АО «НТЦ ИТ РОСА»

ПЛАТФОРМА ВИРТУАЛИЗАЦИИ «ROSA VIRTUALIZATION» (ВЕРСИЯ 3.0)

Руководство администратора

Листов 265

2023

СОДЕРЖАНИЕ

Введение

В данном руководстве содержатся сведения и инструкции для администраторов платформы виртуализации ROSA Virtualization.

ROSA Virtualization — платформа виртуализации с интегрированной системой управления, позволяющая развернуть виртуальный центр обработки данных (ВЦОД) корпоративного уровня в кратчайшие сроки. Система управления средой виртуализации (СУСВ), входящая в состав ROSA Virtualization, обладает русскоязычным графическим интерфейсом, с помощью которого осуществляется централизованное управление

объектами виртуальной среды (гипервизоры, хранилища, кластеры, дата-центры, виртуальные машины и прочие).

ROSA Virtualization обеспечивает создание, управление и эксплуатацию свыше тысячи виртуальных машин в одном ВЦОД. Встроенные механизмы, обеспечивающие защиту информации, использование развитых моделей доступа (дискреционной и ролевой) выгодно отличает ROSA Virtualization от аналогичных решений, например на базе OpenStack.

ROSA Virtualization может эксплуатироваться в ЦОД государственных органов и частных организаций различных масштабов.

Часть I. Администрирование и обслуживание среды виртуализации

Наличие администратора является необходимым условием функционирования среды виртуализации. В обязанности администратора системы виртуализации ROSA Virtualization входят следующие задачи:

- Управление физическими и виртуальными ресурсами, такими как хосты и виртуальные машины, в частности добавление хостов и обновление версий ПО на хостах, импорт доменов, преобразование виртуальных машин, созданных на сторонних гипервизорах, а также управление пулами виртуальных машин.
- Мониторинг всех системных ресурсов на предмет потенциальных проблем, таких как чрезмерная нагрузка на один из хостов, недостаток памяти или места на диске, а также выполнение любых необходимых задач (например, миграция ВМ на другие хосты для снижения нагрузки или высвобождение ресурсов путём выключения машин).
- Своевременное реагирование на изменяющиеся требования ВМ (например, обновление версии ОС или выделение большего объёма памяти).
- Управление изменёнными свойствами объектов с помощью тегов.
- Управление параметрами пользователей и настройка уровней полномочий.
- Диагностика и решение проблем конкретных пользователей или виртуальных машин в масштабе общих функциональных возможностей системы.
- Создание общих и частных отчётов.
- Обеспечение защиты машинных носителей информации.

Глава 1. Настройка глобальных ресурсов

Настройка глобальных ресурсов осуществляется на Портале администрирования в окне **Настроить**.

В этом окне можно настроить такие глобальные ресурсы среды виртуализации как роли, системные права доступа, политики планирования задач, типы экземпляров и пулы адресов MAC. Кроме того, в этом окне можно настроить способы взаимодействия пользователей с ресурсами в окружении, также здесь располагается центральная локация для настройки параметров, которые можно применять к нескольким кластерам.

Окно **Настроить** (Рис. 1) можно открыть из меню **Администрирование** → **Настроить** на Портале администрирования.

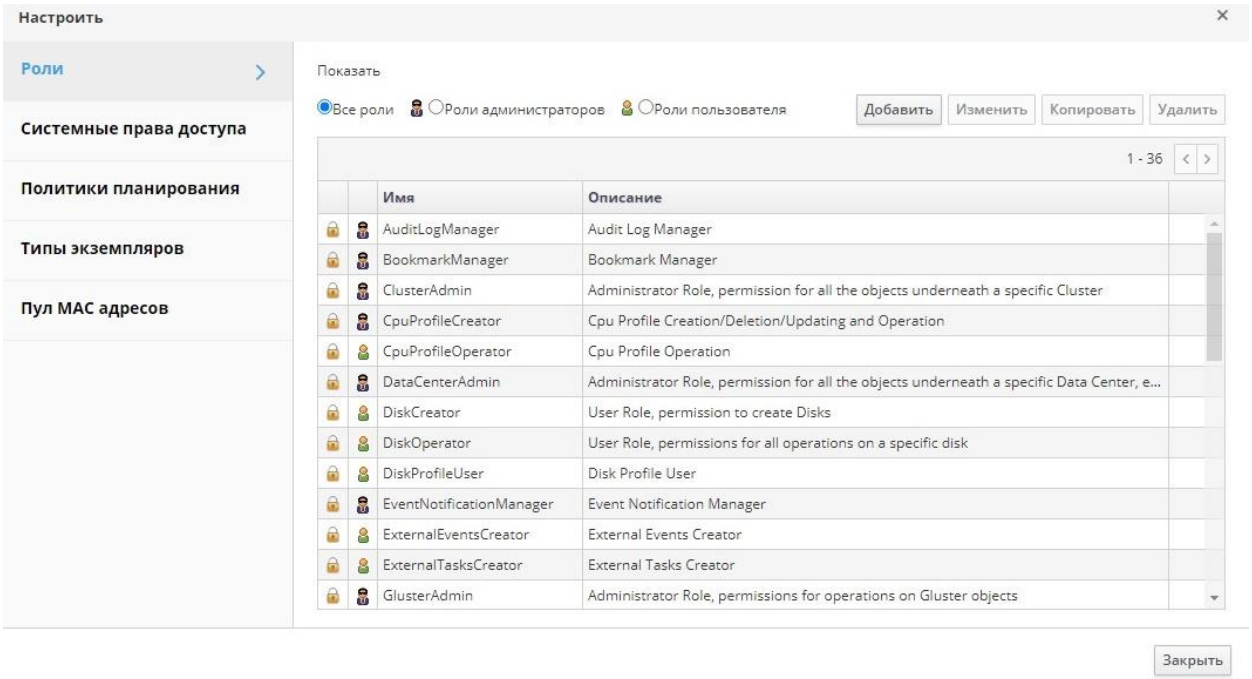

Рис. 1. Настройки системы

1.1. Роли

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

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

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

1.1.1. Добавление новой роли

Добавление роли

1. Нажмите **Администрирование → Настроить**, чтобы открыть окно **Настроить**. По умолчанию выбрана вкладка **Роли**, где отображается список изначальных ролей **Пользователя** и **Администратора**, а также все частные роли.
2. Нажмите **Добавить**.
3. Введите **Имя** и **Описание** новой роли.
4. Для параметра **Тип учётной записи** выберите **Администратор** или **Пользователь**.
5. С помощью кнопок **Развернуть всё** или **Свернуть всё** можно увидеть соответственно больше или меньше подробностей для полномочий объектов,

присутствующих в списке. Также можно развернуть или свернуть параметры для каждого объекта.

6. Для каждого объекта установите или снимите соответствующие флажки для действий, которые нужно разрешить или запретить в настраиваемой роли.
7. Для применения изменений нажмите **OK**. Новая роль будет показана в списке ролей.

1.1.2. Изменение параметров роли

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

Изменение или копирование роли

1. Нажмите **Администрирование → Настроить**, чтобы открыть окно **Настроить.** По умолчанию выбрана вкладка **Роли**, где отображается список изначальных ролей **Пользователя** и **Администратора**, а также все частные роли.
2. Выберите роль, которую нужно изменить. Чтобы открыть окно **Параметры роли**, нажмите **Изменить**, или чтобы открыть окно **Копировать роль**, нажмите **Копировать.**
3. При необходимости измените **Имя** и **Описание** роли.
4. С помощью кнопок **Развернуть всё** или **Свернуть всё** можно увидеть соответственно больше или меньше подробностей для полномочий объектов, присутствующих в списке. Также можно развернуть или свернуть параметры для каждого объекта.
5. Для каждого объекта установите или снимите соответствующие флажки для действий, которые нужно разрешить или запретить в настраиваемой роли.
6. Для применения внесённых изменений нажмите **OK.**

1.1.3. Роль «Пользователь» и примеры авторизации

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

Пример 1.1. Полномочия для кластера

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

Пример 1.2. Полномочия PowerUser на ВМ

Иван — программист в отделе бухгалтерии. Для сборки и тестирования своих программ он использует виртуальные машины. Светлана создала для него виртуальный рабочий стол с названием `ivandesktop`. На ВМ со столом `ivandesktop` Ивану присвоена

роль **UserVmManager**, дающая ему доступ с Портала виртуальных машин к этой единственной ВМ. Поскольку Иван обладает полномочиями **UserVmManager**, то он может вносить изменения в параметры своей виртуальной машины. А поскольку **UserVmManager** является ролью пользователя, то данная роль не даёт ему возможности использовать Портал администрирования.

Пример 1.3. Полномочия роли PowerUser дата-центра

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

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

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

Пример 1.4. Полномочия сетевого администратора

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

Пример 1.5. Полномочия частной роли

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

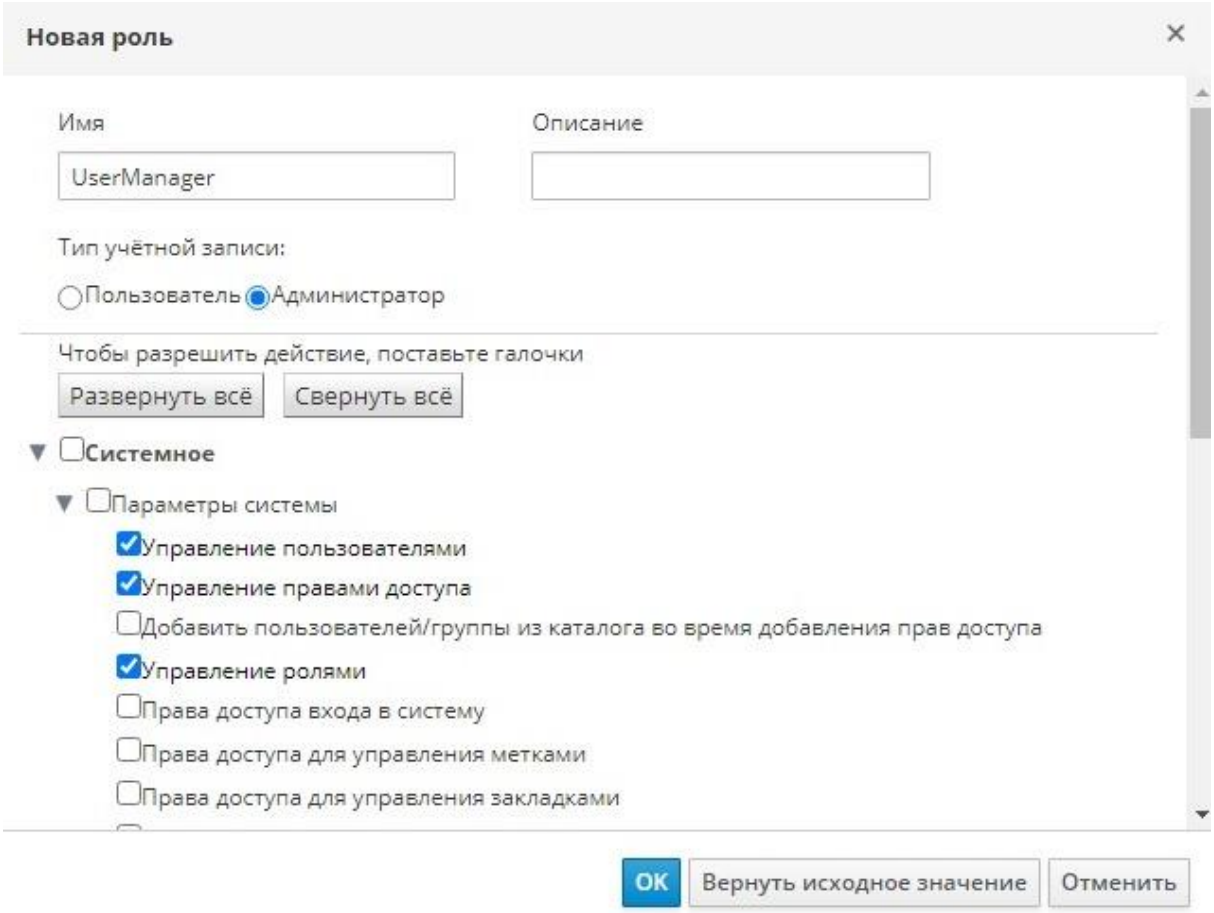

Рис. 2. Частная роль UserManager

Частная роль **UserManager** (Рис. 2) разрешает управление пользователями, полномочиями и ролями. Эти действия собраны в разделе **Система**, являющимся самым верхним объектом иерархии, показанной на Рис. 3, что означает, что эти действия применимы ко всем другим объектам в системе. **Тип учётной записи**, указанной для этой роли — **Администратор**, а это означает, что после присвоения этой роли, Раиса сможет использовать как Портал администрирования, так и Портал ВМ.

Рис. 3. Иерархия объектов системы виртуализации

1.2. Системные полномочия

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

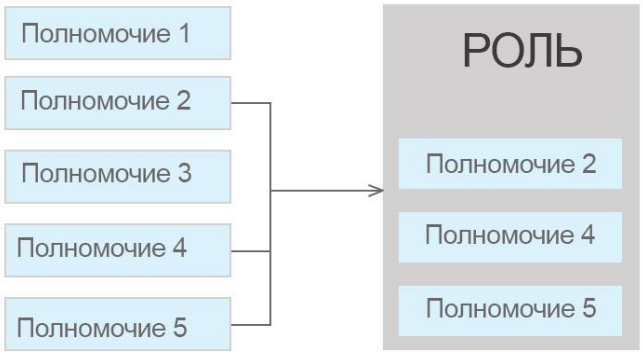

Рис. 4. Полномочия и роли

1.2.1. Свойства пользователя

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

Система виртуализации ROSA Virtualization предоставляет широкий диапазон предварительно настроенных ролей, от администратора с системными полномочиями до конечного пользователя с доступом только к одной ВМ. Хотя роли по умолчанию нельзя изменять или удалять, их можно копировать (клонировать) и редактировать, а также можно создавать новые роли согласно необходимым требованиям.

В системе виртуализации ROSA Virtualization поддерживаются следующие типы ролей:

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

1.2.2. Роли и привилегии пользователей

В **Табл. 1.1.** описываются базовые роли пользователей, предоставляющие полномочия на доступ к виртуальным машинам и их параметрам на Портале ВМ.

Табл. 1.1. Базовые роли пользователей в системе виртуализации

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

В **Табл.1.2** описываются продвинутые роли пользователей, позволяющие выполнять более тонкую настройку полномочий на ресурсы на Портале ВМ.

Табл.1.2. Продвинутые роли пользователей в системе виртуализации

Роль	Привилегии	Примечания
UserTemplateBasedVm	Привилегии, ограниченные только использованием шаблонов	Пользователь может использовать шаблоны для создания виртуальных машин
DiskOperator	Пользователь виртуального диска	Пользователь может использовать, просматривать и изменять виртуальные диски. Пользователь наследует полномочия на использование ВМ, к которой присоединён виртуальный диск
VmCreator	Пользователь может создавать виртуальные машины на Портале ВМ	Эта роль не применяется к конкретной ВМ. Присваивайте эту роль пользователю в масштабах всего окружения в окне **Параметры**, или присваивайте эту роль в конкретных дата-центрах / кластерах. При присвоении этой роли в кластерах, также нужно присваивать роль DiskCreator в масштабах всего дата-центра или конкретных доменов хранилищ
TemplateCreator	Пользователь может создавать, редактировать и удалять шаблоны ВМ в рамках присвоенных ресурсов	Эта роль не присваивается к конкретному шаблону. Присваивайте эту роль пользователю в масштабах всего окружения в окне **Параметры**, или присваивайте эту роль в конкретных дата-

Роль	Привилегии	Примечания
		центрах, кластерах или доменах хранилищ
DiskCreator	Пользователь может создавать, редактировать, управлять и удалять виртуальные диски в рамках присвоенных кластеров или дата-центров	Эта роль не присваивается конкретному виртуальному диску. Присваивайте эту роль пользователю в масштабах всего окружения в окне **Параметры**, или присваивайте эту роль в конкретных дата-центрах, кластерах или доменах хранилищ
TemplateOwner	Пользователь может изменять и удалять шаблоны, присваивать и управлять полномочиями пользователей на шаблон	Эта роль автоматически присваивается пользователю, создающему шаблон. Другие пользователи, не имеющие полномочий TemplateOwner для шаблона, не могут просматривать или использовать этот шаблон
VnicProfileUser	Пользователь логических сетей и сетевых интерфейсов виртуальной машины и шаблона	Пользователь может присоединять или отсоединять сетевые интерфейсы конкретных логических сетей

1.2.3. Роли и привилегии администраторов

В **Табл. 1.3** описываются базовые административные роли, дающие полномочия на доступ и настройку ресурсов на Портале администрирования.

Табл. 1.3. Базовые роли администраторов в системе виртуализации

Роль	Привилегии	Примечания
SuperUser	Системный администратор ROSA Virtualization	Суперпользователь обладает полными полномочиями на все объекты и уровни (администрирует все объекты во всех дата-центрах)
VirtAdmin	Администратор ROSA Virtualization	Пользователь обладает административными полномочиями на все объекты в рамках системы виртуализации
ClusterAdmin	Администратор кластера	Пользователь обладает административными полномочиями на все объекты в рамках конкретного кластера
DataCenterAdmin	Администратор дата-центра	Пользователь обладает административными полномочиями на все объекты в рамках конкретного дата-центра, за исключением хранилища

Примечание — не используйте пользователя-администратора сервера каталогов в качестве пользователя-администратора системы виртуализации. Создайте на сервере каталогов пользователя специально для использования в качестве пользователя-администратора системы виртуализации.

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

В **Табл. 1.4** описываются продвинутые роли администраторов, позволяющие выполнять более тонкую настройку полномочий на ресурсы на Портале администрирования.

Табл. 1.4. Продвинутые роли администраторов в системе виртуализации

Роль	Привилегии	Примечания
TemplateAdmin	Администратор шаблона ВМ	Пользователь может создавать, удалять и настраивать домены хранилищ и сетевые параметры шаблонов, а также перемещать шаблоны между доменами
StorageAdmin	Администратор хранилища	Пользователь может создавать, удалять, настраивать и управлять присвоенным доменом хранилища
HostAdmin	Администратор хоста	Пользователь может присоединять, удалять, настраивать и управлять конкретным хостом
NetworkAdmin	Сетевой администратор	Пользователь может настраивать и управлять сетью конкретного дата-центра или кластера. Сетевой администратор дата-центра или кластера наследует сетевые полномочия на виртуальные пулы в рамках кластера
VmAdmin	Администратор ВМ	Пользователь обладает административными полномочиями на все ВМ
VmDeveloper	Разработчик ВМ	Пользователь обладает привилегиями на создание и управление конфигурацией ВМ и шаблонов
VmPoolAdmin	Системный администратор виртуального пула	Пользователь может создавать, удалять и настраивать виртуальный пул, присваивать и удалять пользователей виртуального пула, а также выполнять базовые операции на ВМ в пуле
GlusterAdmin	Администратор хранилища Gluster	Пользователь может создавать, удалять, настраивать и управлять томами хранилища Gluster
VmImporterExporter	Администратор импорта и экспорта виртуальных машин	Пользователь может импортировать и экспортировать ВМ. Пользователь имеет возможность просматривать все ВМ и шаблоны, экспортированные другими пользователями
SecurityAdmin	Администратор безопасности	Пользователь имеет возможность просматривать журнал событий безопасности и формировать отчеты с данными из этого журнала

1.2.4. Присвоение ресурсу роли администратора или пользователя

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

Присвоение роли ресурсу

1. Найдите название нужного ресурса и нажмите на него, чтобы просмотреть детали.
2. Перейдите на вкладку **Права доступа** (Рис. 5), чтобы указать присвоенных пользователей, роль пользователя и наследуемые полномочия для выбранного ресурса.

3. Нажмите **Добавить**.

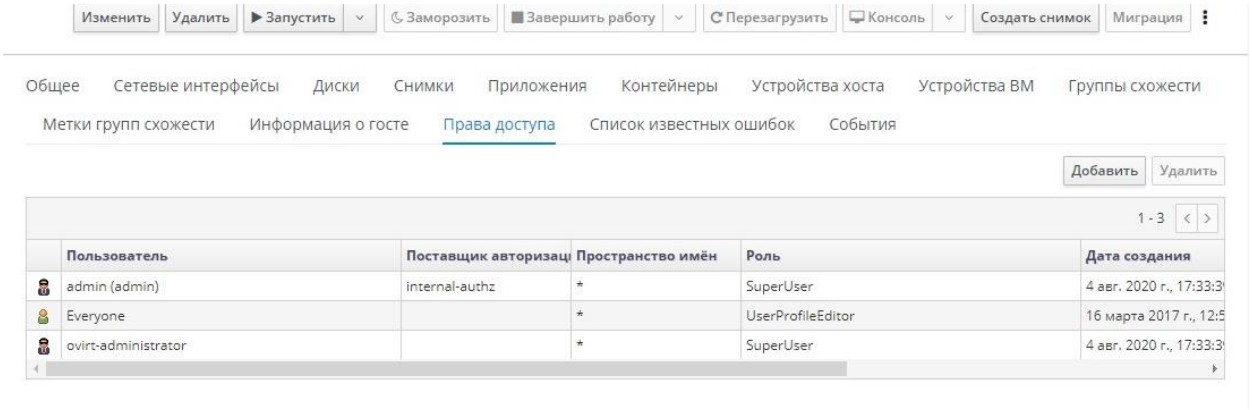

Рис. 5. Вкладка права доступа

4. Укажите имя существующего пользователя в поле **Поиск** и нажмите **Выполнить**. Из полученного списка возможных совпадений выберите пользователя.
5. Из выпадающего списка **Присвоить роль** выберите нужную роль (Рис. 6).
6. Нажмите **OK**.

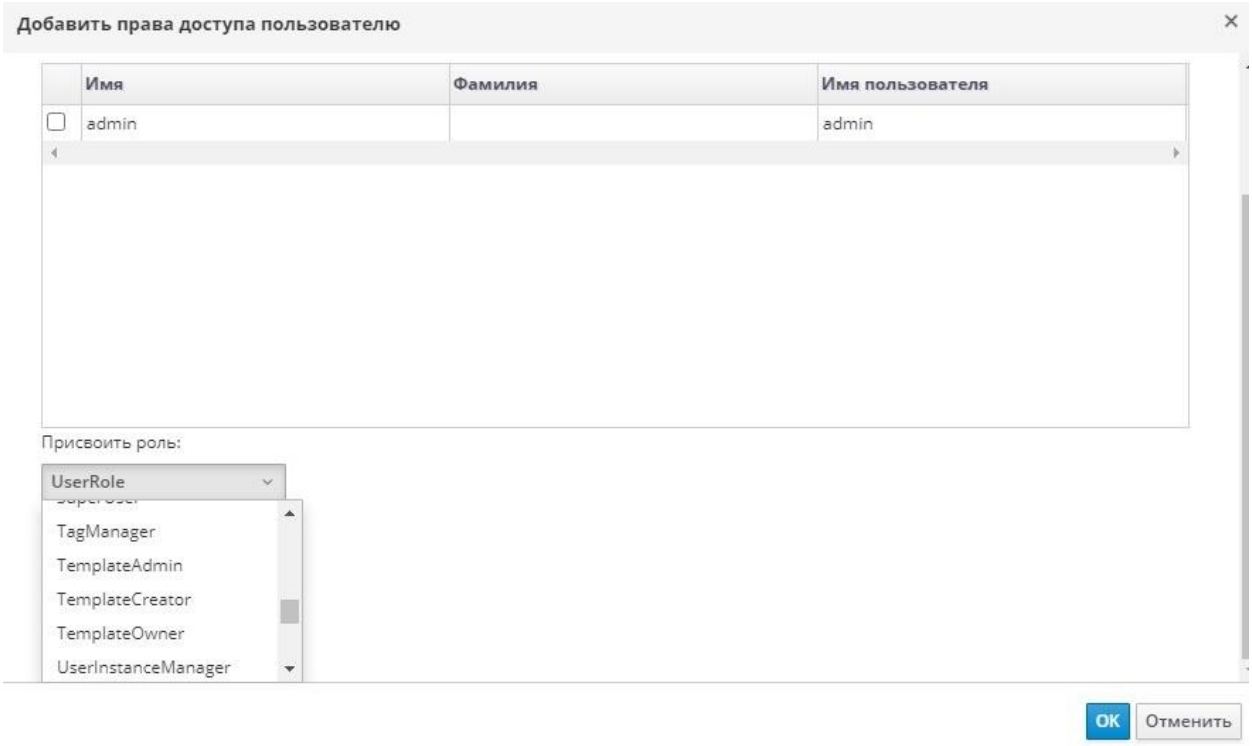

Рис. 6. Присвоение роли пользователю

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

Примечание — присваивать роли и полномочия можно только существующим пользователям.

1.2.5. Удаление роли администратора или пользователя с ресурса

При удалении роли с ресурса пользователь теряет на этом ресурсе наследуемые полномочия, связанные с ролью.

Удаление роли с ресурса

1. Найдите название нужного ресурса и нажмите на него, чтобы просмотреть детали.
2. Перейдите на вкладку **Права доступа**, чтобы указать присвоенных пользователей, роль пользователя и наследуемые полномочия для выбранного ресурса.
3. Выберите пользователя, удаляемого с ресурса.
4. Нажмите кнопку **Удалить** (Рис. 7)**.**
5. Нажмите **OK**.

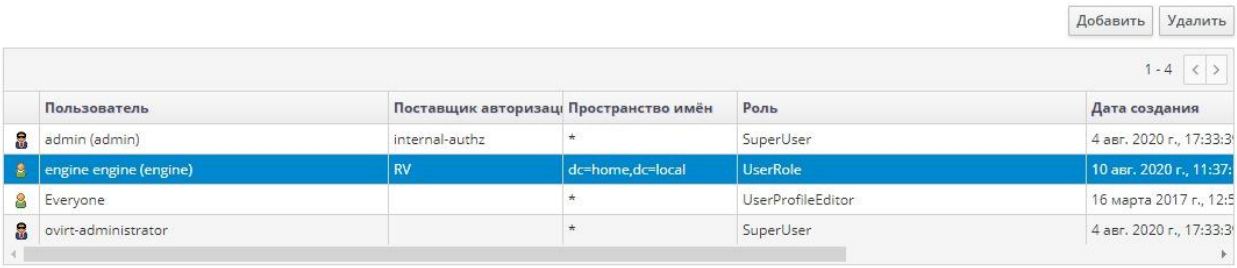

Рис. 7. Удаление роли

1.2.6. Управление системными полномочиями в дата-центре

Администратор дата-центра — это роль системного администратора только для конкретного дата-центра. Она удобна в среде виртуализации с несколькими дата-центрами, где каждому дата-центру требуется администратор. Роль **DataCenterAdmin** является иерархической моделью, таким образом пользователь, которому назначена роль администратора дата-центра, может управлять всеми объектами в дата-центре за исключением хранилища этого дата-центра.

С помощью кнопки **Параметры** на панели заголовков назначайте администраторов дата-центров для всех дата-центров в окружении.

Роль администратора дата-центра разрешает выполнять следующие действия:

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

Для смены администратора дата-центра удалите существующего администратора и создайте нового.

В **Табл. 1.5** описываются административные роли и привилегии, применимые в администрировании дата-центров.

Табл. 1.5. Административные роли с полномочиями в дата-центре

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

1.2.7. Управление системными полномочиями в кластере

Администратор кластера — это роль системного администратора только для конкретного кластера. Она удобна в среде виртуализации с несколькими кластерами, где каждому кластеру требуется администратор. Роль **ClusterAdmin** является иерархической моделью, таким образом пользователь, которому назначена роль администратора кластера, может управлять всеми объектами в кластере.

С помощью кнопки **Параметры** на панели заголовков назначайте администраторов кластеров для всех кластеров в окружении.

Роль администратора кластера разрешает выполнять следующие действия:

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

Для смены администратора кластера удалите существующего администратора и создайте нового.

В **Табл. 1.6** описываются административные роли и привилегии, применимые в администрировании кластеров.

Табл. 1.6. Административные роли с полномочиями в кластере

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

1.2.8. Управление сетевыми системными полномочиями

Сетевой администратор — это роль системного администратора, которую можно применить для конкретной сети или для всех сетей в дата-центре, кластере, хосте, виртуальной машине или шаблоне. Сетевой пользователь может исполнять ограниченные административные роли, такие как просмотр и присоединение сетей на конкретной ВМ или конкретном шаблоне.

Для назначения сетевого администратора всем сетям в окружении используйте кнопку **Параметры** на панели заголовков.

Роль сетевого администратора позволяет выполнять следующие действия:

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

Пользователю, создавшему сеть, автоматически присваиваются полномочия **NetworkAdmin** в созданной сети.

Для смены администратора сети удалите существующего администратора и создайте нового.

В **Табл. 1.7** описываются роли сетевого администратора и сетевого пользователя, а также привилегии, используемые в сетевом администрировании.

Табл. 1.7. Роли сетевого администратора и сетевого пользователя

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

1.2.9. Управление системными полномочиями для хоста

Администратор хоста — это административная роль для одного конкретного хоста. Данная роль удобна для кластеров с множеством хостов, где для каждого хоста нужен системный администратор.

Используйте кнопку **Параметры** на панели заголовков для назначения администратора для всех хостов окружения.

Роль администратора хоста разрешает выполнять следующие действия:

- Настройка параметров хоста.
- Настройка логических сетей.
- Удаление хоста.

Для смены администратора хоста удалите существующего администратора и создайте нового.

В **Табл.1.8** описывается роль администратора, а также привилегии, применяемые для администрирования хостов.

Табл.1.8. Административная роль с полномочиями на хосте

Роль	Привилегии	Примечания
HostAdmin	Администратор хоста	Пользователь может настраивать, управлять и удалять конкретный хост, а также может выполнять действия, касающиеся сети на конкретном хосте

1.2.10. Управление системными полномочиями в домене хранилища

Администратор хранилища — это роль системного администрирования только для одного конкретного домена хранилища. Данная роль удобна в дата-центрах с несколькими доменами хранилищ, где для каждого домена хранилища требуется свой системный администратор.

Используйте кнопку **Параметры** на панели заголовков для назначения администратора хранилища для всех доменов хранилищ окружения.

Роль администратора домена хранилища позволяет выполнять следующие действия:

- Изменение конфигурации домена хранилища.
- Перевод домена хранилища в режим обслуживания.
- Удаление домена хранилища.

Для смены администратора домена хранилища удалите существующего администратора и создайте нового.

В **Табл. 1.9** описываются роли администратора, а также привилегии, применяемые для администрирования доменов хранилищ.

Табл. 1.9. Административные роли с полномочиями в домене хранилища

Роль	Привилегии	Примечания
StorageAdmin	Администратор хранилища	Пользователь может создавать, удалять, настраивать и управлять конкретным доменом хранилища
GlusterAdmin	Администратор хранилища Gluster	Пользователь может создавать, удалять, настраивать и управлять томами хранилища Gluster

1.2.11. Управление системными полномочиями на пул виртуальных машин

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

Роль администратора пула ВМ позволяет выполнять следующие действия:

- Создание, изменение и удаление пулов.
- Добавление и откребление ВМ от пулов.

В **Табл. 1.10** описываются роли администратора, а также привилегии, применяемые для администрирования пулов.

Табл. 1.10. Административные роли с полномочиями в пуле

Роль	Привилегии	Примечания
VmPoolAdmin	Роль системного администратора виртуального пула	Пользователь может создавать, удалять и настраивать виртуальный пул, присваивать и удалять пользователей виртуального пула, а также выполнять базовые операции на виртуальной машине
ClusterAdmin	Администратор кластера	Пользователь может использовать, создавать, удалять и управлять всеми пулами ВМ в конкретном кластере

1.2.12. Управление системными полномочиями на виртуальные диски

Диспетчер виртуализации предоставляет две изначальные роли пользователя виртуальных дисков (**DiskCreator** и **DiskOperator**), но не предоставляет изначальной роли администратора виртуальных дисков.

Роль создателя виртуальных дисков **DiskCreator** предоставляет возможность администрирования виртуальных дисков на Портале ВМ. Роль **DiskCreator** можно применить к конкретным ВМ, к дата-центру, к конкретному домену хранилища или ко всему виртуализированному окружению в целом. Данная роль удобна тем, что позволяет различным пользователям управлять различными виртуальными ресурсами.

Роль создателя виртуальных дисков **DiskCreator** позволяет выполнять следующие действия:

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

В **Табл. 1.11** описываются роли пользователей и привилегии, применимые для использования и администрирования виртуальных дисков на Портале ВМ.

Табл. 1.11. Административные роли с полномочиями на виртуальные диски

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

1.2.13. Настройка шифра для старых версий SPICE

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

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

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

Изменение строки шифра

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

   Например:

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

2. Вставьте в файл следующее содержимое и сохраните файл:

   ```
   name:  oVirt - setup weaker SPICE encryption for old clients
   hosts: hostname
   vars:
   ```

```
    host_deploy_spice_cipher_string: 'DEFAULT:-RC4:-3DES:-DES'
roles:
  - ovirt-host-deploy-spice-encryption
```

3. Запустите только что созданный файл:

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

Как вариант, можно изменить параметры хоста с помощью Ansible playbook `ovirt-host-deploy` с параметром `--extra-vars` и переменной `host_deploy_spice_cipher_string` следующим образом:

```
# ansible-playbook -l hostname --extra-vars host_deploy_spice_cipher_string="DEFAULT:-RC4:-3DES:-DES" /usr/share/ovirt-engine/playbooks/ovirt-host-deploy.yml
```

1.3. Политики планирования

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

Диспетчер системы виртуализации по умолчанию предоставляет пять политик планирования — **Evenly_Distributed**, **Cluster_Maintenance**, **None**, **Power_Saving** и **VM_Evenly_Distributed**. Также можно настроить новые политики, предлагающие тонко настроенный контроль распределения виртуальных машин. Вне зависимости от политики планирования, виртуальная машина не станет начинать работу на хосте с перегруженным ЦП. По умолчанию, ЦП хоста считается перегруженным, если в течение 5 минут его загрузка составляет более 80%, но эти значения можно изменить с помощью политик планирования.

Рис. 8. Политика планирования равномерного распределения (Evenly Distributed)

Политика планирования **Evenly_Distributed** равномерно распределяет загрузку на память и вычисления ЦП между всеми хостами в кластере. Дополнительные ВМ, прикреплённые к хосту, не начнут работу, если этот хост достиг хотя бы одного из

указанных значений для параметров **CpuOverCommitDurationMinutes**, **HighUtilization** или **MaxFreeMemoryForOverUtilized**.

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

Рис. 9. Политика планирования энергосбережения (Power Saving)

Политика планирования **Power_Saving** (Рис. 9) распределяет память и вычислительные мощности ЦП между хостами в выборке доступных хостов для снижения потребления энергии на недостаточно загруженных хостах. Виртуальные машины с хостов, имеющих нагрузку на ЦП ниже указанного значения слабой загрузки в течение интервала времени, превышающего указанный интервал, будут мигрировать на другие хосты с тем, чтобы работу данного хоста можно было завершить. Дополнительные ВМ, прикреплённые к хосту, не начнут работу, если этот хост достиг указанного значения высокого коэффициента использования.

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

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

1.3.1. Создание политик планирования

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

Создание политики планирования

1. Нажмите **Администрирование → Настроить**.
2. Перейдите на вкладку **Политики планирования** (Рис. 10).

3. Нажмите **Добавить**.

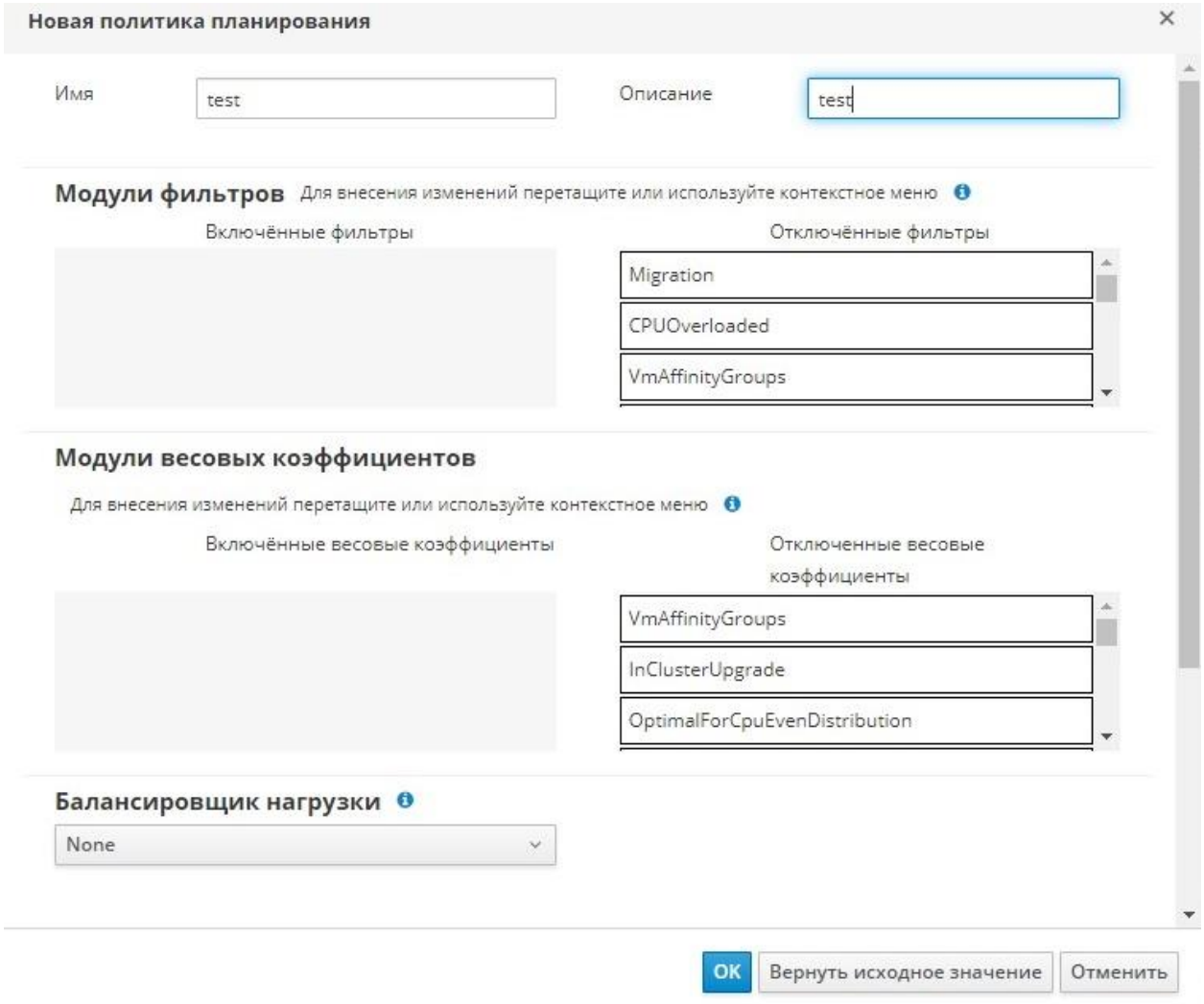

Рис. 10. Создание политики планирования

4. Укажите **Имя** и **Описание** политики планирования.
5. Настройте модули фильтров:
   a. В разделе **Модули фильтров** перетащите предпочитаемые модули фильтров из раздела **Отключённые фильтры** в раздел **Включённые фильтры** для применения фильтров в политике планирования.
   b. Конкретные модули фильтров также можно настроить как **Первый**, чтобы у него был наивысший приоритет, или **Последний**, чтобы он получил самый низкий приоритет, для базовой оптимизации. Чтобы установить приоритет, нажмите на необходимый модуль фильтра, наведите курсор на пункт **Местоположение** и выберите **Первый** или **Последний**.
6. Настройте модули веса:
   a. В разделе **Модули весовых коэффициентов** перетащите предпочитаемые модули веса из области **Отключённые весовые коэффициенты** в область **Включённые весовые коэффициенты**, чтобы применить весовые коэффициенты к политике планирования.
   b. С помощью кнопок + и – слева от включённых модулей веса повышайте или уменьшайте вес этих модулей.
7. Укажите политику балансировки нагрузки:

a. Из выпадающего списка в разделе **Балансировщик нагрузки** выберите политику балансировки нагрузки, которая будет применяться в политике планирования.
b. Из выпадающего списка в разделе **Параметры** выберите свойство балансировки нагрузки, которое нужно применить в политике планирования, и в текстовом поле справа от этого свойства укажите значение.
c. С помощью кнопок **+** и **–** добавьте или удалите дополнительные свойства.

8. Нажмите **OK**.

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

В **Табл. 1.12** приведено подробное описание параметров, доступных в окнах «Новая политика планирования» и «Параметры политики планирования».

Табл. 1.12. Параметры в окнах «Новая политика планирования» и «Параметры политики планирования»

Поле	Описание
Имя	Название политики планирования. Это название используется для наименования этой политики в виртуализированном ЦУ (СУСВ)
Описание	Описание политики планирования. Это поле рекомендуется заполнить, но оно не обязательно
Модули фильтров	Набор фильтров для контролирования хоста, на котором может выполняться ВМ из кластера (включённый фильтр будет отсеивать хосты, не соответствующие условиям фильтра): • `CpuPinning`: хосты, не отвечающие определению привязки задачи к процессору. • `Migration`: предотвращение миграции на один и тот же хост. • `PinToHost`: хосты, отличные от того хоста, за которым закреплена ВМ. • `CPU-Level`: хосты, не соответствующие топологии ЦП виртуальной машины. • `CPU`: хосты с меньшим числом ЦП, чем число, указанное для ВМ. • `Memory`: хосты с недостаточным объёмом памяти для работы ВМ. • `VmAffinityGroups`: хосты, не отвечающие условиям, указанным для ВМ-участницы группы схожести. Например, ВМ в группе схожести должны работать на одном и том же хосте или на разных хостах. • `VmToHostsAffinityGroups`: группа хостов, не отвечающих условиям, указанным для ВМ-участницы группы схожести. Например, виртуальные машины в группе схожести должны выполняться на хостах группы или на отельном хосте, не являющимся участником группы. • `InClusterUpgrade`: хосты, работающие под управлением ОС более ранней версии, чем версия ОС хоста, на котором на данный момент выполняется ВМ. • `HostDevice`: хосты, не поддерживающие устройства, требуемые для ВМ. • `HA`: принудительный запуск ВМ из окружения диспетчера виртуализации только на хостах с положительной оценкой высокой доступности. • `Emulated-Machine`: хосты без должной поддержки эмулируемой машины. • `Network`: хосты, на которых не установлены сети, требуемые контроллером сетевого интерфейса ВМ, или на которых не установлена сеть визуализации кластера. • `HostedEnginesSpares`: резервация места под ВМ диспетчера виртуализации на указанном числе узлов диспетчера виртуализации.

Поле	Описание
	• `Label`: хосты без требуемых меток схожести. • `Compatibility-Version`: запуск ВМ только на хостах с корректной версией совместимости. • `CPUOverloaded`: хосты с перегруженными ЦП.
Модули весовых коэффициентов	Набор весовых коэффициентов для настройки относительного приоритета факторов, учитываемых при определении в кластере хостов, на которых могут выполняться ВМ: • `InClusterUpgrade`: определяет весовой коэффициент хоста в соответствии с версией ОС хоста. Вес сильнее «наказывает» хосты с более ранней версией ОС, чем хосты с версией ОС, аналогичной версии ОС того хоста, на котором в данный момент выполняется ВМ. Таким образом предпочтение всегда отдаётся хостам с более актуальными версиями ОС. • `OptimalForHaReservation`: определяет весовой коэффициент хостов в соответствии с их оценкой высокой доступности. • `None`: определяет весовой коэффициент хостов согласно модулю равномерного распределения. • `OptimalForEvenGuestDistribution`: определяет весовой коэффициент хостов в соответствии с числом ВМ, выполняемых на этих хостах. • `VmAffinityGroups`: определяет весовой коэффициент хостов в соответствии с группой схожести, определённой для ВМ. В соответствии с параметрами этой группы схожести, модуль веса определяет вероятность того, будут ли ВМ в группе схожести выполняться на одном и том же хосте или на разных хостах. • `VmToHostsAffinityGroups`: определяет весовой коэффициент хостов в соответствии с группами схожести, настроенными для машин. Весовой модуль определяет вероятность того, будут ли ВМ в группе схожести выполняться на одном из хостов-участников группы, или на отдельном хосте, не состоящем в группе. • `OptimalForCPUPowerSaving`: определяет весовой коэффициент хостов в соответствии с загрузкой ЦП хостов. Приоритет отдаётся хостам с наиболее высокой загрузкой ЦП. • `OptimalForEvenCpuDistribution`: определяет весовой коэффициент хостов в соответствии с загрузкой ЦП хостов. Приоритет отдаётся хостам с наиболее низкой загрузкой ЦП. • `HA`: определяет весовой коэффициент хостов в соответствии с оценкой их высокой доступности. • `PreferredHosts`: во время настройки ВМ приоритет отдаётся «*предпочитаемым*» хостам. • `OptimalForMemoryPowerSaving`: определяет весовой коэффициент хостов в соответствии с их потреблением памяти. Приоритет отдаётся хостам с более низким объёмом доступной памяти. • `OptimalForMemoryEvenDistribution`: определяет весовой коэффициент хостов в соответствии с их потреблением памяти. Приоритет отдаётся хостам с более высоким объёмом доступной памяти.
Балансировщик нагрузки	В этом выпадающем меню можно выбрать применяемый модуль балансировки нагрузки. Модули балансировки нагрузки определяют логику, используемую во время миграции ВМ с хостов с текущей высокой нагрузкой на хосты с текущей низкой нагрузкой
Параметры	В этом выпадающем меню можно добавить или удалить параметры модулей балансировки нагрузки. Это меню доступно только в случае выбора модуля балансировки нагрузки для политики планирования. По умолчанию, настроенных параметров нет, а доступные параметры относятся к выбранному модулю.

Поле	Описание
	Используйте кнопки + и – для добавления или удаления дополнительных свойств модуля балансировки нагрузки

1.4. Типы экземпляров

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

По умолчанию доступен набор предварительно настроенных типов экземпляров, приведенных в **Табл. 1.13**.

Табл. 1.13. Предварительно настроенные типы экземпляров

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

Администраторы также могут создавать, редактировать и удалять типы экземпляров на вкладке **Типы экземпляров** окна **Параметры**.

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

1.4.1. Создание типов экземпляров

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

Создание типа экземпляра

1. Нажмите **Администрирование → Настроить**.
2. Перейдите на вкладку **Типы экземпляров** (Рис. 11).

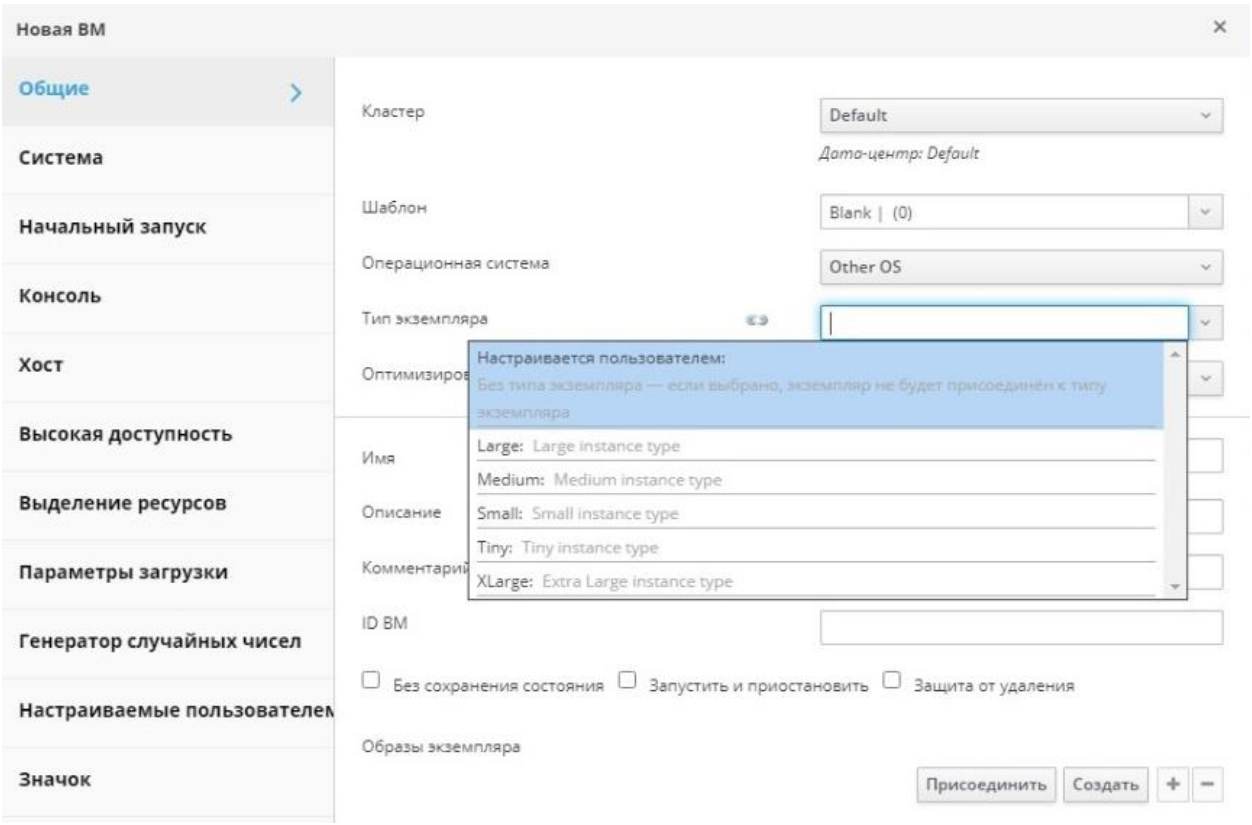

Рис. 11. Выбор типа экземпляра

3. Нажмите **Добавить**.
4. Введите **Имя** и **Описание** типа экземпляра.
5. Нажмите **Показать расширенные параметры** и настройте параметры типа экземпляра так, как это необходимо. Параметры, присутствующие в окне **Новый тип экземпляра**, идентичны параметрам в окне **Новая виртуальная машина**, но присутствуют только поля, имеющие отношение к типам экземпляров (см. Приложение A.1. VDSM).
6. Нажмите **OK**.

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

1.4.2. Изменение типов экземпляров

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

Изменение параметров типов экземпляров

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

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

В параметрах существующих ВМ, основанных на этом типе экземпляра, будут показаны поля со значком цепи, и информация в этих полях будет обновлена. Если во время

изменения типа экземпляра выполнялись ВМ, то рядом с такими ВМ появится оранжевый значок «Изменения, ожидающие применения», а информация в полях со значком цепи будет обновлена во время следующего перезапуска.

1.4.3. Удаление типов экземпляров

Удаление типа экземпляра

1. Нажмите **Администрирование → Настроить**.
2. Перейдите на вкладку **Типы экземпляров**.
3. Выберите удаляемый тип экземпляра.
4. Нажмите **Удалить**.
5. При наличии ВМ, созданных на основе этого типа экземпляра, появится предупреждающее окно со списком привязанных машин. Для удаления типа экземпляра установите флажок **Подтвердить операцию**. В противном случае нажмите **Отмена**.
6. Нажмите **ОК**.

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

1.5. Пулы адресов MAC

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

Несколько кластеров могут разделять один и тот же пул адресов MAC, но каждому кластеру присваивается один пул. Система виртуализации создаёт изначальный пул адресов MAC, который используется в случае, если не будет присвоено ни одного пула. Подробности о присвоении кластерам пулов адресов MAC приведены в п. 8.2.1. Создание нового кластера.

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

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

Полномочия пользователей пула задаются через роли и определяют, какие дата-центры могут использовать пул адресов MAC. Подробности о добавлении новых полномочий пользователям приведены в п. 1.1. Роли.

1.5.1. Создание пулов адресов MAC

Создание пула адресов MAC

1. Нажмите **Администрирование → Настроить**.
2. Перейдите на вкладку **Пул MAC адресов** (Рис. 12).

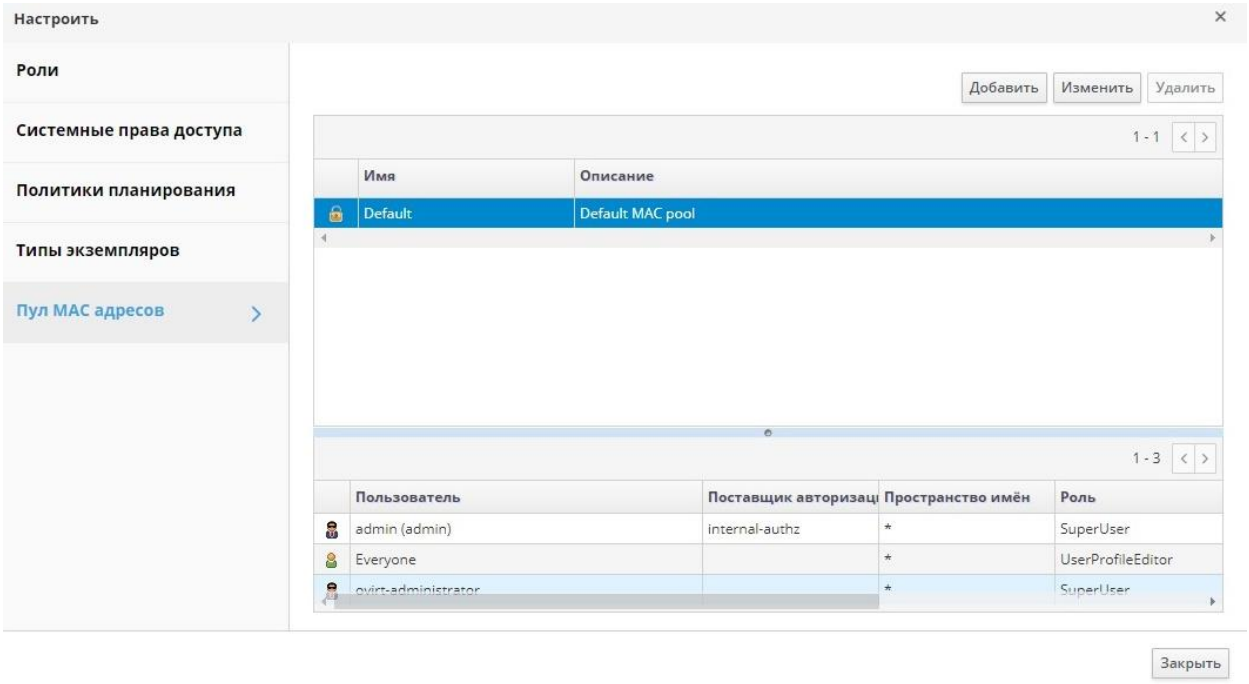

Рис. 12. Меню «Пул MAC адресов»

3. Нажмите **Добавить**.
4. Введите **Имя** и **Описание** нового пула адресов MAC (Рис. 13).
5. Установите флажок **Разрешить дубликаты**, чтобы разрешить использование в пуле одного и того же адреса MAC более одного раза. Пул не будет автоматически использовать дублирующий адрес MAC, но включение параметра, разрешающего дубликаты, означает, что пользователь может вручную использовать дублирующий адрес.

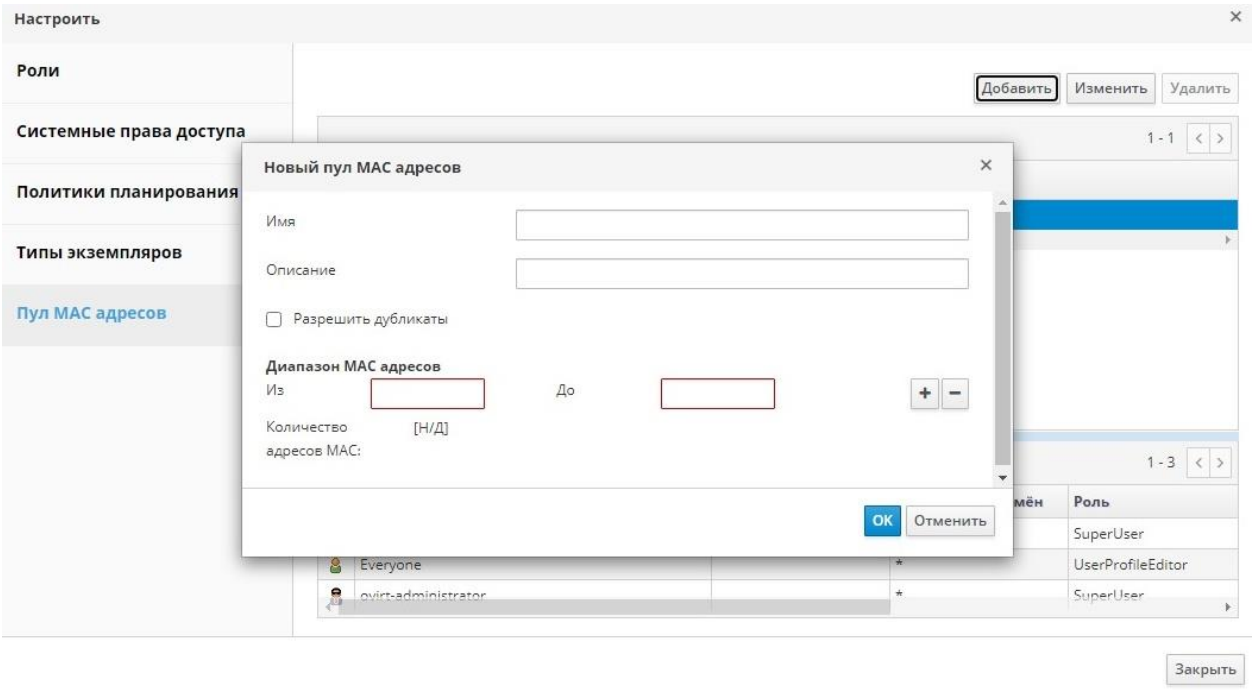

Рис. 13. Новый пул MAC адресов

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

6. Укажите необходимый **Диапазон MAC адресов**. Для указания нескольких диапазонов нажмите кнопку **+** в одной строке с полями **Из** и **До**.
7. Нажмите **OK**.

1.5.2. Изменение пулов адресов MAC

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

Изменение параметров пулов адресов MAC

1. Нажмите **Администрирование → Настроить**.
2. Перейдите на вкладку **Пул MAC адресов** (Рис. 12).
3. Выберите изменяемый пул.
4. Нажмите **Изменить**.
5. Необходимым образом измените поля **Имя**, **Описание**, **Разрешить дубликаты** и **Диапазон MAC адресов**.

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

6. Нажмите **OK**.

1.5.3. Удаление пулов адресов MAC

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

Удаление пула адресов MAC

1. Нажмите **Администрирование → Настроить**.

2. Перейдите на вкладку **Пул MAC адресов** (Рис. 12).
3. Выберите удаляемый пул.
4. Нажмите **Удалить**.
5. Нажмите **OK**.

Глава 2. Панель мониторинга

Панель мониторинга (Рис. 14) предлагает общий обзор состояния системы виртуализации с помощью сводки сведений о её ресурсах и общем коэффициенте использования. Эта сводка может предупредить о проблеме и даёт возможность проанализировать проблемную область.

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

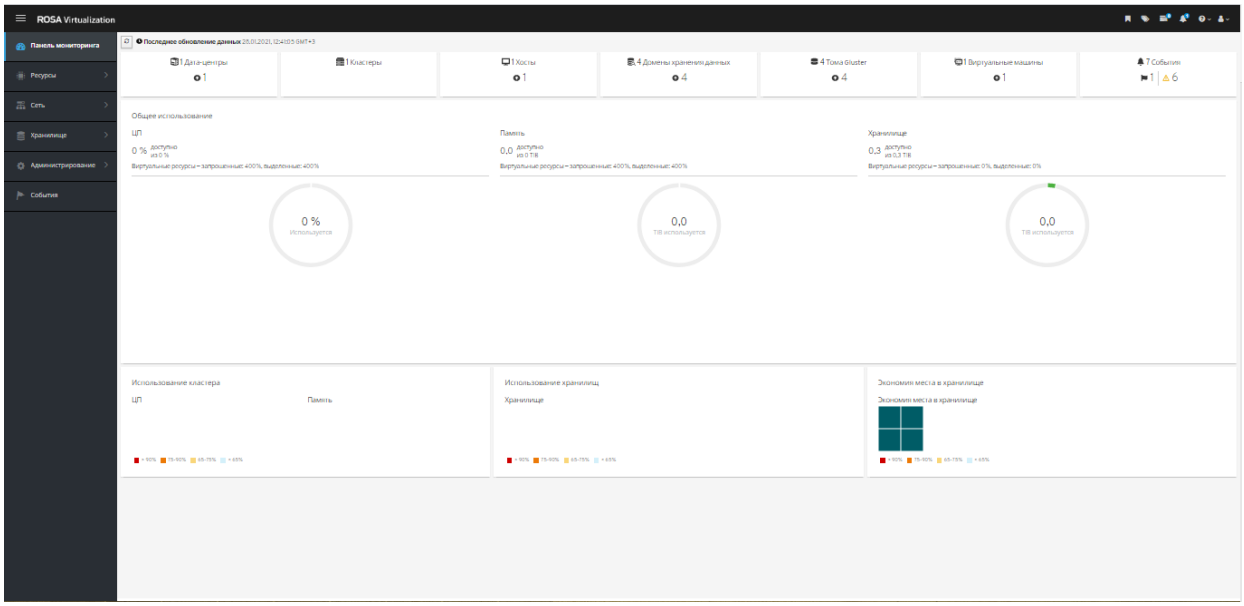

Рис. 14. Панель мониторинга

2.1. Предварительные условия для установки

Для панели мониторинга необходимо установленное и настроенное хранилище данных.

2.2. Общий перечень

Самый верхний раздел панели мониторинга предлагает общий перечень ресурсов системы виртуализации (Рис. 15), в который входят разделы для дата-центров, кластеров, хостов, доменов хранилищ, виртуальных машин и событий. Значки показывают состояние каждого ресурса, а числа — количество ресурсов с этим статусом.

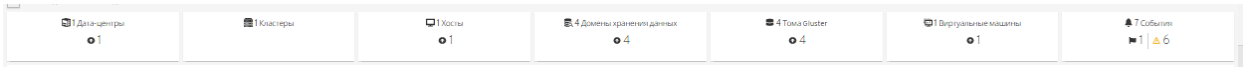

Рис. 15. Общий перечень ресурсов

Заголовок показывает номер типа ресурса, а статус ресурса показывается под заголовком. В **Табл. 2.1** приведено описание статусов ресурсов и значков, отображающих

состояние ресурсов. Нажав на ресурс, можно перейти на соответствующую страницу диспетчера виртуализации. Статус кластеров всегда показывается как «Недоступно».

Табл. 2.1. Статусы ресурсов

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

2.3. Общий коэффициент использования

Раздел **Общее использование** (Рис. 16) показывает коэффициент использования ЦП, памяти и хранилища.

Рис. 16. Общее использование

В верхнем разделе отображается процент доступных ресурсов ЦП, памяти или хранилища, а также процент превышенного выделения ресурсов. Процент превышенного выделения ресурсов ЦП, например, рассчитывается при помощи деления числа виртуальных ядер на число физических ядер, доступных для выполняющихся ВМ, на основании самых свежих данных в хранилище данных.

На круговых графиках отображаются процентные значения использования ЦП, памяти или хранилища, а также среднее потребление для всех хостов на основе среднего потребления за последние 5 минут. Наведение курсора на сегмент кругового графика покажет значение выделенного сегмента.

Линейный график в нижней части отображает тенденции за последние 24 часа. Каждая точка данных показывает среднее потребление за указанный час. Наведение курсора на точку графика покажет время и процентное использование для графика ЦП и объём использования для графиков памяти и хранилища.

2.3.1. Наиболее используемые ресурсы

Нажатие на круговой график (Рис. 16) в разделе общего использования панели мониторинга покажет список наиболее используемых ресурсов ЦП (Рис. 17), памяти или хранилища.

Рис. 17. Наиболее используемые ресурсы (ЦП)

Для ЦП и памяти всплывающий список показывает десять хостов и ВМ с наиболее высоким потреблением. Для хранилища всплывающий список покажет десять наиболее используемых доменов хранилищ и ВМ. Стрелка справа от панели использования показывает тенденции потребления этого ресурса за последнюю минуту.

2.4. Использование кластера

В разделе **Использование кластера** (Рис. 18) на тепловой карте отображается использование ЦП и памяти.

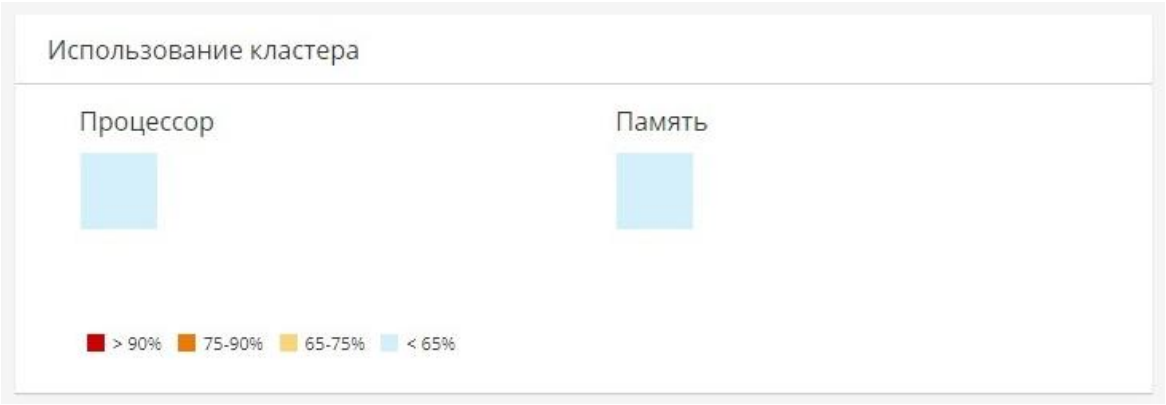

Рис. 18. Использование кластера

2.4.1. Использование ЦП

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

2.4.2. Использование памяти

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

2.5. Использование хранилищ

В разделе **Использование хранилищ** (Рис. 19) на тепловой карте показывается процент использования хранилища.

Рис. 19. Использование хранилищ

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

Глава 3. Поиск

3.1. Операции поиска в системе виртуализации

Портал администрирования предоставляет возможность управления тысячами ресурсов, такими как виртуальные машины, хосты, пользователи и многие другие. Чтобы выполнить поиск, введите поисковый запрос (простой текстовый запрос или на основе предопределенного синтаксиса) в поле поиска, доступное на главной странице каждого ресурса. Поисковые запросы можно сохранять в виде закладок для дальнейшего использования, чтобы не выполнять повторный поиск по ресурсам вручную. Поиск не чувствителен к регистру.

3.2. Примеры поиска и поисковый синтаксис

Поисковые запросы по ресурсам системы виртуализации имеют следующий синтаксис:

```
result type: {criteria} [sortby sort_spec]
```

Примеры синтаксиса

В **Табл. 3.1** показаны примеры использования поисковых запросов, приведенные для понимания того, как выполняется помощь в построении поисковых запросов в системе виртуализации.

Табл. 3.1. Примеры поисковых запросов

Пример	Результат
Hosts: Vms.status = up page 2	Показывает страницу 2 списка всех хостов, на которых размещаются ВМ со статусом *запущена* (Up)
Vms: domain = qa.company.com	Показывает список всех ВМ, выполняющихся в указанном домене
Vms: users.name = Mary	Показывает список всех ВМ, принадлежащих пользователям с именем пользователя Mary
Events: severity > normal sortby time	Показывает список всех событий с серьёзностью выше нормальной и с сортировкой по времени

3.3. Автодополнение поиска

В помощь при создании действенных и эффективных поисковых запросов предлагается функционал автодополнения. При частичном вводе поискового запроса под поисковой панелью раскрывается список возможных вариантов следующей части запроса. Можно либо выбрать пункт из списка и ввести или выбрать следующую часть поискового запроса, либо продолжить вводить запрос вручную.

В **Табл. 3.2** приводятся конкретные примеры того, как автодополнение помогает в составлении следующего поискового запроса — `Hosts: Vms.status = down`

Табл. 3.2. Примеры поисковых запросов, выполненных с использованием автодополнения

Ввод	Показываемые в списках элементы	Действие
h	`Hosts` (только один вариант)	Выбрать или ввести Hosts
Hosts:	Все свойства хоста	Ввести v
Hosts: v	Свойства хоста, начинающиеся с `v`	Выбрать или ввести Vms
Hosts: Vms	Все свойства ВМ	Ввести s
Hosts: Vms.s	Все свойства ВМ, начинающиеся с `s`	Выбрать или ввести status

Ввод	Показываемые в списках элементы	Действие
Hosts: Vms.status	= !=	Выбрать или ввести =
Hosts: Vms.status =	Все значения статуса	Выбрать или ввести down

3.4. Типы результатов поиска

Тип результата даёт возможность выполнять поиск по ресурсам любого из следующих типов:

- **Vms** для списка ВМ.
- **Host** для списка хостов.
- **Pools** для списка пулов.
- **Template** для списка шаблонов.
- **Events** для списка событий.
- **Users** для списка пользователей.
- **Cluster** для списка кластеров.
- **DataCenter** для списка дата-центров.
- **Storage** для списка доменов хранения.

Поскольку каждый тип ресурсов имеет свой уникальный набор свойств и набор других типов ресурсов, связанных с данным типом, то у каждого типа поиска есть набор рабочих сочетаний синтаксиса. Также, для быстрого создания действительных поисковых запросов можно использовать возможности автодополнения.

3.5. Критерии поиска

Критерии поиска указываются в поиске после двоеточия.

