPv6

В большинстве ситуаций zVirt поддерживает статическую адресацию в IPv6-сетях.

zVirt требует, чтобы протокол IPv6 оставался включенным на компьютере или виртуальной машине, где запущен Менеджер управления (их также называют "машиной с Менеджером управления"). Не отключайте IPv6 на машине с Менеджером управления, даже если ваши системы его не используют.

Ограничения IPv6

- Поддерживается только статическая IPv6-адресация. Динамическая IPv6-адресация с DHCP или Автоматическая конфигурация адресов без сохранения состояния (State-less Address Autoconfiguration) не поддерживаются.
- Одновременная адресация IPv4 и IPv6 не поддерживается.
- При работе в OVN-сетях может использоваться только IPv4 или IPv6.
- Переключение кластеров от использования IPv4 к IPv6 не поддерживается.
- Для IPv6 можно задать только один шлюз на хост.
- Если обе сети используют один шлюз (находятся в одной подсети), то можно передать роль маршрута по умолчанию от сети управления (ovirtmgmt) другой логической сети. Хост и Менеджер управления должны иметь один и тот же шлюз IPv6. Если хост и Менеджер управления находятся в разных подсетях, то Менеджер управления может потерять связь с хостом, поскольку шлюз IPv6 был удален.
- Использование домена хранения **glusterfs** с сервером **gluster**, имеющим IPv6-адрес, не поддерживается.

4.11.2. Установка и настройка SR-IOV

В этом разделе описаны шаги по установке и настройке SR-IOV со ссылками на разделы, подробно описывающие каждый шаг.

Порядок действий:

1. Настройте сквозной доступ PCI на хосте.
2. Измените конфигурацию виртуальных функций на сетевой карте.
3. Включите сквозной доступ (**passthrough**) в Профиле vNIC.
4. Настройте виртуальные машины с виртуальными сетевыми картами (vNIC) с включенным SR-IOV, чтобы уменьшить время неработоспособности сети во время миграции.

- Количество виртуальных сетевых карт со сквозным доступом зависит от количества доступных виртуальных функций (VF) на хосте. Например, чтобы запустить виртуальную машину (BM) с тремя картами SR-IOV (vNIC), на хосте должны быть включены как минимум три виртуальные функции.
- Поддерживаются горячее подключение и отключение.
- Поддерживается миграция во время работы.
- Для переноса виртуальной машины на хосте-приемнике также должно быть достаточно доступных виртуальных функций, чтобы ее принять. Во время миграции виртуальная машина высвобождает ряд виртуальных функций на хосте-источнике и занимает такое же количество виртуальных функций на хосте-приемнике.
- На хосте устройство, канал или ifcae будут отображаться как любой другой интерфейс. Это устройство исчезнет, когда будет подключено к виртуальной машине, и снова появится, когда будет освобождено.
- Избегайте подключения устройства хоста непосредственно к виртуальной машине для реализации функции SR-IOV.

Вот пример того, как может выглядеть libvirt XML для интерфейса:

```
----
<interface type='hostdev'>
    <mac address='00:1a:yy:xx:vv:xx'/>
    <driver name='vfio'/>
    <source>
<address type='pci' domain='0x0000' bus='0x05' slot='0x10' function='0x0'/>
    </source>
    <alias name='ua-18400536-5688-4477-8471-be720e9efc68'/>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
</interface>
----
```

Поиск и устранение неполадок

В следующем примере показано, как получить диагностическую информацию о виртуальных функциях, подключенных к интерфейсу.

```
ip -s link show dev enp5s0f0

1: enp5s0f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9000 qdisc mq state UP
mode DEFAULT qlen 1000
    link/ether 86:e2:ba:c2:50:f0 brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors  dropped overrun mcast
    30931671   218401   0       0       0       19165434
    TX: bytes  packets  errors  dropped carrier collsns
    997136     13661    0       0       0       0
    vf 0 MAC 02:00:00:00:00:01, spoof checking on, link-state auto, trust
off, query_rss off
    vf 1 MAC 00:1a:4b:16:01:5e, spoof checking on, link-state auto, trust
off, query_rss off
    vf 2 MAC 02:00:00:00:00:01, spoof checking on, link-state auto, trust
off, query_rss off
```

5. Объединение сетевых интерфейсов (бондинг)

5.1. Методы бондинга

При бондинге несколько сетевых карт объединяются в одно бонд-устройство; это дает следующие преимущества:

- Скорость передачи объединенных сетевых карт выше, чем у одной сетевой карты.
- Объединение сетевых карт обеспечивает отказоустойчивость, так как объединенное устройство не выйдет из строя, пока не откажут все его сетевые карты.

