# Глава 14. Внешние поставщики

## 14.1. Внешние поставщики в системе виртуализации Red Hat

В дополнение к ресурсам, управляемым самим виртуализированным ЦУ, система виртуализации Red Hat может также использовать преимущества ресурсов, управляемых внешними источниками. Поставщики этих ресурсов, известные как «внешние поставщики», могут предоставлять такие ресурсы, как хосты виртуализации, образы ВМ и сети.

На данный момент в системе виртуализации Red Hat имеется поддержка следующих внешних поставщиков:

**Red Hat Satellite: предоставление хостов**

Satellite — это инструментарий для управления всеми аспектами жизненного цикла как физических, так и виртуальных хостов. В системе виртуализации Red Hat хосты под управлением Satellite можно добавлять в виртуализированный ЦУ, где они используются в качестве хостов виртуализации. После добавления экземпляра Satellite в виртуализированный ЦУ, хосты, управляемые этим экземпляром Satellite, могут быть добавлены во время поиска новых доступных хостов в этом экземпляре.

**Служба образов OpenStack (Glance): работа с образами ВМ**

Служба образов OpenStack предоставляет каталог образов виртуальных машин. В системе виртуализации Red Hat эти образы можно импортировать в виртуализированный ЦУ и преобразовать в шаблоны. После добавления службы образов OpenStack в виртуализированный ЦУ, она появляется в виде домена хранилища, не присоединённого ни к одному дата-центру. Виртуальные диски в окружении виртуализации Red Hat также можно экспортировать в службу образов OpenStack в виде виртуальных дисков.

**Организации сетей OpenStack (Neutron): создание сетей**

Организация сетей OpenStack предоставляет программно-определяемые сети. В системе виртуализации Red Hat сети, предоставляемые OpenStack, можно импортировать в виртуализированный ЦУ и использовать для передачи любого типа трафика, а также для создания сложных сетевых топологий. После добавления сетевой конфигурации OpenStack в виртуализированный ЦУ, получить к ним доступ можно, импортировав их вручную.

**Тома OpenStack (Cinder): управление хранилищами**

Тома OpenStack предоставляют управление энергонезависимыми блочными хранилищами для виртуальных жёстких дисков. Тома OpenStack Cinder подготавливаются хранилищем Ceph. В системе виртуализации Red Hat можно создавать диски в хранилище томов OpenStack, которые можно присоединять к ВМ, или использовать как плавающие диски. После добавления тома OpenStack в виртуализированный ЦУ, в хранилище, предоставленном томом OpenStack, можно создавать диски.

**VMware: предоставление виртуальных машин**

Виртуальные машины, созданные в VMware, можно конвертировать с помощью V2V (virt-v2v) и импортировать в окружение виртуализации Red Hat. После добавления в виртуализированный ЦУ поставщика VMware, можно импортировать предоставляемые им ВМ. Преобразование V2V выполняется на выделенном узле прокси как составная часть операции по импортированию.

**RHEL 5 : предоставление виртуальных машин**

Виртуальные машины, созданные в RHEL 5 Xen, можно конвертировать с помощью V2V (virt-v2v) и импортировать в окружение виртуализации Red Hat. После добавления в виртуализированный ЦУ хоста RHEL 5 Xen, можно импортировать предоставляемые им ВМ. Преобразование V2V выполняется на выделенном узле прокси как составная часть операции по импортированию.

**KVM : предоставление виртуальных машин**

Виртуальные машины, созданные в KVM, можно импортировать в окружение виртуализации Red Hat. После добавления в виртуализированный ЦУ хоста KVM, можно импортировать предоставляемые им ВМ.

**Open Virtual Network (OVN): предоставление сетей**

Open Virtual Network (OVN) — это модуль Open vSwitch (OVS), предоставляющий программно-определяемые сети. После добавления OVN в виртуализированный ЦУ можно импортировать существующие сети OVN и создавать сети OVN в ЦУ. OVN также можно установить автоматически в виртуализированный ЦУ с помощью engine-setup.

**Внешний поставщик: предоставление сетей**

Поддерживаемые внешние поставщики программно-определяемых сетей включают в себя любого поставщика с реализацией OpenStack Neutron REST API. В отличие от сетей OpenStack (Neutron), агент Neutron не используется как реализация драйвера виртуального интерфейса на хосте. Вместо этого, драйвер виртуального интерфейса должен предоставляться реализатором поставщика внешней сети.

Внешние поставщики ресурсов добавляются с использованием одного окна, адаптирующегося ко вводу со стороны пользователя. Перед использованием предоставляемых ресурсов в окружении виртуализации Red Hat, необходимо добавить поставщика этого ресурса.

# 14.2. Добавление внешних поставщиков

### 14.2.1. Добавление экземпляра Red Hat Satellite для предоставления хостов

Добавьте экземпляр Satellite в виртуализированный ЦУ для предоставления хостов. Система виртуализации Red Hat версии 4.2 поддерживается Red Hat Satellite 6.1.

**Добавление экземпляра Satellite для предоставления хостов**

1. Нажмите **Администрирование → Поставщики**.
2. Нажмите **Добавить**.
3. Укажите **Имя** и **Описание**.
4. В выпадающем списке **Тип** выберите **Foreman/Satellite.**
5. В текстовом поле **URL поставщика** введите адрес URL или полное доменное имя машины, на которой установлен экземпляр Satellite. Номер порта указывать необязательно.

ВАЖНО

Для добавления экземпляра Satellite нельзя использовать адреса IP.

1. Отметьте галочкой пункт **Требуется аутентификация**.
2. Укажите **Имя пользователя** и **Пароль экземпляра** Satellite. Используется то же самое имя пользователя и пароль, что и для авторизации на портале Satellite.
3. Проверьте данные учётной записи:
   1. Нажмите **Проверить**, чтобы узнать, будет ли успешной аутентификация на экземпляре Satellite с использованием предоставленных данных учётной записи.
   2. Если экземпляр Satellite использует SSL, то откроется окно **Импорт сертификатов поставщика**; нажмите **OK** для импортирования сертификата, предоставляемого экземпляром Satellite, чтобы обеспечить связь виртуализированного ЦУ с этим экземпляром.
4. Нажмите **OK**.

### 14.2.2. Добавление экземпляра образа OpenStack (Glance) для работы с образами

Добавьте экземпляр образа OpenStack (Glance) в виртуализированный ЦУ для работы с образами.

**Добавление экземпляра образа OpenStack (Glance) для управления образами**

1. Нажмите **Администрирование → Поставщики**.
2. Нажмите **Добавить** и введите подробности во вкладке **Общие параметры**. Подробные сведения смотрите в Разделе 11.2.10.
3. Введите **Имя** и **Описание**.
4. В выпадающем списке **Тип** выберите **Образ OpenStack** .
5. В текстовом поле **URL поставщика** введите адрес URL или полное доменное имя машины, на которой установлен экземпляр образа OpenStack.
6. Опционально, отметьте галочкой пункт **Требуется аутентификация** и введите **Имя пользователя** и **Пароль** для пользователя экземпляра образа OpenStack, зарегистрированного в Keystone. Также необходимо указать аутентификационный адрес URL сервера Keystone. Указав **Протокол** (HTTP), **Имя хоста** и **Порт API**.

Укажите **Арендатора** экземпляра образа OpenStack.

1. Проверьте данные учётной записи:
   1. Нажмите **Проверить**, чтобы узнать, будет ли успешной аутентификация на экземпляре образа OpenStack с использованием предоставленных данных учётной записи.
   2. Если экземпляр образа OpenStack использует SSL, то откроется окно **Импорт сертификатов поставщика**; нажмите **OK** для импортирования сертификата, предоставляемого экземпляром образа OpenStack , чтобы обеспечить связь виртуализированного ЦУ с этим экземпляром.
2. Нажмите **OK.**

### 14.2.3. Добавление экземпляра сетей OpenStack (Neutron) для предоставления сетей

Добавьте экземпляр сети OpenStack (neutron) для предоставления сети виртуализированному ЦУ. Для добавления сторонних поставщиков сетей с реализацией OpenStack Neutron REST API смотрите Раздел 11.2.9.

ВАЖНО

В качестве внешних поставщиков сетей система виртуализации Red Hat поддерживает следующие версии платформы OpenStack: 10, 13 и 14.

* OpenStack 10 нужно устанавливать с драйвером OVS.
* OpenStack 13 нужно устанавливать с драйверами OVS, OVN или ODL.
* OpenStack 14 нужно устанавливать с драйвером OVN или ODL.

Чтобы иметь возможность использовать сети neutron, на хостах должны быть настроены агенты neutron. Агенты можно настроить вручную, или же с помощью контроллера Red Hat OpenStack Platform развернуть роль Networker перед добавлением сетевого узла в виртуализированный ЦУ в виде хоста. Рекомендуется использовать контроллер. Автоматическое развёртывание агентов neutron во вкладке **Поставщик сети** окна **Новый хост** не поддерживается.

Хотя и сетевые узлы и обычные хосты можно использовать в одном кластере, виртуальные машины, использующие сети neutron, могут выполняться только на сетевых узлах.

**Добавление сетевого узла в виде хоста**

1. Используйте контроллер Red Hat OpenStack Platform для развёртывания роли Networker на сетевом узле.
2. Активируйте нужные репозитории:
   1. Register your system with the Content Delivery Network, entering your Customer Portal user name and password when prompted:

# subscription-manager register

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

# subscription-manager list --available

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

# subscription-manager attach --pool=poolid

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

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

* 1. Убедитесь в том, что все текущие установленные пакеты обновлены до последних версий:

# yum update

* 1. Перезагрузите машину, если обновлялись какие-либо пакеты ядра.

1. Установите ловушку сетей Openstack:

# yum install vdsm-hook-openstacknet

1. Добавьте сетевой узел в виртуализированный ЦУ в виде хоста. Смотрите Раздел 7.5.1.

ВАЖНО

Не выбирайте поставщика OpenStack Networking во вкладке *Поставщик сети*. На данный момент это действие не поддерживается.

**Добавление экземпляра сетей OpenStack (Neutron) для предоставления сети**

1. Нажмите **Администрирование → Поставщики**.
2. Нажмите **Добавить** и введите подробности во вкладке **Общие параметры**. Подробные сведения смотрите в Разделе 11.2.10.
3. Введите **Имя** и **Описание**.
4. В выпадающем списке **Тип** выберите **Сети OpenStack** .
5. Убедитесь в том, что в поле **Сетевой модуль** выбран **Open vSwitch**.
6. Опционально, отметьте галочкой пункт **Автоматическая синхронизация**. Это активирует автоматическую синхронизацию поставщика внешних сетей с существующими сетями.
7. В текстовом поле **URL поставщика** ведите адрес URL или полное доменное имя машины, на которой установлен экземпляр OpenStack Networking, а затем введите номер порта. Параметр **Только для чтения** выбран по умолчанию, что предотвращает внесение изменений в экземпляр OpenStack Networking со стороны пользователей.
8. Опционально, отметьте галочкой пункт **Требуется аутентификация** и введите **Имя пользователя** и **Пароль** для пользователя экземпляра OpenStack Networking, зарегистрированного в Keystone. Также необходимо указать аутентификационный адрес URL сервера Keystone, указав **Протокол**, **Имя хоста**, **Порт API** и **Версию API**.

Для API версии 2.0 укажите **Арендатора** экземпляра сетей OpenStack. Для API версии 3 укажите **Доменное имя пользователя**, **Имя проекта** и **Доменное имя проекта**.

1. Проверьте данные учётной записи:
   1. Нажмите **Проверить**, чтобы узнать, будет ли успешной аутентификация на экземпляре OpenStack Networking с использованием предоставленных данных учётной записи.
   2. Если экземпляр OpenStack Networking использует SSL, то откроется окно **Импорт сертификатов поставщика**; нажмите **OK** для импортирования сертификата, предоставляемого экземпляром OpenStack Networking , чтобы обеспечить связь виртуализированного ЦУ с этим экземпляром.
2. Перейдите на вкладку **Конфигурация агента**.

ПРЕДУПРЕЖДЕНИЕ

Следующие шаги предоставляются только в виде экспериментального функционала. Система виртуализации Red Hat поддерживает только предварительно настроенные хосты neutron.

1. В поле **Привязка интерфейсов** введите список отображений интерфейсов для агента Open vSwitch (список разделяется запятыми).
2. В списке **Тип брокера** выберите тип брокера сообщений, используемого экземпляром OpenStack Networking.
3. В поле **Хост** укажите URL или полное доменное имя хоста, на котором расположен брокер сообщений.
4. Укажите **Порт**, с которого будет выполняться подключение к брокеру сообщений. Если брокер не использует SSL, то по умолчанию используется порт 5762, а если SSL используется — 5761.
5. Укажите **Имя пользователя** и **Пароль** пользователя OpenStack Networking, зарегистрированного в экземпляре брокера сообщений.
6. Нажмите **OK**.

Экземпляр OpenStack Networking был добавлен в виртуализированный ЦУ. Перед тем, как начать использовать предоставляемые им сети, импортируйте их в виртуализированный ЦУ. Смотрите Раздел 6.3.1.

### 14.2.4. Добавление экземпляра блочного хранилища OpenStack (Cinder) для управления хранилищем

ВАЖНО

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

Добавьте экземпляр блочного хранилища OpenStack (Cinder) в виртуализированный ЦУ для управления хранилищем. Тома OpenStack Cinder предоставляются хранилищем Ceph.

**Добавление экземпляра OpenStack (Cinder) для управления хранилищем**

1. Нажмите **Администрирование → Поставщики**.
2. Нажмите **Добавить** и введите сведения во вкладке **Общие параметры**. Больше сведений об этом поле см. в Разделе 11.2.10.
3. Укажите **Имя** и **Описание**.
4. В выпадающем списке **Тип** выберите **Блочное хранилище OpenStack** .
5. Выберите **Дата-центр**, к которому будут прикреплены тома блочного хранилища OpenStack.
6. В текстовом поле **URL поставщика** ведите адрес URL или полное доменное имя машины, на которой установлен экземпляр блочного хранилища OpenStack, а затем введите номер порта.
7. Опционально, отметьте галочкой пункт **Требуется аутентификация** и введите **Имя пользователя** и **Пароль** для пользователя экземпляра блочного хранилищаOpenStack, зарегистрированного в Keystone. Также необходимо указать аутентификационный адрес URL сервера Keystone, указав **Протокол (**HTTP**)**, **Имя хоста** и **Порт API**.

Укажите **Арендатора** экземпляра блочного хранилища OpenStack .

1. Нажмите **Проверить**, чтобы узнать, будет ли успешной аутентификация на экземпляре блочного хранилища OpenStack с использованием предоставленных данных учётной записи.
2. Нажмите **OK**.
3. При включённой аутентификации Ceph (cephx) также необходимо выполнить следующие шаги. Протокол cephx по умолчанию включён.
   1. С помощью команды ceph auth get-or-create создайте на сервере Ceph новый секретный ключ для пользователя client.cinder . Если для этого пользователя ключ уже существует, получите его с помощью той же команды.
   2. На портале администрирования в списке **Поставщики** выберите только что созданного внешнего поставщика Cinder.
   3. Перейдите на вкладку **Ключи аутентификации**.
   4. Нажмите **Добавить**.
   5. В поле **Значение** укажите секретный ключ.
   6. Скопируйте автоматически созданный **UUID** или введите уже существующий UUID в текстовое поле.
   7. На сервере Cinder добавьте UUID из предыдущего шага и пользователя cinder в файл **/etc/cinder/cinder.conf**:

rbd\_secret\_uuid = UUID

rbd\_user = cinder

Подробности о создании диска блочного хранилища OpenStack (Cinder) смотрите в Разделе 10.6.1.

