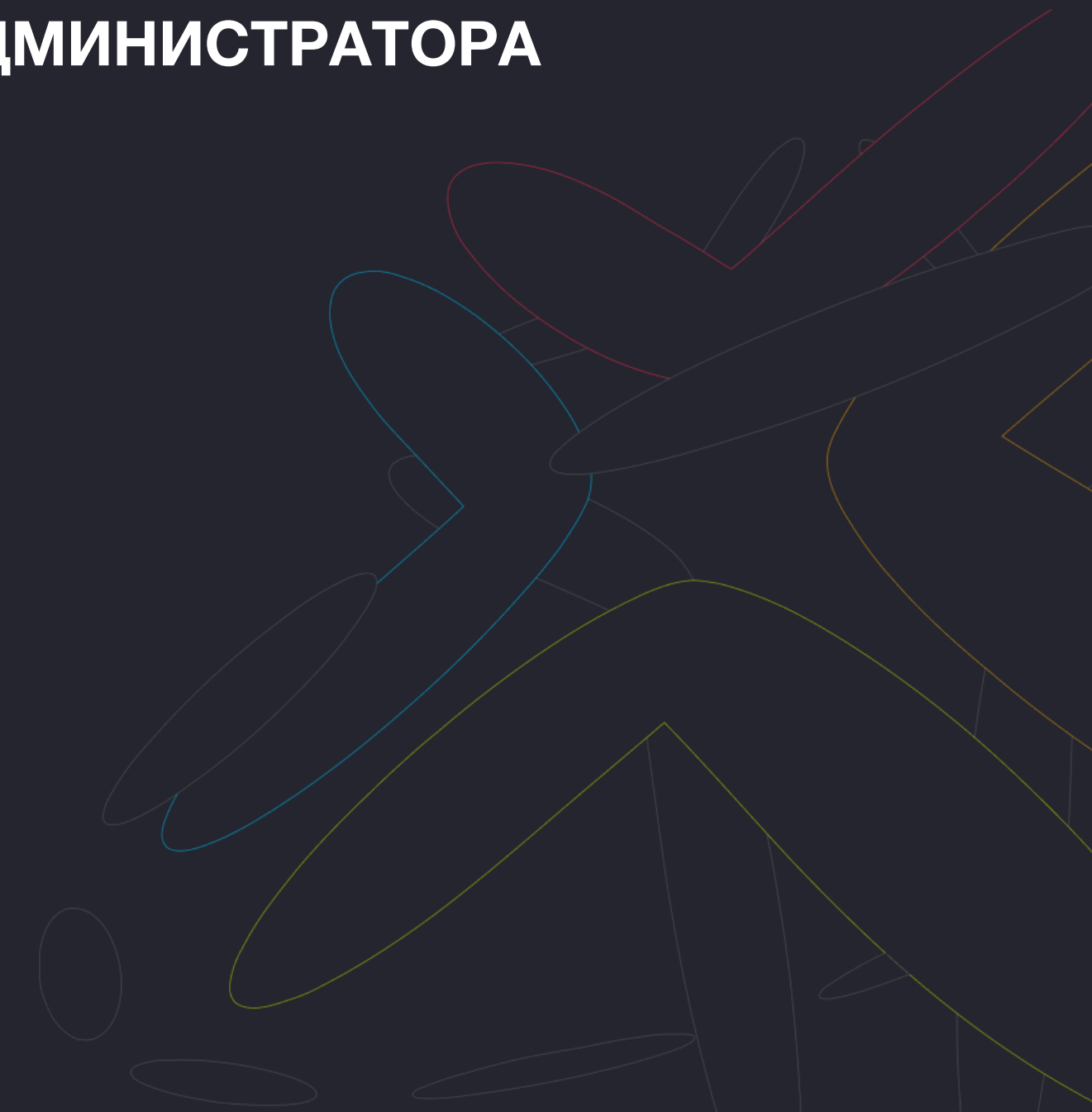
itkey

Руководство по эксплуатации KeyVirt для администратора



Оглавление

Список сокращений

API	Application Programming Interface	Программный интерфейс приложений, описание способов для обмена данными между приложениями
CLI	Command Line Interface	Интерфейс командной строки
CPU	Central Processor Unit	Центральный процессор
CSV	Comma-Separated Values	Текстовый формат для представления табличных данных
DRS	Distributed Resource Scheduler	Планировщик распределенных ресурсов
GPU	Graphical Processor Unit	Графический графический процессор, предназначенный для обработки графики и высокопроизводительных вычислений
HA	High Availability	Высокая доступность
IOPS	Input/Output Operations Per Second	Количество операций ввода-вывода в секунду, выполняемых системой хранения данных
IP-адрес	Internet Protocol Address	Уникальный сетевой адрес в сети передачи данных, построенный по протоколу IP (межсетевому протоколу передачи данных)
ISO-образ	Optical Disc Image	Образ оптического диска
KVM	Kernel-based Virtual Machine	Функция ПО, которую можно установить на физических компьютерах с ОС Linux в целях создания ВМ.
LAN	Local Area Network	Локальная вычислительная сеть
LUN	Logical Unit Number	Адрес блочного устройства (диска) с СХД
MAC-адрес	Media Access Control address	Уникальный аппаратный идентификатор оборудования
NAS	Network Attached Storage	Сетевое хранилище

NIC	Network Interface Controller	Сетевой адаптер
PCI passthrough	Peripheral Component Interconnect passthrough	Проброс устройств на шине PCI
RAM	Random Access Memory	Оперативная память
RDP	Remote Desktop Protocol	Протокол удаленного рабочего стола
REST	Representational State Transfer	Набор архитектурных принципов для построения распределенных масштабируемых веб-сервисов
SAN	Storage Area Network	Сеть хранения данных
SSH	Secure Shell	Сетевой протокол прикладного уровня, предназначеный для безопасного удаленного доступа к UNIX-системам
QEMU	Quick Emulator	Инструмент с открытым исходным кодом для эмуляции и виртуализации работы операционных систем на компьютере
QoS	Quality of Service	Качество обслуживания
vCPU	Virtual Central Processor Unit	Виртуальный процессор
vGPU	Virtual Graphical Processor Unit	Виртуальный графический процессор
VPN	Virtual Private Network	Виртуальная частная сеть
ВМ		Виртуальная машина
ОС		Операционная система
ПК		Персональный компьютер
ПО		Программное обеспечение
СХД		Система хранения данных
ЦОД		Дата-центр (центр обработки данных)

1 ВВЕДЕНИЕ

1.1 Описание программного продукта

KeyVirt – это платформа для управления виртуализацией, которая позволяет управлять виртуальными машинами и хранилищем при помощи различных технологий виртуализации, включая KVM, VMware и Xen. Платформа KeyVirt была создана на базе проекта oVirt. Основные преимущества KeyVirt – это гибкость и масштабируемость, что позволяет настроить виртуальную инфраструктуру под любые нужды и требования. KeyVirt также предлагает широкий спектр функций для управления виртуальными машинами, хранилищами и сетями.
Виртуальная машина – это программная реализация компьютера. Среда KeyVirt позволяет создавать виртуальные рабочие столы и виртуальные серверы. Виртуальные машины объединяют вычислительные задачи и рабочие нагрузки. В традиционных вычислительных средах рабочие нагрузки обычно выполняются на отдельно администрируемых и обновляемых серверах. Виртуальные машины сокращают количество оборудования и средств администрирования, необходимых для выполнения тех же вычислительных задач и рабочих нагрузок.
Большинство задач виртуальных машин в KeyVirt можно выполнять как на Портале виртуальных машин, так и на Портале администратора. Однако пользовательский интерфейс каждого Портала различается, и для некоторых административных задач требуется доступ к Порталу администратора.

1.2 Назначение

Для использования среды KeyVirt требуется Администратор, который будет выполнять следующие действия:

- управление физическими и виртуальными ресурсами, такими как узлы и виртуальные машины; обновление и добавление узлов, импорт доменов, преобразование виртуальных машин, созданных на внешних гипервизорах, и управление пулами виртуальных машин;
- мониторинг общих системных ресурсов на предмет возможных проблем, таких как чрезмерная нагрузка на один из узлов, нехватка памяти или дискового пространства, а также выполнение любых необходимых действий (например, перенос виртуальных машин на другие узлы для уменьшения нагрузки или освобождение ресурсов путем выключения компьютеров);
- реагирование на новые требования виртуальных машин (например, обновление операционной системы или выделение большего объема памяти);
- управление настраиваемыми свойствами объекта с помощью тегов;
- управление поиском, сохраненным в виде общедоступных закладок;
- управление настройками пользователя и настройка уровней разрешений;
- устранение неполадок для конкретных пользователей или виртуальных машин для общей функциональности системы;
- генерация общих и специальных отчетов.

1.3 Предварительные требования

1.3.1 Параметры производительности виртуальной машины

Для виртуальных машин определены следующие максимальные ограничения:

- максимальное количество одновременно работающих ВМ: ограничено ресурсоемкостью предоставленных вычислительных ресурсов;
- максимальное количество виртуальных процессоров для ВМ: 710 (710 для машин Q35, 240 для машин PC);
- максимальный объем памяти на ВМ: 16 ТБ;
- максимальный размер одного диска на ВМ: 8 ТБ.

1.3.2 Поддерживаемые операционные системы виртуальной машины

Рекомендуется использовать следующие ОС:

- GNU/Linux;
- Microsoft Windows;
- FreeBSD.

1.3.3 Требования к браузеру

Для доступа к Порталам рекомендуется использовать последние версии браузеров и операционных систем. В таблице 1 перечислены комбинации версий браузеров и операционных систем, которые можно использовать для получения доступа к Порталу администратора, Порталу виртуальных машин и Порталу мониторинга. Требования к браузеру делятся на уровни:

- Уровень 1. Полностью протестированные комбинации браузера и операционной системы.
- Уровень 2. Комбинации браузера и операционной системы, которые частично протестированы и могут работать.
- Уровень 3. Комбинации браузера и операционной системы, которые не протестированы, но могут работать.

Таблица 1. Требования к браузеру

Уровень поддержки	Операционная система	Браузер
Уровень 1	Корпоративный Linux Любая	Самые последние версии Google Chrome, Microsoft Edge
Уровень 2	Любая	Ранние версии Google Chrome или Mozilla Firefox
Уровень 3	Любая	Другие браузеры

1.3.4 Требования к клиенту

Доступ к консолям виртуальных машин можно получить только с помощью поддерживаемых клиентов Remote Viewer (virt-viewer) в Enterprise Linux и Windows.

Доступ к консолям виртуальных машин осуществляется через протоколы SPICE, VNC или RDP (только для Windows). Графический драйвер QXL может быть установлен в гостевой операционной системе для улучшения и расширения функциональных возможностей SPICE. SPICE в настоящее время поддерживает максимальное разрешение 2560x1600 пикселей.

1.4 Установка сертификата ЦС

При первом доступе к Порталам необходимо установить сертификат, используемый в среде виртуализации, чтобы избежать предупреждений системы безопасности.

Чтобы установить сертификат Центра Сертификации, введите предоставленный адрес сервера в веб-браузер и выберите **Корневой сертификат (Engine CA Certificate)**, как показано на рисунке ниже. Сертификат будет автоматически скачан.

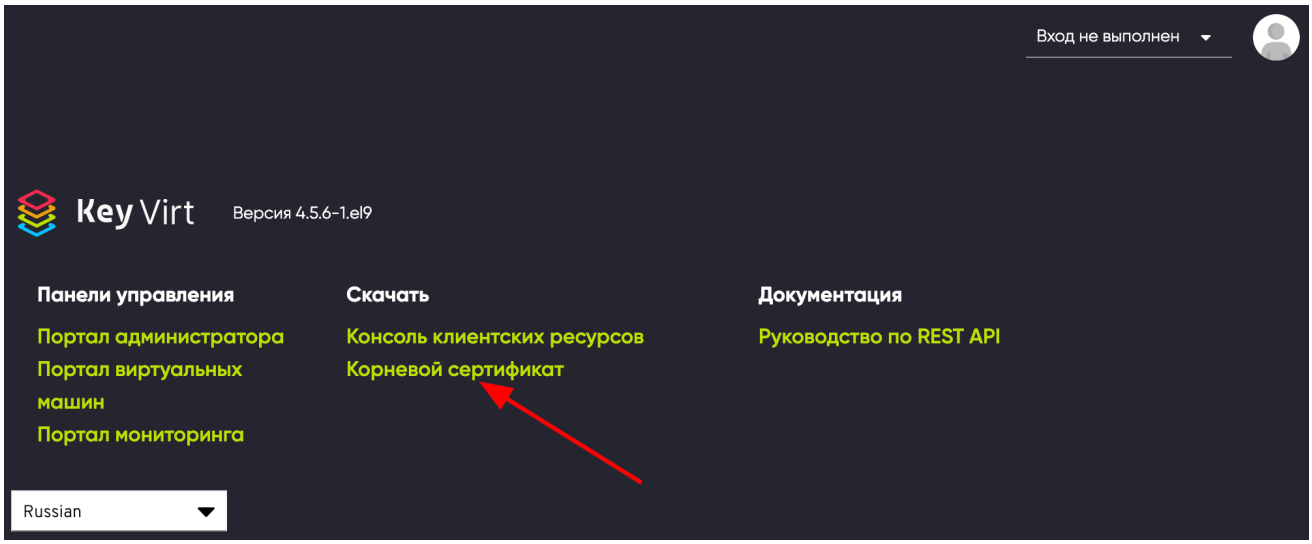


Рисунок 1. Скачивание сертификата ЦС

1.5 Авторизация на Порталах

1. Введите предоставленный адрес сервера в веб-браузер, чтобы получить доступ к экрану приветствия менеджера.
2. Выберите необходимый язык из выпадающего списка в левом нижнем углу страницы.
3. В KeyVirt вход в систему происходит с помощью единого входа (SSO), что позволяет одновременно войти на Портал виртуальных машин и Портал администратора, если у вас есть разрешение. Авторизуйтесь на Портале администратора любым из двух способов:
   1) Щелкните **Портал администратора (Administration Portal)** в левом нижнем углу страницы.
   2) Нажмите **Вход не выполнен** (**Not logged in)** в правом верхнем углу страницы и щелкните **Вход (Log In)**.

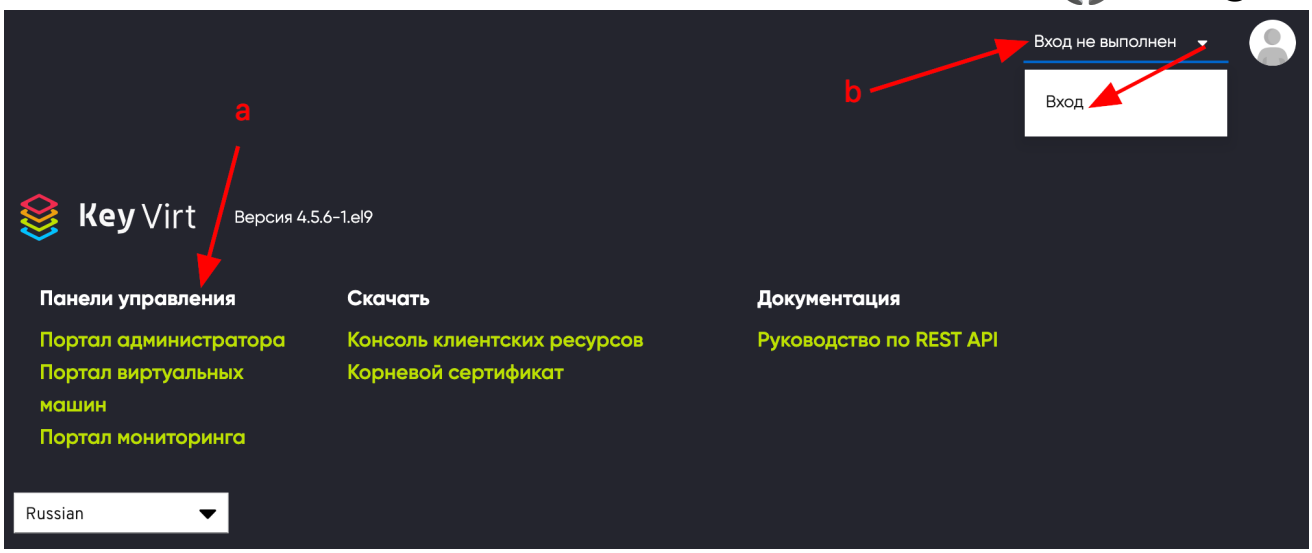


Рисунок 2. Способы входа на Портал виртуальных машин

4. В обоих случаях отобразится страница входа SSO. Выберите язык, а затем введите имя пользователя и пароль в соответствующие поля.

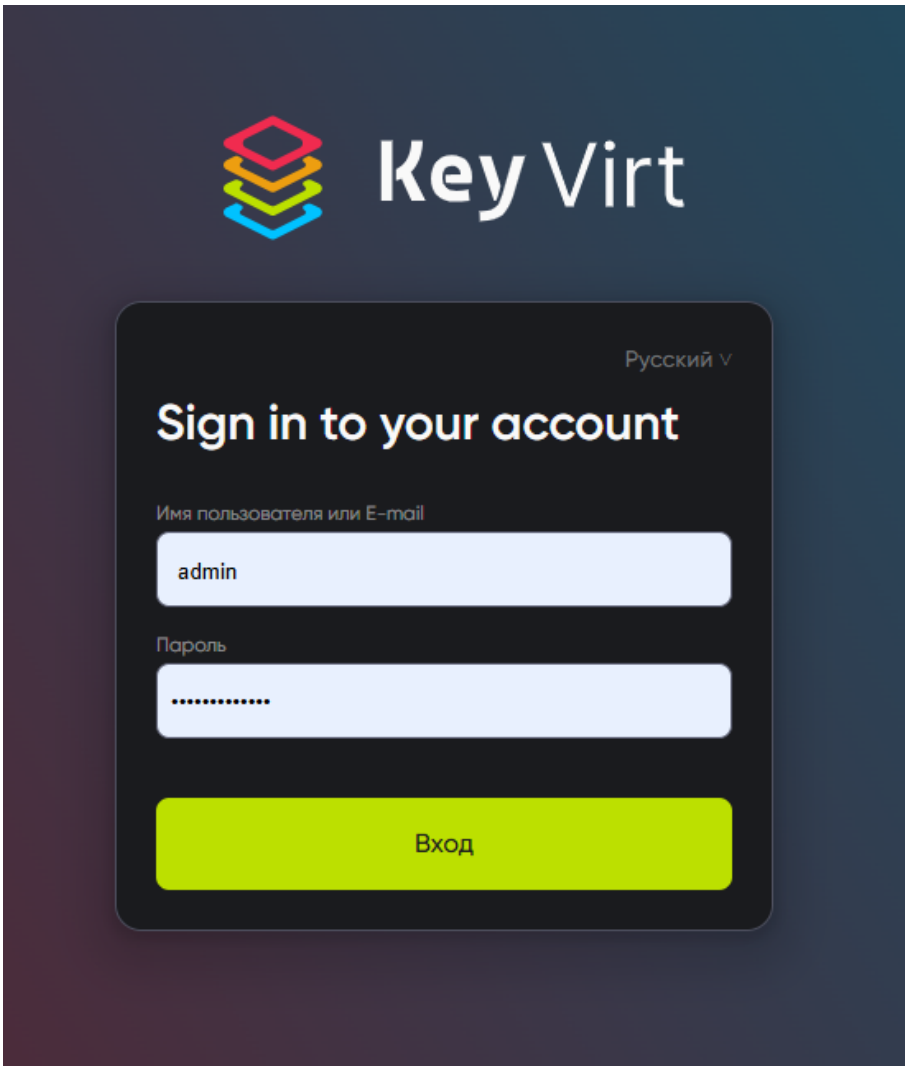


Рисунок 3. Страница входа SSO

5. Щелкните **Вход**. Отображается список назначенных вам виртуальных машин и пулов.

6. Чтобы выйти из Портала, щелкните иконку профиля в правом верхнем углу и выберите **Выйти из системы (Log out)**. После этого вы выйдете из всех Порталов и увидите экран приветствия менеджера.

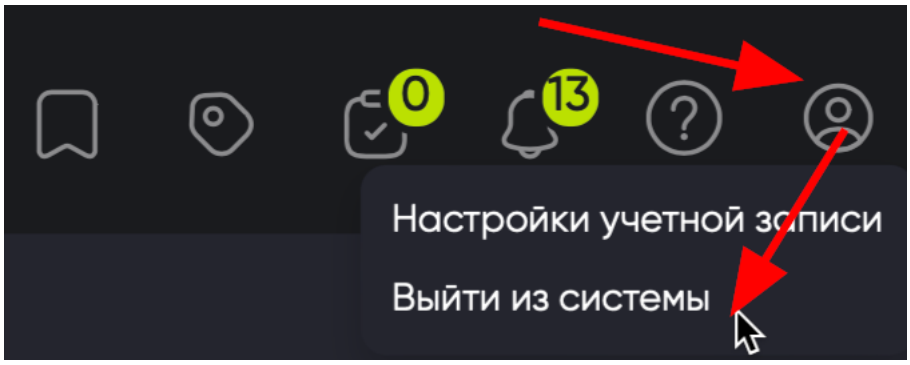


Рисунок 4. Выход из Портала администратора

2 АДМИНИСТРИРОВАНИЕ И ОБСЛУЖИВАНИЕ СРЕДЫ ВИРТУАЛИЗАЦИИ KEYVIRT

2.1 ОБЩИЕ ПАРАМЕТРЫ

Общие параметры среды KeyVirt (пользователи, роли, системные разрешения, политики планирования, типы экземпляров и пулы MAC-адресов) можно настроить на Портале администратора в окне Настройка (Администрирование > Настройка). В этом окне можно настроить способ взаимодействия пользователей с ресурсами и получить основной набор инструментов для настройки параметров, которые могут применяться к нескольким кластерам. Подробнее об интерфейсе далее.

2.1.1 Роли

Роли – это предопределенные наборы привилегий, которые можно настроить в Engine. Роли предоставляют разрешения на доступ и управление различными уровнями ресурсов в дата-центре, а также к определенным физическим и виртуальным ресурсам.

2.1.1.1 Добавление новой роли

Если требуемой роли нет в списке ролей KeyVirt по умолчанию, вы можете создать новую роль и настроить ее в соответствии с вашими целями.
Для добавления новой роли выполните следующие действия:

1. Нажмите Администрирование > Настройка, чтобы открыть окно Настройка. Вкладка «Все роли» будет выбрана по умолчанию.
2. Нажмите Новая.
3. Введите имя и описание новой роли.
4. Выберите тип учетной записи: Пользователь или Администратор.

5. Используйте кнопки Развернуть Всё для просмотра всех возможных разрешений и Свернуть Всё для скрытия всех разрешений.
6. Выберите необходимые разрешения.
7. Нажмите кнопку OK, чтобы применить изменения. Новая роль отобразится в списке ролей.

2.1.1.2 Редактирование или копирование роли

Вы можете изменить настройки для созданных вами ролей, но вы не можете изменить роли по умолчанию.
Для редактирования или копирования роли выполните следующие действия:

1. Нажмите Администрирование > Настройка, чтобы открыть окно Настройка. Вкладка «Все роли» будет выбрана по умолчанию.
2. Выберите роль, которую вы хотите изменить или скопировать.
3. Нажмите Изменить или Копировать. Откроется окно «Изменить Роль» или «Копировать роль».
4. При необходимости отредактируйте имя и описание роли.
5. Используйте кнопки Развернуть Всё для просмотра всех возможных разрешений и Свернуть Всё для скрытия всех разрешений.
6. Выберите необходимые разрешения.
7. Нажмите кнопку OK, чтобы применить изменения.

2.1.2 Системные разрешения

Разрешения позволяют пользователям выполнять действия с объектами, где объекты являются либо отдельными объектами, либо объектами-контейнерами. Любые разрешения, применяемые к объекту-контейнеру, также применяются ко всем объектам внутри этого контейнера (рисунок 5 – 7).

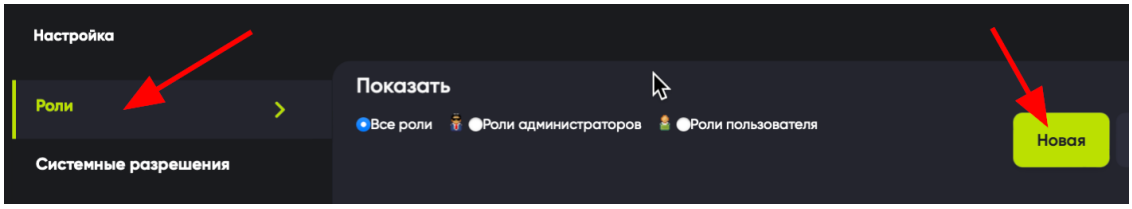


Рисунок 5. Создание пользовательской роли UserManager

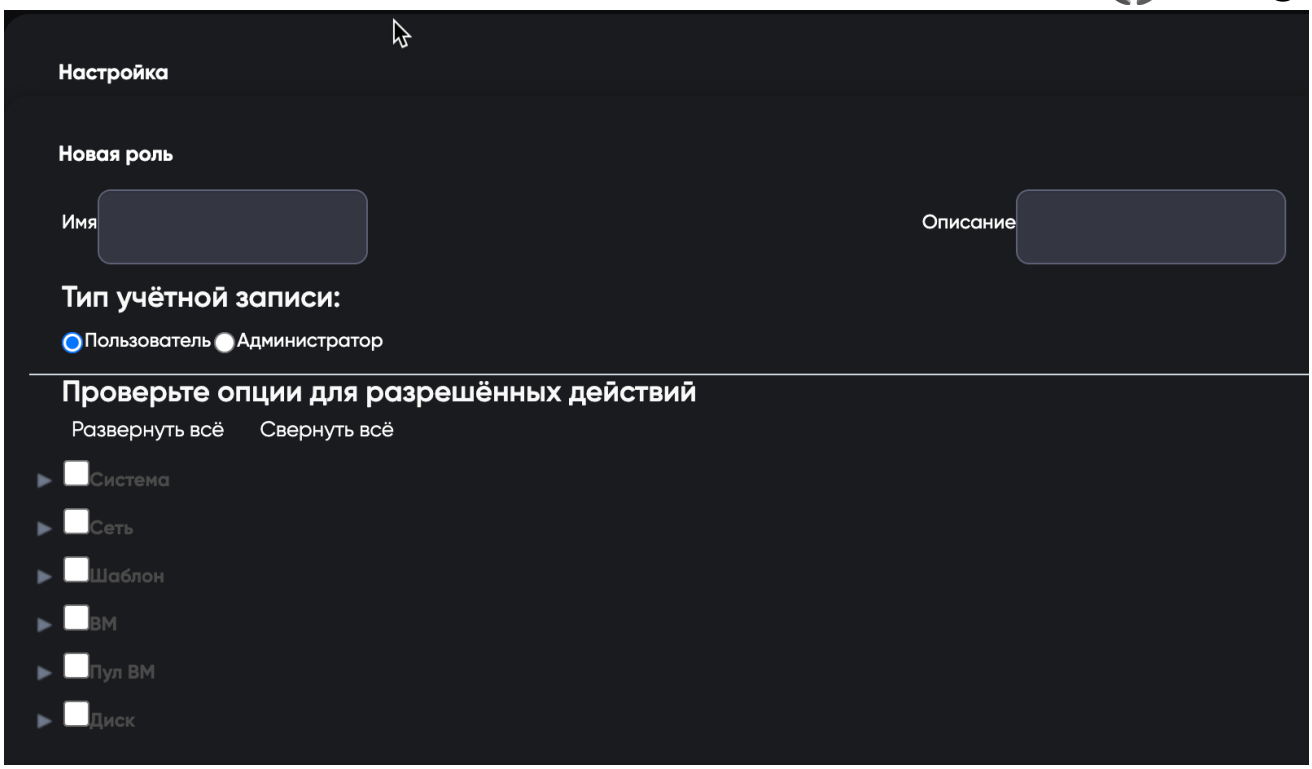


Рисунок 6. Разрешения и роли

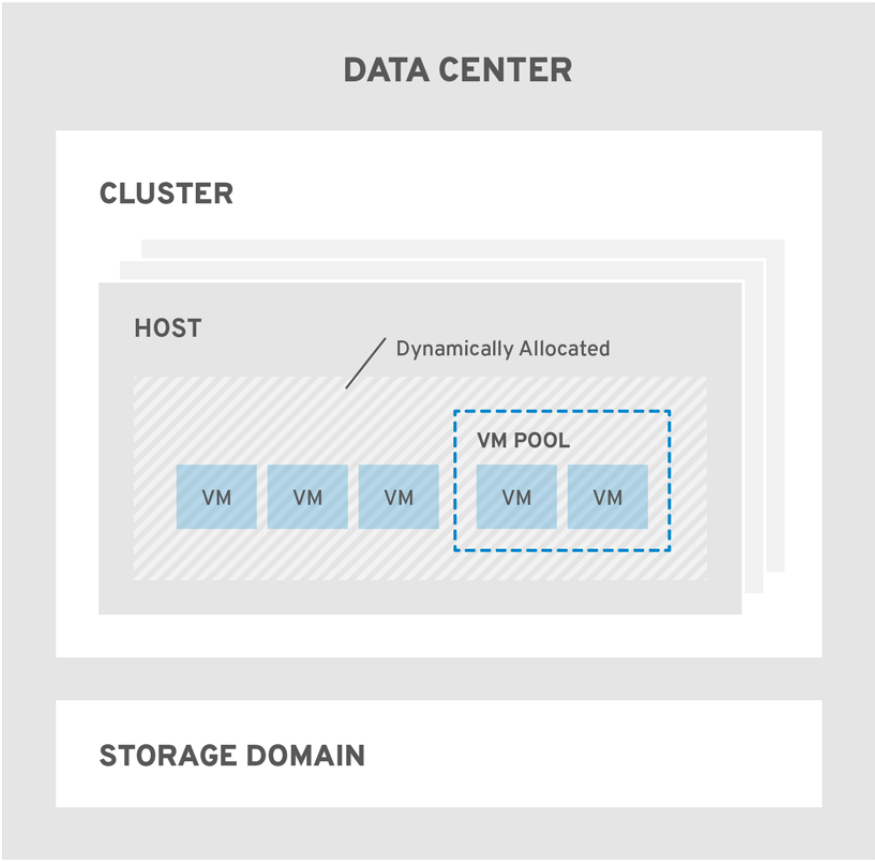


Рисунок 7. Иерархия объектов KeyVirt

Свойства пользователя

Роли и разрешения – это свойства пользователя. Многоуровневое администрирование обеспечивает детализированную иерархию разрешений. Например, администратор дата-центра имеет разрешения на управление всеми

объектами в дата-центре, а администратор узла имеет права системного администратора для одного физического узла. Также один пользователь может иметь разрешения на использование одной виртуальной машины, но не может вносить какие-либо изменения в конфигурации виртуальной машины, в то время как другому пользователю могут быть назначены системные разрешения для внесения изменений в виртуальную машину.

Роли пользователя и администратора
KeyVirt предоставляет ряд предварительно настроенных ролей, от администратора с общесистемными разрешениями до конечного пользователя с доступом к одной ВМ. Созданные по умолчанию роли нельзя изменить, однако их можно клонировать и настраивать, а также создавать новые роли в соответствии с вашими требованиями.

В KeyVirt существует два типа ролей:

- Роль администратора – предоставляет доступ к Порталу администратора для управления физическими и виртуальными ресурсами. Роль администратора предоставляет разрешения на выполнение действий на Портале виртуальных машин. Однако это не имеет никакого отношения к тому, что пользователь может видеть на Портале виртуальных машин.
- Роль пользователя – предоставляет доступ к Порталу виртуальных машин для управления и контроля доступа к виртуальным машинам и шаблонам. Роль пользователя определяет, что пользователь может видеть на Портале виртуальных машин. Разрешения, предоставленные пользователю с ролью администратора, отражаются в действиях, доступных этому пользователю на Портале виртуальных машин.

2.1.2.1 Описание ролей пользователя

В таблице 2 описаны основные роли пользователей, которые имеют доступ и возможность настраивать виртуальные машины на Портале виртуальных машин.

Таблица 2. Основные роли пользователей KeyVirt

Роль	Привилегии	Описание
UserRole	Предоставляет доступ и возможность использовать виртуальные машины и пулы.	Позволяет войти на Портал виртуальных машин, назначить пользователю виртуальные машины и пулы, просмотреть состояние виртуальной машины и сведения о ней.
PowerUserRole	Позволяет создавать виртуальные машины и шаблоны, а также управлять ими.	Данная роль применяется к пользователю для всей среды в окне Конфигурировать или для конкретных дата-центров или кластеров. Например, если роль PowerUserRole применяется на уровне дата-центра,

		пользователь PowerUser может создавать виртуальные машины и шаблоны в дата-центре.
UserVmManager	Системный администратор виртуальной машины.	Позволяет управлять виртуальными машинами, создавать и использовать снапшоты (снимки). Пользователю, создающему виртуальную машину на Портале виртуальных машин, автоматически назначается роль UserVmManager на этой машине.

В таблице 3 описаны расширенные роли пользователей, которые позволяют выполнять более тонкую настройку разрешений для ресурсов на Портале виртуальных машин.

Таблица 3. Расширенные роли пользователей KeyVirt

Роль	Привилегии	Описание
UserTemplate	Ограниченные права на использование только шаблонов.	Позволяет использовать шаблоны для создания виртуальных машин.
DiskOperator	Пользователь виртуального диска.	Позволяет использовать, просматривать и редактировать виртуальные диски. Наследует разрешения на использование виртуальной машины, к которой подключен виртуальный диск.
VmCreator	Позволяет создавать виртуальные машины на Портале виртуальных машин.	Данная роль не применяется к конкретной виртуальной машине. Примените эту роль к пользователю для всей среды в окне Конфигурировать. Можно также применить эту роль для определенных дата-центров или кластеров. При применении этой роли к кластеру необходимо также применить роль создателя диска ко всему дата-центру или к определенным доменам хранения.
TemplateCreator	Позволяет создавать, редактировать,	Данная роль не применяется к определенному шаблону. Примените эту роль к пользователю

	управлять и удалять шаблоны виртуальных машин в рамках назначенных ресурсов.	для всей среды в окне Configure. Можно также применить эту роль для определенных дата-центров, кластеров или доменов хранения
DiskCreator	Позволяет создавать, редактировать, управлять и удалять диски виртуальных машин в назначенных кластерах или дата-центрах.	Данная роль не применяется к определенному виртуальному диску. Примените эту роль к пользователю для всей среды в окне Конфигурировать. Можно также применить эту роль для определенных дата-центров или доменов хранения.
TemplateOwner	Позволяет редактировать и удалять шаблон, назначать и управлять разрешениями пользователей для шаблона.	Данная роль автоматически назначается пользователю, создающему шаблон. Другие пользователи, не имеющие разрешений TemplateOwner, не могут просматривать или использовать шаблон.
VnicProfileUser	Пользователь логической сети и сетевого интерфейса для виртуальной машины и шаблона.	Позволяет подключать или отсоединять сетевые интерфейсы от определенных логических сетей.

2.1.2.2 Описание ролей администратора

В таблице 4 описаны основные роли администратора, которые предоставляют разрешения на доступ и настройку ресурсов на Портале администратора.

Таблица 4. Основные роли системного администратора KeyVirt

Роль	Привилегии	Описание
SuperUser	Системный администратор среды KeyVirt.	Имеет полные разрешения на все объекты и уровни, может управлять всеми объектами во всех дата-центрах.

ClusterAdmin	Администратор кластера.	Обладает правами администратора для всех объектов в определенном кластере.
DataCenter Admin	Администратор дата-центра.	Обладает правами администратора для всех объектов в определенном дата-центре, за исключением хранилища.

Внимание! Не используйте администратора сервера каталогов в качестве администратора KeyVirt. Создайте пользователя на сервере каталогов специально для использования в качестве администратора KeyVirt.

В таблице 5 описаны расширенные роли администратора, которые позволяют более тонко настраивать разрешения для ресурсов на Портале администратора.

Таблица 5. Расширенные роли системного администратора KeyVirt

Роль	Привилегии	Описание
TemplateAdmin	Администратор шаблона виртуальной машины	Позволяет создавать, удалять и настраивать домены хранения и сетевые сведения шаблонов, а также перемещать шаблоны между доменами.
StorageAdmin	Администратор хранилища	Позволяет создавать, удалять, настраивать и управлять назначенным доменом хранения.
HostAdmin	Администратор узла	Позволяет подключать, удалять, настраивать и управлять определенным узлом.
NetworkAdmin	Администратор сети	Позволяет настраивать и управлять сетью конкретного дата-центра или кластера. Сетевой администратор дата-центра или кластера наследует сетевые разрешения для виртуальных пулов в кластере.
VmPoolAdmin	Системный администратор виртуального пула	Позволяет создавать, удалять и настраивать виртуальный пул, назначать и удалять пользователей виртуального пула, а также выполнять основные операции на виртуальной машине в пуле.
VmImporterExporter	Администратор импорта и экспорта виртуальных машин	Позволяет импортировать и экспортировать виртуальные машины. Существует возможность просмотра всех виртуальных машин и шаблонов, экспортированных другими пользователями.

2.1.2.3 Назначение ресурсу роли администратора или пользователя

Вы можете назначить ресурсам (т.е. конкретным виртуальным машинам, шаблонам, пулам, дата-центрам и т.д.) роли администратора или пользователя, чтобы позволить пользователям получать доступ к этому ресурсу или управлять им.

Для назначения роли ресурсу выполните следующие действия:

1. Найдите и нажмите на название ресурса. Откроется подробное описание.
2. Перейдите на вкладку Разрешения (Permissions), чтобы просмотреть список назначенных пользователей, ролей пользователей и унаследованные разрешения для выбранного ресурса.
3. Нажмите кнопку Добавить (Add).
4. Введите имя или логин существующего пользователя в текстовое поле Поиск (Search) и нажмите кнопку Вперед (Go). Выберите пользователя из полученного списка возможных совпадений.
5. Выберите роль из раскрывающегося списка Роль для связи (Role to Assign).
6. Нажмите OK.

Теперь у пользователя есть унаследованные разрешения назначенной роли, доступные для этого ресурса.

2.1.2.4 Удаление из ресурса роли администратора или пользователя

Следует удалить из ресурса роль администратора или пользователя, чтобы пользователь потерял унаследованные разрешения, связанные с ролью для этого ресурса.

Для удаления назначенной ресурсу роли выполните следующие действия:

1. Найдите и нажмите название ресурса. Откроется подробное описание.
2. Перейдите на вкладку Разрешения (Permissions), чтобы просмотреть список назначенных пользователей, ролей пользователей и унаследованные разрешения для выбранного ресурса.
3. Выберите пользователя, которого нужно удалить из ресурса.
4. Нажмите кнопку Удалить (Remove).
5. Нажмите OK.

2.1.2.5 Управление системными разрешениями для дата-центра

Как суперпользователь SuperUser, системный администратор управляет всеми аспектами Портала администратора. Другим пользователям могут быть назначены более конкретные роли администрирования. Эти роли полезны для предоставления пользователю привилегий, ограничивающих его определенным ресурсом. Например, роль DataCenterAdmin имеет права администратора только для назначенного дата-центра, без доступа к хранилищу, а ClusterAdmin имеет права администратора только для назначенного кластера.

Администратор дата-центра выполняет роль системного администратора только для конкретного дата-центра. Это полезно в средах виртуализации с несколькими дата-

центрами, где каждому дата-центру требуется администратор. Роль DataCenterAdmin – это иерархическая модель. Пользователь, которому назначена роль администратора дата-центра, может управлять всеми объектами в дата-центре, за исключением хранилища.

Роль администратора дата-центра разрешает следующие действия:

- создавать и удалять кластеры, связанных с дата-центром;
- добавлять и удалять узлы, виртуальные машины и пулы, связанные с дата-центром;
- менять разрешения пользователя для виртуальных машин, связанных с дата-центром и унаследованные разрешения для выбранного ресурса.

Примечание. Вы можете назначать роли и разрешения только существующим пользователям. Вы можете изменить системного администратора дата-центра, удалив существующего системного администратора и добавив нового системного администратора.

2.1.2.6 Описание ролей администратора дата-центра

В таблице 6 описаны роли и привилегии, применимые к администрированию дата-центра.

Таблица 6. Роли системного администратора KeyVirt

Роль	Привилегии	Описание
DataCenterAdmin	Администратор дата -центра.	Позволяет использовать, создавать, удалять и управлять всеми физическими и виртуальными ресурсами в определенном дата -центре, за исключением хранилища, включая кластеры, узлы, шаблоны и виртуальные машины.
NetworkAdmin	Администратор сети.	Позволяет настраивать и управлять сетью конкретного дата -центра. Сетевой администратор дата-центра также наследует сетевые разрешения для виртуальных машин в дата-центре.

2.1.2.7 Управление системными разрешениями для кластера

Администратор кластера выполняет роль системного администратора только для определенного кластера. Это полезно в дата-центрах с несколькими кластерами, где для каждого кластера требуется системный администратор. Роль ClusterAdmin представляет собой иерархическую модель. Пользователь, которому назначена роль администратора кластера, может управлять всеми объектами в кластере.

Роль администратора кластера позволяет выполнять следующие действия:

- создавать и удалять связанные кластеры;
- добавлять и удалять узлы, виртуальные машины и пулы, связанные с кластером;
- менять разрешения пользователей для виртуальных машин, связанных с кластером.

Роль администратора кластера

В таблице 7 описаны роли и привилегии, применимые к администрированию кластера.

Таблица 7. Роли администратора кластера KeyVirt

Роль	Привилегии	Описание
ClusterAdmin	Администратор кластера.	Позволяет использовать, создавать, удалять и управлять всеми физическими и виртуальными ресурсами в определенном кластере, включая узлы, шаблоны и виртуальные машины. Может настраивать свойства сети в кластере, такие как назначение контекстно-медийных сетей или маркировка сети как необходимой или необязательной. Однако администратор кластера ClusterAdmin не имеет разрешений на присоединение или отсоединение сетей от кластера, для этого требуются разрешения администратора сети NetworkAdmin.
NetworkAdmin	Администратор сети.	Позволяет настраивать и управлять сетью конкретного кластера. Сетевой администратор кластера также наследует сетевые разрешения для виртуальных машин в кластере.

2.1.2.8 Управление системными разрешениями для сети

Администратор сети – это роль системного администратора, которую можно применять для конкретной сети или для всех сетей в дата-центре, кластере, узле, виртуальной машине или шаблоне. Пользователь сети может выполнять ограниченные административные роли, такие как просмотр и подключение сетей на определенной виртуальной машине или шаблоне.

Роль сетевого администратора позволяет выполнять следующие действия:

- создавать, редактировать и удалять сети;
- менять конфигурации сети, включая настройку зеркалирования портов;
- подключать и отключать сети от ресурсов, включая кластеры и виртуальные машины.

Пользователь, который создает сеть, автоматически получает разрешения NetworkAdmin в созданной сети. Вы также можете изменить администратора сети, удалив существующего администратора и добавив нового администратора.

Роль сетевого администратора и пользователя
В таблице 8 описаны роли и привилегии администратора и пользователя, применимые к сетевому администрированию.

Таблица 8. Роли сетевого администратора и пользователя KeyVirt

Роль	Привилегии	Описание
NetworkAdmin	Сетевой администратор для дата-центра, кластера, узла, виртуальной машины или шаблона. Пользователь, который создает сеть, автоматически получает разрешения NetworkAdmin в созданной сети.	Может настраивать и управлять сетью конкретного дата-центра, кластера, узла, виртуальной машины или шаблона. Сетевой администратор дата-центра или кластера наследует сетевые разрешения для виртуальных пулов в кластере. Чтобы настроить зеркальное отображение портов в сети виртуальной машины, примените роль администратора сети в сети и роль UserVmManager в виртуальной машине
VnicProfileUser	Пользователь логической сети и сетевого интерфейса для виртуальной машины и шаблона.	Может подключать или отсоединять сетевые интерфейсы от определенных логических сетей.

2.1.2.9 Управление системными разрешениями для узла

Администратор узла выполняет роль системного администратора только для определенного узла. Это полезно в кластерах с несколькими узлами, где для каждого узла требуется системный администратор.

Роль администратора узла позволяет выполнять следующие действия:

- редактировать конфигурации узла;
- настраивать логическую сеть;
- удалять узел.

Вы также можете изменить системного администратора узла, удалив существующего системного администратора и добавив нового системного администратора.

Роль администратора узла

В таблице 9 описаны роли и привилегии, применимые к администрированию узла.

Таблица 9. Роли администратора узла KeyVirt

Роль	Привилегии	Описание
HostAdmin	Администратор узла.	Позволяет настраивать, управлять и удалять определенный узел. Также можно выполнять операции, связанные с сетью, на определенном узле.

2.1.2.10 Управление системными разрешениями для домена хранения

Администратор хранилища выполняет роль системного администратора только для определенного домена хранилища. Это полезно в дата-центрах с несколькими доменами хранения, где для каждого домена хранения требуется системный администратор.

Роль администратора домена хранения позволяет выполнять следующие действия:

- редактировать конфигурации домена хранения;
- переводить домен хранения в режим обслуживания;
- удалять домен хранения.

Вы также можете изменить системного администратора домена хранения, удалив существующего системного администратора и добавив нового системного администратора.

Роли администратора хранилища

В таблице 10 описаны роли и привилегии администратора, применимые к администрированию домена хранения.

Таблица 10. Роли администратора хранилища KeyVirt

Роль	Привилегии	Описание
StorageAdmin	Администратор хранилища.	Позволяет создавать, удалять, настраивать и управлять определенным доменом хранения.

2.1.2.11 Управление разрешениями системы для пула виртуальных машин

Администратор пула виртуальных машин – это роль системного администратора для пулов виртуальных машин в дата-центре. Эта роль может быть применена к определенным пулам виртуальных машин, к дата-центру или ко всей виртуализированной среде. Позволяет разным пользователям управлять определенными ресурсами пула виртуальных машин.

Роль администратора пула виртуальных машин позволяет выполнять следующие действия:

- создавать, редактировать и удалять пулы виртуальных машин;

- добавлять и отключать виртуальные машины из пула.

Роли администратора пула виртуальных машин

В таблице 11 описаны роли и привилегии администратора, применимые к администрированию пула.

Таблица 11. Роли системного администратора KeyVirt

Роль	Привилегии	Описание
VmPoolAdmin	Роль системного администратора виртуального пула.	Позволяет создавать, удалять и настраивать виртуальный пул, назначать и удалять пользователей виртуального пула, а также выполнять основные операции на виртуальной машине.
ClusterAdmin	Администратор кластера.	Позволяет использовать, создавать, удалять и управлять всеми пулами виртуальных машин в определенном кластере.

2.1.2.12 Управление системными разрешениями для виртуального диска

KeyVirt по умолчанию предоставляет две роли пользователя виртуального диска, но не предоставляет роли администратора виртуального диска по умолчанию. Одна из этих пользовательских ролей – Disk Creator, которая позволяет управлять виртуальными дисками из Портала виртуальных машин. Данная роль может применяться к конкретным виртуальным машинам, дата-центру, определенному домену хранения или ко всей среде виртуализации. Позволяет разным пользователям управлять разными виртуальными ресурсами.

Роль создателя виртуального диска позволяет выполнять следующие действия:

- создавать, редактировать и удалять виртуальные диски, связанные с виртуальными машинами или другими ресурсами;
- менять права пользователей для виртуальных дисков.

Роли пользователей виртуального диска

В таблице 12 описаны роли и привилегии пользователей, применимые к использованию и администрированию виртуальных дисков на портале виртуальных машин.

Таблица 12. Роли системного администратора на Портале виртуальных машин KeyVirt

Роль	Привилегии	Описание
DiskOperator	Пользователь виртуального диска.	Позволяет использовать, просматривать и редактировать виртуальные диски. Наследует разрешения на использование

		виртуальной машины, к которой подключен виртуальный диск.
DiskCreator	Позволяет создавать, редактировать, управлять и удалять виртуальные диски в назначенных кластерах или дата-центрах.	Данная роль не применяется к определенному виртуальному диску. Примените роль DiskCreator к пользователю для всей среды с помощью окна Configure. Можно также применить эту роль для определенных дата-центров, кластеров или доменов хранения.

2.1.3 Политика планирования

Политика планирования – это набор правил, определяющих логику распределения виртуальных машин между узлами в кластере. Политики планирования определяют эту логику с помощью комбинации фильтров, оценок и политики балансировки нагрузки. Модули фильтра применяют жесткие принудительные меры и отфильтровывают узлы, которые не соответствуют условиям, указанным этим фильтром. Модули оценки используются для управления относительным приоритетом факторов, учитываемых при определении узлов в кластере, на которых может работать виртуальная машина.

KeyVirt предоставляет пять политик планирования по умолчанию: None, Evenly_Distributed, VM_Evenly_Distributed, Power_Saving и Cluster_Maintenance. Также возможно создать новые политики планирования, обеспечивающие более точный контроль над распределением виртуальных машин. Независимо от политики планирования, виртуальная машина не запускается на узле с перегруженным процессором. По умолчанию, ЦП узла считается перегруженным, если он имеет нагрузку более 80% в течение 5 минут, но эти значения можно изменить с помощью политик планирования.

Политика планирования **None** отключает балансировку нагрузки или распределение мощности между узлами для уже запущенных виртуальных машин. Это режим «по умолчанию». Когда виртуальная машина запускается, нагрузка на память и ЦП распределяется равномерно между всеми узлами в кластере. Дополнительные виртуальные машины, подключенные к узлу, не запустятся, если этот узел достиг определенного значения CpuOverCommitDurationMinutes, HighUtilization или MaxFreeMemoryForOverUtilized.

Политика планирования **Evenly_Distributed** равномерно распределяет нагрузку на память и ЦП между всеми узлами в кластере. Дополнительные виртуальные машины, подключенные к узлу, не запустятся, если этот узел достиг определенного значения CpuOverCommitDurationMinutes, HighUtilization или MaxFreeMemoryForOverUtilized (рисунок 8).

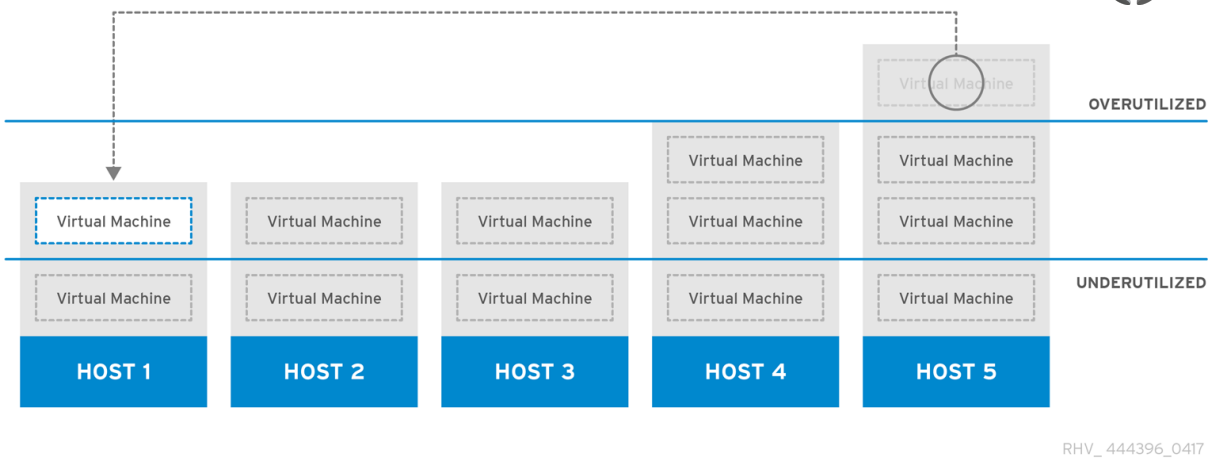


Рисунок 8. Политика равномерно распределенного планирования

Политика планирования **VM_Evenly_Distributed** равномерно распределяет виртуальные машины между узлами на основе количества виртуальных машин. Кластер считается несбалансированным, если на каком-либо узле запущено больше виртуальных машин, чем HighVmCount, и есть хотя бы один узел с числом виртуальных машин, выходящим за пределы MigrationThreshold.

Политика планирования **Power_Saving** распределяет нагрузку на память и ЦП по подмножеству доступных узлов, чтобы снизить энергопотребление на недостаточно загруженных узлах. узлы с загрузкой ЦП ниже минимального значения использования в течение времени, превышающего определенный интервал, перенесут все виртуальные машины на другие узлы, чтобы их можно было отключить. Дополнительные виртуальные машины, подключенные к узлу, не запустятся, если этот узел достиг максимального заданного значения загрузки (рисунок 9).

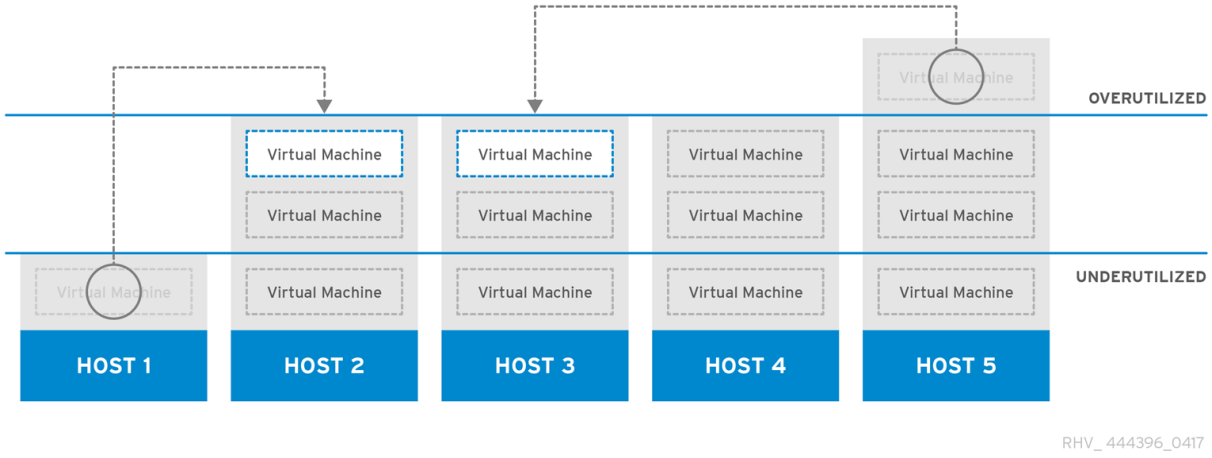


Рисунок 9. Политика планирования энергосбережения

Политика планирования **Cluster_Maintenance** ограничивает активность в кластере во время задач обслуживания. Нельзя запускать новые виртуальные машины, кроме высокодоступных виртуальных машин. Если произойдет сбой узла, виртуальные

машины высокой доступности будут перезапущены должным образом, и любая виртуальная машина сможет мигрировать.

2.1.3.1 Свойства политик планирования

В зависимости от выбранной политики планирования будут отображены некоторые ее свойства с установленными значениями по умолчанию. При необходимости параметры по умолчанию можно отредактировать:

- HighVmCount – задает минимальное количество виртуальных машин, которое должно быть запущено на узле, чтобы включить балансировку нагрузки. Значение по умолчанию равно 10 запущенным виртуальным машинам на одном узле. Балансировка нагрузки включена только в том случае, если в кластере есть хотя бы один узел, на котором запущено не менее указанного HighVmCount виртуальных машин.
- MigrationThreshold – определяет порог перед миграцией виртуальных машин с узла. Это максимальная разница в количестве виртуальных машин между самым высокоиспользуемым узлом и наименее используемым узлом. Кластер сбалансирован, когда на каждом узле кластера количество виртуальных машин находится в пределах порога миграции. Значение по умолчанию равно 5.
- SpmVmGrace – определяет количество зарезервированных на узлах SPM слотов для виртуальных машин. узел SPM будет иметь нагрузку меньше, чем другие узлы, поэтому переменная SpmVmGrace определяет, на сколько меньше виртуальных машин может запускать узел SPM по сравнению с другими узлами. Значение по умолчанию – 5.
- CpuOverCommitDurationMinutes – задает время (в минутах), в течение которого узел может выполнять загрузку ЦП за пределами установленных значений использования, прежде чем политика планирования начнет действовать. Заданный временной интервал защищает от временных скачков загрузки ЦП, активирующих политики планирования и провоцирующих ненужную миграцию виртуальных машин. Не более двух символов. Значение по умолчанию – 2.
- HighUtilization – выражается в процентах. Если узел работает с использованием ЦП на уровне или превышающим значение высокой загрузки в течение определенного интервала времени, HostedEngine переносит виртуальные машины на другие узлы в кластере до тех пор, пока загрузка ЦП узла не станет ниже максимального порога обслуживания. Значение по умолчанию – 80.
- LowUtilization – выражается в процентах. Если узел работает с использованием ЦП ниже минимального значения загрузки в течение определенного интервала времени, HostedEngine переносит виртуальные машины на другие узлы в кластере. Engine выключит исходный хост-компьютер и снова перезапустит его, когда потребуется балансировка нагрузки или в кластере будет недостаточно свободных узлов. Значение по умолчанию – 20.
- ScaleDown – снижает влияние функции резервирования HA путем деления оценки узла на указанную величину. Это необязательное свойство, которое можно добавить в любую политику, в том числе и в политику none.

- HostsInReserve – указывает количество узлов, которые должны продолжать работать, даже если на них нет запущенных виртуальных машин. Это необязательное свойство, которое может быть добавлено к политике power_saving.
- EnableAutomaticHostPowerManagement – включает автоматическое управление питанием для всех узлов в кластере. которое может быть добавлено к политике power_saving. Значение по умолчанию – true.
- MaxFreeMemoryForOverUtilized – определяет минимальный объем свободной памяти, который должен иметь узел, в МБ. Если узел имеет меньше свободной памяти, чем указанная величина, HostedEngine считает, что узел перегружен. Например, если установить для этого свойства значение 1000, узел, имеющий менее 1 ГБ свободной памяти, будет считаться перегруженным. Дополнительные сведения о том, как это свойство взаимодействует с политиками power_saving и evenly_distributed, см. в пункте *Свойства MaxFreeMemoryForOverUtilized и MinFreeMemoryForUnderUtilized*. Вы можете добавить это свойство в политики power_saving и evenly_ distributed. Даже если данное свойство присутствует в списке свойств политики vm_evenly_distributed, оно не применяется к данной политике.
- MinFreeMemoryForUnderUtilized – указывает максимальный объем свободной памяти, который должен иметь узел, в МБ. Если узел имеет больше свободной памяти, чем указанная величина, HostedEngine считает узел недостаточно загруженным. Например, если вы установите для этого параметра значение 10000, узел, имеющий более 10 ГБ свободной памяти, будет использоваться недостаточно. Дополнительные сведения о том, как это свойство взаимодействует с политиками power_saving и evenly_distributed, см. в пункте *Свойства MaxFreeMemoryForOverUtilized и MinFreeMemoryForUnderUtilized*. Вы можете добавить это свойство в политики power_saving и evenly_ distributed. Даже если данное свойство присутствует в списке свойств политики vm_evenly_distributed, оно не применяется к данной политике.
- HeSparesCount – задает количество дополнительных узлов Self-Hosted Engine, которые должны зарезервировать достаточно свободной памяти для запуска виртуальной машины Engine в случае ее миграции или отключения. Другим виртуальным машинам запрещено запускаться на узле Self-Hosted Engine, если это не оставит достаточно свободной памяти для виртуальной машины Engine. Это необязательное свойство, которое можно добавить к политикам power_saving, vm_evenly_distributed и evenly_distributed. Значение по умолчанию равно 0.

Оптимизация планировщика по степени важности/порядку:

- Optimize for Utilization – включает значимые модули в планирование, чтобы обеспечить наилучший выбор.
- Optimize for Speed – пропускает распределение узлов в случаях, когда имеется более 10 ожидающих запросов.

2.1.3.2 Свойства MaxFreeMemoryForOverUtilized и MinFreeMemoryForUnder Utilized

Планировщик имеет фоновый процесс, который переносит виртуальные машины в соответствии с текущей политикой планирования кластера и ее параметрами. На основе различных критериев и их приоритетов в политике планировщик постоянно классифицирует узлы как исходные или конечные, а также переносит отдельные виртуальные машины с первых на последние.

В следующем описании объясняется, как политики кластерного планирования evenly_distributed и power_saving взаимодействуют со свойствами MaxFreeMemoryForOverUtilized и minfreememoryforunderusutilized. Хотя обе политики учитывают загрузку процессора и памяти, загрузка процессора не имеет отношения к свойствам MaxFreeMemoryForOverUtilized и MinFreeMemoryForUnderUtilized.

Если вы определяете свойства MaxFreeMemoryForOverUtilized и MinFreeMemoryForUnderUtilized как часть политики evenly_distributed:

- Узлы, на которых меньше свободной памяти, чем MaxFreeMemoryForOverUtilized, перегружаются и становятся исходными узлами.
- Узлы, на которых больше свободной памяти, чем MinFreeMemoryForUnderUtilized, используются недостаточно и становятся узлами назначения.
- Если параметр MaxFreeMemoryForOverUtilized не определен, планировщик не выполняет миграцию виртуальных машин в зависимости от загрузки памяти. (Продолжается миграция виртуальных машин на основе других критериев политики, таких как загрузка процессора.)
- Если параметр MinFreeMemoryForUnderUtilized не определен, планировщик рассматривает все узлы, имеющие право стать узлами назначения.

Если вы определяете свойства MaxFreeMemoryForOverUtilized и MinFreeMemoryForUnderUtilized как часть политики энергосбережения:

- Узлы, на которых меньше свободной памяти, чем MaxFreeMemoryForOverUtilized, перегружаются и становятся исходными узлами.
- Хосты, у которых больше свободной памяти, чем MinFreeMemoryForUnderUtilized, используются недостаточно и становятся исходными узлами.
- Узлы, на которых больше свободной памяти, чем MaxFreeMemoryForOverUtilized, не перегружаются и становятся узлами назначения.
- Узлы, которые имеют меньше свободной памяти, чем MinFreeMemoryForUnderUtilized, не используются недостаточно и становятся узлами назначения.
- Планировщик предпочитает переносить виртуальные машины на узлы, которые не перегружены и не используются недостаточно. Если этих узлов недостаточно, планировщик может перенести виртуальные машины на недостаточно используемые узлы. Если недостаточно используемые узлы не нужны для этой цели, планировщик может отключить их.

- Если значение MaxFreeMemoryForOverUtilized не определено, ни один узел не будет перегружен. Таким образом, исходными узлами являются только недостаточно используемые узлы, а узлы назначения включают все узлы в кластере.
- Если параметр MinFreeMemoryForUnderUtilized не определен, исходными узлами являются только перегруженные узлы, а узлы, которые не перегружены, являются узлами назначения.
- Чтобы предотвратить чрезмерную загрузку узлом всех физических процессоров, определите отношение виртуального процессора к физическому - VCpuToPhysicalCpuRatio со значением от 0,1 до 2,9. Когда этот параметр установлен, узлы с меньшей загрузкой процессора предпочтительнее при планировании виртуальной машины.

Если при добавлении виртуальной машины коэффициент превышает предельное значение, учитываются как физическая производительность VCPUT, так и загрузка процессора.

В запущенной среде, если физическая пропускная способность узла превышает 2,5, некоторые виртуальные машины могут быть сбалансированы по нагрузке и перемещены на узлы с более низкой пропускной способностью VCPUTOPHYSICAL.

2.1.3.3 Создание политики планирования

Вы можете создавать новые политики планирования для управления логикой распределения виртуальных машин в заданном кластере в вашей среде KeyVirt.

Для создания политики планирования выполните следующие действия:

1. Нажмите *Администрирование* > *Настройка*.
2. Перейдите на вкладку Политика планирования.
3. Нажмите кнопку Новая.
4. Введите имя и описание политики планирования.
5. Настройте модули фильтров:
   1) В разделе Модули фильтров перетащите предпочтительные модули фильтра из раздела Выключенные фильтры в раздел Включенные фильтры.
   2) Определенные модули фильтров также могут быть установлены в качестве первых *Первый*, которым будет дан наивысший приоритет, или последних *Последний*, которым будет дан самый низкий приоритет, для базовой оптимизации. Чтобы установить приоритет, нажмите правой кнопкой мыши на любой модуль фильтра, наведите курсор на *Расположение* и выберите *Первый* или *Последний*.
6. Настройте модули оценки:
   1) В разделе *Вес модулей* перетащите предпочтительные модули из раздела *Выключенные веса* в раздел *Включенные веса и факторы*.
   2) Используйте кнопки «+» и «–» слева от выбранных модулей, чтобы увеличить или уменьшить важность этих модулей.
7. Настройте политику балансировки нагрузки:
   1) В раскрывающемся меню, в разделе *Балансировщик нагрузки* выберите политику балансировки нагрузки.

2) В раскрывающемся меню раздела *Свойства* выберите свойство балансировки и используйте текстовое поле справа от этого свойства для указания значения.
3) Используйте кнопки «+» и «–» для добавления или удаления дополнительных свойств.

8. Нажмите OK.

2.1.3.4 Пояснение к настройкам в окне создания и редактирования политики планирования

В таблице 13 подробно описаны параметры, доступные в окнах *Новая политика планирования* и *Изменить политику планирования*.

Таблица 13. Новая политика планирования и изменение настроек политики планирования

Имя поля	Описание
Имя	Имя политики планирования. Это имя используется для ссылки на политику планирования в KeyVirt.
Описание	Описание политики планирования. Это поле рекомендуется, но не является обязательным.
Модули фильтров	Набор фильтров для управления узлами, на которых может работать виртуальная машина в кластере. Включение фильтра позволит отфильтровать узлы, которые не соответствуют заданным условиям, как показано ниже: • CpuPinning: узлы, которые не удовлетворяют определению закрепления ЦП. • Migration: предотвращение миграции на тот же узел. • PinToHost: узлы, отличные от узла, к которому прикреплена виртуальная машина. • CPU-Level: узлы, которые не соответствуют топологии ЦП виртуальной машины. • CPU: узлы с меньшим количеством процессоров, чем число, назначенное виртуальной машине. • Memory: узлы, на которых недостаточно памяти для запуска виртуальной машины. • VmAffinityGroups: узлы, которые не соответствуют условиям, указанным для виртуальной машины, являющейся членом группы по интересам. Например, виртуальные машины в группе по интересам должны выполняться на одном узле или на разных узлах. • InClusterUpgrade: узлы, на которых установлена более старая операционная система, чем та, на которой в данный момент работает виртуальная машина. • HostDevice: узлы, которые не поддерживают узлустройства, необходимые виртуальной машине.

	• HA: Заставляет виртуальную машину размещенного ядра работать только на узлах с положительным показателем высокой доступности. • Emulated-Machine: узлы, которые не имеют надлежащей поддержки эмулируемых машин. • Network: узлы, на которых не установлены сети, требуемые контроллером сетевого интерфейса виртуальной машины, или на которых не установлена контекстномедийная сеть кластера.
Вес модулей	Набор инструментов для управления относительным приоритетом факторов, учитываемых при определении узлов в кластере, на которых может работать виртуальная машина: • InClusterUpgrade: значимость узлов в соответствии с их версией операционной системы. Политика планирования распределяет виртуальные машины на основе версии операционной системы узла. узлы с более новой операционной системой, чем та, на которой в данный момент работает виртуальная машина, имеют приоритет перед узлами с той же операционной системой. • OptimalForHaReservation: оценивает узлы в соответствии с их высокой оценкой доступности. • None: оценивает узлы в соответствии с модулем равномерного распределения. • OptimalForEvenGuestDistribution: оценивает узлы в соответствии с количеством виртуальных машин, работающих на этих узлах. • VmAffinityGroups: оценивает узлы в соответствии с группами по интересам, определенными для виртуальных машин. Этот модуль определяет, какова вероятность того, что виртуальные машины в группе по интересам будут работать на одном узле или на разных узлах в соответствии с параметрами этой группы по интересам. • OptimalForPowerSaving: оценивает узлы в соответствии с их использованием ЦП, отдавая приоритет узлам с более высокой загрузкой ЦП. • OptimalForEvenDistribution: оценивает узлы в соответствии с их использованием ЦП, отдавая приоритет узлам с более низкой загрузкой ЦП. • HA: оценивает узлы в соответствии с их высокой оценкой доступности.

Балансировщик нагрузки	Это выпадающее меню позволяет выбрать модуль балансировки нагрузки. Модули балансировки нагрузки определяют логику, используемую для переноса виртуальных машин с узлов с высоким уровнем использования на узлы с низким уровнем использования.
Свойства	Это раскрывающееся меню позволяет добавлять или удалять свойства модулей балансировки нагрузки и доступно только при выборе модуля балансировки нагрузки. По умолчанию свойства не определены, а доступные свойства относятся только к выбранному модулю балансировки нагрузки. С помощью кнопок «+» и «–» можно добавлять или удалять дополнительные свойства модуля балансировки нагрузки.

2.1.4 Типы виртуальных машин

Типы ВМ можно использовать для определения конфигурации оборудования виртуальной машины. Выбор типа ВМ при создании или редактировании виртуальной машины автоматически заполнит поля конфигурации оборудования. Это позволяет пользователям создавать несколько виртуальных машин с одинаковой конфигурацией оборудования без необходимости вручную заполнять каждое поле.

Набор предопределенных типов ВМ доступен по умолчанию, как показано в таблице 14:

Таблица 14. Предопределенные типы ВМ

Название	Количество памяти	vCPUs
Tiny	512 MB	1
Small	2 GB	1
Medium	4 GB	2
Large	8 GB	2
XLarge	16 GB	4

Администраторы также могут создавать, редактировать и удалять типы ВМ на вкладке *Настройка – Типы экземпляров*.

Поля в окнах *Новая виртуальная машина* и *Изменить виртуальную машину*, привязанные к типу ВМ, будут иметь рядом с ними значок звена цепи ( ). Если значение одного из этих полей будет изменено, виртуальная машина будет отделена от типа ВМ, перейдя на пользовательский, и цепочка будет выглядеть разорванной ( ). Однако, если значение будет изменено обратно, цепочка снова соединится и тип ВМ вернется к выбранному.

2.1.4.1 Создание типов ВМ

Администраторы могут создавать новые типы ВМ, которые затем могут быть выбраны пользователями при создании или редактировании виртуальных машин.

Для создания типа ВМ выполните следующие действия:

1. Нажмите *Администрирование* > *Настройка*.
2. Перейдите на вкладку *Типы экземпляров*.
3. Нажмите *Новый*.
4. Введите имя и описание для типа экземпляра.
5. Нажмите кнопку *Показать расширенные опции* и настройте необходимые параметры. Параметры, отображаемые в окне *Новый тип экземпляра*, идентичны параметрам в *Новая виртуальная машина*, только с соответствующими полями.
6. Нажмите OK.

Новый тип ВМ появится на вкладке *Типы экземпляров* в окне *Настройка*, и его можно будет выбрать в раскрывающемся списке *Типы экземпляров* при создании или редактировании виртуальной машины.

2.1.4.2 Редактирование типов ВМ

Администраторы могут редактировать существующие типы экземпляров в окне *Настройка*.

Для редактирования свойств типа экземпляра выполните следующие действия:

1. Нажмите *Администрирование* > *Настройка*.
2. Перейдите на вкладку *Типы экземпляров*
3. Выберите тип экземпляра для редактирования.
4. Нажмите *Изменить*.
5. При необходимости измените настройки.
6. Нажмите OK.

Конфигурация типа экземпляра будет обновлена. При создании новой виртуальной машины или при обновлении существующей виртуальной машины на основе этого типа экземпляра применится новая конфигурация.

Существующие виртуальные машины, основанные на этом типе экземпляра, будут отображать поля, отмеченные значком цепочки, которые будут обновлены. Если существующие виртуальные машины работали, когда тип экземпляра был изменен, рядом с ними появится оранжевый значок Pending Changes, а поля со значком цепочки будут обновлены при следующем перезапуске.

2.1.4.3 Удаление типов ВМ

Для удаления типа экземпляра выполните следующие действия:

1. Нажмите *Администрирование* > *Настройка*.
2. Перейдите на вкладку *Типы экземпляров*.
3. Выберите тип экземпляра для удаления.

4. Нажмите *Удалить*.
5. Если какие-либо виртуальные машины основаны на типе удаляемого экземпляра, появится окно предупреждения со списком подключенных виртуальных машин. Чтобы продолжить удаление типа экземпляра, установите флажок *Подтвердить операцию*. В противном случае нажмите кнопку *Отменить*.
6. Нажмите OK.

Тип экземпляра будет удален из списка типов экземпляров и больше не сможет использоваться при создании новой виртуальной машины. Все виртуальные машины, которые были присоединены к удаленному типу экземпляра, теперь будут присоединены к пользовательскому типу (без типа экземпляра).

2.1.5 Пулы MAC-адресов

Пулы MAC-адресов определяют диапазон(ы) MAC-адресов, выделенных для каждого кластера. Для каждого кластера указывается пул MAC-адресов. Используя пулы MAC-адресов, KeyVirt может автоматически генерировать и назначать MAC-адреса новым виртуальным сетевым устройствам, что помогает предотвратить дублирование MAC-адресов. Пулы MAC-адресов более эффективны с точки зрения памяти, когда все MAC-адреса, относящиеся к кластеру, находятся в диапазоне для назначенного пула MAC-адресов.

Один и тот же пул MAC-адресов может использоваться несколькими кластерами, но каждому кластеру назначен один пул MAC-адресов. Пул MAC-адресов по умолчанию создается KeyVirt и используется, если другой пул MAC-адресов не назначен.

Примечание. Если более одного кластера KeyVirt совместно используют сеть, не полагайтесь исключительно на пул MAC-адресов по умолчанию, поскольку виртуальные машины каждого кластера будут пытаться использовать один и тот же диапазон MAC-адресов, что приведет к конфликтам. Чтобы избежать конфликтов MAC-адресов, проверьте диапазоны пула, чтобы убедиться, что каждому кластеру назначен уникальный диапазон.

Пул MAC-адресов назначает следующий доступный MAC-адрес после последнего адреса, который был возвращен в пул. Если в диапазоне больше не осталось адресов, поиск начинается снова с начала диапазона. Если существует несколько диапазонов MAC-адресов с доступными MAC-адресами, определенными в одном пуле MAC-адресов, диапазоны по очереди обслуживают входящие запросы таким же образом, как выбираются доступные MAC-адреса.

2.1.5.1 Создание пулов MAC-адресов

Чтобы создать новый пул MAC-адресов, выполните следующие действия:

1. Нажмите *Администрирование* > *Настройка*.
2. Перейдите на вкладку *Пул MAC адресов*.
3. Нажмите кнопку *Добавить*.
4. Введите имя и описание нового пула MAC-адресов.

5. Установите флажок *Разрешить задвоения*, чтобы разрешить многократное использование MAC-адреса в пуле. Пул MAC-адресов не будет автоматически использовать дубликат MAC-адреса, но включение данного параметра означает, что пользователь может вручную использовать дубликат MAC-адреса.
   Примечание. Если в одном пуле MAC-адресов дубликаты отключены, а в другом включены, то каждый MAC-адрес может использоваться один раз в пуле с отключенными дубликатами, но может использоваться несколько раз в пуле с включенными дубликатами.
6. Введите необходимые диапазоны MAC-адресов в *Диапазон MAC адресов*. Чтобы ввести несколько диапазонов, нажмите кнопку «+» рядом с полями *Из* и *В*.
7. Нажмите OK.

2.1.5.2 Редактирование пулов MAC-адресов

Вы можете редактировать пулы MAC-адресов, чтобы изменить сведения, включая диапазон доступных в пуле MAC-адресов и допустимость дублирования.

Для редактирования свойств пула MAC-адресов выполните следующие действия:

1. Нажмите *Администрирование* > *Настройка*.
2. Перейдите на вкладку *Пул MAC адресов* .
3. Выберите пул MAC-адресов для редактирования.
4. Нажмите *Изменить*.
5. При необходимости измените значения *Имя*, *Описание*, *Разрешить задвоения* и *Диапазон MAC адресов*.
   Примечание. При обновлении диапазона MAC-адресов, MAC-адреса существующих сетевых карт не переназначаются. MAC-адреса, которые уже были назначены, но находятся за пределами нового диапазона MAC-адресов, добавляются как указанные пользователем MAC-адреса и по-прежнему отслеживаются этим пулом MAC-адресов.
6. Нажмите OK.

