АО "НТЦ ИТ РОСА"

СРЕДСТВО ВИРТУАЛИЗАЦИИ "РОСА ВИРТУАЛИЗАЦИЯ 4"

Версия 4.0

Руководство администратора

Часть 3. Эксплуатация

РСЮК.10103-01 32 03

Листов 689

2026

АННОТАЦИЯ

Данное руководство предназначено для системных администраторов, осуществляющих развертывание, сопровождение и контроль функционирования программного средства "Средство виртуализации "РОСА Виртуализация 4" (версия 4.0) РСЮК.10103-01 (далее – РОСА Виртуализация, Система).

Сведения об установке и настройке РОСА Виртуализация содержатся в документах "РОСА Виртуализация 4. Руководство администратора. Часть 1. Установка" РСЮК.10103-01 32 01) и "РОСА Виртуализация 4. Руководство администратора. Часть 2. Установка СУСВ на выделенном хосте" (индекс – РСЮК.10103-01 32 02).

Дополнительные сведения об администрировании РОСА Виртуализация приведены в документах:

– "РОСА Виртуализация 4. Руководство администратора. Часть 4. Виртуальные машины" РСЮК.10103-01 32 04;
– "РОСА Виртуализация 4. Руководство администратора. Часть 5. Виртуальные рабочие места. Инфраструктура VDI" РСЮК.10103-01 32 05;
– "РОСА Виртуализация 4. Руководство администратора. Часть 6. Функции безопасности информации" РСЮК.10103-01 32 06;
– "РОСА Виртуализация 4. Руководство администратора. Часть 7. Руководство по системе резервного копирования" РСЮК.10103-01 32 07;
– "РОСА Виртуализация 4. Руководство пользователя. Портал виртуальных машин" РСЮК.10103-01 34 01.

В руководстве содержатся сведения о параметрах развертывания, настройки и эксплуатации РОСА Виртуализация.

Для разработки документа использованы ссылки на следующие стандарты:

– ГОСТ Р 2.105-2019 "Единая система конструкторской документации (ЕСКД). Общие требования к текстовым документам";
– ГОСТ 2.601 "Единая система программной документации. Виды программных документов";
– ГОСТ 19.101-77 "Единая система программной документации. Виды программ и программных документов";
– ГОСТ 19.105-78 "Единая система программной документации. Общие требования к программным документам";

– ГОСТ 19.503-79 "Единая система программной документации. Руководство системного программиста".

Настоящий документ подготовлен в соответствии с технологической инструкцией "РОСА. Регламент формирования документации к программным продуктам" (индекс РСЮК.11001-02 90 01).

СОДЕРЖАНИЕ

1 Общие сведения....12

1.1. Назначение и функции....12
1.2. Место в экосистеме РОСА....12
1.3. Архитектура....14
1.4. Администрирование и обслуживание....15

2 Администрирование и обслуживание среды виртуализации....16

2.1 Настройка глобальных ресурсов....16

2.1.1 Роли....17
2.1.2 Системные полномочия....28
2.1.3 Политики планирования....52
2.1.4 Схема виртуализации....62
2.1.5 Типы экземпляров....72
2.1.6 Пулы MAC-адресов....84

2.2 Панель мониторинга....87

2.2.1 Предварительные условия для установки....88
2.2.2 Общий перечень....88
2.2.3 Общий коэффициент использования....90
2.2.4 Использование кластера....94
2.2.5 Использование хранилищ....95

2.3 Поиск....96

2.3.1 Операции поиска....96
2.3.2 Примеры поиска и поисковый синтаксис....96
2.3.3 Автодополнение поиска....97
2.3.4 Типы результатов поиска....97
2.3.5 Критерии поиска....98
2.3.6 Несколько критериев поиска и символы подстановки....99
2.3.7 Определение порядка поиска....100
2.3.8 Поиск дата-центров....100
2.3.9 Поиск кластеров....101
2.3.10 Поиск хостов....101
2.3.11 Поиск сетей....103
2.3.12 Поиск хранилищ....104
2.3.13 Поиск дисков....105
2.3.14 Поиск томов....107

2.3.15 Поиск виртуальных машин....108
2.3.16 Поиск пулов....111
2.3.17 Поиск шаблонов....112
2.3.18 Поиск пользователей....113
2.3.19 Поиск событий....115
2.4 Закладки....117
2.4.1 Сохранение строки поискового запроса в виде закладки....117
2.4.2 Редактирование закладок....119
2.4.3 Удаление закладок....121
2.5 Теги....121
2.5.1 Настройка взаимодействия с помощью тегов....121
2.5.2 Создание тегов....122
2.5.3 Редактирование тегов....122
2.5.4 Удаление тега....123
2.5.5 Присвоение тегов объектам и снятие меток с объектов....123
2.5.6 Поиск объектов на основе тегов....126
2.5.7 Сортировка хостов с помощью тегов....126
3 Администрирование ресурсов....128
3.1 Качество обслуживания....128
3.1.1 Качество обслуживания хранилища....128
3.1.2 Качество обслуживания сети виртуальной машины....131
3.1.3 Качество обслуживания сетей хоста....135
3.1.4 Качество обслуживания ЦП....138
3.2 Дата-центры....140
3.2.1 Введение....140
3.2.2 Диспетчер пула хранилища (SPM)....141
3.2.3 Приоритет диспетчера пула хранилища....141
3.2.4 Задачи при работе с дата-центрами....142
3.2.5 Дата-центры и домены хранилищ....151
3.3 Кластеры....155
3.3.1 Введение....155
3.3.2 Задачи при работе с кластерами....157
3.4 Логические сети....200
3.4.1 Задачи при работе с логическими сетями....200
3.4.2 Виртуальные сетевые платы (vNIC)....219
3.4.3 Сети внешних поставщиков....233

3.4.4 Хосты и организация сетей....236
3.4.5 Объединение сетевых интерфейсов....272
3.5 Хосты....277
3.5.1 Введение....277
3.5.2 Гипервизоры РОСА Виртуализация....278
3.5.3 Задачи при работе с хостами....279
3.5.4 Отказоустойчивость хостов....310
3.6 Хранилища....321
3.6.1 Домен хранилища....323
3.6.2 Подготовка и добавление хранилища NFS....324
3.6.3 Подготовка и добавление локального хранилища....327
3.6.4 Управление хранилищами на базе файловой системы, совместимой с POSIX....329
3.6.5 Подготовка и добавление блочного хранилища....331
3.6.6 Подготовка и добавление хранилища Gluster....344
3.6.7 Подключение отказоустойчивого хранилища CephFS....369
3.7 Пулы....393
3.7.1 Пул виртуальных машин....393
3.7.2 Создание пула виртуальных машин (VDI)....395
3.7.3 Параметры и элементы управления пулами....402
3.7.4 Изменение параметров пула виртуальных машин....409
3.7.5 Предварительный запуск виртуальных машин в пуле....409
3.7.6 Добавление виртуальных машин в пул ВМ....410
3.7.7 Открепление виртуальных машин от пула ВМ....411
3.7.8 Удаление пула виртуальных машин....412
3.8 Виртуальные диски....413
3.8.1 Хранилище виртуальной машины....413
3.8.2 Виртуальные диски....414
3.8.3 Очистка после удаления для виртуальных дисков....416
3.8.4 Разделяемые диски....418
3.8.5 Диски с доступом только для чтения....419
3.8.6 Работа с виртуальными дисками....419
4 Администрирование окружения....455
4.1 Администрирование виртуализированного ЦУ....455
4.1.1 Обслуживание виртуализированного ЦУ....455
4.1.2 Администрирование СУСВ....460

4.1.3 Настройка резервирования слотов памяти для виртуализированного ЦУ на дополнительных хостах....462
4.1.4 Добавление узлов виртуализированного ЦУ для СУСВ....463
4.1.5 Загрузка СУСВ в режиме восстановления....464
4.1.6 Удаление хоста из окружения виртуализированного ЦУ....466
4.1.7 Изменение полного доменного имени СУСВ в виртуализированном ЦУ 466

4.2 Резервные копии и миграция....467

4.2.1 Обзор создания резервных копий СУСВ....467
4.2.2 Миграция хранилища данных на отдельную машину....498
4.2.3 Создание и восстановление ВМ из резервных копий с использованием домена хранения резервных копий....505

4.3 Обновление сертификатов до истечения срока их действия....508
4.4 Автоматизация задач конфигурирования с помощью Ansible....509
4.5 Пользователи и роли....509

4.5.1 Что такое пользователи....509
4.5.2 Введение в серверы каталогов....510
4.5.3 Настройка внешнего поставщика LDAP....511
4.5.4 Настройка единого входа для LDAP и Kerberos....527
4.5.5 Авторизация пользователей....534
4.5.6 Администрирование задач пользователей на Портале администрирования....535
4.5.7 Администрирование задач пользователей в консольном режиме....542
4.5.8 Настройка дополнительных локальных доменов....550

4.6 Квоты и политика соглашения об уровне обслуживания....550

4.6.1 Что такое Quota....550
4.6.2 Общие и индивидуальные квоты....552
4.6.3 Расчет квот....552
4.6.4 Включение и изменение режима квот в дата-центре....553
4.6.5 Создание новых политик квотирования....553
4.6.6 Описание параметров порога квоты....555
4.6.7 Присвоение квот объектам....555
4.6.8 Присвоение квоты диску....556
4.6.9 Использование квот для ограничения потребления ресурсов пользователем....556
4.6.10 Редактирование квот....557
4.6.11 Удаление квот....557

4.6.12 Принудительное применение политики соглашения об уровне обслуживания....557
4.7 Система событий (ГОСТ)....558
4.7.1 Поиск событий....560
4.7.2 Обновление событий....561
4.7.3 Экспорт....563
4.8 Уведомления о событиях....565
4.8.1 Настройка уведомлений о событиях на Портале администрирования....565
4.8.2 Отмена уведомлений о событиях на Портале администрирования....568
4.8.3 Параметры уведомлений о событиях в файле ovirt-engine-notifier.conf....568
4.8.4 Настройка отправки ловушек SNMP из диспетчера РОСА Виртуализация....574
4.9 Служебные программы....578
4.9.1 Утилита oVirt Engine Rename....578
4.9.2 Утилита Engine Configuration....582
4.9.3 Утилита Log Collector....583
4.9.4 Утилита Engine Vacuum....588
4.9.5 Утилита отображения имен VDSM на имена сетей....590
5 Сбор сведений об окружении....592
5.1 Мониторинг и наблюдаемость....592
5.1.1 Мониторинг РОСА Виртуализация с помощью хранилища данных и Grafana....592
5.1.2 Отправка метрик и журналов на удаленный экземпляр Elasticsearch 597
5.2 Файлы журналов....599
5.2.1 Файлы журналов процесса установки диспетчера виртуализации....599
5.2.2 Файлы журналов диспетчера РОСА Виртуализация....600
5.2.3 Файлы журналов SPICE....601
5.2.4 Файлы журналов хостов....603
5.2.5 Настройка отладочного уровня журналирования для служб РОСА Виртуализация....604
5.2.6 Основные файлы конфигураций служб РОСА Виртуализация....605
5.2.7 Настройка сервера журналирования хоста....606
5.2.8 Включение использования SyslogHandler для передачи журналов диспетчера РОСА Виртуализация на удаленный сервер syslog....607

6 Дополнительные настройки....609
6.1 Настройка двухфакторной аутентификации....609
6.1.1 Двухфакторная аутентификация для SSH с использованием Рутокен ЭЦП....609
6.1.2 Двухфакторная аутентификация для веб-портала РОСА Виртуализация 613
6.1.3 Двухфакторная аутентификация в локальной консоли с использованием Рутокен ЭЦП....626
6.2 Настройка vGPU....632
6.2.1 Настройка системных параметров хоста....633
6.2.2 Установка драйвера vGPU....636
6.2.3 Настройка драйвера vGPU для ВМ....638
Приложение А VDSM и перехватчики событий....640
А.1 Применение VDSM....640
А.2 Перехватчики событий VDSM....640
А.3 Расширение VDSM с помощью перехватчиков событий....641
А.4 Поддерживаемые события VDSM....641
А.5 Окружение VDSM перехватчиков событий....644
А.6 Объект XML домена перехватчиков событий VDSM....644
А.7 Настройка пользовательских свойств....645
А.7.1 Настройка пользовательского свойства smartcard (свойство ВМ)....645
А.7.2 Настройка пользовательского свойства interface (свойство устройства)....646
А.8 Настраиваемые пользователем свойства ВМ....647
А.9 Оценка пользовательских свойств ВМ в перехватчике событий VDSM....648
А.9.1 Оценка настраиваемых пользователем свойств....648
А.10 Использование модуля перехватчиков событий VDSM....649
А.11 Выполнение перехватчиков событий VDSM....649
А.11.1 Настройка sudo для сценариев перехватчиков событий VDSM....650
А.12 Коды возврата перехватчиков событий VDSM....651
А.13 Примеры перехватчиков событий VDSM....651
А.13.1 Тонкая настройка узла NUMA....651
Приложение Б Свойства сетей, настраиваемые пользователем....654
Б.1 Параметры bridge_opts....654
Б.2 Настройка использования команды ethtool в виртуализированном ЦУ...657

Б.2.1 Добавление ключа ethtool_opts в виртуализированный ЦУ.....657
Б.3 Настройка использования протокола FCoE в виртуализированном ЦУ....658
Б.3.1 Добавление ключа FCoE в виртуализированный ЦУ.....658
Приложение В Модули пользовательского интерфейса.....660
В.1 Модули пользовательского интерфейса.....660
В.2 Жизненный цикл модуля пользовательского интерфейса.....660
В.2.1 Этапы жизненного цикла модуля пользовательского интерфейса....661
В.2.2 Обнаружение модуля пользовательского интерфейса.....661
В.2.3 Загрузка модуля пользовательского интерфейса.....662
В.2.4 Самонастройка модуля пользовательского интерфейса.....662
В.3 Файлы модуля пользовательского интерфейса.....663
В.4 Пример развертывания модуля пользовательского интерфейса.....664
Приложение Г Система виртуализации и шифрование связи.....666
Г.1 Замена сертификата ЦС виртуализированного ЦУ.....666
Г.1.1 Извлечение сертификата и закрытого ключа из файла с расширением *.p12.....666
Г.1.2 Замена сертификата ЦС виртуализированного ЦУ для Apache.....667
Г.2 Настройка шифрованного соединения между виртуализированным ЦУ и сервером LDAP.....669
Г.2.1 Создание сертификата ЦС в кодировке PEM.....670
Г.3 Настройка шифрования соединений VDSM вручную.....671
Г.3.1 Настройка шифрования соединений VDSM вручную.....671
Приложение Д Прокси-сервер.....673
Д.1 Прокси-сервер SPICE.....673
Д.1.1 Обзор SPICE Proxy.....673
Д.1.2 Настройка машины SPICE Proxy.....673
Д.1.3 Включение SPICE Proxy.....674
Д.1.4 Выключение SPICE Proxy.....674
Д.2 Прокси-сервер Squid.....675
Д.2.1 Установка и настройка Squid.....675
Д.3 Прокси-сервер WebSocket.....676
Д.3.1 Обзор прокси-сервера WebSocket.....676
Д.3.2 Миграция WebSocket на отдельную машину.....677

Приложение Е Системные учетные записи.....681
Е.1 Системные записи пользователей виртуализированного ЦУ.....681
Е.2 Группы виртуализированного ЦУ.....681
Е.3 Системные записи пользователей хостов виртуализации.....681
Е.4 Группы хостов виртуализации.....682
Перечень сокращений.....683

1 ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение и функции

РОСА Виртуализация — средство 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 РОСА Виртуализация, обладает русскоязычным графическим интерфейсом, с помощью которого осуществляется централизованное управление объектами виртуальной среды (гипервизорами, хранилищами, кластерами, дата-центрами, виртуальными машинами и прочими).

Версия РОСА Виртуализация, сертифицированная ФСТЭК России, может эксплуатироваться в государственных информационных системах, в том числе, обрабатывающих персональные данные, в значимых объектах критической информационной инфраструктуры, в автоматизированных системах управления производственными и технологическими процессами, а также в информационных системах общего пользования.

РОСА Виртуализация предоставляет возможности для создания, управления и функционирования свыше тысячи виртуальных машин (ВМ) в одном ВЦОД. Наличие встроенных механизмов обеспечения защиты информации (в том числе применение шифрованных виртуальных дисков), использование различных моделей доступа (дискреционной и ролевой модели) выгодно отличает РОСА Виртуализация от других аналогичных решений, например на базе OpenStack.

РОСА Виртуализация может эксплуатироваться в ЦОД государственных органов и частных организаций различных масштабов.

1.2. Место в экосистеме РОСА

Экосистема РОСА представляет собой единый, но при этом открытый для интеграции, многофункциональный комплекс программных продуктов, построенный вокруг собственного Linux-дистрибутива. Экосистема РОСА создается по принципу многоуровневой архитектуры и решает задачи эксплуатации ИТ-инфраструктуры любого масштаба: от операционных систем

для рабочих станций и мобильных устройств до сложных систем управления центрами обработки данных корпоративного уровня.

В основе экосистемы лежит РОСА Платформа – единая технологическая основа, на базе которой создаются операционные системы и инфраструктурные решения РОСА, что обеспечивает их совместимость и технологическое единство.

РОСА Платформа обеспечивает:

– единый репозиторий и контроль состава компонентов;
– управление зависимостями, обновлениями и безопасностью;
– единый подход к разработке, сопровождению и развитию решений.

РОСА Виртуализация является в экосистеме РОСА ключевым технологическим звеном, обеспечивающим высокую доступность и эффективное использование вычислительных ресурсов. Если операционная система РОСА ХРОМ является фундаментом (рабочие станции и серверы), то РОСА Виртуализация — это платформа, на которой оперативно разворачиваются и работают все ИТ-сервисы, необходимые организациям.

РОСА Виртуализация обеспечивает технологическую среду, в которой разворачиваются и функционируют другие ключевые компоненты экосистемы РОСА. Вместе они формируют полный стек для управления ИТ-инфраструктурой организации (таблица 1).

Таблица 1 – Стек для управления ИТ-инфраструктурой

Компонент экосистемы	**Роль внутри виртуальной среды**
РОСА ХРОМ Сервер	Запускается в виде виртуальных машин на платформе РОСА Виртуализация, обеспечивая работу серверных служб
Dynamic Directory	Может быть развернут в виртуальной среде для централизованного управления доступом всей инфраструктуры
РОСА Центр управления	Управляет жизненным циклом операционных систем (включая виртуальные машины), дополняя возможности платформы виртуализации

Расширяя возможности экосистемы, РОСА Виртуализация тесно интегрируется с другими решениями. РОСА Виртуализация — это инфраструктурная платформа экосистемы РОСА, которая:

– обеспечивает консолидацию ресурсов серверов и систем хранения данных;

– служит средой выполнения других продуктов экосистемы (ОС, служб каталогов, систем управления);

– является ключевым инструментом решения задач импортозамещения, предоставляя безопасную, сертифицированную и полнофункциональную замену VMware и Hyper-V;

– позволяет решать современные задачи, включая виртуализацию GPU для ИИ и построение высокодоступной, катастрофоустойчивой ИТ-инфраструктуры.

1.3. Архитектура

Программное обеспечение РОСА Виртуализация состоит из следующих основных функциональных компонентов:

– гипервизор – компонент устанавливается непосредственно на физический сервер без предустановленной ОС и получает прямой доступ к аппаратному оборудованию этого хоста. Гипервизор обеспечивает создание, запуск и функционирование виртуальных машин на своем хосте;

– система управления средой виртуализации (СУСВ) – в базовой конфигурации компонент располагается во внешнем отказоустойчивом хранилище данных. СУСВ предоставляет графический интерфейс для централизованного управления объектами виртуальной среды (гипервизорами, хранилищами, кластерами хостов, дата-центрами, виртуальными машинами и т.п.);

– сервер IPA для идентификации и аутентификации доменных пользователей;

– компонент формирования отчетности;

– компонент резервного копирования;

– клиент для ОС семейства Windows с поддержкой версий от XP SP3 и выше;

– дополнительные компоненты – драйверы паравиртуализации, утилиты и служебные программы.

1.4. Администрирование и обслуживание

Наличие администратора является обязательным и необходимым условием функционирования РОСА Виртуализация.

В обязанности администратора РОСА Виртуализация входят следующие задачи:

– Управление физическими и виртуальными ресурсами, такими как хосты и виртуальные машины, в частности добавление хостов и обновление версий ПО на хостах, создание и импорт доменов, преобразование виртуальных машин, созданных на сторонних гипервизорах, резервное копирование виртуальных машин, а также управление шаблонами и 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 путем выключения машин).

– Своевременное реагирование на изменяющиеся требования ВМ (например, обновление версии ОС или выделение большего объема памяти).

– Управление измененными свойствами объектов с помощью тегов.

– Управление параметрами пользователей и настройка уровней полномочий.

– Диагностика и решение проблем конкретных пользователей или виртуальных машин с использованием общих функциональных возможностей Системы.

– Создание общих и частных отчетов.

– Обеспечение безопасности информации, в том числе с использованием специальных функциональных возможностей Системы.

2 АДМИНИСТРИРОВАНИЕ И ОБСЛУЖИВАНИЕ СРЕДЫ ВИРТУАЛИЗАЦИИ

2.1 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 MAC-адресов. 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" (рисунок 1) можно открыть из меню "Администрирование → Настроить" на Портале администрирования.

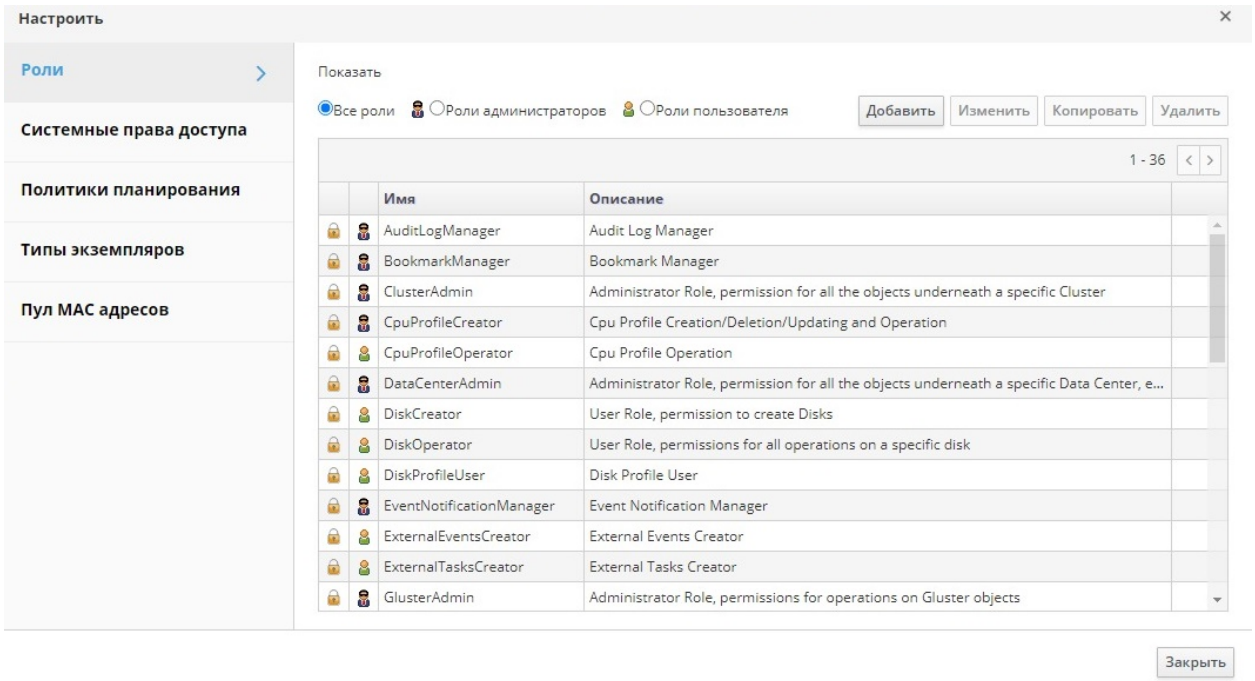


Рисунок 1 – Настройки Системы — секция "Роли"

2.1.1 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.

2.1.1.1 Добавление новой роли

Для добавления роли в Портале администрирования:

а) перейти в "Администрирование → Настроить", чтобы открыть окно "Настроить". По умолчанию выбрана вкладка "Роли" (рисунок 2), где отображается список изначальных ролей Пользователя и Администратора, а также все частные роли;

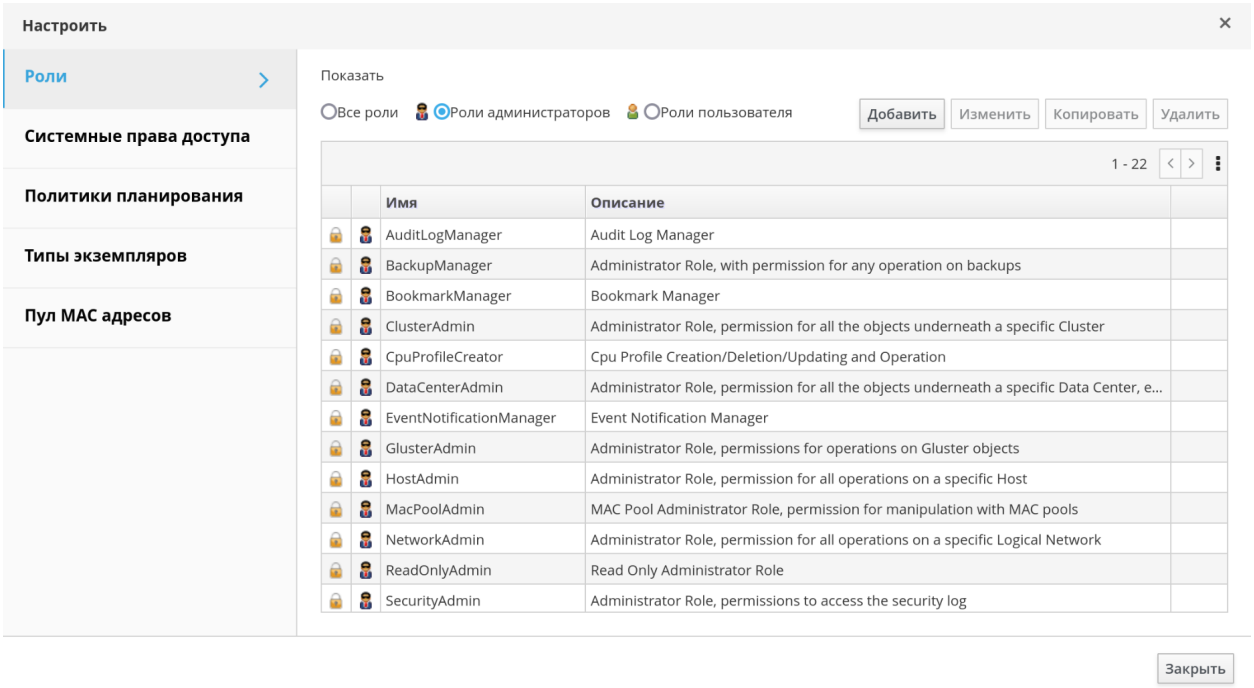


Рисунок 2 – Настройка ролей — Роли администратора

б) нажать кнопку Добавить;
в) ввести "Имя" и "Описание" для новой роли (рисунок 3);

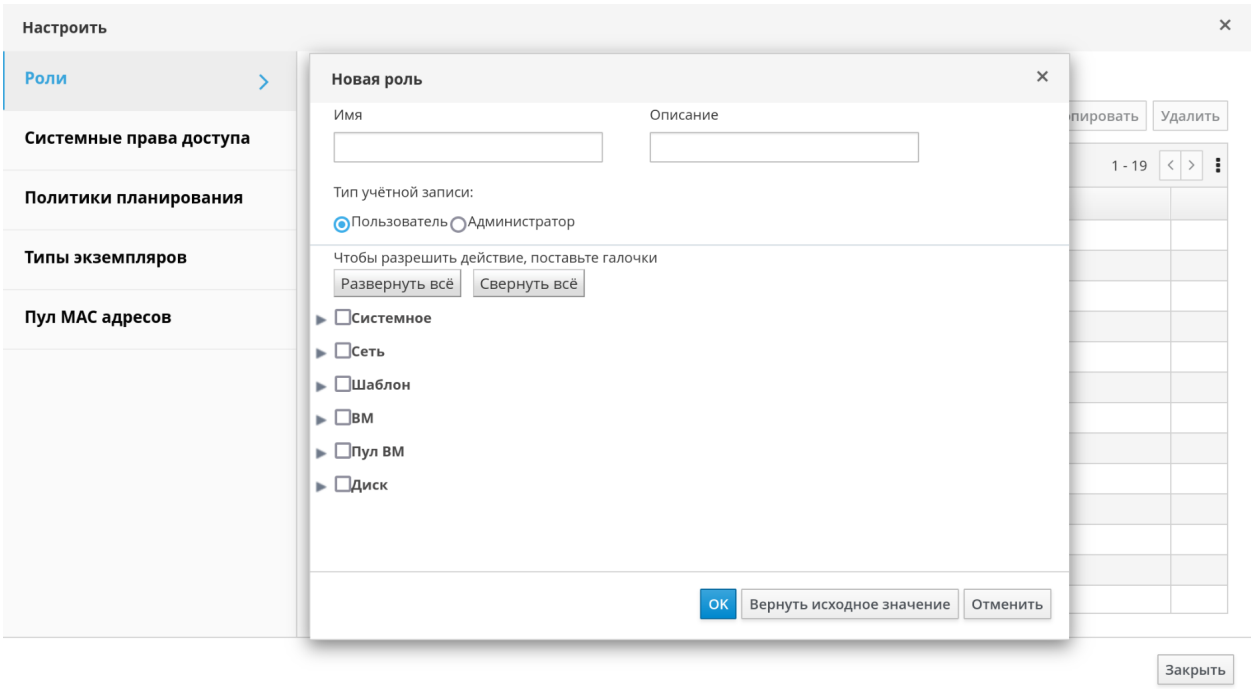


Рисунок 3 – Добавление новой роли

г) для параметра "Тип учетной записи" выбрать тип учетной записи – "Администратор" или "Пользователь";

д) с помощью кнопок Развернуть все (рисунок 4) или Свернуть все можно увидеть соответственно больше или меньше подробностей для полномочий объектов, присутствующих в списке. Также можно развернуть или свернуть параметры для каждого объекта;

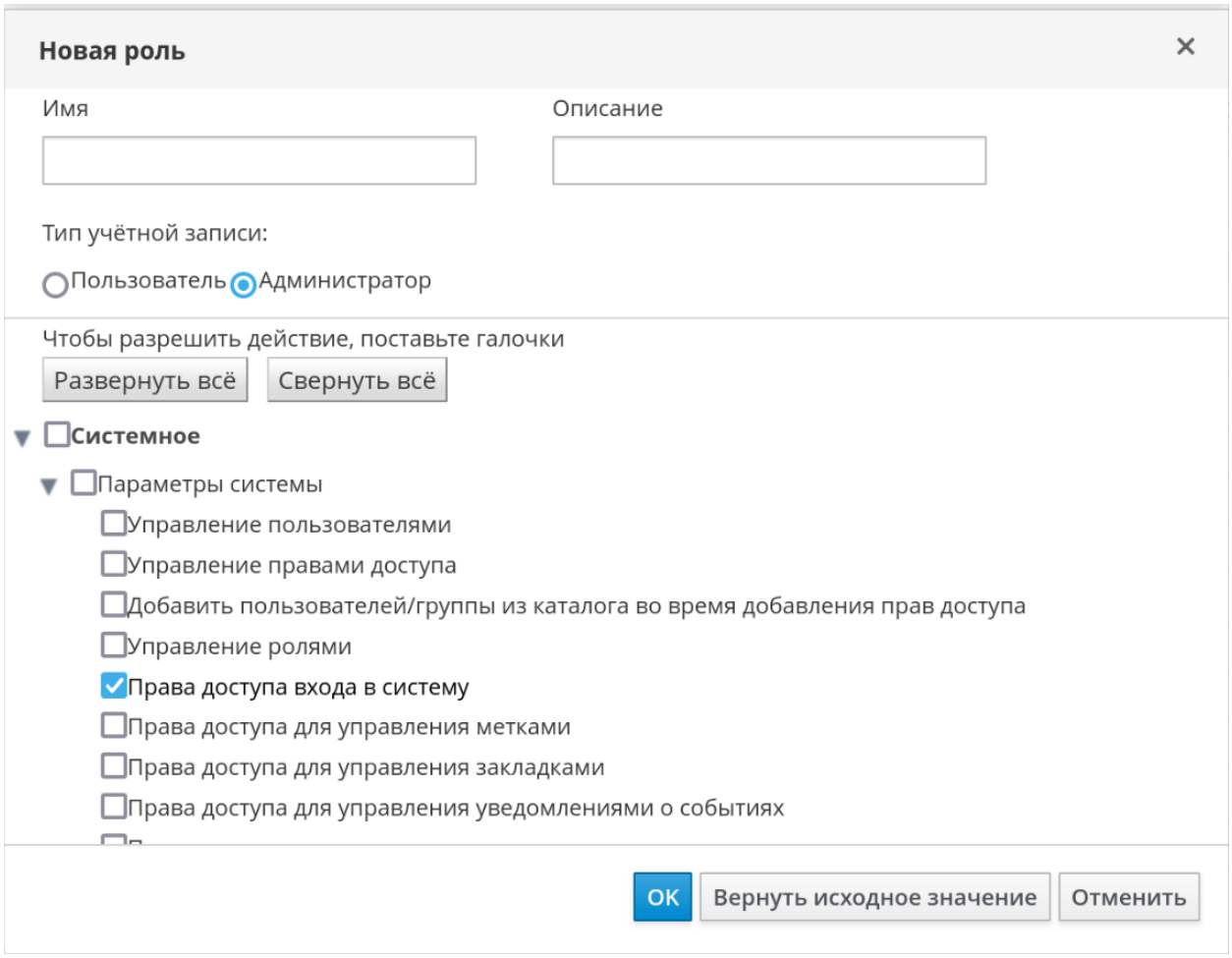


Рисунок 4 – Действия, доступные для настройки новой роли

е) для каждого объекта установить или снять соответствующие флажки для действий, которые нужно разрешить или запретить в настраиваемой роли;

ж) для применения изменений нажать кнопку OK.

Новая роль будет показана в списке ролей.

2.1.1.2 Изменение параметров роли

Параметры созданной администратором роли можно изменять , но нельзя изменять роли по умолчанию. Чтобы изменить роль по умолчанию, нужно скопировать роль и изменить копию роли согласно своим требованиям.

Для изменения или копирования роли требуется выполнить следующие действия:

а) выбрать "Администрирование → Настроить", чтобы открыть окно "Настроить". По умолчанию выбрана вкладка "Роли", где отображается список изначальных ролей Пользователя и Администратора, а также все частные роли;

б) выбрать роль, которую нужно изменить (рисунок 5). Чтобы открыть окно "Параметры роли", нажать кнопку Изменить или, чтобы открыть окно "Копировать" роль, нажать кнопку Копировать;

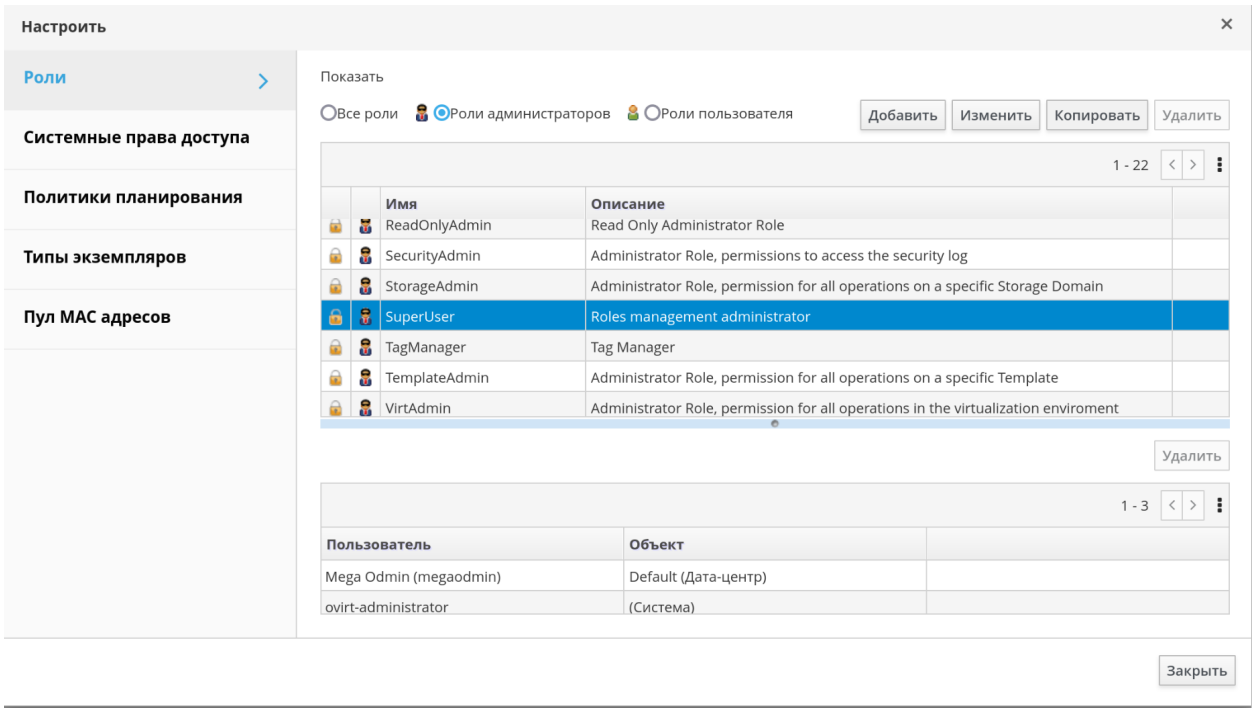


Рисунок 5 – Выбор роли SuperUser для копирования и внесения изменений

в) при необходимости изменить "Имя" и "Описание" роли (рисунок 6);

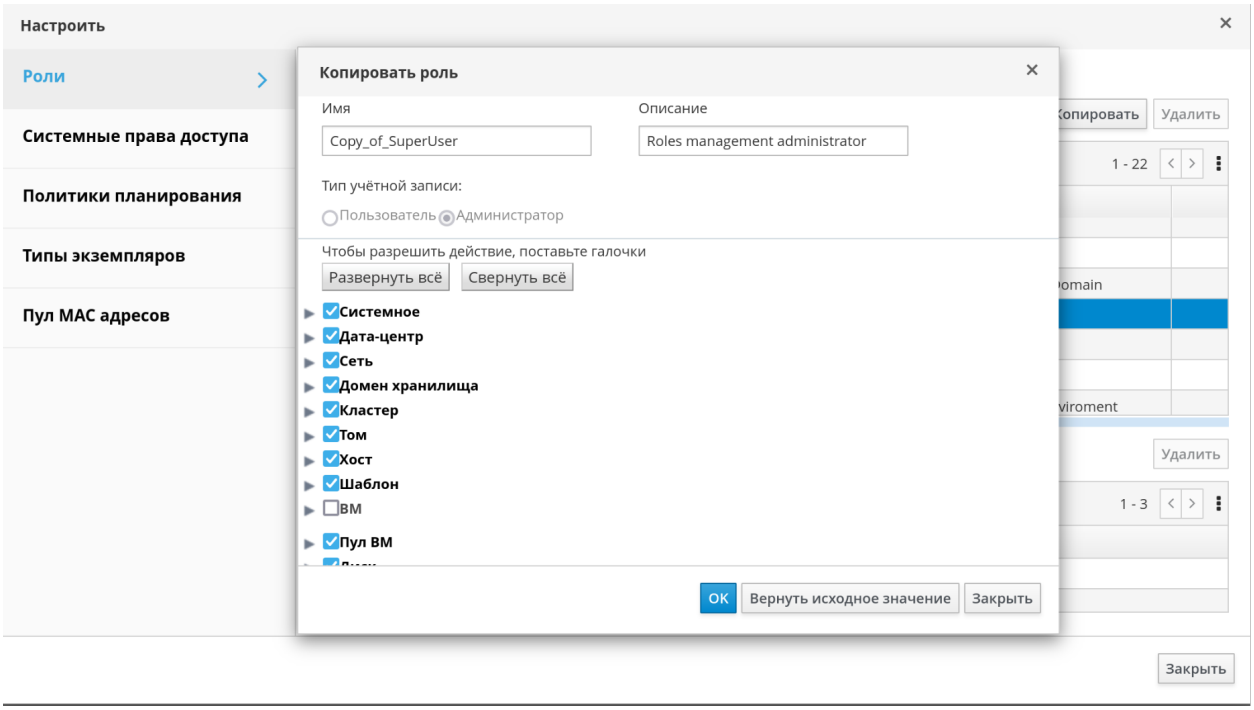


Рисунок 6 – Изменение скопированной роли SuperUser

г) с помощью кнопок `Развернуть все` или `Свернуть все` можно увидеть соответственно больше или меньше подробностей для полномочий объектов, присутствующих в списке. Также можно развернуть или свернуть параметры для каждого объекта;

д) для каждого объекта установить или снять соответствующие флажки для действий, которые нужно разрешить или запретить в настраиваемой роли (рисунок 7);

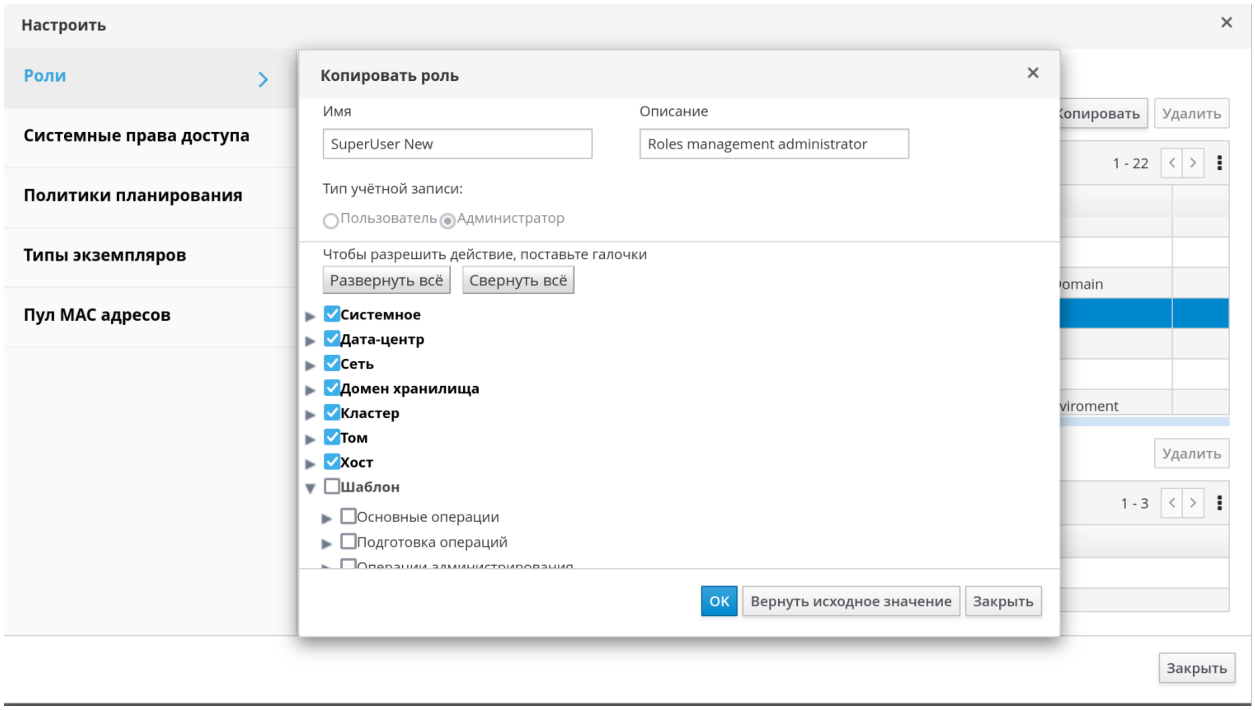


Рисунок 7 – Настройка полномочий по выполняемым действиям для скопированной роли

е) для применения внесенных изменений нажать кнопку OK.

Добавленная роль отобразится в списке ролей для настройки (рисунок 8).

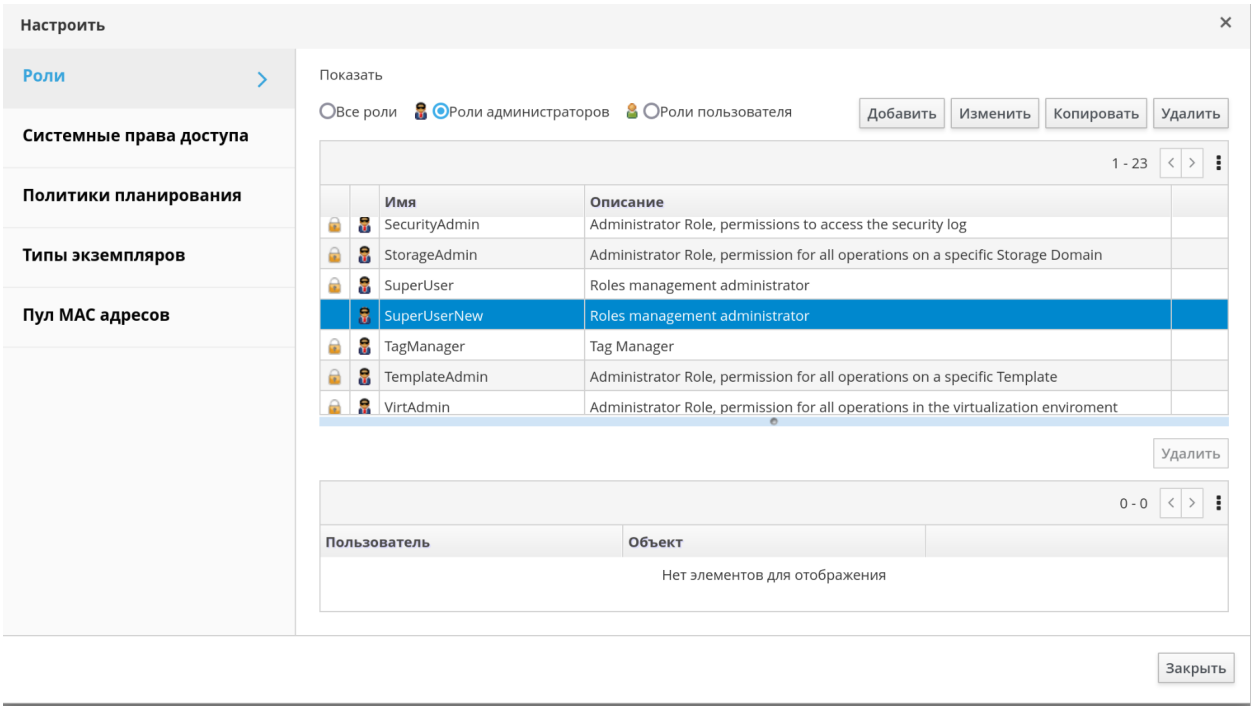


Рисунок 8 – Список ролей с добавленной ролью SuperUserNew

2.1.1.3 Роль пользователя и примеры авторизации

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

2.1.1.3.1 Пример – 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 дает 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.

2.1.1.3.2 Пример – 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 дает ему возможности использовать Портал администрирования.

2.1.1.3.3 Пример – Полномочия роли PowerUser дата-центра

Дарья — руководитель отдела. В дополнение к 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 определенное 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 ее 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.

Следует обратить 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.

2.1.1.3.4 Пример – Полномочия сетевого администратора

Наташа работает сетевым администратором в отделе ИТ. В ее ежедневные обязанности входит создание, управление и удаление сетей в окружении виртуализации ее отдела. Для ее роли нужны административные привилегии на ресурсы и на сети каждого ресурса. Если, например, у Наташи будут привилегии NetworkAdmin в дата-центре отдела ИТ, то она сможет

добавлять и удалять сети в дата-центре, а также присоединять и отсоединять сети для всех ВМ, принадлежащих дата-центру.

2.1.1.3.5 Пример – Полномочия частной роли

Раиса работает в отделе ИТ и отвечает за администрирование учетных записей пользователей в Системе виртуализации. Ей нужны полномочия для добавления учетных записей пользователей и для присвоения им соответствующих ролей и полномочий. Раиса не использует никаких виртуальных машин и не должна иметь доступ 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.

Частная роль UserManager (рисунок 9) разрешает управление пользователями, полномочиями и ролями. Эти действия собраны в разделе "Система", являющимся самым верхним объектом иерархии, показанной на рисунок 10, что означает, что эти действия применимы ко всем другим объектам в Системе.

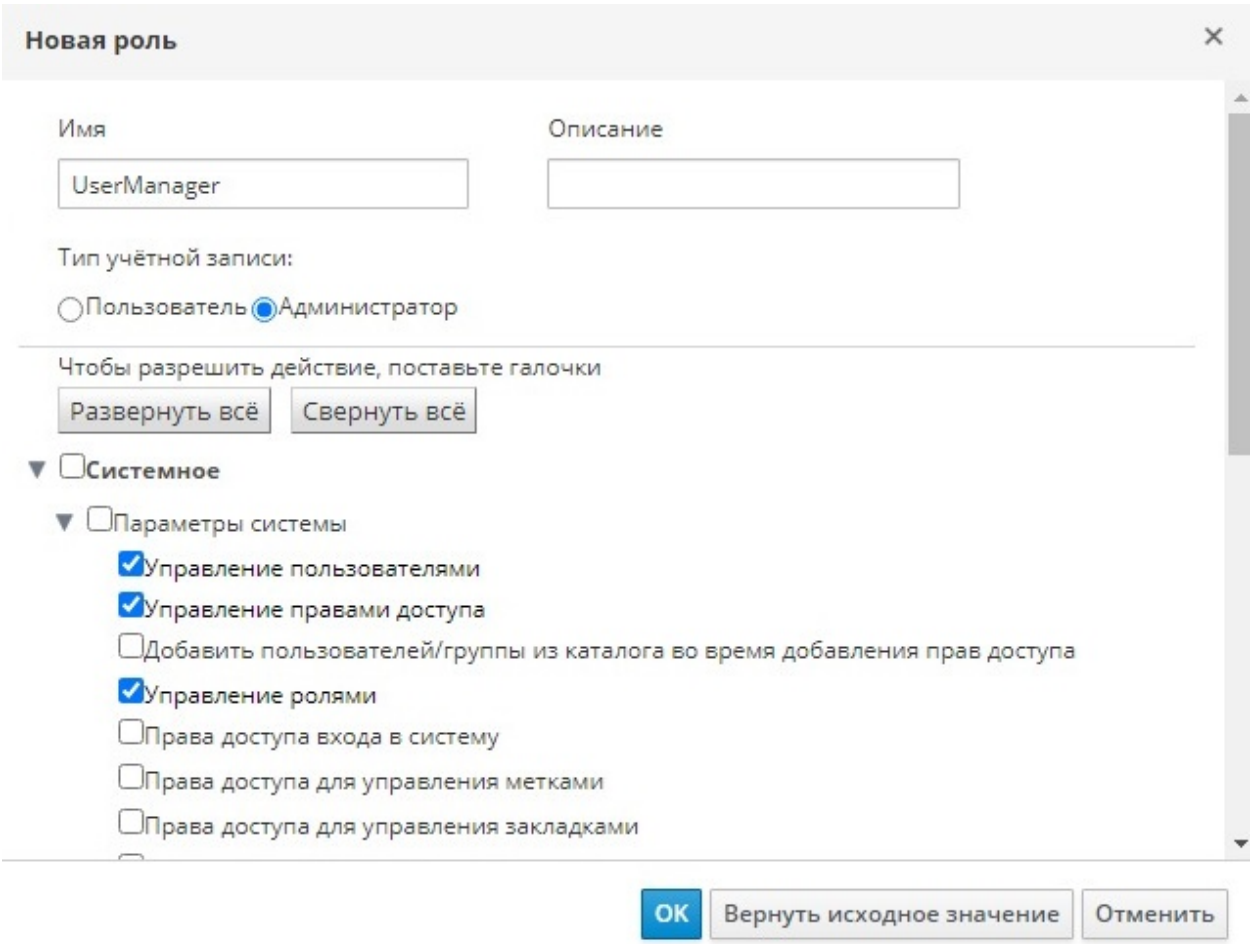


Рисунок 9 – Частная роль UserManager

"Тип учетной записи", указанной для этой роли, — Администратор, а это означает, что после присвоения этой роли Раиса сможет использовать как Портал администрирования, так и Портал ВМ.

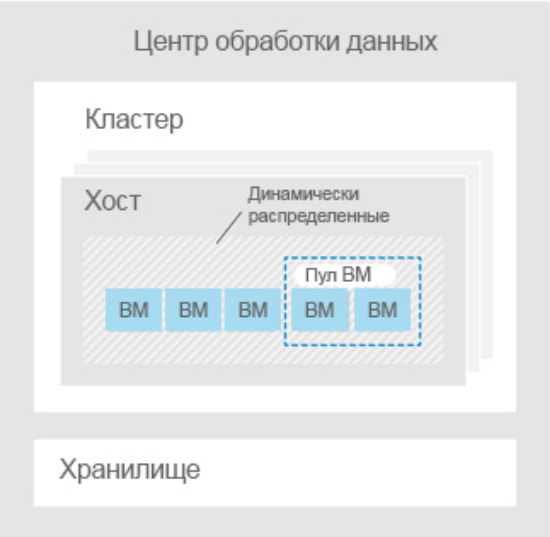


Рисунок 10 – Иерархия объектов Системы виртуализации

2.1.2 Системные полномочия

Полномочия дают пользователям возможность выполнять действия с объектами, где объекты — это либо отдельные объекты, либо контейнерные (рисунок 11). Любые полномочия, применяющиеся к контейнерному объекту, также применимы ко всем членам этого контейнера.

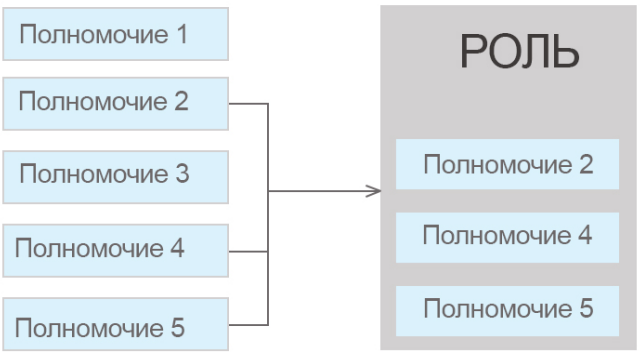


Рисунок 11 – Полномочия и роли

2.1.2.1 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 РОСА Виртуализация 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 РОСА Виртуализация поддерживаются следующие типы ролей:

– 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.

– 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.

2.1.2.2 Роли и привилегии пользователей

В таблице 2 описываются базовые роли пользователей, предоставляющие полномочия на доступ к виртуальным машинам и их параметрам на Портале ВМ.

Таблица 2 – 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	Эту роль присваивают 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 таблице 3 описываются продвинутые роли пользователей, позволяющие выполнять более тонкую настройку полномочий на ресурсы на Портале ВМ.

Таблица 3 – 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 присоединен виртуальный диск
VmCreator	Пользователь может создавать виртуальные машины на Портале ВМ	Эта роль не применяется к конкретной ВМ. Эту роль присваивают пользователю в масштабах всего окружения в окне "Параметры" 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. Эту роль присваивают пользователю в масштабах всего окружения в окне "Параметры" или в конкретных дата-центрах, кластерах или доменах хранилищ

Роль	Привилегии	Примечания
DiskCreator	Пользователь может создавать, редактировать, управлять и удалять виртуальные диски в рамках присвоенных кластеров или дата-центров	Эта роль не присваивается конкретному виртуальному диску. Эту роль присваивают пользователю в масштабах всего окружения в окне "Параметры" или 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

2.1.2.3 Роли и привилегии администраторов

В таблице 4 описываются базовые административные роли, дающие полномочия на доступ и настройку ресурсов на Портале администрирования.

Таблица 4 – Базовые роли администраторов в Системе виртуализации

Роль	Привилегии	Примечания
SuperUser	Системный администратор РОСА Виртуализация	Суперпользователь обладает полными полномочиями на все объекты и уровни (администрирует все объекты во всех дата-центрах)
VirtAdmin	Администратор РОСА Виртуализация	Пользователь обладает административными

Роль	Привилегии	Примечания
		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

Важно — Не следует использовать пользователя-администратора сервера каталогов в качестве пользователя-администратора Системы виртуализации. Рекомендуется создать 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 таблице 5 описываются продвинутые роли администраторов, позволяющие выполнять более тонкую настройку полномочий на ресурсы на Портале администрирования.

Таблица 5 – Продвинутые роли администраторов в Системе виртуализации

Роль	Привилегии	Примечания
TemplateAdmin	Администратор шаблона	Пользователь может создавать,

Роль	Привилегии	Примечания
	ВМ	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

Роль	Привилегии	Примечания
		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

2.1.2.4 Присвоение ресурсу роли администратора или пользователя

Для присвоения роли ресурсу необходимо:

а) найти название нужного ресурса и нажать на него, чтобы просмотреть детали (рисунок 12);

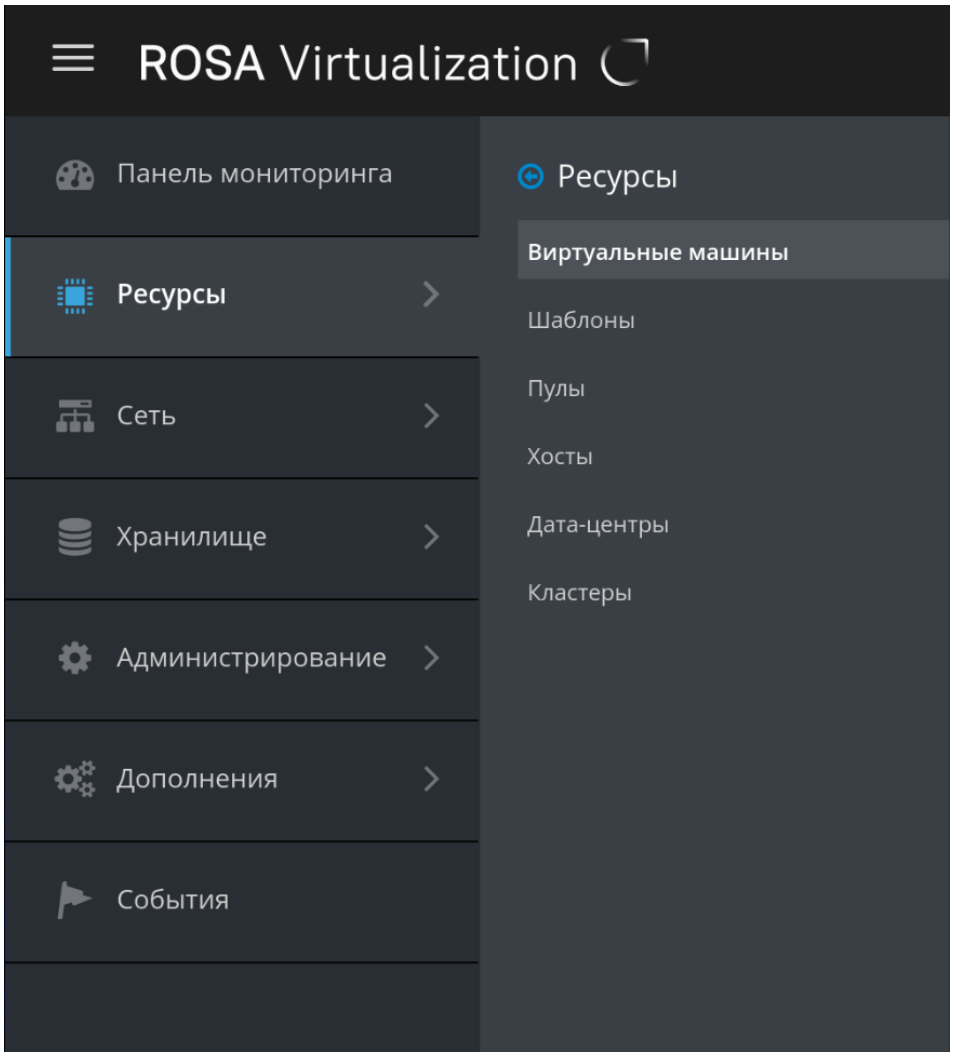


Рисунок 12 – Ресурсы РОСА Виртуализация: "Виртуальные машины", "Шаблоны", "Пулы", "Хосты", "Дата-центры", "Кластеры"

В качестве примера можно рассмотреть выбор "Ресурсы → Виртуальные машины" (рисунок 13).

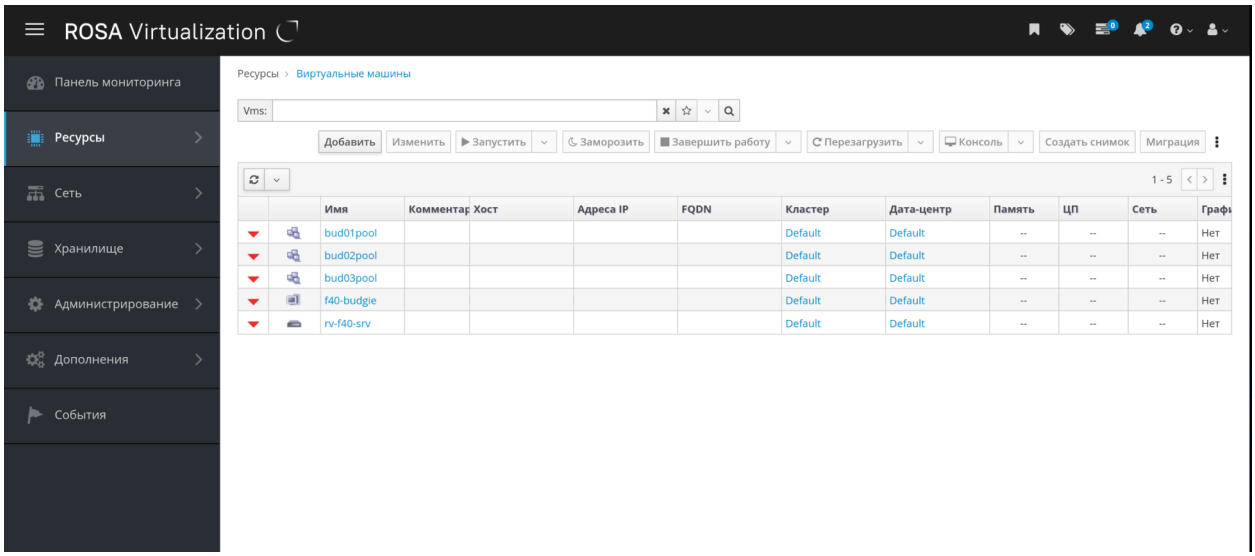


Рисунок 13 – Доступные ресурсы — "Виртуальные машины"

б) перейти на вкладку "Права доступа" (рисунок 14), чтобы указать присвоенных пользователей, роль пользователя и наследуемые полномочия для выбранного ресурса;

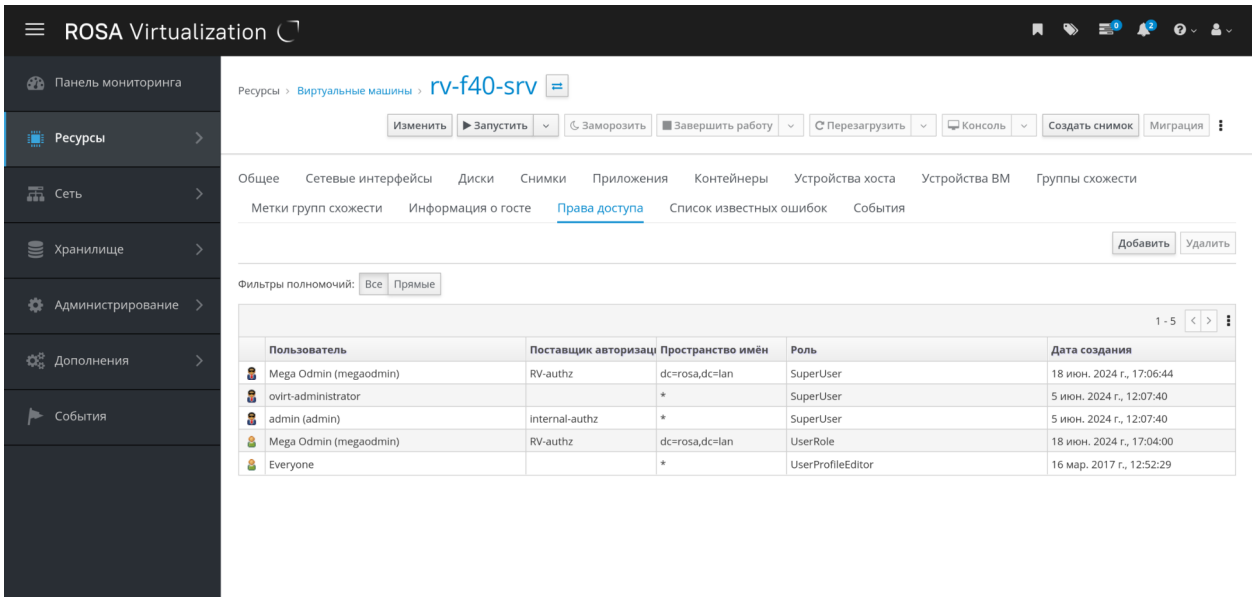


Рисунок 14 – "Права доступа" для выбранного ресурса (виртуальная машина)

в) нажать кнопку Добавить, после чего откроется форма для добавления пользователя и присвоения ему требуемых прав для данного ресурса (рисунок 15);

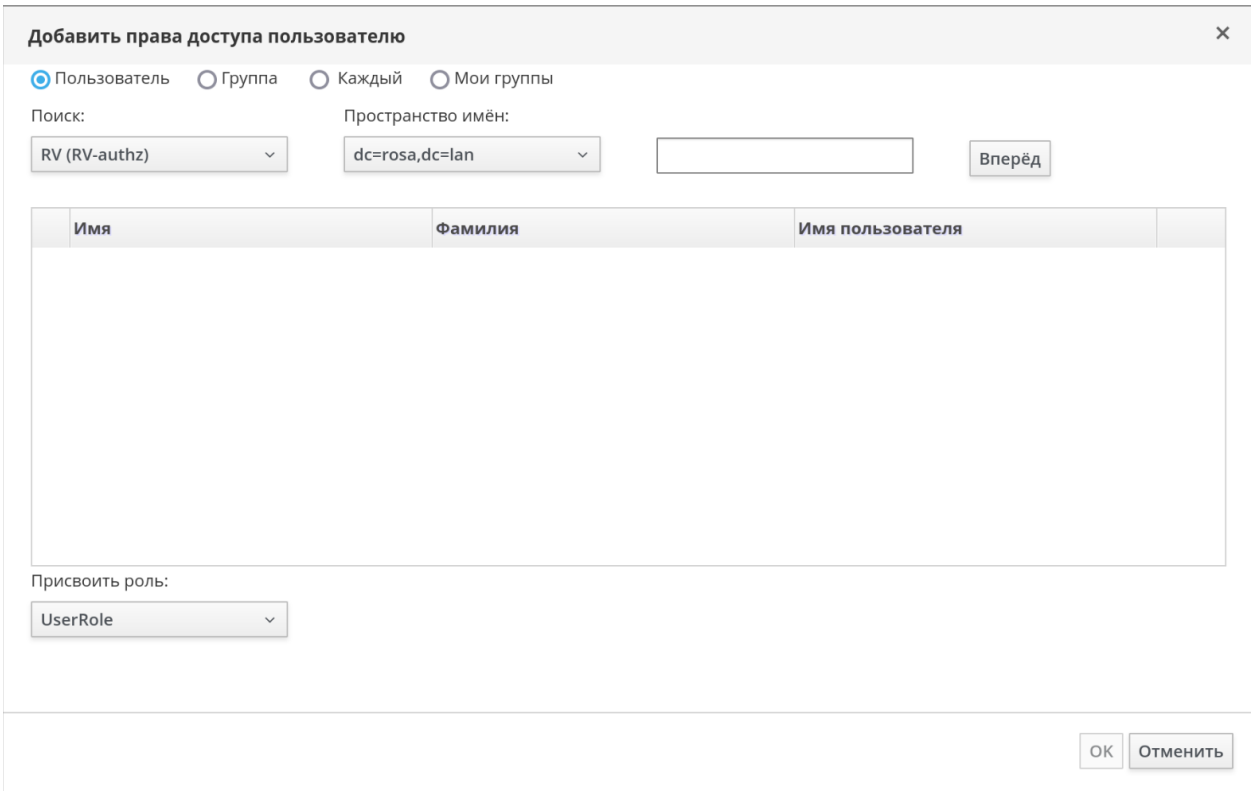


Рисунок 15 – Форма для добавления пользователя и присвоения ему требуемых прав

г) указать имя существующего пользователя в поле "Поиск" и нажать кнопку Вперед. Из полученного списка возможных совпадений выбрать пользователя (рисунок 16);

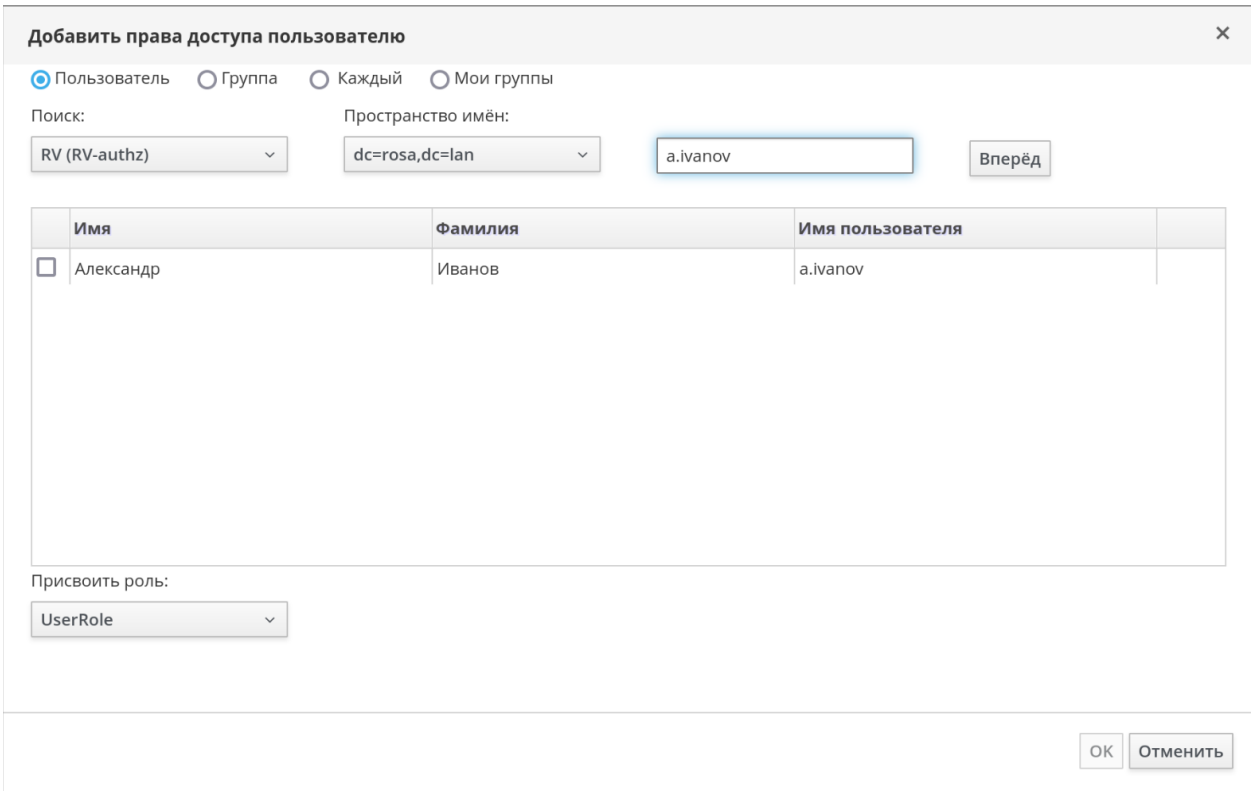


Рисунок 16 – Поиск пользователя

В данном примере нужно найти пользователя a.ivanov (Александр Иванов) из домена RV (подключен как внешний сервер LDAP).

д) из выпадающего списка "Присвоить роль" выбрать нужную роль (рисунок 17);

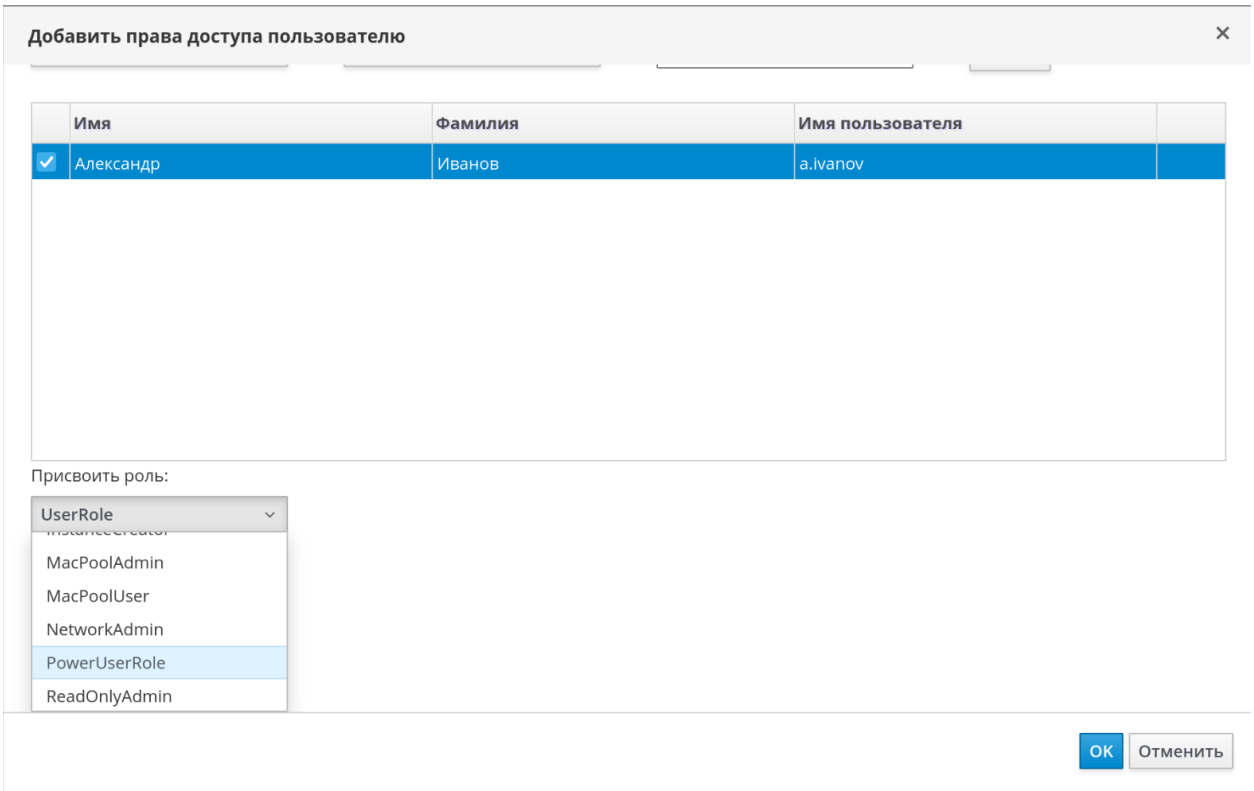


Рисунок 17 – Присвоение роли выбранному пользователю

На рисунке 17 пользователю a.ivanov (Александр Иванов) из домена RV присваивается роль PowerUserRole.

е) нажать кнопку OK.

В результате на указанном ресурсе действуют наследуемые полномочия выбранной роли для определенного пользователя, который получает права доступа или управления этим ресурсом (рисунок 18).

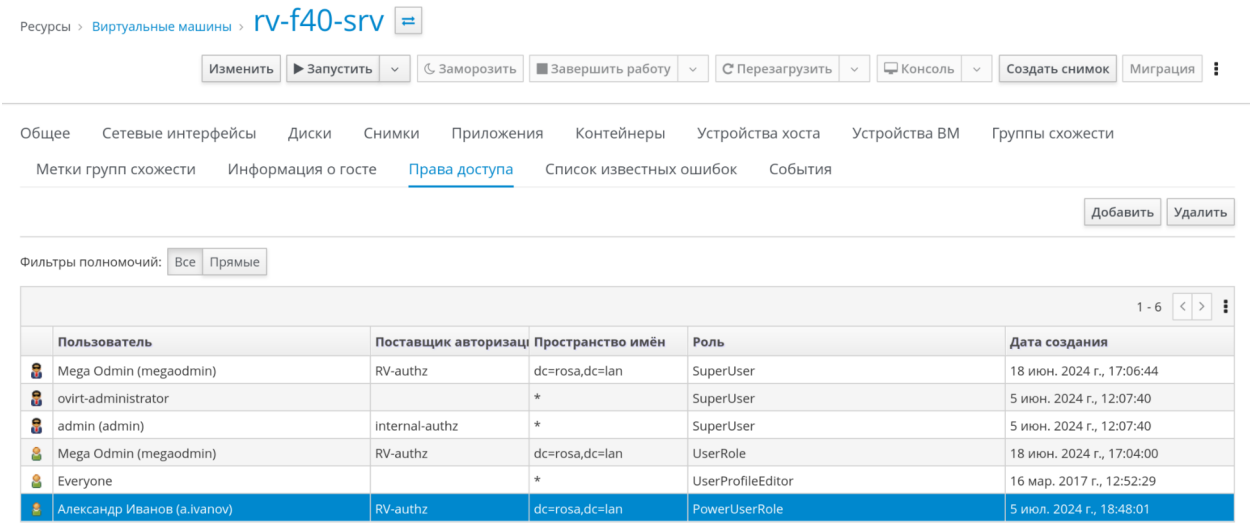


Рисунок 18 – Пользователь a.ivanov получил права (роль) PowerUserRole для выбранного ресурса

Важно — Роли и полномочия можно присваивать только существующим пользователям.

2.1.2.5 Удаление роли администратора или пользователя с ресурса

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

Для удаления роли с ресурса нужно выполнить следующие действия:

а) найти название нужного ресурса и нажать на него, чтобы просмотреть детали;

б) перейти на вкладку "Права доступа", чтобы указать присвоенных пользователей, роль пользователя и наследуемые полномочия для выбранного ресурса;

в) выбрать пользователя, права которого необходимо удалить с данного ресурса (см. рисунок 18);

г) нажать кнопку Удалить (рисунок 19);

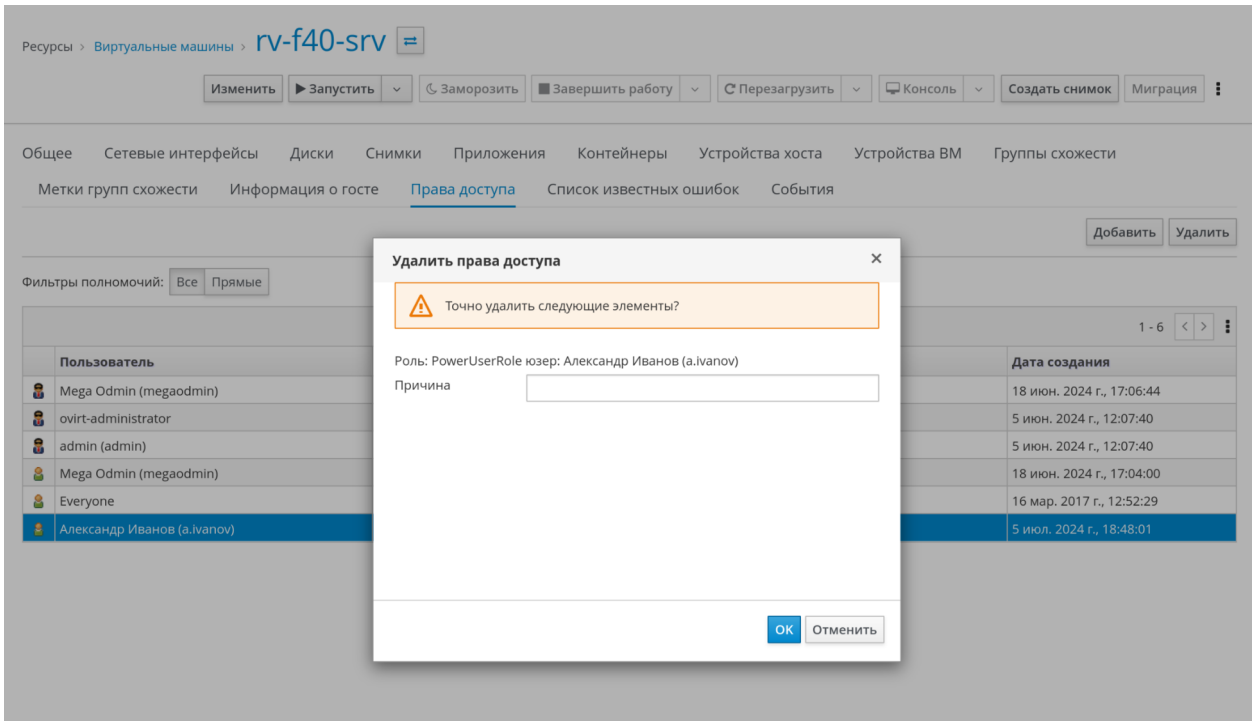


Рисунок 19 – Удаление прав доступа

д) в открывшемся диалоговом окне "Удалить права доступа" нажать кнопку OK для удаления прав доступа для данного пользователя/ресурса.

"Права доступа" для данного пользователя/ресурса будут удалены (рисунок 20).

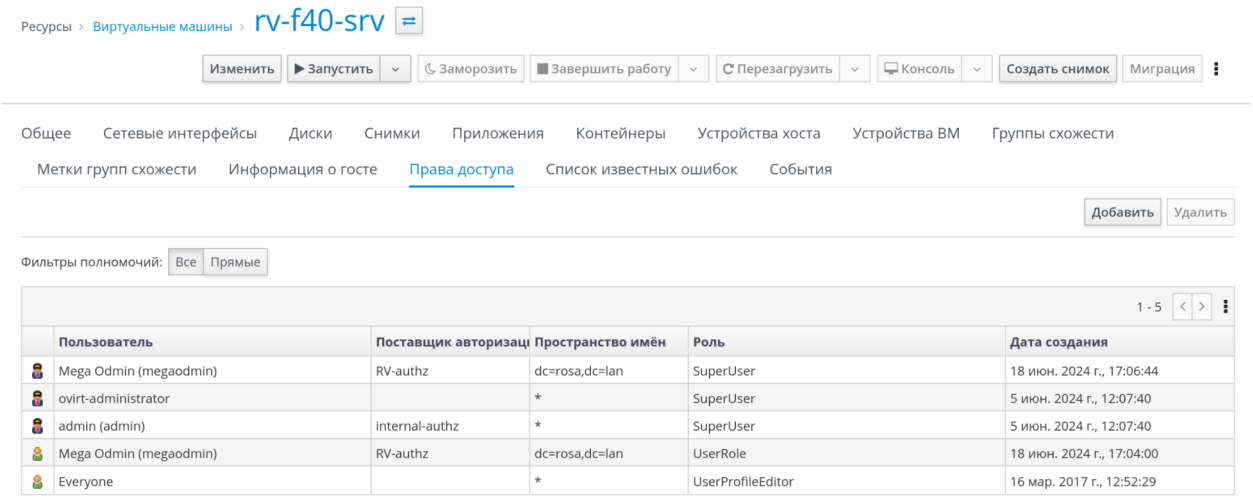


Рисунок 20 – Права пользователя a.ivanov к данному ресурсу удалены

2.1.2.6 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 можно назначать 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 следует удалить существующего администратора и создать нового.

В таблице 6 описываются административные роли и привилегии, применимые в администрировании дата-центров.

Таблица 6 – 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

2.1.2.7 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 можно назначать 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 следует удалить существующего администратора и создать нового.

В таблице 7 описываются административные роли и привилегии, применимые в администрировании кластеров.

Таблица 7 – 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

2.1.2.8 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 нужно использовать 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 следует удалить существующего администратора и создать нового.

В таблице 8 описываются роли сетевого администратора и сетевого пользователя, а также привилегии, используемые в сетевом администрировании.

Таблица 8 – 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 применяют для сети роль NetworkAdmin, а на ВМ – роль UserVmManager

Роль	Привилегии	Примечания
VnicProfileUser	Пользователь логической сети и сетевого интерфейса виртуальной машины и шаблонов	Пользователь может подключать или отключать сетевые интерфейсы для конкретных логических сетей

2.1.2.9 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.

Для назначения администратора для всех хостов окружения нужно использовать кнопку Параметры на панели заголовков.

Роль администратора хоста разрешает выполнять следующие действия:

– настройка параметров хоста;
– настройка логических сетей;
– удаление хоста.

Для смены администратора хоста следует удалить существующего администратора и создать нового.

В таблице 9 описывается роль администратора, а также привилегии, применяемые для администрирования хостов.

Таблица 9 – 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

2.1.2.10 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.

Для назначения администратора хранилища для всех доменов хранилищ окружения нужно использовать кнопку Параметры на панели заголовков.

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 следует удалить существующего администратора и создать нового.

В таблице 10 описываются роли администратора, а также привилегии, применяемые для администрирования доменов хранилищ.

Таблица 10 – 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

2.1.2.11 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 откреплление ВМ от пулов.

В таблице 11 описываются роли администратора, а также привилегии, применяемые для администрирования пулов.

Таблица 11 – 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

2.1.2.12 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 таблице 12 описываются роли пользователей и привилегии, применимые для использования и администрирования виртуальных дисков на Портале ВМ.

Таблица 12 – 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 присоединен 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. Эту роль применяют к пользователю в рамках всего окружения в окне "Параметры". Как вариант, можно применять эту роль для конкретных дата-центров, кластеров или доменов хранилищ

2.1.2.13 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.

Строку шифра можно изменить с помощью файла сценариев Ansible (Ansible playbook).

Для изменения строки шифра нужно:

а) на машине диспетчера виртуализации создать файл в каталоге /usr/share/ovirt-engine/playbooks, например:

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

б) вставить в файл следующее содержимое и сохранить 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
```

в) запустить только что созданный файл Ansible playbook:

```
# 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
```

2.1.3 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 жесткое 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 (рисунок 21). 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.



Рисунок 21 – 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, прикрепленные 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".

Политика планирования Power_Saving (рисунок 22) 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, прикрепленные к хосту, не начнут работу, если этот хост достиг указанного значения высокого коэффициента использования.

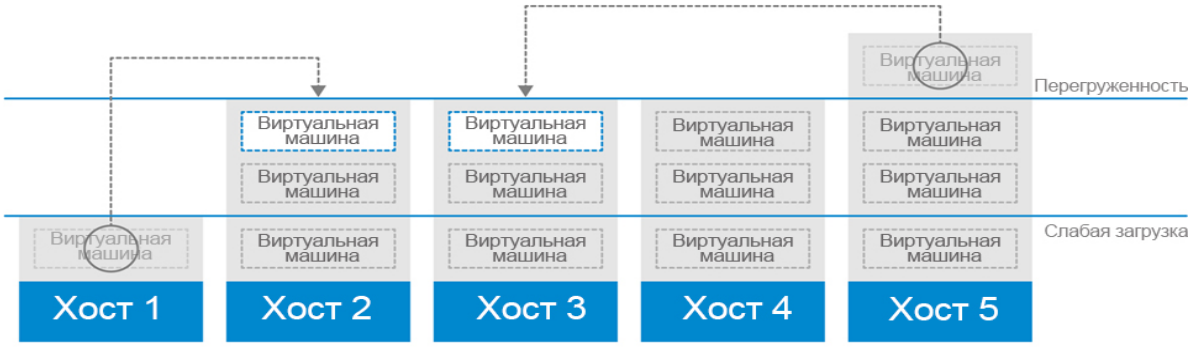


Рисунок 22 – Политика планирования энергосбережения (Power Saving)

Необходимо указать 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, прикрепленные 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.

2.1.3.1 Создание политик планирования

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

Для создания политики планирования нужно выполнить следующие действия:

а) перейти в "Администрирование → Настроить";
б) перейти на вкладку "Политики планирования" (рисунок 23);

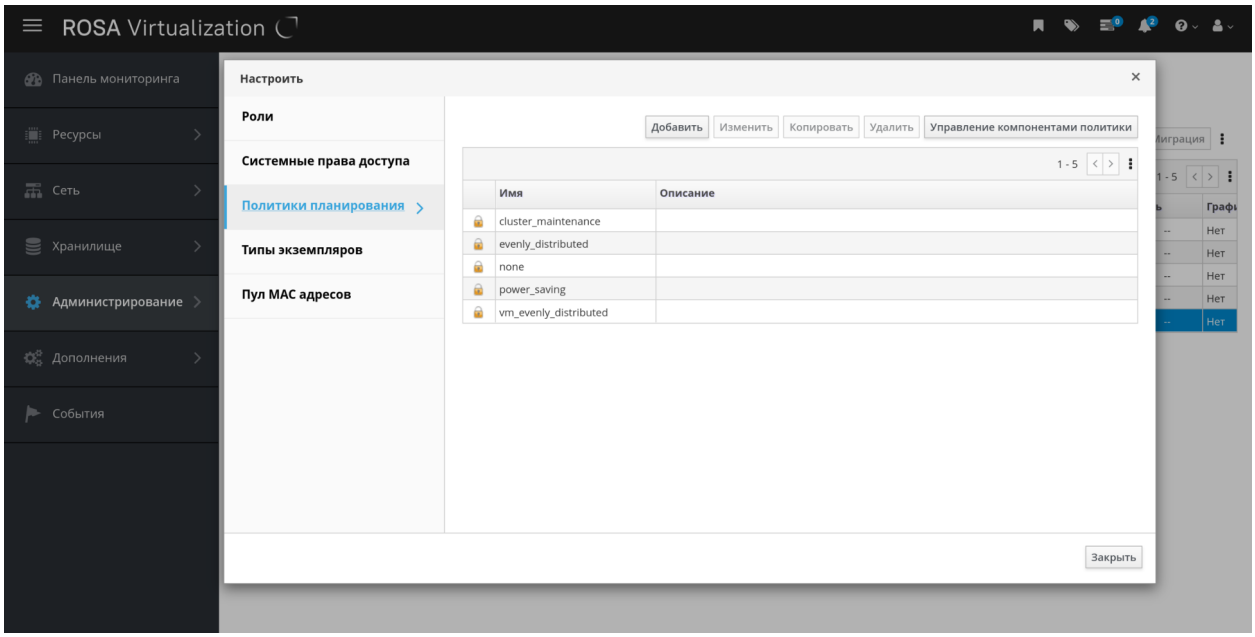


Рисунок 23 – Настройка политик планирования

в) нажать кнопку Добавить для создания новой политики планирования (рисунок 24);

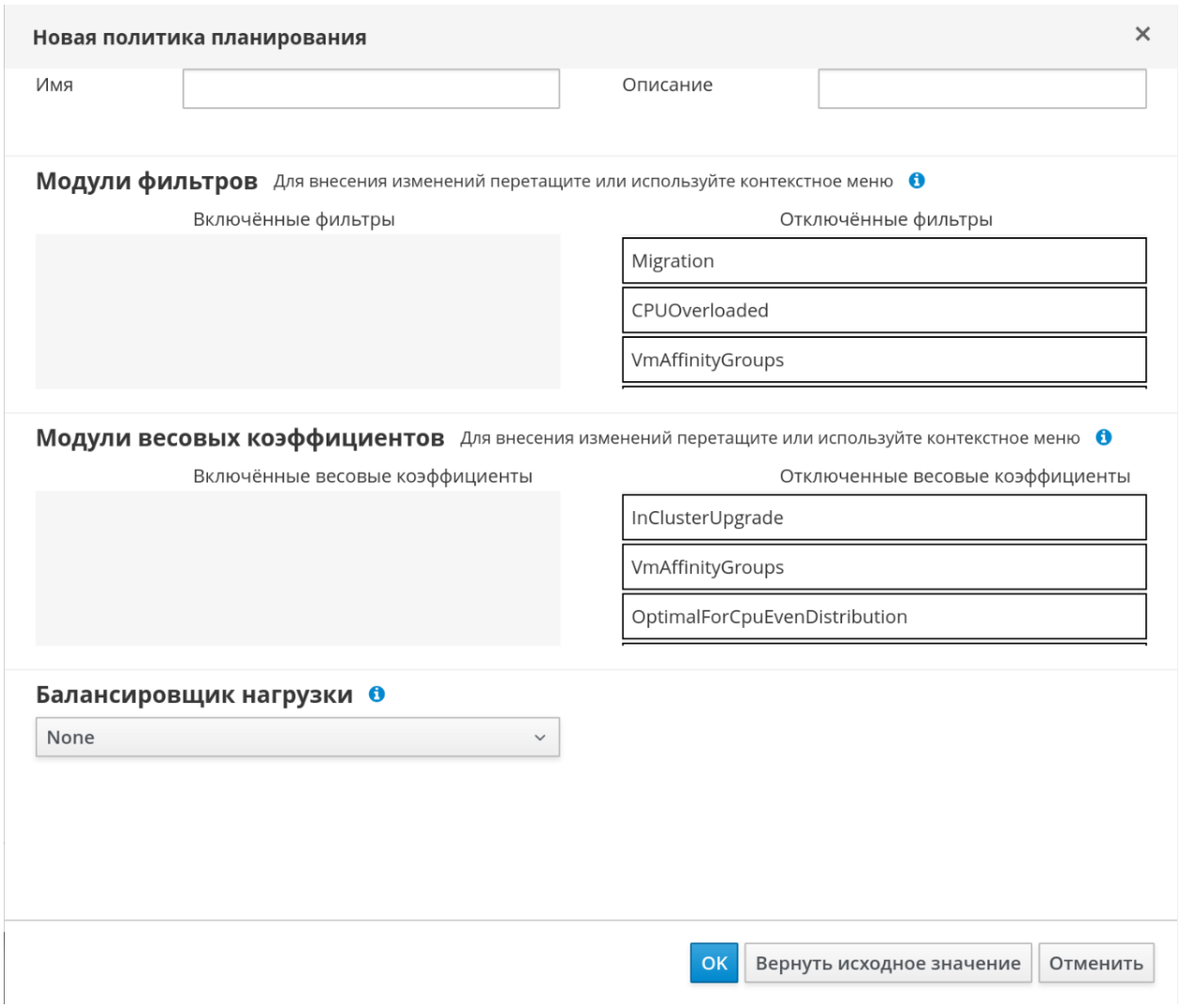


Рисунок 24 – Создание политики планирования

г) указать "Имя" и "Описание" политики планирования;

д) настроить модули фильтров (рисунок 25):

1) в секции "Модули фильтров" переместить предпочитаемые модули фильтров из раздела "Отключенные фильтры" в раздел "Включенные фильтры" для применения фильтров в политике планирования;

2) конкретные модули фильтров также можно настроить как "Первый", чтобы у него был наивысший приоритет, или "Последний", чтобы он получил самый низкий приоритет, для базовой оптимизации. Чтобы установить приоритет, нажать на необходимый модуль фильтра,

навести курсор на пункт "Местоположение" и выбрать "Первый" или "Последний";

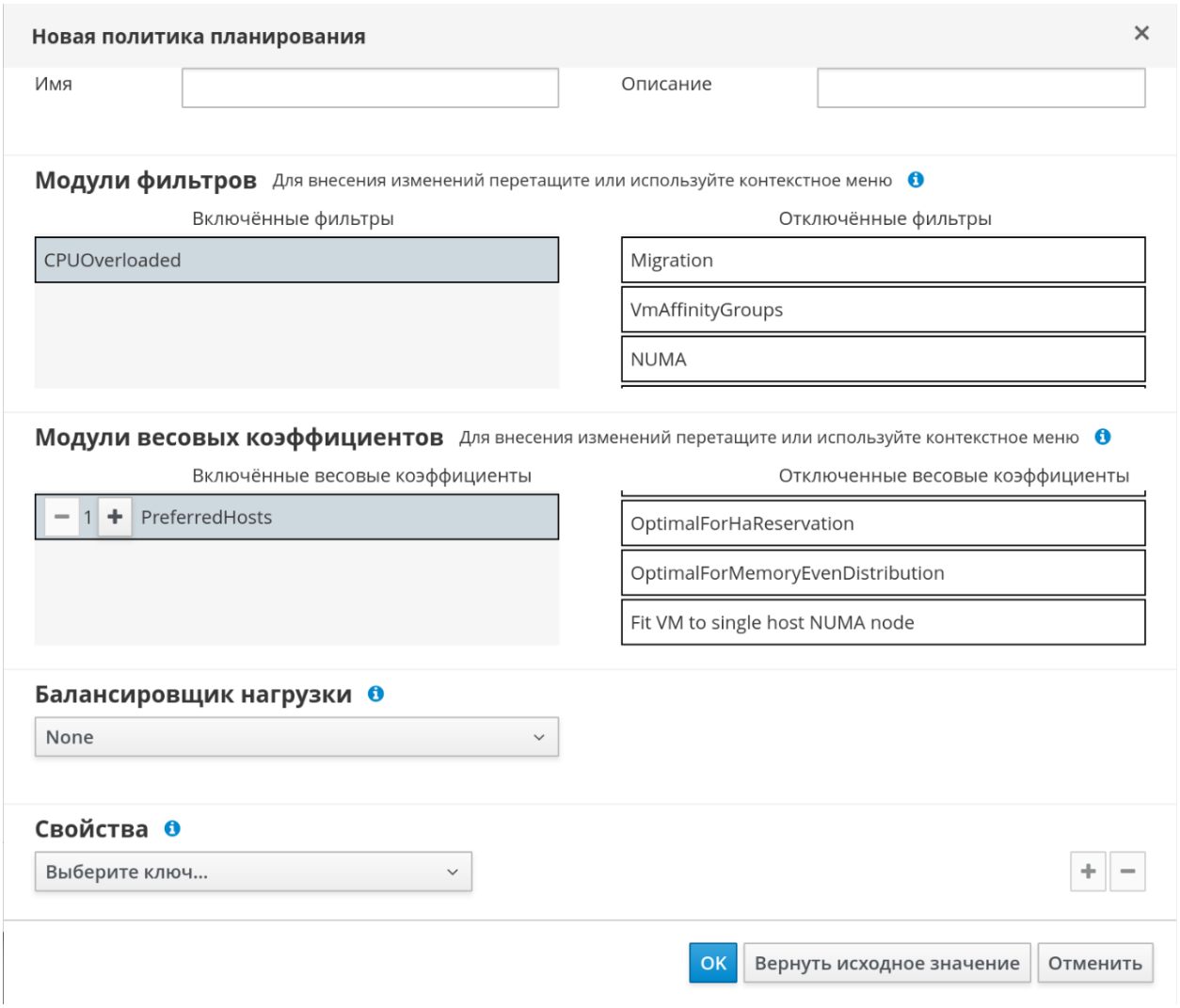


Рисунок 25 – Настройка модулей фильтров для политики планирования

е) настроить модули веса:

1) в секции "Модули весовых коэффициентов" переместить предпочитаемые модули веса из области "Отключенные весовые коэффициенты" в область "Включенные весовые коэффициенты", чтобы применить весовые коэффициенты к политике планирования;

2) с помощью кнопок + и – слева от включенных модулей веса повысить или уменьшить вес этих модулей (рисунок 25);

ж) указать политику балансировки нагрузки (рисунок 26):

1) из выпадающего списка в секции "Балансировщик нагрузки" выбрать политику балансировки нагрузки, которая будет применяться в политике планирования;

2) из выпадающего списка в секции "Параметры" выбрать свойство балансировки нагрузки, которое нужно применить в политике планирования, и в текстовом поле справа от этого свойства указать значение;

3) с помощью кнопок + и – добавить или удалить дополнительные свойства;

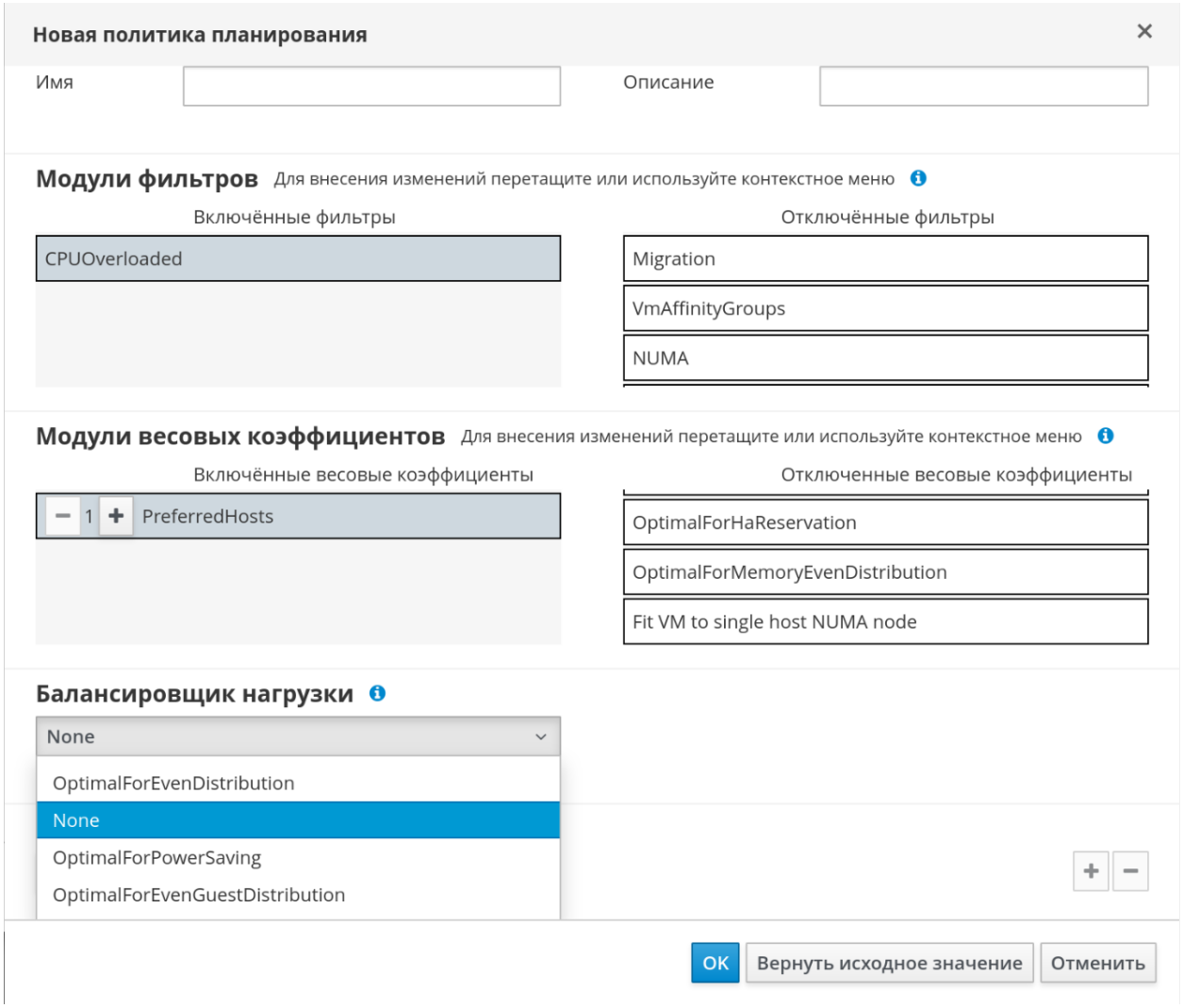


Рисунок 26 – Настройка балансировщика нагрузки

а) нажать кнопку ОК.

Новая политика будет добавлена в список политик планирования (рисунок 27).

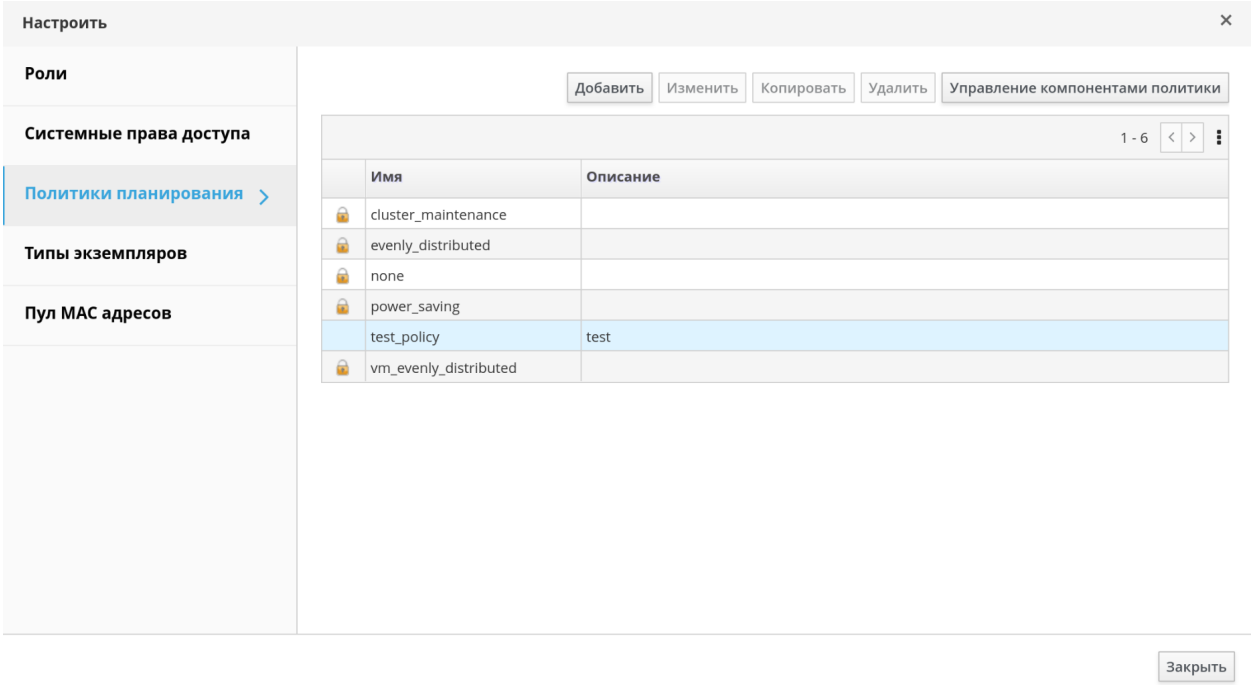


Рисунок 27 – Политика планирования добавлена в список доступных политик планирования

2.1.3.2 Параметры политик планирования

В таблице 13 приведено подробное описание параметров, доступных в окнах "Новая политика планирования" и "Параметры политики планирования".

Таблица 13 – 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

Поле	Описание
	заполнить, но оно не обязательно
Модули фильтров	Набор фильтров для контролирования хоста, на котором может выполняться ВМ из кластера (включенный 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 объемом 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 отдельном хосте, не являющемся 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.

Поле	Описание
	– HostedEnginesSpares – резервация места под ВМ диспетчера виртуализации на указанном числе узлов диспетчера виртуализации. – 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 отдается 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, определенной 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

Поле	Описание
	коэффициент хостов в соответствии с загрузкой ЦП хостов. Приоритет отдается хостам с наиболее высокой загрузкой ЦП. – OptimalForEvenCpuDistribution – определяет весовой коэффициент хостов в соответствии с загрузкой ЦП хостов. Приоритет отдается хостам с наиболее низкой загрузкой ЦП. – HA – определяет весовой коэффициент хостов в соответствии с оценкой их высокой доступности. – PreferredHosts – во время настройки ВМ приоритет отдается "предпочитаемым" хостам. – OptimalForMemoryPowerSaving – определяет весовой коэффициент хостов в соответствии с их потреблением памяти. Приоритет отдается хостам с более низким объемом доступной памяти. – OptimalForMemoryEvenDistribution – определяет весовой коэффициент хостов в соответствии с их потреблением памяти. Приоритет отдается хостам с более высоким объемом 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. Использоать кнопки + и – для добавления или удаления дополнительных свойств модуля балансировки нагрузки

2.1.4 Схема виртуализации

Схема виртуализации являются частью интерфейса РОСА Виртуализация и устанавливается из отдельного дистрибутива.

Для перехода в раздел со схемой виртуализации необходимо в навигационном меню выбрать раздел "Дополнения → Схема виртуализаций" (рисунок 28).

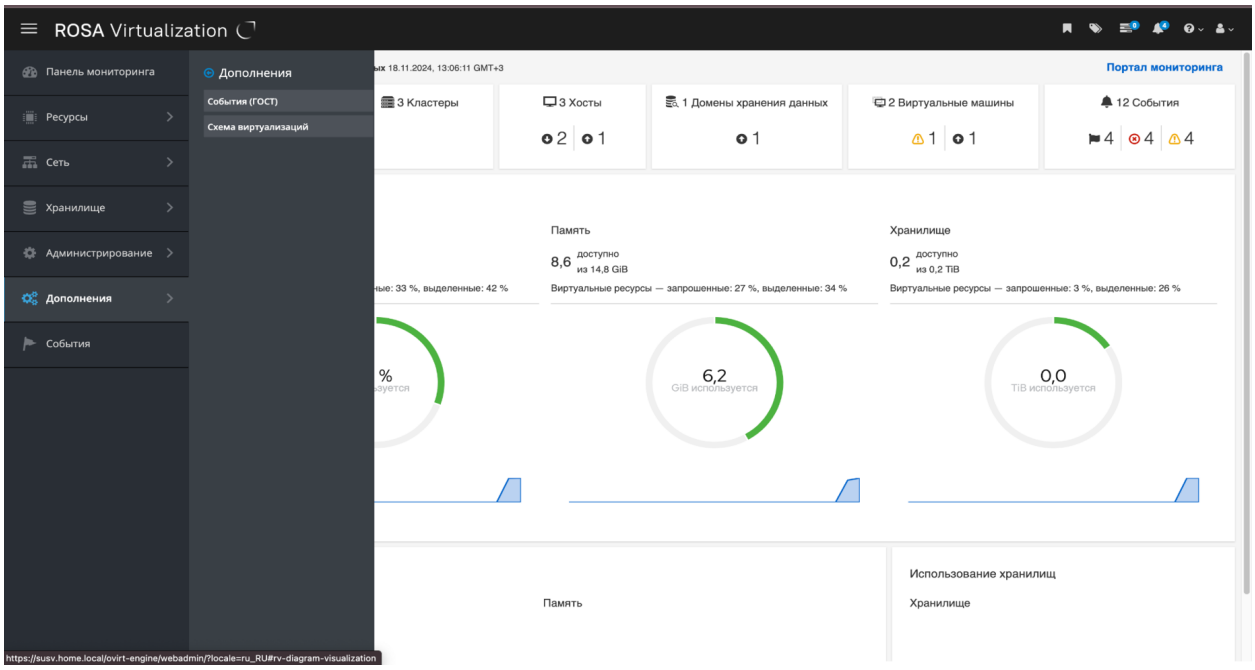


Рисунок 28 – Раздел "Дополнения → Схема виртуализаций"

После этого отобразится графический интерфейс схемы виртуализации (рисунок 29).

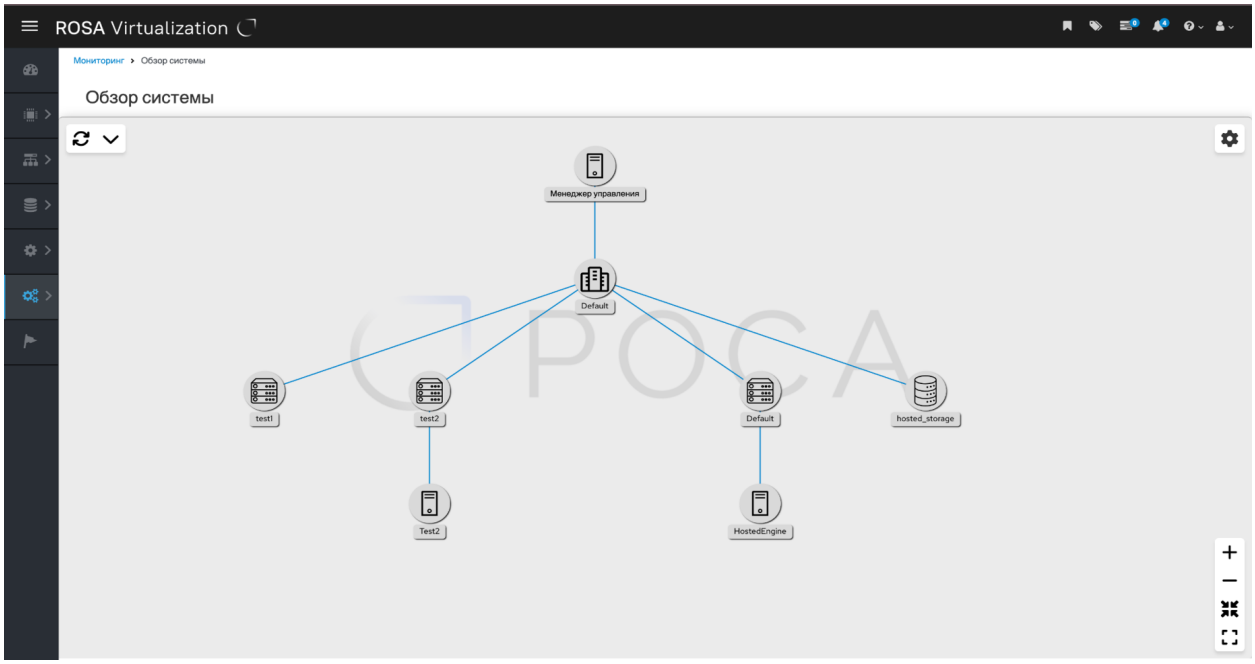


Рисунок 29 – Схема виртуализации

В схеме реализованы четыре основные функции (рисунок 30):

– Детальный просмотр схемы виртуализации;
– Меню автообновления данных – элемент 1;
– Меню настройки схемы – элемент 2;
– Меню управления отображением – элемент 3.

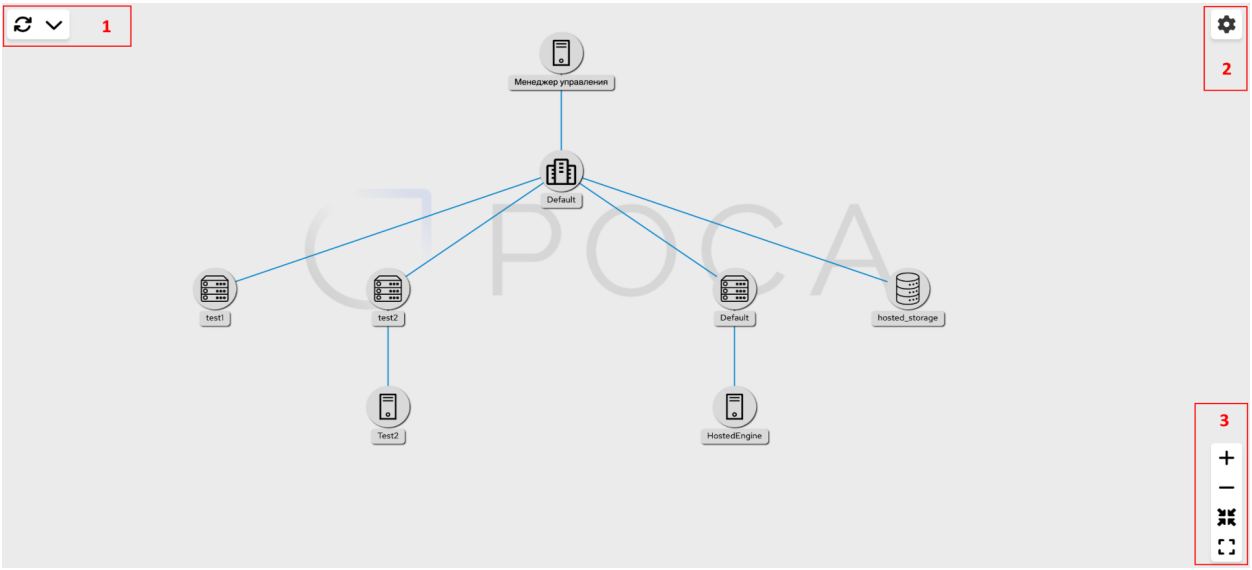


Рисунок 30 – Элементы управления схемы

2.1.4.1 Детальный просмотр схемы виртуализации

Детальный просмотр схемы виртуализации предоставляет расширенные возможности для анализа и управления виртуальной инфраструктурой. Схема представлена в удобной древовидной структуре, что упрощает восприятие взаимосвязей между элементами.

Функциональные возможности:

– Обзор схем – полная схема доступна для масштабирования и перемещения, что позволяет удобно работать с её отдельными элементами.

– Краткая информация – при наведении на любой элемент схемы появляется модальное окно с ключевыми сведениями (рисунок 31).

– Переход к элементу – с помощью кнопки Подробнее можно перейти на страницу элемента для более глубокого изучения (рисунок 32).

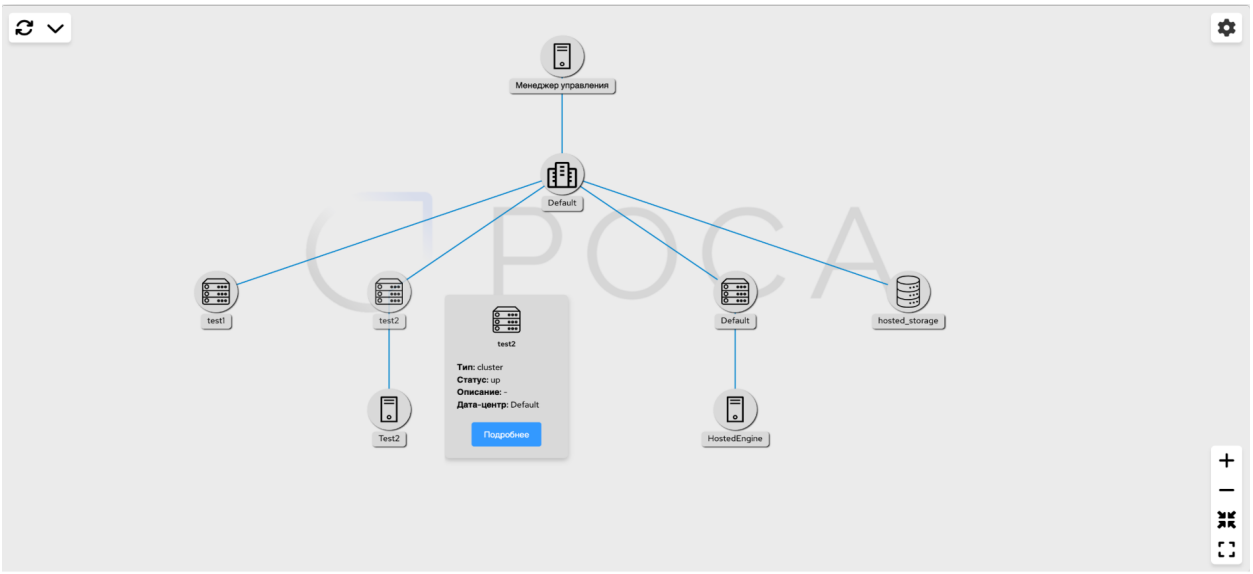


Рисунок 31 – Краткая информация

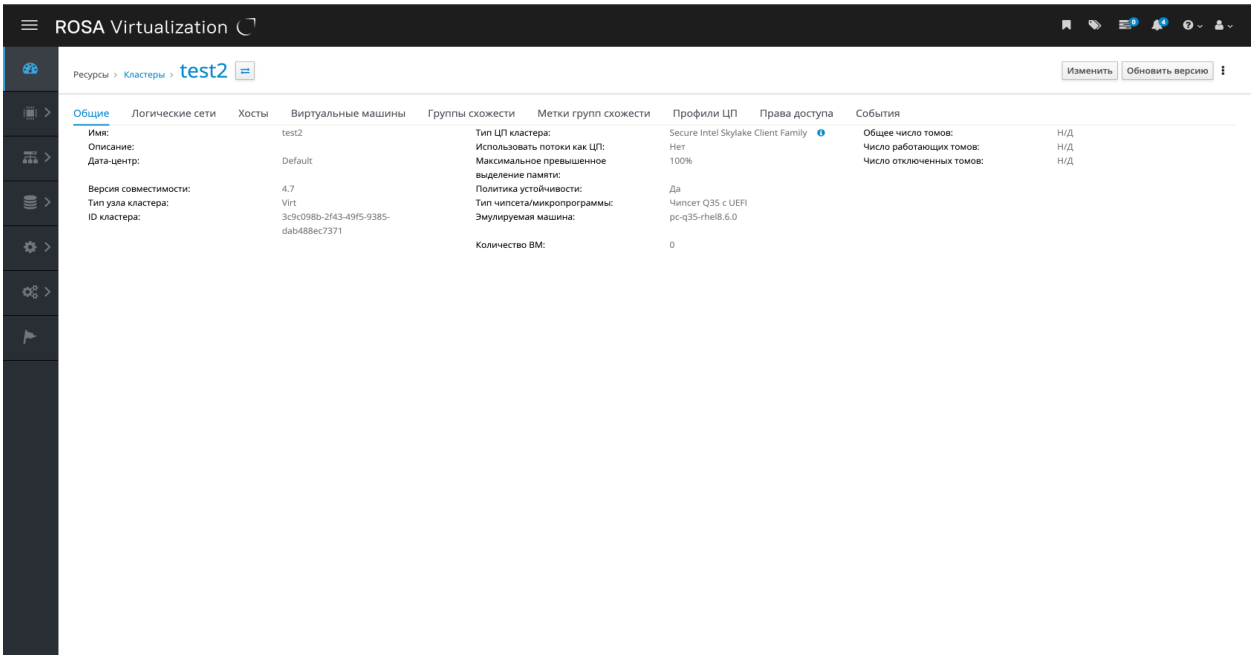


Рисунок 32 – Переход к элементу

2.1.4.2 Меню автообновления данных

Меню предназначено для удобного управления процессом обновления информации в режиме реального времени (рисунок 33).

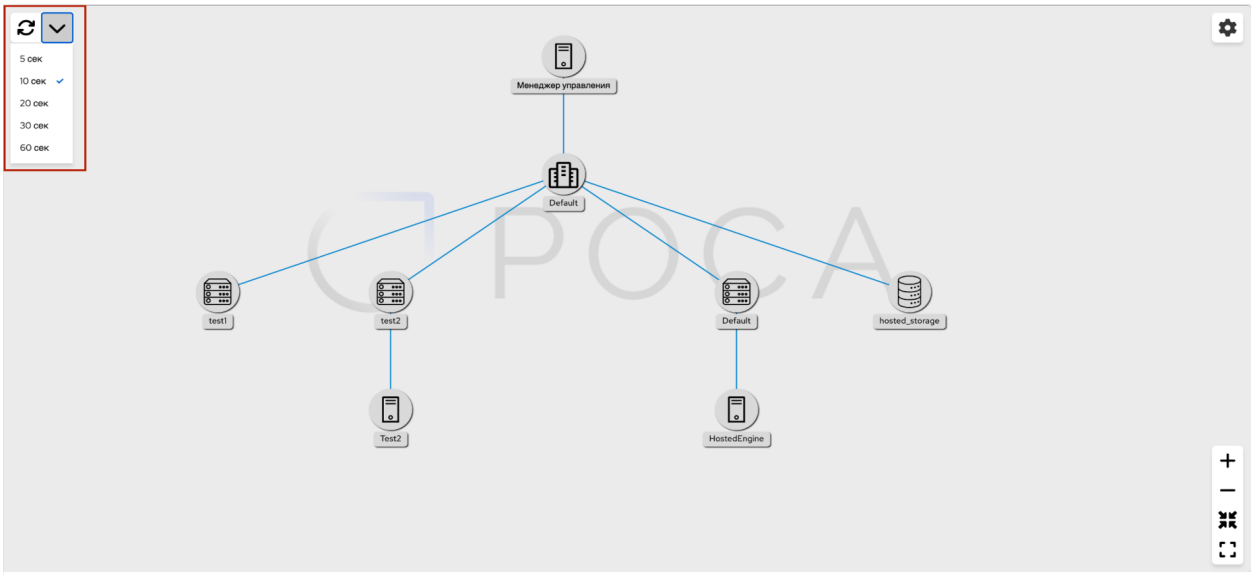


Рисунок 33 – Меню автообновление данных

Основные элементы:

– Кнопка обновления – позволяет вручную обновить данные в любой момент, обеспечивая актуальность отображаемой информации;

– Выпадающее меню – предоставляет выбор интервала автоматического обновления данных. Пользователь может выбрать предпочтительную частоту обновления (например, каждые 5 секунд, 30 секунд и т. д.).

Это меню помогает настроить обновление данных в соответствии с индивидуальными потребностями, обеспечивая баланс между актуальностью и производительностью.

2.1.4.3 Меню настройки схемы

Меню настройки схемы состоит из трёх пунктов (рисунок 34).

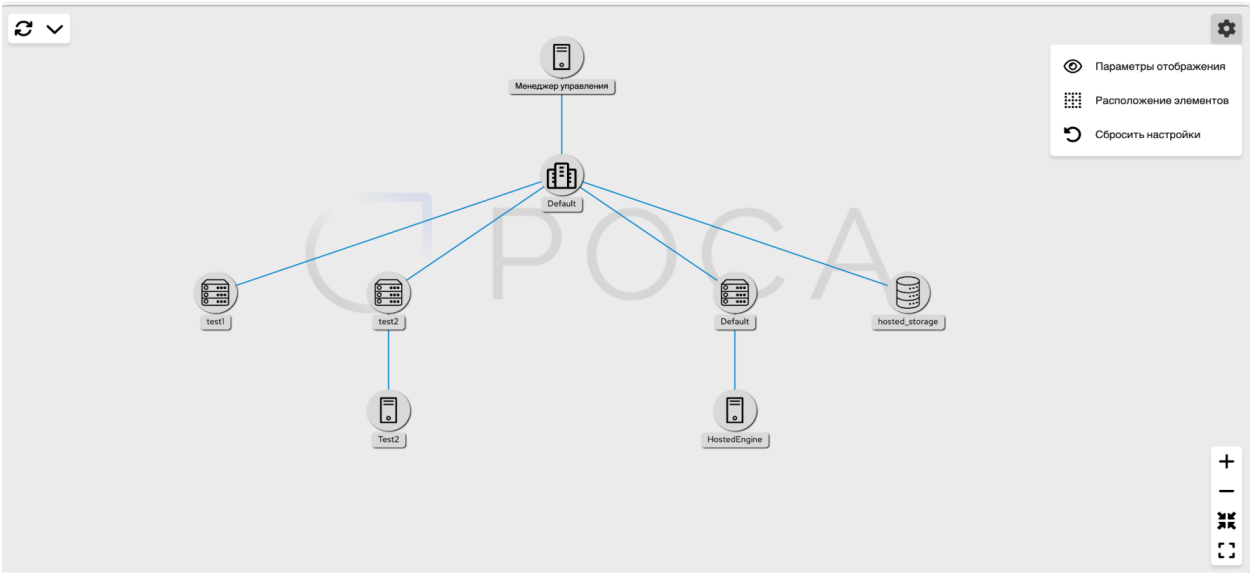


Рисунок 34 – Меню настройки схемы

Пункты меню:

– Параметры отображения – позволяет выбрать элементы для отображения на схеме, например дата-центры, кластеры, узлы и другие сущности. Выбор осуществляется через фильтры, что помогает скрывать ненужные элементы и улучшать восприятие визуализации (рисунок 35).

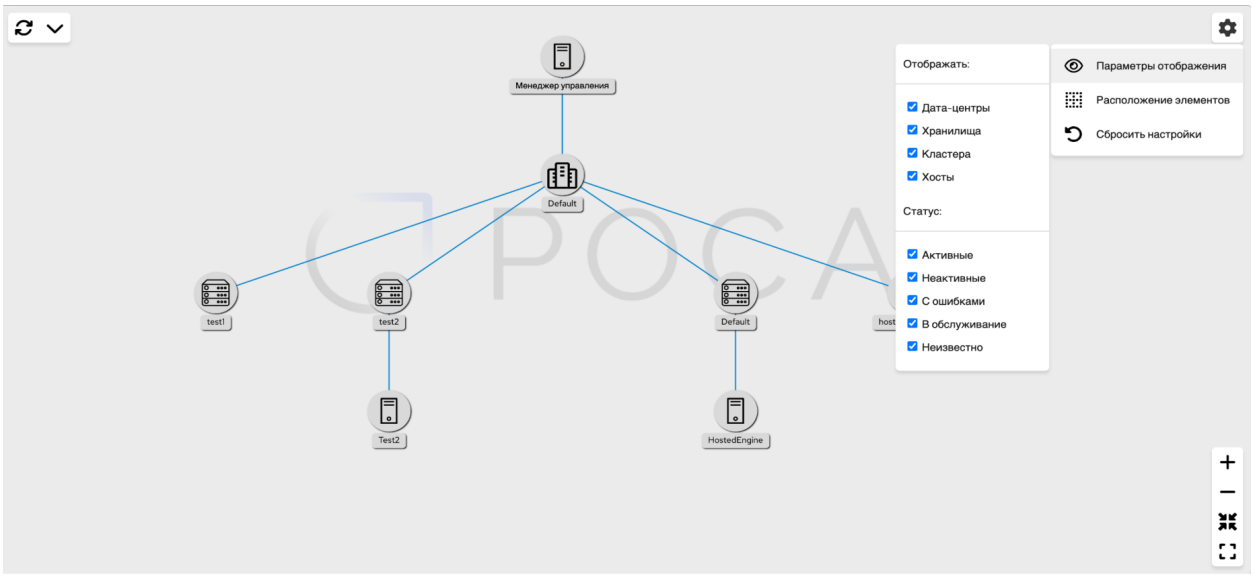


Рисунок 35 – Пункт "Параметры отображения"

– Расположение элементов – предоставляет полный контроль над позицией и визуальными параметрами объектов:

– Редактирование расположения элементов – пользователь может активировать специальный режим. Элемент при выборе выделяется границей. В этом режиме пользователь может перемещать элементы схемы, настраивая их расположение по своему усмотрению (рисунок 36).

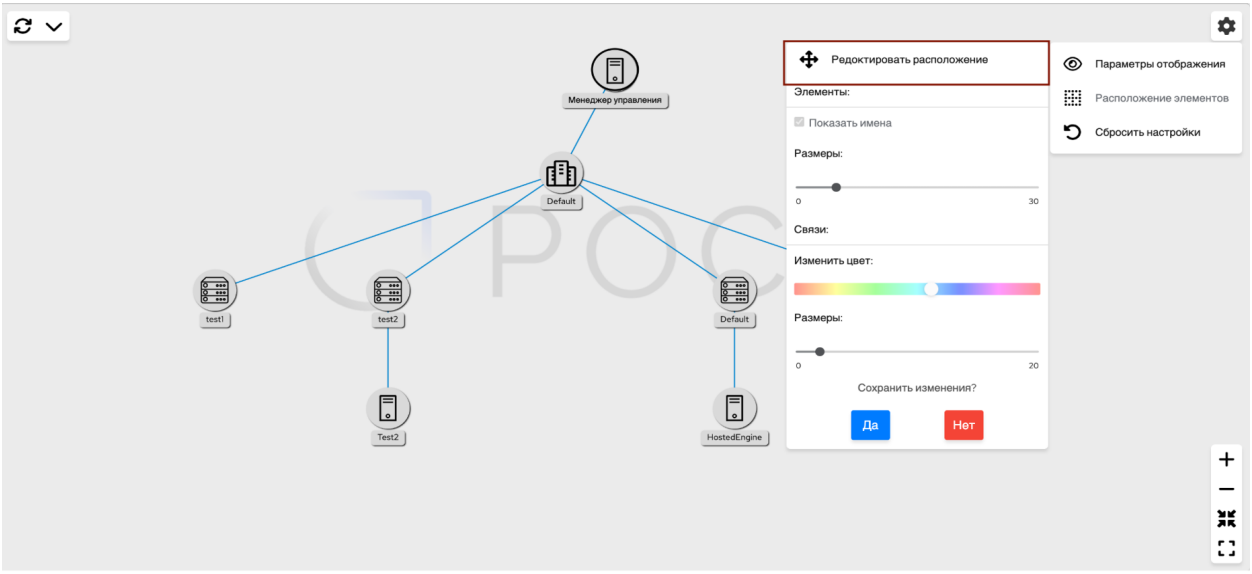


Рисунок 36 – Редактирование расположения элементов

– Кастомизация отображения – настройка параметров элементов, таких как отображение имен, изменение размеров объектов и связей между ними, а также настройка их цвета (рисунок 37).

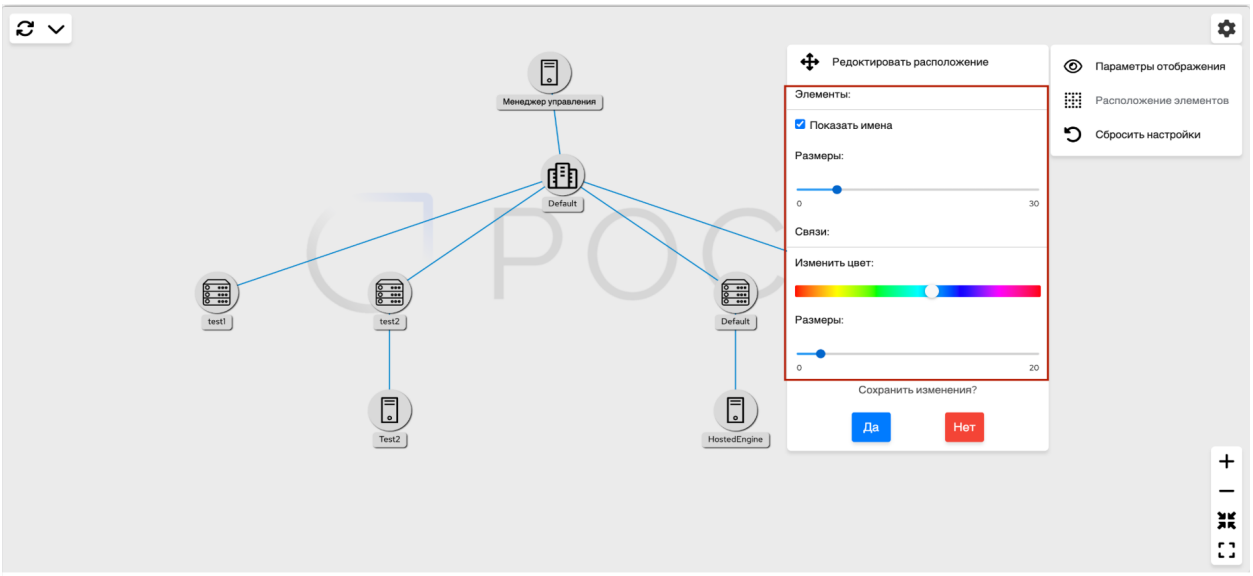


Рисунок 37 – Кастомизация отображения

После завершения редактирования пользователь может сохранить изменения или отменить их, вернув всё в исходное состояние (рисунок 38).

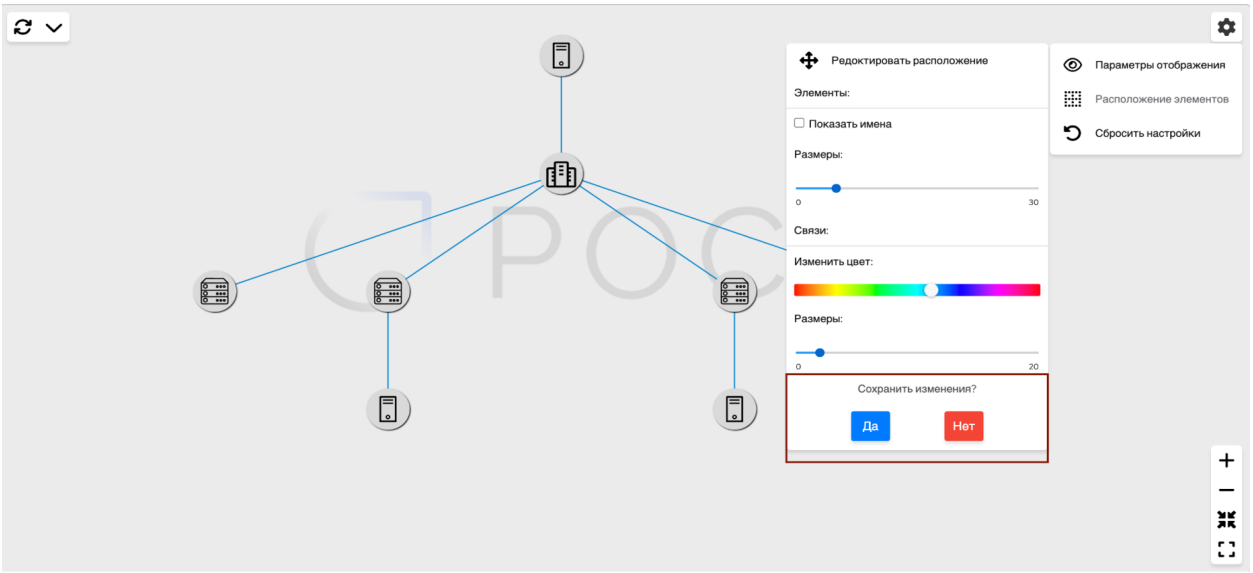


Рисунок 38 – Сохранение изменений

– Сбросить настройки – позволяет восстановить схему к состоянию по умолчанию, отменяя все пользовательские изменения (рисунок 39).

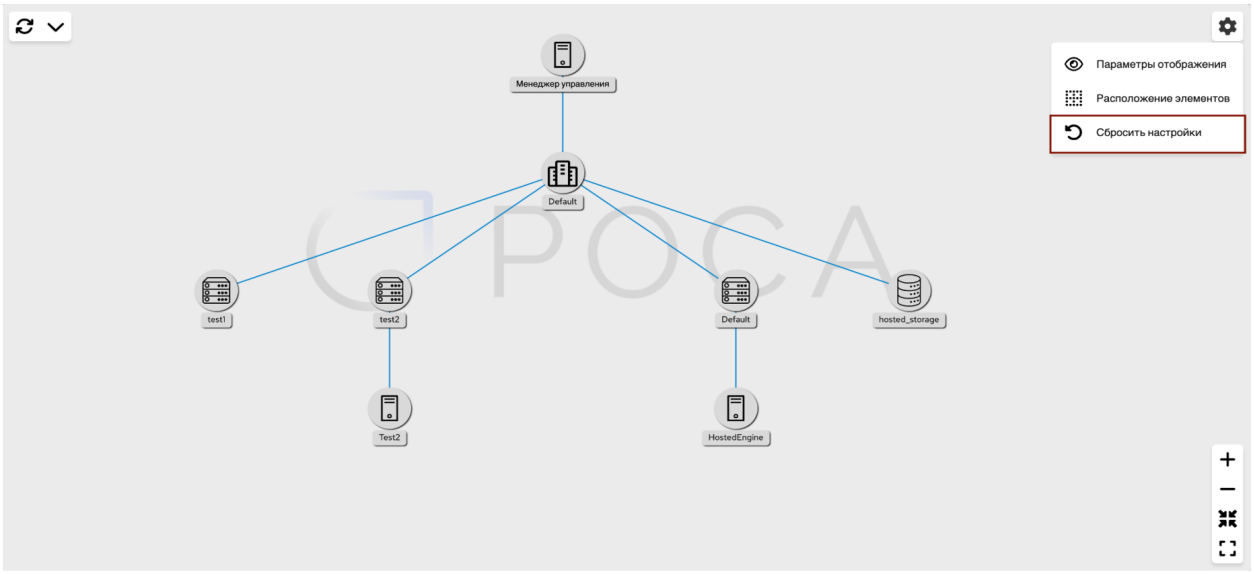


Рисунок 39 – Сброс настроек

2.1.4.4 Меню управления отображением

Меню состоит из четырех основных кнопок, каждая из которых выполняет важную функцию (рисунок 40):

– Увеличение масштаба – приближает отображение дерева для детального изучения;

– Уменьшение масштаба – отдаляет изображение, позволяя увидеть больше структуры дерева;

– Сброс масштаба и положения – возвращает дерево к исходному состоянию по масштабу и центру экрана;

– Полноэкранный режим – раскрывает дерево на весь экран, улучшая обзор и удобство работы.

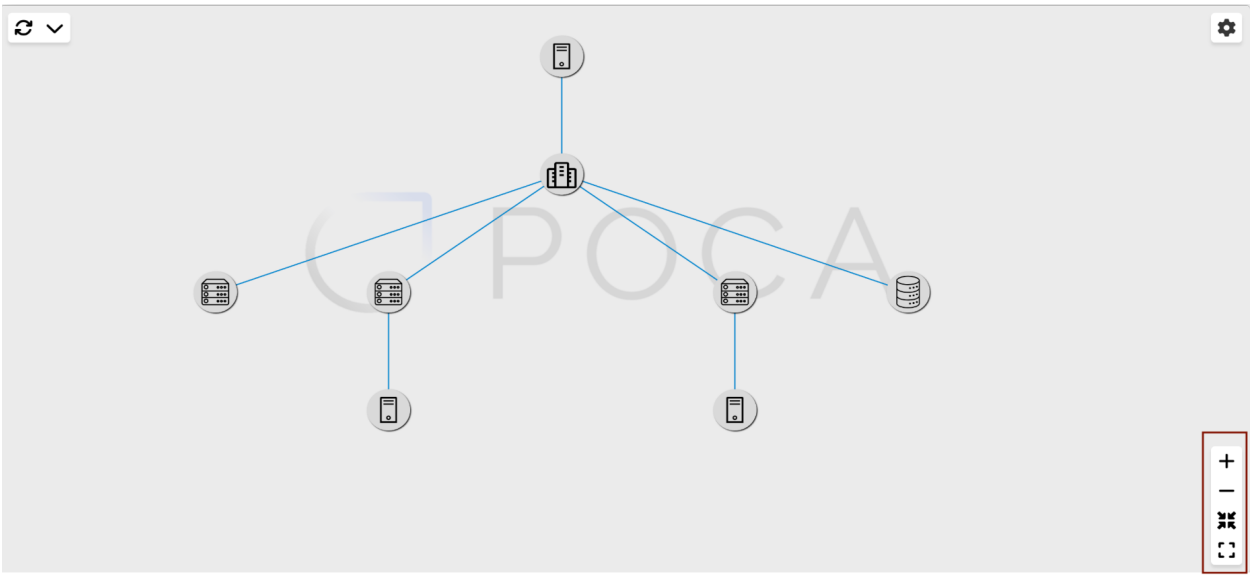


Рисунок 40 – Меню управления отображением

2.1.5 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 дает 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 таблица 14.

Таблица 14 – Предварительно настроенные типы экземпляров

Название	Память	Кол-во виртуальных ЦП
Tiny	512 МБ	1
Small	2 ГБ	1
Medium	4 ГБ	2
Large	8 ГБ	2
XLarge	16 ГБ	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.

2.1.5.1 Создание типов экземпляров

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

Для создания типа экземпляра:

а) перейти в "Администрирование → Настроить";

б) перейти на вкладку "Типы экземпляров" (рисунок 41). В секции справа отобразится список из доступных на данный момент экземпляров;

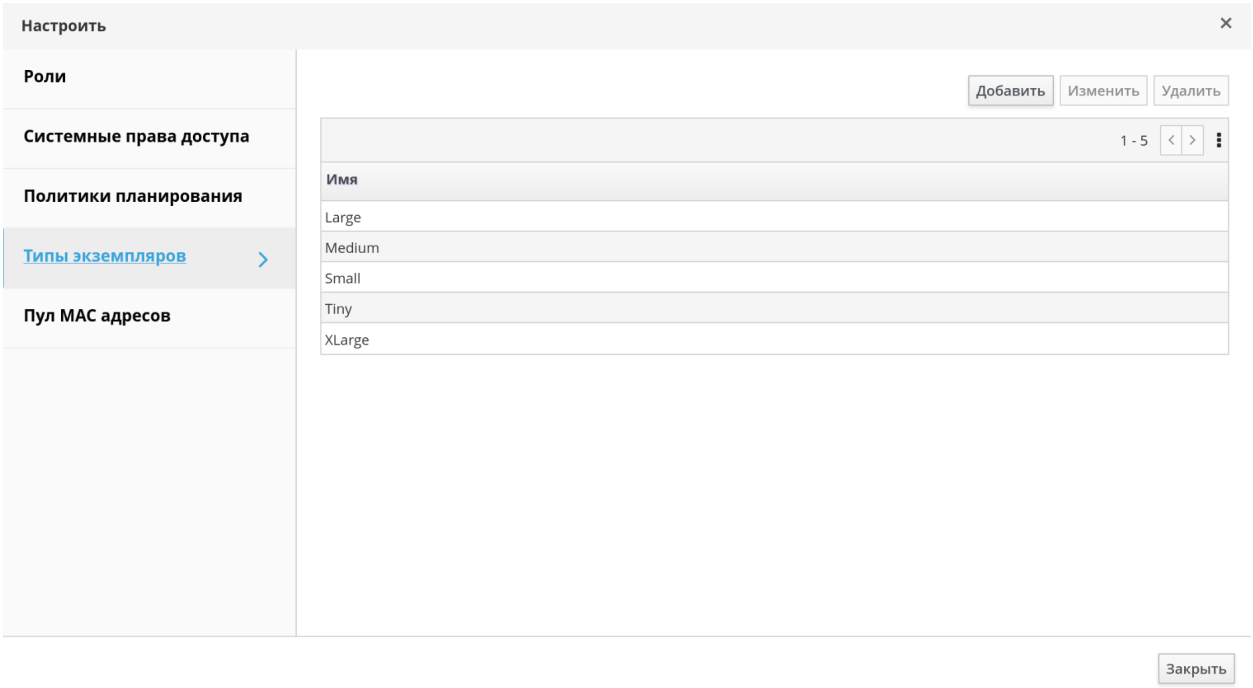


Рисунок 41 – Выбор типа экземпляра в секции "Администрирование → Настроить"

в) нажать кнопку Добавить, после чего откроется экранная форма "Новый тип экземпляра" (рисунок 42);

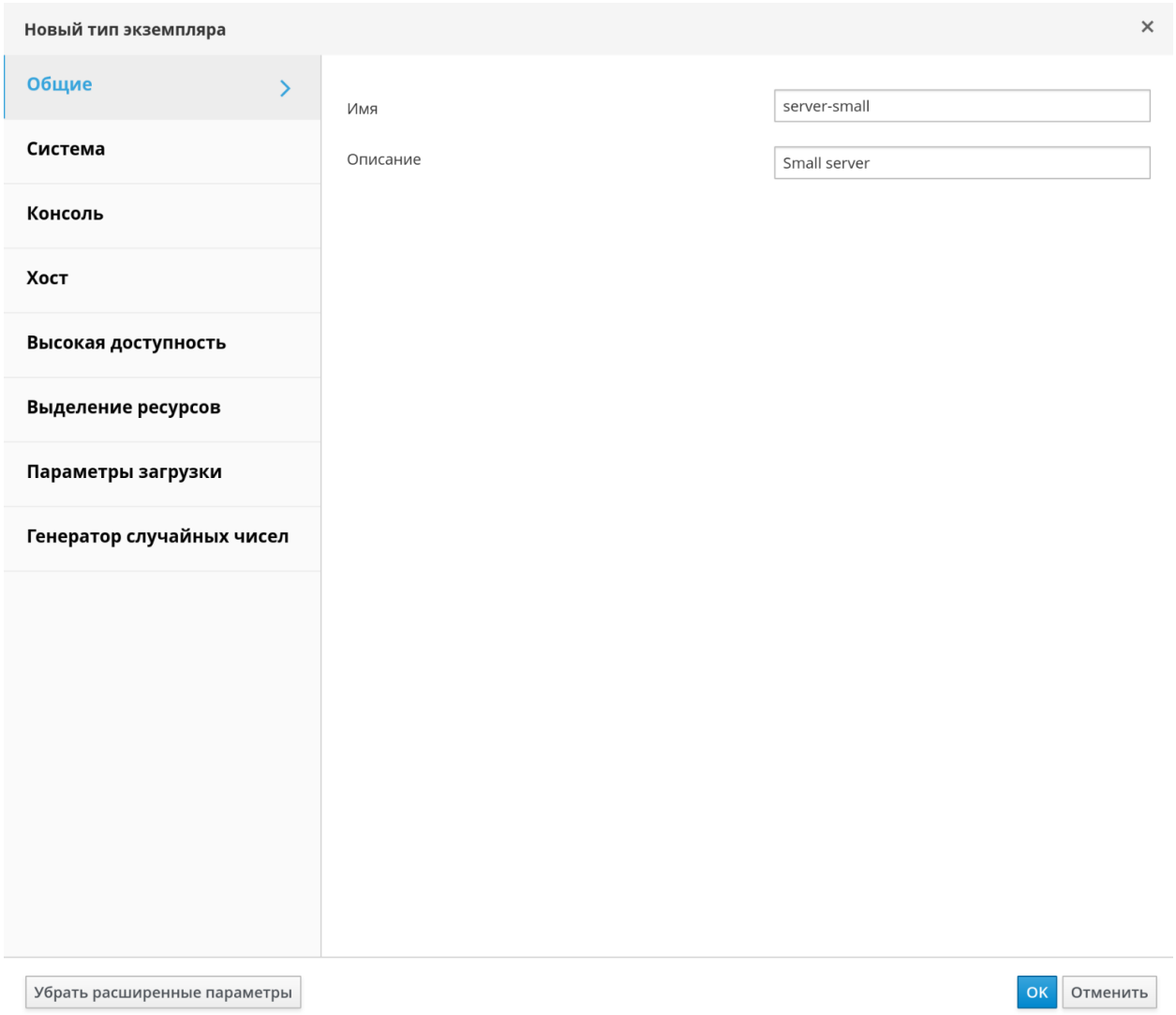


Рисунок 42 – Форма "Новый тип экземпляра" для добавления нового экземпляра

г) ввести "Имя" и "Описание" типа экземпляра;

д) выбрать секцию "Система" и нажать "Дополнительные параметры" (рисунок 43);

е) настроить 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 А.1);

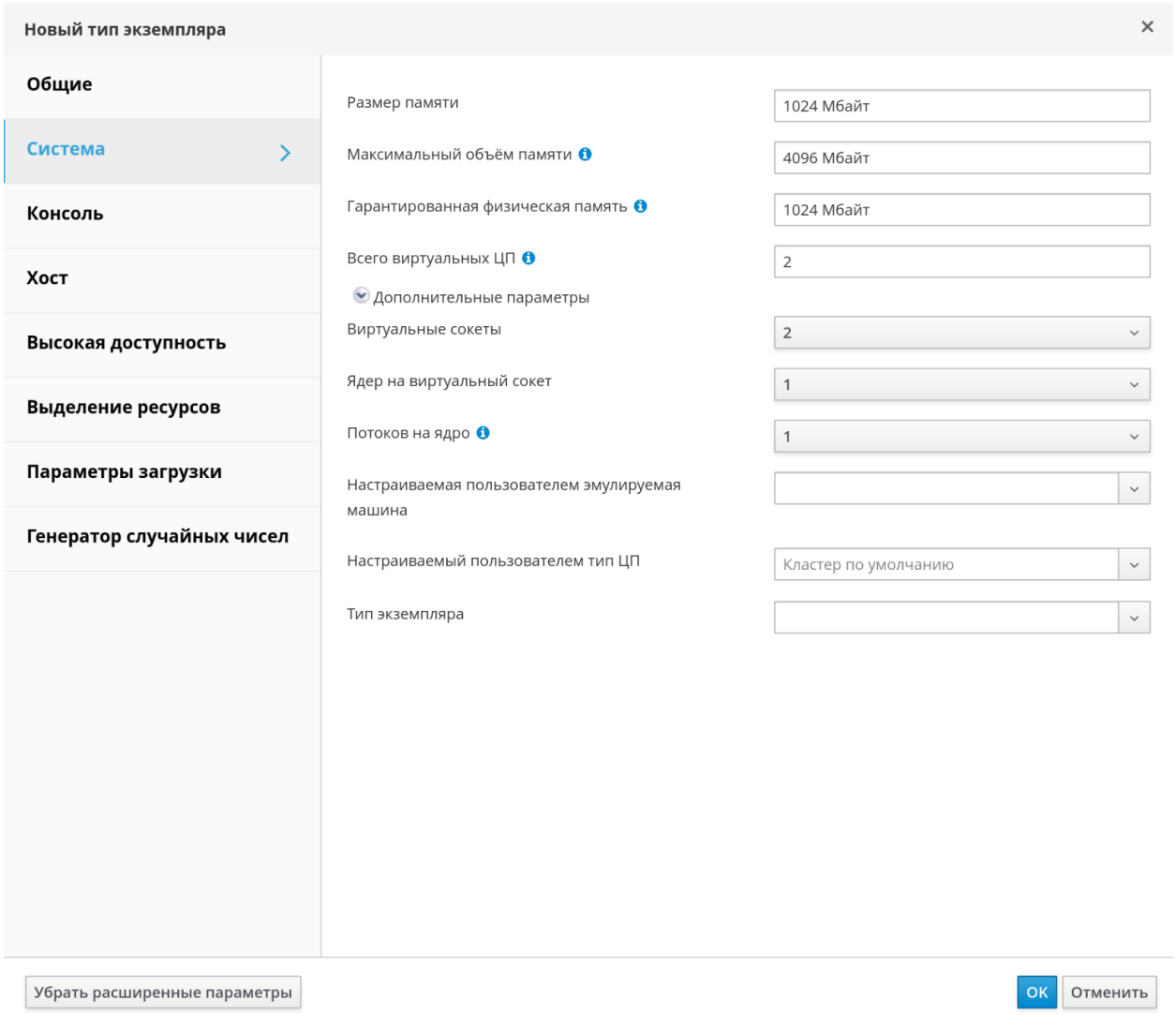


Рисунок 43 – Секция "Система" и подсекция "Дополнительные параметры"

ж) выбрать секцию "Консоль" (рисунок 44) и указать параметры консоли, используемые по умолчанию;

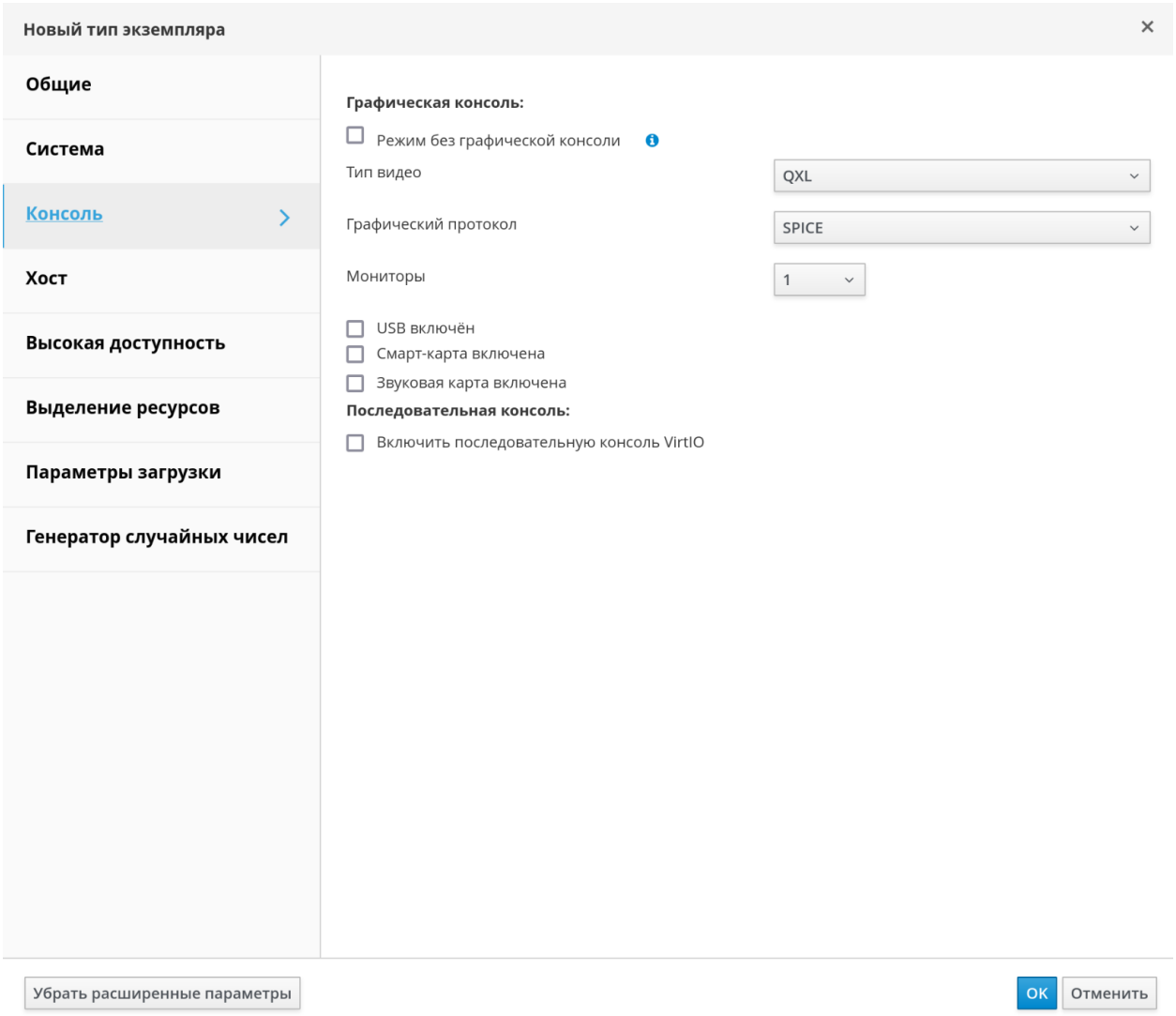


Рисунок 44 – "Новый тип экземпляра" — секция "Консоль"

з) нажать кнопку OK.

Новый тип экземпляра появится во вкладке "Типы экземпляров" в секции "Администрирование → Настроить" (рисунок 47).

Новый тип экземпляра может быть выбран в выпадающем списке "Тип экземпляра" при создании или изменении ВМ ("Ресурсы → Виртуальные машины → Добавить") (рисунок 45).

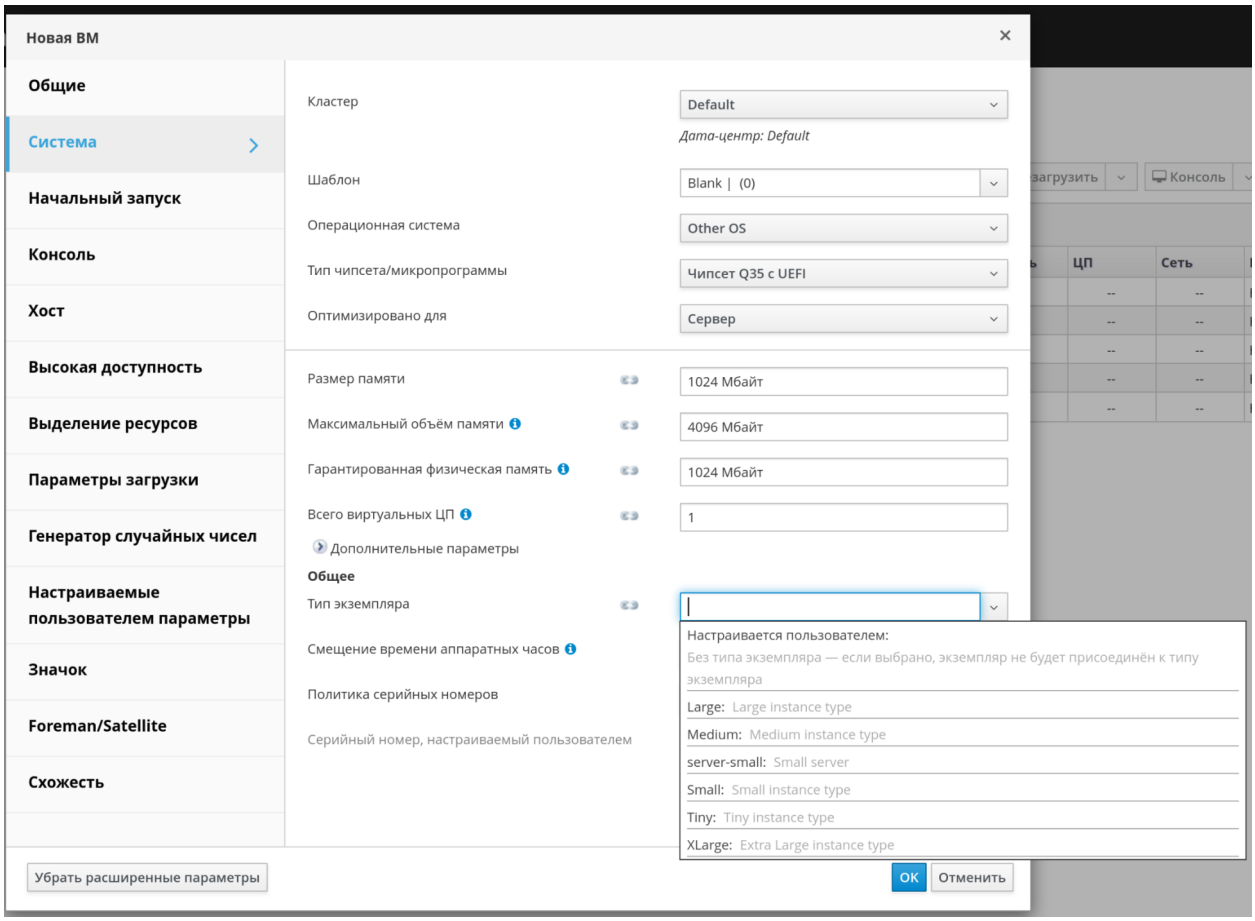


Рисунок 45 – Выбор типа экземпляра при создании новой ВМ

Тип экземпляра новой ВМ отображается во вкладке "Система" (рисунок 46).

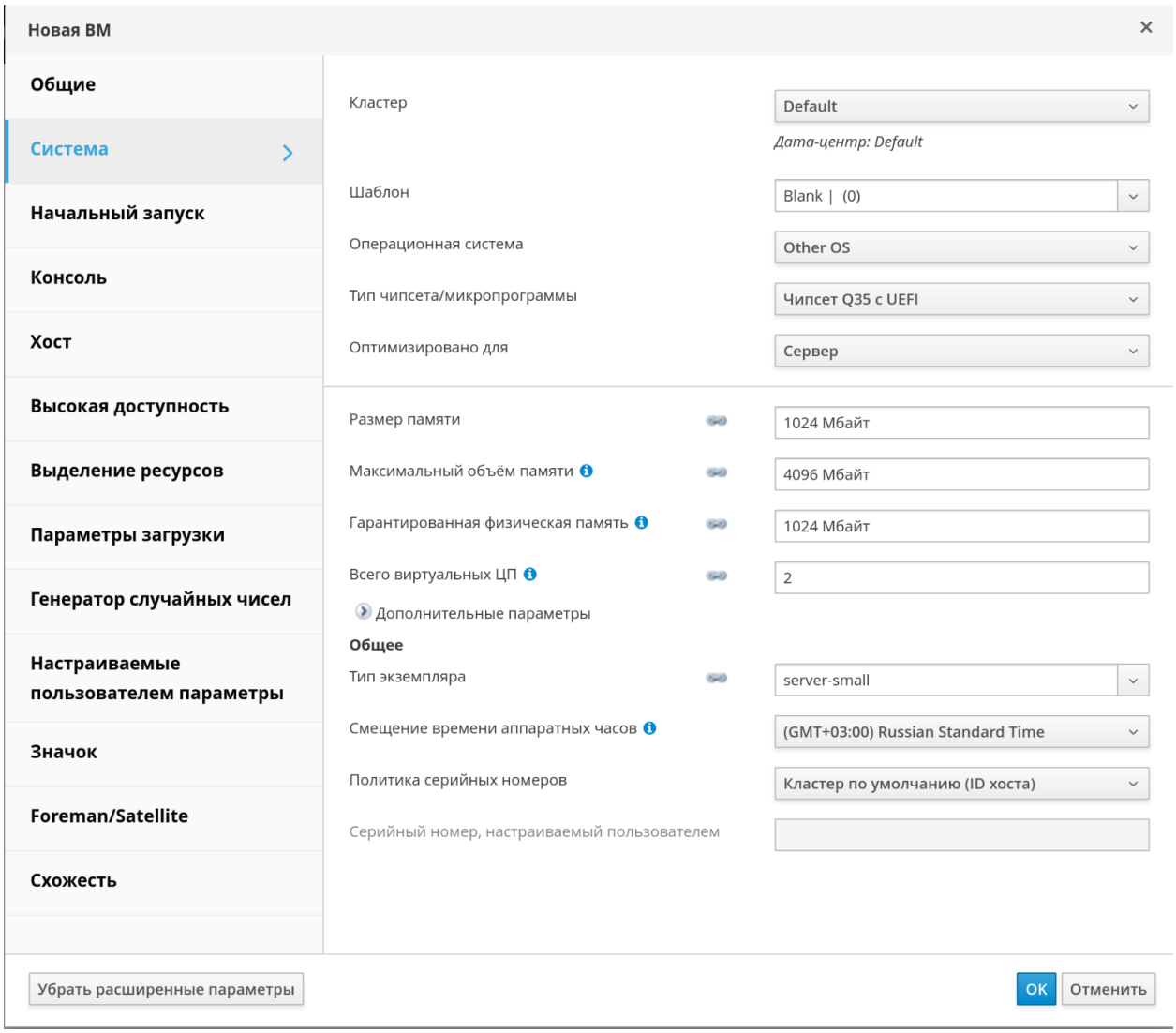


Рисунок 46 – При создании новой ВМ выбран экземпляр (Тип экземпляра) server-small

В примере на рисунок 47 добавлен новый тип экземпляра server-small.

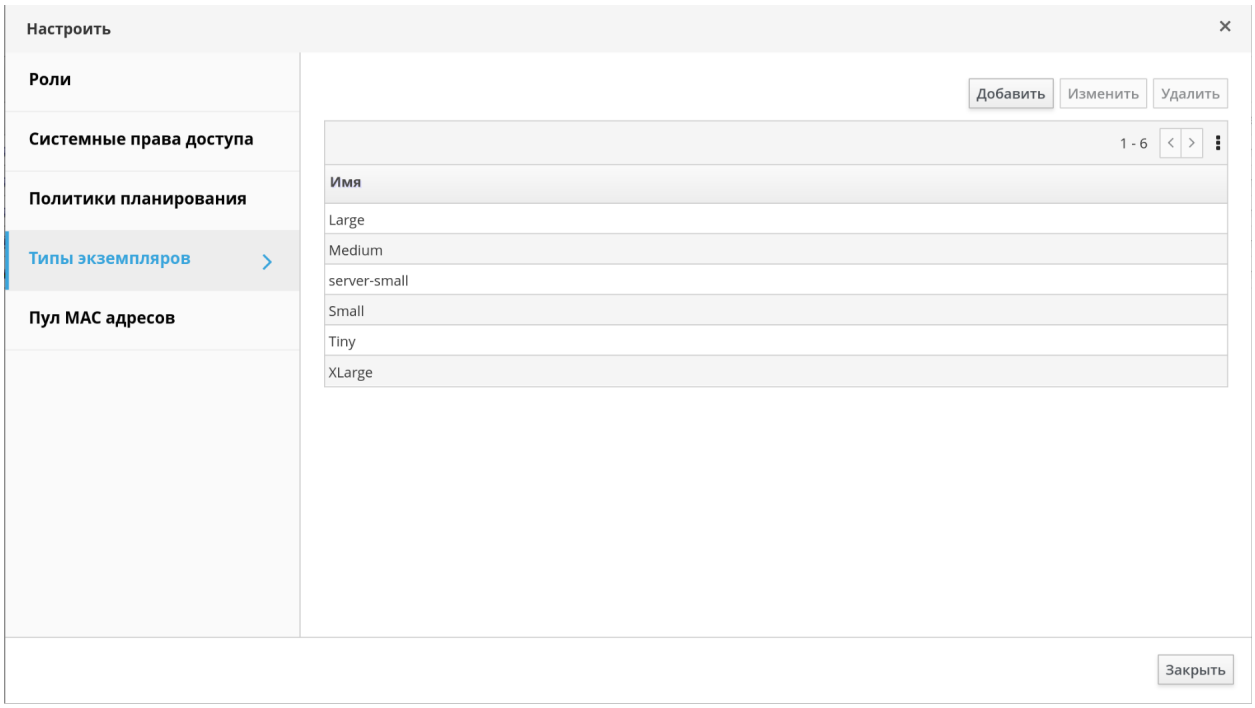


Рисунок 47 – Секция "Типы экземпляров" — список экземпляров с добавленным новым типом экземпляра

2.1.5.2 Изменение типов экземпляров

В окне "Параметры" администраторы могут изменять типы экземпляров.

Для изменения параметров типов экземпляров нужно:

а) выбрать "Администрирование → Настроить";
б) перейти на вкладку "Типы экземпляров";
в) выбрать изменяемый тип экземпляра;
г) нажать кнопку Изменить (рисунок 48);

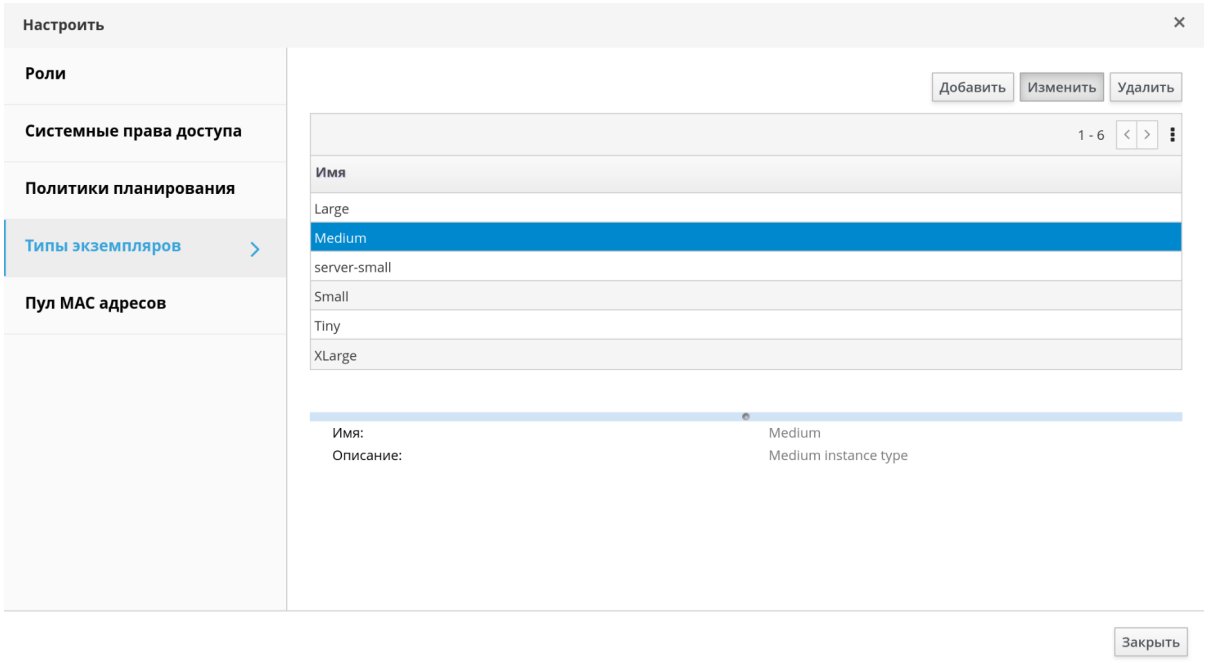


Рисунок 48 – Выбор типа экземпляра для внесения изменений

д) изменить параметры экземпляра так, как это необходимо (рисунок 49);

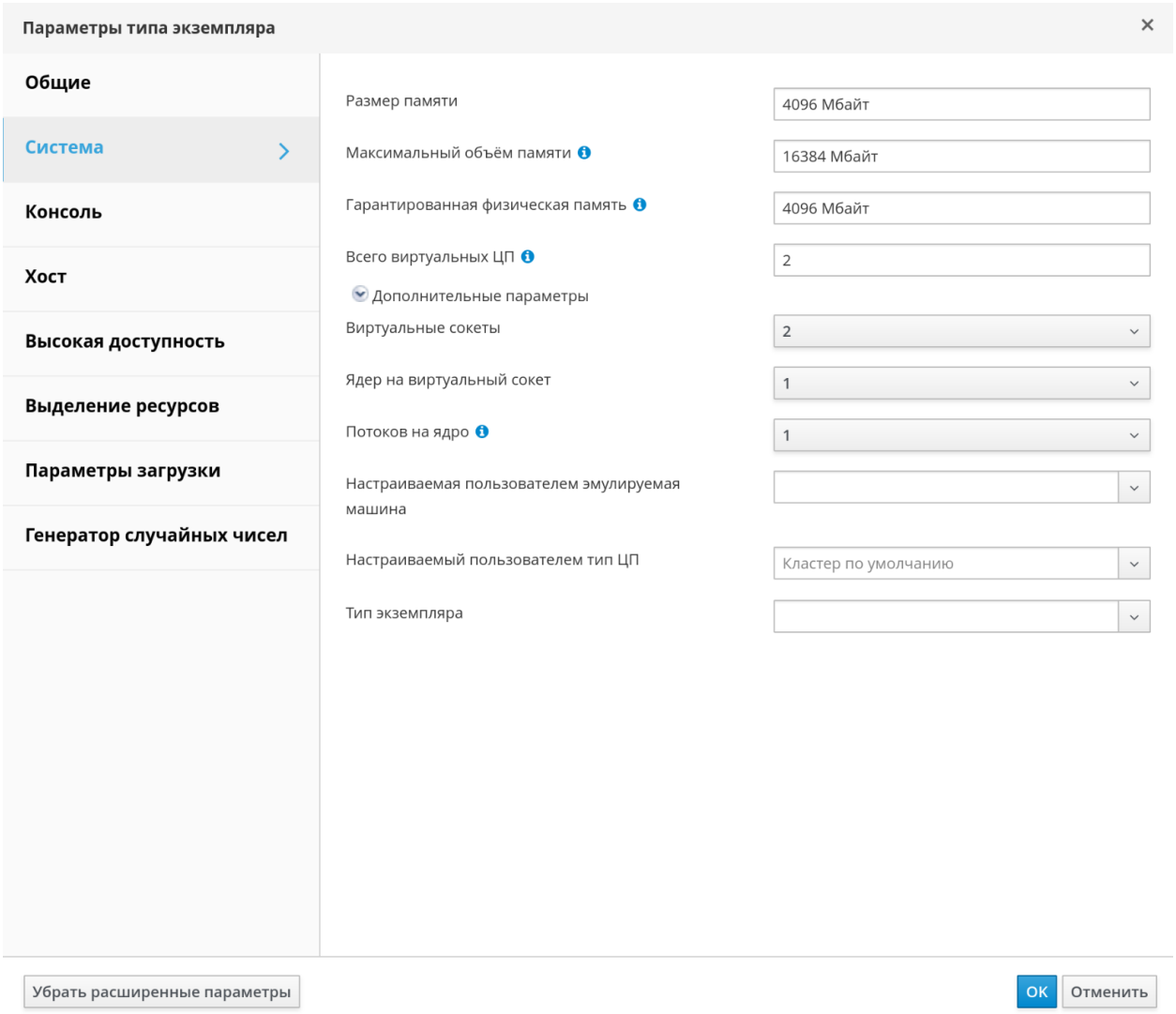


Рисунок 49 – Изменение параметров экземпляра

е) нажать кнопку 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.

2.1.5.3 Удаление типов экземпляров

Для удаления типа экземпляра нужно:

а) выбрать "Администрирование → Настроить";
б) перейти на вкладку "Типы экземпляров";
в) выбрать удаляемый тип экземпляра;
г) нажать кнопку Удалить (рисунок 50);
д) при наличии ВМ, созданных на основе этого типа экземпляра, появится предупреждающее окно со списком привязанных машин. Для удаления типа экземпляра установить флажок "Подтвердить операцию". В противном случае нажать кнопку Отмена;
е) указать причину удаления (опционально) и нажать кнопку OK для подтверждения удаления экземпляра (рисунок 50) или кнопку Отменить для отмены удаления.

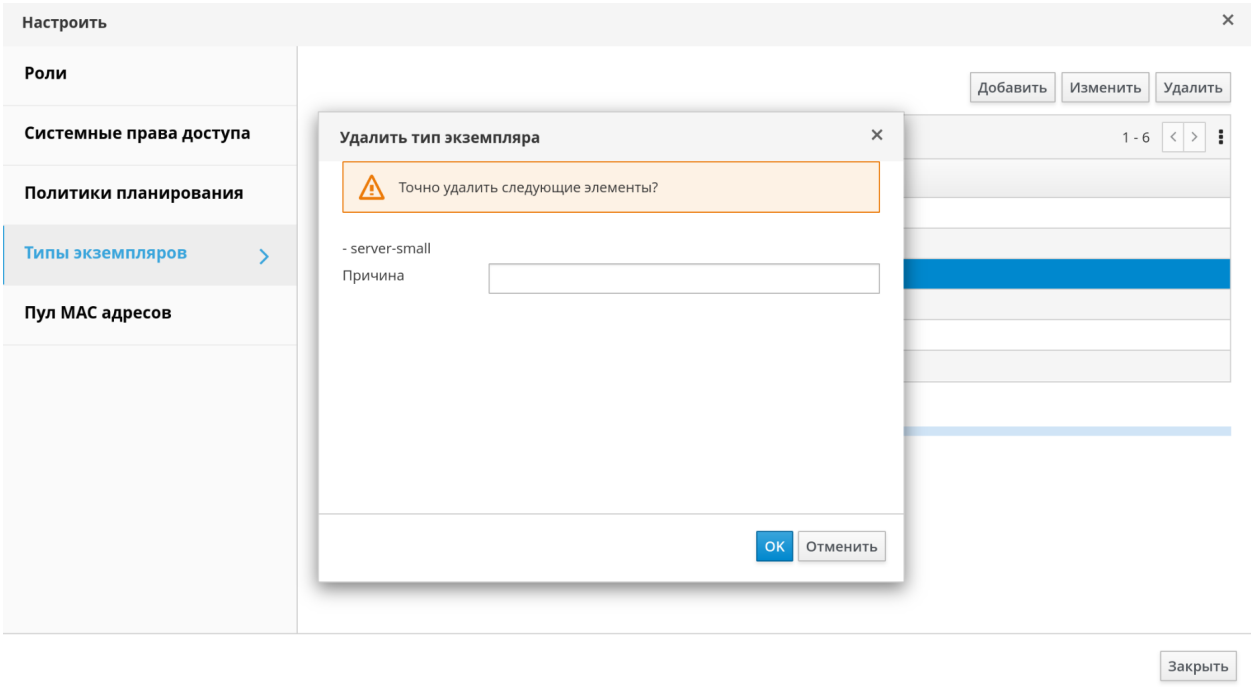


Рисунок 50 – Окно "Удалить тип экземпляра"

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

2.1.6 Пулы MAC-адресов

Пулы MAC-адресов определяют диапазоны MAC-адресов, выделенные для каждого кластера. Пул MAC-адресов настраивается для каждого кластера. Используя пулы MAC-адресов, Система виртуализации может автоматически создавать и присваивать MAC-адреса новым устройствам в виртуальной сети, что помогает предотвратить дублирование адресов. Пулы MAC-адресов 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 MAC-адресов, но каждому кластеру присваивается один пул. Система виртуализации создает изначальный пул MAC-адресов, который используется в случае, если не будет присвоено ни одного пула. Подробности о присвоении кластерам пулов MAC-адресов приведены в п. 3.3.2.1.

Примечание — Если сеть разделяют более одного кластера Системы виртуализации, не нужно полагаться только на изначальный пул MAC-адресов, так как ВМ каждого кластера попытаются использовать один и тот же диапазон адресов, что приведет к конфликтам. Во избежание конфликтов MAC-адресов следует проверять диапазоны пулов, чтобы каждому кластеру был присвоен уникальный диапазон MAC-адресов.

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

Полномочия пользователей пула задаются через роли и определяют, какие дата-центры могут использовать пул MAC-адресов. Подробности о добавлении новых полномочий пользователям приведены в п. 2.1.1.

2.1.6.1 Создание пулов MAC адресов

Для создания пула MAC адресов нужно выполнить следующие действия:

а) выбрать "Администрирование → Настроить";
б) перейти на вкладку "Пул MAC адресов" (рисунок 51);

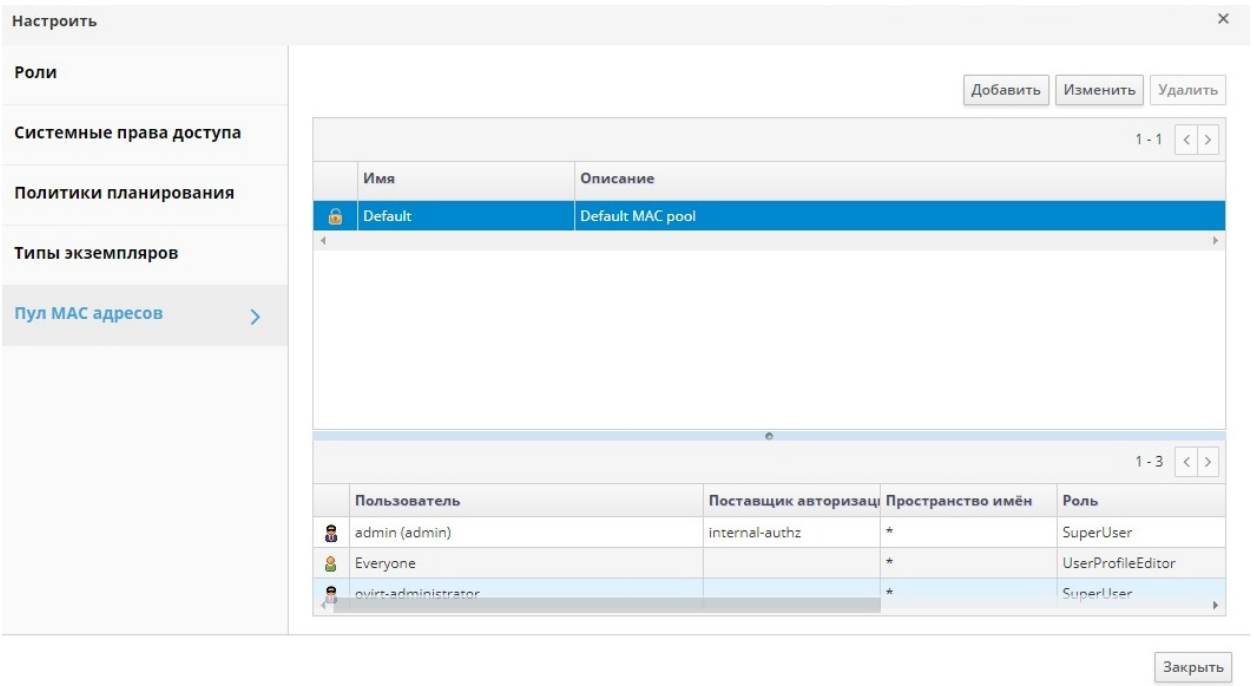


Рисунок 51 – Меню "Пул MAC адресов"

в) нажать кнопку Добавить;
г) ввести "Имя" и "Описание" нового пула MAC-адресов (рисунок 52);
д) установить флажок "Разрешить дубликаты", чтобы разрешить использование в пуле одного и того же MAC-адреса более одного раза. Пул не будет автоматически использовать дублирующий MAC-адрес, но включение параметра, разрешающего дубликаты, означает, что пользователь может вручную использовать дублирующий адрес;

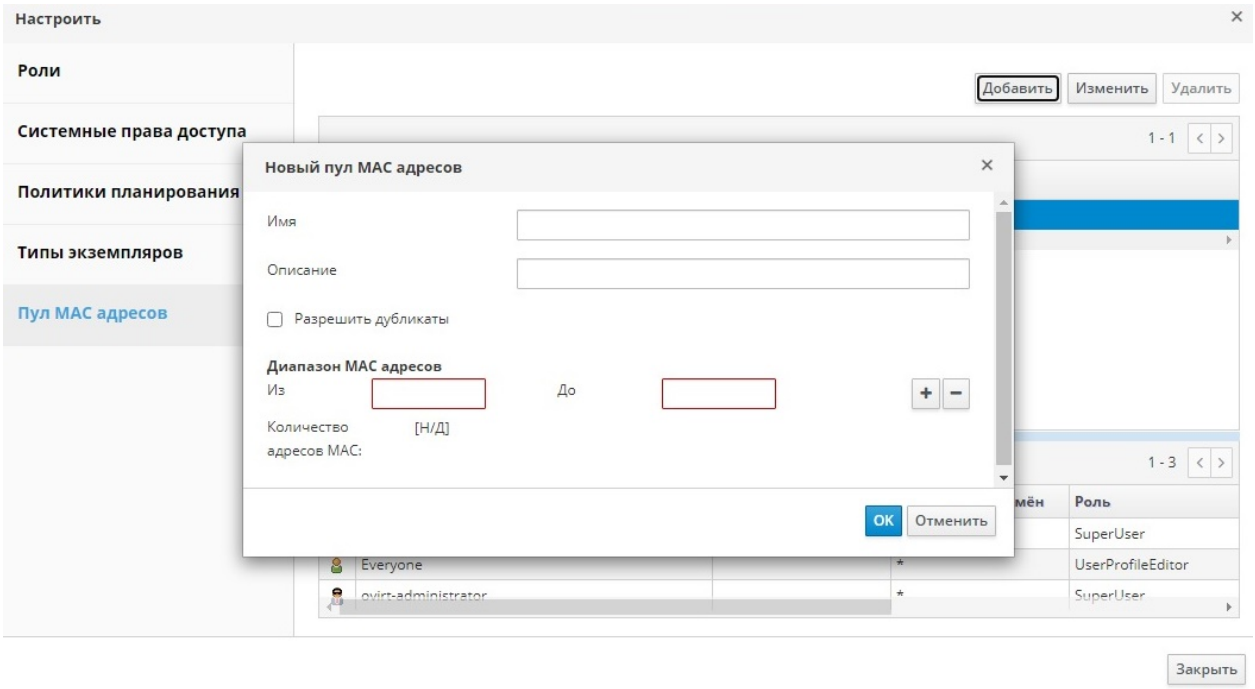


Рисунок 52 – Новый пул MAC-адресов

Примечание — Если в одном пуле дубликаты разрешены, а в другом пуле — нет, то каждый MAC-адрес может один раз использоваться в пуле с запрещенными дубликатами и много раз использоваться в пуле с разрешенными дубликатами.

е) указать необходимый "Диапазон MAC адресов";

ж) для указания нескольких диапазонов нажать кнопку + в одной строке с полями "Из" и "До";

з) нажать кнопку OK.

2.1.6.2 Изменение пулов MAC-адресов

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

Для изменения параметров пулов MAC-адресов нужно выполнить следующие действия:

и) выбрать "Администрирование → Настроить";

к) перейти на вкладку "Пул MAC-адресов" (рисунок 51);

л) выбрать изменяемый пул;

м) нажать кнопку Изменить;

н) нужным образом изменить поля "Имя", "Описание", "Разрешить дубликаты" и "Диапазон MAC-адресов";

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

о) нажать кнопку OK.

2.1.6.3 Удаление пулов MAC-адресов

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

Для удаления пула MAC-адресов нужно:

п) выбрать "Администрирование → Настроить";

р) перейти на вкладку "Пул MAC-адресов";

с) выбрать удаляемый пул;

т) нажать кнопку Удалить;

у) нажать кнопку OK.

2.2 Панель мониторинга

Панель мониторинга (рисунок 53) предлагает общий обзор состояния Системы виртуализации с помощью сводки сведений об ее ресурсах и общем коэффициенте использования. Эта сводка может предупредить о проблеме и дает 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.

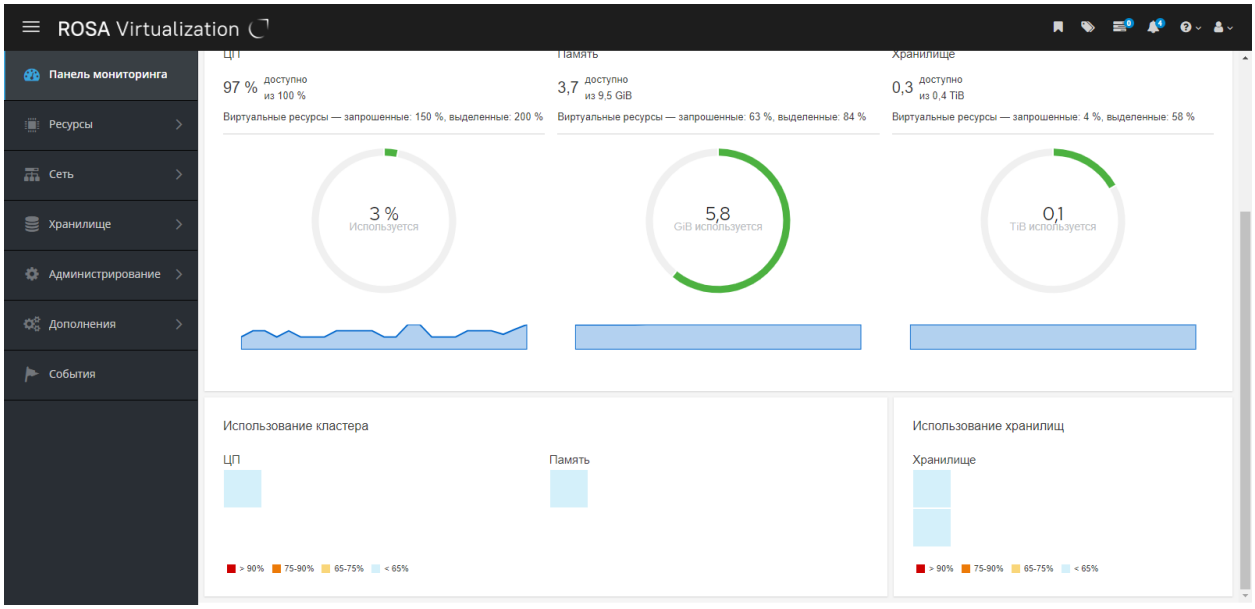


Рисунок 53 – Панель мониторинга

2.2.1 Предварительные условия для установки

Для панели мониторинга необходимо установленное и настроенное хранилище данных.

2.2.2 Общий перечень

Самый верхний раздел панели мониторинга предлагает общий перечень ресурсов Системы виртуализации (рисунок 54), в который входят секции для "Дата-центров", "Кластеров", "Хостов", "Доменов хранилищ", "Виртуальных машин" и "Событий". Значки показывают состояние каждого ресурса, а числа — количество ресурсов с этим статусом.

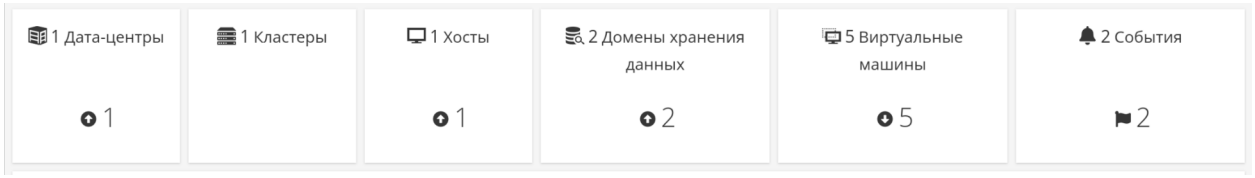


Рисунок 54 – Общий перечень ресурсов в панели мониторинга

Заголовок показывает номер типа ресурса, а статус ресурса показывается под заголовком. В таблице 15 приведено описание статусов ресурсов и значков,

отображающих состояние ресурсов. При нажатии на ресурс можно перейти на соответствующую страницу диспетчера виртуализации. "Статус" кластеров всегда показывается как "Недоступно".

Таблица 15 – Статусы ресурсов

Значок	Статус
	Ни один из этих ресурсов не был добавлен в Систему виртуализации РОСА Виртуализация
	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 – "идет запуск", "работа приостановлена", "идет миграция", "ожидание", "заморожено" или "идет выключение". – Хосты – поиск ограничен хостами со статусами – "не назначен", "в режиме обслуживания", "идет установка", "идет перезагрузка", "подготовка к обслуживанию", "ожидает утверждения" или "идет подключение". – Домены хранилищ – поиск ограничен доменами хранилищ со статусами – "не инициализирован", "не присоединен", "неактивен", "в режиме обслуживания", "подготовка к обслуживанию", "отсоединение" или "активация". – Виртуальные машины – поиск ограничен машинами со статусом – "идет запуск", "работа приостановлена", "идет миграция", "ожидание", "заморожена" или "идет выключение". – События – поиск ограничен серьезностью 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 не запущенными.

Значок	Статус
	– Тома Gluster – поиск ограничен неактивными или отсоединенными 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 отсоединенными или неактивными доменами хранилищ. – Виртуальные машины – поиск ограничен не запущенными машинами, не отвечающими или в перезагрузке
	Показывает число событий с оповещениями о состоянии. Нажатие на значок переносит на страницу "События" с поиском, ограниченным серьезностью оповещения
	Показывает количество событий с ошибкой. Нажатие на значок переносит на страницу "События" с поиском, ограниченным серьезностью ошибки

2.2.3 Общий коэффициент использования

Раздел "Общее использование" (рисунок 55) показывает коэффициент использования ЦП, памяти и хранилища и общее использование ресурсов кластера (рисунок 56).

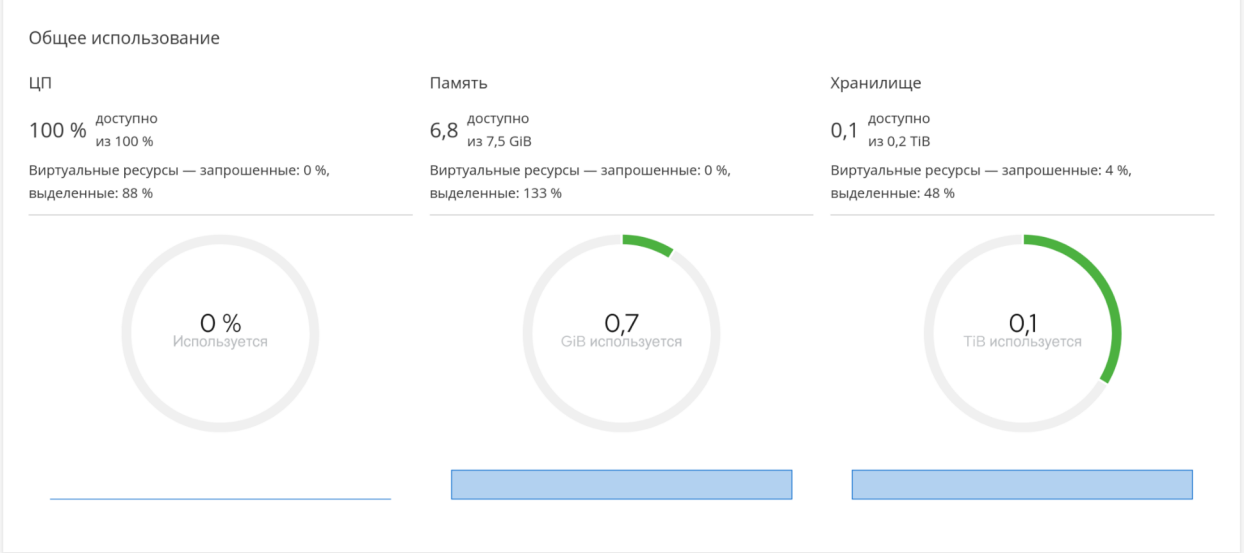


Рисунок 55 – Общее использование ЦП, памяти и хранилища

В верхнем части 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.

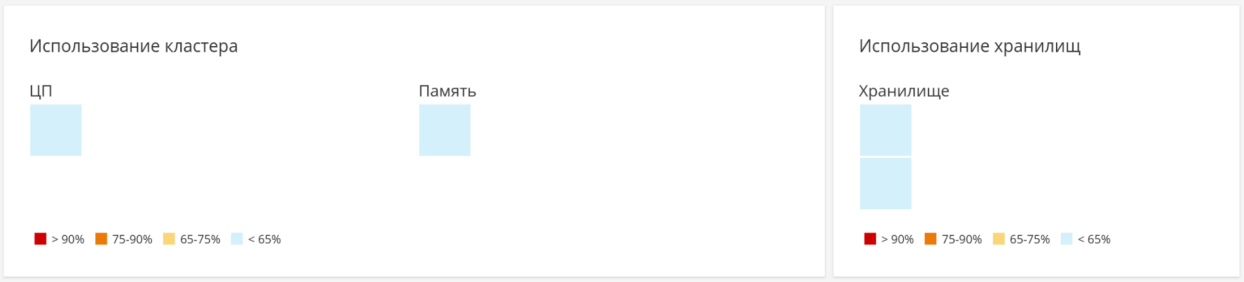


Рисунок 56 – Общее использование ресурсов кластера

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 объем использования для графиков памяти и хранилища.

2.2.3.1 Наиболее используемые ресурсы

При нажатии на круговой график раздела "Общее использование" (рисунок 55) в разделе общего использования панели мониторинга можно посмотреть список наиболее используемых ресурсов ЦП (рисунок 57), памяти (рисунок 58) или хранилища (рисунок 59).

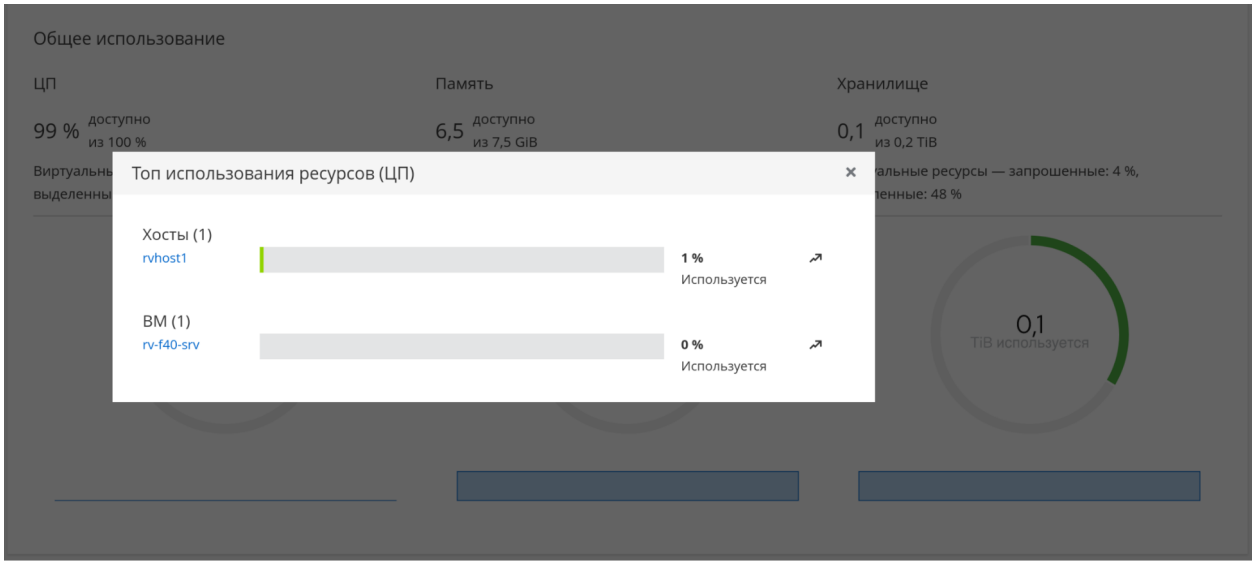


Рисунок 57 – Наиболее используемые ресурсы (ЦП)

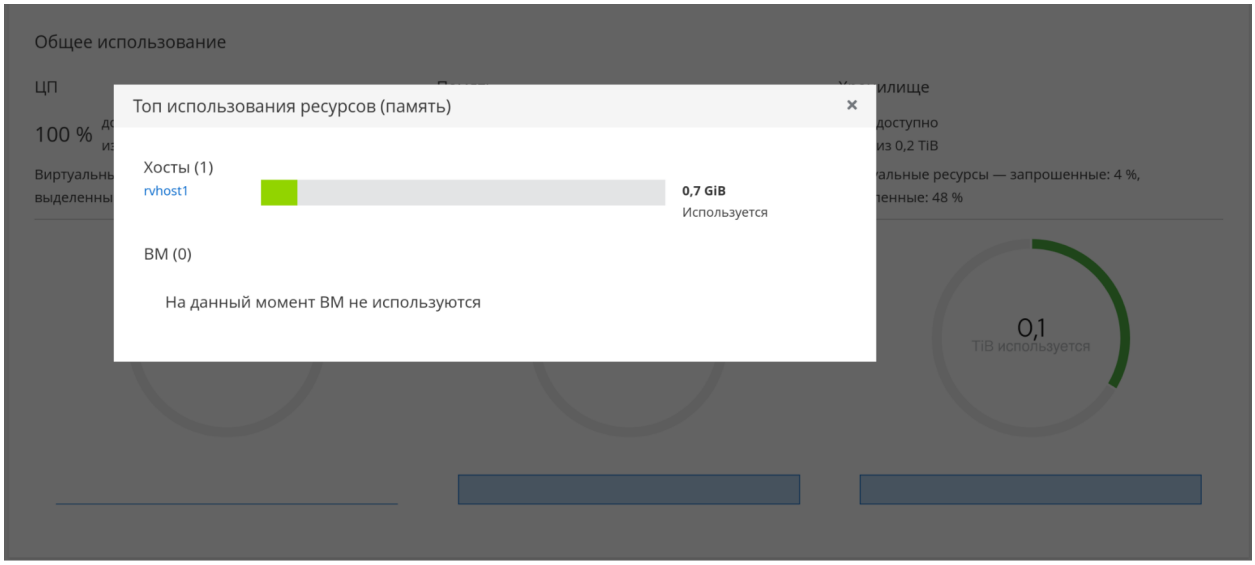


Рисунок 58 – Топ использования ресурсов (память)

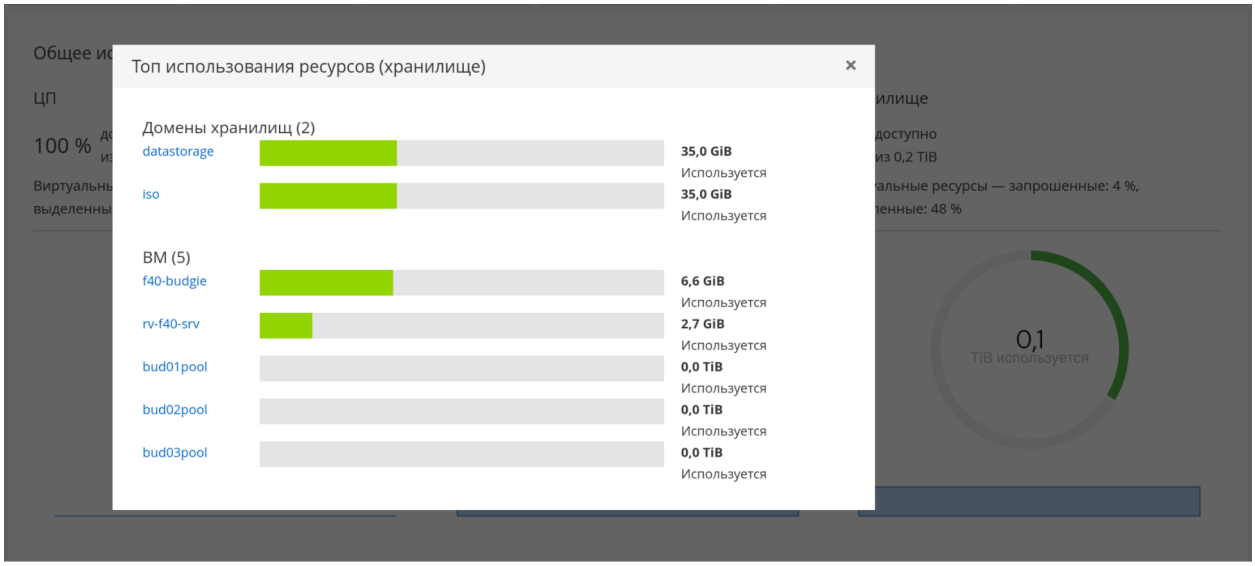


Рисунок 59 – Топ использования ресурсов (хранилище)

Для ЦП и памяти всплывающий список показывает десять хостов и ВМ с наиболее высоким потреблением.

Для хранилища всплывающий список показывает десять наиболее используемых доменов хранилищ и ВМ.

Стрелка справа от панели использования показывает тенденции потребления этого ресурса за последнюю минуту.

2.2.4 Использование кластера

В разделе "Использование кластера" (рисунок 60) на тепловой карте отображается использование ЦП и памяти.

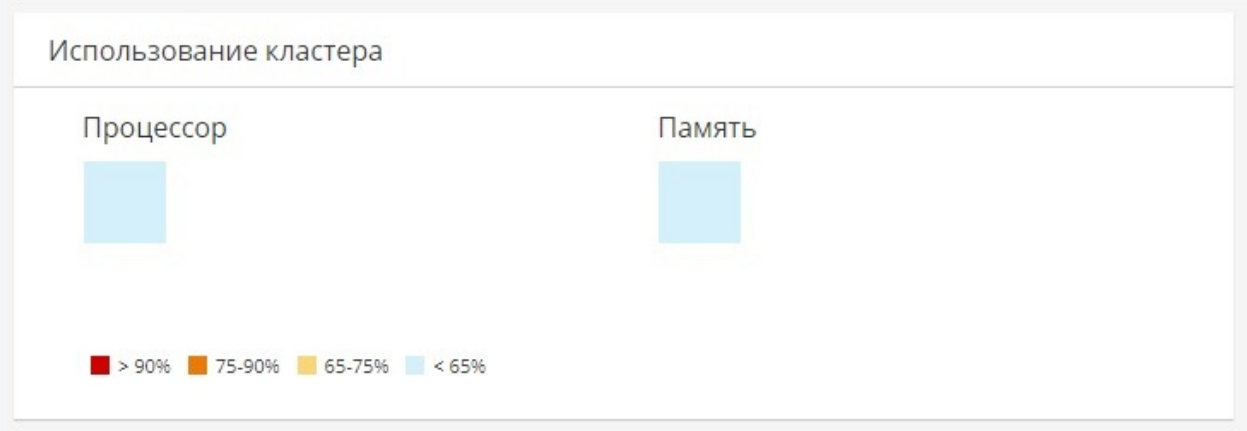


Рисунок 60 – Использование кластера

2.2.4.1 Использование ЦП

Тепловая карта использования ЦП конкретного кластера показывает средний процент использования ЦП за последние 24 часа. При наведении курсора на тепловую карту показывается название кластера. При нажатии на тепловую карту происходит переход в меню "Ресурсы → Хосты" с результатами поиска по конкретному кластеру с фильтром использования ЦП. Расчеты для нахождения общего среднего использования ЦП на кластер проводятся с использованием среднего процента нагрузки ЦП для каждого хоста за последние 24 часа.

2.2.4.2 Использование памяти

Тепловая карта использования памяти конкретного кластера показывает средний процент использования памяти за последние 24 часа. При наведении курсора на тепловую карту показывается название кластера. При нажатии на тепловую карту происходит переход в меню "Ресурсы → Хосты" с

результатами поиска по конкретному кластеру с фильтром использования памяти. Расчеты для нахождения общего среднего использования памяти на кластер в ГБ проводятся с использованием среднего процента нагрузки памяти для каждого хоста за последние 24 часа.

2.2.5 Использование хранилищ

В разделе "Использование хранилищ" (рисунок 61) на тепловой карте показывается процент использования хранилища.



Рисунок 61 – Использование хранилищ

Тепловая карта показывает средний процент использования хранилища за последние 24 часа. Расчеты для нахождения общего среднего использования хранилища кластером проводятся с использованием среднего процента использования хранилища для каждого хоста за последние 24 часа. При наведении курсора на тепловую карту показывается название домена хранилища. При нажатии на тепловую карту происходит переход в меню "Хранилище → Домены" с доменами хранилищ, отсортированными по проценту использования.

2.3 Поиск

2.3.1 Операции поиска

Портал администрирования предоставляет возможность управления тысячами ресурсов, такими как виртуальные машины, хосты, пользователи и многие другие. Чтобы выполнить поиск, введят 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.

2.3.2 Примеры поиска и поисковый синтаксис

Поисковые запросы по ресурсам Системы виртуализации имеют следующий синтаксис:

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

В таблице 16 показаны примеры использования поисковых запросов, приведенные для понимания того, как выполняется помощь в построении поисковых запросов в Системе виртуализации.

Таблица 16 – Примеры поисковых запросов

Пример	Результат
Hosts: Vms.status = up page 2	Показывает вторую страницу 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 серьезностью выше нормальной и с сортировкой по времени

2.3.3 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, затем ввести или выбрать следующую часть поискового запроса, либо продолжить вводить запрос вручную.

В таблице 17 приводятся конкретные примеры того, как автодополнение помогает в составлении следующего поискового запроса: "Hosts: Vms.status = down".

Таблица 17 – 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"
Hosts: Vms.status	"=" "!="	Выбрать или ввести "="
Hosts: Vms.status =	Все значения статуса	Выбрать или ввести "down"

2.3.4 Типы результатов поиска

Тип результата дает 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.

2.3.5 Критерии поиска

Критерии поиска указываются в поиске после двоеточия.

Синтаксис критериев поиска {criteria} следующий:

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

В таблице 18 приведено описание составных частей синтаксиса и примеры критериев поиска:

Таблица 18 – Примеры критериев поиска

Часть	Описание	Значения	Пример	Примечание
prop	Свойство искомого ресурса. Также может быть свойством типа ресурса (obj-type) или меткой (tag)	Ограничить поиск объектами с определенными свойствами. Искать, 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	

Часть	Описание	Значения	Пример	Примечание
operator	Операторы сравнения	"=" "!=" (не равно) ">" "<" ">=" "<="		Параметры значений зависят от свойств
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

2.3.6 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", вводят "m*".

Поиск по двум критериям можно выполнитьс помощью двух логических операторов AND и OR. Например, следующий запрос вернет список всех выполняющихся ВМ пользователей, чьи имена пользователей начинаются с буквы "m":

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

Следующий запрос вернет список всех ВМ с меткой пользователей "paris-loc", 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 идет перед OR, а оператор OR идет перед предполагаемым AND.

2.3.7 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 важностью выше нормальной, отсортированные по времени (в обратном порядке):

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

2.3.8 Поиск дата-центров

В таблице 19 описываются все параметры поиска дата-центров.

Таблица 19 – 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
status	Список	Доступность дата-центра
sortby	Список	Сортирует возвращенные 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
```