### 14.2.5. Добавление экземпляра VMware в качестве поставщика виртуальной машины

Добавление экземпляра VMware vCenter для импорта ВМ из VMware в виртуализированный ЦУ.

В системе виртуализации Red Hat для преобразования виртуальных машин VMware в корректный формат перед их импортом используется V2V. Как минимум на одном хосте должен быть установлен пакет virt-v2v. Пакет virt-v2v по умолчанию доступен на хостах виртуализации и устанавливается на стандартных хостах в качестве зависимости VDSM при добавлении в окружение виртуализации Red Hat. Стандартные хосты должны управляться ОС Red Hat Enterprise Linux 7.2 или более поздней.

ВНИМАНИЕ

Для архитектуры ppc64le пакет virt-v2v недоступен; эти хосты не могут использоваться качестве хостов прокси.

Добавление экземпляра VMware vCenter в качестве поставщика виртуальных машин

1. Нажмите **Администрирование → Поставщики**.
2. Нажмите **Добавить**.
3. Укажите **Имя** и **Описание**.
4. В выпадающем списке **Тип** выберите **Vmware**.
5. Выберите **Дата-центр**, в который будут импортированы машины Vmware, или же выберите **Любой дата-центр**, чтобы указать целевой дата-центр во время конкретных операций импорта.
6. В поле **vCenter** укажите адрес IP или полное доменное имя экземпляра VMware vCenter.
7. В поле **ESXi** укажите адрес IP или полное доменное имя хоста, с которого будут импортированы ВМ.
8. В поле **Дата-центр** укажите название дата-центра, в котором располагается указанный хост ESXi.
9. Если между хостом ESXi и виртуализированным ЦУ уже состоялся обмен сертификатами, оставьте отмеченным пункт **Проверить сертификат SSL сервера** для проверки сертификата хоста ESXi. В противном случае снимите галочку.
10. В выбранном дата-центре выберите хост с установленным пакетом virt-v2v , который будет служить **Хостом прокси** во время операций импорта ВМ. этот хост также должен иметь возможность подключиться к сети внешнего поставщика VMware vCenter. Если в шаге 5 был выбран **Любой дата-центр**, то хост нельзя будет выбрать сейчас, но его можно будет выбрать во время каждой конкретной операции импорта.
11. Укажите **Имя пользователя** и **Пароль** экземпляра VMware vCenter. У пользователя должен быть доступ к дата-центр VMware и хосту ESXi, на котором размещаются виртуальные машины.
12. Проверьте данные учётной записи:
    1. Нажмите **Проверить**, чтобы узнать, будет ли успешной аутентификация на экземпляре VMware vCenter с использованием предоставленных данных учётной записи.
    2. Если экземпляр VMware vCenter использует SSL, то откроется окно **Импорт сертификатов поставщика**; нажмите **OK** для импортирования сертификата, предоставляемого экземпляром VMware vCenter, чтобы обеспечить связь виртуализированного ЦУ с этим экземпляром.
13. Нажмите **OK**.

### 14.2.6. Добавление хоста RHEL 5 Xen в качестве поставщика виртуальных машин

Добавьте хост RHEL 5 Xen для импорта ВМ из Xen в систему виртуализации Red Hat.

В системе виртуализации Red Hat для преобразования виртуальных машин RHEL 5 Xen в корректный формат перед их импортом используется V2V. Как минимум на одном хосте должен быть установлен пакет virt-v2v. Пакет virt-v2v по умолчанию доступен на хостах виртуализации и устанавливается на стандартных хостах в качестве зависимости VDSM при добавлении в окружение виртуализации Red Hat. Стандартные хосты должны управляться ОС Red Hat Enterprise Linux 7.2 или более поздней.

ВНИМАНИЕ

Для архитектуры ppc64le пакет virt-v2v недоступен; эти хосты не могут использоваться качестве хостов прокси.

**Добавление экземпляра RHEL 5 Xen в качестве поставщика ВМ**

1. Включите аутентификацию по открытому ключу между хостом прокси и хостом RHEL 5 Xen:
   1. Авторизуйтесь на хосте прокси и создайте ключи SSH для пользователя **vdsm**.

# sudo -u vdsm ssh-keygen

* 1. Скопируйте открытый ключ пользователя **vdsm** на хост RHEL 5 Xen. Файл хоста прокси **known\_hosts** также будет обновлён для включения ключа хоста RHEL 5 Xen.

# sudo -u vdsm ssh-copy-id root@xenhost.example.com

* 1. Авторизуйтесь на хосте RHEL 5 Xen для проверки корректности авторизации.

# sudo -u vdsm ssh root@xenhost.example.com

1. Нажмите **Администрирование → Поставщики**.
2. Нажмите **Добавить**.
3. Укажите **Имя** и **Описание**.
4. В выпадающем списке **Тип** выберите **Xen**.
5. Выберите **Дата-центр**, в который будут импортированы машины Xen, или же выберите **Любой дата-центр**, чтобы указать целевой дата-центр во время конкретных операций импорта.
6. В поле **URI** укажите адрес URI хоста RHEL 5 Xen.
7. В выбранном дата-центре выберите хост с установленным пакетом virt-v2v , который будет служить **Хостом прокси** во время операций импорта ВМ. Этот хост также должен иметь возможность подключиться к сети внешнего поставщика RHEL 5 Xen. Если в шаге 5 был выбран **Любой дата-центр**, то хост нельзя будет выбрать сейчас, но его можно будет выбрать во время каждой конкретной операции импорта.
8. Нажмите **Проверить**, чтобы узнать, будет ли успешной аутентификация на хосте RHEL 5 Xen.
9. Нажмите **OK**.

### 14.2.7. Добавление хоста KVM в качестве поставщика виртуальных машин

Добавьте хост KVM для импортирования ВМ из KVM в систему виртуализации Red Hat.

**Добавление хоста KVM в качестве поставщика ВМ**

1. Включите аутентификацию по открытому ключу между хостом прокси и хостом KVM:
   1. Авторизуйтесь на хосте прокси и создайте ключи SSH для пользователя **vdsm**.

# sudo -u vdsm ssh-keygen

* 1. Скопируйте открытый ключ пользователя **vdsm** на хост KVM. Файл хоста прокси **known\_hosts** также будет обновлён для включения ключа хоста KVM.

# sudo -u vdsm ssh-copy-id root@kvmhost.example.com

* 1. Авторизуйтесь на хосте KVM для проверки корректности авторизации.

# sudo -u vdsm ssh root@kvmhost.example.com

1. Нажмите **Администрирование → Поставщики**.
2. Нажмите **Добавить**.
3. Укажите **Имя** и **Описание**.
4. В выпадающем списке **Тип** выберите **KVM**.
5. Выберите **Дата-центр**, в который будут импортированы машины KVM, или же выберите **Любой дата-центр**, чтобы указать целевой дата-центр во время конкретных операций импорта.
6. В поле **URI** укажите адрес URI хоста KVM.

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

1. В выбранном дата-центре выберите хост, который будет служить **Хостом прокси** во время операций импорта ВМ. Этот хост также должен иметь возможность подключиться к сети внешнего поставщика KVM. Если в шаге 5 был выбран **Любой дата-центр**, то хост нельзя будет выбрать сейчас. Это поле будет неактивно со значением **Любой хост в дата-центре**. Хост можно будет выбрать во время каждой конкретной операции импорта.
2. Опционально, отметьте галочкой пункт Требует аутентификации и укажите Имя пользователя и Пароль хоста KVM. Пользователь должен иметь доступ к хосту KVM, на котором размещаются ВМ.
3. Нажмите **Проверить**, чтобы узнать, будет ли успешной аутентификация на хосте KVM.
4. Нажмите **OK**.

### 14.2.8. Добавление Open Virtual Network (OVN) в качестве внешнего поставщика сетей

Open Virtual Network (OVN) предоставляет возможность создания сетей без добавления виртуальных LAN или изменения инфраструктуры. OVN — это модуль Open vSwitch (OVS), включающий поддержку виртуальных сетей путём добавления встроенной поддержки OVS для виртуальных перекрытий L2 и L3.

Можно установить нового поставщика сетей OVN (Раздел 11.2.8.1) или добавить уже существующего (Раздел 11.2.8.2).

Также можно подключить сеть OVN к встроенной сети системы виртуализации Red Hat. Подробности смотрите в Разделе 11.2.8.5. Эта возможность доступна только как экспериментальная.

Neutron-подобный REST API предоставляется с помощью ovirt-provider-ovn, что даёт возможность создавать сети, подсети, порты и маршрутизаторы (подробности см. [OpenStack Networking API v2.0](https://developer.openstack.org/api-ref/network/v2/) , Англ.). Эти наложенные сети задействуют обмен информацией между виртуальными машинами.

ВНИМАНИЕ

В качестве внешнего поставщика, OVN поддерживается решением CloudForms, использующим OpenStack (Neutron) API.

Подробные сведения о OVS и OVN смотрите в документации OVS: <http://docs.openvswitch.org/en/latest/> и <http://openvswitch.org/support/dist-docs/> (Англ.).

#### 14.2.8.1. Установка нового поставщика сетей OVN

ПРЕДУПРЕЖДЕНИЕ

Если пакет openvswitch был уже установлен и имеет версию 1:2.6.1 (version 2.6.1, эпоха 1), то установка OVN закончится неудачно при попытке установки последней версии openvswitch . Подробности и решение смотрите на трекере ошибок Red Hat: [BZ#1505398](https://bugzilla.redhat.com/show_bug.cgi?id=1505398).

Во время установки OVN с помощью engine-setup, следующие шаги выполняются автоматически:

* Настройка центрального сервера OVN на машине виртуализированного ЦУ
* Добавление OVN в систему виртуализации Red Hat в качестве внешнего поставщика сетей.
* Настройка ovirt-provider-ovn в качестве сетевого поставщика по умолчанию для кластера по умолчанию (**Default).**
* Настройка подключений хостов к OVN после добавления в кластер.

Если команда engine-setup используется с файлом предварительно настроенных ответов, для установки OVN можно добавить следующую запись:

OVESETUP\_OVN/ovirtProviderOvn=bool:True

**Установка нового поставщика сетей OVN**

1. Установите OVN в виртуализированный ЦУ с помощью engine-setup. Во время установки будут задаваться следующие вопросы:

# Install ovirt-provider-ovn(Yes, No) [Yes]?:

* + При ответе Yes, engine-setup устанавливает ovirt-provider-ovn. Если engine-setup обновляет систему, этот запрос появится, только если ovirt-provider-ovn не был установлен ранее.
  + При ответе No, этот вопрос не будет больше задаваться до следующего запуска engine-setup. Если этот параметр понадобится снова, выполните engine-setup --reconfigure-optional-components.

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

Будет использовать пользователя по умолчанию с паролем, ранее указанным во время процесса установки. Этот параметр доступен только во время новых инсталляций.

# oVirt OVN provider user[admin]:

# oVirt OVN provider password[empty]:

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

ВНИМАНИЕ

Чтобы изменить метод аутентификации позднее, отредактируйте файл /etc/ovirt-provider-ovn/conf.d/10\_engine\_setup.conf или создайте новый файл /etc/ovirt-provider-ovn/conf.d/20\_engine\_setup.conf. Перезапустите службу ovirt-provider-ovn для применения изменений. Дополнительные сведения об аутентификации OVN миотрите в документации <https://github.com/oVirt/ovirt-provider-ovn/blob/master/README.adoc> (Англ.).

1. Добавьте хосты в кластер **Default** . На хостах, добавляемых в этот кластер, связь с OVN настраивается автоматически. Сведения о том, как добавить новые хосты, смотрите в Разделе 7.5.1.

Чтобы хосты использовали существующую сеть, не являющуюся сетью по умолчанию, смотрите сведения в Разделе 11.2.8.4.

1. Добавьте сети в кластер **Default** (смотрите Раздел 6.1.2) и отметьте галочкой пункт **Создать на внешнем поставщике**. ovirt-provider-ovn будет выбран по умолчанию.
2. Чтобы подключить сеть OVN ко встроенной сети системы виртуализации Red Hat , отметьте галочкой пункт **Подключиться к физической сети** и укажите используемую сеть системы виртуализации. Подробности и предварительные условия смотрите в Разделе 11.2.8.5.
3. В выпадающем параметре **Группы безопасности** укажите, будет ли сеть использовать группы безопасности. Более подробно просмотреть доступные параметры можно в Разделе 6.1.7. Теперь можно создавать ВМ, использующие сети OVN.

#### 14.2.8.2. Добавление существующего поставщика сетей OVN

Процесс добавления уже существующего центрального сервера OVN в качестве внешнего поставщика сетей состоит из следующих ключевых этапов:

* Установка поставщика OVN, прокси, использующегося виртуализированным ЦУ для обмена информацией с OVN. Поставщик OVN может быть установлен ан любой машине, но должен иметь связь с центральным сервером OVN и с виртуализированным ЦУ.
* Добавление поставщика OVN в систему виртуализации Red Hat в качестве поставщика внешних сетей.
* Создайте новый кластер, использующий OVN в качестве сетевого поставщика по умолчанию. На хостах, добавляемых в этот кластер, связь с OVN настраивается автоматически.

**Предварительные условия**

Поставщику OVN требуются следующие пакеты, которые должны быть доступны на машине поставщика:

* openvswitch-ovn-central
* openvswitch
* openvswitch-ovn-common
* python-openvswitch

Если эти пакеты недоступны в репозиториях, настроенных на машине поставщика, их можно скачать с сайта OVS: <http://openvswitch.org/download/>.

**Добавление существующего поставщика сетей OVN**

1. Установите и настройте поставщика OVN.
   1. Установите поставщика на соответствующей машине:

# yum install ovirt-provider-ovn

* 1. Если поставщик не устанавливается на той же машине, где установлен виртуализированный ЦУ, добавьте следующую запись в файл /etc/ovirt-provider-ovn/conf.d/10\_engine\_setup.conf (если файл не существует, создайте его):

[OVIRT]

ovirt-host=https://*имя\_хоста\_виртуализированного\_цу*

Это необходимо для аутентификации, если она используется.

* 1. Если поставщик не устанавливается на той же машине, где установлен центральный сервер OVN, добавьте следующую запись в файл /etc/ovirt-provider-ovn/conf.d/10\_engine\_setup.conf (если файл не существует, создайте его):

[OVN REMOTE]

ovn-remote=tcp:*IP\_центрального\_сервера\_*OVN:6641

* 1. Откройте в межсетевом экране порты 9696, 6641 и 6642 чтобы разрешить обмен информацией между поставщиком OVN, центральным сервером OVN и виртуализированным ЦУ. Это можно выполнить 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

* 1. Запустите и включите службу:

# systemctl start ovirt-provider-ovn

# systemctl enable ovirt-provider-ovn

* 1. Настройте прослушивание запросов на портах 6642 и 6641 центрального сервера OVN:

# ovn-sbctl set-connection ptcp:6642

# ovn-nbctl set-connection ptcp:6641

1. На портале администрирования нажмите Администрирование → Поставщики.
2. Нажмите **Добавить** и введите подробности во вкладке **Общие параметры**. Подробности об этих параметрах смотрите в Разделе 11.2.10.
3. Укажите **Имя** и **Описание**.
4. Выберите **Внешний поставщик сети** в списке **Тип**.
5. Щёлкните по текстовому полю Сетевой модуль и в выпадающем меню выберите **Сетевой поставщик oVirt для OVN**.
6. Опционально, отметьте галочкой пункт **Автоматическая синхронизация**. Будет включена автоматическая синхронизация поставщика внешней сети с существующими сетями.