2.1.5.3 Редактирование разрешений пулов MAC-адресов

После создания пула MAC-адресов вы можете изменить его права доступа. Права доступа определяют, какие дата-центры могут использовать пул MAC-адресов.

Для редактирования разрешений пулов MAC-адресов выполните следующие действия:

1. Нажмите *Администрирование* > *Настройка*.
2. Перейдите во вкладку *Пул MAC адресов*.
3. Выберите необходимый пул MAC-адресов.
4. Измените разрешения пользователя для пула MAC-адресов:
   4.1. Чтобы добавить разрешения пользователя в пул MAC-адресов:
      4.1.1. Нажмите *Добавить* на панели разрешений пользователей в нижней части окна *Настройка*.
      4.1.2. Найдите и выберите нужных пользователей.
      4.1.3. Выберите нужную роль из раскрывающегося списка Role to assign.

4.1.4. Нажмите OK, чтобы добавить разрешения пользователя.

4.2. Чтобы удалить разрешения пользователей из пула MAC-адресов:

4.2.1. Выберите разрешение пользователя, которое нужно удалить, на панели разрешений пользователя в нижней части окна *Настройка*.

4.2.2. Нажмите *Удалить*, чтобы удалить разрешения пользователя.

2.1.5.4 Удаление пулов MAC-адресов

Созданные пулы MAC-адресов можно удалить, но пул MAC-адресов по умолчанию удалить нельзя.

Для удаления пула MAC-адресов выполните следующие действия:

1. Нажмите Администрирование > *Настройка*.
2. Перейдите на вкладку *Пул MAC адресов*.
3. Выберите пул MAC-адресов для удаления.
4. Нажмите кнопку *Удалить*.
5. Нажмите OK.

3 ЗНАКОМСТВО С ИНТЕРФЕЙСОМ KEYVIRT

После того как все предварительные условия выполнены, вы как администратор можете подключиться ко всем Порталам. Вы увидите следующий интерфейс при первом подключении:

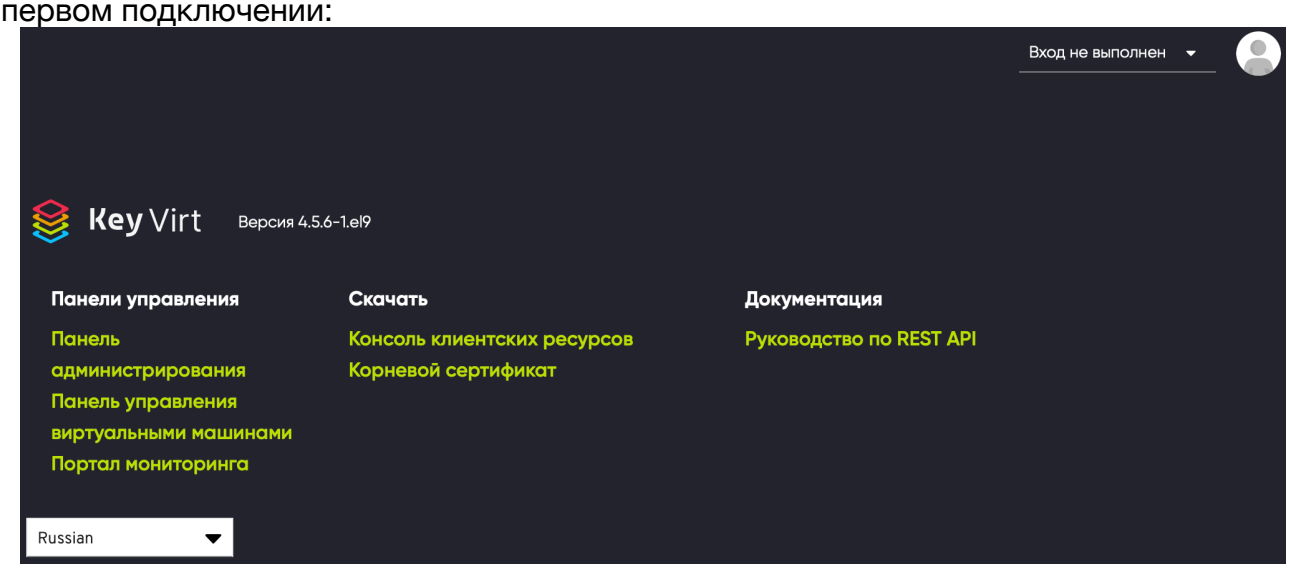


Рисунок 10. Стартовое меню

Далее можно подробнее остановиться на каждом из Порталов.

3.1 ПОРТАЛ АДМИНИСТРАТОРА (Administration Portal)

Портал администратора (рисунок 11) передает состояние системы KeyVirt в сводке ресурсов и использования KeyVirt. Эта сводка может предупредить вас о проблеме, чтобы проанализировать проблемную область.

Информация на Портале по умолчанию обновляется каждые 15 минут из хранилища данных и каждые 15 секунд по умолчанию с помощью Engine API или при каждом обновлении информационной панели. Панель инструментов обновляется, когда пользователь возвращается с другой страницы, или обновляется вручную. Панель инструментов не обновляется автоматически.
Информация о карточке инвентаризации предоставляется Engine API, а информация об использовании предоставляется хранилищем данных. Панель инструментов реализована как компонент плагина пользовательского интерфейса, который автоматически устанавливается и обновляется вместе с Engine.

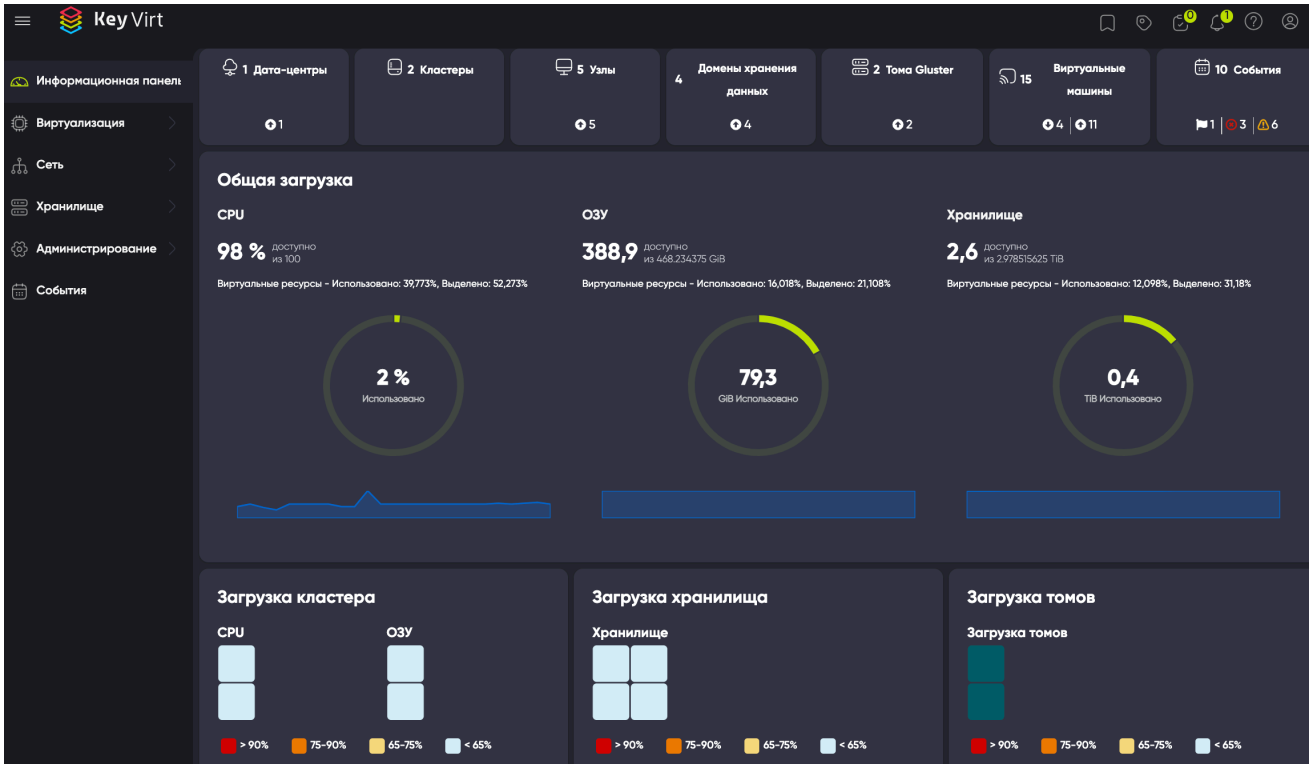


Рисунок 11. Портал администратора

3.1.1 Панель инструментов/Верхняя панель

Панель инструментов в верхней части окна остается неизменной при переключении между любыми разделами и подразделами. Здесь выполняются основные действия с Порталом и аккаунтом.

Рисунок 12. Панель инструментов/Верхняя панель

Данная панель содержит следующие параметры:

- **KeyVirt** – Открывает стартовую страницу со списком всех Порталов.
- **Закладки (Bookmarks)** – Закладки, добавленные ранее.
- **Метки (Tags)** – Теги, добавленные ранее.
- **Задачи (Tasks)** – Задачи, добавленные ранее.
- **Уведомления о событиях и оповещениях (Events and alerts notification)** – Список всех предупреждений (**Alerts**) и уведомлений о событиях (**Events**).
- **Помощь (Help)** – Ссылка на официальную документацию KeyVirt (**Guide**) и подробности о версии продукта (**About**).

- **Account** – Настройки учетной записи (**Account Settings**) и выход из Порталов (**Log out**).

3.1.2 Боковое меню

Навигация по основным разделам осуществляется с помощью бокового меню.

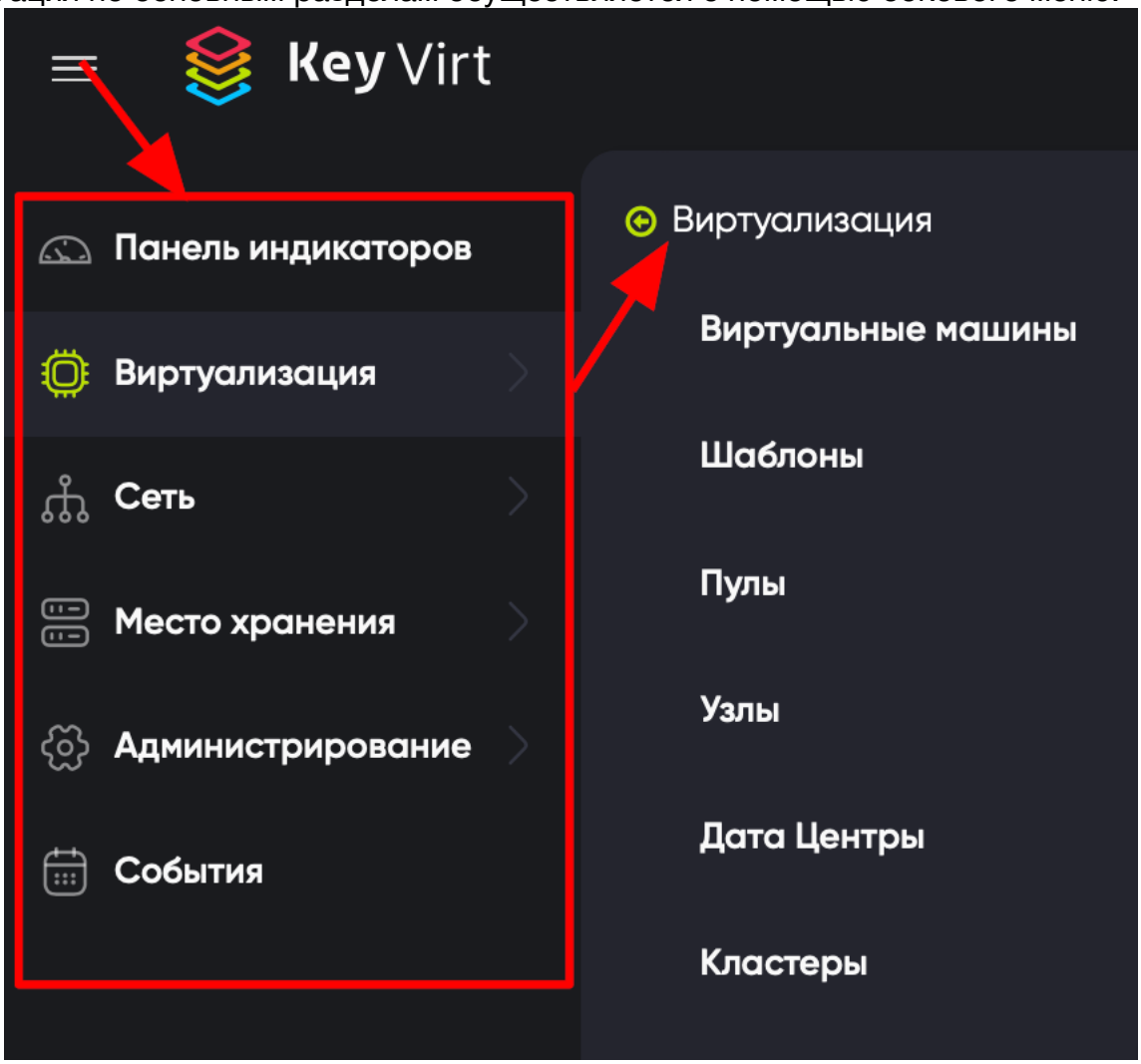


Рисунок 13. Боковое меню

В этом меню доступны следующие разделы:

- **Информационная панель (Dashboard)** – Основной раздел
- **Виртуализация (Compute)** – Вычислительные ресурсы
- **Сеть (Network)** – Сетевые ресурсы
- **Хранилище (Storage)** – Хранилище и связанные задачи
- **Администрирование (Administration)** – Администрирование ресурсов
- **События (Events)** – Уведомления

Названия разделов бокового меню можно свернуть либо развернуть с помощью значка ☰. У каждого из разделов, кроме **Информационная панель** и **События**, есть свои подразделы, которые можно открыть с помощью значка >. Подробнее о каждом разделе см. далее.

3.1.3 Информационная панель (Dashboard)

Это основной раздел, который открывается по умолчанию при подключении к Порталу администратора. Он состоит из следующих подразделов: **Общие сведения**, **Общая нагрузка (Global Utilization)**, **Загрузка кластера (Cluster Utilization)**, **Загрузка хранилища (Storage Utilization)**, **Загрузка томов (Storage Savings)**.

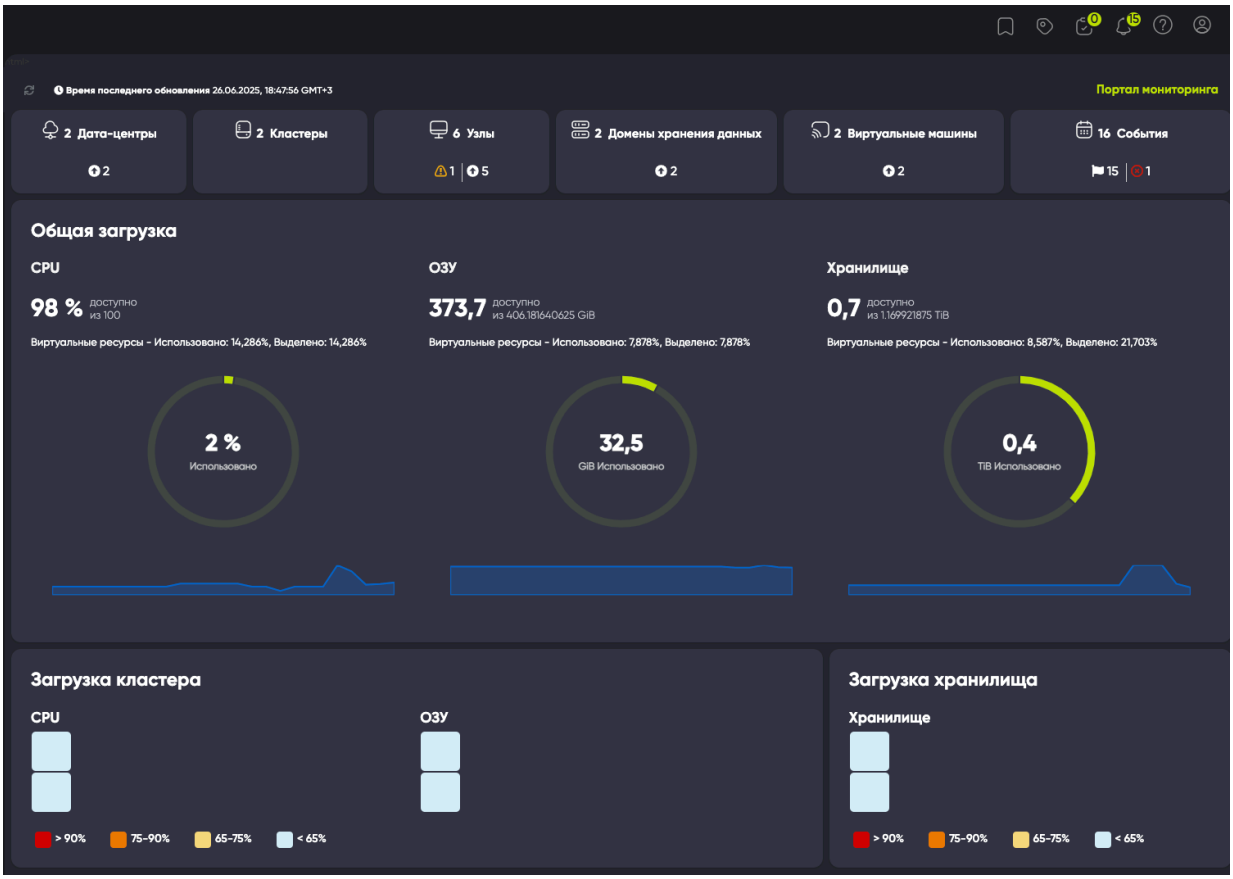


Рисунок 14. Информационная панель

3.1.3.1 Общие сведения

В верхней части Портала администратора можно выполнить следующие действия:

- – принудительное обновление.
- **Портал мониторинга (Monitoring Portal)** – быстрый переход на Портал мониторинга.

Далее на Портале администратора представлен общий перечень ресурсов KeyVirt, включая элементы для дата-центров, кластеров, узлов, доменов хранения данных, виртуальных машин и событий (рисунок 15).

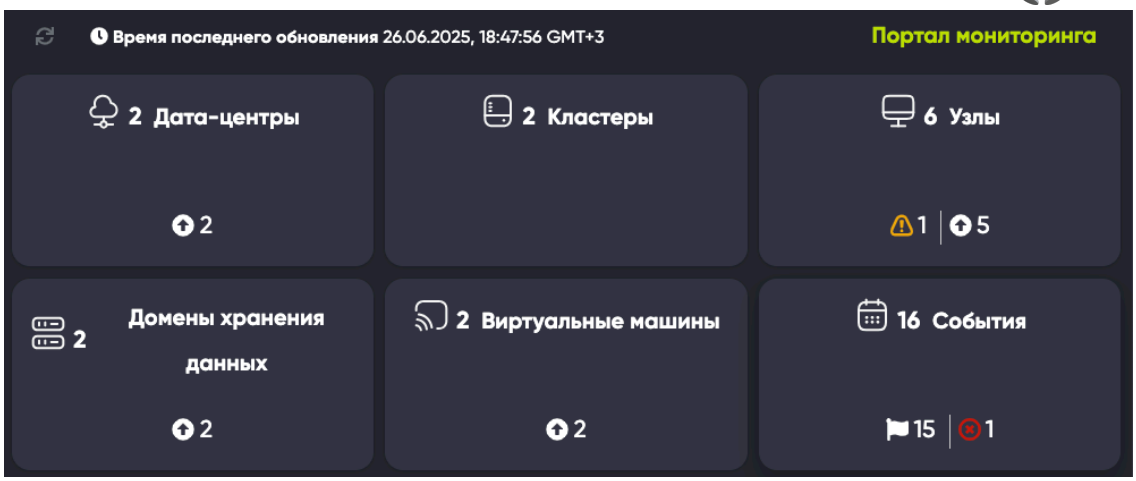


Рисунок 15. Общие сведения

Значки показывают статус каждого ресурса, а числа показывают количество каждого ресурса с этим статусом. Нажав на заголовок ресурса, вы перейдете в соответствующий раздел Портала. Статус для кластеров не отображается.

Таблица 15. Описание статусов ресурсов

Иконка	Статус
	Ни один из этих ресурсов не добавлен в KeyVirt.
	Показывает номер ресурса со статусом предупреждения. При нажатии на значок осуществляется переход на соответствующую страницу с поиском, ограниченным этим ресурсом со статусом предупреждения. Поиск ограничен по-разному для каждого ресурса: • Дата-центры: поиск ограничен дата-центрами, которые не работают или не отвечают. • Хосты: поиск ограничен узлами, которые не назначены, находятся в режиме обслуживания, установке, перезагрузке, подготовке к обслуживанию, ожидающих утверждения или подключении. • Домены хранения: поиск ограничен доменами хранения, которые не инициализированы, не подключены, неактивны, находятся в режиме обслуживания, готовятся к обслуживанию, отсоединяются или активируются. • Виртуальные машины: поиск ограничен виртуальными машинами, которые включаются, приостанавливаются, мигрируют, ожидают, приостанавливаются или выключаются. • События: поиск ограничен событиями с серьезностью предупреждения.
	Показывает номер ресурса в рабочем состоянии. Щелкнув по значку, вы перейдете на соответствующую страницу с поиском, ограниченным доступными ресурсами.
	Показывает номер ресурса в нерабочем состоянии. При нажатии на значок осуществляется переход на соответствующую страницу с поиском, ограниченным ресурсами со статусом *Выключено* (Down). Поиск ограничен по-разному для каждого ресурса:

	• Дата-центры: поиск ограничен дата-центрами, которые не инициализированы, находятся в режиме обслуживания или находятся в нерабочем состоянии. • Хосты: поиск ограничен узлами, которые не отвечают, имеют ошибки, имеют ошибку установки, не работают, инициализируются или отключены. • Домены хранения: поиск ограничивается отсоединенными или неактивными доменами хранения. • Виртуальные машины: поиск ограничен виртуальными машинами, которые не работают, не отвечают или перезагружаются.
	Показывает количество событий со статусом оповещения. Щелкнув по значку, вы перейдете к событиям с предупреждениями.
	Показывает количество событий со статусом ошибки. Щелкнув по значку, вы перейдете к событиям с ошибками.

3.1.3.2 Общая загрузка (Global Utilization)

Раздел Общая загрузка (рисунок 16) показывает использование системой CPU, ОЗУ (оперативной памяти) и доступной емкости хранилища.

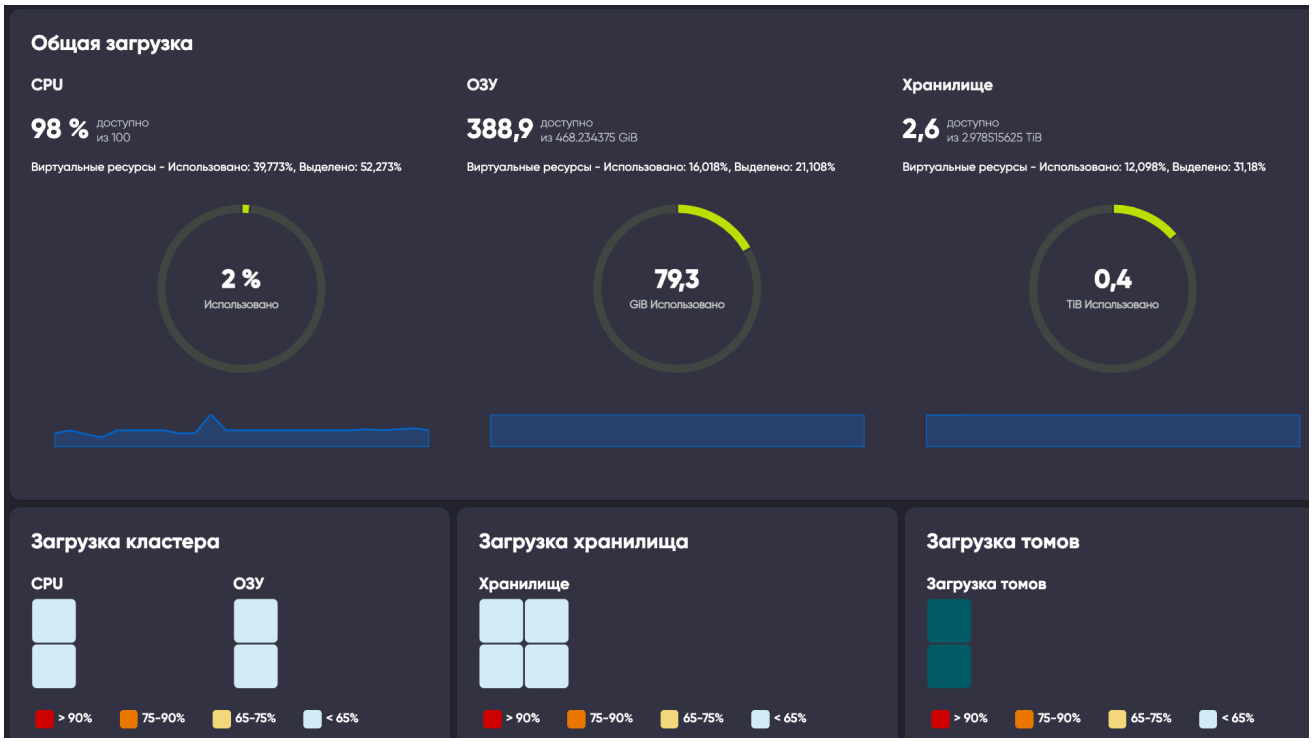


Рисунок 16. Общая загрузка

В верхней части показан процент доступного CPU, памяти или хранилища, а также коэффициент избыточной фиксации. Например, коэффициент избыточной нагрузки для CPU рассчитывается путем деления количества виртуальных ядер на количество физических ядер, доступных для работающих виртуальных машин, на основе последних данных в хранилище данных.

Диаграмма отображает использование в процентах для ЦП, памяти или хранилища и показывает среднее использование для всех узлов на основе среднего использования за последние 5 минут. При наведении курсора на раздел диаграммы отобразится значение выбранного раздела.

Линейный график внизу отображает тенденцию за последние 24 часа. Каждая точка данных показывает среднее использование за определенный час. При наведении указателя мыши на точку на графике отображается время и процент использования для графика CPU, а также объем использования для графиков памяти и хранилища. Если щелкнуть на диаграмму в разделе общей нагрузки на информационной панели, отобразится список наиболее часто используемых ресурсов CPU, памяти или хранилища.
Для CPU и памяти всплывающее окно показывает список из десяти узлов и виртуальных машин с наибольшей загруженностью. Для хранилища всплывающее окно показывает список десяти наиболее часто используемых доменов хранения и виртуальных машин.
Стрелка справа от полосы использования показывает тенденцию использования этого ресурса за последнюю минуту.

3.1.3.3 Нагрузка на кластер (Cluster Utilization)

В разделе Загрузка кластера показано использование кластером ЦП и памяти на тепловой карте.
CPU
Тепловая карта нагрузки на ЦП для конкретного кластера показывает среднюю нагрузку на ЦП за последние 24 часа.
При наведении курсора на тепловую карту отображается имя кластера. Щелчок по тепловой карте позволяет перейти к вычислительным узлам и отобразить результаты поиска по определенному кластеру, отсортированному по загрузке процессора.
Формула, используемая для расчета использования ЦП кластером, представляет собой среднее использование ЦП узла в кластере. Вычисление производится путем использования средней нагрузки на ЦП каждого узла за последние 24 часа, чтобы найти общее среднее использование ЦП кластером.
ОЗУ (Memory)
Тепловая карта использования памяти для определенного кластера, показывающая среднее использование памяти за последние 24 часа.
При наведении курсора на тепловую карту отображается имя кластера. Щелчок по тепловой карте позволяет перейти к вычислительным узлам и отобразить результаты поиска по определенному кластеру, отсортированному по использованию памяти.
Формула, используемая для расчета использования памяти кластером, представляет собой общее использование памяти в кластере в ГБ. Вычисление производится путем использования среднего использования памяти узла для каждого узла за последние 24 часа, чтобы найти общее среднее использование памяти кластером.

3.1.3.4 Нагрузка на хранилище (Storage Utilization)

В разделе *Загрузка хранилища* показано использование хранилища на тепловой карте.
Тепловая карта показывает среднее использование хранилища за последние 24 часа. Формула, используемая для расчета использования хранилища кластером, представляет собой общее использование хранилища в кластере. Вычисление производится путем использования среднего использования хранилища для каждого узла за последние 24 часа, чтобы найти общее среднее использование хранилища кластером.

При наведении курсора на тепловую карту отображается имя домена хранилища. Щелчок по тепловой карте приводит к переходу к доменам хранения, отсортированным по степени использования.

3.1.4 Виртуализация (Compute)

Данный раздел предназначен для управления вычислительными ресурсами, такими как виртуальные машины, узлы и кластеры. Он состоит из следующих подразделов: **Виртуальные машины (Virtual Machines), Шаблоны (Templates), Пулы (Pools) Узлы (Hosts) Дата Центры (Data Centers), Кластеры (Clusters).**
В верхней части окна есть специальный раздел для быстрого поиска по всей таблице на выбранной вкладке. Эта панель также применима для всех подразделов ниже, но меняется тип ресурса в строке поиска. На рисунке внизу поиск осуществляется для виртуальных машин (ВМ).

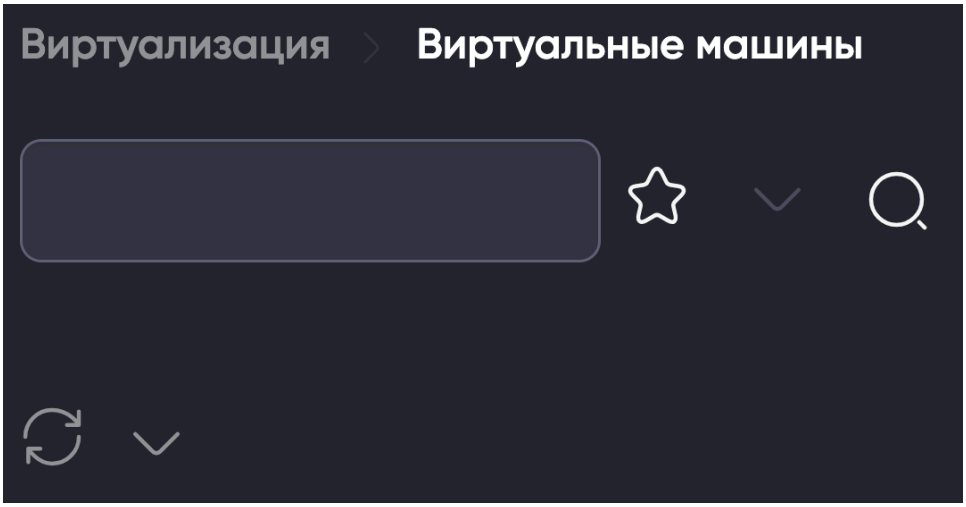


Рисунок 17. Верхняя панель

Строка поиска – строка для выполнения поиска по ключевым словам и закладкам. Можно очистить поле поиска, сохранить поиск и настроить параметры поиска.

- – принудительное обновление.
- ▼ – выбрать частоту обновления.

3.1.4.1 Виртуальные машины (Virtual Machines)

Данный подраздел предназначен для работы с виртуальными машинами и просмотра всех сведений о них.

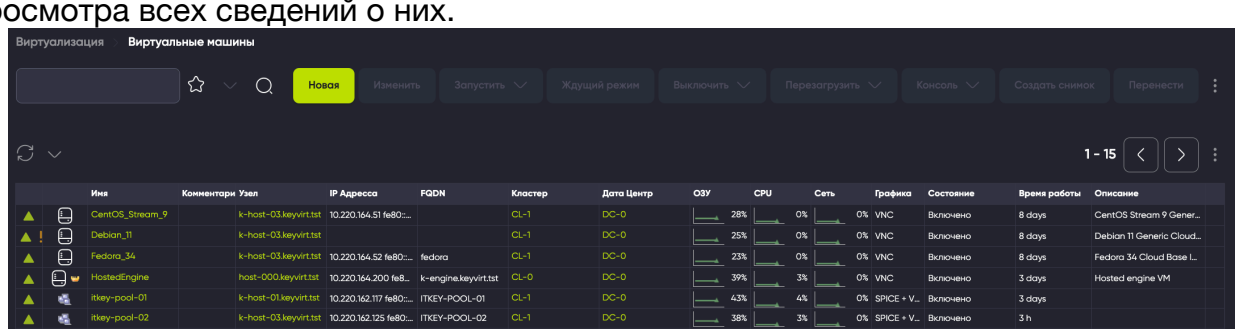


Рисунок 18. Виртуальные машины

Управление виртуальными машинами осуществляется с помощью панели инструментов для ВМ в правом верхнем углу. В зависимости от статуса ВМ, вы можете создавать, редактировать, удалять, приостанавливать, выключать,

мигрировать виртуальные машины, а также создавать для них снимки и открывать консоль.
Таблица с ВМ отображает машины и все подробности о них.

3.1.4.2 Шаблоны (Templates)

Данный подраздел предназначен для работы с шаблонами виртуальных машин и просмотра всех сведений о них. Шаблон – это копия виртуальной машины, которую вы можете использовать для упрощения последующего многократного создания похожих виртуальных машин.

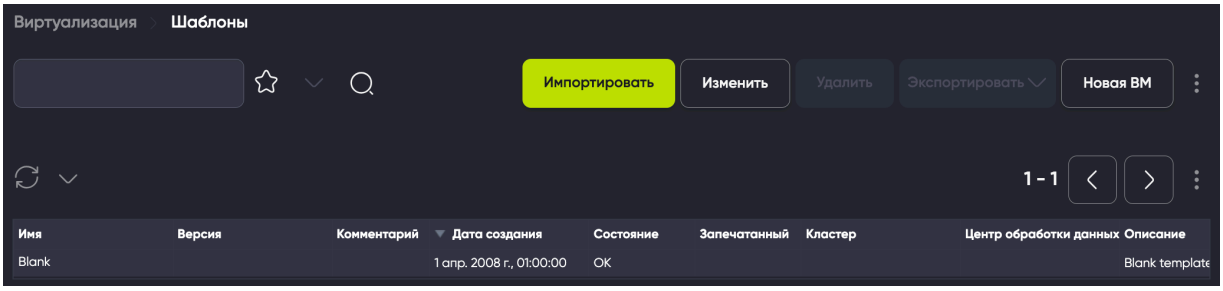


Рисунок 19. Шаблоны

Управление шаблонами осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу. В зависимости от статуса шаблона, вы можете создавать, редактировать, удалять, экспортировать и импортировать шаблоны.
Таблица с шаблонами отображает шаблоны и все подробности о них.

3.1.4.3 Пулы (Pools)

Данный подраздел предназначен для создания, редактирования и удаления пулов MAC-адресов. Пулы MAC-адресов определяют диапазон(ы) MAC-адресов, выделенных для каждого кластера.

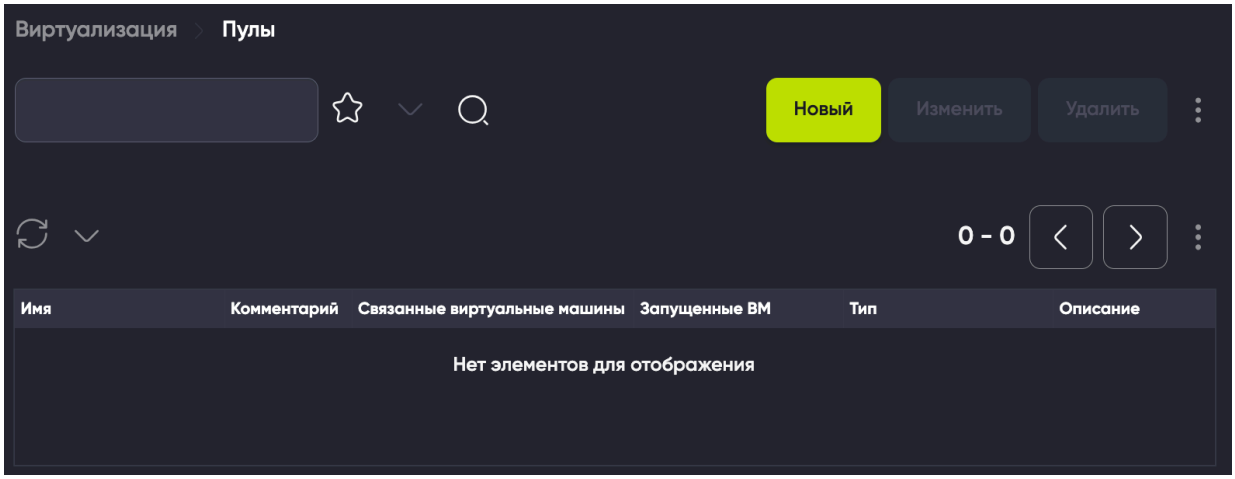


Рисунок 20. Пулы

Управление пулами осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица с пулами отображает пулы и все подробности о них.

3.1.4.4 Узлы (Hosts)

Данный подраздел предназначен для работы с узлами виртуальных машин. Узлы, также известные как гипервизоры, являются физическими серверами, на которых работают виртуальные машины.

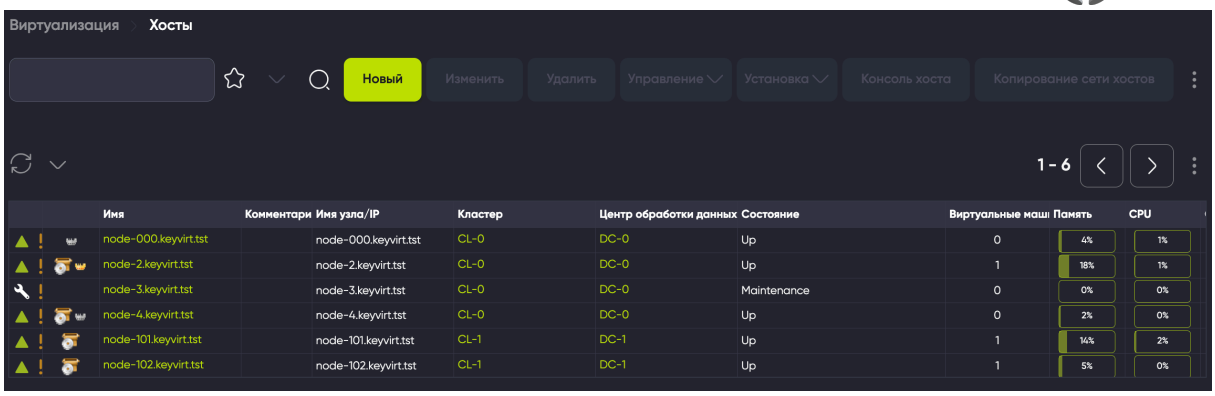


Рисунок 21. Узлы

Управление узлами осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу. В зависимости от статуса узла, вы можете создавать, редактировать, удалять, приостанавливать, выключать, переустанавливать узлы, а также копировать сети узла и открывать консоль.
Таблица с узлами отображает узлы и все подробности о них.

3.1.4.5 Дата-центры (Data Centers)

Данный подраздел предназначен для создания, редактирования и удаления дата-центров. Дата-центры определяют набор ресурсов, используемых в конкретной среде, и считаются контейнерными ресурсами.

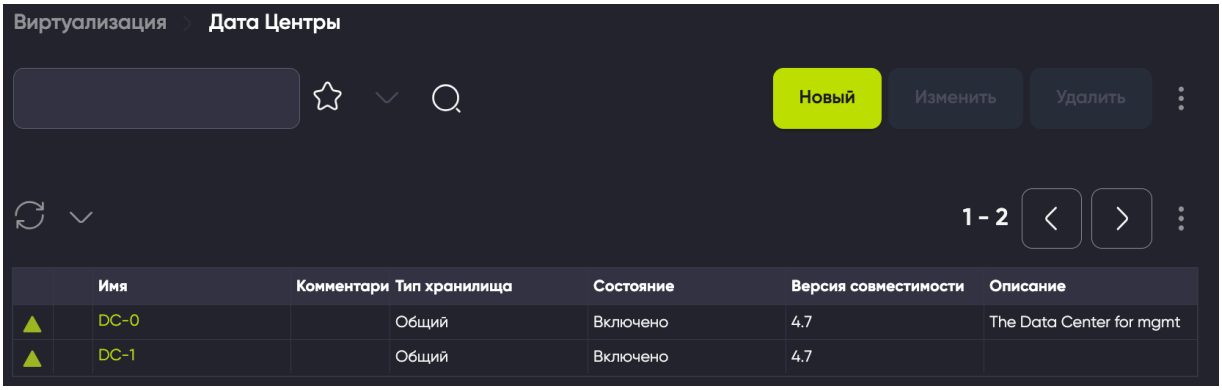


Рисунок 22. Дата-центры

Управление дата-центрами осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица с дата-центрами отображает дата-центры и все подробности о них.

3.1.4.6 Кластеры (Clusters)

Данный подраздел предназначен для создания, редактирования, обновления и удаления кластеров. Кластер – это логическая группа узлов, которые совместно используют одни и те же домены хранения и имеют один и тот же тип процессора.

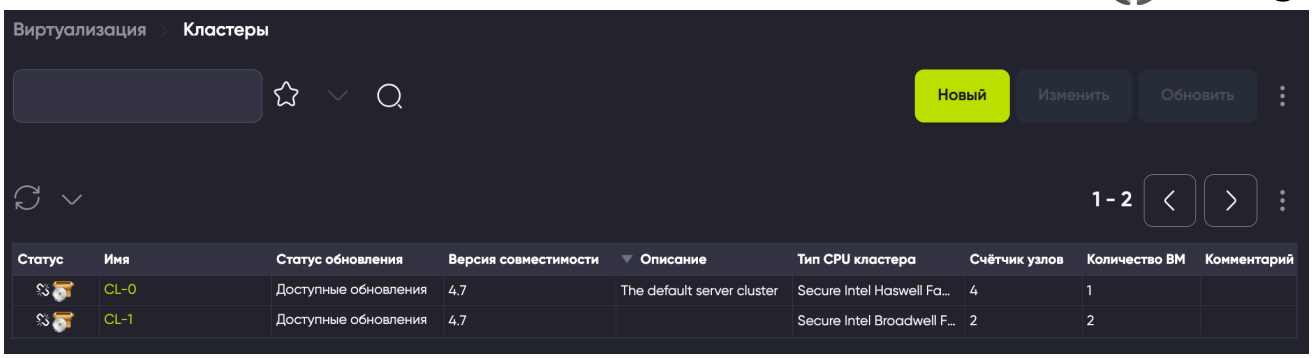


Рисунок 23. Кластеры

Управление кластерами осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица с кластерами отображает кластеры и все подробности о них.

3.1.5 Сеть (Network)

Данный раздел предназначен для управления сетевыми ресурсами, такими как профили vNIC и логические сети. Он состоит из следующих подразделов: **Профили vNIC** (**vNIC Profiles)** и **Сети (Networks)**.
В верхней части окна есть специальный раздел для быстрого поиска по всей таблице на выбранной вкладке. Эта панель также применима для обоих подразделов ниже.
Строка поиска – строка для выполнения поиска по ключевым словам и закладкам. Можно очистить поле поиска, сохранить поиск и настроить параметры поиска.

- – принудительное обновление.
- ▼ – выбрать частоту обновления.

3.1.5.1 Профили vNIC (vNIC Profiles)

Данный подраздел предназначен для создания, редактирования и удаления профилей vNIC.

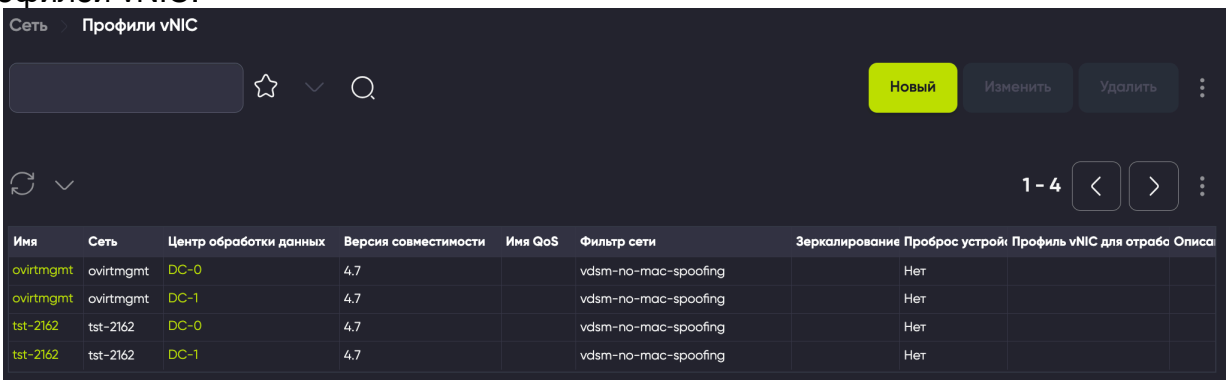
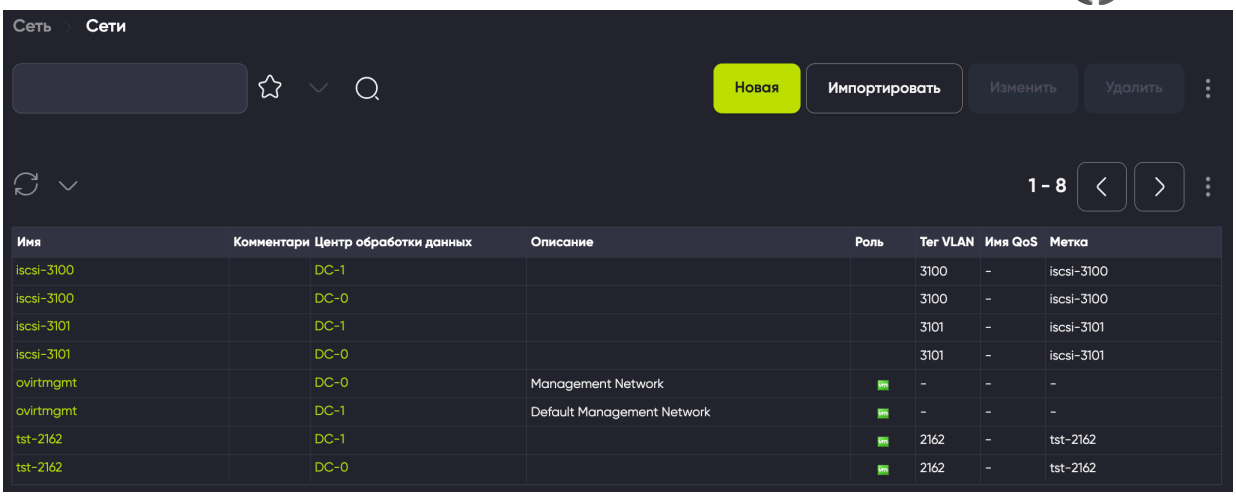


Рисунок 24. Профили vNIC

Управление профилями vNIC осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица отображает профили vNIC и все подробности о них.

3.1.5.2 Сети (Networks)

Данный подраздел предназначен для создания, редактирования, обновления и удаления логических сетей.



Имя	Комментари	Центр обработки данных	Описание	Роль	Тег VLAN	Имя QoS	Метка
iscsi-3100		DC-1			3100	-	iscsi-3100
iscsi-3100		DC-0			3100	-	iscsi-3100
iscsi-3101		DC-1			3101	-	iscsi-3101
iscsi-3101		DC-0			3101	-	iscsi-3101
ovirtmgmt		DC-0	Management Network		-	-	-
ovirtmgmt		DC-1	Default Management Network		-	-	-
tst-2162		DC-1			2162	-	tst-2162
tst-2162		DC-0			2162	-	tst-2162

Рисунок 25. Сети

Управление сетями осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица с сетями отображает сети и все подробности о них.

3.1.6 Хранилище (Storage)

Данный раздел предназначен для управления ресурсами по хранению данных, такими как домены хранения, тома и диски. Он состоит из следующих подразделов: **Дата Центры (Data Centers), Кластеры (Clusters), Домены (Domains), Тома (Volumes), Диски (Disks).**
В верхней части окна есть специальный раздел для быстрого поиска по всей таблице на выбранной вкладке. Эта панель также применима для обоих подразделов ниже.
Строка поиска – строка для выполнения поиска по ключевым словам и закладкам. Можно очистить поле поиска, сохранить поиск и настроить параметры поиска.

- – принудительное обновление.
- ▼ – выбрать частоту обновления.

3.1.6.1 Дата-центры (Data Centers)

Данный подраздел полностью идентичен одноименному подразделу в разделе **Виртуализация**, описанному выше.

3.1.6.2 Домены (Domains)

Данный подраздел предназначен для создания, редактирования, импорта, удаления и управления LUN доменов хранения. Домен хранения – это набор образов, имеющих общий интерфейс хранения. Домен хранения содержит полные образы шаблонов и виртуальных машин или ISO-файлы. Домен хранения может состоять либо из блочных устройств, либо из файловой системы.

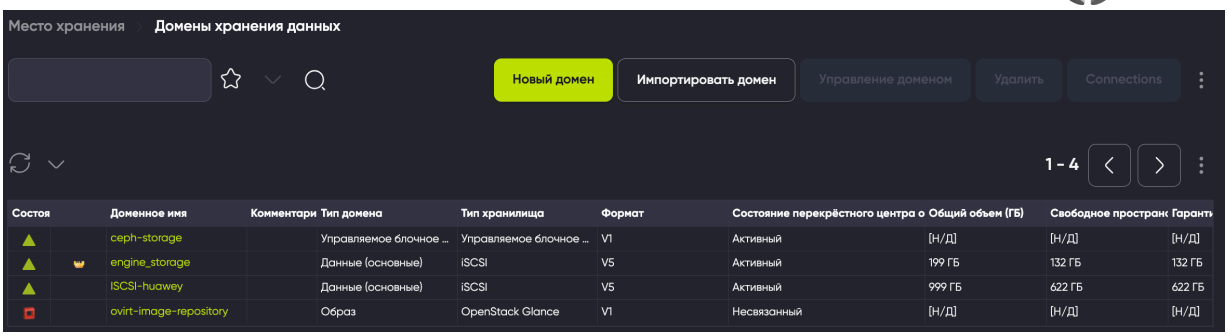


Рисунок 26. Домены

Управление доменами хранения осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица отображает домены и все подробности о них.

3.1.6.3 Тома (Volumes)

Данный подраздел предназначен для создания, запуска, остановки, редактирования и удаления томов.

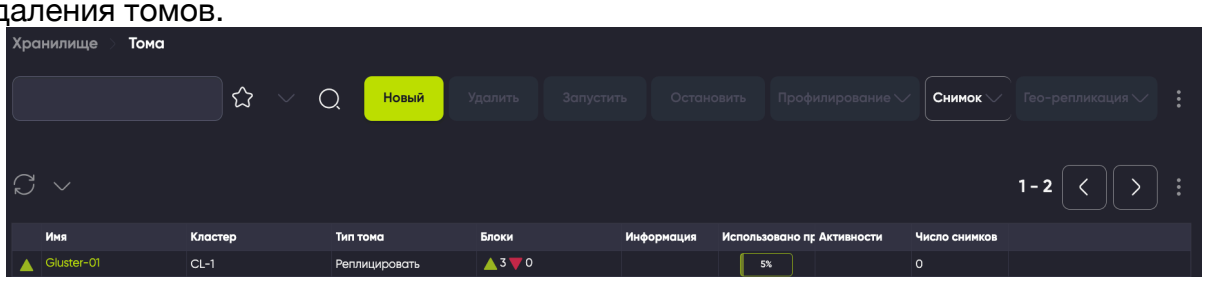


Рисунок 27. Тома

Управление томами осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица отображает тома и все подробности о них.

3.1.6.4 Диски (Disks)

Данный подраздел предназначен для создания, редактирования, копирования, переноса, загрузки, скачивания и удаления виртуальных дисков.

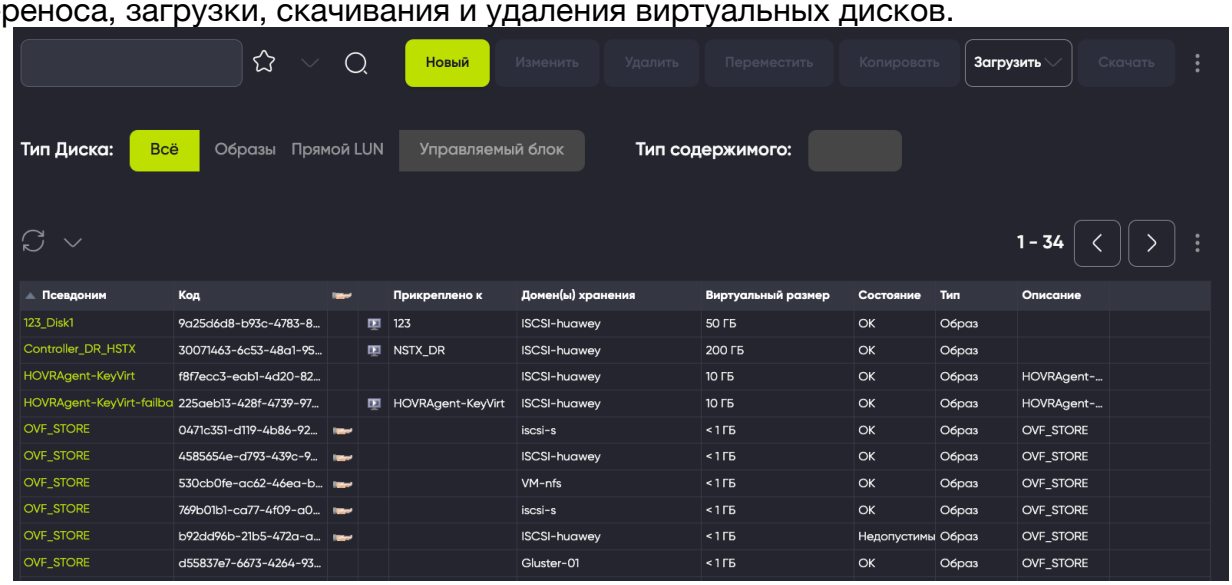


Рисунок 28. Диски

Управление дисками осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица с дисками отображает виртуальные диски и все подробности о них.

3.1.7 Администрирование (Administration)

Данный раздел предназначен для выполнения административных задач для Портала, таких как управление квотами, разрешениями пользователей и настройками учетной записи. Он состоит из следующих подразделов: **Провайдеры** (Providers), **Квота** (Quota), **Активные сессии пользователя** (User Sessions), **Пользователи** (Users), **Исправления** (Errata)**, Настройка** (Configure), **Настройки учетной записи** (Account Settings)**.** В верхней части окна есть специальный раздел для быстрого поиска по всей таблице на выбранной вкладке. Эта панель также применима для обоих подразделов ниже.
Строка поиска – строка для выполнения поиска по ключевым словам и закладкам. Можно очистить поле поиска, сохранить поиск и настроить параметры поиска.

- – принудительное обновление.
- ▼ – выбрать частоту обновления.

3.1.7.1 Провайдеры (Providers)

Данный подраздел предназначен для создания, редактирования и удаления внешних провайдеров. Провайдеры ресурсов, известные как внешние провайдеры, могут предоставлять такие ресурсы, как узлы виртуализации, образы виртуальных машин и сети.

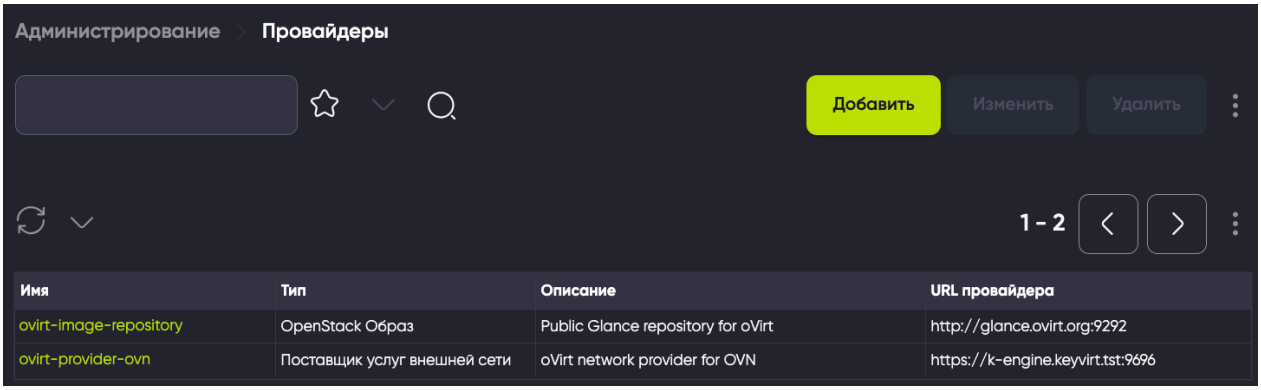


Рисунок 29. Провайдеры

Управление провайдерами осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица с провайдерами отображает провайдеров и все подробности о них.

3.1.7.2 Квота (Quota)

Данный подраздел предназначен для создания, редактирования, копирования и удаления квот. Квота – это инструмент ограничения ресурсов, предоставляемый KeyVirt. Квоты накладываются как дополнительные ограничения к тем, что уже имеются в назначенных ролях пользователя.

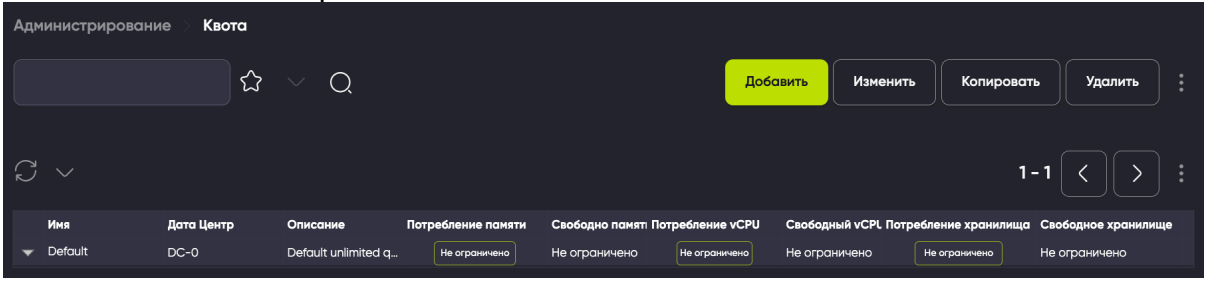


Рисунок 30. Квота

Управление квотами осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица с квотами отображает квоты и все подробности о них.

3.1.7.3 Активные сессии пользователей

Данный подраздел предназначен для работы с активными сессиями всех пользователей KeyVirt.

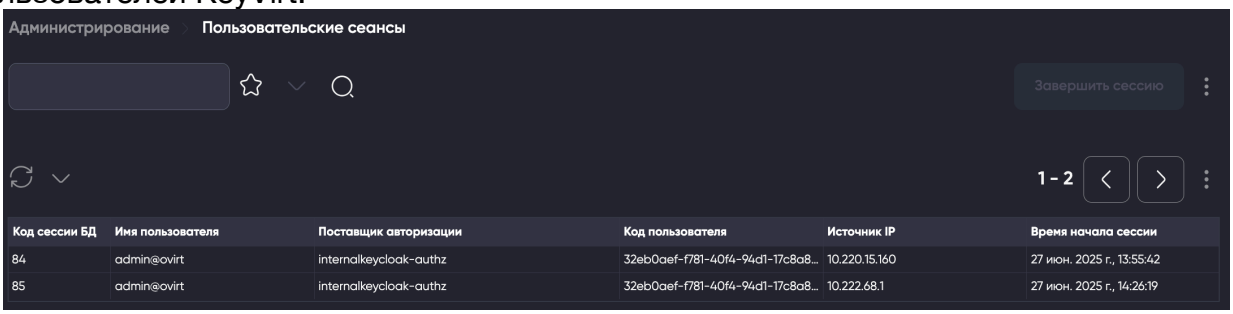


Рисунок 31. Пользовательские сеансы

Управление сессиями осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица отображает сессии и все подробности о них.

3.1.7.4 Пользователи (Users)

Данный подраздел предназначен для создания, редактирования и удаления профилей пользователей KeyVirt и назначения им тегов.

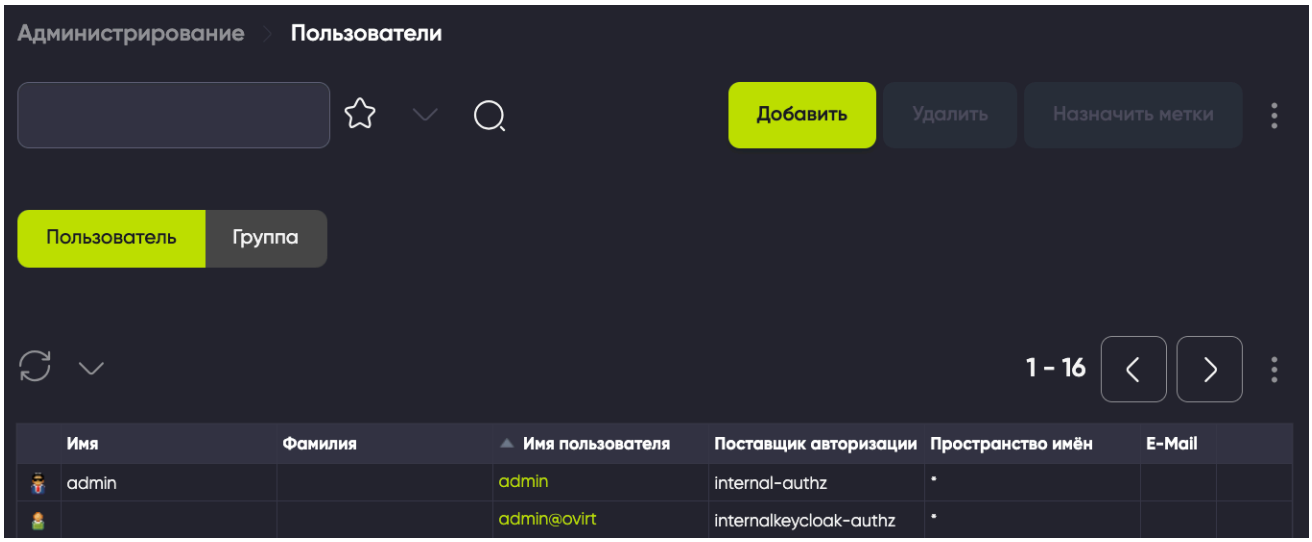


Рисунок 32. Пользователи

Управление пользователями осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица отображает профили пользователей и все подробности о них.

3.1.7.5 Исправления (Errata)

Для отображения сведений об ошибках требуется подключение отдельного сервера Syslog. В противном случае на экране будет отображаться следующее сообщение: Проблема получения исправлений: Движок не связан с провайдером Foreman/Satellite. Ошибки в движке отсутствуют.

3.1.7.6 Настройка (Configure)

Данный подраздел открывается в отдельном окне. Он предназначен для конфигурации параметров учетных записей всех пользователей и основных ресурсов KeyVirt. Здесь доступны следующие вкладки: **Роли** (Roles), **Системные разрешения** (System Permissions), **Политика планирования** (Scheduling Policies), **Типы экземпляров** (Instance Types), **Пул MAC адресов** (MAC Address Pools).

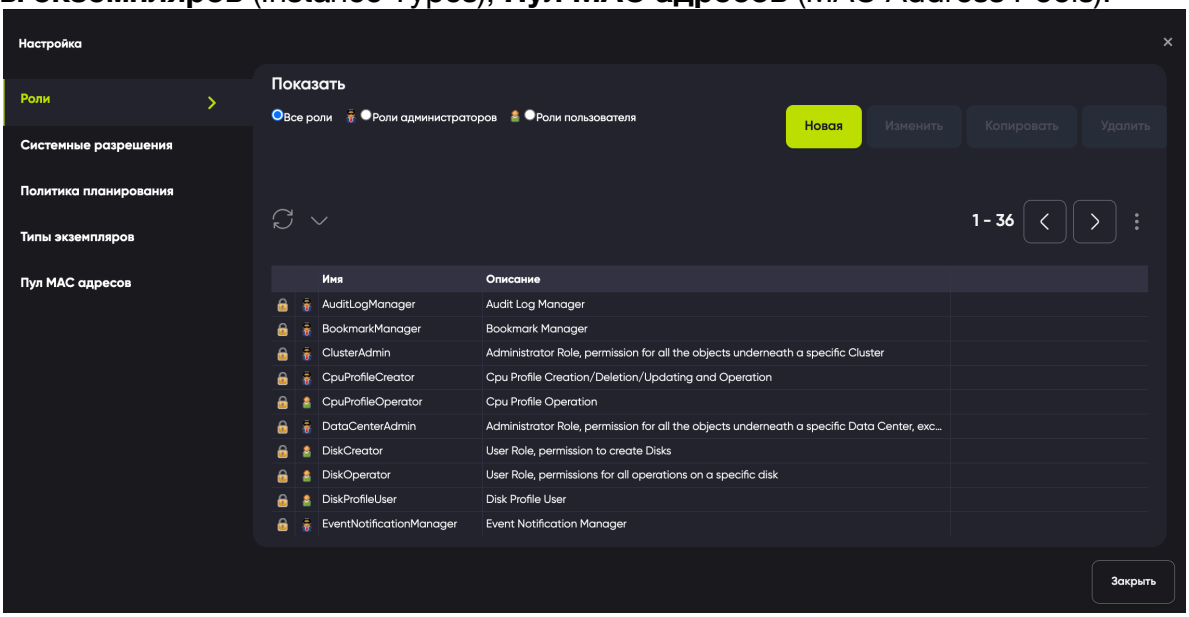


Рисунок 33. Настройка

Вкладки раздела выполняют следующие функции:

- **Роли (Roles)** – Конфигурация ролей.
- **Системные разрешения (System Permissions)** – Конфигурация системных разрешений.
- **Политика планирования (Scheduling Policies)** – Конфигурация политики планирования.
- **Типы экземпляров (Instance Types)** – Конфигурация типов ВМ.
- **Пул MAC адресов** (**MAC Address Pools)** – Конфигурация пулов MAC-адресов.

3.1.7.7 Настройки учетной записи (Account Settings)

Данный подраздел предназначен для конфигурации параметров вашей учетной записи, для чего используется KeyCloak – сервер для единого входа (SSO) и хранения учетных записей. Более подробно о KeyCloak см. на официальном сайте.

3.1.8 События (Events)

Данный подраздел предназначен для работы с уведомлениями KeyVirt.

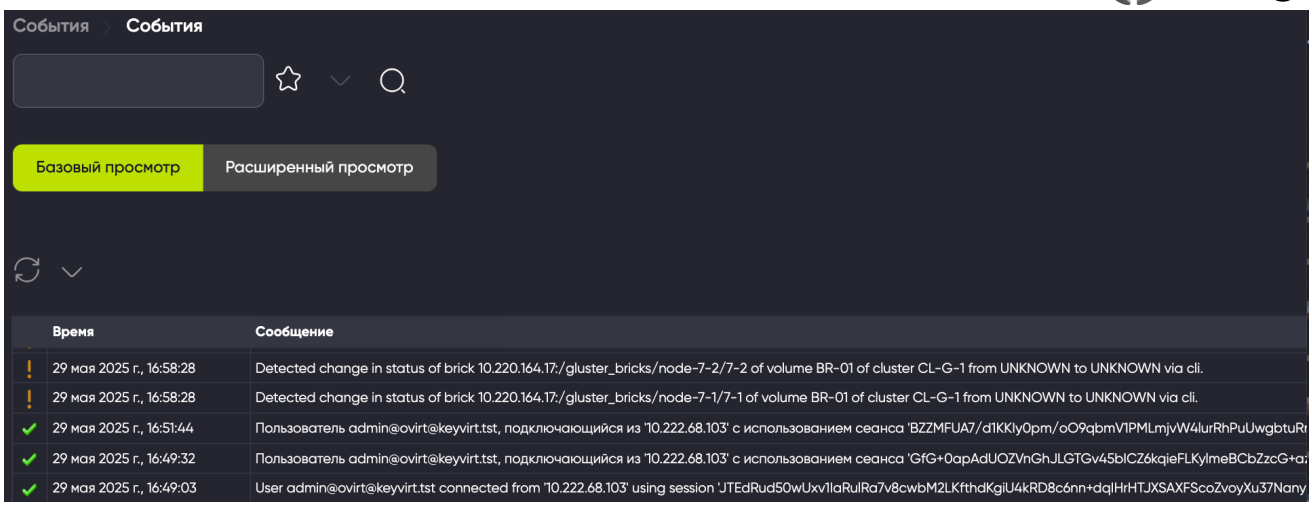


Рисунок 34. События

Управление уведомлениями осуществляется с помощью панели инструментов для шаблонов в правом верхнем углу.
Таблица отображает уведомления и все подробности о них.

3.2 ПОРТАЛ ВИРТУАЛЬНЫХ МАШИН

Портал виртуальных машин предоставляет полный обзор виртуальных машин и позволяет пользователю запускать, останавливать, редактировать и просматривать сведения о виртуальной машине. Действия, доступные на Портале виртуальных машин, устанавливаются системным администратором. Системные администраторы могут делегировать пользователю дополнительные административные задачи, такие как:

- создание, редактирование и удаление виртуальных машин;
- управление виртуальными дисками и сетевыми интерфейсами;
- создание и использование моментальных снимков для восстановления виртуальных машин в предыдущие состояния.

Прямое подключение к виртуальным машинам упрощается с помощью клиентов SPICE или VNC. Оба протокола предоставляют пользователю среду, аналогичную локально установленному рабочему столу. Администратор указывает протокол, используемый для подключения к виртуальной машине во время создания виртуальной машины.

3.2.1 Элементы графического пользовательского интерфейса

Интерфейс у Портала виртуальных машин проще, чем у Портала администратора. Вы можете выполнять общие задачи виртуальной машины, изменять параметры входа и просматривать сообщения на экране Портала. Доступны следующие ключевые элементы: 1) Панель заголовка; 2) Панель инструментов и 3) Панель виртуальных машин. Рисунок ниже отображает расположение этих ключевых элементов на Портале.

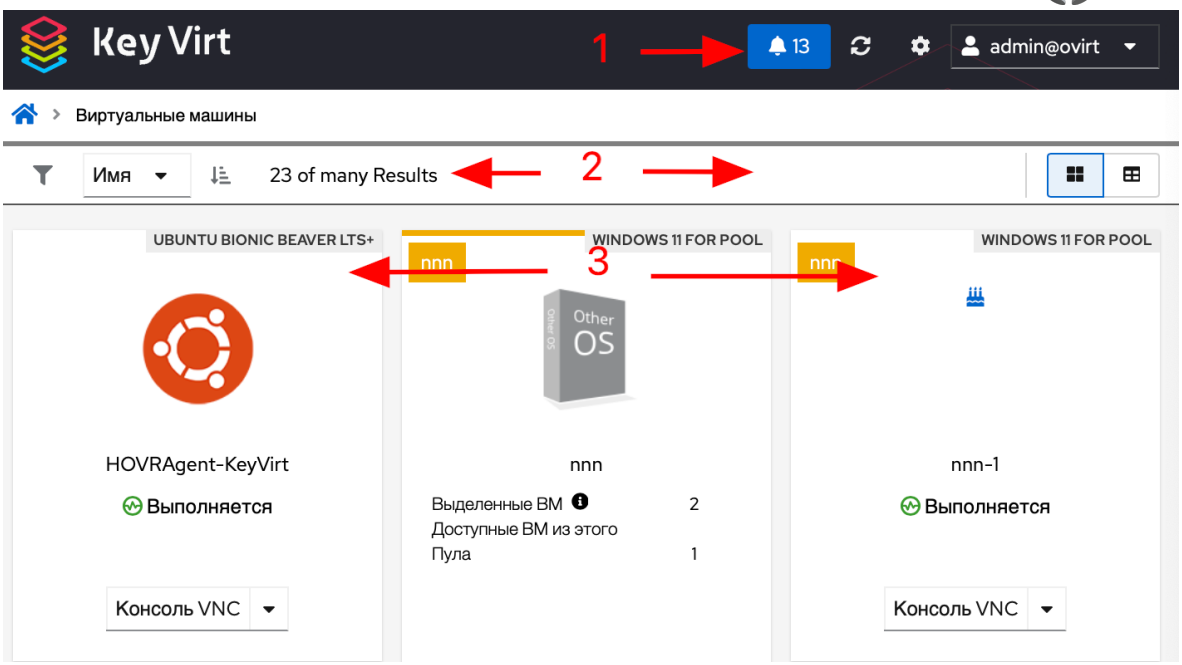


Рисунок 35. Расположение ключевых элементов Портала

3.2.1.1 Панель заголовка (Header bar)

Эта панель доступна в правом верхнем углу Портала.

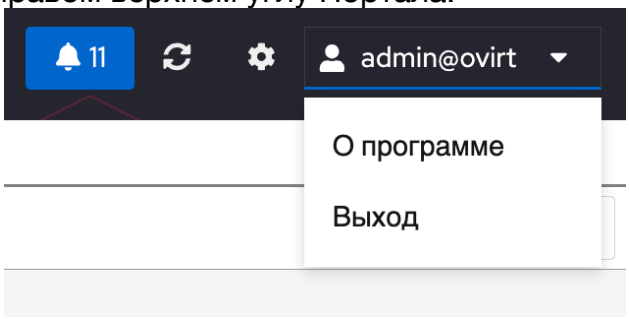


Рисунок 36. Панель заголовка

Панель заголовка содержит следующие кнопки:

- **Уведомления** (Notifications) – отображает уведомления.
- **Обновить** (Refresh) – обновление дисплея вручную. См. также *Интервал обновления*.
- **Настройки учетной записи (**Account Settings) – позволяет настроить параметры вошедшего в систему пользователя, которые сохраняются на сервере.