Синтаксис критериев поиска `{criteria}` следующий:

`<prop><operator><value>` или `<obj-type><prop><operator><value>`

В **Табл. 3.3** приведено описание составных частей синтаксиса и примеры критериев поиска:

Табл. 3.3. Примеры критериев поиска

Часть	Описание	Значения	Пример	Примечание
prop	Свойство искомого ресурса. Также может быть свойством типа ресурса (`obj-type`) или меткой (tag)	Ограничьте поиск объектами с определёнными свойствами. Ищите, например, объекты со свойством **status**	Status	
obj-type	Тип ресурса, который может быть связан с поисковым ресурсом	Системные объекты. Например, дата-центры и ВМ	Users	
operator	Операторы сравнения	= != (не равно) > < >= <=		Параметры значений зависят от свойств

Часть	Описание	Значения	Пример	Примечание
Значение (Value)	То, с чем сравнивается выражение	Запись (строка) Целое число Порядок Дата (форматируется в соответствии с региональными параметрами)	Jones 256 normal	В строках можно использовать символы подстановки ""(две кавычки, без пробелов между ними) могут использоваться в качестве неинициализированной (пустой) строки. Строка или дата, содержащие пробелы, должны заключаться в двойные кавычки

3.6. Несколько критериев поиска и символы подстановки

Символы подстановки можно использовать в части `<value>` синтаксиса для строк. Например, чтобы найти всех пользователей, начинающихся с буквы `m`, введите `m*`.

Выполнить поиск по двум критериям можно с помощью двух логических операторов `AND` и `OR`. Например, следующий запрос вернёт список всех выполняющихся ВМ пользователей, чьи имена пользователей начинаются с буквы `m`:

```
Vms: users.name = m* AND status = Up
```

Следующий запрос вернёт список всех ВМ с меткой `paris-loc` пользователей, чьи имена пользователей начинаются с буквы `m`:

```
Vms: users.name = m* AND tag = "paris-loc"
```

Примечание — при указании двух критериев без операторов `AND` или `OR`, предполагается `AND`. Оператор `AND` идёт перед `OR`, а оператор `OR` идёт перед предполагаемым `AND`.

3.7. Определение порядка поиска

Порядок сортировки возвращаемой информации можно определить с помощью `sortby`. При этом можно указать направление сортировки (`asc` для прямой, `desc` для обратной).

Например, следующий запрос возвращает все события с серьёзностью выше нормальной, отсортированные по времени (в обратном порядке):

```
events: severity > normal sortby time desc
```

3.8. Поиск дата-центров

В **Табл. 3.4** описываются все параметры поиска дата-центров.

Табл. 3.4. Поиск дата-центров

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
`Clusters.`*`clusters-prop`*	Зависит от типа свойства	Свойство кластера, связанное с дата-центром
`name`	Строка	Имя дата-центра
`description`	Строка	Описание дата-центра
`type`	Строка	Тип дата-центра

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
status	Список	Доступность дата-центра
sortby	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

Например, следующий запрос возвращает список дата-центров с типом хранилища NFS и любыми статусами, кроме «*Запущен*» (up):

```
Datacenter: type = nfs and status != up
```

3.9. Поиск кластеров

В **Табл. 3.5** описываются все параметры поиска кластеров.

Табл. 3.5. Поиск кластеров

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
Datacenter.*datacenter-prop*	Зависит от типа свойства	Свойства дата-центра, связанного с кластером
Datacenter	Строка	Дата-центр, к которому принадлежит кластер
name	Строка	Уникальное имя, идентифицирующее кластеры в сети
description	Строка	Описание кластера
initialized	Строка	*Верно* или *ложно* для статуса кластера
sortby	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

Например, следующий запрос возвращает список инициализированных кластеров или кластеров с именем `Default`:

```
Clusters: initialized = true or name = Default
```

3.10. Поиск хостов

В **Табл. 3.6** описываются все параметры поиска хостов.

Табл. 3.6. Поиск хостов

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
Vms.*Vms-prop*	Зависит от типа свойства	Свойство ВМ, связанных с хостом
Templates.*templates-prop*	Зависит от типа свойства	Свойство шаблонов, связанных с хостом
Events.*events-prop*	Зависит от типа свойства	Свойство событий, связанных с хостом
Users.*users-prop*	Зависит от типа свойства	Свойство пользователей, связанных с хостом
name	Строка	Имя хоста
status	Список	Доступность хоста
external_status	Строка	Работоспособность хоста, согласно полученным сообщениям от внешних служб и модулей
cluster	Строка	Кластер, к которому принадлежит хост

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
address	Строка	Уникальное имя, идентифицирующее хост в сети
cpu_usage	Целое число	Процент используемой вычислительной мощности
mem_usage	Целое число	Процент используемой памяти
network_usage	Целое число	Процент используемой сети
load	Целое число	Ожидающие в **run-queue** задачи на процессор, в указанный отрезок времени
version	Целое число	Число версии ОС
cpus	Целое число	Число ЦП на хосте
memory	Целое число	Объём доступной памяти
cpu_speed	Целое число	Вычислительная скорость ЦП
cpu_model	Строка	Тип ЦП
active_vms	Целое число	Число, выполняющихся на данный момент ВМ
migrating_vms	Целое число	Число, мигрирующих на данный момент ВМ
committed_mem	Целое число	Процент выделенной памяти
tag	Строка	Метка, присвоенная хосту
type	Строка	Тип хоста
datacenter	Строка	Дата-центр, к которому принадлежит хост
sortby	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

3.11. Поиск сетей

В **Табл. 3.7** описываются все параметры поиска сетей.

Табл. 3.7. Поиск сетей

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
Cluster_network.*clusternetwork-prop*	Зависит от типа свойства	Свойство кластера, связанное с сетью
Host_Network.*hostnetwork-prop*	Зависит от типа свойства	Свойство хоста, связанное с сетью
name	Строка	Имя, идентифицирующее сеть
description	Строка	Ключевые слова или текст, описывающие сеть, используемые по желанию при создании сети
vlanid	Целое число	VLAN ID сети
stp	Строка	Включён или отключён протокол STP для сети
mtu	Целое число	Максимальное значение MTU логической сети
vmnetwork	Строка	Используется ли сеть только для переноса трафика ВМ
datacenter	Строка	Дата-центр, к которому присоединена сеть
sortby	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
page	Целое число	Номер страницы результатов поиска

3.12. Поиск хранилищ

В **Табл. 3.8** описываются все параметры поиска хранилищ.

Табл. 3.8. Поиск хранилищ

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
Hosts.*hosts-prop*	Зависит от типа свойства	Свойства хостов, связанные с хранилищем
Clusters.*clusters-prop*	Зависит от типа свойства	Свойства кластеров, связанные с хранилищем
name	Строка	Уникальное имя, идентифицирующее хранилище в сети
status	Строка	Статус домена хранения
external_status	Строка	Работоспособность домена хранения, согласно полученным сообщениям от внешних служб и модулей
datacenter	Строка	Дата-центр, которому принадлежит хранилище
type	Строка	Тип хранилища
size	Целое число	Размер хранилища
used	Целое число	Используемый объём хранилища
committed	Целое число	Выделенный объём хранилища
sortby	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

Например, следующий запрос возвращает список хранилищ, общий объём которых больше 200 Гбайт, или с используемым объёмом меньше 50 Гбайт:

```
Storage: size > 200 or used < 50
```

3.13. Поиск дисков

В **Табл. 3.9** описываются параметры поиска дисков.

Примечание — для уменьшения отображаемого числа виртуальных дисков используйте параметры фильтрации `Disk Type` и `Content Type`.

Табл. 3.9. Поиск дисков

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
Datacenters.*datacenters-prop*	Зависит от типа свойства	Свойство дата-центров, связанное с диском
Storages.*storages-prop*	Зависит от типа свойства	Свойство хранилища, связанное с диском
alias	Строка	Имя, идентифицирующее хранилище в сети
description	Строка	Ключевые слова или текст с описанием диска, при желании добавляемые при создании диска
provisioned_size	Целое число	Виртуальный размер диска

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
size	Целое число	Размер диска
actual_size	Целое число	Фактический размер, выделенный диску
creation_date	Целое число	Дата создания диска
bootable	Строка	Можно ли загружаться с диска. Принимаемые значения: 0, 1, да, нет
shareable	Строка	Можно ли присоединять диск одновременно к нескольким ВМ. Принимаемые значения: 0, 1, да, нет
format	Строка	Формат диска. Принимаемые значения: unused, unassigned, cow, raw
status	Строка	Статус диска. Принимаемые значения: unassigned, ok, locked, invalid, illegal
disk_type	Строка	Тип диска. Принимаемые значения: image, lun
number_of_vms	Целое число	Число ВМ, к которым присоединён диск
vm_names	Строка	Имена ВМ, к которым присоединён диск
quota	Строка	Имя квоты, принудительно применяющейся к виртуальному диску
sortby	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

Например, следующий запрос возвращает список виртуальных дисков в формате `unused` и с выделенным размером диска больше 8 Гбайт:

```
Disks: format = unused and provisioned_size > 8
```

3.14. Поиск томов

В **Табл. 3.10** описываются параметры поиска томов.

Табл. 3.10. Поиск томов

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
Cluster	Строка	Имя кластера, связанное с томом
Cluster.*cluster-prop*	Зависит от типа свойства (например: имя, описание, комментарий, архитектура)	Свойства кластеров, связанные с томом
name	Строка	Имя, идентифицирующее том
type	Строка	Принимаемые значения: распределённый (distribute), реплицированный (replicate), распределённый реплицированный

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
		(distributed_replicate), чередующийся (stripe), распределённый чередующийся (distributed_stripe)
transport_type	Целое число	Принимаемые значения: TCP,RDMA
replica_count	Целое число	Число реплик
stripe_count	Целое число	Число чередующихся частей
status	Строка	Статус тома. Принимаемые значения: *запущен* (up) или *не запущен* (down)
sortby	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

Например, следующий запрос возвращает список томов с типом RDMA и с не менее двумя чередующимися частями:

```
Volume: transport_type = rdma and stripe_count >= 2
```

3.15. Поиск виртуальных машин

В **Табл. 3.11** описываются параметры поиска ВМ.

Примечание — на данный момент свойства *Метка сети*, *Настроенная пользователем эмулируемая машина* и *Настроенный пользователем тип ЦП* не поддерживаются в качестве параметров поиска.

Табл. 3.11. Поиск ВМ

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
Hosts.*hosts-prop*	Зависит от типа свойства	Свойство хостов, связанное с ВМ
Templates.*templates-prop*	Зависит от типа свойства	Свойство шаблонов, связанное с ВМ
Events.*events-prop*	Зависит от типа свойства	Свойство событий, связанное с ВМ
Users.*users-prop*	Зависит от типа свойства	Свойство пользователей, связанное с ВМ
Storage.*storage-prop*	Зависит от типа свойства	Свойство устройств хранения, связанное с ВМ
Vnic.*vnic-prop*	Зависит от типа свойства	Свойство VNIC, связанное с ВМ
name	Строка	Имя ВМ
status	Список	Доступность ВМ
ip	Целое число	IP-адрес ВМ
uptime	Целое число	Время работы ВМ в минутах
domain	Строка	Домен (обычно Active Directory), в котором собраны машины
os	Строка	ОС, выбранная при создании ВМ
creationdate	Дата	Дата создания ВМ
address	Строка	Уникальное имя, идентифицирующее ВМ в сети
cpu_usage	Целое число	Используемый процент вычислительной мощности
mem_usage	Целое число	Используемый процент ресурсов памяти

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
network_usage	Целое число	Используемый процент ресурсов сети
memory	Целое число	Максимальная определяемая память
apps	Строка	Приложения, установленные на данный момент в ВМ
cluster	Список	Кластер, к которому принадлежит ВМ
pool	Список	Пул ВМ, к которому принадлежит ВМ
loggedinuser	Строка	Имя пользователя, выполнившего вход в ВМ на данный момент
tag	Список	Метки ВМ
datacenter	Строка	Дата-центр, которому принадлежит ВМ
type	Список	Тип ВМ (сервер или рабочий стол)
quota	Строка	Имя квоты, связанной с ВМ
description	Строка	Ключевые слова или текст с описанием диска, при желании добавляемые при создании ВМ
sortby	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска
next_run_configuration_exists	Логическое значение	Наличие у ВМ параметров с несохраненными изменениями

Например, следующий запрос возвращает список ВМ, имя базового шаблона которых начинается с `Win`, и которые присвоены любому пользователю:

```
Vms: template.name = Win* and user.name = ""
```

3.16. Поиск пулов

В **Табл. 3.12** описываются параметры поиска пулов.

Табл. 3.12. Поиск пулов

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
name	Строка	Имя пула
description	Строка	Описание пула
type	Список	Тип пула
sortby	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

Например, следующий запрос возвращает список пулов с типом `automatic`:

```
Pools: type = automatic
```

3.17. Поиск шаблонов

В **Табл. 3.13** описываются параметры поиска шаблонов.

Табл. 3.13. Поиск по шаблонам

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
Vms.*Vms-prop*	Строка	Свойства ВМ, связанные с шаблоном
Hosts.*hosts-prop*	Строка	Свойства хостов, связанные с шаблоном
Events.*events-prop*	Строка	Свойства событий, связанные с шаблоном
Users.*users-prop*	Строка	Свойства пользователей, связанные с шаблоном

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
name	Строка	Имя шаблона
domain	Строка	Домен шаблона
os	Строка	Тип ОС
creationdate	Целое число	Дата создания шаблона. Формат даты: мм/дд/гг
childcount	Целое число	Число ВМ, созданных на базе шаблона
mem	Целое число	Определяемая память
description	Строка	Описание шаблона
status	Строка	Статус шаблона
cluster	Строка	Кластер, связанный с шаблоном
datacenter	Строка	Дата-центр, связанный с шаблоном
quota	Строка	Квота, связанная с шаблоном
sortby	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

Например, следующий запрос возвращает список шаблонов, на базе которых были созданы ВМ с событиями нормального или более высокого уровня серьёзности, и эти машины выполняются:

```
Template: Events.severity >= normal and Vms.uptime > 0
```

3.18. Поиск пользователей

В **Табл. 3.14** описываются параметры поиска пользователей.

Табл. 3.14. Поиск пользователей

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
Vms.*Vms-prop*	Зависит от типа свойства	Свойство ВМ, связанное с пользователем
Hosts.*hosts-prop*	Зависит от типа свойства	Свойство хостов, связанное с пользователем
Templates.*templates-prop*	Зависит от типа свойства	Свойство шаблонов, связанное с пользователем
Events.*events-prop*	Зависит от типа свойства	Свойство событий, связанное с пользователем
name	Строка	Имя пользователя
lastname	Строка	Фамилия пользователя
usrname	Строка	Уникальное имя пользователя
department	Строка	Учреждение пользователя
group	Строка	Группа пользователей
title	Строка	Должность пользователя
status	Строка	Статус пользователя
role	Строка	Роль пользователя
tag	Строка	Метка пользователя
pool	Строка	Пул пользователя
sortby	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

Например, следующий запрос возвращает список пользователей, на ВМ которых случались события нормального или более высокого уровня серьёзности, и эти машины выполняются или приостановлены:

```
Users: Events.severity > normal and Vms.status = up or Vms.status =
pause
```

3.19. Поиск событий

В **Табл. 3.15** описываются все параметры, которые можно использовать для поиска событий. Для многих параметров предлагается автодополнение (в зависимости от параметров).

Табл. 3.15. Поиск событий

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
`Vms.`*`Vms-prop`*	Зависит от типа свойства	Свойства ВМ, связанные с событием
`Hosts.`*`hosts-prop`*	Зависит от типа свойства	Свойства хостов, связанные с событием
`Templates.`*`templates-prop`*	Зависит от типа свойства	Свойства шаблонов, связанные с событием
`Users.`*`users-prop`*	Зависит от типа свойства	Свойства пользователей, связанные с событием
`Clusters.`*`clusters-prop`*	Зависит от типа свойства	Свойства кластеров, связанные с событием
`Volumes.`*`Volumes-prop`*	Зависит от типа свойства	Свойства томов, связанные с событием
`type`	Список	Тип события
`severity`	Список	Уровень серьёзности события: *предупреждение* / *ошибка* / *нормальный*
`message`	Строка	Описание типа события
`time`	Список	День, когда случилось событие
`usrname`	Строка	Имя пользователя, связанное с событием
`event_host`	Строка	Хост, связанный с событием
`event_vm`	Строка	ВМ, связанная с событием
`event_template`	Строка	Шаблон, связанный с событием
`event_storage`	Строка	Хранилище, связанное с событием
`event_datacenter`	Строка	Дата-центр, связанный с событием
`event_volume`	Строка	Том, связанный с событием
`correlation_id`	Целое число	Идентификационный номер события
`sortby`	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
`page`	Целое число	Номер страницы результатов поиска

Например, следующий запрос возвращает список событий, которые произошли на ВМ с именем `testdesktop` во время выполнения данной ВМ на хосте `gonzo.example.com`:

```
Events: Vms.name = testdesktop and Hosts.name = gonzo.example.com
```

Глава 4. Закладки

4.1. Сохранение строки поискового запроса в виде закладки

Закладку можно использовать для сохранения поискового запроса и поделиться им с другими пользователями.

Сохранение поискового запроса в виде закладки

1. Введите нужный поисковый запрос в строку поиска и запустите поиск.
2. Нажмите на кнопку **Закладка** в виде звёздочки справа от строки поиска, чтобы открыть окно **Новая закладка**.
3. Введите **Имя** закладки.
4. При необходимости, измените поле **Строка поиска**.
5. Нажмите **OK**.

Чтобы найти и выбрать закладку, нажмите на значок **Закладки** () на панели заголовков.

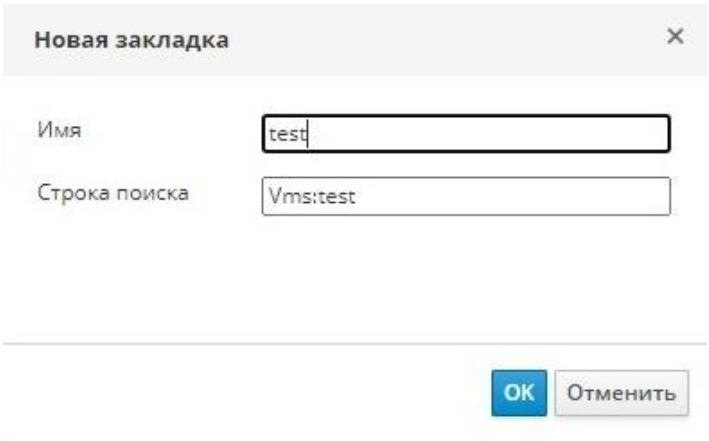

Рис. 20. Создание закладки

4.2. Редактирование закладок

Название и строку поиска закладок можно изменять.

Редактирование закладок

1. Нажмите на значок **Закладки** () на панели заголовков.
2. Выберите закладку и нажмите **Изменить**.
3. Внесите необходимые изменения в поля **Имя** и **Строка поиска**.
4. Нажмите **OK**.

4.3. Удаление закладок

Если закладка больше не нужна, удалите её.

Удаление закладок

1. Нажмите на значок **Закладки** () на панели заголовков.
2. Выберите закладку и нажмите **Удалить**.
3. Нажмите **OK**.

Глава 5. Теги

5.1. Настройка взаимодействия с системой виртуализации с помощью тегов

После установки и настройки параметров платформы виртуализации, рабочий процесс взаимодействия с системой можно настроить с помощью тегов. С помощью тегов можно разделить системные ресурсы по группам и категориям. Это удобно в ситуациях, когда в окружении присутствует множество объектов и администратор хочет сконцентрироваться на работе с какой-то конкретной категорией объектов.

В данном разделе описывается создание и редактирование тегов, присвоение их хостам или ВМ, а также как выполнять поиск, используя теги в качестве поисковых запросов. Теги можно сортировать согласно иерархии, соответствующей структуре, а также согласно производственным требованиям.

Чтобы создать, изменить или удалить тег нажмите на значок **Теги** (🏷) на панели заголовков Портала администрирования.

5.2. Создание тегов

Создание тега

1. Нажмите на значок **Теги** (🏷) на панели заголовков.
2. Нажмите **Добавить** для добавления нового тега, или выберите тег и нажмите **Новый** для создания подчинённого тега.
3. Укажите **Имя** и **Описание** нового тега.
4. Нажмите **OK**.

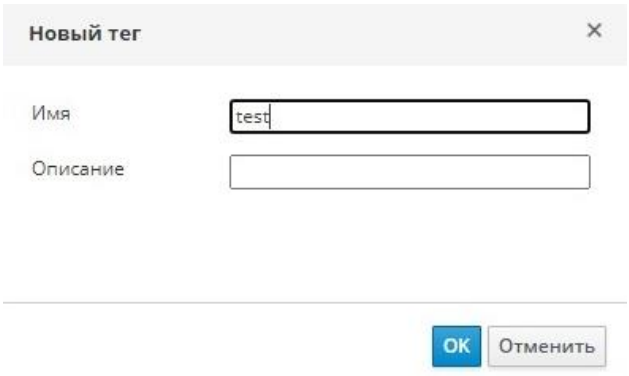

Рис. 21. Создание тега

5.3. Редактирование тегов

Название и описание тегов можно изменять.

Редактирование тега

1. Нажмите на значок **Теги** (🏷) на панели заголовков.
2. Выберите тег, который нужно изменить, и нажмите **Изменить**.
3. При необходимости внесите изменения в поля **Имя** и **Описание**.
4. Нажмите **OK**.

5.4. Удаление тега

Удаление тега

1. Нажмите на значок **Теги** (🏷) на панели заголовков.

2. Выберите тег, который нужно удалить, и нажмите **Удалить**. Будет показано сообщение с предупреждением о том, что удаление метки (тега) также удалит все подчинённые метки.
3. Нажмите **OK**.

В результате все теги и подчинённые теги будут удалены. Теги также снимаются с объектов, которым они были присвоены.

5.5. Присвоение тегов объектам и снятие меток с объектов

Хостам, виртуальным машинам и пользователям можно присваивать теги, а также снимать с них теги.

Присвоение тегов объектам и снятие тегов с объектов

1. Выберите объекты, которым нужно присвоить тег, или с которых нужно снять тег.
2. Нажмите **Больше действий** (⋮), а затем нажмите **Назначить теги**.
3. Установите соответствующий флажок, чтобы присвоить тег объекту, или снимите флажок, чтобы удалить тег объекта.
4. Нажмите **OK**.

В результате указанные теги будут присвоены объектам в виде настраиваемого пользователем свойства, или удалены.

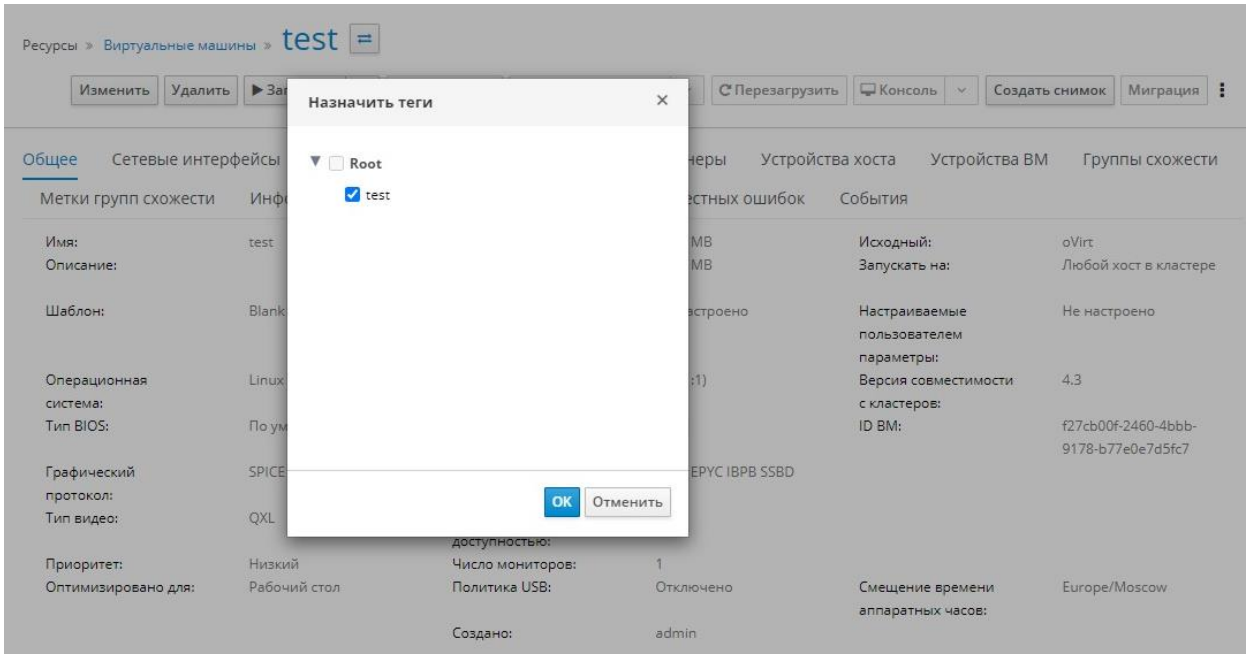

Рис. 22. Присвоение тегов объектам

5.6. Поиск объектов на основе тегов

Введите поисковый запрос с учетом регистра, используя `tag` как свойство, и укажите необходимое значение или набор значений в качестве критерия поиска.

Объекты с тегами, содержащими указанный критерий, будут показаны в списке результатов.

Примечание — если выполнить поиск, используя `tag` как свойство, и одновременно указать оператор неравенства `!=` (например, `Host: Vms.tag!=server1`), то в списке результатов не будут показаны объекты без тегов.

5.7. Сортировка хостов с помощью тегов

Сортировать информацию о хостах можно с помощью тегов, а затем осуществлять поиск хостов, основываясь на этих тегах.

Настройка тегов для хостов

1. Нажмите **Ресурсы → Хосты** и выберите хост.
2. Нажмите **Больше действий** (⋮), а затем нажмите **Присвоить тег**.
3. Установите флажки напротив необходимых тегов.
4. Нажмите **OK**.

В результате хостам будет добавлена дополнительная информация в виде тегов, используя которые можно выполнять поиск.

Часть II. Администрирование ресурсов

Глава 6. Качество обслуживания

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

6.1. Качество обслуживания хранилища

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

6.1.1. Создание записи о качестве обслуживания хранилища

Создание записи о качестве обслуживания хранилища

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS** (Рис. 23).
4. В разделе **Хранилище** нажмите **Добавить**.
5. Укажите **Имя QoS** и **Описание** для записи качества обслуживания.
6. Укажите **Пропускную способность** качества обслуживания, отметив один из переключателей:
   - **Нет**.
   - **Всего** — укажите максимально разрешённую общую пропускную способность в поле **Мбит/сек**.
   - **Чтение/запись** — укажите максимально разрешённую общую пропускную способность для операций чтения в левом поле **Мбит/сек** и максимально разрешённую общую пропускную способность для операций записи в правом поле **Мбит/сек**.
7. Укажите качество обслуживания ввода и вывода (**IOps**), отметив один из переключателей:
   - **Нет**.
   - **Всего** — укажите максимальное разрешённое число операций ввода и вывода в секунду в поле **IOps**.
   - **Чтение/запись** — укажите максимальное разрешённое число операций ввода в секунду в левом поле **IOps** и максимальное разрешённое число операций вывода в секунду в правом поле **IOps**.
8. Нажмите **OK**.

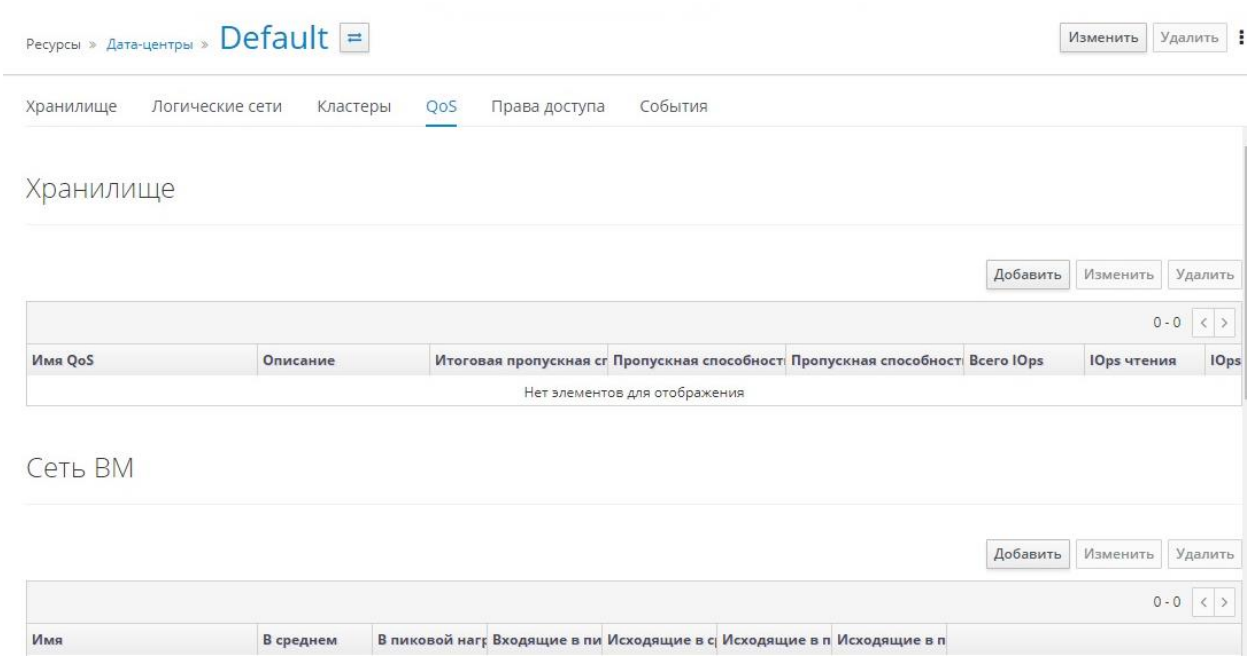

Рис. 23. Меню «Дата-центры»

В результате будет создана запись качества обслуживания для хранилища. После чего на основе этой записи можно создавать профили дисков в доменах хранилища данных, принадлежащих этому дата-центру.

6.1.2. Удаление записи о качестве обслуживания хранилища

Удаление записи качества обслуживания хранилища

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

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

6.2. Качество обслуживания сети виртуальной машины

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

6.2.1. Создание записи о качестве обслуживания сети ВМ

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

Создание записи о качестве обслуживания сети ВМ

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS (**Рис. 24**)**.

4. В разделе **Сеть ВМ** нажмите **Добавить.**
5. В окне **Новая QoS сети ВМ** введите **Имя** записи QoS сети ВМ.
6. Укажите лимиты для **Входящего** и **Исходящего** сетевого трафика.
7. Нажмите **OK**.

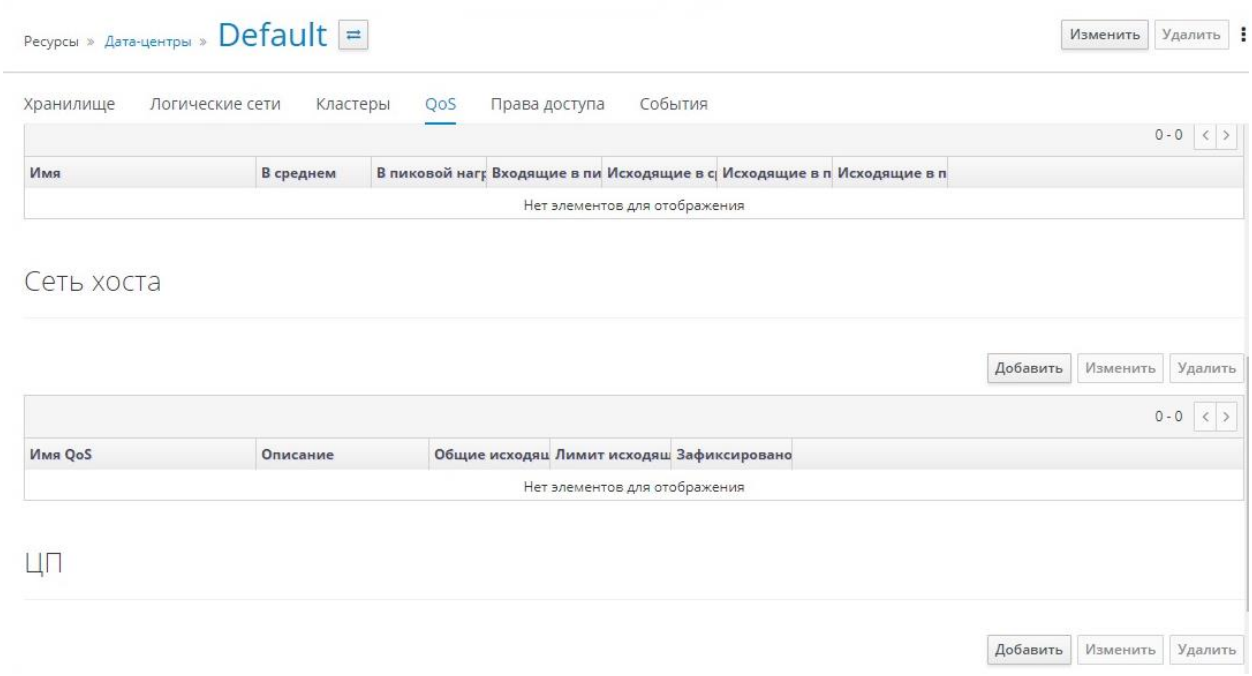

Рис. 24. Меню «Дата-центры»

В результате будет создана запись QoS сети ВМ, которую может использовать контроллер сетевого интерфейса виртуальной сети.

6.2.2. Параметры в окне «Новая QoS сети ВМ»

В **Табл. 6.1** описываются параметры качества обслуживания сети ВМ, которые предоставляют возможность настроить лимиты пропускной полосы как для входящего, так и для исходящего трафика на трёх разных уровнях.

Табл. 6.1. Параметры QoS сети ВМ

Поле	Описание
Дата-центр	Дата-центр, в который будет добавлена политика QoS сети ВМ. Это поле настраивается автоматически согласно выбранному дата-центру
Имя	Название, представляющее политику QoS сети ВМ в виртуализированном ЦУ
Входящий	Параметры, применяемые к входящему трафику. Установите или снимите соответствующие флажки на поле **Входящий** для включения или отключения следующих параметров: • **Средняя**: средняя скорость входящего трафика. • **Пиковая нагрузка**: скорость входящего трафика в период пиковой нагрузки. • **Пиковый всплеск**: скорость входящего трафика во время пиковых всплесков.
Исходящий	Параметры, применяемые к исходящему трафику. Установите или снимите соответствующие флажки на поле **Исходящий** для включения или отключения следующих параметров: • **Средняя**: средняя скорость исходящего трафика. • **Пиковая нагрузка**: скорость исходящего трафика в период пиковой нагрузки.

Поле	Описание
	• **Пиковый всплеск**: скорость исходящего трафика во время пиковых всплесков.

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

```
# engine-config -s MaxAverageNetworkQoSValue=2048
# systemctl restart ovirt-engine
```

6.2.3. Удаление записи о качестве обслуживания сети ВМ

Удаление записи о качестве обслуживания сети ВМ

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

6.3. Качество обслуживания сетей хоста

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

6.3.1. Создание записи о качестве обслуживания для сетей хоста

Создание записи о качестве обслуживания для сетей хоста

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS**.
4. В разделе **Сеть хоста** нажмите **Добавить**.
5. В окне **Новая QoS сети хоста** введите **Имя QoS** и **Описание** для записи о качестве обслуживания.
6. Укажите нужные значения **Взвешенной доли**, **Предела скорости (Мбит/с)** и **Гарантированной скорости (МБ/с)**.
7. Нажмите **OK**.

6.3.2. Параметры в окне «Новая QoS сети хоста»

В **Табл. 6.2** описываются параметры QoS сетей хоста, которые предоставляют возможность настроить лимиты пропускной способности для исходящего трафика.

Табл. 6.2. Параметры QoS сетей хоста

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

Чтобы изменить максимальное значение, разрешённое в полях **Предел скорости (Мбит/с)** и **Гарантированная скорость (МБ/с)**, используйте команду `engine-config` для изменения ключа конфигурации `MaxAverageNetworkQoSValue`. После чего для применения внесённых изменений необходимо перезапустить службу `ovirt-engine`:

```
# engine-config -s MaxAverageNetworkQoSValue=2048
# systemctl restart ovirt-engine
```

6.3.3. Удаление записи о качестве обслуживания для сетей хоста

Удаление записи о качестве обслуживания для сетей хоста

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

6.4. Качество обслуживания ЦП

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

6.4.1. Создание записи качества обслуживания для ЦП

Создание записи качества обслуживания для центрального процессора

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS**.
4. В разделе **ЦП** нажмите **Добавить**.

5. В окне **Новая QoS ЦП** введите **Имя QoS** и **Описание** для записи о качестве обслуживания.
6. В поле **Лимит (%)** введите максимальную вычислительную возможность, разрешаемую записью QoS (при этом не указывайте символ %).
7. Нажмите **OK**.

В результате будет создана запись о качестве обслуживания для ЦП, что позволяет на основе этой записи создавать профили ЦП в кластерах, принадлежащих выбранному дата-центру.

6.4.2. Удаление записи качества обслуживания для ЦП

Удаление записи QoS для центрального процессора

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

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

Глава 7. Дата-центры

7.1. Введение в понятие дата-центров

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

Дата-центр может содержать несколько кластеров, каждый из которых может содержать несколько хостов. У дата-центров может быть несколько связанных с ним доменов хранилищ, а также дата-центр может поддерживать несколько виртуальных машин на каждом из своих хостов. В окружении системы виртуализации ROSA Virtualization может находиться несколько дата-центров. При этом инфраструктура дата-центров позволяет управлять ими отдельно друг от друга.

Все дата-центры управляются средствами одного Портала администрирования.

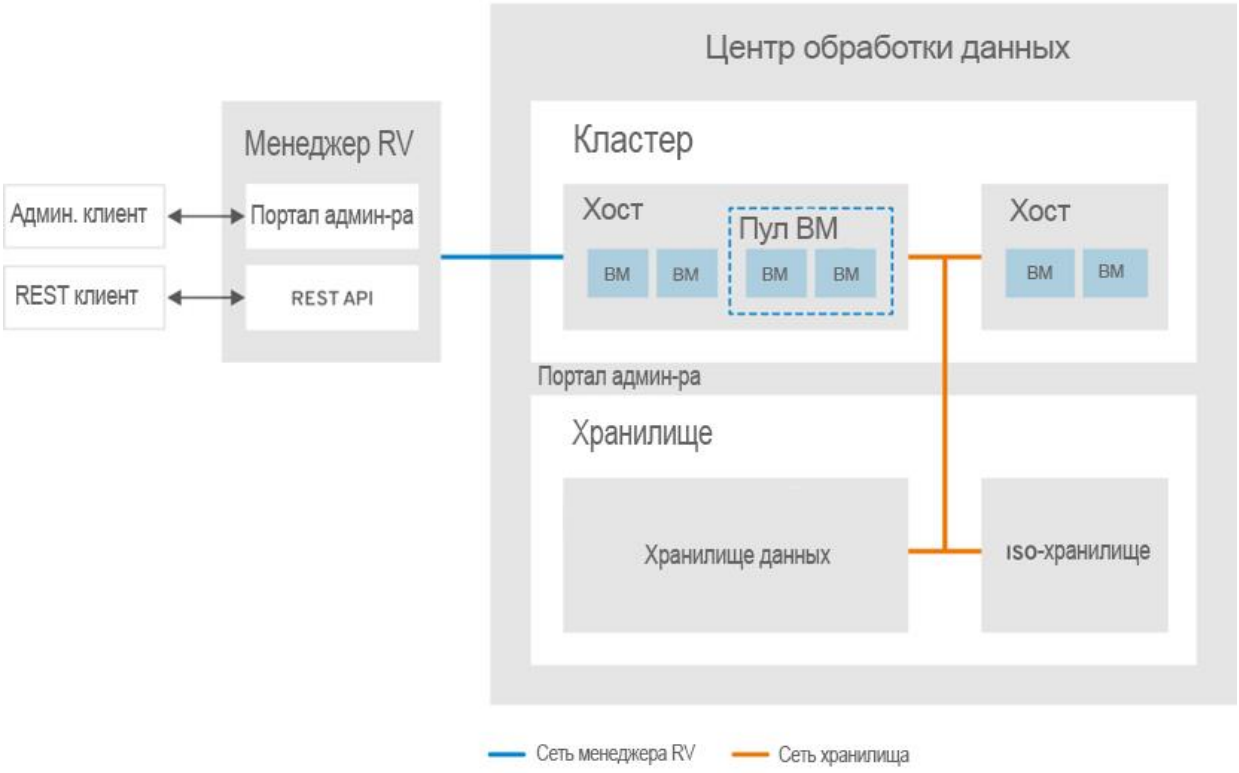

Рис. 25. Дата-центры

В процессе установки система виртуализации ROSA Virtualization создаёт дата-центр по умолчанию. После установки ROSA Virtualization можно настроить дата-центр по умолчанию или создать новые дата-центры.

7.2. Диспетчер пула хранилища (SPM)

Диспетчер пула хранилища (Storage Pool Manager, SPM) — это роль с возможностью управления доменами хранилищ в дата-центре, выделяемая СУСВ (виртуализированным ЦУ) одному из хостов дата-центра.

Объект SPM может работать на любом хосте дата-центра. Роль SPM не исключает выполнения хостом стандартных операций, то есть на хосте, выполняющем роль диспетчера пула хранилища, по-прежнему могут располагаться виртуальные ресурсы.

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

СУСВ (виртуализированный ЦУ) обеспечивает постоянную доступность диспетчера пула хранилища. В случае, если у хоста SPM возникнут проблемы с доступом к хранилищу, виртуализированный ЦУ передаёт роль SPM другому хосту. При запуске диспетчера пула хранилища виртуализированный ЦУ гарантирует, что этот хост будет единственным, выполняющим эту роль.

7.3. Приоритет диспетчера пула хранилища

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

Приоритет SPM для хоста можно изменить на вкладке **SPM** в окне **Параметры хоста** (Рис. 26).

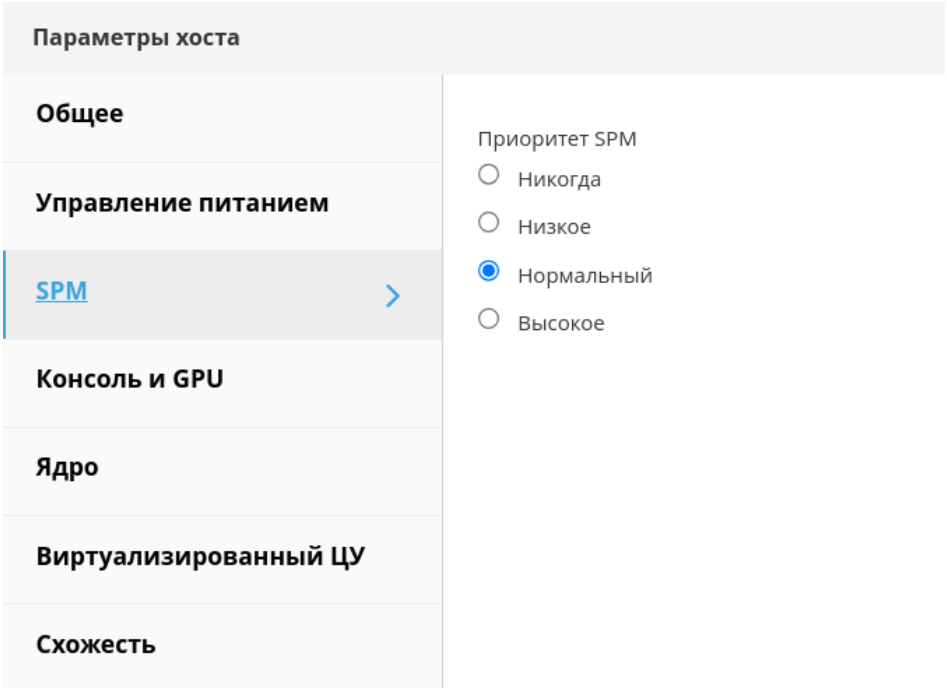

Рис. 26. Параметры хоста

7.4. Задачи при работе с дата-центрами

7.4.1. Создание нового дата-центра

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

Создание нового дата-центра

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите **Добавить**.
3. В окне **Новый дата-центр** (Рис. 27) укажите **Имя** и **Описание** дата-центра.
4. В выпадающих меню выберите **Тип хранилища**, **Версию совместимости** и **Режим квоты** дата-центра.
5. Для создания дата-центра нажмите **OK** и перейдите в окно **Дата-центр — пошаговый помощник**.
6. В окне пошагового помощника присутствует список объектов дата-центра, которые необходимо настроить. Настройте их или отложите настройку, нажав на кнопку **Настроить позже**. Возобновить процесс настройки можно, выбрав дата-центр и перейдя по пунктам меню **Больше действий (⋮) → Пошаговый помощник**.

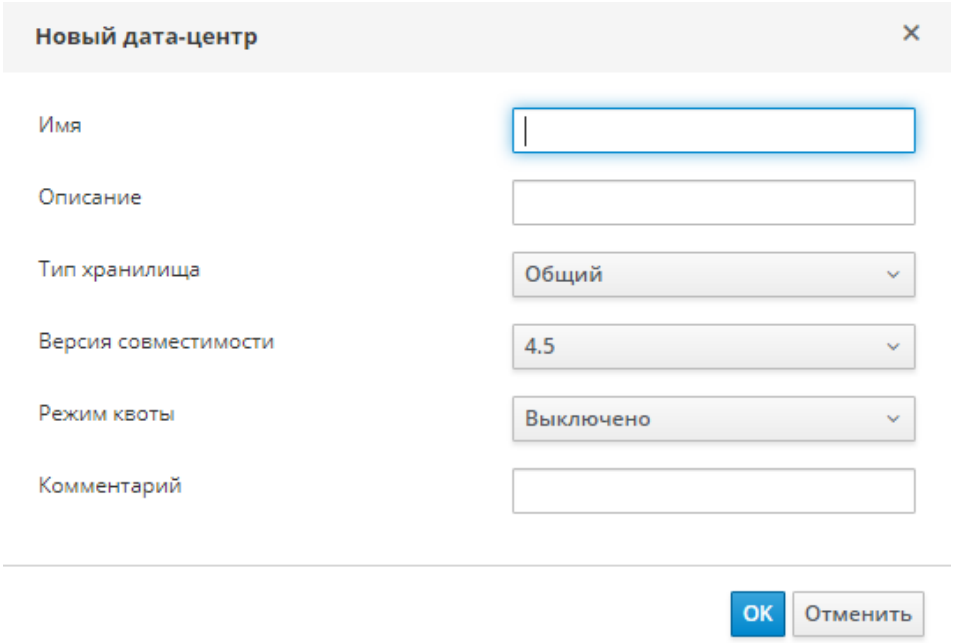

Рис. 27. Создание нового дата-центра

Примечание — *версию совместимости* нельзя будет понизить после указания (регрессия версий не разрешается).

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

Примечание — возможность указать диапазон адресов MAC для дата-центра выполняется на уровне кластера.

7.4.2. Параметры в окнах «Новый дата-центр» и «Параметры дата-центра»

В **Табл. 7.1** описываются параметры дата-центра, присутствующие в окнах **«Новый дата-центр»** и **«Параметры дата-центра»**.

Примечание — при нажатии **OK** недействительные элементы обводятся оранжевым, запрещая применение изменений. Кроме того, в полях ввода указываются ожидаемые значения или диапазон значений.

Табл. 7.1. Параметры дата-центра

Поле	Описание / действие
Имя	Название дата-центра. У этого текстового поля имеется ограничение в 40 символов, а введённое название должно быть уникальным сочетанием любых строчных или прописных букв, цифр, дефисов и знаков подчёркивания
Описание	Описание дата-центра. Заполнение этого поля рекомендуется, но не обязательно
Тип хранилища	Выберите тип хранилища: **Общий** (разделяемый) или **Локальное**. В один и тот же дата-центр можно добавить различные типы доменов хранилищ (iSCSI, NFS, FC, POSIX, Gluster). Тем не менее, локальные и разделяемые домены нельзя смешивать. Изменить тип хранилища можно после инициализации дата-центра
Версия совместимости	Версия системы виртуализации ROSA Virtualization. После обновления виртуализированного ЦУ до новой версии, хосты, кластеры и дата-центры по-прежнему могут иметь более раннюю версию. Перед обновлением до новой версии **Уровня совместимости** дата-центра убедитесь в том, что были обновлены версии всех хостов, а затем кластеров
Режим квоты	Режим квоты — это инструмент ограничения использования ресурсов в составе системы виртуализации ROSA Virtualization. Выберите одно из следующих значений: • **Выключено**: выберите, если не нужно использовать квоты. • **Аудит**: выберите, если нужно изменить параметры квоты. • **Принудительно**: выберите для применения квоты.
Комментарий	По желанию добавьте комментарий о дата-центре в простом текстовом формате

7.4.3. Повторная инициализация дата-центра (процедура восстановления)

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

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

Повторная инициализация дата-центра

1. Нажмите **Ресурсы → Дата-центры** и выберите нужный дата-центр (Рис. 28).
2. Убедитесь в том, что любые домены хранилищ, присоединённые к дата-центру, находятся в режиме обслуживания.
3. Нажмите значок **Больше действий** (⋮), затем пункт **Повторно инициализировать дата-центр**.
4. В окне **Повторная инициализация дата-центра** располагается список всех доступных (отсоединённых, в режиме обслуживания) доменов хранилищ. Установите флажок для домена хранилища, добавляемого в дата-центр.
5. Установите флажок **Подтвердить операцию**.
6. Нажмите **OK**.

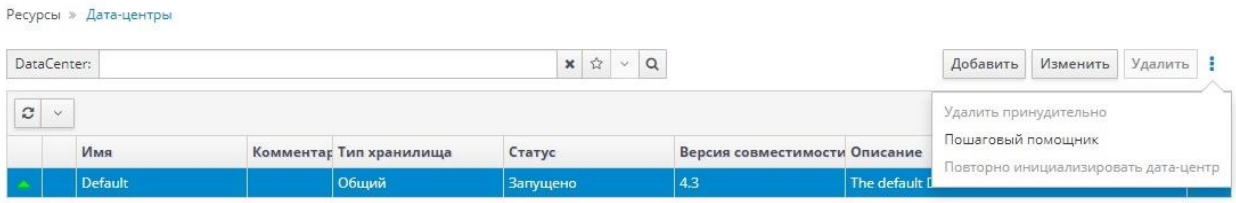

Рис. 28. Повторная инициализация дата-центра

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

7.4.4. Удаление дата-центра

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

Удаление дата-центра

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

7.4.5. Принудительное удаление дата-центра

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

Принудительное удаление не требует активного хоста и навсегда удаляет присоединённый домен хранилища.

Примечание — перед принудительным удалением дата-центра может понадобиться удалить повреждённый домен хранилища.

Принудительное удаление дата-центра

1. Нажмите **Ресурсы** → **Дата-центры** и выберите дата-центр, который нужно удалить.
2. Нажмите на значок **Больше действий** (⋮) и далее **Принудительно удалить**.
3. Установите флажок **Одобрить операцию**.
4. Нажмите **OK**.

В результате дата-центр и присоединённый домен хранилища навсегда будут удалены из окружения виртуализации ROSA Virtualization.

7.4.6. Изменение типа хранилища дата-центра

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

Изменение типа хранилища имеет следующие ограничения**:**

- Общий (разделяемый) на локальное — для дата-центра, который содержит не более одного хоста и одного кластера, поскольку локальный дата-центр это не поддерживает.
- Локальное на общий (разделяемый) — для дата-центра, который не содержит домена локального хранилища.

Изменение типа хранилища дата-центра

1. Нажмите **Ресурсы** → **Дата-центры** и выберите дата-центр, который нужно изменить.
2. Нажмите **Изменить**.

3. Измените **Тип хранилища**.
4. Нажмите **OK**.

7.4.7. Изменение версии совместимости дата-центра

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

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

Изменение версии совместимости дата-центра

1. Нажмите **Ресурсы → Дата-центры** и выберите дата-центр, который нужно изменить.
2. Нажмите **Изменить**.
3. Укажите необходимую **Версию совместимости**.
4. Нажмите **OK**.

7.5. Дата-центры и домены хранилищ

7.5.1. Добавление существующего домена данных к дата-центру

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

Добавление существующего домена данных к дата-центру

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра, чтобы открыть подробные сведения.
3. Перейдите на вкладку **Хранилище** (Рис. 29), чтобы просмотреть список доменов, уже присоединённых к дата-центру.
4. Нажмите **Присоединить данные**.
5. Установите флажок напротив домена данных, который нужно присоединить к дата-центру (при необходимости выберите несколько доменов данных).
6. Нажмите **OK**.

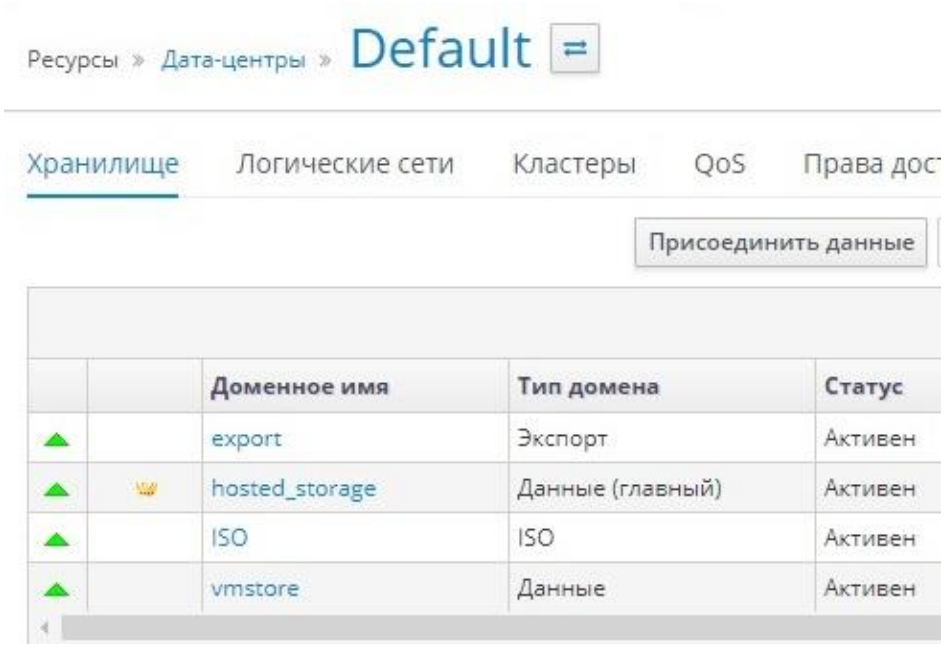

Рис. 29. Добавление существующего домена данных к дата-центру

В результате домен данных будет присоединён к дата-центру и автоматически активирован.

7.5.2. Добавление существующего домена ISO к дата-центру

Домены ISO со статусом **Не присоединён** можно присоединять к дата-центру. При этом к дата-центру можно присоединить только один домен ISO. Домен ISO должен иметь тот же тип хранилища, что и дата-центр.

Добавление существующего домена ISO к дата-центру

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

В результате домен ISO будет присоединён к дата-центру и автоматически активирован.

7.5.3. Присоединение существующего домена экспорта к дата-центру

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

Примечание — домены экспорта являются устаревшими. Домены хранилищ данных можно отсоединять от дата-центра и импортировать в другой дата-центр в том же или в другом окружении. После этого виртуальные машины, плавающие виртуальные диски и шаблоны можно загрузить из импортированного домена хранилища в присоединённый дата-центр. Сведения об импорте доменов хранилищ смотрите в п. 11.7.2. Импорт доменов хранилищ.

Присоединение существующего домена экспорта к дата-центру

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

В результате домен экспорта будет присоединён к дата-центру и автоматически активирован.

7.5.4. Отсоединение доменов хранилищ от дата-центра

Отсоединение домена хранилища от дата-центра отменяет привязку дата-центра к этому домену. Домен хранилища не удаляется из окружения виртуализации ROSA Virtualization и его при необходимости можно будет присоединить к другому дата-центру.

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

Примечание — главное хранилище удалить нельзя, если это единственный доступный домен хранилища.

Отсоединение домена хранилища от дата-центра

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

Примечание — прежде чем домен хранилища исчезнет из отображения подробных сведений, может пройти несколько минут.

Глава 8. Кластеры

8.1. Введение в понятие кластеров

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

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

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

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

В процессе установки система виртуализации ROSA Virtualization создаёт кластер по умолчанию в дата-центре по умолчанию.

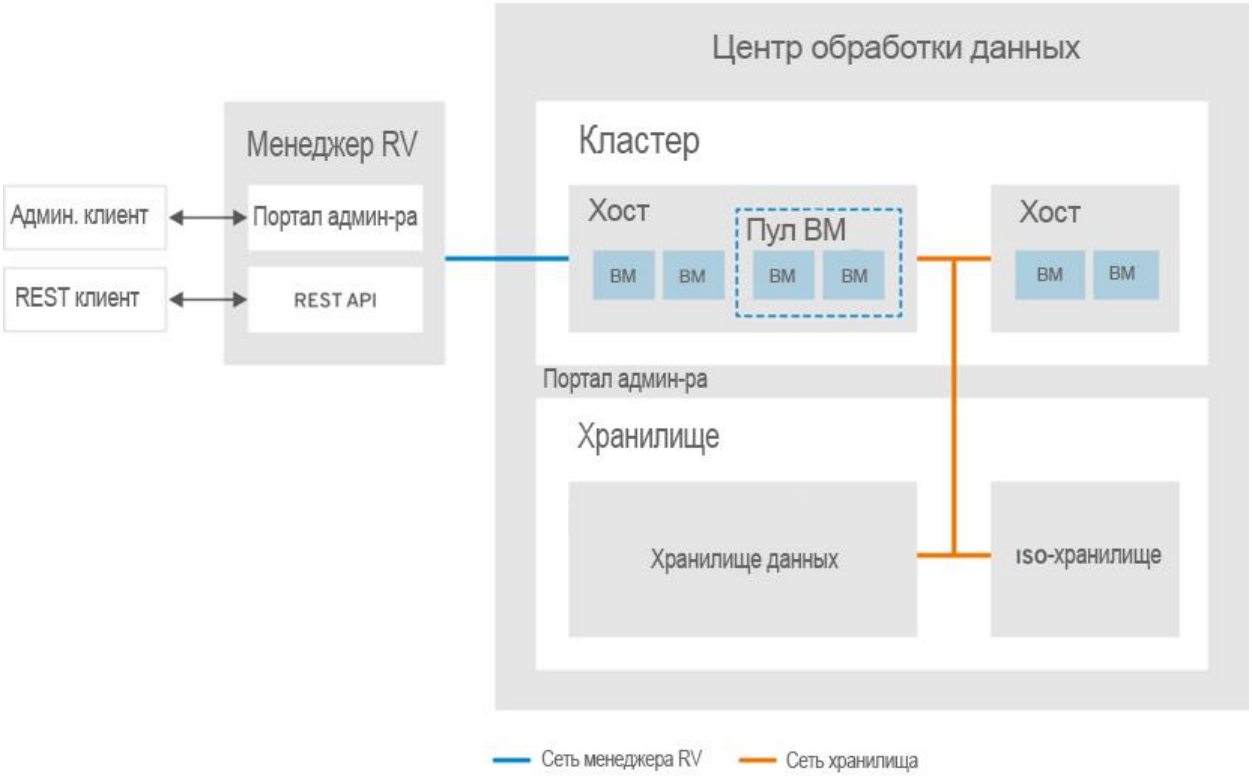

Рис. 30. Кластер

8.2. Задачи при работе с кластерами

Примечание — некоторые параметры кластера не применимы к кластерам Gluster.

8.2.1. Создание нового кластера

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

Создание нового кластера

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

Примечание — как для типа Intel®, так и для типа AMD, указанные в списке модели идут в логическом порядке от самых старых к самым новым. Если в кластер включены хосты с разными моделями ЦП, выбирайте в списке самую старую модель.

7. В выпадающем списке выберите **Версию совместимости** кластера.
8. В выпадающем списке выберите **Тип коммутатора**.
9. Для хостов в кластере выберите **Тип брандмауэра** — ***iptables*** или ***firewalld***.

Примечание — ***iptables*** является устаревшим типом межсетевого экрана.

10. Установите переключатель в положение **Включить службу Virt** или **Включить службу Gluster**, чтобы определить назначение кластера (соответственно кластер будет содержать или виртуальные машины, или узлы с поддержкой Gluster).
11. При необходимости установите флажок **Источник /dev/hwrng** (внешнее аппаратное устройство), чтобы указать устройство для создания случайных чисел, которое будут использовать все хосты в кластере. **Источник /dev/urandom** (устройство Linux) отмечено по умолчанию.
12. Перейдите на вкладку **Оптимизация** для выбора порога разделяемых страниц памяти в кластере, а также при необходимости, включите обработку потоков ЦП и вытеснение памяти на хостах в кластере.
13. Перейдите на вкладку **Политика миграции** для настройки политики миграции ВМ в кластере.
14. Перейдите на вкладку **Политика планирования**, чтобы при необходимости, настроить политику планирования, указать параметры оптимизации планировщика, включить доверенную службу для хостов в кластере, включить резервирование высокой доступности и добавить частную политику порядковых номеров.

15. Перейдите на вкладку **Консоль**, чтобы при необходимости, переопределить глобальные параметры прокси SPICE для хостов в кластере.
16. Перейдите на вкладку **Политика операций блокады**, чтобы включить или отключить возможность проведения операций блокады в кластере и выбрать параметры блокады.
17. Нажмите **Пул MAC адресов**, чтобы указать пул, отличный от пула адресов MAC по умолчанию. Подробности о создании, редактировании или удалении пулов адресов MAC смотрите в п. 1.5. Пулы адресов MAC.
18. Нажмите **OK**, чтобы создать кластер и запустить окно **Кластер — пошаговый помощник**.
19. В окне **Пошаговый помощник** указан список объектов, для которых необходимо настроить взаимодействие с кластером. Настройте эти объекты или отложите настройку, нажав на кнопку **Настроить позже**. Процесс настройки можно возобновить позднее, для чего выберите необходимый кластер, затем нажмите на значок **Больше действий** (⋮), после чего выберите **Пошаговый помощник**.

8.2.2. Общие параметры кластера

В **Табл. 8.1** описываются параметры вкладки **Общее** в окнах **Новый кластер** и **Параметры кластера**.

Примечание — при нажатии **OK** недействительные элементы обводятся оранжевым, запрещая применение изменений. Кроме того, в полях ввода указываются ожидаемые значения или диапазон значений.

Табл. 8.1. Общие параметры кластера

Поле	Описание / действие
Дата-центр	Дата-центр, в котором будет располагаться кластер. Дата-центр должен быть создан до создания кластера
Имя	Название кластера. У этого текстового поля имеется ограничение в 40 символов, а введённое название должно быть уникальным сочетанием любых строчных или прописных букв, цифр, дефисов и знаков подчёркивания
Описание / комментарий	Описание кластера или дополнительные заметки. Заполнение этих полей рекомендуется, но не обязательно
Сеть управления	Логическая сеть, которой будет присвоена роль сети управления. Значение по умолчанию — **ovirtmgmt**. Эта сеть также будет использоваться для миграции ВМ, если сеть миграции не присоединена корректным образом к хостам-источникам или целевым хостам. Изменить сеть управления в существующих кластерах можно, только нажав на кнопку **Управление сетями** на вкладке **Логическая сеть** в детальном просмотре
Архитектура ЦП	Архитектура ЦП в кластере. Типы ЦП показываются в зависимости от выбранной архитектуры: • **Не определено**: доступны все типы ЦП. • **x86_64**: доступны все типы ЦП Intel® и AMD. • **ppc64**: доступен только IBM POWER 8.

Тип ЦП	Тип ЦП в кластере. Список поддерживаемых моделей ЦП:
	• **AMD**
	  ○ Opteron G4
	  ○ Opteron G5
	  ○ EPYC
	• **Intel®**
	  ○ Nehalem

Поле	Описание / действие
	○ Westmere ○ Sandybridge ○ Haswell ○ Haswell-noTSX ○ Broadwell ○ Broadwell-noTSX ○ Skylake (client) ○ Skylake (server) • **IBM POWER 8** Все хосты в кластере должны иметь одинаковый тип ЦП — Intel®, AMD или IBM POWER 8. После создания кластера тип ЦП нельзя изменить без значительных повреждений кластера. Тип ЦП должен быть настроен согласно самой старой модели ЦП в кластере. При этом будут использоваться только возможности, присутствующие во всех моделях. Как для типов ЦП Intel®, так и для типов ЦП AMD модели указываются в логическом порядке от самых старых к самым новым
Версия совместимости	Версия системы виртуализации ROSA Virtualization. Нельзя выбрать версию, более раннюю, чем версия, указанная для дата-центра
Тип коммутатора	Тип коммутатора, используемый в кластере. Стандартным виртуальным коммутатором в системе виртуализации ROSA Virtualization является **Linux Bridge** (OVS предлагает поддержку для сетевых возможностей Open vSwitch)
Тип межсетевого экрана	Указывает тип межсетевого экрана для хостов в кластере — **iptables** или **firewalld**. *ВНИМАНИЕ:* **iptables** является устаревшим типом межсетевого экрана. После смены типа межсетевого экрана в существующем кластере, для применения изменений необходимо переустановить все хосты в кластере
Поставщик сети по умолчанию	Указывает поставщика внешней сети по умолчанию, который будет использоваться в кластере. При выборе Open Virtual Network (OVN) на хостах, добавленных в кластер, автоматически настраивается обмен данными с поставщиком OVN. При смене поставщика сети по умолчанию, для применения изменений необходимо переустановить все хосты в кластере
Максимальный порог журналирования потребления памяти	Указывает порог журналирования для максимального потребления памяти в процентном или абсолютном значении в Мбайт. Сообщение записывается в журнал, если потребление памяти на хосте превышает процентное значение, или если объём доступной на хосте памяти падает ниже абсолютного значения в Мбайт. Значение по умолчанию — `95%`
Включить службу Virt	Если этот переключатель активирован, то хосты в данном кластере будут использоваться для работы виртуальных машин
Включить службу Gluster	Если этот переключатель активирован, то хосты в данном кластере будут использоваться в качестве узлов сервера хранилища Gluster, а не для работы виртуальных машин
Импортировать существующую конфигурацию Gluster	Этот флажок появляется только при активации переключателя **Включить службу Gluster**. Данный параметр позволяет импортировать в СУСВ (виртуализированный ЦУ) уже существующий кластер с поддержкой Gluster и все его присоединённые хосты. Каждый из хостов импортируемого кластера должен соответствовать следующим требованиям: • **Адрес**: укажите IP-адрес или полное доменное имя хоста сервера Gluster. • **Отпечаток**: виртуализированный ЦУ получает отпечаток (fingerprint) хоста для гарантии того, что подключение было выполнено к правильному хосту. • **Пароль root**: укажите пароль root, необходимый для обмена информацией с хостом.

Поле	Описание / действие
Дополнительный источник для генератора случайных чисел	Если этот параметр отмечен флажком, то для всех хостов в кластере станет доступно дополнительное устройство для генерации случайных чисел. Этот параметр включает сквозную энтропию от устройства, создающего случайные числа, к виртуальным машинам

8.2.3. Параметры оптимизации

8.2.3.1. Критерии для памяти

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

8.2.3.2. Критерии для ЦП

Для рабочей нагрузки **без серьёзного потребления ресурсов ЦП** виртуальные машины могут работать, имея общее число ядер процессора, превышающее число ядер на хосте. Таким образом активируются следующие возможности:

- Можно запускать большее число ВМ, что снижает требования к аппаратным составляющим.
- Можно настраивать ВМ с топологией ЦП, которая в противном случае не была бы возможной (например, когда значение количества виртуальных ядер находится между числом ядер хоста и числом потоков хоста).

Для **лучшей производительности** и особенно для **рабочей нагрузки с серьёзным потреблением ресурсов ЦП** необходимо использовать для ВМ ту же топологию, что и на хосте, чтобы и ВМ, и хост рассчитывали на одинаковое использование кэша. При включённой на хосте гиперпоточности, QEMU обрабатывает гиперпотоки хоста как ядра, таким образом ВМ выполняется на одном ядре с несколькими потоками. Такое поведение может повлиять на производительность ВМ, поскольку виртуальное ядро, на самом деле соответствующее гиперпотоку ядра хоста, может разделять один и тот же кэш с другим гиперпотоком на том же ядре хоста, в то время как ВМ считает его отдельным ядром.

В **Табл. 8.2** описываются параметры вкладки **Оптимизация** в окнах **Новый кластер** и **Параметры кластера**.

Табл. 8.2. Параметры оптимизации

Поле	Описание / действие
Оптимизация памяти	Режим оптимизации памяти может принимать следующие значения: • **Отсутствует — отключить превышенное выделение памяти**: отключает общие страницы памяти. • **Для нагрузки сервера — разрешить запланировать 150% физической памяти**: устанавливает порог разделения страниц памяти на 150% от системной памяти на каждом хосте. • **Для нагрузки рабочего стола — разрешить запланировать 200% физической памяти**: устанавливает порог разделения страниц памяти на 200% от системной памяти на каждом хосте.
Симметричная многопоточность	Установка флажка **Симметричная многопоточность отключена** отключает гиперпоточность
Потоки ЦП	Установка флажка **Считать потоки как ядра** даёт хостам возможность запускать ВМ с общим числом ядер процессора, превышающим число ядер на хосте.

Поле	Описание / действие
	Если этот параметр отмечен, то предоставляемые потоки хоста считаются ядрами, которые может использовать ВМ. Например, в системе с 24 ядрами и 2 потоками на ядро (всего 48 потоков) могут выполняться ВМ с числом ядер вплоть до 48, а алгоритмы для расчёта загрузки ЦП хоста будут сопоставлять нагрузку с двойным числом потенциально используемых ядер
Вытеснение памяти	Установка флажка **Включить оптимизацию вытеснения памяти** включает превышенное выделение памяти для ВМ, работающих на хостах в этом кластере. Если этот параметр отмечен, то диспетчер превышенного выделения памяти (Memory Overcommit Manager, MoM) начинает вытеснение памяти, где и когда это возможно. Ограничением служит гарантированный размер памяти, установленный для каждой ВМ. Чтобы выполнять вытеснение памяти, виртуальной машине требуется устройство вытеснения памяти с соответствующими драйверами. Каждая ВМ включает в себя такое устройство, если только оно не было удалено специально. При смене статуса на *запущен*, каждый хост в этом кластере получает обновление политики вытеснения памяти. Если нужно, политику вытеснения памяти на хосте можно обновить вручную, без необходимости смены статуса. Очень важно понимать, что в некоторых сценариях вытеснение памяти может конфликтовать с функцией объединения одинаковых страниц памяти ядром (KSM). В таких случаях MoM постарается перенастроить размер вытесняемой памяти для минимизации конфликта. Кроме того, в некоторых сценариях вытеснение памяти может привести к производительности ВМ ниже оптимальной. Администраторам следует прибегать к оптимизации вытеснения памяти с крайней осторожностью
Контроль KSM	Установка флажка **Включить KSM** даёт возможность MoM выполнять объединение одинаковых страниц памяти как при необходимости, так и тогда, когда выгода от экономии памяти перевешивает вычислительные затраты ЦП. Режим контроля KSM может принимать следующие значения: • **Сделать страницы памяти общими для всей доступной памяти**: наилучшая эффективность KSM. • **Сделать страницы памяти общими внутри узлов NUMA**: наилучшая производительность NUMA.