Использование сетевых карт одного и того же производителя и модели гарантирует поддержку ими одних и тех же параметров и режимов бондинга.

Для используемого по умолчанию в zVirt режима бондинга (Mode 4) Dynamic Link Aggregation требуется коммутатор, поддерживающий 802.3ad.

Логические сети bond-интерфейса должны быть совместимы. Bond-интерфейс может поддерживать только одну логическую сеть, не являющуюся виртуальной локальной сетью (VLAN). Остальные логические сети должны иметь уникальные идентификаторы (ID) VLAN.

Бондинг должен быть включен для портов коммутатора. Для получения конкретных инструкций обратитесь к руководству, предоставленному поставщиком коммутатора.

Создать bond-интерфейс можно одним из следующих способов:

- Вручную на Портале администрирования для конкретного хоста
- Автоматически с помощью службы LLDP Labeler для необъединенных сетевых карт всех хостов в кластере или центре данных

Если в среде используется хранилище iSCSI и нужно настроить избыточность, то выполните инструкции из раздела Настройка многоканального доступа iSCSI.

5.2. Создание Bond-интерфейса на Портале администрирования

Bond-интерфейс можно создать на определенном хосте на Портале администрирования. Bond-интерфейс может передавать как тегированный трафик VLAN, так и нетегированный трафик.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Хосты (Hosts)**.
2. Нажмите имя хоста. Откроется подробное представление.
3. Нажмите вкладку **Сетевые интерфейсы (Network Interfaces)**, чтобы просмотреть список физических сетевых интерфейсов, подключенных к хосту.
4. Нажмите **[Настройка сетей хоста (Setup Host Networks)]**.
5. Проверьте конфигурацию коммутатора. Если коммутатор настроен на предоставление информации Link Layer Discovery Protocol (LLDP), то наведите указатель мыши на физическую сетевую карту, чтобы просмотреть конфигурацию агрегирования порта коммутатора.
6. Перетащите сетевую карту на другую сетевую карту или на Bond-интерфейс.

   Две сетевые карты образуют новый Bond-интерфейс. Сетевая карта и Bond-интерфейс добавляют сетевую карту к существующему Bond-интерфейсу.

   Если логические сети несовместимы, то операция объединения сетевых интерфейсов блокируется.

7. В выпадающих меню выберите **Имя Bond (Bond Name)** и **Режим бондинга (Bonding Mode)**. Подробности см. в разделе Режимы бондинга.

   При выборе режима `Настраиваемый (Custom)` можно ввести параметры бондинга в текстовом поле **Пользовательский режим**, как показано в следующих примерах:

   - Если среда не сообщает о состоянии канала с помощью программы ethtool, то можно настроить мониторинг ARP, введя `mode=1 arp_interval=1 arp_ip_target=192.168.0.2`.

- Сетевую карту с более высокой пропускной способностью можно назначить основным интерфейсом, введя `mode=1 primary=eth0`.

Полный список параметров бондинга и их описания см. в документе Linux Ethernet Bonding Driver HOWTO на сайте Kernel.org.

8. Нажмите **[OK]**.
9. Подключите логическую сеть к новому Bond-интерфейсу и настройте ее. Инструкции см. в разделе Изменение сетевых интерфейсов хоста и назначение логических сетей хостам.

> Логическую сеть нельзя подключить напрямую к отдельной сетевой карте на Bond-интерфейсе.

10. При желании можно выбрать **Проверить соединение между хостом и Engine (Verify connectivity between Host and Engine)**, если хост находится в режиме обслуживания.
11. Нажмите **[OK]**.