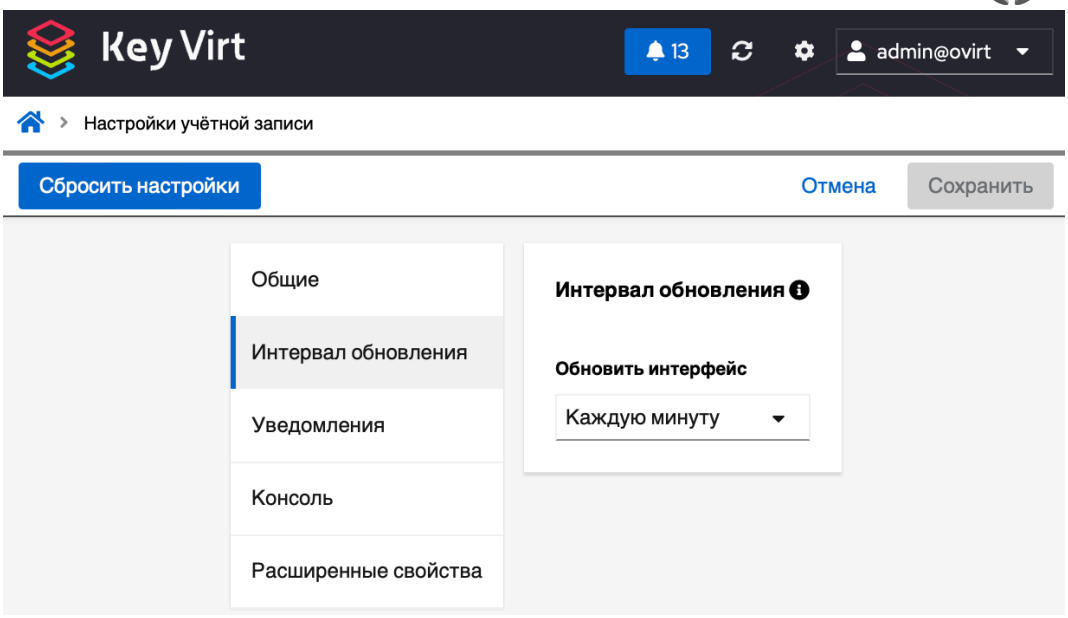


Рисунок 37. Настройки учетной записи

- Сбросить настройки (Reset settings) – позволяет сбросить все параметры обратно к первоначальным установкам по умолчанию.
- Общие (General) – отображает имя пользователя, адрес электронной почты и позволяет изменить язык пользовательского интерфейса.
- Интервал обновления (Refresh Interval) – установите интервал автоматической частоты обновления пользовательского интерфейса.
- Уведомления (Notifications) – позволяет отключить все уведомления за заданный интервал времени. Этот параметр не сохраняется на сервере, поэтому перезагрузка страницы очистит эти настройки.
- Консоль (Console) – настройки применяются глобально для всех ВМ.
  - Выберите предпочитаемую консоль. Это будет первая опция консоли, отображаемая на карте виртуальной машины (консоль VNC, консоль VNC (браузер), консоль SPICE, удаленный рабочий стол).
  - Подключаться автоматически (Connect automatically) – опция автоматического входа в консоль.
    Включает автоматическое подключение к консоли выбранной виртуальной машины после входа пользователя на Портал.
  - Настройки VNC (VNC Options)
  - Настройки VNC (браузер) (VNC (Browser) Options)
  - Настройки SPICE (SPICE Options)
  - Настройки текстовой консоли (Serial Console Options) – ключ SSH для аутентификации.
- Расширенные свойства (Advanced Options) – включите сохранение языковых настроек на сервере. Включите параметр «Выбранный язык/язык запроса URL» на целевой странице, чтобы переопределить выбранный язык настроек пользователя после каждого входа в систему. Это обеспечивает совместимость с предыдущим поведением языковых настроек.

- Пользователь (User) – отображает имя текущего пользователя, вошедшего в систему.
  - О программе (About) – информация о версии Портала.
  - Выход (Log out) – выход из Портала виртуальных машин.

Примечание: Вход в систему определяется на основе возраста сеанса. Значение по умолчанию – 60 секунд. Вход в систему определяется на основе возраста сеанса. Значение по умолчанию – 60 секунд.

3.2.1.2 Панель инструментов (Toolbar)

Панель инструментов позволяет искать виртуальные машины с помощью фильтра по имени, статусу или операционной системе виртуальных машин или объектов пула. Отображается количество работающих в настоящее время виртуальных машин или объектов пула, а также их общее количество.

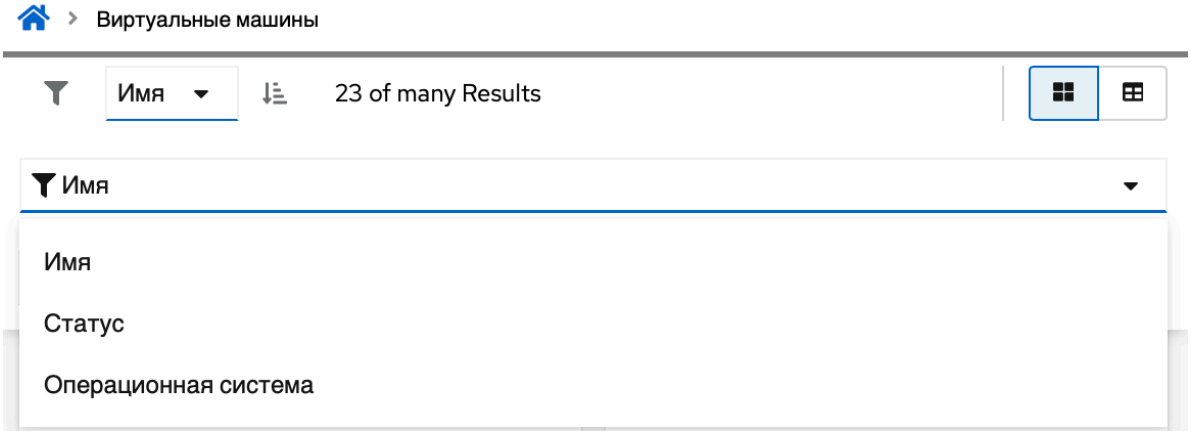


Рисунок 38. Панель инструментов

3.2.1.3 Панель виртуальных машин (Virtual machines panel)

На панели виртуальных машин отображаются карточки виртуальных машин, каждая из которых отображает операционную систему, имя, состояние и параметры управления для виртуальной машины. Чтобы увидеть имя виртуальной машины, нужно навести курсор мыши на середину карточки, где затемнено название.

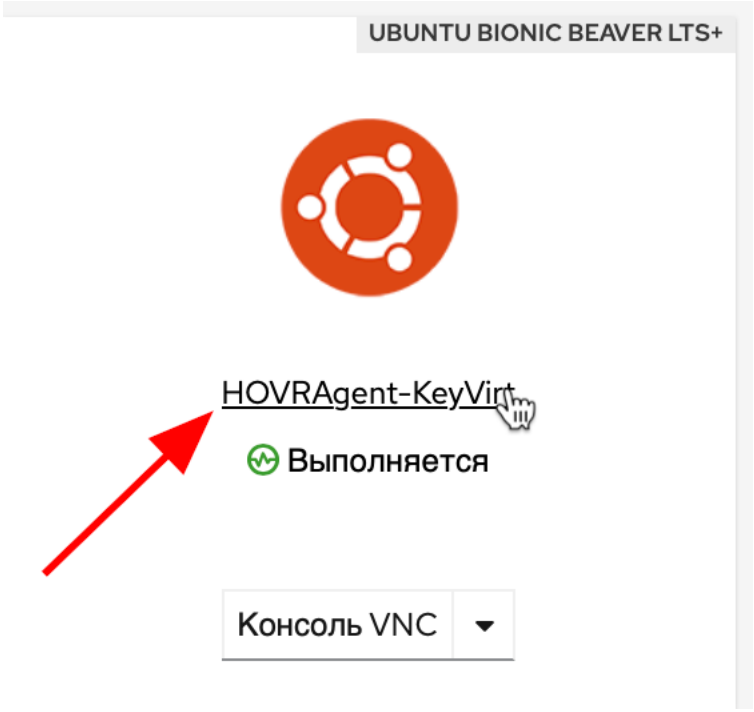


Рисунок 39. Карточка виртуальной машины

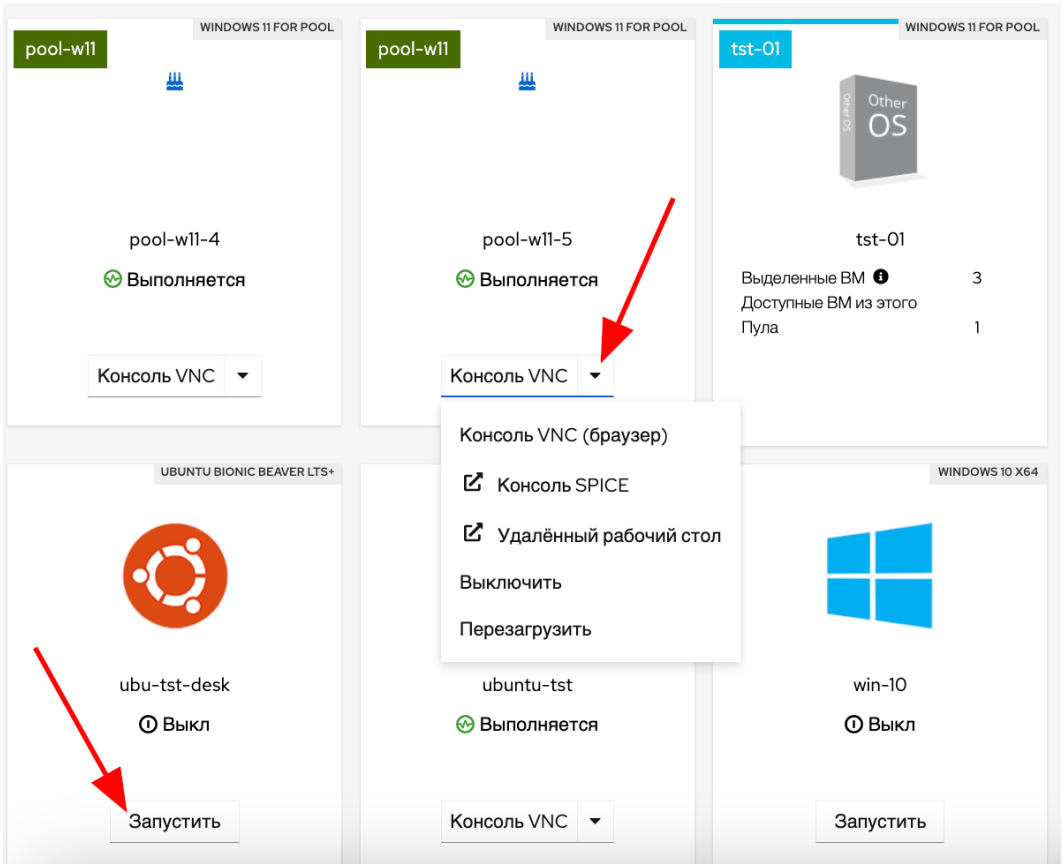


Рисунок 40. Выбор действия для виртуальной машины

- **Run** – Запустить (доступно для выключенных виртуальных машин)
- VNC Console – VNC-консоль
- VNC Console (Browser) – Консоль VNC (браузер)
- Remote Desktop – Удаленный рабочий стол (доступно только для виртуальных машин Windows)
- Take a virtual machine – Взять виртуальную машину (доступно только при использовании пула)
- **Suspend** – Приостановить
- **Shutdown** – Выключить
- **Reboot** – Перезагрузить

Консоль – это окно, позволяющее просматривать начальный экран, экран выключения и рабочий стол виртуальной машины, а также взаимодействовать с этой виртуальной машиной так же, как с физической машиной. По умолчанию используется протокол VNC. При нажатии на кнопку *Консоль* происходит автоматическое скачивание файла с расширением VV (.vv). В KeyVirt приложением для открытия консоли на виртуальной машине по умолчанию является Remote Viewer, которое необходимо установить заранее на клиентском компьютере.

3.2.2 Управление виртуальными машинами

На панели виртуальных машин при нажатии на выбранную виртуальную машину откроется окно, где можно выполнить следующие действия с виртуальной машиной:

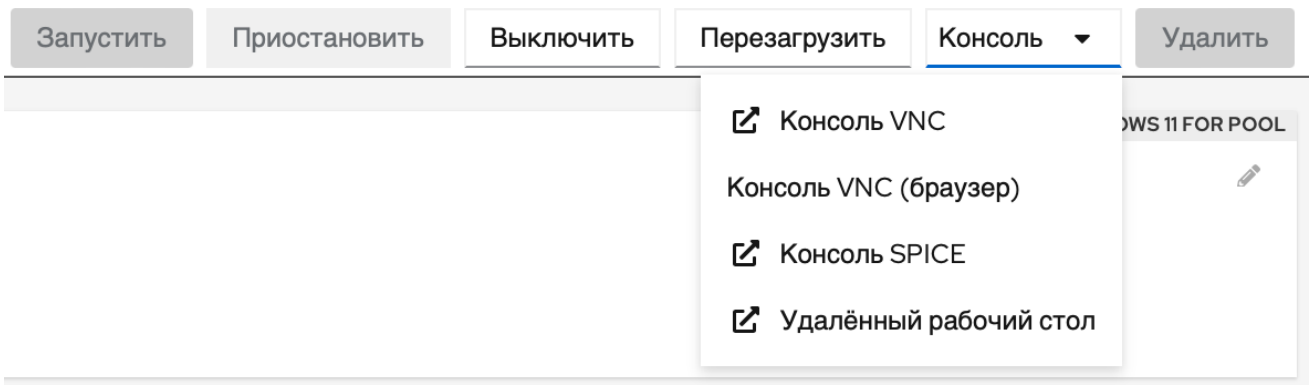


Рисунок 41. Действия с виртуальными машинами

- **Запустить** (Run) – запуск виртуальной машины. Действие доступно, когда виртуальная машина приостановлена или остановлена.
- **Приостановить** (Suspend) – временная остановка виртуальной машины. Действие доступно, когда виртуальная машина работает. Для выполнения этого действия необходимо выбрать кнопку **Приостановить** в раскрывающемся меню.
- **Выключить** (Shutdown) – полная остановка (выключение) виртуальной машины. Действие доступно, когда виртуальная машина работает. Для выполнения этого действия необходимо выбрать кнопку **Выключить** в раскрывающемся меню.
- **Перезагрузить** (Reboot) – перезапуск виртуальной машины. Действие доступно, когда виртуальная машина работает. Для выполнения этого действия необходимо выбрать кнопку **Перезагрузить** в раскрывающемся меню.
- **Консоль** (Console) – получение доступа к консоли виртуальной машины. Действие доступно, когда виртуальная машина работает.
    - VNC console – получение доступа к VNC-консоли.
    - VNC console (Browser) – получение доступа к VNC-консоли в браузере.

Примечание. Прежде чем вы сможете использовать виртуальную машину Linux, вы должны установить нужную операционную систему и зарегистрироваться в Content Delivery Network. Установить операционную систему можно следующими способами:

- Использовать предварительно установленный образ, создав клонированную виртуальную машину на основе шаблона.
- Использовать предустановленный образ с прикрепленного предустановленного диска.
- Установить операционную систему через загрузочное меню PXE или из файла ISO.

Управление ВМ включает создание, редактирование, клонирование ВМ, редактирование свойств ВМ, а также много другое.
Подробнее обо всех задачах см. в разделе *АДМИНИСТРИРОВАНИЕ ВИРТУАЛЬНЫХ МАШИН*.

3.2.3 Просмотр сведений о виртуальных машинах

Чтобы посмотреть сведения о виртуальной машине на Портале виртуальных машин, нужно щелкнуть на имя выбранной машины. Детали отображаются на следующих карточках:

- **Описание и состояние виртуальной машины** (Virtual Machine Description and Status): Операционнная система, Имя, Статус (например, Выполняется, Выключается, Выкл, Ожидает запуска, В ждущем режиме), Описанние.

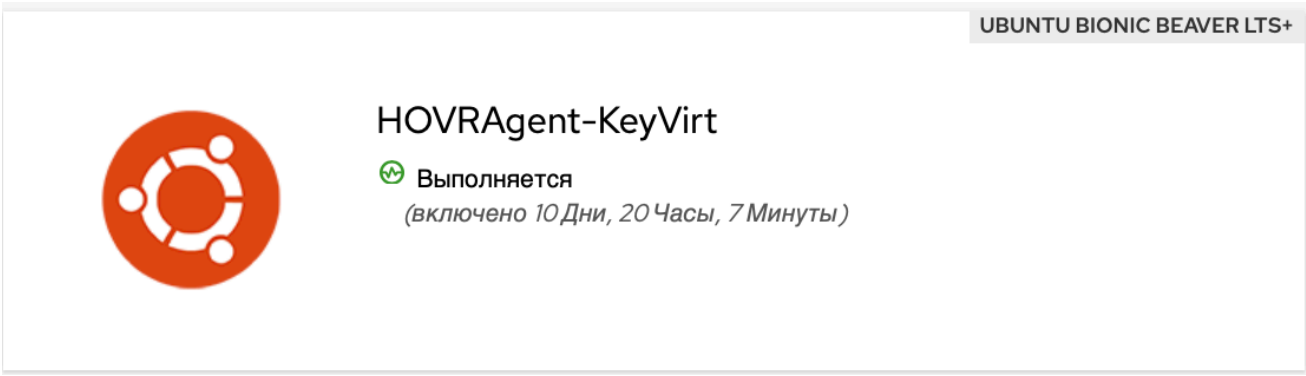


Рисунок 42. Описание и состояние виртуальной машины

- **Подробная информация** (Details): Узел, IP-адрес, FQDN (полное доменное имя виртуальной машины – чтобы получить это значение, гостевой агент должен быть установлен на виртуальной машине), Кластер, Дата-центр, Шаблон, CD, Cloud-Init status (Sysprep на виртуальных машинах Windows), статус Меню загрузки, Console, Оптимизировано для (Сервер/Рабочая Станция/Высокая производительность), CPUs, ОЗУ.

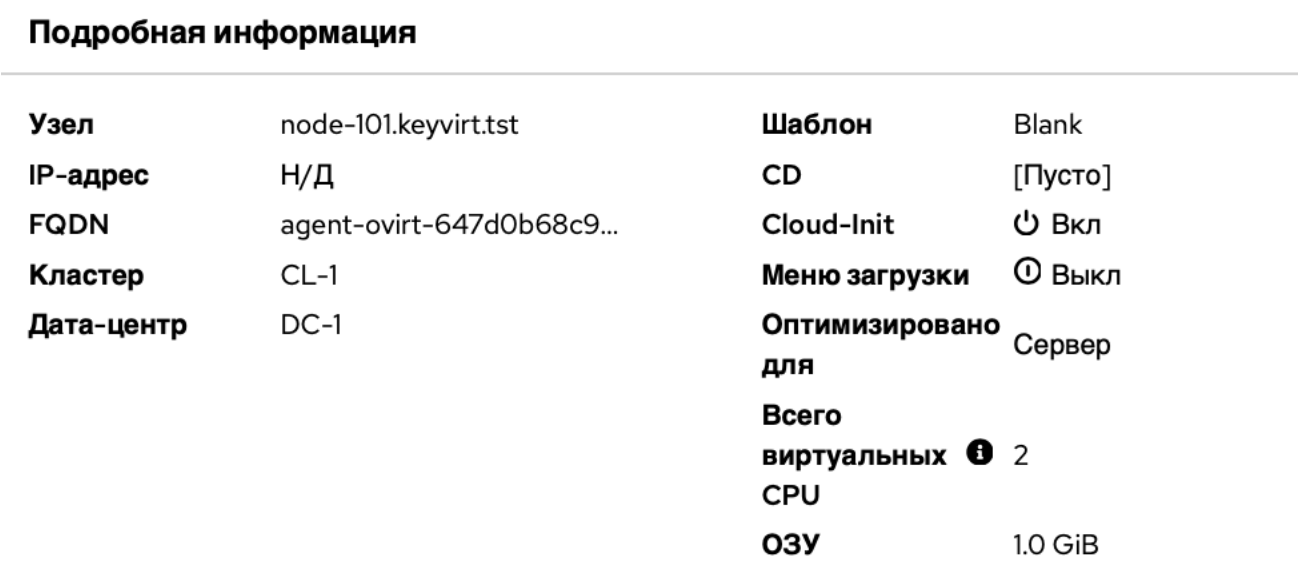


Рисунок 43. Подробная информация

- **Использование ресурсов** (Utilization): отображает статистику использования ЦП, памяти, сети и использования (значения CPU, Networking и Disk отображаются только при работающей виртуальной машине). Отображение использования диска может отличаться, если гостевой агент установлен на виртуальной машине.

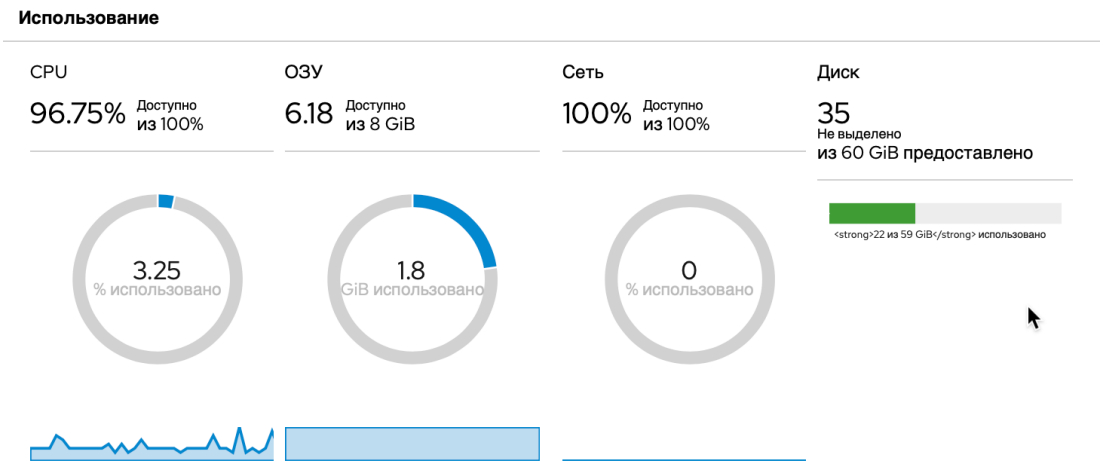


Рисунок 44. Использование ресурсов

- **Снимки состояния** (Snapshots): отображает список сохраненных снимков.

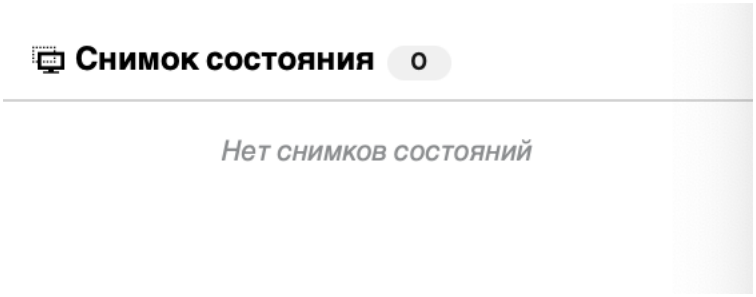


Рисунок 45. Снимки состояния

- **Сетевые интерфейсы** (Network Interfaces): отображает список сетевых интерфейсов, определенных для этой виртуальной машины.

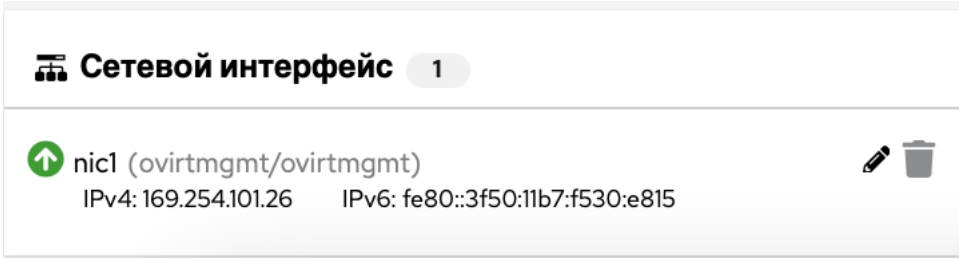


Рисунок 46. Сетевые интерфейсы

- **Диски** (Disks): отображает список дисков, определенных для этой виртуальной машины.

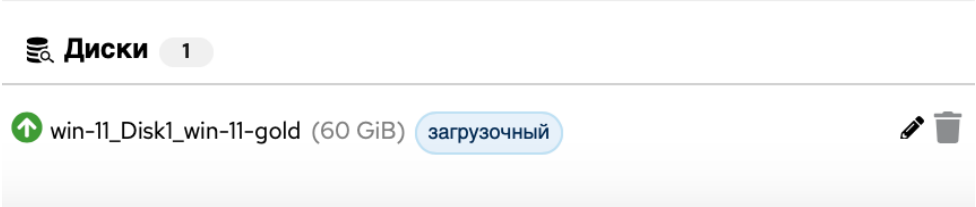


Рисунок 47. Диски

3.3 ПОРТАЛ МОНИТОРИНГА

Мониторинг осуществляется с помощью инструмента визуализации Grafana на Портале мониторинга (Monitoring Portal). Grafana – это веб-инструмент

пользовательского интерфейса, используемый для отображения отчетов на основе данных, собранных из базы данных KeyVirt. Подробнее о работе Grafana можно узнать на официальном сайте.
Для доступа к интерфейсу Grafana требуется авторизация.

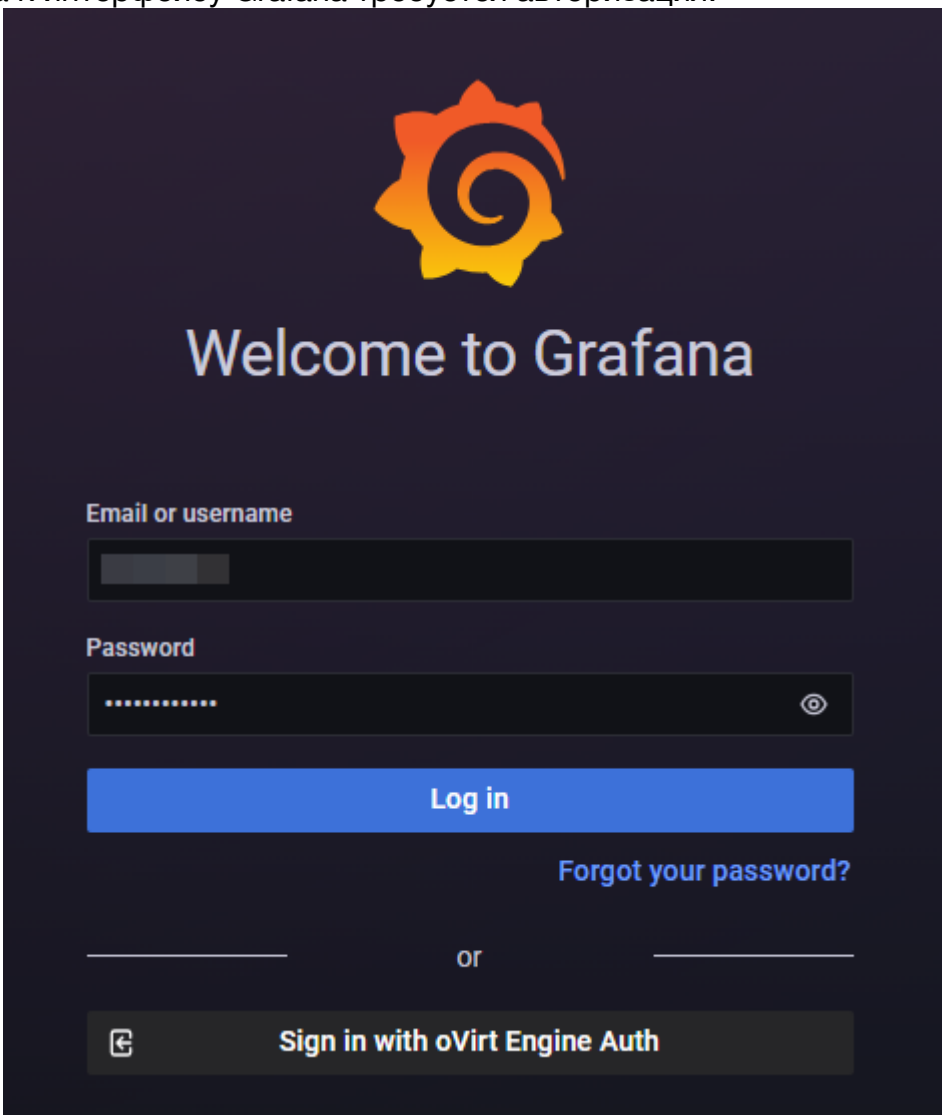


Рисунок 48. Авторизация в Grafana

После успешной авторизации открывается интерфейс Grafana, который выглядит следующим образом:

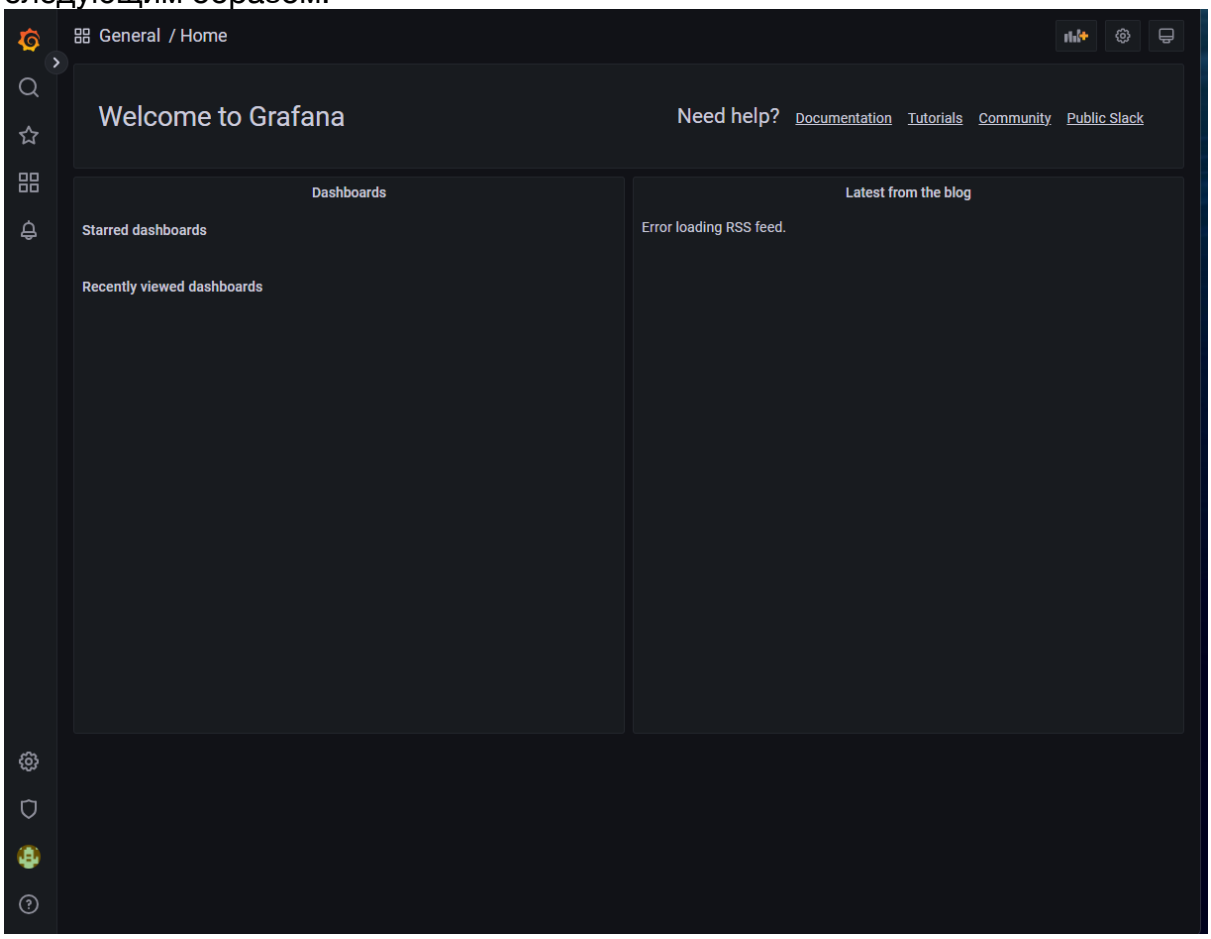


Рисунок 49. Интерфейс Grafana

Подробнее о всех возможностях Grafana см. в Руководстве по управлению Grafana в KeyVirt, а также в официальной документации Grafana.

4 АДМИНИСТРИРОВАНИЕ РЕСУРСОВ

Внимание! Инструкции и общие сведения о пуле виртуальных машин предоставляются отдельно по запросу.

4.1 КАЧЕСТВО ОБСЛУЖИВАНИЯ (QOS)

KeyVirt позволяет создавать записи качества обслуживания (QoS), чтобы обеспечить детальный контроль над уровнем входных и выходных данных, обработки и сетевых возможностей, к которым могут получить доступ ресурсы в вашей среде. Записи качества обслуживания определяются на уровне дата-центра и назначаются профилям, созданным в кластерах и доменах хранения. Затем профили назначаются отдельным ресурсам в кластерах и доменах хранения, где данные профили были созданы.

4.1.1 Качество обслуживания хранилища

Качество обслуживания хранилища определяет максимальный уровень пропускной способности и максимальный уровень операций ввода-вывода для виртуального

диска в домене хранения. Назначение качества обслуживания хранилища для виртуального диска позволяет точно настроить производительность доменов хранения и предотвратить влияние операций хранения, связанных с одним виртуальным диском, на возможности хранения, доступные для других виртуальных дисков, размещенных в том же домене хранения.

4.1.1.1 Создание записи о качестве обслуживания хранилища

Для создания записи качества обслуживания хранилища выполните следующие действия:

1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на название дата-центра. Откроется подробное описание.
3. Нажмите на вкладку *косы(QoS)*.
4. В разделе *Хранилище* нажмите *Новая*.
5. Введите *Имя QoS* и *Описание* для качества обслуживания хранилища.
6. Укажите Пропускная способность качества обслуживания, щелкнув на один из переключателей:
   - Нет
   - Всего – введите максимально допустимую общую пропускную способность в поле МБ/с;
   - Чтение/запись – введите максимально допустимую пропускную способность для операций чтения в левом поле МБ/с и максимально допустимую пропускную способность для операций записи в правом поле МБ/с.
7. Укажите входное и выходное качество обслуживания (IOps), щелкнув на один из переключателей:
   - Нет
   - Всего – введите максимально допустимое количество операций вводавывода в секунду в поле IOps;
   - Чтение/запись – введите максимально допустимое количество операций ввода в секунду в левом поле IOps и максимально допустимое количество операций вывода в секунду в правом поле IOps.
8. Нажмите OK.

Запись о качестве хранения для обслуживания создана. Теперь можно создавать профили дисков на основе этой записи в доменах хранения данных, которые принадлежат дата-центру.

4.1.1.2 Удаление записи о качестве обслуживания в хранилище

Для удаления записи о качестве обслуживания хранилища выполните следующие действия:

1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на название дата-центра. Откроется подробное описание.
3. Нажмите на вкладку *косы(QoS)*.
4. В разделе *Хранилище* выберите запись качества хранилища и нажмите *Удалить*.
5. Нажмите OK.

Если какие-либо профили диска были основаны на этой записи, запись качества хранения для этих профилей автоматически устанавливается на [unlimited].

4.1.2 Качество обслуживания сети виртуальных машин

Качество обслуживания сети виртуальных машин – это функция, которая позволяет создавать профили для ограничения как входящего, так и исходящего трафика отдельных контроллеров виртуального сетевого интерфейса (vNIC). С помощью этой функции можно ограничить пропускную способность на нескольких уровнях, контролируя потребление сетевых ресурсов.

4.1.2.1 Создание записи о качестве обслуживания сети виртуальной машины

Для создания записи качества обслуживания сети виртуальной машины выполните следующие действия:

1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на имя дата-центра, чтобы открыть подробное описание.
3. Перейдите на вкладку *косы(QoS)*.
4. В разделе *Сеть ВМ* нажмите кнопку *Новая*.
5. Введите имя записи качества обслуживания сети виртуальной машины.
6. Введите ограничения для *Входящего* (Inbound) и *Исходящего* (Outbound) сетевого трафика.
7. Нажмите OK.

Запись качества обслуживания сети, которую можно использовать в контроллере виртуального сетевого интерфейса, будет создана.

4.1.2.2 Параметры качества обслуживания сети виртуальных машин

Параметры качества обслуживания сети виртуальной машины позволяют настраивать ограничения пропускной способности как для входящего, так и для исходящего трафика на трех различных уровнях (таблица 16).

Таблица 16. Параметры QoS сети виртуальной машины

Имя поля	Описание
Дата центр	Дата-центр, к которому должна быть добавлена политика QoS сети виртуальных машин. Это поле настраивается автоматически в соответствии с выбранным дата-центром.
Имя	Имя для представления политики QoS сети виртуальной машины в Engine.
Входящий	Параметры, применяемые к входящему трафику. Установите или снимите флажок Inbound, чтобы включить или отключить эти параметры. • Среднее: Средняя скорость входящего трафика. • Пик: Скорость входящего трафика в пиковое время. • Разрыв: Скорость входящего трафика во время частичной потери пакетов.
Исходящий	Параметры, применяемые к исходящему трафику. Установите или снимите флажок Outbound, чтобы включить или отключить эти параметры. • Среднее: Средняя скорость исходящего трафика. • Пик: Скорость исходящего трафика в пиковое время. • Разрыв: Скорость исходящего трафика во время частичной потери пакетов.

Чтобы изменить максимальное значение, разрешенное полями Среднее, Пик или Разрыв, используйте команду engine-config, которая позволяет изменять значения

ключей конфигурации MaxAverageNetworkQoSValue, MaxPeakNetworkQoSValue или MaxBurstNetworkQoSValue. Чтобы изменения вступили в силу, необходимо перезапустить службу ovirt-engine. Например:
engine-config -s MaxAverageNetworkQoSValue=2048
systemctl restart ovirt-engine

4.1.2.3 Удаление записи о качестве обслуживания сети виртуальной машины

Чтобы удалить записи о качестве обслуживания сети виртуальной машины выполните следующие действия:
1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на имя дата-центра, чтобы открыть подробное описание.
3. Перейдите на вкладку *косы(QoS)*.
4. В разделе сеть виртуальной машины *Сеть ВМ* выберите запись качества обслуживания сети виртуальной машины и нажмите кнопку *Удалить*.
5. Нажмите OK.

4.1.3 Качество обслуживания сети узла

Качество обслуживания сети узла позволяет настраивать сети на узле, чтобы обеспечить управление сетевым трафиком через физические интерфейсы. Качество обслуживания хост-сети позволяет точно настроить производительность сети, контролируя потребление сетевых ресурсов на одном и том же контроллере физического сетевого интерфейса. Это помогает предотвратить ситуации, когда одна сеть приводит к тому, что другие сети, подключенные к тому же контроллеру физического сетевого интерфейса, больше не работают из-за интенсивного трафика. Благодаря настройке качества обслуживания хост-сети, эти сети теперь могут работать на одном контроллере физического сетевого интерфейса без проблем с перегрузкой.

4.1.3.1 Создание записи о качестве обслуживания сети узла

Для создания записи качества обслуживания сети узла выполните следующие действия:
1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на имя дата-центра, чтобы открыть подробное описание.
3. Перейдите на вкладку *косы(QoS)*.
4. В разделе *Сеть узла* нажмите кнопку *Новая*.
5. Введите имя QoS и описание для записи качества обслуживания.
6. Введите желаемые значения для *Общие веса*, *Ограничение скорости [Мбит/с]* и *Подтверждённая скорость [Мбит/с]*.
7. Нажмите OK.

4.1.3.2 Параметры качества обслуживания сети узла

Параметры качества обслуживания сети узла позволяют настраивать ограничения пропускной способности для исходящего трафика (таблица 17).
Таблица 17. Параметры QoS сети узла

Имя поля	Описание
Дата центр	Дата-центр, к которому должна быть добавлена политика QoS сети узла. Это поле настраивается автоматически в соответствии с выбранным дата-центром.

Имя QoS	Имя для представления политики QoS сети узла в Engine.
Описание	Описание политики QoS сети узла.
Исходящий	Параметры, применяемые к исходящему трафику. Установите или снимите флажок Outbound, чтобы включить или отключить эти параметры. • *Общие веса* (Weighted Share): показывает, какая часть пропускной способности логического канала должна быть выделена конкретной сети по сравнению с другими сетями, подключенными к тому же логическому каналу. Точная доля зависит от суммы долей всех сетей на этом канале. По умолчанию данное число находится в диапазоне 1-100. • *Ограничение скорости [Мбит/с]* (Rate Limit [Mbps]): Максимальная пропускная способность, используемая сетью. • *Ограничение скорости [Мбит/с]* (Committed Rate [Mbps]): Минимальная пропускная способность, необходимая сети. Установленная подтвержденная скорость не гарантирована и будет варьироваться в зависимости от сетевой инфраструктуры и подтвержденной скорости, запрашиваемой другими сетями на том же логическом канале.

4.1.3.3 Удаление записи о качестве обслуживания сети узла

Для удаления записи о качестве обслуживания хост-сети выполните следующие действия:
1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на имя дата-центра, чтобы открыть подробное описание.
3. Перейдите на вкладку *косы(QoS)*.
4. В разделе *Сеть узла* выберите запись качества обслуживания сети узла и нажмите кнопку *Удалить*.
5. Нажмите кнопку OK при появлении запроса.

4.1.4 Качество обслуживания процессора

Качество обслуживания ЦП определяет максимальный объем вычислительных возможностей, к которым виртуальная машина может получить доступ на узле, где она работает, выраженный в процентах от общей вычислительной мощности, доступной этому узлу. Назначение качества обслуживания ЦП для виртуальной машины позволяет предотвратить влияние рабочей нагрузки на одной виртуальной машине в кластере на ресурсы обработки, доступные другим виртуальным машинам в этом кластере.

4.1.4.1 Создание записи о качестве обслуживания ЦП

Для создания записи качества обслуживания ЦП выполните следующие действия:
1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на имя дата-центра, чтобы открыть подробное описание.
3. Перейдите на вкладку *косы(QoS)*.
4. В разделе CPU нажмите кнопку *Новая*.

5. Введите *Имя QoS* и *Описание* для записи качества обслуживания.
6. Введите максимальную обрабатывающую способность, разрешенную для ввода качества обслуживания, в поле *Ограничение (%)* в процентах.
7. Нажмите OK.

Запись о качестве обслуживания ЦП будет создана. Теперь можно создавать профили ЦП на основе этой записи в кластерах, принадлежащих дата-центру.

4.1.4.2 Удаление записи о качестве обслуживания ЦП

Для удаления записи о качестве обслуживания ЦП выполните следующие действия:

1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на имя дата-центра, чтобы открыть подробное описание.
3. Перейдите на вкладку *косы(QoS)*..
4. В разделе CPU выберите запись качества обслуживания ЦП и нажмите кнопку *Удалить*.
5. Нажмите OK.

4.2 ДАТА-ЦЕНТРЫ

4.2.1 Общие сведения о дата-центрах

Дата-центр – это логическая сущность, определяющая набор ресурсов, используемых в конкретной среде. Дата-центр считается контейнерным ресурсом, поскольку он состоит из логических ресурсов в виде кластеров и узлов, сетевых ресурсов в виде логических сетей и физических сетевых карт, и ресурсов хранения в виде доменов хранения.
Дата-центр может содержать несколько кластеров, которые в свою очередь могут содержать несколько узлов. Также он может иметь несколько доменов хранения, связанных с ним, и поддерживать несколько виртуальных машин на каждом из своих узлов. Среда KeyVirt позволяет содержать несколько дата-центров. Инфраструктура дата-центров позволяет разделить эти центры.
Все дата-центры управляются с Портала администратора (рисунок 50).

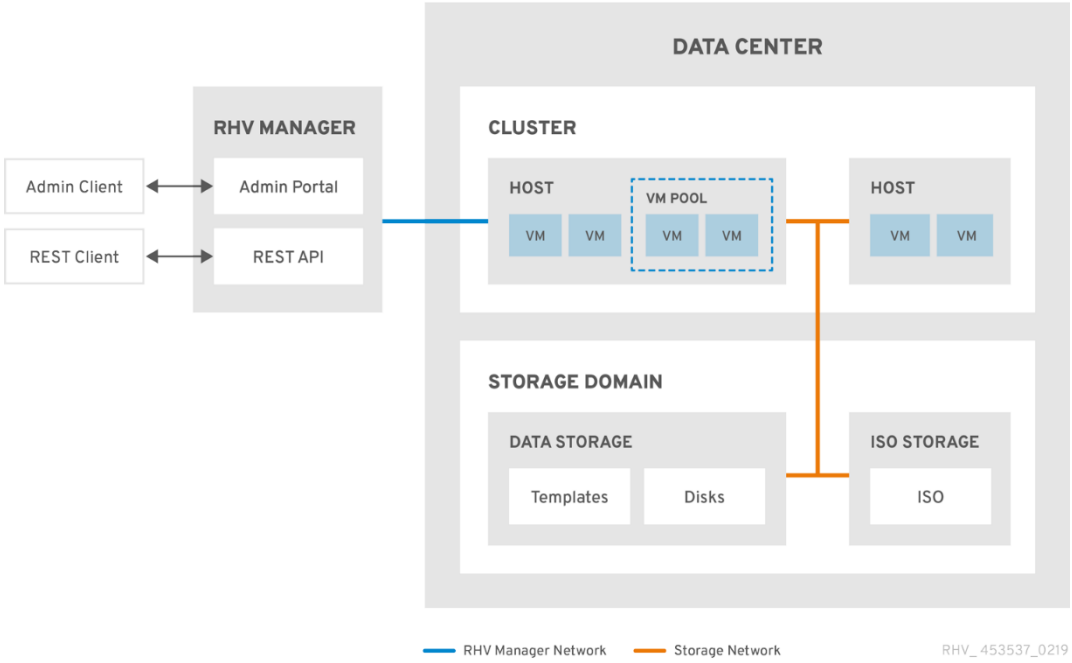


Рисунок 50. Дата-центр

Виртуализация создает дата-центр по умолчанию во время установки. Можно настроить дата-центр по умолчанию или создать новые дата-центры с соответствующими именами.

4.2.1.1 Менеджер пула хранения (SPM)

Менеджер пула хранения (SPM) – это роль, предоставленная одному из узлов в дата-центре, позволяющая ему управлять доменами хранения дата-центра. Сущность SPM может быть запущена на любом узле в дата-центре. Механизм KeyVirt предоставляет роль одному из узлов. SPM не исключает узла из его стандартной операции. узел, работающий как SPM, все еще может размещать виртуальные ресурсы.
SPM управляет доступом к хранилищу, координируя метаданные между доменами хранения. Это включает в себя создание, удаление и управление виртуальными дисками (образами), моментальными снимками и шаблонами, а также выделение хранилища для разреженных блочных устройств (в сети SAN). В дата-центре одновременно может быть только один узел SPM для обеспечения целостности метаданных.
KeyVirt Engine гарантирует, что SPM всегда доступен. Engine перемещает роль SPM на другой узел, если у узла SPM возникают проблемы с доступом к хранилищу. Когда SPM запускается, он гарантирует, что он является единственным узлом, которому предоставлена данная роль, поэтому он получит во временное пользование хранение. Этот процесс может занять некоторое время.

4.2.1.2 Приоритет SPM

Роль SPM использует часть доступных ресурсов узла. Настройка приоритета SPM узла изменяет вероятность того, какому узлу будет назначена роль SPM. Узлу с высоким приоритетом SPM будет назначена роль SPM. Критически важным виртуальным машинам на узлах с низким приоритетом SPM не придется конкурировать с операциями SPM за ресурсы узла. Вы можете изменить приоритет SPM узла на вкладке SPM в окне Edit host.

4.2.2 Задачи дата-центра

4.2.2.1 Создание нового дата-центра

Эта процедура создает дата-центр в вашей среде виртуализации.
Для работы дата-центра требуется функционирующий кластер, узел и домен хранения. Для создания нового дата-центра выполните следующие действия:

1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите кнопку *Новый*.
3. Введите *Имя* и *Описание* дата-центра.
4. В раскрывающемся меню выберите тип, версию совместимости и режим квоты дата-центра.
5. Нажмите кнопку OK, чтобы создать дата-центр и откройте *Дата Центр – Веди меня*.
6. В окне *Веди меня* перечислены объекты, которые необходимо настроить для дата-центра. Настройте эти объекты или отложите настройку, нажав кнопку *Настроить позже*. Конфигурацию можно возобновить, выбрав дата-центр и нажав (⋮) *Контекстное Меню* > *Веди меня*.

Новый дата-центр добавляется в среду виртуализации. Он будет оставаться в состоянии [*Неинициализированный*] до тех пор, пока для него не будут настроены кластер, узел и домен хранения. Используйте *Веди меня* для настройки этих объектов.

4.2.2.2 Описание параметров дата-центра

В таблице 18 описаны параметры дата-центра, отображаемые в окнах *Новый дата центр* и *Изменить дата центр*. Недопустимые записи выделяются оранжевым цветом при нажатии кнопки OK, запрещая принятие изменений. Кроме того, в приглашениях полей указываются ожидаемые значения или диапазон значений.
Таблица 18. Свойства дата-центра

Поле	Описание/Действие
Имя	Название дата-центра. Это текстовое поле имеет ограничение в 40 символов и должно быть уникальным именем с любой комбинацией прописных (A..Z) и строчных букв (a..z), цифр (0..9), дефисов (–) и символов подчеркивания (_).
Описание	Описание дата-центра. Данное поле рекомендуется, но не обязательно.
Тип хранилища	Тип хранилища. Выберите один из следующих вариантов: • *Общий*; • *Локальный*. Тип домена данных определяет тип дата-центра и не может быть изменен после создания без существенных сбоев. В один и тот же дата-центр можно добавить несколько типов доменов хранения (iSCSI, NFS, FC и POSIX), при этом локальные и общие домены нельзя смешивать.
Версия совместимости	Версия KeyVirt. После обновления KeyVirt Engine узлы, кластеры и дата-центры могут оставаться в более ранней версии. Перед обновлением версии совместимости дата-центра убедитесь, что вы обновили все узлы, а затем кластеры.
Режим квоты	Квота – это инструмент ограничения ресурсов, предоставляемый KeyVirt. Выберите один из следующих вариантов: • *Выключено*: Выберите, если вы не хотите реализовывать квоту; • *Аудит*: Выберите, если вы хотите изменить параметры квоты; • *Принудительно*: Выберите для реализации квоты.
Комментарий	При необходимости добавьте простой текстовый комментарий о дата-центре.

4.2.2.3 Повторная инициализация дата-центра: процедура восстановления

Процедура восстановления заменяет домен данных master вашего дата-центра новым доменом данных master; это необходимо в случае повреждения данных

вашего домена данных master. Повторная инициализация дата-центра позволяет восстановить все другие ресурсы, связанные с дата-центром, включая кластеры, узлы и проблемные домены хранения.
Вы можете импортировать любые резервные копии или экспортированные виртуальные машины или шаблоны в новый домен данных master.
Для повторной инициализации дата-центра выполните следующие действия:
1. Нажмите *Виртуализация* > *Дата Центры* и выберите *Дата Центр* для повторной инициализации.
2. Убедитесь, что все домены хранения, подключенные к дата-центру, находятся в режиме обслуживания.
3. Нажмите (⋮) *Контекстное Меню* > *Переинициализировать Дата Центр*.
4. В окне *Переинициализировать Дата Центр* перечислены все доступные (отсоединенные либо в режиме обслуживания) домены хранения. Нажмите на переключатель для домена хранения, добавляемого в дата-центр.
5. Установите флажок *Подтвердить операцию*.
6. Нажмите OK.

Домен хранения присоединяется к дата-центру в качестве домена данных master и активируется. Теперь можно импортировать все резервные копии или экспортированные виртуальные машины или шаблоны в новый домен данных master.

4.2.2.4 Удаление дата-центра

Для удаления дата-центра требуется активный узел. Удаление дата-центра не приведет к удалению связанных ресурсов.
Для удаления дата-центра выполните следующие действия:
1. Убедитесь, что домены хранения, подключенные к дата-центру, находятся в режиме обслуживания.
2. Нажмите *Виртуализация* > *Дата Центры* и выберите *Дата Центр* для удаления.
3. Нажмите кнопку *Удалить*.
4. Нажмите OK.

4.2.2.5 Принудительное удаление дата-центра

Дата-центр не отвечает на запросы, если присоединенный домен хранения поврежден или узел перестает реагировать. В таком случае вы не можете удалить дата-центр ни при каких обстоятельствах.
Процедура Force Remove не требует активного узла. Также безвозвратно удаляется присоединенный домен хранения. Перед принудительным удалением дата-центра может потребоваться уничтожить поврежденный домен хранения.
Для принудительного удаления дата-центра выполните следующие действия:
1. Нажмите *Виртуализация* > *Дата Центры* и выберите *Дата Центр* для удаления.
2. Нажмите (⋮) *Контекстное Меню* > *Удалить принудительно*.
3. Установите флажок *Подтвердить операцию*.
4. Нажмите OK.

Дата-центр и присоединенный домен хранения будут навсегда удалены из среды KeyVirt.

4.2.2.6 Изменение типа хранилища дата-центра

Тип хранилища дата-центра можно изменить после его инициализации. Это полезно для доменов данных, которые используются для перемещения виртуальных машин или шаблонов.

Ограничения:

- Из общего в локальный – для дата-центра, который не содержит более одного узла и более одного кластера, поскольку локальный дата-центр не поддерживает его.
- Из локального в общий – для дата-центра, который не содержит локального домена хранения.

Для изменения типа хранилища дата-центра выполните следующие действия:

1. Нажмите *Виртуализация* > *Дата Центры* и выберите *Дата Центр* для изменения.
2. Нажмите *Изменить*.
3. Измените тип хранилища на нужное значение.
4. Нажмите OK.

4.2.2.7 Изменение версии совместимости дата-центра

Дата-центры KeyVirt имеют версию совместимости. Версия совместимости указывает версию KeyVirt, с которой должен быть совместим дата-центр. Все кластеры в дата-центре должны поддерживать требуемый уровень совместимости.
Внимание! Чтобы изменить версию совместимости дата-центра, необходимо сначала обновить все кластеры в дата-центре до версии, соответствующей требуемой версии совместимости.
Для изменения версии совместимости дата-центра выполните следующие действия:

1. На Портале администратора нажмите *Виртуализация* > *Дата Центры*.
2. Из отображаемого списка выберите *Дата Центр*для изменения.
3. Нажмите кнопку *Изменить*.
4. Измените версию совместимости на требуемое значение.
5. Нажмите кнопку OK, чтобы открыть окно *Изменение версии совместимости дата-центра.*
6. Нажмите OK для подтверждения.

Вы обновили версию совместимости дата-центра.
Внимание! Обновление совместимости также приведет к обновлению всех доменов хранения, принадлежащих дата-центру.

4.2.3 Дата-центры и домены хранения

4.2.3.1 Присоединение существующего домена данных к дата-центру

Домены данных, которые не присоединены, могут быть присоединены к дата-центру. Общие домены хранения нескольких типов (iSCSI, NFS, FC и POSIX) могут быть добавлены в один и тот же дата-центр.
Для присоединения существующего домена данных к дата-центру выполните следующие действия:

1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на имя дата-центра, чтобы открыть подробное описание.
3. Перейдите на вкладку *Хранилище*, чтобы просмотреть список доменов хранения, уже подключенных к дата-центру.
4. Нажмите кнопку *Прикрепить данные*.
5. Установите флажок для домена данных, который будет присоединен к дата-центру. Можно установить несколько флажков для присоединения нескольких доменов данных.
6. Нажмите OK.

4.2.3.2 Присоединение существующего домена ISO к дата-центру

Непривязанный домен ISO может быть присоединен к дата-центру. Домен должен иметь тот же тип хранения, что и дата-центр. К дата-центру можно подключить только один домен ISO.
Для присоединения существующего домена ISO к дата-центру выполните следующие действия:

1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на имя дата-центра, чтобы открыть подробное описание.
3. Перейдите на вкладку *Хранилище*, чтобы просмотреть список доменов хранения, уже подключенных к дата-центру.
4. Нажмите на кнопку *Прикрепить ISO*.
5. Нажмите переключатель для соответствующего домена ISO.
6. Нажмите OK.

Домен ISO будет присоединен к дата-центру и автоматически активируется.

4.2.3.3 Присоединение существующего домена экспорта к дата-центру

Для присоединения существующего домена экспорта к дата-центру выполните следующие действия:

1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на имя дата-центра, чтобы открыть подробное описание.
3. Перейдите на вкладку *Хранилище*, чтобы просмотреть список доменов хранения, уже подключенных к дата-центру.
4. Нажмите кнопку *Подключить экспорт*.
5. Выберите необходимый домен экспорта.
6. Нажмите кнопку OK.

Домен экспорта будет присоединен к дата-центру и автоматически активируется.

4.2.3.4 Отсоединение домена хранения от дата-центра

Отсоединение домена хранения от дата-центра останавливает связь дата-центра с этим доменом. Домен хранения не удаляется из среды KeyVirt. Его можно подключить к другому дата-центру.
Данные, такие как виртуальные машины и шаблоны, остаются прикрепленными к домену хранения.
Примечание. Существует возможность отсоединения последнего главного домена хранения, однако делать это не рекомендуется.
Если главный домен хранения отсоединен, необходимо выполнить его повторную инициализацию.
Если домен хранения будет будет повторно инициализирован, все ваши данные будут потеряны, и домен хранения может не найти снова ваши диски.
Для отсоединения домена хранения от дата-центра выполните следующие действия:

1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на имя дата-центра, чтобы открыть подробное описание.
3. Перейдите на вкладку *Хранилище*, чтобы просмотреть список доменов хранения, уже подключенных к дата-центру.
4. Выберите домен хранения, который нужно отсоединить. Если домен хранения имеет статус *Активный*, нажмите *Перейти в режим Обслуживания.*
5. Нажмите OK для перехода в режим обслуживания.
6. Нажмите *Отсоединить*.

7. Нажмите OK.

Домен хранения будет отсоединен в течение нескольких минут.

4.3 КЛАСТЕРЫ

4.3.1 Общие сведения о кластерах

Кластер – это логическая группа узлов, которые совместно используют одни и те же домены хранения и имеют один и тот же тип процессора (Intel или AMD). Если узлы имеют разные поколения моделей ЦП, они используют только функции, присутствующие во всех моделях.

Каждый кластер в системе должен принадлежать дата-центру, и каждый узел в системе должен принадлежать кластеру. Виртуальные машины динамически выделяются любому узлу в кластере и могут быть перенесены между ними в соответствии с политиками, определенными в кластере, и параметрами виртуальных машин. Кластер – это самый высокий уровень, на котором можно определить политики распределения мощности и нагрузки.

Число узлов и число виртуальных машин, принадлежащих кластеру, отображаются в списке виртуальных машин в разделах *Счетчик узлов* и *Количество ВМ* соответственно.

Кластеры управляют виртуальными машинами или серверами хранения. Эти две задачи являются взаимоисключающими. Один кластер не может поддерживать виртуализацию и узлы хранения вместе.

KeyVirt создает кластер по умолчанию в дата-центре по умолчанию во время установки (рисунок 51).

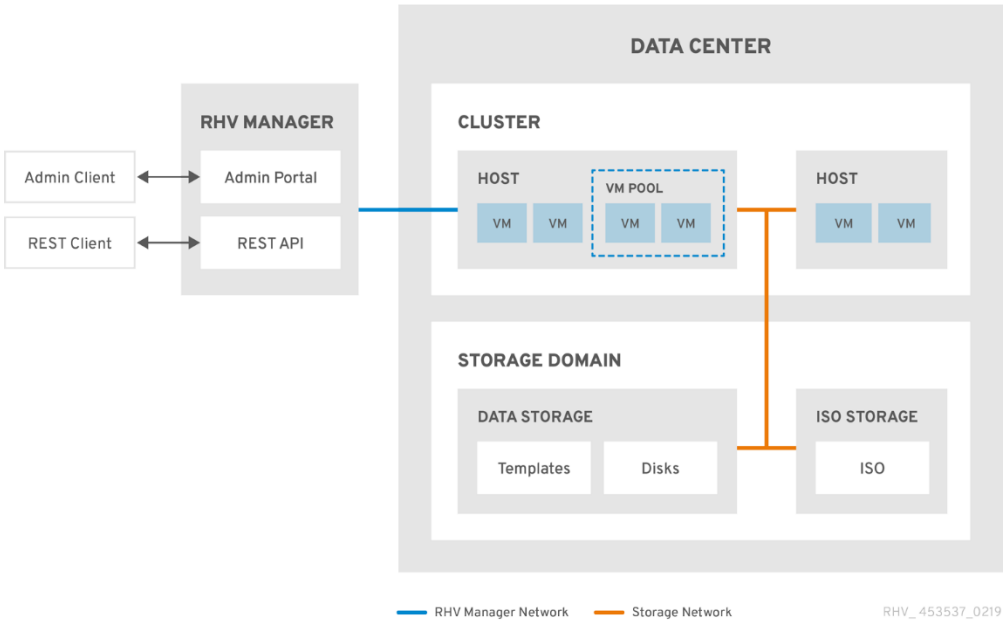


Рисунок 51. Кластер

4.3.2 Задачи кластера

4.3.2.1 Создание нового кластера

Дата-центр может содержать несколько кластеров, а кластер – несколько узлов. Все узлы в кластере должны иметь один и тот же тип процессора (Intel или AMD). Рекомендуется создать узлы перед созданием кластера, чтобы обеспечить

оптимизацию типа ЦП. Однако вы можете настроить узлы позже, используя кнопку *Веди меня*.

Для создания нового кластера выполните следующие действия:

1. Нажмите *Виртуализация* > *Кластеры*.
2. Нажмите кнопку *Новый*.
3. В раскрывающемся списке выберите *Дата Центр*, к которому будет принадлежать кластер.
4. Введите имя и описание кластера.
5. Выберите сеть из раскрывающегося списка *Сеть управления*, чтобы назначить роль сети управления.
6. Выберите *Архитектуру CPU*.
7. Для *Типа CPU* выберите самое старое семейство процессоров CPU среди узлов, которые будут входить в этот кластер. Типы процессоров перечислены в порядке от самых старых до самых новых.
8. Выберите *Режим FIPS* из списка для кластера.
9. В раскрывающемся списке выберите *Версию совместимости* для кластера.
10. Выберите *Типы свитчей* из раскрывающегося списка.
11. Выберите *Тип брандмауера* для узлов в кластере: iptables или firewalld.
12. Установите переключатель *Включить службу Virt*, чтобы определить, будет ли кластер заполнен узлами виртуальных машин.
13. При необходимости установите флажок *источник /dev/hwrng* (внешнее аппаратное устройство), чтобы указать устройство генератора случайных чисел, которое будут использовать все узлы кластера. Флажок *источник /dev/hwrng* (устройство, предоставляемое Linux) включен по умолчанию.
14. Перейдите на вкладку *Оптимизация*, чтобы выбрать пороговое значение общего доступа к страницам памяти для кластера, а также при необходимости включить обработку потоков ЦП и увеличить объем памяти на узлах кластера.
15. Перейдите на вкладку *Политика миграции*, чтобы определить политику миграции виртуальных машин для кластера.
16. Перейдите на вкладку *Политика планирования*, чтобы дополнительно настроить политику планирования, настроить параметры оптимизации планировщика, включить доверенную службу для узлов в кластере, включить резервирование HA и добавить пользовательскую политику серийных номеров.
17. Перейдите на вкладку *Консоль*, чтобы при необходимости переопределить глобальный прокси SPICE, если такой имеется, и укажите адрес прокси SPICE для узлов в кластере.
18. Перейдите на вкладку *Политика ограничения*, чтобы включить или отключить ограничения в кластере, и выберите параметры ограничений.
19. Перейдите на вкладку Пул MAK Адресов, чтобы указать пул MAC адресов.
20. Нажмите кнопку OK, чтобы создать кластер, и откройте окно *Кластер* > *Веди меня*.
21. В окне *Веди меня* перечислены объекты, которые необходимо настроить для кластера. Настройте эти объекты или отложите настройку, нажав кнопку *Настроить позже*; конфигурацию можно возобновить, выбрав кластер и нажав (⋮) *Контекстное Меню* > *Веди меня*.

4.4 ЛОГИЧЕСКАЯ СЕТЬ

4.4.1 Задачи логической сети

4.4.1.1 Выполнение сетевых задач

Сеть – предоставляет пользователям центральное расположение для выполнения операций, связанных с логической сетью, и поиска логических сетей на основе свойств каждой сети или связи с другими ресурсами. Кнопки *Новая*, *Изменить* и *Удалить* позволяют создавать, изменять свойства и удалять логические сети в дата-центрах. Нажмите по каждому имени сети и используйте вкладки подробного описания для выполнения следующих функций:

- присоединение или отсоединение сетей к кластерам и узлам;
- удаление сетевых интерфейсов из виртуальных машин и шаблонов;
- добавление и удаление разрешений для пользователей на доступ к сетям и управление ими. Эти функции также доступны через каждую отдельную вкладку ресурсов.

Предупреждение: не изменяйте сеть в дата-центре или кластере, если какие-либо узлы запущены, поскольку это рискует сделать узел недоступным.
Внимание! Если вы планируете использовать узлы для предоставления каких-либо служб, помните, что службы остановятся, если среда KeyVirt перестанет работать. Это относится ко всем службам, но вы должны быть особенно осведомлены об опасностях запуска следующих служб:

- Directory Services;
- DNS;
- Storage.

4.4.1.2 Создание новой логической сети в дата-центре или кластере

Создайте логическую сеть и определите ее назначение в дата-центре или в кластерах в дата-центре.
Для создания новой логической сети в дата-центре или кластере выполните следующие действия:

1. Нажмите *Виртуализация* > *Дата Центры* или *Виртуализация* > *Кластеры*.
2. Нажмите на имя дата-центра или кластера, чтобы открыть подробное описание.
3. Перейдите на вкладку *Логические сети*.
4. Откройте *Новая логическая сеть*:
   - Во вкладке *Дата Центры* нажмите кнопку *Новая*.
   - Во вкладке *Изменить* нажмите *Добавить сеть*.
5. Введите значения *Имя*, *Описание* и *Комментарий* для логической сети.
6. При необходимости включите *Включить тегирование VLAN*.
7. При необходимости отключите *Сеть ВМ*.
8. При необходимости установите флажок *Создать внешнего поставщика*. При этом отключится метка сети, сеть ВМ и MTU.
9. Выберите внешнего провайдера. Список не включает внешних провайдеров, которые находятся в режиме только для чтения.
   Примечание. Вы можете создать внутреннюю изолированную сеть, выбрав ovirt-provider-oven в списке *Внешний поставщик* и оставив параметр *Подключиться к физической сети* не выбранным.

10. Введите новую метку или выберите существующую метку для логической сети в текстовом поле *Метка сети*.
11. Установите значение MTU: *По умолчанию* (1500) или *Пользовательский*.
12. На вкладке *Кластеры* выберите кластеры, которым будет назначена сеть. Вы также можете указать, будет ли логическая сеть обязательной.
13. Если выбран параметр *Создать внешнего поставщика*, будет видна вкладка *Подсеть*. На вкладке Subnet выберите пункт Создать подсеть и введите имя, CIDR и адрес шлюза, а также выберите шерсию IP подсети, которую будет предоставлять логическая сеть. Вы также можете добавить DNS-серверы по мере необходимости.
14. На вкладке *Профили vNIC* добавьте профили vNIC в логическую сеть по мере необходимости.
15. Нажмите OK.

4.4.1.3 Редактирование логической сети

Логическую сеть нельзя отредактировать или переместить в другой интерфейс, если она не синхронизирована с конфигурацией сети на узле.
При изменении *Сеть ВМ* свойства существующей логической сети, используемой в качестве сети отображения, новые виртуальные машины не могут быть запущены на узле, на котором уже запущены виртуальные машины. Запускать новые виртуальные машины могут только узлы, на которых после изменения *Сеть ВМ* свойства не запущены виртуальные машины.
Для изменения логической сети выполните следующие действия:
1. Выберите *Виртуализация* > *Дата Центры*.
2. Нажмите на название дата-центра. Откроется окно сведений.
3. Перейдите на вкладку *Логические сети* и выберите логическую сеть.
4. Нажмите *Изменить*.
5. Отредактируйте необходимые настройки.
   Вы можете изменить название новой или существующей сети, за исключением сети по умолчанию, без необходимости останавливать виртуальные машины.
6. Нажмите OK.

Примечание. Конфигурация сети с несколькими узлами автоматически применяет обновленные параметры сети ко всем узлам в дата-центре, которому назначена сеть. Изменения могут применяться только в том случае, если виртуальные машины, использующие сеть, не работают. Нельзя переименовать логическую сеть, которая уже настроена на узле. Вы не можете отключить параметр сеть виртуальных машин во время работы виртуальных машин или шаблонов, использующих эту сеть.

4.4.1.4 Удаление логической сети

Логическую сеть можно удалить из меню *Сеть* > *Сети* или *Виртуализация* > *Дата Центры*. В следующей процедуре показано, как удалить логические сети, связанные с дата-центром. Для рабочей среды KeyVirt необходимо иметь по крайней мере одну логическую сеть, используемую в качестве сети управления ovirtmgmt.
Для удаления логической сети выполните следующие действия:
1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на имя дата-центра, чтобы открыть подробное описание.
3. Перейдите на вкладку *Логические сети*, чтобы просмотреть список логических сетей.

4. Выберите логическую сеть и нажмите кнопку *Удалить*.
5. При необходимости установите флажок *Удалить внешние сети от провайдера(ов)*, чтобы удалить логическую сеть как из диспетчера, так и из внешнего провайдера, если сеть предоставляется внешним провайдером. Флажок неактивен, если внешний провайдер находится в режиме только для чтения.
6. Нажмите OK.

Логическая сеть будет удалена из Engine и станет недоступна.

4.4.1.5 Настройка неуправляемой логической сети в качестве маршрута по умолчанию

Маршрут по умолчанию, используемый узлами в кластере, проходит через сеть управления (ovirtmgmt). Следующая процедура предоставляет инструкции для настройки неуправляемой логической сети в качестве маршрута по умолчанию. Необходимые условия:

- Если вы используете пользовательское свойство default_route, вам нужно очистить это свойство от всех вложенных узлов, а затем выполнить данную процедуру.

Для настройки роли маршрута по умолчанию выполните следующие действия:

1. Нажмите *Сеть* > *Сети*.
2. Нажмите на имя логической сети без управления, чтобы настроить ее в качестве маршрута по умолчанию.
3. Перейдите во вкладку *Кластеры*.
4. Нажмите *Управление сетью*.
5. Установите флажок *Маршрут по умолчанию* для соответствующих кластеров.
6. Нажмите OK.

Когда сети подключены к узлу, Маршрут по умолчанию будет задан в выбранной вами сети. Рекомендуется настроить роль маршрута по умолчанию до того, как любой узел будет добавлен в ваш кластер. Если в вашем кластере уже есть узлы, они могут не синхронизироваться до тех пор, пока вы не синхронизируете с ними изменения.

4.4.1.6 Просмотр или редактирование шлюза для логической сети

Пользователи могут определить шлюз, наряду с IP-адресом и маской подсети, для логической сети. Это необходимо, когда на узле существует несколько сетей и трафик должен маршрутизироваться через указанную сеть, а не через шлюз по умолчанию.
Если на узле существует несколько сетей и шлюзы не определены, обратный трафик будет маршрутизироваться через шлюз по умолчанию, который может не дойти до предполагаемого места назначения. Это приведет к тому, что пользователи не смогут пинговать узел.
KeyVirt автоматически обрабатывает несколько шлюзов всякий раз, когда интерфейс поднимается или опускается.
Для просмотра или изменения шлюза для логический сети выполните следующие действия:

1. Нажмите *Виртуализация* > *Узлы*.
2. Нажмите на имя узла, чтобы открыть подробное описание.
3. Перейдите на вкладку *Сетевые интерфейсы*, чтобы просмотреть все сетевые интерфейсы, подключенные к узлу, и их конфигурации.
4. Нажмите *Установка сетей узла*.

5. Наведите курсор на назначенную логическую сеть и нажмите на значок карандаша, чтобы открыть окно *Изменить сеть управления*.

В окне *Изменить сеть управления* отображается имя сети, протокол загрузки, IP-адрес, маска подсети и адреса шлюза. Информацию об адресе можно редактировать вручную, выбрав протокол статической загрузки.

4.4.1.7 Описание общих настроек логической сети

В таблице 19 описаны настройки для вкладки *Общее* в окнах *Новая логическая сеть* и *Изменить логическую сеть*.

Таблица 19. Описание настроек вкладки *Общее* логической сети

Имя поля	Описание
Имя	Имя логической сети. Это текстовое поле должно быть уникальным именем с любой комбинацией прописных (A..Z) и строчных (a..z) букв, цифр (0..9), дефисов (–) и подчеркиваний (_). Обратите внимание, что хотя имя логической сети может быть более 15 символов и содержать символы, отличные от ASCII, идентификатор на узле (vdsm_name) будет отличаться от указанного вами имени.
Описание	Описание логической сети. Это текстовое поле имеет ограничение в 40 символов.
Комментарий	Поле для добавления простого текста, удобочитаемых комментариев относительно логической сети.
Создать внешнего поставщика	Позволяет создать логическую сеть для экземпляра OpenStack Networking, который был добавлен в Manager в качестве внешнего провайдера. Внешний провайдер – позволяет выбрать внешнего провайдера, на котором будет создана логическая сеть.
Включить тегирование VLAN	Маркировка VLAN – это функция безопасности, которая придает всему сетевому трафику, передаваемому в логической сети, особую характеристику. Маркированный трафик VLAN не может быть прочитан интерфейсами, не имеющими этой характеристики. Использование VLAN в логических сетях также позволяет связать один сетевой интерфейс с несколькими логическими сетями с разными тегами VLAN. Введите числовое значение в текстовое поле ввода, если тегирование VLAN включено.
Сеть ВМ	Выберите данный вариант, если эту сеть используют только виртуальные машины. Если сеть используется для трафика, не связанного с виртуальными машинами, например для обмена данными с хранилищем, не устанавливайте этот флажок.
Изоляция порта	Если этот параметр установлен, виртуальные машины на одном узле не могут обмениваться данными и видеть друг друга в этой логической сети. Чтобы этот параметр работал на разных гипервизорах, коммутаторы должны быть настроены с изоляцией PVLAN/порта на соответствующем порту/VLAN, подключенном к гипервизорам, и не должны отражать кадры с какой-либо настройкой разворота пакетов.

MTU	Выберите вариант *По умолчанию*, который устанавливает максимальную единицу передачи (MTU) равной значению, указанному в скобках (), или *Пользовательский*, чтобы задать собственный MTU для логической сети. Вы можете использовать *Пользовательский*, чтобы сопоставить MTU, поддерживаемое вашей новой логической сетью, с MTU, поддерживаемым оборудованием, с которым оно взаимодействует. Введите числовое значение в текстовое поле ввода, если выбрано значение *Пользовательский*.
Метка сети	Позволяет указать новую метку для сети или выбрать из существующих меток, уже прикрепленных к сетевым интерфейсам узла. Если вы выберете существующую метку, логическая сеть будет автоматически назначена всем сетевым интерфейсам узла с этой меткой.
Группы безопасности	Позволяет назначать группы безопасности для портов в этой логической сети. *Отключено* отключает функцию группы безопасности. *Включено* включает эту функцию. Когда порт создается и подключается к этой сети, он будет определен с включенной защитой порта. Это означает, что доступ к виртуальным машинам и с них будет зависеть от групп безопасности, которые в настоящее время предоставляются. *Наследовать от конфигурации* позволяет портам наследовать поведение из файла конфигурации, определенного для всех сетей. По умолчанию файл отключает группы безопасности.

4.4.1.8 Описание настроек вкладки Кластер (Cluster) логической сети

В таблице 20 описаны настройки для вкладки *Кластер* окна *Новая логическая сеть*.

Таблица 20. Описание настроек вкладки *Кластер*

Имя поля	Описание
Подключить/отключить сеть к/от кластера(ам)	Позволяет вам присоединить или отсоединить логическую сеть от кластеров в центре данных и указать, будет ли логическая сеть необходимой для отдельных кластеров. • *Имя* – название кластера, к которому будут применяться настройки. Это значение не может быть отредактировано. • *Прикрепить все* – позволяет подключать или отключать логическую сеть ко всем кластерам в дата-центре или от них. В качестве альтернативы, установите или снимите флажок *Прикрепить* рядом с именем каждого кластера, чтобы присоединить или отсоединить логическую сеть к или от данного кластера. • *Обязательно все* – Позволяет указать, является ли логическая сеть требуемой на всех кластерах. В качестве альтернативы отметьте или снимите флажок *Обязательный* рядом с именем каждого кластера, чтобы указать, является ли логическая сеть требуемой для данного кластера.

4.4.1.9 Описание настроек вкладки vNIC Profiles логической сети

В таблице 21 описаны настройки для вкладки *Профили vNIC*окна *Новая логическая сеть*.

Таблица 21. Описание настроек вкладки *Профили vNIC*

Имя поля	Описание
Профили vNIC	Позволяет указать один или несколько vNIC-профилей для логической сети. Вы можете добавить или удалить vNIC-профиль в или из логической сети, нажав на кнопку плюс или минус рядом с vNIC-профилем. Первое поле предназначено для ввода имени vNIC-профиля. Public – Позволяет Вам указать, доступен ли профиль для всех пользователей. QoS – Позволяет указать профиль качества обслуживания сети (QoS) в профиле vNIC.