2.3.9 Поиск кластеров

В таблице 20 описываются все параметры поиска кластеров.

Таблица 20 – 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	True или False для статуса кластера
sortby	Список	Сортирует возвращенные 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
```

2.3.10 Поиск хостов

В таблице 21 описываются все параметры поиска хостов.

Таблица 21 – 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
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	Объем доступной памяти
cpu_speed	Целое число	Вычислительная скорость ЦП
cpu_model	Строка	Тип ЦП

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
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 возвращенные результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

2.3.11 Поиск сетей

В таблице 22 описываются все параметры поиска сетей.

Таблица 22 – 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

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
stp	Строка	Включен или отключен 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 возвращенные результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

2.3.12 Поиск хранилищ

В таблице 23 описываются все параметры поиска хранилищ.

Таблица 23 – 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

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
datacenter	Строка	Дата-центр, которому принадлежит хранилище
type	Строка	Тип хранилища
size	Целое число	Размер хранилища
used	Целое число	Используемый объем хранилища
committed	Целое число	Выделенный объем хранилища
sortby	Список	Сортирует возвращенные результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

Например, следующий запрос возвращает список хранилищ, общий объем которых больше 200 ГБ или с используемым объемом меньше 50 ГБ:

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

2.3.13 Поиск дисков

В таблице 24 описываются параметры поиска дисков.

Примечание — Для уменьшения отображаемого числа виртуальных дисков использовать параметры фильтрации "Disk Type" и "Content Type".

Таблица 24 – 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

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
		описанием диска, при желании добавляемые при создании диска
provisioned_size	Целое число	Виртуальный размер диска
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 присоединен диск
vm_names	Строка	Имена ВМ, к которым присоединен диск
quota	Строка	Имя квоты, принудительно применяющейся к виртуальному диску
sortby	Список	Сортирует возвращенные результаты согласно одному из свойств ресурса

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

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

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

2.3.14 Поиск томов

В таблице 25 описываются параметры поиска томов.

Таблица 25 – 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: распределенный ("distribute"), реплицированный ("replicate"), распределенный реплицированный ("distributed_replicate"), чередующийся ("stripe"), распределенный чередующийся ("distributed_stripe")
transport_type	Целое число	Принимаемые значения: TCP, RDMA

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
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 возвращенные 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
```

2.3.15 Поиск виртуальных машин

В таблице 26 описываются параметры поиска ВМ.

Поиск ВМ осуществляется в форме "Ресурсы → Виртуальные машины" (рисунок 62).

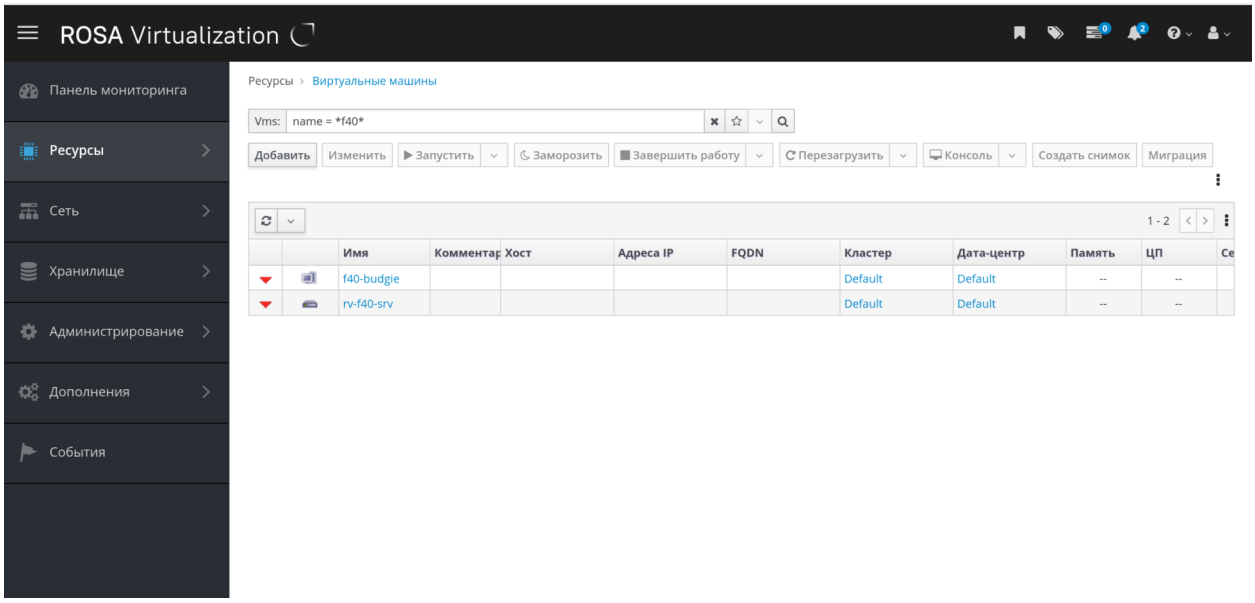


Рисунок 62 – Поиск ВМ по шаблону имени

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

Таблица 26 – 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

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
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
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

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
description	Строка	Ключевые слова или текст с описанием диска, при желании добавляемые при создании ВМ
sortby	Список	Сортирует возвращенные 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 = ""
```

2.3.16 Поиск пулов

В таблице 27 описываются параметры поиска пулов.

Таблица 27 – 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 возвращенные 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
```

2.3.17 Поиск шаблонов

В таблице 28 описываются параметры поиска шаблонов.

Таблица 28 – 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
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 возвращенные результаты согласно одному из свойств ресурса

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
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 серьезности, и эти машины выполняются:

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

2.3.18 Поиск пользователей

В таблице 29 описываются параметры поиска пользователей.

Поиск пользователей осуществляется в форме "Администрирование → Пользователи" (рисунок 63).

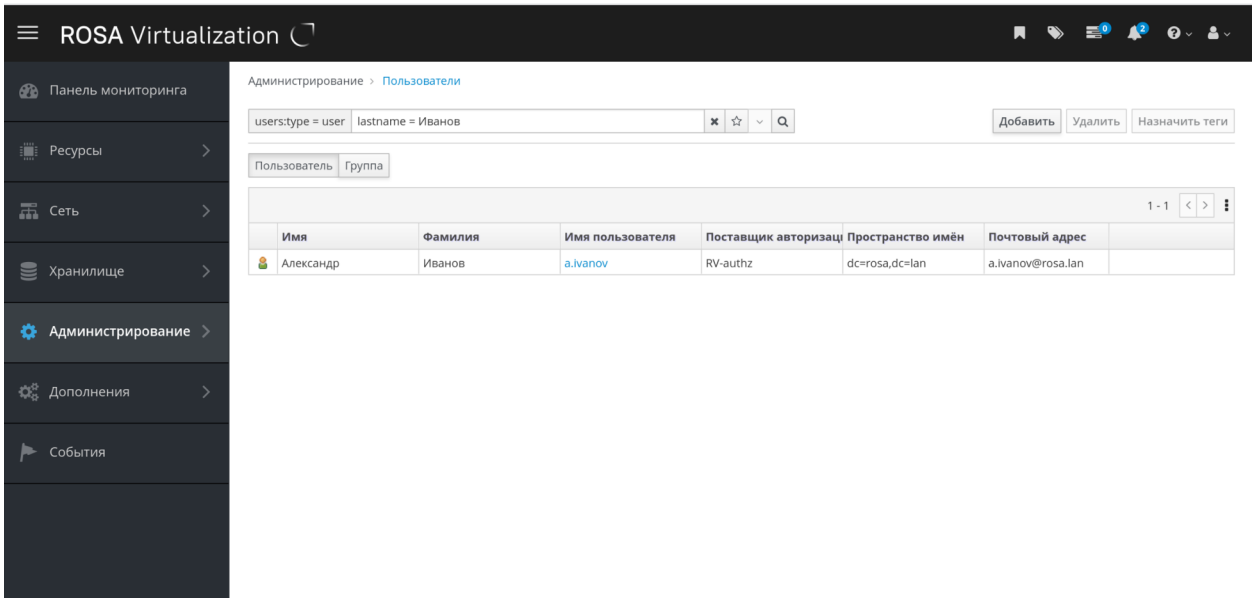


Рисунок 63 – Поиск всех пользователей с фамилией Иванов

Таблица 29 – 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

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
title	Строка	Должность пользователя
status	Строка	Статус пользователя
role	Строка	Роль пользователя
tag	Строка	Метка пользователя
pool	Строка	Пул пользователя
sortby	Список	Сортирует возвращенные 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 серьезности, и эти машины выполняются или приостановлены:

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

2.3.19 Поиск событий

В таблице 30 описываются все параметры, которые можно использовать для поиска событий. Для многих параметров предлагается автодополнение (в зависимости от параметров).

Таблица 30 – 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 серьезности 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 возвращенные 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
```

Следующий запрос возвращает список событий, которые произошли на ВМ с именем rv-f40-srv (рисунок 64):