5.3. Создание Bond-интерфейса с помощью службы LLDP Labeler

Служба LLDP Labeler позволяет автоматически создать Bond-интерфейс со всеми необъединенными сетевыми картами для всех хостов в одном или нескольких кластерах или во всем центре данных. Создаваемый режим бондинга - `(Mode 4) Динамическая агрегация каналов (802.3ad)`.

Нельзя объединять сетевые карты с несовместимыми логическими сетями.

5.3.1. Настройка службы LLDP Labeler

По умолчанию служба LLDP Labeler запускается раз в час. Этот вариант полезен, если вы меняете оборудование (например, сетевые карты, коммутаторы или кабели) или конфигурацию коммутаторов.

Предварительные условия:

- Интерфейсы должны быть подключены к коммутатору Juniper.
- Коммутатор Juniper должен быть настроен для протокола управления агрегацией каналов (Link Aggregation Control Protocol, LACP) с использованием LLDP.

Порядок действий:

1. Задайте `username` и `password` в **/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf**:
   - `username` - имя администратора Менеджера управления. Значение по умолчанию - `admin@internal`.

- `password` - пароль администратора Менеджера управления. Значение по умолчанию - `123456`.

2. Настройте службу LLDP Labeler, обновив следующие значения в **/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf**:
   - `clusters` - разделенный запятыми список кластеров, на которых должна работать служба. Символы подстановки поддерживаются. Например, значение `Cluster*` предпишет службе LLDP Labeler запуститься на всех кластерах, имя которых начинается со слова Cluster. Для запуска службы на всех кластерах в центре данных введите `. **Значение по умолчанию - `Def`**.
   - `api_url` - полный URL-адрес API Менеджера управления. Значение по умолчанию - `https://<Manager_FQDN>/ovirt-engine/api`
   - `ca_file` - путь к файлу сертификата, выданного альтернативным Центром сертификации. Если альтернативные сертификаты не используются, оставьте значение `empty`. По умолчанию - `empty`.
   - `auto_bonding` - включает функции бондинга, имеющиеся у службы LLDP Labeler. Значение по умолчанию - `true`.
   - `auto_labeling` - включает функции присвоения меток, имеющиеся у службы LLDP Labeler. Значение по умолчанию - `true`.
3. При желании можно настроить службу на запуск с другой периодичностью, изменив значение `OnUnitActiveSec` в **/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer**. Значение по умолчанию - `1h`.
4. Настройте службу на запуск прямо сейчас и при загрузке, введя следующую команду:

   ```
   systemctl enable --now ovirt-lldp-labeler
   ```

   Чтобы вызвать службу вручную, введите следующую команду:

   ```
   /usr/bin/python /usr/share/ovirt-lldp-labeler/ovirt_lldp_labeler_cli.py
   ```

5. Подключите логическую сеть к новому объединенному сетевому устройству и настройте ее. Инструкции см. в разделе Изменение сетевых интерфейсов хоста и назначение логических сетей хостам.

Логическую сеть нельзя подключить напрямую к отдельной сетевой карте на Bond-интерфейсе.

5.4. Режимы бондинга

Алгоритм распределения пакетов определяется режимом бондинга (Подробности см. в документе Linux Ethernet Bonding Driver HOWTO). В zVirt режим бондинга по умолчанию - это

(Mode 4) Динамическая агрегация каналов (802.3ad).

zVirt поддерживает следующие режимы бондинга, так как их можно использовать в сетях виртуальных машин (связанных мостами):

(Mode 1) Active-Backup

> Активна одна сетевая карта. Если активная сетевая карта выйдет из строя, то одна из резервных сетевых карт заменит ее как единственную активную сетевую карту в Bond-интерфейсе. MAC-адрес этого Bond-интерфейса виден только на порту сетевого адаптера. Это предотвращает путаницу с MAC-адресами, которая может возникнуть, если MAC-адрес Bond-интерфейса изменится и будет показывать MAC-адрес новой активной сетевой карты.

(Mode 2) Load Balance (balance-xor)

> Сетевая карта, которая передает пакеты, выбирается путем выполнения операции XOR над MAC-адресом источника и MAC-адресом приемника и умножения на modulo общего количества сетевых карт. Этот алгоритм обеспечивает выбор одной и той же сетевой карты для каждого MAC-адреса приемника.

