АО «НТЦ ИТ РОСА»

2/1

Программная система управления средой виртуализации с подсистемой безагентного резервного копирования виртуальных машин «ROSA Virtualization 3.0»

Руководство администратора

РСЮК.10102-01 92 01

Листов 495

2024

СОДЕРЖАНИЕ

Введение **13**
Часть I. Администрирование и обслуживание среды виртуализации **14**
Глава 1. Настройка глобальных ресурсов **14**
1.1. Роли **15**
1.1.1. Добавление новой роли 15
1.1.2. Изменение параметров роли 17
1.1.3. Роль «Пользователь» и примеры авторизации 20
1.2. Системные полномочия **23**
1.2.1. Свойства пользователя 23
1.2.2. Роли и привилегии пользователей 24
1.2.3. Роли и привилегии администраторов 26
1.2.4. Присвоение ресурсу роли администратора или пользователя 29
1.2.5. Удаление роли администратора или пользователя с ресурса 34
1.2.6. Управление системными полномочиями в дата-центре 36
1.2.7. Управление системными полномочиями в кластере 36
1.2.8. Управление сетевыми системными полномочиями 37
1.2.9. Управление системными полномочиями для хоста 38
1.2.10. Управление системными полномочиями в домене хранилища 39
1.2.11. Управление системными полномочиями на пул виртуальных машин 40
1.2.12. Управление системными полномочиями на виртуальные диски 40
1.2.13. Настройка шифра для старых версий SPICE 41
1.3. Политики планирования **42**
1.3.1. Создание политик планирования 44
1.3.2. Параметры в окнах «Новая политика планирования» и «Параметры политики планирования» 48
1.4. Типы экземпляров **51**
1.4.1. Создание типов экземпляров 51
1.4.2. Изменение типов экземпляров 58
1.4.3. Удаление типов экземпляров 60
1.5. Пулы адресов MAC **62**
1.5.1. Создание пулов MAC адресов 63
1.5.2. Изменение пулов адресов MAC 64
1.5.3. Удаление пулов адресов MAC 65
Глава 2. Панель мониторинга **66**
2.1. Предварительные условия для установки **66**
2.2. Общий перечень **66**
2.3. Общий коэффициент использования **68**

2.3.1. Наиболее используемые ресурсы ... 69
2.4. Использование кластера ... 71
2.4.1. Использование ЦП ... 71
2.4.2. Использование памяти ... 72
2.5. Использование хранилищ ... 72
Глава 3. Поиск ... 73
3.1. Операции поиска в системе виртуализации ... 73
3.2. Примеры поиска и поисковый синтаксис ... 73
3.3. Автодополнение поиска ... 73
3.4. Типы результатов поиска ... 74
3.5. Критерии поиска ... 74
3.6. Несколько критериев поиска и символы подстановки ... 76
3.7. Определение порядка поиска ... 76
3.8. Поиск дата-центров ... 76
3.9. Поиск кластеров ... 77
3.10. Поиск хостов ... 77
3.11. Поиск сетей ... 79
3.12. Поиск хранилищ ... 80
3.13. Поиск дисков ... 81
3.14. Поиск томов ... 83
3.15. Поиск виртуальных машин ... 84
3.16. Поиск пулов ... 86
3.17. Поиск шаблонов ... 87
3.18. Поиск пользователей ... 88
3.19. Поиск событий ... 90
Глава 4. Закладки ... 93
4.1. Сохранение строки поискового запроса в виде закладки ... 93
4.2. Редактирование закладок ... 94
4.3. Удаление закладок ... 95
Глава 5. Теги ... 97
5.1. Настройка взаимодействия с системой виртуализации с помощью тегов ... 97
5.2. Создание тегов ... 97
5.3. Редактирование тегов ... 97
5.4. Удаление тега ... 98
5.5. Присвоение тегов объектам и снятие меток с объектов ... 98
5.6. Поиск объектов на основе тегов ... 100
5.7. Сортировка хостов с помощью тегов ... 100
Часть II. Администрирование ресурсов ... 101
Глава 6. Качество обслуживания ... 101
6.1. Качество обслуживания хранилища ... 101

6.1.1. Создание записи о качестве обслуживания хранилища....101
6.1.2. Удаление записи о качестве обслуживания хранилища....103
6.2. Качество обслуживания сети виртуальной машины....103
6.2.1. Создание записи о качестве обслуживания сети ВМ....103
6.2.2. Параметры в окне «Новая QoS сети ВМ»....105
6.2.3. Удаление записи о качестве обслуживания сети ВМ....106
6.3. Качество обслуживания сетей хоста....106
6.3.1. Создание записи о качестве обслуживания для сетей хоста....106
6.3.2. Параметры в окне «Новая QoS сети хоста»....107
6.3.3. Удаление записи о качестве обслуживания для сетей хоста....108
6.4. Качество обслуживания ЦП....108
6.4.1. Создание записи качества обслуживания для ЦП....108
6.4.2. Удаление записи качества обслуживания для ЦП....110
Глава 7. Дата-центры....111
7.1. Введение в понятие дата-центров....111
7.2. Диспетчер пула хранилища (SPM)....112
7.3. Приоритет диспетчера пула хранилища....112
7.4. Задачи при работе с дата-центрами....113
7.4.1. Создание нового дата-центра....113
7.4.2. Параметры в окнах «Новый дата-центр» и «Параметры дата-центра»....118
7.4.3. Повторная инициализация дата-центра (процедура восстановления)....119
7.4.4. Удаление дата-центра....120
7.4.5. Принудительное удаление дата-центра....120
7.4.6. Изменение типа хранилища дата-центра....121
7.4.7. Изменение версии совместимости дата-центра....121
7.5. Дата-центры и домены хранилищ....122
7.5.1. Добавление существующего домена данных к дата-центру....122
7.5.2. Добавление существующего домена ISO к дата-центру....122
7.5.3. Присоединение существующего домена экспорта к дата-центру....123
7.5.4. Отсоединение доменов хранилищ от дата-центра....123
Глава 8. Кластеры....126
8.1. Введение в понятие кластеров....126
8.2. Задачи при работе с кластерами....126
8.2.1. Создание нового кластера....127
8.2.2. Общие параметры кластера....140
8.2.3. Параметры оптимизации....143
8.2.4. Политики миграции....145
8.2.5. Политики планирования....148
8.2.6. Параметры консоли кластера....152

8.2.7. Параметры политики операций блокады....152
8.2.8. Настройка политик управления нагрузкой и энергосбережения на хосте....153
8.2.9. Обновление информации о политике MoM на хостах в кластере....156
8.2.10. Создание профиля ЦП....156
8.2.11. Удаление профиля ЦП....157
8.2.12. Импортирование существующего кластера хранилища Gluster....157
8.2.13. Параметры хранилища Gluster в окне «Добавить хосты»....158
8.2.14. Удаление кластеров....159
8.2.15. Оптимизация памяти....159
8.2.16. Изменение версии совместимости кластера....164

Глава 9. Логические сети....166

9.1. Задачи при работе с логическими сетями....166

9.1.1. Выполнение сетевых задач....166
9.1.2. Создание новой логической сети в дата-центре или кластере....166
9.1.3. Изменение параметров логических сетей....168
9.1.4. Удаление логической сети....169
9.1.5. Настройка логической сети, не являющейся сетью управления, в качестве маршрута по умолчанию....170
9.1.6. Просмотр или редактирование параметров шлюза логической сети....172
9.1.7. Общие параметры логической сети....176
9.1.8. Параметры кластеров при настройке логических сетей....178
9.1.9. Параметры профилей vNIC при настройке логических сетей....178
9.1.10. Настройка конкретного типа трафика для логической сети в окне «Управление сетями»....179
9.1.11. Параметры в окне «Управление сетями»....179
9.1.12. Изменение конфигурации виртуальной функции сетевой платы....180

9.2. Виртуальные сетевые платы (vNIC)....181

9.2.1. Обзор профиля vNIC....181
9.2.2. Создание или изменение профиля vNIC....181
9.2.3. Параметры в окне «Профиль сетевого адаптера ВМ»....185
9.2.4. Включение сквозного доступа в профиле vNIC....186
9.2.5. Удаление профиля vNIC....187
9.2.6. Присвоение групп безопасности профилям vNIC....187
9.2.7. Полномочия пользователей на профили vNIC....189
9.2.8. Настройка профилей vNIC для интеграции с UCS....192

9.3. Сети внешних поставщиков....193

9.3.1. Импортирование сетей из внешних поставщиков....193
9.3.2. Ограничения при использовании сетей внешних поставщиков....194
9.3.3. Настройка подсетей в логических сетях внешних поставщиков....194
9.3.4. Добавление подсетей в логических сетях внешних поставщиков....195
9.3.5. Удаление подсетей из логических сетей внешних поставщиков....195

9.3.6. Присвоение групп безопасности логическим сетям и портам....195
9.4. Хосты и организация сетей....196
9.4.1. Обновление сведений о характеристиках хоста....196
9.4.2. Изменение параметров сетевых интерфейсов и присвоение хостам логических сетей 196
9.4.3. Синхронизация сетей хостов....200
9.4.4. Изменение параметров VLAN хоста....201
9.4.5. Добавление нескольких VLAN на один сетевой интерфейс с использованием логических сетей....202
9.4.6. Присвоение дополнительных адресов IPv4 сетям хостов....203
9.4.7. Добавление сетевых меток сетевым интерфейсам хоста....204
9.4.8. Изменение полного доменного имени хоста....209
9.4.9. Поддержка организации сетей с помощью IPv6....209
9.5. Объединение сетевых интерфейсов....209
9.5.1. Создание устройства сетевой связки вручную на Портале администрирования....210
9.5.2. Создание устройства сетевой связки автоматически с помощью службы меток LLDP 211
9.5.3. Режимы агрегирования....213
Глава 10. Хосты....215
10.1. Введение в понятие хостов....215
Общее описание хоста виртуализации....215
10.2. Гипервизоры ROSA Virtualization....215
Доступ к веб-интерфейсу хоста виртуализации....215
10.3. Задачи при работе с хостами....216
10.3.1. Добавление хостов в виртуализированный ЦУ....216
10.3.2. Общие параметры хоста....224
10.3.3. Параметры управления питанием хоста....226
10.3.4. Параметр приоритета SPM....229
10.3.5. Параметры вкладки «Консоль и GPU»....230
10.3.6. Параметр вкладки «Поставщик сети»....231
10.3.7. Параметры ядра....232
10.3.8. Параметр вкладки «Виртуализированный ЦУ»....234
10.3.9. Настройка параметров управления питанием хоста....235
10.3.10. Настройка параметра приоритета SPM хоста....236
10.3.11. Настройка на хосте сквозного доступа к PCI....236
10.3.12. Перевод хоста в режим обслуживания....238
10.3.13. Активация хоста из режима обслуживания....240
10.3.14. Настройка правил межсетевого экрана хоста....240
10.3.15. Удаление хоста....241
10.3.16. Повторная установка хостов....241

10.3.17. Индивидуализация хостов с помощью меток....242
10.3.18. Просмотр статуса работоспособности хоста....242
10.3.19. Просмотр устройств хоста....242
10.3.20. Доступ к веб-интерфейсу Cockpit с Портала администрирования....243
10.4. Отказоустойчивость хостов....243
10.4.1. Высокая доступность хостов....243
10.4.2. Управление питанием с помощью прокси....244
10.4.3. Настройка параметров операции блокады на хосте....244
10.4.4. Служба Kdump и параметры fence_kdump....245
10.4.5. Мягкая блокада хостов....249
10.4.6. Использование возможностей хоста по управлению питанием....250
10.4.7. Ручное изолирование не отвечающего хоста....251
Глава 11. Хранилища....253
11.1. Домен хранилища....254
11.2. Подготовка и добавление хранилища NFS....255
11.2.1. Подготовка хранилища NFS....255
11.2.2. Добавление хранилища NFS....255
11.2.3. Увеличение объёма хранилища NFS....257
11.3. Подготовка и добавление локального хранилища....258
11.3.1. Подготовка локального хранилища....258
11.3.2. Добавление локального хранилища....259
11.4. Управление хранилищами на базе файловой системы, совместимой с POSIX....259
11.4.1. Подготовка хранилища на базе файловой системы, совместимой с POSIX....259
11.4.2. Добавление хранилища на базе файловой системы, совместимой с POSIX....260
11.5. Подготовка и добавление блочного хранилища....261
11.5.1. Подготовка хранилища iSCSI....261
11.5.2. Добавление хранилища iSCSI....262
11.5.3. Настройка доступа к iSCSI по нескольким путям....267
11.5.4. Миграция логической сети в связку iSCSI....268
11.5.5. Подготовка хранилища FCP....269
11.5.6. Добавление хранилища FCP....270
11.5.7. Увеличение размера хранилища iSCSI или FCP....271
11.5.8. Повторное использование LUN....272
11.6. Подготовка и добавление хранилища Gluster....272
11.7. Импорт существующих доменов хранилищ....272
11.7.1. Обзор процесса импорта существующих доменов хранилищ....272
11.7.2. Импорт доменов хранилищ....274
11.7.3. Миграция доменов хранилищ между дата-центрами в одном окружении....275
11.7.4. Миграция доменов хранилищ между дата-центрами в разных окружениях....275

11.7.5. Импорт виртуальных машин из импортированных доменов данных....276
11.7.6. Импорт шаблонов из импортированных доменов данных....277

11.8. Работа с доменами хранилищ....278

11.8.1. Размещение образов в доменах данных....278
11.8.2. Перевод доменов хранилищ в режим обслуживания....281
11.8.3. Изменение параметров доменов хранилищ....282
11.8.4. Обновление файлов OVF....283
11.8.5. Активация доменов хранилищ из режима обслуживания....283
11.8.6. Отсоединение домена хранения от дата-центра....283
11.8.7. Присоединение домена хранения к дата-центру....283
11.8.8. Удаление домена хранения....284
11.8.9. Разрушение домена хранения....284
11.8.10. Создание профилей дисков....284
11.8.11. Удаление профилей дисков....285
11.8.12. Просмотр состояния работоспособности доменов хранилищ....285
11.8.13. Параметр «Освободить блоки перед удалением»....285

Глава 12. Пулы....287

12.1. Пул виртуальных машин....287

12.1.1. Инфраструктура виртуальных рабочих столов (VDI)....287

12.2. Создание пула виртуальных машин (VDI)....288
12.3. Параметры и элементы управления пулами....294

12.3.1. Общие параметры в окнах «Новый пул» и «Параметры пула»....294
12.3.2. Параметры вкладки «Тип» в окнах «Новый пул» и «Изменить пул»....294
12.3.3. Параметры вкладки «Консоль» в окнах «Новый пул» и «Изменить пул»....295
12.3.4. Параметры вкладки «Хост» в окнах «Новый пул» и «Параметры пула»....295
12.3.5. Параметры вкладки «Выделение ресурсов»....298

12.4. Изменение параметров пула виртуальных машин....299
12.5. Предварительный запуск виртуальных машин в пуле....299
12.6. Добавление виртуальных машин в пул ВМ....300
12.7. Открепление виртуальных машин от пула ВМ....301
12.8. Удаление пула виртуальных машин....301

Глава 13. Виртуальные диски....303

13.1. Хранилище виртуальной машины....303
13.2. Виртуальные диски....303
13.3. Очистка после удаления для виртуальных дисков....305
13.4. Разделяемые диски....307
13.5. Диски с доступом только для чтения....307
13.6. Работа с виртуальными дисками....307

13.6.1. Создание виртуального диска....307
13.6.2. Параметры виртуального диска....309

13.6.3. Обзор процесса динамической миграции между хранилищами....315
13.6.4. Перемещение виртуальных дисков....316
13.6.5. Изменение типа интерфейса диска....316
13.6.6. Копирование виртуальных дисков....317
13.6.7. Шифрование виртуальных дисков....318
13.6.8. Отправка образов в домен хранения данных....322
13.6.9. Импорт образов дисков из импортированного домена хранения....322
13.6.10. Импорт незарегистрированного образа диска из импортированного домена хранения....322
13.6.11. Импорт виртуальных дисков из службы образов OpenStack....323
13.6.12. Экспорт виртуальных дисков в службу образов OpenStack....323
13.6.13. Возвращение хосту дискового пространства, ранее используемого виртуальными дисками....324

Часть III. Администрирование окружения....325
Глава 14. Администрирование виртуализированного ЦУ....325

14.1. Обслуживание виртуализированного ЦУ....325

14.1.1. Режимы обслуживания виртуализированного ЦУ....325
14.1.2. Администрирование СУСВ....328
14.1.3. Настройка резервирования слотов памяти для виртуализированного ЦУ на дополнительных хостах....330
14.1.4. Добавление узлов виртуализированного ЦУ для СУСВ....331
14.1.5. Перенастройка существующего хоста в качестве узла виртуализированного ЦУ...332
14.1.6. Загрузка СУСВ в режиме восстановления....332
14.1.7. Удаление хоста из окружения виртуализированного ЦУ....333
14.1.8. Изменение полного доменного имени СУСВ в виртуализированном ЦУ....334

14.2. Резервные копии и миграция....334

14.2.1. Обзор: создание резервных копий СУСВ....334
14.2.2. Миграция хранилища данных на отдельную машину....357
14.2.3. Создание и восстановление ВМ из резервных копий с использованием домена хранения резервных копий....361

14.3. Обновление сертификатов до истечения срока их действия....364

Последовательность действий по обновлению сертификатов:....364

14.4. Автоматизация задач конфигурирования с помощью Ansible....365
14.5. Пользователи и роли....365

14.5.1. Что такое пользователи....365
14.5.2. Введение в серверы каталогов....365
14.5.3. Настройка внешнего поставщика LDAP....366
14.5.4. Настройка единого входа для LDAP и Kerberos....378
14.5.5. Авторизация пользователей....383
14.5.6. Администрирование задач пользователей на Портале администрирования....384
14.5.7. Администрирование задач пользователей в консольном режиме....386

14.5.8. Настройка дополнительных локальных доменов....392
14.6. Квоты и политика соглашения об уровне обслуживания....392
14.6.1. Что такое Quota....392
14.6.2. Общие и индивидуальные квоты....393
14.6.3. Расчёт квот....394
14.6.4. Включение и изменение режима квот в дата-центре....394
14.6.5. Создание новых политик квотирования....395
14.6.6. Объяснение параметров порога квоты....396
14.6.7. Присвоение квот объектам....396
14.6.8. Использование квот для ограничения потребления ресурсов пользователем....397
14.6.9. Редактирование квот....398
14.6.10. Удаление квот....398
14.6.11. Принудительное применение политики соглашения об уровне обслуживания....398
14.7. Уведомления о событиях....398
14.7.1. Настройка уведомлений о событиях на Портале администрирования....398
14.7.2. Отмена уведомлений о событиях на Портале администрирования....400
14.7.3. Параметры уведомлений о событиях в файле ovirt-engine-notifier.conf....401
14.7.4. Настройка отправки ловушек SNMP из диспетчера ROSA Virtualization....406
14.8. Служебные программы....409
14.8.1. Утилита oVirt Engine Rename....410
14.8.2. Утилита Engine Configuration....413
14.8.3. Утилита Log Collector....414
14.8.4. Утилита Engine Vacuum....418
14.8.5. Утилита отображения имён VDSM на имена сетей....419
Глава 15. Сбор сведений об окружении....420
15.1 Мониторинг и наблюдаемость....420
15.1.1. Мониторинг систем ROSA Virtualization с помощью хранилища данных и Grafana 420
15.1.2. Отправка метрик и журналов на удалённый экземпляр Elasticsearch....424
15.2 Файлы журналов....426
15.2.1. Файлы журналов процесса установки диспетчера виртуализации....426
15.2.2. Файлы журналов диспетчера ROSA Virtualization....427
15.2.3. Файлы журналов SPICE....427
15.2.4. Файлы журналов хостов....429
15.2.5. Настройка отладочного уровня журналирования для служб ROSA Virtualization...430
15.2.6. Основные файлы конфигураций служб ROSA Virtualization....431
15.2.7. Настройка сервера журналирования хоста....431
15.2.8. Включение использования SyslogHandler для передачи журналов диспетчера ROSA Virtualization на удалённый сервер syslog....432
Часть IV. Дополнительные настройки....433

Глава 16. Настройка двухфакторной аутентификации....433

16.1. Двухфакторная аутентификация для SSH с использованием «Рутокен ЭЦП»....433

Настройка двухфакторной аутентификации для SSH....433
Подключение к SSH серверу с настроенной двухфакторной аутентификацией....435

16.2. Двухфакторная аутентификация для web-портала ROSA Virtualization 3.0....435
16.3. Двухфакторная аутентификация в локальной консоли с использованием «Рутокен ЭЦП»....444

Глава 17. Настройка vGPU....448

17.1. Настройка системных параметров хоста....448
17.2. Установка драйвера vGPU....450
17.3. Настройка драйвера vGPU для ВМ....451

Глава 18. Развёртывание подсистемы мониторинга и отчётности Grafana....453

Развёртывание Grafana....453

Приложение А. VDSM и перехватчики событий....454

A.1. VDSM....454
A.2. Перехватчики событий VDSM....454
A.3. Расширение VDSM с помощью перехватчиков событий....454
A.4. Поддерживаемые события VDSM....455
A.5. Окружение VDSM перехватчиков событий....458
A.6. Объект XML домена перехватчиков событий VDSM....458
A.7. Настройка свойств, указываемых пользователем....458

Настройка пользовательского свойства smartcard (свойство ВМ)....459
Настройка пользовательского свойства interface (свойство устройства)....459

A.8. Настраиваемые пользователем свойства ВМ....460
A.9. Оценка пользовательских свойств ВМ в перехватчике событий VDSM....461

Оценка настраиваемых пользователем свойств....461

A.10. Использование модуля перехватчиков событий VDSM....461
A.11. Выполнение перехватчиков событий VDSM....462

Настройка sudo для сценариев перехватчиков событий VDSM....462

A.12. Коды возврата перехватчиков событий VDSM....463
A.13. Примеры перехватчиков событий VDSM....463

Тонкая настройка узла NUMA....463

Приложение В. Свойства сетей, настраиваемые пользователем....466

B.1. Параметры bridge_opts....466
B.2. Настройка использования команды ethtool в виртуализированном ЦУ....469

Добавление ключа ethtool_opts в виртуализированный ЦУ....470

B.3. Настройка использования протокола FCoE в виртуализированном ЦУ....470

Добавление ключа FCoE в виртуализированный ЦУ....470

Приложение C. Модули пользовательского интерфейса....472

C.1. Модули пользовательского интерфейса....472
C.2. Жизненный цикл модуля пользовательского интерфейса....472

C.2.1. Этапы жизненного цикла модуля пользовательского интерфейса....472
C.2.2. Обнаружение модуля пользовательского интерфейса....472
C.2.3. Загрузка модуля пользовательского интерфейса....473
C.2.4. Самонастройка модуля пользовательского интерфейса....473

C.3. Файлы модуля пользовательского интерфейса....474
C.4. Пример развёртывания модуля пользовательского интерфейса....475

Развёртывание модуля Hello World!....475

Приложение D. Система виртуализации и шифрование связи....476

D.1. Замена сертификата ЦС виртуализированного ЦУ....476

Извлечение сертификата и закрытого ключа из файла с расширением *.p12....476
Замена сертификата ЦС виртуализированного ЦУ для Apache....477

D.2. Настройка шифрованного соединения между виртуализированным ЦУ и сервером LDAP....479

Создание сертификата ЦС в кодировке PEM....479

D.3. Настройка шифрования соединений VDSM вручную....480

Настройка шифрования соединений VDSM вручную....480

Приложение E. Прокси....482

E.1. Прокси-сервер SPICE....482

E.1.1. Обзор SPICE Proxy....482
E.1.2. Настройка машины SPICE Proxy....482
E.1.3. Включение SPICE Proxy....483
E.1.4. Выключение SPICE Proxy....483

E.2. Прокси-сервер Squid....484

E.2.1. Установка и настройка Squid....484

E.3. Прокси-сервер WebSocket....485

E.3.1. Обзор прокси-сервера WebSocket....485
E.3.2. Миграция WebSocket на отдельную машину....486

Приложение F. Системные учётные записи....489

F.1. Системные записи пользователей виртуализированного ЦУ....489
F.2. Группы виртуализированного ЦУ....489
F.3. Системные записи пользователей хостов виртуализации....489
F.4. Группы хостов виртуализации....489

Перечень сокращений....491

Введение

В данном руководстве содержатся сведения и инструкции для системных администраторов, осуществляющих развертывание, сопровождение и контроль функционирования программного средства «Программная система управления средой виртуализации с подсистемой безагентного резервного копирования виртуальных машин «ROSA Virtualization 3.0»» РСЮК.10102-01 (далее – ROSA Virtualization).

ROSA Virtualization — платформа виртуализации с интегрированной системой управления, позволяющая развернуть виртуальный центр обработки данных (ВЦОД) корпоративного уровня в кратчайшие сроки. Система управления средой виртуализации (СУСВ), входящая в состав ROSA Virtualization, обладает русскоязычным графическим интерфейсом, с помощью которого осуществляется централизованное управление объектами виртуальной среды (гипервизоры, хранилища, кластеры, дата-центры, виртуальные машины и прочие).

Версия ROSA Virtualization, 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.

ROSA Virtualization 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 ROSA Virtualization от других аналогичных решений, например на базе OpenStack.

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

Часть I. Администрирование и обслуживание среды виртуализации

Наличие администратора является обязательным и необходимым условием функционирования платформы виртуализации ROSA Virtualization.

В обязанности администратора ROSA Virtualization входят следующие задачи:

- Управление физическими и виртуальными ресурсами, такими как хосты и виртуальные машины, в частности добавление хостов и обновление версий ПО на хостах, 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 путём выключения машин).
- Своевременное реагирование на изменяющиеся требования ВМ (например, обновление версии ОС или выделение большего объёма памяти).
- Управление изменёнными свойствами объектов с помощью тегов.
- Управление параметрами пользователей и настройка уровней полномочий.
- Диагностика и решение проблем конкретных пользователей или виртуальных машин с использованием общих функциональных возможностей платформы.
- Создание общих и частных отчётов.
- Обеспечение безопасности информации, в том числе с использованием специальных функциональных возможностей платформы.

Глава 1. Настройка глобальных ресурсов

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

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

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

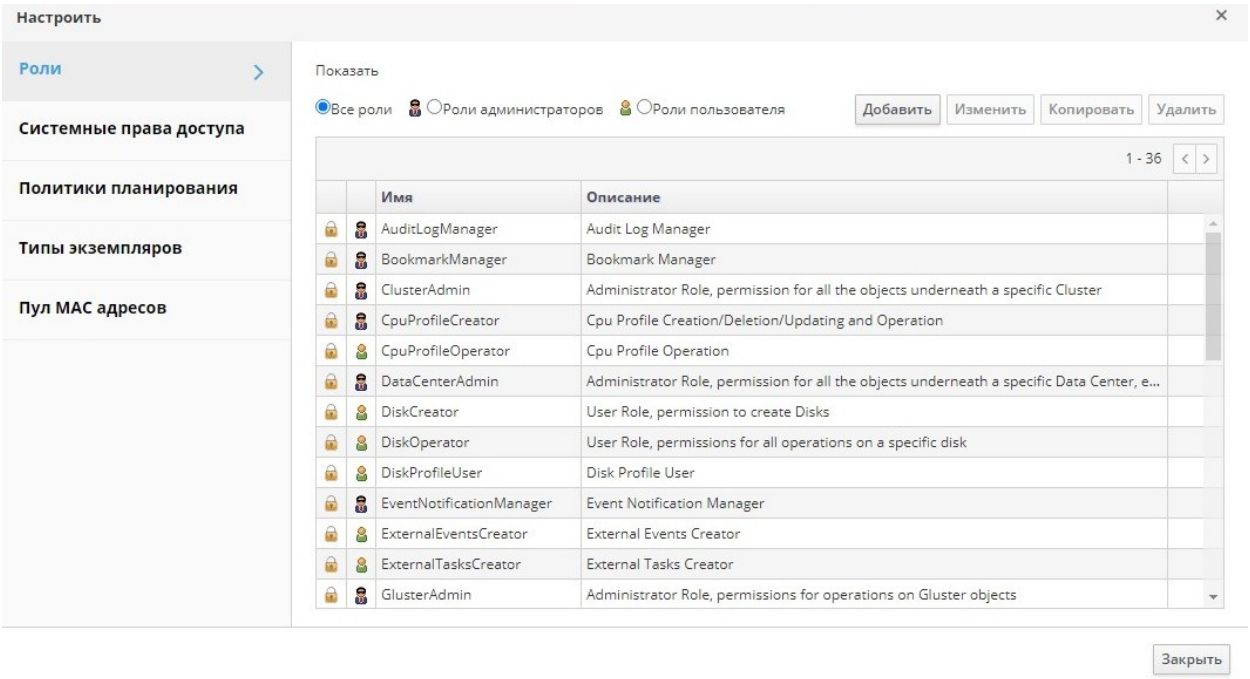

Рис. 1. Настройки системы — секция Роли

1.1. Роли

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

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

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

1.1.1. Добавление новой роли

Добавление роли в Портале администрирования

1. Нажмите **Администрирование → Настроить**, чтобы открыть окно **Настроить**. По умолчанию выбрана вкладка **Роли** (Рис. 1), где отображается список изначальных ролей **Пользователя** и **Администратора** (Рис. 2), а также все частные роли.

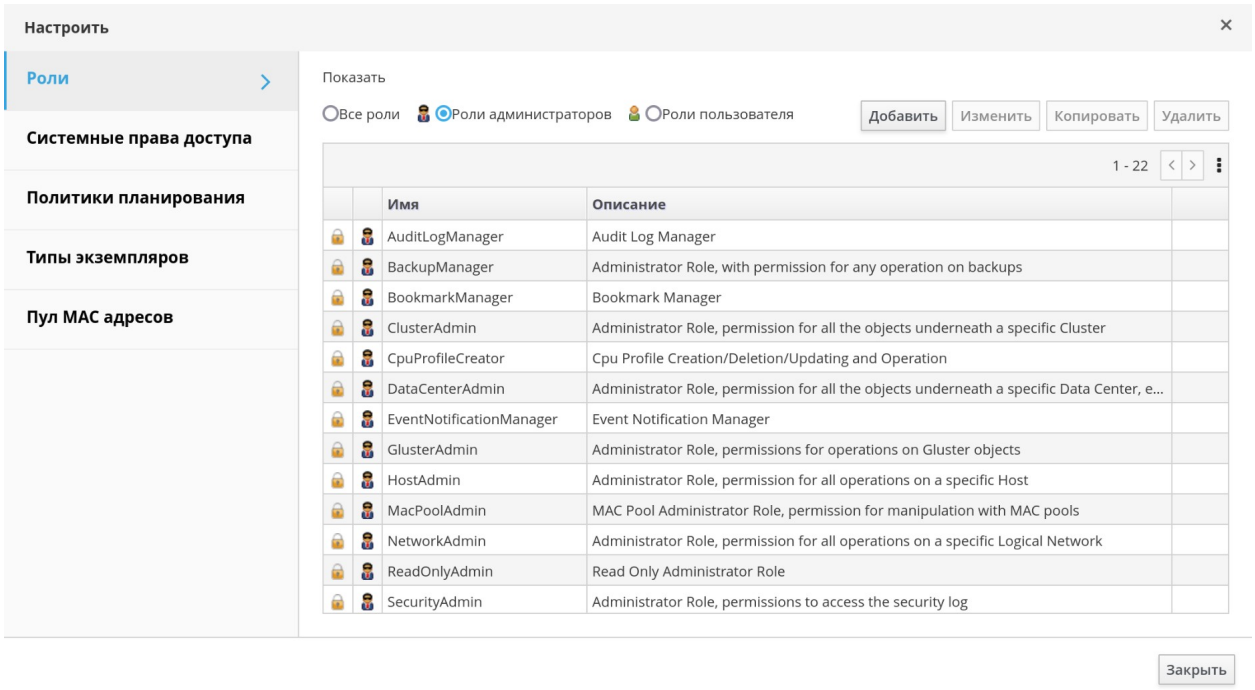

Рис. 2. Настройка ролей — Роли администратора

2. Нажмите **Добавить**.
3. Введите **Имя** и **Описание** новой роли (Рис. 3).

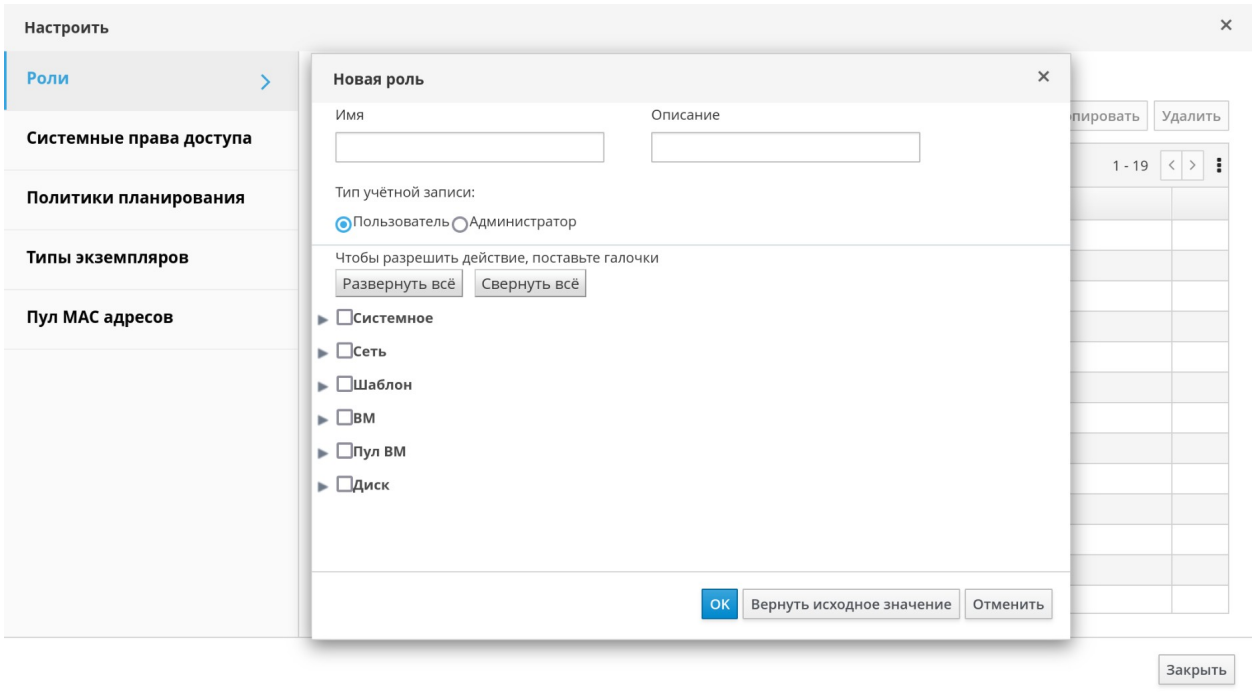

Рис. 3. Добавление новой роли

4. Для параметра **Тип учётной записи** выберите тип учёной записи — **Администратор** или **Пользователь**.
5. С помощью кнопок **Развернуть всё** (Рис. 4) или **Свернуть всё** можно увидеть соответственно больше или меньше подробностей для полномочий объектов, присутствующих в списке. Также можно развернуть или свернуть параметры для каждого объекта.

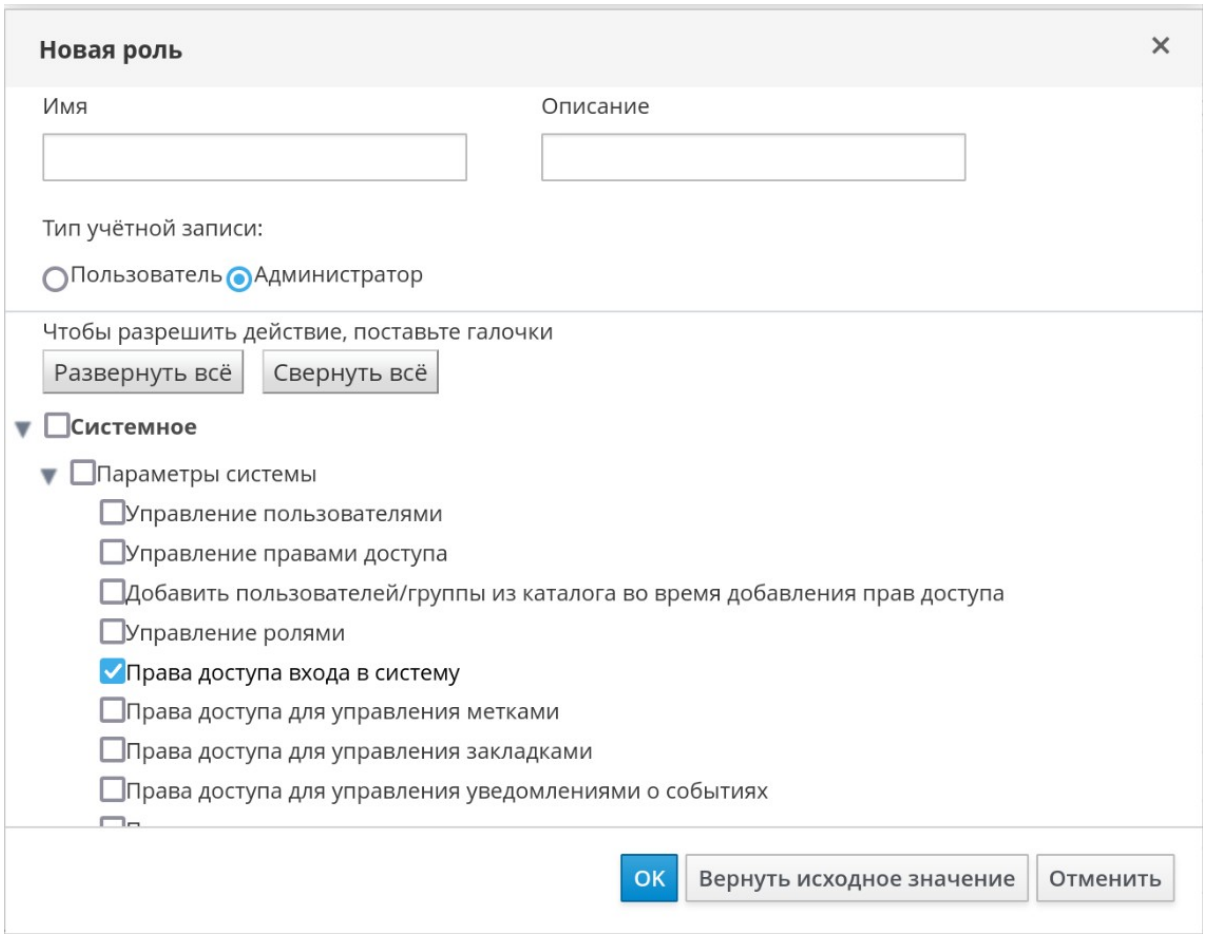

Рис. 4. Действия, доступные для настройки новой роли

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

1.1.2. Изменение параметров роли

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

Изменение или копирование роли

1. Нажмите **Администрирование → Настроить**, чтобы открыть окно **Настроить**. По умолчанию выбрана вкладка **Роли**, где отображается список изначальных ролей **Пользователя** и **Администратора**, а также все частные роли.
2. Выберите роль, которую нужно изменить (Рис. 5). Чтобы открыть окно **Параметры роли**, нажмите **Изменить**, или чтобы открыть окно **Копировать роль**, нажмите **Копировать**.

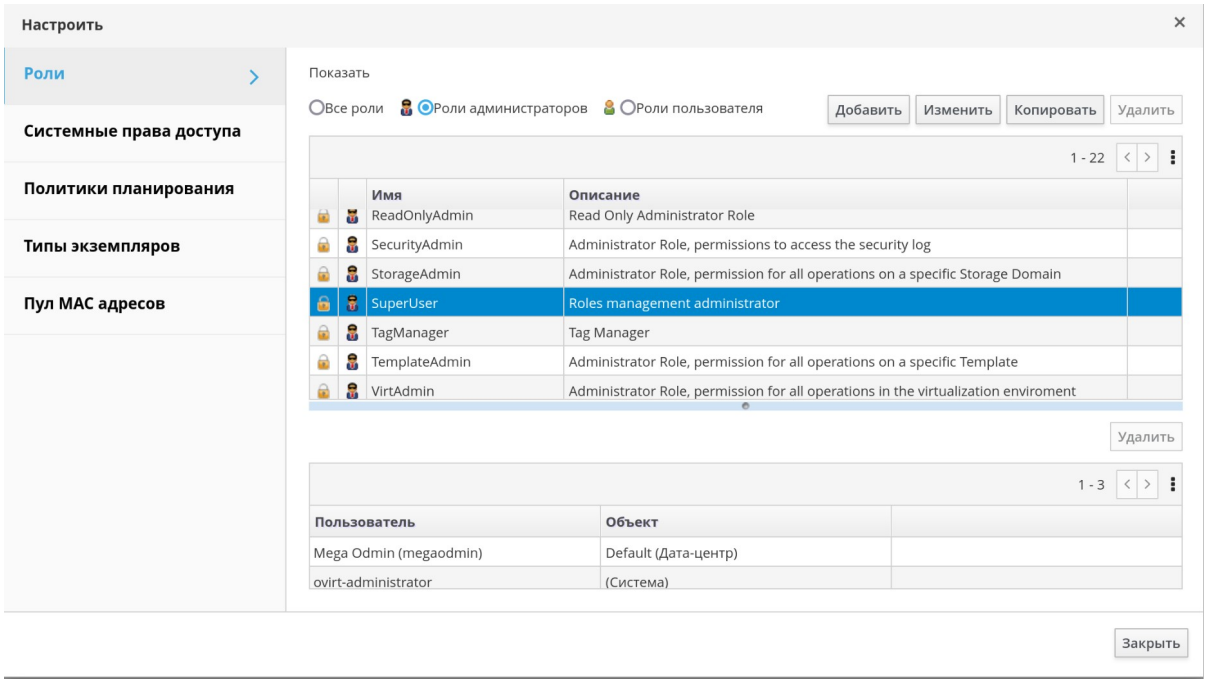

Рис. 5. Выбрана роль SuperUser — её можно скопировать для внесения изменений

3. При необходимости измените **Имя** и **Описание** роли (Рис. 6).

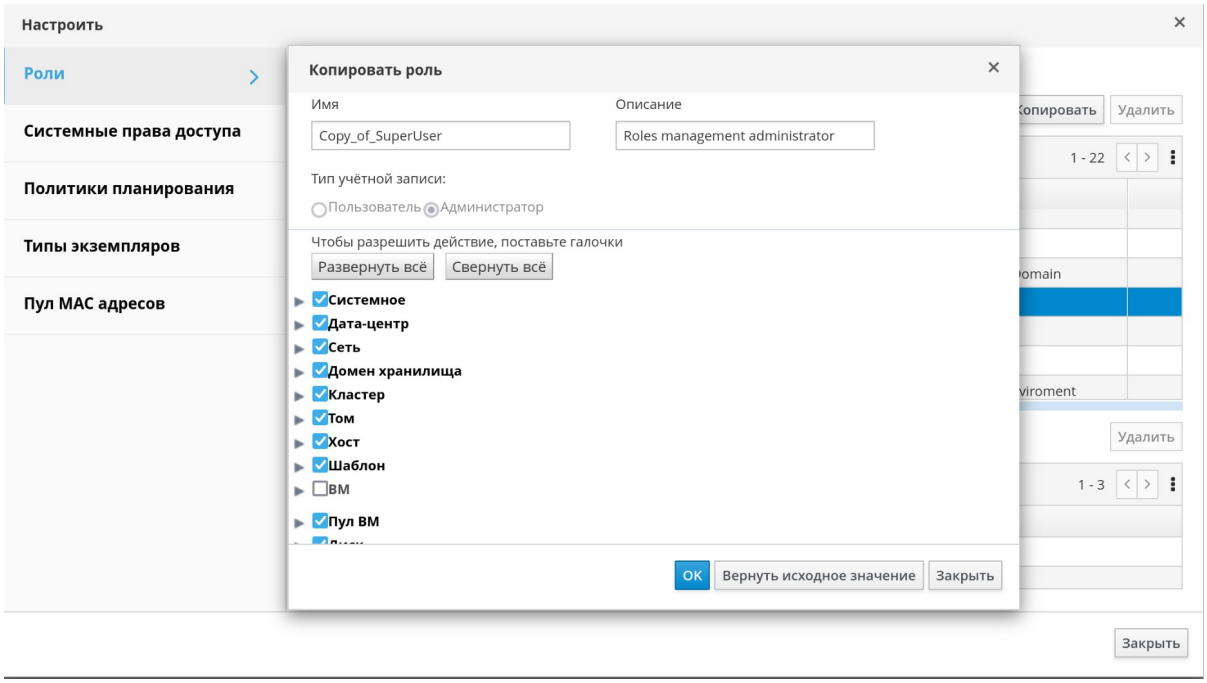

Рис. 6. Изменение скопированной роли SuperUser

4. С помощью кнопок **Развернуть всё** или **Свернуть всё** можно увидеть соответственно больше или меньше подробностей для полномочий объектов, присутствующих в списке. Также можно развернуть или свернуть параметры для каждого объекта.
5. Для каждого объекта установите или снимите соответствующие флажки для действий, которые нужно разрешить или запретить в настраиваемой роли (Рис. 7).

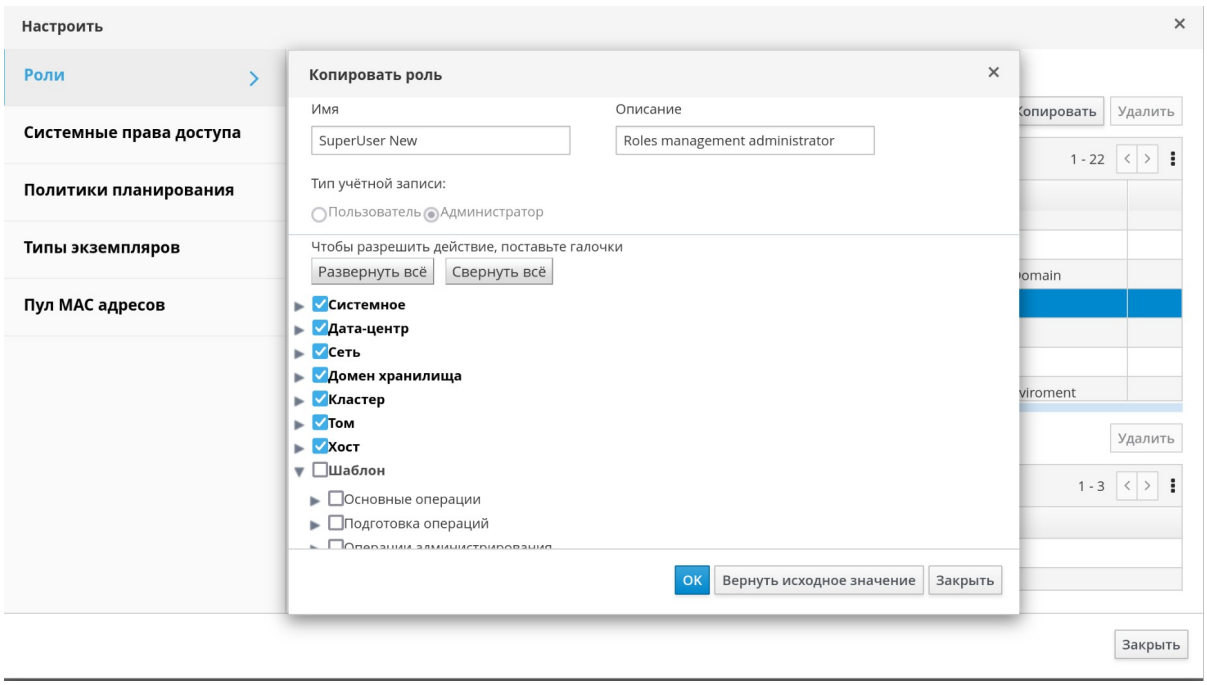

Рис. 7. Настройка полномочий по выполняемым действиям для скопированной роли

6. Для применения внесённых изменений нажмите **OK**. Добавленная роль отобразится в списке ролей для настройки (Рис. 8).

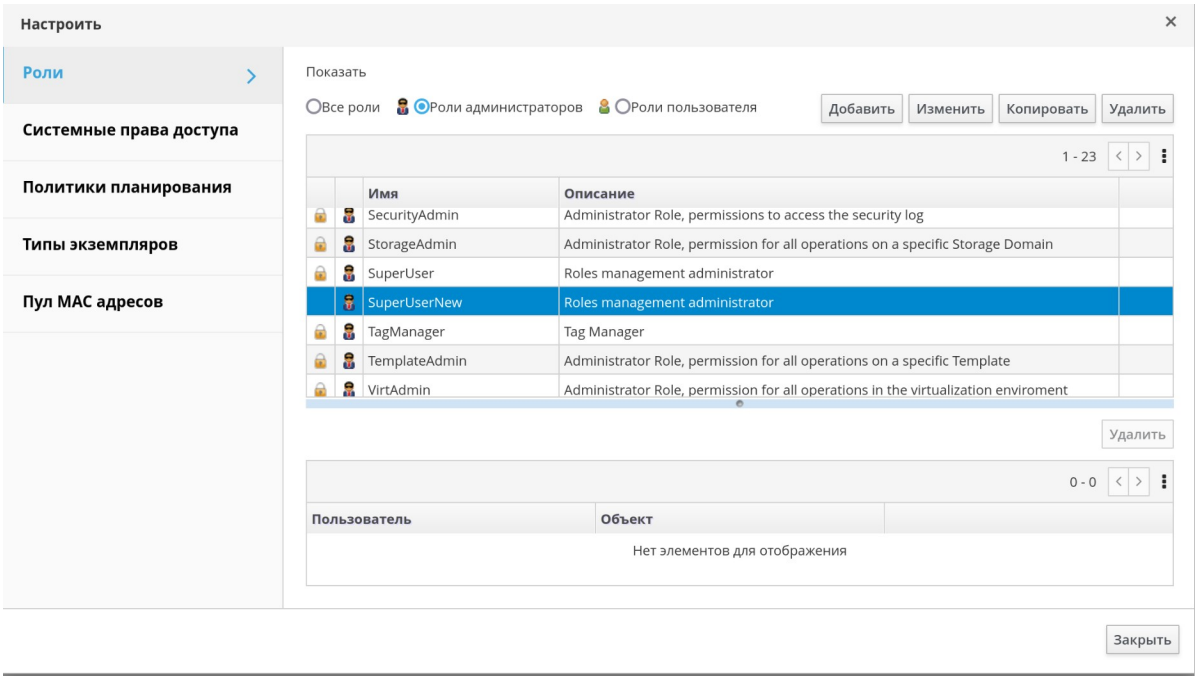

Рис. 8. Список ролей, с добавленной ролью SuperUserNew

1.1.3. Роль «Пользователь» и примеры авторизации

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

Пример 1.1. Полномочия для кластера

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

Пример 1.2. Полномочия PowerUser на ВМ

Иван — программист в отделе бухгалтерии. Для сборки и тестирования своих программ он использует виртуальные машины. Светлана создала для него виртуальный рабочий стол с названием `ivandesktop`. На ВМ со столом `ivandesktop` Ивану присвоена роль **UserVmManager**, дающая ему доступ с Портала виртуальных машин к этой

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

Пример 1.3. Полномочия роли PowerUser дата-центра

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

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

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

Пример 1.4. Полномочия сетевого администратора

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

Пример 1.5. Полномочия частной роли

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

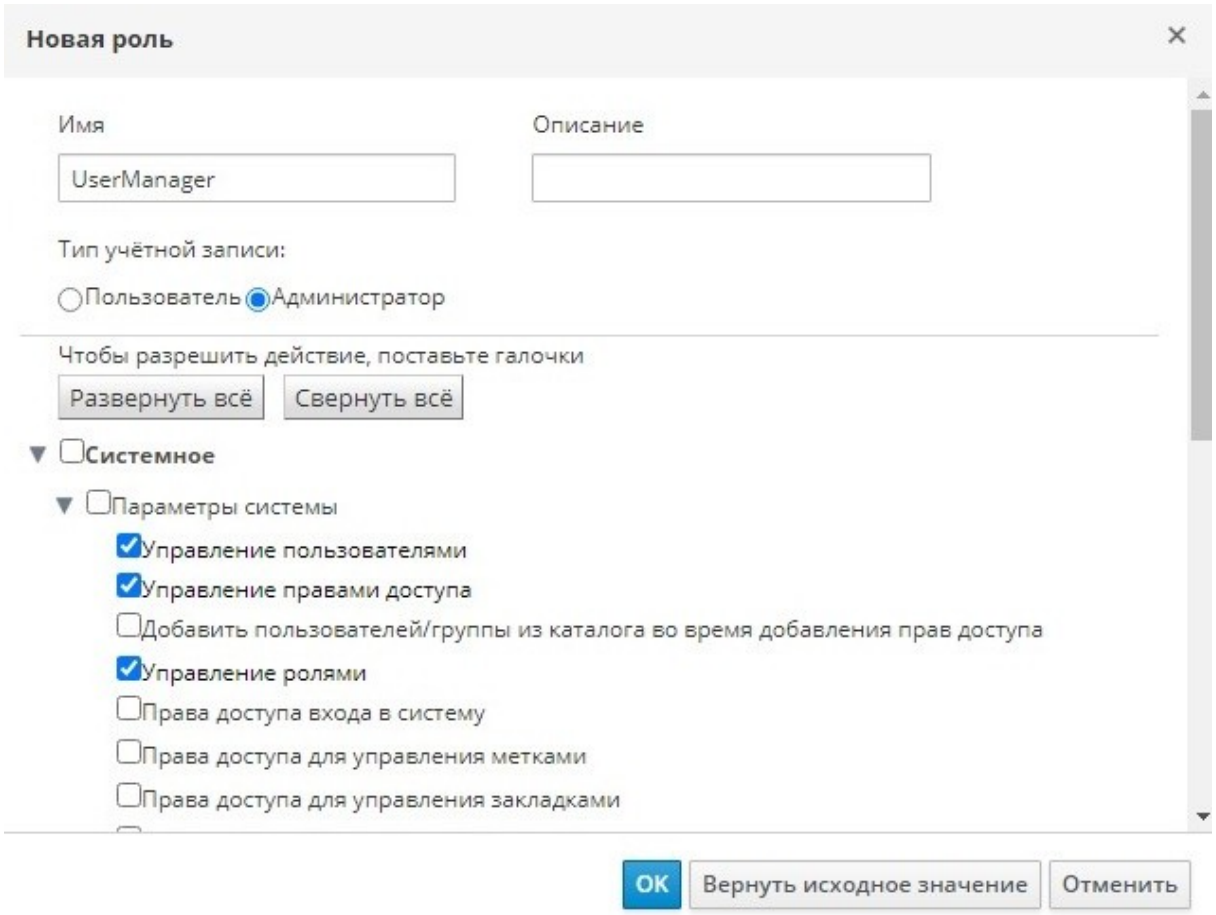

Рис. 9. Частная роль UserManager

Частная роль **UserManager** (Рис. 9) разрешает управление пользователями, полномочиями и ролями. Эти действия собраны в разделе **Система**, являющимся самым верхним объектом иерархии, показанной на Рис. 11: Полномочия и роли, что означает, что эти действия применимы ко всем другим объектам в системе. **Тип учётной записи**, указанной для этой роли — **Администратор**, а это означает, что после присвоения этой роли, Раиса сможет использовать как Портал администрирования, так и Портал ВМ.

Рис. 10: Иерархия объектов системы виртуализации

1.2. Системные полномочия

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

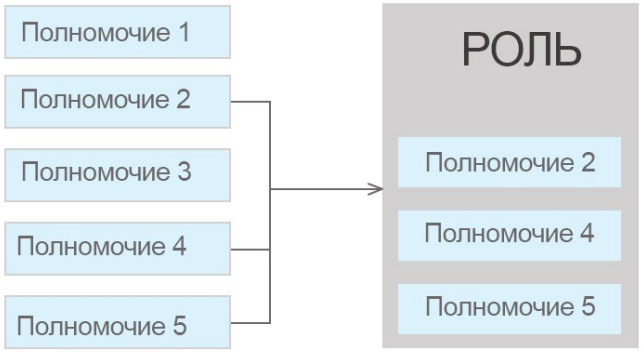

Рис. 11: Полномочия и роли

1.2.1. Свойства пользователя

Роли и полномочия являются свойствами пользователя. Роли — это предварительно настроенные наборы привилегий, предоставляющих доступ к разным уровням физических и виртуальных ресурсов. Многоуровневое администрирование предоставляет тонко настроенную иерархию полномочий. У администратора дата-центра, например, есть полномочия на управление всеми объектами в дата-центре, в то время как у администратора хоста есть полномочия на управление одним физическим хостом. Один

пользователь может иметь полномочия на использование одной ВМ и не иметь полномочий на внесение изменений в параметры ВМ, в то время как у другого пользователя могут присутствовать системные полномочия на ВМ.

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

В системе виртуализации ROSA Virtualization поддерживаются следующие типы ролей:

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

1.2.2. Роли и привилегии пользователей

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

Табл. 1.1. Базовые роли пользователей в системе виртуализации

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

Роль	Привилегии	Примечания
	администратор виртуальной машины	администрировать ВМ, а также создавать и использовать снимки. Пользователю, создавшему машину на Портале ВМ, автоматически присваивается роль UserVmManager на этой ВМ

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

Табл.1.2. Продвинутые роли пользователей в системе виртуализации

Роль	**Привилегии**	**Примечания**
UserTemplateBasedVm	Привилегии, ограниченные только использованием шаблонов	Пользователь может использовать шаблоны для создания виртуальных машин
DiskOperator	Пользователь виртуального диска	Пользователь может использовать, просматривать и изменять виртуальные диски. Пользователь наследует полномочия на использование ВМ, к которой присоединён виртуальный диск
VmCreator	Пользователь может создавать виртуальные машины на Портале ВМ	Эта роль не применяется к конкретной ВМ. Присваивайте эту роль пользователю в масштабах всего окружения в окне **Параметры**, или присваивайте эту роль в конкретных дата-центрах / кластерах. При присвоении этой роли в кластерах, также нужно присваивать роль DiskCreator в масштабах всего дата-центра или конкретных доменов хранилищ
TemplateCreator	Пользователь может создавать, редактировать и удалять шаблоны ВМ в рамках присвоенных ресурсов	Эта роль не присваивается к конкретному шаблону. Присваивайте эту роль пользователю в масштабах всего окружения в окне **Параметры,** или присваивайте эту роль в конкретных дата-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. Присваивайте эту роль пользователю в масштабах всего окружения в окне **Параметры**, или присваивайте эту роль в конкретных дата-центрах, кластерах или доменах хранилищ
TemplateOwner	Пользователь может изменять и удалять шаблоны, присваивать и управлять полномочиями пользователей на шаблон	Эта роль автоматически присваивается пользователю, создающему шаблон. Другие пользователи, не имеющие полномочий TemplateOwner для шаблона, не могут просматривать или использовать этот шаблон
VnicProfileUser	Пользователь логических сетей и сетевых интерфейсов виртуальной машины и шаблона	Пользователь может присоединять или отсоединять сетевые интерфейсы конкретных логических сетей

1.2.3. Роли и привилегии администраторов

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

Табл. 1.3. Базовые роли администраторов в системе виртуализации

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

Роль	Привилегии	Примечания
DataCenterAdmin	Администратор дата-центра	Пользователь обладает административными полномочиями на все объекты в рамках конкретного дата-центра, за исключением хранилища

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

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

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

Табл. 1.4. Продвинутые роли администраторов в системе виртуализации

Роль	Привилегии	Примечания
TemplateAdmin	Администратор шаблона ВМ	Пользователь может создавать, удалять и настраивать домены хранилищ и сетевые параметры шаблонов, а также перемещать шаблоны между доменами
StorageAdmin	Администратор хранилища	Пользователь может создавать, удалять, настраивать и управлять присвоенным доменом хранилища
HostAdmin	Администратор хоста	Пользователь может присоединять, удалять, настраивать и управлять конкретным хостом
NetworkAdmin	Сетевой администратор	Пользователь может настраивать и управлять сетью конкретного дата-центра или кластера. Сетевой администратор дата-центра или кластера наследует сетевые полномочия на виртуальные пулы в рамках кластера

Роль	Привилегии	Примечания
VmAdmin	Администратор ВМ	Пользователь обладает административными полномочиями на все ВМ
VmDeveloper	Разработчик ВМ	Пользователь обладает привилегиями на создание и управление конфигурацией ВМ и шаблонов
VmPoolAdmin	Системный администратор виртуального пула	Пользователь может создавать, удалять и настраивать виртуальный пул, присваивать и удалять пользователей виртуального пула, а также выполнять базовые операции на ВМ в пуле
GlusterAdmin	Администратор хранилища Gluster	Пользователь может создавать, удалять, настраивать и управлять томами хранилища Gluster
VmImporterExporter	Администратор импорта и экспорта виртуальных машин	Пользователь может импортировать и экспортировать ВМ. Пользователь имеет возможность просматривать все ВМ и шаблоны, экспортированные другими пользователями
SecurityAdmin	Администратор безопасности	Пользователь имеет возможность просматривать журнал событий безопасности и формировать отчеты с данными из этого журнала

1.2.4. Присвоение ресурсу роли администратора или пользователя

Присвоение роли ресурсу

1. Найдите название нужного ресурса и нажмите на него, чтобы просмотреть детали (Рис. 12).

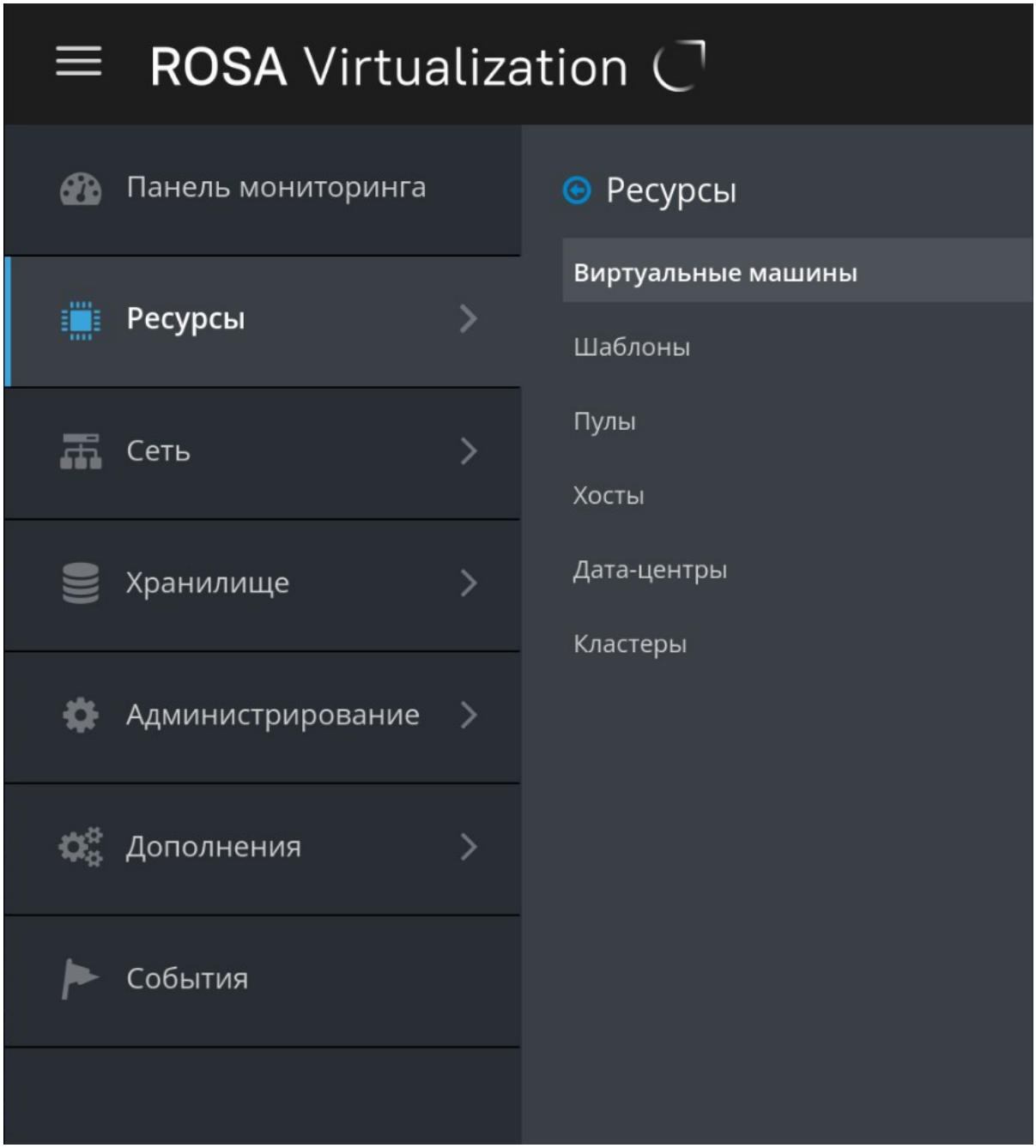

Рис. 12. Ресурсы ROSA Virtualization: Виртуальные машины, Шаблоны, Пулы, хосты, Дата-центры, Кластеры

В качестве примера рассмотрим выбор **Ресурсы → Виртуальные машины** (Рис. 13).

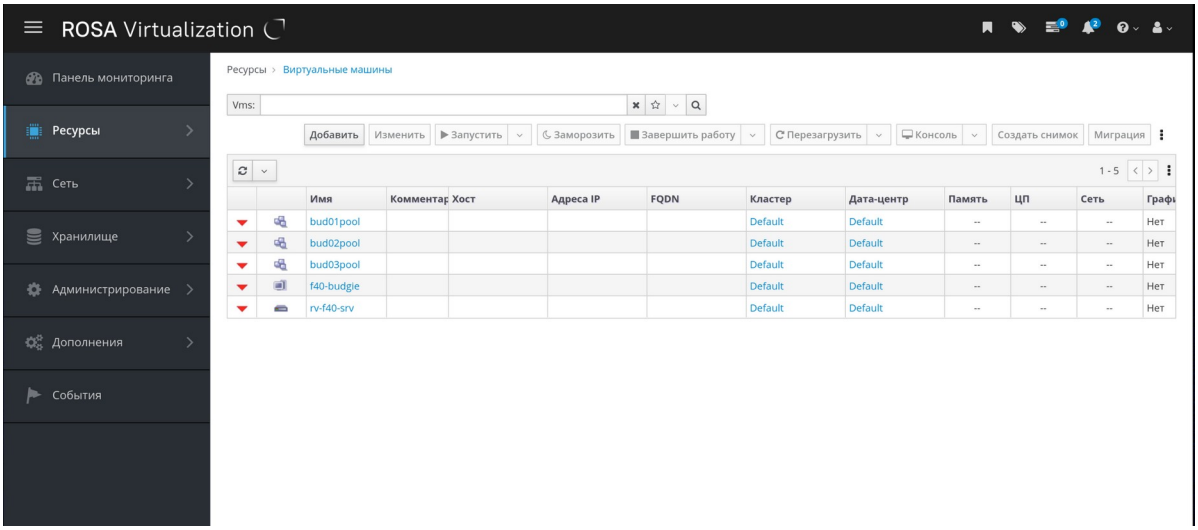

Рис. 13. Доступные ресурсы — Виртуальные машины

2. Перейдите на вкладку **Права доступа** (Рис. 14), чтобы указать присвоенных пользователей, роль пользователя и наследуемые полномочия для выбранного ресурса.

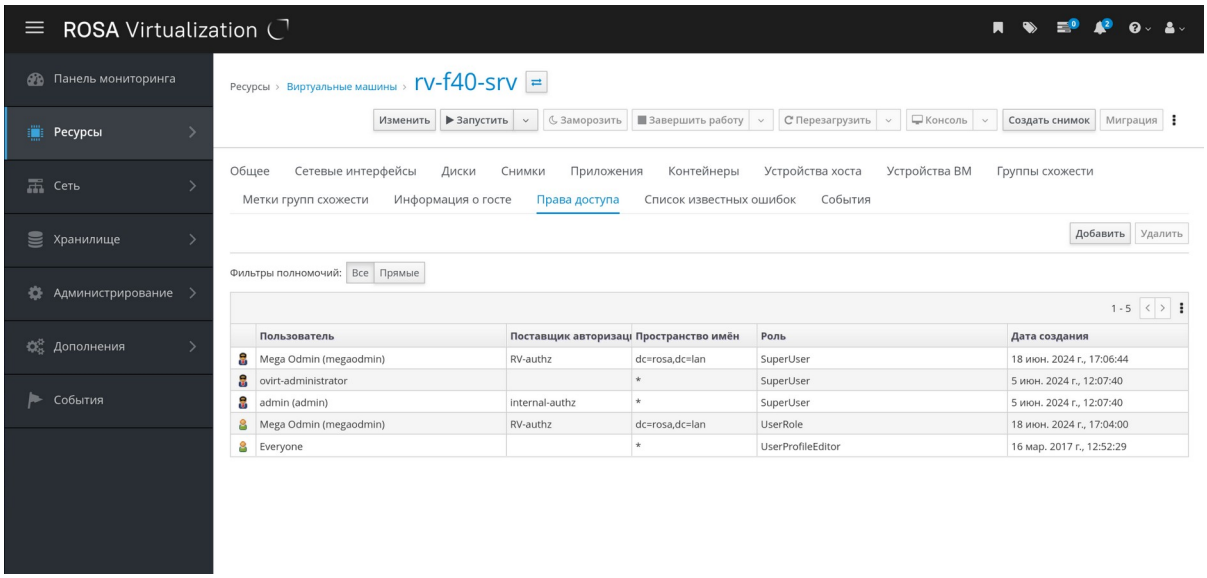

Рис. 14. Права доступа для выбранного ресурса (виртуальная машина)

3. Нажмите **Добавить**. Откроется форма для добавления пользователя и присвоения ему требуемых прав для данного ресурса.

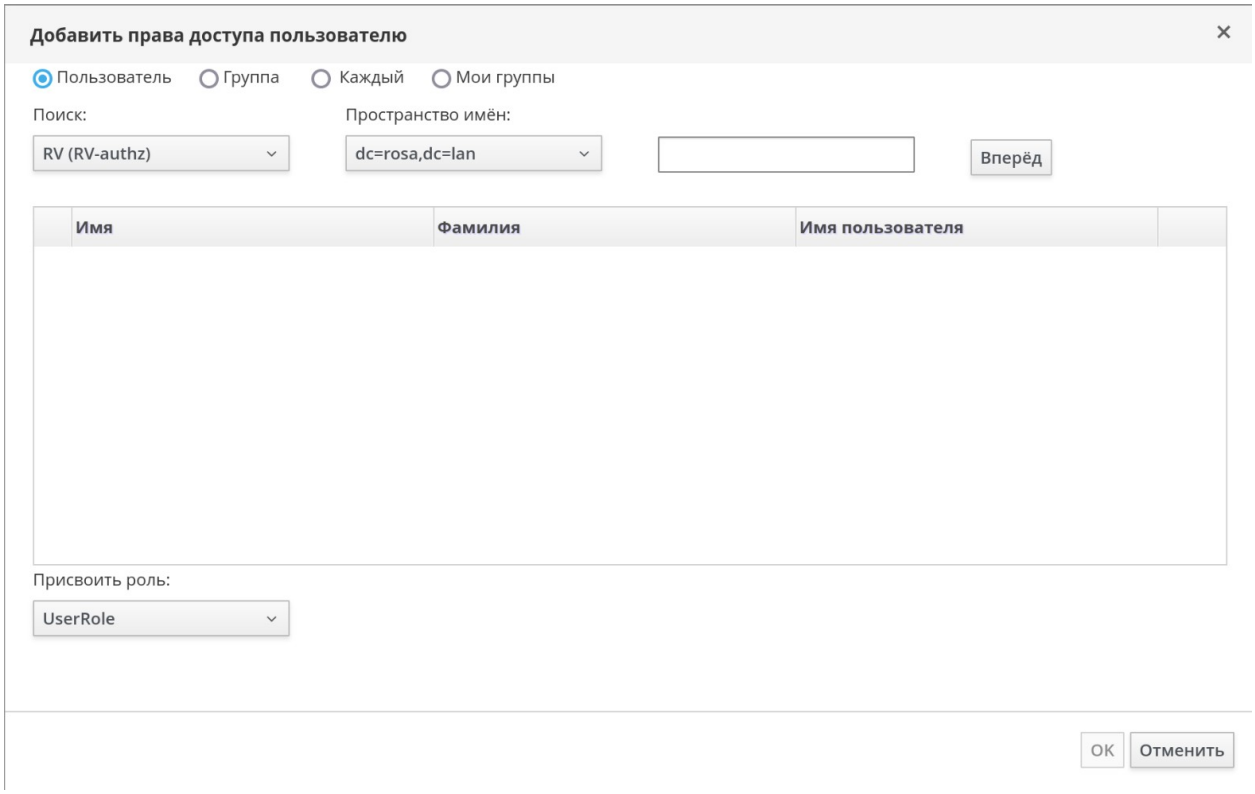

Рис. 15. Форма для добавления пользователя и присвоения ему требуемых прав

4. Укажите имя существующего пользователя в поле **Поиск** и нажмите **Вперёд**. Из полученного списка возможных совпадений выберите пользователя.

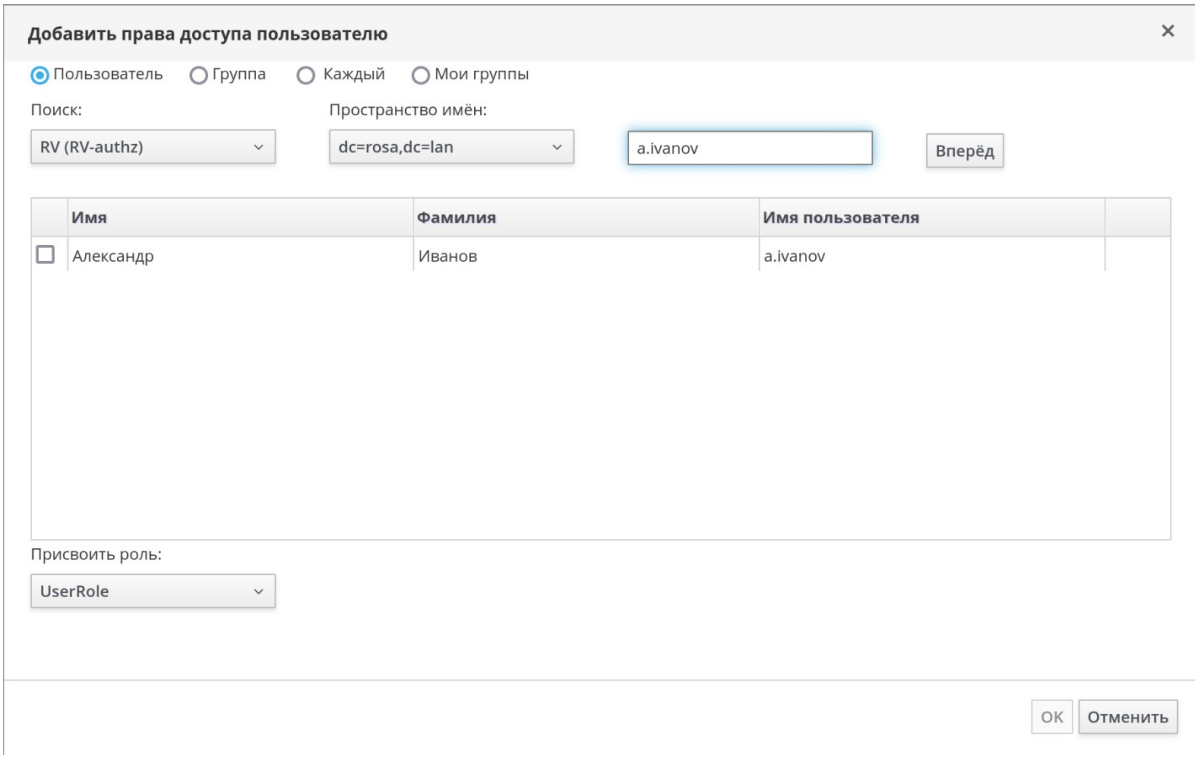

Рис. 16. Поиск пользователя

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

5. Из выпадающего списка **Присвоить роль** выберите нужную роль (Рис. 17).

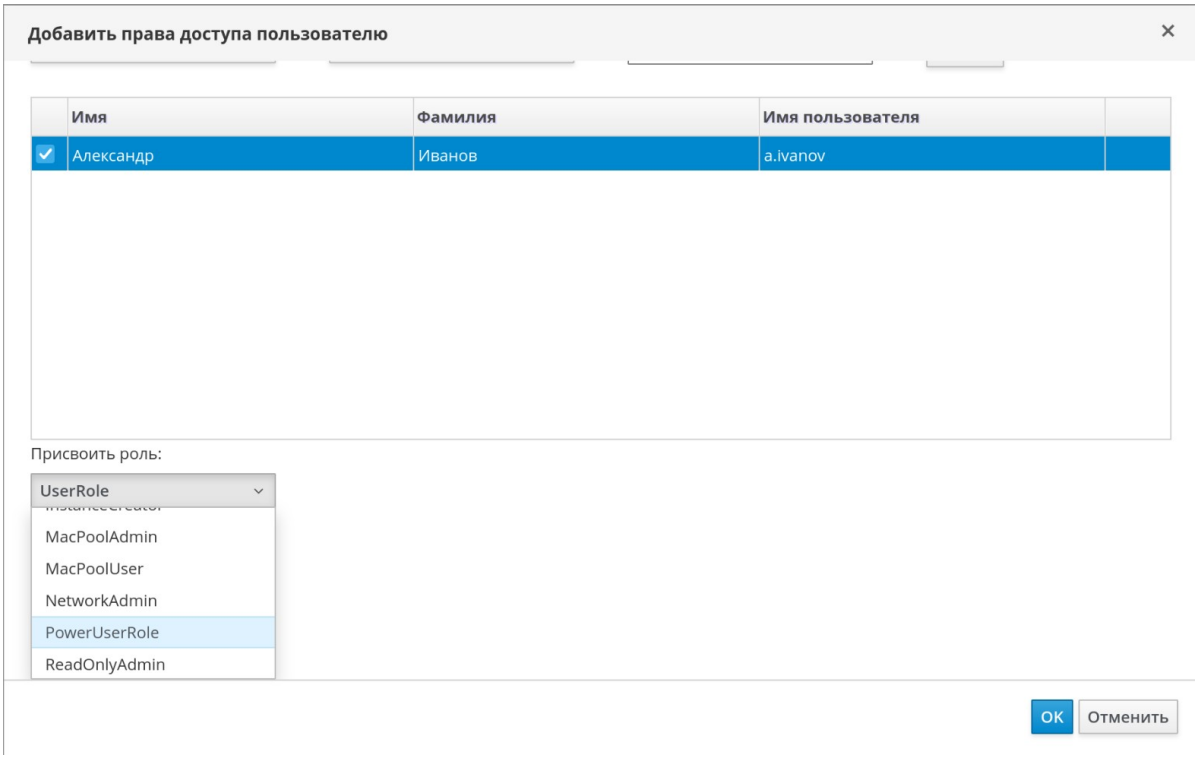

Рис. 17. Присвоение роли выбранному пользователю

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

6. Нажмите **OK**.

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

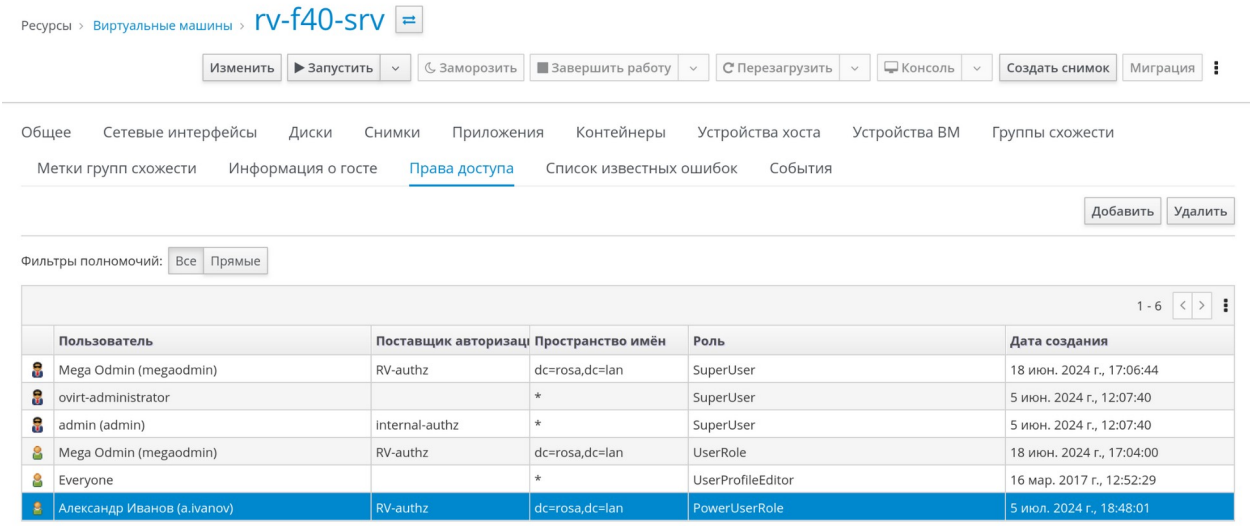

Рис. 18. Пользователь a.ivanov получил права (роль) PowerUserRole для выбранного ресурса

Примечание — присваивать роли и полномочия можно только существующим пользователям.

1.2.5. Удаление роли администратора или пользователя с ресурса

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

Удаление роли с ресурса

1. Найдите название нужного ресурса и нажмите на него, чтобы просмотреть детали.
2. Перейдите на вкладку **Права доступа**, чтобы указать присвоенных пользователей, роль пользователя и наследуемые полномочия для выбранного ресурса.
3. Выберите пользователя, права которого необходимо удалить с данного ресурса (см. пример Рис. 18).
4. Нажмите кнопку **Удалить** (Рис. 19).