```
Events:  Vms.name = rv-f40-srv
```

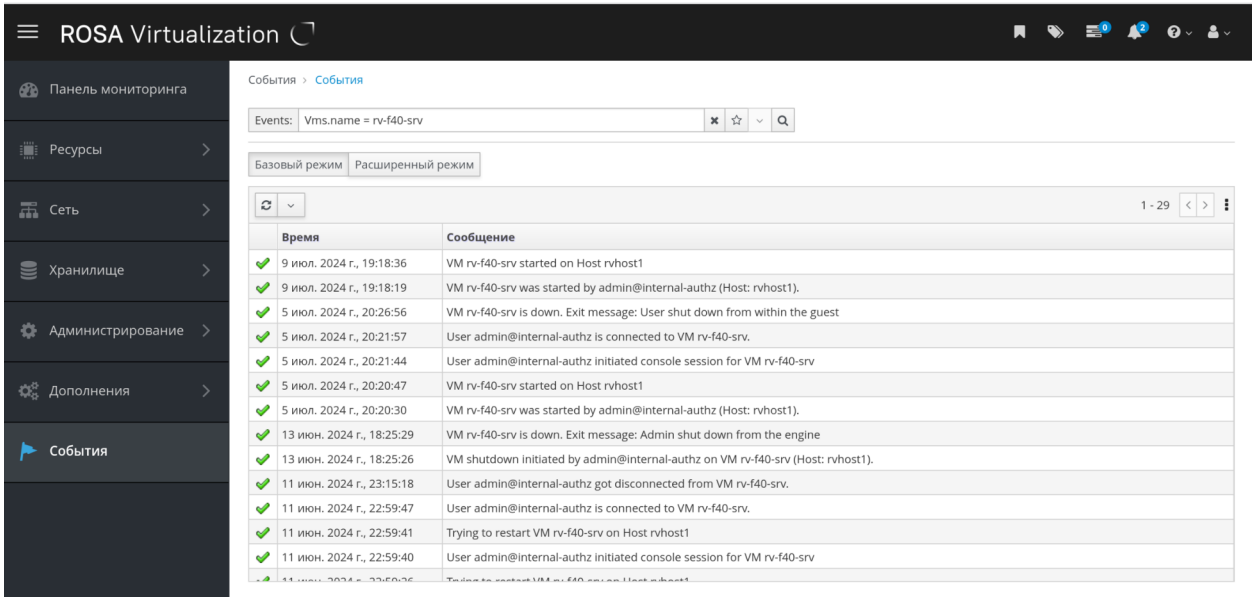


Рисунок 64 – Список событий, которые произошли на ВМ с именем rv-f40-srv

2.4 Закладки

2.4.1 Сохранение строки поискового запроса в виде закладки

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

Для сохранения поискового запроса в виде закладки нужно:

а) ввести нужный поисковый запрос в строку поиска и запустить поиск;

б) нажать на пиктограмму ☆ справа от строки поиска, чтобы открыть окно "Новая закладка" (рисунок 65);

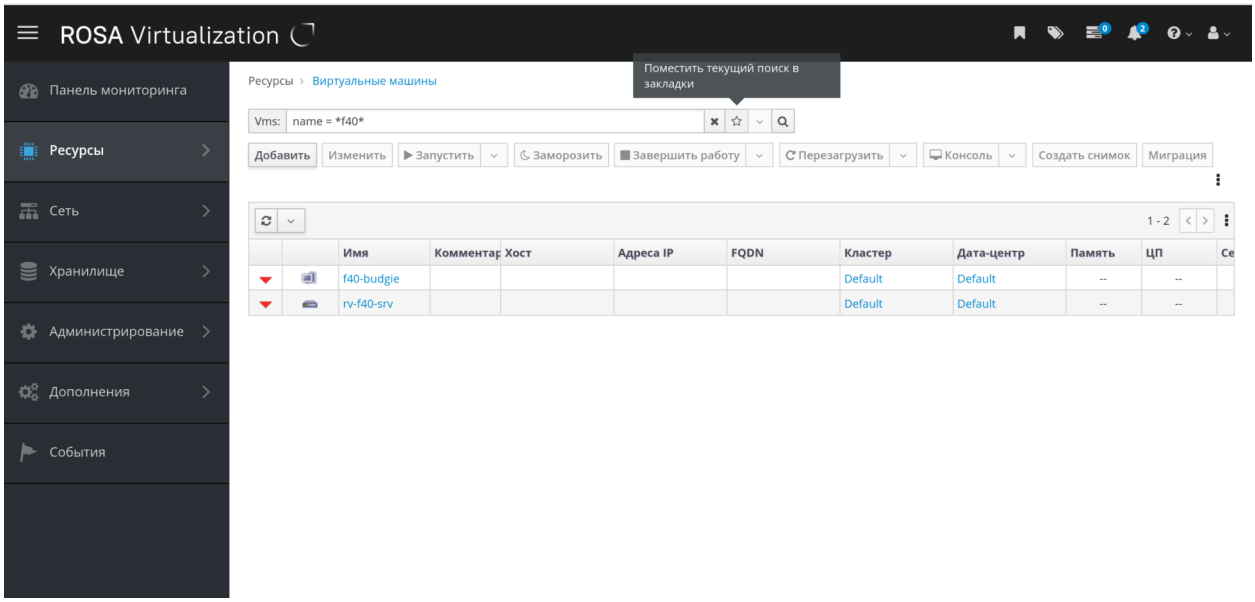


Рисунок 65 – Добавление закладки

в) ввести "Имя" закладки в форме "Новая закладка" (рисунок 66);

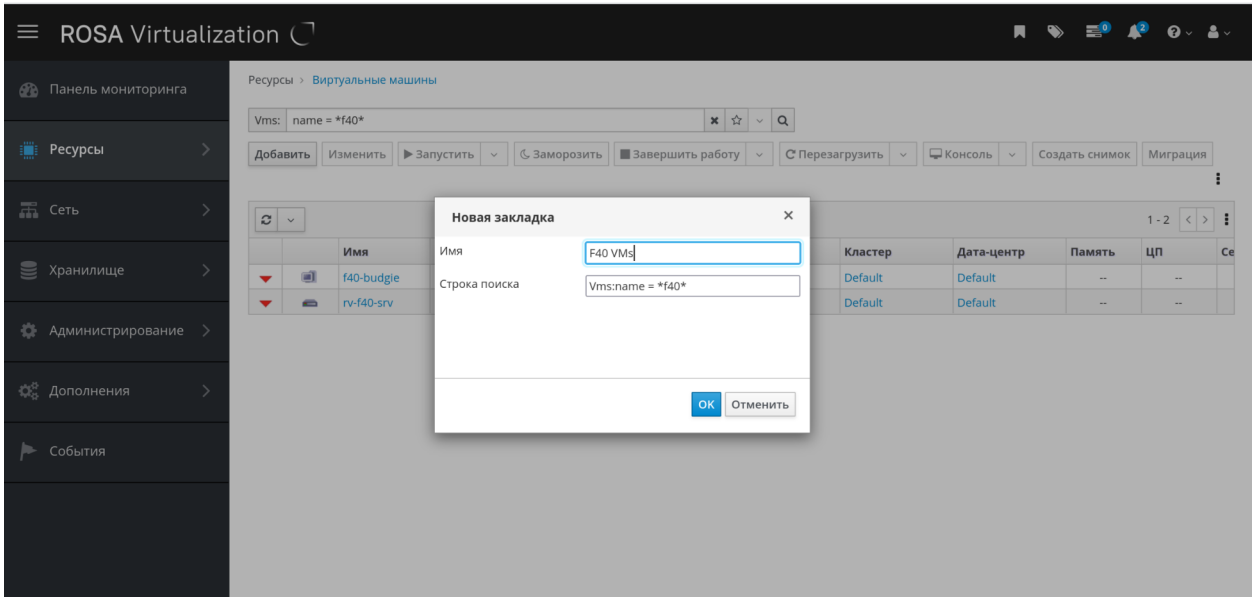
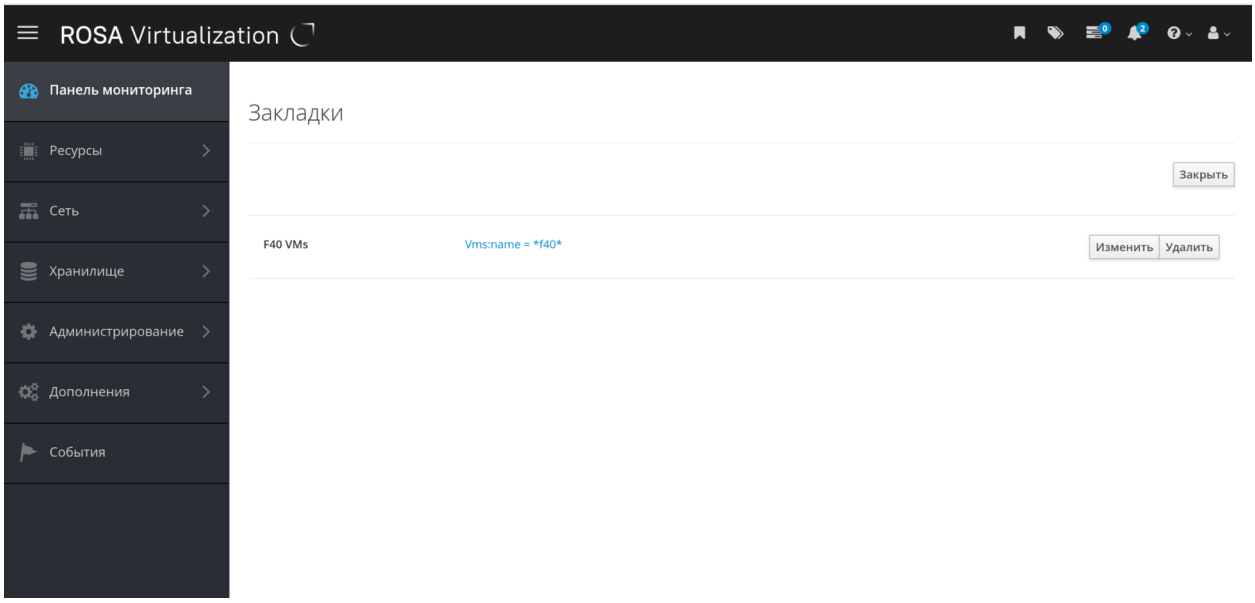


Рисунок 66 – Форма "Новая закладка" для добавления закладки

г) при необходимости изменить поле "Строка поиска";

д) нажать кнопку `OK` для добавления закладки или кнопку `Отменить` для отмены (рисунок 68).

Чтобы найти и выбрать закладку, следует нажать на пиктограмму ("Закладки") на панели заголовков (рисунок 67).



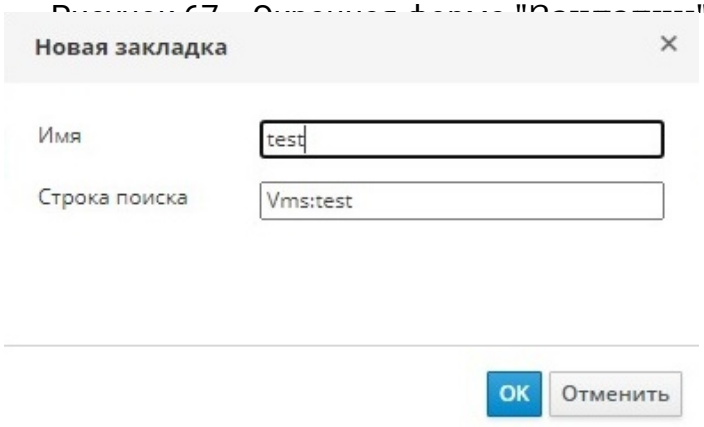


Рисунок 68 – Создание закладки

2.4.2 Редактирование закладок

Название и строку поиска закладок можно изменять.

Для редактирования закладок требуется :

а) нажать на пиктограмму ("Закладки") на панели заголовков;
б) выбрать закладку (рисунок 69) и нажать кнопку Изменить;

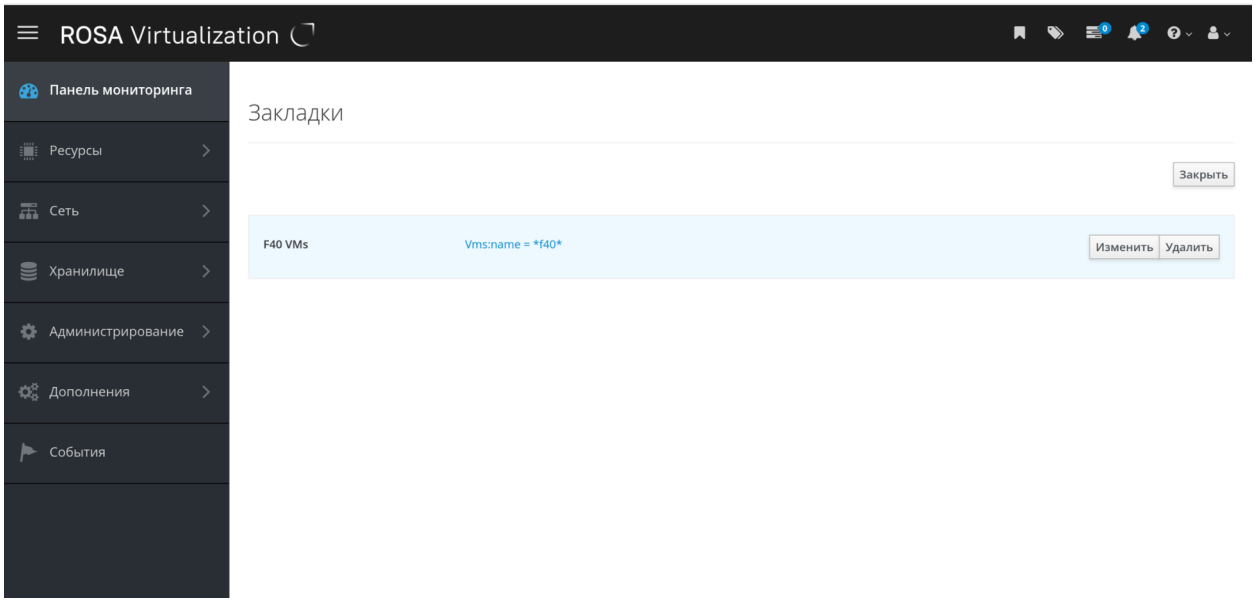


Рисунок 69 – Выбор закладки в форме "Закладки"

в) внести необходимые изменения в поля "Имя" и "Строка поиска" (рисунок 70);

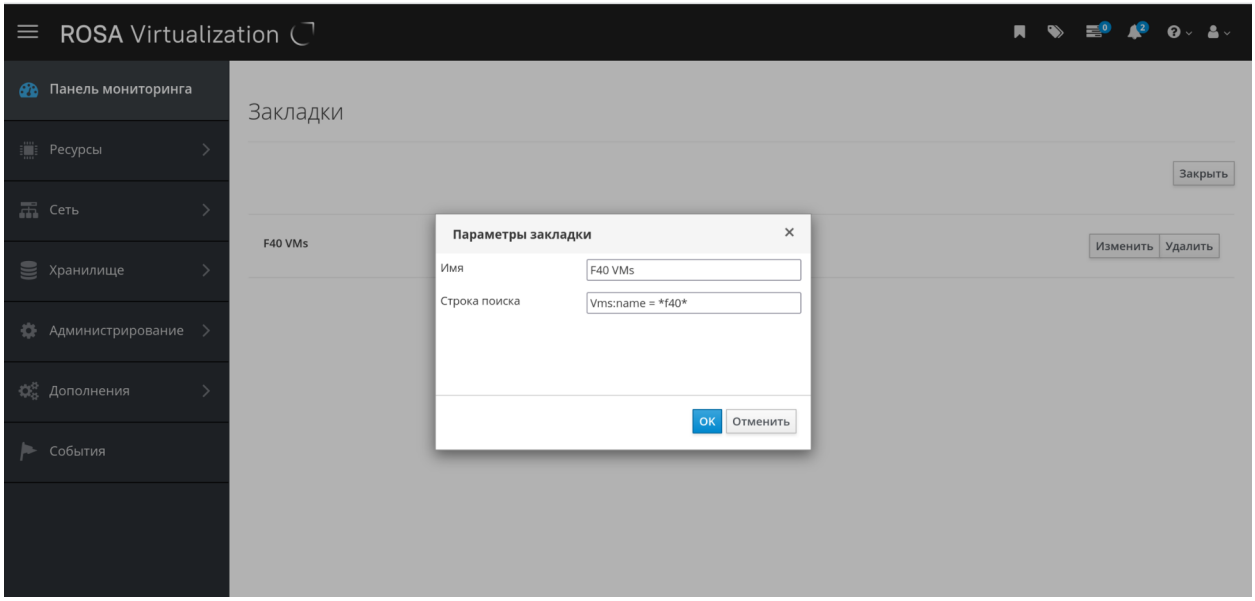


Рисунок 70 – Внесение изменений в закладку

г) нажать кнопку `OK` для сохранения изменений или кнопку `Отменить` для отмены.

2.4.3 Удаление закладок

Если закладка больше не нужна, ее можно удалить.

Для удаления закладок требуется:

а) нажать на значок  ("Закладки") на панели заголовков;

б) выбрать закладку (рисунок 69) и нажать кнопку Удалить;

в) в окне подтверждения удаления закладки (рисунок 71) опционально указать причину удаления в поле "Причина";

г) нажать кнопку OK для сохранения изменений или кнопку Отменить для отмены.

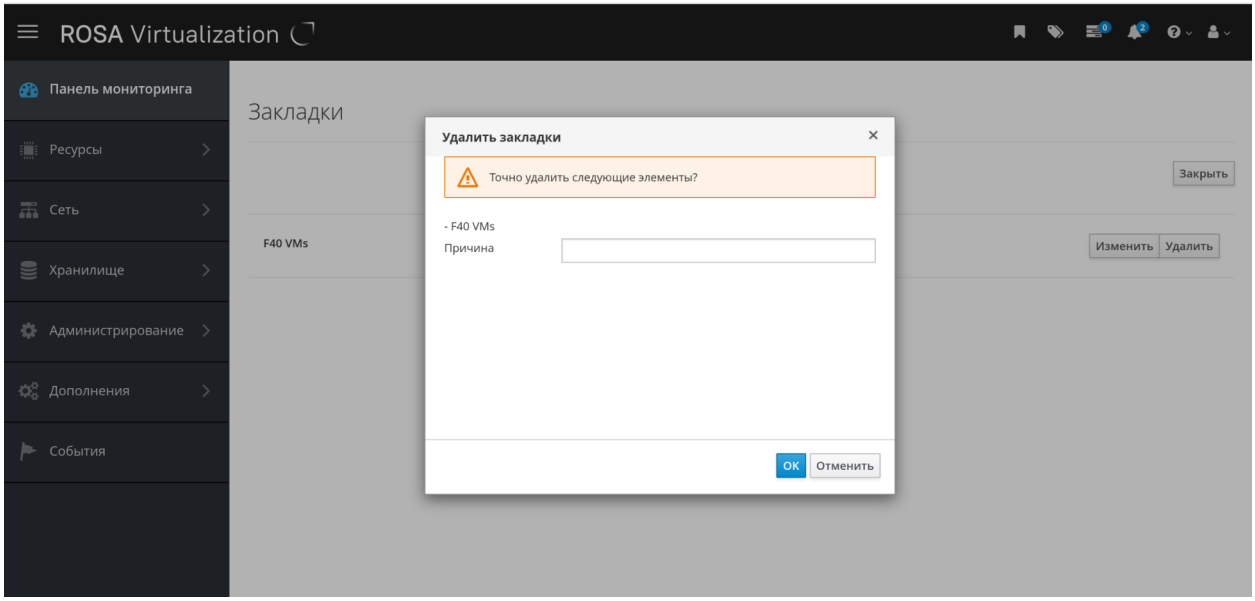


Рисунок 71 – Окно подтверждения удаления закладки

2.5 Теги

2.5.1 Настройка взаимодействия с помощью тегов

После установки и настройки параметров рабочий процесс взаимодействия с РОСА Виртуализация 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 выполнение поиска, используя теги в качестве поисковых запросов. Теги можно сортировать согласно иерархии, соответствующей структуре, а также согласно производственным требованиям.

Чтобы создать, изменить или удалить тег требуется нажать на пиктограмму ("Теги") на панели заголовков Портала администрирования.

2.5.2 Создание тегов

Для создания тега нужно выполнить следующие действия:

а) нажать на пиктограмму ("Теги")на панели заголовков;

б) нажать кнопку Добавить для добавления нового тега или выбрать тег и нажать кнопку Новый для создания подчиненного тега (рисунок 72);

в) указать "Имя" и "Описание" нового тега;

г) нажать кнопку OK.

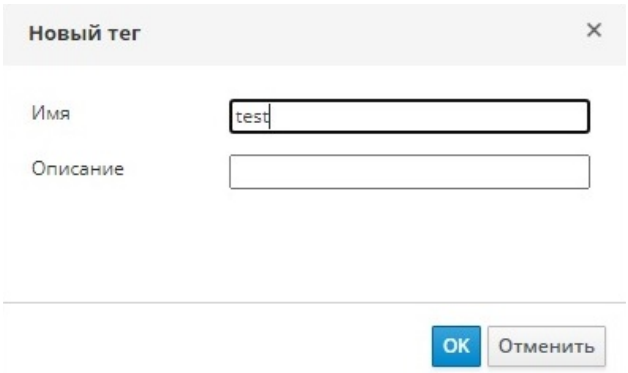


Рисунок 72 – Создание тега

2.5.3 Редактирование тегов

Название и описание тегов можно изменять.

Для редактирования тега требуется:

а) нажать на пиктограмму ("Теги") на панели заголовков;

б) выбрать тег, который нужно изменить, и нажать кнопку Изменить;
в) при необходимости внести изменения в поля "Имя" и "Описание";
г) нажать кнопку OK.

2.5.4 Удаление тега

Для удаления тега нужно:

а) нажать на пиктограмму  ("Теги") на панели заголовков;
б) выбрать тег, который нужно удалить, и нажать кнопку Удалить;
в) при появлении окна с предупреждением (рисунок 73) о том, что удаление метки (тега) также удалит все подчиненные метки, нажать кнопку OK для подтверждения или Отмена — для отмены.

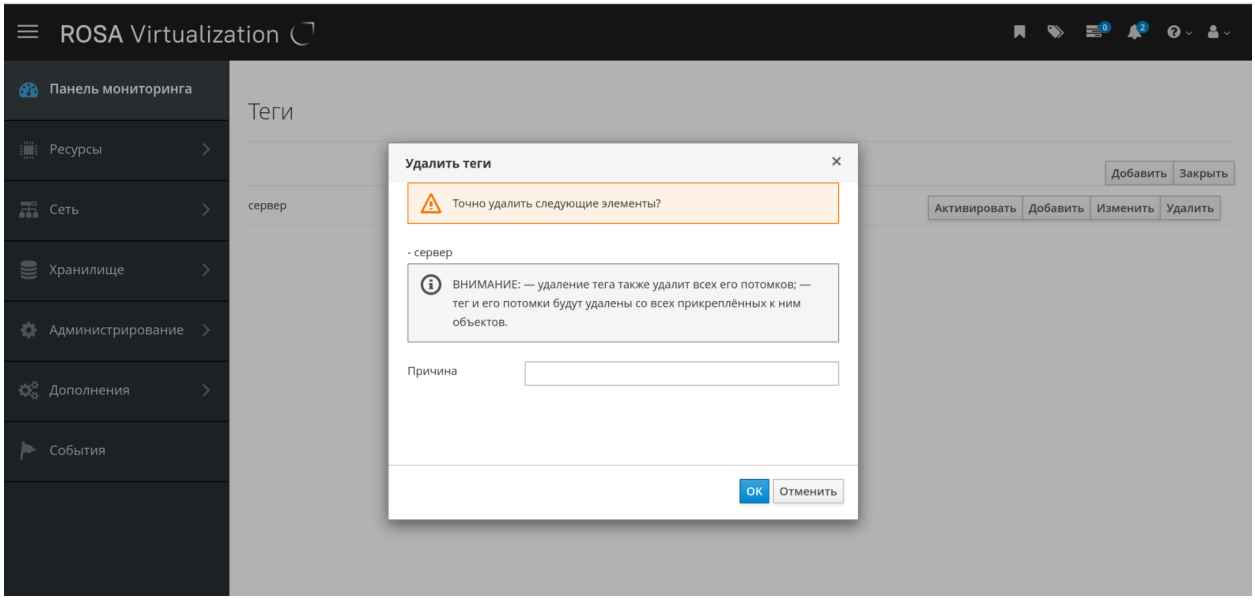


Рисунок 73 – Форма подтверждения удаления тега

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

2.5.5 Присвоение тегов объектам и снятие меток с объектов

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

Для присвоения тегов объектам и снятие тегов с объектов нужно выполнить следующие действия:

а) выбрать объекты, которым нужно присвоить тег или с которых нужно снять тег;

б) нажать пиктограмму ⋮ ("Больше действий"), а затем нажать кнопку `Назначить теги` (рисунок 74);

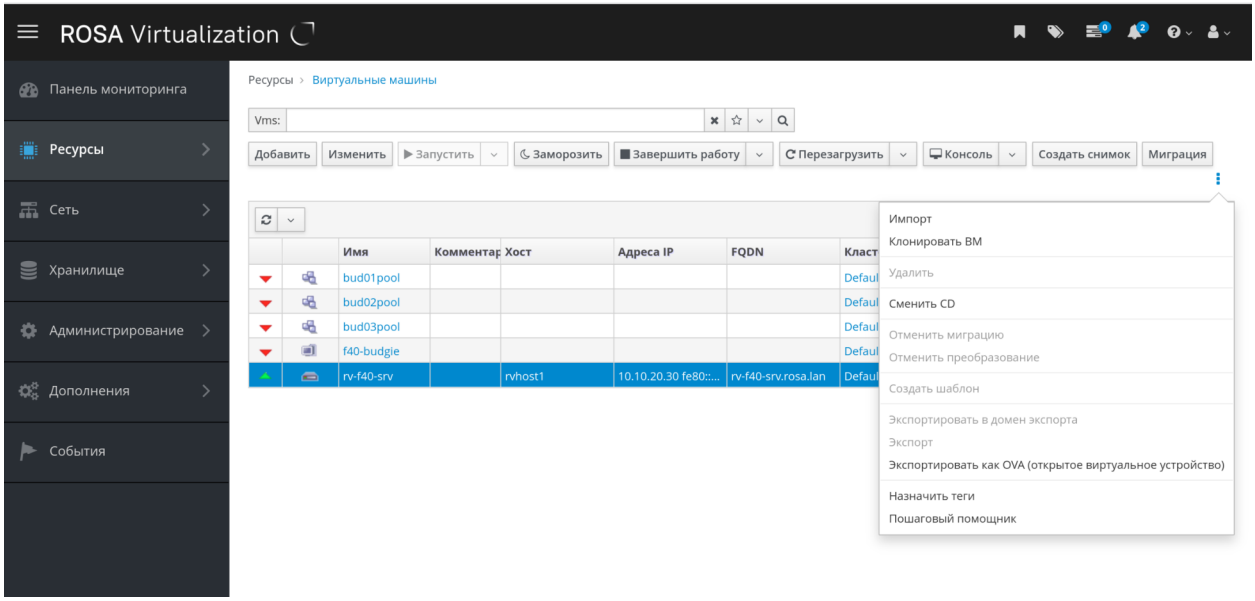


Рисунок 74 – Назначение тега виртуальной машине

в) установить соответствующий флажок, чтобы присвоить тег объекту (рисунок 75), или снять флажок, чтобы удалить тег объекта;

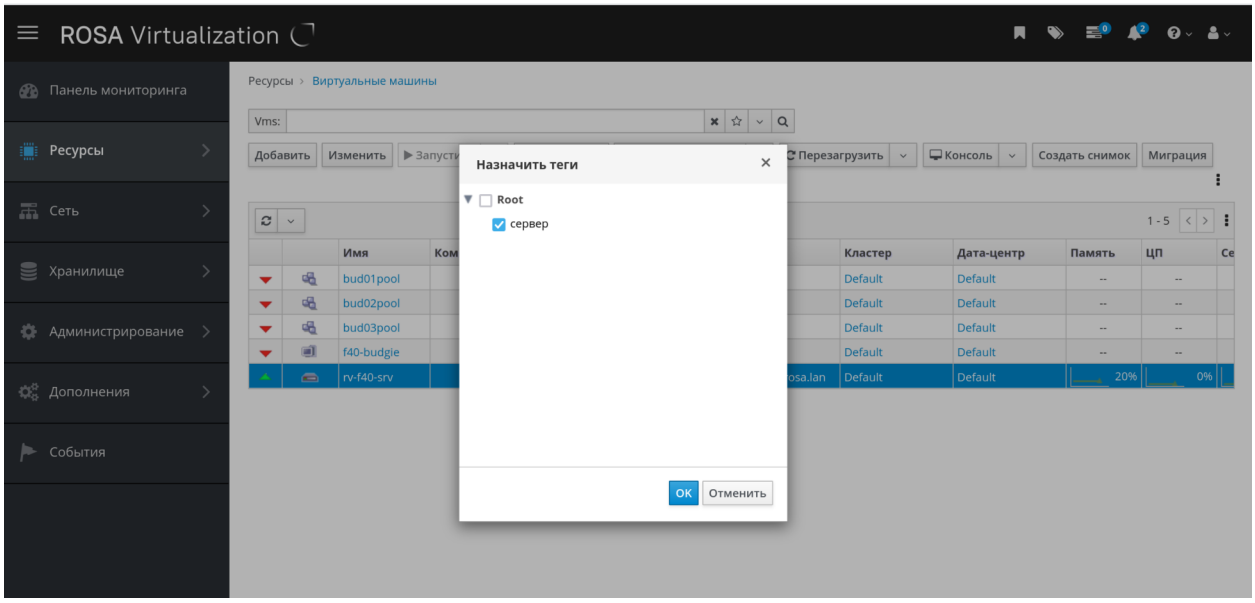


Рисунок 75 – Выбор тега и присвоение его объекту

г) нажать кнопку OK.

В результате указанные теги будут присвоены объектам в виде настраиваемого пользователем свойства (рисунок 76) или удалены.

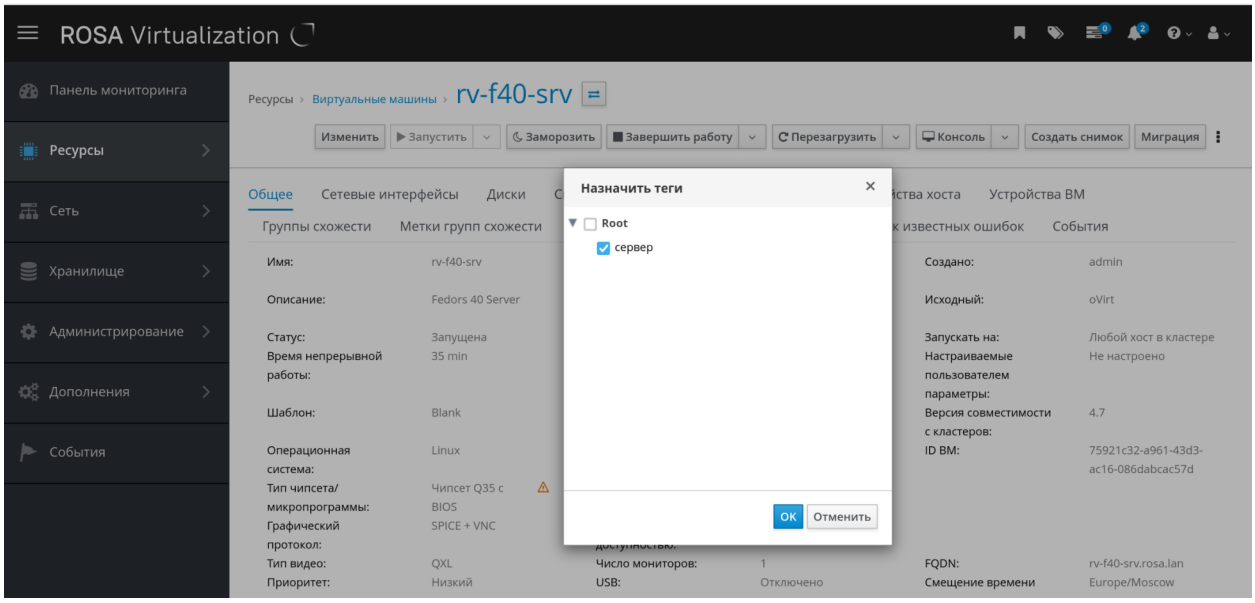


Рисунок 76 – ВМ с присвоенным ей тегом "сервер"

2.5.6 Поиск объектов на основе тегов

Для поиска объектов на основе тегов нужно ввести поисковый запрос с учетом регистра, используя "tag" как свойство, и указать 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.

2.5.7 Сортировка хостов с помощью тегов

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

Для настройки тегов для хостов нужно:

а) перейти в "Ресурсы → Хосты" и выбрать хост;

б) нажать пиктограмму ⋮ ("Больше действий"), а затем нажать кнопку Присвоить тег;

в) установить флажки напротив необходимых тегов;

г) нажать кнопку OK.

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

3 АДМИНИСТРИРОВАНИЕ РЕСУРСОВ

3.1 Качество обслуживания

Система виртуализации РОСА Виртуализация дает 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.

3.1.1 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 дает 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, размещенных в том же домене хранилища.

3.1.1.1 Создание записи о качестве обслуживания хранилища

Для создания записи о качестве обслуживания хранилища нужно выполнить следующие действия:

а) выбрать "Ресурсы → Дата-центры";

б) нажать на название дата-центра (рисунок 77) для подробного просмотра;

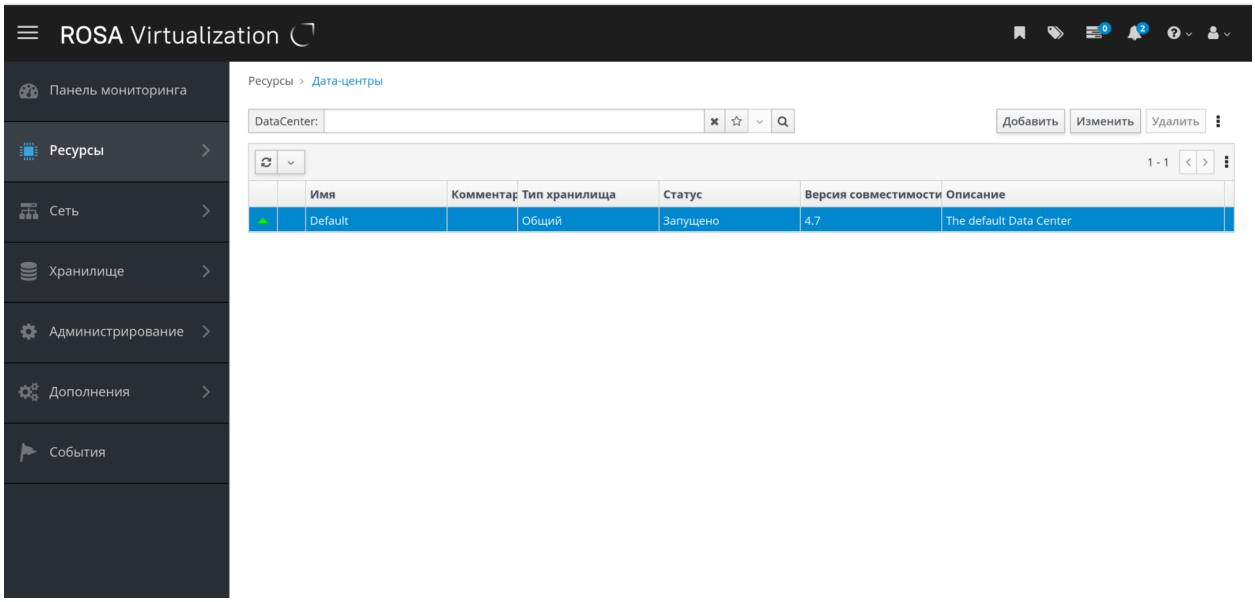


Рисунок 77 – Форма выбора доступных дата-центров

в) перейти на вкладку "QoS" (рисунок 78);

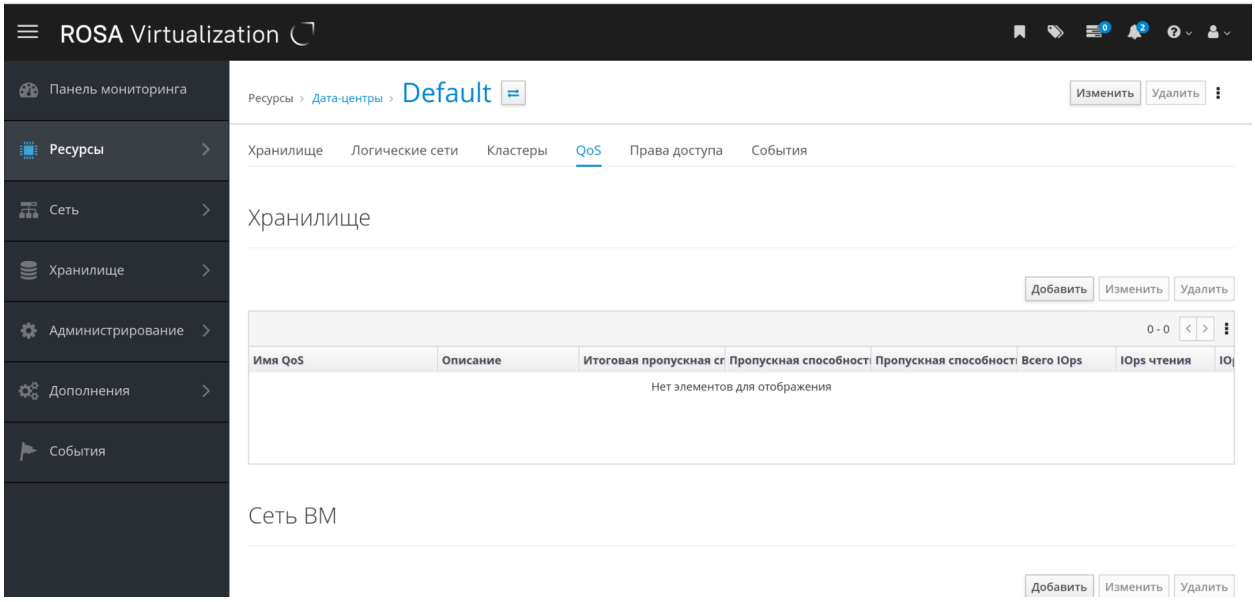


Рисунок 78 – Форма "Дата-центры" — вкладка "QoS"

г) в секции "Хранилище" нажать кнопку Добавить;

д) указать "Имя QoS" и "Описание" (рисунок 79) для новой записи качества обслуживания;

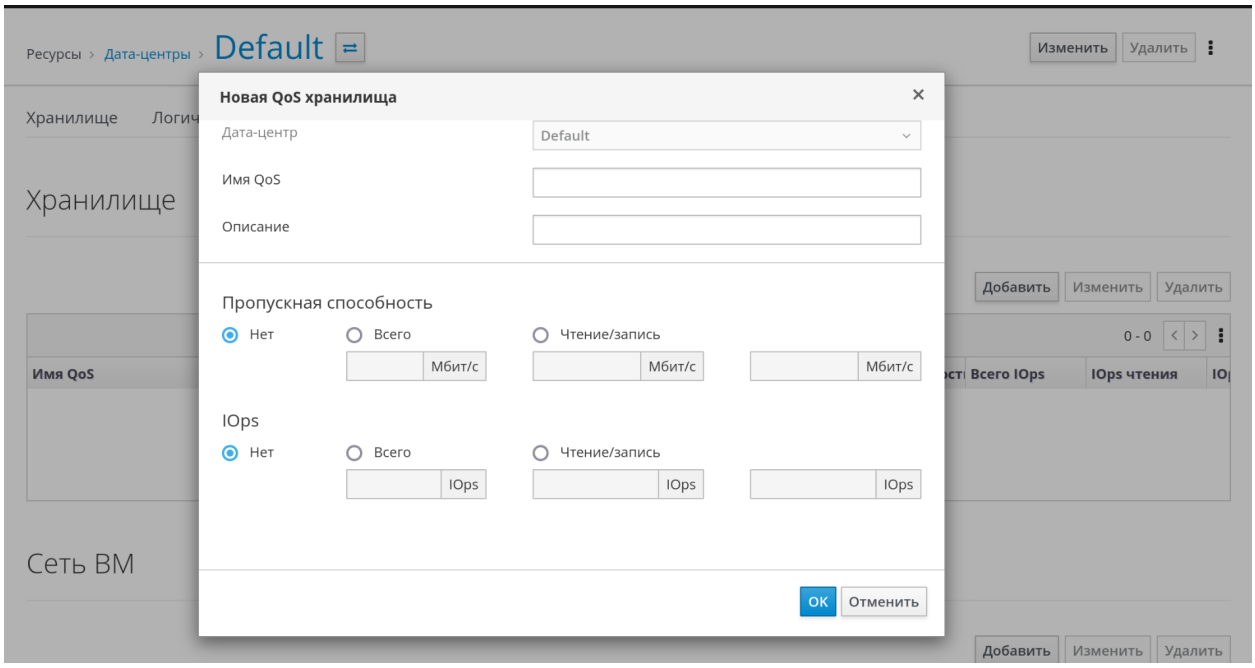


Рисунок 79 – Форма "Новая QoS хранилища"

е) указать "Пропускную способность" качества обслуживания, отметив один из переключателей:

– Нет;

– Всего – указать максимально разрешенную общую пропускную способность в поле "Мбит/сек";

– Чтение/запись – указать максимально разрешенную общую пропускную способность для операций чтения в левом поле "Мбит/сек" и максимально разрешенную общую пропускную способность для операций записи в правом поле "Мбит/сек";

ж) указать качество обслуживания ввода и вывода (IOps), отметив один из переключателей:

– Нет;

– Всего – указать максимальное разрешенное число операций ввода и вывода в секунду в поле IOps;

– Чтение/запись – указать максимальное разрешенное число операций ввода в секунду в левом поле IOps и максимальное разрешенное число операций вывода в секунду в правом поле Iops;

з) нажать кнопку OK.

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

3.1.1.2 Удаление записи о качестве обслуживания хранилища

Для удаления записи качества обслуживания хранилища нужно:

а) выбрать "Ресурсы → Дата-центры";
б) нажать на название дата-центра для подробного просмотра;
в) перейти на вкладку "QoS";
г) в секции "Хранилище" выбрать запись качества обслуживания этого хранилища и нажать кнопку Удалить;
д) нажать кнопку OK.

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

3.1.2 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.

3.1.2.1 Создание записи о качестве обслуживания сети ВМ

Для создания 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, нужно:

а) выбрать "Ресурсы → Дата-центры";
б) нажать на название дата-центра для подробного просмотра;
в) перейти на вкладку "QoS";
г) в секции "Сеть ВМ" нажать кнопку Добавить (рисунок 80);

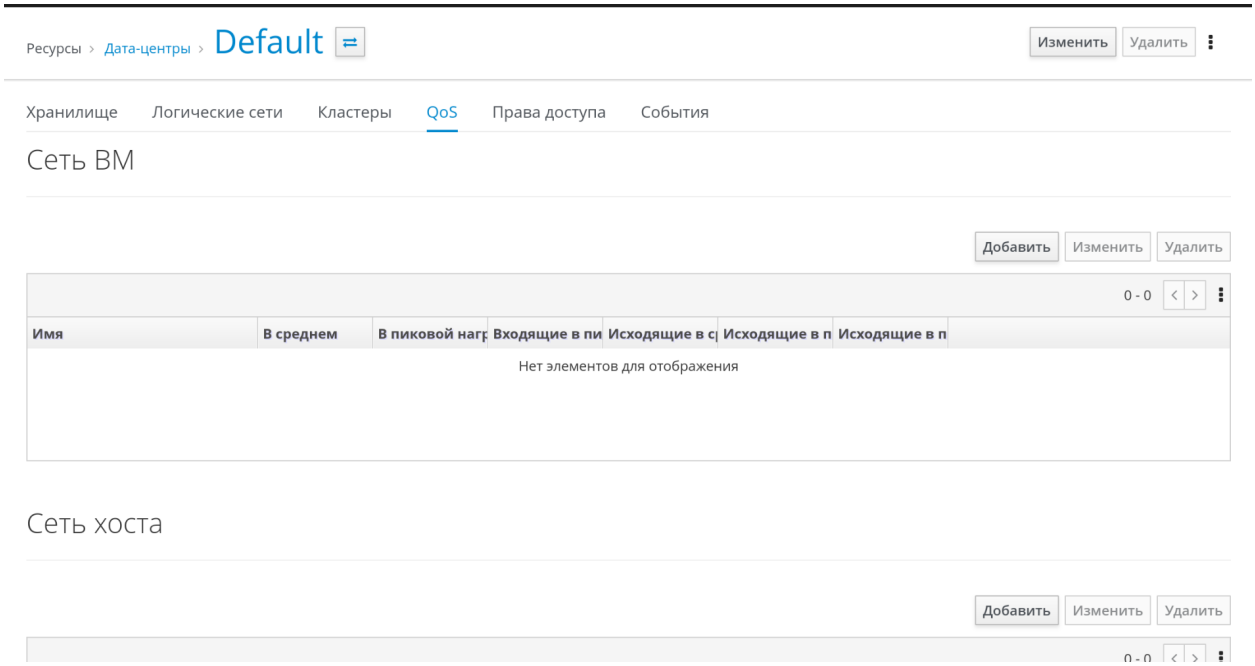


Рисунок 80 – Добавление QoS для "Сеть ВМ"

д) в окне "Новая QoS сети" ВМ ввести "Имя" записи QoS сети ВМ (рисунок 81);

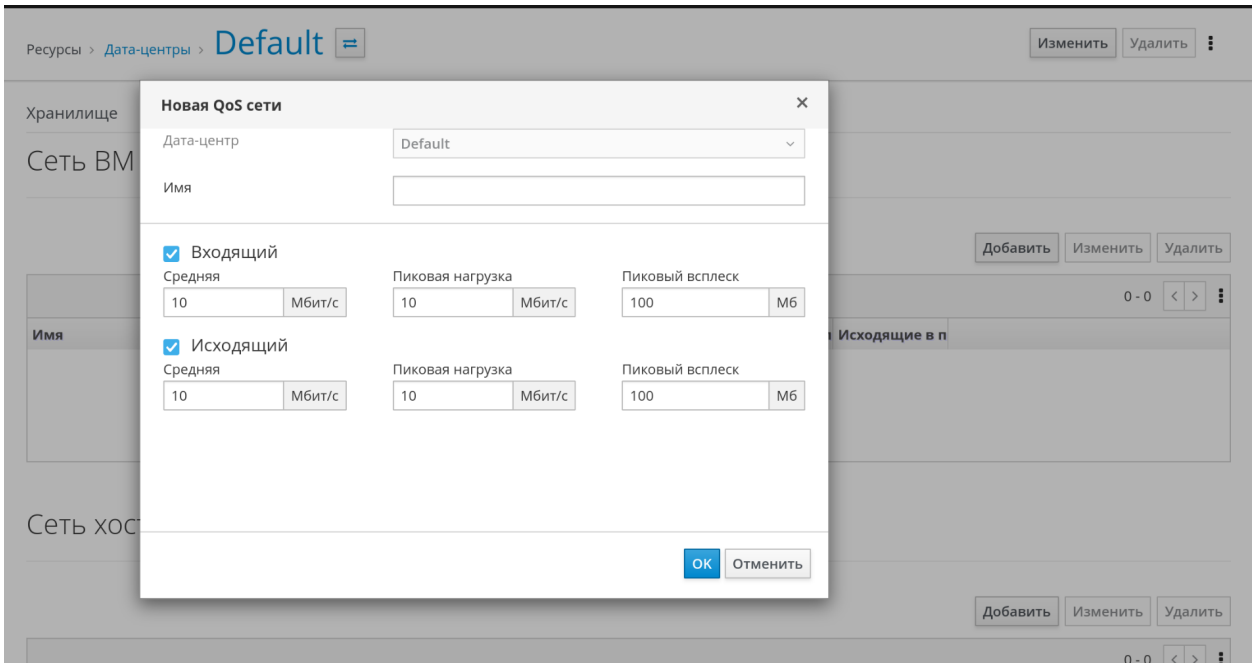


Рисунок 81 – Новая QoS сети

е) указать лимиты для "Входящего" и "Исходящего" сетевого трафика;

ж) нажать кнопку OK.

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

3.1.2.2 Параметры в окне "Новая QoS сети ВМ"

В таблице 31 описываются параметры качества обслуживания сети ВМ, которые предоставляют возможность настроить лимиты пропускной полосы как для входящего, так и для исходящего трафика на трех разных уровнях.

Таблица 31 – 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

Поле	Описание
Входящий	Параметры, применяемые к входящему трафику. Установить или снять 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. Установить или снять 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; – Пиковый всплеск – скорость исходящего трафика во время пиковых всплесков

Чтобы изменить максимальное значение, разрешаемое в полях "Средняя", "Пиковая нагрузка" или "Пиковый всплеск", можно использовать команду `engine-config` для изменения ключей конфигурации MaxAverageNetworkQoSValue, MaxPeakNetworkQoSValue или MaxBurstNetworkQoSValue, после чего для применения внесенных изменений необходимо перезапустить службу ovirt-engine:

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

3.1.2.3 Удаление записи о качестве обслуживания сети ВМ

Для удаления записи о качестве обслуживания сети ВМ требуется:

а) выбрать "Ресурсы → Дата-центры";
б) нажать на название дата-центра для подробного просмотра;
в) перейти на вкладку "QoS";
г) в секции "Сеть ВМ" выбрать запись QoS сети виртуальной машины и нажать кнопку `Удалить`;
д) нажать кнопку `OK`.

3.1.3 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.

3.1.3.1 Создание записи о качестве обслуживания для сетей хоста

Для создания записи о качестве обслуживания для сетей хоста нужно выполнить следующие действия:

а) выбрать "Ресурсы → Дата-центры";

б) нажать на название дата-центра для подробного просмотра;

в) перейти на вкладку "QoS";

г) в секции "Сеть хоста" нажать кнопку Добавить;

д) в окне "Новая QoS сети хоста" ввести "Имя QoS" и "Описание" для записи о качестве обслуживания (рисунок 82);

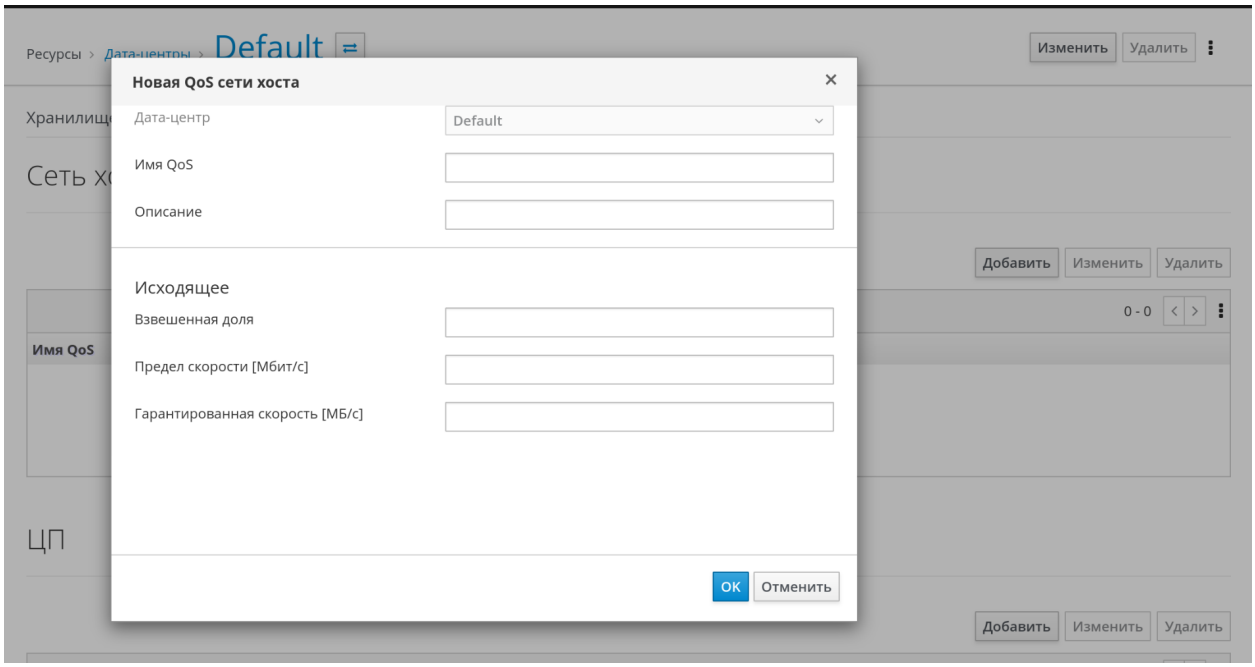


Рисунок 82 – Форма "Новая QoS сети хоста"

е) указать нужные значения "Взвешенной доли", "Предела скорости (Мбит/с)" и "Гарантированной скорости (МБ/с)";

ж) нажать кнопку OK.

3.1.3.2 Параметры в окне "Новая QoS сети хоста"

В таблице 32 описываются параметры QoS сетей хоста, которые предоставляют возможность настроить лимиты пропускной способности для исходящего трафика.

Таблица 32 – 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

Поле	Описание
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, разрешенное в полях "Предел скорости (Мбит/с)" и "Гарантированная скорость (МБ/с)", можно использовать команду `engine-config` для изменения ключа конфигурации MaxAverageNetworkQoSValue, после чего для применения внесенных изменений необходимо перезапустить службу ovirt-engine:

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

3.1.3.3 Удаление записи о качестве обслуживания для сетей хоста

Для удаления записи о качестве обслуживания для сетей хоста нужно:

а) выбрать"Ресурсы → Дата-центры";

б) нажать на название дата-центра для подробного просмотра;

в) перейти на вкладку "QoS";

г) в секции "Сеть хоста" выбрать запись о качестве обслуживания и нажать кнопку `Удалить`;

д) нажать кнопку `OK`.

3.1.4 Качество обслуживания ЦП

Качество обслуживания центрального процессора определяет максимальный объем вычислительной мощности хоста, к которому может получить доступ выполняющаяся на хосте ВМ. Максимальный объем вычислительной мощности хоста, доступный для ВМ, выражается в процентах 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.

3.1.4.1 Создание записи качества обслуживания для ЦП

Для создания записи качества обслуживания для центрального процессора нужно выполнить следующие действия:

а) выбрать "Ресурсы → Дата-центры";
б) нажать на название дата-центра для подробного просмотра;
в) перейти на вкладку "QoS";
г) в секции "ЦП" нажать кнопку Добавить (рисунок 83);

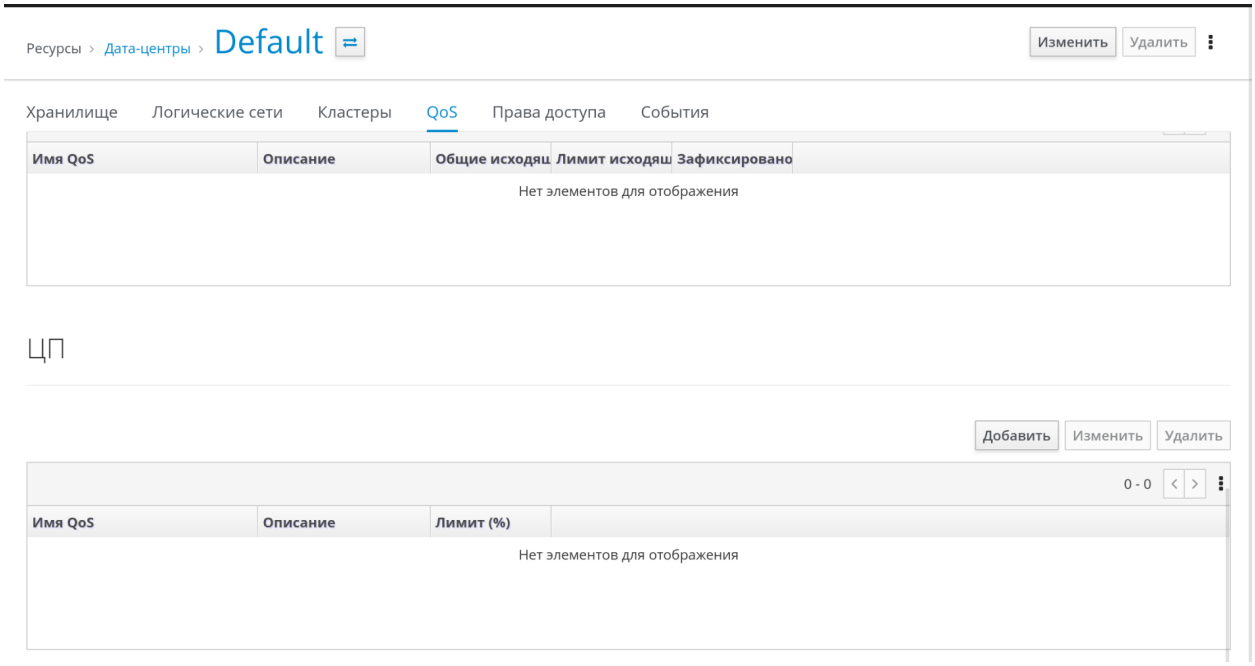


Рисунок 83 – Вкладка "QoS" – секция "ЦП"

д) в окне "Новая QoS ЦП" ввести "Имя QoS" и "Описание" для записи о качестве обслуживания (рисунок 84);

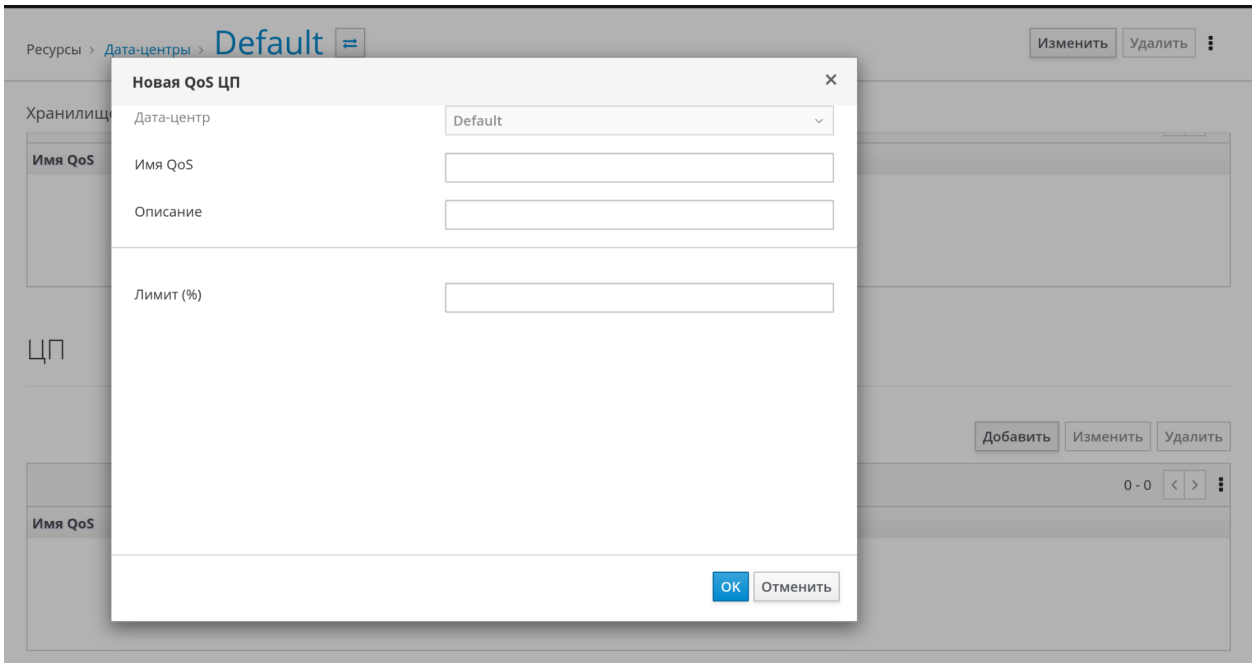


Рисунок 84 – Новая QoS ЦП

е) в поле "Лимит (%)" ввести максимальную вычислительную возможность, разрешаемую записью QoS (при этом не указывать символ "%");

ж) нажать кнопку 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.

3.1.4.2 Удаление записи качества обслуживания для ЦП

Для удаления записи QoS для центрального процессора требуется:

а) выбрать "Ресурсы → Дата-центры"$

б) нажать на название дата-центра для подробного просмотра;

в) перейти на вкладку "QoS";

г) в секции "ЦП" выбрать нужную запись QoS ЦП и нажать кнопку Удалить;

д) нажать кнопку OK.

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

3.2 Дата-центры

3.2.1 Введение

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 РОСА Виртуализация может находиться несколько дата-центров, при этом инфраструктура дата-центров позволяет управлять ими отдельно друг от друга (рисунок 85).

Все дата-центры управляются средствами одного Портала администрирования.

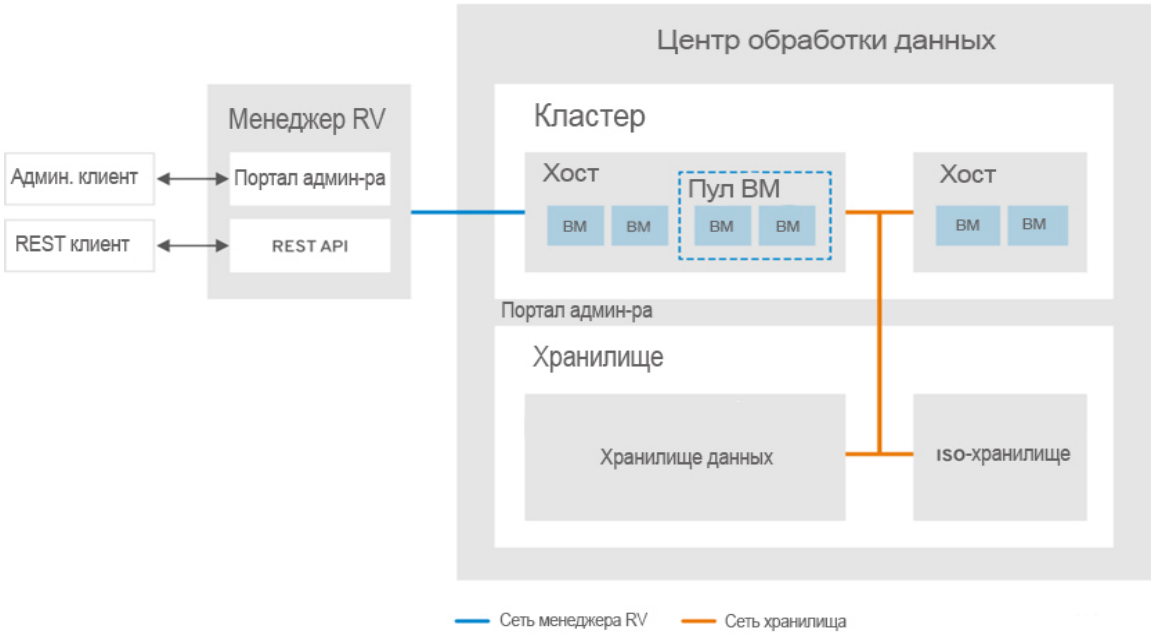


Рисунок 85 – Дата-центры

В процессе установки РОСА Виртуализация создает дата-центр по умолчанию. После установки Системы можно настроить дата-центр по умолчанию или создать новые дата-центры.

3.2.2 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. Управление 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. Такое управление – 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 передает роль SPM другому хосту. При запуске диспетчера пула хранилища виртуализированный ЦУ гарантирует, что этот хост будет единственным, выполняющим эту роль.

3.2.3 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" (рисунок 86).

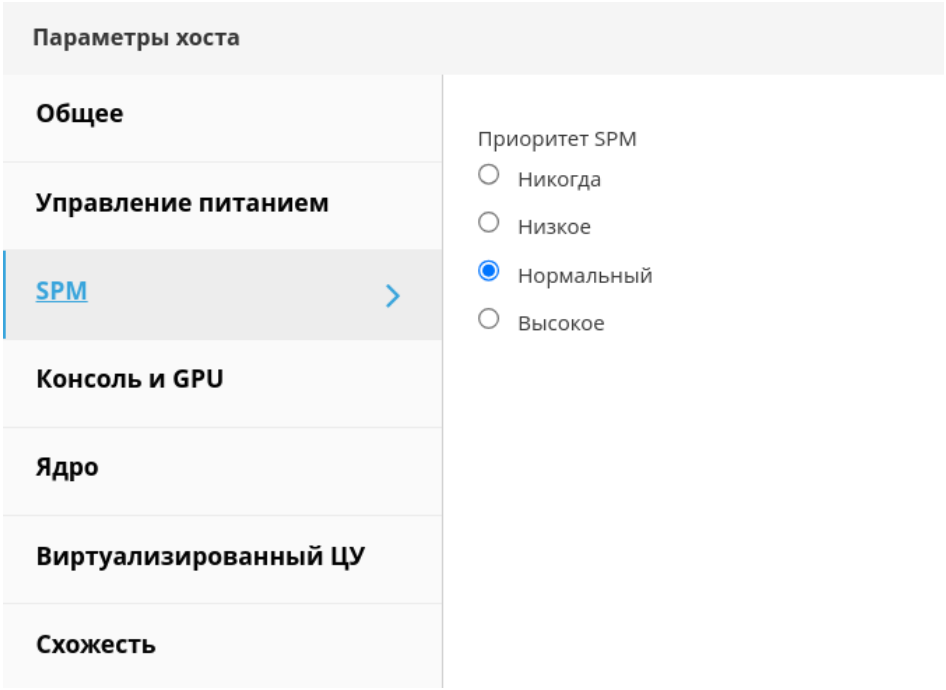


Рисунок 86 – Параметры хоста

3.2.4 Задачи при работе с дата-центрами

3.2.4.1 Создание нового дата-центра

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

Для создания нового дата-центра:

а) выбрать "Ресурсы → Дата-центры" (рисунок 87);

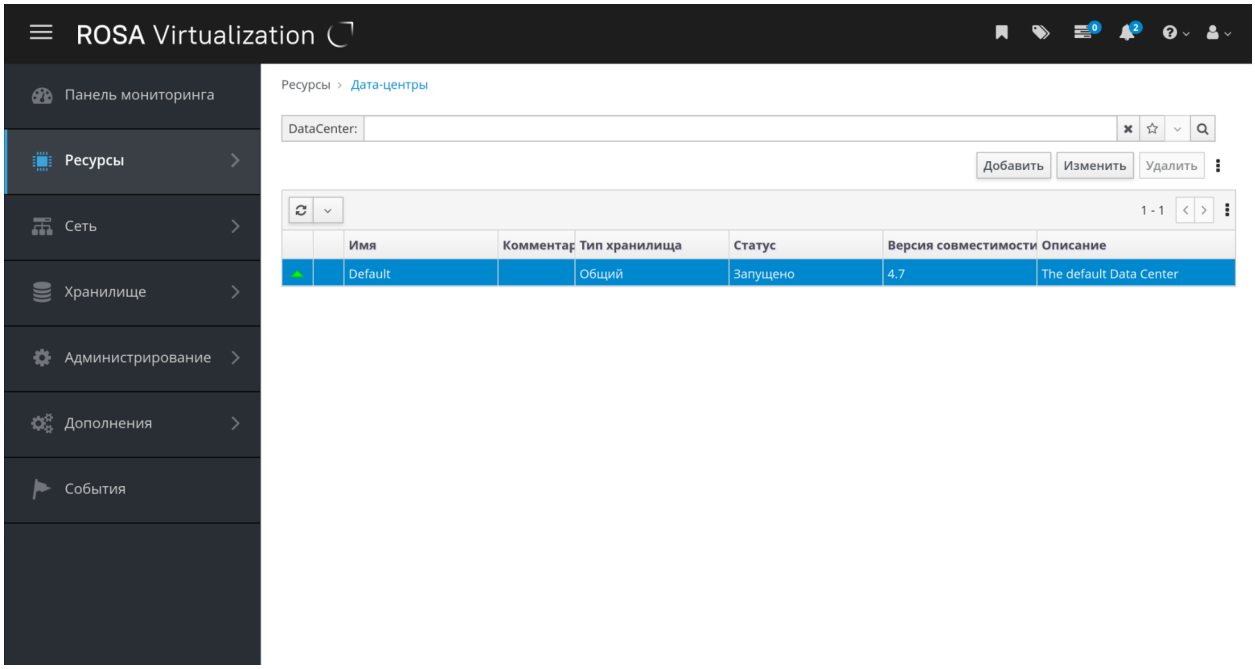


Рисунок 87 – Форма "Ресурсы → Дата-центры"

б) в окне со списком доступных дата-центров нажать кнопку Добавить;

в) в окне "Новый дата-центр" (рисунок 88) указать "Имя" и "Описание" дата-центра;

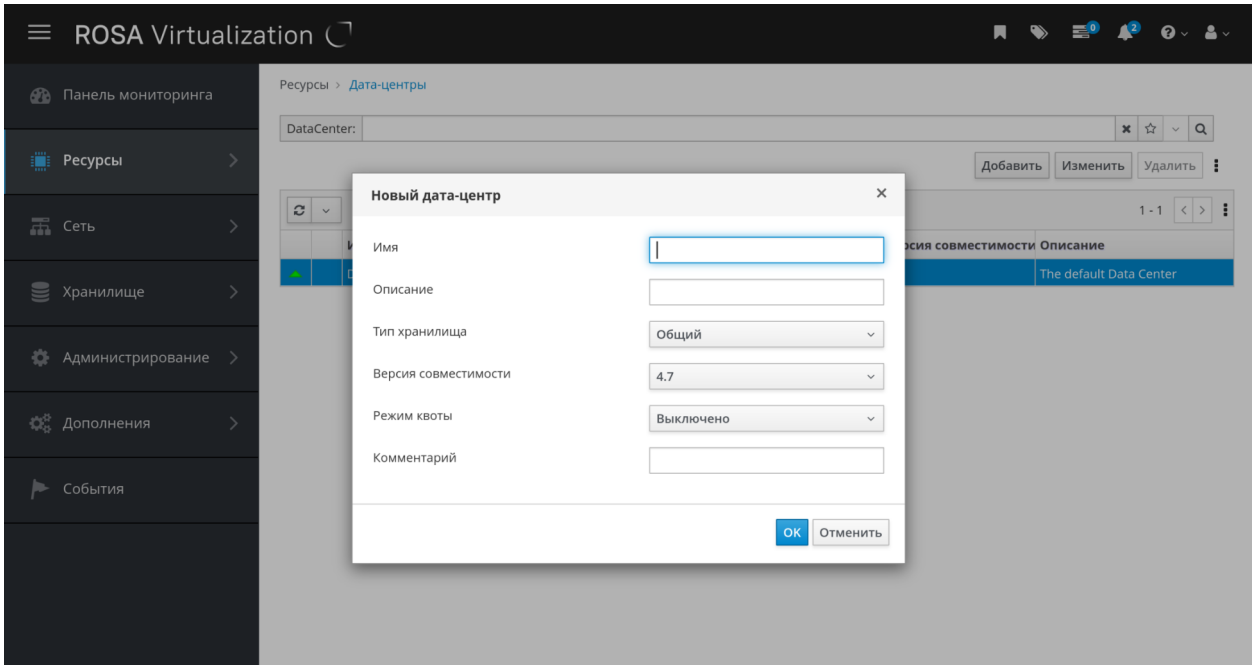


Рисунок 88 – Создание нового дата-центра

г) в выпадающих меню выбрать "Тип хранилища" (рисунок 89), "Версию совместимости" (рисунок 90) и "Режим квоты" (рисунок 91) дата-центра;

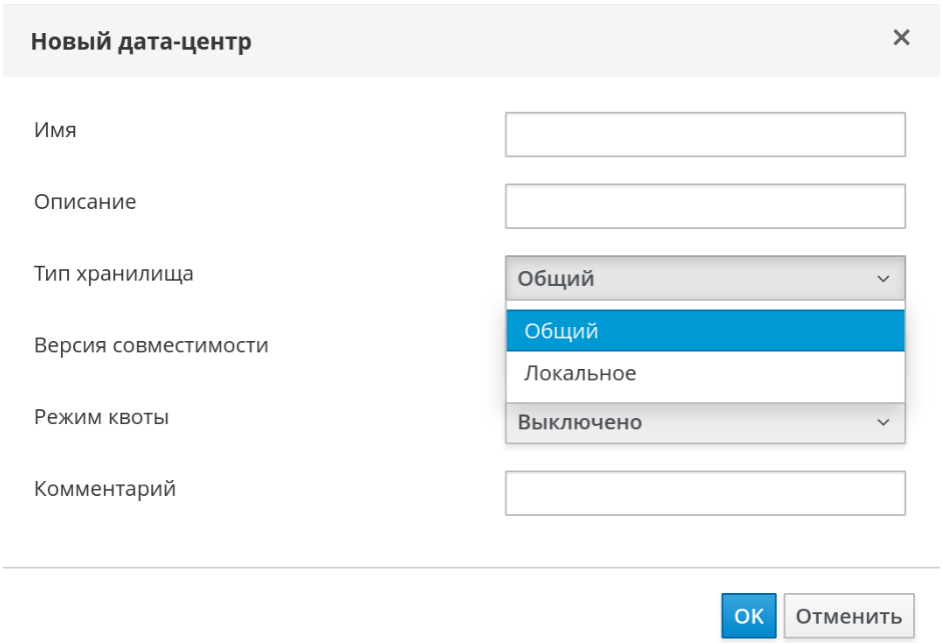


Рисунок 89 – Новый дата-центр – Тип хранилища

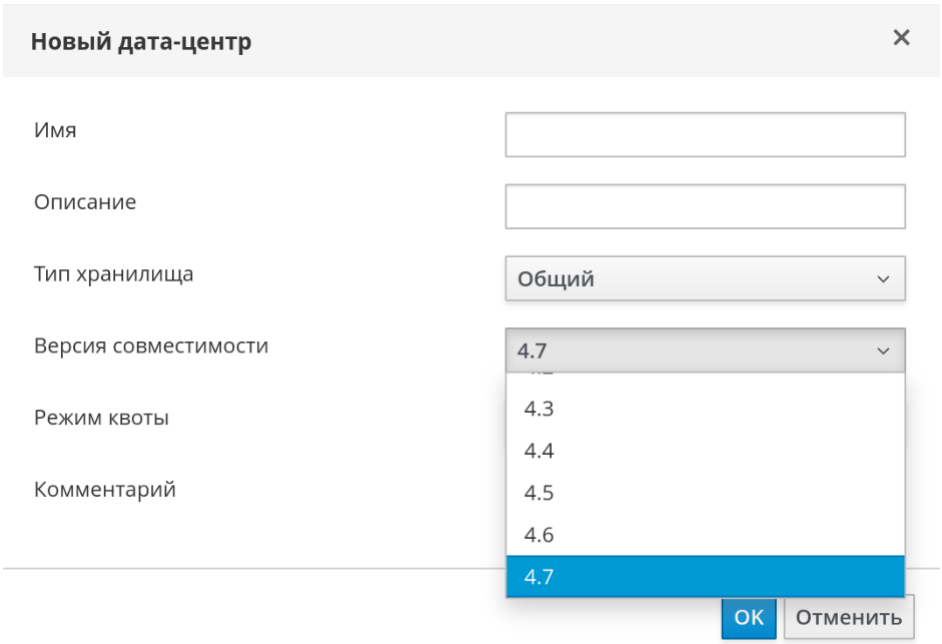


Рисунок 90 – Новый дата-центр – Версия совместимости

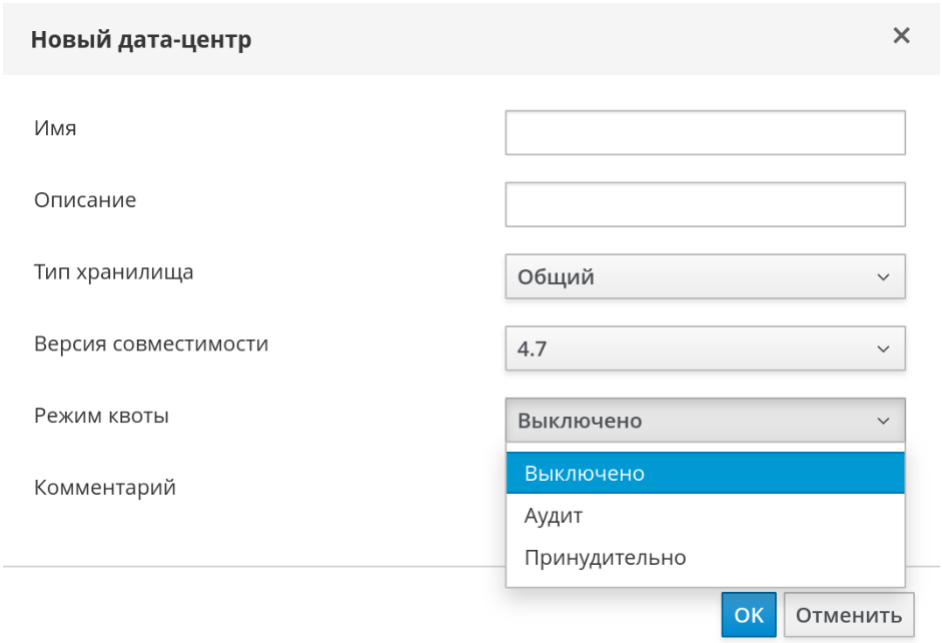


Рисунок 91 – Новый дата-центр – Режим квоты

д) для создания дата-центра нажать кнопку OK и перейти в окно "Дата-центр — пошаговый помощник" (рисунок 92);

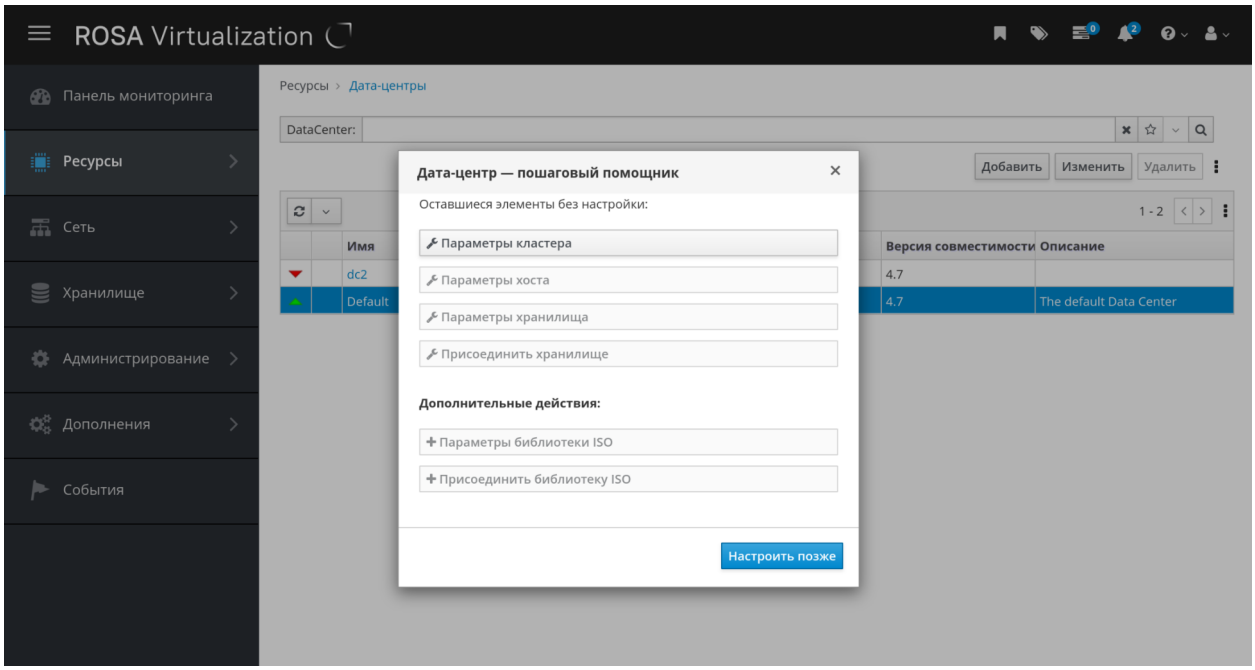


Рисунок 92 – Окно "Дата-центр — пошаговый помощник"

е) в окне пошагового помощника присутствует список объектов дата-центра, которые необходимо настроить или отложить настройку, нажав на кнопку Настроить позже. Можно возобновить процесс настройки, выбрав дата-центр и перейдя по пунктам меню пиктограммы ⋮ ("Больше действий") → "Пошаговый помощник".

Примечания:

– 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 используется "Пошаговый помощник".

– Возможность указания диапазона MAC-адресов для дата-центра выполняется на уровне кластера.

3.2.4.2 Параметры в окнах "Новый дата-центр" и "Параметры дата-центра"

В таблице 33 описываются параметры дата-центра, присутствующие в окнах "Новый дата-центр" и "Параметры дата-центра".

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

Таблица 33 – Параметры дата-центра

Поле	Описание / действие
Имя	Название дата-центра. У этого текстового поля имеется ограничение в 40 символов, а введенное название должно быть уникальным сочетанием любых строчных или прописных букв, цифр, дефисов и знаков подчеркивания
Описание	Описание дата-центра. Заполнение этого поля рекомендуется, но не обязательно
Тип хранилища	Выбрать 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 РОСА Виртуализация. 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 следует убедиться в том, что были обновлены версии всех хостов, а затем кластеров
Режим квоты	Режим квоты — это инструмент ограничения использования ресурсов в составе РОСА Виртуализация. Выбрать одно из следующих значений: – Выключено – если не нужно использовать квоты; – Аудит – если нужно изменить параметры квоты; – Принудительно – для применения квоты

Поле	Описание / действие
Комментарий	По желанию добавить комментарий о дата-центре в простом текстовом формате

3.2.4.3 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.

Для повторной инициализации дата-центра:

а) перейти в "Ресурсы → Дата-центры" и выбрать нужный дата-центр (рисунок 93);

б) убедиться в том, что любые домены хранилищ, присоединенные к дата-центру, находятся в режиме обслуживания;

в) нажать пиктограмму "Больше действий" ⋮, затем пункт "Повторно инициализировать дата-центр";

г) установить флажок для домена хранилища, добавляемого в дата-центр, в списке всех доступных (отсоединенных, в режиме обслуживания) доменов хранилищ в окне "Повторная инициализация дата-центра";

д) установить флажок "Подтвердить операцию";

е) нажать кнопку OK.

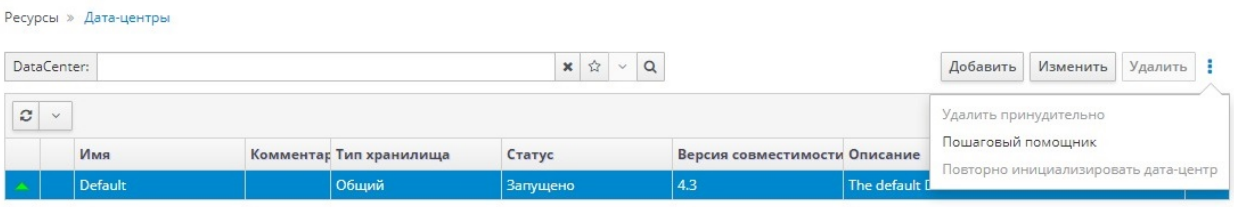


Рисунок 93 – Повторная инициализация дата-центра

В результате домен хранилища будет присоединен 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.

3.2.4.4 Удаление дата-центра

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

Для удаления дата-центра требуется:

а) убедиться в том, что домены хранилищ, присоединенные к дата-центру, находятся в режиме обслуживания;

б) выбрать "Ресурсы → Дата-центры" и выбрать дата-центр, который нужно удалить;

в) нажать кнопку Удалить и в открывшемся окне "Удалить дата-центр(ы)" (рисунок 94) опционально указать причину и подтвердить удаление дата-центра, нажав кнопку OK, или отменить удаление, нажав кнопку Отменить.

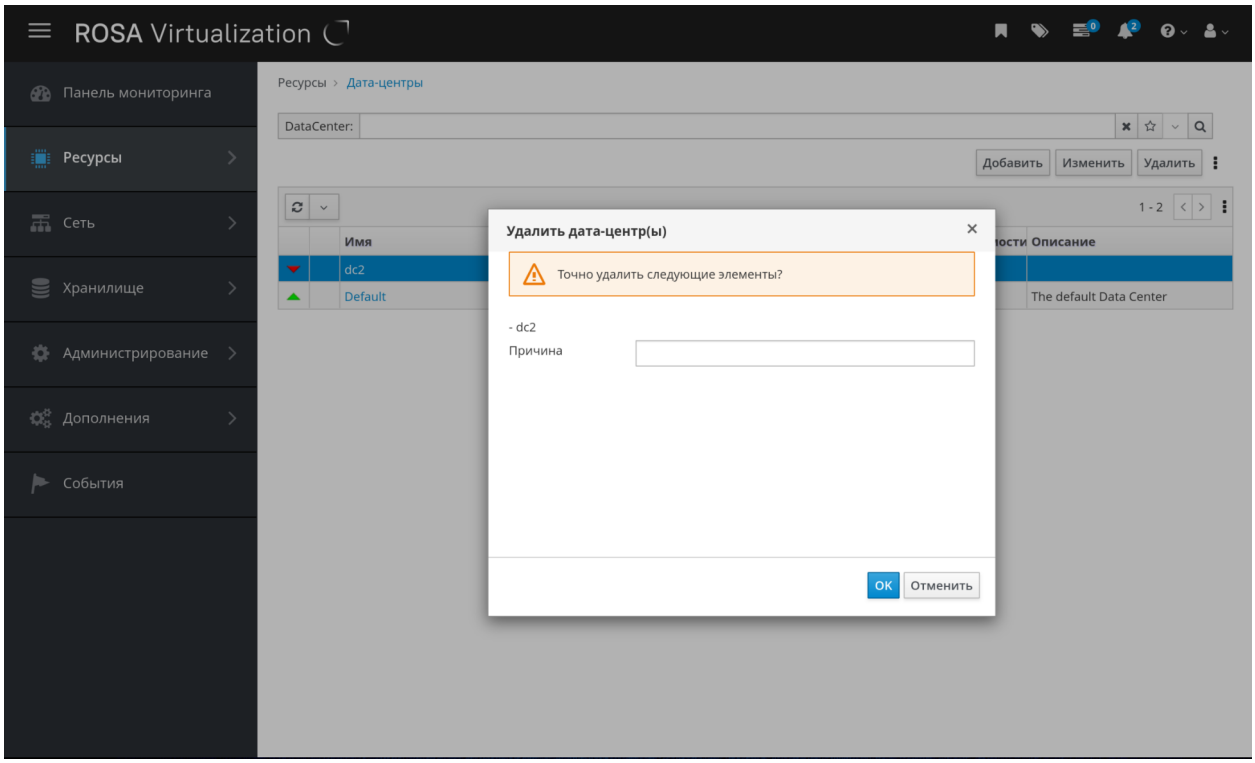


Рисунок 94 – Подтверждение удаления дата-центра

г) после нажатия на кнопку OK выбранный дата-центр будет удален.

3.2.4.5 Принудительное удаление дата-центра

Статус "Не отвечает" присваивается дата-центру, если присоединенный домен хранилища поврежден или если хост получает статус "Не отвечает". В любых других ситуациях удалить дата-центр невозможно.

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

Примечание — Перед принудительным удалением дата-центра может понадобиться удаление поврежденного домена хранилища.

Для принудительного удаления дата-центра требуется:

а) выбрать раздел "Ресурсы → Дата-центры" и выбрать дата-центр, который нужно удалить;

б) нажать на пиктограмму ⋮ ("Больше действий") и далее на кнопку Принудительно удалить;

в) установить флажок "Одобрить операцию";

г) нажать кнопку OK.

В результате дата-центр и присоединенный домен хранилища навсегда будут удалены из окружения виртуализации РОСА Виртуализация.

3.2.4.6 Изменение типа хранилища дата-центра

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

Для изменения типа хранилища имеются 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.

Для изменения типа хранилища дата-центра:

а) выбрать "Ресурсы → Дата-центры" и выбрать дата-центр, который нужно изменить;

б) нажать кнопку Изменить;

в) изменить "Тип хранилища";

г) нажать кнопку OK.

3.2.4.7 Изменение версии совместимости дата-центра

Дата-центры РОСА Виртуализация 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.

Для изменения версии совместимости дата-центра нужно:

а) выбрать "Ресурсы → Дата-центры" и выбрать дата-центр, который нужно изменить;

б) нажать кнопку Изменить;

в) указать необходимую "Версию совместимости";

г) нажать кнопку OK.

3.2.5 Дата-центры и домены хранилищ

3.2.5.1 Добавление существующего домена данных к дата-центру

Домены данных со статусом "Не присоединен" 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.

Для добавления существующего домена данных к дата-центру нужно:

а) выбрать "Ресурсы → Дата-центры";

б) нажать на название дата-центра, чтобы открыть подробные сведения;

в) перейти на вкладку "Хранилище" (рисунок 95), чтобы просмотреть список доменов, уже присоединенных к дата-центру;

г) нажать кнопку Присоединить данные;

д) установить флажок напротив домена данных, который нужно присоединить к дата-центру (при необходимости выбрать несколько доменов данных);

е) нажать кнопку OK.

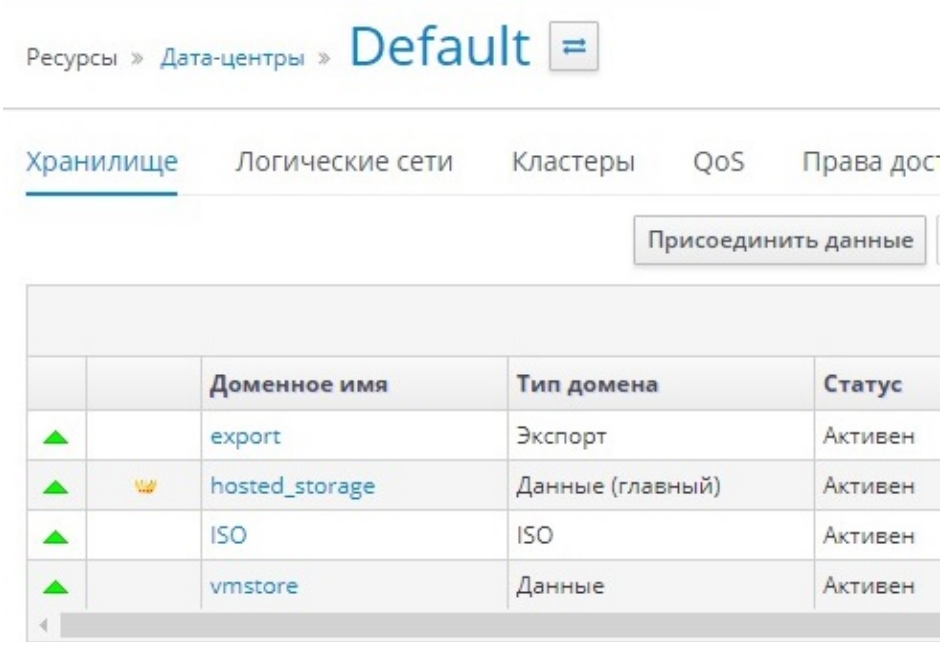


Рисунок 95 – Добавление существующего домена данных к дата-центру

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

3.2.5.2 Добавление существующего домена ISO к дата-центру

Домены ISO со статусом "Не присоединен" можно присоединять к дата-центру. К дата-центру можно присоединить только один домен ISO. Домен ISO должен иметь тот же тип хранилища, что и дата-центр.

Для добавления существующего домена ISO к дата-центру нужно:

а) выбрать"Ресурсы → Дата-центры";

б) нажать на название дата-центра, чтобы открыть подробные сведения;

в) перейти на вкладку "Хранилище", чтобы просмотреть список доменов, уже присоединенных к дата-центру;

г) нажать кнопку Присоединить ISO;

д) установить флажок напротив нужного домена ISO;

е) нажать кнопку OK.

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

3.2.5.3 Присоединение существующего домена экспорта к дата-центру

Домен экспорта со статусом "Не присоединен" 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 присоединенный дата-центр. Сведения об импорте доменов хранилищ см. в п. 3.6.6.1.2.

Для присоединения существующего домена экспорта к дата-центру нужно:

а) выбрать "Ресурсы → Дата-центры";
б) нажать на название дата-центра, чтобы открыть подробные сведения;
в) перейти на вкладку "Хранилище", чтобы просмотреть список доменов, уже присоединенных к дата-центру;
г) нажать кнопку Присоединить экспорт;
д) установить флажок напротив нужного домена экспорта;
е) нажать кнопку OK.

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

3.2.5.4 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 РОСА Виртуализация и его при необходимости можно будет присоединить к другому дата-центру.

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

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

Для отсоединения домена хранилища от дата-центра нужно:

а) выбрать "Ресурсы → Дата-центры";

б) нажать на название дата-центра, чтобы открыть подробные сведения (рисунок 96);

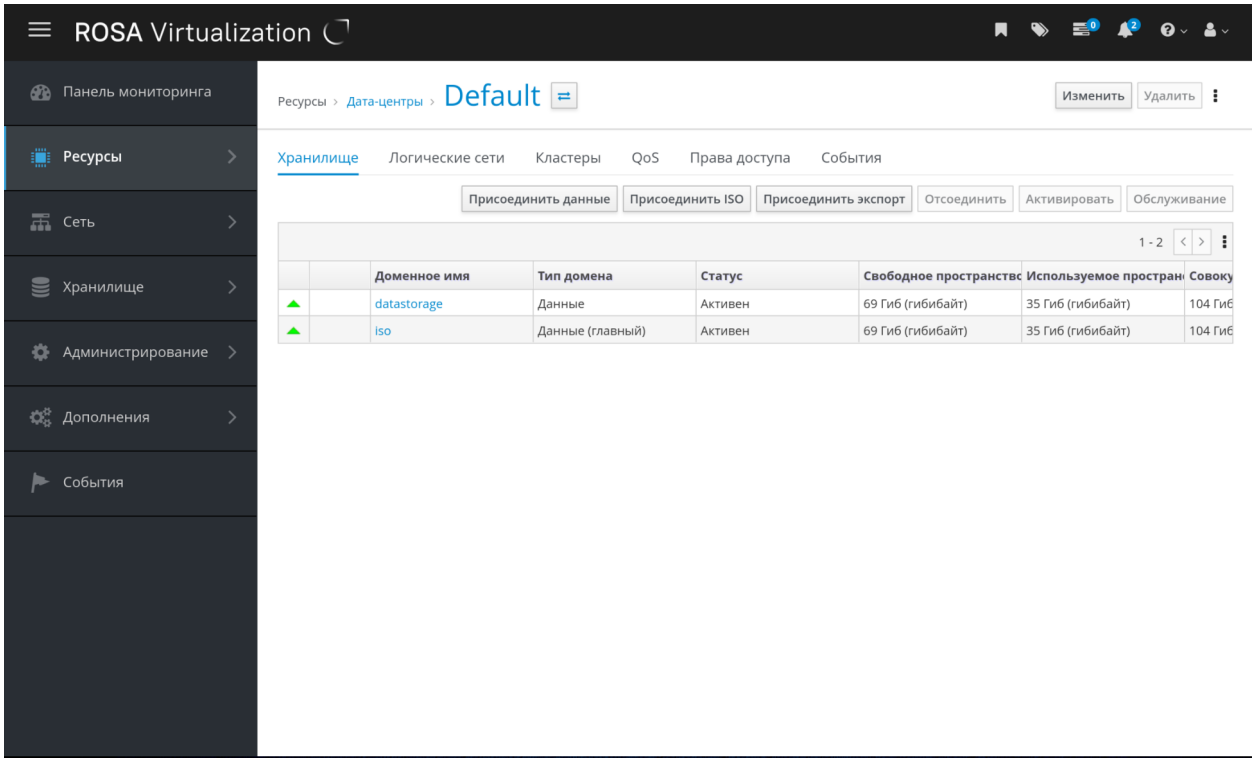


Рисунок 96 – Домены хранилища, присоединенные к дата-центру

в) перейти на вкладку "Хранилище", чтобы просмотреть список доменов, уже присоединенных к дата-центру (рисунок 97);

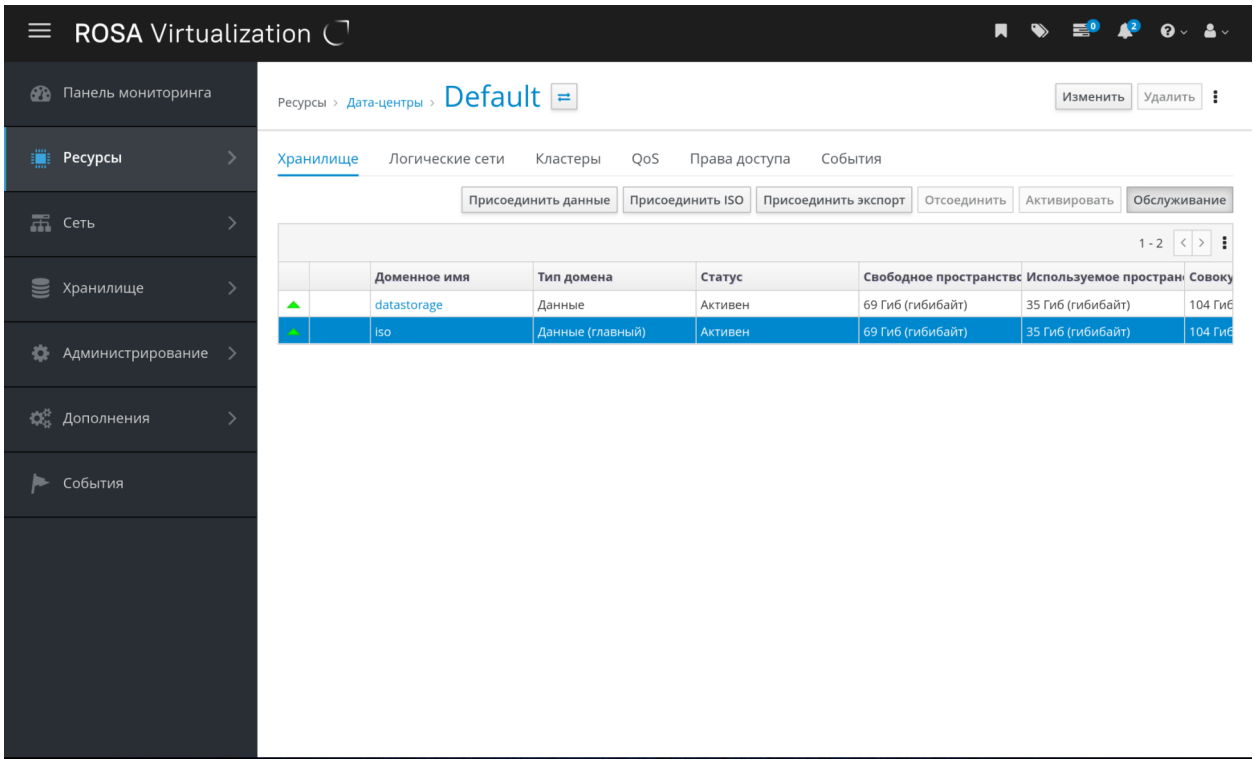


Рисунок 97 – Запуск режима "Обслуживание для выбранного домена"

г) выбрать домен хранилища, который надо отсоединить. Если домен "Активен", нажать кнопку Обслуживание;

д) нажать кнопку OK для запуска режима обслуживания;

е) нажать кнопку Отсоединить;

ж) нажать кнопку OK.

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

3.3 Кластеры

3.3.1 Введение

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, определенным в кластере, и параметрам ВМ. "Кластер" — это самый высокий из возможных уровней, на которых должны быть настроены политики энергосбережения и распределения нагрузки (рисунок 98).

Число хостов и число ВМ, принадлежащих кластеру, отображаются соответственно в списках "Счетчик 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 РОСА Виртуализация создает кластер по умолчанию в дата-центре по умолчанию.

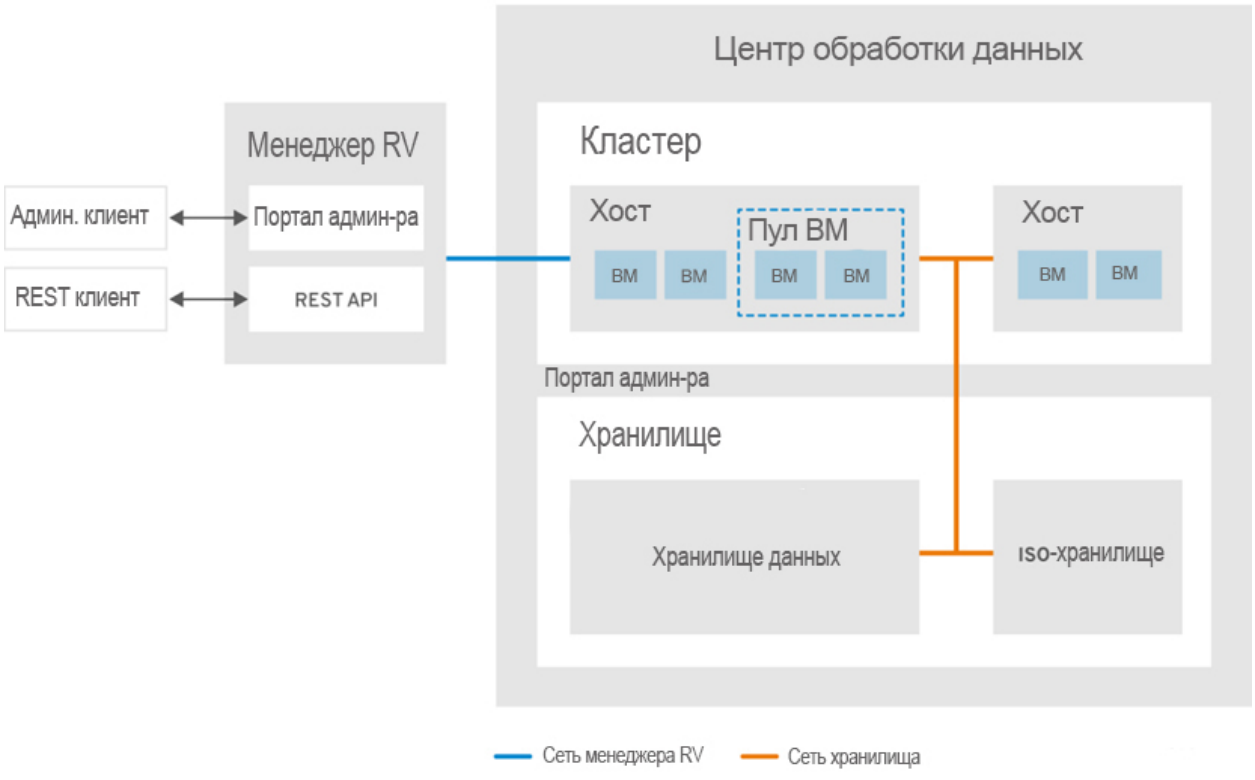


Рисунок 98 – Кластер в центре обработки данных

3.3.2 Задачи при работе с кластерами

Примечание — Некоторые параметры кластера не применимы к кластерам Gluster.

3.3.2.1 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.

Для создания нового кластера нужно:

а) перейти в "Ресурсы → Кластеры" для открытия формы управления кластерами (рисунок 99);

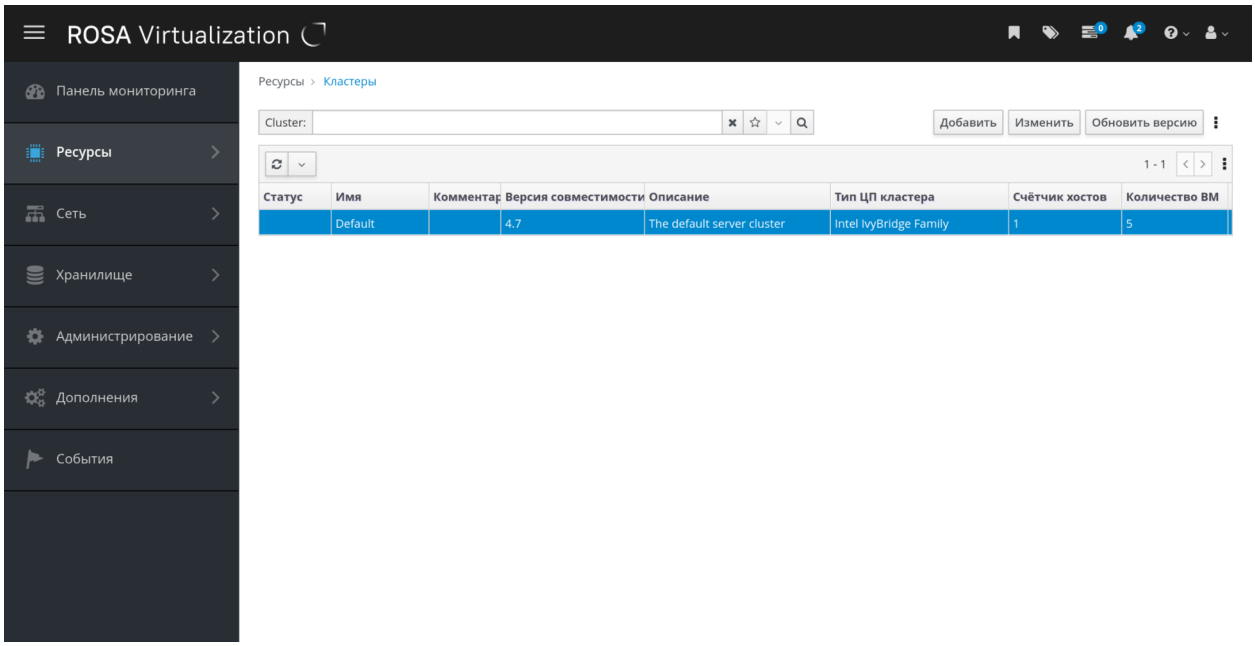


Рисунок 99 – Список доступных кластеров, форма управления кластерами

б) нажать кнопку Добавить;

в) в выпадающем списке выбрать "Дата-центр", к которому будет принадлежать кластер (рисунок 100);

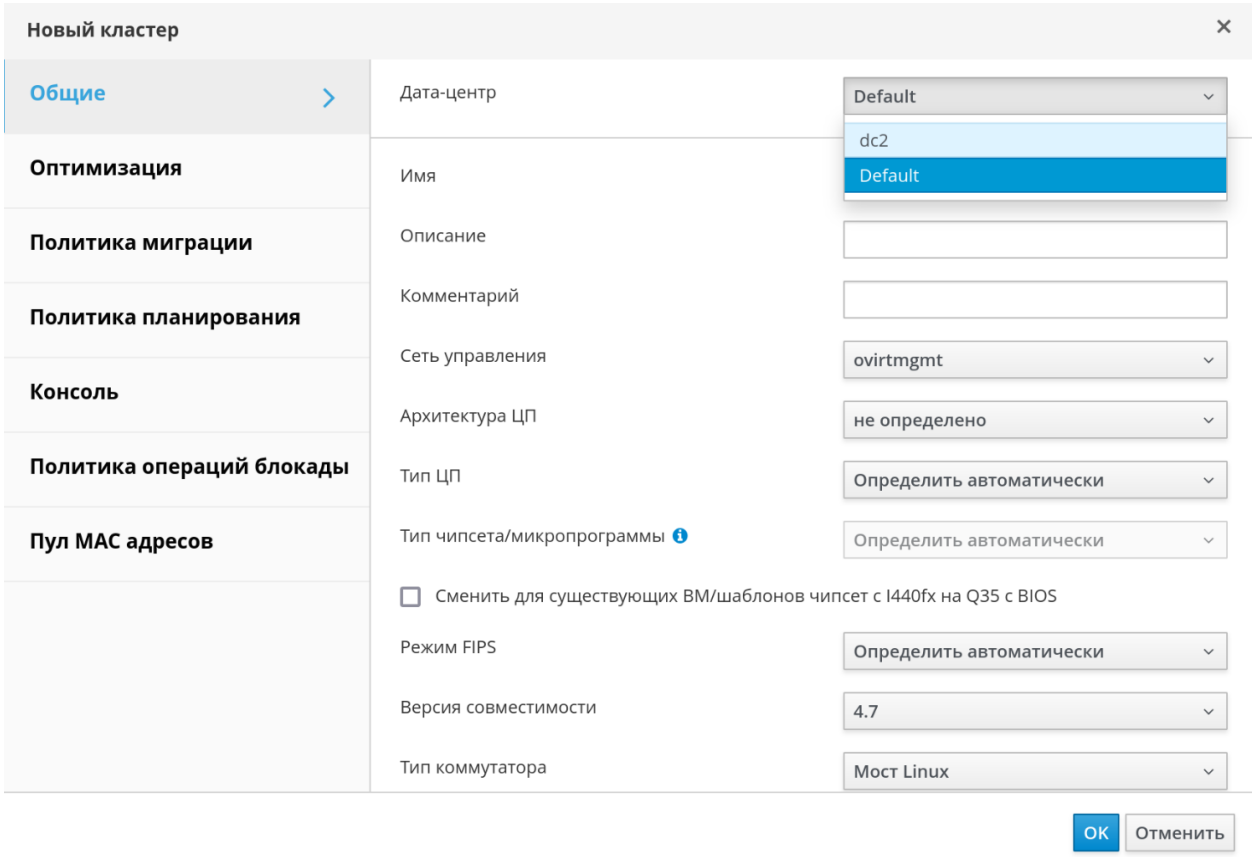


Рисунок 100 – Выбор дата-центра для кластера

г) указать "Имя" и "Описание кластера";

д) в выпадающем списке "Сеть управления" выбрать сеть, которой нужно присвоить роль сети управления;

е) в выпадающих списках выбрать "Архитектуру ЦП" и "Тип ЦП" (рисунки 101-102);

Важно, чтобы семейство процессора совпадало с минимальным типом процессора хостов, к которым предполагается присоединить кластер, в противном случае хост будет нерабочим.

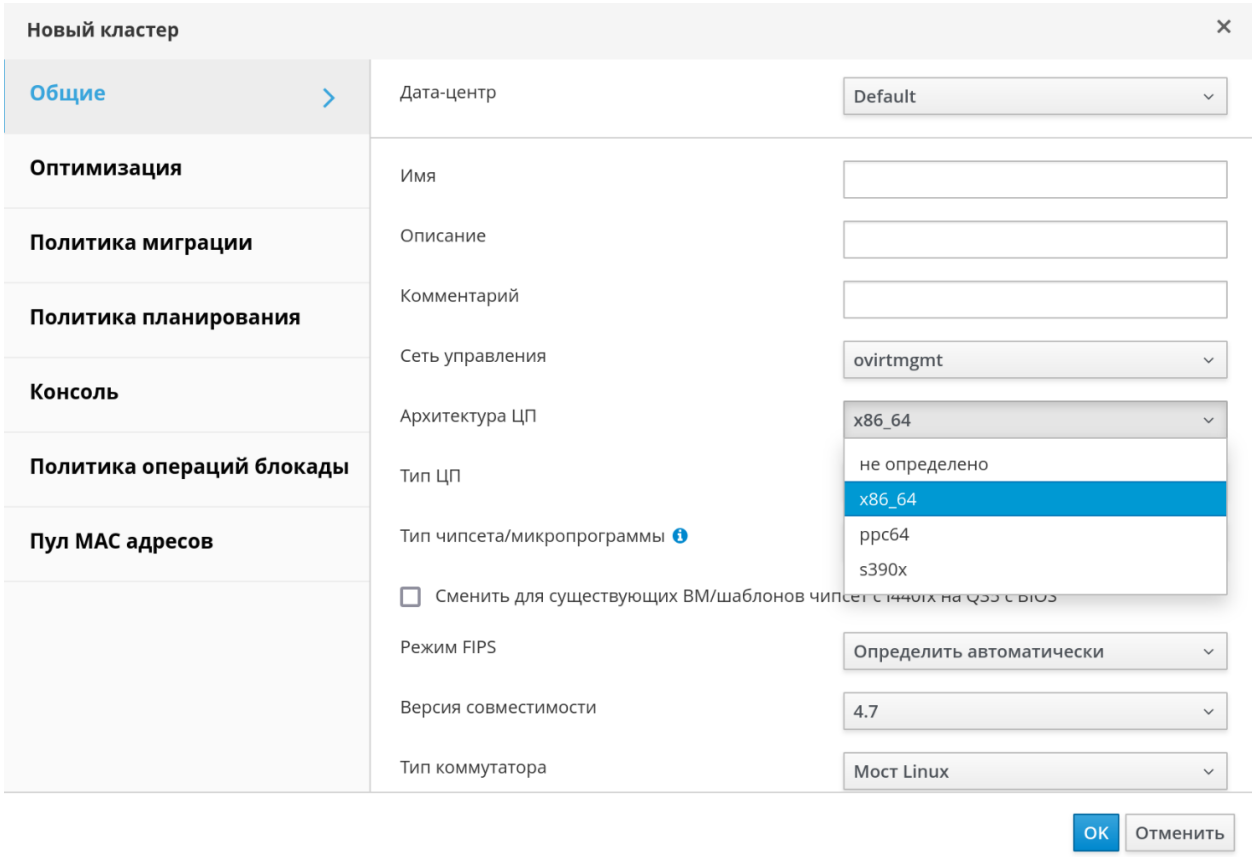


Рисунок 101 – Выбор архитектуры ЦП для кластера

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, в списке выбирают самую старую модель.

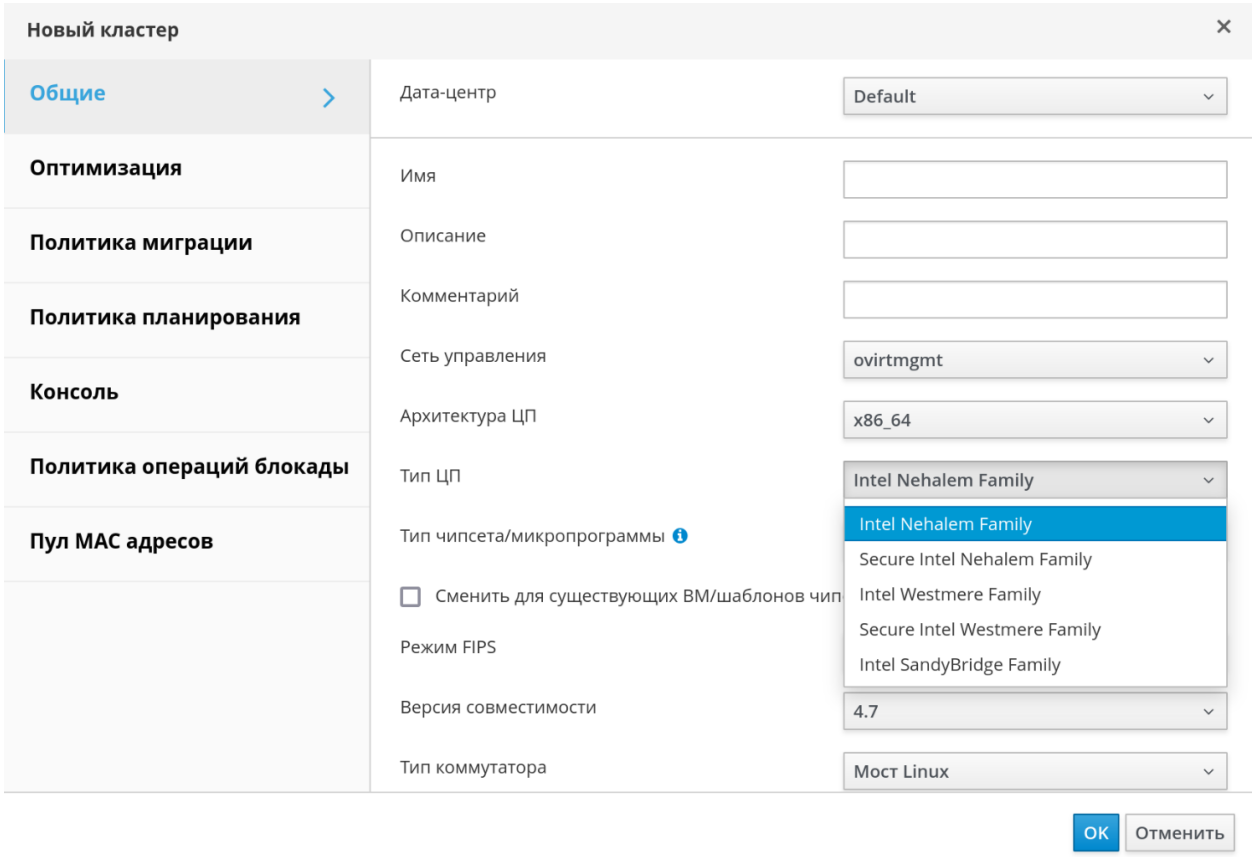


Рисунок 102 – Выбор типа ЦП для кластера

ж) в выпадающем списке выбрать "Тип чипсета/микропрограммы" кластера (рисунок 103);

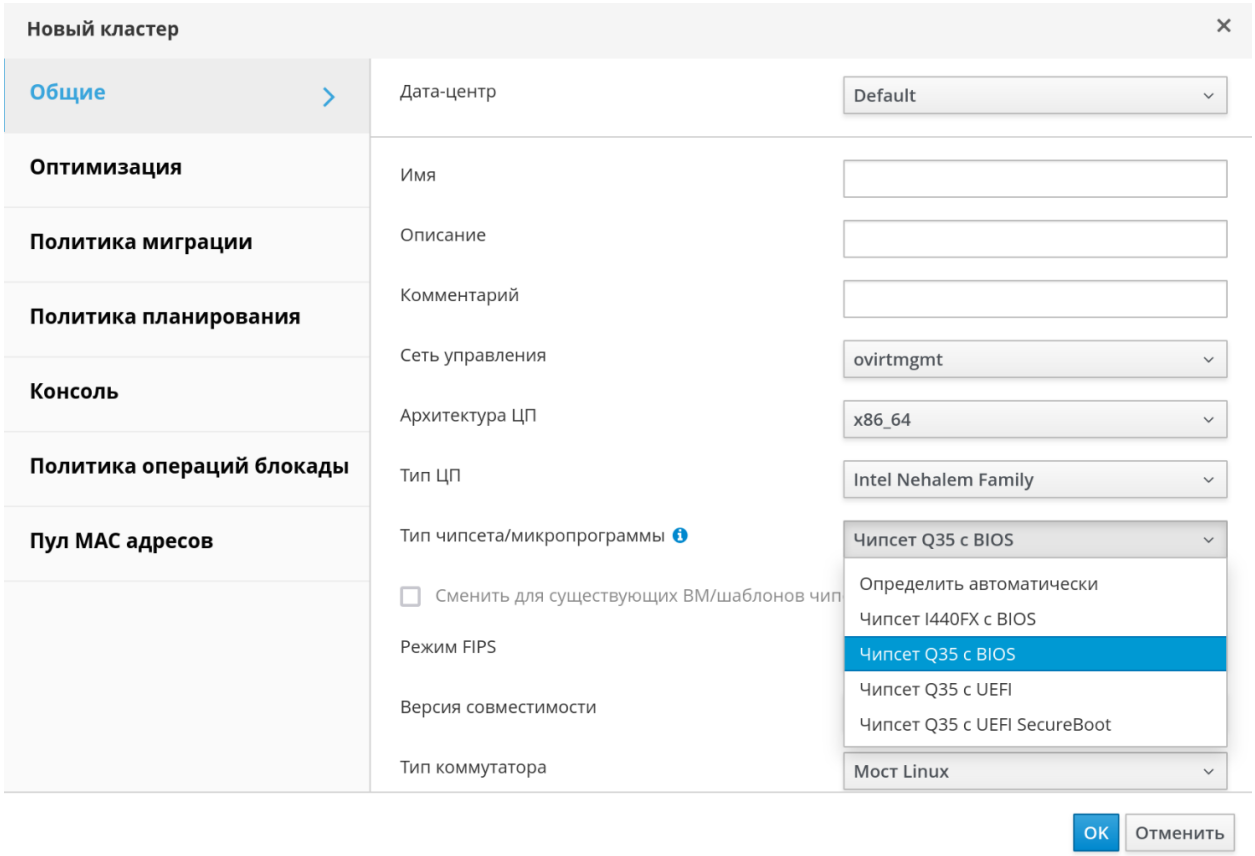


Рисунок 103 – Выбор тип чипсета/микропрограммы кластера.

з) в выпадающем списке выбрать "Версию совместимости кластера";
и) в выпадающем списке выбрать "Тип коммутатора" (рисунок 104);

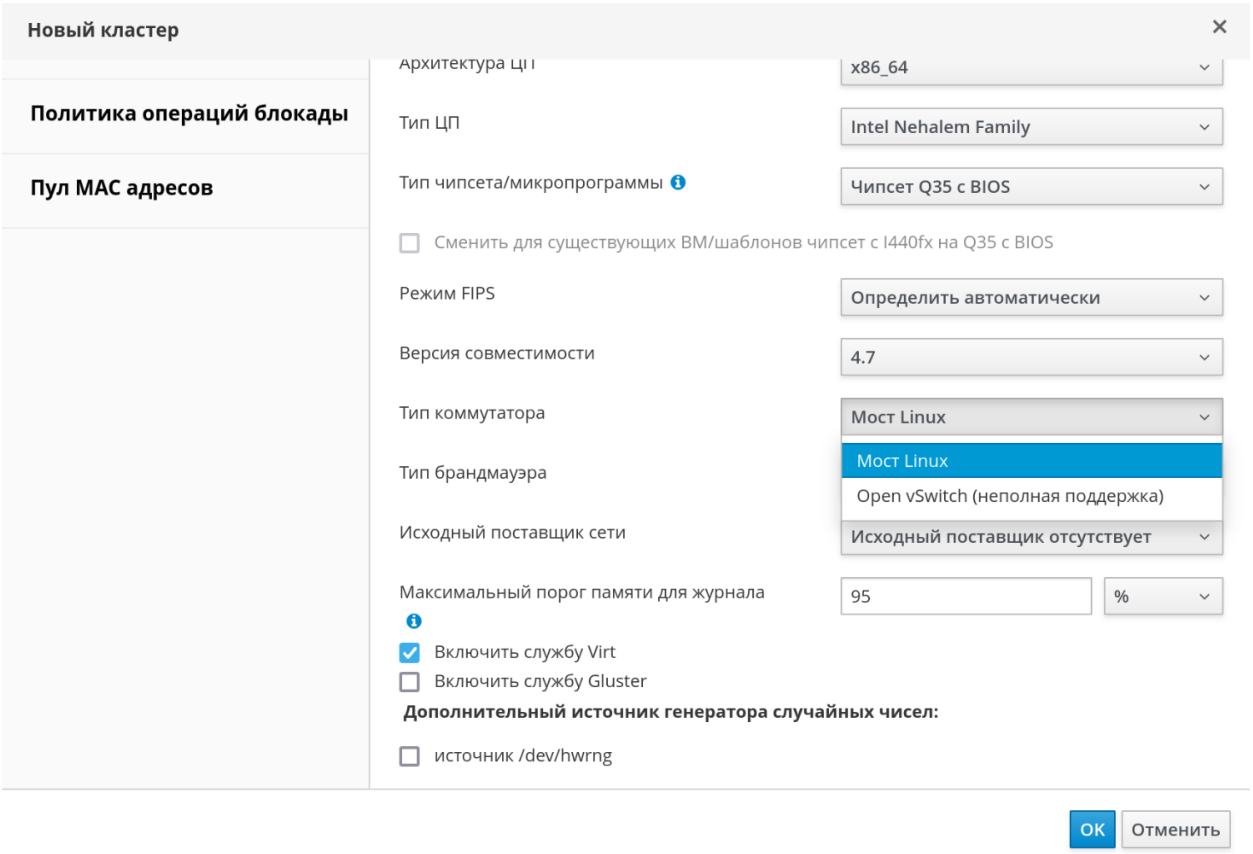


Рисунок 104 – Выбор типа коммутатора кластера

к) для хостов в кластере выбрать "Тип брандмауэра" — iptables или firewalld (рисунок 105);

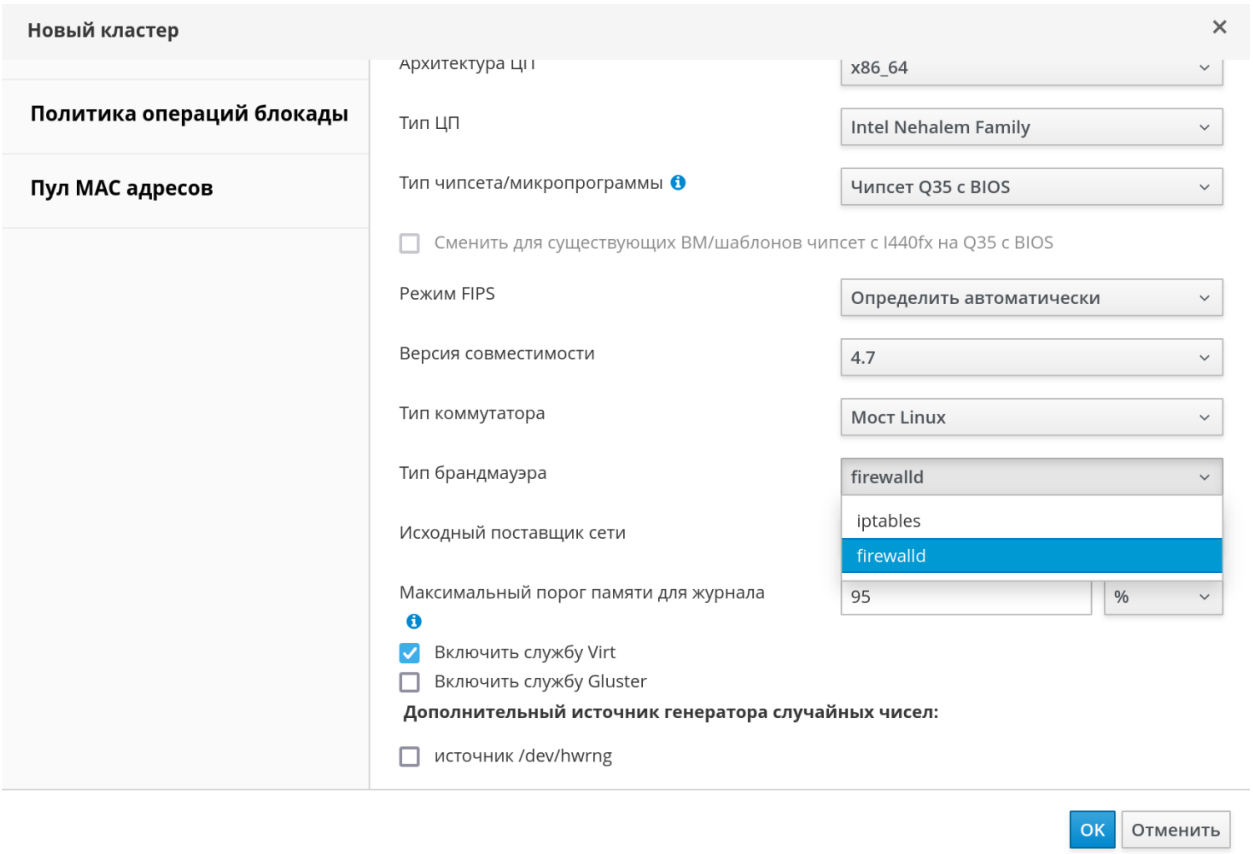


Рисунок 105 – Выбор типа брандмауэра кластера

Примечание – iptables является устаревшим типом межсетевого экрана.

л) установить 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);

м) при необходимости установить 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) отмечен по умолчанию;

н) перейти на вкладку "Оптимизация" для выбора порога разделяемых страниц памяти в кластере, а также при необходимости включить обработку потоков ЦП и вытеснение памяти на хостах в кластере (рисунок 106);

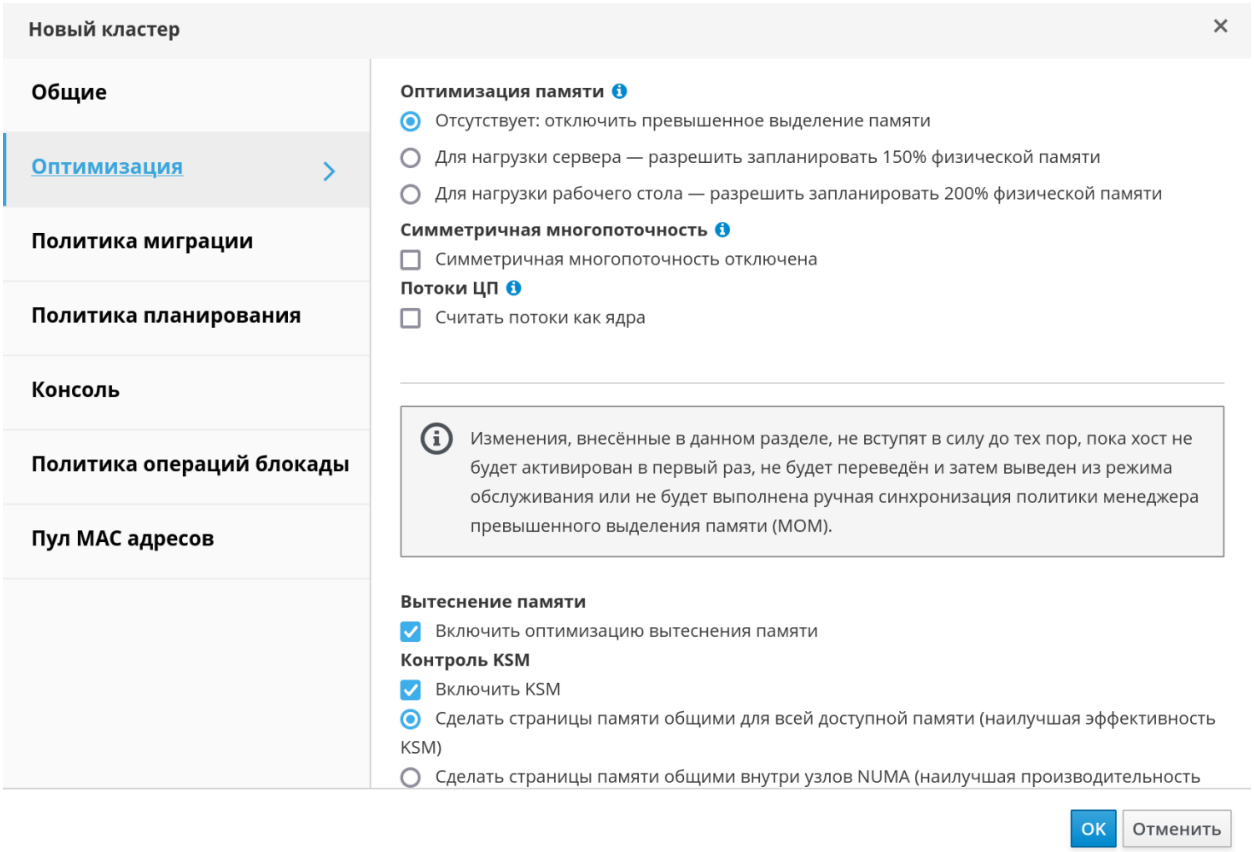


Рисунок 106 – Вкладка "Оптимизация" для настройки параметров оптимизации кластера

о) перейти на вкладку "Политика миграции" для настройки политики миграции ВМ в кластере (рисунок 107);

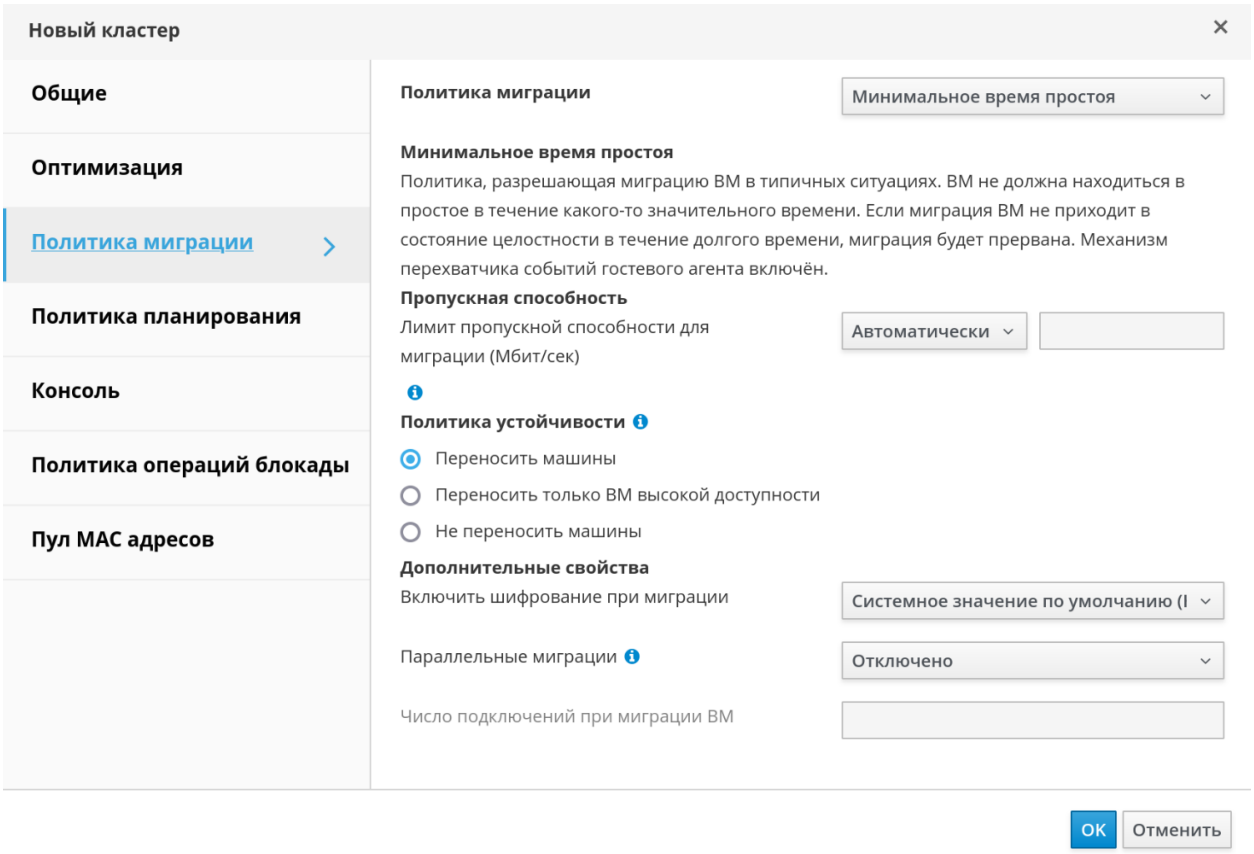


Рисунок 107 – Вкладка "Политика миграции" для настройки политики миграции ВМ в кластере.

п) перейти на вкладку "Политика планирования", чтобы при необходимости настройки политики планирования указать параметры оптимизации планировщика, включить доверенную службу для хостов в кластере, включить резервирование высокой доступности и добавить частную политику порядковых номеров (рисунок 108);

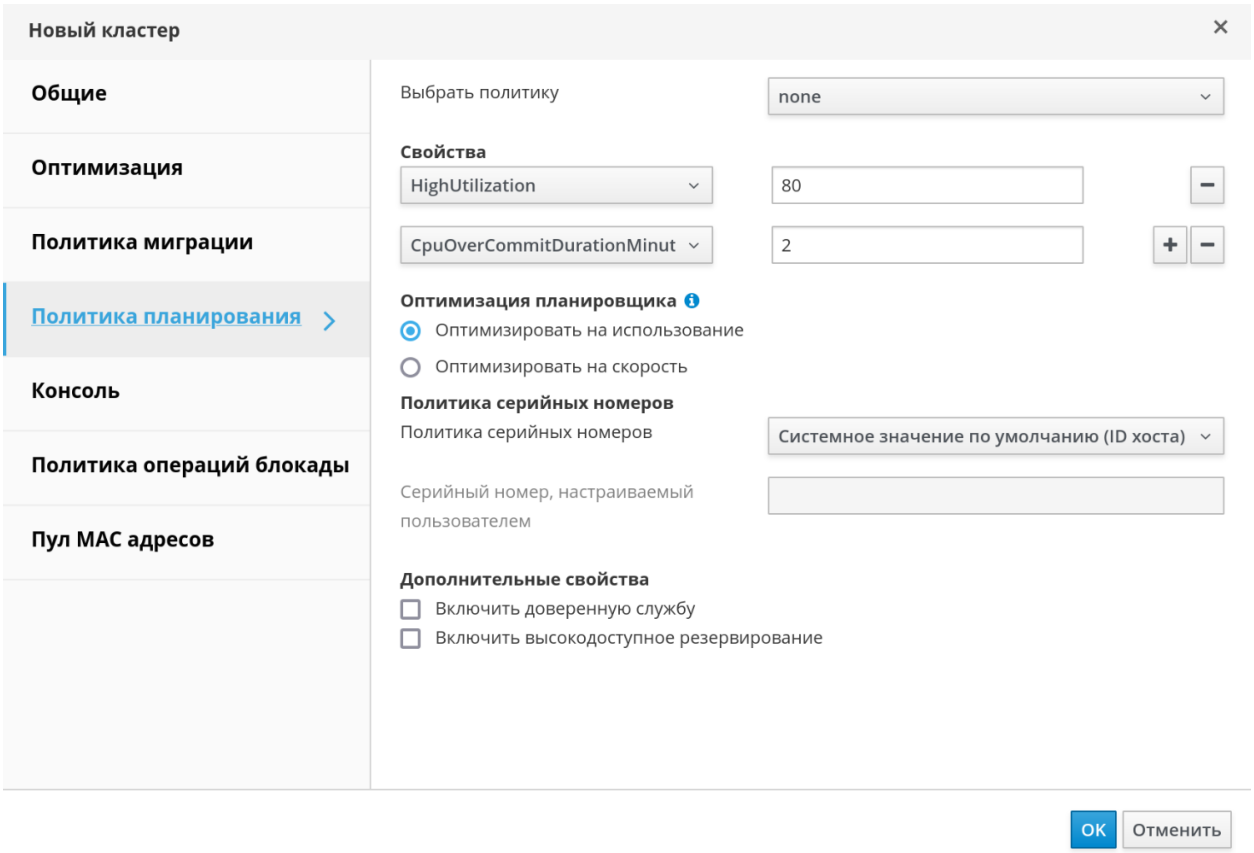


Рисунок 108 – Вкладку "Политика планирования" для настройки политики планирования кластера

р) перейти на вкладку "Консоль", чтобы при необходимости переопределить глобальные параметры прокси SPICE для хостов в кластере (рисунок 109);

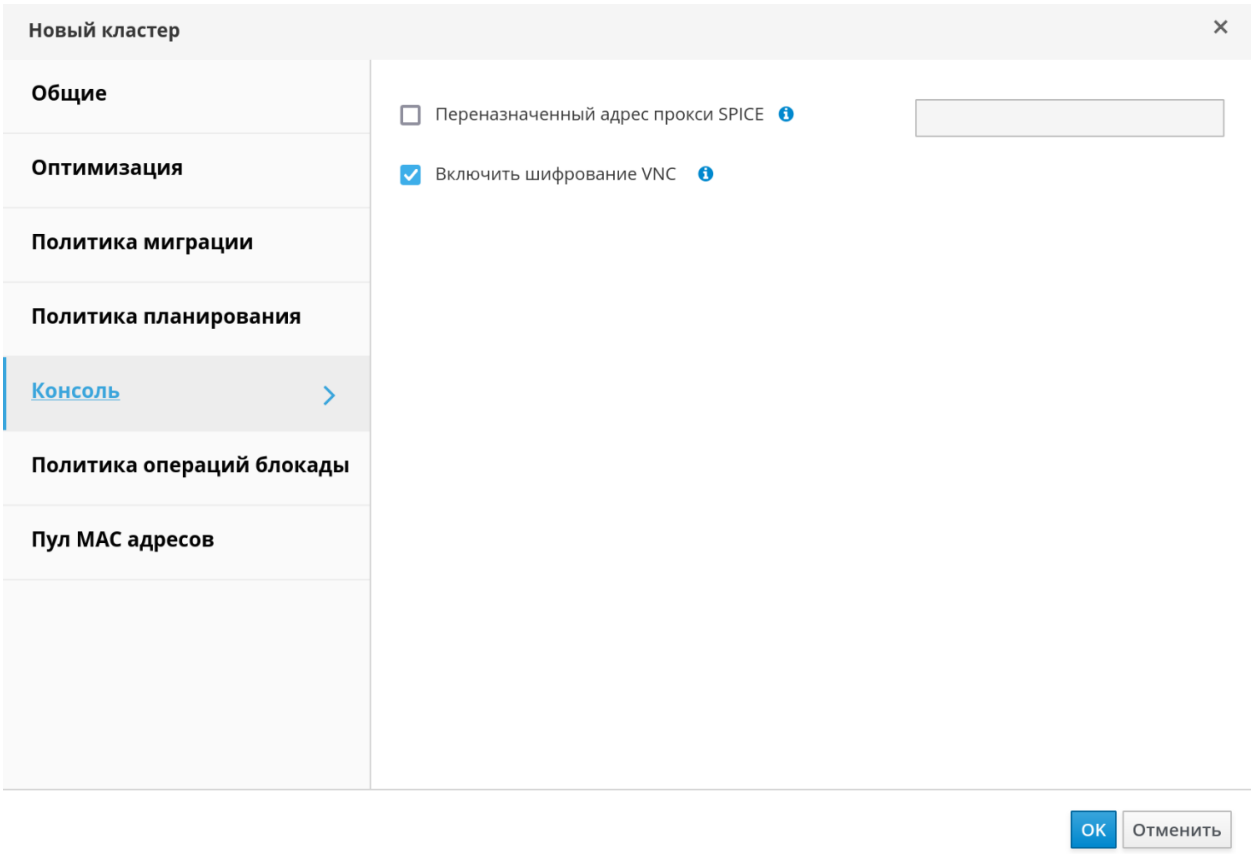


Рисунок 109 – Вкладка "Консоль" для настройки глобальных параметров прокси SPICE для хостов в кластере

с) перейти на вкладку "Политика операций блокады", чтобы включить или отключить возможность проведения операций блокады в кластере и выбрать параметры блокады (рисунок 110);

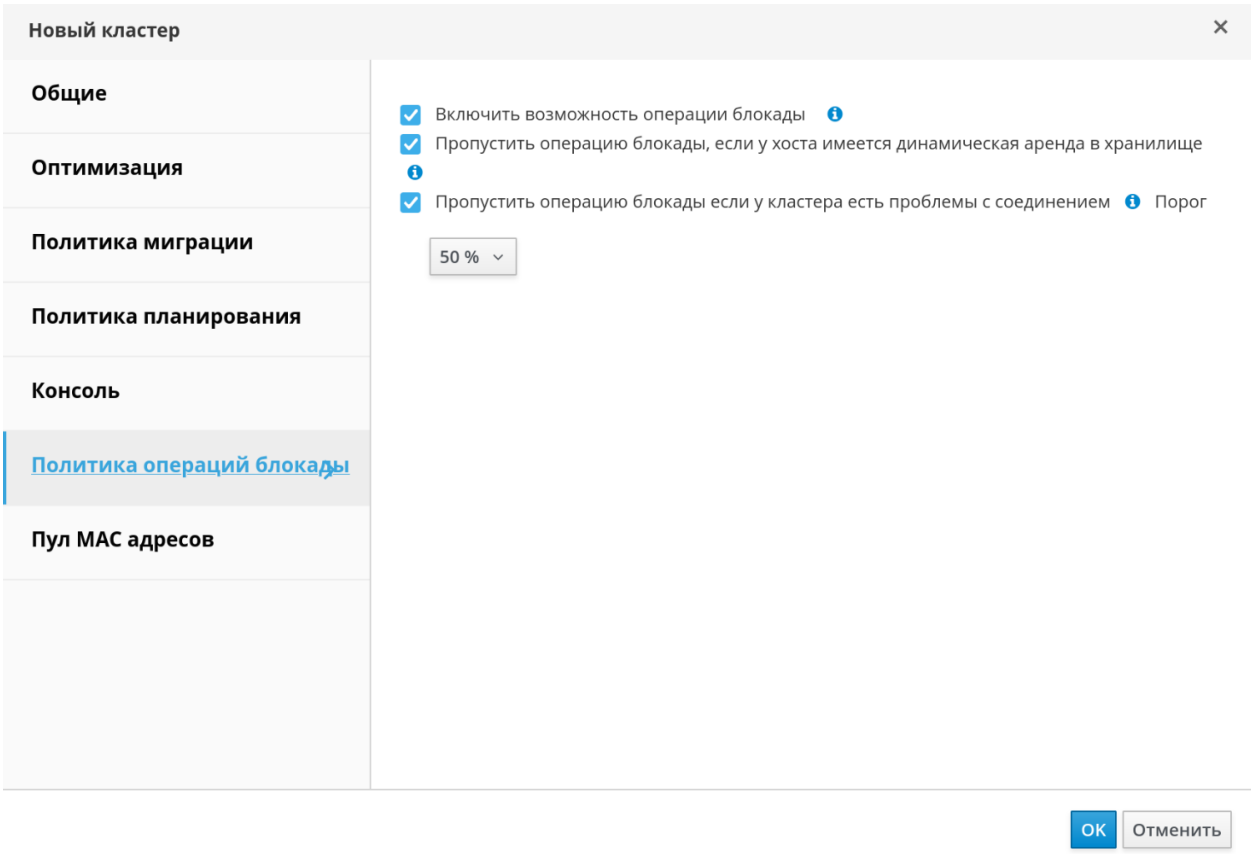


Рисунок 110 – Вкладка "Политика операций блокады"

т) нажать "Пул MAC адресов", чтобы указать пул, отличный от пула MAC-адресов по умолчанию (рисунок 111). Подробности о создании, редактировании или удалении пулов MAC-адресов см. в п. 2.1.6;

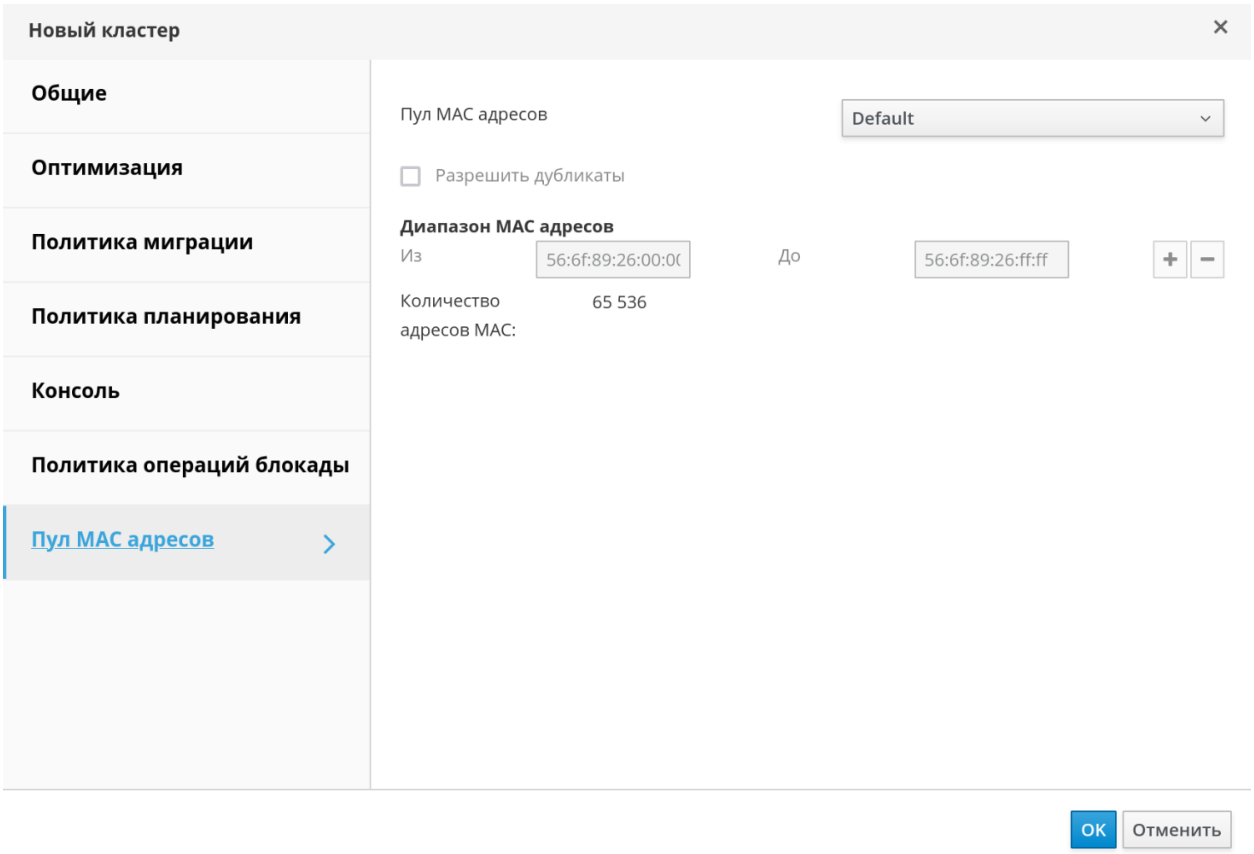


Рисунок 111 – Вкладка "Пул MAC адресов"

у) нажать кнопку OK, чтобы создать кластер и запустить окно "Кластер — пошаговый помощник" (рисунок 112);

ф) в окне "Пошаговый помощник" указан список объектов, для которых необходимо настроить взаимодействие с кластером; настроить эти объекты или отложить настройку, нажав на кнопку Настроить позже. Процесс настройки можно возобновить позднее, для чего выбрать необходимый кластер, затем нажать на пиктограмму ⋮ ("Больше действий"), после чего выбрать "Пошаговый помощник".

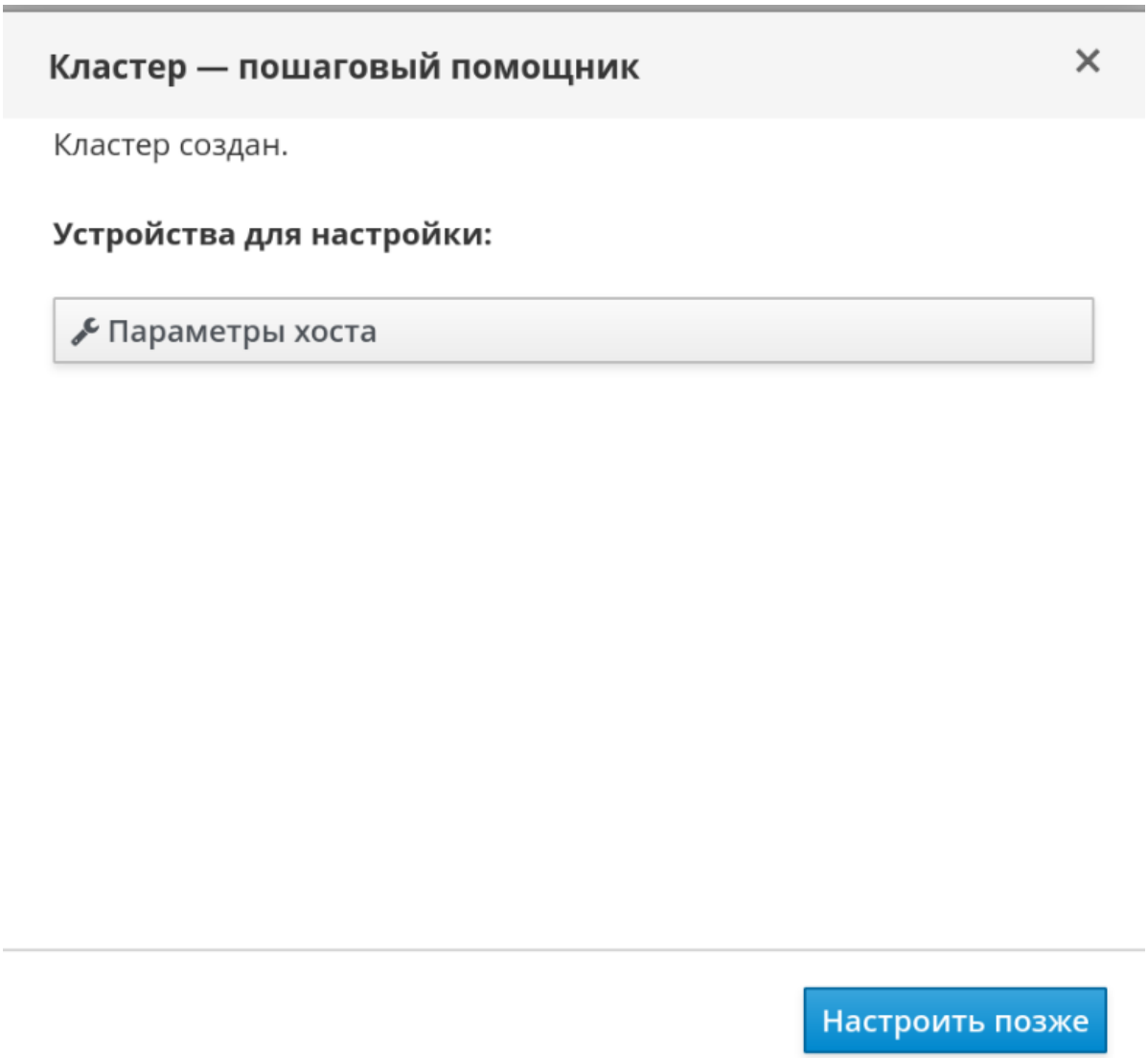


Рисунок 112 – Окно "Кластер — пошаговый помощник"

3.3.2.2 Общие параметры кластера

В таблице 34 описываются параметры вкладки "Общее" в окнах "Новый кластер" и "Параметры кластера".

Примечание – При нажатии кнопки OK недействительные элементы обводятся оранжевым, запрещая применение изменений. Кроме того, в полях ввода указываются ожидаемые значения или диапазон значений.

Таблица 34 – 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 введенное название должно быть уникальным сочетанием любых строчных или прописных букв, цифр, дефисов и знаков подчеркивания
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; –Westmere; –Sandybridge; –Haswell; –Haswell-noTSX; –Broadwell; –Broadwell-noTSX;

Поле	Описание / действие
	– 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 РОСА Виртуализация. Нельзя выбрать версию, более раннюю, чем версия, указанная для дата-центра
Тип коммутатора	Тип коммутатора, используемый в кластере. Стандартным виртуальным коммутатором в РОСА Виртуализация 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. **Важно** – 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	Указывает порог журналирования для максимального потребления памяти в процентном или абсолютном значении в МБ. Сообщение записывается в журнал, если потребление памяти на хосте превышает процентное значение или если

Поле	Описание / действие
памяти	объем доступной на хосте памяти падает ниже абсолютного значения в МБ. 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 присоединенные хосты. Каждый из хостов импортируемого кластера должен соответствовать следующим требованиям: – Адрес – указать 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 – указать пароль root, необходимый для обмена информацией с хостом
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

3.3.2.3 Параметры оптимизации

3.3.2.3.1 Критерии для памяти

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

3.3.2.3.2 Критерии для ЦП

Для рабочей нагрузки **без серьезного 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 иначе 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 серьезным потреблением ресурсов ЦП необходимо использовать для ВМ ту же топологию, что и на хосте, чтобы и ВМ, и хост рассчитывали на одинаковое использование кеша. При включенной 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 кеш с другим гиперпотоком на том же ядре хоста, в то время как ВМ считает его отдельным ядром.

В таблице 35 описываются параметры вкладки "Оптимизация" в окнах "Новый кластер" и "Параметры кластера".

Таблица 35 – 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	Установка флажка "Симметричная многопоточность

Поле	Описание / Действие
многопоточность	отключена" отключает гиперпоточность
Потоки ЦП	Установка флажка "Считать потоки как ядра" дает хостам возможность запускать ВМ с общим числом ядер процессора, превышающим число ядер на хосте. Если этот параметр отмечен, то предоставляемые потоки хоста считаются ядрами, которые может использовать ВМ. Например, в системе с 24-мя ядрами и 2-мя потоками на ядро (всего 48 потоков) могут выполняться ВМ с числом ядер вплоть до 48, а алгоритмы для расчета 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" дает возможность MoM выполнять объединение одинаковых страниц памяти как при необходимости, так и тогда, когда выгода от

Поле	Описание / Действие
	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.

3.3.2.4 Политики миграции

В таблице 36 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.

Таблица 36 – 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 включен
Миграция пост-копирования	По аналогии с политикой минимального простоя ВМ не должны испытывать значительный простой. Политика пост-копирования сначала пытается выполнить предварительное 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 посткопирования по мере перемещения недостающих фрагментов памяти между хостами машина может значительно замедлиться. Если во время фазы пост-копирования что-то пойдет не так (например, случится сбой сети между хостами), то тогда

	процесс миграции приведет к утрате целостности, приостановке работы ВМ и к дальнейшей потере ВМ. Соответственно, прерывание миграции во время фазы пост-копирования невозможно.
Приостановить рабочую нагрузку при необходимости	Политика, дающая возможность миграции ВМ в большинстве ситуаций, включая серьезную рабочую нагрузку на ВМ. В связи с этим машины под серьезной рабочей нагрузкой могут простаивать в течение гораздо более долгого времени, чем с параметрами других политик. При экстремальных рабочих нагрузках миграция все еще может быть прервана. Механизм ловушек гостевого агента включен

Примечание — Если сетевое соединение будет потеряно до завершения посткопирования, то виртуализированный ЦУ приостановит и затем завершит основной процесс выполнения ВМ. Не следует использовать миграцию посткопирования при критической доступности ВМ или в нестабильной сети миграции.

В таблице 37 описываются параметры пропускной способности, которые определяют максимальную пропускную способность как входящих, так и исходящих миграций на каждый отдельный хост.

Таблица 37 – 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 учета и входящей, и исходящей миграции). Соответственно, пропускная способность, настроенная пользователем, должна быть достаточно

Политика	Описание
	высокой для учета 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 таблице 38 описываются параметры политики устойчивости, которые определяют приоритеты ВМ во время миграции.

Таблица 38 – 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 таблице 39 описываются дополнительные параметры, которые применяются к ВМ во время миграции.

Таблица 39 – Дополнительные параметры

Параметр	Описание
Включить шифрование при миграции	Параметр дает 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.

3.3.2.5 Политики планирования

Политики планирования дают возможность указать использование и распределение виртуальных машин между доступными хостами. Политику планирования необходимо настроить, чтобы включить автоматическую балансировку нагрузки для всех хостов в кластере. Вне зависимости от политики планирования, ВМ не начнет 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. 2.1.3).

В таблице 40 описываются параметры вкладки "Политики планирования".

Таблица 40 – Параметры вкладки "Политики планирования"

Поле	Описание / действие
Выберите политику	Выбрать 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, присоединенные 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

Поле	Описание / действие
	перезапущены. – power_saving (энергосбережение) – распределение памяти и нагрузки на вычислительные мощности ЦП внутри группы доступных хостов для снижения потребления энергии на недозагруженных хостах. Хосты с нагрузкой на ЦП 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, присоединенные 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, если 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

Поле	Описание / действие
	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 или если в кластере будет недостаточно свободных хостов. Значение по умолчанию — "20". – ScaleDown – снижает влияние весовой функции на Reservation путем 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

Поле	Описание / действие
	умолчанию — "верно" (true). – MaxFreeMemoryForOverUtilized – указывает минимальный размер свободной памяти (в МБ), требуемый для минимального уровня обслуживания. Если объем 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 объем 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. Во избежание непредсказуемого поведения при указании значения для параметра MaxFreeMemoryForOverUtilized необходимо также указывать значение и для параметра MinFreeMemoryForUnderUtilized. – MinFreeMemoryForUnderUtilized – указывает минимальный размер свободной памяти (в МБ), требуемый для того, чтобы хост считался низкозагруженным. Если объем 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. Во избежание непредсказуемого поведения при указании значения для параметра MaxFreeMemoryForOverUtilized необходимо также указывать значение и для параметра MinFreeMemoryForUnderUtilized.

Поле	Описание / действие
	– HeSparesCount – указывает число дополнительных узлов виртуализированного ЦУ, на которых должна быть зарезервирована память в объеме, 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 объема свободной памяти для ВМ виртуализированного ЦУ, то эти машины не начнут работу. Это дополнительный параметр, который можно добавить к политикам power_saving, vm_evenly_distributed 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, использовать 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 дает возможность задать политику серийных номеров для ВМ в кластере. Выбрать 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 – дает возможность пользователю указать произвольный

Поле	Описание / действие
	порядковый номер в качестве серийного номера ВМ

Если объем 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.

3.3.2.6 Параметры консоли кластера

В таблице 41 описываются параметры вкладки "Консоль" в окнах "Новый кластер" и "Параметры кластера".

Таблица 41 – 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	Установить этот флажок, чтобы включить TLS по протоколу X509VNC

3.3.2.7 Параметры политики операций блокады

В таблице 42 описываются параметры вкладки "Политика операций блокады" в окнах "Новый кластер" и "Параметры кластера".

Таблица 42 – 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 ее можно отключить (например, если возникают или ожидаются временные проблемы с сетью, то администратор может отключить возможность проведения операций блокады до завершения действий по диагностике или обслуживанию). **Следует обратить внимание**, что при

Поле	Описание / действие
	отключенной 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 подключенных 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 включенных 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 включенных возможностях хранилища Gluster. При выбранном параметре операция блокады будет пропускаться при работающих элементах (кирпичах), а выключение хоста приведет к потере кворума

3.3.2.8 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 необходимо настроить политику планирования (см. п. 2.1.3).

Для настройки политик управления нагрузкой и энергосбережения на хосте нужно выполнить следующие действия:

а) перейти в "Ресурсы → Кластеры" и выбрать кластер;

б) нажать кнопку Изменить;

в) перейти на вкладку "Политика планирования" (рисунок 113);

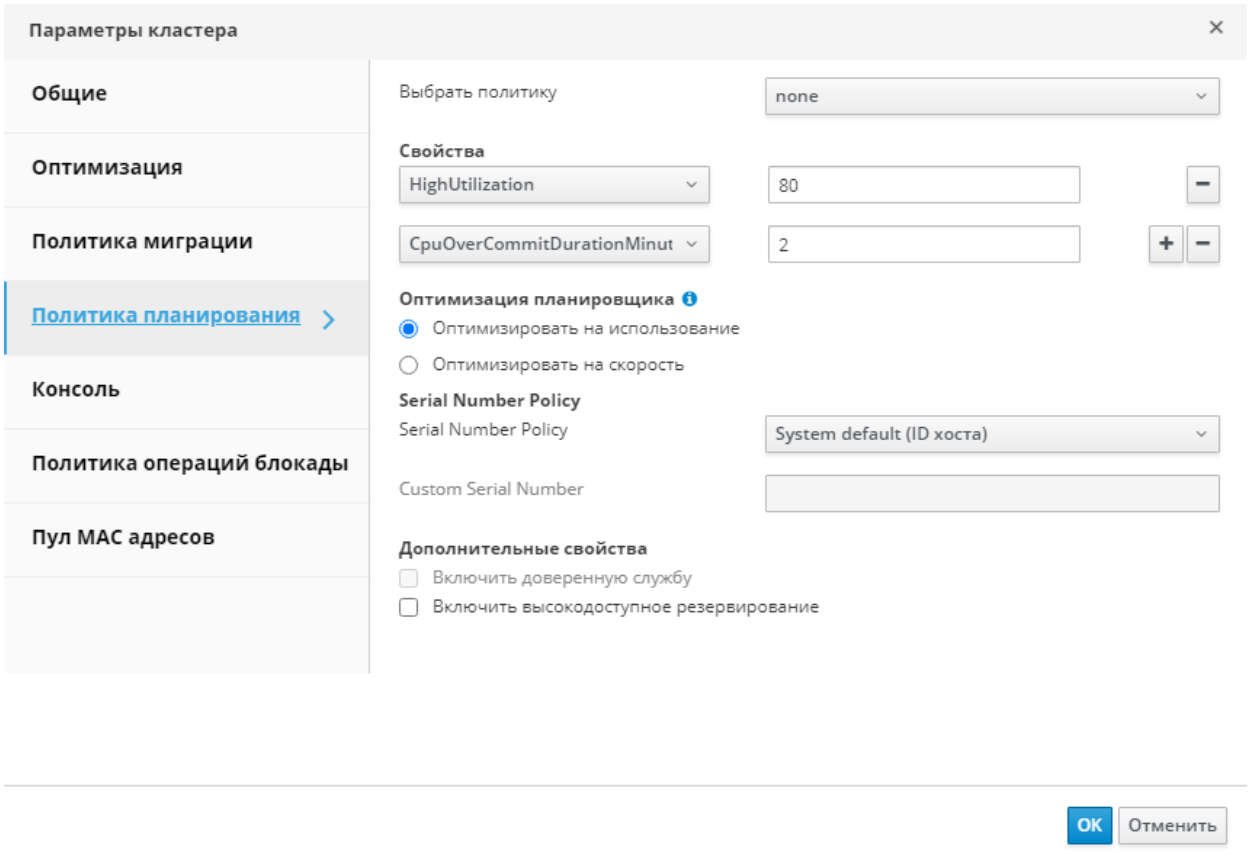


Рисунок 113 – Политика планирования

г) выбрать одну из следующих политик:

– нет;

– vm_evenly_distributed:

– в поле HighVmCount указать минимальное число ВМ, выполняющихся на одном хосте и необходимых для включения балансировки нагрузки;
– в поле MigrationThreshold указать максимальную приемлемую разницу между числом ВМ на самом загруженном хосте и числом ВМ на самом незагруженном хосте;
– в поле SpmVmGrace указать число слотов для ВМ, которое должно быть зарезервировано на хостах SPM;
– при необходимости в поле HeSparesCount указать число дополнительных узлов виртуализированного ЦУ, на которых нужно зарезервировать объем свободной памяти, достаточный для запуска ВМ виртуализированного ЦУ в случае миграции этой ВМ или выключения;

– evenly_distributed:

– в поле CpuOverCommitDurationMinutes указать время (в минутах), в течение которого нагрузка на ЦП хоста может превышать настроенные значения нагрузки перед тем как будет применена политика планирования;
– в поле HighUtilization указать процентное значение нагрузки на ЦП, при котором ВМ будут начинать миграцию на другие хосты;
– в поле MinFreeMemoryForUnderUtilized указать минимальный объем свободной памяти в МБ, при превышении которого ВМ начнут мигрировать на другие хосты;
– в поле MaxFreeMemoryForOverUtilized указать максимальный требуемый объем свободной памяти, при значении меньше которого ВМ начнут миграцию на другие хосты;
– при необходимости в поле HeSparesCount указать число дополнительных узлов виртуализированного ЦУ, на которых нужно зарезервировать объем свободной памяти, достаточный для запуска ВМ виртуализированного ЦУ в случае миграции этой ВМ или выключения;

– power_saving:

– в поле CpuOverCommitDurationMinutes указать время (в минутах), в течение которого нагрузка на ЦП хоста может превышать настроенные значения нагрузки перед тем как будет применена политика планирования;

– в поле LowUtilization указать процент загруженности ЦП, при значении меньше которого хост будет считаться недозагруженным;
– в поле HighUtilization указать процентное значение нагрузки на ЦП, при достижении которого ВМ начнут миграцию на другие хосты;
– в поле MinFreeMemoryForUnderUtilized указать минимальный объем свободной памяти в МБ, при превышении которого ВМ начнут миграцию на другие хосты;
– в поле MaxFreeMemoryForOverUtilized указать максимальный требуемый объем свободной памяти, при значении меньше которого ВМ начнут миграцию на другие хосты;
– при необходимости в поле HeSparesCount указать число дополнительных узлов виртуализированного ЦУ, на которых нужно зарезервировать объем свободной памяти, достаточный для запуска ВМ виртуализированного ЦУ в случае миграции этой ВМ или выключения;

д) выбрать 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;

е) если для верификации хостов используется сервер OpenAttestation, и его конфигурация была настроена с помощью утилиты engine-config, то установить флажок "Включить доверенную службу";

ж) при необходимости установить флажок "Включить высокодоступное резервирование", чтобы виртуализированный ЦУ мог обеспечивать доступность ресурсов в кластере для отказоустойчивых ВМ;

з) при необходимости выбрать 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 указать произвольный порядковый номер (в качестве серийного номера ВМ) в текстовом поле интерфейса;

и) нажать кнопку OK.

3.3.2.9 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 снятия режима обслуживания. Тем не менее при необходимости применить важные изменения можно немедленно, выполнив синхронизацию политики превышенного выделения памяти для хостов, еще имеющих статус "Запущен".

Следующая последовательность действий для синхронизации политики превышенного выделения памяти на хосте должна выполняться на каждом из хостов индивидуально:

а) перейти в "Ресурсы → Кластеры";

б) нажать на название кластера, чтобы открыть подробный просмотр;

в) перейти на вкладку "Хосты" и выбрать хост, для которого нужно обновить политику MoM;

г) нажать кнопку `Синхронизировать политику MoM`.

Информация о политике MoM на хосте будет обновлена без необходимости перемещения хоста в режим обслуживания и после этого обратно в состояние "Запущен".

3.3.2.10 Создание профиля ЦП

Профили ЦП определяют максимальный объем вычислительных возможностей хоста, к которым может получить доступ выполняемая на этом хосте ВМ в составе кластера. Максимальный объем 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.

Для создания профиля ЦП нужно:

а) перейти в "Ресурсы → Кластеры";
б) нажать на название кластера, чтобы открыть подробный просмотр;
в) перейти на вкладку "Профили ЦП";
г) нажать кнопку `Добавить`;
д) указать "Имя" и "Описание" профиля ЦП;
е) из списка "QoS" выбрать запись о качестве обслуживания, которую необходимо применить к профилю ЦП;
ж) нажать кнопку `OK`.

3.3.2.11 Удаление профиля ЦП

Для удаления профиля ЦП требуется:

а) перейти в "Ресурсы → Кластеры";
б) нажать на название кластера, чтобы открыть подробный просмотр;
в) перейти на вкладку "Профили ЦП" и выбрать удаляемый профиль ЦП;
г) нажать кнопку `Удалить`;
д) нажать кнопку `OK`.

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

3.3.2.12 Импорт существующего кластера хранилища Gluster

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

При указании таких параметров, 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 импорт кластера будет невозможно.

Для импорта существующего хранилища Gluster в виртуализированный ЦУ нужно:

а) перейти в "Ресурсы → Кластеры";

б) нажать кнопку Добавить;

в) выбрать "Дата-центр", к которому будет принадлежать кластер;

г) указать "Имя" и "Описание" кластера;

д) установить 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");

з) В поле "Имя" хоста указать 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";

е) указать "Пароль" (пароль сервера) и нажать кнопку OK;

ж) в открывшемся окне "Добавить хосты" со списком хостов в составе кластера для каждого хоста указать "Имя" и "Пароль" root;

з) в случае использования одного и того же пароля для всех хостов установить флажок "Использовать общий пароль" и указать этот пароль в текстовом поле;

и) нажать кнопку Применить, чтобы установить введенный пароль для всех хостов;

к) проверить подлинность всех отпечатков и нажать кнопку OK для применения изменений.

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

3.3.2.13 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 таблице 43 описываются параметры хранилища Gluster в окне "Добавить хосты".

Таблица 43 – Параметры Gluster

Параметр (поле)	Описание
Использовать общий	Установить этот флажок, чтобы для всех хостов в кластере

Параметр (поле)	Описание
пароль	использовался один и тот же пароль. Ввести необходимый пароль в поле "Пароль", затем нажать на кнопку Применить, чтобы установить пароль для всех хостов
Имя	Указать 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, ввести 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"

3.3.2.14 Удаление кластеров

Перед удалением кластера необходимо переместить из него все хосты.

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

Для удаления кластера нужно:

а) перейти в "Ресурсы → Кластеры" и выбрать кластер;
б) убедиться в том, что в кластере нет хостов;
в) нажать кнопку Удалить;
г) нажать кнопку OK.

3.3.2.15 Оптимизация памяти

Для увеличения числа виртуальных машин на хосте можно использовать **превышенное выделение памяти**, при котором объем памяти, выделяемый машине, превышает доступный объем 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 объемный 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).

3.3.2.15.1 Превышенное выделение памяти

Объем превышенного выделения памяти можно ограничить с помощью одного из процентных значений параметра "Оптимизация памяти": "Нет" (0%), "150%" или "200%".

Например, для хоста с 64 ГБ ОЗУ выбор значения в "150%" означает, что превысить выделение памяти можно на дополнительные 32 ГБ, получив всего 96 ГБ виртуальной памяти. Если хост использует 4 ГБ от этого общего объема, то будут доступны оставшиеся 92 ГБ. Большую часть от этого объема можно выделить виртуальной машине (секция "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 следует выбрать лимит, соответствующий следующим типам выполняемых приложений и рабочих нагрузок:

– Для рабочих нагрузок, создающих наиболее значимый постепенный прирост запросов памяти, выбрать более высокий процент, например "200%" или "150%".

– Для критически важных приложений или рабочих нагрузок, создающих внезапные скачки запросов памяти, выбрать более низкое процентное значение, например "150%" или "Нет". Выбор значения "Нет" помогает предотвратить превышенное выделение памяти, но одновременно дает возможность MoM, устройствам вытеснения памяти и KSM продолжать работу по оптимизации виртуальной памяти.

Важно — Перед оптимизацией памяти в рабочей среде всегда сначала нужно провести стресс-тестирование при самых разных условиях.

Чтобы настроить параметры оптимизации памяти, нужно перейти на вкладку "Оптимизация" в окнах "Новый кластер" или "Параметры кластера" (см. п. 3.3.2.3).

Примечания:

– Фактический объем доступной памяти невозможно определить в реальном времени, поскольку объем оптимизации памяти, достигаемый KSM, и объем 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 отсчета следует использовать максимальный объем виртуальной памяти (размер физической памяти и параметр "Оптимизация памяти"). Не рекомендуется использовать в расчетах более низкий объем памяти, достигаемый за счет оптимизации с помощью вытеснения памяти и KSM.

3.3.2.15.2 Раздел подкачки

В таблице 44 приведены общие рекомендации по настройке раздела подкачки.

Таблица 44 – Общие рекомендации по настройке раздела подкачки

Объем ОЗУ	Рекомендуемый размер раздела подкачки	Рекомендуемый размер раздела подкачки (при использовании гибернации)
2 ГБ или меньше	Двойной объем ОЗУ	Тройной объем ОЗУ
2 ГБ – 8 ГБ	Объем, равный объему	Двойной объем ОЗУ

Объем ОЗУ	Рекомендуемый размер раздела подкачки	Рекомендуемый размер раздела подкачки (при использовании гибернации)
	ОЗУ	
8 ГБ – 64 ГБ	Минимум 4 ГБ	Полуторный объем ОЗУ
64 ГБ или больше	Минимум 4 ГБ	Гибернация не рекомендуется

Примечание — Для систем с числом логических процессоров, превышающим 140, или с объемом ОЗУ более 3 ТБ рекомендованный размер раздела подкачки составляет не менее 100 ГБ.

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 объема 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 дает возможность выгрузить память на диск для отсрочки или предотвращения прерывания работы приложения программой-уничтожителем OOM.

– Приложение могло создаваться с учетом 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 объема подкачки может повлиять на возрастающие число обращений к памяти этим процессом, что в итоге сначала приведет 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 объем памяти, в который пишет этот процесс, не превышает объем доступной подкачки, то система просто испытает временное замедление работы.

Применяя данные рекомендации, следует:

– устанавливать размер раздела подкачки в качестве "последней возможности" для наихудшего возможного сценария;

– использовать размер физической памяти и параметр "Оптимизация памяти" в качестве базы для расчета общего объема виртуальной памяти;

– не включать в эти расчеты 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, рекомендуется создавать раздел подкачки достаточно большим из расчета на наихудший возможный сценарий и учитывать резерв для запаса прочности.

3.3.2.15.3 Диспетчер превышенного выделения памяти MoM

Диспетчер превышенного выделения памяти MoM выполняет следующие основные функции:

– ограничивает превышенное выделение памяти путем применения установленного значения параметра "Оптимизация памяти" к хостам в кластере;

– оптимизирует память, управляя процессами вытеснения памяти (ballooning) и объединения одинаковых страниц памяти ядром (KSM);

– не нуждается во включении или отключении.

Если объем 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.

3.3.2.15.4 Вытеснение памяти (ballooning)

Виртуальные машины начинают работу, располагая полным объемом выделенной виртуальной памяти. По мере того как потребление виртуальной памяти превышает объем ОЗУ, хост все больше и больше начинает использовать механизм подкачки. Активированная процедура **вытеснения памяти** заставляет ВМ отдать неиспользуемую часть памяти. Освобожденная память может быть повторно использована другими процессами и другими ВМ на хосте. По причине сокращения объема 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 черный 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 объема виртуальной памяти.

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 объем этого потребления не изменяется).

Чтобы включить механизм вытеснения памяти, нужно перейти на вкладку "Оптимизация" в окне "Новый кластер" или "Параметры кластера". Затем необходимо установить 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. 3.3.2.3).

Каждый хост в данном кластере получает обновление политики вытеснения памяти при смене статуса этого хоста на "Запущен". При необходимости можно обновить информацию о политике вытеснения памяти на хосте без смены статуса (см. п. 3.3.2.9).

3.3.2.15.5 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 остается включенным, 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 скорее всего хост именно ее сохранит в кеше 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. Объем потребляемых KSM ресурсов остается неизменным и в критических условиях. Выполнение одинаковых ВМ и приложений на хосте дает 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.

Примечания:

– После того как KSM объединит большой объем памяти, статистика подсчета памяти, собираемая ядром, может в итоге не отражать реальной картины. Если в Системе присутствует большой объем 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, необходимо перейти на вкладку "Оптимизация" в окне "Новый кластер" или "Параметры кластера", затем установить 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. 3.3.2.3).

3.3.2.16 Изменение версии совместимости кластера

Кластеры в РОСА Виртуализация 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. Следует проверить наличие рядом с хостом значка, обозначающего возможность обновления версии.

Для изменения версии совместимости кластера нужно:

а) в главном меню Портала администрирования перейти в "Ресурсы → Кластеры";

б) выбрать кластер и нажать кнопку Изменить;

в) на вкладке "Общее" изменить "Версию совместимости" на необходимое значение;

г) нажать кнопку OK.

Примечание — Существует вероятность появления сообщения, предупреждающего о некорректной конфигурации некоторых ВМ и шаблонов. Чтобы исправить эту ошибку, следует отредактировать 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 еще 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.

3.4 Логические сети

3.4.1 Задачи при работе с логическими сетями

3.4.1.1 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 соответственно создавать, изменять свойства и удалять логические сети в рамках дата-центра.

При нажатии на имя каждой из сети и при переходе по вкладкам в подробном просмотре можно выполнять следующие действия:

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

Если узлы РОСА Виртуализация планируется использовать для предоставления каких-либо служб, следует учитывать, что службы остановятся, если окружение виртуализации прекратит работать. Это касается всех служб, но особенно четко нужно понимать риски выполнения следующих служб в окружении виртуализации:

– Службы каталогов;
– DNS;
– Хранилище.

3.4.1.2 Создание новой логической сети в дата-центре или кластере

Для создания логической сети и настройки ее использования в дата-центре или в кластерах дата-центра нужно выполнить следующие действия:

а) перейти в "Ресурсы → Дата-центры" или "Ресурсы → Кластеры";
б) нажать на название дата-центра или кластера, чтобы открыть подробный просмотр;
в) перейти на вкладку "Логические сети";
г) открыть окно "Новая логическая сеть" (рисунок 114):

– в подробном просмотре дата-центра нажать кнопку Добавить;
– в подробном просмотре кластера нажать кнопку Добавить сеть;

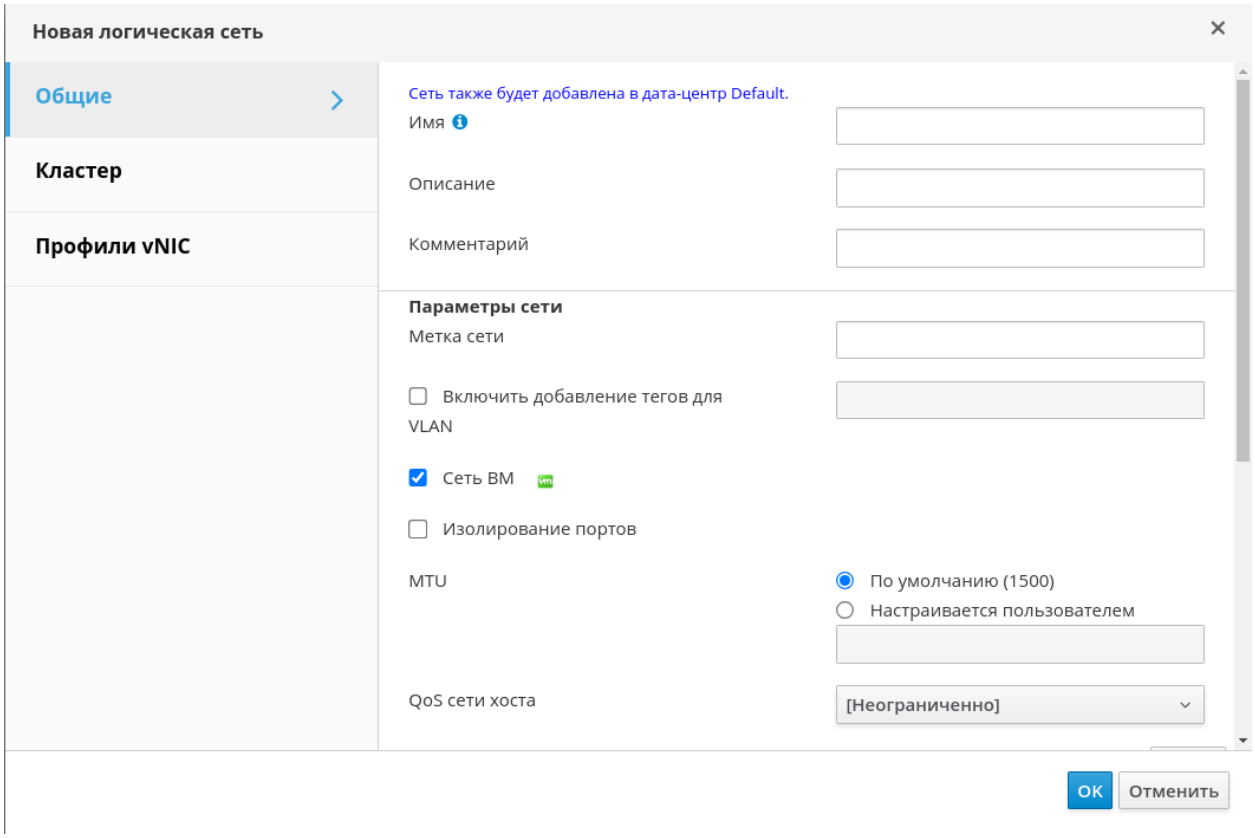


Рисунок 114 – Новая логическая сеть

д) указать "Имя", "Описание" и "Комментарий" для логической сети;

е) опционально включить параметр "Включить добавление тегов для VLAN";

ж) опционально отключить параметр "Сеть ВМ";

з) опционально включить параметр "Изолирование портов", чтобы ВМ не могли обмениваться данными в логической сети;

и) опционально включить параметр "Создать на внешнем поставщике". Таким образом будут отключены параметры "Метка сети", "Сеть ВМ" и "MTU";

к) выбрать "Внешнего поставщика" (в список "Внешний поставщик" не включены внешние поставщики с режимом read-only);

л) чтобы создать внутреннюю изолированную сеть, выбрать в списке "Внешний поставщик" опцию "ovirt-provider-ovn" и не отмечать параметр "Подключиться к физической сети";

л) в поле "Метка сети" ввести новую метку логической сети или выбрать уже существующую;

м) указать значение "MTU" – "По умолчанию (1500)" или "Пользовательское";

н) при выборе в списке "Внешний поставщик" опции "ovirt-provider-ovn" указать необходимость применения в сети "Группы безопасности";

о) во вкладке "Кластер" выбрать кластеры, которым будет присвоена сеть. Также можно указать, будет ли эта логическая сеть необходимой;

п) при выборе пункта "Создать внешнего поставщика" станет видимой вкладка "Подсеть"; указать в этой вкладке "Имя", "CIDR" и "Шлюз". При необходимости можно добавить серверы DNS;

р) во вкладке "Профили vNIC" добавить профили требуемых виртуальных NIC к логической сети;

с) нажать кнопку 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 внесенных изменений, необходимо перезапустить любые выполняющиеся ВМ, использующие эти сети.

3.4.1.3 Изменение параметров логических сетей

Для изменения параметров логической сети нужно:

а) перейти в "Ресурсы → Дата-центры";
б) нажать на название дата-центра, чтобы открыть подробный просмотр;
в) перейти на вкладку "Логические сети" и выбрать логическую сеть;
г) нажать кнопку Параметры;
д) внести необходимые изменения параметров (рисунок 115);

Примечания:

– 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. в п. 3.4.4.4.

– Можно изменить название новой или существующей сети без остановки работы ВМ для всех сетей, кроме сети по умолчанию.

е) нажать кнопку OK.

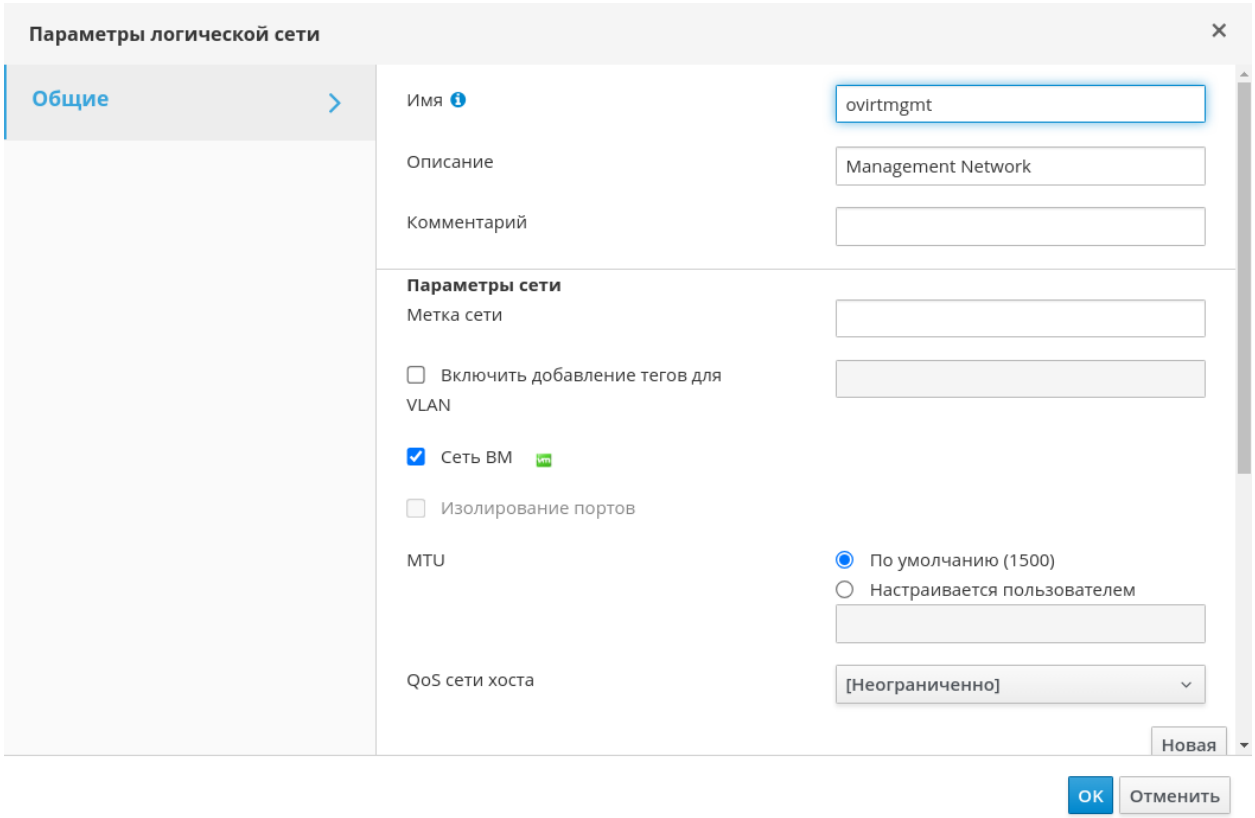


Рисунок 115 – Изменение параметров логической сети

Примечание — В сетевой конфигурации с поддержкой нескольких хостов обновленные 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.

3.4.1.4 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 РОСА Виртуализация необходима как минимум одна логическая сеть, используемая в качестве сети управления ovirtmgmt.

Для удаления логической сети нужно:

а) перейти в "Ресурсы → Дата-центры";

б) нажать на название дата-центра, чтобы открыть подробный просмотр;

в) перейти на вкладку "Логические сети", чтобы просмотреть список логических сетей в дата-центре;

г) выбрать логическую сеть и нажать кнопку Удалить;

д) опционально установить 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;

е) нажать кнопку OK.

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

3.4.1.5 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 прикрепленных хостах.

Для настройки логической сети в качестве маршрута по умолчанию нужно:

а) перейти в "Сеть → Сети";

б) нажать на название логической сети без функции управления (рисунок 116), которая будет настраиваться в качестве маршрута по умолчанию, чтобы перейти к подробному просмотру;

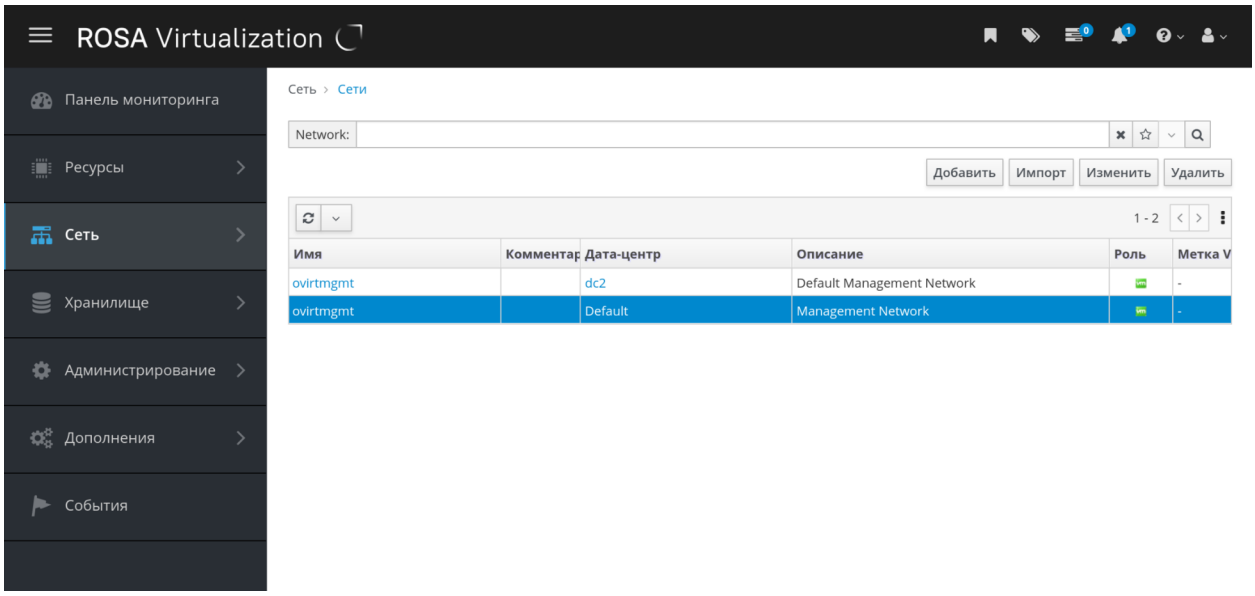


Рисунок 116 – Форма "Сеть → Сети"

Обзор параметров сети ovirtmgmt приведен на рисунке 117.

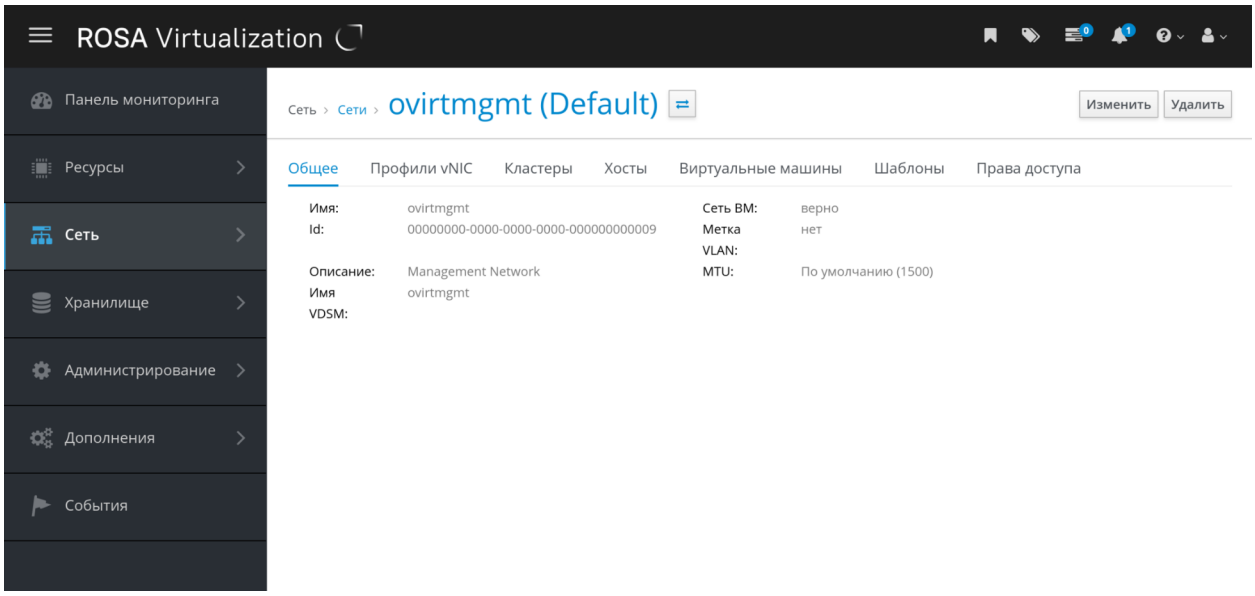


Рисунок 117 – Сеть ovirtmgmt (Default)

в) перейти на вкладку "Кластеры" (рисунок 118);

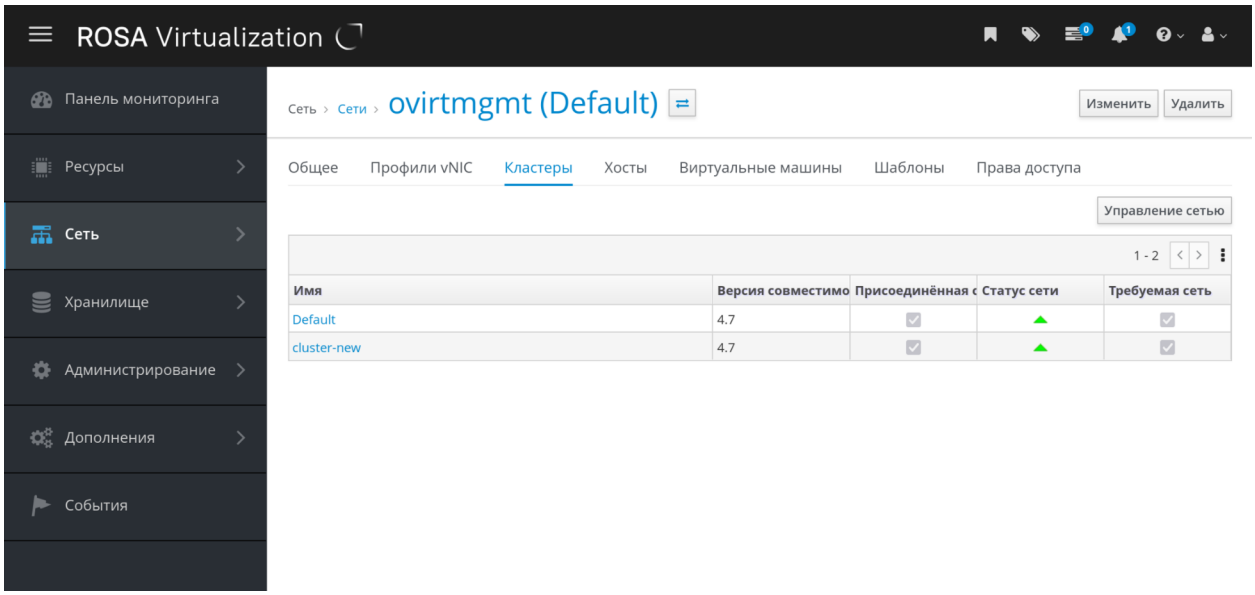


Рисунок 118 – "Сети" – вкладка "Кластеры"

г) нажать "Управление сетью", чтобы открыть окно "Управление сетью" (рисунок 119);

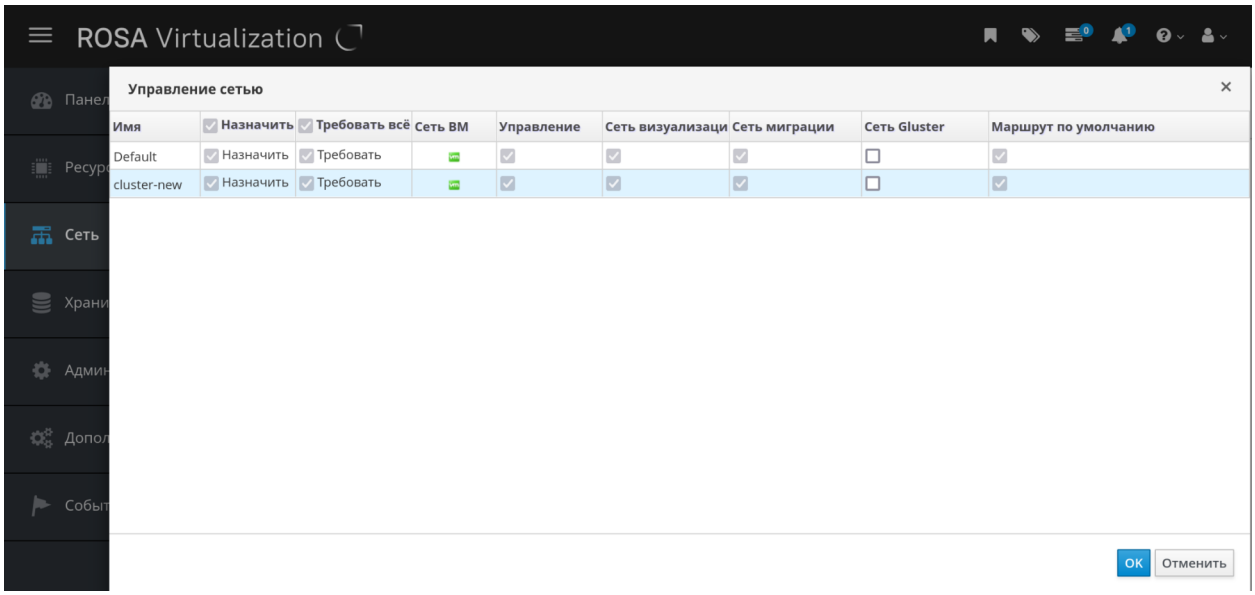


Рисунок 119 – Окно "Управление сетью"

д) установить флажок "Маршрут по умолчанию" для соответствующего кластера;

е) нажать кнопку OK.

Когда сети будут присоединяться к хостам, маршрут хоста по умолчанию 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.
```

3.4.1.6 Просмотр или редактирование параметров шлюза логической сети

Для логической сети можно настроить шлюз, IP-адрес и маску подсети. Это необходимо, если 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 РОСА Виртуализация автоматически обрабатывает несколько шлюзов всякий раз, когда интерфейс начинает или завершает работу.

Для просмотра или редактирования параметров шлюза логической сети нужно:

а) перейти в "Ресурсы → Хосты";

б) нажать на имя хоста, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Сетевые интерфейсы", чтобы увидеть список и параметры сетевых интерфейсов, подключенных к хосту (рисунок 120);

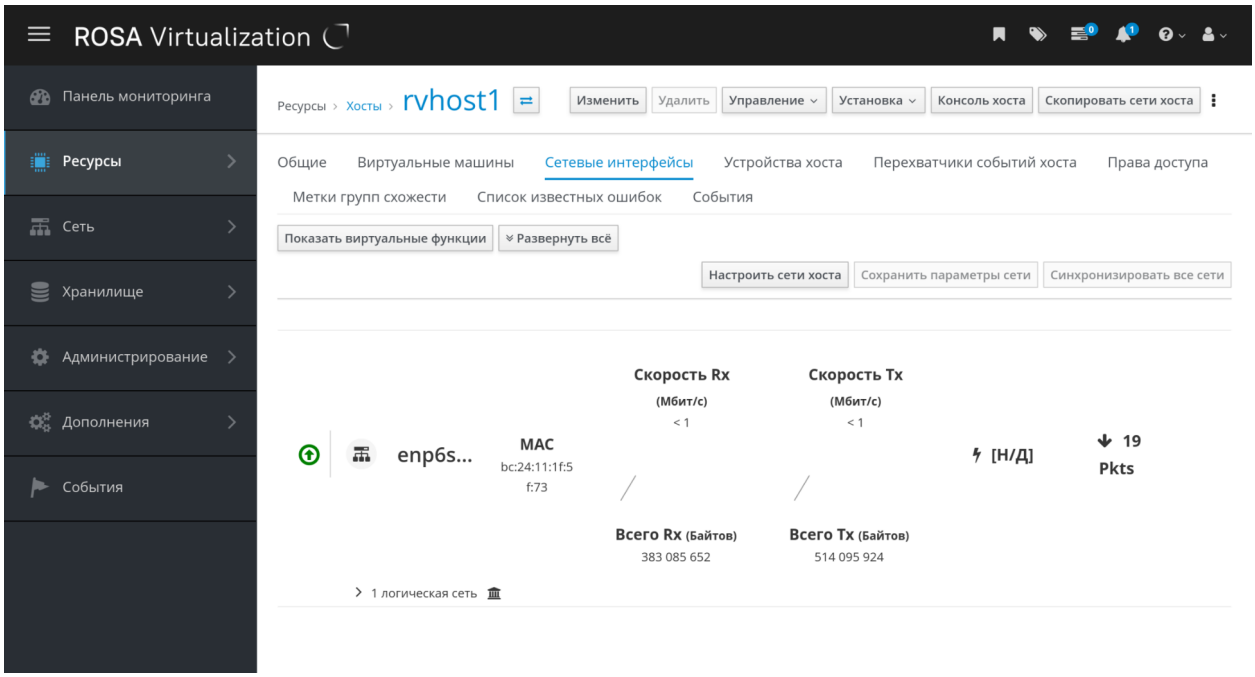


Рисунок 120 – Вкладка "Сетевые интерфейсы" с параметрами сетевых интерфейсов, подключенных к хосту

г) нажать кнопку "Настроить сети хоста", и откроется форма для настройки сетей выбранного хоста (рисунок 121);

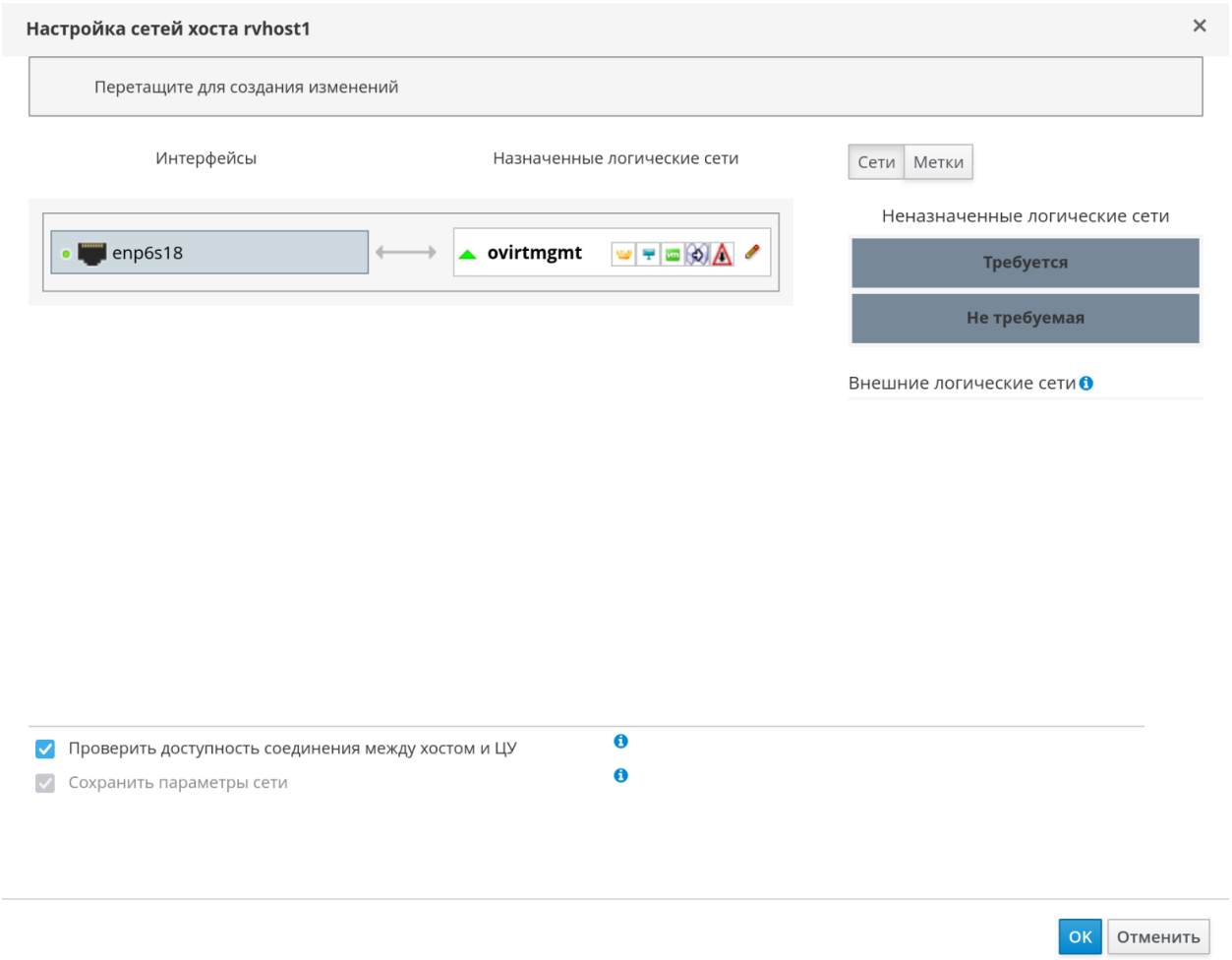


Рисунок 121 – Форма "Настройка сетей хоста"

д) навести курсор на присвоенную логическую сеть и нажать на пиктограмму (карандаш) (рисунок 122), чтобы открыть окно "Изменить сеть управления";

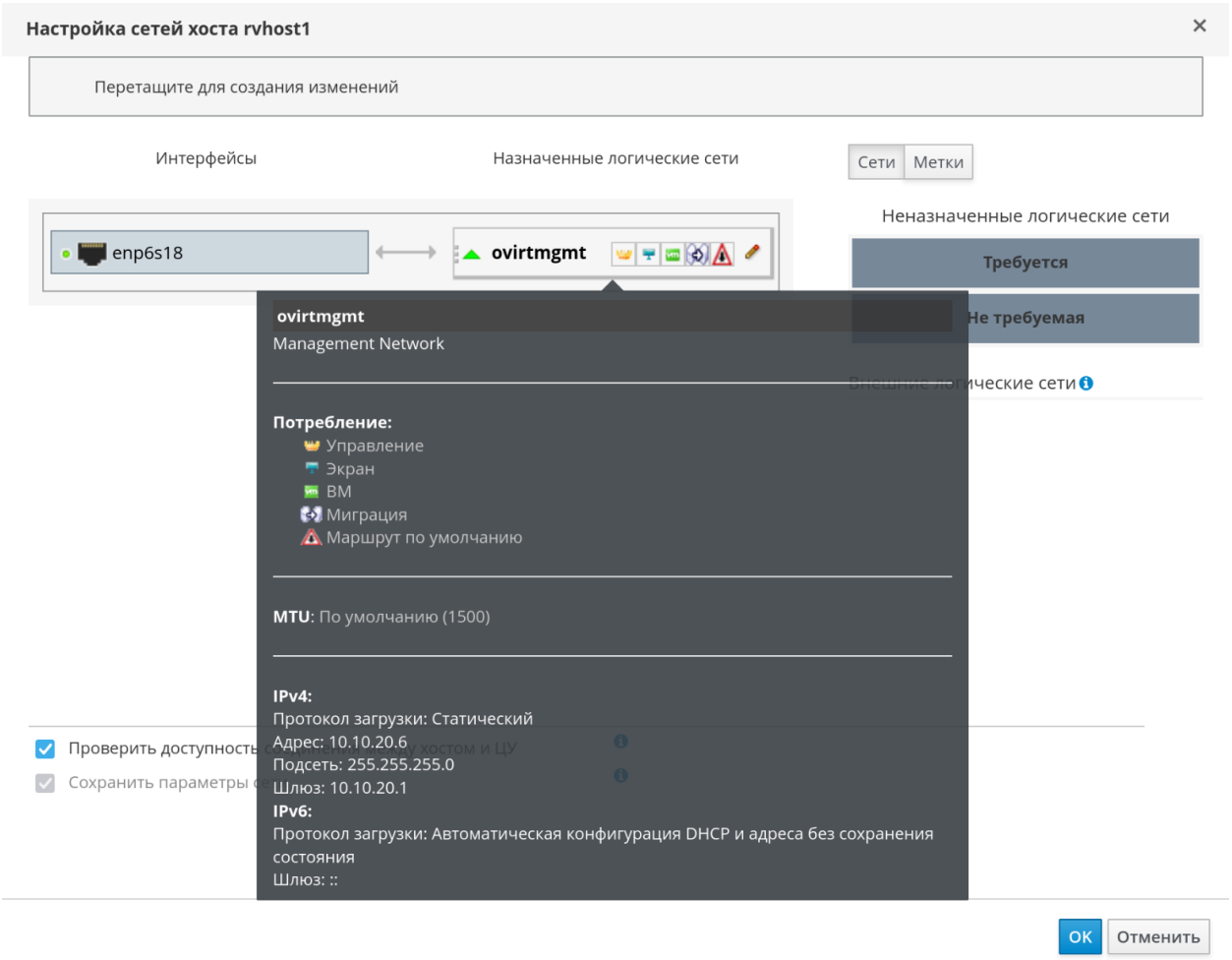


Рисунок 122 – Информация о настроенной сети ovirtmgmt

е) в окне "Изменить сеть управления" (рисунок 123) показывается имя сети, протокол загрузки, а также IP-адреса, маски подсети и шлюза. Для изменения сведений об адресах вручную выбрать "Статический" протокол загрузки;

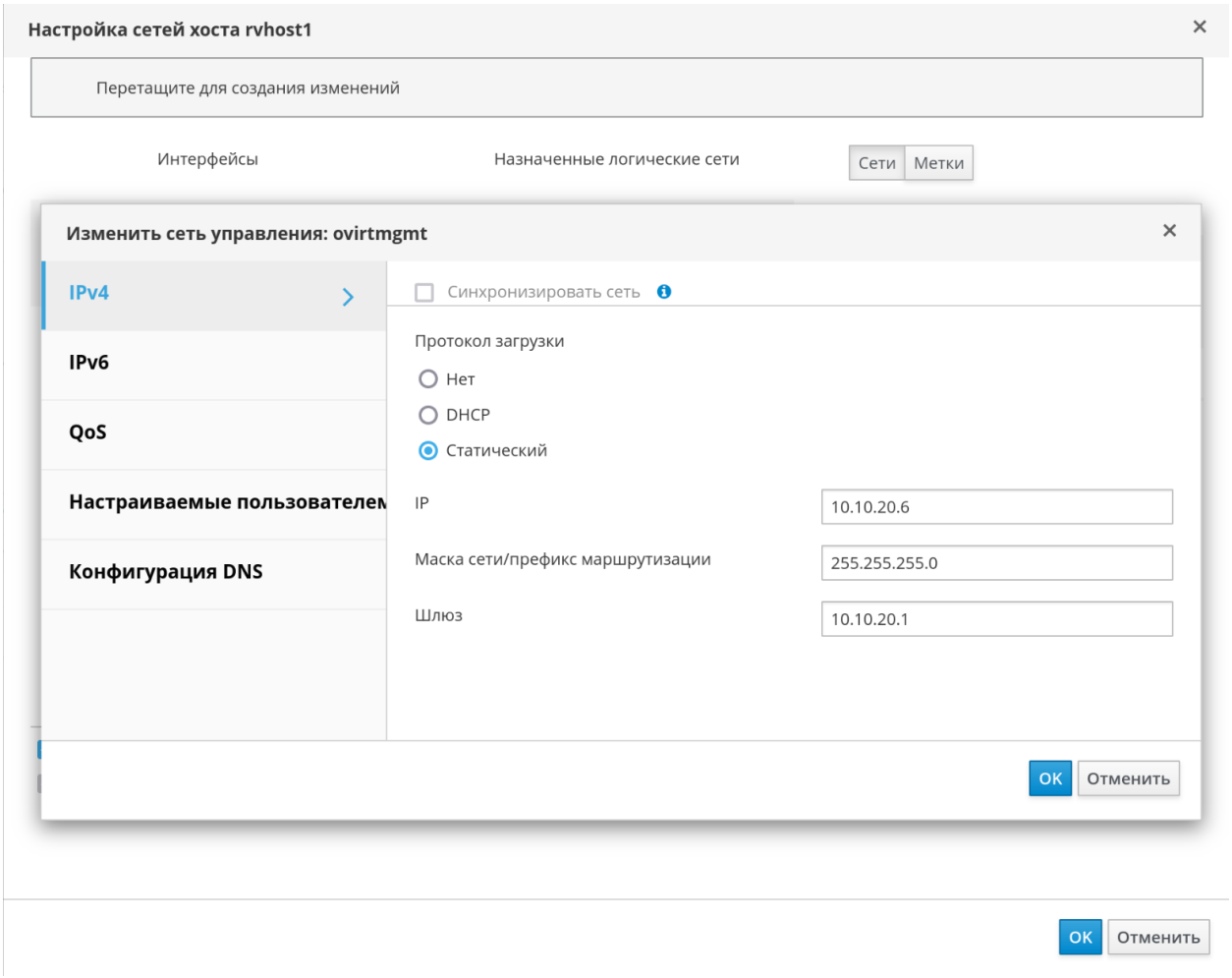


Рисунок 123 – Форма "Изменить сеть управления"

3.4.1.7 Общие параметры логической сети

В таблице 45 описываются параметры вкладки "Общие" в окнах "Новая логическая сеть" и "Параметры логической сети".

Таблица 45 – 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

Поле	Описание
	нижнего подчеркивания. **Следует обратить 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
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 дает возможность одному сетевому интерфейсу быть связанным с несколькими логическими сетями, имеющими разные метки VLAN. Если метки VLAN включены, ввести числовое значение в данное текстовое поле
Сеть ВМ	Отметить этот параметр, если эту сеть используют только ВМ. Если трафик, для передачи которого используется эта сеть, создается не виртуальными машинами (например, обмен информацией между хранилищами), не отмечать этот параметр
MTU	Выбрать 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" указать необходимое число в

Поле	Описание
	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 создается 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

3.4.1.8 Параметры кластеров при настройке логических сетей

В таблице 46 описываются параметры вкладки "Кластер" окна "Новая логическая сеть".

Таблица 46 – 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

Поле	Описание
	названием каждого кластера напротив параметра "Требуемая"

3.4.1.9 Параметры профилей vNIC при настройке логических сетей

В таблице 47 описываются параметры вкладки "Профили vNIC" окна "Новая логическая сеть".

Таблица 47 – 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, нажать соответственно значок + или – 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.

3.4.1.10 Настройка конкретного типа трафика для логической сети в окне "Управление сетями"

Тип трафика в логической сети указывается для оптимизации потока сетевого трафика.

Для настройки типов трафика для логических сетей нужно:

а) перейти в "Ресурсы → Кластеры";
б) нажать на имя кластера, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Логические сети";
г) нажать кнопку Управление сетями;
д) установить необходимые флажки и настроить переключатели (рисунок 124);
е) нажать кнопку OK.

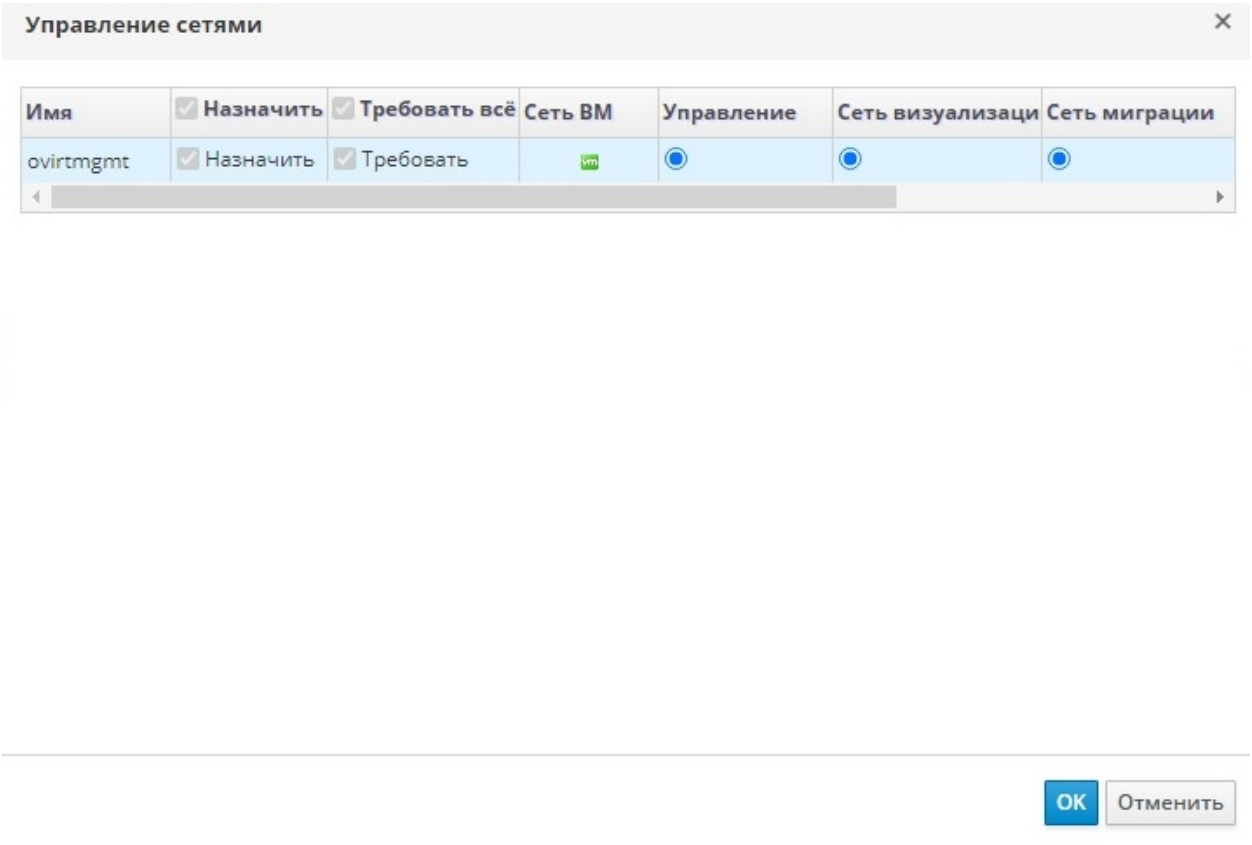


Рисунок 124 – Управление сетями

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

3.4.1.11 Параметры в окне "Управление сетями"

В таблице 48 описываются параметры в окне "Управление сетями".

Таблица 48 – 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 перестает 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 произойдет сбой, то вместо нее будет использована сеть управления (по умолчанию – ovirtmgmt)

3.4.1.12 Изменение конфигурации виртуальной функции сетевой платы

В данном пункте описывается, как установить и настроить технологию виртуализации ввода-вывода с единым корнем (SR-IOV) в РОСА Виртуализация. Дополнительные сведения приведены в п. 3.4.4.

Технология виртуализации ввода-вывода с единым корнем (SR-IOV) дает возможность использования одного устройства 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 еще 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 разрешен 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. 3.4.2.4).

Для редактирования конфигурации виртуальной функции сетевой платы нужно выполнить следующие действия:

а) перейти в "Ресурсы → Хосты";

б) нажать на название хоста с поддержкой SR-IOV, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Сетевые интерфейсы";

г) нажать кнопку Настроить сети хоста;

д) выбрать сетевую карту с поддержкой SR-IOV (отмечается значком 

) и нажать на пиктограмму  (карандаш);

е) чтобы изменить число виртуальных функций, нажать кнопку Параметр числа виртуальных функций и изменить 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.

ж) флажок для параметра "Все сети" проставлен по умолчанию, что разрешает возможность доступа к виртуальным функциям для всех сетей. Чтобы указать отдельные виртуальные сети, которым разрешен доступ к виртуальным функциям, выбрать 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;

з) нажать кнопку OK;

и) в окне "Настроить сети хоста" нажать кнопку ОК.

3.4.2 Виртуальные сетевые платы (vNIC)

3.4.2.1 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 дает 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.

3.4.2.2 Создание или изменение профиля vNIC

Профиль виртуальной сетевой платы создается или изменяется 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.

Для создания или редактирования профиля vNIC нужно выполнить следующие действия:

а) перейти в "Сеть → Сети";

б) нажать на имя логической сети, чтобы перейти к подробному просмотру;

в) нажать на кнопку Изменить, чтобы открыть для просмотра форму "Параметры логической сети" (рисунок 125);

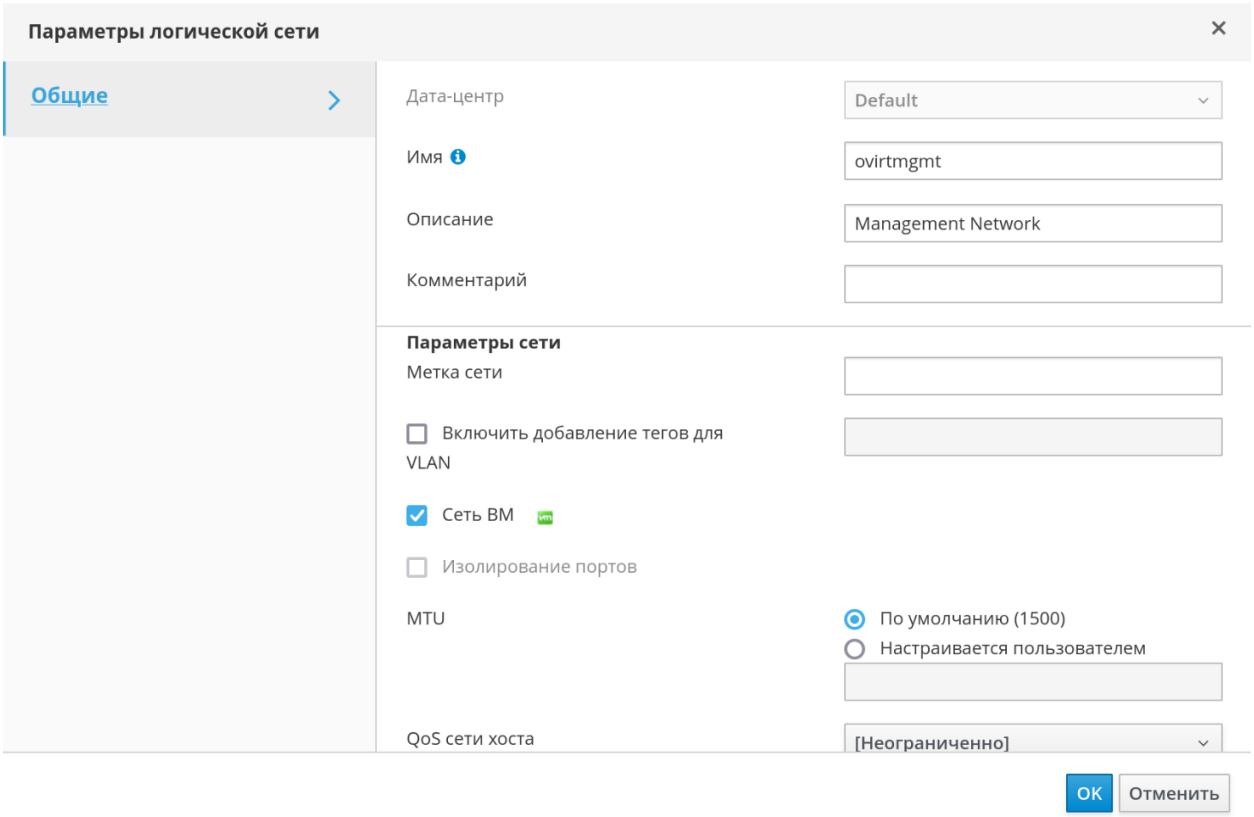


Рисунок 125 – Форма "Параметры логической сети"

г) перейти на вкладку "Профили vNIC" (рисунок 126);

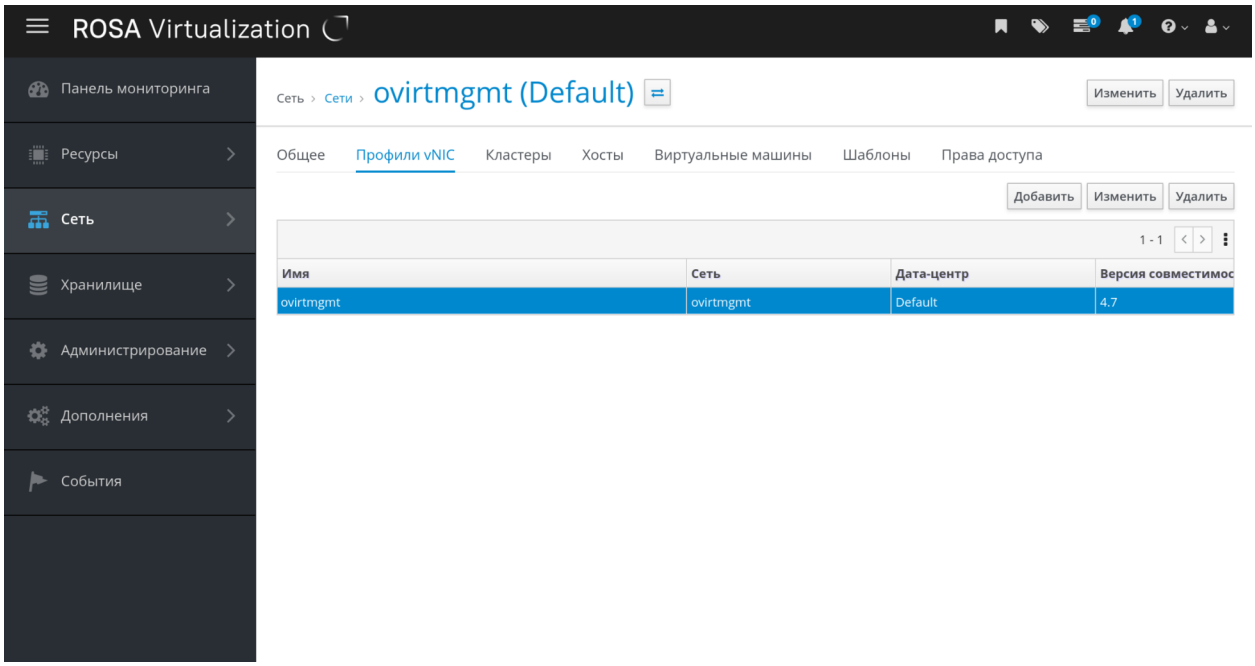


Рисунок 126 – Вкладка "Профили vNIC"

а) нажать кнопку Добавить или Изменить;
д) ввести "Имя" и "Описание" профиля (рисунок 127);

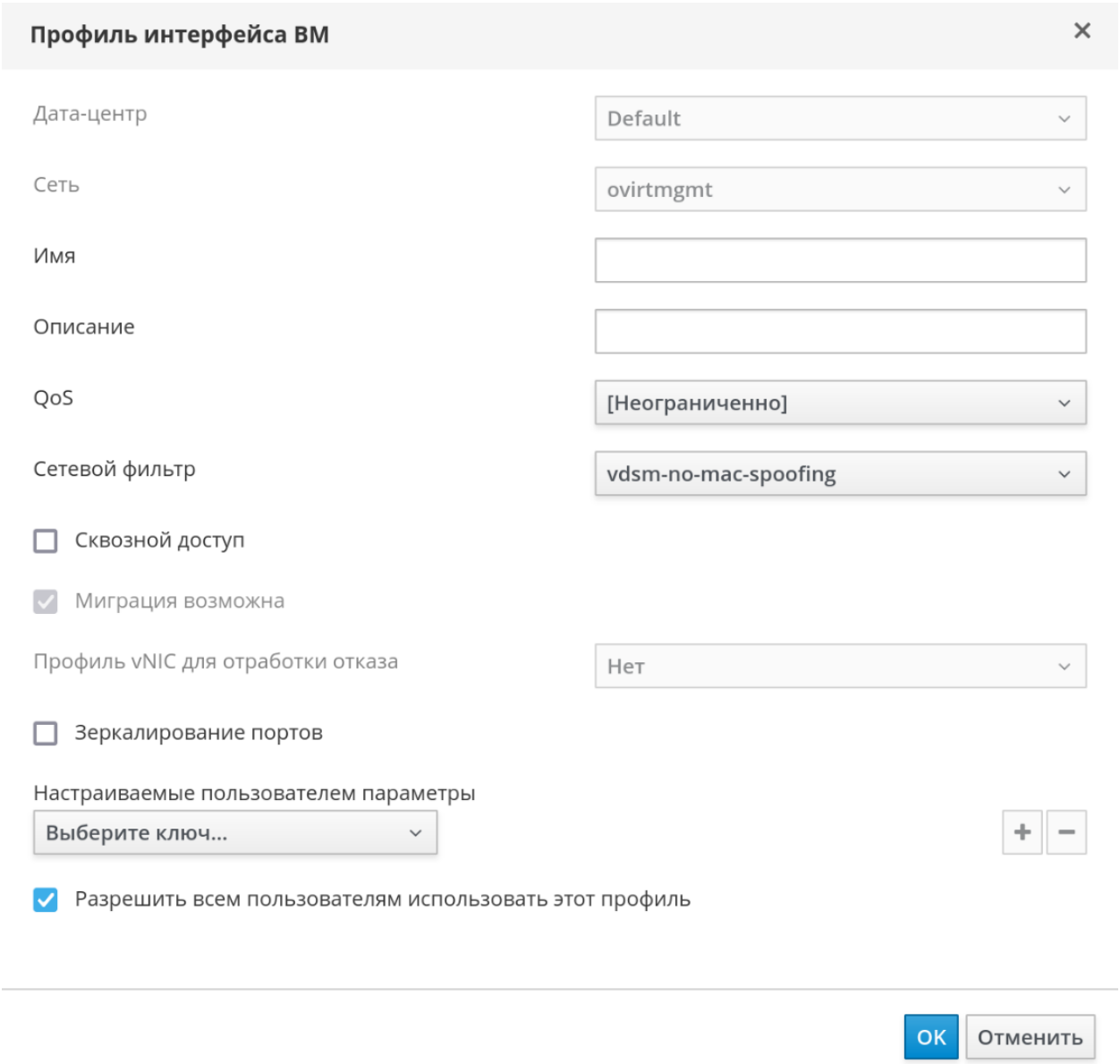


Рисунок 127 – Добавление профиля интерфейса ВМ

е) в списке "QoS" выбрать соответствующую политику качества обслуживания;

ж) из выпадающего списка выбрать "Сетевой фильтр" для управления исходящим и входящим трафиком сетевых пакетов виртуальных машин (рисунок 128);

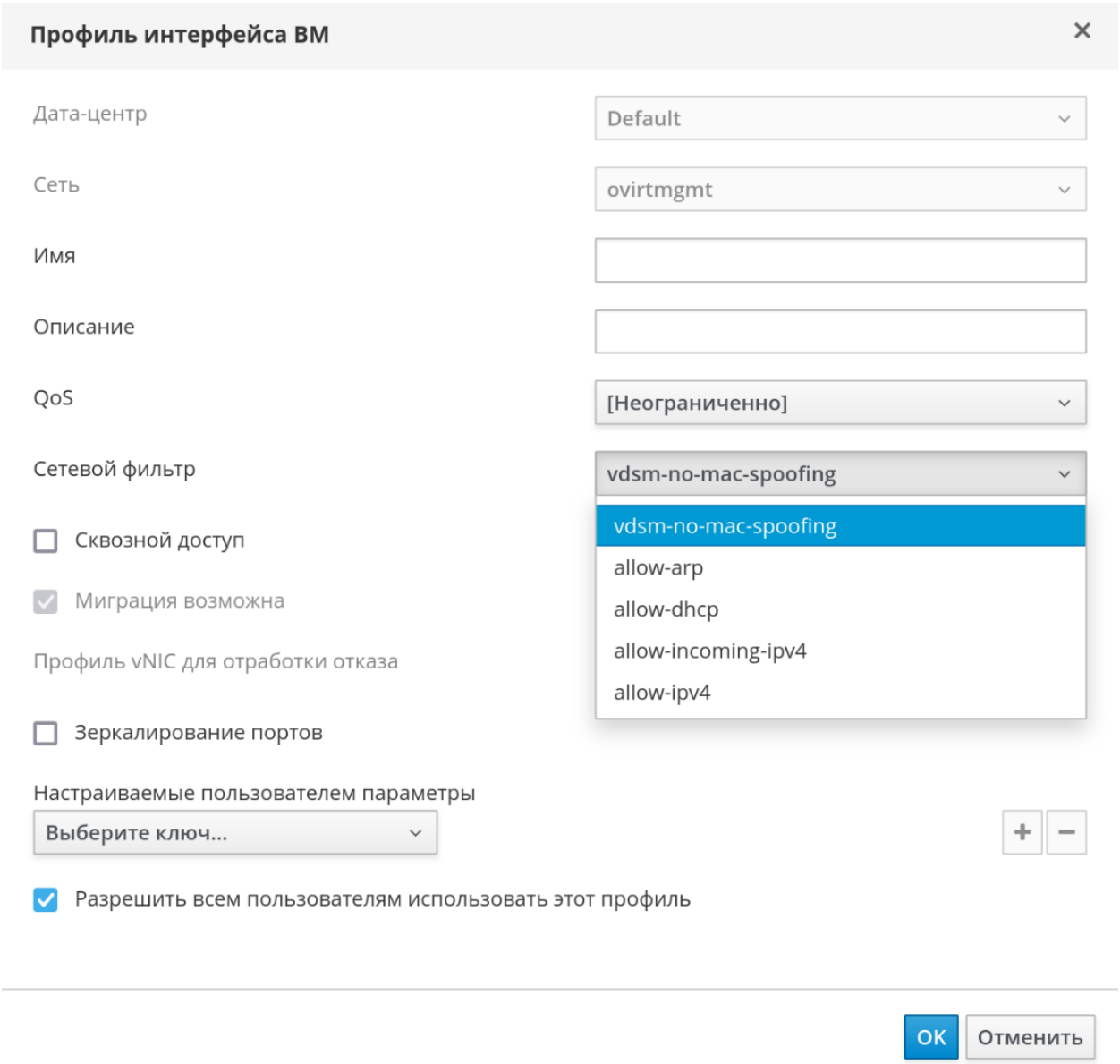


Рисунок 128 – Выбор параметра "Сетевой фильтр" для управления исходящим и входящим трафиком сетевых пакетов

з) установить 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. 3.4.2.4);

и) при выбранном параметре "Сквозной доступ" снять флажок (при необходимости) с параметра "Может мигрировать", чтобы отключить возможность миграции для vNIC, использующих этот профиль;

к) установить переключатели "Зеркалирование портов" и "Разрешить всем пользователям использовать этот профиль" в необходимое положение;

л) выбрать частное свойство из списка свойств; по умолчанию отображается пункт "Выберите ключ..."; добавить или удалить частные свойства с помощью кнопок + или – соответственно;

м) нажать кнопку OK.

Теперь можно применять 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.

3.4.2.3 Параметры в окне "Профиль сетевого адаптера ВМ"

В таблице 49 описываются параметры в окне "Профиль сетевого адаптера ВМ".

Таблица 49 – 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 подчеркивания
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 использовать <No Network Filter>. На доверенных ВМ отказ от использования сетевого фильтра может улучшить производительность
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 присоединен к ВМ. При включении сквозного доступа в профиле vNIC отключаются QoS, сетевые фильтры и зеркалирование портов
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 использовать кнопки + или – соответственно
Разрешить всем пользователям использовать этот профиль	Флажок для переключения доступности профиля для всех пользователей в окружении. По умолчанию этот параметр отмечен

Примечание — РОСА Виртуализация не поддерживает отключение сетевых фильтров с помощью указания значения "false" для параметра EnableMACAntiSpoofingFilterRule" с использованием утилиты engine-config. Рекомендуется использовать для этого параметр <No Network Filter>.

3.4.2.4 Включение сквозного доступа в профиле vNIC

В данном пункте описывается, как установить и настроить технологию виртуализации ввода-вывода с единым корнем (SR-IOV) в РОСА Виртуализация. Дополнительные сведения приведены в п. 3.4.4.

Технология сквозного доступа в профиле vNIC дает 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 присоединен к vNIC, поэтому в процессе следующей пошаговой инструкции создается новый профиль.

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

Для включения сквозного доступа нужно:

а) перейти в "Сеть → Сети";

б) нажать на имя логической сети, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Профили vNIC", чтобы увидеть список всех профилей vNIC для этой логической сети;

г) нажать кнопку Добавить;

д) указать "Имя" и "Описание" профиля;

е) установить флажок для параметра "Сквозной доступ";

ж) опционально отключить параметр "С возможностью миграции" для отключения миграции vNIC, использующих этот профиль;

з) выбрать частное свойство из списка свойств; по умолчанию отображается пункт "Выберите ключ...", добавить или удалить частные свойства с помощью кнопок + или – соответственно;

и) нажать кнопку OK.

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

3.4.2.5 Удаление профиля vNIC

Для удаления профиля vNIC нужно:

а) перейти в "Сеть → Сети";

б) нажать на имя логической сети, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Профили vNIC", чтобы увидеть список всех профилей vNIC;

г) выбрать один или несколько необходимых профилей и нажать кнопку Удалить;

д) нажать кнопку OK.