(Mode 3) Broadcast

> Пакеты передаются на все сетевые карты.

(Mode 4) Dynamic Link Aggregation(802.3ad) (Default)

> Сетевые карты объединяются в группы с одинаковыми настройками скорости и дуплекса. Используются все сетевые карты в активной группе агрегации.

Для **(Mode 4) Dynamic Link Aggregation(802.3ad)** требуется коммутатор, поддерживающий 802.3ad.

Объединенные сетевые карты должны иметь одинаковые идентификаторы агрегатора. Иначе на вкладке **Сетевые интерфейсы (Network Interfaces)** Менеджер управления покажет предупреждающий значок с восклицательным знаком на Bond-интерфейсе, а параметр `ad_partner_mac` Bond-интерфейса будет иметь значение: `00:00:00:00:00:00`. Чтобы проверить идентификаторы агрегатора, введите следующую команду:

```
cat /proc/net/bonding/bond0
```

Следующие режимы бондинга **несовместимы** с логическими сетями виртуальных машин, поэтому с помощью этих режимов к объединенным сетевым устройствам можно подключать только логические сети без виртуальных машин:

(Mode 0) Round-Robin

Сетевые карты передают пакеты в последовательном порядке. Пакеты передаются по циклу, который начинается с первой доступной сетевой карты в Bond-интерфейсе и заканчивается последней доступной сетевой картой в нем. Последующие циклы начинаются с первой доступной сетевой карты.

(Mode 5) Balance-TLB (так же называемый Transmit Load-Balance)

Исходящий трафик распределяется в зависимости от нагрузки по всем сетевым картам в Bond-интерфейсе. Входящий трафик принимается активной сетевой картой. Если сетевая карта, получающая входящий трафик, выйдет из строя, то будет назначена другая сетевая карта.

(Mode 6) Balance-ALB (так же называемый Adaptive Load-Balance)

(Mode 5) Balance-TLB сочетается с балансировкой нагрузки по приему для трафика IPv4. Для балансировки нагрузки по приему используется согласование ARP.

Управление политиками QoS

zVirt позволяет задать политики QoS (quality of service - «качество обслуживания»), которые обеспечивают тщательный контроль на уровне ввода и вывода, обработки и сетевых возможностей, к которым могут получить доступ ресурсы в среде виртуализации. Политики QoS задаются на уровне центра данных и назначаются профилям (которые создаются для кластеров и доменов хранения), vNIC, сетям. Далее профили назначаются конкретным отдельным ресурсам в кластерах (виртуальным машинам) и доменах хранения (дискам), где эти профили были созданы.

1. Политика QoS хранилища

Политика QoS хранилища определяет максимальную пропускную способность и максимальное количество операций ввода/вывода на виртуальный диск в домене хранения. Политика QoS хранилища назначается виртуальному диску, что позволяет выполнить тонкую настройку производительности домена хранения и не дать операциям в хранилище, ассоциированным с одним виртуальным диском, повлиять на возможности хранилища, доступные другим виртуальным дискам, размещенным в том же домене хранения.

1.1. Создание политики QoS хранилища

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.
3. Выберите вкладку **QoS**.
4. В разделе **Хранилище (Storage)**, нажмите **[Новая (New)]**.
5. Введите **Имя QoS (QoS Name)** и **Описание (Description)** для политики QoS.
6. Укажите QoS для **Пропускная способность (Throughput)**, нажав на одну из кнопок-переключателей:
    - **Нет (None)**
    - **Всего (Total)** - Введите максимальное разрешенное значение общей пропускной способности в поле **MB/s**.
    - **Чтение/запись (Read/Write)** - Введите максимальное разрешенное значение пропускной способности для операций чтения в левом поле **MB/s** и максимальное разрешенное значение пропускной способности для операций записи в правом поле **MB/s**.