ВНИМАНИЕ

По умолчанию, автоматическая синхронизация включена для сетевого поставщика **ovirt-provider-ovn**, созданного с помощью утилиты **engine-setup**.

1. В текстовом поле **URL поставщика** укажите адрес URL или полное доменное имя поставщика OVN, а затем номер порта. Если поставщик OVN и центральный сервер OVN находятся на разных машинах, это должен быть URL машины поставщика, а не центрального сервера. Если поставщик OVN находится на той же машине, что и виртуализированный ЦУ, адрес URL может быть адресом по умолчанию: <http://localhost:9696>.
2. Снимите галочку с пункта **Только для чтения**, чтобы разрешить создание новых сетей OVN из виртуализированного ЦУ.
3. Опционально, отметьте галочкой пункт **Требует аутентификации** и введите **Имя пользователя** и **Пароль** для пользователя внешнего поставщика, зарегистрированного в Keystone. Также необходимо настроить аутентификационный URL сервера Keystone, указав **Протокол**, **Имя хоста** и **Порт API**.

Опционально, укажите **Арендатора** внешнего поставщика.

Метод аутентификации должен быть указан в файле /etc/ovirt-provider-ovn/conf.d/10\_engine\_setup.conf (создайте его, если он не существует). Перезапустите службу ovirt-provider-ovn для применения изменений. Более подробные сведения об аутентификации в OVN смотрите по ссылке <https://github.com/oVirt/ovirt-provider-ovn/blob/master/README.adoc> (Англ.).

1. Проверьте данные учётной записи:
   1. Нажмите **Проверить**, чтобы узнать, будет ли успешной аутентификация в OVN с использованием предоставленных данных учётной записи.
   2. Если экземпляр OVN использует SSL, то откроется окно **Импорт сертификатов поставщика**; нажмите **OK** для импортирования сертификата, предоставляемого экземпляром OVN, чтобы обеспечить связь виртуализированного ЦУ с этим экземпляром.
2. Нажмите **OK**.
3. Создайте новый кластер, использующий OVN в качестве сетевого поставщика по умолчанию (см. Раздел 5.2.1), и в выпадающем списке **Поставщик сети по умолчанию** выберите OVN.
4. Добавьте хосты в кластер. На хостах, добавляемых в этот кластер, связь с OVN настраивается автоматически. Сведения о том, как добавить новые хосты, смотрите в Разделе 7.5.1.
5. Импортируйте или добавьте сети OVN в новый кластер. Сведения об импортировании сетей см. в Разделе 6.3.1. Сведения о создании новых сетей, использующих OVN, см. Раздел 9.1.2. Отметьте галочкой пункт **Создать на внешнем поставщике**. ovirt-provider-ovn выбирается по умолчанию.

Чтобы хосты использовали существующую сеть, не являющуюся сетью по умолчанию, смотрите сведения в Разделе 11.2.8.4.

Чтобы подключить сеть OVN к встроенной сети системы виртуализации Red Hat, отметьте галочкой пункт **Подключиться к физической сети** и укажите используемую сеть системы виртуализации Red Hat. Подробности и предварительные условия см. в Разделе 11.2.8.5.

Теперь можно создавать виртуальные машины, использующие сети OVN.

#### 14.2.8.3. Изменение параметров туннельной сети OVN с помощью набора сценариев Ansible

С помощью набора сценариев Ansible ovirt-provider-ovn-driver можно использовать длинные имена для изменения туннельных сетей OVN.

**Набор сценариев Ansible для изменения туннельных сетей 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. Ключ по умолчанию обычно находится в каталоге /etc/pki/ovirt-engine/keys .

**inventory**

Данные инвентаризации ВМ oVirt. Чтобы найти значение, используйте следующий сценарий:

/usr/share/ovirt-engine-metrics/bin/ovirt-engine-hosts-ansible-inventory.

**cluster\_name**

Название кластера, на котором нужно обновить имя.

**ovn\_central**

Адрес IP центрального сервера OVN. Этот адрес должен быть доступен для всех хостов.

**ovirt\_network**

Имя сети oVirt.

**ovn\_tunneling\_interface**

Имя сети VDSM.

ВНИМАНИЕ

Набор сценариев Ansible ovirt-provider-ovn-driver поддерживает использование либо параметра ovirt\_network , либо параметра ovn\_tunneling\_interface. Если в одном наборе сценариев будут присутствовать оба параметра, сценарии не сработают.

**Набор сценариев 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

**Набор сценариев 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

Для запуска набора сценариев Ansible на машине виртуализированного ЦУ перейдите в каталог /usr/share/ovirt-engine/playbooks .

#### 14.2.8.4. Настройка хостов для использования туннельной сети OVN

С помощью набора сценариев Ansible ovirt-provider-ovn-driver на хостах можно настроить использование другой существующей сети вместо сети по умолчанию ovirtmgmt . Доступ к этой сети должны иметь все хосты в кластере.

ВНИМАНИЕ

Набор сценариев Ansible ovirt-provider-ovn-driver обновляет существующие хосты. Набор сценариев необходимо запускать снова при добавлении в кластер новых хостов.

**Настройка использования туннельной сети OVN на хостах**

1. На машине диспетчера виртуализации перейдите в каталог **playbooks**:

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

1. Запустите 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=имя\_кластера ovn\_central=IP\_центр\_сервера\_OVN ovn\_tunneling\_interface=*имя*\_*сети*\_VDSM" ovirt-provider-ovn-driver.yml

Например:

# 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

ВНИМАНИЕ

IP\_центрального\_сервера\_OVN может располагаться в новой сети, но это не является требованием. IP\_центрального\_сервера\_OVN должен быть доступен со всех хостов.

Имя\_сети\_VDSM имеет ограничение в 15 символов. При настройке имени логической сети, имеющего более 15 символов или содержащего не-ASCII символы, будет автоматически создано имя из 15 символов. Инструкции по отображению таких имён смотрите в Разделе 19.7.1.

**Обновление информации о туннельной сети OVN на одном хосте**

Обновить информацию о туннельной сети OVN на одном хосте можно с помощью утилиты vdsm-tool:

# vdsm-tool ovn-config IP\_центрального\_сервера\_OVN IP\_туннеля\_или\_имя\_сети

**Пример 11.1. Обновление хоста с помощью vdsm-tool**

# vdsm-tool ovn-config 192.168.0.1 MyNetwork

#### 14.2.8.5. Подключение сети OVN к физической сети

ВАЖНО

Этот функционал зависит от поддержки Open vSwitch, которая в системе виртуализации Red Hat доступна только как экспериментальная возможность. Экспериментальные возможности не поддерживаются соглашениями об уровне обслуживания, могут иметь неполный функционал и не рекомендуются к использовании на производстве. Эти возможности предоставляют ранний доступ к будущим возможностям продукта, давая клиентам возможность протестировать функциональность и предоставлять отзывы, полезные для разработчиков.

Можно создать сеть внешнего поставщика, перекрывающую встроенную сеть системы виртуализации Red Hat таким образом, что будет создана видимость того, что виртуальные машины в каждой сети разделяют одну и ту же подсеть.

ВАЖНО

Если для сети OVN была создана подсеть, то ВМ, использующая эту сеть, получит адрес IP из подсети. Если необходимо, чтобы IP адрес был выделен физической сетью, не создавайте подсеть для сети OVN.

**Предварительные условия**

* **Тип коммутатора** в кластере должен быть указан как **OVS**. На хостах, добавляемых в этот кластер, не должны быть настроены никакие ранее созданные сети системы виртуализации Red Hat, такие, как мост **ovirtmgmt** .
* На хостах должна быть доступна физическая сеть. Это можно сделать принудительно, указав, что физическая сеть является требуемой для кластера (в окне **Управление сетями** или во вкладке **Кластер** окна **Новая логическая сеть**).

**Создание новой внешней сети, подключённой к физической сети**

1. Нажмите Вычисления → Кластеры.
2. Нажмите на имя кластера, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку Логические сети, а затем нажмите **Добавить сеть**.
4. Укажите **Имя** сети.
5. Отметьте галочкой пункт **Создать на внешнем поставщике**. ovirt-provider-ovn выбирается по умолчанию.
6. Отметьте галочкой пункт **Подключиться к физической сети**, если он не отмечен по умолчанию.
7. Выберите физическую сеть, к которой должна подключиться новая сеть:
   * Нажмите на переключатель **Сеть дата-центра** и выберите физическую сеть в выпадающем списке. Это рекомендуемый выбор.
   * Нажмите на переключатель **Заданный пользователем** и укажите имя физической сети. Если в физической сети включены метки VLAN, также необходимо выбрать пункт **Включить добавление тегов VLAN** и введите тег VLAN для этой физической сети.

ВАЖНО

Имя физической сети не должно иметь более 15 символов и не должно содержать специальных символов.

1. Нажмите **OK**.

### 14.2.9. Добавление поставщика внешней сети

В систему виртуализации Red Hat можно добавить любого поставщика с реализацией OpenStack Neutron REST API. Драйвер виртуального интерфейса должен поставляться реализатором поставщика внешней сети. Справка по развёртыванию сетевого поставщика и драйвера виртуального интерфейса доступна по ссылкам: <https://github.com/mmirecki/ovirt-provider-mock> и <https://github.com/mmirecki/ovirt-provider-mock/blob/master/docs/driver_instalation> (Англ.).

**Добавление поставщика внешней сети для предоставления сети**

1. Нажмите Администрирование → Поставщики.
2. Нажмите **Добавить** и введите значения во вкладке **Общие параметры**. Подробности об этих параметрах смотрите в Разделе 11.2.10.
3. Введите **Имя** и **Описание**.
4. В выпадающем списке **Тип** выберите **Поставщик внешней сети**.
5. Опционально, нажмите на текстовый блок **Сетевой модуль** и в выпадающем списке выберите соответствующий драйвер.
6. Опционально, отметьте галочкой пункт **Автоматическая синхронизация**. Это активирует автоматическую синхронизацию поставщика внешних сетей с существующими сетями. При добавлении поставщиков внешних сетей этот пункт по умолчанию отключён.

ВНИМАНИЕ

Для поставщика сети **ovirt-provider-ovn**, созданной с помощью утилиты **engine-setup**, автоматическая синхронизация по умолчанию включена.

1. В текстовом поле **URL поставщика** ведите адрес URL или полное доменное имя машины, на которой установлен поставщик внешней сети, а затем введите номер порта. Параметр **Только для чтения** отмечен по умолчанию, что предотвращает возможность внесения изменений пользователями в параметры сети.
2. Опционально, отметьте галочкой пункт **Требует аутентификации** и введите **Имя пользователя** и **Пароль** для пользователя внешнего поставщика, зарегистрированного в Keystone. Также необходимо настроить аутентификационный URL сервера Keystone, указав **Протокол**, **Имя хоста** и **Порт API**.  
     
   Опционально, укажите **Арендатора** внешнего поставщика.
3. Проверьте данные учётной записи:
   1. Нажмите **Проверить**, чтобы узнать, будет ли успешной аутентификация на поставщике внешней сети с использованием предоставленных данных учётной записи.
   2. Если поставщик использует SSL, то откроется окно **Импорт сертификатов поставщика**; нажмите **OK** для импортирования сертификата, предоставляемого поставщиком внешней сети, чтобы обеспечить связь виртуализированного ЦУ с этим экземпляром.
4. Нажмите **OK**.

Перед тем, как начать использовать сети этого поставщика, на хостах необходимо установить драйвер виртуального интерфейса и импортировать сети. Сведения об импорте сетей смотрите в Разделе 6.3.1.

### 14.2.10. Объяснение общих параметров добавления поставщика

Во вкладке **Общие** окна **Добавить поставщика** можно занести главные сведения о внешнем поставщике.