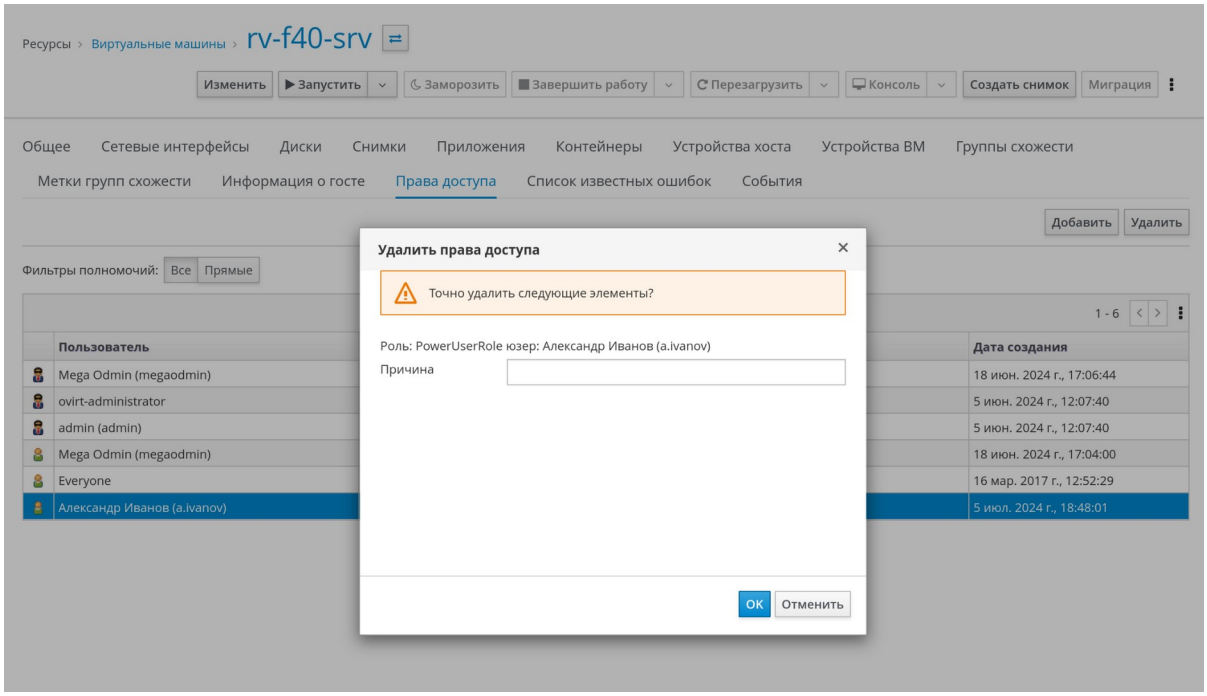

Рис. 19. Удаление прав доступа

5. Откроется форма **Удалить права доступа**. Нажмите **OK** для удаления прав доступа для данного пользователя/ресурса. Права доступа для данного пользователя/ресурса будут удалены (Рис. 20).

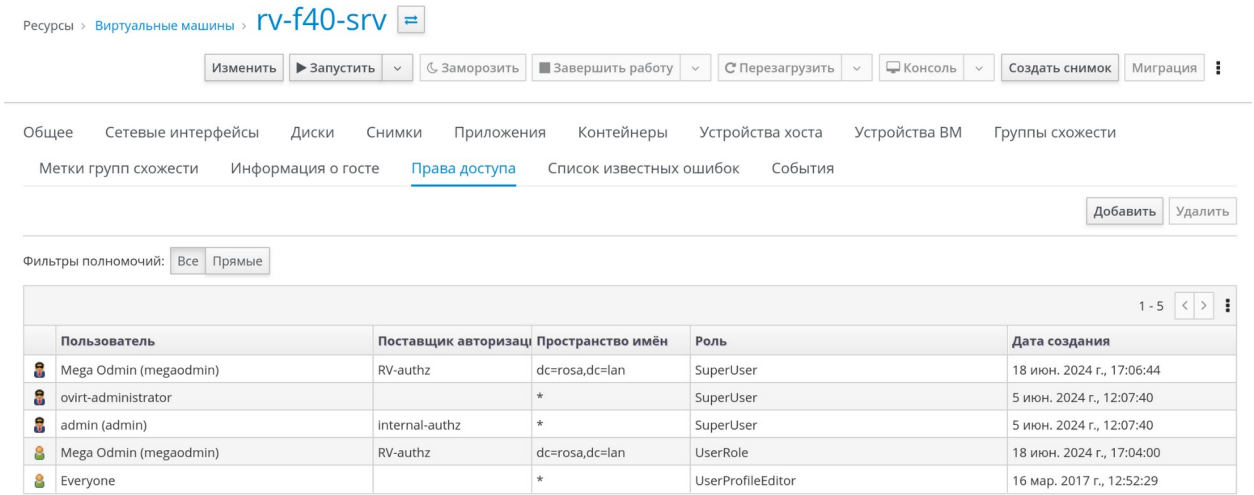

Рис. 20. Права пользователя a.ivanov к данному ресурсу были удалены

1.2.6. Управление системными полномочиями в дата-центре

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

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

Роль администратора дата-центра разрешает выполнять следующие действия:

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

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

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

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

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

1.2.7. Управление системными полномочиями в кластере

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

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

Роль администратора кластера разрешает выполнять следующие действия:

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

Для смены администратора кластера удалите существующего администратора и создайте нового.

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

Табл. 1.6. Административные роли с полномочиями в кластере

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

1.2.8. Управление сетевыми системными полномочиями

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

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

Роль сетевого администратора позволяет выполнять следующие действия:

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

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

Для смены администратора сети удалите существующего администратора и создайте нового.

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

Табл. 1.7. Роли сетевого администратора и сетевого пользователя

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

1.2.9. Управление системными полномочиями для хоста

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

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

Роль администратора хоста разрешает выполнять следующие действия:

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

Для смены администратора хоста удалите существующего администратора и создайте нового.

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

Табл.1.8. Административная роль с полномочиями на хосте

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

1.2.10. Управление системными полномочиями в домене хранилища

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

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

Роль администратора домена хранилища позволяет выполнять следующие действия:

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

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

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

Табл. 1.9. Административные роли с полномочиями в домене хранилища

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

1.2.11. Управление системными полномочиями на пул виртуальных машин

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

Роль администратора пула ВМ позволяет выполнять следующие действия:

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

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

Табл. 1.10. Административные роли с полномочиями в пуле

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

1.2.12. Управление системными полномочиями на виртуальные диски

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

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

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

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

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

Табл. 1.11. Административные роли с полномочиями на виртуальные диски

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

1.2.13. Настройка шифра для старых версий SPICE

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

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

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

Изменение строки шифра

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

Например:

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

2. Вставьте в файл следующее содержимое и сохраните файл:

```
        name:  oVirt - setup weaker SPICE encryption for old clients
        hosts: hostname
        vars:
          host_deploy_spice_cipher_string: 'DEFAULT:-RC4:-3DES:-DES'
        roles:
          - ovirt-host-deploy-spice-encryption
```

3. Запустите только что созданный файл Ansible playbook:

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

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

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

1.3. Политики планирования

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

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

Рис. 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, прикреплённые к хосту, не начнут работу, если этот хост достиг хотя бы одного из указанных значений для параметров **CpuOverCommitDurationMinutes**, **HighUtilization** или **MaxFreeMemoryForOverUtilized**.

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

Рис. 22. Политика планирования энергосбережения (Power Saving)

Политика планирования **Power_Saving** (Рис. 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,

прикреплённые к хосту, не начнут работу, если этот хост достиг указанного значения высокого коэффициента использования.

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

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

1.3.1. Создание политик планирования

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

Создание политики планирования

1. Нажмите **Администрирование → Настроить**.
2. Перейдите на вкладку **Политики планирования** (Рис. 23).

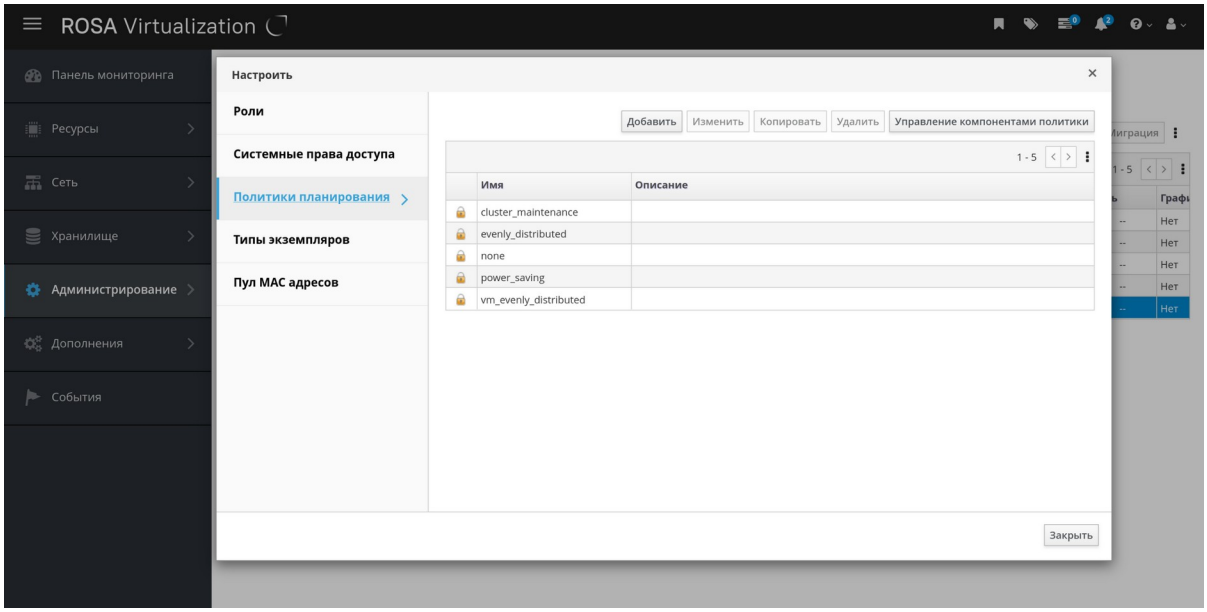

Рис. 23. Настройка политик планирования

3. Нажмите **Добавить** для создания новой политики планирования (Рис. 24).

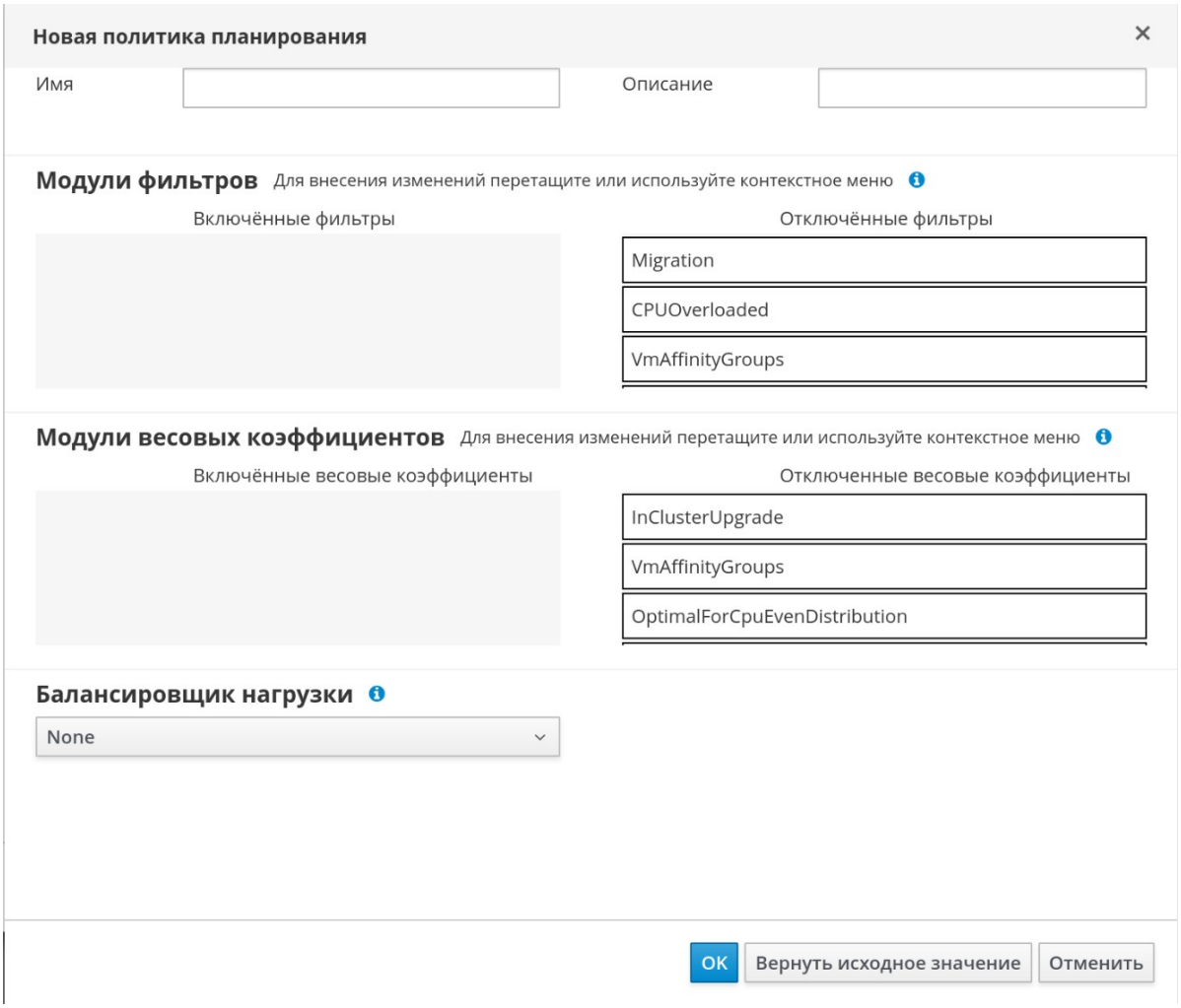

Рис. 24. Создание политики планирования

4. Укажите **Имя** и **Описание** политики планирования.
5. Настройте модули фильтров (Рис. 25):
    a. В разделе **Модули фильтров** перетащите предпочитаемые модули фильтров из раздела **Отключённые фильтры** в раздел **Включённые фильтры** для применения фильтров в политике планирования.
    b. Конкретные модули фильтров также можно настроить как **Первый**, чтобы у него был наивысший приоритет, или **Последний**, чтобы он получил самый низкий приоритет, для базовой оптимизации. Чтобы установить приоритет, нажмите на необходимый модуль фильтра, наведите курсор на пункт **Местоположение** и выберите **Первый** или **Последний**.

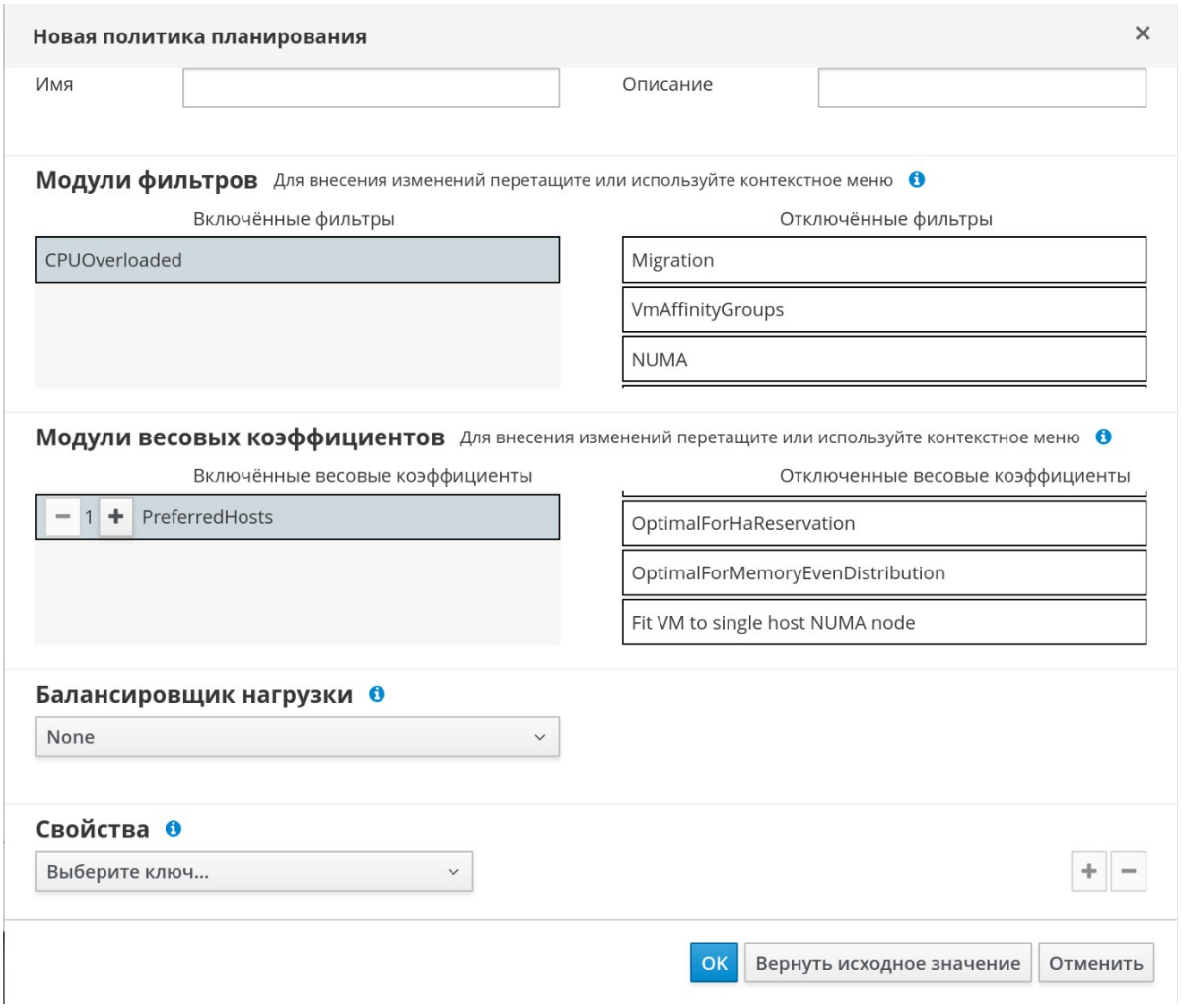

Рис. 25. Настройка модулей фильтров для политики планирования

6. Настройте модули веса:

    a. В разделе **Модули весовых коэффициентов** перетащите предпочитаемые модули веса из области **Отключённые весовые коэффициенты** в область **Включённые весовые коэффициенты**, чтобы применить весовые коэффициенты к политике планирования.
    b. С помощью кнопок + и – слева от включённых модулей веса повышайте или уменьшайте вес этих модулей (Рис. 25).

7. Укажите политику балансировки нагрузки (Рис. 26):

    a. Из выпадающего списка в разделе **Балансировщик нагрузки** выберите политику балансировки нагрузки, которая будет применяться в политике планирования.
    b. Из выпадающего списка в разделе **Параметры** выберите свойство балансировки нагрузки, которое нужно применить в политике

планирования, и в текстовом поле справа от этого свойства укажите значение.

c. С помощью кнопок + и – добавьте или удалите дополнительные свойства.

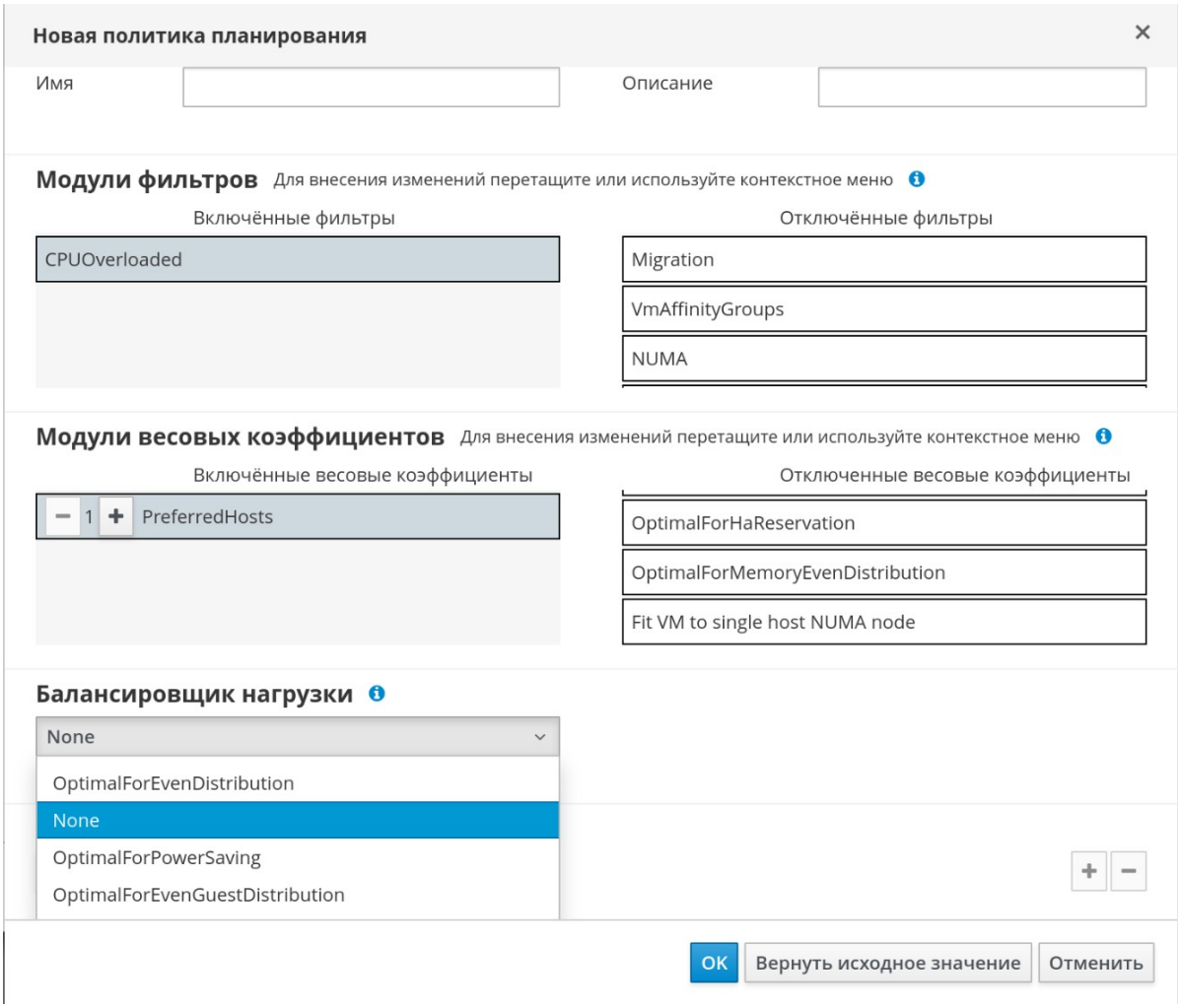

Рис. 26. Настройка балансировщика нагрузки

8. Нажмите **OK**. Новая политика будет добавлена в список политик планирования (Рис. 27).

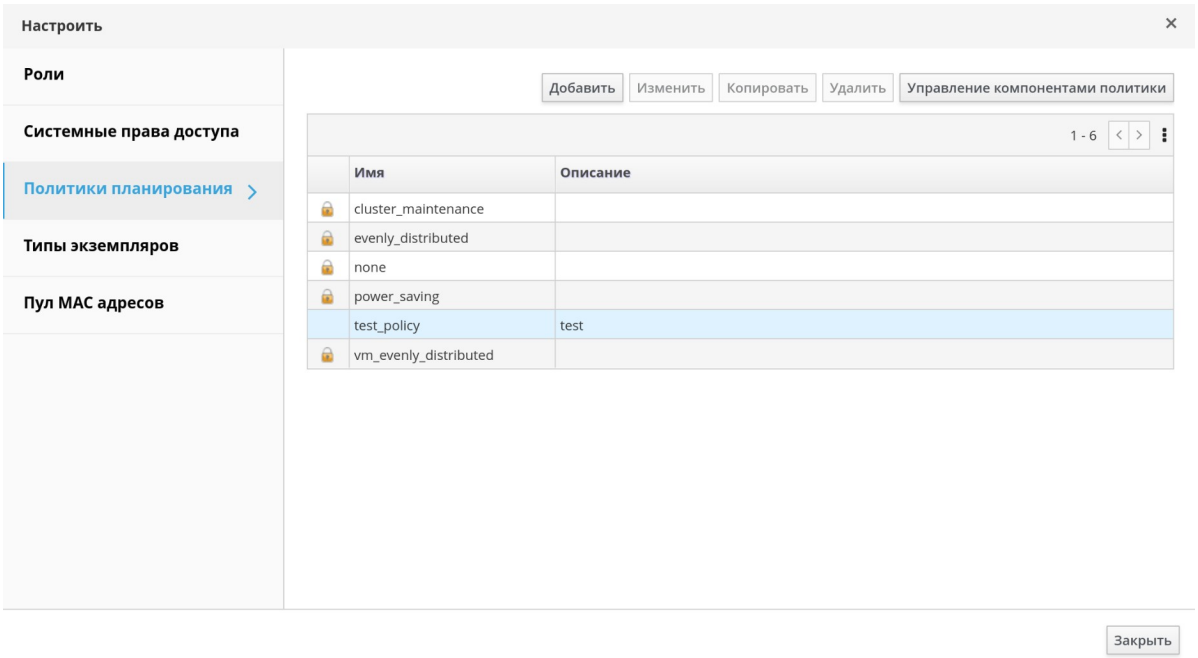

Рис. 27. Политика планирования добавлена в список доступных политик планирования

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

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

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

Поле	Описание
Имя	Название политики планирования. Это название используется для наименования этой политики в виртуализированном ЦУ (СУСВ)
Описание	Описание политики планирования. Это поле рекомендуется заполнить, но оно не обязательно
Модули фильтров	Набор фильтров для контролирования хоста, на котором может выполняться ВМ из кластера (включённый фильтр будет отсеивать хосты, не соответствующие условиям фильтра): • `CpuPinning`: хосты, не отвечающие определению привязки задачи к процессору. • `Migration`: предотвращение миграции на один и тот же хост. • `PinToHost`: хосты, отличные от того хоста, за которым закреплена ВМ.

Поле	Описание
	• `CPU-Level`: хосты, не соответствующие топологии ЦП виртуальной машины. • `CPU`: хосты с меньшим числом ЦП, чем число, указанное для ВМ. • `Memory`: хосты с недостаточным объёмом памяти для работы ВМ. • `VmAffinityGroups`: хосты, не отвечающие условиям, указанным для ВМ-участницы группы схожести. Например, ВМ в группе схожести должны работать на одном и том же хосте или на разных хостах. • `VmToHostsAffinityGroups`: группа хостов, не отвечающих условиям, указанным для ВМ-участницы группы схожести. Например, виртуальные машины в группе схожести должны выполняться на хостах группы или на отельном хосте, не являющимся участником группы. • `InClusterUpgrade`: хосты, работающие под управлением ОС более ранней версии, чем версия ОС хоста, на котором на данный момент выполняется ВМ. • `HostDevice`: хосты, не поддерживающие устройства, требуемые для ВМ. • `HA`: принудительный запуск ВМ из окружения диспетчера виртуализации только на хостах с положительной оценкой высокой доступности. • `Emulated-Machine`: хосты без должной поддержки эмулируемой машины. • `Network`: хосты, на которых не установлены сети, требуемые контроллером сетевого интерфейса ВМ, или на которых не установлена сеть визуализации кластера. • `HostedEnginesSpares`: резервация места под ВМ диспетчера виртуализации на указанном числе узлов диспетчера виртуализации. • `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

Поле	Описание
	отдаётся хостам с более актуальными версиями ОС. • `OptimalForHaReservation`: определяет весовой коэффициент хостов в соответствии с их оценкой высокой доступности. • `None`: определяет весовой коэффициент хостов согласно модулю равномерного распределения. • `OptimalForEvenGuestDistribution`: определяет весовой коэффициент хостов в соответствии с числом ВМ, выполняемых на этих хостах. • `VmAffinityGroups`: определяет весовой коэффициент хостов в соответствии с группой схожести, определённой для ВМ. В соответствии с параметрами этой группы схожести, модуль веса определяет вероятность того, будут ли ВМ в группе схожести выполняться на одном и том же хосте или на разных хостах. • `VmToHostsAffinityGroups`: определяет весовой коэффициент хостов в соответствии с группами схожести, настроенными для машин. Весовой модуль определяет вероятность того, будут ли ВМ в группе схожести выполняться на одном из хостов-участников группы, или на отдельном хосте, не состоящем в группе. • `OptimalForCPUPowerSaving`: определяет весовой коэффициент хостов в соответствии с загрузкой ЦП хостов. Приоритет отдаётся хостам с наиболее высокой загрузкой ЦП. • `OptimalForEvenCpuDistribution`: определяет весовой коэффициент хостов в соответствии с загрузкой ЦП хостов. Приоритет отдаётся хостам с наиболее низкой загрузкой ЦП. • `HA`: определяет весовой коэффициент хостов в соответствии с оценкой их высокой доступности. • `PreferredHosts`: во время настройки ВМ приоритет отдаётся «*предпочитаемым*» хостам. • `OptimalForMemoryPowerSaving`: определяет весовой коэффициент хостов в соответствии с их потреблением памяти. Приоритет отдаётся хостам с более низким объёмом доступной памяти. • `OptimalForMemoryEvenDistribution`: определяет весовой коэффициент хостов в соответствии с их потреблением памяти. Приоритет отдаётся хостам с более высоким объёмом доступной памяти.
Балансировщик нагрузки	В этом выпадающем меню можно выбрать применяемый модуль балансировки нагрузки. Модули балансировки нагрузки определяют логику, используемую во время

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

1.4. Типы экземпляров

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

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

Табл. 1.13. Предварительно настроенные типы экземпляров

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

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

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

1.4.1. Создание типов экземпляров

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

Создание типа экземпляра

1. Нажмите **Администрирование → Настроить**.
2. Перейдите на вкладку **Типы экземпляров** (Рис. 28). В секции справа отобразится список из доступных на данный момент экземпляров.

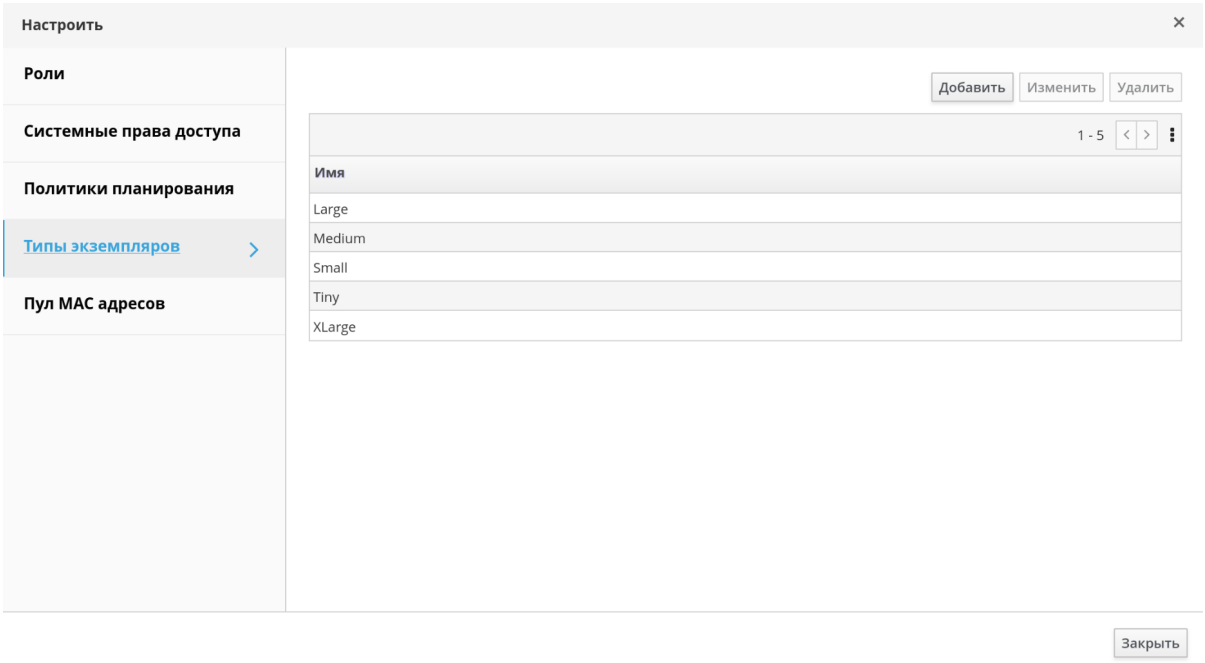

Рис. 28. Выбор типа экземпляра в секции Администрирование → Настроить

3. Нажмите **Добавить**. Откроется экранная форма **Новый тип экземпляра**.

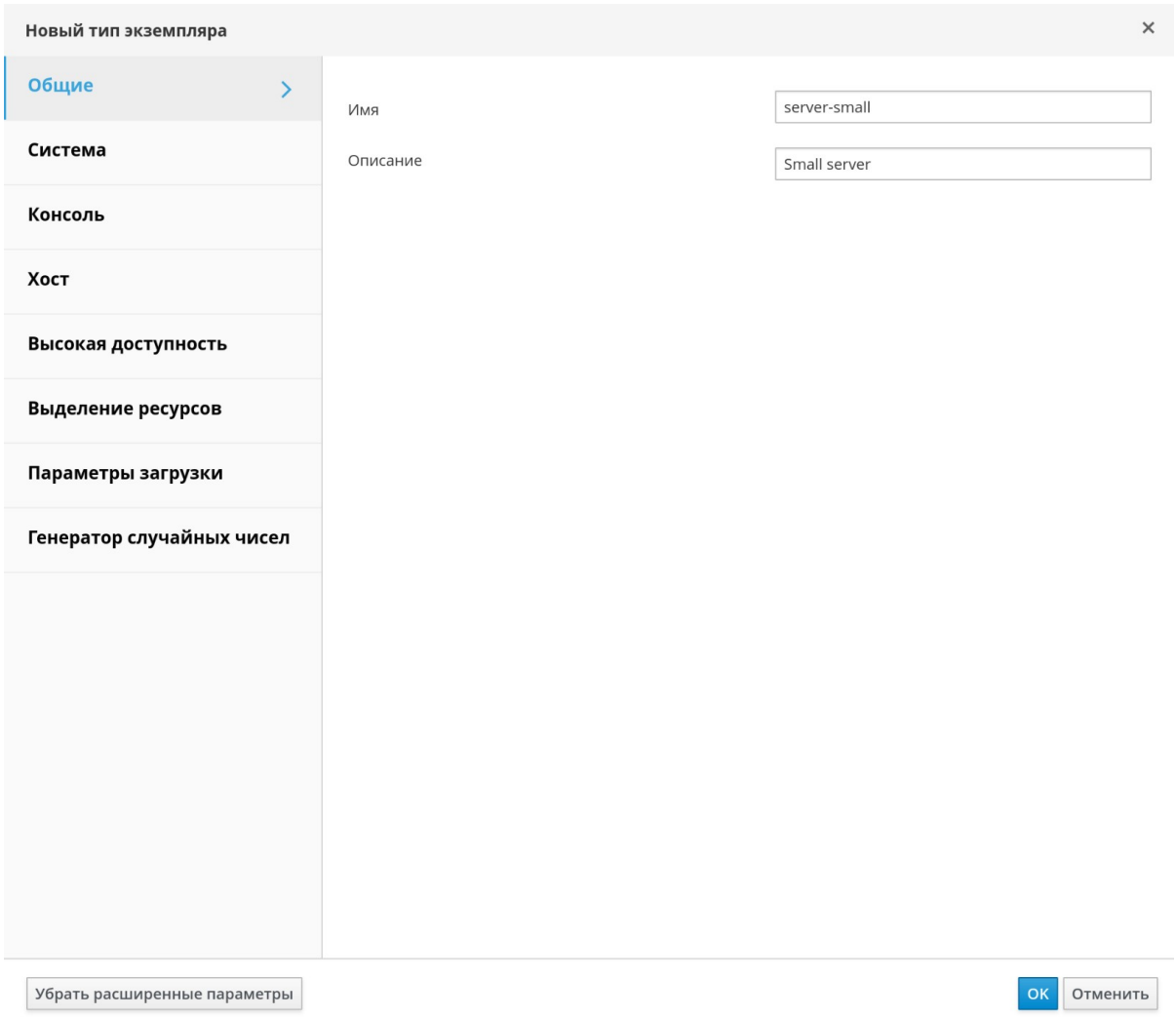

Рис. 29. Форма Новый тип экземпляра, для добавления нового экземпляра

4. Введите **Имя** и **Описание** типа экземпляра (Рис. 29).
5. Выберите секцию **Система** и нажмите **Дополнительные параметры** (Рис. 30). Настройте параметры типа экземпляра так, как это необходимо. Параметры, присутствующие в окне **Новый тип экземпляра**, идентичны параметрам в окне **Новая виртуальная машина**, но присутствуют только поля, имеющие отношение к типам экземпляров (см. Приложение А.1. VDSM).

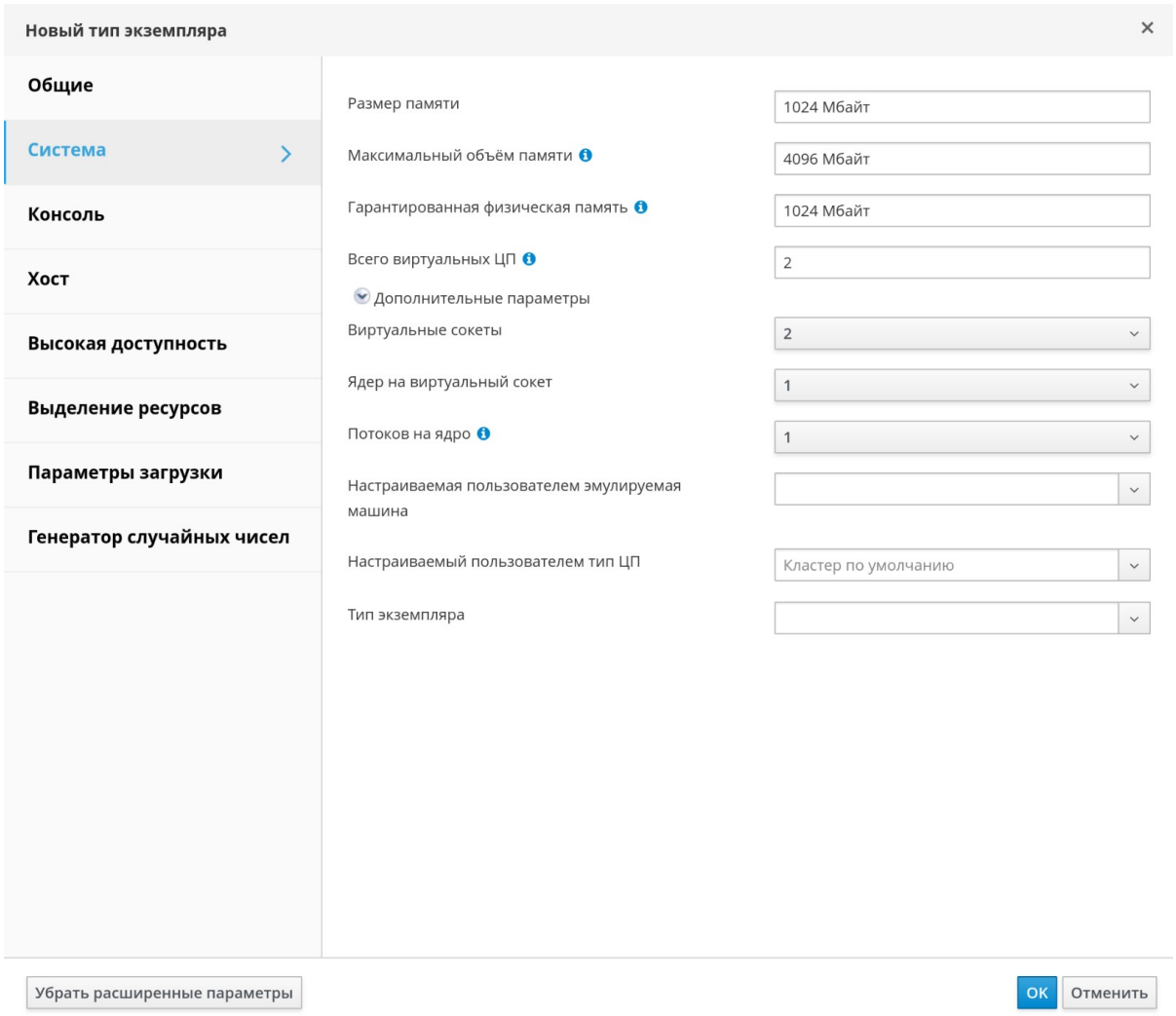

Рис. 30. Секцию Система и подсекция Дополнительные параметры

6. Выберите секцию **Консоль** (Рис. 31) и укажите параметры консоли, используемые по умолчанию.

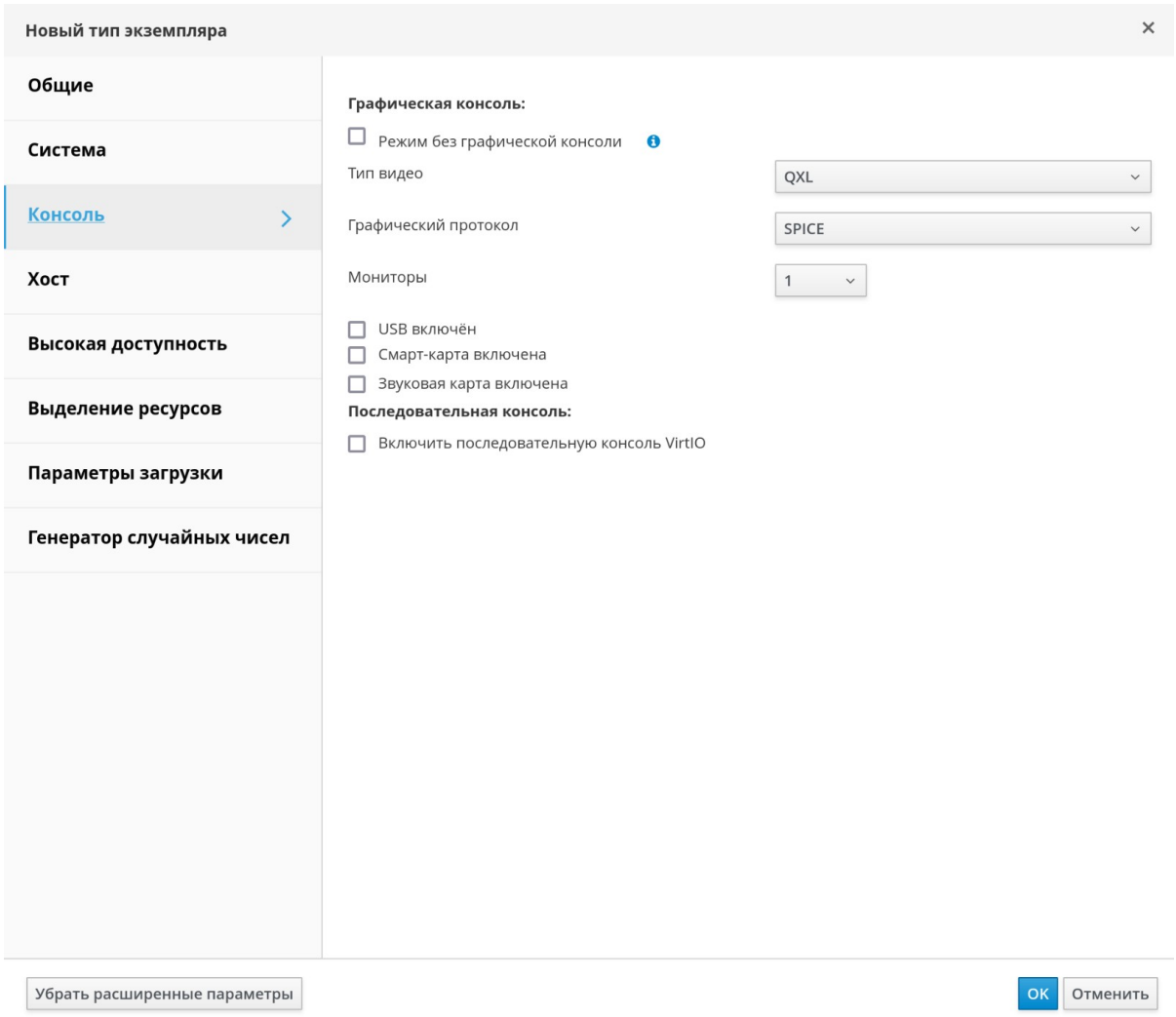

Рис. 31. Новый тип экземпляра — секция Консоль

7. Нажмите **OK**.

Новый тип экземпляра появится во вкладке **Типы экземпляров** в секции **Администрирование → Настроить** (Рис. 34), и может быть выбран в выпадающем списке **Тип экземпляра** при создании или изменении ВМ (**Ресурсы → Виртуальные машины → Добавить** , Рис. 32).

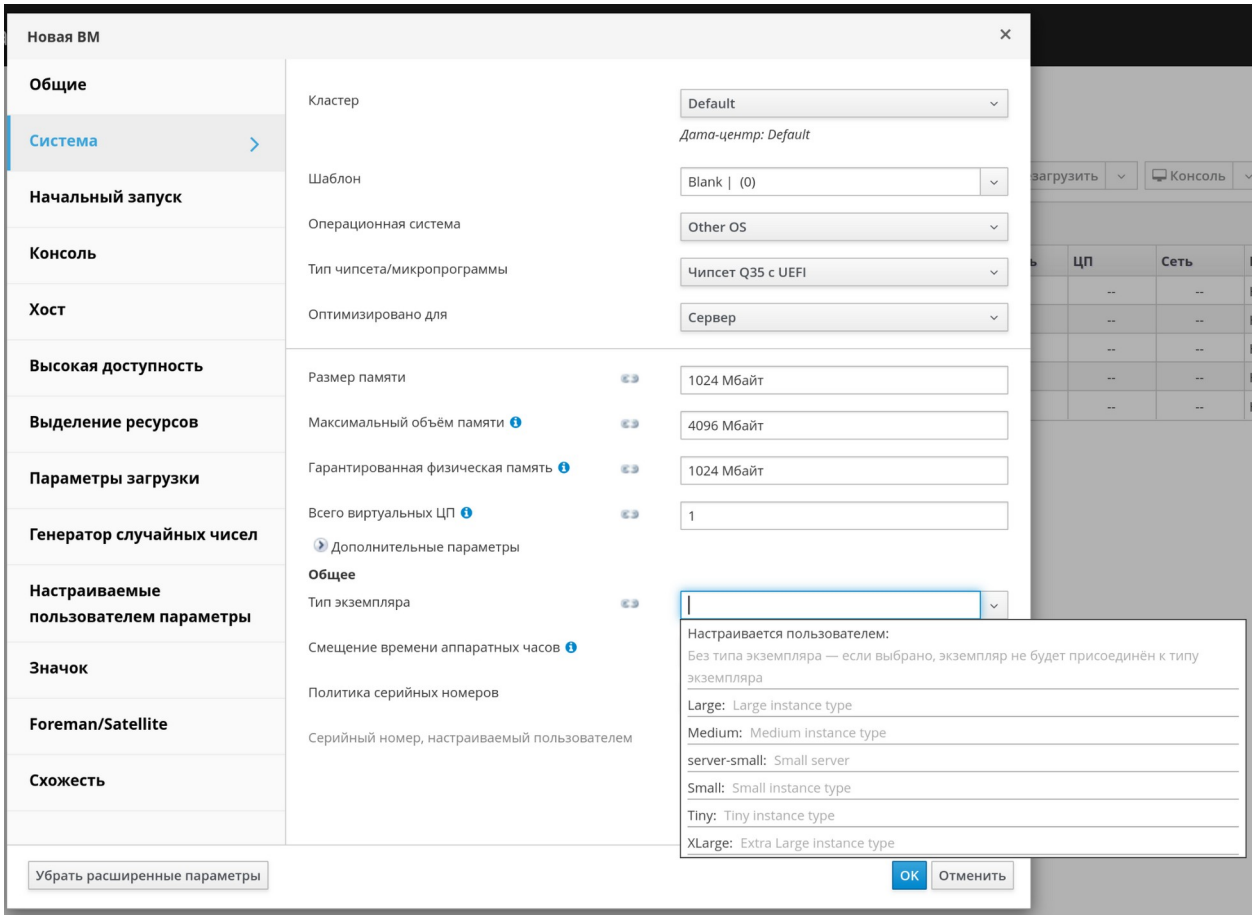

Рис. 32. Выбор типа экземпляра при создании новой ВМ

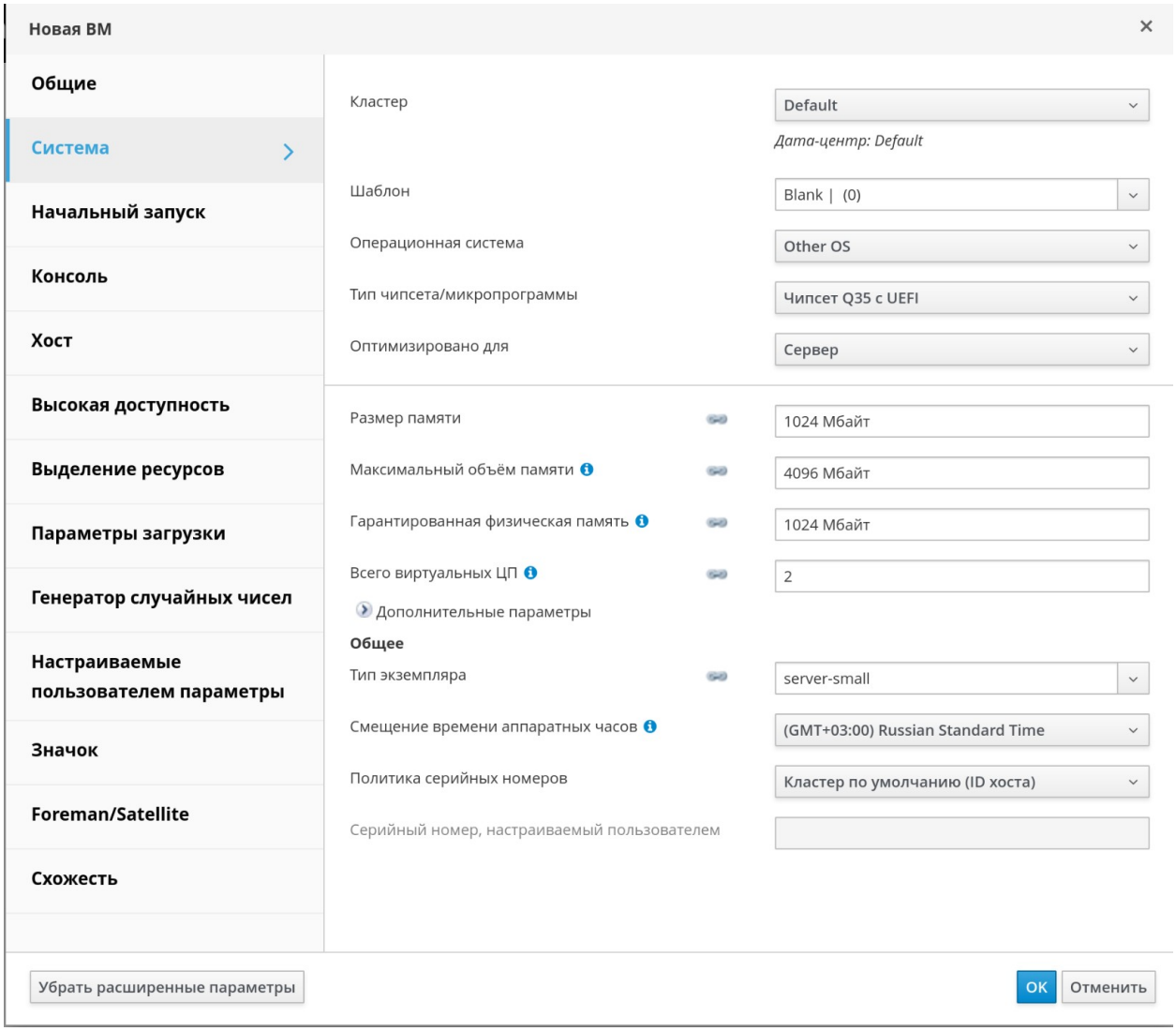

Рис. 33. При создании новой ВМ выбран экземпляр (Тип экземпляра) server-small

Пример:
Добавлен новый тип экземпляра `server-small` (Рис. 34).

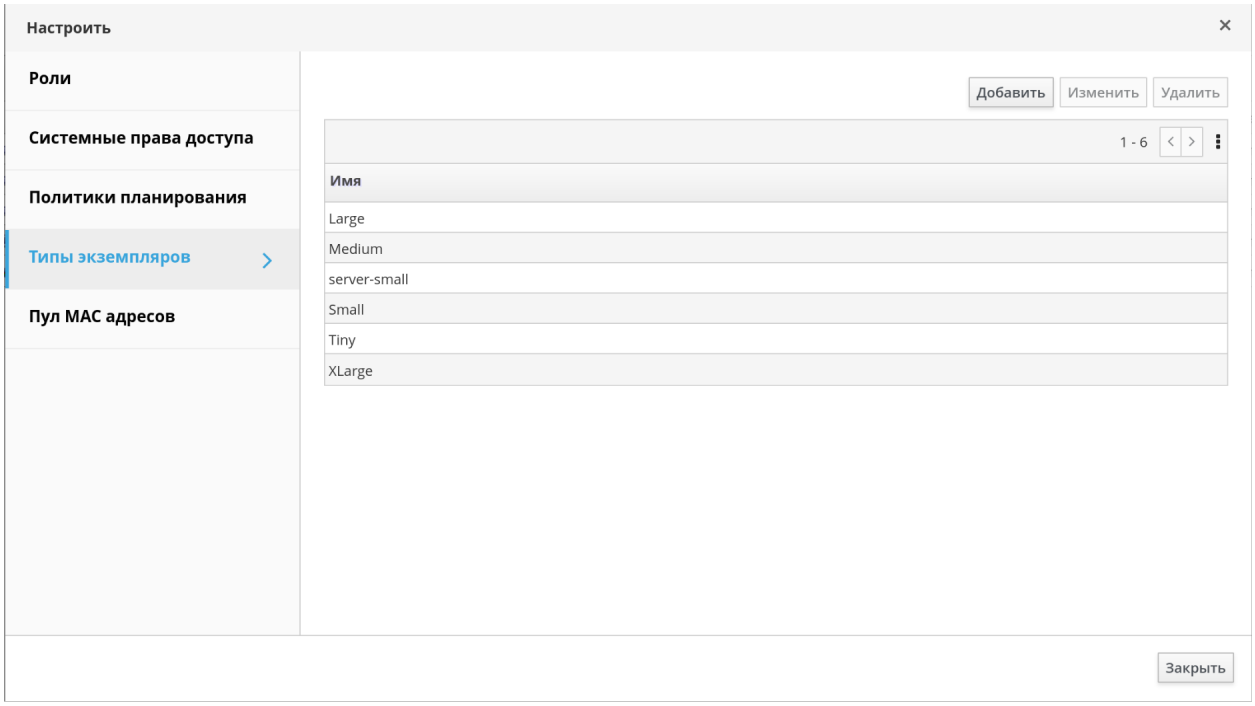

Рис. 34. Секция Типы экземпляров — список экземпляров с добавленным новым типом экземпляра

1.4.2. Изменение типов экземпляров

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

Изменение параметров типов экземпляров

1. Нажмите **Администрирование → Настроить**.
2. Перейдите на вкладку **Типы экземпляров**.
3. Выберите изменяемый тип экземпляра.
4. Нажмите **Изменить** (Рис. 35).

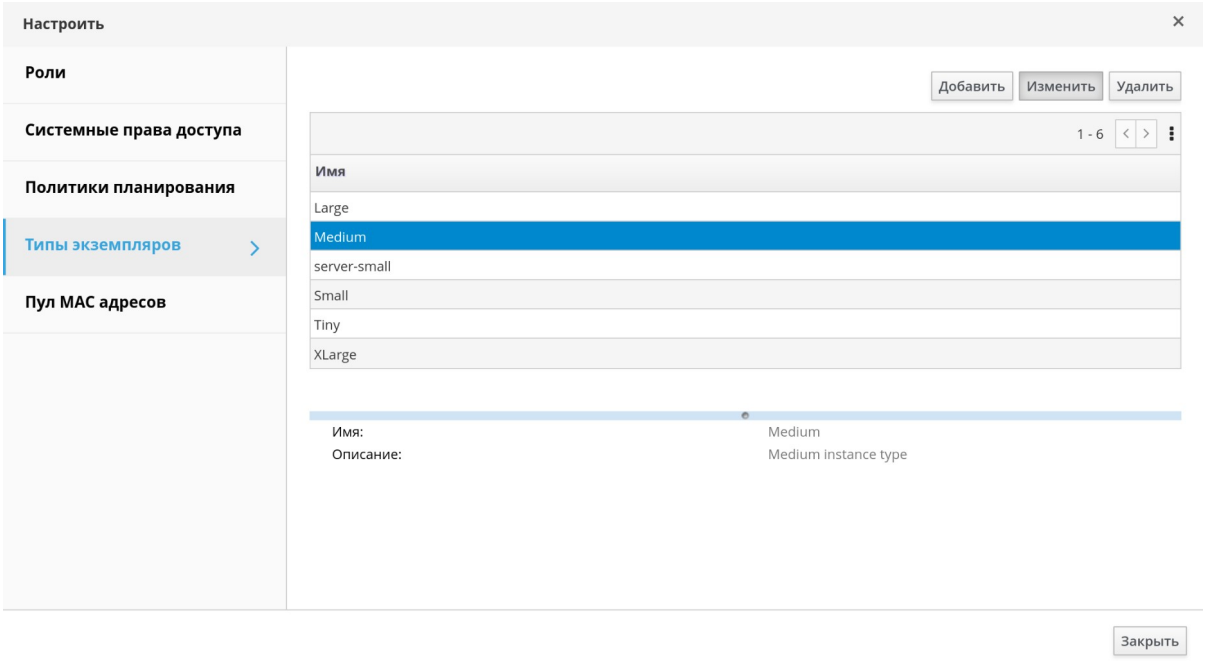

Рис. 35. Выбор типа экземпляра для внесения изменений

5. Измените параметры экземпляра так, как это необходимо (Рис. 36).

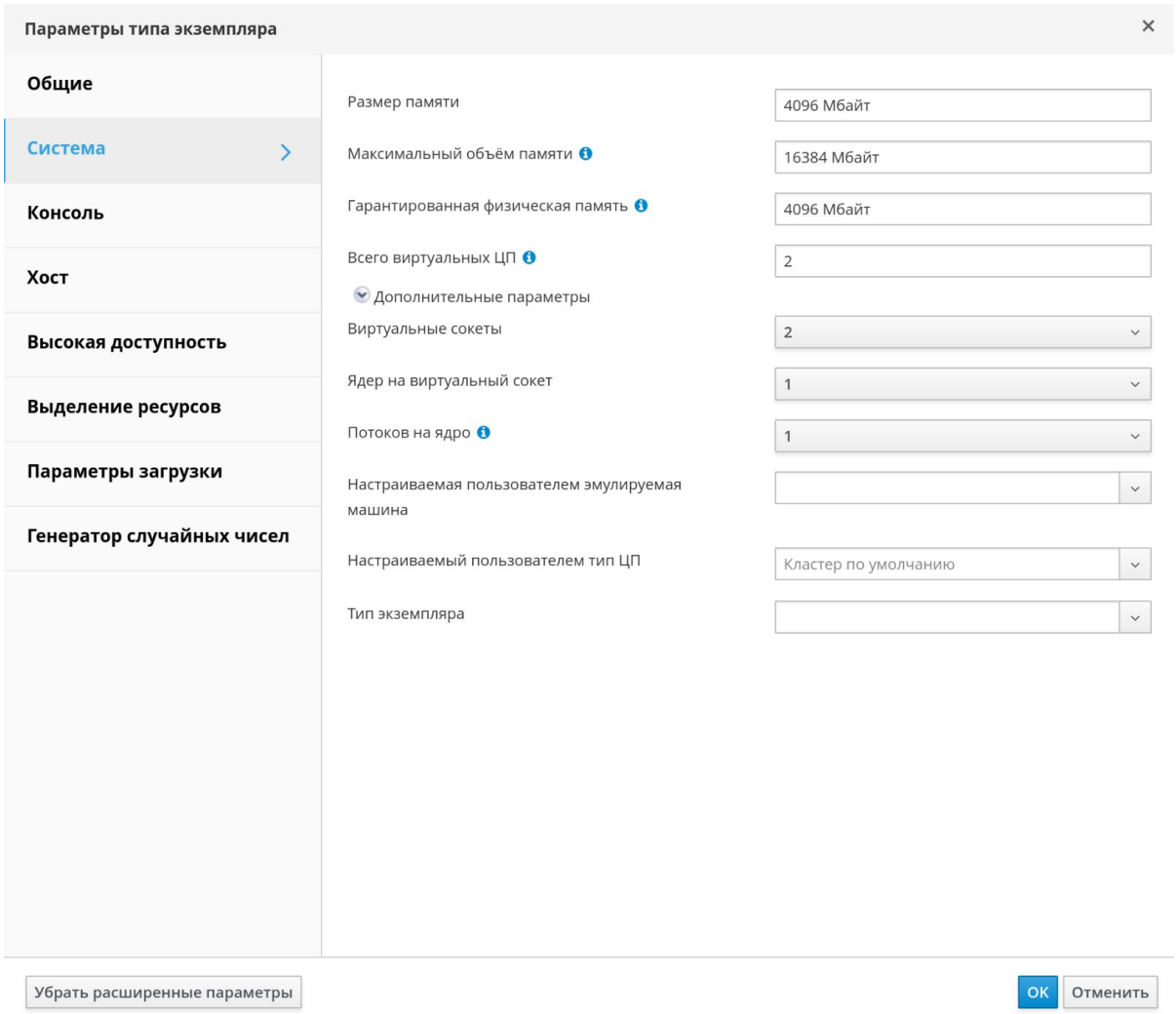

Рис. 36. Изменение параметров экземпляра

6. Нажмите **OK**.

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

В параметрах существующих ВМ, основанных на этом типе экземпляра, будут показаны поля со значком цепи, и информация в этих полях будет обновлена. Если во время изменения типа экземпляра выполнялись ВМ, то рядом с такими ВМ появится оранжевый значок «Изменения, ожидающие применения», а информация в полях со значком цепи будет обновлена во время следующего перезапуска.

1.4.3. Удаление типов экземпляров

Удаление типа экземпляра

1. Нажмите **Администрирование → Настроить**.
2. Перейдите на вкладку **Типы экземпляров**.
3. Выберите удаляемый тип экземпляра.

4. Нажмите **Удалить**.

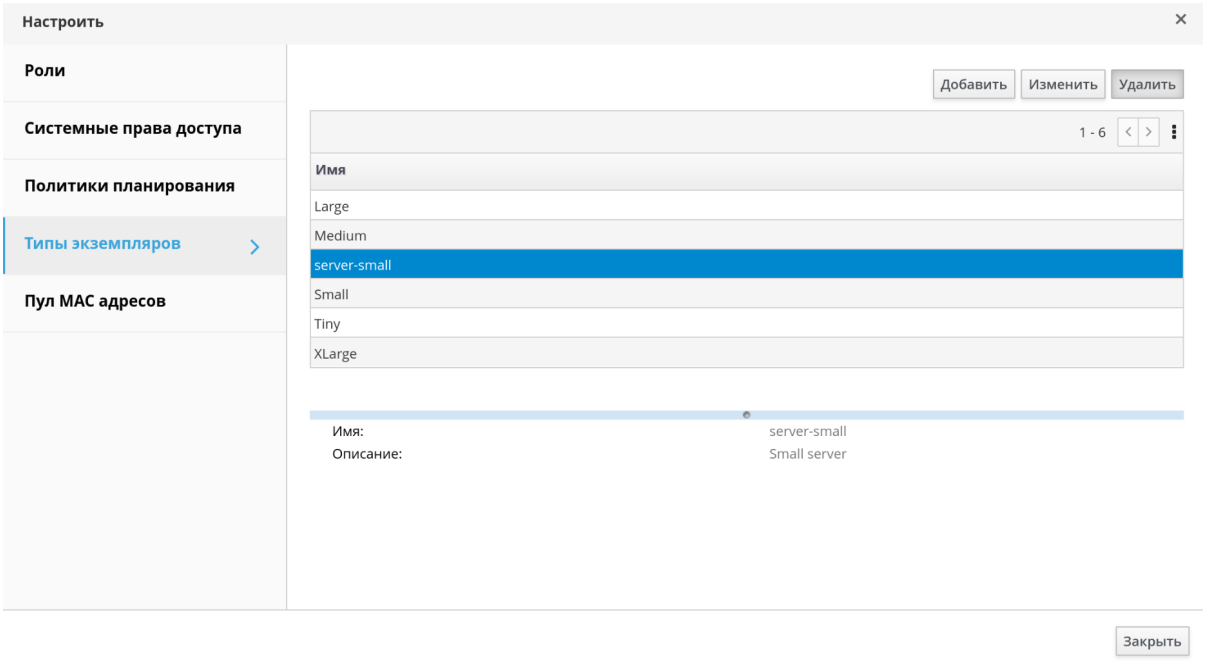

Рис. 37. Удаление выбранного типа экземпляра

5. При наличии ВМ, созданных на основе этого типа экземпляра, появится предупреждающее окно со списком привязанных машин. Для удаления типа экземпляра установите флажок **Подтвердить операцию**. В противном случае нажмите **Отмена**.

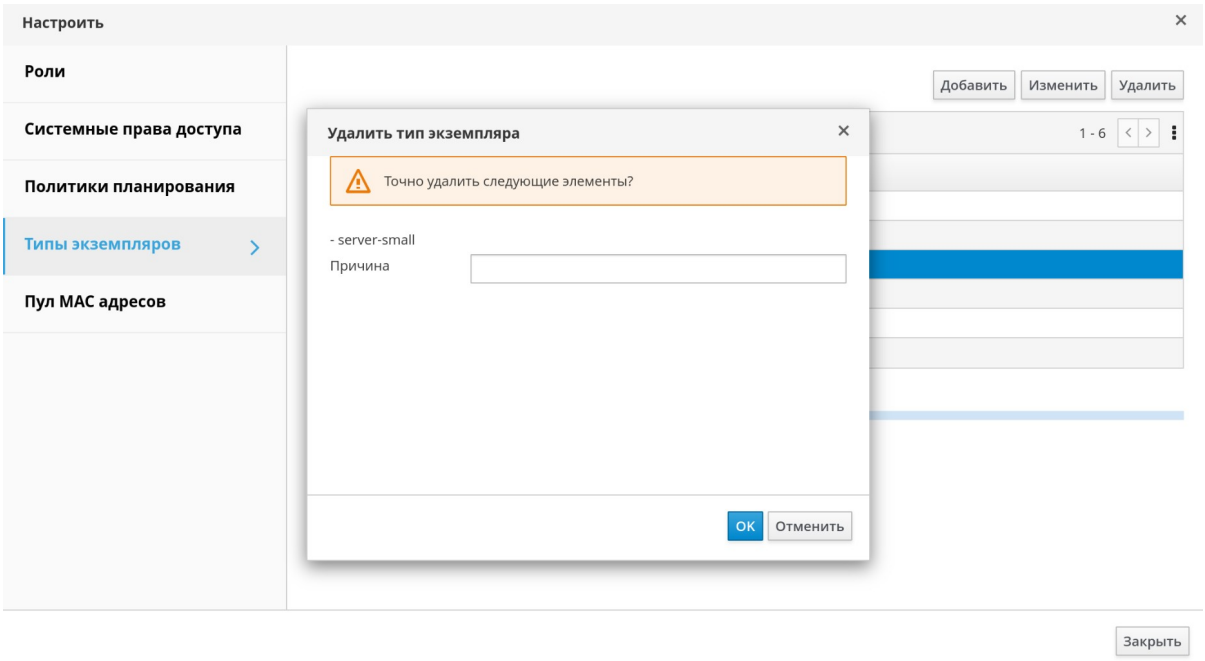

Рис. 38. Удалить тип экземпляра - подтвердить удаление (опционально: указать причину удаления)

6. Нажмите **OK** для подтверждения удаления экземпляра (Рис. 38), или **Отменить** для отмены удаления.

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

1.5. Пулы адресов MAC

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

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

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

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

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

1.5.1. Создание пулов MAC адресов

Создание пула MAC адресов

1. Нажмите **Администрирование → Настроить**.
2. Перейдите на вкладку **Пул MAC адресов** (Рис. 39).

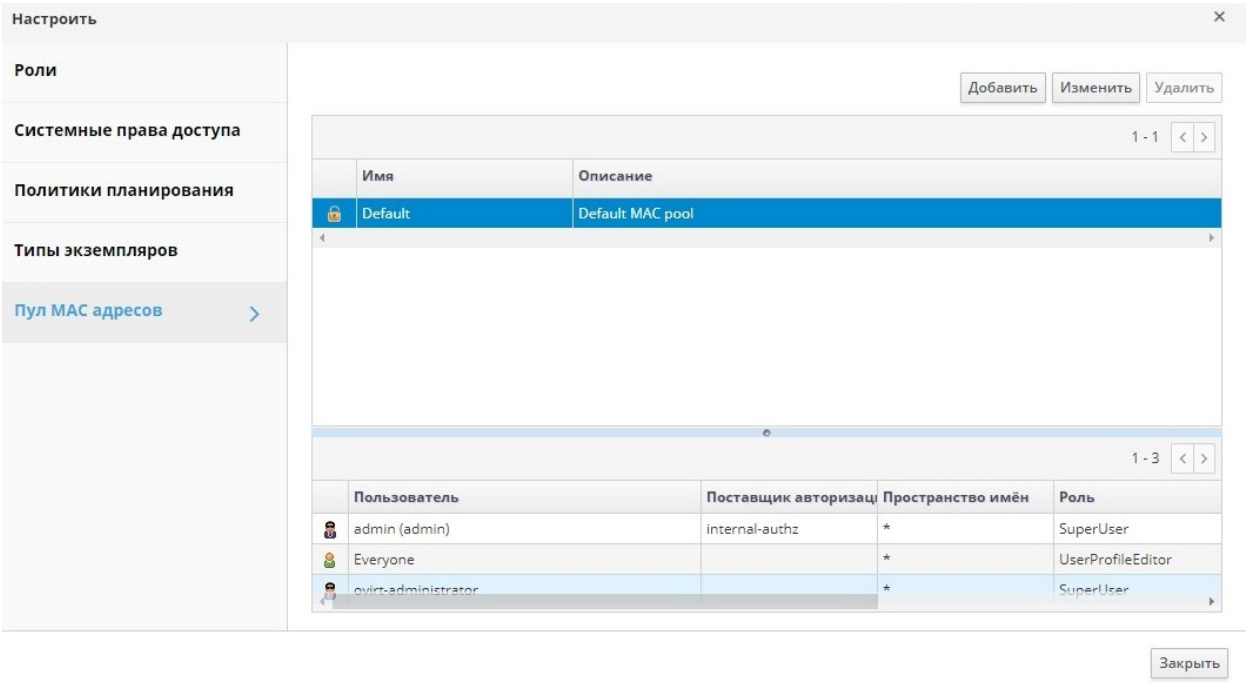

Рис. 39. Меню «Пул MAC адресов»

3. Нажмите **Добавить**.
4. Введите **Имя** и **Описание** нового пула адресов MAC (Рис. 40).

5. Установите флажок **Разрешить дубликаты**, чтобы разрешить использование в пуле одного и того же адреса MAC более одного раза. Пул не будет автоматически использовать дублирующий адрес MAC, но включение параметра, разрешающего дубликаты, означает, что пользователь может вручную использовать дублирующий адрес.

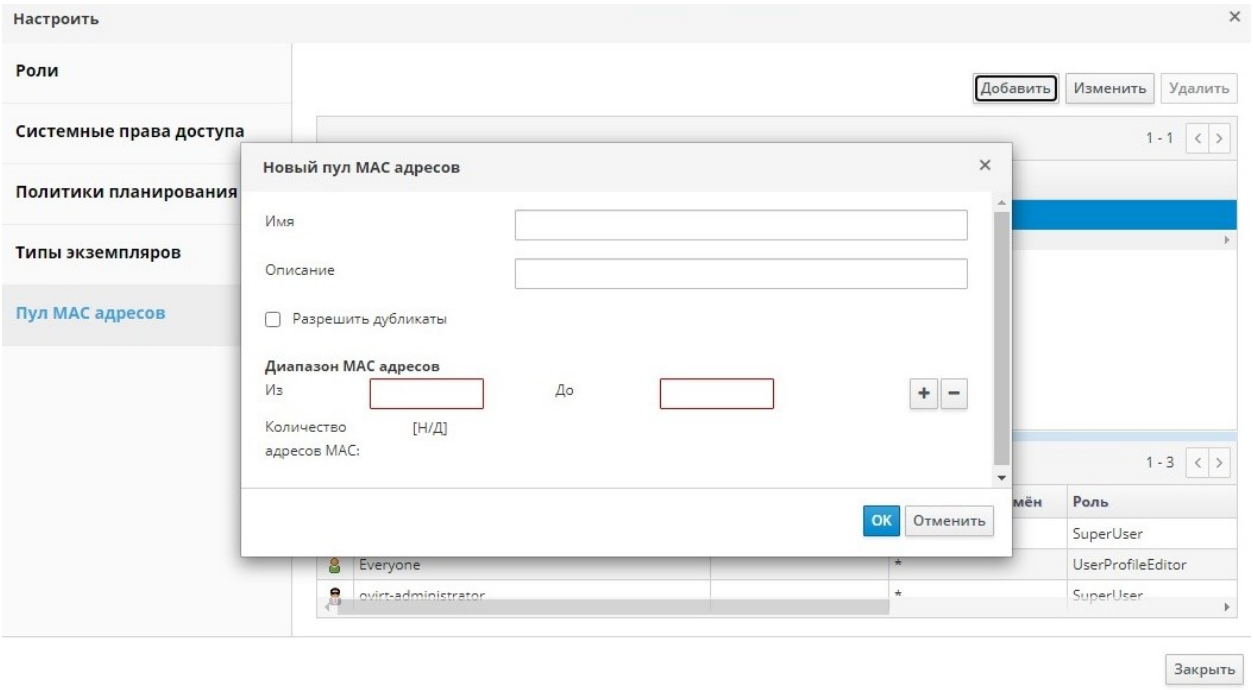

Рис. 40. Новый пул MAC адресов

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

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

1.5.2. Изменение пулов адресов MAC

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

Изменение параметров пулов адресов MAC

1. Нажмите **Администрирование → Настроить**.
2. Перейдите на вкладку **Пул MAC адресов** (Рис. 39).
3. Выберите изменяемый пул.
4. Нажмите **Изменить**.
5. Необходимым образом измените поля **Имя**, **Описание**, **Разрешить дубликаты** и **Диапазон MAC адресов**.

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

6. Нажмите **OK**.

1.5.3. Удаление пулов адресов MAC

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

Удаление пула адресов MAC

1. Нажмите **Администрирование → Настроить**.
2. Перейдите на вкладку **Пул MAC адресов** (Рис. 39).
3. Выберите удаляемый пул.
4. Нажмите **Удалить**.
5. Нажмите **ОК**.

Глава 2. Панель мониторинга

Панель мониторинга (Рис. 41) предлагает общий обзор состояния системы виртуализации с помощью сводки сведений о её ресурсах и общем коэффициенте использования. Эта сводка может предупредить о проблеме и даёт возможность проанализировать проблемную область.

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

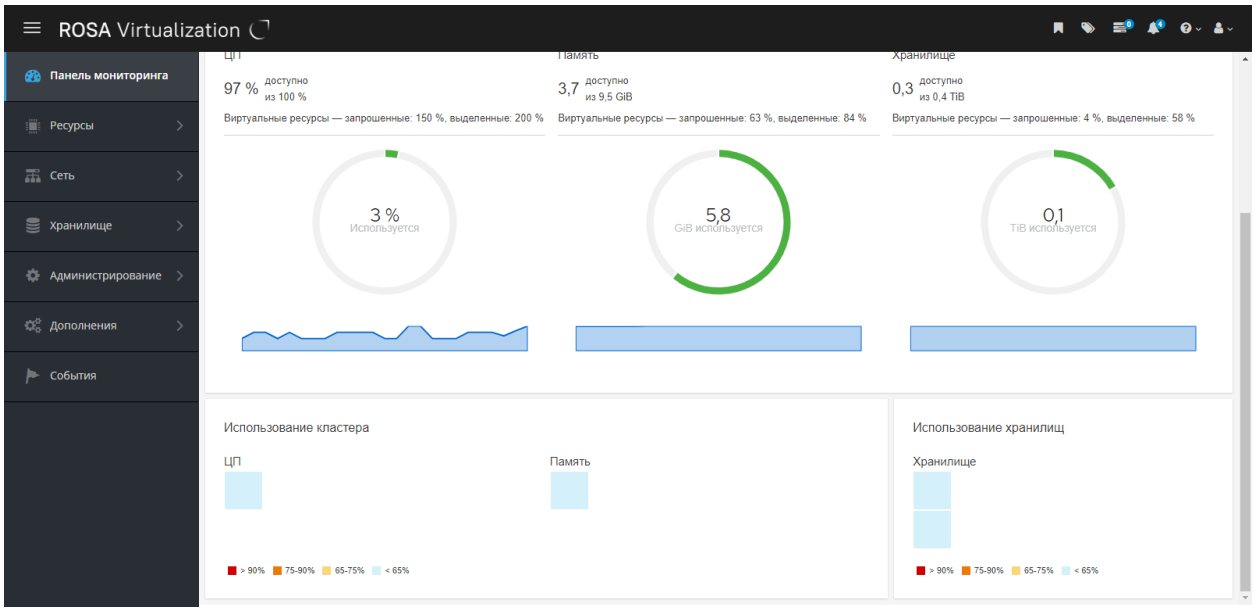

Рис. 41. Панель мониторинга

2.1. Предварительные условия для установки

Для панели мониторинга необходимо установленное и настроенное хранилище данных.

2.2. Общий перечень

Самый верхний раздел панели мониторинга предлагает общий перечень ресурсов системы виртуализации (Рис. 42), в который входят разделы для дата-центров, кластеров, хостов, доменов хранилищ, виртуальных машин и событий. Значки показывают состояние каждого ресурса, а числа — количество ресурсов с этим статусом.

Рис. 42. Общий перечень ресурсов в панели мониторинга

Заголовок показывает номер типа ресурса, а статус ресурса показывается под заголовком. В Табл. 2.1 приведено описание статусов ресурсов и значков, отображающих состояние ресурсов. Нажав на ресурс, можно перейти на соответствующую страницу диспетчера виртуализации. Статус кластеров всегда показывается как «Недоступно».

Табл. 2.1. Статусы ресурсов

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

Значок	Статус
	инициализации, в режиме обслуживания или незапущенными. • **Тома Gluster**: поиск ограничен неактивными или отсоединёнными томами. • **Хосты**: поиск ограничен хостами не отвечающими, с ошибкой, с ошибкой инсталляции, в нерабочем состоянии, в процессе инициализации или не запущенными. • **Домены хранилищ**: поиск ограничен отсоединёнными или неактивными доменами хранилищ. • **Виртуальные машины**: поиск ограничен незапущенными машинами, не отвечающими или в перезагрузке.
	Показывает число событий с оповещениями о состоянии. Нажатие на значок переносит на страницу **События** с поиском, ограниченным серьёзностью оповещения
	Показывает количество событий с ошибкой. Нажатие на значок переносит на страницу **События** с поиском, ограниченным серьёзностью ошибки

2.3. Общий коэффициент использования

Раздел **Общее использование** (Рис. 43) показывает коэффициент использования ЦП, памяти и хранилища.