4.4.1.10 Назначение конкретного типа трафика для логической сети с помощью окна управления сетями

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

Для указания типа трафика для логической сети выполните следующие действия:

1. Нажмите *Виртуализация* > *Кластеры*.
2. Нажмите на имя кластера, чтобы открыть подробное описание.
3. Перейдите на вкладку *Логические сети*.
4. Нажмите *Управление сетями*.
5. Выберите необходимые настройки.
6. Нажмите OK.

Примечание. Логические сети, предлагаемые внешними провайдерами, должны использоваться в качестве сетей виртуальных машин; им нельзя назначать специальные кластерные роли, такие как отображение или миграция.

4.4.1.11 Описание настроек в окне управления сетями

В таблице 22 описаны настройки окна *Управление сетями*.

Таблица 22. Описание настроек вкладки *Управление сетями*

Имя поля	Описание
Связать	Назначает логическую сеть всем узлам в кластере.
Обязательный	Сеть с пометкой *Обязательный* должна оставаться работоспособной, чтобы связанные с ней узлы могли функционировать должным образом. Если требуемая сеть перестает функционировать, любые связанные с ней узлы становятся нерабочими.
Сеть ВМ	Логическая сеть с пометкой *Сеть ВМ* несет сетевой трафик, имеющий отношение к сети виртуальных машин.
Показать сеть	Логическая сеть с пометкой *Показать сеть* передает сетевой трафик, имеющий отношение к SPICE и виртуальному сетевому контроллеру.
Сеть миграции	Логическая сеть с пометкой *Сеть миграции* несет трафик миграции виртуальных машин и хранилищ. Если в этой сети произойдет сбой, вместо нее будет использоваться сеть управления (ovirtmgmt по умолчанию).

4.4.1.12 Настройка виртуальных функций на сетевой карте

Single Root I/O Virtualization (SR-IOV) позволяет использовать каждую конечную точку PCIe в качестве нескольких отдельных устройств с помощью физических функций (PF) и виртуальных функций (VF). Плата PCIe может иметь от одного до восьми PF. Каждый PF может иметь множество VF. Количество VF, которое он может иметь, зависит от конкретного типа устройства PCIe.
Для конфигурирования сетевых интерфейсных контроллеров (NIC), поддерживающих SR-IOV, используется Engine. В нем можно настроить количество виртуальных частот на каждой сетевой карте.
По умолчанию все виртуальные сети имеют доступ к виртуальным функциям. Вы можете отключить это значение по умолчанию и указать, какие сети имеют доступ к виртуальным функциям.
Для настройки виртуальных функций на сетевой карте выполните следующие действия:

1. Нажмите *Виртуализация* > *Узлы*.
2. Нажмите на имя узла с поддержкой SR-IOV, чтобы открыть подробное описание.
3. Перейдите во вкладку *Сетевые интерфейсы*.
4. Нажмите *Установка сетей узла*.
5. Выберите сетевой адаптер с поддержкой SR-IOV, помеченный значком (

) , и нажмите на значок карандаша.
6. При необходимости, чтобы изменить количество виртуальных функций, нажмите выпадающую кнопку *Количество настроек VF* и отредактируйте текстовое поле *Число VF*.

Примечание. Изменение количества VFs удаляет все предыдущие VFs на сетевом интерфейсе перед созданием новых VFs. Это включает в себя любые VF, у которых есть виртуальные машины, подключенные напрямую.

7. При необходимости, чтобы ограничить виртуальные сети, которые имеют доступ к виртуальным функциям, выберите *Конкретные сети*.
8. Нажмите OK.
9. В окне *Установка сетей узла* нажмите OK.

4.4.2 Виртуальные сетевые интерфейсные карты (vNICs)

Профиль виртуальной сетевой карты (vNIC) – это набор параметров, которые можно применить к отдельным виртуальным сетевым картам в Engine. Профиль vNIC позволяет применять профили сетевого QoS к vNIC, включать или отключать зеркалирование портов, добавлять или удалять пользовательские свойства. Профиль vNIC также предоставляет дополнительный уровень административной гибкости, поскольку разрешение на использование (потребление) этих профилей может быть предоставлено определенным пользователям. Таким образом, вы можете контролировать качество обслуживания, которое различные пользователи получают из данной сети.

4.4.2.1 Создание или изменение vNIC-профиля

Создайте или отредактируйте профиль виртуального контроллера сетевого интерфейса (vNIC) для регулирования пропускной способности сети для пользователей и групп.

Примечание. Если вы включаете или отключаете зеркалирование портов, все виртуальные машины, использующие соответствующий профиль, должны находиться в выключенном состоянии перед редактированием.
Создание или изменение а vNIC-профиля:

1. Нажмите *Сеть* > *Сети*.
2. Нажмите на имя логической сети, чтобы открыть подробное описание.
3. Перейдите на вкладку *Профили vNIC*.
4. Нажмите *Новый* или *Изменить*.
5. Введите имя и описание профиля.
6. Выберите соответствующую политику качества обслуживания из списка QoS.
7. Выберите фильтр сети из выпадающего списка для управления трафиком сетевых пакетов к виртуальным машинам и от них.
8. Установите флажок *Проброс устройств*, чтобы включить проброс устройств vNIC и разрешить прямое назначение устройства виртуальной функции. Включение свойства *Проброс устройств* отключит QoS, сетевую фильтрацию и зеркалирование портов, поскольку они несовместимы.
9. Если выбрана опция *Проброс устройств*, снимите флажок *Мигрируемый*, чтобы отключить миграцию для vNIC, использующих этот профиль.
10. Используйте флажки *Зеркалирование порта* и *Разрешить всем пользователям доступ к этому профилю* для переключения данных опций.
11. Выберите пользовательское свойство из списка пользовательских свойств, в котором по умолчанию отображается *Выберите ключ…*. Используйте кнопки «+» и «–» для добавления или удаления пользовательских свойств.
12. Нажмите OK.

Примените этот профиль к пользователям и группам, чтобы регулировать пропускную способность их сети. Если вы отредактировали профиль сетевой карты, необходимо либо перезапустить виртуальную машину, либо отключить, а затем подключить сетевую карту в горячем режиме, если гостевая операционная система поддерживает горячее подключение и горячее отключение сетевой карты.

4.4.2.2 Объяснение настроек в окне профиля интерфейса виртуальной машины

В таблице 23 подробно описаны настройки профиля интерфейса витруальной машины.
Таблица 23. Описание настроек профиля интерфейса виртуальной машины

Имя поля	Описание
Сеть	Выпадающий список доступных сетей, к которым нужно применить профиль vNIC.
Имя	Имя профиля vNIC. Это должно быть уникальное имя с любой комбинацией заглавных (A..Z) и строчных (a..z) букв, цифр (0..9), дефисов (–) и знаков подчеркивания (_) в пределах от 1 до 50 символов.
Описание	Описание профиля vNIC. Это поле является рекомендуемым, но не обязательным.
Косы (QoS)	Выпадающий список доступных политик качества обслуживания сети для применения к профилю vNIC. Политики QoS регулируют входящий и исходящий сетевой трафик vNIC.

Фильтр сети	Выпадающий список доступных сетевых фильтров для применения к профилю vNIC. Сетевые фильтры повышают безопасность сети, фильтруя типы пакетов, которые могут быть отправлены на виртуальные машины и с виртуальных машин. Фильтр по умолчанию – vdsm-no-mac-spoofing, который представляет собой комбинацию из no-mac-spoofing и noarp-mac-spoofing. Используйте для виртуальных сетей и связей виртуальных машин. На доверенных виртуальных машинах выбор неиспользования сетевого фильтра может повысить производительность.
Проброс устройств	Свойство *Проброс устройств* позволяет виртуальной сетевой карте напрямую подключаться к виртуальной функции сетевой карты узла. Свойство *Проброс устройств* нельзя редактировать, если профиль vNIC подключен к виртуальной машине. QoS, сетевые фильтры и зеркалирование портов отключены в профиле vNIC, если включен *Проброс устройств*.
Мигрируемый	Флажок, позволяющий установить, могут ли vNIC, использующие этот профиль, быть перемещены. Миграция включена по умолчанию для обычных профилей vNIC; флажок установлен и не может быть изменен. Когда установлен флажок *Проброс устройств*, параметр *Мигрируемый* становится доступным, и при необходимости его можно снять, чтобы отключить миграцию *Проброс устройств* vNIC.
Профиль vNIC для отработки отказа	Раскрывающееся меню для выбора доступных профилей vNIC, которые действуют как устройство аварийного переключения. Доступно, только если установлены флажки *Проброс устройств* и *Мигрируемый*.
Зеркалирование порта	Флажок для включения зеркалирования портов. Зеркалирование портов копирует сетевой трафик уровня 3 в логической сети на виртуальный интерфейс виртуальной машины. По умолчанию он не выбран.
Настраиваемые параметры	Выпадающее меню для выбора доступных пользовательских свойств для применения к профилю vNIC. Используйте кнопки «+» и «–» для добавления и удаления свойств соответственно.
Разрешить всем пользователям доступ к этому профилю	Флажок для переключения доступности профиля для всех пользователей в среде. По умолчанию он установлен.

4.4.2.3 Включение Проброса устройств (Passthrough) в vNIC-профиле

Свойство *Проброс устройств* профиля vNIC позволяет напрямую подключить vNIC к виртуальной функции (VF) сетевой карты с поддержкой SR-IOV. При этом vNIC будет обходить программную виртуализацию сети и подключаться непосредственно к VF для прямого назначения устройства.
Проброс устройств не может быть включен, если профиль vNIC уже подключен к vNIC; данная процедура создает новый профиль, чтобы избежать этого. Если

профиль vNIC имеет включенное свойство *Проброс устройств*, QoS, сетевые фильтры и зеркалирование портов не могут быть включены в том же профиле.
Для включения параметра *Проброс устройств* выполните следующие действия:

1. Нажмите *Сеть* > *Сети*.
2. Нажмите на имя логической сети, чтобы открыть подробное описание.
3. Перейдите на вкладку *Профили vNIC*, чтобы просмотреть все профили vNIC для данной логической сети.
4. Нажмите *Новый*.
5. Введите имя и описание профиля.
6. Установите флажок *Проброс устройств*.
7. По желанию снимите флажок *Мигрируемый*, чтобы отключить миграцию для vNIC, использующих этот профиль.
8. При необходимости выберите пользовательское свойство из списка пользовательских свойств, в котором по умолчанию отображается *Выберите ключ…*. Используйте кнопки «+» и «–» для добавления или удаления пользовательских свойств.
9. Нажмите OK.

Профиль vNIC теперь поддерживает проброс устройств. Чтобы использовать этот профиль для прямого подключения виртуальной машины к сетевой карте или PCI VF, подключите логическую сеть к сетевой карте и создайте новую PCI Passthrough vNIC на нужной виртуальной машине, которая использует профиль passthrough vNIC.

4.4.2.4 Удаление vNIC-профиля

Удалите профиль сетевой карты, чтобы удалить его из виртуализированной среды.
Для удаления vNIC-профиля выполните следующие действия:

1. Нажмите *Сеть* > *Сети*.
2. Нажмите на имя логической сети, чтобы открыть подробное описание.
3. Перейдите на вкладку vNIC-профили, чтобы просмотреть все профили vNIC для данной логической сети.
4. Выберите 1 или более профилей и нажмите *Удалить*.
5. Нажмите OK.

4.4.2.5 Назначение групп безопасности профилям vNIC

Эта функция доступна только при добавлении OpenStack Networking (neutron) в качестве провайдера внешней сети. Группы безопасности не могут быть созданы через Engine. Вы должны создавать группы безопасности через OpenStack.
Вы можете назначить группы безопасности профилю vNIC сетей, которые были импортированы из экземпляра OpenStack Networking и используют плагин Open vSwitch.
Группа безопасности – это набор строго соблюдаемых правил, которые позволяют фильтровать входящий и исходящий трафик через сетевой интерфейс. В следующей процедуре описано, как прикрепить группу безопасности к профилю vNIC. Группа безопасности идентифицируется с помощью ID этой группы безопасности, зарегистрированной в экземпляре OpenStack Networking. Вы можете найти идентификаторы групп безопасности для данного арендатора, выполнив следующую команду на системе, на которой установлена OpenStack Networking:
neutron security-group-list
Для назначения групп безопасности профилям vNIC выполните следующие действия:

1. Нажмите *Сеть* > *Сети*.
2. Нажмите на имя логической сети, чтобы открыть подробное описание.
3. Перейдите на вкладку *Профили vNIC*.
4. Нажмите *Новый*, или выберите существующий vNIC профиль и нажмите *Изменить*.
5. В раскрывающемся списке пользовательских свойств выберите SecurityGroups. Если оставить выпадающий список пользовательских свойств пустым, будут применены настройки безопасности по умолчанию, которые разрешают весь исходящий трафик и межсетевое взаимодействие, но запрещают весь входящий трафик за пределами группы безопасности по умолчанию. Обратите внимание, что последующее удаление свойства SecurityGroups не повлияет на примененную группу безопасности.
6. В текстовом поле введите идентификатор группы безопасности, которую нужно прикрепить к профилю vNIC.
7. Нажмите OK.

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

4.4.2.6 Разрешения пользователей для профилей vNIC

Настройте разрешения пользователей для назначения пользователей на определенные профили vNIC. Назначьте пользователю роль VnicProfileUser, чтобы он мог использовать профиль. Ограничьте доступ пользователей к определенным профилям, удалив их разрешение на этот профиль.
Разрешения пользователей для профилей vNIC:

1. Нажмите *Сеть* > *Профили vNIC*.
2. Нажмите на имя профиля vNIC, чтобы открыть подробное описание.
3. Перейдите на вкладку *Разрешения*, чтобы показать текущие разрешения пользователя для профиля.
4. Нажмите *Добавить* или *Удалить*, чтобы изменить разрешения пользователей для профиля vNIC.
5. В окне *Добавить разрешение пользователю* выбрит *Мои группы*, чтобы отобразить ваши группы пользователей. Вы можете использовать этот параметр для предоставления разрешений другим пользователям в ваших группах.

После этого разрешения пользователя для профиля vNIC будут настроены.

4.4.2.7 Настройка профилей vNIC для интеграции с UCS

Унифицированная вычислительная система Cisco (UCS) используется для управления такими аспектами дата-центра, как вычислительные, сетевые ресурсы и ресурсы хранения данных.
vdsm-hook-vmfex-dev позволяет виртуальным машинам подключаться к определенным UCS профилям портов Cisco путем настройки профиля vNIC. Профили портов, определяемые UCS, содержат свойства и параметры, используемые для настройки виртуальных интерфейсов в UCS. vdsm-hook-vmfex-dev установлен по умолчанию в VDSM.
При создании виртуальной машины, использующей профиль vNIC, она будет использовать сетевую карту Cisco vNIC.

Процедура настройки профиля vNIC для интеграции с UCS включает в себя настройку пользовательского свойства устройства. При настройке пользовательского свойства устройства все имеющиеся в нем значения перезаписываются. При комбинировании новых и существующих пользовательских свойств включайте все пользовательские свойства в команду, используемую для установки значения ключа. Несколько пользовательских свойств разделяются точкой с запятой.

Примечание. Профиль порта UCS должен быть настроен в Cisco UCS перед настройкой профиля vNIC.

Для настройки пользовательского свойства устройства выполните следующие действия:

1. В KeyVirt Engine настройте пользовательское свойство vmfex и установите уровень совместимости кластера с помощью –cver:
   engine-config -s CustomDeviceProperties='type=interface; prop=vmfex=^[a-zA-Z0-9_.-]2,32$' --cver=4.4
2. Убедитесь, что было добавлено свойство пользовательского устройства vmfex:
   engine-config -g CustomDeviceProperties
3. Перезапустите службу ovirt-engine:
   systemctl restart ovirt-engine.service

Конфигурируемый профиль vNIC может принадлежать новой или существующей логической сети.

Для настройки профиля сетевой карты vNIC для интеграции UCS выполните следующие действия:

1. Нажмите *Сеть* > *Сети*.
2. Нажмите на имя логической сети, чтобы открыть подробное описание.
3. Перейдите на вкладку *Профили vNIC*.
4. Нажмите *Новый* или *Изменить*.
5. Введите имя и описание профиля.
6. Выберите пользовательское свойство vmfex в списке пользовательских свойств и введите имя профиля порта UCS.
7. Нажмите OK.

4.5 УЗЛЫ

4.5.1 Общие сведения о узлах

Узлы (хосты виртуализации), также известные как гипервизоры, являются физическими серверами, на которых работают виртуальные машины. Полная виртуализация обеспечивается с помощью загружаемого модуля ядра Linux, называемого KVM (Kernel-based Virtual Machine).

KVM может одновременно размещать несколько виртуальных машин под управлением операционных систем Linux. Виртуальные машины запускаются как отдельные процессы и потоки Linux на главной машине и управляются удаленно механизмом KeyVirt. Среда KeyVirt имеет один или несколько узлов, подключенных к ней.

KeyVirt поддерживает два способа установки узлов. Можно использовать установочный носитель узла или установить пакеты гипервизора в стандартной установке ОС.

Внимание! Вы можете определить тип отдельного узла в KeyVirt, выбрав имя узла, чтобы открыть подробные сведения, и проверив описание ОС в разделе программное обеспечение.
Узлы используют настроенные профили, которые обеспечивают оптимизацию виртуализации.
Узел KeyVirt имеет включенные функции безопасности. Security Enhanced Linux (SELinux) и iptables firewall полностью настроены и включены по умолчанию.
Состояние SELinux на выбранном узле отображается в режиме SELinux на вкладке Общие панели сведений. Engine может открывать необходимые порты на узлах ОС, когда он добавляет их в среду.
Физический узел на платформе KeyVirt:

- должен принадлежать только одному кластеру в системе;
- должен иметь процессоры, поддерживающие расширения аппаратной виртуализации AMD-V или Intel VT;
- должен иметь процессор, который поддерживает все функциональные возможности, предоставляемые типом виртуального процессора, выбранным при создании кластера;
- имеет минимум 2 ГБ оперативной памяти;
- может иметь назначенного системного администратора с системными разрешениями.

Для узлов KeyVirt предусмотрены следующие максимальные ограничения:

- максимальный размер оперативной памяти: 12ТБ;
- максимальное количество логических ядер ЦП или потоков: 768;
- максимальное количество одновременных живых миграций: входящих – 2, исходящих – 2.
- пропускная способность динамической миграции: по умолчанию 52МБ на миграцию. При использовании других политик миграции будут использоваться адаптивные значения пропускной способности в зависимости от скорости физического устройства.

4.5.2 KeyVirt Node (узел KeyVirt)

Узел KeyVirt, он же KeyVirt Node, устанавливается с помощью специальной сборки Enterprise Linux, содержащей только пакеты, необходимые для размещения виртуальных машин. Он использует интерфейс установки Anaconda, основанный на использовании узлами Enterprise Linux, и может быть обновлен через KeyVirt Engine или через yum. Использование команды yum – единственный способ установить дополнительные пакеты и сохранить их после обновления.
Узел KeyVirt имеет пользовательский интерфейс Cockpit для мониторинга ресурсов узла и выполнения административных задач. Прямой доступ к узлу KeyVirt через SSH или консоль не поддерживается, поэтому пользовательский интерфейс Cockpit предоставляет графический пользовательский интерфейс для задач, выполняемых перед добавлением узла к Engine, таких как настройка сети и развертывание Self-Hosted Engine, а также может использоваться для запуска команд терминала через вкладку Терминал.
Доступ к пользовательскому интерфейсу предоставляется по адресу https://HostFQDNorIP:9090 в вашем веб-браузере. Cockpit для узла KeyVirt включает пользовательскую панель мониторинга виртуализации, которая отображает

состояние работоспособности узла, ключ узла SSH, состояние Self-Hosted Engine, виртуальные машины и статистику виртуальных машин.
Примечание. Пользовательские аргументы ядра загрузки могут быть добавлены в узел KeyVirt с помощью инструмента grubby. Инструмент grubby вносит постоянные изменения в файл grub.cfg. Перейдите на вкладку Терминал в пользовательском интерфейсе Cockpit узла, чтобы использовать команды grubby.
Предупреждение. Не создавайте ненадежных пользователей на узле, так как это может привести к использованию локальных уязвимостей безопасности.

4.5.3 Изменение настроек сети на узлах и Engine

При переносе системы виртуализации в другую сеть необходимо внести изменения в настройки сетевых интерфейсов узлов и Engine.

4.6 ХРАНИЛИЩЕ

KeyVirt использует централизованную систему хранения образов дисков виртуальных машин, ISO-файлов и моментальных снимков. Сеть хранения данных может быть реализована с помощью:

- сетевой файловой системы (NFS);
- других файловых систем, совместимых с POSIX;
- интерфейса малой компьютерной системы интернета (iSCSI);
- локального хранилища, подключенного непосредственно к узлам виртуализации;
- протокола оптоволоконного канала (FCP);
- параллельных NFS (pNFS).

Настройка хранилища является обязательным условием для нового дата-центра, поскольку дата-центр не может быть инициализирован, если домены хранения не подключены и не активированы.
Как системный администратор KeyVirt, вы должны создать, настроить, подключить и поддерживать хранилище для виртуализированного предприятия. Вы должны быть знакомы с типами хранилищ и их использованием.
Чтобы добавить домены хранения, у вас должен быть успешный доступ к Порталу администратора, и должен быть хотя бы один подключенный узел со статусом Up.
KeyVirt имеет три типа доменов хранения:

- Домен данных: домен данных содержит виртуальные жесткие диски и OVF-файлы всех виртуальных машин и шаблонов в дата-центре. Кроме того, моментальные снимки виртуальных машин также хранятся в домене данных. Домен данных не может быть общим для всех дата-центров. Домены данных нескольких типов (iSCSI, NFS, FC и POSIX) могут быть добавлены в один и тот же дата-центр при условии, что все они являются общими, а не локальными доменами. Домен данных необходимо присоединить к дата-центру, прежде чем к нему можно будет присоединить домены других типов.
- Домен ISO: домены ISO хранят файлы ISO (или логические компактдиски), используемые для установки и загрузки операционных систем и приложений для виртуальных машин. Домен ISO устраняет потребность дата-центра в физических носителях. Домен ISO может быть общим для различных дата-центров. Домены ISO могут быть основаны только на NFS. В дата-центр можно добавить только один домен ISO.

- Домен экспорта: домены экспорта – это временные хранилища данных, которые используются для копирования и перемещения образов виртуальных машин между дата-центрами и средами. Домены экспорта можно использовать для резервного копирования виртуальных машин. Домен экспорта можно перемещать между дата-центрами, однако одновременно он может быть активен только в одном дата-центре. Экспорт доменов может осуществляться только на основе NFS. В дата-центр можно добавить только один домен экспорта.

Примечание. Домен хранения экспорта устарел. Домены хранения данных можно отсоединить от дата-центра и импортировать в другой дата-центр в той же или в другой среде. Затем виртуальные машины, плавающие виртуальные диски и шаблоны могут быть загружены из импортированного домена хранения в подключенный дата-центр.

Внимание! Приступайте к настройке и подключению хранилища для среды KeyVirt только после определения потребностей в хранилище вашего дата-центра.

4.6.1 Общие сведения о доменах хранения

Домен хранения – это набор образов, имеющих общий интерфейс хранения. Домен хранения содержит полные образы шаблонов и виртуальных машин (включая моментальные снимки) или ISO-файлы. Домен хранения может состоять либо из блочных устройств (SAN-iSCSI или FCP), либо из файловой системы (NAS – NFS или других файловых систем, совместимых с POSIX).

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

В SAN (iSCSI/FCP) каждый виртуальный диск, шаблон или снимок является логическим томом. Блочные устройства объединяются в логическую сущность, называемую группой томов, а затем разделяются с помощью LVM (Logical Volume Manager) на логические тома для использования в качестве виртуальных жестких дисков.

Виртуальные диски могут иметь один из двух форматов: QCOW2 или RAW. Тип хранилища может быть либо разреженным, либо предварительно распределенным. Моментальные снимки всегда разрежены, но могут быть созданы для дисков любого формата.

Виртуальные машины с общим доменом хранения можно переносить между узлами, принадлежащими к одному кластеру.

4.6.2 Подготовка и добавление хранилища NFS

4.6.2.1 Подготовка хранилища NFS

Вы можете настроить общие ресурсы NFS в файловом хранилище или на удаленном сервере, которые будут служить доменом хранения данных на корпоративном сервере Linux. После экспорта общих ресурсов в удаленное хранилище и их настройки в системе управления они будут автоматически импортированы на узлы KeyVirt.

Чтобы Engine мог хранить данные в доменах хранения, представленных экспортируемыми каталогами, в них должны иметься определенные учетные записи системных пользователей и их группы. Следующая процедура устанавливает разрешения для одного каталога. Вам необходимо повторить шаги chown и chmod для всех каталогов, которые будут использоваться в качестве доменов хранения в KeyVirt.

Требования:

1. Установите пакет NFS utils:

```
# dnf install nfs-utils -y
```

2. Чтобы проверить включенные версии:

```
# cat /proc/fs/nfsd/versions
```

3. Включите следующие службы:

```
# systemctl enable nfs-server
# systemctl enable rpcbind
```

Процедура подготовки хранилища:

1. Создайте группу kvm:

```
# groupadd kvm -g 36
```

2. Создайте пользователя vdsm в группе kvm:

```
# useradd vdsm -u 36 -g kvm
```

3. Создайте каталог storage и измените права доступа:

```
# mkdir /storage
# chmod 0755 /storage
# chown 36:36 /storage/
```

4. Добавьте каталог storage в /etc/exports с соответствующими разрешениями:

```
# vi /etc/exports
# cat /etc/exports
 /storage *(rw)
```

5. Перезапустите следующие службы:

```
# systemctl restart rpcbind
# systemctl restart nfs-server
```

6. Чтобы увидеть, какой экспорт доступен для определенного IP-адреса:

```
# exportfs
 /nfs_server/srv
                10.46.11.3/24
 /nfs_server       <world>
```

Примечание. Если изменения /etc/exports были внесены после запуска служб, команду exportfs -ra можно использовать для перезагрузки изменений. После выполнения всех вышеперечисленных этапов каталог экспорта должен быть готов, и его можно протестировать на другом узле, чтобы убедиться, что его можно использовать.

4.6.2.2 Добавление хранилища NFS

Данная процедура предполагает, что вы уже экспортировали общие ресурсы. Перед созданием домена ISO и домена экспорта необходимо создать домен данных. Используйте эту же процедуру для создания домена ISO и домена экспорта, выбрав ISO или Export из списка функций домена:

1. На Портале администратора нажмите *Хранилище* > *Домены*.
2. Нажмите кнопку *Новый домен*.
3. Введите имя домена хранения.

4. Примите значения по умолчанию для списков *Дата Центр*, *Функция домена*, *Тип хранилища*, *Формат* и *Узел*.
5. Введите путь экспорта, который будет использоваться для домена хранения. Путь экспорта должен быть в формате 123.123.0.10:/data (для IPv4), [2001:0:0:0:0:0:0:5db1]:/data (для IPv6) или domain.example.com:/data.
6. При необходимости можно настроить дополнительные параметры:
   1) Нажмите *Дополнительные параметры*.
   2) Введите процентное значение в поле *Индикатор предупреждения о нехватке места*. Если свободное пространство, доступное в домене хранения, меньше этого процента, пользователю отображаются и регистрируются предупреждающие сообщения.
   3) Введите значение ГБ в поле *Действие блокировки при критическом значении свободного места.* Если свободное пространство, доступное в домене хранения, меньше этого значения, сообщения об ошибках отображаются пользователю и регистрируются в журнале. Любое новое действие, которое потребляет пространство, даже временно, будет заблокировано.
   4) Установите флажок в поле *Очистить после удаления* для включения опции очистки после удаления. Данный параметр можно изменить после создания домена, однако это не изменит свойство очистки после удаления для уже существующих дисков.
7. Нажмите OK.

Новый домен данных NFS отображается на вкладке *Хранилище* со статусом *Заблокирован* (Locked), пока диск не будет подготовлен. Домен данных затем будет автоматически присоединен к дата-центру.

4.6.2.3 Увеличение объема хранилища NFS

Чтобы увеличить объем хранилища NFS, можно либо создать новый домен хранения и добавить его в существующий дата-центр, либо увеличить доступное свободное пространство на сервере NFS. Первый вариант см. в разделе *Добавление хранилища NFS*.

Второй вариант описан в процедуре ниже. Данная процедура объясняет, как увеличить доступное свободное пространство на существующем сервере NFS.

Для увеличения существующего домена хранения NFS выполните следующие действия:

1. Нажмите *Хранилище* > *Домены*.
2. Нажмите на имя домена хранилища NFS, чтобы открыть подробное описание.
3. Перейдите на вкладку *Дата Центр* и нажмите *Перейти в режим Обслуживания*, чтобы перевести домен хранения в режим обслуживания. Данное действие размонтирует существующий общий ресурс и позволит изменить размер домена хранения.
4. На сервере NFS измените размер хранилища.
5. В области сведений перейдите на вкладку *Дата Центр* и нажмите кнопку Activate, чтобы подключить домен хранения.

4.6.3 Подготовка и добавление локального хранилища

Диск виртуальной машины, на котором используется устройство хранения, физически установленное на узле виртуальной машины, называется локальным устройством хранения.
Устройство хранения должно быть частью домена хранения. Тип домена хранения для локального хранилища называется локальным доменом хранения.
Настройка узла для использования локального хранилища автоматически создает и добавляет узел к новому домену локального хранилища, дата-центру и кластеру, к которым нельзя добавить никакой другой узел. Кластеры с несколькими узлами требуют, чтобы все узлы имели доступ ко всем доменам хранения, что невозможно с локальным хранилищем. Виртуальные машины, созданные в кластере с одним узлом, нельзя перенести, ограничить или запланировать.

4.6.3.1 Подготовка локального хранилища

На узле KeyVirt (KeyVirt Node) локальное хранилище всегда должно определяться в файловой системе, отдельной от **/** (root). Используйте отдельный логический том или диск, чтобы предотвратить возможную потерю данных во время обновлений.
Процедура для узлов Enterprise Linux:
1. На узле создайте каталог, который будет использоваться для локального хранилища:
   # mkdir -p /data/images
2. Убедитесь, что каталог имеет разрешения, разрешающие доступ на чтение / запись пользователю vdsm (UID 36) и группе kvm (GID 36):
   # chown 36:36 /data /data/images
   # chmod 0755 /data /data/images

Процедура для узлов KeyVirt:
Создайте локальное хранилище на логическом томе:
1. Создайте каталог локального хранилища:
   # mkdir /data
   # lvcreate -L $SIZE rhvh -n data
   # mkfs.ext4 /dev/mapper/rhvh-data
   # echo "/dev/mapper/rhvh-data /data ext4 defaults,discard 1 2" >> /etc/fstab
   # mount /data
2. Смонтируйте новое локальное хранилище:
   # mount -a
3. Убедитесь, что каталог имеет разрешения, разрешающие доступ на чтение / запись пользователю vdsm (UID 36) и группе kvm (GID 36):
   # chown 36:36 /data /rhvh-data
   # chmod 0755 /data /rhvh-data

4.6.3.2 Добавление локального домена хранения

При добавлении локального домена хранения к узлу настройка пути к каталогу локального хранилища автоматически создает и размещает узел в локальном дата-центре, локальном кластере и локальном домене хранения.
Процедура:
1. Нажмите *Виртуализация* > *Узлы* и выберите узел.
2. Нажмите *Управление* > *Перейти в режим Обслуживания* и OK. Статус узла меняется на обслуживание.

3. Нажмите *Управление* > *Настроить локальное хранилище*.
4. Нажмите кнопки *Изменить* рядом с полями *Дата центр*, *Кластер* и *Хранилище*, чтобы настроить и присвоить имя локальному домену хранения.
5. Укажите путь к вашему локальному хранилищу в поле ввода текста.
6. Если применимо, перейдите на вкладку *Оптимизация*, чтобы настроить политику оптимизации памяти для нового локального кластера хранения.
7. Нажмите OK.

Engine настраивает локальный дата-центр с локальным кластером, локальным доменом хранения. Это также изменяет статус узла на Up.
Верификация:

1. Выберите *Хранилище* > *Домены*.
2. Найдите домен локального хранилища, который вы только что добавили.

Статус домена должен быть *Активный*, а значение в столбце *Тип хранилища* должно быть *Локальный на хосте*.
Теперь вы можете загрузить образ диска в новый домен локального хранилища.

4.6.4 Подготовка и добавление POSIX-совместимого хранилища файловой системы

Поддержка файловой системы POSIX позволяет вам монтировать файловые системы, используя те же параметры монтирования, которые вы обычно используете при их монтировании вручную из командной строки. Эта функциональность предназначена для предоставления доступа к хранилищу, не представленному с помощью NFS, iSCSI или FCP.
Любая POSIX-совместимая файловая система, используемая в качестве домена хранения в KeyVirt, должна быть кластерной файловой системой, такой как Global File System 2 (GFS2), и должна поддерживать разреженные файлы и прямой ввод-вывод. Общая файловая система Интернета (CIFS), например, не поддерживает прямой ввод-вывод, что делает ее несовместимой с KeyVirt.
Внимание! Не монтируйте хранилище NFS, создавая домен хранилища файловой системы, совместимый с POSIX. Вместо этого всегда создавайте домен хранения NFS.

4.6.4.1 Добавление POSIX-совместимого хранилища файловой системы

В этой процедуре показано, как подключить существующее хранилище файловой системы, совместимое с POSIX, к вашей среде KeyVirt в качестве домена данных.
Процедура:

1. Нажмите *Хранилище* > *Домены*.
2. Нажмите *Новый домен*.
3. Введите имя домена хранения.
4. Выберите дата-центр, который будет связан с доменом хранения. Выбранный дата-центр должен относиться к типу POSIX (POSIX compliant FS). В качестве альтернативы выберите (none).
5. Выберите *Данные* из раскрывающегося списка *Функция домена*, а из раскрывающегося списка *Тип хранилища* выберите POSIX compliant FS.
   Если применимо, выберите *Формат* в раскрывающемся меню.
6. Выберите узел из раскрывающегося списка Host.
7. Введите путь к файловой системе POSIX, как вы обычно указываете его команде mount.

8. Введите тип VFS, как вы обычно указываете его команде mount с помощью аргумента -t. Список допустимых типов VFS вы можете посмотреть с помощью man mount.
9. Введите дополнительные параметры монтирования, как вы обычно указываете их команде mount с помощью аргумента -o. Параметры монтирования должны быть указаны в списке через запятую. Список допустимых параметров монтирования можно посмотреть с помощью man mount.
10. При желании вы можете настроить дополнительные параметры.
    1. Нажмите *Дополнительные параметры*.
    2. Введите процентное значение в поле *Индикатор предупреждения о малом количестве пространства*. Если свободное пространство, доступное в домене хранения, ниже этого процента, для пользователя отображаются и регистрируются предупреждающие сообщения.
    3. Введите значение ГБ в поле *Индикатор предупреждения о малом количестве пространства*. Если свободное пространство, доступное в домене хранения, ниже этого значения, сообщения об ошибках отображаются для пользователя и регистрируются в журнале, а любое новое действие, которое потребляет пространство, даже временно, будет заблокировано.
    4. Установите флажок *Очистить после удаления*, чтобы включить опцию очистки после удаления. Этот параметр можно изменить после создания домена, но это не изменит свойства очистки после удаления уже существующих дисков.
11. Нажмите OK.

4.6.5 Подготовка и добавление блочного хранилища

4.6.5.1 Подготовка хранилища iSCSI

KeyVirt поддерживает хранилище iSCSI, представляющее собой домен хранения, созданный из группы томов, состоящей из LUN. Группы томов и LUN не могут быть подключены более чем к одному домену хранения одновременно.
Если вы используете блочное хранилище и намереваетесь развернуть виртуальные машины на необработанных устройствах или direct LUN и управлять ими с помощью диспетчера логических томов (LVM), вам необходимо создать фильтр, чтобы скрыть гостевые логические тома. Это предотвратит активацию гостевых логических томов при загрузке узла, что может привести к устаревшим логическим томам и повреждению данных. Используйте команду vdsm-tool config-lvm-filter для создания фильтров для LVM.
Если ваш узел загружается из хранилища SAN и теряет подключение к хранилищу, файловые системы хранилища становятся доступными только для чтения и остаются в этом состоянии после восстановления подключения.
Чтобы предотвратить эту ситуацию, добавьте в корневую файловую систему SAN файл конфигурации с несколькими путями для загрузочного LUN, чтобы убедиться, что он ставится в очередь при наличии подключения:

```
# cat /etc/multipath/conf.d/host.conf
multipaths {
   multipath {
      wwid boot_LUN_wwid
      no_path_retry queue
   }
```

4.6.5.2 Добавление хранилища iSCSI

В этой процедуре показано, как подключить существующее хранилище iSCSI к вашей среде KeyVirt в качестве домена данных.
Процедура:

1. Нажмите *Хранилище* > *Домены*.
2. Нажмите *Новый домен*.
3. Введите имя нового домена хранения.
4. Выберите *Дата Центр* из выпадающего списка.
5. Выберите *Данные* в качестве *Функции домена* и iSCSI в качестве *Тип хранилища*.
6. Выберите необходимый активный узел.

Связь с доменом хранения осуществляется с выбранного узла, а не напрямую с Engine. Поэтому все узлы должны иметь доступ к устройству хранения, прежде чем можно будет настроить домен хранения.

7. Engine может сопоставлять цели iSCSI с LUN или LUN с целями iSCSI. В окне *Новый домен* автоматически отображаются известные цели с неиспользуемыми LUN, если выбран тип хранилища iSCSI. Если цель, которую вы используете для добавления хранилища, не отображается, вы можете использовать обнаружение цели, чтобы найти ее; в противном случае перейдите к следующему шагу.
8. Нажмите *Обнаружение целей*, чтобы включить параметры обнаружения целей. Когда цели обнаружены и зарегистрированы, в окне *Новый домен* автоматически отображаются цели с LUN, неиспользуемыми средой.

Также отображаются LUN, используемые для внешней среды.
Примечание. Вы можете использовать параметры *Обнаружение целей*, чтобы добавить LUN на несколько целей или несколько путей к одним и тем же LUN.
Если вы используете метод REST API discoveriscsi для обнаружения целей iscsi, вы можете использовать полное доменное имя или IP-адрес, но вы должны использовать сведения iscsi из результатов обнаруженных целей, чтобы войти в систему с помощью метода REST API iscsilogin.

1. Введите полное доменное имя или IP-адрес узла iSCSI в поле *Адрес*.
2. Введите порт для подключения к узлу при просмотре целей в поле *Порт*. Значение по умолчанию – 3260.
3. Если для защиты хранилища используется протокол CHAP, установите флажок *Аутентификация пользователей*. Введите значения для имя пользователя CHAP и CHAP.
   Вы можете определить учетные данные для цели iSCSI для определенного узла с помощью REST API.
4. Нажмите *Обнаружение*.
5. Выберите одну или несколько целей из результатов обнаружения и нажмите *Войти* для одной цели или *Войти в систему Везде* для нескольких целей.

Примечание. Если требуется доступ к нескольким путям, вы должны обнаружить и войти в цель по всем требуемым путям. Изменение домена хранения для добавления дополнительных путей в настоящее время не поддерживается.
При использовании метода REST API iscsilogin для входа в систему необходимо использовать сведения iscsi из результатов обнаруженных целей в discoveriscsi методе.

9. Нажмите кнопку + рядом с нужной целью. Это расширит запись и отобразит все неиспользуемые LUN, подключенные к цели.
10. Нажмите кнопку *Добавить* для каждого LUN, который вы используете для создания домена хранения.
11. При желании вы можете настроить дополнительные параметры:
    1. Нажмите *Дополнительные параметры*.
    2. Введите процентное значение в поле *Индикатор предупреждения о малом количестве пространства*. Если свободное пространство, доступное в домене хранения, ниже этого процента, для пользователя отображаются и регистрируются предупреждающие сообщения.
    3. Введите значение ГБ в поле *Действие блокировки при критическом значении свободного места*. Если свободное пространство, доступное в домене хранения, ниже этого значения, сообщения об ошибках отображаются для пользователя и регистрируются в журнале, а любое новое действие, которое потребляет пространство, даже временно, будет заблокировано.
    4. Установите флажок *Очистить после удаления*, чтобы включить опцию очистки после удаления. Этот параметр можно изменить после создания домена, но это не изменит свойства очистки после удаления уже существующих дисков.
    5. Установите флажок *Освободить после удаления* (Discard After Delete), чтобы включить параметр *Освободить после удаления*. Этот параметр можно изменить после создания домена. Этот параметр доступен только для блокировки доменов хранения.
12. Нажмите OK.

Если вы настроили несколько путей подключения хранилища к одному и тому же целевому объекту, выполните процедуру, описанную в разделе *Настройка многопутевого подключения iSCSI*, чтобы выполнить привязку iSCSI.

Если вы хотите перенести текущую сеть хранения на связь iSCSI, см. раздел *Миграция логической сети на связь iSCSI*.

4.6.5.3 Настройка многопутевого подключения iSCSI

Многопутевое подключение iSCSI позволяет создавать и управлять группами логических сетей и подключений к хранилищу iSCSI. Несколько сетевых путей между узлами и хранилищем iSCSI предотвращают простои узла, вызванные сбоем сетевого пути.

Механизм подключает каждый узел в дата-центре к каждой цели, используя сетевые карты или виртуальные локальные сети, назначенные логическим сетям в связке iSCSI.

Вы можете создать связь iSCSI с несколькими целями и логическими сетями для резервирования.

Требования:

- Одна или несколько целей iSCSI
- Одна или несколько логических сетей, отвечающих следующим требованиям:
- Не определено как обязательное или сеть виртуальных машин
- Назначен хост-интерфейсу
- Назначен статический IP-адрес в той же VLAN и подсети, что и другим логическим сетям в связке iSCSI.

Multipath не поддерживается для развертываний Self-Hosted Engine.

Процедура:

1. Нажмите *Виртуализация* > *Дата Центры*.
2. Нажмите на название дата-центра. Откроется представление сведений.
3. На вкладке *Множество путей iSCSI* нажмите Add.
4. В окне *Добавить iSCSI* Бонд введите имя и описание.
5. Выберите логическую сеть из *Логические сети* и домен хранения из *Цели хранилища.* Вы должны выбрать все пути к одной и той же цели.
6. Нажмите OK.

Хосты в дата-центре подключаются к целевым объектам iSCSI через логические сети в связке iSCSI.

4.6.5.4 Миграция логической сети на связку iSCSI

Если у вас есть логическая сеть, которую вы создали для трафика iSCSI и настроили поверх существующей сетевой связи, вы можете перенести ее на связь iSCSI в той же подсети без сбоев или простоев.

Процедура:

1. Измените текущую логическую сеть, чтобы она не была *Обязательной*:
    1. Нажмите *Виртуализация* > *Кластеры*.
    2. Нажмите на имя кластера. Откроется представление сведений.
    3. На вкладке *Логические сети* выберите текущую логическую сеть (net-1) и нажмите *Управление сетями*.
    4. Снимите флажок *Обязательный* и нажмите OK.
2. Создайте новую логическую сеть, которая не требуется и не является сетью виртуальных машин:
    1. Нажмите *Добавить сеть*. Откроется окно *Новая логическая сеть*.
    2. На вкладке *Общее* введите Name (net-2) и снимите флажок *Сеть ВМ*.
    3. На вкладке *Кластер* снимите флажок *Обязательный* и нажмите OK.
3. Удалите текущую сетевую связь и переназначьте логические сети:
    1. Нажмите *Виртуализация* > *Узлы*.
    2. Нажмите на имя узла. Откроется представление сведений.
    3. На вкладке *Сетевые интерфейсы* нажмите *Установка сетей узла*.
    4. Перетащите net-1 вправо, чтобы отменить его назначение.
    5. Перетащите текущую связь вправо, чтобы удалить ее.
    6. Перетащите net-1 и net-2 влево, чтобы назначить их физическим интерфейсам.
    7. Нажмите на значок карандаша net-2. Откроется окно редактирования сети .
    8. Во вкладке IPV4 выберите *Статический*.
    9. Введите IP- адрес и *Маска сети/префикс* подсети и нажмите OK.
4. Создайте связь iSCSI:
    1. Нажмите *Виртуализация* > *Дата Центры*
    2. Нажмите на название дата-центра. Откроется представление сведений.
    3. На вкладке *Множество путей iSCSI* нажмите *Добавить*.
    4. В окне *Добавить* iSCSI Bond введите *Имя*, выберите сети net-1 и net-2 и нажмите OK.

В вашем дата-центре есть соединение iSCSI, содержащее старую и новую логические сети.

4.6.5.5 Подготовка хранилища FCP

KeyVirt поддерживает хранилище SAN, создавая домен хранения из группы томов, состоящей из уже существующих LUN. Ни группы томов, ни LUN не могут быть присоединены более чем к одному домену хранения одновременно.
Системным администраторам KeyVirt необходимы практические знания концепций сетей хранения данных (SAN). SAN обычно использует протокол Fibre Channel (FCP) для трафика между узлами и общим внешним хранилищем. По этой причине SAN иногда может называться хранилищем FCP.
Внимание! Если вы используете блочное хранилище и намереваетесь развернуть виртуальные машины на необработанных устройствах или прямых LUN и управлять ими с помощью диспетчера логических томов (LVM), вам необходимо создать фильтр, чтобы скрыть гостевые логические тома. Это предотвратит активацию гостевых логических томов при загрузке узла, что может привести к устаревшим логическим томам и повреждению данных. Используйте команду vdsm-tool config-lvm-filter для создания фильтров для LVM.
Если ваш узел загружается из хранилища SAN и теряет подключение к хранилищу, файловые системы хранилища становятся доступными только для чтения и остаются в этом состоянии после восстановления подключения.
Чтобы предотвратить эту ситуацию, добавьте в корневую файловую систему SAN файл конфигурации с несколькими путями для загрузочного LUN, чтобы убедиться, что он ставится в очередь при наличии подключения:

```
# cat /etc/multipath/conf.d/host.conf
multipaths {
   multipath {
      wwid boot_LUN_wwid
      no_path_retry queue
   }
 }
```

4.6.5.6 Добавление хранилища FCP

В этой процедуре показано, как подключить существующее хранилище FCP к вашей среде KeyVirt в качестве домена данных.

1. Нажмите *Хранилище* > *Домены*.
2. Нажмите *Новый домен*.
3. Введите имя домена хранения.
4. Выберите дата-центр FCP из раскрывающегося списка.
5. Если у вас еще нет подходящего дата-центра FCP, выберите (none).
6. Выберите функцию домена и тип хранилища из раскрывающихся списков. Типы доменов хранения, несовместимые с выбранным дата-центром, недоступны.
7. Выберите активный узел в поле Host. Если это не первый домен данных в дата-центре, необходимо выбрать узел SPM дата-центра.

Внимание! Вся связь с доменом хранения осуществляется через выбранный узел, а не напрямую из Engine. В системе должен существовать хотя бы один активный узел, привязанный к выбранному дата-центру. Все узлы должны иметь доступ к устройству хранения, прежде чем можно будет настроить домен хранения.

8. В окне *Новый домен* автоматически отображаются известные цели с неиспользуемыми LUN, если в качестве типа хранилища выбран Fibre Channel. Установите флажок LUN ID, чтобы выбрать все доступные LUN.
9. При желании вы можете настроить дополнительные параметры.

1. Нажмите *Дополнительные параметры*.
2. Введите процентное значение в поле *Индикатор предупреждения о малом количестве пространства*. Если свободное пространство, доступное в домене хранения, ниже этого процента, для пользователя отображаются и регистрируются предупреждающие сообщения.
3. Введите значение ГБ в поле *Действие блокировки при критическом значении свободного места* . Если свободное пространство, доступное в домене хранения, ниже этого значения, сообщения об ошибках отображаются для пользователя и регистрируются в журнале, а любое новое действие, которое потребляет пространство, даже временно, будет заблокировано.
4. Установите флажок *Очистить после удаления*, чтобы включить опцию очистки после удаления. Этот параметр можно изменить после создания домена, но это не изменит свойства очистки после удаления уже существующих дисков.
5. Установите флажок *Освободить после удаления* (Discard After Delete), чтобы включить параметр *Освободить после удаления*. Этот параметр можно изменить после создания домена. Этот параметр доступен только для блокировки доменов хранения.

10. Нажмите OK.

4.6.5.7 Увеличение хранилища iSCSI или FCP

Существует несколько способов увеличить размер хранилища iSCSI или FCP:

- Добавить существующий LUN в текущий домен хранения.
- Создать новый домен хранения с новыми LUN и добавьте его в существующий дата-центр. См. *Добавление хранилища iSCSI*.
- Расширить домен хранения, изменив размер базовых LUN.

В следующей процедуре объясняется, как расширить хранилище сети хранения данных (SAN) путем добавления нового LUN в существующий домен хранения.

Требования:

- Статус домена хранения должен быть *Активный*.
- LUN должен быть доступен для всех узлов со статусом *Активный*, иначе операция завершится ошибкой и LUN не будет добавлен в домен. Однако сами узлы это не затронет. Если недавно добавленный узел или узел, выходящий из обслуживания или состояния *NonOperational*, не может получить доступ к LUN, состояние узла будет *NonOperational*.

4.6.5.8 Увеличение существующего домена хранения iSCSI или FCP

1. Нажмите *Хранилище* > *Домены* и выберите домен iSCSI или FCP.
2. Нажмите *Управление доменом*.
3. Нажмите *Цели* > *LUN'ы* и нажмите кнопку расширения *Обнаружение целей*.
4. Введите информацию о подключении к серверу хранения и нажмите *Обнаружение*, чтобы инициировать подключение.
5. Нажмите *LUN'ы* > *Цели* и установите флажок нового доступного LUN.
6. Нажмите OK, чтобы добавить LUN в выбранный домен хранения.

Это увеличит домен хранения на размер добавленного LUN.

При расширении домена хранения путем изменения размера базовых LUN эти LUN также необходимо обновить на Портале администратора.

4.6.5.9 Обновление размера LUN

1. Нажмите *Хранилище* > *Домены* и выберите домен iSCSI или FCP.
2. Нажмите *Управление доменом*.
3. Нажмите *LUN'ы* > *Цели*.
4. В столбце Additional Size нажмите кнопку Add Additional_Storage_Size для LUN для обновления.
5. Нажмите OK, чтобы обновить LUN и указать новый размер хранилища.

4.6.5.10 Повторное использование LUN

LUN нельзя повторно использовать как есть для создания домена хранения или виртуального диска. Если вы попытаетесь повторно использовать LUN, на Портале администратора появится следующее сообщение об ошибке:
Physical device initialization failed. Please check that the device is empty and accessible by the host.
Self-Hosted Engine показывает следующую ошибку во время установки:
[ERROR] Error creating Volume Group: Failed to initialize physical device: ("[u'/dev/mapper/000000000000000000000000000000000']",)
[ERROR] Failed to execute stage 'Misc configuration': Failed to initialize physical device: ("[u'/dev/mapper/000000000000000000000000000000000']",)
Перед повторным использованием LUN необходимо очистить старую таблицу разделов.
Внимание! Вы должны запустить следующую процедуру на правильном LUN, чтобы случайно не уничтожить данные:

1. Удалите сопоставления разделов в <LUN_ID> :

   kpartx -dv /dev/mapper/<LUN_ID>

2. Сотрите подписи файловой системы или рейда в <LUN_ID> :

   wipefs -a /dev/mapper/<LUN_ID>

3. Сообщите операционной системе об изменении таблицы разделов на <LUN_ID> :

   partprobe

4.6.5.11 Удаление устаревших LUN

При удалении домена хранения устаревшие ссылки LUN могут оставаться на сервере хранения. Это может привести к замедлению многопутевого сканирования, загромождению файлов журналов и конфликтам идентификаторов LUN.
KeyVirt не управляет серверами iSCSI и, следовательно, не может автоматически удалять LUN при удалении домена хранения. Администратор может вручную удалить устаревшие ссылки на LUN с ролью Ansible remove_stale_lun.yml. Эта роль удаляет устаревшие ссылки на LUN со всех узлов, принадлежащих данному дата-центру. Для получения дополнительной информации об этой роли и ее переменных см. Удаление роли Stale LUN в коллекции oVirt Ansible.
Предполагается, что вы управляете remove_stale_lun.yml на ВМ с Engine, так как ключ SSH Engine уже добавлен на все узлы. Если плейбук не запущен на машине с Engine, пользовательский SSH-ключ должен быть добавлен ко всем узлам, принадлежащим дата-центру, или пользователь должен предоставить соответствующий файл инвентаризации.
Процедура:
1. Нажмите *Хранилище* > *Домены*.

2. Нажмите на имя домена хранения. Откроется представление сведений.
3. Перейдите на вкладку *Дата Центр*.
4. Нажмите *Перейти в режим Обслуживания*, затем нажмите OK.
5. Нажмите *Отсоединить*, затем нажмите OK.
6. Нажмите *Удалить*.
7. Нажмите OK, чтобы удалить домен хранения из исходной среды.
8. Удалите LUN с сервера хранения.
9. Удалите устаревшие LUN с узла с помощью Ansible:
   # ansible-playbook --extra-vars "lun=<LUN>"
   /usr/share/ansible/collections/ansible_collections/ovirt/ovirt/roles/remove_stale_lun/examples/remove_stale_lun.yml

где LUN – это LUN, удаленный с сервера хранения на шагах выше.

Если удалить устаревший LUN с узла с помощью Ansible без предварительного удаления LUN с сервера хранения, устаревший LUN снова появится на узле при следующем повторном сканировании iSCSI VDSM.

4.6.5.12 Создание LVM-фильтра

Фильтр LVM – это опция, которую можно настроить /etc/lvm/lvm.conf для приема устройств в список томов или отклонения устройств из списка томов на основе запроса регулярного выражения. Например, для игнорирования /dev/cdrom можно использовать filter=["r|^/dev/cdrom$|"]или добавить в команду следующий параметр lvm: lvs --config 'devices{filter=["r|cdrom|"]}'.
Это простой способ запретить узлу сканировать и активировать логические тома, которые не требуются непосредственно этому узлу. В частности, решение предназначено для логических томов в общем хранилище, управляемом KeyVirt, и логических томов, созданных узлом в необработанных томах KeyVirt. Это решение необходимо, поскольку сканирование и активация других логических томов может привести к повреждению данных, медленной загрузке или другим проблемам.
Решение состоит в настройке фильтра LVM на каждом узле, что позволяет LVM на узле сканировать только те логические тома, которые требуются узлу.
Вы можете использовать эту команду vdsm-tool config-lvm-filter для анализа текущей конфигурации LVM и принятия решения о необходимости настройки фильтра.
Если фильтр LVM еще не настроен, команда создает параметр фильтра LVM для узла и добавляет этот параметр в конфигурацию LVM.

4.6.6 Импорт существующих доменов хранения

4.6.6.1 Общие сведения о доменах хранения

Помимо добавления новых доменов хранения, которые не содержат данных, вы можете импортировать существующие домены хранения и получать доступ к содержащимся в них данным. Импортируя домены хранения, вы можете восстановить данные в случае сбоя в базе данных Manager и перенести данные из одного дата-центра или среды в другой.
Ниже приведен обзор импорта каждого типа домена хранения:
Data
Импорт существующего домена хранилища данных позволяет получить доступ ко всем виртуальным машинам и шаблонам, содержащимся в домене хранилища данных. После импорта домена хранения необходимо вручную импортировать виртуальные машины, образы плавающих дисков и шаблоны в целевой дата-центр.
Процесс импорта виртуальных машин и шаблонов, содержащихся в домене

хранения данных, аналогичен процессу импорта домена хранения экспорта. Однако, поскольку домены хранения данных содержат все виртуальные машины и шаблоны в данном дата-центре, рекомендуется импортировать домены хранения данных для восстановления данных или крупномасштабной миграции виртуальных машин между дата-центрами или средами.

Примечание. Вы можете импортировать существующие домены хранения данных, которые были подключены к дата-центрам, с правильным поддерживаемым уровнем совместимости.

ISO

Импорт существующего домена хранения ISO позволяет получить доступ ко всем файлам ISO и виртуальным дискетам, содержащимся в домене хранения ISO. Никаких дополнительных действий после импорта домена хранения для доступа к этим ресурсам не требуется; вы можете подключить их к виртуальным машинам по мере необходимости.

Export

Импорт существующего домена хранения экспорта позволяет получить доступ ко всем образам и шаблонам виртуальных машин, содержащимся в домене хранения экспорта. Поскольку экспортные домены предназначены для экспорта и импорта образов и шаблонов виртуальных машин, импорт экспортных доменов хранения является рекомендуемым методом миграции небольшого количества виртуальных машин и шаблонов внутри среды или между средами. Сведения об экспорте и импорте виртуальных машин и шаблонов в экспортные домены хранения и из них см. в разделе *Экспорт и импорт виртуальных машин и шаблонов* в *Руководстве по эксплуатации KeyVirt для пользователя*.

При подключении домена хранения к целевому дата-центру он может быть обновлен до более нового формата домена хранения и не может повторно подключаться к исходному дата-центру. Это нарушает использование домена данных в качестве замены доменов экспорта.

4.6.6.2 Импорт доменов хранения

Импортируйте домен хранения, который ранее был подключен к дата-центру в той же среде или в другой среде. Эта процедура предполагает, что домен хранения больше не подключен к какому-либо дата-центру в любой среде, чтобы избежать повреждения данных. Чтобы импортировать и подключить существующий домен хранения данных к дата-центру, необходимо инициализировать целевой дата-центр.

Процедура:

1. Нажмите *Хранилище* > *Домены*
2. Нажмите *Импортировать домен*.
3. Выберите дата-центр, в который вы хотите импортировать домен хранения.
4. Введите имя домена хранения.
5. Выберите функцию домена и тип хранилища из раскрывающихся списков.
6. Выберите узел из раскрывающегося списка Host.

Вся связь с доменом хранения осуществляется через выбранный узел, а не напрямую из Engine. В системе должен существовать хотя бы один активный узел, привязанный к выбранному дата-центру. Все узлы должны иметь доступ к устройству хранения, прежде чем можно будет настроить домен хранения.

7. Введите сведения о домене хранения.

Поля для указания сведений о домене хранения меняются в зависимости от значений, выбранных вами в списках *Функция домена* и *Тип хранилища*. Эти поля аналогичны полям, доступным для добавления нового домена хранения.

8. Установите флажок *Включить домен в Дата Центре*, чтобы активировать домен хранения после его привязки к выбранному дата-центру.
9. Нажмите OK.

Теперь вы можете импортировать виртуальные машины и шаблоны из домена хранения в дата-центр.
При подключении домена хранения к целевому дата-центру он может быть обновлен до более нового формата домена хранения и не может повторно подключаться к исходному дата-центру. Это нарушает использование домена данных в качестве замены доменов экспорта.

4.6.6.3 Миграция доменов хранения между дата-центрами в одной среде

Перенесите домен хранения из одного дата-центра в другой в той же среде KeyVirt, чтобы предоставить целевому дата-центру доступ к данным, содержащимся в домене хранения. Эта процедура включает в себя отсоединение домена хранения от одного дата-центра и присоединение его к другому дата-центру.
Примечание. При переносе домена хранения данных в дата-центр с более высоким уровнем совместимости, чем исходный дата-центр, обновляется версия формата хранения домена хранения.
Если по какой-либо причине вы хотите переместить домен хранения обратно в исходный дата-центр, например, для переноса виртуальных машин в новый дата-центр, имейте в виду, что более поздняя версия не позволяет повторно подключить домен хранилища данных к исходному дата-центру.
Портал администратора предложит вам подтвердить, что вы хотите обновить формат домена хранения, например, с V3 до V5. Он также предупреждает, что вы не сможете подключить его обратно к более старому дата-центру с более низким уровнем DC.
Чтобы обойти эту проблему, вы можете создать целевой дата-центр с той же версией совместимости, что и исходный дата-центр. Если вам больше не нужно поддерживать более низкую версию совместимости, вы можете увеличить версию совместимости целевого дата-центра.
Процедура:

1. Выключите все виртуальные машины, работающие в требуемом домене хранения.
2. Нажмите *Хранилище* > *Домены*.
3. Нажмите на имя домена хранения. Откроется представление сведений.
4. Перейдите на вкладку *Дата Центр*.
5. Нажмите *Перейти в режим Обслуживания*, затем нажмите OK.
6. Нажмите *Отсоединить*, затем нажмите OK.
7. Нажмите *Прикрепить*.
8. Выберите целевой дата-центр и нажмите OK.

Домен хранилища присоединяется к целевому дата-центру и автоматически активируется. Теперь вы можете импортировать виртуальные машины и шаблоны из домена хранения в целевой дата-центр.

4.6.6.4 Миграция доменов хранения между дата-центрами в разных средах

Перенесите домен хранения из одной среды KeyVirt в другую, чтобы среда назначения могла получить доступ к данным, содержащимся в домене хранения. Эта

процедура включает удаление домена хранения из одной среды KeyVirt и его импорт в другую среду. Чтобы импортировать и подключить существующий домен хранения данных к дата-центру KeyVirt, исходный дата-центр домена хранения должен иметь правильный поддерживаемый уровень совместимости.
Процедура:
1. Войдите на Портал администратора исходной среды.
2. Выключите все виртуальные машины, работающие в требуемом домене хранения.
3. Нажмите *Хранилище* > *Домены*.
4. Нажмите на имя домена хранения. Откроется окно со сведениями.
5. Перейдите на вкладку *Дата Центр*.
6. Нажмите *Перейти в режим Обслуживания*, затем нажмите OK.
7. Нажмите *Отсоединить*, затем нажмите OK.
8. Нажмите *Удалить*.
9. В окне Удалить хранилище (хранилища) убедитесь, что флажок *Форматирование домена, т.е. содержимое хранилища будет потеряно!* не установлен. На этом шаге данные сохраняются в домене хранения для последующего использования.
10. Нажмите OK, чтобы удалить домен хранения из исходной среды.
11. Войдите на Портал администратора целевой среды.
12. Нажмите *Хранилище* > *Домены*.
13. Нажмите *Импортировать домен*.
14. Выберите целевой дата-центр из раскрывающегося списка *Дата Центр*.
15. Введите имя домена хранения.
16. Выберите функцию домена и тип хранилища из соответствующих раскрывающихся списков.
17. Выберите узел из раскрывающегося списка Host.
18. Введите сведения о домене хранения.

Поля для указания сведений о домене хранения меняются в зависимости от значения, выбранного в раскрывающемся списке *Тип хранилища*. Эти поля аналогичны полям, доступным для добавления нового домена хранения.
19. Установите флажок *Включить домен в Дата Центре*, чтобы автоматически активировать домен хранения при его подключении.
20. Нажмите OK.

Домен хранилища привязывается к целевому дата-центру в новой среде KeyVirt и автоматически активируется. Теперь вы можете импортировать виртуальные машины и шаблоны из импортированного домена хранения в целевой дата-центр. При подключении домена хранения к целевому дата-центру он может быть обновлен до более нового формата домена хранения и не может повторно подключаться к исходному дата-центру. Это нарушает использование домена данных в качестве замены доменов экспорта.

4.6.6.5 Импорт шаблонов из импортированных доменов хранения данных

Импортируйте шаблон из домена хранилища данных, который вы импортировали в свою среду KeyVirt. Эта процедура предполагает, что импортированный домен хранилища данных подключен к дата-центру и активирован.
Процедура:
1. Нажмите *Хранилище* > *Домены*.
2. Нажмите на имя импортированного домена хранения. Откроется окно со сведениями.

3. Перейдите на вкладку *Импорт Шаблона*.
4. Выберите один или несколько шаблонов для импорта.
5. Нажмите *Импортировать*.
6. Убедитесь, что для каждого шаблона в окне *Импорт Шаблона(ов)* в списке *Кластер* выбран правильный целевой кластер.
7. Сопоставьте профили vNIC внешней виртуальной машины с профилями, присутствующими в целевом кластере (кластерах):
    1. Нажмите vNic Profiles Mapping.
    2. Выберите профиль vNIC для использования в раскрывающемся списке *Целевой профиль vNIC*.
    3. Если в окне *Импорт Шаблона(ов)* выбрано несколько целевых кластеров, выберите каждый целевой кластер в раскрывающемся списке *Кластер назначения* и убедитесь, что сопоставления правильные.
    4. Нажмите OK.
8. Нажмите OK.

Импортированные шаблоны больше не отображаются в списке на вкладке *Импорт Шаблона*.

4.6.7 Задачи хранения

Требуется браузер с поддержкой HTML 5 – например, Firefox 35, Internet Explorer 10, Chrome 13 или более поздней версии.
Можно выполнять следующие задачи для домена хранения:

- Загрузка изображений в домен хранилища данных
- Загрузка файлов образов VirtIO в домен хранения
- Загрузка изображений в домен ISO
- Перевод доменов хранения в режим обслуживания
- Редактирование доменов хранения
- Обновление OVF
- Активация доменов хранения из режима обслуживания
- Отсоединение домена хранения от дата-центра
- Присоединение домена хранения к дата-центру
- Удаление домена хранения
- Безвозвратное удаление домена хранения
- Создание профиля диска
- Удаление профиля диска
- Просмотр состояния работоспособности домена хранения
- Настройка удаления после удаления для домена хранения
- Включение поддержки 4K в средах с более чем 250 узлами
- Мониторинг доступного пространства в домене хранения

4.7 ВИРТУАЛЬНЫЙ ДИСК

4.7.1 Общие сведения о хранилище виртуальных машин

KeyVirt поддерживает три типа хранения: NFS, iSCSI и FCP. В каждом типе имеется узел, известный как диспетчер пулов хранения (SPM), который управляет доступом между узлами и хранилищем. узел SPM – это единственный узел, который имеет

полный доступ в пуле хранения. SPM может изменять метаданные домена хранения и метаданные пула. Все остальные узлы могут получить доступ только к данным образа жесткого диска виртуальной машины.
По умолчанию в NFS, локальном или POSIX-совместимом дата-центре SPM создает виртуальный диск с использованием тонкого подготовленного формата в виде файла в файловой системе.
В iSCSI и других блочных дата-центрах SPM создает группу томов поверх предоставленных номеров логических блоков (LUN) и создает логические тома для использования в качестве виртуальных дисков. Виртуальные диски в блочном хранилище предварительно распределяются по умолчанию.
Если виртуальный диск предварительно выделен, создается логический том указанного размера в ГБ. Виртуальная машина может быть смонтирована на сервере Enterprise Linux с помощью kpartx, vgscan, vgchange или mount для изучения процессов или проблем виртуальной машины.
Если виртуальный диск недостаточно подготовлен, создается логический том объемом 1 ГБ. Логический том постоянно контролируется узлом, на котором запущена виртуальная машина. Как только использование приближается к пороговому значению, узел уведомляет SPM, и SPM расширяет логический том на 1 ГБ. узел отвечает за возобновление работы виртуальной машины после расширения логического тома. Если виртуальная машина переходит в состояние приостановки, это означает, что SPM не может продлить диск вовремя. Это происходит, если SPM слишком занят или если недостаточно места для хранения.
Виртуальный диск с предварительно выделенным форматом (RAW) имеет значительно более высокую скорость записи, чем виртуальный диск с форматом тонкой подготовки (QCOW2). Тонкая подготовка занимает значительно меньше времени для создания виртуального диска. Формат тонкого представления подходит для виртуальных машин, не требующих интенсивного ввода-вывода.
Предварительно выделенный формат рекомендуется для виртуальных машин с высокой скоростью записи ввода-вывода. Если виртуальная машина способна записывать более 1 ГБ каждые четыре секунды, по возможности используйте предварительно выделенные диски.

4.7.2 Общие сведения о виртуальных дисках

KeyVirt предлагает варианты хранения Preallocated (толстое резервирование) и Sparse (тонкое резервирование).

- **Preallocated**
  Предварительно выделенный виртуальный диск заранее выделяет все хранилища, необходимые для виртуальной машины. Например, предварительно выделенный логический том размером 20 ГБ, созданный для раздела данных виртуальной машины, будет занимать 20 ГБ дискового пространства сразу после создания.
- **Sparse**
  Разреженное распределение позволяет администратору определить общее хранилище, которое будет назначено виртуальной машине, но хранилище выделяется только по мере необходимости. Например, 20-гигабайтный логический том с тонким резервированием будет занимать 0 гигабайт дискового пространства при первом создании. При установке операционной системы он может занимать размер установленного файла, и будет продолжать расти по мере добавления данных максимум до 20 ГБ.

Идентификатор виртуального диска можно просмотреть в разделе *Хранилище* > *Диски*. Идентификатор используется для идентификации виртуального диска, так как имя устройства (например, /dev/vda0) может измениться, что приведет к повреждению диска. Вы также можете просмотреть идентификатор виртуального диска в /dev/disk/by-id.
Виртуальный размер диска (Virtual Size) можно просмотреть в разделе *Хранилище* > *Диски*, а на вкладке *Диски* – в подробном просмотре для доменов хранения, виртуальных машин и шаблонов. Виртуальный размер – это общий объем дискового пространства, который виртуальная машина может использовать. Это число, которое вы вводите в поле Размер (ГБ) при создании или редактировании виртуального диска.
Вы можете просмотреть фактический размер диска (Actual Size) на вкладке *Диски* в подробном описании для доменов и шаблонов хранилищ. Фактический размер – это объем дискового пространства, который был выделен виртуальной машине до сих пор. Предварительно выделенные диски показывают одинаковое значение для *Виртуального размера* и *Фактического разера*. Разделенные диски могут показывать разные значения в зависимости от того, сколько дискового пространства было выделено.
Возможные комбинации типов и форматов хранилищ описаны в таблице 24.
Таблица 24. Комбинации с разрешенным хранением

Место хранения	**Формат**	**Тип**	**Примечание**
NFS	Raw	Preallocated	Файл с исходным размером, равным объему памяти, определённому для виртуального диска, не имеет форматирования.
NFS	Raw	Sparse	Файл с исходным размером, близким к нулю, без форматирования.
NFS	QCOW2	Sparse	Файл с исходным размером, близким к нулю, и имеющим форматирование QCOW2. Последующие слои будут отформатированы QCOW2.
SAN	Raw	Preallocated	Блочное устройство с исходным размером, равным объему памяти, заданному для виртуального диска, не имеет форматирования.
SAN	QCOW2	Sparse	Блочное устройство с начальным размером, который намного меньше, чем размер, определенный для виртуального диска (в настоящее время 1 ГБ), имеет формат QCOW2, для которого пространство выделяется по мере необходимости (в настоящее время с шагом в 1 ГБ).

4.7.3 Настройки для очистки виртуальных дисков после удаления

Параметр wipe_after_delete, рассматриваемый на Портале администратора как флаг *Очистить после удаления*, заменит использованные данные нулями при удалении

виртуального диска. Если флаг установлен в значение false, что является значением по умолчанию, то при удалении диска эти блоки будут открыты для повторного использования, но данные не будут удалены. Следовательно, эти данные могут быть восстановлены, так как блоки не были возвращены к нулю.
Параметр wipe_after_delete работает только на хранилище блоков. На файловом хранилище, например, NFS, опция ничего не делает, потому что файловая система гарантирует отсутствие данных.
Включение параметра wipe_after_delete для виртуальных дисков более безопасно, и рекомендуется, если виртуальный диск содержит какие-либо конфиденциальные данные. Это более сложная операция, и пользователи могут столкнуться со снижением производительности и увеличением времени удаления.
Примечание. Функция очистки после удаления отличается от безопасного удаления и не может гарантировать, что данные будут удалены из хранилища, просто новые диски, созданные в том же хранилище, не будут раскрывать данные со старых дисков.
Флаг wipe_after_delete по умолчанию может быть изменен на true во время процесса установки или с помощью инструмента engine-config в Engine. Перезапустите службу ovirt-engine, чтобы изменение настроек вступило в силу.
Примечание. Изменение значения по умолчанию флага wipe_after_delete не повлияет на свойство *Очистить после удаления* уже существующих дисков.
Установка параметра SANWipeAfterDelete по умолчанию в значение true с помощью инструмента конфигурации Engine:

1. Запустите engine-config с параметром --set:
   # engine-config --set SANWipeAfterDelete=true
2. Перезапустите ovirt-engine, чтобы изменения вступили в силу:
   # systemctl restart ovirt-engine.service

Файл /var/log/vdsm/vdsm.log, расположенный на узле, можно проверить, чтобы убедиться, что виртуальный диск был успешно очищен и удален. При успешной очистке лог-файл будет содержать запись storage_domain_id/volume_id was zeroed and will be deleted. Например:
a9cb0625-d5dc-49ab-8ad1-72722e82b0bf/a49351a7-15d8-4932-8d67- 512a369f9d61 was zeroed and will be deleted
В случае неудачной очистки диска появится сообщение журнала вида zeroing storage_domain_id/volume_id failed. Zero and remove this volume manually. Например: finished with VG:a9cb0625-d5dc-49ab-8ad1-72722e82b0bf LVs: 'a49351a7-15d8-4932-8d67-512a369f9d61': ImgsPar(imgs=['11f8b3be-fa96-4f6a-bb83-14c9b12b6e0d'], parent='00000000-0000- 0000-0000-000000000000'), img: 11f8b3be-fa96-4f6a-bb83-14c9b12b6e0d
В случае неудачного удаления диска появится сообщение Remove failed for some of VG: storage_domain_id zeroed volumes: list_of_volume_ids.

4.7.4 Общие диски в KeyVirt

Некоторые приложения требуют совместного использования хранилища между серверами. KeyVirt позволяет вам пометить жесткие диски виртуальной машины как разделяемые (Shareable) и прикрепить эти диски к виртуальным машинам. Таким образом, один виртуальный диск может использоваться несколькими гостями кластера.
Общие диски нельзя использовать в любой ситуации. Для таких приложений, как кластерные серверы баз данных и другие высокодоступные службы, общие диски

подходят. Присоединение общего диска к нескольким гостям, которые не являются клиентами кластера, скорее всего, приведет к повреждению данных, поскольку их чтение и запись на диск не координируются.
Вы не можете сделать снимок общего диска. Виртуальные диски, на которых сделаны снимки, впоследствии не могут быть помечены как разделяемые.
Вы можете пометить диск, к которому предоставляется общий доступ, как при его создании, так и при последующем редактировании диска.

4.7.5 Диски только для чтения в KeyVirt

Некоторые приложения требуют от администраторов совместного использования данных с правами только на чтение. Это можно сделать при создании или редактировании диска, прикрепленного к виртуальной машине, через вкладку *Диски* в подробном описании виртуальной машины, установив флажок Read Only (только для чтения). Таким образом, один диск может быть прочитан несколькими гостями кластера, в то время как администратор сохраняет права на запись.
Вы не можете изменить статус диска, доступного только для чтения, во время работы виртуальной машины.
Примечание. Для установки журналируемой файловой системы требуется доступ для чтения и записи. Использование параметра Read Only не подходит для виртуальных дисков, содержащих такие файловые системы (например, EXT3 , EXT4 или XFS).

4.7.6 Задачи виртуального диска

4.7.6.1 Создание виртуального диска

Создание диска Image полностью управляется Engine. Для дисков Direct LUN требуются уже существующие цели, подготовленные извне.
Вы можете создать виртуальный диск, который будет подключен к определенной виртуальной машине.
Для создания виртуального диска, прикрепленного к виртуальной машине, выполните следующие действия:
1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите по имени виртуальной машины. Откроется подробное описание.
3. Перейдите на вкладку *Диски*.
4. Нажмите кнопку .
5. Нажмите на соответствующую кнопку, чтобы указать, каким будет виртуальный диск: *Образ* или *Прямой LUN*.
6. Выберите опции, необходимые для виртуального диска. Опции меняются в зависимости от выбранного типа диска.
7. Нажмите OK.