8.2.4. Политики миграции

В **Табл. 8.3** описываются политики миграции, которые определяют условия для динамической миграции ВМ в случае сбоев работы хоста. Эти условия включают в себя простой ВМ во время миграции, пропускную способность сети и то, каким образом выставляются приоритеты виртуальных машин.

Табл. 8.3. Политики миграции

Политика	Описание
Минимальный простой	Политика, разрешающая миграцию ВМ в типичных ситуациях. ВМ не должны испытывать значительный простой. Миграция будет прервана, если после долгого промежутка времени ВМ не достигнет состояния целостности (в зависимости от итераций QEMU, с максимальным интервалов в 500 миллисекунд). Механизм ловушек гостевого агента включён
Миграция пост-копирования	По аналогии с политикой минимального простоя, ВМ не должны испытывать значительный простой. Политика пост-копирования сначала пытается выполнить пред-копирование для проверки возможности конфликтов. Если ВМ не достигает состояния целостности после долгого промежутка времени, то происходит переключение на пост-копирование. Недостаток этой политики в том, что во время фазы пост-копирования по мере перемещения недостающих фрагментов памяти между хостами машина может значительно замедлиться.

Политика	Описание
	Если во время фазы пост-копирования что-то пойдёт не так (например, случится сбой сети между хостами), то тогда процесс миграции приведёт к утрате целостности, приостановке работы ВМ и к дальнейшей потере ВМ. Соответственно, прерывание миграции во время фазы пост-копирования невозможно. Примечание — если сетевое соединение оборвётся до завершения пост-копирования, то виртуализированный ЦУ приостановит и затем завершит основной процесс выполнения ВМ. Не используйте миграцию пост-копирования при критической доступности ВМ или в нестабильной сети миграции
Приостановить рабочую нагрузку при необходимости	Политика, дающая возможность миграции ВМ в большинстве ситуаций, включая серьёзную рабочую нагрузку на ВМ. В связи с этим машины под серьёзной рабочей нагрузкой могут простаивать в течение гораздо более долгого времени, чем с параметрами других политик. При экстремальных рабочих нагрузках миграция всё ещё может быть прервана. Механизм ловушек гостевого агента включён

В **Табл. 8.4** описываются параметры пропускной способности, которые определяют максимальную пропускную способность как входящих, так и исходящих миграций на каждый отдельный хост.

Табл. 8.4. Параметры пропускной способности

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

В **Табл. 8.5** описываются параметры политики устойчивости, которые определяют приоритеты ВМ во время миграции.

Табл. 8.5. Параметры политики устойчивости

Поле	Описание / действие
Переносить виртуальные машины	Все виртуальные машины мигрируют в порядке их настроенного приоритета
Переносить только ВМ с высокой доступностью	Мигрируют только высокодоступные машины для предотвращения перегрузки других хостов
Не переносить ВМ	Запрещает миграцию виртуальных машин

В **Табл. 8.6** описываются дополнительные параметры, которые применяются к ВМ во время миграции.

Табл. 8.6. Дополнительные параметры

Параметр	Описание
Включить шифрование при миграции	Параметр даёт возможность указать, будет ли использоваться шифрование во время динамических миграций ВМ. По умолчанию шифрование во время миграции ВМ отключено на уровне кластера. Параметр может принимать следующие значения: • **Значение по умолчанию**: используется значение **Зашифровать** или **Не шифровать** (по умолчанию), настроенное на уровне кластера. • **Зашифровать**: значение переопределяет настройку на уровне кластера и включает шифрование при миграции ВМ. • **Не шифровать**: значение переопределяет настройку на уровне кластера и отключает шифрование при миграции ВМ.

8.2.5. Политики планирования

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

В **Табл. 8.7** описываются параметры вкладки **Политики планирования**.

Табл. 8.7. Параметры вкладки «Политики планирования»

Поле	Описание / действие
Выберите политику	Выберите необходимую политику планирования из выпадающего списка: • **None (отсутствует)**: режим по умолчанию — без балансировки нагрузки или разделения энергосбережения между хостами уже работающих ВМ. При запуске ВМ нагрузка на память и вычислительные ресурсы ЦП равномерно распределяются между всеми хостами в кластере. Дополнительные ВМ не начнут работу, если нагрузка хоста достигла ранее настроенных значений `CpuOverCommitDurationMinutes`, `HighUtilization` или `MaxFreeMemoryForOverUtilized`. • **evenly_distributed (равномерное распределение)**: равномерно распределяет память и вычислительные ресурсы ЦП между всеми хостами в кластере. Дополнительные ВМ, присоединённые к хосту, не начнут работу, если нагрузка хоста достигла ранее настроенных значений `CpuOverCommitDurationMinutes`, `HighUtilization` или `MaxFreeMemoryForOverUtilized`. • **cluster_maintenance (обслуживание кластера)**: ограничивает активность в кластере во время выполнения задач обслуживания. Нельзя запускать никакие ВМ, включая высокодоступные, но можно выполнять миграцию любых ВМ. В случае сбоя хоста, высокодоступные ВМ будут корректно перезапущены. • **power_saving (энергосбережение)**: распределение памяти и нагрузки на вычислительные мощности ЦП внутри группы доступных хостов для снижения потребления энергии на недозагруженных хостах.

Поле	Описание / действие
	Хосты с нагрузкой на ЦП меньше значения низкого использования в течение большего промежутка времени, чем указанный промежуток, выполнят миграцию всех ВМ на другие хосты с тем, чтобы можно было произвести отключение этого хоста. Дополнительные ВМ, присоединённые к этому хосту, не начнут работу, если хост достиг указанного значения высокой загрузки. • **vm_evenly_distributed (равномерное распределение ВМ)**: ВМ равномерно распределяются между хостами, основываясь на количестве машин. Кластер считается несбалансированным, если на любом из хостов выполняется больше ВМ, чем указано в значении `HighVmCount`, и если существует минимум один хост, число выполняемых ВМ на котором больше, чем указано в значении `MigrationThreshold`.
Параметры	В зависимости от выбранной политики планирования станут доступными следующие параметры: • **HighVmCount**: указывает минимальное число ВМ, выполняемых на хосте и необходимых для включения балансировки нагрузки. Балансировка нагрузки включается только тогда, когда в кластере присутствует хотя бы один хост с числом работающих машин, как минимум равным значению `HighVmCount`. Значение по умолчанию — 10. • **MigrationThreshold**: настраивает буфер до того, как ВМ мигрируют с хоста. Это значение представляет собой максимальную инклюзивную разницу числа ВМ между самым высокозагруженным хостом и самым низкозагруженным хостом. Кластер считается сбалансированным, когда число ВМ на каждом хосте не выходит за значение порога миграции. Значение по умолчанию — 5. • **SpmVmGrace**: определяет число слотов ВМ, зарезервированных на хостах SPM. У хостов SPM более низкая нагрузка, чем у обычных хостов, поэтому этот параметр определяет, насколько меньше ВМ будут выполняться на хосте SPM, по сравнению с другими хостами. Значение по умолчанию — 5. • **CpuOverCommitDurationMinutes**: указывает промежуток времени (в минутах**)**, в течение которого нагрузка на ЦП хоста может превышать настроенные значения до того, как будет применена политика планирования. Указанный временной интервал защищает от активации политик планирования по причине кратковременных пиков нагрузки на ЦП и последующих нежелательных миграций ВМ. Допускается максимум два знака. Значение по умолчанию — 2. • **HighUtilization**: выражается в процентном значении. Если нагрузка на ЦП хоста равна или превышает значение высокой нагрузки в течение указанного промежутка времени, то виртуализированный ЦУ выполняет миграцию ВМ на другие хосты в кластере до тех пор, пока нагрузка на ЦП хоста не будет превышать максимальный порог обслуживания. Значение по умолчанию — 80. • **LowUtilization**: выражается в процентном значении. Если нагрузка на ЦП хоста меньше значения низкой нагрузки в течение указанного промежутка времени, то виртуализированный ЦУ выполняет миграцию ВМ на другие хосты в кластере. Виртуализированный ЦУ выключит машину с исходным хостом, и включит ВМ только тогда, когда это будет необходимо из соображений балансировки нагрузки,

Поле	Описание / действие
	или если в кластере будет недостаточно свободных хостов. Значение по умолчанию — 20. • **ScaleDown**: снижает влияние весовой функции `HA Reservation`, путём деления значения оценки степени высокой готовности хоста на указанное число. Это дополнительный параметр, который можно добавлять к любой политике, включая политику **none**. • **HostsInReserve**: указывает число хостов, которые всегда должны работать, даже если на них отсутствуют ВМ. Это дополнительный параметр, который можно добавить к политике **power_saving**. • **EnableAutomaticHostPowerManagement**: включает автоматическое управление энергосбережением на всех хостах кластера. Это дополнительный параметр, который можно добавить к политике **power_saving**. Значение по умолчанию — верно (true). • **MaxFreeMemoryForOverUtilized**: указывает минимальный размер свободной памяти (в Мбайт), требуемый для минимального уровня обслуживания. Если объём доступной памяти хоста будет равен или меньше этого значения, то виртуализированный ЦУ будет выполнять миграцию ВМ на другие хосты этого кластера в течение всего времени, пока объём доступной памяти хоста будет находиться меньше значения порога минимального уровня обслуживания. Это дополнительный параметр, который можно указать для политик **power_saving** и **evenly_distributed.** Значение 0 для параметров `MaxFreeMemoryForOverUtilized` и `MinFreeMemoryForUnderUtilized` отключает балансировку памяти. Для избежания непредсказуемого поведения, при указании значения для параметра `MaxFreeMemoryForOverUtilized` необходимо также указывать значение и для параметра `MinFreeMemoryForUnderUtilized`. • **MinFreeMemoryForUnderUtilized**: указывает минимальный размер свободной памяти (в Мбайт), требуемый для того, чтобы хост считался низкозагруженным. Если объём доступной памяти хоста будет иметь значение меньше указанного в этом параметре, то виртуализированный ЦУ выполнит миграцию ВМ на другие хосты в кластере и автоматически отключит машину хоста. Машина будет включена снова по соображениям балансировки нагрузки, или если в кластере будет недостаточно свободных хостов. Это дополнительный параметр, который можно указать для политик **power_saving** и **evenly_distributed.** Значение 0 для параметров `MaxFreeMemoryForOverUtilized` и `MinFreeMemoryForUnderUtilized` отключает балансировку памяти. Для избежания непредсказуемого поведения, при указании значения для параметра `MaxFreeMemoryForOverUtilized` необходимо также указывать значение и для параметра `MinFreeMemoryForUnderUtilized`. • **HeSparesCount**: указывает число дополнительных узлов виртуализированного ЦУ, на которых должна быть зарезервирована память в объёме, достаточном для запуска виртуальной машины виртуализированного ЦУ на случай миграции этой ВМ или отключения. Если запуск других машин на узле виртуализированного ЦУ не оставит достаточного объёма свободной памяти для ВМ виртуализированного ЦУ, то эти машины не начнут работу. Это дополнительный параметр, который можно добавить к политикам

Поле	Описание / действие
	power_saving, **vm_evenly_distributed** и **evenly_distributed**. Значение по умочанию — 0.
Оптимизация планировщика	Оптимизация планировщика для определения весового коэффициента/ распределения хостов: • **Оптимизировать на использование**: в планирование включаются весовые модули для наилучшего выбора. • **Оптимизировать на скорость**: определение весового коэффициента хоста пропускается в тех случаях, когда в очереди находится больше десяти запросов.
Включить доверенную службу	Включить интеграцию с сервером OpenAttestation. Чтобы включить возможность этого параметра, используйте утилиту `engine-config` для указания сведений о сервере OpenAttestation
Включить резервирование высокой доступности	Разрешить виртуализированному ЦУ выполнять наблюдения за доступными мощностями кластера для отказоустойчивых ВМ. Виртуализированный ЦУ обеспечивает наличие в кластере необходимых ресурсов для миграции высокодоступных ВМ в случае внезапного отказа их текущего хоста
Политика серийных номеров	Параметр даёт возможность задать политику серийных номеров для ВМ в кластере. Выберите одну из следующих возможностей: • **Значение по умолчанию**: используется значение (**ID хоста** (по умолчанию)), настроенное на уровне кластера. • **ID хоста**: в качестве серийного номера ВМ указывается UUID хоста. • **ID машины**: в качестве серийного номера ВМ указывается UUID ВМ. • **Настраиваемый пользователем серийный номер**: даёт возможность пользователю указать произвольный порядковый номер в качестве серийного номера ВМ.

Если объём свободной памяти хоста падает меньше значения 20%, то такие команды вытеснения памяти как `mom.Controllers.Balloon — INFO Ballooning guest:half1 from 1096400 to 1991580` записываются в файл журнала диспетчера MoM */var/log/vdsm/mom.log*.

8.2.6. Параметры консоли кластера

В **Табл. 8.8** описываются параметры вкладки **Консоль** в окнах **Новый кластер** и **Параметры кластера**.

Табл. 8.8. Параметры консоли

Поле	Описание / действие
Переназначенный адрес прокси SPICE	Прокси, с помощью которого клиент SPICE подключается к виртуальным машинам. Адрес должен указываться в следующем формате: `протокол://[хост]:[порт]`
Включить шифрование VNC	Установите этот флажок, чтобы включить TLS по протоколу X509Vnc

8.2.7. Параметры политики операций блокады

В **Табл. 8.9** описываются параметры вкладки **Политика операций блокады** в окнах **Новый кластер** и **Параметры кластера**.

Табл. 8.9. Параметры политики операций блокады

Поле	Описание / действие
Включить возможность операций блокады	Разрешает проведений операций блокады в кластере. По умолчанию эта возможность присутствует, но при необходимости её можно отключить

Поле	Описание / действие
	(например, если возникают или ожидаются временные проблемы с сетью, то администратор может отключить возможность проведения операций блокады до завершения действий по диагностике или обслуживанию). Обратите внимание, что при отключённой возможности проведения операций блокады, высокодоступные ВМ, выполняемые на не отвечающих хостах, не будут перезапущены в другом месте
Пропустить операцию блокады, если у хоста имеется динамическая аренда в хранилище	Если этот флажок установлен, то операции блокады не будут выполняться на любых хостах со статусом *не отвечает*, по-прежнему подключённых к хранилищу
Пропустить операцию блокады, если у кластера есть проблемы с соединением	Если этот флажок установлен и процентное значение хостов в кластере, испытывающих проблемы с соединением, равно или больше указанного значения **Порога**, то операции блокады временно не будут выполняться. Значение **Порога** выбирается из выпадающего списка и имеет следующие доступные значения: 25, 50, 75 и 100
Пропустить операцию блокады, если имеются работающие элементы (кирпичи) Gluster	Параметр доступен только при включённых возможностях хранилища Gluster. При выбранном параметре операция блокады будет пропускаться, если присутствуют работающие элементы (кирпичи), к которым есть доступ с других одноранговых узлов
Пропустить операцию блокады, если не выполнены требования кворума Gluster	Параметр доступен только при включённых возможностях хранилища Gluster. При выбранном параметре операция блокады будет пропускаться при работающих элементах (кирпичах), а выключение хоста приведёт к потере кворума

8.2.8. Настройка политик управления нагрузкой и энергосбережения на хосте

Политики планирования **evenly_distributed** (равномерное распределение) и **power_saving** (энергосбережение) дают возможность указать приемлемые значения потребления ресурсов памяти и ЦП, а также порог значений, после превышения которого виртуальные машины должны мигрировать с хоста или на хост. Политика планирования **vm_evenly_distributed** (равномерное распределение ВМ) равномерно распределяет ВМ между хостами, руководствуясь количеством машин. Для включения автоматической балансировки нагрузки хостов в кластере настройте политику планирования (см. п. 1.3. Политики планирования).

Настройка политик управления нагрузкой и энергосбережения на хосте

1. Нажмите **Ресурсы → Кластеры и выберите кластер**.
2. Нажмите **Изменить**.
3. Перейдите на вкладку **Политика планирования** (Рис. 31).

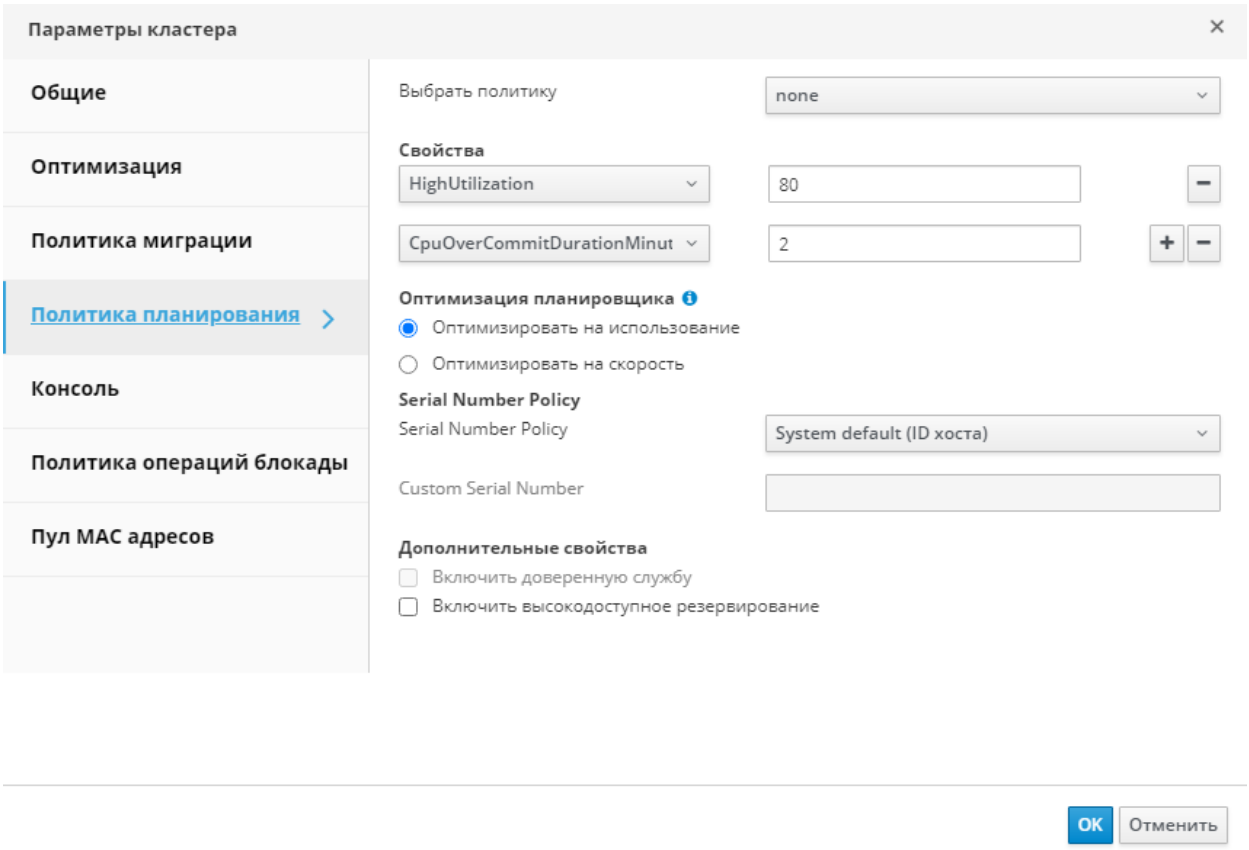

Рис. 31. Политика планирования

4. Выберите одну из следующих политик:
   - **нет**
   - **vm_evenly_distributed**
     a. В поле **HighVmCount** укажите минимальное число ВМ, выполняющихся на одном хосте и необходимых для включения балансировки нагрузки.
     b. В поле **MigrationThreshold** укажите максимальную приемлемую разницу между числом ВМ на самом загруженном хосте и числом ВМ на самом незагруженном хосте.
     c. В поле **SpmVmGrace** укажите число слотов для ВМ, которое должно быть зарезервировано на хостах SPM.
     d. При необходимости в поле **HeSparesCount** укажите число дополнительных узлов виртуализированного ЦУ, на которых нужно зарезервировать объём свободной памяти, достаточный для запуска ВМ виртуализированного ЦУ в случае миграции этой ВМ или выключения.
   - **evenly_distributed**
     a. В поле **CpuOverCommitDurationMinutes** укажите время (в минутах), в течение которого нагрузка на ЦП хоста может превышать настроенные значения нагрузки перед тем, как будет применена политика планирования.
     b. В поле **HighUtilization** укажите процентное значение нагрузки на ЦП, при котором ВМ будут начинать миграцию на другие хосты.
     c. В поле **MinFreeMemoryForUnderUtilized** укажите минимальный объём свободной памяти в Мбайт, при превышении которого ВМ начнут мигрировать на другие хосты.

d. В поле **MaxFreeMemoryForOverUtilized** укажите максимальный требуемый объём свободной памяти, при значении меньше которого ВМ начнут миграцию на другие хосты.
e. При необходимости в поле **HeSparesCount** укажите число дополнительных узлов виртуализированного ЦУ, на которых нужно зарезервировать объём свободной памяти, достаточный для запуска ВМ виртуализированного ЦУ в случае миграции этой ВМ или выключения.

- **power_saving**
  a. В поле **CpuOverCommitDurationMinutes** укажите время (в минутах), в течение которого нагрузка на ЦП хоста может превышать настроенные значения нагрузки перед тем, как будет применена политика планирования.
  b. В поле **LowUtilization** укажите процент загруженности ЦП, при значении меньше которого хост будет считаться недозагруженным.
  c. В поле **HighUtilization** укажите процентное значение нагрузки на ЦП, при достижении которого ВМ начнут миграцию на другие хосты.
  d. В поле **MinFreeMemoryForUnderUtilized** укажите минимальный объём свободной памяти в Мбайт, при превышении которого ВМ начнут миграцию на другие хосты.
  e. В поле **MaxFreeMemoryForOverUtilized** укажите максимальный требуемый объём свободной памяти, при значении меньше которого ВМ начнут миграцию на другие хосты.
  f. При необходимости в поле **HeSparesCount** укажите число дополнительных узлов виртуализированного ЦУ, на которых нужно зарезервировать объём свободной памяти, достаточный для запуска ВМ виртуализированного ЦУ в случае миграции этой ВМ или выключения.

5. Выберите одно из следующих значений **Оптимизации планировщика** кластера:
   - **Оптимизировать на использование** — включение в планирование весовых модулей для лучшего выбора.
   - **Оптимизировать на скорость** — пропуск измерения веса хоста в тех случаях, когда в очереди находится более 10 запросов.
6. Если для верификации хостов используется сервер OpenAttestation и его конфигурация была настроена с помощью утилиты `engine-config`, то установите флажок **Включить доверенную службу**.
7. При необходимости установите флажок **Включить высокодоступное резервирование**, чтобы виртуализированный ЦУ мог обеспечивать доступность ресурсов в кластере для отказоустойчивых ВМ.
8. При необходимости выберите одно из следующих значений **Политики серийных номеров** для ВМ в кластере:
   - **ID хоста** — в качестве серийного номера ВМ указывается UUID хоста.
   - **ID машины** — в качестве серийного номера ВМ указывается UUID ВМ.
   - **Настраиваемый пользователем серийный номер** — при выборе этого значения дополнительно укажите произвольный порядковый номер (в качестве серийного номера ВМ) в текстовом поле интерфейса.
9. Нажмите **OK**.

8.2.9. Обновление информации о политике MoM на хостах в кластере

Диспетчер превышенного выделения памяти MoM хоста отвечает за обработку возможностей вытеснения памяти и объединения одинаковых страниц памяти ядром (KSM).

Изменения параметров этих функций на уровне кластера передаются хостам только после того, как хост вновь получит статус «*Запущен*» после перезагрузки или после снятия режима обслуживания. Тем не менее, при необходимости, применить важные изменения можно немедленно, выполнив синхронизацию политики превышенного выделения памяти для хостов, ещё имеющих статус «*Запущен*».

Следующая последовательность действий должна выполняться на каждом из хостов индивидуально.

Синхронизация политики превышенного выделения памяти на хосте

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

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

8.2.10. Создание профиля ЦП

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

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

Создание профиля ЦП

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

8.2.11. Удаление профиля ЦП

Удаление профиля ЦП

1. Нажмите **Ресурсы → Кластеры**.
2. Нажмите на название кластера, чтобы открыть подробный просмотр.

3. Перейдите на вкладку **Профили ЦП** и выберите удаляемый профиль ЦП.
4. Нажмите **Удалить**.
5. Нажмите **OK**.

Если этот удаленный профиль был ранее присвоен каким-либо ВМ, то этим ВМ автоматически будет присвоен профиль ЦП `по умолчанию`.

8.2.12. Импортирование существующего кластера хранилища Gluster

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

При указании таких параметров любого хоста в кластере, как IP-адрес или имя и пароль хоста, на этом хосте с помощью протокола SSH выполняется команда `gluster peer status`, а затем выводится список хостов, принадлежащих кластеру. Необходимо вручную заверить отпечаток для каждого хоста и указать пароль хоста.

Если один из хостов в кластере не запущен или недоступен, то выполнить импортирование кластера будет невозможно.

Импортирование существующего хранилища Gluster в виртуализированный ЦУ

1. Нажмите **Ресурсы → Кластеры**.
2. Нажмите **Добавить**.
3. Выберите **Дата-центр**, к которому будет принадлежать кластер.
4. Укажите **Имя** и **Описание** кластера.
5. Установите флажки **Включить службу Gluster** и **Импорт существующей конфигурации Gluster** (при этом поле **Импорт существующей конфигурации Gluster** будет показано только при ранее выбранном параметре **Включить службу Gluster)**.
6. В поле **Имя хоста** укажите имя хоста или IP-адрес любого сервера в кластере. Будет показан **Отпечаток SSH** для подтверждения того, что выполняется подключение к нужному хосту. Если хост недоступен или появилась ошибка сети, то в поле **Отпечаток** будет выведена **Ошибка получения отпечатка**.
7. Укажите **Пароль** (пароль сервера) и нажмите **OK**.
8. Будет показано окно **Добавить хосты** и список хостов в составе кластера.
9. Для каждого хоста укажите **Имя** и **Пароль root**.
10. В случае использования одного и того же пароля для всех хостов установите флажок **Использовать общий пароль** и укажите этот пароль в текстовом поле.
11. Нажмите **Применить**, чтобы установить введённый пароль для всех хостов.
12. Проверьте подлинность всех отпечатков и нажмите **OK** для применения изменений.

После импорта хостов сценарий самозагрузки установит на хостах необходимые пакеты VDSM и автоматически перезагрузит хосты.

8.2.13. Параметры хранилища Gluster в окне «Добавить хосты»

В окне **Добавить хосты** можно указать подробные сведения о хостах, импортируемых в составе кластера хранилища Gluster. Это окно появляется после того, как в окне **Новый кластер** был установлен флажок **Включить службу Gluster** и указаны все необходимые сведения о хосте.

В **Табл. 8.10** описываются параметры хранилища Gluster в окне **Добавить хосты**.

Табл. 8.10. Параметры Gluster

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

8.2.14. Удаление кластеров

Перед удалением кластера переместите из него все хосты.

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

Удаление кластера

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

8.2.15. Оптимизация памяти

Для увеличения числа виртуальных машин на хосте можно использовать *превышенное выделение памяти*, при котором объём памяти, выделяемый машине, превышает доступный объём ОЗУ за счет использования файла (раздела) подкачки.

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

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

Таким образом для оптимизации памяти рекомендуется выполнить следующие действия:

- Ограничить превышенное выделение памяти с помощью параметра **Оптимизация памяти** и *диспетчера превышенного выделения памяти (MoM).*

- Создать раздел подкачки, достаточно объёмный для того, чтобы потенциально обеспечить максимальный запрос на виртуальную память и одновременно не выходить за пределы безопасности.
- Уменьшить размер виртуальной памяти, включив *вытеснение памяти (ballooning)* и *объединение одинаковых страниц памяти ядром (KSM).*

8.2.15.1. Превышенное выделение памяти

Ограничить объём превышенного выделения памяти можно с помощью одного из процентных значений параметра **Оптимизация памяти** — **Нет** (0%)**, 150%** или **200%**.

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

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

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

Примечание — перед оптимизацией памяти в рабочей среде, всегда сначала проводите стресс-тестирование при самых разных условиях.

Чтобы настроить параметры оптимизации памяти перейдите на вкладку **Оптимизация** в окнах **Новый кластер** или **Параметры кластера** (см. п. 8.2.3. Параметры оптимизации).

Дополнительные примечания:

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

8.2.15.2. Раздел подкачки

В **Табл. 8.11** приведены общие рекомендации по настройке раздела подкачки.

Табл. 8.11. Общие рекомендации по настройке раздела подкачки

Объём ОЗУ	Рекомендуемый размер раздела подкачки	Рекомендуемый размер раздела подкачки (при использовании гибернации)
2 Гбайт или меньше	Двойной объём ОЗУ	Тройной объём ОЗУ
2 Гбайт - 8 Гбайт	Объём, равный объёму ОЗУ	Двойной объём ОЗУ
8 Гбайт - 64 Гбайт	Минимум 4 Гбайт	Полуторный объём ОЗУ
64 Гбайт или больше	Минимум 4 Гбайт	Гибернация не рекомендуется

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

Дополнительные рекомендации по настройке раздела подкачки:

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

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

Примечание — чтобы повысить шансы предотвращения состояния нехватки памяти, создавайте раздел подкачки достаточно большим из расчёта на наихудший возможный сценарий плюс учитывайте резерв для запаса прочности.

8.2.15.3. Диспетчер превышенного выделения памяти MoM

Диспетчер превышенного выделения памяти MoM выполняет следующие основные функции:

- Диспетчер MoM ограничивает превышенное выделение памяти путём применения установленного значения параметра **Оптимизация памяти** к хостам в кластере.
- Диспетчер MoM оптимизирует память, управляя процессами *вытеснения памяти (ballooning)* и *объединения одинаковых страниц памяти ядром (KSM).*

Диспетчер MoM не нуждается во включении или отключении.

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

8.2.15.4. Вытеснение памяти (ballooning)

Виртуальные машины начинают работу, располагая полным объёмом выделенной виртуальной памяти. По мере того, как потребление виртуальной памяти превышает объём ОЗУ, хост всё более и более начинает использовать механизм подкачки. Активированная процедура *вытеснения памяти* заставляет ВМ отдать неиспользуемую часть памяти. Освобождённая память может быть повторно использована другими процессами и другими ВМ на хосте. По причине сокращения объёма используемой памяти сокращается и число обращений к разделу подкачки, а также улучшается производительность.

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

Устройства вытеснения памяти не координируются напрямую друг с другом, а зависят от диспетчера превышенного выделения памяти MoM, постоянно наблюдающего за потребностями каждой ВМ, и при необходимости инструктирующего устройство вытеснения памяти для выполнения увеличения или уменьшения объёма виртуальной памяти.

Дополнительные примечания:

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

Чтобы включить механизм вытеснения памяти, перейдите на вкладку **Оптимизация** в окне **Новый кластер** или **Параметры кластера**. Затем установите флажок **Включить оптимизацию памяти balloon**. Этот параметр включает механизм вытеснения памяти на виртуальных машинах, выполняющихся на хостах в данном кластере, и диспетчер MoM начинает вытеснение памяти, где это возможно, при этом ограничением служит только размер гарантированной памяти каждой ВМ (см. п. 8.2.3. Параметры оптимизации).

Каждый хост в данном кластере получает обновление политики вытеснения памяти при смене статуса этого хоста на «*Запущен*». При необходимости обновить информацию о политике вытеснения памяти на хосте можно без смены статуса (см. п. 8.2.9. Обновление информации о политике MoM на хостах в кластере).

8.2.15.5. Объединение одинаковых страниц памяти ядром (KSM)

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

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

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

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

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

Дополнительные примечания:

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

Чтобы включить механизм объединения одинаковых страниц памяти ядром, перейдите на вкладку **Оптимизация** в окне **Новый кластер** или **Параметры кластера.**

Затем установите флажок **Включить KSM**. Этот параметр заставляет диспетчер превышенного выделения памяти MoM запускать KSM, когда это необходимо, в том числе когда преимущества экономии памяти при объединении одинаковых страниц памяти перевешивают затраты ЦП на работу KSM (см. п. 8.2.3. Параметры оптимизации).

8.2.16. Изменение версии совместимости кластера

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

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

Изменение версии совместимости кластера

1. В главном меню Портала администрирования нажмите **Ресурсы → Кластеры**.
2. Выберите кластер и нажмите **Изменить**.
3. На вкладке **Общее** смените **Версию совместимости** на необходимое значение.
4. Нажмите **ОК**.

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

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

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

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

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

Глава 9. Логические сети

9.1. Задачи при работе с логическими сетями

9.1.1. Выполнение сетевых задач

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

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

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

Доступ к этому функционалу также возможен для каждого индивидуального ресурса.

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

Если узлы системы виртуализации ROSA Virtualization планируется использовать для предоставления каких-либо служб, помните, что службы остановятся, если окружение виртуализации прекратит работать. Это касается всех служб, но особенно чётко нужно понимать риски выполнения следующих служб в окружении виртуализации:

- Службы каталогов.
- DNS.
- Хранилище.

9.1.2. Создание новой логической сети в дата-центре или кластере

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

Создание новой логической сети в дата-центре или в кластере

1. Нажмите **Ресурсы → Дата-центры** или **Ресурсы → Кластеры**.
2. Нажмите на название дата-центра или кластера, чтобы открыть подробный просмотр.
3. Перейдите на вкладку **Логические сети**.
4. Откройте окно **Новая логическая сеть** (Рис. 32):
   - В подробном просмотре дата-центра нажмите **Добавить**.
   - В подробном просмотре кластера нажмите **Добавить сеть**.

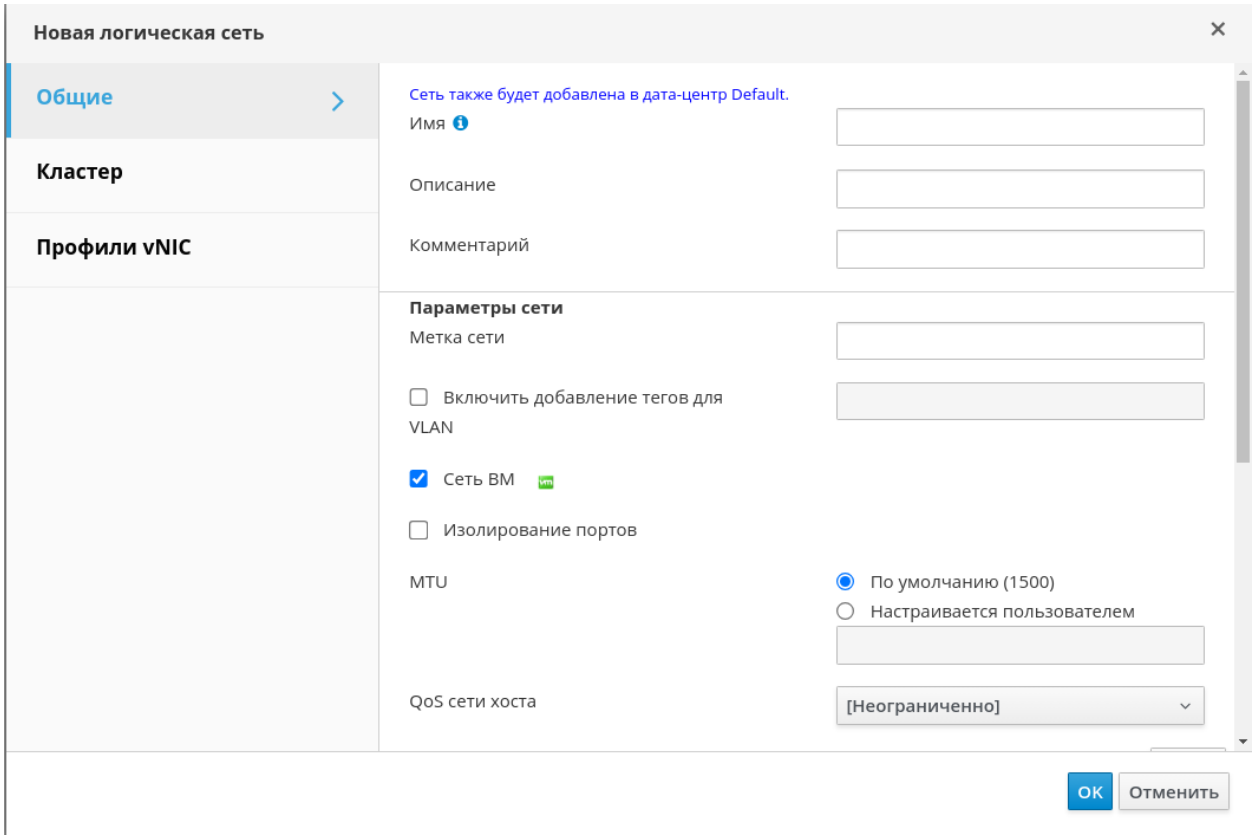

Рис. 32. Новая логическая сеть

5. Укажите **Имя**, **Описание** и **Комментарий** для логической сети.
6. Опционально включите параметр **Включить добавление тегов для VLAN**.
7. Опционально отключите параметр **Сеть ВМ**.
8. Опционально включите параметр **Изолирование портов**, чтобы ВМ не могли обмениваться данными в логической сети.
9. Опционально включите параметр **Создать на внешнем поставщике**. Таким образом будут отключены параметры **Метка сети**, **Сеть ВМ** и **MTU**.
10. Выберите **Внешнего поставщика**. В список **Внешний поставщик** не включены внешние поставщики с режимом `read-only`.
    Чтобы создать внутреннюю изолированную сеть, выберите в списке **Внешний поставщик** пункт **ovirt-provider-ovn** и не отмечайте параметр **Подключиться к физической сети**.
11. В поле **Метка сети** введите новую метку логической сети или выберите уже существующую.
12. Укажите значение **MTU**: **По умолчанию (1500)** или **Пользовательское**.
13. При выборе в списке **Внешний поставщик** пункта **ovirt-provider-ovn** укажите необходимо ли в сети применять **Группы безопасности**.
14. Во вкладке **Кластер** выберите кластеры, которым будет присвоена сеть. Также можно указать, будет ли эта логическая сеть требуемой сетью.
15. При выборе пункта **Создать внешнего поставщика** станет видимой вкладка **Подсеть**. Укажите в этой вкладке **Имя**, **CIDR** и **Шлюз**. При необходимости можно добавить серверы DNS.
16. Во вкладке **Профили vNIC** добавьте профили требуемых виртуальных NIC к логической сети.
17. Нажмите **OK**.

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

Примечание — при создании новых логических сетей или внесении изменений в существующие логические сети, используемые в качестве сетей визуализации, для того чтобы новые сети стали доступны или для применения внесённых изменений необходимо перезапустить любые выполняющиеся ВМ, использующие эти сети.

9.1.3. Изменение параметров логических сетей

Примечание — логическую сеть нельзя редактировать или переместить на другой интерфейс, если она не синхронизирована с сетевой конфигурацией на хосте. Информацию о том, как синхронизировать сети, см. п. 9.4.3. Синхронизация сетей хостов.

Изменение параметров логической сети

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра, чтобы открыть подробный просмотр.
3. Перейдите на вкладку **Логические сети** и выберите логическую сеть.
4. Нажмите **Параметры**.
5. Внесите необходимые изменения параметров (Рис. 33).

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

6. Нажмите **OK**.

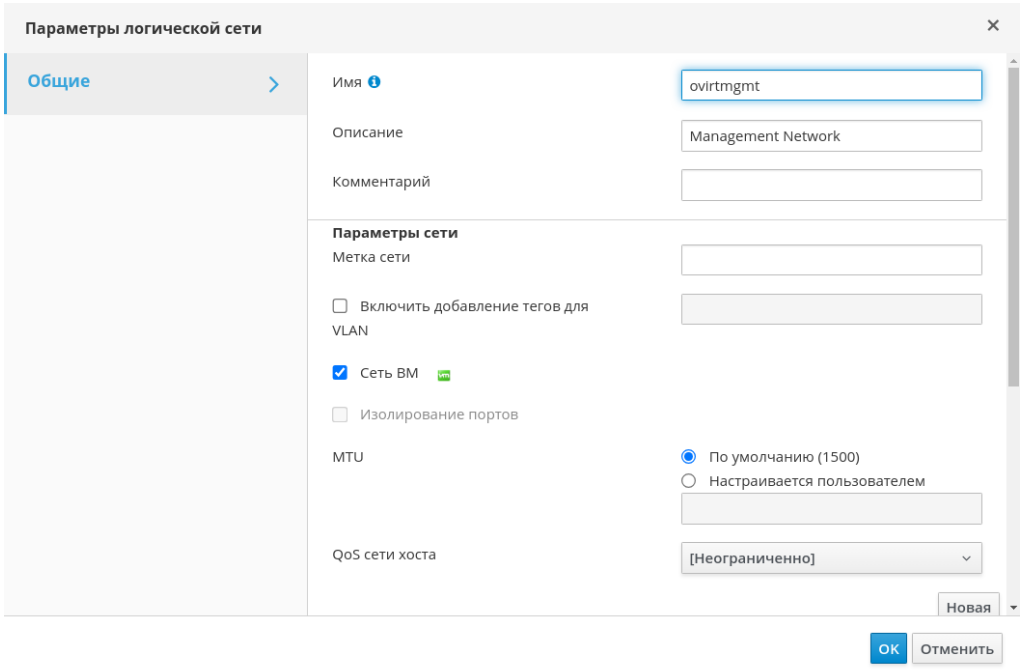

Рис. 33. Изменение параметров логической сети

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

9.1.4. Удаление логической сети

Удаление логической сети выполняется из меню **Сеть → Сети** или **Ресурсы → Дата-центры**. В следующей пошаговой последовательности показывается, как удалить логические сети, связанные с дата-центром.

Примечание — для окружения виртуализации ROSA Virtualization необходима как минимум одна логическая сеть, используемая в качестве сети управления `ovirtmgmt`.

Удаление логической сети

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

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

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

Маршрут по умолчанию, используемый хостами в кластере, проложен через сеть управления `ovirtmgmt`. В следующей пошаговой инструкции показано, как настроить логическую сеть, не являющуюся сетью управления, в качестве маршрута по умолчанию.

Примечание — если используется частный параметр `default_route`, то перед выполнением данной инструкции необходимо будет сначала удалить пользовательское значение на всех прикреплённых хостах.

Настройка логической сети в качестве маршрута по умолчанию

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

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

Примечания, связанные с IPv6:

- Для IPv6 поддерживается только статическая адресация.

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

9.1.6. Просмотр или редактирование параметров шлюза логической сети

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

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

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

Просмотр или редактирование параметров шлюза логической сети

1. Нажмите **Ресурсы → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**, чтобы увидеть список и параметры сетевых интерфейсов, подключённых к хосту.
4. Нажмите кнопку **Настроить сети хоста**.
5. Наведите курсор на присвоенную логическую сеть и нажмите на значок карандаша, чтобы открыть окно **Изменить сеть управления**.
6. В окне **Изменить сеть управления** показывается имя сети, протокол загрузки, а также IP-адреса, маски подсети и шлюза. Для изменения сведений об адресах вручную выберите **Статический** протокол загрузки.

9.1.7. Общие параметры логической сети

В **Табл. 9.1** описываются параметры вкладки **Общие** в окнах **Новая логическая сеть** и **Параметры логической сети**.

Табл. 9.1. Параметры вкладки «Общие» в окнах «Новая логическая сеть» и «Параметры логической сети»

Поле	Описание
Имя	Название логической сети. Это текстовое поле должно содержать уникальное название, состоящее из любого сочетания строчных и прописных букв, чисел, тире и символа нижнего подчёркивания. Обратите внимание, что хотя в названии логической сети может быть больше 15 символов, и оно может содержать символы, не входящие в таблицу ASCII, идентификатор на хосте `vdsm_name` будет отличаться от указанного названия
Описание	Описание логической сети. Предел для этого текстового поля — 40 символов
Комментарий	Поле для добавления комментария для логической сети в простом текстовом формате

Поле	Описание
Создать на внешнем поставщике	Параметр позволяет создать логическую сеть до экземпляра OpenStack Networking, добавленного в виртуализированный ЦУ в качестве внешнего поставщика (параметр **Внешний поставщик** позволяет выбрать внешнего поставщика, на котором будет создана логическая сеть)
Включить добавление тегов для VLAN	Добавление тегов для VLAN — это средство защиты, выдающее всему сетевому трафику, передающемуся по логической сети, особые характеристики. Трафик с тегами VLAN не может быть прочитан интерфейсами, не имеющими таких же характеристик. Использование виртуальных LAN в логических сетях также даёт возможность одному сетевому интерфейсу быть связанным с несколькими логическими сетями, имеющими разные метки VLAN. Если метки VLAN включены, введите числовое значение в данное текстовое поле
Сеть ВМ	Отметьте этот параметр, если эту сеть используют только ВМ. Если трафик, для передачи которого используется эта сеть, создаётся не виртуальными машинами (например, обмен информацией между хранилищами), не отмечайте этот параметр
MTU	Выберите либо значение **По умолчанию**, которое устанавливает максимальный размер пакета согласно числу, указанному в скобках (), либо значение **Пользовательское**, чтобы указать необходимое число MTU для логической сети. Этот параметр можно использовать, чтобы привести в соответствие число MTU, поддерживаемое логической сетью, с числом MTU, поддерживаемым аппаратными составляющими интерфейса. При выборе значения **Пользовательское** укажите необходимое число в текстовом поле
Метка сети	Параметр позволяет указать новую метку сети или выбрать метку из существующих, уже присвоенных сетевым интерфейсам хоста. При выборе существующей метки логическая сеть будет автоматически присвоена всем сетевым интерфейсам хоста с этой меткой
Группы безопасности	Параметр позволяет присвоить группы безопасности портам в этой логической сети. Значение **Отключено** отключает группы безопасности, значение **Включено** — включает. При создании и подключении порта к этой сети, порт создаётся с активированной безопасностью. Это означает, что доступ к ВМ или от ВМ выполняется согласно настроенным на данный момент группам безопасности. Значение **Наследовать из конфигурации** означает, что порты наследуют поведение, указанное в файле конфигурации, общем для всех сетей

9.1.8. Параметры кластеров при настройке логических сетей

В **Табл. 9.2** описываются параметры вкладки **Кластер** окна **Новая логическая сеть**.

Табл. 9.2. Параметры вкладки «Кластер» окна «Новая логическая сеть»

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

9.1.9. Параметры профилей vNIC при настройке логических сетей

В **Табл. 9.3** описываются параметры вкладки **Профили vNIC** окна **Новая логическая сеть**.

Табл. 9.3. Параметры вкладки «Профили vNIC» окна «Новая логическая сеть»

Поле	Описание
Профили vNIC	Позволяет указать один или более профилей vNIC логической сети. Чтобы добавить или удалить профиль логической сети, нажмите соответственно значок + (плюс) или – (минус) рядом с профилем vNIC. Первое поле служит для указания имени профиля. **Открытый** — будет ли профиль доступен всем пользователям. **QoS** — профиль качества обслуживания сети, назначенный профилю vNIC.

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

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

Настройка типов трафика для логических сетей

1. Нажмите **Ресурсы → Кластеры**.
2. Нажмите на имя кластера, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Логические сети**.
4. Нажмите **Управление сетями**.
5. Установите необходимые флажки и настройте переключатели (Рис. 34).
6. Нажмите **OK**.

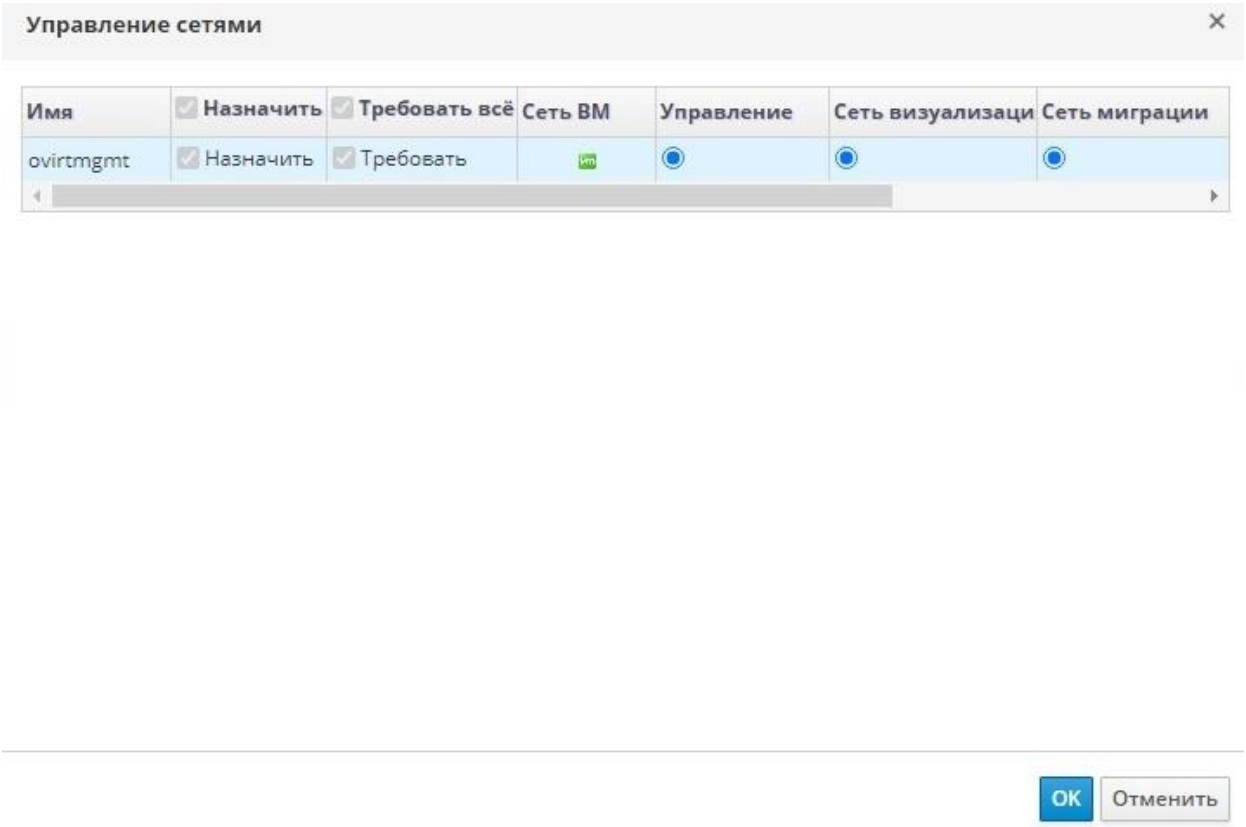

Рис. 34. Управление сетями

Примечание — логические сети, предоставленные внешними поставщиками, должны использоваться только как сети виртуальных машин, в связи с этим им нельзя присвоить специальные кластерные роли, такие как сеть визуализации или сеть миграции.

9.1.11. Параметры в окне «Управление сетями»

В **Табл. 9.4** описываются параметры в окне **Управление сетями**.

Табл. 9.4. Параметры в окне «Управление сетями»

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

9.1.12. Изменение конфигурации виртуальной функции сетевой платы

В данном подразделе описывается как установить и настроить технологию виртуализации ввода-вывода с единым корнем (SR-IOV) в системе виртуализации ROSA Virtualization. Дополнительные сведения приведены в п. 9.4. Хосты и организация сетей.

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

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

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

Для возможности прямого подключения vNIC к виртуальной функции, в профиле vNIC необходимо активировать возможность сквозного доступа (см. п. 9.2.4. Включение сквозного доступа в профиле vNIC).

Редактирование конфигурации виртуальной функции сетевой платы

1. Нажмите **Ресурсы → Хосты**.
2. Нажмите на название хоста с поддержкой SR-IOV, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**.
4. Нажмите кнопку **Настроить сети хоста**.
5. Выберите сетевую карту с поддержкой SR-IOV (отмечается значком ) и нажмите на значок карандаша.

6. Чтобы изменить число виртуальных функций, нажмите кнопку **Параметр числа виртуальных функций** и измените значение в поле **Число виртуальных функций**.

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

7. Флажок для параметра **Все сети** проставлен по умолчанию, что разрешает возможность доступа к виртуальным функциям для всех сетей. Чтобы указать отдельные виртуальные сети, которым разрешён доступ к виртуальным функциям, выберите переключатель **Конкретные сети**, чтобы увидеть список всех сетей. Затем можно либо отметить нужные сети, либо с помощью текстового поля **Метки** автоматически выбрать все сети с нужными сетевыми метками.
8. Нажмите **OK**.
9. В окне **Настроить сети хоста** нажмите **OK**.

9.2. Виртуальные сетевые платы (vNIC)

9.2.1. Обзор профиля vNIC

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

9.2.2. Создание или изменение профиля vNIC

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

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

Создание или редактирование профиля vNIC

1. Нажмите **Сеть → Сети**.
2. Нажмите на имя логической сети, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Профили vNIC**.
4. Нажмите **Добавить** или **Изменить**.
5. Введите **Имя** и **Описание** профиля.
6. В списке **QoS** выберите соответствующую политику качества обслуживания.
7. Из выпадающего списка выберите **Сетевой фильтр** для управления исходящим и входящим трафиком сетевых пакетов виртуальных машин.
8. Установите флажок для параметра **Сквозной доступ**, чтобы включить возможность сквозного доступа для vNIC и разрешить прямое присвоение

виртуальной функции устройствам. Включение сквозного доступа отключит QoS, сетевую фильтрацию и зеркалирование портов, так как эти возможности несовместимы со сквозным доступом (см. п. 9.2.4. Включение сквозного доступа в профиле vNIC).

9. При выбранном параметре **Сквозной доступ** снимите флажок (при необходимости) с параметра **Может мигрировать**, чтобы отключить возможность миграции для vNIC, использующих этот профиль.
10. Установите переключатели **Зеркалирование портов** и **Разрешить всем пользователям использовать этот профиль** в необходимое положение.
11. Выберите частное свойство из списка свойств. По умолчанию отображается пункт **Выберите ключ…**. Добавьте или удалите частные свойства с помощью кнопок **+** (плюс) или **–** (минус) соответственно.
12. Нажмите **OK**.

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

9.2.3. Параметры в окне «Профиль сетевого адаптера ВМ»

В **Табл. 9.5** описываются параметры в окне **Профиль сетевого адаптера ВМ**.

Табл. 9.5. Параметры в окне «Профиль сетевого адаптера ВМ»

Поле	Описание
Сеть	Выпадающий список доступных сетей, к которым можно применить профиль vNIC
Имя	Название профиля vNIC. Это должно быть уникальное имя от 1 до 50 символов, состоящее из любого сочетания прописных и строчных букв, чисел, тире и знаков подчёркивания
Описание	Описание профиля vNIC. Заполнение этого поля рекомендуется, но не является обязательным
QoS	Выпадающий список доступных политик качества обслуживания сетей, которые можно применить к профилю vNIC. Политики QoS регулируют входящий и исходящий трафик vNIC
Сетевой фильтр	Выпадающий список доступных сетевых фильтров, которые можно применить к профилю vNIC. Сетевые фильтры повышают безопасность сети, фильтруя типы пакетов, которые могут быть посланы с ВМ или на ВМ. Фильтр по умолчанию `vdsm-no-mac-spoofing`, являющийся комбинацией `no-mac-spoofing` и `no-arp-mac-spoofing`. Для виртуальных LAN и сетевых связок ВМ используйте `<No Network Filter>`. На доверенных ВМ отказ от использования сетевого фильтра может улучшить производительность. Примечание — ROSA Virtualization не поддерживает отключение сетевых фильтров с помощью указания значения `false` для параметра `EnableMACAntiSpoofingFilterRules` с использованием утилиты `engine-config`. Используйте для этого параметр `<No Network Filter>`
Сквозной доступ	Флажок для переключения свойства сквозного доступа. Сквозной доступ позволяет vNIC напрямую подключаться к виртуальной функции сетевой карты хоста. Свойство сквозного доступа нельзя редактировать, если профиль vNIC присоединён к ВМ. При включении сквозного доступа в профиле vNIC отключаются QoS, сетевые фильтры и зеркалирование портов

Поле	Описание
С возможностью миграции	Флажок для переключения возможности миграции vNIC, использующей этот профиль. В обычных профилях vNIC миграция включена по умолчанию (флажок выставлен и не доступен для отключения). При отмеченном параметре **Сквозной доступ** становится доступным параметр **С возможностью миграции**. В данном случае при необходимости параметр можно отключить, чтобы запретить миграцию vNIC со сквозным доступом
Зеркалирование портов	Флажок для переключения зеркалирования портов. Зеркалирование портов копирует сетевой трафик третьего уровня из логической сети на виртуальный интерфейс ВМ. По умолчанию этот параметр не отмечен
Частные свойства устройства	Выпадающее меню для выбора доступных частных свойств, применимых к профилю vNIC. Для добавления или удаления свойств используйте кнопки + или – соответственно
Разрешить всем пользователям использовать этот профиль	Флажок для переключения доступности профиля для всех пользователей в окружении. По умолчанию этот параметр отмечен

9.2.4. Включение сквозного доступа в профиле vNIC

В данном подразделе описывается как установить и настроить технологию виртуализации ввода-вывода с единым корнем (SR-IOV) в системе виртуализации ROSA Virtualization. Дополнительные сведения приведены в п. 9.4. Хосты и организация сетей.

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

Сквозной доступ нельзя включить, если профиль vNIC уже присоединён к vNIC. Поэтому в процессе следующей пошаговой инструкции создаётся новый профиль.

Примечание — если в профиле vNIC включается сквозной доступ, то в этом же профиле нельзя будет включить QoS, сетевые фильтры и зеркалирование портов.

Включение сквозного доступа

1. Нажмите **Сеть → Сети**.
2. Нажмите на имя логической сети, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Профили vNIC**, чтобы увидеть список всех профилей vNIC для этой логической сети.
4. Нажмите **Добавить.**
5. Укажите **Имя** и **Описание** профиля.
6. Установите флажок для параметра **Сквозной доступ**.
7. Опционально отключите параметр **С возможностью миграции** для отключения миграции vNIC, использующих этот профиль.
8. Выберите частное свойство из списка свойств. По умолчанию отображается пункт **Выберите ключ…**. Добавьте или удалите частные свойства с помощью кнопок + (плюс) или – (минус) соответственно.
9. Нажмите **ОК**.

Профиль vNIC теперь поддерживает технологию сквозного доступа. Чтобы напрямую присоединить ВМ к сетевой плате или виртуальной функции PCI, подключите логическую сеть к сетевой плате и создайте на нужной ВМ, использующей профиль vNIC с поддержкой сквозного доступа, новую vNIC со сквозным доступом к PCI.

9.2.5. Удаление профиля vNIC

Удаление профиля vNIC

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

9.2.6. Присвоение групп безопасности профилям vNIC

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

Примечание — возможность присвоения групп безопасности профилям vNIC доступна только при конфигурации внешнего поставщика OpenStack Networking (neutron). Группы безопасности нельзя создать средствами виртуализированного ЦУ, их необходимо создавать при помощи OpenStack. Группа безопасности опознаётся с помощью идентификатора этой группы, зарегистрированном в экземпляре OpenStack Networking. Найти идентификаторы групп безопасности указанного участника можно, выполнив следующую команду в системе с установленным комплексом OpenStack Networking:

```
# neutron security-group-list
```

Присвоение групп безопасности профилям vNIC

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

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

9.2.7. Полномочия пользователей на профили vNIC

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

Пользовательские полномочия на профиль vNIC

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

9.2.8. Настройка профилей vNIC для интеграции с UCS

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

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

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

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

Примечание — профиль порта UCS должен быть настроен в системе Cisco UCS до настройки профиля vNIC.

Настройка частного свойства устройства

1. Настройте частное свойство `vmfex` в виртуализированном ЦУ и с помощью опции `--cver` укажите уровень совместимости кластера:

```
# engine-config -s CustomDeviceProperties='{type=interface;prop=
{vmfex=^[a-zA-Z0-9_.-]{2,32}$}}' --cver=4.5
```

2. Убедитесь в том, что частное свойство `vmfex` добавлено:

```
# engine-config -g CustomDeviceProperties
```

3. Перезапустите службу `ovirt-engine`:

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

Настраиваемый профиль vNIC может принадлежать к новой или уже существующей логической сети (подробную инструкцию по настройке новой логической сети см. п. 9.1.2. Создание новой логической сети в дата-центре или кластере).

Настройка профиля vNIC для интеграции в UCS

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

9.3. Сети внешних поставщиков

9.3.1. Импортирование сетей из внешних поставщиков

Чтобы иметь возможность использовать сети от внешнего поставщика (OpenStack Networking или любой другой сторонний поставщик с реализацией OpenStack Neutron REST API), зарегистрируйте поставщика в виртуализированном ЦУ.

Затем выполните следующую последовательность действий, чтобы импортировать сети этого поставщика в виртуализированный ЦУ для возможности их использования виртуальными машинами.

Импортирование сетей внешнего поставщика

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

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

9.3.2. Ограничения при использовании сетей внешних поставщиков

Существуют следующие ограничения при использовании логических сетей, импортированных с внешнего поставщика, в системе виртуализации ROSA Virtualization:

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

9.3.3. Настройка подсетей в логических сетях внешних поставщиков

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

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

Если в качестве внешнего поставщика был добавлен OVN (`ovirt-provider-ovn`), то несколько подсетей можно соединить между собой с помощью роутеров. Для управления этими роутерами можно использовать OpenStack Networking API v2.0. Тем не менее, обратите внимание, что у `ovirt-provider-ovn` есть свои ограничения, в частности отсутствует реализация Source NAT (`enable_snat`) в OpenStack API.

9.3.4. Добавление подсетей в логических сетях внешних поставщиков

Добавление подсетей в логических сетях внешних поставщиков

1. Нажмите **Сеть → Сети**.
2. Нажмите на имя логической сети, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Подсети**.
4. Нажмите **Добавить**.

5. Укажите **Имя** и **CIDR** новой подсети.
6. Из выпадающего списка **Версия IP** выберите **IPv4** или **IPv6**.
7. Нажмите **OK**.

Примечание — для IPv6 поддерживается только статическая адресация.

9.3.5. Удаление подсетей из логических сетей внешних поставщиков

Удаление подсетей из логических сетей внешних поставщиков

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

9.3.6. Присвоение групп безопасности логическим сетям и портам

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

В системе виртуализации ROSA Virtualization группы безопасности по умолчанию отключены.

Примечание — возможность присвоения групп безопасности логическим сетям и портам доступна, только если в качестве внешнего поставщика сетей выбран OVN (`ovirt-provider-ovn`). Обратите внимание, что в виртуализированном ЦУ нельзя создавать группы безопасности. Группы безопасности необходимо создавать с помощью OpenStack Networking API v2.0 или Ansible.

Добавление групп безопасности в логические сети

1. Нажмите **Ресурсы → Кластеры**.
2. Нажмите на имя кластера, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Логические сети**.
4. Нажмите **Добавить сеть** и настройте свойства сети (см. п. 9.1.2. Создание новой логической сети в дата-центре или кластере). В частности, выберите из выпадающего списка **Внешний поставщик** пункт **`ovirt-provider-ovn`**.
5. Из выпадающего списка **Защита сетевых портов** выберите **Включено** (см. п. 9.1.7. Общие параметры логической сети).
6. Нажмите **`OK`**.
7. Создайте группы безопасности и правила групп безопасности с помощью OpenStack Networking API v2.0 или Ansible.
8. Обновите информацию о настроенных группах безопасности на портах.
9. Опционально укажите, будет ли этот функционал безопасности включён на уровне портов (на данный момент это возможно только с помощью OpenStack Networking API). Если атрибут **`port_security_enabled`** не был указан, то его значение по умолчанию будет совпадать со значением в той сети, которой он принадлежит.

9.4. Хосты и организация сетей

9.4.1. Обновление сведений о характеристиках хоста

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

Обновление сведений о характеристиках хоста

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

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

9.4.2. Изменение параметров сетевых интерфейсов и присвоение хостам логических сетей

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

Примечания:

- Единственным способом изменить IP-адрес хоста в системе виртуализации является удаление хоста и повторное его добавление.
- Сведения о том, как изменить параметры VLAN хоста, приведены в п. 9.4.4. Изменение параметров VLAN хоста.
- Логические сети внешних поставщиков невозможно присвоить физическим сетевым интерфейсам хоста. Такие сети присваиваются хостам динамически по мере требований со стороны ВМ.
- Если коммутатор был настроен на предоставление сведений о протоколе LLDP, для просмотра текущей конфигурации порта коммутатора наведите курсор на физический сетевой интерфейс. Это может помочь в предотвращении создания неправильных конфигураций. Перед присвоением логических сетей рекомендуется проверить следующую информацию:
  - *Описание порта (TLV тип 4)* и *Системное имя (TLV тип 5)*. Параметры помогают определить, на какие порты и на какой коммутатор накладываются интерфейсы хоста.
  - *Идентификатор VLAN порта*. Параметр показывает встроенный идентификатор VLAN, настроенный на порте коммутатора для кадров Ethernet без меток. Все виртуальные LAN, настроенные на порте коммутатора, показываются в виде сочетаний *VLAN имя* и *VLAN идентификатор*.

Изменение параметров сетевых интерфейсов и присвоение хостам логических сетей

1. Нажмите **Ресурсы → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**.
4. Нажмите **Настроить сети хоста**.

5. При необходимости наведите курсор на сетевой интерфейс хоста, чтобы просмотреть сведения о конфигурации, предоставляемой коммутатором.
6. Подключите логическую сеть к физическому сетевому интерфейсу хоста — выберите и перетащите логическую сеть в область **Назначенные логические сети** рядом с физическим сетевым интерфейсом хоста.

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

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

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

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

При смене IP-адреса сети управления хоста, хост необходимо переустановить, чтобы настроить IP-адрес.

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

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

   c. Используйте параметры во вкладке **QoS** для переопределения качества обслуживания сети по умолчанию. Выберите **Переопределить QoS** и укажите нужные значения в следующих полях:
      - **Взвешенная доля**: означает, какую долю пропускной способности логического канала нужно выделить конкретной сети относительно других сетей, прикреплённых к этому же логическому каналу. Точная доля зависит от суммы долей всех сетей на этом канале. По умолчанию это число в диапазоне от 1 до 100.
      - **Предел скорости (Мбит/с)**: максимальная пропускная способность сети.
      - **Гарантированная скорость (Мбит/с)**: минимальная пропускная способность, требуемая для сети. Гарантированная скорость на деле не гарантируется, и будет изменяться в зависимости от сетевой

инфраструктуры и гарантированной скорости, запрашиваемой другими сетями на этом же логическом канале.

d. Для настройки сетевого моста перейдите на вкладку **Настраиваемые пользователем параметры** и в выпадающем списке выберите **bridge_opts**. Введите действительный ключ и значение, придерживаясь следующего синтаксиса: *ключ=значение*. Несколько записей разделяются символом пробела. Действительными являются следующие ключи со значениями, приведенными в качестве примера (см. раздел B.1. Параметры bridge_opts):

```
forward_delay=1500
gc_timer=3765
group_addr=1:80:c2:0:0:0
group_fwd_mask=0x0
hash_elasticity=4
hash_max=512
hello_time=200
hello_timer=70
max_age=2000
multicast_last_member_count=2
multicast_last_member_interval=100
multicast_membership_interval=26000
multicast_querier=0
multicast_querier_interval=25500
multicast_query_interval=13000
multicast_query_response_interval=1000
multicast_query_use_ifaddr=0
multicast_router=1
multicast_snooping=1
multicast_startup_query_count=2
multicast_startup_query_interval=3125
```

e. Чтобы настроить свойства Ethernet, перейдите на вкладку **Настраиваемые пользователем параметры** и в выпадающем списке выберите параметр **ethtool_opts**. Укажите действительное значение, используя формат командных аргументов `ethtool`.
Например:

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

В этом поле допускаются символы подстановки. Например, чтобы применить один и тот же параметр ко всем интерфейсам этой сети, используйте следующие значения:

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

Параметр **ethtool_opts** по умолчанию недоступен и его необходимо добавить с помощью утилиты настройки виртуализированного ЦУ (см. раздел B.2. Настройка использования команды ethtool в виртуализированном ЦУ).

f. Для настройки протокола FCoE перейдите на вкладку **Настраиваемые пользователем параметры** и в выпадающем списке выберите параметр **fcoe**. Введите действительный ключ и значение, придерживаясь следующего синтаксиса: *ключ=значение*. Минимальное требуемое значение: `enable=yes`. Также можно добавить `dcb= and auto_vlan=[yes|no]`. Отделяйте записи

символом пробела. Параметр **fcoe** по умолчанию недоступен и его необходимо добавить с помощью утилиты настройки виртуализированного ЦУ (см. раздел В.3. Настройка использования протокола FCoE в виртуализированном ЦУ).

Примечание — для использования FCoE рекомендуется отдельная выделенная логическая сеть.

g. Чтобы сменить сеть хоста по умолчанию с сети управления (`ovirtmgmt`) на сеть, не являющуюся сетью управления, настройте маршрут этой сети по умолчанию (см. п. 9.1.5. Настройка логической сети, не являющейся сетью управления, в качестве маршрута по умолчанию).
h. Если определение логической сети не синхронизировано с сетевой конфигурацией на хосте, установите флажок для параметра **Синхронизировать сеть** (см. п. 9.4.3. Синхронизация сетей хостов).