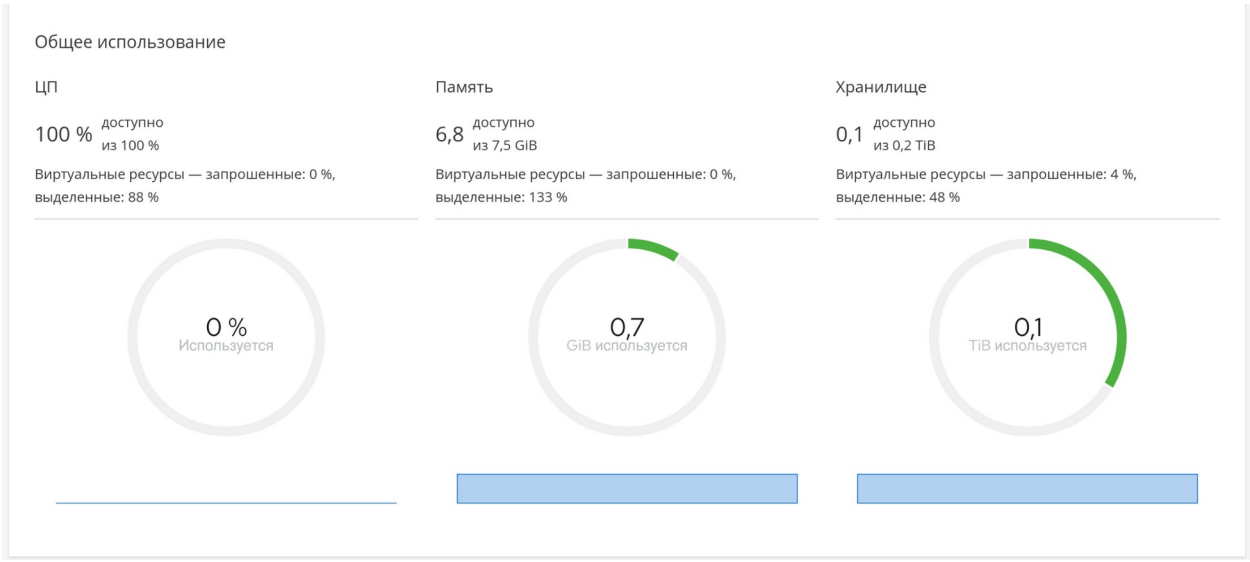

Рис. 43. Общее использование ЦП, памяти и хранилища

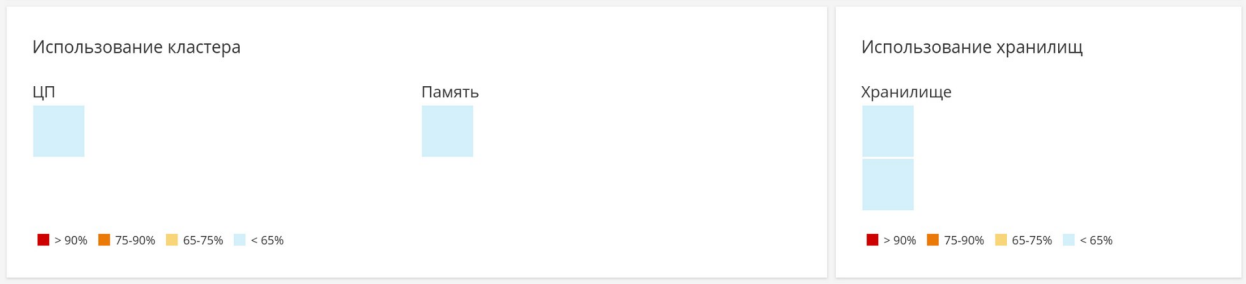

Рис. 44. Общее использование ресурсов кластера

В верхнем разделе отображается процент доступных ресурсов ЦП, памяти или хранилища (Рис. 43), 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 (Рис. 43) отображаются процентные значения использования ЦП, памяти или хранилища, а также среднее потребление для всех хостов на основе среднего потребления за последние 5 минут. Наведение курсора на сегмент кругового графика покажет значение выделенного сегмента.

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

2.3.1. Наиболее используемые ресурсы

Нажатие на круговой график раздела **Общее использование** (Рис. 43) в разделе общего использования панели мониторинга покажет список наиболее используемых ресурсов **ЦП** (Рис. 45), **памяти** (Рис. 46) или **хранилища** (Рис. 47).

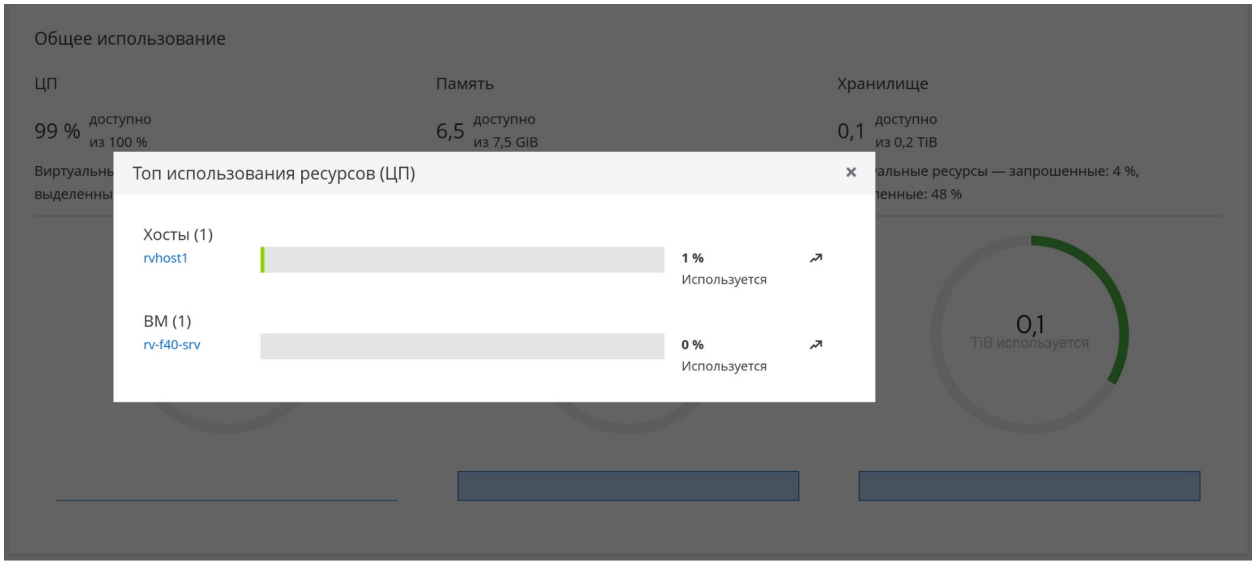

Рис. 45. Наиболее используемые ресурсы (ЦП)

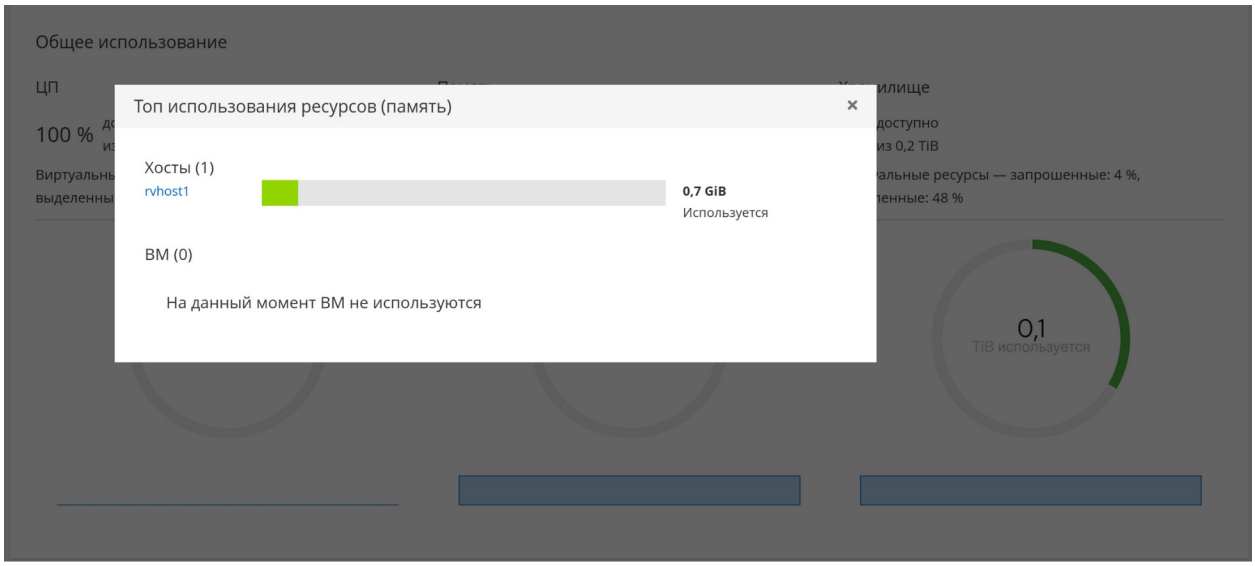

Рис. 46. Топ использования ресурсов (память)

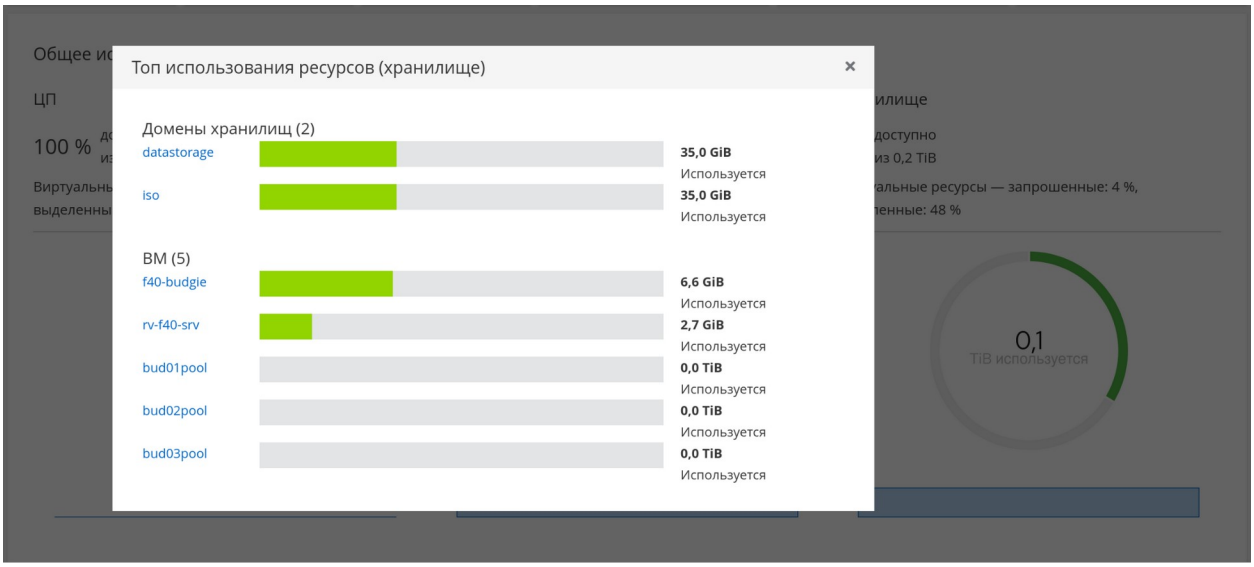

Рис. 47. Топ использования ресурсов (хранилище)

- Для ЦП и памяти всплывающий список показывает десять хостов и ВМ с наиболее высоким потреблением.
- Для хранилища всплывающий с 0щ9писок покажет десять наиболее используемых доменов хранилищ и ВМ.

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

2.4. Использование кластера

В разделе **Использование кластера** (Рис. 48) на тепловой карте отображается использование ЦП и памяти.

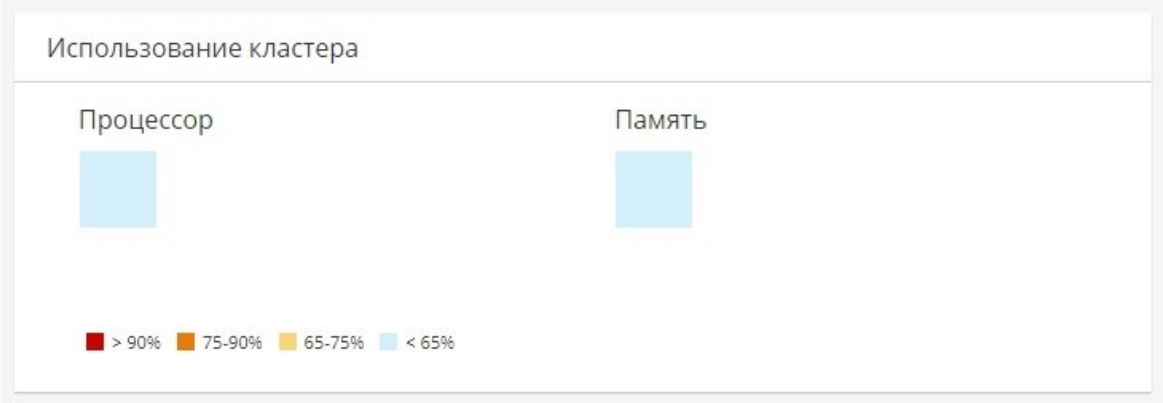

Рис. 48. Использование кластера

2.4.1. Использование ЦП

Тепловая карта использования ЦП конкретного кластера, показывает средний процент использования ЦП за последние 24 часа. Наведение курсора на тепловую карту показывает название кластера. Нажатие на тепловую карту переносит в меню **Ресурсы → Хосты** с результатами поиска по конкретному кластеру с фильтром использования ЦП.

Расчёты для нахождения общего среднего использования ЦП на кластер делаются с использованием среднего процента нагрузки ЦП для каждого хоста за последние 24 часа.

2.4.2. Использование памяти

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

2.5. Использование хранилищ

В разделе **Использование хранилищ** (Рис. 49) на тепловой карте показывается процент использования хранилища.

Рис. 49. Использование хранилищ

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

Глава 3. Поиск

3.1. Операции поиска в системе виртуализации

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

3.2. Примеры поиска и поисковый синтаксис

Поисковые запросы по ресурсам системы виртуализации имеют следующий синтаксис:

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

Примеры синтаксиса

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

Табл. 3.1. Примеры поисковых запросов

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

3.3. Автодополнение поиска

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

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

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

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

3.4. Типы результатов поиска

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

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

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

3.5. Критерии поиска

Критерии поиска указываются в поиске после двоеточия.

Синтаксис критериев поиска `{criteria}` следующий:

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

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

Табл. 3.3. Примеры критериев поиска

Часть	Описание	Значения	Пример	Примечание
prop	Свойство искомого ресурса. Также может быть свойством типа ресурса (`obj-type`) или меткой (tag)	Ограничьте поиск объектами с определёнными свойствами. Ищите, например, объекты со свойством **status**	Status	
obj-type	Тип ресурса, который может быть связан с поисковым ресурсом	Системные объекты. Например, дата-центры и ВМ	Users	
operator	Операторы сравнения	= != (не равно) > < >= <=		Параметры значений зависят от свойств
Значение (Value)	То, с чем сравнивается выражение	Запись (строка) Целое число Порядок Дата (форматируется в соответствии с региональными параметрами)	Jones 256 normal	В строках можно использовать символы подстановки "" (две кавычки, без пробелов между ними) могут использоваться в качестве неинициализированной (пустой) строки. Строка или дата, содержащие пробелы, должны заключаться в двойные кавычки

3.6. Несколько критериев поиска и символы подстановки

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

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

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

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

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

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

3.7. Определение порядка поиска

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

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

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

3.8. Поиск дата-центров

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

Табл. 3.4. Поиск дата-центров

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
`Clusters.`*`clusters-prop`*	Зависит от типа свойства	Свойство кластера, связанное с дата-центром
`name`	Строка	Имя дата-центра
`description`	Строка	Описание дата-центра
`type`	Строка	Тип дата-центра
`status`	Список	Доступность дата-центра
`sortby`	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
`page`	Целое число	Номер страницы результатов

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

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

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

3.9. Поиск кластеров

В Табл. 3.5 описываются все параметры поиска кластеров.

Табл. 3.5. Поиск кластеров

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

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

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

3.10. Поиск хостов

В Табл. 3.6 описываются все параметры поиска хостов.

Табл. 3.6. Поиск хостов

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

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
`memory`	Целое число	Объём доступной памяти
`cpu_speed`	Целое число	Вычислительная скорость ЦП
`cpu_model`	Строка	Тип ЦП
`active_vms`	Целое число	Число, выполняющихся на данный момент ВМ
`migrating_vms`	Целое число	Число, мигрирующих на данный момент ВМ
`committed_mem`	Целое число	Процент выделенной памяти
`tag`	Строка	Метка, присвоенная хосту
`type`	Строка	Тип хоста
`datacenter`	Строка	Дата-центр, к которому принадлежит хост
`sortby`	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
`page`	Целое число	Номер страницы результатов поиска

3.11. Поиск сетей

В Табл. 3.7 описываются все параметры поиска сетей.

Табл. 3.7. Поиск сетей

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
`Cluster_network.`*`clusternetwork-prop`*	Зависит от типа свойства	Свойство кластера, связанное с сетью
`Host_Network.`*`hostnetwork-prop`*	Зависит от типа свойства	Свойство хоста, связанное с сетью
`name`	Строка	Имя, идентифицирующее сеть
`description`	Строка	Ключевые слова или текст, описывающие сеть, используемые

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
		по желанию при создании сети
`vlanid`	Целое число	VLAN ID сети
`stp`	Строка	Включён или отключён протокол STP для сети
`mtu`	Целое число	Максимальное значение MTU логической сети
`vmnetwork`	Строка	Используется ли сеть только для переноса трафика ВМ
`datacenter`	Строка	Дата-центр, к которому присоединена сеть
`sortby`	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
`page`	Целое число	Номер страницы результатов поиска

3.12. Поиск хранилищ

В Табл. 3.8 описываются все параметры поиска хранилищ.

Табл. 3.8. Поиск хранилищ

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
`Hosts.`*`hosts-prop`*	Зависит от типа свойства	Свойства хостов, связанные с хранилищем
`Clusters.`*`clusters-prop`*	Зависит от типа свойства	Свойства кластеров, связанные с хранилищем
`name`	Строка	Уникальное имя, идентифицирующее хранилище в сети
`status`	Строка	Статус домена хранения
`external_status`	Строка	Работоспособность домена

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
		хранения, согласно полученным сообщениям от внешних служб и модулей
`datacenter`	Строка	Дата-центр, которому принадлежит хранилище
`type`	Строка	Тип хранилища
`size`	Целое число	Размер хранилища
`used`	Целое число	Используемый объём хранилища
`committed`	Целое число	Выделенный объём хранилища
`sortby`	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
`page`	Целое число	Номер страницы результатов поиска

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

Storage: size > 200 or used < 50

3.13. Поиск дисков

В Табл. 3.9 описываются параметры поиска дисков.

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

Табл. 3.9. Поиск дисков

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
`Datacenters.`*`datacenters-prop`*	Зависит от типа свойства	Свойство дата-центров, связанное с диском
`Storages.`*`storages-prop`*	Зависит от типа свойства	Свойство хранилища, связанное с диском
`alias`	Строка	Имя, идентифицирующее хранилище в сети

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
`description`	Строка	Ключевые слова или текст с 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 присоединён диск
`vm_names`	Строка	Имена ВМ, к которым присоединён диск
`quota`	Строка	Имя квоты, принудительно применяющейся к виртуальному диску
`sortby`	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
`page`	Целое число	Номер страницы результатов поиска

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

Disks: format = `unused` and provisioned_size > 8

3.14. Поиск томов

В Табл. 3.10 описываются параметры поиска томов.

Табл. 3.10. Поиск томов

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
`Cluster`	Строка	Имя кластера, связанное с томом
`Cluster.`*`cluster-prop`*	Зависит от типа свойства (например: имя, описание, комментарий, архитектура)	Свойства кластеров, связанные с томом
`name`	Строка	Имя, идентифицирующее том
`type`	Строка	Принимаемые значения: распределённый (`distribute`), реплицированный (`replicate`), распределённый реплицированный (`distributed_replicate`), чередующийся (`stripe`), распределённый чередующийся (`distributed_stripe`)
`transport_type`	Целое число	Принимаемые значения: `TCP,RDMA`
`replica_count`	Целое число	Число реплик
`stripe_count`	Целое число	Число чередующихся частей
`status`	Строка	Статус тома. Принимаемые значения: *запущен* (`up`) или *не запущен* (`down`)
`sortby`	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса

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

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

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

3.15. Поиск виртуальных машин

В Табл. 3.11 описываются параметры поиска ВМ.

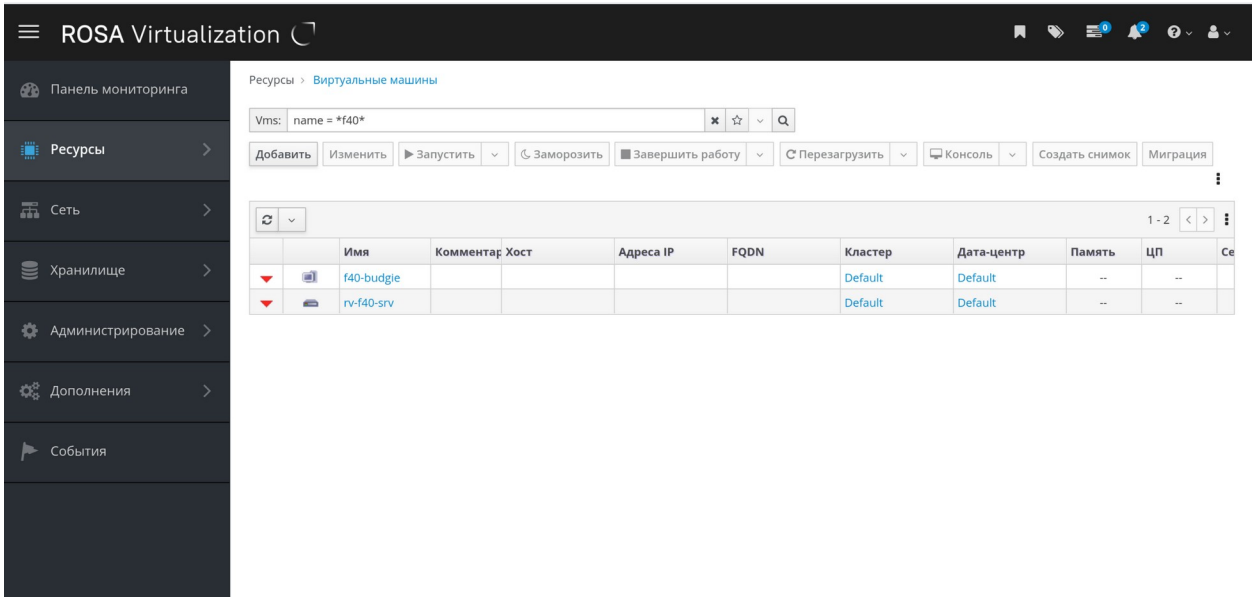

Рис. 50. Поиск ВМ по шаблону имени

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

Табл. 3.11. Поиск ВМ

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
Hosts.hosts-prop	Зависит от типа свойства	Свойство хостов, связанное с ВМ
Templates.templates-prop	Зависит от типа свойства	Свойство шаблонов, связанное с ВМ

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

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

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

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

3.16. Поиск пулов

В Табл. 3.12 описываются параметры поиска пулов.

Табл. 3.12. Поиск пулов

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

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

```
Pools: type = automatic
```

3.17. Поиск шаблонов

В Табл. 3.13 описываются параметры поиска шаблонов.

Табл. 3.13. Поиск по шаблонам

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

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
mem	Целое число	Определяемая память
description	Строка	Описание шаблона
status	Строка	Статус шаблона
cluster	Строка	Кластер, связанный с шаблоном
datacenter	Строка	Дата-центр, связанный с шаблоном
quota	Строка	Квота, связанная с шаблоном
sortby	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
page	Целое число	Номер страницы результатов поиска

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

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

3.18. Поиск пользователей

В Табл. 3.14 описываются параметры поиска пользователей.

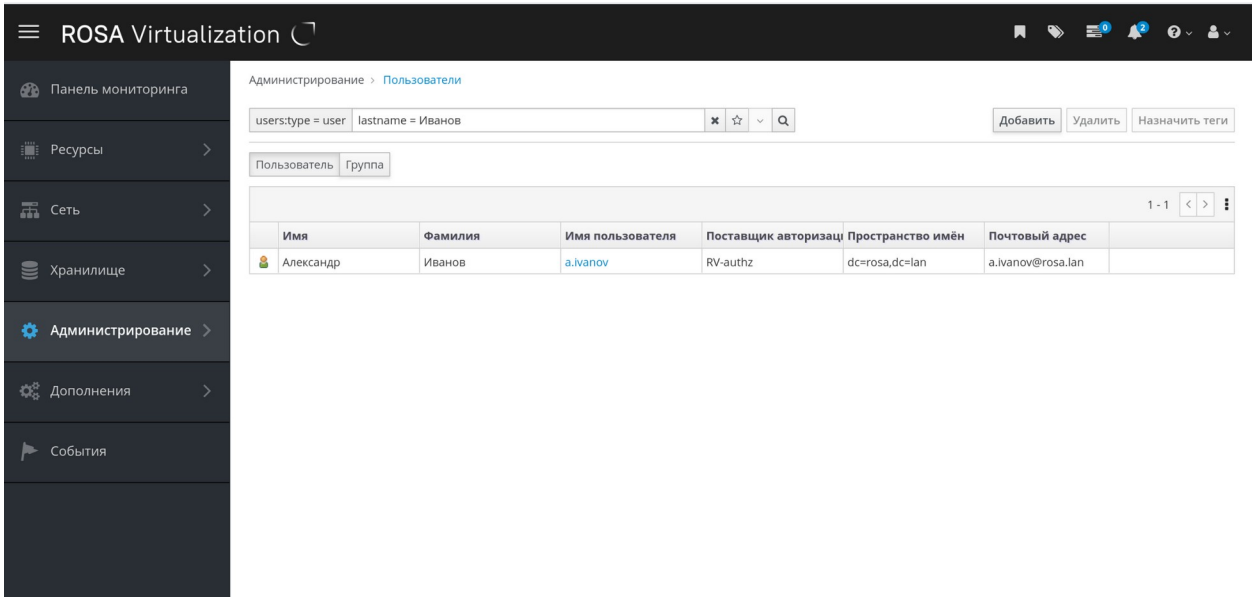

Рис. 51. Поиск всех пользователей с фамилией Иванов

Табл. 3.14. Поиск пользователей

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
`Vms.Vms-prop`	Зависит от типа свойства	Свойство ВМ, связанное с пользователем
`Hosts.hosts-prop`	Зависит от типа свойства	Свойство хостов, связанное с пользователем
`Templates.templates-prop`	Зависит от типа свойства	Свойство шаблонов, связанное с пользователем
`Events.events-prop`	Зависит от типа свойства	Свойство событий, связанное с пользователем
`name`	Строка	Имя пользователя
`lastname`	Строка	Фамилия пользователя
`usrname`	Строка	Уникальное имя пользователя
`department`	Строка	Учреждение пользователя
`group`	Строка	Группа пользователей
`title`	Строка	Должность пользователя

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
`status`	Строка	Статус пользователя
`role`	Строка	Роль пользователя
`tag`	Строка	Метка пользователя
`pool`	Строка	Пул пользователя
`sortby`	Список	Сортирует возвращённые результаты согласно одному из свойств ресурса
`page`	Целое число	Номер страницы результатов поиска

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

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

3.19. Поиск событий

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

Табл. 3.15. Поиск событий

Свойство (ресурса или типа ресурса)	Тип	Описание (отсылка)
`Vms.Vms-prop`	Зависит от типа свойства	Свойства ВМ, связанные с событием
`Hosts.hosts-prop`	Зависит от типа свойства	Свойства хостов, связанные с событием
`Templates.templates-prop`	Зависит от типа свойства	Свойства шаблонов, связанные с событием
`Users.users-prop`	Зависит от типа свойства	Свойства пользователей, связанные с событием

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

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

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

Следующий запрос возвращает список событий, которые произошли на ВМ с именем `rv-f40-srv`:

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

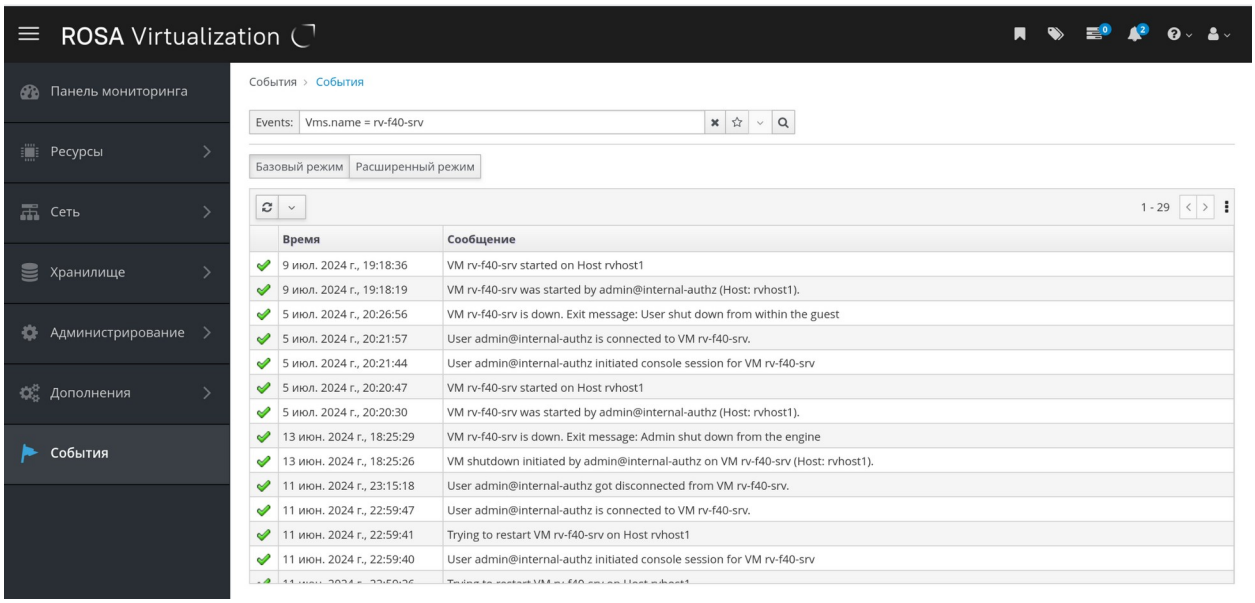

Рис. 52. Список событий, которые произошли на ВМ с именем `rv-f40-srv`

Глава 4. Закладки

4.1. Сохранение строки поискового запроса в виде закладки

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

Сохранение поискового запроса в виде закладки

1. Введите нужный поисковый запрос в строку поиска и запустите поиск.
2. Нажмите на кнопку **Закладка** в виде звёздочки справа от строки поиска (Рис. 53), чтобы открыть окно **Новая закладка**.

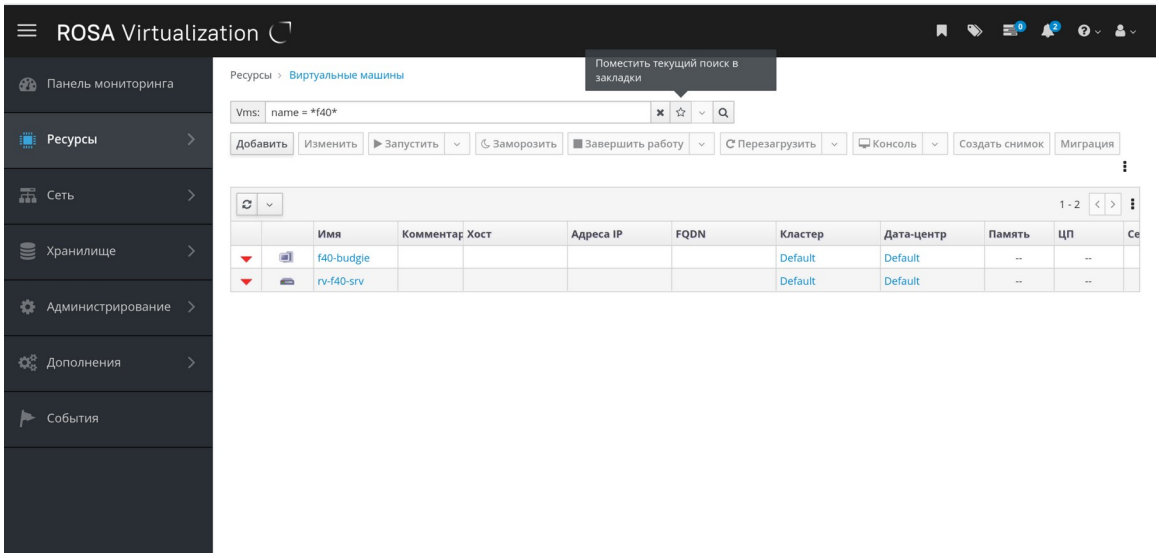

Рис. 53. Нажмите на кнопку **Закладка** в виде звёздочки справа от строки поиска, для добавления закладки

3. Введите **Имя** закладки в форме **Новая закладка** (Рис. 54).

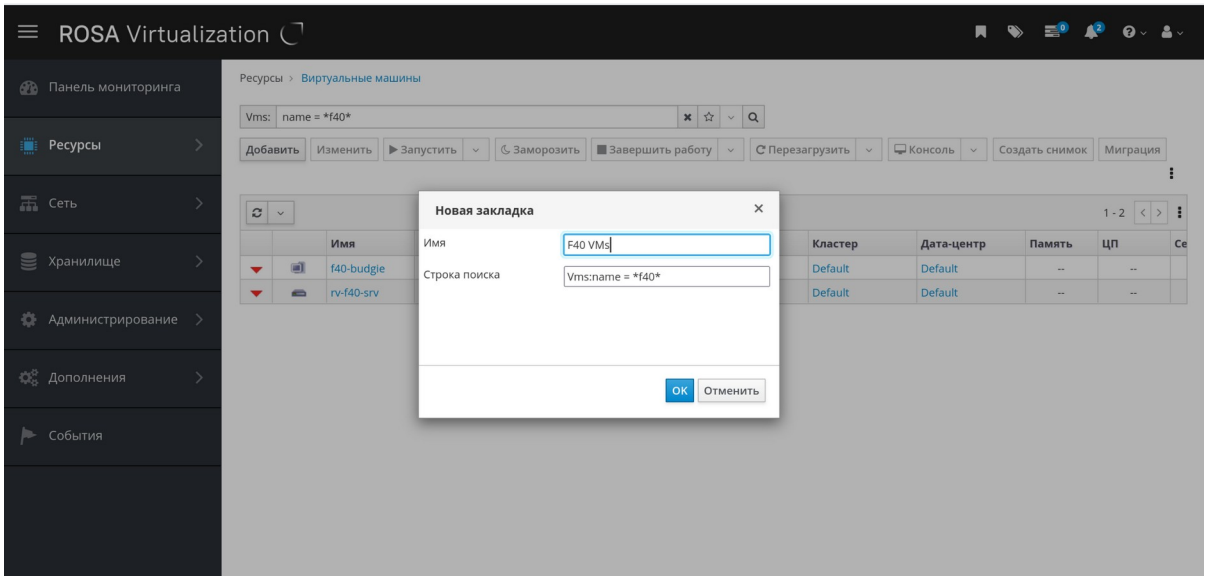

Рис. 54. Форма Новая закладка, для добавления закладки

4. При необходимости, измените поле **Строка поиска**.
5. Нажмите **OK** для добавления закладки (Рис. 54), или **Отменить** для отмены.

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

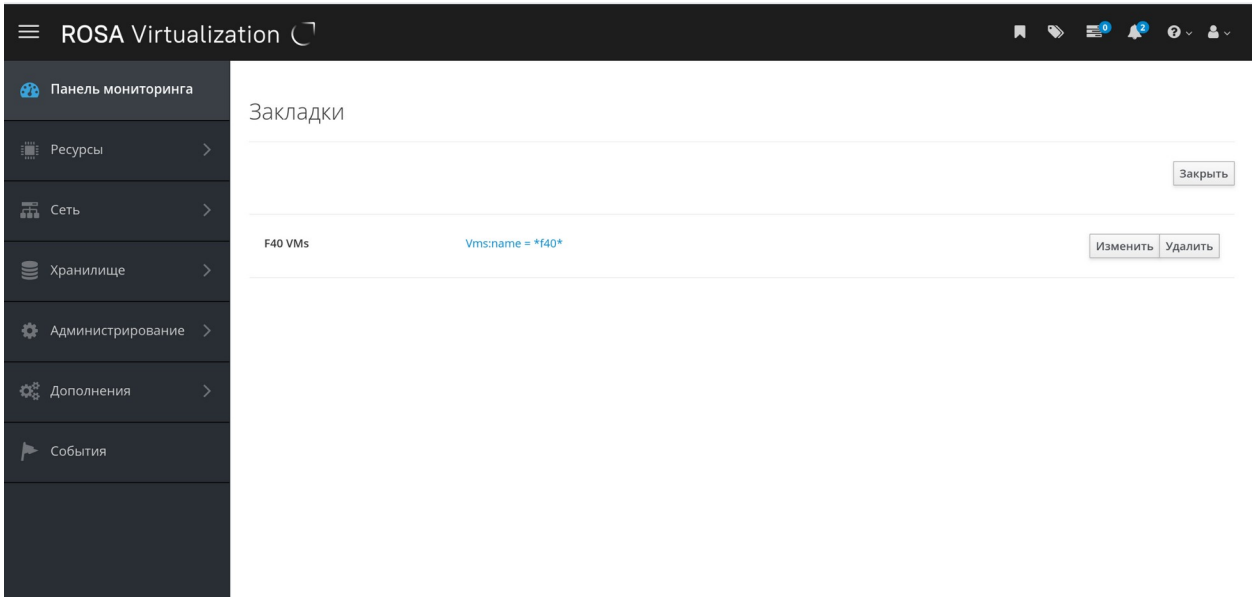

Рис. 55. Экранная форма Закладки

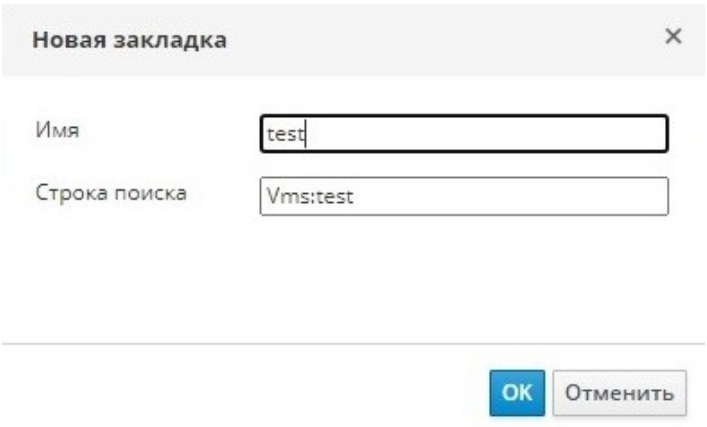

Рис. 56. Создание закладки

4.2. Редактирование закладок

Название и строку поиска закладок можно изменять.

Редактирование закладок

1. Нажмите на значок **Закладки** ( ) на панели заголовков.
2. Выберите закладку (Рис. 57) и нажмите **Изменить**.

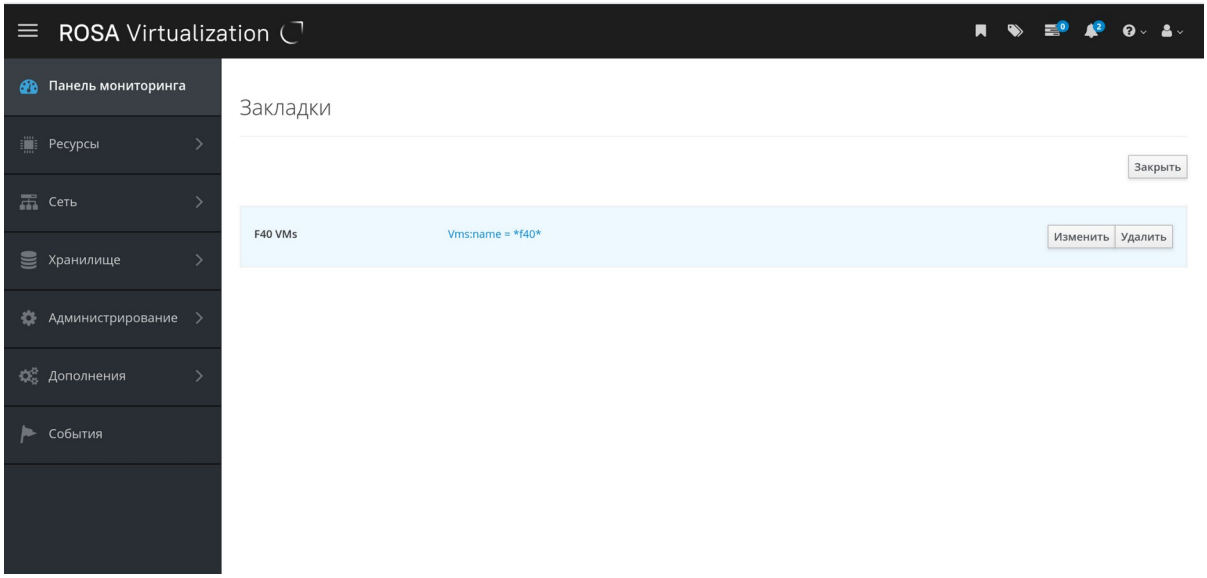

Рис. 57. Выбор закладки в форме Закладки

3. Внесите необходимые изменения в поля **Имя** и **Строка поиска**.

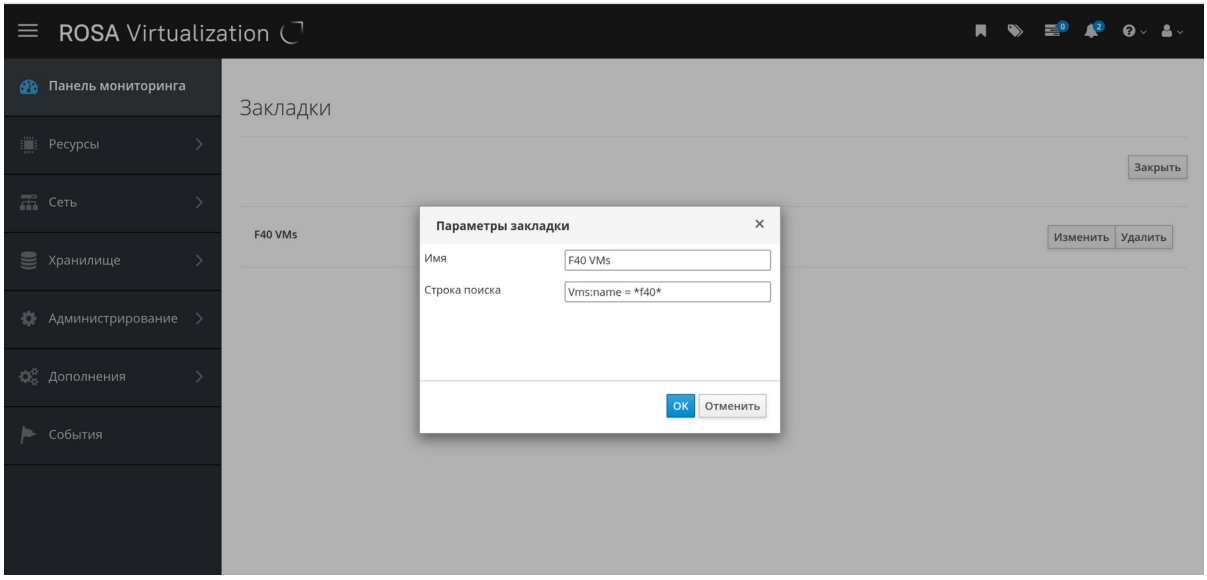

Рис. 58. Внесение изменений в закладку

4. Нажмите **OK** для сохранения изменений, или **Отменить** для отмены.

4.3. Удаление закладок

Если закладка больше не нужна, удалите её.

Удаление закладок

1. Нажмите на значок **Закладки** (🔖) на панели заголовков.
2. Выберите закладку (Рис. 57) и нажмите **Удалить**.
3. Нажмите **OK** для сохранения изменений, или **Отменить** для отмены**.**

В окне подтверждения удаления закладки (Рис. 59) укажите причину удаления (поле **Причина**; параметр опционален)

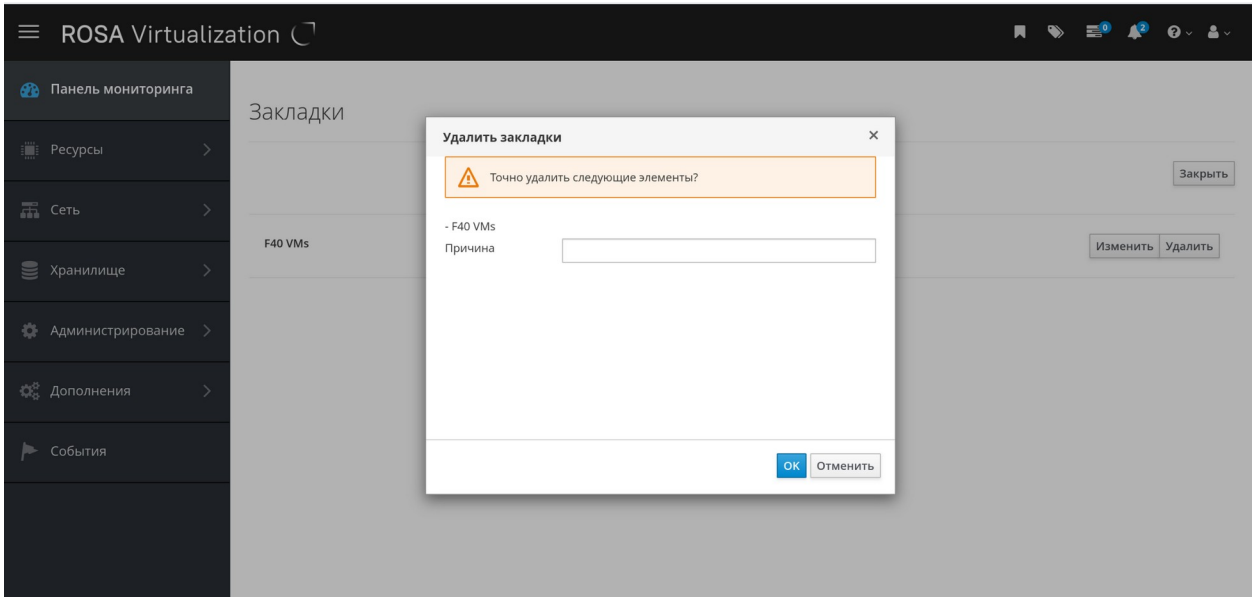

Рис. 59. Окно подтверждения удаления закладки

Глава 5. Теги

5.1. Настройка взаимодействия с системой виртуализации с помощью тегов

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

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

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

5.2. Создание тегов

Создание тега

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

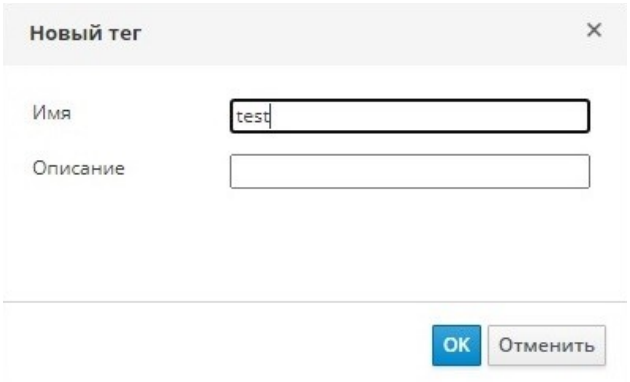

Рис. 60. Создание тега

5.3. Редактирование тегов

Название и описание тегов можно изменять.

Редактирование тега

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

5.4. Удаление тега

Удаление тега

1. Нажмите на значок **Теги** (🏷) на панели заголовков.
2. Выберите тег, который нужно удалить, и нажмите **Удалить**. Будет показано сообщение с предупреждением (Рис. 61) о том, что удаление метки (тега) также удалит все подчинённые метки.

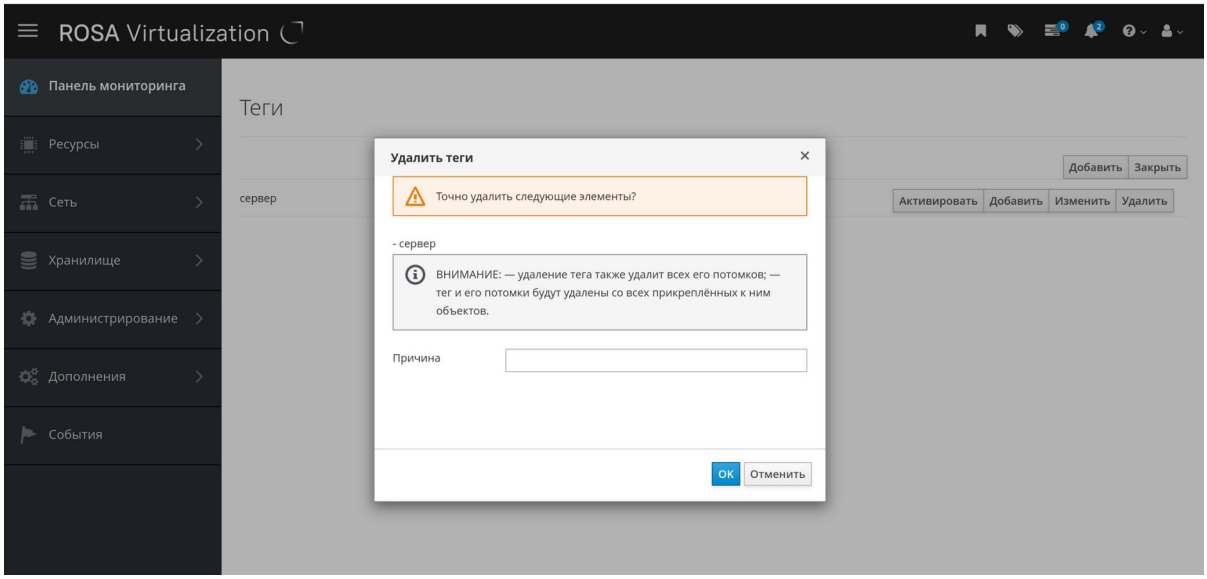

Рис. 61. Форма подтверждения удаления тега

3. Нажмите **OK**.

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

5.5. Присвоение тегов объектам и снятие меток с объектов

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

Присвоение тегов объектам и снятие тегов с объектов

1. Выберите объекты, которым нужно присвоить тег, или с которых нужно снять тег.
2. Нажмите **Больше действий** (⋮), а затем нажмите **Назначить теги** (Рис. 62).

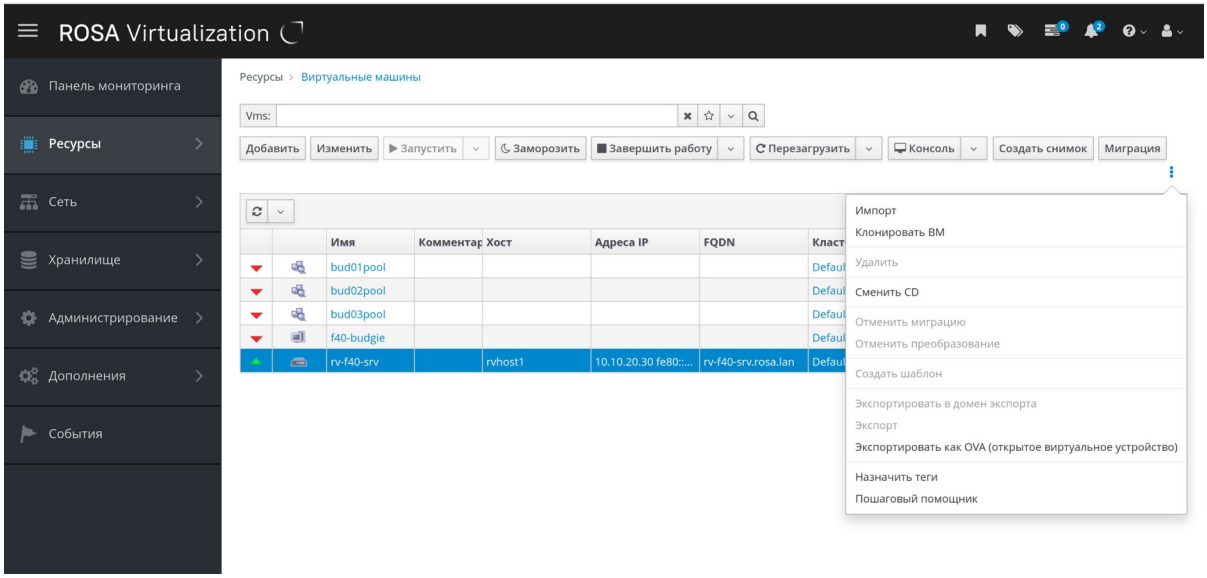

Рис. 62. Назначение тега виртуальной машине

3. Установите соответствующий флажок, чтобы присвоить тег объекту (Рис. 63), или снимите флажок, чтобы удалить тег объекта.

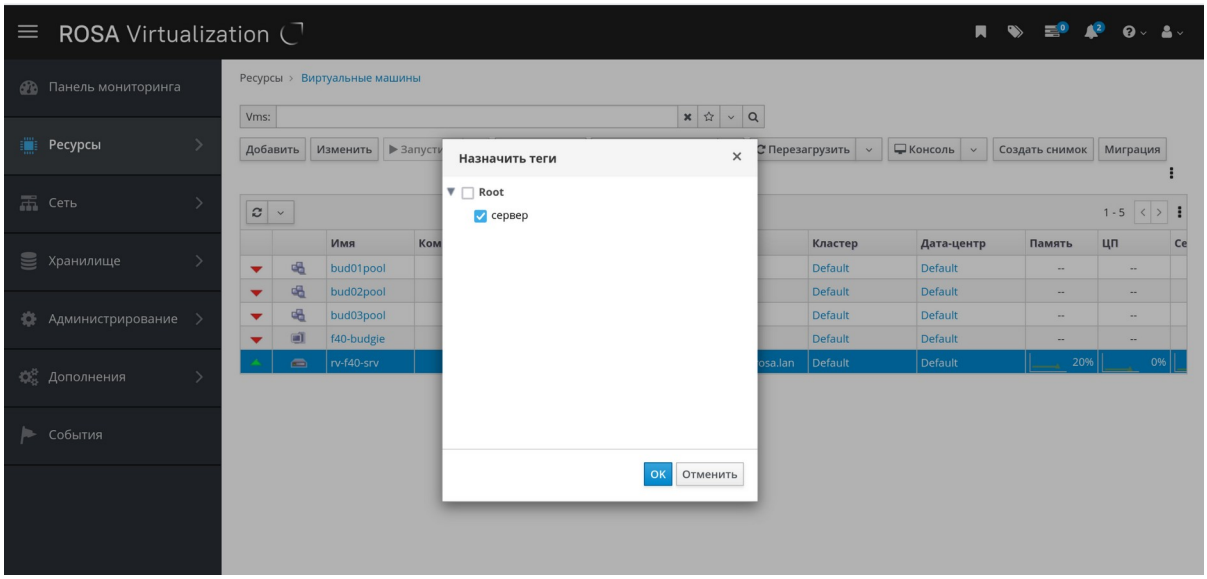

Рис. 63. Выбор тега и присвоение его объекту

4. Нажмите **OK**.

В результате указанные теги будут присвоены объектам в виде настраиваемого пользователем свойства (Рис. 64), или удалены.

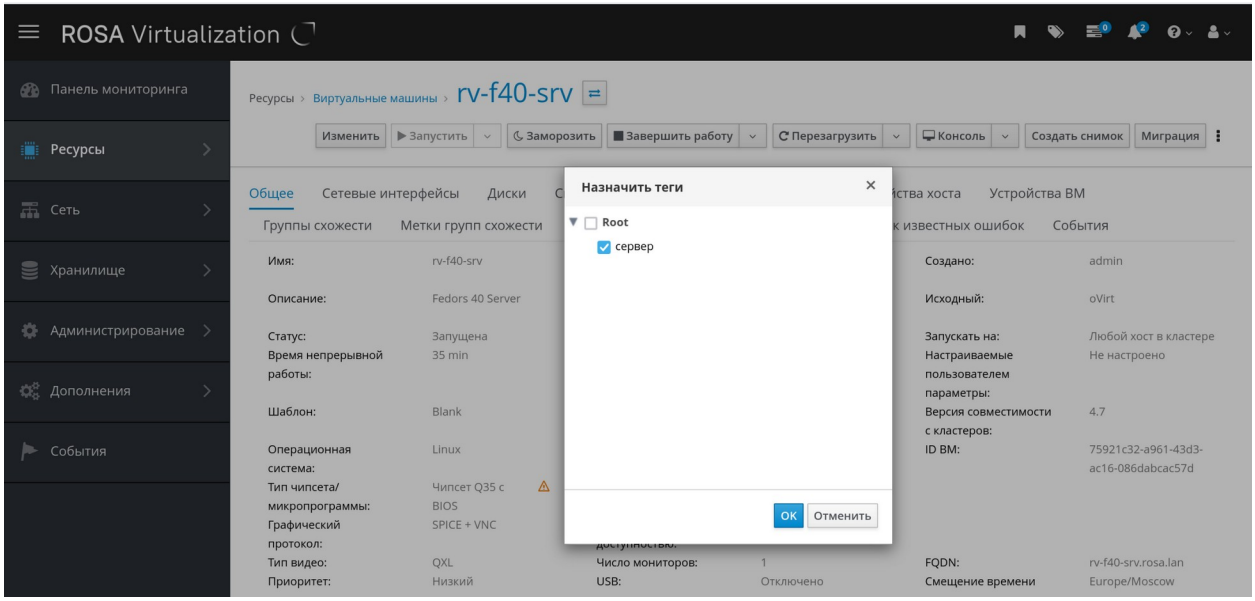

Рис. 64. ВМ с присвоенным ей тегом «сервер»

5.6. Поиск объектов на основе тегов

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

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

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

5.7. Сортировка хостов с помощью тегов

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

Настройка тегов для хостов

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

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

Часть II. Администрирование ресурсов
Глава 6. Качество обслуживания

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

6.1. Качество обслуживания хранилища

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

6.1.1. Создание записи о качестве обслуживания хранилища

Создание записи о качестве обслуживания хранилища

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра (Рис. 65) для открытия подробного просмотра.

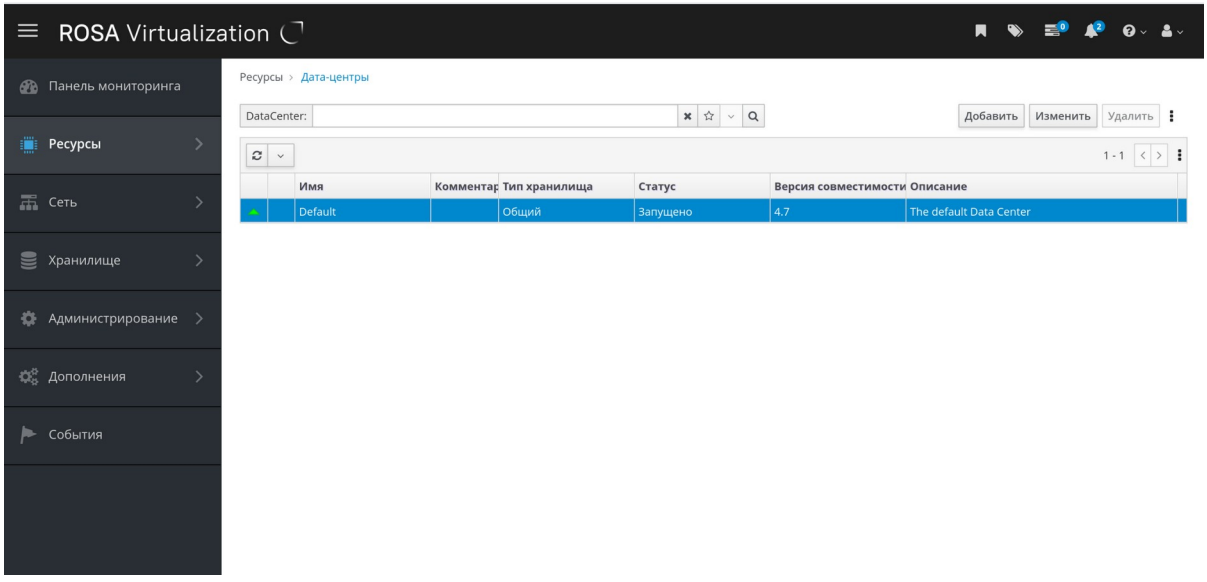

Рис. 65. Форма выбора доступных датацентров

3. Перейдите на вкладку **QoS** (Рис. 66).

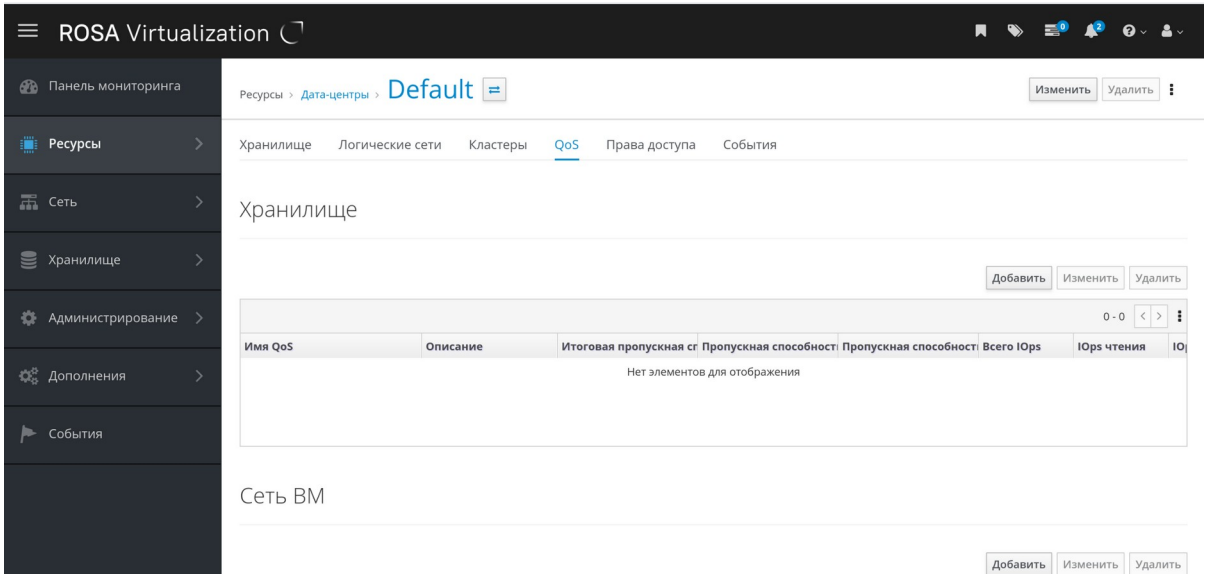

Рис. 66. Форма Дата-центры — вкладка QoS

4. В разделе **Хранилище** нажмите **Добавить** (Рис. 66).
5. Укажите **Имя QoS** и **Описание** (Рис. 67) для новой записи качества обслуживания.

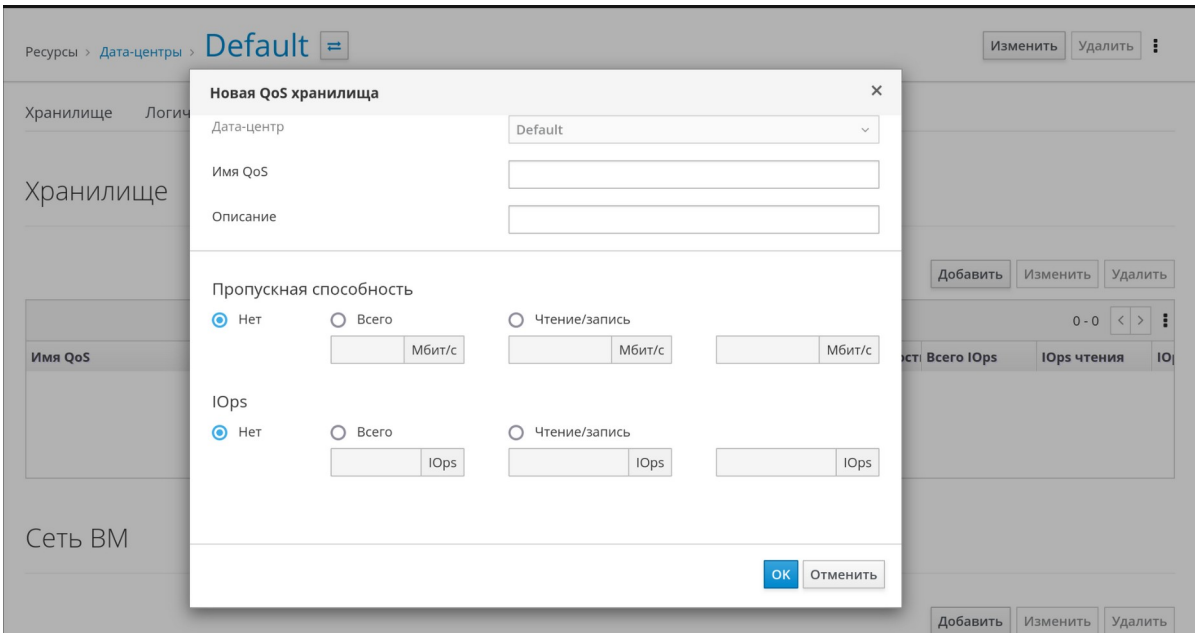

Рис. 67. Форма Новая QoS хранилища

6. Укажите **Пропускную способность** качества обслуживания, отметив один из переключателей:
   - **Нет**.
   - **Всего** — укажите максимально разрешённую общую пропускную способность в поле **Мбит/сек**.

- **Чтение/запись** — укажите максимально разрешённую общую пропускную способность для операций чтения в левом поле **Мбит/сек** и максимально разрешённую общую пропускную способность для операций записи в правом поле **Мбит/сек**.

7. Укажите качество обслуживания ввода и вывода (**IOps**), отметив один из переключателей:

   - **Нет**.
   - **Всего** — укажите максимальное разрешённое число операций ввода и вывода в секунду в поле **IOps**.
   - **Чтение/запись** — укажите максимальное разрешённое число операций ввода в секунду в левом поле **IOps** и максимальное разрешённое число операций вывода в секунду в правом поле **IOps**.
8. Нажмите **OK**.

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

6.1.2. Удаление записи о качестве обслуживания хранилища

Удаление записи качества обслуживания хранилища

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

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

6.2. Качество обслуживания сети виртуальной машины

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

6.2.1. Создание записи о качестве обслуживания сети ВМ

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

Создание записи о качестве обслуживания сети ВМ

1. Нажмите **Ресурсы → Дата-центры**.

2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS**.
4. В разделе **Сеть ВМ** нажмите **Добавить** (Рис. 68).

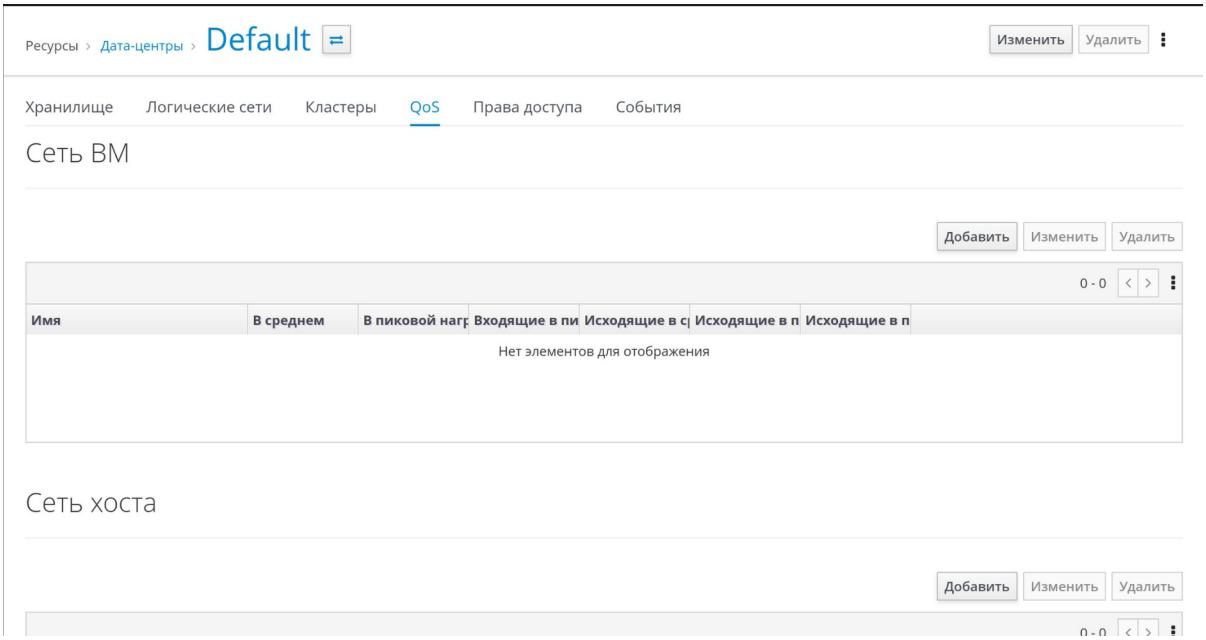

Рис. 68. Добавление QoS для Сеть ВМ

5. В окне **Новая QoS сети ВМ** введите **Имя** записи QoS сети ВМ (Рис. 69).

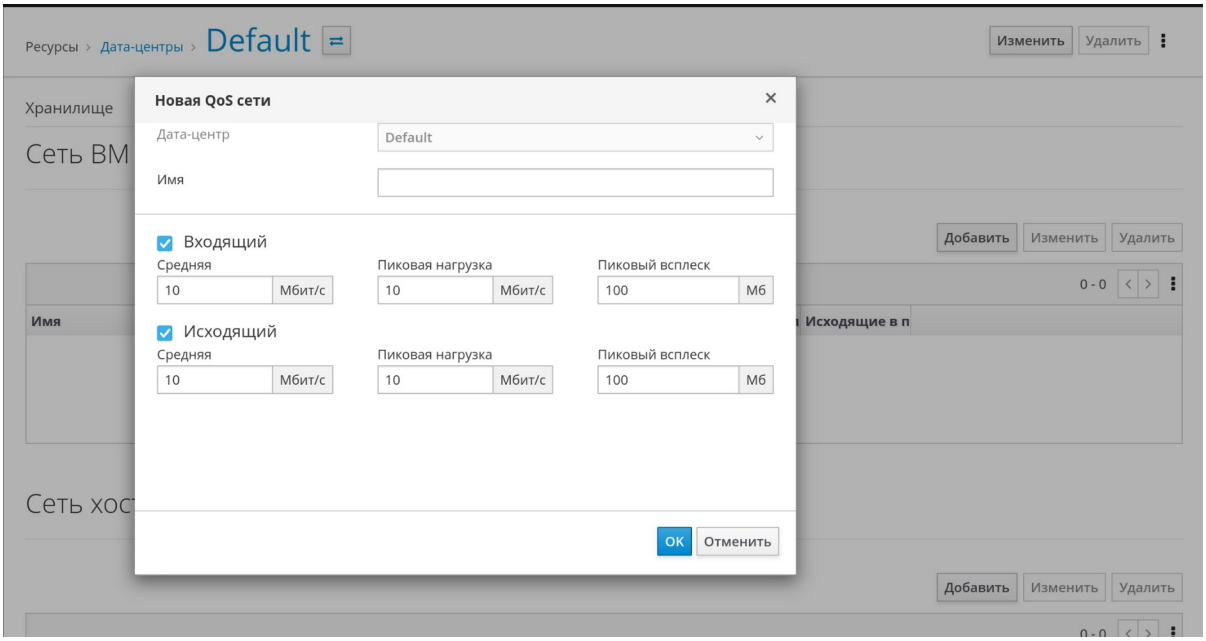

Рис. 69. Новая QoS сети

6. Укажите лимиты для **Входящего** и **Исходящего** сетевого трафика.
7. Нажмите **OK**.

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

6.2.2. Параметры в окне «Новая QoS сети ВМ»

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

Табл. 6.1. Параметры QoS сети ВМ

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

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

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

6.2.3. Удаление записи о качестве обслуживания сети ВМ

Удаление записи о качестве обслуживания сети ВМ

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

6.3. Качество обслуживания сетей хоста

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

6.3.1. Создание записи о качестве обслуживания для сетей хоста

Создание записи о качестве обслуживания для сетей хоста

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS**.
4. В разделе **Сеть хоста** нажмите **Добавить** (Рис. 70).

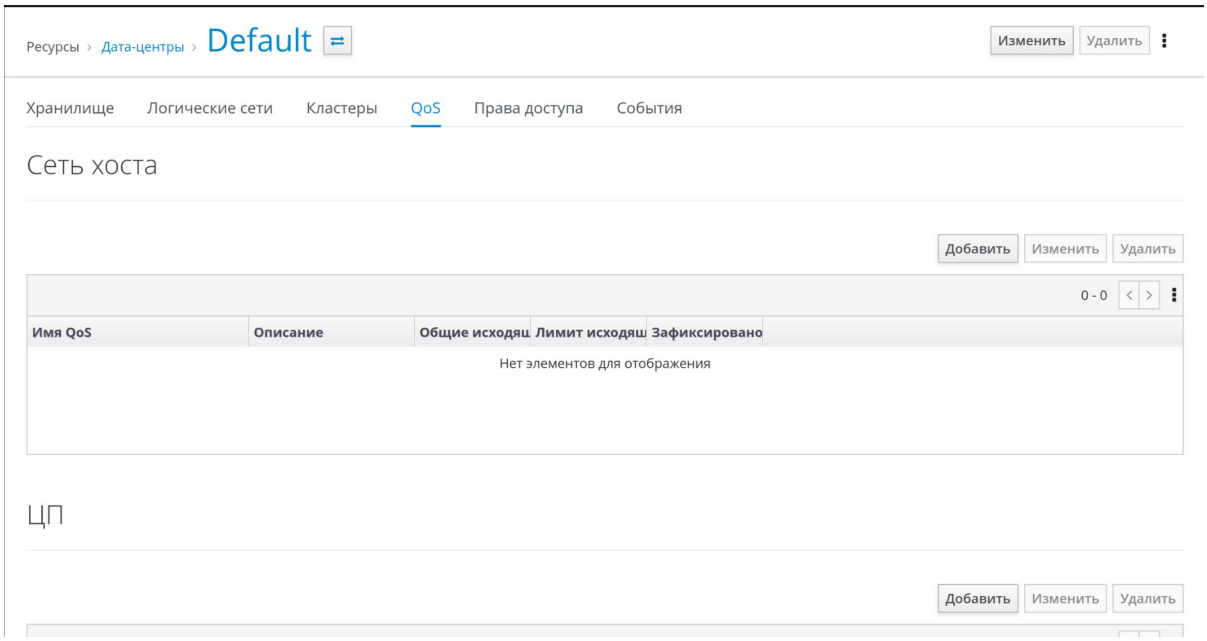

Рис. 70. QoS - Сеть хоста

5. В окне **Новая QoS сети хоста** введите **Имя QoS** и **Описание** для записи о качестве обслуживания.

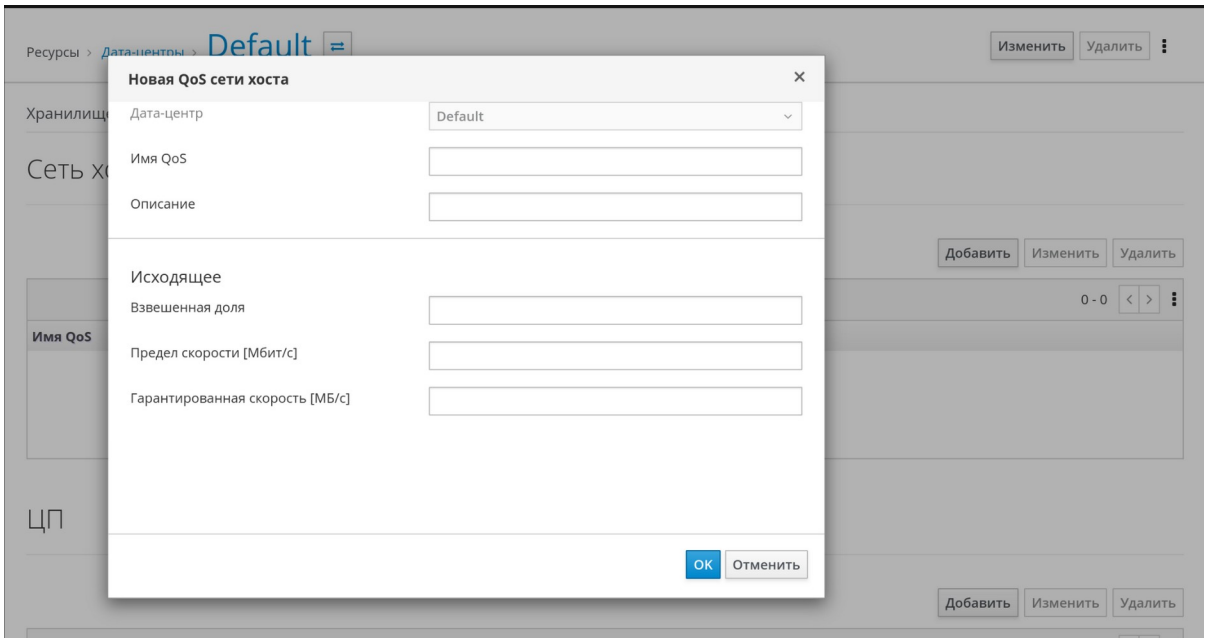

Рис. 71. Форма Новая QoS сети хоста

6. Укажите нужные значения **Взвешенной доли**, **Предела скорости** (Мбит/с) и **Гарантированной скорости** (МБ/с).
7. Нажмите **OK**.

6.3.2. Параметры в окне «Новая QoS сети хоста»

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

Табл. 6.2. Параметры QoS сетей хоста

Поле	Описание
Дата-центр	Дата-центр, в который будет добавлена политика QoS сетей хоста. Это поле настраивается автоматически согласно выбранному дата-центру
Имя QoS	Название, представляющее политику QoS в виртуализированном ЦУ
Описание	Описание политики QoS сетей хоста
Исходящее	Параметры, которые будут применяться к исходящему трафику: • **Взвешенная доля**: определяет, какую долю пропускной способности логического канала нужно выделить для конкретной сети относительно других сетей, привязанных к тому же логическому каналу. Точная доля зависит от

Поле	Описание
	суммы долей всех сетей на этом канале. По умолчанию, это число в диапазоне от 1 до 100. • **Предел скорости (Мбит/с)**: максимальная пропускная способность, используемая сетью. • **Гарантированная скорость (МБ/с)**: минимальная пропускная способность, требуемая для сети. Запрошенная скорость не является гарантированной и будет меняться в зависимости от сетевой инфраструктуры и гарантированных скоростей, запрошенных другими сетями на том же логическом канале.

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

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

6.3.3. Удаление записи о качестве обслуживания для сетей хоста

Удаление записи о качестве обслуживания для сетей хоста

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

6.4. Качество обслуживания ЦП

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

6.4.1. Создание записи качества обслуживания для ЦП

Создание записи качества обслуживания для центрального процессора

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра для открытия подробного просмотра.
3. Перейдите на вкладку **QoS**.
4. В разделе **ЦП** нажмите **Добавить** (Рис. 72).

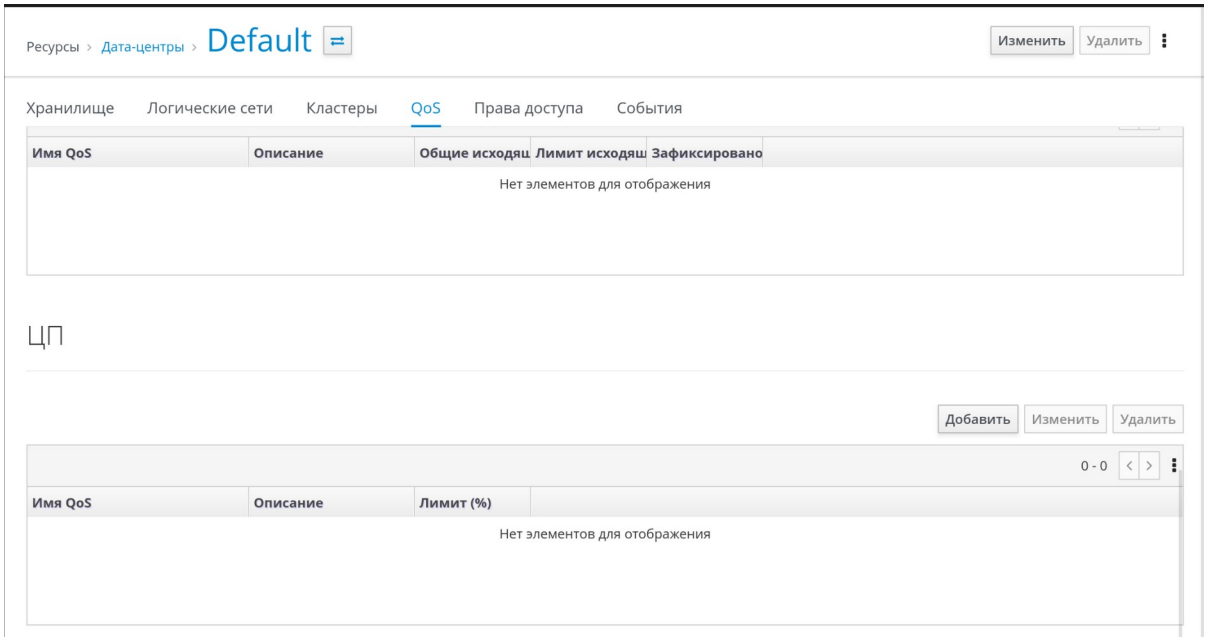

Рис. 72. QoS ЦП

5. В окне **Новая QoS ЦП** введите **Имя QoS** и **Описание** для записи о качестве обслуживания.