Через некоторое время новый диск появится в описании ВМ.
Вы также можете создать плавающий виртуальный диск, который не принадлежит ни одной виртуальной машине. Вы можете прикрепить этот диск к одной виртуальной машине или к нескольким виртуальным машинам, если диск является общим.
Для создания плавающего виртуального диска выполните следующие действия:
1. Нажмите *Хранилище* > *Диски*.
2. Нажмите *Новый*.

3. Нажмите на соответствующую кнопку, чтобы указать, будет ли виртуальный диск *Образ* или *Прямой LUN*.
4. Выберите опции, необходимые для виртуального диска. Опции меняются в зависимости от выбранного типа диска.
5. Нажмите OK.

4.7.6.2 Описание параметров виртуального диска

Поскольку окна создания нового виртуального диска для плавающих и прикрепленных виртуальных дисков очень похожи, их настройки описаны в одной таблице 25.

Таблица 25. Параметры *Новый виртуальный диск* и *Изменить виртуальный диск:* Образ

Имя поля	Описание
Размер (ГБ)	Размер нового виртуального диска в Гб.
Псевдоним	Имя виртуального диска, ограниченное 40 символами.
Описание	Описание виртуального диска. Это поле рекомендуется, но не является обязательным.
Интерфейс	Это поле появляется только при создании подключенного диска. Виртуальный интерфейс, который диск представляет виртуальным машинам. VirtIO быстрее, но требует драйверов. Windows не включает эти драйверы, но вы можете установить их с ISO-образа Virtio-win. Устройства IDE и SATA не требуют специальных драйверов.
Дата Центр	Это поле появляется только при создании плавающего диска. Дата-центр, в котором будет доступен виртуальный диск.
Домен хранения	Домен хранения, в котором будет храниться виртуальный диск. Выпадающий список показывает все домены хранения, доступные в данном дата-центре, а также общее пространство и текущее доступное пространство в домене хранения.
Политика выделения	Политика инициализации для нового виртуального диска. • *Предварительное выделение* выделяет весь размер диска в домене хранения на момент создания виртуального диска. Виртуальный размер и фактический размер предварительно выделенного диска одинаковы. Предопределенные виртуальные диски занимают больше времени на создание, чем виртуальные диски с тонким резервированием, но имеют лучшую производительность чтения и записи. Предопределенные виртуальные диски рекомендуются для серверов и других виртуальных машин с интенсивным вводом/выводом данных. Если виртуальная машина способна записывать более 1 ГБ каждые четыре секунды, используйте предустановленные диски там, где это возможно. • *Тонкое выделение* выделяет 1 ГБ в момент создания виртуального диска и устанавливает максимальный

	предел размера, до которого диск может вырасти. Виртуальный размер диска – это максимальный предел; реальный размер диска – это пространство, которое было выделено до сих пор. Тонкие диски с резервированием создаются быстрее, чем предварительно распределенные диски, и допускают избыточное резервирование хранилища. Для настольных компьютеров рекомендуется использовать виртуальные диски с тонким резервированием.
Профиль диска	Профиль диска, назначенный виртуальному диску. Профили диска определяют максимальный объем пропускной способности и максимальный уровень входных и выходных операций для виртуального диска в домене хранения данных. Профили дисков определяются на уровне домена хранилища исходя из качества хранения служебных записей, созданных для дата-центров.
Включение дисков	Это поле появляется только при создании подключенного диска. Активируйте виртуальный диск сразу после создания.
Очистить после удаления	Позволяет включить расширенную защиту для стирания конфиденциальных материалов при удалении виртуального диска.
Загрузочный	Это поле появляется только при создании подключенного диска. Позволяет включить загрузочный флаг на виртуальном диске.
Может быть общим	Позволяет подключать виртуальный диск к нескольким виртуальным машинам одновременно.
Только для чтения	Это поле появляется только при создании подключенного диска. Позволяет установить диск как доступный только для чтения. Один и тот же диск может быть вставлен как доступный только для чтения на одной виртуальной машине, так и перезаписываемый на другой.
Включить инкрементное резервное копирование	Включает добавочное резервное копирование на виртуальный диск. Инкрементное резервное копирование требует, чтобы диски были отформатированы в формате QCOW2, а не в формате RAW.
Принять изменения	Это поле появляется только при создании подключенного диска. Позволяет уменьшить тонкий диск с резервированием во время работы виртуальной машины. Для блочного хранилища базовое устройство хранения должно поддерживать вызовы диска, и опция не может быть использована с параметром *Очистить после удаления*, если только базовое хранилище не поддерживает свойство diskard_zeroes_data. Для файлового хранилища базовая файловая система и блочное устройство должны поддерживать discard-

	вызовы. Если все требования выполнены, команды SCSI UNMAP, изданные с гостевых виртуальных машин, передаются QEMU в базовое хранилище, чтобы освободить неиспользуемое пространство.

Настройки *Прямого LUN* могут отображаться в меню *Цели* > *LUN'ы* или *LUN'ы* > *Цели*. *Цели* > *LUN'ы* сортирует доступные LUN в соответствии с узлом, на котором они обнаружены, тогда как *LUN'ы* > *Цели* отображает единый список LUN.
Заполните поля в разделе *Обнаружение целей* и нажмите *Обнаружение*, чтобы обнаружить целевой сервер. Затем вы можете нажать кнопку Login All, чтобы составить список доступных LUN на целевом сервере, и, используя кнопки рядом с каждым LUN, выбрать нужные LUN для добавления.
Использование LUN непосредственно в качестве образов жесткого диска виртуальной машины устраняет уровень абстракции между виртуальными машинами и их данными.
При использовании *Прямого LUN* в качестве образа жесткого диска виртуальной машины необходимо учитывать следующие моменты:

- Миграция в реальном времени образов жесткого диска с *Прямого LUN* не поддерживается.
- Диски *Прямой LUN* не включаются в экспорт виртуальной машины.
- Диски *Прямой LUN* не включаются в снимки виртуальной машины.

Таблица 26. Параметры *Новый виртуальный диск* и *Изменить виртуальный диск*: Прямой LUN

Имя поля	Описание
Псевдоним	Имя виртуального диска, ограниченное 40 символами.
Описание	Описание виртуального диска. Это поле рекомендуется, но не является обязательным. По умолчанию в это поле вставляются последние 4 символа LUN ID. Поведение по умолчанию можно настроить, установив конфигурационный ключ PopulateDirectLUNDiskDescriptionWithLUNId в соответствующее значение с помощью команды engineconfig. Конфигурационный ключ может быть установлен в -1 – для использования полного идентификатора LUN, или в 0 – для игнорирования этой функции. Положительное целое число заполняет описание с соответствующим количеством символов LUN ID.
Интерфейс	Это поле появляется только при создании подключенного диска. Виртуальный интерфейс, который представляет диск виртуальным машинам. VirtIO быстрее, но требуются специальные драйверы. Windows не включает эти драйверы, но их можно установить с ISO. IDE- и SATA-устройства не требуют специальных драйверов. Тип интерфейса можно обновлять после остановки всех виртуальных машин, к которым подключен диск.
Дата Центр	Это поле появляется только при создании плавающего диска. Дата-центр, в котором будет доступен виртуальный диск.

Узел	Узел, на котором будет установлен LUN. Вы можете выбрать любой узел в дата-центре.
Тип хранилища	Тип внешнего LUN для добавления. Вы можете выбрать либо iSCSI, либо Fibre Channel.
Обнаружение целей	Этот раздел может быть расширен при использовании внешних LUN iSCSI, при этом выбраны Цели > Lun'ы. • *Адрес* – имя узла или IP-адрес целевого сервера. • *Порт* – порт, с помощью которого можно попытаться установить соединение с целевым сервером. Порт по умолчанию – 3260. • *Аутентификация пользователей:* – сервер iSCSI требует аутентификации пользователя. Поле User Authentication (Аутентификация пользователя) отображается, когда вы используете внешние LUN'ы iSCSI. • *Имя пользователя CHAP* – имя пользователя с разрешением на вход в LUNs. Это поле доступно, когда установлен флажок Аутентификация пользователя. • *Пароль* CHAP – пароль пользователя с разрешением на вход в LUN. Это поле доступно, если установлен флажок *Аутентификация пользователей*.
Включение дисков	Это поле появляется только при создании подключенного диска. Активируйте виртуальный диск сразу после создания.
Загрузочный	Это поле появляется только при создании подключенного диска. Позволяет включить загрузочный флаг на виртуальном диске.
Может быть общим	Позволяет подключать виртуальный диск к нескольким виртуальным машинам одновременно.
Только для чтения	Это поле появляется только при создании подключенного диска. Позволяет установить диск как доступный только для чтения. Один и тот же диск может быть вставлен как доступный только для чтения на одной виртуальной машине, так и перезаписываемый на другой.
Принять изменения	Это поле появляется только при создании подключенного диска. Позволяет уменьшить тонкий диск с резервированием во время работы виртуальной машины. При включенной опции команды SCSI UNMAP, выдаваемые гостевыми виртуальными машинами, передаются QEMU в основное хранилище, чтобы освободить неиспользуемое пространство.
Включить проброс SCSI	Это поле появляется только при создании подключенного диска. Доступно при установке интерфейса на VirtIO-SCSI. При установке данного флажка возможно подключение физического SCSI-

	устройства к виртуальному диску. Интерфейс VirtIOSCSI с включенной функцией просмотра SCSI автоматически включает поддержку SCSI-диска. *Только для чтения* не поддерживается, когда этот флажок установлен. Если этот флажок не установлен, виртуальный диск использует эмулируемое SCSI устройство. *Только для чтения* поддерживается на эмулированных дисках VirtIO-SCSI.
Разрешить привилегии ввода/вывода SCSI	Это поле появляется только при создании подключенного диска. Доступно, если установлен флажок *Включить проброс SCSI*. При установке этого флажка разрешается доступ к нефильтрованным SCSI Generic I/O (SG_IO), что позволяет использовать привилегированные команды SG_IO на диске. Это необходимо для постоянных резервирований.
Используется резервирование SCSI	Это поле появляется только при создании подключенного диска. Доступно, если установлены флажки *Включить проброс SCSI* и *Разрешить привилегии ввода/вывода SCSI*. Выбор этого флажка отключает миграцию для любой виртуальной машины, использующей этот диск, чтобы предотвратить потерю доступа к диску для виртуальных машин, использующих SCSI резервирование.

Примечание. Для монтирования журналируемой файловой системы требуется доступ для чтения и записи. Использование параметра *Только для чтения* не подходит для виртуальных дисков, содержащих такие файловые системы (например, EXT3 , EXT4 или XFS).

4.7.6.3 Обзор динамической миграции хранилища

Виртуальные диски можно переносить с одного домена хранения на другой во время работы виртуальной машины, к которой они подключены. Это называется динамической миграцией хранилища. Когда диск, подключенный к работающей виртуальной машине, перемещается, снимок цепочки образов этого диска создается в домене исходного хранилища, а вся цепочка образов реплицируется в домене целевого хранилища. Убедитесь, что у вас достаточно места как в домене исходного, так и в целевом домене хранения, чтобы разместить и цепь образов дисков, и снимок. Новый снимок создается при каждой попытке миграции живого хранилища, даже если миграция не удалась. При использовании миграции живого хранилища учитывайте следующее:

- Вы можете переносить несколько дисков в реальном времени одновременно.
- Несколько дисков для одной виртуальной машины могут находиться в нескольких доменах хранения, но цепочка образов для каждого диска должна находиться в одном домене хранения.
- Можно осуществлять прямой перенос дисков между любыми двумя доменами хранения в одном дата-центре.
- Нельзя переносить в реальном времени прямые образы жестких дисков LUN или дисков, помеченных как разделяемые.

4.7.6.4 Подключение существующего диска к виртуальной машине

Плавающие диски – это диски, не связанные ни с одной виртуальной машиной. Плавающие диски могут минимизировать время, необходимое для настройки виртуальных машин. Назначение плавающего диска хранилищем для виртуальной машины избавляет от необходимости ждать предварительного выделения диска во время создания виртуальной машины.
Плавающие диски можно подключить к одной виртуальной машине или к нескольким виртуальным машинам, если диск является общим. Каждая виртуальная машина, использующая общий диск, может использовать другой тип интерфейса диска. После подключения плавающего диска к виртуальной машине виртуальная машина может получить к нему доступ.
Для присоединения виртуальных дисков к виртуальным машинам выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку *Диски*.
4. Нажмите *Прикрепить*.
5. Выберите один или несколько виртуальных дисков из списка доступных дисков и выберите требуемый интерфейс из раскрывающегося списка *Интерфейс*.
6. Нажмите OK.

4.7.6.5 Перемещение виртуального диска

Виртуальные диски, подключенные к виртуальной машине или действующие как плавающий виртуальный диск, можно перемещать из одного домена хранения в другой. Вы можете переместить виртуальный диск, подключенный к работающей виртуальной машине; это называется переносом живого хранилища. В качестве альтернативы можно отключить виртуальную машину перед продолжением перемещения. При перемещении диска учитывайте следующее:

- Вы можете переместить несколько дисков одновременно.
- Можно перемещать диски между любыми двумя доменами хранения в одном дата-центре.
- Если виртуальный диск прикреплен к виртуальной машине, которая была создана на основе шаблона и использовала опцию выделения хранилища тонких ресурсов, необходимо скопировать диски для шаблона, на котором была основана виртуальная машина, в тот же домен хранения, что и виртуальный диск.

Для перемещения виртуального диска выполните следующие действия:

1. Нажмите кнопку *Хранилище* > *Диски* и выберите один или несколько виртуальных дисков для перемещения.
2. Нажмите *Копировать*.
3. В списке *Цель* выберите домен хранения, в который будут перемещены виртуальные диски.
4. В списке *Профиль диска* выберите профили диска, если применимо.
5. Нажмите OK.

Виртуальные диски перемещаются в целевой домен хранения. Во время процедуры перемещения в столбце *Состояние* отображается строка *Заблокировано* и индикатор выполнения операции перемещения.

4.7.6.6 Изменение типа интерфейса диска

Пользователи могут изменить тип интерфейса диска после его создания. Это позволяет прикрепить существующий диск к виртуальной машине, которая требует другого типа интерфейса. Например, диск, использующий интерфейс VirtIO, может быть прикреплен к виртуальной машине, требующей интерфейс VirtIO-SCSI или IDE. Это обеспечивает гибкость при переносе дисков с целью резервного копирования и восстановления или аварийного восстановления. Интерфейс диска для дисков с общим доступом также может быть обновлен для каждой виртуальной машины. Это означает, что каждая виртуальная машина, использующая общий диск, может использовать разные типы интерфейсов.
Чтобы обновить тип интерфейса диска, все виртуальные машины, использующие диск, должны быть сначала остановлены.
Для изменения типа дискового интерфейса выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и остановите соответствующую виртуальную машину (машины).
2. Нажмите по имени виртуальной машины. Откроется подробное описание.
3. Перейдите на вкладку *Диски* и выберите диск.
4. Нажмите *Изменить*.
5. В списке *Интерфейс* выберите новый тип интерфейса и нажмите OK.

Вы можете прикрепить диск к другой виртуальной машине, которая требует другого типа интерфейса.
Для присоединения диска к другой виртуальной машине с помощью другого типа интерфейса выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и остановите соответствующие виртуальные машины.
2. Нажмите по имени виртуальной машины. Откроется подробное описание.
3. Перейдите на вкладку *Диски* и выберите диск.
4. Нажмите *Удалить*, затем нажмите OK.
5. Вернитесь на вкладку *Виртуальные машины* и нажмите на имя новой виртуальной машины, к которой будет подключен диск.
6. Перейдите на вкладку *Диски* и нажмите *Прикрепить*.
7. Выберите диск в окне *Подключенние виртуальных дисков* и в раскрывающемся списке *Интерфейс* выберите соответствующий интерфейс.
8. Нажмите OK.

4.7.6.7 Копирование виртуального диска

Вы можете скопировать виртуальный диск из одного домена хранения в другой. Скопированный диск можно прикрепить к виртуальным машинам.
Для копирования виртуального диска выполните следующие действия:

1. Нажмите кнопку *Хранилище* > *Диски* и выберите один или несколько виртуальных дисков.
2. Нажмите *Копировать*.
3. Дополнительно введите новое имя в поле *Псевдоним*.
4. В списке *Цель* выберите домен хранения, в который будут скопированы виртуальные диски.
5. В списке *Профиль диска* выберите профили дисков, где применимо.
6. Нажмите OK.

Виртуальные диски имеют статус *Заблокирован* во время копирования.

4.7.6.8 Увеличение доступного размера виртуального диска

Вы можете увеличить доступный размер виртуального диска, пока виртуальный диск подключен к виртуальной машине. Изменение размера виртуального диска не приводит к изменению размера базовых разделов или файловых систем на этом виртуальном диске. Используйте утилиту fdisk для изменения размера разделов и файловых систем по мере необходимости.
Для увеличения доступного размера виртуальных дисков выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку *Диски* и выберите диск для редактирования.
4. Нажмите *Изменить*.
5. Введите значение в поле *Увеличить размер на (ГБ).*
6. Нажмите OK.

Состояние целевого диска на короткое время меняется на *Заблокирован*, в течение которого размер диска изменяется. Когда изменение размера диска завершено, состояние диска становится OK.

4.7.6.9 Подключение виртуального диска на горячую

Вы можете подключать виртуальные диски на горячую. Такое подключение означает включение или отключение устройств во время работы виртуальной машины.
Примечание. Гостевая операционная система должна поддерживать подключение виртуальных дисков на горячую.

Для подключения виртуальных дисков на горячую выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку *Диски* и выберите виртуальный диск для замены на горячую.
4. Нажмите (⋮) *Контекстное Меню*, затем нажмите *Выйти из режима обслуживания*, чтобы включить диск, или *Выключить*, чтобы отключить диск.
5. Нажмите OK.

4.7.6.10 Улучшение производительности диска

На Портале администратора в окне *Изменить виртуальную машину* на вкладке *Выделение ресурсов* виртуальной машины установлен флажок *Включены потоки ввода-вывода* по умолчанию, а количество потоков равно 1.
Предположим, виртуальная машина имеет несколько дисков с контроллерами VirtIO, и ее рабочие нагрузки в значительной степени используют эти контроллеры. В этом случае вы можете повысить производительность, увеличив количество потоков ввода-вывода.
Однако также учтите, что увеличение числа потоков ввода-вывода уменьшает пул потоков виртуальной машины. Если ваши рабочие нагрузки не используют контроллеры VirtIO и потоки, которые вы им выделяете, увеличение количества потоков ввода-вывода может снизить общую производительность.
Чтобы найти оптимальное количество потоков, сравните производительность вашей виртуальной машины с рабочими нагрузками до и после корректировки количества потоков.

Процедура:
1. Перейдите в *Виртуализация* > *Виртуальные машины* и выключите виртуальную машину.
2. Нажмите на имя виртуальной машины.
3. В области сведений перейдите на вкладку *Устройства ВМ*.
4. Подсчитайте количество контроллеров с типом virtio или virtio-scsi.
5. Нажмите *Изменить*.
6. В окне *Изменить виртуальную машину* перейдите на вкладку *Выделение ресурсов*.
7. Убедитесь, что установлен флажок *Включены потоки ввода-вывода* (то есть включен).
8. Справа от *Включены потоки ввода-вывода* увеличьте количество потоков, но не превышайте количество контроллеров, тип которых – virtio или virtio-scsi.
9. Нажмите OK.
10. В области сведений выберите вкладку *Диски*.
11. Для каждого диска используйте (⋮) *Контекстное Меню*, чтобы деактивировать и активировать диск. Это действие переназначает диски контроллерам.
12. Нажмите *Запустить*, чтобы запустить виртуальную машину.

Этапы проверки

- Чтобы увидеть, какие контроллеры имеют поток ввода-вывода, нажмите *Устройства ВМ* в области сведений и найдите ioThreadid= в столбце *Специальные параметры*.
- Чтобы увидеть сопоставление дисков с контроллерами, войдите на хост-компьютер и введите следующую команду:

```
# virsh -r dumpxml virtual_machine_name
```

Загрузка изображений в домен хранилища данных

Вы можете загружать образы виртуальных дисков и образы ISO в свой домен хранилища данных на Портале администратора или с помощью REST API. Дополнительные сведения см. в разделе *Загрузка изображений в домен хранилища данных*.

4.7.6.11 Импорт образа диска из импортированного домена хранения

Вы можете импортировать плавающие виртуальные диски из импортируемого домена хранения.

Примечание. В Engine можно импортировать только QEMU-совместимые диски.

Для импорта образа диска выполните следующие действия:
1. Нажмите *Хранилище* > *Домены*.
2. Нажмите на имя импортируемого домена хранения, чтобы открыть подробное описание.
3. Перейдите на вкладку *Импорт диска*.
4. Выберите один или несколько дисков и нажмите кнопку *Импорт*.
5. Выберите соответствующий *Профиль диска* для каждого диска.
6. Нажмите кнопку OK.

4.7.6.12 Импорт незарегистрированного образа диска из импортированного домена хранения

Вы можете импортировать плавающие виртуальные диски из домена хранения данных. Плавающие диски, созданные вне среды KeyVirt, не регистрируются в

Engine. Можно осуществить сканирование домена хранилища для выявления незарегистрированных плавающих дисков для импорта.
Примечание. Только QEMU-совместимые диски могут быть импортированы в Engine.
Для импорта образа диска выполните следующие действия:
1. Нажмите *Хранилище* > *Домены*.
2. Нажмите по имени домена хранения, чтобы открыть подробное описание.
3. Нажмите (⋮) *Контекстное Меню*, затем Нажмите *Сканировать диски*, чтобы механизм мог идентифицировать незарегистрированные диски.
4. Перейдите на вкладку *Импорт диска*.
5. Выберите один или несколько образов диска и нажмите кнопку *Импортировать*.
6. Выберите соответствующий *Профиль диска* для каждого диска.
7. Нажмите OK.

4.7.6.13 Импорт виртуального диска из службы образов OpenStack

Виртуальные диски, управляемые OpenStack Image Service, могут быть импортированы в Engine, если данный OpenStack Image Service был добавлен в Engine в качестве внешнего провайдера.
Для импорта таких виртуальных дисков выполните следующие действия:
1. Нажмите *Хранилище* > *Домены*.
2. Нажмите на имя домена службы OpenStack Image Service, чтобы открыть подробное описание.
3. Перейдите на вкладку Images и выберите образ.
4. Нажмите *Импортировать*.
5. Выберите дата-центр, в который будет импортирован образ.
6. В раскрывающемся списке *Доменное имя* выберите домен хранения, в котором будет храниться образ.
7. При необходимости выберите квоту, которая будет применяться к образу, в раскрывающемся списке *Квота*.
8. Нажмите кнопку OK.

4.7.6.14 Экспорт виртуального диска в службу образов OpenStack

Виртуальные диски могут быть экспортированы в службу OpenStack Image Service, которая была добавлена в Engine как внешний провайдер.
Примечание. Виртуальные диски можно экспортировать только в том случае, если они не имеют нескольких томов, не являются тонкими и не имеют снимков.
Процедура:
1. Нажмите *Хранилище* > *Диски* и выберите диски для экспорта.
2. Нажмите (⋮) *Контекстное Меню*, а затем *Экспортировать*.
3. В раскрывающемся списке *Доменное имя* выберите службу OpenStack Image Service, в которую будут экспортированы диски.
4. В раскрывающемся списке *Квота* выберите квоту для дисков, если необходимо применить квоту.
5. Нажмите OK.

4.7.6.15 Освобождение виртуального дискового пространства

Виртуальные диски, использующие тонкую инициализацию, не сжимаются автоматически после удаления файлов с них. Например, если фактический размер

диска составляет 100 ГБ и вы удаляете 50 ГБ файлов, то выделенный размер диска остается 100 ГБ, а оставшиеся 50 ГБ не возвращаются на узел, и поэтому не могут быть использованы другими виртуальными машинами. Это неиспользованное дисковое пространство может быть восстановлено узлом путем выполнения операции *Дефрагментация* на дисках виртуальной машины. При этом свободное место с образа диска передается узлу. Вы можете разрежать (спарсифицировать) несколько виртуальных дисков параллельно.
Выполните эту операцию перед клонированием виртуальной машины, созданием шаблона на основе виртуальной машины или очисткой дискового пространства хранилища.
Ограничения:

- Домены хранения NFS должны использовать NFS версии 4.2 или выше.
- Нельзя освобождать пространство диска, использующего *Прямой LUN* (Управляемый блок).
- Нельзя освобождать пространство диска, использующего предварительную политику распределения. Если вы создаете виртуальную машину из шаблона, вы должны выбрать Thin (Тонкий) в поле Storage Allocation (Выделение хранилища), или, если вы выбрали Clone (Клонирование), убедитесь, что шаблон основан на виртуальной машине с тонкой настройкой.
- Вы можете разрежать только активные снимки.

Для освобождения дискового пространства выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выключите нужную виртуальную машину.
2. Нажмите по имени виртуальной машины, чтобы открыть подробное описание.
3. Перейдите на вкладку *Диски*. Убедитесь, что состояние диска соответствует значению OK.
4. Нажмите (⋮) *Контекстное Меню*, затем нажмите *Дефрагментация*.
5. Нажмите OK.

4.7.6.16 Удаление виртуального диска с виртуальной машины

Для удаления виртуальных дисков с виртуальных машин выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку *Диски* и выберите виртуальный диск, который нужно удалить.
4. Нажмите (⋮) *Контекстное Меню*, затем нажмите *Выключить*.
5. Нажмите OK.
6. Нажмите *Удалить*.
7. При необходимости установите флажок *Удалить окончательно*, чтобы полностью удалить виртуальный диск из среды. Если вы не выберете этот параметр, например, потому что диск является общим, виртуальный диск останется в *Хранилище* > *Диски*.
8. Нажмите OK.

Если диск был создан как блочное хранилище, например iSCSI, и при создании диска был установлен флажок *Очистить после удаления*, вы можете просмотреть

файл журнала на узле, чтобы убедиться, что данные были удалены после полного удаления диска.
Если диск был создан как блочное хранилище, например iSCSI, и флажок *Освободить после удаления* был установлен в домене хранилища до того, как диск был удален, на логическом томе вызывается команда blkdiscard, и базовое хранилище уведомляется. что блоки свободны. Blkdiscard также вызывается на логическом томе при удалении виртуального диска, если виртуальный диск подключен хотя бы к одной виртуальной машине с установленным флажком Enable Discard.

4.8 ВНЕШНИЕ ПРОВАЙДЕРЫ

4.8.1 Общие сведения о внешних провайдерах

В дополнение к ресурсам, управляемым самим Engine, KeyVirt также может использовать ресурсы, управляемые внешними источниками. Провайдеры этих ресурсов, известные как внешние провайдеры, могут предоставлять такие ресурсы, как узлы виртуализации, образы виртуальных машин и сети.

В настоящее время KeyVirt поддерживает следующих внешних провайдеров:

KubeVirt/Openshift Virtualization

Openshift Virtualization (ранее называвшаяся контейнерной виртуализацией или CNV) позволяет включать виртуальные машины (ВМ) в контейнерные рабочие процессы, чтобы вы могли разрабатывать, управлять и развертывать виртуальные машины параллельно с контейнерами и без сервера. В KeyVirt Engine добавление этого провайдера является одним из требований для использования виртуализации Openshift.

Служба образов OpenStack (Glance) для управления образами

Служба образов OpenStack предоставляет каталог образов виртуальных машин. В KeyVirt эти образы можно импортировать в KeyVirt Engine и использовать в качестве плавающих дисков или прикреплять к виртуальным машинам и преобразовывать в шаблоны. После того, как вы добавите службу образов OpenStack в Engine, она появится как домен хранения, не привязанный ни к какому дата-центру. Виртуальные диски в среде KeyVirt также можно экспортировать в службу образов OpenStack как виртуальные диски.

Примечание. Поддержка OpenStack Glance больше не рекомендуется. Эта функция будет удалена в более позднем выпуске.

VMware для подготовки виртуальных машин

Виртуальные машины, созданные в VMware, можно преобразовать с помощью V2V (virt-v2v) и импортировать в среду KeyVirt. После добавления провайдера VMware в Engine вы можете импортировать виртуальные машины, которые он предоставляет. Преобразование V2V выполняется на назначенном прокси-сервере как часть операции импорта.

Открытая виртуальная сеть (OVN) для подготовки сети

Open Virtual Network (OVN) – это расширение Open vSwitch (OVS), предоставляющее программно определяемые сети. После добавления OVN в Engine вы можете импортировать существующие сети OVN и создавать новые сети OVN из Engine. Вы также можете автоматически установить OVN на Engine, используя файлы engine-setup.

4.8.2 Добавление внешнего провайдера

4.8.2.1 Добавление узла KVM в качестве провайдера виртуальных машин

Процедура:

1. Включите аутентификацию по открытому ключу между прокси-узлом и узлом KVM:
   1. Войдите на прокси-сервер и сгенерируйте SSH-ключи для пользователя vdsm:
      # sudo -u vdsm ssh-keygen
   2. Скопируйте открытый ключ пользователя vdsm на узел KVM. Файл known_hosts прокси-хоста также будет обновлен, чтобы включить в него ключ узла узла KVM:
      # sudo -u vdsm ssh-copy-id root@kvmhost.example.com
   3. Войдите на узел KVM, чтобы убедиться, что логин работает правильно:
      # sudo -u vdsm ssh root@kvmhost.example.com
2. Выберите *Администрирование* > *Провайдеры*.
3. Нажмите *Добавить*.
4. Заполните поля *Имя* и *Описание*.
5. Выберите KVM из раскрывающегося списка *Тип*.
6. Выберите дата-центр, в который будут импортированы виртуальные машины KVM, или выберите *Любой Дата Центр*, чтобы указать конечный дата-центр во время отдельных операций импорта.
7. Введите URI узла KVM в поле URI:
   qemu+ssh://root@host.example.com/system
8. Выберите узел в выбранном дата-центре в качестве прокси-хоста во время операций импорта виртуальной машины. Этот узел также должен иметь возможность подключаться к сети внешнего провайдера KVM. Если вы выбрали *Любой Дата Центр* в поле *Дата Центр* выше, вы не сможете выбрать узел здесь. Поле выделено серым цветом и показывает Любой *Узел* в Дата-центре. Вместо этого вы можете указать узел во время отдельных операций импорта.
9. При необходимости установите флажок *Требуется авторизация* и введите имя пользователя и пароль для узла KVM. Пользователь должен иметь доступ к узлу KVM, на котором находятся виртуальные машины.
10. Нажмите *Тестировать*, чтобы проверить, можете ли вы успешно пройти аутентификацию на узле KVM, используя предоставленные учетные данные.
11. Нажмите OK.

4.8.2.2 Установка нового сетевого провайдера OVN

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

Вы также можете подключить сеть OVN к собственной сети. Дополнительные сведения см. в разделе *Подключение сети OVN к физической сети*.

ovirt-provider-ovn предоставляет сетевой REST API OpenStack. Вы можете использовать этот API для создания сетей, подсетей, портов и маршрутизаторов.

Установка OVN с помощью engine-setup выполняет следующие действия:

- Настраивает центральный сервер OVN на компьютере с ядром.
- Добавляет OVN в KeyVirt в качестве внешнего сетевого провайдера.
- Только в кластере по умолчанию устанавливает для провайдера сети по умолчанию значение ovirt-provider-ovn.
- Установка OVN изменяет настройки сетевого провайдера по умолчанию только в кластере по умолчанию, но не в других кластерах.
- Изменение параметра сетевого провайдера по умолчанию не приводит к обновлению узлов в этом кластере для использования сетевого провайдера по умолчанию.
- Чтобы узлы и виртуальные машины могли использовать OVN, выполните дополнительные задачи, описанные в пункте *Дальнейшие действия* в конце этого раздела.

Процедура:

1. При необходимости, если вы используете предварительно настроенный файл ответов с engine-setup, добавьте следующую запись для установки OVN:
   OVESETUP_OVN/ovirtProviderOvn= bool:True
2. Запустите engine-setup на компьютере с Engine.
3. Если вы не используете предварительно настроенный файл ответов, поставьте Yes, когда engine-setup спросит:
   Configuring ovirt-provider-ovn also sets the Default cluster's default network provider to ovirt-provider-ovn.
   Non-Default clusters may be configured with an OVN after installation.
   Configure ovirt-provider-ovn (Yes, No) [Yes]:
4. Ответьте на следующий вопрос:
   Use default credentials (admin@internal) for ovirt-provider-ovn (Yes, No) [Yes]?:

Если выбрано Yes, engine-setup использует пользователя и пароль Engine по умолчанию, указанные ранее в процессе установки. Эта опция доступна только при новых установках.

OVN provider user[admin]:

OVN provider password[empty]:

Вы можете использовать значения по умолчанию или указать пользователя и пароль провайдера OVN.

Чтобы изменить метод аутентификации позже, вы можете отредактировать файл /etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf или создать новый файл /etc/ovirt-

provider-ovn/conf.d/20_engine_setup.conf. Перезапустите службу ovirt-provider-ovn, чтобы изменения вступили в силу.

4.8.2.3 Дальнейшие действия

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

1. Добавьте сеть в кластер по умолчанию.
    1. При этом установите флажок *Создать внешнего поставщика*. Это создает сеть на основе ovirt-provider-ovn.
    2. При необходимости, чтобы подключить сеть OVN к физической сети, установите флажок *Подключиться к физической сети* и укажите сеть KeyVirt для использования.
    3. При необходимости, определите, должна ли сеть использовать группу безопасности, и выберите ее из раскрывающегося списка Security Groups. Для получения дополнительной информации о доступных параметрах см. Описание общих настроек логической сети.
2. Добавьте узлы в или переустановите узлы в кластере по умолчанию, чтобы они использовали нового сетевого провайдера по умолчанию кластера, ovirt-provider-ovn.
3. При необходимости, отредактируйте кластеры, отличные от стандартных, и установите для провайдера сети по умолчанию значение ovirt-provider-ovn.
    1. При необходимости переустановите узлы в каждом кластере, отличном от стандартного, чтобы они использовали нового провайдера сети по умолчанию кластера, ovirt-provider-ovn.

Дополнительные ресурсы:

Чтобы настроить ваши узлы на использование существующей сети, отличной от сети по умолчанию, см. раздел *Настройка узлов для туннельной сети OVN*.

4.8.2.4 Обновление туннельной сети OVN на одном узле

Вы можете обновить туннельную сеть OVN на одном узле с помощью vdsm-tool:
vdsm-tool ovn-config OVN_Central_IP Tunneling_IP_or_Network_Name Host_FQDN
Доменное имя Host_FQDN должно соответствовать полному доменному имени, указанному в ядре для этого узла.
Пример. Обновление узла с vdsm-tool
vdsm-tool ovn-config 192.168.0.1 MyNetwork MyFQDN

4.8.2.5 Подключение сети OVN к физической сети

Вы можете создать сеть внешнего провайдера, которая накладывается на собственную сеть KeyVirt, чтобы создавалось впечатление, что виртуальные машины на каждой из них совместно используют одну и ту же подсеть.
Если вы создали подсеть для сети OVN, виртуальная машина, использующая эту сеть, получит оттуда IP-адрес. Если вы хотите, чтобы физическая сеть выделяла IP-адрес, не создавайте подсеть для сети OVN.

Требования:

- В кластере должен быть выбран OVS в качестве типа коммутатора. На узлах, добавленных в этот кластер, не должно быть настроено никаких ранее существовавших сетей KeyVirt, таких как мост ovirtmgmt.

- Физическая сеть должна быть доступна на узлах. Вы можете применить это, установив физическую сеть в соответствии с требованиями для кластера (в окне *Управление сетями* или на вкладке *Кластер* окна *Новая логическая сеть*).

Процедура:

1. Выберите *Виртуализация* > *Кластеры*.
2. Нажмите на название кластера. Откроется окно сведений.
3. Перейдите на вкладку *Логические сети* и нажмите *Добавить сеть*.
4. Введите имя для сети.
5. Установите флажок *Создать внешнего поставщика*. По умолчанию выбрано ovirt-provider-ovn.
6. Установите флажок *Подключиться к физической сети*, если он еще не установлен по умолчанию.
7. Выберите физическую сеть для подключения к новой сети:
   1. Нажмите переключатель *Сеть Дата-центра* и выберите физическую сеть из выпадающего списка. Это рекомендуемый вариант.
   2. Нажмите переключатель Custom (Своё) и введите название физической сети. Если в физической сети включена пометка VLAN, необходимо также установить флажок Enable VLAN tagging и ввести тег VLAN физической сети.

      Имя физической сети не должно быть длиннее 15 символов или содержать специальные символы.
8. Нажмите OK.

4.8.2.6 Объяснение общих параметров добавления провайдера

Вкладка *Общее* в окне *Добавить поставщика* позволяет зарегистрировать основные сведения о внешнем провайдере.

Таблица 27. *Добавить поставщика*: *Общее*

Настройка	Объяснение
Имя	Имя, представляющее провайдера в Engine.
Описание	Описание провайдера в виде простого и понятного текста.
Тип	Тип внешнего провайдера. Изменение этого параметра изменяет доступные поля для настройки провайдера. **External Network Provider** • Networking Plugin: определяет, какая реализация драйвера будет использоваться на узле для обработки операций сетевой карты. Если внешний сетевой провайдер с плагином KeyVirt Network Provider for OVN добавлен в качестве сетевого провайдера по умолчанию для кластера, это также определяет, какой драйвер будет установлен на узлах, добавленных в кластер. • Automatic Synchronization: позволяет указать, будет ли провайдер автоматически синхронизироваться с существующими сетями. • Provider URL: URL-адрес или полное доменное имя компьютера, на котором размещен внешний сетевой провайдер. Вы должны добавить номер порта для внешнего сетевого провайдера в конец URL-адреса или полного доменного имени. По умолчанию этот номер порта равен 9696.

	• Read Only: позволяет указать, можно ли изменить провайдера внешней сети с Портала администратора. • *Требуется авторизация*: позволяет указать, требуется ли проверка подлинности для доступа к внешнему сетевому провайдеру. • Username: Имя пользователя для подключения к внешнему сетевому провайдеру. Если вы проходите проверку подлинности с помощью Active Directory, имя пользователя должно быть в формате username@domain@auth_profile вместо username@domain по умолчанию. • Password: пароль, с помощью которого должно быть аутентифицировано указанное выше имя пользователя. • Protocol: протокол, используемый для связи с сервером Keystone. По умолчанию используется HTTPS. • Hostname: IP-адрес или имя узла сервера Keystone. • API port: номер порта API сервера Keystone. • API Version: версия сервера Keystone. Значение равно v2.0, а поле отключено. • Tenant Name: необязательно. Имя проекта (тенанта), участником которого является внешний сетевой провайдер. **Foreman/Satellite** • Provider URL: URL-адрес или полное доменное имя компьютера, на котором размещен экземпляр Satellite. Вам не нужно добавлять номер порта в конец URL-адреса или полного доменного имени. • *Требуется авторизация*: позволяет указать, требуется ли аутентификация для провайдера. Аутентификация обязательна при выборе Foreman/Satellite. • Username: имя пользователя для подключения к экземпляру Satellite. Это имя пользователя должно быть именем пользователя, используемым для входа на портал подготовки в экземпляре Satellite. • Password: пароль, с помощью которого должно быть аутентифицировано указанное выше имя пользователя. Этот пароль должен быть паролем, используемым для входа на портал подготовки в экземпляре Satellite. **KubeVirt/OpenShift Virtualization** • Provider URL: URL-адрес или полное доменное имя и номер порта OKD API. По умолчанию этот номер порта равен 6443. • Token: токен доступа OAuth для аутентификации этого подключения к API. • Certificate Authority: Сертификат CA, которому следует доверять при выполнении запросов https. • Prometheus URL: URL-адрес службы prometheus кластера OpenShift. Если вы не укажете этот URL, программа попытается автоматически определить этот URL. • Prometheus Certificate Authority: Сертификат X509 для prometheus. Если вы не укажете этот центр сертификации,

	провайдер использует вместо него центр сертификации KubeVirt. **OpenStack Image** • Provider URL: URL-адрес или полное доменное имя компьютера, на котором размещена служба изображений OpenStack. Вы должны добавить номер порта для службы изображений OpenStack в конец URL-адреса или полного доменного имени. По умолчанию этот номер порта равен 9292. • *Требуется авторизация*: позволяет указать, требуется ли проверка подлинности для доступа к службе изображений OpenStack. • Username: имя пользователя для подключения к серверу Keystone. Это имя пользователя должно быть именем пользователя для службы изображений OpenStack, зарегистрированной в экземпляре Keystone, участником которого является служба изображений OpenStack. • Password: пароль, с помощью которого должно быть аутентифицировано указанное выше имя пользователя. Этот пароль должен быть паролем для службы изображений OpenStack, зарегистрированной в экземпляре Keystone, участником которого является служба изображений OpenStack. • Protocol: протокол, используемый для связи с сервером Keystone. Для этого параметра должно быть установлено значение HTTP. • Hostname: IP-адрес или имя узла сервера Keystone. • API port: номер порта API сервера Keystone. • API Version: версия службы Keystone. Значение равно v2.0, а поле отключено. • Tenant Name: имя тенанта OpenStack, участником которого является служба изображений OpenStack. **OpenStack Volume** • *Дата Центр*: дата-центр, к которому будут подключены тома хранилища OpenStack Volume. • Provider URL: URL-адрес или полное доменное имя компьютера, на котором размещен экземпляр тома OpenStack. Необходимо добавить номер порта для экземпляра тома OpenStack в конец URL-адреса или полного доменного имени. По умолчанию этот номер порта равен 8776. • *Требуется авторизация*: позволяет указать, требуется ли проверка подлинности для доступа к службе томов OpenStack. • Username: имя пользователя для подключения к серверу Keystone. Это имя пользователя должно быть именем пользователя для тома OpenStack, зарегистрированного в экземпляре Keystone, членом которого является экземпляр тома OpenStack.

	• Password: пароль, с помощью которого должно быть аутентифицировано указанное выше имя пользователя. Этот пароль должен быть паролем для тома OpenStack, зарегистрированного в экземпляре Keystone, членом которого является экземпляр тома OpenStack. • Protocol: протокол, используемый для связи с сервером Keystone. Для этого параметра должно быть установлено значение HTTP. • Hostname: IP-адрес или имя узла сервера Keystone. • API port: номер порта API сервера Keystone. • API Version: версия сервера Keystone. Значение равно v2.0, а поле отключено. • Tenant Name: имя клиента OpenStack, членом которого является экземпляр тома OpenStack. **KVM** • *Дата Центр*: укажите дата-центр, в который будут импортированы виртуальные машины KVM, или выберите Any Data Center, чтобы вместо этого указать целевой дата-центр во время отдельных операций импорта (используя функцию *Импортировать* на вкладке *Виртуальные машины*). • URI: URI узла KVM. • Proxy Host: выберите узел в выбранном дата-центре, который будет выполнять функции узла во время операций импорта виртуальной машины. Этот узел также должен иметь возможность подключаться к сети внешнего провайдера KVM. Если вы выбрали Any Data Center, вы не можете выбрать узел здесь, но вместо этого можете указать узел во время отдельных операций импорта (используя функцию *Импортировать* на вкладке *Виртуальные машины*). • *Требуется авторизация*: позволяет указать, требуется ли аутентификация для доступа к узлу KVM. • Username: имя пользователя для подключения к узлу KVM. • Password: пароль, с помощью которого должно быть аутентифицировано указанное выше имя пользователя.
Test	Позволяет пользователям проверять указанные учетные данные. Эта кнопка доступна для всех типов провайдеров.

4.8.3 Редактирование внешнего провайдера

Чтобы внести изменения для внешнего провайдера:

1. Нажмите *Администрирование* > *Провайдеры* и выберите внешнего провайдера для редактирования.
2. Нажмите *Изменить*.
3. Измените текущие значения для провайдера на предпочтительные значения.
4. Нажмите OK.

4.8.4 Удаление внешнего провайдера

Чтобы удалить внешнего провайдера:

1. Нажмите *Администрирование* > *Провайдеры* и выберите внешнего провайдера для удаления.
2. Нажмите *Удалить*.
3. Нажмите OK.

5 АДМИНИСТРИРОВАНИЕ ВИРТУАЛЬНЫХ МАШИН

5.1 ВИРТУАЛЬНЫЕ МАШИНЫ И РАЗРЕШЕНИЯ

5.1.1 Управление системными разрешениями для виртуальной машины

В качестве суперпользователя системный администратор управляет всеми аспектами портала администратора. Другим пользователям можно назначить более конкретные административные роли. Эти ограниченные роли администратора полезны для предоставления пользователю административных привилегий, ограничивающих его доступ к определенному ресурсу. Например, роль DataCenterAdmin имеет права администратора только для назначенного центра обработки данных, за исключением хранилища для этого центра обработки данных, а роль ClusterAdmin имеет права администратора только для назначенного кластера. UserVmManager – это роль системного администратора для виртуальных машин в центре обработки данных. Эту роль можно применить к конкретным виртуальным машинам, центру обработки данных или всей виртуализированной среде; это полезно, поскольку позволяет разным пользователям управлять определенными виртуальными ресурсами.
Роль администратора виртуальной машины пользователя разрешает следующие действия:

- Создание, редактирование и удаление виртуальных машин.
- Запуск, приостановка, завершение работы и остановка виртуальных машин.

5.2 ОСНОВНЫЕ ЗАДАЧИ ВИРТУАЛЬНЫХ МАШИН

Установка виртуальной машины включает следующие ключевые шаги:

1. Создание виртуальной машины. Для создания ВМ необходим сетевой интерфейс и предварительно созданный виртуальный диск.
2. Запуск виртуальной машины и установка операционной системы.
3. Включение необходимых репозиториев для вашей операционной системы.
4. Установка гостевых агентов и драйверов для дополнительных функций виртуальной машины.

5.2.1 Создание виртуальной машины

Примечание. Прежде чем вы сможете использовать новую виртуальную машину, вы должны установить операционную систему и зарегистрироваться в Content Delivery Network. Установить операционную систему можно следующими способами:

- Использовать предварительно установленный образ, создав клонированную виртуальную машину на основе шаблона.
- Использовать предустановленный образ с прикрепленного предустановленного Диска.
- Установить операционную систему через загрузочное меню PXE или из файла ISO.

Для создания виртуальной машины выполните следующие действия:
1. Нажмите кнопку Новый на панели инструментов для *Виртуальные машины*.
2. Задайте следующие поля:
    - *Имя* – Имя виртуальной машины может содержать только прописные или строчные буквы, цифры, символы подчеркивания (_), дефисы (-) или точки (.). Использование специальных символов и пробелов не допускается;
    - *Описание* (опционально);
    - *Кластер*;
    - *Шаблон*;
    - *Операционная система*;
    - *Гарантированная ОЗУ* (Physical Memory Guaranteed);
    - CPUs;
    - *Консоль*;
    - *Последовательность загрузки* (Boot sequence):
        - Первое устройство;
        - Вторичное устройство.
    - *Запуск инициализации* - Cloud-Init;
    - *Логотип*.
3. Нажмите OK.

Новая виртуальная машина будет создана и отобразится в списке виртуальных машин со статусом *Выключено*. Вы можете изменить некоторые из этих параметров позже, включая набор микросхем и тип BIOS.

5.2.2 Запуск и подключение к виртуальной машине

Для запуска и подключения к виртуальной машине выполните следующие действия:
1. На панели виртуальных машин нажмите кнопку Запустить (Run) на карточке виртуальной машины, чтобы запустить эту виртуальную машину.
2. Нажмите кнопку *Консоль*, чтобы подключиться к виртуальной машине.
3. Вам будет предложено загрузить файл в формате **.vv**
4. Откройте файл с помощью remote-viewer. Откроется окно консоли. Теперь вы можете использовать виртуальную машину так же, как и физический рабочий стол.

Примечание. Виртуальная машина не запускается на узле, на котором перегружен CPU.

Установка гостевых агентов и драйверов

Гостевые агенты, инструменты и драйверы обеспечивают дополнительные функции для виртуальных машин, такие как корректное завершение работы или перезагрузка виртуальных машин с портала виртуальных машин и портала администратора. Инструменты и агенты также предоставляют информацию для виртуальных машин, такую как:

- Использование ресурсов;
- IP-адреса.

Гостевые агенты, инструменты и драйверы распространяются в виде файла ISO, который можно прикрепить к виртуальным машинам. Этот файл ISO упакован как файл RPM, который вы можете установить и обновить с машины Engine.

Вам необходимо установить гостевые агенты и драйверы на виртуальной машине, чтобы включить эти функции для этой машины.

Таблица 28. Используемые драйверы guest

Драйвер	Описание	Работает на
virtio-net	Паравиртуализированный сетевой драйвер обеспечивает повышенную производительность по сравнению с эмулируемыми устройствами, такими как rtl.	Сервере и рабочем столе
virtio-block	Паравиртуализированный драйвер жесткого диска обеспечивает повышенную производительность ввода-вывода по сравнению с эмулируемыми устройствами, такими как IDE, за счет оптимизации координации и взаимодействия между виртуальной машиной и гипервизором. Драйвер дополняет программную реализацию virtio-устройства, используемого узлом для выполнения роли аппаратного устройства.	Сервере и рабочем столе
virtio-scsi	Паравиртуализированный драйвер жесткого диска iSCSI предлагает функциональность, аналогичную устройству virtio-block, с некоторыми дополнительными улучшениями. В частности, этот драйвер поддерживает добавление сотен устройств и присваивает устройствам имена, используя стандартную схему именования устройств SCSI.	Сервере и рабочем столе
virtio-serial	Virtio-serial обеспечивает поддержку нескольких последовательных портов. Повышенная производительность используется для быстрой связи между виртуальной машиной и узлом, что позволяет избежать сетевых осложнений. Такая быстрая связь необходима гостевым агентам и для других функций, таких как копирование-вставка в буфер обмена между виртуальной машиной и узлом и ведение журнала.	Сервере и рабочем столе
virtio-balloon	Virtio-balloon используется для управления объемом памяти, к которому фактически обращается виртуальная машина. Оно	Сервере и рабочем столе

	обеспечивает улучшенное использование избыточной памяти.	
qxl	Паравиртуализированный драйвер дисплея снижает загрузку процессора на узле и обеспечивает более высокую производительность за счет снижения пропускной способности сети при большинстве рабочих нагрузок.	Сервере и рабочем столе

Таблица 29. Гостевые агенты и инструменты KeyVirt

Гостевой агент или инструмент	Описание	Работает на
qemu-guest-agent	Используется вместо ovirt-guest-agent-common на корпоративных виртуальных машинах Linux 8. Оно установлено и включено по умолчанию.	Сервере и рабочем столе
spice-agent	Агент SPICE поддерживает несколько мониторов и отвечает за поддержку режима клиентской мыши, чтобы обеспечить лучший пользовательский интерфейс и повышенную скорость реагирования, чем эмуляция QEMU. Захват курсора не требуется в режиме клиентской мыши. SPICE agent снижает использование полосы пропускания при использовании по глобальной сети за счет снижения уровня отображения, включая глубину цвета, отключение обоев, сглаживание шрифтов и анимацию. Агент SPICE обеспечивает поддержку буфера обмена, позволяя выполнять операции вырезания и вставки текста и изображений между клиентом и виртуальной машиной, а также автоматическую настройку гостевого отображения в соответствии с настройками на стороне клиента. На виртуальных машинах под управлением Windows агент SPICE состоит из vdservice и vdagent.	Сервере и рабочем столе

5.2.3 Редактирование виртуальных машин

Примечание. Роль пользователя должна иметь разрешение на редактирование виртуальной машины. Вы можете редактировать диски и сетевые интерфейсы виртуальной машины в представлении сведений о виртуальной машине.
Вы можете редактировать следующие параметры ВМ на отдельных карточках:

- **Virtual Machine name and description** (Имя и описание виртуальной машины)

- **Details** (Подробности):
  - Template (шаблон) – отображает имя шаблона, используемого для создания этой виртуальной машины.
  - Change CD (изменить компакт-диск) – позволяет выбрать файл ISO, доступный виртуальной машине в качестве компакт-диска.
  - CPUs (ЦП) – позволяет настроить количество виртуальных ЦП, доступных для виртуальной машины.
  - Memory (ОЗУ) – позволяет настроить виртуальную память, доступную для виртуальной машины.
- **Details – Advanced Options** (детали – дополнительные параметры):
  - Cloud-Init – инструмент cloud-init позволяет автоматизировать развертывание виртуальных машин. Если для этого параметра установлено значение ON, отображаются поля Имя узла и SSH-ключи.
  - Operating System (операционная система) – позволяет выбрать операционную систему, установленную на этой виртуальной машине.
  - Boot Menu (меню загрузки) – если установлено значение ON, в консоли появляется меню загрузки, позволяющее выбрать загрузочное устройство.
  - Boot Order (порядок загрузки) – First Device и Second Device (первое или второе устройство, которое будет проверено на загрузку)
- **Snapshots** (Снимки) – список сохраненных снимков.
  - Нажмите на значок *Изменить*, чтобы отобразить кнопку *Создать снимок* (Create Snapshot) для создания нового снимка.
  - Нажмите на значок information, restore или delete, чтобы просмотреть сведения, восстановить снимок или удалить снимок.
- **Network Interfaces** (Сетевые интерфейсы) – список сетевых интерфейсов, определенных для выбранной виртуальной машины.
  - Нажмите на значок *Изменить*, чтобы отобразить кнопку Create NIC для создания новой записи сетевого интерфейса.
  - Нажмите на значок *Изменить* или *Удалить*, чтобы изменить или удалить сетевой интерфейс.
- **Disks** (Диски) – список дисков, определенных для выбранной виртуальной машины.
  - Нажмите на значок *Изменить*, чтобы отобразить кнопку Create Disc для создания новой записи на диске.
  - Нажмите на значок *Изменить* или Delete, чтобы изменить или удалить диск.

5.2.4 Редактирование свойств виртуальных машин

Изменения параметров хранилища, операционной системы или сети могут отрицательно повлиять на виртуальную машину. Прежде чем вносить какие-либо изменения, убедитесь, что у вас есть правильные данные. Виртуальные машины можно редактировать во время работы, и некоторые изменения (перечисленные в процедуре ниже) будут применены немедленно. Чтобы применить все остальные изменения, виртуальную машину необходимо выключить и перезапустить.
Примечание. Внешние виртуальные машины (отмеченные префиксом external) нельзя редактировать через Engine.
Для редактирования виртуальных машин выполните следующие действия:
1. Нажмите *Виртуализация* > *Виртуальные машины*.

2. Выберите виртуальную машину для редактирования.
3. Нажмите *Изменить*.

При необходимости измените настройки. Изменения следующих параметров вступают в силу немедленно:

- Имя
- Описание
- Комментарий
- Оптимизировано для (Рабочий стол/Сервер/Высокая производительность)
- Защита от удаления
- Сетевые интерфейсы
- Размер памяти
- Виртуальные сокеты
- Использовать пользовательское время простоя при миграции
- Высокая доступность
- Приоритет очереди запуска/миграции
- Выключить строгую проверку пользователей
- Значок

4. Нажмите OK.
5. Если появится всплывающее окно *Изменения, которые могут быть применены немедленно*:, нажмите OK.

Некоторые изменения вступают в силу немедленно. Все остальные изменения применяются при завершении работы и перезапуске виртуальной машины. До этого момента значок ожидающих изменений () отображается как напоминание о перезапуске виртуальной машины.

5.2.5 Перезагрузка виртуальных машин

Для виртуальных машин есть два вида перезагрузки: обычная и аварийная (сброс настроек). В обоих случаях консоль виртуальной машины остается открытой, пока гостевая операционная система перезапускается.

Если гостевая операционная система не загружается или перестает отвечать на запросы, необходима аварийная перезагрузка.

Внимание! Для данной процедуры требуется доступ к Порталу администратора.

Для обычной перезагрузки виртуальной машины выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите работающую виртуальную машину.
2. Нажмите *Перезагрузить*.
3. Нажмите OK в окне подтверждения *Перезагрузить виртуальную машину(ы)*.

Для аварийной перезагрузки виртуальной машины выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите работающую виртуальную машину.
2. Нажмите стрелку вниз рядом с *Перезагрузить*, затем нажмите *Сброс*.
3. Нажмите OK в окне подтверждения *Сброс виртуальной машины (машин)*.

В обоих случаях статус виртуальной машины меняется на *Выполняется перезагрузка*, прежде чем вернется в статус *Включено*.

5.2.6 Удаление виртуальных машин

Кнопка *Удалить* отключена во время работы виртуальных машин; вы должны выключить виртуальную машину, прежде чем сможете ее удалить.

Для удаления виртуальной машины выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину для удаления.
2. Нажмите (⋮) *Контекстное Меню, затем* нажмите *Удалить*.
3. При необходимости установите флажок *Удалить диск(и)*, чтобы удалить виртуальные диски, подключенные к виртуальной машине вместе с виртуальной машиной. Если флажок *Удалить диск(и)* снят, виртуальные диски остаются в среде как плавающие.
4. Нажмите OK.

5.2.7 Клонирование виртуальных машин

Вы можете клонировать виртуальные машины без предварительного создания шаблона или моментального снимка.

Для клонирования виртуальной машины выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину для клонирования.
2. Нажмите (⋮) *Контекстное Меню*, затем нажмите *Клонировать ВМ*.
3. Введите имя клона для новой виртуальной машины.
4. Нажмите OK.

5.3 ДОПОЛНИТЕЛЬНАЯ КОНФИГУРАЦИЯ ВИРТУАЛЬНЫХ МАШИН

5.3.1 Протоколы подключения для настройки параметров консоли

Протоколы подключения – это базовая технология, используемая для предоставления графических консолей для виртуальных машин и позволяющая пользователям работать с виртуальными машинами так же, как с физическими машинами. В настоящее время KeyVirt поддерживает следующие протоколы подключения:

SPICE

Простой протокол для независимой вычислительной среды (SPICE) – рекомендуемый протокол подключения как для виртуальных машин Linux, так и для виртуальных машин Windows. Чтобы открыть консоль для виртуальной машины с помощью SPICE, используйте Remote Viewer.

VNC

Виртуальные сетевые вычисления (VNC) можно использовать для открытия консолей как для виртуальных машин Linux, так и для виртуальных машин Windows. Чтобы открыть консоль для виртуальной машины с помощью VNC, используйте Remote Viewer или клиент VNC.

RDP

Протокол удаленного рабочего стола (RDP) может использоваться только для открытия консолей для виртуальных машин Windows и доступен только при доступе к виртуальным машинам с компьютера Windows, на котором установлен удаленный рабочий стол. Прежде чем вы сможете подключиться к виртуальной машине Windows с помощью RDP, вы должны настроить удаленный общий доступ на виртуальной машине и настроить брандмауэр, чтобы разрешить подключения к удаленному рабочему столу.

5.3.2 Последовательная консоль для виртуальных машин

5.3.2.1 Открытие последовательной консоли для виртуальной машины

Вы можете получить доступ к последовательной консоли виртуальной машины из командной строки вместо того, чтобы открывать консоль из Портала администратора или Портала виртуальных машин. Последовательная консоль эмулируется через каналы VirtIO с использованием SSH и пар ключей. Engine действует как прокси для соединения, предоставляет информацию о размещении виртуальной машины и хранит ключи аутентификации. Вы можете добавить открытые ключи для каждого пользователя либо с Портала администратора, либо с Портала виртуальных машин. Вы можете получить доступ к последовательной консоли только для тех виртуальных машин, для которых у вас есть соответствующие разрешения.

Примечание. Чтобы получить доступ к последовательной консоли виртуальной машины, пользователь должен иметь разрешение UserVmManager, SuperUser или UserInstanceManager на этой виртуальной машине. Эти разрешения должны быть явно определены для каждого пользователя. Недостаточно назначить эти разрешения для всех пользователей виртуальной машины.

Доступ к последовательной консоли осуществляется через TCP-порт 2222. Этот порт открывается вовремя engine-setup при новых установках. Использование последовательной консоли требует настройки правил брандмауэра.

Последовательная консоль полагается на пакеты ovirt-vmconsole и ovirtvmconsole-proxy на Engine, и пакеты ovirt-vmconsole и ovirt-vmconsole-host на узлах виртуализации. Чтобы установить пакеты в существующих установках, переустановите узел.

Внимание! Включение последовательной консоли виртуальной машины возможно только на Портале администратора.

5.3.2.2 Подключение к последовательной консоли виртуальной машины

На клиентском компьютере подключитесь к последовательной консоли виртуальной машины:

- Если доступна одна виртуальная машина, эта команда подключает пользователя к этой виртуальной машине:

```
# ssh -t -p 2222 ovirt-vmconsole@Manager_FQDN -i .ssh/serialconsolekey
 Enterprise Linux Server release 6.7 (Santiago)
 Kernel 2.6.32-573.3.1.el6.x86_64 on an x86_64
 USER login:
```

- Если доступно более одной виртуальной машины, в этой команде перечислены доступные виртуальные машины и их идентификаторы:

```
# ssh -t -p 2222 ovirt-vmconsole@Manager_FQDN -i .ssh/serialconsolekey list
 1. vm1 [vmid1]
 2. vm2 [vmid2]
 3. vm3 [vmid3]
 > 2
 Enterprise Linux Server release 6.7 (Santiago)
 Kernel 2.6.32-573.3.1.el6.x86_64 on an x86_64
 USER login:
```

Введите номер машины, к которой вы хотите подключиться, и нажмите Enter.

- В качестве альтернативы можно подключиться непосредственно к виртуальной машине, используя ее уникальный идентификатор или имя:

```
# ssh -t -p 2222 ovirt-vmconsole@Manager_FQDN connect --vm-id vmid1
# ssh -t -p 2222 ovirt-vmconsole@Manager_FQDN connect --vm-name vm1
```

5.3.2.3 Отключение от последовательной консоли виртуальной машины

Нажмите любую клавишу, за которой следует **~ .**, чтобы закрыть сеанс последовательной консоли.

При аварийном отключении сеанса последовательной консоли возникает тайм-аут TCP. Вы не сможете повторно подключиться к последовательной консоли виртуальной машины, пока не истечет время ожидания.

5.3.3 Настройка сторожевого таймера (Watchdog)

Вы можете добавить на виртуальную машину сторожевой таймер, чтобы отслеживать действия операционной системы.

Процедура:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите *Изменить*.
3. Перейдите на вкладку *Высокая доступность*.
4. Выберите модель сторожевого таймера для использования в раскрывающемся списке *Модель наблюдателя* (Watchdog Model).
5. Выберите действие из раскрывающегося списка *Действие наблюдателя* (Watchdog Action). Это действие, которое выполняет виртуальная машина при запуске сторожевого таймера.
6. Нажмите OK.

5.3.3.1 Установка сторожевого таймера

Чтобы активировать сторожевой таймер, подключеный к виртуальной машине, вы должны установить пакет watchdog на эту виртуальную машину и запустить службу watchdog.

Для установки Watchdogs на Linux выполните следующие действия:

1. Войдите в систему на виртуальной машине, к которой подключена контрольная карта.
2. Установите watchdog пакет и зависимости:
   # yum install watchdog
3. Отредактируйте файл/etc/watchdog.conf и раскомментируйте следующую строку:
   watchdog-device = /dev/watchdog
4. Сохраните изменения.
5. Запустите службу watchdog и убедитесь, что эта служба запускается при загрузке:

6. Enterprise Linux 6:
   # service watchdog start
   # chkconfig watchdog on
7. Enterprise Linux 7:
   # systemctl start watchdog.service
   # systemctl enable watchdog.service

5.3.3.2 Подтверждение функциональности сторожевого таймера

Убедитесь, что сторожевой таймер подключен к виртуальной машине и что служба watchdog активна.

Примечание. Эта процедура предназначена только для проверки функциональности сторожевых таймеров и не должна выполняться на физических машинах.

Для подтверждения функциональности Watchdog выполните следующие действия:

1. Войдите в систему на виртуальной машине, к которой подключена контрольная карта.
2. Подтвердите, что виртуальная машина идентифицировала контрольную карту:
   # lspci | grep watchdog -i
3. Выполните одну из следующих команд, чтобы подтвердить, что сторожевой таймер активен:

4. Запустите kernel panic:
   # echo c > /proc/sysrq-trigger
5. Завершите службу watchdog:
   # kill -9 pgrep watchdog

5.3.3.3 Параметры сторожевого таймера в watchdog.conf

Ниже приводится список параметров для настройки службы watchdog, доступных в файле /etc/watchdog.conf. Чтобы настроить параметр, необходимо

раскомментировать этот параметр и перезапустить службу watchdog после сохранения изменений.

Таблица 30. Описание параметров watchdog

Имя переменной	Значение по умолчанию	Примечание
ping	N/A	IP-адрес, который сторожевой таймер пытается пропинговать, чтобы проверить, доступен ли этот адрес. Вы можете указать несколько IP-адресов, добавив дополнительные ping строки.
interface	N/A	Сетевой интерфейс, который будет отслеживать сторожевой таймер для проверки наличия сетевого трафика. Вы можете указать несколько сетевых интерфейсов, добавив дополнительные interface строки.
file	/var/log/messages	Файл в локальной системе, который сторожевой таймер будет отслеживать на предмет изменений. Вы можете указать несколько файлов, добавив дополнительные строки file.
change	1407	Количество контрольных интервалов, по истечении которых контрольный таймер проверяет наличие изменений в файлах. В строке непосредственно после каждой change строки должна быть указана строка file, которая применяется к строке file непосредственно над этой строкой change.
max-load-1	24	Максимальная средняя нагрузка, которую виртуальная машина может выдержать в течение одной минуты. Если это среднее значение превышено, то запускается сторожевой таймер. Значение 0 отключает эту функцию.
max-load-5	18	Максимальная средняя нагрузка, которую виртуальная машина может выдержать в течение пятиминутного периода. Если это среднее значение превышено, то запускается сторожевой таймер. Значение 0 отключает эту функцию. По умолчанию значение этой переменной равно значению, равному примерно трем четвертям от max-load-1.
max-load-15	12	Максимальная средняя нагрузка, которую виртуальная машина может выдержать в течение пятнадцатиминутного периода. Если это среднее значение превышено, то запускается сторожевой таймер. Значение 0 отключает эту функцию. По умолчанию значение этой

		переменной равно значению, примерно вдвое меньшему, чем max-load-1.
min-memory	1	Минимальный объем виртуальной памяти, который должен оставаться свободным на виртуальной машине. Это значение измеряется в страницах. Значение 0 отключает эту функцию.
repair-binary	/usr/sbin/repair	Путь и имя двоичного файла в локальной системе, который будет запущен при запуске сторожевого таймера. Если указанный файл устраняет проблемы, не позволяющие watchdog сбросить счетчик watchdog, то действие watchdog не запускается.
test-binary	N/A	Путь и имя двоичного файла в локальной системе, который сторожевой таймер будет пытаться запустить в течение каждого интервала. Тестовый двоичный файл позволяет указать файл для выполнения пользовательских тестов.
test-timeout	N/A	Ограничение по времени в секундах, в течение которого могут выполняться пользовательские тесты. Значение 0 позволяет выполнять пользовательские тесты неограниченное время.
temperature-device	N/A	Путь и имя устройства для проверки температуры компьютера, на котором запущена служба watchdog.
max-temperature	120	Максимально допустимая температура для компьютера, на котором запущена служба watchdog. При достижении этой температуры машина будет остановлена. Преобразование единиц измерения не учитывается, поэтому необходимо указать значение, соответствующее используемой контрольной карте.
admin	root	Адрес электронной почты, на который отправляются уведомления по электронной почте.
interval	10	Интервал в секундах между обновлениями сторожевого устройства. Сторожевое устройство ожидает обновления не реже одного раза в минуту, и если в течение одной минуты обновлений нет, то запускается сторожевой таймер. Этот одноминутный период жестко запрограммирован в драйверах для сторожевого устройства и не может быть настроен.
logtick	1	Когда для watchdog включено подробное ведение журнала, служба watchdog

		периодически записывает сообщения журнала в локальную систему. Значение logtick представляет собой количество контрольных интервалов, после которых записывается сообщение.
realtime	yes	Указывает, заблокирован ли сторожевой таймер в памяти. Значение yes блокирует сторожевой таймер в памяти, чтобы он не был выгружен из памяти, в то время как значение no позволяет выгружать сторожевой таймер из памяти. Если сторожевой таймер выгружен из памяти и не выгружен обратно до того, как счетчик сторожевого таймера достигнет нуля, то запускается сторожевой таймер.
priority	1	Приоритет расписания, когда значение realtime – yes.
pidfile	/var/run/syslogd.pid	Путь и имя файла PID-файла, который отслеживает сторожевой таймер, чтобы увидеть, все еще активен ли соответствующий процесс. Если соответствующий процесс не активен, то запускается сторожевой таймер.

5.3.4 Настройка виртуального NUMA

На Портале администратора вы можете настроить виртуальные узлы NUMA на виртуальной машине и привязать их к физическим узлам NUMA на одном или нескольких узлах. Политика узла по умолчанию заключается в планировании и запуске виртуальных машин на любых доступных ресурсах на узле. В результате ресурсы, поддерживающие виртуальную машину большого размера, которая не может поместиться в одном сокете узла, могут быть распределены по нескольким узлам NUMA. Со временем эти ресурсы могут перемещаться, что приводит к плохой и непредсказуемой производительности. Настройте и закрепите виртуальные узлы NUMA, чтобы избежать этого и повысить производительность.

Внимание! Настройка виртуальных узлов NUMA возможна только на Портале администратора.

Для настройки виртуального NUMA требуется узел с поддержкой NUMA. Чтобы проверить, включен ли NUMA на узле, войдите на узел и запустите numactl --hardware. Выходные данные этой команды должны показать, как минимум два узла NUMA. Вы также можете просмотреть топологию NUMA узла на Портале администратора, выбрав узел на вкладке *Узлы* и нажав NUMA Support. Эта кнопка доступна только в том случае, если выбранный узел имеет как минимум два узла NUMA.

Для настройки виртуального NUMA выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите *Изменить*.
3. Нажмите *Показать расширенные опции*.

4. Перейдите на вкладку *Узел*.
5. Выберите *Указанные узлы* и выберите узел(ы) из списка. Выбранный узел(ы) должен иметь как минимум два узла NUMA.
6. Нажмите *Привязка NUMA*.
7. В окне NUMA Topology выберите и перетащите виртуальные узлы NUMA из поля справа, чтобы разместить узлы NUMA слева, как требуется, и нажмите OK.
8. Выберите Strict, Preferred или Irrelative из раскрывающегося списка Tune Mode на каждом узле NUMA. Если выбранный режим является Preferred, количество узлов NUMA должно быть установлено равным 1.
9. Вы также можете автоматически настроить политику закрепления NUMA, выбрав Resize and Pin NUMA в раскрывающемся списке CPU Pinning Polcy под настройками CPU Allocation на вкладке *Выделение ресурсов*. Распределение ресурсов:

    - None – Выполняется без какого-либо закрепления процессора.
    - Manual – Запускает указанный вручную виртуальный процессор на определенном физическом процессоре и определенном узле. Доступно только тогда, когда виртуальная машина закреплена на узле.
    - Resize and Pin NUMA – Изменяет размер виртуального процессора и топологии NUMA виртуальной машины в соответствии с узлом и привязывает их к ресурсам узла.
    - Dedicated – Для размещения физических процессоров используются исключительно виртуальные процессоры. Доступно для уровня совместимости с кластерами 4.7 или более поздней версии. Если на виртуальной машине включена функция NUMA, все узлы должны быть отключены.
    - Isolate Threads – Для размещения физических процессоров используются исключительно виртуальные процессоры. Каждый виртуальный процессор получает физическое ядро. Доступно для уровня совместимости с кластерами 4.7 или более поздней версии. Если на виртуальной машине включена функция NUMA, все узлы должны быть отключены.

10. Нажмите OK.

Если вы не привязываете виртуальный узел NUMA к узлу NUMA узла, система по умолчанию использует узел NUMA, который содержит систему ввода-вывода с отображением памяти хост-устройства (MMIO), при условии, что имеется одно или несколько хост-устройств, и все эти устройства относятся к одному узлу NUMA.

5.3.5 Включение мониторинга SAP

Включите мониторинг SAP на виртуальной машине через Портал администратора.

Для этого выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите *Изменить*.

3. Перейдите на вкладку *Пользовательские параметры*.
4. Выберите sap_agent из раскрывающегося списка. Убедитесь, что для дополнительного раскрывающегося меню установлено значение True. Если были заданы предыдущие свойства, нажмите на значок плюса, чтобы добавить новое правило свойства, и выберите sap_agent.
5. Нажмите OK.

5.3.6 Управление синхронизацией виртуальной машины KVM

Виртуализация создает различные проблемы для учета рабочего времени виртуальных машин. Виртуальные машины, которые используют счетчик меток времени (TSC) в качестве источника синхронизации, могут иметь проблемы с синхронизацией, поскольку некоторые процессоры не имеют постоянного счетчика меток времени. Виртуальные машины, работающие без точного хронометража, могут серьезно повлиять на некоторые сетевые приложения, поскольку ваша виртуальная машина будет работать быстрее или медленнее, чем фактическое время.

KVM решает эту проблему, предоставляя виртуальным машинам паравиртуализированные часы. KVM pvclock обеспечивает стабильный источник синхронизации для поддерживающих его гостевых систем KVM. В настоящее время только виртуальные машины Enterprise Linux 5.4 и более поздних версий полностью поддерживают паравиртуализированные часы.

Виртуальные машины могут иметь несколько проблем, вызванных неточными часами и счетчиками:

- Часы могут не синхронизироваться с фактическим временем, что делает сеансы недействительными и влияет на сети.
- Виртуальные машины с более медленными часами могут иметь проблемы с переносом.

Эти проблемы существуют на других платформах виртуализации, и всегда следует проверять время.

Демон протокола сетевого времени (NTP) должен работать на узле и виртуальных машинах. Включите службу ntpd и добавьте ее в последовательность запуска по умолчанию:

- Для Enterprise Linux 6:

```
# service ntpd start
 # chkconfig ntpd on
```

- Для Enterprise Linux 7:

```
# systemctl start ntpd.service
 # systemctl enable ntpd.service
```

Использование службы ntpd должно минимизировать влияние рассогласования часов во всех случаях.

NTP-серверы, которые вы пытаетесь использовать, должны быть в рабочем состоянии и доступны для ваших узлов и виртуальных машин.

5.3.7 Определение того, имеет ли ваш ЦП постоянный счетчик отметок времени

Ваш ЦП имеет постоянный счетчик отметок времени, если установлен флаг constant_tsc. Чтобы определить, есть ли у вашего процессора флаг constant_tsc, выполните следующую команду:

$ cat /proc/cpuinfo | grep constant_tsc

Если какой-либо вывод задан, ваш процессор имеет constant_tsc бит. Если выходной сигнал не отображается, следуйте приведенным ниже инструкциям.

5.3.8 Настройка узлов без постоянного счетчика отметок времени

Системы без счетчиков постоянных отметок времени требуют дополнительной настройки. Функции управления питанием мешают точному отсчету времени и должны быть отключены, чтобы виртуальные машины точно отслеживали время с помощью KVM.
Примечание. Эти инструкции предназначены только для процессоров AMD версии F.

Если в ЦП отсутствует constant_tsc бит, отключите все функции управления питанием. Каждая система имеет несколько таймеров, которые используются для отсчета времени. TSC нестабилен на узле, что иногда вызвано изменениями cpufreq, состоянием глубокого сна C или миграцией на узел с более быстрым TSC. Состояния глубокого сна C могут остановить TSC. Чтобы предотвратить использование ядром состояний глубокого сна C, добавьте «processor.max_cstate = 1» к параметрам загрузки ядра в файле grub.conf на узле:

term Enterprise Linux Server (2.6.18-159.el5)
root (hd0,0)
kernel /vmlinuz-2.6.18-159.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet processor.max_cstate=1

Отключите cpufreq (необходимо только на узлах без constant_tsc) путем редактирования конфигурационного файла /etc/sysconfig/cpuspeed и измените переменные MIN_SPEED и MAX_SPEED на переменные с самой высокой доступной частотой. Действительные ограничения можно найти в файлах /sys/devices/system/cpu/cpu/cpufreq/ scaling_available_frequencies.