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

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

9.4.3. Синхронизация сетей хостов

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

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

Хост может получить статус «*вне синхронизации*» в следующих случаях:

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

Использование следующих практических решений может предотвратить рассинхронизацию хостов:

- Вносите изменения на Портале администрирования, а не локально на хосте.
- Изменяйте параметры VLAN только согласно инструкциям, приведенным в п. 9.4.4. Изменение параметров VLAN хоста.

Синхронизация хостов

Синхронизация определений сетевых интерфейсов хоста включает в себя применение используемых определений виртуализированного ЦУ на хосте. Если эти

определения не являются требуемыми определениями, то после синхронизации хостов, обновите определения хостов с помощью интерфейса на Портале администрирования.

Сети хостов можно синхронизировать на трёх уровнях:

- На уровне каждой логической сети.
- На уровне каждого хоста.
- На уровне каждого кластера.

Синхронизация сетей хоста на уровне логической сети

1. Нажмите **Ресурсы → Хосты.**
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы.**
4. Нажмите **Настроить сети хоста.**
5. Наведите курсор на сеть «*вне синхронизации*» и нажмите на значок карандаша, чтобы открыть окно **Свойства сети.**
6. Установите флажок для параметра **Синхронизировать сеть.**
7. Нажмите **OK** для применения изменений.
8. Нажмите **OK,** чтобы закрыть окно **Настроить сети хоста.**

Синхронизация сетей хоста на уровне хоста

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

Синхронизация сетей хоста на уровне кластера

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

Примечание — синхронизировать сети хоста можно также с помощью REST API.

9.4.4. Изменение параметров VLAN хоста

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

Изменение параметров VLAN хоста с сохранением синхронизации сетей

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

При смене VLAN ID сети управления появляется следующее предупреждение:

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

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

Примечание — при смене VLAN ID сети управления, для последующего применения нового значения VLAN ID необходимо переустановить хост.

9.4.5. Добавление нескольких VLAN на один сетевой интерфейс с использованием логических сетей

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

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

Добавление нескольких VLAN на один сетевой интерфейс с использованием логических сетей

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

После выполнения приведенной процедуры добавьте логическую сеть к каждому хосту в кластере, отредактировав параметры сетевой платы на каждом хосте в кластере. Таким образом сеть будет готова к эксплуатации.

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

9.4.6. Присвоение дополнительных адресов IPv4 сетям хостов

Сети хоста, такие как сеть управления `ovirtmgmt`, изначально создаются только с одним IP-адресом. Это означает, что если в файле конфигурации сетевой платы (например, */etc/sysconfig/network-scripts/ifcfg-eth01*) настроено несколько IP-адресов, то сети хоста будет присвоен только первый указанный IP-адрес. Остальные адреса могут потребоваться

при подключении к хранилищу или к серверу в отдельной частной подсети, использующей ту же самую сетевую плату.

Ловушка `vdsm-hook-extra-ipv4-addrs` даёт возможность настроить дополнительные адреса IPv4 для сетей хоста.

В следующей пошаговой инструкции задачи, относящиеся к хосту, должны быть выполнены на каждом хосте, для которого необходимо настроить дополнительные IP-адреса.

Присвоение дополнительных адресов IPv4 сетям хоста

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

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

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

   ```
   # engine-config -s 'UserDefinedNetworkCustomProperties=ipv4_addrs=.*'
   ```

3. Перезапустите службу `ovirt-engine`:

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

4. В главном меню Портала администрирования нажмите **Ресурсы → Хосты**.
5. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
6. Перейдите на вкладку **Сетевые интерфейсы** и нажмите **Настроить сети хоста**.
7. Наведите курсор на присвоенную логическую сеть и нажмите на значок карандаша.
8. Из выпадающего списка **Настраиваемые пользователем параметры** выберите пункт **ipv4_addr** и добавьте дополнительный IP-адрес и префикс сети (например, 5.5.5.5/24). Обратите внимание, что несколько IP-адресов должны разделяться запятой.
9. Нажмите **OK**, чтобы закрыть окно **Параметры сети**.
10. Нажмите **OK**, чтобы закрыть окно **Настроить сети хоста**.

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

9.4.7. Добавление сетевых меток сетевым интерфейсам хоста

Использование сетевых меток сильно упрощает выполнение административных задач, связанных с присвоением логических сетей сетевым интерфейсам хоста. Присвоение метки ролевой сети (например, сети миграции или сети визуализации) позволяет осуществлять массовое развёртывание этой сети на всех хостах с помощью протокола DHCP. Этот способ массового развёртывания был выбран вместо способа указывания статических адресов, так как задачу многократного вписывания статических IP-адресов невозможно масштабировать.

Существуют следующие способы добавления меток сетевому интерфейсу хоста:

- Вручную на Портале администрирования.
- Автоматически с помощью службы меток LLDP.

Добавление сетевых меток хосту вручную на Портале администрирования

1. Нажмите **Ресурсы → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**.
4. Нажмите **Настроить сети хоста**.
5. Нажмите **Метки**.
6. Нажмите **Новая метка**. Выберите физический сетевой интерфейс, которому нужно назначить метку.
7. В поле **Метка** введите имя сетевой метки.
8. Нажмите **ОК**.

Добавление сетевых меток хосту автоматически с помощью службы меток LLDP

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

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

Предварительные условия:

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

Последовательность действий

1. Настройте параметры `username` и `password` в файле `/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf`:
   - `username` - имя пользователя администратора виртуализированного ЦУ. Значение по умолчанию: `admin@internal`.
   - `password` - пароль администратора виртуализированного ЦУ. Значение по умолчанию: `123456`.
2. Настройте службу меток LLDP. Для этого обновите следующие значения в файле `etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf`:
   - `clusters` - список кластеров (через запятую), на которых должна выполняться служба. Например, `Cluster*` означает, что служба меток будет выполняться в кластерах, название которых начинается со слова `Cluster`. Чтобы служба меток выполнялась во всех кластерах в дата-центре, введите символ `*` (звёздочка). Значение по умолчанию: `Def*`.
   - `api_url` - полный URL-адрес API виртуализированного ЦУ. Значение по умолчанию: `https://`*`полное_доменное_имя_ЦУ`*`/ovirt-engine/api`.
   - `ca_file` - путь до частного файла сертификата центра сертификации. Если сертификат не используется, оставьте пустое поле. Значение по умолчанию: пустое поле.
   - `auto_bonding` – параметр включает возможности службы меток LLDP по созданию сетевых агрегаций. Значение по умолчанию: `true`.
   - `auto_labeling` - параметр включает возможности службы меток LLDP по созданию меток. Значение по умолчанию: `true`.
3. При необходимости можно настроить выполнение службы с другими интервалами. Для этого измените значение параметра `OnUnitActiveSec` в файле

`etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer`. Значение по умолчанию: `1h` (1 час).

4. Выполните следующую команду для текущего и автоматического (при загрузке) запуска службы:

```
# systemctl enable --now ovirt-lldp-labeler
```

Примечание — для запуска службы `ovirt-lldp-labeler` вручную выполните следующую команду:

```
# /usr/bin/python /usr/share/ovirt-lldp-labeler/ovirt_lldp_labeler_cli.py
```

В результате будет присвоена сетевая метка сетевому интерфейсу хоста. Новые логические сети с такой же меткой будут автоматически присваиваться всем сетевым интерфейсам хоста, имеющим ту же метку. Удаление метки логической сети автоматически удалит эту сеть со всех сетевых интерфейсов хоста с такой же меткой.

9.4.8. Изменение полного доменного имени хоста

Изменение полного доменного имени (FQDN) хоста

1. Переведите хост в режим обслуживания, при котором выполняется динамическая миграция ВМ на другой хост (см. п. 10.3.12. Перевод хоста в режим обслуживания).
2. Нажмите **Удалить**, а затем нажмите **OK**, чтобы удалить хост с Портала администрирования.
3. Укажите новое имя хоста с помощью утилиты `hostnamectl`:

```
# hostnamectl set-hostname новое_полное_доменное_имя
```

4. Перезагрузите хост.
5. Повторно зарегистрируйте хост в виртуализированном ЦУ.

9.4.9. Поддержка организации сетей с помощью IPv6

В большинстве контекстов система виртуализации ROSA Virtualization поддерживает статические сети IPv6.

Примечание — системе виртуализации ROSA Virtualization необходима включённая поддержка протокола IPv6 на тех компьютерах или ВМ, где работает виртуализированный ЦУ. Не отключайте поддержку IPv6 на этих компьютерах или ВМ, даже если в системе IPv6 не используется.

Ограничения, связанные с IPv6:

- Поддерживается только статическая адресация IPv6. Динамическая адресация с помощью DHCP, а также автоматическая настройка адресов без сохранения состояния не поддерживаются.
- Адресация для двойного стека (IPv4 и IPv6) не поддерживается.
- Сетевые конфигурации OVN могут использовать только IPv4 или IPv6.
- Перевод кластеров с использования IPv4 на использование IPv6 не поддерживается.
- Для IPv6 можно настроить только один шлюз на хост.
- Если две сети разделяют один шлюз (находятся в одной подсети), то можно перенести роль маршрута по умолчанию из сети управления (`ovirtmgmt`) в другую логическую сеть. Хост и виртуализированный ЦУ должны иметь один и

тот же шлюз IPv6. Если хост и виртуализированный ЦУ находятся в разных подсетях, ЦУ может потерять связь с хостом из-за потенциального удаления шлюза IPv6.

- Использование домена хранилищ на базе `glusterfs`, где сервер `gluster` использует адресацию IPv6, не поддерживается.

9.5. Объединение сетевых интерфейсов

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

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

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

Примечание — режим агрегации по умолчанию `(Режим 4) Динамическое агрегирование каналов` требует коммутатора с поддержкой стандарта 802.3ad.

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

На портах коммутатора должна быть включена возможность агрегации.

Создать устройство связки можно одним из следующих способов:

- На Портале администрирования вручную для конкретного хоста.
- Автоматически с помощью службы меток LLDP (см. п. 9.4.7. Добавление сетевых меток сетевым интерфейсам хоста) для не агрегированных сетевых карт всех хостов кластера или дата-центра.

Если в окружении используется хранилище iSCSI и есть необходимость резервирования (избыточности), следуйте инструкциям для настройки механизма доступа iSCSI по нескольким путям (см. п. 11.5.3. Настройка доступа к iSCSI по нескольким путям).

9.5.1. Создание устройства сетевой связки вручную на Портале администрирования

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

Создание устройства связки вручную на Портале администрирования

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

6. Перетащите сетевую карту на другую карту (две сетевые карты формируют новую связку) или в связку (добавление новой сетевой карты в уже существующую связку).

Примечание — если сетевые карты являются несовместимыми, то операция агрегирования будет заблокирована.

7. В выпадающих списках **Имя связки** и **Режим связки** выберите соответствующие пункты.

   При выборе **Пользовательского** режима связки введите параметры связки в текстовое поле (список параметров агрегирования и их описание можно посмотреть по ссылке *Linux Ethernet Bonding Driver HOWTO*).

   Например:

   — Если существующее окружение не сообщает о состоянии каналов с помощью `ethtool`, для настройки наблюдения за протоколом разрешения адресов (ARP) введите: `mode=1 arp_interval=1 arp_ip_target=192.168.0.2`

   — Для назначения сетевой карты с самой высокой пропускной способностью в качестве первичного интерфейса введите: `mode=1 primary=eth0`

8. Нажмите **OK**.
9. Присоедините к новой связке логическую сеть. После чего настройте логическую сеть.

Примечание — логическую сеть невозможно присоединить напрямую к отдельной сетевой карте в связке.

10. При необходимости, если хост находится в режиме обслуживания, выберите пункт **Проверить доступность соединения между хостом и ЦУ**.
11. Нажмите **OK**.

9.5.2. Создание устройства сетевой связки автоматически с помощью службы меток LLDP

Служба меток LLDP даёт возможность автоматического создания устройства сетевой связки с использованием всех несвязанных сетевых плат для всех хостов в одном или более кластерах или в дата-центре.

Создание устройства сетевой связки осуществляется в режиме агрегирования по умолчанию — `(Режим 4) Динамическое агрегирование каналов`.

Сетевые платы с несовместимыми логическими сетями нельзя агрегировать.

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

Предварительные условия:

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

Последовательность действий

1. Настройте параметры `username` и `password` в файле `/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf`:

— `username` - имя пользователя администратора виртуализированного ЦУ. Значение по умолчанию: `admin@internal`.

— `password` - пароль администратора виртуализированного ЦУ. Значение по умолчанию: `123456`.

2. Настройте службу меток LLDP. Для этого обновите следующие значения в файле `etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf`:

— `clusters` - список кластеров (через запятую), на которых должна выполняться служба. Например, `Cluster*` означает, что служба меток будет выполняться в кластерах, название которых начинается со слова `Cluster`. Чтобы служба меток выполнялась во всех кластерах в дата-центре, введите символ `*` (звёздочка). Значение по умолчанию: `Def*`.

— `api_url` - полный URL-адрес API виртуализированного ЦУ. Значение по умолчанию: `https://`*`полное_доменное_имя_ЦУ`*`/ovirt-engine/api`.

— `ca_file` - путь до частного файла сертификата центра сертификации. Если сертификат не используется, оставьте пустое поле. Значение по умолчанию: пустое поле.

— `auto_bonding` – параметр включает возможности службы меток LLDP по созданию сетевых агрегаций. Значение по умолчанию: `true`.

— `auto_labeling` - параметр включает возможности службы меток LLDP по созданию меток. Значение по умолчанию: `true`.

3. При необходимости можно настроить выполнение службы с другими интервалами. Для этого измените значение параметра `OnUnitActiveSec` в файле `etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer`. Значение по умолчанию: `1h` (1 час).

4. Выполните следующую команду для текущего и автоматического (при загрузке) запуска службы:

```
# systemctl enable --now ovirt-lldp-labeler
```

Примечание — для запуска службы `ovirt-lldp-labeler` вручную выполните следующую команду:

```
# /usr/bin/python /usr/share/ovirt-lldp-labeler/ovirt_lldp_labeler_cli.py
```

5. Присоедините к новой связке логическую сеть. После чего настройте логическую сеть.

Примечание — логическую сеть невозможно присоединить напрямую к отдельной сетевой карте в связке.

9.5.3. Режимы агрегирования

Алгоритм рассеивания пакетов определяется режимом агрегирования.

Режим агрегирования по умолчанию — `(Режим 4) динамическое агрегирование каналов`.

Система виртуализации ROSA Virtualization поддерживает следующие режимы агрегирования каналов, которые могут использоваться в сетях виртуальных машин (мостовые сети):

- `(Режим 1) Active-Backup` — активной является только одна сетевая карта. При сбое активной карты её заменяет одна из запасных. Адрес MAC этой связки

виден только на порте сетевого адаптера, что предотвращает путаницу, которая может случиться в случае смены адреса MAC связки, в соответствии с адресом MAC новой активной сетевой карты.

- `(Режим 2) Load Balance (balance-xor)` — сетевая карта, передающая пакеты, выбирается с помощью выполнения операции XOR для исходного и целевого адресов MAC, умноженных на фактор `modulo` общего числа сетевых карт. Этот алгоритм обеспечивает выбор одной и той же сетевой карты для каждого из целевых адресов MAC.
- `(Режим 3) Broadcast` — пакеты передаются на все сетевые карты.
- `(Режим 4) Dynamic Link Aggregation(802.3ad)` — режим агрегирования по умолчанию. Сетевые карты объединяются в группы, разделяющие одни и те же параметры скорости и дуплекса. В активной группе связки используются все сетевые карты.

Физические интерфейсы в связке должны иметь одни и те же идентификаторы агрегатора. В противном случае во вкладке **Сетевые интерфейсы** виртуализированный ЦУ пометит связку значком ! (восклицательный знак), и укажет значение `00:00:00:00:00:00` для параметра связки `ad_partner_mac`.

Для просмотра идентификаторов агрегатора выполните следующую команду:

```
# cat /proc/net/bonding/bond0
```

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

- `(Режим 0) Round-Robin` — сетевые карты передают пакеты в последовательном порядке. Пакеты передаются в петле, которая начинается с первой доступной сетевой платы в связке и заканчивается в последней доступной плате. Последующие петли начинаются с первой доступной сетевой платы.
- `(Режим 5) Balance-TLB (Transmit Load-Balance)` — в зависимости от нагрузки, исходящий трафик распределяется по всем сетевым картам в связке. Входящий трафик получает активная сетевая карта. В случае сбоя карты, получающей трафик, выделяется другая сетевая карта.
- `(Режим 6) Balance-ALB (Adaptive Load-Balance)` — для балансировки входящей нагрузки используется согласование ARP.

Глава 10. Хосты

10.1. Введение в понятие хостов

Хосты, также известные как гипервизоры — это физические серверы, на которых выполняются гипервизоры ROSA Virtualization.

Система виртуализации ROSA Virtualization может поддерживать одновременную работу многих ВМ под управлением ОС Windows или ОС Linux. На машине хоста виртуальные машины выполняются как отдельные процессы и потоки Linux, а управляются эти ВМ удалённо виртуализированным ЦУ. К виртуализированному ЦУ присоединяется один или несколько хостов виртуализации.

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

Обычный хост — это физический 64-битный сервер с модулями Intel® VT или AMD-V под управлением гипервизора ROSA Virtualization.

Физический хост платформы системы виртуализации ROSA Virtualization должен соответствовать следующим техническим характеристикам:

- Хост принадлежит только одному кластеру в системе виртуализации ROSA Virtualization.
- Хост имеет ЦП с поддержкой модулей аппаратной виртуализации AMD-V или Intel® VT.
- Хост имеет процессор с поддержкой всех функций того типа виртуального ЦП, который был выбран при создании кластера, к которому принадлежит данный хост.
- Хост имеет объем ОЗУ — минимум 2 Гбайт.
- Хост обслуживается системным администратором с системными полномочиями.

10.2. Гипервизоры ROSA Virtualization

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

Доступ к веб-интерфейсу Cockpit осуществляется в веб-браузере по адресу `https://`*полное_доменное_имя_хоста_или_IP*`:9090`.

В составе Cockpit также есть панель мониторинга **Виртуализация**, где показывается состояние работоспособности хоста, ключ SSH хоста, статус виртуализированного ЦУ, виртуальные машины и их статистика.

Для сбора информации отладки на хостах виртуализации используется инструмент автоматизированных отчётов об ошибках (`Automatic Bug Reporting Tool`).

10.3. Задачи при работе с хостами

10.3.1. Добавление хостов в виртуализированный ЦУ

Добавление хоста в систему виртуализации ROSA Virtualization может занять некоторое время, по мере выполнения платформой следующих шагов — проверка требований виртуализации, установка пакетов и создание моста.

Примечание — перед добавлением хоста при создании моста управления, использующего статический адрес IPv6, отключите управление `Network Manager` в конфигурационном файле сетевых интерфейсов (`ifcfg`) данного хоста.

Добавление хоста в виртуализированный ЦУ

1. В главном меню Портала администрирования нажмите **Ресурсы → Хосты**.
2. Нажмите **Добавить**.
3. Из выпадающего списка выберите **Дата-центр** и **Кластер хоста** для нового хоста.
4. Укажите **Имя** и **Адрес** нового хоста. В поле **Порт SSH** автоматически добавится стандартный номер порта SSH — 22.
5. Выберите метод аутентификации, используемый диспетчером виртуализации для подключения к хосту:
   - При использовании аутентификации по паролю введите пароль суперпользователя `root`.
   - При использовании аутентификации по открытому ключу SSH скопируйте ключ из поля **Открытый ключ SSH** в файл `/root/.ssh/authorized_keys` хоста.
6. Опционально нажмите на кнопку **Дополнительные параметры**, чтобы настроить следующие дополнительные параметры хоста:
   - Отключить автоматическую настройку межсетевого экрана.
   - Добавить отпечаток SSH хоста для повышения уровня безопасности. Это можно сделать вручную или получить отпечаток автоматически.
7. Опционально настройте управление питанием, если у хоста есть поддерживаемая карта управления питанием.
8. Нажмите **OK**.

Новый хост появится в списке хостов со статусом **Устанавливается**, при этом проследить за процессом установки можно в разделе **События** в **Секции уведомлений** (🔔).

После некоторого ожидания статус хоста сменится на **Запущен**.

10.3.2. Общие параметры хоста

Общие параметры хоста применяются во время изменения сведений о хосте под управлением гипервизора ROSA Virtualization или при добавлении хоста в виртуализированный ЦУ.

В **Табл. 10.1** описываются параметры вкладки **Общие** окон **Новый хост** или **Параметры хоста**.

Табл. 10.1. Общие параметры хоста

Поле	Описание
Кластер хоста	Кластер и дата-центр, к которым принадлежит хост

Поле	Описание
Использовать Foreman/Satellite	Установите или снимите флажок, чтобы соответственно просмотреть или скрыть параметры добавления хостов, поставляемых поставщиком хостов системы Satellite. Также доступны следующие возможности: **Обнаруженные хосты** • **Обнаруженные хосты**: выпадающий список, заполняемый именами хостов Satellite, обнаруженных диспетчером виртуализации. • **Группы хостов**: выпадающий список доступных групп хостов. • **Вычислительные ресурсы**: выпадающий список гипервизоров, предоставляющих вычислительные ресурсы. **Подготовленные хосты** • **Хосты поставщиков**: выпадающий список, заполняемый именами хостов, предоставляемых выбранным внешним поставщиком. Элементы списка фильтруются в соответствии с любыми поисковыми запросами, введёнными в **Поисковом фильтре поставщика.** • **Поисковый фильтр поставщиков**: текстовое поле для поиска хостов, предоставленных выбранным внешним поставщиком. Этот параметр зависит от поставщика (подробности создания поисковых запросов смотрите в документации поставщика). Для просмотра всех хостов оставьте это поле пустым.
Имя	Имя хоста. У этого текстового поля имеется ограничение в 40 символов, а введённое наименование должно быть уникальным сочетанием любых строчных или прописных букв, цифр, дефисов и знаков подчёркивания
Комментарий	Поле для добавления комментария о хосте в простом текстовом формате
Имя хоста	IP-адрес хоста или разрешаемое имя хоста. При использовании разрешаемого имени необходимо обеспечить совпадение разрешаемого имени хоста со всеми IP-адресами (IPv4 и IPv6), используемыми в сети управления хоста
Пароль	Пароль суперпользователя `root`. Пароль можно указать только при добавлении хоста и после этого изменению пароль `root` не подлежит
Открытый ключ SSH	При использовании аутентификации по открытому ключу SSH скопируйте содержимое данного текстового блока в файл `/root/.ssh/authorized_hosts` хоста
Автоматически настроить брандмауэр хоста	При добавлении нового хоста виртуализированный ЦУ может открыть требуемые порты в конфигурации межсетевого экрана данного хоста. Этот **Дополнительный параметр** включён по умолчанию
Отпечаток SSH	Этот **Дополнительный параметр** предоставляет возможность получить отпечаток SSH хоста и сопоставить его с ожидаемым отпечатком, проверив таким образом их соответствие

10.3.3. Параметры управления питанием хоста

В **Табл. 10.2** описываются параметры вкладки **Управление питанием** окон **Новый хост** или **Параметры хоста**.

Табл. 10.2. Параметры управления питанием хоста

Поле	Описание
Включить управление питанием	Включает управление питанием на хосте. Установите флажок для этого параметра для активации остальных полей во вкладке **Управление питанием**
Интеграция kdump	Предотвращает проведение операции блокады на хосте во время выполнения аварийного дампа ядра, чтобы не прерывать дамп
Отключить контроль политики над управлением питанием	Управление питанием контролируется **Политикой планирования** кластера хоста. При включённом управлении питанием и достижении указанного значения низкого потребления виртуализированный ЦУ

Поле	Описание
	выключит машину хоста и запустит её снова из расчёта балансировки нагрузки, или когда в кластере не будет достаточного числа свободных хостов. Установите флажок для этого параметра, чтобы отключить контроль со стороны политики
Агенты в последовательном порядке	Список агентов операции блокады. Агенты операции блокады могут быть последовательными, параллельными или совмещенными. По умолчанию, агенты операции блокады являются последовательными. Если агенты операции блокады используются последовательно, то сначала, для остановки или запуска хоста, используется первичный агент, а в случае его сбоя — вторичный. Если агенты работают параллельно, то на команду остановки хоста должны отреагировать оба агента. При этом, если на команду запуска хоста отреагирует один агент, то хост начнёт работу. Для смены последовательности, в которой используются агенты, используйте кнопки со стрелками ↑ (вверх) и ↓ (вниз). Чтобы сделать двух агентов операции блокады параллельными, выберите одного агента из выпадающего списка **Одновременно с:** рядом с другим агентом. Дополнительных агентов можно добавить в группу параллельно выполняющихся агентов, выбрав группу из выпадающего списка **Одновременно с:** рядом с дополнительным агентом
Добавить агента блокады	Для добавления нового агента блокады нажмите на кнопку со знаком + (плюс). В результате будет открыто окно **Параметры агента блокады** (подробные сведения об этих параметрах приведены в **Табл. 10.3**)
Предпочитаемый прокси для управления питанием	По умолчанию этот **Дополнительный параметр** указывает, что диспетчер виртуализации будет искать прокси операции блокады в рамках того же кластера, в состав которого входит хост, а в случае неудачного поиска — в том же дата-центре

В **Табл. 10.3** содержится описание полей в окне **Параметры агента блокады**.

Табл. 10.3. Параметры агента блокады

Поле	Описание
Адрес	Адрес для доступа к устройству управления питанием хоста. Укажите разрешаемое имя хоста или IP-адрес
Имя пользователя	Учётная запись пользователя, которая будет получать доступ к устройству управления питанием хоста. Для устройства можно создать и настроить специального пользователя, или использовать пользователя по умолчанию
Пароль	Пароль пользователя, получающего доступ к устройству управления питанием хоста
Тип	Выберите тип устройства управления питанием хоста: • **apc** - коммутатор питания по сети серии APC MasterSwitch (нельзя использовать с устройствами серии APC 5.x). • **apc_snmp** - коммутатор питания по сети серии APC 5.x. • **bladecenter** - удалённый супервизор-адаптер IBM Bladecenter. • **cisco_ucs** - Cisco Unified Computing System. • **drac5** - контроллер удалённого доступа Dell для компьютеров Dell. • **drac7** - контроллер удалённого доступа Dell для компьютеров Dell. • **eps** - коммутатор питания по сети ePowerSwitch 8M+. • **hpblade** - HP BladeSystem. • **ilo**, **ilo2**, **ilo3**, **ilo4** - HP Integrated Lights-Out. • **ipmilan** - устройства управления Intelligent Platform Management Interface и Sun Integrated Lights Out Management. • **rsa** - удалённый супервизор-адаптер IBM.

Поле	Описание
	• **rsb** - интерфейс управления Fujitsu-Siemens RSB. • **wti** - коммутатор питания по сети WTI.
Порт	Номер порта, используемого устройством управления питанием для связи с хостом
Слот	Число для идентификации платы устройства управления питанием хоста
Параметры	Параметры конкретного устройства управления питанием хоста указываются в виде «ключ=значение» (доступные параметры приведены в документации конкретного устройства). Примечание — в поле **Параметры** необходимо указать значение `ssl_insecure=1` при выборе типа **cisco_ucs**
Защищённое	Установите флажок для защищённого подключения к хосту с помощью SSH, SSL или других протоколов аутентификации, в зависимости от агента управления питанием хоста

10.3.4. Параметр приоритета SPM

В **Табл. 10.4** описывается параметр вкладки **SPM** окон **Новый хост** или **Параметры хоста**.

Табл. 10.4. Параметр приоритета SPM

Поле	Описание
Приоритет SPM	Определяет вероятность того, что хосту будет присвоена роль SPM (диспетчера пула хранилища). Выберите **Низкий**, **Нормальный**, **Высокий** приоритет или значение **Никогда**. Значение по умолчанию — **Нормальный**. **Низкий** приоритет означает сниженную вероятность присвоения роли SPM, **Высокий** — повышенную. Значение **Никогда** означает, что хосту не будет присвоена роль SPM

10.3.5. Параметры вкладки «Консоль и GPU»

В **Табл. 10.5** описываются параметры вкладки **Консоль и GPU** окон **Новый хост** и **Параметры хоста**.

Табл. 10.5. Параметры вкладки «Консоль и GPU»

Поле	Описание
Переназначить адрес экрана	Установите флажок для этого параметра, чтобы переназначить адрес экрана хоста. Параметр удобен в том случае, когда хосты определяются внутренним IP и находятся за межсетевым экраном NAT. При подключении пользователя к ВМ из-за пределов внутренней сети будет возвращаться открытый IP или FQDN ВМ, который во внешней сети разрешается на открытый IP, вместо частного адреса хоста, на котором выполняется ВМ
Адрес экрана	Указанный адрес экрана будет использоваться для всех ВМ, выполняющихся на этом хосте. Адрес должен указываться в формате FQDN или IP
Размещение vGPU	Выберите тип размещения vGPU: • **Консолидированное** — предпочтительным является запуск как можно большого числа vGPU на доступных физических картах. • **Раздельное** — каждый vGPU размещается на отдельной физической карте.

10.3.6. Параметр вкладки «Поставщик сети»

В **Табл. 10.6** описывается параметр вкладки **Поставщик сети** окон **Новый хост** и **Параметры хоста**.

Табл. 10.6. Параметр вкладки «Поставщик сети»

Поле	Описание
Поставщик внешней сети	В случае наличия поставщика внешней сети и необходимости того, чтобы сеть хоста предоставлялась внешним поставщиком, выберите необходимого поставщика из списка

10.3.7. Параметры ядра

В **Табл. 10.7** описываются параметры вкладки **Ядро** окон **Новый хост** и **Параметры хоста**.

Наиболее часто встречающиеся параметры загрузки ядра приводятся в виде флажков для удобства быстрого выбора.

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

Примечание — перед тем, как вносить изменения в параметры хостов, присоединённых к виртуализированному ЦУ, эти хосты необходимо перевести в режим обслуживания. Затем, для применения внесённых изменений, эти хосты необходимо переустановить.

Табл. 10.7. Параметры ядра

Поле	Описание
Сквозной доступ к устройству хоста и SR-IOV	Включает флаг IOMMU ядра для возможности использования виртуальной машиной устройства хоста, как устройства, напрямую подключённого к ВМ. Аппаратное и программное обеспечение должны поддерживать IOMMU. Для аппаратного обеспечения должны быть включены модули виртуализации и IOMMU. Примечание — в IBM POWER8 функционал IOMMU активирован по умолчанию
Вложенная виртуализация	Активирует флаги `vmx` или `svm` для возможности запуска виртуальных машин внутри виртуальных машин. Параметр предназначается для задач оценки и не поддерживает эксплуатацию системы виртуализации ROSA Virtualization в промышленном режиме. На хосте должна быть установлена ловушка `vdsm-hook-nestedvt`
Небезопасные прерывания	Параметр может быть включён в случаях сбоя сквозного доступа при активированном IOMMU. Обратите внимание, что этот параметр может быть активирован, только если ВМ хоста являются доверенными, так как активный данный параметр потенциально открывает хост для атак MSI со стороны виртуальных машин. Этот параметр рассматривается только как обходное решение при использовании несертифицированного аппаратного обеспечения для задач оценки
Перераспределение PCI	Параметр может быть включён, если сетевая плата с поддержкой SR-IOV не может выделить виртуальный функционал в связи с проблемами памяти. Аппаратное и программное обеспечение хоста должно поддерживать перераспределение PCI.

Поле	Описание
	Этот параметр рассматривается только как обходное решение при использовании несертифицированного аппаратного обеспечения для задач оценки
Занести Nouveau в чёрный список	При использовании драйвера vGPU поставщика установите этот флажок, чтобы избежать конфликтов с драйвером Nouveau
Режим FIPS	Установите флажок для этого параметра, чтобы включить режим FIPS
Синхронная многопоточность (SMT) отключена	Установите флажок для этого параметра, чтобы отключить гиперпоточность
Командная строка ядра	Поле даёт возможность добавить дополнительные параметры ядра к параметрам по умолчанию

Примечание — в случае, если параметры загрузки ядра отображаются серым цветом, нажмите на кнопку **Сбросить**. В результате параметры загрузки ядра станут доступны.

10.3.8. Параметр вкладки «Виртуализированный ЦУ»

В **Табл. 10.8** описывается параметр вкладки **Виртуализированный ЦУ** окон **Новый хост** и **Параметры хоста**.

Табл. 10.8. Параметр вкладки «Виртуализированный ЦУ»

Поле	Описание
Выберите действие по развёртыванию виртуализированного ЦУ	Выберите действие по развёртыванию виртуализированного ЦУ: • **Нет** — никаких действий не требуется. • **Развернуть** — выберите это действие, чтобы развернуть хост в качестве узла виртуализированного ЦУ, или чтобы хост мог запустить виртуализированный ЦУ при выходе из строя основного узла виртуализированного ЦУ. • **Свернуть** — выберите это действие для узла виртуализированного ЦУ, чтобы свернуть установку хоста и удалить все конфигурации, относящиеся к виртуализированному ЦУ.

10.3.9. Настройка параметров управления питанием хоста

Для того, чтобы использовать функционал высокой доступности хоста и высокой доступности ВМ, должно быть настроено управление питанием хоста.

Настройка параметров управления питанием хоста

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

Примечание — если параметр **Интеграция kdump** включается или отключается на хосте, этот хост необходимо переустановить для настройки параметров kdump.

7. Опционально установите флажок **Отключить контроль управления питанием со стороны политики**, если управление питанием хоста не должно контролироваться политикой планирования кластера хоста.
8. Для добавления нового устройства управления питаниям нажмите на кнопку + (плюс).
9. В окне **Параметры агента блокады** укажите **Имя пользователя** и **Пароль** для устройства управления питанием.
10. Выберите **Тип** устройства управления питанием из выпадающего списка.
11. В поле **Адрес** укажите IP-адрес.
12. Укажите номер **Порта SSH**, используемого устройством управления питанием для связи с хостом.
13. Укажите номер **Слота**, используемого для идентификации платы устройства управления питанием.
14. Настройте **Параметры** устройства управления питанием в форме списка записей «ключ=значение», разделённых запятыми.

Примечание — в случае использования как адресов IPv4, так и адресов IPv6 (по умолчанию), оставьте поле **Параметры** пустым. При использовании только адресов IPv4 введите в поле **Параметры** значение `inet4_only=1`. При использовании только адресов IPv6 введите в поле **Параметры** значение `inet6_only=1`.

15. Установите флажок **Защищённое**, чтобы включить защищённое соединение между устройством управления питанием и хостом.
16. Чтобы убедиться в том, что все значения корректны, нажмите **Проверка**. В случае успешной проверки будет показано сообщение — *Проверка выполнена, статус хоста: запущен*.
17. Нажмите **ОК**, чтобы закрыть окно **Параметры агента блокады**.
18. Во вкладке **Управление питанием** при необходимости разверните **Дополнительные параметры**, и с помощью кнопок со стрелками ↑ (вверх) и ↓ (вниз) настройте порядок, в котором виртуализированный ЦУ будет выполнять поиск прокси операции блокады в кластере хоста и в дата-центре.
19. Нажмите **ОК**.

В результате на Портале администрирования появится и станет доступным выпадающее меню **Управление → Управление питанием**.

10.3.10. Настройка параметра приоритета SPM хоста

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

Параметр приоритета SPM хоста изменяет вероятность присвоения роли SPM хосту (например, хосту с высоким приоритетом роль SPM будет присвоена раньше хоста с низким приоритетом).

Настройка параметра приоритета SPM

1. Нажмите **Ресурсы → Хосты**.
2. Нажмите **Изменить**.

3. Перейдите на вкладку **SPM**.
4. Установите флажок в значение **Низкий**, **Нормальный** (по умолчанию), **Высокий** для указания необходимого приоритета SPM хоста, или в значение **Никогда**, чтобы хосту не была присвоена роль SPM.
5. Нажмите **OK**.

10.3.11. Настройка на хосте сквозного доступа к PCI

В данном подразделе описывается как установить и настроить технологию SR-IOV в системе виртуализации ROSA Virtualization.

Включение технологии сквозного доступа даёт возможность виртуальной машине использовать устройство хоста так, как если бы оно было напрямую подключено к ВМ. Чтобы включить функцию сквозного доступа к PCI, необходимо активировать модули виртуализации и функционал IOMMU.

Примечание — аппаратное обеспечение хоста должно соответствовать требованиям применения сквозного доступа к PCI.

Подготовка хоста для применения сквозного доступа к PCI

1. Включите в BIOS модули виртуализации и IOMMU.
2. Включите флаг IOMMU в ядре.

   Для этого установите флажок **Сквозной доступ к устройству хоста и SR-IOV** при добавлении хоста в виртуализированный ЦУ, или вручную отредактируйте конфигурационный файл загрузчика `grub` (см. следующую процедуру ручной активации IOMMU).

Примечание — IOMMU активирован по умолчанию при использовании аппаратного обеспечения IBM POWER8.

В следующей пошаговой инструкции потребуется перезагрузка хоста. Если хост уже был присоединён к виртуализированному ЦУ, обязательно сначала переведите хост в режим обслуживания.

Ручная активация IOMMU

1. Для включения IOMMU отредактируйте конфигурационный файл загрузчика `grub`:
   - Для Intel® добавьте запись `intel_iommu=on` в конец строки `GRUB_CMDLINE_LINUX` в конфигурационном файле `/etc/default/grub`:

     ```
     GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... intel_iommu=on
     ```

   - Для AMD добавьте запись `amd_iommu=on` в конец строки `GRUB_CMDLINE_LINUX` в конфигурационном файле `/etc/default/grub`:

     ```
     GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... amd_iommu=on
     ```

Примечание — вместо записей `intel_iommu=on` или `amd_iommu=on` рекомендуется использовать записи `intel_iommu=pt` или `amd_iommu=pt` соответственно для Intel® или AMD. Параметр `pt` активирует IOMMU только для устройств, используемых в сквозном доступе, что улучшает производительность хоста. Но параметр `pt` может поддерживаться не всеми аппаратными составляющими. Если параметр `pt` не работает на конкретном хосте, используйте исходный параметр `on`.

2. Если сквозной доступ будет неудачным по причине отсутствия поддержки переназначения прерываний аппаратными составляющими, то в случае доверенных ВМ используйте параметр `allow_unsafe_interrupts`. Этот параметр не включается по умолчанию, поскольку его активация потенциально может открыть хост атакам MSI со стороны ВМ. Для активации этого параметра добавьте запись `allow_unsafe_interrupts=1` в строку `options` в конфигурационном файле `/etc/modprobe.d`:

   ```
   options vfio_iommu_type1 allow_unsafe_interrupts=1
   ```

3. Обновите информацию в файле `grub.cfg` и перезагрузите хост для применения изменений:

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

10.3.12. Перевод хоста в режим обслуживания

Многие задачи обслуживания, включая настройку сетевой конфигурации и установку обновлений ПО, требуют перевода хостов в режим обслуживания. Хосты должны переводиться в режим обслуживания до того, как могут произойти события, способные потенциально нарушить корректную работу VDSM, такие как перезагрузка или сбои в работе сети, хранилищ.

При переводе хоста в режим обслуживания, виртуализированный ЦУ попытается выполнить миграцию всех работающих ВМ на альтернативные хосты. При этом будут применятся стандартные предварительные условия динамической миграции. В частности, в кластере должен присутствовать как минимум один хост с ресурсами, достаточными для выполнения мигрирующих ВМ.

Примечание — виртуальные машины, привязанные к хосту и не подлежащие миграции, выключаются. Для проверки, какие машины привязаны к хосту, нажмите кнопку **Привязано к хосту** на вкладке **Виртуальные машины** в подробном просмотре хоста.

Перевод хоста в режим обслуживания

1. Нажмите **Ресурсы → Хосты** и выберите хост.
2. Нажмите **Управление → Обслуживание**. В результате будет открыто окно **Хосты обслуживания** (Рис. 35).
3. Опционально укажите **Причину** перемещения хоста в режим обслуживания, которая будет указана в журнале и при повторной активации хоста из режима обслуживания.

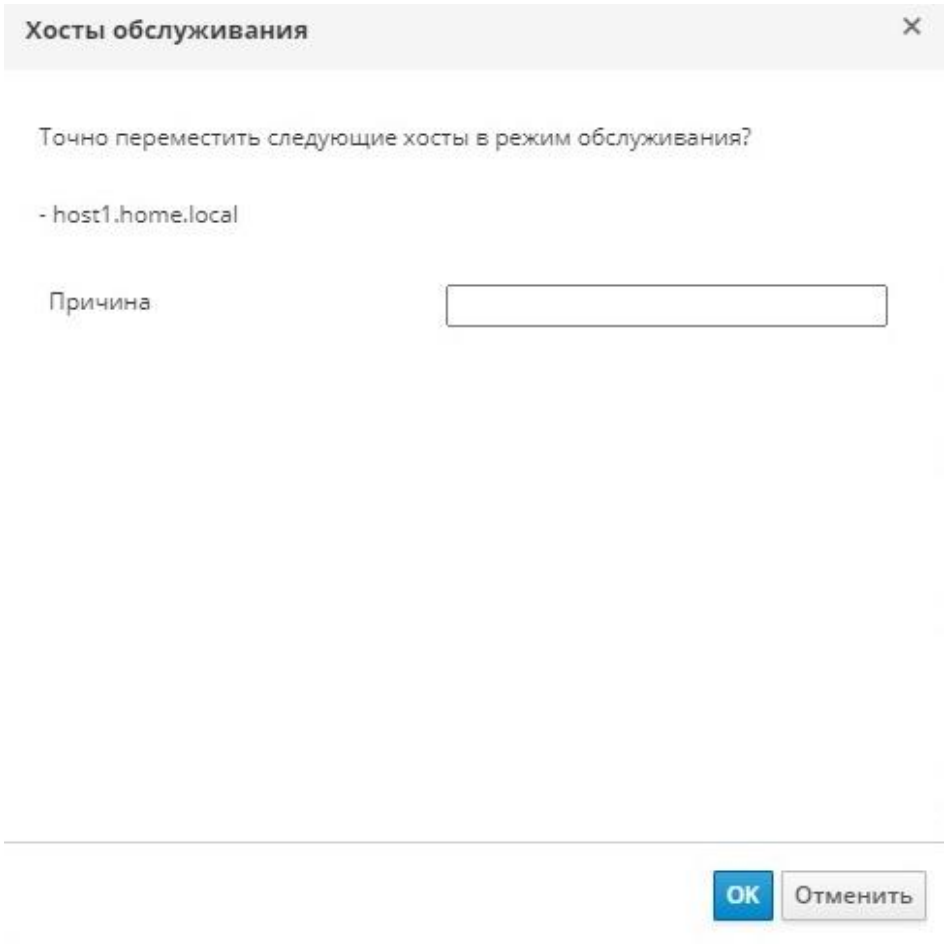

Рис. 35. Перемещение хоста в режим обслуживания

Примечание — поле **Причина** для указания обстоятельств перевода хоста в режим обслуживания появится, только если эта возможность была включена в параметрах кластера (см. п. 8.2.2. Общие параметры кластера).

4. Опционально выберите нужные параметры для хостов с поддержкой Gluster:
   - Выберите параметр **Игнорировать кворум Gluster и проверки самовосстановления** для избежания проверок по умолчанию. По умолчанию во время перевода хоста в режим обслуживания, виртуализированный ЦУ проверяет, не был ли потерян кворум Gluster. Виртуализированный ЦУ также проверяет хост на наличие задач по самовосстановлению, на которые может повлиять перевод хоста в режим обслуживания. Если кворум будет потерян, или если выполняются действия по самовосстановлению, которые не должны быть затронуты, виртуализированный ЦУ не разрешит перевести хост в режим обслуживания. Используйте этот параметр, только если нет никаких других способов перевести хост в режим обслуживания.
   - Выберите параметр **Остановить службу Gluster**, чтобы остановить выполнение всех служб Gluster во время перевода хоста в режим обслуживания.

Примечание — указанные параметры появятся в окне **Хосты обслуживания**, только если выбранный хост поддерживает Gluster.

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

Статус хоста изменится на значение «*Подготовка к обслуживанию*», а после успешного окончания подготовки — на значение «*Обслуживание*». Если хосту была присвоена роль SPM (диспетчер пула хранилища), то роль SPM переходит к другому хосту. Когда хосты находятся в режиме обслуживания, VDSM не прекращает свою работу. Все выполняющиеся ВМ мигрируют на другие хосты.

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

10.3.13. Активация хоста из режима обслуживания

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

Активация хоста из режима обслуживания

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

Статус хоста изменится на значение «*Не присвоено*», а после завершения операции — на значение «*Запущен*». Теперь на хосте могут выполняться виртуальные машины. ВМ, мигрировавшие с хоста при переводе хоста в режим обслуживания, не возвращаются автоматически, но их можно вернуть вручную. Если до перевода в режим обслуживания хост выполнял роль SPM (диспетчер пула хранилища), эта роль не возвращается автоматически к хосту при активации из режима обслуживания.

10.3.14. Настройка правил межсетевого экрана хоста

С помощью утилиты Ansible можно настроить постоянную конфигурацию правил межсетевого экрана хоста.

Примечание — кластер должен быть настроен на работу с `firewalld`, а не с устаревшим типом межсетевого экрана `iptables`.

Настройка правил межсетевого экрана для хостов

1. Для добавления частного порта межсетевого экрана отредактируйте файл `/etc/ovirt-engine/ansible/ovirt-host-deploy-post-tasks.yml.example` на машине диспетчера виртуализации следующим образом:

```
firewalld:
  port: "12345/tcp"
  permanent: yes
  immediate: yes
  state: enabled
```

2. Сохраните файл как `/etc/ovirt-engine/ansible/ovirt-host-deploy-post-tasks.yml`.

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

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

10.3.15. Удаление хоста

Удаление хоста

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

10.3.16. Повторная установка хостов

Для повторной установки хостов виртуализации и стандартных хостов используйте Портал администрирования, и учитывайте следующие предварительные условия:

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

В следующую последовательность действий включаются остановка и перезапуск хостов.

Повторная установка хостов

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

После успешной переустановки хост будет иметь статус «*Запущен*». Все ВМ, мигрировавшие с хоста, теперь смогут вернуться.

Примечание — после успешной регистрации хоста виртуализации в виртуализированном ЦУ и последующей переустановки, этот хост может получить ошибочный статус «*Сбой установки*». В этом случае, нажмите **Управление → Активировать** на Портале администрирования, в результате статус хоста сменится на «*Запущен*», и хост будет готов к работе.

10.3.17. Индивидуализация хостов с помощью меток

Метки можно использовать для хранения информации о хостах, а затем выполнять поиск на основе этих меток.

Индивидуальная настройка хостов с помощью меток

1. Нажмите **Ресурсы → Хосты** и выберите хост.
2. Нажмите **Больше действий** (⋮), затем нажмите **Назначить теги**.
3. Установите флажки для необходимых меток.
4. Нажмите **OK**.

10.3.18. Просмотр статуса работоспособности хоста

В дополнение к обычному **Статусу**, у хостов есть внешний статус работоспособности. Информация о внешнем статусе работоспособности доставляется модулями или внешними системами, или же настраивается администратором.

Внешний статус работоспособности отображается слева от имени хоста в виде следующих значков:

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

Чтобы узнать дополнительные подробности о работоспособности хоста нажмите на имя хоста и перейдите на вкладку **События**.

Примечание — внешний статус работоспособности хоста также можно узнать с помощью REST API (элемент `external_status` в запросе `GET`).

10.3.19. Просмотр устройств хоста

Просмотр устройств хоста

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

Во вкладке **Устройства хоста** приводится подробный список устройств хоста, включая информацию о том, подключено ли устройство к ВМ и используется ли этой ВМ в данный момент. Если на хосте можно настроить прямое присвоение устройств, то эти устройства можно напрямую подключить к ВМ для улучшения производительности.

10.3.20. Доступ к веб-интерфейсу Cockpit с Портала администрирования

По умолчанию Cockpit доступен как на хостах виртуализации, так и на стандартных хостах. Для доступа к веб-интерфейсу используйте браузер, где укажите соответствующий URL в адресной строке, или Портал администрирования.

Доступ к Cockpit с Портала администрирования

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

В результате в новом окне браузера будет открыта страница входа веб-интерфейса Cockpit.

10.4. Отказоустойчивость хостов

10.4.1. Высокая доступность хостов

В системе виртуализации ROSA Virtualization хост со статусом «*Не отвечает*» отличается от хоста со статусом «*В нерабочем состоянии*». Нерабочие хосты могут обмениваться информацией с диспетчером виртуализации, но имеют некорректную конфигурацию (например, отсутствие локальной сети). Не отвечающие хосты не могут поддерживать связь с диспетчером виртуализации.

Для поддержания отзывчивости хостов в кластере, диспетчер виртуализации использует операции блокады (огораживание). Огораживание позволяет кластеру среагировать на неожиданный сбой хоста и принудительно применить доступные политики экономии питания, балансировки нагрузки и доступности ВМ. Параметры операции блокады устройства управления питанием хоста должны быть настроены, и их корректность необходимо время от времени тестировать. Во время операции огораживания не отвечающий хост перезагружается, и если хост не вернётся к активному состоянию в течение указанного времени, то останется не отвечающим в ожидании ручного вмешательства для решения проблемы.

Примечание — для автоматической проверки параметров операции блокады настройте следующие параметры `engine-config` — `PMHealthCheckEnabled` (по умолчанию `false`) и `PMHealthCheckIntervalInSec` (по умолчанию `3600` секунд). При значении `true` параметр `PMHealthCheckEnabled` будет проверять всех агентов хоста согласно временному интервалу, указанному параметром `PMHealthCheckIntervalInSec`, и в случае обнаружения проблемы выдаст предупреждение.

После перезагрузки действия по управлению питанием могут быть выполнены автоматически хостом-прокси или вручную на Портале администрирования. Все ВМ, выполняющиеся на не отвечающих хостах, будут остановлены, а высокодоступные ВМ будут запущены на другом хосте. Для действий по управлению питанием необходимо как минимум два хоста.

Примечание — на хосте, где выполняются высокодоступные ВМ, управление питанием должно быть включено и настроено.

После запуска диспетчера виртуализации и окончания времени молчания (по умолчанию `5` минут), диспетчер виртуализации автоматически попытается огородить не отвечающие хосты, на которых включено управление питанием.

Примечание — время молчания можно настроить с помощью параметра `DisableFenceAtStartupInSec`. Данный параметр `engine-config` помогает предотвратить ситуации, когда диспетчер виртуализации пытается выполнить операцию блокады для загружающихся хостов. Это может случиться после перебоя в работе дата-центра, так как процесс загрузки хоста занимает больше времени, чем процесс загрузки диспетчера виртуализации.

10.4.2. Управление питанием с помощью прокси

Виртуализированный ЦУ не связывается напрямую с агентами операции блокады. Для обмена командами с устройством управления питанием хоста виртуализированный ЦУ использует прокси. Для выполнения действий устройства управления питанием

виртуализированный ЦУ использует VDSM, поэтому другой хост в окружении играет роль прокси для операции блокады.

Хост-прокси имеет статус «*Запущен*» или «*Обслуживание*», и находится в том же кластере или дата-центре, что и огораживаемый хост.

10.4.3. Настройка параметров операции блокады на хосте

Параметры операции блокады настраиваются во вкладке **Управление питанием** окон **Новый хост** или **Параметры хоста**. Управление питанием даёт возможность системе огородить проблемный хост, используя такие дополнительные интерфейсы, как карта удалённого доступа RAC.

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

Настройка параметров операции блокады на хосте

1. Нажмите **Ресурсы → Хосты** и выберите хост.
2. Нажмите **Изменить.**
3. Перейдите на вкладку **Управление питанием** (Рис. 36).
4. Установите флажок **Включить управление питанием**, чтобы активировать поля ввода.
5. Установите флажок **Интеграция Kdump**, чтобы предотвратить огораживание хоста во время выполнения аварийного дампа ядра.

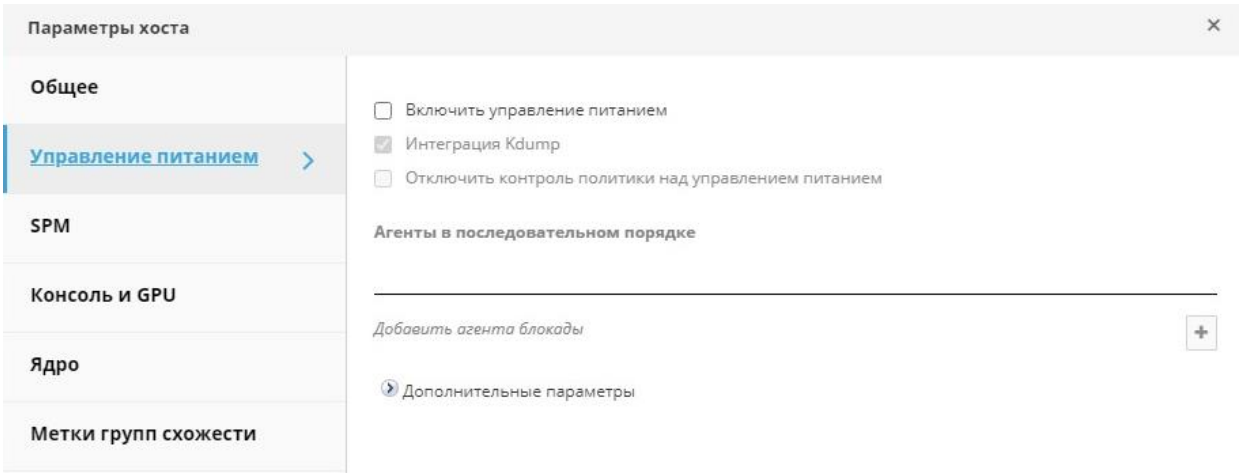

Рис. 36. Управление питанием хоста

Примечание — хост необходимо переустановить каждый раз при изменении (активации или деактивации) параметра **Интеграция Kdump**.

6. Опционально установите флажок **Отключить контроль управления питанием со стороны политик**, если управление питанием хоста не должно контролироваться политикой планирования кластера, в который входит хост.
7. Нажмите на кнопку **+** (плюс), чтобы открыть окно **Параметры агента блокады** для добавления нового устройства управления питанием.
8. Укажите **Адрес**, **Имя пользователя** и **Пароль** для устройства управления питанием.
9. Из выпадающего списка выберите **Тип** устройства управления питанием.
10. Укажите номер **Порта SSH**, используемый устройством управления питанием для связи с хостом.

11. Укажите номер **Слота**, используемого для идентификации платы устройства управления питанием.
12. Настройте **Параметры** устройства управления питанием в форме списка записей «ключ=значение», разделённых запятыми.
13. Установите флажок **Защищённое**, чтобы включить защищённое соединение между устройством управления питанием и хостом.
14. Чтобы убедиться в том, что все значения корректны, нажмите **Проверка**. В случае успешной проверки будет показано сообщение — *Проверка выполнена, статус хоста: запущен*.

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

15. Нажмите **OK** для закрытия окна **Параметры агента блокады**.
16. Опционально во вкладке **Управление питанием** разверните **Дополнительные параметры**, и с помощью кнопок со стрелками ↑ (вверх) и ↓ (вниз) укажите порядок, в котором виртуализированный ЦУ будет вести поиск хоста-прокси для операции блокады в кластере или дата-центре.
17. Нажмите **OK**.

Обратите внимание, что **!** (восклицательный знак) рядом с именем хоста исчез, что означает успешную настройку управления питанием хоста.

10.4.4. Служба Kdump и параметры fence_kdump

Для просмотра статуса службы Kdump нажмите на имя хоста во вкладке **Общие**. Значения статуса службы Kdump:

- **Включено**: Kdump настроен, и служба Kdump выполняется.
- **Отключено**: служба Kdump не выполняется (в этом случае интеграция Kdump не будет работать должным образом).
- **Неизвестно**: данный статус отображается только на хостах с более ранними версиями VDSM, не сообщающими о статусе Kdump.

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

Но существуют случаи, когда бывает необходима продвинутая конфигурация `fence_kdump`. В окружениях с более сложными сетевыми параметрами может понадобиться вручную настроить виртуализированный ЦУ и/или слушатель `fence_kdump`.

Например, если полное доменное имя виртуализированного ЦУ разрешается не на всех хостах с активированной **Интеграцией Kdump**, то настроить правильное имя хоста или адрес IP можно с помощью `engine-config`:

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

Другие примеры случаев, когда также могут понадобиться изменения конфигурации:

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

Частные параметры обнаружения `fence_kdump` рекомендуются для продвинутых пользователей, поскольку внесение изменений в изначальную конфигурацию необходимо только в усложнённых сетевых конфигурациях.

Настройка слушателя fence_kdump

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

Примечание — изменённые значения параметров также должны быть согласованы с параметрами `engine-config`, приведенными в **Табл. 10.10**.

3. Перезапустите слушатель fence_kdump:

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

В **Табл. 10.9** описываются параметры настройки слушателя `fence_kdump`.

Табл. 10.9. Параметры настройки слушателя fence_kdump

Переменная	Описание	Примечание
LISTENER_ADDRESS	IP-адрес, на который будут приходить сообщения fence_kdump. Значение по умолчанию — 0.0.0.0	При изменении значения этот параметр должен соответствовать значению параметра `FenceKdumpDestinationAddress` в `engine-config`
LISTENER_PORT	Указывает порт, на который будут приходить сообщения fence_kdump. Значение по умолчанию — 7410	При изменении значения этот параметр должен соответствовать значению параметра `FenceKdumpDestinationPort` в `engine-config`
HEARTBEAT_INTERVAL	Указывает интервал (в секундах) обновлений периодического сигнала слушателя. Значение по умолчанию — 30	При изменении значения этот параметр должен быть равен (или быть меньше) половинному значению параметра `FenceKdumpListenerTimeout` в `engine-config`
SESSION_SYNC_INTERVAL	Указывает интервал (в секундах) синхронизации сеансов Kdump в памяти хоста слушателя с базой данных. Значение по умолчанию — 5	При изменении значения этот параметр должен быть равен (или быть меньше) половинному значению параметра `KdumpStartedTimeout` в `engine-config`
REOPEN_DB_CONNECTION_INTERVAL	Указывает интервал (в секундах) для повторного открытия соединения к базе данных,	

Переменная	Описание	Примечание
	которая ранее была недоступна. Значение по умолчанию — 30	
KDUMP_FINISHED_TIMEOUT	Определяет максимальный период ожидания (в секундах) после последнего полученного сообщения от хостов, на которых выполняется Kdump. По истечению этого периода поток Kdump хоста будет помечен как ЗАВЕРШЕНО. Значение по умолчанию — 60	При изменении значения этот параметр должен быть равен (или быть больше) двойному значению параметра `FenceKdumpMessageInterval` в `engine-config`

Настройка Kdump с помощью engine-config

Для просмотра текущих параметров Kdump выполните следующую команду:

```
# engine-config -g ПАРАМЕТР
```

1. Отредактируйте конфигурацию Kdump, согласно синтаксису *ПАРАМЕТР=значение*:

   ```
   # engine-config -s ПАРАМЕТР=значение
   ```

Примечание — изменённые значения параметров также должны быть согласованы с параметрами настройки слушателя `fence_kdump`, приведенными в **Табл. 10.9**.

2. Перезапустите службу `ovirt-engine`:

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

3. Переустановите все хосты, а также при необходимости активируйте параметр **Интеграция Kdump** (см. **Табл. 10.10**).

В **Табл. 10.10** описываются параметры конфигурации Kdump.

Табл. 10.10. Параметры конфигурации Kdump

Переменная	Описание	Примечание
FenceKdumpDestinationAddress	Имена хостов или IP-адреса, на которые будут посылаться сообщения fence_kdump. Значение по умолчанию — пустая строка (используется FQDN диспетчера виртуализации)	При изменении значения этот параметр должен соответствовать значению параметра `LISTENER_ADDRESS` в конфигурации слушателя fence_kdump, а все хосты с включённой **Интеграцией Kdump** должны быть переустановлены
FenceKdumpDestinationPort	Указывает порт, на который необходимо посылать сообщения fence_kdump. Значение по умолчанию — 7410	При изменении значения этот параметр должен соответствовать значению параметра `LISTENER_PORT` в конфигурации слушателя fence_kdump, а все хосты с включённой **Интеграцией Kdump** должны быть переустановлены
FenceKdumpMessageInterval	Указывает временной интервал (в секундах) между сообщениями, посылаемыми fence_kdump. Значение по умолчанию — 5	При изменении значения этот параметр должен быть равен (или быть меньше) половинному значению параметра `KDUMP_FINISHED_TIMEOUT` в файле конфигурации слушателя fence_kdump, а все хосты с

Переменная	Описание	Примечание
		включённой **Интеграцией Kdump** должны быть переустановлены
FenceKdumpListenerTimeout	Определяет максимальный период ожидания (в секундах) после последнего периодического сигнала, в течение которого слушатель fence_kdump ещё считается работающим. Значение по умолчанию — 90	При изменении значения этот параметр должен быть равен (или быть больше) половинному значению параметра `HEARTBEAT_INTERVAL` в файле конфигурации слушателя fence_kdump
KdumpStartedTimeout	Определяет максимальный период ожидания (в секундах) до первого получения сообщения от хоста, выполняющего kdump (для определения того, что процедуры kdump начали выполняться). Значение по умолчанию — 30	При изменении значения этот параметр должен быть равен (или быть больше) двойному значению параметра `SESSION_SYNC_INTERVAL` в файле конфигурации слушателя fence_kdump и параметра `FenceKdumpMessageInterval`

10.4.5. Мягкая блокада хостов

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

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

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

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

если было настроено управление питанием, выполнение операции блокады передаётся внешнему агенту.

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

10.4.6. Использование возможностей хоста по управлению питанием

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

Использование возможностей хоста по управлению питанием

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

Примечание — если управление питанием не включено, для перезапуска или остановки работы хоста сначала выберите необходимый хост, затем из выпадающего меню **Управление** выберите один из следующих пунктов: **Управление SSH**, **Перезапустить** или **Остановить**.

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

10.4.7. Ручное изолирование не отвечающего хоста

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

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

Ручное изолирование не отвечающего хоста

1. Нажмите **Ресурсы → Хосты** и убедитесь в том, что хост действительно имеет статус «*Не отвечает*».
2. Перезагрузите хост вручную (например, осуществите физическое взаимодействие с аппаратурой непосредственно в серверной).
3. Выберите хост, нажмите **Больше действий** (⋮) и далее **Подтвердить, что хост был перезагружен**.
4. Установите флажок **Одобрить действие** и нажмите **OK**.
5. Если перезагрузка хоста занимает много времени, настройте параметр `ServerRebootTimeout` и укажите сколько секунд должно длиться ожидание перед тем, как хост получит статус «*Не отвечает*»:

```
# engine-config --set ServerRebootTimeout=целое_число
```

Глава 11. Хранилища

Система виртуализации ROSA Virtualization использует централизованную систему хранилищ для виртуальных дисков, файлов ISO и снимков.

В обязанности администратора входит создание, настройка, присоединение и поддержка хранилищ. Дополнительно администратору необходимо иметь представление о типах хранилищ и случаях их использования.

Сеть хранения в системе виртуализации ROSA Virtualization может быть реализована следующими средствами:

- Сетевая файловая система NFS.
- Экспорт GlusterFS.
- Любые POSIX-совместимые ФС.
- Интерфейс iSCSI.
- Локальные хранилища, присоединённые непосредственно к хостам виртуализации.
- Протокол Fibre Channel (FCP).
- Параллельный доступ pNFS.

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

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

В системе виртуализации ROSA Virtualization используются следующие типы доменов хранилищ:

- **Домен данных.**
  В доменах данных хранятся виртуальные жёсткие диски и файлы OVF всех ВМ и шаблонов в дата-центре. Кроме того, в доменах данных хранятся снимки ВМ. Домены данных не могут быть общими для разных дата-центров. Домены данных нескольких различных типов (iSCSI, NFS, FC, POSIX и Gluster) могут быть добавлены в один дата-центр при условии, что они являются разделяемыми, а не локальными. Домен данных необходимо присоединить к дата-центру, перед тем как присоединять к дата-центру домены других типов.
- **Домен ISO.**
  В доменах ISO хранятся файлы образов ISO (или логические носители CD), используемые для установки и загрузки операционных систем и приложений виртуальных машин. Наличие домена ISO отменяет необходимость физических носителей для дата-центров. Домен ISO может быть общим для разных дата-центров. Домены ISO могут создаваться только на базе файловой системы NFS. К дата-центру может быть присоединён только один домен ISO.

Примечание — домены ISO являются устаревшими, поэтому для хранения образов ISO рекомендуется использовать домен данных, созданный на базе файловой системы NFS.

- **Домен экспорта.**

Домены экспорта — это временные репозитории хранения, используемые для копирования и перемещения образов между дата-центрами и окружениями виртуализации ROSA Virtualization. Домен экспорта можно использовать для создания резервных копий ВМ. Домен экспорта можно перемещать между дата-центрами, при этом домен экспорта может быть активным одновременно только в одном из дата-центров. Домены экспорта можно создавать только на базе файловой системы NFS. К дата-центру может быть присоединён только один домен экспорта.

Примечание — домены хранилищ экспорта являются устаревшими. Домены хранилищ данных можно отсоединить от дата-центра и импортировать в другие дата-центры в том же или в другом окружении. После чего, виртуальные машины, «плавающие» виртуальные диски и шаблоны можно загрузить из домена хранения в прикреплённый дата-центр. Подробные сведения об импорте доменов хранилищ см. п. 11.7.2. Импорт доменов хранилищ.

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

11.1. Домен хранилища

Домен хранилища — это собрание образов, имеющих общий интерфейс хранения. Домен хранилища содержит полные образы шаблонов и ВМ (включая снимки), или файлов ISO.

Домен хранилища может быть создан на базе блочных устройств (iSCSI или FCP) или файловых систем (NFS, GlusterFS, или других POSIX-совместимых ФС).

Если домен хранилища создан на базе блочных устройств, то каждый виртуальный диск, шаблон или снимок являются логическими томами. Блочные устройства собираются в логическую сущность, называемую «группой томов», а затем разделяются диспетчером логических томов LVM (Logical Volume Manager) на логические тома для их использования в качестве виртуальных жёстких дисков.

В файловых системах все виртуальные диски, шаблоны и снимки являются файлами.

Виртуальные диски могут иметь два формата — QCOW2 или raw. Тип хранилища может быть разреженный (тонкое резервирование) или предварительно зарезервированный. Снимки всегда имеют разреженный тип, но могут быть сделаны для виртуальных дисков любого из вышеперечисленных форматов.

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

11.2. Подготовка и добавление хранилища NFS

11.2.1. Подготовка хранилища NFS

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

Для того, чтобы виртуализированный ЦУ мог хранить данные в доменах хранилищ, представленных экспортированными каталогами, необходимы специальные системные учётные записи пользователей и системные группы пользователей.

В следующей последовательности действий описывается настройка прав доступа для каталога */exports/data*. Шаги с использованием команд `chown` и `chmod` необходимо повторить для каждого каталога, который планируется использовать в качестве домена хранилищ в системе виртуализации ROSA Virtualization.

Последовательность действий

1. Создайте группу `kvm`:

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

2. Создайте пользователя `vdsm` в группе `kvm`:

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

3. Укажите значение 36:36 для изменения владельцев каталога */exports/data* на `vdsm:kvm`:

   ```
   # chown -R 36:36 /exports/data
   ```

4. Измените режим доступа к каталогу */exports/data* так, чтобы владелец имел доступ на чтение и запись, а группа и другие пользователи имели доступ на чтение и выполнение:

   ```
   # chmod 0755 /exports/data
   ```

11.2.2. Добавление хранилища NFS

В следующей последовательности действий описывается как присоединить существующее хранилище NFS к окружению виртуализации ROSA Virtualization в качестве домена данных.

Последовательность действий

1. На Портале администрирования выберите **Хранилище → Домены**.
2. Нажмите **Добавить домен**.
3. В окне **Новый домен** укажите **Имя** домена хранилища (Рис. 37).
4. Примите значения по умолчанию для списков **Дата-центр**, **Функции домена**, **Тип хранилища**, **Формат** и **Хост**.
5. Введите **Путь экспорта**, используемый для домена хранилища. Путь должен иметь формат *123.123.0.10:/data* (для IPv4), *[2001:0:0:0:0:0:0:5db1]:/data* (для IPv6) или *domain.example.com:/data*.
6. При необходимости нажмите **Дополнительные параметры** для настройки следующих значений:
   a. В поле **Индикатор предупреждения о недостатке места (%)** укажите значение в процентах. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупреждающее сообщение, а событие будет занесено в журнал.
   b. В поле **Блокатор при отсутствии места (ГБ)** введите значение в Гбайт. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого значения, пользователю будет показано сообщение об ошибке, событие

будет занесено в журнал, а любое новое действие (даже временное), которому необходимо дисковое пространство, будет заблокировано.

c. Установите флажок **Забить нулями после удаления**. Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя.

7. Нажмите **OK**.