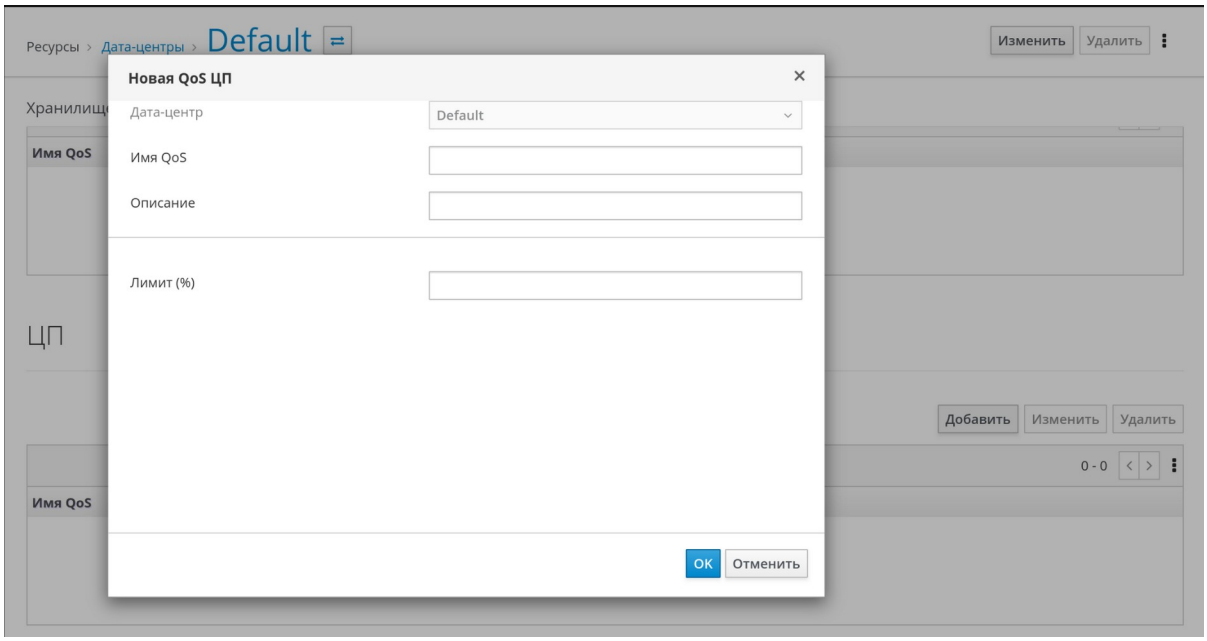

Рис. 73. Новая QoS ЦП

6. В поле **Лимит (%)** введите максимальную вычислительную возможность, разрешаемую записью QoS (при этом не указывайте символ %).
7. Нажмите **OK**.

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

6.4.2. Удаление записи качества обслуживания для ЦП

Удаление записи QoS для центрального процессора

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

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

Глава 7. Дата-центры

7.1. Введение в понятие дата-центров

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

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

Все дата-центры управляются средствами одного **Портала администрирования**.

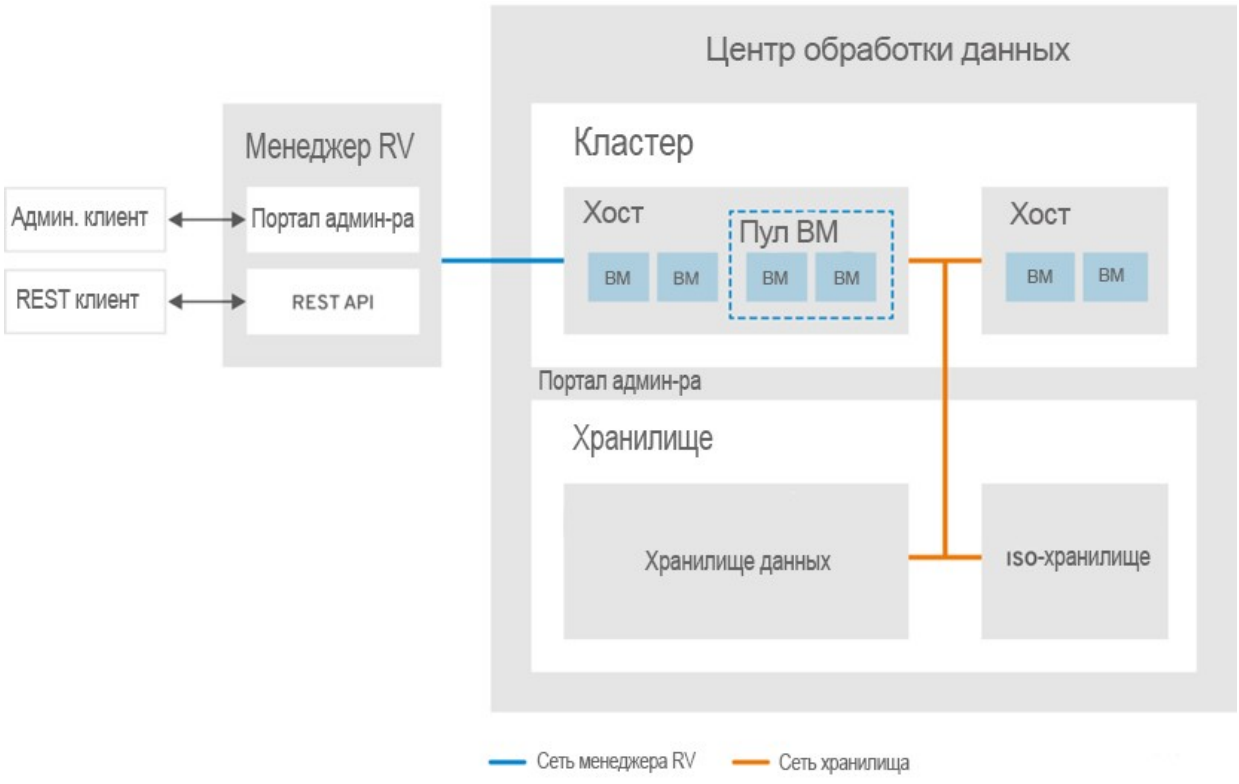

Рис. 74. Дата-центры

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

7.2. Диспетчер пула хранилища (SPM)

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

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

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

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

7.3. Приоритет диспетчера пула хранилища

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

Приоритет SPM для хоста можно изменить на вкладке **SPM** в окне **Параметры хоста** (Рис. 75).

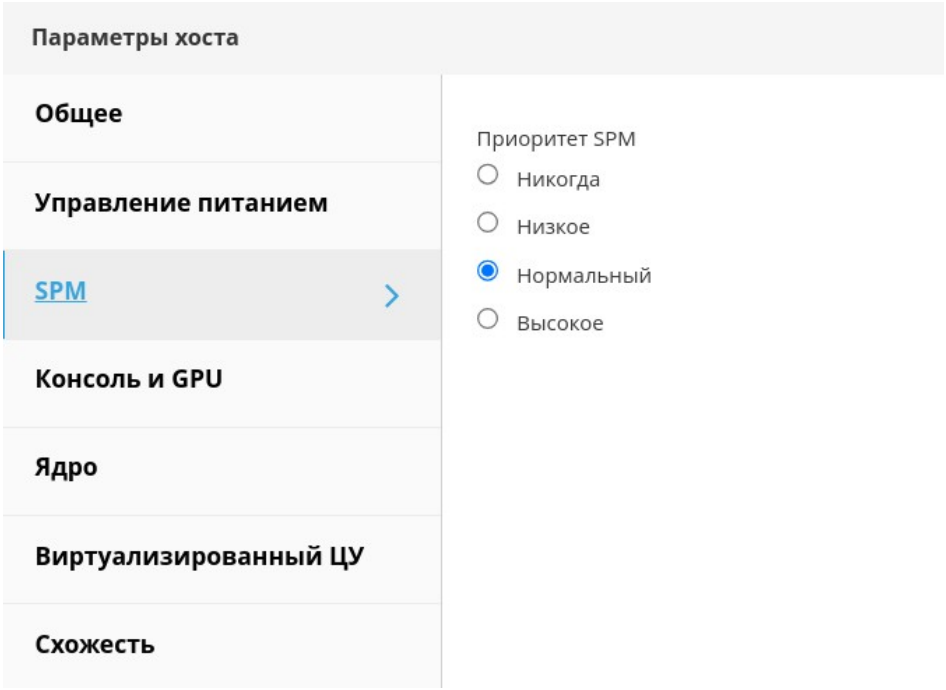

Рис. 75. Параметры хоста

7.4. Задачи при работе с дата-центрами

7.4.1. Создание нового дата-центра

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

Создание нового дата-центра

1. Нажмите **Ресурсы** → **Дата-центры** (Рис. 76). Откроется окно со списком доступных дата-центров.

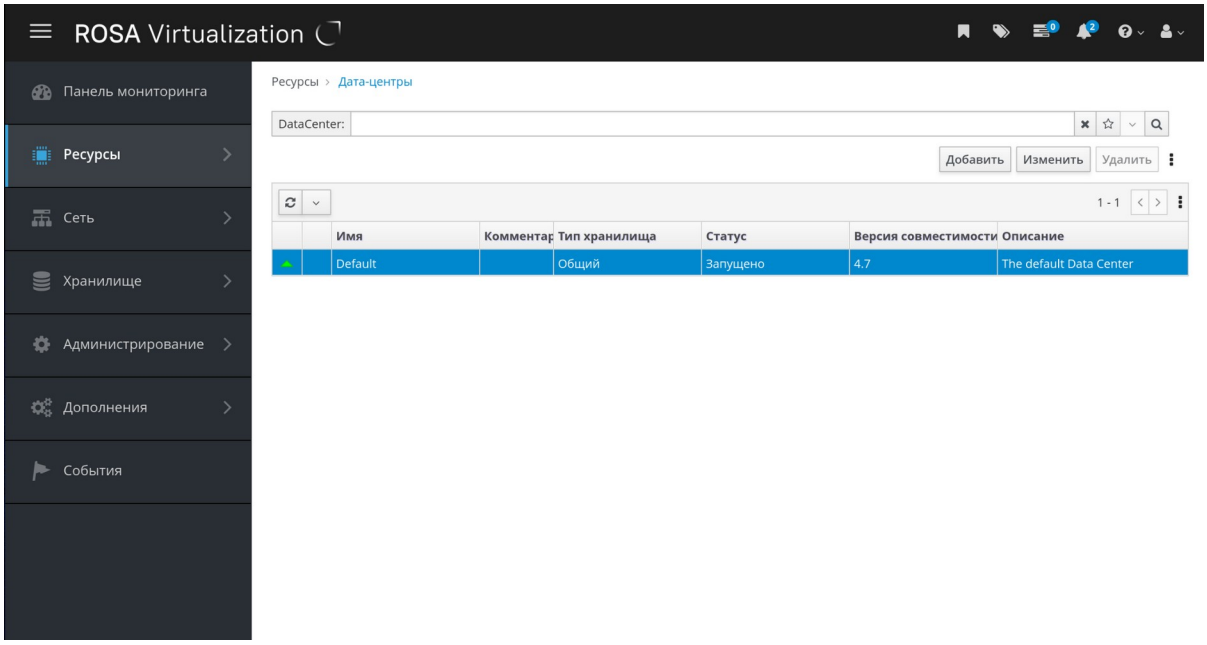

Рис. 76. Форма Ресурсы → Дата-центры

2. Нажмите **Добавить**.
3. В окне **Новый дата-центр** (Рис. 77) укажите **Имя** и **Описание** дата-центра.

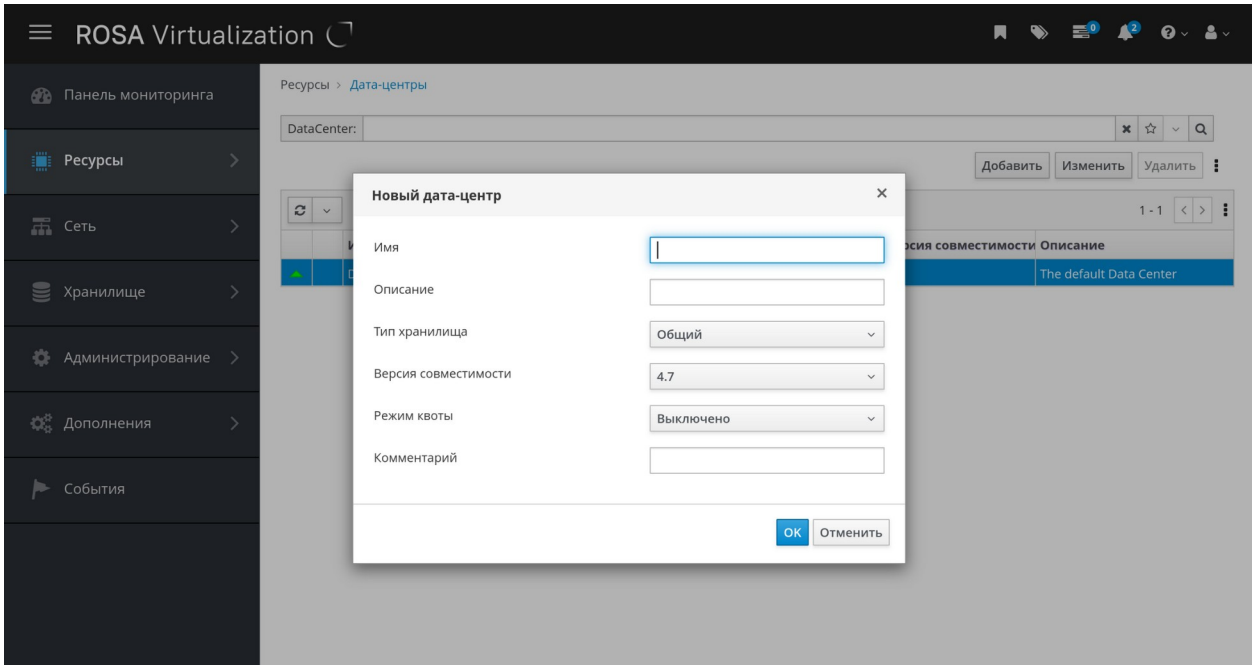

Рис. 77. Создание нового дата-центра

4. В выпадающих меню выберите **Тип хранилища** (Рис. 78), **Версию совместимости** (Рис. 79) и **Режим квоты** (Рис. 80) дата-центра.

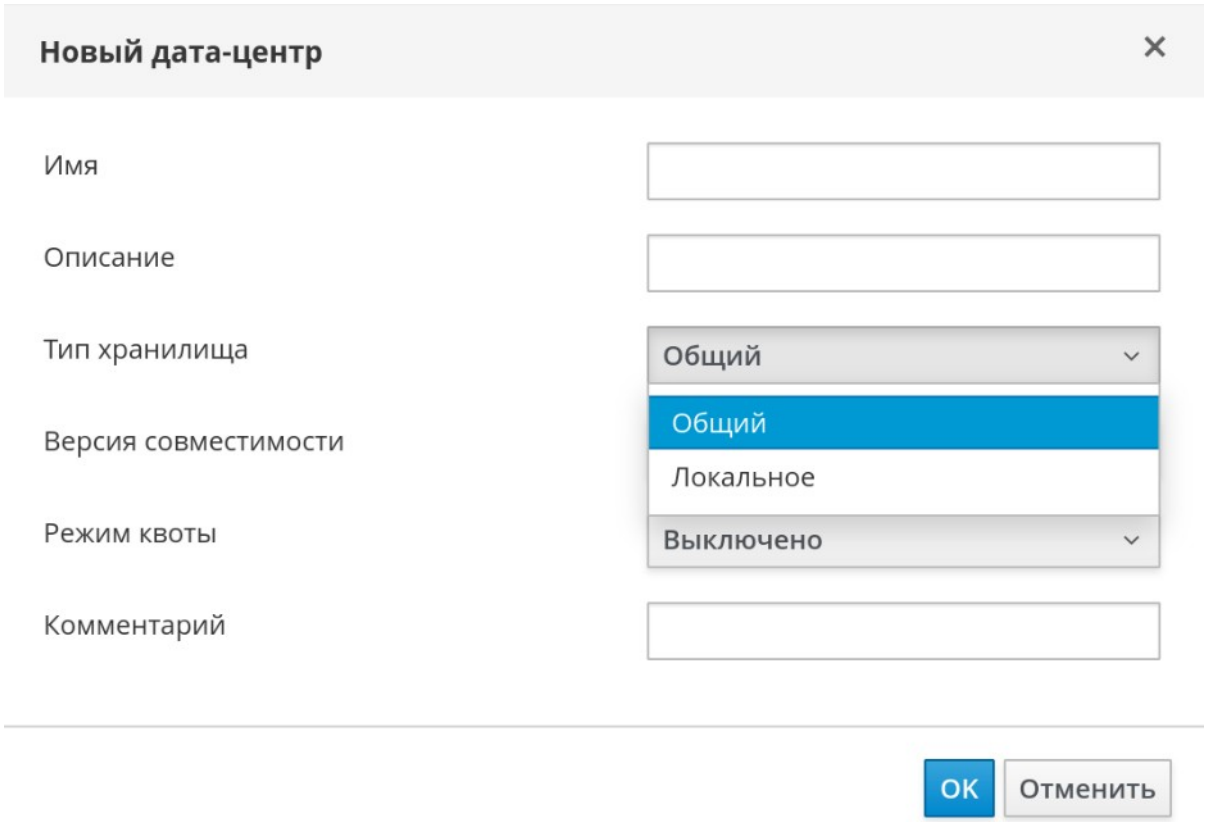

Рис. 78. Новый дата-центр - Тип хранилища

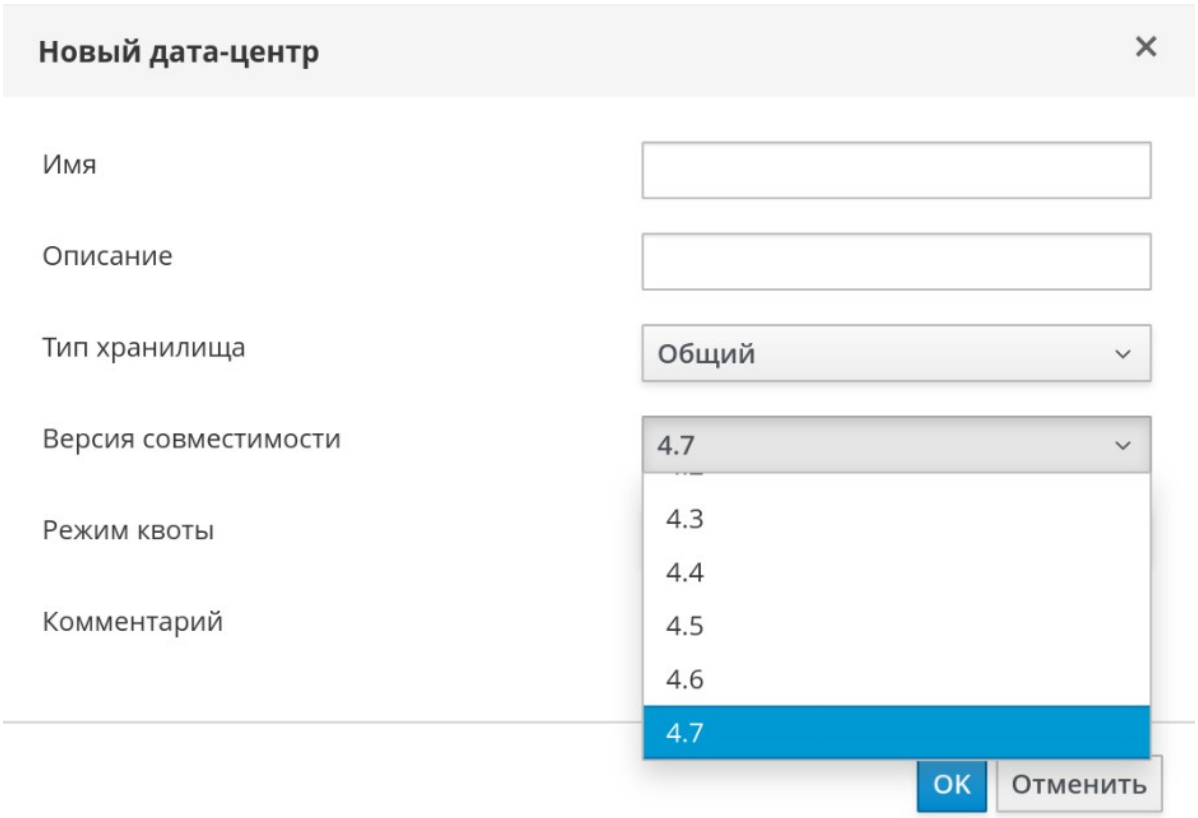

Рис. 79. Новый дата-центр - Версия совместимости

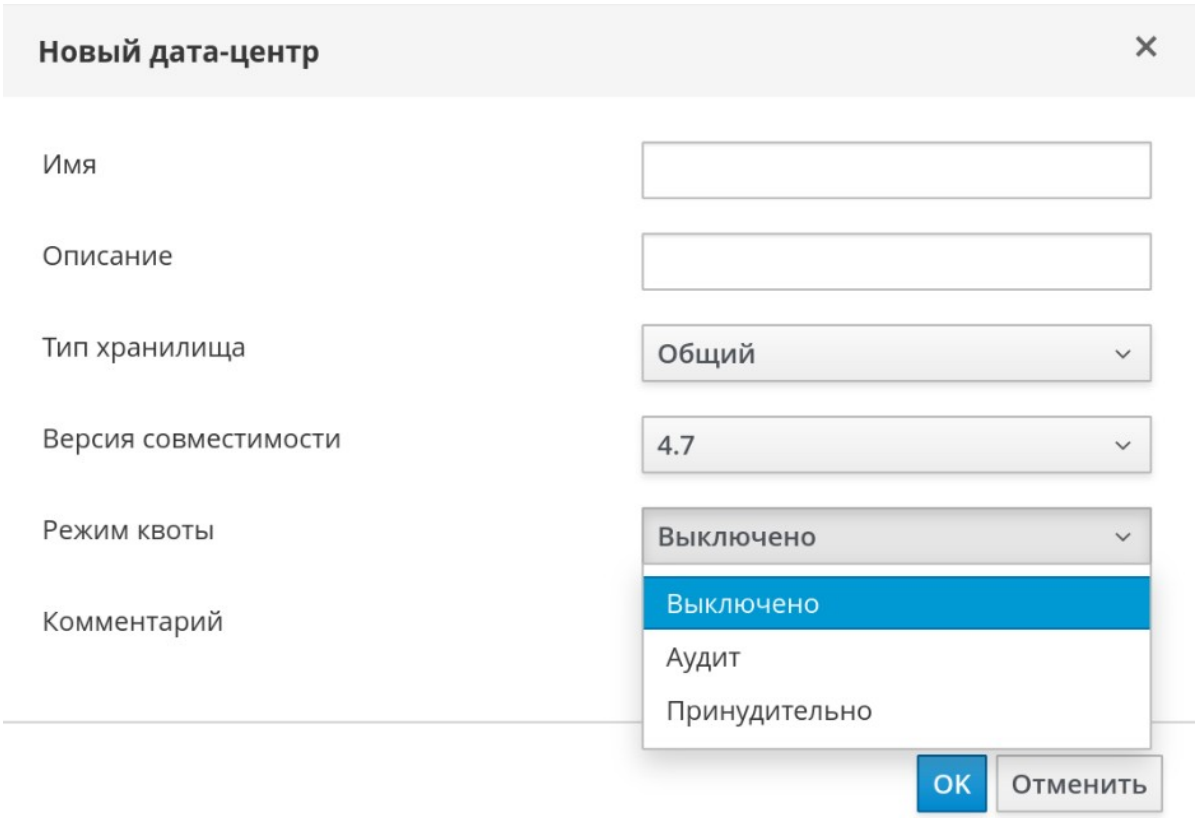

Рис. 80. Новый дата-центр - Режим квоты

5. Для создания дата-центра нажмите **OK** и перейдите в окно **Дата-центр — пошаговый помощник** (Рис. 81).

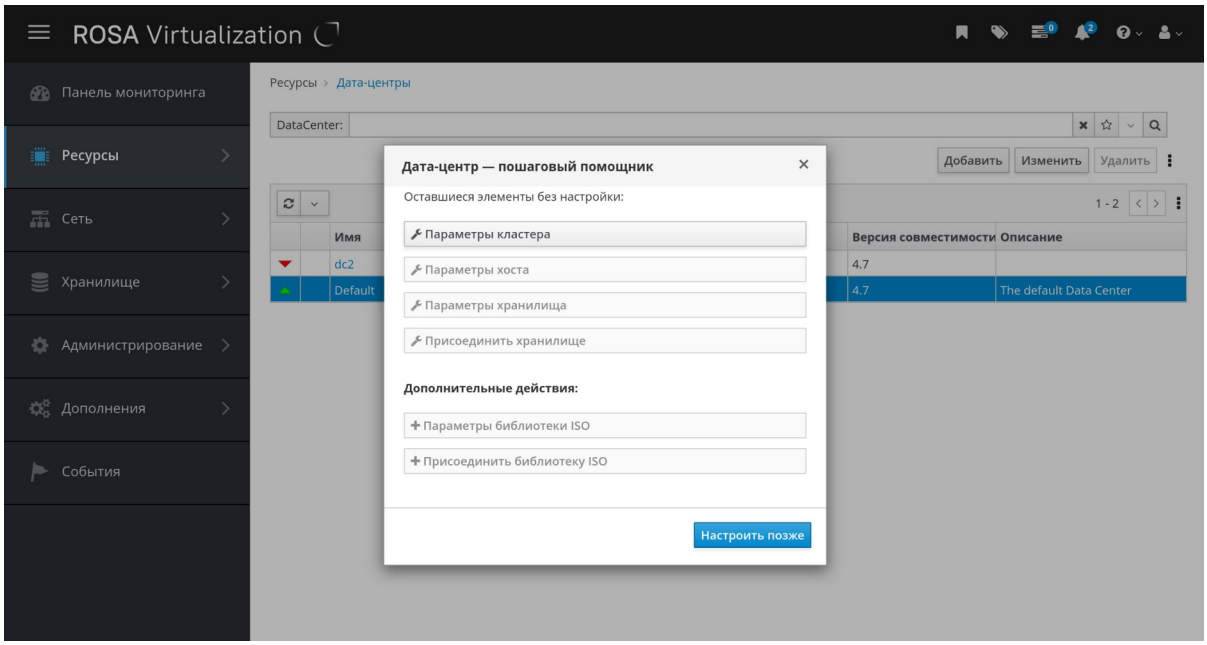

Рис. 81. Окно Дата-центр — пошаговый помощник

6. В окне пошагового помощника присутствует список объектов дата-центра, которые необходимо настроить. Настройте их или отложите настройку, нажав на кнопку **Настроить позже**. Возобновить процесс настройки можно, выбрав дата-центр и перейдя по пунктам меню **Больше действий** (⋮) → **Пошаговый помощник**.

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

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

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

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

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

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

Табл. 7.1. Параметры дата-центра

Поле	Описание / действие
Имя	Название дата-центра. У этого текстового поля имеется ограничение в 40 символов, а введённое название должно быть уникальным сочетанием любых строчных или прописных букв, цифр, дефисов и знаков подчёркивания
Описание	Описание дата-центра. Заполнение этого поля рекомендуется, но не обязательно
Тип хранилища	Выберите тип хранилища: **Общий** (разделяемый) или **Локальное**. В один и тот же дата-центр можно добавить различные типы доменов хранилищ (iSCSI, NFS, FC, POSIX, Gluster). Тем не менее, локальные и разделяемые домены нельзя смешивать. Изменить тип хранилища можно после инициализации дата-центра
Версия совместимости	Версия системы виртуализации ROSA Virtualization. После обновления виртуализированного ЦУ до новой версии, хосты, кластеры и дата-центры по-прежнему могут иметь более раннюю версию. Перед обновлением до новой версии **Уровня совместимости** дата-центра убедитесь в том, что были обновлены версии всех хостов, а затем кластеров

Поле	Описание / действие
Режим квоты	Режим квоты — это инструмент ограничения использования ресурсов в составе системы виртуализации ROSA Virtualization. Выберите одно из следующих значений: • **Выключено**: выберите, если не нужно использовать квоты. • **Аудит**: выберите, если нужно изменить параметры квоты. • **Принудительно**: выберите для применения квоты.
Комментарий	По желанию добавьте комментарий о дата-центре в простом текстовом формате

7.4.3. Повторная инициализация дата-центра (процедура восстановления)

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

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

Повторная инициализация дата-центра

1. Нажмите **Ресурсы → Дата-центры** и выберите нужный дата-центр (Рис. 82).
2. Убедитесь в том, что любые домены хранилищ, присоединённые к дата-центру, находятся в режиме обслуживания.
3. Нажмите значок **Больше действий** (⋮), затем пункт **Повторно инициализировать дата-центр**.
4. В окне **Повторная инициализация дата-центра** располагается список всех доступных (отсоединённых, в режиме обслуживания) доменов хранилищ. Установите флажок для домена хранилища, добавляемого в дата-центр.
5. Установите флажок **Подтвердить операцию**.
6. Нажмите **OK**.

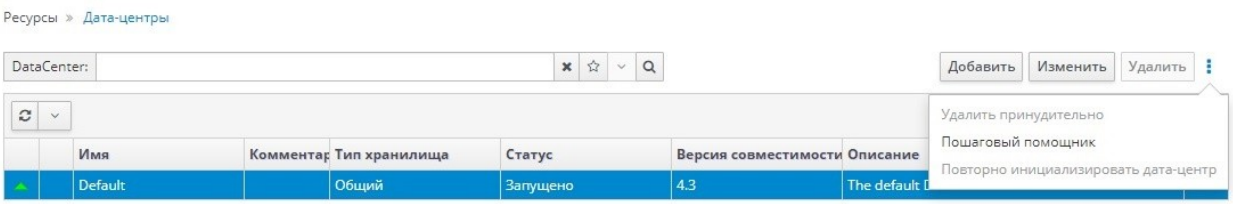

Рис. 82. Повторная инициализация дата-центра

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

7.4.4. Удаление дата-центра

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

Удаление дата-центра

1. Убедитесь в том, что домены хранилищ, присоединённые к дата-центру, находятся в режиме обслуживания.
2. Нажмите **Ресурсы** → **Дата-центры** и выберите дата-центр, который нужно удалить.
3. Нажмите **Удалить**. Откроется форма **Удалить дата-центр(ы)** (Рис. 83), подтвердите удаление дата-центра в данной форме, нажав **OK**, или нажмите **Отменить** для отмены.

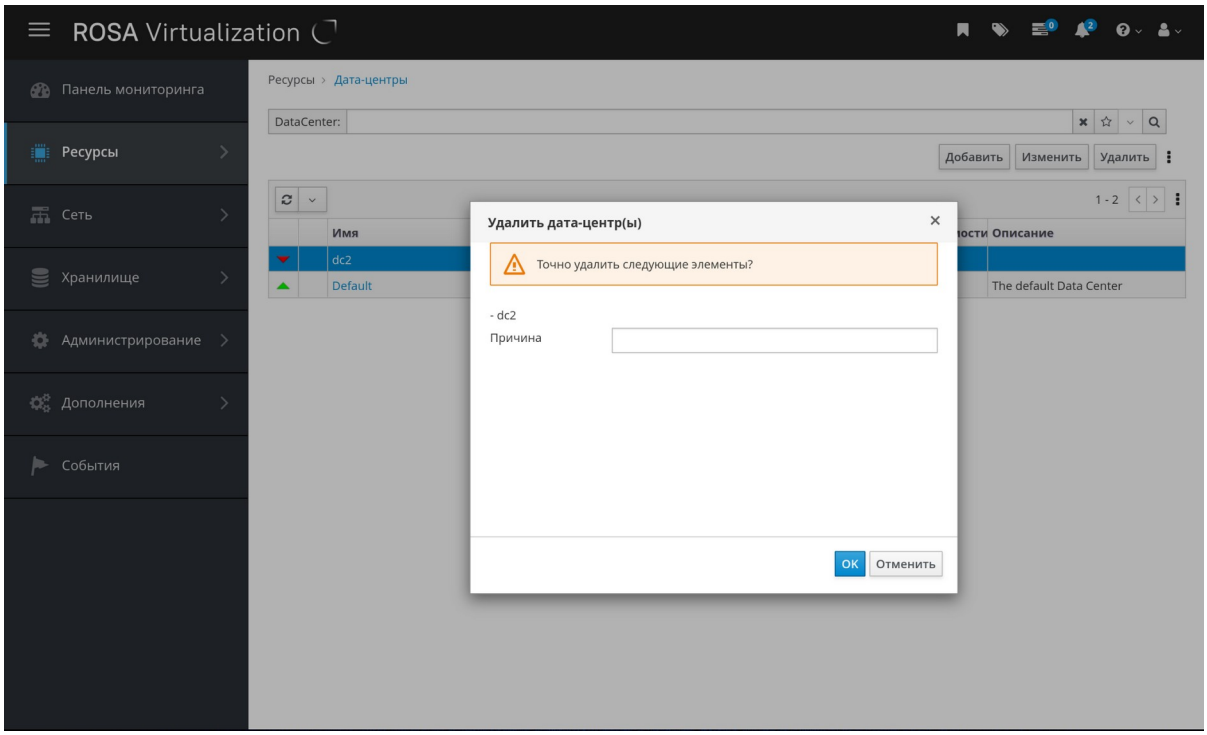

Рис. 83. Подтверждение удаления дата-центра

4. После нажатия на **OK** выбранный дата-центр будет удален.

7.4.5. Принудительное удаление дата-центра

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

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

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

Принудительное удаление дата-центра

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

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

7.4.6. Изменение типа хранилища дата-центра

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

Изменение типа хранилища имеет следующие ограничения**:**

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

Изменение типа хранилища дата-центра

1. Нажмите **Ресурсы** → **Дата-центры** и выберите дата-центр, который нужно изменить.
2. Нажмите **Изменить**.
3. Измените **Тип хранилища**.
4. Нажмите **ОК**.

7.4.7. Изменение версии совместимости дата-центра

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

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

Изменение версии совместимости дата-центра

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

7.5. Дата-центры и домены хранилищ

7.5.1. Добавление существующего домена данных к дата-центру

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

Добавление существующего домена данных к дата-центру

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра, чтобы открыть подробные сведения.
3. Перейдите на вкладку **Хранилище** (Рис. 84), чтобы просмотреть список доменов, уже присоединённых к дата-центру.
4. Нажмите **Присоединить данные**.
5. Установите флажок напротив домена данных, который нужно присоединить к дата-центру (при необходимости выберите несколько доменов данных).
6. Нажмите **OK**.

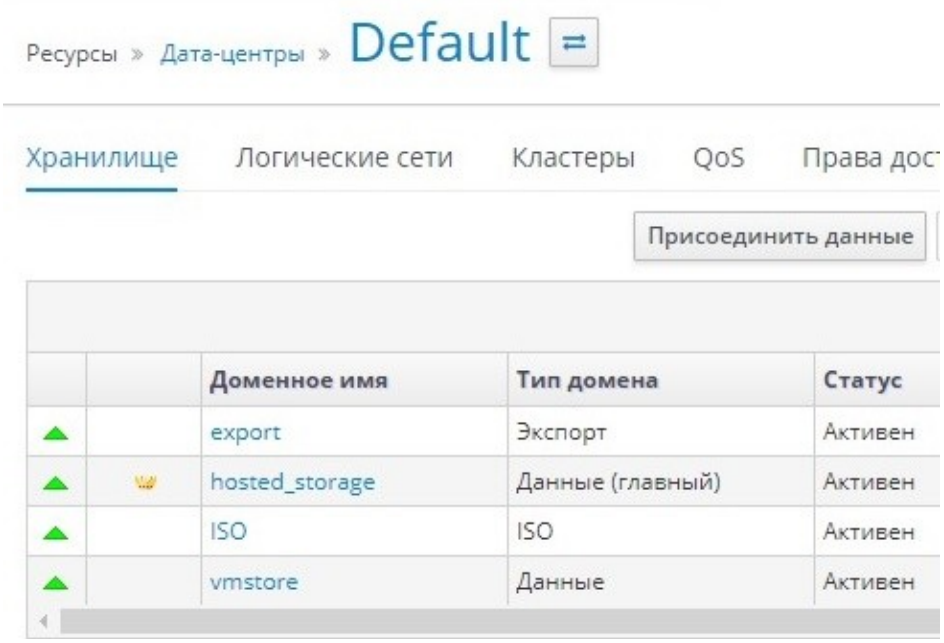

Рис. 84. Добавление существующего домена данных к дата-центру

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

7.5.2. Добавление существующего домена ISO к дата-центру

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

Добавление существующего домена ISO к дата-центру

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра, чтобы открыть подробные сведения.

3. Перейдите на вкладку **Хранилище**, чтобы просмотреть список доменов, уже присоединённых к дата-центру.
4. Нажмите **Присоединить ISO**.
5. Установите флажок напротив нужного домена ISO.
6. Нажмите **OK**.

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

7.5.3. Присоединение существующего домена экспорта к дата-центру

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

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

Присоединение существующего домена экспорта к дата-центру

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

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

7.5.4. Отсоединение доменов хранилищ от дата-центра

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

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

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

Отсоединение домена хранилища от дата-центра

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра, чтобы открыть подробные сведения.
3. Перейдите на вкладку **Хранилище**, чтобы просмотреть список доменов, уже присоединённых к дата-центру (Рис. 85).

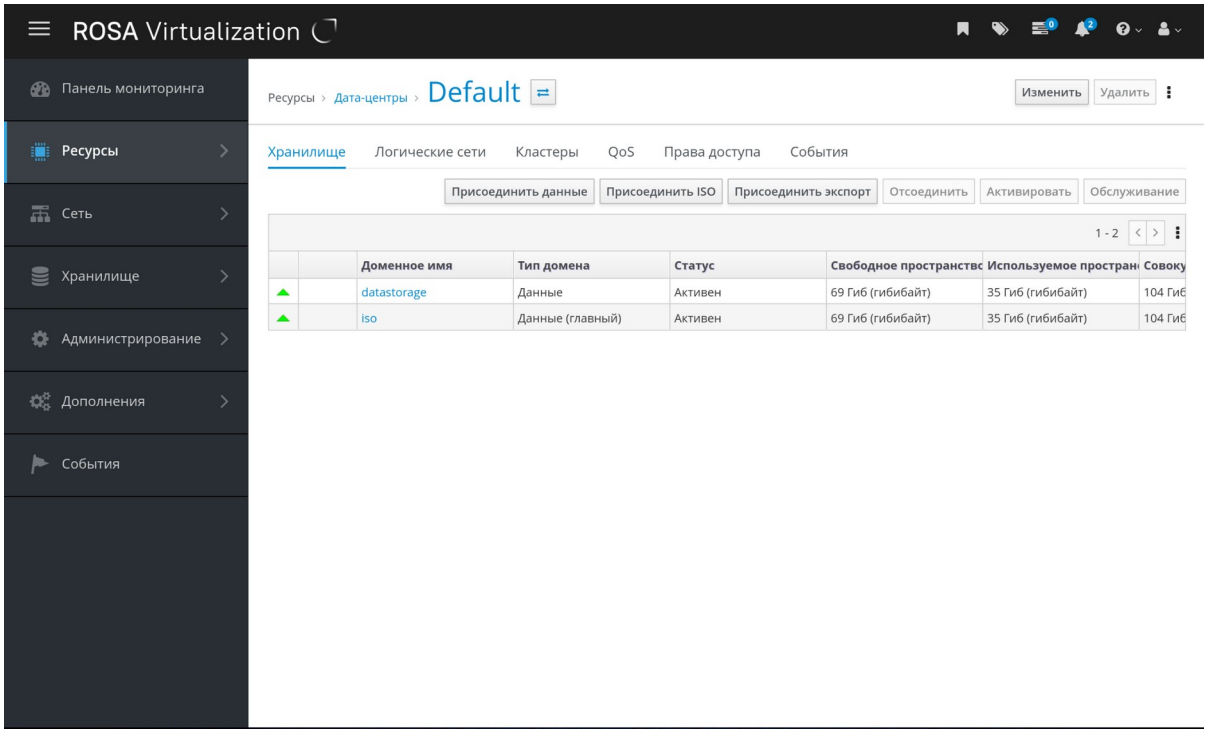

Рис. 85. Домены хранилища, присоединенные к дата-центру

4. Выберите домен хранилища, который надо отсоединить. Если домен *Активен*, нажмите **Обслуживание**.

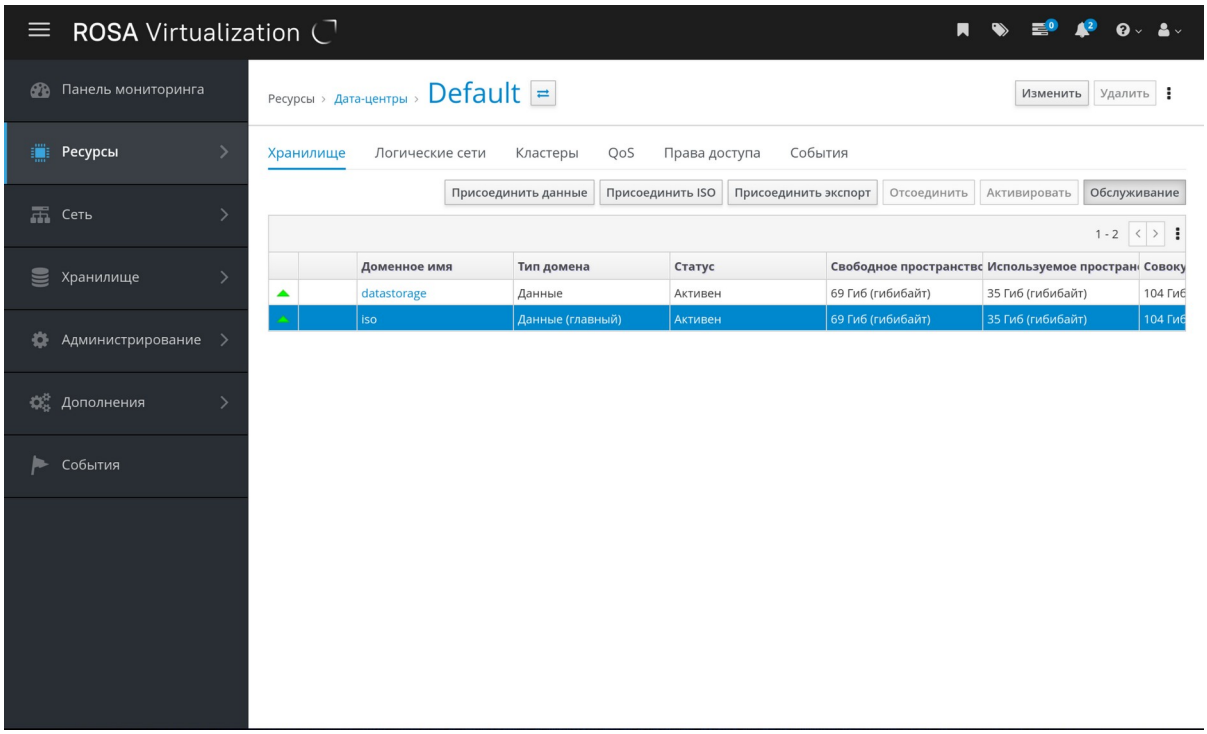

Рис. 86. Запуск режима Обслуживание для выбранного домена

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

6. Нажмите **Отсоединить**.
7. Нажмите **ОК**.

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

Глава 8. Кластеры

8.1. Введение в понятие кластеров

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

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

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

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

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

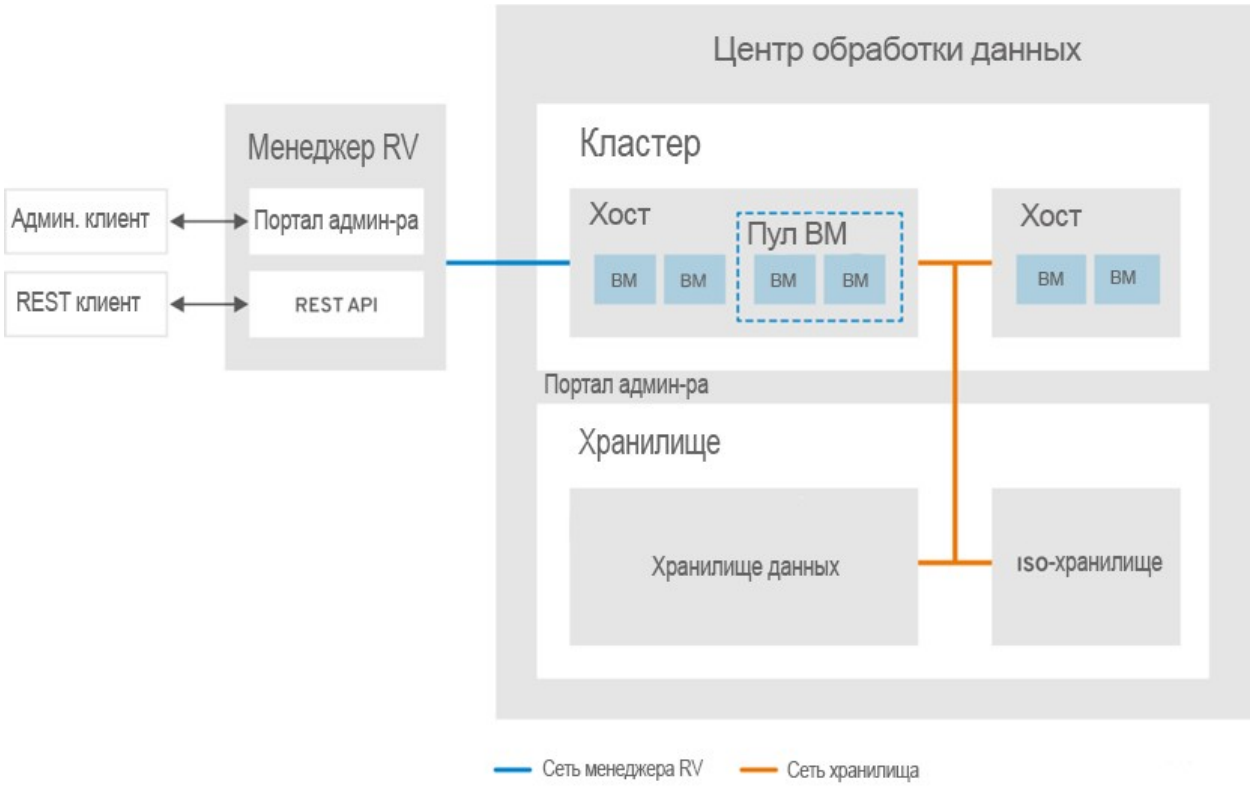

Рис. 87. Кластер в Центре обработки данных

8.2. Задачи при работе с кластерами

Примечание — некоторые параметры кластера не применимы к кластерам Gluster.

8.2.1. Создание нового кластера

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

Создание нового кластера

1. Нажмите **Ресурсы → Кластеры**.
2. Нажмите **Добавить**.

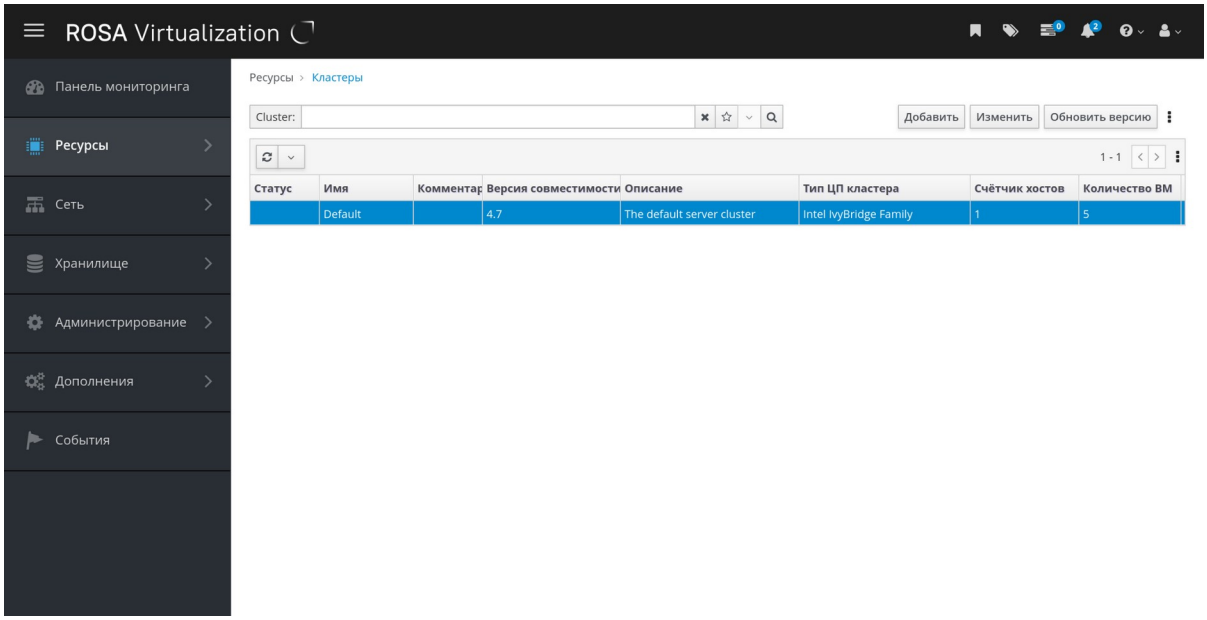

Рис. 88. Список доступных кластеров, форма управления кластерами

3. В выпадающем списке выберите **Дата-центр**, к которому будет принадлежать кластер.

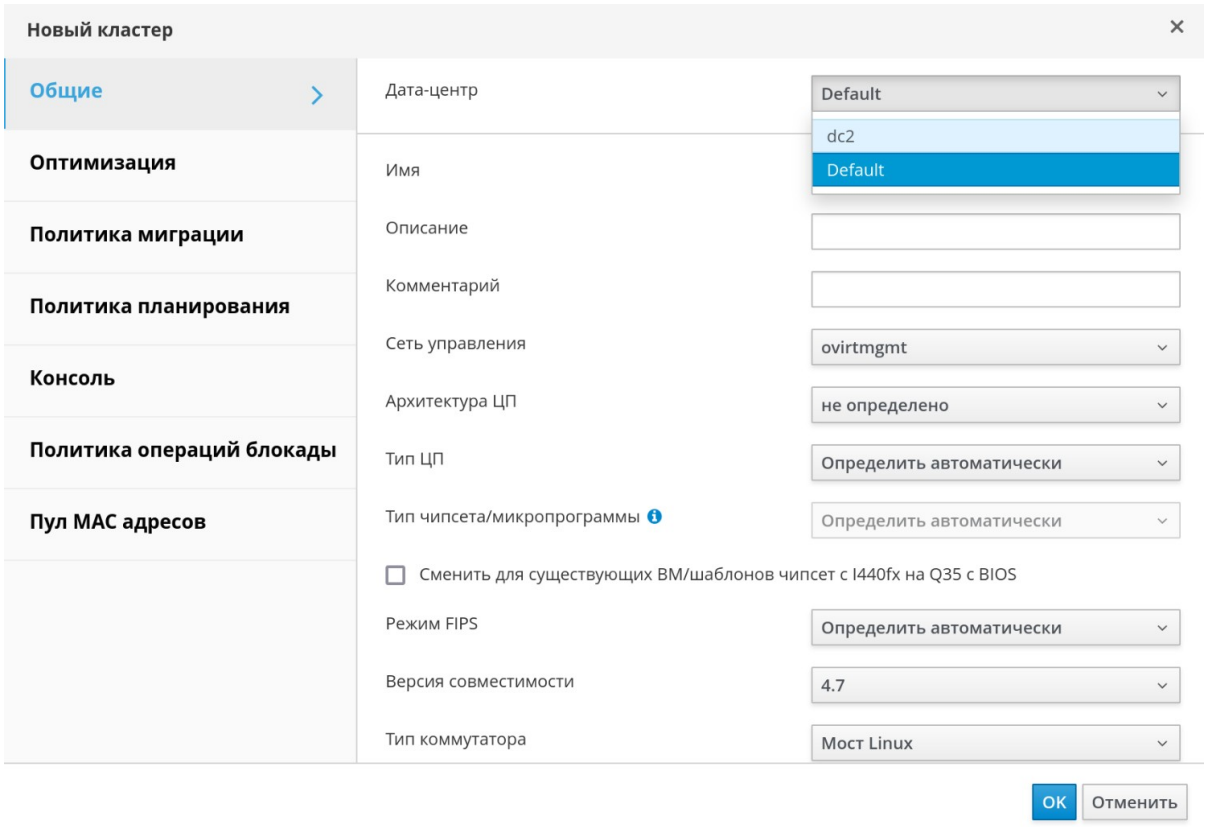

Рис. 89. Выбор дата-центра для кластера

4. Укажите **Имя** и **Описание** кластера.
5. В выпадающем списке **Сеть управления** выберите сеть, которой нужно присвоить роль сети управления.
6. В выпадающих списках выберите **Архитектуру ЦП** и **Тип ЦП**.
   Важно, чтобы семейство процессора совпадало с минимальным типом процессора хостов, к которым предполагается присоединить кластер, в противном случае хост будет нерабочим.

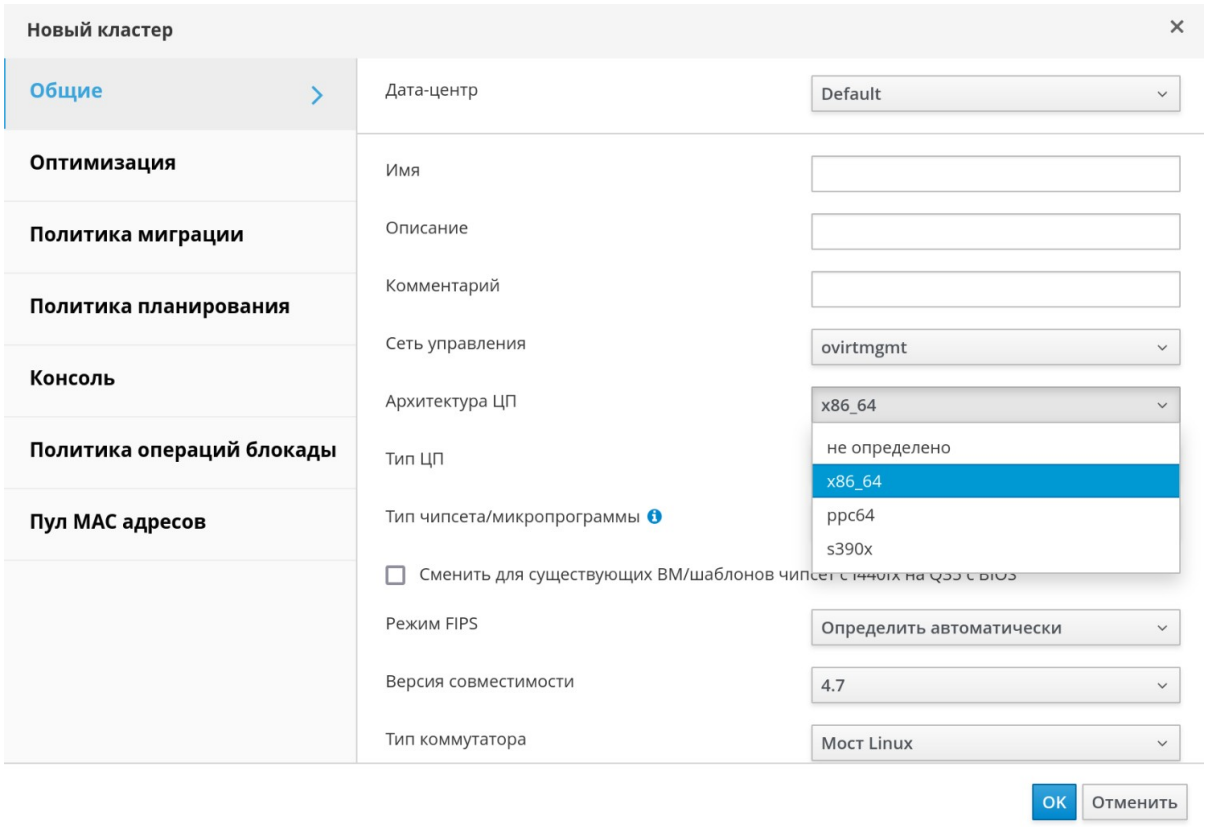

Рис. 90. Выбор архитектуры ЦП для кластера

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, выбирайте в списке самую старую модель.

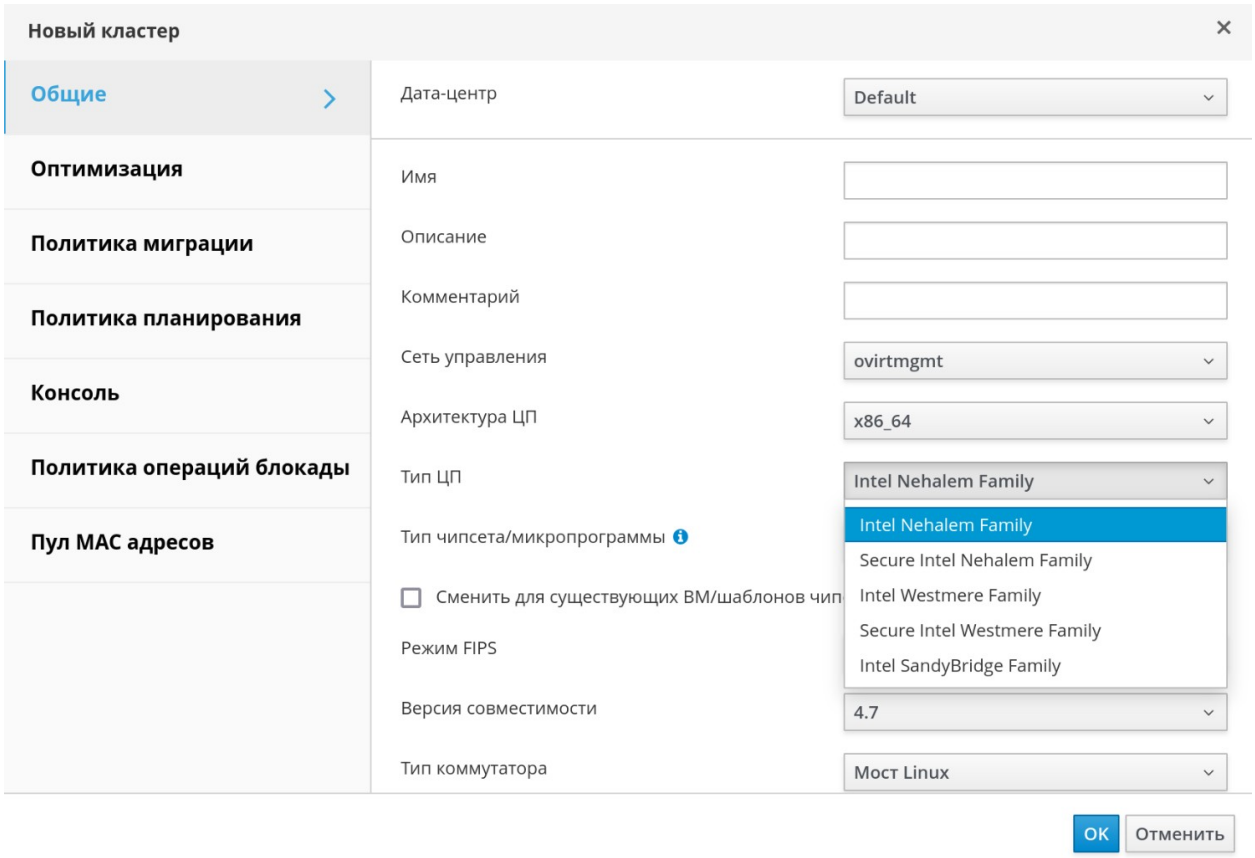

Рис. 91. Выбор типа ЦП для кластера

7. В выпадающем списке выберите **Тип чипсета/микропрограммы** кластера.

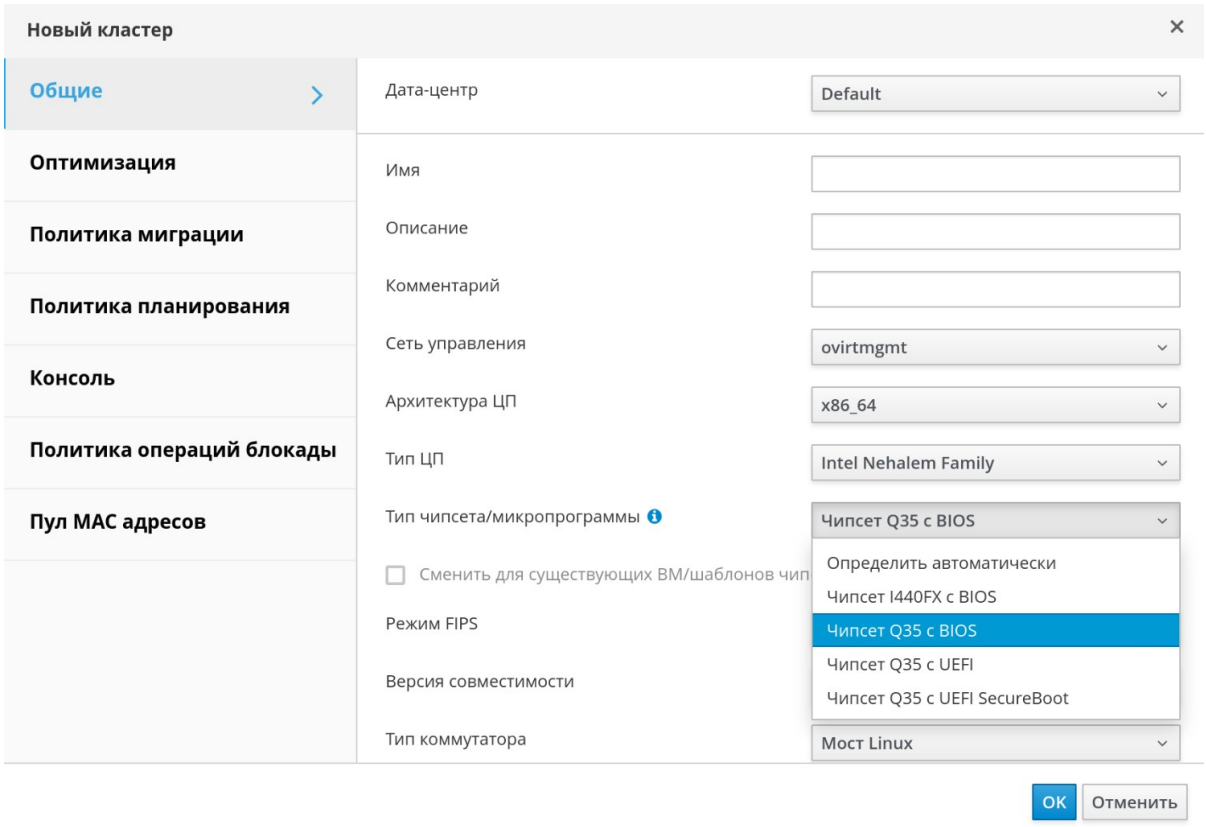

Рис. 92. Выбор тип чипсета/микропрограммы кластера.

8. В выпадающем списке выберите **Версию совместимости** кластера.
9. В выпадающем списке выберите **Тип коммутатора**.

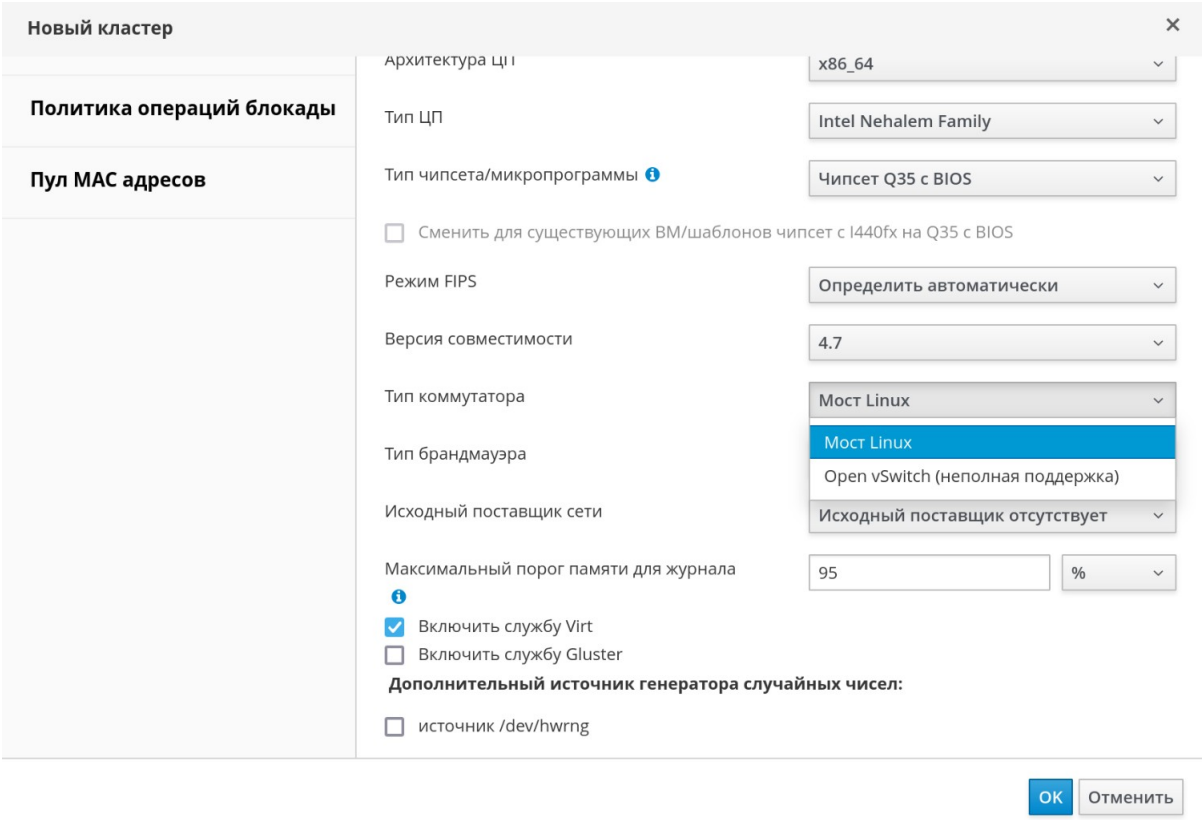

Рис. 93. Выбор типа коммутатора кластера

10. Для хостов в кластере выберите **Тип брандмауэра** — ***iptables*** или ***firewalld***.

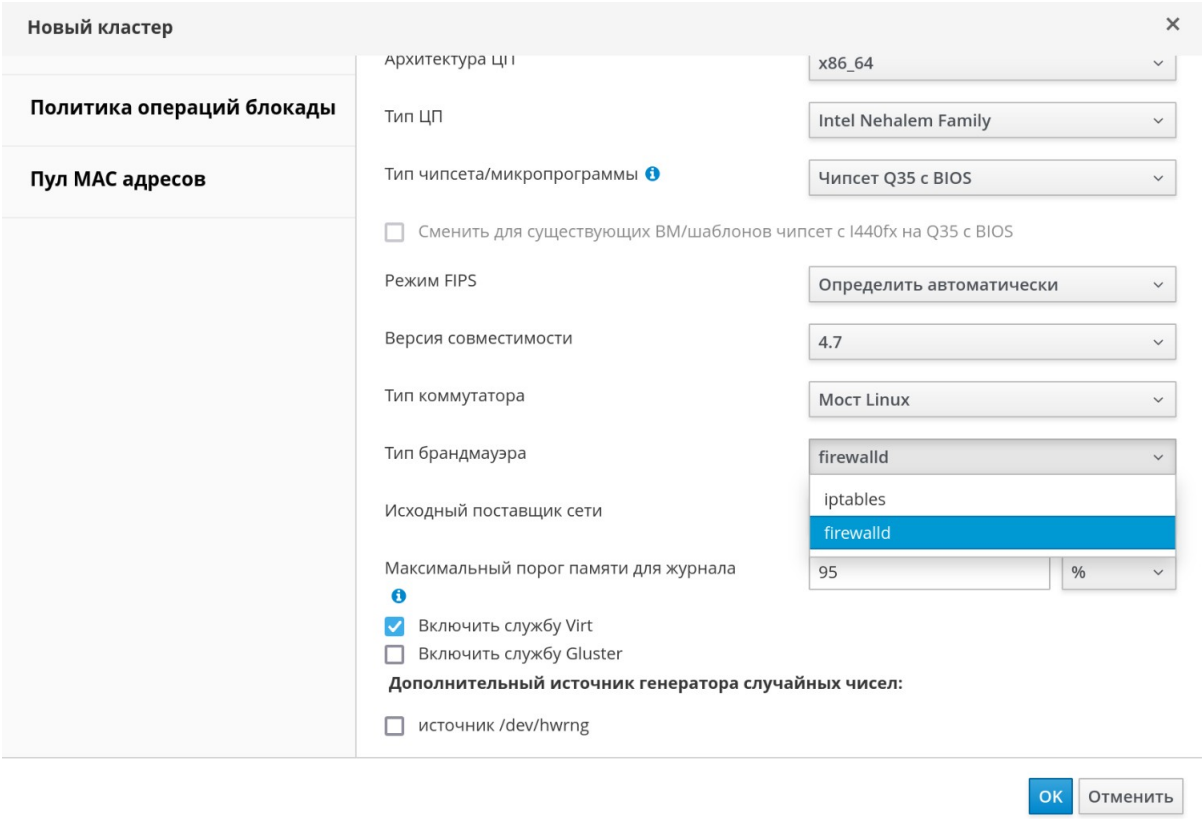

Рис. 94. Выбор типа брандмауэра кластера

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

11. Установите переключатель в положение **Включить службу Virt** или **Включить службу Gluster**, чтобы определить назначение кластера (соответственно кластер будет содержать или виртуальные машины, или узлы с поддержкой Gluster).
12. При необходимости установите флажок **Источник /dev/hwrng** (внешнее аппаратное устройство), чтобы указать устройство для создания случайных чисел, которое будут использовать все хосты в кластере. **Источник /dev/urandom** (устройство Linux) отмечено по умолчанию.
13. Перейдите на вкладку **Оптимизация** для выбора порога разделяемых страниц памяти в кластере, а также при необходимости, включите обработку потоков ЦП и вытеснение памяти на хостах в кластере.

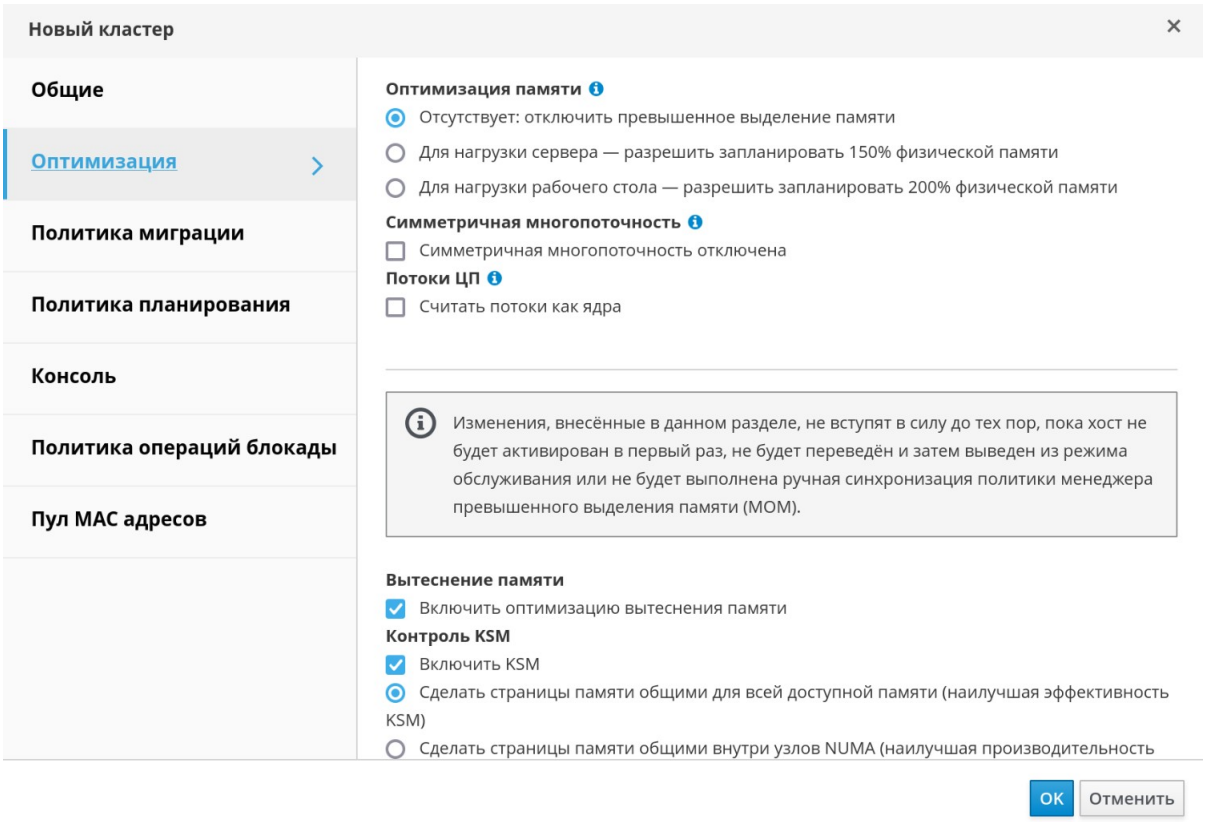

Рис. 95. Вкладка Оптимизация для настройки параметров оптимизации кластера

14. Перейдите на вкладку **Политика миграции** для настройки политики миграции ВМ в кластере.

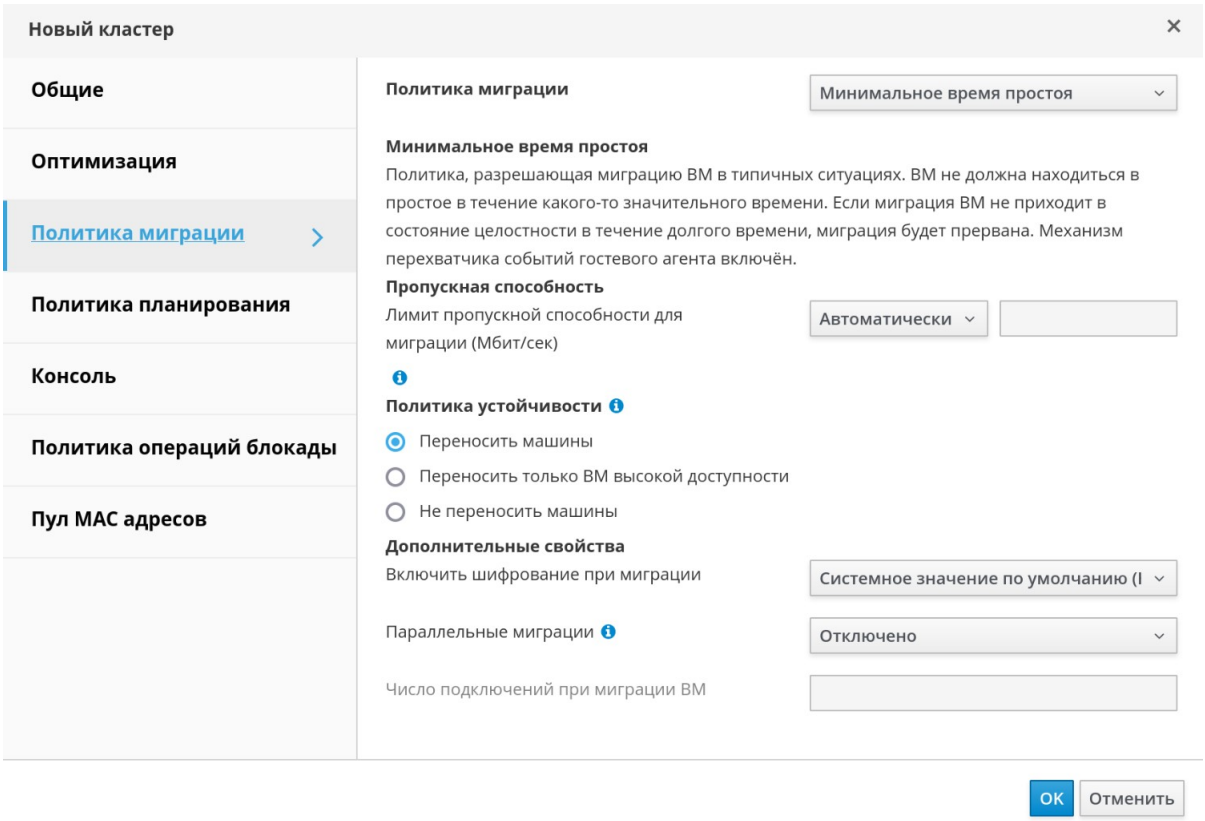

Рис. 96. Вкладка Политика миграции для настройки политики миграции ВМ в кластере.

15. Перейдите на вкладку **Политика планирования**, чтобы при необходимости, настроить политику планирования, указать параметры оптимизации планировщика, включить доверенную службу для хостов в кластере, включить резервирование высокой доступности и добавить частную политику порядковых номеров.

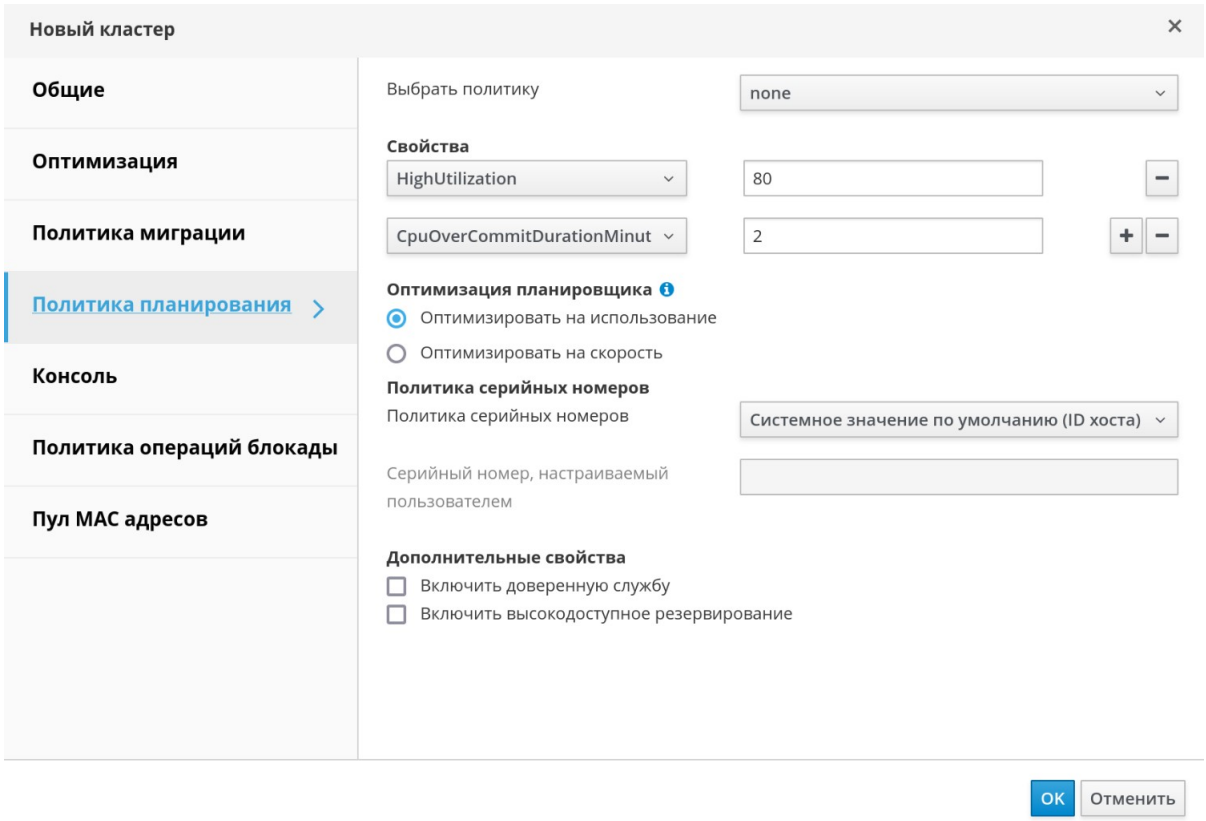

Рис. 97. Вкладку Политика планирования для настройки политики планирования кластера

16. Перейдите на вкладку **Консоль**, чтобы при необходимости, переопределить глобальные параметры прокси SPICE для хостов в кластере.

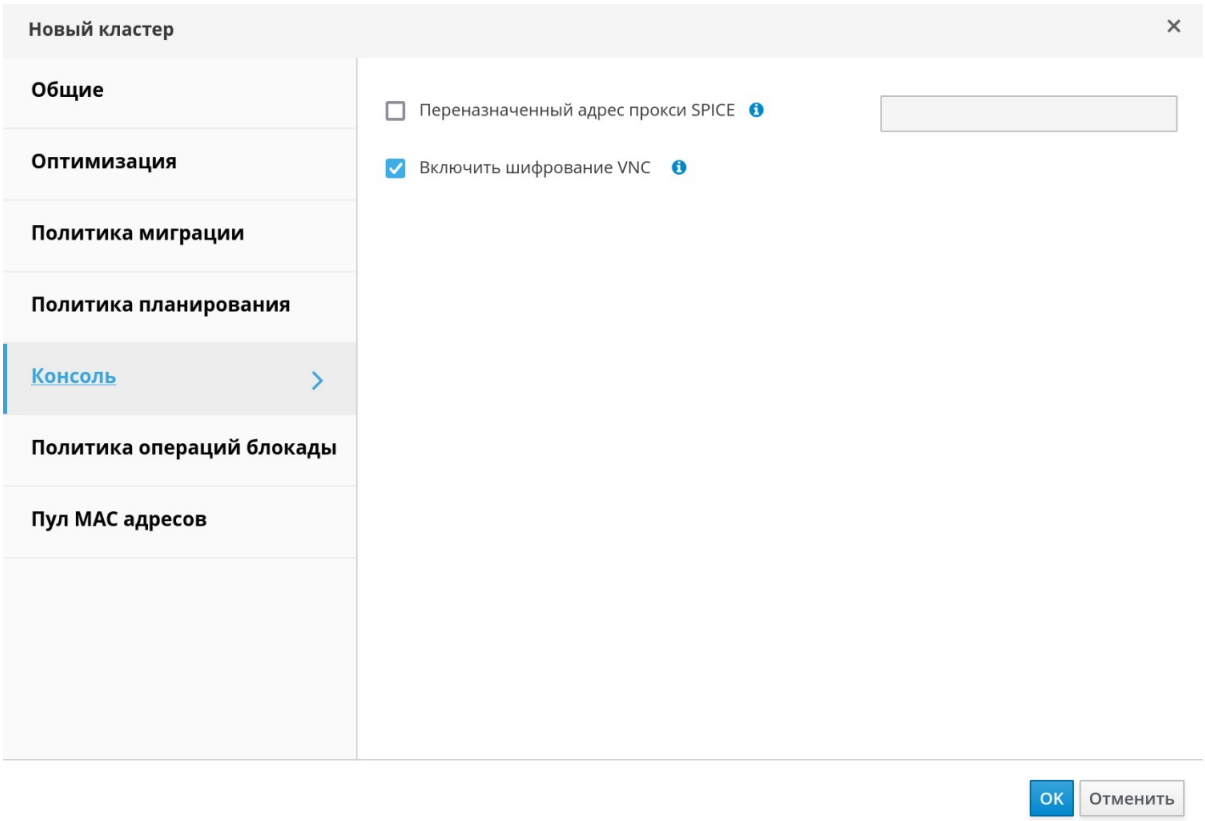

Рис. 98. Вкладка Консоль для настройки глобальных параметров прокси SPICE для хостов в кластере

17. Перейдите на вкладку **Политика операций блокады**, чтобы включить или отключить возможность проведения операций блокады в кластере и выбрать параметры блокады.