5.3.9 Использование инструмента engine-config для получения предупреждений, когда узлы не синхронизируются

Вы можете использовать инструмент engine-config для настройки предупреждений, когда ваши узлы не синхронизируются.

Для смещения времени на узлах есть 2 важных параметра: EnableHostTimeDrift и HostTimeDriftInSec. EnableHostTimeDrift, со значением false по умолчанию, может быть включен для получения предупреждений о сдвиге времени узла. Параметр HostTimeDriftInSec используется для установки максимально допустимого дрейфа, прежде чем начать оповещения об их отправке.

Оповещения отправляются один раз в час для каждого узла.

5.3.10 Добавление устройства с доверенным платформенным модулем

Устройства Trusted Platform Module (TPM) предоставляют безопасный криптопроцессор, предназначенный для выполнения криптографических операций, таких как генерация криптографических ключей, случайных чисел и хэшей, или для хранения данных, которые можно использовать для безопасной проверки конфигураций программного обеспечения. Устройства TPM обычно используются для шифрования дисков.

QEMU и libvirt реализуют поддержку эмулируемых устройств TPM 2.0, которые KeyVirt использует для добавления устройств TPM к виртуальным машинам.

После добавления эмулируемого устройства TPM в виртуальную машину его можно использовать как обычное устройство TPM 2.0 в гостевой ОС.

Примечание. Если для виртуальной машины хранятся данные TPM, а устройство TPM отключено в виртуальной машине, данные TPM удаляются без возможности восстановления.

5.3.10.1 Включение устройства TPM

1. На экране *Новая виртуальная машина* или *Изменить виртуальную машину* нажмите *Показать расширенные опции*.
2. На вкладке *Выделение ресурсов* установите флажок TPM Device Enabled.

Ограничения

Применяются следующие ограничения:

- Устройства TPM можно использовать только на компьютерах x86_64 с микропрограммой UEFI и на машинах PowerPC с установленной микропрограммой pSeries.
- Виртуальные машины с устройствами TPM не могут иметь моментальные снимки с памятью.
- Хотя Engine периодически извлекает и сохраняет данные TPM, нет гарантии, что Engine всегда будет иметь самую последнюю версию данных TPM.

Примечание. Этот процесс может занять 120 секунд или более, и вы должны дождаться его завершения, прежде чем сможете сделать моментальный снимок работающей виртуальной машины, клонировать работающую виртуальную машину или выполнить миграцию работающей виртуальной машины.

- Устройства TPM можно включить только для виртуальных машин под управлением RHEL 7 или более поздней версии и Windows 8.1 или более поздней версии.
- Виртуальные машины и шаблоны с данными TPM нельзя экспортировать или импортировать.

5.4 ИЗМЕНЕНИЕ ПАРАМЕТРОВ ВИРТУАЛЬНЫХ МАШИН

5.4.1 Сетевые интерфейсы

5.4.1.1 Добавление нового сетевого интерфейса

К виртуальным машинам можно добавить несколько сетевых интерфейсов. Это позволяет разместить вашу виртуальную машину в нескольких логических сетях.

Для добавления сетевых интерфейсов к виртуальным машинам выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Нажмите на вкладку *Сетевые интерфейсы*.
4. Нажмите *Новый*.
5. Введите имя сетевого интерфейса.
6. Выберите профиль и тип сетевого интерфейса из раскрывающихся списков. Выпадающие списки заполняются в соответствии с профилями и типами сетей, доступных для кластера и карты сетевого интерфейса, доступных для виртуальной машины.
7. Установите флажок Custom MAC address и введите требуемый MAC-адрес сетевой карты.
8. Нажмите OK.

Новый сетевой интерфейс указан на вкладке *Сетевые интерфейсы* в подробном представлении виртуальной машины. Когда сетевая карта определена на виртуальной машине и подключена к сети, для *Состояние соединения* по умолчанию установлено значение *Включено*.

5.4.1.2 Редактирование сетевого интерфейса

Чтобы изменить какие-либо сетевые настройки, вы должны отредактировать сетевой интерфейс. Эта процедура может выполняться на запущенных виртуальных машинах, но некоторые действия могут выполняться только на виртуальных машинах, которые не работают.

Для редактирования сетевых интерфейсов выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Нажмите на вкладку *Сетевые интерфейсы* и выберите сетевой интерфейс для редактирования.
4. Нажмите *Изменить*.
5. При необходимости измените настройки. Вы можете указать имя, профиль, тип и пользовательский MAC адрес.
6. Нажмите OK.

5.4.1.3 Подключение сетевого интерфейса на горячую

Сетевые интерфейсы можно устанавливать на горячую. Подключение на горячую означает включение и отключение устройств во время работы виртуальной машины.

Примечание. Гостевая операционная система должна поддерживать сетевые интерфейсы с заменой на горячую.

Для подключения сетевых интерфейсов на горячую выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Нажмите на вкладку *Сетевые интерфейсы* и выберите сетевой интерфейс для замены на горячую.
4. Нажмите *Изменить*.
5. Установите *Состояние карты* в *Подключён*, чтобы включить сетевой интерфейс, или установите его в *Не подключён*, чтобы отключить сетевой интерфейс.
6. Нажмите OK.

5.4.1.4 Удаление сетевого интерфейса

Для удаления сетевых интерфейсов выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Нажмите на вкладку *Сетевые интерфейсы* и выберите сетевой интерфейс, который нужно удалить.
4. Нажмите *Удалить*.
5. Нажмите OK.

5.4.1.5 Настройка виртуальной машины для игнорирования сетевых адаптеров

Вы можете настроить ovirt-guest-agent на виртуальной машине для игнорирования определенных сетевых адаптеров. Это предотвращает появление в отчетах IP-адресов, связанных с сетевыми интерфейсами, созданными определенным программным обеспечением. Необходимо указать имя и номер сетевого интерфейса, которые вы хотите внести в черный список (например, eth0, docker0).

Примечание. Перед первым запуском гостевого агента необходимо внести сетевые адаптеры в черный список на виртуальной машине.

Для внесения сетевых интерфейсов в черный список выполните следующие действия:

1. В файле конфигурации /etc/ovirt-guest-agent.conf на виртуальной машине вставьте следующую строку с игнорируемыми сетевыми адаптерами, разделенными пробелами:
   ignored_nics = first_NIC_to_ignore second_NIC_to_ignore
2. Запустите агент:
   systemctl start ovirt-guest-agent

Некоторые операционные системы виртуальных машин автоматически запускают гостевой агент во время установки.

Примечание. Если операционная система вашей виртуальной машины автоматически запускает гостевой агент или вам нужно настроить черный список на

многих виртуальных машинах, используйте настроенную виртуальную машину в качестве шаблона для создания дополнительных виртуальных машин.

5.4.2 Виртуальные диски

См. подробнее в разделе выше.

5.4.3 Виртуальная память

5.4.3.1 Подключение / изменение объема оперативной памяти на горячую

Вы можете подключить виртуальную память на горячую. Каждый раз, когда выполняется замена памяти на горячую, она отображается как новое устройство памяти на вкладке Устройства ВМ в подробном представлении виртуальной машины, максимум до 16 доступных слотов. Когда виртуальная машина перезапускается, эти устройства удаляются из вкладки VM Devices без уменьшения объема памяти виртуальной машины, что позволяет оперативно подключать больше устройств памяти. В случае сбоя замены на горячую (например, если больше нет доступных слотов), увеличение памяти будет применено при перезапуске виртуальной машины.
Примечание. Эта функция не поддерживается для виртуальной машины сервера управления средой виртуализации.

Для подключения виртуальной памяти на горячую выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите работающую виртуальную машину.
2. Нажмите *Изменить*.
3. Перейдите на вкладку *Система*.
4. Увеличьте *Размер памяти*, указав общий требуемый объем. Объем памяти должен быть кратен 256 МБ. По умолчанию максимальный объем памяти, разрешенный для виртуальной машины, установлен в 4 раза больше указанного размера памяти. Хотя значение изменяется в пользовательском интерфейсе, максимальное значение на горячую не устанавливается, и вы увидите значок ожидающих изменений. Чтобы этого избежать, вы можете вернуть максимальный объем памяти к исходному значению.
5. Нажмите OK. Это действие открывает окно Pending Virtual Machine changes, так как некоторые значения, такие как maxMemorySizeMb и minAllocatedMem не изменятся, пока виртуальная машина не будет перезапущена. Однако действие замены на горячую запускается изменением значения *Размер памяти*, которое можно применить немедленно.
6. Нажмите OK.

Объявленная память виртуальной машины обновляется на вкладке *Общее* в представлении сведений. Вы можете увидеть недавно добавленное устройство памяти на вкладке VM Devices в подробном просмотре.

5.4.3.2 Отключение виртуальной памяти на горячую

Вы можете отключить виртуальную память на горячую. Отключение на горячую означает отключение устройств во время работы виртуальной машины.

- Только память, добавленная с помощью подключения на горячую, может быть отключена на горячую.
- Операционная система виртуальной машины должна поддерживать отключение памяти на горячую.
- На виртуальных машинах не должно быть включено устройство всплывающего окна памяти. По умолчанию эта функция отключена.
- Все блоки оперативной памяти должны иметь значение online_movable в правилах управления устройствами виртуальной машины.

Если какое-либо из этих условий не выполняется, операция отключения памяти на горячую может завершиться ошибкой или вызвать непредвиденное поведение.

Для отключения виртуальной памяти на горячую выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите работающую виртуальную машину.
2. Нажмите на вкладку *Устройства ВМ*.
3. В столбце Отключение на Горячую нажмите Отключение на Горячую рядом с устройством памяти, которое нужно удалить.
4. Нажмите кнопку OK в окне *Горячее отсоединение памяти*.

При необходимости значение Гарантированное ОЗУ для виртуальной машины уменьшается автоматически.

5.4.4 Подключение виртуальных ЦП на горячую

Вы можете подключать виртуальные ЦП на горячую. Подключение на горячую означает включение или отключение устройств во время работы виртуальной машины.

Отключение виртуального ЦП на горячую поддерживается только в том случае, если виртуальный ЦП ранее был подключен на горячую. Виртуальные ЦП виртуальной машины не могут быть оперативно отключены от меньшего количества виртуальных ЦП, чем было изначально создано.

Применяются следующие предварительные условия:

- Операционная система виртуальной машины должна быть явно установлена в окне *Новая виртуальная машина* или *Изменить виртуальную машину*.
- Операционная система виртуальной машины должна поддерживать подключение ЦП на горячую.
- На виртуальных машинах Windows должны быть установлены гостевые агенты.

Подключение виртуальных ЦП на горячую:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите работающую виртуальную машину.
2. Нажмите *Изменить*.
3. Перейдите на вкладку *Система*.
4. При необходимости измените значение *Виртуальные сокеты*.
5. Нажмите OK.

5.4.5 Прикрепление виртуальной машины к нескольким узлам

Виртуальные машины можно привязать к нескольким узлам. Привязка нескольких узлов позволяет виртуальной машине работать на определенном подмножестве узлов в кластере, а не на одном конкретном узле или на всех узлах в кластере. Виртуальная машина не может работать на других узлах в кластере, даже если все указанные узлы недоступны. Привязка нескольких узлов может использоваться для ограничения виртуальных машин узлами, например, с одинаковой физической конфигурацией оборудования.

В случае сбоя узла высокодоступная виртуальная машина автоматически перезапускается на одном из других узлов, к которому эта виртуальная машина прикреплена.

Для привязки виртуальной машины к нескольким узлам выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите *Изменить*.
3. Перейдите на вкладку *Узел*.
4. Выберите переключатель *Указанные узлы* в разделе *Запускается на* и выберите два или более узла из списка.
5. Перейдите на вкладку *Высокая доступность*.
6. Установите флажок *Высокая доступность*.
7. В раскрывающемся списке Priority выберите *Низкий*, *Средний*, или *Высокий*. Когда запускается миграция, создается очередь, в которой сначала переносятся виртуальные машины с высоким приоритетом. Если в кластере не хватает ресурсов, переносятся только виртуальные машины с высоким приоритетом.
8. Нажмите OK.

5.4.6 Просмотр виртуальных машин, закрепленных на узле

Вы можете просматривать виртуальные машины, прикрепленные к узлу, даже когда виртуальные машины отключены. Используйте список *Закреплен за текущим узлом*, чтобы увидеть, какие виртуальные машины будут затронуты и какие виртуальные машины потребуют перезапуска вручную после того, как узел снова станет активным.

Для просмотра виртуальных машин, закрепленных на узле, выполните следующие действия:

1. Нажмите *Виртуализация* > *Узлы*.
2. Нажмите на имя узла, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку *Виртуальные машины*.
4. Нажмите *Закреплен за текущим узлом*.

5.4.7 Смена компакт-диска на виртуальной машине

Вы можете изменить компакт-диск, доступный для виртуальной машины во время ее работы, используя образы ISO, которые были загружены в домен данных кластера виртуальной машины.

Для смены компакт-диска на виртуальной машине выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите работающую виртуальную машину.
2. Нажмите (⋮) *Контекстное Меню*, затем нажмите *Сменить CD*.
3. Выберите вариант из раскрывающегося списка:
    - Выберите файл ISO из списка, чтобы извлечь компакт-диск, который в настоящее время доступен виртуальной машине, и смонтировать этот файл ISO как компакт-диск.
    - Выберите *[Извлечь]* из списка, чтобы извлечь компакт-диск, который в данный момент доступен виртуальной машине.
4. Нажмите OK.

5.4.8 Проверка подлинности смарт-карты

Смарт-карты – это внешняя аппаратная функция безопасности, наиболее часто встречающаяся в кредитных картах, но также используемая многими предприятиями в качестве токенов аутентификации. Смарт-карты можно использовать для защиты виртуальных машин KeyVirt.

Для включения смарт-карты выполните следующие действия:

1. Убедитесь, что оборудование смарт-карты подключено к клиентскому компьютеру и установлено в соответствии с инструкциями производителя.
2. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
3. Нажмите *Изменить*.
4. Нажмите на вкладку *Консоль* и установите флажок *Смарт карты включены*.
5. Нажмите OK.
6. Подключитесь к работающей виртуальной машине, нажав кнопку *Консоль*. Теперь проверка подлинности смарт-карты передается с клиентского оборудования на виртуальную машину.

Примечание. Если оборудование смарт-карты установлено неправильно, включение функции смарт-карты приведет к тому, что виртуальная машина не загрузится должным образом.

5.4.8.1 Настройка клиентских систем для совместного использования смарт-карт

- Смарт-карты могут потребовать определенные библиотеки для доступа к своим сертификатам. Эти библиотеки должны быть видимы для библиотеки NSS, которая spice-gtk использует смарт-карту для гостя. NSS ожидает, что библиотеки предоставят интерфейс PKCS #11.

- Убедитесь, что архитектура модуля соответствует архитектуре spice-gtk / remote-viewer. Например, если у вас есть только 32-битная библиотека PKCS #11, вы должны установить 32-битную сборку virt-viewer, чтобы смарт-карты работали.

Вы можете настроить виртуальную машину на высокую производительность, чтобы она работала с показателями производительности, максимально приближенными к обычному железу. Когда вы выбираете оптимизацию высокой производительности, виртуальная машина настраивается с набором автоматических и рекомендованных ручных настроек для максимальной эффективности.

Внимание! Параметр высокой производительности доступен только на Портале администратора при выборе параметра *Высокая производительность* в раскрывающемся списке *Оптимизировано для* в окне *Изменить* или *Новый* для виртуальных машин, шаблонов и пулов. Этот параметр недоступен на Портале виртуальных машин.

5.5 СНИМКИ

5.5.1 Создание снимка виртуальной машины

Моментальный снимок – это представление операционной системы и приложений виртуальной машины на любом или всех доступных дисках в определенный момент времени. Сделайте снимок виртуальной машины, прежде чем вносить в нее изменения, которые могут иметь непредвиденные последствия. Вы можете использовать снимок, чтобы вернуть виртуальную машину в предыдущее состояние.

Для создания снимка на Портале администратора выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Нажмите на вкладку *Снимки* и нажмите *Создать*.
4. Введите описание снимка.
5. Выберите *Диски для включения*, используя флажки. Если диски не выбраны, создается частичный снимок виртуальной машины без диска. Вы можете предварительно просмотреть этот снимок, чтобы просмотреть конфигурацию виртуальной машины. Обратите внимание, что фиксация частичного моментального снимка приведет к тому, что виртуальная машина останется без диска.
6. Выберите *Сохранить ОЗУ*, чтобы включить в снимок память работающей виртуальной машины.
7. Нажмите OK.

Операционная система и приложения виртуальной машины на выбранном диске хранятся в моментальном снимке, который можно просмотреть или восстановить. Снимок создается со статусом *Заблокирован*, который меняется на Ok. Когда вы выберите снимок, его подробности отображаются в раскрывающихся списках *Общее*, *Диски*, *Сетевые интерфейсы* и *Установленные приложения* на вкладке *Снимки*.

5.5.2 Использование снимка для восстановления виртуальной машины

Снимок можно использовать для восстановления виртуальной машины до ее предыдущего состояния. Восстановление виртуальной машины из снимка должно производиться на выключенной виртуальной машине.

Выполните следующие действия на Портале администратора:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Нажмите на вкладку *Снимки*, чтобы просмотреть список доступных снимков.
4. Выберите снимок для восстановления на верхней панели. Подробные сведения о снимке отображаются на нижней панели.
5. Нажмите кнопку раскрывающегося меню *Предпросмотр* и выберите Пользовательский.
6. Установите флажки, чтобы выбрать VM Configuration, Memory и диски, которые вы хотите восстановить, затем нажмите OK. Это позволяет создавать и восстанавливать из настроенного моментального снимка, используя конфигурацию и диски из нескольких снимков. Статус снимка изменится на Preview Mode. Состояние виртуальной машины ненадолго изменится на *Образ заблокирован*, прежде чем вернуться в Down.
7. Запустите виртуальную машину; она запускается с использованием образа диска моментального снимка.
8. Нажмите Commit, чтобы навсегда восстановить виртуальную машину до состояния моментального снимка. Все последующие снимки стираются. Либо нажмите кнопку Undo, чтобы деактивировать моментальный снимок и вернуть виртуальную машину в предыдущее состояние.

5.5.3 Создание виртуальной машины из снимка

Вы можете использовать моментальный снимок для создания новой виртуальной машины. Для создания виртуальной машины из снимка выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Нажмите на вкладку *Снимки*, чтобы просмотреть список доступных снимков.
4. Выберите снимок в отображаемом списке и нажмите *Клонировать*.
5. Введите имя виртуальной машины.
6. Нажмите OK.

Через некоторое время клонированная виртуальная машина появится на вкладке *Виртуальные машины* в панели навигации со статусом *Образ заблокирован*. Виртуальная машина остается в этом состоянии до тех пор, пока KeyVirt не завершит создание виртуальной машины. Для создания виртуальной машины с предварительно выделенным жестким диском объемом 20 ГБ требуется около пятнадцати минут. Когда виртуальная машина готова к использованию, ее статус

меняется с *Образ заблокирован* на *Выключено* в *Виртуализация* > *Виртуальные машины*.

5.5.4 Удаление снимка

Вы можете удалить моментальный снимок виртуальной машины и навсегда удалить его из среды KeyVirt.

Для удаления снимка на Портале администратора:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Нажмите на вкладку *Снимки*, чтобы просмотреть снимки для этой виртуальной машины.
4. Выберите снимок, который нужно удалить.
5. Нажмите *Удалить*.
6. Нажмите OK.

Примечание. Если удаление не удалось, устраните основную проблему (например, отказавший узел, недоступное запоминающее устройство или даже временную проблему с сетью) и повторите попытку.

5.6 ХОСТ-УСТРОЙСТВА

Чтобы повысить производительность, вы можете подключить хост-устройство к виртуальной машине. Хост-устройства – это физические устройства, подключенные к определенному хост-компьютеру, например:

- Ленточные накопители, диски и чейнджеры SCSI;
- Сетевые карты PCI, графические процессоры и HBA;
- USB-мыши, камеры и диски.

Чтобы добавить хост-устройство к виртуальной машине, используйте свойства *Устройства узла* (Host Devices) виртуальной машины. Сначала выберите один из узлов кластера и тип устройства. Затем выберите и подключите одно или несколько хост-устройств к этому узлу.

Примечание. При изменении параметра Pinned Host текущие хост-устройства удаляются. Когда вы сохраняете эти изменения, в настройках узла виртуальной машины для параметра *Запускается на* (Start Running On) задается значение *Указанные узлы* и указывается узел, который вы выбрали ранее с помощью параметра Pinned Host.

Когда вы завершите подключение одного или нескольких хост-устройств, запустите виртуальную машину, чтобы применить изменения. Виртуальная машина запускается на узле, к которому подключены хост-устройства. Если виртуальная машина не может запуститься на указанном узле или получить доступ к хост-устройству, она отменяет операцию запуска и выдает сообщение об ошибке с информацией о причине.

Требования:

- Состояние узла Up.

- Хост настроен для прямого назначения устройств.

5.6.1 Добавление хост-устройства к виртуальной машине

1. На Портале администратора нажмите *Виртуализация* > *Виртуальные машины*.
2. Выключите виртуальную машину.
3. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
4. Перейдите на вкладку *Устройства узла*.
5. Нажмите Add Device. Откроется панель Add Host Devices.
6. Используйте Pinned Host, чтобы выбрать узел, на котором работает виртуальная машина.
7. Используйте Capability к списку устройств pci, scsi или usb_device.
8. Используйте Available Host Devices для выбора устройств.
9. Нажмите стрелку вниз, чтобы переместить устройства на Host Devices to be attached.
10. Нажмите OK, чтобы подключить эти устройства к виртуальной машине и закрыть окно.
11. При необходимости, если вы подключаете хост-устройство SCSI, настройте оптимальный драйвер.

    1. Нажмите кнопку *Изменить*. Откроется панель *Изменить виртуальную машину*.
    2. Перейдите на вкладку *Пользовательские параметры*.
    3. Нажмите *Выберите ключ* и выберите scsi_hostdev в нижней части раскрывающегося списка.
    4. В большинстве случаев выбирайте scsi-hd. В противном случае для ленточных устройств или устройств смены компакт-дисков выберите параметр scsi_generic.
    5. Нажмите кнопку OK.

12. Запустите виртуальную машину.
13. Во время запуска виртуальной машины следите за сообщениями об ошибках Operation Canceled.

5.6.2 Прикрепление виртуальной машины к другому узлу

Вы можете использовать вкладку *Устройства узла* для подробного представления виртуальных машин, чтобы привязать ее к определенному узлу. Если к виртуальной машине подключены какие-либо хост-устройства, привязка ее к другому узлу автоматически удаляет хост-устройства из виртуальной машины.

Для прикрепления виртуальной машины к узлу выполните следующие действия:

1. Нажмите на имя виртуальной машины и перейдите на вкладку *Устройства узла*.
2. Нажмите Pin to another host. Откроется окно Pin VM to Host.
3. Используйте раскрывающееся меню Host, чтобы выбрать узел.
4. Нажмите OK, чтобы закрепить виртуальную машину на выбранном узле.

5.7 AFFINITY-ГРУППЫ

Группы соответсвия (affinity-группы) помогают определить, где работают выбранные виртуальные машины по отношению друг к другу и указанным узлам. Эта возможность помогает управлять сценариями рабочих нагрузок, такими как лицензионные требования, рабочие нагрузки с высокой доступностью и аварийное восстановление.

Правило соответсвия виртуальных машин

При создании группы соответсвия вы выбираете виртуальные машины, которые принадлежат к этой группе. Для того, чтобы определить, где эти виртуальные машины могут работать по отношению друг к другу, включите VM Affinity Rule (Правило соответствия виртуальной машины): правило положительного соответсвияа пытается запустить виртуальные машины вместе на одном узле; а правило отрицательного соответсвияа пытается запустить виртуальные машины на отдельных узлах. Если правило не может быть выполнено, результат зависит от того, включен ли модуль взвешивания или фильтра.

Правило соответсвия узлов

При желании вы можете добавить узлы в группы соответсвия. Для того, чтобы определить, где виртуальные машины в группе могут работать по отношению к узлам в группе, включите Host Affinity Rule. Положительное правило пытается запустить виртуальные машины на узлах в группе сродства; правило отрицательного соответсвияа пытается запустить виртуальные машины на узлах, не входящих в группу соответсвияа. Если правило не может быть выполнено, результат зависит от того, включен ли модуль веса или фильтра.

Модуль взвешивания по умолчанию

По умолчанию оба правила (правило соответсвия ВМ и правило соответсвия узлов) применяют модуль оценки в политике планирования кластера. С модулем оценки планировщик пытается выполнить правило, но позволяет виртуальным машинам в группе соответсвия работать в любом случае, если правило не может быть выполнено. Например, с положительным VM Affinity Rule и включенным модулем оценки планировщик пытается запустить все виртуальные машины группы сопоставления на одном узле. Однако, если на одном узле недостаточно ресурсов для этого, планировщик запускает виртуальные машины на нескольких узлах.

Для этого модуля к работе, секция политики планирования weight module должна содержать ключевые слова VmAffinityGroups и VmToHostsAffinity Groups.

Опция принудительного исполнения и модуль фильтра

Оба правила (правило соответсвия ВМ и правило соответсвия узлов) имеют параметр Enforcing, который применяет модуль фильтра в политике планирования кластера. Модуль фильтра имеет приоритет над модулем оценки. При включенном модуле фильтра планировщик требует выполнения правила. Если правило не может быть выполнено, модуль фильтра предотвращает запуск виртуальных машин в группе соответсвия.

Например, если включены Host Affinity Rule и Enforcing (включен модуль фильтрации), планировщик требует, чтобы виртуальные машины группы

сопоставления работали на узлах, которые являются частью группы соответсвия. А если эти узлы не работают, планировщик вообще не запускает виртуальные машины.

Чтобы модуль работал, секция политики планирования filter module должна содержать ключевые слова VmAffinityGroups и VmToHostsAffinity Groups.

5.7.1 Создание группы соответсвия (Affinity)

Вы можете создавать новые группы соответсвия на Портале администратора. Выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку Группы Соответсвия.
4. Нажмите *Новая*.
5. Введите имя и описание для группы соответсвия.
6. В раскрывающемся списке *Правило соответствия виртуальной машины* выберите *Положительная*, чтобы применить положительное соответствие, или Отрицательная, чтобы применить отрицательное соответствие. Выберите *Отключено*, чтобы отключить правило соответсвия.
7. Выберите флажок *Принудительно*, чтобы применить жесткое исполнение (hard enforcement), или не выбирайте, чтобы применить мягкое исполнение (soft enforcement).
8. Используйте раскрывающийся список, чтобы выбрать виртуальные машины, которые будут добавлены в группу соответсвия. Используйте кнопки «+» и «–» для добавления или удаления дополнительных виртуальных машин.
9. Нажмите OK.

5.7.2 Редактирование группы соответсвия (Affinity)

Для редактирования групп соответсвия выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку Группы Соответсвия.
4. Нажмите *Изменить*.
5. Измените раскрывающееся меню *Правило соответствия виртуальной машины* и установите флажок *Принудительно* на предпочтительные значения и используйте кнопки «+» и «–» для добавления или удаления виртуальных машин в группу сопоставления или из нее.
6. Нажмите OK.

5.7.3 Удаление группы соответсвия (Affinity)

Для удаления группы соответсвия выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите на имя виртуальной машины, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку Группы Соответсвия.
4. Нажмите *Удалить*.
5. Нажмите OK.

Политика соответсвия, применявшаяся к виртуальным машинам, входившим в эту группу соответсвия, больше не применяется.

- **Примечание**. Чтобы метки соответсвия работали, раздел модуля фильтра политик планирования должен содержать файлы Label.
- Если группа соответсвия и метка соответсвия конфликтуют друг с другом, затронутые виртуальные машины не запускаются.

Каждое правило зависит от веса и модулей фильтрации в политике планирования кластера.

- **Внимание**! Чтобы правило сопоставления виртуальных машин работало, политика планирования должна иметь ключевое слово VmAffinityGroups в разделах Weight module и Filter module.
- Чтобы правило соответсвия узлов работало, политика планирования должна содержать ключевое слово VmToHostsAffinityGroups в разделах Weight module и Filter module.

Группы соответсвия применяются к виртуальным машинам в кластере.

При перемещении виртуальной машины из одного кластера в другой она удаляется из групп соответсвия в исходном кластере.

Виртуальные машины не нужно перезапускать, чтобы правила группы соответсвия вступили в силу.

5.7.4 Устранение неполадок в группах соответсвия (Affinity)

Чтобы предотвратить проблемы с группами соответсвия:

- Планируйте и документируйте сценарии и ожидаемые результаты при использовании группы соответсвия.
- Проверяйте и тестируйте результаты в различных условиях.
- Следуйте рекомендациям по управлению изменениями.
- Используйте параметр Enforcing, только если он необходим.

Если вы наблюдаете проблемы с неработающими виртуальными машинами:

- Убедитесь, что кластер имеет политику планирования, чей модуль оценки и модуль фильтра содержат VmAffinityGroups и VmToHostsAffinityGroups.
- Проверьте наличие конфликтов между метками соответсвия и группами соответсвия.

Возможные конфликты между метками соответсвия и группами соответсвия:

- Помните, что метка соответсвия является эквивалентом группы соответсвия с Host affinity rule, который отмечен как Positive со включенной опцией Enforcing.
- Помните, что, если метка соответсвия и группа соответсвия конфликтуют друг с другом, пересекающийся набор виртуальных машин не запустится.
- Определите, возможен ли конфликт:
  - Осмотрите раздел модуля фильтра политик планирования кластера. Они должны содержать как ключевое слово Label, так и ключевое слово VmAffinityGroups или VmToHostsAffinityGroups. В противном случае конфликт невозможен (наличие VmAffinityGroups и VmToHostsAffinityGroups в разделе модуля оценки не имеет значения, потому что Label в разделе модуля фильтра будут отменены).
  - Изучите группы соответсвия. Они должны содержать правило, для которого включена опция Enforcing. В противном случае конфликт невозможен.
- Если возможен конфликт, определите набор виртуальных машин, которые могут быть задействованы:
  - Изучите метки соответсвия и группы соответсвия. Составьте список виртуальных машин, которые являются членами как метки соответсвия и группы соответсвия с включенной опцией Enforcing.
  - Для каждого узла и виртуальной машины в этом пересекающемся наборе проанализируйте условия, при которых возникает потенциальный конфликт.
- Определите, соответствуют ли фактически неработающие виртуальные машины виртуальным машинам, указанным в анализе.
- Наконец, реструктурируйте группы соответсвия и метки соответсвия, чтобы избежать непреднамеренных конфликтов.
- Убедитесь, что любые изменения приводят к ожидаемым результатам при различных условиях.

5.8 AFFINITY-МЕТКИ

На Портале администратора можно создавать и изменять метки соответсвия (affinity-метки). Метки соответсвия используются вместе с группами соответсвия для установки любого вида соответсвия между виртуальными машинами и узлами (жесткого, мягкого, положительного, отрицательного). Метки соответсвия можно создавать и редактировать в представлении сведений о виртуальной машине, узле или кластере. См. раздел *Affinity-группы* для получения дополнительной информации о жесткости и полярности соответсвия.

Примечание. Метки соответсвия являются подмножеством групп соответсвия и могут конфликтовать с ними. В случае конфликта виртуальная машина не запустится.

5.8.1 Создание метки соответсвия (Affinity)

Для создания метки соответсвия выполните следующие действия:

1. Нажмите *Виртуализация* > *Кластеры* и выберите соответствующий кластер.

2. Нажмите на имя кластера, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку *Приоритеты*.
4. Нажмите *Новый*.
5. Введите имя метки соответсвия.
6. Используйте раскрывающиеся списки, чтобы выбрать виртуальные машины и узлы, которые будут связаны с меткой. Используйте кнопку «+», чтобы добавить дополнительные виртуальные машины и узлы.
7. Нажмите OK.

5.8.2 Редактирование метки соответсвия (Affinity)

Для редактирования метки соответсвия выполните следующие действия:

1. Нажмите *Виртуализация* > *Кластеры* и выберите соответствующий кластер.
2. Нажмите на имя кластера, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку *Приоритеты*.
4. Выберите метку, которую хотите отредактировать.
5. Нажмите *Изменить*.
6. Используйте кнопки «+» и «–» для добавления или удаления виртуальных машин и узлов из метки соответсвия или из нее.
7. Нажмите OK.

5.8.3 Удаление метки соответсвия (Affinity)

Для удаления метки соответсвия выполните следующие действия:

1. Нажмите *Виртуализация* > *Кластеры* и выберите соответствующий кластер.
2. Нажмите на имя кластера, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку *Приоритеты*.
4. Выберите ярлык, который хотите удалить.
5. Нажмите *Изменить*.
6. Используйте кнопки «–», чтобы удалить все виртуальные машины и узлы с метки.
7. Нажмите OK.
8. Нажмите *Удалить*.
9. Нажмите OK.

5.9 ЭКСПОРТ И ИМПОРТ ВИРТУАЛЬНЫХ МАШИН И ШАБЛОНОВ

Вы можете экспортировать виртуальные машины и шаблоны из центров обработки данных и импортировать их в ту же или другую среду KeyVirt. Вы можете экспортировать или импортировать виртуальные машины с помощью домена экспорта, домена данных или с помощью узла виртуализации. Когда вы экспортируете или импортируете виртуальную машину или шаблон, сохраняются свойства, включая основные сведения, такие как имя и описание, выделение ресурсов и параметры высокой доступности этой виртуальной машины или шаблона.

Разрешения и роли пользователей виртуальных машин и шаблонов включены в файлы OVF, поэтому, когда домен хранения отсоединяется от одного центра обработки данных и присоединяется к другому, виртуальные машины и шаблоны могут быть импортированы с их исходными разрешениями и ролями пользователей. Для успешной регистрации разрешений пользователя и роля, связанные с разрешениями виртуальных машин или шаблонов, должны существовать в центре обработки данных до процесса регистрации.

Вы также можете использовать функцию V2V для импорта виртуальных машин от других провайдеров виртуализации, таких как VMware, или для импорта виртуальных машин Windows. V2V преобразует виртуальные машины, чтобы их можно было разместить в KeyVirt.

5.9.1 Экспорт виртуальной машины в домен экспорта

Экспортируйте виртуальную машину в экспортный домен, чтобы ее можно было импортировать в другой центр обработки данных. Перед тем, как начать, экспортный домен необходимо подключить к центру обработки данных, в котором находится виртуальная машина, которую нужно экспортировать.

Примечание. Перед экспортом или импортом виртуальные машины необходимо выключить**.**

Для экспорта виртуальной машины в домен экспорта выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите (⁝) *Контекстное Меню*, затем нажмите *Экспорт в Домен экспорта*.
3. При желании установите следующие флажки в окне *Экспортировать виртуальную машину*:

    - *Перезаписать принудительно*: отменяет существующие образы виртуальной машины в экспортном домене.
    - *Консолидировать Снимки*: создает один экспортный том на диск. Этот параметр удаляет точки восстановления моментальных снимков и включает шаблон в виртуальную машину на основе шаблона, а также удаляет все зависимости виртуальной машины от шаблона. Для виртуальной машины, зависящей от шаблона, выберите этот параметр, экспортируйте шаблон вместе с виртуальной машиной или убедитесь, что шаблон существует в целевом центре обработки данных.

Когда вы создаете виртуальную машину из шаблона, нажимая *Виртуализация* > *Шаблоны* и выбрав *Новая ВМ*, вы увидите два варианта выделения памяти в разделе *Выделение хранилища* на вкладке *Выделение ресурсов*:

- Если выбрано *Клонирование* (Clone), виртуальная машина не зависит от шаблона. Шаблон не обязательно должен существовать в целевом центре обработки данных.
- Если выбран вариант *Тонкий* (Thin), виртуальная машина зависит от шаблона, поэтому шаблон должен существовать в целевом центре обработки данных или экспортироваться вместе с виртуальной

машиной. Или установите флажок *Консолидировать Снимки*, чтобы свернуть диск-шаблон и виртуальный диск в один диск. Чтобы проверить, какой вариант был выбран, нажмите на имя виртуальной машины и перейдите на вкладку *Общее* в окне сведений.

4. Нажмите OK.

Начнется экспорт виртуальной машины. Виртуальная машина отобразится в *Виртуализация* > *Виртуальные машины* со статусом *Образ заблокирован* во время экспорта. В зависимости от размера образов жестких дисков вашей виртуальной машины и оборудования хранения это может занять до часа. Перейдите на вкладку *События*, чтобы просмотреть прогресс. По завершении виртуальная машина была экспортирована в домен экспорта и отображается на вкладке *Импорт виртуальной машины* в представлении сведений о домене экспорта.

5.9.2 Экспорт виртуальной машины в домен данных

Вы можете экспортировать виртуальную машину в домен данных, чтобы сохранить клон виртуальной машины в качестве резервной копии. При экспорте виртуальной машины, зависящей от шаблона, целевой домен хранения должен включать этот шаблон. Когда вы создаете виртуальную машину из шаблона, вы можете выбрать один из двух вариантов выделения хранилища:

- Клонирование (Clone): Виртуальная машина не зависит от шаблона. Шаблон не обязательно должен существовать в целевом домене хранения.
- Тонкий (Thin): виртуальная машина зависит от шаблона, поэтому шаблон должен существовать в целевом домене хранения.

Чтобы проверить, какой параметр выбран, нажмите на имя виртуальной машины и нажмите на вкладку *Общее* в представлении сведений.

Требования:

- Домен данных должен быть прикреплен к центру обработки данных.
- ВМ выключена.

Процедура:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите *Экспорт*.
3. Придумайте имя экспортируемой виртуальной машине.
4. Выберите домен данных из списка *Домен хранения*.
5. Дополнительно нажмите *Консолидировать Снимки*, чтобы хоэкспортировать виртуальную машину без снимков.
6. Нажмите OK.

Диски перенесены в новый домен.

Примечание. Когда вы перемещаете диск из одного типа домена данных в другой, формат диска изменяется соответственно. Например, если диск находится в домене данных NFS и имеет разреженный формат, то, если вы переместите диск в домен

iSCSI, его формат изменится на предварительно выделенный. Это отличается от использования экспортного домена, потому что экспортный домен – это NFS.

Во время экспорта виртуальная машина отображается со статусом *Образ заблокирован*. В зависимости от размера образов жестких дисков вашей виртуальной машины и вашего оборудования для хранения это может занять до часа. Выберите вкладку *События*, чтобы просмотреть ход выполнения. По завершении виртуальная машина будет экспортирована в домен данных и появится в списке виртуальных машин.

5.9.3 Импорт виртуальной машины из домена экспорта

У вас есть виртуальная машина в экспортном домене. Прежде чем виртуальную машину можно будет импортировать в новый центр обработки данных, экспортный домен должен быть присоединен к целевому центру обработки данных. Для импорта виртуальной машины в необходимый центр обработки данных выполните следующие действия:

1. Нажмите *Хранилище* > *Домены* и выберите экспортный домен. Экспортный домен должен иметь статус *Активный*.
2. Нажмите на имя экспортного домена, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку *Импорт виртуальной машины*, чтобы отобразить доступные виртуальные машины для импорта.
4. Выберите одну или несколько виртуальных машин для импорта и нажмите *Импортировать*.
5. Выберите *Кластер назначения*.
6. Установите флажок *Консолидировать Снимки*, чтобы удалить точки восстановления снимков.
7. Нажмите на виртуальную машину, которую нужно импортировать, и перейдите на дополнительную вкладку Диски. На этой вкладке вы можете использовать раскрывающиеся списки *Политика выделения* и *Домен хранения*, чтобы выбрать, будет ли диск, используемый виртуальной машиной, тонко выделенным или предварительно выделенным, а также можно выбрать домен хранения, на котором будет храниться диск. Также отображается значок, указывающий, какой из дисков, которые нужно импортировать, действует как загрузочный диск для этой виртуальной машины.
8. Нажмите OK, чтобы импортировать виртуальные машины. Окно *Импорт конфликтующих виртуальных машин* открывается, если виртуальная машина существует в виртуализированной среде. Выберите один из следующих переключателей:

    - Не импортирвать
    - Импортировать как клон – введите уникальное имя виртуальной машины в поле *Новое имя*

9. При необходимости установите флажок *Применить ко всем*, чтобы импортировать все дублированные виртуальные машины с одинаковым суффиксом, а затем введите суффикс в поле *Суффикс для добавления к клонируемым ВМ*.

10. Нажмите OK.

Во время одной операции импорта вы можете импортировать только виртуальные машины с одинаковой архитектурой. Если какая-либо из импортируемых виртуальных машин имеет архитектуру, отличную от архитектуры других импортируемых виртуальных машин, отобразится предупреждение, и вам будет предложено изменить свой выбор, чтобы импортировались только виртуальные машины с такой же архитектурой.

5.9.4 Импорт виртуальной машины из домена данных

Вы можете импортировать виртуальную машину в один или несколько кластеров из домена хранилища данных.

Требования:

- Если вы импортируете виртуальную машину из импортированного домена хранения данных, импортированный домен хранения должен быть подключен к центру обработки данных и активирован.

Процедура импорта:

1. Нажмите *Хранилище* > *Домены*.
2. Нажмите на имя импортированного домена хранения. Откроется представление сведений.
3. Перейдите на вкладку *Импорт виртуальной машины*.
4. Выберите одну или несколько виртуальных машин для импорта.
5. Нажмите *Импортировать*.
6. Для каждой виртуальной машины в окне *Импорт виртуальных(ой) машин(ы)* убедитесь, что в списке *Кластер* выбран правильный целевой кластер.
7. Сопоставьте профили vNIC внешней виртуальной машины с профилями, присутствующими в целевом кластере (кластерах):

1. Нажмите *Отображение внешних профилей vNIC*.
2. Выберите профиль vNIC для использования в раскрывающемся списке *Целевой профиль vNIC*.
3. Если в окне *Импорт виртуальных(ой) машин(ы)* выбрано несколько целевых кластеров, выберите каждый целевой кластер в раскрывающемся списке *Кластер назначения* и убедитесь, что сопоставления верны.
4. Нажмите OK.

8. При обнаружении конфликта MAC-адресов рядом с именем виртуальной машины появляется восклицательный знак. Наведите указатель мыши на значок, чтобы просмотреть всплывающую подсказку, отображающую тип возникшей ошибки.

Установите флажок *Переопределить плохие MACs*, чтобы переназначить новые MAC-адреса всем проблемным виртуальным машинам. Кроме того, вы можете установить флажок *Переопределить* для каждой виртуальной машины.

Примечание. Если нет доступных адресов для назначения, операция импорта завершится ошибкой. Однако в случае MAC-адресов, которые находятся за

пределами диапазона пула MAC-адресов кластера, можно импортировать виртуальную машину без переназначения нового MAC-адреса.

9. Нажмите OK.

Импортированные виртуальные машины больше не отображаются в списке на вкладке *Импорт виртуальной машины*.

5.9.5 Импорт виртуальной машины от провайдера VMware

Импортируйте виртуальные машины от провайдера VMware vCenter в вашу среду KeyVirt. Вы можете импортировать от провайдера, вводя его данные в окне *Импорт виртуальных(ой) машин(ы)* во время каждой операции импорта, или вы можете добавить провайдера VMware в качестве внешнего провайдера и выбрать предварительно настроенного провайдера во время операций импорта.

KeyVirt использует V2V для импорта виртуальных машин VMware. Для файлов OVA единственным форматом диска, поддерживаемым KeyVirt, является VMDK.

Примечание. Пакет virt-v2v недоступен для архитектуры ppc64le, и эти узлы нельзя использовать в качестве прокси-хостов.
В случае сбоя импорта обратитесь к соответствующему файлу журнала /var/log/vdsm/import/ и /var/log/vdsm/vdsm.log на прокси-сервер для получения подробной информации.

Требования:

- Пакет virt-v2v должен быть установлен по крайней мере на одном узле, который в этой процедуре называется прокси-хостом. Пакет virt-v2v доступен по умолчанию на узлах KeyVirt и устанавливается на узлах Enterprise Linux в качестве зависимости от VDSM при добавлении в среду KeyVirt.
- Хосты Enterprise Linux должны быть Enterprise Linux 7.2 или более поздней версии.
- К центру обработки данных подключены как минимум один домен данных и один домен хранения ISO.

Примечание. Вы можете мигрировать только в общее хранилище, такое как NFS, iSCSI или FCP. Локальное хранилище не поддерживается.

Хотя домен хранения ISO устарел, он необходим для миграции.

- Файл образа для виртуальных машин Windows virtio-win_version.iso загружается в домен хранилища ISO. Этот образ включает гостевые инструменты, необходимые для миграции виртуальных машин Windows.
- Перед импортом виртуальная машина должна быть выключена. Запуск виртуальной машины через VMware во время процесса импорта может привести к повреждению данных.
- Операция импорта может включать только виртуальные машины с одинаковой архитектурой. Если какая-либо виртуальная машина для импорта имеет другую архитектуру, появится предупреждение, и вам будет предложено изменить свой выбор, чтобы включить только виртуальные машины с такой же архитектурой.

Процедура импорта:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите (⋮) *Контекстное Меню* и выберите *Импортировать*. Откроется окно *Импорт виртуальных(ой) машин(ы)*.
3. Выберите VMware из списка *Источник*.
4. Если вы настроили провайдера VMware как внешнего провайдера, выберите его в списке *Внешний Провайдер*. Убедитесь, что учетные данные провайдера верны. Если вы не указали целевой центр обработки данных или прокси-сервер при настройке внешнего провайдера, выберите эти параметры сейчас.
5. Если вы не настроили провайдера VMware или хотите выполнить импорт от нового провайдера VMware, укажите следующие сведения:
    1. Выберите из списка *Дата Центр*, в котором будет доступна виртуальная машина.
    2. Введите IP-адрес или полное доменное имя экземпляра VMware vCenter в поле vCenter.
    3. Введите IP-адрес или полное доменное имя узла, с которого будут импортированы виртуальные машины, в поле ESXi.
    4. Введите имя центра обработки данных и кластера, в котором находится указанный узел ESXi, в поле *Дата Центр*.
    5. Если вы обменялись сертификатом SSL между узлом ESXi и Engine, оставьте флажок Verify server's SSL certificate, чтобы проверить сертификат узла ESXi. Если нет, снимите флажок.
    6. Введите имя пользователя и пароль для экземпляра VMware vCenter. У пользователя должен быть доступ к центру обработки данных VMware и узлу ESXi, на котором находятся виртуальные машины.
    7. Выберите узел в выбранном центре обработки данных с virt-v2v, который будет использоваться в качестве прокси-хоста во время операций импорта виртуальной машины. Этот узел также должен иметь возможность подключаться к сети внешнего провайдера VMware vCenter.
6. Нажмите Load, чтобы отобразить список виртуальных машин провайдера VMware, которые можно импортировать.
7. Выберите одну или несколько виртуальных машин из списка *Виртуальные машины на источнике* и с помощью стрелок переместите их в список *Виртуальные машины для импорта*. Нажмите *Далее*.

Примечание. Если сетевое устройство виртуальной машины использует тип драйвера e1000 или rtl8139, виртуальная машина будет использовать тот же тип драйвера после импорта в KeyVirt.

При необходимости вы можете изменить тип драйвера на VirtIO вручную после импорта. Если сетевое устройство использует типы драйверов, отличные от e1000 или rtl8139, тип драйвера автоматически изменяется на VirtIO во время импорта. Параметр Attach VirtIO-drivers позволяет внедрять драйверы VirtIO в импортированные файлы виртуальной машины, чтобы при изменении драйвера на VirtIO устройство правильно обнаруживалось операционной системой.

8. Выберите *Кластер*, в котором будут находиться виртуальные машины.
9. Выберите *Профиль CPU* для виртуальных машин.
10. Установите флажок *Консолидировать Снимки*, чтобы удалить точки восстановления снимков и включить шаблоны в виртуальные машины на основе шаблонов.
11. Установите флажок *Клонирование*, чтобы изменить имя виртуальной машины и MAC-адреса, а также клонировать все диски, удалив все моментальные снимки. Если виртуальная машина отображается с предупреждающим символом рядом с ее именем или имеет галочку в виртуальной машине в столбце VM in System, необходимо клонировать виртуальную машину и изменить ее имя.
12. Нажмите на каждую виртуальную машину, которую нужно импортировать, и перейдите на дополнительную вкладку *Диски*. Используйте списки *Политика выделения* и *Домен хранения*, чтобы выбрать, будет ли диск, используемый виртуальной машиной, тонко выделенным или предварительно выделенным, и выберите домен хранения, в котором будет храниться диск. Также отображается значок, указывающий, какой из дисков, которые нужно импортировать, действует как загрузочный диск для этой виртуальной машины.
13. Если вы установили флажок *Клонирование*, измените имя виртуальной машины на дополнительной вкладке *Общее*.
14. Нажмите OK, чтобы импортировать виртуальные машины.

Тип ЦП виртуальной машины должен совпадать с типом ЦП кластера, в который она импортируется.

Чтобы просмотреть тип CPU кластера на Портале администратора:

1. Нажмите *Виртуализация* > *Кластеры*.
2. Выберите кластер.
3. Нажмите *Изменить*.
4. Перейдите на вкладку *Общее*.

Если тип ЦП виртуальной машины отличается, настройте тип ЦП импортированной виртуальной машины:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Выберите виртуальную машину.
3. Нажмите *Изменить*.
4. Перейдите на вкладку *Система*.
5. Нажмите стрелку Advanced Options.
6. Укажите Custom CPU Type и нажмите OK.

5.9.6 Экспорт виртуальной машины на узел

Вы можете экспортировать виртуальную машину по определенному пути или смонтировать общее хранилище NFS на узле в центре обработки данных KeyVirt. В результате экспорта будет создан пакет Open Virtual Appliance (OVA).

Для экспорта виртуальной машины на узел выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите (⋮) *Контекстное Меню*, затем нажмите *Экспортировать как OVA*.
3. Выберите узел из раскрывающегося списка Host.
4. Введите абсолютный путь к каталогу экспорта в поле *Каталог*, включая косую черту в конце. Например, /images2/ova/.
5. При необходимости измените имя файла по умолчанию в поле *Имя*.
6. Нажмите OK.

Статус экспорта можно посмотреть на вкладке *События*.

5.9.7 Импорт виртуальной машины с узла

Импортируйте файл Open Virtual Appliance (OVA) в среду KeyVirt. Вы можете импортировать файл с любого узла KeyVirt в центре обработки данных.

Внимание! В настоящее время можно импортировать только KeyVirt и OVA, созданные VMware. KVM и Xen не поддерживаются.

Для импорта файла OVA выполните следующие действия:

1. Скопируйте файл OVA на узел в вашем кластере в расположение файловой системы, например, var /tmp. Расположение может быть локальным каталогом или удаленным монтированием nfs, если в нем достаточно места и он доступен пользователю qemu (UID 36).
2. Убедитесь, что у файла OVA есть разрешения, разрешающие доступ для чтения / записи пользователю qemu (UID 36) и группе kvm (GID 36):

```
# chown 36:36 path_to_OVA_file/file.OVA
```

3. Нажмите *Виртуализация* > *Виртуальные машины*.
4. Нажмите (⋮) *Контекстное Меню* и выберите *Импортировать*. Откроется окно *Импорт виртуальных(ой) машин(ы)*.
    1. Выберите *Готовый виртуальный образ (OVA)* из списка *Источник*.
    2. Выберите узел из списка *Узел*.
    3. В поле *Путь к файлу* укажите абсолютный путь к файлу OVA.
    4. Нажмите *Загрузить*, чтобы отобразить виртуальную машину для импорта.
    5. Выберите виртуальную машину из списка *Виртуальные машины на источнике* и с помощью стрелок переместите ее в список *Виртуальные машины для импорта*.
5. Нажмите *Далее*.
    1. Выберите *Домен хранения* для виртуальной машины.
    2. Выберите *Кластер* назначения, в котором будут находиться виртуальные машины.
    3. Выберите *Профиль CPU* для виртуальных машин.
    4. Выберите *Политику выделения* для виртуальных машин.
    5. При желании установите флажок Attach VirtIO-Drivers и выберите соответствующий образ в списке, чтобы добавить драйверы VirtIO.
    6. Выберите *Политику выделения* для виртуальных машин.

7. Выберите виртуальную машину на вкладке *Общее* и выберите *Операционная система*.
8. На вкладке *Сетевые интерфейсы* выберите имя сети и имя профиля.
9. Перейдите на вкладку *Диски*, чтобы просмотреть имя (Alias), виртуальный размер и актуальный размер виртуальной машины.

6. Нажмите OK, чтобы импортировать виртуальные машины.

5.9.8 Импорт виртуальной машины с узла KVM

Импортируйте виртуальные машины из KVM в свою среду KeyVirt. KeyVirt преобразует виртуальные машины KVM в правильный формат перед их импортом. Вы должны включить аутентификацию по открытому ключу между узлом KVM и по крайней мере одним узлом в конечном центре обработки данных (этот узел упоминается в следующей процедуре как прокси-узел).

Внимание! Виртуальная машина должна быть выключена перед импортом. Запуск виртуальной машины через KVM во время процесса импорта может привести к повреждению данных.

Примечание. Операция импорта может включать только виртуальные машины, которые используют одну и ту же архитектуру. Если какая-либо импортируемая виртуальная машина имеет другую архитектуру, появится предупреждение и вам будет предложено изменить выбранный параметр, включив в него только виртуальные машины с одинаковой архитектурой.

Если импорт завершается неудачей, смотрите детали в соответствующем файле журнала в /var/log/vdsm/import/ и в /var/log/vdsm/vdsm.log на узле прокси-сервера.

5.9.9 Импорт виртуальной машины из KVM

Внимание! Для данной процедуры требуется доступ к Порталу администратора.

1. Включите аутентификацию по открытому ключу между прокси-узлом и KVM-узлом:

    1. Войдите на прокси-сервер и сгенерируйте SSH-ключи для vdsm:
       # sudo -u vdsm ssh-keygen
    2. Скопируйте открытый ключ пользователя vdsm к узлу KVM. Файл прокси-сервера хостинга known_hosts также будет обновлен, чтобы включить ключ узла, хоста KVM.
       # sudo -u vdsm ssh-copy-id root@kvmhost.example.com
    3. Войдите на узел KVM, чтобы убедиться, что логин работает правильно:
       # sudo -u vdsm ssh root@kvmhost.example.com

4. Войдите на Портал администратора.
5. Нажмите *Виртуализация* > *Виртуальные машины*.
6. Нажмите (⋮) *Контекстное Меню* (дополнительные действия) и выберите *Импортировать*. Откроется *Импорт виртуальных(ой) машин(ы)*.
7. Выберите *Дата Центр*, которое содержит прокси-сервер.
8. Выберите KVM (через Libvirt) из выпадающего списка *Источник*.

9. При необходимости выберите KVM-провайдера *Внешний Провайдер* из выпадающего списка. URI будет предварительно заполнен правильным URI. Подробнее см. *Добавление узла KVM в качестве провайдера виртуальной машины*.
10. Введите URI узла KVM в следующем формате: qemu+ssh://root@kvmhost.example.com/system
11. Сохраняйте *Требуется авторизация*.
12. Введите root в Username.
13. Введите пароль пользователя root узла KVM.
14. Выберите Proxy Host из выпадающего списка.
15. Нажмите Load, чтобы составить список виртуальных машин на узле KVM, которые можно импортировать.
16. Выберите одну или несколько виртуальных машин из списка *Виртуальные машины на источнике* и с помощью стрелок переместите их в список *Виртуальные машины для импорта*.
17. Нажмите *Далее*.
18. Выберите *Кластер*, в котором будут находиться виртуальные машины.
19. Выберите *Профиль CPU* для виртуальных машин.
20. При необходимости выберите *Консолидировать Снимки*, чтобы удалить точки восстановления моментальных снимков и включить шаблоны в виртуальные машины на основе шаблонов.
21. При необходимости выберите *Клонирование*, чтобы изменить имя виртуальной машины и MAC-адреса и клонировать все диски, удалив все снимки. Если виртуальная машина отображается с предупреждающим символом рядом со своим именем или имеет галочку в столбце VM in System, вы должны клонировать виртуальную машину и изменить ее имя.
22. Выберите каждую виртуальную машину, которую необходимо импортировать, и нажмите *Диски*. Используйте списки *Политика выделения* и *Домен хранения* для выбора того, будет ли диск, используемый виртуальной машиной, быть тонко подготовленным или предварительно выделенным, и выберите домен хранения, на котором будет храниться диск. Также отображается значок, указывающий, какой из импортируемых дисков выступает в качестве загрузочного диска для данной виртуальной машины.
23. Если вы выбрали *Клонирование*, измените имя виртуальной машины на вкладке *Общее*.
24. Нажмите OK, чтобы импортировать виртуальные машины.

Тип процессора виртуальной машины должен совпадать с типом процессора кластера, в который она импортируется.

Для просмотра типа процессора на Портале администратора:

1. Нажмите *Виртуализация* > *Кластеры*.
2. Выберите кластер.
3. Нажмите *Изменить*.
4. Нажмите на *Общее*.

Если тип процессора виртуальной машины отличается, настройте тип процессора импортированной виртуальной машины:

1. Нажмите *Виртуализация* > *Кластеры*.
2. Выберите виртуальную машину.
3. Нажмите *Изменить*.
4. Нажмите на *Система*.
5. Нажмите на *Дополнительные параметры*.
6. Укажите Custom CPU Type и нажмите OK.

5.10 МИГРАЦИЯ ВИРТУАЛЬНЫХ МАШИН МЕЖДУ УЗЛАМИ

Живая миграция дает возможность перемещать работающую виртуальную машину между физическими узлами без прерывания обслуживания. Виртуальная машина остается включенной, а пользовательские приложения продолжают работать, пока виртуальная машина перемещается на новый физический узел. В фоновом режиме оперативная память виртуальной машины копируется с исходного узла на целевой. Хранение и сетевое подключение не изменяются.

Внимание! Для данной процедуры требуется доступ к порталу администратора.

Примечание. Виртуальную машину, использующую vGPU, нельзя перенести на другой узел.

5.10.1 Требования для оперативной миграции

Вы можете использовать живую миграцию (live-миграцию) для беспрепятственного перемещения виртуальных машин для поддержки ряда общих задач обслуживания. Ваша среда должна быть правильно настроена для поддержки живой миграции задолго до ее использования. Как минимум, для успешной миграции виртуальных машин в реальном времени должны быть выполнены следующие предварительные условия:

- Исходный и целевой узлы являются членами одного кластера, что обеспечивает совместимость ЦП между ними. **Примечание**. Живая миграция виртуальных машин между разными кластерами обычно не рекомендуется.
- Хосты источника и назначения имеют статус Up.
- Хосты источника и назначения имеют доступ к одним и тем же виртуальным сетям и VLAN.
- Хосты источника и назначения имеют доступ к домену хранения данных, в котором находится виртуальная машина.
- У узла назначения достаточно ЦП для поддержки требований виртуальной машины.
- У узла назначения достаточно неиспользуемой ОЗУ для поддержки требований виртуальной машины.
- У переносимой виртуальной машины нет cache!=none настраиваемых свойств.

Живая миграция выполняется с использованием сети управления и включает передачу больших объемов данных между узлами. Параллельные миграции могут привести к перегрузке сети управления. Для достижения максимальной

производительности создайте отдельные логические сети для управления, хранения, отображения и данных виртуальных машин, чтобы минимизировать риск насыщения сети.

5.10.2 Настройка виртуальных машин с vNIC с поддержкой SR-IOV для уменьшения сбоев сети во время миграции

Виртуальные машины с vnic, непосредственно подключенные к виртуальной функции (VF) сетевой карты узла с поддержкой SR-IOV, могут быть дополнительно сконфигурированы для уменьшения простоев сети во время динамической миграции:

1. Убедитесь, что на узле назначения есть доступный VF.
2. Установите параметры Passthrough и Migratable в профиле vNIC.
3. Включите подключение на горячую для сетевого интерфейса виртуальной машины.
4. Убедитесь, что виртуальная машина имеет резервную копию VirtIO vNIC в дополнение к сквозной vNIC, чтобы поддерживать сетевое соединение виртуальной машины во время миграции.
5. Перед настройкой связи установите параметр VirtIO vNIC No Network Filter.
6. Добавьте оба vNIC в качестве ведомых устройств под связью активного резервного копирования на виртуальной машине, а pass through venice – в качестве основного интерфейса.

Профили подключения и vNIC могут иметь одну из следующих конфигураций:

- Рекомендуется: связь не настроена, fail_over_mac=active и VF vNIC является основным ведомым устройством. Отключите фильтр подмены MAC-адресов профиля VirtIO vNIC, чтобы гарантировать, что трафик, проходящий через VirtIO vNIC, не будет отброшен, поскольку он использует MAC-адрес VF vNIC.
- Связь настроена с помощью fail_over_mac=active. Эта политика аварийного переключения гарантирует, что MAC-адрес связи всегда является MAC-адресом активного ведомого устройства. Во время аварийного переключения MAC-адрес виртуальной машины изменяется с небольшим нарушением трафика.

5.10.3 Оптимизация оперативной миграции

Миграция виртуальной машины в реальном времени может потребовать значительных ресурсов. Чтобы оптимизировать живую миграцию, вы можете установить следующие два глобальных параметра для каждой виртуальной машины в среде, для каждой виртуальной машины в кластере или для отдельной виртуальной машины.

Параметр Auto Converge migrations позволяет указать, будет ли автоматическая конвергенция использоваться во время живой миграции виртуальных машин. Большие виртуальные машины с высокими рабочими нагрузками могут загрязнять память быстрее, чем скорость передачи, достигаемая во время живой миграции, и предотвращать конвергенцию миграции. Возможности автоматической конвергенции в QEMU позволяют форсировать конвергенцию миграции виртуальных

машин. QEMU автоматически обнаруживает отсутствие конвергенции и запускает ограничение количества виртуальных ЦП на виртуальной машине.

Параметр Enable migration compression позволяет указать, используется ли сжатие миграции во время живой миграции виртуальной машины. Эта функция использует Xor Binary Zero Run-Length-Encoding для сокращения времени простоя виртуальных машин и общего времени живой миграции для виртуальных машин, на которых выполняются рабочие нагрузки с интенсивной записью в память, или для любого приложения с шаблоном обновления разреженной памяти. Оба параметра по умолчанию отключены глобально.

Настройка автоматической конвергенции и сжатия при миграции для миграции виртуальных машин:

1. Включите автоматическую конвергенцию на глобальном уровне:
   # engine-config -s DefaultAutoConvergence=True
2. Включите сжатие миграции на глобальном уровне:
   # engine-config -s DefaultMigrationCompression=True
3. Перезапустите службу ovirt-engine, чтобы изменения вступили в силу:
   # systemctl restart ovirt-engine.service
4. Настройте параметры оптимизации для кластера:
   1. Нажмите *Виртуализация* > *Кластеры* и выберите кластер.
   2. Нажмите *Изменить*.
   3. Перейдите на вкладку *Политика миграции*.
   4. В списке миграции Auto Converge выберите Inherit from global setting, Auto Converge или Don't Auto Converge.
   5. В списке Enable migration compression list выберите Inherit from global setting, Compress или Don’t Compress.
   6. Нажмите OK.
5. Настройте параметры оптимизации на уровне виртуальной машины:
   1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
   2. Нажмите *Изменить*.
   3. Выберите вкладку *Узел*.
   4. В списке миграции Auto Converge выберите *Наследовать из настроек кластера*, Auto Converge или Don't Auto Converge.
   5. В списке Enable migration compression list выберите Inherit from global setting, Compress или Don’t Compress.
   6. Нажмите OK.

5.10.4 Хуки для гостевого агента

Хуки – это скрипты, которые запускают активность на виртуальной машине при возникновении ключевых событий:

- До миграции;
- После миграции;
- Перед спящим режимом;

- После гибернации.

Базовый каталог конфигурации хуков – это /etc/ovirt-guest-agent/ hooks.d в системах Linux и C:\Program Files\Redhat\RHEV\Drivers\Agent в Windows.
Каждое событие имеет соответствующий подкаталог:
before_migration и after_migration, before_hibernation и after_hibernation. Все файлы или символические ссылки в этом каталоге будут применяться.

Пользователь-исполнитель в системах Linux – ovirtagent. Если для сценария требуются разрешения root, повышение прав должно быть выполнено создателем сценария хука. В системах Windows пользователем-исполнителем является пользователь System Service.

5.10.5 Автоматическая миграция виртуальной машины

KeyVirt Engine автоматически инициирует динамическую миграцию всех виртуальных машин, работающих на узле, когда узел переводится в режим обслуживания. Целевой узел для каждой виртуальной машины оценивается по мере миграции виртуальной машины, чтобы распределить нагрузку по кластеру.

KeyVirt Engine автоматически инициирует динамическую миграцию виртуальных машин, чтобы поддерживать уровни балансировки нагрузки или энергосбережения в соответствии с политикой планирования. Укажите политику планирования, которая лучше всего соответствует потребностям вашей среды. Вы также можете отключить автоматическую или даже ручную живую миграцию определенных виртуальных машин, если это необходимо.

Если ваши виртуальные машины настроены для обеспечения высокой производительности и/или если они были закреплены (с помощью параметра Passthrough Host CPU, CPU Pinning или NUMA Pinning), для режима миграции устанавливается значение Allow manual migration only. Однако при необходимости его можно изменить на режим Allow Manual and Automatic. Следует проявлять особую осторожность при изменении параметра миграции по умолчанию, чтобы это не привело к миграции виртуальной машины на узел, который не поддерживает высокую производительность или закрепление.

5.10.6 Предотвращение автоматической миграции виртуальной машины

KeyVirt Engine позволяет отключить автоматическую миграцию виртуальных машин. Вы также можете отключить ручную миграцию виртуальных машин, настроив виртуальную машину для работы только на определенном узле.

Возможность отключить автоматическую миграцию и требовать, чтобы виртуальная машина работала на определенном узле, полезна при использовании продуктов высокой доступности приложений, таких как Cluster Suite.

Для предотвращения автоматической миграции виртуальных машин выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите *Изменить*.

3. Перейдите на вкладку *Узел*.
4. В разделе *Запускается на* выберите *Любой узел в Кластере* или *Указанные узлы*, что позволяет выбрать несколько узлов.

   Явное назначение виртуальной машины конкретному узлу и отключение миграции не совместимы с высокой доступностью KeyVirt.
   Если к виртуальной машине напрямую подключены хост-устройства и указан другой узел, хост-устройства с предыдущего узла будут автоматически удалены с виртуальной машины.

5. Выберите Allow manual migration only или Do not allow migration из Migration parameters в раскрывающемся списке.
6. Нажмите OK.

5.10.7 Перенос виртуальных машин вручную

Работающую виртуальную машину можно в реальном времени перенести на любой узел в назначенном кластере узлов. Живая миграция виртуальных машин не вызывает прерывания обслуживания. Перенос виртуальных машин на другой узел особенно полезен, если нагрузка на конкретный узел слишком высока.

Для виртуальных машин высокой производительности и/или виртуальных машин, определенных с Проброс CPU узла, Закрепление CPU или Привязка NUMA, режим миграции по умолчанию Manual. Выберите Select Host Automatically, чтобы виртуальная машина переместилась на узел с максимальной производительностью.

Когда вы переводите узел в режим обслуживания, виртуальные машины, работающие на этом узле, автоматически переносятся на другие узлы в том же кластере. Вам не нужно вручную переносить эти виртуальные машины.

Для переноса виртуальных машин вручную выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите работающую виртуальную машину.
2. Нажмите *Перенести*.
3. Используйте переключатели, чтобы выбрать *Автоматический выбор узла* или выберите узел назначения (Select Destination Host), и указажите узел в раскрывающемся списке.
   Если выбран параметр *Автоматический выбор узла*, система определяет узел, на который переносится виртуальная машина, в соответствии с правилами балансировки нагрузки и управления питанием, установленными в политике планирования.
4. Нажмите OK.

Во время миграции прогресс отображается на индикаторе выполнения миграции. После завершения миграции столбец Host обновится, чтобы отобразить узел, на который была перенесена виртуальная машина.

5.10.8 Установка приоритета миграции

KeyVirt Engine ставит в очередь одновременные запросы на перенос виртуальных машин с заданного узла. Процесс балансировки нагрузки выполняется каждую

минуту. узлы, уже вовлеченные в событие миграции, не включаются в цикл миграции, пока не завершится их событие миграции. Когда в очереди есть запрос на миграцию и доступные узлы в кластере для его выполнения, событие миграции запускается в соответствии с политикой балансировки нагрузки для кластера.

Вы можете повлиять на порядок очереди миграции, задав приоритет каждой виртуальной машины; например, настройка критически важных виртуальных машин для миграции раньше других. Миграции будут упорядочены по приоритету: сначала будут перенесены виртуальные машины с наивысшим приоритетом.

Для установки приоритета миграции выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите *Изменить*.
3. Выберите вкладку *Высокая доступность*.
4. В раскрывающемся списке Priority выберите *Низкий*, *Средний*, или *Высокий*.
5. Нажмите OK.

5.10.9 Отмена текущей миграции виртуальных машин

Миграция виртуальной машины занимает больше времени, чем вы ожидали. Прежде чем вносить какие-либо изменения в среду, вы должны знать, где работают все виртуальные машины.

Для отмены текущей миграции виртуальной машины выполните следующие действия:

1. Выберите мигрирующую виртуальную машину. Она отображается в *Виртуализация* > *Виртуальные машины* со статусом Migration from.
2. Нажмите (⋮) *Контекстное Меню*, затем *Отменить миграцию*. Состояние виртуальной машины возвращается из состояния Migration from на Up.

5.10.10 Уведомление о событиях и журналах при автоматической миграции

Когда виртуальный сервер автоматически переносится из-за функции высокой доступности, подробности автоматической миграции документируются на вкладке События и в журнале ядра, чтобы помочь в устранении неполадок, как показано в следующих примерах:

- Уведомление на вкладке *События* Портала администратора:

  Highly Available Virtual_Machine_Name failed. It will be restarted automatically.

  Virtual_Machine_Name was restarted on Host Host_Name

- Уведомление в движке engine.log:

  This log can be found on the KeyVirt Engine at /var/log/ovirt-engine/engine.log: Failed to start Highly Available VM. Attempting to restart. VM Name: Virtual_Machine_Name, VM Id:_Virtual_Machine_ID_Number_

5.11 ВЫСОКАЯ ДОСТУПНОСТЬ ВИРТУАЛЬНЫХ МАШИН

Повышение времени безотказной работы за счет высокой доступности виртуальных машин.
Внимание! Для данной процедуры требуется доступ к порталу администратора.

5.11.1 Общие сведения о высокой доступности виртуальных машин

Для виртуальных машин с критическими рабочими нагрузками рекомендуется высокая доступность. Виртуальная машина с высокой доступностью автоматически перезапускается либо на исходном узле, либо на другом узле в кластере, если ее процесс прерывается, например, в следующих сценариях:

- Хост становится неработоспособным из-за сбоя оборудования.
- Хост переводится в режим обслуживания на время запланированного простоя.
- Хост становится недоступным, потому что он потерял связь с внешним хранилищем.

Виртуальная машина с высокой доступностью не перезапустится, если она полностью завершена, например, в следующих сценариях:

- Виртуальная машина отключена из гостевой системы.
- Виртуальная машина выключена.
- Хост выключает администратор без предварительного перевода в режим обслуживания.

С доменами хранения V4 или новее виртуальные машины имеют дополнительную возможность арендовать специальный том в хранилище, что позволяет виртуальной машине запускаться на другом узле, даже если исходный узел теряет питание. Эта функция также предотвращает запуск виртуальной машины на двух разных узлах, что может привести к повреждению дисков виртуальной машины.

Благодаря высокой доступности прерывание обслуживания минимально, поскольку виртуальные машины перезапускаются в течение нескольких секунд без вмешательства пользователя. Высокая доступность обеспечивает сбалансированность ваших ресурсов за счет перезапуска гостей на узле с низким текущим использованием ресурсов или на основе любых настроенных вами политик балансировки нагрузки или энергосбережения. Это гарантирует, что будет достаточно ресурсов для перезапуска виртуальных машин в любое время.

Высокая доступность и ошибки ввода-вывода хранилища

Если возникает ошибка ввода-вывода хранилища, виртуальная машина приостанавливается. Вы можете определить, как узел будет обрабатывать виртуальные машины высокой доступности после восстановления соединения с доменом хранения; они могут быть либо возобновлены, либо некорректно выключены, либо оставаться приостановленными.

Рекомендации по обеспечению высокой доступности

Хосту с высокой доступностью требуется устройство управления питанием и параметрами ограждения. Кроме того, чтобы виртуальная машина была высокодоступной, когда ее узел перестал работать, ее необходимо запустить на другом доступном узле в кластере. Чтобы включить миграцию высокодоступных виртуальных машин:

- Для узлов, на которых запущены высокодоступные виртуальные машины, необходимо настроить управление питанием.
- Хост, на котором запущена виртуальная машина с высокой доступностью, должен быть частью кластера, в котором есть другие доступные узлы.
- Хост назначения должен быть запущен.
- Хосты источника и назначения должны иметь доступ к домену данных, в котором находится виртуальная машина.
- Хосты источника и назначения должны иметь доступ к одним и тем же виртуальным сетям и VLAN.
- На узле назначения должно быть достаточно ЦП, который не используются для поддержки требований виртуальной машины.
- На целевом узле должно быть достаточно оперативной памяти, которая не используется для поддержки требований виртуальной машины.

5.11.2 Область применения высокой доступности

5.11.2.1 Виртуальные машины

Если вы измените режим оптимизации работающей виртуальной машины на высокую производительность, некоторые изменения конфигурации потребуют перезапуска виртуальной машины. Чтобы изменить режим оптимизации новой или существующей виртуальной машины на высокую производительность, вам может потребоваться вручную внести изменения в кластер и конфигурацию закрепленного узла. У высокопроизводительной виртуальной машины есть определенные ограничения, поскольку повышение производительности приводит к снижению гибкости:

- Если закрепление установлено для потоков ЦП, потоков ввода-вывода, потоков эмулятора или узлов NUMA, в соответствии с рекомендуемыми настройками, только подмножество узлов кластера может быть назначено высокопроизводительной виртуальной машине.
- Многие устройства автоматически отключаются, что ограничивает удобство использования виртуальной машины.

5.11.2.2 Шаблоны и пулы

Высокопроизводительные шаблоны и пулы создаются и редактируются так же, как виртуальные машины. Если для создания новых виртуальных машин используется высокопроизводительный шаблон или пул, эти виртуальные машины наследуют это свойство и его конфигурации. Однако некоторые настройки не наследуются и должны быть установлены вручную:

- Закрепление процессора
- Виртуальная NUMA и топология закрепления NUMA

- Топология закрепления потоков ввода-вывода и эмулятора
- Сквозной хост-процессор

5.11.3 Создание высокопроизводительной виртуальной машины, шаблона или пула

Чтобы создать высокопроизводительную виртуальную машину, шаблон или пул:

1. В окне *Новая* или *Изменить* для выбранного ресурса выберите *Высокая производительность* в раскрывающемся меню *Оптимизировано для*.
   При выборе этого параметра автоматически выполняются определенные изменения конфигурации этой виртуальной машины, которые вы можете просмотреть, перейдя на другие вкладки. Вы можете вернуть им исходные настройки или переопределить их. При изменении параметра его последнее значение сохраняется.
2. Нажмите OK.
   1. Если вы не установили никаких ручных настроек, появится экран Настройки высокопроизводительно виртуальной машины (High Performance Virtual Machine/Pool Settings), описывающий рекомендуемые ручные настройки.
   2. Если вы настроили некоторые настройки вручную, на экране High Performance Virtual Machine/Pool Settings отображаются настройки, которые вы не устанавливали.
   3. Если вы установили все рекомендуемые вручную настройки, экран High Performance Virtual Machine/Pool Settings не отображается.
3. Если отображается High Performance Virtual Machine/Pool Settings, нажмите кнопку *Отменить*, чтобы вернуться в новый или редактировать окно для выполнения ручной настройки. В качестве альтернативы нажмите OK, чтобы проигнорировать рекомендации. Результатом может стать снижение уровня производительности.
4. Нажмите OK.
5. Тип оптимизации можно просмотреть на вкладке *Общее* подробного представления виртуальной машины, пула или шаблона.