3.4.2.6 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 опознается 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
```

Для присвоения групп безопасности профилям vNIC нужно:

а) перейти в "Сеть → Сети";

б) нажать на имя логической сети, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Профили vNIC";

г) нажать кнопку Добавить или выбрать уже существующий профиль vNIC и нажать кнопку Изменить;

д) из выпадающего списка частных свойств выбрать SecurityGroups. Пустое поле частного свойства означает применение параметров безопасности по умолчанию, которые разрешают исходящий трафик и обмен информацией, но

запрещают весь входящий трафик извне первоначальной группы безопасности. **Следует обратить внимание**, если свойство SecurityGroups в дальнейшем будет удалено, это не повлияет на выбранную группу безопасности (рисунок 129);

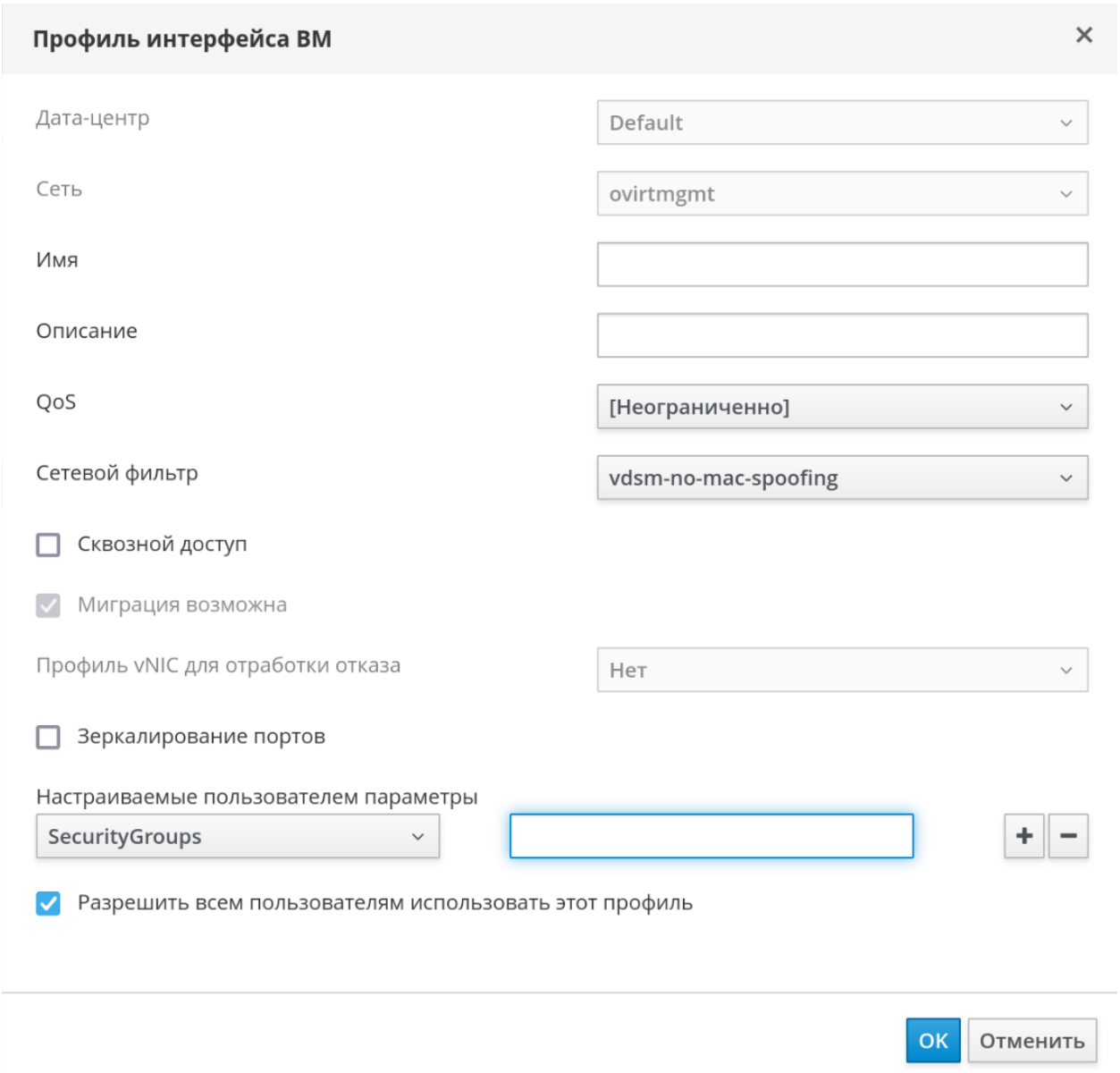


Рисунок 129 – Настройка параметра SecurityGroups

е) ввести ID группы безопасности в текстовое поле, чтобы присвоить ее профилю vNIC;

ж) нажать кнопку OK.

В результате группа безопасности будет присоединена к профилю vNIC. Весь трафик, проходящий через логическую сеть, к которой присоединен данный профиль, будет фильтроваться согласно правилам, определенным для этой группы безопасности.

3.4.2.7 Полномочия пользователей на профили vNIC

Полномочия пользователей настраивают, чтобы привязать пользователей к определенным профилям vNIC. При присвоении роли VnicProfileUser пользователь получает возможность использовать этот профиль. Чтобы запретить пользователям доступ к определенным профилям, требуется удалить их полномочия на этот профиль.

Для настройки пользовательских полномочий на профиль vNIC нужно выполнить следующие действия:

а) перейти в "Сеть → Профиль vNIC";
б) нажать на профиль vNIC, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Права доступа", чтобы просмотреть текущие полномочия пользователя для этого профиля (рисунок 130);

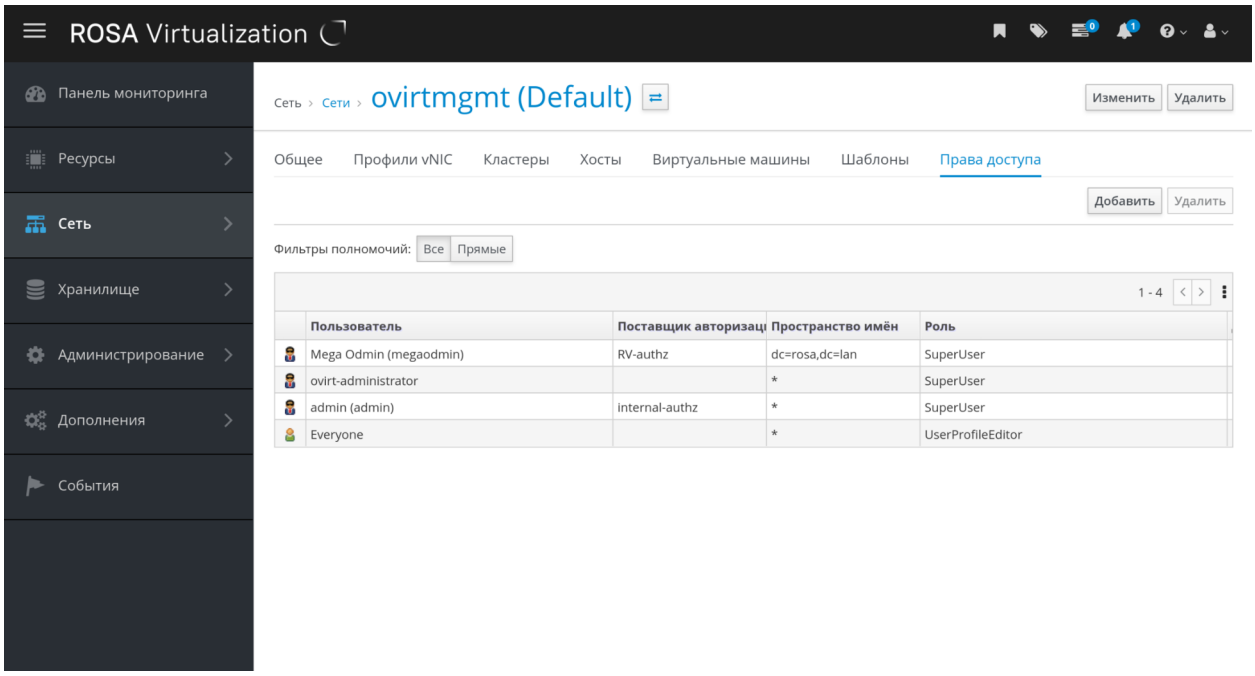


Рисунок 130 – Вкладка "Права доступа"

г) чтобы изменить полномочия пользователя на профиль vNIC, нажать кнопку Добавить или Удалить (рисунок 131);

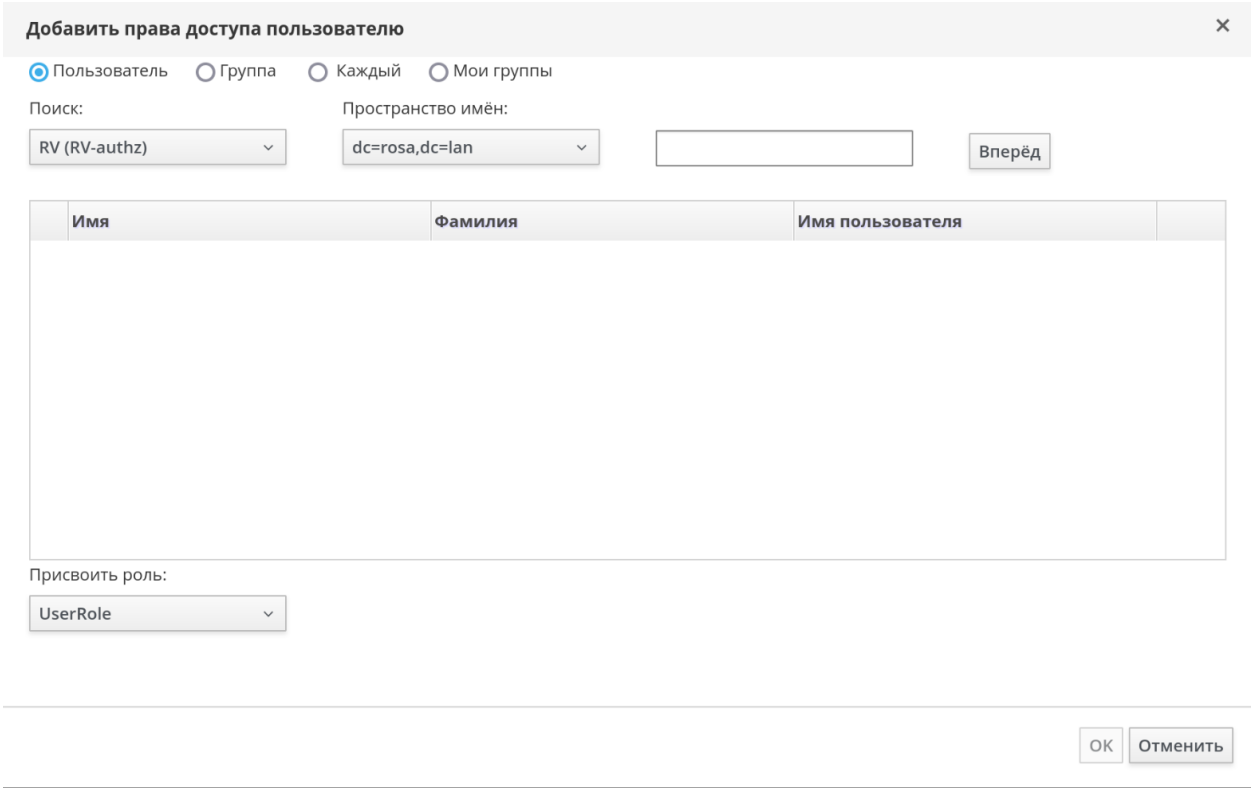


Рисунок 131 – Форма "Добавить права доступа пользователю"

д) в окне "Добавить полномочия пользователю" выбрать "Мои группы", чтобы отобразить группы пользователя. Этот параметр можно использовать для добавления полномочий другим пользователям в этих группах (рисунок 132);

е) нажать кнопку ОК.

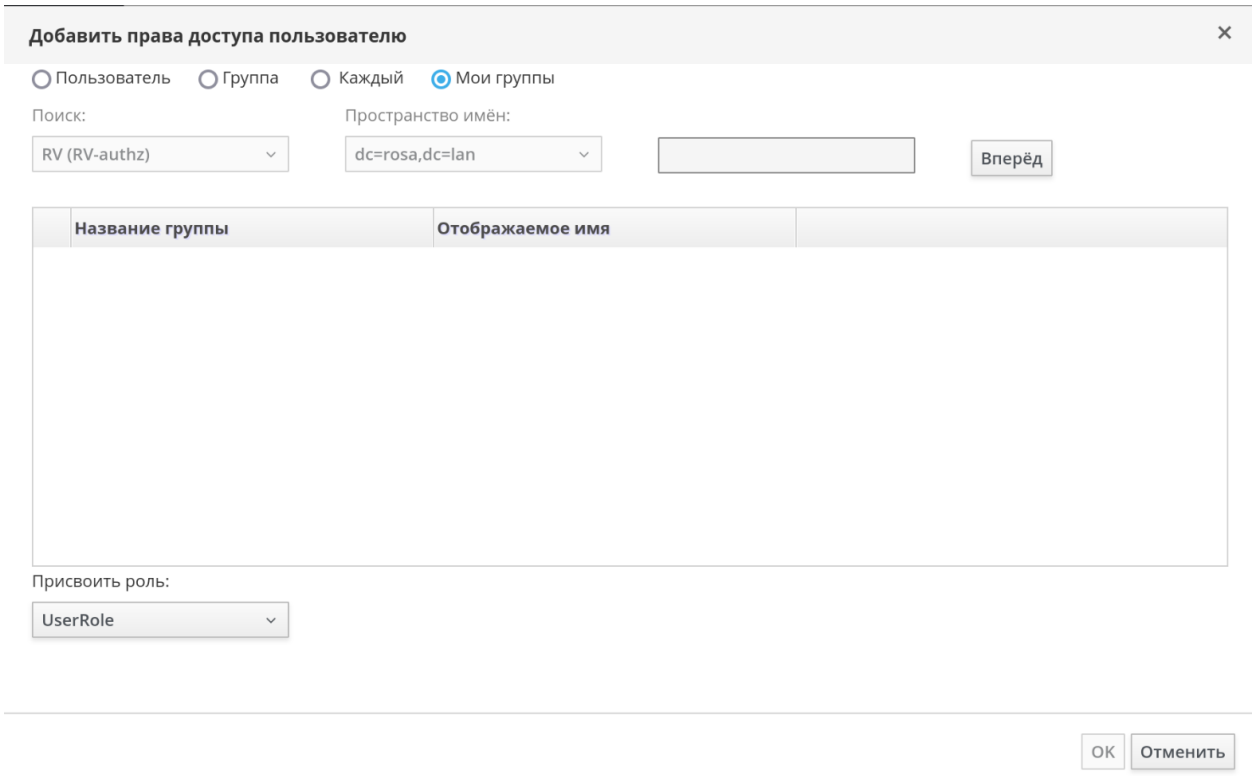


Рисунок 132 – Форма "Мои группы"

3.4.2.8 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 дает 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 следует указывать все частные свойства в команде, с помощью которой настраивается значение ключей. Указываемые свойства разделяются точкой с запятой.

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

Для настройки частного свойства устройства нужно:

а) настроить частное свойство vmfex в виртуализированном ЦУ и с помощью опции --cver указать уровень совместимости кластера:

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

б) убедиться в том, что частное свойство vmfex добавлено:

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

в) перезапустить 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. в п. 3.4.1.2).

Для настройки профиля vNIC для интеграции в UCS необходимо:

а) перейти в "Сеть → Сети";
б) нажать на имя логической сети, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Профили vNIC";
г) нажать кнопку Добавить или выбрать уже существующий профиль vNIC и нажать кнопку Изменить;
д) указать "Имя" и "Описание" профиля;
е) В списке частных свойств выбрать свойство vmfex и ввести название профиля порта UCS;
ж) нажать кнопку OK.

3.4.3 Сети внешних поставщиков

3.4.3.1 Импорт 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), необходимо зарегистрировать поставщика в виртуализированном ЦУ.

Затем требуется выполнить следующую последовательность действий, чтобы импортировать сети этого поставщика в виртуализированный ЦУ для возможности их использования виртуальными машинами:

а) перейти в "Сеть → Сети";

б) нажать кнопку Импорт;

в) из выпадающего списка "Поставщик сетей" выбрать внешнего поставщика. Сети, предоставляемые этим поставщиком, обнаруживаются автоматически и указываются в списке "Сети поставщика";

г) в списке "Сети поставщика" установить флажки для сетей, которые нужно импортировать, и нажать значок ↓ (стрелка вниз), чтобы переместить эти сети в список "Сети для импорта";

д) имя импортируемой сети можно настроить, нажав на имя сети в столбце "Имя" и изменив текст;

е) из выпадающего списка "Дата-центр" выбрать дата-центр, в который будут импортированы сети;

ж) опционально снять флажок с параметра "Разрешить всем", чтобы сеть не была доступна всем пользователям;

з) нажать кнопку Импортировать.

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

3.4.3.2 Ограничения при использовании сетей внешних поставщиков

Существуют следующие ограничения при использовании логических сетей, импортированных с внешнего поставщика, в РОСА Виртуализация:

– 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, подключенных 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.

3.4.3.3 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 следует обратить внимание, что у ovirt-provider-ovn есть свои ограничения, в частности отсутствует реализация Source NAT (enable_snat) в OpenStack API.

3.4.3.4 Добавление подсетей в логических сетях внешних поставщиков

Для добавления подсетей в логических сетях внешних поставщиков нужно:

а) перейти в "Сеть → Сети";
б) нажать на имя логической сети, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Подсети";
г) нажать кнопку Добавить;
д) указать "Имя" и "CIDR" новой подсети;
е) из выпадающего списка "Версия IP" выбрать IPv4 или IPv6;
ж) нажать кнопку OK.

Примечание — Для IPv6 поддерживается только статическая адресация.

3.4.3.5 Удаление подсетей из логических сетей внешних поставщиков

Для удаления подсетей из логических сетей внешних поставщиков нужно:

а) перейти в "Сеть → Сети";
б) нажать на имя логической сети, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Подсети";
г) выбрать подсеть и нажать кнопку Удалить;
д) нажать кнопку OK.

3.4.3.6 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 РОСА Виртуализация 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).

Следует обратить внимание, что в виртуализированном ЦУ нельзя создавать группы безопасности. Группы безопасности необходимо создавать с помощью OpenStack Networking API v2.0 или Ansible.

Для добавления групп безопасности в логические сети нужно:

а) перейти в "Ресурсы → Кластеры";
б) нажать на имя кластера, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Логические сети";
г) нажать кнопку Добавить сеть и настроить свойства сети (см. п. 3.4.1.2), в частности выбрать из выпадающего списка "Внешний поставщик" пункт ovirt-provider-ovn;
д) из выпадающего списка "Защита сетевых портов" выбрать "Включено" (см. п. 3.4.1.7);
е) нажать кнопку OK.
ж) создать группы безопасности и правила групп безопасности с помощью OpenStack Networking API v2.0 или Ansible;
з) обновить информацию о настроенных группах безопасности на портах;
и) опционально указать, будет ли этот функционал безопасности включен 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.

3.4.4 Хосты и организация сетей

3.4.4.1 Конфигурация Network Manager с сохранением состояния (nmstate)

В версиях РОСА Виртуализация 2.1 и выше для настройки сетей хостов используются конфигурации Network Manager с сохранением состояния (nmstate). В

версиях РОСА Виртуализация 2.0 и более ранних для этих задач использовались сетевые сценарии настройки интерфейсов (ifcfg).

Чтобы начать использовать nmstate, нужно обновить версии СУСВ и хостов согласно руководству по обновлению РОСА Виртуализация.

Администраторам нет необходимости отдельно устанавливать и настраивать nmstate. Использование программы включено по умолчанию, и она выполняется в фоновом режиме.

Важно – Для изменения сетевой конфигурации хостов на кластерах всегда следует использовать СУСВ, в противном случае будет получена неподдерживаемая конфигурация.

Переход на использование nmstate проходит практически незаметно. Изменяется только процесс настройки сетевой конфигурации хоста:

а) после добавления хоста в кластер вносить изменения в его сетевую конфигурацию только при помощи СУСВ;

б) изменение сетевой конфигурации хоста без использования СУСВ может создать неподдерживаемую конфигурацию;

в) для исправления неподдерживаемой конфигурации её нужно заменить на поддерживаемую: при помощи СУСВ синхронизировать сеть хоста. Подробности см. в п. 3.4.4.4;

г) сетевые конфигурации хостов должны изменяться без использования инструментария СУСВ только в одном случае: настройка статического маршрута на хосте. Подробности см. в п. 3.4.4.9.

Переход на nmstate повысил эффективность применения СУСВ изменений, вносимых из Cockpit и Anaconda до того, как хосты были добавлены. В результате этого перехода также были исправлены некоторые ошибки кода, например, когда ранее настроенные параметры статических адресов IPv6 изменялись при добавлении и развёртывании хостов в случаях, если Network Manager управлял интерфейсами.

3.4.4.2 Обновление сведений о характеристиках хоста

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

Для обновления сведений о характеристиках хоста нужно:

а) перейти в "Ресурсы → Хосты" и выбрать хост (рисунок 133);

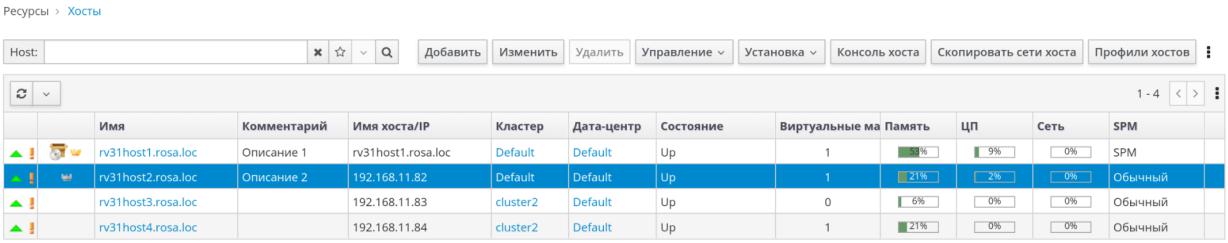


Рисунок 133 – Выбор хоста для обновления параметров хоста

б) выбрать в меню "Управление → Обновить сведения о характеристиках хоста" (рисунок 134);

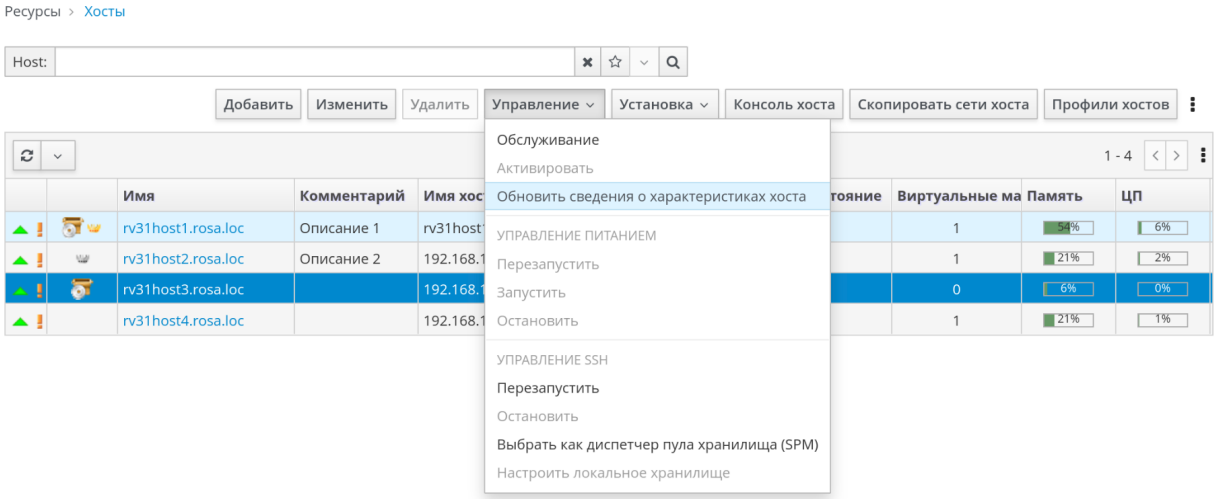


Рисунок 134 – Обновление сведений о характеристиках хоста

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

3.4.4.3 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 изменения IP-адреса хоста в Системе виртуализации является удаление хоста и повторное его добавление.

– Сведения о том, как изменить параметры VLAN хоста, приведены в п. 3.4.4.6.

– 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 нужно навести 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.

Для изменения параметров сетевых интерфейсов и присвоение хостам логических сетей нужно:

а) перейти в "Ресурсы → Хосты" (рисунок 133);

б) нажать на имя хоста, чтобы перейти к подробному просмотру (рисунок 135);

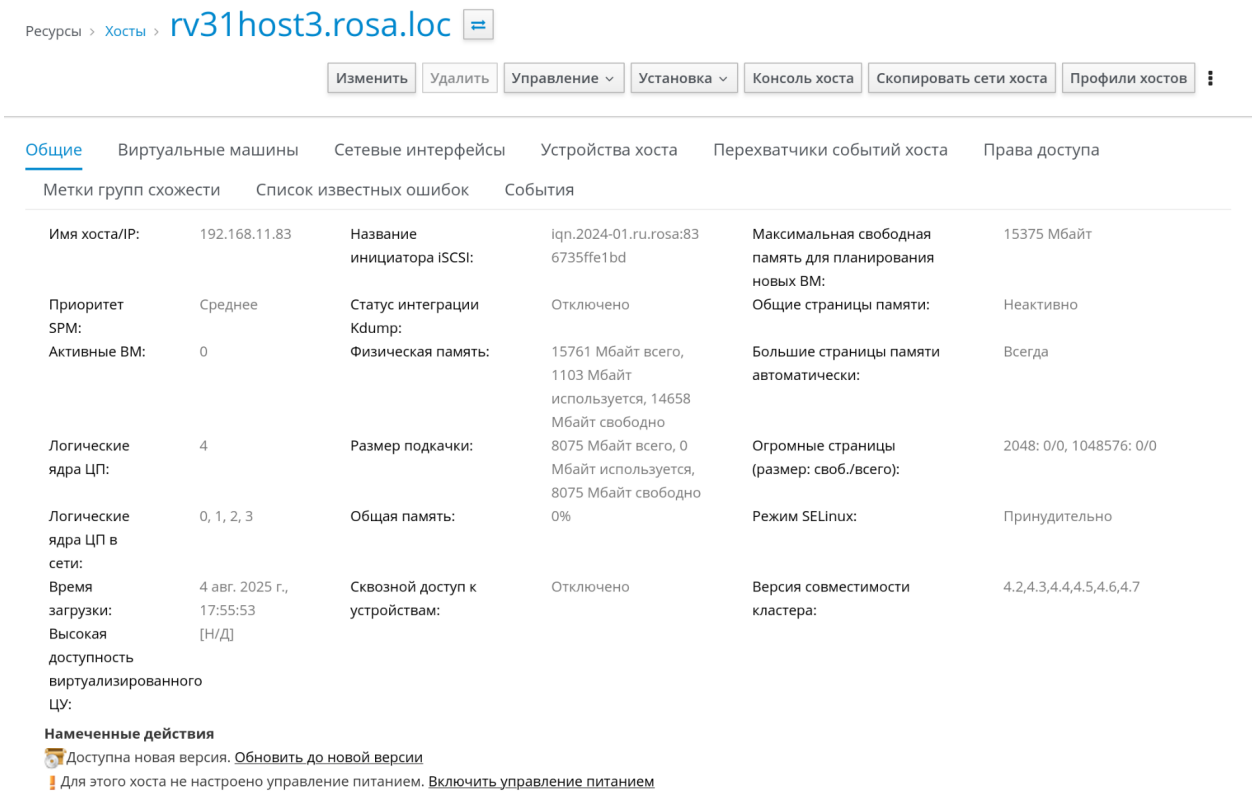


Рисунок 135 – Общая информация о параметрах хоста

в) перейти на вкладку "Сетевые интерфейсы" (рисунок 136);

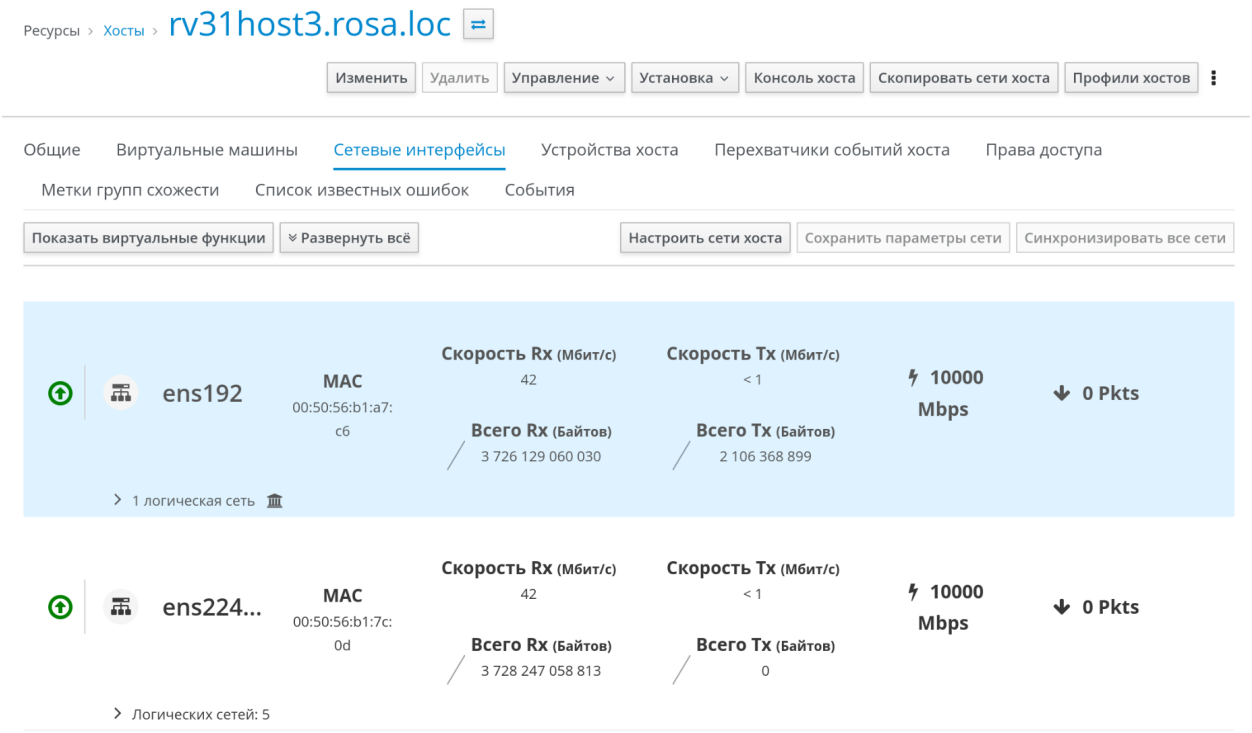


Рисунок 136 – Информация о сетевых интерфейсах хоста

г) нажать кнопку `Настроить сети хоста` (рисунок 137);

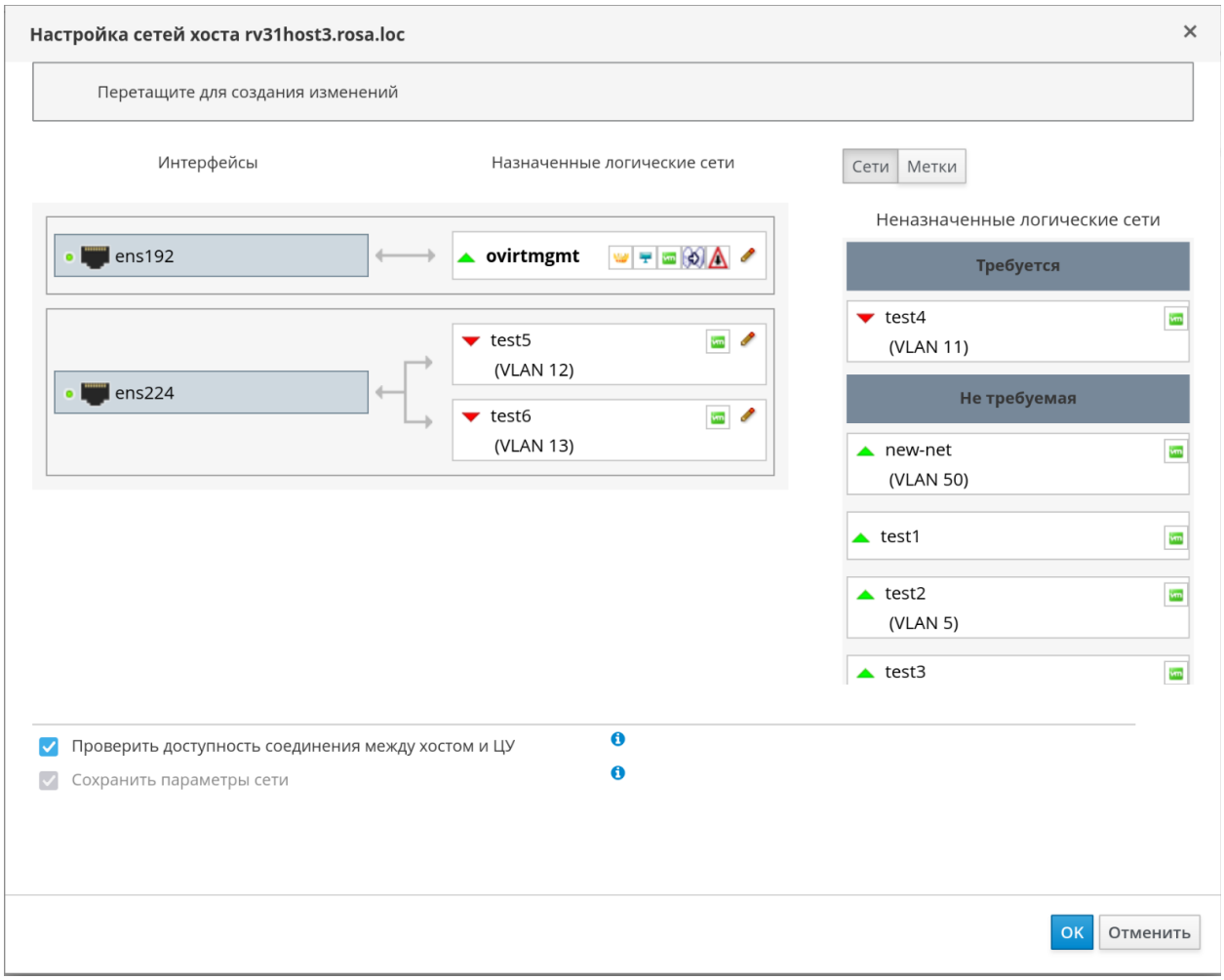


Рисунок 137 – Настройка сетей хоста

д) при необходимости навести курсор на сетевой интерфейс хоста, чтобы просмотреть сведения о конфигурации, предоставляемой коммутатором;

е) подключить логическую сеть к физическому сетевому интерфейсу хоста, выбрав и переместив логическую сеть в область "Назначенные логические сети" рядом с физическим сетевым интерфейсом хоста (рисунок 138);

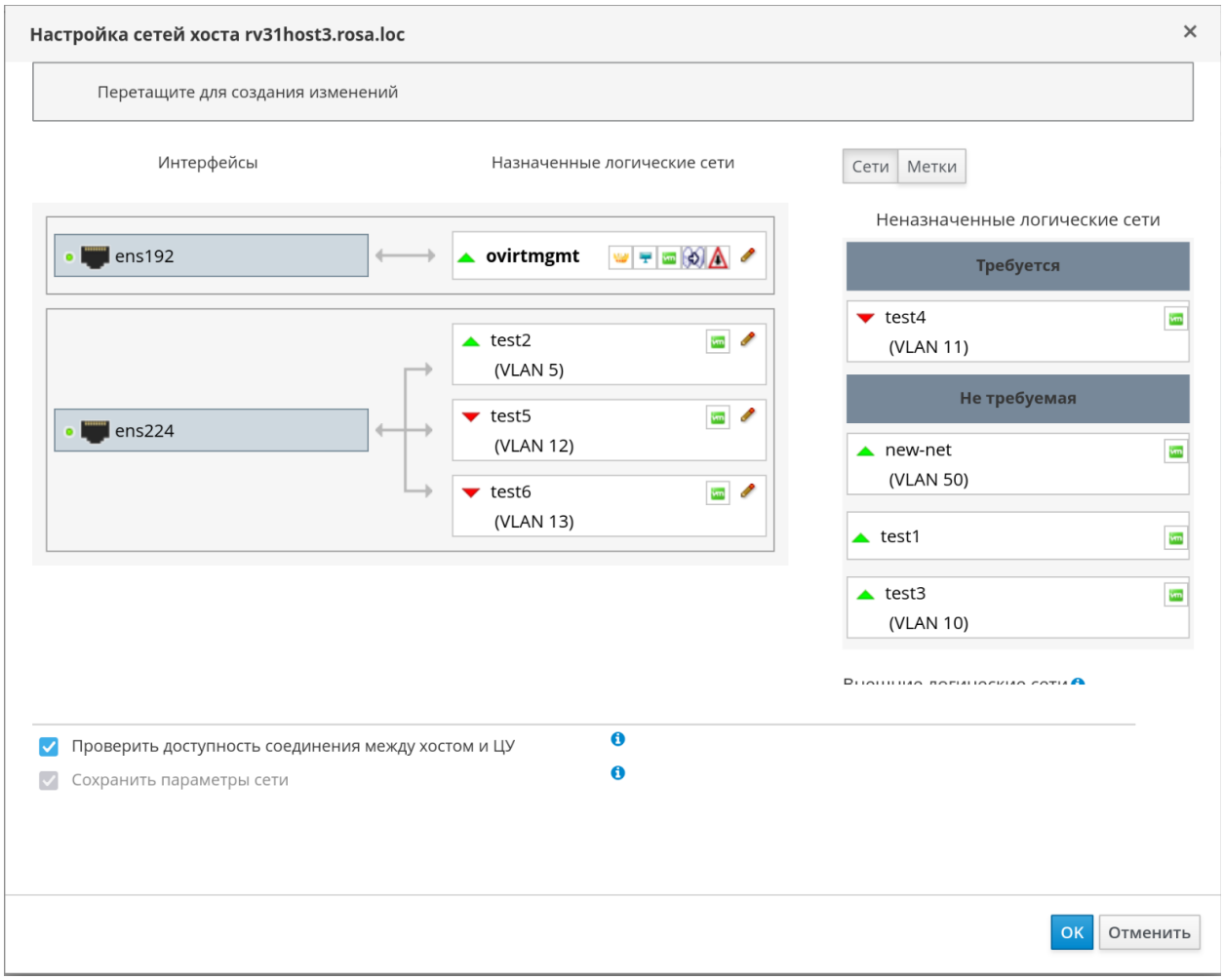


Рисунок 138 – Добавление логической сети

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

ж) настроить локальную сеть:

1) навести курсор на присвоенную логическую сеть и нажать на пиктограмму (карандаш), чтобы открыть окно "Изменить сеть управления" (рисунок 139);

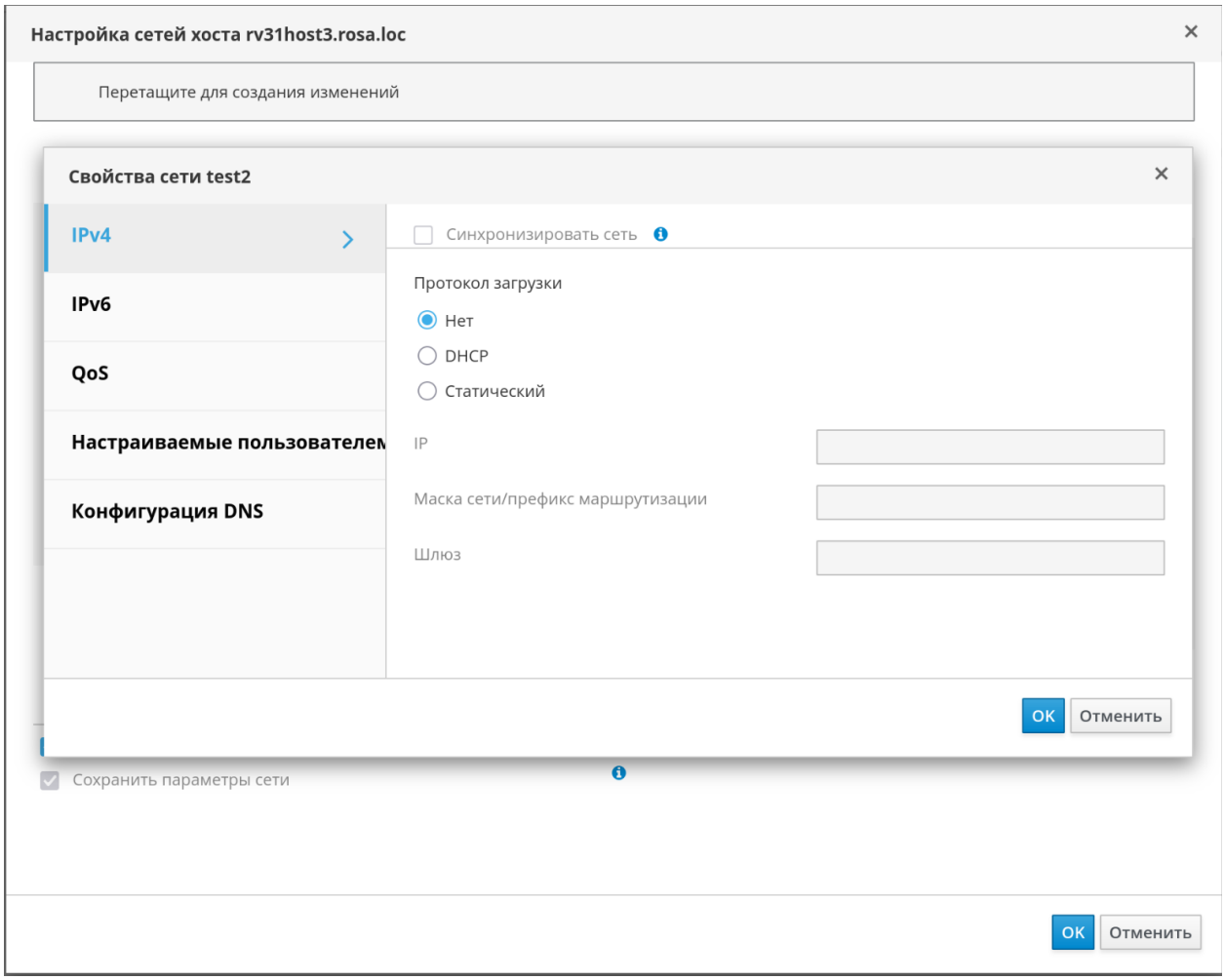


Рисунок 139 – Изменение свойств сети

2) во вкладке "IPv4" выбрать протокол загрузки: "Нет", "DHCP" или "Статический";

3) при выборе протокола "Статический" указать "IP", "Префикс сетевой маски/маршрутизации" и "Шлюз";

Важно — Для протокола IPv6 поддерживаются только статическая адресация. Для настройки логической сети перейти на вкладку "IPv6" и создать следующие записи:

– указать "Статический протокол загрузки";

– указать длину "Префикса маршрутизации" с помощью прямой косой черты и десятичного числа (например, /48);

– указать "IP" — полный адрес IPv6 сетевого интерфейса хоста (например, "2001:db8:1:0:0:6");

– указать "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.

Важно – Следует:

– настроить 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.

– использовать параметры во вкладке "QoS" для переопределения качества обслуживания сети по умолчанию (рисунок 140):

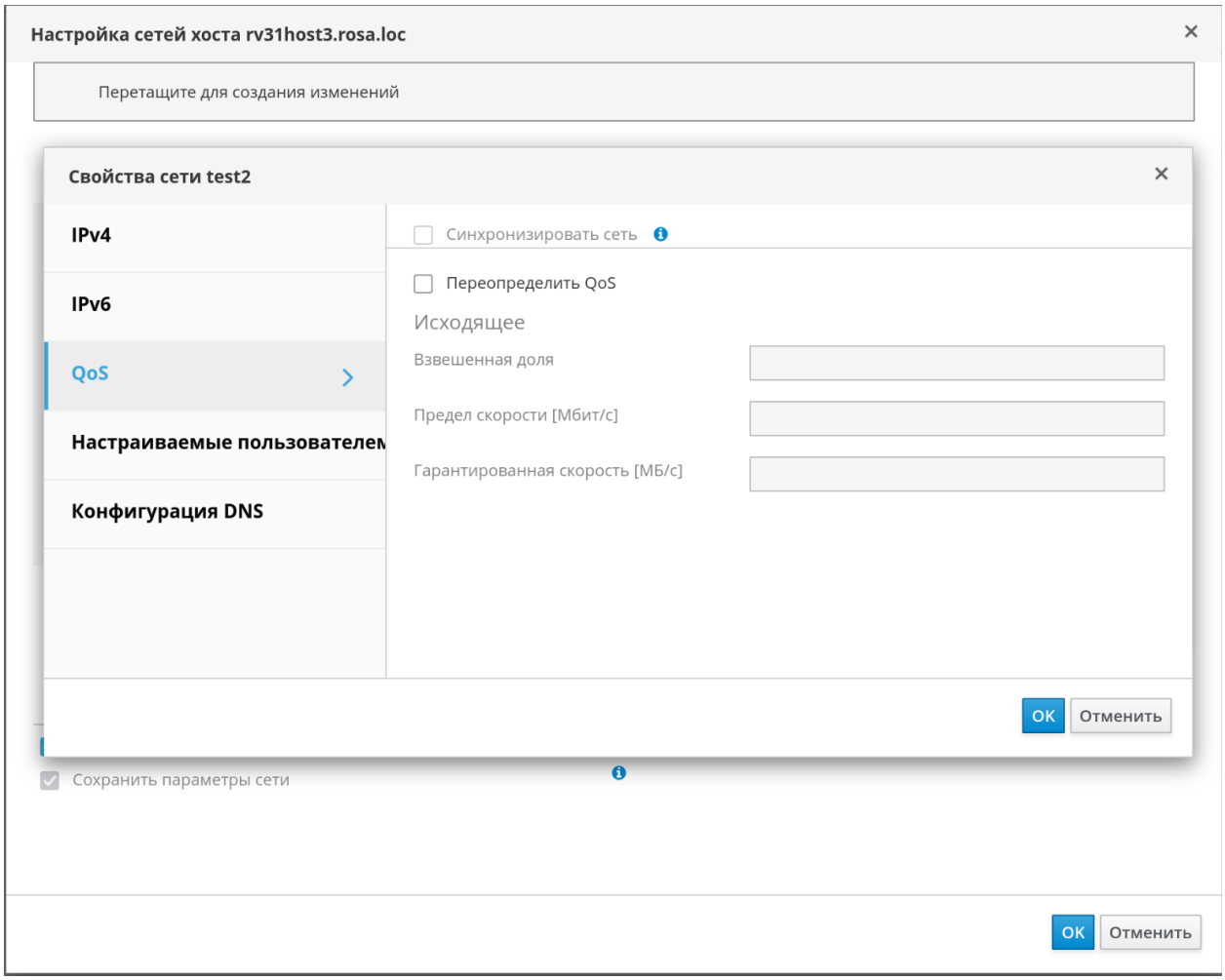


Рисунок 140 – Настройка QoS

– выбрать "Переопределить QoS" и указать нужные значения в следующих полях:

– Взвешенная доля – означает, какую долю пропускной способности логического канала нужно выделить конкретной сети относительно других сетей, прикрепленных 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 самом деле не гарантируется и будет изменяться в

зависимости от сетевой инфраструктуры и гарантированной скорости, запрашиваемой другими сетями на этом же логическом канале;

4) для настройки сетевого моста перейти на вкладку "Настраиваемые пользователем параметры" и в выпадающем списке выбрать bridge_opts (рисунок 141);

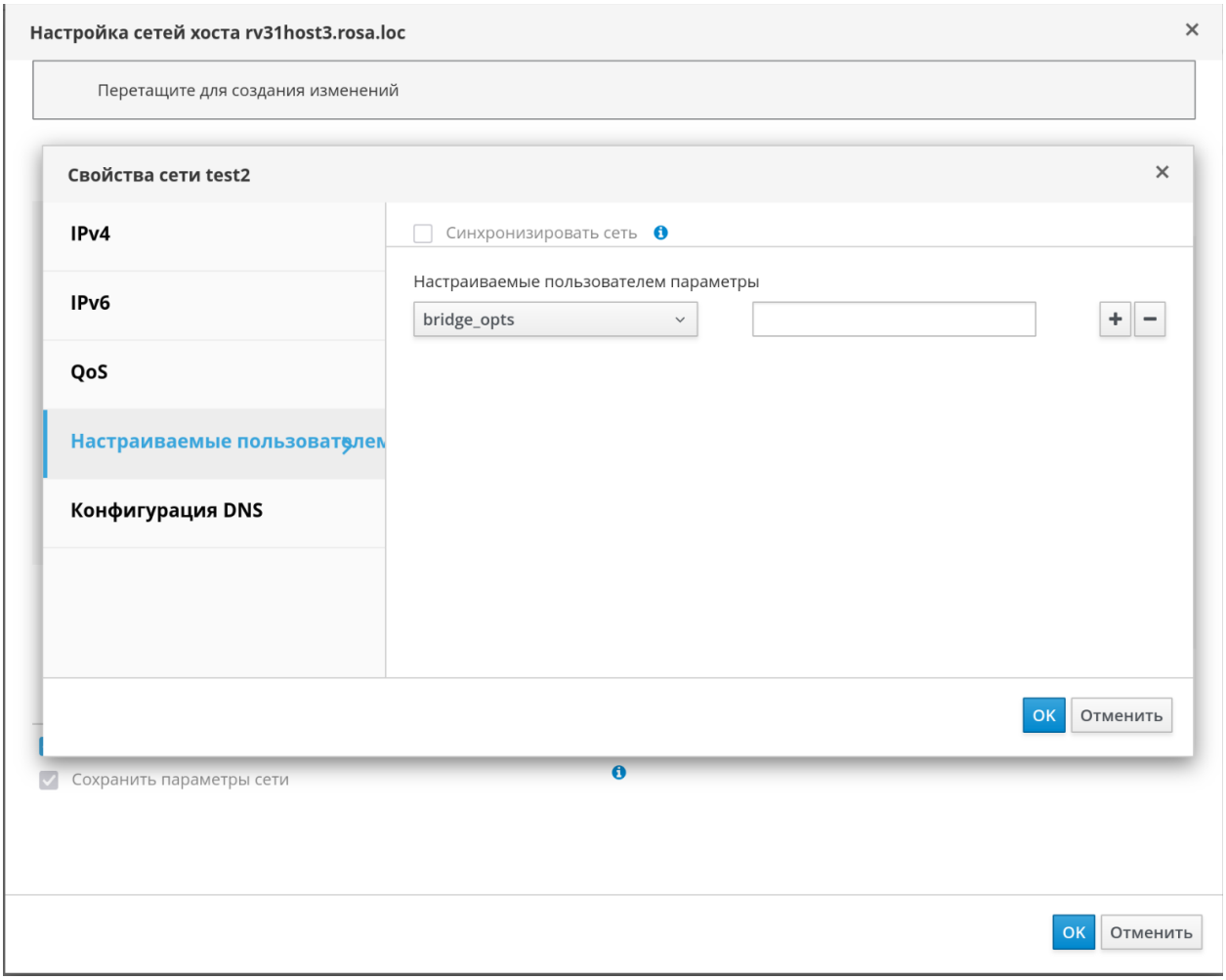


Рисунок 141 – Настраиваемые пользователем параметры свойств сети

5) ввести 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 Б.1):

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

6) чтобы настроить свойства Ethernet, перейти на вкладку "Настраиваемые пользователем параметры", в выпадающем списке выбрать параметр "ethtool_opts", указать 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, использовать следующие значения:

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

Важно — Параметр ethtool_opts по умолчанию недоступен, и его необходимо добавить с помощью утилиты настройки виртуализированного ЦУ (см. п.Б.24.9.2).

7) для настройки протокола FCoE перейти на вкладку "Настраиваемые пользователем параметры", в выпадающем списке выбрать параметр "fcoe" и ввести действительный ключ и значение, придерживаясь следующего синтаксиса: "ключ=значение". Минимальное требуемое значение: "enable=yes". Также можно добавить "dcb= and auto_vlan=[yes|no]" (записи отделяются символом пробела);

Важно — Параметр "fcoe" по умолчанию недоступен и его необходимо добавить с помощью утилиты настройки виртуализированного ЦУ (см. п. 4.9.2).

Примечание — Для использования FCoE рекомендуется отдельная выделенная логическая сеть.

8) чтобы сменить сеть хоста по умолчанию с сети управления (ovirtmgmt) на сеть, не являющуюся сетью управления, настроить маршрут этой сети по умолчанию (см. п. 3.4.1.5);
9) если определение логической сети не синхронизировано с сетевой конфигурацией на хосте, установить флажок для параметра "Синхронизировать сеть" (см. п. 3.4.4.4);

з) отметить параметр "Проверить доступность соединения между хостом и ЦУ", чтобы проверить сетевое соединение. Это действие эффективно только для хостов, находящихся в режиме обслуживания;

и) нажать кнопку OK.

Примечание — Если не все карты сетевых интерфейсов хоста отображаются в ЦУ, следует выбрать меню "Управление → Обновить сведения о характеристиках хоста", чтобы обновить список карт сетевых интерфейсов, доступных для этого хоста.

3.4.4.4 Синхронизация сетей хостов

Виртуализированный ЦУ помечает сетевой интерфейс статусом "вне синхронизации", если 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 .

Если 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 или изменение "Пользовательского MTU" на физическом хосте).
– Хост был перемещен 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:

– Внесение изменений на Портале администрирования, а не локально на хосте.
– Изменение параметров VLAN только согласно инструкциям, приведенным в п. 3.4.4.6.

3.4.4.5 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 можно обновить определения хостов с помощью интерфейса на Портале администрирования.

Сети хостов можно синхронизировать на трех уровнях:

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

Для синхронизации сетей хоста на уровне логической сети необходимо:

а) перейти в "Ресурсы → Хосты";
б) нажать на имя хоста, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Сетевые интерфейсы";
г) нажать "Настроить сети хоста";

д) навести курсор на сеть "вне синхронизации" и нажать на пиктограмму  (карандаш), чтобы открыть окно "Свойства сети";

е) установить флажок для параметра "Синхронизировать сеть";

ж) нажать кнопку `OK` для применения изменений;

з) нажать кнопку `OK`, чтобы закрыть окно "Настроить сети хоста".

Для синхронизации сетей хоста на уровне хоста нужно нажать на кнопку `Синхронизировать все сети` во вкладке "Сетевые интерфейсы" хоста, чтобы синхронизировать все интерфейсы хоста, находящиеся "вне синхронизации".

Для синхронизации сетей хоста на уровне кластера требуется нажать 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.

3.4.4.6 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.

Для изменения параметров VLAN хоста с сохранением синхронизации сетей нужно:

а) переместить хост в режим обслуживания;

б) вручную удалить сеть управления с хоста, после чего хост станет доступен для подключений из новой VLAN;

в) добавить хост в кластер, при этом ВМ, не подключенные 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.

3.4.4.7 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.

Важно — 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".

Для добавления нескольких VLAN на один сетевой интерфейс с использованием логических сетей нужно выполнить следующие действия:

а) перейти в "Ресурсы → Хосты";
б) нажать на имя хоста, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Сетевые интерфейсы";
г) нажать кнопку Настроить сети хоста;
д) переместить 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;
е) изменить параметры логических сетей:

1) навести курсор на присвоенную логическую сеть и нажать на пиктограмму (карандаш);
2) если определение логической сети не синхронизировано с сетевой конфигурацией на хосте, установить флажок для параметра "Синхронизировать сеть";
3) выбрать "Протокол" загрузки: "Нет", "DHCP" или "Статический";
4) указать "IP" и "Маску подсети";
5) нажать кнопку OK;

ж) установить флажок для параметра "Проверить доступность соединения между хостом и ЦУ", чтобы выполнить проверку сети. **Следует**

обратить внимание, что это может быть сделано только для хостов, находящихся в режиме обслуживания;

з) нажать кнопку OK.

После выполнения приведенной процедуры следует добавить 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.

3.4.4.8 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 дает 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.

Для присвоения дополнительных адресов IPv4 сетям хоста нужно:

а) на хосте, для которого необходимо настроить дополнительно адреса IPv4, установить пакет ловушки VDSM. Этот пакет по умолчанию доступен на хостах виртуализации, но на простых хостах его необходимо устанавливать дополнительно. Выполнить следующую команду:

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

б) в виртуализированном ЦУ выполнить следующую команду для добавления ключа:

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

в) перезапустить службу ovirt-engine:

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

г) в главном меню Портала администрирования перейти в "Ресурсы → Хосты";

д) нажать на имя хоста, чтобы перейти к подробному просмотру;

е) перейти на вкладку "Сетевые интерфейсы" и выбрать "Настроить сети хоста";

ж) навести курсор на присвоенную логическую сеть и нажать на значок карандаша;

з) из выпадающего списка "Настраиваемые пользователем параметры" выбрать пункт "ipv4_addr" и добавить дополнительный IP-адрес и префикс сети (например, "5.5.5.5/24"). **Следует обратить внимание**, что несколько IP-адресов должны разделяться запятой;

и) нажать кнопку `OK`, чтобы закрыть окно "Параметры сети";

к) нажать кнопку `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.

3.4.4.9 Добавление сетевых меток сетевым интерфейсам хоста

Использование сетевых меток очень 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 развертывание этой сети на всех хостах с помощью протокола DHCP. Этот способ массового развертывания был выбран вместо способа указания 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.

3.4.4.9.1 Добавление сетевых меток хосту вручную на Портале администрирования

Для добавления сетевых меток хосту вручную на Портале администрирования нужно выполнить следующие действия:

а) перейти в "Ресурсы → Хосты";
б) нажать на имя хоста, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Сетевые интерфейсы";
г) выбрать "Настроить сети хоста";
д) нажать кнопку `Метки` (рисунок 142);

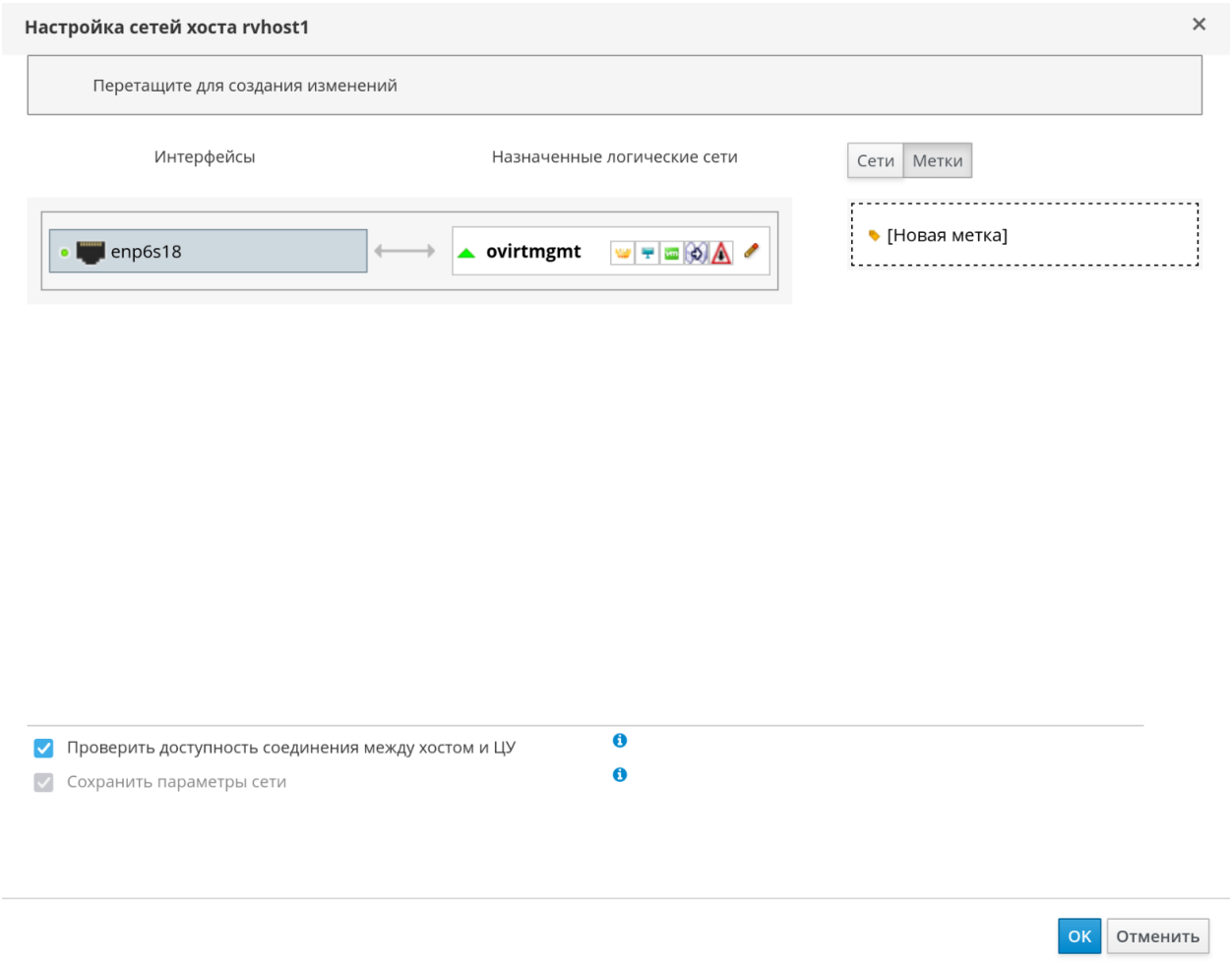


Рисунок 142 – "Настройка сетей хоста" – добавление меток

е) нажать кнопку `Новая метка` и выбрать физический сетевой интерфейс, которому нужно назначить метку (рисунок 143);

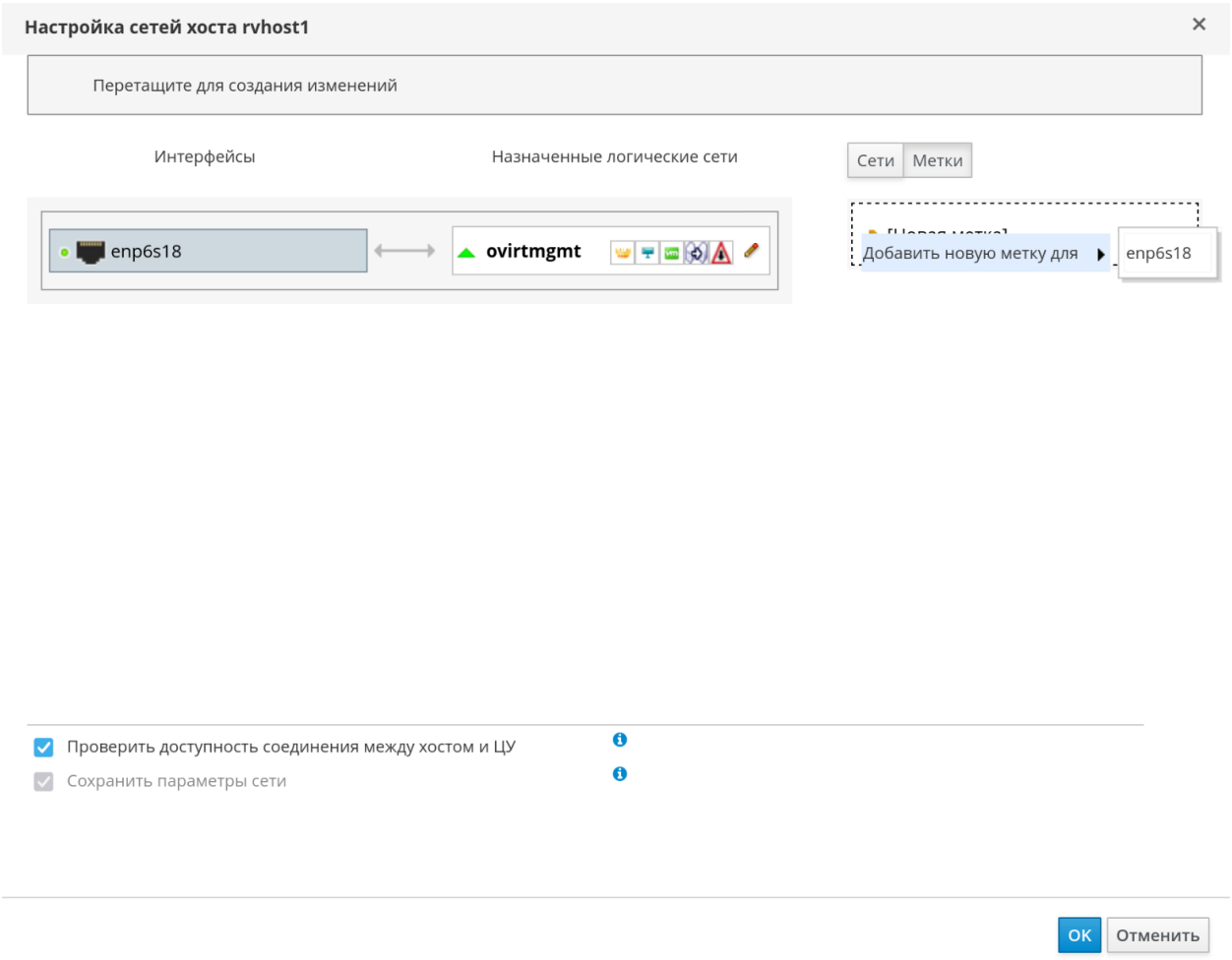


Рисунок 143 – Выбор интерфейса для добавления новой метки

ж) в поле "Метка" ввести имя сетевой метки (рисунок 144);

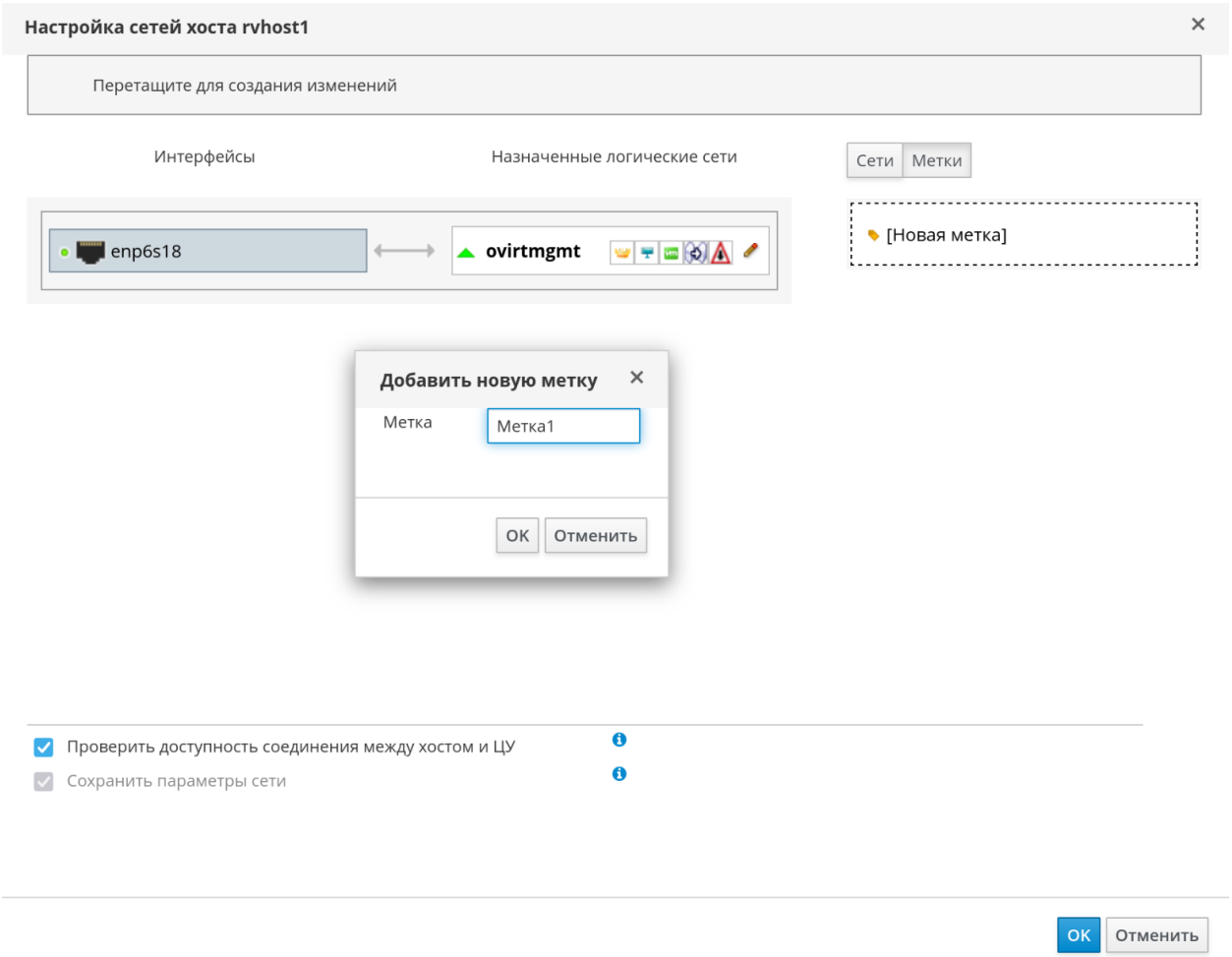


Рисунок 144 – Форма "Добавить новую метку"

з) нажать кнопку OK.

3.4.4.9.2 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 один раз в час. Это удобно при замене аппаратных составляющих (сетевых карт, коммутаторов или кабелей) или изменении конфигураций коммутаторов.

Предварительные условия:

– интерфейс должен быть подключен к коммутатору Juniper;

– коммутатор Juniper должен предоставлять Port VLAN с помощью LLDP.

Последовательность действий:

а) настроить 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";

б) настроить службу меток LLDP, для чего обновить 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, ввести символ "*" (звездочка). 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, оставить 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";

в) при необходимости можно настроить выполнение службы с другими интервалами, изменив значение параметра OnUnitActiveSec в файле /etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer. Значение по умолчанию – "1h" (1 час);

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

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

Примечание – Для запуска службы ovirt-lldp-labeler вручную следует выполнить следующую команду:

```
# /usr/bin/python \
```

```
/usr/share/ovirt-lldp-labeler/ovirt_lldp_labeler_cli.py
```

В результате сетевая метка будет присвоена 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.

3.4.4.10 Изменение полного доменного имени хоста

Для изменения полного доменного имени (FQDN) хоста нужно выполнить следующие действия:

а) перевести хост в режим обслуживания, при котором выполняется динамическая миграция ВМ на другой хост (см. п. 3.5.3.6);

б) нажать кнопку Удалить, а затем нажать кнопку OK, чтобы удалить хост с Портала администрирования;

в) указать новое имя хоста с помощью утилиты hostnamectl:

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

г) перезагрузить хост;

д) повторно зарегистрировать хост в виртуализированном ЦУ.

3.4.4.11 Настройка профилей хостов с использованием сетевых меток

Настройку профилей хостов с использованием сетевых меток можно выполнить с помощью веб-интерфейса Портала администрирования.

Под профилем хоста понимается совокупность сетевых настроек, основанная на использовании сетевых меток (Network Labels).

Сетевая метка (Network Label) — это текстовая метка (например: "prod", "backup", "vlan100", "management"), которая может быть привязана к:

– логической сети;
– физическим сетевым интерфейсам (NIC) на хостах.

Когда виртуальная машина подключается к сети с определенной меткой, СУСВ автоматически выбирает подходящий физический интерфейс на хосте, где эта метка активна, и подключает виртуальный адаптер к соответствующему VLAN или мосту (рисунок 145).

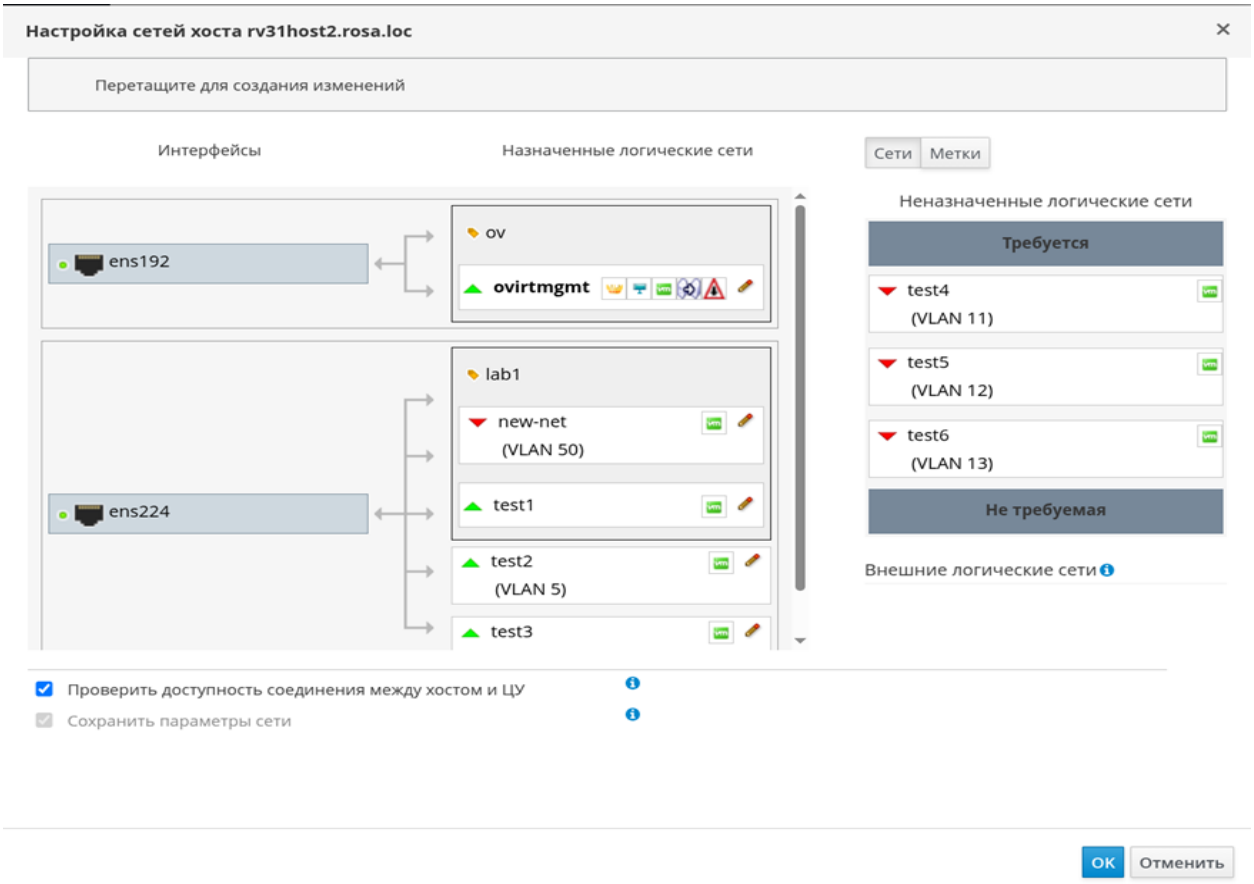


Рисунок 145 – Настройка сетей хоста

Настройка профилей хостов предоставляет возможность:

– централизованно управлять сетевыми конфигурациями;
– обеспечивать единообразие настройки хостов;
– упрощать развертывание и обслуживание инфраструктуры.

3.4.4.11.1 Создание профиля хоста

Для создания профиля хоста необходимо:

а) выбрать нужный хост в разделе "Ресурсы → Хосты" (рисунок 146);

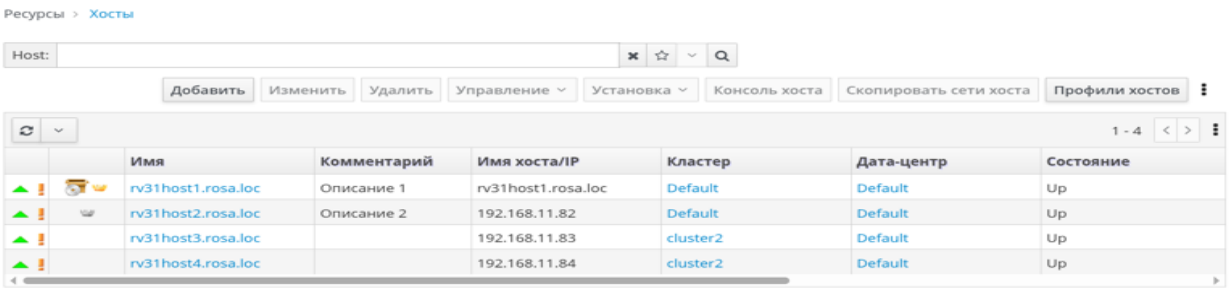


Рисунок 146 – Выбор хоста в разделе "Ресурсы → Хосты"

б) нажать кнопку `Профили хостов` в разделе "Хосты", чтобы открыть форму создания профиля "Профили хостов" (рисунок 147);

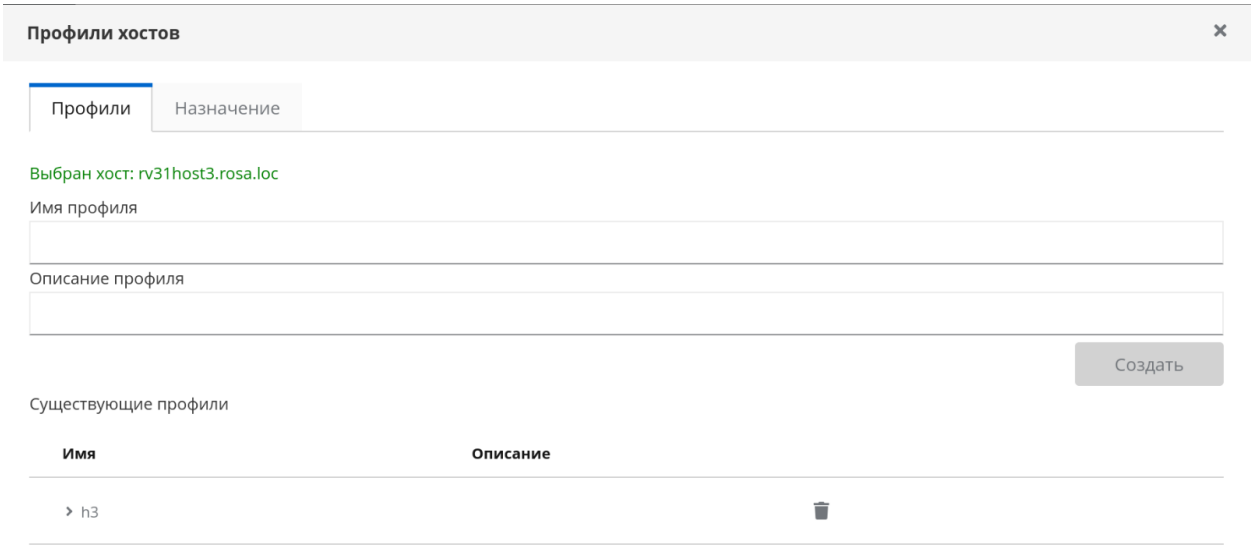


Рисунок 147 – Форма "Профили хостов"

в) указать:

– "Имя профиля" — обязательно;
– "Описание" — опционально (рисунок 148);

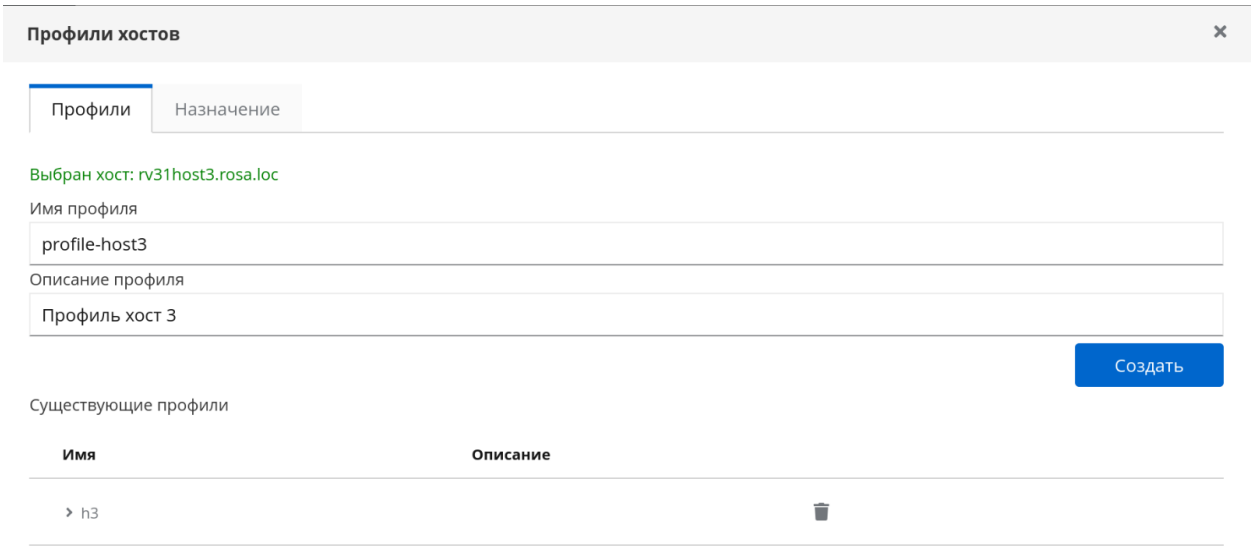


Рисунок 148 – Задание имени и описания профиля

г) нажать кнопку `Создать`.

В результате профиль хоста будет добавлен (рисунок 149).

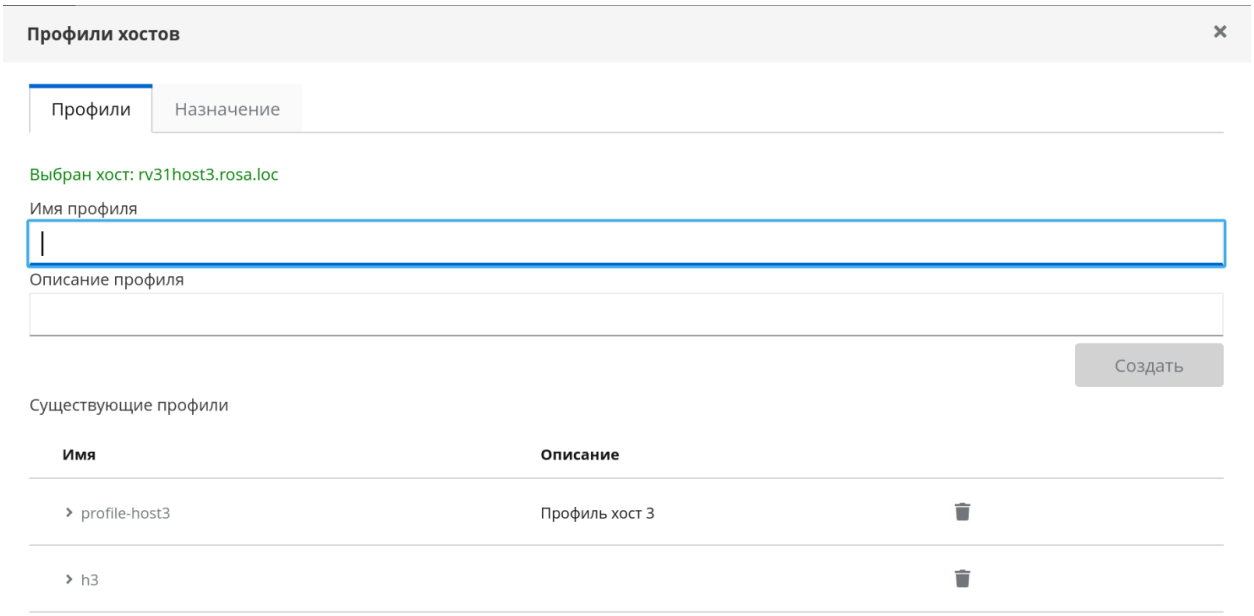


Рисунок 149 – Список доступных профилей хостов

После создания профиль появится в списке. Список отображается в виде древовидной структуры (рисунок 150), где:

– узлы — это профили;

– при раскрытии узла отображаются интерфейсы и соответствующие сетевые метки (рисунок 150).

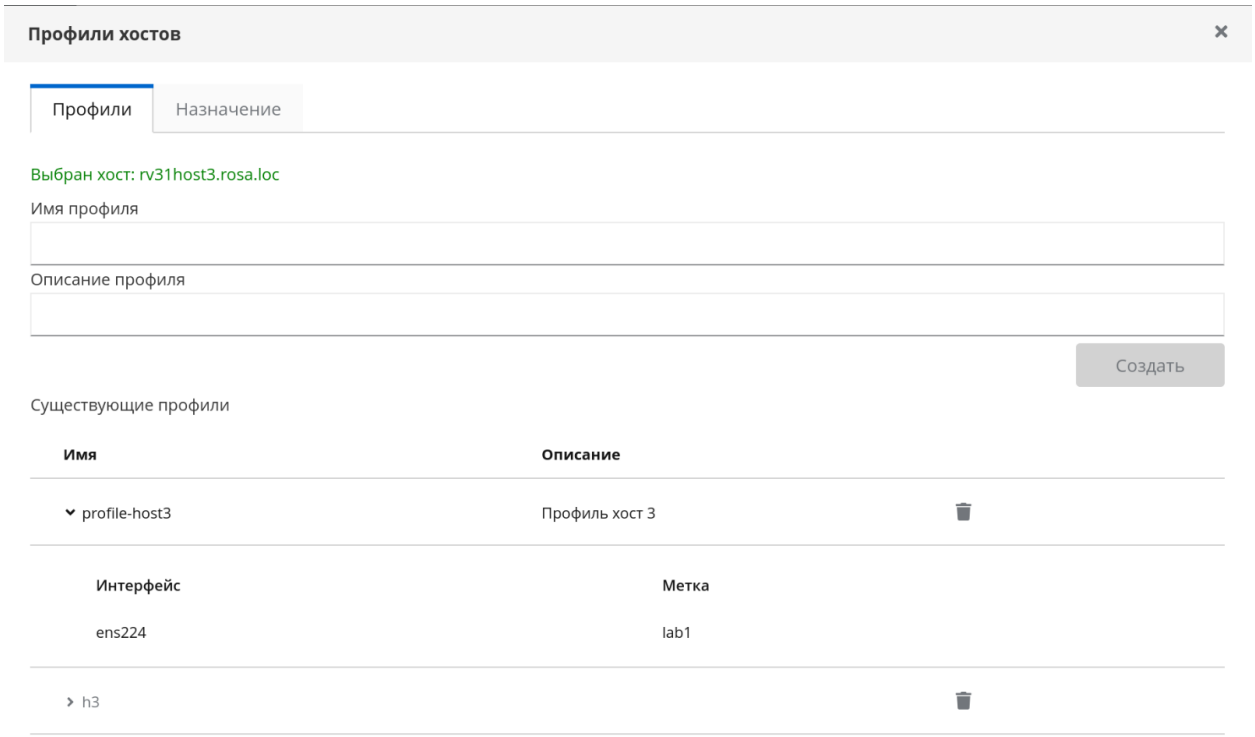


Рисунок 150 – Древовидная структура с параметрами профилей хостов

3.4.4.11.2 Назначение профиля хоста

Для назначения профиля одному или нескольким хостам требуется:

а) перейти на вкладку "Профили хостов → Назначение" (рисунок 151);

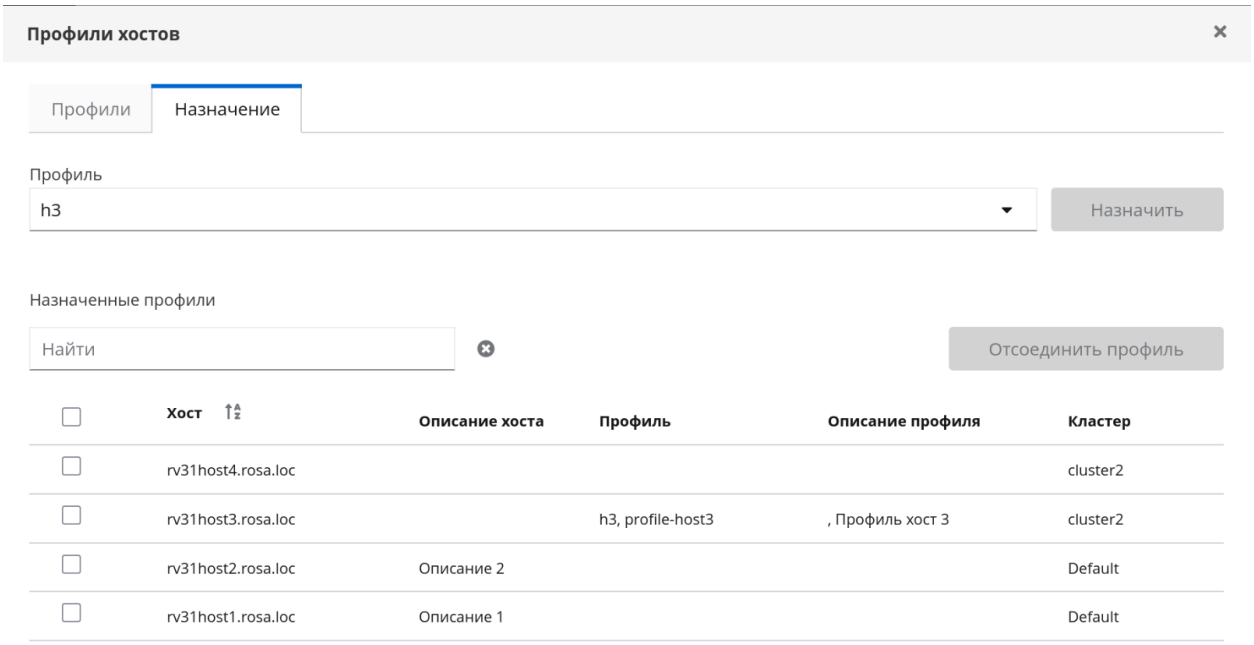


Рисунок 151 – Вкладка "Профили хостов → Назначение"

б) в выпадающем списке "Профиль" выбрать необходимый профиль (рисунок 152);

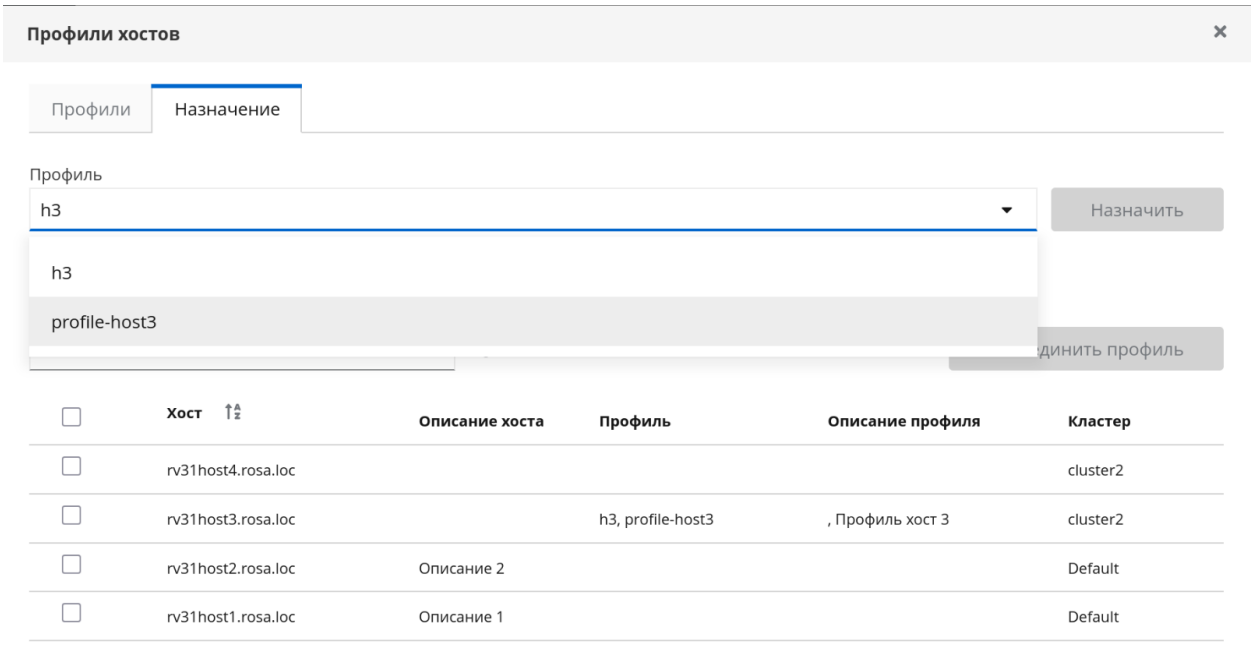


Рисунок 152 – Список доступных профилей хостов

в) в таблице "Назначенные профили" установить флажки напротив нужных хостов (рисунок 153);

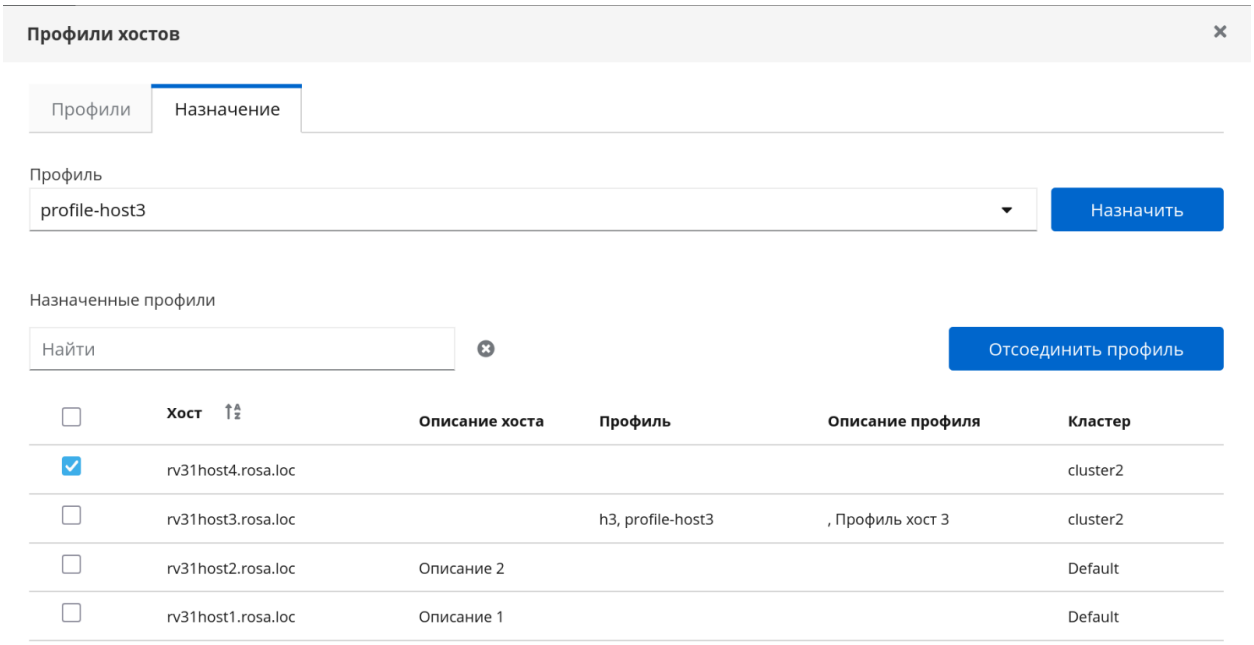


Рисунок 153 – Выбор хостов для назначения профилей

г) нажать кнопку Назначить.

После завершения операции имя профиля появится в столбце "Профиль" у выбранных хостов (рисунок 154).

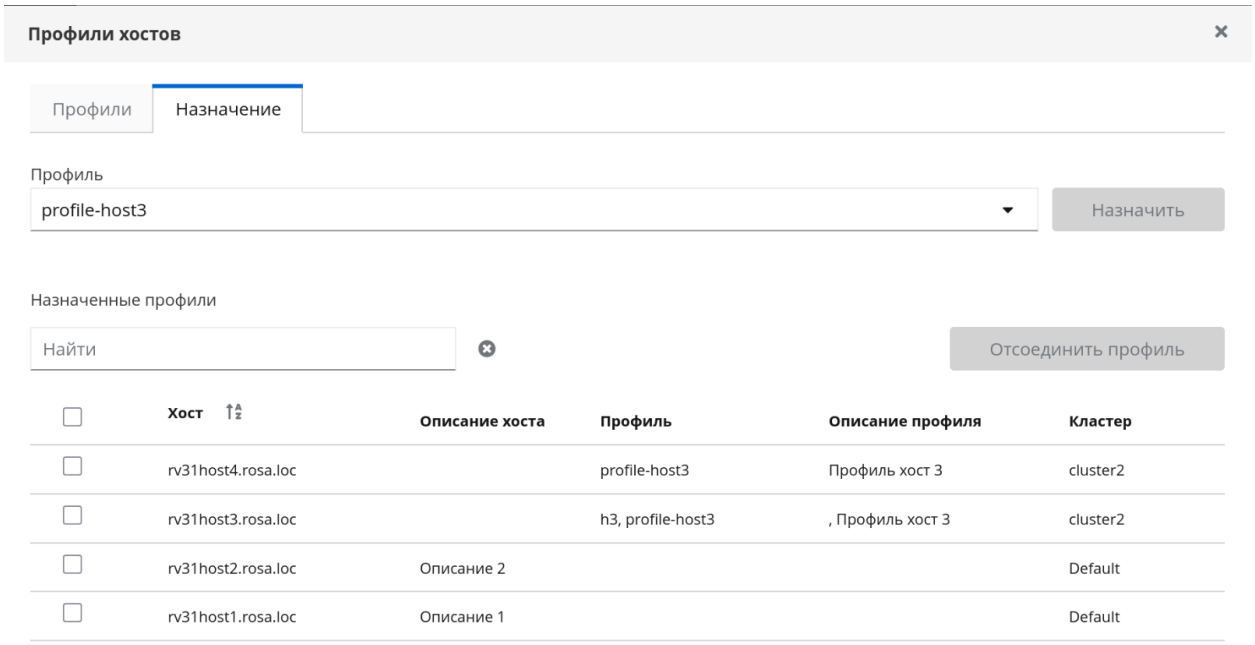


Рисунок 154 – Список хостов, включая хосты с добавленным профилем

3.4.4.11.3 Отсоединение профиля хоста

Для отсоединения профиля от хоста нужно:

а) перейти на вкладку "Профили хостов → Назначение";

б) в списке "Профиль" выбрать профиль, который требуется отсоединить (рисунок 155);

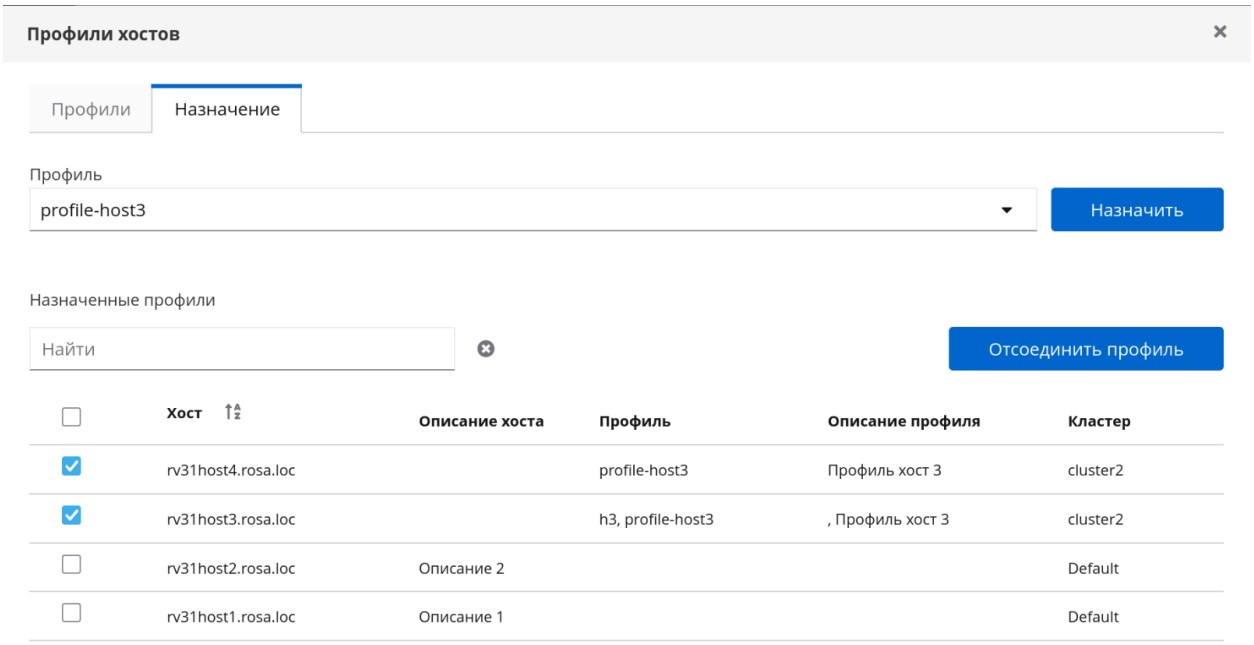


Рисунок 155 – Выбор хостов для отсоединения профиля

в) в таблице "Назначенные профили" отметить хосты, у которых нужно убрать профиль (рисунок 155);

г) нажать кнопку `Отсоединить профиль`.

После выполнения операции имя отсоединяемого профиля исчезнет у выбранных хостов (рисунок 156).

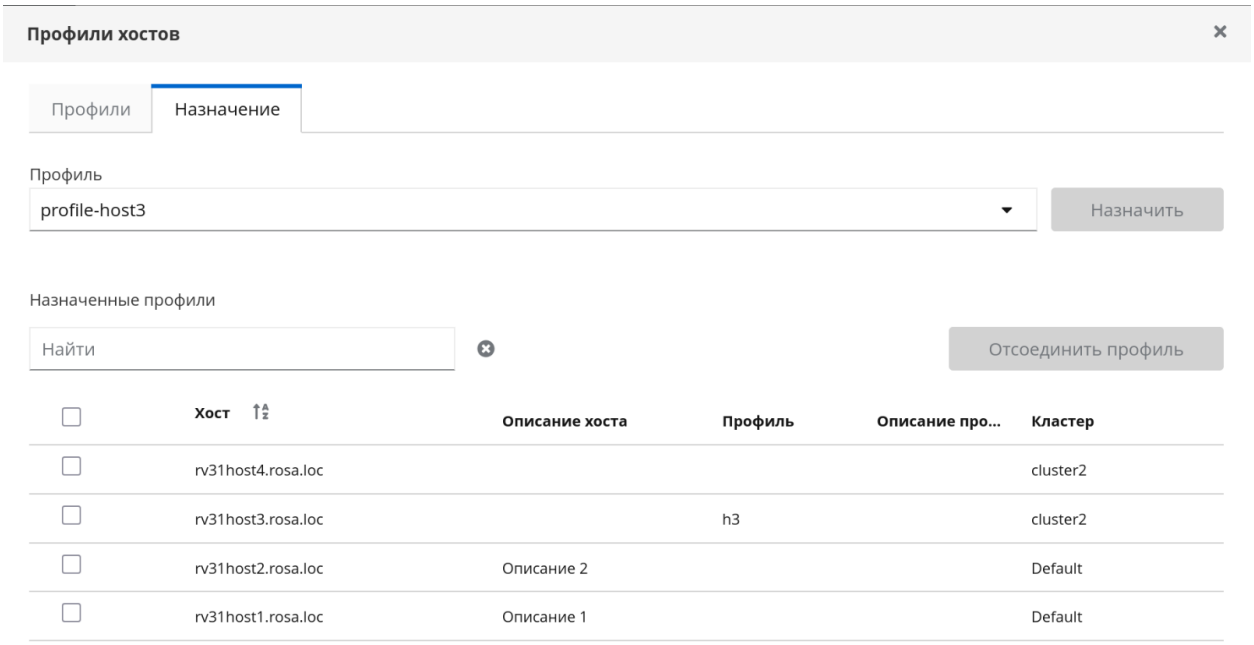


Рисунок 156 – Обновленный список хостов и профилей

3.4.4.11.4 Удаление профиля хоста

Чтобы удалить профиль нужно:

а) перейти на вкладку "Профили" (рисунок 157);
б) в таблице "Существующие профили" найти нужный профиль;
в) нажать пиктограмму удаления рядом с именем профиля.

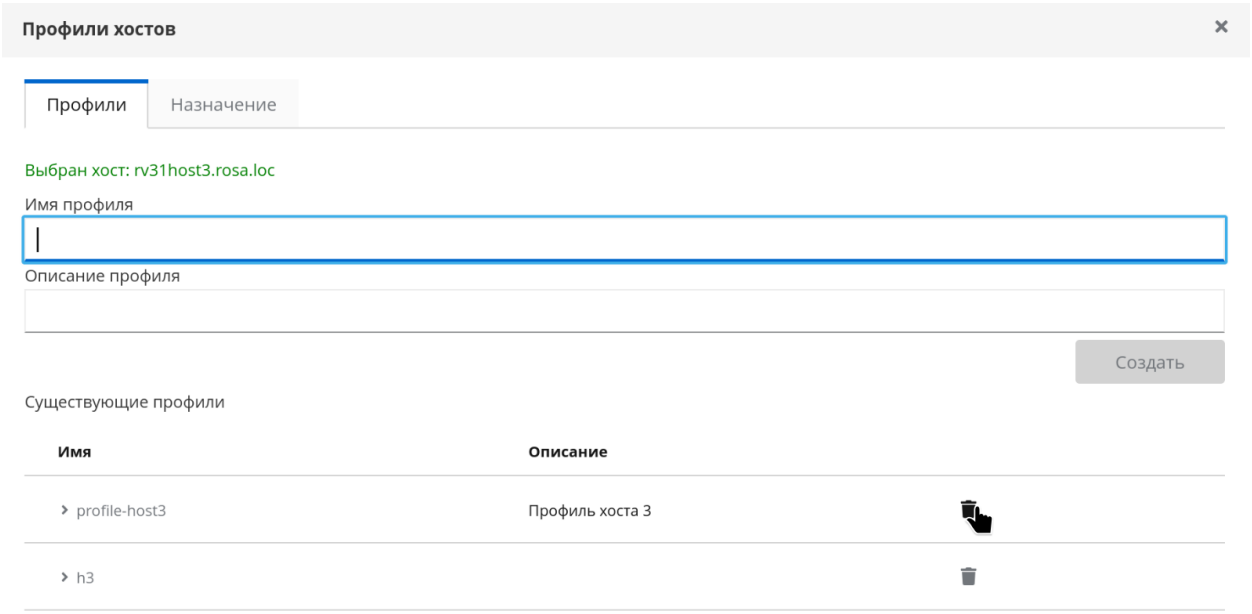


Рисунок 157 – Удаление профиля

Указанный профиль будет удален.

3.4.4.12 Поддержка организации сетей с помощью IPv6

В большинстве контекстов РОСА Виртуализация поддерживает статические сети IPv6.

Примечание — Системе виртуализации РОСА Виртуализация необходима включенная поддержка протокола IPv6 на тех компьютерах или ВМ, где работает виртуализированный ЦУ. Не следует отключать 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.

3.4.5 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 коммутатор 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. 3.4.4.9) для неагрегированных сетевых карт всех хостов кластера или дата-центра.

Если в окружении используется хранилище iSCSI и есть необходимость резервирования (избыточности), см. инструкции для настройки механизма доступа iSCSI по нескольким путям (см. п. 3.6.5.3).

3.4.5.1 Создание устройства сетевой связки вручную на Портале администрирования

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

Для создания устройства связки вручную на Портале администрирования нужно выполнить следующие действия:

а) перейти в "Ресурсы → Хосты";

б) нажать на имя хоста, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Сетевые интерфейсы", чтобы увидеть список физических сетевых интерфейсов, присоединенных к хосту;

г) нажать "Настроить сети хоста";

д) проверить параметры коммутатора. Если на коммутаторе было настроено предоставление информации о протоколе обнаружения топологии канального уровня (LLDP), навести курсор на область физического интерфейса, чтобы просмотреть конфигурацию агрегирования портов коммутатора;

е) переместить 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.

ж) в выпадающих списках "Имя связки" и "Режим связки" выбрать соответствующие пункты;

з) при выборе "Пользовательского" режима связки ввести 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) ввести: "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 ввести: "mode=1 primary=eth0";

и) нажать кнопку OK;

к) присоединить к новой связке логическую сеть, после чего настроить логическую сеть;

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

л) при необходимости, если хост находится в режиме обслуживания, выбрать пункт "Проверить доступность соединения между хостом и ЦУ";

м) нажать кнопку OK.

3.4.5.2 Создание устройства сетевой связки автоматически с помощью службы меток LLDP

Служба меток LLDP дает 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 агрегировать нельзя.

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

Предварительные условия:

– Интерфейс должен быть подключен к коммутатору Juniper.

– Протокол управления агрегированием каналов на коммутаторе Juniper должен быть настроен с использованием LLDP.

Последовательность действий:

а) настроить 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";

б) настроить службу меток LLDP, для чего обновить 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, ввести символ "*" (звездочка). 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, оставить 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";

в) при необходимости можно настроить выполнение службы с другими интервалами, для чего изменить значение параметра "OnUnitActiveSec" в файле /etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer. Значение по умолчанию – "1h" (1 час);

г) выполнить следующую команду для текущего и автоматического (при загрузке) запуска службы:

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

Примечание — Для запуска службы ovirt-lldp-labeler вручную следует выполнить следующую команду:

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

д) присоединить к новой связке логическую сеть, после чего настроить логическую сеть.

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

3.4.5.3 Режимы агрегирования

Алгоритм рассеивания пакетов определяется режимом агрегирования.

Режим агрегирования по умолчанию — "(Режим 4) Динамическое агрегирование каналов".

Система виртуализации РОСА Виртуализация 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 ее заменяет одна из запасных. MAC-адрес этой связки виден только на порте сетевого адаптера, что предотвращает путаницу, которая может случиться в случае смены MAC-адреса связки, в соответствии с MAC-адресом новой активной сетевой карты;

– (Режим 2) Load Balance (balance-xor) — сетевая карта, передающая пакеты, выбирается с помощью выполнения операции XOR для исходного и целевого MAC-адресов, умноженных на фактор modulo общего числа сетевых карт. Этот алгоритм обеспечивает выбор одной и той же сетевой карты для каждого из целевых MAC-адресов;

– (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 нужно выполнить следующую команду:

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

Система виртуализации РОСА Виртуализация 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.

3.5 Хосты

3.5.1 Введение

Хосты, также известные как гипервизоры, — это физические серверы, на которых выполняются гипервизоры РОСА Виртуализация.

Система виртуализации РОСА Виртуализация 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 удаленно 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 в виртуализированном ЦУ можно открыть необходимые порты этих хостов.

3.5.1.1 Общее описание хоста виртуализации

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

Физический хост РОСА Виртуализация должен соответствовать следующим техническим характеристикам:

– принадлежит только одному кластеру в Системе (см. 3.3);

– имеет ЦП с поддержкой модулей аппаратной виртуализации AMD-V или Intel® VT;

– имеет процессор с поддержкой всех функций того типа виртуального ЦП, который был выбран при создании кластера, к которому принадлежит данный хост;

– имеет объем ОЗУ минимум 2 ГБ;

– обслуживается системным администратором с системными полномочиями (администратор имеет права суперпользователя).

3.5.2 Гипервизоры РОСА Виртуализация

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.

3.5.2.1 Доступ к веб-интерфейсу хоста виртуализации

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

Номер порта 9090 — это стандартный номер порта для доступа к веб-интерфейсу Cockpit.

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 отчетов об ошибках (Automatic Bug Reporting Tool).

3.5.3 Задачи при работе с хостами

3.5.3.1 Добавление хостов в виртуализированный ЦУ

Добавление хоста в Систему виртуализации РОСА Виртуализация может занять некоторое время по мере выполнения Системой следующих шагов: проверка требований виртуализации, установка пакетов и создание моста.

Примечание — Перед добавлением хоста в Систему виртуализации РОСА Виртуализация необходимо осуществить его предварительную настройку, аналогичную настройке хоста при первичной установке Системы виртуализации (см. "РОСА Виртуализация 4. Руководство администратора. Часть 1. Установка" РСЮК.10103-01 32 01).

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

3.5.3.1.1 Необходимые условия для добавления нового хоста в инсталляцию РОСА Виртуализация

При добавлении нового хоста в инсталляцию РОСА Виртуализация необходимо добавить на новый хост в конфигурационный файл /etc/hosts информацию обо всех уже имеющихся в Системе виртуализации хостах, СУСВ, сервере IPA (или другом сервере каталогов). В файл /etc/hosts на ранее установленных хостах и в СУСВ добавляется информация о новом хосте.

Процедура добавления хоста в виртуализированный ЦУ включает в себя следующие этапы, описанные в пп. 3.5.3.1.2–3.5.3.1.5:

– Первичная установка и инициализация хоста.
– Настройка системных параметров хоста гипервизора.
– Добавление в файл /etc/hosts на ранее установленных хостах и в СУСВ информации о новом хосте.
– Добавление хоста в виртуализированный ЦУ с использованием Портала администрирования.

3.5.3.1.2 Первичная установка и инициализация хоста

Установка гипервизора РОСА Виртуализация осуществляется непосредственно на физический сервер без предустановленной ОС.

Процедура установки и первичной инициализации хоста описывается в п. 3.2 документа "РОСА Виртуализация 4. Руководство администратора. Часть 1. Установка" (РСЮК.10103-01 32 01).

3.5.3.1.3 Настройка системных параметров хоста гипервизора

Настройка параметров системного окружения осуществляется администратором в консоли каждого из хостов с установленным гипервизором.

3.5.3.1.3.1 Доступ к консоли с использованием веб-интерфейса

Для доступа к консоли в веб-интерфейсе хоста нужно перейти на вкладку "Терминал" панели навигации интерфейса соответствующего хоста гипервизора (рисунок 158).



Рисунок 158 – Консоль хоста в веб-интерфейсе

3.5.3.1.4 Доступ к консоли с использованием командной строки

Для доступа к консоли хоста можно воспользоваться SSH-соединением.

Для получения доступа к консоли через SSH необходимо использовать имя учетной записи суперпользователя root и пароль, выбранный ранее при установке, а именно выполнить команду в терминале, указав имя хоста (в примере ниже имя хоста host1.rosa.lan следует заменить на имя хоста, развернутого в вашем ЦОД):

```
# ssh root@host1.rosa.lan
```

Примечание – Команды по настройке хоста, указанные в п. 3.5.3.1.4.2, могут выполняться в консоли с доступом через SSH или в терминале, открытом в браузере веб-интерфейсе администрирования хоста

3.5.3.1.4.1 Разрешение имен DNS

При отсутствии в сети сервера DNS можно использовать конфигурационный файл /etc/hosts для настройки разрешения имен DNS в IP-адреса сетевых ресурсов.

Конфигурационный файл /etc/hosts содержит построчный список IP-адресов и соответствующих имен DNS для их преобразования при обращении.

3.5.3.1.4.2 Редактирование файла /etc/hosts с именами хостов

В консоли хоста нужно открыть редактор mc (mcedit) и указать в файле /etc/hosts IP-адреса и имена DNS взаимодействующих компонентов РОСА Виртуализация – хостов с установленными гипервизорами, ВМ СУСВ и сервера IPA.

Для начала редактирования файла /etc/hosts с использованием редактора mcedit нужно выполнить команду в консоли:

```
# mcedit /etc/hosts
```

После завершения редактирования следует выйти из редактора, сохранив результат. Для выхода из редактора можно использовать клавишу `Esc`. Если в файл были внесены изменения, то будет предложено их сохранить или выйти без сохранения. Для сохранения внесенных изменений при выходе из редактора необходимо выбрать в диалоговом окне "Сохранить при выходе" опцию "Да".

Примечания:

– Для сохранения результатов редактирования файла в редакторе mcedit следует нажать `F2`. Для выхода из редактора нажимают `F10`. При использовании редактора в окне браузера также можно нажать на кнопки `F2` и `F10`, используя курсор мыши и левую клавишу мыши.

– Также можно использовать для редактирования любой другой текстовый редактор, например vi. Для редактирования файла с использованием редактора vi нужно выполнить команду:

```
# vi /etc/hosts
```

Для выхода из редактора vi необходимо использовать команду `:q`.

Для перехода в режим редактирования в редакторе vi (режим INSERT) можно нажать клавишу `Insert`. После внесения необходимых изменений следует нажать клавишу `Esc`, затем ввести команду `:x`.

Пример файла /etc/hosts с IP-адресами и именами DNS взаимодействующих компонентов РОСА Виртуализация – хостов с установленными гипервизорами, ВМ СУСВ и сервера IPA:

```
10.10.20.4     susv.rosa.lan       # ВМ СУСВ
10.10.20.6     host1.rosa.lan      # хост гипервизора
10.10.20.7     host2.rosa.lan      # хост гипервизора
10.10.20.8     host3.rosa.lan      # хост гипервизора
10.10.20.9     ipa.rosa.lan        # сервер IPA
10.10.20.10    host4.rosa.lan      # хост гипервизора
```

Данный пример файла /etc/hosts предполагает, что ранее в РОСА Виртуализация уже были установлены хосты host1 – host3, и сейчас осуществляется добавление нового хоста host4. Файл добавляется на новый хост host4. На ранее установленные хосты и в СУСВ необходимо добавить строку в файл /etc/hosts с указанием IP адреса нового хоста:

```
10.10.20.10    host4.rosa.lan      # хост гипервизора
```

Важно – Эта операция должна быть выполнена на каждом из ранее установленных хостов и в СУСВ.

Важно – При наличии в сетевом окружении сервера DNS соответствующие записи с именами хостов и их IP-адресами должны быть внесены на сервер DNS. При этом добавленные имена хостов должны быть разрешимы на каждом из хостов и в СУСВ.

Примечание – Указание в файле /etc/hosts IP-адресов и имен DNS взаимодействующих компонентов РОСА Виртуализация позволяет обеспечить функционирование системы при недоступном корпоративном DNS сервере.

После завершения настройки системных параметров нового хоста гипервизора можно переходить к его добавлению в виртуализированный ЦУ.

3.5.3.1.5 Добавление хоста в виртуализированный ЦУ

Для добавления хоста в виртуализированный ЦУ нужно выполнить следующие действия:

а) в главном меню Портала администрирования перейти в "Ресурсы → Хосты", и откроется форма с отображением информации о доступных хостах (рисунок 159);

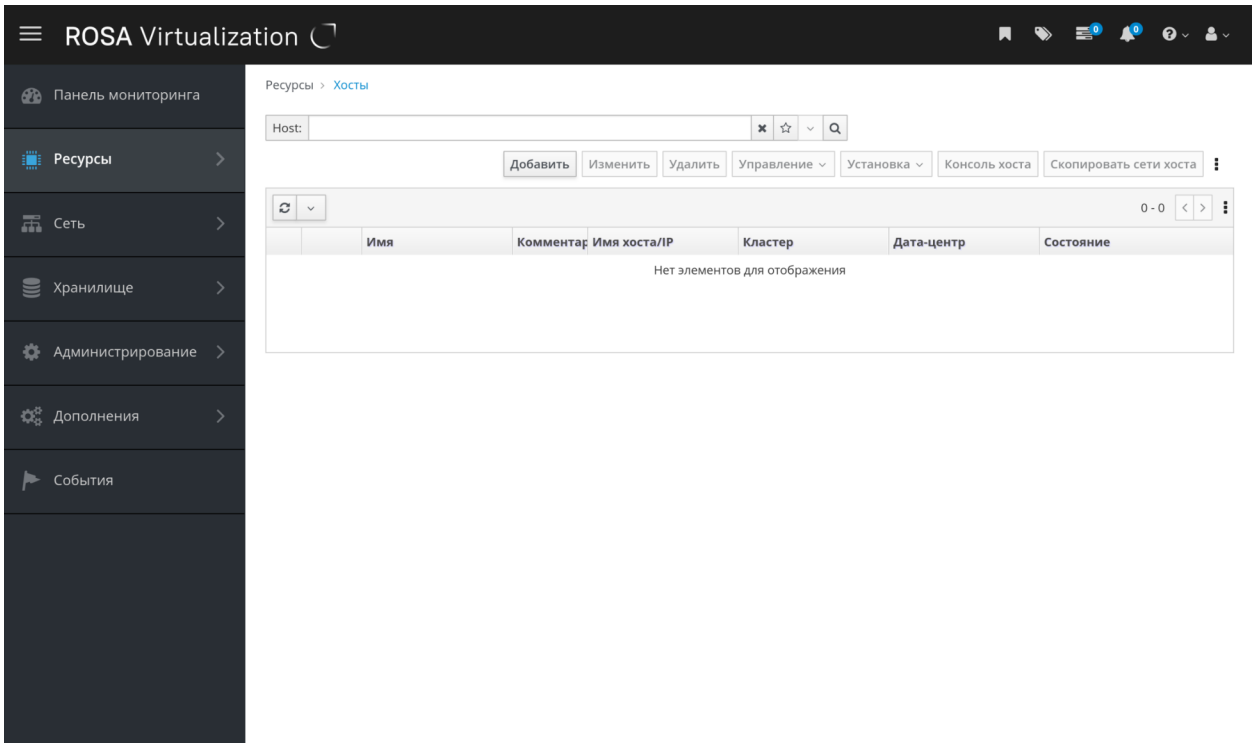


Рисунок 159 – Форма "Ресурсы → Хосты" с отображением информации о доступных хостах

б) нажать кнопку Добавить для добавления хоста в РОСА Виртуализация, и откроется форма "Новый хост" для определения параметров добавляемого хоста (рисунок 160);

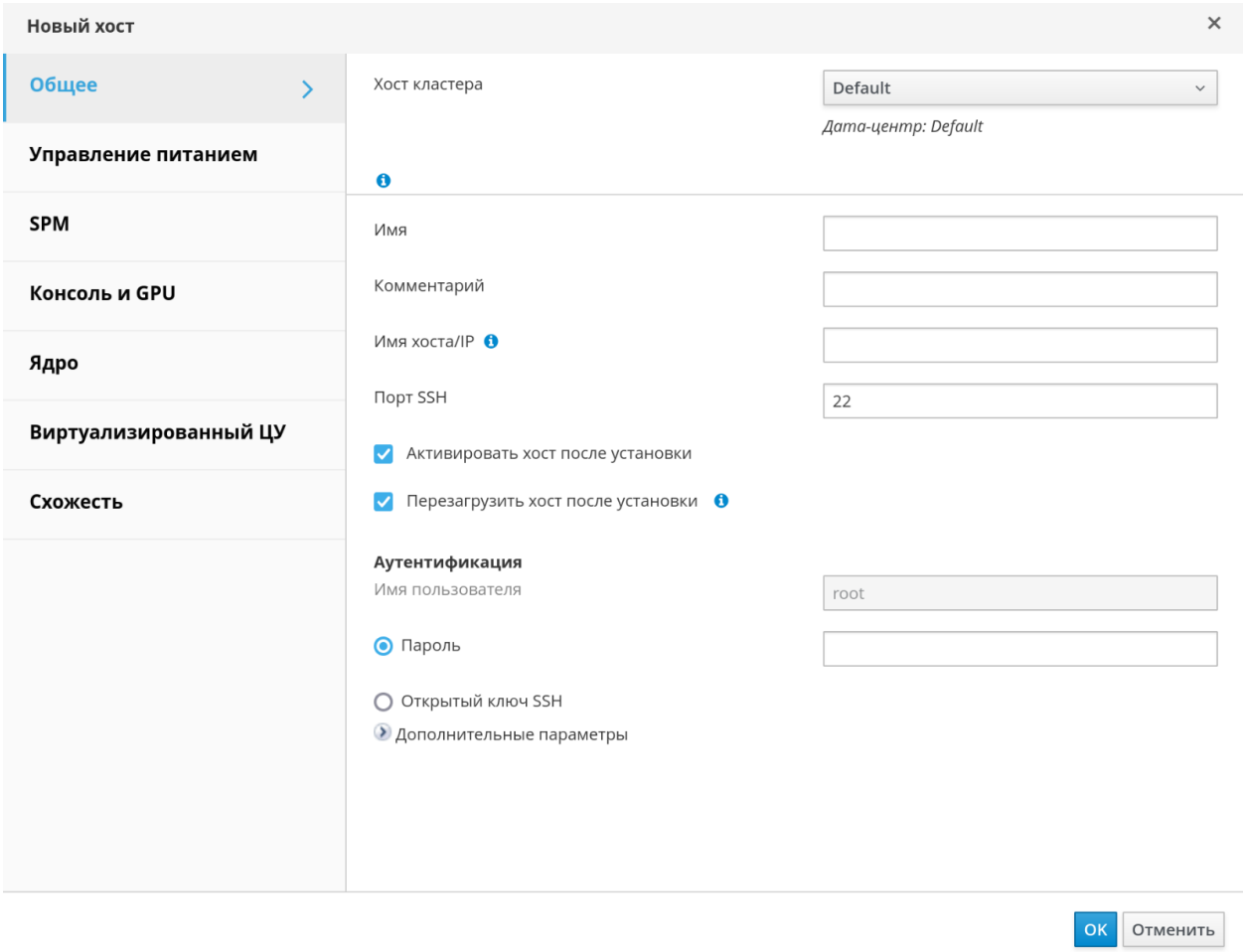


Рисунок 160 – Форма "Новый хост". Вкладка "Общие"

в) из выпадающего списка выбрать "Дата-центр" и "Хост кластера" для нового хоста. По умолчанию используется дата-центр default и кластер default;

г) указать "Имя хоста / IP" нового хоста (рисунок 160). В поле "Порт SSH" автоматически добавится стандартный номер порта SSH — 22;

д) выбрать метод аутентификации, используемый диспетчером виртуализации для подключения к хосту:

– при использовании аутентификации по паролю ввести пароль суперпользователя root в поле "Пароль";

– при использовании аутентификации по открытому ключу SSH скопировать ключ из поля "Открытый ключ SSH" (рисунок 161) в файл /root/.ssh/authorized_keys на хост, добавляемый в СУСВ;

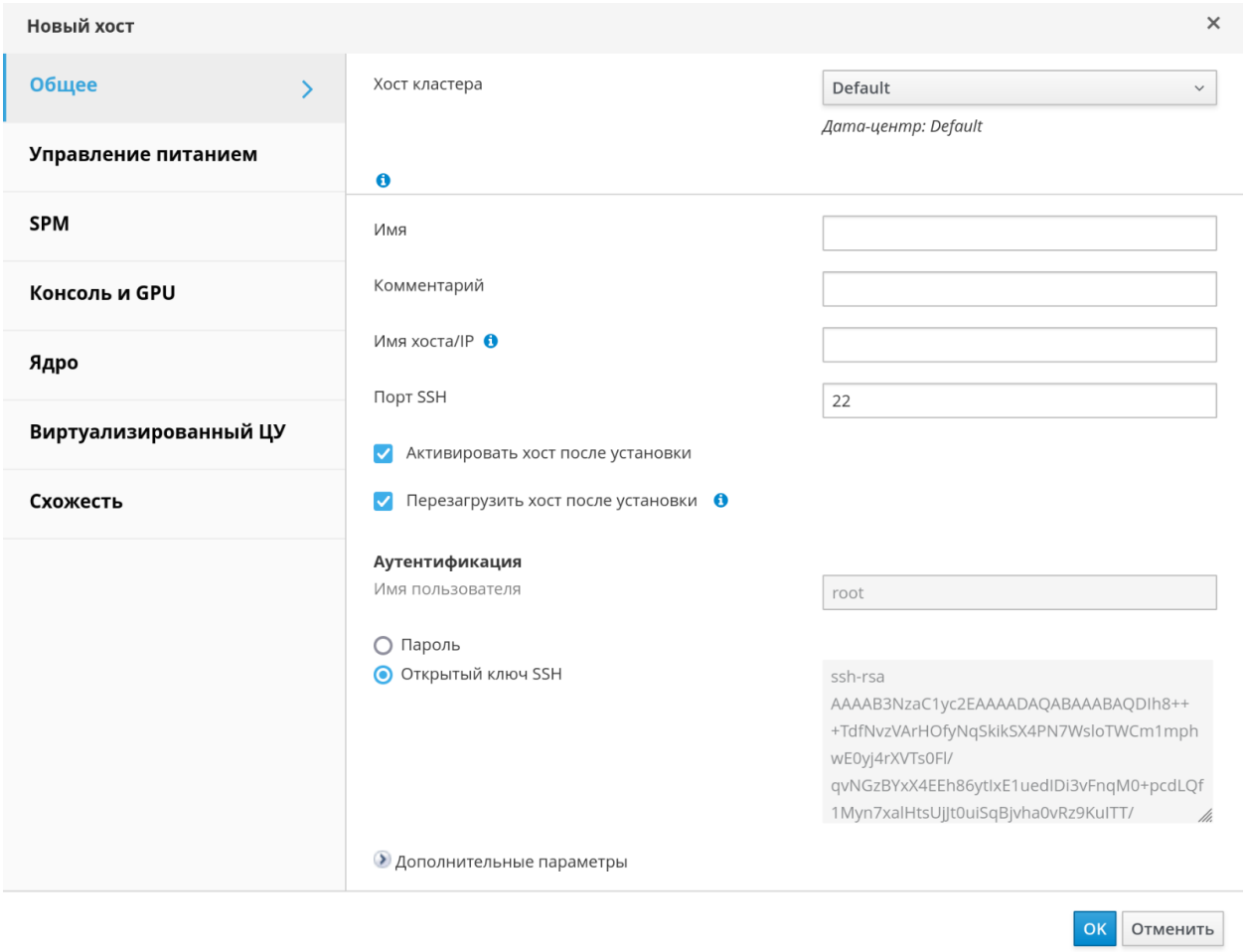


Рисунок 161 – Ключ из поля "Открытый ключ SSH" необходимо скопировать на хост

е) опционально нажать на кнопку Дополнительные параметры (рисунок 162), 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;

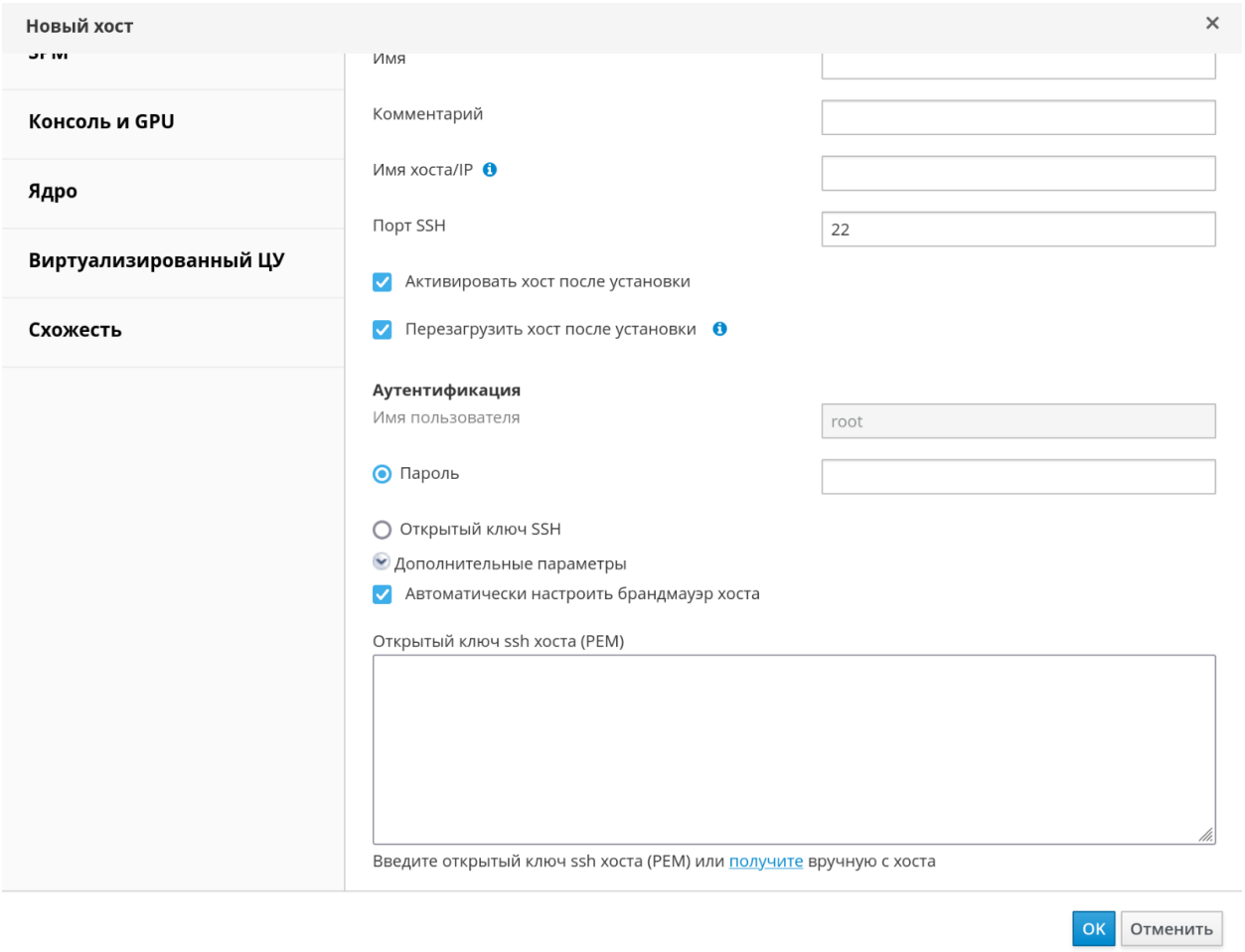


Рисунок 162 – "Новый хост" — настройка дополнительных параметров

б) опционально настроить "Управление питанием" на вкладке "Управление питанием" (рисунок 163), если у хоста есть поддерживаемая карта управления питанием;

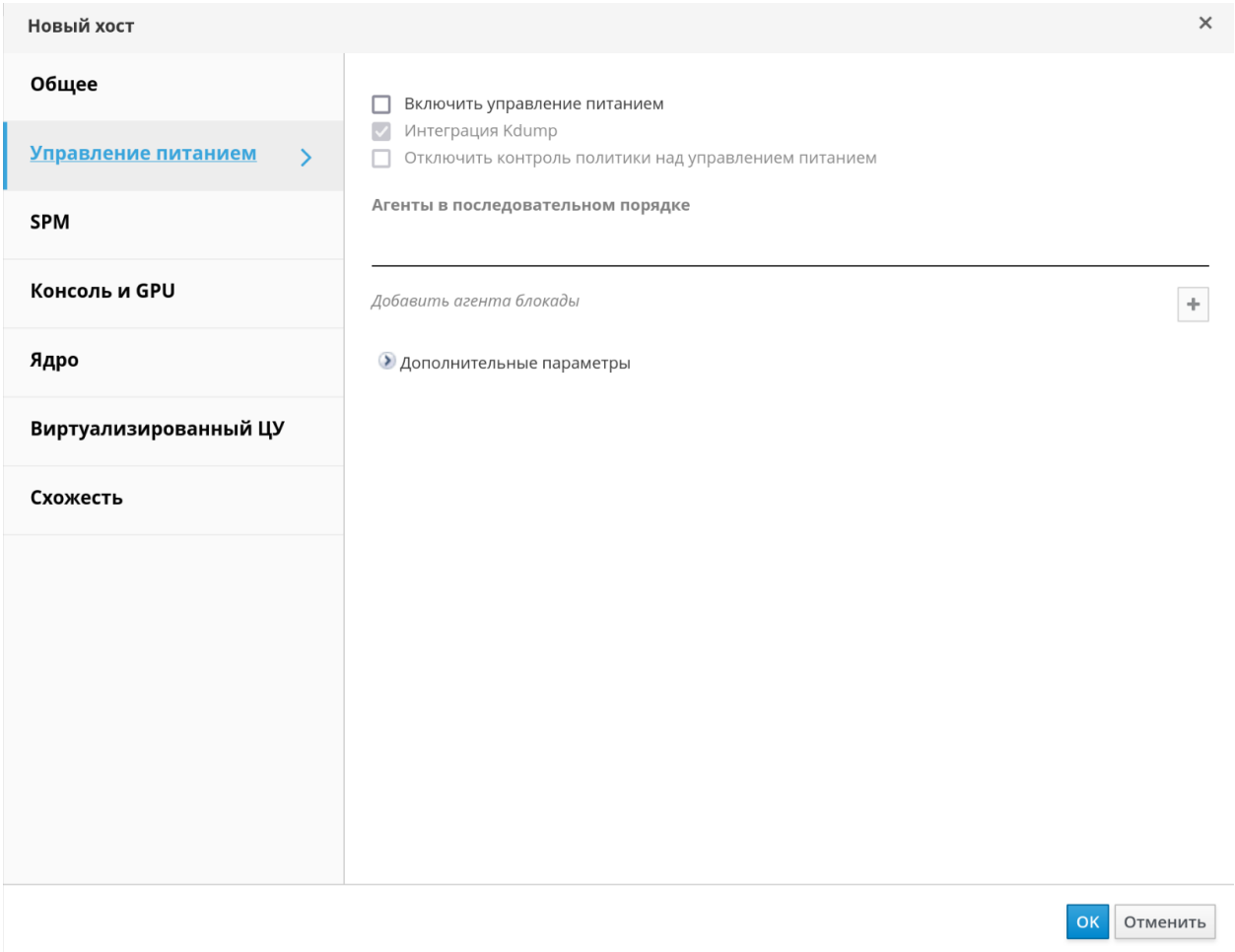


Рисунок 163 – "Новый хост" — вкладка "Управление питанием"

ж) нажать кнопку OK.

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

После некоторого ожидания статус хоста сменится на "Запущен".

3.5.3.2 Параметры хоста

3.5.3.2.1 Общие параметры

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

В таблице 50 описываются параметры вкладки "Общие" окон "Новый хост" или "Параметры хоста".

Таблица 50 – Общие "Параметры хоста"

Поле	Описание
Кластер хоста	Кластер и дата-центр, к которым принадлежит хост
Использовать Foreman/Satellite	Установить или снять 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, введенными 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 см. в документации поставщика). Для просмотра всех хостов оставить это поле пустым

Поле	Описание
Имя	Имя хоста. У этого текстового поля имеется ограничение в 40 символов, а введенное наименование должно быть уникальным сочетанием любых строчных или прописных букв, цифр, дефисов и знаков подчеркивания
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 скопировать 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 включен по умолчанию
Отпечаток SSH	Этот дополнительный параметр предоставляет возможность получить отпечаток SSH хоста и сопоставить его с ожидаемым отпечатком, проверив таким образом их соответствие

3.5.3.2.2 Параметры вкладки "Управление питанием"

В таблице 51 описываются параметры вкладки "Управление питанием" (рисунок 163) окон "Новый хост" или "Параметры хоста".

Таблица 51 – Параметры управления питанием хоста

Поле	Описание
Включить управление питанием	Включает "Управление питанием" на хосте. Установить флажок для этого параметра для активации остальных полей во вкладке "Управление питанием"
Интеграция kdump	Предотвращает проведение операции блокады на хосте во

Поле	Описание
	время выполнения аварийного дампа ядра, чтобы не прерывать дамп
Отключить контроль политики над управлением питанием	Управление питанием контролируется "Политикой планирования" кластера хоста. При включенном управлении питанием и достижении указанного значения низкого потребления виртуализированный ЦУ выключит машину хоста и запустит ее снова из расчета балансировки нагрузки или при недостаточном числе свободных хостов в кластере. Установить 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 начнет работу. Для смены последовательности, в которой используются агенты, использовать кнопки со стрелками ↑ (вверх) и ↓ (вниз). Чтобы сделать двух агентов операции блокады параллельными, выбрать 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 нажать на кнопку со знаком +. В результате будет открыто окно "Параметры агента блокады"
Предпочитаемый	По умолчанию этот дополнительный параметр указывает,

Поле	Описание
прокси для управления питанием	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 таблице 52 содержится описание полей в окне "Параметры агента блокады".

Таблица 52 – Параметры агента блокады

Поле	Описание
Адрес	Адрес для доступа к устройству управления питанием хоста. указать разрешаемое имя хоста или IP-адрес
Имя пользователя	Учетная 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	Выбрать 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 – удаленный супервизор-адаптер IBM Bladecenter; – cisco_ucs – Cisco Unified Computing System; – drac5 – контроллер удаленного доступа Dell для компьютеров Dell; – drac7 – контроллер удаленного 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 – удаленный супервизор-адаптер IBM; – rsb – интерфейс управления Fujitsu-Siemens RSB;

Поле	Описание
	– 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
Защищенное	Установить флажок для защищенного подключения к хосту с помощью SSH, SSL или других протоколов аутентификации, в зависимости от агента управления питанием хоста

3.5.3.2.3 Параметр вкладки "SPM"

В таблице 53 описывается параметр вкладки "SPM" окон "Новый хост" или "Параметры хоста" (рисунок 164).

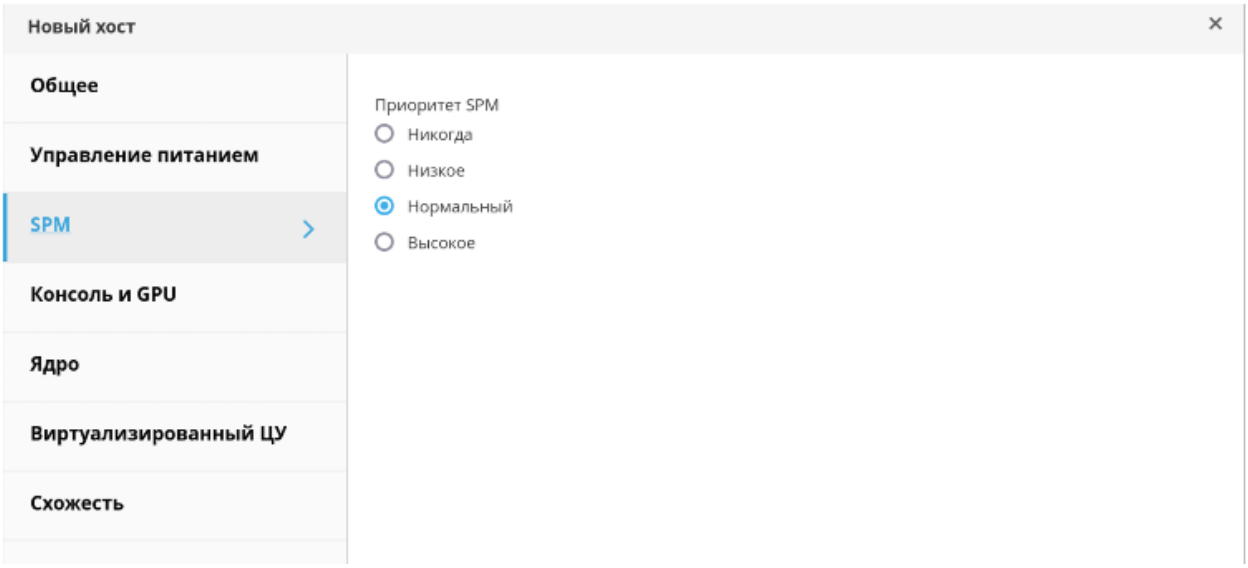


Рисунок 164 – Вкладка "SPM"

Таблица 53 – Параметр приоритета SPM

Поле	Описание
Приоритет SPM	Определяет вероятность того, что хосту будет присвоена роль SPM (диспетчера пула хранилища). Выбрать "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

3.5.3.2.4 Параметры вкладки "Консоль и GPU"

В таблице 54 описываются параметры вкладки "Консоль и GPU" окон "Новый хост" и "Параметры хоста" (рисунок 165).

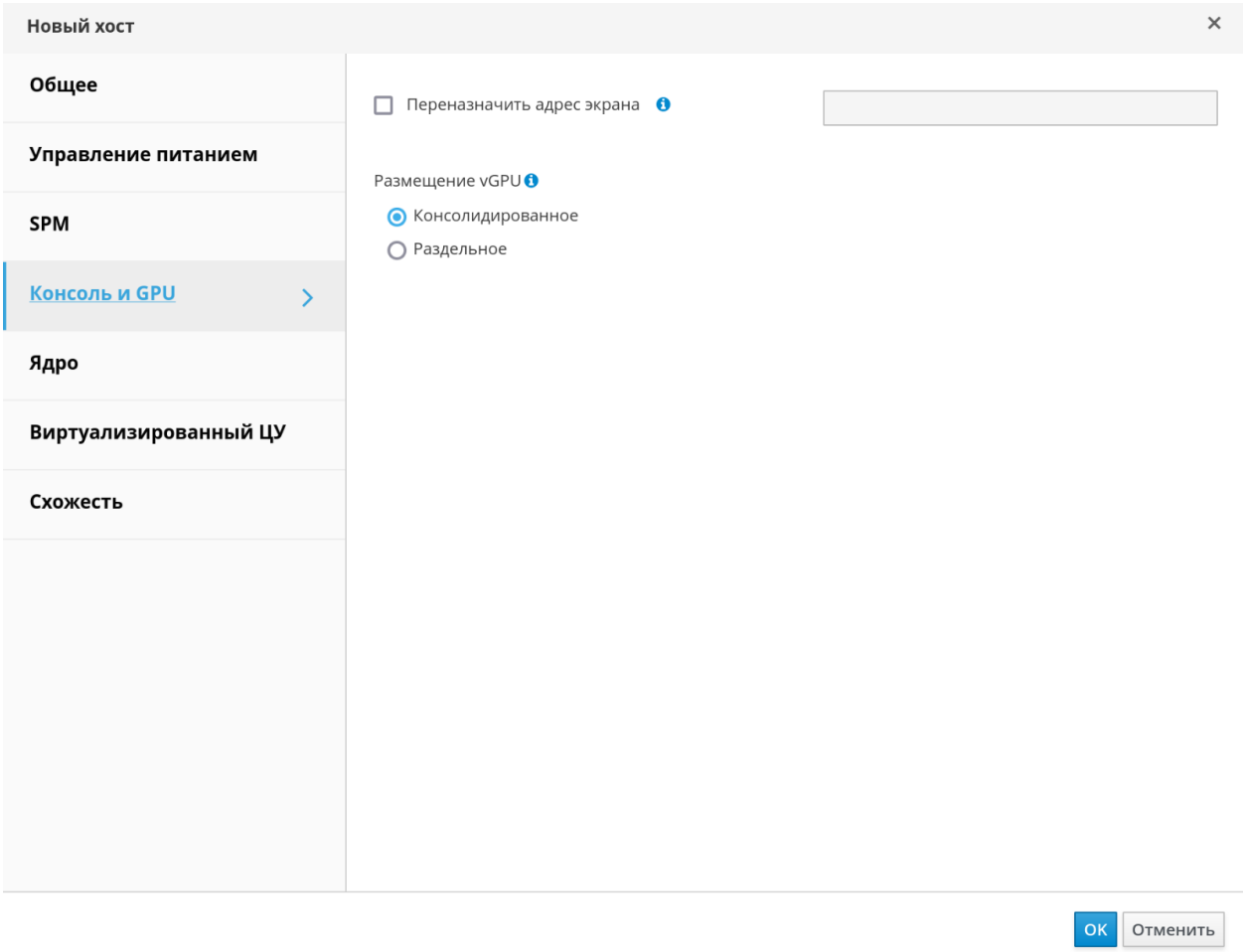


Рисунок 165 – Вкладка "Консоль и GPU"

Таблица 54 – Параметры вкладки "Консоль и GPU"

Поле	Описание
Переназначить адрес экрана	Установить 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.

Поле	Описание
	Адрес должен указываться в формате FQDN или IP
Размещение vGPU	Выбрать тип размещения vGPU: – Консолидированное – предпочтительным является запуск как можно большого числа vGPU на доступных физических картах. – Раздельное – каждый vGPU размещается на отдельной физической карте.

3.5.3.2.5 Параметр вкладки "Поставщик сети"

В таблице 55 описывается параметр вкладки "Поставщик сети" окон "Новый хост" и "Параметры хоста".

Таблица 55 – Параметр вкладки "Поставщик сети"

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

3.5.3.2.6 Параметры вкладки "Ядро"

В таблице 56 описываются параметры вкладки "Ядро" (рисунок 166) окон "Новый хост" и "Параметры хоста".

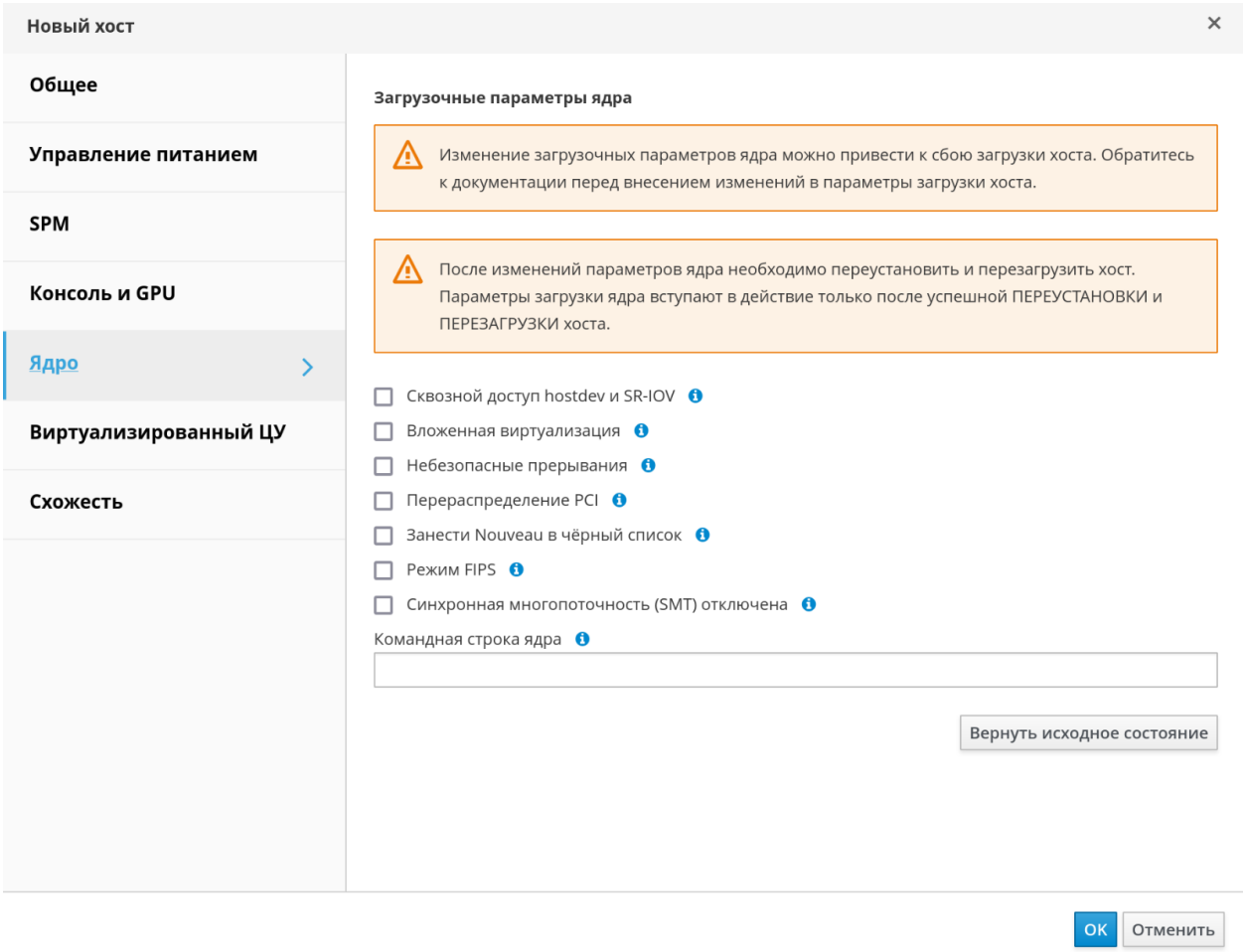


Рисунок 166 – Вкладки "Ядро" (параметры ядра хоста)

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

Для более сложного редактирования и добавления любых необходимых дополнительных параметров можно использовать 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, присоединенных к виртуализированному ЦУ, эти хосты необходимо перевести в "режим обслуживания". Затем для применения внесенных изменений эти хосты необходимо переустановить.

Таблица 56 – 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 подключенного к ВМ. Аппаратное и программное обеспечение должны поддерживать IOMMU. Для аппаратного обеспечения должны быть включены модули виртуализации и IOMMU.
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 в промышленном режиме. На хосте должна быть установлена ловушка vdsm-hook-nestedvt
Небезопасные прерывания	Параметр может быть включен в случаях сбоя сквозного доступа при активированном IOMMU. **Следует обратить 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 включен, 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. Этот параметр рассматривается только как обходное решение при использовании несертифицированного аппаратного обеспечения для задач оценки
Занести Nouveau в черный список	При использовании драйвера vGPU поставщика установить этот флажок, чтобы избежать конфликтов с драйвером Nouveau
Режим FIPS	Установить флажок для этого параметра, чтобы

Поле	Описание
	включить режим FIPS
Синхронная многопоточность (SMT) отключена	Установить флажок для этого параметра, чтобы отключить гиперпоточность
Командная строка ядра	Поле дает возможность добавить дополнительные параметры ядра к параметрам по умолчанию

Примечания:

– В случае если параметры загрузки ядра отображаются серым цветом, следует нажать на кнопку Сбросить. В результате параметры загрузки ядра станут доступны.

– В IBM POWER8 функционал IOMMU активирован по умолчанию.

3.5.3.2.7 Параметр вкладки "Виртуализированный ЦУ"

В таблице 57 описывается параметр вкладки "Виртуализированный ЦУ" (рисунок 167) окон "Новый хост" и "Параметры хоста".

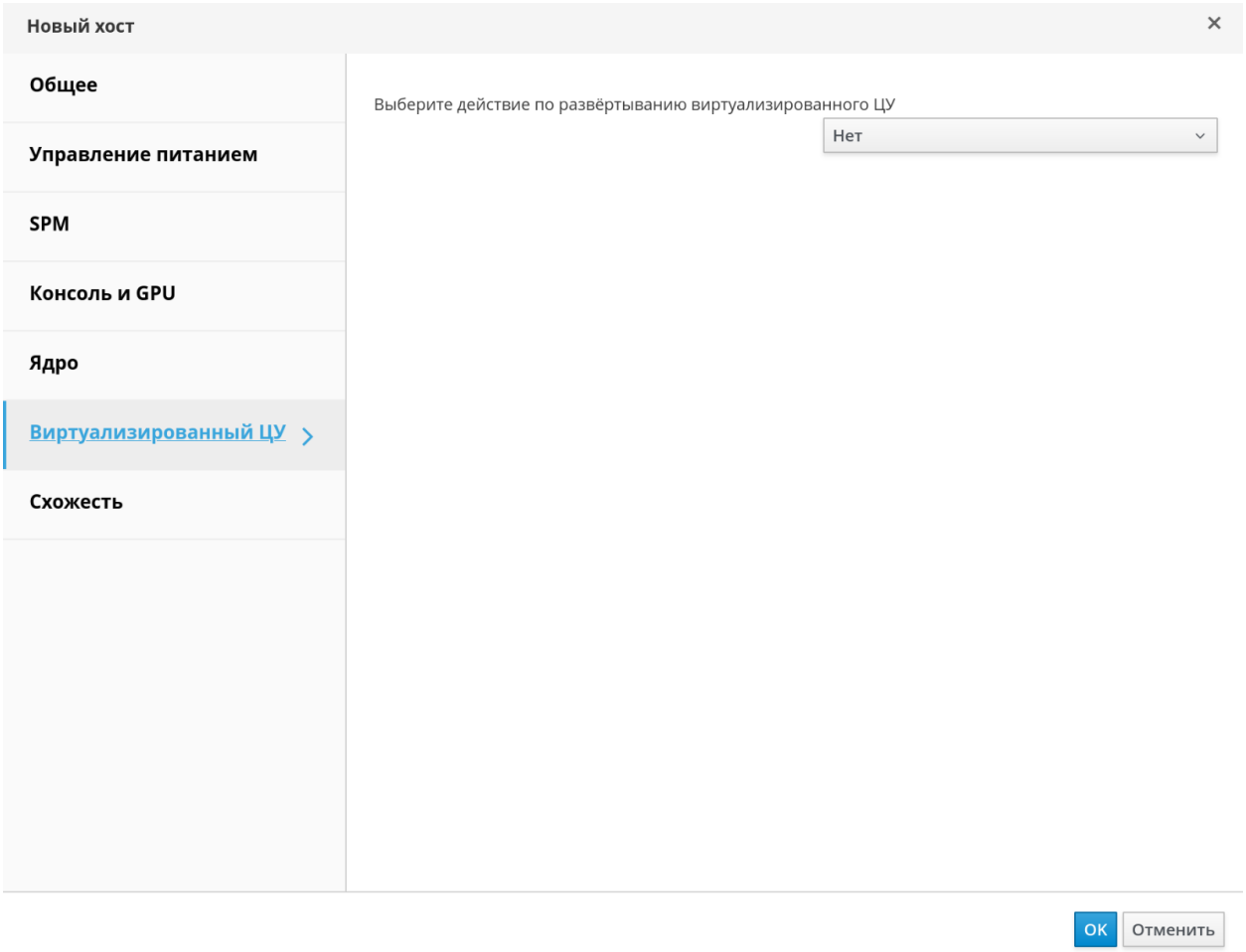


Рисунок 167 – Вкладка "Виртуализированный ЦУ"

Таблица 57 – Параметр вкладки "Виртуализированный ЦУ"

Поле	Описание
Выберите действие по развертыванию виртуализированного ЦУ	Выбрать действие по развертыванию виртуализированного ЦУ: – Нет — никаких действий не требуется; – Развернуть — выбрать 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 — выбрать это действие для узла виртуализированного ЦУ, чтобы свернуть установку хоста и удалить все конфигурации, относящиеся к

Поле	Описание
	виртуализированному ЦУ

3.5.3.3 Настройка параметров управления питанием хоста

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

Для настройки параметров управления питанием хоста необходимо:

а) в главном меню Портала администрирования выбрать "Ресурсы → Хосты" и выбрать хост;

б) выбрать "Управление → Обслуживание" и нажать кнопку OK для подтверждения;

в) после перевода хоста в режим обслуживания нажать кнопку Изменить;

г) перейти на вкладку "Управление питанием";

д) установить флажок "Включить управление питанием", чтобы активировать соответствующие поля;

е) установить 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".

ж) опционально установить флажок "Отключить контроль управления питанием со стороны политики", если "Управление питанием" хоста не должно контролироваться политикой планирования кластера хоста;

з) для добавления нового устройства управления питанием нажать на кнопку +;

и) в окне "Параметры агента блокады" указать "Имя пользователя" и "Пароль" для устройства управления питанием;

к) выбрать "Тип" устройства управления питанием из выпадающего списка;

л) в поле "Адрес" указать IP-адрес;

м) указать номер "Порта SSH", используемого устройством управления питанием для связи с хостом;

н) указать номер "Слота", используемого для идентификации платы устройства управления питанием;

о) настроить "Параметры" устройства управления питанием в форме списка записей "ключ-значение", разделенных запятыми;

Примечание — В случае использования как адресов IPv4, так и адресов IPv6 (по умолчанию), следует оставить поле "Параметры" пустым. При использовании только адресов IPv4 нужно ввести в поле "Параметры" значение "inet4_only=1", а при использовании только адресов IPv6 ввести в поле "Параметры" значение "inet6_only=1".

п) установить флажок "Защищенное", чтобы включить защищенное соединение между устройством управления питанием и хостом;

р) чтобы убедиться в том, что все значения корректны, нажать кнопку Проверка. В случае успешной проверки будет показано сообщение: "Проверка выполнена, статус хоста: запущен";

с) нажать кнопку OK, чтобы закрыть окно "Параметры агента блокады";

т) во вкладке "Управление питанием" при необходимости развернуть "Дополнительные параметры" и с помощью кнопок со стрелками ↑ (вверх) и ↓ (вниз) настроить порядок, в котором виртуализированный ЦУ будет выполнять поиск прокси для операции блокады в кластере хоста и в дата-центре;

у) нажать кнопку OK.

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

3.5.3.4 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).

Для настройки параметра приоритета SPM нужно выполнить следующие действия:

а) перейти в "Ресурсы → Хосты";

б) нажать кнопку Изменить;

в) перейти на вкладку "SPM" (рисунок 164);

г) установить 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;

д) нажать кнопку OK.

3.5.3.5 Настройка на хосте сквозного доступа к PCI

В данном разделе описывается, как установить и настроить технологию SR-IOV в РОСА Виртуализация.

Включение технологии сквозного доступа дает 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.

Для подготовки хоста для применения сквозного доступа к PCI необходимо:

а) включить в BIOS модули виртуализации и IOMMU;

б) включить флаг "IOMMU" в ядре.

Для этого нужно установить флажок "Сквозной доступ к устройству хоста и SR-IOV" при добавлении хоста в виртуализированный ЦУ или вручную отредактировать 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 присоединен к виртуализированному ЦУ, необходимо сначала перевести хост в режим обслуживания.

Для ручной активации IOMMU нужно выполнить следующие действия:

а) отредактировать конфигурационный файл загрузчика grub:

– для Intel® добавить 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 добавить 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, следует использовать исходный параметр on.

б) если сквозной доступ будет неудачным по причине отсутствия поддержки переназначения прерываний аппаратными составляющими, то в случае доверенных ВМ использовать 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 добавить запись "allow_unsafe_interrupts=1" в строку options в конфигурационном файле /etc/modprobe.d:

```
options vfio_iommu_type1 allow_unsafe_interrupts=1
```

в) обновить информацию в файле grub.cfg и перезагрузить хост для применения изменений:

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

3.5.3.6 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 применяться 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, следует нажать кнопку Привязано к хосту на вкладке "Виртуальные машины" в подробном просмотре хоста.

Для перевода хоста в режим обслуживания:

а) перейти в "Ресурсы → Хосты" и выбрать хост;

б) нажать "Управление → Обслуживание". В результате будет открыто окно "Хосты обслуживания" (рисунок 168);

в) опционально указать "Причину" перемещения хоста в режим обслуживания, которая будет указана в журнале и при повторной активации хоста из режима обслуживания;

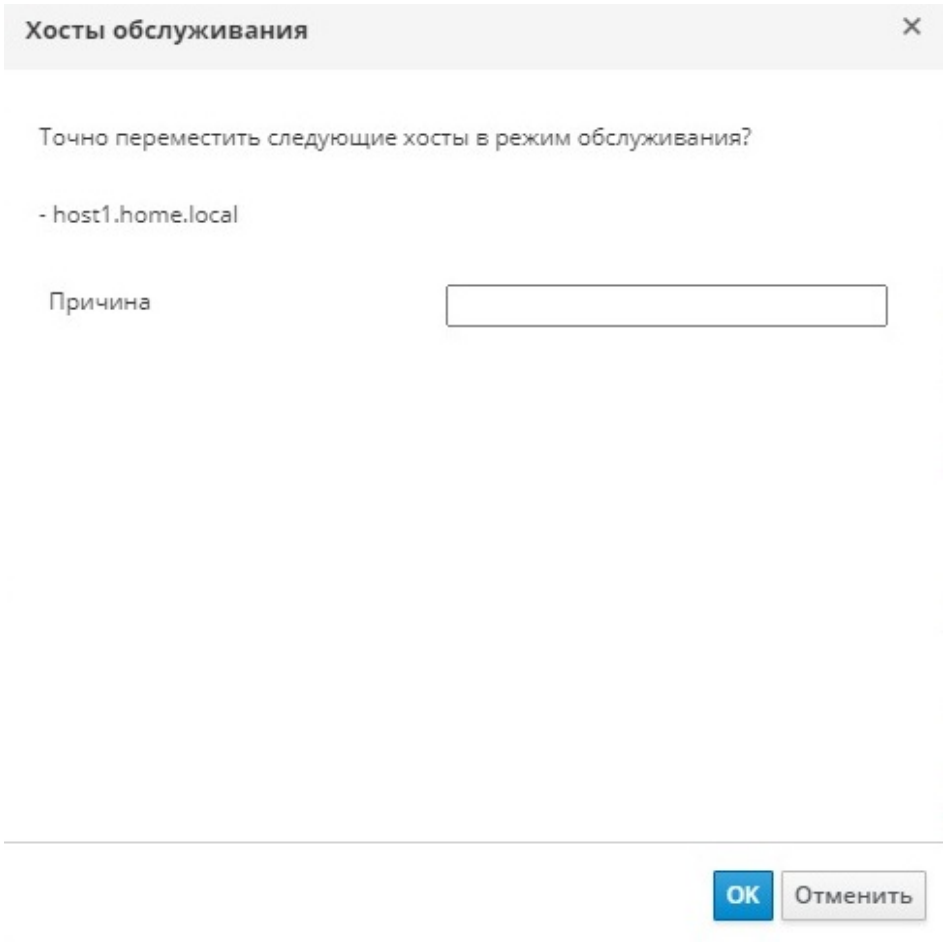


Рисунок 168 – Перемещение хоста в режим обслуживания

Примечание — Поле "Причина" для указания обстоятельств перевода хоста в режим обслуживания появится только в случае, если эта возможность была включена в параметрах кластера (см. п. 3.3.2.2).

г) опционально выбрать нужные параметры для хостов с поддержкой Gluster:

– выбрать 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. Этот параметр используется только в случае, если нет никаких других способов перевести хост в режим обслуживания;
– выбрать 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.

д) нажать кнопку 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 следует нажать на хосте "Управление → Активировать" для остановки действий по переводу этого хоста в режим обслуживания, а затем на виртуальной машине нажать кнопку Прервать миграцию для остановки миграции.

3.5.3.7 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, убедиться в том, что выполнение всех задач завершено.

Для активации хоста из режима обслуживания необходимо:

а) нажать "Ресурсы → Хосты" и выбрать хост;
б) нажать "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.

3.5.3.8 Настройка правил межсетевого экрана хоста

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

Важно — Кластер должен быть настроен на работу с firewalld, а не с устаревшим типом межсетевого экрана iptables.

Для настройки правил межсетевого экрана для хостов нужно выполнить следующие действия:

а) для добавления частного порта межсетевого экрана отредактировать 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
```

б) сохранить файл как /etc/ovirt-engine/ansible/ovirt-host-deploy-post-tasks.yml.

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

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

3.5.3.9 Удаление хоста

Для удаление хоста нужно:

а) нажать "Ресурсы → Хосты" и выбрать хост;

б) нажать "Управление → Обслуживание";

в) после перевода хоста в режим обслуживания нажать кнопку Удалить, чтобы открыть окно подтверждения "Удалить хост(ы)";

г) если хост является частью кластера хранилища Gluster и на хосте имеются кирпичи тома или если хост не отвечает, установить флажок "Принудительное удаление";

д) нажать кнопку OK.

3.5.3.10 Повторная установка хостов

Для повторной установки хостов виртуализации и стандартных хостов необходимо использовать Портал администрирования и учитывать 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 выключить некоторые из ВМ до начала перевода хостов в режим обслуживания.

– Перед началом повторной установки следует убедиться, что кластер содержит более одного хоста. Не рекомендуется обновлять ПО на всех хостах одновременно. Один из хостов должен быть доступен для выполнения задач роли SPM (диспетчер пула хранилища).

В следующую последовательность действий для повторной установки включаются остановка и перезапуск хостов:

а) нажать "Ресурсы → Хосты" и выбрать хост;

б) нажать "Управление → Обслуживание";

в) нажать "Установка → Повторная установка", чтобы открыть окно "Установка хоста";

г) нажать кнопку 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 следует нажать "Управление → Активировать" на Портале администрирования. В результате статус хоста сменится на "Запущен", и хост будет готов к работе.

3.5.3.11 Индивидуализация хостов с помощью меток

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

Для индивидуальной настройки хостов с помощью меток нужно:

а) нажать "Ресурсы → Хосты" и выбрать хост;

б) нажать пиктограмму ⋮ (Больше действий), затем нажать кнопку `Назначить теги`;

в) установить флажки для необходимых меток;

г) нажать кнопку `OK`.

3.5.3.12 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, следует нажать на имя хоста и перейти на вкладку "События".

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

3.5.3.13 Просмотр устройств хоста

Для просмотра устройств хоста требуется:

а) нажать "Ресурсы → Хосты";
б) нажать на имя хоста, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Устройства хоста".

Во вкладке "Устройства хоста" приводится подробный список устройств хоста, включая информацию о подключении устройства к ВМ и об использовании ВМ в данный момент. Если на хосте можно настроить прямое присвоение устройств, то эти устройства можно напрямую подключить к ВМ для улучшения производительности.

3.5.3.14 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 используется браузер, в котором нужно указать соответствующий URL в адресной строке, или Портал администрирования.

Для доступа к Cockpit с Портала администрирования нужно:

а) в Портале администрирования нажать "Ресурсы → Хосты" и выбрать хост;

б) нажать кнопку `Консоль хоста`.

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

3.5.4 Отказоустойчивость хостов

3.5.4.1 Высокая доступность хостов

В РОСА Виртуализация 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). Неотвечающие 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 неотвечающий хост

перезагружается, и если хост не вернется к активному состоянию в течение указанного времени, то останется неотвечающим в ожидании ручного вмешательства для решения проблемы.

Примечание — Для автоматической проверки параметров операции блокады рекомендуется настроить 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 неотвечающих 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 неотвечающие 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.

3.5.4.2 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.

3.5.4.3 Настройка параметров операции блокады на хосте

Параметры операции блокады настраиваются во вкладке "Управление питанием" окон "Новый хост" или "Параметры хоста". Управление питанием дает возможность Системе огородить проблемный хост, используя такие дополнительные интерфейсы, как карта удаленного 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.

Для настройки параметров операции блокады на хосте нужно выполнить следующие действия:

а) нажать "Ресурсы → Хосты" и выбрать хост;

б) нажать кнопку Изменить;

в) перейти на вкладку "Управление питанием" (рисунок 169);

г) установить флажок "Включить управление питанием", чтобы активировать поля ввода;

д) установить флажок "Интеграция Kdump", чтобы предотвратить огораживание хоста во время выполнения аварийного дампа ядра;

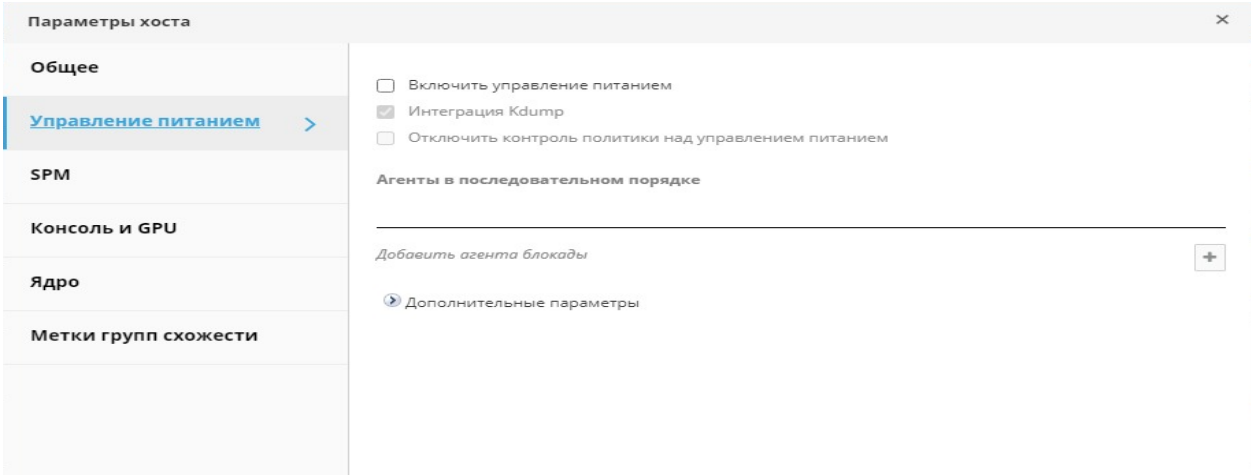


Рисунок 169 – "Управление питанием" хоста

Примечание — Хост необходимо переустанавливать каждый раз при изменении (активации или деактивации) параметра "Интеграция Kdump".

е) опционально установить флажок "Отключить контроль управления питанием со стороны политик", если управление питанием хоста не должно контролироваться политикой планирования кластера, в который входит хост;

ж) нажать на кнопку +, чтобы открыть окно "Параметры агента блокады" для добавления нового устройства управления питанием;

з) указать "Адрес", "Имя пользователя" и "Пароль" для устройства управления питанием;

и) из выпадающего списка выбрать "Тип" устройства управления питанием;

к) указать номер "Порта SSH", используемый устройством управления питанием для связи с хостом;

л) указать номер "Слота", используемого для идентификации платы устройства управления питанием;

м) настроить "Параметры" устройства управления питанием в форме списка записей "ключ-значение", разделенных запятыми;

н) установить флажок "Защищенное", чтобы включить защищенное соединение между устройством управления питанием и хостом;

о) чтобы убедиться в том, что все значения корректны, нажать кнопку 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.

п) нажать кнопку OK для закрытия окна "Параметры агента блокады";

р) опционально во вкладке "Управление питанием" развернуть "Дополнительные параметры" и с помощью кнопок со стрелками ↑ (вверх) и ↓ (вниз) указать порядок, в котором виртуализированный ЦУ будет вести поиск хоста-прокси для операции блокады в кластере или дата-центре;

с) нажать кнопку OK.

Следует обратить внимание, что "!" (восклицательный знак) рядом с именем хоста исчез, что означает успешную настройку управления питанием хоста.

3.5.4.4 Служба Kdump и параметры fence_kdump

Для просмотра статуса службы Kdump нужно нажать 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" создает 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.

При этом 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 настройки частного интервала 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 усложненных сетевых конфигурациях.

Для настройки слушателя fence_kdump необходимо:

а) создать новый файл (например, my-fence-kdump.conf) в каталоге /etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/;

б) указать частные параметры согласно синтаксису "ПАРАМЕТР=значение" и сохранить файл;

Примечание – Измененные значения параметров также должны быть согласованы с параметрами engine-config, приведенными в 3.5.4.4.1.

в) перезапустить слушатель fence_kdump:

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

В таблице 58 описываются параметры настройки слушателя fence_kdump.

Таблица 58 – 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.	При изменении значения этот параметр должен быть равен (или быть меньше) половинному значению параметра KdumpStartedTimeout в engine-config

Переменная	Описание	Примечание
	Значение по умолчанию — "5"	
REOPEN_DB_CONNECTION_INTERVAL	Указывает интервал (в секундах) для повторного открытия соединения к базе данных, 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

3.5.4.4.1 Настройка Kdump с помощью engine-config

Для просмотра текущих параметров Kdump необходимо выполнить следующую команду:

```
# engine-config -g ПАРАМЕТР
```

Для настройки Kdump с помощью engine-config нужно выполнить следующие действия:

а) отредактировать конфигурацию Kdump согласно синтаксису "ПАРАМЕТР=значение":

```
# engine-config -s ПАРАМЕТР=значение
```

Важно — Измененные значения параметров также должны быть согласованы с параметрами настройки слушателя fence_kdump, приведенными в таблица 58.

б) перезапустить службу ovirt-engine:

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

в) переустановить все хосты, а также при необходимости активировать параметр "Интеграция Kdump".

В таблице 59 описываются параметры конфигурации Kdump.

Таблица 59 – 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 включенной "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 включенной "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 включенной "Интеграцией Kdump" должны быть переустановлены
FenceKdumpListenerTi	Определяет	При изменении значения этот

Переменная	Описание	Примечание
meout	максимальный период ожидания (в секундах) после последнего периодического сигнала, в течение которого слушатель fence_kdump еще считается работающим. Значение по умолчанию — "90"	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

3.5.4.5 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, остается 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 неотвечающем 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). По истечении времени ожидания подключения между диспетчером виртуализации и хостом происходит следующее:

а) при первом сбое сети статус хоста меняется на "Идет подключение";

б) диспетчер виртуализации выполняет три попытки запросить у VDSM его статус или ждет в течение временно́го интервала, определенного 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);

в) если по истечении интервала хост по-прежнему не отвечает, выполняется команда `vdsm restart` с использованием протокола SSH;

г) 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 передается 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.

3.5.4.6 Использование возможностей хоста по управлению питанием

При настроенном на хосте управлении питанием можно получить доступ к некоторому числу параметров управления питанием через интерфейс Портала администрирования. Хотя каждое устройство управления питанием обладает своими настраиваемыми параметрами, все они поддерживают базовые возможности запуска, остановки и перезапуска хоста.

Для использования возможностей хоста по управлению питанием нужно выполнить следующие действия:

а) нажать "Ресурсы → Хосты" и выбрать хост.

б) Из выпадающего меню "Управление питанием" выбрать 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 дает ему присоединиться к кластеру. "Статус" готового к использованию хоста изменяется на "Запущен".

– Остановить – параметр выключает питание хоста. Перед тем как использовать этот параметр, убедиться в том, что ВМ, выполняющиеся на хосте, уже мигрировали на другие хосты в кластере. В противном случае произойдет аварийное прерывание работы этих ВМ, и на другом хосте будут перезапущены только высокодоступные ВМ. После остановки хоста статус изменяется на "В нерабочем состоянии".

в) нажать кнопку OK.

Примечание – Если "Управление питанием" не включено, для перезапуска или остановки работы хоста сначала выбрать необходимый хост, затем из выпадающего меню "Управление" выбрать 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 начнет работу. В случае последовательных агентов для остановки или запуска хоста сначала используется первичный агент, а в случае его сбоя используется вторичный агент.

3.5.4.7 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.

Важно — параметр "Подтвердить, что хост был перезагружен" следует использовать только в случае, если хост был перезагружен вручную. Использование этого параметра во время работы хоста может привести к повреждению образа ВМ.

Для ручного изолирования не отвечающего хоста необходимо:

а) нажать "Ресурсы → Хосты" и убедиться в том, что хост действительно имеет статус "Не отвечает";

б) перезагрузить хост вручную (например, осуществить физическое взаимодействие с оборудованием непосредственно в серверной);

в) выбрать хост, нажать пиктограмму ⋮ (Больше действий) и далее кнопку `Подтвердить`, что хост был перезагружен;

г) установить флажок "Одобрить действие" и нажать кнопку `OK`;

д) если перезагрузка хоста занимает много времени, настроить параметр ServerRebootTimeout и указать, сколько секунд должно длиться ожидание перед тем, как хост получит статус "Не отвечает":

```
# engine-config --set ServerRebootTimeout=целое_число
```

3.6 Хранилища

Система виртуализации РОСА Виртуализация использует централизованную систему хранилищ для виртуальных дисков, файлов ISO и снимков ВМ.