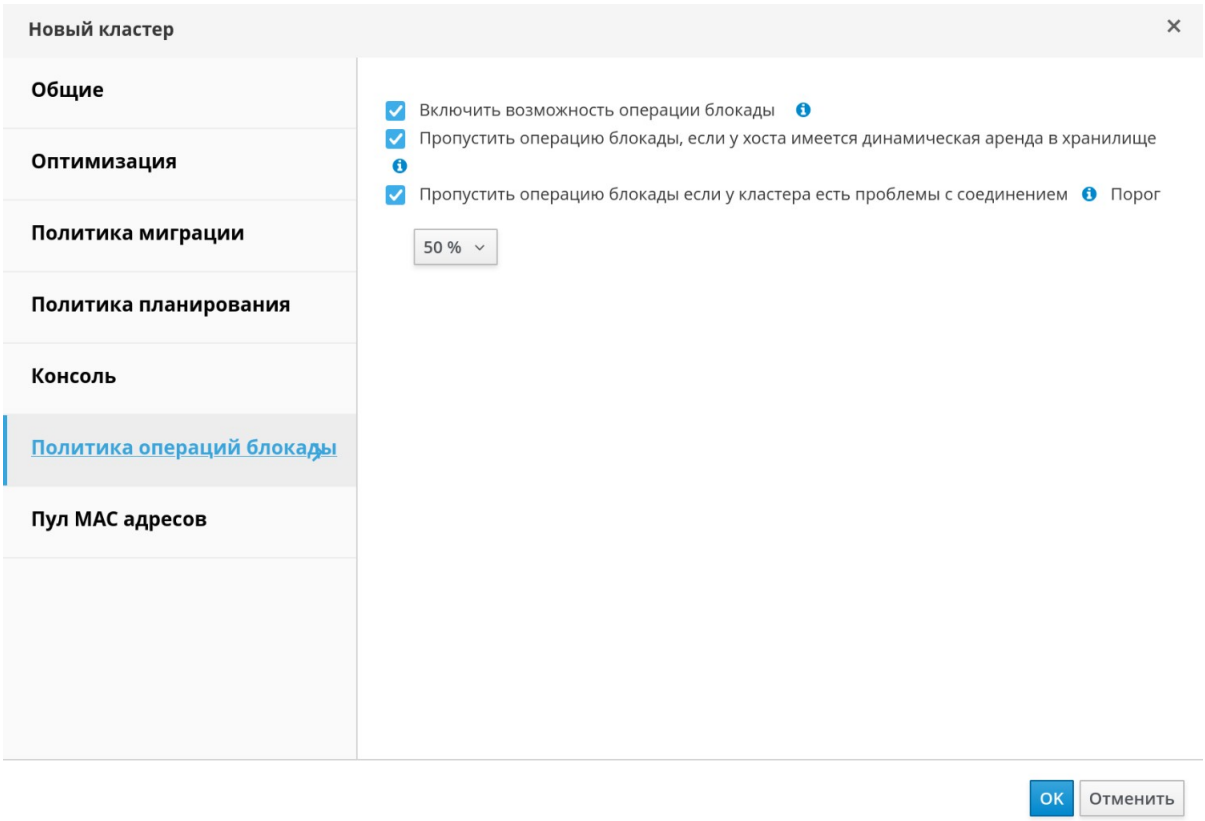

Рис. 99. Вкладка Политика операций блокады

18. Нажмите **Пул MAC адресов**, чтобы указать пул, отличный от пула адресов MAC по умолчанию. Подробности о создании, редактировании или удалении пулов адресов MAC смотрите в п. 1.5. Пулы адресов MAC.

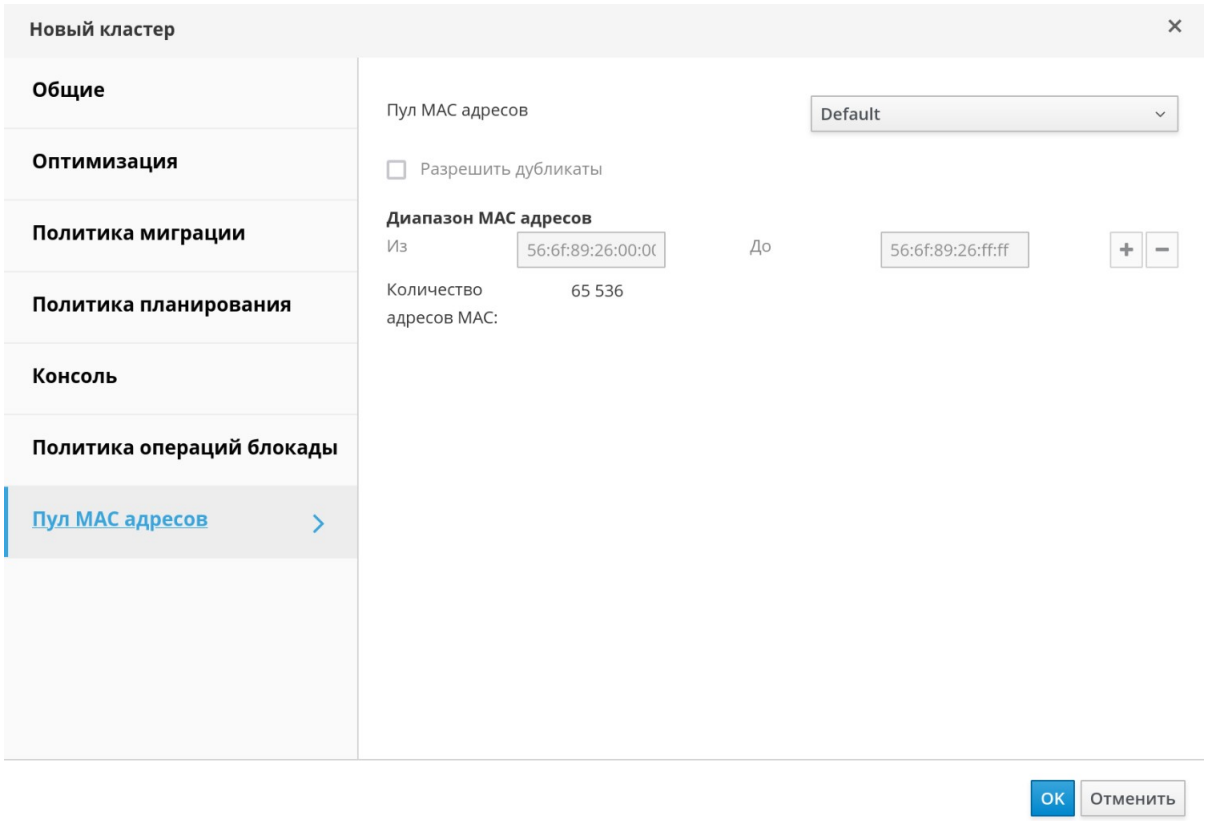

Рис. 100. Вкладка Пул MAC адресов

19. Нажмите **OK**, чтобы создать кластер и запустить окно **Кластер — пошаговый помощник** (Рис. 101).
20. В окне **Пошаговый помощник** указан список объектов, для которых необходимо настроить взаимодействие с кластером (Рис. 101). Настройте эти объекты или отложите настройку, нажав на кнопку **Настроить позже**. Процесс настройки можно возобновить позднее, для чего выберите необходимый кластер, затем нажмите на значок **Больше действий** (⋮), после чего выберите **Пошаговый помощник**.

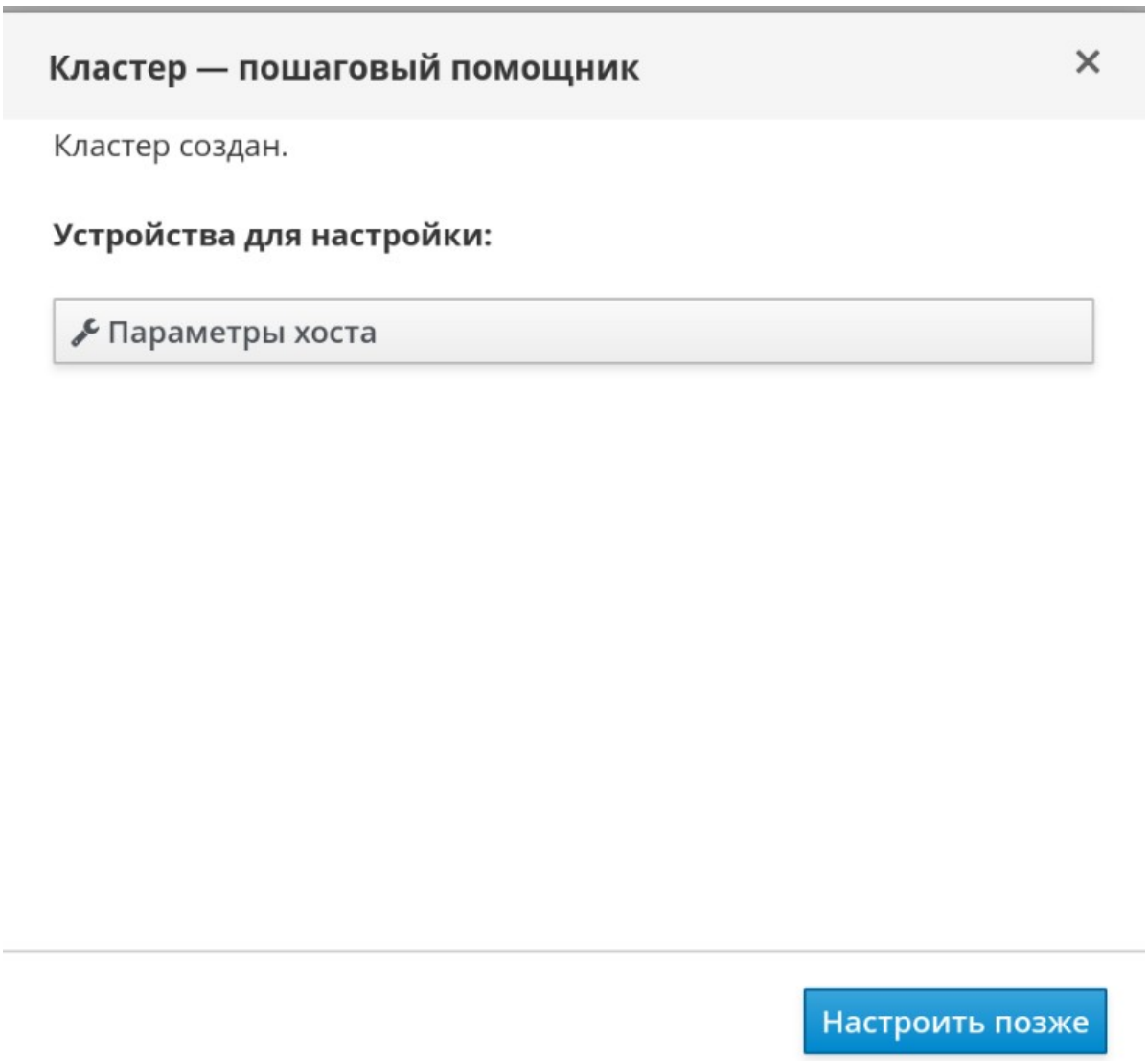

Рис. 101. Окно Кластер — пошаговый помощник.

8.2.2. Общие параметры кластера

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

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

Табл. 8.1. Общие параметры кластера

Поле	Описание / действие
Дата-центр	Дата-центр, в котором будет располагаться кластер. Дата-центр должен быть создан до создания кластера

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

Тип ЦП	Тип ЦП в кластере. Список поддерживаемых моделей ЦП:
	• AMD
	  ○ Opteron G4
	  ○ Opteron G5
	  ○ EPYC
	• Intel®
	  ○ Nehalem
	  ○ Westmere
	  ○ Sandybridge
	  ○ Haswell
	  ○ Haswell-noTSX
	  ○ Broadwell
	  ○ Broadwell-noTSX
	  ○ Skylake (client)
	  ○ Skylake (server)
	• IBM POWER 8
	Все хосты в кластере должны иметь одинаковый тип ЦП — Intel®, AMD или IBM POWER 8. После создания кластера тип ЦП нельзя изменить без значительных повреждений кластера. Тип ЦП должен быть настроен согласно самой старой модели ЦП в кластере. При этом будут использоваться только возможности, присутствующие во всех моделях. Как для типов ЦП Intel®, так и для типов ЦП AMD модели указываются в

Поле	Описание / действие
	логическом порядке от самых старых к самым новым
Версия совместимости	Версия системы виртуализации ROSA Virtualization. Нельзя выбрать версию, более раннюю, чем версия, указанная для дата-центра
Тип коммутатора	Тип коммутатора, используемый в кластере. Стандартным виртуальным коммутатором в системе виртуализации ROSA Virtualization является **Linux Bridge** (OVS предлагает поддержку для сетевых возможностей Open vSwitch)
Тип межсетевого экрана	Указывает тип межсетевого экрана для хостов в кластере — **iptables** или **firewalld**. *ВНИМАНИЕ:* **iptables** является устаревшим типом межсетевого экрана. После смены типа межсетевого экрана в существующем кластере, для применения изменений необходимо переустановить все хосты в кластере
Поставщик сети по умолчанию	Указывает поставщика внешней сети по умолчанию, который будет использоваться в кластере. При выборе Open Virtual Network (OVN) на хостах, добавленных в кластер, автоматически настраивается обмен данными с поставщиком OVN. При смене поставщика сети по умолчанию, для применения изменений необходимо переустановить все хосты в кластере
Максимальный порог журналирования потребления памяти	Указывает порог журналирования для максимального потребления памяти в процентном или абсолютном значении в Мбайт. Сообщение записывается в журнал, если потребление памяти на хосте превышает процентное значение, или если объём доступной на хосте памяти падает ниже абсолютного значения в Мбайт. Значение по умолчанию — **95%**
Включить службу Virt	Если этот переключатель активирован, то хосты в данном кластере будут использоваться для работы виртуальных машин
Включить службу Gluster	Если этот переключатель активирован, то хосты в данном кластере будут использоваться в качестве узлов сервера хранилища Gluster, а не для работы виртуальных машин
Импортировать существующую конфигурацию Gluster	Этот флажок появляется только при активации переключателя **Включить службу Gluster**. Данный параметр позволяет импортировать в СУСВ (виртуализированный ЦУ) уже существующий кластер с поддержкой Gluster и все его присоединённые хосты. Каждый из хостов импортируемого кластера должен

Поле	Описание / действие
	соответствовать следующим требованиям: • **Адрес**: укажите IP-адрес или полное доменное имя хоста сервера Gluster. • **Отпечаток**: виртуализированный ЦУ получает отпечаток (fingerprint) хоста для гарантии того, что подключение было выполнено к правильному хосту. • **Пароль root**: укажите пароль root, необходимый для обмена информацией с хостом.
Дополнительный источник для генератора случайных чисел	Если этот параметр отмечен флажком, то для всех хостов в кластере станет доступно дополнительное устройство для генерации случайных чисел. Этот параметр включает сквозную энтропию от устройства, создающего случайные числа, к виртуальным машинам

8.2.3. Параметры оптимизации

8.2.3.1. Критерии для памяти

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

8.2.3.2. Критерии для ЦП

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

- Можно запускать большее число ВМ, что снижает требования к аппаратным составляющим.

- Можно настраивать ВМ с топологией ЦП, которая в противном случае не была бы возможной (например, когда значение количества виртуальных ядер находится между числом ядер хоста и числом потоков хоста).

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

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

Табл. 8.2. Параметры оптимизации

Поле	Описание / действие
Оптимизация памяти	Режим оптимизации памяти может принимать следующие значения: • Отсутствует — отключить превышенное выделение памяти: отключает общие страницы памяти. • **Для нагрузки сервера — разрешить запланировать 150% физической памяти**: устанавливает порог разделения страниц памяти на 150% от системной памяти на каждом хосте. • **Для нагрузки рабочего стола — разрешить запланировать 200% физической памяти**: устанавливает порог разделения страниц памяти на 200% от системной памяти на каждом хосте.
Симметричная многопоточность	Установка флажка **Симметричная многопоточность отключена** отключает гиперпоточность
Потоки ЦП	Установка флажка **Считать потоки как ядра** даёт хостам возможность запускать ВМ с общим числом ядер процессора, превышающим число ядер на хосте. Если этот параметр отмечен, то предоставляемые потоки хоста считаются ядрами, которые может использовать ВМ. Например, в системе с 24 ядрами и 2 потоками на ядро (всего 48 потоков) могут выполняться ВМ с числом ядер вплоть до 48, а алгоритмы для расчёта загрузки ЦП хоста будут сопоставлять нагрузку с двойным числом потенциально используемых ядер
Вытеснение памяти	Установка флажка **Включить оптимизацию вытеснения памяти** включает превышенное выделение памяти для ВМ, работающих на хостах в этом кластере. Если этот параметр отмечен, то диспетчер превышенного выделения памяти (Memory Overcommit Manager, MoM) начинает вытеснение памяти, где и когда это возможно. Ограничением служит гарантированный размер памяти, установленный для каждой ВМ. Чтобы выполнять вытеснение памяти, виртуальной машине требуется устройство вытеснения памяти с соответствующими драйверами. Каждая ВМ включает в себя такое устройство, если только оно не было удалено специально. При смене статуса на *запущен*, каждый хост в этом кластере получает обновление политики вытеснения памяти. Если нужно, политику вытеснения памяти на хосте можно обновить

Поле	Описание / действие
	вручную, без необходимости смены статуса. Очень важно понимать, что в некоторых сценариях вытеснение памяти может конфликтовать с функцией объединения одинаковых страниц памяти ядром (KSM). В таких случаях MoM постарается перенастроить размер вытесняемой памяти для минимизации конфликта. Кроме того, в некоторых сценариях вытеснение памяти может привести к производительности ВМ ниже оптимальной. Администраторам следует прибегать к оптимизации вытеснения памяти с крайней осторожностью
Контроль KSM	Установка флажка **Включить KSM** даёт возможность MoM выполнять объединение одинаковых страниц памяти как при необходимости, так и тогда, когда выгода от экономии памяти перевешивает вычислительные затраты ЦП. Режим контроля KSM может принимать следующие значения: • Сделать страницы памяти общими для всей доступной памяти: наилучшая эффективность KSM. • Сделать страницы памяти общими внутри узлов NUMA: наилучшая производительность NUMA.

8.2.4. Политики миграции

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

Табл. 8.3. Политики миграции

Политика	Описание
Минимальный простой	Политика, разрешающая миграцию ВМ в типичных ситуациях. ВМ не должны испытывать значительный простой. Миграция будет прервана, если после долгого промежутка времени ВМ не достигнет состояния целостности (в зависимости от итераций QEMU, с максимальным интервалов в 500 миллисекунд). Механизм ловушек гостевого агента включён
Миграция пост-копирования	По аналогии с политикой минимального простоя, ВМ не должны испытывать значительный простой. Политика пост-копирования сначала пытается выполнить пред-копирование для проверки возможности конфликтов. Если ВМ не достигает состояния целостности после долгого промежутка времени, то происходит переключение на пост-копирование. Недостаток

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

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

Табл. 8.4. Параметры пропускной способности

Политика	Описание
Автоматически	Значение пропускной способности копируется из параметра **Предел скорости (Мбит/с)** конфигурации **QoS сети хоста** дата-центра. Если предел скорости не был назначен, значение рассчитывается как минимальная из скоростей канала на получающих и отправляющих сетевых интерфейсах. Если предел скорости не был назначен, а скорости канала неизвестны, значение определяется, исходя из локального параметра VDSM на посылающем хосте
Значение по умолчанию гипервизора	Пропускная способность контролируется локальным параметром VDSM на отправляющем хосте

Политика	Описание
Настраивается пользователем	Значение в Мбит/с настраивается пользователем и разделяется на число одновременных миграций (по умолчанию — 2, для учёта и входящей, и исходящей миграции). Соответственно, пропускная способность, настроенная пользователем, должна быть достаточно высокой для учёта всех одновременных миграций. Например, если частная пропускная способность указана как 600 Мбит/с, то максимальная пропускная способность при миграции ВМ фактически составит 300 Мбит/с

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

Табл. 8.5. Параметры политики устойчивости

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

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

Табл. 8.6. Дополнительные параметры

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

8.2.5. Политики планирования

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

В Табл. 8.7 описываются параметры вкладки Политики планирования.

Табл. 8.7. Параметры вкладки «Политики планирования»

Поле	Описание / действие
Выберите политику	Выберите необходимую политику планирования из выпадающего списка: • **None (отсутствует)**: режим по умолчанию — без балансировки нагрузки или разделения энергосбережения между хостами уже работающих ВМ. При запуске ВМ нагрузка на память и вычислительные ресурсы ЦП равномерно распределяются между всеми хостами в кластере. Дополнительные ВМ не начнут работу, если нагрузка хоста достигла ранее настроенных значений `CpuOverCommitDurationMinutes`, `HighUtilization` или `MaxFreeMemoryForOverUtilized`. • **evenly_distributed (равномерное распределение)**: равномерно распределяет память и вычислительные ресурсы ЦП между всеми хостами в кластере. Дополнительные ВМ, присоединённые к хосту, не начнут работу, если нагрузка хоста достигла ранее настроенных значений `CpuOverCommitDurationMinutes`, `HighUtilization` или `MaxFreeMemoryForOverUtilized`. • **cluster_maintenance (обслуживание кластера)**: ограничивает активность в кластере во время выполнения задач обслуживания. Нельзя запускать никакие ВМ, включая высокодоступные, но можно выполнять миграцию любых ВМ. В случае сбоя хоста, высокодоступные ВМ будут корректно перезапущены. • **power_saving (энергосбережение)**: распределение памяти и нагрузки на вычислительные мощности ЦП внутри группы доступных хостов для снижения потребления энергии на недозагруженных хостах. Хосты с нагрузкой на ЦП меньше значения низкого использования в течение большего промежутка времени, чем указанный промежуток, выполнят миграцию всех ВМ на другие хосты с тем, чтобы можно было произвести отключение этого хоста. Дополнительные ВМ, присоединённые к этому хосту, не начнут работу, если хост достиг указанного значения высокой

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

Поле	Описание / действие
	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 `HA Reservation`, путём деления значения оценки степени высокой готовности хоста на указанное число. Это дополнительный параметр, который можно добавлять к любой политике, включая политику **none**. • **HostsInReserve**: указывает число хостов, которые всегда должны работать, даже если на них отсутствуют ВМ. Это дополнительный параметр, который можно добавить к политике **power_saving**. • **EnableAutomaticHostPowerManagement**: включает автоматическое управление энергосбережением на всех хостах кластера. Это дополнительный параметр, который можно добавить к политике **power_saving**. Значение по умолчанию — верно (true). • **MaxFreeMemoryForOverUtilized**: указывает минимальный размер свободной памяти (в Мбайт), требуемый для минимального уровня обслуживания. Если объём доступной памяти хоста будет равен или меньше этого значения, то виртуализированный ЦУ будет выполнять миграцию ВМ на другие хосты этого кластера в течение всего времени, пока объём доступной памяти хоста будет находиться меньше значения порога минимального уровня обслуживания. Это дополнительный параметр, который можно указать для политик **power_saving** и **evenly_distributed**. Значение 0 для параметров `MaxFreeMemoryForOverUtilized` и `MinFreeMemoryForUnderUtilized` отключает балансировку памяти. Для избежания непредсказуемого поведения, при указании значения для параметра `MaxFreeMemoryForOverUtilized` необходимо также указывать значение и для параметра `MinFreeMemoryForUnderUtilized`. • **MinFreeMemoryForUnderUtilized**: указывает минимальный размер свободной памяти (в Мбайт), требуемый для того, чтобы хост считался

Поле	Описание / действие
	низкозагруженным. Если объём доступной памяти хоста будет иметь значение меньше указанного в этом параметре, то виртуализированный ЦУ выполнит миграцию ВМ на другие хосты в кластере и автоматически отключит машину хоста. Машина будет включена снова по соображениям балансировки нагрузки, или если в кластере будет недостаточно свободных хостов. Это дополнительный параметр, который можно указать для политик **power_saving** и **evenly_distributed**. Значение 0 для параметров `MaxFreeMemoryForOverUtilized` и `MinFreeMemoryForUnderUtilized` отключает балансировку памяти. Для избежания непредсказуемого поведения, при указании значения для параметра `MaxFreeMemoryForOverUtilized` необходимо также указывать значение и для параметра `MinFreeMemoryForUnderUtilized`. • **HeSparesCount**: указывает число дополнительных узлов виртуализированного ЦУ, на которых должна быть зарезервирована память в объёме, достаточном для запуска виртуальной машины виртуализированного ЦУ на случай миграции этой ВМ или отключения. Если запуск других машин на узле виртуализированного ЦУ не оставит достаточного объёма свободной памяти для ВМ виртуализированного ЦУ, то эти машины не начнут работу. Это дополнительный параметр, который можно добавить к политикам **power_saving**, **vm_evenly_distributed** и **evenly_distributed**. Значение по умочанию — 0.
Оптимизация планировщика	Оптимизация планировщика для определения весового коэффициента/ распределения хостов: • **Оптимизировать на использование**: в планирование включаются весовые модули для наилучшего выбора. • **Оптимизировать на скорость**: определение весового коэффициента хоста пропускается в тех случаях, когда в очереди находится больше десяти запросов.
Включить доверенную службу	Включить интеграцию с сервером OpenAttestation. Чтобы включить возможность этого параметра, используйте утилиту `engine-config` для указания сведений о сервере OpenAttestation
Включить резервирование высокой доступности	Разрешить виртуализированному ЦУ выполнять наблюдения за доступными мощностями кластера для отказоустойчивых ВМ. Виртуализированный ЦУ обеспечивает наличие в кластере необходимых ресурсов для миграции высокодоступных ВМ в случае внезапного отказа их текущего хоста

Поле	**Описание / действие**
Политика серийных номеров	Параметр даёт возможность задать политику серийных номеров для ВМ в кластере. Выберите одну из следующих возможностей: • **Значение по умолчанию**: используется значение (**ID хоста** (по умолчанию)), настроенное на уровне кластера. • **ID хоста**: в качестве серийного номера ВМ указывается UUID хоста. • **ID машины**: в качестве серийного номера ВМ указывается UUID ВМ. • **Настраиваемый пользователем серийный номер**: даёт возможность пользователю указать произвольный порядковый номер в качестве серийного номера ВМ.

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

8.2.6. Параметры консоли кластера

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

Табл. 8.8. Параметры консоли

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

8.2.7. Параметры политики операций блокады

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

Табл. 8.9. Параметры политики операций блокады

Поле	Описание / действие
Включить возможность операций блокады	Разрешает проведений операций блокады в кластере. По умолчанию эта возможность присутствует, но при необходимости её можно отключить (например, если возникают или ожидаются временные проблемы с сетью, то администратор может отключить возможность проведения операций блокады до завершения действий по диагностике

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

8.2.8. Настройка политик управления нагрузкой и энергосбережения на хосте

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

Настройка политик управления нагрузкой и энергосбережения на хосте

1. Нажмите **Ресурсы → Кластеры и выберите кластер**.
2. Нажмите **Изменить**.
3. Перейдите на вкладку **Политика планирования** (Рис. 102).

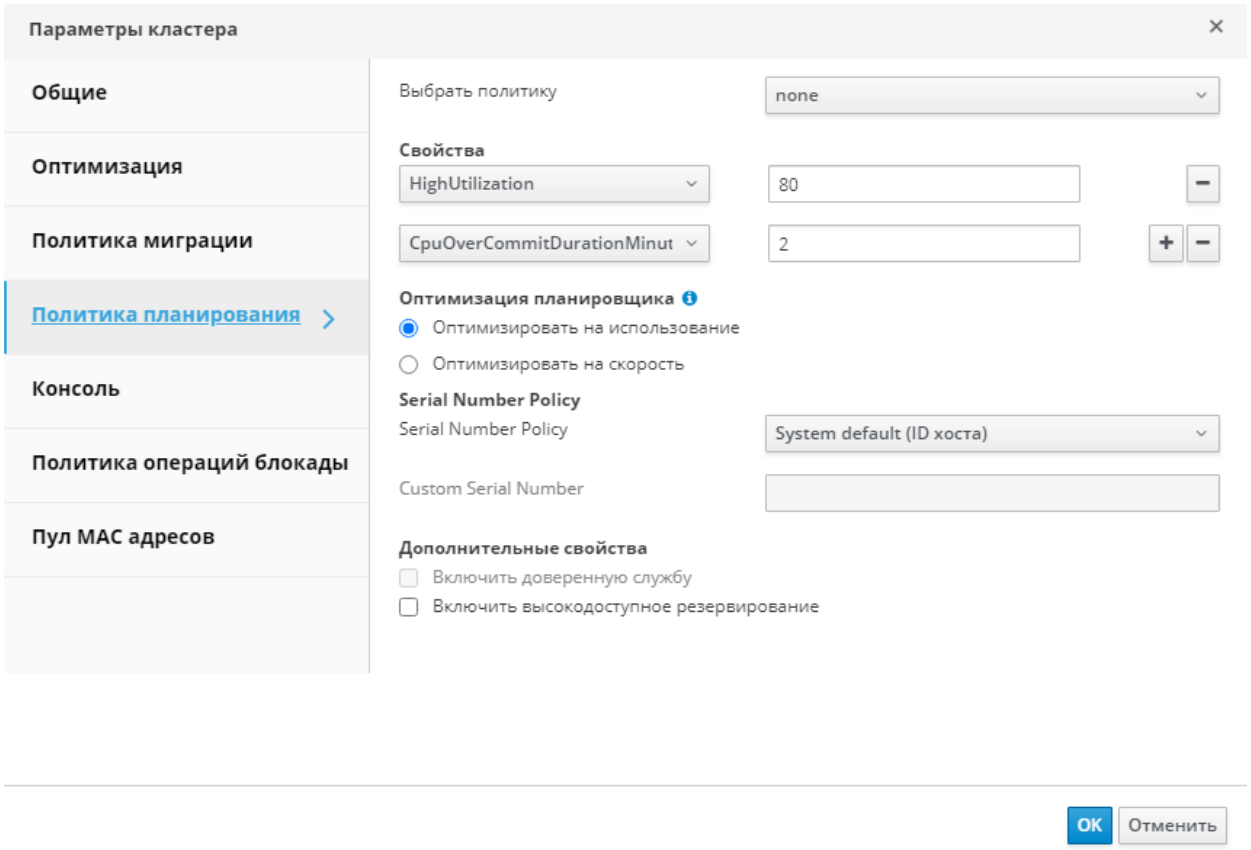

Рис. 102. Политика планирования

4. Выберите одну из следующих политик:

   - **нет**
   - **vm_evenly_distributed**

     a. В поле **HighVmCount** укажите минимальное число ВМ, выполняющихся на одном хосте и необходимых для включения балансировки нагрузки.
     b. В поле **MigrationThreshold** укажите максимальную приемлемую разницу между числом ВМ на самом загруженном хосте и числом ВМ на самом незагруженном хосте.
     c. В поле **SpmVmGrace** укажите число слотов для ВМ, которое должно быть зарезервировано на хостах SPM.
     d. При необходимости в поле **HeSparesCount** укажите число дополнительных узлов виртуализированного ЦУ, на которых нужно зарезервировать объём свободной памяти, достаточный для запуска ВМ виртуализированного ЦУ в случае миграции этой ВМ или выключения.

   - **evenly_distributed**

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

- **power_saving**

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

5. Выберите одно из следующих значений **Оптимизации планировщика** кластера:

- **Оптимизировать на использование** — включение в планирование весовых модулей для лучшего выбора.
- **Оптимизировать на скорость** — пропуск измерения веса хоста в тех случаях, когда в очереди находится более 10 запросов.

6. Если для верификации хостов используется сервер OpenAttestation и его конфигурация была настроена с помощью утилиты `engine-config`, то установите флажок **Включить доверенную службу**.
7. При необходимости установите флажок **Включить высокодоступное резервирование**, чтобы виртуализированный ЦУ мог обеспечивать доступность ресурсов в кластере для отказоустойчивых ВМ.

8. При необходимости выберите одно из следующих значений **Политики серийных номеров** для ВМ в кластере:

   - **ID хоста** — в качестве серийного номера ВМ указывается UUID хоста.
   - **ID машины** — в качестве серийного номера ВМ указывается UUID ВМ.
   - **Настраиваемый пользователем серийный номер** — при выборе этого значения дополнительно укажите произвольный порядковый номер (в качестве серийного номера ВМ) в текстовом поле интерфейса.
9. Нажмите **OK**.

8.2.9. Обновление информации о политике MoM на хостах в кластере

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

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

Следующая последовательность действий должна выполняться на каждом из хостов индивидуально.

Синхронизация политики превышенного выделения памяти на хосте

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

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

8.2.10. Создание профиля ЦП

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

Максимальный объём выражается в процентном соотношении к общей вычислительной мощности, доступной для этого хоста. Профили ЦП создаются на базе профилей ЦП, настроенных в дата-центрах, и не применяются автоматически ко всем ВМ в кластере. Для того, чтобы профили вступили в силу, их необходимо вручную присваивать виртуальным машинам индивидуально.

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

Создание профиля ЦП

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

8.2.11. Удаление профиля ЦП

Удаление профиля ЦП

1. Нажмите **Ресурсы → Кластеры**.
2. Нажмите на название кластера, чтобы открыть подробный просмотр.
3. Перейдите на вкладку **Профили ЦП** и выберите удаляемый профиль ЦП.
4. Нажмите **Удалить**.
5. Нажмите **OK**.

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

8.2.12. Импортирование существующего кластера хранилища Gluster

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

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

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

Импортирование существующего хранилища Gluster в виртуализированный ЦУ

1. Нажмите **Ресурсы → Кластеры**.
2. Нажмите **Добавить**.
3. Выберите **Дата-центр**, к которому будет принадлежать кластер.
4. Укажите **Имя** и **Описание** кластера.

5. Установите флажки Включить службу Gluster и Импорт существующей конфигурации Gluster (при этом поле Импорт существующей конфигурации Gluster будет показано только при ранее выбранном параметре Включить службу Gluster).

6. В поле **Имя хоста** укажите имя хоста или IP-адрес любого сервера в кластере. Будет показан **Отпечаток SSH** для подтверждения того, что выполняется подключение к нужному хосту. Если хост недоступен или появилась ошибка сети, то в поле **Отпечаток** будет выведена **Ошибка получения отпечатка**.

7. Укажите **Пароль** (пароль сервера) и нажмите **OK**.
8. Будет показано окно **Добавить хосты** и список хостов в составе кластера.
9. Для каждого хоста укажите **Имя** и **Пароль root**.
10. В случае использования одного и того же пароля для всех хостов установите флажок **Использовать общий пароль** и укажите этот пароль в текстовом поле.

11. Нажмите **Применить**, чтобы установить введённый пароль для всех хостов.

12. Проверьте подлинность всех отпечатков и нажмите **OK** для применения изменений.

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

8.2.13. Параметры хранилища Gluster в окне «Добавить хосты»

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

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

Табл. 8.10. Параметры Gluster

Параметр (поле)	Описание
Использовать общий пароль	Установите этот флажок, чтобы для всех хостов в кластере использовался один и тот же пароль. Введите необходимый пароль в поле **Пароль**, затем нажмите на кнопку **Применить**, чтобы установить пароль для всех хостов
Имя	Укажите название хоста
Имя хоста/IP	Поле заполняется автоматически на основании данных о полном доменном имени или IP-адресе хоста, указанных в окне **Новый кластер**
Пароль root	Чтобы использовать различные пароли *root* для каждого

Параметр (поле)	Описание
	хоста, введите пароль в этом поле. Данные в этом поле переопределяют общий пароль, указанный для всех хостов в кластере
Отпечаток	Для подтверждения того, что выполняется подключение к нужному хосту, здесь будет показан его отпечаток. Это поле заполняется автоматически на базе данных об отпечатке хоста, указанных в окне **Новый кластер**

8.2.14. Удаление кластеров

Перед удалением кластера переместите из него все хосты.

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

Удаление кластера

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

8.2.15. Оптимизация памяти

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

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

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

Таким образом для оптимизации памяти рекомендуется выполнить следующие действия:

- Ограничить превышенное выделение памяти с помощью параметра **Оптимизация памяти** и *диспетчера превышенного выделения памяти (MoM)*.
- Создать раздел подкачки, достаточно объёмный для того, чтобы потенциально обеспечить максимальный запрос на виртуальную память и одновременно не выходить за пределы безопасности.

- Уменьшить размер виртуальной памяти, включив вытеснение памяти (ballooning) и объединение одинаковых страниц памяти ядром (KSM).

8.2.15.1. Превышенное выделение памяти

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

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

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

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

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

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

Дополнительные примечания:

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

8.2.15.2. Раздел подкачки

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

Табл. 8.11. Общие рекомендации по настройке раздела подкачки

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

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

Дополнительные рекомендации по настройке раздела подкачки:

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

Применяя данные рекомендации, следуйте совету по установке размера раздела подкачки в качестве «последней возможности» для наихудшего возможного сценария. Используйте размер физической памяти и параметр **Оптимизация памяти** в качестве

базы для расчёта общего объёма виртуальной памяти. Не включайте в эти расчёты сокращение памяти с помощью оптимизации диспетчером превышенного выделения памяти MoM, вытеснения памяти и объединения одинаковых страниц памяти ядром (KSM).

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

8.2.15.3. Диспетчер превышенного выделения памяти MoM

Диспетчер превышенного выделения памяти MoM выполняет следующие основные функции:

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

Диспетчер MoM не нуждается во включении или отключении.

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

8.2.15.4. Вытеснение памяти (ballooning)

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

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

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

Дополнительные примечания:

- Вытеснение памяти и превышенное выделение памяти не рекомендуется применять для рабочих нагрузок, требующих постоянной высокой производительности и низких значений задержки.

- Вытеснение памяти рекомендуется применять там, где увеличение численности ВМ (из соображений экономии) играет бо̀льшую роль, чем производительность.
- Вытеснение памяти не имеет значительного влияния на загруженность ЦП (KSM потребляет некоторые количество ресурсов ЦП, но в стрессовых условиях объём этого потребления не изменяется).

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

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

8.2.15.5. Объединение одинаковых страниц памяти ядром (KSM)

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

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

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

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

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

Дополнительные примечания:

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

Чтобы включить механизм объединения одинаковых страниц памяти ядром, перейдите на вкладку **Оптимизация** в окне **Новый кластер** или **Параметры кластера**. Затем установите флажок **Включить KSM**. Этот параметр заставляет диспетчер превышенного выделения памяти MoM запускать KSM, когда это необходимо, в том числе когда преимущества экономии памяти при объединении одинаковых страниц памяти перевешивают затраты ЦП на работу KSM (см. п. 8.2.3. Параметры оптимизации).

8.2.16. Изменение версии совместимости кластера

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

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

Изменение версии совместимости кластера

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

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

После обновления версии совместимости кластера необходимо обновить версию совместимости всех работающих или приостановленных ВМ, перезапустив их с помощью Портала администрирования или с помощью REST API, а не из гостевых ОС. Машины, которым нужна перезагрузка, отмечены значком изменений . Нельзя изменить версию

совместимости снимка виртуальной машины, находящегося в предпросмотре. Сначала необходимо зафиксировать изменения или отменить предварительный просмотр.

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

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

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

Глава 9. Логические сети

9.1. Задачи при работе с логическими сетями

9.1.1. Выполнение сетевых задач

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

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

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

Доступ к этому функционалу также возможен для каждого индивидуального ресурса.

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

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

- Службы каталогов.
- DNS.
- Хранилище.

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

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

Создание новой логической сети в дата-центре или в кластере

1. Нажмите **Ресурсы → Дата-центры** или **Ресурсы → Кластеры**.
2. Нажмите на название дата-центра или кластера, чтобы открыть подробный просмотр.
3. Перейдите на вкладку **Логические сети**.
4. Откройте окно **Новая логическая сеть** (Рис. 103):
    - В подробном просмотре дата-центра нажмите **Добавить**.
    - В подробном просмотре кластера нажмите **Добавить сеть**.

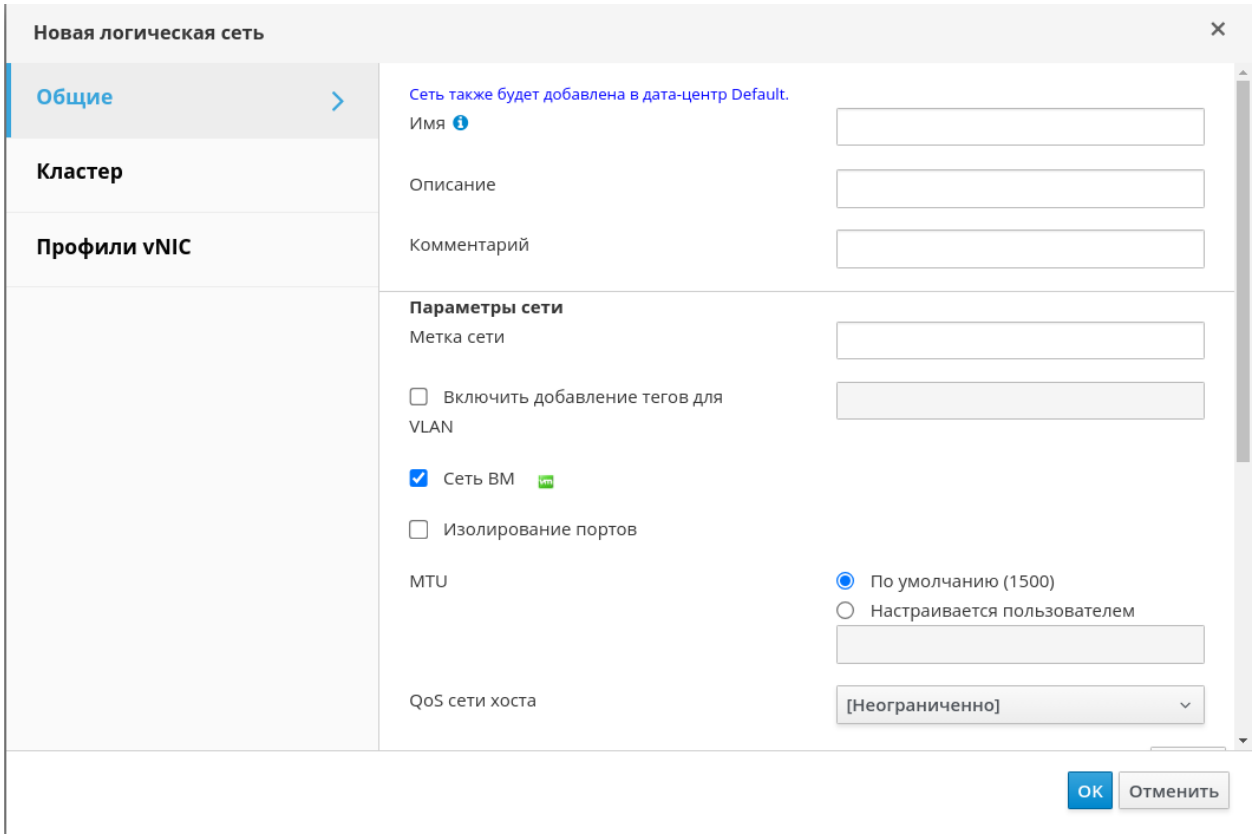

Рис. 103. Новая логическая сеть

5. Укажите **Имя**, **Описание** и **Комментарий** для логической сети.
6. Опционально включите параметр Включить добавление тегов для VLAN.
7. Опционально отключите параметр **Сеть ВМ**.
8. Опционально включите параметр **Изолирование портов**, чтобы ВМ не могли обмениваться данными в логической сети.
9. Опционально включите параметр **Создать на внешнем поставщике**. Таким образом будут отключены параметры **Метка сети**, **Сеть ВМ** и **MTU**.
10. Выберите **Внешнего поставщика**. В список **Внешний поставщик** не включены внешние поставщики с режимом `read-only`.

Чтобы создать внутреннюю изолированную сеть, выберите в списке **Внешний поставщик** пункт **ovirt-provider-ovn** и не отмечайте параметр **Подключиться к физической сети**.

11. В поле **Метка сети** введите новую метку логической сети или выберите уже существующую.
12. Укажите значение MTU: По умолчанию (1500) или Пользовательское.
13. При выборе в списке **Внешний поставщик** пункта **ovirt-provider-ovn** укажите необходимо ли в сети применять **Группы безопасности**.
14. Во вкладке **Кластер** выберите кластеры, которым будет присвоена сеть. Также можно указать, будет ли эта логическая сеть требуемой сетью.

15. При выборе пункта **Создать внешнего поставщика** станет видимой вкладка **Подсеть**. Укажите в этой вкладке **Имя**, **CIDR** и **Шлюз**. При необходимости можно добавить серверы DNS.
16. Во вкладке **Профили vNIC** добавьте профили требуемых виртуальных NIC к логической сети.
17. Нажмите **OK**.

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

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

9.1.3. Изменение параметров логических сетей

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

Изменение параметров логической сети

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на название дата-центра, чтобы открыть подробный просмотр.
3. Перейдите на вкладку **Логические сети** и выберите логическую сеть.
4. Нажмите **Параметры**.
5. Внесите необходимые изменения параметров (Рис. 104).

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

6. Нажмите **OK**.

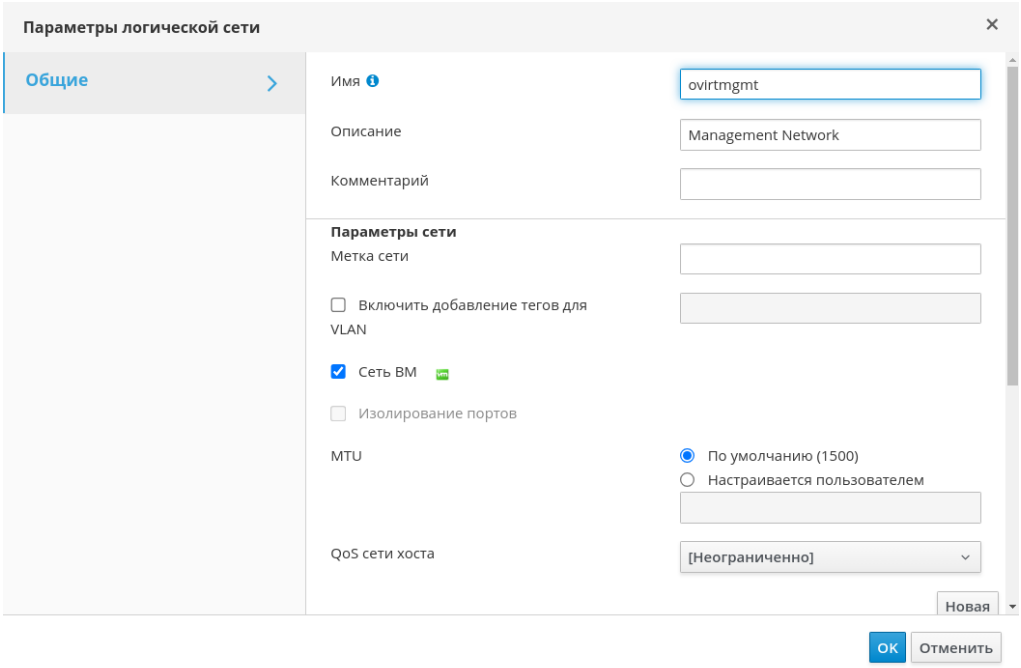

Рис. 104. Изменение параметров логической сети

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

9.1.4. Удаление логической сети

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

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

Удаление логической сети

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

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

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

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

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

Настройка логической сети в качестве маршрута по умолчанию

1. Нажмите **Сеть → Сети**.
2. Нажмите на название логической сети без функции управления (Рис. 105), которая будет настраиваться в качестве маршрута по умолчанию, чтобы перейти к подробному просмотру (Рис. 105).

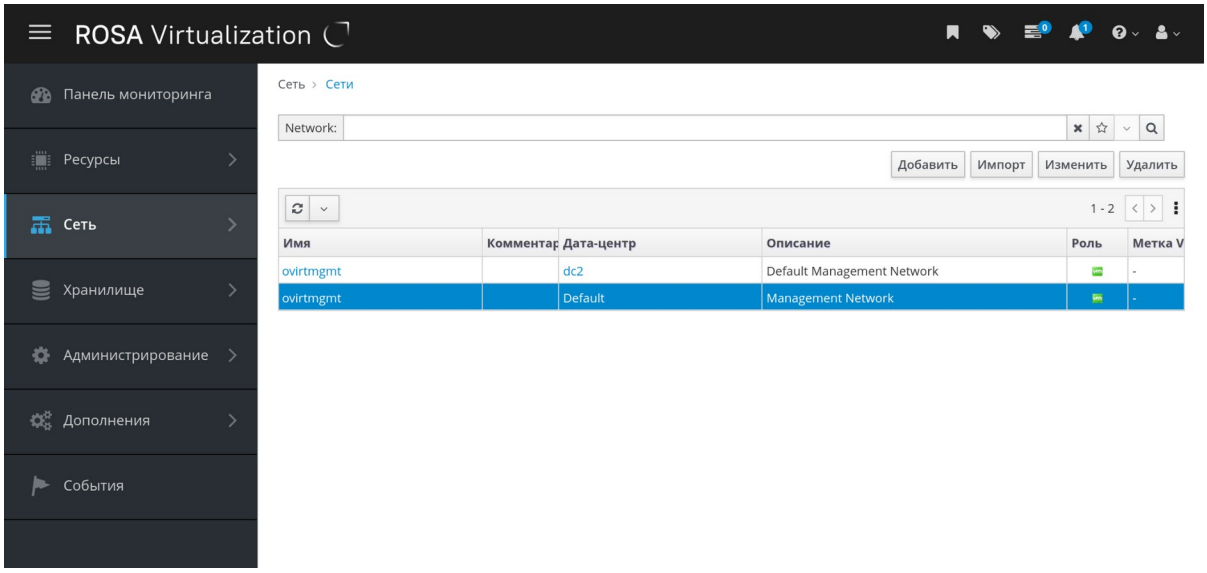

Рис. 105. Форма Сеть → Сети

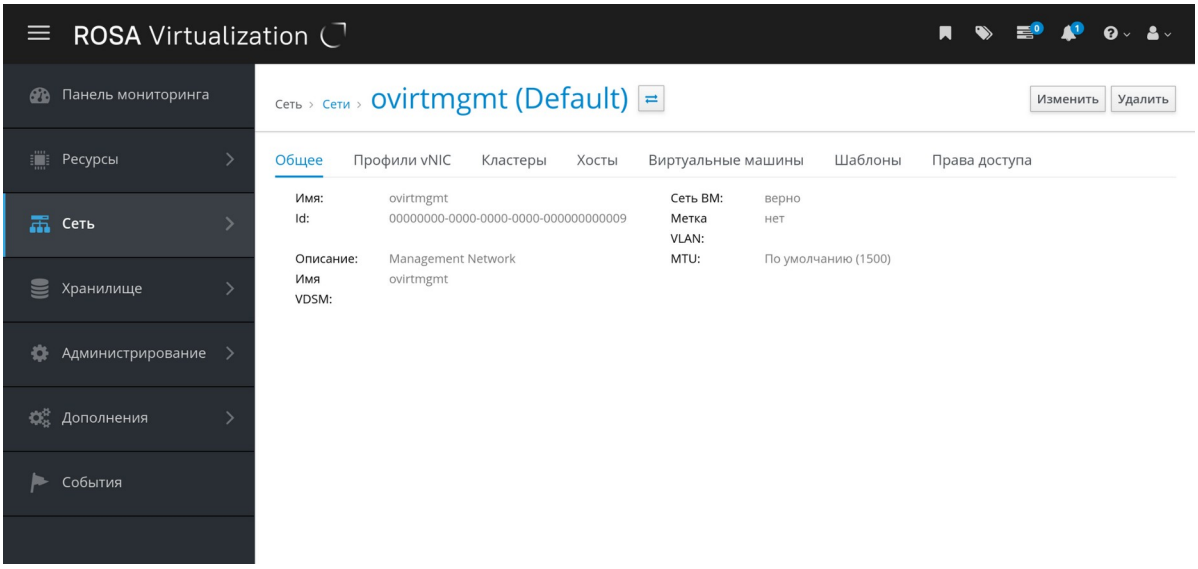

Рис. 106. Сеть ovirtmgmt (Default)

3. Перейдите на вкладку **Кластеры**.

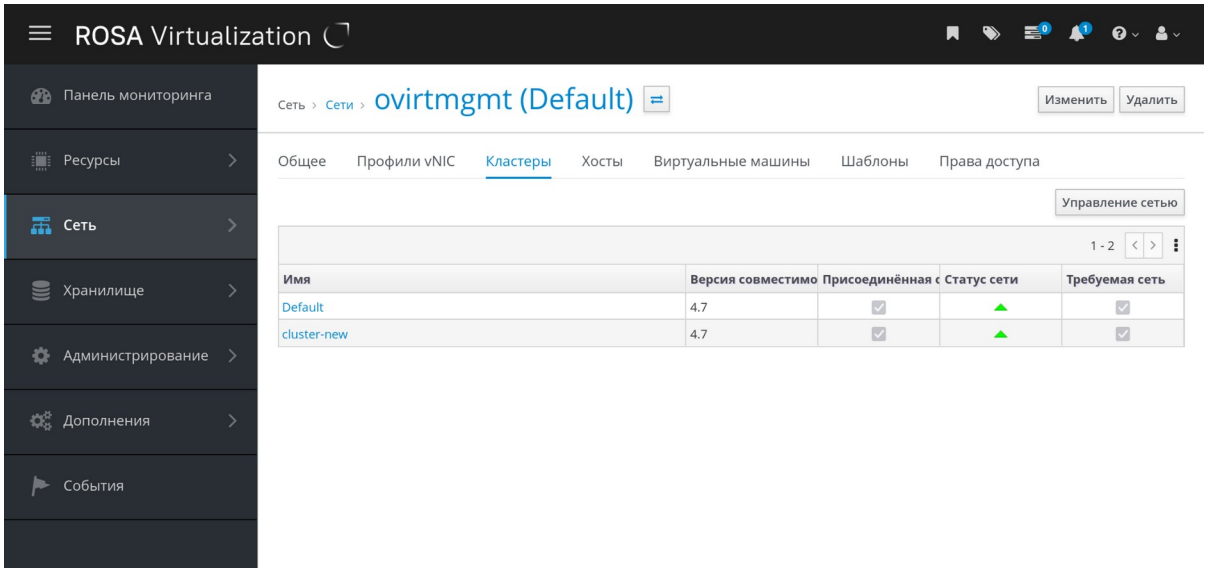

Рис. 107. Сети — вкладка Кластеры

4. Нажмите **Управление сетью**, чтобы открыть окно **Управление сетью**.

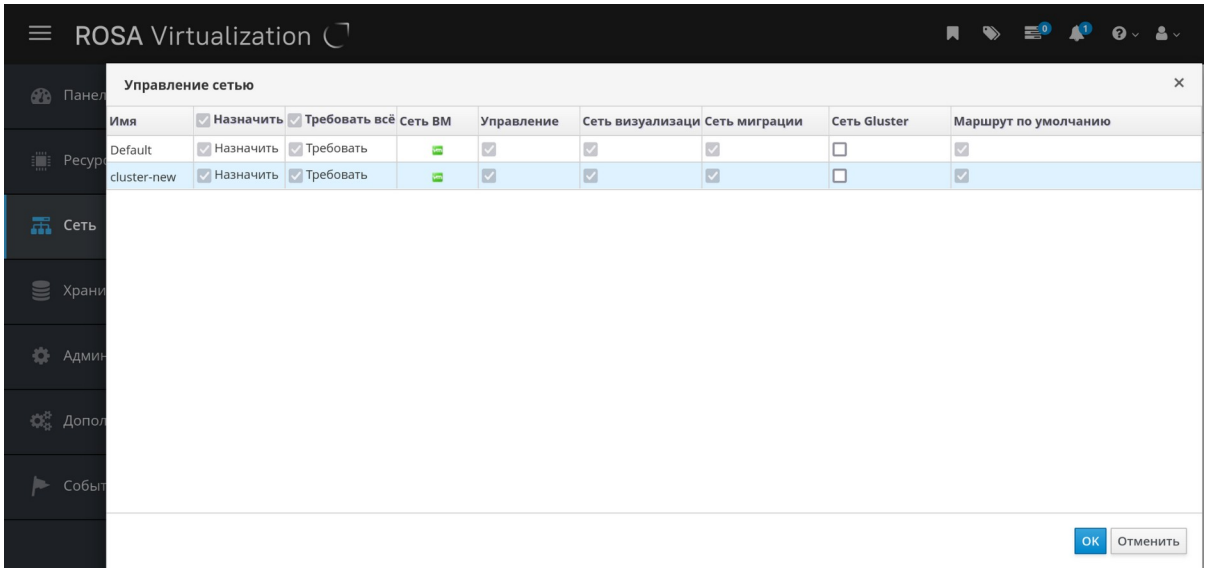

Рис. 108. Окно Управление сетью

5. Установите флажок **Маршрут по умолчанию** для соответствующего кластера.
6. Нажмите **OK**.

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

Примечания, связанные с IPv6:

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

9.1.6. Просмотр или редактирование параметров шлюза логической сети

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

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

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

Просмотр или редактирование параметров шлюза логической сети

1. Нажмите **Ресурсы → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**, чтобы увидеть список и параметры сетевых интерфейсов, подключенных к хосту (Рис. 109).

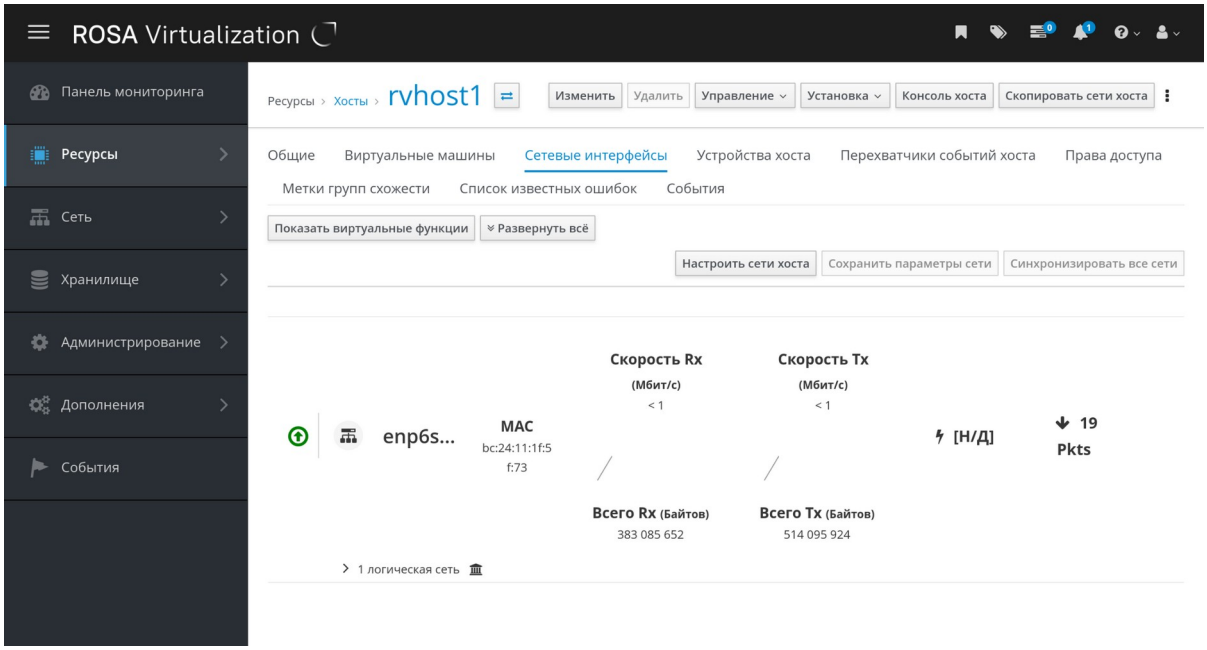

Рис. 109. Вкладка Сетевые интерфейсы, с параметрами сетевых интерфейсов, подключенных к хосту

4. Нажмите кнопку **Настроить сети хоста**. Откроется форма для настройки сетей выбранного хоста (Рис. 110).

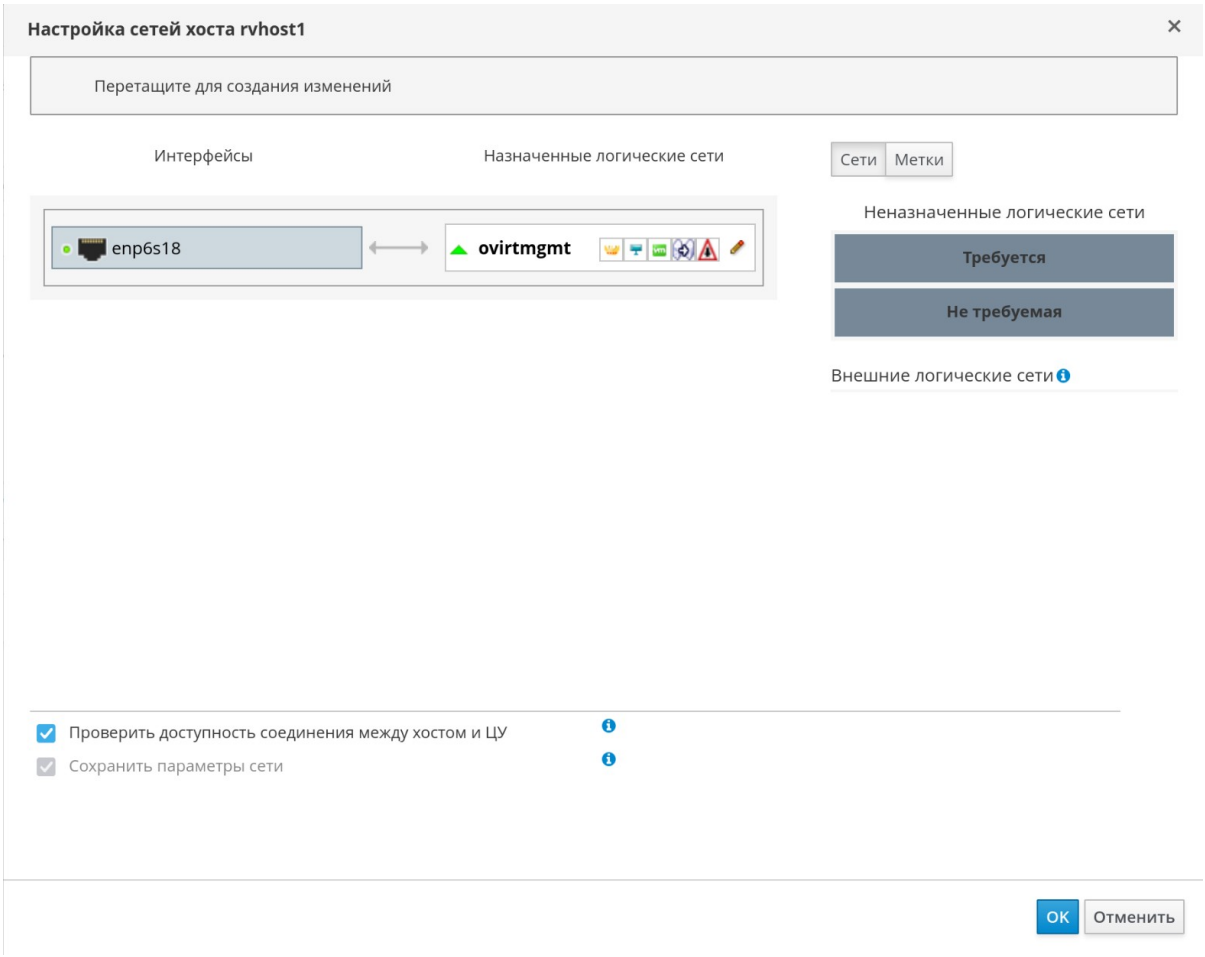

Рис. 110. Форма Настройка сетей хоста

5. Наведите курсор на присвоенную логическую сеть и нажмите на значок карандаша (Рис. 111), чтобы открыть окно **Изменить сеть управления**.

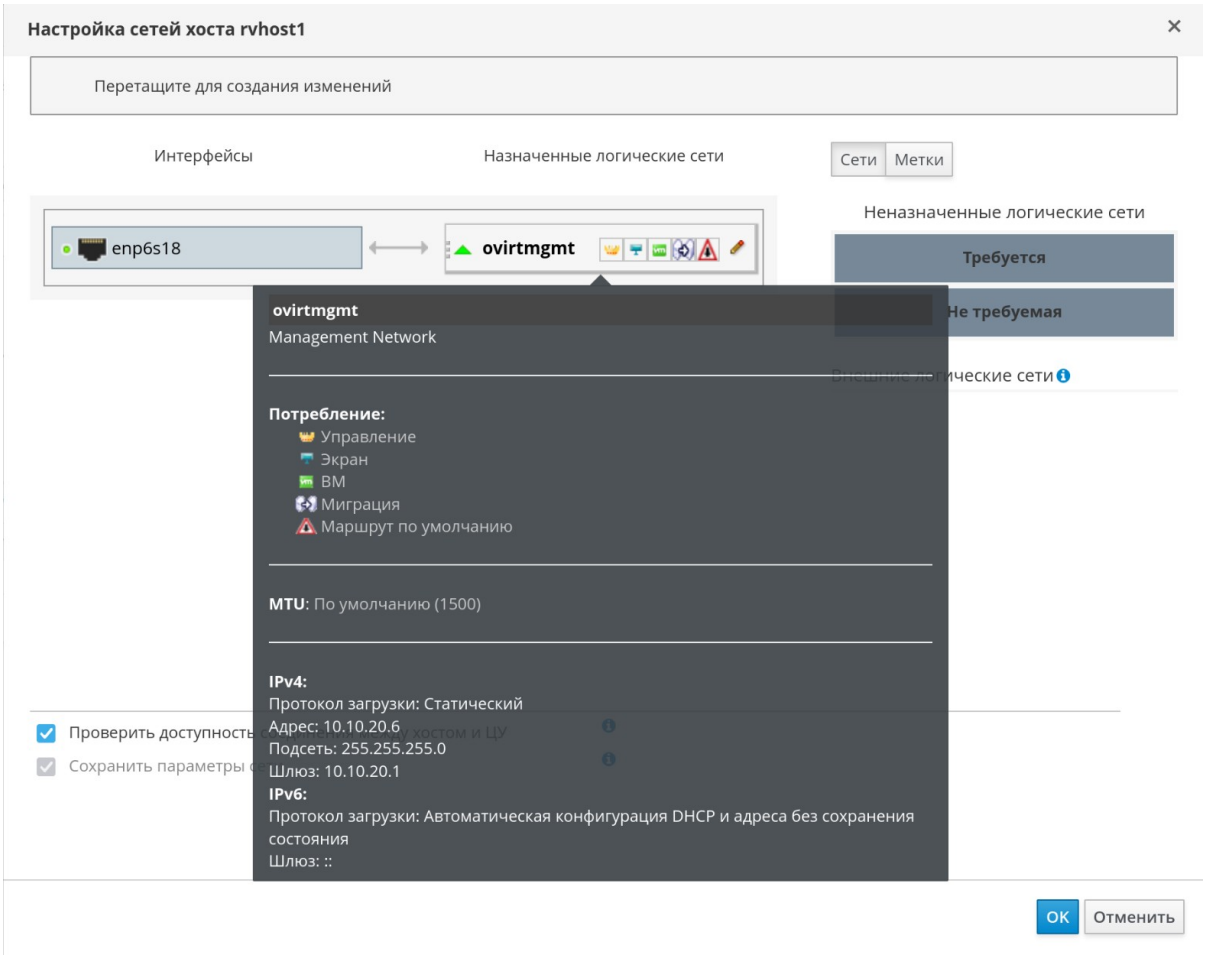

Рис. 111. Информация о настроенной сети ovirtmgmt

6. В окне **Изменить сеть управления** (Рис. 112) показывается имя сети, протокол загрузки, а также IP-адреса, маски подсети и шлюза. Для изменения сведений об адресах вручную выберите **Статический** протокол загрузки.

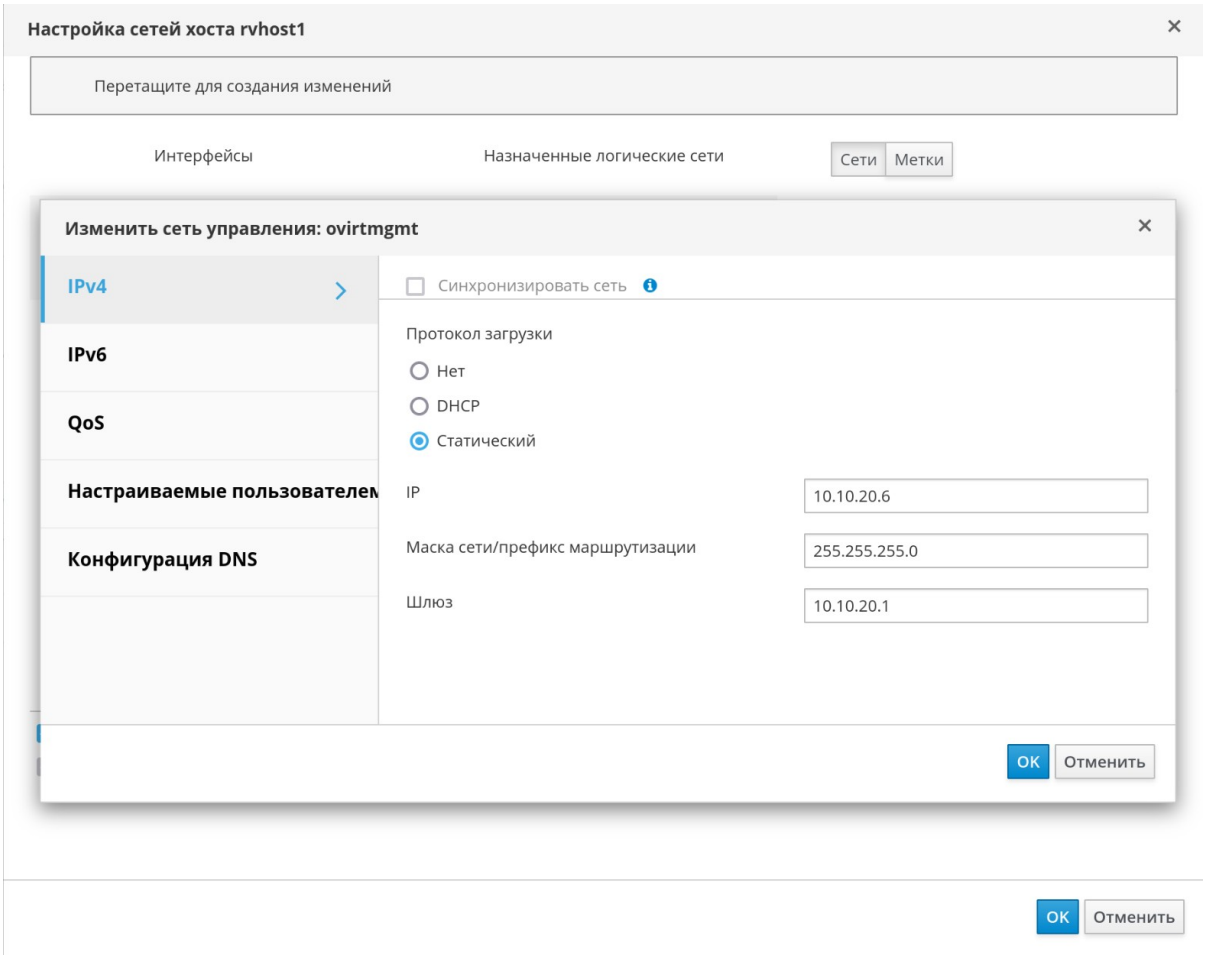

Рис. 112. Форма Изменить сеть управления

9.1.7. Общие параметры логической сети

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

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

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

Поле	Описание
	— 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 даёт возможность одному сетевому интерфейсу быть связанным с несколькими логическими сетями, имеющими разные метки VLAN. Если метки VLAN включены, введите числовое значение в данное текстовое поле
Сеть ВМ	Отметьте этот параметр, если эту сеть используют только ВМ. Если трафик, для передачи которого используется эта сеть, создаётся не виртуальными машинами (например, обмен информацией между хранилищами), не отмечайте этот параметр
MTU	Выберите либо значение **По умолчанию**, которое устанавливает максимальный размер пакета согласно числу, указанному в скобках (), либо значение **Пользовательское**, чтобы указать необходимое число MTU для логической сети. Этот параметр можно использовать, чтобы привести в соответствие число MTU, поддерживаемое логической сетью, с числом MTU, поддерживаемым аппаратными составляющими интерфейса. При выборе значения **Пользовательское** укажите необходимое число в текстовом поле
Метка сети	Параметр позволяет указать новую метку сети или выбрать метку из существующих, уже присвоенных сетевым интерфейсам хоста. При выборе существующей метки логическая сеть будет автоматически присвоена всем сетевым интерфейсам хоста с этой меткой
Группы безопасности	Параметр позволяет присвоить группы безопасности портам в этой логической сети. Значение **Отключено** отключает группы безопасности, значение **Включено** — включает. При создании и подключении порта к этой сети, порт создаётся с активированной безопасностью. Это означает, что доступ к ВМ

Поле	Описание
	или от ВМ выполняется согласно настроенным на данный момент группам безопасности. Значение **Наследовать из конфигурации** означает, что порты наследуют поведение, указанное в файле конфигурации, общем для всех сетей

9.1.8. Параметры кластеров при настройке логических сетей

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

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

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

9.1.9. Параметры профилей vNIC при настройке логических сетей

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

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

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

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

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

Настройка типов трафика для логических сетей

1. Нажмите **Ресурсы → Кластеры**.
2. Нажмите на имя кластера, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Логические сети**.
4. Нажмите **Управление сетями**.
5. Установите необходимые флажки и настройте переключатели (Рис. 113).
6. Нажмите **OK**.

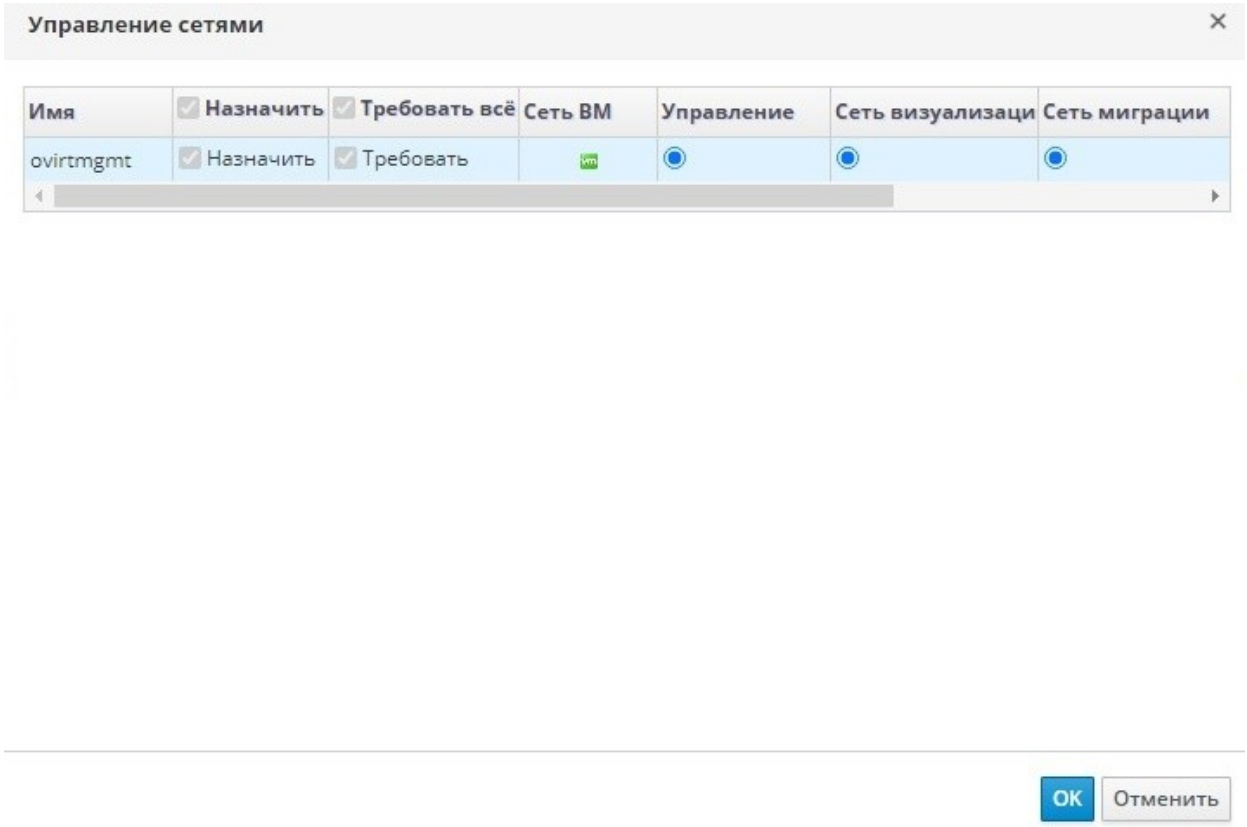

Рис. 113. Управление сетями

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

9.1.11. Параметры в окне «Управление сетями»

В Табл. 9.4 описываются параметры в окне Управление сетями.

Табл. 9.4. Параметры в окне «Управление сетями»

Поле	Описание / действие
Присвоить	Присваивает логическую сеть всем хостам в кластере

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

9.1.12. Изменение конфигурации виртуальной функции сетевой платы

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

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

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

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

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

Редактирование конфигурации виртуальной функции сетевой платы

1. Нажмите **Ресурсы → Хосты**.
2. Нажмите на название хоста с поддержкой SR-IOV, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**.
4. Нажмите кнопку **Настроить сети хоста**.

5. Выберите сетевую карту с поддержкой SR-IOV (отмечается значком ) и нажмите на значок карандаша.
6. Чтобы изменить число виртуальных функций, нажмите кнопку **Параметр числа виртуальных функций** и измените значение в поле **Число виртуальных функций**.

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

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

9.2. Виртуальные сетевые платы (vNIC)

9.2.1. Обзор профиля vNIC

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

9.2.2. Создание или изменение профиля vNIC

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

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

Создание или редактирование профиля vNIC

1. Нажмите **Сеть → Сети**.
2. Нажмите на имя логической сети, чтобы перейти к подробному просмотру.
   Нажмите на **Изменить**, чтобы открыть для просмотра форму **Параметры логической сети**.

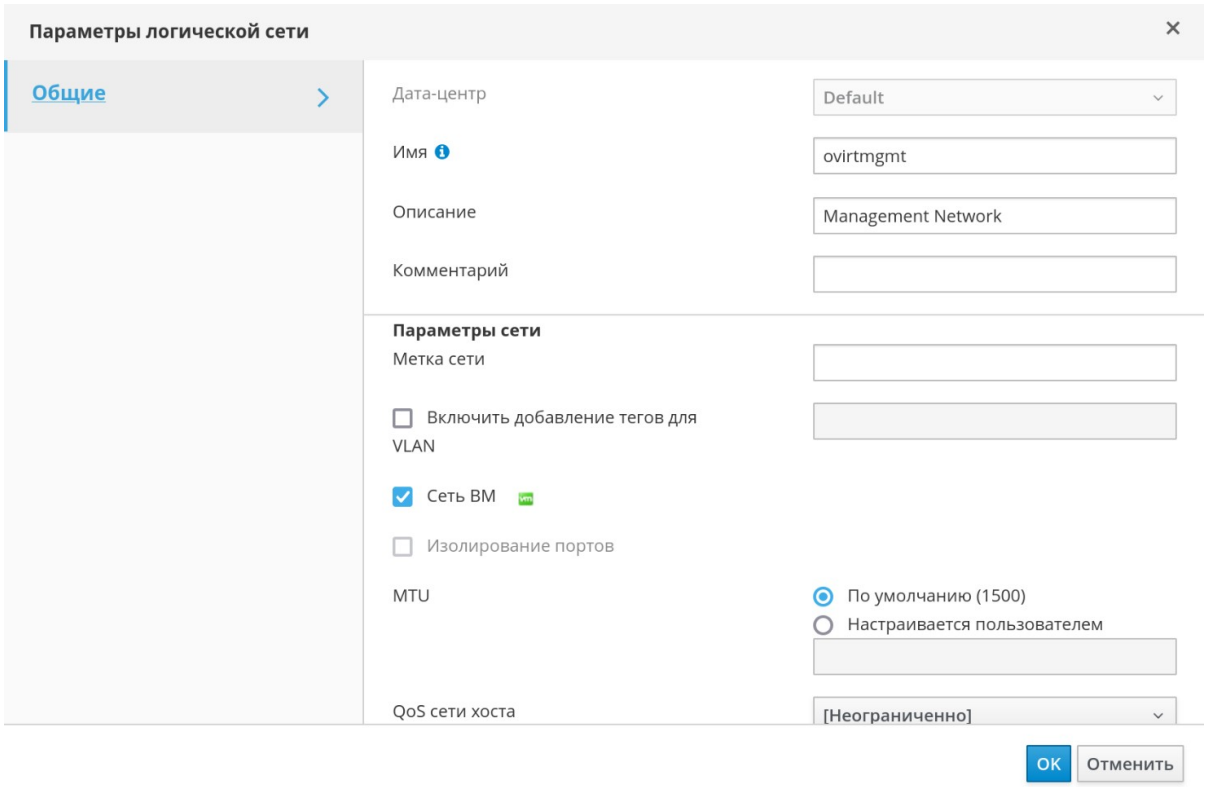

Рис. 114. Форма Параметры логической сети

3. Перейдите на вкладку **Профили vNIC**.