Примечание. Некоторые конфигурации могут переопределять параметры высокой производительности. Например, конфигурация типа экземпляра не повлияет на конфигурацию высокой производительности, если вы выберете тип экземпляра для виртуальной машины перед тем, как выберете *Высокая производительность* в раскрывающемся меню *Оптимизировано для* и выполните конфигурацию вручную. Однако, если вы выбираете тип экземпляра после высокопроизводительных конфигураций, вам следует проверить окончательную конфигурацию на разных вкладках, чтобы убедиться, что высокопроизводительные конфигурации не были переопределены типом экземпляра.

Обычно приоритет отдается последней сохраненной конфигурации.

5.11.3.1 Автоматические настройки конфигурации высокой доступности

В таблице 31 приведены автоматические настройки. В столбце Включено (Y/N) указаны конфигурации, которые включены или отключены. В столбце *Применимо к* указаны соответствующие ресурсы:

- VM – Виртуальная машина
- T – Шаблон
- P – Пул
- C – Кластер

Таблица 31. Автоматические настройки конфигурации высокой производительности

Настройка	Включено (Y/N)	Применимо к
Headless Mode (вкладка *Консоль*)	Y	VM, T, P
USB Enabled (вкладка *Консоль*)	N	VM, T, P
Smartcard Enabled (вкладка *Консоль*)	N	VM, T, P
Soundcard Enabled (вкладка *Консоль*)	N	VM, T, P
Enable VirtIO serial console (вкладка *Консоль*)	Y	VM, T, P
Allow manual migration only (вкладка *Узел*)	Y	VM, T, P
Pass-Through Host CPU (вкладка *Узел*)	Y	VM, T, P
Highly Available [1] (вкладка *Высокая доступность*)	N	VM, T, P
No-Watchdog (вкладка *Высокая доступность*)	N	VM, T, P
Memory Balloon Device (вкладка *Выделение ресурсов*)	N	VM, T, P
I/O Threads Enabled [2] (вкладка *Выделение ресурсов*)	Y	VM, T, P
Паравиртуализированный генератор случайных чисел PCI-устройства (вкладка *Генератор случайных чисел*)	Y	VM, T, P
Топология закрепления потоков ввода-вывода и эмулятора	Y	VM, T
Уровень кэша CPU 3	Y	VM, T, P

1. *Высокая доступность* не включается автоматически. Если вы выберете его вручную, высокая доступность должна быть включена только для закрепленных узлов.
2. Количество потоков ввода-вывода = 1.

5.11.3.2 Топология закрепления потоков ввода-вывода и эмулятора (автоматические настройки)

Топология закрепления потоков ввода-вывода и эмулятора требует, чтобы потоки ввода-вывода, узлы NUMA и закрепление NUMA были включены и настроены для виртуальной машины. В противном случае в журнале появится предупреждение.

Топология закрепления:

- Первые два процессора каждого узла NUMA закреплены.
- Если все vCPU помещаются в один узел NUMA узла:
  - Первые два виртуальных ЦП автоматически зарезервированы / закреплены.
  - Остальные виртуальные ЦП доступны для ручного закрепления виртуальных ЦП.
- Если виртуальная машина охватывает более одного узла NUMA:
  - Первые два процессора узла NUMA с наибольшим количеством контактов зарезервированы / закреплены.

- Оставшиеся закрепленные узлы NUMA предназначены только для закрепления виртуальных ЦП. Пулы не поддерживают закрепление потоков ввода-вывода и эмулятора.

Примечание. Если центральный ЦП привязан как к потокам виртуального ЦП, так и к потокам ввода-вывода / эмулятора, в журнале появится предупреждение, и вам будет предложено рассмотреть возможность изменения топологии закрепления ЦП, чтобы избежать этой ситуации.

5.11.3.3 Значки высокой производительности

Следующие значки указывают на состояние высокопроизводительной виртуальной машины в окне *Виртуализация* > *Виртуальные машины*.

Таблица 32. Состояния высокопроизводительной виртуальной машины

Значок	Описание
	Высокопроизводительная виртуальная машина
	Высокопроизводительная виртуальная машина с настройкой следующего запуска
	Высокопроизводительная виртуальная машина без состояния
	Высокопроизводительная виртуальная машина без состояния с настройкой следующего запуска
	Виртуальная машина в высокопроизводительном пуле
	Виртуальная машина в высокопроизводительном пуле с настройкой следующего запуска

5.11.3.4 Настройка рекомендуемых ручных настроек

Вы можете настроить рекомендуемые ручные настройки либо в окне *Новый*, либо в окне *Изменить*. Если рекомендуемая настройка не выполнена, на экране Настройки высокопроизводительно виртуальной машины (High Performance Virtual Machine/Pool Settings) отображается рекомендуемый параметр при сохранении ресурса.

5.11.3.5 Ручные настройки высокопроизводительной виртуальной машины

В следующей таблице приведены рекомендуемые ручные настройки. В столбце Включено (Y/N) указаны конфигурации, которые должны быть включены или отключены. В столбце *Применимо к* указаны соответствующие ресурсы:

- VM – Виртуальная машина
- T – Шаблон
- P – Пул
- C – Кластер

Таблица 33. Ручные высокопроизводительной виртуальной машины

Настройка	Включено (Y/N)	Применимо к
NUMA Node Count (вкладка *Узел*)	Y	VM
Tune Mode (экран *Привязка NUMA*)	Y	VM

NUMA Pinning (вкладка *Узел*)	Y	VM
CPU Pinning topology (вкладка *Выделение ресурсов*)	Y	VM, P
hugepages (вкладка *Пользовательские параметры*)	Y	VM, T, P
KSM (вкладка *Оптимизация*)	N	C

5.11.3.6 Закрепление процессоров

Чтобы закрепить виртуальные ЦП на физическом процессоре конкретного узла:

1. На вкладке *Узел* выберите переключатель *Указанные узлы*.
2. На вкладке *Выделение ресурсов* введите *Топология привязки CPU*, убедившись, что конфигурация соответствует конфигурации закрепленного узла.
3. Убедитесь, что конфигурация виртуальной машины совместима с конфигурацией узла:

    - Количество сокетов виртуальной машины не должно быть больше количества сокетов узла.
    - Количество ядер виртуальной машины на виртуальный сокет не должно превышать количество ядер узла.
    - Рабочие нагрузки с интенсивным использованием ЦП работают лучше всего, когда узел и виртуальная машина ожидают одинакового использования кэша. Для достижения максимальной производительности количество потоков виртуальной машины на ядро не должно быть больше, чем у узла.

Для закрепления ЦП предъявляются следующие требования:

- Если узел поддерживает NUMA, необходимо учитывать параметры NUMA узла (память и процессоры), поскольку виртуальная машина должна соответствовать конфигурации NUMA узла.
- Нужно учитывать топологию закрепления потоков ввода-вывода и эмулятора.

5.11.3.7 Настройка узлов NUMA и топологии закрепления

Чтобы установить узлы NUMA и топологию закрепления, вам понадобится закрепленный узел с поддержкой NUMA с как минимум двумя узлами NUMA.

1. На вкладке *Узел* выберите количество узлов NUMA и режим тонкой настройки из раскрывающихся списков.
2. Нажмите *Привязка NUMA*.
3. В окне NUMA Topology нажмите и перетащите виртуальные узлы NUMA из поля справа на физические узлы NUMA узла слева.

5.11.3.8 Настройка страниц памяти большого размера (huge pages)

Страницы памяти большого размера заранее выделяются при запуске виртуальной машины (по умолчанию динамическое размещение отключено).

Чтобы настроить такие страницы, выполните следующие действия:

1. На вкладке *Пользовательские параметры* выберите hugepages из списка пользовательских свойств, которые отображают *Выберите ключ* по умолчанию.
2. Введите размер страницы в КБ.

Для таких страниц вы должны установить самый большой размер, поддерживаемый закрепленным узлом. Рекомендуемый размер для x86_64 – 1 ГБ. К размеру страницы предъявляются следующие требования:

- Размер страница памяти большого размера виртуальной машины должен быть того же размера, что и размер страница памяти большого размера закрепленного узла.
- Объем памяти виртуальной машины должен соответствовать выбранному размеру свободных страниц памяти большого размера закрепленного узла.
- Размер узла NUMA должен быть кратным выбранному размеру страницы памяти большого размера.

Чтобы включить динамическое размещение страниц памяти большого размера:

1. Отключите фильтр HugePages в планировщике.
2. В разделе [performance] в /etc/vdsm/vdsm.conf установите следующее значение:
   use_dynamic_hugepages = true

5.11.3.9 Сравнение динамических и статических страниц памяти большого размера

В таблице 34 показаны преимущества и недостатки динамических и статических страниц памяти большого размера.

Таблица 34. Преимущества и недостатки динамических и статических страниц памяти большого размера

Настройка	**Преимущества**	**Недостатки**	**Рекомендации**
Динамические	1. Требуется меньше настроек. 2. Меньше расходуемой памяти (т.е. страницы памяти большого размера свободны на узле в ожидании возможных входящих миграций)	Сбой выделения из-за фрагментации	Используйте страницы размером 2МБ
Статистические	Предсказуемые результаты	1. Требуется командная строка ядра в конфигурации Edit Host на Портале администратора.	

		2. Требуется перезагрузка узла.	

5.11.3.10 Отключение KSM

Чтобы отключить Kernel Same-page Merging (KSM) для кластера:

1. Нажмите *Виртуализация* > *Кластеры* и выберите кластер.
2. Нажмите *Изменить*.
3. На вкладке *Оптимизация* снимите флажок *Включить KSM*.

5.12 ШАБЛОНЫ

Шаблон – это копия виртуальной машины, которую вы можете использовать для упрощения последующего многократного создания похожих виртуальных машин. Шаблоны фиксируют конфигурацию программного обеспечения, оборудования и программного обеспечения, установленного на виртуальной машине, на которой основан шаблон. Виртуальная машина, на которой основан шаблон, называется исходной виртуальной машиной.
Когда шаблон создается на основе виртуальной машины, добавляется копия диска виртуальной машины, доступная только для чтения. Этот доступный только для чтения диск становится базовым образом диска для нового шаблона и любых виртуальных машин, созданных на основе этого шаблона. Таким образом, шаблон не может быть удален, пока в среде существуют виртуальные машины, созданные на основе шаблона.
Виртуальные машины, созданные на основе шаблона, используют тот же тип сетевой карты и драйвера, что и исходная виртуальная машина, но им назначаются отдельные уникальные MAC-адреса.

5.12.1 Шаблоны и разрешения

5.12.1.1 Управление системными разрешениями для шаблона

В качестве SuperUser системный администратор управляет всеми аспектами Портала администратора. Другим пользователям могут быть назначены более конкретные административные роли. Эти ограниченные роли администратора полезны для предоставления пользователю административных привилегий, которые ограничивают его конкретным ресурсом. Например, роль DataCenterAdmin предоставляет права администратора только для назначенного центра обработки данных, за исключением хранилища для этого центра обработки данных, а ClusterAdmin предоставляет права администратора только для назначенного кластера.

Администратор шаблонов – это системная администраторская роль для шаблонов в центре обработки данных. Эта роль может применяться к конкретным виртуальным машинам, центру обработки данных или ко всей виртуализированной среде. Это может пригодиться, чтобы позволить разным пользователям управлять определенными виртуальными ресурсами. Роль администратора шаблона позволяет выполнять следующие действия:

- Создавать, редактировать, экспортировать и удалять связанные шаблоны.
- Импортировать и экспортировать шаблоны.

Вы можете назначать роли и разрешения только существующим пользователям.

В таблице ниже описаны роли и привилегии администратора, применимые к администрированию шаблона.

Таблица 35. Роли системного администратора KeyVirt

Роль	Привилегии	Детали
TemplateAdmin	Может выполнять все операции над шаблонами	Имеет право на создание, удаление и настройку домена хранения шаблона и сведений о сети, а также на перемещение шаблонов между доменами.
NetworkAdmin	Администратор сети	Может настраивать и управлять сетями, подключенными к шаблонам.

Подробнее о разрешениях и ролях см. в разделе *Системные разрешения* выше.

5.12.2 Запечатывание виртуальных машин

В этом разделе описаны процедуры по запечатыванию виртуальных машин Linux и Windows. Запечатывание – это процесс удаления всех специфичных для системы деталей из виртуальной машины перед созданием шаблона на основе этой виртуальной машины. Запечатывание необходимо, чтобы одни и те же детали не отображались на нескольких виртуальных машинах, созданных на основе одного и того же шаблона. Также необходимо обеспечить функциональность других функций, таких как предсказуемый порядок vNIC.

5.12.2.1 Запечатывание виртуальной машины Linux

Чтобы запечатать виртуальную машину Linux в процессе создания шаблона, установите флажок Seal Template в окне New Template.

5.12.2.2 Запечатывание виртуальной машины Windows

Шаблон, созданный для виртуальных машин Windows, должен быть обобщен (запечатан) перед использованием для развертывания виртуальных машин. Это гарантирует, что настройки, зависящие от машины, не будут воспроизведены в шаблоне.

Sysprep используется для запечатывания шаблонов Windows перед использованием. Sysprep генерирует полный файл ответов автоматической установки. Значения по умолчанию для нескольких операционных систем Windows доступны в каталоге /usr/share/ovirt-engine/conf/sysprep/. Эти файлы действуют как шаблоны для Sysprep. Поля в этих файлах можно копировать, вставлять и изменять по мере необходимости. Это определение переопределит любые значения, введенные в поля *Запуск инициализации* (Initial Run) окна *Изменить виртуальную машину*.

Файл Sysprep можно редактировать, чтобы влиять на различные аспекты виртуальных машин Windows, созданных из шаблона, к которому прикреплен файл Sysprep. К ним относятся подготовка Windows, настройка необходимого членства в домене, настройка имени узла и настройка политики безопасности.

Строки замены можно использовать для замены значений, предоставленных в файлах по умолчанию в каталоге /usr/share/ovirt-engine/ conf/sysprep/. Например, "<Domain><![CDATA[$JoinDomain$"]></Domain>" может использоваться для указания домена, к которому нужно присоединиться.

5.12.2.3 Предварительные условия для подготовки системы (Sysprep) виртуальной машины Windows

Примечание. Не перезагружайте виртуальную машину во время работы Sysprep.

Перед запуском Sysprep убедитесь, что настроены следующие параметры:

- Параметры виртуальной машины Windows определены правильно.
- Если нет, нажмите *Изменить* в *Виртуализация* > *Виртуальные машины* и введите необходимую информацию в поля *Операционная система* и *Кластер*.
- Правильный ключ продукта был определен в файле переопределения на Engine.

Файл переопределения должен быть создан в /etc/ovirt-engine/osinfo.conf.d/, иметь имя файла, которое помещается после /etc/ovirt-engine/osinfo.conf.d/00-defaults.properties и оканчивается на .properties. Например, /etc/ovirt-engine/osinfo.conf.d/10-productkeys.properties. Последний файл будет иметь приоритет и переопределит любой другой предыдущий файл.

Если нет, скопируйте значения по умолчанию для вашей операционной системы Windows из /etc/ovirt-engine/osinfo.conf.d/00-defaults.properties в файл переопределения и введите свои значения в поля productKey.value и sysprepPath.value.

Процедура:

1. На виртуальной машине Windows запустите Sysprep из каталога C:\Windows\System32\sysprep\sysprep.exe.
2. Введите следующую информацию в Sysprep:
    - В разделе System Cleanup Action выберите Enter System Outof-Box-Experience (OOBE).
    - Установите флажок Generalize, если вам нужно изменить системный идентификационный номер (SID) компьютера.
    - В разделе Shutdown Options выберите Shutdown.
3. Нажмите OK, чтобы завершить процесс запечатывания. Виртуальная машина автоматически выключается по завершении.

Виртуальная машина Windows 7, Windows 2008 или Windows 2012 будет запечатана и готова к созданию шаблона, который будет использоваться для развертывания виртуальных машин.

5.12.3 Создание шаблона

Создайте шаблон из существующей виртуальной машины, чтобы использовать его в качестве образца для создания дополнительных виртуальных машин.

Примечание. В RHV 4.4, чтобы запечатать виртуальную машину RHEL 8 для шаблона, ее уровень кластера должен быть 4,4, а все узлы в кластере должны быть основаны на RHEL 8. Вы не можете запечатать виртуальную машину RHEL 8, если вы установили для нее уровень кластера 4.3, чтобы он мог работать на узлах RHEL 7.

Когда вы создаете шаблон, в качестве формата диска вы указываете raw или QCOW2:

- Диски QCOW2 имеют тонкое предоставление.
- Raw диски в файловом хранилище имеют тонкое предоставление.
- Raw диски в блочном хранилище выделяются заранее.

Для создания шаблона выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите исходную виртуальную машину.
2. Убедитесь, что виртуальная машина выключена и находится в состоянии *Выключено*.
3. Нажмите (⋮) *Контекстное Меню*, затем нажмите *Создать шаблон*.
4. Введите имя, описание и комментарий для шаблона.
5. В раскрывающемся списке *Кластер* выберите кластер, с которым нужно связать шаблон. По умолчанию он тот же самый, что и на исходной виртуальной машине.
6. При необходимости выберите профиль ЦП для шаблона из раскрывающегося списка *Профиль CPU*.
7. При необходимости установите флажок *Создать в качестве дополнительной версии шаблона*, выберите Root Template и введите Sub-Version Name, чтобы создать новый шаблон как подшаблон существующего шаблона.
8. В разделе *Распределение диска* введите псевдоним (Alias) для диска в текстовое поле *Псевдоним*. Выберите формат диска в раскрывающемся списке *Формат*, домен хранения, на котором будет храниться диск, из раскрывающегося списка Target и профиль диска в раскрывающемся списке *Профиль диска*. По умолчанию они такие же, как у исходной виртуальной машины.
9. Установите флажок *Разрешить всем пользователям доступ к шаблону*, чтобы сделать шаблон общедоступным.
10. Установите флажок *Копировать разрешения ВМ*, чтобы скопировать разрешения исходной виртуальной машины в шаблон.
11. Установите флажок *Шаблон печати* (только для Linux), чтобы запечатать шаблон.

    Запечатывание, при котором используется команда virt-sysprep, удаляет системные данные с виртуальной машины перед созданием шаблона на основе этой виртуальной машины. Это предотвращает появление деталей исходной виртуальной машины в последующих виртуальных машинах, созданных с использованием того же шаблона. Это также обеспечивает функциональность других функций, таких как предсказуемый порядок vNIC.
12. Нажмите OK.

Виртуальная машина отображает статус создания шаблона *Образ заблокирован*. Процесс создания шаблона может занять до часа в зависимости от

размера виртуального диска и возможностей вашего оборудования хранения. По завершении шаблон добавляется на вкладку *Шаблоны*. Теперь вы можете создавать новые виртуальные машины на основе шаблона.

При создании шаблона виртуальная машина копируется, так что и существующая виртуальная машина, и ее шаблон можно использовать после создания шаблона.

5.12.4 Редактирование шаблона

После создания шаблона его свойства можно редактировать. Поскольку шаблон является копией виртуальной машины, параметры, доступные при редактировании шаблона, идентичны параметрам в окне *Изменить виртуальную машину*.
Для редактирования шаблона выполните следующие действия:
1. Нажмите *Виртуализация* > *Шаблоны* и выберите шаблон.
2. Нажмите *Изменить*.
3. Измените необходимые свойства. Нажмите *Показать расширенные опции* и при необходимости измените настройки шаблона. Параметры, отображаемые в *Изменить шаблон*, идентичны параметрам в окне *Изменить виртуальную машину*, но содержат только соответствующие поля.
4. Нажмите OK.

5.12.5 Удаление шаблона

Если вы использовали шаблон для создания виртуальной машины с использованием параметра распределения хранилища с тонким выделением ресурсов, этот шаблон нельзя удалить, поскольку он нужен виртуальной машине для продолжения работы. Однако клонированные виртуальные машины не зависят от шаблона, из которого они были клонированы, и шаблон можно удалить.
Для удаления шаблона выполните следующие действия:
1. Нажмите *Виртуализация* > *Шаблоны* и выберите шаблон.
2. Нажмите *Удалить*.
3. Нажмите OK.

5.12.6 Экспорт шаблонов

5.12.6.1 Перенос шаблонов в домен экспорта

Экспортируйте шаблоны в экспортный домен, чтобы переместить их в другой домен данных, либо в той же среде KeyVirt, либо в другой.

Для экспорта отдельных шаблонов в экспортный домен выполните следующие действия:

1. Нажмите *Виртуализация* > *Шаблоны* и выберите шаблон.
2. Нажмите *Экспортировать*.
3. Установите флажок *Перезаписать принудительно*, чтобы заменить любую более раннюю версию шаблона в экспортном домене.
4. Нажмите OK, чтобы начать экспорт шаблона. Это может занять до часа в зависимости от размера виртуального диска и вашего оборудования хранения.

Повторяйте эти шаги до тех пор, пока домен экспорта не будет содержать все шаблоны для миграции, прежде чем вы начнете процесс импорта.

1. Нажмите *Хранилище* > *Домены* и выберите экспортный домен.
2. Нажмите на имя домена, чтобы просмотреть подробную информацию.
3. Перейдите на вкладку *Импорт Шаблона*, чтобы просмотреть все экспортированные шаблоны в экспортном домене.

5.12.6.2 Копирование шаблона виртуального жесткого диска

Если вы перемещаете виртуальную машину, созданную на основе шаблона с выбранным параметром распределения хранилища с тонким предоставлением, диски шаблона необходимо скопировать в тот же домен хранения, что и виртуальный диск.

Для копирования виртуального жесткого диска выполните следующие действия:

1. Нажмите *Хранилище* > *Диски*.
2. Выберите диск(и) шаблона для копирования.
3. Нажмите *Копировать*.
4. Выберите *Цель* для домена данных из раскрывающегося списка.
5. Нажмите OK.

Будет создана копия шаблона виртуального жесткого диска в том же или другом домене хранения. Если вы копировали шаблонный диск при подготовке к перемещению виртуального жесткого диска, теперь вы можете переместить виртуальный жесткий диск**.**

5.12.7 Импорт шаблонов

5.12.7.1 Импорт шаблона в центр обработки данных

Для импорта шаблона из только что присоединенного экспортного домена в центр обработки данных выполните следующие действия:

1. Нажмите *Хранилище* > *Домены* и выберите только что присоединенный экспортный домен.
2. Нажмите на имя домена, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку *Импорт Шаблона* и выберите шаблон.
4. Нажмите *Импортировать*.
5. Используйте раскрывающиеся списки для выбора *Кластер назначения* и *Профиль CPU*.
6. Выберите шаблон, чтобы просмотреть сведения о нем, затем выберите вкладку *Диски* и выберите *Домен хранения*, в который нужно импортировать шаблон.
7. Нажмите OK.
8. Если появится окно Import Template Conflict, введите New Name для шаблона или установите флажок Apply to all и введите Suffix to add to the cloned Templates. Нажмите OK.
9. Нажмите Close.

Шаблон импортируется в целевой центр обработки данных. Это может занять до часа, в зависимости от вашего устройства хранения. Вы можете просмотреть прогресс импорта на вкладке *События*.

После завершения процесса импорта шаблоны будут отображаться в *Виртуализация* > *Шаблоны*. Шаблоны могут создавать новые виртуальные машины или запускать существующие импортированные виртуальные машины на основе этого шаблона.

5.12.7.2 Импорт виртуального диска из службы образов OpenStack

Виртуальные диски, управляемые службой образов OpenStack, можно импортировать в Engine, если эта служба образов OpenStack была добавлена в Engine в качестве внешнего провайдера.

Внимание! Для данной процедуры требуется доступ к Порталу администратора.

Процедура:

1. Нажмите *Хранилище* > *Домены* и выберите домен OpenStack Image Service.
2. Нажмите на имя домена хранения, чтобы перейти к просмотру сведений.
3. Перейдите на вкладку Images и выберите изображение для импорта.
4. Нажмите *Импортировать*.
5. Выберите *Дата Центр*, в который будет импортирован виртуальный диск.
6. Выберите домен хранения, в котором будет храниться виртуальный диск, из раскрывающегося списка Domain Name.
7. При желании выберите *Квота* для применения к виртуальному диску.
8. Установите флажок Import as Template.
9. Выберите кластер, в котором виртуальный диск будет доступен в качестве шаблона.
10. Нажмите OK.

Образ импортируется как шаблон и отобразится на вкладке *Шаблоны*. Теперь вы можете создавать виртуальные машины на основе шаблона.

5.12.8 Использование Cloud-Init

Cloud-Init – это инструмент для автоматизации начальной настройки виртуальных машин, такой как настройка имени узла, сетевых интерфейсов и авторизованных ключей. Его можно использовать при подготовке виртуальных машин, которые были развернуты на основе шаблона, чтобы избежать конфликтов в сети.

Чтобы использовать этот инструмент, пакет cloud-init должен быть сначала установлен на виртуальной машине. После установки служба Cloud-Init запускается в процессе загрузки для поиска инструкций по настройке. Затем вы можете использовать параметры в окне *Разовый запуск*, чтобы предоставить эти инструкции только один раз, или параметры в окнах *Новая виртуальная машина*, *Изменить виртуальную машину* и *Изменить шаблон*, чтобы предоставлять эти инструкции при каждом запуске виртуальной машины. Кроме того, вы можете настроить Cloud-Init с помощью Ansible, Python, Java или Ruby.

5.12.8.1 Сценарии использования Cloud-Init

Cloud-Init можно использовать для автоматизации настройки виртуальных машин в различных сценариях. Вот несколько распространенных сценариев:

- **Виртуальные машины, созданные на основе шаблонов**

Вы можете использовать параметры Cloud-Init в разделе Запуск Инициализации окна *Разовый запуск* для инициализации виртуальной машины, созданной на основе шаблона. Это позволяет вам настроить виртуальную машину при первом запуске виртуальной машины.

- **Шаблоны виртуальных машин**

Вы можете использовать параметры Use Cloud-Init/Sysprep на вкладке *Запуск инициализации* (Initial Run) окна *Изменить шаблон*, чтобы указать параметры для настройки виртуальных машин, созданных на основе этого шаблона.

- **Пулы виртуальных машин**

Вы можете использовать параметры Use Cloud-Init/Sysprep на вкладке Запуск Инициализации в окне Новый Пул (New Pool), чтобы указать параметры для настройки виртуальных машин, взятых из этого пула виртуальных машин. Это позволяет указать набор стандартных параметров, которые будут применяться каждый раз, когда виртуальная машина будет взята из этого пула виртуальных машин. Вы можете унаследовать или переопределить параметры, указанные для шаблона, на котором основана виртуальная машина, или указать параметры для самого пула виртуальных машин.

5.12.8.2 Установка Cloud-Init

В этой процедуре описывается, как установить Cloud-Init на виртуальной машине. После установки Cloud-Init вы можете создать шаблон на основе этой виртуальной машины. Виртуальные машины, созданные на основе этого шаблона, могут использовать функции Cloud-Init, такие как настройка имени узла, часового пояса, пароля root, авторизованных ключей, сетевых интерфейсов, службы DNS и т.д. при загрузке.

Для установки Cloud-Init выполните следующие действия:

1. Войдите в виртуальную машину.
2. Включите репозитории:

- Для Enterprise Linux 6:

```
# subscription-manager repos \
    --enable=rhel-6-server-rpms \
    --enable=rhel-6-server-rh-common-rpms
```

- Для Enterprise Linux 7:

```
# subscription-manager repos \
   --enable=rhel-7-server-rpms \
    --enable=rhel-7-server-rh-common-rpms
```

- Для Enterprise Linux 8 обычно не требуется включать репозитории для установки Cloud-Init. Пакет Cloud-Init является частью репозитория

AppStream, rhel-8-for-x86_64-appstream-rpms, который включен по умолчанию в Enterprise Linux 8.

3. Установите пакет cloud-init и зависимости:
   # dnf install cloud-init

Для версий Enterprise Linux до версии 8 вместо dnf install cloud-init используйте команду yum install cloud-init.

5.12.8.3 Использование Cloud-Init для подготовки шаблона

Пока пакет cloud-init установлен на виртуальной машине Linux, вы можете использовать виртуальную машину для создания шаблона с поддержкой облачной инициализации. Укажите набор стандартных параметров, которые будут включены в шаблон, как описано в следующей процедуре, или, в качестве альтернативы, пропустите этапы настройки Cloud-Init и настройте их при создании виртуальной машины на основе этого шаблона.

Примечание. Хотя в следующей процедуре описывается, как использовать Cloud-Init при подготовке шаблона, те же настройки также доступны в окнах *Новая виртуальная машина*, *Изменить шаблон* и *Разовый запуск*.

Для использования Cloud-Init для подготовки шаблона выполните следующие действия:

1. Нажмите *Виртуализация* > *Шаблоны* и выберите шаблон.
2. Нажмите *Изменить*.
3. Нажмите *Показать расширенные опции*.
4. Перейдите на вкладку Запуск Инициализации и установите флажок Use Cloud-Init/Sysprep.
5. Введите имя узла в текстовое поле VM hostname.
6. Установите флажок *Настроить временную зону* и выберите часовой пояс из раскрывающегося списка *Временная зона*.
7. Разверните раздел *Аутентификация*.
   - Установите флажок *Пользователь уже установил пароль* (Use already configured password), чтобы использовать существующие учетные данные, или снимите этот флажок и введите пароль пользователя root в текстовые поля *Пароль* и *Подтвердите пароль*, чтобы указать новый пароль пользователя root.
   - Введите любые ключи SSH, которые нужно добавить в файл авторизованных узлов на виртуальной машине, в текстовой области *Ключи SSH авторизации*.
   - Установите флажок *Пересоздать ключи SSH*, чтобы повторно создать ключи SSH для виртуальной машины.
8. Разверните раздел *Сети*.
   - Введите любые DNS-серверы в текстовое поле *Сервера DNS*.
   - Введите любые домены поиска DNS в текстовое поле *Домен поиска DNS*.
   - Установите флажок *Имя сетевого интерфейса в гостевой системе* (In-guest Network Interface) и используйте кнопки *Добавить новый* и *Удалить*

выбранные, чтобы добавить или удалить сетевые интерфейсы на виртуальной машине или из нее.

Примечание. Вы должны указать правильное имя сетевого интерфейса и номер (например, eth0, eno3, enp0s). В противном случае интерфейсное соединение виртуальной машины будет установлено, но не будет иметь сетевой конфигурации cloud-init.

9. Разверните раздел *Пользовательский скрипт* и введите любые пользовательские сценарии в текстовой области *Пользовательский скрипт*.
10. Нажмите OK.

Теперь вы можете подготовить новые виртуальные машины с помощью этого шаблона.

5.12.8.4 Использование Cloud-Init для инициализации виртуальной машины

Используйте Cloud-Init для автоматизации первоначальной настройки виртуальной машины Linux. Вы можете использовать поля Cloud-Init для настройки имени узла виртуальной машины, часового пояса, пароля root, авторизованных ключей, сетевых интерфейсов и службы DNS. Вы также можете указать собственный сценарий, сценарий в формате YAML, который будет запускаться при загрузке. Пользовательский сценарий допускает дополнительную конфигурацию Cloud-Init, которая поддерживается Cloud-Init, но недоступна в полях Cloud-Init.

Эта процедура запускает виртуальную машину с набором настроек Cloud-Init. Если соответствующие параметры включены в шаблон, на котором основана виртуальная машина, просмотрите параметры, при необходимости внесите изменения и нажмите OK, чтобы запустить виртуальную машину.

Выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите кнопку Run раскрывающегося списка и выберите *Разовый запуск*.
3. Разверните раздел Запуск Инициализации и установите флажок Cloud-Init.
4. Введите имя узла в текстовое поле VM hostname.
5. Установите флажок *Настроить временную зону* и выберите часовой пояс в раскрывающемся меню *Временная зона*.
6. Установите флажок *Пользователь уже установил пароль*, чтобы использовать существующие учетные данные, или снимите этот флажок и введите пароль пользователя root в текстовые поля *Пароль* и *Подтвердите пароль*, чтобы указать новый пароль пользователя root.
7. Введите любые ключи SSH, которые нужно добавить в файл авторизованных узлов на виртуальной машине, в текстовой области *Ключи SSH авторизации*.
8. Установите флажок *Пользователь уже установил пароль*, чтобы повторно создать ключи SSH для виртуальной машины.
9. Введите любые DNS-серверы в текстовое поле *Сервера DNS*.
10. Введите любые домены поиска DNS в текстовое поле *Домен поиска DNS*.

11. Установите флажок Network и используйте кнопки «+» и «–» , чтобы добавить или удалить сетевые интерфейсы на виртуальной машине или из нее.

    Вы должны указать правильное имя сетевого интерфейса и номер (например, eth0, eno3, enp0s). В противном случае интерфейсное соединение виртуальной машины будет установлено, но конфигурация сети cloud-init в нем не будет определена.
12. Введите настраиваемый сценарий в текстовую область *Пользовательский скрипт*. Убедитесь, что значения, указанные в сценарии, подходят. В противном случае действие завершится неудачно.
13. Нажмите OK.

Чтобы проверить, установлен ли Cloud-Init на виртуальной машине, выберите виртуальную машину и нажмите на вложенную вкладку *Приложения*. Все отображается, только если установлен гостевой агент.

5.12.9 Использование Sysprep

Sysprep – это инструмент, используемый для автоматизации настройки виртуальных машин Windows, например, для настройки имен узлов, сетевых интерфейсов, авторизованных ключей, настройки пользователей или для подключения к Active Directory. Sysprep устанавливается во всех версиях Windows.

KeyVirt расширяет возможности Sysprep за счет использования технологии виртуализации для развертывания виртуальных рабочих станций на основе единого шаблона. KeyVirt создает индивидуальный файл автоответа для каждой виртуальной рабочей станции.

Sysprep создает полный файл ответов для автоматической установки. Значения по умолчанию для нескольких операционных систем Windows доступны в каталоге /usr/share/ovirt-engine/conf/sysprep/. Вы также можете создать собственный Sysprep-файл и указать ссылку на него из файла osinfo в каталоге /etc/ovirt-engine/osinfo.conf.d/. Эти файлы действуют как шаблоны для Sysprep. Поля в этих файлах можно копировать и редактировать по мере необходимости. Это определение переопределит любые значения, введенные в поля Запуск Инициализации окна *Изменить виртуальную машину*.

Файл переопределения должен быть создан в /etc/ovirt-engine/osinfo.conf.d/, иметь имя файла, которое ставится после /etc/ovirt-engine/osinfo.conf.d/00-defaults.properties, и заканчиваться на .properties. Например, /etc/ovirt-engine/osinfo.conf.d/10-productkeys.properties. Последний файл будет иметь приоритет и переопределит любой другой предыдущий файл.

Скопируйте значения по умолчанию для вашей операционной системы Windows из /etc/ovirt-engine/osinfo.conf.d/00-defaults.properties в файл переопределения и введите свои значения в поля productKey.value и sysprepPath.value.

Пример. Значения конфигурации Windows 7 по умолчанию:

```
# Windows7(11, OsType.Windows, false),false
 os.windows_7.id.value = 11
 os.windows_7.name.value = Windows 7
 os.windows_7.derivedFrom.value = windows_xp
```

os.windows_7.sysprepPath.value = ${ENGINE_USR}/conf/sysprep/sysprep.w7
os.windows_7.productKey.value =
os.windows_7.devices.audio.value = ich6
os.windows_7.devices.diskInterfaces.value.3.3 = IDE, VirtIO_SCSI, VirtIO
os.windows_7.devices.diskInterfaces.value.3.4 = IDE, VirtIO_SCSI, VirtIO
os.windows_7.devices.diskInterfaces.value.3.5 = IDE, VirtIO_SCSI, VirtIO
os.windows_7.isTimezoneTypeInteger.value = false

5.12.9.1 Настройка Sysprep на шаблоне

Вы можете использовать эту процедуру, чтобы указать набор стандартных параметров Sysprep для включения в шаблон, или же вы можете настроить параметры Sysprep при создании виртуальной машины на основе этого шаблона.

Строки замены можно использовать для замены значений, предоставленных в файлах по умолчанию в каталоге /usr/share/ovirt-engine/conf/sysprep/. Например, "<Domain><![CDATA[$JoinDomain$"]></Domain>" может использоваться для указания домена, к которому нужно присоединиться.

Требования:

- Параметры виртуальной машины Windows определены правильно. Если нет, перейдите в *Виртуализация* > *Виртуальные машины*, нажмите *Изменить* и введите необходимую информацию в поля *Операционная система* и *Кластер*.
- Правильный ключ продукта был определен в файле переопределения.

Для использования Sysprep для подготовки шаблона выполните следующие действия:

1. Соберите виртуальную машину Windows с необходимыми исправлениями и программным обеспечением.
2. Закройте виртуальную машину Windows.
3. Создайте шаблон на основе виртуальной машины Windows.
4. Обновите файл Sysprep в текстовом редакторе, если требуются дополнительные изменения.

Теперь вы можете подготовить новые виртуальные машины с помощью этого шаблона.

5.12.9.2 Использование Sysprep для инициализации виртуальной машины

Используйте Sysprep для автоматизации начальной настройки виртуальной машины Windows. Вы можете использовать поля Sysprep для настройки имени узла виртуальной машины, часового пояса, пароля root, авторизованных ключей, сетевых интерфейсов и службы DNS.

Использование Sysprep для инициализации виртуальной машины запускает виртуальную машину с набором Sysprep настроек. Если соответствующие параметры включены в шаблон, на котором основана виртуальная машина, просмотрите параметры и при необходимости внесите изменения.

Выполните следующие действия:

1. Создайте новую виртуальную машину Windows на основе шаблона необходимой виртуальной машины Windows.
2. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
3. Нажмите на кнопку *Запустить* раскрывающегося списка и выберите *Разовый запуск*.
4. Разверните раздел *Запуск инициализации*, установите флажок *Использовать sysprep*.
5. Разверните раздел *Параметры загрузки*, установите флажок *Прикрепить CD* и выберите требуемый ISO-образ Windows из раскрывающегося списка.
6. Переместите CD-ROM в верхнюю часть поля *Предпочитаемая последовательность загрузки*.
7. При необходимости настройте любые дополнительные параметры *Разового запуска*.
8. Нажмите OK.

5.12.10 Создание виртуальной машины на основе шаблона

Создайте виртуальную машину из шаблона, чтобы на виртуальных машинах можно было предварительно настроить операционную систему, сетевые интерфейсы, приложения и другие ресурсы.

Виртуальные машины, созданные из шаблона, зависят от этого шаблона. Таким образом, вы не можете удалить шаблон с Engine, если виртуальная машина была создана из этого шаблона. Однако вы можете клонировать виртуальную машину из шаблона, чтобы удалить зависимость от этого шаблона.

Если тип BIOS виртуальной машины отличается от типа BIOS шаблона, Engine может изменить устройства в виртуальной машине, что может помешать загрузке операционной системы. Например, если в шаблоне используются диски IDE и набор микросхем i440fx, изменение типа BIOS на набор микросхем Q35 автоматически изменяет диски IDE на диски SATA. Поэтому настройте набор микросхем и тип BIOS в соответствии с набором микросхем и типом BIOS шаблона.

Для создания виртуальной машины на основе шаблона выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите New.
3. Выберите кластер, на котором будет работать виртуальная машина.
4. Выберите шаблон из списка *Основано на шаблоне*.
5. Введите имя, описание, и любые комментарии, а в остальных полях примите значения по умолчанию, унаследованные от шаблона. При необходимости их можно изменить.
6. Перейдите на вкладку *Выделение ресурсов*.
7. Выберите *Клонирование* в *Выделение хранилища*.
8. Выберите формат диска. Если вы выберете *Тонкий*, формат диска будет QCOW2. Если вы выбрали *Клонирование*, выберите QCOW2 или Raw для формата диска.

9. Используйте раскрывающийся список *Цель*, чтобы выбрать домен хранения, в котором будет храниться виртуальный диск виртуальной машины.
10. Нажмите OK.

Виртуальная машина отображается на вкладке *Виртуальные машины*.

5.12.11 Клонирование виртуальной машины на основе шаблона

Клонированные виртуальные машины основаны на шаблонах и наследуют настройки шаблона. Клонированная виртуальная машина не зависит от шаблона, на котором она была основана после создания. Это означает, что шаблон можно удалить, если не существует других зависимостей.
Если вы клонируете виртуальную машину из шаблона, имя шаблона, на котором эта виртуальная машина была основана, отображается на вкладке *Общее* окна *Изменить виртуальную машину* для этой виртуальной машины. Если вы измените имя этого шаблона, имя шаблона на вкладке *Общее* также будет обновлено. Однако, если вы удалите шаблон из KeyVirt, вместо него будет отображаться исходное имя этого шаблона.
Для клонирования виртуальной машины на основе шаблона выполните следующие действия:
1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите New.
3. Выберите *Кластер*, на котором будет работать виртуальная машина.
4. Выберите шаблон из раскрывающегося меню *Основано на шаблоне*.
5. Введите имя, описание и любые комментарии. Вы можете принять значения по умолчанию, унаследованные от шаблона, в остальных полях или изменить их при необходимости.
6. Перейдите на вкладку *Выделение ресурсов*.
7. Выберите переключатель *Клонирование* на вкладке *Выделение хранилища*.
8. Выберите формат диска из раскрывающегося списка *Формат*. Это влияет на скорость операции клонирования и объем дискового пространства, изначально необходимого новой виртуальной машине.

- QCOW2 (по умолчанию):

– Более быстрая операция клонирования;
– Оптимизированное использование емкости хранилища;
– Дисковое пространство выделяется только по мере необходимости.

- Raw:

– Более медленная операция клонирования;
– Оптимизированные операции чтения и записи виртуальной машины;
– Все дисковое пространство, запрошенное в шаблоне, выделяется во время операции клонирования.

9. Используйте раскрывающееся меню *Цель*, чтобы выбрать домен хранения, в котором будет храниться виртуальный диск виртуальной машины.
10. Нажмите OK.
Примечание. Клонирование виртуальной машины может занять некоторое время. Необходимо создать новую копию диска с шаблоном. В это время виртуальная машина имеет статус сначала *Образ заблокирован*, затем *Выключено*.

Виртуальная машина создается и отображается на вкладке *Виртуальные машины*. Теперь вы можете назначать ей пользователей и начать использовать ее после завершения операции клонирования.

6 УПРАВЛЕНИЕ СРЕДОЙ ВИРТУАЛИЗАЦИИ

6.1 АДМИНИСТРИРОВАНИЕ СЕРВЕРА УПРАВЛЕНИЯ СРЕДОЙ ВИРТУАЛИЗАЦИИ (SELF-HOSTED ENGINE)

6.1.1 Поддержка сервера управления средой виртуализации

6.1.1.1 Режимы обслуживания сервера управления средой виртуализации

Режимы обслуживания позволяют запускать, останавливать и изменять виртуальную машину Engine без вмешательства со стороны агентов высокой доступности, а также перезапускать и изменять узлы в системе, не мешая работе Engine.
Существует три режима обслуживания:

- global – всем агентам высокой доступности в кластере отключен мониторинг состояния ВМ Engine. Применяется для любых операций по настройке или обновлению KeyVirt, требующих остановки службы ovirtengine;
- local – агент высокой доступности на узле, введенном в режим обслуживания, отключен от наблюдения за состоянием виртуальной машины Engine. Если в момент перехода в режим обслуживания на узле была запущена ВМ управления Engine, то она мигрирует на другой доступный узел. Данный режим рекомендуется при применении системных изменений или обновлений к локальному ядру узла;
- none – отключает режим обслуживания, обеспечивая работу агентов высокой доступности.

6.1.1.2 Включение локального режима обслуживания

Включение режима локального обслуживания останавливает агент высокой доступности на одном локальном узле ядра.
Для включения локального режима обслуживания из Портала администратора выполните следующие действия:

1. Переведите выбранный узел в режим локального обслуживания:
   - На Портале администратора нажммите *Виртуализация* > *Узлы* и выберите узел.
   - Нажмите *Управление* > *Перейти в режим Обслуживания*, а затем ОК. Для этого узла автоматически запустится режим локального обслуживания.
2. После того, как вы выполнили все задачи обслуживания, отключите режим обслуживания:
   - На Портале администратора нажмите *Виртуализация* > *Узлы* и выберите узел.
   - Нажмите *Управление* > *Выйти из режима обслуживания*.

Для включения локального режима обслуживания из командной строки выполните следующие действия:

1. Зайдите на узел и переведите его в режим локального обслуживания командой:
   # hosted-engine --set-maintenance --mode=local
2. После того, как вы выполнили все задачи, отключите режим обслуживания:
   # hosted-engine --set-maintenance --mode=none

6.1.1.3 Включение глобального режима обслуживания

Включение режима глобального обслуживания останавливает агенты высокой доступности на всех узлах ядра, размещенных в кластере.
Для настройки режима глобального обслуживания из портала администратора выполните следующие действия:

1. Переведите все узлы виртуализации в режим глобального обслуживания:
   - На Портале администратора нажмите *Виртуализация* > *Узлы* и выберите любой собственный узел ядра.
   - Нажмите на значок ⋮ (контекстное меню), затем нажмите *Включить глобальный режим обслуживания высокой доступности*.
2. После того, как вы выполнили все задачи обслуживания, отключите режим обслуживания:
   - На Портале администратора нажмите *Виртуализация* > *Узлы* и выберите любой узел.
   - Нажмите на значок ⋮ (контекстное меню), затем нажмите *Выключить глобальный режим обслуживания высокой доступности*.

Для настройки режима глобального обслуживания из командной строки выполните следующие действия:

1. Зайдите на любой узел ядра и переведите его в режим глобального обслуживания:
   # hosted-engine --set-maintenance --mode=global
2. После того, как вы выполнили все задачи обслуживания, отключите режим глобального обслуживания:
   hosted-engine --set-maintenance --mode=none

6.1.1.4 Администрирование BM Engine

Утилита hosted-engine предоставляет множество команд для администрирования виртуальной машины Engine. Вы можете запустить hosted-engine на подготовленном узле Engine. Чтобы просмотреть все доступные команды, запустите hostedengine --help. Для получения дополнительной информации о конкретной команде запустите hosted-engine -- --help.

6.1.1.5 Обновление конфигурации системы сервера управления

Чтобы обновить конфигурацию Engine, используйте команду hostedengine --set-shared-config. После выполнения команды конфигурация Engine будет обновлена в общем домене хранения после первоначального развертывания.
Чтобы просмотреть текущие значения конфигурации, используйте команду:
hosted-engine --get-shared-config
Чтобы просмотреть список всех доступных ключей конфигурации и соответствующих им типов, введите следующую команду:
hosted-engine --set-shared-config key --type=type --help
Здесь <type> может принимать одно из следующих значений:

- he_local – задает значения в локальном экземпляре etc/ovirt-hosted-engine/ hosted-engine.conf на локальном узле, чтобы только этот узел использовал новые значения. Чтобы включить новое значение, перезапустите службы ovirt-ha-agent и ovirt-ha-broker.
- he_shared – задает значения в etc/ovirt-hosted-engine/hosted-engine.conf в общем хранилище, поэтому все узлы, развернутые после изменения конфигурации, используют эти значения. Чтобы включить новое значение на узле, повторно разверните этот узел.
- ha – устанавливает значения в /var/lib/ovirt-hosted-engine-ha/ha.conf в локальном хранилище. Новые настройки вступают в силу немедленно.
- broker – устанавливает значения в /var/lib/ovirt-hosted-engine-ha/broker.conf в локальном хранилище. Перезапустите службу ovirt-ha-broker, чтобы активировать новые настройки.

6.1.1.6 Настройка уведомлений по электронной почте

Вы можете настроить уведомления по электронной почте с помощью SMTP для любых переходов состояния высокой доступности на собственных узлах ядра. Ключи, которые можно обновить, включают следующее: email.destination-emails, email.smtp-port, email.smtp-server, email.source-email, notify.state_transition.
Чтобы настроить уведомления по электронной почте, выполните следующие действия:

1. На узле с self-hosted engine установите ключ smtp-server на нужный адрес SMTP-сервера:

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

Примечание. Чтобы убедиться, что файл конфигурации self-hosted engine был обновлен, выполните:

```
# hosted-engine --get-shared-config smtp-server --type=broker
broker : smtp.example.com, type : broker
```

2. Убедитесь, что порт SMTP по умолчанию (порт 25) настроен:

```
# hosted-engine --get-shared-config smtp-port --type=broker
broker : 25, type : broker
```

3. Укажите адрес электронной почты, который SMTP-сервер должен использовать для отправки уведомлений. Можно указать только один адрес:

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

4. Укажите адрес электронной почты для получения уведомлений пользователем. Чтобы указать несколько адресов электронной почты, разделите каждый адрес запятой:

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

Чтобы убедиться в том, что SMTP правильно настроен для вашей среды виртуализации, измените состояние высокой доступности на узле self-hosted engine и проверьте, были ли отправлены уведомления по электронной почте. Например, вы можете изменить состояние высокой доступности, переведя агенты высокой доступности в режим обслуживания. Дополнительную информацию см. в разделе *Поддержка сервера управления средой виртуализации (Self-Hosted Engine)*.

6.1.2 Настройка слотов памяти, зарезервированных для сервера управления на дополнительных узлах

Если виртуальная машина Engine отключается или ее необходимо перенести, на узле self-hosted engine должно быть достаточно памяти, чтобы виртуальная машина Engine могла перезапуститься или мигрировать на него. Эта память может быть зарезервирована на нескольких собственных узлах ядра с помощью политики планирования. Политика планирования проверяет, останется ли достаточно памяти для запуска виртуальной машины Engine на указанном количестве дополнительных узлов self-hosted engine перед запуском или миграцией любых виртуальных машин. Дополнительную информацию о политиках планирования см. в разделе *Создание политики планирования*.

Чтобы добавить в KeyVirt Engine дополнительные узлы self-hosted engine, см. раздел *Добавление узлов сервера управления в менеджер управления средой виртуализации*.

Для настройки слотов памяти, зарезервированных для Self-Hosted Engine на дополнительных узлах, выполните следующие действия:

1. Нажмите *Виртуализация* > *Кластеры* и выберите необходимый кластер.
2. Нажмите *Изменить*.
3. Перейдите на вкладку *Политика планирования*.
4. Нажмите «+» и выберите HeSparesCount.
5. Введите количество дополнительных узлов Engine, которые будут резервировать достаточно свободной памяти для запуска виртуальной машины Engine.
6. Нажмите OK.

6.1.3 Добавление узлов сервера управления в менеджер управления средой виртуализации

Добавляйте узлы self-hosted engine так же, как обычные узлы, но с дополнительным шагом по развертыванию узла в качестве узла Self-Hosted Engine. Домен общего хранилища определяется автоматически, и узел можно использовать в качестве резервного узла для размещения виртуальной машины Engine, когда это необходимо. Вы также можете подключить стандартные узлы к среде виртуализации, но они не могут размещать виртуальную машину Engine. Нужно как минимум два узла self-hosted engine, чтобы обеспечить высокую доступность виртуальной машины Engine.

Требования:

- Все узлы должны находиться в одном кластере.
- Если вы повторно используете узел self-hosted engine, удалите его существующую конфигурацию. См. подробности в главе *Удаление узла из среды Self-Hosted Engine*.

Для добавления узлов необходимо выполнить следующие действия:

1. На Портале администратора нажмите *Виртуализация* > *Узлы*.
2. Нажмите *Новый*.
3. Используйте раскрывающийся список, чтобы выбрать дата-центр и кластер узлов для нового узла.
4. Введите имя и адрес нового узла. Стандартный порт SSH (порт 22) автоматически заполняется в поле SSH Port.

5. Выберите метод аутентификации, который будет использоваться Engine для доступа к узлу.
   - Введите пароль пользователя root, чтобы использовать аутентификацию по паролю.
   - Либо скопируйте ключ, отображаемый в поле SSH PublicKey в /root/.ssh/authorized_keys, на узле, чтобы использовать аутентификацию с открытым ключом.
6. При необходимости настройте управление питанием, если узел имеет поддерживаемую карту управления питанием.
7. Перейдите на вкладку Hosted Engine.
8. Выберите *Развернуть*.
9. Нажмите OK.

6.1.4 Переустановка существующего узла в качестве узла локального узла Engine Node

Вы можете преобразовать существующий стандартный узел в узел, поддерживающий автономную систему управления, на котором может размещаться виртуальная машина Engine.
Внимание! При установке или переустановке операционной системы узла KeyVirt настоятельно рекомендуем сначала отключить любое существующее хранилище, не относящееся к ОС, которое подключено к узлу, чтобы избежать случайной инициализации этих дисков и потенциальной потери данных.
Процедура:
1. Нажмите *Виртуализация* > *Узлы* и выберите узел.
2. Нажмите *Управление* > *Перейти в режим Обслуживания* и OK.
3. Нажмите *Установка* > *Переустановить*.
4. Перейдите на вкладку Hosted Engine и выберите *Развернуть* в раскрывающемся списке.
5. Нажмите OK.

Хост переустанавливается с конфигурацией собственного ядра и помечается значком короны на Портале администратора.

6.1.5 Загрузка виртуальной машины Engine в режиме восстановления

Для загрузки виртуальной машины Engine в режиме восстановления в случае, когда она не запускается, выполните следующие действия:

1. Подключитесь к одному из узлов hosted-engine:

$ ssh root@host_address

2. Переведите систему в режим глобального обслуживания:

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

3. Проверьте, есть ли уже работающий экземпляр виртуальной машины Engine:

hosted-engine --vm-status
Если экземпляр виртуальной машины Engine запущен, подключитесь к его узлу:
ssh root@host_address

4. Выключите виртуальную машину:

hosted-engine --vm-shutdown
Примечание. Если виртуальная машина не выключается, выполните следующую команду:
hosted-engine --vm-poweroff

5. Запустите виртуальную машину Engine в режиме паузы:

hosted-engine --vm-start-paused

6. Установите временный пароль VNC:

hosted-engine --add-console-password
Команда выводит информацию, необходимую для входа в виртуальную машину Engine с помощью VNC.
7. Войдите в виртуальную машину Engine с помощью VNC. Виртуальная машина Engine все еще приостановлена, поэтому может показаться, что она зависла.
8. Возобновите виртуальную машину Engine с помощью следующей команды на ее узле:

/usr/bin/virsh -c qemu:///system?authfile=/etc/ovirt-hosted-engine/virsh_auth.conf resume HostedEngine
Примечание. После выполнения следующей команды появится меню загрузки. Вам необходимо войти в режим восстановления, прежде чем загрузчик продолжит нормальный процесс загрузки. Ознакомьтесь со следующим шагом по входу в режим восстановления, прежде чем продолжить выполнение данной команды.
9. Загрузите виртуальную машину Engine в режиме восстановления.
10. Отключите режим глобального обслуживания:
hosted-engine --set-maintenance --mode=none
После этого вы можете запускать задачи восстановления на виртуальной машине Engine.

6.1.6 Удаление узла из системы сервера управления средой виртуализации

Чтобы удалить узел из вашей среды, переведите его в режим обслуживания, отмените развертывание и, при необходимости, удалите его. Узлом можно управлять как обычным узлом после того, как службы высокой доступности были остановлены, а файлы конфигурации Self-Hosted Engine были удалены.
Для удаления узла из системы Self-Hosted Engine выполните следующие действия:
1. На Портале администратора нажмите *Виртуализация* > *Узлы* и выберите необходимый узел self-hosted engine.
2. Нажмите *Управление* > *Перейти в режим Обслуживания*, затем нажмите OK.
3. Нажмите *Установка* > *Переустановить*
4. Перейдите на вкладку Hosted Engine и выберите *Удалить* (Undeploy) из раскрывающегося списка. Это действие останавливает службы ovirt-haagent и ovirt-ha-broker и удаляет файл конфигурации Self-Hosted Engine.
5. Нажмите OK.
6. При желании нажмите *Удалить*. Откроется окно подтверждения *Удалить Узел (узлы)*.
7. Нажмите OK.

6.1.7 Обновление сервера управления средой виртуализации

Чтобы обновить систему до актуальной версии, необходимо перевести среду в режим глобального обслуживания, а затем выполнить стандартную процедуру обновления.

6.1.7.1 Включение режима глобального обслуживания

Перед выполнением любых задач по настройке или обновлению на виртуальной машине Engine необходимо перевести систему виртуализации в режим глобального обслуживания.
Для включения режима глобального обслуживания выполните следующие действия:

1. Войдите в один из узлов и включите режим глобального обслуживания командой:

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

2. Прежде чем продолжить, убедитесь, что среда находится в режиме глобального обслуживания:

```
# hosted-engine --vm-status
```

Вы должны будете увидеть сообщение о том, что кластер находится в глобальном режиме обслуживания.

6.1.7.2 Обновление менеджера управления средой виртуализации

Для обновления KeyVirt Engine выполните следующие действия:

1. На машине Engine проверьте, доступны ли пакеты для обновления:

```
# engine-upgrade-check
```

2. Обновите установочные пакеты:

```
# dnf update ovirt\*setup\*
```

3. Обновите KeyVirt Engine с помощью скрипта engine-setup. В рамках выполнения скрипта engine-setup вам будут заданы вопросы по настройке, затем служба ovirt-engine будет остановлена. Будут загружены и установлены обновленные пакеты, а также создана резервная копия и обновлена база данных. После этого выполнится настройка после установки и запустится служба ovirtengine.

```
# engine-setup
```

После успешного завершения скрипта появится следующее сообщение:
Execution of setup completed successfully
Примечание. Скрипт engine-setup также используется в процессе установки HostedEngine и сохраняет указанные значения конфигурации. Во время обновления сохраненные значения отображаются при предварительном просмотре конфигурации и могут оказаться устаревшими, если для обновления конфигурации после установки использовался engine-config. Например, если engine-config использовался для обновления значения параметра SANWipeAfterDelete в «true» после установки, engine-setup в предварительном просмотре конфигурации выведет «SANWipeAfterDelete: False». Однако обновленные значения не будут перезаписаны engine-setup.
Внимание! Процесс обновления может занять некоторое время. Не останавливайте процесс до его завершения.

4. Обновите базовую операционную систему и любые дополнительные пакеты, установленные на Engine:

```
# yum update --nobest
```

Внимание! Если какие-либо пакеты ядра были обновлены:

1. Отключите режим глобального обслуживания.
2. Перезагрузите машину, чтобы завершить обновление.

6.1.7.3 Отключение режима глобального обслуживания

Для отключения режима глобального обслуживания выполните следующие действия:

1. Войдите в виртуальную машину Engine и выключите ее.
2. Войдите в один из узлов системы виртуализации и отключите режим глобального обслуживания:

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

Когда вы выходите из режима глобального обслуживания, ovirt-ha-agent запускает виртуальную машину Engine, после чего Engine автоматически запускается. Запуск Engine может занять до десяти минут.

3. Убедитесь, что среда работает:

```
# hosted-engine --vm-status
```

Перечисленная информация включает статус Engine. Значение для состояния Engine должно быть следующего вида:

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

Примечание. Когда виртуальная машина все еще загружается, а Engine еще не запущен, статус Engine будет следующим:

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

В этом случае подождите несколько минут и повторите попытку.

6.1.8 Изменение полного доменного имени Engine

Для обновления записей полного доменного имени (FQDN) Engine можно использовать команду ovirt-engine-rename.
Инструмент проверяет, предоставляет ли Engine локальный домен ISO или хранилище данных. Если это так, инструмент предлагает пользователю извлечь, выключить или перевести в режим обслуживания любую виртуальную машину или домен хранилища, подключенный к хранилищу, прежде чем продолжить операцию. Это гарантирует, что виртуальные машины не потеряют связь со своими виртуальными дисками, а домены хранения ISO не потеряют связь во время процесса переименования.
Когда команда engine-setup запускается в чистой среде, она создает ряд сертификатов и ключей, в которых используется полное доменное имя Engine, указанное в процессе установки. Если полное доменное имя Engine позднее необходимо изменить (например, из-за переноса машины, на которой размещен Engine, в другой домен), записи полного доменного имени должны быть обновлены, чтобы отразить новое имя. Команда ovirt-engine-rename автоматизирует эту задачу.

6.1.8.1 Описание команды KeyVirt Engine Rename

Когда команда engine-setup запускается в чистой среде, она создает ряд сертификатов и ключей, в которых используется полное доменное имя Engine, указанное в процессе установки. Если полное доменное имя Engine позднее

необходимо изменить (например, из-за переноса машины, на которой размещен Engine, в другой домен), записи полного доменного имени должны быть обновлены, чтобы отразить новое имя. Команда ovirt-engine-rename автоматизирует эту задачу. Команда ovirt-engine-rename обновляет записи полного доменного имени Engine в следующих файлах:

- /etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf;
- /etc/ovirt-engine/logcollector.conf.d/10-engine-setup.conf;
- /etc/pki/ovirt-engine/cert.conf;
- /etc/pki/ovirt-engine/cert.template;
- /etc/pki/ovirt-engine/certs/apache.cer;
- /etc/pki/ovirt-engine/keys/apache.key.nopass;
- /etc/pki/ovirt-engine/keys/apache.p12.

Примечание. Хотя команда ovirt-engine-rename создает новый сертификат для веб-сервера, на котором работает Engine, она не влияет на сертификат для Engine или центр сертификации. В связи с этим использование команды ovirt-engine-rename связано с определенным риском. Поэтому по возможности рекомендуется изменить полное доменное имя Engine, выполнив engine-cleanup и engine-setup.
Примечание. В процессе обновления старое имя узла должно быть разрешено. В некоторых случаях Engine Rename Tool выводит сообщение вида:
[ERROR] Host name is not valid: did not resolve into an IP address
В этом случае добавьте старое имя узла в файл /etc/hosts, используйте Engine Rename Tool, а затем удалите старое имя узла из файла /etc/hosts.

6.1.8.2 Синтаксис команды KeyVirt Engine Rename

Основной синтаксис команды ovirt-engine-rename:
/usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
Команда также принимает следующие параметры:

- --newname= – позволяет указать новое полное доменное имя для Engine без взаимодействия с пользователем;
- --log= – позволяет указать путь и имя файла, в который должны быть записаны журналы операции переименования;
- --config= – позволяет указать путь и имя файла конфигурации для загрузки в операцию переименования;
- --config-append= – позволяет указать путь и имя файла конфигурации для добавления к операции переименования. Этот параметр можно использовать для указания пути и имени существующего файла ответов для автоматизации операции переименования;
- --generate-answer= – позволяет указать путь и имя файла, в который ovirt-engine-rename записываются ваши ответы и значения, измененные командой.

6.1.8.3 Процедура смены доменного имени Engine

1. Подготовьте все DNS и другие соответствующие записи для нового полного доменного имени.
2. Обновите конфигурацию DHCP-сервера, если DHCP используется.
3. Обновите имя узла в Engine.
4. Выполните следующую команду:
/usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
5. При появлении запроса нажмите Enter, чтобы остановить обслуживание Engine:

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

6. При появлении запроса введите новое полное доменное имя для Engine:

New fully qualified server name:new_engine_fqdn
Команда ovirt-engine-rename обновляет записи полного доменного имени Engine.

Для Self-Hosted Engine выполните следующие дополнительные действия:

1. Выполните следующую команду на каждом существующем локальном узле ядра:

hosted-engine --set-shared-config fqdn new_engine_fqdn --type=he_local
Эта команда изменяет полное доменное имя в локальной копии./etc/ovirt-hosted-engine-ha/hosted-engine.conf на каждом узле self-hosted engine.

2. Выполните следующую команду на одном из узлов self-hosted engine:

hosted-engine --set-shared-config fqdn new_engine_fqdn --type=he_shared
Эта команда изменяет полное доменное имя в основной копии /etc/ovirt-hosted-engine-ha/hosted-engine.conf в общем домене хранения.

Теперь все новые и существующие узлы self-hosted engine используют новое полное доменное имя.

Примечание. Инструмент переименования KeyVirt Engine предназначен для работы только на локальных машинах. Изменение имени Engine не приводит к автоматическому обновлению имени на удаленных компьютерах хранилища данных. Изменение имен на удаленных машинах СХД необходимо выполнять вручную.

Для удаленного развертывания хранилища данных выполните следующие действия на удаленном компьютере (не на компьютере Engine):

1. Удалите следующие файлы PKI:

/etc/pki/ovirt-engine/apache-ca.pem /etc/pki/ovirt-engine/apache-grafana-ca.pem /etc/pki/ovirt-engine/certs/* /etc/pki/ovirt-engine/keys/*

2. В следующих файлах обновите полное доменное имя Engine на новое имя (например, vm-new-name.local_lab_server.redhat.com):

/etc/grafana/grafana.ini /etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-database.conf /etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf

3. Запустите engine-setup с offline-переключателем, чтобы предотвратить обновления в это время:

engine-setup --offline

6.2 РЕЗЕРВНЫЕ КОПИИ И МИГРАЦИЯ

6.2.1 Резервное копирование и восстановление менеджера управления средой виртуализации

Используйте инструмент engine-backup для регулярного создания резервных копий Engine. Инструмент создает резервную копию базы данных Engine и файлов конфигурации в один файл, и его можно запускать, не прерывая работу службы ovirt-engine.

6.2.1.1 Синтаксис команды engine-backup

Команда engine-backup работает в одном из двух основных режимов:
engine-backup --mode=backup
engine-backup --mode=restore
Эти два режима дополнительно расширены набором параметров, которые позволяют указать область резервного копирования и различные учетные данные для базы данных Engine. Запустите engine-backup –help для получения полного списка параметров и их функции.

Основные параметры

- --mode

Указывает, будет ли команда выполнять операцию резервного копирования или операцию восстановления. Доступны два варианта – backup и restore. Это обязательный параметр.

- --file

Указывает путь и имя файла, в который должны быть сохранены резервные копии в режиме резервного копирования, а также путь и имя файла, из которого считываются данные резервной копии в режиме восстановления. Это обязательный параметр как в режиме резервного копирования, так и в режиме восстановления.

- --log

Указывает путь и имя файла, в который должны быть записаны журналы операции резервного копирования или восстановления. Этот параметр необходим как в режиме резервного копирования, так и в режиме восстановления.

- --scope

Указывает область операции резервного копирования или восстановления. Существует четыре варианта: all, который выполняет резервное копирование или восстановление всех баз данных и данных конфигурации; files, который создает резервные копии или восстанавливает только файлы в системе; db, который выполняет резервное копирование или восстановление только базы данных Engine; и dwhdb, который выполняет резервное копирование или восстановление только базы данных хранилища данных. Область действия по умолчанию – all. Параметр --scope может быть указан несколько раз в одной и той же engine-backup-команде.

6.2.1.2 Параметры базы данных Engine

Следующие параметры доступны только при использовании команды engine-backup в режиме restore. Приведенный ниже синтаксис параметра применим к восстановлению базы данных Engine. Те же параметры существуют для восстановления базы данных хранилища данных.

- --provision-db

Создает базу данных PostgreSQL для восстановления резервной копии базы данных ядра. Это обязательный параметр при восстановлении резервной копии на удаленном узле или при новой установке, для которой еще не настроена база данных PostgreSQL. Когда эта опция используется в режиме восстановления, опция --restore-permissions добавляется по умолчанию.

- --provision-all-databases

Создает базы данных для всех дампов памяти, включенных в архив. Если включено, это значение используется по умолчанию.

- --change-db-credentials

Позволяет указать альтернативные учетные данные для восстановления базы данных Engine, используя учетные данные, отличные от тех, которые хранятся в самой резервной копии.

- --restore-permissions или --no-restore-permissions

Восстанавливает или не восстанавливает разрешения пользователей базы данных. Один из этих параметров необходим при восстановлении резервной копии. Когда опция --provision-* используется в режиме восстановления, --restore-permissions применяется по умолчанию.

Примечание. Если резервная копия содержит разрешения для дополнительных пользователей базы данных, восстановление резервной копии с помощью опций --restore-permissions и --provision-db (или --provision-dwh-db) создает дополнительных пользователей со случайными паролями. Вы должны изменить эти пароли вручную, если дополнительным пользователям требуется доступ к восстановленной системе.

6.2.1.3 Создание резервной копии с помощью команды engine-backup

Вы можете создать резервную копию KeyVirt Engine с помощью команды engine-backup, пока Engine активен. Добавьте одно из следующих значений к параметру --scope, чтобы указать, что вы хотите создать резервную копию:

- all

Полная резервная копия всех баз данных и файлов конфигурации на Engine. Это значение по умолчанию для параметра --scope.

- files

  Резервное копирование только файлов в системе

- db

  Резервная копия только базы данных Engine

- dwhdb

  Резервное копирование только базы данных хранилища данных

- cinderlibdb

  Резервная копия только базы данных Cinderlib

- grafanadb

  Резервная копия только базы данных Grafana

  Вы можете указать параметр --scope несколько раз.

Вы также можете настроить команду engine-backup для резервного копирования дополнительных файлов. Оно восстанавливает все, что создает резервные копии.

Внимание! Для восстановления базы данных при новой установке KeyVirt Engine одной резервной копии базы данных недостаточно. Engine также требуется доступ к

файлам конфигурации. Если вы укажете область, отличную от all, вы также должны включить файловую систему --scope=files или создать резервную копию.
Для полного объяснения команды engine-backup введите engine-backup --help на машине Engine.
Процедура:

1. Войдите в систему на компьютере Engine.
2. Создайте резервную копию:
   # engine-backup

По умолчанию применяются следующие настройки:
--scope=all
--mode=backup

Команда создает резервную копию в /var/lib/ovirt-engine-backup/file_name.backup и файл журнала в /var/log/ovirt-engine-backup/log_file_name.

Используйте file_name.tar для восстановления среды.

6.2.1.4 Восстановление резервной копии с помощью команды engine-backup

Восстановление резервной копии с помощью команды engine-backup включает в себя больше шагов, чем создание резервной копии, в зависимости от назначения восстановления. Например, команда engine-backup может использоваться для восстановления резервных копий при новых установках KeyVirt поверх существующих установок KeyVirt и с использованием локальных или удаленных баз данных.

6.2.1.5 Восстановление резервной копии для новой установки

Команда engine-backup может использоваться для восстановления резервной копии новой установки Engine. Следующую процедуру необходимо выполнить на компьютере, на котором установлена базовая операционная система и установлены необходимые пакеты для Engine, но команда engine-setup еще не была запущена. Эта процедура предполагает, что к файлу или файлам резервной копии можно получить доступ с компьютера, на котором резервная копия должна быть восстановлена.

Процедура:

1. Войдите в систему на ВМ Engine. Если вы восстанавливаете базу данных Engine на удаленном узле, вам необходимо будет войти в систему и выполнить соответствующие действия на этом узле. Аналогично, при восстановлении хранилища данных на удаленном узле вам необходимо будет войти в систему и выполнить соответствующие действия на этом узле.
2. Восстановите полную резервную копию или резервную копию только для базы данных.
   - Восстановите полную резервную копию:
     # engine-backup --mode=restore --file=file_name --log=log_file_name --provision-db

Когда опция --provision-* используется в режиме восстановления, --restore-permissions применяется по умолчанию.
Если хранилище данных также восстанавливается как часть полной резервной копии, подготовьте дополнительную базу данных:
engine-backup --mode=restore --file=file_name --log=log_file_name --provision-db --provision-dwh-db

- Восстановите резервную копию только для базы данных, восстановив файлы конфигурации и резервную копию базы данных:

  # engine-backup --mode=restore --scope=files --scope=db --file=file_name --log=log_file_name --provision-db

Приведенный выше пример восстанавливает резервную копию базы данных Engine.
engine-backup --mode=restore --scope=files --scope=dwhdb --file=file_name --log=log_file_name --provision-dwh-db
Приведенный выше пример восстанавливает резервную копию базы данных хранилища данных.
В случае успеха отобразятся следующие выходные данные:
You should now run engine-setup.
Done.

3. Выполните следующую команду и следуйте подсказкам, чтобы настроить восстановленный Engine:

   # engine-setup

KeyVirt Engine был восстановлен до версии, сохраненной в резервной копии.

6.2.1.6 Восстановление резервной копии для перезаписи существующей установки

Команда engine-backup может восстановить резервную копию на ВМ, на которой уже установлен и настроен Engine. Это полезно, когда вы создали резервную копию среды, выполнили изменения в этой среде, а затем хотите отменить изменения, восстановив среду из резервной копии.

Изменения, внесенные в среду с момента создания резервной копии, такие как добавление или удаление узла, не появятся в восстановленной среде. Вы должны повторить эти изменения.

Процедура:

1. Войдите в систему на ВМ Engine.
2. Удалите файлы конфигурации и очистите базу данных, связанную с Engine:
   # engine-cleanup

Команда engine-cleanup только очищает базу данных Engine; она не удаляет базу данных или пользователя, которому принадлежит эта база данных.

3. Восстановите полную резервную копию или резервную копию только для базы данных. Вам не нужно создавать новую базу данных или указывать учетные данные базы данных, поскольку пользователь и база данных уже существуют.
   - Восстановите полную резервную копию:

engine-backup --mode=restore --file=file_name --log=log_file_name --restore-permissions

- Восстановите резервную копию только для базы данных, восстановив файлы конфигурации и резервную копию базы данных:

engine-backup --mode=restore --scope=files --scope=db --scope=dwhdb --file=file_name --log=log_file_name --restore-permissions
Чтобы восстановить только базу данных Engine (например, если база данных хранилища данных расположена на другом компьютере), вы можете опустить параметр --scope=dwhdb.
В случае успеха отобразятся следующие выходные данные:

You should now run engine-setup.
Done.

4. Перенастройте Engine:

engine-setup

6.2.1.7 Восстановление резервной копии с другими учетными данными

Команда engine-backup может восстановить резервную копию на компьютере, на котором уже установлен и настроен Engine, но учетные данные базы данных в резервной копии отличаются от учетных данных базы данных на компьютере, на котором должна быть восстановлена резервная копия. Это полезно, когда вы сделали резервную копию установки и хотите восстановить установку из резервной копии в другую систему.
Внимание! При восстановлении резервной копии для перезаписи существующей установки необходимо выполнить команду engine-cleanup для очистки существующей установки перед использованием команды engine-backup. Команда engine-cleanup только очищает базу данных Engine и не удаляет базу данных или пользователя, которому принадлежит эта база данных. Таким образом, вам не нужно создавать новую базу данных или указывать учетные данные базы данных. Однако, если учетные данные владельца базы данных ядра неизвестны, вы должны изменить их, прежде чем сможете восстановить резервную копию.
Процедура:

1. Войдите на компьютер Engine.
2. Выполните следующую команду и следуйте инструкциям, чтобы удалить файлы конфигурации ядра и очистить базу данных Engine:
   # engine-cleanup
3. Измените пароль для владельца базы данных engine, если учетные данные этого пользователя неизвестны:
   - Введите в командную строку postgresql:
     # su – postgres -c 'psql'
   - Измените пароль пользователя, которому принадлежит база данных engine:
     postgres=# alter role user_name encrypted password 'new_password';

При необходимости повторите это для пользователя, которому принадлежит база данных ovirt_engine_history.

4. Восстановите полную резервную копию или резервную копию только для базы данных с параметром --change-db-credentials для передачи учетных данных новой базы данных. A database_location для базы данных, локальной для Engine, является localhost.

Примечание. В следующих примерах используется опция --*password для каждой базы данных без указания пароля, которая запрашивает пароль для каждой базы данных. Кроме того, вы можете использовать параметры --*passfile=password_file для каждой базы данных, чтобы безопасно передавать пароли инструменту engine-backup без необходимости в интерактивных подсказках.