7. Укажите QoS для операций ввода/вывода (**IOps**), нажав на одну из кнопок-переключателей:
    - **Нет**
    - **Всего (Total)** - Введите максимальное разрешенное количество операций ввода/вывода в секунду в поле **IOps**.
    - **Чтение/запись (Read/Write)** - Введите максимальное разрешенное количество операций ввода в секунду в левом поле **IOps** и максимальное разрешенное количество операций вывода в секунду в правом поле **IOps**.
8. Нажмите **[OK]**.

После создания политики QoS хранилища можно на базе этой политики создать профили дисков в доменах хранения, которые относятся к центру данных.

1.2. Применение политики QoS хранилища

Порядок действий:

1. Нажмите **Хранилище (Storage) > Домены (Domains)**.
2. Нажмите на имя нужного домена хранения для перехода в подробное представление.
3. Перейдите на вкладку **Профили диска**.
4. Нажмите **[Новый]** или, если необходимо применить QoS хранилища к существующему профилю, нажмите **[Изменить]**.
5. В окне создания/редактирования профиля диска в меню **QoS** выберите созданную политику.
6. Нажмите **[OK]**.

Теперь политики можно применять к нужным дискам при их создании или редактировании. Для этого в окне создания/редактирования диска в меню **Профиль диска** выберите профиль с назначенной политикой QoS.

Для применения политик QoS хранилища к дискам работающих виртуальных машин, эти виртуальные машины необходимо выключить и снова включить.

1.3. Удаление политики QoS хранилища

Существующую политику QoS хранилища можно удалить.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.

3. Выберите вкладку **QoS**.
4. Под **Хранилищем (Storage)** выберите политику QoS хранилища и нажмите **[Удалить (Remove)]**.
5. Нажмите **[OK]**.

Если какой-либо из профилей дисков был основан на этой политике, то политика QoS хранилища для этих профилей автоматически задается как `[unlimited]`.

2. Политика QoS сети виртуальных машин

Политика QoS сети виртуальных машин позволяет создавать профили для ограничения как входящего, так и исходящего трафика на отдельных виртуальных сетевых картах. С помощью этой функции можно ограничить полосу пропускания на нескольких уровнях и контролировать потребление сетевых ресурсов.

2.1. Создание политики QoS сети виртуальных машин

Политика QoS сети виртуальных машин создается для регулирования сетевого трафика с помощью профиля виртуальной сетевой карты (vNIC).

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.
3. Выберите вкладку **QoS**.
4. В разделе **Сеть ВМ (VM Network)** нажмите **[Новая (New)]**. Откроется окно **Новая политика QoS сети (New Network QoS)**.
5. Введите **Имя (Name)** для политики QoS сети виртуальных машин.
6. Введите ограничения для **Входящий (Inbound)** и **Исходящий (Outbound)** сетевого трафика.
7. Нажмите **[OK]**.

Вы создали политику QoS сети виртуальных машин, которая может использоваться на виртуальной сетевой карте.

2.2. Описание настроек в окнах "Новая политика QoS сети (New Network QoS)" и "Изменить QoS сети (Edit Network QoS)"

Настройки политики QoS сети виртуальных машин позволяют сконфигурировать ограничения полосы пропускания как для входящего, так и для исходящего трафика на трех отдельных уровнях.

Таблица 1. Настройки политики QoS сети виртуальных машин

Название поля	Описание
Центр данных (Data Center)	Центр данных, к которому добавляется политика QoS сети виртуальных машин. Данное поле настраивается автоматически в соответствии с выбранным центром данных.
Имя (Name)	Имя, используемое для представления политики QoS сети виртуальных машин в Менеджере.
Входящий (Inbound)	Настройки для применения к входящему трафику. Установите или уберите флажок **Входящий (Inbound)** для включения или выключения этих настроек. • **Средняя (Average)**: Средняя скорость входящего трафика. • **Максимальная (Peak)**: Скорость входящего трафика во время пиковых нагрузок. • **Скачкообразная (Burst)**: Скорость входящего трафика во время скачков нагрузки.
Исходящий (Outbound)	Настройки для применения к исходящему трафику. Установите или уберите флажок **Исходящий (Outbound)** для включения или выключения этих настроек. • **Средняя (Average)**: Средняя скорость исходящего трафика. • **Максимальная (Peak)**: Скорость исходящего трафика во время пиковых нагрузок. • **Скачкообразная (Burst)**: Скорость исходящего трафика во время скачков нагрузки.