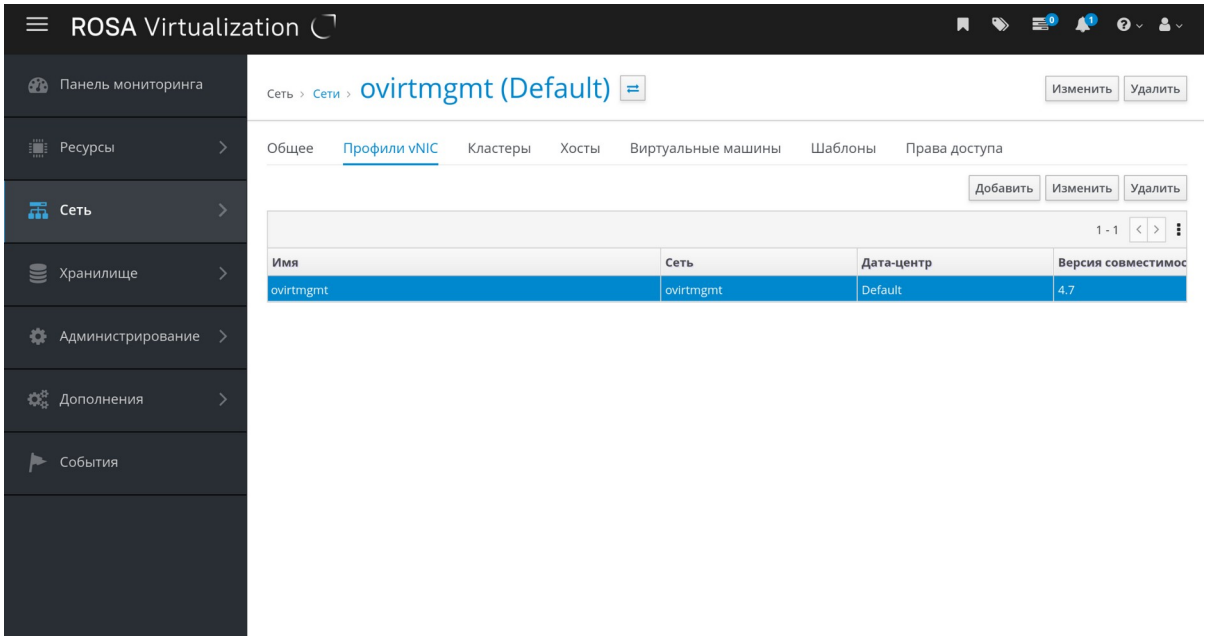

Рис. 115. Вкладка Профили vNIC

4. Нажмите **Добавить** или **Изменить**.

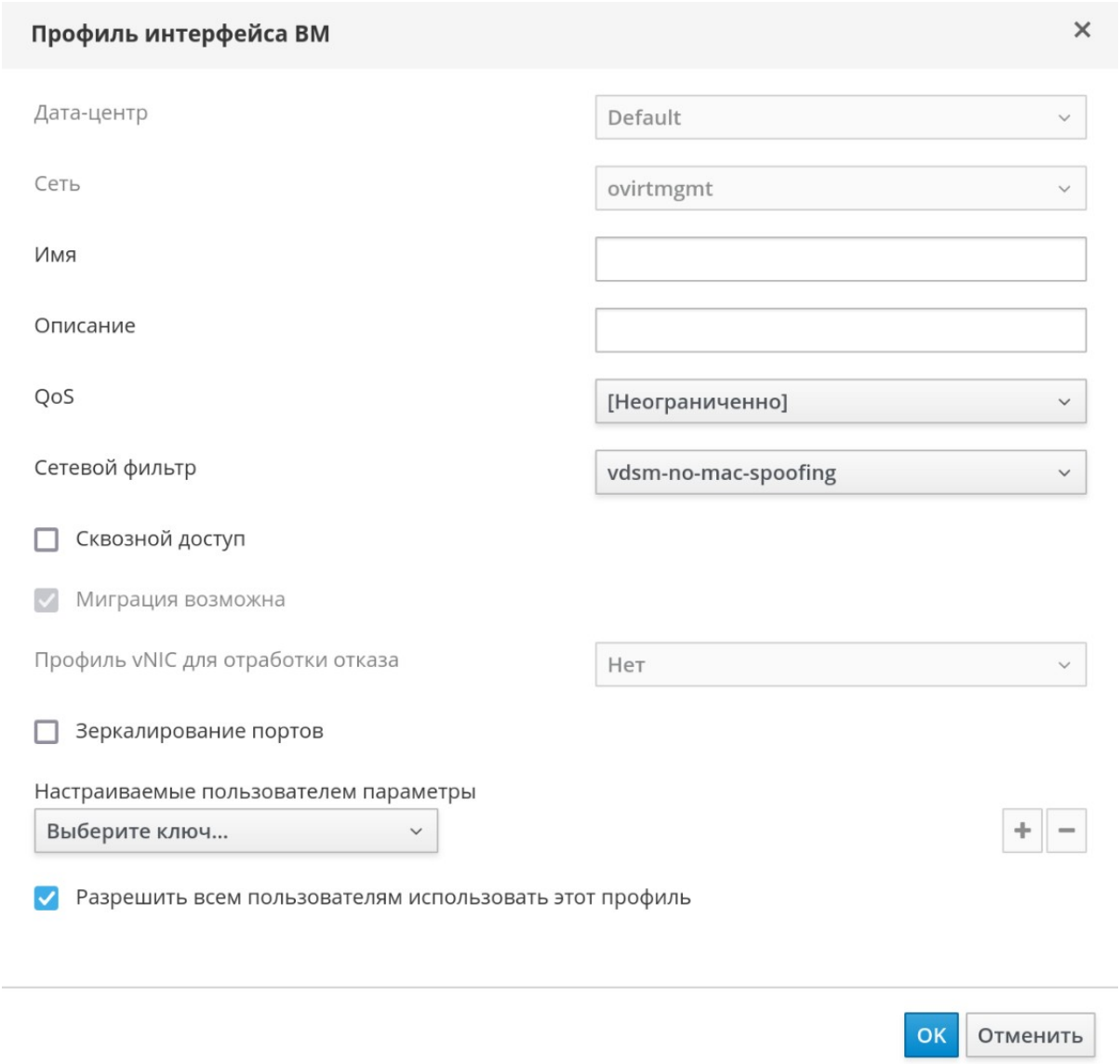

Рис. 116. Добавление профиля интерфейса ВМ

5. Введите **Имя** и **Описание** профиля.
6. В списке **QoS** выберите соответствующую политику качества обслуживания.
7. Из выпадающего списка выберите **Сетевой фильтр** для управления исходящим и входящим трафиком сетевых пакетов виртуальных машин (Рис. 117).

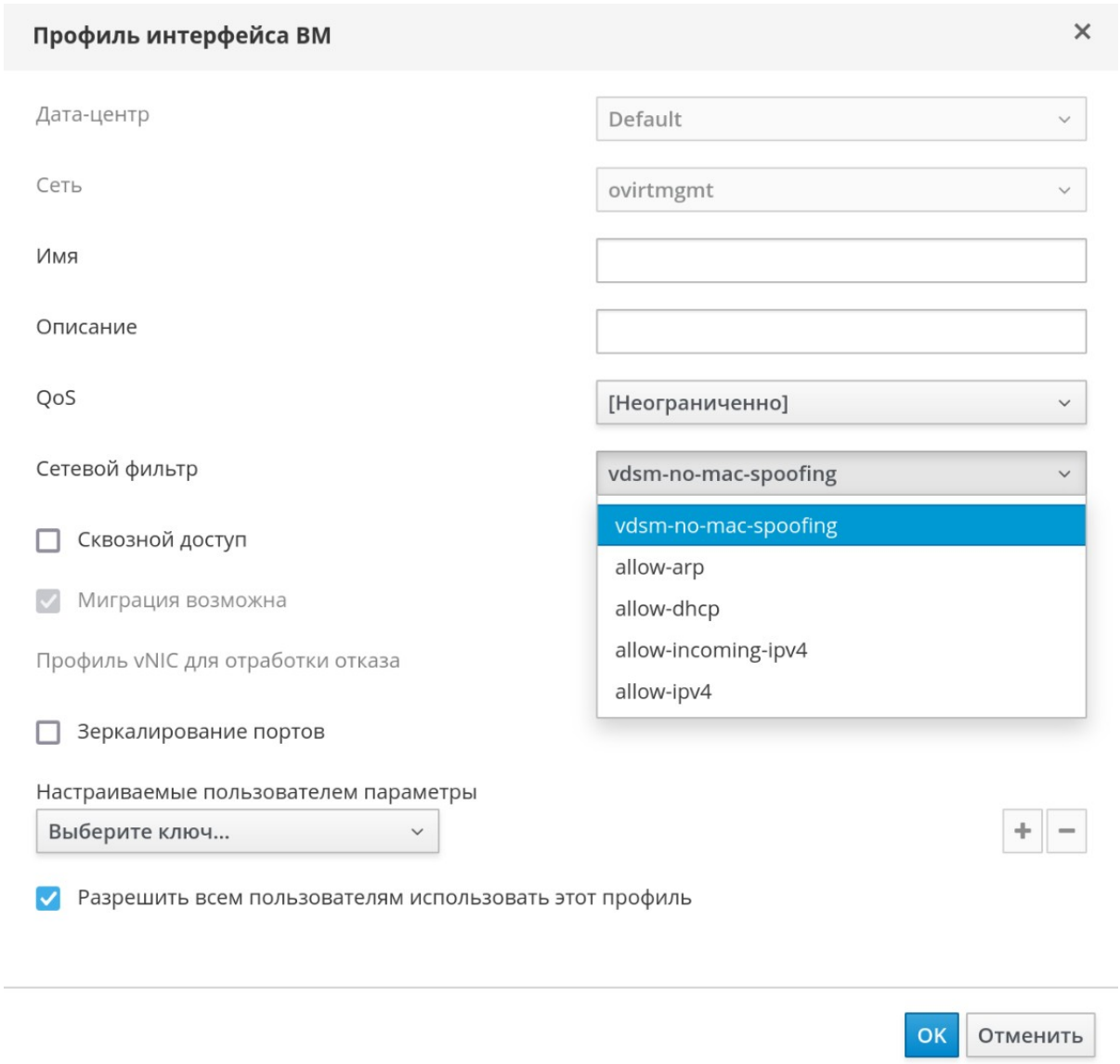

Рис. 117. Выбор параметра Сетевой фильтр для управления исходящим и входящим трафиком сетевых пакетов

8. Установите флажок для параметра **Сквозной доступ**, чтобы включить возможность сквозного доступа для vNIC и разрешить прямое присвоение виртуальной функции устройствам. Включение сквозного доступа отключит QoS, сетевую фильтрацию и зеркалирование портов, так как эти возможности несовместимы со сквозным доступом (см. п. 9.2.4. Включение сквозного доступа в профиле vNIC).
9. При выбранном параметре **Сквозной доступ** снимите флажок (при необходимости) с параметра **Может мигрировать**, чтобы отключить возможность миграции для vNIC, использующих этот профиль.
10. Установите переключатели **Зеркалирование портов** и **Разрешить всем пользователям использовать этот профиль** в необходимое положение.

11. Выберите частное свойство из списка свойств. По умолчанию отображается пункт **Выберите ключ…**. Добавьте или удалите частные свойства с помощью кнопок + (плюс) или – (минус) соответственно.
12. Нажмите **OK**.

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

9.2.3. Параметры в окне «Профиль сетевого адаптера ВМ»

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

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

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

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

9.2.4. Включение сквозного доступа в профиле vNIC

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

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

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

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

Включение сквозного доступа

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

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

9.2.5. Удаление профиля vNIC

Удаление профиля vNIC

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

9.2.6. Присвоение групп безопасности профилям vNIC

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

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

выполнив следующую команду в системе с установленным комплексом OpenStack Networking:

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

Присвоение групп безопасности профилям vNIC

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

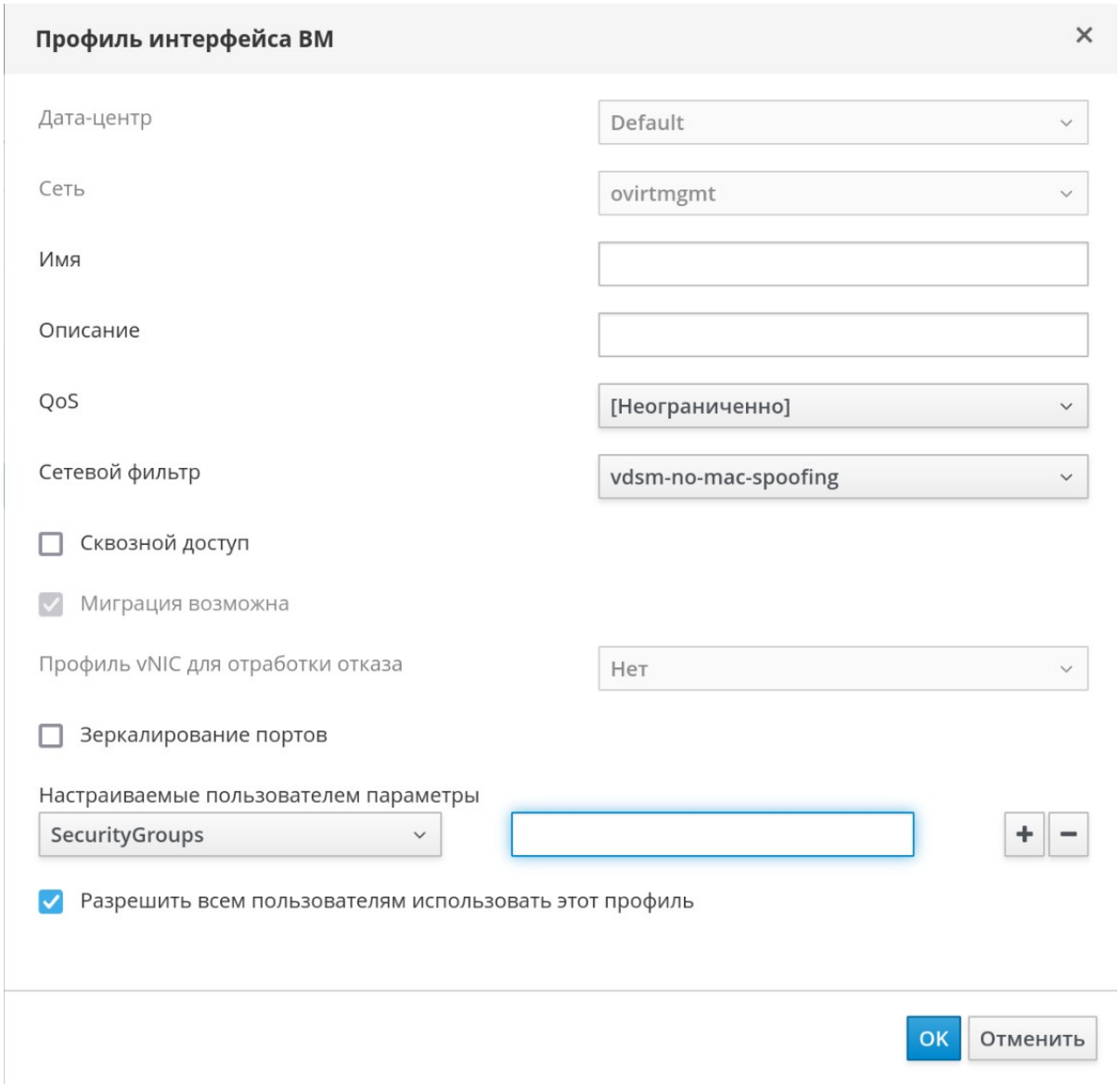

Рис. 118. Настройка параметра SecurityGroups

6. Введите ID группы безопасности в текстовое поле, чтобы присвоить её профилю vNIC.
7. Нажмите **OK**.

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

9.2.7. Полномочия пользователей на профили vNIC

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

Пользовательские полномочия на профиль vNIC

1. Нажмите **Сеть → Профиль vNIC**.
2. Нажмите на профиль vNIC, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Права доступа**, чтобы просмотреть текущие полномочия пользователя для этого профиля.

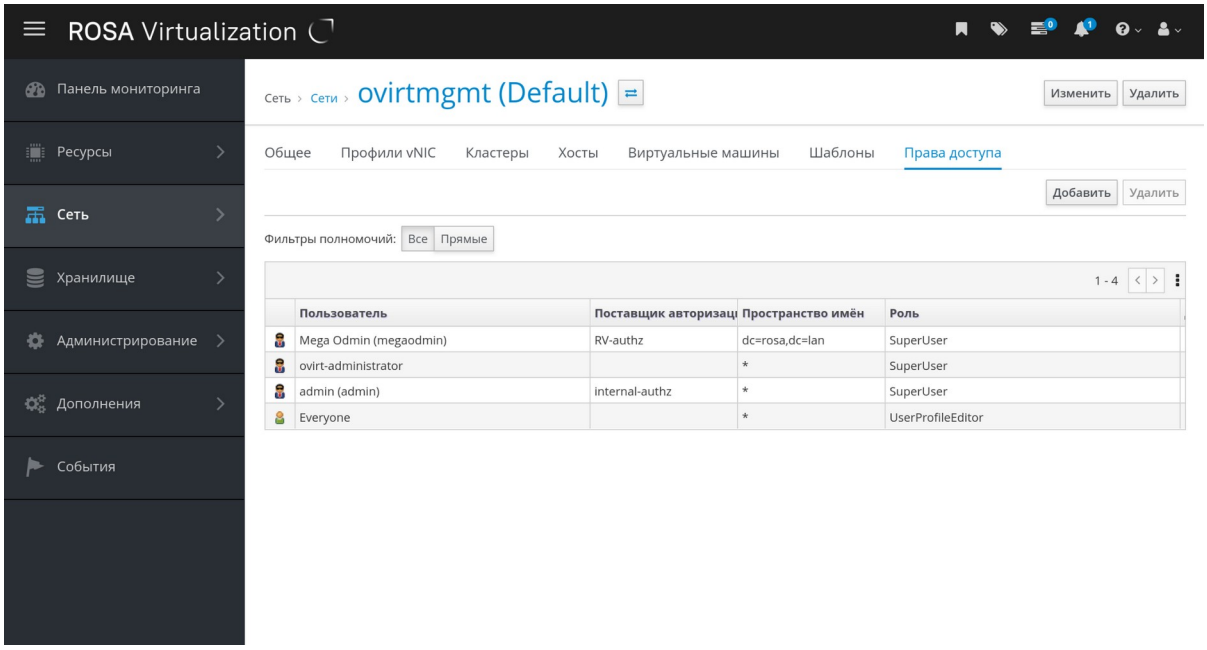

Рис. 119. Вкладка Права доступа

4. Чтобы изменить полномочия пользователя на профиль vNIC нажмите **Добавить** или **Удалить**.

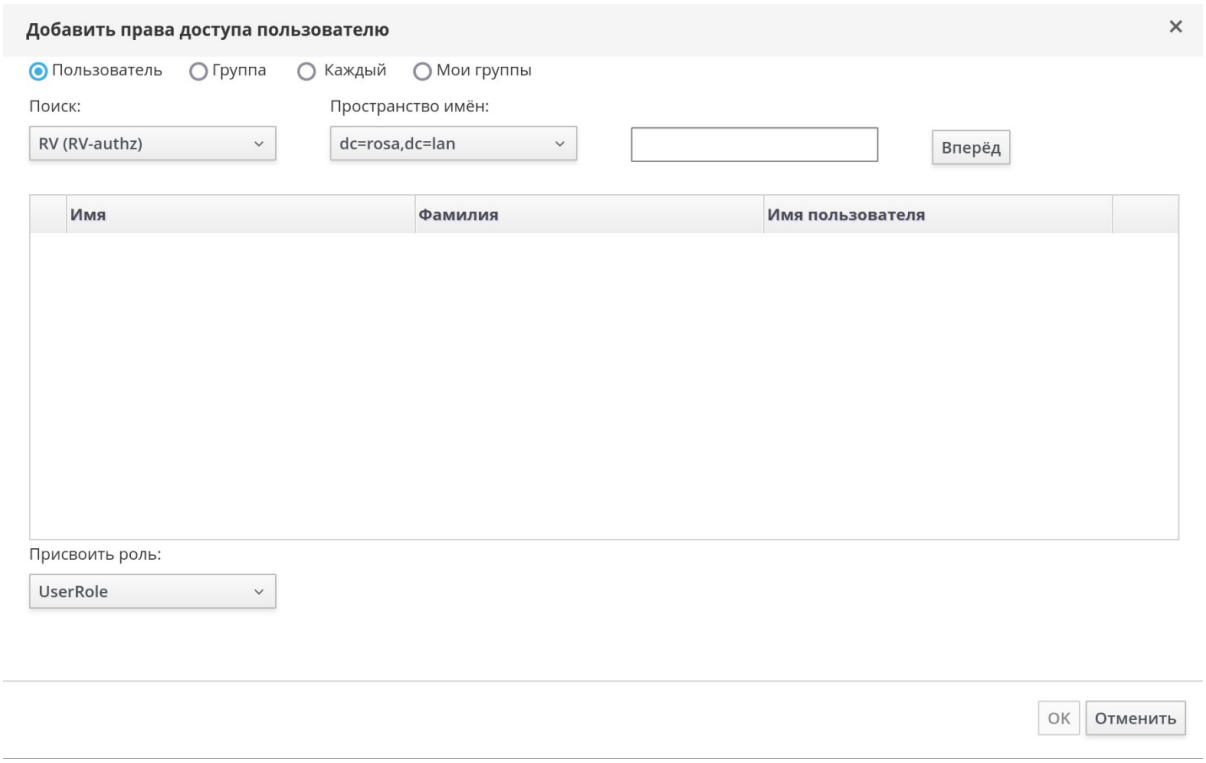

Рис. 120. Форма Добавить права доступа пользователю

5. В окне **Добавить полномочия пользователю** нажмите **Мои группы**, чтобы отобразить группы пользователя. Этот параметр можно использовать для добавления полномочий другим пользователям в этих группах.

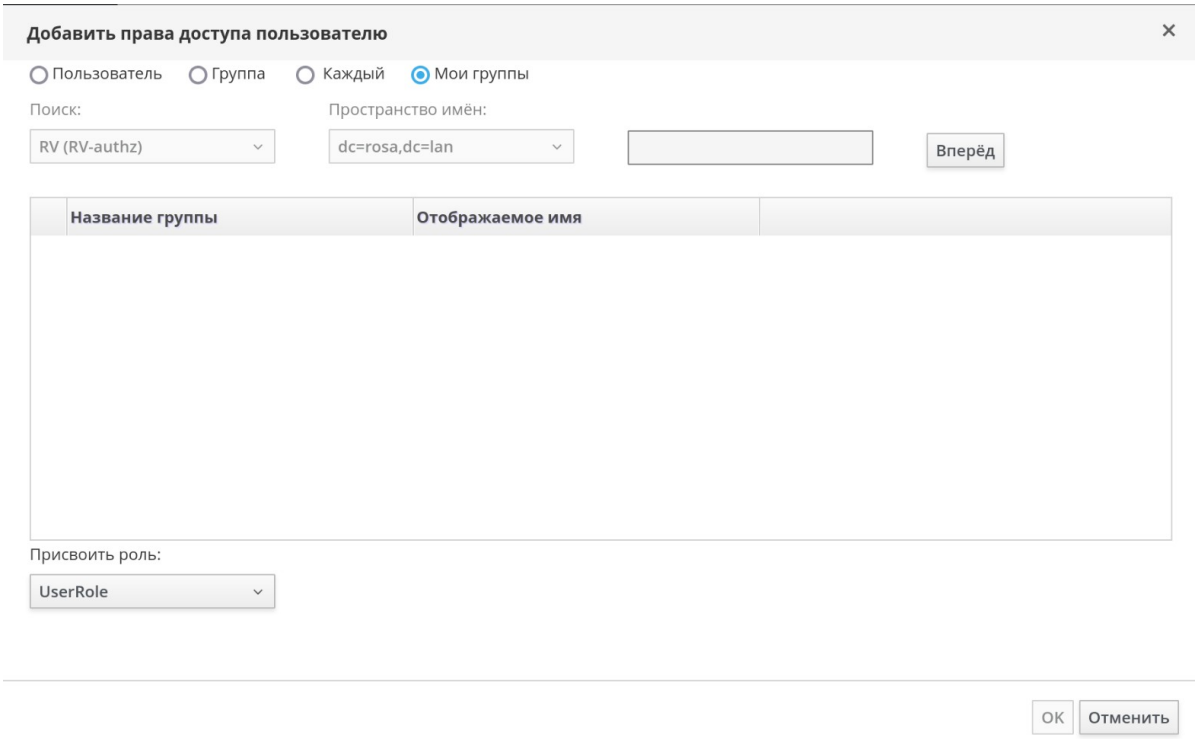

Рис. 121. Форма Мои группы

9.2.8. Настройка профилей vNIC для интеграции с UCS

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

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

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

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

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

Настройка частного свойства устройства

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

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

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

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

3. Перезапустите службу `ovirt-engine`:

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

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

Настройка профиля vNIC для интеграции в UCS

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

9.3. Сети внешних поставщиков

9.3.1. Импортирование сетей из внешних поставщиков

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

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

Импортирование сетей внешнего поставщика

1. Нажмите **Сеть → Сети**.
2. Нажмите **Импорт**.

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

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

9.3.2. Ограничения при использовании сетей внешних поставщиков

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

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

9.3.3. Настройка подсетей в логических сетях внешних поставщиков

Логическая сеть внешнего поставщика может присваивать IP-адреса виртуальным машинам только в том случае, если в этой логической сети была настроена одна или несколько подсетей. Если подсети не были настроены, виртуальным машинам не будут присвоены IP-адреса. При наличии одной подсети, виртуальным машинам будут присвоены адреса из этой подсети, а при наличии нескольких подсетей, ВМ будут

присвоены адреса из одной из доступных подсетей. За присвоение IP-адресов отвечает служба DHCP, предоставляемая внешним поставщиком сети, в которой располагается логическая сеть.

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

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

9.3.4. Добавление подсетей в логических сетях внешних поставщиков

Добавление подсетей в логических сетях внешних поставщиков

1. Нажмите **Сеть → Сети**.
2. Нажмите на имя логической сети, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Подсети**.
4. Нажмите **Добавить**.
5. Укажите **Имя** и **CIDR** новой подсети.
6. Из выпадающего списка **Версия IP** выберите **IPv4** или **IPv6**.
7. Нажмите **OK**.

Примечание — для IPv6 поддерживается только статическая адресация.

9.3.5. Удаление подсетей из логических сетей внешних поставщиков

Удаление подсетей из логических сетей внешних поставщиков

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

9.3.6. Присвоение групп безопасности логическим сетям и портам

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

В системе виртуализации ROSA Virtualization группы безопасности по умолчанию отключены.

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

Добавление групп безопасности в логические сети

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

9.4. Хосты и организация сетей

9.4.1. Обновление сведений о характеристиках хоста

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

Обновление сведений о характеристиках хоста

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

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

9.4.2. Изменение параметров сетевых интерфейсов и присвоение хостам логических сетей

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

Примечания:

- Единственным способом изменить IP-адрес хоста в системе виртуализации является удаление хоста и повторное его добавление.
- Сведения о том, как изменить параметры VLAN хоста, приведены в п. 9.4.4. Изменение параметров VLAN хоста.
- Логические сети внешних поставщиков невозможно присвоить физическим сетевым интерфейсам хоста. Такие сети присваиваются хостам динамически по мере требований со стороны ВМ.

- Если коммутатор был настроен на предоставление сведений о протоколе LLDP, для просмотра текущей конфигурации порта коммутатора наведите курсор на физический сетевой интерфейс. Это может помочь в предотвращении создания неправильных конфигураций. Перед присвоением логических сетей рекомендуется проверить следующую информацию:

– *Описание порта (TLV тип 4)* и *Системное имя (TLV тип 5)*. Параметры помогают определить, на какие порты и на какой коммутатор накладываются интерфейсы хоста.
– *Идентификатор VLAN порта*. Параметр показывает встроенный идентификатор VLAN, настроенный на порте коммутатора для кадров Ethernet без меток. Все виртуальные LAN, настроенные на порте коммутатора, показываются в виде сочетаний *VLAN имя* и *VLAN идентификатор*.

Изменение параметров сетевых интерфейсов и присвоение хостам логических сетей

1. Нажмите **Ресурсы → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**.
4. Нажмите **Настроить сети хоста**.
5. При необходимости наведите курсор на сетевой интерфейс хоста, чтобы просмотреть сведения о конфигурации, предоставляемой коммутатором.
6. Подключите логическую сеть к физическому сетевому интерфейсу хоста — выберите и перетащите логическую сеть в область **Назначенные логические сети** рядом с физическим сетевым интерфейсом хоста.

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

7. Настройте локальную сеть:

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

   b. Во вкладке **IPv4** выберите протокол загрузки — **Нет**, **DHCP** или **Статический**. При выборе статического протокола укажите **IP**, **Префикс сетевой маски/маршрутизации** и **Шлюз**.

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

- Укажите Статический протокол загрузки.

- Укажите длину **Префикса маршрутизации** с помощью прямой косой черты и десятичного числа (например: /48).

- Укажите **IP** — полный адрес IPv6 сетевого интерфейса хоста (например: 2001:db8::1:0:0:6).

- Укажите **Шлюз** — адрес IPv6 маршрутизатора источника (например: 2001:db8::1:0:0:1).

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

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

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

c. Используйте параметры во вкладке **QoS** для переопределения качества обслуживания сети по умолчанию. Выберите **Переопределить QoS** и укажите нужные значения в следующих полях:

   - **Взвешенная доля**: означает, какую долю пропускной способности логического канала нужно выделить конкретной сети относительно других сетей, прикреплённых к этому же логическому каналу. Точная доля зависит от суммы долей всех сетей на этом канале. По умолчанию
     это число в диапазоне от 1 до 100.
   - **Предел скорости (Мбит/с)**: максимальная пропускная способность сети.
   - **Гарантированная скорость (Мбит/с)**: минимальная пропускная способность, требуемая для сети. Гарантированная скорость на деле не гарантируется, и будет изменяться в зависимости от сетевой инфраструктуры и гарантированной скорости, запрашиваемой другими сетями на этом же логическом канале.

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

```
forward_delay=1500
gc_timer=3765
group_addr=1:80:c2:0:0:0
```

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

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

Например:

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

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

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

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

f. Для настройки протокола FCoE перейдите на вкладку **Настраиваемые пользователем параметры** и в выпадающем списке выберите параметр **fcoe**. Введите действительный ключ и значение, придерживаясь следующего синтаксиса: *ключ=значение*. Минимальное требуемое значение: `enable=yes`. Также можно добавить `dcb= and auto_vlan=[yes|no]`. Отделяйте записи символом пробела. Параметр **fcoe** по умолчанию недоступен и его необходимо добавить с помощью утилиты настройки виртуализированного ЦУ (см. Раздел В.3. Настройка использования протокола FCoE в виртуализированном ЦУ).

Примечание — для использования FCoE рекомендуется отдельная выделенная логическая сеть.

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

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

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

9.4.3. Синхронизация сетей хостов

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

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

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

- Изменения конфигурации были сделаны на хосте, а не в окне **Настроить логические сети** (например, изменение идентификатора VLAN на физическом хосте / изменение **Пользовательского MTU** на физическом хосте).

- Хост был перемещён в другой дата-центр с тем же сетевым именем, но с другими значениями / параметрами.
- Свойство сети **Сеть ВМ** было изменено при помощи удаления моста вручную с хоста.

Использование следующих практических решений может предотвратить рассинхронизацию хостов:

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

Синхронизация хостов

Синхронизация определений сетевых интерфейсов хоста включает в себя применение используемых определений виртуализированного ЦУ на хосте. Если эти определения не являются требуемыми определениями, то после синхронизации хостов, обновите определения хостов с помощью интерфейса на Портале администрирования.

Сети хостов можно синхронизировать на трёх уровнях:

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

Синхронизация сетей хоста на уровне логической сети

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

Синхронизация сетей хоста на уровне хоста

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

Синхронизация сетей хоста на уровне кластера

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

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

9.4.4. Изменение параметров VLAN хоста

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

Изменение параметров VLAN хоста с сохранением синхронизации сетей

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

При смене VLAN ID сети управления появляется следующее предупреждение:

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

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

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

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

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

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

Добавление нескольких VLAN на один сетевой интерфейс с использованием логических сетей

1. Нажмите **Ресурсы → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**.
4. Нажмите **Настроить сети хоста**.
5. Перетащите логические сети с метками VLAN в область **Присвоенные логические сети** рядом с физическим сетевым интерфейсом. Благодаря меткам VLAN физическому сетевому интерфейсу можно присвоить несколько логических сетей.

6. Измените параметры логических сетей:

    a. Наведите курсор на присвоенную логическую сеть и нажмите на значок карандаша.
    b. Если определение логической сети не синхронизировано с сетевой конфигурацией на хосте, установите флажок для параметра **Синхронизировать сеть**.
    c. Выберите Протокол загрузки:
        - **Нет**.
        - **DHCP**.
        - **Статический**.
    d. Укажите **IP** и **Маску подсети**.
    e. Нажмите **OK**.
7. Установите флажок для параметра **Проверить доступность соединения между хостом и ЦУ**, чтобы выполнить проверку сети. Обратите внимание, что это может быть сделано только для хостов, находящихся в режиме обслуживания.
8. Нажмите **OK**.

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

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

9.4.6. Присвоение дополнительных адресов IPv4 сетям хостов

Сети хоста, такие как сеть управления `ovirtmgmt`, изначально создаются только с одним IP-адресом. Это означает, что если в файле конфигурации сетевой платы (например, */etc/sysconfig/network-scripts/ifcfg-eth01*) настроено несколько IP-адресов, то сети хоста будет присвоен только первый указанный IP-адрес. Остальные адреса могут потребоваться при подключении к хранилищу или к серверу в отдельной частной подсети, использующей ту же самую сетевую плату.

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

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

Присвоение дополнительных адресов IPv4 сетям хоста

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

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

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

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

3. Перезапустите службу `ovirt-engine`:

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

4. В главном меню Портала администрирования нажмите **Ресурсы → Хосты**.
5. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
6. Перейдите на вкладку **Сетевые интерфейсы** и нажмите **Настроить сети хоста.**
7. Наведите курсор на присвоенную логическую сеть и нажмите на значок карандаша.
8. Из выпадающего списка **Настраиваемые пользователем параметры** выберите пункт **ipv4_addr** и добавьте дополнительный IP-адрес и префикс сети (например,

5.5.5.5/24). Обратите внимание, что несколько IP-адресов должны разделяться запятой.

9. Нажмите **OK**, чтобы закрыть окно **Параметры сети**.
10. Нажмите **OK**, чтобы закрыть окно **Настроить сети хоста**.

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

9.4.7. Добавление сетевых меток сетевым интерфейсам хоста

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

Существуют следующие способы добавления меток сетевому интерфейсу хоста:

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

Добавление сетевых меток хосту вручную на Портале администрирования

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

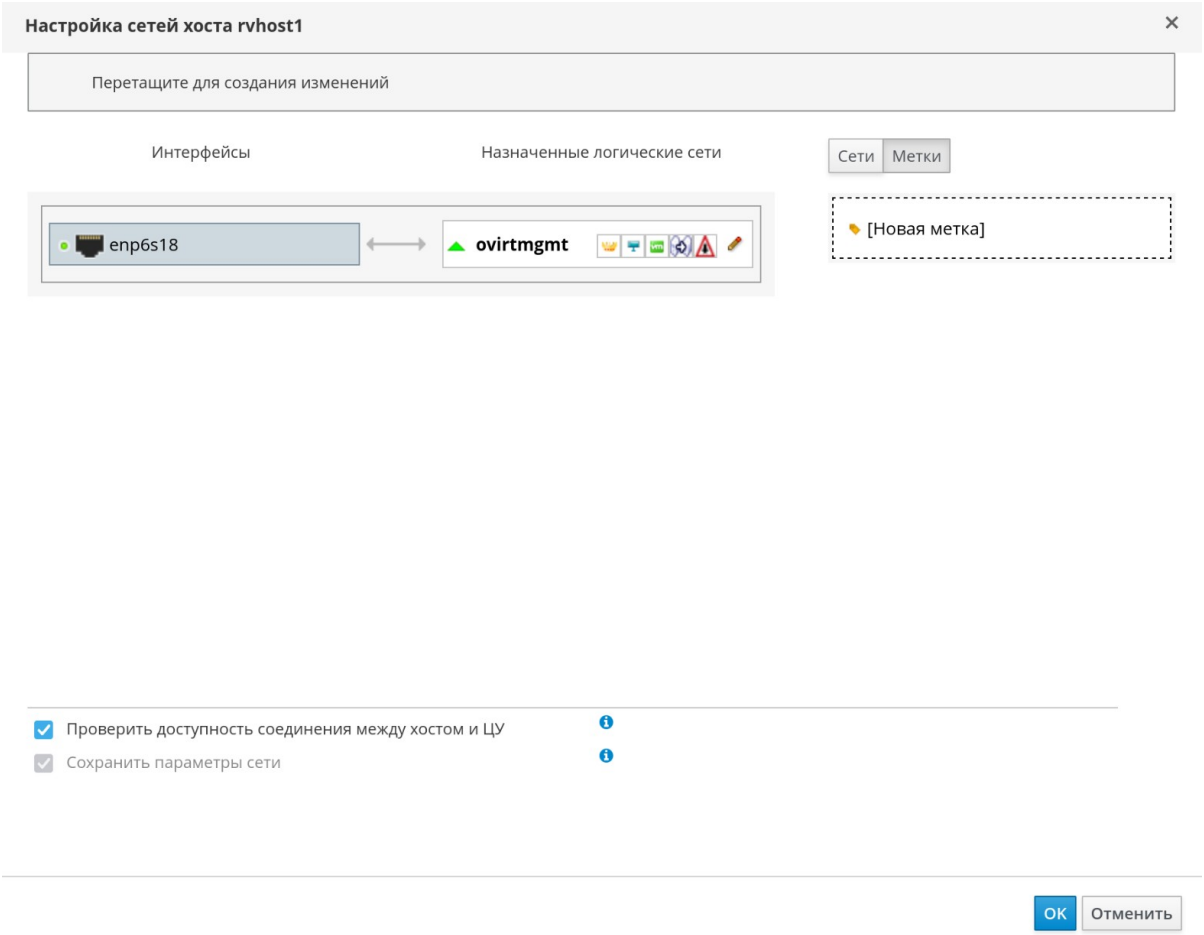

Рис. 122. Настройка сетей хоста - добавление меток

6. Нажмите **Новая метка**. Выберите физический сетевой интерфейс, которому нужно назначить метку.

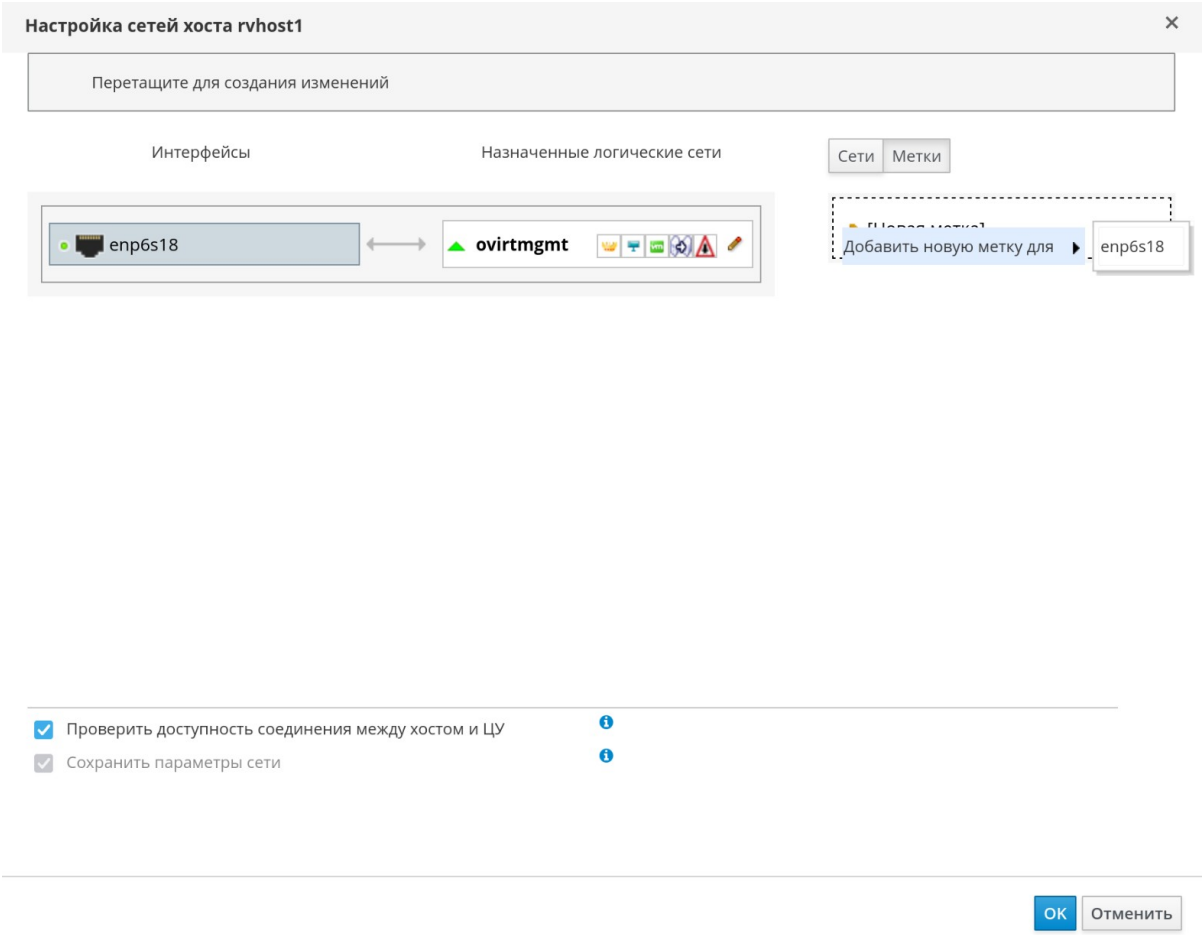

Рис. 123. Выбор интерфейса для добавления новой метки

7. В поле **Метка** введите имя сетевой метки.

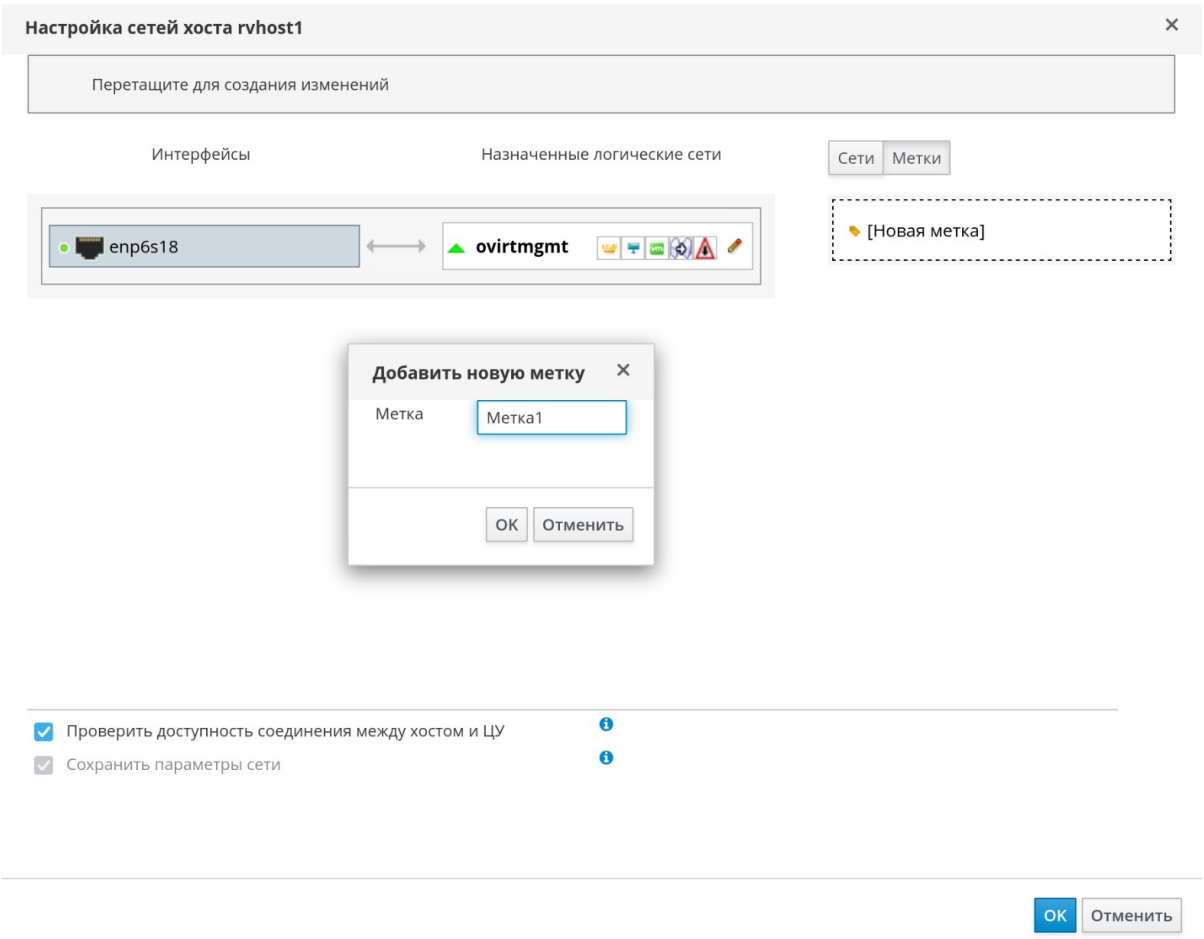

Рис. 124. Форма Добавить новую метку

8. Нажмите **OK**.

Добавление сетевых меток хосту автоматически с помощью службы меток LLDP

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

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

Предварительные условия:

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

Последовательность действий

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

- `username` - имя пользователя администратора виртуализированного ЦУ. Значение по умолчанию: `admin@internal`.
- `password` - пароль администратора виртуализированного ЦУ. Значение по умолчанию: `123456`.

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

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

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

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

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

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

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

9.4.8. Изменение полного доменного имени хоста

Изменение полного доменного имени (FQDN) хоста

1. Переведите хост в режим обслуживания, при котором выполняется динамическая миграция ВМ на другой хост (см. п. 10.3.12. Перевод хоста в режим обслуживания).
2. Нажмите **Удалить**, а затем нажмите **ОК**, чтобы удалить хост с Портала администрирования.

3. Укажите новое имя хоста с помощью утилиты `hostnamectl`:

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

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

9.4.9. Поддержка организации сетей с помощью IPv6

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

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

Ограничения, связанные с IPv6:

- Поддерживается только статическая адресация IPv6. Динамическая адресация с помощью DHCP, а также автоматическая настройка адресов без сохранения состояния не поддерживаются.
- Адресация для двойного стека (IPv4 и IPv6) не поддерживается.
- Сетевые конфигурации OVN могут использовать только IPv4 или IPv6.
- Перевод кластеров с использования IPv4 на использование IPv6 не поддерживается.
- Для IPv6 можно настроить только один шлюз на хост.
- Если две сети разделяют один шлюз (находятся в одной подсети), то можно перенести роль маршрута по умолчанию из сети управления (`ovirtmgmt`) в другую логическую сеть. Хост и виртуализированный ЦУ должны иметь один и тот же шлюз IPv6. Если хост и виртуализированный ЦУ находятся в разных подсетях, ЦУ может потерять связь с хостом из-за потенциального удаления шлюза IPv6.
- Использование домена хранилищ на базе `glusterfs`, где сервер `gluster` использует адресацию IPv6, не поддерживается.

9.5. Объединение сетевых интерфейсов

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

- Скорость передачи нескольких агрегированных интерфейсов выше, чем у одного отдельного интерфейса.

- Устойчивость к отказам, так как устройство связки не откажет до тех пор, пока не откажут все интерфейсы в его составе.

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

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

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

На портах коммутатора должна быть включена возможность агрегации.

Создать устройство связки можно одним из следующих способов:

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

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

9.5.1. Создание устройства сетевой связки вручную на Портале администрирования

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

Создание устройства связки вручную на Портале администрирования

1. Нажмите **Ресурсы → Хосты**.
2. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Сетевые интерфейсы**, чтобы увидеть список физических сетевых интерфейсов, присоединённых к хосту.
4. Нажмите **Настроить сети хоста**.
5. Проверьте параметры коммутатора. Если на коммутаторе было настроено предоставление информации о протоколе обнаружения топологии канального уровня (LLDP), наведите курсор на область физического интерфейса, чтобы просмотреть конфигурацию агрегирования портов коммутатора.
6. Перетащите сетевую карту на другую карту (две сетевые карты формируют новую связку) или в связку (добавление новой сетевой карты в уже существующую связку).

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

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

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

Например:

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

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

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

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

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

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

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

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

Сетевые платы с несовместимыми логическими сетями нельзя агрегировать.

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

Предварительные условия:

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

Последовательность действий

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

   - `username` - имя пользователя администратора виртуализированного ЦУ. Значение по умолчанию: `admin@internal`.
   - `password` - пароль администратора виртуализированного ЦУ. Значение по умолчанию: `123456`.

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

   - `clusters` - список кластеров (через запятую), на которых должна выполняться служба. Например, `Cluster*` означает, что служба меток будет выполняться в кластерах, название которых начинается со слова `Cluster`. Чтобы служба меток выполнялась во всех кластерах в дата-центре, введите символ `*` (звёздочка). Значение по умолчанию: `Def*`.
   - `api_url` - полный URL-адрес API виртуализированного ЦУ. Значение по умолчанию: `https://`*`полное_доменное_имя_ЦУ`*`/ovirt-engine/api`.
   - `ca_file` - путь до частного файла сертификата центра сертификации. Если сертификат не используется, оставьте пустое поле. Значение по умолчанию: пустое поле.
   - `auto_bonding` – параметр включает возможности службы меток LLDP по созданию сетевых агрегаций. Значение по умолчанию: `true`.
   - `auto_labeling` - параметр включает возможности службы меток LLDP по созданию меток. Значение по умолчанию: `true`.

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

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

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

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

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

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

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

9.5.3. Режимы агрегирования

Алгоритм рассеивания пакетов определяется режимом агрегирования.

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

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

- `(Режим 1) Active-Backup` — активной является только одна сетевая карта. При сбое активной карты её заменяет одна из запасных. Адрес MAC этой связки виден только на порте сетевого адаптера, что предотвращает путаницу, которая может случиться в случае смены адреса MAC связки, в соответствии с адресом MAC новой активной сетевой карты.
- `(Режим 2) Load Balance (balance-xor)` — сетевая карта, передающая пакеты, выбирается с помощью выполнения операции XOR для исходного и целевого адресов MAC, умноженных на фактор `modulo` общего числа сетевых карт. Этот алгоритм обеспечивает выбор одной и той же сетевой карты для каждого из целевых адресов MAC.
- `(Режим 3) Broadcast` — пакеты передаются на все сетевые карты.
- `(Режим 4) Dynamic Link Aggregation(802.3ad)` — режим агрегирования по умолчанию. Сетевые карты объединяются в группы, разделяющие одни и те же параметры скорости и дуплекса. В активной группе связки используются все сетевые карты.

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

Для просмотра идентификаторов агрегатора выполните следующую команду:

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

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

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

- `(Режим 6) Balance-ALB (Adaptive Load-Balance)` — для балансировки входящей нагрузки используется согласование ARP.

Глава 10. Хосты

10.1. Введение в понятие хостов

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

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

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

Общее описание хоста виртуализации

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

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

- Хост принадлежит только одному кластеру в системе виртуализации ROSA Virtualization (см. Глава 8. Кластеры)
- Хост имеет ЦП с поддержкой модулей аппаратной виртуализации AMD-V или Intel® VT.
- Хост имеет процессор с поддержкой всех функций того типа виртуального ЦП, который был выбран при создании кластера, к которому принадлежит данный хост.
- Хост имеет объем ОЗУ — минимум 2 Гбайт.
- Хост обслуживается системным администратором с системными полномочиями (администратор имеет права суперпользователя).

10.2. Гипервизоры ROSA Virtualization

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

Доступ к веб-интерфейсу 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 отчётов об ошибках (`Automatic Bug Reporting Tool`).

10.3. Задачи при работе с хостами

10.3.1. Добавление хостов в виртуализированный ЦУ

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

Примечание — Перед добавлением хоста в систему виртуализации ROSA Virtualization необходимо осуществить его предварительную настройку, аналогичную настройке хоста при первичной установке системы виртуализации (см. Руководство по установке РСЮК.10102-01 92 01).

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

Необходимые условия для добавления нового хоста в инсталляцию ROSA Virtualization

При добавлении нового хоста в инсталляцию ROSA Virtualization необходимо добавить на новый хост в конфигурационный файл `/etc/hosts` информацию о 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:

- 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

Первичная установка и инициализация хоста

Установка гипервизора ROSA Virtualization осуществляется непосредственно на физический сервер без предустановленной ОС.

Процедура установки и первичной инициализации хоста описывается в Руководстве по установке (РСЮК.10102-01 92 01) — секция **3.2. Установка гипервизора**.

Настройка системных параметров хоста гипервизора

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

Доступ к консоли с использованием веб-интерфейса

Для доступа к консоли в веб-интерфейсе хоста перейдите на вкладку “Терминал” панели навигации интерфейса соответствующего хоста гипервизора (Рис. 125).

Рис. 125. Консоль хоста в веб-интерфейсе

Доступ к консоли с использованием веб-интерфейса

Для доступа к консоли хоста можно воспользоваться SSH соединением.

Для получения доступа к консоли через SSH используйте имя учетной записи суперпользователя `root`, и пароль, выбранный ранее при установке.

Выполните команду в терминале, указав имя хоста (в примере ниже — имя хоста `host1.home.local`, замените его на имя хоста, развернутого в вашем ЦОД):

```
# ssh root@host1.home.local
```

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

Разрешение имен DNS

При отсутствии в сети сервера DNS используйте 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.

Редактирование файла /etc/hosts с именами хостов, используемых в системе

В консоли хоста откройте редактор `mc` (`mcedit`) и укажите в файле `/etc/hosts` IP-адреса и имена DNS взаимодействующих компонентов ROSA Virtualization – хостов с установленными гипервизорами, ВМ СУСВ и сервера IPA.

Для начала редактирования файла `/etc/hosts` с использованием редактора `mcedit` выполните команду в консоли:

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

После завершения редактирования выйдите из редактора, сохранив результат. Для выхода из редактора можно использовать кнопку `Esc`. Если в файл были внесены изменения, то вам предложат их сохранить, или выйти без сохранения. Выберите опцию «**Сохранить при выходе**» - «**Да**» для сохранения внесенных изменений при выходе из редактора.

Примечание – Для сохранения результатов редактирования файла в редакторе `mcedit` нажмите **F2**. Для выхода из редактора нажмите **F10**. При использовании редактора в окне браузера вы можете нажать на кнопки F2 и F10, используя курсор мыши и левую клавишу мыши.

Примечание – Вы также можете использовать для редактирования любой другой текстовый редактор, например `vi`.

Для редактирования файла с использованием редактора `vi` выполните команду:

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

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

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

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

```
192.168.0.70  vm          vm.home.local          # ВМ СУСВ
192.168.0.71  host1       host1.home.local       # хост гипервизора
192.168.0.72  host2       host2.home.local       # хост гипервизора
192.168.0.73  host3       host3.home.local       # хост гипервизора
192.168.0.74  ipa         ipa.home.local         # сервер IPA
192.168.0.75  host4       host4.home.local       # хост гипервизора
```

Данный пример файла `/etc/hosts` предполагает, что ранее в системе виртуализации ROSA Virtualization уже были установлены хосты `host1 - host3`, и сейчас осуществляется добавление нового хоста `host4`. Файл добавляется на новый хост `host4`, также вносятся изменения на других ранее установленных хостах и в СУСВ.

Повторите процедуру редактирования файла `/etc/hosts` на каждом из хостов с установленным гипервизором.

Пример

Ранее в системе виртуализации ROSA Virtualization уже были установлены хосты `host1 - host3`, и сейчас осуществляется добавление нового хоста `host4`. На ранее установленные хосты и в СУСВ необходимо добавить строку в файл `/etc/hosts` с указанием IP адреса нового хоста.

```
        192.168.0.75  host4       host4.home.local       # хост гипервизора
```

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

Примечание – 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 на сервер имена хостов и их IP адреса должны быть разрешимы на каждом из хостов и в СУСВ.

Примечание – Указание в файле `/etc/hosts` IP-адресов и имен DNS взаимодействующих компонентов ROSA Virtualization 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.

Добавление хоста в виртуализированный ЦУ

1. В главном меню **Портала администрирования** нажмите **Ресурсы → Хосты**. Откроется форма с отображением информации о доступных хостах.

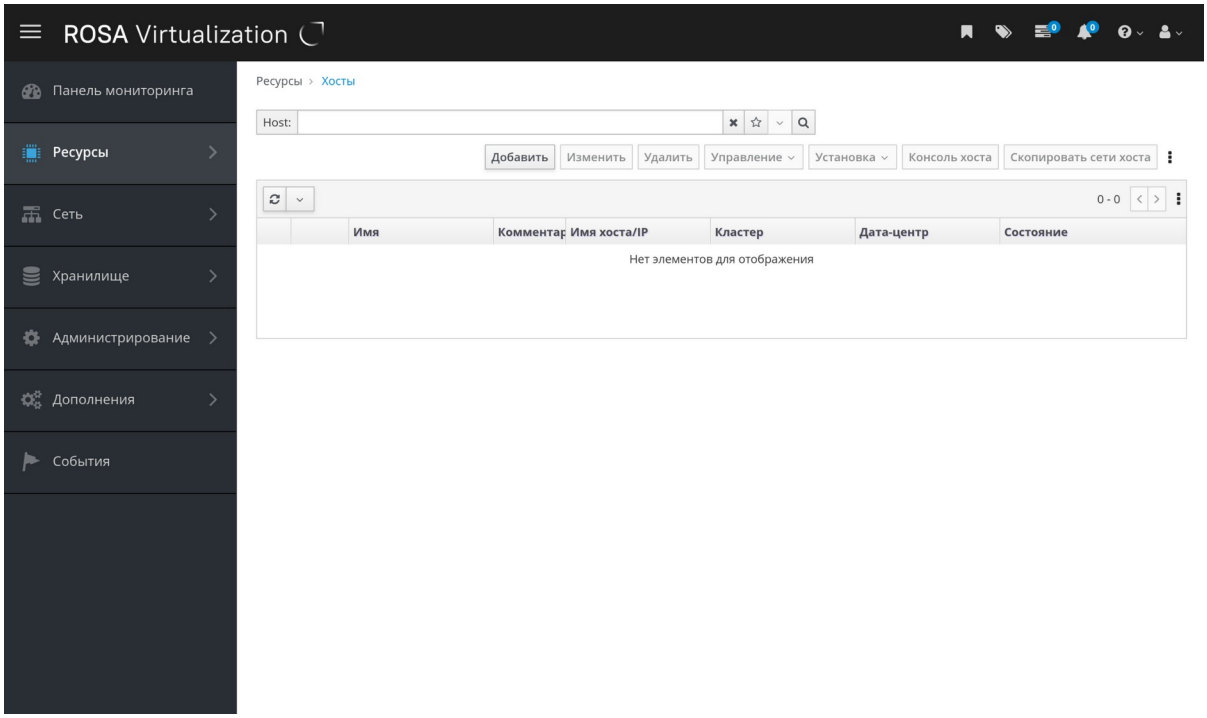

Рис. 126. Форма Ресурсы → Хосты, с отображением информации о доступных хостах.

2. Нажмите **Добавить** для добавления хоста в систему виртуализации ROSA Virtualization. Откроется форма **Новый хост** для определения параметров добавляемого хоста (Рис. 127).

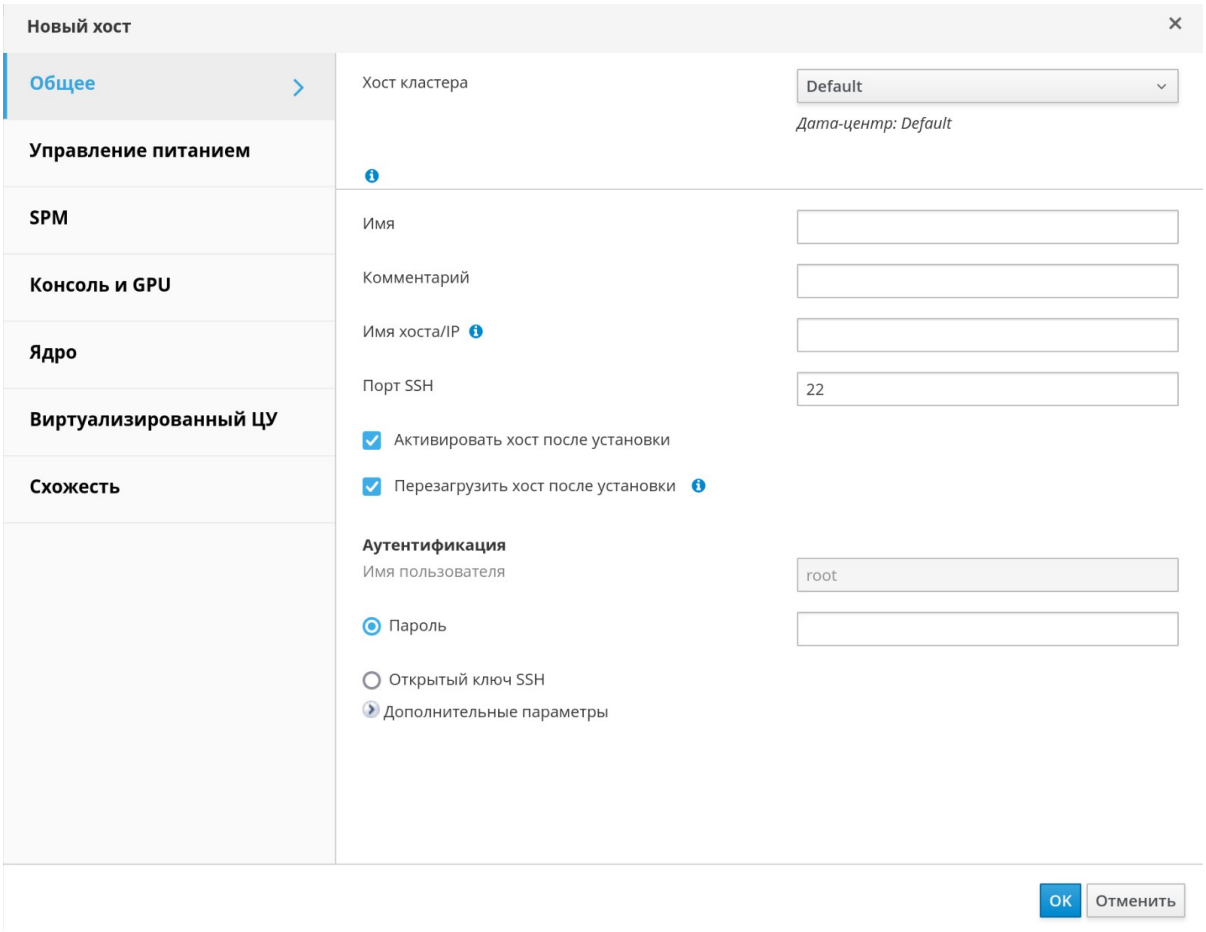

Рис. 127. Форма Новый хост — вкладка Общие

3. Из выпадающего списка выберите **Дата-центр** и **Кластер хоста** для нового хоста. По умолчанию используется дата-центр default, кластер default.
4. Укажите **Имя хоста / IP Адрес** нового хоста (Рис. 127). В поле **Порт SSH** автоматически добавится стандартный номер порта SSH — `22`.
5. Выберите метод аутентификации, используемый диспетчером виртуализации для подключения к хосту:
    - При использовании аутентификации по паролю введите пароль суперпользователя `root` в поле **Пароль** (Рис. 127).
    - При использовании аутентификации по открытому ключу SSH скопируйте ключ из поля **Открытый ключ SSH** (Рис. 128) в файл `/root/.ssh/authorized_keys` на хост, добавляемый в СУСВ.

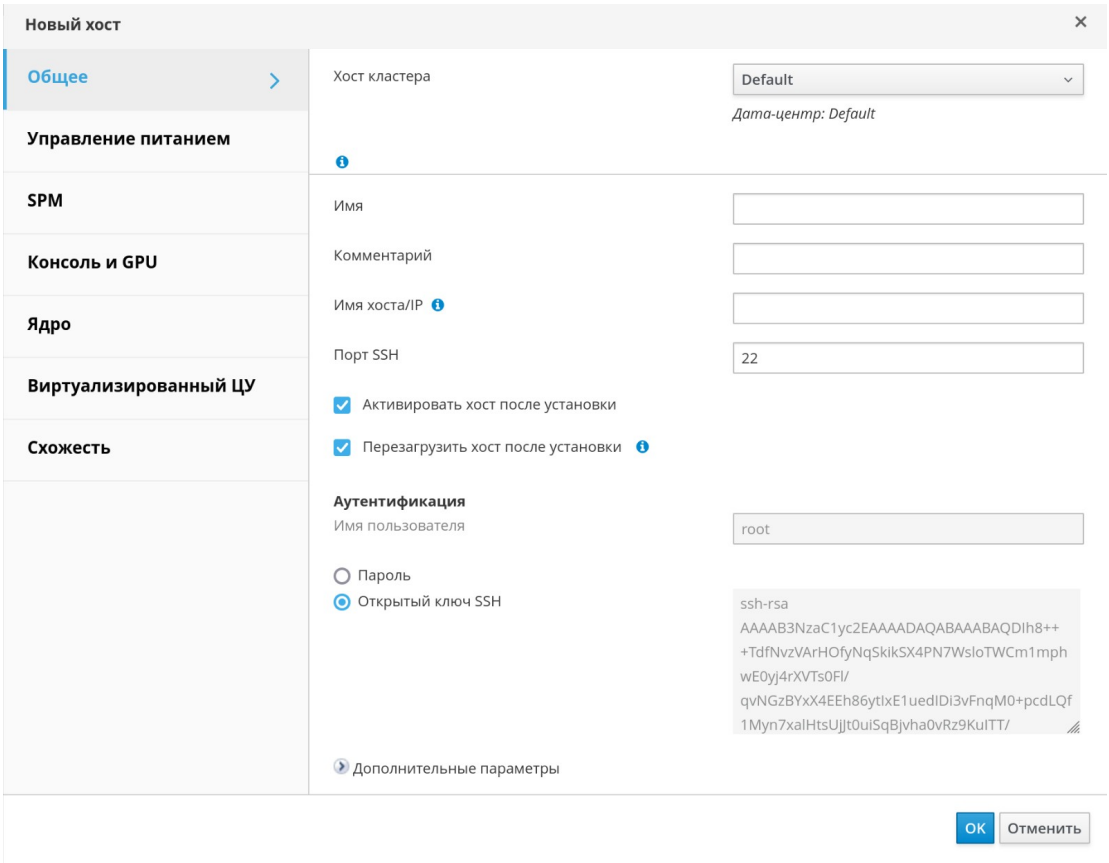

Рис. 128. Ключ из поля Открытый ключ SSH необходимо скопировать на хост

6. Опционально нажмите на кнопку **Дополнительные параметры** (Рис. 129), 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.

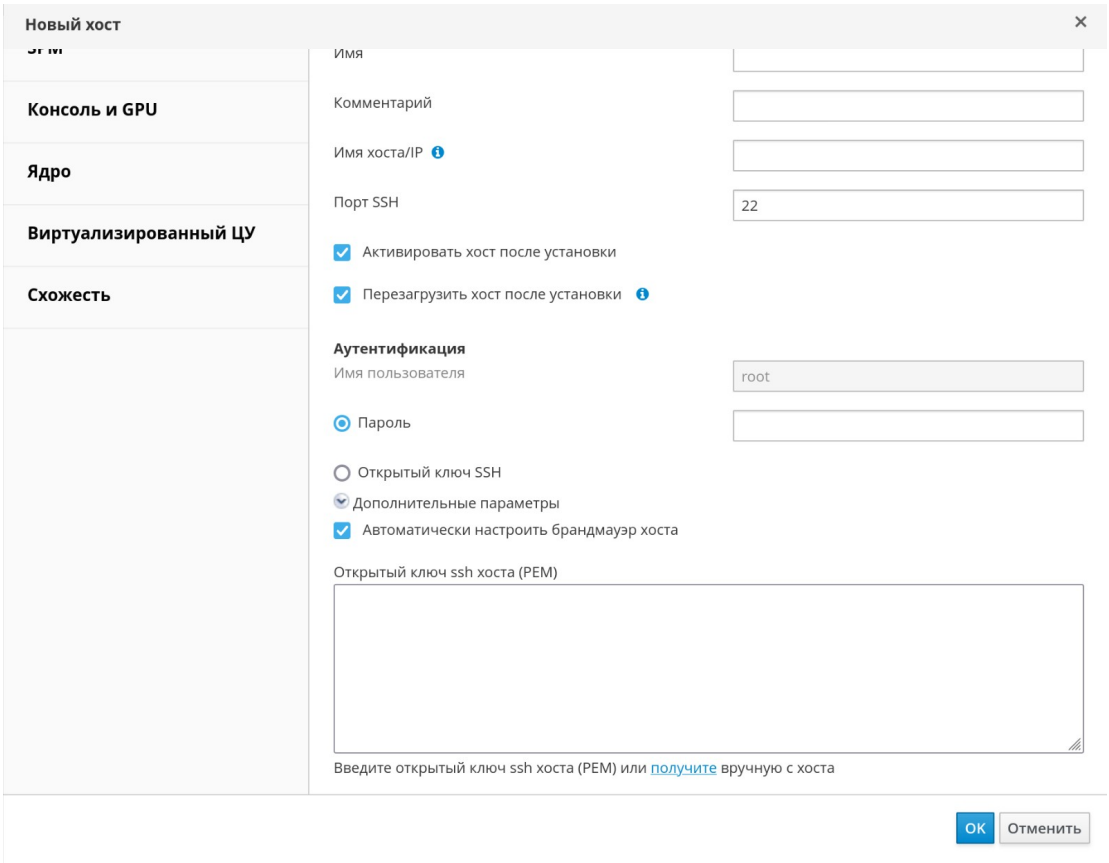

Рис. 129. Новый хост — настройка дополнительных параметров

7. Опционально настройте управление питанием на вкладке **Управление питанием** (Рис. 130), если у хоста есть поддерживаемая карта управления питанием.

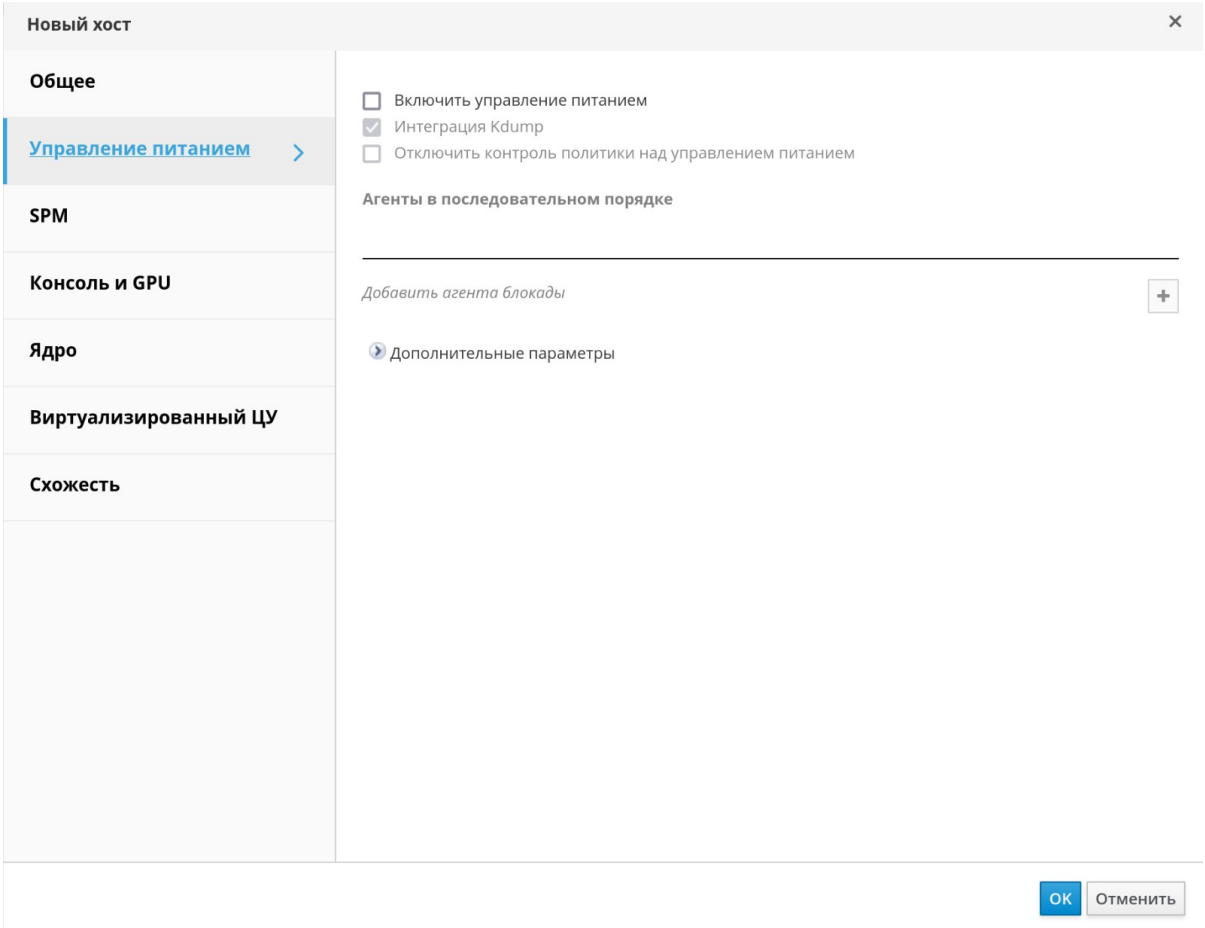

Рис. 130. Новый хост — вкладка Управление питанием

8. Нажмите **OK**.

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

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

10.3.2. Общие параметры хоста

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

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

Табл. 10.1. Общие параметры хоста

Поле	Описание
Кластер хоста	Кластер и дата-центр, к которым принадлежит хост
Использовать	Установите или снимите флажок, чтобы соответственно

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

Поле	Описание
Автоматически настроить брандмауэр хоста	При добавлении нового хоста виртуализированный ЦУ может открыть требуемые порты в конфигурации межсетевого экрана данного хоста. Этот **Дополнительный параметр** включён по умолчанию
Отпечаток SSH	Этот **Дополнительный параметр** предоставляет возможность получить отпечаток SSH хоста и сопоставить его с ожидаемым отпечатком, проверив таким образом их соответствие

10.3.3. Параметры управления питанием хоста

В Табл. 10.2 описываются параметры вкладки **Управление питанием** (Рис. 130) окон **Новый хост** или **Параметры хоста**.

Табл. 10.2. Параметры управления питанием хоста

Поле	Описание
Включить управление питанием	Включает управление питанием на хосте. Установите флажок для этого параметра для активации остальных полей во вкладке **Управление питанием**
Интеграция kdump	Предотвращает проведение операции блокады на хосте во время выполнения аварийного дампа ядра, чтобы не прерывать дамп
Отключить контроль политики над управлением питанием	Управление питанием контролируется **Политикой планирования** кластера хоста. При включённом управлении питанием и достижении указанного значения низкого потребления виртуализированный ЦУ выключит машину хоста и запустит её снова из расчёта балансировки нагрузки, или когда в кластере не будет достаточного числа свободных хостов. Установите флажок для этого параметра, чтобы отключить контроль со стороны политики
Агенты в последовательном порядке	Список агентов операции блокады. Агенты операции блокады могут быть последовательными, параллельными или совмещенными. По умолчанию, агенты операции блокады являются последовательными. Если агенты операции блокады используются последовательно, то сначала, для остановки или запуска хоста, используется первичный агент, а в случае его сбоя — вторичный.

Поле	Описание
	Если агенты работают параллельно, то на команду остановки хоста должны отреагировать оба агента. При этом, если на команду запуска хоста отреагирует один агент, то хост начнёт работу. Для смены последовательности, в которой используются агенты, используйте кнопки со стрелками ↑ (вверх) и ↓ (вниз). Чтобы сделать двух агентов операции блокады параллельными, выберите одного агента из выпадающего списка **Одновременно с:** рядом с другим агентом. Дополнительных агентов можно добавить в группу параллельно выполняющихся агентов, выбрав группу из выпадающего списка **Одновременно с:** рядом с дополнительным агентом
Добавить агента блокады	Для добавления нового агента блокады нажмите на кнопку со знаком + (плюс). В результате будет открыто окно **Параметры агента блокады** (подробные сведения об этих параметрах приведены в **Табл. 10.3**)
Предпочитаемый прокси для управления питанием	По умолчанию этот **Дополнительный параметр** указывает, что диспетчер виртуализации будет искать прокси операции блокады в рамках того же кластера, в состав которого входит хост, а в случае неудачного поиска — в том же дата-центре

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

Табл. 10.3. Параметры агента блокады

Поле	Описание
Адрес	Адрес для доступа к устройству управления питанием хоста. Укажите разрешаемое имя хоста или IP-адрес
Имя пользователя	Учётная запись пользователя, которая будет получать доступ к устройству управления питанием хоста. Для устройства можно создать и настроить специального пользователя, или использовать пользователя по умолчанию
Пароль	Пароль пользователя, получающего доступ к устройству управления питанием хоста
Тип	Выберите тип устройства управления питанием хоста: • **apc** - коммутатор питания по сети серии APC MasterSwitch (нельзя использовать с устройствами серии APC 5.x).

Поле	Описание
	• **apc_snmp** - коммутатор питания по сети серии APC 5.x. • **bladecenter** - удалённый супервизор-адаптер IBM Bladecenter. • **cisco_ucs** - Cisco Unified Computing System. • **drac5** - контроллер удалённого доступа Dell для компьютеров Dell. • **drac7** - контроллер удалённого доступа Dell для компьютеров Dell. • **eps** - коммутатор питания по сети ePowerSwitch 8M+. • **hpblade** - HP BladeSystem. • **ilo**, **ilo2**, **ilo3**, **ilo4** - HP Integrated Lights-Out. • **ipmilan** - устройства управления Intelligent Platform Management Interface и Sun Integrated Lights Out Management. • **rsa** - удалённый супервизор-адаптер IBM. • **rsb** - интерфейс управления Fujitsu-Siemens RSB. • **wti** - коммутатор питания по сети WTI.
Порт	Номер порта, используемого устройством управления питанием для связи с хостом
Слот	Число для идентификации платы устройства управления питанием хоста
Параметры	Параметры конкретного устройства управления питанием хоста указываются в виде «ключ-значение» (доступные параметры приведены в документации конкретного устройства). Примечание — в поле **Параметры** необходимо указать значение `ssl_insecure=1` при выборе типа **cisco_ucs**
Защищённое	Установите флажок для защищённого подключения к хосту с помощью SSH, SSL или других протоколов аутентификации, в зависимости от агента управления питанием хоста

10.3.4. Параметр приоритета SPM

В Табл. 10.4 описывается параметр вкладки **SPM** окон **Новый хост** или **Параметры хоста** (Рис. 131).