**Таблица 14.1. Добавить поставщика: общие параметры**

|  |  |
| --- | --- |
| **Параметр** | **Объяснение** |
| Имя | Имя, представляющее поставщика в виртуализированном ЦУ. |
| Описание | Человекочитаемое описание поставщика в простом текстовом формате. |
| Тип | Тип внешнего поставщика. Изменение этого параметра изменяет доступность различных полей для настройки поставщика.  **Foreman/Satellite**   * **URL поставщика**: URL или полное доменное имя машины, на которой размещается экземпляр Satellite. В конце адреса URL или полного доменного имени добавлять номер порта не требуется. * **Требует аутентификации:** даёт возможность указать, необходима ли поставщику аутентификация. При выборе **Foreman/Satellite** аутентификация обязательна. * **Имя пользователя**: имя пользователя для подключения к экземпляру Satellite. Это должно быть имя пользователя для авторизации на портале выделения ресурсов экземпляра Satellite. * **Пароль**: пароль, с помощью которого будет проходить аутентификация вышеуказанного пользователя. Это должен быть пароль для авторизации на портале выделения ресурсов экземпляра Satellite.   **Образ OpenStack**   * **URL поставщика**: адрес URL или полное доменное имя машины, на которой располагается служба образов OpenStack. В конце адреса URL или полного доменного имени необходимо добавить номер порта службы образов OpenStack. По умолчанию — 9292. * **Требует аутентификации:** даёт возможность указать, необходима ли аутентификация при доступе к службе образов OpenStack. * **Имя пользователя**: имя пользователя для подключения к серверу Keystone. Это должно быть именем пользователя службы образов OpenStack, зарегистрированного в экземпляре Keystone, участником которого является служба образов OpenStack. * **Пароль**: пароль, с помощью которого будет проходить аутентификация вышеуказанного пользователя. Это должен быть пароль для службы образов OpenStack, зарегистрированной на экземпляре Keystone, участником которого является служба образов OpenStack. * **Протокол**: протокол для связи с сервером Keystone. Здесь необходимо указать HTTP. * **Имя хоста**: адрес IP или имя хоста сервера Keystone. * **Порт API**: номер порта API сервера Keystone. * **Версия API**: версия службы Keystone. Здесь указано значение v2.0, и поле является неактивным. * **Имя арендатора**: имя арендатора OpenStack, членом которого является служба образов OpenStack.   **Сети OpenStack**   * **Сетевой модуль**: сетевой модуль, с помощью которого происходит подключение к серверу OpenStack Networking. Для сетей OpenStack единственным параметром является **Open vSwitch, он выбран по умолчанию.** * **Автоматическая синхронизация**: даёт возможность указать, будет ли поставщик автоматически синхронизироваться с существующими сетями. * **URL поставщика:** адрес URL или полное доменное имя машины, на которой располагается экземпляр OpenStack Networking. В конце адреса URL или полного доменного имени необходимо добавить номер порта OpenStack Networking. По умолчанию — 9696. * **Только для чтения**: даёт возможность указать, можно ли изменять параметры экземпляра OpenStack Networking на портале администрирования. * **Требует аутентификации:** даёт возможность указать, необходима ли аутентификация при доступе к службе OpenStack Networking. * **Имя пользователя**: имя пользователя для подключения к экземпляру OpenStack Networking. Это должно быть именем пользователя OpenStack Networking, зарегистрированного в экземпляре Keystone, участником которого является экземпляр OpenStack Networking. * **Пароль**: пароль, с помощью которого будет проходить аутентификация вышеуказанного пользователя. Это должен быть пароль для OpenStack Networking, зарегистрированной на экземпляре Keystone, участником которого является экземпляр OpenStack Networking. * **Протокол**: протокол для связи с сервером Keystone. По умолчанию — **HTTPS**. * **Имя хоста**: адрес IP или имя хоста сервера Keystone. * **Порт API**: номер порта API сервера Keystone. * **Версия API**: версия сервера Keystone, присутствует в URL. Если в URL указано v2.0, выберите **v2.0**, если v3— выбирайте v3.   При выборе версии v3 в поле **Версия API** появляются следующие поля:   * **Доменное имя пользователя**: имя пользователя, настроенное в домене.   В Keystone API v3 домены используются для определения административных границ объектов служб в OpenStack. Домены дают возможность группировать пользователей вместе в различных целях, таких, как настройка конфигураций отдельных доменов или параметры безопасности.   * **Имя проекта**: указывает имя проекта в OpenStack Identity API v3. * **Доменное имя проекта**: указывает доменное имя проекта в OpenStack Identity API v3.   При выборе версии **v2.0** в поле **Версия API** появляется следующее поле:   * **Имя арендатора**: появляется, только если в поле **Версия API** была выбрана версия v2. Имя арендатора OpenStack, членом которого является экземпляр OpenStack Networking.   **Том OpenStack**   * **Дата-центр**: дата-центр, к которому будут присоединены тома хранилища OpenStack Volume. * **URL поставщика:** адрес URL или полное доменное имя машины, на которой располагается экземпляр OpenStack Volume. В конце адреса URL или полного доменного имени необходимо добавить номер порта OpenStack Volume. По умолчанию — 8776. * **Требует аутентификации:** даёт возможность указать, необходима ли аутентификация при доступе к службе OpenStack Volume. * **Имя пользователя**: имя пользователя для подключения к серверу Keystone. Это должно быть именем пользователя OpenStack Volume, зарегистрированного в экземпляре Keystone, участником которого является экземпляр OpenStack Volume. * **Пароль**: пароль, с помощью которого будет проходить аутентификация вышеуказанного пользователя. Это должен быть пароль экземпляра тома OpenStack, зарегистрированной на экземпляре Keystone, участником которого является этот экземпляр тома OpenStack. * **Протокол**: протокол для связи с сервером Keystone. Необходимо указать значение HTTP. * **Имя хоста**: адрес IP или имя хоста сервера Keystone. * **Порт API**: номер порта API сервера Keystone. * **Версия API**: версия сервера Keystone. Здесь указано значение v2.0, и поле неактивно. * **Имя арендатора**: имя арендатора OpenStack, участником экземпляра которого является экземпляр тома OpenStack.   **VMware**   * **Дата-центр:** укажите дата-центр,в который будут импортированы виртуальные машины Vmware, или же выберите **Любой дата-центр**, чтобы указать целевой дата-центр во время конкретных операций импорта (функция **Импорт** во вкладке **Виртуальные машины**). * **vCenter**: адрес IP или полное доменное имя экземпляра VMware vCenter. * **ESXi**: адрес IP или полное доменное имя хоста, с которого будут импортированы ВМ. * **Дата-центр**: название дата-центра, в котором располагается указанный хостESXi. * **Кластер**: название кластера, в котором располагается указанный хостESXi. * **Проверить сертификат SSL сервера**: нужно ли проверять сертификат SSL сервера во время подключения. * **Хост прокси**: выберите хост в указанном дата-центре с установленным virt-v2v , который будет служить хостом во время операций импорта виртуальных машин. Этот хост также должен иметь подключение к сети внешнего поставщика VMware vCenter. При выборе пункта **Любой дата-центр** ранее, здесь нельзя будет выбрать хост, но его можно будет указать во время отдельных операций импорта (функция **Импорт** во вкладке **Виртуальные машины**). * **Имя пользователя**: имя пользователя для подключения к экземпляру VMware vCenter. У пользователя должен быть доступ к в дата-центру VMware и хосту ESXi, на котором располагаются ВМ. * **Пароль**: пароль, с помощью которого выполняется аутентификация вышеуказанного пользователя.   **RHEL 5 Xen**   * **Дата-центр:** укажите дата-центр, в который будут импортированы виртуальные машины Xen, или же выберите **Любой дата-центр**, чтобы указать целевой дата-центр во время конкретных операций импорта (функция **Импорт** во вкладке **Виртуальные машины**). * **URI**: адрес URI хоста RHEL 5 Xen. * **Хост прокси**: выберите хост в указанном дата-центре с установленным virt-v2v , который будет служить хостом во время операций импорта виртуальных машин. Этот хост также должен иметь подключение к сети внешнего поставщика RHEL 5 Xen. При выборе пункта **Любой дата-центр** ранее, здесь нельзя будет выбрать хост, но его можно будет указать во время отдельных операций импорта (функция **Импорт** во вкладке **Виртуальные машины**).   **KVM**   * **Дата-центр:** укажите дата-центр, в который будут импортированы виртуальные машины KVM, или же выберите **Любой дата-центр**, чтобы указать целевой дата-центр во время конкретных операций импорта (функция **Импорт** во вкладке **Виртуальные машины**). * **URI**: адрес URI хоста KVM. * **Хост прокси**: выберите хост в указанном дата-центре с установленным virt-v2v , который будет служить хостом во время операций импорта виртуальных машин. Этот хост также должен иметь подключение к сети внешнего поставщика KVM. При выборе пункта **Любой дата-центр** ранее, здесь нельзя будет выбрать хост, но его можно будет указать во время отдельных операций импорта (функция **Импорт** во вкладке **Виртуальные машины**). * **Требует аутентификации:** даёт возможность указать, необходима ли аутентификация при доступе к хосту KVM. * **Имя пользователя**: имя пользователя для подключения к хосту KVM. * **Пароль**: пароль, с помощью которого выполняется аутентификация вышеуказанного пользователя.   **Внешний поставщик сети**   * **Сетевой модуль**: определяет, какая реализация драйвера будет использоваться на хосте для обработки операций на физическом сетевом интерфейсе. Если в качестве поставщика сети кластера по умолчанию добавлен поставщик с сетевым модулем oVirt Network Provider for OVN, то он также определяет, какой из драйверов будет установлен на хостах, добавляемых в кластер. * **Автоматическая синхронизация**: даёт возможность указать, будет ли поставщик автоматически синхронизироваться с существующими сетями. * **URL поставщика:** адрес URL или полное доменное имя машины, на которой располагается внешний поставщик сетей. В конце адреса URL или полного доменного имени необходимо добавить номер порта внешнего поставщика сетей. По умолчанию — 9696. * **Только для чтения:** даёт возможность указать, можно ли изменять параметры внешнего поставщика на портале администрирования. * **Требует аутентификации:** даёт возможность указать, необходима ли аутентификация при доступе к внешнему поставщику. * **Имя пользователя**: имя пользователя для подключения к поставщику внешних сетей. При аутентификации в Active Directory имя пользователя должно быть в формате *имя\_пользователя*@*домен*@*профиль\_аутентификации* вместо формата по умолчанию *имя\_пользователя*@*домен*. * **Пароль**: пароль, с помощью которого выполняется аутентификация вышеуказанного пользователя. * **Протокол**: протокол для связи с сервером Keystone. По умолчанию — **HTTPS**. * **Имя хоста**: адрес IP или имя хоста сервера Keystone. * **Порт API**: номер порта API сервера Keystone. * **Версия API**: версия сервера Keystone. Здесь указано значение v2.0, и поле неактивно. * **Имя арендатора**: опционально. Имя арендатора, участником которого является внешний поставщик. |
| Проверить | Даёт возможность проверить указанные данные учётной записи. Эта кнопка доступна для всех типов поставщиков. |

### 14.2.11. Объяснение пунктов вкладки «Параметры агента» окна «Добавить поставщика»

Во вкладке **Параметры агента** окна **Добавить поставщика** можно заполнить сведения о сетевых модулях. Эта вкладка доступна только для типа поставщика **Сети OpenStack**.

**Таблица 14.2. Добавить поставщика: Параметры агента**

|  |  |
| --- | --- |
| **Параметр** | **Объяснение** |
| **Наложения интерфейсов** | Список отображений, через запятую, в формате *метка:интерфейс*. |
| **Тип брокера** | Тип брокера сообщений, используемого в экземпляре OpenStack Networking. Выбирайте **RabbitMQ** или **Qpid.** |
| Хост | Адрес URL или подное доменное имя машины, на которой установлен брокер сообщений. |
| Порт | Удалённый порт, с которого выполняется подключение к вышеозначенному хосту. По умолчанию, если на хосте активирован SSL, номер порта — 5761, если SSL не активирован — 5762. |
| Имя пользователя | Имя пользователя для аутентификации вышеуказанного экземпляра сетей OpenStack на брокере сообщений. По умолчанию, имя этого пользователя — neutron. |
| Пароль | Пароль, с помощью которого выполняется аутентификация вышеуказанного имени пользователя. |

**14.3. Изменение параметров внешнего поставщика**

**Изменение параметров внешнего поставщика**

1. Нажмите Администрирование → Поставщики и выберите нужного поставщика.
2. Нажмите Изменить.
3. Измените текущие значения параметров на нужные.
4. Нажмите **OK**.

**14.4. Удаление внешних поставщиков**

**Удаление внешнего поставщика**

1. Нажмите Администрирование → Поставщики и выберите поставщика для удаления.
2. Нажмите **Удалить**.
3. Нажмите **OK**.

# Часть III. Администрирование окружения

# Глава 15. Администрирование виртуализированного ЦУ

## 15.1. Обслуживание виртуализированного ЦУ

#### Режимы обслуживания виртуализированного ЦУ

Режимы обслуживания дают возможность запускать, останавливать и изменять виртуальную машину диспетчера виртуализации, не вмешиваясь в работу агентов высокой доступности, а также перезапускать и изменять параметры узлов виртуализированного ЦУ в окружении, не вмешиваясь в работу виртуализированного ЦУ.

Следующие три режима обслуживания можно применять принудительно:

* global – отключает мониторинг состояния ВМ диспетчера виртуализации со стороны всех агентов высокой доступности. Глобальный режим обслуживания необходимо применять для любых операций настройки или обновления ПО, во время которых останавливается служба ovirt-engine, таких, как обновление до последней версии системы виртуализации Red Hat.
* local – отключает мониторинг состояния ВМ диспетчера виртуализации со стороны агента высокой доступности на узле, подающем команду. Узел освобождается от обязанности размещения на нём ВМ диспетчера виртуализации на всё время, пока применяется этот режим обслуживания; если во время применения этого режима на узле размещалась ВМ диспетчера виртуализации, диспетчер мигрирует на другой узел, при его наличии. Локальный режим облуживания рекомендуется применять во время внесения изменений в параметры системы или при обновлении версий ПО узла виртуализированного ЦУ.
* none – отключает режим обслуживания, обеспечивая работу агентов высокой доступности.

#### Применение режима локального обслуживания

Остановка агента высокой доступности на одном узле виртуализированного ЦУ.

**Применение локального режима обслуживания с портала администрирования**

1. Поместите узел виртуализированного ЦУ а режим локального обслуживания:
   1. На портале администрирования нажмите **Вычисления → Хосты** и выберите узел виртуализированного ЦУ.
   2. Нажмите **Управление → Обслуживание**. Локальный режим обслуживания будет автоматически запущен для выбранного узла.
2. После завершения задач по обслуживанию, отключите режим обслуживания:
   1. На портале администрирования нажмите Вычисления → Хосты и выберите узел виртуализированного ЦУ.
   2. Нажмите Управление → Активировать.

**Применение локального режима обслуживания из консольного режима**

1. Авторизуйтесь на узле виртуализированного ЦУ и поместите его в локальный режим обслуживания:

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

1. После завершения задач по обслуживанию, отключите режим обслуживания:

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

#### Применение режима глобального обслуживания

Остановка агентов высокой доступности на всех узлах виртуализированного ЦУ в кластере.

**Применение глобального режима обслуживания с портала администрирования**

1. Поместите все узлы виртуализированного ЦУ в режим глобального обслуживания:
   1. На портале администрирования нажмите **Вычисления → Хосты** и выберите любой узел виртуализированного ЦУ.
   2. Нажмите **Больше действий** (), затем нажмите **Включить глобальное обслуживание высокой доступности.**
2. После завершения задач по обслуживанию, отключите режим обслуживания:
   1. На портале администрирования нажмите **Вычисления → Хосты** и выберите любой узел виртуализированного ЦУ.
   2. Нажмите **Больше действий** (), затем нажмите **Выключить глобальное обслуживание высокой доступности.**

**Применение глобального режима обслуживания из консольного режима**

1. Авторизуйтесь на любом узле виртуализированного ЦУ и поместите его в глобальный режим обслуживания:

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

1. После завершения задач по обслуживанию, отключите режим обслуживания:

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

# 15.2. Администрирование виртуальной машины диспетчера виртуализации

В составе утилиты hosted-engine есть множество команд, помогающих в администрировании виртуальной машины диспетчера виртуализации. Утилиту hosted-engine можно запустить на любом из узлов виртуализированного ЦУ. Для просмотра всех доступных команд выполните hosted-engine --help. Дополнительные сведения о конкретной команде можно получить, выполнив hosted-engine --команда --help.

### 15.2.1. Обновление конфигурации виртуализированного ЦУ

Для обновления конфигурации виртуализированного ЦУ используйте команду hosted-engine --set-shared-config. Эта команда обновляет конфигурацию виртуализированного ЦУ в разделяемом домене хранения после начального развёртывания.

Для просмотра текущих значений параметров используйте команду hosted-engine --get-shared-config.

Для просмотра списка всех доступных ключей конфигурации и их соответствующих типов введите:

# hosted-engine --set-shared-config key --type=type --help

Где type может быть одним из следующих:

|  |  |
| --- | --- |
| he\_local | Настраивает значения в локальном экземпляре файла etc/ovirt-hosted-engine/hosted-engine.conf на локальном хосте, чтобы новые значения использовались только на этом хосте. Для активации новых значений перезапустите службы ovirt-ha-agent и ovirt-ha-broker. |
| he\_shared | Настраивает значения в файле etc/ovirt-hosted-engine/hosted-engine.conf в разделяемом хранилище, чтобы все хосты, разворачиваемые после изменения конфигурации, использовали эти значения. Чтобы применить на хосте новые значения, повторно разверните этот хост. |
| ha | Настраивает значения в файле /var/lib/ovirt-hosted-engine-ha/ha.conf локального хранилища. Новые значения применяются мгновенно. |
| broker | Настраивает значения в файле /var/lib/ovirt-hosted-engine-ha/broker.conf локального хранилища. Для активации новых значений перезапустите службу ovirt-ha-broker. |

### 15.2.2. Настройка почтовых уведомлений

Для любых переходов состояний высокой доступности на узлах виртуализированного ЦУ можно настроить почтовые уведомления. Обновление информации доступно для следующих ключей:

smtp-server, smtp-port, source-email, destination-emails и state\_transition.

**Чтобы настроить почтовые уведомления**:

1. На узле виртуализированного ЦУ укажите нужный адрес сервера SMTP для ключа smtp-server:

# hosted-engine --set-shared-config smtp-server smtp.example.com --type=broker

ВНИМАНИЕ

Для проверки обновлений в файле конфигурации виртуализированного ЦУ выполните:

# hosted-engine --get-shared-config smtp-server --type=broker

broker : smtp.example.com, type : broker

1. Проверьте, был ли ранее настроен порт SMTP по умолчанию (порт 25):

# hosted-engine --get-shared-config smtp-port --type=broker

broker : 25, type : broker

1. Укажите почтовый адрес, с которого сервер SMTP будет отправлять сообщения. Можно указать только один адрес.