- Восстановите полную резервную копию:

```
# engine-backup --mode=restore --file=file_name --log=log_file_name --change-db-credentials --db-host=database_location --db-name=database_name --db-user=engine --db-password --no-restore-permissions
```

Если хранилище данных также восстанавливается как часть полной резервной копии, включите измененные учетные данные для дополнительной базы данных:

```
engine-backup --mode=restore --file=file_name --log=log_file_name --change-db-credentials --db-host=database_location --db-name=database_name --db-user=engine --db-password --change-dwh-db-credentials --dwh-db-host=database_location --dwh-db-name=database_name --dwh-db-user=ovirt_engine_history --dwh-db-password --no-restore-permissions
```

- Восстановите резервную копию только для базы данных, восстановив файлы конфигурации и резервную копию базы данных:

```
# engine-backup --mode=restore --scope=files --scope=db --file=file_name --log=log_file_name --change-db-credentials --db-host=database_location --db-name=database_name --db-user=engine --db-password --no-restore-permissions
```

Приведенный выше пример восстанавливает резервную копию базы данных Engine.

```
# engine-backup --mode=restore --scope=files --scope=dwhdb --file=file_name --log=log_file_name --change-dwh-db-credentials --dwh-db-host=database_location --dwh-db-name=database_name --dwh-db-user=ovirt_engine_history --dwh-db-password --no-restore-permissions
```

Приведенный выше пример восстанавливает резервную копию базы данных хранилища данных.

В случае успеха отобразятся следующие выходные данные:

```
You should now run engine-setup.
Done.
```

5. Выполните следующую команду и следуйте инструкциям, чтобы перенастроить брандмауэр и убедиться, что служба ovirt-engine настроена правильно:

```
# engine-setup
```

6.2.1.8 Резервное копирование и восстановление Self-Hosted Engine

Вы можете создать резервную копию Self-Hosted Engine и восстановить его в новой автономной среде. Используйте эту процедуру для таких задач, как перенос среды в новый автономный домен хранилища Engine с другим типом хранилища.

Когда вы указываете файл резервной копии во время развертывания, резервная копия восстанавливается на новой виртуальной машине Engine с новым автономным доменом хранения Engine. Старый Engine удален, а старый автономный домен хранилища Engine переименован и может быть удален вручную после подтверждения корректной работы новой среды. Настоятельно рекомендуется развертывание на новом узле. Если узел, используемый для развертывания, существовал в резервной среде, он будет удален из восстановленной базы данных, чтобы избежать конфликтов в новой среде. При развертывании на новом узле необходимо присвоить узлу уникальное имя. Повторное использование имени существующего узла, включенного в резервную копию, может вызвать конфликты в новой среде.

Операция резервного копирования и восстановления включает следующие шаги:

1. Создание резервной копии исходного Engine с помощью engine-backup.
2. Развертывание нового Self-Hosted Engine и восстановление резервной копии.

3. Включение репозиториев Engine на новой виртуальной машине Engine.
4. Переустановка узлов Engine, чтобы обновить их конфигурацию.
5. Удаление старого домена хранилища Self-Hosted Engine.

Эта процедура предполагает, что у вас есть доступ и вы можете вносить изменения в исходный Engine.

Требования:

- Полное доменное имя, подготовленное для вашего Engine и хостинга. В DNS должны быть установлены записи прямого и обратного поиска. Новый Engine должен иметь то же полное доменное имя, что и исходный Engine.
- Уровень совместимости дата-центра должен быть установлен на последнюю версию, чтобы обеспечить совместимость с обновленной версией хранилища.
- В среде должен быть хотя бы один постоянный узел. Этот узел (и любые другие обычные узлы) останется активным для размещения роли SPM и любых запущенных виртуальных машин. Если обычный узел еще не является SPM, переместите роль SPM перед созданием резервной копии, выбрав обычный узел и нажав *Управление* > *Выбрать как SPM*.

  Если обычные узлы недоступны, есть два способа добавить один:
- Удалите конфигурацию Self-Hosted Engine с узла (но не удаляйте узел из среды).
- Добавьте новый постоянный узел.

6.2.1.9 Резервное копирование исходного Engine

Создайте резервную копию исходного Engine с помощью команды engine-backup и скопируйте файл резервной копии в отдельное расположение, чтобы к нему можно было получить доступ в любой момент процесса.

Процедура:

1. Войдите в систему на одном из узлов self-hosted engine и переведите среду в режим глобального обслуживания:
   # hosted-engine --set-maintenance --mode=global
2. Войдите в исходный Engine и остановите службу ovirt-engine:
   # systemctl stop ovirt-engine
   # systemctl disable ovirt-engine

Хотя остановка запуска исходного Engine не обязательна, это рекомендуется, поскольку это гарантирует отсутствие изменений в среде после создания резервной копии. Кроме того, это не позволяет исходному Engine и новому Engine одновременно управлять существующими ресурсами.

3. Выполните команду engine-backup, указав имя файла резервной копии, который нужно создать, и имя файла журнала, который нужно создать для хранения журнала резервной копии:
   # engine-backup --mode=backup --file=file_name --log=log_file_name
4. Скопируйте файлы на внешний сервер. В следующем примере storage.example.com – это полное доменное имя сервера сетевого хранилища, на котором будет храниться резервная копия до тех пор, пока она не понадобится, и /backup/ – любая указанная папка или путь.
   # scp -p file_name log_file_name storage.example.com:/backup/
5. Войдите в систему на одном из автономных узлов Engine и завершите работу исходной виртуальной машины Engine:
   # hosted-engine --vm-shutdown

После создания резервной копии ядра разверните новое self-hosted engine и восстановите резервную копию на новой виртуальной машине.

6.2.1.10 Восстановление резервной копии на новом Self-Hosted Engine

Запустите скрипт hosted-engine на новом узле и используйте опцию --restore-from-file=path/to/file_name для восстановления резервной копии Engine во время развертывания.

Внимание! Если вы используете хранилище iSCSI, а ваш целевой iSCSI фильтрует соединения в соответствии с ACL инициатора, развертывание может завершиться с ошибкой STORAGE_DOMAIN_UNREACHABLE. Чтобы предотвратить это, необходимо обновить конфигурацию iSCSI перед началом развертывания автономного ядра:

- При повторном развертывании на существующем узле необходимо обновить настройки инициатора iSCSI узла в /etc/iscsi/initiatorname.iscsi. IQN инициатора должен совпадать с тем, который ранее был сопоставлен с целевым объектом iSCSI, или обновлен до нового IQN, если это применимо.
- При развертывании на новом узле необходимо обновить целевую конфигурацию iSCSI, чтобы принимать подключения с этого узла.

Обратите внимание, что IQN может быть обновлен на стороне узла (инициатор iSCSI) или на стороне хранилища (целевой iSCSI).

Процедура:

1. Скопируйте файл резервной копии на новый узел. В следующем примере host.example.com – это полное доменное имя узла, а /backup/ – любая указанная папка или путь:
   # scp -p file_name host.example.com:/backup/
2. Войдите на новый узел.
3. Если вы выполняете развертывание на узле KeyVirt, ovirt-hosted-engine-setup уже установлен, поэтому пропустите этот шаг. При развертывании в Enterprise Linux установите ovirt-hosted-engine-setup пакет:
   # dnf install ovirt-hosted-engine-setup
4. Используйте оконный менеджер tmux для запуска скрипта, чтобы избежать потери сеанса в случае сбоя в работе сети или терминала.

Установите и запустите tmux:

```
# dnf -y install tmux
# tmux
```

5. Запустите скрипт hosted-engine, указав путь к файлу резервной копии:
   # hosted-engine --deploy --restore-from-file=backup/file_name

Чтобы в любой момент выйти из скрипта, используйте CTRL+D для прерывания развертывания.

6. Выберите Yes, чтобы начать развертывание.
7. Настройте сеть. Скрипт определяет возможные сетевые адаптеры для использования в качестве моста управления средой.
8. Если вы хотите использовать пользовательское устройство для установки виртуальной машины, введите путь к архиву OVA. В противном случае оставьте это поле пустым, чтобы использовать устройство Engine.
9. Введите пароль root для Engine.

10. Введите открытый ключ SSH, который позволит вам войти в Engine как пользователь root, и укажите, следует ли разрешать доступ SSH для пользователя root.
11. Введите конфигурацию процессора и памяти виртуальной машины.
12. Введите MAC-адрес для виртуальной машины Engine или примите случайно сгенерированный. Если вы хотите предоставить виртуальной машине ядра IP-адрес через DHCP, убедитесь, что у вас есть действительное резервирование DHCP для этого MAC-адреса. Сценарий развертывания не будет настраивать DHCP-сервер для вас.
13. Введите сведения о сети виртуальной машины. Если вы указываете Static, введите IP-адрес Engine.
    Внимание! Статический IP-адрес должен принадлежать к той же подсети, что и узел. Например, если узел находится в версии 10.1.1.0 /24, IP-адрес виртуальной машины ядра должен находиться в том же диапазоне подсети (10.1.1.1-254/24).
14. Укажите, следует ли добавлять записи для виртуальной машины Engine и базового узла в /etc/hosts файл виртуальной машины. Вы должны убедиться, что имена узлов разрешимы.
15. Укажите имя и номер TCP-порта SMTP-сервера, адрес электронной почты, используемый для отправки уведомлений по электронной почте, и разделенный запятыми список адресов электронной почты для получения этих уведомлений:
16. Введите пароль для пользователя admin@internal для доступа к Порталу администратора.

Скрипт создает виртуальную машину. Это может занять некоторое время, если необходимо установить устройство Engine.

Если узел становится неработоспособным из-за отсутствия необходимой сети или подобной проблемы, развертывание приостанавливается и отображается сообщение, подобное следующему:

[INFO] You can now connect to https://<host name>:6900/ovirt-engine/ and check the status of this host and eventually remediate it, please continue only when the host is listed as 'up'
[INFO] TASK [ovirt.ovirt.hosted_engine_setup : include_tasks]
[INFO] ok: [localhost]
[INFO] TASK [ovirt.ovirt.hosted_engine_setup : Create temporary lock file]
[INFO] changed: [localhost]
[INFO] TASK [ovirt.ovirt.hosted_engine_setup : Pause execution until /tmp/ansible.<random>_he_setup_lock is removed, delete it once ready to proceed]

Приостановка процесса позволяет:

- Подключиться к Порталу администратора, используя указанный URL.
- Оценить ситуацию, выяснить, почему узел не работает, и исправить все, что необходимо. Например, если это развертывание было восстановлено из резервной копии, и резервная копия включала необходимые сети для кластера узлов, можно настроить сети, подключив к этим сетям соответствующие сетевые адаптеры узла.
- Как только все будет выглядеть нормально и статус узла повышен, можно удалить файл блокировки, представленный в сообщении выше. Развертывание продолжается.

17. Выберите тип используемого хранилища:

- Для NFS введите версию, полный адрес и путь к хранилищу, а также любые параметры подключения.
  Примечание. Не используйте точку подключения старого домена хранение Engine для нового домена хранения, так как вы рискуете потерять данные виртуальной машины.
- Для iSCSI введите сведения о Портале и выберите цель и LUN из автоматически определяемых списков. Во время развертывания можно выбрать только один целевой объект iSCSI, но для подключения всех Порталов одной группы Порталов поддерживается многолучевость.
  Чтобы указать более одного целевого объекта iSCSI, необходимо включить многопутевую передачу перед развертыванием self-hosted engine. Существует также инструмент Multipath Helper, который генерирует скрипт для установки и настройки multipath с различными опциями.
- Для Fibre Channel выберите LUN из автоматически определяемого списка. Адаптеры шины узла должны быть настроены и подключены, а LUN не должен содержать никаких существующих данных.

18. Введите размер диска Engine.

Выполнение сценария продолжается до завершения развертывания.

19. В процессе развертывания изменяются SSH-ключи Engine. Чтобы клиентские компьютеры могли получать доступ к новому Engine без ошибок SSH, удалите запись исходного Engine из файла .ssh/known_hosts на всех клиентских компьютерах, которые обращались к исходному Engine.

По завершении развертывания войдите в систему на виртуальной машине new Engine и включите необходимые репозитории.

6.2.1.11 Включение репозиториев Engine

В Enterprise Linux 8 вы можете проверить, какие репозитории в данный момент включены, выполнив dnf repolist.

1. Включите модуль javapackages-tools:
   # dnf module -y enable javapackages-tools
2. Включите модуль pki-deps:
   # dnf module -y enable pki-deps
3. Включите версию 12 модуля postgresql:
   # dnf module -y enable postgresql:12
4. Включите версию 2.3 модуля mod_auth_openidc:
   # dnf module -y enable mod_auth_openidc:2.3
5. Включите версию 14 модуля nodejs:
   # dnf module -y enable nodejs:14
6. Синхронизируйте установленные пакеты, чтобы обновить их до последних доступных версий.
   # dnf distro-sync --nobest

Engine и его ресурсы теперь работают в новой автономной среде. Узлы Self-Hosted Engine необходимо переустановить в Engine, чтобы обновить их конфигурацию Self-Hosted Engine. Стандартные узлы не затронуты. Выполните процедуру, описанную в следующем разделе, для каждого узла автономного ядра.

6.2.1.12 Переустановка узлов

Переустановите узлы KeyVirt (KeyVirt Node) и узлы Enterprise Linux с Портала администратора. Процедура включает в себя остановку и перезапуск узла.
Примечание. При установке или переустановке операционной системы узла KeyVirt настоятельно рекомендует сначала отсоединить все существующие хранилища, не связанные с операционной системой, которые подключены к узлу, чтобы избежать случайной инициализации этих дисков и, как следствие, потенциальной потери данных.
Требования:

- Если в кластере включена миграция, виртуальные машины могут автоматически мигрировать на другой узел в кластере. Поэтому переустановите узел, пока его использование относительно невелико.
- Убедитесь, что в кластере достаточно памяти для выполнения обслуживания его узлами. Если в кластере не хватает памяти, миграция виртуальных машин зависнет, а затем завершится сбоем. Чтобы уменьшить использование памяти, выключите некоторые или все виртуальные машины перед переводом узла на обслуживание.
- Перед выполнением переустановки убедитесь, что кластер содержит более одного узла. Не пытайтесь переустановить все узлы одновременно. Один узел должен оставаться доступным для выполнения задач диспетчера пула хранения (SPM).

Процедура:

1. Нажмите *Виртуализация* > *Узлы* и выберите узел.
2. Нажмите *Управление* > *Перейти в режим Обслуживания* и OK.
3. Нажмите *Установка* > *Переустановить*. Откроется окно *Установка Узла*.
4. Перейдите на вкладку Hosted Engine и выберите *Развернуть* из выпадающего списка.
5. Нажмите OK, чтобы переустановить узел.

После переустановки узла и возвращения его статуса на Up вы можете перенести виртуальные машины обратно на узел.
Внимание! После регистрации узла KeyVirt в KeyVirt Engine и его переустановки Портал администратора может ошибочно отобразить его статус как Install Failed. Нажмите *Управление* > *Выйти из режима Обслуживания*, и узел перейдет в статус Up и будет готов к использованию.
После переустановки узлов автономного ядра вы можете проверить состояние новой среды, выполнив следующую команду на одном из узлов:
hosted-engine --vm-status
Во время восстановления старый домен хранения self-hosted engine был переименован, но не был удален из новой среды на случай, если восстановление было ошибочным. После подтверждения того, что среда работает нормально, вы можете удалить старый домен хранения self-hosted engine.

6.2.1.13 Удаление домена хранения

Если в вашем дата-центре есть домен хранения, который вы хотите удалить из виртуальной среды, вы можете это сделать, выполнив следующую процедуру:

1. Нажмите *Хранилище* > *Домены*.
2. Переведите домен хранилища в режим обслуживания и отсоедините его:
    1. Нажмите имя домена хранилища. Откроется окно сведений.

2. Нажмите на вкладку *Дата Центр*.
3. Нажмите *Перейти в режим Обслуживания*, затем нажмите OK.
4. Нажмите *Отсоединить*, затем нажмите OK.

3. Нажмите *Удалить*.
4. При необходимости установите флажок *Форматирование домена, т.е. содержимое хранилища будет потеряно!*, чтобы удалить содержимое домена.
5. Нажмите OK.

Домен хранения безвозвратно удален из среды.

6.2.1.14 Восстановление Self-Hosted Engine из существующей резервной копии

Если Self-Hosted Engine недоступен из-за проблем, которые невозможно устранить, вы можете восстановить его в новой среде, используя резервную копию, сделанную до возникновения проблемы, если таковая имеется.
Восстановление Self-Hosted Engine включает в себя следующие ключевые действия:

1. Развертывание нового Self-Hosted Engine и восстановление резервной копии.
2. Включение репозиториев Engine на новой виртуальной машине Engine.
3. Переустановка узлов self-hosted engine, чтобы обновить их конфигурацию.
4. Удаление старого домена хранилища Engine.

Эта процедура предполагает, что у вас нет доступа к исходному Engine и что новый узел может получить доступ к файлу резервной копии.
Требования:

- Полное доменное имя, подготовленное для вашего Engine и хостинга. В DNS должны быть установлены записи прямого и обратного поиска. Новый Engine должен иметь то же полное доменное имя, что и исходный Engine.

Подробности по шагам *Восстановление резервной копии на новом Self-Hosted Engine*, *Переустановка узлов* и *Удаление домена хранения* см. выше в главе *Резервное копирование и восстановление Self-Hosted Engine.*

6.2.1.15 Перезапись Self-Hosted Engine из существующей резервной копии

Если Self-Hosted Engine доступен, но возникает проблема, такая как повреждение базы данных или ошибка конфигурации, которую трудно откатить, вы можете восстановить среду до предыдущего состояния, используя резервную копию, сделанную до возникновения проблемы, если таковая имеется.
Восстановление предыдущего состояния Self-Hosted Engine включает в себя следующие шаги:

1. Перевод среды в режим глобального обслуживания.
2. Восстановление резервной копии на виртуальной машине Engine.
3. Отключение режима глобального обслуживания.

Для дополнительной информации о параметрах engine-backup --mode=restore см. *Резервное копирование и восстановление Engine*.

6.2.1.16 Включение режима глобального обслуживания

Вы должны перевести среду Self-Hosted Engine в режим глобального обслуживания перед выполнением любых задач настройки или обновления на виртуальной машине Engine.
Процедура:

1. Войдите в систему на одном из узлов self-hosted engine и включите режим глобального обслуживания:
   # hosted-engine --set-maintenance --mode=global
2. Прежде чем продолжить, убедитесь, что среда находится в режиме глобального обслуживания:
   # hosted-engine --vm-status

Вы должны увидеть сообщение, указывающее, что кластер находится в режиме глобального обслуживания.

6.2.1.17 Восстановление резервной копии для перезаписи существующей установки

Команда engine-backup может восстановить резервную копию на компьютере, на котором уже установлен и настроен Engine. Это полезно, когда вы создали резервную копию среды, выполнили изменения в этой среде, а затем хотите отменить изменения, восстановив среду из резервной копии.
Изменения, внесенные в среду с момента создания резервной копии, такие как добавление или удаление узла, не появятся в восстановленной среде. Вы должны повторить эти изменения.
Процедура:

1. Войдите в систему на компьютере Engine.
2. Удалите файлы конфигурации и очистите базу данных, связанную с Engine:
   # engine-cleanup

Команда engine-cleanup только очищает базу данных Engine; она не удаляет базу данных или пользователя, которому принадлежит эта база данных.

3. Восстановите полную резервную копию или резервную копию только для базы данных. Вам не нужно создавать новую базу данных или указывать учетные данные базы данных, поскольку пользователь и база данных уже существуют.
   - Восстановите полную резервную копию:
     # engine-backup --mode=restore --file=file_name --log=log_file_name --restore-permissions
   - Восстановите резервную копию только для базы данных, восстановив файлы конфигурации и резервную копию базы данных:
     # engine-backup --mode=restore --scope=files --scope=db --scope=dwhdb --file=file_name --log=log_file_name --restore-permissions

Чтобы восстановить только базу данных Engine (например, если база данных хранилища данных расположена на другом компьютере), вы можете опустить параметр --scope=dwhdb.
В случае успеха отобразятся следующие выходные данные:

You should now run engine-setup.
Done.

4. Перенастройте Engine:
   # engine-setup

6.2.1.18 Отключение режима глобального обслуживания

Процедура:

1. Войдите в виртуальную машину Engine и выключите ее.

2. Войдите в систему на одном из узлов Self-Hosted Engine и отключите режим глобального обслуживания:
   # hosted-engine --set-maintenance --mode=none

При выходе из режима глобального обслуживания ovirt-ha-agent запускает виртуальную машину Engine, а затем Engine запускается автоматически. Запуск Engine может занять до десяти минут.

3. Подтвердите, что среда запущена:
   # hosted-engine --vm-status

Приведенная информация включает в себя состояние двигателя. Значение Engine status должно быть:
{"health": "good", "vm": "up", "detail": "Up"}
Когда виртуальная машина все еще загружается, а Engine еще не запущен, Engine status следующий:
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
Если это произойдет, подождите несколько минут и повторите попытку.

Когда среда снова будет запущена, вы сможете запустить все виртуальные машины, которые были остановлены, и проверить, что ресурсы в среде работают должным образом.

6.2.2 Резервное копирование и восстановление виртуальных машин с помощью домена хранилища резервных копий

Домен хранилища резервных копий – это домен, который вы можете использовать специально для хранения и переноса виртуальных машин и шаблонов виртуальных машин с целью резервного копирования и восстановления для аварийного восстановления, миграции или любой другой модели использования резервного копирования или восстановления. Резервный домен отличается от домена без резервного копирования тем, что все виртуальные машины в резервном домене находятся в отключенном состоянии. Виртуальная машина не может работать в резервном домене.
Вы можете настроить любой домен хранения данных в качестве резервного домена. Вы можете включить или отключить этот параметр, установив или сняв флажок в диалоговом окне *Управление доменом*. Вы можете включить этот параметр только после того, как все виртуальные машины в этом домене хранения будут остановлены.
Вы не можете запустить виртуальную машину, хранящуюся в резервном домене. Менеджер блокирует эту и любую другую операцию, которая может привести к аннулированию резервной копии. Однако вы можете запустить виртуальную машину на основе шаблона, хранящегося в резервном домене, если диски виртуальной машины не являются частью резервного домена.
Как и в случае с другими типами доменов хранения, вы можете присоединять или отсоединять резервные домены к дата-центру или из дата-центра. Таким образом, в дополнение к хранению резервных копий, вы можете использовать резервные домены для переноса виртуальных машин между дата-центрами.

Преимущества

Ниже перечислены некоторые причины использования резервного домена, а не домена экспорта:

- В дата-центре может быть несколько доменов для хранения резервных копий, в отличие от только одного домена экспорта.

- Вы можете выделить домен хранилища резервных копий для резервного копирования и аварийного восстановления.
- Вы можете перенести резервную копию виртуальной машины, шаблона или моментального снимка в домен хранилища резервных копий
- Перенос большого количества виртуальных машин, шаблонов или файлов OVF с резервными доменами выполняется значительно быстрее, чем с доменами экспорта.
- Резервный домен использует дисковое пространство более эффективно, чем домен экспорта.
- Резервные домены поддерживают как файловое хранилище (NFS), так и блочное хранилище (Fibre Channel и iSCSI). Это отличается от доменов экспорта, которые поддерживают только файловое хранилище.
- Вы можете динамически включать и отключать настройку резервного копирования для домена хранения, принимая во внимание ограничения.

Ограничения:

- Любая виртуальная машина или шаблон в домене _backup должны хранить все свои диски в этом же домене.
- Все виртуальные машины в домене хранения должны быть выключены, прежде чем вы сможете настроить его в качестве резервного домена.
- Вы не можете запустить виртуальную машину, которая хранится в резервном домене, поскольку это может привести к манипулированию данными на диске.
- Резервный домен не может быть целевым для томов памяти, поскольку тома памяти поддерживаются только для активных виртуальных машин.
- Вы не можете просмотреть виртуальную машину в резервном домене.
- Оперативная миграция виртуальной машины в резервный домен невозможна.
- Вы не можете установить резервный домен в качестве master домена.
- Вы не можете настроить домен self-hosted engine в качестве резервного домена.
- Не используйте домен хранилища по умолчанию в качестве резервного домена.

6.2.2.1 Настройка домена хранения данных в качестве резервного домена

Требования:

- Все диски, принадлежащие виртуальной машине или шаблону в домене хранения, должны находиться в одном домене.
- Все виртуальные машины в домене должны быть выключены.

Процедура:

1. На Портале администратора выберите *Хранилище* > *Домены*.
2. Создайте новый домен хранения или выберите существующий домен хранения и нажмите *Управление доменом*. Откроется диалоговое окно *Управление доменом*.
3. В разделе *Дополнительные параметры* установите флажок *Резервная копия*.

Теперь домен является резервным.

6.2.2.2 Резервное копирование или восстановление виртуальной машины или моментального снимка с использованием резервного домена

Вы можете создать резервную копию отключенной виртуальной машины или моментального снимка. Затем вы можете сохранить резервную копию в том же дата-центре и восстановить ее по мере необходимости или перенести в другой дата-центр.

Резервное копирование виртуальной машины:

1. Создайте резервный домен. Подробности см. в разделе *Настройка домена хранения в качестве резервного домена для резервного копирования.*
2. Создайте новую виртуальную машину на основе виртуальной машины, которую вы хотите создать для резервного копирования:
3. Чтобы создать резервную копию снимка, сначала создайте виртуальную машину на основе снимка. Подробности см. в разделе *Создание виртуальной машины из моментального снимка* в руководстве пользователя.
4. Чтобы создать резервную копию виртуальной машины, сначала клонируйте виртуальную машину. Подробности см. в разделе *Клонирование виртуальной машин*ы в руководстве пользователя. Прежде чем продолжить, убедитесь, что клон выключен.
5. Экспортируйте новую виртуальную машину в резервный домен. Подробности см. в разделе *Экспорт виртуальной машины в домен данных* в руководстве пользователя.

Восстановление виртуальной машины:

6. Убедитесь, что домен хранилища резервных копий, в котором хранится резервная копия виртуальной машины, подключен к дата-центру.
7. Импортируйте виртуальную машину из резервного домена. Подробности см. в разделе *Импорт виртуальных машин из домена данных*.

6.2.3 Резервное копирование и восстановление виртуальных машин с помощью API резервного копирования и восстановления

6.2.3.1 API резервного копирования и восстановления

API резервного копирования и восстановления – это набор функций, который позволяет выполнять полное резервное копирование и восстановление виртуальных машин или на уровне файлов. API объединяет несколько компонентов KeyVirt, таких как моментальные снимки в реальном времени и REST API, для создания временных томов, которые могут быть подключены к виртуальной машине, содержащей программное обеспечение для резервного копирования, предоставляемое независимым поставщиком программного обеспечения, и работы с ними.

6.2.3.2 Резервное копирование виртуальной машины

Используйте API резервного копирования и восстановления для резервного копирования виртуальной машины. Предполагается, что у вас есть две виртуальные машины: виртуальная машина для резервного копирования и виртуальная машина, на которой установлено программное обеспечение для управления резервным копированием.

Процедура:

1. Используя REST API, создайте снимок виртуальной машины для резервного копирования:
   POST /api/vms/{vm:id}/snapshots/ HTTP/1.1 Accept: application/xml Content-type: application/xml <snapshot> <description>BACKUP</description> </snapshot>
   - Здесь замените {vm:id} на идентификатор виртуальной машины, снимок которой вы создаете. Этот идентификатор доступен на вкладке *Общее* в

окнах *Новая виртуальная машина* и *Изменить виртуальную машину* на Портале администратора и Портале виртуальных машин.

- При создании снимка виртуальной машины ее текущие данные конфигурации сохраняются в атрибуте data атрибута configuration в initialization под снимком.

Вы не можете создавать снимки дисков, помеченных как общедоступные или основанных на дисках direct LUN.

2. Извлеките данные конфигурации виртуальной машины из атрибута data под снимком:
   GET /api/vms/{vm:id}/snapshots/{snapshot:id} HTTP/1.1 All-Content: true Accept: application/xml Content-type: application/xml
   - Здесь замените {vm:id} на идентификатор виртуальной машины, снимок которой вы сделали ранее. Замените {snapshot:id} на идентификатор моментального снимка.
   - Добавьте заголовок All-Content: true для получения дополнительных данных OVF в ответе. Данные OVF в XML-ответе расположены в элементе конфигурации виртуальной машины <initialization><configuration>. Позже вы будете использовать эти данные для восстановления виртуальной машины.
3. Получите идентификатор моментального снимка:
   GET /api/vms/{vm:id}/snapshots/ HTTP/1.1
   Accept: application/xml
   Content-type: application/xml
4. Определите идентификатор диска моментального снимка:
   GET /api/vms/{vm:id}/snapshots/{snapshot:id}/disks HTTP/1.1 Accept: application/xml
   Content-type: application/xml
5. Прикрепите снимок к резервной виртуальной машине в качестве активного вложения на диске с правильным 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>
   ```

Здесь замените {vm:id} на идентификатор виртуальной машины резервной копии, а не виртуальной машины, снимок которой вы сделали ранее. Замените {disk:id} на идентификатор диска. Замените {snapshot:id} на идентификатор моментального снимка.

6. Используйте программное обеспечение резервного копирования на виртуальной машине резервного копирования для создания резервной копии данных на диске моментального снимка.
7. Удалите вложение с диска моментального снимка с виртуальной машины резервного копирования:

DELETE /api/vms/{vm:id}/diskattachments/{snapshot:id} HTTP/1.1
Accept: application/xml
Content-type: application/xml

Здесь замените {vm:id} на идентификатор виртуальной машины резервной копии, а не виртуальной машины, снимок которой вы сделали ранее. Замените {snapshot:id} на идентификатор моментального снимка.

8. При необходимости удалите снимок:
   DELETE /api/vms/{vm:id}/snapshots/{snapshot:id} HTTP/1.1 Accept: application/xml
   Content-type: application/xml

Здесь замените {vm:id} на идентификатор виртуальной машины, снимок которой вы сделали ранее. Замените {snapshot:id} на идентификатор моментального снимка.
Вы создали резервную копию состояния виртуальной машины на определенный момент времени с помощью программного обеспечения для резервного копирования, установленного на отдельной виртуальной машине.

6.2.3.3 Восстановление виртуальной машины

Восстановите виртуальную машину, резервная копия которой была создана с помощью API резервного копирования и восстановления. Предполагается, что у вас есть резервная виртуальная машина, на которой установлено программное обеспечение, использовавшееся для управления предыдущей резервной копией.
Процедура:

1. На Портале администратора создайте плавающий диск, на который будет восстановлена резервная копия. Подробнее о том, как создать плавающий диск, см. в разделе *Создание виртуального диска*.
2. Подключите диск к виртуальной машине резервного копирования:
   POST /api/vms/{vm:id}/disks/ HTTP/1.1
   Accept: application/xml
   Content-type: application/xml

   ```
    <disk id="_{disk:id}_">
   </disk>
   ```

Здесь замените {vm:id} на идентификатор этой виртуальной машины резервной копии, а не виртуальной машины, снимок которой вы сделали ранее. Замените {disk:id} на идентификатор диска, полученный при резервном копировании виртуальной машины.

3. Используйте программу резервного копирования для восстановления резервной копии на диск.
4. Отсоедините диск от резервной виртуальной машины:
   DELETE /api/vms/{vm:id}/disks/{disk:id} HTTP/1.1
   Accept: application/xml
   Content-type: application/xml

   ```
    <action>
      <detach>true</detach>
   </action>
   ```

Здесь замените {vm:id} на идентификатор этой виртуальной машины резервной копии, а не виртуальной машины, снимок которой вы сделали ранее. Замените {disk:id} на идентификатор диска.

5. Создайте новую виртуальную машину, используя данные конфигурации восстанавливаемой виртуальной машины:
   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>
   ```

Чтобы переопределить любое из значений в ovf при создании виртуальной машины, переопределите элемент перед или после элемента initialization (не в самом элементе initialization).

6. Подключите диск к новой виртуальной машине:
   POST /api/vms/{vm:id}/disks/ HTTP/1.1
   Accept: application/xml
   Content-type: application/xml

   ```
   <disk id="_{disk:id}_">
    </disk>
   ```

Здесь замените {vm:id} на идентификатор новой виртуальной машины, а не виртуальной машины, снимок которой вы сделали ранее. Замените {disk:id} на идентификатор диска.
Вы восстановили виртуальную машину с помощью резервной копии, созданной с помощью API резервного копирования и восстановления.

6.3 АВТОРИЗАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

В KeyVirt для авторизации и аутентификации используется KeyCloak – сервер для единого входа (SSO) и хранения учетных записей. Более подробно о KeyCloak см. на официальном сайте.

6.4 ПОЛИТИКА КВОТ

6.4.1 Общие сведения о квотах

Квота – это инструмент ограничения ресурсов, предоставляемый KeyVirt. Квоты накладываются как дополнительные ограничения к тем, что уже имеются в назначенных ролях пользователя.
Квота – это объект дата-центра.
Квота позволяет администраторам среды KeyVirt ограничивать доступ пользователей к памяти, процессору и хранилищу. Квота определяет ресурсы памяти и ресурсы хранения, которые администратор может назначать пользователям. В результате пользователи могут использовать только назначенные им ресурсы. Когда ресурсы квоты исчерпаны, KeyVirt не разрешает дальнейшие действия пользователя.
Существует два вида квот:

- Квота вычислительных мощностей – ограничивает потребление ресурсов среды выполнения, таких как ЦП и память.
- Квота хранилища – ограничивает объем доступного хранилища.

Таблица 36. Описание режимов квот

Режим квоты	Функция
Принудительно (Enforced)	Вводит квоту в режим Audit и ограничивает ресурсы для группы или пользователя, на которые распространяется квота.
Аудит (Audit)	Регистрирует нарушение квоты без блокировки и используется для проверки квот. В данном режиме можно увеличивать или уменьшать объемы квот доступных вычислительных мощностей или хранилища.
Выключено (Disabled)	Отключает ограничения на использование вычислительных мощностей и хранилища, определенные квотами.

Когда пользователь пытается запустить виртуальную машину, характеристики виртуальной машины сравниваются с допустимым объемом памяти и допустимым объемом вычислительных мощностей, установленным в применимой квоте.
Если запуск виртуальной машины приведет к тому, что совокупные ресурсы всех запущенных виртуальных машин, на которые распространяется квота, превышают допуск, определенный в квоте, то Engine откажет в запуске виртуальной машины.
Когда пользователь создает новый диск, запрошенный размер диска добавляется к совокупному использованию всех других дисков, на которые распространяется применимая квота. Если новый диск суммарно с уже существующими дисками, занимает места больше, чем разрешено квотой, то его создание завершается ошибкой.
Квота позволяет совместно использовать ресурсы одного и того же оборудования. Она поддерживает жесткие и мягкие ограничения. Администраторы могут использовать квоту для установки пороговых значений ресурсов. Пользователь воспринимает эти ограничения как 100% использование ресурса. Чтобы предотвратить сбои, когда пользователь неожиданно превышает это пороговое значение, есть возможность установить резерв.
Grace (резерв) – это значение, на которое квота может быть кратковременно превышена. Когда пороговые значения превышены, пользователю оправляется предупреждение.

Внимание! Квота накладывает ограничения на запуск виртуальных машин. Игнорирование этих ограничений может привести к ситуации, в которой пользователь не сможет использовать свои виртуальные машины и виртуальные диски. Когда квота работает в режиме Enforced, нельзя использовать виртуальные машины и диски, которым не назначены квоты. Чтобы включить виртуальную машину, ей должна быть назначена квота. Чтобы создать моментальный снимок виртуальной машины, для диска, связанного с виртуальной машиной, должна быть назначена квота. При создании шаблона на виртуальной машине вам будет предложено выбрать квоту, которую вы хотите использовать для шаблона. Это позволяет настроить шаблон (и все будущие машины, созданные на основе шаблона) на использование квоты, отличной от квоты виртуальной машины и диска, из которых создается шаблон.

6.4.2 Групповые и индивидуальные квоты

Пользователи с разрешениями SuperUser могут создавать квоты для отдельных пользователей или квоты для групп.
Групповые квоты могут быть установлены для пользователей Active Directory. Например, если группе из десяти пользователей выделена квота в 1 ТБ хранилища, и один из десяти пользователей заполняет весь терабайт, то вся группа превысит квоту, и ни один из десяти пользователей не сможет использовать ни одно из хранилищ, связанное с их группой.
Индивидуальная квота устанавливается только для отдельного пользователя. Как только отдельный пользователь израсходует или превысит свою квоту хранилища или квоту вычислительных мощностей, он больше не сможет использовать данные ресурсы.

6.4.3 Учет квот

Когда квота назначается пользователю или ресурсу, каждое действие этого пользователя или ресурса, связанное с хранилищем, виртуальным ЦП или памятью, приводит к потреблению или освобождению квоты. Поскольку квота действует как верхний порог, ограничивающий доступ пользователя к ресурсам, расчеты квоты могут отличаться от фактического текущего использования пользователем. Квота рассчитывается для максимально возможного использования, а не для фактического.
Примеры учета квот:

- Пользователь запускает виртуальную машину с 1 виртуальным ЦП и 1024 МБ памяти. Действие потребляет 1 виртуальный ЦП и 1024 МБ квоты, назначенной этому пользователю. Когда виртуальная машина останавливается, 1 виртуальный ЦП и 1024 МБ ОЗУ высвобождаются обратно в соответствии с квотой, назначенной этому пользователю. Потребление квоты во время выполнения учитывается только во время фактического использования ресурсов пользователем.
- Пользователь создает виртуальный диск тонкой настройки объемом 10 ГБ. Фактическое использование диска может указывать на то, что используется только 3 ГБ этого диска. Однако потребление квоты будет составлять 10 ГБ – максимально возможное использование данного диска.

6.4.4 Включение и изменение режима квоты в дата-центре

Данная процедура включает или изменяет режим квоты в дата-центре. Перед определением квот необходимо выбрать режим квоты. Для этого требуется войти на Портал администратора. Используйте режим Audit, чтобы проверить назначенную квоту и убедиться, что она работает так, как ожидается. Не обязательно иметь квоту в режиме Audit, чтобы создать или изменить квоту.
Для включения и изменения режима квоты выполните следующий алгоритм действий:

1. Нажмите *Виртуализация* > *Дата Центры* и выберите *Дата Центр*.
2. Нажмите *Изменить*.
3. В раскрывающемся списке *Режим квоты* измените режим квоты на *Принудительно*.
4. Нажмите OK.

Если режим квоты установлен на *Аудит* во время тестирования, то следует изменить его на *Принудительно*, чтобы настройки квоты вступили в силу.

6.4.5 Создание новой политики квот

После того как режим квоты установлен в статусе *Аудит* или *Принудительно*, можно определить политику квот для управления использованием ресурсов в дата-центре. Для этого выполните следующие действия:

1. Нажмите *Администрирование* > *Квота*.
2. Нажмите *Добавить*.
3. Заполните поля *Имя* и *Описание*.
4. Выберите *Дата Центр*.
5. В разделе *ОЗУ и CPU* используйте зеленый ползунок, чтобы установить *Порог кластера*.
6. В разделе *ОЗУ и CPU* с помощью синего ползунка установите *Порог Grace*.
7. Нажмите на переключатель *Все кластера* или *Указанные кластера*. Если вы выберете *Указанные кластера*, установите флажки для кластеров, к которым вы хотите добавить политику квот.
8. Нажмите *Изменить*. Откроется окно *Редактировать квоту*.
   - В поле *ОЗУ* выберите либо переключатель *Не ограничено*, чтобы разрешить неограниченное использование ресурсов памяти в кластере, либо выберите переключатель *Ограничить до*, чтобы установить объем памяти, установленный этой квотой. Если вы выберете переключатель *Ограничить до*, введите квоту памяти в мегабайтах (МБ) в поле MB.
   - В поле CPU выберите переключатель *Не ограничено* или переключатель *Ограничить до*, чтобы установить количество «ядер» ЦП, установленное этой квотой. Если вы выберете переключатель *Ограничить до*, введите количество виртуальных ЦП в поле vCPUs.
   - Нажмите OK в окне *Редактировать квоту*.
9. В разделе *Хранилище* с помощью зеленого ползунка установите *Порог хранения*.
10. В разделе *Хранилище* с помощью синего ползунка установите *Хранилище Grace*.
11. Нажмите переключатель *Все домены хранения* или *Указанные домены хранения*. Если вы выберете *Указанные домены хранения*, установите флажки для доменов хранения, к которым вы хотите добавить политику квот.

12. Нажмите *Изменить*. Откроется окно *Редактировать квоту*.
    - В поле Storage Quota выберите либо переключатель *Не ограничено*, чтобы разрешить неограниченное использование хранилища, либо переключатель *Ограничить до*, чтобы установить объем хранилища, до которого квота будет ограничивать пользователей. Если вы выберете переключатель *Ограничить до*, введите размер квоты хранилища в гигабайтах (ГБ) в поле GB.
    - Нажмите OK в окне *Редактировать квоту*.
13. Нажмите OK в окне *Новая квота*.

6.4.6 Настройки порога квоты

В таблице 37 рассмотрены типы порогов квот и их определения.
Таблица 37. Типы порогов квот

Параметр	Определение
Пороговое значение кластера	Количество ресурсов кластера, доступных для каждого дата-центра.
Резерв кластера	Объем кластера, доступный для дата-центра после исчерпания порогового значения кластера дата-центра.
Пороговое значение хранилища	Количество ресурсов хранения, доступных для каждого дата-центра.
Резерв (grace) хранилища	Объем хранилища, доступный для дата-центра после исчерпания порогового значения хранилища для дата-центра.

Если для квоты установлено значение 100 ГБ с резервом 20%, то пользователи не смогут использовать хранилище после использования 120 ГБ хранилища.
Если для той же квоты установлено пороговое значение 70%, то клиенты получают предупреждение, когда они превышают 70 ГБ использования хранилища (но они сохраняют возможность использовать хранилище до тех пор, пока не достигнут 120 ГБ хранилища).
Пороговое значение и резерв устанавливаются относительно квоты. Пороговое значение можно рассматривать как мягкий предел, и его превышение генерирует предупреждение. Резерв может рассматриваться как жесткий предел, превышение которого делает невозможным дальнейшее потребление ресурсов хранения.

6.4.7 Назначение квоты объекту

Для назначения квоты виртуальной машине:
1. Нажмите *Виртуализация* > *Виртуальные машины* и выберите виртуальную машину.
2. Нажмите *Изменить*.
3. Выберите квоту, которую вы хотите использовать для виртуальной машины, из раскрывающегося списка *Квота*.
4. Нажмите OK.

Для назначения квоты для диска:
1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите на имя виртуальной машины. Откроется окно сведений.
3. Перейдите на вкладку *Диски* и выберите диск, который вы планируете связать с квотой.

4. Нажмите *Изменить*.
5. Выберите квоту, которую вы хотите использовать для виртуального диска, в раскрывающемся списке *Квота*.
6. Нажмите OK.

Внимание! Квота должна быть выбрана для всех объектов, связанных с виртуальной машиной, чтобы эта виртуальная машина работала. Если вы не выберете квоту для объектов, связанных с виртуальной машиной, виртуальная машина не будет работать. Ошибка, которую Engine выдает в данной ситуации, является общей, что затрудняет определение возникновения ошибки, потому что квота не связана со всеми объектами, относящимися к данной виртуальной машине. Невозможно делать моментальные снимки виртуальных машин, которым не назначена квота. Невозможно создать шаблоны виртуальных машин, виртуальным дискам которых не назначены квоты.

6.4.8 Использование квоты для ограничения ресурсов пользователя

Чтобы использовать квоты для ограничения ресурсов, к которым у пользователя есть доступ, выполните следующий алгоритм действий:

1. Нажмите *Администрирование* > *Квота*.
2. Нажмите на имя целевой квоты. Откроется окно сведений.
3. Перейдите на вкладку *Потребители*.
4. Нажмите *Добавить*.
5. В поле *Поиск* введите имя пользователя, которого вы хотите связать с квотой.
6. Нажмите Go.
7. Установите флажок рядом с именем пользователя.
8. Нажмите OK.

Через некоторое время пользователь появится на вкладке *Потребители* в подробном представлении.

6.4.9 Редактирование квот

Чтобы изменить существующие квоты, выполните следующий алгоритм действий:

1. Нажмите *Администрирование* > *Квота* и выберите квоту.
2. Нажмите *Изменить*.
3. Отредактируйте поля по мере необходимости.
4. Нажмите OK.

6.4.10 Удаление квот

Чтобы удалить существующие квоты, выполните следующие действия:

1. Нажмите *Администрирование* > *Квота* и выберите квоту.
2. Нажмите *Удалить*.
3. Нажмите OK.

6.4.11 Применение политики соглашения об уровне обслуживания

Чтобы настроить функции ЦП для применения политики соглашения об уровне обслуживания, выполните следующие действия:

1. Нажмите *Виртуализация* > *Виртуальные машины*.
2. Нажмите New или выберите виртуальную машину и нажмите *Изменить*.
3. Перейдите на вкладку *Выделение ресурсов*.
4. Укажите общие ресурсы ЦП в *Общие CPU*. Возможные варианты: *Низкий*, *Средний*, *Высокий*, *Настраиваемый*, *Выключено*. Виртуальные машины со значением *Высокий* получают в два раза больше общих ресурсов, чем со значением *Средний*, а виртуальные машины со значением *Средний* получают вдвое больше общих ресурсов, чем виртуальные машины со значением *Низкий*. Значение *Выключено* указывает VDSM на использование более старого алгоритма для определения распределения ресурсов; обычно количество ресурсов, выдаваемых на этих условиях, составляет 1020.

Потребление ЦП пользователями после выполненных действий регулируется установленной вами политикой.

6.5 УВЕДОМЛЕНИЯ О СОБЫТИЯХ

6.5.1 Настройка уведомлений о событиях

Hosted Engine может уведомлять назначенных пользователей по электронной почте, когда в управляемой им среде происходят определенные события. Чтобы использовать эту функцию, необходимо настроить агент рассылки сообщений. Через Портал администратора можно настроить только уведомления по электронной почте. Ловушки SNMP должны быть настроены на машине Engine. SNMP-ловушка (SNMP-trap) – это особый сигнал, отправляемый системой с поддержкой протокола SNMP. Как правило, подобные сигналы отправляются для того, чтобы оповестить администратора о наступлении каких-то критических событий.

Для настройки рассылки выполните следующий алгоритм действий:

1. Убедитесь, что у вас есть доступ к серверу электронной почты, который может принимать автоматические сообщения от Engine и доставлять их в список рассылки.
2. Нажмите *Администрирование* > *Пользователи* и выберите пользователя.
3. Нажмите на *Имя пользователя*, чтобы перейти на страницу сведений.
4. На вкладке *Уведомления о событиях* нажмите *Управление событиями*.
5. Используйте кнопку *Развернуть всё* или кнопки расширения для конкретной темы, чтобы просмотреть события.
6. Установите соответствующие флажки.
7. Введите адрес электронной почты в поле *Получатель почты*.

Примечание. Адрес электронной почты может быть адресом электронной почты текстового сообщения (например, 1234567890@carrierdomainname.com) или групповым адресом электронной почты, который включает адреса электронной почты и адреса электронной почты текстовых сообщений.

8. Нажмите OK.
9. На машине Engine скопируйте ovirt-engine-notifier.conf в новый файл с именем 90-email-notify.conf:

cp /usr/share/ovirt-engine/services/ovirt-engine-notifier/ ovirt-engine-notifier.conf /etc/ovirt-engine/notifier/notifier.conf. d/90-email-notify.conf

10. Отредактируйте 90-email-notify.conf, удалив все, кроме раздела EMAIL Notifications.
11. Введите корректные переменные электронной почты, как в примере ниже. Данный файл переопределяет значения в исходном файле ovirt-enginenotifier.conf.

```
#--------------------#
# EMAIL Notifications #
#--------------------#

# The SMTP mail server address. Required.
MAIL_SERVER=myemailserver.example.com

# The SMTP port (usually 25 for plain SMTP, 465 for SMTP with SSL, 587 for SMTP with TLS)
MAIL_PORT=25

# Required if SSL or TLS enabled to authenticate the user. Used also to specify 'from' user address if mail server
# supports, when MAIL_FROM is not set. Address is in RFC822 format
MAIL_USER=

# Required to authenticate the user if mail server requires authentication or if SSL or TLS is enabled
SENSITIVE_KEYS="${SENSITIVE_KEYS},MAIL_PASSWORD"
MAIL_PASSWORD=

# Indicates type of encryption (none, ssl or tls) should be used to communicate with mail server.
MAIL_SMTP_ENCRYPTION=none

# If set to true, sends a message in HTML format.
HTML_MESSAGE_FORMAT=false

# Specifies 'from' address on sent mail in RFC822 format, if supported by mail server.
MAIL_FROM=rhevm2017@example.com

# Specifies 'reply-to' address on sent mail in RFC822 format.
MAIL_REPLY_TO=

# Interval to send smtp messages per # of IDLE_INTERVAL
MAIL_SEND_INTERVAL=1

# Amount of times to attempt sending an email before failing.
MAIL_RETRIES=4
```

Примечание. Дополнительные параметры см. в файле /etc/ovirt-engine/notifier/notifier.conf.d/README.

12. Включите и перезапустите службу ovirt-engine-notifier, чтобы применить внесенные вами изменения:

```
# systemctl daemon-reload
# systemctl enable ovirt-engine-notifier.service
# systemctl restart ovirt-engine-notifier.service
```

Указанный пользователь теперь будет получать электронные письма на основе событий в среде KeyVirt. Выбранные события отображаются на вкладке *Уведомления о событиях* для указанного пользователя.

6.5.2 Отмена уведомлений о событиях

Когда пользователь настроил некоторые ненужные уведомления по электронной почте и хочет их отменить, необходимо выполнить следующие действия:

1. Нажмите *Администрирование* > *Пользователи*.
2. Нажмите на *Имя пользователя*. Откроется подробное описание.
3. Перейдите на вкладку *Уведомления о событиях*, чтобы просмотреть список событий, о которых пользователь получает уведомления по электронной почте.
4. Нажмите *Управление событиями*.
5. Используйте кнопку *Развернуть всё* или кнопки расширения для конкретной темы, чтобы просмотреть события.
6. Снимите соответствующие флажки, чтобы удалить уведомление об этом событии.
7. Нажмите OK.

6.5.3 Параметры уведомлений о событиях

Файл конфигурации уведомлений о событиях можно найти по пути /usr/share/ ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf.

Таблица 38. Описание параметров уведомлений о событиях

Имя переменной	Значение по умолчанию	Примечание
SENSITIVE_KEYS	none	Разделенный запятыми список ключей, которые не будут регистрироваться.
JBOSS_HOME	/usr/share/ovirtengine-wildfly	Расположение сервера приложений JBoss, используемого Engine.
ENGINE_ETC	/etc/ovirt-engine	Расположение каталога etc, используемого Engine.
ENGINE_LOG	/var/log/ovirt-engine	Расположение каталога logs, используемого Engine.
ENGINE_USR	/usr/share/ovirtengine	Расположение каталога usr, используемого Engine.
ENGINE_JAVA_MODULEPATH	$ENGINE_USR/modules	Путь к файлу, к которому добавляются модули JBoss.
NOTIFIER_DEBUG_ ADDRESS	none	Адрес машины, которую можно использовать для удаленной отладки виртуальной машины Java, используемой уведомителем.
NOTIFIER_STOP_ TIME	30	Время в секундах, по истечении которого служба завершит работу.
NOTIFIER_STOP_ INTERVAL	1	Время в секундах, на которое будет увеличиваться счетчик времени ожидания.

INTERVAL_IN_ SECONDS	120	Интервал в секундах между экземплярами отправки сообщений получателям.
IDLE_INTERVAL	30	Интервал в секундах, между которыми будут выполняться задачи с низким приоритетом.
DAYS_TO_KEEP _ HISTORY	0	Данная переменная задает количество дней, в течение которых отправленные события будут сохраняться в таблице истории. Если переменная не установлена, события остаются в таблице истории на неопределенный срок.
FAILED_QUERIE S_ NOTIFICATION_ THRESHOLD	30	Количество неудачных запросов, после которых отправляется уведомление по электронной почте. Уведомление по электронной почте отправляется после первой неудачной попытки получения уведомлений, а затем каждый раз, когда достигается количество сбоев, указанное этой переменной. Если вы укажете значение «0» или «1», электронное письмо будет отправляться при каждом сбое.
FAILED_QUERIE S_ NOTIFICATION_ RECIPIENTS	none	Адреса электронной почты получателей, которым будут отправляться уведомления по электронной почте. Адреса электронной почты должны быть разделены запятой. Данная запись устарела из-за переменной FILTER.
DAYS_TO_SEND _ ON_STARTUP	0	Количество дней старых событий, которые будут обработаны и отправлены при запуске уведомителя.
FILTER	exclude:*	Алгоритм, используемый для определения триггеров и получателей уведомлений по электронной почте. Значение этой переменной состоит из комбинации include или exclude, события и получателя. Например, include:VDC_START (smtp:mail@example.com) $FILTER.
MAIL_SERVER	none	Адрес почтового SMTP-сервера. Обязательно.
MAIL_PORT	25	Порт, используемый для связи. Возможные значения включают: 25 – обычный SMTP; 465 – SMTP с SSL; 587 – SMTP с TLS.
MAIL_USER	none	Если SSL включен для аутентификации пользователя, эта переменная должна

		быть установлена. Данная переменная также используется для указания адреса пользователя «от кого», когда переменная MAIL_FROM не установлена. Некоторые почтовые серверы не поддерживают эту функцию. Адрес в формате RFC822.
SENSITIVE_KEYS	$SENSITIVE_KEYS, MAIL_PASSWORD	Требуется для аутентификации пользователя, если почтовый сервер требует аутентификации или включены SSL или TLS.
MAIL_PASSWORD	none	Требуется для аутентификации пользователя, если почтовый сервер требует аутентификации или включены SSL или TLS.
MAIL_SMTP_ ENCRYPTION	none	Тип шифрования, который будет использоваться при обмене данными. Возможные значения: none, ssl, tls.
HTML_MESSAGE_ FORMAT	false	Почтовый сервер отправляет сообщения в формате HTML, если для этой переменной установлено значение true.
MAIL_FROM	none	Эта переменная указывает адрес отправителя в формате RFC822, если он поддерживается почтовым сервером.
MAIL_REPLY_TO	none	Эта переменная указывает адреса для ответа в формате RFC822 на отправленную почту, если она поддерживается почтовым сервером.
MAIL_SEND_ INTERVAL	1	Количество SMTP-сообщений, отправляемых для каждого IDLE_INTERVAL.
MAIL_RETRIES	4	Количество попыток отправить электронное письмо до сбоя.
SNMP_MANAGERS	none	IP-адреса или полные доменные имена машин, которые будут действовать как менеджеры SNMP. Записи должны быть разделены пробелом и могут содержать номер порта. Например, manager1.example.com manager2.example.com:164.
SNMP_ COMMUNITY	public	Сообщество SNMP.
SNMP_OID	1.3.6.1.4.1.2312.13.1.1	Идентификаторы объекта-ловушки по умолчанию для предупреждений. Все типы ловушек отправляются с добавлением информации о событии диспетчеру SNMP, когда этот OID определен. Обратите внимание, что

		изменение ловушки по умолчанию препятствует тому, чтобы сгенерированные ловушки соответствовали информационной базе управления Engine.
SNMP_VERSION	2	Определяет, какую версию SNMP использовать. Поддерживаются ловушки SNMP версии 2 и версии 3. Возможные значения: 2 или 3.
SNMP_ENGINE_ID	none	Идентификатор механизма, используемый для ловушек SNMPv3. Этот идентификатор является уникальным идентификатором устройства, подключенного через SNMP.
SNMP_USERNAME	none	Имя пользователя, используемое для ловушек SNMPv3.
SNMP_AUTH_PROTOCOL	none	Протокол авторизации SNMPv3. Возможные значения: MD5, SHA.
SNMP_AUTH_PASSPHRASE	none	Парольная фраза, используемая, когда для SNMP_SECURITY_LEVEL установлено значение AUTH_NOPRIV и AUTH_PRIV.
SNMP_PRIVACY_ PROTOCOL	none	Протокол конфиденциальности SNMaPv3. Возможные значения: AES128, AES192, AES256. Внимание. AES192 и AES256 не определены в RFC3826, поэтому перед их включением убедитесь, что ваш SNMP-сервер поддерживает эти протоколы.
SNMP_PRIVACY_ PASSPHRASE	none	Парольная фраза конфиденциальности SNMPv3, используемая, когда SNMP_SECURITY_LEVEL установлено значение AUTH_PRIV.
SNMP_SECURITY_ LEVEL	1	Уровень безопасности SNMPv3. Возможные значения: 1-NOAUTH_NOPRIV; 2- AUTH_NOPRIV; 3-AUTH_PRIV.
ENGINE_INTERVAL _IN_SECONDS	300	Интервал в секундах между мониторингом машины, на которой установлен Engine. Интервал измеряется с момента завершения мониторинга.
ENGINE_MONITOR _RETRIES	3	Указывает, сколько раз уведомитель пытается отслеживать состояние машины, на которой установлен Engine, за заданный интервал после сбоя.

ENGINE_TIMEOUT _IN_SECONDS	30	Время ожидания в секундах, прежде чем уведомитель попытается отслеживать состояние машины, на которой установлен Engine, в заданный интервал после сбоя.
IS_HTTPS_ PROTOCOL	false	Эта запись должна быть установлена true, если JBoss работает в защищенном режиме.
SSL_PROTOCOL	TLS	Протокол, используемый коннектором конфигурации JBoss, когда включен SSL
SSL_IGNORE_ CERTIFICATE_ ERRORS	false	Это значение должно быть установлено true, если JBoss работает в безопасном режиме и ошибки SSL следует игнорировать.
SSL_IGNORE_ HOST_ VERIFICATION	false	Это значение должно быть установлено true, если JBoss работает в безопасном режиме и проверка имени узла должна игнорироваться.
REPEAT_NON_ RESPONSIVE_ NOTIFICATION	false	Эта переменная указывает, будут ли повторяющиеся сообщения об ошибках отправляться подписчикам, если машина, на которой установлен Engine, не отвечает.
ENGINE_PID	/var/lib/ovirt-engine/ovirt-engine.pid	Путь и имя файла PID Engine.

6.5.4 Настройка Hosted Engine для отправки ловушек SNMP

Настройте Hosted Engine на отправку ловушек Simple Network Management Protocol (SNMP) одному или нескольким внешним SNMP-менеджерам. Ловушки SNMP содержат информацию о системных событиях; они используются для мониторинга вашей среды KeyVirt. Количество и тип ловушек, отправляемых SNMP-менеджеру, можно определить в Hosted Engine. KeyVirt поддерживает ZZZ. SNMP версии 3 поддерживает следующие уровни безопасности:

- NoAuthNoPriv – ловушки SNMP отправляются без какой-либо авторизации или конфиденциальности.
- AuthNoPriv – ловушки SNMP отправляются с авторизацией по паролю, но без конфиденциальности.
- AuthPriv – ловушки SNMP отправляются с авторизацией по паролю и конфиденциальностью.

Для настройки необходимо иметь:

- Один или несколько внешних SNMP-менеджеров, настроенных на получение ловушек.
- IP-адреса или полные доменные имена машин, которые будут действовать как SNMP-менеджеры. Опционально определите порт, через который Engine будет получать уведомления о ловушках. По умолчанию используется UDP-порт 162.

- Сообщество SNMP (только для SNMP версии 2). Несколько SNMP-менеджеров могут принадлежать к одному сообществу. Системы управления и агенты могут взаимодействовать, только если они находятся в одном сообществе. По умолчанию сообщество является общедоступным.
- Идентификатор объекта ловушки для оповещений. Hosted Engine предоставляет OID по умолчанию 1.3.6.1.4.1.2312.13.1.1.1. Все типы ловушек, дополненные информацией о событии, отправляются менеджеру SNMP, когда определен этот OID. Обратите внимание, что изменение ловушки по умолчанию предотвращает соответствие сгенерированных ловушек базе управляющей информации Engine.
- Имя пользователя SNM (для SNMP версии 3), уровни безопасности 1, 2 и 3.
- Парольная фраза SNMP (для SNMP версии 3), уровни безопасности 2 и 3.
- Частная парольная фраза SNMP (для SNMP версии 3), уровень безопасности 3.

Примечание. Engine предоставляет базы управляющей информации (MIB) в /usr/share/doc/ovirt-engine/mibs/OVIRT-MIB.txt и /usr/share/doc/ ovirt-engine/mibs/REDHAT-MIB.txt. Прежде чем продолжить, загрузите MIB в диспетчер SNMP.

Значения конфигурации SNMP по умолчанию существуют в Engine в файле конфигурации демона уведомления о событиях /usr/share/ovirt-engine/ services/ovirt-engine-notifier/ovirt-engine-notifier.conf. Значения, описанные ниже, основаны на значениях по умолчанию или примерах, представленных в этом файле.

Внимание! Не редактируйте этот файл напрямую, так как системные изменения, такие как обновления, могут удалить любые изменения, внесенные вами в этот файл. Вместо этого скопируйте этот файл в /etc/ovirtengine/notifier/notifier.conf.d/-snmp.conf, где указан приоритет, с которым должен выполняться файл.

Для настройки отправки ловушек SNMP выполните следующие действия:

1. В Engine создайте файл конфигурации SNMP с именем файла – snmp.conf, где <integer> – целое число, указывающее порядок, в котором обрабатываются файлы. Например:

vi /etc/ovirt-engine/notifier/notifier.conf.d/20-snmp.conf

Скопируйте настройки SNMP по умолчанию из файла конфигурации демона уведомлений о событиях /usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf. Этот файл включает встроенные комментарии для всех настроек.

2. Укажите менеджера(ов) SNMP, сообщество SNMP (только для SNMP версии 2) и OID в формате:

SNMP_MANAGERS="_manager1.example.com_ manager2.example.com:162"
SNMP_COMMUNITY=public
SNMP_OID=1.3.6.1.4.1.2312.13.1.1

3. Определите, использовать ли SNMP версии 2 (по умолчанию) или версии 3:

SNMP_VERSION=3

4. Укажите значение для SNMP_ENGINE_ID. Например, для SNMP версии 3:

SNMP_ENGINE_ID="80:00:00:00:01:02:05:05"

5. При использовании SNMP версии 3 укажите уровень безопасности для ловушек SNMP:

- Уровень безопасности 1, ловушки NoAuthNoPriv:

SNMP_USERNAME=NoAuthNoPriv

SNMP_SECURITY_LEVEL=1

- Уровень безопасности 2, ловушки AuthNoPriv от имени пользователя ovirtengine с парольной фразой аутентификации SNMP authpass.

SNMP_USERNAME=ovirtengine
SNMP_AUTH_PROTOCOL=MD5
SNMP_AUTH_PASSPHRASE=authpass
SNMP_SECURITY_LEVEL=2

- Уровень безопасности 3, ловушки AuthPriv, от имени пользователя ovirtengine с парольной фразой SNMP Auth authpass и частной парольной фразой SNMP Priv privpass. Например:

SNMP_USERNAME=ovirtengine
SNMP_AUTH_PROTOCOL=MD5
SNMP_AUTH_PASSPHRASE=authpass
SNMP_PRIVACY_PROTOCOL=AES128
SNMP_PRIVACY_PASSPHRASE=privpass
SNMP_SECURITY_LEVEL=3

6. Определите, какие события отправлять SNMP-менеджеру:

- Отправлять все события в профиль SNMP по умолчанию:

FILTER="include:*(snmp:) ${FILTER}"

- Отправлять все события с серьезностью ERROR или ALERT в профиль SNMP по умолчанию:

FILTER="include:*:ERROR(snmp:) ${FILTER}"
FILTER="include:*:ALERT(snmp:) ${FILTER}"

- Отправлять события для VDC_START на указанный адрес электронной почты:

FILTER="include:VDC_START(snmp:mail@example.com) ${FILTER}"

- Отправлять события для всего, кроме VDC_START, в профиль SNMP по умолчанию:

FILTER="exclude:VDC_START include:*(snmp:) ${FILTER}"

- Это фильтр по умолчанию, определенный в ovirt-engine-notifier.conf; если вы не отключите этот фильтр или не примените переопределяющие фильтры, уведомления не будут отправляться:

FILTER="exclude:*"

7. Сохраните файл.
8. Запустите службу ovirt-engine-notifier и убедитесь, что эта служба запускается при загрузке:

systemctl start ovirt-engine-notifier.service
systemctl enable ovirt-engine-notifier.service

Проверьте диспетчер SNMP, чтобы убедиться, что ловушки принимаются.

Примечание. SNMP_MANAGERS, MAIL_SERVER или оба параметра должны быть правильно определены в /usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf или в файле переопределения, чтобы служба notifier могла корректно работать.

Пример файла конфигурации SNMP

Пример файла конфигурации для SNMP версии 3 основан на настройках в ovirt-engine-notifier.conf. Специальный файл конфигурации SNMP, такой как этот, имеет приоритет над настройками в файлах ovirt-enginenotifier.conf.
Скопируйте настройки SNMP по умолчанию из файла конфигурации демона уведомлений о событиях /usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf в /etc/ovirt-engine/notifier/notifier.conf.d/<_integer_>-snmp.conf, где <_integer_> – это число, указывающее приоритет, с которым файл должен запускаться. Этот файл включает встроенные комментарии для всех настроек.
/etc/ovirt-engine/notifier/notifier.conf.d/20-snmp.conf
SNMP_MANAGERS="manager1.example.com manager2.example.com:162"
SNMP_COMMUNITY=public
SNMP_OID=1.3.6.1.4.1.2312.13.1.1
FILTER="include:*(snmp:)"
SNMP_VERSION=3
SNMP_ENGINE_ID="80:00:00:00:01:02:05:05"
SNMP_USERNAME=<username>
SNMP_AUTH_PROTOCOL=MD5
SNMP_AUTH_PASSPHRASE=<authpass>
SNMP_PRIVACY_PROTOCOL=AES128
SNMP_PRIVACY_PASSPHRASE=<privpass>
SNMP_SECURITY_LEVEL=3

6.6 СБОР ИНФОРМАЦИИ ОБ ОБОРУДОВАНИИ

6.6.1 МОНИТОРИНГ И НАБЛЮДЕНИЕ

Подробнее см. раздел *Руководство по эксплуатации Портала мониторинга KeyVirt*.

6.6.2 ЛОГ-ФАЙЛЫ

6.6.2.1 Лог-файлы установки Engine

К лог-файлам установки Engine относятся:

- /var/log/ovirt-engine/setup/ovirt-engine-remove-.log – лог от команды engine-cleanup. Данная команда используется для сброса установки Engine. Лог создается каждый раз при выполнении команды. Дата и время запуска используются в имени файла, чтобы разрешить существование нескольких логов.
- /var/log/ovirt-engine/setup/ovirt-engine-setup-.log – лог от команды engine-setup. Лог создается каждый раз при выполнении команды. Дата и время запуска используются в имени файла, чтобы разрешить одновременное существование нескольких логов.

6.6.2.2 Лог-файлы Engine

Таблица 39. Сервисная активность

Лог-файл	Описание
/var/log/ovirt-engine/engine.log	Отражает все сбои графического интерфейса Engine, запросы Active Directory, проблемы с базой данных и другие события.

/var/log/ovirt-engine/host-deploy	Файлы журналов с узлов, развернутых из Engine.
/var/lib/ovirt-engine/setup-history.txt	Отслеживает установку и обновление пакетов, связанных с Engine.
/var/log/httpd/ovirt-requests-log	Регистрирует файлы запросов к KeyVirt Engine через HTTPS, включая время выполнения каждого запроса. Заголовок Correlation-Id включен, чтобы вы могли сравнивать запросы при сравнении файла журнала с /var/log/ovirt-engine/engine.log.
/var/log/ovn-provider/ovirt-provider-ovn.log	Регистрирует действия поставщика OVN. Сведения о журналах Open vSwitch см. в официальной документации Open vSwitch.

6.6.2.3 Лог-файлы SPICE

Лог-файлы SPICE полезны при устранении неполадок с подключением SPICE. Чтобы начать отладку SPICE, измените уровень лога на debugging. Затем определите местоположение лога.
И клиенты, используемые для доступа к гостевым машинам, и сами гостевые машины имеют лог-файлы SPICE. Для логов на стороне клиента, если клиент SPICE был запущен с использованием собственного клиента, для которого загружен файл console.vv, используйте команду remote-viewer, чтобы включить отладку и создать вывод лога.
Таблица 40. Описание логов

Тип журнала	Расположение журнала	Чтобы изменить уровень журнала
Узел SPICE с гипервизором	/var/log/libvirt/qemu/(guest_name).log	Запустить export SPICE_DEBUG_LEVEL=5 на узле / гипервизоре перед запуском гостевой. Эта переменная анализируется QEMU, и при запуске в масштабах всей системы будет выведена отладочная информация всех виртуальных машин в системе. Эта команда должна выполняться на каждом узле в кластере. Эта команда работает только для каждого узла / гипервизора, а не для каждого кластера.

Таблица 41. Журналы spice-vdagent для гостевых компьютеров

Тип журнала	Расположение журнала	Чтобы изменить уровень журнала
Гостевой Windows	C:\Windows\Temp\vdagent.log C:\Windows\Temp\vdservice.log	Не применимо

Тип журнала	Расположение журнала	Чтобы изменить уровень журнала
Гостевой Enterprise Linux	Использование journal ctl как пользователь root.	Для запуска службы spice-vdagentd в режиме отладки, поскольку пользователь root создает файл /etc/sysconfig/spice-vdagentd с этой записью: SPICE_VDAGENTD_EXTRA_ARGS=”-d -d” Для запуска spice-vdagent в режиме отладки из командной строки: $ killall – u $ USER spice-vdagent $ spice-vdagent -x -d [-d] [| и tee spice-vdagent.log]

6.6.2.4 Лог-файлы SPICE для клиентов SPICE, запущенных с использованием файлов console.vv

Для клиентских машин Linux:

1. Включите отладку SPICE, запустив команду remote-viewer с помощью опции --spice-debug. При появлении запроса введите URL-адрес подключения, например, spice://virtual_machine_IP:port:
   # remote-viewer --spice-debug
2. Чтобы запустить клиент SPICE с параметром debug и передать ему файл .vv, загрузите файл console.vv и запустите команду remote-viewer с помощью опции --spice-debug, при этом выберите и укажите полный путь к файлу console.vv.
   # remote-viewer --spice-debug /path/to/console.vv

Для клиентских машин Windows:

1. В версиях virt-viewer 2.0-11.el7ev и новее virt-viewer.msi устанавливает virt-viewer и debug-viewer.exe.
2. Запустите команду remote-viewer с помощью аргумента spice-debug и направьте команду по пути к консоли:
   remote-viewer --spice-debug path\to\console.vv
3. Для просмотра логов подключитесь к виртуальной машине. Вы увидите командную строку с запущенным GDB, которая выводит стандартный вывод и стандартную ошибку remote-viewer.

6.6.2.5 Лог-файлы узла

К лог-файлам узла относятся:

- /var/log/messages – лог-файл, используемый libvirt. Используйте для просмотра лога journalctl. Для просмотра лога вы должны быть членом групп adm, systemd-journal или wheel.
- /var/journal/vdsm/vdsm.log – лог-файл для VDSM, агента Engine на узле(ax).
- /var/log/vdsm/import/import-.log – файл журнала с подробным описанием импорта виртуальных машин с узла KVM или провайдера VMWare, включая информацию об ошибках импорта. UUID – это UUID виртуальной машины, которая была импортирована, а Date – это дата и время начала импорта.
- /var/log/vdsm/supervdsm.log – записывает задачи VDSM, которые выполнялись с разрешениями суперпользователя.

- /var/log/vdsm/upgrade.log – VDSM использует этот файл журнала во время обновления узла для регистрации изменений конфигурации.
- /var/journal/vdsm/mom.log – регистрирует действия диспетчера избыточного выделения памяти VDSM.

6.6.2.6 Настройка ведения журнала на уровне отладки

Вы можете настроить журналы следующих служб KeyVirt на уровень отладки, изменив файл sysconfig для каждой службы:

- ovirt-engine.service – /etc/sysconfig/ovirt-engine;
- ovirt-engine-dwhd.service – /etc/sysconfig/ovirt-engine-dwhd;
- ovirt-fence-kdump-listener.service – /etc/sysconfig/ovirt-fence-kdump-listener;
- ovirt-websocket-proxy.service – /etc/sysconfig/ovirt-websocket-proxy.

Эта модификация затрагивает выполнение логирование оболочкой Python, а не основным сервисным процессом.
Настройка ведения журнала на уровне отладки полезна для отладки проблем, связанных с запуском, например, если основной процесс не запускается из-за отсутствия или неправильной среды выполнения Java или библиотеки.
Требования: Убедитесь, что файл sysconfig, который вы хотите изменить, существует. При необходимости создайте его.
Для настройки журнала выполните следующие действия:

1. Добавьте следующее в файл сервиса sysconfig:
   OVIRT_SERVICE_DEBUG=1
2. Перезапустите службу:
   # systemctl restart <service>

Файл журнала службы sysconfig теперь настроен на уровень отладки.

6.6.2.7 Основные файлы конфигурации сервисов

Помимо файла sysconfig, каждый из этих сервисов KeyVirt (таблица 42) имеет еще один конфигурационный файл, который используется чаще.
Таблица 42. Файлы конфигураций для сервисов KeyVirt

Тип журнала	Расположение журнала	Изменение уровня журнала
Журналы SPICE для серверов SPICE гипервизора		
Хост / гипервизор SPICE Server	/var/log/libvirt/qemu/ (guest_name).log	Запустите export SPICE_DEBUG_LEVEL=5 на узле/гипервизоре до запуска гостевой ОС. Эта переменная анализируется QEMU, и если она запущена для всей системы, будет записана отладочная информация обо всех виртуальных машинах в системе. Эту команду необходимо выполнить на каждом узле в кластере. Эта команда работает только для каждого узла/гипервизора, а не для каждого кластера.
Журналы SPICE для гостевых машин		

Гостевая ОС Windows	C:\Windows\Temp\ vdagent.log C:\Windows\Temp\ vdservice.log	Не применимо
Гостевая ОС Linux	Используйте journalctl в качестве пользователя root.	Чтобы запустить службу spice-vdagentd в режиме отладки, от имени пользователя root создайте файл /etc/sysconfig/spice-vdagentd со следующей записью: SPICE_VDAGENTD_ EXTRA_ARGS="-d -d" Чтобы запустить spice-vdagent в режиме отладки, из командной строки выполните: killall – u $USER spicevdagent spice-vdagent -x -d [-d] [|& tee spice-vdagent.log]

6.6.2.8 Настройка хост-сервера регистрации

Узлы создают и обновляют лог-файлы, записывая свои действия и проблемы. Централизованный сбор этих лог-файлов упрощает отладку.
Эту процедуру следует использовать на централизованном сервере логов. Можно использовать отдельный лог-сервер или использовать описанную ниже процедуру, чтобы включить логирование узла в Engine.
Для настройки хост-сервера регистрации выполните следующие действия:

1. Проверьте, разрешает ли брандмауэр трафик на UDP 514 портирован и открыт для syslog служебный трафик:
   # firewall-cmd --query-service=syslog

Если результат является no разрешить трафик на UDP 514 порт с:
firewall-cmd --add-service=syslog --permanent # firewall-cmd --reload

2. Создайте новый файл .conf на сервере системного журнала, например, /etc/rsyslog.d/from_remote.conf, и добавьте следующие строки:

   template(name="DynFile" type="string"
   string="/var/log/%HOSTNAME%/%PROGRAMNAME%.log")
   RuleSet(name="RemoteMachine"){ action(type="omfile" dynaFile="DynFile") }
   Module(load="imudp")
   Input(type="imudp" port="514" ruleset="RemoteMachine")
3. Перезапустите службу rsyslog:
   # systemctl restart rsyslog.service
4. Войдите в гипервизор и в /etc/rsyslog.conf добавьте следующую строку:
   *.info;mail.none;authpriv.none;cron.none @<syslog-FQDN>:514
5. Перезапустите службу rsyslog на гипервизоре:
   # systemctl restart rsyslog.service

Теперь ваш централизованный лог-сервер настроен на получение и хранение сообщений и безопасных журналов с ваших узлов виртуализации.