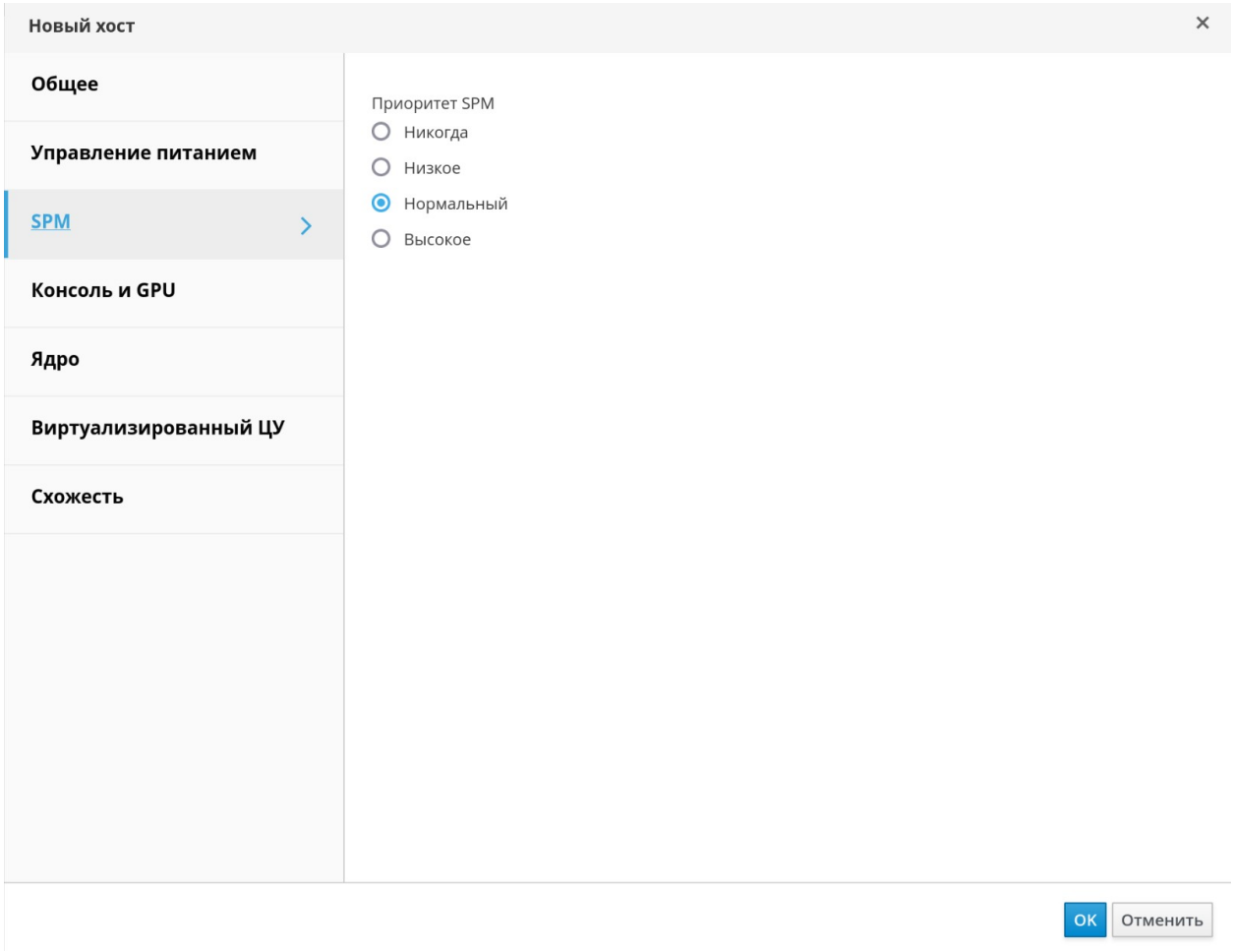

Рис. 131. Вкладка SPM

Табл. 10.4. Параметр приоритета SPM

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

10.3.5. Параметры вкладки «Консоль и GPU»

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

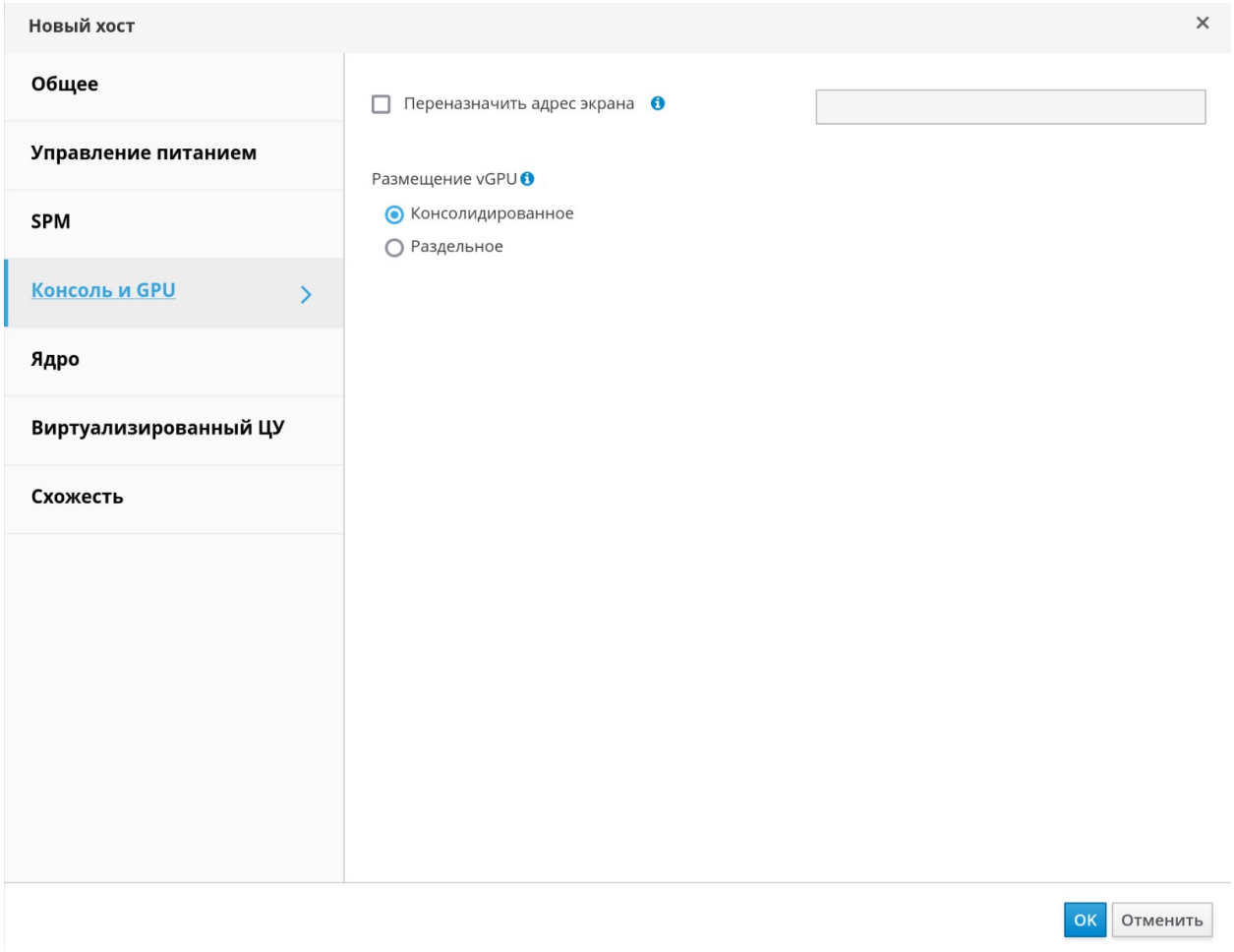

Рис. 132. Вкладка Консоль и GPU

Табл. 10.5. Параметры вкладки «Консоль и GPU»

Поле	Описание
Переназначить адрес экрана	Установите флажок для этого параметра, чтобы переназначить адрес экрана хоста. Параметр удобен в том случае, когда хосты определяются внутренним IP и находятся за межсетевым экраном NAT. При подключении пользователя к ВМ из-за пределов внутренней сети будет возвращаться открытый IP или FQDN ВМ, который во внешней сети разрешается на открытый IP, вместо частного адреса хоста, на котором выполняется ВМ
Адрес экрана	Указанный адрес экрана будет использоваться для всех

Поле	Описание
	ВМ, выполняющихся на этом хосте. Адрес должен указываться в формате FQDN или IP
Размещение vGPU	Выберите тип размещения vGPU: • **Консолидированное** — предпочтительным является запуск как можно большого числа vGPU на доступных физических картах. • **Раздельное** — каждый vGPU размещается на отдельной физической карте.

10.3.6. Параметр вкладки «Поставщик сети»

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

Табл. 10.6. Параметр вкладки «Поставщик сети»

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

10.3.7. Параметры ядра

В Табл. 10.7 описываются параметры вкладки **Ядро** (Рис. 133) окон **Новый хост** и **Параметры хоста**.

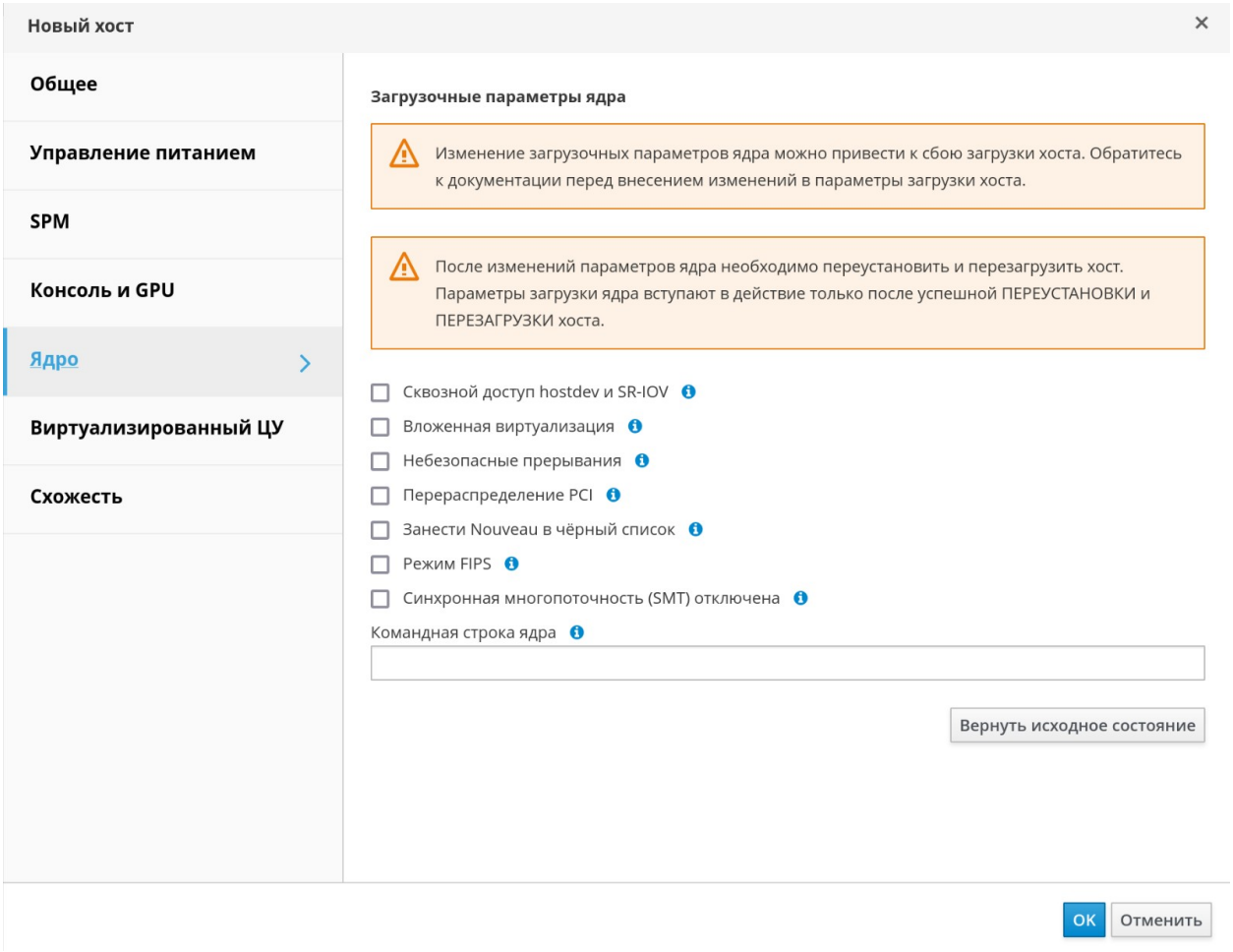

Рис. 133. Вкладки Ядро (параметры ядра хоста)

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

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

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

Табл. 10.7. Параметры ядра

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

Поле	Описание
Командная строка ядра	Поле даёт возможность добавить дополнительные параметры ядра к параметрам по умолчанию

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

10.3.8. Параметр вкладки «Виртуализированный ЦУ»

В Табл. 10.8 описывается параметр вкладки **Виртуализированный ЦУ** (Рис. 134) окон **Новый хост** и **Параметры хоста**.

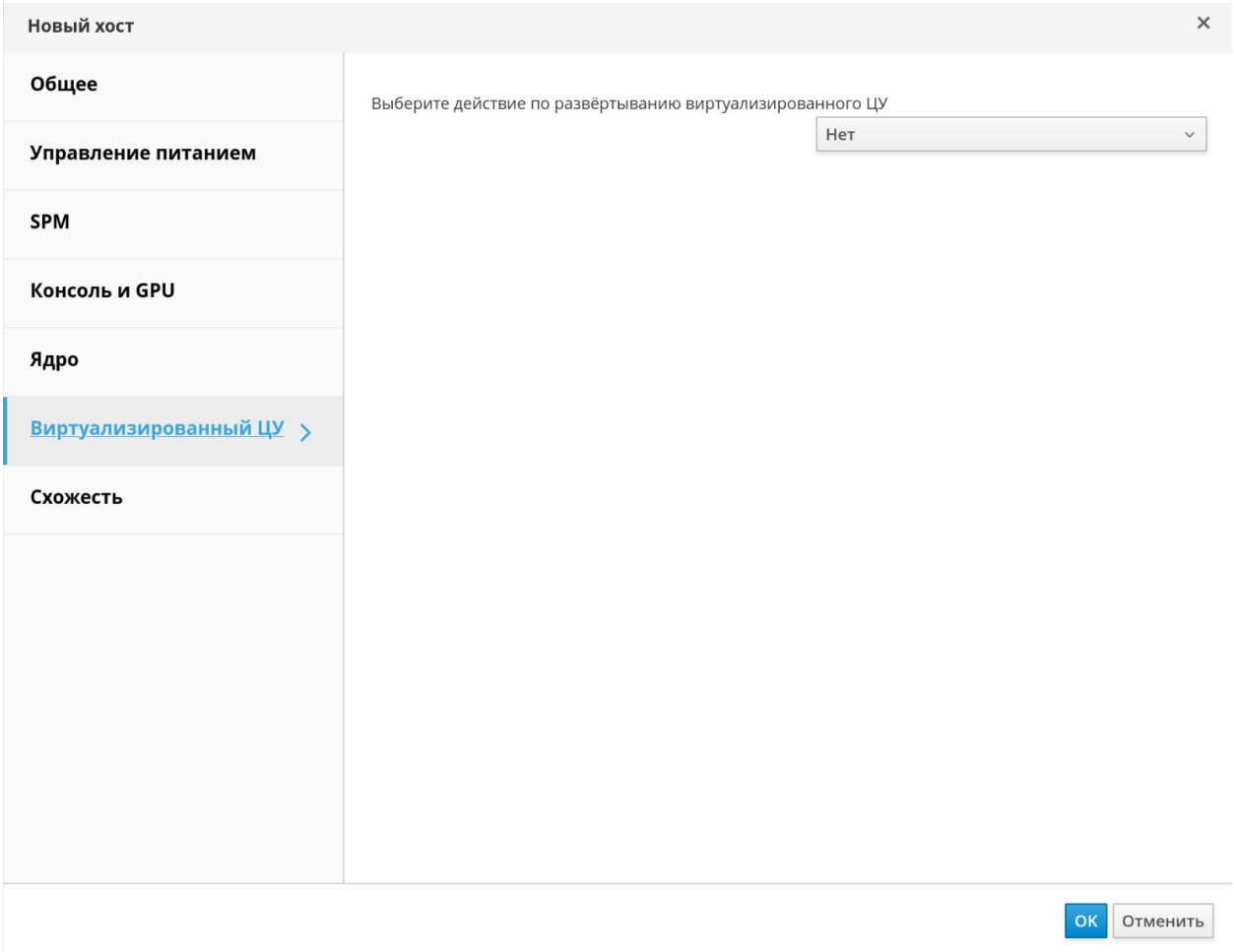

Рис. 134. Вкладка Виртуализированный ЦУ

Табл. 10.8. Параметр вкладки «Виртуализированный ЦУ»

Поле	Описание
Выберите действие	Выберите действие по развёртыванию виртуализированного ЦУ: • **Нет** — никаких действий не требуется.

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

10.3.9. Настройка параметров управления питанием хоста

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

Настройка параметров управления питанием хоста

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

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

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

Примечание — в случае использования как адресов IPv4, так и адресов IPv6 (по умолчанию), оставьте поле **Параметры** пустым. При использовании только адресов IPv4

введите в поле **Параметры** значение `inet4_only=1`. При использовании только адресов IPv6 введите в поле **Параметры** значение `inet6_only=1`.

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

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

10.3.10. Настройка параметра приоритета SPM хоста

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

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

Настройка параметра приоритета SPM

1. Нажмите **Ресурсы → Хосты**.
2. Нажмите **Изменить**.
3. Перейдите на вкладку **SPM** (Рис. 131).
4. Установите флажок в значение **Низкий**, **Нормальный** (по умолчанию), **Высокий** для указания необходимого приоритета SPM хоста, или в значение **Никогда**, чтобы хосту не была присвоена роль SPM.
5. Нажмите **OK**.

10.3.11. Настройка на хосте сквозного доступа к PCI

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

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

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

Подготовка хоста для применения сквозного доступа к PCI

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

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

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

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

Ручная активация IOMMU

1. Для включения IOMMU отредактируйте конфигурационный файл загрузчика `grub`:

   - Для Intel® добавьте запись `intel_iommu=on` в конец строки `GRUB_CMDLINE_LINUX` в конфигурационном файле `/etc/default/grub`:

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

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

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

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

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

`allow_unsafe_interrupts=1` в строку `options` в конфигурационном файле `/etc/modprobe.d`:

```
options vfio_iommu_type1 allow_unsafe_interrupts=1
```

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

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

10.3.12. Перевод хоста в режим обслуживания

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

При переводе хоста в режим обслуживания, виртуализированный ЦУ попытается выполнить миграцию всех работающих ВМ на альтернативные хосты. При этом будут 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, нажмите кнопку **Привязано к хосту** на вкладке **Виртуальные машины** в подробном просмотре хоста.

Перевод хоста в режим обслуживания

1. Нажмите **Ресурсы → Хосты** и выберите хост.
2. Нажмите **Управление → Обслуживание**. В результате будет открыто окно **Хосты обслуживания** (Рис. 135).
3. Опционально укажите **Причину** перемещения хоста в режим обслуживания, которая будет указана в журнале и при повторной активации хоста из режима обслуживания.

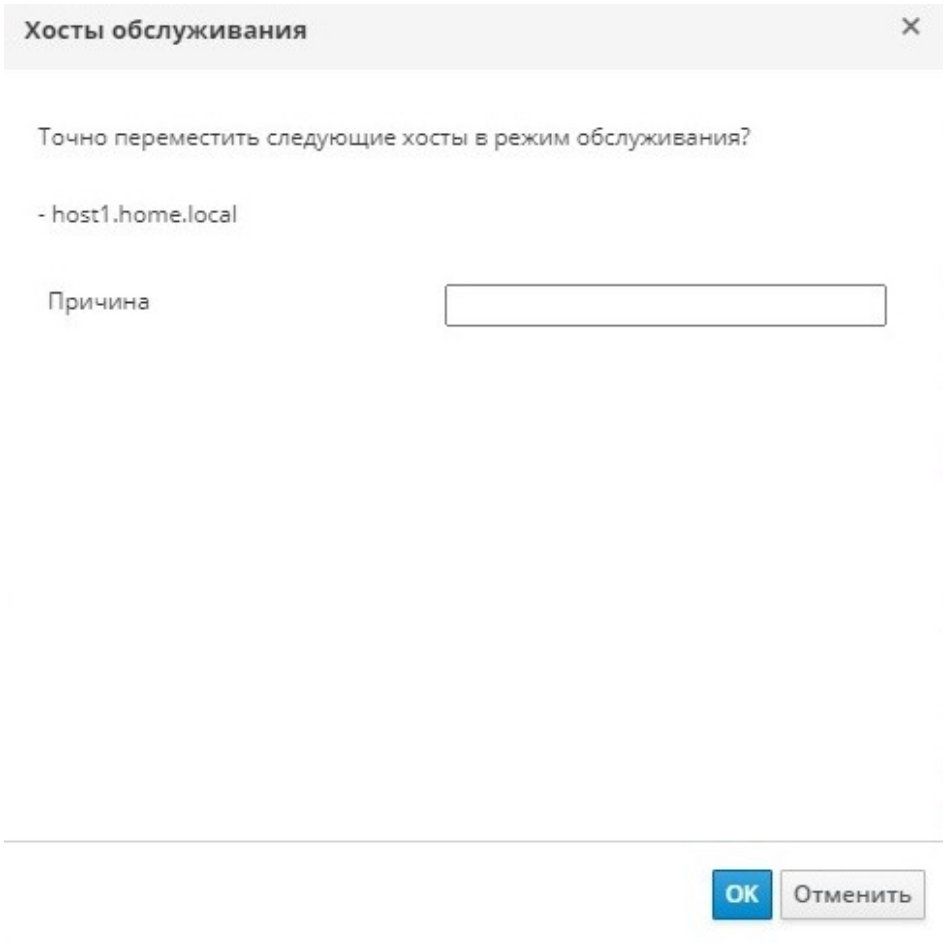

Рис. 135. Перемещение хоста в режим обслуживания

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

4. Опционально выберите нужные параметры для хостов с поддержкой Gluster:

   - Выберите параметр **Игнорировать кворум Gluster и проверки самовосстановления** для избежания проверок по умолчанию. По умолчанию во время перевода хоста в режим обслуживания, виртуализированный ЦУ проверяет, не был ли потерян кворум Gluster. Виртуализированный ЦУ также проверяет хост на наличие задач по самовосстановлению, на которые может повлиять перевод хоста в режим обслуживания. Если кворум будет потерян, или если выполняются действия по самовосстановлению, которые не должны быть затронуты, виртуализированный ЦУ не разрешит перевести хост в режим обслуживания. Используйте этот параметр, только если нет никаких других способов перевести хост в режим обслуживания.

   - Выберите параметр **Остановить службу Gluster**, чтобы остановить выполнение всех служб Gluster во время перевода хоста в режим обслуживания.

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

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

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

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

10.3.13. Активация хоста из режима обслуживания

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

Активация хоста из режима обслуживания

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

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

10.3.14. Настройка правил межсетевого экрана хоста

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

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

Настройка правил межсетевого экрана для хостов

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

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

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

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

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

10.3.15. Удаление хоста

Удаление хоста

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

10.3.16. Повторная установка хостов

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

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

В следующую последовательность действий включаются остановка и перезапуск хостов.

Повторная установка хостов

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

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

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

10.3.17. Индивидуализация хостов с помощью меток

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

Индивидуальная настройка хостов с помощью меток

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

10.3.18. Просмотр статуса работоспособности хоста

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

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

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

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

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

10.3.19. Просмотр устройств хоста

Просмотр устройств хоста

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

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

10.3.20. Доступ к веб-интерфейсу Cockpit с Портала администрирования

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

Доступ к Cockpit с Портала администрирования

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

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

10.4. Отказоустойчивость хостов

10.4.1. Высокая доступность хостов

В системе виртуализации ROSA Virtualization хост со статусом «*Не отвечает*» отличается от хоста со статусом «*В нерабочем состоянии*». Нерабочие хосты могут обмениваться информацией с диспетчером виртуализации, но имеют некорректную конфигурацию (например, отсутствие локальной сети). Не отвечающие хосты не могут поддерживать связь с диспетчером виртуализации.

Для поддержания отзывчивости хостов в кластере, диспетчер виртуализации использует операции блокады (огораживание). Огораживание позволяет кластеру среагировать на неожиданный сбой хоста и принудительно применить доступные политики экономии питания, балансировки нагрузки и доступности ВМ. Параметры операции блокады устройства управления питанием хоста должны быть настроены, и их корректность необходимо время от времени тестировать. Во время операции огораживания не отвечающий хост перезагружается, и если хост не вернётся к активному состоянию в течение указанного времени, то останется не отвечающим в ожидании ручного вмешательства для решения проблемы.

Примечание — для автоматической проверки параметров операции блокады настройте следующие параметры `engine-config — PMHealthCheckEnabled` (по умолчанию `false`) и `PMHealthCheckIntervalInSec` (по умолчанию `3600` секунд). При значении `true` параметр `PMHealthCheckEnabled` будет проверять всех агентов хоста согласно временному интервалу, указанному параметром `PMHealthCheckIntervalInSec`, и в случае обнаружения проблемы выдаст предупреждение.

После перезагрузки действия по управлению питанием могут быть выполнены автоматически хостом-прокси или вручную на Портале администрирования. Все ВМ, выполняющиеся на не отвечающих хостах, будут остановлены, а высокодоступные ВМ будут запущены на другом хосте. Для действий по управлению питанием необходимо как минимум два хоста.

Примечание — на хосте, где выполняются высокодоступные ВМ, управление питанием должно быть включено и настроено.

После запуска диспетчера виртуализации и окончания времени молчания (по умолчанию `5` минут), диспетчер виртуализации автоматически попытается огородить не отвечающие хосты, на которых включено управление питанием.

Примечание — время молчания можно настроить с помощью параметра `DisableFenceAtStartupInSec`. Данный параметр `engine-config` помогает предотвратить ситуации, когда диспетчер виртуализации пытается выполнить операцию блокады для загружающихся хостов. Это может случиться после перебоя в работе дата-центра, так как процесс загрузки хоста занимает больше времени, чем процесс загрузки диспетчера виртуализации.

10.4.2. Управление питанием с помощью прокси

Виртуализированный ЦУ не связывается напрямую с агентами операции блокады. Для обмена командами с устройством управления питанием хоста виртуализированный ЦУ использует прокси. Для выполнения действий устройства управления питанием виртуализированный ЦУ использует VDSM, поэтому другой хост в окружении играет роль прокси для операции блокады.

Хост-прокси имеет статус «*Запущен*» или «*Обслуживание*», и находится в том же кластере или дата-центре, что и огораживаемый хост.

10.4.3. Настройка параметров операции блокады на хосте

Параметры операции блокады настраиваются во вкладке **Управление питанием** окон **Новый хост** или **Параметры хоста**. Управление питанием даёт возможность системе огородить проблемный хост, используя такие дополнительные интерфейсы, как карта удалённого доступа RAC.

Все действия по управлению питанием выполняются через хост-прокси, а не напрямую виртуализированным ЦУ. Для действий по управлению питанием необходимо как минимум два хоста.

Настройка параметров операции блокады на хосте

1. Нажмите **Ресурсы → Хосты** и выберите хост.
2. Нажмите **Изменить**.
3. Перейдите на вкладку **Управление питанием** (Рис. 136).
4. Установите флажок **Включить управление питанием**, чтобы активировать поля ввода.
5. Установите флажок **Интеграция Kdump**, чтобы предотвратить огораживание хоста во время выполнения аварийного дампа ядра.

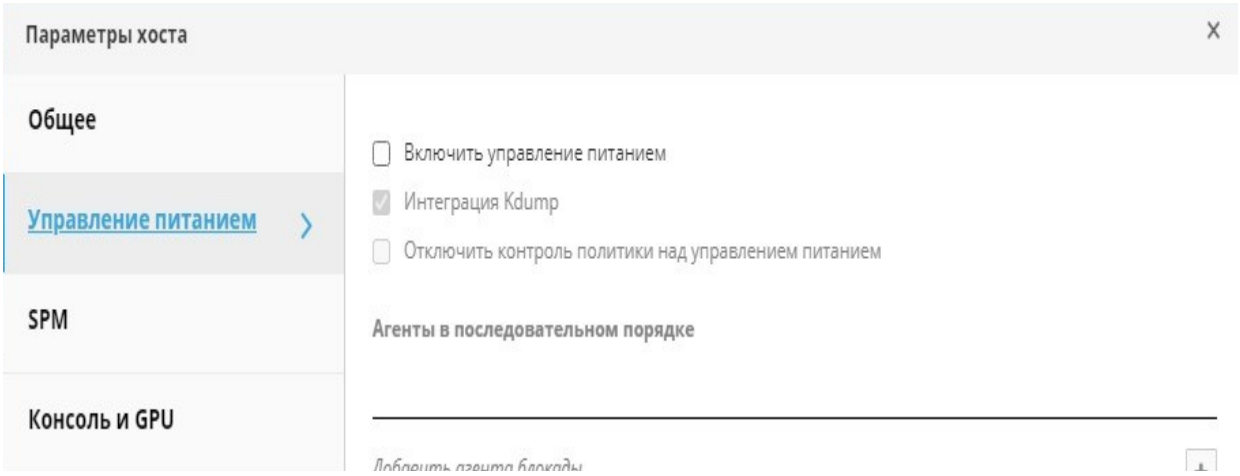

Рис. 136. Управление питанием хоста

Примечание — хост необходимо переустановить каждый раз при изменении (активации или деактивации) параметра **Интеграция Kdump**.

6. Опционально установите флажок **Отключить контроль управления питанием со стороны политик**, если управление питанием хоста не должно контролироваться политикой планирования кластера, в который входит хост.
7. Нажмите на кнопку + (плюс), чтобы открыть окно **Параметры агента блокады** для добавления нового устройства управления питанием.
8. Укажите **Адрес**, **Имя пользователя** и **Пароль** для устройства управления питанием.
9. Из выпадающего списка выберите **Тип** устройства управления питанием.
10. Укажите номер **Порта SSH**, используемый устройством управления питанием для связи с хостом.
11. Укажите номер **Слота**, используемого для идентификации платы устройства управления питанием.
12. Настройте **Параметры** устройства управления питанием в форме списка записей «ключ-значение», разделённых запятыми.
13. Установите флажок **Защищённое**, чтобы включить защищённое соединение между устройством управления питанием и хостом.
14. Чтобы убедиться в том, что все значения корректны, нажмите **Проверка**. В случае успешной проверки будет показано сообщение — *Проверка выполнена, статус хоста: запущен*.

Примечание — параметры управления питанием (идентификатор пользователя, пароль, дополнительные параметры) тестируются виртуализированным ЦУ во время настройки, а после этого только вручную. При выборе игнорирования предупреждений о некорректных параметрах, или если параметры изменяются на аппаратных компонентах устройств управления питанием без внесения соответствующих изменений в виртуализированном ЦУ, в самый ответственный момент может случиться сбой операции блокады.

15. Нажмите **OK** для закрытия окна **Параметры агента блокады**.
16. Опционально во вкладке **Управление питанием** разверните **Дополнительные параметры**, и с помощью кнопок со стрелками ↑ (вверх) и ↓ (вниз) укажите порядок, в котором виртуализированный ЦУ будет вести поиск хоста-прокси для операции блокады в кластере или дата-центре.
17. Нажмите **OK**.

Обратите внимание, что **!** (восклицательный знак) рядом с именем хоста исчез, что означает успешную настройку управления питанием хоста.

10.4.4. Служба Kdump и параметры fence_kdump

Для просмотра статуса службы Kdump нажмите на имя хоста во вкладке **Общие**. Значения статуса службы Kdump:

- **Включено**: Kdump настроен, и служба Kdump выполняется.

- **Отключено**: служба Kdump не выполняется (в этом случае интеграция Kdump не будет работать должным образом).
- **Неизвестно**: данный статус отображается только на хостах с более ранними версиями VDSM, не сообщающими о статусе Kdump.

Включение параметра **Интеграция Kdump** во вкладке **Управление питанием** окон **Новый хост** или **Параметры хоста** создаёт стандартную конфигурацию агента `fence_kdump`. Если сетевая конфигурация окружения не слишком сложна, а полное доменное имя диспетчера виртуализации разрешается на всех хостах, то исходных параметров `fence_kdump` будет достаточно для использования.

Но существуют случаи, когда бывает необходима продвинутая конфигурация `fence_kdump`. В окружениях с более сложными сетевыми параметрами может понадобиться вручную настроить виртуализированный ЦУ и/или слушатель `fence_kdump`.

Например, если полное доменное имя виртуализированного ЦУ разрешается не на всех хостах с активированной **Интеграцией Kdump**, то настроить правильное имя хоста или адрес IP можно с помощью `engine-config`:

```
engine-config -s FenceKdumpDestinationAddress=A.B.C.D
```

Другие примеры случаев, когда также могут понадобиться изменения конфигурации:

- Виртуализированный ЦУ с двумя сетевыми картами, одна из которых общедоступна, а вторая предназначена для сообщений `fence_kdump`.
- Необходимость запуска слушателя `fence_kdump` по-другому IP-адресу или на другом порту.
- Необходимость настроить частный интервал для уведомлений `fence_kdump` в целях предотвращения возможных потерь пакетов.

Частные параметры обнаружения `fence_kdump` рекомендуются для продвинутых пользователей, поскольку внесение изменений в изначальную конфигурацию необходимо только в усложнённых сетевых конфигурациях.

Настройка слушателя fence_kdump

1. Создайте новый файл (например, `my-fence-kdump.conf`) в каталоге `/etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/`.

2. Укажите частные параметры, согласно синтаксису *ПАРАМЕТР=значение* и сохраните файл.

Примечание — изменённые значения параметров также должны быть согласованы с параметрами `engine-config`, приведенными в **Табл. 10.10**.

3. Перезапустите слушатель fence_kdump:

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

В **Табл. 10.9** описываются параметры настройки слушателя `fence_kdump`.

Табл. 10.9. Параметры настройки слушателя fence_kdump

Переменная	Описание	Примечание
LISTENER_ADDRESS	IP-адрес, на который будут приходить сообщения fence_kdump. Значение по умолчанию — 0.0.0.0	При изменении значения этот параметр должен соответствовать значению параметра FenceKdumpDestinationAddress в engine-config
LISTENER_PORT	Указывает порт, на который будут приходить сообщения fence_kdump. Значение по умолчанию — 7410	При изменении значения этот параметр должен соответствовать значению параметра FenceKdumpDestinationPort в engine-config
HEARTBEAT_INTERVAL	Указывает интервал (в секундах) обновлений периодического сигнала слушателя. Значение по умолчанию — 30	При изменении значения этот параметр должен быть равен (или быть меньше) половинному значению параметра FenceKdumpListenerTimeout в engine-config
SESSION_SYNC_INTERVAL	Указывает интервал (в секундах) синхронизации сеансов Kdump в памяти хоста слушателя с базой данных. Значение по умолчанию — 5	При изменении значения этот параметр должен быть равен (или быть меньше) половинному значению параметра KdumpStartedTimeout в engine-config
REOPEN_DB_CONNECTION_INTERVAL	Указывает интервал (в секундах) для повторного открытия соединения к базе данных, которая ранее была недоступна. Значение по умолчанию — 30	
KDUMP_FINISHED_TIMEOUT	Определяет максимальный период ожидания (в секундах) после последнего полученного сообщения от хостов, на которых выполняется Kdump. По истечению этого периода поток Kdump хоста будет помечен как ЗАВЕРШЕНО. Значение по умолчанию — 60	При изменении значения этот параметр должен быть равен (или быть больше) двойному значению параметра FenceKdumpMessageInterval в engine-config

Настройка Kdump с помощью engine-config

Для просмотра текущих параметров Kdump выполните следующую команду:

```
# engine-config -g ПАРАМЕТР
```

1. Отредактируйте конфигурацию Kdump, согласно синтаксису *ПАРАМЕТР=значение*:

```
# engine-config -s ПАРАМЕТР=значение
```

Примечание — изменённые значения параметров также должны быть согласованы с параметрами настройки слушателя `fence_kdump`, приведенными в **Табл. 10.9**.

2. Перезапустите службу `ovirt-engine`:

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

3. Переустановите все хосты, а также при необходимости активируйте параметр **Интеграция Kdump** (см. **Табл. 10.10**).

В **Табл. 10.10** описываются параметры конфигурации Kdump.

Табл. 10.10. Параметры конфигурации Kdump

Переменная	Описание	Примечание
`FenceKdumpDestinationAddress`	Имена хостов или IP-адреса, на которые будут посылаться сообщения fence_kdump. Значение по умолчанию — пустая строка (используется FQDN диспетчера виртуализации)	При изменении значения этот параметр должен соответствовать значению параметра LISTENER_ADDRESS в конфигурации слушателя fence_kdump, а все хосты с включённой **Интеграцией Kdump** должны быть переустановлены
`FenceKdumpDestinationPort`	Указывает порт, на который необходимо посылать сообщения fence_kdump. Значение по умолчанию — 7410	При изменении значения этот параметр должен соответствовать значению параметра LISTENER_PORT в конфигурации слушателя fence_kdump, а все хосты с включённой **Интеграцией Kdump** должны быть переустановлены

Переменная	Описание	Примечание
`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 включённой **Интеграцией Kdump** должны быть переустановлены
`FenceKdumpListenerTimeout`	Определяет максимальный период ожидания (в секундах) после последнего периодического сигнала, в течение которого слушатель fence_kdump ещё считается работающим. Значение по умолчанию — 90	При изменении значения этот параметр должен быть равен (или быть больше) половинному значению параметра HEARTBEAT_INTERVAL в файле конфигурации слушателя fence_kdump
`KdumpStartedTimeout`	Определяет максимальный период ожидания (в секундах) до первого получения сообщения от хоста, выполняющего kdump (для определения того, что процедуры kdump начали выполняться). Значение по умолчанию — 30	При изменении значения этот параметр должен быть равен (или быть больше) двойному значению параметра SESSION_SYNC_INTERVAL в файле конфигурации слушателя fence_kdump и параметра FenceKdumpMessageInterval

10.4.5. Мягкая блокада хостов

Иногда, в связи с неожиданными проблемами, хосты могут перестать отвечать, но несмотря на то, что VDSM бывает не в состоянии ответить на запрос, виртуальная машина, зависящая от VDSM, остаётся работающей и доступной. В таких ситуациях перезапуск VDSM возвращает возможность VDSM отвечать на запросы и разрешает проблему.

Мягкая блокада (огораживание) с использованием SSH — это процесс, во время которого диспетчер виртуализации пытается перезапустить VDSM на не отвечающем хосте с помощью протокола SSH. В случае неудачи ответственность за проведение

операции блокады падает на внешнего агента огораживания, если ранее агент был настроен.

Мягкое огораживание с помощью SSH выполняется следующим образом: на хосте должна быть настроена и включена возможность проведения операции блокады, а также должен существовать действительный хост-прокси (второй хост, имеющий статус «*Запущен*» в том же дата-центре). При истечении времени ожидания подключения между диспетчером виртуализации и хостом происходит следующее:

1. При первом сбое сети статус хоста меняется на «*Идёт подключение*».
2. Диспетчер виртуализации выполняет три попытки запросить у VDSM его статус или ждёт в течение временно́го интервала, определённого загрузкой хоста. Формула определения этого интервала настраивается с помощью значений `TimeoutToResetVdsInSeconds` (по умолчанию 60 сек.) + [`DelayResetPerVmInSeconds` (по умолчанию 0.5 сек.)] x (число выполняющихся на хосте ВМ) + [`DelayResetForSpmInSeconds` (по умолчанию 20 сек.)] x 1 (если хост выполняет роль SPM) или 0 (если хост не выполняет роль SPM). Чтобы дать VDSM максимальное время на ответ, диспетчер виртуализации выбирает наибольший из двух вышеупомянутых параметров (три попытки определить статус VDSM или интервал, рассчитанный по приведенной формуле).
3. Если по истечении интервала хост по-прежнему не отвечает, выполняется команда `vdsm restart` с использованием протокола SSH.
4. Если команда `vdsm restart` не сможет восстановить соединение между хостом и диспетчером виртуализации, то статус хоста меняется на «*Не отвечает*» и если было настроено управление питанием, выполнение операции блокады передаётся внешнему агенту.

Примечание — мягкое огораживание с помощью SSH может выполняться для хостов без настроенного управления питанием. Эта операция отличается от обычного огораживания, которое может выполняться только для хостов с настроенным управлением питанием.

10.4.6. Использование возможностей хоста по управлению питанием

При настроенном на хосте управлении питанием, получить доступ к некоторому числу параметров управления питанием можно через интерфейс Портала администрирования. Хотя каждое устройство управления питанием обладает своими настраиваемыми параметрами, все они поддерживают базовые возможности запуска, остановки и перезапуска хоста.

Использование возможностей хоста по управлению питанием

1. Нажмите **Ресурсы → Хосты** и выберите хост.
2. Из выпадающего меню **Управление питанием** выберите одну из следующих возможностей:
    - **Перезапустить**: параметр останавливает работу хоста, пока статус хоста не сменится на «*Не запущен*». После того, как агент удостоверился в том, что хост не запущен, высокодоступные ВМ перезапускаются на другом хосте в

кластере. Затем агент перезапускает хост и статус готового к использованию хоста изменяется на «*Запущен*».

- **Запустить**: параметр запускает хост и даёт ему присоединиться к кластеру. Статус готового к использованию хоста изменяется на «*Запущен*».

- **Остановить**: параметр выключает питание хоста. Перед тем, как использовать этот параметр, убедитесь в том, что ВМ, выполняющиеся на хосте, уже мигрировали на другие хосты в кластере. В противном случае случится аварийное прерывание работы этих ВМ, и на другом хосте будут перезапущены только высокодоступные ВМ. После остановки хоста статус изменяется на «*В нерабочем состоянии*».

3. Нажмите **ОК**.

Примечание — если управление питанием не включено, для перезапуска или остановки работы хоста сначала выберите необходимый хост, затем из выпадающего меню **Управление** выберите один из следующих пунктов: **Управление SSH**, **Перезапустить** или **Остановить**.

Если на хосте было настроено два агента блокады, их можно использовать по очереди или параллельно. В случае параллельных агентов, для остановки хоста нужно, чтобы оба агента ответили на команду **Остановить**; а когда один из агентов ответит на команду **Запустить**, хост начнёт работу. В случае последовательных агентов, для остановки или запуска хоста сначала используется первичный агент, а в случае его сбоя используется вторичный агент.

10.4.7. Ручное изолирование не отвечающего хоста

В случае, если хост внезапно перестает отвечать (например, по причине аппаратного сбоя), то это может значительно повлиять на производительность окружения. При этом, в случае отсутствия устройства управления питанием или в случае некорректной настройки такого устройства, хост можно перезапустить вручную.

Примечание — используйте параметр **Подтвердить, что хост был перезагружен** только в случае, если хост был перезагружен вручную. Использование этого параметра во время работы хоста может привести к повреждению образа ВМ.

Ручное изолирование не отвечающего хоста

1. Нажмите **Ресурсы → Хосты** и убедитесь в том, что хост действительно имеет статус «*Не отвечает*».
2. Перезагрузите хост вручную (например, осуществите физическое взаимодействие с аппаратурой непосредственно в серверной).
3. Выберите хост, нажмите Больше действий (⋮) и далее Подтвердить, что хост был перезагружен.
4. Установите флажок **Одобрить действие** и нажмите **ОК**.

5. Если перезагрузка хоста занимает много времени, настройте параметр `ServerRebootTimeout` и укажите сколько секунд должно длиться ожидание перед тем, как хост получит статус «*Не отвечает*»:

```
# engine-config --set ServerRebootTimeout=целое_число
```

Глава 11. Хранилища

Система виртуализации ROSA Virtualization использует централизованную систему хранилищ для виртуальных дисков, файлов ISO и снимков ВМ.

В обязанности администратора входит создание, настройка, присоединение и поддержка хранилищ. Дополнительно администратору необходимо иметь представление о типах хранилищ и сценариях их использования.

Сеть хранения в системе виртуализации ROSA Virtualization может быть реализована следующими средствами:

- Сетевая файловая система NFS.
- Экспорт GlusterFS.
- Любые POSIX-совместимые файловые системы.
- Интерфейс iSCSI.
- Локальные хранилища, присоединённые непосредственно к хостам виртуализации.
- Протокол Fibre Channel (FCP).
- Параллельный доступ pNFS.

Настроенное хранилище является предварительным условием для создания дата-центра, поскольку дата-центр невозможно инициализировать до тех пор, пока не будут присоединены и активированы домены хранилищ.

Для добавления доменов хранилищ необходим рабочий доступ на **Портал администрирования**, а также как минимум один подключённый хост со статусом «*Запущен*».

В системе виртуализации ROSA Virtualization используются следующие типы доменов хранилищ:

- Домен данных.

В доменах данных хранятся виртуальные жёсткие диски и файлы OVF всех ВМ и шаблонов в дата-центре. Кроме того, в доменах данных хранятся снимки ВМ. Домены данных не могут быть общими для разных дата-центров. Домены данных нескольких различных типов (iSCSI, NFS, FC, POSIX и Gluster) могут быть добавлены в один дата-центр при условии, что они являются разделяемыми, а не локальными. Домен данных необходимо присоединить к дата-центру, перед тем как присоединять к дата-центру домены других типов.

- **Домен ISO**.

В доменах ISO хранятся файлы образов ISO (или логические носители CD), используемые для установки и загрузки операционных систем и приложений виртуальных машин. Наличие домена ISO отменяет необходимость физических носителей для дата-центров. Домен ISO может быть общим для разных дата-центров. Домены ISO могут создаваться только на базе файловой системы NFS. К дата-центру может быть присоединён только один домен ISO.

Примечание — домены ISO являются устаревшими, поэтому для хранения образов ISO рекомендуется использовать домен данных, созданный на базе файловой системы NFS.

- **Домен экспорта**.

Домены экспорта — это временные репозитории хранения, используемые для копирования и перемещения образов между дата-центрами и окружениями виртуализации ROSA Virtualization. Домен экспорта можно использовать для создания резервных копий ВМ. Домен экспорта можно перемещать между дата-центрами, при этом домен экспорта может быть активным одновременно только в одном из дата-центров. Домены экспорта можно создавать только на базе файловой системы NFS. К дата-центру может быть присоединён только один домен экспорта.

Примечание — домены хранилищ экспорта являются устаревшими. Домены хранилищ данных можно отсоединить от дата-центра и импортировать в другие дата-центры в том же или в другом окружении. После чего, виртуальные машины, «плавающие» виртуальные диски и шаблоны можно загрузить из домена хранения в прикреплённый дата-центр. Подробные сведения об импорте доменов хранилищ см. п. 11.7.2. Импорт доменов хранилищ.

Начинайте настройку и присоединение хранилищ к окружению виртуализации ROSA Virtualization только после того, как были определены требования к хранилищам со стороны дата-центров.

11.1. Домен хранилища

Домен хранилища — это собрание образов, имеющих общий интерфейс хранения. Домен хранилища содержит полные образы шаблонов и ВМ (включая снимки), или файлов ISO.

Домен хранилища может быть создан на базе блочных устройств (iSCSI или FCP) или файловых систем (NFS, GlusterFS, или других POSIX-совместимых 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 жёстких дисков.

В файловых системах все виртуальные диски, шаблоны и снимки являются файлами.

Виртуальные диски могут иметь два формата — QCOW2 или raw. Тип хранилища может быть разреженный (тонкое резервирование) или предварительно зарезервированный. Снимки всегда имеют разреженный тип, но могут быть сделаны для виртуальных дисков любого из вышеперечисленных форматов.

ВМ, разделяющие один и тот же домен хранилища, могут мигрировать между хостами в одном кластере.

11.2. Подготовка и добавление хранилища NFS

11.2.1. Подготовка хранилища NFS

Создайте общие ресурсы NFS в хранилище файлов или на удалённом сервере в качестве доменов хранилищ. После экспорта этих общих ресурсов в удалённое хранилище и настройки их конфигурации в виртуализированном ЦУ, они будут автоматически импортированы на хосты виртуализации.

Для того, чтобы виртуализированный ЦУ мог хранить данные в доменах хранилищ, представленных экспортированными каталогами, необходимы специальные системные учётные записи пользователей и системные группы пользователей.

В следующей последовательности действий описывается настройка прав доступа для каталога */exports/data*. Шаги с использованием команд `chown` и `chmod` необходимо повторить для каждого каталога, который планируется использовать в качестве домена хранилищ в системе виртуализации ROSA Virtualization.

Последовательность действий по подготовке хранилища NFS

1. Создайте группу `kvm`:

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

2. Создайте пользователя `vdsm` в группе `kvm`:

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

3. Укажите значение 36:36 для изменения владельцев каталога */exports/data* на `vdsm:kvm`:

```
# chown -R 36:36 /exports/data
```

4. Измените режим доступа к каталогу */exports/data* так, чтобы владелец имел доступ на чтение и запись, а группа и другие пользователи имели доступ на чтение и выполнение:

```
# chmod 0755 /exports/data
```

11.2.2. Добавление хранилища NFS

В следующей последовательности действий описывается как присоединить существующее хранилище NFS к окружению виртуализации ROSA Virtualization в качестве домена данных.

Последовательность действий по добавлению хранилища NFS

1. На Портале администрирования выберите **Хранилище → Домены**.
2. Нажмите **Добавить домен**.
3. В окне **Новый домен** укажите **Имя** домена хранилища (Рис. 137).

4. Примите значения по умолчанию для списков **Дата-центр**, **Функции домена**, **Тип хранилища**, **Формат** и **Хост**.
5. Введите **Путь экспорта**, используемый для домена хранилища. Путь должен иметь формат *123.123.0.10:/data* (для IPv4), *[2001:0:0:0:0:0:0:5db1]:/data* (для IPv6) или *domain.example.com:/data*.

6. При необходимости нажмите **Дополнительные параметры** для настройки следующих значений:

    a. В поле **Индикатор предупреждения о недостатке места (%)** укажите значение в процентах. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупреждающее сообщение, а событие будет занесено в журнал.
    b. В поле **Блокатор при отсутствии места (ГБ)** введите значение в Гбайт. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого значения, пользователю будет показано сообщение об ошибке, событие будет занесено в журнал, а любое новое действие (даже временное), которому необходимо дисковое пространство, будет заблокировано.
    c. Установите флажок **Забить нулями после удаления**. Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя.
7. Нажмите **OK**.

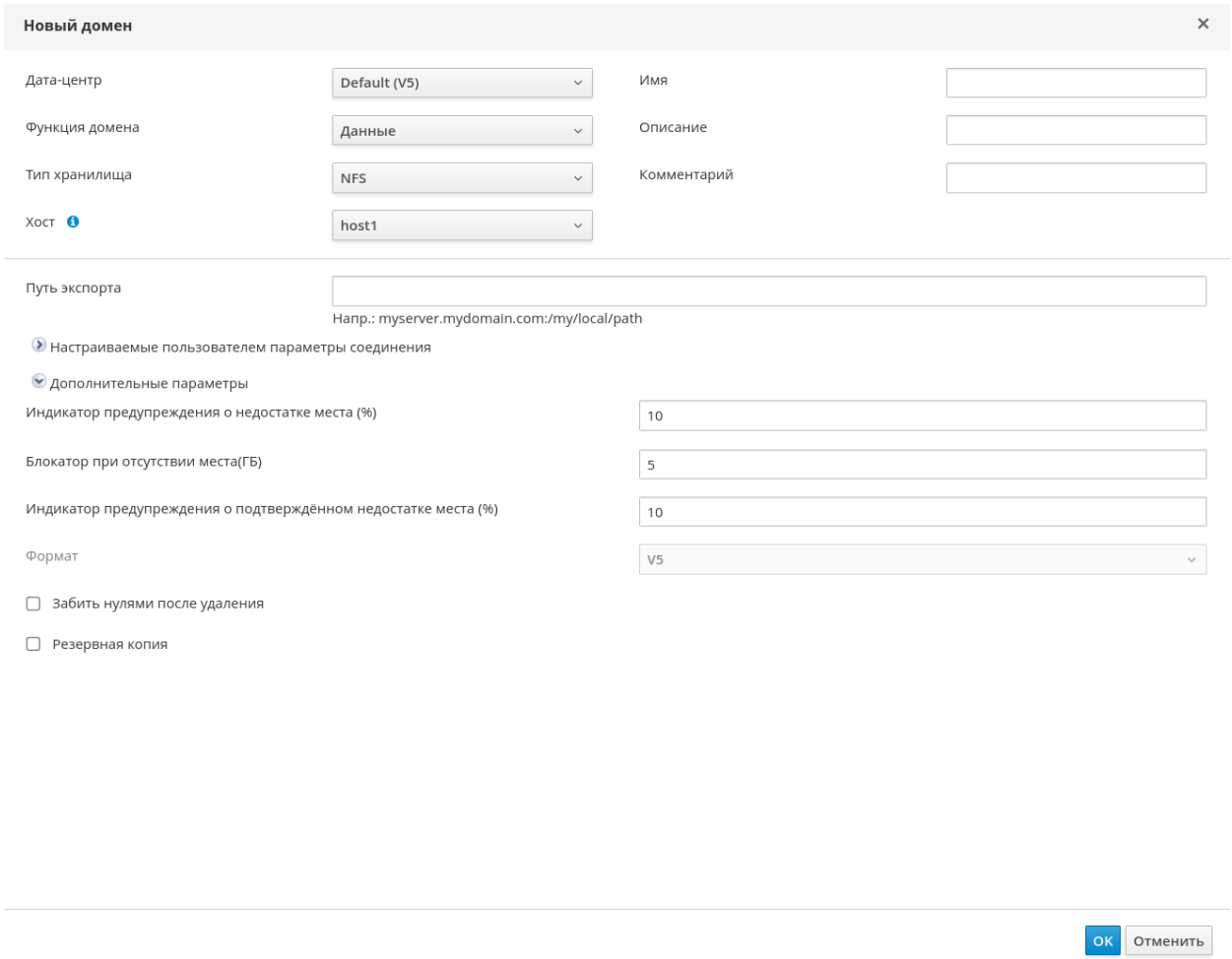

Рис. 137. Добавление хранилища NFS

Примечание — Новый домен данных NFS будет иметь статус «*Заблокировано*» до тех пор, пока не будет подготовлен диск, после чего домен будет автоматически подключён к дата-центру.

Добавлению хранилища NFS для домена ISO или домена экспорта

При необходимости использовать домен экспорта или домен ISO выполните вышеперечисленные действия, но в списке **Функция домена** выберите значение **Экспорт** или **ISO**.

11.2.3. Увеличение объёма хранилища NFS

Для увеличения объёма хранилища NFS можно либо создать новый домен хранилища и добавить его в существующий дата-центр, либо увеличить доступный объём на сервере NFS.

Увеличение существующего домена хранилища NFS

1. Нажмите **Хранилище** → **Домены**.
2. Нажмите на название существующего домена NFS, чтобы перейти к подробному просмотру.

3. Перейдите на вкладку **Дата-центр** и нажмите **Обслуживание**, чтобы перевести домен хранилища в режим обслуживания. Это действие размонтирует существующий общий ресурс и даст возможность изменить размер домена хранилища.
4. Измените размер хранилища на сервере NFS до необходимого объёма.
5. В подробном просмотре перейдите на вкладку **Дата-центр** и нажмите **Активировать** для того, чтобы смонтировать домен хранилища.

11.3. Подготовка и добавление локального хранилища

11.3.1. Подготовка локального хранилища

Локальный домен хранилища можно настроить на хосте. При настройке локального хранилища на хосте, хост автоматически добавляется в новый дата-центр и кластер, состоящий из одного хоста. Кластеры, состоящие из множества хостов, требуют, чтобы у каждого хоста имелся доступ ко всем доменам хранилищ, что невозможно в случае локального хранилища.

Примечание — Виртуальные машины, созданные в кластере с единственным хостом, не могут мигрировать, их нельзя изолировать (огородить) или добавить в планирование.

Примечание — На хостах виртуализации локальные хранилища всегда должны настраиваться на файловой системе, отделённой от корневого раздела `/`. Для предотвращения потенциальных потерь данных во время обновления версий ПО рекомендуется использовать отдельный логический том.

Подготовка локального хранилища на стандартных хостах

1. Создайте каталог (например */data/images*), который будет использоваться как локальное хранилище:

```
# mkdir -p /data/images
```

2. Измените владельцев каталога */data/images* на пользователя `vdsm` и группу `kvm`, и установите права на чтение и запись в каталоге */data/images* для владельца:

```
# chown 36:36 /data /data/images
# chmod 0755 /data /data/images
```

Подготовка локального хранилища на хостах виртуализации

На хосте виртуализации рекомендуется создать локальное хранилище на логическом томе следующим образом:

1. Создайте каталог локального хранилища:

```
# mkdir /data
# lvcreate -L $SIZE rhvh -n data
```

```
# mkfs.ext4 /dev/mapper/rhvh-data
# echo "/dev/mapper/rhvh-data /data ext4 defaults,discard 1 2" \
>> /etc/fstab
# mount /data
```

2. Смонтируйте новое локальное хранилище и затем измените владельца и права доступа:

```
# mount -a
# chown 36:36 /data /rhvh-data
# chmod 0755 /data /rhvh-data
```

11.3.2. Добавление локального хранилища

Добавление локального хранилища помещает хост в новый дата-центр и кластер.

В следующей последовательности действий соединено в окне параметров локального хранилища создание дата-центра, кластера и хранилища.

Последовательность действий по добавлению локального хранилища

1. Нажмите **Ресурсы → Хосты** и выберите хост.
2. Нажмите **Управление → Обслуживание** и далее нажмите OK.
3. Нажмите **Управление → Настроить**.
4. Нажмите на кнопки **Изменить** рядом с полями **Дата-центр**, **Кластер** и **Хранилище**, чтобы настроить домен локального хранилища.
5. В текстовом поле укажите путь до локального хранилища.
6. При необходимости перейдите на вкладку **Оптимизация**, чтобы настроить политику оптимизации памяти для нового кластера локального хранилища.
7. Нажмите **OK**.

В результате хост присоединится к сети в собственном дата-центре.

11.4. Управление хранилищами на базе файловой системы, совместимой с POSIX

11.4.1. Подготовка хранилища на базе файловой системы, совместимой с POSIX

Поддержка файловой системы стандарта POSIX даёт возможность монтировать файловые системы с теми же самыми параметрами монтирования, которые обычно применяются при ручном монтировании из командной строки.

Любая файловая система, совместимая с POSIX и используемая в качестве домена хранилища в системе виртуализации ROSA Virtualization, должна быть кластерной, а также должна поддерживать разреженные файлы и прямой ввод-вывод. Например, файловая система CIFS (Common Internet File System) не поддерживает механизм прямого ввода-вывода, что делает CIFS несовместимой с системой виртуализации ROSA Virtualization.

Примечание — *не монтируйте* хранилище NFS, создавая домен хранилища на базе ФС, совместимой с POSIX. Всегда создавайте для этого домен хранилища NFS.

11.4.2. Добавление хранилища на базе файловой системы, совместимой с POSIX

В следующей последовательности действий описывается как присоединить к системе виртуализации ROSA Virtualization в качестве домена данных существующее хранилище на базе файловой системы, совместимой с POSIX.

Последовательность действий по добавлению хранилища на базе файловой системы, совместимой с POSIX

1. Нажмите **Хранилище → Домены**.
2. Нажмите **Добавить домен**.
3. В окне **Новый домен** укажите **Имя** для домена хранилища (Рис. 138).
4. Выберите **Дата-центр**, связанный с доменом хранилища (выбранный дата-центр должен иметь тип POSIX), или при отсутствии такого дата-центра выберите **Нет**.
5. Из выпадающего списка **Функция домена** выберите **Данные**, а из списка **Тип хранилища** выберите **POSIX-совместимая ФС**.
6. Из выпадающего списка выберите **Хост**.
7. Укажите **Путь** до POSIX-совместимой ФС в формате команды `mount`.
8. Укажите **Тип VFS** в формате команды `mount` с аргументом `-t`.
9. Укажите дополнительные **Параметры монтирования** в формате команды `mount` с аргументом `-o`. Параметры монтирования должны указываться в виде списка, разделённого запятыми.
10. При необходимости нажмите **Дополнительные параметры** для настройки следующих значений:
    a. В поле **Индикатор предупреждения о недостатке места (%)** укажите значение в процентах. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупреждающее сообщение, а событие будет занесено в журнал.
    b. В поле **Блокатор при отсутствии места (ГБ)** введите значение в Гбайт. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого значения, пользователю будет показано сообщение об ошибке, событие будет занесено в журнал, а любое новое действие (даже временное), которому необходимо дисковое пространство, будет заблокировано.
    c. Установите флажок **Забить нулями после удаления**. Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя.
11. Нажмите **OK**.

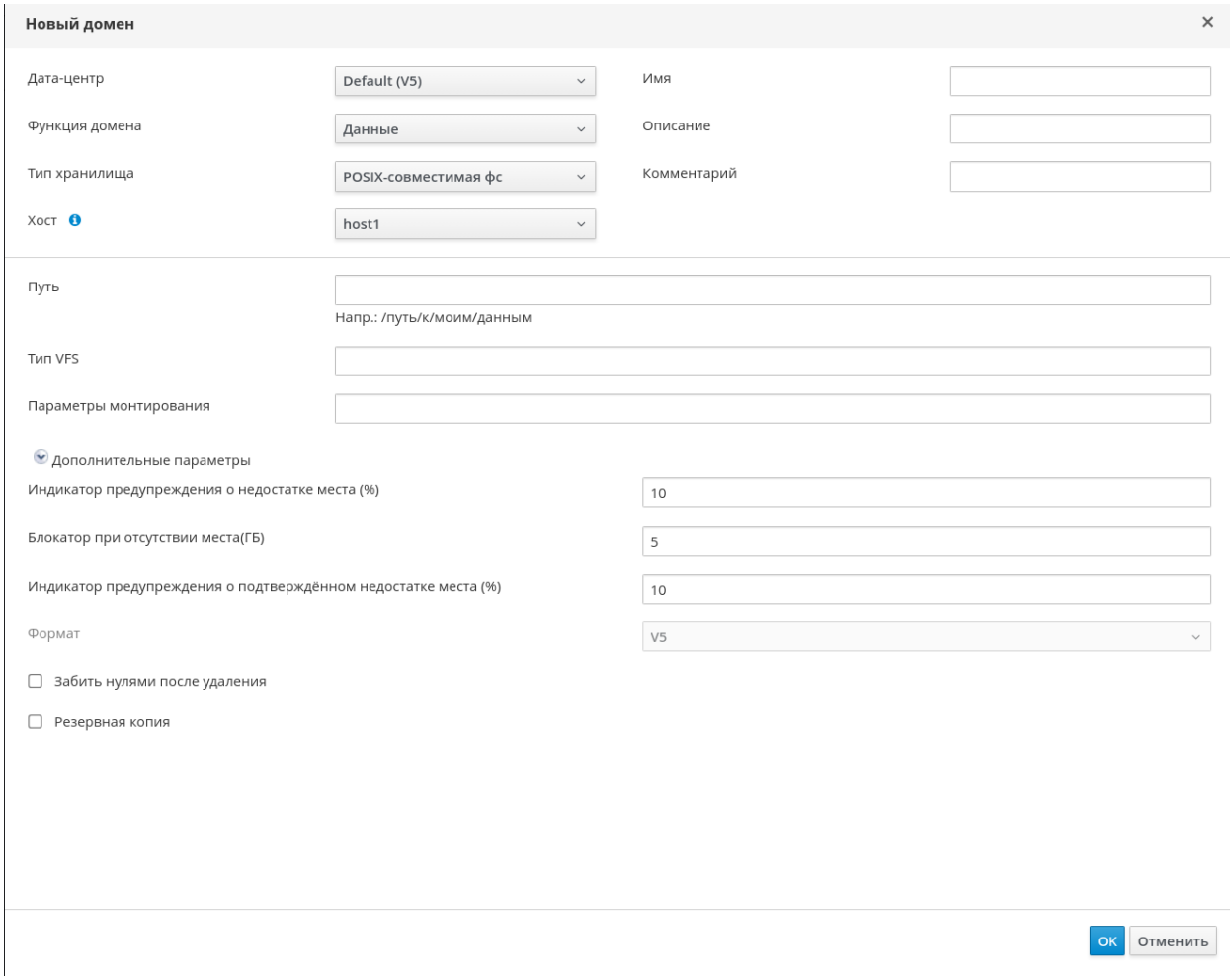

Рис. 138. Добавление хранилища с POSIX-совместимой файловой системой

11.5. Подготовка и добавление блочного хранилища

11.5.1. Подготовка хранилища iSCSI

Система виртуализации ROSA Virtualization поддерживает хранилища iSCSI.

Хранилище iSCSI представляет собой домен хранилища из группы томов на базе LUN. Группы томов и номера LUN нельзя присоединить более чем к одному домену хранилища одновременно.

Примечания:

- При использовании блочного хранилища и планировании размещения ВМ на устройствах raw или прямых LUN под управлением диспетчера логических томов необходимо создать фильтр для скрытия гостевых логических томов. Это предотвратит активацию гостевых томов при загрузке хоста, что потенциально может привести к повреждению данных.
- Система виртуализации ROSA Virtualization на данный момент не поддерживает хранилища с размером блоков в 4Кбайт. Блочные хранилища необходимо настраивать в старом режиме (512 байт на блок).
- В ситуации, когда хост загружается из хранилища SAN и впоследствии теряет связь с хранилищем, файловые системы хранилища становятся доступны только для чтения и остаются в этом состоянии после восстановления связи. Для

предотвращения этой ситуации рекомендуется добавить в корневую ФС SAN замещающий конфигурационный файл доступа по нескольким путям к загрузочным LUN, чтобы обеспечить постановку их в очередь при наличии соединения:

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

11.5.2. Добавление хранилища iSCSI

В следующей последовательности действий описывается как присоединить к системе виртуализации ROSA Virtualization в качестве домена данных существующее хранилище iSCSI.

Последовательность действий по добавлению хранилища iSCSI

1. Нажмите **Хранилище → Домены**.
2. Нажмите **Добавить домен**.
3. В окне **Новый домен** укажите **Имя домена хранилища** (Рис. 139).

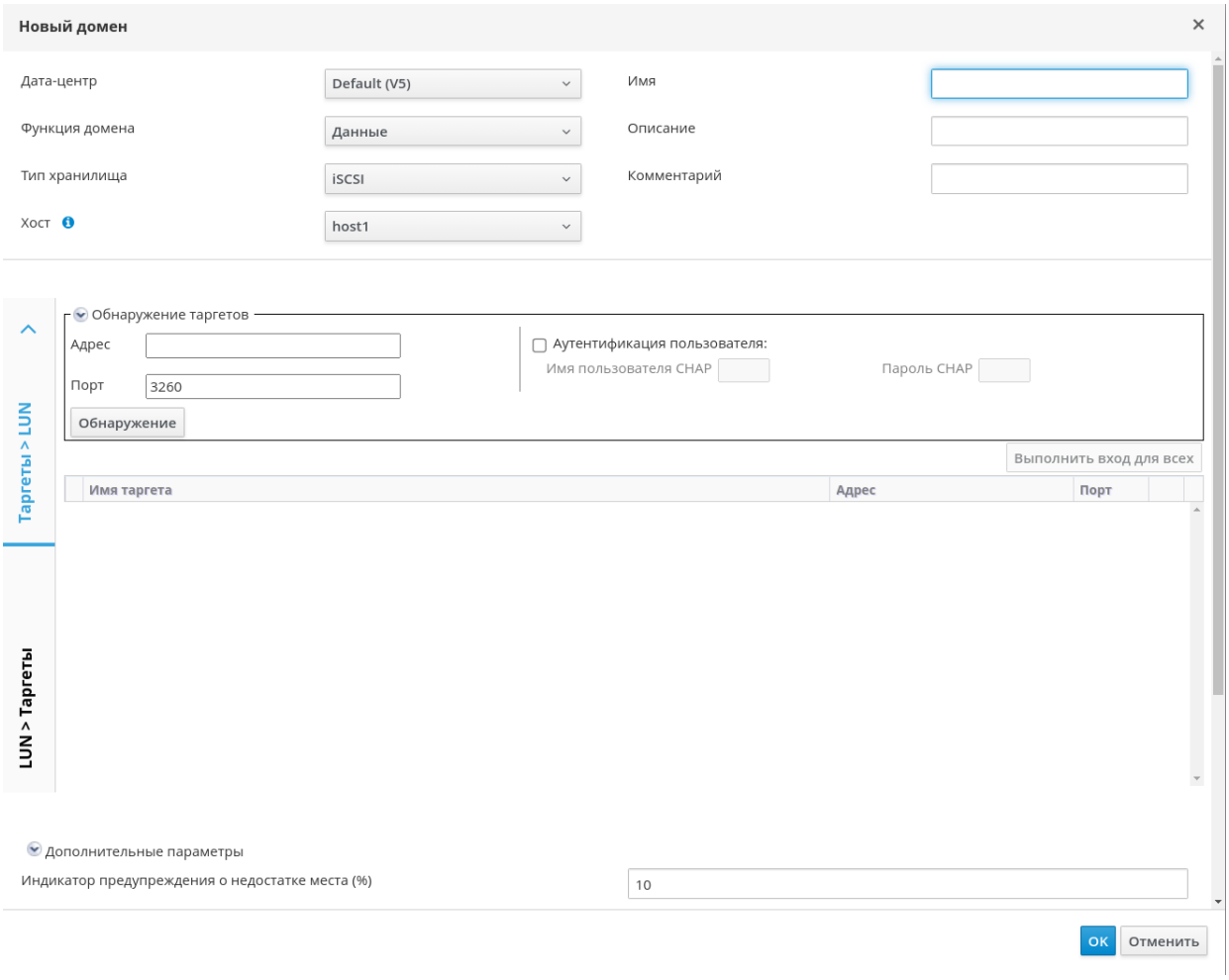

Рис. 139. Добавление хранилища iSCSI

4. Выберите **Дата-центр**.
5. В качестве **Функции** домена выберите **Данные**, а в качестве **Типа хранилища** выберите **iSCSI**.
6. Из выпадающего списка **Хост** выберите активный хост.

Примечание — подключение к домену хранилища идёт от выбранного хоста, а не напрямую из виртуализированного ЦУ, поэтому у всех хостов должен быть доступ к устройству хранения, до того как будет настроен домен хранилища.

7. Виртуализированный ЦУ может отобразить цели iSCSI на номера LUN или номера LUN на цели iSCSI. В окне **Новый домен** при выборе типа хранилища **iSCSI** автоматически отображаются известные цели с неиспользуемыми LUN. Опционально, если отсутствует цель, используемая для добавления хранилища, выполните следующие действия по обнаружению целей:

    a. Для активации возможности обнаружения целей нажмите **Обнаружить цели**. В результате в окне **Новый домен** автоматически будут показаны цели с неиспользуемыми в окружении LUN, а также будут показаны LUN, используемые вне окружения. Параметр **Обнаружить цели** можно использовать для добавления LUN ко многим целям или нескольких путей к одним и тем же LUN.

    b. В поле **Адрес** введите полное доменное имя или IP-адрес хоста iSCSI (Рис. 140).

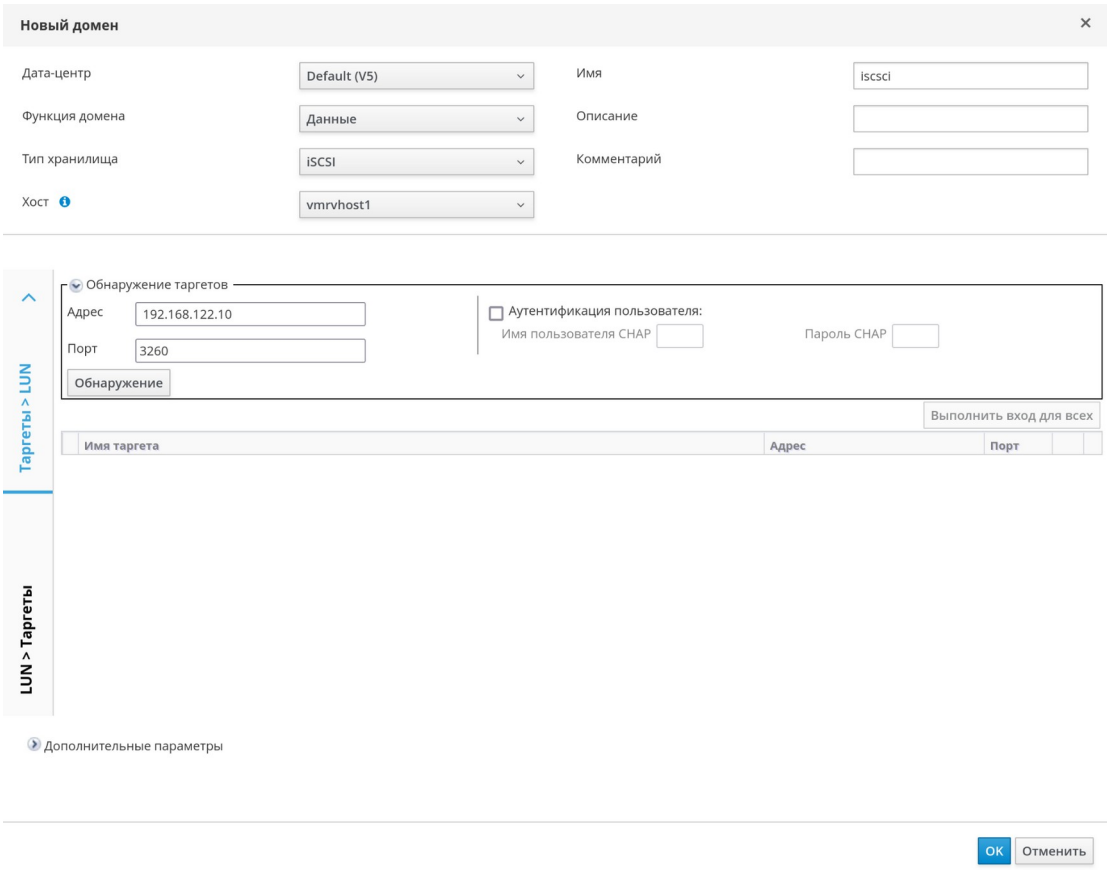

Рис. 140. Секция Обнаружение таргетов для хранилища типа iSCSI

c. В поле **Порт** укажите номер порта, к которому будет подключаться хост при просмотре целей (Рис. 140). Значение по умолчанию — `3260`.
d. Если для защиты хранилища используется CHAP, установите флажок **Аутентификация пользователей** и далее введите **Имя пользователя CHAP** и **Пароль CHAP** (Рис. 140).

Примечание — настроить учётные записи цели iSCSI для конкретного хоста можно с помощью REST API.

e. Нажмите **Обнаружение**.
f. Выберите одну или несколько целей из списка с результатами обнаружения (Рис. 141).

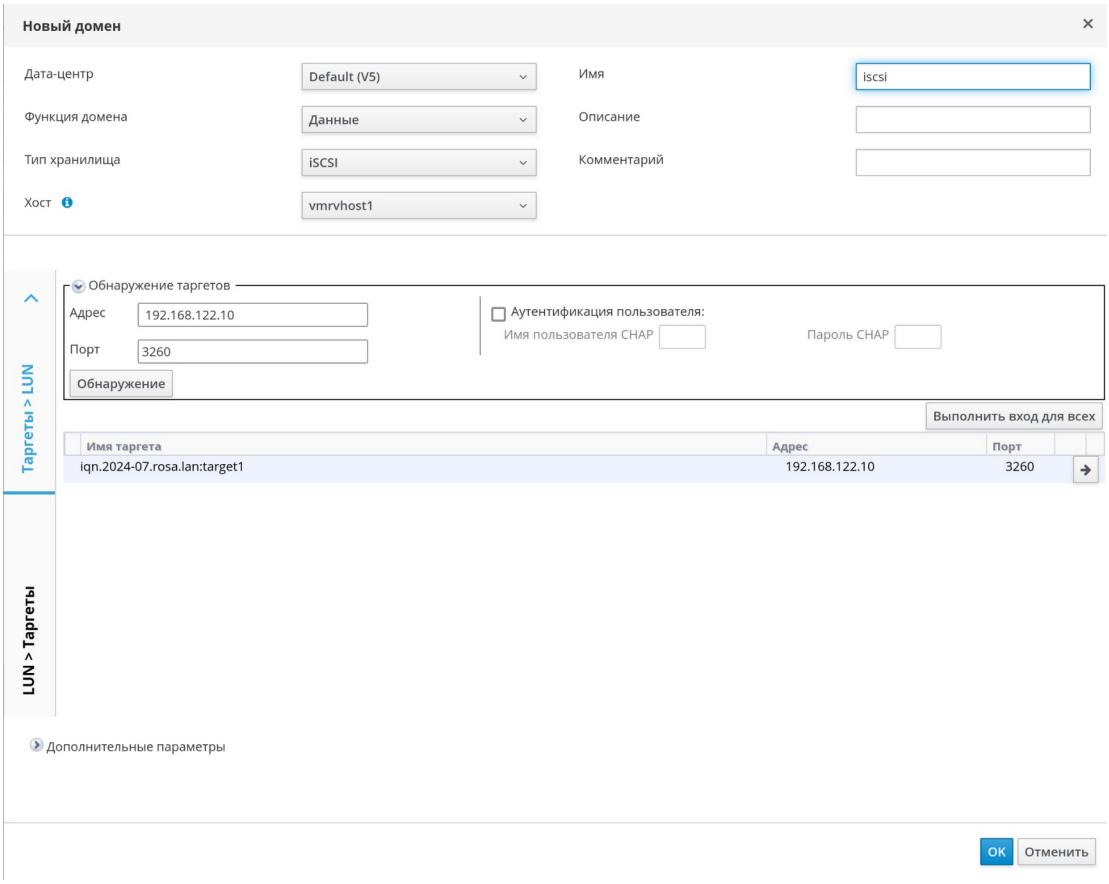

Рис. 141. Список целей iSCSI - результаты обнаружения целей

g. Нажмите **Вход в систему** при выборе одной цели или нажмите **Выполнить вход для всех** при выборе нескольких целей (стрелка вправо, в правой части формы, Рис. 141).

Примечание — если для доступа требуется более одного пути, необходимо обнаружить и выполнить вход на цели с использованием всех путей. Изменение домена хранилища для добавления дополнительных путей на данный момент не поддерживается.

8. Нажмите на кнопку + (плюс) рядом с необходимой целью (Рис. 142). Элемент раскроется и будут показаны все неиспользуемые LUN, присоединённые к цели.

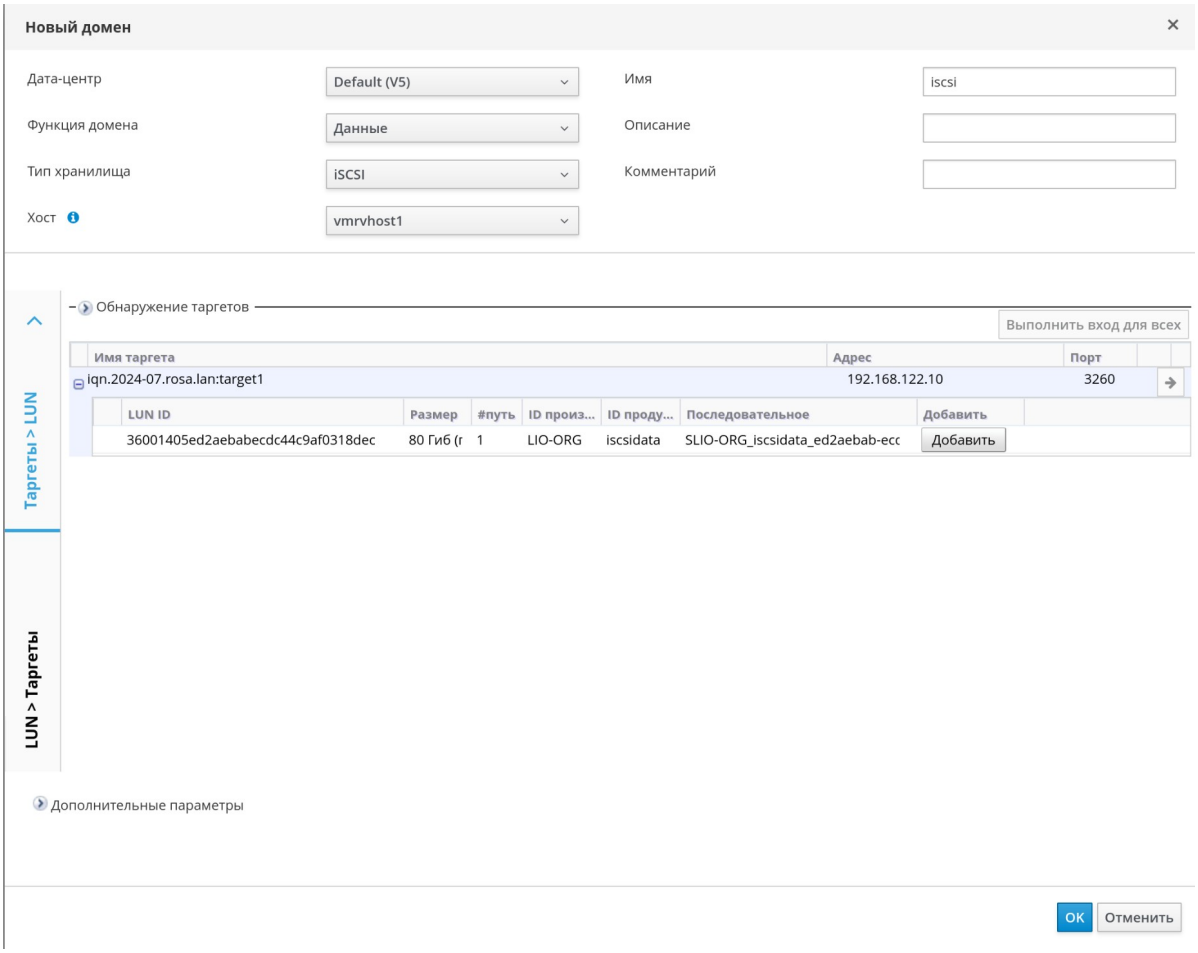

Рис. 142. Добавление цели iSCSI — нажмите Добавить для добавления

9. Установите флажок для каждого LUN, используемого для создания домена хранилища.
10. При необходимости нажмите **Дополнительные параметры** для настройки следующих значений:
    a. В поле **Индикатор предупреждения о недостатке места (%)** укажите значение в процентах. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупреждающее сообщение, а событие будет занесено в журнал.
    b. В поле **Блокатор при отсутствии места (ГБ)** введите значение в Гбайт. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого значения, пользователю будет показано сообщение об ошибке, событие будет занесено в журнал, а любое новое действие (даже временное), которому необходимо дисковое пространство, будет заблокировано.

c. Установите флажок **Забить нулями после удаления**. Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя.

11. Нажмите **OK**. После проведения инициализации хранилище iSCSI будет добавлено в список доступных хранилищ.