# hosted-engine --set-shared-config source-email source@example.com --type=broker

1. Укажите целевой почтовый адрес для получения сообщений. Для указания нескольких адресов, разделяйте их запятыми.

# hosted-engine --set-shared-config destination-emails destination1@example.com,destination2@example.com --type=broker

Чтобы проверить корректность настройки SMTP в окружении виртуализированного ЦУ, измените статус высокой доступности на узле виртуализированного ЦУ и проверьте, было ли послано почтовое сообщение. Можно, например, изменить статус высокой доступности, поместив агентов высокой доступности в режим обслуживания. Подробности см. в Разделе 15.1.

# 15.3. Резервирование слотов памяти для виртуализированного ЦУ на дополнительных хостах

В случае выключения или необходимости миграции виртуальной машины диспетчера виртуализации, на узле виртуализированного ЦУ должно быть достаточно памяти для перезапуска или миграции на этот узел ВМ диспетчера виртуализации. Эта память может быть зарезервирована на нескольких узлах виртуализированного ЦУ с помощью политики планирования. Перед запуском или миграцией любых ВМ, политика планирования проверяет, останется ли на указанном числе дополнительных узлов виртуализированного ЦУ достаточно памяти для запуска ВМ диспетчера виртуализации.

Сведения о добавлении дополнительных узлов виртуализированного ЦУ смотрите в Разделе 15.4.

**Резервирование слотов памяти для виртуализированного ЦУ на дополнительных хостах**

1. Нажмите Вычисления → Кластеры и выберите кластер с узлами виртуализированного ЦУ.
2. Нажмите Изменить.
3. Перейдите на вкладку **Политика планирования**.
4. Нажмите **+** и выберите **HeSparesCount**.
5. Введите число дополнительных узлов виртуализированного ЦУ, на которых будет зарезервирован объём памяти, достаточный для запуска виртуальной машины виртуализированного ЦУ.
6. Нажмите OK.

# 15.4. Добавление узлов виртуализированного ЦУ

Узлы виртуализированного ЦУ добавляются тем же способом что и стандартные хосты, с дополнительным шагом развёртывания хоста в качестве узла виртуализированного ЦУ. Разделяемый домен хранения определяется автоматически, и узел в случае необходимости может использоваться как запасной хост для размещения ВМ диспетчера виртуализации. Стандартные хосты также возможно присоединять к окружению виртуализированного ЦУ, но они не могут размещать ВМ диспетчера виртуализации. Для обеспечения высокой доступности ВМ диспетчера виртуализации мы рекомендуем иметь как минимум два узла виртуализированного ЦУ. Дополнительные хосты также можно добавлять с помощью REST API.

**Дополнительные условия**

* При повторном использовании узла виртуализированного ЦУ, удалите на узле существующую конфигурацию виртуализированного ЦУ, см. Раздел 15.7.

ВАЖНО

При создании моста управления, использующего статический адрес IPv6, перед добавлением хоста отключите в конфигурации интерфейса моста управление со стороны network manager: укажите NM\_CONTROLLED=no в соответствующем файле ifcfg.

**Последовательность действий**

1. На портале администрирования нажмите **Вычисления → Хосты**.
2. Нажмите **Добавить**.
3. В выпадающем списке выберите **Дата-центр** и **Кластер хоста** для нового хоста.
4. Укажите **Имя** и **Адрес** нового хоста. В поле **Порт SSH** автоматически будет указан стандартный порт SSH, порт 22.
5. Выберите метод аутентификации, с помощью которого виртуализированный ЦУ будет получать доступ к хосту.
   * Для аутентификации по паролю укажите пароль root
   * Или же скопируйте ключ, показываемый в поле **Открытый ключ SSH**, в файл **/root/.ssh/authorized\_keys** на хосте, для использования аутентификации по открытому ключу.
6. Опционально, настройте управление питанием, если у хоста есть поддерживаемая карта.
7. Перейдите на вкладку **Виртуализированный ЦУ**.
8. Выберите **Развернуть**.
9. Нажмите OK.

**15.5. Повторная установка уже существующего хоста в качестве узла виртуализированного ЦУ**

Существующий стандартный хост в окружении виртуализированного ЦУ можно превратить в узел виртуализированного ЦУ с возможностью размещать ВМ диспетчера виртуализации.

**Последовательность действий**

1. Нажмите Вычисления → Хосты и выберите хост.
2. Нажмите Управление → Обслуживание и затем нажмите OK.
3. Нажмите Установка → Повторная установка.
4. Перейдите на вкладку **Виртуализированный ЦУ** и в выпадающем списке выберите **Развернуть**.
5. Нажмите OK.

Хост будет переустановлен с конфигурацией виртуализированного ЦУ и помечается значком короны на портале администрирования.

# 15.6. Загрузка виртуальной машины диспетчера виртуализации в режиме восстановления

В данном разделе описывается загрузка виртуальной машины диспетчера виртуализации в режиме восстановления в случае, если машина не запускается.

1. Подключитесь к одному из узлов виртуализированного ЦУ:

$ ssh root@адрес\_хоста

1. Переведите виртуализированный ЦУ в глобальный режим обслуживания:

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

1. Проверьте, присутствует ли уже работающий экземпляр ВМ диспетчера виртуализации:

# hosted-engine --vm-status

В случае, если экземпляр ВМ выполняется, подключитесь к её хосту:

# ssh root@адрес\_хоста

1. Выключите ВМ:

# hosted-engine --vm-shutdown

ВНИМАНИЕ

Если ВМ не выключается, выполните следующую команду:

# hosted-engine --vm-poweroff

1. Запустите машину диспетчера в приостановленном режиме:

hosted-engine --vm-start-paused

1. Укажите временный пароль VNC:

hosted-engine --add-console-password

Данная команда выводит всю информацию, необходимую для авторизации в системе VNC на ВМ диспетчера.

1. Авторизуйтесь на ВМ диспетчера виртуализации с помощью VNC. Машина диспетчера по-прежнему приостановлена, и кажется, что она зависла.
2. Возобновите выполнение ВМ диспетчера, выполнив следующую команду на её хосте:

ПРЕДУПРЕЖДЕНИЕ

После выполнения следующей команды появится меню загрузчика. Необходимо войти в режим восстановления до того, как загрузчик продолжит нормальный процесс загрузки. Перед тем, как выполнять данную команду, прочитайте описание следующего шага о вхождении в режим восстановления.

# /usr/bin/virsh -c qemu:///system?authfile=/etc/ovirt-hosted-engine/virsh\_auth.conf resume HostedEngine

1. Загрузите ВМ диспетчера виртуализации в режиме восстановления.
2. Отключите глобальный режим обслуживания:

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

Теперь на ВМ диспетчера можно выполнять задачи по восстановлению.

**15.7. Удаление хоста из окружения виртуализированного ЦУ**

Чтобы удалить узел виртуализированного ЦУ из окружения, поместите узел в режим обслуживания, сверните узел и, опционально, удалите его. После остановки служб высокой доступности и удаления конфигурационных файлов виртуализированного ЦУ, узлом можно управлять, как обычным хостом.

**Удаление хоста из окружения виртуализированного ЦУ**

1. На портале администрирования нажмите Вычисления → Хосты и выберите узел виртуализированного ЦУ.
2. Нажмите Управление → Обслуживание и затем нажмите OK.
3. Нажмите Установка → Повторная установка.
4. Перейдите на вкладку **Виртуализированный ЦУ** и в выпадающем списке выберите пункт **СВЕРНУТЬ УСТАНОВКУ**. Это действие останавливает работу служб ovirt-ha-agent и ovirt-ha-broker и удаляет файл конфигурации виртуализированного ЦУ.
5. Нажмите OK.
6. Опционально, нажмите **Удалить** для запуска окна подтверждения **Удалить хост(ы)** и нажмите OK.

# 15.8. Изменение полного доменного имени диспетчера виртуализации

Для изменения информации о записях полного доменного имени (FQDN) диспетчера виртуализации можно использовать команду ovirt-engine-rename.

Подробности смотрите в Разделе 22.1.3.

# Глава 16. Резервные копии и миграция

## 16.1. Создание и восстановление резервных копий диспетчера виртуализации

### 16.1.1. Обзор: создание резервных копий диспетчера виртуализации

Для регулярного создания резервных копий диспетчера виртуализации используйте утилиту engine-backup. Утилита создаёт резервные копии базы данных и конфигурационных файлов виртуализированного ЦУ в виде единого файла и не прерывая работу службы ovirt-engine.

### 16.1.2. Синтаксис команды engine-backup

Команда engine-backup работает в одном из двух базовых режимов:

# engine-backup --mode=backup

# engine-backup --mode=restore

Эти два режима далее расширяются с помощью набора параметров, дающих возможность указать область для резервного копирования и данные другой учётной записи для базы данных виртуализированного ЦУ. Чтобы просмотреть полный список параметров и их функцию, выполните engine-backup --help.

**Базовые параметры**

**--mode**

Указывает, будет ли команды выполнять операцию резервного копирования или операцию восстановления. Доступно два параметра: backup и restore. Это требуемый параметр.

**--file**

Уточняет путь и имя файла, в который будет записываться резервная копия в режиме создания, а также путь и имя файла, из которого будут восстанавливаться данные в режиме восстановления. Этот параметр является требуемым как в режиме создания, так и в режиме восстановления.

**--log**

Указывает путь и имя файла, в который будет писаться журнал операции создания резервной копии или её восстановления. Этот параметр является требуемым как в режиме создания, так и в режиме восстановления.

**--scope**

Указывает область операции резервирования или восстановления. Есть четыре параметра: all, для резервирования или восстановления всех баз данных и конфигураций; files, для резервирования или восстановления только файлов в системе; db, для резервирования или восстановления только базы данных диспетчера виртуализации; и dwhdb, для резервирования или восстановления только базы данных хранилища данных (Data Warehouse). Область по умолчанию — all.

В одной команде engine-backup параметр --scope можно указывать несколько раз.

**Параметры базы данных диспетчера виртуализации**

Следующие параметры доступны только при использовании команды engine-backup в режиме restore . Синтаксис параметра, приведённый ниже, применяется для восстановления базы данных диспетчера виртуализации. Аналогичный параметр существует для восстановления базы данных хранилища данных (Data Warehouse). Синтаксис параметра для хранилища данных смотрите в выводе engine-backup --help.

**--provision-db**

Создаёт базу данных PostgreSQL, в которую будет восстановлена база данных диспетчера. Это требуемый параметр при восстановлении из резервной копии на удалённом хосте или в свежей установке, где ещё нет настроенной базы данных PostgreSQL.

**--change-db-credentials**

Даёт возможность указать данные альтернативной учётной записи при восстановлении базы данных диспетчера виртуализации с использованием другой учётной записи, чем та, которая сохранена в резервной копии. Дополнительные ключи, требуемые для этого параметра, смотрите в выводе engine-backup –help.

**--restore-permissions or --no-restore-permissions**

Восстанавливает (или не восстанавливает) полномочия пользователей базы данных. При восстановлении из резервной копии требуется один из этих параметров.

ВНИМАНИЕ

Если резервная копия предоставляет базе данных дополнительных пользователей, то восстановление с параметрами --restore-permissions и --provision-db (или --provision-dwh-db) создаст дополнительных пользователей со случайными паролями. Если этим пользователям требуется доступ к восстановленной системе, то эти пароли необходимо будет сменить вручную. См. <https://access.redhat.com/articles/2686731>

### 16.1.3. Создание резервной копии с помощью команды engine-backup

Резервная копия диспетчера виртуализации может быть создана с помощью команды engine-backup при активном диспетчере. Для указания, какой тип резервной копии необходимо создать, добавьте один из следующих аргументов к параметру –scope:

* all: полная резервная копия всех баз данных и файлов конфигураций диспетчера виртуализации
* files: резервная копия только файлов в системе
* db: резервная копия только базы данных диспетчера
* dwhdb: резервная копия только базы данных хранилища данных

ВАЖНО

Для восстановления резервной копии в свежей установке диспетчера виртуализации одной резервной копии базы данных недостаточно; виртуализированному ЦУ требуется также доступ к файлам конфигурации. Любая резервная копия, указывающая другую область, чем область по умолчанию, т.е. all, должна также сопровождаться областью files, т.е. резервной копией файловой системы.

**Пример использования команды engine-backup**

1. Авторизуйтесь на машине, где выполняется виртуализированный ЦУ.
2. Создайте резервную копию:

**Пример 16.1. Создание полной резервной копии**

# engine-backup --scope=all --mode=backup --file=имя\_файла --log=имя\_файла\_журнала

**Пример 16.2. Создание резервной копии базы данных диспетчера виртуализации**

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

Для создания резервной копии базы данных хранилища данных (Data Warehouse), замените параметр db параметром dwhdb.

Для указанного пути и имени файла будет создан файл формата tar, содержащий резервную копию.

Теперь файлы tar, содержащие резервные копии, можно использовать для восстановления окружения.

### 16.1.4. Восстановление из резервной копии с помощью команды engine-backup

Процесс восстановления из резервной копии с помощью команды engine-backup состоит из большего числа шагов, чем процесс создания резервной копии, в зависимости от целевого места восстановления. Команду engine-backup можно, например, использовать для развёртывания резервных копий в свежую установку системы виртуализации Red Hat, поверх уже существующих установок и с использованием локальных или удалённых баз данных.

ВАЖНО

Резервные копии можно восстанавливать только в окружения, имеющие ту же мажорную версию релиза, что и система, для которой была создана резервная копия. Резервная копия системы виртуализации Red Hat с версией 4.2, например, может быть восстановлена только в другую систему виртуализации версии 4.2. Чтобы узнать версию системы виртуализации в резервной копии, распакуйте её и просмотрите значение в файле *****version*****, расположенном в корневом каталоге распакованных файлов.

### 16.1.5. Восстановление резервной копии в свежую установку

Резервные копии можно разворачивать в свежую установку виртуализированного ЦУ. Описываемая ниже последовательность действий может быть выполнена на машине, где была установлена базовая ОС, а также требуемые пакеты виртуализированного ЦУ, но ещё не выполнялась команда engine-setup. Данная последовательность действий предполагает, что к файлам резервной копии есть доступ с машины, на которой будет разворачиваться эта резервная копия.

**Восстановление резервной копии в свежей установке**

1. Авторизуйтесь на машине диспетчера виртуализации. Если база данных виртуализированного ЦУ восстанавливается на удалённом хосте, то на этом хосте необходимо будет авторизоваться и выполнить необходимые действия. Аналогично, при восстановлении хранилища данных на удалённом хосте, на этом хосте также необходимо будет авторизоваться и выполнить необходимые действия.
2. Восстановите полную резервную копию или копию только базы данных.
   * Восстановите полную резервную копию:

# engine-backup --mode=restore --file=имя\_файла --log=имя\_файла\_журнала --provision-db --restore-permissions

Если в составе полной резервной копии восстанавливается также и хранилище данных, предоставьте дополнительную базу данных:

engine-backup --mode=restore --file=имя\_файла --log=имя\_файла\_журнала --provision-db --provision-dwh-db --restore-permissions

* + Восстановите резервную копию только базы данных, развернув только файлы конфигурации и резервную копию базы данных:

# engine-backup --mode=restore --scope=files --scope=db --file=имя\_файла --log=имя\_файла\_журнала --provision-db --restore-permissions

Пример выше разворачивает резервную копию базы данных виртуализированного ЦУ.