В обязанности администратора входят создание, настройка, присоединение и поддержка хранилищ. Дополнительно администратору необходимо иметь представление о типах хранилищ и сценариях их использования.

Сеть хранения в РОСА Виртуализация может быть реализована следующими средствами:

– Сетевая файловая система NFS.
– Экспорт GlusterFS.
– Любые POSIX-совместимые файловые системы.
– Интерфейс iSCSI.
– Локальные хранилища, присоединенные 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 необходимы рабочий доступ на Портал администрирования, а также как минимум один подключенный хост со статусом "Запущен".

В РОСА Виртуализация используются следующие типы доменов хранилищ:

– **Домен данных**.

В доменах данных хранятся виртуальные жесткие 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 присоединен 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 РОСА Виртуализация. 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 присоединен 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 этого виртуальные машины, "плавающие" виртуальные диски и шаблоны можно загрузить из домена хранения в прикрепленный дата-центр. Подробные сведения об импорте доменов хранилищ см. в п. 3.6.6.1.2.

Настройку и присоединение хранилищ к окружению виртуализации POCA Виртуализация следует начинать только после того, как были определены требования к хранилищам со стороны дата-центров.

3.6.1 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 файловых систем).

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 жестких 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.

3.6.2 Подготовка и добавление хранилища NFS

3.6.2.1 Подготовка хранилища NFS

Общие ресурсы NFS создаются в хранилище файлов или на удаленном сервере в качестве доменов хранилищ. После экспорта этих общих ресурсов в удаленное 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 учетные 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 РОСА Виртуализация.

Последовательность действий по подготовке хранилища NFS:

а) создать группу kvm:

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

б) создать пользователя vdsm в группе kvm:

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

в) указать значение "36:36" для изменения владельцев каталога /exports/data на vdsm:kvm:

```
# chown -R 36:36 /exports/data
```

г) изменить 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
```

3.6.2.2 Добавление хранилища NFS

В следующей последовательности действий описывается как присоединить существующее хранилище NFS к окружению виртуализации РОСА Виртуализация в качестве домена данных.

Последовательность действий по добавлению хранилища NFS:

а) на Портале администрирования выбрать "Хранилище → Домены";

б) нажать кнопку Добавить домен;

в) в окне "Новый домен" указать "Имя" домена хранилища (рисунок 170);

г) принять значения по умолчанию для списков "Дата-центр", "Функции домена", "Тип хранилища", "Формат" и "Хост";

д) ввести "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";

е) при необходимости нажать кнопку Дополнительные параметры для настройки следующих значений:

– в поле "Индикатор предупреждения о недостатке места (%)" указать значение в процентах. Если объем свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупреждающее сообщение, а событие будет занесено в журнал;

– в поле "Блокатор при отсутствии места (ГБ)" ввести значение в ГБ. Если объем 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;

– установить флажок "Забить нулями после удаления". Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя;

ж) нажать кнопку OK.

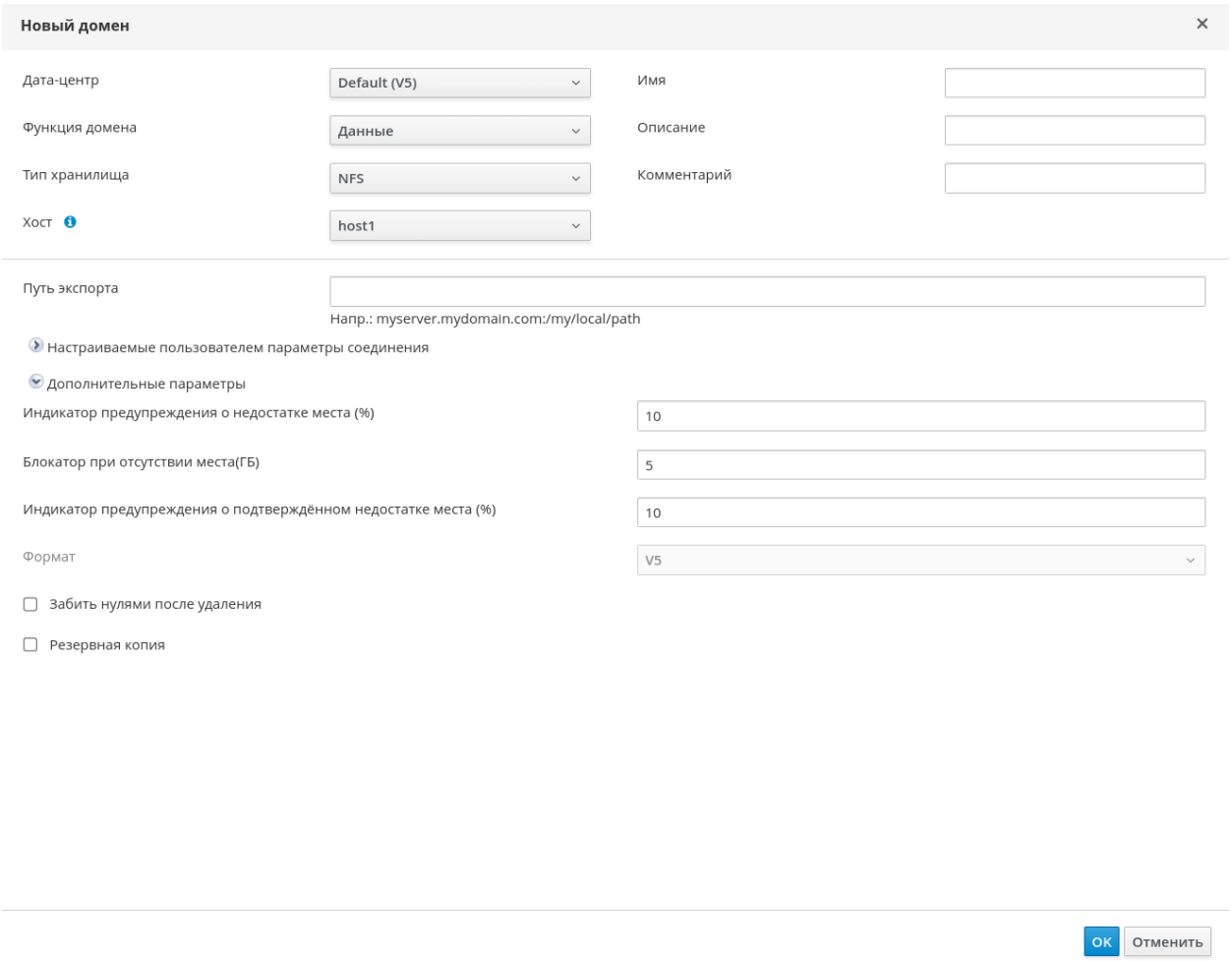


Рисунок 170 – Добавление хранилища NFS

Примечание – "Новый домен" данных NFS будет иметь статус "Заблокировано" до тех пор, пока не будет подготовлен диск, после чего домен будет автоматически подключен к дата-центру.

Для добавления хранилища NFS при необходимости использования домена экспорта или домен ISO можно выполнить вышеперечисленные действия, но в списке "Функция домена" выбрать значение "Экспорт" или "ISO".

3.6.2.3 Увеличение объема хранилища NFS

Для увеличения объема хранилища NFS можно либо создать новый домен хранилища и добавить его в существующий дата-центр, либо увеличить доступный объем на сервере NFS.

Для увеличения существующего домена хранилища NFS нужно выполнить следующие действия:

а) нажать "Хранилище → Домены";

б) нажать на название существующего домена NFS, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Дата-центр" и нажать кнопку Обслуживание, чтобы перевести домен хранилища в режим обслуживания. Это действие размонтирует существующий общий ресурс и даст возможность изменить размер домена хранилища;

г) изменить размер хранилища на сервере NFS до необходимого объема;

д) в подробном просмотре перейти на вкладку "Дата-центр" и нажать кнопку Активировать, чтобы смонтировать домен хранилища.

3.6.3 Подготовка и добавление локального хранилища

3.6.3.1 Подготовка локального хранилища

Локальный домен хранилища можно настроить на хосте. При настройке локального хранилища хост автоматически добавляется в новый дата-центр и кластер, состоящий из одного хоста. Для кластеров, состоящих из множества хостов, требуется, чтобы у каждого хоста имелся доступ ко всем доменам хранилищ, что невозможно в случае локального хранилища.

Примечания:

– Виртуальные машины, созданные в кластере с единственным хостом, не могут мигрировать, их нельзя изолировать (огородить) или добавить в планирование.

– На хостах виртуализации локальные хранилища всегда должны настраиваться на файловой системе, отделенной от корневого каталога "/". Для предотвращения потенциальных потерь данных во время обновления версий ПО рекомендуется использовать отдельный логический том.

Для подготовки локального хранилища на стандартных хостах нужно выполнить следующие действия:

а) создать каталог (например, /data/images), который будет использоваться как локальное хранилище:

```
# mkdir -p /data/images
```

б) изменить владельцев каталога /data/images на пользователя vdsm и группу kvm и установить права на чтение и запись в каталоге /data/images для владельца:

```
# chown 36:36 /data /data/images
# chmod 0755 /data /data/images
```

На хосте виртуализации рекомендуется создать локальное хранилище на логическом томе следующим образом:

а) создать 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
```

б) смонтировать новое локальное хранилище и затем изменить владельца и права доступа:

```
# mount -a
# chown 36:36 /data /rhvh-data
# chmod 0755 /data /rhvh-data
```

3.6.3.2 Добавление локального хранилища

Добавление локального хранилища помещает хост в новый дата-центр и кластер.

В следующей последовательности действий в окне параметров локального хранилища соединено создание дата-центра, кластера и хранилища.

Последовательность действий по добавлению локального хранилища:

а) нажать "Ресурсы → Хосты" и выбрать хост;
б) нажать "Управление → Обслуживание" и далее нажать OK;

в) нажать "Управление → Настроить";

г) нажать на кнопки кнопку Изменить рядом с полями "Дата-центр", "Кластер" и "Хранилище", чтобы настроить домен локального хранилища;

д) в текстовом поле указать путь до локального хранилища;

е) при необходимости перейти на вкладку "Оптимизация", чтобы настроить политику оптимизации памяти для нового кластера локального хранилища;

ж) нажать кнопку OK.

В результате хост присоединится к сети в собственном дата-центре.

3.6.4 Управление хранилищами на базе файловой системы, совместимой с POSIX

3.6.4.1 Подготовка хранилища на базе файловой системы, совместимой с POSIX

Поддержка файловой системы стандарта POSIX дает 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 РОСА Виртуализация, 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.

Примечание — Не следует монтировать хранилище NFS, создавая домен хранилища на базе ФС, совместимой с POSIX. Всегда рекомендуется создавать для этого домен хранилища NFS.

3.6.4.2 Добавление хранилища на базе файловой системы, совместимой с POSIX

В следующей последовательности действий описывается, как присоединить к РОСА Виртуализация в качестве домена данных существующее хранилище на базе файловой системы, совместимой с POSIX.

Последовательность действий по добавлению хранилища на базе файловой системы, совместимой с POSIX:

а) нажать "Хранилище → Домены";

б) нажать кнопку Добавить домен;

в) в окне "Новый домен" указать "Имя" для домена хранилища (рисунок 171);

г) выбрать "Дата-центр", связанный с доменом хранилища (выбранный дата-центр должен иметь тип POSIX), или при отсутствии такого дата-центра выбрать "Нет";

д) из выпадающего списка "Функция домена" выбрать "Данные", а из списка "Тип хранилища" выбрать "POSIX-совместимая ФС";

е) из выпадающего списка выбрать "Хост";

ж) указать "Путь" до POSIX-совместимой ФС в формате команды mount;

з) указать "Тип VFS" в формате команды mount с аргументом "-t";

и) указать дополнительные "Параметры монтирования" в формате команды mount с аргументом "-o". Параметры монтирования должны указываться в виде списка, разделенного запятыми;

к) при необходимости нажать кнопку Дополнительные параметры для настройки следующих значений:

– в поле "Индикатор предупреждения о недостатке места (%)" указать значение в процентах. Если объем свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупреждающее сообщение, а событие будет занесено в журнал;

– в поле "Блокатор при отсутствии места (ГБ)" ввести значение в ГБ. Если объем 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;

– установить флажок "Забить нулями после удаления". Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя;

л) нажать кнопку OK.

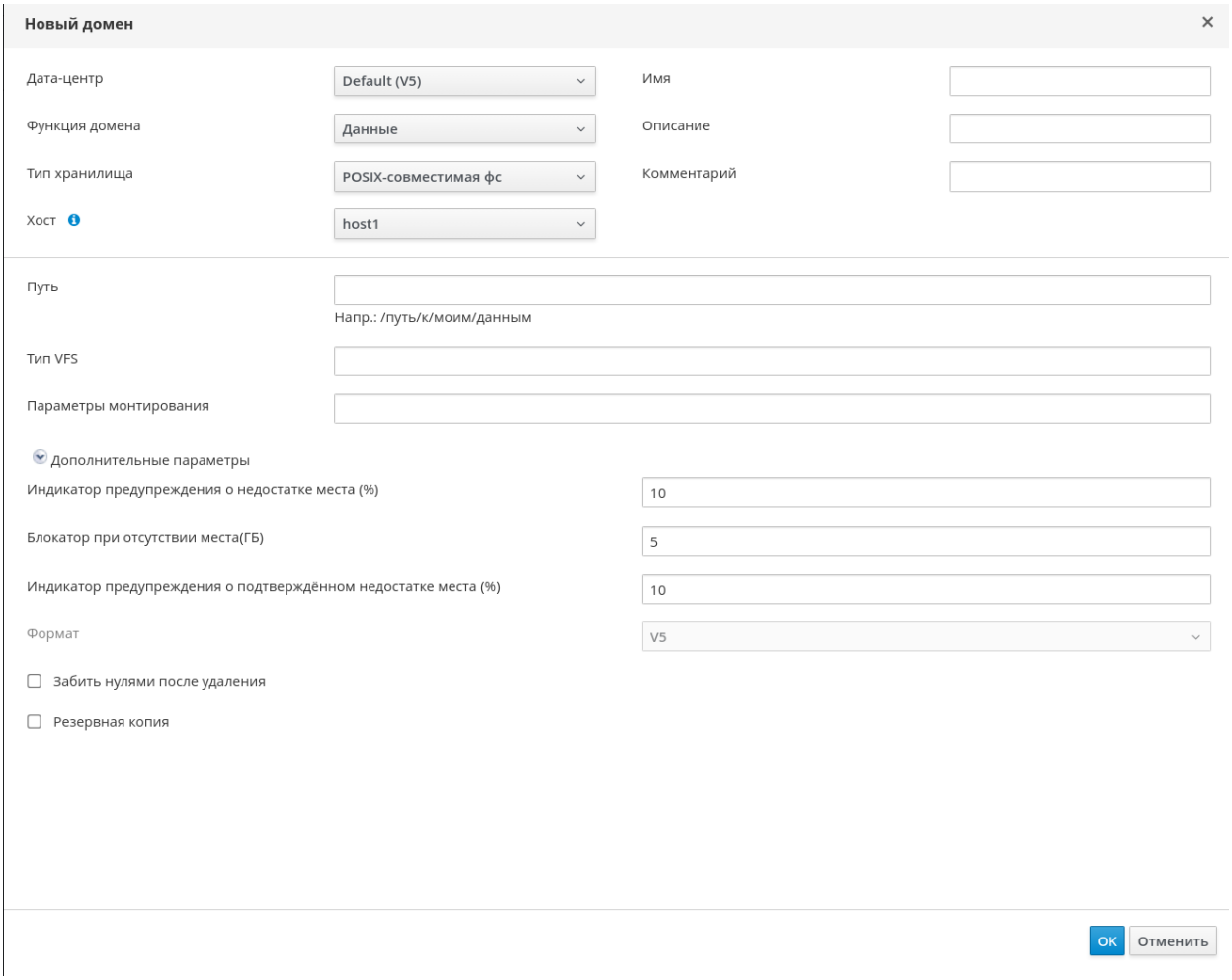


Рисунок 171 – Добавление хранилища с POSIX-совместимой файловой системой

3.6.5 Подготовка и добавление блочного хранилища

3.6.5.1 Подготовка хранилища iSCSI

Система виртуализации POCA Виртуализация 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.

Важно:

– При использовании блочного хранилища и планировании размещения ВМ на устройствах raw или прямых LUN под управлением диспетчера логических томов необходимо создать фильтр для скрытия гостевых логических томов. Это предотвратит активацию гостевых томов при загрузке хоста, что потенциально может привести к повреждению данных.

– Система виртуализации РОСА Виртуализация на данный момент не поддерживает хранилища с размером блоков в 4КБ. 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 файловую систему 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
  }
```

3.6.5.2 Добавление хранилища iSCSI

В следующей последовательности действий описывается, как присоединить к РОСА Виртуализация в качестве домена данных существующее хранилище iSCSI.

Последовательность действий по добавлению хранилища iSCSI:

а) нажать "Хранилище → Домены";

б) нажать кнопку Добавить домен;

в) В окне "Новый домен" указать "Имя домена хранилища" (рисунок 172);

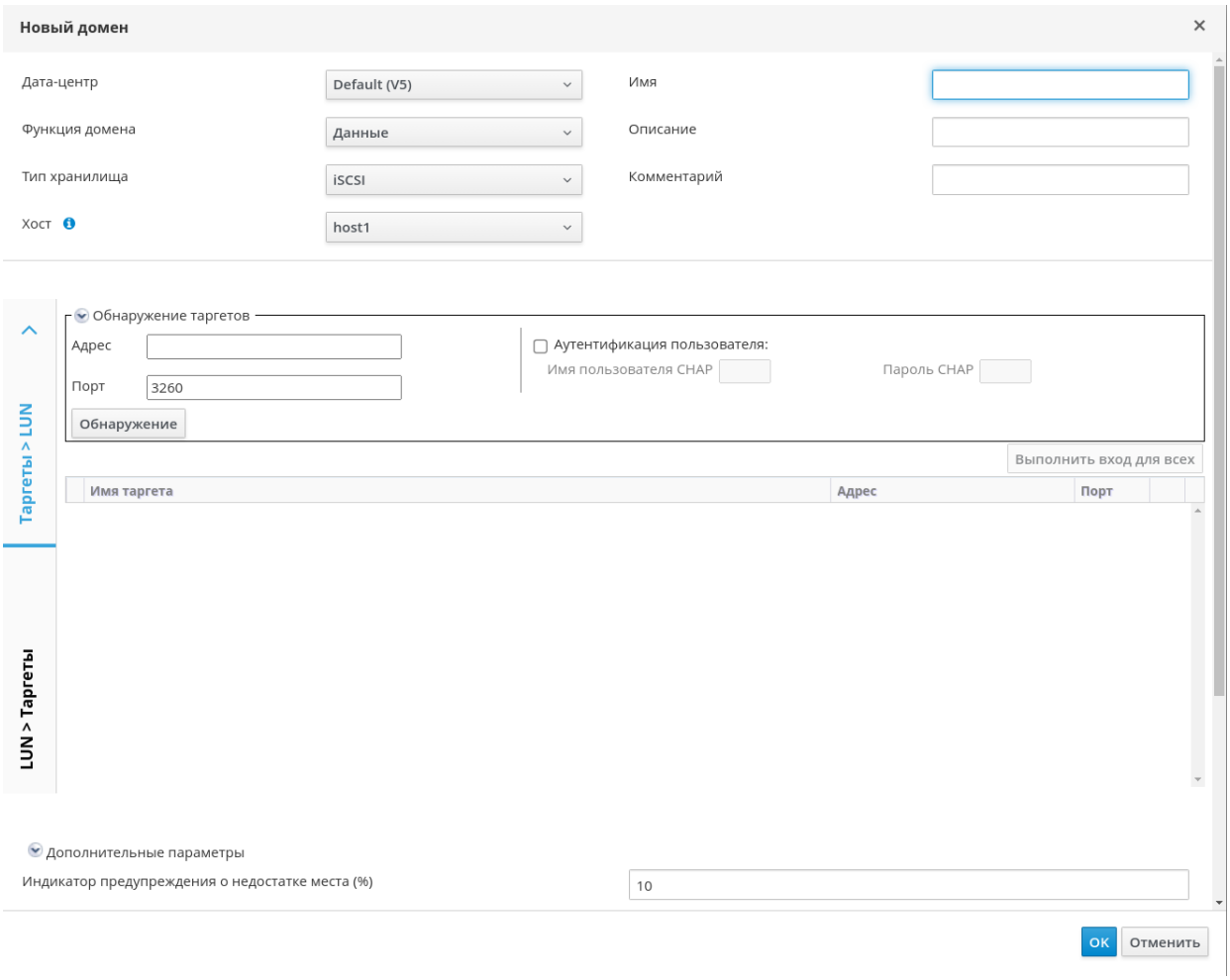


Рисунок 172 – Добавление хранилища iSCSI

г) выбрать "Дата-центр";

д) в качестве "Функции" домена выбрать "Данные", а в качестве "Типа хранилища" выбрать "iSCSI";

е) из выпадающего списка "Хост" выбрать активный хост;

Примечание — Подключение к домену хранилища идет 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.

ж) 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, выполнить следующие действия по обнаружению целей:

– для активации возможности обнаружения целей нажать "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;

– в поле "Адрес" ввести полное доменное имя или IP-адрес хоста iSCSI (рисунок 173);

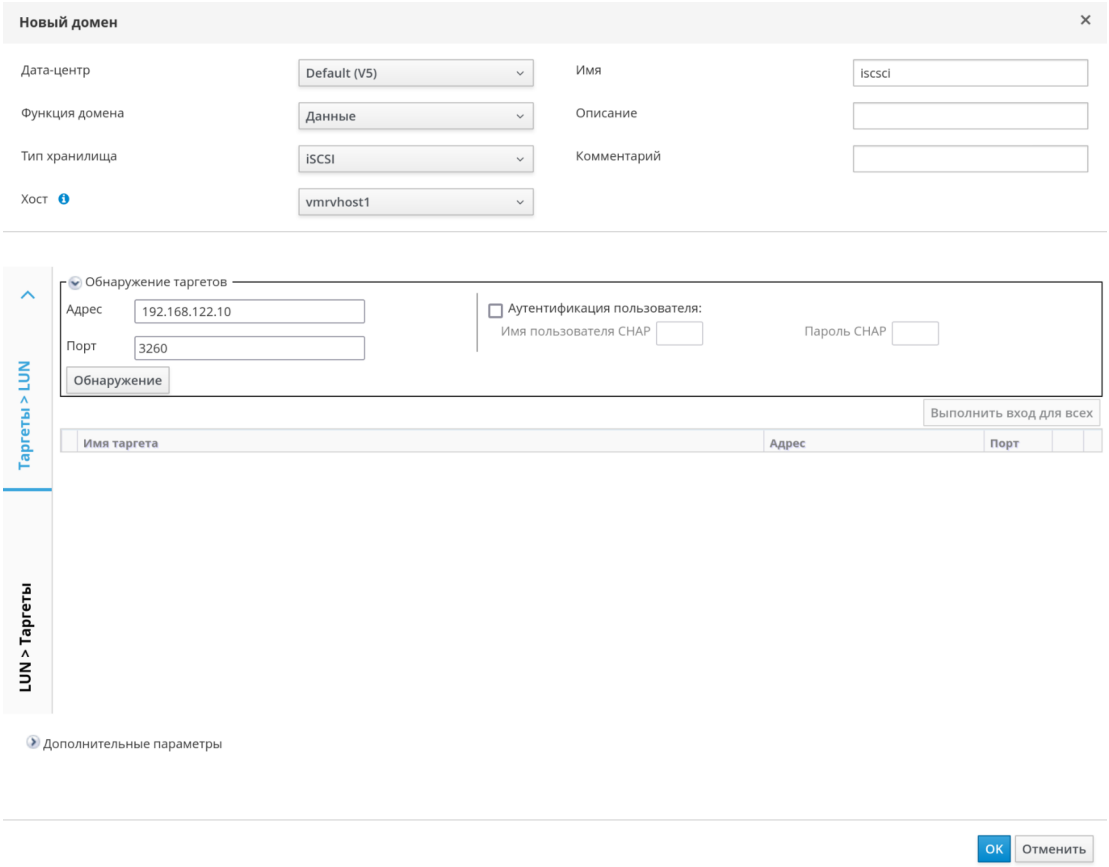


Рисунок 173 – Секция "Обнаружение таргетов" для хранилища типа iSCSI

– в поле "Порт" указать номер порта, к которому будет подключаться хост при просмотре целей (рисунок 173). Значение по умолчанию — "3260";

– если для защиты хранилища используется CHAP, установить флажок "Аутентификация пользователей" и далее ввести "Имя пользователя CHAP" и "Пароль CHAP" (рисунок 173);

Примечание — Учетные записи цели iSCSI для конкретного хоста можно настроить с помощью REST API.

– нажать "Обнаружение";

– выбрать одну или несколько целей из списка с результатами обнаружения (рисунок 174);

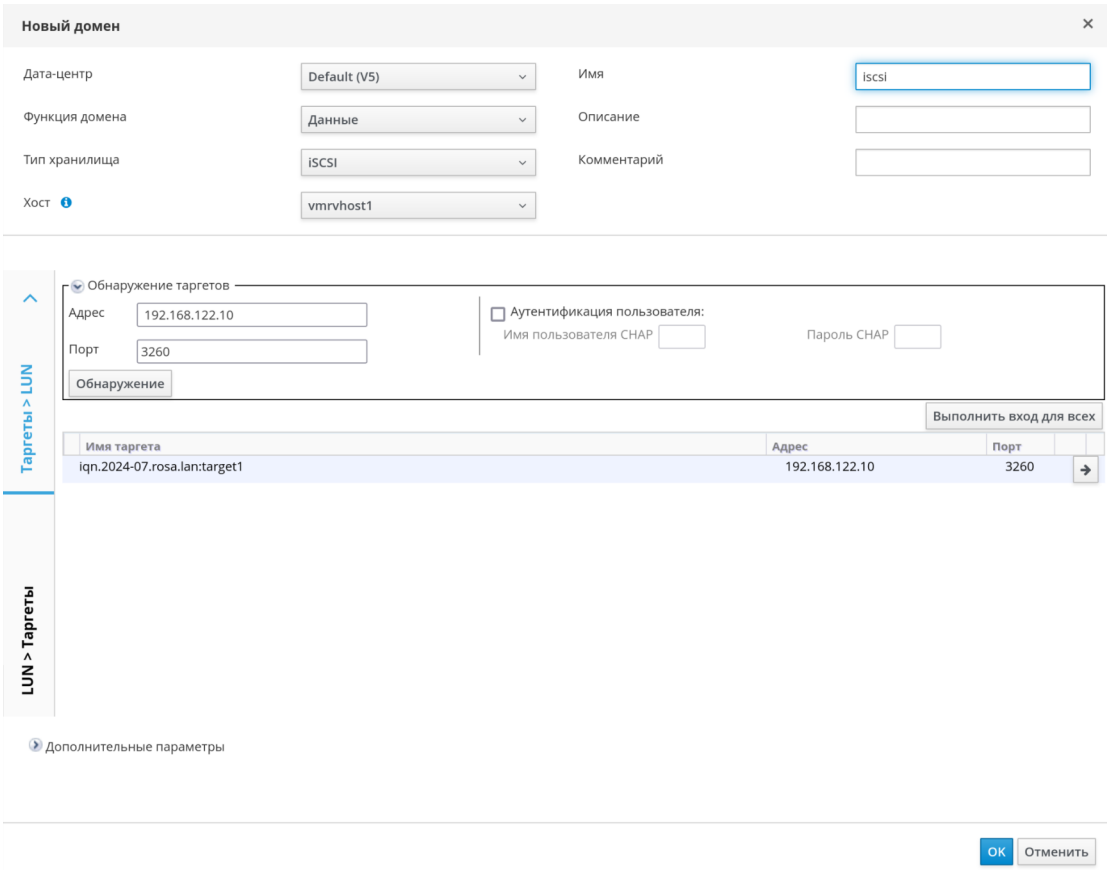


Рисунок 174 – Список целей iSCSI – результаты обнаружения целей

– нажать кнопку Вход в систему при выборе одной цели или нажать кнопку Выполнить вход для всех при выборе нескольких целей (стрелка → (вправо) в правой части формы на рисунке 174);

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.

з) нажать на кнопку + рядом с необходимой целью (рисунок 175). Элемент раскроется и будут показаны все неиспользуемые LUN, присоединенные к цели. Для добавления цели нажать кнопку Добавить;

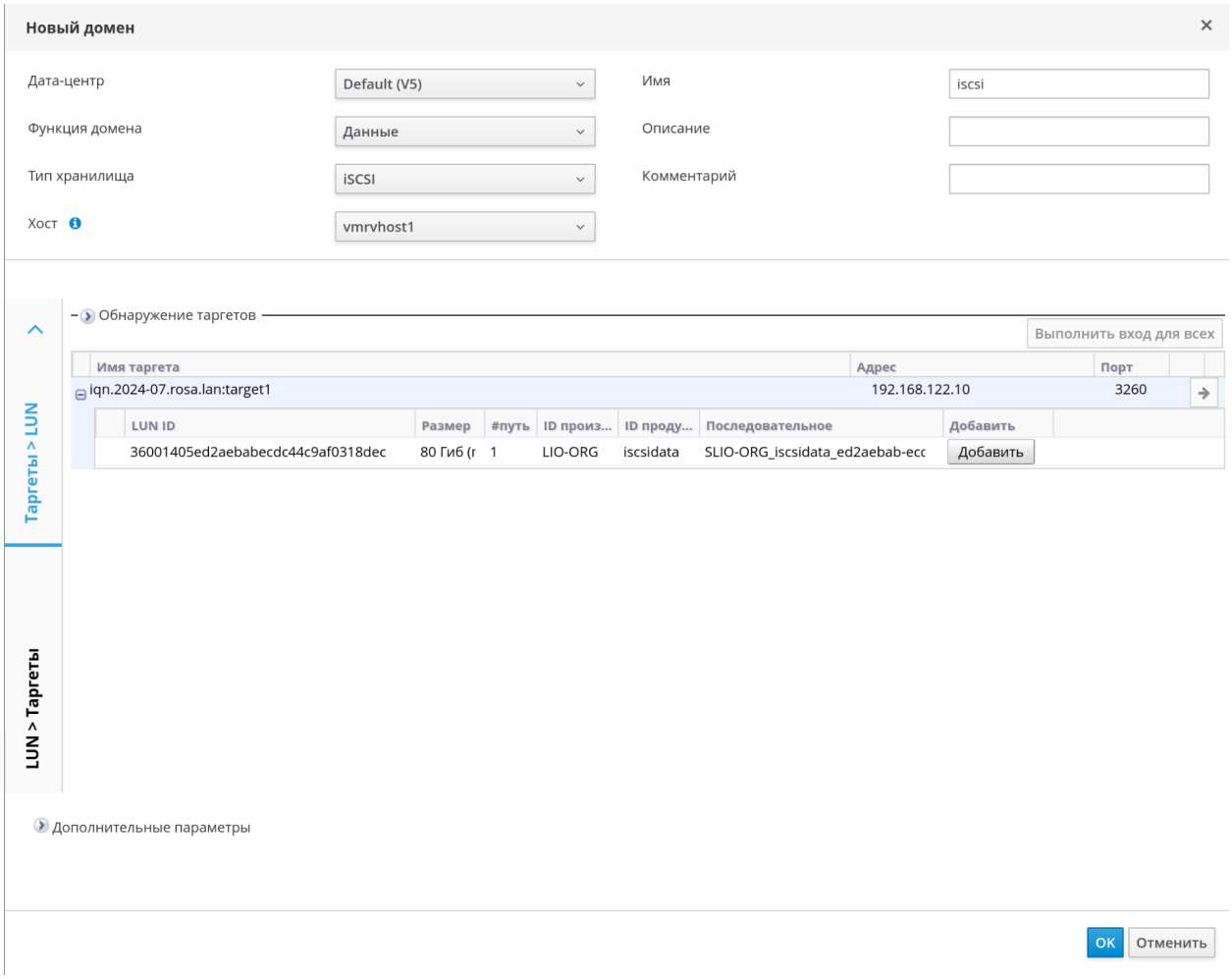


Рисунок 175 – Добавление цели iSCSI

и) установить флажок для каждого LUN, используемого для создания домена хранилища;

к) при необходимости нажать кнопку Дополнительные параметры для настройки следующих значений:

– в поле "Индикатор предупреждения о недостатке места (%)" указать значение в процентах. Если объем свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупреждающее сообщение, а событие будет занесено в журнал;

– в поле "Блокатор при отсутствии места (ГБ)" ввести значение в ГБ. Если объем 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;

– установить флажок "Забить нулями после удаления". Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя;

л) нажать кнопку OK.

После проведения инициализации хранилище iSCSI будет добавлено в список доступных хранилищ (рисунок 176).

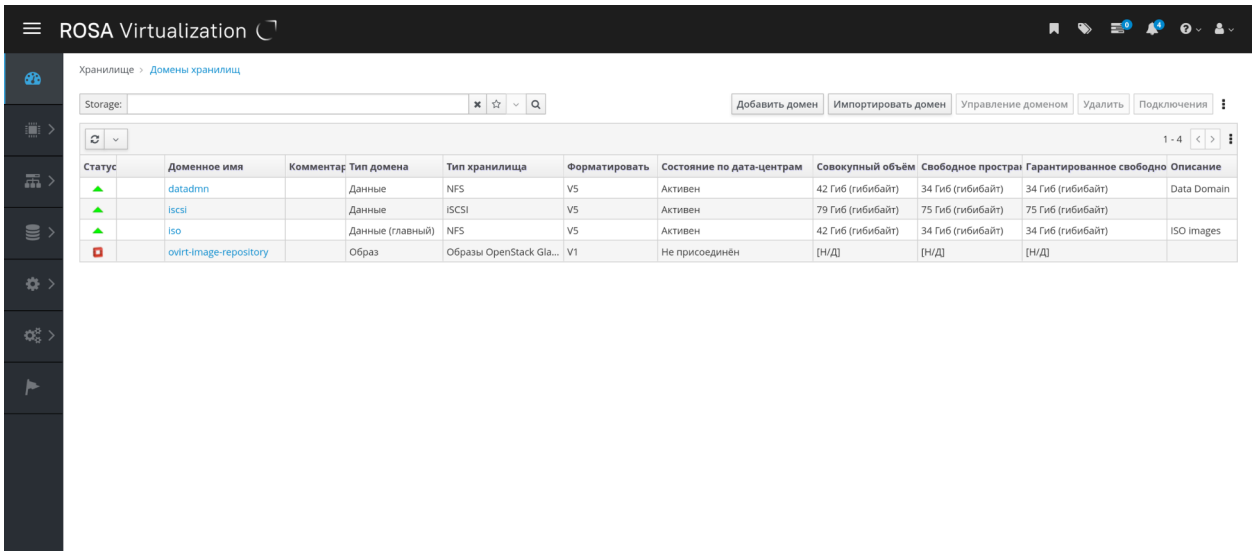


Рисунок 176 – Домен хранилища с типом хранилища iSCSI добавлен и активен

Если к одной цели было настроено несколько соединений из хранилищ, то для завершения создания связки iSCSI см. инструкцию, приведенную в п. 3.6.5.3.

В случае если текущая сеть хранилища должна мигрировать в связку iSCSI, см. п. 3.6.6.1.4.

3.6.5.3 Настройка доступа к iSCSI по нескольким путям

Доступ к iSCSI по нескольким путям дает 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. 3.6.5.2), а также одной или нескольких логических сетей (см. п. 3.4.1.2), отвечающих следующим требованиям:

– Логическая сеть не является требуемой сетью или сетью виртуальной машины.

– Логическая сеть присвоена интерфейсу хоста (см. п. 3.4.4.3).

– Логической сети присвоен статический IP-адрес в той же VLAN и подсети, в которой размещаются другие логические сети в связке iSCSI (см. п. 3.4.4.3).

Для настройки доступа к iSCSI по нескольким путям требуется :

а) нажать "Ресурсы → Дата-центры";

б) нажать на имя дата-центра, чтобы перейти к подробному просмотру;

в) на вкладке "Доступ к iSCSI по нескольким путям" нажать кнопку Добавить;

г) в окне "Добавить связку iSCSI" указать "Имя" и "Описание";

д) выбрать 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;

е) нажать кнопку OK.

В результате хосты в дата-центре будут подключены к целям iSCSI с помощью логических сетей в связке iSCSI.

3.6.5.4 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.

Для миграции логической сети в связку iSCSI нужно:

а) изменить текущую логическую сеть так, чтобы она не была "Требуемой":

1) нажать "Ресурсы → Кластеры";
2) нажать на название кластера, чтобы перейти к подробному просмотру;
3) во вкладке "Логические сети" выбрать текущую логическую сеть (например, "net-1") и нажать "Управление сетями";
4) снять флажок "Требуется" и нажать кнопку OK;

б) создать новую логическую сеть, не являющуюся "Требуемой" и не являющуюся "Сетью ВМ":

1) нажать кнопку Добавить сеть, чтобы открыть окно "Новая логическая сеть";
2) во вкладке "Общие" ввести "Имя" (например, "net-2") и снять флажок "Сеть ВМ";
3) во вкладке "Кластер" снять флажок "Требовать" и нажать кнопку OK;

в) удалить текущую сетевую связку и заново присвоить логические сети:

1) нажать "Ресурсы → Хосты";
2) нажать на имя хоста, чтобы перейти к подробному просмотру;
3) во вкладке "Сетевые интерфейсы" нажать "Настроить сети хоста";
4) переместить сеть "net-1" вправо, чтобы заново присвоить эту сеть;
5) переместить текущую связку вправо для удаления;
6) переместить сети "net-1" и "net-2" влево, чтобы присвоить эти сети физическим интерфейсам;
7) нажать на значок карандаша рядом с сетью "net-2", чтобы открыть окно "Свойства сети";
8) во вкладке "IPV4" выбрать "Статический";
9) указать "IP" и "Сетевую маску/префикс маршрутизации подсети" и нажать кнопку OK;

г) создать связку iSCSI:

1) нажать "Ресурсы → Дата-центры";
2) нажать на имя дата-центра, чтобы перейти к подробному просмотру;

3) во вкладке "Доступ к iSCSI по нескольким путям" нажать кнопку Добавить;
4) в окне "Добавить связку iSCSI" указать "Имя", выбрать сети "net-1" и "net-2" и нажать кнопку OK.

В результате в дата-центре теперь будет связка iSCSI, включающая в себя и старую (net-1), и новую (net-2) логические сети.

3.6.5.5 Подготовка хранилища FCP

Система виртуализации РОСА Виртуализация поддерживает хранилище SAN путем 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.

Важно — Администраторы РОСА Виртуализация 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 РОСА Виртуализация на данный момент не поддерживает хранилища с размером блоков в 4КБ. 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
```

```
}
```

3.6.5.6 Добавление хранилища FCP

В следующей последовательности действий описывается как присоединить к РОСА Виртуализация в качестве домена данных существующее хранилище FCP.

Последовательность действий по добавлению хранилища FCP:

а) нажать "Хранилище → Домены";
б) нажать "Добавить домен";
в) указать "Имя" домена хранилища;
г) из выпадающего списка выбрать "Дата-центр FCP" или при отсутствии такого дата-центра выбрать "Нет";
д) из выпадающих списков выбрать "Функцию домена" и "Тип хранилища". Типы доменов хранилища, несовместимые с выбранным дата-центром, не будут доступны;
е) в поле "Хост" выбрать активный хост. Если этот домен данных не первый в этом дата-центре, необходимо выбрать SPM-хост дата-центра;

Важно — Подключение к домену хранилища идет через выбранный хост, а не напрямую из виртуализированного ЦУ. В Системе должен существовать как минимум один активный хост, присоединенный к выбранному дата-центру. До начала настройки домена хранилища у всех хостов должен быть доступ к устройству хранения.

ж) при выборе типа хранилища "Оптоволокно" в окне "Новый домен" автоматически показываются известные цели с неиспользуемыми LUN. Установить флажок "LUN ID", чтобы выбрать все доступные LUN;
з) опционально нажать кнопку `Дополнительные параметры` для настройки следующих значений:

– в поле "Индикатор предупреждения о недостатке места" ввести процентное значение. Если объем свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупреждающее сообщение, а событие будет занесено в журнал;
– в поле "Блокатор при отсутствии места (ГБ)" ввести значение в ГБ. Если объем 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;

– установить флажок "Забить нулями после удаления". Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя;

и) нажать кнопку OK.

Примечание — Во время подготовки к использованию домен данных FCP будет иметь статус "Заблокировано". Домен автоматически присоединится к дата-центру, когда будет готов к использованию.

3.6.5.7 Увеличение размера хранилища iSCSI или FCP

Для увеличения объема 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. 3.6.6.1.2).

– Расширение домена хранения за счет 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".

Для увеличения размера существующего хранилища iSCSI или FCP нужно:

а) нажать "Хранилище → Домены" и выбрать домен iSCSI или FCP;

б) нажать "Управление доменом";

в) нажать "Таргеты > LUN" и далее нажать кнопку Обнаружить таргеты;

г) указать сведения о подключении для сервера хранилища и далее нажать кнопку Обнаружить для инициации подключения;

д) нажать "Таргеты > LUN" и установить флажок для нового доступного LUN;

е) нажать кнопку `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.

Для обновления информации о размере LUN на Портале администрирования требуется :

а) нажать "Хранилище → Домены" и выбрать домен iSCSI или FCP;
б) нажать "Управление доменом";
в) нажать "LUN > Таргеты";
г) в столбце "Дополнительный размер" нажать на кнопку `Добавить дополнительный размер хранилища` для обновления информации о LUN;
д) нажать кнопку `OK`, чтобы LUN отображал новый размер хранилища.

3.6.5.8 Повторное использование LUN

Следует обратить 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 следует выполнить 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
```

Важно — Это действие необходимо выполнить для корректного LUN во избежание непреднамеренного повреждения данных.

3.6.6 Подготовка и добавление хранилища Gluster

Процесс развертывания хранилища Gluster приведен в документе "РОСА Виртуализация 4. Руководство администратора. Часть 1. Установка" РСЮК.10103-01 32 01.

3.6.6.1 Импорт существующих доменов хранилищ

3.6.6.1.1 Обзор процесса импорта существующих доменов хранилищ

Кроме добавления новых доменов хранилищ, не содержащих данные, можно импортировать уже существующие и получить 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 дает 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, присоединенных к дата-центрам, возможен при корректном поддерживаемом уровне совместимости.

– Домен ISO.

Импорт существующего домена хранения ISO дает 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 дает 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 этого виртуальные машины, "плавающие" виртуальные диски и шаблоны можно загрузить из домена хранения в прикрепленный дата-центр. Подробные сведения об импорте доменов хранилищ см. п. 3.6.6.1.2.

Следует обратить внимание, что после прикрепления домена хранения к целевому дата-центру домен может быть обновлен 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.

3.6.6.1.2 Импорт доменов хранилищ

Для предотвращения возможного повреждения данных при импорте домена хранения, ранее прикрепленного к дата-центру в том же или в другом окружении, подразумевается, что домен хранения уже не прикреплен ни к одному из дата-центров в любом окружении.

Следует обратить внимание, что целевой дата-центр должен быть инициализирован для импорта и прикрепления существующего домена хранения к этому дата-центру.

Для импорта домена хранения нужно выполнить следующие действия:

а) нажать "Хранилище → Домены";

б) нажать кнопку Импортировать домен;

в) выбрать "Дата-центр", в который нужно импортировать домен хранения;

г) указать "Имя" домена хранения (рисунок 177);

д) из выпадающих списков выбрать "Функцию домена" и "Тип хранилища";

е) выбрать "Хост".

Важно — Подключение к домену осуществляется через выбранный хост, а не напрямую из виртуализированного ЦУ. Таким образом, должен существовать как минимум один активный хост, присоединенный к выбранному дата-центру. До начала настройки домена у всех хостов должен быть доступ к устройству хранения.

ж) указать 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.

з) установить флажок "Активировать домен в дата-центре", чтобы активировать домен хранения после присоединения его к выбранному дата-центру;

и) нажать кнопку ОК.

В результате из домена хранения теперь можно импортировать ВМ и шаблоны в выбранный дата-центр.

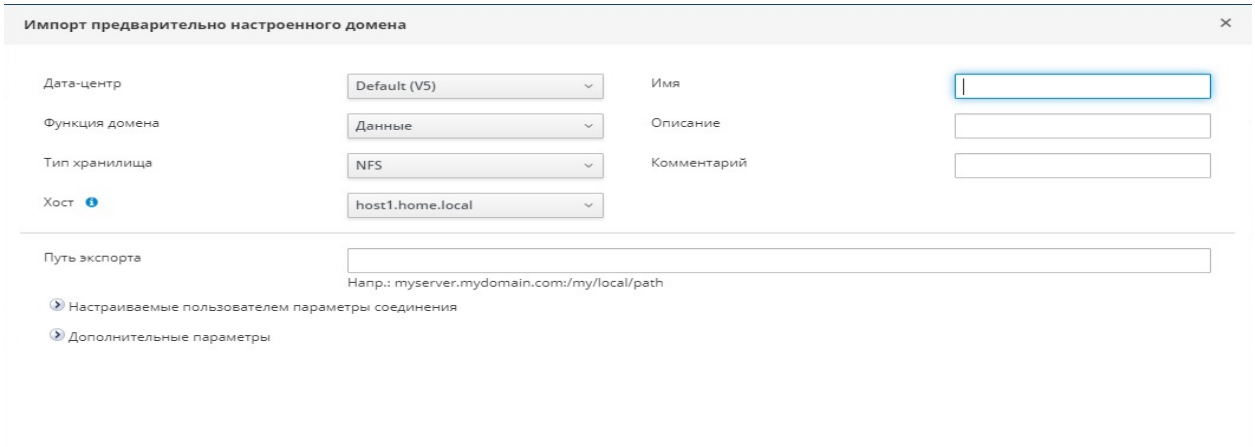


Рисунок 177 – Импорт домена хранения

3.6.6.1.3 Миграция доменов хранилищ между дата-центрами в одном окружении

При миграции домена хранения между дата-центрами в границах окружения РОСА Виртуализация осуществляется откребление домена от одного дата-центра и прикребление к другому дата-центру, чтобы целевой дата-центр получил доступ к данным, хранящимся в домене.

Для миграции домена хранения между дата-центрами в одном окружении нужно:

а) выключить все ВМ, выполняющиеся в домене хранения;

б) нажать "Хранилище → Домены";

в) нажать на название домена хранения, чтобы перейти к подробному просмотру;

г) перейти на вкладку "Дата-центр";

д) нажать "Обслуживание" и нажать кнопку OK;

е) нажать "Отсоединить" и нажать кнопку OK;

ж) нажать кнопку Присоединить;

з) выбрать целевой дата-центр и нажать кнопку OK.

В результате домен хранения прикреплен к целевому дата-центру и автоматически активируется, что позволяет импортировать ВМ и шаблоны из домена хранения в целевой дата-центр.

3.6.6.1.4 Миграция доменов хранилищ между дата-центрами в разных окружениях

При миграции домена хранения между дата-центрами в разных окружениях РОСА Виртуализация 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.

Для миграции домена хранения между дата-центрами в разных окружениях нужно выполнить следующие действия:

а) войти на Портал администрирования в исходном окружении;

б) выключить все ВМ, выполняющиеся в домене хранения;

в) нажать "Хранилище → Домены";

г) нажать на название домена хранения, чтобы перейти к подробному просмотру;

д) перейти на вкладку "Дата-центр";

е) нажать "Обслуживание" и нажать кнопку OK;

ж) нажать "Открепить" и нажать кнопку OK;

з) нажать кнопку Удалить;

и) в окне "Удалить хранилище" убедиться в том, что флажок "Форматировать домен" не установлен, т. е. содержимое хранилища не будет потеряно, и данные в домене сохранятся для последующего использования;

к) нажать кнопку OK для удаления домена хранения из исходного окружения;

л) войти на Портал администрирования в целевом окружении;

м) нажать "Хранилище → Домены";

н) нажать кнопку Импортировать домен;

о) из выпадающего списка "Дата-центр" выбрать целевой дата-центр;

п) ввести "Имя" домена хранения;

р) из соответствующих выпадающих списков выбрать "Функцию домена" и "Тип хранилища";

с) выбрать "Хост";

т) указать 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.

у) установить флажок "Активировать домен дата-центра", чтобы домен хранения был активирован автоматически при присоединении;

ф) нажать кнопку OK.

В результате домен хранения будет присоединен к целевому дата-центру в новом окружении РОСА Виртуализация и автоматически активирован, что позволяет импортировать ВМ и шаблоны из домена хранения в целевой дата-центр.

3.6.6.1.5 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 присоединен к дата-центру и активирован.

Для импорта ВМ из импортированного домена данных нужно выполнить следующие действия:

а) нажать "Хранилище → Домены";

б) нажать на имя импортированного домена данных, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Импорт ВМ";

г) выбрать одну или несколько ВМ для импорта;

д) нажать кнопку Импортировать;

е) убедиться, что для каждой ВМ в окне "Импорт ВМ" выбран корректный целевой кластер из списка "Кластер";

ж) отобразить внешние профили vNIC ВМ на профили, присутствующие в целевом кластере:

1) нажать "Отображение профилей vNIC";

2) выбрать используемый профиль vNIC из выпадающего списка "Целевой профиль vNIC";

3) если в окне "Импорт ВМ" было выбрано несколько целевых кластеров, выбрать каждый целевой кластер из выпадающего списка "Целевой кластер" и убедиться в том, что отображения корректны;

4) нажать кнопку OK;

з) при обнаружении конфликта MAC-адресов рядом с именем ВМ появится "!" (восклицательный знак). Навести курсор на "!" (восклицательный знак), чтобы просмотреть всплывающую подсказку с возникшей ошибкой. Установить флажок "Повторно присвоить неправильные MAC", чтобы повторно присвоить конфликтующие MAC-адреса всем проблемным ВМ;

Примечание — Импорт ВМ закончится неудачей в случае отсутствия доступных MAC-адресов для присвоения. Тем не менее возможен импорт ВМ без присвоения новых адресов при использовании MAC-адресов, расположенных вне диапазона пула MAC-адресов кластера.

и) нажать кнопку OK.

3.6.6.1.6 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 присоединен к дата-центру и активирован.

Для импорта шаблонов из импортированного домена данных нужно выполнить следующие действия:

а) нажать "Хранилище → Домены";

б) нажать на имя импортированного домена данных, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Импорт шаблонов";

г) выбрать один или несколько шаблонов для импорта;

д) нажать кнопку `Импортировать`;

е) убедиться, что для каждого шаблона в окне "Импорт шаблонов" выбран корректный целевой кластер из списка "Кластер";

ж) отобразить внешние профили vNIC на профили, присутствующие в целевом кластере:

1) нажать кнопку `Отображение профилей vNIC`;

2) выбрать используемый профиль vNIC из выпадающего списка "Целевой профиль vNIC";

3) если в окне "Импорт шаблонов" было выбрано несколько целевых кластеров, выбрать каждый целевой кластер из выпадающего списка "Целевой кластер" и убедиться в том, что отображения корректны;

4) нажать кнопку `OK`;

з) нажать кнопку `OK`.

3.6.6.2 Работа с доменами хранилищ

3.6.6.2.1 Размещение образов в доменах данных

Образы виртуальных дисков и образы ISO в домен хранения данных можно загрузить 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 или использовать для загрузки ВМ.

Так как функция загрузки (отправки) образов в домен использует HTML5 API, в качестве предварительных условий для размещения образов в доменах данных 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 импорта центра сертификации следует перейти по адресу https://адрес_диспетчера_виртуализации/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA и включить все параметры доверия.

– Браузер с поддержкой HTML5.

Для размещения образа в домене хранения данных нужно выполнить следующие действия:

а) нажать "Хранилище → Домены хранилищ → ISO → Диски" (рисунок 178);

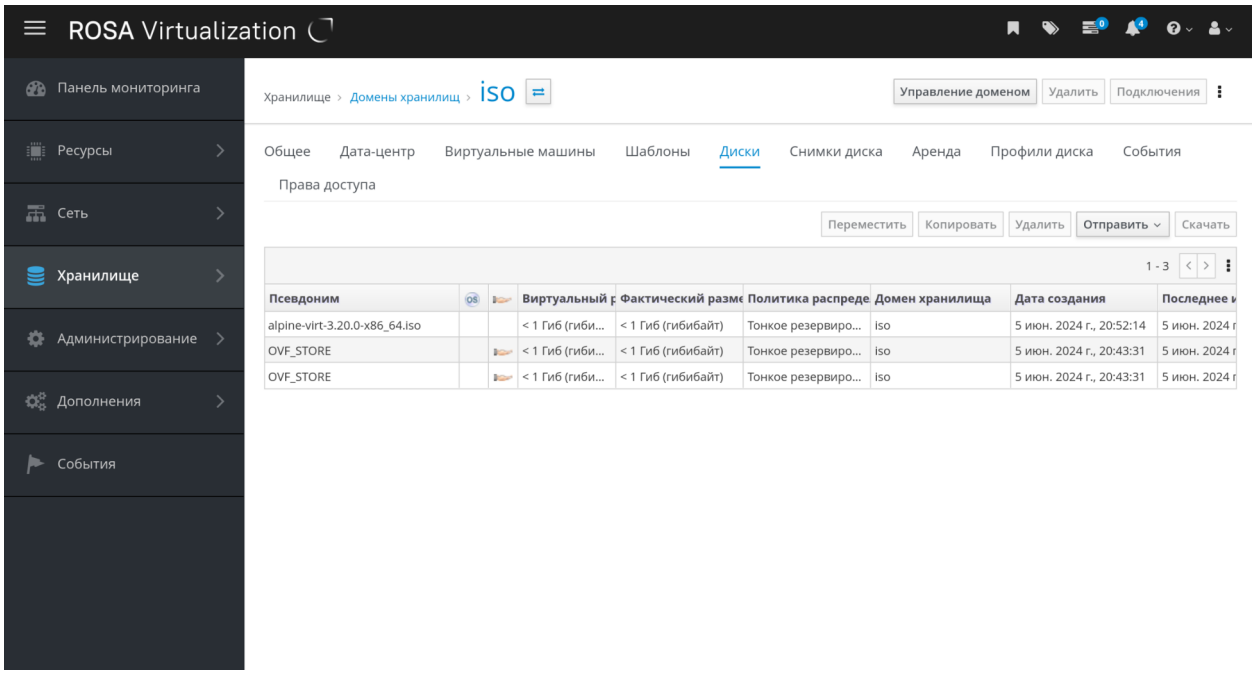


Рисунок 178 – Секция "Хранилище → Домены хранилищ → ISO", вкладка "Диски"

б) в меню нажать кнопку Отправить и выбрать "Начать" (рисунок 179);

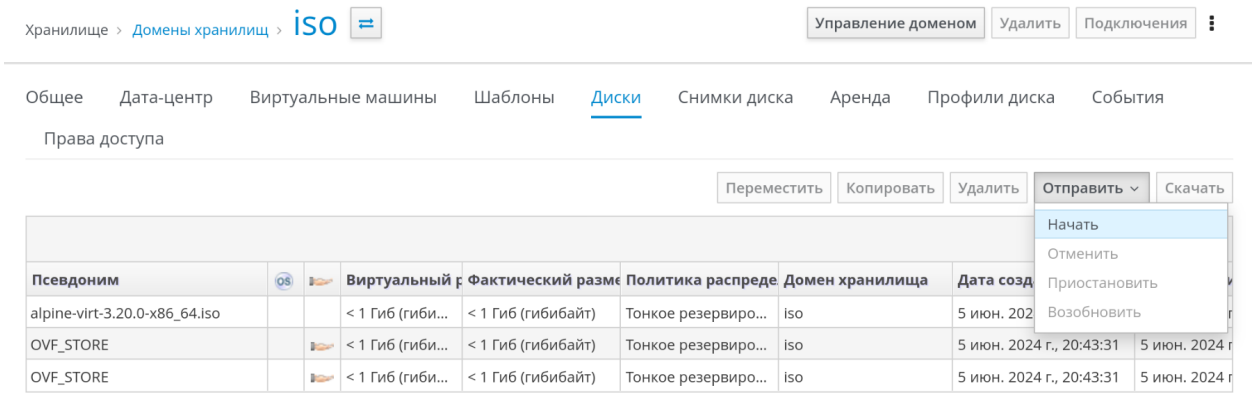


Рисунок 179 – Форма для отправки образа диска в хранилище

в) нажать кнопку `Выберите файл` и выбрать образ для загрузки в домен (рисунок 180);

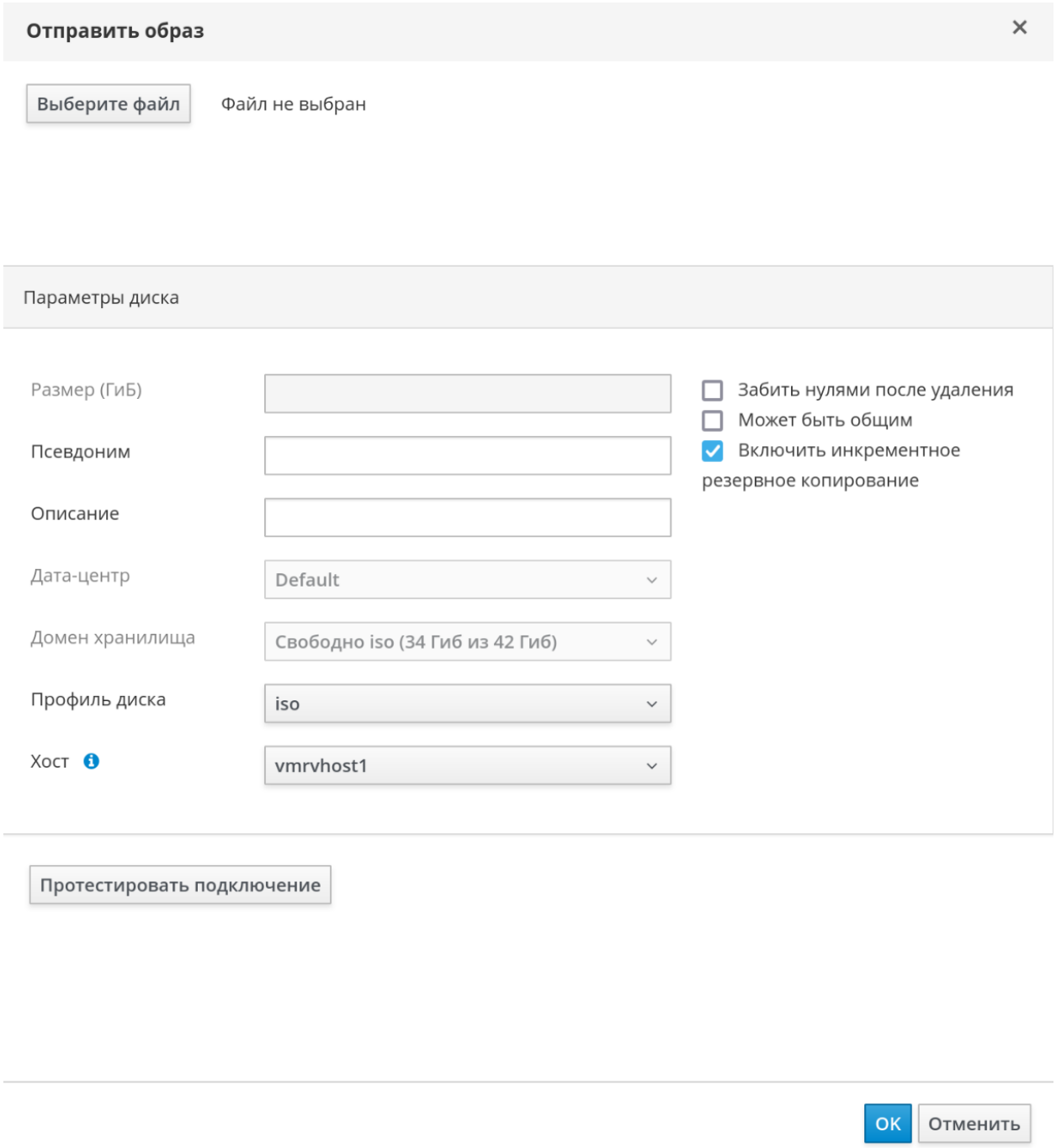


Рисунок 180 – Выбор файла с образом диска для отправки в домен

г) заполнить поля "Параметры диска";
д) нажать кнопку OK.

Статус загрузки образа в домен отображается с помощью индикатора выполнения.

В меню по нажатию кнопки Отправить можно приостановить, отменить или возобновить отправку файлов.

3.6.6.2.1.1 Увеличение значения времени ожидания отправки

Для увеличения значения времени ожидания отправки необходимо:

а) в случае превышения времени ожидания окончания отправки и появления соответствующего сообщения "Причина: превышение времени ожидания в связи с неактивностью передачи" выполнить следующую команду для увеличения значения времени ожидания:

```
    # engine-config -s
TransferImageClientInactivityTimeoutInSeconds=6000
```

б) перезапустить службу ovirt-engine:

```
    # systemctl restart ovirt-engine
```

3.6.6.2.2 Перевод доменов хранилищ в режим обслуживания

Перед откреплением и удалением домена хранения следует обязательно перевести 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.

Для перевода домена хранения в режим обслуживания нужно:

а) выключить все ВМ, выполняющиеся в домене хранения;
б) нажать "Хранилище → Домены";
в) нажать на имя домена, чтобы перейти к подробному просмотру;
г) перейти на вкладку "Дата-центр";
д) нажать кнопку Обслуживание;

Примечание — Опционально установить флажок "Игнорировать сбой обновления OVF" для перемещения домена хранения в режим обслуживания даже при сбое обновления OVF.

е) нажать кнопку кнопку 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.

3.6.6.2.3 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 присоединенного, 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.

Для изменения параметров активного домена хранения нужно:

а) нажать "Хранилище → Домены" и выбрать домен хранения;

б) нажать "Управление доменом";

в) при необходимости изменить значения доступных полей;

г) нажать кнопку OK.

Для изменения параметров неактивного домена хранения нужно:

а) нажать "Хранилище → Домены";

б) если домен хранения активен, переместить домен в режим обслуживания:

1) нажать на имя домена, чтобы перейти к подробному просмотру;

2) перейти на вкладку "Дата-центр";

3) нажать кнопку Обслуживание;

4) нажать кнопку OK;

в) нажать кнопку Управление доменом;

г) изменить путь к хранилищу и другие необходимые сведения. Сведения о новых сетевых соединениях должны иметь тот же тип хранилища, что и исходное соединение;

д) нажать кнопку OK;

е) активировать домен хранения:

1) нажать на имя домена хранения, чтобы перейти к подробному просмотру;

2) перейти на вкладку "Дата-центр";

3) нажать кнопку Активировать.

3.6.6.2.4 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).

Для обновления файлов OVF нужно:

а) нажать "Хранилище → Домены";

б) выбрать домен хранения, нажать кнопку ⋮ (Больше действий) и далее нажать кнопку Обновить файлы OVF.

3.6.6.2.5 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.

Для активации домена хранения из режима обслуживания необходимо:

а) нажать "Хранилище → Домены";

б) нажать на имя неактивного домена, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Дата-центры";

г) нажать кнопку Активировать.

Примечание — При попытке активации домена ISO до активации домена данных будет показано соответствующее сообщение об ошибке, и домен ISO не будет активирован.

3.6.6.2.6 Отсоединение домена хранения от дата-центра

Домен хранения необходимо отсоединить от одного дата-центра, чтобы выполнить миграцию домена в другой дата-центр.

Для отсоединения домена хранения от дата-центра нужно:

а) нажать "Хранилище → Домены";

б) нажать на имя домена, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Дата-центр";

г) нажать кнопку Обслуживание;

д) нажать кнопку OK для инициации режима обслуживания;

е) нажать кнопку Отсоединить;

ж) нажать кнопку OK, чтобы отсоединить домен хранения.

В результате домен хранения будет отсоединен от текущего дата-центра и готов для присоединения к другому дата-центру.

3.6.6.2.7 Присоединение домена хранения к дата-центру

Для присоединения домена хранения к дата-центру нужно:

а) нажать "Хранилище → Домены";

б) нажать на имя домена, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Дата-центр";

г) нажать кнопку Присоединить;

д) выбрать необходимый дата-центр;

е) нажать кнопку OK.

В результате домен хранения будет присоединен к выбранному дата-центру и автоматически активирован.

3.6.6.2.8 Удаление домена хранения

Для удаления домена хранения нужно:

а) нажать "Хранилище → Домены";

б) переместить домен хранения в режим обслуживания и отсоединить домен:

1) нажать на имя домена, чтобы перейти к подробному просмотру;
2) перейти на вкладку "Дата-центр";
3) нажать кнопку Обслуживание и далее нажать кнопку OK;
4) нажать кнопку Отсоединить и далее нажать кнопку OK;

в) нажать кнопку Удалить;

г) опционально установить флажок "Форматировать домен", чтобы окончательно стереть все содержимое домена, т.е. содержимое хранилища будет потеряно;

д) нажать кнопку OK.

3.6.6.2.9 Разрушение домена хранения

Домен хранения, содержащий ошибки, не всегда возможно удалить посредством стандартной процедуры. Разрушение домена хранения принудительно удаляет домен из окружения.

Для разрушения домена хранения:

а) нажать "Хранилище → Домены".

б) выбрать домен хранилища, нажать кнопку ⋮ (Больше действий) и далее нажать кнопку Разрушить;

в) установить флажок "Одобрить операцию";

г) нажать кнопку OK.

3.6.6.2.10 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.

Для создания профиля диска нужно выполнить следующие действия:

а) нажать "Хранилище → Домены";
б) нажать на имя домена, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Профили диска";
г) нажать кнопку Добавить;
д) ввести "Имя" и "Описание" профиля диска;
е) в списке "QoS" выбрать запись о качестве обслуживания, которую нужно применить к профилю диска;
ж) нажать кнопку OK.

3.6.6.2.11 Удаление профилей дисков

Для удаления профиля диска нужно:

а) нажать "Хранилище → Домены";
б) нажать на имя домена, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Профили диска";
г) выбрать удаляемый профиль диска;
д) нажать кнопку Удалить;
е) нажать кнопку OK.

3.6.6.2.12 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, требуется нажать на имя домена и перейти 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 можно использовать набор events.

3.6.6.2.13 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) освобожденное 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.

3.6.6.3 Управление хостами хранилища Gluster

3.6.6.3.1 Масштабирование тома GlusterFS

Для масштабирования тома GlusterFS необходимо выполнить следующие действия:

а) на вкладке "Ресурсы → Хосты" добавить хост с подготовленным устройством хранения данных и дождаться перезагрузки и активации хоста;

б) при необходимости выполнить настройку сети, предоставляющей доступ к GlusterFS (рисунок 181);

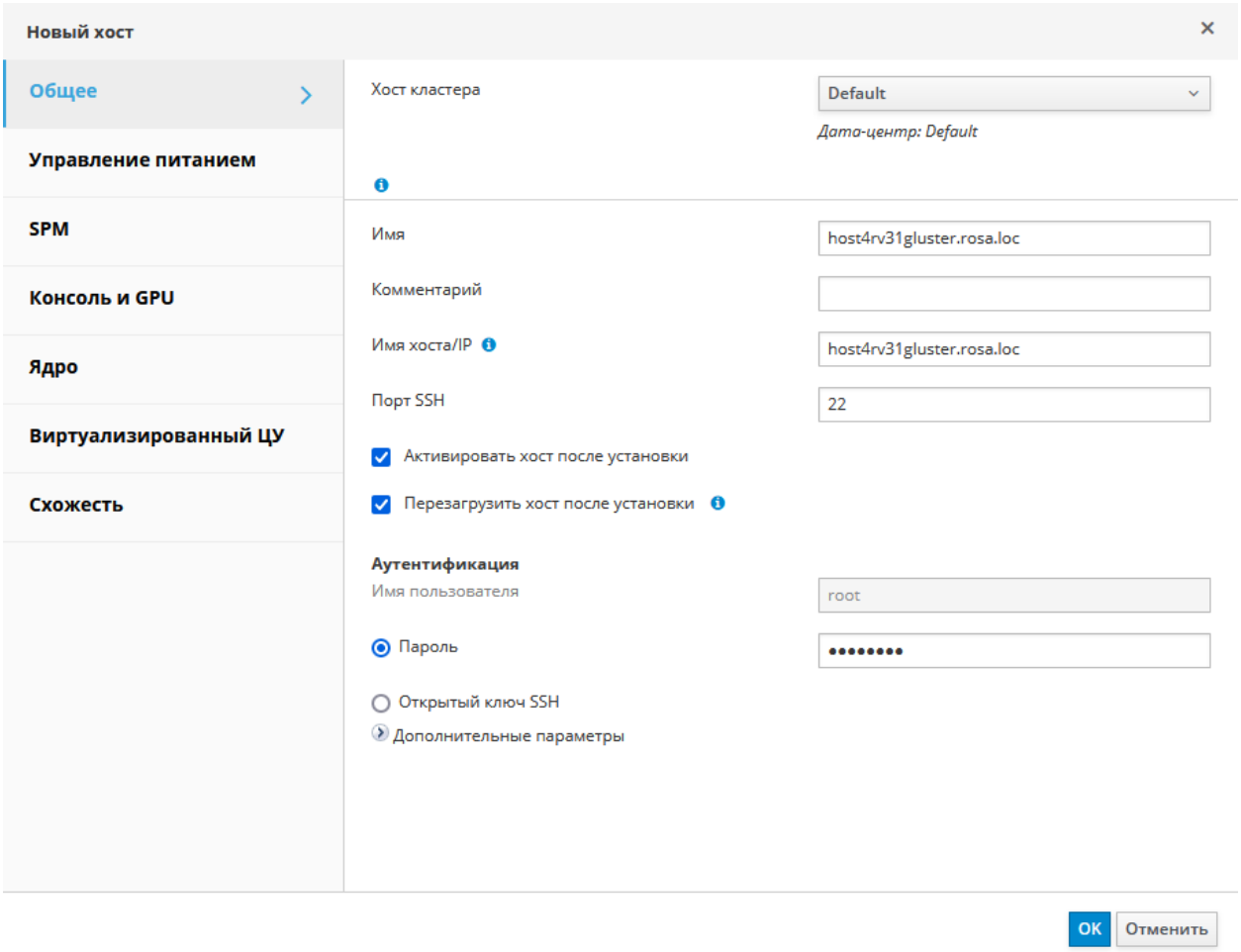


Рисунок 181 – Добавление хоста с подготовленным устройством хранения данных

в) на вкладке "Ресурсы → Хосты" нажать на имя добавленного хоста и перейти на страницу "Устройства хранения";

г) выделить нужное устройство и нажать кнопку `Создать элемент тома` (рисунок 182);

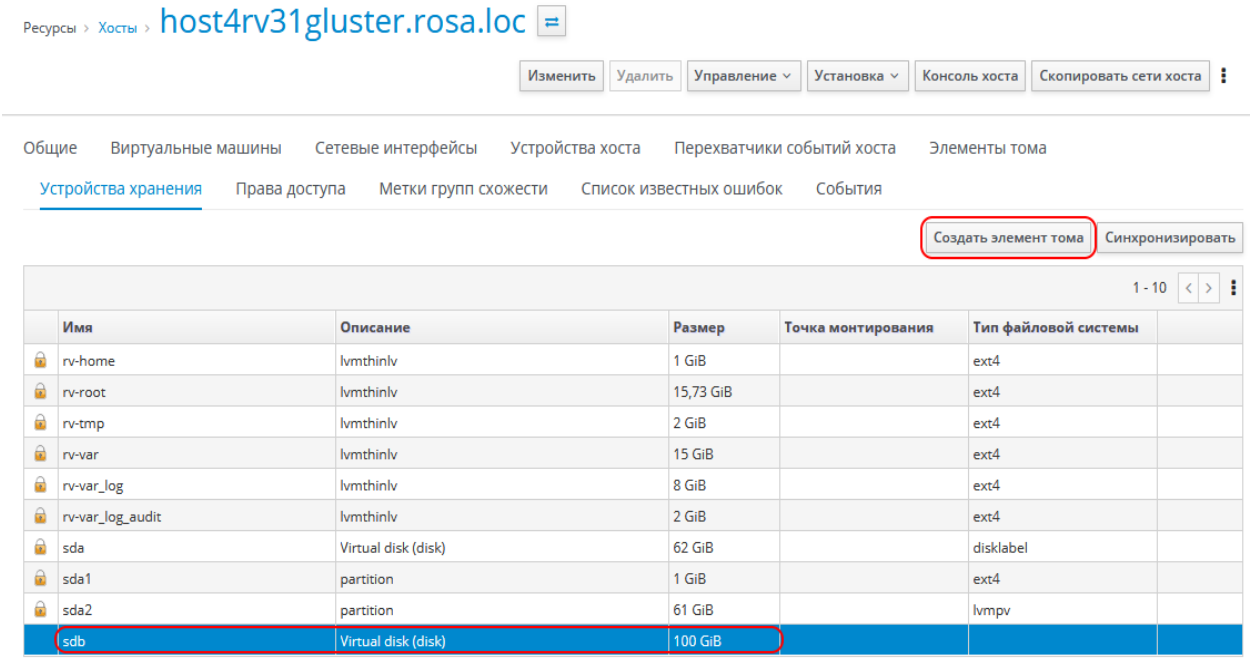


Рисунок 182 – Устройства хранения хоста

д) задать имя элемента тома в поле "Имя элемента тома" и нажать клавишу Tab, после чего поле "Точка монтирования" должно заполниться автоматически;

е) если для выбранного устройства хранения используется RAID, то указать его тип, выбрав из списка "Тип RAID" необходимый тип;

ж) задать размер тома в поле "Размер";

з) нажать кнопку OK (рисунок 183).

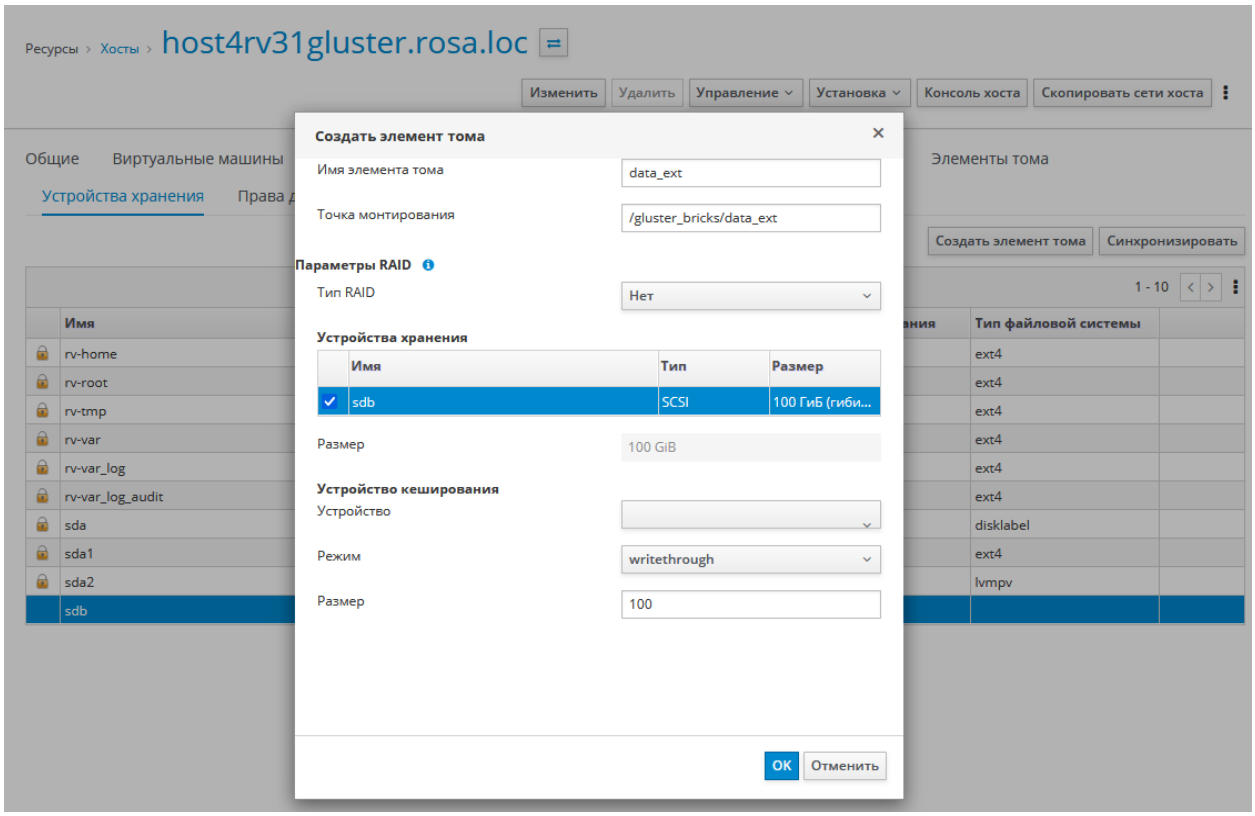


Рисунок 183 – Создание элемента тома

Правильно созданный и готовый к подключению элемент тома выглядит так, как показано на рисунке 184.

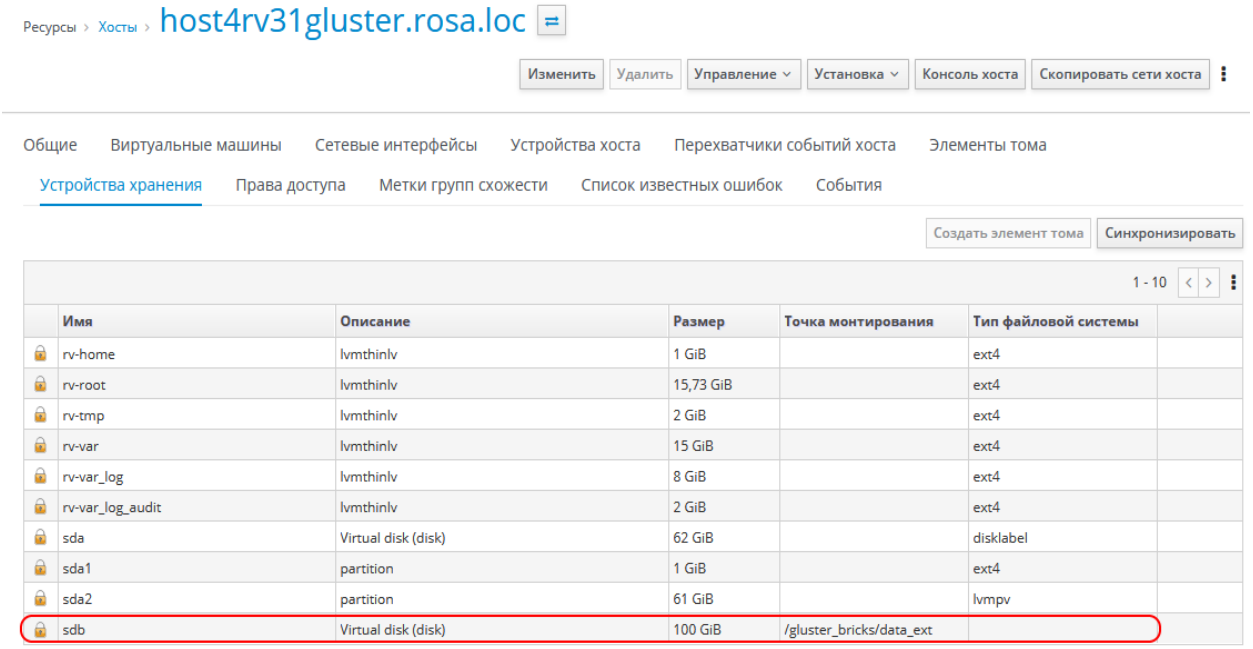


Рисунок 184 – Устройства хранения хоста с созданным элементом тома

Примечание – После создания элемента тома и до окончания всей процедуры расширения тома GlusterFS нельзя нажимать кнопку Синхронизировать или же перезагружать хост с подготовленным устройством хранения данных для GlusterFS.

и) выполнить все описанные выше действия последовательно для каждого хоста, участвующего в расширении тома GlusterFS. Количество новых элементов тома должно быть кратно числу реплик;

к) перейти на вкладку "Хранилище → Тома";

л) нажать на имя расширяемого тома и перейти на страницу "Элементы тома";

м) нажать кнопку Добавить и заполнить таблицу новыми элементами тома с каждого подготовленного для этой задачи хоста. Количество добавляемых элементов тома должно быть кратно числу реплик;

н) нажать кнопку ОК. Потребуется некоторое время, не менее 5 минут, для подключения новых элементов тома и получения данных Self-Heal (рисунок 185);

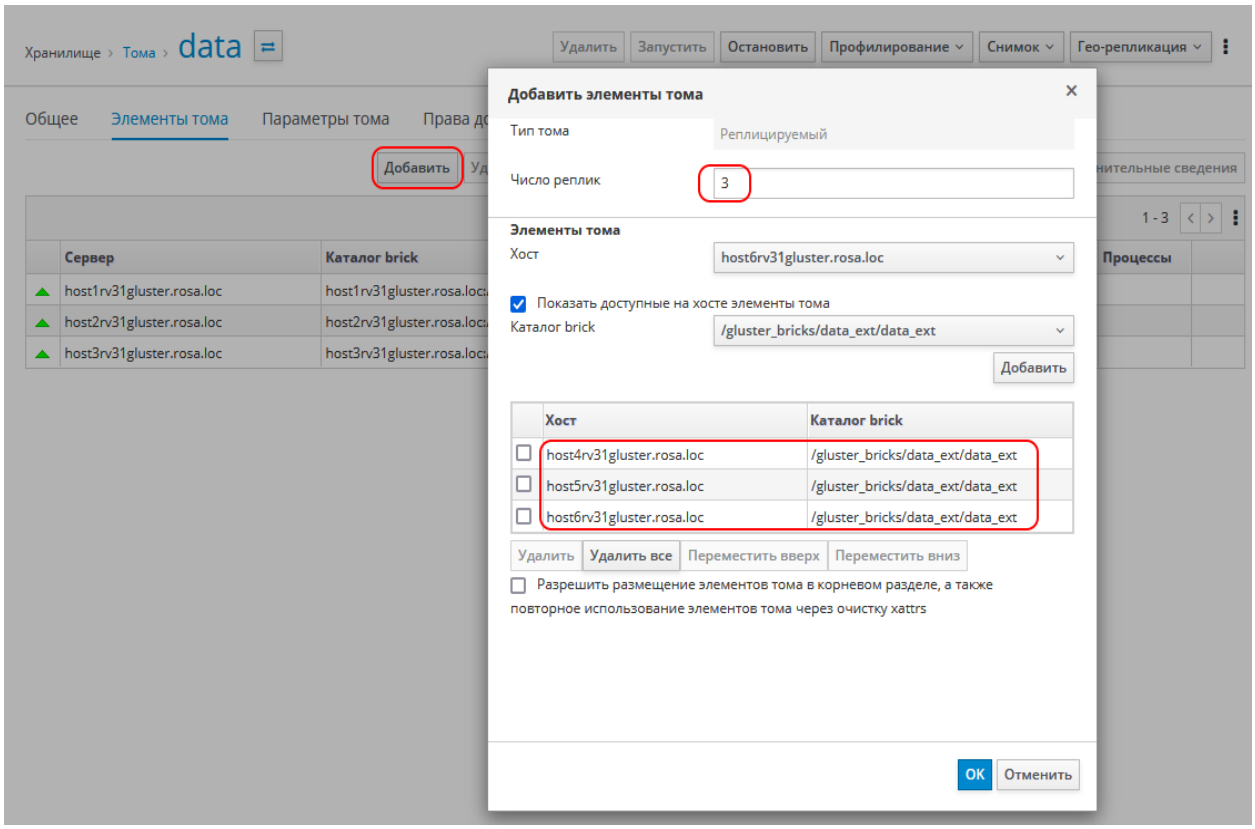


Рисунок 185 – Добавление элементов тома

о) после успешного завершения подключения новых элементов тома данные Self-Heal должны перейти в статус "OK", а элемент тома в активное состояние (рисунок 186).

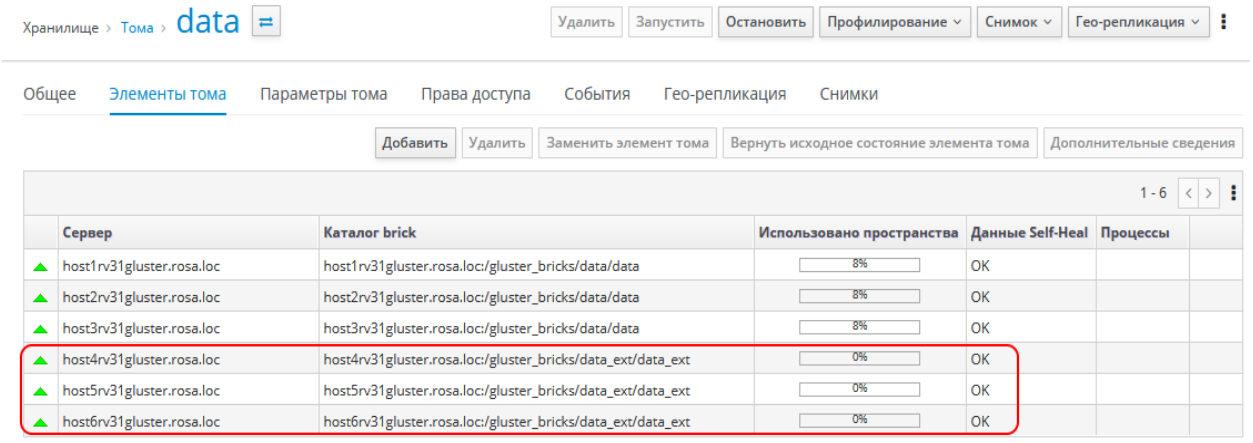


Рисунок 186 – Элементы тома и их состояние

3.6.6.3.2 Замена элемента тома в случае его полной недоступности

В случае поломки хоста может потребоваться замена элемента тома.

Для замены элемента тома требуется выполнить следующие действия:

а) открыть вкладку "Ресурсы → Хосты";

б) выбрать в списке хостов неисправный хост и перевести его в режим обслуживания;

в) добавить в кластер новый хост с именем, отличающимся от имени хоста, который требуется заменить (рисунок 187);

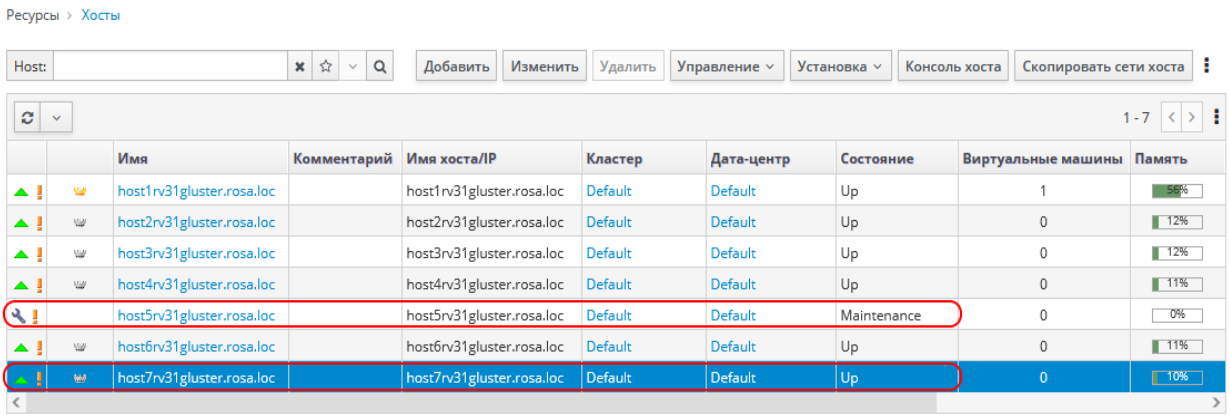


Рисунок 187 – Список хостов с добавленным новым хостом

г) на вкладке "Ресурсы → Хосты" нажать на имя добавленного хоста и перейти на страницу "Устройства хранения";

д) выбрать нужное устройство хранения и нажать кнопку Создать элемент тома (рисунок 188);

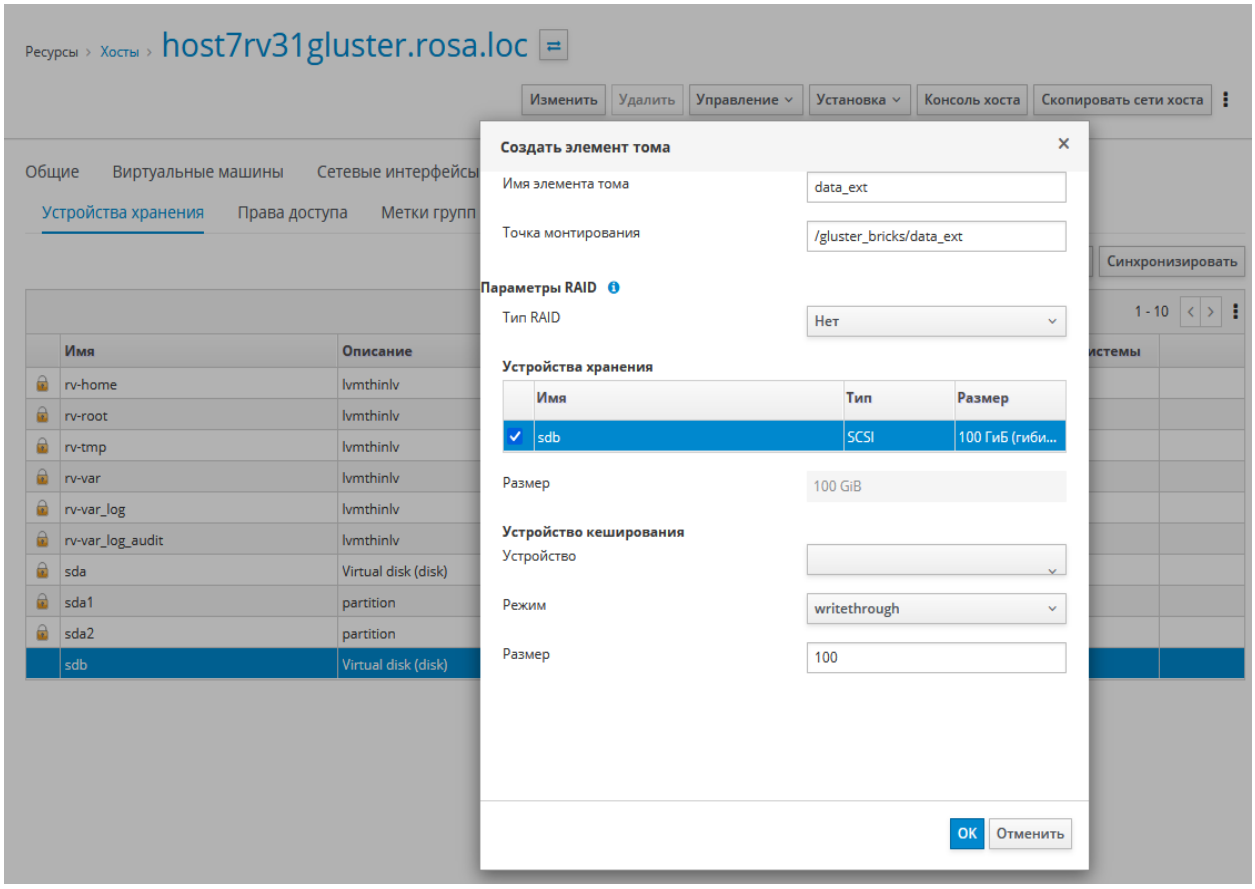


Рисунок 188 – Создание элементов тома

е) задать в поле "Имя элемента тома" имя элемента тома и нажать клавишу Tab, после чего поле "Точка монтирования" должно заполниться автоматически;

ж) если для выбранного устройства хранения используется RAID, то указать его тип, выбрав необходимое значение из списка "Тип RAID" в группе "Параметры RAID";

з) задать размер тома в поле "Размер" и нажать кнопку OK. Желательно, чтобы имя элемента тома было точно таким же, как и на неисправном хосте, который требуется заменить;

и) перейти на вкладку "Хранилище → Тома" и нажать на имя поврежденного тома;

к) перейти на вкладку "Элементы тома", выделить поврежденный элемент тома и нажать кнопку Заменить элемент тома (рисунок 189);

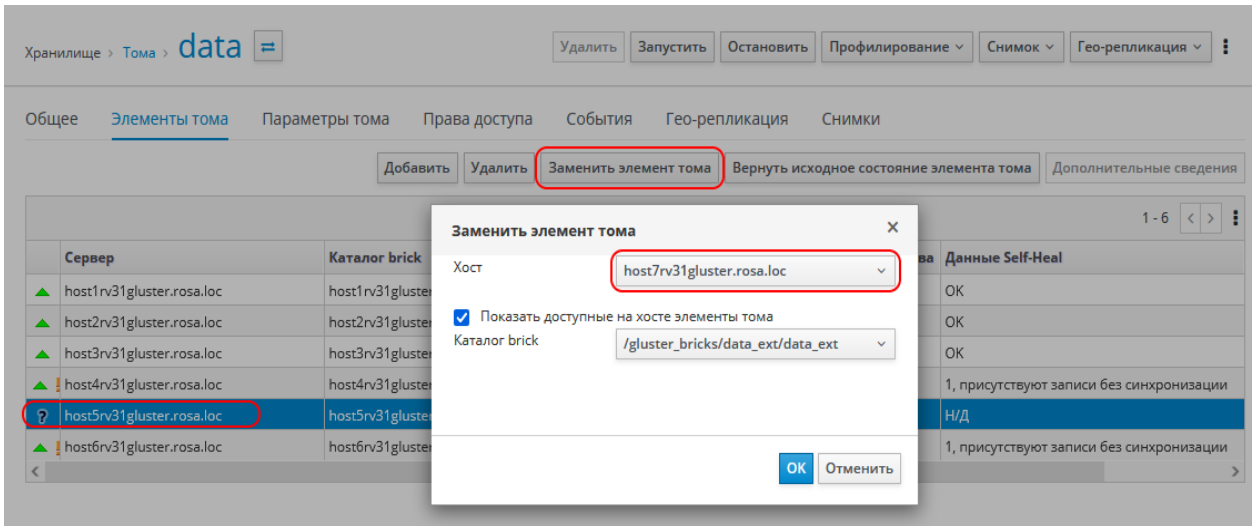


Рисунок 189 – Замена элементов тома

л) в поле "Хост" формы замены элемента тома выбрать ранее добавленный хост с подготовленным новым элементом тома, в поле "Каталог brick" выбрать элемент тома (рисунок 189);

м) нажать кнопку OK. Потребуется некоторое время, не менее 5 минут, для замены старого элемента тома на новый, получения данных Self-Heal и перехода в активное состояние (рисунок 190);

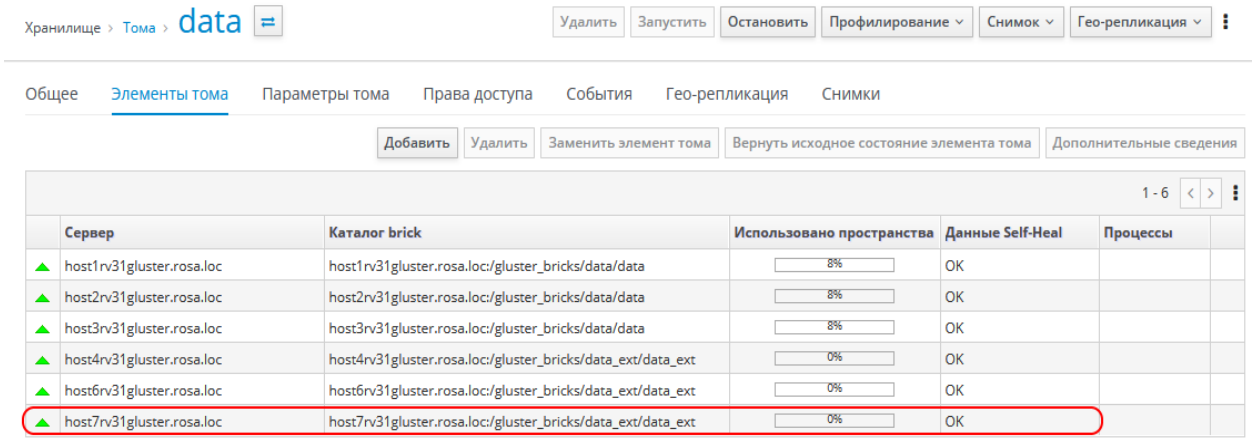


Рисунок 190 – Элементы тома и их состояние

н) после успешной замены элемента тома перейти на вкладку "Ресурсы → Хосты" и выполнить процедуру удаления неисправного хоста виртуализации, в форме "Удалить хосты" подтвердив удаление хоста, нажав на кнопку OK (рисунок 201).

3.6.7 Подключение отказоустойчивого хранилища CephFS

Важно – В данном разделе описываются процесс и параметры настройки "Средства виртуализации "РОСА Виртуализация 4" при подключения хранилища CephFS. Данный раздел не является руководством по настройке и администрированию кластера хранилища Ceph. Для настройки и администрирования кластера хранилища Ceph следует обратиться к соответствующему руководству поставщика хранилища. Для самостоятельной установки хранилища Ceph можно воспользоваться документацией по ссылке https://docs.ceph.com/en/latest/.

3.6.7.1 Требования к программным и аппаратным средствам

3.6.7.1.1 Требования к РОСА Виртуализация

Требования к РОСА Виртуализация включают следующие условия:

– Развернута базовая конфигурация РОСА Виртуализация, предназначенная для использования в промышленном режиме функционирования в качестве средства виртуализации вычислительных центров.

– Используется РОСА Виртуализация версии 4.0 или новее.

3.6.7.1.2 Отказоустойчивое хранилище Ceph

Требования к хранилищу Ceph включают следующие условия:

– Развернута конфигурация отказоустойчивого хранилища Ceph – кластер, хосты, мониторы (MON), серверы метаданных (MDS), устройства хранения объектов (OSD).

– Используется версия Ceph 18.x или 19.x.

3.6.7.2 Создание и настройка файловой системы CephFS в кластере Ceph

Все действия по созданию и настройке файловой системы Ceph (CephFS) можно выполнить с помощью веб-интерфейса администрирования кластера Ceph.

3.6.7.2.1 Проверка версии Ceph и работоспособности кластера

3.6.7.2.1.1 Проверка версии Ceph в веб-интерфейсе

Для проверки версии Ceph в веб-интерфейсе следует:

а) открыть в веб-браузере интерфейс администрирования Ceph. Обычно это интерфейс Ceph Dashboard, доступный по URL-адресу вашего кластера. Адрес выглядит как http://<ip-адрес-вашего-кластера>:<порт>, где порт по умолчанию — 8080;

б) войти в панель администрирования, для чего ввести свои учетные данные для получения доступа к панели управления (логин и пароль администратора) (рисунок 191);



Рисунок 191 – Форма для ввода логина и пароля для доступа в интерфейс администрирования Ceph

в) после входа в Систему и появления главной панели управления ("Панель мониторинга") найти информацию о версии, которая располагается в группе "Ceph version" секции "Details" (рисунок 192).

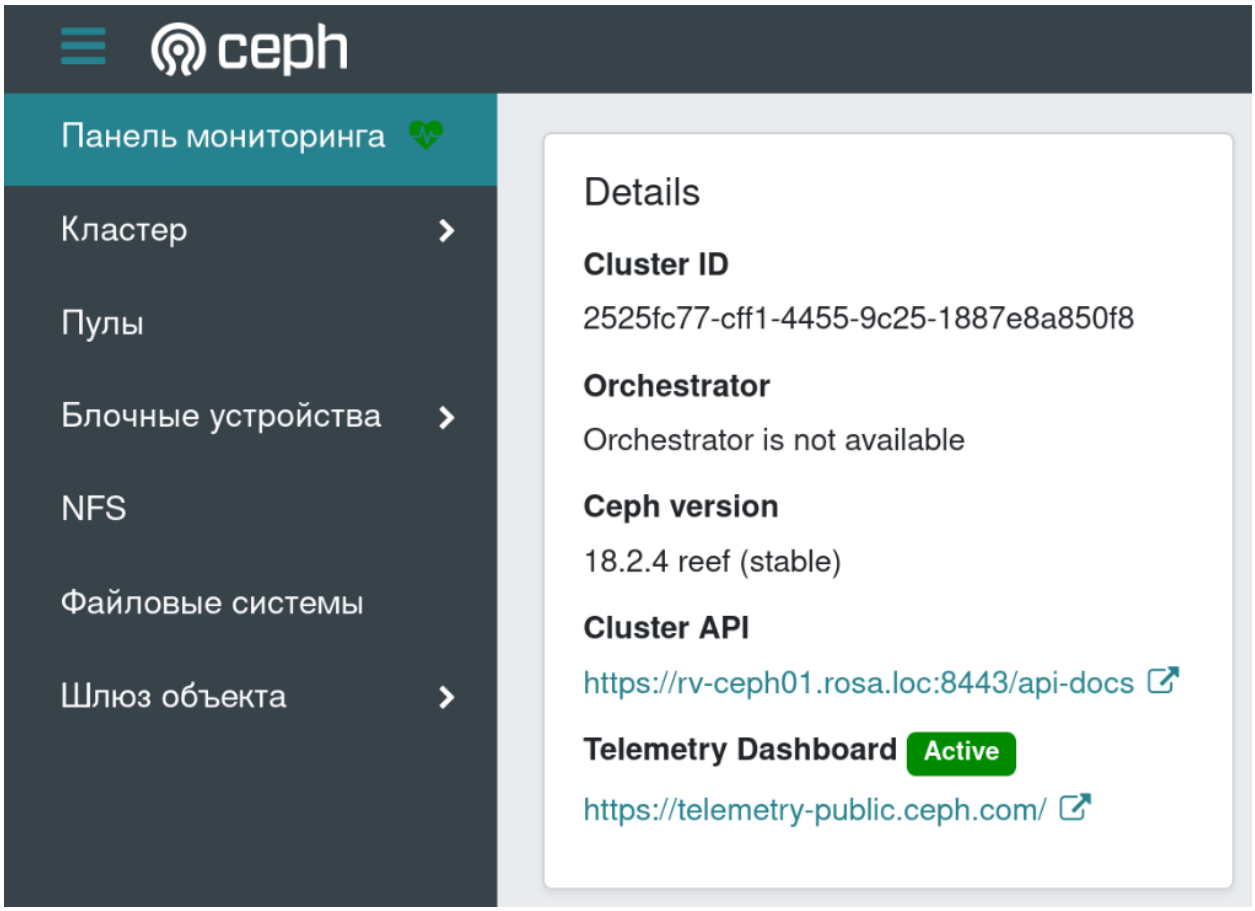


Рисунок 192 – Информация о версии Ceph в веб-интерфейсе

В данном примере используется Ceph версии "18.2.4 reef (stable)".

Данная версия подходит для подключения хранилища CephFS к РОСА Виртуализация.

3.6.7.2.1.2 Проверка работоспособности кластера Ceph в веб-интерфейсе

В п. 3.6.7.2.1.1 описаны действия по входу в интерфейс администрирования Ceph и проверке версии Ceph.

Для проверки работоспособности кластера Ceph в веб-интерфейсе нужно:

а) открыть в веб-интерфейсе Ceph "Панель мониторинга" и найти в панели мониторинга секцию "Status" (рисунок 193). Если рядом со словом "Кластер" стоит значок (флажок в круге зеленого цвета), то кластер функционирует в штатном режиме;

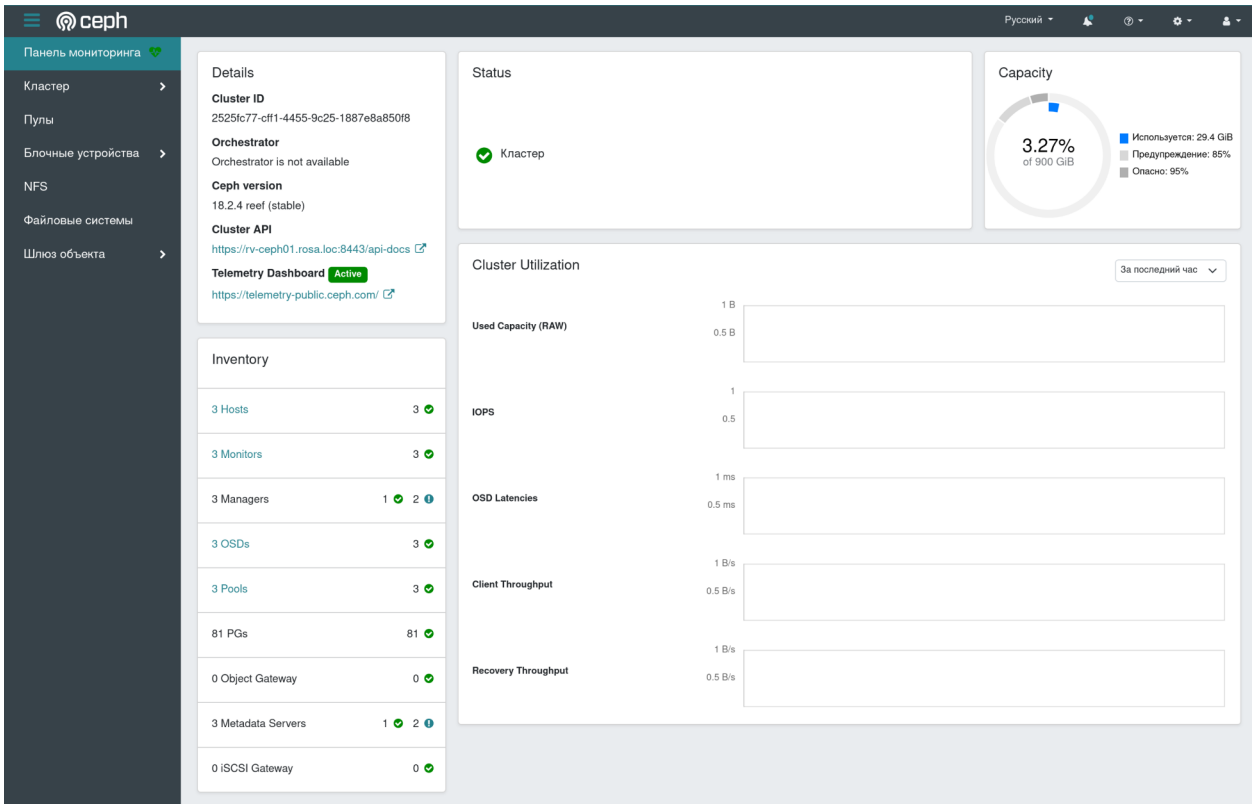


Рисунок 193 – Панель мониторинга веб-интерфейса Ceph

б) найти в панели мониторинга секцию "Inventory" (рисунок 194). В этой секции отображается информация о хостах Ceph, мониторах, менеджерах, OSD, пулах и серверах метаданных (MDS). Хосты Ceph, мониторы, менеджеры, OSD, пулы и сервер метаданных (MDS) должны быть активны (напротив соответствующего параметра стоит значок ✅ (флажок в круге зеленого цвета).

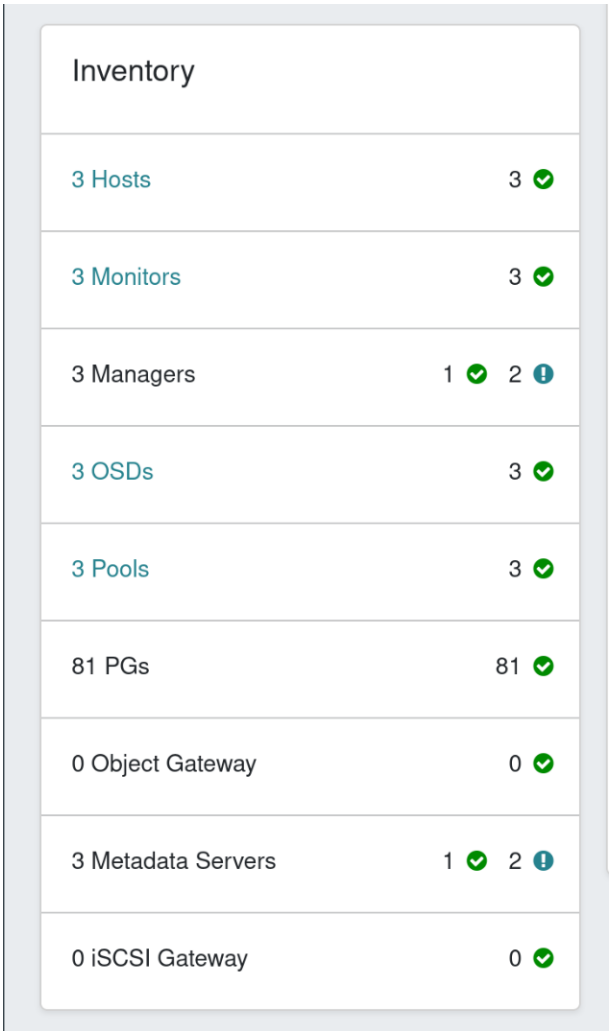


Рисунок 194 – Хранилище Ceph — секция "Inventory"

Примечание – Object Gateway и iSCSI Gateway не требуются для подключения CephFS к POCA Виртуализация. Подключение использует возможности CephFS.

3.6.7.2.1.3 Проверка версии Ceph в командной строке

Для проверки версии Ceph в командной строке нужно выполнить вход на хост Ceph с помощью SSH и затем выполнить в консоли команду `ceph --version`:

```
[root@rv-ceph01 ~]# ceph --version
```

```
    ceph version 18.2.4
(e7ad5345525c7aa95470c26863873b581076945d) reef (stable)
```

В данном примере используется Ceph версии "18.2.4 reef (stable)". Данная версия подходит для подключения хранилища CephFS к РОСА Виртуализация.

3.6.7.2.1.4 Проверка работоспособности кластера Ceph в командной строке

Для проверки работоспособности кластера Ceph в командной строке выполнить вход на хост Ceph с помощью ssh, и затем выполнить в консоли команду ceph status:

```
    [root@rv-ceph01 ~]# ceph status
      cluster:
        id:     2525fc77-cff1-4455-9c25-1887e8a850f8
        health: HEALTH_OK

      services:
        mon: 3 daemons, quorum rv-ceph01,rv-ceph02,rv-ceph03
(age 14h)
        mgr: rv-ceph01(active, since 11d), standbys: rv-ceph02,
rv-ceph03
        mds: 1/1 daemons up, 2 standby
        osd: 3 osds: 3 up (since 11d), 3 in (since 6w)

      data:
        volumes: 1/1 healthy
        pools:   3 pools, 81 pgs
        objects: 2.20k objects, 8.3 GiB
        usage:   29 GiB used, 871 GiB / 900 GiB avail
        pgs:     81 active+clean

      io:
        client:   513 KiB/s rd, 3.6 KiB/s wr, 1 op/s rd, 1 op/s
wr
```

Статус "health: HEALTH_OK" сообщает о том, что кластер работоспособен.

Проверку работоспособности кластера Ceph можно также выполнить, используя фильтр `grep` для получения статуса кластера:

```
[root@rv-ceph01 ~]# ceph status | grep health:
    health: HEALTH_OK
```

3.6.7.2.2 Создание файловой системы Ceph

Для создания необходимо открыть в браузере веб-интерфейс администрирования кластера Ceph и выбрать в боковой панели управления секцию "Файловые системы". В результате откроется экранная форма для управления файловыми системами Ceph (рисунок 195).

Далее следует нажать на кнопку `+ Создание`, ввести в поле "Имя" имя файловой системы cephfs_rv и нажать на кнопку `Создание файловой системы` для создания файловой системы с указанным именем (рисунок 195).

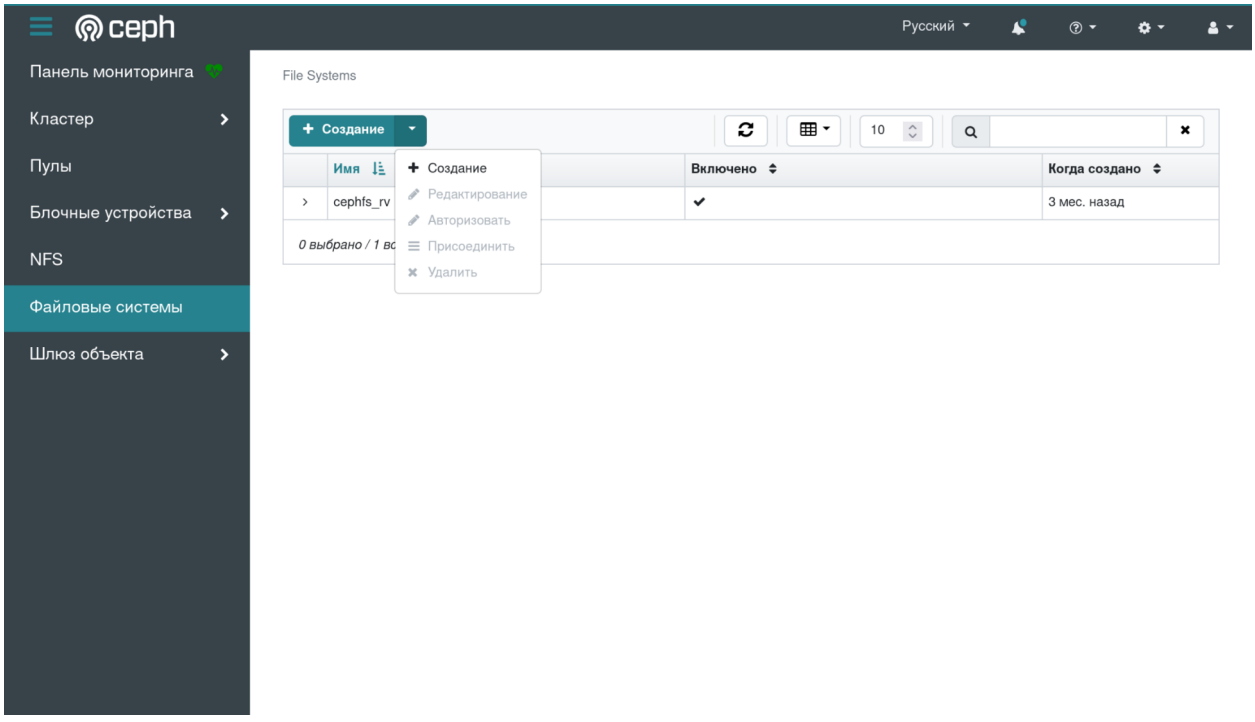


Рисунок 195 – Интерфейс формы "Файловые системы"

После создания файловая система отобразится в списке доступных файловых систем Ceph (рисунок 196).

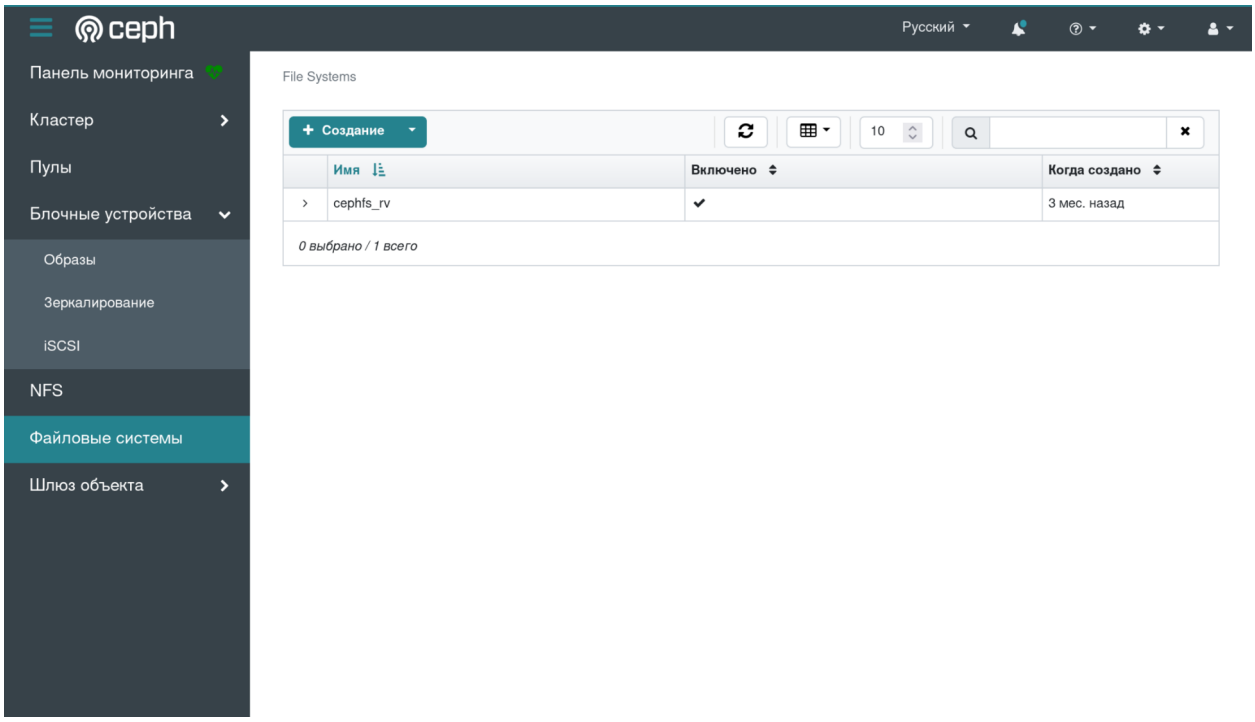


Рисунок 196 – Список доступных файловых систем Ceph

3.6.7.2.3 Создание группы подтомов

В файловой системе cephfs_rv необходимо создать "Группу подтомов (Subvolume group)" с именем vdsm_kvm и соответствующими значениями в полях UID – "36", GID – "36".

Права доступа на директорию следует оставить без изменений: 755 (rwxr-xr-x).

Для создания группы подтомов нужно выполнить следующие действия:

а) выбрать файловую систему в верхней части формы и затем дополнительную секцию "Группы подтомов" в нижней части формы;

б) нажать на кнопку + Создание для создания группы подтомов (рисунок 197);

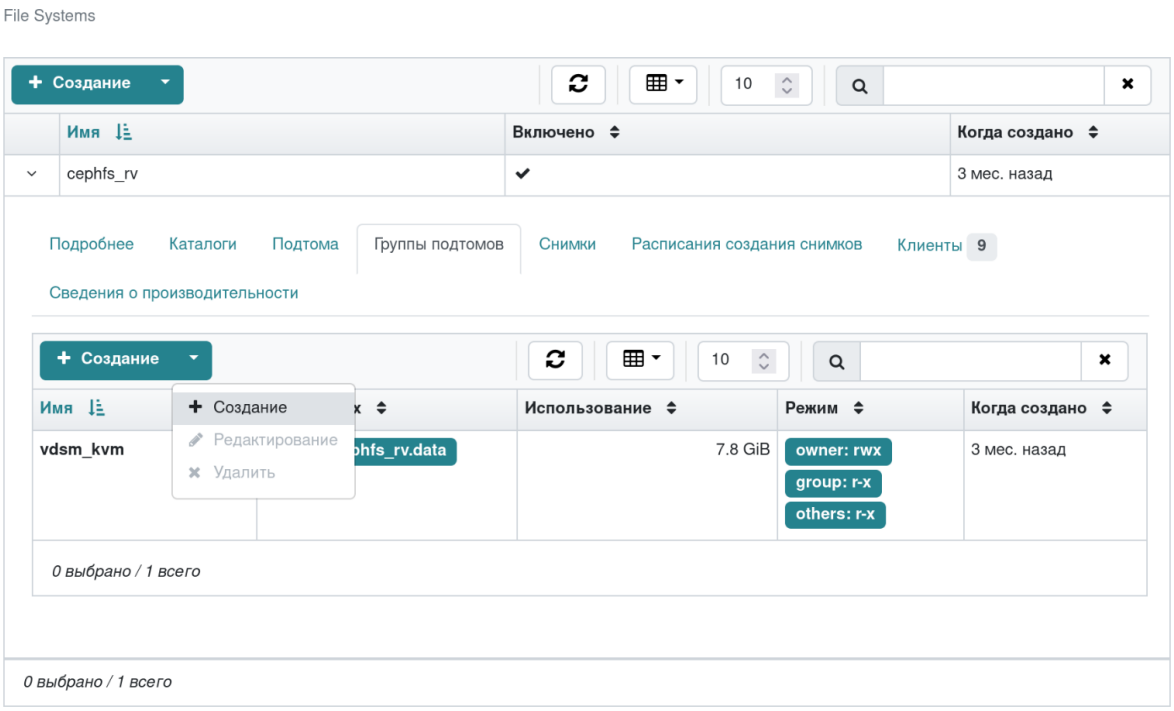


Рисунок 197 – Создание группы подтомов

в) ввести в поле "Имя" имя группы "vdsm_kvm", в поле UID – "36", в поле GID – "36" (рисунок 198).

г) нажать на кнопку Создание группы подтома для создания группы подтома с указанными выше параметрами.

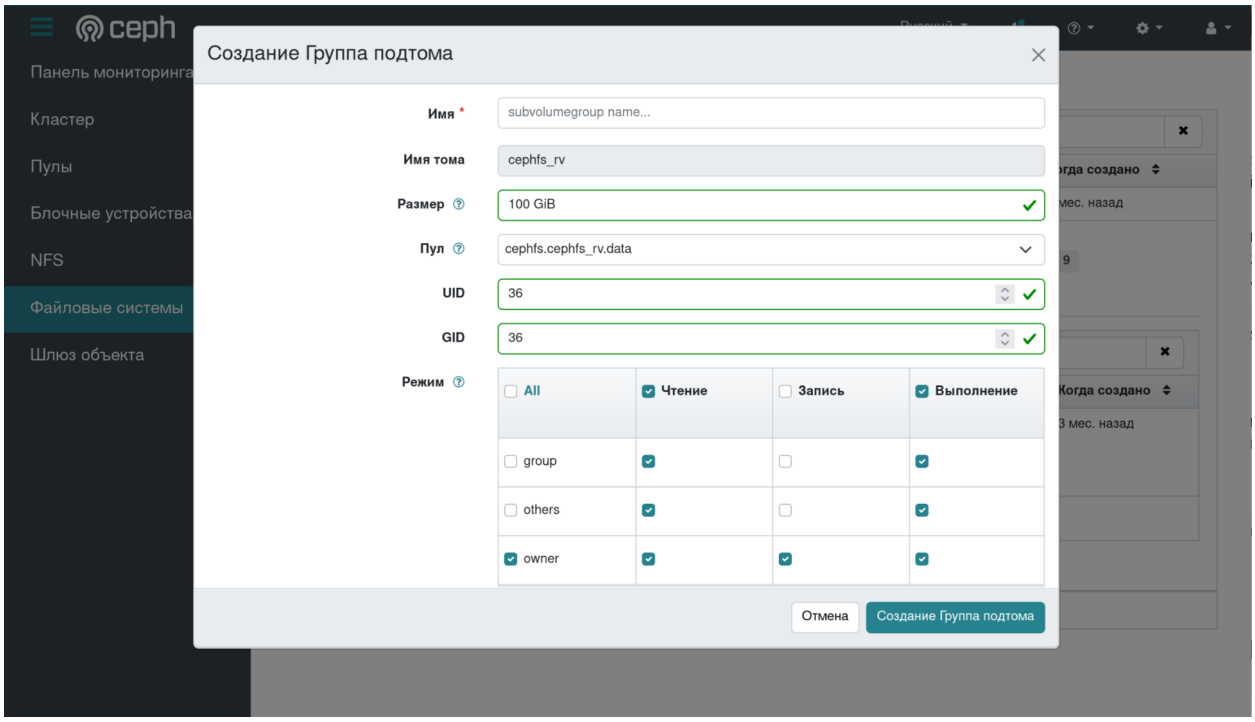


Рисунок 198 – Создание группы подтомов с именем vdsm_kvm

3.6.7.2.4 Создание подтома vmstore

В файловой системе cephfs_rv необходимо создать "Подтом (Subvolume)" с именем vmstore, принадлежащий ранее созданной группе подтомов с именем vdsm_kvm.

Нет необходимости устанавливать какие-либо значения в полях "UID", "GID" или менять права доступа на директорию. Все эти параметры будут унаследованы от группы подтомов с vdsm_kvm.

В верхней части формы "Файловые системы" нужно выбрать файловую систему cephfs_rv и далее дополнительную секцию "Подтома" в нижней части формы, затем нажать на кнопку `+ Создание` для создания группы подтома (рисунок 199).

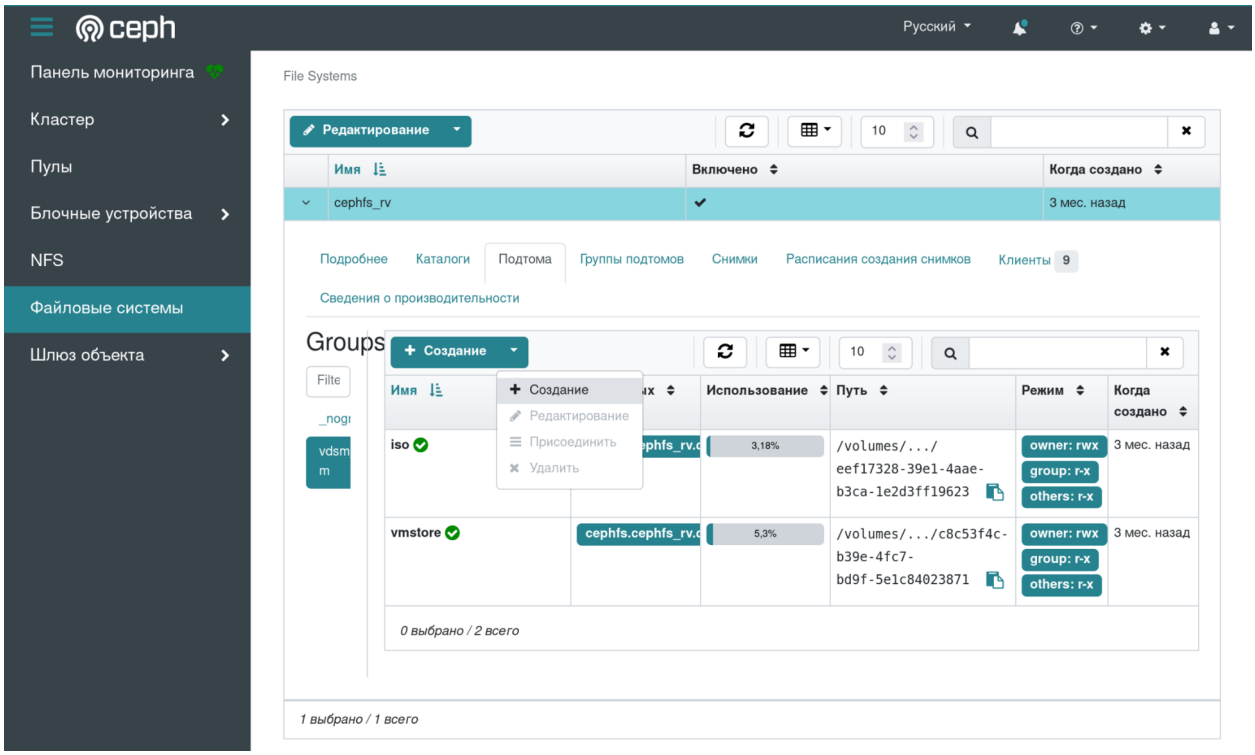


Рисунок 199 – Создание подтома

Затем следует ввести в поле "Имя" имя подтома vmstore и нажать на кнопку Создание подтома для создания подтома с указанным именем (рисунок 200).

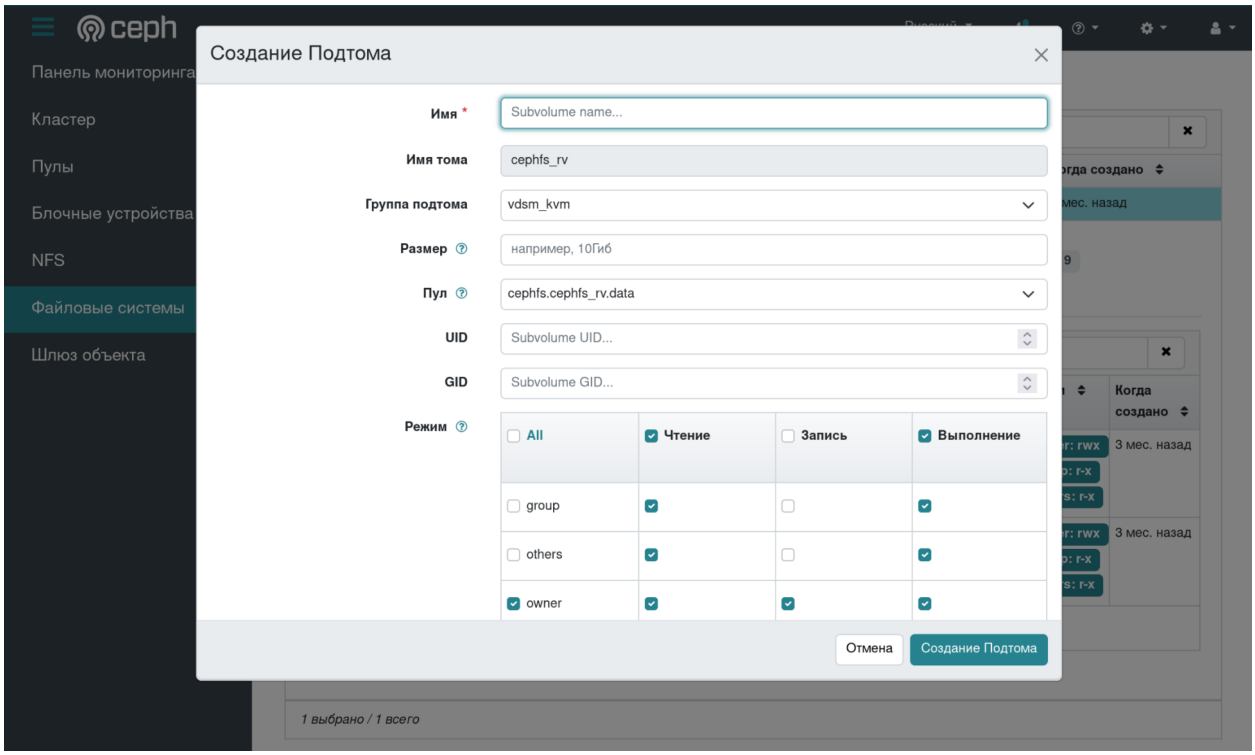


Рисунок 200 – Определение параметров создаваемого подтома

Значение в поле "Путь" ("Path") в дальнейшем понадобится для подключения подтома к РОСА Виртуализация на веб-портале администрирования.

Это значение можно скопировать в буфер обмена, нажав на соответствующую кнопку, как показано на рисунке 201.

Пример – Значение пути к подтому vmstore на рисунке 201:

```
/volumes/vdsm_kvm/vmstore/c8c53f4c-b39e-4fc7-bd9f-5e1c84023871
```

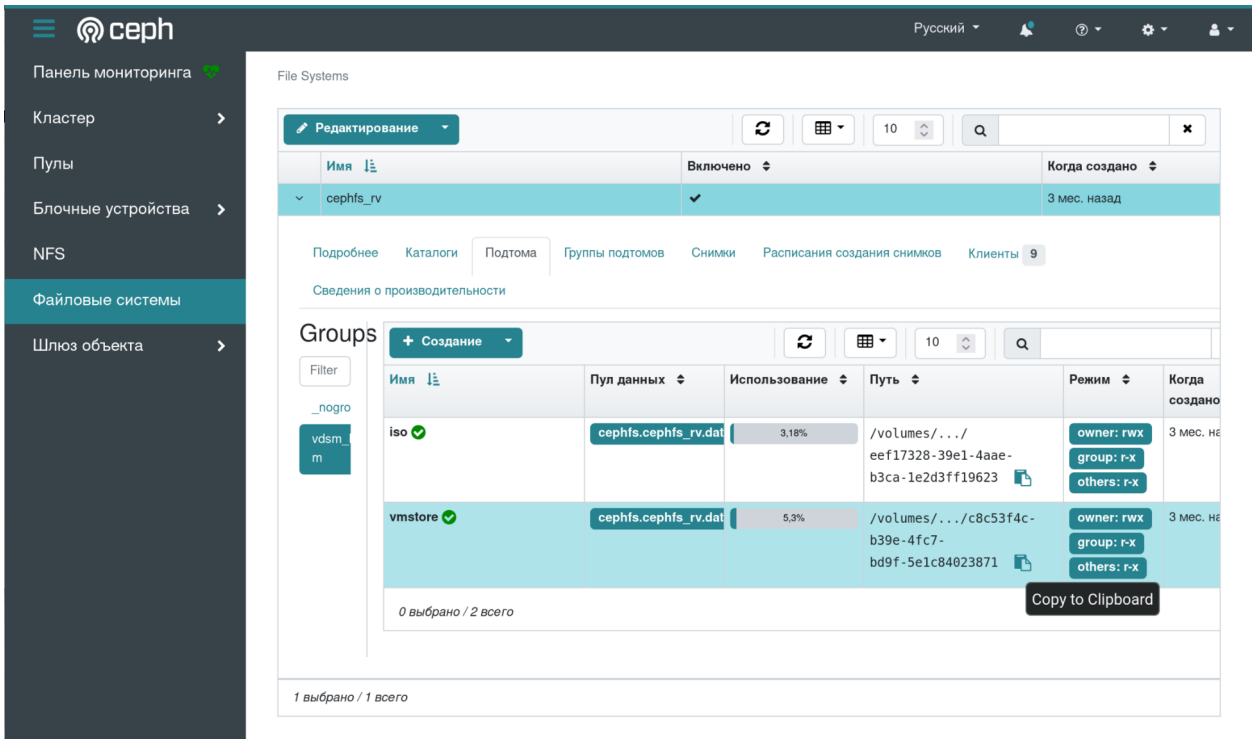


Рисунок 201 – Копирование пути к подтому vmstore в буфер обмена

3.6.7.2.5 Создание пользователя-клиента Ceph

Для создания пользователя-клиента Ceph нужно:

а) выбрать в боковой панели управления секцию "Кластер → Пользователи Ceph", и откроется экранная форма для управления пользователями кластера Ceph (рисунок 202);

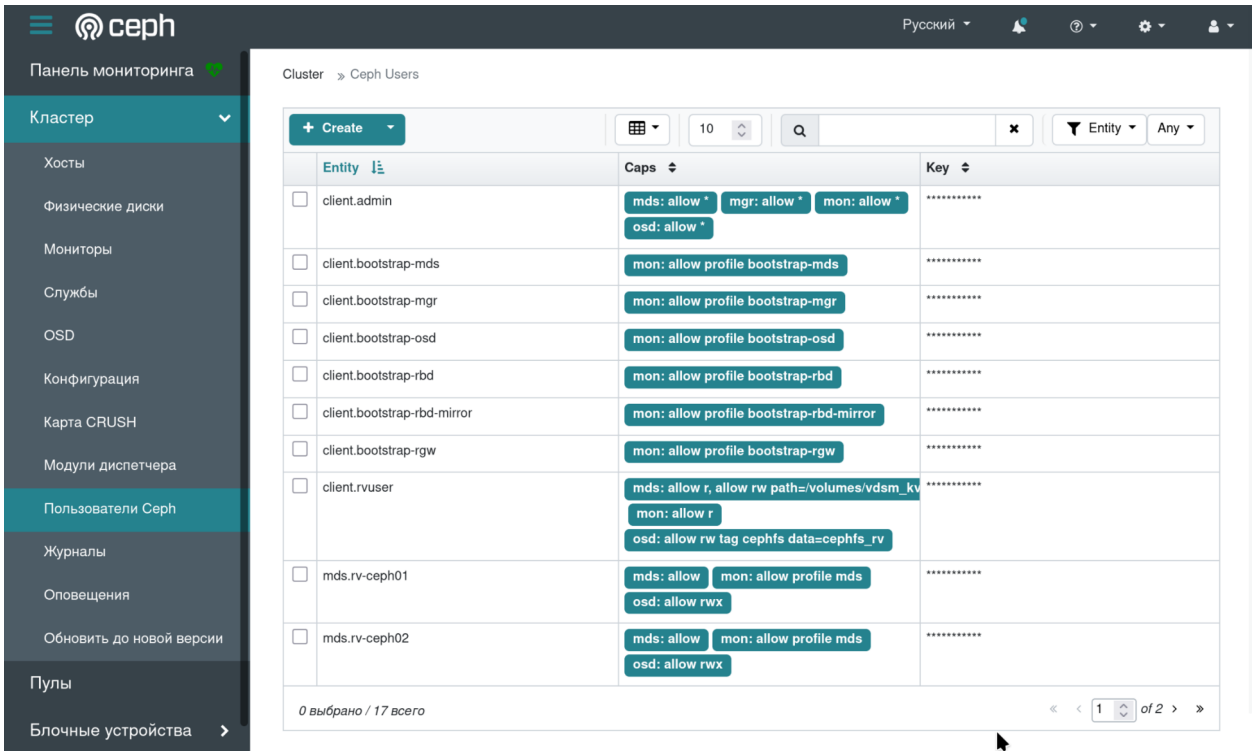


Рисунок 202 – Управление пользователями кластера Ceph

б) создать пользователя client.rvuser с соответствующими правами доступа к ранее созданной файловой системе cephfs_rv и разрешением на чтение/запись метаданных для всех Subvolume в группе vdsm_kvm, для чего нажать на кнопку `+ Create` (рисунок 203), добавить сущности и права доступа, приведенные в таблице 60;

Таблица 60 – Сущности и права сущности для пользователя rvuser

Сущность	Права сущности
mon	allow r, allow rw path=/volumes/vdsm_kvm
mds	allow r
osd	allow rw tag cephfs data=cephfs_rv

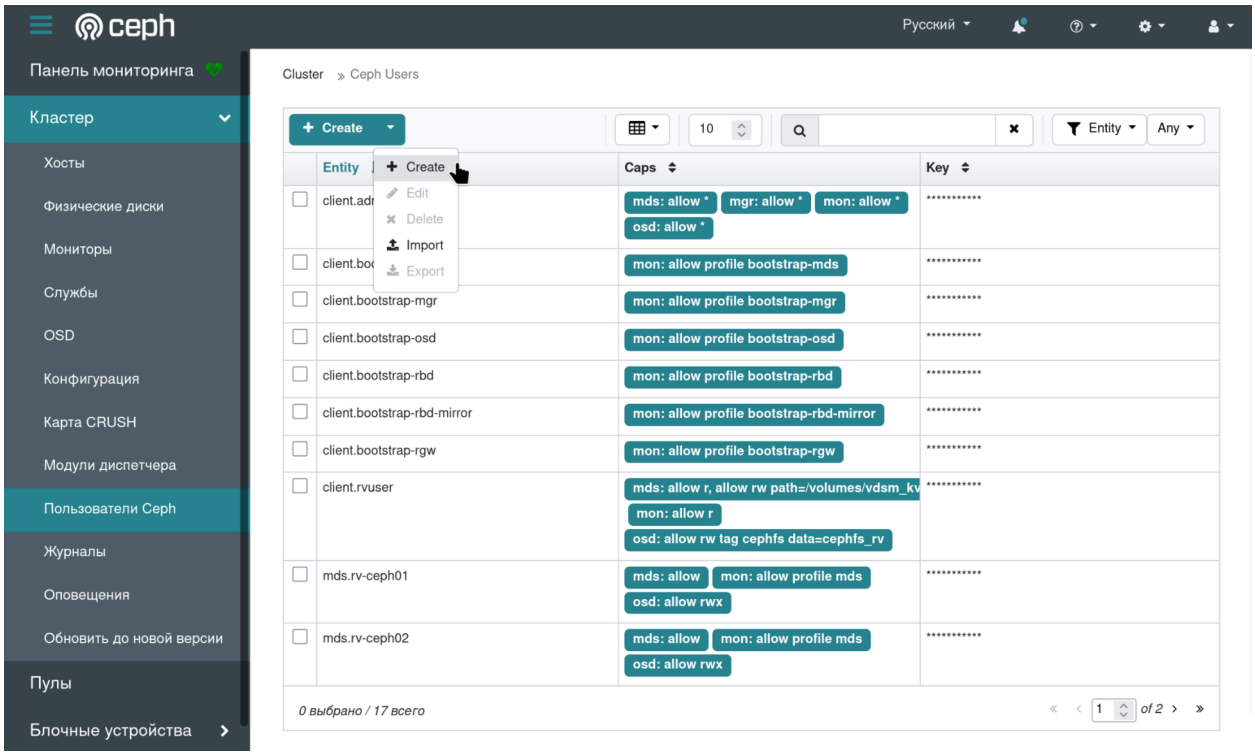


Рисунок 203 – Добавление пользователя в кластер Ceph

в) после завершения ввода данных нажать на кнопку `Create user` (`Создать пользователя`) (рисунок 204).

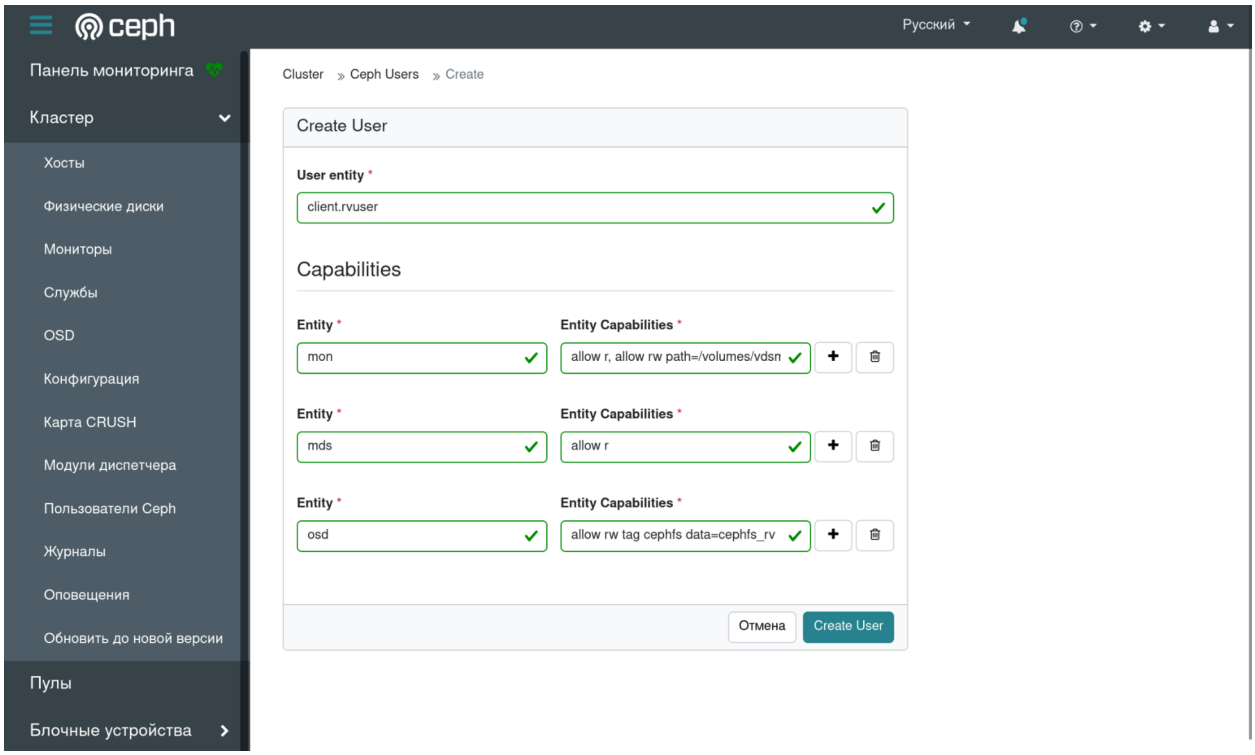


Рисунок 204 – Создание пользователя rvuser с правами доступа к сущностям mon, mds, osd

Пользователь rvuser будет добавлен в кластер Ceph. При необходимости внесения изменения в параметры пользователя можно выбрать пользователя в списке и воспользоваться опцией в меню "Edit" (Редактировать) (рисунок 205).

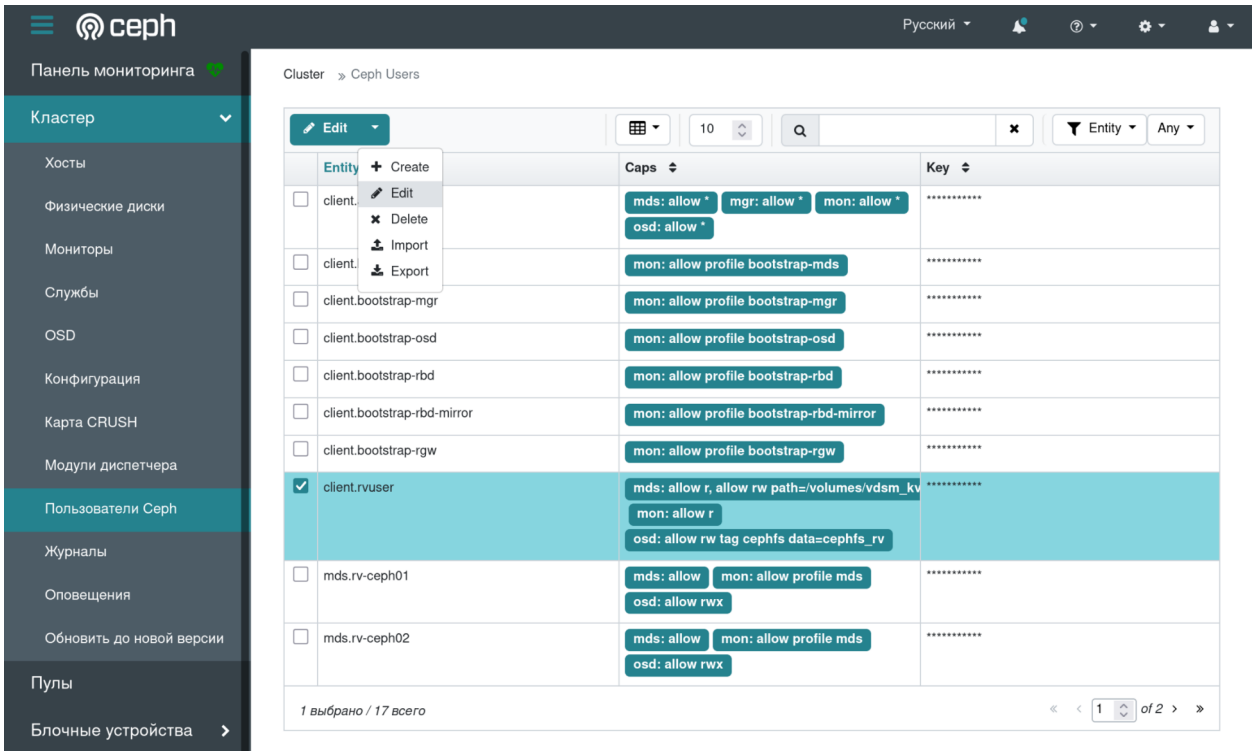


Рисунок 205 – Информация о пользователе rvuser в разделе "Пользователи Ceph"

3.6.7.3 Добавление домена хранилища CephFS в Портале администрирования РОСА Виртуализация

Для добавления домена хранилища CephFS нужно:

а) войти в браузере на Портал администрирования РОСА Виртуализация и выбрать в боковой панели управления пункт меню "Хранилище → Домены"; откроется экранная форма для управления доменами хранилищ "Хранилище → Домены хранилищ";

б) нажать на кнопку Добавить домен для добавление нового домена хранилища, и откроется экранная форма для добавления нового домена;

в) в поле "Тип хранилища" выбрать тип хранилища "CEPH" (рисунок 206);

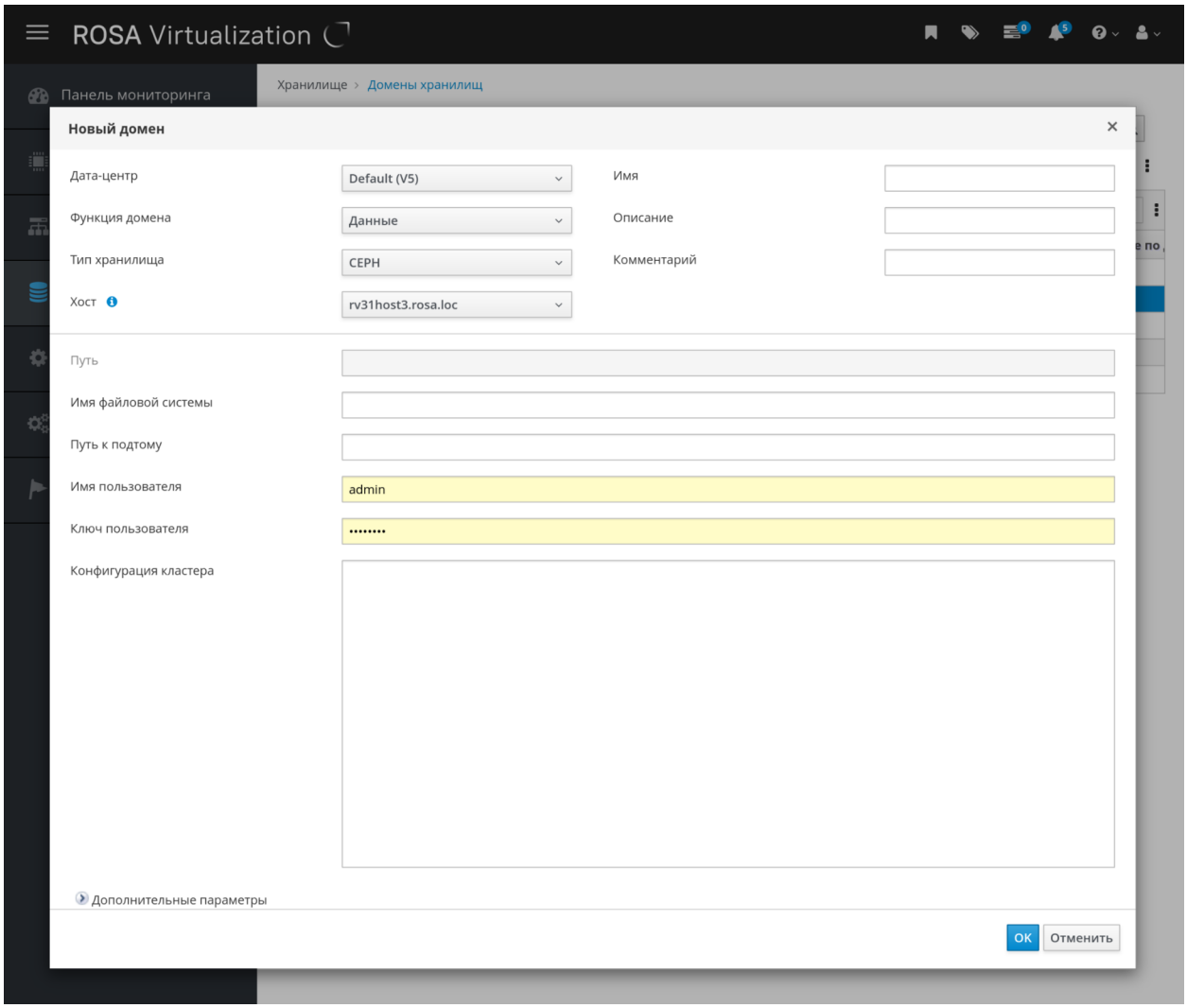


Рисунок 206 – Экранная форма для добавления нового домена

г) настроить параметры добавляемого хранилища (рисунок 207):

1) в поле "Имя" указать имя добавляемого домена, например cephfs_vmstore для домена, предназначенного для хранения данных ВМ;
2) в поле "Описание" указать описание для добавляемого домена;
3) в поле "Комментарий" ввести дополнительный комментарий для добавляемого домена;

Примечание – Описание и комментарий к домену будут отображаться в списке доменов на экранной форме доменами хранилищ "Хранилище → Домены хранилищ".

4) в поле "Имя файловой системы" указать имя добавляемой файловой системы "cephfs_rv", которое было указано в веб-интерфейсе администрирования кластера Ceph при создании файловой системы на вкладке "Файловые системы" (File Systems);

Примечание – При добавлении дополнительных файловых систем CephFS следует указывать в поле "Имя файловой системы" соответствующее имя добавляемой файловой системы.

д) в поле "Путь к подтому" вставить значение из поля "Путь" (Path) для подтома (Subvolume) с именем "vmstore". Значение поля "Путь" можно скопировать в буфер обмена в веб-интерфейсе администрирования кластера Ceph;

е) в поле "Имя пользователя" указать "rvuser" – ту часть сущности пользователя (User entity), которая была указана после точки при создании пользователя client.rvuser в веб-интерфейсе администрирования кластера Ceph;

ж) в поле "Ключ пользователя" вставить значение "key" для пользователя client.rvuser, которое можно получить, выполнив команду в консоли на одном из хостов кластера Ceph:

```
# ceph auth get client.rvuser
```

Пример выполнения команды на одном из хостов кластера Ceph:

```
[root@rv-ceph01 ~]# ceph auth get client.rvuser
[client.rvuser]
        key = AQAdTIpnp5BiEhAAVneGqAVUOaB0LIveqUJ9qQ==
        caps mds = "allow r, allow rw
path=/volumes/vdsm_kvm"
        caps mon = "allow r"
        caps osd = "allow rw tag cephfs data=cephfs_rv"
```

В данном примере значением ключа "key" является: "AQAdTIpnp5BiEhAAVneGqAVUOaB0LIveqUJ9qQ==".

з) в поле "Конфигурация кластера" нет необходимости указывать все содержимое файла ceph.conf. Достаточно указать минимальную конфигурацию, в которой присутствуют поля fsid и mon_host. Этого будет достаточно, чтобы обеспечить отказоустойчивость хранилища при наличии нескольких мониторов в конфигурации кластера Ceph. Минимальную конфигурацию кластера Ceph можно получить можно с помощью консольной команды:

```
# ceph config generate-minimal-conf
```

Параметры конфигурационного файла Ceph:

```
[global]
    fsid = <fsid>
    mon_initial_members = <имя_mon_узла>
    mon_host = <ip_mon_узла>
    public_network = <ip_сеть>
    cluster_network = <ip_сеть>

[mon.<имя_mon_узла>]
    host = <имя_mon_узла>
    mon_addr = <ip_mon_узла>

[osd]
    osd_journal_size = 10000
```

где:

– fsid (File System Identifier) – это уникальный идентификатор кластера Ceph. Он используется для распознавания различных кластеров и обеспечения их целостности. Каждый кластер Ceph должен иметь свой собственный fsid, который генерируется автоматически при инициализации кластера. Этот идентификатор представляет собой UUID (Universally Unique Identifier), и его значение должно быть уникальным для каждого кластера, чтобы избежать конфликтов;

– mon_initial_members – это параметр в конфигурационном файле Ceph, который определяет список начальных мониторов (MON) в кластере Ceph. Этот параметр важен для правильной инициализации кластера и его работы. Значение mon_initial_members представляет собой разделенный запятыми список имен мониторов, которые будут использоваться при первой инициализации кластера. Например:

```
mon_initial_members = mon1, mon2, mon3
```

Имена, указанные в этом списке, должны соответствовать именам, которые назначены вашим мониторам. Эти имена используются для связи между мониторами и для формирования кворума.

Мониторы Ceph работают по принципу кворума, что означает, что для принятия решений необходима доступностьбольшинства (более половины) мониторов. mon_initial_members помогает Системе понять, какие мониторы участвуют в формировании кворума.

– mon_host — это параметр в конфигурации Ceph, который определяет адреса (или имена) мониторов (MON) кластера Ceph. Мониторы отвечают за отслеживание состояния кластера, управление его метаданными и обеспечивают согласованность данных.

Параметр mon_host может содержать один или несколько IP-адресов или доменных имен, разделенных запятыми. Например:

```
[global]
mon_host = 192.168.1.1,192.168.1.2,192.168.1.3
```

В этом примере указаны три адреса мониторов, которые будут использоваться клиентами и другими компонентами Ceph для связи с монитором кластера.

Пример выполнения команды для получения минимальной конфигурации кластера Ceph:

```
[root@rv-ceph01 ~]# ceph config generate-minimal-conf
# minimal ceph.conf for 2525fc77-cff1-4455-9c25-1887e8a850f8
[global]
        fsid = 2525fc77-cff1-4455-9c25-1887e8a850f8
        mon_host =
[v2:192.168.11.181:3300/0,v1:192.168.11.181:6789/0]
[v2:192.168.11.182:3300/0,v1:192.168.11.182:6789/0]
[v2:192.168.11.183:3300/0,v1:192.168.11.183:6789/0]
```

Команда выводит минимальный конфигурационный файл для кластера Ceph на стандартный вывод (stdout) терминала. Файл не сохраняется автоматически в каком-либо месте.

Если требуется сохранить его в файл (например, ceph-minimal.conf), можно перенаправить вывод команды в файл:

```
# ceph config generate-minimal-conf > ceph-minimal.conf
```

Примечание – Вывод данной команды будет сохранен в текущем фолдере.

Для просмотра содержимого сгенерированного минимального конфигурационного файла можно использовать команду `cat`:

```
[root@rv-ceph01 ~]# cat ceph-minimal.conf
# minimal ceph.conf for 2525fc77-cff1-4455-9c25-1887e8a850f8
[global]
        fsid = 2525fc77-cff1-4455-9c25-1887e8a850f8
        mon_host =
[v2:192.168.11.181:3300/0,v1:192.168.11.181:6789/0]
[v2:192.168.11.182:3300/0,v1:192.168.11.182:6789/0]
[v2:192.168.11.183:3300/0,v1:192.168.11.183:6789/0]
```

и) нажать кнопку `OK` для добавления нового домена хранилища Ceph в РОСА Виртуализация (рисунок 207).

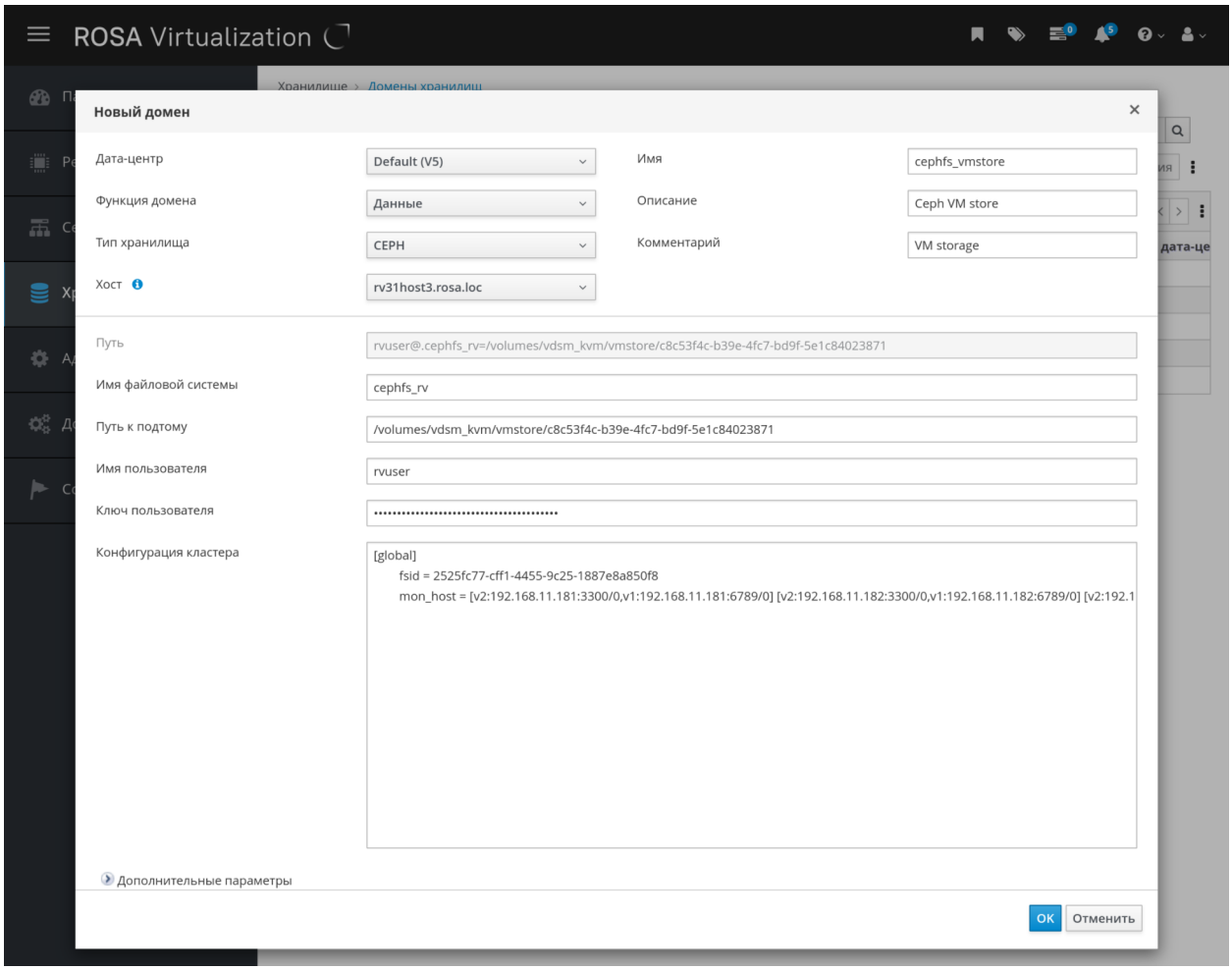


Рисунок 207 – Добавления нового домена Ceph с именем cephfs_vmstore

Домен с именем cepfs_vmstore был добавлен в РОСА Виртуализация и отображается в списке доступных доменов хранилищ (рисунок 208).

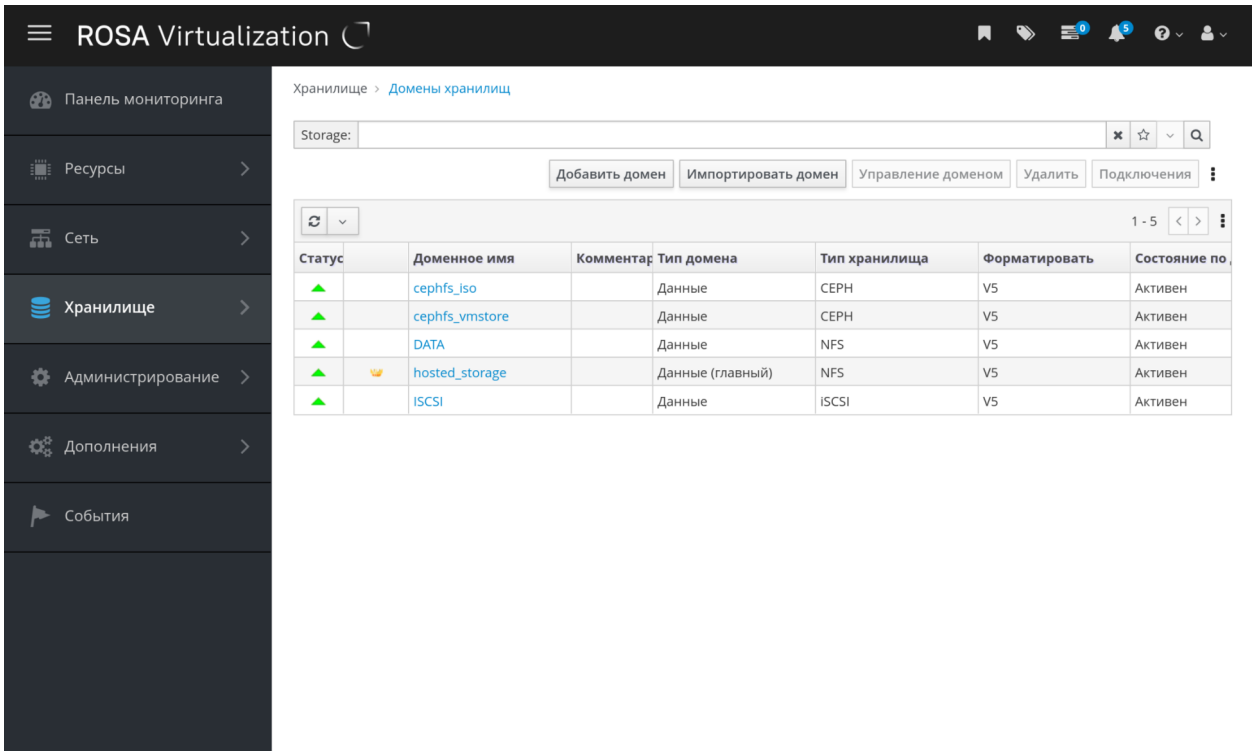


Рисунок 208 – Домены хранилищ РОСА Виртуализация

Следует повторить операцию по добавлению домена для домена cepfs_iso, предназначенного для хранения ISO-дисков.

Подключение отказоустойчивого хранилища CephFS к РОСА Виртуализация завершено, и подключенные хранилища можно использовать.

3.7 Пулы

3.7.1 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 и соответственно не сохраняются изменения в данных и конфигурации ВМ после перезагрузки. Тем не менее можно создать конфигурацию пула с фиксацией состояния, то есть с сохранением изменений, внесенных 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 заберет пользователь. Такая настройка дает пользователям возможность немедленно начать работу с машиной, но такие ВМ потребляют системные ресурсы не только во время работы, но и во время простоя.

3.7.1.1 Инфраструктура виртуальных рабочих столов (VDI)

Предоставление инфраструктуры VDI означает возможность использования стандартизированного рабочего стола (требуемую версию операционной системы и набор корпоративных приложений). Это гарантирует, что все пользователи будут иметь одинаковый пользовательский опыт.

Для развертывания решения VDI необходимо иметь кластер виртуализации с внешним механизмом аутентификации, таким как Active Directory, корпоративный каталог с использованием FreeIPA или аналогичный. Также необходимо подготовить шаблон виртуальной машины с операционной системой для настольного компьютера, используемой в компании, сконфигурированной в соответствии с корпоративным стандартом и потребностями пользователей (электронная почта, корпоративные приложения, программное обеспечение для обеспечения безопасности и т.д.). Подготовка шаблона ВМ осуществляется администратором.

С помощью РОСА Виртуализация создается пул виртуальных машин, используя шаблон ВМ для рабочего стола и определяя общее количество копий ВМ, которые можно запустить в кластере. Эти ВМ могут быть динамически выделены и удалены, то есть при выключении ВМ содержимое диска ВМ и локальные данные удаляются или они могут быть сконфигурированы как ВМ, сохраняющие пользовательские данные и настройки внутри виртуальной машины до тех пор, пока этот экземпляр не будет удален.

3.7.1.2 Вход пользователя в Портал ВМ

Когда пользователь входит в Портал ВМ, используя свой корпоративный профиль (логин/пароль, используемые для входа на корпоративные ресурсы), и запускает (забирает) виртуальную машину из пула, экземпляр ВМ на основе шаблона будет выделен этому пользователю и может быть запущен в любое время, когда пользователю это понадобится.

Работа пользователя с пулом виртуальных машин (удаленный рабочий стол, VDI) описана в документе "РОСА Виртуализация 4. Руководство пользователя. Портал виртуальных машин" (РСЮК.10103-01 34 01).

3.7.2 Создание пула виртуальных машин (VDI)

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.

3.7.2.1 Параметры конфигурационного файла sysprep для ВМ под управлением ОС Windows

Если пулу не нужно присоединяться к домену, нужно использовать 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:

а) скопировать разделы, имеющие отношение к каждой ОС Windows, из /usr/share/ovirt-engine/conf/osinfo-defaults.properties в новый файл и сохранить его как 99-defaults.properties;

б) в файле 99-defaults.properties указать ключ активации ОС Windows и путь до частного файла sysprep:

```
    os.operating_system.productKey.value=Windows_product_activat
ion_key
    ...
    os.operating_system.sysprepPath.value =
${ENGINE_USR}/conf/sysprep/ sysprep.operating_system
```

в) создать новый файл sysprep, где указать 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.

3.7.2.2 Создание пула ВМ

Для создания пула ВМ нужно выполнить следующие действия:

а) нажать "Ресурсы → Пулы";

б) нажать кнопку Добавить, чтобы открыть окно "Новый пул" (рисунок 209);

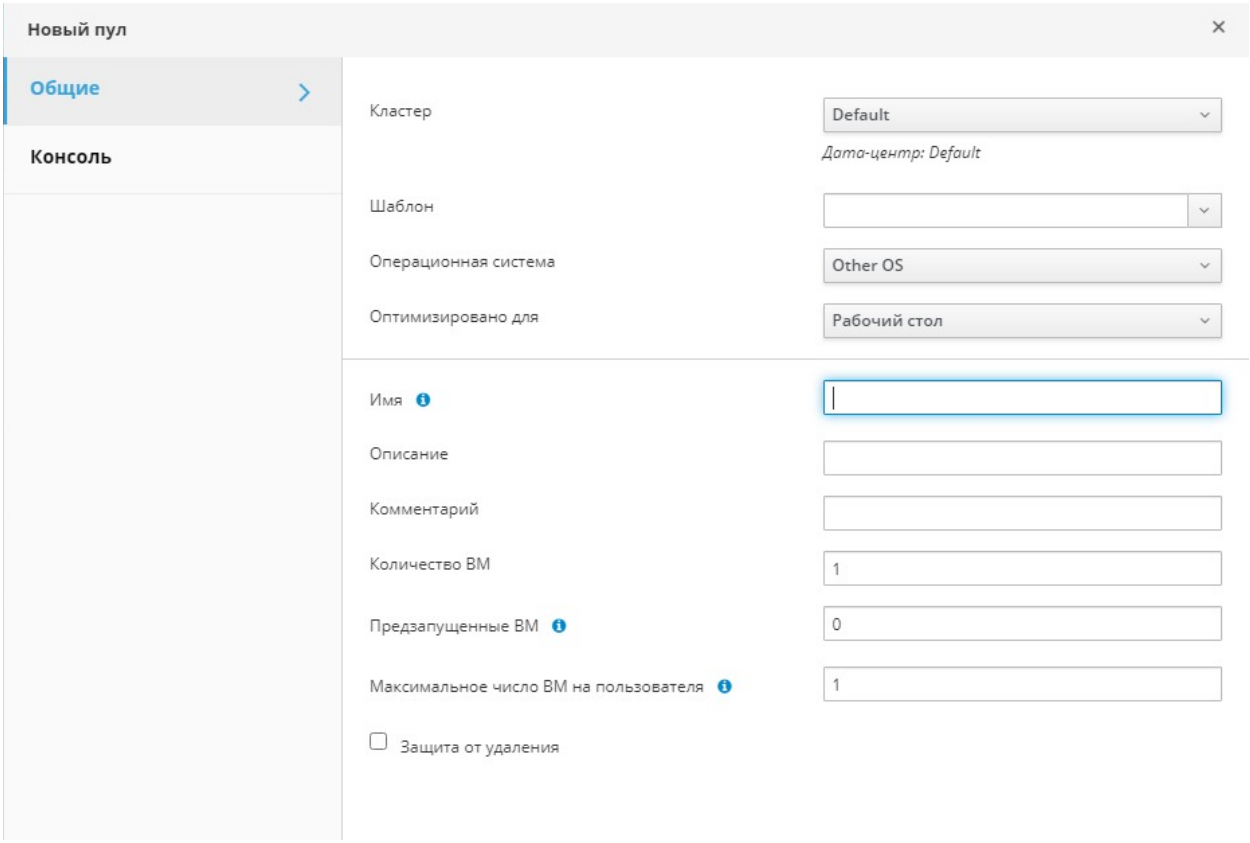


Рисунок 209 – Создание пула ВМ

в) из выпадающего списка выбрать "Кластер";

г) из выпадающего списка выбрать "Шаблон" и версию. Шаблон предоставляет стандартные значения параметров для всех ВМ в пуле (рисунок 210);

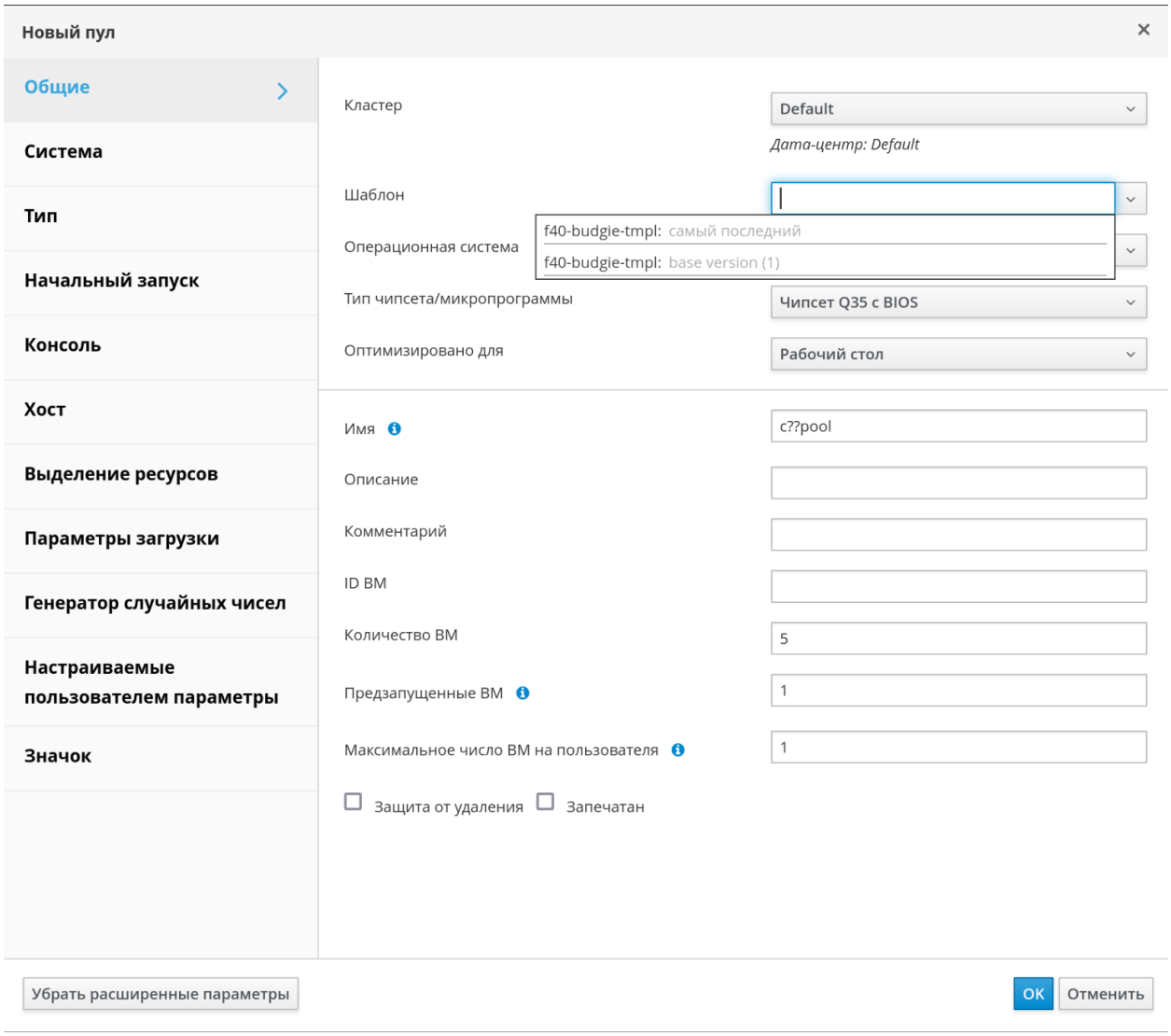


Рисунок 210 – Выбор шаблона ВМ и версии шаблона ВМ для создания пула

Примечание – Если в Системе отсутствует предварительно созданный шаблон, то его необходимо создать. Это можно сделать в секции "Ресурсы → Шаблоны".

д) из выпадающего списка выбрать "Операционную систему";

е) из выпадающего списка выбрать "Тип чипсета/микропрограмму";

ж) используя значения из выпадающего списка "Оптимизировано для", оптимизировать 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.

з) указать "Имя" и опционально "Описание" и "Комментарий" для пула;

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"). Нумерацию ВМ можно нстроить с использованием символа "?" (вопросительный знак) в качестве метки-заполнителя (например, имени пула "MyPool-???" соответствует следующая нумерация виртуальных машин: "MyPool-001", "MyPool-002", ..., "MyPool-010").

и) указать "Количество ВМ" для пула;

к) указать количество ВМ с предварительным запуском в поле "Предзапущенные ВМ";

л) указать "Максимальное число ВМ на пользователя", которое разрешено запускать одному пользователю в течение сеанса. Минимальное значение — "1" (одна виртуальная машина на одного пользователя);

м) опционально установить флажок "Защита от удаления";

н) если создается пул ВМ не под управлением ОС Windows или используется исходный файл sysprep, то перейти к следующему шагу (п. 3.7.2.3).

3.7.2.3 Создание частного файла sysprep для пула ВМ

В случае создания частного файла sysprep для пула ВМ под управлением ОС Windows необходимо выполнить следующие действия:

а) нажать на кнопку Показать дополнительные параметры;

б) перейти на вкладку "Начальный запуск" и установить флажок "Cloud-Init/Sysprep";

в) нажать "Аутентификация" и ввести "Имя пользователя" и "Пароль" или выбрать "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.

г) нажать "Настраиваемый пользователем сценарий" и вставить в текстовый блок содержимое исходного файла sysprep, расположенного по пути /usr/share/ovirt-engine/conf/sysprep/;

д) при необходимости изменить значения следующих параметров конфигурационного файла sysprep (следует обратить внимание, что значения этих параметров нельзя изменить во вкладке "Начальный запуск"):

– Key (ключ активации). Если предварительно настроенный ключ активации ОС Windows не будет использоваться, то заменить <![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>
```

к) при необходимости значения других параметров конфигурационного файла sysprep заполнить во вкладке "Начальный запуск";

е) опционально указать "Тип пула":

1) перейти на вкладку "Тип" и выбрать "Тип пула":

– Вручную – возвращение ВМ в пул осуществляется вручную администратором;

– Автоматически – возвращение ВМ в пул осуществляется автоматически;

2) установить флажок "Пул с сохранением состояния", чтобы ВМ запускались в режиме с сохранением состояния. Это обеспечивает сохранение в ВМ изменений, внесенных предыдущим пользователем;

3) нажать кнопку OK;

ж) при необходимости переопределить прокси SPICE:

1) во вкладке "Консоль" установить флажок "Переопределить SPICE прокси";

2) в поле "Переназначенный адрес прокси SPICE" указать адрес прокси SPICE, который заменит глобальный прокси;

3) нажать кнопку OK;

з) если пул состоит из ВМ под управлением ОС Windows, то нажать "Ресурсы → Виртуальные машины", далее выбрать каждую ВМ и нажать "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:

а) проверить, не присоединено ли к ВМ под управлением ОС Windows устройство флоппи-дискеты с файлом Unattend (например, A:\Unattend.xml);

б) в панели задач ОС Windows нажать "Пуск", затем "Выполнить", далее в текстовый блок "Открыть" ввести "regedit" и нажать кнопку OK;

в) в левой панели реестра выбрать пункт меню "HKEY_LOCAL_MACHINE → SYSTEM → Setup";

г) нажать правой кнопкой мыши в правой панели реестра и из контекстного меню выбрать "Создать → Строковой параметр";

д) указать имя ключа "UnattendFile";

е) дважды нажать левой кнопкой мыши по новому ключу и в качестве значения ключа ввести имя файла Unattend и путь к этому файлу (например, A:\Unattend.xml);

ж) сохранить изменения в реестре, сохранить состояние ВМ и создать новый шаблон.