Чтобы изменить максимальное значение, разрешенное в полях `Средняя (Average)`, `Максимальная (Peak)` или `Скачкообразная (Burst)`, используйте команду `engine-config` для изменения значения конфигурационных ключей MaxAverageNetworkQoSValue (по-умолчанию 17179 Мб/с), MaxPeakNetworkQoSValue (по-умолчанию 34359 Мб/с) или MaxBurstNetworkQoSValue (по-умолчанию 10240 Мб/с). Для сохранения изменений перезапустите службу **ovirt-engine**.

Пример 1. Изменение максимального значения NetworkQoSValue

```
engine-config -s MaxAverageNetworkQoSValue=2048
systemctl restart ovirt-engine
```

2.3. Применение политики QoS сети виртуальных машин

Порядок действий:

1. Нажмите **Сеть (Network)** > **Сети (Networks)**.
2. Нажмите на имя нужной сети для перехода в подробное представление.
3. Перейдите на вкладку **Профили vNIC**.
4. Нажмите **[Новый]** или, если необходимо применить QoS сети виртуальных машин к существующему профилю, нажмите **[Изменить]**.
5. В окне создания/редактирования профиля vNIC в меню **QoS** выберите созданную политику.
6. Нажмите **[OK]**.

Теперь политики можно применять к нужным виртуальным сетевым картам при создании или редактировании ВМ. Для этого при добавлении vNIC используйте профиль VNIC с назначенной политикой QoS.

2.4. Удаление политики QoS сети виртуальных машин

Существующую политику QoS сети виртуальных машин можно удалить.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.
3. Выберите вкладку **QoS**.
4. Под **Сеть ВМ (VM Network)** выберите политику QoS сети виртуальных машин и нажмите **[Удалить (Remove)]**.
5. Нажмите **[OK]**.

3. Политика QoS сети хоста

Политика QoS сети хоста конфигурирует сети на хосте для активации контроля сетевого трафика через физические интерфейсы. Политика QoS сети хоста позволяет выполнить тонкую настройку производительности сети через контроль потребления сетевых ресурсов на той же физической сетевой карте. В результате удается предотвратить ситуации, когда из-за интенсивного трафика одна сеть препятствует работе других сетей, подключенных к той же физической сетевой карте. Благодаря сконфигурированной политике QoS сети

хоста эти сети могут функционировать на одной и той же физической сетевой карте без риска перегрузки.

3.1. Создание политики QoS сети хоста

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.
3. Выберите вкладку **QoS**.
4. В разделе **Сеть хоста(Host Network)**, нажмите **[Новая (New)]**.
5. Введите **Имя QoS (QoS Name)** и описание для политики QoS.
6. Введите необходимые значения для **Общие веса (Weighted Share)**, **Ограничение скорости (Мб/с) (Rate Limit)** и **Подтверждённая скорость (Мб/с) (Committed Rate)**.
7. Нажмите **[OK]**.

3.2. Описание настроек в окнах "Новая политика QoS сети хоста (New Host Network Quality of Service)" и "Изменить политику QoS сети хоста (Edit Host Network Quality of Service)"

Через настройки политики QoS сети хоста можно сконфигурировать ограничения полосы пропускания для исходящего трафика.

Таблица 2. Настройки политики QoS сети хоста

Название поля	Описание
Центр данных (Data Center)	Центр данных, к которому добавляется политика QoS сети хоста. Данное поле настраивается автоматически в соответствии с выбранным центром данных.
Имя QoS (QoS Name)	Имя, используемое для представления политики QoS сети хоста в Менеджере.
Описание (Description)	Описание политики QoS сети хоста.