# engine-backup --mode=restore --scope=files --scope=dwhdb --file=имя\_файла --log=имя\_файла\_журнала --provision-dwh-db --restore-permissions

Пример выше разворачивает резервную копию базы данных хранилища данных.

В случае успеха выводится следующее сообщение:

You should now run engine-setup.

Done.

1. Запустите следующую команду и следуйте указаниям для настройки виртуализированного ЦУ, восстановленного из резервной копии:

# engine-setup

Виртуализированный ЦУ был восстановлен в версии, сохранённой в резервной копии. Информацию о смене полного доменного имени системы виртуализации Red Hat смотрите в Разделе 22.1.1.

### 16.1.6. Восстановление резервной копии для перезаписи уже существующей установки

С помощью команды engine-backup можно развернуть резервную копию на машине, где уже был установлен и настроен виртуализированный ЦУ. Это бывает удобно в ситуациях, когда была сделана резервная копия окружения, в параметры окружения были затем внесены изменения, и эти изменения необходимо откатить с помощью восстановления окружения из резервной копии.

Изменения, внесённые в параметры окружения со времени создания резервной копии, такие, как добавление или удаление хостов, не будут присутствовать в восстановленном окружении. Эти изменения следует внести повторно.

**Последовательность действий**

1. Авторизуйтесь на машине диспетчера виртуализации.
2. Удалите файлы конфигурации и очистите базы данных, связанных с виртуализированным ЦУ:

# engine-cleanup

Команда engine-cleanup только очищает базу данных диспетчера виртуализации; она не выполняет сброс базы данных и не удаляет пользователя-владельца базы данных.

1. Выполните полное восстановление или восстановление только базы данных. Нет необходимости создавать новую базу данных или указывать данные учётной записи, поскольку и пользователь и сама база данных уже существуют.
   * Полное восстановление:

# engine-backup --mode=restore --file=имя\_файла --log=имя\_файла\_журнала --restore-permissions

* + Восстановите резервную копию только базы данных, восстановив файлы конфигурации и резервную копию базы данных:

# engine-backup --mode=restore --scope=files --scope=db --scope=dwhdb --file=имя\_файла --log=имя\_файла\_журнала --restore-permissions

ВНИМАНИЕ

Чтобы восстановить только базу данных диспетчера виртуализации (если, например, база данных хранилища данных расположена на другой машине), опустите параметр --scope=dwhdb.

В случае успеха выводится следующее сообщение:

You should now run engine-setup.

Done.

1. Повторно настройте виртуализированный ЦУ:

# engine-setup

### 16.1.7. Восстановление резервной копии с другими учётными данными

Команда engine-backup может восстановить резервную копию на машине, где уже был установлен и настроен виртуализированный ЦУ, но данные учётной записи базы данных в резервной копии отличаются от данных учётной записи базы данных на машине. Это удобно в ситуациях, когда была сделана резервная копия установленной системы, и её нужно развернуть в другой системе.

ВАЖНО

При восстановлении из резервной копии в ситуации перезаписи уже существующей установки, для очистки существующей установки необходимо выполнить команду engine-cleanup перед запуском команды engine-backup. Команда engine-cleanup только очищает базу данных диспетчера виртуализации; она не выполняет сброс базы данных и не удаляет пользователя-владельца базы данных. Таким образом нет необходимости создавать новую базу данных или указывать данные её учётной записи. Тем не менее, если данные учётной записи владельца базы данных виртуализированного ЦУ неизвестны, их нужно сменить перед развёртыванием резервной копии.

**Развёртывание резервной копии с другими данными учётной записи**

1. Авторизуйтесь на машине виртуализированного ЦУ.
2. Выполните следующую команду и следуйте подсказкам для удаления файлов конфигурации виртуализированного ЦУ и очистки базы данных диспетчера виртуализации:

# engine-cleanup

1. Смените пароль владельца базы данных engine, если данные учётной записи этого пользователя неизвестны:
   1. Войдите в командную строку postgresql:

# su - postgres -c 'scl enable rh-postgresql10 -- psql'

* 1. Смените пароль пользователя-владельца базы данных engine:

postgres=# alter role имя\_пользователя encrypted password 'новый\_пароль';

При необходимости, повторите процедуру для пользователя-владельца базы данных ovirt\_engine\_history.

1. Восстановите полную резервную копию или резервную копию только базы данных с параметром --change-db-credentials для передачи данных учётной записи новой базы данных. Значение database\_location для локальной базы данных виртуализированного ЦУ — localhost.

ВНИМАНИЕ

В примерах ниже для каждой базы данных используется параметр --\*password без указания пароля, вследствие этого для каждой базы данных запрашивается пароль. Как вариант, для каждой базы данных можно использовать параметр --\*passfile=файл\_пароля, для безопасной передачи паролей утилите engine-backup без использования интерактивного ввода.

* 1. Восстановление полной резервной копии:

# engine-backup --mode=restore --file=имя\_файла --log=имя\_файла\_журнала --change-db-credentials --db-host=местоположение\_бд --db-name=имя\_бд --db-user=engine --db-password --no-restore-permissions

Если хранилище данных также восстанавливается как часть полной резервной копии, для дополнительной базы данных укажите пересмотренные данные учётной записи:

engine-backup --mode=restore --file=имя\_файла --log=имя\_файла\_журнала --change-db-credentials --db-host=местоположение\_бд --db-name=имя\_бд --db-user=engine --db-password --change-dwh-db-credentials --dwh-db-host=местоположение\_бд --dwh-db-name=имя\_бд --dwh-db-user=ovirt\_engine\_history --dwh-db-password --no-restore-permissions

* 1. Restore a database-only backup by restoring the configuration files and the database backup: Восстановите только резервную копию базы данных, развернув файлы конфигурации и резервную копию базы данных

# engine-backup --mode=restore --scope=files --scope=db --file=имя\_файла --log=имя\_файла\_журнала --change-db-credentials --db-host=местоположение\_бд --db-name=имя\_бд --db-user=engine --db-password --no-restore-permissions

Пример выше восстанавливает резервную копию базы данных диспетчера виртуализации.

# engine-backup --mode=restore --scope=files --scope=dwhdb --file=имя\_файла --log=имя\_файла\_журнала --change-dwh-db-credentials --dwh-db-host=местоположение\_бд --dwh-db-name=имя\_бд --dwh-db-user=ovirt\_engine\_history --dwh-db-password --no-restore-permissions

Пример выше восстанавливает резервную копию базы данных хранилища данных.

В случае успеха выводится следующее сообщение:

You should now run engine-setup.

Done.

1. Запустите следующую команду и следуйте указаниям для повторной настройки параметров межсетевого экрана и проверки корректности настройки службы ovirt-engine:

# engine-setup

### 16.1.8. Создание и восстановление резервной копии виртуализированного ЦУ

В новом виртуализированном окружении можно создавать резервную копию виртуализированного ЦУ, а также восстанавливать ЦУ из резервной копии. Используйте эту процедуру для таких задач, как миграция окружения в новый домен хранения виртуализированного ЦУ с другим типом хранилища.

При указании файла резервной копии во время развёртывания нового виртуализированного ЦУ, резервная копия восстанавливается на машине нового виртуализированного ЦУ, с новым доменом хранилища виртуализированного ЦУ. Старый ЦУ удаляется, а старый домен хранения виртуализированного ЦУ переименовывается и может быть удалён вручную после подтверждения корректной работы нового окружения. Настоятельно рекомендуется развёртывание на новом хосте; если хост, используемый для развёртывания, существовал в окружении, для которого была сделана резервная копия, он будет удалён из восстановленной базы данных для избежания конфликтов в новом окружении.

Процедура создания и восстановления резервной копии включает в себя следующие ключевые действия:

1. Создание резервной копии исходного виртуализированного ЦУ с помощью утилиты engine-backup.
2. Развёртывание нового виртуализированного ЦУ и восстановление резервной копии.
3. Активация репозиториев виртуализированного ЦУ на машине нового ЦУ.
4. Повторная установка узлов виртуализированного ЦУ для обновления их конфигурации.
5. Удаление старого домена хранилища виртуализированного ЦУ.

Данная процедура предполагает существование доступа к исходному виртуализированному ЦУ и возможности вносить изменения в его параметры.

**Предварительные условия**

* Полное доменное имя, подготовленное для диспетчера виртуализации и его хоста. Должны быть настроены записи прямого и обратного просмотра DNS. Новый виртуализированный ЦУ должен иметь такое же полное доменное имя, что и старый ЦУ.
* Версия исходного виртуализированного ЦУ должна быть обновлена до последней минорной версии. Версия ЦУ в резервной копии должна соответствовать версии нового ЦУ.
* В окружении должен присутствовать как минимум один стандартный хост. Этот хост (а также и любые другие стандартные хосты) должен оставаться активным для принятия роли диспетчера пула хранилища (SPM) и любых выполняющихся ВМ. Если стандартный хост ещё не выполняет роли SPM, переместите эту роль перед созданием резервной копии, выбрав стандартный хост и нажав пункты меню Управление → Выбрать в качестве SPM.

В случае отсутствия стандартных хостов, есть два способа добавить хост:

* + Удалите конфигурацию виртуализированного ЦУ с узла (но не удаляйте узел из окружения). Смотрите Раздел 15.7.
  + Добавьте новый стандартный хост. Смотрите Раздел 10.5.1.

#### 16.1.8.1. Создание резервной копии исходного виртуализированного ЦУ

Создайте резервную копию исходного виртуализированного ЦУ с помощью команды engine-backup и скопируйте файл резервной копии в отдельное местоположение, чтобы получить к нему доступ в любой момент во время процедуры.

**Последовательность действий**

1. Авторизуйтесь на одном из узлов виртуализированного ЦУ и переместите окружение в глобальный режим обслуживания:

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

1. Авторизуйтесь в исходном виртуализированном ЦУ и остановите службу ovirt-engine:

# systemctl stop ovirt-engine

# systemctl disable ovirt-engine

ВНИМАНИЕ

Хотя остановка работы исходного виртуализированного ЦУ не является обязательной, она рекомендуется, так как предохраняет окружение от изменений после создания резервной копии. Кроме того, таким образом предотвращается управление существующими ресурсами обоими виртуализированными ЦУ одновременно.

1. Выполните команду engine-backup, указав имя создаваемого файла резервной копии и имя создаваемого файла журнала процесса создания резервной копии:

# engine-backup --mode=backup --file=имя\_файла --log=имя\_файла\_журнала

1. Скопируйте файлы на внешний сервер. В примере ниже, storage.example.com является полным доменным именем сервера сетевого хранилища, где будет храниться резервная копия до того момента, когда она понадобится, а /backup/ — любой указанный каталог или путь.

# scp -p имя\_файла имя\_файла\_журнала storage.example.com:/backup/

1. Авторизуйтесь на одном из узлов виртуализированного ЦУ и выключите ВМ исходного виртуализированного ЦУ:

# hosted-engine --vm-shutdown

После создания резервной копии виртуализированного ЦУ разверните новый ЦУ и восстановите резервную копию на новой ВМ.

#### 16.1.8.2. Восстановление резервных копий в новом виртуализированном ЦУ

Запустите на новом хосте сценарий hosted-engine с параметром --restore-from-file=путь/до/имени\_файла для восстановления резервной копии виртуализированного ЦУ во время установки.

ВАЖНО

Если используется хранилище iSCSI, и если цель iSCSI фильтрует подключения согласно списку управления доступом инициатора, то установка может закончиться неудачно с ошибкой STORAGE\_DOMAIN\_UNREACHABLE. Чтобы предотвратить ошибку, необходимо перед началом развёртывания виртуализированного ЦУ обновить конфигурацию iSCSI:

* При развёртывании на существующем хосте необходимо обновить параметры инициатора iSCSI в файле /etc/iscsi/initiatorname.iscsi. Типизированное имя iSCSI (IQN) инициатора должно быть таким же, что и имя, ранее отображённое на цель iSCSI, или же обновлённым до нового IQN, если это применимо.
* При развёртывании на новом хосте необходимо обновить конфигурацию цели iSCSI, чтобы она могла принимать подключения с хоста.

Обратите внимание, что типизированное имя iSCSI можно обновить или на стороне хоста (инициатор iSCSI) или на стороне хранилища (цель iSCSI).

**Последовательность действий**

1. Скопируйте файл резервной копии на новый хост. В примере ниже, host.example.com является полным доменным именем хоста, а /backup/ — любой указанный каталог или путь.

# scp -p имя\_файла host.example.com:/backup/

1. Авторизуйтесь на новом хосте. Если установка выполняется на хосте виртуализации, то утилита для развёртывания виртуализированного ЦУ доступна по умолчанию. Если установка выполняется на стандартном хосте, пакет необходимо установить:

# yum install ovirt-hosted-engine-setup

1. Для запуска сценария мы рекомендуем использовать менеджер окон screen, в целях избежания потери сеанса в случае сбоя сети или терминала. Установите и запустите screen:

# yum install screen

# screen

В случае истечения времени ожидания сеанса или прерывания соединения, выполните screen -d -r для восстановления сеанса развёртывания.

1. Запустите сценарий hosted-engine, указав путь до файла резервной копии :

# hosted-engine --deploy --restore-from-file=backup/имя\_файла

Чтобы в любое время остановить выполнение сценария и прервать развёртывание, используйте **CTRL**+**D**.

1. Выберите **Yes** для начала установки.
2. Настройте сеть. Сценарий определяет сетевые карты, которые возможно использовать в качестве моста управления в окружении.
3. Если для установки ВМ нужно использовать другой программно-аппаратный комплекс, укажите путь до архива OVA. Для использования программно-аппаратного комплекса диспетчера виртуализации оставьте это поле пустым.
4. Укажите полное доменное имя ВМ диспетчера виртуализации.
5. Укажите пароль root диспетчера виртуализации
6. Укажите открытый ключ SSH, с помощью которого будет выполняться авторизация пользователя root, а также укажите, нужно ли активировать доступ для root по протоколу SSH.
7. Укажите конфигурацию ЦП и памяти виртуальной машины.
8. Введите адрес MAC виртуальной машины диспетчера виртуализации или примите случайно созданный. Если ВМ должна получать адрес IP с помощью DHCP, убедитесь, что для этого адреса MAC есть действительное резервирование DHCP, так как сценарий развёртывания сервер DHCP не настраивает.
9. Укажите сведения о сетевой конфигурации ВМ. При указании **Статической** сети, укажите адрес IP диспетчер виртуализации.

ВАЖНО

Статический адрес IP должен принадлежать той же подсети, что и хост. Если, например, хост находится в подсети 10.1.1.0/24, то IP ВМ диспетчера должен находиться в том же диапазоне (10.1.1.1-254/24).

1. Укажите, нужно ли добавлять записи для ВМ диспетчера виртуализации и базового хоста в файл /etc/hosts виртуальной машины. Необходимо убедиться в том, что имена хостов разрешаются.
2. Укажите имя и номер порта TCP сервера SMTP, почтовый адрес, с которого будут отсылаться уведомления, а также список, через запятую, адресов, получающих эти уведомления:
3. Укажите пароль пользователя admin@internal для доступа к порталу администрирования.

Сценарий создаст виртуальную машину. В случае установки программно-аппаратного комплекса диспетчера виртуализации это может занять некоторое время.

1. Выберите используемый тип хранилища:
   * Для типа NFS укажите версию, полный адрес и путь до хранилища, а также любые параметры монтирования.