В результате будет создан пул виртуальных машин с указанным числом одинаковых ВМ.

Для просмотра ВМ из пула можно использовать меню "Ресурсы → Виртуальные машины" или нажать на имя пула, чтобы перейти к подробному просмотру (при отображении виртуальные машины из пула отличаются от независимых ВМ своим значком).

3.7.3 Параметры и элементы управления пулами

3.7.3.1 Общие параметры в окнах "Новый пул" и "Параметры пула"

В таблице 61 описываются параметры пула во вкладке "Общие" окон "Новый пул" и "Параметры пула".

Все другие параметры идентичны параметрам окна "Новая ВМ".

Таблица 61 – 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 дает возможность указать число тех ВМ в пуле, которые будут предварительно запущены перед размещением в пуле и будут забираться пользователями уже работающими.

Поле	Описание
	Значение параметра должно быть от "0" до общего числа ВМ в пуле
Количество ВМ / Увеличить число ВМ в пуле на	Параметр дает возможность указать конкретное количество ВМ, которые нужно создать и сделать доступными в пуле. 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 дает 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

3.7.3.2 Параметры вкладки "Тип" в окнах "Новый пул" и "Изменить пул"

В таблице 62 описываются параметры пула во вкладке "Тип" окон "Новый пул" и "Изменить пул".

Таблица 62 – 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, внесенные предыдущим пользователем, сохранятся в ВМ

3.7.3.3 Параметры вкладки "Консоль" в окнах "Новый пул" и "Изменить пул"

В таблице 63 описываются параметры пула во вкладке "Консоль" окон "Новый пул" и "Изменить пул".

Все другие параметры идентичны параметрам окна "Новая ВМ" и "Параметры виртуальной машины".

Таблица 63 – Параметры консоли

Поле	Описание
Переназначить SPICE прокси	Установить флажок для этого пункта, чтобы включить переопределение прокси SPICE, указанного в глобальной конфигурации. Эту возможность используют, 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

3.7.3.4 Параметры вкладки "Хост" в окнах "Новый пул" и "Параметры пула"

В таблице 64 описываются параметры пула во вкладке Хост окон "Новый пул" и "Параметры пула".

Таблица 64 – Параметры хоста

Поле	Вложенный элемент	Описание
Начать выполнение на:		Параметр позволяет указать предпочитаемый хост, на котором должна выполняться ВМ.

Поле	Вложенный элемент	Описание
		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. Выбрать 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	По умолчанию политика миграции

Поле	Вложенный элемент	Описание
	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 включен. – В случае необходимости приостановить рабочую нагрузку. Разрешается миграция ВМ в большинстве ситуаций, включая испытывающие серьезную нагрузку ВМ. В связи с этим разрешается более значительный простой ВМ, чем при других значениях данного параметра. Миграция все еще может быть прервана при экстремальных нагрузках. Механизм перехватчиков событий гостевого агента включен
	Включить шифрование при миграции	Параметр дает 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.

Поле	Вложенный элемент	Описание
		– 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 дает 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 счетчика 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 объем памяти недоступен, память можно выделить из других узлов. – Чередование. Память выделяется из всех узлов в

Поле	Вложенный элемент	Описание
		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. Для привязки виртуальных узлов NUMA для размещения узлов NUMA нажать и переместить 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"

3.7.3.5 Параметры вкладки "Выделение ресурсов"

В таблице 65 описываются параметры пула во вкладке "Выделение ресурсов" окон "Новый пул" и "Изменить пул".

Все другие параметры идентичны параметрам окна "Новая ВМ".

Таблица 65 – Параметры выделения ресурсов

Поле	Вложенный элемент	Описание
Выделение дисковых ресурсов	Автоматический выбор цели	Установить этот флажок, чтобы домен хранилища с наибольшим объемом 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

Поле	Вложенный элемент	Описание
		случаях будет формат raw

3.7.4 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.

Для изменения параметров пула ВМ нужно:

а) нажать "Ресурсы → Пулы" и выбрать пул ВМ;
б) нажать кнопку Изменить;
в) изменить свойства пула ВМ;
г) нажать кнопку OK.

3.7.5 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 ждет 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.

Примечание — Максимальное число предварительно запущенных ВМ равно числу ВМ в пуле.

Для предварительного запуска ВМ в пуле нужно:

а) нажать "Ресурсы → Пулы" и выбрать пул ВМ;

б) нажать кнопку Изменить;

в) в поле "Предзапущенные ВМ" указать число ВМ, которые необходимо предварительно запустить;

г) перейти на вкладку "Тип" и убедиться в том, что значение "Тип пула" указано как "Автоматически";

д) нажать кнопку ОК.

3.7.6 Добавление виртуальных машин в пул ВМ

Для добавления виртуальных машин в пул ВМ необходимо:

а) нажать "Ресурсы → Пулы" и выбрать пул ВМ;

б) нажать кнопку Изменить;

в) в поле "Увеличить число ВМ в пуле на ..." указать число дополнительных ВМ (рисунок 211);

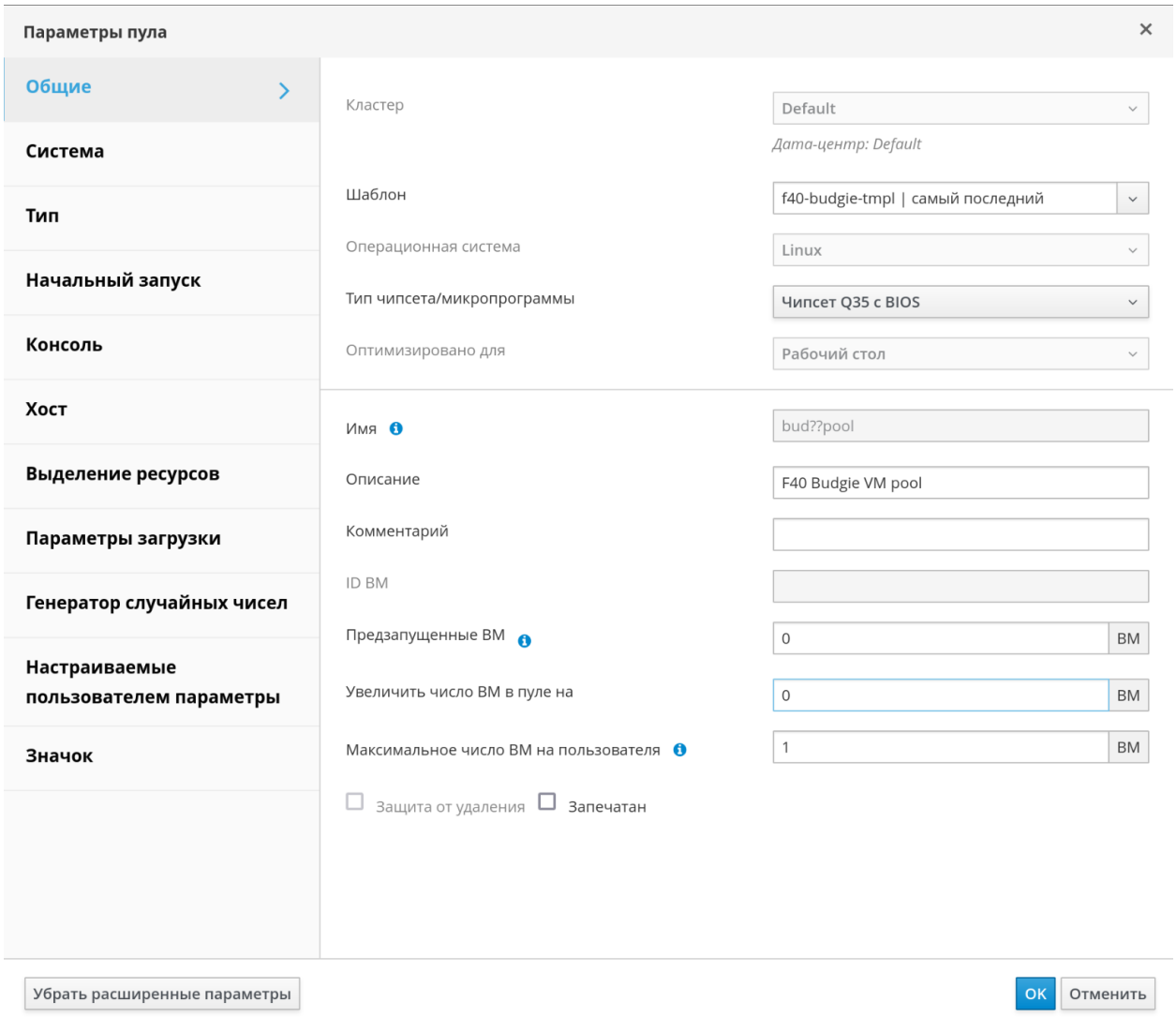


Рисунок 211 – Добавление виртуальных машин в пул ВМ

г) нажать кнопку OK.

3.7.7 Откреплeние виртуальных машин от пула ВМ

Виртуальные машины можно откреплять от пула ВМ. Откреплeние машины удаляет ВМ из пула, и машина становится независимой ВМ.

Для откреплeния виртуальных машин от пула ВМ нужно:

а) нажать "Ресурсы → Пулы";
б) нажать на имя пула, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Виртуальные машины", чтобы просмотреть список ВМ в пуле;

г) убедиться в том, что машина имеет статус "Не запущена", так как работающую ВМ открепить нельзя;

д) выбрать одну или несколько ВМ и нажать кнопку Отсоединить (рисунок 212);

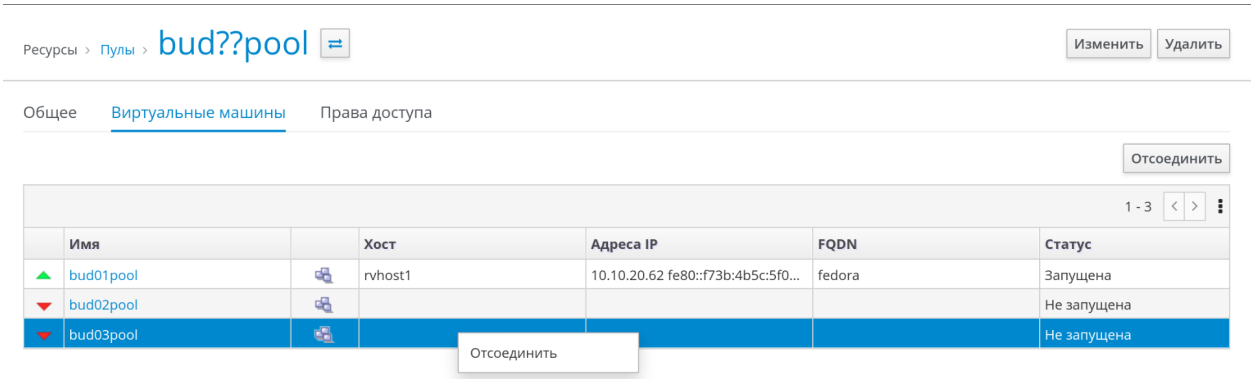


Рисунок 212 – Открепление виртуальных машин от пула ВМ

е) нажать кнопку ОК.

Примечание — Откреплённая виртуальная машина по-прежнему существует в окружении, и к такой ВМ можно получить доступ из меню "Ресурсы → Виртуальные машины". Следует обратить внимание, что значок ВМ изменится для обозначения того, что откреплённая от пула ВМ машина стала независимой.

3.7.8 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.

Для удаления пула ВМ нужно:

а) нажать "Ресурсы → Пулы" и выбрать пул ВМ;

б) нажать кнопку Удалить (рисунок 213);

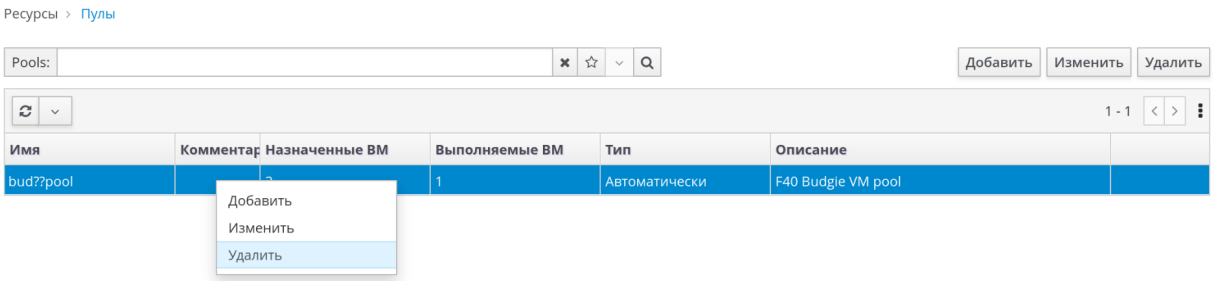


Рисунок 213 – Удаление пула ВМ

в) нажать кнопку ОК.

3.8 Виртуальные диски

3.8.1 Хранилище виртуальной машины

Система виртуализации POCA Виртуализация 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 жесткого диска ВМ.

По умолчанию в дата-центрах на базе NFS, локальных или совместимых с POSIX, хост SPM создает 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 создает 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) создается логический том указанного размера в ГБ.

Для виртуального диска тонкого резервирования создается логический том с начальным размером в 1 ГБ. За логическим томом ведется постоянное наблюдение со стороны хоста, на котором выполняется ВМ. Как только используемый объем приближается к пороговому значению, хост оповещает SPM, и SPM увеличивает размер логического тома еще на 1 ГБ. 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 объемом более 1 ГБ каждые четыре секунды, всегда при возможности использовать предварительно зарезервированные диски в формате raw.

3.8.2 Виртуальные диски

Система виртуализации РОСА Виртуализация предлагает следующие возможности для выделения свободного дискового пространства в хранилище:

– **Предварительное резервирование** – Предварительно зарезервированный виртуальный диск заранее резервирует все выделенное место в хранилище, предназначенное для виртуальной машины. Таким образом, предварительно зарезервированный логический том размером в 20 ГБ, созданный для раздела размещения данных ВМ, займет все 20 ГБ свободного места в хранилище сразу после своего создания.

– **Тонкое резервирование разреженного типа** – Тонкое резервирование разреженного типа дает возможность администратору определить общий объем

места в хранилище, выделяемого виртуальной машине, но это место выделяется только при необходимости. Логический том тонкого резервирования размером в 20 ГБ займет при создании 0 ГБ. После установки операционной системы размер диска будет равен размеру установленных файлов и будет увеличиваться до максимального размера в 20 ГБ по мере добавления данных.

ID (идентификатор) виртуального диска можно просмотреть в меню "Хранилище → Диски". Этот идентификатор служит для обозначения виртуального диска, поскольку название устройства (например, /dev/vda0) может поменяться, что приведет, в свою очередь, к повреждению диска. Также просмотреть ID виртуального диска можно в /dev/disk/by-id.

"Виртуальный размер" диска можно просмотреть в меню "Хранилище → Диски" и на вкладке "Диски" области подробного просмотра для доменов хранилищ, ВМ и шаблонов. Виртуальный размер — это общий объем дискового пространства, который может использовать ВМ. Таким образом, это число, которое администратор указывает в поле "Размер (ГБ)" при создании или изменении параметров виртуального диска.

"Фактический размер" диска можно просмотреть на вкладке "Диски" области подробного просмотра доменов хранилищ и шаблонов. Фактический размер — это объем дискового пространства, выделенный виртуальной машине на текущий момент. Предварительно зарезервированные диски показывают одинаковое значение как для "Виртуального размера", так и для "Фактического размера". "Диски" разреженного 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 РОСА Виртуализация.

В таблице 66 описываются возможные сочетания форматов и типов, разрешенные для хранилищ в РОСА Виртуализация.

Таблица 66 – Сочетания форматов и типов, разрешенные для хранилищ

Хранилище	Формат	Тип	Примечание
NFS	raw	Предварительное резервирование	Файл без форматирования, начальный размер которого равен объему, определенному

Хранилище	Формат	Тип	Примечание
			для виртуального диска
NFS	raw	Разреженный	Файл без форматирования, начальный размер которого близок к нулю
NFS	QCOW2	Разреженный	Файл в формате QCOW2, начальный размер которого близок к нулю
SAN	raw	Предварительное резервирование	Блочное устройство без форматирования, начальный размер которого равен объему хранилища, выделенного для виртуального диска
SAN	QCOW2	Разреженный	Блочное устройство, начальный размер которого намного меньше, чем размер, определенный для виртуального диска (на данный момент — 1 ГБ). Выделяемое по мере необходимости пространство форматируется как QCOW2 (на данный момент шаг выделения — 1 ГБ)

3.8.3 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 стерты. 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 защищенного удаления и не дает 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.

Для установки значения по умолчанию "true" для параметра SANWipeAfterDelete с помощью утилиты настройки виртуализированного ЦУ нужно:

а) запустить утилиту engine-config с опцией "--set" и указанным значением "true" для параметра "SANWipeAfterDelete":

```
# engine-config --set SANWipeAfterDelete=true
```

б) перезапустить 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 запись следующего вида:

```
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 запись вида:

```
    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
```

3.8.4 Разделяемые диски

Некоторым приложениям необходимо, чтобы хранилище было общим хранилищем серверов. Система виртуализации РОСА Виртуализация дает возможность пометить жесткие 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, скорее 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.

Флажок "Может быть общим" для диска возможно установить либо во время его создания, либо во время изменения параметров диска.

3.8.5 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, присоединенного 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).

3.8.6 Работа с виртуальными дисками

3.8.6.1 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 РОСА Виртуализация с помощью окна "Внешние поставщики".

Для создания виртуального диска, присоединенного к конкретной ВМ, нужно выполнить следующие действия:

а) нажать "Ресурсы → Виртуальные машины";
б) нажать на имя ВМ, чтобы перейти к подробному просмотру;
в) перейти на вкладку "Диски";
г) нажать кнопку Добавить;

д) перейти на соответствующую вкладку, чтобы создать виртуальный диск с типом "Образ", виртуальный диск с "Прямыми LUN" или виртуальный диск "Cinder" (рисунок 214);

е) выбрать параметры, требуемые для виртуального диска. Параметры изменяются в зависимости от выбранного типа диска;

ж) нажать кнопку OK.

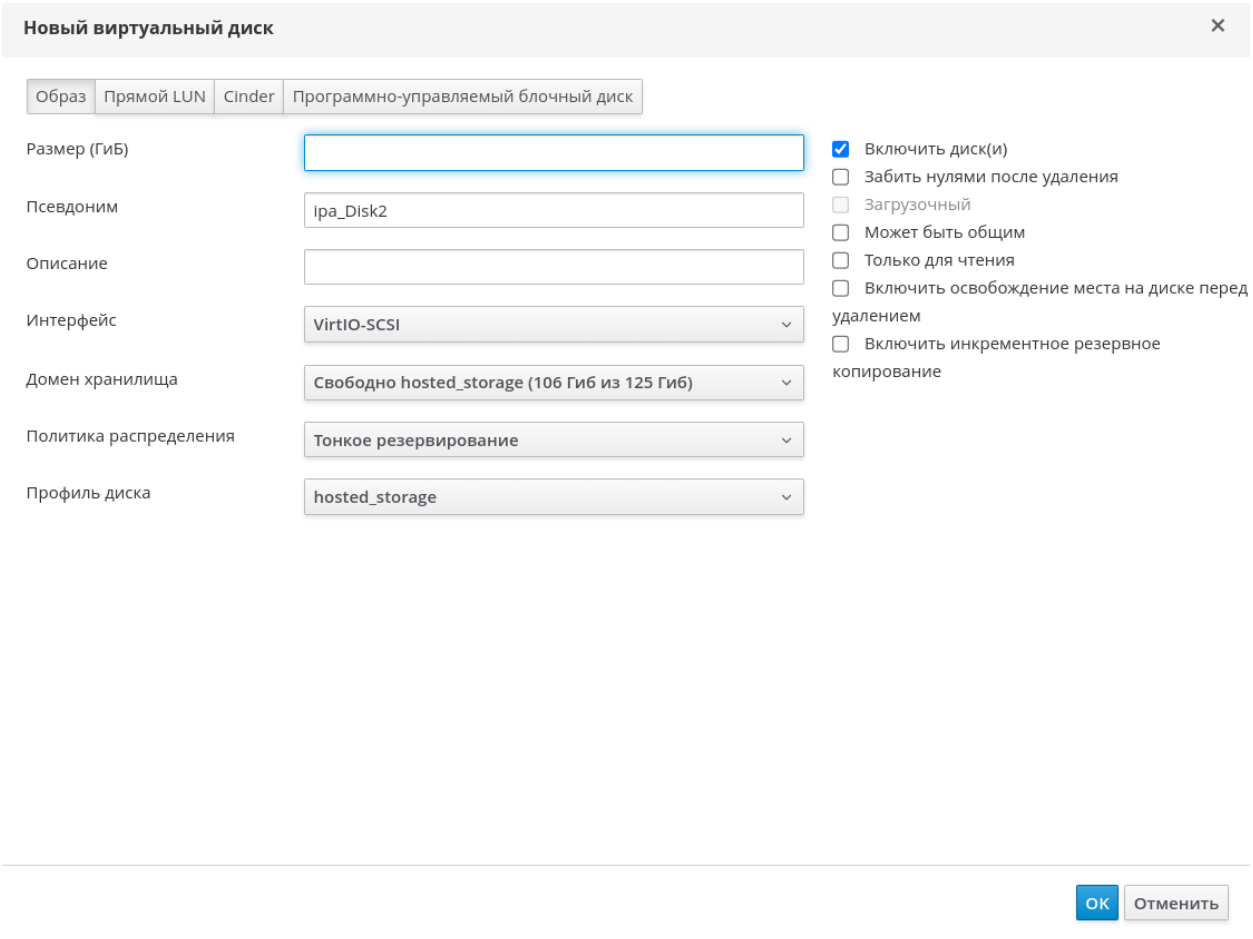


Рисунок 214 – Создание нового виртуального диска

3.8.6.1.1 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. 3.8.6.2).

Для создания "плавающего" виртуального диска нужно:

а) нажать "Хранилище → Диски";

б) нажать кнопку Добавить;

в) нажать на соответствующую кнопку, чтобы указать, будет ли виртуальный диск "Образом", "Прямым LUN" или "Cinder";

г) выбрать параметры, требуемые для виртуального диска. Параметры изменяются в зависимости от выбранного типа диска;

д) нажать кнопку OK.

3.8.6.2 Параметры виртуального диска

3.8.6.2.1 Параметры образа виртуального диска

В таблице 67 описываются параметры образа виртуального диска в окнах "Новый виртуальный диск" и "Параметры виртуального диска".

Таблица 67 – Параметры образа виртуального диска

Поле	Описание
Размер (ГиБ)	Размер нового виртуального диска в ГБ
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 присоединенного диска). Тип интерфейса можно обновлять после остановки всех ВМ, к которым присоединен 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

Поле	Описание
	общий объем хранилища в домене и объем, доступный на данный момент
Политика распределения	Политика распределения для нового виртуального диска. Для выбора доступны следующие значения: – Предварительное резервирование. Во время создания виртуального диска в домене хранилища выделяется весь объем 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 ГБ каждые 4 секунды, при возможности использовать предварительно зарезервированные диски. – Тонкое резервирование. Во время создания виртуального диска выделяется 1 ГБ 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 присоединенного

Поле	Описание
	диска)
Забить нулями после удаления	Параметр дает возможность включить повышенную защиту в виде удаления конфиденциальной информации при удалении виртуальных дисков
Загрузочный	Параметр дает возможность пометить виртуальный диск как загрузочный (параметр доступен только при создании присоединенного диска)
Может быть общим	Параметр дает возможность присоединить виртуальный диск к нескольким виртуальным машинам одновременно
Только для чтения	Параметр дает возможность предоставить доступ к виртуальному диску только для чтения (параметр доступен только при создании присоединенного 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 дает возможность сжать диск тонкого резервирования во время работы ВМ (параметр доступен только при создании присоединенного диска). Если параметр включен, 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

3.8.6.2.2 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 необходимо заполнить поля в разделе "Обнаружение таргетов" и нажать кнопку `Обнаружить`. Далее нужно нажать кнопку `Выполнить вход для всех` для получения списка всех доступных LUN на целевом сервере, после чего с помощью переключателей рядом с каждым LUN выбрать 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 жестких дисков ВМ необходимо учитывать следующие особенности:

– Динамическая миграция прямых LUN в виде образов жестких 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 таблице 68 описываются параметры виртуального диска с прямыми LUN в окнах "Новый виртуальный диск" и "Параметры виртуального диска".

Таблица 68 – 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 присоединенного диска). Тип интерфейса можно обновлять

Поле	Описание
	после остановки всех ВМ, к которым присоединен 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 — установить 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 присоединенного диска)
Загрузочный	Параметр дает возможность пометить виртуальный диск как загрузочный (параметр доступен только при создании присоединенного диска)
Может быть	Параметр дает возможность присоединить виртуальный диск

Поле	Описание
общим	к нескольким виртуальным машинам одновременно
Только для чтения	Параметр дает возможность предоставить доступ к виртуальному диску только для чтения (параметр доступен только при создании присоединенного 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 дает возможность сжать диск тонкого резервирования во время работы ВМ (параметр доступен только при создании присоединенного диска). Если параметр включен, 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 присоединенного диска и в случае, если для параметра "Интерфейс" указано значение "VirtIO-SCSI". Выбор этого флажка включает сквозной доступ виртуального диска к физическому устройству SCSI. Интерфейс VirtIO-SCSI с включенным 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 присоединенного 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 присоединенного 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

Поле	Описание
	потери доступа к диску со стороны ВМ, использующих резервирование SCSI

3.8.6.2.3 Параметры виртуального диска Cinder

Для виртуальных дисков Cinder требуется доступ к экземпляру тома OpenStack, который был добавлен в окружение виртуализации РОСА Виртуализация 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 таблице 69 описываются параметры виртуального диска Cinder в окнах "Новый виртуальный диск" и "Параметры виртуального диска".

Таблица 69 – Параметры виртуального диска Cinder

Поле	Описание
Размер (ГБ)	Размер нового виртуального диска в ГБ
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 присоединенного диска). Тип интерфейса можно обновлять после остановки всех ВМ, к которым присоединен 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

Поле	Описание
	диск. В выпадающем списке показываются все домены хранилищ, доступные в указанном дата-центре, а также отображается общий объем хранилища в домене и объем, 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 присоединенного диска)
Загрузочный	Параметр дает возможность пометить виртуальный диск как загрузочный (параметр доступен только при создании присоединенного диска)
Может быть общим	Параметр дает возможность присоединить виртуальный диск к нескольким виртуальным машинам одновременно
Только для чтения	Параметр дает возможность предоставить доступ к виртуальному диску только для чтения (параметр доступен только при создании присоединенного диска). Один и тот же диск может быть доступен только для чтения для одной ВМ, но доступен для записи для другой ВМ

3.8.6.3 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, присоединенного к выполняющейся ВМ, в исходном домене хранения создается 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 создается новый снимок, даже если эта попытка будет неудачной.

При использовании динамической миграции между хранилищами учитывать 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 жестких дисков с прямыми LUN или общих дисков.

3.8.6.4 Перемещение виртуальных дисков

В следующей последовательности действий описывается процесс перемещения виртуального диска, присоединенного к ВМ, или "плавающего" виртуального диска из одного домена хранения в другой.

При перемещении виртуальных дисков поддерживается динамическая миграция. Таким образом, диски, присоединенные к выполняющейся ВМ, также можно перемещать или, как вариант, нужно завершить работу ВМ перед началом миграции.

При перемещении виртуальных дисков учитывать следующие особенности процесса:

– Возможно перемещение нескольких виртуальных дисков одновременно.

– Диски могут перемещаться между двумя любыми доменами хранения одного дата-центра.

– Если виртуальный диск присоединен 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.

Для перемещения виртуального диска необходимо:

а) нажать "Хранилище → Диски"" и выбрать один или несколько виртуальных дисков для перемещения;

б) нажать кнопку Переместить;

в) в списке "Таргет" выбрать домен хранения, в который будет перемещен виртуальный диск;

г) при необходимости в списке "Профиль диска" выбрать профиль диска;

д) нажать кнопку 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.

3.8.6.5 Изменение типа интерфейса диска

После создания диска пользователь может изменить тип интерфейса диска. Это дает 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.

Для изменения типа интерфейса диска нужно:

а) нажать "Ресурсы → Виртуальные машины" и остановить работу необходимых ВМ;

б) нажать на имя ВМ, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Диски" и выбрать диск;

г) нажать кнопку Изменить;

д) из выпадающего списка "Интерфейс" выбрать новый тип интерфейса;

е) нажать кнопку OK.

Также диск можно присоединять к различным ВМ, требующим другого типа интерфейса.

Для присоединения диска к ВМ, использующим другой тип интерфейса, требуется :

а) нажать "Ресурсы → Виртуальные машины" и остановить работу соответствующих ВМ;

б) нажать на имя ВМ, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Диски" и выбрать диск;

г) нажать кнопку Удалить, затем нажать кнопку OK;

д) вернуться в меню "Виртуальные машины" и нажать на имя новой ВМ, к которой будет присоединен диск;

е) перейти на вкладку "Диски", затем нажать кнопку Присоединить;

ж) выбрать диск в окне "Присоединить виртуальные диски" и выбрать соответствующий интерфейс из выпадающего списка "Интерфейс";

з) нажать кнопку OK.

3.8.6.6 Копирование виртуальных дисков

Виртуальный диск можно скопировать из одного домена хранения в другой, после чего скопированный диск можно присоединять к виртуальным машинам.

Для копирования виртуального диска нужно выполнить следующие действия:

а) нажать "Хранилище → Диски"" и выбрать один или несколько виртуальных дисков;

б) нажать кнопку Копировать;

в) опционально ввести новое имя в поле "Псевдоним";

г) в списке "Таргет" выбрать домен хранения, в который будут скопированы виртуальные диски;

д) при необходимости в списке "Профиль диска" выбрать профиль диска;

е) нажать кнопку 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.

3.8.6.7 Шифрование виртуальных дисков

В целях обеспечения защиты информации пользователь может создавать и использовать в работе шифрованные виртуальные диски в дополнение к обычным виртуальным дискам. Интерфейс представляет собой веб-приложение и предназначен для создания зашифрованных дисков, а также для шифрования существующих дисков.

Важно — Для поддержки функции шифрования виртуальных дисков должны быть установлены дополнительные пакеты в окружение виртуализации РОСА Виртуализация.

3.8.6.7.1 Ограничения по использованию шифрованных виртуальных дисков

При использовании шифрованных виртуальных дисков есть некоторые ограничения по выполняемым над ними действиям. При развертывании дата-центра, подключении дискового хранилища и создании шифрованных дисков необходимо учитывать эти ограничения:

– Создание snapshots для шифрованных дисков невозможно. Если создан snapshot для шифрованного диска, то ВМ с таким диском не запустится.
– Резервное копирования для шифрованных дисков не поддерживается.
– Шифрованные диски создаются только для NFS-хранилища.
– Хост, на котором создаются шифрованные диски, помимо установленных пакетов, должен иметь роль SPM.

3.8.6.7.2 Установка плагина шифрования дисков

Системные требования для установки пакета:

– CPU – не менее 2;
– оперативная память – не менее 1 ГБ;
– диск – не меньше 50 ГБ.

Перед установкой пакетов нужно вставить носитель с дистрибутивом РОСА Виртуализация в привод DVD и выполнить в консоли хоста следующую команду для монтирования носителя:

```
# mount /dev/cdrom/ /mnt/
```

С диска РОСА Виртуализация нужно установить систему, выбрав в наборе программ для установки "Минимальная установка" и выполнив команду:

```
dnf install rv-disk-encrypt
```

3.8.6.7.3 Шифрование виртуальных дисков

Шифрование диска осуществляется пользователем через интерфейс Портала администрирования.

Для шифрования диска нужно перейти в панели управления в раздел "Дополнения → Шифрование дисков" (рисунок 215). В открывшемся окне основным элементом интерфейса является дерево элементов, в котором узлами представлены виртуальные машины.

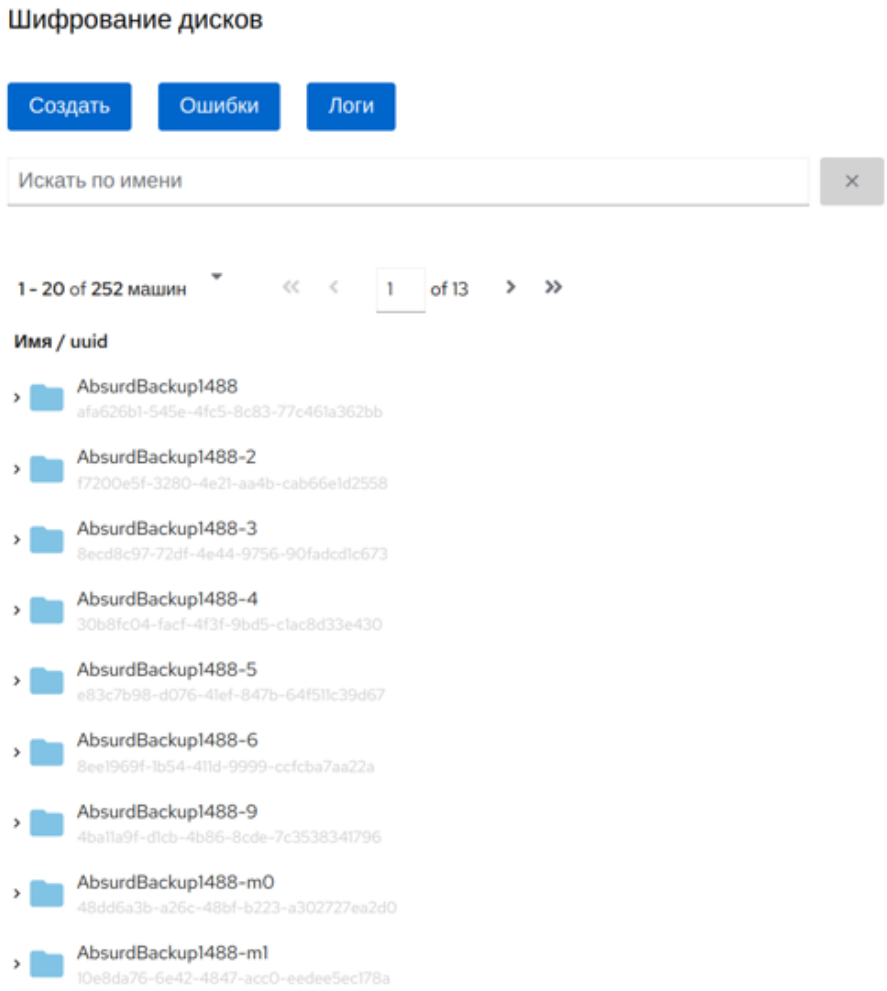


Рисунок 215 – Шифрование дисков

Если нажать на иконку папки или имя ВМ, то папка откроется и будет выглядеть как на рисунке 216.

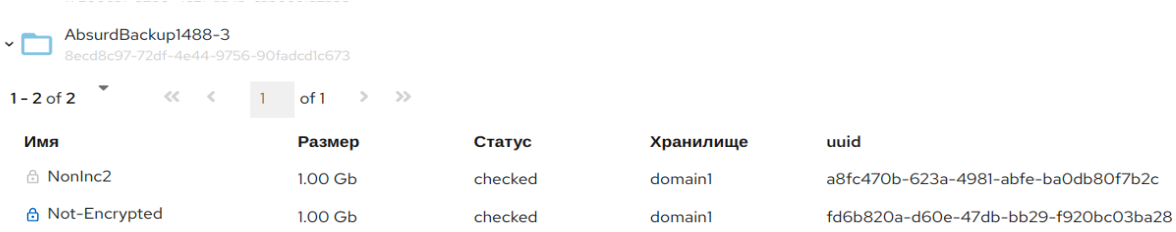


Рисунок 216 – Данные о ВМ

На рисунке показаны диски, прикрепленные к этой машине, обозначенные пиктограммами:

– – зашифрованные;
– – не зашифрованные, но которые можно зашифровать.

Для того чтобы зашифровать диск, нужно нажать на синюю пиктограмму , появится окно (рисунок 217).

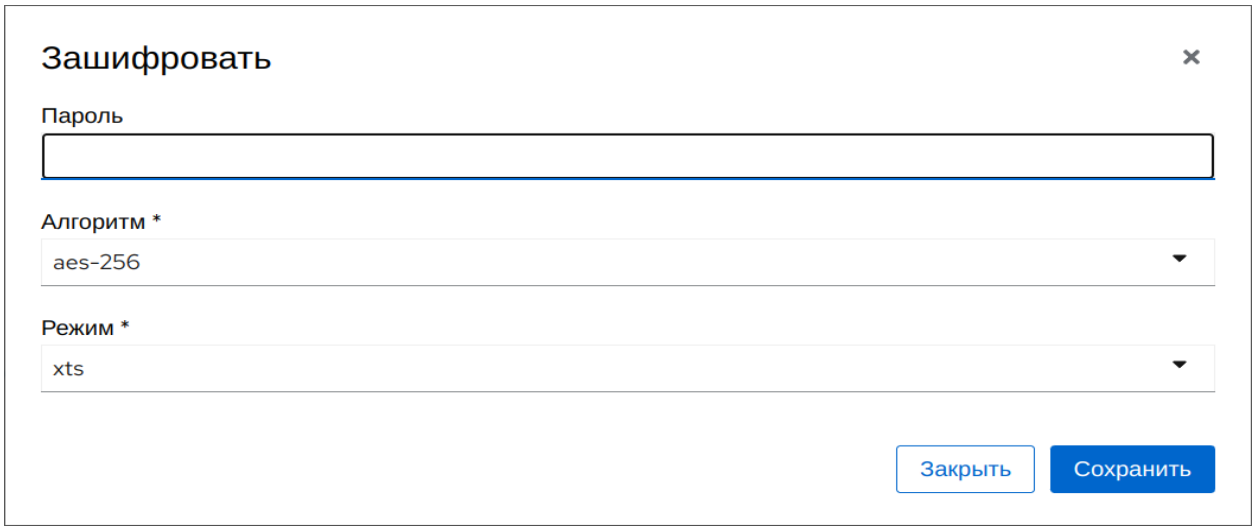


Рисунок 217 – Параметры шифрования диска

В форме нужно указать пароль и нажать кнопку Сохранить, пиктограмма сменится на крутящийся элемент. По успешном завершении процесса появится соответствующее сообщение, при этом цвет пиктограммы изменится с синего на серый.

3.8.6.7.4 Создание шифрованных виртуальных дисков

Создание шифрованного диска осуществляется пользователем через интерфейс Портала администрирования.

Примечание — Создание шифрованных виртуальных дисков возможно только для хранилища типа NFS.

Для создания шифрованного диска нужно перейти в панели управления в раздел "Дополнения → Шифрование дисков" (рисунок 218). В открывшемся окне основным элементом интерфейса является дерево элементов, в котором узлами представлены виртуальные машины.

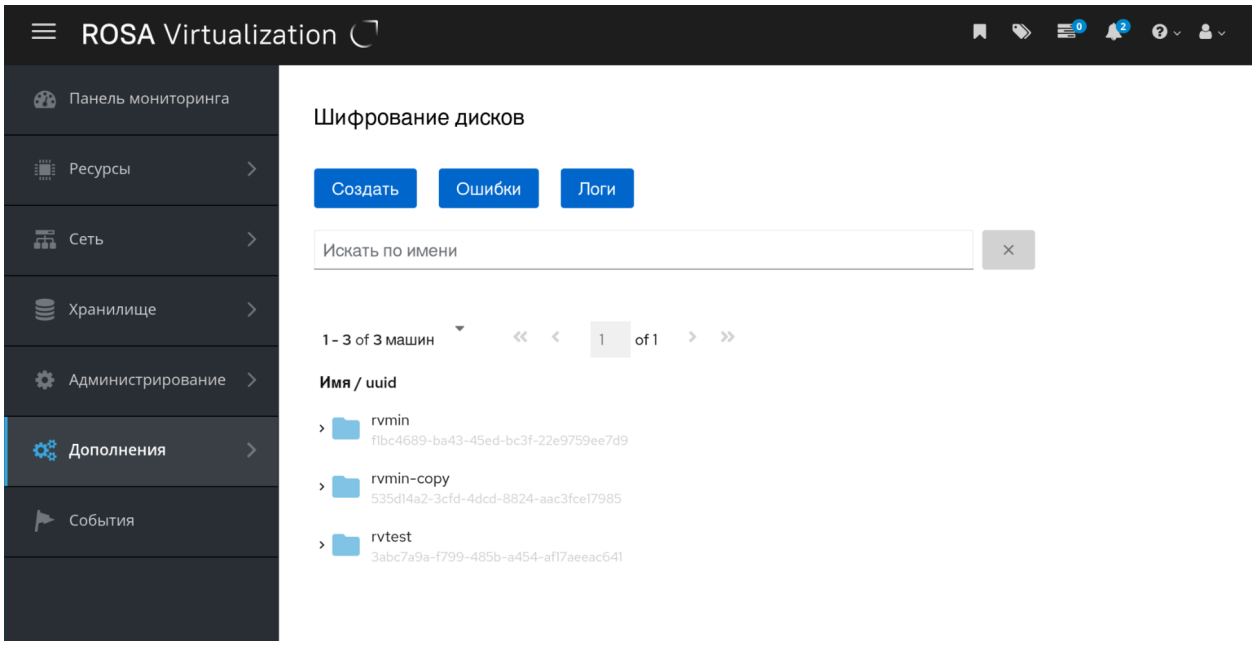


Рисунок 218 – Раздел "Дополнения → Шифрование дисков"

ж) нажать кнопку Создать;

з) в открывшемся окне для создания шифрованного диска (рисунок 219) заполнить поля:

– Имя – ввести наименование диска (пробелы в названии диска использовать не допускаются);
– Пароль – задать "Пароль" для шифрования диска;

Важно — В случае утери пароля работа на другом хосте с диском или перенесенной копией этого диска будет невозможна.

– Размер (гб) – указать размер диска в ГБ;
– Дата-центр – выбрать дата-центр;
– Хранилище – выбрать хранилище (домен хранения);
– Алгоритм шифрования – выбрать алгоритм шифрования диска;
– Режим – выбрать режим шифрования диска;

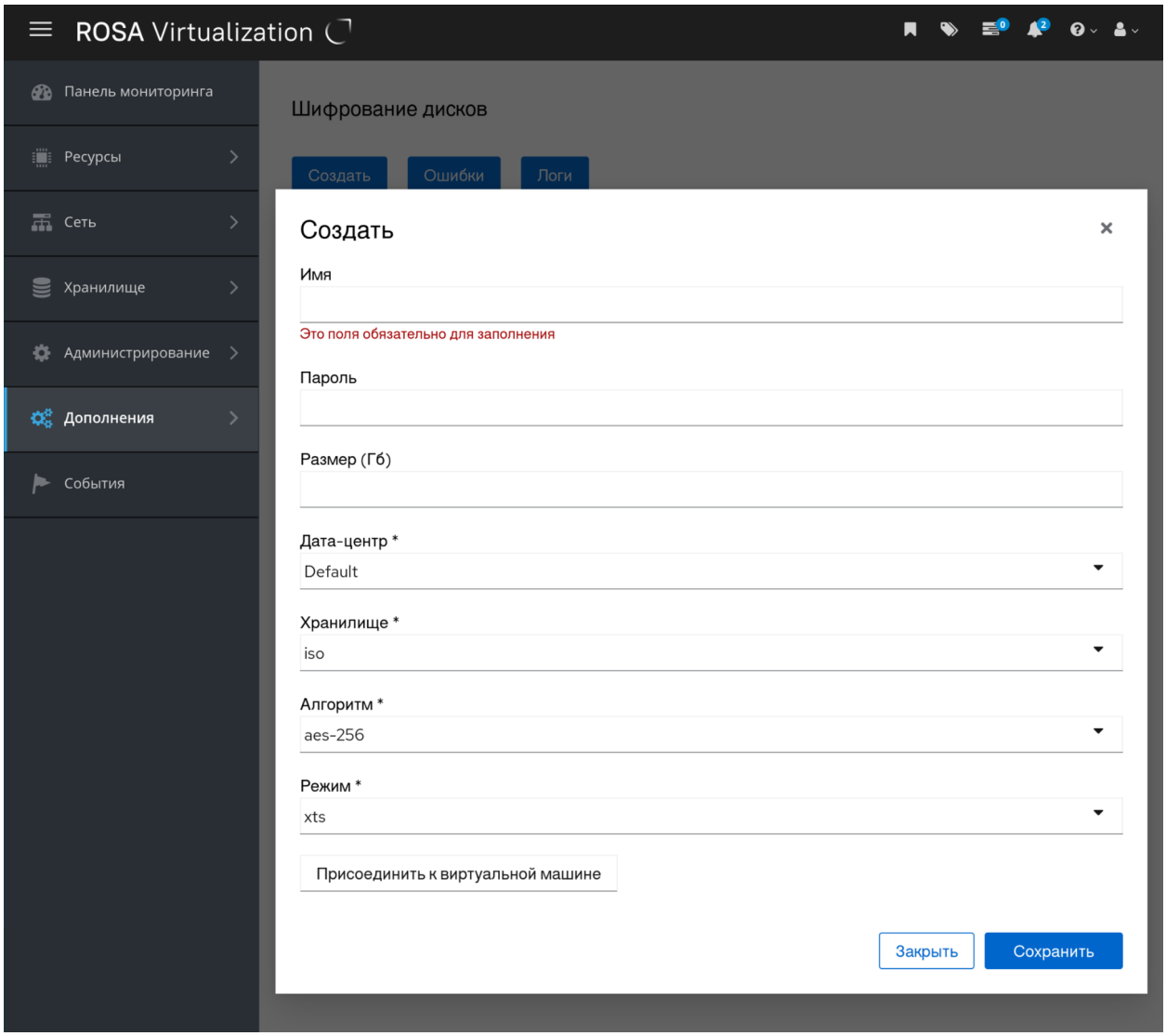


Рисунок 219 – Создание шифрованного диска

и) нажать на кнопку Сохранить (рисунок 220).

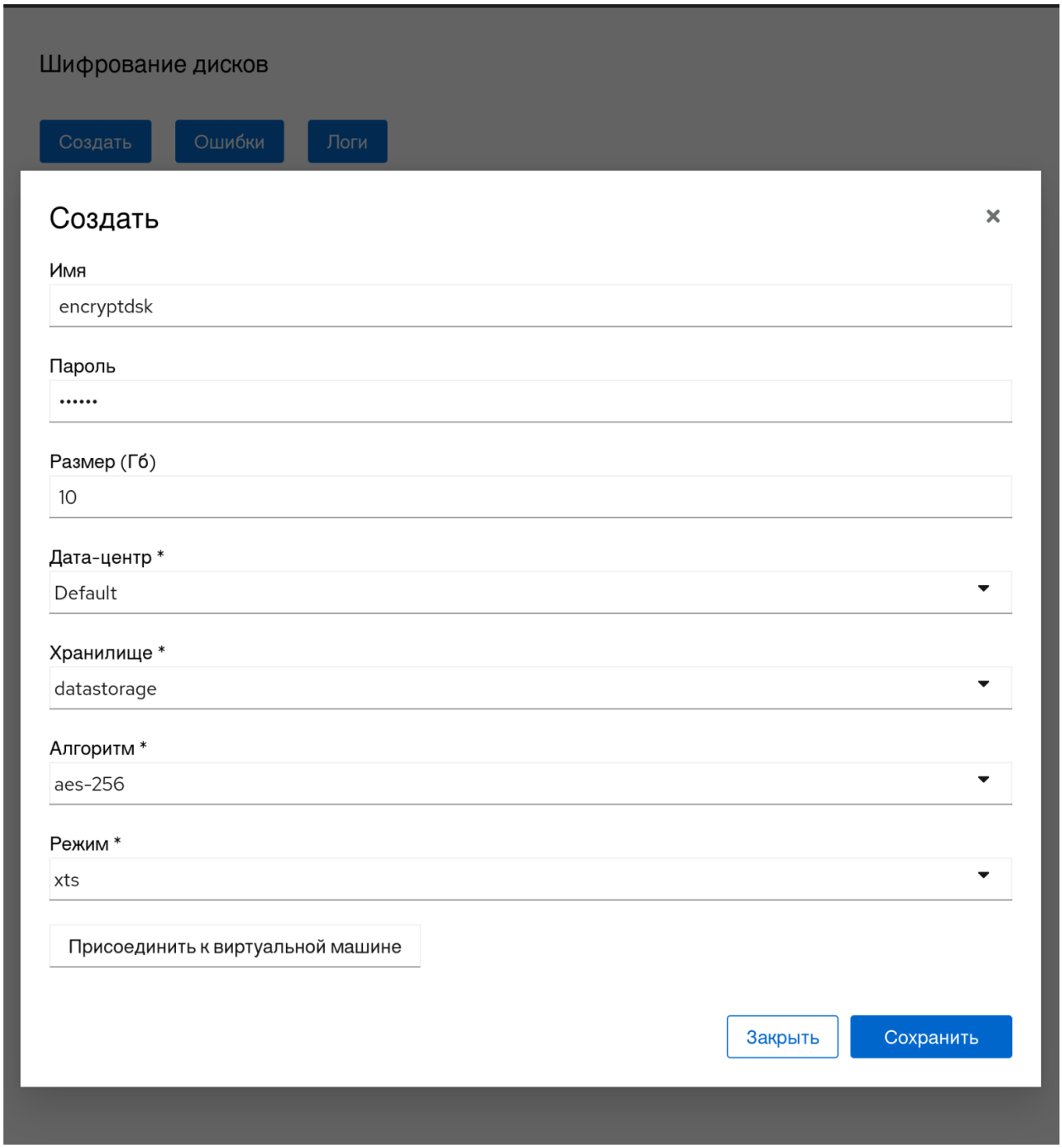


Рисунок 220 – Окно создания шифрованного диска с заполненными параметрами

Создаваемый шифрованный диск будет иметь статус "Запущено создание диска" (рисунок 221).

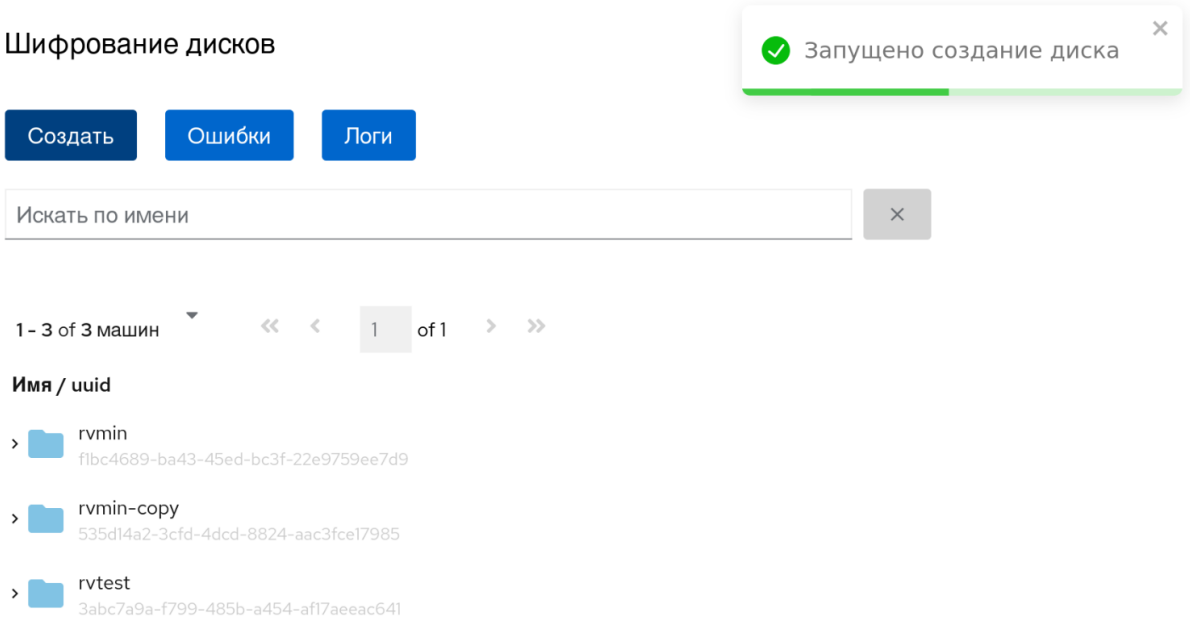


Рисунок 221 – Статус "Запущено создание диска"

После завершения создания шифрованного диска статус будет изменен на "Диск создан" (рисунок 222).

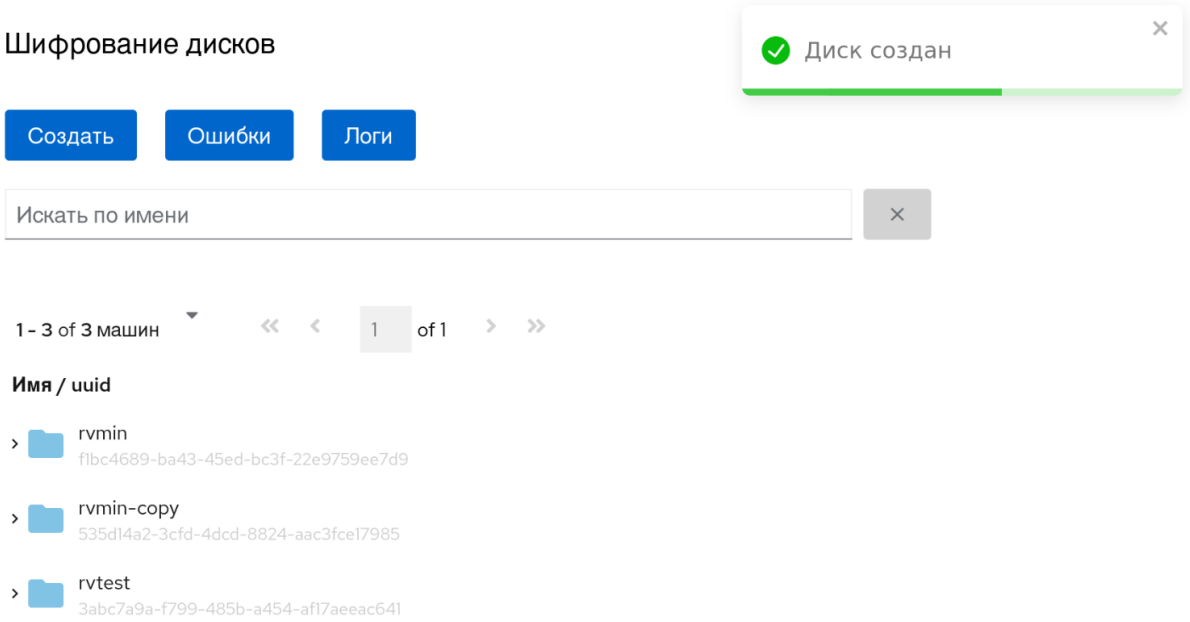


Рисунок 222 – Статус "Диск создан"

После создания шифрованного диска этот диск будет отображен в общем списке доступных в хранилище дисков (рисунок 223).

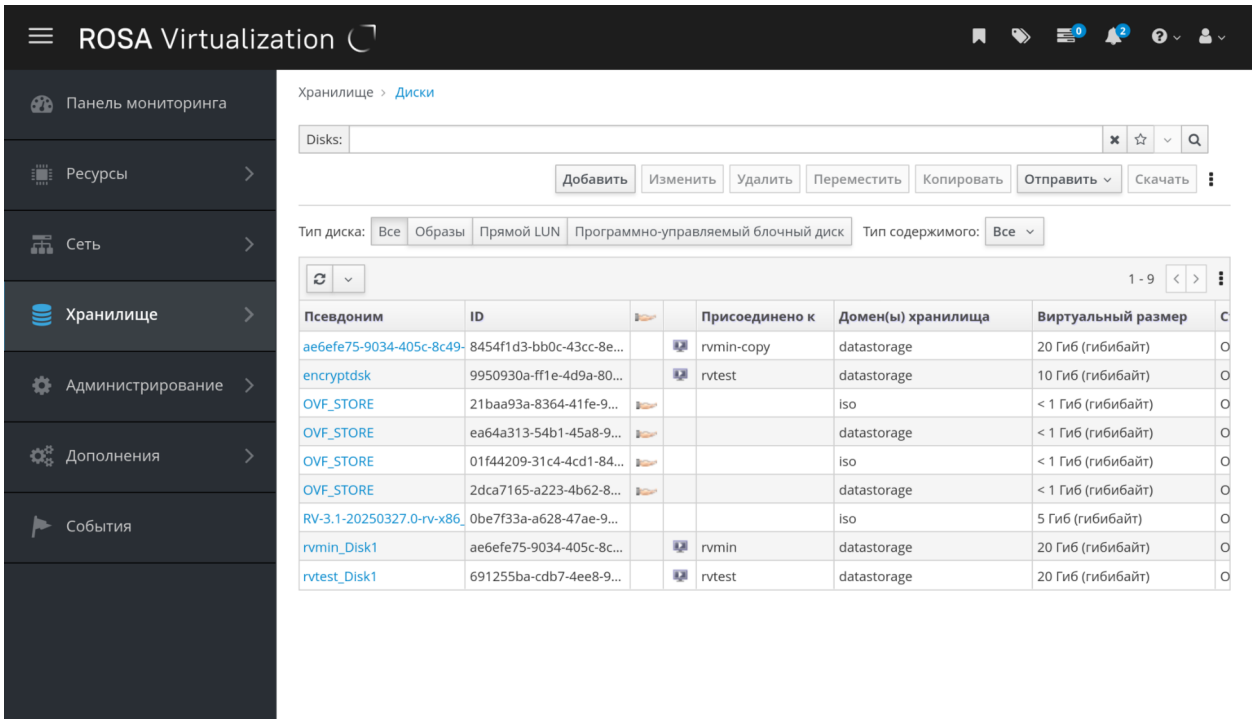


Рисунок 223 – Общий списков доступных в хранилище дисков, включая вновь созданный шифрованный диск

Операционная работа с шифрованными дисками (в том числе присоединение диска к ВМ, копирование/удаление диска и т. п.) осуществляется точно так же, как с обычными виртуальными дисками.

С помощью кнопки Присоединить к виртуальной машине можно выбрать ВМ, к которой будет присоединен диск после его создания (рисунок 224).

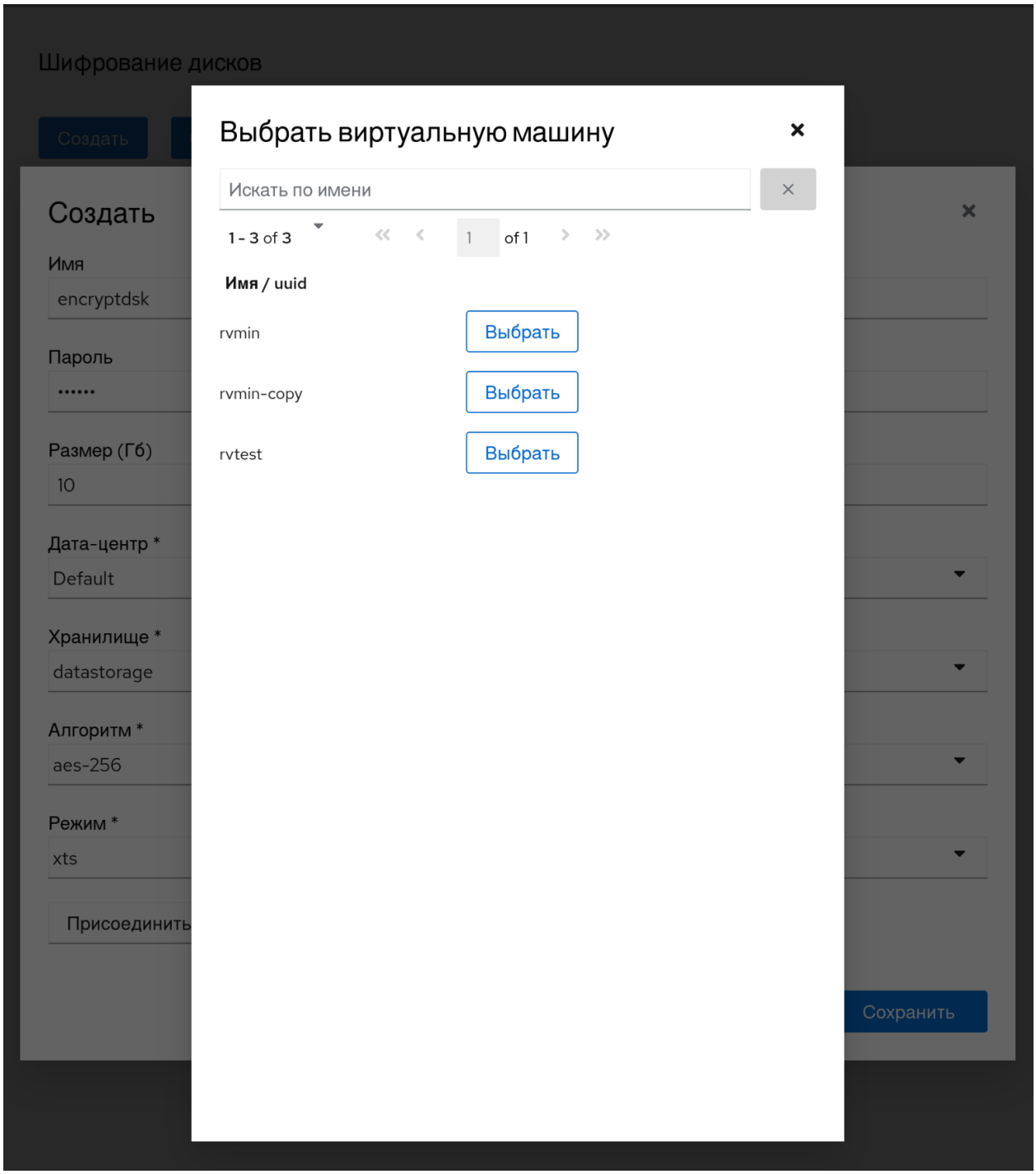


Рисунок 224 – Выбор ВМ, к которой необходимо присоединить шифрованный диск

После выбора ВМ для присоединения шифрованного диска название виртуальной машины будет отображаться в форме создания шифрованного диска (рисунок 225).

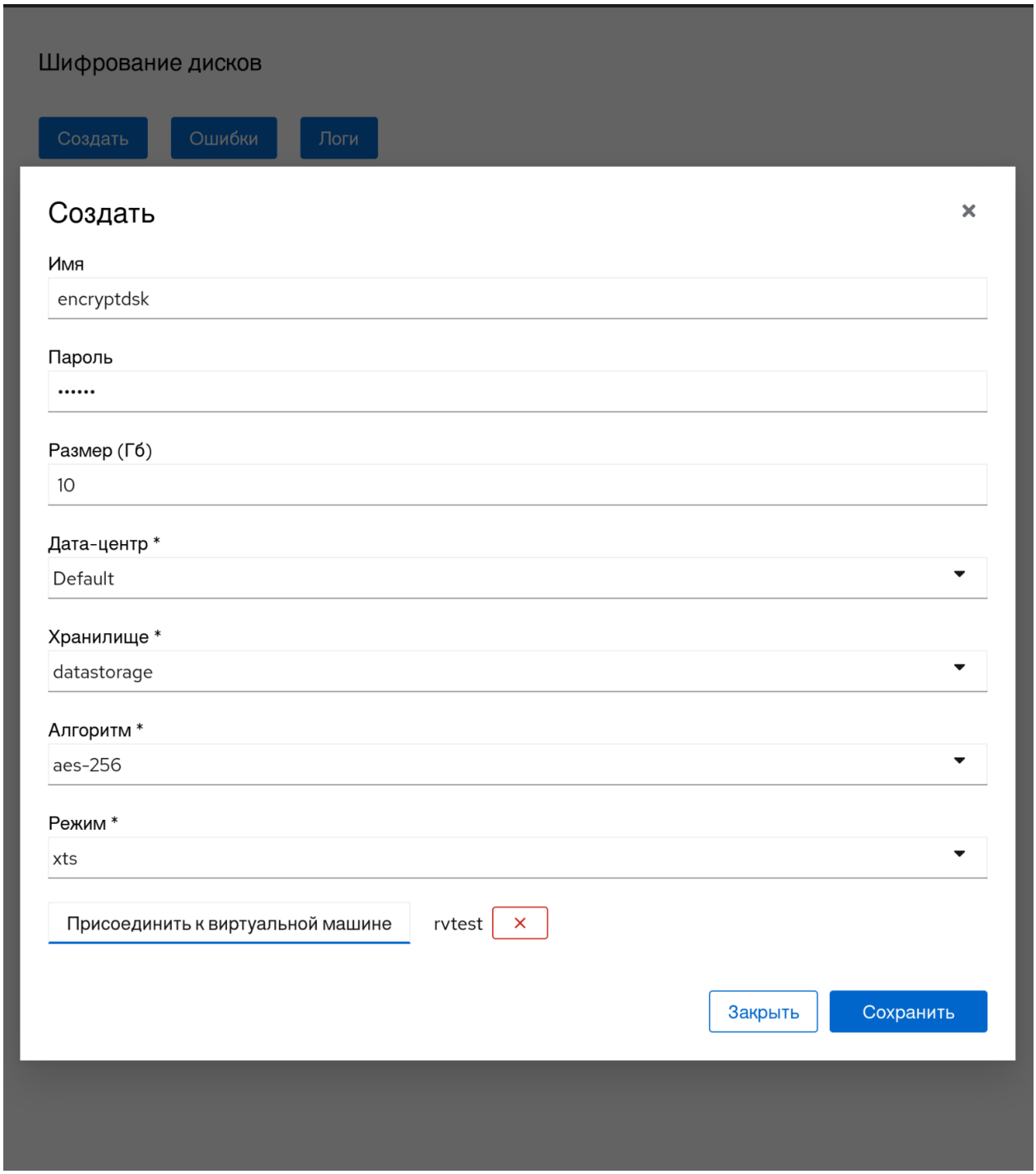


Рисунок 225 – Присоединение шифрованного диска к ВМ при его создании

После создания шифрованного диска, присоединенного к ВМ, этот диск будет отображен в общем списке доступных в хранилище дисков с указанием ВМ, к которой он присоединен, в поле "Присоединен к" (рисунок 223).

Следует обратить внимание, что создание снимков для шифрованных дисков не допускается, а ВМ с таким диском не запустится.

Важно — При создании нового шифрованного диска следует сохранить пароль диска в надежном месте. В случае его утери работа с копиями диска, перенесенными на другой хост, будет невозможна.

3.8.6.7.5 Создание копии шифрованного диска

После создания шифрованный диск появится в общей таблице дисков, и с ним можно выполнить операции, предусмотренные для управления дисками в хранилище (рисунок 226).

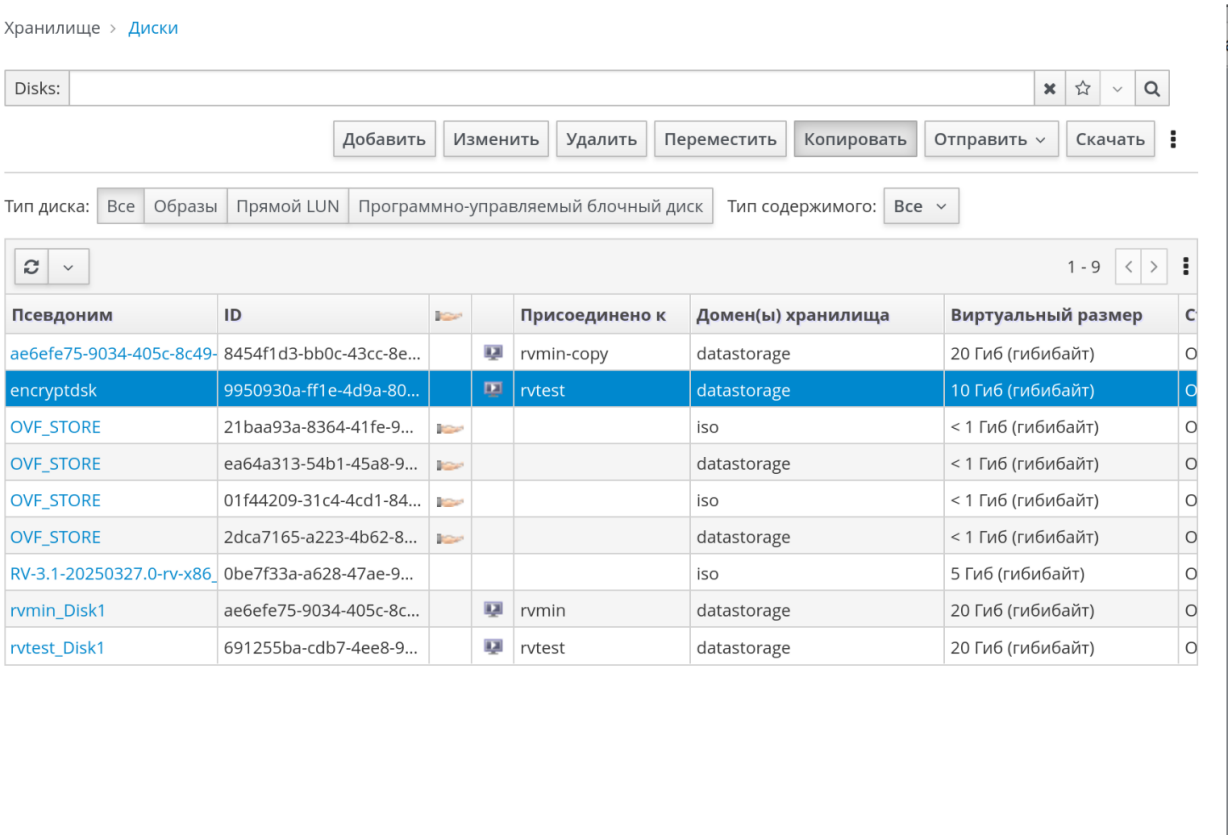


Рисунок 226 – Общий список дисков в хранилище с выбранным шифрованным диском encryptdsk

Копия шифрованного диска создается стандартными средствами.

Для создания копии нужно выбрать диск и нажать на кнопку Копировать (рисунок 226).

Затем в поле "Таргет" следует выбрать хранилище, в которое необходимо скопировать диск (рисунок 227).

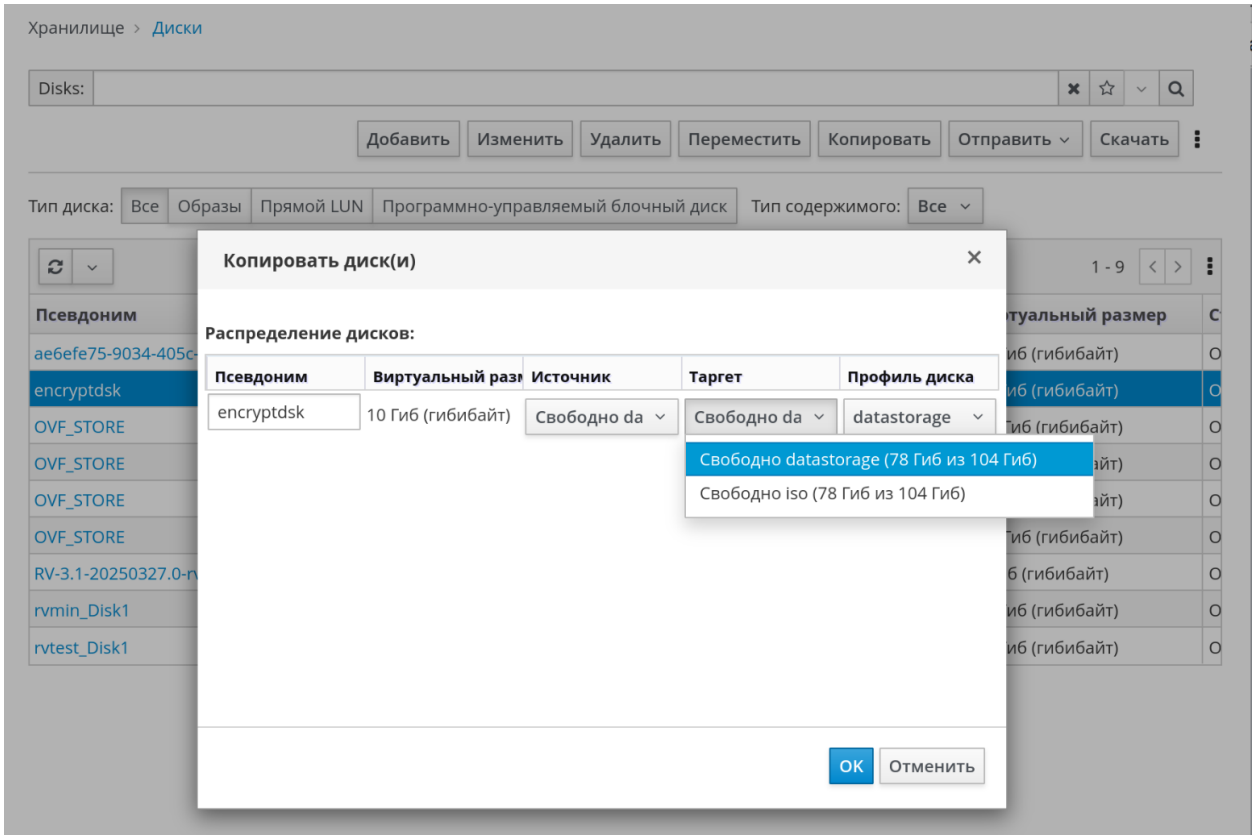


Рисунок 227 – Выбор целевого хранилища для копирования диска

После создания копии диск также отобразится в списке доступных в хранилище дисков.

3.8.6.7.6 Присоединение шифрованного диска к ВМ

Присоединение шифрованного диска к ВМ производится как стандартными средствами, так и через интерфейс окна шифрования дисков.

Для создания диска, присоединенного к ВМ, необходимо в форме создания шифрованного диска нажать кнопку Присоединить к виртуальной машине и выбрать нужную ВМ.

После того как диск присоединен к ВМ, в таблице дисков появится название ВМ, к которой присоединен диск.

3.8.6.7.7 Удаление шифрованного диска

Удаление шифрованного диска происходит стандартными средствами на вкладке "Хранилище → Диски" через интерфейс Портала администрирования ВМ.

Для удаления диска нужно выбрать его в списке дисков хранилища и нажать на кнопку Удалить (рисунок 228).

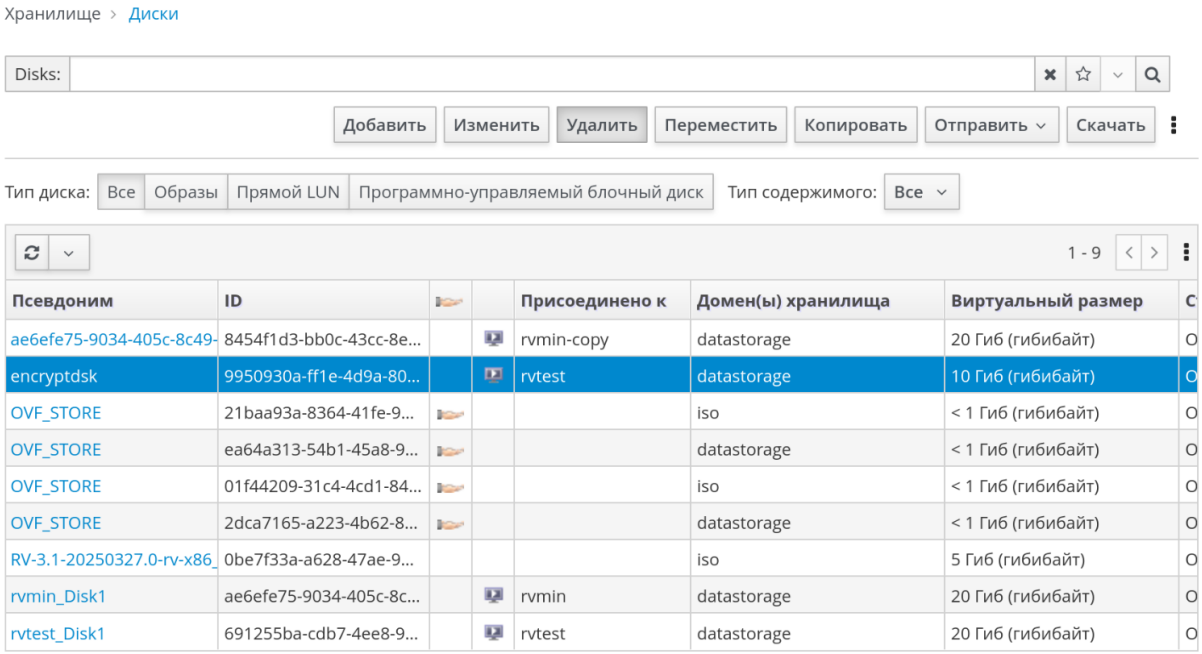


Рисунок 228 – Удаление выбранного диска

В открывшейся форма для подтверждения согласия на удаление диска (рисунок 229) нажать на кнопку OK для подтверждения удаления диска или кнопку Отменить – для отмены.

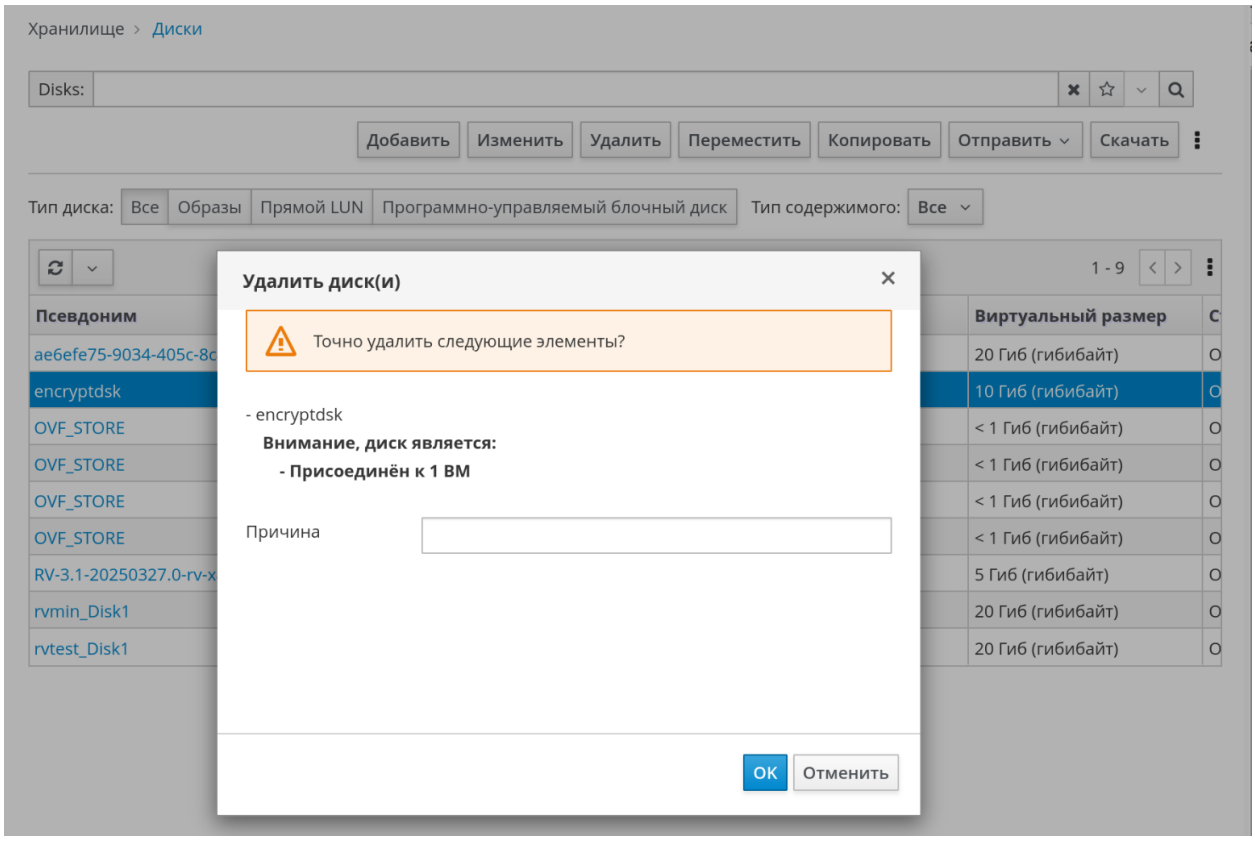


Рисунок 229 – Форма подтверждения удаления диска

3.8.6.7.8 Скачивание шифрованного диска

Скачивание шифрованного диска происходит стандартными средствами на вкладке "Хранилище → Диски" через интерфейс Портала администрирования ВМ.

Для скачивания шифрованного диска нужно выбрать требуемый диск из списка и нажать на кнопку Скачать (рисунок 230).

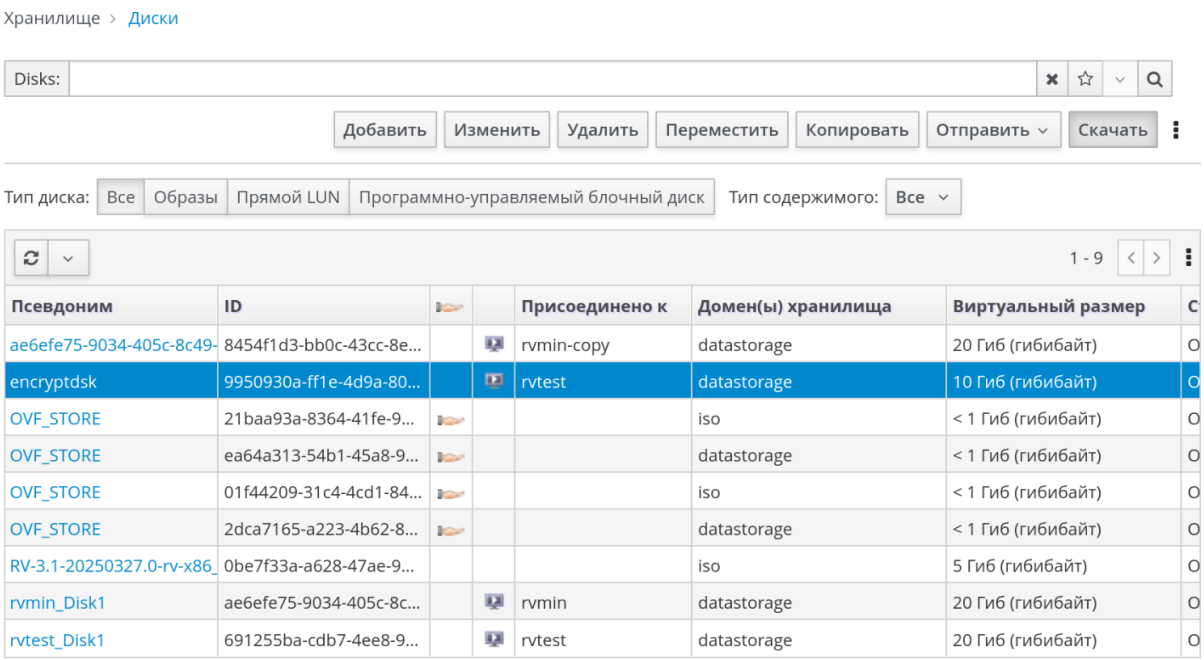


Рисунок 230 – Скачивание диска из хранилища

3.8.6.7.9 Установка шифрованного диска на другой хост

Для установки шифрованного диска на другой хост нужно выполнить следующие действия:

а) файл диска, который был скачан с первого хоста, отправляется на новый хост стандартными средствами на вкладке "Хранилище → Диски" через интерфейс Портала администрирования ВМ;

Важно — При загрузке внешнего шифрованного диска на хост следует убедиться, что опция инкрементного резервного копирования выключена, иначе диск будет неработоспособным.

После того как диск будет отправлен в Систему, он появится в таблице шифрованных дисков;

Установленный шифрованный диск с другого хоста будет запрашивать пароль, который был присвоен диску при создании. Если пароль утерян или были отправлены неверные данные, работа с диском будет невозможна (рисунок 231);

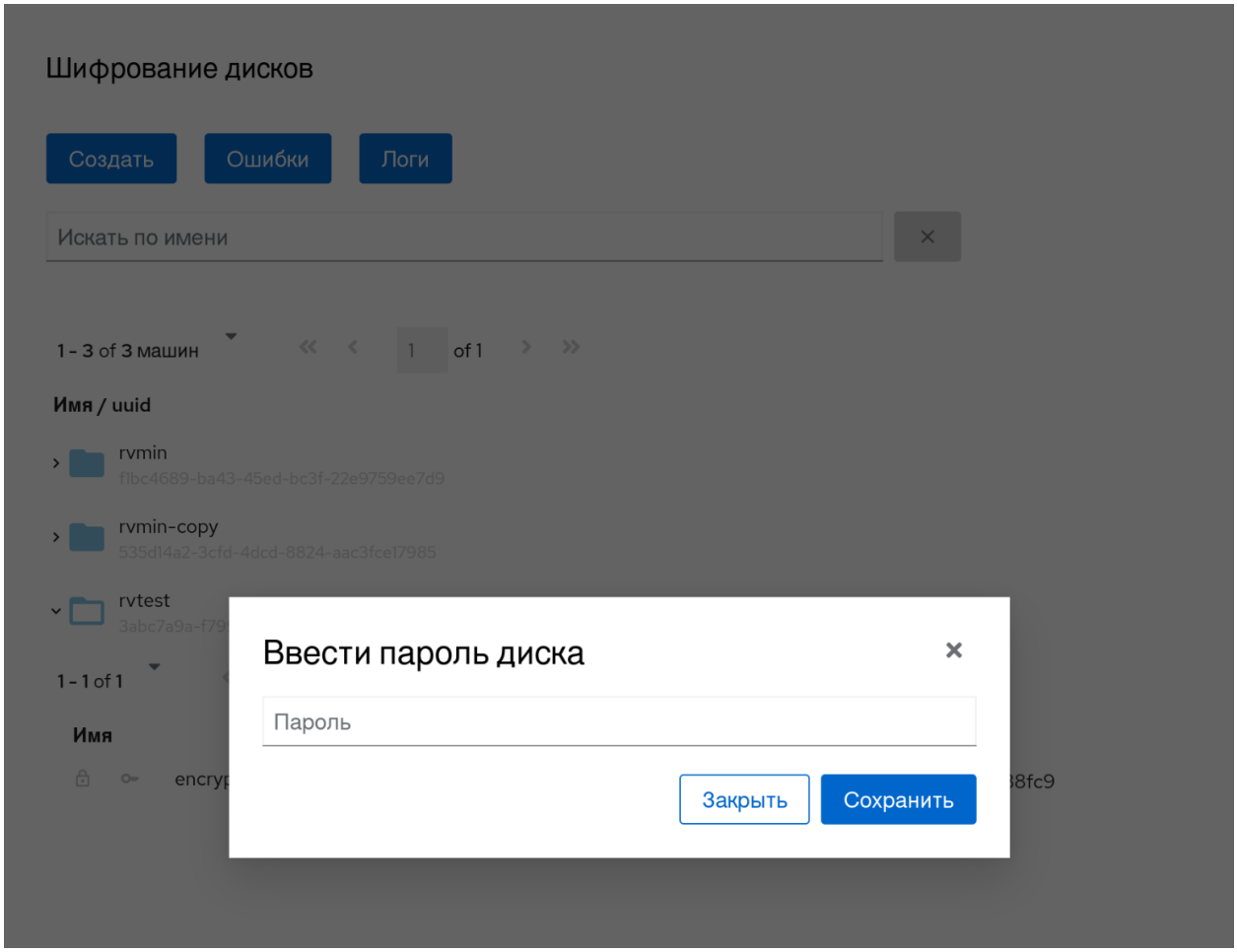


Рисунок 231 – Ввод пароля для шифрованного диска

б) для завершения установки диска на новый хост ввести пароль и нажать кнопку Сохранить.

Примечания:

– Создание snapshots для шифрованных дисков невозможно. Если создан snapshot для шифрованного диска, то ВМ с таким диском не запустится.

– Резервное копирования для шифрованных дисков не поддерживается.

– Шифрованные диски создаются только для NFS-хранилища.

– Хост, на котором создаются шифрованные диски, помимо установленных пакетов, должен иметь роль SPM.

3.8.6.7.10 Ошибки при создании шифрованного диска

Если при создании шифрованного диска возникнут ошибки, то они будут отображаться в интерфейсе Портала администрирования ВМ.

Примечание — Создание snapshots для шифрованных дисков невозможно. Если создан snapshot для шифрованного диска, то ВМ с таким диском запущена не будет.

Важно — При загрузке внешнего шифрованного диска на хост следует убедиться, что опция инкрементного резервного копирования выключена (рисунок 232). В противном случае диск будет неработоспособным.

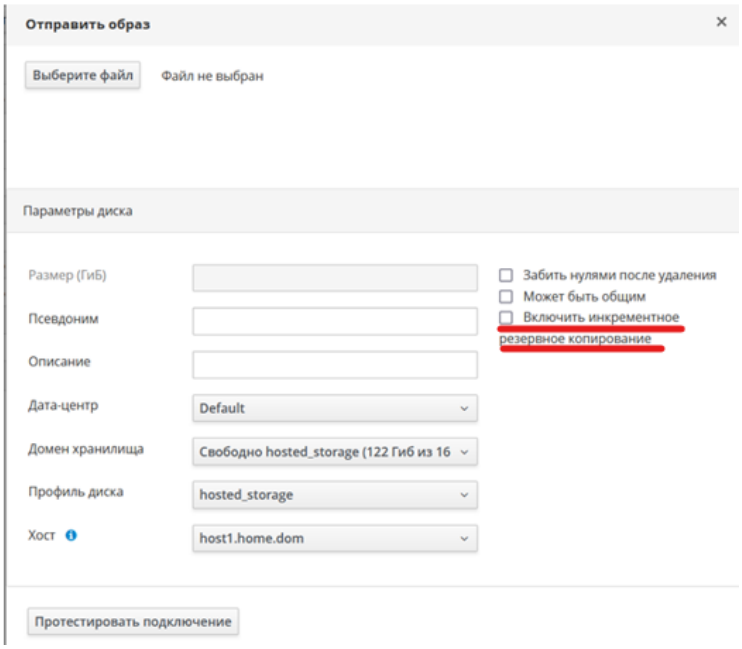


Рисунок 232 – Деактивированная опция инкрементного резервного копирования

3.8.6.8 Отправка образов в домен хранения данных

Образы виртуальных дисков и образы ISO можно отправить в домен хранения данных на Портале администрирования или с помощью REST API.

3.8.6.9 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.

Для импорта образа диска нужно:

а) нажать "Хранилище → Домены";

б) нажать на имя импортированного домена хранения, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Импорт диска";

г) выбрать один или несколько образов дисков и нажать кнопку Импортировать;

д) выбрать соответствующий "Профиль диска" для каждого диска;

е) нажать кнопку OK.

3.8.6.10 Импорт незарегистрированного образа диска из импортированного домена хранения

"Плавающие" виртуальные диски, созданные вне окружения виртуализации РОСА Виртуализация, не регистрируются виртуализированным ЦУ.

Для опознания незарегистрированных "плавающих" дисков с последующим импортом выполняют сканирование домена хранения.

Примечание — В виртуализированный ЦУ можно импортировать только диски, совместимые с QEMU.

Для импорта незарегистрированного образа диска необходимо:

а) нажать "Хранилище → Домены";

б) нажать на имя импортированного домена хранения, чтобы перейти к подробному просмотру;

в) нажать кнопку ⋮ (Больше действий), затем нажать кнопку Сканирование дисков, чтобы виртуализированный ЦУ идентифицировал незарегистрированные виртуальные диски;

г) перейти на вкладку "Импорт дисков";

д) выбрать один или несколько образов дисков и нажать кнопку Импортировать;

е) выбрать соответствующий "Профиль диска" для каждого диска;

ж) нажать кнопку OK.

3.8.6.11 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.

Для импорта виртуального диска из службы образов OpenStack нужно выполнить следующие действия:

а) нажать "Хранилище → Домены";

б) нажать на имя домена службы образов OpenStack, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Образы" и выбрать образ;

г) нажать кнопку Импорт;

д) выбрать "Дата-центр", в который будет импортирован образ;

е) из выпадающего списка "Имя домена" выбрать домен хранения, в котором будет храниться образ;

ж) опционально в списке "Квота" выбрать квоту, применяемую к образу;

з) нажать кнопку ОК.

При необходимости после импорта виртуальный диск можно присоединить к ВМ.

3.8.6.12 Экспорт виртуальных дисков в службу образов OpenStack

Виртуальные диски могут быть экспортированы в службу образов OpenStack, которая предварительно 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.

Для экспорта виртуального диска в службу образов OpenStack нужно выполнить следующие действия:

а) нажать "Хранилище → Диски" и выбрать один или несколько экспортируемых дисков;

б) нажать кнопку ⋮ (Больше действий), затем нажать кнопку Экспорт;

в) из выпадающего списка "Имя домена" выбрать службу образов OpenStack, в которую будут экспортированы диски;

г) опционально в списке "Квота" выбрать квоту, применяемую к дискам;

д) нажать кнопку OK.

3.8.6.13 Возвращение хосту дискового пространства виртуальных дисков

Виртуальные диски, использующие тонкое резервирование пространства в хранилище, не сжимаются автоматически после удаления файлов. Например, если фактический размер диска равен 100 ГБ и будет удалено 50 ГБ файлов, выделенное пространство диска по-прежнему останется 100 ГБ, а оставшиеся 50 ГБ не возвращаются хосту и соответственно не могут использоваться виртуальными машинами.

Для того чтобы вернуть хосту неиспользуемое дисковое пространство, требуется выполнить 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 следует выбрать параметр "Тонкое" в поле "Резервирование хранилища" или при выборе "Клонирования" и убедиться в том, что шаблон основан на ВМ с тонким резервированием.

– Разреживать можно только активные снимки дисков.

Для разреживания диска необходимо:

а) нажать "Ресурсы → Виртуальные машины" и выключить необходимую ВМ;

б) нажать на имя ВМ, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Диски" и убедиться в том, что диск имеет статус "OK";

г) нажать кнопку ⋮ (Больше действий), затем нажать кнопку Разредить;

д) нажать кнопку 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.

4 АДМИНИСТРИРОВАНИЕ ОКРУЖЕНИЯ

4.1 Администрирование виртуализированного ЦУ

4.1.1 Обслуживание виртуализированного ЦУ

Режимы обслуживания дают возможность запускать, останавливать и изменять параметры ВМ СУСВ без вмешательств со стороны агентов высокой доступности, а также перезапускать и изменять параметры узлов виртуализированного ЦУ, не пересекаясь с работой СУСВ.

Существует три режима обслуживания:

– Глобальный – Мониторинг состояния СУСВ со стороны всех агентов высокой доступности в кластере отключается. Глобальный режим должен применяться для любых операций по настройке или обновлению, требующих остановки службы ovirt-engine.

– Локальный – Мониторинг состояния СУСВ со стороны агента высокой доступности на узле, отдающем команду, отключается. В локальном режиме обслуживания узел исключается из числа узлов, на которых может размещаться СУСВ; если во время перевода в этот режим на узле размещается СУСВ, то она мигрирует на другой узел при условии доступности такого узла. Локальный режим рекомендуется во время применения изменений системных параметров узла виртуализированного ЦУ.

– Нет – Режим обслуживания отключается, обеспечивая работу агентов высокой доступности.

4.1.1.1 Активация локального режима обслуживания

Включение локального режима обслуживания останавливает работу агента высокой доступности на отдельном узле виртуализированного ЦУ.

Для активации локального режима обслуживания с Портала администрирования необходимо:

а) перевести узел виртуализированного ЦУ в локальный режим обслуживания:

1) на Портале администрирования нажать "Ресурсы → Хосты" и выбрать узел виртуализированного ЦУ;
2) выбрать "Управление → Обслуживание" (рисунок 233);

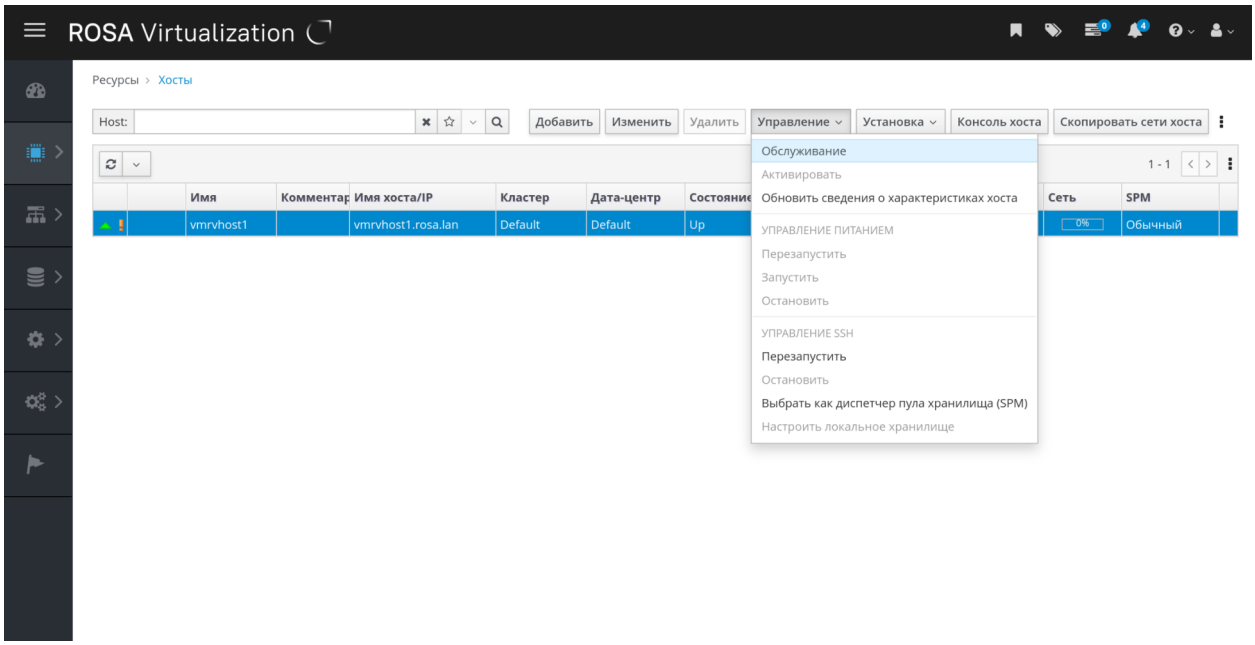


Рисунок 233 – Активация локального режима обслуживания хоста

3) опционально указать причину перевода хоста в режим обслуживания (рисунок 234). Выбранный узел будет автоматически помещен в локальный режим обслуживания;

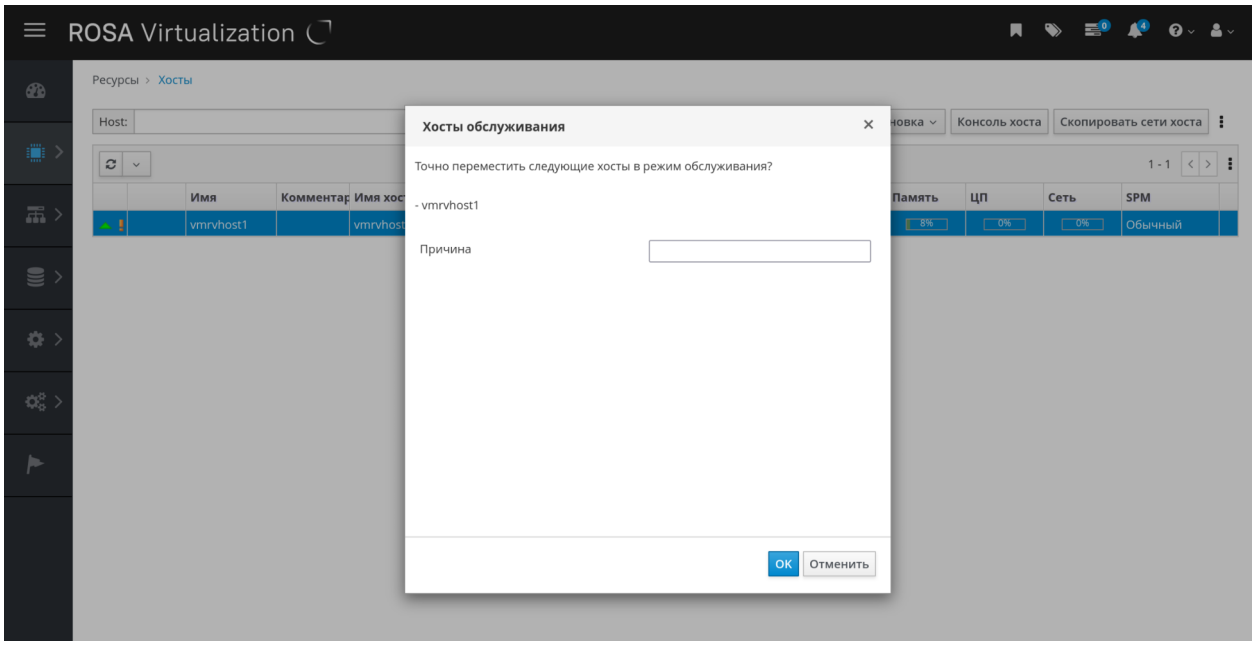


Рисунок 234 – Форма подтверждения перевода хоста в режим обслуживания

б) выполнив необходимые задачи по обслуживанию, отключить режим обслуживания:

1) на Портале администрирования нажать "Ресурсы → Хосты" и выбрать узел виртуализированного ЦУ;
2) нажать "Управление → Активировать" для активации хоста, находящегося в режиме обслуживания (рисунок 235).

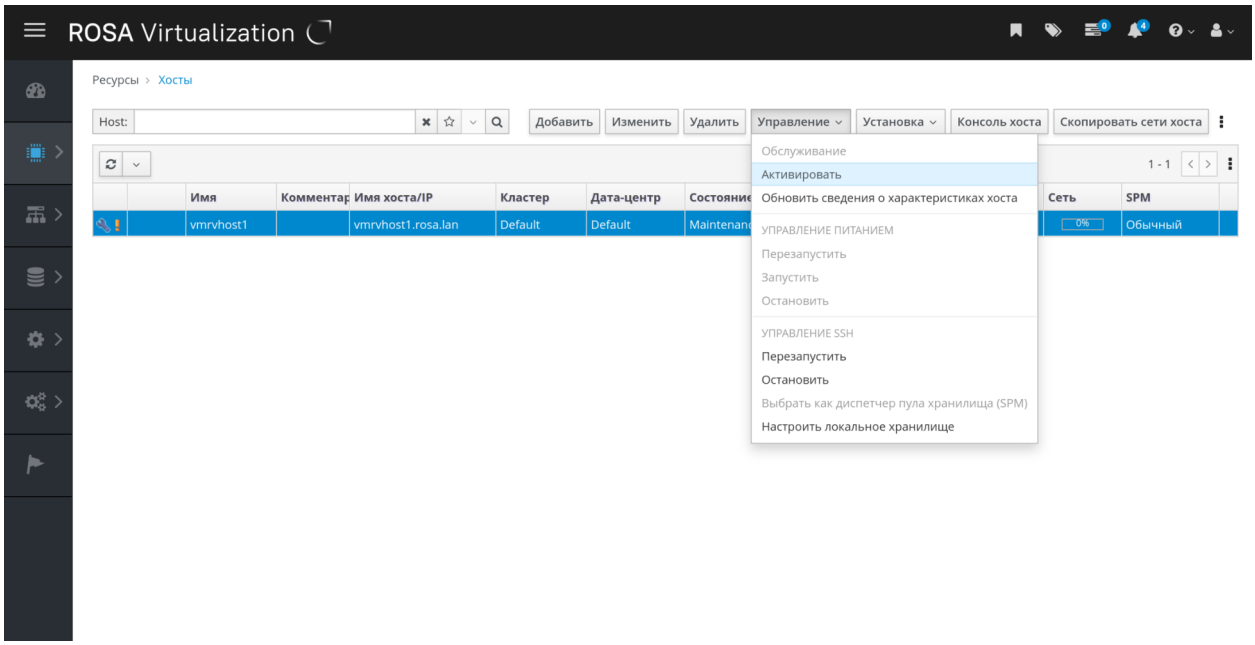


Рисунок 235 – Активация хоста, находящегося в режиме обслуживания

Для активации локального режима обслуживания из командной строки необходимо:

а) войти в Систему на узле виртуализированного ЦУ и перевести его в локальный режим обслуживания:

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

б) выполнив необходимые задачи по обслуживанию, отключить режим обслуживания:

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

4.1.1.2 Активация глобального режима обслуживания

Включение глобального режима обслуживания останавливает работу агентов высокой доступности на всех узлах виртуализированного ЦУ в кластере.

Для активации глобального режима обслуживания через интерфейс Портала администрирования нужно выполнить следующие действия:

а) перевести все узлы виртуализированного ЦУ в глобальный режим обслуживания:

1) на Портале администрирования нажать "Ресурсы → Хосты" и выбрать любой узел виртуализированного ЦУ;

2) нажать пиктограмму ⋮ (Больше действий), затем нажать кнопку `Включить глобальное обслуживание высокой доступности` (рисунок 236);

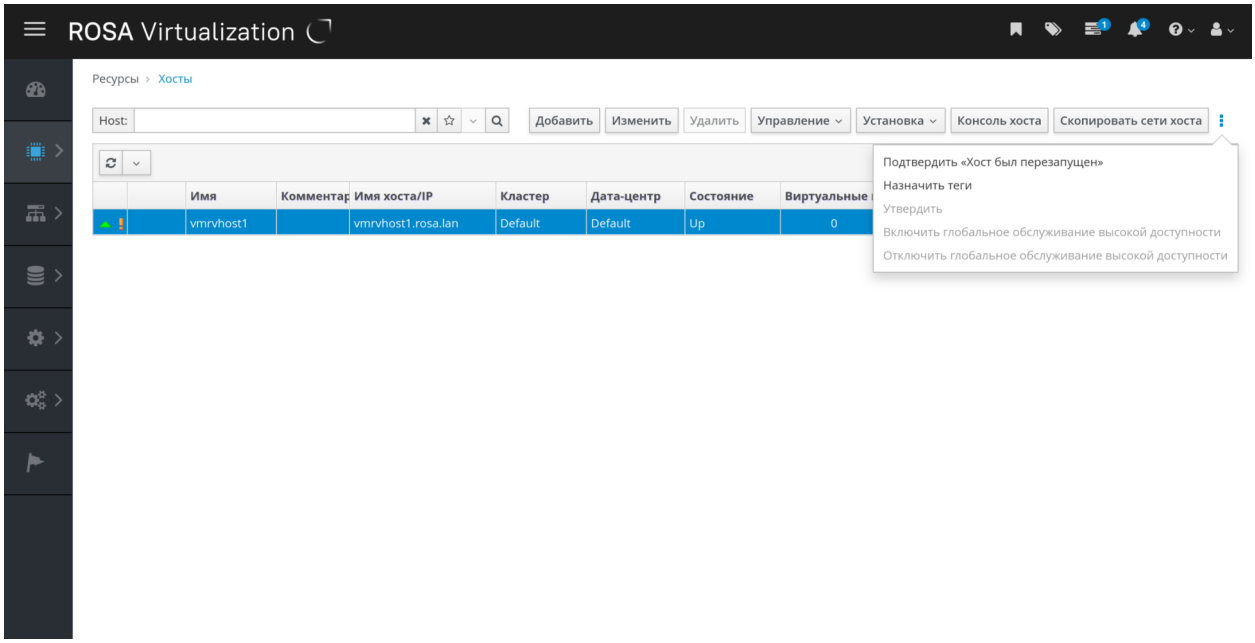


Рисунок 236 – Меню "Больше действий" в форме для управления хостами

б) выполнить необходимые задачи по обслуживанию и отключить режим обслуживания:

1) на Портале администрирования нажать "Ресурсы → Хосты" и выбрать любой узел виртуализированного ЦУ;

2) нажать пиктограмму ⋮ (Больше действий), затем нажать кнопку `Отключить глобальное обслуживание высокой доступности`;

Для активации глобального режима обслуживания из командной строки необходимо:

а) войти в Систему на узле виртуализированного ЦУ и перевести его в глобальный режим обслуживания:

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

б) выполнив необходимые задачи по обслуживанию, отключить режим обслуживания:

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

4.1.2 Администрирование СУСВ

Утилита hosted-engine предоставляет в помощь администраторам множество команд для работы с СУСВ. Утилиту можно запускать на любом узле виртуализированного ЦУ. Для просмотра всех доступных команд следует выполнить:

```
hosted-engine –help
```

Дополнительные сведения по отдельной команде можно просмотреть, выполнив:

```
hosted-engine --<команда> --help
```

4.1.2.1 Обновление конфигурации виртуализированного ЦУ

Для обновления конфигурации виртуализированного ЦУ используется команда:

```
# hosted-engine --set-shared-config.
```

Эта команда обновляет конфигурацию виртуализированного ЦУ в домене разделяемого хранилища после выполнения начального развертывания.

Для просмотра значений текущей конфигурации используется команда:

```
# hosted-engine --get-shared-config.
```

Для получения списка всех доступных ключей конфигурации и их соответствующих типов нужно ввести следующую команду:

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

где параметр "type" может принимать одно из значений, указанных в таблице 70.

Таблица 70 – Значения параметра "type"

Параметр	Значения параметра type
he_local	Настраивает значения в локальном экземпляре файла /etc/ovirt-hosted-engine/hosted-engine.conf на локальном хосте так, чтобы новые значения использовались только на этом хосте. Для активации

Параметр	Значения параметра type
	новых значений перезапустить службы ovirt-ha-broker
he_shared	Настраивает значения файла /etc/ovirt-hosted-engine/hosted-engine.conf в разделяемом хранилище так, чтобы все хосты, которые будут развернуты после изменений конфигурации, использовали эти значения. Для активации новых значений на хосте развернуть этот хост повторно
ha	Настраивает значения в файле /var/lib/ovirt-hosted-engine-ha/ha.conf в локальном хранилище. Новые параметры вступают в силу немедленно
broker	Настраивает значения в файле /var/lib/ovirt-hosted-engine-ha/broker.conf в локальном хранилище. Для применения новых значений перезапустить службу ovirt-ha-broker

4.1.2.2 Настройка почтовых уведомлений

Для каждого изменения состояния высокой доступности на узлах виртуализированного ЦУ можно настроить почтовые уведомления с помощью SMTP. Обновляемые ключи включают в себя: "smtp-server", "smtp-port", "source-email", "destination-emails" и "state_transition".

Для настройки почтовых уведомлений нужно выполнить следующие действия:

а) на узле виртуализированного ЦУ настроить требуемый адрес сервера SMTP для ключа "smtp-server":

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

Примечание — Для проверки обновленных значений в конфигурации виртуализированного ЦУ выполнить:

```
    # hosted-engine --get-shared-config smtp-server --type=broker \
    broker : smtp.example.com, type : broker
```

б) проверить конфигурация порта SMTP по умолчанию (порт 25):

```
    # hosted-engine --get-shared-config smtp-port –type=broker
    broker : 25, type : broker
```

в) указать почтовый адрес, с которого сервер SMTP будет отправлять уведомления. Можно указать только один адрес:

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

г) указать адрес, на котором будут приниматься почтовые уведомления. Для указания нескольких адресов использовать запятые:

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

Для проверки корректности параметров SMTP, настроенных для окружения виртуализированного ЦУ, изменить состояние высокой доступности на узле виртуализированного ЦУ и убедиться, что пришло почтовое уведомление. Возможно изменить состояние, например, переведя агента высокой доступности в режим обслуживания. Дополнительные сведения см. в п. 4.1.1.

4.1.3 Настройка резервирования слотов памяти для виртуализированного ЦУ на дополнительных хостах

В случае если необходимо выключить или выполнить миграцию СУСВ, объем памяти на узле виртуализированного ЦУ должен быть достаточным для перезапуска или миграции на этот узел СУСВ. Эту память можно зарезервировать на нескольких узлах виртуализированного ЦУ с помощью политики планирования. Перед выполнением запуска или миграции любых ВМ эта политика проверяет, останется ли достаточно памяти для запуска ВМ на указанном числе дополнительных узлов виртуализированного ЦУ.

Сведения о том, как добавить дополнительные узлы виртуализированного ЦУ в СУСВ, см. в п. 4.1.4.

Для настройки на дополнительных хостах слотов памяти, зарезервированных для виртуализированного ЦУ нужно:

а) нажать "Ресурсы → Кластеры" и выбрать кластер, в котором располагаются узлы виртуализированного ЦУ;

б) нажать кнопку Изменить;

в) перейти на вкладку "Политика планирования";

г) нажать кнопку + и выбрать "HeSparesCount";

д) ввести число дополнительных узлов виртуализированного ЦУ, на которых будет зарезервирован объем памяти, достаточный для запуска ВМ виртуализированного ЦУ;

е) нажать кнопку OK.

4.1.4 Добавление узлов виртуализированного ЦУ для СУСВ

Узлы виртуализированного ЦУ добавляются точно так же, как добавляются стандартные хосты, с дополнительным шагом по развертыванию хоста как узла виртуализированного ЦУ. Домен разделяемого хранилища обнаруживается автоматически, и узел можно использовать как запасной хост для размещения СУСВ при необходимости. Также стандартный хост можно прикрепить к окружению виртуализированного ЦУ, но на этих хостах невозможно размещать СУСВ. Для обеспечения высокой доступности машине диспетчера необходимо иметь не менее двух узлов виртуализированного ЦУ.

Предварительные условия для добавления узлов виртуализированного ЦУ для СУСВ:

– все узлы виртуализированного ЦУ должны располагаться в одном и том же кластере;

– Если узел виртуализированного ЦУ будет использоваться повторно, следует удалить существующую конфигурацию его виртуализированного ЦУ.

Порядок действий по добавлению узлов виртуализированного ЦУ для СУСВ:

а) на Портале администрирования нажать "Ресурсы → Хосты";

б) нажать кнопку Добавить;

в) сведения по настройке параметров дополнительных хостов см. в п. 3.5;

г) в выпадающем списке выбрать дата-центр и кластер хоста для нового хоста;

д) ввести "Имя" и "Адрес" нового хоста. Стандартный порт SSH – 22 – будет автоматически введен в соответствующем поле;

е) выбрать метод аутентификации, который диспетчер будет использовать при доступе к хосту:

– для аутентификации по паролю ввести пароль пользователя root;

– для аутентификации по открытому ключу скопировать ключ из поля "Открытый ключ SSH" в файл /root/.ssh/authorized_keys на хосте;

ж) перейти на вкладку "Виртуализированный ЦУ";

з) выбрать "Развернуть";

и) нажать кнопку OK.

4.1.4.1 Перенастройка существующего хоста в качестве узла виртуализированного ЦУ

Существующий стандартный хост в окружении виртуализированного ЦУ можно превратить в узел виртуализированного ЦУ, пригодного для размещения ВМ диспетчера.

Примечание — Во время установки или переустановки ОС хоста настоятельно рекомендуется предварительно открепить любые не относящиеся к ОС хранилища, прикрепленные к хосту, во избежание случайной инициализации дисков хранилища и возможной потери данных на них.

Последовательность действий по перенастройке существующего хоста в качестве узла виртуализированного ЦУ:

а) нажать "Ресурсы → Хосты" и выбрать хост;

б) нажать "Управление → Обслуживание" и нажать кнопку OK для подтверждения перевода хоста в режим обслуживания (рисунок 234);

в) нажать "Установка → Переустановить";

г) перейти на вкладку "Виртуализированный ЦУ" и в выпадающем списке выбрать "Развернуть";

д) нажать кнопку OK.

Хост будет переустановлен с конфигурацией виртуализированного ЦУ и затем будет помечен пиктограммой "корона" на Портале администрирования.

4.1.5 Загрузка СУСВ в режиме восстановления

В данном пункте описывается способ загрузки СУСВ в режим аварийного восстановления в случаях, когда ВМ не запускается:

а) подключиться к одному из узлов виртуализированного ЦУ (host_address – адрес хоста):

```
$ ssh root@host_address
```

б) перевести виртуализированный ЦУ в глобальный режим обслуживания:

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

в) проверить наличие уже выполняющегося экземпляра ВМ диспетчера:

```
# hosted-engine --vm-status
```

г) если экземпляр ВМ диспетчера уже выполняется, подключиться к ее хосту:

```
# ssh root@host_address
```

д) выключить ВМ, выполнив в консоли команду:

```
# hosted-engine --vm-shutdown
```

е) если ВМ не выключается, выполнить следующую команду:

```
# hosted-engine --vm-poweroff
```

ж) запустить ВМ диспетчера в режиме паузы:

```
# hosted-engine --vm-start-paused
```

з) настроить временный пароль VNC:

```
# hosted-engine --add-console-password
```

Данная команда выводит сведения, необходимые для выполнения входа на ВМ диспетчера с помощью консоли VNC.

и) войти в Систему ВМ диспетчера с помощью VNC. ВМ диспетчера по-прежнему на паузе, поэтому кажется зависшей;

к) возобновить работу ВМ диспетчера с помощью следующей команды, выполняемой на ее хосте:

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

Важно — После выполнения данной команды будет показано меню загрузчика. Войти в режим восстановления необходимо до того, как загрузчик

продолжит процесс обычной загрузки. Перед тем как выполнять данную команду, следует ознакомиться с описанием следующего шага по переходу в режим восстановления.

л) загрузить ВМ диспетчера в режиме восстановления;

м) отключить глобальный режим обслуживания:

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

Теперь на СУСВ можно выполнять работы по ее восстановлению.

4.1.6 Удаление хоста из окружения виртуализированного ЦУ

Чтобы удалить узел виртуализированного ЦУ из окружения, требуется перевести узел в режим обслуживания, свернуть установку узла и (опционально) удалить ее. После остановки служб высокой доступности и удаления файлов конфигурации виртуализированного ЦУ можно управлять узлом как обычным хостом.

Последовательность действий по удалению хоста из окружения виртуализированного ЦУ

а) на Портале администрирования нажать "Ресурсы → Хосты" и выбрать узел виртуализированного ЦУ;

б) нажать "Управление → Обслуживание" и далее нажать кнопку `OK`;

в) нажать "Установка → Переустановить";

г) перейти на вкладку "Виртуализированный ЦУ" и в выпадающем списке выбрать "Свернуть установку". Данное действие останавливает работу служб ovirt-ha-agent и ovirt-ha-broker и удаляет файл конфигурации виртуализированного ЦУ;

д) нажать кнопку `OK`;

е) опционально нажать кнопку `Удалить`: будет открыто окно с подтверждением удаления хостов.

ж) нажать кнопку `OK`.

4.1.7 Изменение полного доменного имени СУСВ в виртуализированном ЦУ

С помощью команды `ovirt-engine-rename` можно обновлять записи полного доменного имени (FQDN).

Утилитой проверяется, предоставляет ли СУСВ локальный ISO-образ или домен хранения данных: в этом случае предлагается пользователю выключить или перевести в режим обслуживания любую ВМ или домен хранения данных, подключенные к хранилищу, прежде чем продолжить операцию. Это гарантирует, что ВМ не потеряют связь со своими виртуальными дисками, а домены хранения ISO-образов не потеряют связь в процессе переименования.

Для изменения полного доменного имени нужно:

а) подготовить все записи DNS и другие необходимые записи для нового полного доменного имени;

б) обновить конфигурацию DHCP-сервера, если используется DHCP;

в) обновить имя хоста в СУСВ;

г) выполнить следующую команду:

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

д) при появлении запроса нажать клавишу `Enter`, чтобы остановить работу двигателя:

```
During execution engine service will be stopped (OK, Cancel)
[OK]:
```

е) при появлении следующего запроса ввести новое полное доменное имя для СУСВ и нажать `Enter`:

```
New fully qualified server name:new_engine_fqdn
```

В результате запись полного доменного имени (FQDN) будет изменена.

4.2 Резервные копии и миграция

В данной главе рассмотрен процесс создания резервных копий СУСВ и восстановление СУСВ из резервных копий.

4.2.1 Обзор создания резервных копий СУСВ

Для регулярного резервного копирования СУСВ необходимо использовать утилиту engine-backup. Утилита создает резервные копии БД СУСВ и файлов конфигурации в одном файле, и ее можно запускать без прерывания работы службы ovirt-engine.

4.2.1.1 Синтаксис команды engine-backup

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

```
# engine-backup --mode=backup
# engine-backup --mode=restore
```

Эти два режима можно расширить набором параметров, позволяющих уточнить область данных для резервного копирования, а также указать различные учетные данные для БД СУСВ. Полный список параметров и их назначение можно просмотреть, выполнив команду:

```
engine-backup --help
```

Базовые параметры команды engine-backup:

--mode – указывает режим выполнения команды: операция создания резервной копии или операция восстановления из резервной копии. Доступные параметры: backup (по умолчанию), restore и verify. Для операций verify или restore необходимо также указать параметр mode;

--file – указывает путь и имя файла (например, file_name.backup), в котором будет сохранена резервная копия в режиме создания резервных копий, и из которого будут читаться данные в режиме восстановления (по умолчанию – /var/lib/ovirt-engine-backup/);

--log – указывает путь и имя файла (например, log_file_name), в который будет записываться журнал операции создания или восстановления резервной копии (по умолчанию – /var/log/ovirt-engine-backup/);

--scope – указывает область данных, включаемых в создание или восстановление резервной копии. Возможны четыре параметра:

– all (по умолчанию) — для создания резервной копии или восстановления всех баз данных и данных конфигураций;
– files — для создания резервной копии или восстановления только файлов Системы;
– db — для создания резервной копии или восстановления только БД СУСВ;
– dwhdb — для создания резервной копии или восстановления только БД хранилища данных.

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

Параметры БД СУСВ доступны только при использовании команды `engine-backup` в режиме restore. Синтаксис параметров, описанный ниже, применяется при восстановлении БД СУСВ. Те же параметры существуют для восстановления БД хранилища данных. Синтаксис параметров для хранилища данных см. в выводе команды:

```
engine-backup –help
```

--provision-db – создает БД PostgreSQL, в которую будет восстанавливаться резервная копия БД СУСВ. Этот параметр является обязательным при восстановлении из резервной копии на удаленном хосте или в свежей установке, не имеющей уже настроенной БД PostgreSQL. При использовании в режиме восстановления к этому параметру по умолчанию добавляется параметр —restore-permissions;

--provision-all-databases – создает БД для всех дампов памяти, включенных в архив. Если параметр включен, это является значением по умолчанию;

--change-db-credentials – дает возможность указать другие учетные данные при восстановлении БД СУСВ с учетными данными, отличными от сохраненных непосредственно в архиве. Дополнительные параметры, необходимые данному параметру, см. в выводе команды `backup –help`;

--restore-permissions или —no-restore-permissions – восстанавливает или не восстанавливает полномочия пользователей БД. Один из этих параметров является требуемым при восстановлении из резервной копии. При использовании параметра --provision-* в режиме восстановления --restore-permissions применяется по умолчанию.

Примечание — Если в резервной копии содержатся предоставления полномочий дополнительным пользователям БД, то при восстановлении с использованием параметров --restore-permissions и --provision-db (или --provision-dwh-db) создаются дополнительные пользователи со случайно созданными паролями. Если дополнительным пользователям требуется доступ к восстановленной Системе, то эти пароли необходимо сменить вручную. См. дополнительную информацию по ссылке.

4.2.1.2 Создание резервных копий с помощью команды engine-backup

Резервные копии СУСВ при активной СУСВ можно создавать с помощью команды `engine-backup`.

Для указания, что именно требуется поместить в архив, добавляют один из следующих аргументов к параметру --scope:

– all – полная резервная копия всех БД и файлов конфигурации СУСВ. Это является значением по умолчанию для параметра —scope;
– files – резервная копия только файлов в Системе;
– db – резервная копия только БД СУСВ;
– dwhdb – резервная копия только БД хранилища данных;
– cinderlibdb – резервная копия только БД Cinderlib;
– grafanadb – резервная копия только БД Grafana.

Параметр --scope можно указывать несколько раз.

Команду `engine-backup` можно настроить на создание резервной копии для дополнительных файлов. При восстановлении эта команда восстанавливает все файлы из архива.

Примечания:

– Для восстановления из резервной копии в свежей установке СУСВ недостаточно только архива с БД СУСВ, также нужен доступ к файлам конфигурации. При указании области действия, отличной от all, необходимо также указать --scope=files, либо создать резервную копию файловой системы.

– Полные сведения о команде `engine-backup` можно получить в выводе команды `engine-backup –help` на машине СУСВ.

Последовательность действий для создания резервных копий с помощью команды `engine-backup`:

а) войти в Систему на машине СУСВ;
б) создать резервную копию:

```
# engine-backup
```

Следующие параметры применяются по умолчанию: --scope=all; --mode=backup.

Эта команда создает резервную копию в /var/lib/ovirt-engine-backup/file_name.backup и файл журнала /var/log/ovirt-engine-backup/log_file_name.

Для сохранения окружения используется файл архива file_name.tar.

В примерах ниже показываются несколько разных сценариев создания резервных копий.

Пример 1. Создание полной резервной копии:

```
# engine-backup
```

Пример 2. Резервная копия БД СУСВ:

```
# engine-backup --scope=files --scope=db
```

Пример 3. Резервная копия БД хранилища данных:

```
# engine-backup --scope=files --scope=dwhdb
```

Пример 4. Добавление в архив конкретных файлов:

а) создать каталог для хранения специальных параметров конфигурации команды `engine-backup`:

```
# mkdir -p /etc/ovirt-engine-backup/engine-backup-config.d
```

б) создать в новом каталоге текстовый файл с именем ntp-chrony.sh и следующим содержимым:

```
BACKUP_PATHS="${BACKUP_PATHS}
/etc/chrony.conf
/etc/ntp.conf
/etc/ovirt-engine-backup"
```

в) при запуске команды `engine-backup` использовать –scope=files.

В создание и восстановление из резервной копии входят /etc/chrony.conf, /etc/ntp.conf и /etc/ovirt-engine-backup.

4.2.1.3 Восстановление из резервной копии с помощью команды engine-backup

Восстановление из резервной копии при помощи команды `engine-backup` требует большего числа шагов, чем создание резервной копии, в

зависимости от места назначения восстановления. Например, команду `engine-backup` можно использовать для восстановления резервных копий в свежую установку РОСА Виртуализация поверх уже имеющейся установки РОСА Виртуализация, а также использовать локальные или удаленные БД.

4.2.1.3.1 Восстановление из резервной копии в свежую установку

Команду `engine-backup` можно использовать для восстановления из резервной копии в свежую установку диспетчера РОСА Виртуализация. Нижеописанная процедура должна выполняться на машине с установленной хост-системой, но где еще не запускалась команда `engine-setup`. Данная процедура предполагает, что с машины, на которой будет восстановлена резервная копия, есть доступ к файлам с резервной копией.

Последовательность действий для восстановления из резервной копии:

а) выполнить вход в Систему на машине диспетчера. Если восстанавливается БД СУСВ на удаленный хост, то необходимо также войти в Систему на этом хосте и выполнить там требуемые действия. Аналогичным образом при восстановлении БД хранилища данных на удаленный хост на этом хосте необходимо войти в Систему и выполнить требуемые действия;

б) выполнить полное восстановление либо только восстановление резервной копии БД:

– Полное восстановление:

```
# engine-backup --mode=restore --file=file_name \
--log=log_file_name --provision-db
```

При использовании параметра `--provision-*` в режиме восстановления параметр `--restore-permissions` применяется по умолчанию.

Если во время полного восстановления также восстанавливается и хранилище данных, указать дополнительную БД:

```
# engine-backup --mode=restore --file=file_name \
--log=log_file_name --provision-db -- provision-dwh-db
```

– При восстановлении резервной копии только БД восстановить файлы конфигурации и архив БД:

```
# engine-backup --mode=restore --scope=files --scope=db \
--file=file_name -- log=log_file_name --provision-db
```

В примере ниже восстанавливается резервная копия БД диспетчера.

```
# engine-backup --mode=restore --scope=files --scope=dwhdb \
--file=file_name -- log=log_file_name --provision-dwh-db
```

В примере ниже восстанавливается резервная копия БД хранилища данных. В случае успеха показывается следующее сообщение:

```
You should now run engine-setup. Done.
```

в) для создания конфигурации восстановленного диспетчера запустить команду и следовать подсказкам:

```
# engine-setup
```

В результате СУСВ будет восстановлен в версии, сохраненной в резервной копии.

4.2.1.3.2 Восстановление из резервной копии с перезаписью существующей установки

Команда `engine-backup` может восстановить резервную копию на машину, где уже была установлена и настроена СУСВ. Это удобно в ситуациях, когда сначала была создана резервная копия окружения, затем в окружение были внесены изменения, а далее необходимо эти изменения отменить с восстановлением окружения.

Изменения, внесенные после создания резервной копии, такие как добавление или удаление хостов, не будут присутствовать в восстановленном окружении.

Последовательность действий для выполнения восстановления из резервной копии с перезаписью существующей установки

а) войти в Систему на машине СУСВ;

б) удалить файлы конфигурации и очистить БД, связанную с диспетчером, выполнив команду:

```
# engine-cleanup
```

Примечание — Команда `engine-cleanup` только очищает БД СУСВ; БД не будет удалена из Системы, а также не будут удалены пользователи, владеющие этой БД.

в) восстановление полной резервной копии или резервной копии только БД. Нет необходимости создавать новую БД или указывать учетные записи, т. к. пользователи и БД уже существуют.

– Восстановление из полной резервной копии:

```
# engine-backup --mode=restore --file=file_name \
--log=log_file_name --restore- permissions
```

– Восстановление только БД с помощью восстановления файлов конфигурации и архива БД:

```
# engine-backup --mode=restore --scope=files --scope=db \
--scope=dwhdb -- file=file_name --log=log_file_name --
restore-permissions
```

Примечание — Чтобы восстановить только БД диспетчера (если, например, БД хранилища данных расположена на другой машине), можно опустить параметр --scope=dwhdb.

В случае успеха будет показано следующее сообщение:

```
You should now run engine-setup.
Done.
```

г) повторная настройка диспетчера:

```
# engine-setup
```

4.2.1.3.3 Восстановление из резервной копии с использованием других учетных данных

Команда `engine-backup` может восстановить резервную копию на машину, где СУСВ уже ранее была установлена и настроена, в ситуации, когда данные учетных записей БД в резервной копии отличаются от данных, используемых на машине, где будет восстановлена эта резервная копия. Это удобно, если в одной Системе нужно развернуть из резервной копии установку, созданную и настроенную в другой Системе.

Примечание — При восстановлении из резервной копии с перезаписью существующей установки перед запуском команды `engine-backup` необходимо выполнить команду `engine-cleanup` для очистки существующей установки. Команда `engine-cleanup` только очищает БД СУСВ, но не удаляет ее из Системы и не удаляет пользователей-владельцев этой БД, поэтому нет необходимости создавать новую БД или указывать данные учетных записей. Тем не менее, если данные учетной записи владельца БД неизвестны, их нужно изменить до того, как выполнять восстановление из резервной копии.

Последовательность действий по восстановлению из резервной копии с использованием других учетных данных:

а) выполнить вход в Систему на машине СУСВ;

б) для удаления файлов конфигурации диспетчера и очистки БД СУСВ запустить следующую команду и следовать подсказкам:

```
# engine-cleanup
```

в) сменитm пароль владельца БД engine, если данные его учетной записи неизвестны:

1) войти в командную строку postgresql:

```
# su – postgres -c 'psql'
```

2) сменить пароль пользователя-владельца БД engine:

```
postgres=# alter role user_name encrypted password
'new_password';
```

В случае необходимости повторить эти действия для пользователя-владельца БД ovirt_engine_history.

г) восстановить полный архив или архив только с БД с параметром --change-db-credentials для передачи учетных данных новой БД. Значение параметра database_location для БД, локальной относительно диспетчера, равно "localhost".

Примечание – В следующем примере параметр --*password используется для каждой БД без указания пароля, в результате этого для каждого пароля БД выводится запрос командной строки.

Как вариант, для каждой БД можно использовать параметр --*passfile=password_file для защищенной передачи паролей утилите engine-backup без необходимости вводить пароли в интерактивном запросе командной строки.

Для восстановления полной резервной копии выполняют:

```
# engine-backup --mode=restore --file=file_name --
log=log_file_name \
--change-db- credentials --db-host=database_location –db \
name=database_name --db-user=engine --db-password --no-
restore-permissions
```

Если в составе полного восстановления также восстанавливается БД хранилища данных, то необходимо включить данные учетных записей для дополнительной БД:

```
    # engine-backup --mode=restore --file=file_name --
log=log_file_name \
    --change-db-credentials --db-host=database_location \
    --dbname=database_name --db-user=engine --db-password \
    --change-dwh-db-credentials --dwh-db-host=database_location
\
    --dwh-db- name=database_name --dwh-db-
user=ovirt_engine_history \
    --dwh-db-password --no-restore-permissions
```

Восстановление только резервной копии БД с помощью восстановления файлов конфигурации и архива БД:

```
    # engine-backup --mode=restore --scope=files --scope=db \
    --file=file_name --log=log_file_name --change-db-credentials
\
    --db-host=database_location --db- name=database_name \
    --db-user=engine --db-password --no-restore-permissions
```

В примере ниже восстанавливается резервная копия БД диспетчера.