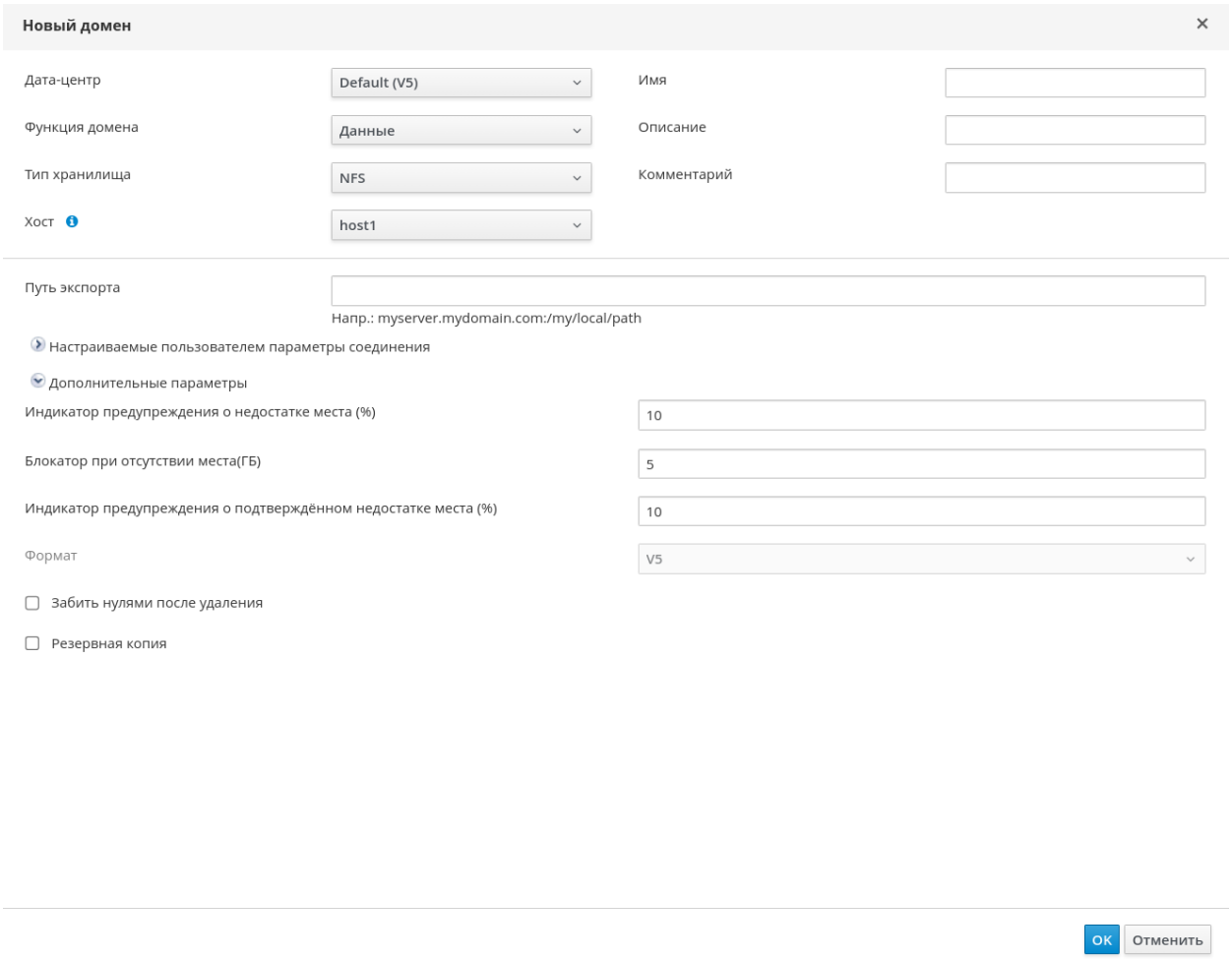

Рис. 37. Добавление хранилища NFS

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

Примечание — при необходимости использовать домен экспорта или домен ISO выполните вышеперечисленные действия, но в списке **Функция домена** выберите значение **Экспорт** или **ISO**.

11.2.3. Увеличение объёма хранилища NFS

Для увеличения объёма хранилища NFS можно либо создать новый домен хранилища и добавить его в существующий дата-центр, либо увеличить доступный объём на сервере NFS.

Увеличение существующего домена хранилища NFS

1. Нажмите **Хранилище → Домены**.
2. Нажмите на название существующего домена NFS, чтобы перейти к подробному просмотру.

3. Перейдите на вкладку **Дата-центр** и нажмите **Обслуживание**, чтобы перевести домен хранилища в режим обслуживания. Это действие размонтирует существующий общий ресурс и даст возможность изменить размер домена хранилища.
4. Измените размер хранилища на сервере NFS до необходимого объёма.
5. В подробном просмотре перейдите на вкладку **Дата-центр** и нажмите **Активировать** для того, чтобы смонтировать домен хранилища.

11.3. Подготовка и добавление локального хранилища

11.3.1. Подготовка локального хранилища

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

Примечание — на хостах виртуализации локальные хранилища всегда должны настраиваться на файловой системе, отделённой от корневого раздела `/`. Для предотвращения потенциальных потерь данных во время обновления версий ПО рекомендуется использовать отдельный логический том.

Подготовка локального хранилища на стандартных хостах

1. Создайте каталог (например */data/images*), который будет использоваться как локальное хранилище:

```
# mkdir -p /data/images
```

2. Измените владельцев каталога */data/images* на пользователя `vdsm` и группу `kvm`, и установите права на чтение и запись в каталоге */data/images* для владельца:

```
# chown 36:36 /data /data/images
# chmod 0755 /data /data/images
```

Подготовка локального хранилища на хостах виртуализации

Рекомендуется создать локальное хранилище на логическом томе следующим образом:

1. Создайте каталог локального хранилища:

```
# mkdir /data
# lvcreate -L $SIZE rhvh -n data
# mkfs.ext4 /dev/mapper/rhvh-data
# echo "/dev/mapper/rhvh-data /data ext4 defaults,discard 1 2" >>
/etc/fstab
# mount /data
```

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

```
# mount -a
# chown 36:36 /data /rhvh-data
# chmod 0755 /data /rhvh-data
```

11.3.2. Добавление локального хранилища

Добавление локального хранилища помещает хост в новый дата-центр и кластер.

В следующей последовательности действий соединено в окне параметров локального хранилища создание дата-центра, кластера и хранилища.

Последовательность действий

1. Нажмите **Ресурсы → Хосты** и выберите хост.
2. Нажмите **Управление → Обслуживание** и далее нажмите **OK**.
3. Нажмите **Управление → Настроить**.
4. Нажмите на кнопки **Изменить** рядом с полями **Дата-центр**, **Кластер** и **Хранилище**, чтобы настроить домен локального хранилища.
5. В текстовом поле укажите путь до локального хранилища.
6. При необходимости перейдите на вкладку **Оптимизация**, чтобы настроить политику оптимизации памяти для нового кластера локального хранилища.
7. Нажмите **OK**.

В результате хост присоединится к сети в собственном дата-центре.

11.4. Управление хранилищами на базе файловой системы, совместимой с POSIX

11.4.1. Подготовка хранилища на базе файловой системы, совместимой с POSIX

Поддержка файловой системы стандарта POSIX даёт возможность монтировать файловые системы с теми же самыми параметрами монтирования, которые обычно применяются при ручном монтировании из командной строки.

Любая файловая система, совместимая с POSIX и используемая в качестве домена хранилища в системе виртуализации ROSA Virtualization, должна быть кластерной, а также должна поддерживать разреженные файлы и прямой ввод-вывод. Например, файловая система CIFS (Common Internet File System) не поддерживает механизм прямого ввода-вывода, что делает CIFS несовместимой с системой виртуализации ROSA Virtualization.

Примечание — *не монтируйте* хранилище NFS, создавая домен хранилища на базе ФС, совместимой с POSIX. Всегда создавайте для этого домен хранилища NFS.

11.4.2. Добавление хранилища на базе файловой системы, совместимой с POSIX

В следующей последовательности действий описывается как присоединить к системе виртуализации ROSA Virtualization в качестве домена данных существующее хранилище на базе ФС, совместимой с POSIX.

Последовательность действий

1. Нажмите **Хранилище → Домены**.
2. Нажмите **Добавить домен**.
3. В окне **Новый домен** укажите **Имя** для домена хранилища (Рис. 38).
4. Выберите **Дата-центр**, связанный с доменом хранилища (выбранный дата-центр должен иметь тип POSIX), или при отсутствии такого дата-центра выберите **Нет**.
5. Из выпадающего списка **Функция домена** выберите **`Данные`**, а из списка **Тип хранилища** выберите **`POSIX-совместимая ФС`**.

6. Из выпадающего списка выберите **Хост**.
7. Укажите **Путь** до POSIX-совместимой ФС в формате команды `mount`.
8. Укажите **Тип VFS** в формате команды `mount` с аргументом `-t`.
9. Укажите дополнительные **Параметры монтирования** в формате команды `mount` с аргументом `-o`. Параметры монтирования должны указываться в виде списка, разделённого запятыми.
10. При необходимости нажмите **Дополнительные параметры** для настройки следующих значений:
    a. В поле **Индикатор предупреждения о недостатке места (%)** укажите значение в процентах. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупреждающее сообщение, а событие будет занесено в журнал.
    b. В поле **Блокатор при отсутствии места (ГБ)** введите значение в Гбайт. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого значения, пользователю будет показано сообщение об ошибке, событие будет занесено в журнал, а любое новое действие (даже временное), которому необходимо дисковое пространство, будет заблокировано.
    c. Установите флажок **Забить нулями после удаления**. Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя.
11. Нажмите **OK**.

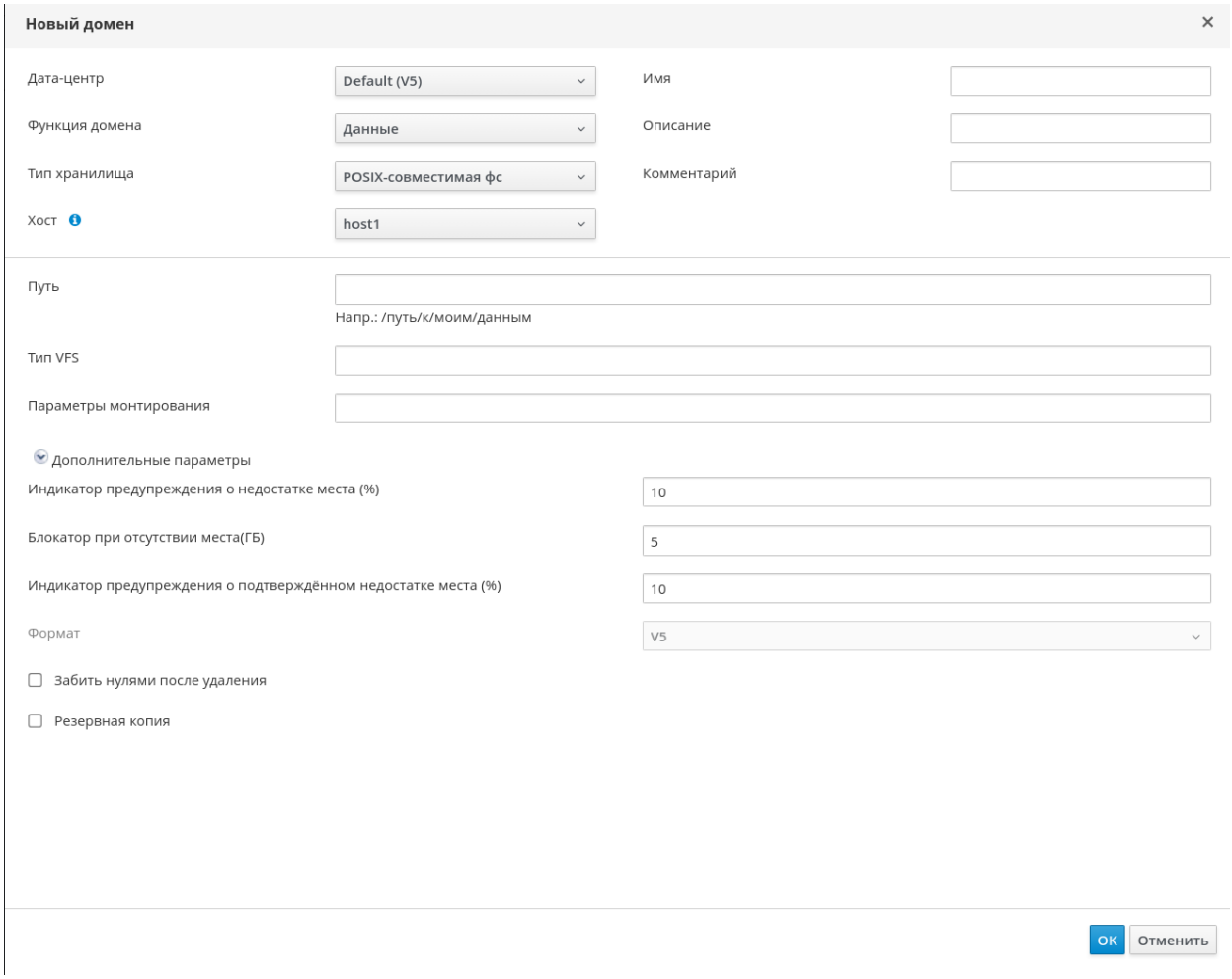

Рис. 38. Добавление хранилища POSIX

11.5. Подготовка и добавление блочного хранилища

11.5.1. Подготовка хранилища iSCSI

Система виртуализации ROSA Virtualization поддерживает хранилища iSCSI.

Хранилище iSCSI представляет собой домен хранилища из группы томов на базе LUN. Группы томов и номера LUN нельзя присоединить более чем к одному домену хранилища одновременно.

Примечания:

- При использовании блочного хранилища и планировании размещения ВМ на устройствах raw или прямых LUN под управлением диспетчера логических томов необходимо создать фильтр для скрытия гостевых логических томов. Это предотвратит активацию гостевых томов при загрузке хоста, что потенциально может привести к повреждению данных.
- Система виртуализации ROSA Virtualization на данный момент не поддерживает хранилища с размером блоков в 4Кбайт. Блочные хранилища необходимо настраивать в старом режиме (512 байт на блок).
- В ситуации, когда хост загружается из хранилища SAN и впоследствии теряет связь с хранилищем, файловые системы хранилища становятся доступны только для чтения и остаются в этом состоянии после восстановления связи. Для предотвращения этой ситуации рекомендуется добавить в корневую ФС SAN замещающий конфигурационный файл доступа по нескольким путям к

загрузочным LUN, чтобы обеспечить постановку их в очередь при наличии соединения:

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

11.5.2. Добавление хранилища iSCSI

В следующей последовательности действий описывается как присоединить к системе виртуализации ROSA Virtualization в качестве домена данных существующее хранилище iSCSI.

Последовательность действий

1. Нажмите **Хранилище → Домены.**
2. Нажмите **Добавить домен**.
3. В окне **Новый домен** укажите **Имя** домена хранилища (Рис. 39).

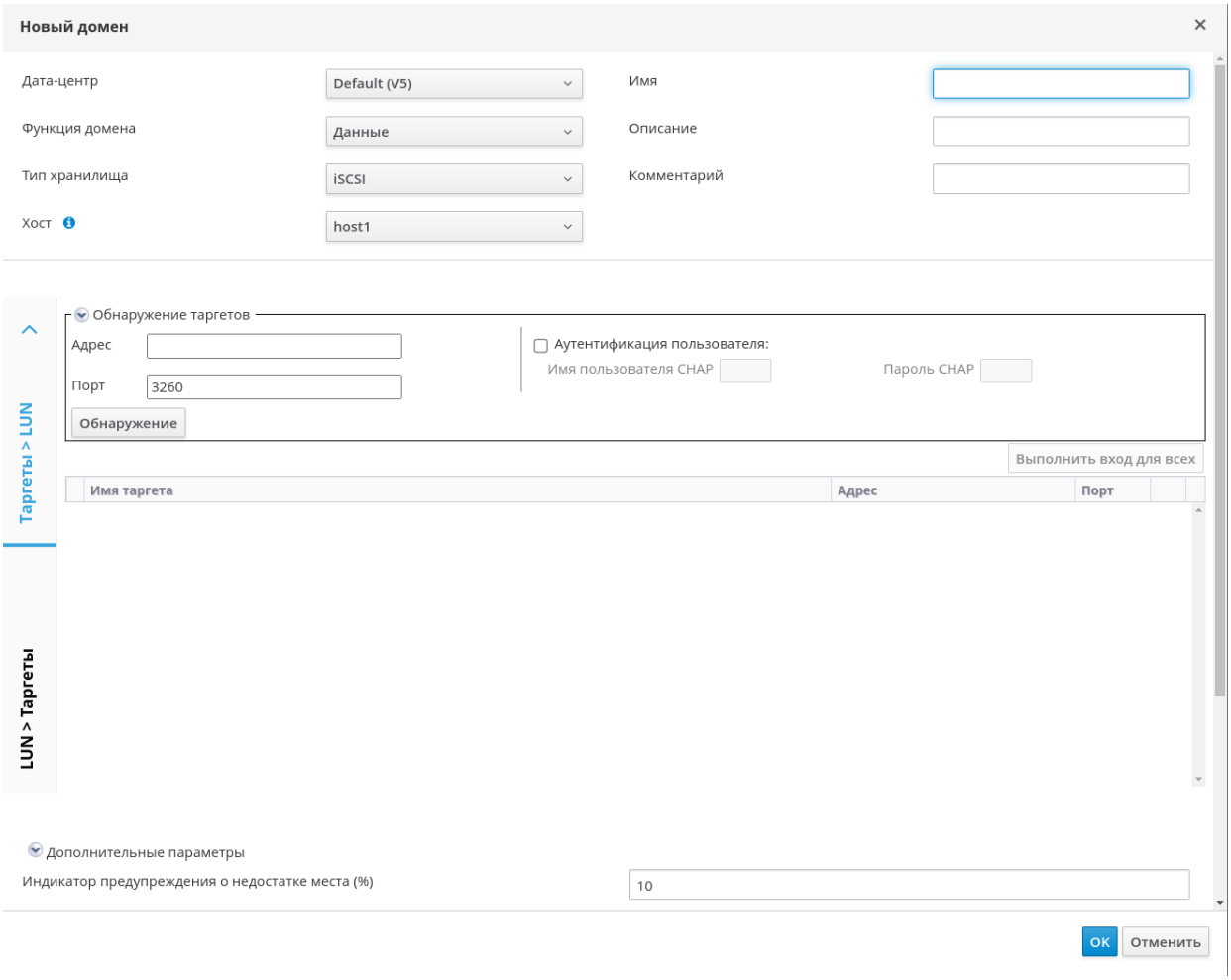

Рис. 39. Добавление хранилища iSCSI

4. Выберите **Дата-центр**.
5. В качестве **Функции** домена выберите **Данные**, а в качестве **Типа хранилища** выберите **iSCSI**.
6. Из выпадающего списка **Хост** выберите активный хост.

Примечание — подключение к домену хранилища идёт от выбранного хоста, а не напрямую из виртуализированного ЦУ, поэтому у всех хостов должен быть доступ к устройству хранения, до того как будет настроен домен хранилища.

7. Виртуализированный ЦУ может отобразить цели iSCSI на номера LUN или номера LUN на цели iSCSI. В окне **Новый домен** при выборе типа хранилища **iSCSI** автоматически отображаются известные цели с неиспользуемыми LUN. Опционально, если отсутствует цель, используемая для добавления хранилища, выполните следующие действия по обнаружению целей:
   a. Для активации возможности обнаружения целей нажмите **Обнаружить цели**. В результате в окне **Новый домен** автоматически будут показаны цели с неиспользуемыми в окружении LUN, а также будут показаны LUN, используемые вне окружения. Параметр **Обнаружить цели** можно использовать для добавления LUN ко многим целям или нескольких путей к одним и тем же LUN.
   b. В поле **Адрес** введите полное доменное имя или IP-адрес хоста iSCSI.
   c. В поле **Порт** укажите номер порта, к которому будет подключаться хост при просмотре целей. Значение по умолчанию — `3260`.
   d. Если для защиты хранилища используется CHAP, установите флажок **Аутентификация пользователей** и далее введите **Имя пользователя CHAP** и **Пароль CHAP**.

Примечание — настроить учётные записи цели iSCSI для конкретного хоста можно с помощью REST API.

   e. Нажмите **Обнаружить**.
   f. Выберите одну или несколько целей из списка с результатами обнаружения.
   g. Нажмите **Вход в систему** при выборе одной цели или нажмите **Выполнить вход для всех** при выборе нескольких целей.

Примечание — если для доступа требуется более одного пути, необходимо обнаружить и выполнить вход на цели с использованием всех путей. Изменение домена хранилища для добавления дополнительных путей на данный момент не поддерживается.

8. Нажмите на кнопку + (плюс) рядом с необходимой целью. Элемент раскроется и будут показаны все неиспользуемые LUN, присоединённые к цели.
9. Установите флажок для каждого LUN, используемого для создания домена хранилища.
10. При необходимости нажмите **Дополнительные параметры** для настройки следующих значений:
    a. В поле **Индикатор предупреждения о недостатке места (%)** укажите значение в процентах. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупреждающее сообщение, а событие будет занесено в журнал.
    b. В поле **Блокатор при отсутствии места (ГБ)** введите значение в Гбайт. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого значения, пользователю будет показано сообщение об ошибке, событие будет занесено в журнал, а любое новое действие (даже

временное), которому необходимо дисковое пространство, будет заблокировано.

c. Установите флажок **Забить нулями после удаления**. Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя.

11. Нажмите **OK**.

Если к одной цели было настроено несколько соединений из хранилищ, то для завершения создания связки iSCSI следуйте инструкции, приведенной в п. 11.5.3. Настройка доступа к iSCSI по нескольким путям.

В случае, если текущая сеть хранилища должна мигрировать в связку iSCSI, см. п. 11.7.4. Миграция доменов хранилищ между дата-центрами в разных окружениях.

11.5.3. Настройка доступа к iSCSI по нескольким путям

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

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

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

Предварительным условием для настройки доступа к iSCSI по нескольким путям является наличие одной или нескольких целей iSCSI (см. п. 11.5.2. Добавление хранилища iSCSI), а также одной или нескольких логических сетей (см. п. 9.1.2. Создание новой логической сети в дата-центре или кластере), отвечающих следующим требованиям:

- Логическая сеть не является требуемой сетью или сетью виртуальной машины.
- Логическая сеть присвоена интерфейсу хоста (см. п. 9.4.2. Изменение параметров сетевых интерфейсов и присвоение хостам логических сетей).
- Логической сети присвоен статический IP-адрес в той же VLAN и подсети, в которой размещаются другие логические сети в связке iSCSI (см. п. 9.4.2. Изменение параметров сетевых интерфейсов и присвоение хостам логических сетей).

Настройка доступа к iSCSI по нескольким путям

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

В результате хосты в дата-центре будут подключены к целям iSCSI с помощью логических сетей в связке iSCSI.

11.5.4. Миграция логической сети в связку iSCSI

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

Миграция логической сети в связку iSCSI

1. Измените текущую логическую сеть так, чтобы она не была **Требуемой**:
   a. Нажмите **Ресурсы → Кластеры**.
   b. Нажмите на название кластера, чтобы перейти к подробному просмотру.
   c. Во вкладке **Логические сети** выберите текущую логическую сеть (например, `net-1`) и нажмите **Управление сетями**.
   d. Снимите флажок **Требуется** и нажмите **OK**.
2. Создайте новую логическую сеть, не являющуюся **Требуемой** и не являющуюся **Сетью ВМ**:
   a. Нажмите **Добавить сеть**, чтобы открыть окно **Новая логическая сеть**.
   b. Во вкладке **Общие** введите **Имя** (например, `net-2`) и снимите флажок **Сеть ВМ**.
   c. Во вкладке **Кластер** снимите флажок **Требовать** и нажмите **OK**.
3. Удалите текущую сетевую связку и заново присвойте логические сети:
   a. Нажмите **Ресурсы → Хосты**.
   b. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
   c. Во вкладке **Сетевые интерфейсы** нажмите **Настроить сети хоста**.
   d. Перетащите сеть `net-1` вправо, чтобы заново присвоить эту сеть.
   e. Перетащите текущую связку вправо для удаления.
   f. Перетащите сети `net-1` и `net-2` влево, чтобы присвоить эти сети физическим интерфейсам.
   g. Нажмите на значок карандаша рядом с сетью `net-2`, чтобы открыть окно **Свойства сети**.
   h. Во вкладке **IPV4** выберите **Статический**.
   i. Укажите **IP** и **Сетевую маску/префикс маршрутизации** подсети и нажмите **OK**.
4. Создайте связку **iSCSI**:
   a. Нажмите **Ресурсы → Дата-центры**.
   b. Нажмите на имя дата-центра, чтобы перейти к подробному просмотру.
   c. Во вкладке **Доступ к iSCSI по нескольким путям** нажмите **Добавить**.
   d. В окне **Добавить связку iSCSI** укажите **Имя**, выберите сети `net-1` и `net-2`, и нажмите **OK**.

В результате в дата-центре теперь будет связка iSCSI, включающая в себя и старую (`net-1`), и новую (`net-2`) логические сети.

11.5.5. Подготовка хранилища FCP

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

Администраторы системы виртуализации ROSA Virtualization должны иметь практические знания о теории и принципах работы сетей хранения данных SAN. Как

правило, для переноса трафика между хостом и общим внешним хранилищем SAN используется протокол FCP. В связи с этим, SAN иногда называют *хранилищем FCP*.

Примечания:

- При использовании блочного хранилища и планировании размещения ВМ на устройствах raw или прямых LUN под управлением диспетчера логических томов необходимо создать фильтр для скрытия гостевых логических томов. Это предотвратит активацию гостевых томов при загрузке хоста, что потенциально может привести к повреждению данных.
- Система виртуализации ROSA Virtualization на данный момент не поддерживает хранилища с размером блоков в 4Кбайт. Блочные хранилища необходимо настраивать в старом режиме (512 байт на блок).
- В ситуации, когда хост загружается из хранилища SAN и впоследствии теряет связь с хранилищем, файловые системы хранилища становятся доступны только для чтения и остаются в этом состоянии после восстановления связи. Для предотвращения этой ситуации рекомендуется добавить в корневую ФС SAN замещающий конфигурационный файл доступа по нескольким путям к загрузочным LUN, чтобы обеспечить постановку их в очередь при наличии соединения:

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

11.5.6. Добавление хранилища FCP

В следующей последовательности действий описывается как присоединить к системе виртуализации ROSA Virtualization в качестве домена данных существующее хранилище FCP.

Последовательность действий

1. Нажмите **Хранилище → Домены**.
2. Нажмите **Добавить домен**.
3. Укажите **Имя** домена хранилища.
4. Из выпадающего списка выберите **Дата-центр** FCP, или при отсутствии такого дата-центра выберите **Нет**.
5. Из выпадающих списков выберите **Функцию домена** и **Тип хранилища**. Типы доменов хранилища, несовместимые с выбранным дата-центром, не будут доступны.
6. В поле **Хост** выберите активный хост. Если этот домен данных не первый в этом дата-центре, необходимо выбрать SPM хост дата-центра.

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

7. При выборе типа хранилища **Оптоволокно**, в окне **Новый домен** автоматически показываются известные цели с неиспользуемыми LUN. Установите флажок **LUN ID**, чтобы выбрать все доступные LUN.
8. Опционально нажмите **Дополнительные параметры** для настройки следующих значений:
   a. В поле **Индикатор предупреждения о недостатке места** введите процентное значение. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупреждающее сообщение, а событие будет занесено в журнал.
   b. В поле **Блокатор при отсутствии места (ГБ)** введите значение в Гбайт. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого значения, пользователю будет показано сообщение об ошибке, событие будет занесено в журнал, а любое новое действие (даже временное), которому необходимо дисковое пространство, будет заблокировано.
   c. Установите флажок **Забить нулями после удаления**. Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя.
9. Нажмите **OK**.

Во время подготовки к использованию домен данных FCP будет иметь статус «*Заблокировано*». Домен автоматически присоединится к дата-центру, когда будет готов к использованию.

11.5.7. Увеличение размера хранилища iSCSI или FCP

Для увеличения объёма хранилища iSCSI или FCP существуют следующие способы:

- Добавление существующего LUN в текущий домен хранения.
- Создание нового домена с новыми LUN, и добавление этого домена в существующий дата-центр (см. п. 11.7.2. Импорт доменов хранилищ).
- Расширение домена хранения за счёт изменения размера базовых LUN.

В следующей последовательности действий описывается как расширить хранилище сети хранения данных SAN при помощи добавления нового номера LUN в существующий домен хранения со статусом «*Запущен*».

Примечание — все хосты со статусом «*Запущен*» должны иметь доступ к LUN, в противном случае действие закончится неудачей, и LUN не будет добавлен в домен хранения. При этом хосты не будут затронуты. Если недавно добавленный хост, а также хост, выходящий из режима обслуживания или из статуса «*В нерабочем состоянии*», не будет иметь доступа к LUN, то такой хост получит статус «*В нерабочем состоянии*».

Увеличение размера существующего хранилища iSCSI или FCP

1. Нажмите **Хранилище → Домены** и выберите домен iSCSI или FCP.
2. Нажмите **Управление доменом.**
3. Нажмите **Таргеты > LUN** и далее нажмите **Обнаружить таргеты.**
4. Укажите сведения о подключении для сервера хранилища и далее нажмите **Обнаружить** для инициации подключения.
5. Нажмите **Таргеты > LUN** и установите флажок для нового доступного LUN.

6. Нажмите **OK**, чтобы добавить LUN в выбранный домен хранения.

В результате домен хранения увеличится на размер добавленного LUN.

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

Обновление информации о размере LUN на Портале администрирования

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

11.5.8. Повторное использование LUN

Обратите внимание, что номера LUN не могут быть повторно использованы в их текущем состоянии для создания домена хранилища или виртуального диска. При попытке повторно использовать LUN будет выведено следующее сообщение об ошибке на Портале администрирования:

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

Виртуализированный ЦУ покажет следующую ошибку во время установки:

```
[ ERROR ] Error creating Volume Group: Failed to initialize physical device: ("[u'/dev/mapper/000000000000000000000']",)

[ ERROR ] Failed to execute stage 'Misc configuration': Failed to initialize physical device: ("[u'/dev/mapper/000000000000000000000']",)
```

Перед повторным использованием номера LUN необходимо очистить старую таблицу разделов от LUN. Для этого выполните команду `dd` с указанием идентификатора LUN, который необходимо использовать повторно, максимального числа байтов для одновременного чтения и записи, а также числа копируемых входных блоков:

```
# dd if=/dev/zero of=/dev/mapper/LUN_ID bs=1M count=200 oflag=direct
```

Примечание — это действие необходимо выполнить для корректного LUN во избежание непреднамеренного повреждения данных.

11.6. Подготовка и добавление хранилища Gluster

Процесс развёртывания хранилища Gluster приведен в документе «Платформа виртуализации «ROSA Virtualization» (версия 3.0). Импорт существующих доменов хранилищ

11.7.1. Обзор процесса импорта существующих доменов хранилищ

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

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

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

Примечание — импорт существующих доменов хранения данных, присоединённых к дата-центрам, возможен при корректном поддерживаемом уровне совместимости.

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

Примечание — домены ISO являются устаревшими, поэтому для хранения образов ISO рекомендуется использовать домен данных, созданный на базе файловой системы NFS.

- **Домен экспорта**.
  Импорт существующего домена хранения экспорта даёт доступ ко всем образам ВМ и шаблонам, хранящимся в этом домене. Поскольку домены экспорта созданы для экспорта и импорта образов ВМ и шаблонов, импорт доменов хранения экспорта рекомендуется осуществлять при небольших миграциях ВМ и шаблонов внутри окружения или между окружениями.

Примечание — домены хранилищ экспорта являются устаревшими. Домены хранилищ данных можно отсоединить от дата-центра и импортировать в другие дата-центры в том же или в другом окружении. После чего, виртуальные машины, «плавающие» виртуальные диски и шаблоны можно загрузить из домена хранения в прикреплённый дата-центр. Подробные сведения об импорте доменов хранилищ см. п. 11.7.2. Импорт доменов хранилищ.

Обратите внимание, что после прикрепления домена хранения к целевому дата-центру домен может быть обновлён до нового формата, после чего повторное прикрепление к исходному дата-центру может быть невозможным. В свою очередь, это может нарушить процесс использования доменов данных в качестве замены доменам экспорта.

11.7.2. Импорт доменов хранилищ

Для предотвращения возможного повреждения данных при импорте домена хранения, ранее прикреплённого к дата-центру в том же или в другом окружении, подразумевается, что домен хранения уже не прикреплён ни к одному из дата-центров в любом окружении.

Обратите внимание, что целевой дата-центр должен быть инициализирован для импорта и прикрепления существующего домена хранения к этому дата-центру.

Импорт домена хранения

1. Нажмите **Хранилище → Домены**.
2. Нажмите **Импортировать домен**.
3. Выберите **Дата-центр**, в который нужно импортировать домен хранения.
4. Укажите **Имя** домена хранения (Рис. 40).
5. Из выпадающих списков выберите **Функцию домена** и **Тип хранилища**.
6. Выберите **Хост**.

Примечание — подключение к домену осуществляется через выбранный хост, а не напрямую из виртуализированного ЦУ. Таким образом должен существовать как минимум один активный хост, присоединённый к выбранному дата-центру. До начала настройки домена у всех хостов должен быть доступ к устройству хранения.

7. Укажите сведения о домене хранения.

Примечание — поля для ввода сведений о домене хранения изменяются в зависимости от значений, выбранных в списках **Функция домена** и **Тип хранилища**. Эти поля аналогичны полям, отображаемым при добавлении нового домена хранения.

8. Установите флажок **Активировать домен в дата-центре**, чтобы активировать домен хранения после присоединения его к выбранному дата-центру.
9. Нажмите **OK**.

В результате из домена хранения теперь можно импортировать ВМ и шаблоны в выбранный дата-центр.

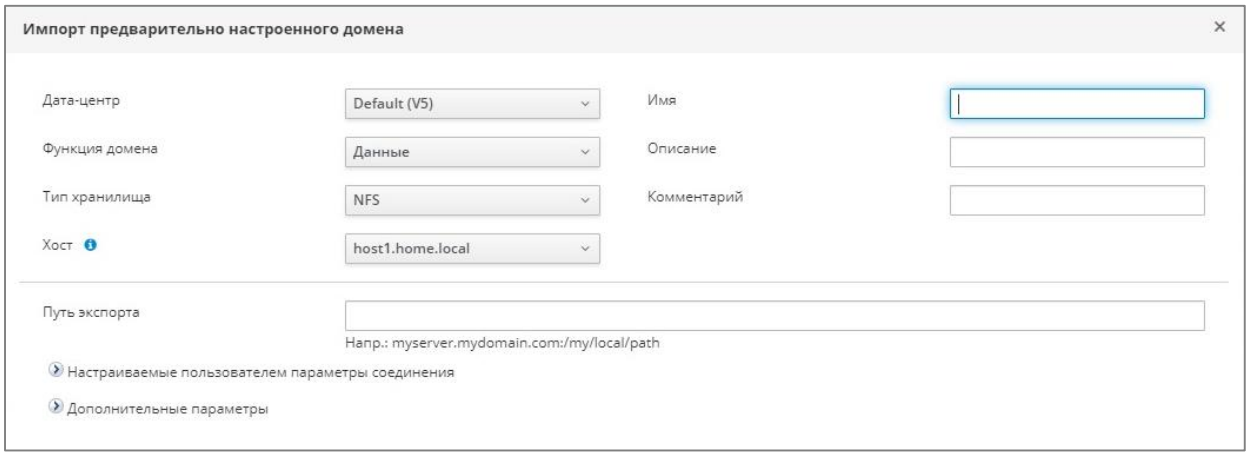

Рис. 40. Импорт домена хранения

11.7.3. Миграция доменов хранилищ между дата-центрами в одном окружении

При миграции домена хранения между дата-центрами в границах окружения системы виртуализации ROSA Virtualization осуществляется откреплением домена от одного дата-центра и прикрепление к другому дата-центру, чтобы целевой дата-центр получил доступ к данным, хранящимся в домене.

Миграция домена хранения между дата-центрами в одном окружении

1. Выключите все ВМ, выполняющиеся в домене хранения.
2. Нажмите **Хранилище → Домены.**
3. Нажмите на название домена хранения, чтобы перейти к подробному просмотру.

4. Перейдите на вкладку **Дата-центр**.
5. Нажмите **Обслуживание** и нажмите **OK**.
6. Нажмите **Отсоединить** и нажмите **OK**.
7. Нажмите **Присоединить**.
8. Выберите целевой дата-центр и нажмите **OK**.

В результате домен хранения прикреплён к целевому дата-центру и автоматически активируется, что позволяет импортировать ВМ и шаблоны из домена хранения в целевой дата-центр.

11.7.4. Миграция доменов хранилищ между дата-центрами в разных окружениях

При миграции домена хранения между дата-центрами в разных окружениях системы виртуализации ROSA Virtualization осуществляется удаление домена из одного окружения и импорт домена в другое окружение, чтобы целевое окружение получило доступ к данным, хранящимся в домене.

Дата-центры в разных окружениях должны иметь корректный поддерживаемый уровень совместимости для обеспечения возможности импорта и присоединения домена хранения данных.

Миграция домена хранения между дата-центрами в разных окружениях

1. Войдите на Портал администрирования в исходном окружении.
2. Выключите все ВМ, выполняющиеся в домене хранения.
3. Нажмите **Хранилище → Домены**.
4. Нажмите на название домена хранения, чтобы перейти к подробному просмотру.
5. Перейдите на вкладку **Дата-центр**.
6. Нажмите **Обслуживание** и нажмите **OK**.
7. Нажмите **Открепить** и нажмите **OK**.
8. Нажмите **Удалить**.
9. В окне **Удалить хранилище** убедитесь в том, что флажок **Форматировать домен, т.е. содержимое хранилища будет потеряно** не установлен. Таким образом данные в домене сохраняются для последующего использования.
10. Нажмите **OK** для удаления домена хранения из исходного окружения.
11. Войдите на Портал администрирования в целевом окружении.
12. Нажмите **Хранилище → Домены**.
13. Нажмите **Импортировать домен**.
14. Из выпадающего списка **Дата-центр** выберите целевой дата-центр.
15. Введите **Имя** домена хранения.
16. Из соответствующих выпадающих списков выберите **Функцию домена** и **Тип хранилища**.
17. Выберите **Хост**.
18. Укажите сведения о домене хранения.

Примечание — поля для ввода сведений о домене хранения изменяются в зависимости от значений, выбранных в списках **Функция домена** и **Тип хранилища**. Эти поля аналогичны полям, отображаемым при добавлении нового домена хранения.

19. Установите флажок **Активировать домен дата-центра**, чтобы домен хранения был активирован автоматически при присоединении.

20. Нажмите **OK**.

В результате домен хранения будет присоединён к целевому дата-центру в новом окружении системы виртуализации ROSA Virtualization и автоматически активирован, что позволяет импортировать ВМ и шаблоны из домена хранения в целевой дата-центр.

11.7.5. Импорт виртуальных машин из импортированных доменов данных

Импорт ВМ из импортированного домена хранения данных может осуществляться в один или несколько целевых кластеров.

В следующей последовательности действий предполагается, что ранее импортированный домен хранения данных был присоединён к дата-центру и активирован.

Импорт ВМ из импортированного домена данных

1. Нажмите **Хранилище → Домены**.
2. Нажмите на имя импортированного домена данных, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Импорт ВМ**.
4. Выберите одну или несколько ВМ для импорта.
5. Нажмите **Импортировать**.
6. Убедитесь, что для каждой ВМ в окне **Импорт ВМ** выбран корректный целевой кластер из списка **Кластер**.
7. Отобразите внешние профили vNIC ВМ на профили, присутствующие в целевом кластере:
   a. Нажмите **Отображение профилей vNIC**.
   b. Выберите используемый профиль vNIC из выпадающего списка **Целевой профиль vNIC**.
   c. Если в окне **Импорт ВМ** было выбрано несколько целевых кластеров, выберите каждый целевой кластер из выпадающего списка **Целевой кластер** и убедитесь в том, что отображения корректны.
   d. Нажмите **OK**.
8. При обнаружении конфликта адресов MAC, рядом с именем ВМ появится восклицательный знак. Наведите курсор на восклицательный знак, чтобы просмотреть всплывающую подсказку с возникшей ошибкой. Установите флажок **Повторно присвоить неправильные MAC**, чтобы повторно присвоить конфликтующие адреса MAC всем проблемным ВМ.

Примечание — импорт ВМ закончится неудачей в случае отсутствия доступных адресов MAC для присвоения. Тем не менее, возможен импорт ВМ без присвоения новых адресов при использовании адресов MAC, расположенных вне диапазона пула адресов MAC кластера.

9. Нажмите **OK**.

11.7.6. Импорт шаблонов из импортированных доменов данных

Импорт шаблонов из импортированного домена хранения данных может осуществляться в один или несколько целевых кластеров.

В следующей последовательности действий предполагается, что ранее импортированный домен хранения данных был присоединён к дата-центру и активирован.

Импорт шаблонов из импортированного домена данных

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

11.8. Работа с доменами хранилищ

11.8.1. Размещение образов в доменах данных

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

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

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

Предварительные условия

Так как функция загрузки (отправки) в домен использует HTML5 API, в окружении необходимо иметь следующие компоненты:

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

  Для импортирования центра сертификации перейдите по адресу `https://`*`адрес_диспетчера_виртуализации`*`/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA` и включите все параметры доверия.
- Браузер с поддержкой HTML5.

Размещение образа в домене хранения данных

1. Нажмите **Хранилище → Диски**.
2. В меню **Отправить** выберите **Начать**.
3. Нажмите **Выберите файл** и выберите образ для загрузки в домен.
4. Заполните поля **Параметры диска**.

5. Нажмите **OK**.

Статус загрузки образа в домен отображается с помощью индикатора выполнения.

В меню **Отправить** можно приостановить, отменить или возобновить отправку файлов.

Увеличение значения времени ожидания отправки

1. В случае превышения времени ожидания окончания отправки и появлении соответствующего сообщения «`Причина: превышение времени ожидания в связи с неактивностью передачи`» выполните следующую команду для увеличения значения времени ожидания:

```
# engine-config -s TransferImageClientInactivityTimeoutInSeconds=6000
```

2. Перезапустите службу `ovirt-engine`:

```
# systemctl restart ovirt-engine
```

11.8.2. Перевод доменов хранилищ в режим обслуживания

Перед откреплением и удалением домена хранения обязательно переведите этот домен в режим обслуживания. Это необходимо для присвоения другому домену данных роли домена мастер-данных.

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

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

Перевод домена хранения в режим обслуживания

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

Примечание — опционально установите флажок **Игнорировать сбой обновления OVF** для перемещения домена хранения в режим обслуживания даже при сбое обновления OVF.

6. Нажмите **OK**.

В результате домен хранения деактивируется и в списке результатов получает статус «*Неактивен*».

Неактивные домены хранения можно изменять, отключать, удалять или активировать повторно в дата-центре.

Примечание — активировать, отсоединять и помещать домены в режим обслуживания можно также во вкладке **Хранилище** в подробном просмотре дата-центра, к которому присоединены эти домены.

11.8.3. Изменение параметров доменов хранилищ

Параметры доменов хранилищ можно изменить на Портале администрирования. При этом параметры **Дата-центр**, **Функция домена**, **Тип хранилища** и **Формат** изменить нельзя.

Параметры, доступные для изменения, зависят от статуса домена хранения («*Активен*» или «*Неактивен*»):

- **Активен**.
  Для домена с активным статусом можно изменить значение следующих полей: **Имя**, **Описание**, **Комментарий**, **Индикатор предупреждения о недостатке места (%)**, **Блокировщик действия при критической нехватке места**, **Забить нулями после удаления** и **Освободить блоки перед удалением**.
  Поле **Имя** можно изменить только для активного домена хранения. Другие поля также можно изменить при неактивном домене.
- **Неактивен**.
  Для неактивного домена, то есть находящегося в режиме обслуживания или не присоединённого, можно изменить значения всех полей, за исключением полей **Имя**, **Дата-центр**, **Функция домена**, **Тип хранилища** и **Формат**.
  Изменить параметры сетевых соединений, параметры монтирования, а также другие дополнительные параметры можно только для неактивного домена. Эти параметры поддерживаются только для типов доменов NFS, POSIX и локальных.

Примечание — сетевые соединения хранилищ iSCSI нельзя редактировать на Портале администрирования, но можно редактировать с помощью REST API.

Изменение параметров активного домена хранения

1. Нажмите **Хранилище → Домены** и выберите домен хранения.
2. Нажмите **Управление доменом**.
3. При необходимости измените значения доступных полей.
4. Нажмите **OK**.

Изменение параметров неактивного домена хранения

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

11.8.4. Обновление файлов OVF

По умолчанию файлы OVF обновляются каждые 60 минут.

Также файлы OVF можно обновить вручную (например, после импорта ВМ или критически важного обновления ПО).

Обновление файлов OVF

1. Нажмите **Хранилище → Домены**.
2. Выберите домен хранения, нажмите **Больше действий** (⋮) и далее нажмите **Обновить файлы OVF**.

11.8.5. Активация доменов хранилищ из режима обслуживания

Если ранее домен хранения был переведен в режим обслуживания, то для возобновления использования необходимо активировать этот домен из режима обслуживания.

Активация домена хранения из режима обслуживания

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

Примечание — при попытке активации домена ISO до активации домена данных будет показано соответствующее сообщение об ошибке и домен ISO не будет активирован.

11.8.6. Отсоединение домена хранения от дата-центра

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

Отсоединение домена хранения от дата-центра

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

В результате домен хранения будет отсоединён от текущего дата-центра и готов для присоединения к другому дата-центру.

11.8.7. Присоединение домена хранения к дата-центру

Присоединение домена хранения к дата-центру

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

В результате домен хранения будет присоединён к выбранному дата-центру и автоматически активирован.

11.8.8. Удаление домена хранения

Удаление домена хранения

1. Нажмите **Хранилище → Домены**.
2. Переместите домен хранения в режим обслуживания и отсоедините домен:
   a. Нажмите на имя домена, чтобы перейти к подробному просмотру.

b. Перейдите на вкладку **Дата-центр**.
c. Нажмите **Обслуживание** и далее нажмите **OK**.
d. Нажмите **Отсоединить** и далее нажмите **OK**.

3. Нажмите **Удалить**.
4. Опционально установите флажок **Форматировать домен, т.е. содержимое хранилища будет потеряно**, чтобы окончательно стереть всё содержимое домена.
5. Нажмите **OK**.

11.8.9. Разрушение домена хранения

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

Разрушение домена хранения

1. Нажмите **Хранилище → Домены**.
2. Выберите домен хранилища, нажмите **Больше действий** (⋮) и далее нажмите **Разрушить**.
3. Установите флажок **Одобрить операцию**.
4. Нажмите **OK**.

11.8.10. Создание профилей дисков

Профили дисков определяют максимальные уровни пропускной способности и операций ввода-вывода виртуальных дисков в домене хранения.

Профили дисков создаются на базе профилей хранилищ, настроенных в дата-центрах.

Профили дисков назначаются вручную каждому виртуальному диску.

В следующей последовательности действий подразумевается, что ранее в дата-центре, к которому принадлежит домен хранения, была настроена одна или несколько записей о качестве обслуживания хранилищ.

Создание профиля диска

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

11.8.11. Удаление профилей дисков

Удаление профиля диска

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

11.8.12. Просмотр состояния работоспособности доменов хранилищ

В дополнение к обычному **Статусу** у доменов хранилищ есть внешний статус работоспособности. Информация о внешнем статусе работоспособности доставляется модулями или внешними системами, или же настраивается администратором.

Внешний статус работоспособности отображается слева от имени домена в виде следующих значков:

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

Чтобы узнать дополнительные подробности о работоспособности домена хранения нажмите на имя домена и перейдите на вкладку **События**.

Примечание — внешний статус работоспособности домена также можно узнать с помощью REST API (элемент `external_status` в запросе `GET`). Для указания статуса работоспособности домена через REST API используйте набор `events`.

11.8.13. Параметр «Освободить блоки перед удалением»

Если параметр **Освободить блоки перед удалением** включен, при удалении логического тома вызывается команда `blkdiscard` и базовое хранилище оповещается о том, что блоки свободны. Далее массив хранилища может использовать (выделять по запросу) освобождённое пространство.

Параметр **Освободить блоки перед удалением** эффективен и доступен только для доменов блочных хранилищ, таких как iSCSI или FCP (хранилище должно поддерживать `Discard`). Для файловых хранилищ, таких как NFS, этот параметр недоступен.

Параметр **Освободить блоки перед удалением** можно включить как при создании домена блочного хранилища iSCSI или FCP, так и при изменении параметров этого домена.

Глава 12. Пулы

12.1. Пул виртуальных машин

Пул виртуальных машин — это группа ВМ, являющихся клонами одного и того же шаблона, которые могут использоваться по требованию любым пользователем в указанной группе. Пулы ВМ дают администраторам возможность быстро настроить набор стандартных ВМ для пользователей.

Пользователи при осуществлении доступа к пулу ВМ получают для своей работы ВМ из пула. Когда пользователи забирают ВМ из пула, они получают любую ВМ, если хотя бы одна машина в пуле является доступной. ОС и конфигурация ВМ, получаемой пользователем из пула, аналогичны ОС и конфигурации шаблона, на базе которого был создан пул, но каждый раз забирая машину из пула, пользователь не получает одного и того же участника пула. Также пользователи могут получить несколько ВМ из одного и того же пула, в зависимости от параметров пула.

По умолчанию пулы ВМ не сохраняют состояние, соответственно изменения в данных и конфигурации ВМ не сохраняются после перезагрузки. Тем не менее, можно создать конфигурацию пула с фиксацией состояния, то есть с сохранением изменений, внесённых предыдущим пользователем. Но если на ВМ, взятой из пула, пользователь настроит свои консольные параметры, то эти параметры станут параметрами по умолчанию для этого пользователя в данном пуле ВМ.

Примечание — при доступе с Портала администрирования к ВМ, взятым из пула, эти ВМ сохраняют состояние, так как у администраторов должна быть возможность при необходимости записать изменения на диск.

Таким образом, ВМ в пуле начинают работу тогда, когда их получают пользователи, и выключаются, когда пользователи завершают работу с машиной. Тем не менее, в пуле могут присутствовать предварительно запущенные ВМ, которые не выключаются и простаивают до того момента, пока их не заберёт пользователь. Такая настройка даёт пользователям возможность немедленно начать работу с машиной, но такие ВМ потребляют системные ресурсы не только во время работы, но и во время простоя.

12.2. Создание пула виртуальных машин

Создание пула виртуальных машин осуществляется из нескольких ВМ, предварительно созданных на базе общего шаблона.

Примечание — при создании пула ВМ под управлением ОС Windows окружением используются параметры конфигурационного файла `sysprep`.

Параметры конфигурационного файла `sysprep` для ВМ под управлением ОС Windows

Если пулу не нужно присоединяться к домену, используйте файл `sysprep` со значениями по умолчанию, расположенный в `/usr/share/ovirt-engine/conf/sysprep/`.

Если пул должен присоединиться к домену, то для каждой из ОС Windows рекомендуется создать частный файл `sysprep` следующим образом:

1. Скопируйте разделы, имеющие отношение к каждой ОС Windows, из `/usr/share/ovirt-engine/conf/osinfo-defaults.properties` в новый файл, и сохраните его как `99-defaults.properties`.

2. В файле `99-defaults.properties` укажите ключ активации ОС Windows и путь до частного файла `sysprep`:

```
os.operating_system.productKey.value=Windows_product_activation_key
...
os.operating_system.sysprepPath.value = ${ENGINE_USR}/conf/sysprep/
sysprep.operating_system
```

3. Создайте новый файл `sysprep`, где укажите домен, пароль домена и администратора домена:

```
<Credentials>
    <Domain>Домен_AD</Domain>
    <Password>Пароль_домена</Password>
    <Username>Администратор_домена</Username>
</Credentials>
```

Примечание — при необходимости создания различных параметров `sysprep` для разных пулов ВМ под управлением ОС Windows рекомендуется создать частный файл `sysprep` на Портале администрирования.

Создание пула ВМ

1. Нажмите **Ресурсы → Пулы**.
2. Нажмите **Добавить**, чтобы открыть окно **Новый пул**.

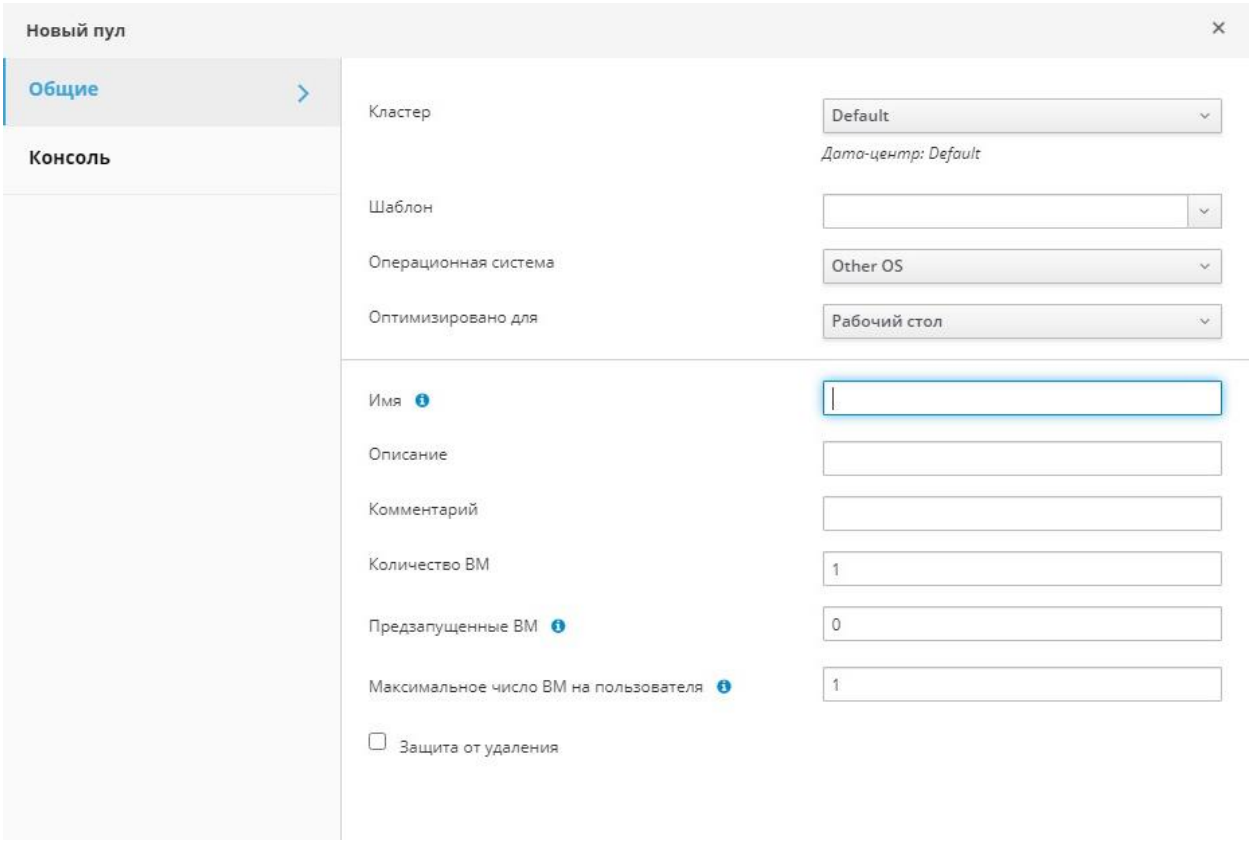

Рис. 41. Создание пула ВМ

3. Из выпадающего списка выберите **Кластер**.
4. Из выпадающего списка выберите **Шаблон** и версию. Шаблон предоставляет стандартные значения параметров для всех ВМ в пуле.
5. Из выпадающего списка выберите **Операционную систему**.

6. Используя значения из выпадающего списка **Оптимизировано для** оптимизируйте виртуальные машины для **Рабочего стола** или **Сервера**.

Примечание — оптимизация **Высокая производительность** не рекомендуется для пулов, поскольку высокопроизводительная ВМ прикрепляется к одному хосту и к конкретным ресурсам. Пул, содержащий несколько таких ВМ, не будет работать эффективно.

7. Укажите **Имя** для пула и опционально **Описание** и **Комментарий**.

Примечание — имя пула с числовым суффиксом применяется к каждой ВМ в пуле (например, имени пула `MyPool` соответствует следующая нумерация виртуальных машин `MyPool-1`, `MyPool-2`, … `MyPool-10`). Настроить нумерацию ВМ можно с использованием символа ? (вопросительный знак) в качестве метки-заполнителя (например, имени пула `MyPool-???` соответствует следующая нумерация виртуальных машин `MyPool-001`, `MyPool-002`, … `MyPool-010`).

8. Укажите **Количество ВМ** для пула.
9. Укажите количество ВМ с предварительным запуском в поле **Предзапущенные ВМ**.
10. Укажите **Максимальное число ВМ на пользователя**, которое разрешено запускать одному пользователю в течение сеанса. Минимальное значение — 1.
11. Опционально установите флажок **Защита от удаления**.
12. Если создаётся пул ВМ не под управлением ОС Windows, или используется исходный файл `sysprep` перейдите к следующему шагу.
    В случае создания частного файла `sysprep` для пула ВМ под управлением ОС Windows выполните следующие действия:
    - Нажмите на кнопку **Показать дополнительные параметры**.
    - Перейдите на вкладку **Начальный запуск** и установите флажок **Cloud-Init/Sysprep**.
    - Нажмите **Аутентификация** и введите **Имя пользователя** и **Пароль**, или выберите **Использовать уже настроенный пароль**.

Примечание — значение в поле **Имя пользователя** является пользовательским именем локального администратора. Изменить значение по умолчанию (`user`) можно или в разделе **Аутентификация** или в частном файле `sysprep`.

- Нажмите **Настраиваемый пользователем сценарий** и вставьте в текстовый блок содержимое исходного файла `sysprep`, расположенного по следующему пути `/usr/share/ovirt-engine/conf/sysprep/`.
- При необходимости измените значения следующих параметров конфигурационного файла `sysprep` (обратите внимание, что значения этих параметров нельзя изменить во вкладке **Начальный запуск**):
  — `Key` (ключ активации).
  Если предварительно настроенный ключ активации ОС Windows не будет использоваться замените `<![CDATA[$ProductKey$]]>` на действительный ключ:

```
<ProductKey>
    <Key><![CDATA[$ProductKey$]]></Key>
</ProductKey>
```

— `Domain` (домен, к которому присоединяется ВМ под управлением ОС Windows), `Password` (пароль домена) и `Username` (имя администратора):

```
<Credentials>
    <Domain>Домен_AD</Domain>
    <Password>Пароль_домена</Password>
    <Username>Администратор_домена</Username>
</Credentials>
```

— `FullName` (полное имя локального администратора):

```
<UserData>
…
    <FullName>локальный_администратор</FullName>
…
</UserData>
```

— `DisplayName` и `Name` (имя локального администратора):

```
<LocalAccounts>
    <LocalAccount wcm:action="add">
        <Password>
            <Value><![CDATA[$AdminPassword$]]></Value>
            <PlainText>true</PlainText>
        </Password>
        <DisplayName>Local_Administrator</DisplayName>
        <Group>administrators</Group>
        <Name>Local_Administrator</Name>
    </LocalAccount>
</LocalAccounts>
```

- При необходимости значения других параметров конфигурационного файла `sysprep` заполните во вкладке **Начальный запуск**.

13. Опционально укажите **Тип пула**:
    - Перейдите на вкладку **Тип** и выберите **Тип пула**:
      — **Вручную**.
      Возвращение ВМ в пул осуществляется вручную администратором.
      — **Автоматически**.
      Возвращение ВМ в пул осуществляется автоматически.
    - Установите флажок **Пул с сохранением состояния**, чтобы ВМ запускались в режиме с сохранением состояния. Это обеспечивает сохранение в ВМ изменений, внесённых предыдущим пользователем.
    - Нажмите **OK**.
14. При необходимости переопределите прокси SPICE:
    - Во вкладке **Консоль** установите флажок **Переопределить SPICE прокси**.
    - В поле **Переназначенный адрес прокси SPICE** укажите адрес прокси SPICE, который заменит глобальный прокси.
    - Нажмите **OK**.
15. Если пул состоит из ВМ под управлением ОС Windows нажмите **Ресурсы → Виртуальные машины**, далее выберите каждую ВМ и нажмите **Запустить → Однократный запуск.**

Примечание — если ВМ не запускается, а в файле журнала `%WINDIR%\panther\UnattendGC\setupact.log` появляется запись `Info [windeploy.exe] Found no unattend file`, то в реестр ВМ под управлением ОС Windows, на базе которой создавался шаблон для пула, необходимо добавить ключ `UnattendFile` следующим образом:

- Проверьте, не присоединено ли к ВМ под управлением ОС Windows устройство флоппи-дискеты с файлом `Unattend` (например, `A:\Unattend.xml`).
- В панели задач ОС Windows нажмите **Пуск**, затем **Выполнить**, далее в текстовый блок **Открыть** введите `regedit` и нажмите **ОК**.
- В левой панели реестра выберите пункт меню **HKEY_LOCAL_MACHINE → SYSTEM → Setup**.
- Сделайте щелчок правой кнопкой мыши в правой панели реестра и из контекстного меню выберите **Создать → Строковой параметр**.
- Укажите имя ключа **UnattendFile**.
- Сделайте двойной щелчок по новому ключу и в качестве значения ключа введите имя файла `Unattend` и путь к этому файлу (например, `A:\Unattend.xml`).
- Сохраните изменения в реестре, сохраните состояние ВМ и создайте новый шаблон.

В результате будет создан пул виртуальных машин с указанным числом одинаковых ВМ.

Для просмотра ВМ из пула используйте меню **Ресурсы → Виртуальные машины** или нажмите на имя пула, чтобы перейти к подробному просмотру (при отображении виртуальные машины из пула отличаются от независимых ВМ своим значком).

12.3. Параметры и элементы управления пулами

12.3.1. Общие параметры в окнах «Новый пул» и «Параметры пула»

В **Табл. 12.1** описываются параметры пула во вкладке **Общие** окон **Новый пул** и **Параметры пула**.

Все другие параметры идентичны параметрам окна **Новая ВМ**.

Табл. 12.1. Общие параметры

Поле	Описание
Шаблон	Шаблон и версия шаблона, на которых основан пул машин. Если создать пул на основе версии шаблона `latest`, то все ВМ в пуле при перезагрузке автоматически получат последнюю версию шаблона
Описание	Описание пула ВМ
Комментарий	Поле для добавления комментария для пула ВМ, в простом текстовом формате
Предварительно запущенные ВМ	Параметр даёт возможность указать число тех ВМ в пуле, которые будут предварительно запущены перед размещением в пуле и будут забираться пользователями уже работающими. Значение параметра должно быть между `0` и общим числом ВМ в пуле
Количество ВМ / Увеличить число ВМ в пуле на	Параметр даёт возможность указать конкретное количество ВМ, которые нужно создать и сделать доступными в пуле.

Поле	Описание
	По умолчанию максимальное число ВМ, создаваемых в пуле — 1000. Это значение можно настроить с помощью ключа `MaxVmsInPool` команды `engine-config`
Максимальное число ВМ на пользователя	Параметр даёт возможность указать максимальное число ВМ, доступных пользователю в пуле в любое время. Значение параметра должно быть в диапазоне от 1 до 32 767
Защита от удаления	Параметр защищает ВМ в пуле от удаления

12.3.2. Параметры вкладки «Тип» в окнах «Новый пул» и «Изменить пул»

В **Табл. 12.2** описываются параметры пула во вкладке **Тип** окон **Новый пул** и **Изменить пул**.

Табл. 12.2. Параметры типа

Поле	Описание
Тип пула	В этом выпадающем меню можно указать тип пула ВМ. Доступны следующие значения: • **Автоматически**. После того, как пользователь закончит работу с ВМ, взятой из пула, ВМ автоматически возвращается в пул. • **Вручную**. После того, как пользователь закончит работу с ВМ, взятой из пула, ВМ возвращается в пул только вручную администратором.
Пул с сохранением состояния	Параметр позволяет указать, будет ли сохраняться состояние ВМ в пуле после того, как ВМ будет передана другому пользователю. Это означает, что изменения, внесённые предыдущим пользователем, сохранятся в ВМ

12.3.3. Параметры вкладки «Консоль» в окнах «Новый пул» и «Изменить пул»

В **Табл. 12.3** описываются параметры пула во вкладке **Консоль** окон **Новый пул** и **Изменить пул**.

Все другие параметры идентичны параметрам окна **Новая ВМ** и **Параметры виртуальной машины**.

Табл. 12.3. Параметры консоли

Поле	Описание
Переназначить SPICE прокси	Установите флажок для этого пункта, чтобы включить переопределение прокси SPICE, указанного в глобальной конфигурации. Используйте эту возможность, если пользователь находится вне той сети, в которой располагаются хосты (например, пользователь подключается через портал ВМ)
Переназначенный адрес SPICE прокси	Прокси, с помощью которого клиент SPICE подключается к виртуальным машинам. Значение этого прокси переопределяет как глобальное значение прокси SPICE, настроенное для окружения виртуализации, так и значение, настроенное для кластера, которому принадлежит пул ВМ, если такой кластер существует. Адрес должен соответствовать следующему формату: `протокол://`*`хост`*`:`*`порт`*

12.3.4. Параметры вкладки «Хост» в окнах «Новый пул» и «Параметры пула»

В **Табл. 12.4** описываются параметры пула во вкладке **Хост** окон **Новый пул** и **Параметры пула**.

Табл. 12.4. Параметры хоста

Поле	Вложенный элемент	Описание
Начать выполнение на:		Параметр позволяет указать предпочитаемый хост, на котором должна выполняться ВМ. Доступны следующие значения: • **Любой хост в кластере**. ВМ может запускаться и выполняться на любом доступном хосте в кластере. • **Конкретный хост**. ВМ начинает работу на конкретном указанном хосте в кластере, но виртуализированный ЦУ или администратор могут выполнить миграцию ВМ на другой хост в кластере в зависимости от параметров миграции и параметров высокой доступности ВМ. Выберите хост или группу хостов из списка доступных хостов.
Параметры миграции	Режим миграции	Параметр режима миграции ВМ может принимать следующие значения (если следующие значения не используются, ВМ будет мигрировать в соответствии с политикой кластера): • **Разрешить ручную и автоматическую миграции**. ВМ может мигрировать с одного хоста на другой автоматически, согласно статусу окружения, или может быть перенесена администратором вручную. • **Разрешить только ручную миграцию**. Миграция ВМ с одного хоста на другой может выполняться только вручную администратором. • **Не разрешать миграцию**. Миграция ВМ (ручная или автоматическая) запрещена.
	Политика миграции	По умолчанию политика миграции определяется на уровне кластера. Для переопределения параметра (на уровне хоста) доступны следующие значения: • **Минимальное время простоя**. Разрешается миграция ВМ в типичных ситуациях с незначительным временем простоя. Миграция будет прервана, если после долгого времени не будет достигнуто состояние целостности (зависит от итераций QEMU, максимальный интервал — 500 миллисекунд). Механизм перехватчиков событий гостевого агента включён. • **В случае необходимости приостановить рабочую нагрузку**. Разрешается миграция ВМ в большинстве ситуаций, включая те, когда ВМ испытывает серьёзную нагрузку. В связи с этим разрешается более значительный простой ВМ, чем при других значениях данного параметра. Миграция всё ещё может быть прервана при

Поле	Вложенный элемент	Описание
		экстремальных нагрузках. Механизм перехватчиков событий гостевого агента включён.
	Включить шифрование при миграции	Параметр даёт возможность указать, будет ли использоваться шифрование во время динамических миграций ВМ. По умолчанию шифрование во время миграции ВМ отключено на уровне кластера. Параметр может принимать следующие значения: • **Значение по умолчанию.** Используется значение **Зашифровать** или **Не шифровать** (по умолчанию), настроенное на уровне кластера. • **Зашифровать.** Значение переопределяет настройку на уровне кластера и включает шифрование при миграции ВМ. • **Не шифровать.** Значение переопределяет настройку на уровне кластера и отключает шифрование при миграции ВМ.
Параметры ЦП	Сквозной доступ к ЦП хоста	Этот флажок даёт возможность ВМ использовать преимущества физического ЦП хоста, на котором ВМ размещены
	Идентичная частота TSC	Этот флажок разрешает миграцию ВМ только на хосты с такой же частотой счётчика метки времени
Параметры NUMA	Число узлов NUMA	Число виртуальных узлов NUMA, присваиваемых ВМ. При **Предпочитаемом** значении параметра **Режим настройки** (см. строку ниже), это число должно быть равно 1
	Режим настройки	Метод выделения памяти. Для параметра доступны следующие значения: • **Строгий.** Выделение памяти закончится неудачей, если на целевом узле память выделить нельзя. • **Предпочитаемый.** Память выделяется из исходного предпочитаемого узла. Если достаточный объём памяти недоступен, память можно выделить из других узлов. • **Чередование.** Память выделяется из всех узлов в алгоритме кругового обслуживания.
	Привязка NUMA	Привязка NUMA осуществляется в окне **Топология NUMA**, в котором отображается общее число ЦП хоста, памяти и узлов NUMA, а также виртуальные узлы NUMA ВМ. Привяжите виртуальные узлы NUMA для размещения узлов NUMA. Для этого нажмите и перетащите каждый виртуальный узел NUMA из блока справа на узел NUMA в блок слева. При настроенной привязке NUMA, для параметра **Режим миграции** будет доступно единственное значение **Разрешить только ручную миграцию**

12.3.5. Параметры вкладки «Выделение ресурсов» в окнах «Новый пул» и «Изменить пул»

В **Табл. 12.5** описываются параметры пула во вкладке **Выделение ресурсов** окон **Новый пул** и **Изменить пул**.

Все другие параметры идентичны параметрам окна **Новая ВМ**.

Табл. 12.5. Параметры выделения ресурсов

Поле	Вложенный элемент	Описание
Выделение дисковых ресурсов	Автоматический выбор цели	Установите этот флажок, чтобы домен хранилища с наибольшим объёмом свободного места выбирался автоматически. При этом поля **Цель** и **Профиль диска** будут неактивными
	Формат	Поле доступно только для чтения и всегда показывает значение **QCOW2**, за исключением случаев, когда домен имеет тип OpenStack Volume (Cinder). В этих случаях формат будет **raw**

12.4. Изменение параметров пула виртуальных машин

После создания пула ВМ можно изменить параметры пула.

Параметры, доступные при изменении свойств пула ВМ, идентичны параметрам, доступным при создании нового пула ВМ, за исключением того, что параметр **Число ВМ** заменяется параметром **Увеличить число ВМ в пуле на**…

Примечание — при изменении параметров пула ВМ, вносимые изменения влияют только на новые ВМ. При этом ВМ, существующие на момент внесения изменений, останутся незатронутыми.

Изменение параметров пула ВМ

1. Нажмите **Ресурсы → Пулы** и выберите пул ВМ.
2. Нажмите **Изменить.**
3. Измените свойства пула ВМ.
4. Нажмите **ОК.**

12.5. Предварительный запуск виртуальных машин в пуле

По умолчанию виртуальные машины в пуле ВМ выключены. Когда пользователь запрашивает машину из пула, машина запускается и присваивается пользователю. И наоборот, предварительно запущенная ВМ уже работает и ждёт присвоения пользователю, что снижает время ожидания начала работы. После выключения предварительно запущенной ВМ, машина возвращается в пул и восстанавливается до исходного состояния.