ПРЕДУПРЕЖДЕНИЕ

Не используйте точку монтирования старого домена хранения виртуализированного ЦУ для нового домена, так как при этом существует риск потери данных ВМ.

* + Для типа iSCSI укажите сведения о портале и выберите цель и LUN из списков автоопределения. Во время развёртывания можно выбрать только одну цель iSCSI, но для подключения всех порталов из одной группы есть поддержка доступа по нескольким путям.

ВНИМАНИЕ

Чтобы иметь возможность указать более одной цели iSCSI необходимо включить доступ по нескольким путям до начала установки виртуализированного ЦУ. Также существует утилита [Multipath Helper](https://access.redhat.com/labs/multipathhelper/#/) , создающая сценарий для установки и настройки доступа по нескольким путям с различными параметрами.

* + Для хранилища Gluster укажите полный адрес и путь до хранилища, а также любые параметры монтирования.

ПРЕДУПРЕЖДЕНИЕ

Не используйте точку монтирования старого домена хранения для нового домена, так как при этом существует риск потери данных ВМ.

ВАЖНО

Поддерживаются только хранилища replica 3 Gluster. Убедитесь в том, что имеется следующая конфигурация:

В файле **/etc/glusterfs/glusterd.vol** на всех трёх серверах Gluster для параметра rpc-auth-allow-insecure укажите значение on.

option rpc-auth-allow-insecure on

Настройте том следующим образом:

gluster volume set \_volume\_ cluster.quorum-type auto

gluster volume set \_volume\_ network.ping-timeout 10

gluster volume set \_volume\_ auth.allow \\*

gluster volume set \_volume\_ group virt

gluster volume set \_volume\_ storage.owner-uid 36

gluster volume set \_volume\_ storage.owner-gid 36

gluster volume set \_volume\_ server.allow-insecure on

* + Для протокола Fibre Channel выберите LUN в списке автоопределения. Адаптеры шины хоста должен быть настроен и подключён, а LUN не должен содержать никаких существующих данных. Сведения о повторном использовании LUN смотрите в Разделе 11.5.8.

1. Укажите размер диска диспетчера виртуализации.

Сценарий будет продолжать работу до окончания установки.

1. Процесс установки изменяет ключи SSH диспетчера виртуализации. Чтобы клиентские машины могли получать доступ к новому диспетчеру без ошибок SSH, удалите запись исходного диспетчера виртуализации из файла .ssh/known\_hosts на всех клиентских машинах, ранее получавших доступ к исходному виртуализированному ЦУ.

По завершении развёртывания авторизуйтесь на ВМ диспетчера и подключите необходимые репозитории.

#### 16.1.8.3. Enabling the Red Hat Virtualization Manager Repositories

Подключение репозиториев.

#### 16.1.9.3. Повторная установка хостов

Переустановите хост виртуализации и стандартные хосты с помощью портала администрирования. В последовательность действий входят шаги по остановке и перезапуску работы хоста.

**Предварительные условия**

* Если миграция разрешена на уровне кластера, ВМ автоматически мигрируют на другой хост в кластере; поэтому рекомендуется выполнять переустановку хостов во время относительно низкой загрузки хостов.
* Убедитесь в том, что в кластере достаточные запасы памяти для выполнения обслуживания хоста. Если в кластере недостаточно памяти, процесс миграции ВМ зависнет и затем закончится неудачей. Снизить потребление памяти для этой операции можно, выключив некоторые ВМ до помещения хоста в режим облуживания.
* Перед выполнением переустановки убедитесь в том, что в кластере больше одного хоста. Не пытайтесь переустанавливать все хосты одновременно, поскольку один из хостов должен быть доступен для выполнения задач диспетчера пула хранилища (SMP).

**Последовательность действий**

1. Нажмите Вычисления → Хосты и выберите хост.
2. Нажмите Управление → Обслуживание.
3. Нажмите Установка → Переустановить для открытия окна **Установить хост**.
4. Перейдите на вкладку **Виртуализированный ЦУ** и в выпадающем списке выберите **РАЗВЕРНУТЬ**.
5. Нажмите **OK** чтобы переустановить хост.

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

ВАЖНО

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

Проверить статус нового окружения после переустановки узлов виртуализированного ЦУ можно с помощью следующей команды на одном из узлов:

# hosted-engine --vm-status

Во время восстановления старый домен хранения виртуализированного ЦУ был переименован, но не удалён из нового окружения, на случай неудачного восстановления. Убедившись, что окружение работает нормально, старый домен хранения можно удалить.

#### 16.1.9.4. Удаление домена хранения

В дата-центре есть домен хранения, который необходимо удалить из виртуализированного окружения.

**Последовательность действий**

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

Домен хранения будет навсегда удалён из окружения.

### 16.1.10. Переопределение виртуализированного ЦУ с помощью восстановления резервной копии

В случаях, когда к виртуализированному ЦУ есть доступ, но присутствуют такие проблемы, как повреждение базы данных или ошибка конфигурации, которую трудно откатить, предыдущее состояние окружения можно восстановить с помощью резервной копии, сделанной до того, как появились проблемы, в случае её наличия.

Процедура восстановления предыдущего состояния виртуализированного ЦУ включает в себя следующие шаги:

1. Поместите окружение в глобальный режим обслуживания.
2. Восстановите резервную копию на ВМ диспетчер виртуализации.
3. Отключите глобальный режим обслуживания.

Подробные сведения о параметрах engine-backup --mode=restore смотрите в Разделе 16.1.

#### 16.1.10.1. Активация глобального режима обслуживания

Перед выполнением любого процесса обновления или настройки параметров на ВМ диспетчера виртуализации, окружение виртуализированного ЦУ необходимо поместить в глобальный режим обслуживания.

**Последовательность действий**

1. Авторизуйтесь на узлах виртуализированного ЦУ и активируйте глобальный режим обслуживания:

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

1. Перед тем, как продолжить, убедитесь, что окружение находится в режиме обслуживания:

# hosted-engine --vm-status

Должно появиться сообщение, указывающее, что кластер находится в режиме обслуживания.

#### 16.1.10.2. Восстановление резервной копии для перезаписи существующей установки

С помощью команды engine-backup можно восстановить резервную копию на машине, где уже был установлен и настроен виртуализированный ЦУ. Это удобно в ситуациях, когда была сделана резервная копия окружения, затем в окружение были внесены изменения, которые необходимо откатить с помощью восстановления окружения из резервной копии.

Изменения, внесённые в параметры окружения после создания резервной копии, такие, как добавление или удаление хоста, не будут присутствовать в восстановленном окружении. Эти изменения необходимо будет выполнить снова.

**Последовательность действий**

1. Авторизуйтесь на машине диспетчера виртуализации.
2. Удалите файлы конфигурации и очистите базу данных, связанную с диспетчером:

# engine-cleanup

Команда engine-cleanup очищает только базу данных виртуализированного ЦУ; она не сбрасывает базу данных и не удаляет пользователя-владельца этой базы данных.

1. Восстановите полную резервную копию или резервную копию только базы данных. Нет необходимости создавать новую базу данных или указывать данные учётной записи базы данных поскольку и пользователь и база данных уже существуют.
   * Восстановите полную резервную копию:

# engine-backup --mode=restore --file=имя\_файла --log=имя\_файла\_журнала --restore-permissions

* + Восстановите резервную копию только базы данных, восстановив конфигурационные файлы и резервную копию базы данных:

# engine-backup --mode=restore --scope=files --scope=db --scope=dwhdb --file=имя\_файла --log=имя\_файла\_журнала --restore-permissions

ВНИМАНИЕ

Чтобы восстановить только базу данных диспетчера виртуализации (если, например, база данных хранилища данных расположена на другой машине), опустите параметр --scope=dwhdb.

В случае успеха будет показано следующее сообщение:

You should now run engine-setup.

Done.

1. Повторно настройте виртуализированный ЦУ

# engine-setup

#### 16.1.10.3. Отключение глобального режима обслуживания

**Последовательность действий**

1. Авторизуйтесь на ВМ диспетчера виртуализации и завершите её работу.
2. Авторизуйтесь на узах виртуализированного ЦУ и отключите глобальный режим обслуживания:

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

После выхода из режима глобального обслуживания, ovirt-ha-agent запускает виртуальную машину диспетчера виртуализации, после чего диспетчер стартует автоматически. Запуск диспетчера виртуализации может занимать до десяти минут.

1. Убедитесь в том, что окружение заработало:

# hosted-engine --vm-status

Выводимая информация включает в себя статус виртуализированного ЦУ (**Engine Status**), это должно быть одно из следующих значений:

{"health": "good", "vm": "up", "detail": "Up"}

ВНИМАНИЕ

Пока ВМ загружается и виртуализированный ЦУ не начал работу, виртуализированный ЦУ имеет статус:

{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}

В этом случае подождите несколько минут и попробуйте снова.

После того, как окружение снова заработало, можно запустить ранее остановленные ВМ и убедиться в том, что ресурсы в окружении ведут себя ожидаемым образом.

# 16.2. Миграция баз данных системы виртуализации Red Hat на удалённые серверы

### 16.2.1. Миграция базы данных диспетчера виртуализации на удалённый сервер

После начальной настройки диспетчера виртуализации (engine) можно перенести его базу данных на удалённый сервер баз данных. Для создания резервной копии базы данных и её восстановления на новом сервере используйте команду engine-backup.

На новом сервере базы данных должна быть установлена ОС Red Hat Enterprise Linux 7 и подключены репозитории.

##### Миграция базы данных диспетчера виртуализации на удалённый сервер

1. Авторизуйтесь на ВМ диспетчера виртуализации и остановите службу ovirt-engine, чтобы её работа не мешала процессу создания резервной копии:

# systemctl stop ovirt-engine.service

1. Создайте резервную копию базы данных engine:

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

1. Скопируйте файл резервной копии на новый сервер базы данных:

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

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

# yum install ovirt-engine-tools-backup

1. Восстановите базу данных на новом сервере базы данных. *Имя\_файла* — это файл резервной копии, скопированный с машины диспетчера виртуализации.

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

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

# systemctl start ovirt-engine.service

### 16.2.2. Миграция базы данных виртуализированного ЦУ на удалённый сервер

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

На новом сервере базы данных должна быть установлена ОС Red Hat Enterprise Linux 7 и подключены необходимые репозитории.

##### Миграция базы данных виртуализированного ЦУ на удалённый сервер

1. Авторизуйтесь на узле виртуализированного ЦУ и поместите окружение в режим обслуживания global. Это действие отключает агентов высокой доступности и предотвращает миграцию ВМ диспетчера во время выполнения процедуры:

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

1. Авторизуйтесь на машине диспетчера виртуализации и остановите службу ovirt-engine, чтобы её работа не мешала процессу создания резервной копии:

# systemctl stop ovirt-engine.service

1. Создайте резервную копию базы данных engine:

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

1. Скопируйте файл резервной копии на новый сервер базы данных:

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

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

# yum install ovirt-engine-tools-backup

1. Восстановите базу данных на новом сервере базы данных. *Имя\_файла* — это файл резервной копии, скопированный с машины диспетчера виртуализации.

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

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

# systemctl start ovirt-engine.service

1. Авторизуйтесь в виртуализированном ЦУ и отключите режим обслуживания, запустив выполнение агентов высокой доступности:

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

### 16.2.3. Миграция хранилища данных на отдельную машину

В данном разделе описывается, как перенести базу данных и службу хранилища данных из диспетчера виртуализации на отдельную машину. Размещение службы хранилища данных на отдельной машине снижает нагрузку на каждую отдельную машину и даёт возможность каждой из служб избежать потенциальных конфликтов, вызываемых разделением ресурсов ЦП и памяти с другими процессами.

Службу хранилища данных (Data Warehouse) можно перенести и подключить её к существующей базе данных хранилища данных (ovirt\_engine\_history), или же, перед миграцией службы, можно перенести базу данных хранилища данных на отдельную машину. Если база данных располагается на машине диспетчера виртуализации, то миграция базы данных в дополнение к миграции службы ещё более снижает уровень конкуренции за ресурсы на машине диспетчера. Базу данных можно перенести на ту же машину, на которую будет мигрировать и служба хранилища данных, а можно на машину, отделённую как от машины диспетчера виртуализации, так и от машины службы хранилища данных.

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

Миграция базы данных хранилища данных (ovirt\_engine\_history) должна выполняться до миграции службы хранилища данных. Для создания резервной копии базы данных и её восстановления используйте команду engine-backup.

Сведения о миграции только службы хранилища данных смотрите в Разделе 16.2.3.2.

На новом сервере базы данных должна быть установлена ОС Red Hat Enterprise Linux 7 и подключены необходимые репозитории.

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

1. Создайте резервную копию базы данных хранилища данных и её конфигурационных файлов на машине диспетчера виртуализации:

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

1. Скопируйте файл резервной копии с машины диспетчера на новую машину:

# scp /tmp/file\_name root@new.dwh.server.com:/tmp

1. Установите engine-backup на новой машине:

# yum install ovirt-engine-tools-backup

1. Установите пакет сервера PostgreSQL:

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

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

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

# systemctl enable rh-postgresql10-postgresql

# systemctl start rh-postgresql10-postgresql

1. Восстановите базу данных хранилища данных на новой машине. *Имя\_файла* — это файл резервной копии, скопированный с машины диспетчера виртуализации.

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

База данных хранилища данных теперь располагается на машине, отдельной от той, на которой располагается диспетчер виртуализации. После успешного восстановления базы данных хранилища данных выводится запрос на запуск команды engine-setup. Перед выполнением этой команды выполните миграцию службы хранилища данных.

#### 16.2.3.2. Миграция службы хранилища данных на отдельную машину

Служба хранилища данных, установленная и настроенная на машине диспетчера виртуализации, может мигрировать на отдельную машину. Размещение службы хранилища данных на отдельной машине помогает снизить нагрузку на машину диспетчера виртуализации.

Обратите внимание, что в данной процедуре выполняется миграция только службы хранилища данных.

Сведения о миграции базы данных хранилища данных (ovirt\_engine\_history) до начала миграции службы хранилища данных смотрите в Разделе 16.2.3.1.

**Предварительные условия**

* На одной и той же машине ранее должны были быть установлены и настроены диспетчер виртуализации и хранилище данных.
* Для настройки новой машины хранилища данных необходимо иметь следующие данные:
  + Пароль из файла диспетчера виртуализации **/etc/ovirt-engine/engine.conf.d/10-setup-database.conf** .
  + Разрешённый доступ с машины хранилища данных на порт TCP 5432 машины с базой данных диспетчера виртуализации.
  + Имя пользователя и пароль базы данных хранилища данных из файла диспетчера виртуализации **/etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-database.conf** . Если миграция базы данных ovirt\_engine\_history выполнялась согласно инструкции из Раздела 16.2.3.1, то резервная копия содержит эти учётные данные, настроенные ранее при развёртывании базы данных на этой машине.