```
    # engine-backup --mode=restore --scope=files --scope=dwhdb \
    --file=file_name --log=log_file_name --change-dwh-db-
credentials \
    --dwh-db-host=database_location --dwh-db-name=database_name
\
    --dwh-db-user=ovirt_engine_history –dwh-db-password \
    --no-restore-permissions
```

В примере ниже восстанавливается резервная копия БД хранилища данных. В случае успеха показывается следующее сообщение:

```
    You should now run engine-setup.
    Done.
```

Для повторной настройки межсетевого экрана и проверки корректности настройки службы ovirt-engine следует выполнить следующую команду:

```
    # engine-setup
```

4.2.1.4 Создание резервной копии и восстановление из резервной копии виртуализированного ЦУ

Для виртуализированного ЦУ также можно создавать резервные копии и восстанавливать на их базе виртуализированный ЦУ в новом окружении. Эти действия выполняют для таких задач, как миграция окружений в новые домены хранилищ виртуализированного ЦУ с другими типами хранилищ.

При указании файла резервной копии во время развертывания архив восстанавливается на новой СУСВ с новым доменом хранилища виртуализированного ЦУ. Старый диспетчер удаляется, а старый домен хранилища переименовывается и может быть удален вручную после проверки корректности работы нового окружения. Настоятельно рекомендуется выполнять развертывание на свежем хосте; если в архиве резервной копии окружения присутствовал хост, использованный для развертывания, он будет удален из восстановленной БД для избегания конфликтов в новом окружении. При развертывании на новом хосте новому хосту нужно присвоить новое имя. Повторное использование имени существующего хоста, включенного в резервную копию, может привести к конфликтам в новом окружении.

4.2.1.4.1 Создание резервной копии виртуализированного ЦУ

Последовательность действий по созданию и восстановлению резервной копии включает в себя следующие ключевые шаги:

а) создать резервную копию исходной СУСВ с помощью утилиты engine-backup;

б) развернуть новый виртуализированный ЦУ и восстановить СУСВ из резервной копии;

в) подключить репозитории СУСВ на новой СУСВ;

г) переустановить узлы виртуализированного ЦУ для обновления их конфигурации;

д) удалить домен хранилищ старого виртуализированного ЦУ.

Данная процедура предполагает, что у администратора есть доступ к исходному диспетчеру и права на внесение изменений.

4.2.1.4.2 Предварительные требования для создания резервной копии виртуализированного ЦУ

Предварительные требования для создания резервной копии виртуализированного ЦУ:

– Полное доменное имя, подготовленное для СУСВ и хоста. В DNS должны быть настроены записи для прямого и обратного поиска. Полное доменное имя новой СУСВ должно совпадать с именем исходной СУСВ.

– Уровень совместимости ЦОД должен быть настроен на последнюю версию для обеспечения совместимости с обновленной версией хранилища.

– В окружении должен присутствовать минимум один обычный хост. Этот хост (а также любые другие обычные хосты) будет оставаться активным для выполнения роли диспетчера пула хранилища (SPM) и размещения любых выполняющихся ВМ. Если обычный хост еще не является диспетчером пула хранилища, следует передать эту роль до начала создания резервной копии, выбрав обычный хост и нажав "Управление → Выбрать как диспетчер пула хранилища (SPM)".

В случае отсутствия доступных обычных хостов есть два способа их добавить:

– Удалить конфигурацию виртуализированного ЦУ на узле (но не удалять узел из окружения) (см. п. 4.1.6).

– Добавить новый обычный хост (см. п. 4.1.4).

4.2.1.4.3 Создание резервной копии исходной СУСВ

Резервная копия исходной СУСВ создается с помощью команды `engine-backup` и копирования файла архива резервной копии в отдельное местоположение, чтобы к нему сохранялся доступ в любой момент работы.

Дополнительные сведения о параметрах `engine-backup --mode=backup` см. в п. 4.2.1.2.

Последовательность действий по созданию резервной копии исходной СУСВ

а) выполнить вход в Систему на одном из узлов виртуализированного ЦУ и переключить окружение в глобальный режим обслуживания:

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

б) выполнить вход в Систему на исходной СУСВ и остановить службу ovirt-engine:

```
# systemctl stop ovirt-engine
# systemctl disable ovirt-engine
```

Примечание – Хотя остановка работы исходной СУСВ не является обязательной, это рекомендуется сделать, т. к. это обеспечивает защиту окружения от

внесения изменений после создания резервной копии. Кроме того, это предотвращает возможность одновременного управления существующими ресурсами со стороны и исходной и новой СУСВ.

в) выполнить команду `engine-backup`, указав имя создаваемого файла резервной копии и имя файла создаваемого журнала процесса создания резервной копии:

```
# engine-backup --mode=backup --file=file_name --
log=log_file_name
```

г) скопировать файлы на внешний сервер. В примере ниже storage.example.com является полным доменным именем сервера сетевого хранилища, на котором будет храниться резервная копия до того момента, когда она понадобится, а /backup/ — это любая предназначенная папка или путь:

```
# scp -p file_name log_file_name
storage.example.com:/backup/
```

д) выполнить вход в Систему на одном из узлов виртуализированного ЦУ и выключить исходную СУСВ:

```
# hosted-engine --vm-shutdown
```

После создания резервной копии СУСВ требуется развернуть новый виртуализированный ЦУ и восстановить резервную копию на новой ВМ.

4.2.1.4.4 Восстановление резервной копии в новом виртуализированном ЦУ

Для восстановления резервной копии диспетчера во время развертывания нужно запустить сценарий hosted-engine на новом хосте и использовать параметр --restore-from-file=*path/to/file_name*.

Примечания:

— Если используется хранилище iSCSI, и цель iSCSI фильтрует подключения согласно списку управления доступом (ACL) инициатора, то развертывание может закончиться неудачно с ошибкой STORAGE_DOMAIN_UNREACHABLE. Для предотвращения этой ошибки необходимо обновить конфигурацию iSCSI до начала развертывания виртуализированного ЦУ:

— Если выполняется повторное развертывание на уже существующем хосте, то необходимо обновить параметры инициатора iSCSI хоста в файле /etc/iscsi/initiatorname.iscsi. Типизированное имя (IQN) инициатора должно

совпадать с именем, ранее отображенным на цель iSCSI, либо необходимо его обновить до нового IQN, если это применимо.

– При развертывании на свежем хосте необходимо обновить конфигурацию цели iSCSI для принятия подключений с этого хоста.

Следует обратить внимание, что IQN можно обновлять либо на стороне хоста (инициатор iSCSI), либо на стороне хранилища (цель iSCSI).

Последовательность действий по восстановлению резервной копии в новом виртуализированном ЦУ

а) скопировать файл резервной копии на новый хост. В примере ниже host.example.com является полным доменным именем хоста, а /backup/ — это любая предназначенная папка или путь:

```
# scp -p file_name host.example.com:/backup/
```

б) войти в Систему на новом хосте;

в) чтобы избежать обрыва сеанса в случае неполадок с сетью или терминалом, для запуска сценария использовать оконный менеджер tmux, для запуска которого использовать следующую команду в консоли:

```
# tmux
```

г) запустить сценарий hosted-engine, указав путь до файла с резервной копией:

```
# hosted-engine --deploy
–restore-from-file=/backup/file_name
```

Чтобы остановить работу сценария и прервать развертывание в любой момент, можно использовать клавиши `CTRL+D`.

д) чтобы начать развертывание, выбрать "Yes";

е) настроить сеть. Сценарий обнаружит сетевые контроллеры, пригодные для использования в качестве моста управления окружением;

ж) при необходимости использования настраиваемого программно-аппаратного устройства для установки ВМ указать путь к архиву OVA, иначе оставить поле пустым;

з) ввести пароль root для СУСВ;

и) ввести открытый ключ SSH, с помощью которого можно будет выполнить вход в Систему диспетчера в качестве пользователя root, и указать, нужно ли разрешать доступ с использованием SSH для root;

к) ввести конфигурацию памяти и ЦП для ВМ;

л) указать MAC-адрес для ВМ диспетчера или принять случайно созданный адрес. Если ВМ должна получать адрес IP с помощью DHCP, убедиться в наличии действительного зарезервированного DHCP для этого MAC-адреса. Сценарий развертывания не настраивает сервер DHCP;

м) указать сетевые параметры ВМ. При указании статического IP указать IP диспетчера;

Примечание — Статический IP должен принадлежать к той же самой подсети, что и хост. Если, например, хост располагается в "10.1.1.0/24", то IP ВМ СУСВ должен располагаться в том же диапазоне подсети ("10.1.1.1-254/24").

н) указать, нужно ли добавлять запись ВМ диспетчера и запись базового хоста в файл /etc/hosts на ВМ, и убедиться в разрешаемости имен хостов;

о) указать имя и номер порта TCP сервера SMTP, почтовый адрес для отсылки уведомлений и список адресов-получателей этих сообщений через запятую;

п) указать пароль пользователя admin@internal для доступа к Порталу администрирования. Сценарий создаст ВМ.

Примечание — Если в связи с отсутствующей требуемой сетью или аналогичной проблемой хост перейдет в нерабочее состояние, процесс развертывания приостановится и будет выведено сообщение, аналогичное следующему:

```
     [ INFO ] You can now connect to https://<host name>:6900/ovirt-
engine/ and check the status of this host and eventually remediate it,
please continue only when the host is listed as 'up'
     [ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : include_tasks] [
INFO ] ok: [localhost]
     [ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : Create temporary
lock file] [ INFO ] changed: [localhost]
     [ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : Pause execution
until
     /tmp/ansible.<random>_he_setup_lock is removed, delete it once
ready to proceed]
```

Приостановка процесса дает возможность администратору:

– подключиться к Порталу администрирования с помощью предоставленного URL;

– оценить ситуацию, понять, почему хост в нерабочем состоянии, и исправить все, что необходимо исправить. Если, например, данное развертывание было восстановлено из резервной копии, и в архив

были включены сети, требуемые для кластера хоста, то нужно настроить сети, прикрепив необходимые сетевые контроллеры хоста к этим сетям;

– как только все будет исправлено, и хост получит статус "работоспособен", удалить временный файл блокировки, указанный в системном сообщении, приведенном выше;

р) настроить тип используемого хранилища:

1) для NFS указать версию, полный адрес и путь до хранилища, а также любые параметры монтирования;

Примечание — Не следует использовать точку монтирования старого домена хранилища виртуализированного ЦУ для нового домена хранилища, т. к. присутствует риск потери данных.

2) указать сведения о портале для iSCSI и выбрать цель и LUN из списка автоматически обнаруженных. Во время развертывания можно выбрать только одну цель iSCSI, но для подключения всех порталов из одной группы поддерживается механизм доступа по нескольким путям;

Примечание — Для возможности указания более одной цели iSCSI необходимо включить использование механизма доступа по нескольким путям до начала развертывания виртуализированного ЦУ.

3) для хранилища Gluster указать полный адрес и путь до хранилища вместе с любыми параметрами монтирования;

Примечания:

– Не следует использовать точку монтирования строго домена хранилища виртуализированного ЦУ для нового домена хранилища, т. к. присутствует риск потери данных ВМ.

– Поддерживаются только хранилища Gluster с типом replica 1 и replica 3. Необходимо убедиться, что том настроен следующим образом:

```
     gluster volume set VOLUME_NAME group virt
     gluster volume set VOLUME_NAME performance.strict-o-direct on
gluster volume set VOLUME_NAME network.remote-dio off gluster volume
set VOLUME_NAME storage.owner-uid 36
     gluster volume set VOLUME_NAME storage.owner-gid 36 gluster
volume set VOLUME_NAME network.ping-timeout 30
```

4) для Fibre Channel выбрать LUN из списка автоматически обнаруженных. Адаптеры шины хоста должны быть заранее настроены и подключены, а LUN не должен содержать никаких существующих

данных. Сведения о том, как повторно использовать уже существующий LUN, см. в п. 3.6.5.8;

с) указать размер диска диспетчера;

т) сценарий продолжит свое выполнение до завершения развертывания; в процессе развертывания будут изменены ключи SSH диспетчера;

у) чтобы разрешить клиентским машинам доступ к новому диспетчеру без ошибок, связанных с SSH, удалить запись исходного диспетчера из файла .ssh/known_hosts на любой из клиентских машин, ранее имевших доступ к исходному диспетчеру;

ф) после завершения развертывания выполнить вход в Систему на ВМ новой СУСВ и подключить необходимые репозитории.

4.2.1.4.5 Повторная установка хостов

Действия по переустановке хостов РОСА Виртуализация на Портале администрирования включают в себя остановку и перезапуск работы хостов.

Примечание — Настоятельно рекомендуется перед началом установки или переустановки ОС хостов отсоединить любые существующие, не относящиеся к ОС хранилища, прикрепленные к хостам. Это позволит избежать случайной инициализации этих дисков и связанной с этим возможной потери данных.

Предварительные требования для повторной установки хостов:

– Если в кластере включена возможность миграции, ВМ могут автоматически мигрировать на любой другой хост в кластере. Соответственно, следует переустанавливать хост в момент его относительно низкой нагрузки.

– Необходимо убедиться в том, что объем памяти в кластере достаточен для выполнения обслуживания хостов кластера. При нехватке памяти в кластере миграция ВМ зависнет и затем завершится сбоем. Для снижения потребления памяти перед помещением хоста в режим обслуживания рекомендуется выключить некоторые или все ВМ.

– Перед началом переустановки нужно убедиться в том, что в кластере находится более одного хоста. Не следует пытаться начать переустановку всех хостов одновременно. Один хост всегда должен быть доступен для выполнения задач диспетчера пула хранилища (SPM).

Последовательность действий по повторной установка хостов:

а) нажать "Ресурсы → Хосты" и выбрать хосты;

б) выбрать "Управление → Обслуживание" и нажать кнопку OK;

в) выбрать "Установка → Переустановить";

г) в открывшемся окне "Установить хост" перейти на вкладку "Виртуализированный ЦУ" и в выпадающем списке выбрать "Развернуть";

д) для переустановки хоста нажать кнопку OK.

После окончания процесса переустановки хоста, когда статус хоста снова будет "Работоспособен", можно выполнить миграцию ВМ обратно на хост.

Примечание — После выполнения регистрации хоста РОСА Виртуализация в СУСВ статус этого хоста на Портале администрирования может ошибочно показывать "Сбой установки". Следует нажать "Управление→Активировать", и статус хоста сменится на "Работоспособен", а хост будет готов к использованию.

После переустановки узлов виртуализированного ЦУ статус нового окружения можно проверить, выполнив на одном из узлов следующую команду:

```
# hosted-engine –vm-status
```

Во время восстановления старый домен хранилища виртуализированного ЦУ был переименован, но не был удален на случай, если при восстановлении случится сбой. После подтверждения того, что окружение работает нормально, старый домен можно удалить.

4.2.1.4.6 Восстановление виртуализированного ЦУ из существующей резервной копии

Если виртуализированный ЦУ становится недоступен в связи с неустранимыми проблемами, его можно восстановить в новом окружении с помощью резервной копии, созданной до того, как начались проблемы, если такая резервная копия доступна.

При указании файла резервной копии во время развертывания этот архив восстанавливается на новой ВМ и с новым доменом хранилища виртуализированного ЦУ. Старый диспетчер удаляется, а старый домен хранилища виртуализированного ЦУ переименовывается и удаляется вручную после проверки корректности работы нового окружения.

Настоятельно рекомендуется выполнять развертывание на свежем хосте; если хост, используемый для развертывания, существовал в окружении, для которого создавалась резервная копия, то он будет удален из восстановленной БД во избежание конфликтов в новом окружении. Если развертывание выполняется на новом хосте, этому хосту необходимо присвоить уникальное имя. Повторное использование имени хоста, включенного в резервную копию, может привести к конфликтам в новом окружении.

Последовательность восстановления виртуализированного ЦУ состоит из следующих ключевых действий:

а) Развертывание нового виртуализированного ЦУ и восстановление резервной копии.

б) Подключение репозиториев СУСВ на новой ВМ СУСВ.

в) Переустановка узлов виртуализированного ЦУ для обновления их конфигурации.

г) Удаление старого домена хранилища виртуализированного ЦУ.

Данная процедура подразумевает, что у администратора нет доступа к исходному диспетчеру и что у нового хоста есть доступ к файл резервной копии.

Предварительные требования для восстановления виртуализированного ЦУ:

– Полное доменное имя, подготовленное для СУСВ и хоста. В DNS должны быть настроены записи для прямого и обратного поиска.

– Полное доменное имя нового диспетчера должно совпадать с именем исходного диспетчера.

4.2.1.4.7 Восстановление из резервной копии на новом виртуализированном ЦУ

Для восстановления диспетчера из резервной копии во время развертывания нужно запустить на новом хосте сценарий hosted-engine с помощью параметра --restore-from-file=*path/to/file_name*.

Примечание — Если используется хранилище iSCSI и цель iSCSI фильтрует подключения согласно списку управления доступом (ACL) инициатора, то развертывание может закончиться неудачно с ошибкой "STORAGE_DOMAIN_UNREACHABLE". Для предотвращения этой ошибки необходимо обновить конфигурацию iSCSI до начала развертывания виртуализированного ЦУ:

– Если выполняется повторное развертывание на уже существующем хосте, то необходимо обновить параметры инициатора iSCSI хоста в файле /etc/iscsi/initiatorname.iscsi. Типизированное имя (IQN) инициатора должно совпадать с именем, ранее отображенным на цель iSCSI, либо необходимо его обновить до нового IQN, если это применимо.

– При развертывании на свежем хосте необходимо обновить конфигурацию цели iSCSI для принятия подключений с этого хоста.

Следует обратить внимание, что IQN можно обновлять либо на стороне хоста (инициатор iSCSI), либо на стороне хранилища (цель iSCSI).

Последовательность действий по восстановлению из резервной копии на новом виртуализированном ЦУ:

а) скопировать файл резервной копии на новый хост. В примере ниже host.example.com — это полное доменное имя хоста, а /backup/ — любая назначенная папка или путь:

```
# scp -p file_name host.example.com:/backup/
```

б) выполнить вход в Систему на новом хосте;

в) чтобы избежать обрыва сеанса в случае неполадок с сетью или терминалом, для запуска сценария использовать оконный менеджер tmux. Запустить tmux командой:

```
# tmux
```

г) запустить сценарий hosted-engine, указав путь до файла с резервной копии:

```
# hosted-engine --deploy
--restore-from-file=backup/file_name
```

Чтобы остановить работу сценария и прервать развертывание в любой момент, можно использовать клавиши `CTRL+D`.

д) чтобы начать развертывание, выбрать "Yes";

е) настроить сеть. Сценарий обнаруживает сетевые контроллеры, пригодные к использованию в качестве моста для управления окружением;

ж) при необходимости использования настраиваемого программно-аппаратного устройств для установки ВМ, указать путь к архиву OVA. В противном случае оставить поле пустым;

з) ввести пароль root для диспетчера;

и) ввести открытый ключ SSH, с помощью которого можно будет выполнить вход в Систему диспетчера в качестве пользователя root, и указать, нужно ли разрешать доступ с использованием SSH для root;

к) ввести конфигурацию памяти и ЦП для ВМ;

л) указать MAC-адрес для ВМ диспетчера или принять случайно созданный адрес. Если ВМ должна получать IP-адрес с помощью DHCP, убедиться в наличии действительного зарезервированного DHCP для этого MAC-адреса. Сценарий развертывания не настраивает сервер DHCP;

м) указать сетевые параметры ВМ. При указании статического IP указать IP СУСВ;

Примечание — Статический IP должен принадлежать к той же самой подсети, что и хост. Если, например, хост располагается в "10.1.1.0/24", то IP ВМ СУСВ должен располагаться в том же диапазоне подсети ("10.1.1.1-254/24").

н) указать, нужно ли добавлять запись ВМ диспетчера и запись базового хоста в файл /etc/hosts на ВМ; убедиться в разрешаемости имен хостов;

о) указать имя и номер порта TCP сервера SMTP, почтовый адрес для отсылки уведомлений и список адресов-получателей этих сообщений через запятую;

п) указать пароль пользователя admin@internal для доступа к Порталу администрирования. Сценарий создаст ВМ.

Примечание — Если в связи с отсутствующей требуемой сетью или аналогичной проблемой хост перейдет в нерабочее состояние, процесс развертывания приостановится и будет выведено сообщение, аналогичное следующему:

```
      [ INFO  ] You can now connect to https://<host name>:6900/ovirt-
engine/ and check the status of this host and eventually remediate it,
please continue only when the host is listed as 'up'
      [ INFO  ] TASK [ovirt.ovirt.hosted_engine_setup : include_tasks] [
INFO  ] ok: [localhost]
      [ INFO  ] TASK [ovirt.ovirt.hosted_engine_setup : Create temporary
lock file] [ INFO  ] changed: [localhost]
      [ INFO  ] TASK [ovirt.ovirt.hosted_engine_setup : Pause execution until
      /tmp/ansible.<random>_he_setup_lock is removed, delete it once ready
to proceed]
```

Приостановка процесса дает возможность администратору:

– Подключиться к Порталу администрирования с помощью предоставленного URL.

– Оценить ситуацию, понять, почему хост в нерабочем состоянии, и исправить все, что необходимо исправить. Если, например, данное развертывание было восстановлено из резервной копии, и в архив были включены сети, требуемые для кластера хоста, то нужно настроить сети, прикрепив необходимые сетевые контроллеры хоста к этим сетям.

– Как только все будет починено, и хост получит статус "работоспособен", удалить временный файл блокировки, указанный в системном сообщении, приведенном выше. Процесс развертывания продолжается.

р) выбрать тип используемого хранилища:

– для NFS указать версию, полный адрес и путь до хранилища, а также любые параметры монтирования.

Примечание — Не следует использовать точку монтирования старого домена хранилища виртуализированного ЦУ для нового домена, т. к. существует риск потери данных ВМ.

– указать сведения о портале для iSCSI и выбрать цель и LUN из списка автоматически обнаруженных. Во время развертывания можно выбрать только одну цель iSCSI, но для подключения всех порталов из одной группы поддерживается механизм доступа по нескольким путям.

Примечание — Для возможности указания более одной цели iSCSI необходимо включить использования механизма доступа по нескольким путям до начала развертывания виртуализированного ЦУ.

– для хранилища Gluster указать полный адрес и путь до хранилища, вместе с любыми параметрами монтирования.

Примечания:

– Не следует использовать точку монтирования старого домена хранилища виртуализированного ЦУ для нового домена, т. к. существует риск потери данных ВМ

– Поддерживаются только хранилища Gluster с типом replica 1 и replica 3. Убедитесь, что том настроен следующим образом:

```
     gluster volume set VOLUME_NAME group virt
     gluster volume set VOLUME_NAME performance.strict-o-direct on gluster
volume set VOLUME_NAME network.remote-dio off gluster volume set
VOLUME_NAME storage.owner-uid 36
     gluster volume set VOLUME_NAME storage.owner-gid 36 gluster volume
set VOLUME_NAME network.ping-timeout 30
```

– Для Fibre Channel выбрать LUN из списка автоматически обнаруженных. Адаптеры шины хоста должны быть заранее настроены и подключены, а LUN не должен содержать никаких существующих данных.

с) указать размер диска диспетчера. Сценарий продолжит свое выполнение до завершения развертывания.

т) В процессе развертывания будут изменены ключи SSH диспетчера. Чтобы разрешить клиентским машинам доступ к новому диспетчеру без ошибок, связанных с SSH, удалить запись исходного диспетчера из файла

.ssh/known_hosts на любой из клиентских машин, ранее имевших доступ к исходному диспетчеру.

у) После завершения развертывания выполнить вход в Систему на ВМ новой СУСВ и подключить необходимые репозитории.

4.2.1.4.8 Переустановка хостов

Переустановка хостов РОСА Виртуализация на Портале администрирования включает в себя остановку и перезапуск работы хостов.

Примечание — При установке или переустановке хоста настоятельно рекомендуется предварительно отсоединить любые хранилища, не относящиеся к ОС. Это поможет избежать риска случайной инициализации дисков и связанной с этим потери данных.

Предварительные требования для переустановки хостов:

– Если в кластере включена возможность миграции, ВМ могут автоматически мигрировать на любой другой хост в кластере. Соответственно, рекомендуется переустанавливать хост в момент его относительно низкой нагрузки.

– Следует убедиться в том, что объем памяти в кластере достаточен для выполнения обслуживания хостов кластера. При нехватке памяти в кластере миграция ВМ зависнет и затем завершится сбоем. Для снижения потребления памяти перед помещением хоста в режим обслуживания выключить некоторые или все ВМ.

– Перед началом переустановки нужно убедиться в том, что в кластере находится более одного хоста. Не следует пытаться начать переустановку всех хостов одновременно. Один хост всегда должен быть доступен для выполнения задач диспетчера пула хранилища (SPM).

Последовательность действий по переустановке хостов:

а) нажать "Ресурсы → Хосты" и выбрать хосты;

б) выбрать "Управление → Обслуживание" и нажать кнопку OK;

в) выбрать "Установка → Переустановить". Будет открыто окно "Установить хост";

г) перейти на вкладку "Виртуализированный ЦУ" и в выпадающем списке выбрать "Развернуть";

д) для переустановки хоста нажать кнопку OK.

После переустановки хоста и после того, как хост снова получит статус "Работоспособен", можно выполнить миграцию ВМ назад на хост.

Примечание — После выполнения регистрации хоста РОСА Виртуализация в СУСВ статус этого хоста на Портале администрирования может ошибочно показывать "Сбой установки". нажать "Управление → Активировать", и статус хоста сменится на "Работоспособен", а хост будет готов к использованию.

После переустановки узлов виртуализированного ЦУ статус нового окружения можно проверить, выполнив на одном из узлов следующую команду:

```
# hosted-engine --vm-status
```

Во время восстановления старый домен хранилища виртуализированного ЦУ будет переименован, но не будет удален на случай, если при восстановлении случится сбой. После подтверждения того, что окружение работает нормально, старый домен можно удалить.

4.2.1.4.9 Удаление домена хранилища

Последовательность действий по удалению домена хранилища в ЦОД из виртуализированного окружения:

а) нажать "Хранилище → Домены";
б) перевести домен хранилища в режим обслуживания и отсоединить его:

1) нажать на имя домена хранилища для подробного просмотра;
2) перейти на вкладку "Дата-центр";
3) нажать кнопку Обслуживание, затем нажать кнопку OK;
4) нажать кнопку Отсоединить, затем нажать кнопку OK;

в) нажать кнопку Удалить;
г) опционально выбрать "Форматировать домен", т. е. содержимое хранилища будет потеряно, и поставить флажок для удаления содержимого домена;
д) нажать кнопку OK.

Домен хранилища будет навсегда удален из окружения.

4.2.1.5 Перезапись виртуализированного ЦУ существующей резервной копией

В ситуации, когда виртуализированный ЦУ доступен, но испытывает проблемы, такие как повреждение БД или ошибки конфигурации, которые трудно откатить, то окружение можно восстановить до предыдущего состояния с помощью резервной копии, созданной до того, как появились проблемы (если она была сделана).

4.2.1.5.1 Процесс восстановления виртуализированного ЦУ до предыдущего состояния

Процесс восстановления виртуализированного ЦУ до предыдущего состояния состоит из следующих шагов:

а) перевести окружение в глобальный режим обслуживания;
б) восстановить резервную копию на ВМ СУСВ;
в) отключить режим обслуживания.

Дополнительные сведения о параметрах `engine-backup --mode=restore` см. в п. 4.2.1.2.

4.2.1.5.2 Активация глобального режима обслуживания

До начала выполнения любых задач по настройке или обновлению на ВМ СУСВ окружение виртуализированного ЦУ необходимо перевести в глобальный режим обслуживания.

Последовательность действий по активации глобального режима обслуживания:

а) выполнить вход в Систему на одном из узлов виртуализированного ЦУ и переключить окружение в глобальный режим обслуживания:

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

б) перед тем как продолжить, убедиться, что окружение находится в глобальном режиме обслуживания:

```
# hosted-engine --vm-status
```

В результате должно появиться сообщение, указывающее, что окружение находится в глобальном режиме обслуживания.

4.2.1.5.3 Восстановление из резервной копии для перезаписи существующей установки

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

Изменения, внесенные в окружение после того, как была создана резервная копия, такие как добавление или удаление хостов, не будут

присутствовать в восстановленном окружении. Это изменения нужно будет внести повторно.

Последовательность действий по восстановлению из резервной копии для перезаписи существующей установки:

а) выполнить вход в Систему на ВМ СУСВ;

б) удалить файлы конфигурации и очистить БД, связанную с диспетчером.

```
# engine-cleanup
```

Примечание — Команда `engine-cleanup` только очищает БД диспетчера; БД не будет удалена из Системы, а также не будут удалены пользователи, владеющие этой БД.

в) восстановить полную резервную копию или резервную копию только БД, в которой нет необходимости создавать новую БД или указывать учетные записи, т. к. пользователи и БД уже существуют:

– восстановление из полной резервной копии:

```
# engine-backup --mode=restore --file=file_name --
log=log_file_name \
--restore- permissions
```

– восстановление только БД с помощью восстановления файлов конфигурации и архива БД:

```
# engine-backup --mode=restore --scope=files --scope=db --
scope=dwhdb \
-- file=file_name --log=log_file_name --restore-permissions
```

Примечание — Чтобы восстановить только БД СУСВ (если, например, БД хранилища данных расположена на другой машине), можно опустить параметр --scope=dwhdb.

В случае успеха будет показано следующее сообщение:

```
You should now run engine-setup.
Done.
```

г) повторно настроить диспетчер:

```
# engine-setup
```

4.2.1.5.4 Отключение глобального режима обслуживания

Последовательность действий по отключению глобального режима обслуживания:

а) войти в Систему ВМ СУСВ и выключить ее;

б) войти в Систему на одном из узлов виртуализированного ЦУ и отключить глобальный режим обслуживания:

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

После выхода из глобального режима обслуживания ovirt-ha-agent запускает ВМ СУСВ, а затем автоматически запускается СУСВ.

в) убедиться в том, что окружение работает:

```
# hosted-engine --vm-status
```

В выводимых сведениях присутствует статус виртуализированного ЦУ. Значение статуса должно быть одним из следующих: {"health": "good", "vm": "up", "detail": "Up"}.

Пока ВМ не начала работу и только загружается, ЦУ еще не запущен и может иметь один из следующих статусов: {"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}. В этом случае следует подождать несколько минут и повторить попытку.

После того как окружение снова начало работу, можно запустить все ранее остановленные ВМ и проверить корректность поведения ресурсов в окружении.

4.2.1.6 Резервное копирование конфигурационных файлов и баз данных

В Системе реализованы функциональность и настройка программы резервного копирования, которая позволяет создавать резервные копии конфигурационных файлов и баз данных, а также управлять их расписанием и хранилищами.

4.2.1.6.1 Раздел "Бэкап"

В разделе "Бэкап" можно вручную запустить процесс создания резервной копии. Здесь также доступны различные опции для настройки резервного копирования, такие как выбор типов данных (конфигурационные файлы, базы данных), указание путей и выбор хранилища (рисунок 237).

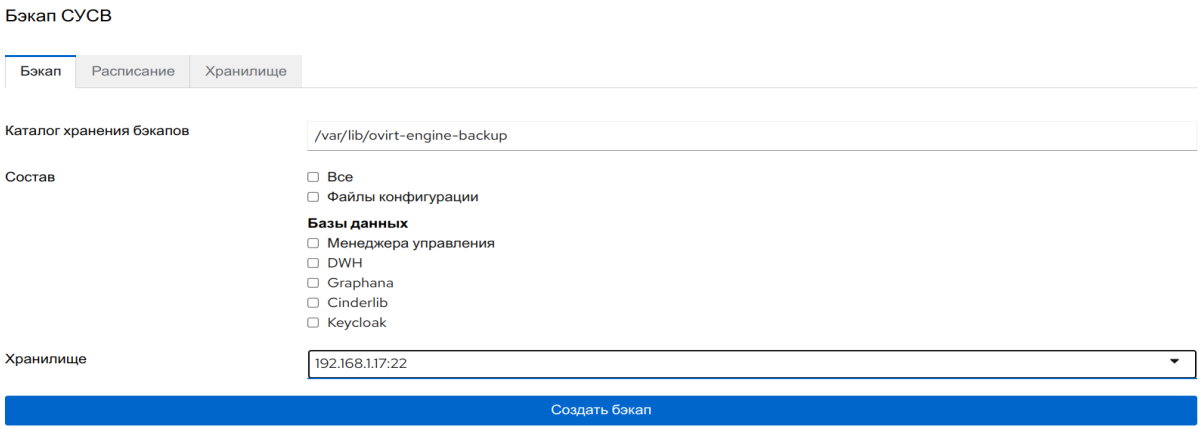


Рисунок 237 – Вкладка "Бэкап"

Резервное копирование будет запущено по нажатию кнопки Создать бэкап. Если резервное копирование завершится успешно, то появится сообщение об успешном завершении. Если возникнет ошибка, будет представлен подробный лог по этапам выполнения резервного копирования.

4.2.1.6.2 Раздел "Расписание"

На вкладке "Расписание" можно настроить автоматическое выполнение резервного копирования в заданное время. Возможно указать периодичность запуска, время и другие параметры, чтобы резервное копирование происходило без участия администратора (рисунок 238).

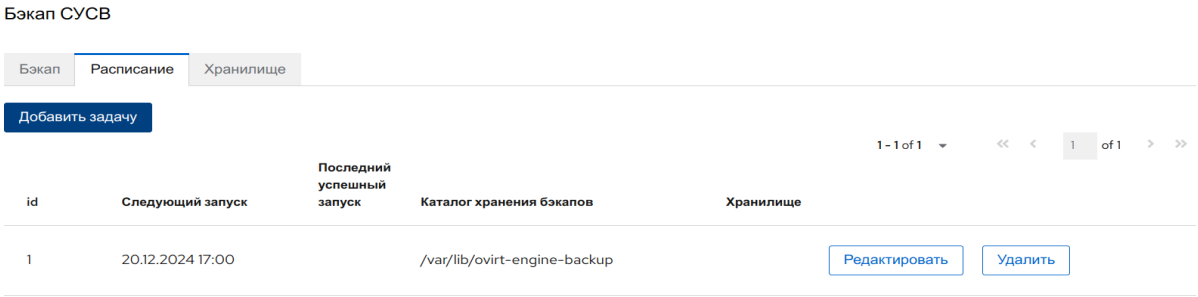


Рисунок 238 – Вкладка "Расписание"

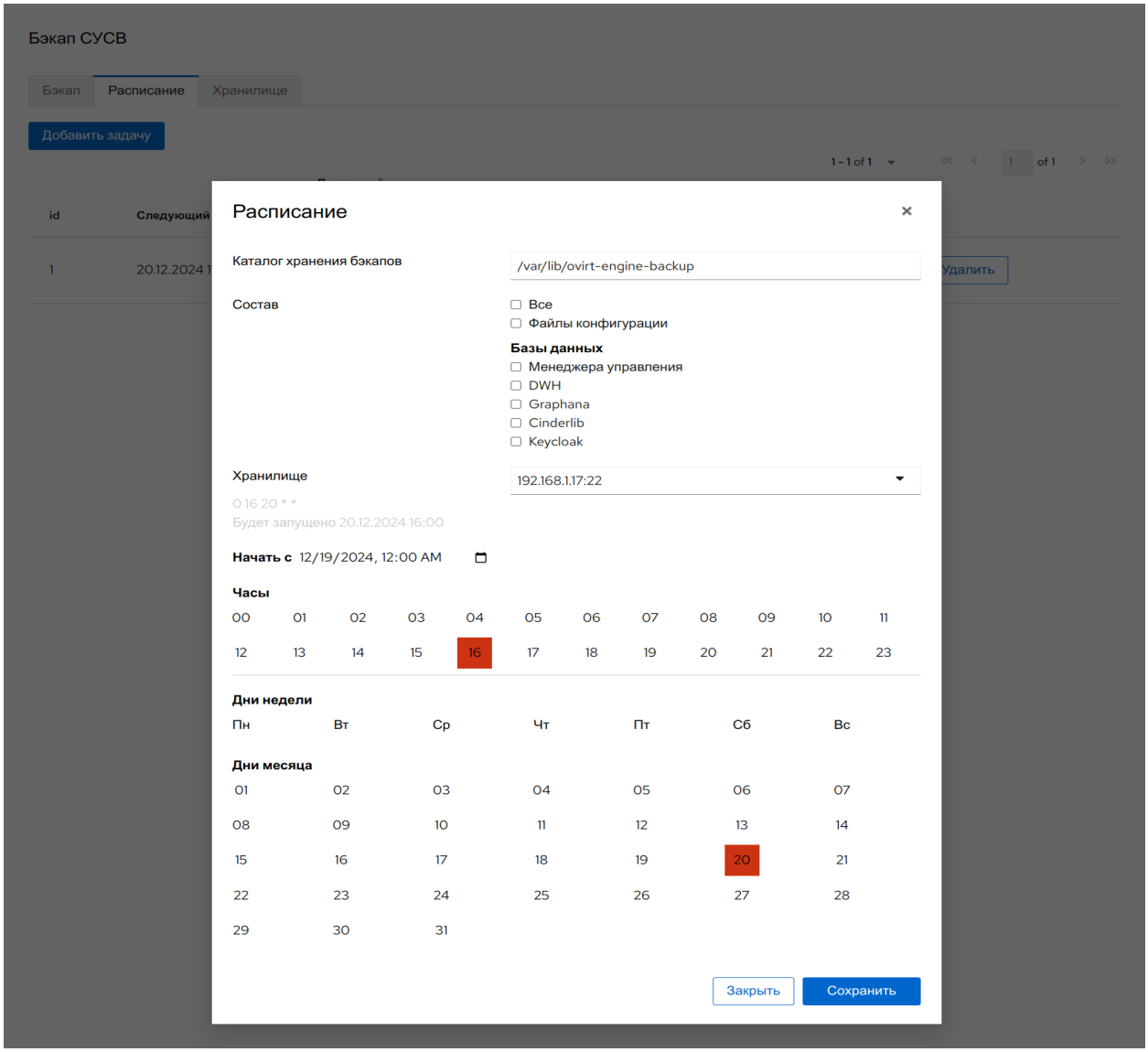


Рисунок 239 – Форма добавления расписания

В этой форме (рисунок 239) нужно заполнить те же параметры что и при ручном запуске, а также настроить cron-выражение для запуска по расписанию. Для этого нужно выбрать часы (1 или несколько), дни недели (можно не заполнять, тогда считается, что выбраны все дни недели), дни месяца (1 или несколько). Также нужно выбрать дату "Начать с". С этой даты и времени будет рассчитан первый запуск. В форме есть подсказка "Будет запущено". Меняя дату можно подстроить дату и время первого запуска. Последующие запуски будут рассчитаны автоматически.

После запуска задачи у нее будет обновляться параметр "Последний успешный запуск" в таблице.

4.2.1.6.3 Раздел "Хранилища"

В разделе "Хранилища" можно создавать и настраивать удаленные хранилища, куда будут копироваться резервные копии (рисунок 240). Хранилище представляет собой удаленную машину, к которой осуществляется доступ по SSH. Здесь также можно редактировать существующие хранилища, изменяя их параметры (рисунок 241).

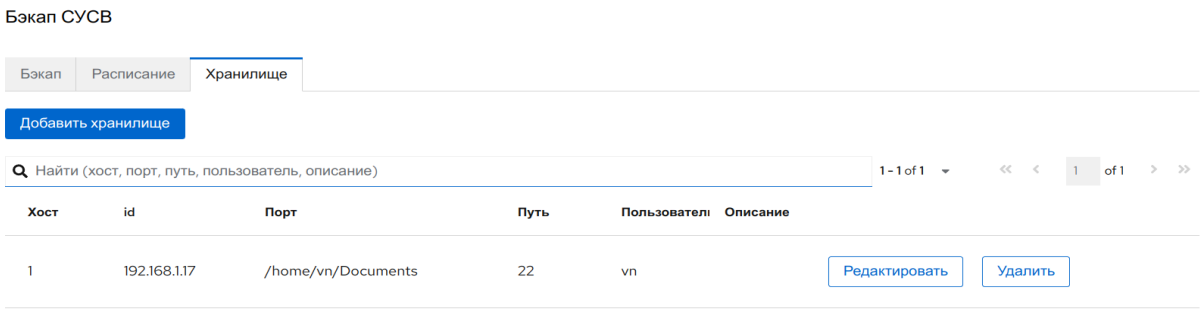


Рисунок 240 – Вкладка "Хранилища"

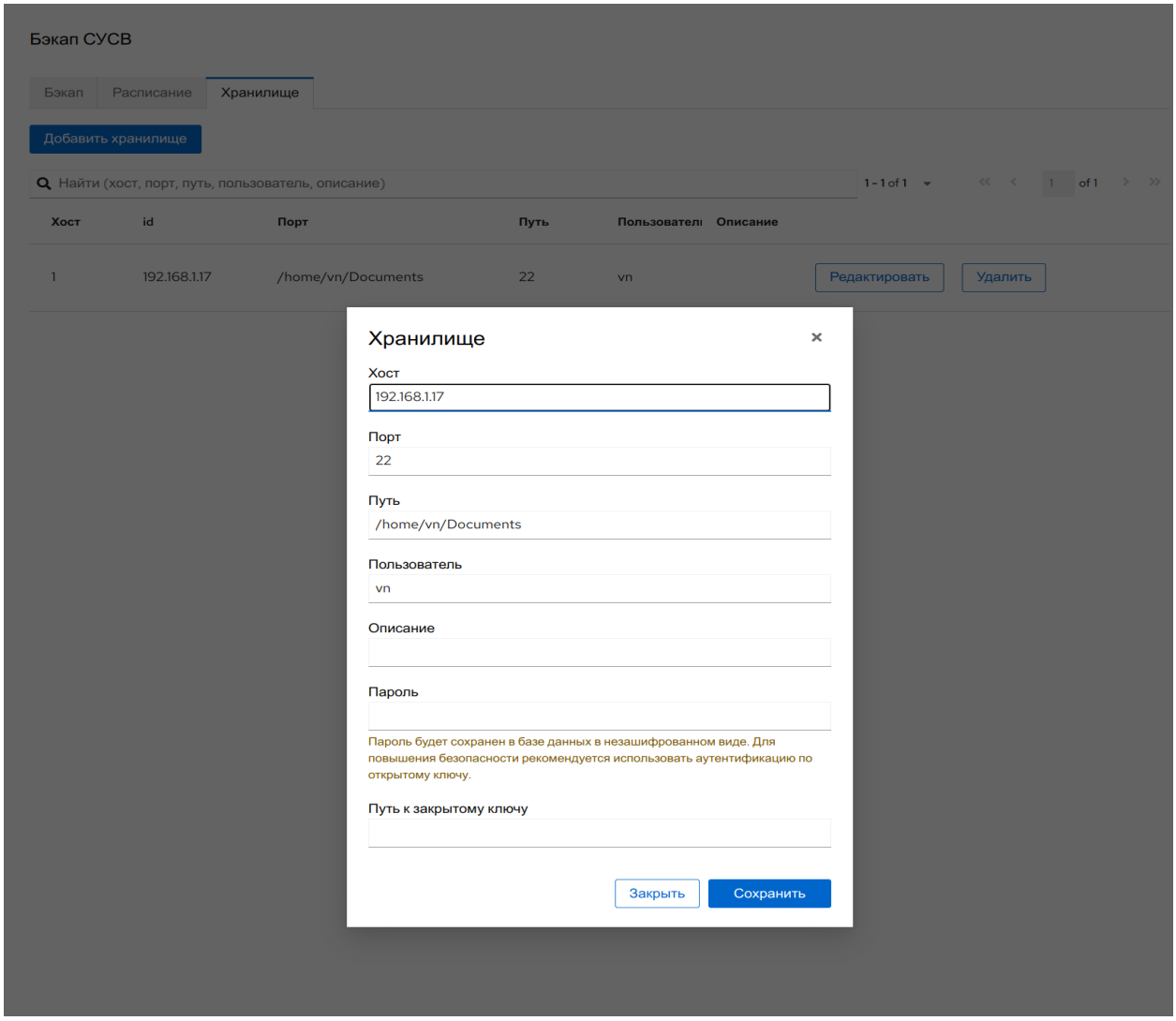


Рисунок 241 – Форма редактирования "Хранилища"

Программа резервного копирования предоставляет удобный интерфейс для управления резервными копиями данных. С ее помощью можно обеспечить безопасность важных конфигурационных файлов и баз данных, настроив автоматическое резервное копирование и управление хранилищами.

4.2.2 Миграция хранилища данных на отдельную машину

В данном разделе описывается процесс миграции БД хранилища данных и службы с машины СУСВ на отдельную машину. Размещение службы Data Warehouse на отдельной машине снижает нагрузку на каждой отдельной

машине, а также помогает избежать потенциальных конфликтов, возникающих при разделении ресурсов ЦП и памяти между различными процессами.

Примечание — На одной и той же машине поддерживается только совместная установка БД хранилища данных, службы Data Warehouse и Grafana, хотя каждый из этих компонентов можно установить отдельно от других на отдельной машине.

Существуют следующие возможности миграции:

– Можно выполнить миграцию службы Data Warehouse с машины СУСВ и подключить ее к существующей БД хранилища данных (ovirt_engine_history).
– Можно выполнить миграцию БД хранилища данных с машины СУСВ, а затем перенести службу Data Warehouse.

4.2.2.1 Миграция БД хранилища данных на отдельную машину

До начала миграции службы Data Warehouse нужно перенести БД хранилища данных (ovirt_engine_history). Для создания резервной копии БД и восстановления ее на машине новой БД необходимо использовать команду `engine-backup`. Дополнительные сведения об `engine-backup` см. в выводе команды:

```
engine-backup --help
```

Примечание — На одной и той же машине поддерживается только совместная установка БД хранилища данных, службы Data Warehouse и Grafana, хотя каждый из этих компонентов можно установить отдельно от других на отдельной машине.

На новом сервере БД должна быть установлена минимальная конфигурация.

Для миграции БД хранилища данных на отдельную машину нужно выполнить следующие действия:

а) создать резервную копию БД и файлов конфигурации хранилища данных на диспетчере:

```
# engine-backup --mode=backup --scope=grafanadb --
scope=dwhdb \
--scope=files -- file=file_name --log=log_file_name
```

б) скопировать файл резервной копии с диспетчера на новую машину:

```
# scp /tmp/file_name root@new.dwh.server.com:/tmp
```

в) установить engine-backup на новой машине:

```
# dnf install ovirt-engine-tools-backup
```

г) установить пакет сервера PostgreSQL:

```
# dnf install postgresql-server postgresql-contrib
```

д) инициализировать БД PostgreSQL, запустить службу postgresql и настроить запуск этой службы при загрузке:

```
# su – postgres -c 'initdb'
# systemctl enable postgresql
# systemctl start postgresql
```

е) восстановить БД хранилища данных на новой машине из файла file_name — это файл резервной копии, скопированный с диспетчера.

```
# engine-backup --mode=restore --scope=files --
scope=grafanadb \
--scope=dwhdb -- file=file_name --log=log_file_name --
provision-dwh-db
```

При использовании параметра --provision-* в режиме восстановления параметр --restore-permissions применяется по умолчанию.

БД хранилища данных теперь располагается на машине, отдельной от машины, на которой располагается диспетчер. После успешного восстановления БД хранилища данных подсказка командной строки указывает выполнить команду `engine-setup`. До запуска этой команды нужно выполнить миграцию службы Data Warehouse.

4.2.2.2 Миграция службы Data Warehouse на отдельную машину

Служба Data Warehouse, установленная и настроенная на СУСВ, может мигрировать на отдельную машину. Размещение службы Data Warehouse на отдельной машине помогает снизить нагрузку на машину СУСВ.

Следует обратить внимание, что в процессе данной процедуры выполняется миграция только службы Data Warehouse.

Сведения о том, как выполнить миграцию БД хранилища данных (ovirt_engine_history) до миграции службы Data Warehouse, приведены в п. 4.2.2.1.

Примечание — На одной и той же машине поддерживается только совместная установка БД хранилища данных, службы Data Warehouse и Grafana, хотя каждый из этих компонентов можно установить отдельно от других на отдельной машине.

Предварительные требования для миграции службы Data Warehouse на отдельную машину:

– СУСВ и хранилище данных должны быть ранее установлены на одну и ту же машину.

– Для настройки новой машины хранилища данных необходимы следующие сведения:

– пароль из файла /etc/ovirt-engine/engine.conf.d/10-setup-database.conf на диспетчере;

– возможность доступа с машины хранилища данных на машину диспетчера на порте TCP 5432;

– имя пользователя и пароль для БД хранилища данных из файла /etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-database.conf на диспетчере. Если миграция БД ovirt_engine_history проводилась по инструкции, описанной в п. 4.2.2.1, то файл резервной копии содержит эти данные, т. к. они были созданы во время настройки БД на этой машине.

Инструкция состоит из нескольких шагов, описанных в пп. 4.2.2.2.1–4.2.2.2.3:

а) остановка службы Data Warehouse на машине диспетчера;
б) настройка новой машины хранилища данных;
в) создание конфигурации на новой машине хранилища данных;
г) отключение пакета Data Warehouse на машине диспетчера.

4.2.2.2.1 Остановка службы Data Warehouse на машине диспетчера

Последовательность действий по остановке службы Data Warehouse на машине диспетчера:

а) остановка службы Data Warehouse:

```
# systemctl stop ovirt-engine-dwhd.service
```

б) если БД размещается на удаленной машине, то необходимо предоставить доступ, вручную отредактировав файл postgres.conf, изменив строку "listen_addresses" в файле /var/lib/pgsql/data/postgresql.conf следующим образом:

```
listen_addresses = '*'
```

Если эта строка отсутствует или была закомментирована, необходимо добавить ее вручную.

Если БД размещается на машине диспетчера и была настроена во время чистой установки СУСВ, то доступ предоставляется по умолчанию.

в) перезапустить службу postgresql:

```
# systemctl restart postgresql
```

4.2.2.2.2 Настройка новой машины хранилища данных

Порядок шагов или параметры, представленные в данном разделе, могут отличаться в зависимости от имеющегося окружения:

а) если на одну и ту же машину переносится и БД ovirt_engine_history, и служба Data Warehouse, выполнить команду, указанную ниже, иначе перейти к следующему шагу:

```
# sed -i '/^ENGINE_DB_/d' \
/etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-
database.conf
# sed -i \
-e 's;^\(OVESETUP_ENGINE_CORE/enable=bool\):True;\1:False;' \
-e '/^OVESETUP_CONFIG\/fqdn/d' \
/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

б) удалить файлы PKI apache/grafana, чтобы они могли быть созданы заново командой `engine-setup` с корректными значениями:

```
# rm -f \
/etc/pki/ovirt-engine/certs/apache.cer \
/etc/pki/ovirt-engine/certs/apache-grafana.cer \
/etc/pki/ovirt-engine/keys/apache.key.nopass \
/etc/pki/ovirt-engine/keys/apache-grafana.key.nopass  \
/etc/pki/ovirt-engine/apache-ca.pem \
/etc/pki/ovirt-engine/apache-grafana-ca.pem
```

в) для начала создания конфигурации хранилища данных на машине запустить команду:

```
# engine-setup
```

г) нажать клавишу `Enter` для принятия автоматически определенного имени хоста либо ввести свое имя хоста и нажать клавишу `Enter`:

```
     Host fully qualified DNS name of this server [autodetected
host name]:
```

д) для автоматической настройки межсетевого экрана нажать `Enter` либо ввести "No" и нажать клавишу `Enter` для сохранения существующих параметров:

```
     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]:
```

ж) если была выбрана автоматическая настройка межсетевого экрана, но активные диспетчеры межсетевых экранов отсутствуют, то будет предложено выбрать диспетчер из списка поддерживаемых возможностей;

з) ввести имя диспетчера межсетевого экрана и нажать клавишу `Enter`, что применимо и в тех случаях, когда доступен только один диспетчер межсетевых экранов;

е) ввести полное доменное имя и пароль диспетчера; для принятия значений по умолчанию в каждом из других полей нажать клавишу `Enter`:

```
     Host fully qualified DNS name of the engine server []: engine-
fqdn
     Setup needs to do some actions on the remote engine server.
Either automatically, using ssh as root to access it, or you will be
prompted to manually perform each such action.
     Please choose one of the following:
     - Access remote engine server using ssh as root
     - Perform each action manually, use files to copy content around
(1, 2) [1]:
     ssh port on remote engine server [22]:
     root password on remote engine server engine-fqdn: password
```

ж) указать полное доменное имя и пароль машины БД диспетчера; для принятия значений по умолчанию в каждом из других полей, нажать `Enter`:

```
     Engine database host []: manager-db-fqdn
     Engine database port [5432]:
     Engine database secured connection (Yes, No) [No]: Engine
database name [engine]:
     Engine database user [engine]: Engine database password:
password
```

з) подтвердить параметры установки:

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

Теперь служба Data Warehouse настроена на удаленной машине, и можно приступать к отключению службы Data Warehouse на машине диспетчера.

4.2.2.2.3 Отключение службы Data Warehouse на диспетчере

Предварительные требования к машине:

– служба Grafana на машине должна быть отключена:

```
     # systemctl disable --now grafana-server.service
```

Последовательность действий по отключению службы Data Warehouse на диспетчере:

а) перезапустить диспетчер на машине диспетчера:

```
     # service ovirt-engine restart
```

б) для изменения файла /etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf и указания параметра "False" выполнить следующую команду:

```
     # sed -i \
     -e 's;^\(OVESETUP_DWH_CORE/enable=bool\):True;\1:False;' \
     -e
's;^\(OVESETUP_DWH_CONFIG/remoteEngineConfigured=bool\):True;
\1:False;' \
     /etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
     # sed -i \
     -e 's;^\(OVESETUP_GRAFANA_CORE/enable=bool\):True;\1:False;'
\
     /etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

в) отключить службу Data Warehouse:

```
    # systemctl disable ovirt-engine-dwhd.service
```

г) удалить файлы Data Warehouse:

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

Служба Data Warehouse теперь размещается на машине, отдельной от машины диспетчера.

4.2.3 Создание и восстановление ВМ из резервных копий с использованием домена хранения резервных копий

4.2.3.1 Что такое домены хранения резервных копий

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

Доменом хранения резервных копий может стать любой домен хранения. Для этого нужно включить или отключить параметр, выставив или убрав флажок в диалоговом блоке "Управление доменом". Этот параметр можно активировать только после того, как работа всех ВМ в этом домене хранения будет завершена.

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

Как и в случае других типов доменов хранения, домены хранения резервных копий можно присоединять к дата-центрам и отсоединять от них. Таким образом, в дополнение к функции хранения резервных копий домены

хранения резервных копий можно использовать для миграции ВМ между дата-центрами.

Некоторые причины для использования доменов хранения резервных копий вместо доменов экспорта:

– В дата-центре может существовать несколько доменов хранения резервных копий, но только один домен экспорта. Домен хранения резервных копий можно выделить для создания резервных копий и восстановления в аварийных ситуациях.

– В домен хранения резервных копий можно переместить резервные копии ВМ, шаблоны или снимки.

– По сравнению с доменами экспорта, в доменах хранения резервных копий процессы миграции большого числа ВМ, шаблонов или файлов OVF проходят значительно быстрее.

– По сравнению с доменами экспорта в доменах хранения резервных копий дисковое пространство используется более эффективно.

– В отличие от доменов экспорта, которые поддерживают только хранение файлов, домены хранения резервных копий поддерживают как файловое (NFS, Gluster), так и блочное хранение (Fiber Channel и iSCSI).

– Принимая во внимание ограничения, параметр хранения резервных копий для домена хранения можно включать и отключать динамически.

Ограничения использования**:**

– Диски любых ВМ или шаблонов, располагающихся в домене хранения резервных копий, должны размещаться в этом же домене.

– Все ВМ в домене хранения должны быть выключены перед тем, как этот домен можно будет сделать доменом хранения резервных копий.

– ВМ, хранящуюся в домене хранения резервных копий, нельзя запустить, так как при этом будет выполняться обработка дисковых данных.

– Домены хранения резервных копий не предназначены для томов памяти, так как тома памяти поддерживаются только активными ВМ.

– В домене хранения резервных копий нельзя выполнить предварительный просмотр ВМ.

– Динамическая миграция ВМ в домен хранения резервных копий невозможна.

– Домен хранения резервных копий не может быть **главным** доменом.

– Домен виртуализированного ЦУ нельзя сделать доменом хранения резервных копий.

– Не использовать домен хранилищ по умолчанию в качестве домена хранения резервных копий.

4.2.3.2 Настройка домена хранения данных в качестве домена хранения резервных копий

Предварительные требования для настройки домена хранения данных:

– Диски любых ВМ или шаблонов, располагающихся в домене хранения резервных копий, должны размещаться в этом же домене.

– Все ВМ в домене должны быть выключены.

Последовательность действий для настройки домена хранения данных в качестве домена хранения резервных копий:

а) на Портале администрирования выбрать "Хранилище → Домены";

б) создать новый домен хранения или выбрать уже существующий и нажать "Управление доменом";

в) в открывшемся окне "Управление доменами" в "Дополнительных параметрах" отметить флажком пункт "Хранение резервных копий".

В результате домен станет доменом хранения резервных копий.

4.2.3.3 Создание и восстановление резервной копии ВМ или снимка с помощью домена хранения резервных копий

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

Последовательность действий при создании резервной копии виртуальной машины

а) создать домен хранения резервных копий (см. п. 4.2.3.2);

б) создать новую ВМ на основе ВМ, для которой нужно создать резервную копию:

– для создания резервной копии снимка сначала на базе этого снимка создать ВМ;

– для создания резервной копии ВМ машину сначала нужно клонировать и, перед тем как продолжить, убедиться в том, что клон выключен;

в) экспортировать новую ВМ в домен хранения резервных копий.

Последовательность действий при восстановлении ВМ из резервной копии

а) убедиться в том, что домен хранения резервных копий, в котором хранится резервная копия ВМ, присоединен к дата-центру;

б) импортировать ВМ из домена хранения резервных копий.

Управление резервным копированием ВМ подробно описано в документе «Руководство администратора. Часть 7. Система резервного копирования" (индекс РСЮК.10103-01 32 07).

4.3 Обновление сертификатов до истечения срока их действия

Срок жизни самоподписанных внутренних сертификатов между гипервизорами и диспетчером составляет 10 лет.

Примечание — Не следует пропускать сроков обновления сертификатов. Просроченный сертификат приводит к тому, что диспетчер и хосты перестают отвечать, а процесс восстановления занимает время и не защищен от ошибок.

Последовательность действий по обновлению сертификатов:

а) обновление сертификатов хоста:

1) на Портале администрирования нажать "Ресурсы → Хосты";
2) нажать "Управление → Обслуживание" и кнопку `OK`. ВМ должны автоматически мигрировать с хоста. В случае прикрепленных ВМ или других причин для невозможности миграции машины необходимо выключить вручную;
3) после того, как на хосте не останется ВМ, и после помещения хоста в режим обслуживания нажать "Установка → Регистрация сертификата";
4) после завершения регистрации нажать "Управление → Активировать";

б) обновить сертификаты диспетчера:

– только для виртуализированного ЦУ – войти в Систему на хосте и перевести его в глобальный режим обслуживания.

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

– виртуализированный ЦУ и отдельно размещенный диспетчер – войти в Систему на диспетчере и выполнить.

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

Сценарий engine-setup задаст вопросы по конфигурации. Следует отвечать согласно вашей ситуации либо использовать файл с ответами:

– ввести "Yes" после нижеследующего вопроса engine-setup:

```
Renew certificates? (Yes, No) [Yes]:
```

в) только для виртуализированного ЦУ – войти в Систему на хосте и отключить глобальный режим обслуживания:

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

4.4 Автоматизация задач конфигурирования с помощью Ansible

Ansible — это средство автоматизации, используемое при настройке систем, развертывании ПО и выполнении последовательных обновлений. В РОСА Виртуализация включена ограниченная версия Ansible для автоматизации таких задач постустановки, как установка и настройка дата-центров, управление пользователями или действия с виртуальными машинами.

Ansible, по сравнению с различными REST API и SDK, предоставляет более простой способ автоматизации конфигурирования РОСА Виртуализация

Различные варианты установки Ansible, а также сведения по работе с Ansible см. в документации Ansible.

4.5 Пользователи и роли

4.5.1 Что такое пользователи

В РОСА Виртуализация существует два типа доменов пользователей:

– локальный домен;
– внешний домен.

Во время процесса установки виртуализированного ЦУ создается домен по умолчанию с названием internal, а также пользователь по умолчанию admin.

Дополнительных пользователей в домене internal можно создавать с помощью утилиты ovirt-aaa-jdbc-tool. Учетные записи, создаваемые в локальных доменах, называются "локальными пользователями". Также к окружению РОСА Виртуализация можно присоединять внешние серверы каталогов, такие как Active Directory, OpenLDAP и многие другие поддерживаемые серверы, и использовать их в качестве внешних доменов. Учетные записи, создаваемые во внешних доменах, называются "пользователями каталогов".

Как локальным пользователям, так и пользователям каталогов необходимо присваивать соответствующие роли и полномочия на Портале администрирования, для того чтобы эти пользователи могли функционировать в окружении. Существует два основных типа ролей пользователя: конечный пользователь и администратор. Роль конечного пользователя использует и управляет виртуальными ресурсами с Портала ВМ. Роль администратора поддерживает системную инфраструктуру с Портала администрирования. Эти роли можно присваивать пользователям как для работы с отдельными ресурсами, такими как виртуальные машины или хосты, так и для работы с иерархией объектов, например, с кластерами и дата-центрами.

4.5.2 Введение в серверы каталогов

Во время установки СУСВ создает пользователя admin в домене internal. Этот пользователь также называется admin@internal. Назначение этой учетной записи — использование во время создания начальной конфигурации окружения и для устранения неполадок в работе. После присоединения внешнего сервера каталогов, добавления пользователей каталога и присвоения им соответствующих ролей и полномочий учетную запись admin@internal можно отключить, если она больше не нужна.

4.5.2.1 Поддерживаемые серверы каталогов

Поддерживаются следующие серверы каталогов:

– 389ds;
– 389ds RFC-2307 Schema;
– Active Directory;
– IBM Security Directory Server;
– IBM Security Directory Server RFC-2307 Schema;
– FreeIPA;
– iDM;

– Novell eDirectory RFC-2307 Schema;
– OpenLDAP RFC-2307 Schema;
– OpenLDAP Standard Schema;
– Oracle Unified Directory RFC-2307 Schema;
– RFC-2307 Schema (Generic);
– Red Hat Directory Server (RHDS);
– Red Hat Directory Server (RHDS) RFC-2307 Schema;
– iPlanet.

Важно — Если в качестве сервера каталогов используется Active Directory, а в создании шаблонов и ВМ планируется использовать sysprep, то в этом случае пользователю-администратору РОСА Виртуализация должен быть делегирован контроль над:

– присоединением компьютеров к домену;
– изменением членства в группах.

4.5.3 Настройка внешнего поставщика LDAP

4.5.3.1 Создание конфигурации внешнего поставщика LDAP (интерактивная установка)

Расширение ovirt-engine-extension-aaa-ldap дает пользователям возможность легко настроить параметры их внешнего каталога. Расширение ovirt-engine-extension-aaa-ldap поддерживает множество различных типов серверов LDAP, а для помощи в настройке большинства типов LDAP предоставляется интерактивный сценарий установки.

Если нужный тип сервера LDAP не указан в сценарии интерактивной установки или же необходимо больше параметров для настройки, то файлы конфигурации можно изменить вручную. Подробнее см. в п. 4.5.3.

Пример для Active Directory см. в п. 4.5.3.2.

Предварительные условия для настройка внешнего поставщика LDAP:

– Должно быть известно доменное имя сервера DNS или сервера LDAP.
– Для настройки защищенного соединения между сервером LDAP и диспетчером следует убедиться в том, что был подготовлен сертификат удостоверяющего центра в формате PEM.

– Необходимо иметь как минимум одну пару "имя учетной записи – пароль" для выполнения поисковых запросов и запросов по входам в Систему в Active Directory.

Последовательность действий по созданию конфигурации внешнего поставщика LDAP:

а) для начала интерактивной установки запустить команду:

```
# ovirt-engine-extension-aaa-ldap-setup
```

б) выбрать тип LDAP, введя соответствующий номер. Если схема сервера LDAP неизвестна, выбрать стандартную схему для имеющегося типа сервера LDAP. Для Active Directory следовать последовательности действий для присоединения Active Directory;

```
Available LDAP implementations:
- 389ds
- 389ds RFC-2307 Schema 3 – Active Directory
- IBM Security Directory Server
IBM Security Directory Server RFC-2307 Schema 6 – IPA
Novell eDirectory RFC-2307 Schema 8 – OpenLDAP RFC-2307 Schema
- OpenLDAP Standard Schema
Oracle Unified Directory RFC-2307 Schema 11 – RFC-2307 Schema
(Generic)
- RHDS
- RHDS RFC-2307 Schema
- iPlanet Please select:
```

в) для принятия значений по умолчанию и конфигурации разрешения доменного имени для имени сервера LDAP нажать клавишу `Enter`:

```
It is highly recommended to use DNS resolution for LDAP
server.
If for some reason you intend to use hosts or plain address
disable DNS usage. Use DNS (Yes, No) [Yes]:
```

г) выбрать метод для политики DNS:

– для варианта 1 серверы DNS, перечисленные в /etc/resolv.conf, используются для разрешения IP-адреса; убедиться в том, что файл /etc/resolv.conf обновлен до корректных значений серверов DNS;

– для варианта 2 ввести полное доменное имя (FQDN) или IP-адрес сервера LDAP. Для обнаружения имени домена можно использовать команду `dig` и запись SRV. Запись SRV имеет следующий формат:

```
_service._protocol.domain_name
```

Пример:

```
dig _ldap._tcp.example.ru SRV.
```

– для варианта 3 ввести список серверов LDAP, разделенных пробелами; использовать либо полные доменные имена серверов, либо их IP-адреса. Данная политика предоставляет балансировку нагрузки между серверами LDAP. Запросы распределяются между всеми серверами LDWP согласно алгоритму циклического перебора;

– для варианта 4 указать список серверов LDAP, разделенных пробелами; использовать либо полное доменное имя серверов, либо их IP-адреса. Данная политика настраивает первый сервер LDAP в качестве сервера по умолчанию, отвечающего на запросы. Если первый сервер недоступен, запрос переходит следующему серверу в списке.

```
- Single server
- DNS domain LDAP SRV record
- Round-robin between multiple hosts
- Failover between multiple hosts Please select:
```

д) выбрать метод защищенного соединения, поддерживаемый имеющимся сервером LDAP, и указать этот метод для получения сертификата ЦС в формате PEM:

– File – дает возможность указать полный путь до сертификата;

– URL – дает возможность указать адрес URL сертификата;

– Inline – дает возможность вставить содержимое сертификата в терминал;

– System – дает возможность указать местоположение по умолчанию для всех файлов ЦС;

– Insecure – пропускает проверку сертификата, но подключение по-прежнему шифруется с использованием TLS;

```
NOTE:
```

```
    It is highly recommended to use secure protocol to access
the LDAP server. Protocol startTLS is the standard recommended
method to do so.
    Only in cases in which the startTLS is not supported,
fallback to non standard ldaps protocol.
    Use plain for test environments only.
    Please select protocol to use (startTLS, ldaps, plain)
[startTLS]: startTLS
    Please select method to obtain PEM encoded CA certificate
(File, URL, Inline, System, Insecure):
    Please enter the password:
```

Примечание — LDAPS — это защищенный протокол LDAP (Lightweight Directory Access Protocol Over Secure Socket Links). Для подключений SSL следует выбирать параметр "ldaps".

е) ввести отличительное имя (DN) пользователя поиска. Этот пользователь должен иметь полномочия для просмотра всех пользователей и групп на сервер каталогов и должен быть указан в примечаниях LDAP. Если разрешается анонимный поиск, просто нажать клавишу `Enter`.

```
    Enter search user DN (for example
uid=username,dc=example,dc=com or leave empty for anonymous):
uid=user1,ou=Users,ou=department-1,dc=example,dc=com
    Enter search user password:
```

ж) ввести отличительное имя базы:

```
    Please enter base DN (dc=example,dc=ru) [dc=example,dc=ru]:
ou=department- 1,dc=example,dc=ru
```

з) если для ВМ планируется настроить единый вход, выбрать "Yes". **Следует обратить внимание**, что этот вариант не может быть использован параллельно с единым входом на Портал администрирования. Сценарий напомнит, что имя профиля должно совпадать с именем домена. И далее потребуется следовать инструкциям п. 4.2 "Настройка единого входа для ВМ" документа "РОСА Виртуализация 4. Руководство администратора. Часть 4. Виртуальные машины" РСЮК.10103-01 32 04).

```
    Are you going to use Single Sign-On for Virtual Machines (Yes,
No) [Yes]:
```

и) указать имя профиля. "Имя" профиля является видимым для пользователей на странице входа в Систему. В данном примере используется example.ru.

Примечание — Чтобы переименовать профиль после завершения настройки домена, нужно отредактировать атрибут ovirt.engine.aaa.authn.profile.name в файле /etc/ovirt-engine/extensions.d/example.ru.-authn.properties. Для применения изменений перезапустить службу ovirt-engine.

```
    Please specify profile name that will be visible to users:
example.ru
```

Важно — Пользователь, впервые выполняющий вход в Систему, должен выбрать профиль в выпадающем списке "Профиль" (рисунок 242). Эта информация сохранится в файлах cookie браузера и будет автоматически указана в следующий раз.

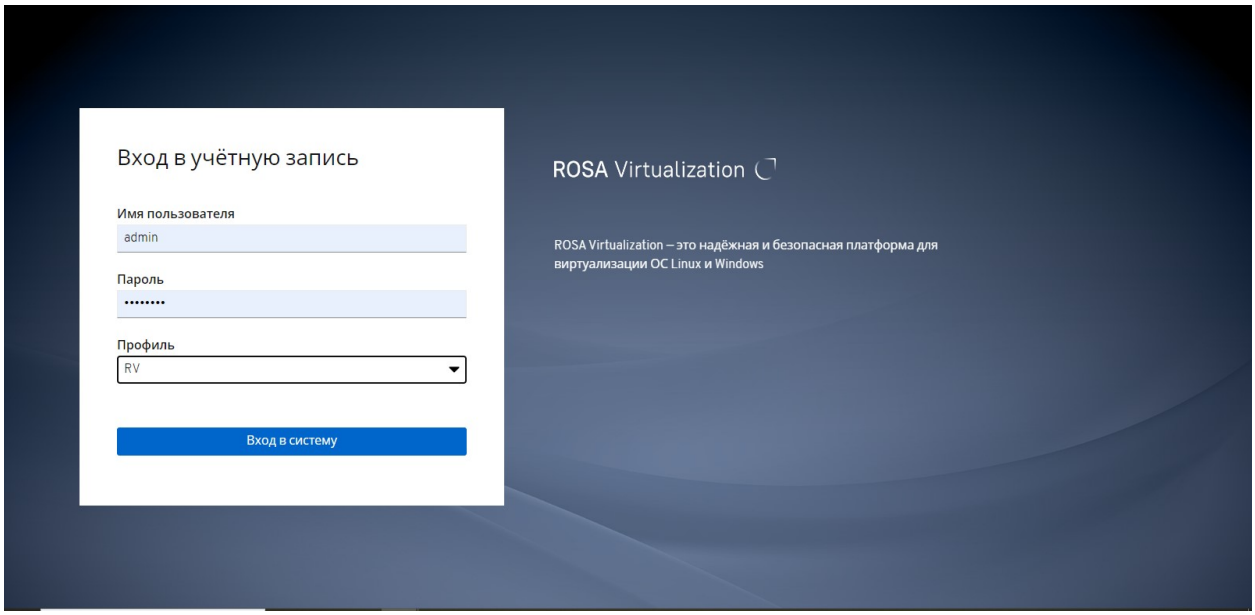


Рисунок 242 – Страница входа в Систему на Портале администрирования

к) протестировать возможность входа в Систему, чтобы убедиться в том, что сервер LDAP корректно подключен к РОСА Виртуализация. В запросе на вход указать имя пользователя и пароль:

```
    NOTE:
    It is highly recommended to test drive the configuration
before applying it into engine. Login sequence is executed
```

```
automatically, but it is recommended to also execute Search
sequence manually after successful Login sequence.
     Please provide credentials to test login flow: Enter user
name:
     Enter user password:
     [ INFO ] Executing login sequence…
     …
     [ INFO ] Login sequence executed successfully
```

л) проверить корректность информации пользователя. Если она неверна, выбрать "Abort":

```
     Please make sure that user details are correct and group
membership meets expectations (search for PrincipalRecord and
GroupRecord titles).
     Abort if output is incorrect.
     Select test sequence to execute (Done, Abort, Login, Search)
[Abort]:
```

м) рекомендуется вручную протестировать функционал поиска. Для создания запроса выбрать "Principal" для учетных записей пользователей или "Group" – для учетных записей групп. Если также должна выводиться информация об учетной записи группы пользователя, выбрать значение "Yes" для пункта "Resolve Groups". Будет создано и выведено на экран три конфигурационных файла.

```
     Select test sequence to execute (Done, Abort, Login, Search)
[Search]: Search
     Select entity to search (Principal, Group) [Principal]: Term
to search, trailing '*' is allowed: testuser1 Resolve Groups
(Yes, No) [No]:
```

н) для завершения настройки выбрать "Done":

```
     Select test sequence to execute (Done, Abort, Login, Search)
[Abort]: Done
     [ INFO ] Stage: Transaction setup [ INFO ] Stage: Misc
configuration
```

```
     [ INFO ] Stage: Package installation [ INFO ] Stage: Misc
configuration
     [ INFO ] Stage: Transaction commit [ INFO ] Stage: Closing
up CONFIGURATION SUMMARY
     Profile name is: example.ru
     The following files were created:
     /etc/ovirt-engine/aaa/example.ru.properties
     /etc/ovirt-engine/extensions.d/example.ru.properties
     /etc/ovirt-engine/extensions.d/example.ru-authn.properties
[ INFO ] Stage: Clean up
     Log file is available at /tmp/ovirt-engine-extension-aaa-
ldap-setup-20171004101225- mmneib.log:
     [ INFO ] Stage: Pre-termination [ INFO ] Stage: Termination
```

о) перезапустить службу ovirt-engine:

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

Созданный профиль теперь доступен на страницах входа в Систему Портала администрирования и Портала ВМ. Чтобы присвоить пользовательской учетной записи на сервере LDAP соответствующие роли и полномочия, например, для входа в Систему на Портале ВМ, следует обратиться к сведениям в п. 4.5.6.

Примечание – Дополнительную информацию см. в файле README расширения для аутентификации и авторизации в LDAP по пути /usr/share/doc/ovirt-engine-extension-aaa-ldap-версия.

4.5.3.2 Присоединение Active Directory

Предварительные условия для присоединения к Active Directory:

– Администратору должно быть известно имя Active Directory.

Примечание – Примеры часто встречающихся конфигураций Active Directory, которые нельзя создать с помощью утилиты ovirt-engine-extension-aaa-ldap-setup, можно найти в файле /usr/share/ovirt-engine-extension-aaa-ldap/examples/README.md.

– Необходимо либо добавить сервер DNS, который может разрешать имя леса Active Directory в файл /etc/resolv.conf на машине диспетчера

виртуализации, либо записать серверы DNS Active Directory и затем указать их по запросу сценария интерактивной установки.

– Для настройки защищенного соединения между сервером LDAP и машиной диспетчера необходимо убедиться в том, что был подготовлен сертификат ЦС в формате PEM. Подробности см. в п. 4.5.4.

– В случае если анонимный поиск не поддерживается, в Active Directory должен быть доступен пользователь с полномочиями на просмотр всех пользователей и групп для выполнения поиска. Следует записать отличительное имя (DN) этого пользователя. Не рекомендуется использовать пользователя Active Directory с административными полномочиями.

– Для выполнения поисковых запросов и запросов по входам в Систему в Active Directory необходимо иметь как минимум одну пару "имя учетной записи – пароль".

– Если при развертывании Active Directory охватывается несколько доменов, нужно ознакомиться с ограничениями, указанными в файле /usr/share/ovirt-engine-extension-aaa-ldap/profiles/ad.properties.

Последовательность действий по присоединению к серверу Active Directory:

а) для начала интерактивной установки запустить команду:

```
# ovirt-engine-extension-aaa-ldap-setup
```

б) выбрать тип LDAP, введя соответствующий номер. Вопросы, касающиеся LDAP и выводимые сценарием после этого шага, зависят от типа LDAP.

```
Available LDAP implementations:
- 389ds
- 389ds RFC-2307 Schema
- Active Directory
- IBM Security Directory Server
- IBM Security Directory Server RFC-2307 Schema
- IPA
- Novell eDirectory RFC-2307 Schema
- OpenLDAP RFC-2307 Schema
- OpenLDAP Standard Schema
- Oracle Unified Directory RFC-2307 Schema
- RFC-2307 Schema (Generic)
```

```
     - RHDS
     - RHDS RFC-2307 Schema
     - iPlanet
     Please select: 3
```

в) указать имя леса Active Directory. Если DNS диспетчера виртуализации не разрешает имя леса, сценарий предложит указать список имен серверов DNS для Active Directory через пробел:

```
     Please enter Active Directory Forest name: ad-
example.test.ru
     [ INFO ] Resolving Global Catalog SRV record for ad-
example.test.ru
     [ INFO ] Resolving LDAP SRV record for ad-example.test.ru
```

г) выбрать метод защиты соединения, поддерживаемый сервером LDAP, а также указать способ получения сертификата центра сертификации в формате PEM. Вариант "File" дает возможность указать полный путь до сертификата. Вариант "URL" дает возможность указать адрес URL сертификата. Вариант "Inline" используется для вставки содержимого сертификата в консольную строку. Вариант "System" дает возможность указать путь до местоположения всех файлов центра сертификации. Вариант "Insecure" дает возможность использовать startTLS в незащищенном режиме.

```
     NOTE:
     It is highly recommended to use secure protocol to access
the LDAP server. Protocol startTLS is the standard recommended
method to do so.
     Only in cases in which the startTLS is not supported,
fallback to non standard ldaps protocol. Use plain for test
environments only.
     Please select protocol to use (startTLS, ldaps, plain)
[startTLS]: startTLS
     Please select method to obtain PEM encoded CA certificate
(File, URL, Inline, System, Insecure): File
     Please enter the password:
```

Примечание — LDAPS — это защищенный протокол LDAP (Lightweight Directory Access Protocol Over Secure Socket Links). Для подключений SSL следует выбирать параметр "ldaps".

д) ввести отличительное имя (DN) пользователя поиска. Этот пользователь должен иметь полномочия для просмотра всех пользователей и групп на сервер каталогов и должен быть указан в примечаниях LDAP. Если разрешается анонимный поиск, просто нажать клавишу `Enter`:

```
    Enter search user DN (empty for anonymous):
cn=user1,ou=Users,dc=test,dc=ru
     Enter search user password:
```

е) указать, нужно ли использовать единый вход для ВМ. Эта возможность используется по умолчанию, но ее невозможно использовать параллельно с настроенным единым входом на Портал администрирования. Сценарий напомнит, что имя профиля должно совпадать с именем домена. И далее потребуется следовать инструкциям п. 4.2 "Настройка единого входа для ВМ" документа "РОСА Виртуализация 4. Руководство администратора. Часть 4. Виртуальные машины" РСЮК.10103-01 32 04).

```
    Are you going to use Single Sign-On for Virtual Machines
(Yes, No) [Yes]:
```

ж) указать имя профиля. "Имя" профиля является видимым для пользователей на странице входа в Систему. В данном примере используется test.ru.

```
    Please specify profile name that will be visible to
users:test.ru
```

Важно — Пользователь, впервые выполняющий вход в Систему, должен выбрать профиль в выпадающем списке "Профиль" (рисунок 243). Эта информация сохранится в файлах cookie браузера и будет автоматически указана в следующий раз.

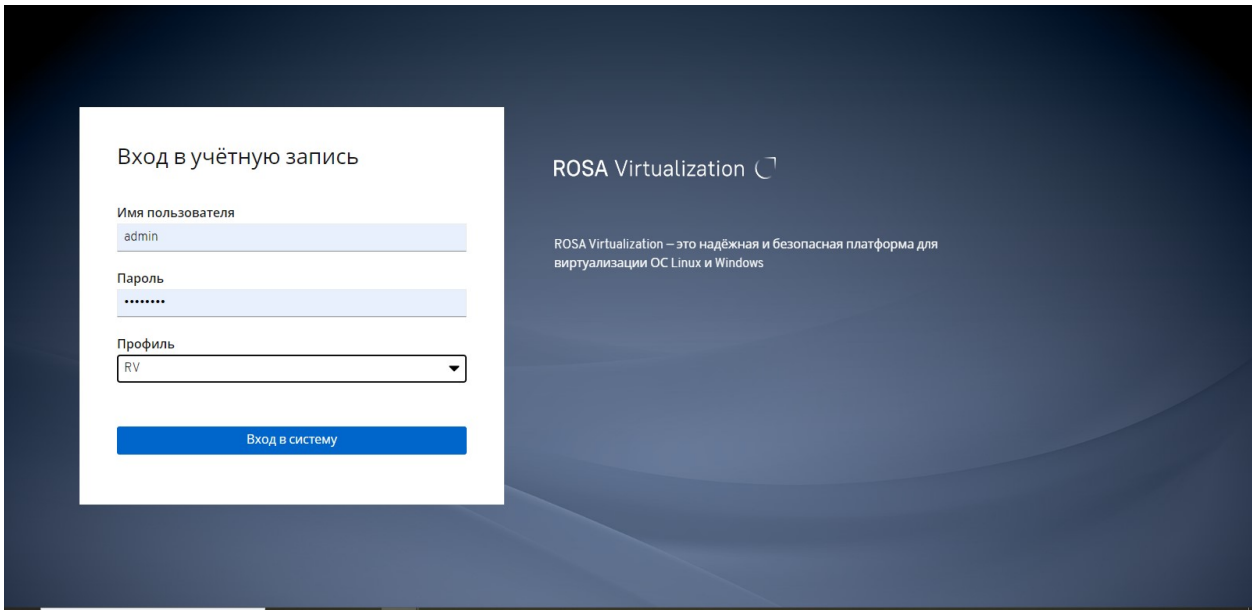


Рисунок 243 – Страница входа в Систему на Портале администрирования

з) протестировать возможность входа в Систему и поиск, чтобы убедиться в том, что сервер LDAP корректно подключен к окружению РОСА Виртуализация. В запросе на вход в Систему указать имя пользователя и пароль. Для создания запроса выбрать "Principal" для учетных записей пользователей или "Group" – для учетных записей групп. Если также должна выводиться информация об учетной записи группы пользователя, выбрать значение "Yes" для пункта "Resolve Groups". Для завершения настройки выбрать "Done". Будет создано и выведено на экран три конфигурационных файла.

```
    NOTE:
    It is highly recommended to test drive the configuration
before applying it into engine. Login sequence is executed
automatically, but it is recommended to also execute Search
sequence manually after successful Login sequence.
    Select test sequence to execute (Done, Abort, Login, Search)
[Abort]: Login Enter search user name: testuser1
    Enter search user password:
    [ INFO ] Executing login sequence...
    ...
```

```
     Select test sequence to execute (Done, Abort, Login, Search)
[Abort]: Search Select entity to search (Principal, Group)
[Principal]:
     Term to search, trailing '*' is allowed: testuser1
     Resolve Groups (Yes, No) [No]:
     [ INFO ] Executing login sequence...
     ...
     Select test sequence to execute (Done, Abort, Login, Search)
[Abort]: Done [ INFO ] Stage: Transaction setup
     [ INFO ] Stage: Misc configuration
     [ INFO ] Stage: Package installation [ INFO ] Stage: Misc
configuration
     [ INFO ] Stage: Transaction commit
     [ INFO ] Stage: Closing up CONFIGURATION SUMMARY
     Profile name is: test.ru
     The following files were created:
     /etc/ovirt-engine/aaa/test.ru.properties
     /etc/ovirt-engine/extensions.d/test.ru-authz.properties
     /etc/ovirt-engine/extensions.d/test.ru-authn.properties
[ INFO ] Stage: Clean up
     Log file is available at /tmp/ovirt-engine-extension-aaa-
ldap-setup-20160114064955- 1yar9i.log:
     [ INFO ] Stage: Pre-termination [ INFO ] Stage: Termination
```

и) созданный профиль теперь доступен на страницах входа в Систему Портала администрирования и Портала ВМ. Чтобы присвоить пользовательской учетной записи на сервере LDAP соответствующие роли и полномочия, например, для входа в Систему на Портале ВМ, следует обратиться к сведениям в п. 4.5.6.

Примечание — Дополнительные сведения см. в файле README расширения аутентификации и авторизации LDAP по пути /usr/share/doc/ovirt-engine-extension-aaa-ldap-версия.

4.5.3.3 Настройка внешнего поставщика LDAP (вручную)

Расширение ovirt-engine-extension-aaa-ldap использует протокол LDAP для получения доступа к серверам каталогов и является полностью настраиваемым. Если не планируется настройка одноразового входа на Портал ВМ или Портал администрирования, то аутентификация Kerberos не требуется.

Если интерактивный способ установки в предыдущем пункте не предоставляет всех нужных возможностей, то файлы конфигурации для присоединения сервера LDAP можно изменить вручную. В последовательности действий ниже используются базовые сведения. Конкретные значения зависят от исходных условий.

Последовательность действий по настройке внешнего поставщика LDAP:

а) установить пакет расширения LDAP на диспетчере РОСА Виртуализация:

```
    # dnf install ovirt-engine-extension-aaa-ldap
```

б) скопировать файл шаблона конфигурации LDAP в каталог /etc/ovirt-engine. Файлы шаблонов доступны для Active Directory (ad) и других типов каталогов (simple). В данном примере используется шаблон simple:

```
    # cp -r
/usr/share/ovirt-engine-extension-aaa-ldap/examples/simple/. \
    /etc/ovirt-engine
```

в) переименовать файлы конфигурации для соответствия имени профиля, который должен быть видимым для пользователей на страницах входа в Систему Порталов ВМ и администрирования:

```
    # mv /etc/ovirt-engine/aaa/profile1.properties \
    /etc/ovirt-engine/aaa/example.properties
    # mv /etc/ovirt-engine/extensions.d/profile1-
authn.properties \
    /etc/ovirt- engine/extensions.d/example-authn.properties
    # mv /etc/ovirt-engine/extensions.d/profile1-
authz.properties  \
    /etc/ovirt- engine/extensions.d/example-authz.properties
```

г) изменить файл конфигурации LDAP property, раскомментировав строки с типом сервера LDAP и обновив информацию в полях домена и пароля:

```
# vi /etc/ovirt-engine/aaa/example.properties
```

Пример профиля – раздел server LDAP:

```
# Select one #
include = <openldap.properties> #include =
<389ds.properties> #include = <rhds.properties> #include =
<ipa.properties> #include = <iplanet.properties>
#include = <rfc2307-389ds.properties> #include = <rfc2307-
rhds.properties> #include = <rfc2307-openldap.properties>
#include = <rfc2307-edir.properties> #include = <rfc2307-
generic.properties>
# Server #
vars.server = ldap1.company.com

# Search user and its password. #
vars.user =
uid=search,cn=users,cn=accounts,dc=company,dc=com vars.password
= 123456

pool.default.serverset.single.server = ${global:vars.server}
pool.default.auth.simple.bindDN = ${global:vars.user}
pool.default.auth.simple.password = ${global:vars.password}
```

При использовании протоколов TLS или SSL для обмена информацией с сервером LDAP нужно получить сертификат ЦС для сервера LDAP и с его помощью создать файл открытого ключа. Затем следует раскомментировать строки, указанные ниже, и указать полный путь к открытому ключу и паролю доступа к файлу.

Пример профиля – раздел keystore:

```
# Create keystore, import certificate chain and uncomment
# if using tls.
pool.default.ssl.startTLS = true
pool.default.ssl.truststore.file = /full/path/to/myrootca.jks
pool.default.ssl.truststore.password = password
```

д) просмотреть файл параметров аутентификации. "Имя" профиля, видимое пользователям на страницах входа в Систему на Портале администрирования и на Портале ВМ, определяется файлом ovirt.engine.aaa.authn.profile.name. Местоположение профиля конфигурации должно совпадать с местоположением файла конфигурации LDAP. Для всех полей можно оставить значения по умолчанию.

```
    # vi /etc/ovirt-engine/extensions.d/example-authn.properties
```

Пример файла конфигурации аутентификации:

```
    ovirt.engine.extension.name = example-authn
ovirt.engine.extension.bindings.method = jbossmodule
    ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa.ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.ldap.AuthnExtension
    ovirt.engine.extension.provides =
org.ovirt.engine.api.extensions.aaa.Authn
ovirt.engine.aaa.authn.profile.name = example
ovirt.engine.aaa.authn.authz.plugin = example-authz
    config.profile.file.1 = ../aaa/example.properties
```

е) местоположение профиля конфигурации должно совпадать с местоположением файла конфигурации LDAP. Для всех полей можно оставить значения по умолчанию:

```
    # vi /etc/ovirt-engine/extensions.d/example-authz.properties
```

Пример файла конфигурации авторизации:

```
    ovirt.engine.extension.name = example-authz
ovirt.engine.extension.bindings.method = jbossmodule
    ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa.ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.ldap.AuthzExtension
    ovirt.engine.extension.provides =
org.ovirt.engine.api.extensions.aaa.Authz config.profile.file.1
= ../aaa/example.properties
```

ж) установить соответствующие права доступа и указать владельца файла профиля:

```
# chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties
# chmod 600 /etc/ovirt-engine/aaa/example.properties
```

з) перезапустить службу engine:

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

и) созданный профиль example теперь доступен на страницах входа в Систему Портала администрирования и Портала ВМ. Чтобы присвоить пользовательской учетной записи на сервере LDAP соответствующие роли и полномочия, например, для входа в Систему на Портале ВМ, обратиться к сведениям в п. 4.5.6.

Примечание – Дополнительную информацию см. в файле README расширения для аутентификации и авторизации в LDAP по пути /usr/share/doc/ovirt-engine-extension-aaa-ldap-версия.

4.5.3.4 Удаление внешнего поставщика LDAP

В данной последовательности показывается процесс удаления настроенного внешнего поставщика LDAP и его пользователей.

Последовательность действий по удалению внешнего поставщика LDAP:

а) удалить файлы конфигурации поставщика LDAP, заменив имя по умолчанию profile1:

```
# rm /etc/ovirt-engine/extensions.d/profile1-
authn.properties
# rm /etc/ovirt-engine/extensions.d/profile1-
authz.properties
# rm /etc/ovirt-engine/aaa/profile1.properties
```

б) перезапустить службу ovirt-engine:

```
# systemctl restart ovirt-engine
```

в) во вкладке "Пользователи" Портала администрирования выбрать пользователей этого поставщика (пользователи со значением "profile1-authz" для параметра "Поставщик авторизации") и нажать кнопку Удалить.

4.5.4 Настройка единого входа для LDAP и Kerberos

Механизм единого входа дает возможность пользователям войти в Систему на Портале ВМ или Портале администрирования без повторного ввода пароля. Данные учетной записи для аутентификации получаются с сервера Kerberos. Для настройки единого входа на Портале администрирования необходимо настроить два расширения: ovirt-engine-extension-aaa-misc и ovirt-engine-extension-aaa-ldap, а также два модуля Apache: mod_auth_gssapi и mod_session. Есть возможность настроить единый вход без использования Kerberos, но ее описание выходит за рамки данного руководства.

Примечание — При активированном едином входе на Портал ВМ невозможен единый вход в виртуальные машины. При активированном едином входе на Портал ВМ в пароле нет необходимости, поэтому невозможно передать этот пароль для входа в Систему на ВМ.

В данном примере предполагается, что:

– на существующем центре распределения ключей (KDC) используется версия MIT Kerberos 5;

– для сервера KDC имеются полномочия администратора;

– клиент Kerberos установлен на СУСВ и на ВМ пользователя;

– для создания принципалов служб Kerberos и файлов таблиц ключей использовалась утилита kadmin.

Последовательность действий для настройки единого входа для LDAP и Kerberos:

а) на сервере KDC на машине диспетчера РОСА Виртуализация создать принципала службы и файл keytab для службы Apache;

б) на диспетчере РОСА Виртуализация установить пакеты расширений аутентификации и авторизации, а также модуль аутентификации Kerberos для Apache;

в) настроить файлы расширений.

4.5.4.1 Настройка Kerberos для службы Apache

Для настройки Kerberos для службы Apache нужно выполнить следующие действия:

а) на сервере KDC использовать утилиту kadmin для создания принципала для службы Apache на машине диспетчера виртуализации (принципал службы — это ссылочный идентификатор службы Apache):

```
# kadmin
kadmin> addprinc -randkey HTTP/fqdn-of-rhevm@REALM.COM
```

б) создать файл keytab для службы Apache, в котором хранится общий секретный ключ:

Примечание — Во время создания и восстановления резервных копий команде `engine-backup` указывается файл /etc/httpd/http.keytab. Если файлу keytab было дано другое имя, следует убедиться, что для него была создана и восстановлена резервная копия.

```
kadmin> ktadd -k /tmp/http.keytab HTTP/fqdn-of-
rhevm@REALM.COM
kadmin> quit
```

в) скопировать файл keytab с сервера KDC на машину диспетчера виртуализации:

```
# scp /tmp/http.keytab root@rhevm.example.com:/etc/httpd
```

4.5.4.2 Настройка единого входа для Портала ВМ или Портала администрирования

Для настройки единого входа для Портала ВМ или Портала администрирования нужно выполнить следующие действия:

а) на машине диспетчера виртуализации установить соответствующие права доступа и указать владельца файла таблицы ключей:

```
# chown apache /etc/httpd/http.keytab
# chmod 400 /etc/httpd/http.keytab
```

б) установить пакет расширения для аутентификации, пакет расширения для LDAP, а также модули Apache mod_auth_gssapi и mod_session:

```
# dnf install ovirt-engine-extension-aaa-misc \
ovirt-engine-extension-aaa-ldap mod_auth_gssapi mod_session
```

в) скопировать файл шаблона конфигурации SSO в каталог /etc/ovirt-engine. Файлы шаблонов доступны для Active Directory (ad-sso) и для других

типов каталогов (simple-sso). В данном примере используется шаблон конфигурации simple-sso:

```
    # cp -r
/usr/share/ovirt-engine-extension-aaa-ldap/examples/simple-sso/.
\
    /etc/ovirt-engine
```

г) переместить файл ovirt-sso.conf в каталог настройки Apache:

Примечание — Во время создания и восстановления резервных копий команде `engine-backup` указывается файл /etc/httpd/conf.d/ovirt-sso.conf. Если этому файлу было дано другое имя, следует убедиться, что для него была создана и восстановлена резервная копия.

```
    # mv /etc/ovirt-engine/aaa/ovirt-sso.conf /etc/httpd/conf.d
```

д) просмотреть файл метода аутентификации. Этот файл не нужно редактировать, поскольку данные области автоматически получаются из файла keytab.

```
    # vi /etc/httpd/conf.d/ovirt-sso.conf
```

Пример файла метода аутентификации:

```
    <LocationMatch ^/ovirt-engine/sso/(interactive-login-
negotiate|oauth/token-http- auth)|^/ovirt-engine/api>
    <If "req('Authorization') !~ /^(Bearer|Basic)/i">
RewriteEngine on
    RewriteCond %{LA-U:REMOTE_USER} ^(.*)$ RewriteRule ^(.*)$ -
[L,NS,P,E=REMOTE_USER:%1] RequestHeader set X-Remote-User %
{REMOTE_USER}s

    AuthType GSSAPI AuthName "Kerberos Login"

    # Modify to match installation GssapiCredStore
keytab:/etc/httpd/http.keytab GssapiUseSessions On
    Session On
    SessionCookieName ovirt_gssapi_session
path=/private;httponly;secure;
```

```
    Require valid-user
    ErrorDocument 401 "<html><meta http-equiv=\"refresh\"
content=\"0; url=/ovirt-
engine/sso/login-unauthorized\"/><body><a
href=\"/ovirt-engine/sso/login-
unauthorized\">Here</a></body></html>"
    </If>
    </LocationMatch>
```

е) переименовать файлы конфигурации для соответствия с именем профиля, который должен быть видимым для пользователей на страницах входа в Систему Порталов ВМ и администрирования:

```
    # mv /etc/ovirt-engine/aaa/profile1.properties \
    /etc/ovirt-engine/aaa/example.properties
    # mv /etc/ovirt-engine/extensions.d/profile1-http-
authn.properties \
    /etc/ovirt-engine/extensions.d/example-http-authn.properties
    # mv /etc/ovirt-engine/extensions.d/profile1-http-
mapping.properties \
    /etc/ovirt-engine/extensions.d/example-http-
mapping.properties
    # mv /etc/ovirt-engine/extensions.d/profile1-
authz.properties \
    /etc/ovirt- engine/extensions.d/example-authz.properties
```

ж) изменить файл конфигурации LDAP property, убрав комментарии со строк с типом сервера LDAP и обновив информацию в полях домена и пароля:

```
    # vi /etc/ovirt-engine/aaa/example.properties
```

Пример профиля – раздел сервера LDAP:

```
    # Select one
    include = <openldap.properties>
    #include = <389ds.properties>
    #include = <rhds.properties>
    #include = <ipa.properties>
    #include = <iplanet.properties>
```

```
    #include = <rfc2307-389ds.properties>
    #include = <rfc2307-rhds.properties>
    #include = <rfc2307-openldap.properties>
    #include = <rfc2307-edir.properties>
    #include = <rfc2307-generic.properties>

    # Server
    #vars.server = ldap1.company.com

    # Search user and its password. #
    vars.user =
uid=search,cn=users,cn=accounts,dc=company,dc=com vars.password
= 123456

    pool.default.serverset.single.server = ${global:vars.server}
pool.default.auth.simple.bindDN = ${global:vars.user}
pool.default.auth.simple.password = ${global:vars.password}
```

Если для обмена информацией с сервером LDAP используются протоколы TLS или SSL, необходимо получить сертификат корневого центра сертификации для сервера LDAP и с его помощью создать файл открытого ключа. Следует раскомментировать строки, указанные ниже, и указать полный путь к открытому ключу и паролю доступа к файлу.

Пример профиля – раздел keystore:

```
    # Create keystore, import certificate chain and uncomment
    # if using ssl/tls.
    pool.default.ssl.startTLS = true
    pool.default.ssl.truststore.file = /full/path/to/myrootca.jks
    pool.default.ssl.truststore.password = password
```

з) просмотреть файл параметров аутентификации. "Имя" профиля, видимое пользователям на страницах входа в Систему на Портале администрирования и на Портале ВМ, определяется файлом ovirt.engine.aaa.authn.profile.name. Местоположение профиля конфигурации должно совпадать с местоположением файла конфигурации LDAP. Для всех полей можно оставить значения по умолчанию.

```
     # vi /etc/ovirt-engine/extensions.d/example-http-
authn.properties
```

Пример файла параметров аутентификации:

```
     ovirt.engine.extension.name = example-http-authn
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.http.AuthnExtension
     ovirt.engine.extension.provides =
org.ovirt.engine.api.extensions.aaa.Authn
ovirt.engine.aaa.authn.profile.name = example-http
ovirt.engine.aaa.authn.authz.plugin = example-authz
ovirt.engine.aaa.authn.mapping.plugin = example-http-mapping
config.artifact.name = HEADER
     config.artifact.arg = X-Remote-User
```

и) просмотреть файл параметров авторизации. Местоположение профиля конфигурации должно совпадать с местоположением файла конфигурации LDAP. Для всех полей можно оставить значения по умолчанию.

```
     #  vi /etc/ovirt-engine/extensions.d/example-
authz.properties
```

Пример файла параметров авторизации:

```
     ovirt.engine.extension.name = example-authz
ovirt.engine.extension.bindings.method = jbossmodule
     ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa.ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.ldap.AuthzExtension
     ovirt.engine.extension.provides =
org.ovirt.engine.api.extensions.aaa.Authz config.profile.file.1
= ../aaa/example.properties
```

к) просмотреть файл конфигурации отображения аутентификации. Местоположение профиля конфигурации должно совпадать с местоположением

файла конфигурации LDAP. Расширение имени профиля конфигурации должно совпадать со значением "ovirt.engine.aaa.authn.mapping.plugin" в файле конфигурации аутентификации. Для всех полей можно оставить значения по умолчанию.

```
    # vi /etc/ovirt-engine/extensions.d/example-http-
mapping.properties
```

Пример файла параметров отображения аутентификации:

```
    ovirt.engine.extension.name = example-http-mapping
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.mapping.MappingExtension
ovirt.engine.extension.provides =
org.ovirt.engine.api.extensions.aaa.Mapping
config.mapAuthRecord.type = regex
    config.mapAuthRecord.regex.mustMatch = true
    config.mapAuthRecord.regex.pattern  =  ^(?<user>.*?)((\\\\(?
<at>@)(?<suffix>.*?)@.*)|(?
    <realm>@.*))$
    config.mapAuthRecord.regex.replacement = ${user}${at}$
{suffix}
```

л) установить соответствующие права доступа и указать владельца файла конфигурации:

```
    # chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties
    # chown ovirt:ovirt \
    /etc/ovirt-engine/extensions.d/example-http-authn.properties
    # chown ovirt:ovirt \
    /etc/ovirt-engine/extensions.d/example-http-
mapping.properties
    # chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-
authz.properties
    # chmod 600 /etc/ovirt-engine/aaa/example.properties
```

```
    # chmod 640 /etc/ovirt-engine/extensions.d/example-http-
authn.properties
    # chmod 640 /etc/ovirt-engine/extensions.d/example-http-
mapping.properties
    # chmod 640 /etc/ovirt-engine/extensions.d/example-
authz.properties
```

м) перезапустить службу Apache и службу ovirt-engine:

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

4.5.5 Авторизация пользователей

4.5.5.1 Модель авторизации пользователей

Управление авторизацией в РОСА Виртуализация базируется на сочетании трех составляющих:

- Пользователь, выполняющий действие.
- Тип этого выполняемого действия.
- Объект, над которым выполняется это действие.

4.5.5.2 Действия пользователей

Чтобы действие выполнилось успешно, у пользователя должны быть соответствующие полномочия на объект, над которым выполняется действие. У каждого типа действий есть соответствующие полномочия.

Некоторые действия выполняются более чем над одним объектом. Копирование шаблона в другой домен хранения, например, влияет и на шаблон, и на целевой домен хранения. Пользователь, выполняющий это действие, должен иметь полномочия на все объекты, подпадающие под влияние этого действия.

4.5.6 Администрирование задач пользователей на Портале администрирования

Интерфейс Системы предназначен для управления локальными пользователями. Управление пользователями происходит посредством использования утилиты ovirt-aaa-jdbc-tool.

Система представляет собой веб-приложение и состоит из фронтенд-части и бэкенд-части. Данные хранятся в СУБД.

Для работы веб-приложения необходимо обеспечить следующие системные требования:

– CPU – не менее 2;
– оперативная память – не менее 1 ГБ;
– диск – не меньше 1 ГБ.

Для установки с диска РОСА Виртуализация, выбрав в наборе программ "Минимальная установка", выполнить команду:

```
dnf install rv-aaa-users
```

Для работы необходимо открыть интерфейс Портала администратора и перейти в раздел "Дополнения → Пользователи". Интерфейс состоит из двух вкладок "Пользователи" и "Группы" (рисунок 244).

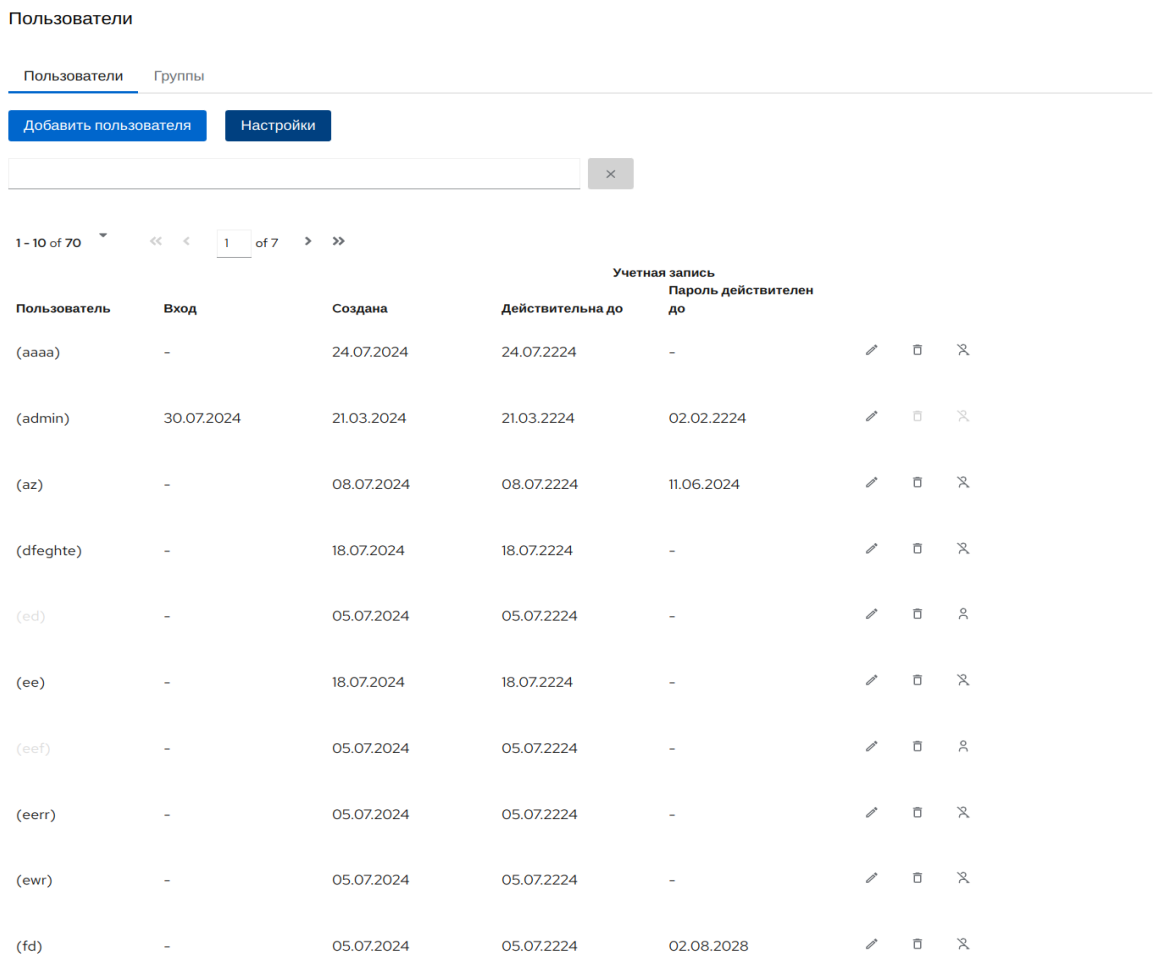


Рисунок 244 – Пользователи

Во вкладке "Пользователи" в таблице постранично показаны все пользователи (по умолчанию по 10 пользователей на странице). Для каждого пользователя показано имя, дата последнего входа, дата создания учетной записи, срок действия учетной записи, срок действия пароля (если он есть). Для каждого пользователя в строке расположены пиктограммы для редактирования, удаления, разблокировки и деактивации пользователя.

4.5.6.1 Добавление пользователя

Для добавления нового пользователя нужно нажать кнопку Добавить пользователя, после чего откроется окно (рисунок 245).

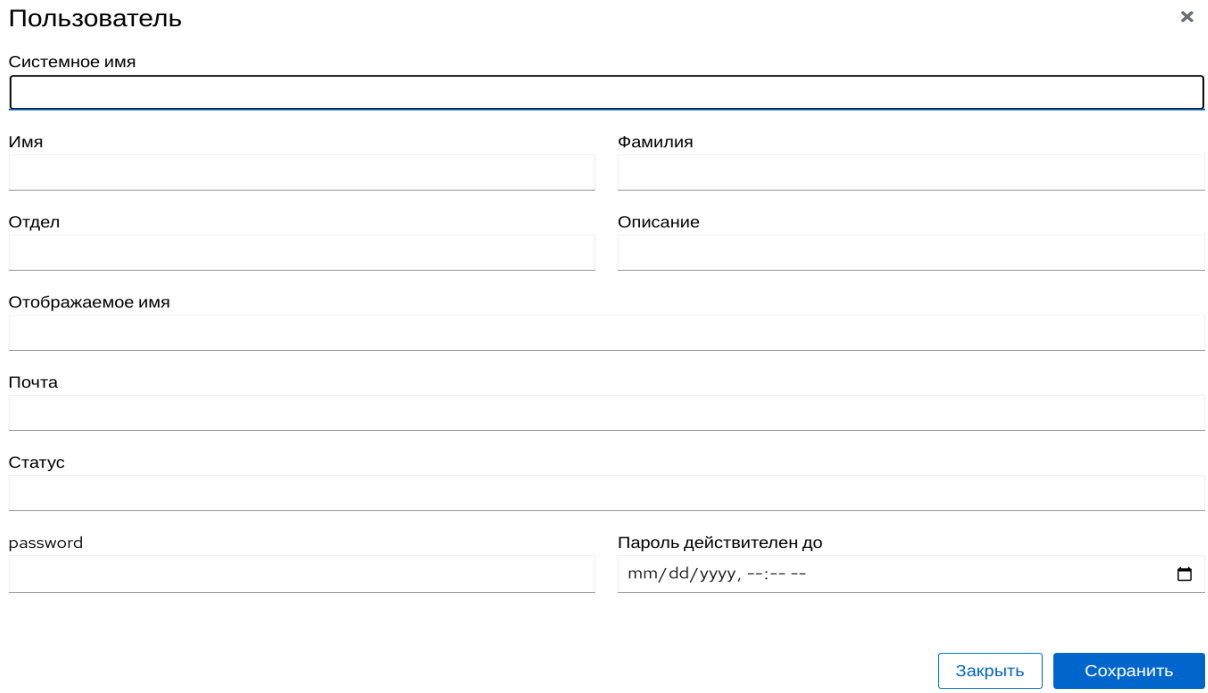


Рисунок 245 – Добавление пользователя

В форме обязательным полем является только поле "Системное имя". После заполнения требуемых полей следует нажать кнопку "Сохранить". Окно закроется, появится крутящийся элемент, по исчезновении которого пользователь будет создан. Хотя в таблице новый пользователь может не присутствовать, но его уже можно найти через поисковую строку (рисунок 246).



Рисунок 246 – Поисковая строка

4.5.6.2 Редактирование пользователя

Для редактирования сведений о пользователе нужно нажать на кнопку , появится окно, аналогичное окну при создании пользователя. Далее следует заполнить требуемые поля и нажать кнопку Сохранить.

4.5.6.3 Удаление пользователя

Для удаления пользователя нужно нажать на кнопку , появится диалоговое окно для подтверждения, в котором требуется нажать кнопку Да.

4.5.6.4 Выключение пользователя

В Системе возможно выключение (disable) пользователя . После выключения пользователь не сможет войти в Систему.

Включение осуществляется нажатием пиктограммы .

После выключения пиктограмму изменится на , которая, в свою очередь, служит для включения пользователя.

4.5.6.5 Блокировка пользователя

Пользователь блокируется автоматически после нескольких попыток ввода неправильного пароля. Количество попыток, после которых учетная запись блокируется, зависит от настроек. Для разблокирования нужно нажать на пиктограмму .

Затем следует указать пароль и нажать кнопку Сохранить, пиктограмма сменится на крутящийся элемент. По завершении процесса появится сообщение об успешном завершении, и цвет пиктограммы изменится синего на серый.

4.5.6.6 Настройка

Для настройки параметров работы с пользователями нужно нажать на кнопку Настройки", после чего появится окно (рисунок 247).

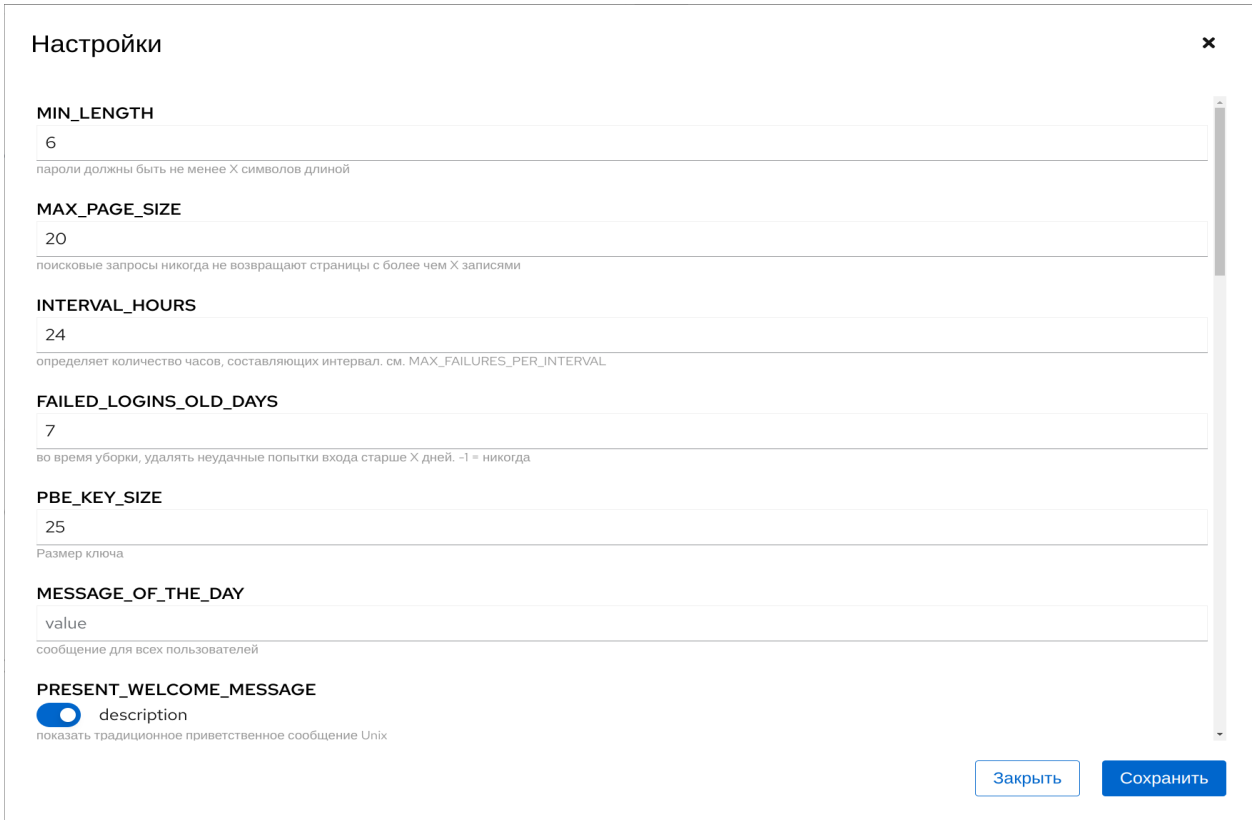


Рисунок 247 – Параметры паролей

Все поля для настройки снабжены коротким пояснением.

4.5.6.7 Работа с группами пользователей

Группы пользователей в интерфейсе Портала администрирования показаны в виде дерева на вкладке "Группы" (рисунок 248).

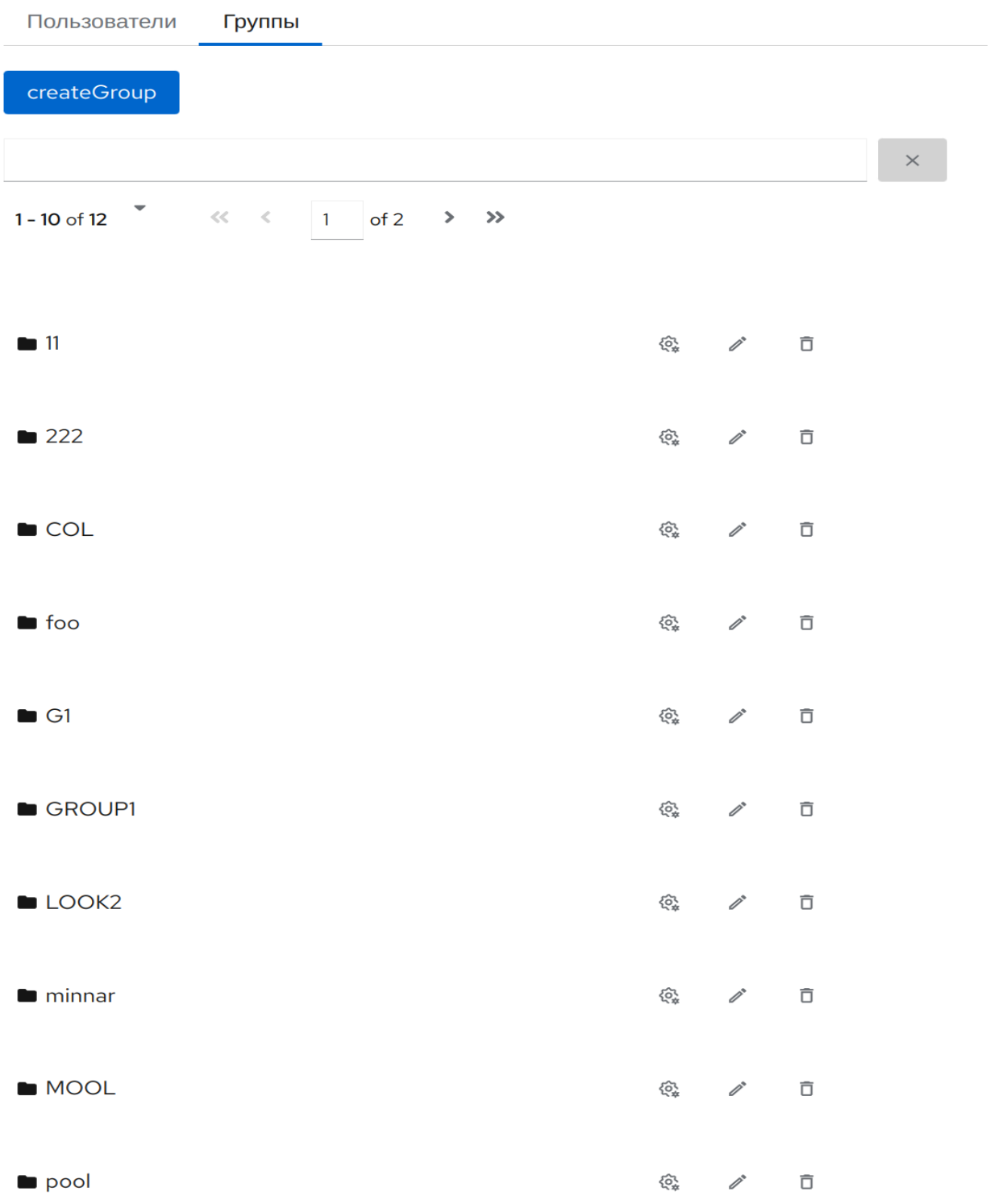


Рисунок 248 – Группы пользователей

Узлами дерева являются группы, при этом группа может иметь в своем составе другие группы и пользователей.

Для добавления новой группы нужно нажать кнопку `Добавить группу`, после чего откроется окно (рисунок 249).



Рисунок 249 – Добавление группы

После заполнение требуемых полей следует нажать кнопку `Сохранить`.

Редактирование и удаление групп реализовано аналогично интерфейсу работы с пользователями с теми же пиктограммами и функциями.

Для редактирования состава группы нужно нажать пиктограмму и в открывшемся окне выбрать пользователей и группы, которые будут включены в состав группы (рисунок 250).

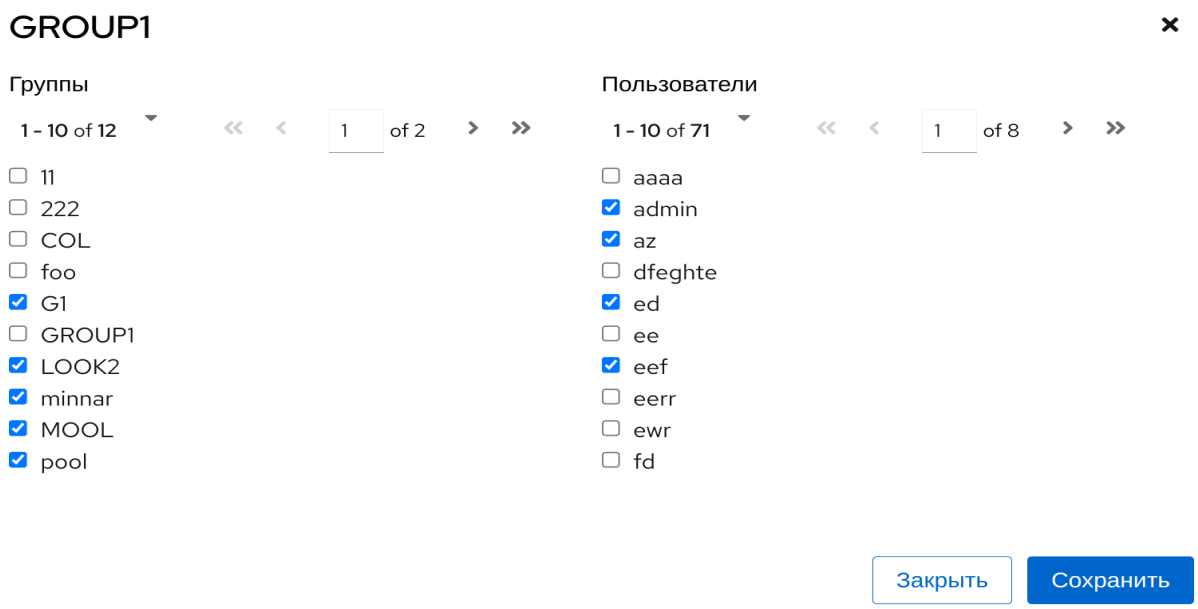


Рисунок 250 – Редактирование состава группы

4.5.7 Администрирование задач пользователей в консольном режиме

С помощью утилиты ovirt-aaa-jdbc-tool можно управлять учетными записями пользователей во внутреннем домене. Изменения, внесенные при помощи этой утилиты, применяются мгновенно и не требуют перезапуска службы ovirt-engine. Полный список параметров для работы с пользователями можно просмотреть в выводе команды:

```
ovirt-aaa-jdbc-tool user –help
```

Примеры наиболее часто встречающихся случаев использования описаны в данном разделе.

Важно — Администратор должен выполнить вход в Систему на машине СУСВ.

4.5.7.1 Создание нового пользователя

Администратор может создавать учетные записи новых пользователей. Дополнительный параметр --attribute передает подробности.

```
# ovirt-aaa-jdbc-tool user add test1 \
--attribute=firstName=John --attribute=lastName=Doe
adding user test1...
user added successfully
```

Теперь только что созданного пользователя можно добавить на Портал администрирования и присвоить ему подходящие роли и полномочия.

Чтобы просмотреть полный список параметров, нужно выполнить команду:

```
ovirt-aaa-jdbc-tool user add --help.
```

4.5.7.2 Настройка пароля пользователя

Администратор может создавать пароли, при этом необходимо указать значение параметра --password-valid-to, в противном случае время истечения действия пароля по умолчанию равно текущему времени.

Формат значения по умолчанию: "гггг-ММ-дд ЧЧ:мм:ссX", где "X" — значение смещения часового пояса от UTC. В данном примере значение "0800" означает время по Гринвичу (GMT) минус 8 часов. Для нулевого смещения используют значение "Z".

```
# ovirt-aaa-jdbc-tool user password-reset test1 \
--password-valid-to="2025-08-01 12:00:00-0800"
Password:
updating user test1... user updated successfully
```

Дополнительные параметры см. в выводе команды:

```
ovirt-aaa-jdbc-tool user password-reset --help.
```

Примечание — По умолчанию политика паролей для учетных записей пользователей во внутренних доменах имеет следующие ограничения:

– Минимум 6 символов.
– При смене пароля нельзя снова назначить три предыдущих пароля.
– Чтобы получить дополнительные сведения о политике паролей и других значениях по умолчанию, следует выполнить команду:

```
ovirt-aaa- jdbc-tool settings show.
```

Сразу после обновления пароля необходимо вручную распространить изменения в ovirt-provider-ovn. В противном случае пользователь admin будет заблокирован, т. к. для синхронизации сетей из ovirt-provider-ovn диспетчер РОСА Виртуализация продолжит использовать старый пароль. Для внесения нового пароля в ovirt-provider-ovn необходимо выполнить следующие действия:

а) на Портале администрирования выбрать "Администрирование → Поставщики";

б) выбрать ovirt-provider-ovn;

в) нажать кнопку Изменить и ввести новый пароль в поле "Пароль";

г) нажать кнопку Проверить, чтобы протестировать успешность аутентификации с предоставленными данными учетной записи;

д) в случае успешности проверки нажать кнопку OK.

4.5.7.3 Настройка интервала истечения времени ожидания сеанса пользователя

Администратор может настроить интервал истечения времени ожидания сеанса пользователя следующей командой:

```
# engine-config --set UserSessionTimeOutInterval=integer
```

4.5.7.4 Предварительное шифрование паролей пользователей

С помощью сценария ovirt-engine-crypto-tool администратор может создавать предварительно зашифрованные пароли пользователей. Эта возможность удобна, если пользователи и пароли добавляются в базу данных с помощью сценариев.

Примечание — Пароли хранятся в базе данных диспетчера виртуализации в зашифрованном виде. Сценарий ovirt-engine-crypto-tool используется потому, что все пароли должны быть зашифрованы с использованием одного и того же алгоритма.

Для предварительно зашифрованных паролей нельзя выполнить проверку действительности пароля. Пароль будет принят, даже если он не отвечает условиям политики валидации паролей.

Для шифрования пароля нужно выполнить следующие действия:

а) выполнить команду:

```
    # /usr/share/ovirt-engine/bin/ovirt-engine-crypto-tool.sh
pbe-encode
```

Сценарий предложит ввести пароль.

Как вариант, чтобы зашифровать один пароль, указанный в первой строке файла, можно использовать параметр --password=file:файл. Эта возможность удобна для автоматизации. В примере ниже файл — это текстовый файл с паролем, который нужно зашифровать:

```
    # /usr/share/ovirt-engine/bin/ovirt-engine-crypto-tool.sh
pbe-encode \
    --password=file:file
```

б) с помощью сценария ovirt-aaa-jdbc-tool с параметром --encrypted указать новый пароль:

```
    # ovirt-aaa-jdbc-tool user password-reset test1 \
    --password-valid-to="2025-08-01 12:00:00- 0800" --encrypted
```

в) ввести и подтвердить зашифрованный пароль:

```
    Password:
    Reenter password:
    updating user test1...
    user updated successfully
```

4.5.7.5 Просмотр информации о пользователях

Администратор может просматривать подробные сведения об учетных записях пользователей:

```
    # ovirt-aaa-jdbc-tool user show test1
```

Указанная команда выводит больше сведений, чем можно получить на экране "Администрирование → Пользователи" на Портале администрирования.

4.5.7.6 Изменение информации о пользователях

Администратор может обновлять информацию о пользователях, например почтовый адрес:

```
    # ovirt-aaa-jdbc-tool user edit test1 --
attribute=email=jdoe@example.com
```

4.5.7.7 Удаление пользователей

Администратор может удалять учетные записи пользователей:

```
    # ovirt-aaa-jdbc-tool user delete test1
```

Удаление пользователя с Портала администрирования описано в п. 4.5.6.3.

4.5.7.8 Отключение внутреннего пользователя-администратора

Администратор может отключать пользователей в локальных доменах, включая пользователя admin@internal, создаваемого во время выполнения `engine-setup`. Перед отключением изначального пользователя admin следует убедиться в том, что в окружении имеется еще как минимум один пользователь с полными административными полномочиями.

Последовательность действий по отключению внутреннего пользователя-администратора:

а) выполнить вход в Систему на машине с установленным диспетчером виртуализации;

б) убедиться в том, что в окружение был добавлен еще один пользователь с ролью SuperUser (подробности см. в п. 4.5.6.1);

в) отключить изначального пользователя admin:

```
    # ovirt-aaa-jdbc-tool user edit admin --flag=+disabled
```

Примечание — Чтобы включить отключенного пользователя, выполняют команду:

```
    # ovirt-aaa-jdbc-tool user edit username --flag=-disabled
```

4.5.7.9 Управление группами

С помощью утилиты ovirt-aaa-jdbc-tool можно управлять учетными записями групп во внутреннем домене. Управление учетными записями групп аналогично управлению учетными записями пользователей. Полный список возможностей для групп см. в выводе команды:

```
    ovirt-aaa-jdbc-tool group –help
```

В данном разделе приводятся общие примеры.

4.5.7.9.1 Создание группы пользователей

Данная последовательность действий позволяет создать группу пользователей, добавить пользователей в группу и просматривать сведения о группе:

а) выполнить вход в Систему на машине с установленным диспетчером виртуализации;

б) создать новую группу:

```
# ovirt-aaa-jdbc-tool group add group1
```

в) добавить пользователей, которые должны уже быть созданы ранее, в группу:

```
# ovirt-aaa-jdbc-tool group-manage useradd group1 --
user=test1
```

Примечание — Полный список параметров управления группами см. в выводе команды:

```
ovirt-aaa-jdbc-tool group- manage --help
```

г) просмотреть сведения об учетной записи группы:

```
# ovirt-aaa-jdbc-tool group show group1
```

д) добавить только что созданную группу на Портале администрирования и выделить группе необходимые роли и полномочия.

Пользователи-участники группы наследуют роли и полномочия группы.

4.5.7.9.2 Создание вложенных групп

Данная процедура позволяет создать группу внутри группы:

а) выполнить вход в Систему на машине с установленным диспетчером виртуализации;

б) создать новую группу:

```
# ovirt-aaa-jdbc-tool group add group1
```

в) создать вторую группу:

```
# ovirt-aaa-jdbc-tool group add group1-1
```

г) добавить вторую группу к первой:

```
    # ovirt-aaa-jdbc-tool group-manage groupadd group1 --
group=group1-1
```

д) добавить первую группу на Портале администрирования и присвоить группе необходимые роли и полномочия.

4.5.7.10 Запрос сведений о группах и пользователях

Модуль query дает возможность запросить сведения о пользователях и группах. Полный список параметров можно посмотреть в выводе команды:

```
    ovirt-aaa-jdbc-tool query --help
```

4.5.7.10.1 Просмотр сведений об учетных записях всех пользователей или групп

Данная последовательность действий позволяет просмотреть информацию обо всех учетных записях:

а) выполнить вход в Систему на машине с установленным диспетчером виртуализации;

б) получить список сведений об учетных записях:

– учетные записи всех пользователей:

```
    # ovirt-aaa-jdbc-tool query --what=user
```

– учетные записи всех групп:

```
    # ovirt-aaa-jdbc-tool query --what=group
```

4.5.7.10.2 Получение списка учетных записей с применением фильтра

Данная процедура показывает, как применять фильтры при получении списка сведений об учетных записях:

а) выполнить вход в Систему на машине с установленным диспетчером виртуализации;

б) применить фильтр к информации об учетной записи с помощью параметра –pattern.

Например, чтобы получить список учетных записей с именами, начинающимися с символа "j", выполняют команду:

```
    # ovirt-aaa-jdbc-tool query --what=user --pattern="name=j*"
```

Чтобы получить список групп со значением "marketing" атрибута department, выполняю команду:

```
    # ovirt-aaa-jdbc-tool query --what=group --
pattern="department=marketing"
```

4.5.7.11 Управление параметрами учетных записей

Для изменения исходных параметров учетной записи используется модуль ovirt-aaa-jdbc-tool settings.

4.5.7.11.1 Обновление информации о параметрах учетной записи

Данная последовательность действий показывает, как изменить изначальные параметры учетной записи:

а) выполнить вход в Систему на машине с установленным диспетчером виртуализации;

б) для просмотра всех доступных параметров выполнить следующую команду:

```
    # ovirt-aaa-jdbc-tool settings show
```

в) изменить необходимые параметры:

– в данном примере изначальное значение длительности сеанса пользователя (10080 минут) изменяется на 60 минут для всех учетных записей пользователей:

```
    # ovirt-aaa-jdbc-tool settings set --name=MAX_LOGIN_MINUTES
--value=60
```

– в данном примере изменяется значение числа неудачных попыток входа в Систему, которые может выполнить пользователь до того, как его учетная запись будет заблокирована (значение по умолчанию – "5"):

```
    # ovirt-aaa-jdbc-tool settings set --
name=MAX_FAILURES_SINCE_SUCCESS \
    --value=3
```

Примечание — Для разблокирования учетной записи пользователя нужно выполнить команду:

```
    ovirt-aaa-jdbc-tool user unlock test1
```

4.5.8 Настройка дополнительных локальных доменов

Создание дополнительных локальных доменов, помимо изначального домена internal, также поддерживается. Это выполняется с помощью расширения ovirt-engine-extension-aaa-jdbc, дающего возможность создания более одного домена без присоединения внешних серверов каталогов, хотя такой сценарий использования не очень часто встречается в корпоративных окружениях.

Дополнительно созданные локальные домены не будут обновляться автоматически во время стандартных обновлений версий РОСА Виртуализация: после выходов следующих версий эти домены необходимо будет обновлять вручную. Дополнительные сведения о создании дополнительных локальных доменов и об обновлении версий этих доменов см. в файле README, расположенном по пути /usr/share/doc/ovirt-engine-extension-aaa-jdbc-версия/README.admin.

4.6 Квоты и политика соглашения об уровне обслуживания

4.6.1 Что такое Quota

Quota — это утилита ограничения ресурсов, предоставляемая РОСА Виртуализация. Quota может быть описана в виде слоя ограничений, располагающегося поверх слоя ограничений, налагаемых полномочиями пользователей.

Quota является объектом дата-центра.

Quota предоставляет возможность администраторам окружений Системы РОСА Виртуализация ограничивать доступ пользователей к памяти, ЦП и хранилищам. Quota определяет объем ресурсов памяти и хранилища, который администраторы могут выделить пользователям. В итоге пользователи могут расходовать только те ресурсы, которые им были выделены.

Существует два различных типа квот:

– Quota времени выполнения ограничивает потребление ресурсов времени выполнения, таких как ЦП и память;
– Quota хранилища ограничивает доступный объем хранилища.

У Quota, как и у SELinux, есть три режима, представленных в таблице 71.

Таблица 71 – Режимы квот

Режим	Функция
Принудительный	Этот режим осуществляет квоту, настроенную в режиме "Аудит", ограничивая ресурсы для группы или пользователя, подпадающего под квоту
Аудит	В данном режиме осуществляется журналирование нарушений квоты без блокирования пользователей. Этот режим можно использовать для тестирования квот. В режиме "Аудит" можно повышать или понижать размер квоты времени выполнения и размер квоты на использование хранилища для пользователей, подпадающих под эту квоту
Отключен	Этот режим отключает ограничения времени выполнения и ограничения на использования хранилища, установленные квотой

При попытке пользователя запустить ВМ ее спецификации сравниваются с допустимыми нормами хранилища и допустимыми нормами времени выполнения, указанными в применимой квоте.

Если при запуске ВМ все агрегированные ресурсы всех выполняющихся ВМ, покрываемых квотой, превышают допустимую норму, определенную квотой, то в этом случае диспетчер виртуализации откажется запускать машину.

При создании нового диска пользователем запрошенный размер диска добавляется к общему объему дисков, покрываемых применимой квотой. Если общий объем, включая объем нового диска, превышает объем, разрешенный квотой, то диск не будет создан.

Quota допускает разделение ресурсов одного аппаратного обеспечения. Есть поддержка мягкого и жесткого порогов. Администраторы могут использовать квоту для настройки порогов использования ресурсов. С точки зрения пользователя, эти пороги выглядят как стопроцентное использование данного ресурса. Для предотвращения сбоев при неожиданном превышении этих порогов в интерфейсе присутствует поддержка "льготного" значения, на которое может быть превышено пороговое значение в течение краткого периода времени. При превышении порога пользователю показывается предупреждение.

Примечание — Квота накладывает ограничения на выполнение виртуальных машин. Игнорирование этих ограничений с большой вероятностью приведет к ситуациям, при которых использование ВМ и виртуальных дисков станет невозможным.

В принудительном режиме квоты виртуальные машины и диски, не имеющие присвоенных квот, не могут использоваться.

Для возможности запуска ВМ этой ВМ должна быть присвоена квота.

Для создания снимка ВМ диску, связанному с этой ВМ, должна быть присвоена квота.

При создании шаблона на базе ВМ будет предложено выбрать квоту, которую должен потреблять шаблон. Это дает возможность указать для шаблона (и для всех будущих ВМ, которые будут созданы на базе этого шаблона) другую квоту, чем квоты, настроенные для ВМ и диска, на базе которых создается этот шаблон.

4.6.2 Общие и индивидуальные квоты

Пользователи с полномочиями SuperUser могут создавать квоты для отдельных пользователей или квоты для групп.

Для пользователей Active Directory можно настроить групповые квоты. Если группе из десяти пользователей будет назначена квота в 1 ТБ в хранилище, а один из этих десяти пользователей заполнит весь этот объем, то в таком случае квота будет превышена для всей группы, и ни один из десяти пользователей не сможет использовать хранилище, связанное с этой группой.

Квота отдельного пользователя настраивается для одного пользователя. Как только вся квота хранилища времени выполнения будет превышена отдельным пользователем, этот пользователь больше не сможет использовать хранилище, связанное с его квотой.

4.6.3 Расчет квот

При назначенной пользователю или ресурсу квоте каждое действие этого потребителя или действие с ресурсом, включающим хранилище, виртуальный ЦП или память, приводит к потреблению квоты или освобождению квоты.

Поскольку квота действует как верхний предел, ограничивающий пользовательский доступ к ресурсам, рассчитанное значение квоты может отличаться от текущего потребления пользователем. Квота рассчитывается для максимального потенциала роста, а не для текущего потребления.

Пример расчета квоты:

Пользователь запустил ВМ с 1 виртуальным ЦП и 1024 МБ памяти. Это действие потребляет 1 виртуальный ЦП и 1024 МБ квоты, выделенной этому пользователю. После остановки этой ВМ 1 ЦП и 1024 МБ ОЗУ возвращаются обратно в квоту, присвоенную этому пользователю. Потребление квоты времени выполнения считается только во время фактического времени выполнения потребителя. Пользователь создает виртуальный диск тонкого резервирования размером в 10 ГБ. Фактическое потребление дискового объема может указывать, что используется только 3 ГБ. Но потребление квоты, тем не менее, будет составлять 10 ГБ, т.е. максимальный потенциал роста этого диска.

4.6.4 Включение и изменение режима квот в дата-центре

Данная последовательность действий включает или изменяет режим квоты в дата-центре. Перед определением квот необходимо выбрать режим квоты. Чтобы иметь возможность выполнять шаги данной процедуры, необходимо выполнить вход на Портал администрирования.

Для тестирования квоты и проверки соответствия ожиданиям используется режим "Аудит". Для создания или изменения квоты режим "Аудит" необязателен.

Последовательность действий по включению и изменению режима квот в дата-центре:

а) нажать "Ресурсы → Дата-центры" и выбрать дата-центр;

б) нажать кнопку Изменить;

в) в выпадающем списке "Режим квоты" изменить режим на "Принудительный";

г) нажать кнопку OK.

Если во время тестирования установить режим "Аудит", то для того чтобы параметры квоты вступили в силу, режим необходимо сменить на "Принудительный".

4.6.5 Создание новых политик квотирования

Если администратор включил режим квоты либо в режиме "Аудит", либо в режиме "Принудительный", то теперь необходимо настроить политику квоты для управления потреблением ресурсов в дата-центре.

Последовательность действий по созданию новых политик квотирования:

а) нажать "Администрирование → Квота";

б) нажать кнопку Добавить;

в) заполнить поля "Название" и "Описание";

г) выбрать "Дата-центр";

д) в секции "Память и ЦП" с помощью зеленого бегунка настроить "Порог кластера";

е) в секции "Память и ЦП" с помощью голубого бегунка настроить "Льготу кластера";

ж) активировать переключатель "Все кластеры" или переключатель "Конкретные кластеры". При выборе переключателя "Конкретные кластеры" отметить кластеры, для которых нужно добавить политику квоты;

з) нажать кнопку Изменить, чтобы открыть окно "Изменить квоту";

и) в поле "Память" активировать либо переключатель "Без ограничений", чтобы не ограничивать использование ресурсов памяти в кластере, либо активировать переключатель "Ограничить до", чтобы указать объем памяти, установленный для этой квоты. При выборе переключателя "Ограничить до" указать объем памяти в МБ в поле "МБ";

к) в поле "ЦП" активировать либо переключатель "Без ограничений", либо переключатель "Ограничить до", чтобы указать объем ЦП, установленный для этой квоты. При выборе переключателя "Ограничить до" указать число виртуальных ЦП в поле "ЦП";

л) нажать кнопку OK в окне "Изменить квоту";

м) в секции "Хранилище" с помощью зеленого бегунка настроить "Порог хранилища";

н) в секции "Хранилище" с помощью голубого бегунка настроить "Льготу хранилища";

о) активировать переключатель "Все домены хранилищ" или "Конкретные домены хранилищ". При выборе переключателя "Конкретные домены хранилищ" отметить домены хранения, для которых нужно добавить политику квоты;

п) нажать кнопку Изменить, чтобы открыть окно "Изменить квоту";

р) в поле "Квота хранилища" активировать либо переключатель "Без ограничений", чтобы не ограничивать использование ресурсов хранилища, либо активировать переключатель "Ограничить до", чтобы указать объем хранилища, до которого пользователи будут ограничены квотой. При выборе переключателя "Ограничить до" указать объем размера квоты на хранилище в ГБ в поле "ГБ";

с) нажать кнопку OK в окне "Изменить квоту";

т) нажать кнопку OK в окне "Новая квота".

4.6.6 Описание параметров порога квоты

Параметры квот представлены в таблица 72.

Таблица 72 – Пороги и льготы квот

Параметр	Определение
Порог кластера	Объем ресурсов кластера, доступный для каждого из дата-центров
Льгота кластера	Объем ресурсов кластера, доступный дата-центру после исчерпания объема, указанного значением порога кластера дата-центра
Порог хранилища	Объем ресурсов хранилища, доступный для каждого из дата-центров
Льгота хранилища	Объем ресурсов хранилища, доступный дата-центру после исчерпания объема, указанного значением порога хранилища

При квоте, установленной в 100 ГБ со льготой в 20%, потребителям будет запрещено использование хранилища после того, как используемый ими объем хранилища достигнет 120 ГБ. Если та же самая квота имеет значение порога в 70%, тогда потребителям выводится предупреждение в момент, когда используемый ими объем превысит 70 ГБ (но остается возможность потреблять хранилище до тех пор, пока потребляемый объем не достигнет 120 ГБ).

Как значение "Порога", так и значение "Льготы" настраиваются относительно значения квоты. "Порог" можно представить как "мягкий предел" – при его превышении выводится предупреждение. "Льготу" можно представить как "жесткое ограничение" – при его превышении дальнейшее потребление ресурсов хранилища становится невозможным.

4.6.7 Присвоение квот объектам

Для присвоения квот виртуальным машинам нужно:

а) нажать "Ресурсы → ВМ" и выбрать виртуальную машину;
б) нажать кнопку Изменить;

в) в выпадающем списке "Квота" выбрать квоту, которую будет потреблять выбранная ВМ;

г) нажать кнопку ОК.

4.6.8 Присвоение квоты диску

Для присвоения квоты диску требуется:

а) нажать "Ресурсы → ВМ";

б) нажать на имя ВМ, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Диски" и выбрать диск, который планируется связать с квотой;

г) нажать кнопку Изменить;

д) в выпадающем списке "Квота" выбрать квоту, которую будет потреблять выбранный виртуальный диск;

е) нажать кнопку ОК.

Примечание — Для работы ВМ необходимо, чтобы для всех объектов, связанных с этой ВМ, была выбрана квота. Если квота для всех объектов не будет выбрана, ВМ не будет работать. Ошибка, которую выдает при этом диспетчер виртуализации, является очень общей, что затрудняет нахождение ее связи с отсутствием присвоения квот объектам, связанным с виртуальной машиной. Нельзя сделать снимок ВМ, которой не была присвоена квота. Нельзя сделать шаблон на базе ВМ, виртуальным дискам которой не были присвоены квоты.

4.6.9 Использование квот для ограничения потребления ресурсов пользователем

Данная последовательность действий показывает, как с помощью квот ограничить доступные пользователю ресурсы.

Последовательность действий по использованию квот для ограничения потребления ресурсов пользователем:

а) выбрать "Администрирование → Квота";

б) нажать на название целевой квоты, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Потребители";

г) нажать кнопку Добавить;

д) в поле "Поиск" ввести имя пользователя, которого нужно связать с квотой;

е) нажать кнопку Выполнить;

ж) установить флажок рядом с именем пользователя;

з) нажать кнопку OK.

Через некоторое время пользователь появится во вкладке "Потребители".

4.6.10 Редактирование квот

Данная последовательность действий показывает, как изменять существующие квоты.

Последовательность действий по редактированию квот:

а) нажать "Администрирование → Квота" и выбрать квоту;

б) нажать кнопку Изменить;

в) внести необходимые изменения;

г) нажать кнопку OK.

4.6.11 Удаление квот

Данная последовательность действий показывает, как удалять квоты.

Последовательность действий по удалению квот:

а) нажать "Администрирование → Квота" и выбрать квоту;

б) нажать кнопку Удалить;

в) нажать кнопку OK.

4.6.12 Принудительное применение политики соглашения об уровне обслуживания

Данная последовательность действий показывает, как настроить параметры ЦП согласно соглашению об уровне обслуживания.

Последовательность действий по принудительному применению политики соглашения об уровне обслуживания

а) нажать "Ресурсы → ВМ";

б) нажать кнопку Создать или выбрать ВМ и нажать кнопку Изменить;

в) перейти на вкладку "Выделение ресурсов";

г) указать "Ресурсы ЦП" с возможными значениями:

– "Высокое" – ВМ получают в два раза больше ресурсов, чем ВМ, для которых указано "Среднее" значение;
– "Среднее" – ВМ со "Средним" значением получают в два раза больше ресурсов, чем ВМ, для которых указано "Низкое" значение;
– "Низкое";
– "Отключено" – указывает, что для расчета распределения долей демон VDSM должен использовать старый алгоритм; как правило, число долей, распределяемых в этих условиях, равно "1020".

Потребление ресурсов ЦП пользователями теперь управляется настроенной политикой.

4.7 Система событий (ГОСТ)

Графический интерфейс системы событий (ГОСТ) являются частью интерфейса РОСА Виртуализация и устанавливается из отдельного дистрибутива.

Для перехода в раздел событий (ГОСТ) необходимо в меню выбрать "Дополнения → События (ГОСТ)" (Рисунок №1). В открывшейся рабочей области отобразится графический интерфейс, позволяющий просматривать события в виде таблицы по 100 записей (рисунок 251). В таблице можно выполнять следующие действия:

– просмотр прошлых событий с использованием пагинации кнопками < и >;

– сортировка событий по любому параметру нажатием мышью на заголовки столбцов: первое нажатие осуществляет сортировку по возрастанию, второе – по убыванию, а третье отменяет сортировку;

– отображение полной информации о событии в отдельном окне двукратным нажатием мыши на событие (рисунок 252).

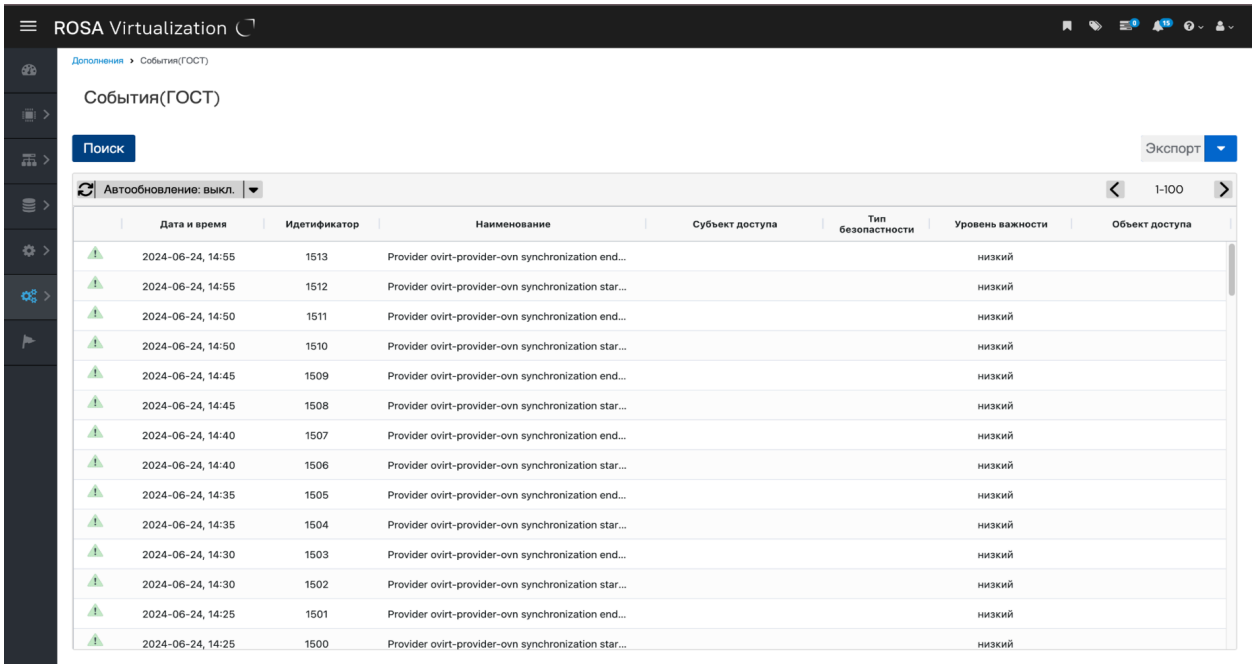


Рисунок 251 – События (ГОСТ)

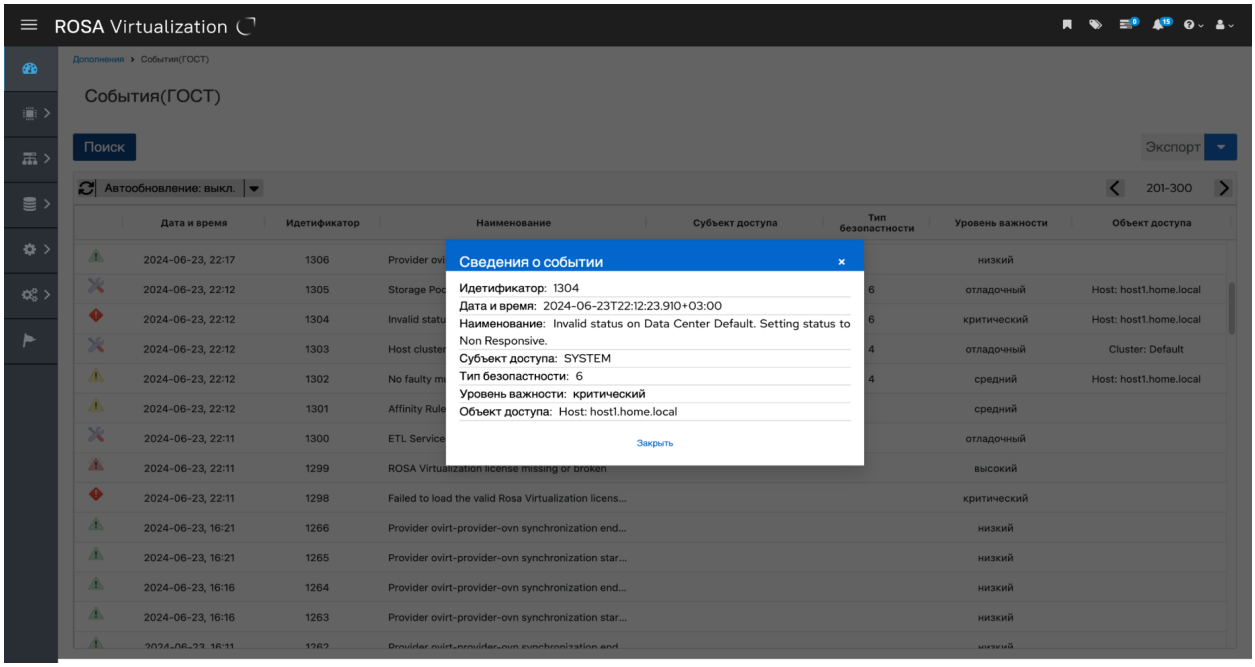


Рисунок 252 – Просмотр сведений о событии

4.7.1 Поиск событий

Функция позволяет фильтровать события (ГОСТ) по следующим параметрам (рисунок 253):

– Наименование событий;
– Дата и время;
– Уровень важности.

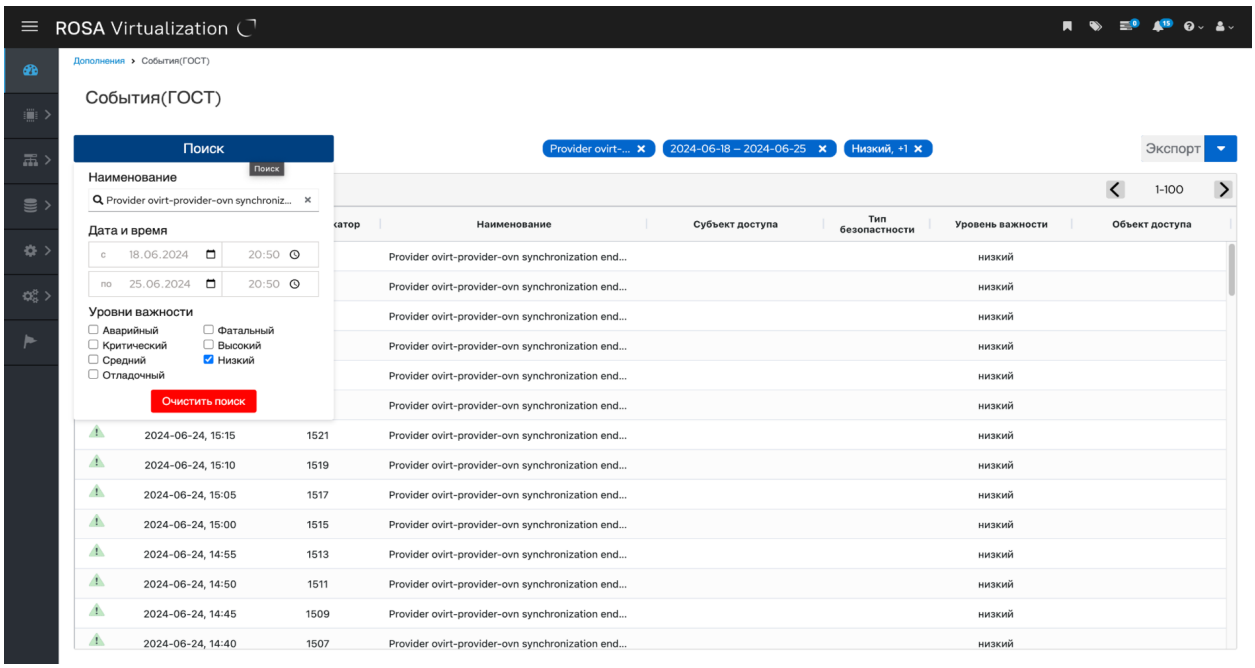


Рисунок 253 – Фильтрация событий

Для очистки всех фильтров можно нажать на кнопку `Очистить поиск`.

При использовании функции поиска в верхней части таблицы появляются активные фильтры, параметры которых можно редактировать (рисунок 254).

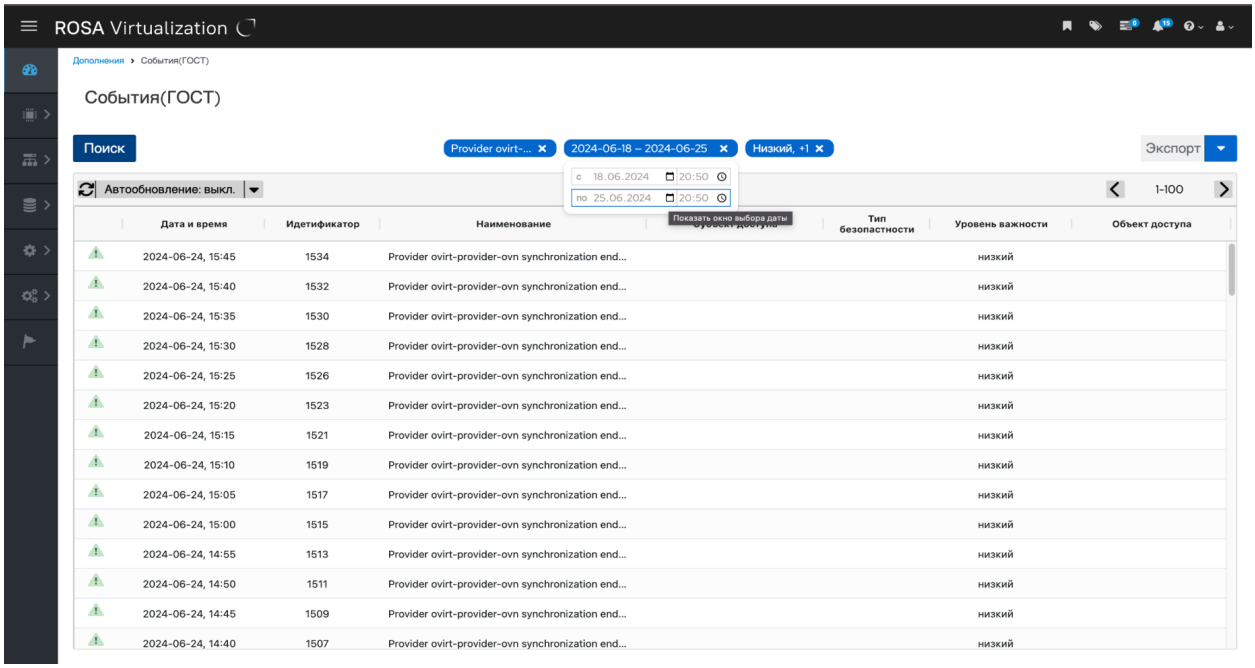


Рисунок 254 – Редактирование фильтра

Чтобы очистить конкретный параметр, нужно нажать на пиктограмму  у соответствующего активного фильтра.

4.7.2 Обновление событий

В системе событий (ГОСТ) реализованы возможности обновления и мониторинга новых событий.

Для обновления событий необходимо нажать на пиктограмму  (рисунок 255). Если появились новые события, они отобразятся в таблице и будут выделены серым цветом; при появлении нескольких событий будут выделены только первое и последнее. Если на экране отображаются не первые 100 записей, при нажатии на пиктограмму обновления произойдет перемещение на первые 100 записей и обновление событий.

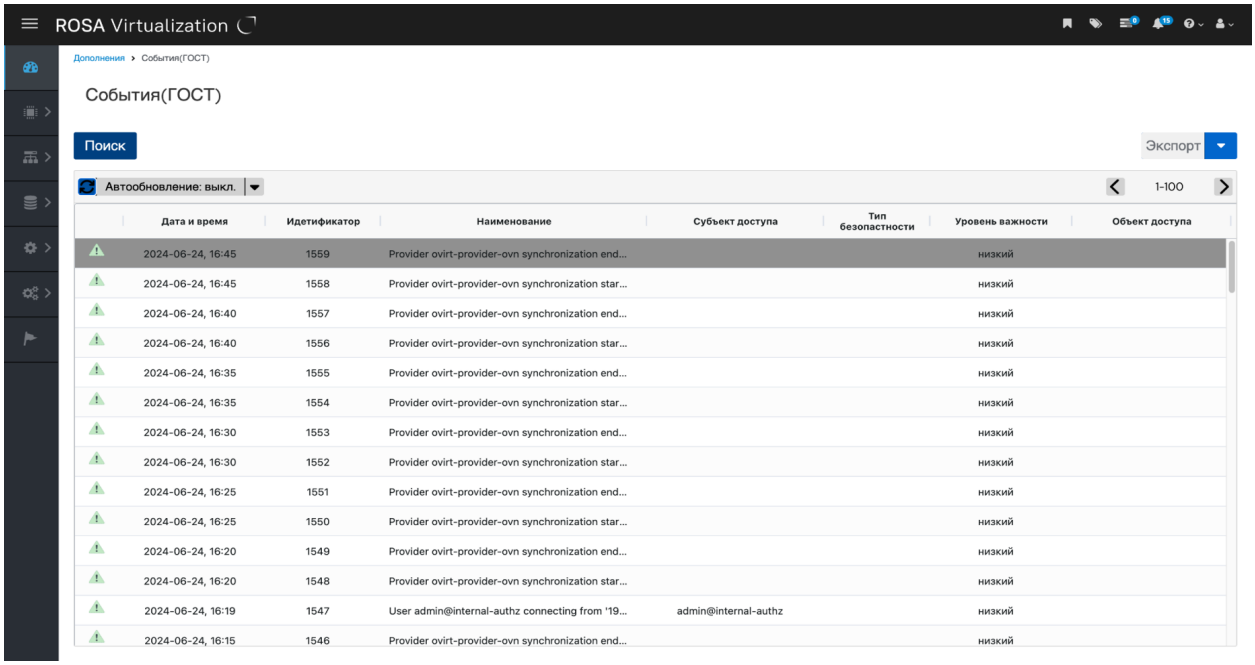


Рисунок 255 – Обновление событий

Мониторинг новых событий осуществляется через функцию автообновления событий. Для ее активации нужно выбрать интервал автообновления (рисунок 256). При этом, если в таблице отображаются не первые 100 записей, произойдет перемещение на первые 100 записей. Отключение автообновления происходит в следующих случаях:

– при перемещении на прошлые события (начиная с 200, 300 и т. д.);

– через 3 минуты, если окно с событиями (ГОСТ) неактивно или браузер свернут, отобразится диалоговое окно с сообщением об отключении, при закрытии которого автообновление снова включится;

– через 15 минут, если пользователь неактивен при открытом окне с событиями (ГОСТ), отобразится диалоговое окно с сообщением об отключении, при закрытии которого автообновление снова включится.

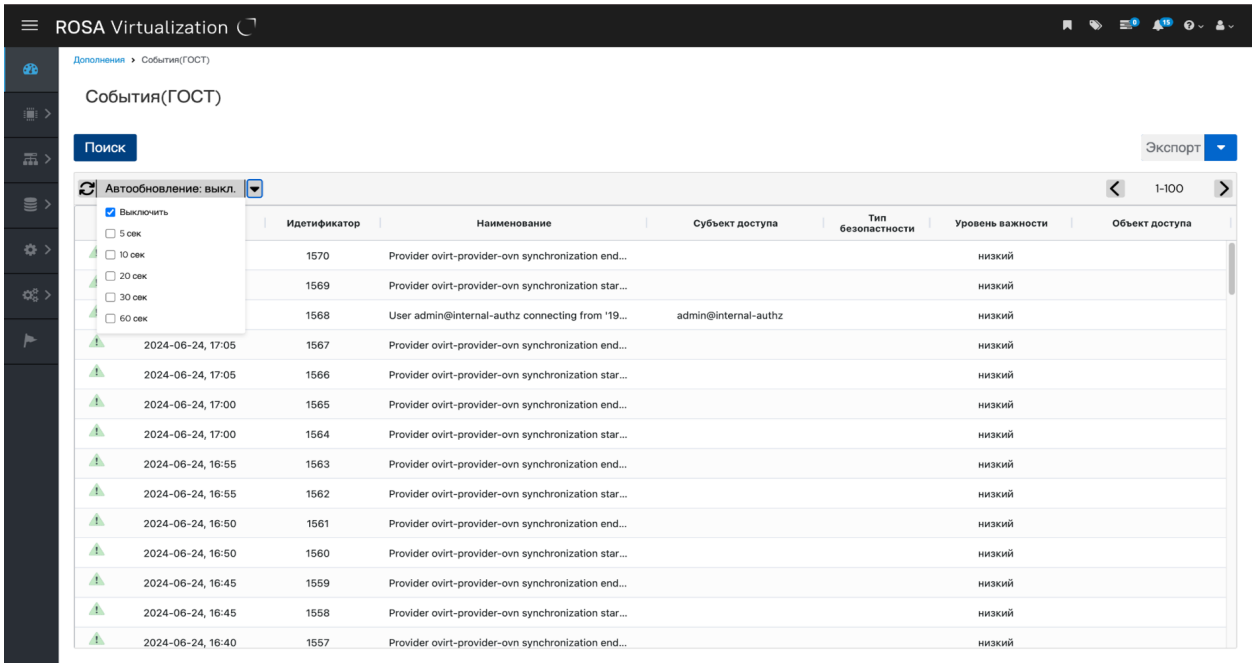


Рисунок 256 – Автообновление событий

4.7.3 Экспорт

В Системе реализован экспорт событий в файлы форматов .pdf, .odt, .docx, .txt, .csv (рисунок 257). Для экспорта необходимо выбрать формат файла. После выбора кнопка экспорта станет активной и изменит цвет. По нажатию начнется процесс экспорта файла (рисунок 258), который по завершении будет загружен на компьютер (рисунок 259).

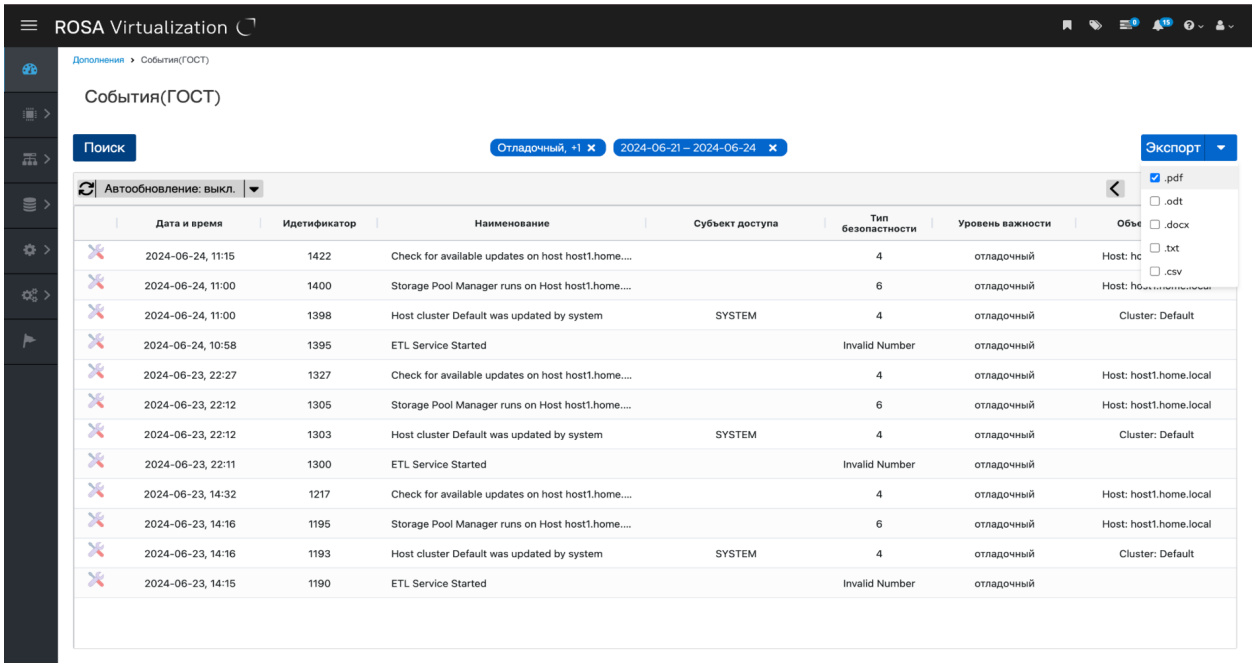


Рисунок 257 – Выбор формата файла для экспорта

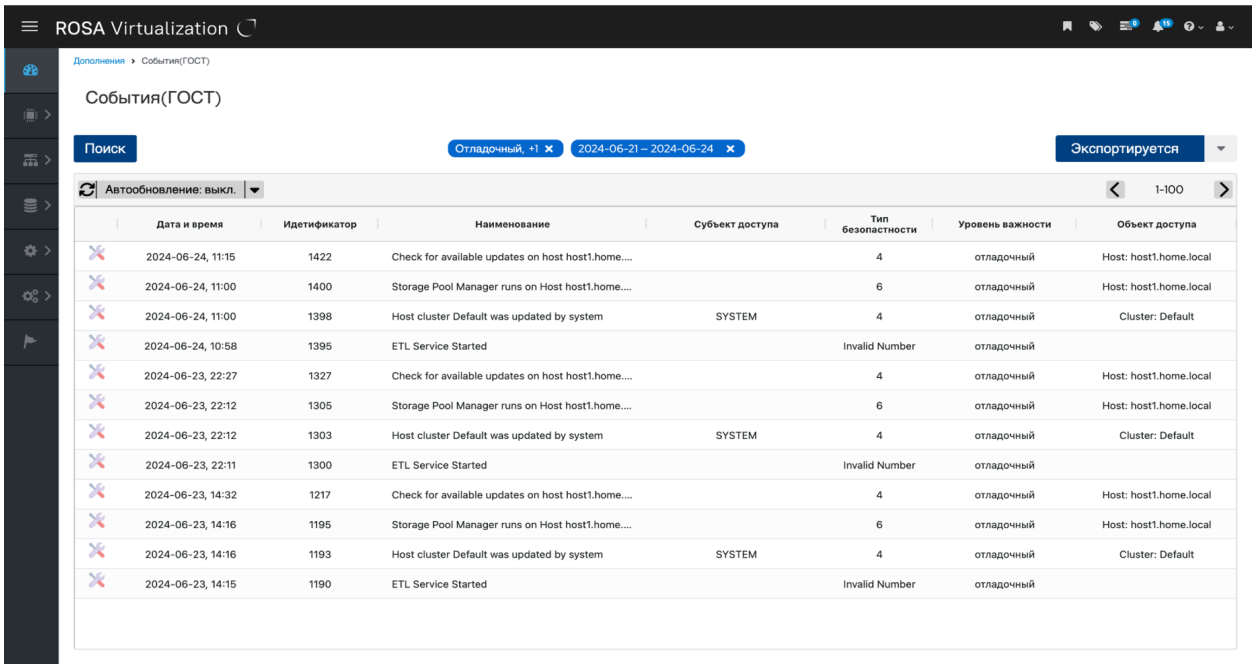


Рисунок 258 – Процесс экспорта

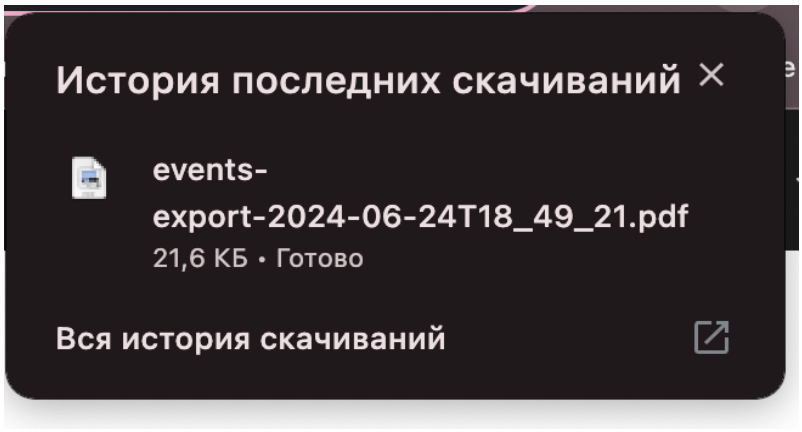


Рисунок 259 – Результат экспорта

4.8 Уведомления о событиях

4.8.1 Настройка уведомлений о событиях на Портале администрирования

При возникновении конкретных событий в окружении, управляемом диспетчером Системы РОСА Виртуализация, диспетчер может послать почтовое сообщение предварительно назначенным пользователям с уведомлением об этом событии. Чтобы использовать эту возможность, необходимо настроить агента пересылки сообщений. На Портале администрирования можно настроить только почтовые уведомления. Ловушки SNMP настраиваются на машине СУСВ.

Последовательность действий по настройке уведомлений о событиях:

а) убедиться в том, что имеется доступ на почтовый сервер, который может принимать автоматизированные сообщения из виртуализированного ЦУ и доставлять их по списку адресатов;

б) нажать "Администрирование → Пользователи" и выбрать пользователя;

в) нажать на "Имя" пользователя, чтобы перейти на страницу подробного просмотра;

г) на вкладке "Уведомления о событиях" нажать кнопку Управление событиями;

д) для просмотра событий использовать кнопку Развернуть все или отдельные кнопки развертывания по темам;

е) отметить флажками необходимые элементы;

ж) в поле "Получатель почты" ввести почтовый адрес;

з) нажать кнопку OK.

Примечание — Почтовый адрес может быть адресом для отправления СМС (например, 1234567890@carrierdomainname.com) или почтовым адресом группы, включающим в себя как обычные почтовые адреса, так и почтовые адреса для отправления СМС.

и) на машине диспетчера скопировать ovirt-engine-notifier.conf в новый файл с именем 90-email-notify.conf:

```
    # cp /usr/share/ovirt-engine/services/ovirt-engine-
notifier/ovirt-engine-notifier.conf /etc/ovirt-
engine/notifier/notifier.conf.d/90-email-notify.conf
```

к) отредактировать файл 90-email-notify.conf, удалив все, кроме раздела "EMAIL Notifications";

л) указать корректные почтовые переменные, следуя примеру ниже. Данный файл переопределяет значения в исходном файле ovirt-engine-notifier.conf file.