Предварительно запущенные ВМ подходят для окружений, в которых пользователям нужен немедленный доступ к машинам, не выделенным специально для этого пользователя. Предварительно запущенные ВМ могут находиться только в автоматических пулах.

Максимальное число предварительно запущенных ВМ равно числу ВМ в пуле.

Предварительный запуск ВМ в пуле

1. Нажмите **Ресурсы → Пулы** и выберите пул ВМ.
2. Нажмите **Изменить.**
3. В поле **Предзапущенные ВМ** укажите число ВМ, которые необходимо предварительно запустить.
4. Перейдите на вкладку **Тип**. Убедитесь в том, что значение **Тип пула** указано как **Автоматически.**
5. Нажмите **ОК.**

12.6. Добавление виртуальных машин в пул ВМ

Добавление виртуальных машин в пул ВМ

1. Нажмите **Ресурсы → Пулы** и выберите пул ВМ.
2. Нажмите **Изменить**.
3. В поле **Увеличить число ВМ в пуле на …** укажите число дополнительных ВМ.
4. Нажмите **OK**.

12.7. Открепление виртуальных машин от пула ВМ

Виртуальные машины можно откреплять от пула ВМ. Открепление машины удаляет ВМ из пула, и машина становится независимой ВМ.

Открепление виртуальных машин от пула ВМ

1. Нажмите **Ресурсы → Пулы**.
2. Нажмите на имя пула, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Виртуальные машины**, чтобы просмотреть список ВМ в пуле.
4. Убедитесь в том, что машина имеет статус «*Не запущена*», так как работающую ВМ открепить нельзя.
5. Выберите одну или несколько ВМ и нажмите **Открепить**.
6. Нажмите **OK**.

Примечание — открепленная виртуальная машина по-прежнему существует в окружении, и к такой ВМ можно получить доступ из меню **Ресурсы → Виртуальные машины**. Обратите внимание, что значок ВМ изменится, для обозначения того, что откреплённая от пула ВМ машина стала независимой.

12.8. Удаление пула виртуальных машин

Пул ВМ можно удалить из дата-центра. Сначала необходимо удалить или открепить все ВМ из пула ВМ. При этом открепление ВМ от пула ВМ сохранит виртуальные машины в качестве независимых ВМ.

Удаление пула ВМ

1. Нажмите **Ресурсы → Пулы** и выберите пул ВМ.
2. Нажмите **Удалить**.
3. Нажмите **OK**.

Глава 13. Виртуальные диски

13.1. Хранилище виртуальной машины

Система виртуализации ROSA Virtualization поддерживает следующие типы хранилищ — NFS, iSCSI и FCP.

Вне зависимости от типа хранилища в системе существует хост, который называется диспетчером пула хранилищ (SPM) и управляет связью между хостами и хранилищем. Хост SPM является единственным узлом с полным доступом в рамках пула хранилищ и может изменять метаданные домена хранилищ, а также метаданные пула. Все другие хосты имеют доступ только к данным, содержащимся в образе жёсткого диска ВМ.

По умолчанию в дата-центрах на базе NFS, локальных или совместимых с POSIX, хост SPM создаёт виртуальные диски с помощью формата тонкого резервирования в виде файла в файловой системе.

В дата-центрах на базе iSCSI и в других блочных дата-центрах, таких как FCP, хост SPM создаёт группу томов поверх предоставленных номеров LUN, а логические тома используются как виртуальные диски. По умолчанию виртуальные диски в блочных хранилищах являются предварительно зарезервированными.

Для предварительно зарезервированного виртуального диска («*толстого*» диска) создаётся логический том указанного размера в Гбайт.

Для виртуального диска тонкого резервирования создаётся логический том с начальным размером в 1 Гбайт. За логическим томом ведётся постоянное наблюдение со стороны хоста, на котором выполняется ВМ. Как только используемый объём приближается к пороговому значению, хост оповещает SPM, и SPM увеличивает размер логического тома ещё на 1 Гбайт. За возобновление работы ВМ после увеличения размера логического тома отвечает хост. Если работа ВМ будет приостановлена, это означает, что SPM не смог вовремя увеличить размер диска (например, если в хранилище недостаточно свободного дискового пространства).

Скорость записи виртуального диска в формате предварительного резервирования raw значительно выше, чем скорость записи виртуального диска в формате тонкого резервирования QCOW2. При этом время создания виртуального диска тонкого резервирования значительно меньше. Формат тонкого резервирования QCOW2 подходит для ВМ без интенсивных процессов ввода-вывода. Формат предварительного резервирования raw подходит для ВМ с высокой интенсивностью записи процессов ввода-вывода. Если ВМ записывает процессы ввода-вывода объёмом более 1 Гбайт каждые четыре секунды, всегда при возможности используйте предварительно зарезервированные диски в формате raw.

13.2. Виртуальные диски

Система виртуализации ROSA Virtualization предлагает следующие возможности для выделения свободного дискового пространства в хранилище:

- **Предварительное резервирование**.
  Предварительно зарезервированный виртуальный диск заранее резервирует всё выделенное место в хранилище, предназначенное для виртуальной машины. Таким образом, предварительно зарезервированный логический том размером в

20 Гбайт, созданный для раздела размещения данных ВМ, займёт все 20 Гбайт свободного места в хранилище сразу после своего создания.

- **Тонкое резервирование разрежённого типа**.
  Тонкое резервирование разрежённого типа даёт возможность администратору определить общий объём места в хранилище, выделяемого виртуальной машине, но это место выделяется только при необходимости. Логический том тонкого резервирования размером в 20 Гбайт займёт при создании 0 Гбайт. После установки операционной системы размер диска будет равен размеру установленных файлов и будет увеличиваться до максимального размера в 20 Гбайт по мере добавления данных.

Просмотреть **ID** (идентификатор) виртуального диска можно в меню **Хранилище → Диски**. Этот идентификатор служит для обозначения виртуального диска, поскольку название устройства (например, `/dev/vda0`) может поменяться, что приведёт в свою очередь к повреждению диска. Также просмотреть ID виртуального диска можно в `/dev/disk/by-id`.

Просмотреть **Виртуальный размер** диска можно в меню **Хранилище → Диски** и на вкладке **Диски** области подробного просмотра для доменов хранилищ, ВМ и шаблонов. Виртуальный размер — это общий объём дискового пространства, который может использовать ВМ. Таким образом это число, которое администратор указывает в поле **Размер (Гбайт)** при создании или изменении параметров виртуального диска.

Просмотреть **Фактический размер** диска можно на вкладке **Диски** области подробного просмотра доменов хранилищ и шаблонов. Фактический размер — это объём дискового пространства, выделенный виртуальной машине на текущий момент. Предварительно зарезервированные диски показывают одинаковое значение как для **Виртуального размера**, так и для **Фактического размера**. Диски разрежённого типа как правило показывают различные значения **Виртуального** и **Фактического размера**, в зависимости от того, сколько места было реально выделено диску в хранилище.

Примечание — при создании виртуального диска Cinder, формат и тип диска обрабатывается внутренними процессами Cinder, а не системой виртуализации ROSA Virtualization.

В **Табл. 13.1** описываются возможные сочетания форматов и типов, разрешённые для хранилищ в системе виртуализации ROSA Virtualization.

Табл. 13.1. Сочетания форматов и типов, разрешённые для хранилищ

Хранилище	Формат	Тип	Примечание
NFS	raw	Предварительное резервирование	Файл без форматирования, начальный размер которого равен объёму, определённому для виртуального диска
NFS	raw	Разрежённый	Файл без форматирования, начальный размер которого близок к нулю
NFS	QCOW2	Разрежённый	Файл в формате QCOW2, начальный размер которого близок к нулю
SAN	raw	Предварительное резервирование	Блочное устройство без форматирования, начальный размер которого равен объёму хранилища, выделенного для виртуального диска
SAN	QCOW2	Разрежённый	Блочное устройство, начальный размер которого намного меньше, чем размер, определённый для виртуального диска (на данный момент — 1 Гбайт). Выделяемое по мере необходимости пространство

Хранилище	Формат	Тип	Примечание
			форматируется как QCOW2 (на данный момент шаг выделения — 1 Гбайт)

13.3. Очистка после удаления для виртуальных дисков

Активация флага `wipe_after_delete`, представленного на Портале администрирования в виде флажка **Забить нулями после удаления**, заменяет старые данные нулями при удалении виртуального диска. При указанном значении «*неверно*» (по умолчанию флаг деактивирован) во время удаления диска блоки будут освобождены для повторного использования, но данные не будут стёрты. Следовательно, эти данные потенциально можно восстановить, так как блоки не были забиты нулями.

Флаг `wipe_after_delete` эффективен только для блочных хранилищ. В применении к файловому хранилищу, например NFS, этот параметр не имеет смысла, так как файловая система обеспечивает полное удаление данных.

Активация флага `wipe_after_delete` для виртуальных дисков является дополнительной защитой и рекомендуется в том случае, если на виртуальных дисках хранятся любые сведения конфиденциального характера.

Данная операция требует более интенсивных вычислительных затрат, чем операция стандартного удаления, и система может испытывать снижение производительности и необходимость в увеличенном времени для выполнения операции очистки после удаления.

Примечание — функциональность замены данных нулями не является аналогом защищённого удаления и не даёт гарантии того, что данные будут удалены из хранилища, но гарантирует то, что новые диски, созданные в том же хранилище, не предоставят доступ к предыдущим данным.

Значение по умолчанию для флага `wipe_after_delete` можно изменить на `true` во время процесса настройки или с помощью утилиты `engine-config` в виртуализированном ЦУ.

Примечание — изменение значения по умолчанию для флага `wipe_after_delete` не влияет на значение параметра **Забить нулями после удаления** для уже существующих дисков.

Установка значения по умолчанию `true` для параметра `SANWipeAfterDelete` с помощью утилиты настройки виртуализированного ЦУ

1. Запустите утилиту `engine-config` с опцией `--set` и указанным значением `true` для параметра `SANWipeAfterDelete`:

   ```
   # engine-config --set SANWipeAfterDelete=true
   ```

2. Перезапустите службу `ovirt-engine` для применения изменений:

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

Информация о выполнении операций очистки после удаления виртуальных дисков журналируется в файле `/var/log/vdsm/vdsm.log` на хосте.

В случае удачного заполнения нолями блоков диска журнал будет содержать следующую запись:

`id_домена_хранилища/id_тома` `was zeroed and will be deleted`

Например:

```
a9cb0625-d5dc-49ab-8ad1-722e82b0bf/a49351a7-15d8-4932-8d67-51a36f9d61
was zeroed and will be deleted
```

При неудачном заполнении нолями блоков диска журнал будет содержать следующую запись:

```
zeroing id_домена_хранилища/id_тома failed
Zero and remove this volume manually
```

В случае удачного удаления диска журнал будет содержать следующую запись:

```
finished with VG: id_домена_хранилища LVs: список_id_томов, img: id_образа
```

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
```

При неудачном удалении диска журнал будет содержать следующую запись:

```
Remove failed for some of VG: id_домена_хранилища zeroed volumes:
список_id_томов
```

13.4. Разделяемые диски

Некоторым приложениям необходимо, чтобы хранилище было общим хранилищем серверов. Система виртуализации ROSA Virtualization даёт возможность пометить жёсткие диски ВМ флажком **Может быть общим** и присоединять эти диски к ВМ. Таким образом один виртуальный диск может использоваться несколькими гостями с поддержкой кластеров.

Разделяемые диски не должны использоваться во всех ситуациях. Общие диски рекомендуются для таких применений как серверы баз данных, собранные в кластеры. Но присоединение общего диска ко многим гостям, не имеющим поддержки кластера, скорей всего вызовет повреждение данных, поскольку их операции чтения и записи на диск не скоординированы.

Для общего диска нельзя создать снимок. Виртуальные диски со сделанными снимками нельзя пометить как общие.

Установить флажок **Может быть общим** для диска возможно либо во время его создания, либо во время изменения параметров диска.

13.5. Диски с доступом только для чтения

Некоторым приложениям необходимо, чтобы разделяемые администраторами данные были доступны только для чтения. Данная возможность реализуется при создании или изменении параметров диска, присоединённого к ВМ, на вкладке **Диски** области подробного просмотра ВМ с помощью флажка **Только для чтения**. Таким образом один диск может читаться несколькими гостями с поддержкой кластера, а привилегии на запись остаются только у администратора.

Во время работы ВМ нельзя сменить состояние диска с установленным параметром **Только для чтения**.

Примечание — монтирование журналируемой файловой системы требует доступа на чтение и запись. Использование параметра **Только для чтения** не является

желательным для виртуальных дисков, содержащих такие файловые системы (например EXT3, EXT4 или XFS).

13.6. Работа с виртуальными дисками

13.6.1. Создание виртуального диска

Процесс создания дисков с типом **Образ** полностью управляется виртуализированным ЦУ. Диски с **Прямыми LUN** требуют уже существующих подготовленных внешних целей. Дискам **Cinder** необходим доступ к экземпляру тома OpenStack, который должен быть предварительно добавлен в окружение виртуализации ROSA Virtualization с помощью окна **Внешние поставщики**.

Создание виртуального диска, присоединённого к конкретной ВМ

1. Нажмите **Ресурсы → Виртуальные машины**.
2. Нажмите на имя ВМ, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Диски**.
4. Нажмите **Добавить**.
5. Перейдите на соответствующую вкладку, чтобы создать виртуальный диск с типом **Образ**, виртуальный диск с **Прямыми LUN** или виртуальный диск **Cinder** (Рис. 42).
6. Выберите параметры, требуемые для виртуального диска. Параметры изменяются в зависимости от выбранного типа диска.
7. Нажмите **OK**.

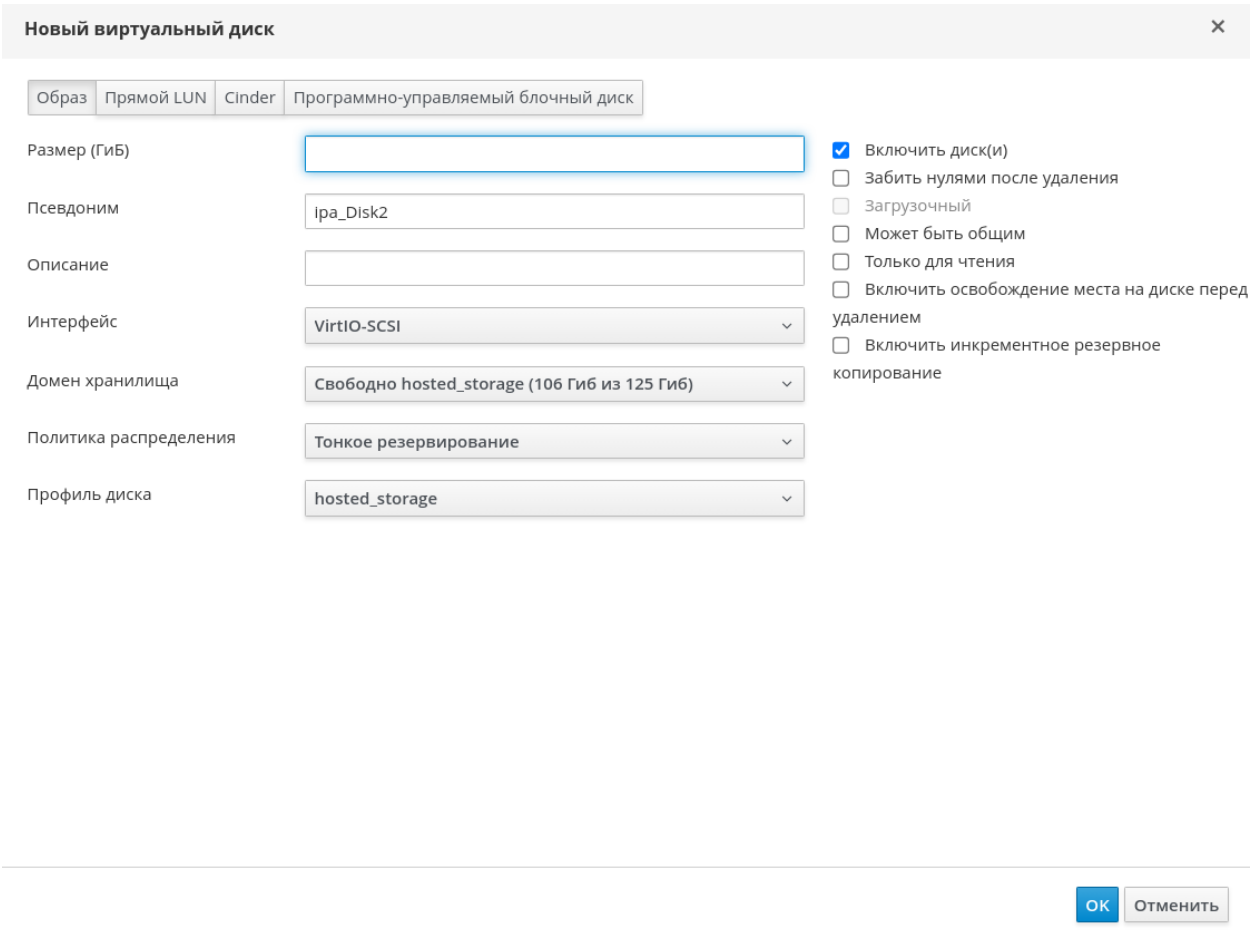

Рис. 42. Создание нового виртуального диска

Создание «плавающего» виртуального диска

При необходимости можно создать «плавающий» виртуальный диск, не принадлежащий ни одной ВМ. Этот диск можно присоединить к одной ВМ или к нескольким, а также этот диск может быть общим. При создании «плавающего» виртуального диска некоторые параметры будут недоступны (см. п. 13.6.2. Параметры виртуального диск).

1. Нажмите **Хранилище → Диски.**
2. Нажмите **Добавить**.
3. Нажмите на соответствующую кнопку, чтобы указать, будет ли виртуальный диск **Образом**, **Прямым LUN** или диском **Cinder**.
4. Выберите параметры, требуемые для виртуального диска. Параметры изменяются в зависимости от выбранного типа диска.
5. Нажмите **OK**.

Примечание — создание виртуальных дисков является экспериментальной функцией. Экспериментальные возможности не поддерживаются соглашениями об уровне обслуживания, могут иметь неполный функционал и не рекомендуются к использованию на производстве. Эти возможности предоставляют ранний доступ к будущим возможностям продукта, давая клиентам возможность протестировать функциональность и предоставить отзывы, полезные для разработчиков.

13.6.2. Параметры виртуального диска

13.6.2.1. Параметры образа виртуального диска

В **Табл. 13.2** описываются параметры образа виртуального диска в окнах **Новый виртуальный диск** и **Параметры виртуального диска**.

Табл. 13.2. Параметры образа виртуального диска

Поле	Описание
Размер (ГиБ)	Размер нового виртуального диска в Гбайт
Псевдоним	Название виртуального диска (ограничение — 40 символов)
Описание	Описание виртуального диска (необязательное, но рекомендуемое для заполнения поле)
Интерфейс	Виртуальный интерфейс, предоставляемый диском виртуальной машине (параметр доступен только при создании присоединённого диска). Тип интерфейса можно обновлять после остановки всех ВМ, к которым присоединён диск. Интерфейс **VirtIO** более быстрый, но требует специальных драйверов. В ОС семейства ROSA эти драйверы присутствуют. В ОС семейства Windows драйверы отсутствуют, но их можно установить с образа гостевых утилит или с виртуальной дискеты. Устройствам **IDE** специальные драйверы не требуются
Дата-центр	Дата-центр, в котором будет использоваться виртуальный диск (параметр доступен только при создании плавающих дисков)
Домен хранения	Домен хранения, в котором будет храниться виртуальный диск. В выпадающем списке показаны все домены хранилищ, доступные в указанном дата-центре, а также отображается общий объём хранилища в домене и объём, доступный на данный момент
Политика распределения	Политика распределения для нового виртуального диска. Для выбора доступны следующие значения: • **Предварительное резервирование.**

Поле	Описание
	Во время создания виртуального диска в домене хранилища выделяется весь объём диска. Виртуальный и зарезервированный размеры равны. На создание предварительно зарезервированного виртуального диска затрачивается больше времени, чем на создание виртуального диска тонкого резервирования, но они имеют лучшие показатели чтения и записи. Предварительно зарезервированные виртуальные диски рекомендуются для размещения серверов и других ВМ с интенсивными процессами ввода-вывода. Если ВМ в процессе работы записывает более 1 Гбайт каждые 4 секунды, при возможности используйте предварительно зарезервированные диски. • **Тонкое резервирование.** Во время создания виртуального диска выделяется 1 Гбайт хранилища и настраивается максимальный предел размера, до которого может вырасти диск. Виртуальный размер диска является максимальным пределом, а фактический размер — место, выделенное на данный момент. Диски тонкого резервирования создаются быстрее предварительно зарезервированных дисков и позволяют использовать превышенное выделение ресурсов хранилища. Виртуальные диски тонкого резервирования рекомендуются для рабочих столов.
Профиль диска	Профиль диска, присвоенный виртуальному диску. Профили дисков определяют максимальную пропускную способность и максимальный уровень операций ввода-вывода для виртуального диска в домене хранения. Профили дисков определяются на уровне домена хранения на основании записей о качестве обслуживания хранилищ, созданных для дата-центров
Включить диск(и)	Немедленная активация виртуального диска после создания (параметр доступен только при создании присоединённого диска)
Забить нулями после удаления	Параметр даёт возможность включить повышенную защиту в виде удаления конфиденциальной информации при удалении виртуальных дисков
Загрузочный	Параметр даёт возможность пометить виртуальный диск как загрузочный (параметр доступен только при создании присоединённого диска)
Может быть общим	Параметр даёт возможность присоединить виртуальный диск к нескольким виртуальным машинам одновременно
Только для чтения	Параметр даёт возможность предоставить доступ к виртуальному диску только для чтения (параметр доступен только при создании присоединённого диска). Один и тот же диск может быть доступен только для чтения для одной ВМ, но доступен для записи для другой ВМ
Освободить блоки	Параметр даёт возможность сжать диск тонкого резервирования во время работы ВМ (параметр доступен только при создании присоединённого диска). Если параметр включён, команды SCSI UNMAP, вызванные гостевой ВМ, передаются QEMU в базовое хранилище для освобождения неиспользуемого пространства. Базовое устройство блочного хранилища должно поддерживать вызовы discard, а параметр не может использоваться вместе с параметром **Забить нулями после удаления**, если только базовое хранилище не поддерживает свойство discard_zeroes_data. Для файлового хранилища соответствующая базовая файловая система и блочное устройство должны поддерживать вызовы discard
Включить инкрементное резервное копирование	Технологический параметр, который не используется (игнорируется) в процессе пользовательской настройки

13.6.2.2. Параметры виртуального диска с прямыми LUN

Параметр **Прямой LUN** может присутствовать либо в меню **Таргеты > LUN**, либо в меню **LUN > Таргеты**. Меню **Таргеты > LUN** сортирует доступные номера LUN согласно хостам, на которых обнаружены LUN, в то время как меню **LUN > Таргеты** отображает одиночный список LUN.

Для обнаружения целевого сервера заполните поля в разделе **Обнаружение таргетов** и нажмите кнопку **Обнаружить**. Далее нажмите кнопку **Выполнить вход для всех** для получения списка всех доступных LUN на целевом сервере, после чего с помощью переключателей рядом с каждым LUN, выберите добавляемые LUN.

Прямое использование LUN в качестве образов дисков ВМ удаляет слой абстракции между виртуальными машинами и данными.

При использовании прямых LUN в качестве образов жёстких дисков ВМ необходимо учитывать следующие особенности:

- Динамическая миграция прямых LUN в виде образов жёстких дисков в хранилище не поддерживается.
- Диски в виде прямых LUN не включаются в экспорт ВМ.
- Диски в виде прямых LUN не включаются в снимки ВМ.

В **Табл. 13.3** описываются параметры виртуального диска с прямыми LUN в окнах **Новый виртуальный диск** и **Параметры виртуального диска**.

Табл. 13.3. Параметры виртуального диска с прямыми LUN

Поле	Описание
Псевдоним	Название виртуального диска (ограничение — 40 символов)
Описание	Описание виртуального диска (необязательное, но рекомендуемое для заполнения поле). По умолчанию в поле присутствует 4 последних символа LUN ID. Поведение по умолчанию можно настроить, выставив соответствующее значение ключа `PopulateDirectLUNDiskDescriptionWithLUNId` с помощью команды `engine-config`. Ключ может иметь значение `-1` для использования полного идентификатора LUN, или `0`, чтобы эта возможность игнорировалась. При указании положительного целого числа описание заполняется соответствующим числом символов идентификатора LUN
Интерфейс	Виртуальный интерфейс, предоставляемый диском виртуальной машине (параметр доступен только при создании присоединённого диска). Тип интерфейса можно обновлять после остановки всех ВМ, к которым присоединён диск. Интерфейс **VirtIO** более быстрый, но требует специальных драйверов. В ОС семейства ROSA эти драйверы присутствуют. В ОС семейства Windows драйверы отсутствуют, но их можно установить с образа гостевых утилит или с виртуальной дискеты. Устройствам **IDE** специальные драйверы не требуются
Дата-центр	Дата-центр, в котором будет использоваться виртуальный диск (параметр доступен только при создании плавающих дисков)
Хост	Хост, на котором будет смонтирован LUN. Можно выбрать любой хост в дата-центре
Тип хранилища	Тип добавляемых внешних LUN. Для выбора доступны значения **iSCSI** или **Оптоволокно**
Обнаружение целей	При использовании внешних LUN iSCSI и выбранном меню **Таргеты > LUN**, в разделе **Обнаружение целей** будут доступны следующие поля:

	• **Адрес** — имя хоста или IP-адрес целевого сервера. • **Порт** — порт, с которого будет выполняться подключение к целевому серверу. Номер порта по умолчанию — 3260. • **Аутентификация пользователя** — установите этот флажок для аутентификации пользователя на сервере iSCSI. • **Имя пользователя CHAP** — имя пользователя, имеющего полномочия входа в систему на LUN. Это поле становится видимым при отмеченном пункте **Аутентификация пользователя**. • **Пароль CHAP** — пароль пользователя, имеющего полномочия входа в систему на LUN. Это поле становится видимым при отмеченном пункте **Аутентификация пользователя**.
Активировать диск(и)	Немедленная активация виртуального диска после создания (параметр доступен только при создании присоединённого диска)
Загрузочный	Параметр даёт возможность пометить виртуальный диск как загрузочный (параметр доступен только при создании присоединённого диска)
Может быть общим	Параметр даёт возможность присоединить виртуальный диск к нескольким виртуальным машинам одновременно
Только для чтения	Параметр даёт возможность предоставить доступ к виртуальному диску только для чтения (параметр доступен только при создании присоединённого диска). Один и тот же диск может быть доступен только для чтения для одной ВМ, но доступен для записи для другой ВМ
Включить освобождение блоков	Параметр даёт возможность сжать диск тонкого резервирования во время работы ВМ (параметр доступен только при создании присоединённого диска). Если параметр включён, команды SCSI UNMAP, вызванные гостевой ВМ, передаются QEMU в базовое хранилище для освобождения неиспользуемого пространства
Включить сквозной доступ к SCSI	Параметр доступен только при создании присоединённого диска и в случае, когда для параметра **Интерфейс** указано значение **VirtIO-SCSI**. Выбор этого флажка включает сквозной доступ виртуального диска к физическому устройству SCSI. Интерфейс VirtIO-SCSI с включённым сквозным доступом к SCSI автоматически включает в себя поддержку освобождения блоков. Если этот флажок отмечен, параметр **Только для чтения** не поддерживается. Если этот параметр не отмечен, виртуальное устройство использует эмулируемое устройство SCSI. Для эмулируемых дисков VirtIO-SCSI поддерживается параметр **Только для чтения**
Включить привилегированный ввод-вывод SCSI	Параметр доступен только при создании присоединённого диска и при выбранном параметре **Включить сквозной доступ к SCSI**. Выбор этого параметра включает доступ SCSI Generic I/O (SG_IO) без фильтрации, разрешая привилегированные команды SG_IO для диска. Этот параметр требуется для постоянного резервирования
Использует резервирование SCSI	Параметр доступен только при создании присоединённого диска и при выбранных параметрах **Включить сквозной доступ к SCSI** и **Включить привилегированный ввод-вывод SCSI**. Выбор этого параметра отключает возможность миграции для любой ВМ, использующей этот диск, с целью предотвращения потери доступа к диску со стороны ВМ, использующих резервирование SCSI

13.6.2.3. Параметры виртуального диска Cinder

Для виртуальных дисков Cinder требуется доступ к экземпляру тома OpenStack, который был добавлен в окружение виртуализации ROSA Virtualization с помощью окна **Внешние поставщики**.

При отсутствии доступных доменов хранения томов OpenStack, для которых имеются разрешения на создание дисков в соответствующих дата-центрах, интерфейс настройки параметров виртуальных дисков Cinder будет недоступен.

В **Табл. 13.4** описываются параметры виртуального диска Cinder в окнах **Новый виртуальный диск** и **Параметры виртуального диска**.

Табл. 13.4. Параметры виртуального диска Cinder

Поле	Описание
Размер (Гбайт)	Размер нового виртуального диска в Гбайт
Псевдоним	Название виртуального диска (ограничение — 40 символов)
Описание	Описание виртуального диска (необязательное, но рекомендуемое для заполнения поле)
Интерфейс	Виртуальный интерфейс, предоставляемый диском виртуальной машине (параметр доступен только при создании присоединённого диска). Тип интерфейса можно обновлять после остановки всех ВМ, к которым присоединён диск. Интерфейс **VirtIO** более быстрый, но требует специальных драйверов. В ОС семейства ROSA эти драйверы присутствуют. В ОС семейства Windows драйверы отсутствуют, но их можно установить с образа гостевых утилит или с виртуальной дискеты. Устройствам **IDE** специальные драйверы не требуются
Дата-центр	Дата-центр, в котором будет использоваться виртуальный диск (параметр доступен только при создании плавающих дисков)
Домен хранения	Домен хранения, в котором будет располагаться виртуальный диск. В выпадающем списке показываются все домены хранилищ, доступные в указанном дата-центре, а также отображается общий объём хранилища в домене и объём, доступный на данный момент
Тип тома	Тип тома виртуального диска. В выпадающем списке показываются все доступные типы томов. Тип тома будет управляться и настраиваться в OpenStack Cinder
Активировать диск(и)	Немедленная активация виртуального диска после создания (параметр доступен только при создании присоединённого диска)
Загрузочный	Параметр даёт возможность пометить виртуальный диск как загрузочный (параметр доступен только при создании присоединённого диска)
Может быть общим	Параметр даёт возможность присоединить виртуальный диск к нескольким виртуальным машинам одновременно
Только для чтения	Параметр даёт возможность предоставить доступ к виртуальному диску только для чтения (параметр доступен только при создании присоединённого диска). Один и тот же диск может быть доступен только для чтения для одной ВМ, но доступен для записи для другой ВМ

13.6.3. Обзор процесса динамической миграции между хранилищами

Существует возможность выполнения миграции виртуальных дисков из одного домена хранения в другой во время работы ВМ, к которой эти диски присоединены. Этот процесс называется динамической миграцией. При миграции диска, присоединённого к выполняющейся ВМ, в исходном домене хранения создаётся снимок цепочки образа этого диска, и вся эта цепочка образа реплицируется в целевом домене. Поэтому необходимо убедиться в том, что в доменах хранения (исходном и целевом) существует свободное дисковое пространство для размещения цепочки образа диска и снимка. При каждой

попытке динамической миграции между хранилищами создаётся новый снимок, даже если эта попытка будет неудачной.

При использовании динамической миграции между хранилищами учитывайте следующие особенности процесса:

- Динамическая миграция может осуществляться для нескольких дисков одновременно.
- Несколько дисков одной ВМ могут располагаться более, чем в одном домене хранилищ, но цепочки образов каждого диска должны располагаться в одном домене.
- Динамическая миграция может проводиться между двумя любыми доменами хранения в одном дата-центре.
- Не поддерживается динамическая миграция образов жёстких дисков с прямыми LUN или общих дисков.

13.6.4. Перемещение виртуальных дисков

В следующей последовательности действий описывается процесс перемещения виртуального диска, присоединённого к ВМ или «плавающего» виртуального диска из одного домена хранения в другой.

При перемещении виртуальных дисков поддерживается динамическая миграция, таким образом диски, присоединённые к выполняющейся ВМ, также можно перемещать, или как вариант, завершите работу ВМ перед началом миграции.

При перемещении виртуальных дисков учитывайте следующие особенности процесса:

- Возможно перемещение нескольких виртуальных дисков одновременно.
- Диски могут перемещаться между двумя любыми доменами хранения одного дата-центра.
- Если виртуальный диск присоединён к ВМ, созданной на базе шаблона с использованием тонкого резервирования пространства в хранилище, необходимо скопировать диски, на базе которых был создан шаблон, в тот же домен хранения, что и виртуальный диск.

Перемещение виртуального диска

1. Нажмите **Хранилище → Диски** и выберите один или несколько виртуальных дисков для перемещения.
2. Нажмите **Переместить**.
3. В списке **Таргет** выберите домен хранения, в который будет перемещён виртуальный диск.
4. При необходимости в списке **Профиль диска** выберите профиль диска.
5. Нажмите **OK**.

В результате выбранные виртуальные диски будут перемещены в целевой домен хранения. Во время процесса перемещения в столбце **Статус** будет отображаться надпись `Заблокировано`, а ход процесса будет показан в виде индикатора прогресса.

13.6.5. Изменение типа интерфейса диска

После создания диска пользователь может изменить тип интерфейса диска. Это даёт возможность присоединить уже существующий диск к ВМ, требующей другого типа интерфейса. Например диск, использующий интерфейс `VirtIO`, можно присоединить к ВМ,

требующей интерфейс VirtIO-SCSI или IDE. Эта возможность предоставляет гибкость в осуществлении миграции дисков в целях создания и восстановления резервных копий или восстановления после сбоев. Тип интерфейса общих дисков также можно обновлять для каждой из ВМ. Это означает, что каждая ВМ, использующая разделяемые диски, может использовать различные типы интерфейсов.

Перед изменением типа интерфейса диска, работа всех ВМ, использующих этот диск, должна быть остановлена.

Изменение типа интерфейса диска

1. Нажмите **Ресурсы → Виртуальные машины** и остановите работу необходимых ВМ.
2. Нажмите на имя ВМ, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Диски** и выберите диск.
4. Нажмите **Изменить.**
5. Из выпадающего списка **Интерфейс** выберите новый тип интерфейса.
6. Нажмите **OK.**

Также диск можно присоединять к различным ВМ, требующим другого типа интерфейса.

Присоединение диска к ВМ, использующим другой тип интерфейса

1. Нажмите **Ресурсы → Виртуальные машины** и остановите работу соответствующих ВМ.
2. Нажмите на имя ВМ, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Диски** и выберите диск.
4. Нажмите **Удалить**, затем нажмите **OK.**
5. Вернитесь в меню **ВМ** и нажмите на имя новой ВМ, к которой будет присоединён диск.
6. Перейдите на вкладку **Диски**, затем нажмите **Присоединить.**
7. Выберите диск в окне **Присоединить виртуальные диски** и выберите соответствующий интерфейс из выпадающего списка **Интерфейс.**
8. Нажмите **OK.**

13.6.6. Копирование виртуальных дисков

Виртуальный диск можно скопировать из одного домена хранения в другой. После чего скопированный диск можно присоединять к виртуальным машинам.

Копирование виртуального диска

1. Нажмите **Хранилище → Диски** и выберите один или несколько виртуальных дисков.
2. Нажмите **Копировать.**
3. Опционально введите новое имя в поле **Псевдоним.**
4. В списке **Таргет** выберите домен хранения, в который будут скопированы виртуальные диски.
5. При необходимости в списке **Профиль диска** выберите профиль диска.
6. Нажмите **OK.**

В результате выбранные виртуальные диски будут скопированы в целевой домен хранения. Во время процесса копирования в столбце **Статус** будет отображаться надпись Заблокировано, а ход процесса будет показан в виде индикатора прогресса.

13.6.7. Отправка образов в домен хранения данных

Отправить образы виртуальных дисков и образы ISO в домен хранения данных можно на Портале администрирования или с помощью REST API.

13.6.8. Импорт образов дисков из импортированного домена хранения

«Плавающие» виртуальные диски можно импортировать из домена хранения.

Примечание — в виртуализированный ЦУ можно импортировать только диски, совместимые с QEMU.

Импорт образа диска

1. Нажмите **Хранилище → Домены**.
2. Нажмите на имя импортированного домена хранения, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Импорт диска**.
4. Выберите один или несколько образов дисков и нажмите **Импортировать**.
5. Выберите соответствующий **Профиль диска** для каждого диска.
6. Нажмите **OK**.

13.6.9. Импорт незарегистрированного образа диска из импортированного домена хранения

«Плавающие» виртуальные диски, созданные вне окружения виртуализации ROSA Virtualization, не регистрируются виртуализированным ЦУ.

Выполните сканирование домена хранения для опознания незарегистрированных «плавающих» дисков для их последующего импорта.

Примечание — в виртуализированный ЦУ можно импортировать только диски, совместимые с QEMU.

Импорт незарегистрированного образа диска

1. Нажмите **Хранилище → Домены**.
2. Нажмите на имя импортированного домена хранения, чтобы перейти к подробному просмотру.
3. Нажмите **Больше действий** (⋮), затем нажмите **Сканирование дисков**, чтобы виртуализированный ЦУ идентифицировал незарегистрированные виртуальные диски.
4. Перейдите на вкладку **Импорт дисков**.
5. Выберите один или несколько образов дисков и нажмите **Импортировать**.
6. Выберите соответствующий **Профиль диска** для каждого диска.
7. Нажмите **OK**.

13.6.10. Импорт виртуальных дисков из службы образов OpenStack

Виртуальные диски, управляемые службой образов OpenStack, можно импортировать в виртуализированный ЦУ. При этом служба образов OpenStack ранее должна быть добавлена в виртуализированный ЦУ в качестве внешнего поставщика.

Импорт виртуального диска из службы образов OpenStack

1. Нажмите **Хранилище → Домены**.

2. Нажмите на имя домена службы образов OpenStack, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Образы** и выберите образ.
4. Нажмите **Импорт**.
5. Выберите **Дата-центр**, в который будет импортирован образ.
6. Из выпадающего списка **Имя домена** выберите домен хранения, в котором будет храниться образ.
7. Опционально в списке **Квота** выберите квоту, применяемую к образу.
8. Нажмите **ОК**.

При необходимости после импорта виртуальный диск можно присоединить к ВМ.

13.6.11. Экспорт виртуальных дисков в службу образов OpenStack

Виртуальные диски могут быть экспортированы в службу образов OpenStack, которая ранее должна быть добавлена в виртуализированный ЦУ в качестве внешнего поставщика.

Примечание — экспорт виртуальных дисков возможен, только в том случае, если у дисков отсутствуют множественные тома, диски не имеют снимков и не являются дисками тонкого резервирования.

Экспорт виртуального диска в службу образов OpenStack

1. Нажмите **Хранилище** → **Диски** и выберите один или несколько экспортируемых дисков.
2. Нажмите **Больше действий** (⋮), затем нажмите **Экспорт**.
3. Из выпадающего списка **Имя домена** выберите службу образов OpenStack, в которую будут экспортированы диски.
4. Опционально в списке **Квота** выберите квоту, применяемую к дискам.
5. Нажмите **ОК**.

13.6.12. Возвращение хосту дискового пространства, ранее используемого виртуальными дисками

Виртуальные диски, использующие тонкое резервирование пространства в хранилище, не сжимаются автоматически после удаления файлов. Например, если фактический размер диска равен 100 Гбайт, и будет удалено 50 Гбайт файлов, выделенное пространство диска по-прежнему останется 100 Гбайт, а оставшиеся 50 Гбайт не возвращаются хосту и соответственно не могут использоваться виртуальными машинами.

Для того, чтобы вернуть хосту неиспользуемое дисковое пространство выполните процедуру разреживания диска ВМ, в результате которой свободное пространство переносится с образа диска на хост. При этом разреживать можно несколько дисков одновременно.

Рекомендуется выполнять разреживание диска перед клонированием ВМ, созданием шаблона на базе ВМ или очисткой пространства на диске в домене хранения.

Процедура разреживания диска имеет ряд следующих ограничений:

- Домены хранения NFS должны использовать версию NFS 4.2 или выше.
- Нельзя разреживать диск, использующий прямой LUN.
- Нельзя разреживать диск Cinder.
- Нельзя разреживать диск, использующий политику предварительного резервирования пространства в хранилище.

Примечание — при создании ВМ из шаблона выберите параметр **Тонкое** в поле **Резервирование хранилища**, или при выборе **Клонирования**, убедитесь в том, что шаблон основан на ВМ с тонким резервированием.

- Разреживать можно только активные снимки дисков.

Разреживание диска

1. Нажмите **Ресурсы → Виртуальные машины** и выключите необходимую ВМ.
2. Нажмите на имя ВМ, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Диски** и убедитесь в том, что диск имеет статус `OK`.
4. Нажмите **Больше действий** (⋮), затем нажмите **Разредить**.
5. Нажмите **OK**.

В процессе разреживания диска на вкладке **События** появится сообщение `Начало разреживания`, при этом статус диска изменится на значение `Заблокировано`.

После завершения разреживания диска на вкладке **События** появится сообщение `Разрежено успешно`, при этом статус диска изменится на значение `OK`.

В результате неиспользуемое дисковое пространство будет возвращено хосту и станет доступно для использования другими ВМ.

Глава 14. Настройка двухфакторной аутентификации

14.1. Двухфакторная аутентификация на Портале администрирования с использованием «Рутокен ЭЦП»

Двухфакторная аутентификация на Портале администрирования системы виртуализации ROSA Virtualization основана на токене (в качестве примера используется «Рутокен ЭЦП») с закрытым ключом и сертификатом ключа, а также имени и пароле пользователя, осуществляющего вход на Портал администрирования.

Для обеспечения данного процесса потребуется замена корневого сертификата ЦС виртуализированного ЦУ на корневой сертификат ЦС сервера IPA, так как генерация закрытых ключей и сертификатов для пользователей ROSA Virtualization будет осуществляться на сервере IPA.

Примечание — для замены корневого сертификата ЦС виртуализированного ЦУ необходимо наличие как минимум двух хостов, чтобы обеспечить возможность миграции виртуальных машин для последующей переустановки всех подключенных хостов. Крайне не рекомендуется перезагружать хосты до полного завершения процедуры замены сертификата.

14.1.1. Замена сертификата ЦС виртуализированного ЦУ

Сертификат ЦС виртуализированного ЦУ должен быть заменен на сертификат ЦС сервера IPA из файла `/root/cacert.p12`, который создаётся в процессе установки сервера IPA.

Примечание — файл `/root/cacert.p12` защищен паролем пользователя Directory Manager, указанным при установке сервера IPA.

Для извлечения сертификата ЦС сервера IPA из файла `/root/cacert.p12` перейдите в консоли сервера IPA в директорию `/root` и выполните следующие команды в зависимости от версии установленных пакетов `openssl` и `ipa-server` (при выводе запроса на ввод пароля `Enter Import Password` введите пароль пользователя Directory Manager):

- `openssl.x86_64_1.1.1g` и `ipa-server.x86_64_4.8.7`:

```
# openssl pkcs12 -in cacert.p12 -nodes -nokeys | sed -n '/subject=.*CN.*=.*Certificate Authority/,/^-----END CERTIFICATE-----/p' | sed -n '/^-----BEGIN CERTIFICATE-----/,/^-----END CERTIFICATE-----/p' > ipa-ca.pem
Enter Import Password: <пароль Directory Manager сервера IPA>
```

```
# openssl pkcs12 -in cacert.p12 -nodes -nocerts | sed -n '/friendlyName: caSigningCert cert-pki-ca/,/^-----END PRIVATE KEY-----/p' | sed -n '/^-----BEGIN PRIVATE KEY-----/,/^-----END PRIVATE KEY-----/p' > ipa-ca.key
Enter Import Password: <пароль Directory Manager сервера IPA>
```

При выполнении эти команды извлекают сертификат ЦС сервера IPA (`subject=O = EXAMPLE.COM, CN = Certificate Authority`) и закрытый ключ (`friendlyName: caSigningCert cert-pki-ca`) из файла `cacert.p12`, и сохраняют их соответственно в файлы `ipa-ca.pem` и `ipa-ca.key` в текущей директории `/root` сервера IPA.

- `openssl.x86_64_1.0.2k` и `ipa-server.x86_64_4.6.5`:

```
# openssl pkcs12 -in cacert.p12 -nodes -nokeys | sed -n
'/subject=.*CN.*=.*Certificate Authority/,/^-----END CERTIFICATE-----
/p' | sed -n '/^-----BEGIN CERTIFICATE-----/,/^-----END CERTIFICATE----
-/p' > ipa-ca.pem
Enter Import Password: <пароль Directory Manager сервера IPA>

# openssl pkcs12 -in cacert.p12 -nodes -nocerts | sed -n '/friendlyName:
CN=Certificate Authority/,/^-----END PRIVATE KEY-----/p' | sed '1,2d' >
ipa-ca.key
Enter Import Password: <пароль Directory Manager сервера IPA>
```

При выполнении эти команды извлекают сертификат ЦС сервера IPA (`subject=/O=EXAMPLE.COM/CN=Certificate Authority`) и закрытый ключ (`friendlyName: CN=Certificate Authority,O=EXAMPLE.COM`) из файла `cacert.p12`, и сохраняют их соответственно в файлы `ipa-ca.pem` и `ipa-ca.key` в текущей директории `/root` сервера IPA.

Далее скопируйте файл сертификата `ipa-ca.pem` с сервера IPA на ВМ виртуализированного ЦУ в директорию `/etc/pki/ovirt-engine`, а файл закрытого ключа `ipa-ca.key` в директорию `/etc/pki/ovirt-engine/private`.

Замена корневого сертификата ЦС выполняется с помощью скрипта `ovirt-pki-enroll`. Создайте файл `ovirt_hosts` в той директории, из которой предполагается запускать этот скрипт (например, в директории `/root`). В этом файле должны быть прописаны полные доменные имена всех хостов, подключенных к виртуализированному ЦУ.

Файл `ovirt_hosts` имеет следующий формат:

```
[ovirt_hosts]
rosa-virt01.example.com
rosa-virt02.example.com
```

Замена сертификата ЦС осуществляется в режиме глобального обслуживания. На одном из хостов с установленным гипервизором, входящем в состав виртуализированного ЦУ, включите режим глобального обслуживания:

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

Для замены сертификата ЦС выполните следующую команду в консоли ВМ виртуализированного ЦУ:

```
# ovirt-pki-enroll --name=ipa-ca --new-key
```

В приведенной команде опция `--name` указывает на общую часть в именах файлов сертификата ЦС и закрытого ключа (в данном случае `ipa-ca` от ipa-ca.pem и ipa-ca.key, которые были скопированы в /etc/pki/ovirt-engine и /etc/pki/ovirt-engine/private соответственно), а опция `--new-key` указывает на необходимость пересоздать закрытые ключи.

Для применения изменений перезапустите следующие службы:

```
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-provider-ovn
# systemctl restart ovirt-imageio
# systemctl restart httpd
```

После пересоздания закрытых ключей восстановите работу компонента `ovirt-provider-ovn`. Для этого на Портале администрирования выберите пункт меню "**Администрирование**" → "**Поставщики**", далее выберите строку **ovirt-provider-ovn** и нажмите кнопку "**Изменить**", чтобы открыть окно "**Параметры поставщика**" (Рис. 43).

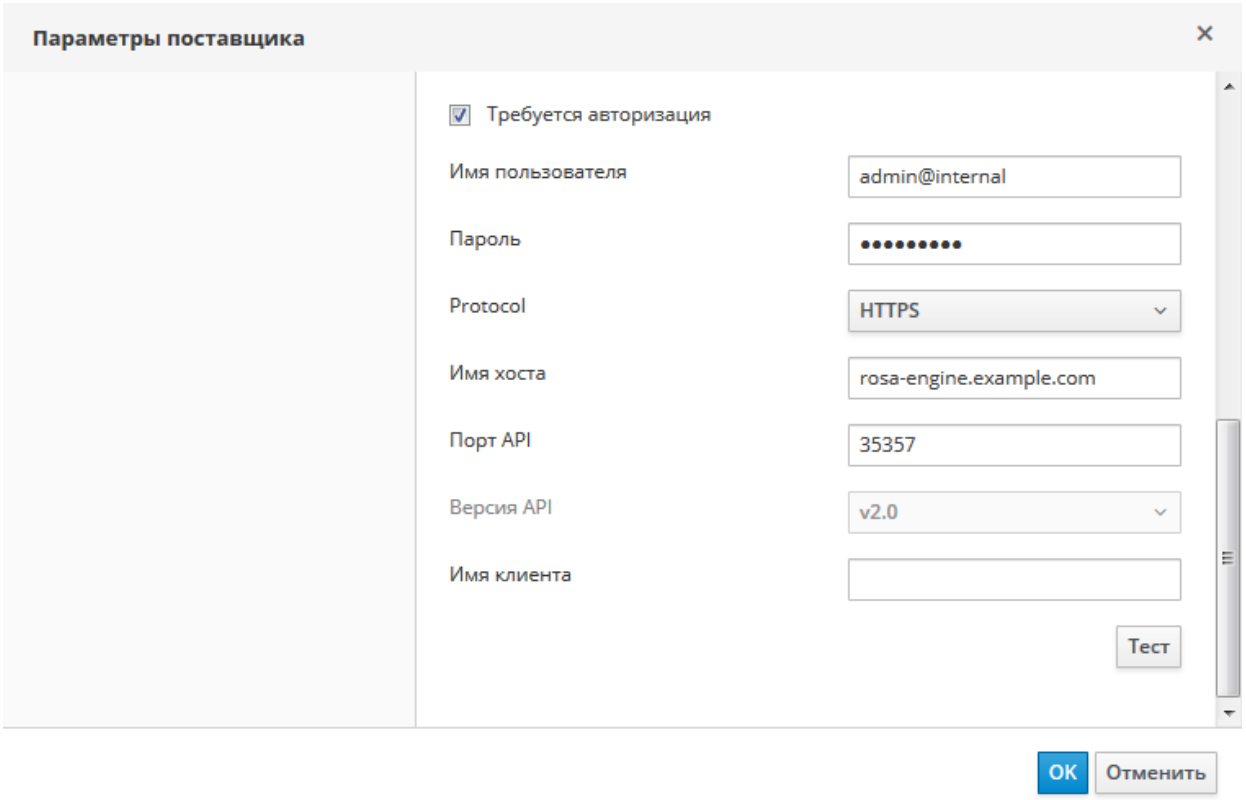

Рис. 43. Изменение параметров поставщика

В открывшемся окне введите пароль для пользователя `admin@internal` (учётная запись администратора во внутреннем домене виртуализированного ЦУ). Далее нажмите кнопку "**Тест**" и согласитесь с импортированием сертификата. После удачного завершения теста нажмите кнопку "**ОК**".

Для замены сертификатов на хостах выполните переустановку всех хостов. Для этого на Портале администрирования выберите пункт меню "**Ресурсы**" → "**Хосты**". Далее для перевода хоста в режим обслуживания нажмите "**Управление**" → "**Обслуживание**". Затем для запуска переустановки хоста нажмите "**Установка**" → "**Переустановить**".

Примечание — хост с запущенной ВМ виртуализированного ЦУ переустанавливается в последнюю очередь. Если процедура миграции ВМ виртуализированного ЦУ заканчивается ошибкой, то достаточно завершить работу хоста с запущенной ВМ виртуализированного ЦУ и дождаться запуска ВМ виртуализированного ЦУ на любом другом уже переустановленном хосте. После чего вновь запустить отключенный хост и выполнить переустановку этого хоста.

Для завершения процедуры замены сертификата ЦС виртуализированного ЦУ отключите режим глобального обслуживания:

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

14.1.2. Генерация закрытого ключа и сертификата для пользователя

Генерация закрытого ключа и сертификата ключа для необходимого пользователя (например, для пользователя `ovirtadmin`) осуществляется в консоли сервера IPA.

При необходимости для создания пользователя `ovirtadmin` выполните следующие команды:

```
# kinit admin
# ipa user-add ovirtadmin --first=ovirtadmin --last=ovirtadmin
```

Создайте закрытый ключ и запрос на выпуск сертификата для пользователя `ovirtadmin` следующим образом:

```
# openssl req -new -sha256 -nodes -newkey rsa:2048 -keyout ovirtadmin.key
-out ovirtadmin.csr -subj '/CN=ovirtadmin/O=EXAMPLE.COM'
```

В результате выполнения приведенной команды будут созданы в текущей директории файл `ovirtadmin.key` с закрытым ключом и файл `ovirtadmin.csr` с запросом на выпуск сертификата ключа.

Создайте сертификат ключа для пользователя `ovirtadmin`, используя файл `ovirtadmin.csr` с запросом на выпуск сертификата:

```
# ipa cert-request ovirtadmin.csr --principal=ovirtadmin --certificate-
out=ovirtadmin.pem
```

В результате выполнения приведенной команды будет создан в текущей директории файл `ovirtadmin.pem` с сертификатом ключа.

Примечание — закрытые ключи и сертификаты ключей для других пользователей, которые должны иметь доступ на Портал администрирования с использованием двухфакторной аутентификации, создаются аналогичным способом.

Если импорт закрытого ключа и сертификата ключа на токен пользователя будет осуществляться под управлением ОС семейства Windows предварительно создайте в текущей директории файл `ovirtadmin.p12`, содержащий закрытый ключ и сертификат ключа:

```
# openssl pkcs12 -export -out ovirtadmin.p12 -inkey ovirtadmin.key -in
ovirtadmin.pem
```

14.1.3. Импорт закрытого ключа и сертификата на «Рутокен ЭЦП»

Импорт закрытого ключа и сертификата на предварительно подготовленный к работе «Рутокен ЭЦП» может осуществляться как под управлением ОС семейства ROSA (например, ROSA Desktop Cobalt), так и под управлением ОС семейства Windows (например, Windows 10).

14.1.3.1. Подготовка «Рутокен ЭЦП» в ОС ROSA Desktop Cobalt

Для работы с «Рутокен ЭЦП» установите в систему библиотеку `rtPKCS11ecp` для ОС GNU/Linux, доступную на странице https://www.rutoken.ru/support/download/pkcs/ и утилиту администрирования токена `rtadmin` для ОС GNU/Linux, доступную на странице https://dev.rutoken.ru/pages/viewpage.action?pageId=7995615.

Примечание — после установки в систему библиотека `rtPKCS11ecp` будет вызываться из файла `/usr/lib64/librtpkcs11ecp.so`.

При необходимости выполните следующие команды для создания симлинка, чтобы обеспечить корректную работу утилиты `rtadmin` в ОС ROSA Desktop Cobalt:

```
# cd /usr/lib64/
# ln -s libdl.so.2 libdl.so
```

Также установите в систему дополнительные пакеты `opensc`, `pcsc-lite`, `pcsc-lite-ccid`. Для этого выполните следующую команду в консоли ОС ROSA Desktop Cobalt:

```
# yum install opensc
```

В процессе установки пакета `opensc` будут автоматически установлены необходимые дополнительные пакеты `pcsc-lite`, `pcsc-lite-ccid` в качестве зависимостей.

Для применения изменений перезагрузите компьютер.

Подключите «Рутокен ЭЦП» к USB-порту компьютера и выполните следующую команду для проверки работоспособности токена:

```
# pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -T
Available slots:
Slot 0 (0x0): Aktiv Rutoken ECP 00 00
  token label        : Rutoken
  token manufacturer : Aktiv Co.
  token model        : Rutoken ECP
  token flags          : login required, rng, token initialized, PIN
initialized
  hardware version   : 20.5
  firmware version   : 23.2
  serial num         : 3ac65c5d
  pin min/max        : 6/32
```

Для форматирования «Рутокен ЭЦП» выполните следующую команду:

```
$ ./rtadmin -f -q -z /usr/lib64/librtpkcs11ecp.so –a <PIN-код
администратора> -u <PIN-код пользователя>
```

Далее скопируйте с сервера IPA на компьютер с ОС ROSA Desktop Cobalt предварительно подготовленный файл `ovirtadmin.key` с закрытым ключом и файл `ovirtadmin.pem` с сертификатом ключа.

Выполните следующие команды, чтобы сконвертировать файлы `ovirtadmin.key` и `ovirtadmin.pem` в формат DER:

```
$ openssl rsa -in ovirtadmin.key -out ovirtadmin_key.der -outform DER
$ openssl x509 -in ovirtadmin.pem -out ovirtadmin_cert.der -outform DER
```

Для импорта закрытого ключа и сертификата ключа на «Рутокен ЭЦП» выполните следующие команды:

```
$ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l -y privkey -w
ovirtadmin_key.der --id 10 --label login_ovirtadmin
Please enter User PIN: <PIN-код пользователя>
```

```
$ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l -y cert -w
ovirtadmin_cert.der --id 10 --label login_ovirtadmin
Please enter User PIN: <PIN-код пользователя>
```

Для просмотра объектов, записанных на «Рутокен ЭЦП» выполните следующую команду:

```
# pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -O -l
Using slot 0 with a present token (0x0)
Logging in to "Rutoken".
Please enter User PIN: <PIN-код пользователя>
Private Key Object; RSA
  label:      login_ovirtadmin
  ID:         10
  Usage:      decrypt, sign
  Access:     sensitive
Certificate Object; type = X.509 cert
  label:      login_ovirtadmin
  subject:    DN: O=EXAMPLE.COM, CN=ovirtadmin
  ID:         10
```

14.1.3.2. Подготовка «Рутокен ЭЦП» в ОС Windows 10

Для работы с «Рутокен ЭЦП» установите в систему библиотеку `rtPKCS11ecp` для ОС Windows, доступную на странице https://www.rutoken.ru/support/download/pkcs/ и распространяемую в составе драйверов «Рутокен ЭЦП», а также утилиту администрирования токена `rtadmin` для ОС Windows, доступную на странице https://dev.rutoken.ru/pages/viewpage.action?pageId=7995615.

Примечание — после установки в систему библиотека `rtPKCS11ecp` будет вызываться из файла `C:\Windows\System32\rtPKCS11ECP.dll`.

Подключите «Рутокен ЭЦП» к USB-порту компьютера.

Для форматирования «Рутокен ЭЦП» выполните следующую команду:

```
rtadmin.exe -f -q -z C:\Windows\System32\rtPKCS11ECP.dll -a <PIN-код администратора> -u <PIN-код пользователя>
```

Далее скопируйте с сервера IPA на компьютер с ОС Windows 10 предварительно подготовленный файл `ovirtadmin.p12`, содержащий закрытый ключ и сертификат ключа.

Для импорта закрытого ключа и сертификата ключа на «Рутокен ЭЦП» запустите Панель управления Рутокен (Рис. 44), где на вкладке **Сертификаты** выберите необходимый токен и нажмите кнопку **Импортировать**. Затем укажите путь к файлу `ovirtadmin.p12` и нажмите кнопку **Открыть**.

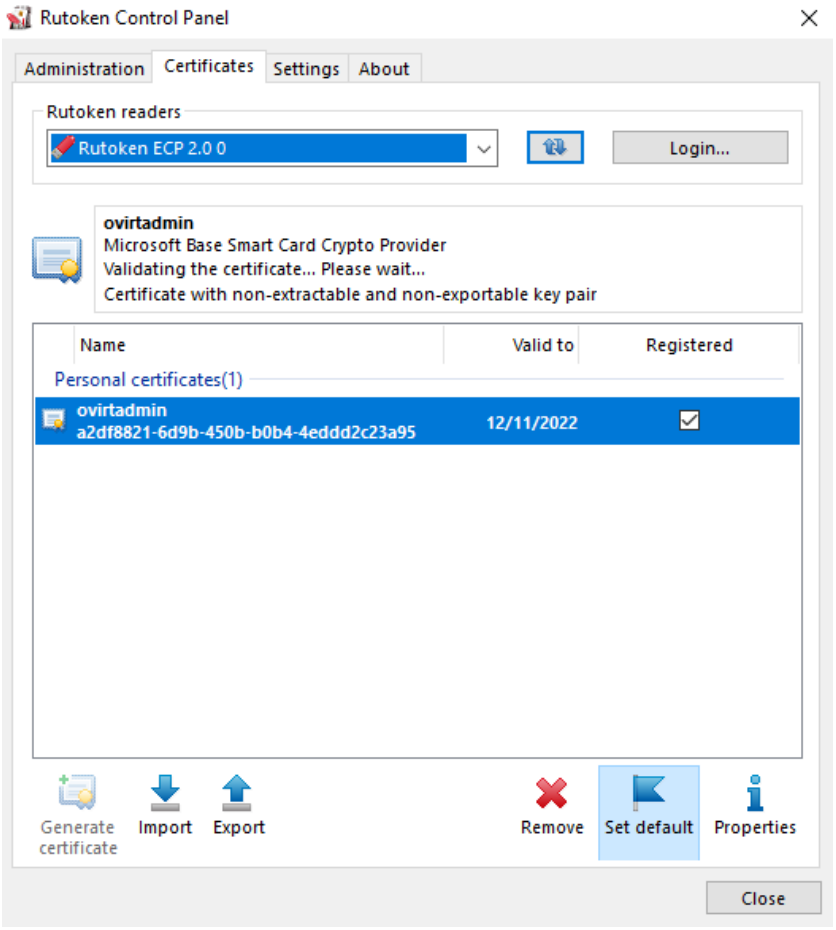

Рис. 44. Панель управления Рутокен

14.1.4. Настройка конфигурации веб-сервера Apache

Для обеспечения возможности двухфакторной аутентификации на Портале администрирования системы виртуализации ROSA Virtualization создайте конфигурационный файл `/etc/httpd/conf.d/certs-verify.conf` для веб-сервера Apache со следующими строками:

```
RequestHeader set X-Cert-User "%{SSL_CLIENT_S_DN_CN}s"
<LocationMatch ^/ovirt-engine/sso/(interactive-login-negotiate|oauth/
token-http-auth)>
  SSLVerifyClient require
  SSLVerifyDepth 10
</LocationMatch>
```

Также отредактируйте файл `/etc/ovirt-engine/engine.conf.d/60-ovirt-2fa.conf`, где для переменной TWO_FACTOR_AUTHENTICATION установите значение true (`TWO_FACTOR_AUTHENTICATION=true`), а для переменной OVIRT_ADMIN_LOGIN (сертификат для этого пользователя (логин учётной записи на сервере IPA) будет сопоставлен с внутренней учётной записью admin виртуализированного ЦУ) — значение ovirtadmin (`OVIRT_ADMIN_LOGIN=ovirtadmin`).

Для применения изменений в конфигурации перезапустите службу веб-сервера Apache:

```
# systemctl restart httpd
```

В случае необходимости контролировать отозванные сертификаты потребуется дополнительная настройка веб-сервера Apache, который может работать как с сервисом OCSP на сервере IPA, так и со списком CRL.

Для настройки веб-сервера Apache на работу с OCSP отредактируйте конфигурационный файл `/etc/httpd/conf.d/certs-verify.conf` следующим образом:

```
SSLOCSPEnable on
SSLOCSPOverrideResponder on
SSLOCSPDefaultResponder "http://ipa-ca.example.com/ca/ocsp"

RequestHeader set X-Cert-User "%{SSL_CLIENT_S_DN_CN}s"
<LocationMatch   ^/ovirt-engine/sso/(interactive-login-negotiate|oauth/
token-http-auth)>
  SSLVerifyClient require
  SSLVerifyDepth 10
</LocationMatch>
```

Примечание — в переменной `SSLOCSPDefaultResponder` укажите адрес сервера IPA, который будет отвечать на запросы OCSP.

Для настройки веб-сервера Apache на работу со списком CRL отредактируйте конфигурационный файл `/etc/httpd/conf.d/certs-verify.conf` следующим образом:

```
SSLCARevocationCheck chain
SSLCARevocationFile /etc/pki/ovirt-engine/apache-ca.crl

RequestHeader set X-Cert-User "%{SSL_CLIENT_S_DN_CN}s"
<LocationMatch   ^/ovirt-engine/sso/(interactive-login-negotiate|oauth/
token-http-auth)>
  SSLVerifyClient require
  SSLVerifyDepth 10
</LocationMatch>
```

Список CRL автоматически формируется на сервере IPA и доступен в виде файла для загрузки по ссылке `http://ipa-ca.example.com/ipa/crl/MasterCRL.bin`.

Выполните следующую команду, чтобы конвертировать в PEM-формат и загрузить файл со списком CRL на веб-сервер Apache:

```
# curl -L http://ipa-ca.example.com/ipa/crl/MasterCRL.bin | openssl crl
-inform DER -outform PEM -out /etc/pki/ovirt-engine/apache-ca.crl
```

Примечание — список CRL имеет дату/время начала действия и дату/время окончания действия и через несколько часов после генерации на сервере IPA теряет свою актуальность. Рекомендуется настроить автоматическое обновление файла со списком CRL на веб-сервере Apache (например, использовать планировщик заданий `cron`).

14.1.5. Настройка браузера для работы с «Рутокен ЭЦП»

Для обеспечения возможности двухфакторной аутентификации на Портале администрирования системы виртуализации ROSA Virtualization администратор должен настроить используемый браузер в соответствии с документацией изготовителя на работу с «Рутокен ЭЦП».

Например, для настройки браузера `Firefox` на работу с «Рутокен ЭЦП» введите в адресной строке браузера следующий URL — `about:preferences#advanced`, или перейдите по вкладкам меню **Edit → Preferences → Advanced → Certificates** (Рис. 45).

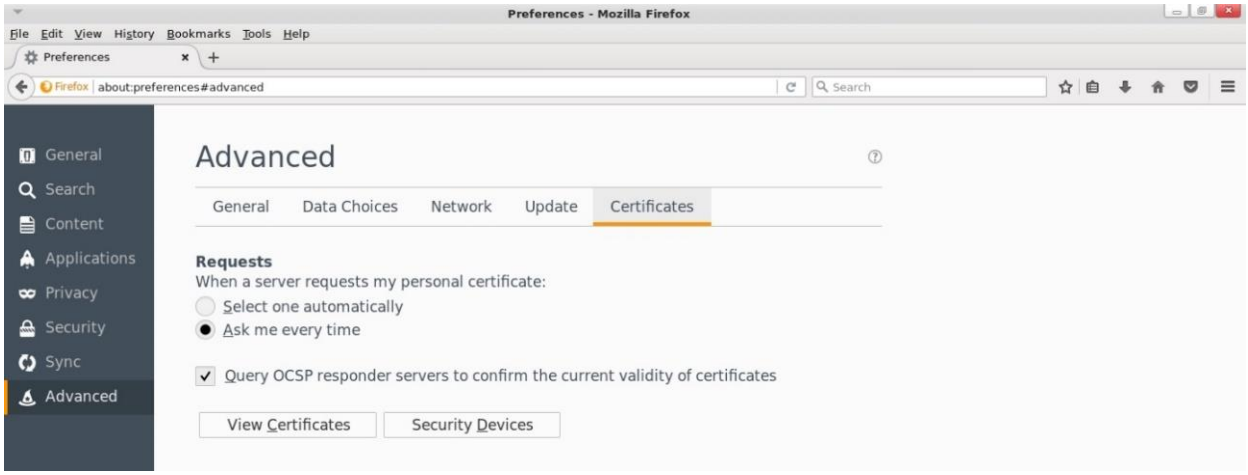

Рис. 45. Вкладка Certificates

Далее нажмите кнопку **Security Devices**, затем в открывшемся окне **Device Manager** (Рис. 46) нажмите **Load** и в поле **Module filename** укажите расположение библиотеки `rtPKCS11ecp`.

Для завершения настройки нажмите кнопку **OK**.

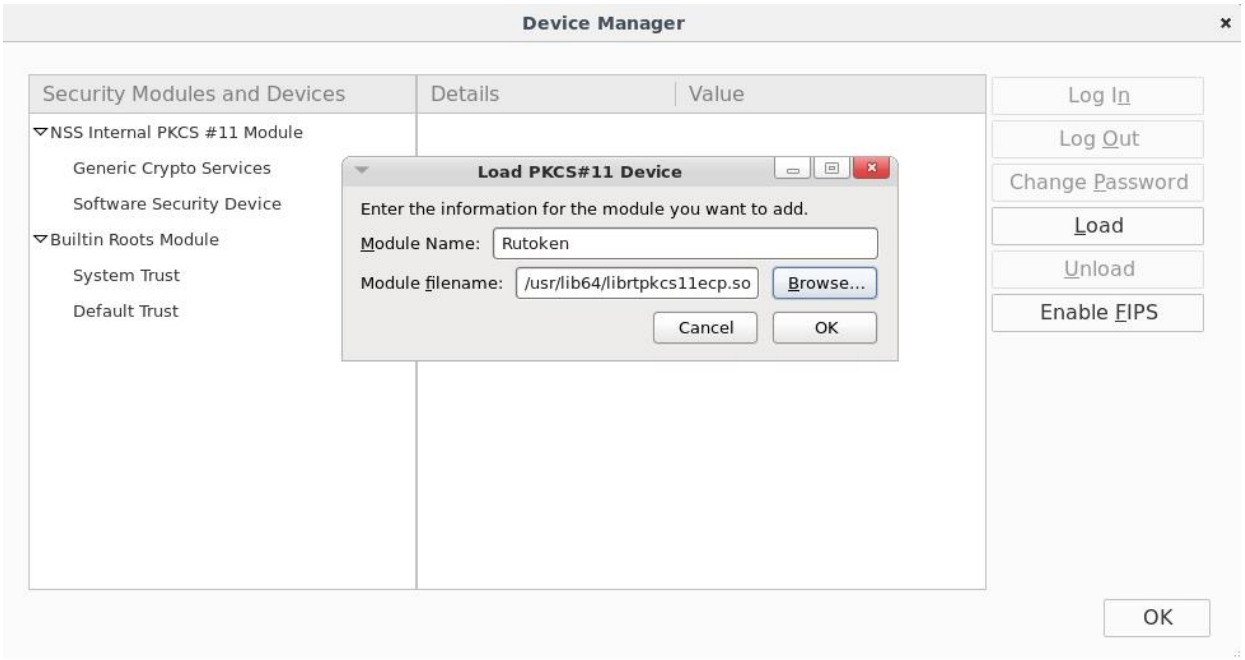

Рис. 46. Окно Device Manager

14.2. Двухфакторная аутентификация в локальной консоли хоста с использованием «Рутокен ЭЦП»

В качестве примера следующая процедура настройки двухфакторной аутентификации для локальной консоли с использованием «Рутокен ЭЦП» будет осуществляться на хосте с установленным гипервизором ROSA Virtualization.

Предварительно осуществите действия, приведенные в пп. 14.1.2. Генерация закрытого ключа и сертификата для пользователя и 14.1.3. Импорт закрытого ключа и сертификата на «Рутокен ЭЦП».

14.2.1. Настройка конфигурации PAM

Установите в систему дополнительный пакет для модуля `pam_pkcs11`:

```
# yum install pam_pkcs11
```

После установки пакета `pam_pkcs11` перезагрузите систему:

```
# reboot
```

Создайте следующую структуру каталогов и установите указанные права доступа:

```
# mkdir /etc/pam_pkcs11/{nssdb,cacerts,crls}
# chmod 0644 /etc/pam_pkcs11/{nssdb,cacerts,crls}
```

Скопируйте корневой сертификат ЦС с сервера IPA на хост:

```
# curl -o /etc/pam_pkcs11/cacerts/ipa-ca.crt --insecure -L https://ipa-ca.example.com/ipa/config/ca.crt
```

Создайте пустую базу данных для сертификатов и импортируйте в эту базу данных корневой сертификат ЦС, скопированный с сервера IPA:

```
# certutil -N -d /etc/pam_pkcs11/nssdb --empty-password
#  certutil  -A  -i  /etc/pam_pkcs11/cacerts/ipa-ca.crt  -n  ipa-ca  -t "CT,CT,CT" -d /etc/pam_pkcs11/nssdb
```

Создайте резервную копию файла `/etc/pam_pkcs11/pam_pkcs11.conf`:

```
# mv /etc/pam_pkcs11/pam_pkcs11.conf /etc/pam_pkcs11/pam_pkcs11.conf.default
```

Отредактируйте файл `/etc/pam_pkcs11/pam_pkcs11.conf` следующим образом:

```
pam_pkcs11 {
  debug = false;
  nullok = false;
  card_only = false;

  use_first_pass = false;
  try_first_pass = false;
  use_authtok = false;

  wait_for_card = false;
  use_pkcs11_module = rutokenecp;

  pkcs11_module rutokenecp {
    module = /usr/lib64/librtpkcs11ecp.so;
    description = "Rutoken PKCS#11";
    slot_num = 0;

    nss_dir = /etc/pam_pkcs11/nssdb;
    ca_dir = /etc/pam_pkcs11/cacerts;
    crl_dir = /etc/pam_pkcs11/crls;
    cert_policy = ca,signature;
  }

  use_mappers = subject;
  mapper_search_path = /usr/lib64/pam_pkcs11;

  mapper subject {
    debug = false;
    module = internal;
    ignorecase = false;
    mapfile = file:///etc/pam_pkcs11/subject_mapping;
  }
}
```

В файл `/etc/pam.d/login` добавьте строку `auth [success=ok ignore=ignore default=die] pam_pkcs11.so nodebug wait_for_card` после строки `auth substack system-auth` следующим образом:

```
auth    substack    system-auth
auth  [success=ok  ignore=ignore  default=die]  pam_pkcs11.so  nodebug
wait_for_card
```

Для сопоставления сертификата, хранящегося на токене, и учётной записи пользователя, под которой будет осуществляться локальный вход в систему, создайте файл `/etc/pam_pkcs11/subject_mapping` со следующими строками:

```
# Mapping file for Certificate Subject
# format: Certificate Subject -> login
#
CN=ovirtadmin,O=EXAMPLE.COM -> root
```

Обратите внимание, что локальный вход в систему будет возможен только под учётной записью того пользователя, для которого сопоставлен сертификат в файле `/etc/pam_pkcs11/subject_mapping`.

14.2.2. Локальный вход в систему

Для локального входа в систему подключите «Рутокен ЭЦП» к USB-порту хоста, после чего введите системный логин и пароль пользователя, а также PIN-код токена этого пользователя (Рис. 47).

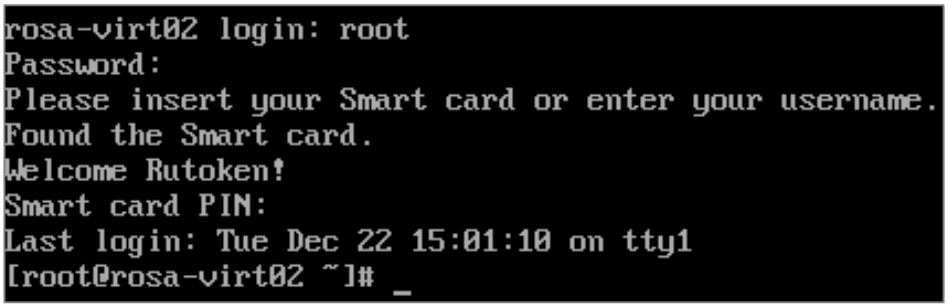

Рис. 47. Локальный вход в систему с использованием «Рутокен ЭЦП»

Без наличия соответствующего токена осуществить вход в систему будет невозможно (Рис. 48).

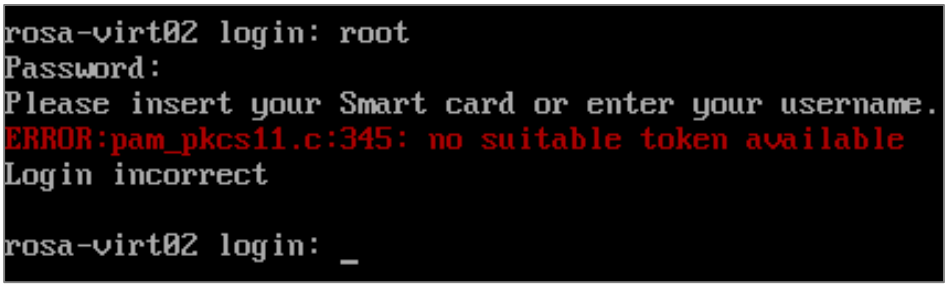

Рис. 48. Сообщение об ошибке при попытке входа в систему без «Рутокен ЭЦП»

Глава 15. Настройка vGPU

В данном руководстве описывается процесс настройки vGPU на примере NVIDIA Tesla T4.

Процесс настройки vGPU состоит из выполнения последовательности действий сначала в консоли хоста с подключенным vGPU, а затем на Портале администрирования.

15.1. Настройка системных параметров хоста

Для упрощения настройки загрузчика GRUB необходимо, чтобы хост не был подключен к виртуализированному ЦУ.

Настройка загрузчика GRUB

В консоли хоста выполните следующую команду:

```
# echo 'blacklist nouveau' >> /etc/modprobe.d/nvidia-installer-disable-nouveau.conf
```

В конфигурационный файл `/etc/default/grub` в строку `GRUB_CMDLINE_LINUX` добавьте параметры загрузки ядра `rdblacklist=nouveau` и `intel_iommu=on` следующим образом:

```
GRUB_CMDLINE_LINUX="crashkernel=auto resume=/dev/mapper/rv-swap rd.lvm.lv=rv/root rd.lvm.lv=rv/swap rdblacklist=nouveau intel_iommu=on loglevel=4"
```

Для обновления конфигурации загрузчика GRUB выполните в консоли хоста следующую команду в зависимости от типа используемой системы загрузки:

- UEFI:

  ```
  # grub2-mkconfig -o /boot/efi/EFI/rosa/grub.cfg
  ```

- BIOS:

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

Для применения изменений перезагрузите хост:

```
# reboot
```

15.2. Установка драйвера vGPU

Комплект драйверов для NVIDIA Tesla T4 состоит из файлов `1-NVIDIA-Linux-x86_64-460.73.01-grid-4.18.0-305.rv3.run` и `2-NVIDIA-Linux-x86_64-460.73.02-vgpu-kvm-4.18.0-305.rv3.run`.

Скопируйте указанные файлы на хост и установите права на выполнение для этих файлов:

```
# chmod +x 1-NVIDIA-Linux-x86_64-460.73.01-grid-4.18.0-305.rv3.run 2-NVIDIA-Linux-x86_64-460.73.02-vgpu-kvm-4.18.0-305.rv3.run
```

Для установки драйвера выполните в консоли хоста следующую команду:

```
# ./1-NVIDIA-Linux-x86_64-460.73.01-grid-4.18.0-305.rv3.run
```

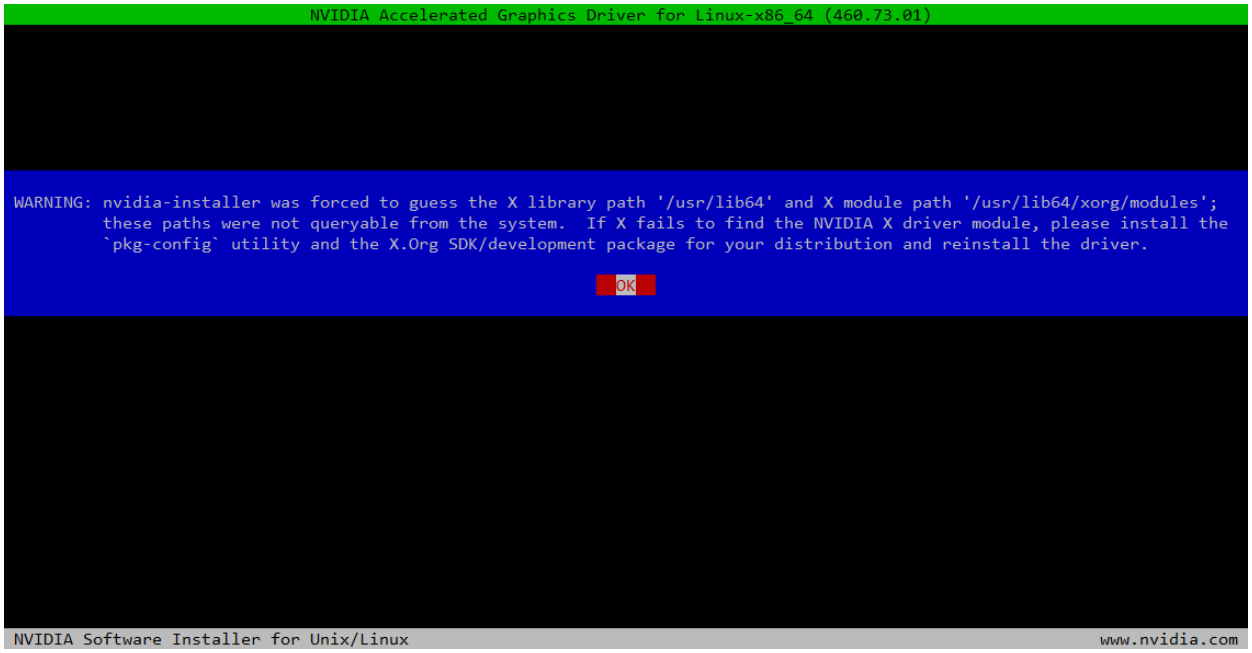

Рис. 49. Установка драйвера NVIDIA

В процессе установки при выводе запроса на добавление 32-битных библиотек `Install NVIDIA's 32-bit compatibility libraries?` выберите значение `No`.

В случае появления сообщения о невозможности определить путь установки конфигурационных файлов (Рис. 50) используйте опцию `--glvnd-egl-config-path` в команде установки драйвера для уточнения пути.

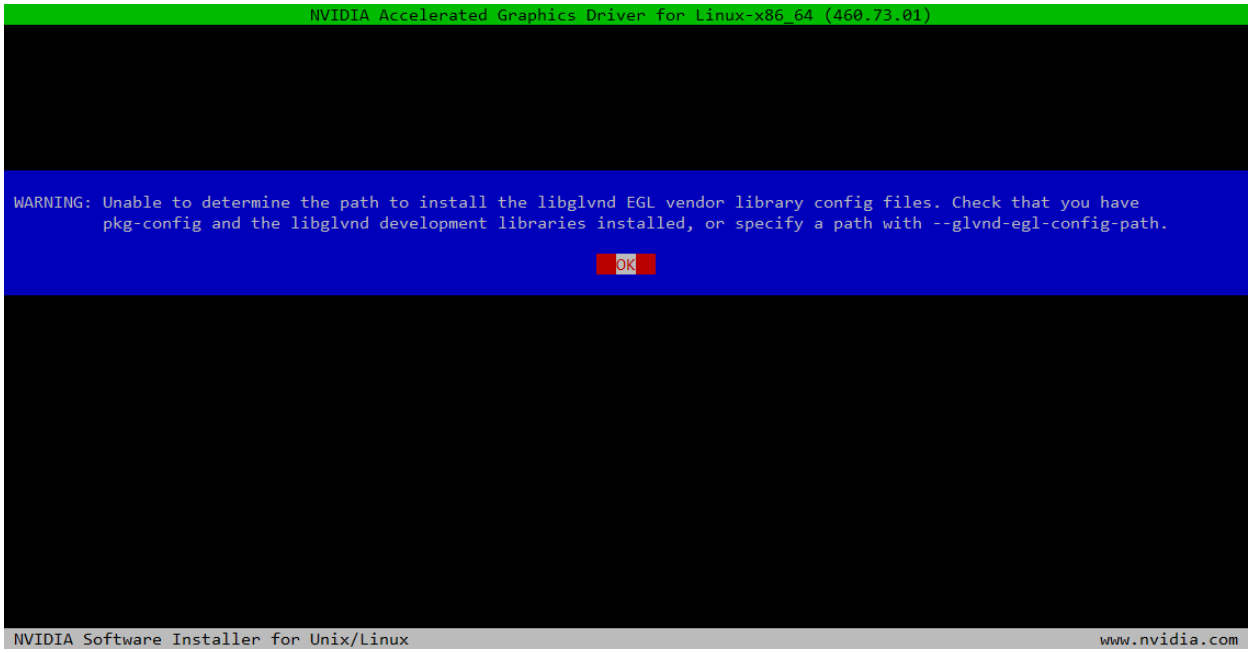

Рис. 50. Сообщение о необходимости уточнения пути установки драйвера

После завершения процесса появится соответствующее сообщение об успешной установке драйвера.

Для запуска драйвера выполните в консоли хоста следующую команду:

```
# ./2-NVIDIA-Linux-x86_64-460.73.02-vgpu-kvm-4.18.0-305.rv3.run
```

При наличии в системе установленного драйвера предыдущей версии, программа установки выведет запрос на удаление этого драйвера (Рис. 51). Для продолжения установки выберите значение `Continue installation`.

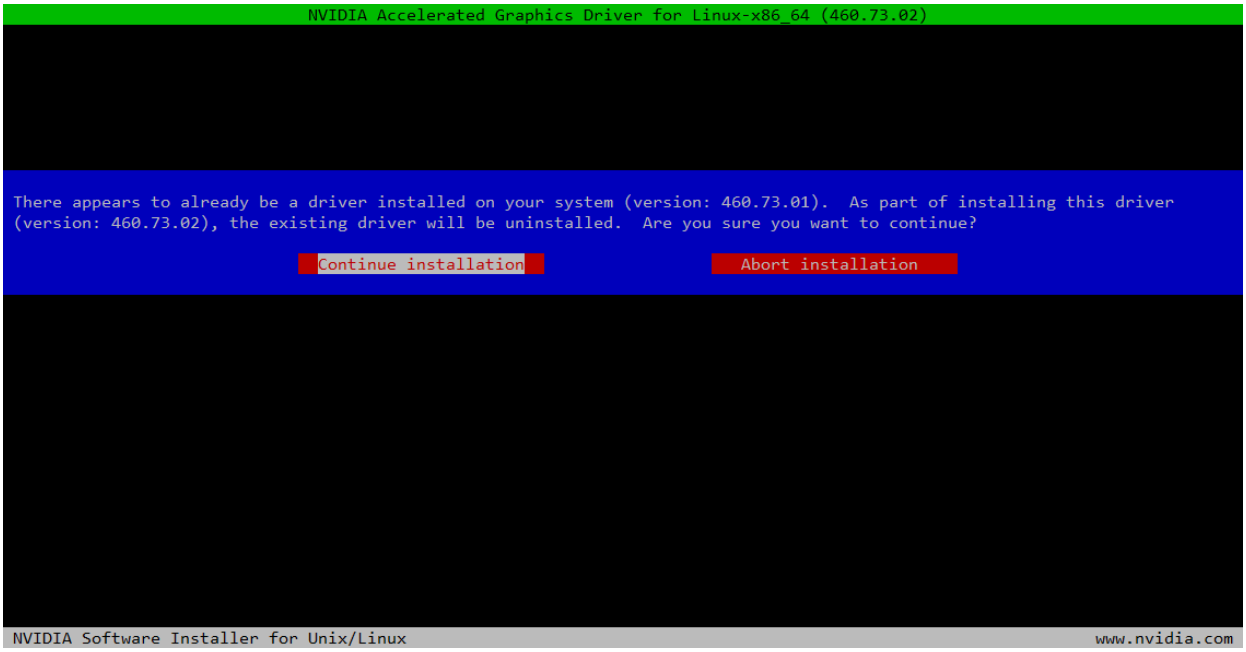

Рис. 51. Продолжение установки с удалением старой версии драйвера

После появления сообщения об успешном завершении процесса установки и настройки драйвера перезагрузите хост:

```
# reboot
```

После перезагрузки хоста выполните следующие команды для отображения модулей ядра, используемых vGPU:

```
# lspci -knn | grep -A 15 NVIDIA
```

```
65:00.0 3D controller [0302]: NVIDIA Corporation TU104GL [Tesla T4] [10de:1eb8] (rev a1)
        Subsystem: NVIDIA Corporation Device [10de:12a2]
        Kernel driver in use: nvidia
        Kernel modules: nouveau, nvidia_vgpu_vfio, nvidia
```

```
# lsmod | grep vfio
```

```
nvidia_vgpu_vfio       65536  0
nvidia              34127872  10 nvidia_vgpu_vfio
vfio_mdev              16384  0
mdev                   20480  2 vfio_mdev,nvidia_vgpu_vfio
vfio_iommu_type1       36864  0
vfio                   36864  3 vfio_mdev,nvidia_vgpu_vfio,vfio_iommu_type1
```

При успешной установке драйвера NVIDIA вывод утилиты `nvidia-smi` будет содержать следующую информацию:

```
# nvidia-smi
```

```
Wed Jul 14 10:46:55 2021
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 460.73.02    Driver Version: 460.73.02    CUDA Version: N/A      |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|                               |                      |               MIG M. |
|===============================+======================+======================|
|   0  Tesla T4            On   | 00000000:65:00.0 Off |                    0 |
| N/A   35C    P8    16W /  70W |     75MiB / 15359MiB |      0%      Default |
```

```
|                                         |                      |                  N/A |
+-----------------------------------------+----------------------+----------------------+

+---------------------------------------------------------------------------------------+
| Processes:                                                                            |
|  GPU   GI   CI        PID   Type   Process name                  GPU Memory |
|        ID   ID                                                   Usage      |
|=======================================================================================|
|  No running processes found                                                           |
+---------------------------------------------------------------------------------------+
```

Для продолжения настройки vGPU подключите хост к виртуализированному ЦУ, используя для этого Портал администрирования.

15.3. Настройка драйвера vGPU для ВМ

Настройка драйвера vGPU для ВМ осуществляется на Портале администрирования.

Настройка драйвера vGPU для ВМ

1. Нажмите **Ресурсы → Виртуальные машины**.
2. Выберите необходимую ВМ.
3. Перейдите на вкладку **Устройства хоста** и нажмите **Управление vGPU**, чтобы открыть соответствующее окно (Рис. 52).
4. Выберите vGPU, которое будет подключено к ВМ.
5. Установите переключатель **Вторичный видеоадаптер для VNC** в положение **Выкл.**
6. Нажмите **Сохранить**.

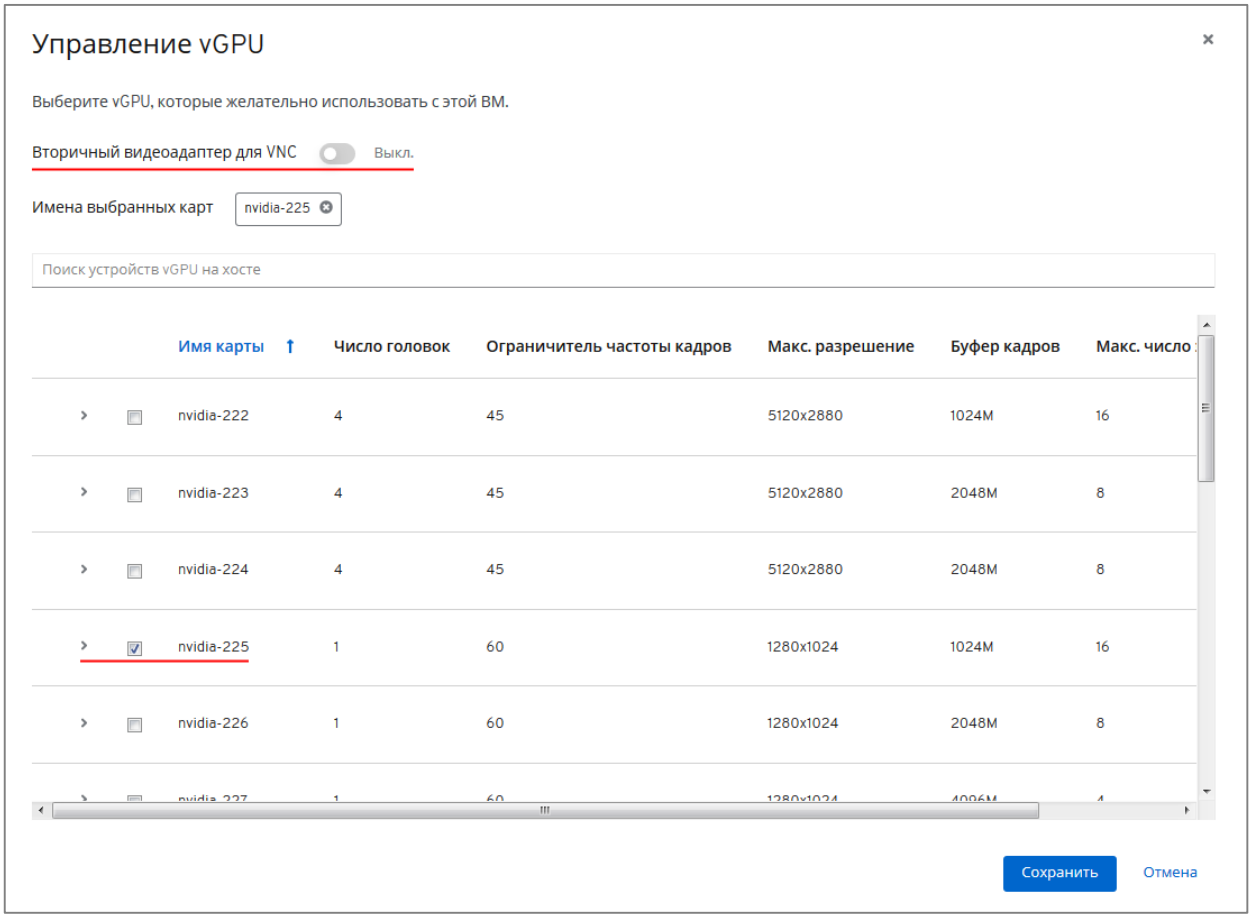

Рис. 52. Управление vGPU

Далее запустите ВМ и подключитесь к SPICE консоли для установки драйвера vGPU, используя для этого диспетчер устройств ВМ.

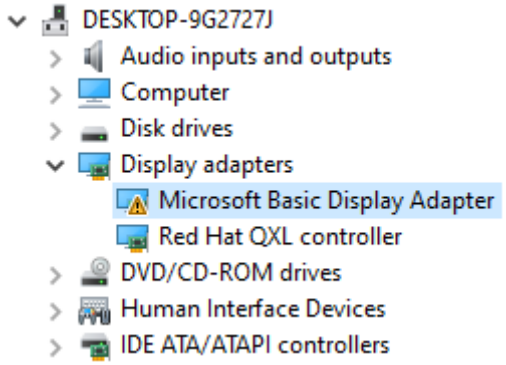

Рис. 53. Диспетчер устройств ВМ до установки драйвера

После установки драйвера выключите ВМ, затем в окне **Управление vGPU** установите переключатель **Вторичный видеоадаптер для VNC** в положение **Вкл.**, после чего запустите ВМ.

В результате в диспетчере устройств ВМ появится соответствующий видеоадаптер.

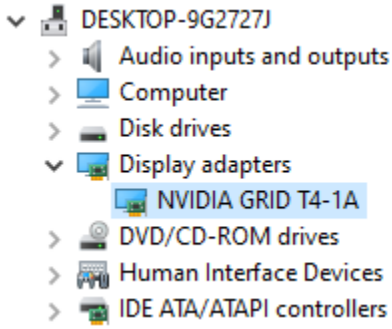

Рис. 54. Отображение видеоадаптера в диспетчере устройств ВМ

Примечание — для отображения используемых ресурсов vGPU выполните в консоли хоста следующую команду:

```
# nvidia-smi
Thu Jul 15 11:52:31 2021
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 460.73.02    Driver Version: 460.73.02    CUDA Version: N/A      |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|                               |                      |               MIG M. |
|===============================+======================+======================|
|   0  Tesla T4            On   | 00000000:65:00.0 Off |                    0 |
| N/A   35C    P8    16W /  70W |   1027MiB / 15359MiB |      2%      Default |
|                               |                      |                  N/A |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                                  |
|  GPU   GI   CI        PID   Type   Process name                  GPU Memory |
|        ID   ID                                                   Usage      |
|=============================================================================|
|    0   N/A  N/A    365401    C+G   vgpu                                944MiB |
+-----------------------------------------------------------------------------+
```

Глава 16. Развёртывание подсистемы мониторинга и отчётности Grafana

Grafana — это мультиплатформенное веб-приложение для аналитики и интерактивной визуализации.

Развёртывание Grafana

1. Переведите окружение в режим глобального обслуживания:

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

2. Войдите в систему, предназначенную для развёртывания Grafana, и выполните следующую команду:

   ```
   # engine-setup --reconfigure-optional-components
   ```

3. При выводе следующих запросов нажмите клавишу `Enter`, чтобы установить Grafana:

   ```
   Configure Grafana on this host (Yes, No) [Yes]:
   Renew certificate (Yes, No) [Yes]:
   ```

4. Отключите глобальный режим обслуживания:

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

Для доступа к панелям управления Grafana нажмите **Портал мониторинга** на странице приветствия Портала администрирования, или перейдите по адресу `https://`*`<доменное_имя/IP-адрес_виртуализированного_ЦУ>`*`/ovirt-engine-grafana`.

Глава 17. Администрирование подсистемы резервного копирования и восстановления

17.1. Использование веб-сервиса управления резервными копиями

Веб-сервис управления системой безагентного резервного копирования позволяет вам управлять созданием, ротацией и удалением резервных копий ваших виртуальных машин. Чтобы использовать веб-сервис, выполните следующие шаги:

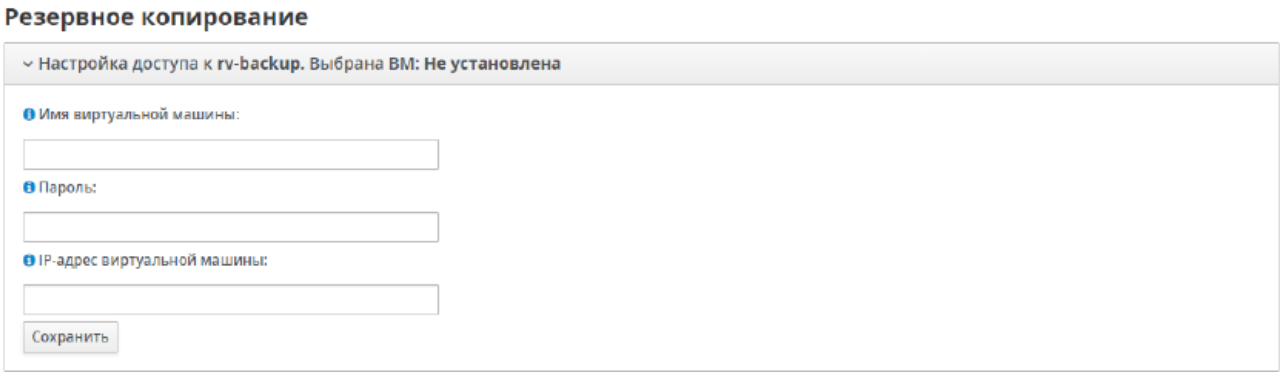

Рис. 55. Настройка доступа

Для работы с резервным копированием необходимо настроить доступ к соответствующей ВМ. Необходимо вписать имя ВМ, ее пароль и ip-адрес. Для того чтобы соединение прошло успешно, необходимо включить соответствующую ВМ. После успешного соединения панель настройки скроется и будет видно имя ВМ, предназначенной для резервного копирования.

Примечание: По мере развития системы резервного копирования, этот список будет расширяться.

17.2. Таблица со списком виртуальных машин

На главной странице веб-сервиса вы найдете таблицу, содержащую последние пять созданных виртуальных машин. Каждая запись в таблице содержит следующую информацию: название виртуальной машины, описание, дата создания и статус “Только хранилище”. Если виртуальная машина присутствует в хранилище и на сервере управления, статус “Только хранилище” будет “Нет”. Если виртуальная машина существует только в хранилище, но удалена с сервера управления, статус будет “Да”. Если нужной виртуальной машины нет в таблице, ее можно добавить вручную.

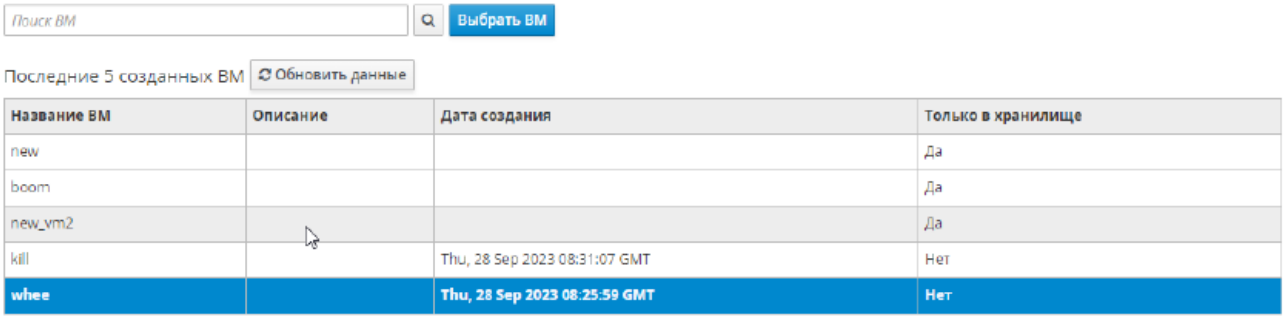

Рис. 56. Список виртуальных машин.

17.3. Операции с виртуальными машинами

Вы можете выполнять различные операции с виртуальными машинами, такие как создание резервной копии, восстановление из резервной копии и удаление резервных копий.

Для этого выберите нужную виртуальную машину из таблицы и нажмите на соответствующую кнопку.

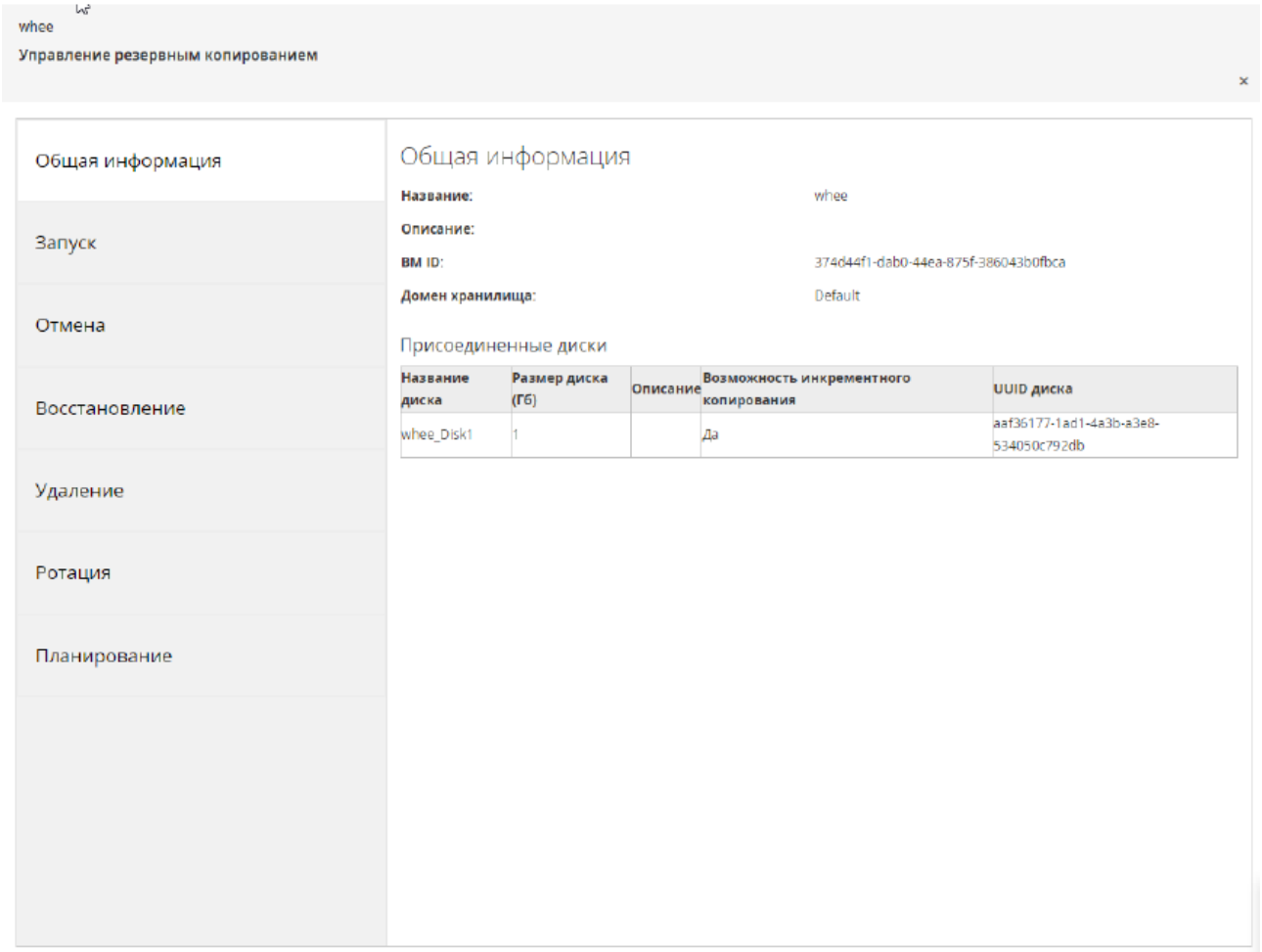

Рис. 57. Операции с виртуальными машинами.

17.4. Общая информация о виртуальной машине

На странице общей информации о виртуальной машине вы можете просмотреть информацию о состоянии резервного копирования виртуальной машины. Здесь вы найдете информацию о том, когда была создана последняя резервная копия, сколько места она занимает, и когда она была последней раз обновлена. Также здесь можно просмотреть список доступных резервных копий для выбранной виртуальной машины.

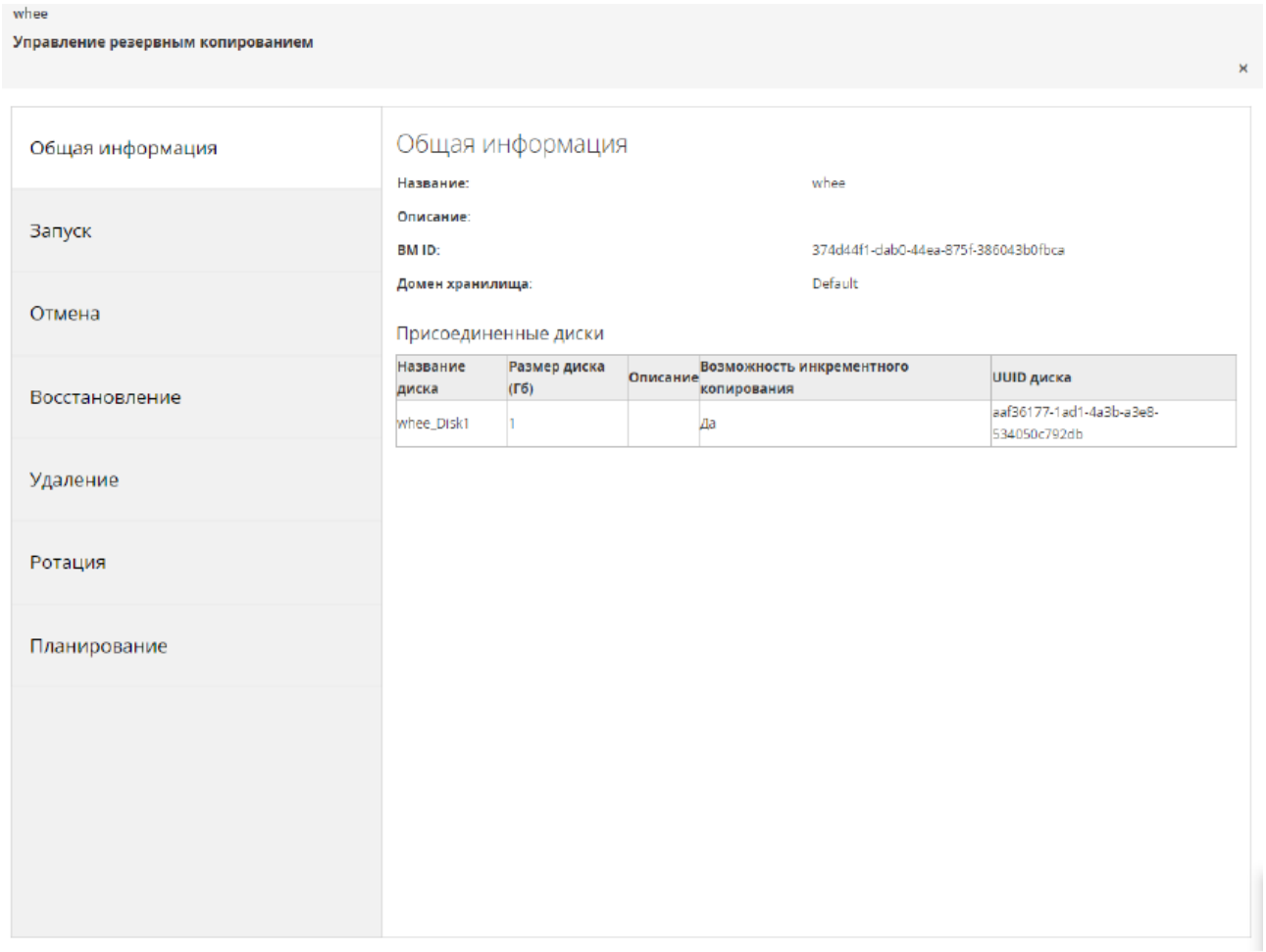

Рис. 58. Общая информация о виртуальной машине.

17.5. Создание резервной копии виртуальной машины

Для создания резервной копии выберите виртуальную машину в таблице и нажмите кнопку “Создать резервную копию”. Веб-сервис создаст резервную копию выбранной виртуальной машины и отобразит информацию о созданной резервной копии на странице общей информации.

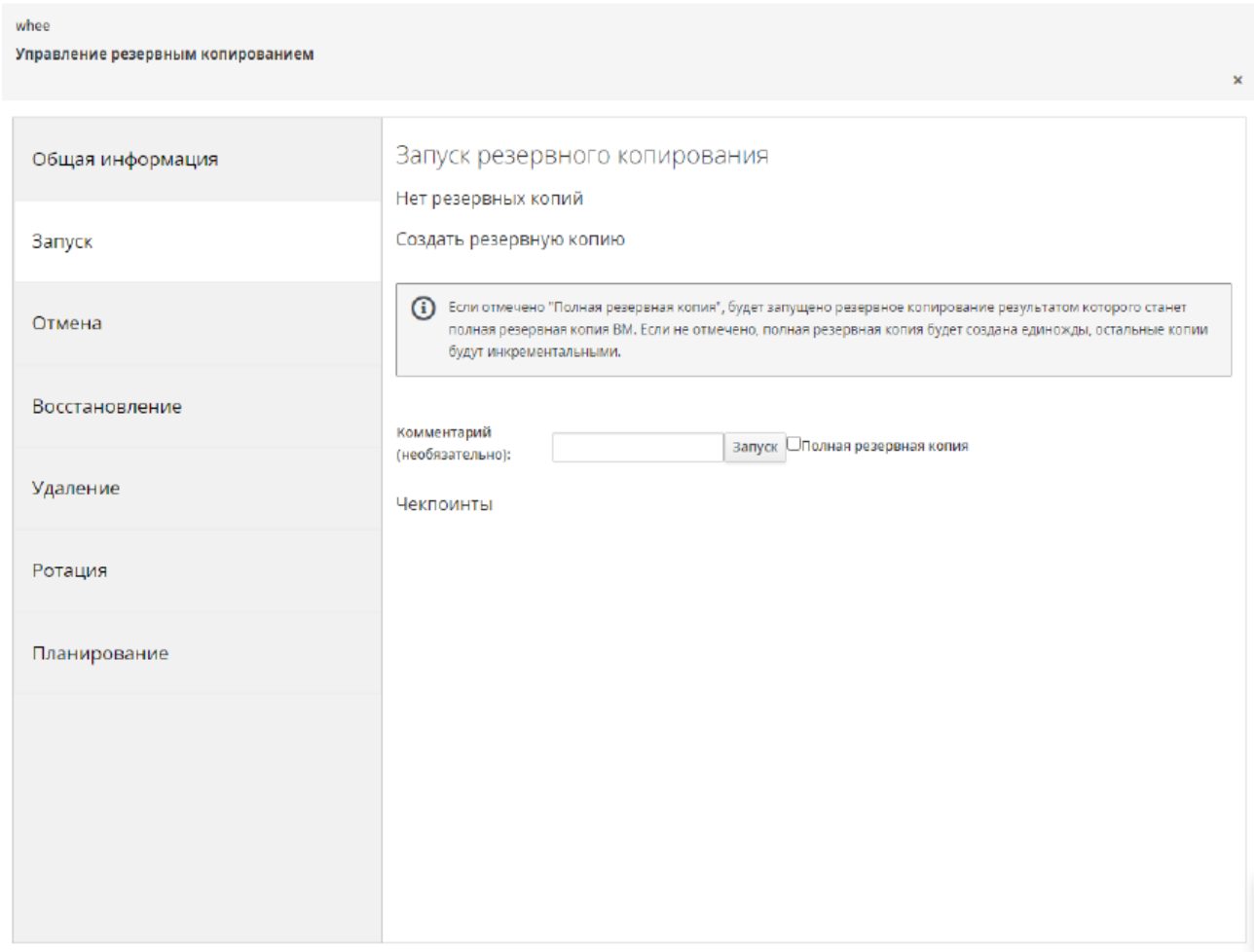

Рис.59. Создание резервной копии.

17.6. Отмена создания резервной копии

Если вы случайно начали создавать резервную копию виртуальной машины, вы можете отменить этот процесс. Для этого на странице общей информации выберите нужную резервную копию и нажмите кнопку “Отменить создание”. Веб-сервис отменит процесс создания резервной копии.

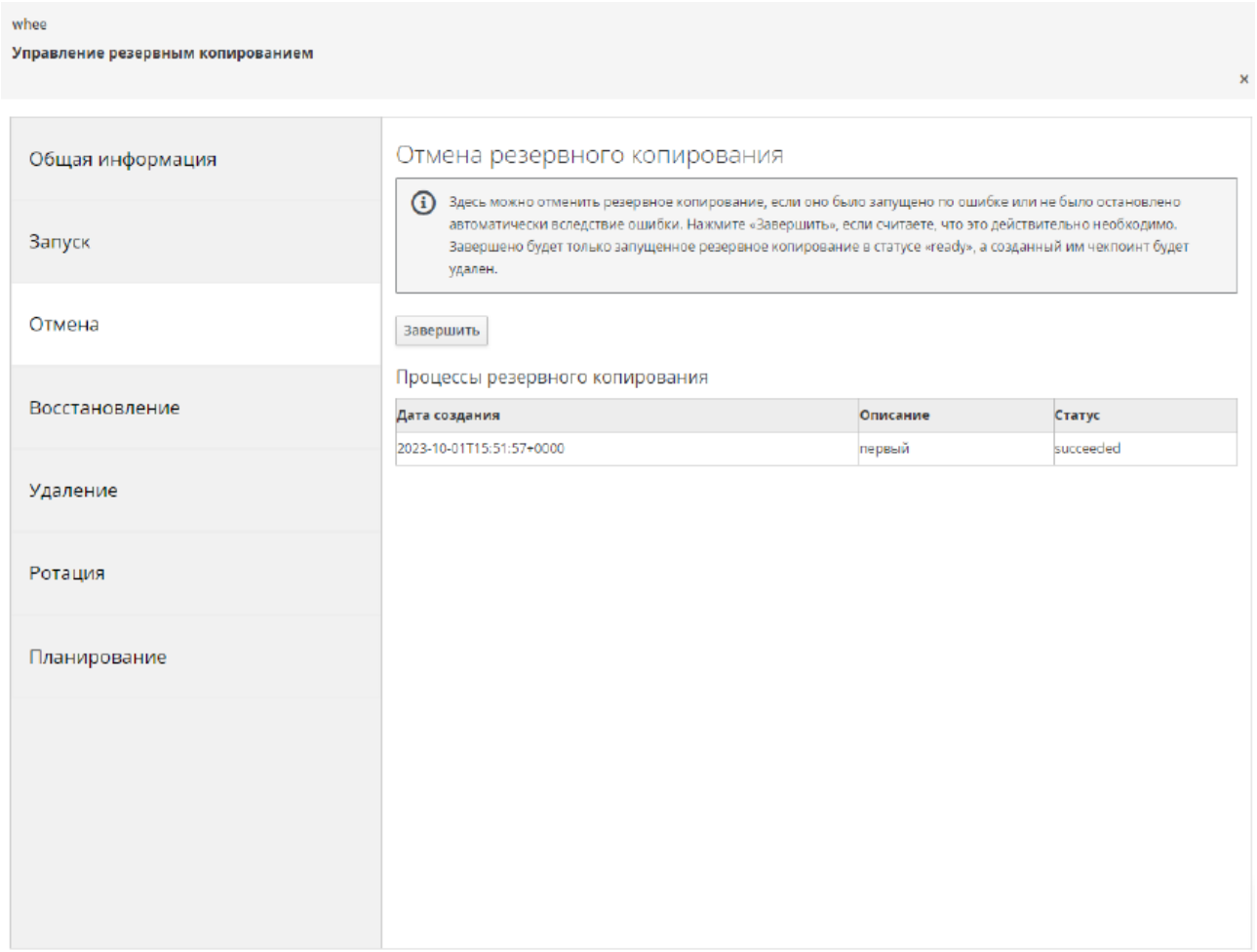

Рис. 60. Отмена создания резервной копии.

17.7. Восстановление виртуальной машины из резервной копии

Если необходимо восстановить виртуальную машину, выберите нужную резервную копию из списка и нажмите кнопку “Восстановить”. Веб-сервис восстановит выбранную виртуальную машину и отобразит ее на главной странице.

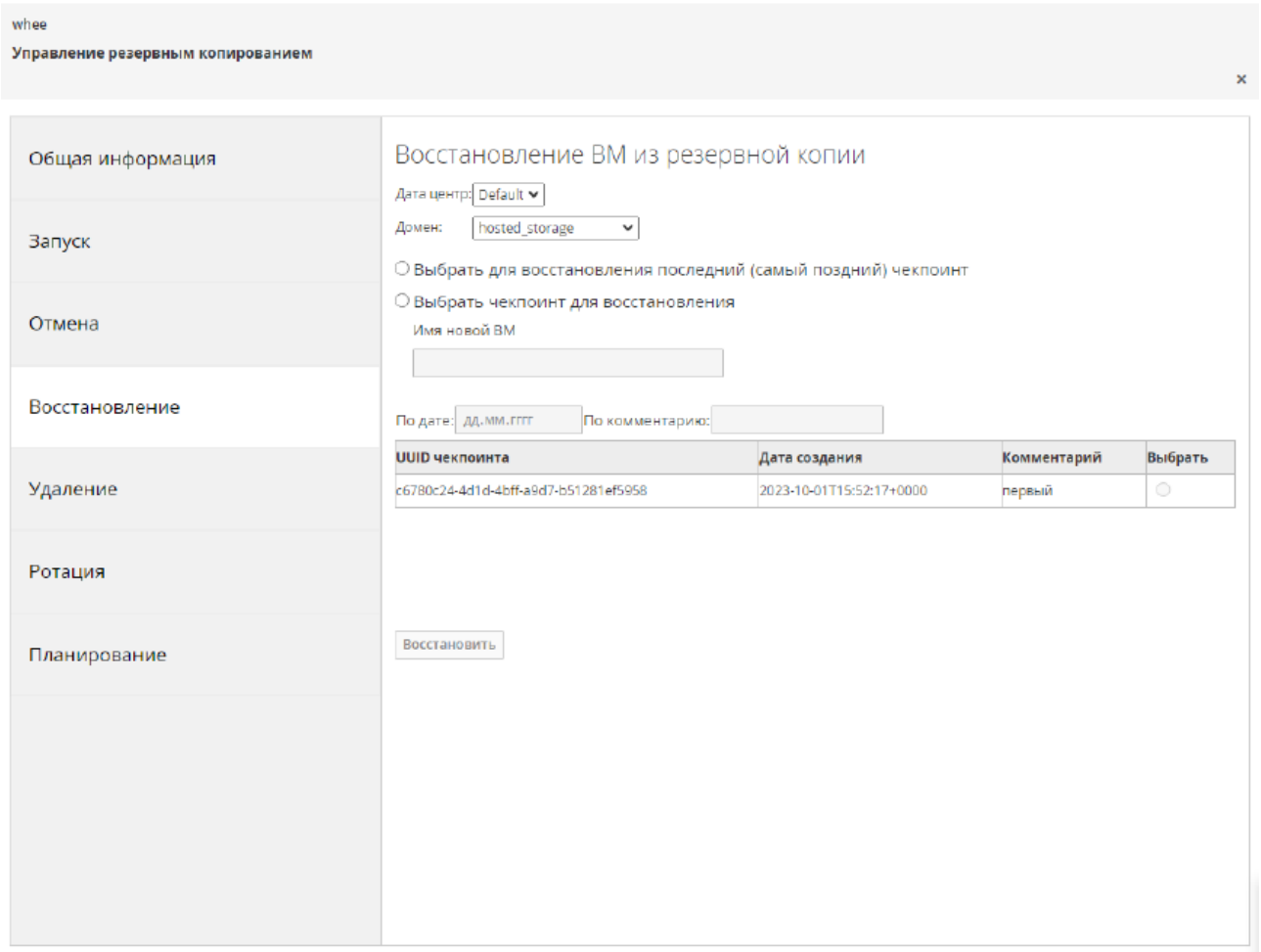

Рис.61. Управление созданием резервных копий.

17.8. Ротация резервных копий

Вы также можете ротировать (менять) резервные копии. Для этого перейдите на страницу общей информации и выберите нужную резервную копию. Затем нажмите кнопку “Ротировать” и веб-сервис удалит текущую резервную копию, заменив ее новой.

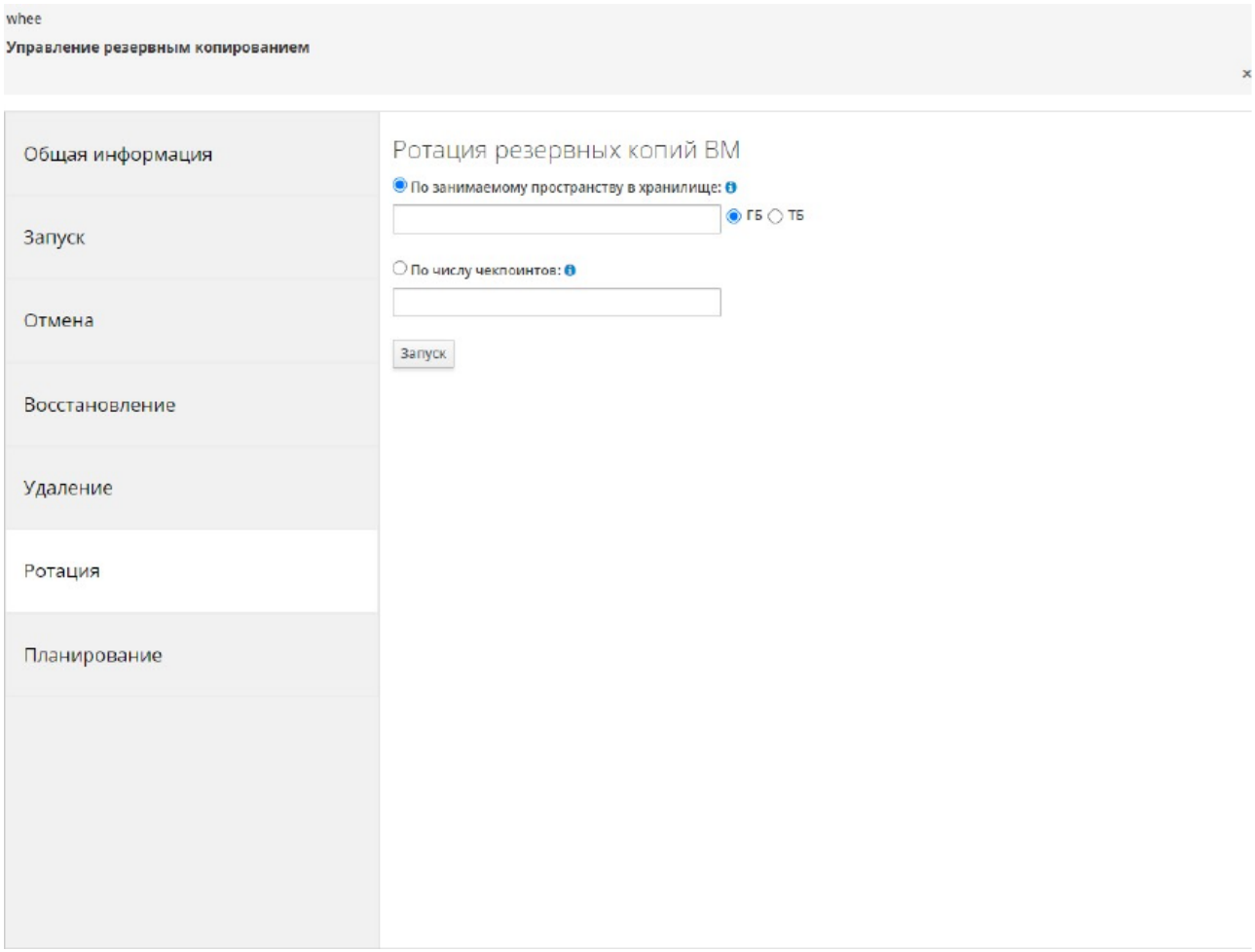

Рис.62. Ротация резервных копий.

17.9. Удаление резервных копий виртуальных машин

Доступно три вида удаления резервных копий: * Удаление последнего чекпоинта. * Удаление всех чекпоинтов. * Очистка хранилища от файлов удаленных чекпоинтов.

Предупреждение!

После того, как будет удален последний или все чекпоинты, необходимо в обязательной порядке выполнить очистку хранилища от удаленных чекпоинтов!

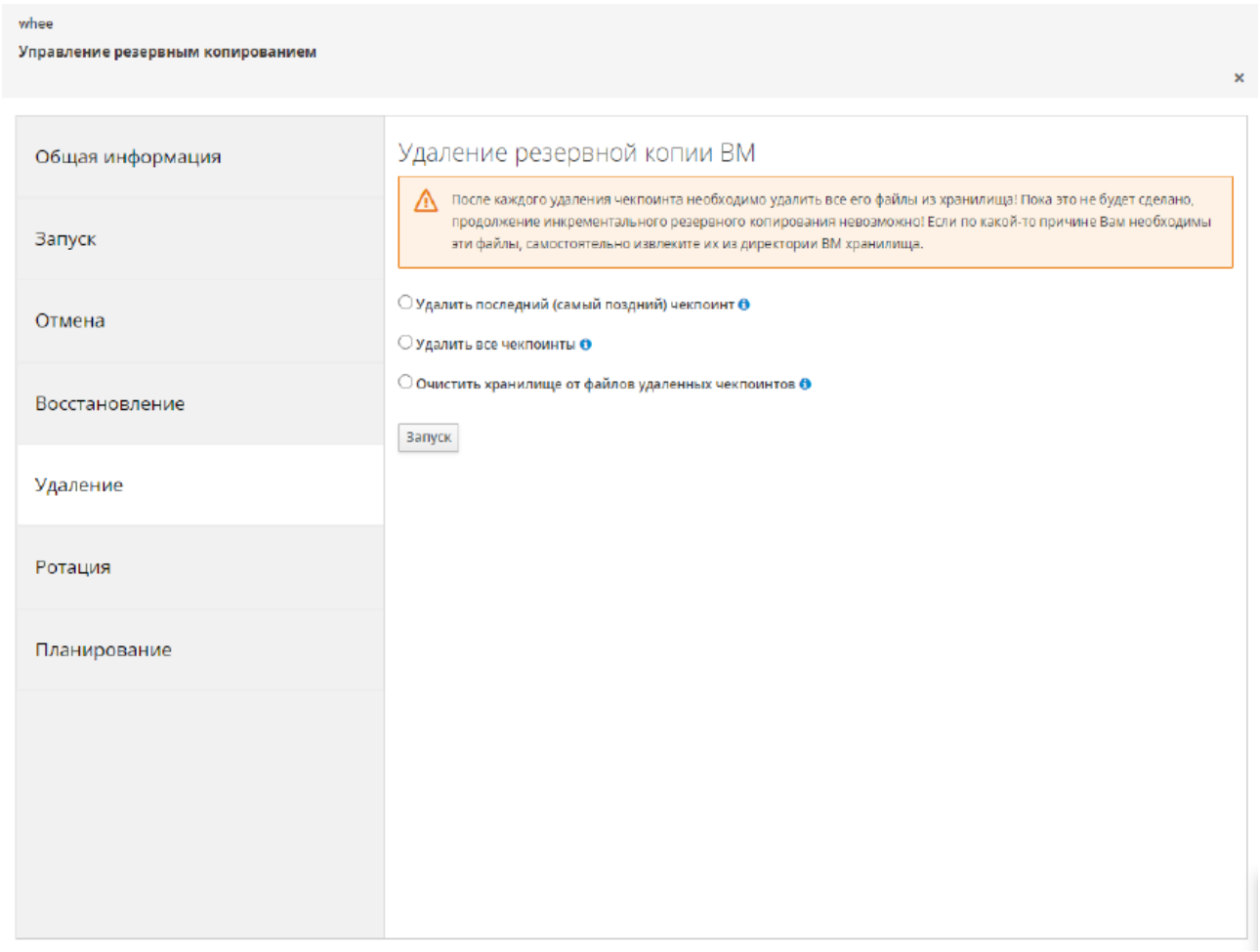

Рис.63. Удаление резервных копий.

17.10. Планирование задач по расписанию

Процесс выполнения операций может занимать некоторое время, особенно если выполняется операция создания или ротации резервной копии большой виртуальной машины. Веб-сервис уведомит вас о завершении операции и отобразит результат в таблице виртуальных машин.

Веб-сервис позволяет планировать задачи по расписанию. Вы можете запланировать создание резервных копий или ротацию резервных копий по определенному расписанию. Для этого откройте страницу планирования задач и настройте расписание в соответствии с вашими требованиями.

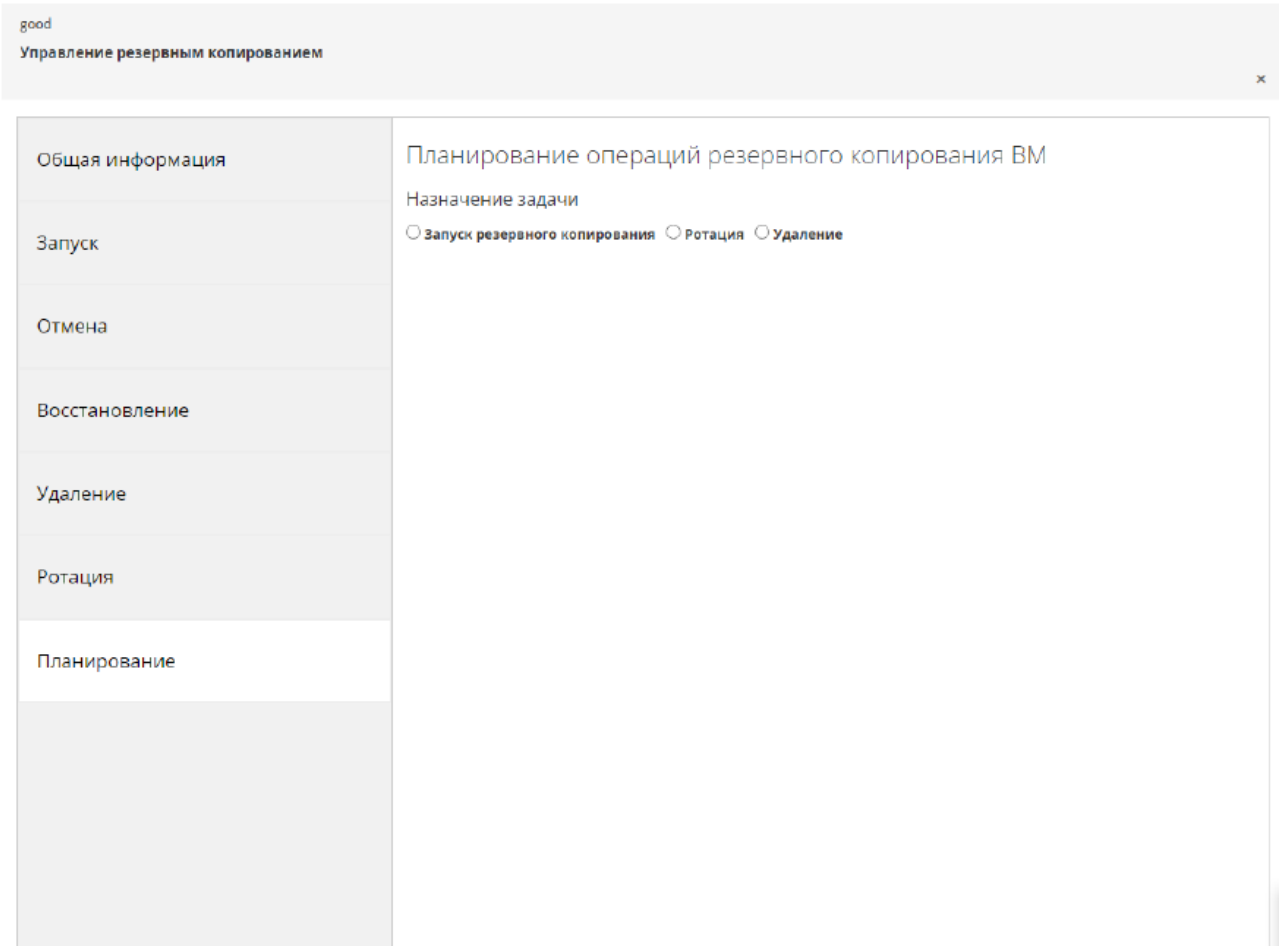

Рис.64. Планирование операций резервного копирования.

Для того, чтобы назначить задачу на запланированную дату, выберите задачу и ее параметры. После того, как задача будет выбрана, появится панель для выбора параметров планирования. Доступны следующие параметры планирования: * Однократно * Ежедневно * Еженедельно * Ежемесячно.

Предупреждение!

Минимальный интервал между операциями для одной ВМ должен составлять не менее 30 минут!

Примечание:

Если выбран параметр «Однократно», то ему доступна опция «Операция не прерывает серию в случае ошибки». Данная опция необходима, в случае если для ВМ будет запланирована серия задач, то при ошибке в выполнении какой-либо задачи, последующие задачи будут выполняться. Если не выставить эту опцию, то последующие задачи будут отменены.

Все запланированные операции находятся на главной странице в таблице «Запланированные операции».

Запланированные операции

Имя ВМ	Операция	Тип	Параметры операции	Подробности	Статус задачи	Удалить задачу
good	Ротация	Ротация по количеству чекпоинтов	2 checkpoints	Ежедневно. В 15:00:00 каждые 5 дн.	Назначена на выполнение	Удалить
good	Резервное копирование	Инкрементальное резервное копирование		Ежемесячно. В 10:00:00 в 1,7,13,19,25 день месяца Июль,Октябрь,Декабрь	Назначена на выполнение	Удалить
good	Удаление	Очищение хранилища от устаревших чекпоинтов		Еженедельно. В 20:00:00 по Вторник,Воскресенье	Назначена на выполнение	Удалить
good	Удаление	Удаление последнего чекпоинта		Еженедельно. В 19:30:00 по Вторник,Воскресенье	Назначена на выполнение	Удалить
good	Резервное копирование	Инкрементальное резервное копирование		Ежедневно. В 18:05:00 каждые 1 дн.	Назначена на выполнение	Удалить
good	Резервное копирование	Инкрементальное резервное копирование		Один раз. В 2023-10-01 17:05:00	Выполнено	Удалить

Рис.65. Запланированные операции.

Задачу можно удалить кнопкой «Удалить».

17.11. Процесс выполнения операций

На главной странице также находится таблица, в которой отображаются события резервного копирования.

Журнал событий резервного копирования Очистить статусы

Дата и время	ВМ UUID	Имя ВМ	Тип	Сообщение
2023-10-01T17:05:00+0000	438a6c6f-c44c-4464-ac06-3fb4dc2179c3	good	Creating a backup	Backup created successfully!
2023-10-01T16:52:33+0000	438a6c6f-c44c-4464-ac06-3fb4dc2179c3	good	Удаление последнего чекпоинта из ВМ	19:52:35 Check of backup storage for remaining metafiles completed. 19:52:35 StorageError[E110]: VM[good] not found in the backup storage.
2023-10-01T16:52:05+0000	438a6c6f-c44c-4464-ac06-3fb4dc2179c3	good	Удаление последнего чекпоинта из ВМ	19:52:07 Check of backup storage for remaining metafiles completed. 19:52:07 VM[438a6c6f-c44c-4464-ac06-3fb4dc2179c3, local] checkpoints map has been removed! 19:52:07 The local checkpoint map of VM[438a6c6f-c44c-4464-ac06-3fb4dc2179c3, local] was removed because the last Checkpoint[800588b4-f8c3-4cda-8593-e5a0c6b1db3f] was deleted. Do not forget to clean the backup storage with the "backup clean --local" command!
2023-10-01T16:51:47+0000	438a6c6f-c44c-4464-ac06-3fb4dc2179c3	good	Ротация по количеству чекпоинтов	19:51:48 Rotation for VM[438a6c6f-c44c-4464-ac06-3fb4dc2179c3, local] backups is not required.
2023-10-01T16:50:37+0000	438a6c6f-c44c-4464-ac06-3fb4dc2179c3	good	Восстановление из резервной копии на новую ВМ	Восстановление из резервной копии успешно выполнено!
2023-10-01T16:48:53+0000	438a6c6f-c44c-4464-ac06-3fb4dc2179c3	good	Creating a backup	Backup created successfully!

Рис. 66. Журнал событий резервного копирования.

Журнал можно очистить кнопкой «Очистить статусы».

Приложение A. VDSM и перехватчики событий

A.1. VDSM

Виртуализированный ЦУ использует службу VDSM для управления виртуальными и физическими хостами. Кроме этого, VDSM управляет и выполняет наблюдение за хранилищами хостов, ресурсами памяти и ресурсами сетей. Также эта служба участвует в координации создания виртуальных машин, в сборе статистики и в других задачах администрирования хостов. VDSM выполняется в виде демона на каждом из хостов под управлением виртуализированного ЦУ и отвечает на вызовы XML-RPC клиентов. При этом виртуализированный ЦУ работает как клиент VDSM.

A.2. Перехватчики событий VDSM

VDSM расширяется с помощью перехватчиков событий (hooks). Перехватчики событий — это сценарии, выполняемые на хосте в момент запуска ключевых событий. При старте поддерживаемого события VDSM запускает на хосте любые выполняемые сценарии перехватчиков событий из `/usr/libexec/vdsm/hooks/`*`пп_имя-события/`* в алфавитно-цифровом порядке. Обычно каждому из сценариев перехватчика присваивается двузначный номер, включаемый в начало имени файла, для придания порядка, в котором запускаются сценарии. Сценарии перехватчиков событий можно создавать на любом из языков программирования. В примерах, приведенных в приложении A, используется Python.

Обратите внимание, что выполняются все сценарии, настроенные для события на хосте. Если необходимо, чтобы указанный перехватчик событий запускался только для определённого набора виртуальных машин, выполняемых на этом хосте, тогда необходимо, чтобы это обеспечивал сам сценарий с помощью оценки настраиваемых пользователем свойств ВМ (см. подраздел A.7. Настройка свойств, указываемых пользователем).

Предупреждение — перехватчики событий VDSM могут вмешиваться в работу системы виртуализации ROSA Virtualization. Программная ошибка перехватчика может потенциально привести к фатальному сбою в работе ВМ и к потере данных. Перехватчики событий VDSM должны быть реализованы разработчиками с осторожностью и тщательно тестироваться перед применением.

A.3. Расширение VDSM с помощью перехватчиков событий

В приложении A описывается как расширить VDSM с помощью перехватчиков, запускаемых при определённых событиях. Расширение VDSM с помощью перехватчиков событий является экспериментальной технологией, поэтому информация в приложении A предназначена для опытных разработчиков.

С помощью настраиваемых пользователем свойств ВМ, перехватчикам событий можно передавать дополнительные параметры, специфичные для данной ВМ.

A.4. Поддерживаемые события VDSM

В **Табл. A.1** описываются поддерживаемые события VDSM.

Табл. A.1. Поддерживаемые события VDSM

Название	Описание
before_vm_start	Перед запуском ВМ
after_vm_start	После запуска ВМ

Название	Описание
before_vm_cont	Перед продолжением выполнения ВМ
after_vm_cont	После продолжения выполнения ВМ
before_vm_pause	Перед приостановкой работы ВМ
after_vm_pause	После приостановки работы ВМ
before_vm_hibernate	Перед входом ВМ в режим гибернации
after_vm_hibernate	После входа ВМ в режим гибернации
before_vm_dehibernate	Перед выходом ВМ из режима гибернации
after_vm_dehibernate	После выхода ВМ из режима гибернации
before_vm_migrate_source	Перед миграцией ВМ выполняются на исходном хосте, с которого осуществляется миграция
after_vm_migrate_source	После миграции ВМ выполняются на исходном хосте, с которого осуществляется миграция
before_vm_migrate_destination	Перед миграцией ВМ выполняются на целевом хосте, на который осуществляется миграция
after_vm_migrate_destination	После миграции ВМ выполняются на целевом хосте, на который осуществляется миграция
after_vm_destroy	После разрушения ВМ
before_vdsm_start	Перед запуском VDSM на хосте. Перехватчики событий before_vdsm_start выполняются от имени суперпользователя `root` и не наследуют окружение процесса VDSM
after_vdsm_stop	После остановки VDSM на хосте. Перехватчики событий after_vdsm_stop выполняются от имени суперпользователя `root` и не наследуют окружение процесса VDSM
before_nic_hotplug	Перед горячим подключением сетевой карты к машине
after_nic_hotplug	После горячего подключения сетевой карты к машине
before_nic_hotunplug	Перед горячим отключением сетевой карты от машины
after_nic_hotunplug	После горячего отключения сетевой карты от машины
after_nic_hotplug_fail	После сбоя горячего подключения сетевой карты к машине
after_nic_hotunplug_fail	После сбоя горячего отключения сетевой карты от машины
before_disk_hotplug	Перед горячим подключением диска к машине
after_disk_hotplug	После горячего подключения диска к машине
before_disk_hotunplug	Перед горячим отключением диска от машины
after_disk_hotunplug	После горячего отключения диска от машины
after_disk_hotplug_fail	После сбоя горячего подключения диска к машине
after_disk_hotunplug_fail	После сбоя горячего отключения диска от машины
before_device_create	Перед созданием устройства, поддерживающего настраиваемые пользователями свойства
after_device_create	После создания устройства, поддерживающего настраиваемые пользователями свойства
before_update_device	Перед обновлением устройства, поддерживающего настраиваемые пользователями свойства
after_update_device	После обновления устройства, поддерживающего настраиваемые пользователями свойства
before_device_destroy	Перед разрушением устройства, поддерживающего настраиваемые пользователями свойства
after_device_destroy	После разрушения устройства, поддерживающего настраиваемые пользователями свойства
before_device_migrate_destination	Перед миграцией устройства выполняются на целевом хосте, на который осуществляется миграция
after_device_migrate_destination	После миграции устройства выполняются на целевом хосте, на который осуществляется миграция
before_device_migrate_source	Перед миграцией устройства выполняются на исходном хосте, с которого осуществляется миграция

Название	Описание
after_device_migrate_source	После миграции устройства выполняются на исходном хосте, с которого осуществляется миграция
after_network_setup	После настройки сети при запуске машины хоста
before_network_setup	Перед настройкой сети при запуске машины хоста

A.5. Окружение VDSM перехватчиков событий

Большинство сценариев перехватчиков событий выполняются от имени пользователя `vdsm` и наследуют окружение процесса VDSM.

Исключениями являются сценарии перехватчиков, запускаемых событиями `before_vdsm_start` и `after_vdsm_stop`. Сценарии перехватчиков, запускаемых этими событиями, выполняются от имени суперпользователя `root` и не наследуют окружение процесса VDSM.

A.6. Объект XML домена перехватчиков событий VDSM

При запуске сценариев перехватчиков событий к окружению добавляется переменная `_hook_domxml`, которая содержит путь до XML-представления домена `libvirt` соответствующей ВМ.

Исключениями являются следующие перехватчики событий, у которых переменная `_hook_domxml` содержит XML-представление сетевой карты, а не виртуальной машины:

- `*_nic_hotplug_*`
- `*_nic_hotunplug_*`
- `*_update_device`
- `*_device_create`
- `*_device_migrate_*`

Примечание — перехватчики событий `before_migration_destination` и `before_dehibernation` на данный момент получают XML домена исходного хоста (XML домена цели будет иметь некоторые отличия).

VDSM использует формат XML домена библиотеки `libvirt` для описания виртуальных машин. Сведения об этом формате можно найти по ссылке http://libvirt.org/formatdomain.html.

UUID виртуальной машины можно получить с помощью XML домена, а также в виде значения переменной окружения `vmId`.

A.7. Настройка свойств, указываемых пользователем

Настраиваемые пользователем свойства, принимаемые диспетчером виртуализации и, в свою очередь, передаваемые пользовательским перехватчикам событий определяются с помощью команды `engine-config`. Выполняйте эту команду с правами суперпользователя `root` на хосте, где установлен диспетчер виртуализации.

Конфигурационные ключи `UserDefinedVMProperties` и `CustomDeviceProperties` команды `engine-config` используются для хранения имён поддерживаемых пользовательских свойств виртуальной машины и устройства соответственно. В этих ключах также присутствуют регулярные выражения, определяющие действительные значения для каждого именованного пользовательского свойства.

Несколько пользовательских свойств разделяются точками с запятой без пробела. Обратите внимание, что при указании конфигурационного ключа, все уже содержащиеся в

нём существующие значения перезаписываются. При указании новых и уже существующих пользовательских свойств в команду необходимо включать все пользовательские свойства, используемые для указания значения ключа.

После обновления ключа конфигурации необходимо перезапустить службу `ovirt-engine` для применения изменений.

Настройка пользовательского свойства `smartcard` (свойство ВМ)

1. Выполните следующую команду для проверки уже имеющихся пользовательских свойств ВМ, настроенных ключом конфигурации `UserDefinedVMProperties`:

   ```
   # engine-config -g UserDefinedVMProperties
   ```

   Из вывода ниже видно, что уже настроено пользовательское свойство `memory` (при этом регулярное выражение `^[0-9]+$` гарантирует, что пользовательское свойство `memory` будет содержать только числовые символы):

   ```
   # engine-config -g UserDefinedVMProperties
   UserDefinedVMProperties:  version: 3.6
   UserDefinedVMProperties:  version: 4.0
   UserDefinedVMProperties:  memory=^[0-9]+$ version: 4.0
   ```

2. Добавьте новое пользовательское свойство `smartcard` к уже настроенному пользовательскому свойству `memory`. При этом укажите, что новое свойство `smartcard` может принимать значения `true` или `false`:

   ```
   # engine-config -s UserDefinedVMProperties='memory=^[0-9]+$;
   smartcard=^(true|false)$' --cver=4.0
   ```

3. Выполните следующую команду для проверки конфигурации пользовательских свойств `memory` и `smartcard`:

   ```
   # engine-config -g UserDefinedVMProperties
   UserDefinedVMProperties:  version: 3.6
   UserDefinedVMProperties:  version: 4.0
   UserDefinedVMProperties:  memory=^[0-9]+$;smartcard=^(true|false)$
   version: 4.0
   ```

4. Для применения изменений в конфигурации пользовательских свойств ВМ перезапустите службу `ovirt-engine`:

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

Настройка пользовательского свойства `interface` (свойство устройства)

1. Выполните следующую команду для проверки уже имеющихся пользовательских свойств устройства, настроенных ключом конфигурации `CustomDeviceProperties`:

   ```
   # engine-config -g CustomDeviceProperties
   ```

   Из вывода ниже видно, что пользовательские свойства для устройства ещё не были настроены:

   ```
   # engine-config -g CustomDeviceProperties
   CustomDeviceProperties:  version: 3.6
   CustomDeviceProperties:  version: 4.0
   ```

2. Добавьте новое пользовательское свойство `interface`. При этом укажите, что значение параметра `prop` настраивается в диапазоне от 0 до 99999, а параметр `duplex` может принимать значения `full` или `half`:

```
# engine-config -s CustomDeviceProperties="{type=interface;prop=
{speed=^([0-9]{1,5})$;duplex=^(full|half)$}}" --cver=4.0
```

3. Выполните следующую команду для проверки конфигурации пользовательского свойства `interface`:

```
# engine-config -g CustomDeviceProperties
UserDefinedVMProperties:  version: 3.6
UserDefinedVMProperties:  version: 4.0
UserDefinedVMProperties: {type=interface;prop={speed=^([0-9]{1,5})$;
duplex=^(full|half)$}} version: 4.0
```

4. Для применения изменений в конфигурации пользовательских свойств устройства перезапустите службу `ovirt-engine`:

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

A.8. Настраиваемые пользователем свойства ВМ

Как только пользовательские свойства были настроены в виртуализированном ЦУ, можно начинать настраивать их на виртуальных машинах. Пользовательские свойства настраиваются во вкладке **Настраиваемые пользователем свойства** окон **Новая ВМ** и **Параметры виртуальной машины** на Портале администрирования.

Пользовательские свойства также можно настроить в диалоговом блоке **Запуск ВМ**. Свойства, настраиваемые в этом блоке, применяются к ВМ только до следующего выключения этой ВМ.

Вкладка **Настраиваемые пользователем свойства** предоставляет возможность выбора из списка настроенных пользовательских свойств. После выбора ключа пользовательского свойства открывается дополнительное поле, в котором необходимо указать значение выбранного ключа. Добавляйте дополнительные пары «ключ-значение», нажимая на кнопку + (плюс), и удаляйте их с помощью кнопки – (минус).

A.9. Оценка пользовательских свойств ВМ в перехватчике событий VDSM

Во время вызова сценариев перехватчиков событий каждый ключ, указанный в поле **Настраиваемые пользователем свойства** виртуальной машины, добавляется в качестве переменной окружения. Хотя регулярные выражения, используемые для валидации полей **Настраиваемых пользователем свойств**, предоставляют некоторую защиту, необходимо обеспечить также оценку соответствия ввода значениям, ожидаемым регулярными выражениями.

Оценка настраиваемых пользователем свойств

Следующий пример, написанный на Python, проверят существование пользовательского свойства `key1`. Если свойство настроено, тогда его значение выводится в стандартных ошибках. Если пользовательское свойство `key1` не настроено, никаких действий не предпринимается.