Данная инструкция включает в себя четыре шага:

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

##### 16.2.3.2.1. Установка ПО на новой машине хранилища данных

Подключите репозитории системы виртуализации Red Hat и установите пакет настройки хранилищ данных на машине под управлением ОС Red Hat Enterprise Linux 7:

1. Подключите необходимые репозитории:
2. Убедитесь в том, что все установленные на данный момент пакеты обновлены до новейших версий:

# yum update

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

# yum install ovirt-engine-dwh-setup

##### 16.2.3.2.2. Останов работы службы хранилища данных на машине диспетчера виртуализации

1. Остановите работу службы хранилища данных:

# systemctl stop ovirt-engine-dwhd.service

1. Если база данных располагается на удалённой машине, доступ необходимо предоставить вручную, внеся изменения в файл **postgres.conf**. Измените файл **/var/opt/rh/rh-postgresql10/lib/pgsql/data/postgresql.conf** и измените строку **listen\_addresses** следующим образом:

listen\_addresses = '\*'

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

Если база данных располагается на машине диспетчера виртуализации и была настроена во время установки диспетчера виртуализации с нуля, то доступ предоставляется по умолчанию.

Дополнительные сведения о конфигурации и миграции базы данных хранилища данных смотрите в Разделе 16.2.3.1.

1. Перезапустите службу postgresql:

# systemctl restart rh-postgresql10-postgresql

##### 16.2.3.2.3. Настройка конфигурации новой машины хранилища данных

Порядок параметров конфигурации, показанный в данном разделе, может отличаться в зависимости от окружения.

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

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

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

# sed -i \

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

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

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

1. Запустите команду engine-setup, чтобы начать процесс создания конфигурации хранилища данных на машине:

# engine-setup

1. Для создания конфигурации хранилища данных нажмите **Ввод**:

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

1. Для принятия автоматически определённого имени хоста нажмите **Ввод**, или же введите альтернативное имя хоста и нажмите **Ввод**:

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

1. Для автоматического создания конфигурации межсетевого экрана нажмите **Ввод**, или же введите **No** и нажмите **Ввод**, чтобы сохранить существующую конфигурацию:

Setup can automatically configure the firewall on this system.

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

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

Если была выбрана автоматическая настройка, но ни один из диспетчеров межсетевого экрана не активен, будет предложено выбрать диспетчер межсетевого экрана из списка поддерживаемых возможностей. Введите название диспетчера межсетевого экрана и нажмите **Ввод**. Это применимо и в тех случаях, когда в списке присутствует только одно наименование.

1. Введите полное доменное имя и пароль диспетчера виртуализации. Чтобы принять значения по умолчанию в каждом из других полей, нажмите **Ввод**:

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

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

Please choose one of the following:

1 - Access remote engine server using ssh as root

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

(1, 2) [1]:

ssh port on remote engine server [22]:

root password on remote engine server engine-fqdn: password

1. Введите полное доменное имя и пароль машины базы данных диспетчера виртуализации. Чтобы принять значения по умолчанию в каждом из других полей, нажмите **Ввод**:

Engine database host []: manager-db-fqdn

Engine database port [5432]:

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

Engine database name [engine]:

Engine database user [engine]:

Engine database password: password

1. Подтвердите параметры установки:

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

Служба хранилища данных теперь настроена на удалённой машине. Переходите к отключению службы на машине диспетчера виртуализации.

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

1. Перезапустите диспетчер виртуализации на машине диспетчера:

# service ovirt-engine restart

1. Выполните следующую команду, чтобы внести изменения в файл **/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf** и указать значение **False** для параметров:

# sed -i \

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

-e 's;^\(OVESETUP\_DWH\_CONFIG/remoteEngineConfigured=bool\):True;\1:False;' \

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

1. Отключите службу хранилища данных:

# systemctl disable ovirt-engine-dwhd.service

1. Удалите файлы хранилища данных:

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

Служба хранилища данных теперь размещается на машине, отдельной от машины диспетчера виртуализации.

# 16.3. Создание и восстановление резервных копий виртуальных машин с помощью домена хранения резервных копий

### 16.3.1. Что такое домен хранения резервных копий

Домен хранения резервных копий — это домен, который может использоваться специально для хранения и миграции ВМ и шаблонов ВМ в целях создания резервных копий и восстановления в аварийных ситуациях, во время миграций, или при любых других моделях использования механизма резервный копий. Домен хранения резервных копий отличается от других доменов тем, что все ВМ в домене хранения резервных копий находятся в выключенном состоянии. В домене хранения резервных копий виртуальные машины выполняться не могут.

Доменом хранения резервных копий может стать любой домен хранения. Включить или отключить этот параметр можно, выставив или убрав галочку в диалоговом блоке **Управление доменом**. Активировать этот параметр можно только после того, как работа всех ВМ в этом домене хранения будет завершена.

ВМ, хранящуюся в домене хранения резервных копий, нельзя запустить. Диспетчер виртуализации блокирует это действие, а также любое другое действие, которое может сделать резервную копию недействительной. Тем не менее, можно запустить ВМ, созданную на базе шаблона, хранящегося в домене хранения резервных копий, если диски этой ВМ не являются частью домена хранения резервных копий.

Как и в случае других типов доменов хранения, домены хранения резервных копий можно присоединять к/отсоединять от дата-центров. Таким образом, в дополнение к функции хранения резервных копий, домены хранения резервных копий можно использовать для миграции ВМ между дата-центрами.

**Преимущества**

Укажем некоторые причины для использования доменов хранения резервных копий вместо доменов экспорта:

* В дата-центре может существовать несколько доменов хранения резервных копий, но только один домен экспорта.
* Домен хранения резервных копий можно выделить для создания резервных копий и восстановления в аварийных ситуациях.
* Резервные копии ВМ, шаблоны или снимки можно переместить в домен хранения резервных копий.
* По сравнению с доменами экспорта, в доменах хранения резервных копий процессы миграции большого числа ВМ, шаблонов или файлов OVF проходят значительно быстрее
* По сравнению с доменами экспорта, в доменах хранения резервных копий дисковое пространство используется более эффективно
* В отличие от доменов экспорта, которые поддерживают только хранение файлов, домены хранения резервных копий поддерживают как файловое (NFS, Gluster), так и блочное хранение (оптоволокно и iSCSI)
* Принимая во внимание ограничения, параметр хранения резервных копий для домена хранения можно включать и отключать динамически.

**Ограничения**

* Диски любых ВМ или шаблонов, располагающихся в домене хранения резервных копий, должны размещаться в этом же домене.
* Все ВМ в домене хранения должны быть выключены перед тем, как этот домен можно будет сделать доменом хранения резервных копий
* ВМ, хранящуюся в домене хранения резервных копий, нельзя запустить, так как при этом будет выполняться обработка дисковых данных
* Домены хранения резервных копий не предназначены для томов памяти, так как тома памяти поддерживаются только активными ВМ
* В домене хранения резервных копий нельзя выполнить предварительный просмотр ВМ
* Динамическая миграция ВМ в домен хранения резервных копий невозможна
* Домен хранения резервных копий не может быть главным доменом
* Домен виртуализированного ЦУ нельзя сделать доменом хранения резервных копий
* Не используйте домен хранения по умолчанию в качестве домена хранения резервных копий

### 16.3.2. Настройка домена хранения данных в качестве домена хранения резервных копий

**Предварительные условия**

* Диски любых ВМ или шаблонов, располагающихся в домене хранения резервных копий, должны размещаться в этом же домене
* Все ВМ в домене должны быть выключены

**Последовательность действий**

1. На портале администрирования выберите Хранилище → Домены.
2. Создайте новый домен хранения или выберите уже существующий и нажмите **Управление доменом**. Откроется диалоговый блок **Управление доменами**.
3. В **Дополнительных параметрах** отметьте галочкой пункт **Хранение резервных копий**.

Домен стал доменом хранения резервных копий.

### 16.3.3. Создание или восстановление резервной копии ВМ или снимка с помощью домена хранения резервных копий

Для выключенной ВМ или для снимка можно создать резервную копию. После этого резервную копию можно хранить в том же дата-центре и восстановить её при необходимости, или же выполнить её миграцию в другой дата-центр.

**Последовательность действий: создание резервной копии виртуальной машины**

1. Создайте домен хранения резервных копий. Смотрите Раздел 16.3.2.
2. Создайте новую ВМ на основе ВМ, для которой нужно создать резервную копию:
   * Для создания резервной копии снимка, сначала на базе этого снимка создайте ВМ.
   * Для создания резервной копии ВМ, машину сначала нужно клонировать. И перед тем, как продолжить, убедитесь в том, что клон выключен.
3. Экспортируйте новую ВМ в домен хранения резервных копий.

**Последовательность действий: восстановление ВМ из резервной копии**

1. Убедитесь в том, что домен хранения резервных копий, в котором хранится резервная копия ВМ, присоединён к дата-центру.
2. Импортируйте ВМ из домена хранения резервных копий. Смотрите Раздел 11.7.5.

**Сопутствующая информация**

* Раздел 11.7.2.
* Раздел 11.7.3
* Раздел 11.7.4.
* Раздел 11.7.5

# 16.4. Резервное копирование и восстановление виртуальных машин с помощью API резервного копирования и восстановления

### 16.4.1. API резервного копирования и восстановления

API резервного копирования и восстановления представляет собой набор функций, дающих возможность выполнять резервное копирование и восстановление ВМ, полностью или только на уровне файлов. API сочетает в себе несколько компонентов системы виртуализации Red Hat, таких, как динамические снимки и REST API для создания и работы с временными томами, которые можно подключить к ВМ, на которой установлено ПО для резервного копирования от независимого поставщика.

### 16.4.2. Создание резервной копии виртуальной машины

Используйте API резервного копирования и восстановления для резервного копирования ВМ. В данной процедуре подразумевается наличие двух ВМ: машина, для которой нужно создать резервную копию, и машина, на которой установлено ПО для резервного копирования (запасная машина).

**Создание резервной копии виртуальной машины**

1. С помощью REST API создайте снимок ВМ, для которой нужно создать резервную копию :

POST /api/vms/{vm:id}/snapshots/ HTTP/1.1

Accept: application/xml

Content-type: application/xml

<snapshot>

<description>BACKUP</description>

</snapshot>

ВНИМАНИЕ

Замените здесь {vm:id} на VM ID той виртуальной машины, для которой создаётся снимок. Этот идентификатор можно посмотреть на вкладке *Общее* окон *Новая ВМ* и *Параметры ВМ* на *Портале администрирования* и на *Портале ВМ*

При создании снимка ВМ, данные текущей конфигурации сохраняются в атрибуте data атрибута configuration в разделе initialization снимка.

ВАЖНО

Невозможно сделать снимки дисков, которые могут быть общими, а также дисков на базе прямых LUN.

1. Получите данные конфигурации виртуальной машины из атрибута data снимка:

GET /api/vms/{vm:id}/snapshots/{snapshot:id} HTTP/1.1

All-Content: true

Accept: application/xml

Content-type: application/xml

ВНИМАНИЕ

Замените здесь {vm:id} идентификатором ВМ, для которой ранее был сделан снимок. Замените {snapshot:id} на идентификатор снимка.

Добавьте заголовок All-Content: true , чтобы в ответе получить дополнительные данные OVF. Данные OVF в ответе XML располагаются в границах элемента конфигурации ВМ, <initialization><configuration>. Позже эти данные будут использованы для восстановления ВМ из резервной копии.

1. Получите идентификатор снимка:

GET /api/vms/{vm:id}/snapshots/ HTTP/1.1

Accept: application/xml

Content-type: application/xml

1. Идентифицируйте ID диска в снимке:

GET /api/vms/{vm:id}/snapshots/{snapshot:id}/disks HTTP/1.1

Accept: application/xml

Content-type: application/xml

1. Присоедините снимок к машине с установленным ПО для создания резервных копий в качестве вложения активного диска с корректным типом интерфейса (например, **virtio\_scsi**):

POST /api/vms/{vm:id}/diskattachments/ HTTP/1.1

Accept: application/xml

Content-type: application/xml

<disk\_attachment>

<active>true</active>

<interface>\_virtio\_scsi\_</interface>

<disk id="{disk:id}">

<snapshot id="{snapshot:id}"/>

</disk>

</disk\_attachment>

ВНИМАНИЕ

Замените здесь {vm:id} на идентификатор *запасной* машины, а не машины, для которой ранее был создан снимок. Замените {disk:id} на идентификатор диска. Замените {snapshot:id} на идентификатор снимка.

1. С помощью ПО, установленного на запасной машине, создайте резервную копию данных на диске-снимке.
2. Удалите вложение в виде диска-снимка с запасной ВМ:

DELETE /api/vms/{vm:id}/diskattachments/{snapshot:id} HTTP/1.1

Accept: application/xml

Content-type: application/xml

ВНИМАНИЕ

Замените здесь {vm:id} на идентификатор *запасной* ВМ, а не ВМ, для которой ранее был создан снимок. Замените {snapshot:id} на идентификатор снимка.

1. Опционально, удалите снимок:

DELETE /api/vms/{vm:id}/snapshots/{snapshot:id} HTTP/1.1

Accept: application/xml

Content-type: application/xml

ВНИМАНИЕ

Замените здесь {vm:id} на идентификатор ВМ, для которой ранее был сделан снимок. Замените {snapshot:id} на идентификатор снимка.

С помощью ПО, установленного на отдельной ВМ, мы создали резервную копию состояния ВМ на определённый момент времени.

### 16.4.3. Восстановление ВМ из резервной копии

Восстановите ВМ, для которой была создана резервная копия, с помощью API резервного копирования и восстановления. В данной процедуре подразумевается, что в наличии имеется ВМ, на которой установлено ПО, ранее использованное для создания резервной копии (запасная ВМ).

**Восстановление ВМ из резервной копии**

1. На портале администрирования создайте плавающий диск, где будет восстановлена резервная копия. Сведения о создании плавающего диска смотрите в Разделе 13.6.1.
2. Присоедините диск к запасной ВМ:

POST /api/vms/{vm:id}/disks/ HTTP/1.1

Accept: application/xml

Content-type: application/xml

<disk id="{disk:id}">

</disk>

ВНИМАНИЕ

Замените здесь {vm:id} на идентификатор *запасной* ВМ, а не той ВМ, для которой ранее была сделана резервная копия. Замените {disk:id} на идентификатор диска, подученный во время создания резервной копии ВМ.

1. С помощью ПО резервного копирования восстановите резервную копию диска.
2. Отсоедините диск от запасной ВМ:

DELETE /api/vms/{vm:id}/disks/{disk:id} HTTP/1.1

Accept: application/xml

Content-type: application/xml

<action>

<detach>true</detach>

</action>

ВНИМАНИЕ

Замените здесь {vm:id} на идентификатор этой *запасной* ВМ, в не ВМ, для которой ранее была сделана резервная копия. Замените {disk:id} на идентификатор диска.

1. Создайте новую ВМ, используя данные конфигурации восстанавливаемой ВМ:

POST /api/vms/ HTTP/1.1

Accept: application/xml

Content-type: application/xml

<vm>

<cluster>

<name>cluster\_name</name>

</cluster>

<name>\_NAME\_</name>

<initialization>

<configuration>

<data>

<!-- omitting long ovf data -->

</data>

<type>ovf</type>

</configuration>

</initialization>

...

</vm>

ВНИМАНИЕ

Чтобы во время создания ВМ переназначить любые значения в OVF, переопределите значение элемента, идущего перед или после элемента initialization . Но не внутри этого элемента.

1. Присоедините диск к новой ВМ:

POST /api/vms/{vm:id}/disks/ HTTP/1.1

Accept: application/xml

Content-type: application/xml

<disk id="{disk:id}">

</disk>

ВНИМАНИЕ

Замените здесь {vm:id} на идентификатор *новой* ВМ, а не той ВМ, для которой ранее была сделана резервная копия. Замените {disk:id} на идентификатор диска.

Виртуальная машина была восстановлена из резервной копии, созданной с использованием API резервного копирования и восстановления.