```
    #   #
    # EMAIL Notifications #
    #   #

    # The SMTP mail server address. Required.
    MAIL_SERVER=myemailserver.example.com

    # The SMTP port (usually 25 for plain SMTP, 465 for SMTP
with SSL, 587 for SMTP with TLS)
    MAIL_PORT=25

    # Required if SSL or TLS enabled to authenticate the user.
Used also to specify 'from' user address if mail server
    # supports, when MAIL_FROM is not set. Address is in RFC822
format MAIL_USER=

    # Required to authenticate the user if mail server requires
authentication or if SSL or TLS is enabled
```

```
     SENSITIVE_KEYS="${SENSITIVE_KEYS},MAIL_PASSWORD"
MAIL_PASSWORD=

     # Indicates type of encryption (none, ssl or tls) should be
used to communicate with mail server.
     MAIL_SMTP_ENCRYPTION=none

     # If set to true, sends a message in HTML format.
     HTML_MESSAGE_FORMAT=false

     # Specifies 'from' address on sent mail in RFC822 format, if
supported by mail server.
     MAIL_FROM=rhevm2017@example.com

     # Specifies 'reply-to' address on sent mail in RFC822
format. MAIL_REPLY_TO=

     # Interval to send smtp messages per # of IDLE_INTERVAL
MAIL_SEND_INTERVAL=1



     # Amount of times to attempt sending an email before
failing. MAIL_RETRIES=4
```

Примечание – Дополнительные параметры см. в файле /etc/ovirt-engine/notifier/notifier.conf.d/README.

м) для применения внесенных изменений активировать и перезапустить службу ovirt-engine-notifier:

```
     # systemctl daemon-reload
     # systemctl enable ovirt-engine-notifier.service
     # systemctl restart ovirt-engine-notifier.service
```

Указанный пользователь с этого момента будет получать почтовые сообщения о событиях в окружении Системы РОСА Виртуализация. Выбранные события будут показываться во вкладке "Уведомления о событиях" этого пользователя.

4.8.2 Отмена уведомлений о событиях на Портале администрирования

Если пользователь ранее настроил ненужные почтовые уведомления и хочет их отменить, то применяется следующая последовательность действий по отмене уведомлений о событиях на Портале администрирования:

а) нажать "Администрирование → Пользователи";

б) нажать на "Имя" пользователя, чтобы перейти к подробному просмотру;

в) перейти на вкладку "Уведомления о событиях", чтобы просмотреть события, для которых пользователь ранее настроил получение почтовых уведомлений;

г) нажать кнопку Управление событиями;

д) для просмотра событий использовать кнопку Развернуть все или отдельные кнопки развертывания по темам;

е) снять соответствующие флажки для отмены уведомлений по этим событиям;

ж) нажать кнопку OK.

4.8.3 Параметры уведомлений о событиях в файле ovirt-engine-notifier.conf

Файл конфигурации уведомителя о событиях можно найти по пути /usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf.

В таблице 73 описаны переменные для файла ovirt-engine-notifier.conf.

Таблица 73 – Переменные в файле ovirt-engine-notifier.conf

Имя переменной	По умолчанию	Примечание
SENSITIVE_KEYS	нет	Список ключей через запятую, которые не будут регистрироваться
JBOSS_HOME	/opt/rh/eap7/root/usr/share/wildfly	Местоположение сервера приложений JBoss, используемого диспетчером виртуализации
ENGINE_ETC	/etc/ovirt-	Местоположение каталога etc,

Имя переменной	По умолчанию	Примечание
	engine	используемого диспетчером виртуализации
ENGINE_LOG	/var/log/ovirt-engine	Местоположение каталога logs, используемого диспетчером виртуализации
ENGINE_USR	/usr/share/ovirt-engine	Местоположение каталога usr, используемого диспетчером виртуализации
ENGINE_JAVA_MODULEPATH	${ENGINE_USR}/modules	Путь, в конец которого добавляются модули JBoss
NOTIFIER_DEBUG_ADDRESS	нет	Адрес машины, которую можно использовать для выполнения удаленной отладки виртуальной машины Java, используемой уведомителем
NOTIFIER_STOP_TIME	30	Истечение времени ожидания службы в секундах
NOTIFIER_STOP_INTERVAL	1	Промежуток времени в секундах, на который будет увеличен счетчик истечения времени ожидания
INTERVAL_IN_SECONDS	120	Интервал в секундах между доставками сообщений подписчикам.
IDLE_INTERVAL	30	Интервал в секундах, по истечению которого будут выполняться задачи с низким приоритетом
DAYS_TO_KEEP_HISTORY	0	Эта переменная указывает число дней, в течение которых доставленные сообщения будут сохраняться в таблице истории. Если эта переменная не настроена, события хранятся бесконечно долго
FAILED_QUERIES_NOTIFICATIO	30	Число неудачных запросов, после которых будет послано почтовое

Имя переменной	По умолчанию	Примечание
N_THRESHOLD		уведомление. Уведомление отсылается после первого сбоя и затем по одному разу после того, как в очередной раз будет достигнуто число сбоев, указанное данной переменной. Если указать значение "1" или "0", почтовое уведомление будет отправляться после каждого сбоя
FAILED_QUERIES_NOTIFICATIO N_RECIPIENTS	нет	Почтовые адреса получателей, на которые будут отсылаться почтовые уведомления. Адреса разделяются запятыми. Этот элемент стал устаревшим после введение переменной FILTER
DAYS_TO_SEND_ON_STARTUP	0	Число дней, когда происходили старые события, которые будут обработаны и для которых будут посланы сообщения при запуске уведомителя. Если значение равно "0", а служба останавливается и запускается после некоторого временного промежутка, то все уведомления, случившиеся в промежутке между моментами остановки и запуска службы, будут утеряны. Если эти уведомления необходимо получать, указать значение "1" или выше
FILTER	exclude:*	Алгоритм, используемый для определения пусковых событий для отправки уведомлений, а также получателей этих сообщений. Значение этой переменной включает в себя сочетание значений "include" или "exclude", событие и получателя. Например: "include:VDC_START(smtp:mail@example.com) ${FILTER}"

Имя переменной	По умолчанию	Примечание
MAIL_SERVER	нет	Адрес почтового сервера SMTP. Обязательное значение
MAIL_PORT	25	Порт, используемый для связи. Возможные значения: "25" – для простого SMTP, "465" – для SMTP с SSL, "587" – для SMTP с TLS
MAIL_USER	нет	Эту переменную необходимо настроить, если для аутентификации пользователей используется SSL. Также эта переменная используется для указания почтового адреса пользователя-отправителя, если переменная MAIL_FROM не настроена. Некоторые почтовые адреса не поддерживают этот функционал. Адрес указывается в формате RFC822
SENSITIVE_KEYS	${SENSITIVE_KEYS},MAIL_PASSWORD	Необходима для аутентификации пользователя, если почтовый сервер требует аутентификации или если используется SSL или TLS
MAIL_PASSWORD	нет	Необходима для аутентификации пользователя, если почтовый сервер требует аутентификации или если используется SSL или TLS
MAIL_SMTP_ENCRYPTION	нет	Тип шифрования, используемый при подключении. Возможные значения: "none", "ssl", "tls".
HTML_MESSAGE_FORMAT	false	При значении "true" сервер отсылает сообщения в формате HTML
MAIL_FROM	none	Эта переменная указывает адрес отправителя в формате RFC822, если он поддерживается почтовым сервером
MAIL_REPLY_TO	none	Эта переменная указывает адрес получателя в формате RFC822, если он

Имя переменной	По умолчанию	Примечание
		поддерживается почтовым сервером
MAIL_SEND_INTERVAL	1	Число сообщений SMTP, отправляемых для каждого интервала IDLE_INTERVAL
MAIL_RETRIES	4	Число попыток послать почту перед регистрацией сбоя
SNMP_MANAGERS	нет	IP-адреса или полные доменные имена машин, которые будут выполнять роль диспетчеров SNMP. Записи должны разделяться пробелом и могут содержать номер порта. Например: manager1.example.com; manager2.example.com:164
SNMP_COMMUNITY	public	(Только для SNMP версии 2) Общая строка SNMP
SNMP_OID	1.3.6.1.4.1.2312.13.1.1	Изначальный идентификатор объекта ловушки для предупреждений. При настроенном OID все типы ловушек отправляются (с добавленной информацией о событии) диспетчеру SNMP. Следует обратить внимание, что изменение ловушки по умолчанию делает невозможным ее соответствие административной базе данных диспетчера
SNMP_VERSION	2	Используемая версия SNMP. Поддерживаются ловушки SNMP версии 2 и версии 3. Возможные значения: "2" или 3
SNMP_ENGINE_ID	none	(SNMPv3) ID диспетчера, используемого для ловушек SNMPv3. Этот ID является уникальным идентификатором устройства, подключенного с помощью SNMP
SNMP_USERNAME	нет	(SNMPv3) Имя пользователя, используемого для ловушек SNMPv3

Имя переменной	По умолчанию	Примечание
SNMP_AUTH_PROTOCOL	нет	(SNMPv3) Протокол авторизации SNMPv3. Возможные значения: "MD5", "SHA"
SNMP_AUTH_PASSPHRASE	нет	(SNMPv3) Парольная фраза, если для параметра SNMP_SECURITY_LEVEL указаны значения "AUTH_NOPRIV" и "AUTH_PRIV"
SNMP_PRIVACY_PROTOCOL	нет	(SNMPv3) Протокол конфиденциальности SNMPv3. Возможные значения: "AES128", "AES192", "AES256." Для протоколов AES192 и AES256 не обозначены в RFC3826, поэтому перед включением использования этих протоколов следует убедиться, что сервер их поддерживает
SNMP_PRIVACY_PASSPHRASE	none	Парольные фразы конфиденциальности SNMPv3, используемые, если для параметра SNMP_SECURITY_LEVEL указано значение "AUTH_PRIV"
SNMP_SECURITY_LEVEL	1	(SNMPv3) Уровень защиты SNMPv3. Возможные значения: – 1 – NOAUTH_NOPRIV – 2 – AUTH_NOPRIV – 3 – AUTH_PRIV
ENGINE_INTERVAL_IN_SECOND S	300	Интервал в секундах между событиями мониторинга машины, на которой установлен диспетчер. Интервал отсчитывается от момента завершения мониторинга
ENGINE_MONITOR_RETRIES	3	Число попыток уведомителя выполнить мониторинг машины диспетчера за указанный интервал после неудачной попытки
ENGINE_TIMEOUT_IN_SECOND S	30	Интервал ожидания в секундах перед тем, как уведомитель попытается

Имя переменной	По умолчанию	Примечание
		выполнить мониторинг машины диспетчера за указанный интервал после неудачной попытки
IS_HTTPS_PROTOCOL	false	Если JBoss выполняется в защищенном режиме, данная переменная должна иметь значение "true"
SSL_PROTOCOL	TLS	Протокол, используемый коннектором конфигурации JBoss при включенном SSL
SSL_IGNORE_CERTIFICATE_ERRORS	false	Данная переменная должна иметь значение "true", если JBoss выполняется в защищенном режиме, а ошибки SSL должны будут игнорироваться
SSL_IGNORE_HOST_VERIFICATION	false	Данная переменная должна иметь значение "true", если JBoss выполняется в защищенном режиме, а ошибки верификации имени хоста должны будут игнорироваться
REPEAT_NON_RESPONSIVE_NOTIFICATION	false	Данная переменная указывает, будут ли отправляться подписчикам повторяющиеся сообщения об ошибках, если машина, на которой установлен диспетчер виртуализации, не отвечает
ENGINE_PID	/var/lib/ovirt-engine/ovirt-engine.pid	Путь и имя файла PID диспетчера виртуализации

4.8.4 Настройка отправки ловушек SNMP из диспетчера POCA Виртуализация

Отправка ловушек протокола SNMP (Simple Network Management Protocol – простой протокол сетевого управления) настраивается из диспетчера POCA Виртуализация на один или несколько внешних диспетчеров SNMP. Ловушки

SNMP содержат сведения о системных событиях и используются для наблюдения за окружением РОСА Виртуализация. Число и тип ловушек, отправляемых диспетчеру SNMP, можно настроить на диспетчере виртуализации.

Система РОСА Виртуализация поддерживает версии SNMP 2 и 3. В SNMP версии 3 поддерживаются следующие уровни защиты:

– NoAuthNoPriv – ловушки SNMP отправляются без необходимости авторизации или защиты конфиденциальности данных;

– AuthNoPriv – ловушки SNMP отправляются с авторизацией по паролю, но без защиты конфиденциальности данных;

– AuthPriv – ловушки SNMP отправляются с авторизацией по паролю и с защитой конфиденциальности данных.

Последовательность действий по настройке отправки ловушек SNMP:

а) на одном или более внешних диспетчерах SNMP настраивается получение ловушек;

б) IP-адреса или полные доменные имена машин, которые будут выполнять роль диспетчеров SNMP – опционально настроить порт, на котором диспетчер будет получать уведомления от ловушек. Порт по умолчанию: порт UDP, 162.

в) Комьюнити SNMP (только для SNMP версии 2) – несколько диспетчеров SNMP могут принадлежать к одному и тому же комьюнити. Системы управления и агенты могут взаимодействовать между собой только в границах одного комьюнити (по умолчанию – "public");

г) Идентификатор объектов ловушек для уведомлений – диспетчер РОСА Виртуализация предоставляет OID по умолчанию: "1.3.6.1.4.1.2312.13.1.1". При настройке данного OID все ловушки, дополненные сведениями о событии, отправляются диспетчеру SNMP. Следует обратить внимание, что изменение ловушки по умолчанию отменяет соответствие создаваемых ловушек требованиям базы MIB диспетчера;

д) Имя пользователя SNMP – для SNMP версии 3 и уровням защиты 1,2 и 3;

е) Парольная фраза SNMP – для SNMP версии 3 и уровням защиты 2 и 3;

ж) Закрытая парольная фраза – для SNMP версии 3 и уровня защиты 3;

Примечание – Диспетчер РОСА Виртуализация предоставляет базы MIB в файлах /usr/share/doc/ovirt-engine/mibs/OVIRT-MIB.txt. Следует загрузить базы в диспетчер SNMP до того, как продолжить.

Значение конфигурации SNMP по умолчанию присутствует на диспетчере в файле конфигурации демона уведомлений о событиях по пути /usr/share/ovirt-

engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf. Значения, упоминаемые в последовательности действий ниже, базируются на значениях по умолчанию либо примерных значениях из этого файла. Не следует редактировать файл напрямую, т. к. такие системные изменения, как обновления, могут в дальнейшем изменить его значения. Для редактирования файла нужно создать его копию в виде /etc/ovirt-engine/notifier/notifier.conf.d/<целое_число>-snmp.conf, где <целое_число> является числом, указывающим приоритет, с которым должен запускаться этот файл.

Последовательность действий по настройке отправки ловушек SNMP из диспетчера РОСА Виртуализация:

а) создать на диспетчере файл конфигурации SNMP с именем <целое_число>-snmp.conf, где <целое_число> — это число, указывающее порядок обработки файлов, например:

```
# vi /etc/ovirt-engine/notifier/notifier.conf.d/20-snmp.conf
```

Примечание — Следует скопировать значения SNMP по умолчанию из файла конфигурации демона уведомлений о событиях по пути /usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf. В этом файле есть построковые комментарии для каждого из параметров.

б) указать диспетчеров SNMP, комьюнити SNMP (только для SNMP версии 2) и OID в формате, приведенном в примере ниже:

```
SNMP_MANAGERS="manager1.example.com
manager2.example.com:162" SNMP_COMMUNITY=public
SNMP_OID=1.3.6.1.4.1.2312.13.1.1
```

в) указать используемую версию SNMP: версию 2 (по умолчанию) или 3:

```
SNMP_VERSION=3
```

г) указать значение "SNMP_ENGINE_ID", например:

```
SNMP_ENGINE_ID="80:00:00:00:01:02:05:05"
```

д) для SNMP версии 3 указать уровень защиты ловушек SNMP:

– Уровень защиты 1; ловушки NoAuthNoPriv:

```
SNMP_USERNAME=NoAuthNoPriv SNMP_SECURITY_LEVEL=1
```

– Уровень защиты 2; ловушки AuthNoPriv; от имени пользователя ovirtengine; с парольной фразой SNMP Auth authpass:

```
SNMP_USERNAME=ovirtengine SNMP_AUTH_PROTOCOL=MD5
SNMP_AUTH_PASSPHRASE=authpass SNMP_SECURITY_LEVEL=2
```

– Уровень защиты 3; ловушки AuthPriv; от имени пользователя ovirtengine; с парольной фразой SNMP Auth authpass и закрытой парольной фразой SNMP privpass., например:

```
SNMP_USERNAME=ovirtengine SNMP_AUTH_PROTOCOL=MD5
SNMP_AUTH_PASSPHRASE=authpass SNMP_PRIVACY_PROTOCOL=AES128
SNMP_PRIVACY_PASSPHRASE=privpass SNMP_SECURITY_LEVEL=3
```

е) указать, какие события отправляются на диспетчер SNMP, основываясь на примере событий:

– Отправлять все события на профиль SNMP по умолчанию:

```
FILTER="include:*(snmp:) ${FILTER}"
```

– Отправлять все события с уровнем серьезности ERROR или ALERT на профиль SNMP по умолчанию:

```
FILTER="include:*:ERROR(snmp:)  ${FILTER}"
FILTER="include:*:ALERT(snmp:) ${FILTER}"
```

– Отправлять события VDC_START на указанный почтовый адрес:

```
FILTER="include:VDC_START(snmp:mail@example.com) ${FILTER}"
```

– Отправлять все события, кроме событий VDC_START, на профиль SNMP по умолчанию:

```
FILTER="exclude:VDC_START include:*(snmp:) ${FILTER}"
```

Это фильтр по умолчанию, настроенный в ovirt-engine-notifier.conf. Если этот фильтр не будет отключен либо будут активированы перезаписывающие фильтры, уведомления о событиях отсылаться не будут:

```
FILTER="exclude:*"
```

VDC_START — это пример доступных сообщений журнала аудита. Полный список сообщений журнала аудита можно найти в файле /usr/share/doc/ovirt-engine/AuditLogMessages.properties. Как вариант, можно фильтровать журнальные сообщения в рамках диспетчера SNMP.

ж) сохранить файл;

з) запустить службу ovirt-engine-notifier и настроить запуск этой службы при загрузке:

```
# systemctl start ovirt-engine-notifier.service
# systemctl enable ovirt-engine-notifier.service
```

и) проверить получение ловушек на диспетчере SNMP.

Примечание — Для возможности работы службы уведомлений либо один из параметров "SNMP_MANAGERS", "MAIL_SERVER", либо оба эти параметра должны быть корректно настроены в файле /usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf или в перезаписывающем его файле.

4.9 Служебные программы

4.9.1 Утилита oVirt Engine Rename

4.9.1.1 Применение утилиты oVirt Engine Rename

При запуске команды `engine-setup` в чистом окружении создается некоторое количество сертификатов и ключей, использующих полное доменное имя диспетчера, предоставленное во время процесса настройки. Если полное доменное имя диспетчера позже нужно будет сменить (например, как последствие миграции ВМ, размещающей диспетчера, в другой домен), то информация в записях с полным доменным именем должна быть обновлена для отражения нового имени. Эту задачу автоматизирует команда `ovirt-engine-rename`.

Команда `ovirt-engine-rename` обновляет записи полного доменного имени диспетчера по следующим местоположениям:

– /etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf;
– /etc/ovirt-engine/isouploader.conf.d/10-engine-setup.conf;
– /etc/ovirt-engine/logcollector.conf.d/10-engine-setup.conf;
– /etc/pki/ovirt-engine/cert.conf;
– etc/pki/ovirt-engine/cert.template;
– /etc/pki/ovirt-engine/certs/apache.cer;
– /etc/pki/ovirt-engine/keys/apache.key.nopass;
– /etc/pki/ovirt-engine/keys/apache.p12.

Примечание — Начиная с версии 3.0, появилась возможность добавления большего числа имен для доступа к веб-интерфейсу диспетчера.

Чтобы убедиться в том, что выбранные имена разрешаются на IP-адрес машины диспетчера, нужно добавить соответствующие записи на сервер DNS или в /etc/hosts (для проверки использовать команду `ping enginename` или `getent hosts enginename`).

Далее необходимо выполнить следующие команды:

```
    # echo \
    'SSO_ALTERNATE_ENGINE_FQDNS="alias1.example.com
alias2.example.com"' \
    > /etc/ovirt-engine/engine.conf.d/99-custom-sso-setup.conf
    # systemctl restart ovirt-engine.service
    . List the alternate names separated by spaces.
```

Также возможно добавить IP-адрес машины диспетчера, но использование IP-адресов вместо имен DNS не является лучшей практикой.

Примечание — Несмотря на то, что команда `ovirt-engine-rename` создает новый сертификат для веб-сервера, на котором выполняется диспетчер, она не влияет на сертификат для самого диспетчера или на ЦС. В связи с этим при использовании команды `ovirt-engine-rename` существует некоторый риск, особенно в окружениях, прошедших через процесс обновления с РОСА Виртуализация более ранних версий. Соответственно, везде, где возможно, рекомендуется изменять полное доменное имя диспетчера с помощью команд `engine-cleanup` и `engine-setup`.

Важно — Во время процесса обновления старое имя хоста должно оставаться разрешаемым. Если работа утилиты oVirt Engine Rename завершится сбоем со следующим сообщением:

```
    [ ERROR ] Host name is not valid:
    <OLD FQDN> did not resolve into an IP address,
```

следует добавить старое имя хоста в файл /etc/hosts, запустить утилиту oVirt Engine Rename и затем удалить старое имя хоста из /etc/hosts.

4.9.1.2 Синтаксис команды oVirt Engine Rename

Базовый синтаксис команды `ovirt-engine-rename`:

```
    # /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

Команда также принимает следующие параметры:

– --newname=[new name] – указывает новое полное доменное имя диспетчера без необходимости действий со стороны пользователей;

– --log=[file] – указывает путь и имя файла, в который будет записываться журнал операции переименования;

– --config=[file] – указывает путь и имя файла конфигурации для использования во время операции переименования;

– --config-append=[file] – указывает путь и имя существующего файла конфигурации для добавления с ответами для автоматизации операции переименования;

– --generate-answer=[file] – указывает путь и имя файла, в котором записаны ответы и значения, измененные командой `ovirt-engine-rename`.

4.9.1.3 Переименование СУСВ с помощью утилиты oVirt Engine Rename

С помощью команды `ovirt-engine-rename` можно обновлять записи полного доменного имени (FQDN) СУСВ.

Утилита проверяет, предоставляет ли СУСВ локальный домен ISO или домен хранения данных. При предоставлением, перед тем как продолжать, утилита предлагает пользователю извлечь, выключить или перевести в режим обслуживания любые ВМ или домены хранения, подключенные к хранилищу, что обеспечивает сохранение подключения ВМ к своим виртуальным дискам и предотвращает потерю возможности подключения доменов хранилищ ISO во время процесса переименования.

Последовательность действий по переименованию СУСВ с помощью утилиты oVirt Engine Rename:

а) подготовить все DNS и другие записи, необходимые для нового FQDN;

б) обновить конфигурацию сервера DHCP, в случае если используется DHCP;

в) обновить имя хоста на СУСВ;

г) выполнить следующую команду:

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

д) по запросу команды нажать клавишу `Enter` для остановки службы engine:

```
    During execution engine service will be stopped (OK, Cancel)
[OK]:
```

е) по запросу команды ввести новый FQDN для СУСВ:

```
    New fully qualified server name:new_engine_fqdn
```

Команда `ovirt-engine-rename` обновит записи FQDN СУСВ.

Для виртуализированного ЦУ нужно выполнить следующие дополнительные шаги:

а) на каждом из существующих узлов виртуализированного ЦУ выполнить следующую команду:

```
    # hosted-engine --set-shared-config fqdn new_engine_fqdn --
type=he_local
```

Данная команда изменяет полное доменное имя в каждой локальной копии файла /etc/ovirt-hosted-engine-ha/hosted-engine.conf на всех узлах виртуализированного ЦУ.

б) на каждом из узлов виртуализированного ЦУ выполнить следующую команду:

```
    # hosted-engine --set-shared-config fqdn new_engine_fqdn --
type=he_shared
```

Данная команда изменяет полное доменное имя в главной копии файла /etc/ovirt-hosted-engine-ha/hosted-engine.conf разделяемого домена хранения.

Теперь все новые и уже существующие узлы виртуализированного ЦУ используют новое полное доменное имя.

Примечание — Утилита oVirt Engine Rename предназначена для работы только на локальных машинах. Смена имени диспетчера не изменяет автоматически имя на удаленных машинах хранилища данных. Смена имени на этих машинах должна выполняться вручную.

Для развертываний в удаленных хранилищах данных нужно выполнить следующие шаги на удаленной машине (не на машине диспетчера):

а) удалить следующие файлы PKI:

```
    /etc/pki/ovirt-engine/apache-ca.pem/etc/pki/ovirt-engine/
apache-grafana-
ca.pem/etc/pki/ovirt-engine/certs/*/etc/pki/ovirt-engine/keys/*
```

б) обновить полное доменное имя СУСВ в следующих файлах (например, vm-new-name.local_lab_server.example.ru):

```
    /etc/grafana/grafana.ini/etc/ovirt-engine-dwh/ovirt-engine-
dwhd.conf.d/10-setup-database.conf
    /etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

в) выполнить `engine-setup` с атрибутом --offline для исключения выполнения обновлений в это время:

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

4.9.2 Утилита Engine Configuration

4.9.2.1 Применение утилиты Engine Configuration

Утилита Engine Configuration является консольной утилитой для настройки глобальных параметров окружения РОСА Виртуализация. Утилита взаимодействует со списком отображений "ключ-значение", которые хранятся в базе данных диспетчера виртуализации, и дает возможность получить список всех ключей и значений, доступных для настройки. Кроме того, для каждого из уровней настройки РОСА Виртуализация могут храниться различные значения.

Примечание — Для получения или настройки значений ключей конфигурации выполнение виртуализированного ЦУ или платформы JBoss не обязательно. Поскольку отображения "значение-ключ" конфигурации хранятся в базе данных диспетчера виртуализации, их можно обновлять при работающей службе postgresql. Далее изменения применяются при перезапуске службы ovirt-engine.

4.9.2.2 Синтаксис команды engine-config

Утилиту Engine Configuration можно запускать на машине, на которой установлен диспетчер виртуализации. Для получения подробных сведений об использовании см. вывод справки:

```
    # engine-config --help
```

Стандартные задачи:

– Вывод списка доступных ключей конфигурации:

```
# engine-config --list
```

– Вывод списка доступных значений конфигурации:

```
# engine-config --all
```

– Получение значения ключа конфигурации:

```
# engine-config --get ИМЯ_КЛЮЧА
```

Для получения значения указанной версии ключа, нужно заменить "ИМЯ_КЛЮЧА" на имя нужного ключа. Для указания версии конфигурации получаемого значения следует использовать параметр --cver. Если версия не указывается, выводятся значения для всех существующих версий.

– Настройка значения ключа конфигурации:

```
# engine-config --set ИМЯ_КЛЮЧА=ЗНАЧЕНИЕ_КЛЮЧА --cver=ВЕРСИЯ
```

Следует заменить "ИМЯ_КЛЮЧА" на имя конкретного настраиваемого ключа и заменить "ЗНАЧЕНИЕ_КЛЮЧА" на настраиваемое значение. В окружениях с несколькими версиями конфигурации необходимо указать значение "ВЕРСИЯ".

– Для применения изменений перезапустить службу ovirt-engine:

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

4.9.3 Утилита Log Collector

4.9.3.1.1 Применение утилиты Log Collector

Утилита для сбора файлов журналов Log Collector включена в состав ПО СУСВ. С ее помощью можно легко собрать необходимые файлы журналов в окружении РОСА Виртуализация, например, для создания сводки при обращении в техподдержку.

По умолчанию утилита не установлена. Для установки необходимо выполнить в консоли СУСВ команду

```
# dnf install ovirt-log-collector
```

Исполняемая команда сборщика – `ovirt-log-collector`. Для ее запуска необходимо выполнить вход в Систему в качестве пользователя root и предоставить административные полномочия в окружении виртуализации.

Команда `ovirt-log-collector -h` показывает сведения об ее применении, включая список всех действительных параметров.

4.9.3.2 Синтаксис команды ovirt-log-collector

Базовый синтаксис команды сборщика журналов:

```
# ovirt-log-collector options list all|clusters|datacenters
# ovirt-log-collector options collect
```

Поддерживаются два режима выполнения:

– list – параметр выводит список хостов, кластеров или дата-центров, присоединенных к диспетчеру виртуализации. Можно выполнять фильтрацию на основе списка объектов;

– collect – параметр выполняет сбор файлов журналов в виртуализированном ЦУ. Собранные файлы помещаются в файл архива в каталоге /tmp/logcollector. Каждому из файлов журналов команда `ovirt-log-collector` присваивает конкретное имя.

При отсутствии других параметров действие по умолчанию — вывод списка доступных хостов вместе с дата-центром и кластером, которым они принадлежат. Для получения некоторых файлов журналов будет предложено ввести имя и пароль пользователя.

Для детализации требуемых действий у команды `ovirt-log-collector` существует множество параметров.

4.9.3.2.1 Общие параметры ovirt-log-collector

Общие параметры ovirt-log-collector:

– --version – отображает номер версии используемой команды и возвращает приглашение командной строки;

– -h, --help – отображает сведения об использовании команды и возвращает приглашение командной строки;

– --conf-file=ПУТЬ – настраивает "ПУТЬ" до конфигурационного файла, который должна использовать утилита;

– --local-tmp=ПУТЬ – настраивает "ПУТЬ" в качестве каталога для сохранения журналов (каталог по умолчанию – /tmp/logcollector);

– --ticket-number=ЗАЯВКА – настраивает "ЗАЯВКУ" в качестве номера заявки в службу поддержки;

– --upload= СЕРВЕР_FTP – указывает "СЕРВЕР_FTP" в качестве цели при отсылке полученных файлов журналов по FTP (этот параметр используют только по рекомендации работников техподдержки);

– --log-file=ПУТЬ – указывает "ПУТЬ" для имени файла, который используется командой для вывода журнала;

– --quiet – режим без сообщений, при котором вывод сообщений в консоль является минимальным (по умолчанию выключен);

– -v, --verbose – режим подробной информации; расширенный вывод сообщений в консоль (по умолчанию выключен);

– --time-only – выводит только сведения о разнице во времени между хостами без создания сводки для техподдержки;

4.9.3.2.2 Параметры диспетчера виртуализации

С помощью этих параметров выполняется фильтрация собранных файлов журналов и указываются сведения об аутентификации виртуализированного ЦУ.

Эти параметры можно комбинировать в конкретные команды. Например, команда:

```
    # ovirt-log-collector --user=admin@internal --cluster
ClusterA,ClusterB \
    --hosts "SalesHost"*
```

конкретно указывает пользователя admin@internal и настраивает сбор журналов только для хостов SalesHost в кластерах A и B.

Параметры диспетчера виртуализации:

– --no-hypervisors – исключает хосты виртуализации из сбора файлов журналов;

– --one-hypervisor-per-cluster – собирает журналы только с одного гипервизора в кластере (диспетчера пула хранилища, при его наличии);

– -u ПОЛЬЗОВАТЕЛЬ, --user= ПОЛЬЗОВАТЕЛЬ – указывает имя пользователя для входа в Систему. "ПОЛЬЗОВАТЕЛЬ" указывается в формате пользователь@домен, где "пользователь" — это имя пользователя, а "домен" — имя используемого домена служб каталогов. Этот пользователь должен существовать в службе каталогов и должен быть известен диспетчеру виртуализации;

– -r FQDN, --rhevm=FQDN – указывает полное доменное имя диспетчера виртуализации, с которого нужно собрать файлы журналов, где "FQDN" необходимо заменить на полное доменное имя диспетчера.

Подразумевается, что сборщик журналов запущен на том же локальном хосте, что и диспетчер виртуализации; значение по умолчанию — "localhost";

– -c КЛАСТЕР, --cluster=КЛАСТЕР – в дополнение к файлам журналов диспетчера виртуализации, собирает файлы с хостов виртуализации в указанном "КЛАСТЕРЕ". Необходимые кластеры должны указываться в виде списка имен кластеров или шаблонов для совпадения через запятую;

– -d ДАТА-ЦЕНТР, --data-center= ДАТА-ЦЕНТР – в дополнение к файлам журналов диспетчера виртуализации собирает файлы с хостов виртуализации в указанном "ДАТА-ЦЕНТРЕ". Необходимые дата-центры должны указываться в виде списка имен дата-центров или шаблонов для совпадения через запятую;

– -H СПИСОК_ХОСТОВ, --hosts= СПИСОК_ХОСТОВ – в дополнение к файлам журналов диспетчера виртуализации, собирает файлы с хостов виртуализации в указанном "СПИСКЕ_ХОСТОВ". Включаемые хосты должны указываться в виде списка имен хостов, полных доменных имен или IP-адресов. Также принимаются шаблоны для совпадения.

4.9.3.2.3 Параметры SSH

Параметры SSH:

– --ssh-port=ПОРТ – указывает "ПОРТ" для использования в подключениях по протоколу SSH между хостами виртуализации;

– -k ФАЙЛ_КЛЮЧА, --key-file= ФАЙЛ_КЛЮЧА – указывает "ФАЙЛ_КЛЮЧА" в качестве ключа SSH, используемого для доступа к хостам виртуализации;

– --max-connections=MAX_CONNECTIONS – указывает "MAX_CONNECTIONS" как максимально возможное число параллельных подключений по протоколу SSH для получения файлов журналов с хостов виртуализации. Число по умолчанию – "10".

4.9.3.2.4 Параметры базы данных PostgreSQL

С помощью параметров pg-user и dbname необходимо указать имя пользователя базы данных и имя базы данных, если значения по умолчанию были ранее изменены.

Если база данных находится не на локальном хосте, следует использовать параметр pg-dbhost. Для сбора удаленных файлов журналов можно использовать дополнительный параметр pg-host-key. Для успешного сбора удаленных файлов журналов на сервере базы данных должно быть установлено расширение PostgreSQL – SOS.

Параметры базы данных PostgreSQL:

– --no-postgresql – отключает сбор с базы данных. Сборщик журналов подключится к базе данных PostgreSQL диспетчера виртуализации и включит эти данные в отчет о журналах, если только не будет указан параметр —no-postgresql;

– --pg-user= ПОЛЬЗОВАТЕЛЬ – указывает "ПОЛЬЗОВАТЕЛЯ" в качестве пользователя, используемого для подключению к серверу базы данных (по умолчанию – "postgres");

– --pg-dbname= ИМЯ_БД – указывает "ИМЯ_БД" в качестве имени базы данных для подключения к серверу баз данных (по умолчанию – "rhevm");

– --pg-dbhost= ХОСТ_БД – указывает "ХОСТ_БД" в качестве имени хоста сервера база данных (по умолчанию – "localhost");

– --pg-host-key= ФАЙЛ_КЛЮЧА – указывает "ФАЙЛ_КЛЮЧА" в качестве открытого файла идентификации на сервер базы данных. Значение по умолчанию отсутствует; этот параметр необходим, только если база данных существует не на локальном хосте.

4.9.3.3 Базовое использование Log Collector

При запуске без дополнительных параметров команда `ovirt-log-collector` по умолчанию собирает все файлы журналов с диспетчера виртуализации и его присоединенных хостов. Также собираются файлы журналов базы данных, если только не был указан параметр --no-postgresql. В примере ниже Log Collector выполняется для сбора файлов журналов СУСВ и трех присоединенных хостов:

```
    # ovirt-log-collector
    INFO: Gathering oVirt Engine information...
    INFO: Gathering PostgreSQL the oVirt Engine database and log
files from localhost...
    Please provide REST API password for the admin@internal
oVirt Engine user (CTRL+D to abort): About to collect
information from 3 hypervisors. Continue? (Y/n):
    INFO: Gathering information from selected hypervisors...
INFO: collecting information from 192.168.122.250 INFO:
collecting information from 192.168.122.251 INFO: collecting
information from 192.168.122.252
```

```
    INFO: finished collecting information from 192.168.122.250
INFO: finished collecting information from 192.168.122.251 INFO:
finished collecting information from 192.168.122.252 Creating
compressed archive...
    INFO Log files have been collected and placed in
/tmp/logcollector/sosreport-rhn-account- 20110804121320-
ce2a.tar.xz.
    The MD5 for this file is 6d741b78925998caff29020df2b2ce2a
and its size is 26.7M
```

4.9.4 Утилита Engine Vacuum

4.9.4.1 Применение утилиты Engine Vacuum

Утилита Engine Vacuum поддерживает базы данных PostgreSQL, обновляя информацию в таблицах и удаляя устаревшие строки, освобождая пространство на диске. Сведения о команде VACUUM и ее параметрах см. в документации PostgreSQL.

Исполняемая команда утилиты – `engine-vacuum`. Для ее запуска необходимо выполнить вход в Систему в качестве пользователя root и предоставить административные полномочия в окружении РОСА Виртуализация.

Как вариант, утилиту можно запустить во время выполнения команды `engine-setup` для настройки параметров существующей установки:

```
    $ engine-setup
    ...
    [ INFO ] Stage: Environment customization
    ...
    Perform full vacuum on the engine database engine@localhost?
    This operation may take a while depending on this setup
health and the configuration of the db vacuum process.
    See https://www.postgresql.org/docs/12/static/sql-
vacuum.html (Yes, No) [No]:
```

С параметром "Yes" утилита Engine Vacuum запускается в режиме подробного вывода.

4.9.4.2 Режимы Engine Vacuum

Утилита Engine Vacuum имеет два режима:

– Standard Vacuum

Рекомендуется к частому запуску. Standard vacuum удаляет устаревшие версии в строках таблиц и индексов и помечает это пространство как доступное для будущего использования. Часто обновляемые таблицы должны очищаться таким образом на регулярной основе. Тем не менее стандартная очистка не возвращает пространство операционной системе. Без дополнительных параметров standard vacuum обрабатывает каждую таблицу в базе данных.

– Full Vacuum

Не рекомендуется для повседневного использования. Рекомендуется в случаях, когда необходимо освободить значительный объем свободного пространства, ранее используемого таблицей. Full vacuum сжимает таблицы, записывая новые копии файлов таблиц, освобожденных от беиспользуемого пространства, тем самым давая возможность ОС получить это пространство. Работа в этом режиме занимает значительный объем времени. Для работы в этом режиме необходимо дополнительное место на диске для хранения новой копии таблицы до окончания процедуры и удаления старой копии. Поскольку этому режиму необходима эксклюзивная блокировка таблицы, он не может выполняться параллельно с работой других пользователей с этой таблицей.

4.9.4.3 Синтаксис команды engine-vacuum

Команда `engine-vacuum` имеет следующий базовый синтаксис:

```
# engine-vacuum
# engine-vacuum параметр
```

При запуске команды `engine-vacuum` без дополнительных параметров выполняется стандартная очистка.

У команды `engine-vacuum` есть некоторое число параметров для дальнейшей детализации.

4.9.4.4 Общие параметры команды engine-vacuum

Общие параметры команды `engine-vacuum`:

– -h --help – выводит сведения об использовании;

– -a – выполняет стандартную очистку, анализ базы данных и обновляет статистическую информацию оптимизатора;

– -A – анализирует базу данных и обновляет статистику оптимизатора, без очистки;

– -f – выполняет полную очистку;

– -v – выполняется в режиме подробного вывода в консоль;

– -t table_name – очищает конкретную таблицу или таблицы.

Пример команды:

```
# engine-vacuum -f -v -t vm_dynamic -t vds_dynamic
```

4.9.5 Утилита отображения имен VDSM на имена сетей

Если имя логической сети состоит более чем из 15 символов или содержит символы не в кодировке ASCII, Система автоматически создает имя-идентификатор на хосте (vdsm_name); оно включает в себя буквы "on" и первые 13 символов уникального идентификатора сети, например "ona1b2c3d4e5f6g". Именно это имя отображается в файлах журналов хоста. Чтобы просмотреть список имен логических сетей и их автоматически созданных сетевых имен, нужно использовать утилиту VDSM to Network Name Mapping, расположенную в каталоге /usr/share/ovirt-engine/bin/.

Последовательность действий по отображению имен VDSM на имена логических сетей:

а) во время первого запуска утилиты настроить переменную среды "PASSWORD", являющуюся паролем пользователя базы данных с правами на чтение базы данных диспетчера виртуализации, например, выполнить команду:

```
# export PASSWORD=DatabaseUserPassword
```

б) запустить утилиту VDSM to Network Name Mapping:

```
# vdsm_to_network_name_map --user USER
```

где "ПОЛЬЗОВАТЕЛЬ (USER)" — это пользователь базы данных с правами на чтение базы данных диспетчера виртуализации, пароль которого присвоен переменной среды PASSWORD.

Утилита отобразит список имен логических сетей, отображенных на их соответствующие идентификаторы на хосте.

Утилиту можно запустить со следующими флагами:

– --host — имя хоста/IP-адрес сервера баз данных (значение по умолчанию – "localhost");

– --port — номер порта сервера БД (значение по умолчанию – "5432");

– --database — имя базы данных (значение по умолчанию – "engine" – имя базы данных диспетчера виртуализации);

– --secure — активирует защищенное соединение с базой данных (по умолчанию утилита выполняется с незащищенным соединением).

5 СБОР СВЕДЕНИЙ ОБ ОКРУЖЕНИИ

5.1 Мониторинг и наблюдаемость

В этой главе предлагается несколько способов настройки мониторинга РОСА Виртуализация и получения системных метрик и журналов. В числе этих методов:

– Мониторинг РОСА Виртуализация с помощью хранилища данных и Grafana.
– Отсылка метрик на удаленный экземпляр Elasticsearch.

5.1.1 Мониторинг РОСА Виртуализация с помощью хранилища данных и Grafana

5.1.1.1 Обзор Grafana

Grafana — это веб-утилита с графическим интерфейсом для создания отчетов на базе данных, собранных в БД PostgreSQL хранилища данных oVirt с именем ovirt_engine_history. Подробности о доступных сводных панелях отчетов см. в пп. 5.1.1.4–5.1.1.5.

Данные диспетчера виртуализации собираются каждую минуту и агрегируются в почасовых и ежедневных наборах данных. Собранные данные хранятся согласно параметру масштаба, настраиваемому в конфигурации хранилища данных во время выполнения engine-setup (масштаб Basic или Full):

– Basic (по умолчанию) – выборки данных, сохраненных за 24 часа, почасовых данных за 1 месяц; для ежедневных данных выборки не сохраняются.
– Full (рекомендуется) – выборки данных, сохраненных за 24 часа, почасовых данных за 2 месяца, ежедневных данные за 5 лет.

Для полномасштабных данных может потребоваться миграция хранилища данных на отдельную ВМ.

Примечание — На одной и той же машине поддерживается только совместная установка БД хранилища данных, службы Data Warehouse и Grafana, хотя каждый из этих компонентов можно установить отдельно от других на отдельной машине.

5.1.1.2 Установка Grafana

Интеграция с Grafana включается и устанавливается по умолчанию при выполнении команды `engine-setup` для СУСВ в отдельной установке диспетчера, а также при установке виртуализированного ЦУ.

Для установки Grafana нужно выполнить следующие действия:

а) перевести окружение в режим глобального обслуживания:

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

б) войти в Систему, предназначенную для развертывания Grafana, и выполнить следующую команду:

```
# engine-setup --reconfigure-optional-components
```

в) при выводе следующих запросов нажать клавишу `Enter`, чтобы установить Grafana:

```
Configure Grafana on this host (Yes, No) [Yes]:
Renew certificate (Yes, No) [Yes]:
```

г) отключить глобальный режим обслуживания:

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

Для доступа к панелям управления Grafana нужно нажать "Портал мониторинга" на странице приветствия Портала администрирования или перейти по адресу https://<доменное_имя/IP-адрес_виртуализированного_ЦУ>/ovirt-engine-grafana.

5.1.1.3 Настройка механизма единого входа для Grafana

Команда `engine-setup` автоматически настраивает на Grafana разрешение для уже существующих пользователей диспетчера на выполнение входа с Портала администрирования с помощью механизма единого входа, но не создает пользователей автоматически. Новых пользователей нужно создать (раздел "Invite" в графическом интерфейсе Grafana) и подтвердить, только после этого они могут входить в Систему:

а) настроить почтовый адрес пользователя на диспетчере, если он еще не настроен;

б) выполнить вход в систему Grafana для существующего пользователя admin (изначально настроенный admin);

в) нажать "Configuration → Users" и выбрать "Invite";

г) ввести почтовый адрес и имя, затем выбрать "Роль";

д) выслать приглашение, используя одну из следующих возможностей:

– выбрать "Send invite mail" и нажать кнопку `Submit`, для чего необходимо иметь рабочий локальный почтовый сервер, настроенный на машине с Grafana;

– выбрать "Pending Invites";

– найти нужную запись, выбрать "Copy invite", скопировать ссылку и использовать ее для создания учетной записи, либо скопировав напрямую в адресную строку браузера, либо отослав ее другому пользователю.

Примечание — При использовании возможности с отложенными приглашениями почтовое сообщение не отсылается, и почтовый адрес на самом деле может не существовать — сработает любой адрес, выглядящий корректным и похожий на настроенный почтовый адрес пользователя диспетчера.

Для входа на Портал мониторинга с этой учетной записью нужно:

а) выполнить вход на приветственной странице веб-администрирования РОСА Виртуализация с помощью учетной записи с этим почтовым адресом;

б) чтобы перейти на панель мониторинга Grafana, выбрать "Портал мониторинга";

в) выбрать "Вход с помощью oVirt Engine Auth".

5.1.1.4 Встроенные панели мониторинга Grafana

В начальной установке Grafana доступны панели мониторинга со сводками из ЦОД, кластера, хоста и ВМ, приведенные в таблице 74.

Таблица 74 – Встроенные панели мониторинга Grafana

Тип панели мониторинга	Содержимое
Панели оперативных отчетов	Системная панель: потребление ресурсов и время непрерывной работы для хостов и доменов хранилищ в Системе согласно свежим конфигурациям. Панель ЦОД: потребление ресурсов, пиковые нагрузки и время непрерывной работы для кластеров, хостов и доменов хранилищ в выбранном ЦОД согласно свежим конфигурациям. Панель кластеров: потребление ресурсов, пиковые

Тип панели мониторинга	Содержимое
	нагрузки, превышенное выделение ресурсов и время непрерывной работы для хостов и ВМ в выбранном кластере согласно свежим конфигурациям. Панель хостов: подробные сведения о последней и предыдущих конфигурациях, метрики потребления ресурсов для выбранного хоста за указанный период. Панель ВМ: подробные сведения о последней и предыдущих конфигурациях, метрики потребления ресурсов для выбранной ВМ за указанный период. Панель оперативного отчета: потребление пользовательских ресурсов и число ОС для хостов и ВМ в выбранных кластерах за указанный период
Инвентарные панели	Инвентарная панель: число хостов, ВМ, выполняющихся ВМ, потребление ресурсов и показатели превышенного выделения ресурсов для выбранных ЦОД согласно свежим конфигурациям. Инвентарная панель хостов: полное доменное имя, версия VDSM, версия ОС, модель ЦП, ядра ЦП, объем памяти, дата создания, дата удаления, подробные аппаратные сведения для выбранных хостов согласно свежим конфигурациям. Инвентарная панель доменов хранилищ: тип домена, тип хранилища, доступный объем на дисках, используемое место на дисках, общий объем дисков, дата создания и дата удаления для выбранных доменов хранилищ за указанный период. Инвентарная панель ВМ: имя шаблона, ОС, ядра ЦП, объем памяти, дата создания и дата удаления для выбранных ВМ согласно свежим конфигурациям
Панели уровня обслуживания	Панель времени непрерывной работы: запланированный простой, незапланированный простой, общее время для хостов, ВМ высокой доступности и всех ВМ в выбранном кластере за указанный период. Панель времени непрерывной работы хостов: время непрерывной работы, запланированный простой и незапланированный простой для выбранных хостов за указанный период. Панель времени непрерывной работы ВМ: время

Тип панели мониторинга	Содержимое
	непрерывной работы, запланированный простой и незапланированный простой для выбранных ВМ за указанный период. Уровень обслуживания кластеров Панель хостов: время производительности выбранных хостов выше и ниже порогов ЦП и памяти за указанный период. Панель ВМ: время производительности выбранных ВМ выше и ниже порогов ЦП и памяти за указанный период
Панели тенденций	Панель тенденций: показатели потребления ЦП и памяти для 5 самых загруженных и 5 самых незагруженных ВМ и хостов в выбранных кластерах за указанный период. Панель тенденций для хостов: потребление ресурсов (число ВМ, ЦП, память и прием/передача для сетей) для выбранных хостов за указанный период. Панель тенденций для ВМ: потребление ресурсов (число ВМ, ЦП, память, прием/передача для сетей, ввод-вывод для дисков) для выбранных ВМ за указанный период. Панель потребления ресурсов на хостах — ежедневное и ежечасное потребление ресурсов (число ВМ, ЦП, память, прием/передача для сетей) для выбранных хостов за указанный период. Панель потребления ресурсов ВМ — ежедневное и ежечасное потребление ресурсов (ЦП, память, прием/передача для сетей, ввод-вывод для дисков) для выбранных ВМ за указанный период

Примечание — На панелях Grafana присутствуют прямые ссылки на Портал администрирования РОСА Виртуализация, что позволяет быстро просмотреть дополнительные сведения о кластерах, хостах и ВМ.

5.1.1.5 Настраиваемые панели Grafana

Панели Grafana можно копировать и изменять, а также создавать пользовательские панели согласно требованиям отображения сводок отчетов.

Примечание — Встроенные панели нельзя перенастроить.

5.1.2 Отправка метрик и журналов на удаленный экземпляр Elasticsearch

Важно — Для развертывания данной возможности необходимо иметь опыт работы по настройке и обслуживанию Elasticsearch.

На диспетчере и хостах РОСА Виртуализация можно настроить отправку данных метрик и журналов на существующий экземпляр Elasticsearch, для чего следует запустить роль Ansible, настраивающую collectd и rsyslog на диспетчере и на всех хостах для сбора метрик engine.log, vdsm.log и collectd и отправки их на экземпляр Elasticsearch.

5.1.2.1 Установка collectd и rsyslog

В данном разделе описано развертывание collectd и rsyslog на хостах для сбора журналов и метрик.

Примечание — Данную последовательность действий нет необходимости повторять для новых хостов. Новые хосты при добавлении автоматически настраиваются диспетчером для отправки данных на Elasticsearch во время выполнения host-deploy.

Последовательность действий по установке collectd и rsyslog:

а) выполнить вход на машине диспетчера с помощью SSH;

б) скопировать /etc/ovirt-engine-metrics/config.yml.example для создания /etc/ovirt-engine- metrics/config.yml.d/config.yml:

```
# cp /etc/ovirt-engine-metrics/config.yml.example  \
/etc/ovirt-engine- metrics/config.yml.d/config.yml
```

в) изменить параметры ovirt_env_name и elasticsearch_host в config.yml и сохранить файл, при необходимости добавив следующие дополнительные параметры:

```
use_omelasticsearch_cert: false
rsyslog_elasticsearch_usehttps_metrics: !!str off
rsyslog_elasticsearch_usehttps_logs: !!str off
```

– если используются сертификаты, для параметра use_omelasticsearch_cert указать значение "true";

– для отключения журналирования или метрик использовать параметры rsyslog_elasticsearch_usehttps_metrics и/или rsyslog_elasticsearch_usehttps_logs;

г) развернуть collectd и rsyslog на хостах:

```
# /usr/share/ovirt-engine-metrics/setup/ansible/configure_ovirt_machines_for_metrics.sh
```

Сценарий configure_ovirt_machines_for_metrics.sh запускает роль Ansible, включающую в себя набор linux-system-roles, и использует их для развертывания и настройки rsyslog на хосте. Rsyslog собирает метрики из collectd и отправляет их в Elasticsearch.

5.1.2.2 Схема журналирования и анализ журналов

Для интерактивного просмотра данных, собранных в РОСА Виртуализация, можно использовать страницу "Обнаружение". Каждый набор собранных данных представляется в виде документа. Документы составляются из следующих файлов журналов:

– engine.log – содержит сведения обо всех аварийных сбоях графического интерфейса виртуализированного ЦУ, поиски по Active Directory, проблемы с БД и другие события.

– vdsm.log – файл журнала VDSM – агента диспетчера на хостах виртуализации – содержит события, связанные с хостами.

Поля в файлах просмотров данных описаны в таблице 75.

Таблица 75 – Доступные поля в файлах просмотров данных

Параметр	Описание
_id	Уникальный ID документа
_index	ID индекса, к которому принадлежит документ. Индекс с префиксом project.ovirt-logs является единственным значимым индексом на странице обнаружения
hostname	Для engine.log это имя хоста диспетчера. Для vdsm.log это имя хоста
level	Степень серьезности журнальной записи:

Параметр	Описание
	"TRACE", "DEBUG", "INFO", "WARN", "ERROR", "FATAL"
message	Тело сообщения документа
ovirt.class	Название класса Java, создавшего данный журнал
ovirt.correlationid	Только для engine.log. Данный ID используется для корреляции множественных путей одной задачи, выполняемой диспетчером
ovirt.thread	Имя потока Java, внутри которого была создана запись
tag	Предварительно настроенные наборы метаданных, которые можно использовать для фильтрации данных
@timestamp	Время [time](Troubleshooting#information-is-missing-from-kibana) выпуска записи
_score	Н/Д
_type	Н/Д
ipaddr4	IP-адрес машины
ovirt.cluster_name	Только для vdsm.log. Имя кластера, которому принадлежит хост
ovirt.engine_fqdn	Полное доменное имя диспетчера
ovirt.module_lineno	Файл и номер строки в этом файле, запускающей команду, настроенную в ovirt.class

5.2 Файлы журналов

5.2.1 Файлы журналов процесса установки диспетчера виртуализации

Файлы журналов процесса установки диспетчера виртуализации приведены в таблице 76.

Таблица 76 – Установка диспетчера виртуализации

Файл журнала	Описание
/var/log/ovirt-engine/engine-cleanup_гггг_мм_дд_чч_мм_сс.log	Журнал команды `engine-cleanup`. Эта команда используется для отката установки диспетчера РОСА Виртуализация к изначальным параметрам. Журнал создается при каждом запуске команды. Дата и время запуска команды используется в имени файла для возможности одновременного существования нескольких журналов
/var/log/ovirt-engine/engine-db-install-гггг_мм_дд_чч_мм_сс.log	Журнал команды `engine-setup` с подробностями создания и настройки БД виртуализированного ЦУ
/var/log/ovirt-engine/ovirt-engine-dwh-setup- гггг_мм_дд_чч_мм_сс.log	Журнал команды `ovirt-engine-dwh-setup`. Эта команда создает отчетную БД ovirt_engine_history. Журнал создается при каждом запуске команды. Дата и время запуска команды используется в имени файла для возможности одновременного существования нескольких журналов
/var/log/ovirt-engine/setup/ovirt-engine-setup-ггггммддччммсс.log	Журнал команды `engine-setup`. Журнал создается при каждом запуске команды. Дата и время запуска команды используется в имени файла для возможности одновременного существования нескольких журналов

5.2.2 Файлы журналов диспетчера РОСА Виртуализация

Файлы журналов диспетчера РОСА Виртуализация приведены в таблице 77.

Таблица 77 – Активность служб

Файл журнала	Описание
/var/log/ovirt-engine/engine.log	Отображает все аварийные сбои в GUI диспетчера РОСА Виртуализация, поиск в Active Directory, проблемы в БД и другие события
/var/log/ovirt-engine/host-deploy	Файлы журналов хостов, развернутых с помощью диспетчера виртуализации
/var/lib/ovirt-engine/setup-history.txt	Отслеживание установок и обновлений пакетов, связанных с диспетчером РОСА Виртуализация
/var/log/httpd/ovirt-requests-log	Файлы журналов запросов по HTTPS, посланных на диспетчер, включая длительность каждого запроса. Включает в себя заголовок Correlation-Id для возможности сравнения запросов при сравнении файла журнала с /var/log/ovirt-engine/engine.log
/var/log/ovn-provider/ovirt-provider-ovn.log	Журналы активности поставщика OVN. Сведения о журналах Open vSwitch см. в документации по Open vSwitch

5.2.3 Файлы журналов SPICE

Файлы журналов SPICE удобны в ситуациях поиска и решения проблем с подключениями SPICE. Для начала запуска журналирования SPICE нужно сменить уровень журналирования на debugging, затем указать местоположение файла журнала.

Файлы журналов SPICE существуют как для клиентов, получающих доступ к гостевым машинам, так и для самих гостевых машин. Для активации журналирования и создания вывода журналов на стороне клиента, если клиент SPICE был запущен с помощью встроенного клиента, для которого был скачан файл console.vv, следует использовать команду `remote-viewer`.

5.2.3.1 Журналы SPICE для серверов SPICE гипервизора

В таблице 78 приведены параметры журналов SPICE для серверов SPICE гипервизора.

Таблица 78 – Журналы SPICE для серверов SPICE гипервизора

Тип журнала	Местоположение журнала	Смена уровня журналирования
Сервер SPICE хоста/гипервизора	/var/log/libvirt/qemu/(guest_name).log	Перед запуском гостя выполнить на хосте/гипервизоре команду `export SPICE_DEBUG_LEVEL=5`. Эту переменную обрабатывает QEMU, и при общесистемном запуске отладочная информация будет выводиться для всех ВМ в Системе. Эта команда должна быть запущена на каждом хосте в кластере. Команда работает на уровне хоста/гипервизора, а не на уровне кластера

5.2.3.2 Журналы SPICE для гостевых машин

В таблице 79 приведены параметры журналов spice-vdagent для гостевых машин.

Таблица 79 – Журналы spice-vdagent для гостевых машин

Тип журнала	Местоположение журнала	Смена уровня журналирования
Windows Guest	C:\Windows\Temp\vdagent.log C:\Windows\Temp\vdservice.log	Не применимо

5.2.3.3 Журналы SPICE для клиентов, запущенных с помощью console.vv

Для клиентских машин на Linux нужно выполнить следующие действия:

а) включить отладку SPICE, выполнив команду `remote-viewer` с параметром --spice-debug. По запросу команды ввести URL подключения, например "spice://virtual_machine_IP:port":

```
# remote-viewer --spice-debug
```

б) для запуска клиента SPICE с параметром debug и для передачи ему файла .vv скачать файл console.vv, запустить команду `remote-viewer` с параметром --spice-debug и указать полный путь до файла console.vv.

```
# remote-viewer --spice-debug /path/to/console.vv
```

Для клиентских машин на Windows нужно выполнить следующие действия:

а) в версиях virt-viewer 2.0-11.el7ev и более поздних файл virt-viewer.msi устанавливает virt-viewer и debug-viewer.exe;

б) запустить команду `remote-viewer` с аргументом spice-debug, указав путь до до файла console.vv:

```
remote-viewer --spice-debug path\to\console.vv
```

Для просмотра журналов нужно подключиться к ВМ, чтобы получить приглашение командной строки с выполняющимся GDB со стандартным выводом и стандартные ошибки для `remote-viewer`.

5.2.4 Файлы журналов хостов

В таблице 80 приведена информация о файлах журналов хостов.

Таблица 80 – Файлы журналов хостов

Файл журнала	Описание
/var/log/messages	Файл журнала, используемый libvirt. Для просмотра журнала использовать journalctl. Для просмотра нужно участие в группе adm, systemd-journal или wheel
/var/log/vdsm/spm-lock.log	Файл журнала с подробностями о возможности хоста получить аренду в роли диспетчера пула хранилищ. В журнале указывается, когда хост получил, сбросил, обновил или не смог обновить аренду

Файл журнала	Описание
/var/log/vdsm/vdsm.log	Файл журнала VDSM – агента диспетчера на хостах.
/tmp/ovirt-host-deploy-Date.log	Журнал развертывания хоста, который после удачного развертывания копируется на диспетчер в виде /var/log/ovirt-engine/host-deploy/ovirt-Date-Host-Correlation_ID.log
/var/log/vdsm/import/import-UUID-Date.log	Файл журнала с подробностями импортов ВМ с хоста KVM, из поставщика VMWare или с хоста RHEL 5 Xen, включая сведения о сбоях импорта. UUID — это UUID импортируемой ВМ, Data — дата и время начала импорта
/var/log/vdsm/supervdsm.log	Журнал задач VDSM, запущенных с полномочиями SuperUser
/var/log/vdsm/upgrade.log	VDSM использует этот файл во время обновления хоста для фиксации изменений в конфигурации
/var/log/vdsm/mom.log	Журналирует активность диспетчера превышения выделения памяти VDSM

5.2.5 Настройка отладочного уровня журналирования для служб РОСА Виртуализация

Отладочный уровень журналов служб РОСА Виртуализация, указанных в таблице 81, можно настроить, отредактировав файл sysconfig каждой из служб.

Примечание — Указание отладочного уровня для журналирования может открыть доступ к такой конфиденциальной информации, как пароли или внутренние данные ВМ. Следует убедиться, что у недоверенных или неавторизованных пользователей не будет доступа к журналам отладки.

Таблица 81 – Службы РОСА Виртуализация и пути до файлов sysconfig

Сервис	Путь файла
ovirt-engine.service	/etc/sysconfig/ovirt-engine
ovirt-engine-dwhd.service	/etc/sysconfig/ovirt-engine-dwhd

Сервис	Путь файла
ovirt-fence-kdump-listener.service	/etc/sysconfig/ovirt-fence-kdump-listener
ovirt-websocket-proxy.service	/etc/sysconfig/ovirt-websocket-proxy

Это изменение влияет на журналирование, выполняемое оболочкой Python, а не процессом главной службы.

Указание отладочного уровня журналирования удобно для проблем отладки, относящихся к процессам запуска, например, если главный процесс не сможет стартовать в связи с отсутствием или с некорректностью библиотеки или среды выполнения Java.

Необходимо убедиться в существовании файла sysconfig, который требуется изменить. Можно создать его при необходимости.

Последовательность действий для настройки отладочного уровня журналирования для служб РОСА Виртуализация:

а) добавить следующее содержимое в файл sysconfig службы:

```
OVIRT_SERVICE_DEBUG=1
```

б) перезапустить службу:

```
# systemctl restart <service>
```

Уровень файла журнала sysconfig службы теперь будет отладочным.

Сообщения журналов, создаваемые с этим параметром, поступают в системный журнал, поэтому создаваемые файлы нужно искать в /var/log/messages, а не в конкретных файлах журналов служб. Также их можно просмотреть с помощью команды `journalctl`.

5.2.6 Основные файлы конфигураций служб РОСА Виртуализация

В дополнение к файлам sysconfig для каждой службы РОСА Виртуализация существует еще один файл конфигурации, используемый гораздо чаще (таблица 82).

Таблица 82 – Службы и конфигурационные файлы РОСА Виртуализация

Служба	Путь до файла sysconfig	Главный файл конфигурации
ovirt-engine.service	/etc/sysconfig/ovirt-engine	/etc/ovirt-engine/engine.conf.d/*.conf
ovirt-engine-dwhd.service	/etc/sysconfig/ovirt-engine-dwhd	/etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/*.conf
ovirt-fence-kdump-listener.service	/etc/sysconfig/ovirt-fence-kdump-listener	/etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/*.conf
ovirt-websocket-proxy.service	/etc/sysconfig/ovirt-websocket-proxy	/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/*.conf

5.2.7 Настройка сервера журналирования хоста

Хосты создают и обновляют файлы журналов, записывают действия и неполадки. Централизованный сбор этих файлов журналов упрощает отладку.

Данная последовательность действий должна применяться на централизованном сервере журналов. Можно использовать отдельный сервер или использовать данную процедуру для включения использования журналирования хостов в диспетчере РОСА Виртуализация.

Последовательность действий по настройке сервера журналирования хоста:

а) проверить, разрешен ли трафик на порте UDP 514, и открыт ли он для трафика службы syslog:

```
# firewall-cmd --query-service=syslog
```

б) при выводе "no" разрешить трафик на порте UDP 514 с помощью команд:

```
# firewall-cmd --add-service=syslog --permanent
# firewall-cmd --reload
```

в) создать новый файл .conf на сервере syslog, например /etc/rsyslog.d/from_remote.conf, и добавить в него следующие строки:

```
    template(name="DynFile" type="string"
string="/var/log/%HOSTNAME%/%PROGRAMNAME%.log")
RuleSet(name="RemoteMachine"){ action(type="omfile"
dynaFile="DynFile") }
    Module(load="imudp")
    Input(type="imudp" port="514" ruleset="RemoteMachine")
```

г) перезапустить службу rsyslog:

```
    # systemctl restart rsyslog.service
```

д) выполнить вход в Систему на гипервизоре и добавить следующую строку в /etc/rsyslog.conf:

```
    *.info;mail.none;authpriv.none;cron.none @<syslog-FQDN>:514
```

е) перезапустить службу rsyslog на гипервизоре:

```
    # systemctl restart rsyslog.service
```

Централизованный сервер теперь настроен на получение, хранение и обеспечение защиты для файлов журналов хостов виртуализации.

5.2.8 Включение использования SyslogHandler для передачи журналов диспетчера POCA Виртуализация на удаленный сервер syslog

В данной реализации используется диспетчер журналов JBoss EAP SyslogHandler с настройкой передачи записи журналов из engine.log и server.log на сервер syslog.

Следующая последовательность действий выполняется на центральном сервере syslog. Можно использовать отдельный сервер журналирования или выполнить процедуру для передачи файлов engine.log и server.log с диспетчера на сервер syslog. См. также п. 5.2.7.

Для настройки реализации SyslogHandler нужно выполнить следующие действия:

а) в каталоге /etc/ovirt-engine/engine.conf.d создать файл 90-syslog.conf со следующим содержимым:

```
    SYSLOG_HANDLER_ENABLED=true
    SYSLOG_HANDLER_SERVER_HOSTNAME=localhost
```

```
SYSLOG_HANDLER_FACILITY=USER_LEVEL
```

б) разрешить трафик rsyslog в SELinux:

```
# semanage port -a -t syslogd_port_t -p udp 514
```

в) создать файл конфигурации /etc/rsyslog.d/rv.conf со следующим содержимым:

```
user.* /var/log/jboss.log
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")
```

г) перезапустить службу rsyslog:

```
# systemctl restart rsyslog.service
```

д) если межсетевой экран включен и активен, выполнить следующую команду для добавления необходимых правил для открытия портов rsyslog в Firewalld:

```
# firewall-cmd --permanent --add-port=514/udp
# firewall-cmd --reload
```

е) перезапустить диспетчер РОСА Виртуализация:

```
# systemctl restart ovirt-engine
```

Сервер syslog теперь может получать и хранить файлы engine.log.

6 ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

6.1 Настройка двухфакторной аутентификации

6.1.1 Двухфакторная аутентификация для SSH с использованием Рутокен ЭЦП

В данном разделе рассматривается пример настройки двухфакторной аутентификации с использованием "Рутокен ЭЦП".

6.1.1.1 Настройка двухфакторной аутентификации для SSH

Для примера настройки двухфакторной аутентификации для SSH консоли используется хост с гипервизором под управлением РОСА Виртуализация. В качестве токена для аутентификации используется ранее подготовленный USB "Рутокен ЭЦП 2.0" для двухфакторной аутентификации на веб-портале РОСА Виртуализация для пользователя ovirtadmin. С процедурой подготовки токена можно ознакомиться в соответствующем разделе документации.

Последовательность действий для настройки двухфакторной аутентификации для SSH:

а) подключить токен к USB порту компьютера, на котором ранее выполнялась подготовка этого токена, и с помощью консольной команды проверить его работоспособность:

```
    # 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         : 6/249
       uri                 :
pkcs11:model=Rutoken%20ECP;manufacturer=Aktiv%20Co.;serial=3ac65
c5d;token=Rutoken
```

б) для просмотра объектов, хранящихся на токене, можно воспользоваться командой:

```
     # 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>
     Certificate Object; type = X.509 cert
       label:      login_ovirtadmin
       subject:    DN: O=EXAMPLE.COM, CN=ovirtadmin
       serial:     0B
       ID:         10
       uri:
pkcs11:model=Rutoken%20ECP;manufacturer=Aktiv%20Co.;serial=3ac65
c5d;token=Rutoken;id=%10;object=login_ovirtadmin;type=cert
     Private Key Object; RSA
       label:      login_ovirtadmin
       ID:         10
       Usage:      decrypt, sign
       Access:     sensitive
       Allowed mechanisms: RSA-PKCS,RSA-PKCS-PSS,RSA-X-509,MD5-
RSA-PKCS,SHA1-RSA-PKCS,SHA224-RSA-PKCS,SHA256-RSA-PKCS,SHA384-
RSA-PKCS,SHA512-RSA-PKCS,SHA1-RSA-PKCS-PSS,SHA224-RSA-PKCS-
PSS,SHA256-RSA-PKCS-PSS,SHA384-RSA-PKCS-PSS,SHA512-RSA-PKCS-
PSS,RSA-PKCS-OAEP
       uri:
pkcs11:model=Rutoken%20ECP;manufacturer=Aktiv%20Co.;serial=3ac65
c5d;token=Rutoken;id=%10;object=login_ovirtadmin;type=private
```

в) создать публичный ключ для консоли SSH на основе пользовательского сертификата, хранящегося на подключенном USB-токене:

```
$ ssh-keygen -D /usr/lib64/librtpkcs11ecp.so -I 0:10 > ovirtadmin_key.pub
```

г) используя утилиту ssh-copy-id, скопировать полученный публичный ключ ovirtadmin_key.pub на хост, на котором требуется настроить двухфакторную аутентификацию для консоли SSH :

```
$ ssh-copy-id -f -i ovirtadmin_key.pub root@rosa-virt01.example.com
```

д) для включения двухфакторной аутентификации для консоли SSH на хосте с гипервизором отредактировать конфигурационный файл SSH-сервера /etc/ssh/sshd_config, изменив или добавив соответствующие строки (рисунок 260):

```
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
PasswordAuthentication yes
PermitEmptyPasswords no
```

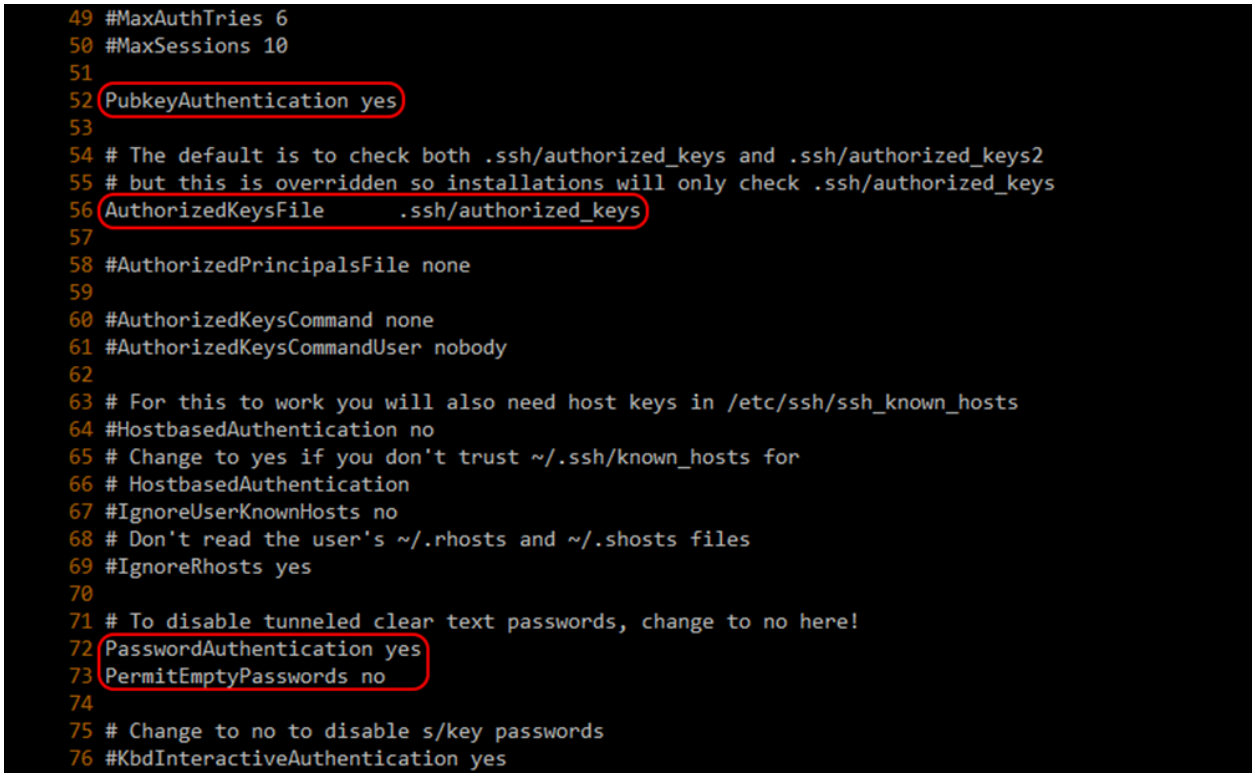


Рисунок 260 – Редактирование файла /etc/ssh/sshd_config

е) такая конфигурация SSH-сервера будет требовать обязательной аутентификации по SSH-ключу и паролю, что приведет к нарушению работы между виртуальной машиной СУСВ и хостом. Чтобы предотвратить такую ситуацию, необходимо в самом конце файла /etc/ssh/sshd_config добавить строки (рисунок 261):

```
Match Address 192.168.1.164
        AuthenticationMethods publickey password
```

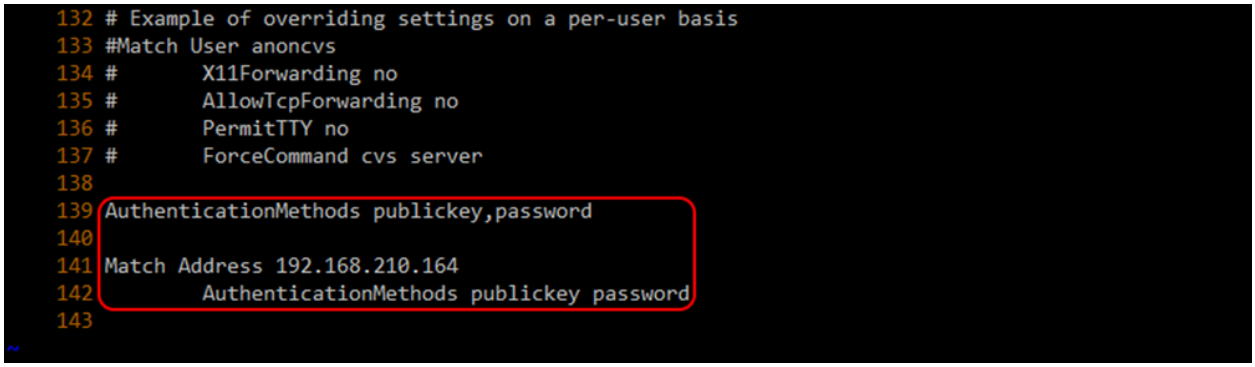


Рисунок 261 – Дополнение в файл /etc/ssh/sshd_config

В поле "Match Address" указывается IP-адрес виртуальной машины СУСВ. В результате сделанных настроек SSH-подключение между СУСВ и хостами будет требовать аутентификацию только по SSH-ключу или паролю, а во всех остальных случаях будут требоваться оба типа аутентификации одновременно.

ж) перезапустить сервис sshd:

```
# systemctl restart sshd
```

6.1.1.2 Подключение к SSH-серверу с настроенной двухфакторной аутентификацией

Для подключения к SSH-серверу с настроенной двухфакторной аутентификацией используется стандартный SSH-клиент для операционных систем GNU/Linux:

```
$ ssh -I /usr/lib64/librtpkcs11ecp.so root@rosa-
virt01.example.com
Enter PIN for 'Rutoken': <PIN-код пользователя>
root@rosa-virt01.example.com's password: <Пароль
пользователя root>
```

6.1.2 Двухфакторная аутентификация для веб-портала РОСА Виртуализация

Двухфакторная аутентификация на веб-портале РОСА Виртуализация основана на USB-токене с приватным ключом и клиентским сертификатом, имени пользователя и его пароле. Для этого потребуется полная замена корневого сертификата СУСВ.

Важно — Для замены корневого сертификата необходимо наличие двух и более хостов виртуализации, чтобы была возможность миграции виртуальных машин для последующей переустановки всех подключенных хостов. Процедура замены корневого сертификата может быть не безопасна, поэтому рекомендуется проводить ее на ранней стадии настройки Системы виртуализации. Крайне не рекомендуется перезагружать хосты до полного завершения процедуры замены сертификатов.

В данном примере продемонстрирован способ замены корневого сертификата РОСА Виртуализация и всех сертификатов, подписанных им. Новый корневой сертификат и приватный ключ будет взят из файла /root/cacert.p12, который создается в процессе установки IPA-сервера. Файл защищен паролем, о чем свидетельствует скриншот, полученный в процессе установки IPA (рисунок 262);

```
Be sure to back up the CA certificate stored in /root/cacert.p12
This file is required to create replicas. The password for this
file is the Directory Manager password
```

Рисунок 262 – Сообщение о защите файла паролем

Чтобы извлечь сертификат и приватный ключ из файла cacert.p12, необходимо в консоли IPA-сервера перейти в директорию /root и выполнить команды:

```
    # 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, указанный
при установки IPA сервера>

    # 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, указанный
при установки IPA сервера>
```

Эти команды извлекают сертификат "subject=O = EXAMPLE.COM, CN = Certificate Authority" и приватный ключ "friendlyName: caSigningCert cert-pki-ca" из файла cacert.p12 и сохраняют их в файлы ipa-ca.pem и ipa-ca.key соответственно.

Далее нужно скопировать файл сертификата ipa-ca.pem на виртуальную машину СУСВ в директорию /etc/pki/ovirt-engine, а файл приватного ключа

ipa-ca.key – в директорию /etc/pki/ovirt-engine/private. Замена корневого сертификата выполняется с помощью скрипта ovirt-pki-enroll. Для его работы требуется создать файл ovirt_hosts в той директории, из которой предполагается запускать скрипт, например, в директории /root. В этом файле должны быть прописаны все хосты, подключенные к СУСВ. В качестве имени хоста может быть использовано короткое доменное имя (rosa-virt01), полное доменное имя (rosa-virt01.example.com) или же IP-адрес (192.168.1.162), в зависимости от того, что было прописано в поле "Имя хоста/IP" при добавлении хоста в Систему виртуализации (рисунок 263).

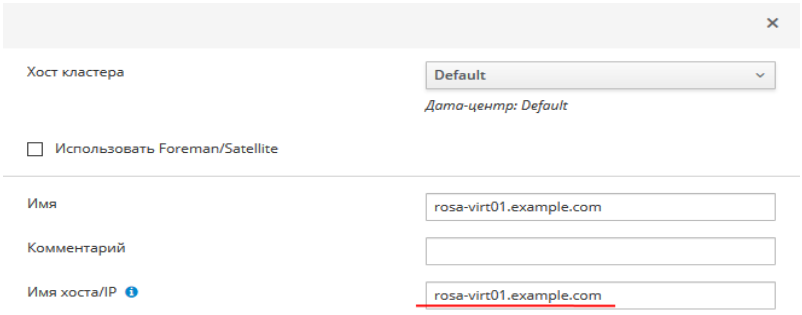


Рисунок 263 – Параметр "Имя хоста" при добавлении хоста

Согласно этим данным нужно заполнить файл ovirt_hosts. В конце файла после всех введенных данных требуется добавить пустую строку. Формат файла ovirt_hosts поддерживает различные комбинации написания имени хоста:

```
[ovirt_hosts]
rosa-virt01.example.com
192.168.1.172
rosa-virt03
```

Затем на любом из активных хостов Системы, который был настроен для запуска и миграции виртуализированного ЦУ, следует включить режим глобального обслуживания, выполнив команду в консоли хоста:

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

Для замены сертификата нужно выполнить команду в консоли виртуальной машины СУСВ:

```
# ovirt-pki-enroll --name=ipa-ca --new-key
```

Если скрипт завершил свою работу из-за того, что не удалось определить домен, для которого были созданы предыдущие сертификаты, можно указать его принудительно, используя соответствующий ключ --domain:

```
# ovirt-pki-enroll --domain=example.com --name=ipa-ca --new-key
```

где:

– --name – это общая часть в именах новых файлов корневого сертификата и ключа (в данном случае "ipa-ca" от файлов ipa-ca.pem и ipa-ca.key);

– --new-key – указывает на необходимость пересоздания приватных ключей для сертификатов;

– --domain – домен локальной сети в котором находятся подключенные хосты.

После этого необходимо перезапустить сервисы:

```
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-provider-ovn
# systemctl restart ovirt-imageio
# systemctl restart httpd
```

После пересоздания приватных ключей нарушится работа компонента ovirt-provider-ovn. Чтобы это исправить, необходимо зайти на Портал администрирования РОСА Виртуализация в раздел "Администрирование → Поставщики", выбрать строку ovirt-provider-ovn и нажать кнопку Изменить;

В открывшемся окне (рисунок 264) нужно ввести пароль для пользователя admin@internal (учетная запись администратора во внутреннем домене СУСВ), нажать кнопку Тест и согласиться импортировать сертификат.

После удачного завершения теста следует нажать кнопку ОК;

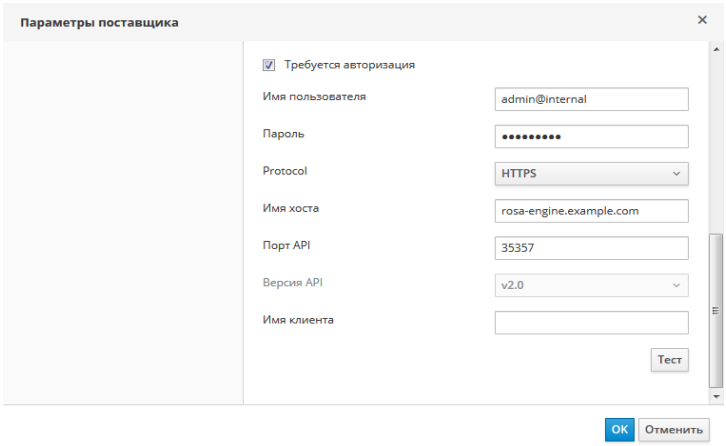


Рисунок 264 – Окно "Параметры поставщика"

Так как многие сервисы продолжают работать на старом корневом сертификате, то для восстановления функции миграции виртуальных машин необходимо перезапустить сервис libvirtd на каждом хосте, выполнив команду:

```
# systemctl restart libvirtd
```

Для полного завершения процедуры замены сертификатов на подключенных хостах требуется выполнить переустановку всех хостов. Это можно сделать в разделе "Ресурсы → Хосты". Если на хостах есть виртуальные машины, которые не имеют возможности миграции на другой хост, то следует заранее позаботиться об их выключении:

а) перевести хост в режим обслуживания, нажав "Управление → Обслуживание";

б) запустить переустановку хоста, нажав "Установка → Переустановить".

Хост с виртуальной машиной HostedEngine переустанавливается в последнюю очередь.

На данном этапе процесс замены корневого сертификата СУСВ считается завершенным, и можно отключить режим глобального обслуживания, выполнив в консоли хоста, с которого он был включен, команду:

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

Для создания приватного ключа и клиентского сертификата нужно выполнить следующие действия:

а) в качестве центра сертификации будет использоваться IPA-сервер. Первоначально требуется создать приватный ключ и запрос для сертификата пользователя admin внутреннего домена СУСВ. Так как на IPA-сервере такой пользователь уже существует, и нет возможности стандартными средствами создать для него сертификат, то необходимо добавить нового пользователя, например, ovirtadmin. Для этого в консоли IPA-сервера выполнить команды:

```
# kinit admin
# ipa user-add ovirtadmin --first=ovirtadmin \
--last=ovirtadmin
```

б) создать приватный ключ и запрос для сертификата пользователя ovirtadmin:

```
# openssl req -new -sha256 -nodes -newkey rsa:2048 \
-keyout ovirtadmin.key -out ovirtadmin.csr \
-subj '/CN=ovirtadmin/O=EXAMPLE.COM'
```

в) создать сертификат и сохранить его в файл ovirtadmin.pem:

```
# ipa cert-request ovirtadmin.csr --principal=ovirtadmin \
--certificate-out=ovirtadmin.pem
```

Сертификаты для других пользователей, которые будут иметь доступ к веб-порталу РОСА Виртуализация, создаются аналогичным способом.

г) если импорт приватного ключа и сертификата пользователя на USB-токен планируется выполнять под ОС Windows, то необходимо создать файл ovirtadmin.p12, содержащий в себе приватный ключ и сертификат:

```
# openssl pkcs12 -export -out ovirtadmin.p12 -inkey
ovirtadmin.key \
-in ovirtadmin.pem
```

На данном этапе процесс создания приватного ключа и клиентского сертификата считается завершенным.

Для импорта приватного ключа и сертификата пользователя в качестве аппаратного хранилища приватного ключа и сертификата в данном примере будет использован USB "Рутокен ЭЦП 2.0":

а) если для подготовки токена используется ROSA Desktop Cobalt, то необходимо убедиться, что следующие пакеты установлены, а если они

отсутствуют, то установить opensc, pcsc-lite, pcsc-lite-ccid и перезагрузить компьютер;

б) установить соответствующую версию библиотеки PKCS#11 https://www.rutoken.ru/support/download/pkcs/ и утилиту для администрирования токена https://dev.rutoken.ru/pages/viewpage.action?pageId=7995615. После установки пакета PKCS#11 необходимая для работы с токеном библиотека будет находиться в директории /usr/lib64/librtpkcs11ecp.so;

в) для корректной работы утилиты rtadmin в ROSA Desktop Cobalt может потребоваться однократно выполнить команды для создания симлинка:

```
# cd /usr/lib64/
# ln -s libdl.so.2 libdl.so
```

г) подключить Рутокен к USB-порту компьютера;

в) убедиться в работоспособности библиотеки PKCS#11 и токена можно с помощью консольной команды (пример выполнения – на рисунке 265):

```
$ 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        : 6/249
  uri                : pkcs11:model=Rutoken%20ECP;manufacturer=Aktiv%20Co.;serial=3ac65c5d;token=Rutoken
```

Рисунок 265 – Результат выполнения команды pkcs11-tool

д) выполнить форматирование токена:

```
$ ./rtadmin -f -q -z /usr/lib64/librtpkcs11ecp.so \
-a <PIN-код администратора> -u <PIN-код пользователя>
```

е) импортировать приватный ключ и сертификат пользователя на USB-токен, предварительно сконвертировав их в формат DER, используя следующие команды:

```
$ openssl rsa -in ovirtadmin.key -out ovirtadmin_key.der
-outform DER
```

```
    $ openssl x509 -in ovirtadmin.pem -out ovirtadmin_cert.der
-outform DER

    $ 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>
```

г) для просмотра объектов, хранящихся на токене, можно воспользоваться командой:

```
    $ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -O -l
```

ж) если для подготовки токена используется ОС Windows, необходимо установить соответствующую версию библиотеки PKCS#11, которая распространяется в составе драйверов Рутокен https://www.rutoken.ru/support/download/pkcs/ и утилиту для администрирования https://dev.rutoken.ru/pages/viewpage.action?pageId=7995615. После установки драйверов библиотека PKCS#11, необходимая для работы с токеном, будет находиться по пути C:\Windows\System32\rtPKCS11ECP.dll. Подключить Рутокен к USB-порту компьютера и выполнить его форматирование:

```
    rtadmin.exe -f -q -z C:\Windows\System32\rtPKCS11ECP.dll -a
<PIN-код администратора> -u <PIN-код пользователя>
```

з) открыть панель управления Рутокен, перейти на вкладку "Сертификаты", выбрать токен и нажать на кнопку `Импорт` (рисунок 266);

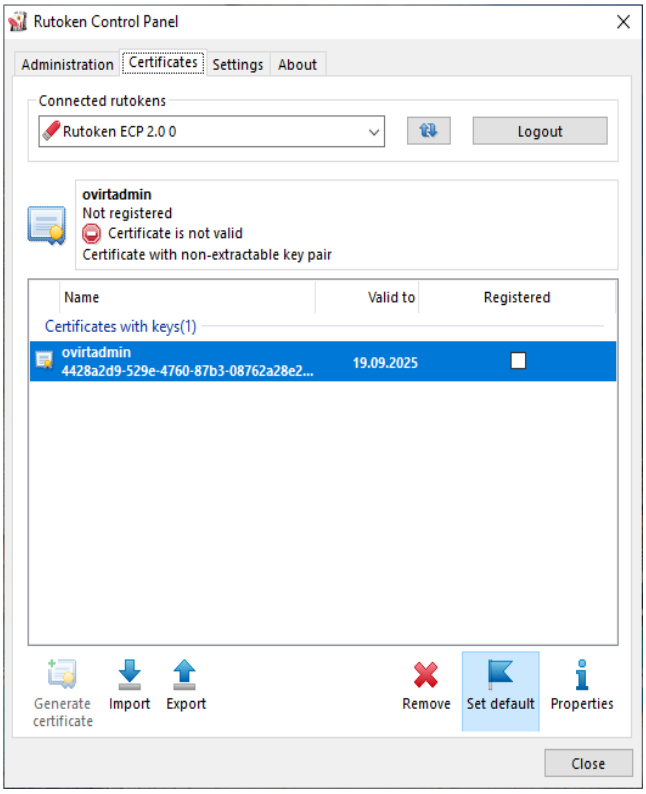


Рисунок 266 – Контрольная панель Рутокен – вкладка "Сертификаты"

и) указать путь к ранее подготовленному файлу ovirtadmin.p12, ввести пароль который был задан при его создании и нажать на кнопку Импорт (рисунок 267);

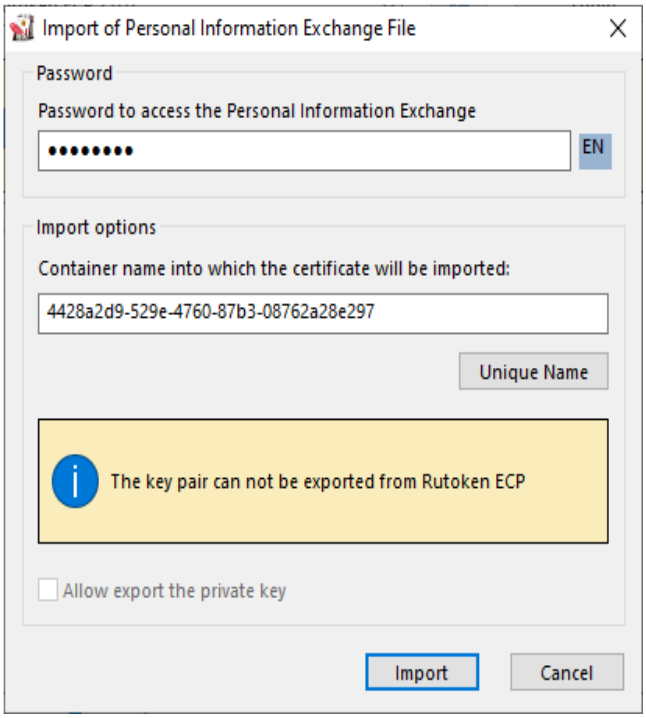


Рисунок 267 – Ввод пароля для файла

к) ввести ПИН-код пользователя для подключенного токена. В результате приватный ключ и сертификат пользователя из файла ovirtadmin.p12 будут импортированы на устройство Рутокен (рисунок 268).

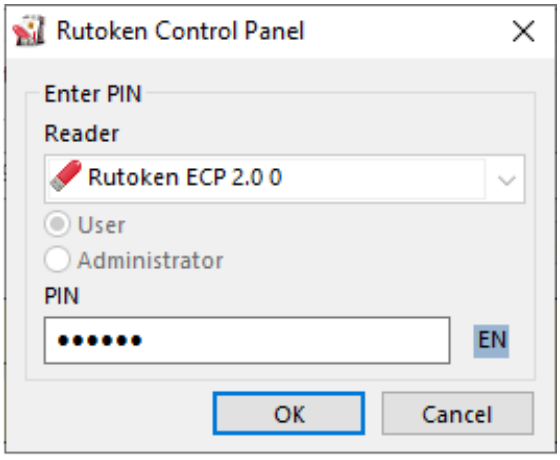


Рисунок 268 – Ввод ПИН-кода для "Рутокен ЭЦП"

Для включения двухфакторной аутентификации на веб-портале РОСА Виртуализация необходимо:

а) создать конфигурационный файл /etc/httpd/conf.d/x509-cert-verify.conf:

```
    SSLProtocol -all +TLSv1.2
    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>
```

б) отредактировать файл /etc/ovirt-engine/engine.conf.d/60-ovirt-2fa.conf, установив для переменной TWO_FACTOR_AUTHENTICATION значение "true":

```
    TWO_FACTOR_AUTHENTICATION=true
```

в) для переменной OVIRT_ADMIN_LOGIN установить значение "ovirtadmin" (логин учетной записи на IPA-сервере, сертификат от которой будет сопоставлен с внутренней учетной записью admin в СУСВ):

```
    OVIRT_ADMIN_LOGIN=ovirtadmin
```

г) перезапустить сервис httpd:

```
    # systemctl restart httpd
```

При необходимости контроля отозванных сертификатов требуется дополнительная настройка httpd-сервера. Контроль может осуществляться с помощью сервиса OCSP, предоставляемого IPA сервером, либо с помощью CRL:

– Вариант с использованием OCSP более прост в реализации, и для его настройки достаточно отредактировать ранее созданный файл /etc/httpd/conf.d/x509-cert-verify.conf:

```
    SSLOCSPEnable on
    SSLOCSPOverrideResponder on
    SSLOCSPDefaultResponder "http://ipa-ca.example.com/ca/ocsp"

    SSLProtocol -all +TLSv1.2
    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>
```

В переменной "SSLOCSPDefaultResponder" прописывается адрес IPA-сервера, который в данном примере выступает в роли центра сертификации и будет отвечать на OCSP запросы.

– Вариант контроля отозванных сертификатов на основе CRL более сложен в реализации и требует больше настроек:

1) в первую очередь необходимо подготовить список отозванных сертификатов. Он автоматически формируется на IPA-сервере и доступен по адресу http://ipa-ca.example.com/ipa/crl/MasterCRL.bin;
2) скачать файл с последующей конвертацией в PEM-формат для совместимости с httpd-сервером:

```
    # 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
```

3) отредактировать ранее созданный файл /etc/httpd/conf.d/x509-cert-verify.conf:

```
    SSLCARevocationCheck chain
    SSLCARevocationFile /etc/pki/ovirt-engine/apache-ca.crl

    SSLProtocol -all +TLSv1.2
    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>
```

Вне зависимости от того, какой вариант контроля отозванных сертификатов был выбран, после всех настроек требуется перезапустить сервис httpd:

```
# systemctl restart httpd
```

Примечание – CRL-файл имеет "дату/время" начала действия и "дату/время" окончания действия и быстро устаревает (через несколько часов после генерации на IPA-сервере). Это надо учитывать и позаботиться об автоматическом обновлении списка отозванных сертификатов для httpd-сервера (можно реализовать через планировщик заданий cron).

Пример настройки браузера Firefox для работы с USB "Рутокен ЭЦП 2.0":

а) в адресной строке браузера ввести "about:preferences#privacy" или перейти по вкладкам меню "Tools → Settings → Privacy & Security" (рисунок 269);

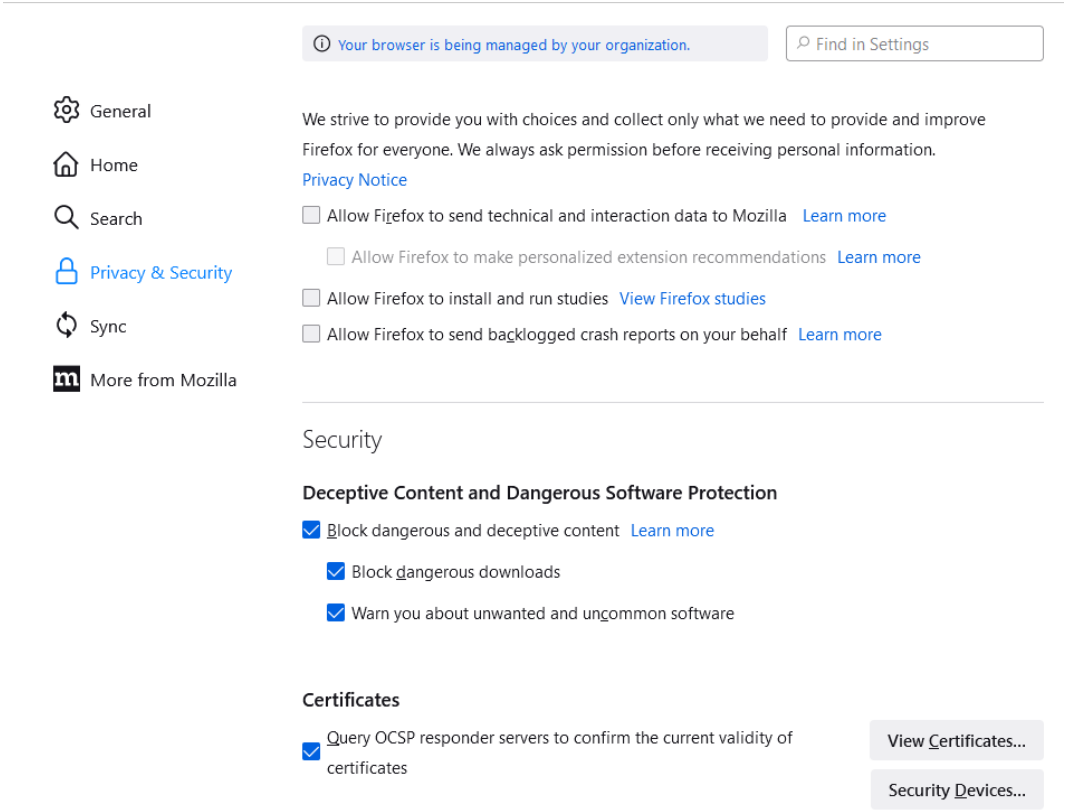


Рисунок 269 – Настройки браузера Firefox

б) нажать кнопку `Security Devices`;

в) в окне "Device Manager" нажать кнопку `Load` и заполнить все поля, указав расположение ранее установленной библиотеки PKCS#11 (librtpkcs11ecp.so – для операционных систем Linux или rtPKCS11ECP.dll – для операционных систем Windows) (рисунок 270).

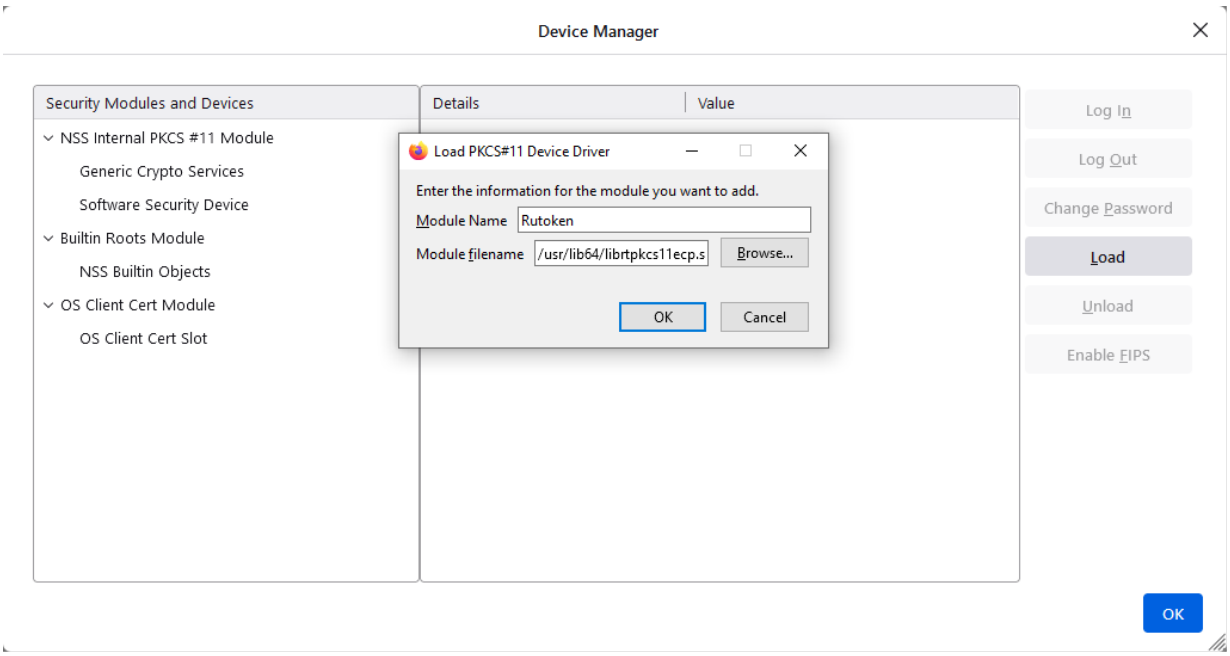


Рисунок 270 – Настройки браузера с библиотеками библиотекой PKCS#11

6.1.3 Двухфакторная аутентификация в локальной консоли с использованием Рутокен ЭЦП

Все действия по настройке двухфакторной аутентификации для локальной консоли выполняются на хосте с гипервизором под управлением РОСА Виртуализация:

а) убедиться, что на хосте установлены следующие пакеты и, если они отсутствуют, установить: opensc, pcsc-lite, pcsc-lite-ccid, pam_pkcs11, nss-tools;

б) установить библиотеку PKCS#11 для операционных систем GNU/Linux x64 https://www.rutoken.ru/support/download/pkcs/;

в) после установки пакета библиотека PKCS#11, необходимая для работы с токеном, будет находиться по пути /usr/lib64/librtpkcs11ecp.so. В качестве токена для аутентификации используется ранее подготовленный USB "Рутокен ЭЦП 2.0" для двухфакторной аутентификации на веб-портале РОСА Виртуализация для пользователя ovirtadmin. С процедурой подготовки токена можно ознакомиться в соответствующем разделе документации;

г) подключить токен к USB-порту хоста и с помощью консольной команды проверить его работоспособность:

```
# 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        : 6/249
       uri                :
pkcs11:model=Rutoken%20ECP;manufacturer=Aktiv%20Co.;serial=3ac65
c5d;token=Rutoken
```

д) для просмотра объектов, хранящихся на токене, можно воспользоваться командой:

```
     # 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>
     Certificate Object; type = X.509 cert
       label:      login_ovirtadmin
       subject:    DN: O=EXAMPLE.COM, CN=ovirtadmin
       serial:     0B
       ID:         10
       uri:
pkcs11:model=Rutoken%20ECP;manufacturer=Aktiv%20Co.;serial=3ac65
c5d;token=Rutoken;id=%10;object=login_ovirtadmin;type=cert
     Private Key Object; RSA
       label:      login_ovirtadmin
       ID:         10
       Usage:      decrypt, sign
       Access:     sensitive
```

```
      Allowed mechanisms: RSA-PKCS,RSA-PKCS-PSS,RSA-X-509,MD5-
RSA-PKCS,SHA1-RSA-PKCS,SHA224-RSA-PKCS,SHA256-RSA-PKCS,SHA384-
RSA-PKCS,SHA512-RSA-PKCS,SHA1-RSA-PKCS-PSS,SHA224-RSA-PKCS-
PSS,SHA256-RSA-PKCS-PSS,SHA384-RSA-PKCS-PSS,SHA512-RSA-PKCS-
PSS,RSA-PKCS-OAEP
      uri:
pkcs11:model=Rutoken%20ECP;manufacturer=Aktiv%20Co.;serial=3ac65
c5d;token=Rutoken;id=%10;object=login_ovirtadmin;type=private
```

e) для настройки модуля pam_pkcs11:

1) создать структуру каталогов и установить необходимые права доступа:

```
    # mkdir /etc/pam_pkcs11/{nssdb,cacerts,crls}
    # chmod 0644 /etc/pam_pkcs11/{nssdb,cacerts,crls}
```

2) скачать корневой сертификат с IPA-сервера:

```
    # curl -o /etc/pam_pkcs11/cacerts/ipa-ca.crt --insecure -L
https://ipa-ca.example.com/ipa/config/ca.crt
```

3) создать пустую базу данных для сертификатов и импортировать в нее корневой сертификат, полученный с IPA-сервера:

```
    # 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
```

4) при необходимости проверить присутствие корневого сертификата в базе данных командой:

```
    # certutil -L -d /etc/pam_pkcs11/nssdb

    Certificate Nickname                                        Trust
Attributes

SSL,S/MIME,JAR/XPI

    ipa-ca                                                      CT,C,C
```

5) преименовать существующий конфигурационный файл /etc/pam_pkcs11/pam_pkcs11.conf:

```
# mv /etc/pam_pkcs11/pam_pkcs11.conf \
/etc/pam_pkcs11/pam_pkcs11.conf.default
```

6) создать новый файл /etc/pam_pkcs11/pam_pkcs11.conf со следующим содержимым:

```
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;
      }
    }
```

7) для сопоставления сертификата, хранящегося на токене, и учетной записи пользователя root, под которой будет осуществляться локальный вход в Систему, создать файл /etc/pam_pkcs11/subject_mapping, примерно следующего содержания:

```
# Mapping file for Certificate Subject
# format: Certificate Subject -> login
#
CN=ovirtadmin,O=EXAMPLE.COM -> root
```

8) получить строку "CN=ovirtadmin,O=EXAMPLE.COM" для добавления в файл с помощью утилиты pkcs11_inspect, предварительно подключив токен к USB-порту и выполнив команду:

```
# pkcs11_inspect
PIN for token: <PIN-код пользователя>
Printing data for mapper subject:
CN=ovirtadmin,O=EXAMPLE.COM
```

Вход в Систему через локальную консоль будет возможен только под той учетной записью, для которой сопоставлен сертификат в файле /etc/pam_pkcs11/subject_mapping.

ж) включить двухфакторную аутентификацию для локальной консоли:

1) внести соответствующие изменения в систему PAM, отредактировав файл /etc/pam.d/system-auth, как показано на рисунке 271;

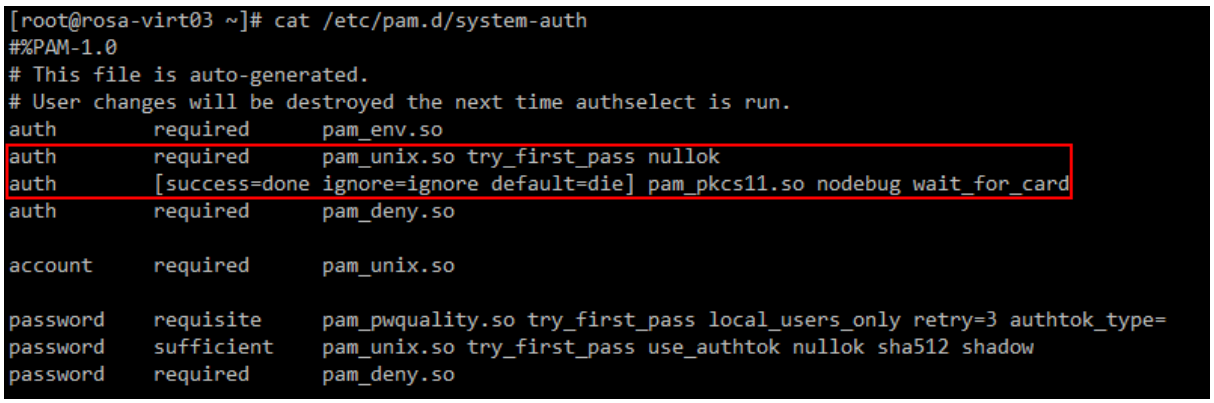


Рисунок 271 – Редактирование файла /etc/pam.d/system-auth

2) в файле заменить одну строку:

```
auth        sufficient    pam_unix.so try_first_pass nullok
```

на две новые строки:

```
auth        required      pam_unix.so try_first_pass nullok
auth  [success=done ignore=ignore default=die] pam_pkcs11.so
nodebug wait_for_card
```

В результате после всех сделанных настроек система PAM будет требовать ввода login/password и запрашивать ПИН-код к подключенному USB-токену (рисунок 272).

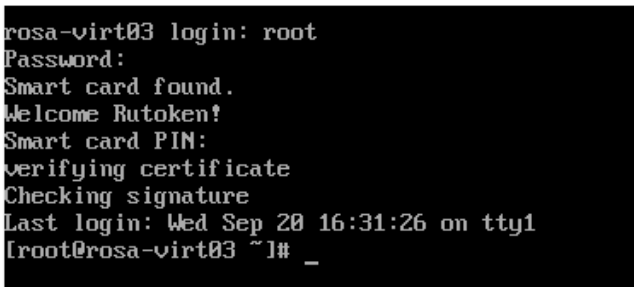


Рисунок 272 – Ввод ПИН-кода для "Рутокен ЭЦП"

В случае отсутствия USB-токена аутентификация будет прервана (рисунок 273).

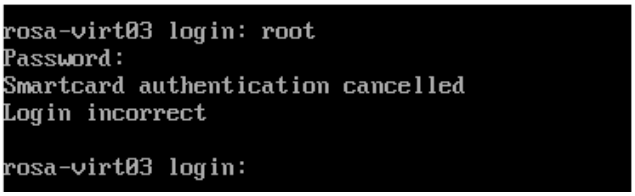


Рисунок 273 -Сбой аутентификации "Рутокен ЭЦП"

В консоль будет выведено сообщение:

```
Smartcard authentication cancelled
```

Аналогичный результат будет при вводе неправильных учётных данных (рисунок 274).

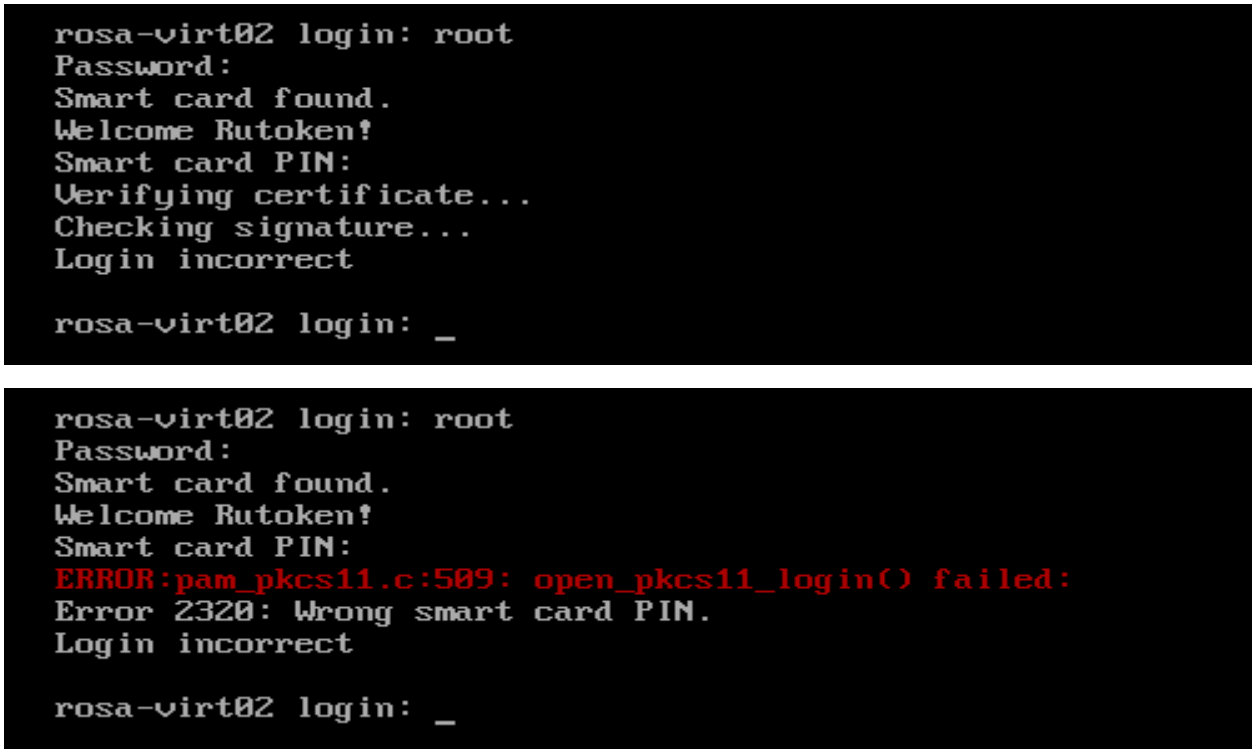


Рисунок 274 – Сообщения при вводе неправильных учётных данных

6.2 Настройка vGPU

В данном разделе описывается процесс настройки vGPU на примере NVIDIA RTX A6000.

6.2.1 Настройка системных параметров хоста

Все нижеперечисленные действия выполняются в консоли хоста с подключенным vGPU. Также для упрощения настройки загрузчика GRUB необходимо, чтобы хост не был подключен к СУСВ:

а) отредактировать в файле /etc/default/grub строку "GRUB_CMDLINE_LINUX", добавив параметры загрузки ядра "modprobe.blacklist=nouveau intel_iommu=on", чтобы получилась строка аналогичного вида:

```
    GRUB_CMDLINE_LINUX="crashkernel=auto resume=/dev/mapper/rv-swap rd.lvm.lv=rv/root rd.lvm.lv=rv/swap modprobe.blacklist=nouveau intel_iommu=on loglevel=4"
```

б) обновить конфигурацию загрузчика GRUB, выполнив одну из команд в зависимости от типа используемой системы загрузки:

– для UEFI:

```
    # grub2-mkconfig -o /boot/efi/EFI/rosa/grub.cfg
```

– для BIOS:

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

в) для установки драйверов:

1) включить репозиторий DVD и смонтировать диск в директорию /mnt:

```
    # dnf config-manager --set-enabled DVD
    # mount -t iso9660 -o ro /dev/sr0 /mnt
```

2) установить пакеты с драйверами и включить сервисы:

```
    # dnf install nvidia-vgpu-kvm nvidia-vgpu-kvm-kmod
    # systemctl enable nvidia-vgpu-mgr.service
    # systemctl enable nvidia-vgpud.service
```

3) перезагрузить хост;

г) проверить, с какими параметрами загрузилось ядро, с помощью команд:

```
    # dmesg | grep "Command line"
    # cat /proc/cmdline
```

з) проверить, какие модули ядра используются для vGPU, с помощью команд:

– `lspci`:

```
# lspci -knn | grep -A 15 NVIDIA
41:00.0 3D controller [0302]: NVIDIA Corporation Device
[10de:26b1] (rev a1)
        Subsystem: NVIDIA Corporation Device [10de:16a1]
        Kernel driver in use: nvidia
        Kernel modules: nouveau, nvidia_vgpu_vfio, nvidia
```

– `lsmod`:

```
# lsmod | grep -E 'vfio|nvidia'
nvidia_vgpu_vfio   65536 0
nvidia          35315712  11
vfio_mdev          16384  0
mdev               24576  2 vfio_mdev,nvidia_vgpu_vfio
vfio_iommu_type1   36864  0
vfio               36864  3
vfio_mdev,nvidia_vgpu_vfio,vfio_iommu_type1
drm               577536  7
drm_kms_helper,drm_vram_helper,ast,nvidia,drm_ttm_helper,ttm
```

Если установка драйвера прошла успешно, то вывод утилиты nvidia-smi будет аналогичного вида:

```
# nvidia-smi
Mon Aug 21 16:55:38 2023
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 470.82       Driver Version: 470.82       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  NVIDIA A16          On   | 00000000:45:00.0 Off |                    0 |
|  0%   39C    P8    15W /  62W |      0MiB / 15105MiB |      0%      Default |
|                               |                      |                  N/A |
+-------------------------------+----------------------+----------------------+
```

```
+-----------------------------------------------------------------------------+
| Processes:                                                                  |
|  GPU   GI   CI        PID   Type   Process name                  GPU Memory |
|        ID   ID                                                   Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

и) создать файл /etc/cron.d/sriov-manage со следующим содержанием:

```
 PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin
@reboot root sleep 60 && /usr/lib/nvidia/sriov-manage -e ALL
> /dev/null 2>&1
```

к) перезагрузить хост. Если все прошло успешно, то после перезагрузки можно увидеть список доступных vGPU в Системе:

```
 # lspci | grep NVIDIA
41:00.0 3D controller: NVIDIA Corporation Device 26b1 (rev a1)
41:00.4 3D controller: NVIDIA Corporation Device 26b1 (rev a1)
41:00.5 3D controller: NVIDIA Corporation Device 26b1 (rev a1)
41:00.6 3D controller: NVIDIA Corporation Device 26b1 (rev a1)
41:00.7 3D controller: NVIDIA Corporation Device 26b1 (rev a1)
41:01.0 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:01.1 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:01.2 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:01.3 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:01.4 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:01.5 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:01.6 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:01.7 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:02.0 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:02.1 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:02.2 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:02.3 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:02.4 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:02.5 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:02.6 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:02.7 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:03.0 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:03.1 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
```

```
41:03.2 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:03.3 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:03.4 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:03.5 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:03.6 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:03.7 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:04.0 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:04.1 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:04.2 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
41:04.3 3D controller: NVIDIA Corporation Device 26b1 (rev ff)
```

д) подключить хост к СУСВ стандартным способом, используя Портал Администрирования.

6.2.2 Установка драйвера vGPU

На следующем шаге настройки необходимо создать ВМ и установить гостевую ОС стандартным способом:

а) выключить ВМ и на Портале администрирования в разделе "Ресурсы – Виртуальные машины" открыть окно со свойствами настраиваемой ВМ, нажав на ссылку в поле "Имя";

б) перейти на вкладку "Устройства хоста" и нажать кнопку Управление vGPU;

в) в открывшемся окне выбрать vGPU, которое будет подключено к виртуальной машине, перевести переключатель "Вторичный видеоадаптер для VNC" в положение "Выкл.", нажать кнопку Сохранить (рисунок 275);

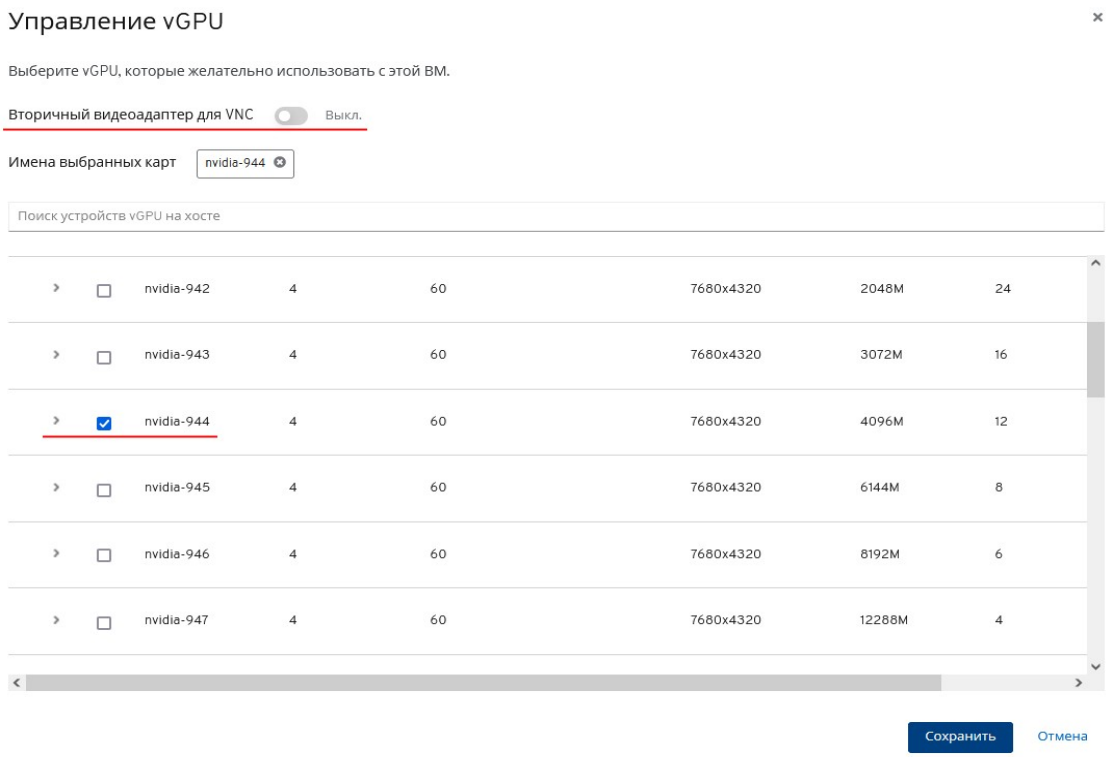


Рисунок 275 – Настройка vGPU

г) запустить ВМ и подключиться к SPICE консоли для установки vGPU драйвера. Диспетчер устройств до установки драйвера не будет отображать подключенных видеоадаптеров, как указано на рисунке 276.

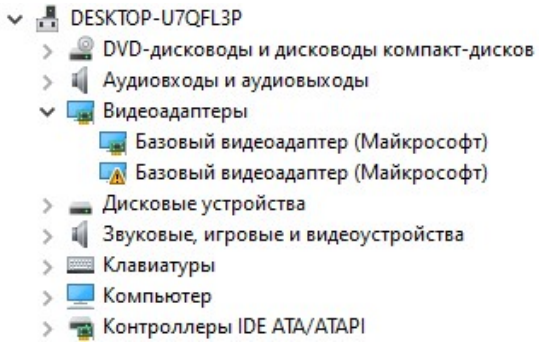


Рисунок 276 – Диспетчер устройств до установки vGPU драйвера

6.2.3 Настройка драйвера vGPU для ВМ

После установки для настройки драйвера vGPU для ВМ нужно выполнить следующие действия:

а) выключить ВМ, вновь открыть окно "Управление vGPU" и перевести переключатель "Вторичный видеоадаптер для VNC" в положение "Вкл." (рисунок 277);

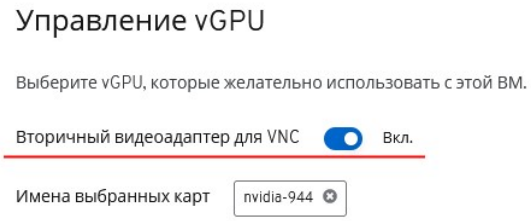


Рисунок 277 – Активация параметра "Вторичный видеоадаптер для VNC"

б) запустить вновь ВМ.

В диспетчере устройств должен появиться соответствующий видеоадаптер (рисунок 278).

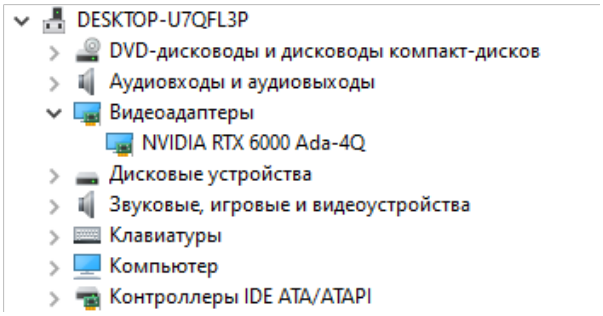


Рисунок 278 – Отображение подключенного видеоустройства в "Диспетчере устройств"

На хосте с помощью утилиты nvidia-smi можно отслеживать используемые ресурсы vGPU:

```
# nvidia-smi
Tue Aug 22 10:04:45 2023
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 470.82       Driver Version: 470.82       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  NVIDIA A16          On   | 00000000:45:00.0 Off |                    0 |
|  0%   37C    P8    15W /  62W |   3648MiB / 15105MiB |     10%      Default |
|                               |                      |                  N/A |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                                  |
|  GPU   GI   CI        PID   Type   Process name                  GPU Memory |
|        ID   ID                                                   Usage      |
|=============================================================================|
|    0   N/A  N/A    274838    C+G   vgpu                             3648MiB |
+-----------------------------------------------------------------------------+
```

ПРИЛОЖЕНИЕ А
VDSM И ПЕРЕХВАТЧИКИ СОБЫТИЙ

А.1 Применение VDSM

Виртуализированный ЦУ использует службу VDSM (Virtual Desktop and Server Manager) для управления виртуальными и физическими хостами, хранилищами хостов, ресурсами памяти и ресурсами сетей 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.

А.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/nn_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 настоящем Приложении А, используется Python.

Следует обратить внимание, что выполняются все сценарии, настроенные для события на хосте. Если необходимо, чтобы указанный перехватчик событий запускался только для определенного набора виртуальных машин, выполняемых на этом хосте, то требуется, чтобы это обеспечивал сам сценарий с помощью оценки настраиваемых пользователем свойств ВМ (см. п. А.7).

Следует обратить внимание, что перехватчики событий VDSM могут вмешиваться в работу РОСА Виртуализация. 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 А описывается, как расширить VDSM с помощью перехватчиков, запускаемых при определенных событиях. Расширение VDSM с помощью перехватчиков событий является экспериментальной технологией, поэтому информация 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 таблице 83 описываются поддерживаемые события VDSM.

Таблица 83 – Поддерживаемые события VDSM

Название	Описание
before_vm_start	Перед запуском ВМ
after_vm_start	После запуска ВМ
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

Название	Описание
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

Название	Описание
	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

Название	Описание
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
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 пользовательских свойств

Настраиваемые пользователем свойства, принимаемые диспетчером виртуализации и, в свою очередь, передаваемые пользовательским перехватчикам событий определяются с помощью команды `engine-config`. Эту команду следует выполнять с правами суперпользователя root на хосте, где установлен диспетчер виртуализации.

Конфигурационные ключи UserDefinedVMProperties и CustomDeviceProperties команды `engine-config` используются для хранения имен 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. Следует обратить внимание, что при указании конфигурационного ключа все уже содержащиеся в нем 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.

A.7.1 Настройка пользовательского свойства smartcard (свойство ВМ)

Для настройки пользовательского свойства smartcard (свойство ВМ) нужно:

а) выполнить 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
```

б) добавить новое пользовательское свойство smartcard к уже настроенному пользовательскому свойству memory, при этом указать, что новое свойство smartcard может принимать значения "true" или "false":

```
# engine-config -s UserDefinedVMProperties='memory=^[0-9]+$;
\
smartcard=^(true|false)$' --cver=4.0
```

в) выполнить 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
```

г) для применения изменений в конфигурации пользовательских свойств ВМ перезапустить службу ovirt-engine:

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

А.7.2 Настройка пользовательского свойства interface (свойство устройства)

Для настройки пользовательского свойства interface (свойство устройства) нужно:

а) выполнить 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 еще не были настроены:

```
# engine-config -g CustomDeviceProperties
CustomDeviceProperties:  version: 3.6
CustomDeviceProperties:  version: 4.0
```

б) добавить новое пользовательское свойство interface, при этом указать, 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
```

в) выполнить 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
```

г) для применения изменений в конфигурации пользовательских свойств устройства перезапустить службу ovirt-engine:

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

А.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. Можно добавлять дополнительные пары "ключ-значение", нажимая на кнопку +, и удалять их с помощью кнопки –.

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.

A.9.1 Оценка настраиваемых пользователем свойств

Следующий пример, написанный на Python, проверяет существование пользовательского свойства key1. Если свойство настроено, то 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 поставляется 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 измененный объект можно снова сохранить в XML-библиотеки libvirt.

В таблице 84 описываются функции модуля перехватчиков событий, предназначенные для поддержки разработки перехватчиков.

Таблица 84 – 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. Эти действия нужно выполнять с осторожностью. Сценарии перехватчиков событий потенциально

могут нарушить работу VDSM, а сценарии с программными ошибками могут привести к перерывам в работе окружения РОСА Виртуализация. В частности, никогда не следует изменять UUID домена и не пытаться 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.

A.11.1 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:

а) выполнить вход в Систему хоста виртуализации с правами root;
б) открыть файл /etc/sudoers в текстовом редакторе;
в) добавить 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` пользователю не будет предлагаться 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 таблице 85 описываются коды возврата сценариев перехватчиков событий. Коды возврата определяют, обрабатывает ли VDSM сценарий.

Таблица 85 – 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.

A.13.1 Тонкая настройка узла NUMA

Данный сценарий перехватчика событий дает возможность отрегулировать выделение памяти на хосте NUMA с использованием настроенного пользователем свойства numaset:

```
    numaset=^(interleave|strict|preferred):[\^]?\d+(-\d+)?(,
[\^]?\d+(-\d+)?)*$
```

Используемое регулярное выражение дает 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 Б
СВОЙСТВА СЕТЕЙ, НАСТРАИВАЕМЫЕ ПОЛЬЗОВАТЕЛЕМ

Б.1 Параметры bridge_opts

В таблице 86 описываются параметры "bridge_opts".

Таблица 86 – 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 войдет в состояние передачи данных. Этот параметр дает 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 передает мост, проверяется и очищается от устаревших записей
group_addr	При отправке общего запроса значение параметра устанавливается на "0". 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 дает возможность мосту передавать локальные адреса групп каналов. Смена изначального значения параметра разрешает нестандартное поведение моста
hash_elasticity	Максимальная длина цепи, разрешенная в хэш-таблице. Значение параметра вступает в силу после добавления новой многоадресной группы. Если после повторного хеширования 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

Параметр	Описание
	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 "мертвым", и начнется 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 ждет 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 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

Параметр	Описание
	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 дает возможность включать или отключать порты с подключенными 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

Параметр	Описание
	многоадресного трафика на портах
multicast_snooping	Параметр дает 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 дает возможность пользователю повторно включить отслеживание, если оно было автоматически выключено из-за хеш-конфликта, но, если хеш-конфликт не был разрешен, 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

Б.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.

Б.2.1 Добавление ключа ethtool_opts в виртуализированный ЦУ

Для добавления ключа ethtool_opts в виртуализированный ЦУ необходимо:

а) выполнить следующую команду на машине виртуализированного ЦУ:

```
    # engine-config -s
UserDefinedNetworkCustomProperties=ethtool_opts=.* --cver=4.0
```

б) для применения изменений в конфигурации перезапустить службу ovirt-engine:

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

в) на тех хостах, где нужно настроить параметры `ethtool`, установить 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 чего выполнить следующую команду:

```
# yum install vdsm-hook-ethtool-options
```

В результате на Портале администрирования станет доступен ключ ethtool_opts.

Б.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, можно выполнить следующую команду:

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

Б.3.1 Добавление ключа FCoE в виртуализированный ЦУ

Для добавления ключа FCoE в виртуализированный ЦУ нужно:

а) выполнить следующую команду на машине виртуализированного ЦУ:

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

б) для применения изменений в конфигурации перезапустить службу ovirt-engine:

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

в) на тех хостах, где нужно настроить параметры FCoE, установить пакет с перехватчиками событий VDSM. По умолчанию пакет vdsm-hook-fcoe установлен на хостах виртуализации, а на стандартных хостах его необходимо установить дополнительно, для чего выполнить следующую команду:

```
# yum install vdsm-hook-fcoe
```

В результате на Портале администрирования станет доступен ключ fcoe.

ПРИЛОЖЕНИЕ В
МОДУЛИ ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА

B.1 Модули пользовательского интерфейса

В Системе виртуализации POCA Виртуализация 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 POCA Виртуализация 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 поглощен отдельными модулями. Каждый модуль получает отдельный экземпляр pluginApi, давая возможность Порталу администрирования контролировать вызовы функций API этого модуля со стороны каждого отдельного модуля с учетом жизненного цикла модуля.

B.2 Жизненный цикл модуля пользовательского интерфейса

B.2.1 Этапы жизненного цикла модуля пользовательского интерфейса

Базовый жизненный цикл модуля пользовательского интерфейса разделен на следующие этапы:

– Обнаружение модуля UI.
– Загрузка модуля UI.
– Самонастройка модуля UI.

B.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.

В.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 создает 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.

В.2.4 Самонастройка модуля пользовательского интерфейса

Процесс самонастройки модуля UI состоит из последовательного выполнения следующих шагов:

а) получить экземпляр pluginApi для указанного модуля;

б) опционально получить объект конфигурации модуля времени выполнения;

в) зарегистрировать функции соответствующего обработчика событий;

г) сообщить 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();
```

В.3 Файлы модуля пользовательского интерфейса

В таблице 87 описываются файлы модуля UI, а также указывается расположение этих файлов в Системе.

Таблица 87 – 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>/	<resourcePath>

Файл	Расположение	Примечания
	PluginHostPage.html	настраивается с помощью соответствующего атрибута дескриптора модуля

В.4 Пример развертывания 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.

Для развертывания модуля "Hello World!" нужно:

а) создать 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"
    }
```

б) создать 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 (рисунок 279) появится при выполнении входа в Систему на Портале администрирования виртуализированного ЦУ.



Рисунок 279 – Заставка модуля "Hello World!"

ПРИЛОЖЕНИЕ Г
СИСТЕМА ВИРТУАЛИЗАЦИИ И ШИФРОВАНИЕ СВЯЗИ

Г.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 следует убедиться 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.

Важно — Не следует изменять 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, необходимо извлечь их с помощью инструкции (п. Г.1.1), в которой подразумевается, что полученный файл находится в /tmp/apache.p12. В случае других форматов файла рекомендуется связаться со сторонним ЦС для консультации.

Г.1.1 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.

Для извлечения сертификата и закрытого ключа из файла с расширением *.p12 нужно:

а) создать резервную копию текущего файла apache.p12:

```
# cp -p /etc/pki/ovirt-engine/keys/apache.p12 \
/etc/pki/ovirt-engine/keys/apache.p12.bck
```

б) заменить текущий файл на файл, полученный из стороннего ЦС:

```
# cp /tmp/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

в) извлечь закрытый ключ и сертификат ключа в необходимое местоположение (если файл защищен паролем, добавить параметр "-passin pass:_password_", в котором заменить "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
```

Г.1.2 Замена сертификата ЦС виртуализированного ЦУ для Apache

Для замены сертификата ЦС виртуализированного ЦУ для Apache нужно:

а) перевести окружение в режим глобального обслуживания:

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

б) добавить сертификат стороннего ЦС в хранилище доверенных сертификатов хоста:

```
# cp /tmp/3rd-party-ca-cert.pem
/etc/pki/ca-trust/source/anchors
# update-ca-trust
```

в) удалить 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
```

г) сохранить сертификат ЦС как /etc/pki/ovirt-engine/apache-ca.pem:

```
    # cp /tmp/3rd-party-ca-cert.pem
/etc/pki/ovirt-engine/apache-ca.pem
```

д) создать 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
```

е) скопировать закрытый ключ в необходимое местоположение:

```
    # cp /tmp/apache.key
/etc/pki/ovirt-engine/keys/apache.key.nopass
```

ж) указать суперпользователя root в качестве владельца закрытого ключа и настроить права доступа "0640":

```
    # chown root:ovirt
/etc/pki/ovirt-engine/keys/apache.key.nopass
    # chmod 640 /etc/pki/ovirt-engine/keys/apache.key.nopass
```

з) скопировать сертификат в необходимое местоположение:

```
    # cp /tmp/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

и) перезапустить веб-сервер Apache:

```
    # systemctl restart httpd.service
```

к) создать 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=""
```

л) скопировать файл /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf, переименовав этот файл с применением для индекса номера больше 10 (например, "99-setup.conf) и добавив 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
```

м) перезапустить службу ovirt-websocket-proxy:

```
# systemctl restart ovirt-websocket-proxy.service
```

н) если файл /etc/ovirt-provider-ovn/conf.d/10-setup-ovirt-provider-ovn.conf был отредактирован вручную, убедиться, что в виртуализированном ЦУ в качестве источника сертификата по-прежнему используется /etc/pki/ovirt-engine/apache-ca.pem;

о) для включения в engine-backup возможности обновления при восстановлении создать 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
```

п) перезапустить службу ovirt-provider-ovn:

```
# systemctl restart ovirt-provider-ovn.service
```

р) перезапустить службу ovirt-engine:

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

с) отключить 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.

Г.2 Настройка шифрованного соединения между виртуализированным ЦУ и сервером LDAP

Для настройки шифрованного соединения между виртуализированным ЦУ и сервером LDAP необходимо получить корневой сертификат ЦС сервера LDAP, скопировать этот сертификат на машину виртуализированного ЦУ и создать сертификат ЦС в кодировке PEM.

Тип файла ключа может быть любым типом, поддерживаемым Java. В приведенной в п. Г.2.1 процедуре используется файл ключа с расширением *.jks в формате Java KeyStore.

Примечание — Дополнительные сведения о создании сертификатов ЦС в кодировке PEM, а также об импорте сертификатов можно посмотреть в разделе "X.509 CERTIFICATE TRUST STORE" файла README в каталоге /usr/share/doc/ovirt-engine-extension-aaa-ldap-версия.

Г.2.1 Создание сертификата ЦС в кодировке PEM

Для создания сертификата ЦС в кодировке PEM нужно выполнить следующие действия:

а) на машине виртуализированного ЦУ скопировать корневой сертификат ЦС сервера LDAP в каталог /tmp и импортировать 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 создает сертификат ЦС в кодировке PEM myrootca.jks в каталоге /etc/ovirt-engine/aaa/.

б) обновить 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, следует заменить ${local:_basedir} на полный путь до сертификата.

Г.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 рекомендуется использовать стойкое шифрование.

Г.3.1 Настройка шифрования соединений VDSM вручную

Для настройки шифрования соединений VDSM вручную нужно:

а) нажать "Ресурсы → Хосты" и выбрать хост;

б) нажать "Управление → Обслуживание", чтобы открыть окно подтверждения "Хосты на обслуживании";

в) нажать кнопку OK, чтобы запустить режим обслуживания;

г) создать на хосте файл /etc/vdsm/vdsm.conf.d/99-custom-ciphers.conf со следующим параметром:

```
    [vars]
    ssl_ciphers = HIGH
```

д) перезапустить службу VDSM:

```
    # systemctl restart vdsm
```

е) нажать "Ресурсы → Хосты" и выбрать хост;

ж) нажать "Управление → Активировать", чтобы повторно активировать хост.

ПРИЛОЖЕНИЕ Д
ПРОКСИ-СЕРВЕР

Д.1 Прокси-сервер SPICE

Д.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.

Д.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 POCA Виртуализация. Для предоставления служб прокси используется Squid.

Для установка прокси-сервера Squid нужно:

а) установить Squid на машине прокси, выполнив команду:

```
# yum install squid
```

б) в конфигурационном файле /etc/squid/squid.conf в строке "http_access deny CONNECT" заменить значение "!SSL_ports" на значение "! Safe_ports";

в) запустить службу squid и включить автоматический запуск этой службы в процессе загрузки Системы:

```
# systemctl enable squid.service --now
```

г) разрешить исходящие запросы на службу squid в зоне по умолчанию межсетевого экрана firewalld:

```
# firewall-cmd --permanent --add-service=squid
```

д) для применения изменений в конфигурации перезапустить службу межсетевого экрана firewalld:

```
# firewall-cmd --reload
```

В результате данная машина будет настроена для протокола SPICE в качестве прокси.

Необходимо активировать (включить) прокси перед тем, как подключаться извне к сетям РОСА Виртуализация.

Д.1.3 Включение SPICE Proxy

В следующей последовательности действий описывается, как активировать (включить) прокси для протокола SPICE.

Для активации SPICE Proxy нужно:

а) на машине виртуализированного ЦУ выполнить следующую команду с применением утилиты engine-config для настройки прокси:

```
# engine-config -s SpiceProxyDefault=someProxy
```

б) перезапустить службу ovirt-engine:

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

В результате SPICE Proxy будет активирован (включен), предоставляя возможность подключения извне к сетям РОСА Виртуализация 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 РОСА Виртуализация. 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.

Д.1.4 Выключение SPICE Proxy

В следующей последовательности действий описывается, как выключить (деактивировать) прокси для протокола SPICE.

Для выключения SPICE Proxy нужно:

а) на машине виртуализированного ЦУ выполнить следующую команду для очистки прокси SPICE:

```
# engine-config -s SpiceProxyDefault=""
```

б) перезапустить службу ovirt-engine:

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

В результате SPICE Proxy будет деактивирован (выключен) и подключение извне к сетям РОСА Виртуализация через прокси-сервер для протокола SPICE станет невозможным.

Д.2 Прокси-сервер Squid

Д.2.1 Установка и настройка Squid

В данном разделе описывается, как установить и настроить прокси-сервер Squid для Портала ВМ.

Прокси-сервер Squid используется в качестве ускорителя передачи данных за счет кеширования часто просматриваемого содержимого, что повышает пропускную способность и снижает время откликов.

Для настройки прокси-сервера Squid нужно:

а) получить в установленном порядке закрытый ключ и сертификат ключа для порта HTTPS прокси-сервера Squid в виде файлов proxy.key и proxy.cer соответственно;

б) установить Squid на машине прокси:

```
# yum install squid
```

в) переместить полученные файлы proxy.key и proxy.cer с закрытым ключом и сертификатом ключа в каталог машины прокси (например, /etc/squid);

г) установить права на чтение файлов proxy.key и proxy.cer для пользователя squid:

```
# chgrp squid /etc/squid/proxy.*
```

```
# chmod 640 /etc/squid/proxy.*
```

д) Squid должен верифицировать сертификат ЦС, используемый виртуализированным ЦУ, для чего скопировать с виртуализированного ЦУ сертификат ЦС /etc/pki/ovirt-engine/ca.pem на машину прокси в каталог /etc/squid и установить права на чтение файла сертификата ca.pem для пользователя squid:

```
# chgrp squid /etc/squid/ca.pem
# chmod 640 /etc/squid/ca.pem
```

е) для принудительного режима SELinux изменить 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
```

ж) заменить 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
```

з) перезапустить службу прокси-сервера Squid:

```
# systemctl restart squid.service
```

Примечание — Для увеличения интервала времени простоя Squid перед разрывом соединения (по умолчанию – 15 минут простоя) следует настроить параметр read_timeout в файле конфигурации Squid /etc/squid/squid.conf (например, значение "read_timeout 10 hours" увеличивает интервал времени простоя до 10 часов).

Д.3 Прокси-сервер WebSocket

Д.3.1 Обзор прокси-сервера WebSocket

Прокси-сервер WebSocket дает 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 пользователям 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.

Д.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.

Для удаления WebSocket с машины виртуализированного ЦУ требуется:

а) запустить утилиту engine-cleanup на машине виртуализированного ЦУ:

```
# engine-cleanup
```

б) при запросе на удаление всех компонентов ввести "No":

```
Do you want to remove all components? (Yes, No) [Yes]: No
```

в) при запросе на удаление виртуализированного ЦУ (engine) ввести "No":

```
Do you want to remove the engine? (Yes, No) [Yes]: No
```

г) при запросе на удаление прокси-сервера WebSocket ввести "Yes":

```
Do you want to remove the WebSocket proxy? (Yes, No) [No]: Yes
```

д) при запросах на удаление любых других компонентов вводить "No".

Для установки WebSocket на отдельной машине нужно:

а) установить прокси-сервер WebSocket:

```
# yum install ovirt-engine-websocket-proxy
```

б) запустить 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 ввести "No".

в) при выводе следующего запроса нажать клавишу `Enter` для запуска процесса настройки конфигурации прокси-сервера WebSocket на данной машине:

```
Configure WebSocket Proxy on this machine? (Yes, No) [Yes]:
```

г) при выводе следующего запроса нажать клавишу `Enter`, чтобы принять автоматически определенное имя хоста, или ввести альтернативное имя хоста (следует обратить внимание, что при использовании виртуальных хостов автоматически определенное имя хоста может быть неправильным):

```
Host fully qualified DNS name of this server
[host.example.com]:
```

д) при выводе следующего запроса нажать 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]:
```

е) при выводе следующего запроса ввести полное доменное имя (FQDN) машины виртуализированного ЦУ:

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

ж) при выводе следующего запроса нажать клавишу `Enter`, чтобы утилита engine-setup автоматически выполнила необходимые настройки на машине виртуализированного ЦУ, или ввести 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]:
```

е) для настройки вручную:

1) при выводе следующего запроса нажать клавишу `Enter`, чтобы принять номер порта SSH по умолчанию, или указать номер порта SSH машины виртуализированного ЦУ:

```
    ssh port on remote engine server [22]:
```

2) указать пароль суперпользователя root для выполнения входа в Систему на машине виртуализированного ЦУ:

```
    root password on remote engine server
engine_host.example.com:
```

з) при выводе следующего запроса ввести "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]:
```

и) при выводе ранее настроенных параметров нажать 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]:
```

ж) ознакомиться 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
```

к) осуществить вход в Систему на машине виртуализированного ЦУ и выполнить следующие команды для завершения настройки:

```
     # engine-config -s WebSocketProxy=host.example.com:6100
     # systemctl restart ovirt-engine.service
```

ПРИЛОЖЕНИЕ Е
СИСТЕМНЫЕ УЧЕТНЫЕ ЗАПИСИ

Е.1 Системные записи пользователей виртуализированного ЦУ

Во время установки пакета rhevm создаются следующие системные учетные записи пользователей с соответствующими идентификаторами (UID) для поддержки РОСА Виртуализация:

– 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.

Е.2 Группы виртуализированного ЦУ

Во время установки пакета rhevm создаются следующие системные учетные записи групп пользователей с соответствующими идентификаторами (GID) для поддержки РОСА Виртуализация:

– 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.

Е.3 Системные записи пользователей хостов виртуализации

Во время установки пакетов vdsm и qemu-kvm-rhev на хостах виртуализации создаются следующие системные учетные 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 учетной записью в Системе, во время установки пакетов vdsm и qemu-kvm-rhev возникнет конфликт.

Е.4 Группы хостов виртуализации

Во время установки пакетов vdsm и qemu-kvm-rhev на хостах виртуализации создаются следующие системные учетные 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.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Определение
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
Хранилище объектов Ceph	Основной набор программного обеспечения для хранения данных, в котором хранятся данные пользователя (MON+OSD)
ЦОД	Центр обработки данных
ЦП	Центральный процессор
ЦС	Центр сертификации (удостоверяющий центр)
ЦУ	Центр управления
ABRT (Automatic Bug Reporting Tool)	средство автоматического обнаружения ошибок
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)
Ceph	Распределенное сетевое хранилище и файловая система с распределенным управлением метаданными
Ceph OSD Демон, Ceph OSD	Программное обеспечение Ceph OSD, взаимодействующее с логическим диском (OSD)

Сокращение	Определение
CephFS (The Ceph File System)	Файловая система Ceph; POSIX-совместимая файловая система, построенная на основе распределенного хранилища объектов Ceph
cephx	Протокол аутентификации Ceph. Cephx работает как Kerberos, но не имеет единой точки отказа
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 имен
DVD (Digital Versatile Disc)	Цифровой многоцелевой диск
Ext3	Журналируемая файловая система
Ext4	Журналируемая файловая система
FAT (File allocation table)	Таблица размещения файлов
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
Gluster, GlusterFS	Распределенная, параллельная, линейно масштабируемая файловая система с возможностью защиты от сбоев
GPU (Graphics Processing Unit)	Графический ускоритель (процессор)

Сокращение	Определение
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

Сокращение	Определение
LVM (Logical Volume Management)	Менеджер логических томов
MAC (Media Access Control)	Уникальный идентификатор сетевого оборудования
MDS (The Ceph MetaData Server daemon), Ceph-MDS	Сервер метаданных Ceph; программное обеспечение метаданных Ceph
MGR (The Ceph manager)	Менеджер Ceph; программное обеспечение Ceph Manager, которое собирает данные по состоянию всего кластера в одном месте
MIB (Management Information Base)	База управляющей информации
MoM (Memory Overcommit Manager)	Диспетчер превышенного выделения памяти
MON (The Ceph monitor)	Монитор Ceph; программное обеспечение монитора Ceph
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
OSD (Object Storage Device)	Устройство хранения объектов; физическая или логическая единица хранения в Ceph, логический диск
OVA (Open Virtual Appliance)	Файл (архив в формате OVF) виртуальной машины
OVF (Open Virtualization Format)	Формат образа виртуальной машины
OVN (Open Virtual Network)	Виртуальная сеть с поддержкой OVS
OVS (Open vSwitch)	Виртуальный коммутатор

Сокращение	Определение
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
PV (Physical Volume)	физический том
PXE (Preboot eXecution Environment)	среда для загрузки компьютера с помощью сетевой карты
QCOW (QEMU Copy on Write)	Формат образа виртуального диска
QEMU (Quick Emulator)	Эмулятор аппаратного обеспечения различных платформ
QoS (Quality of Service)	Качество обслуживания
QXL	паравиртуализированное графическое устройство для QEMU/KVM, оптимизированное для удаленного доступа через протокол SPICE
RAC (Remote Access Card)	Карта удаленного доступа
RDMA (Remote Direct Memory Access)	Удаленный прямой доступ к памяти
RDP (Remote Desktop Protocol)	Протокол удаленного рабочего стола
RHDS (Red Hat® Directory Server)	Сервер службы каталогов
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

Сокращение	Определение
	уровне ядра ОС
SMT (Symmetric Multiprocessing)	Синхронная многопоточность (гиперпоточность)
SNMP (Simple Network Management Protocol)	Простой протокол сетевого управления
SPICE (Simple Protocol for Independent Computing Environments)	Протокол удаленного 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)	Защищенная оболочка
SSL (Secure Sockets Layer)	Уровень защищенных 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)	Счетчик метки времени
UCS (Unified Computing System)	Система унифицированных вычислений компании Cisco
UEFI (Unified Extensible Firmware Interface)	Объединенный интерфейс расширяемой прошивки
UI (User Interface)	Пользовательский интерфейс
UID (User Identifier)	Идентификатор пользователя
URI (Uniform Resource Identifier)	Унифицированный идентификатор ресурса
URL (Uniform Resource Locator)	Сетевой адрес ресурса
USB (Universal Serial Bus)	Универсальная последовательная шина
UUID (Universally Unique Identifier)	Уникальный идентификатор элемента
V4 (формат)	Внутренний номер формата (версия) oVirt
VDI (Virtual Desktop Infrastructure)	Инфраструктура виртуальных рабочих мест

Сокращение	Определение
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
VFAT	Virtual file allocation table – виртуальная таблица размещения файлов
VFS (Virtual File System)	Виртуальная файловая система
VGA (Video Graphics Array)	Видеоадаптер VGA
VGPU (Virtual Graphics Processing Unit)	Виртуальный графический ускоритель (процессор)
VirtIO	семейство паравиртуализованных устройств для виртуальных машин, которое дает гостевой ОС эффективный и стандартизованный способ общения с хостом/гипервизором.
VLAN (Virtual Local Area Network)	Виртуальная локальная вычислительная сеть
VMDK (Virtual Machine Disk)	Формат образа диска виртуальной машины VMware
VNC (Virtual Network Computing)	Система (протокол) удаленного доступа в виртуальных сетях
VNIC (Virtual Network Interface Controller)	Виртуальный сетевой адаптер
XFS	Высокопроизводительная 64-битная журналируемая файловая система
XML (eXtensible Markup Language)	Расширяемый язык разметки
XOR (eXclusive OR)	Исключающее "ИЛИ" (логическая операция)
YAML (Yet Another Markup Language)	Язык разметки