Название поля	Описание
Исходящий (Outbound)	Настройки для применения к исходящему трафику. • **Общие веса (Weighted Share)**: Означает, какая часть пропускной способности логического канала связи должна быть выделена для конкретной сети относительно других сетей, подключенных к тому же логическому каналу. Точная доля зависит от суммарного количества долей всех сетей на этом канале связи. По умолчанию это число в диапазоне 1-100. • **Ограничение скорости (Мб/с) (Rate Limit)**: Максимальная полоса пропускания для использования сетью. • **Подтверждённая скорость (Мб/с) (Committed Rate)**: Минимальная полоса пропускания, требуемая для сети. Требуемая **Подтверждённая скорость** не гарантируется и будет варьироваться в зависимости от сетевой инфраструктуры и **Подтверждённой скорости**, требуемой для других сетей на том же логическом канале связи.

Чтобы изменить максимальное значение, разрешенное в полях `Ограничение скорости (Мб/с) (Rate Limit)` или `Подтверждённая скорость (Мб/с) (Committed Rate)`, используйте команду `engine-config` для изменения значения конфигурационного ключа `MaxAverageNetworkQoSValue` (по-умолчанию 17179 Мб/с). Для сохранения изменения требуется перезапустить службу **ovirt-engine**.

Пример 2. Изменение максимального значения NetworkQoSValue

```
engine-config -s MaxAverageNetworkQoSValue=2048
systemctl restart ovirt-engine
```

3.3. Применение политики QoS сети хоста

Порядок действий:

1. Нажмите **Сеть (Network)** > **Сети (Networks)**.
2. Нажмите **[Новая]** или, если необходимо применить QoS сети хоста к существующей сети, выделите нужную сеть и нажмите **[Изменить]**
3. В окне создания/редактирования логической сети в меню **QoS сети хоста** выберите созданную политику.
4. Нажмите **[OK]**.

Политика будет применяться при назначении логической сети хосту.

3.4. Удаление политики QoS сети хоста

Политику QoS сети хоста можно удалить.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.
3. Выберите вкладку **QoS**.
4. Под **Сеть хоста (Host Network)** выберите политику QoS сети хоста и нажмите **[Удалить (Remove)]**.
5. При появлении запроса нажмите **[OK]**.

4. Политика QoS ЦП

Политика QoS ЦП определяет максимальную вычислительную мощность, которую виртуальная машина может получить на хосте, на котором она работает, выраженную в процентах от общей вычислительной мощности, доступной этому хосту. Назначив виртуальной машине политику QoS ЦП, можно сделать так, чтобы процесс на одной виртуальной машине в кластере не влиял на вычислительные ресурсы, доступные другим виртуальным машинам в этом кластере.

4.1. Создание политики QoS ЦП

Создайте политику QoS ЦП

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.
3. Выберите вкладку **QoS**.
4. Под ЦП (CPU), нажмите **[Новая (New)]**.
5. Введите **Имя QoS (QoS Name)** и **Описание (Description)** для политики QoS.
6. Введите в поле **Ограничение (%) (Limit (%))** максимальную вычислительную мощность, которая разрешается политикой QoS ЦП. Не вводите символ `%`.
7. Нажмите **[OK]**.

4.2. Применение политики QoS ЦП

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Кластеры (Clusters)**.
2. Нажмите на имя нужного кластера для перехода в подробное представление.
3. Перейдите на вкладку **Профили ЦП**.
4. Нажмите **[Новый]** или, если необходимо применить QoS ЦП к существующему профилю, нажмите **[Изменить]**.
5. В окне создания/редактирования профиля ЦП в меню **QoS** выберите созданную политику.
6. Нажмите **[OK]**.

Теперь политики можно применять к нужным виртуальным машинам при их создании или редактировании. Для в окне создания/редактирования ВМ перейдите на вкладку **Выделение ресурсов** и в меню **Профиль ЦП** выберите нужный профиль с назначенной политикой QoS.

4.3. Удаление политики QoS ЦП

Политику QoS ЦП можно удалить.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Центры данных (Data Centers)**.
2. Нажмите на имя центра данных. Откроется подробное представление.
3. Выберите вкладку **QoS**.
4. В разделе **ЦП (CPU)** выберите политику QoS ЦП и нажмите **[Удалить (Remove)]**.
5. Нажмите **[OK]**.

Если какой-либо из профилей ЦП был основан на той политике, то политика QoS ЦП для этих профилей автоматически задается как [unlimited].