```
#!/usr/bin/python

import os
```

```
import sys

if os.environ.has_key('key1'):
 sys.stderr.write('key1 value was : %s\n' % os.environ['key1'])
else:
    sys.exit(0)
```

A.10. Использование модуля перехватчиков событий VDSM

В составе VDSM поставляется модуль перехватчиков событий, написанный на Python, который предоставляет вспомогательные функции для сценариев перехватчиков событий VDSM. Данный модуль предоставляется в качестве примера, и относится только к перехватчикам VDSM, написанным на Python.

Модуль перехватчиков событий поддерживает чтение XML библиотеки `libvirt` виртуальной машины в объект DOM. Далее, сценарии перехватчиков событий управляют объектом с помощью Python, встроенного в библиотеку `xml.dom` (http://docs.python.org/release/2.6/library/xml.dom.html). Затем с помощью модуля перехватчиков изменённый объект можно снова сохранить в XML библиотеки `libvirt`.

В **Табл. A.2** описываются функции модуля перехватчиков событий, предназначенные для поддержки разработки перехватчиков.

Табл. A.2. Функции модуля перехватчиков событий

Имя	Аргумент	Описание
`tobool`	строка	Преобразовывает строку «верно» или «ложно» в логическое значение
`read_domxml`		Читает XML библиотеки libvirt виртуальной машины в объект DOM
`write_domxml`		Записывает XML библиотеки libvirt виртуальной машины в объект DOM

A.11. Выполнение перехватчиков событий VDSM

Некоторые сценарии перехватчиков событий могут редактировать XML домена и изменять параметры VDSM виртуальной машины. Выполнять эти действия нужно с осторожностью. Сценарии перехватчиков событий потенциально могут нарушить работу VDSM, а сценарии с программными ошибками могут привести к перерывам в работе окружения системы виртуализации ROSA Virtualization. В частности, никогда не изменяйте UUID домена, и не пытайтесь удалять устройства из доменов без достаточного понимания процесса и последствий.

Как сценарий `before_vdsm_start`, так и сценарий `after_vdsm_stop` выполняются от имени суперпользователя `root`. Другие сценарии, которым необходим доступ `root`, должны писаться с использованием команды `sudo` для повышения привилегий. Для поддержки этого необходимо обновить информацию в файле `/etc/sudoers` так, чтобы пользователь `vdsm` мог использовать `sudo` без повторного введения пароля, так как сценарии перехватчиков событий выполняются без вмешательства со стороны пользователя.

Настройка `sudo` для сценариев перехватчиков событий VDSM

В следующем примере команда `sudo` будет настроена так, чтобы разрешить пользователю `vdsm` выполнять команду `/bin/chown` от имени суперпользователя `root`.

1. Выполните вход в систему хоста виртуализации с правами `root`.
2. Откройте файл `/etc/sudoers` в текстовом редакторе.
3. Добавьте в файл следующую строку:

```
vdsm ALL=(ALL) NOPASSWD: /bin/chown
```

В результате пользователь `vdsm` может запускать команду `/bin/chown` от имени суперпользователя `root`. Параметр `NOPASSWD` указывает, что при вызове `sudo` не будет предлагаться пользователю ввести пароль.

Таким образом после внесения этих изменений, в перехватчиках событий VDSM также можно использовать команду `sudo` для запуска `/bin/chown` от имени суперпользователя `root`.

В следующем коде на Python команда `sudo` используется для выполнения `/bin/chown` с правами суперпользователя `root` относительно файла `/my_file`:

```
retcode = subprocess.call( ["/usr/bin/sudo", "/bin/chown", "root",
"/my_file"] )
```

Примечание — поток стандартных ошибок сценариев перехватчиков событий собирается в журнале VDSM. Эту информацию можно использовать при отладке сценариев перехватчиков событий.

A.12. Коды возврата перехватчиков событий VDSM

В **Табл. A.3** описываются коды возврата сценариев перехватчиков событий. Коды возврата определяют, обрабатывает ли VDSM сценарий.

Табл. A.3. Коды возврата перехватчиков событий

Код	Описание
0	Сценарий перехватчика событий успешно завершил работу
1	Сценарий перехватчика событий завершился сбоем, нужно обрабатывать другие перехватчики
2	Сценарий перехватчика событий завершился сбоем, другие перехватчики обрабатывать не нужно
>2	Зарезервировано

A.13. Примеры перехватчиков событий VDSM

Примечание — все сценарии перехватчиков событий, устанавливаемые в систему администратором, вне зависимости от их происхождения, должны быть тщательно протестированы для конкретного окружения.

Тонкая настройка узла NUMA

Данный сценарий перехватчика событий даёт возможность отрегулировать выделение памяти на хосте NUMA с использованием настроенного пользователем свойства `numaset`:

```
numaset=^(interleave|strict|preferred):[\^]?\d+(-\d+)?(,[\^]?\d+(-\d+)?)*$
```

Используемое регулярное выражение даёт возможность настроенному пользователем свойству `numaset` конкретной ВМ указать как режим распределения памяти (`interleave`, `strict`, `preferred`), так и используемый узел. При этом два значения разделяются двоеточием (`:`).

С помощью регулярного выражения можно указать `nodeset` как:

- Конкретный узел (например `numaset=strict:1` указывает, что будет использован только узел 1).
- Диапазон узлов (например `numaset=strict:1-4` указывает, что будут использоваться узлы с 1 по 4).

- Неиспользуемый узел (например `numaset=strict:^3` указывает, что узел 3 не будет использоваться).
- Любое сочетание вышеуказанных значений, через запятые (например `numaset=strict:1-4,6` указывает, что будут использоваться узлы с 1 по 4, а также узел 6).

Сценарий перехватчика событий `/usr/libexec/vdsm/hooks/before_vm_start/50_numa`:

```
#!/usr/bin/python

import os
import sys
import hooking
import traceback

'''
numa hook
=========
add numa support for domain xml:

<numatune>
    <memory mode="strict" nodeset="1-4,^3" />
</numatune>

memory=interleave|strict|preferred

numaset="1" (use one NUMA node)
numaset="1-4" (use 1-4 NUMA nodes)
numaset="^3" (don't use NUMA node 3)
numaset="1-4,^3,6" (or combinations)

syntax:
    numa=strict:1-4
'''

if os.environ.has_key('numa'):
    try:
        mode, nodeset = os.environ['numa'].split(':')

        domxml = hooking.read_domxml()

        domain = domxml.getElementsByTagName('domain')[0]
        numas = domxml.getElementsByTagName('numatune')

        if not len(numas) > 0:
            numatune = domxml.createElement('numatune')
            domain.appendChild(numatune)

            memory = domxml.createElement('memory')
            memory.setAttribute('mode', mode)
            memory.setAttribute('nodeset', nodeset)
            numatune.appendChild(memory)

            hooking.write_domxml(domxml)
        else:
```

```
            sys.stderr.write('numa: numa already exists in domain
xml')
            sys.exit(2)
    except:
        sys.stderr.write('numa: [unexpected error]: %s\n' %
traceback.format_exc())
        sys.exit(2)
```

Приложение B. Свойства сетей, настраиваемые пользователем

B.1. Параметры bridge_opts

В **Табл. B.1** описываются параметры `bridge_opts`.

Табл. B.1. Параметры bridge_opts

Параметр	Описание
forward_delay	Временной интервал в децисекундах, во время которого мост слушает и получает информацию. Если за это время не будет обнаружена петля коммутации, мост войдёт в состояние передачи данных. Этот параметр даёт время на проверку трафика и структуры сети до начала обычной работы сети
gc_timer	Параметр указывает время сборки мусора в децисекундах, после которого база данных, данные для которой передаёт мост, проверяется и очищается от устаревших записей
group_addr	При отправке общего запроса значение параметра устанавливается на ноль. При отправке запроса, касающегося конкретной группы, а также запроса, касающегося группы и источника, значение параметра устанавливается на IP-адрес многоадресной рассылки
group_fwd_mask	Параметр даёт возможность мосту передавать локальные адреса групп каналов. Смена изначального значения параметра разрешает нестандартное поведение моста
hash_elasticity	Максимальная длина цепи, разрешённая в хэш-таблице. Значение параметра вступает в силу после добавления новой многоадресной группы. Если после повторного хэширования значение не может быть соблюдено, то происходит хэш-конфликт, и отслеживание отключается
hash_max	Максимальное число хэш-сегментов в таблице. Значение параметра должно быть степенью числа 2. Значение вступает в силу немедленно, и это значение не может быть меньше текущего значения записей многоадресных групп
hello_time	Временной интервал в децисекундах между отправками сообщений 'hello', сообщающих о местоположении моста в сетевой топологии. Применяется, только если данный мост является корневым мостом связующего дерева
hello_timer	Время в децисекундах с последней отправки сообщения 'hello'
max_age	Максимальный промежуток времени в децисекундах, для получения сообщения 'hello' от другого корневого моста, после которого мост будет считаться «мёртвым» и начнётся процесс перехвата полномочий
multicast_last_member_count	Параметр указывает число запросов 'last member', посылаемых в многоадресную группу, после принятия сообщения 'leave group' от хоста
multicast_last_member_interval	Время в децисекундах между запросами 'last member'
multicast_membership_interval	Время в децисекундах, в течение которого мост ждёт ответа от участника многоадресной группы перед прекращением отправки многоадресного трафика на хост
multicast_querier	Параметр указывает, будет ли на мосту активно работать многоадресный опрашиватель или нет. При получении мостом запроса 'multicast host membership' от хоста в другой сети, этот хост отслеживается в течение таймера, основанного на времени получения запроса и времени интервала между многоадресными запросами. Если мост позднее попытается перенаправить трафик этого запроса на членство в многоадресной группе, или обменяется информацией с запрашивающим многоадресным роутером, то указанный таймер

Параметр	Описание
	подтвердит действительность опрашивателя. Если опрашиватель действителен, многоадресный трафик доставляется с помощью существующей многоадресной таблицы моста. Если опрашиватель не действителен, трафик посылается со всех портов моста. Для увеличения производительности в широковещательных доменах с существующим или ожидаемым многоадресным членством должен работать как минимум один многоадресный опрашиватель
multicast_querier_interval	Максимальный промежуток времени в децисекундах от последнего запроса 'multicast host membership', полученного от хоста, для подтверждения того, что хост действителен
multicast_query_use_ifaddr	Логическое значение. По умолчанию «0», и в этом случае опрашиватель в качестве адреса-источника для запросов IPv4 использует 0.0.0.0. При изменении значения по умолчанию, в качестве адреса-источника устанавливается IP-адрес моста
multicast_query_interval	Время в децисекундах между сообщениями запросов, посылаемых мостом для подтверждения действительности участия в многоадресных группах. В этом промежутке, а также если мост попросили отослать запрос на членство в этой многоадресной группе, мост проверяет состояние своего собственного опрашивателя, основываясь на времени получения запроса плюс значение multicast_query_interval. Если запрос был послан в рамках значения последнего интервала multicast_query_interval, то повторно он не посылается
multicast_query_response_interval	Промежуток времени в децисекундах, в течение которого мосту можно ответить на запрос после отправки. Значение должно быть меньше или равно значению multicast_query_interval
multicast_router	Параметр даёт возможность включать или отключать порты с подключёнными мультивещательными маршрутизаторами. Порт с одним или несколькими мультивещательными маршрутизаторами получит весь многоадресный трафик. Параметр может принимать следующие значения: 0 — полностью отключает; 1 — система с помощью запросов автоматически определяет присутствие маршрутизаторов; 2 — активирует постоянное получение всего многоадресного трафика на портах
multicast_snooping	Параметр даёт возможность включать или отключать механизм отслеживания. Процесс отслеживания трафика позволяет мосту прослушивать трафик между маршрутизаторами и хостами для поддержания карты фильтрации многоадресного трафика на соответствующие каналы. Параметр даёт возможность пользователю повторно включить отслеживание, если оно было автоматически выключено из-за хэш-конфликта, но если хэш-конфликт не был разрешён, отслеживание включено не будет
multicast_startup_query_count	Параметр указывает число запросов, отправленных при запуске для определения информации о многоадресном членстве
multicast_startup_query_interval	Время в децисекундах между запросами, отправленными при запуске для определения информации о многоадресном членстве

B.2. Настройка использования команды ethtool в виртуализированном ЦУ

На Портале администрирования можно настроить свойства `ethtool` для сетевых карт хоста. По умолчанию ключ `ethtool_opts` недоступен, его необходимо добавить в

виртуализированный ЦУ с помощью утилиты настройки ЦУ. Также на хостах необходимо установить дополнительный пакет перехватчиков событий для VDSM.

Добавление ключа ethtool_opts в виртуализированный ЦУ

1. Выполните следующую команду на машине виртуализированного ЦУ для добавления ключа `ethtool_opts`:

   ```
   # engine-config -s UserDefinedNetworkCustomProperties=ethtool_opts=.*
   --cver=4.0
   ```

2. Для применения изменений в конфигурации перезапустите службу `ovirt-engine`:

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

3. На тех хостах, где нужно настроить параметры `ethtool`, установите пакет с перехватчиками событий VDSM. По умолчанию пакет `vdsm-hook-ethtool-options` установлен на хостах виртуализации, а на стандартных хостах его необходимо установить дополнительно. Для этого выполните следующую команду:

   ```
   # yum install vdsm-hook-ethtool-options
   ```

В результате на Портале администрирования станет доступен ключ `ethtool_opts`.

B.3. Настройка использования протокола FCoE в виртуализированном ЦУ

На Портале администрирования можно настроить параметры протокола FCoE для сетевых карт хоста. По умолчанию ключ `fcoe` недоступен, его необходимо добавить в виртуализированный ЦУ с помощью утилиты настройки ЦУ. Также на хостах необходимо установить дополнительный пакет перехватчиков событий для VDSM. В зависимости от типа карты FCoE на хосте, может потребоваться настройка дополнительных параметров.

Примечание — для проверки, был ли уже активирован ключ `fcoe`, выполните следующую команду:

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

Добавление ключа fcoe в виртуализированный ЦУ

1. Выполните следующую команду на машине виртуализированного ЦУ для добавления ключа `fcoe`:

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

2. Для применения изменений в конфигурации перезапустите службу `ovirt-engine`:

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

3. На тех хостах, где нужно настроить параметры FCoE, установите пакет с перехватчиками событий VDSM. По умолчанию пакет `vdsm-hook-fcoe` установлен на хостах виртуализации, а на стандартных хостах его необходимо установить дополнительно. Для этого выполните следующую команду:

   ```
   # yum install vdsm-hook-fcoe
   ```

В результате на Портале администрирования станет доступен ключ `fcoe`.

Приложение C. Модули пользовательского интерфейса

C.1. Модули пользовательского интерфейса

В системе виртуализации ROSA Virtualization существует поддержка модулей пользовательского интерфейса (модулей UI), что позволяет интегрировать Портал администрирования с другими системами. Каждый модуль UI представляет собой набор расширений UI, который можно поместить в пакет и распространять для использования в системе виртуализации.

Модули пользовательского интерфейса системы виртуализации ROSA Virtualization интегрируются в Портал администрирования напрямую на клиенте с помощью языка программирования JavaScript. Модули вызываются Порталом администрирования и выполняются во время выполнения JavaScript веб-браузера. Модули UI могут использовать язык JavaScript и его библиотеки.

Во время ключевых событий в течение времени их выполнения Портал администрирования вызывает отдельные модули с помощью функций обработки событий, представляющих собой обмен информацией между Порталом администрирования и модулем. Хотя Портал администрирования поддерживает множество функций обработки событий, модуль объявляет только те функции, которые представляют интерес для его реализации. Перед запуском в работу Порталом администрирования, каждый модуль должен зарегистрировать соответствующие функции обработки событий как часть последовательности программы самозагрузки модуля.

Для облегчения обмена информацией между модулем UI и Порталом администрирования открывается доступ к API модуля как к глобальному (верхнего уровня) объекту pluginApi, который может быть поглощён отдельными модулями. Каждый модуль получает отдельный экземпляр pluginApi, давая возможность Порталу администрирования контролировать вызовы функций API этого модуля со стороны каждого отдельного модуля с учётом жизненного цикла модуля.

C.2. Жизненный цикл модуля пользовательского интерфейса

C.2.1. Этапы жизненного цикла модуля пользовательского интерфейса

Базовый жизненный цикл модуля пользовательского интерфейса разделён на следующие этапы:

- Обнаружение модуля UI.
- Загрузка модуля UI.
- Самонастройка модуля UI.

C.2.2. Обнаружение модуля пользовательского интерфейса

Создание дескрипторов модуля — это первый шаг в процессе обнаружения модуля UI. Дескрипторы модуля содержат важные метаданные модуля и возможные конфигурации модуля UI.

Как часть обработки запросов страницы HTML Портала администрирования (`HTTP GET`), инфраструктура модуля UI пытается обнаружить и загрузить дескрипторы из локальной файловой системы. Для каждого дескриптора инфраструктура также пытается загрузить соответствующие пользовательские конфигурации, используемые для

переопределения параметров модуля по умолчанию (если такие есть) и настроить поведение модуля во время исполнения. Пользовательская конфигурация модуля является опциональной. После загрузки дескрипторов и соответствующих файлов пользовательских конфигураций, `oVirt Engine` собирает данные модуля UI и встраивает их в страницу HTML Портала администрирования для оценки во время исполнения.

По умолчанию дескрипторы модуля расположены в `$ENGINE_USR/ui-plug-ins` с отображением по умолчанию на `ENGINE_USR=/usr/share/ovirt-engine`, что настроено в локальной конфигурации `oVirt Engine`. Ожидается, что дескрипторы модуля отвечают требованиям спецификаций формата JSON, но в дескрипторах разрешаются комментарии в стиле Java/C++ (`/*` и `//`) в качестве дополнения к спецификациям JSON.

По умолчанию пользовательские конфигурации модуля расположены в `$ENGINE_ETC/ui-plug-ins`, с отображением по умолчанию на `ENGINE_USR=/usr/share/ovirt-engine`, что настроено в локальной конфигурации `oVirt Engine`. Ожидается, что пользовательские конфигурации модуля отвечают требованиям тех же спецификаций, что и дескрипторы.

Примечание — конфигурационные файлы модуля обычно следуют соглашению о наименованиях `<descriptorFileName>-config.json`.

C.2.3. Загрузка модуля пользовательского интерфейса

После обнаружения и встраивания данных модуля UI в страницу HTML Портала администрирования осуществляется загрузка модуля в составе запуска приложения (если только для модуля не была отключена такая загрузка).

Для каждого обнаруженного модуля Портал администрирования создаёт элемент HTML `iframe`, используемый для загрузки страницы хоста модуля. Страница хоста модуля необходима для начала процесса самонастройки, используемого для оценки кода модуля в контексте элемента `iframe` этого модуля. Инфраструктура модуля UI поддерживает обслуживание файлов ресурсов модуля (например, страница хоста модуля) из локальной файловой системы. Страница хоста модуля загружается в элемент `iframe`, и происходит оценка кода модуля. После оценки кода модуль UI обменивается информацией с Порталом администрирования с помощью API.

C.2.4. Самонастройка модуля пользовательского интерфейса

Процесс самонастройки модуля UI состоит из последовательного выполнения следующих шагов:

1. Получите экземпляр `pluginApi` для указанного модуля.
2. Опционально получите объект конфигурации модуля времени выполнения.
3. Зарегистрируйте функции соответствующего обработчика событий.
4. Сообщите инфраструктуре модуля UI, что можно инициализировать модуль.

Примечание — следующий отрывок кода демонстрирует процесс самонастройки модуля UI:

```
// Access plug-in API using 'parent' due to this code being evaluated
within the context of an iframe element.
// As 'parent.pluginApi' is subject to Same-Origin Policy, this will
only work when WebAdmin HTML page and plug-in
// host page are served from same origin. WebAdmin HTML page and plug-
in host page will always be on same origin
```

```
// when using UI plug-in infrastructure support to serve plug-in
resource files.
var api = parent.pluginApi('MyPlugin');

// Runtime configuration object associated with the plug-in (or an
empty object).
var config = api.configObject();

// Register event handler function(s) for later invocation by UI plug-
in infrastructure.
api.register({
     // UiInit event handler function.
         UiInit: function() {
                         // Handle UiInit event.
                                 window.alert('Favorite music band is '
+ config.band);
                                         }
});

// Notify UI plug-in infrastructure to proceed with plug-in
initialization.
api.ready();
```

C.3. Файлы модуля пользовательского интерфейса

В **Табл. C.1** описываются файлы модуля UI, а также указывается расположение этих файлов в системе.

Табл. C.1. Файлы модуля UI

Файл	Расположение	Примечания
Файлы дескриптора модуля (метаданные)	/usr/share/ovirt-engine/ui-plugins/my-plugin.json	
Пользовательские файлы конфигурации модуля	/etc/ovirt-engine/ui-plugins/my-plugin-config.json	
Файлы ресурсов модуля	/usr/share/ovirt-engine/ui-plugins/<resourcePath>/PluginHostPage.html	<resourcePath> настраивается с помощью соответствующего атрибута дескриптора модуля

C.4. Пример развёртывания модуля пользовательского интерфейса

В следующей пошаговой инструкции описывается процесс создания модуля UI, запускающего программу `Hello World!` при выполнении входа в систему на Портале администрирования виртуализированного ЦУ.

Развёртывание модуля `Hello World!`

1. Создайте следующий дескриптор модуля в виде файла `/usr/share/ovirt-engine/ui-plugins/helloWorld.json` в виртуализированном ЦУ:

```
{
    "name": "HelloWorld",
    "url": "/ovirt-engine/webadmin/plugin/HelloWorld/start.html",
    "resourcePath": "hello-files"
}
```

2. Создайте следующую страницу хоста модуля в виде файла `/usr/share/ovirt-engine/ui-plugins/hello-files/start.html` в виртуализированном ЦУ:

```
<!DOCTYPE html><html><head>
<script>
    var api = parent.pluginApi('HelloWorld');
    api.register({
  UiInit: function() { window.alert('Hello world'); }
    });
    api.ready();
</script>
</head><body></body></html>
```

В случае успешной реализации модуля `Hello World!` следующая заставка (G) появится при выполнении входа в систему на Портале администрирования виртуализированного ЦУ.

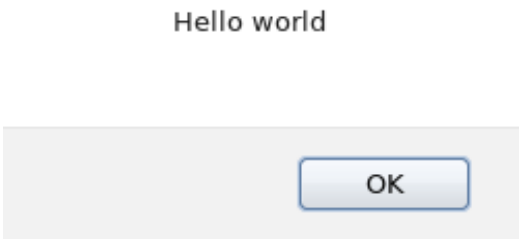

Рис. 55. Заставка модуля Hello World!

Приложение D. Система виртуализации и шифрование связи

D.1. Замена сертификата ЦС виртуализированного ЦУ

Идентификацию пользователей виртуализированного ЦУ, подключающихся с использованием протокола HTTPS, можно выполнять с помощью сертификата стороннего Центра сертификации (ЦС) организации.

Примечание — использование сертификата стороннего ЦС для подключений по протоколу HTTPS не влияет на сертификат, используемый для аутентификации между виртуализированным ЦУ и хостами, так как в последнем случае используется самоподписанный сертификат, созданный виртуализированным ЦУ.

Перед выполнением процедуры замены сертификата ЦС виртуализированного ЦУ убедитесь в наличии и характеристиках следующих информационных объектов:

- Сертификат стороннего ЦС. Цепочка сертификатов должна отслеживаться вплоть до корневого сертификата. В процедуре подразумевается, что сертификат стороннего ЦС находится в `/tmp/3rd-party-ca-cert.pem`.
- Закрытый ключ, который планируется для использования с Apache httpd, не должен содержать пароль. В процедуре подразумевается, что закрытый ключ находится в `/tmp/apache.key`.
- Сертификат ключа, выпущенный сторонним ЦС. В процедуре подразумевается, что сертификат ключа находится в `/tmp/apache.cer`.

Предупреждение — не изменяйте владельца и права доступа к каталогу `/etc/pki` и его подкаталогам. Права доступа для каталогов `/etc/pki` и `/etc/pki/ovirt-engine` должны оставаться правами по умолчанию, то есть `755`.

Если закрытый ключ и сертификат ключа были получены из стороннего ЦС в виде файла с расширением `*.p12`, извлеките их с помощью следующей инструкции, в которой подразумевается, что полученный файл находится в `/tmp/apache.p12`. В случае других форматов файла свяжитесь со сторонним ЦС для консультации.

Извлечение сертификата и закрытого ключа из файла с расширением `*.p12`

Примечание — внутренний ЦС системы хранит закрытый ключ и сертификат ключа в файле `/etc/pki/ovirt-engine/keys/apache.p12`.

1. Создайте резервную копию текущего файла `apache.p12`:

```
# cp -p /etc/pki/ovirt-engine/keys/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12.bck
```

2. Замените текущий файл на файл, полученный из стороннего ЦС:

```
# cp /tmp/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

3. Извлеките закрытый ключ и сертификат ключа в необходимое местоположение (если файл защищён паролем, добавьте параметр `-passin pass:`*`password`*, где замените *`password`* текущим паролем):

```
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nocerts -nodes > /tmp/apache.key
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nokeys > /tmp/apache.cer
```

Замена сертификата ЦС виртуализированного ЦУ для Apache

1. Переведите окружение в режим глобального обслуживания:

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

2. Добавьте сертификат стороннего ЦС в хранилище доверенных сертификатов хоста:

```
# cp /tmp/3rd-party-ca-cert.pem /etc/pki/ca-trust/source/anchors
# update-ca-trust
```

3. Удалите символьную ссылку `/etc/pki/ovirt-engine/apache-ca.pem` на `/etc/pki/ovirt-engine/ca.pem`, настроенную в виртуализированном ЦУ по умолчанию:

```
# rm /etc/pki/ovirt-engine/apache-ca.pem
```

4. Сохраните сертификат ЦС как `/etc/pki/ovirt-engine/apache-ca.pem`:

```
# cp /tmp/3rd-party-ca-cert.pem /etc/pki/ovirt-engine/apache-ca.pem
```

5. Создайте резервную копию закрытого ключа и сертификата ключа:

```
# cp /etc/pki/ovirt-engine/keys/apache.key.nopass /etc/pki/ovirt-engine/keys/apache.key.nopass.bck
# cp /etc/pki/ovirt-engine/certs/apache.cer /etc/pki/ovirt-engine/certs/apache.cer.bck
```

6. Скопируйте закрытый ключ в необходимое местоположение:

```
# cp /tmp/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
```

7. Укажите суперпользователя `root` в качестве владельца закрытого ключа и настройте права доступа `0640`:

```
# chown root:ovirt  /etc/pki/ovirt-engine/keys/apache.key.nopass
# chmod 640 /etc/pki/ovirt-engine/keys/apache.key.nopass
```

8. Скопируйте сертификат в необходимое местоположение:

```
# cp /tmp/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

9. Перезапустите веб-сервер Apache:

```
# systemctl restart httpd.service
```

10. Создайте новый файл конфигурации `/etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf` для хранилища доверенных сертификатов со следующими параметрами:

```
ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

11. Скопируйте файл `/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf`, переименуйте этот файл с применением для индекса номера больше 10 (например, `99-setup.conf`) и добавьте в новый переименованный файл следующие параметры:

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/certs/apache.cer
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```

12. Перезапустите службу `ovirt-websocket-proxy`:

```
# systemctl restart ovirt-websocket-proxy.service
```

13. Если файл `/etc/ovirt-provider-ovn/conf.d/10-setup-ovirt-provider-ovn.conf` был отредактирован вручную убедитесь, что в виртуализированном ЦУ в качестве источника сертификата по-прежнему используется `/etc/pki/ovirt-engine/apache-ca.pem`.
14. Для включения в `engine-backup` возможности обновления при восстановлении создайте новый файл `/etc/ovirt-engine-backup/engine-backup-config.d/update-system-wide-pki.sh` со следующими строками:

```
BACKUP_PATHS="${BACKUP_PATHS}
/etc/ovirt-engine-backup"
cp -f /etc/pki/ovirt-engine/apache-ca.pem
/etc/pki/ca-trust/source/anchors/3rd-party-ca-cert.pem
update-ca-trust
```

15. Перезапустите службу `ovirt-provider-ovn`:

```
# systemctl restart ovirt-provider-ovn.service
```

16. Перезапустите службу `ovirt-engine`:

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

17. Отключите глобальный режим обслуживания:

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

В результате при подключении пользователей к Порталу администрирования и Порталу ВМ не будет появляться предупреждение о подлинности сертификата, используемого для шифрования трафика HTTPS.

D.2. Настройка шифрованного соединения между виртуализированным ЦУ и сервером LDAP

Для настройки шифрованного соединения между виртуализированным ЦУ и сервером LDAP получите корневой сертификат ЦС сервера LDAP, скопируйте этот сертификат на машину виртуализированного ЦУ и создайте сертификат ЦС в кодировке PEM.

Тип файла ключа может быть любым типом, поддерживаемым Java. В приведенной ниже процедуре используется файл ключа с расширением `*.jks` в формате Java KeyStore.

Примечание — дополнительные сведения о создании сертификатов ЦС в кодировке PEM, а также об импортировании сертификатов можно посмотреть в разделе `X.509 CERTIFICATE TRUST STORE` файла `README` в каталоге `/usr/share/doc/ovirt-engine-extension-aaa-ldap-`*`версия`*.

Создание сертификата ЦС в кодировке PEM

1. На машине виртуализированного ЦУ скопируйте корневой сертификат ЦС сервера LDAP в каталог `/tmp` и импортируйте корневой сертификат с применением команды `keytool` для создания сертификата ЦС в кодировке PEM:

```
$ keytool -importcert -noprompt -trustcacerts -alias myrootca -file
/tmp/myrootca.pem -keystore /etc/ovirt-engine/aaa/myrootca.jks -
storepass password
```

Приведенная команда импортирует корневой сертификат ЦС в файл */tmp/myrootca.pem* и создаёт сертификат ЦС в кодировке PEM *myrootca.jks* в каталоге */etc/ovirt-engine/aaa/*.

2. Обновите информацию о сертификате в файле `/etc/ovirt-engine/aaa/profile1.properties` с использованием startTLS (рекомендуемый способ) или SSL:
   - С использованием startTLS:

     ```
     # Create keystore, import certificate chain and uncomment
     pool.default.ssl.startTLS = true
     pool.default.ssl.truststore.file = ${local:_basedir}/myrootca.jks
     pool.default.ssl.truststore.password = password
     ```

   - С использованием SSL:

     ```
     # Create keystore, import certificate chain and uncomment
     pool.default.serverset.single.port = 636
     pool.default.ssl.enable = true
     pool.default.ssl.truststore.file = ${local:_basedir}/myrootca.jks
     pool.default.ssl.truststore.password = password
     ```

Примечание — `${local:_basedir}` является каталогом, в котором расположен файл конфигурации LDAP `property`, который указывает на каталог `/etc/ovirt-engine/aaa`. Если сертификат ЦС в кодировке PEM был создан в другом каталоге, замените `${local:_basedir}` на полный путь до сертификата.

D.3. Настройка шифрования соединений VDSM вручную

Шифрование соединений VDSM с виртуализированным ЦУ и с другими экземплярами VDSM можно настроить вручную.

Ручная настройка требуется только для хостов в кластерах с уровнем кластера 3.6, 4.0 и 4.1. Стойкое шифрование на хостах в кластерах с уровнем 4.2 настраивается автоматически во время переустановок хостов. При наличии кластеров 3.6, 4.0 или 4.1 с хостами виртуализации версии 4.2 используйте стойкое шифрование.

Настройка шифрования соединений VDSM вручную

1. Нажмите **Ресурсы → Хосты** и выберите хост.
2. Нажмите **Управление → Обслуживание**, чтобы открыть окно подтверждения **Хосты на обслуживании**.
3. Нажмите **OK**, чтобы запустить режим обслуживания.
4. Создайте на хосте файл `/etc/vdsm/vdsm.conf.d/99-custom-ciphers.conf` со следующим параметром:

   ```
   [vars]
   ssl_ciphers = HIGH
   ```

5. Перезапустите службу VDSM:

   ```
   # systemctl restart vdsm
   ```

6. Нажмите **Ресурсы → Хосты** и выберите хост.
7. Нажмите **Управление → Активировать**, чтобы повторно активировать хост.

Приложение Е. Прокси

Е.1. Прокси-сервер SPICE

Е.1.1. Обзор SPICE Proxy

SPICE Proxy — это утилита, используемая для подключения клиентов SPICE к ВМ, когда клиенты SPICE находятся вне сети, соединяющей гипервизоры. Настройка SPICE Proxy состоит из установки на машине прокси-сервера `Squid` и настройки межсетевого экрана для разрешения трафика прокси. Процесс включения SPICE Proxy состоит из запуска на виртуализированном ЦУ утилиты `engine-config` для настройки значения ключа `SpiceProxyDefault`, состоящего из имени и порта прокси. Процесс выключения SPICE Proxy состоит из запуска на виртуализированном ЦУ утилиты `engine-config` для удаления ранее настроенного значения ключа `SpiceProxyDefault`.

Примечание — утилиту SPICE Proxy можно использовать только в сочетании с одиночным клиентом SPICE и нельзя использовать для подключения к ВМ, использующим noVNC.

Е.1.2. Настройка машины SPICE Proxy

В следующей последовательности действий описывается как настроить машину в качестве SPICE Proxy. SPICE Proxy делает возможным подключение извне к сети системы виртуализации ROSA Virtualization. Для предоставления служб прокси используется `Squid`.

Установка `Squid`

1. Установите `Squid` на машине прокси:

   ```
   # yum install squid
   ```

2. В конфигурационном файле `/etc/squid/squid.conf` в строке `http_access deny CONNECT` замените значение `!SSL_ports` на значение `!Safe_ports`.
3. Запустите службу `squid` и включите автоматический запуск этой службы в процессе загрузки системы:

   ```
   # systemctl enable squid.service --now
   ```

4. Разрешите исходящие запросы на службу `squid` в зоне по умолчанию межсетевого экрана `firewalld`:

   ```
   # firewall-cmd --permanent --add-service=squid
   ```

5. Для применения изменений в конфигурации перезапустите службу межсетевого экрана `firewalld`:

   ```
   # firewall-cmd --reload
   ```

В результате данная машина будет настроена для протокола SPICE в качестве прокси.

Активируйте (включите) прокси перед тем, как подключаться извне к сетям системы виртуализации ROSA Virtualization.

Е.1.3. Включение SPICE Proxy

В следующей последовательности действий описывается как активировать (включить) прокси для протокола SPICE.

Активация SPICE Proxy

1. На машине виртуализированного ЦУ выполните следующую команду с применением утилиты `engine-config` для настройки прокси:

   ```
   # engine-config -s SpiceProxyDefault=someProxy
   ```

2. Перезапустите службу `ovirt-engine`:

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

В результате SPICE Proxy будет активирован (включён), предоставляя возможность подключения извне к сетям системы виртуализации ROSA Virtualization через прокси-сервер для протокола SPICE.

Запись прокси должна быть в формате `protocol://[host]:[port]`.

Примечание — поддержка прокси HTTPS доступна только для клиентов SPICE, поставляемых в составе системы виртуализации ROSA Virtualization. Клиенты в более ранних версиях ОС поддерживают только HTTP. Если указать HTTPS для клиентов более ранних версий, клиент проигнорирует настройку прокси и будет пробовать прямое подключение к хосту.

E.1.4. Выключение SPICE Proxy

В следующей последовательности действий описывается как выключить (деактивировать) прокси для протокола SPICE.

Выключение SPICE Proxy

1. На машине виртуализированного ЦУ выполните следующую команду для очистки прокси SPICE:

   ```
   # engine-config -s SpiceProxyDefault=""
   ```

2. Перезапустите службу `ovirt-engine`:

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

В результате SPICE Proxy будет деактивирован (выключен) и подключение извне к сетям системы виртуализации ROSA Virtualization через прокси-сервер для протокола SPICE станет невозможным.

E.2. Прокси-сервер Squid

E.2.1. Установка и настройка Squid

В данном подразделе объясняется как установить и настроить прокси-сервер Squid для Портала ВМ.

Прокси-сервер Squid используется в качестве ускорителя передачи данных за счет кэширования часто просматриваемого содержимого, что повышает пропускную способность и снижает время откликов.

Настройка прокси-сервера Squid

1. Получите в установленном порядке закрытый ключ и сертификат ключа для порта HTTPS прокси-сервера Squid в виде файлов `proxy.key` и `proxy.cer` соответственно.
2. Установите Squid на машине прокси:

   ```
   # yum install squid
   ```

3. Переместите полученные файлы `proxy.key` и `proxy.cer` с закрытым ключом и сертификатом ключа в каталог машины прокси (например, `/etc/squid`).
4. Установите права на чтение файлов `proxy.key` и `proxy.cer` для пользователя `squid`:

```
# chgrp squid /etc/squid/proxy.*
# chmod 640 /etc/squid/proxy.*
```

5. Squid должен верифицировать сертификат ЦС, используемый виртуализированным ЦУ. Для этого скопируйте с виртуализированного ЦУ сертификат ЦС `/etc/pki/ovirt-engine/ca.pem` на машину прокси в каталог `/etc/squid`, и установите права на чтение файла сертификата `ca.pem` для пользователя `squid`:

```
# chgrp squid /etc/squid/ca.pem
# chmod 640 /etc/squid/ca.pem
```

6. Для принудительного режима SELinux измените контекст порта 443, тем самым разрешив Squid использовать порт 443:

```
# yum install policycoreutils-python
# semanage port -m -p tcp -t http_cache_port_t 443
```

7. Замените текущий файл конфигурации Squid `/etc/squid/squid.conf` следующим содержимым:

```
https_port  443  key=/etc/squid/proxy.key  cert=/etc/squid/proxy.cer
ssl-bump defaultsite=engine.example.com
cache_peer engine.example.com parent 443 0 no-query originserver ssl
sslcafile=/etc/squid/ca.pem name=engine login=PASSTHRU
cache_peer_access engine allow all
ssl_bump allow all
http_access allow all
```

8. Перезапустите службу прокси-сервера Squid:

```
# systemctl restart squid.service
```

Примечание — для увеличения интервала времени простоя Squid перед разрывом соединения (по умолчанию 15 минут простоя) настройте параметр `read_timeout` в файле конфигурации Squid `/etc/squid/squid.conf` (например, следующее значение `read_timeout 10 hours` увеличивает интервал времени простоя до 10 часов).

E.3. Прокси-сервер WebSocket

E.3.1. Обзор прокси-сервера WebSocket

Прокси-сервер WebSocket даёт возможность пользователям подключаться к ВМ с помощью консоли noVNC. Клиент noVNC использует веб-сокеты для передачи данных VNC, но сервер VNC в QEMU не поддерживает технологию веб-сокетов, поэтому между клиентом и сервером VNC необходимо расположить прокси WebSocket. При этом прокси WebSocket может выполняться на любой машине, имеющей доступ к сети, включая машину виртуализированного ЦУ.

Примечание — прокси-сервер WebSocket и консоль noVNC являются экспериментальными технологиями. Экспериментальные возможности не поддерживаются

соглашениями об уровне обслуживания, могут иметь неполную функциональность и не рекомендуются к использованию на производстве, но предоставляют ранний доступ к будущим возможностям продукта, давая клиентам средство протестировать функциональность и предоставить отзывы, полезные для разработчиков.

Прокси-сервер WebSocket можно установить и настроить на машине виртуализированного ЦУ во время начального создания конфигурации ЦУ или на отдельной машине. Также можно провести миграцию WebSocket с машины виртуализированного ЦУ на отдельную машину.

E.3.2. Миграция WebSocket на отдельную машину

По соображениям безопасности или производительности прокси-сервер WebSocket может выполняться на отдельной машине. Действия по переносу WebSocket с машины виртуализированного ЦУ на отдельную машину включают в себя удаление конфигурации WebSocket с машины виртуализированного ЦУ, а затем установку прокси на отдельной машине.

Удаление WebSocket с машины виртуализированного ЦУ

1. Для удаления конфигурации прокси-сервера WebSocket запустите утилиту `engine-cleanup` на машине виртуализированного ЦУ:

   ```
   # engine-cleanup
   ```

2. При запросе на удаление всех компонентов введите `No`:

   ```
   Do you want to remove all components? (Yes, No) [Yes]: No
   ```

3. При запросе на удаление виртуализированного ЦУ (`engine`) введите `No`:

   ```
   Do you want to remove the engine? (Yes, No) [Yes]: No
   ```

4. При запросе на удаление прокси-сервера WebSocket введите `Yes`:

   ```
   Do you want to remove the WebSocket proxy? (Yes, No) [No]: Yes
   ```

5. При запросах на удаление любых других компонентов введите `No`.

Установка WebSocket на отдельной машине

1. Установите прокси-сервер WebSocket:

   ```
   # yum install ovirt-engine-websocket-proxy
   ```

2. Запустите утилиту `engine-setup` для настройки конфигурации прокси-сервера WebSocket:

   ```
   # engine-setup
   ```

Примечание — если в системе ранее был установлен пакет `rhvm`, то при выводе запроса о необходимости настройки виртуализированного ЦУ на этом хосте введите `No`.

3. При выводе следующего запроса нажмите клавишу `Enter` для запуска процесса настройки конфигурации прокси-сервера WebSocket на данной машине:

   ```
   Configure WebSocket Proxy on this machine? (Yes, No) [Yes]:
   ```

4. При выводе следующего запроса нажмите клавишу `Enter`, чтобы принять автоматически определённое имя хоста, или введите альтернативное имя хоста (обратите внимание, что при использовании виртуальных хостов автоматически определённое имя хоста может быть неправильным):

```
Host fully qualified DNS name of this server [host.example.com]:
```

5. При выводе следующего запроса нажмите клавишу `Enter`, чтобы утилита `engine-setup` автоматически настроила межсетевой экран и открыла порты, необходимые для внешних соединений (в противном случае, нужные порты необходимо будет открыть вручную):

```
Setup can automatically configure the firewall on this system.
Note: automatic configuration of the firewall may overwrite current
settings.
Do you want Setup to configure the firewall? (Yes, No) [Yes]:
```

6. При выводе следующего запроса введите полное доменное имя (FQDN) машины виртуализированного ЦУ:

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

7. При выводе следующего запроса нажмите клавишу `Enter`, чтобы утилита `engine-setup` автоматически выполнила необходимые настройки на машине виртуализированного ЦУ, или введите цифру 2, чтобы выполнить эти настройки вручную:

```
Setup will need to do some actions on the remote engine server. Either
automatically, using ssh as root to access it, or you will be prompted
to manually perform each such action.
Please choose one of the following:
1 - Access remote engine server using ssh as root
2 - Perform each action manually, use files to copy content around
(1, 2) [1]:
```

   Настройка вручную:

   a. При выводе следующего запроса нажмите клавишу `Enter`, чтобы принять номер порта SSH по умолчанию, или укажите номер порта SSH машины виртуализированного ЦУ:

```
ssh port on remote engine server [22]:
```

   b. Укажите пароль суперпользователя `root` для выполнения входа в систему на машине виртуализированного ЦУ:

```
root password on remote engine server engine_host.example.com:
```

8. При выводе следующего запроса введите `Yes` для просмотра правил `iptables` на предмет их отличия от текущих параметров:

```
Generated iptables rules are different from current ones.
Do you want to review them? (Yes, No) [No]:
```

9. При выводе ранее настроенных параметров нажмите клавишу `Enter`, чтобы подтвердить текущую конфигурацию:

```
--== CONFIGURATION PREVIEW ==--

Firewall manager                          : iptables
Update Firewall                           : True
Host FQDN                                 : host.example.com
Configure WebSocket Proxy                 : True
Engine Host FQDN                          : engine_host.example.com
```

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

Ознакомьтесь со следующими инструкциями для использования настроенного прокси-сервера WebSocket на машине виртуализированного ЦУ:

```
Manual actions are required on the engine host in order to enroll
certs for this host and configure the engine about it.

Please execute this command on the engine host:
   engine-config -s WebSocketProxy=host.example.com:6100
and than restart the engine service to make it effective
```

10. Осуществите вход в систему на машине виртуализированного ЦУ и выполните следующие команды для завершения настройки:

```
# engine-config -s WebSocketProxy=host.example.com:6100
# systemctl restart ovirt-engine.service
```

Приложение F. Системные учётные записи

F.1. Системные записи пользователей виртуализированного ЦУ

Во время установки пакета `rhevm` создаются следующие системные учётные записи пользователей с соответствующими идентификаторами (UID) для поддержки системы виртуализации ROSA Virtualization:

- Пользователь **`vdsm`** (UID `36`), предназначенный для поддержки работы инструментов монтирования и доступа к доменам хранения NFS.
- Пользователь **`ovirt`** (UID `108`).
- Пользователь **`ovirt-vmconsole`** (UID `498`), предназначенный для гостевой последовательной консоли.

F.2. Группы виртуализированного ЦУ

Во время установки пакета `rhevm` создаются следующие системные учётные записи групп пользователей с соответствующими идентификаторами (GID) для поддержки системы виртуализации ROSA Virtualization:

- Группа **`kvm`** (GID `36`). В группу входит пользователь `vdsm`.
- Группа **`ovirt`** (GID `108`). В группу входит пользователь `ovirt`.
- Группа **`ovirt-vmconsole`** (GID `498`). В группу входит пользователь `ovirt-vmconsole`.

F.3. Системные записи пользователей хостов виртуализации

Во время установки пакетов `vdsm` и `qemu-kvm-rhev` на хостах виртуализации создаются следующие системные учётные записи пользователей с соответствующими идентификаторами (UID):

- Пользователь **`vdsm`** (UID `36`).
- Пользователь **`qemu`** (UID `107`).
- Пользователь **`sanlock`** (UID `179`).
- Пользователь **`ovirt-vmconsole`** (UID `498`).

Примечание — назначенные идентификаторы пользователей (UID) и идентификаторы групп (GID) могут отличаться от системы к системе. Для пользователя **`vdsm`** зафиксировано значение UID `36`, а для группы **`kvm`** зафиксировано значение GID `36`. Если UID `36` или GID `36` уже используются другой учётной записью в системе, во время установки пакетов `vdsm` и `qemu-kvm-rhev` возникнет конфликт.

F.4. Группы хостов виртуализации

Во время установки пакетов `vdsm` и `qemu-kvm-rhev` на хостах виртуализации создаются следующие системные учётные записи групп пользователей с соответствующими идентификаторами (GID):

- Группа **`kvm`** (GID `36`). В группу входят пользователи `qemu` и `sanlock`.
- Группа **`qemu`** (GID `107`). В группу входят пользователи `vdsm` и `sanlock`.
- Группа **`ovirt-vmconsole`** (GID `498`). В группу входит пользователь `ovirt-vmconsole`.

Приложение G.
Защита машинных носителей информации

Администратором системы виртуализации ROSA Virtualization должен быть реализован перечень мер по обеспечению защиты машинных носителей информации.

G.1. Учёт машинных носителей информации

Администратором должен быть обеспечен учёт следующих машинных носителей информации, используемых в системе виртуализации ROSA Virtualization для хранения и обработки информации:

- Съёмные машинные носители информации (флэш-накопители, внешние накопители на жёстких дисках и иные устройства).
- Портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства).
- Машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жёстких дисках).

Учёт машинных носителей информации включает присвоение регистрационных (учётных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенные производителями этих машинных носителей информации, номера инвентарного учёта, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

Учёт съёмных машинных носителей информации ведётся в журналах учёта машинных носителей информации.

Учёт машинных носителей информации, встроенных в портативные или стационарные технические средства, может вестись в журналах материально-технического учёта в составе соответствующих технических средств. При использовании в составе одного технического средства системы виртуализации ROSA Virtualization нескольких встроенных машинных носителей информации, конструктивно объединённых в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

Регистрационные или иные номера подлежат занесению в журналы учёта машинных носителей информации или журналы материально-технического учёта с указанием пользователя или группы пользователей, которым разрешён доступ к машинным носителям информации.

Раздельному учёту в журналах учёта подлежат съёмные (в том числе портативные) перезаписываемые машинные носители информации (флэш-накопители, съёмные жёсткие диски).

G.2. Управление доступом к машинным носителям информации

Администратором должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым в системе виртуализации ROSA Virtualization:

- Определение должностных лиц, имеющих физический доступ к следующим машинным носителям информации:
  - Съёмные машинные носители информации (флэш-накопители, внешние накопители на жёстких дисках и иные устройства).
  - Портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства).
  - Машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жёстких дисках).
- Предоставление физического доступа к машинным носителям информации только тем лицам, которым этот доступ действительно необходим для выполнения своих должностных обязанностей (функций).

G.3. Контроль перемещения машинных носителей информации за пределы контролируемой зоны

Администратором должен обеспечиваться контроль перемещения используемых в системе виртуализации ROSA Virtualization машинных носителей информации за пределы контролируемой зоны.

Контроль перемещения машинных носителей информации за пределы контролируемой зоны предусматривает выполнение администратором следующих действий:

- Определение должностных лиц, имеющих права на перемещение машинных носителей информации за пределы контролируемой зоны.
- Предоставление прав на перемещение машинных носителей информации за пределы контролируемой зоны только тем лицам, которым эти права действительно необходимы для выполнения своих должностных обязанностей (функций).
- Учёт перемещаемых машинных носителей информации.
- Периодическая проверка наличия машинных носителей информации.

G.4. Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах

Администратором системы виртуализации ROSA Virtualization должно обеспечиваться исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах.

Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах предусматривает выполнение администратором следующих действий:

- Определение типов машинных носителей информации, подлежащих хранению в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации).

- Физический контроль и хранение машинных носителей информации в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации).
- Защита машинных носителей информации до уничтожения (стирания) с них данных и остаточной информации (информации, которую можно восстановить после удаления с помощью нештатных средств и методов) с использованием средств стирания данных и остаточной информации.

G.5. Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации

Администратором должен обеспечиваться контроль использования интерфейсов ввода (вывода) информации на машинные носители информации в системе виртуализации ROSA Virtualization.

Контроль использования (разрешение или запрет) интерфейсов ввода (вывода) информации на машинные носители информации предусматривает выполнение следующих действий:

- Определение администратором разрешенных и (или) запрещенных к использованию интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации в системе виртуализации ROSA Virtualization.
- Определение администратором категорий пользователей, которым предоставлены права доступа к разрешенным к использованию интерфейсам ввода (вывода).
- Принятие следующих и иных мер, которые исключают возможность использования запрещенных интерфейсов ввода (вывода):
  - Опечатывание интерфейсов ввода (вывода).
  - Использование механических запирающих устройств.
  - Удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода).
  - Применение средств защиты информации, обеспечивающих контроль использования интерфейсов ввода (вывода).
- Контроль доступа пользователей к разрешенным к использованию интерфейсам ввода (вывода).

G.6. Контроль ввода (вывода) информации на машинные носители информации

Администратором должен обеспечиваться контроль ввода (вывода) информации на машинные носители информации в системе виртуализации ROSA Virtualization.

Контроль ввода (вывода) информации на машинные носители информации предусматривает выполнение следующих действий:

- Определение администратором типов носителей информации, ввод (вывод) информации на которые подлежит контролю.
- Определение администратором категорий пользователей, которым предоставлены полномочия по вводу (выводу) информации на машинные носители.

- Запрет действий по вводу (выводу) информации для пользователей, не имеющих полномочий на ввод (вывод) информации на машинные носители информации, и на носители информации, на которые запрещен ввод (вывод) информации.
- Регистрация действий пользователей и событий по вводу (выводу) информации на машинные носители информации.

G.7. Контроль подключения машинных носителей информации

Администратором должен обеспечиваться контроль подключения машинных носителей информации в системе виртуализации ROSA Virtualization.

Контроль подключения машинных носителей информации предусматривает выполнение следующих действий:

- Определение администратором типов носителей информации, подключение которых к системе виртуализации ROSA Virtualization разрешено.
- Определение администратором категорий пользователей, которым предоставлены полномочия по подключению носителей к системе виртуализации ROSA Virtualization.
- Запрет подключения носителей информации, подключение которых к системе виртуализации ROSA Virtualization не разрешено.
- Регистрация действий пользователей и событий по подключению носителей к системе виртуализации ROSA Virtualization.

G.8. Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями и в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)

Администратором системы виртуализации ROSA Virtualization должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями и в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями и в сторонние организации для ремонта или утилизации.

Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съёмных и несъёмных машинных носителях информации.

Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации должны быть разработаны администратором системы виртуализации ROSA Virtualization и включены в организационно-распорядительные документы по защите информации.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ВМ	—	виртуальная машина
ВЦОД	—	виртуальный центр обработки данных
ОЗУ	—	оперативное запоминающее устройство
ОС	—	операционная система
ПО	—	программное обеспечение
СУСВ	—	система управления средой виртуализации
ФС	—	файловая система
ФСТЭК	—	федеральная служба по техническому и экспортному контролю
ЦОД	—	центр обработки данных
ЦП	—	центральный процессор
ЦС	—	центр сертификации (удостоверяющий центр)
ЦУ	—	центр управления
API *(Application Programming Interface)*	—	программный интерфейс приложения
ARP (*Address Resolution Protocol*)	—	протокол разрешения адресов
BIOS *(Basic Input/Output System)*	—	базовая система ввода-вывода
CA *(Certification Authority)*	—	центр сертификации (удостоверяющий центр)
CD *(Compact Disc)*	—	компакт-диск
CHAP *(Challenge Handshake Authentication Protocol)*	—	протокол аутентификации с косвенным согласованием
CIDR *(Classless Inter-Domain Routing)*	—	бесклассовая IP-адресация
CIFS *(Common Internet File System)*	—	единая файловая система сети интернет
CRL *(Certificate Revocation List)*	—	список отозванных сертификатов
DHCP *(Dynamic Host Configuration Protocol)*	—	протокол динамической настройки хоста
DNS *(Domain Name System)*	—	система доменных имён
FC *(Fibre Channel)*	—	оптоволоконный канал
FCoE *(Fibre Channel over Ethernet)*	—	протокол FC, работающий поверх Ethernet
FCP *(Fibre Channel Protocol)*	—	транспортный протокол FC
FIPS *(Federal Information Processing Standards)*	—	федеральные стандарты обработки информации
FQDN *(Fully Qualified Domain Name)*	—	полное доменное имя хоста
GID *(Group Identifier)*	—	идентификатор группы
GPU *(Graphics Processing Unit)*	—	графический ускоритель (процессор)
GRUB *(Grand Unified Bootloader)*	—	унифицированный загрузчик ОС

HTML *(HyperText Markup Language)* — язык гипертекстовой разметки
HTTP *(HyperText Transfer Protocol)* — протокол передачи гипертекста
HTTPS *(HyperText Transfer Protocol Secure)* — безопасная версия протокола HTTP
ID *(Identification Data)* — идентификатор
IDE *(Integrated Drive Electronics)* — параллельный интерфейс подключения накопителей к компьютеру
IOMMU *(Input/Output Memory Management Unit)* — блок управления памятью для операций ввода-вывода
IP *(Internet Protocol)* — межсетевой протокол
IPA *(Identity, Policy and Audit)* — система идентификации и аутентификации пользователей, задания политик доступа и аудита
iSCSI *(Internet Small Computer System Interface)* — версия протокола SCSI, базирующаяся на TCP/IP
ISO *(International Organization for Standardization)* — международная организация, занимающаяся выпуском стандартов
IT *(Information Technology)* — информационные технологии
JSON *(JavaScript Object Notation)* — текстовый формат обмена данными, основанный на JavaScript
KSM *(Kernel Shared Memory)* — объединение одинаковых страниц памяти ядром ОС
LAN *(Local Area Network)* — локальная вычислительная сеть
LDAP *(Lightweight Directory Access Protocol)* — протокол доступа к каталогам
LKM *(Loadable Kernel Module)* — загружаемый модуль ядра ОС
LLDP *(Link Layer Discovery Protocol)* — канальный протокол (протокол обнаружения уровня связи)
LUN *(Logical Unit Number)* — номер логического устройства
LVM *(Logical Volume Management)* — менеджер логических томов
MAC *(Media Access Control)* — уникальный идентификатор сетевого оборудования
MoM *(Memory Overcommit Manager)* — диспетчер превышенного выделения памяти
MTU *(Maximum Transmission Unit)* — максимальная единица передачи данных
NAT *(Network Address Translation)* — преобразование сетевых адресов
NFS *(Network File Sharing)* — сетевая файловая система
NIC *(Network Interface Controller)* — сетевой адаптер
NUMA *(Non-Uniform Memory Access)* — неравномерный доступ к памяти
OCSP *(Online Certificate Status Protocol)* — протокол проверки статуса сертификата
OOM *(Out of Memory)* — уничтожитель перерасхода памяти

OVF *(Open Virtualization Format)* — формат образа виртуальной машины
OVN *(Open Virtual Network)* — виртуальная сеть с поддержкой OVS
OVS *(Open vSwitch)* — виртуальный коммутатор
PAM *(Pluggable Authentication Modules)* — подключаемые модули аутентификации
PCI *(Peripheral Component Interconnect)* — межсетевое соединение периферийных компонентов
PEM *(Privacy-Enhanced Mail)* — формат файлов для сертификатов
PF *(Physical Function)* — физическая функция PCI Express (PCIe) в SR-IOV
PIN *(Personal Identification Number)* — персональный идентификационный номер (код)
PKCS *(Public Key Cryptography Standards)* — стандарты (спецификации, протоколы) криптографии с открытым ключом
POSIX *(Portable Operating System Interface)* — переносимый интерфейс операционных систем
QCOW *(QEMU Copy on Write)* — формат образа виртуального диска
QEMU *(Quick Emulator)* — эмулятор аппаратного обеспечения различных платформ
QoS *(Quality of Service)* — качество обслуживания
RAC *(Remote Access Card)* — карта удалённого доступа
RDMA *(Remote Direct Memory Access)* — удалённый прямой доступ к памяти
RPC *(Remote Procedure Call)* — вызов удаленных процедур
SAN *(Storage Area Network)* — сеть хранения данных
SCSI *(Small Computer System Interface)* — системный интерфейс
SELinux *(Security Enhanced Linux)* — система контроля доступа, реализованная на уровне ядра ОС
SMT *(Symmetric Multiprocessing)* — синхронная многопоточность (гиперпоточность)
SPICE *(Simple Protocol for Independent Computing Environments)* — протокол удалённого доступа (простой протокол для независимых вычислительных сред)
SPM *(Storage Pool Manager)* — диспетчер пула хранилища
SR-IOV *(Single Root Input/Output Virtualization)* — виртуализация ввода-вывода с единым корнем
SSH *(Secure Shell)* — защищённая оболочка
SSL *(Secure Sockets Layer)* — уровень защищённых сокетов
STP *(Spanning Tree Protocol)* — канальный протокол (протокол связующего дерева)
TCP *(Transmission Control Protocol)* — протокол управления передачей данных
TLS *(Transport Layer Security)* — протокол безопасности транспортного уровня
TLV *(Tag (Type) Length Value)* — метод записи данных в файлах и протоколах
TSC *(Time Stamp Counter)* — счётчик метки времени
UCS *(Unified Computing System)* — система унифицированных вычислений компании Cisco

UEFI *(Unified Extensible Firmware Interface)* — объединённый интерфейс расширяемой прошивки
UI *(User Interface)* — пользовательский интерфейс
UID *(User Identifier)* — идентификатор пользователя
URL *(Uniform Resource Locator)* — сетевой адрес ресурса
USB *(Universal Serial Bus)* — универсальная последовательная шина
UUID *(Universally Unique Identifier)* — уникальный идентификатор элемента
VDSM *(Virtual Desktop and Server Manager)* — служба для управления виртуальными и физическими хостами, хранилищами хостов, ресурсами памяти и ресурсами сетей
VF *(Virtual Function)* — виртуальная функция PCI Express (PCIe) в SR-IOV
VFS *(Virtual File System)* — виртуальная файловая система
VGPU *(Virtual Graphics Processing Unit)* — виртуальный графический ускоритель (процессор)
VLAN *(Virtual Local Area Network)* — виртуальная локальная вычислительная сеть
VNC *(Virtual Network Computing)* — система (протокол) удалённого доступа в виртуальных сетях
VNIC *(Virtual Network Interface Controller)* — виртуальный сетевой адаптер
XML *(eXtensible Markup Language)* — расширяемый язык разметки
XOR *(eXclusive OR)* — исключающее «ИЛИ» (логическая операция)