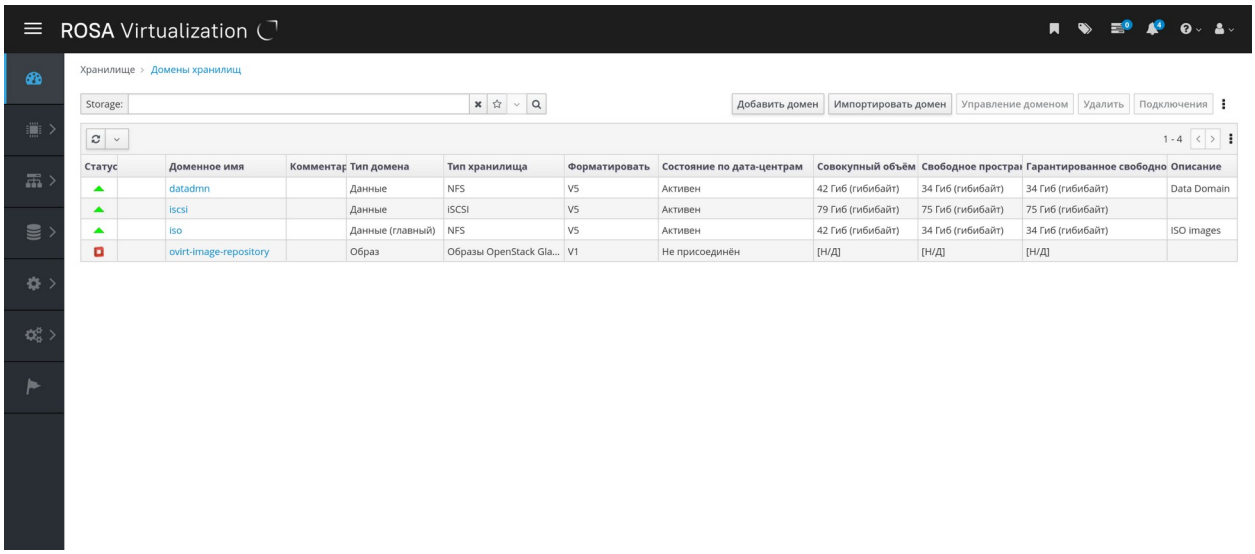

Рис. 143. Домен хранилища с типом хранилища iSCSI добавлен и активен

Если к одной цели было настроено несколько соединений из хранилищ, то для завершения создания связки iSCSI следуйте инструкции, приведенной в п. 11.5.3. Настройка доступа к iSCSI по нескольким путям.

В случае, если текущая сеть хранилища должна мигрировать в связку iSCSI, см. п. 11.7.4. Миграция доменов хранилищ между дата-центрами в разных окружениях.

11.5.3. Настройка доступа к iSCSI по нескольким путям

Доступ к iSCSI по нескольким путям даёт возможность создания и управления группами логических сетей и подключений к хранилищу iSCSI. Конфигурация нескольких сетевых путей от хоста до хранилища iSCSI предохраняет хост от простоя во время потенциального сбоя сетевого пути.

С помощью сетевых карт или VLAN, присвоенных логическим путям в связке iSCSI, виртуализированный ЦУ подключает каждый хост в дата-центре к каждой из целей.

В целях избыточности связку iSCSI можно создать с помощью нескольких целей iSCSI и логических сетей.

Предварительным условием для настройки доступа к iSCSI по нескольким путям является наличие одной или нескольких целей iSCSI (см. п. 11.5.2. Добавление хранилища iSCSI), а также одной или нескольких логических сетей (см. п. 9.1.2. Создание новой логической сети в дата-центре или кластере), отвечающих следующим требованиям:

- Логическая сеть не является требуемой сетью или сетью виртуальной машины.
- Логическая сеть присвоена интерфейсу хоста (см. п. 9.4.2. Изменение параметров сетевых интерфейсов и присвоение хостам логических сетей).
- Логической сети присвоен статический IP-адрес в той же VLAN и подсети, в которой размещаются другие логические сети в связке iSCSI (см. п. 9.4.2. Изменение параметров сетевых интерфейсов и присвоение хостам логических сетей).

Настройка доступа к iSCSI по нескольким путям

1. Нажмите **Ресурсы → Дата-центры**.
2. Нажмите на имя дата-центра, чтобы перейти к подробному просмотру.
3. На вкладке Доступ к iSCSI по нескольким путям нажмите Добавить.
4. В окне **Добавить связку iSCSI** укажите **Имя** и **Описание**.
5. Выберите логическую сеть из списка **Логические сети** и домен хранилища из списка **Таргеты хранилища**, при этом все пути до одной и той же цели должны быть выбраны.
6. Нажмите **OK**.

В результате хосты в дата-центре будут подключены к целям iSCSI с помощью логических сетей в связке iSCSI.

11.5.4. Миграция логической сети в связку iSCSI

При наличии логической сети, созданной для передачи трафика iSCSI и настроенной поверх существующей сетевой связки, эту сеть можно перенести в связку iSCSI в той же подсети с нулевым временем простоя и без сбоев.

Миграция логической сети в связку iSCSI

1. Измените текущую логическую сеть так, чтобы она не была **Требуемой**:
    a. Нажмите **Ресурсы → Кластеры**.
    b. Нажмите на название кластера, чтобы перейти к подробному просмотру.
    c. Во вкладке **Логические сети** выберите текущую логическую сеть (например, `net-1`) и нажмите **Управление сетями**.
    d. Снимите флажок **Требуется** и нажмите **OK**.

2. Создайте новую логическую сеть, не являющуюся **Требуемой** и не являющуюся **Сетью ВМ**:
    a. Нажмите **Добавить сеть**, чтобы открыть окно Новая логическая сеть.
    b. Во вкладке **Общие** введите **Имя** (например, `net-2`) и снимите флажок **Сеть ВМ**.
    c. Во вкладке **Кластер** снимите флажок **Требовать** и нажмите **OK**.

3. Удалите текущую сетевую связку и заново присвойте логические сети:
    a. Нажмите **Ресурсы → Хосты**.

b. Нажмите на имя хоста, чтобы перейти к подробному просмотру.
c. Во вкладке Сетевые интерфейсы нажмите Настроить сети хоста.
d. Перетащите сеть `net-1` вправо, чтобы заново присвоить эту сеть.
e. Перетащите текущую связку вправо для удаления.
f. Перетащите сети `net-1` и `net-2` влево, чтобы присвоить эти сети физическим интерфейсам.
g. Нажмите на значок карандаша рядом с сетью `net-2`, чтобы открыть окно **Свойства сети**.
h. Во вкладке **IPV4** выберите **Статический**.
i. Укажите **IP** и Сетевую маску/префикс маршрутизации подсети и нажмите **OK**.

4. Создайте связку **iSCSI**:

a. Нажмите **Ресурсы → Дата-центры**.
b. Нажмите на имя дата-центра, чтобы перейти к подробному просмотру.
c. Во вкладке Доступ к iSCSI по нескольким путям нажмите Добавить.
d. В окне **Добавить связку iSCSI** укажите **Имя**, выберите сети `net-1` и `net-2`, и нажмите **OK**.

В результате в дата-центре теперь будет связка iSCSI, включающая в себя и старую (`net-1`), и новую (`net-2`) логические сети.

11.5.5. Подготовка хранилища FCP

Система виртуализации ROSA Virtualization поддерживает хранилище SAN путём создания домена хранилища из группы томов, созданной из ранее существовавших LUN. Ни группы томов, ни номера LUN нельзя присоединить более чем к одному домену хранилища одновременно.

Примечание — Администраторы системы виртуализации ROSA Virtualization должны иметь практические знания о теории и принципах работы сетей хранения данных SAN. Как правило, для переноса трафика между хостом и общим внешним хранилищем SAN используется протокол FCP. В связи с этим, SAN иногда называют *хранилищем FCP*.

Примечания:

- При использовании блочного хранилища и планировании размещения ВМ на устройствах raw или прямых LUN под управлением диспетчера логических томов необходимо создать фильтр для скрытия гостевых логических томов. Это предотвратит активацию гостевых томов при загрузке хоста, что потенциально может привести к повреждению данных.
- Система виртуализации ROSA Virtualization на данный момент не поддерживает хранилища с размером блоков в 4Кбайт. Блочные хранилища необходимо настраивать в старом режиме (512 байт на блок).
- В ситуации, когда хост загружается из хранилища SAN и впоследствии теряет связь с хранилищем, файловые системы хранилища становятся доступны только для чтения и остаются в этом состоянии после восстановления связи. Для

предотвращения этой ситуации рекомендуется добавить в корневую ФС SAN замещающий конфигурационный файл доступа по нескольким путям к загрузочным LUN, чтобы обеспечить постановку их в очередь при наличии соединения:

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

11.5.6. Добавление хранилища FCP

В следующей последовательности действий описывается как присоединить к системе виртуализации ROSA Virtualization в качестве домена данных существующее хранилище FCP.

Последовательность действий по добавлению хранилища FCP

1. Нажмите **Хранилище → Домены**.
2. Нажмите **Добавить домен**.
3. Укажите **Имя** домена хранилища.
4. Из выпадающего списка выберите **Дата-центр FCP**, или при отсутствии такого дата-центра выберите **Нет**.
5. Из выпадающих списков выберите **Функцию домена** и **Тип хранилища**. Типы доменов хранилища, несовместимые с выбранным дата-центром, не будут доступны.
6. В поле **Хост** выберите активный хост. Если этот домен данных не первый в этом дата-центре, необходимо выбрать SPM хост дата-центра.

Примечание — подключение к домену хранилища идёт через выбранный хост, а не напрямую из виртуализированного ЦУ. В системе должен существовать как минимум один активный хост, присоединённый к выбранному дата-центру. До начала настройки домена хранилища у всех хостов должен быть доступ к устройству хранения.

7. При выборе типа хранилища **Оптоволокно**, в окне **Новый домен** автоматически показываются известные цели с неиспользуемыми LUN. Установите флажок **LUN ID**, чтобы выбрать все доступные LUN.
8. Опционально нажмите **Дополнительные параметры** для настройки следующих значений:
    a. В поле **Индикатор предупреждения о недостатке места** введите процентное значение. Если объём свободного пространства, доступного в домене хранилища, будет ниже этого процентного значения, пользователю будет показано предупреждающее сообщение, а событие будет занесено в журнал.
    b. В поле **Блокатор при отсутствии места (ГБ)** введите значение в Гбайт. Если объём свободного пространства, доступного в домене хранилища,

будет ниже этого значения, пользователю будет показано сообщение об ошибке, событие будет занесено в журнал, а любое новое действие (даже временное), которому необходимо дисковое пространство, будет заблокировано.

c. Установите флажок **Забить нулями после удаления**. Этот выбор можно изменить после создания домена, но для уже существующих дисков этот параметр изменить нельзя.

9. Нажмите **OK**.

Примечание — Во время подготовки к использованию домен данных FCP будет иметь статус «*Заблокировано*». Домен автоматически присоединится к дата-центру, когда будет готов к использованию.

11.5.7. Увеличение размера хранилища iSCSI или FCP

Для увеличения объёма хранилища iSCSI или FCP существуют следующие способы:

- Добавление существующего LUN в текущий домен хранения.
- Создание нового домена с новыми LUN, и добавление этого домена в существующий дата-центр (см. п. 11.7.2. Импорт доменов хранилищ).
- Расширение домена хранения за счёт изменения размера базовых LUN.

В следующей последовательности действий описывается как расширить хранилище сети хранения данных SAN при помощи добавления нового номера LUN в существующий домен хранения со статусом «*Запущен*».

Примечание — все хосты со статусом «*Запущен*» должны иметь доступ к LUN, в противном случае действие закончится неудачей, и LUN не будет добавлен в домен хранения. При этом хосты не будут затронуты. Если недавно добавленный хост, а также хост, выходящий из режима обслуживания или из статуса «*В нерабочем состоянии*», не будет иметь доступа к LUN, то такой хост получит статус «*В нерабочем состоянии*».

Увеличение размера существующего хранилища iSCSI или FCP

1. Нажмите **Хранилище → Домены** и выберите домен iSCSI или FCP.
2. Нажмите **Управление доменом**.
3. Нажмите **Таргеты** > **LUN** и далее нажмите **Обнаружить таргеты**.
4. Укажите сведения о подключении для сервера хранилища и далее нажмите **Обнаружить** для инициации подключения.
5. Нажмите **Таргеты > LUN** и установите флажок для нового доступного LUN.
6. Нажмите **OK**, чтобы добавить LUN в выбранный домен хранения.

В результате домен хранения увеличится на размер добавленного LUN.

При расширении домена хранения с помощью изменения размера базовых LUN, информация об этих LUN также должна быть обновлена на Портале администрирования.

Обновление информации о размере LUN на Портале администрирования

1. Нажмите **Хранилище → Домены** и выберите домен iSCSI или FCP.
2. Нажмите **Управление доменом**.

3. Нажмите **LUN** > **Таргеты**.
4. В столбце **Дополнительный размер** нажмите на кнопку **Добавить дополнительный размер хранилища** для обновления информации о LUN.
5. Нажмите **OK**, чтобы LUN отображал новый размер хранилища.

11.5.8. Повторное использование LUN

Обратите внимание, что номера LUN не могут быть повторно использованы в их текущем состоянии для создания домена хранилища или виртуального диска. При попытке повторно использовать LUN будет выведено следующее сообщение об ошибке на Портале администрирования:

```
        Сбой инициализации физического устройства. Убедитесь, что устройство
    пусто и у хоста есть к нему доступ.
```

Виртуализированный ЦУ покажет следующую ошибку во время установки:

```
        [ ERROR ] Error creating Volume Group: Failed to initialize physical
    device: ("[u'/dev/mapper/000000000000000000000']",)
        [ ERROR ] Failed to execute stage 'Misc configuration': Failed to
    initialize physical device: ("[u'/dev/mapper/000000000000000000000']",)
```

Перед повторным использованием номера LUN необходимо очистить старую таблицу разделов от LUN. Для этого выполните команду `dd` с указанием идентификатора LUN, который необходимо использовать повторно, максимального числа байтов для одновременного чтения и записи, а также числа копируемых входных блоков:

```
# dd if=/dev/zero of=/dev/mapper/LUN_ID bs=1M count=200 oflag=direct
```

Примечание — это действие необходимо выполнить для корректного LUN во избежание непреднамеренного повреждения данных.

11.6. Подготовка и добавление хранилища Gluster

Процесс развёртывания хранилища Gluster приведен в документе «Платформа виртуализации *«ROSA Virtualization» (версия 3.0). Руководство по установке»* РСЮК.10102-01 91 01.

11.7. Импорт существующих доменов хранилищ

11.7.1. Обзор процесса импорта существующих доменов хранилищ

Кроме добавления новых доменов хранилищ, не содержащих данных, можно импортировать уже существующие и получать доступ к хранящимся в них данным. С помощью импорта домена хранилища можно восстанавливать данные после сбоев в базе данных виртуализированного ЦУ, а также переносить данные из одного дата-центра или окружения в другое.

Ниже приводится общий обзор процесса импорта для каждого из типов доменов хранилищ:

- **Домен данных**.

Импорт существующего домена хранения данных даёт доступ ко всем ВМ и шаблонам, хранящимся в этом домене. После импорта домена данных необходимо вручную импортировать ВМ, образы «плавающих» виртуальных дисков и шаблоны в целевой дата-центр. Процесс импорта ВМ и шаблонов, хранящихся в домене данных, аналогичен процессу экспорта домена хранилищ. Но, поскольку домены хранения данных содержат все ВМ и шаблоны указанного дата-центра, импорт доменов хранения данных рекомендуется осуществлять в целях восстановления данных или при масштабных миграциях ВМ между дата-центрами или окружениями.

Примечание — импорт существующих доменов хранения данных, присоединённых к дата-центрам, возможен при корректном поддерживаемом уровне совместимости.

- **Домен ISO**.

Импорт существующего домена хранения ISO даёт доступ ко всем файлам ISO и виртуальным дискам, хранящимся в этом домене. После завершения процесса импорта для доступа к этим ресурсам не требуется дополнительных действий, их можно присоединять к виртуальным машинам по требованию.

Примечание — домены ISO являются устаревшими, поэтому для хранения образов ISO рекомендуется использовать домен данных, созданный на базе файловой системы NFS.

- **Домен экспорта**.

Импорт существующего домена хранения экспорта даёт доступ ко всем образам ВМ и шаблонам, хранящимся в этом домене. Поскольку домены экспорта созданы для экспорта и импорта образов ВМ и шаблонов, импорт доменов хранения экспорта рекомендуется осуществлять при небольших миграциях ВМ и шаблонов внутри окружения или между окружениями.

Примечание — домены хранилищ экспорта являются устаревшими. Домены хранилищ данных можно отсоединить от дата-центра и импортировать в другие дата-центры в том же или в другом окружении. После чего, виртуальные машины, «плавающие» виртуальные диски и шаблоны можно загрузить из домена хранения в прикреплённый дата-центр. Подробные сведения об импорте доменов хранилищ см. п. 11.7.2. Импорт доменов хранилищ.

Обратите внимание, что после прикрепления домена хранения к целевому дата-центру домен может быть обновлён до нового формата, после чего повторное прикрепление к исходному дата-центру может быть невозможным. В свою очередь, это может нарушить процесс использования доменов данных в качестве замены доменам экспорта.

11.7.2. Импорт доменов хранилищ

Для предотвращения возможного повреждения данных при импорте домена хранения, ранее прикреплённого к дата-центру в том же или в другом окружении, подразумевается, что домен хранения уже не прикреплён ни к одному из дата-центров в любом окружении.

Обратите внимание, что целевой дата-центр должен быть инициализирован для импорта и прикрепления существующего домена хранения к этому дата-центру.

Импорт домена хранения

1. Нажмите **Хранилище → Домены**.
2. Нажмите **Импортировать домен**.
3. Выберите **Дата-центр**, в который нужно импортировать домен хранения.
4. Укажите **Имя** домена хранения (Рис. 144).
5. Из выпадающих списков выберите **Функцию домена** и **Тип хранилища**.
6. Выберите **Хост**.

Примечание — подключение к домену осуществляется через выбранный хост, а не напрямую из виртуализированного ЦУ. Таким образом должен существовать как минимум один активный хост, присоединённый к выбранному дата-центру. До начала настройки домена у всех хостов должен быть доступ к устройству хранения.

7. Укажите сведения о домене хранения.

Примечание — поля для ввода сведений о домене хранения изменяются в зависимости от значений, выбранных в списках **Функция домена** и **Тип хранилища**. Эти поля аналогичны полям, отображаемым при добавлении нового домена хранения.

8. Установите флажок **Активировать домен в дата-центре**, чтобы активировать домен хранения после присоединения его к выбранному дата-центру.
9. Нажмите **OK**.

В результате из домена хранения теперь можно импортировать ВМ и шаблоны в выбранный дата-центр.

Рис. 144. Импорт домена хранения

11.7.3. Миграция доменов хранилищ между дата-центрами в одном окружении

При миграции домена хранения между дата-центрами в границах окружения системы виртуализации ROSA Virtualization осуществляется открепление домена от одного дата-центра и прикрепление к другому дата-центру, чтобы целевой дата-центр получил доступ к данным, хранящимся в домене.

Миграция домена хранения между дата-центрами в одном окружении

1. Выключите все ВМ, выполняющиеся в домене хранения.
2. Нажмите **Хранилище → Домены**.
3. Нажмите на название домена хранения, чтобы перейти к подробному просмотру.
4. Перейдите на вкладку **Дата-центр**.
5. Нажмите **Обслуживание** и нажмите **OK**.
6. Нажмите **Отсоединить** и нажмите **OK**.
7. Нажмите **Присоединить**.
8. Выберите целевой дата-центр и нажмите **OK**.

В результате домен хранения прикреплён к целевому дата-центру и автоматически активируется, что позволяет импортировать ВМ и шаблоны из домена хранения в целевой дата-центр.

11.7.4. Миграция доменов хранилищ между дата-центрами в разных окружениях

При миграции домена хранения между дата-центрами в разных окружениях системы виртуализации ROSA Virtualization осуществляется удаление домена из одного окружения и импорт домена в другое окружение, чтобы целевое окружение получило доступ к данным, хранящимся в домене.

Дата-центры в разных окружениях должны иметь корректный поддерживаемый уровень совместимости для обеспечения возможности импорта и присоединения домена хранения данных.

Миграция домена хранения между дата-центрами в разных окружениях

1. Войдите на **Портал администрирования** в исходном окружении.
2. Выключите все ВМ, выполняющиеся в домене хранения.
3. Нажмите **Хранилище → Домены**.
4. Нажмите на название домена хранения, чтобы перейти к подробному просмотру.
5. Перейдите на вкладку **Дата-центр**.
6. Нажмите **Обслуживание** и нажмите **OK**.
7. Нажмите **Открепить** и нажмите **OK**.
8. Нажмите **Удалить**.
9. В окне **Удалить хранилище** убедитесь в том, что флажок **Форматировать домен, т.е. содержимое хранилища будет потеряно** не установлен. Таким образом данные в домене сохраняются для последующего использования.
10. Нажмите **OK** для удаления домена хранения из исходного окружения.

11. Войдите на **Портал администрирования** в целевом окружении.
12. Нажмите **Хранилище → Домены**.
13. Нажмите **Импортировать домен**.
14. Из выпадающего списка **Дата-центр** выберите целевой дата-центр.
15. Введите **Имя** домена хранения.
16. Из соответствующих выпадающих списков выберите **Функцию домена** и **Тип хранилища**.
17. Выберите **Хост**.
18. Укажите сведения о домене хранения.

Примечание — поля для ввода сведений о домене хранения изменяются в зависимости от значений, выбранных в списках **Функция домена** и **Тип хранилища**. Эти поля аналогичны полям, отображаемым при добавлении нового домена хранения.

19. Установите флажок **Активировать домен дата-центра**, чтобы домен хранения был активирован автоматически при присоединении.
20. Нажмите **OK**.

В результате домен хранения будет присоединён к целевому дата-центру в новом окружении системы виртуализации ROSA Virtualization и автоматически активирован, что позволяет импортировать ВМ и шаблоны из домена хранения в целевой дата-центр.

11.7.5. Импорт виртуальных машин из импортированных доменов данных

Импорт ВМ из импортированного домена хранения данных может осуществляться в один или несколько целевых кластеров.

В следующей последовательности действий предполагается, что ранее импортированный домен хранения данных был присоединён к дата-центру и активирован.

Импорт ВМ из импортированного домена данных

1. Нажмите **Хранилище → Домены**.
2. Нажмите на имя импортированного домена данных, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Импорт ВМ**.
4. Выберите одну или несколько ВМ для импорта.
5. Нажмите **Импортировать**.
6. Убедитесь, что для каждой ВМ в окне **Импорт ВМ** выбран корректный целевой кластер из списка **Кластер**.
7. Отобразите внешние профили vNIC ВМ на профили, присутствующие в целевом кластере:
    a. Нажмите **Отображение профилей vNIC**.
    b. Выберите используемый профиль vNIC из выпадающего списка **Целевой профиль vNIC**.

c. Если в окне **Импорт ВМ** было выбрано несколько целевых кластеров, выберите каждый целевой кластер из выпадающего списка **Целевой кластер** и убедитесь в том, что отображения корректны.
d. Нажмите **OK**.

8. При обнаружении конфликта адресов MAC, рядом с именем ВМ появится восклицательный знак. Наведите курсор на восклицательный знак, чтобы просмотреть всплывающую подсказку с возникшей ошибкой. Установите флажок **Повторно присвоить неправильные MAC**, чтобы повторно присвоить конфликтующие адреса MAC всем проблемным ВМ.

   Примечание — импорт ВМ закончится неудачей в случае отсутствия доступных адресов MAC для присвоения. Тем не менее, возможен импорт ВМ без присвоения новых адресов при использовании адресов MAC, расположенных вне диапазона пула адресов MAC кластера.

9. Нажмите **OK**.

11.7.6. Импорт шаблонов из импортированных доменов данных

Импорт шаблонов из импортированного домена хранения данных может осуществляться в один или несколько целевых кластеров.

В следующей последовательности действий предполагается, что ранее импортированный домен хранения данных был присоединён к дата-центру и активирован.

Импорт шаблонов из импортированного домена данных

1. Нажмите **Хранилище → Домены**.
2. Нажмите на имя импортированного домена данных, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Импорт шаблонов**.
4. Выберите один или несколько шаблонов для импорта.
5. Нажмите **Импортировать**.
6. Убедитесь, что для каждого шаблона в окне **Импорт шаблонов** выбран корректный целевой кластер из списка **Кластер**.
7. Отобразите внешние профили vNIC на профили, присутствующие в целевом кластере:
   a. Нажмите Отображение профилей vNIC.
   b. Выберите используемый профиль vNIC из выпадающего списка **Целевой профиль vNIC**.
   c. Если в окне **Импорт шаблонов** было выбрано несколько целевых кластеров, выберите каждый целевой кластер из выпадающего списка **Целевой кластер** и убедитесь в том, что отображения корректны.
   d. Нажмите **OK**.
8. Нажмите **OK**.

11.8. Работа с доменами хранилищ

11.8.1. Размещение образов в доменах данных

Загрузить образы виртуальных дисков и образы ISO в домен хранения данных можно с помощью Портала администрирования или REST API.

Виртуальные диски, совместимые с QEMU, можно присоединять к виртуальным машинам. Диски должны иметь тип raw или QCOW2. Диски, созданные на базе виртуального диска с типом QCOW2, нельзя сделать общими, а файл виртуального диска с типом QCOW2 не должен иметь резервной копии.

Образы ISO можно присоединять к ВМ в качестве CD-дисков или использовать для загрузки ВМ.

Предварительные условия для размещение образов в доменах данных

Так как функция загрузки (отправки) образов в домен использует HTML5 API, в окружении необходимо иметь следующие компоненты:

- Прокси ввода-вывода изображений `ovirt-imageio-proxy`, настроенный с помощью `engine-setup`.

- Центр сертификации, импортированный в веб-браузер, с помощью которого осуществляется доступ на Портал администрирования.

Для импортирования центра сертификации перейдите по адресу `https://`*`адрес_диспетчера_виртуализации`*`/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA` и включите все параметры доверия.

- Браузер с поддержкой HTML5.

Размещение образа в домене хранения данных

1. Нажмите **Хранилище → Домены хранилищ → ISO → Диски** (Рис. 145).

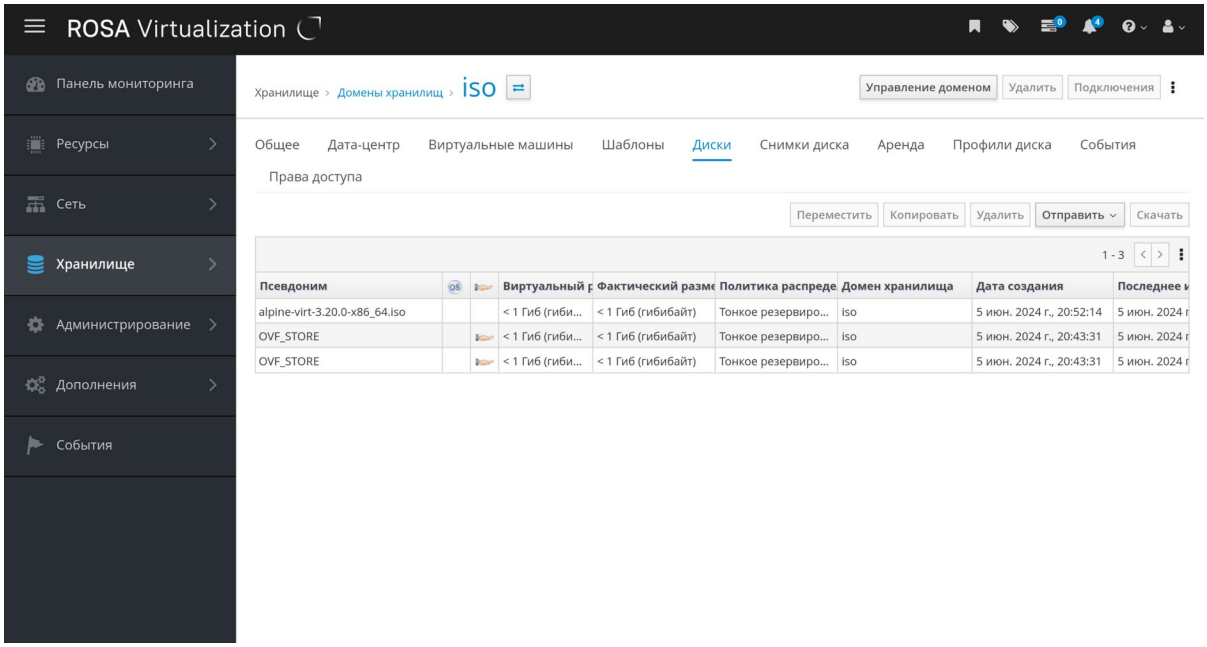

Рис. 145. Хранилище → Домены хранилищ → ISO , вкладка Диски

2. В меню **Отправить** выберите **Начать** (Рис. 146).

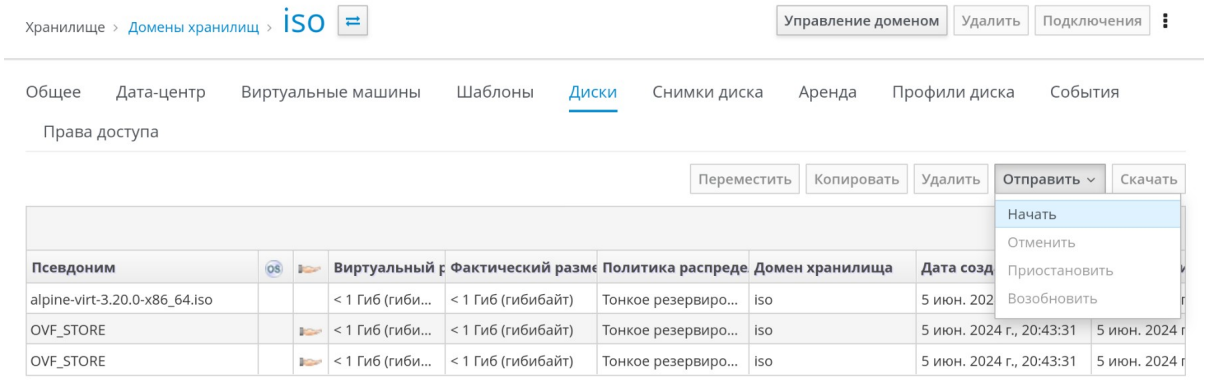

Рис. 146. Форма для отправки образа диска в хранилище

3. Нажмите **Выберите файл** и выберите образ для загрузки в домен.

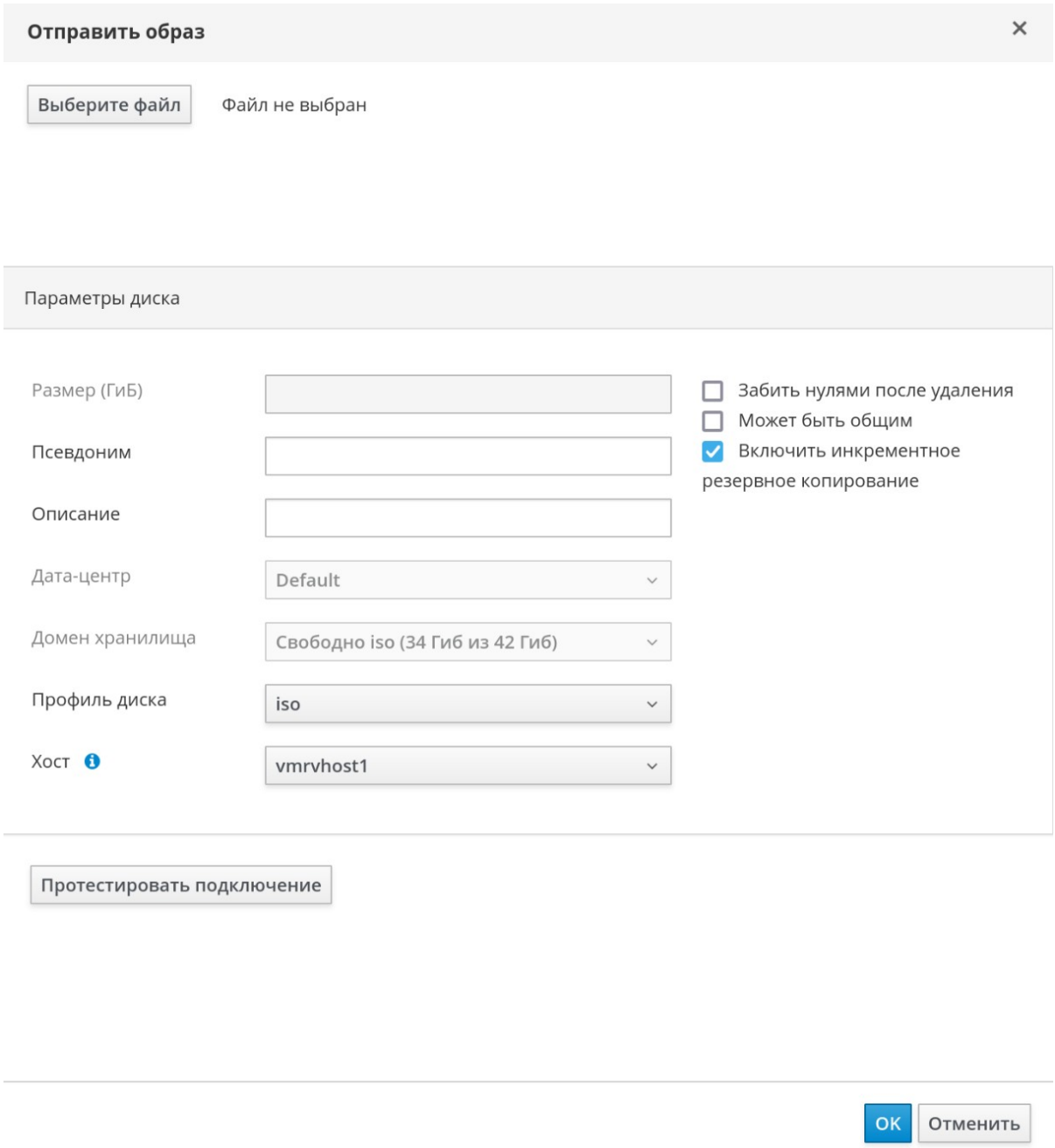

Рис. 147. Выбор файла с образом диска для отправки в домен

4. Заполните поля **Параметры диска**.
5. Нажмите **OK**.

Статус загрузки образа в домен отображается с помощью индикатора выполнения.

В меню **Отправить** можно приостановить, отменить или возобновить отправку файлов.

Увеличение значения времени ожидания отправки

1. В случае превышения времени ожидания окончания отправки и появлении соответствующего сообщения «`Причина: превышение времени ожидания в связи с неактивностью передачи`» выполните следующую команду для увеличения значения времени ожидания:

```
# engine-config -s TransferImageClientInactivityTimeoutInSeconds=6000
```

2. Перезапустите службу `ovirt-engine`:

```
# systemctl restart ovirt-engine
```

11.8.2. Перевод доменов хранилищ в режим обслуживания

Перед откреплением и удалением домена хранения обязательно переведите этот домен в режим обслуживания. Это необходимо для присвоения другому домену данных роли домена мастер-данных.

Примечание — домен хранения нельзя переместить в режим обслуживания, если у ВМ имеется аренда в этом домене. ВМ сначала необходимо выключить, удалить аренду или переместить аренду в другой домен хранения.

Расширение доменов iSCSI с помощью добавления дополнительных LUN можно выполнять только при активном домене.

Перевод домена хранения в режим обслуживания

1. Выключите все ВМ, выполняющиеся в домене хранения.
2. Нажмите **Хранилище → Домены**.
3. Нажмите на имя домена, чтобы перейти к подробному просмотру.
4. Перейдите на вкладку **Дата-центр**.
5. Нажмите **Обслуживание**.

Примечание — опционально установите флажок **Игнорировать сбой обновления OVF** для перемещения домена хранения в режим обслуживания даже при сбое обновления OVF.

6. Нажмите **OK**.

В результате домен хранения деактивируется и в списке результатов получает статус «*Неактивен*».

Неактивные домены хранения можно изменять, отключать, удалять или активировать повторно в дата-центре.

Примечание — активировать, отсоединять и помещать домены в режим обслуживания можно также во вкладке **Хранилище** в подробном просмотре дата-центра, к которому присоединены эти домены.

11.8.3. Изменение параметров доменов хранилищ

Параметры доменов хранилищ можно изменить на Портале администрирования. При этом параметры **Дата-центр**, **Функция домена**, **Тип хранилища** и **Формат** изменить нельзя.

Параметры, доступные для изменения, зависят от статуса домена хранения («*Активен*» или «*Неактивен*»):

- **Активен**.

Для домена с активным статусом можно изменить значение следующих полей: Имя, Описание, Комментарий, Индикатор предупреждения о недостатке места (%), Блокировщик действия при критической нехватке места, Забить нулями после удаления и Освободить блоки перед удалением.

Поле **Имя** можно изменить только для активного домена хранения. Другие поля также можно изменить при неактивном домене.

- **Неактивен**.

Для неактивного домена, то есть находящегося в режиме обслуживания или не присоединённого, можно изменить значения всех полей, за исключением полей **Имя**, **Дата-центр**, **Функция домена**, **Тип хранилища** и **Формат**.

Изменить параметры сетевых соединений, параметры монтирования, а также другие дополнительные параметры можно только для неактивного домена. Эти параметры поддерживаются только для типов доменов NFS, POSIX и локальных.

Примечание — сетевые соединения хранилищ iSCSI нельзя редактировать на Портале администрирования, но можно редактировать с помощью REST API.

Изменение параметров активного домена хранения

1. Нажмите **Хранилище → Домены** и выберите домен хранения.
2. Нажмите **Управление доменом**.
3. При необходимости измените значения доступных полей.
4. Нажмите **ОК**.

Изменение параметров неактивного домена хранения

1. Нажмите **Хранилище → Домены**.
2. Если домен хранения активен, переместите домен в режим обслуживания:
    a. Нажмите на имя домена, чтобы перейти к подробному просмотру.
    b. Перейдите на вкладку **Дата-центр**.
    c. Нажмите **Обслуживание**.
    d. Нажмите **ОК**.
3. Нажмите **Управление доменом**.
4. Измените путь к хранилищу и другие необходимые сведения. Сведения о новых сетевых соединениях должны иметь тот же тип хранилища, что и исходное соединение.
5. Нажмите **ОК**.
6. Активируйте домен хранения:
    a. Нажмите на имя домена хранения, чтобы перейти к подробному просмотру.
    b. Перейдите на вкладку **Дата-центр**.

c. Нажмите **Активировать**.

11.8.4. Обновление файлов OVF

По умолчанию файлы OVF обновляются каждые 60 минут.

Также файлы OVF можно обновить вручную (например, после импорта ВМ или критически важного обновления ПО).

Обновление файлов OVF

1. Нажмите **Хранилище → Домены**.
2. Выберите домен хранения, нажмите **Больше действий** (⋮) и далее нажмите **Обновить файлы OVF**.

11.8.5. Активация доменов хранилищ из режима обслуживания

Если ранее домен хранения был переведен в режим обслуживания, то для возобновления использования необходимо активировать этот домен из режима обслуживания.

Активация домена хранения из режима обслуживания

1. Нажмите **Хранилище → Домены**.
2. Нажмите на имя неактивного домена, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Дата-центры**.
4. Нажмите **Активировать**.

Примечание — при попытке активации домена ISO до активации домена данных будет показано соответствующее сообщение об ошибке и домен ISO не будет активирован.

11.8.6. Отсоединение домена хранения от дата-центра

Отсоедините домен хранения от одного дата-центра, чтобы выполнить миграцию домена в другой дата-центр.

Отсоединение домена хранения от дата-центра

1. Нажмите **Хранилище → Домены**.
2. Нажмите на имя домена, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Дата-центр**.
4. Нажмите **Обслуживание**.
5. Нажмите **ОК** для инициации режима обслуживания.
6. Нажмите **Отсоединить**.
7. Нажмите **ОК**, чтобы отсоединить домен хранения.

В результате домен хранения будет отсоединён от текущего дата-центра и готов для присоединения к другому дата-центру.

11.8.7. Присоединение домена хранения к дата-центру

Присоединение домена хранения к дата-центру

1. Нажмите **Хранилище → Домены.**
2. Нажмите на имя домена, чтобы перейти к подробному просмотру.

3. Перейдите на вкладку **Дата-центр**.
4. Нажмите **Присоединить**.
5. Выберите необходимый дата-центр.
6. Нажмите **OK**.

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

11.8.8. Удаление домена хранения

Удаление домена хранения

1. Нажмите **Хранилище → Домены**.
2. Переместите домен хранения в режим обслуживания и отсоедините домен:
    a. Нажмите на имя домена, чтобы перейти к подробному просмотру.
    b. Перейдите на вкладку **Дата-центр**.
    c. Нажмите **Обслуживание** и далее нажмите **OK**.
    d. Нажмите **Отсоединить** и далее нажмите **OK**.
3. Нажмите **Удалить**.
4. Опционально установите флажок **Форматировать домен,** *т.е. содержимое хранилища будет потеряно*, чтобы окончательно стереть всё содержимое домена.
5. Нажмите **OK**.

11.8.9. Разрушение домена хранения

Домен хранения, содержащий ошибки, не всегда возможно удалить посредством стандартной процедуры. Разрушение домена хранения принудительно удаляет домен из окружения.

Разрушение домена хранения

1. Нажмите **Хранилище → Домены**.
2. Выберите домен хранилища, нажмите **Больше действий** (⋮) и далее нажмите **Разрушить**.
3. Установите флажок **Одобрить операцию**.
4. Нажмите **OK**.

11.8.10. Создание профилей дисков

Профили дисков определяют максимальные уровни пропускной способности и операций ввода-вывода виртуальных дисков в домене хранения.

Профили дисков создаются на базе профилей хранилищ, настроенных в дата-центрах.

Профили дисков назначаются вручную каждому виртуальному диску.

В следующей последовательности действий подразумевается, что ранее в дата-центре, к которому принадлежит домен хранения, была настроена одна или несколько записей о качестве обслуживания хранилищ.

Создание профиля диска

1. Нажмите **Хранилище → Домены**.
2. Нажмите на имя домена, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Профили диска**.
4. Нажмите **Добавить**.
5. Введите **Имя** и **Описание** профиля диска.
6. В списке **QoS** выберите запись о качестве обслуживания, которую нужно применить к профилю диска.
7. Нажмите **OK**.

11.8.11. Удаление профилей дисков

Удаление профиля диска

1. Нажмите **Хранилище → Домены**.
2. Нажмите на имя домена, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Профили диска**.
4. Выберите удаляемый профиль диска.
5. Нажмите **Удалить**.
6. Нажмите **OK**.

11.8.12. Просмотр состояния работоспособности доменов хранилищ

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

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

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

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

Примечание — внешний статус работоспособности домена также можно узнать с помощью REST API (элемент `external_status` в запросе `GET`). Для указания статуса работоспособности домена через REST API используйте набор `events`.

11.8.13. Параметр «Освободить блоки перед удалением»

Если параметр **Освободить блоки перед удалением** включен, при удалении логического тома вызывается команда `blkdiscard` и базовое хранилище оповещается о том, что блоки свободны. Далее массив хранилища может использовать (выделять по запросу) освобождённое пространство.

Параметр **Освободить блоки перед удалением** эффективен и доступен только для доменов блочных хранилищ, таких как iSCSI или FCP (хранилище должно поддерживать `Discard`). Для файловых хранилищ, таких как NFS, этот параметр недоступен.

Параметр **Освободить блоки перед удалением** можно включить как при создании домена блочного хранилища iSCSI или FCP, так и при изменении параметров этого домена.

Глава 12. Пулы

12.1. Пул виртуальных машин

Пул виртуальных машин — это группа ВМ, являющихся клонами одного и того же шаблона, которые могут использоваться по требованию любым пользователем в указанной группе. Пулы ВМ дают администраторам возможность быстро настроить набор стандартных ВМ для пользователей.

Пользователи при осуществлении доступа к пулу ВМ получают для своей работы ВМ из пула. Когда пользователи забирают ВМ из пула, они получают любую ВМ, если хотя бы одна машина в пуле является доступной. ОС и конфигурация ВМ, получаемой пользователем из пула, аналогичны ОС и конфигурации шаблона, на базе которого был создан пул, но каждый раз забирая машину из пула, пользователь не получает одного и того же участника пула. Также пользователи могут получить несколько ВМ из одного и того же пула, в зависимости от параметров пула.

По умолчанию пулы ВМ не сохраняют состояние, соответственно изменения в данных и конфигурации ВМ не сохраняются после перезагрузки. Тем не менее, можно создать конфигурацию пула с фиксацией состояния, то есть с сохранением изменений, внесённых предыдущим пользователем. Но если на ВМ, взятой из пула, пользователь настроит свои консольные параметры, то эти параметры станут параметрами по умолчанию для этого пользователя в данном пуле ВМ.

Примечание — при доступе с Портала администрирования к ВМ, взятым из пула, эти ВМ сохраняют состояние, так как у администраторов должна быть возможность при необходимости записать изменения на диск.

Таким образом, ВМ в пуле начинают работу тогда, когда их получают пользователи, и выключаются, когда пользователи завершают работу с машиной. Тем не менее, в пуле могут присутствовать предварительно запущенные ВМ, которые не выключаются и простаивают до того момента, пока их не заберёт пользователь. Такая настройка даёт пользователям возможность немедленно начать работу с машиной, но такие ВМ потребляют системные ресурсы не только во время работы, но и во время простоя.

12.1.1. Инфраструктура виртуальных рабочих столов (VDI)

Предоставление инфраструктуры VDI означает предоставление возможности использовать стандартизированный рабочий стол (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 ROSA Virtualization вы создаете 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.

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 руководстве «Портал виртуальных машин. Руководство пользователя» (РСЮК.10102-01 93 01).

12.2. 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`.

Параметры конфигурационного файла `sysprep` для ВМ под управлением ОС Windows

Если пулу не нужно присоединяться к домену, используйте файл `sysprep` со значениями по умолчанию, расположенный в `/usr/share/ovirt-engine/conf/sysprep/`.

Если пул должен присоединиться к домену, то для каждой из ОС Windows рекомендуется создать частный файл `sysprep` следующим образом:

1. Скопируйте разделы, имеющие отношение к каждой ОС Windows, из `/usr/share/ovirt-engine/conf/osinfo-defaults.properties` в новый файл, и сохраните его как `99-defaults.properties`.

2. В файле `99-defaults.properties` укажите ключ активации ОС Windows и путь до частного файла `sysprep`:

```
        os.operating_system.productKey.value=Windows_product_activation_key
        ...
        os.operating_system.sysprepPath.value = ${ENGINE_USR}/conf/sysprep/
    sysprep.operating_system
```

3. Создайте новый файл `sysprep`, где укажите домен, пароль домена и администратора домена:

```
<Credentials>
    <Domain>Домен_AD</Domain>
    <Password>Пароль_домена</Password>
    <Username>Администратор_домена</Username>
</Credentials>
```

Примечание — при необходимости создания различных параметров `sysprep` для разных пулов ВМ под управлением ОС Windows рекомендуется создать частный файл `sysprep` на Портале администрирования.

Создание пула ВМ

1. Нажмите **Ресурсы → Пулы**.
2. Нажмите **Добавить**, чтобы открыть окно **Новый пул**.

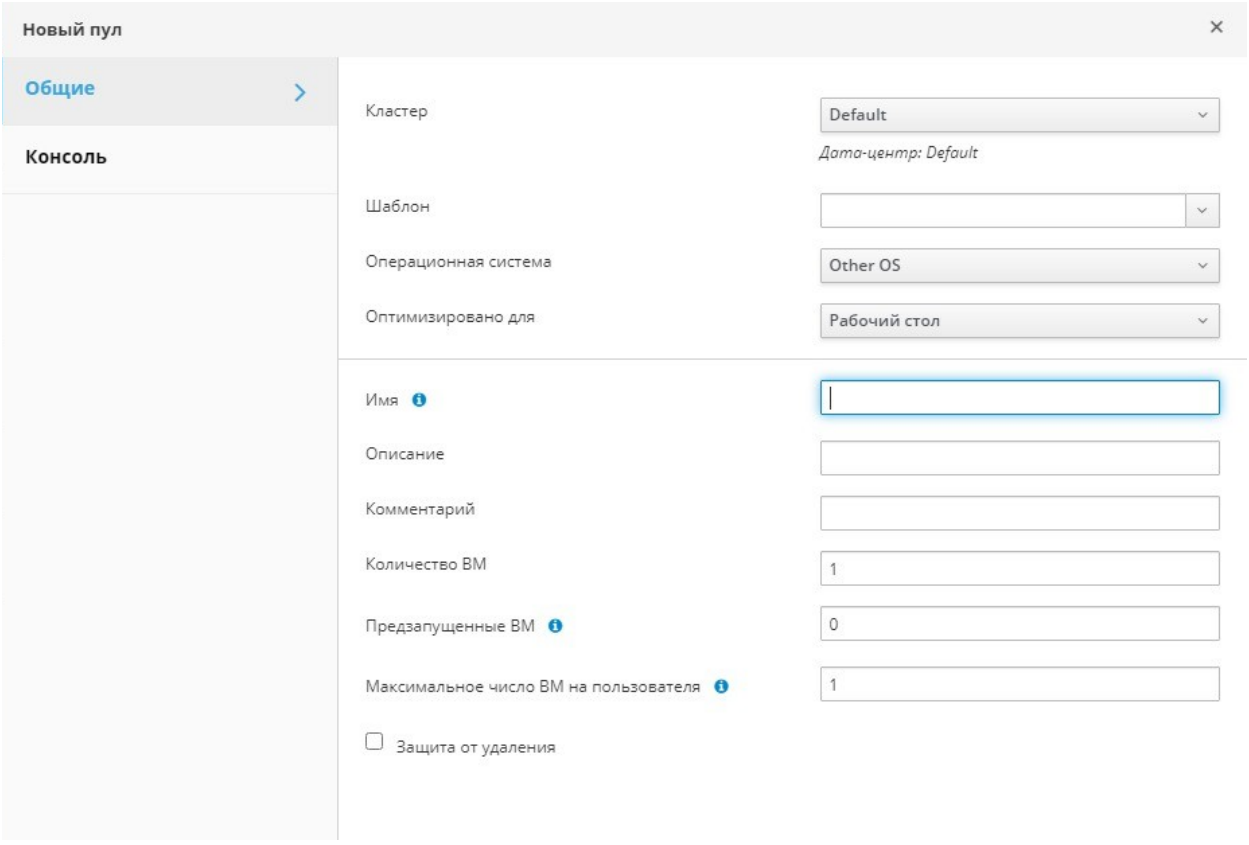

Рис. 148. Создание пула ВМ

3. Из выпадающего списка выберите **Кластер**.
4. Из выпадающего списка выберите **Шаблон** и версию. Шаблон предоставляет стандартные значения параметров для всех ВМ в пуле.

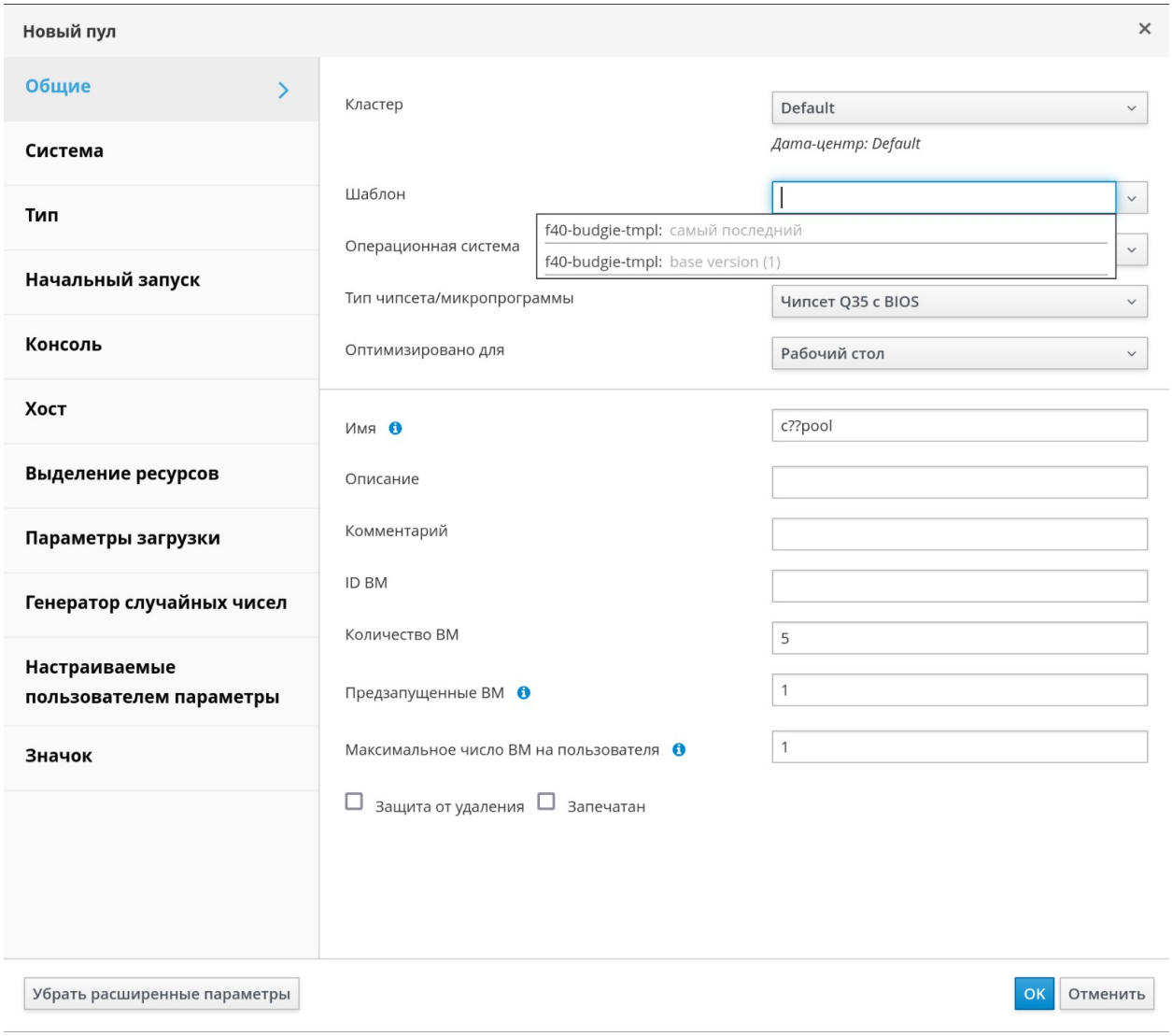

Рис. 149 - Выбор шаблона ВМ и версии шаблона ВМ для создания пула

Примечание — если в системе отсутствует предварительно созданный шаблон, то его необходимо создать. Это можно сделать в секции **Ресурсы → Шаблоны**.

5. Из выпадающего списка выберите **Операционную систему**.
6. Из выпадающего списка выберите **Тип чипсета/микропрограмму**.
7. Используя значения из выпадающего списка **Оптимизировано для** оптимизируйте виртуальные машины для **Рабочего стола** или **Сервера**.

   Примечание — оптимизация **Высокая производительность** не рекомендуется для пулов, поскольку высокопроизводительная ВМ прикрепляется к одному хосту и к конкретным ресурсам. Пул, содержащий несколько таких ВМ, не будет работать эффективно.

8. Укажите **Имя** для пула и опционально **Описание** и **Комментарий**.

Примечание — имя пула с числовым суффиксом применяется к каждой ВМ в пуле (например, имени пула `MyPool` соответствует следующая нумерация виртуальных машин `MyPool-1`, `MyPool-2`, … `MyPool-10`). Настроить нумерацию ВМ можно с использованием символа **?** (вопросительный знак) в качестве метки-заполнителя (например, имени пула `MyPool-???` соответствует следующая нумерация виртуальных машин: `MyPool-001`, `MyPool-002`, … `MyPool-010`).

9. Укажите **Количество ВМ** для пула.
10. Укажите количество ВМ с предварительным запуском в поле **Предзапущенные ВМ**.
11. Укажите **Максимальное число ВМ на пользователя**, которое разрешено запускать одному пользователю в течение сеанса. Минимальное значение — 1 (одна виртуальная машина на одного пользователя).
12. Опционально установите флажок **Защита от удаления**.
13. Если создаётся пул ВМ не под управлением ОС Windows, или используется исходный файл `sysprep`, то перейдите к следующему шагу.

Создания частного файла `sysprep` для пула ВМ

В случае создания частного файла `sysprep` для пула ВМ под управлением ОС Windows выполните следующие действия:

- Нажмите на кнопку **Показать дополнительные параметры**.
- Перейдите на вкладку **Начальный запуск** и установите флажок **Cloud-Init/Sysprep**.
- Нажмите **Аутентификация** и введите **Имя пользователя** и **Пароль**, или выберите **Использовать уже настроенный пароль**.

Примечание — значение в поле **Имя пользователя** является пользовательским именем локального администратора. Изменить значение по умолчанию (`user`) можно или в разделе **Аутентификация** или в частном файле `sysprep`.

- Нажмите **Настраиваемый пользователем сценарий** и вставьте в текстовый блок содержимое исходного файла `sysprep`, расположенного по следующему пути `/usr/share/ovirt-engine/conf/sysprep/`.
- При необходимости измените значения следующих параметров конфигурационного файла `sysprep` (обратите внимание, что значения этих параметров нельзя изменить во вкладке **Начальный запуск**):

  – `Key` (ключ активации).

Если предварительно настроенный ключ активации ОС Windows не будет использоваться, то замените `<![CDATA[$ProductKey$]]>` на действительный ключ:

```
<ProductKey>
    <Key><![CDATA[$ProductKey$]]></Key>
</ProductKey>
```

- `Domain` (домен, к которому присоединяется ВМ под управлением ОС Windows), `Password` (пароль домена) и `Username` (имя администратора):

```
<Credentials>
    <Domain>Домен_AD</Domain>
    <Password>Пароль_домена</Password>
    <Username>Администратор_домена</Username>
</Credentials>
```

- `FullName` (полное имя локального администратора):

```
<UserData>
…
    <FullName>локальный_администратор</FullName>
…
</UserData>
```

- `DisplayName` и `Name` (имя локального администратора):

```
<LocalAccounts>
    <LocalAccount wcm:action="add">
        <Password>
            <Value><![CDATA[$AdminPassword$]]></Value>
            <PlainText>true</PlainText>
        </Password>
        <DisplayName>Local_Administrator</DisplayName>
        <Group>administrators</Group>
        <Name>Local_Administrator</Name>
    </LocalAccount>
</LocalAccounts>
```

- При необходимости значения других параметров конфигурационного файла `sysprep` заполните во вкладке **Начальный запуск**.

14. Опционально укажите **Тип пула**:

- Перейдите на вкладку **Тип** и выберите **Тип пула**:

  - **Вручную**.
    Возвращение ВМ в пул осуществляется вручную администратором.
  - **Автоматически**.

Возвращение ВМ в пул осуществляется автоматически.

- Установите флажок **Пул с сохранением состояния**, чтобы ВМ запускались в режиме с сохранением состояния. Это обеспечивает сохранение в ВМ изменений, внесённых предыдущим пользователем.
- Нажмите **ОК**.

15. При необходимости переопределите прокси SPICE:

    - Во вкладке **Консоль** установите флажок **Переопределить SPICE прокси**.
    - В поле **Переназначенный адрес прокси SPICE** укажите адрес прокси SPICE, который заменит глобальный прокси.
    - Нажмите **ОК**.

16. Если пул состоит из ВМ под управлением ОС Windows, то нажмите **Ресурсы → Виртуальные машины**, далее выберите каждую ВМ и нажмите **Запустить → Однократный запуск.**

Примечание — если ВМ не запускается, а в файле журнала `%WINDIR%\panther\UnattendGC\setupact.log` появляется запись `Info [windeploy.exe] Found no unattend file`, то в реестр ВМ под управлением ОС Windows, на базе которой создавался шаблон для пула, необходимо добавить ключ `UnattendFile` следующим образом:

- Проверьте, не присоединено ли к ВМ под управлением ОС Windows устройство флоппи-дискеты с файлом `Unattend` (например, `A:\Unattend.xml`).
- В панели задач ОС Windows нажмите **Пуск**, затем **Выполнить**, далее в текстовый блок **Открыть** введите `regedit` и нажмите **ОК**.
- В левой панели реестра выберите пункт меню **HKEY_LOCAL_MACHINE → SYSTEM → Setup**.
- Сделайте щелчок правой кнопкой мыши в правой панели реестра и из контекстного меню выберите **Создать → Строковой параметр**.
- Укажите имя ключа **UnattendFile**.
- Сделайте двойной щелчок по новому ключу и в качестве значения ключа введите имя файла `Unattend` и путь к этому файлу (например, `A:\Unattend.xml`).
- Сохраните изменения в реестре, сохраните состояние ВМ и создайте новый шаблон.

В результате будет создан пул виртуальных машин с указанным числом одинаковых ВМ.

Для просмотра ВМ из пула используйте меню **Ресурсы → Виртуальные машины** или нажмите на имя пула, чтобы перейти к подробному просмотру (при отображении виртуальные машины из пула отличаются от независимых ВМ своим значком).

12.3. Параметры и элементы управления пулами

12.3.1. Общие параметры в окнах «Новый пул» и «Параметры пула»

В Табл. 12.1 описываются параметры пула во вкладке **Общие** окон **Новый пул** и **Параметры пула**.

Все другие параметры идентичны параметрам окна **Новая ВМ**.

Табл. 12.1. Общие параметры

Поле	Описание
Шаблон	Шаблон и версия шаблона, на которых основан пул машин. Если создать пул на основе версии шаблона `latest`, то все ВМ в пуле при перезагрузке автоматически получат последнюю версию шаблона
Описание	Описание пула ВМ
Комментарий	Поле для добавления комментария для пула ВМ, в простом текстовом формате
Предварительно запущенные ВМ	Параметр даёт возможность указать число тех ВМ в пуле, которые будут предварительно запущены перед размещением в пуле и будут забираться пользователями уже работающими. Значение параметра должно быть между `0` и общим числом ВМ в пуле
Количество ВМ / Увеличить число ВМ в пуле на	Параметр даёт возможность указать конкретное количество ВМ, которые нужно создать и сделать доступными в пуле. По умолчанию максимальное число ВМ, создаваемых в пуле — 1000. Это значение можно настроить с помощью ключа `MaxVmsInPool` команды `engine-config`
Максимальное число ВМ на пользователя	Параметр даёт возможность указать максимальное число ВМ, доступных пользователю в пуле в любое время. Значение параметра должно быть в диапазоне от `1` до `32 767`
Защита от удаления	Параметр защищает ВМ в пуле от удаления

12.3.2. Параметры вкладки «Тип» в окнах «Новый пул» и «Изменить пул»

В **Табл. 12.2** описываются параметры пула во вкладке **Тип** окон **Новый пул** и **Изменить пул**.

Табл. 12.2. Параметры типа

Поле	Описание
Тип пула	В этом выпадающем меню можно указать тип пула ВМ. Доступны следующие значения: • **Автоматически**. После того, как пользователь закончит работу с ВМ, взятой из пула, ВМ автоматически возвращается в пул. • **Вручную**. После того, как пользователь закончит работу с ВМ, взятой из пула, ВМ возвращается в пул только вручную администратором.
Пул с сохранением состояния	Параметр позволяет указать, будет ли сохраняться состояние ВМ в пуле после того, как ВМ будет передана другому пользователю. Это означает, что изменения, внесённые предыдущим пользователем, сохранятся в ВМ

12.3.3. Параметры вкладки «Консоль» в окнах «Новый пул» и «Изменить пул»

В Табл. 12.3 описываются параметры пула во вкладке Консоль окон Новый пул и Изменить пул.

Все другие параметры идентичны параметрам окна **Новая ВМ** и **Параметры виртуальной машины**.

Табл. 12.3. Параметры консоли

Поле	Описание
Переназначить SPICE прокси	Установите флажок для этого пункта, чтобы включить переопределение прокси SPICE, указанного в глобальной конфигурации. Используйте эту возможность, если пользователь находится вне той сети, в которой располагаются хосты (например, пользователь подключается через портал ВМ)
Переназначенный адрес SPICE прокси	Прокси, с помощью которого клиент SPICE подключается к виртуальным машинам. Значение этого прокси переопределяет как глобальное значение прокси SPICE, настроенное для окружения виртуализации, так и значение, настроенное для кластера, которому принадлежит пул ВМ, если такой кластер существует. Адрес должен соответствовать следующему формату: протокол://*хост*:*порт*

12.3.4. Параметры вкладки «Хост» в окнах «Новый пул» и «Параметры пула»

В Табл. 12.4 описываются параметры пула во вкладке Хост окон Новый пул и Параметры пула.

Табл. 12.4. Параметры хоста

Поле	Вложенный элемент	Описание
Начать выполнение на:		Параметр позволяет указать предпочитаемый хост, на котором должна выполняться ВМ. Доступны следующие значения: • **Любой хост в кластере.** ВМ может запускаться и выполняться на любом доступном хосте в кластере. • **Конкретный хост.** ВМ начинает работу на конкретном указанном хосте в кластере, но виртуализированный ЦУ или администратор могут выполнить миграцию ВМ на другой хост в кластере в зависимости от параметров миграции и параметров высокой доступности ВМ. Выберите хост или группу хостов из списка доступных хостов.
Параметры миграции	**Режим миграции**	Параметр режима миграции ВМ может принимать следующие значения (если следующие значения не используются, ВМ будет мигрировать в соответствии с политикой кластера): • **Разрешить ручную и автоматическую миграции.** ВМ может мигрировать с одного хоста на другой автоматически, согласно статусу окружения, или может быть перенесена администратором вручную. • **Разрешить только ручную миграцию.** Миграция ВМ с одного хоста на другой может выполняться только вручную администратором. • **Не разрешать миграцию.** Миграция ВМ (ручная или автоматическая) запрещена.
	Политика миграции	По умолчанию политика миграции определяется на уровне кластера. Для переопределения параметра (на уровне хоста) доступны следующие значения: • **Минимальное время простоя.**

Поле	Вложенный элемент	Описание
		Разрешается миграция ВМ в типичных ситуациях с незначительным временем простоя. Миграция будет прервана, если после долгого времени не будет достигнуто состояние целостности (зависит от итераций QEMU, максимальный интервал — 500 миллисекунд). Механизм перехватчиков событий гостевого агента включён. • В случае необходимости приостановить рабочую нагрузку. Разрешается миграция ВМ в большинстве ситуаций, включая те, когда ВМ испытывает серьёзную нагрузку. В связи с этим разрешается более значительный простой ВМ, чем при других значениях данного параметра. Миграция всё ещё может быть прервана при экстремальных нагрузках. Механизм перехватчиков событий гостевого агента включён.
	Включить шифрование при миграции	Параметр даёт возможность указать, будет ли использоваться шифрование во время динамических миграций ВМ. По умолчанию шифрование во время миграции ВМ отключено на уровне кластера. Параметр может принимать следующие значения: • Значение по умолчанию. Используется значение **Зашифровать** или **Не шифровать** (по умолчанию), настроенное на уровне кластера. • **Зашифровать.** Значение переопределяет настройку на уровне кластера и включает шифрование при миграции ВМ. • **Не шифровать.** Значение переопределяет настройку на уровне кластера и отключает шифрование при миграции ВМ.
Параметры ЦП	**Сквозной доступ к ЦП хоста**	Этот флажок даёт возможность ВМ использовать преимущества физического ЦП хоста, на котором ВМ размещены
	Идентичная частота TSC	Этот флажок разрешает миграцию ВМ только на хосты с такой же частотой

Поле	Вложенный элемент	Описание
		счётчика метки времени
Параметры NUMA	Число узлов NUMA	Число виртуальных узлов NUMA, присваиваемых ВМ. При **Предпочитаемом** значении параметра **Режим настройки** (см. строку ниже), это число должно быть равно 1
	Режим настройки	Метод выделения памяти. Для параметра доступны следующие значения: • Строгий. Выделение памяти закончится неудачей, если на целевом узле память выделить нельзя. • Предпочитаемый. Память выделяется из исходного предпочитаемого узла. Если достаточный объём памяти недоступен, память можно выделить из других узлов. • Чередование. Память выделяется из всех узлов в алгоритме кругового обслуживания.
	Привязка NUMA	Привязка NUMA осуществляется в окне **Топология NUMA**, в котором отображается общее число ЦП хоста, памяти и узлов NUMA, а также виртуальные узлы NUMA ВМ. Привяжите виртуальные узлы NUMA для размещения узлов NUMA. Для этого нажмите и перетащите каждый виртуальный узел NUMA из блока справа на узел NUMA в блок слева. При настроенной привязке NUMA, для параметра **Режим миграции** будет доступно единственное значение **Разрешить только ручную миграцию**

12.3.5. Параметры вкладки «Выделение ресурсов»

Рассмотрим параметры вкладки «Выделение ресурсов» в окнах «Новый пул» и «Изменить пул».

В Табл. 12.5 описываются параметры пула во вкладке Выделение ресурсов окон Новый пул и Изменить пул.

Все другие параметры идентичны параметрам окна **Новая ВМ**.

Табл. 12.5. Параметры выделения ресурсов

Поле	Вложенный элемент	Описание
Выделение дисковых ресурсов	Автоматический выбор цели	Установите этот флажок, чтобы домен хранилища с наибольшим объёмом свободного места выбирался автоматически. При этом поля **Цель** и **Профиль диска** будут неактивными
	Формат	Поле доступно только для чтения и всегда показывает значение **QCOW2**, за исключением случаев, когда домен имеет тип OpenStack Volume (Cinder). В этих случаях формат будет **raw**

12.4. Изменение параметров пула виртуальных машин

После создания пула ВМ можно изменить параметры пула.

Параметры, доступные при изменении свойств пула ВМ, идентичны параметрам, доступным при создании нового пула ВМ, за исключением того, что параметр **Число ВМ** заменяется параметром **Увеличить число ВМ в пуле на**…

Примечание — при изменении параметров пула ВМ, вносимые изменения влияют только на новые ВМ. При этом ВМ, существующие на момент внесения изменений, останутся незатронутыми.

Изменение параметров пула ВМ

1. Нажмите **Ресурсы → Пулы** и выберите пул ВМ.
2. Нажмите **Изменить**.
3. Измените свойства пула ВМ.
4. Нажмите **ОК**.

12.5. Предварительный запуск виртуальных машин в пуле

По умолчанию виртуальные машины в пуле ВМ выключены. Когда пользователь запрашивает машину из пула, машина запускается и присваивается пользователю. И наоборот, предварительно запущенная ВМ уже работает и ждёт присвоения пользователю, что снижает время ожидания начала работы. После выключения предварительно запущенной ВМ, машина возвращается в пул и восстанавливается до исходного состояния.

Предварительно запущенные ВМ подходят для окружений, в которых пользователям нужен немедленный доступ к машинам, не выделенным специально для этого пользователя. Предварительно запущенные ВМ могут находиться только в автоматических пулах.

Примечание — Максимальное число предварительно запущенных ВМ равно числу ВМ в пуле.

Предварительный запуск ВМ в пуле

1. Нажмите **Ресурсы → Пулы** и выберите пул ВМ.
2. Нажмите **Изменить**.
3. В поле **Предзапущенные ВМ** укажите число ВМ, которые необходимо предварительно запустить.
4. Перейдите на вкладку **Тип**. Убедитесь в том, что значение **Тип пула** указано как **Автоматически**.
5. Нажмите **OK**.

12.6. Добавление виртуальных машин в пул ВМ

Добавление виртуальных машин в пул ВМ

1. Нажмите **Ресурсы → Пулы** и выберите пул ВМ.
2. Нажмите **Изменить**.
3. В поле **Увеличить число ВМ в пуле на …** укажите число дополнительных ВМ.

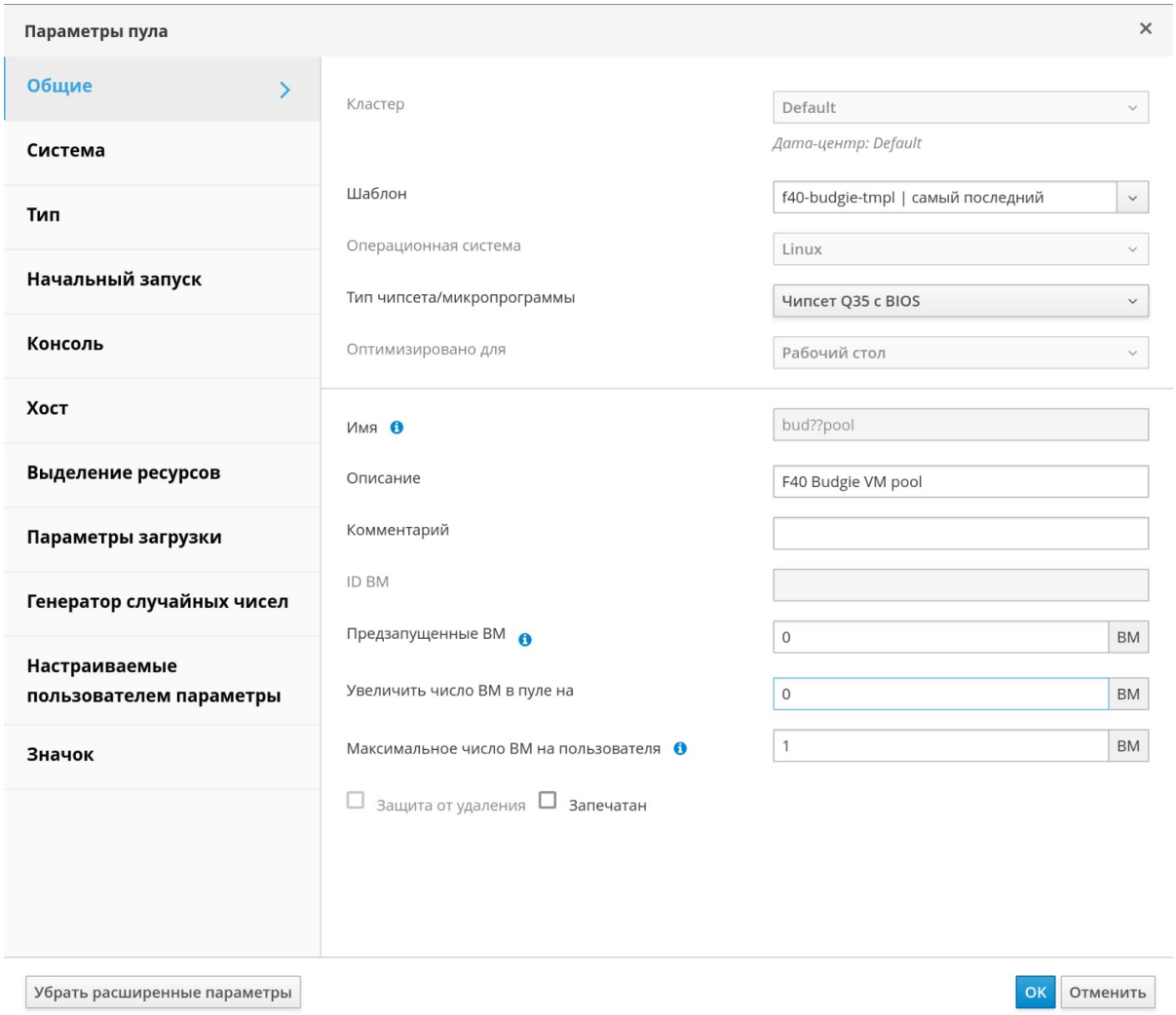

Рис. 150: Добавление виртуальных машин в пул ВМ

4. Нажмите **OK**.

12.7. Открепление виртуальных машин от пула ВМ

Виртуальные машины можно откреплять от пула ВМ. Открепление машины удаляет ВМ из пула, и машина становится независимой ВМ.

Открепление виртуальных машин от пула ВМ

1. Нажмите **Ресурсы → Пулы**.
2. Нажмите на имя пула, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Виртуальные машины**, чтобы просмотреть список ВМ в пуле.
4. Убедитесь в том, что машина имеет статус «*Не запущена*», так как работающую ВМ открепить нельзя.
5. Выберите одну или несколько ВМ и нажмите **Отсоединить**.

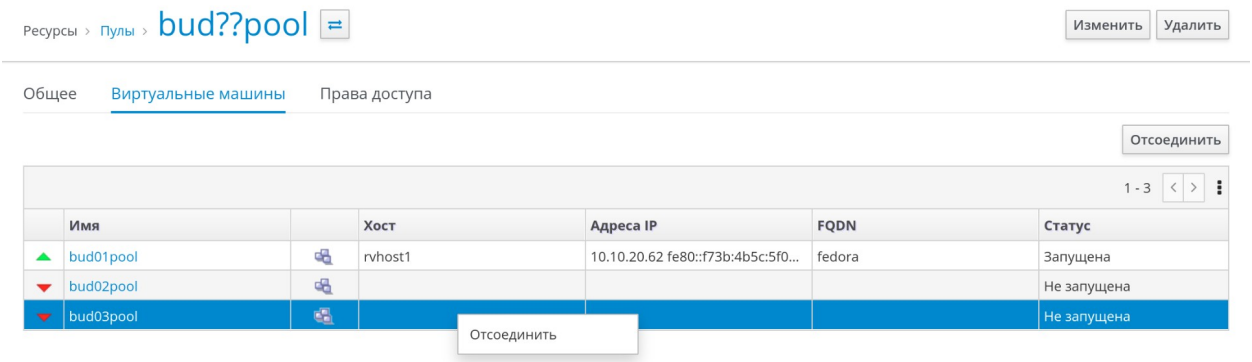

Рис. 151 - Открепление виртуальных машин от пула ВМ

6. Нажмите **ОК**.

Примечание — открепленная виртуальная машина по-прежнему существует в окружении, и к такой ВМ можно получить доступ из меню **Ресурсы → Виртуальные машины**. Обратите внимание, что значок ВМ изменится, для обозначения того, что откреплённая от пула ВМ машина стала независимой.

12.8. Удаление пула виртуальных машин

Пул ВМ можно удалить из дата-центра. Сначала необходимо удалить или открепить все ВМ из пула ВМ. При этом открепление ВМ от пула ВМ сохранит виртуальные машины в качестве независимых ВМ.

Удаление пула ВМ

1. Нажмите **Ресурсы → Пулы** и выберите пул ВМ.
2. Нажмите **Удалить**.

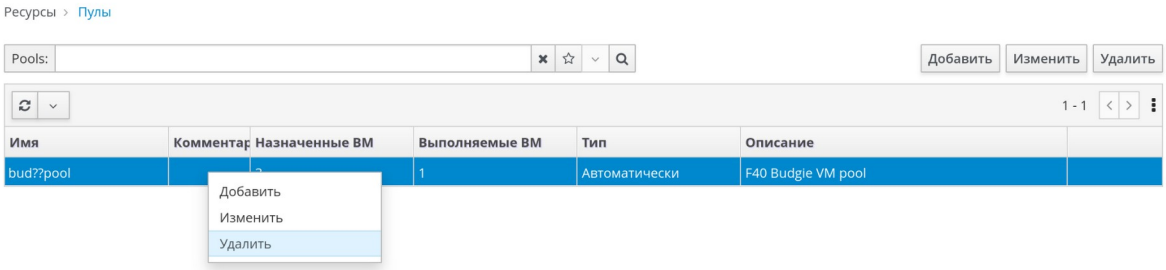

Рис. 152 - Удаление пула ВМ

3. Нажмите **ОК**.

Глава 13. Виртуальные диски

13.1. Хранилище виртуальной машины

Система виртуализации ROSA Virtualization поддерживает следующие типы хранилищ — NFS, iSCSI и FCP.

Вне зависимости от типа хранилища в системе существует хост, который называется диспетчером пула хранилищ (SPM) и управляет связью между хостами и хранилищем. Хост SPM является единственным узлом с полным доступом в рамках пула хранилищ и может изменять метаданные домена хранилищ, а также метаданные пула. Все другие хосты имеют доступ только к данным, содержащимся в образе жёсткого диска ВМ.

По умолчанию в дата-центрах на базе NFS, локальных или совместимых с POSIX, хост SPM создаёт виртуальные диски с помощью формата тонкого резервирования в виде файла в файловой системе.

В дата-центрах на базе iSCSI и в других блочных дата-центрах, таких как FCP, хост SPM создаёт группу томов поверх предоставленных номеров LUN, а логические тома используются как виртуальные диски. По умолчанию виртуальные диски в блочных хранилищах являются предварительно зарезервированными.

Для предварительно зарезервированного виртуального диска («*толстого*» диска) создаётся логический том указанного размера в Гбайт.

Для виртуального диска тонкого резервирования создаётся логический том с начальным размером в 1 Гбайт. За логическим томом ведётся постоянное наблюдение со стороны хоста, на котором выполняется ВМ. Как только используемый объём приближается к пороговому значению, хост оповещает SPM, и SPM увеличивает размер логического тома ещё на 1 Гбайт. За возобновление работы ВМ после увеличения размера логического тома отвечает хост. Если работа ВМ будет приостановлена, это означает, что SPM не смог вовремя увеличить размер диска (например, если в хранилище недостаточно свободного дискового пространства).

Скорость записи виртуального диска в формате предварительного резервирования raw значительно выше, чем скорость записи виртуального диска в формате тонкого резервирования QCOW2. При этом время создания виртуального диска тонкого резервирования значительно меньше. Формат тонкого резервирования QCOW2 подходит для ВМ без интенсивных процессов ввода-вывода. Формат предварительного резервирования raw подходит для ВМ с высокой интенсивностью записи процессов ввода-вывода. Если ВМ записывает процессы ввода-вывода объёмом более 1 Гбайт каждые четыре секунды, всегда при возможности используйте предварительно зарезервированные диски в формате raw.

13.2. Виртуальные диски

Система виртуализации ROSA Virtualization предлагает следующие возможности для выделения свободного дискового пространства в хранилище:

- Предварительное резервирование.

Предварительно зарезервированный виртуальный диск заранее резервирует всё выделенное место в хранилище, предназначенное для виртуальной машины. Таким образом, предварительно зарезервированный логический том размером в 20 Гбайт, созданный для раздела размещения данных ВМ, займёт все 20 Гбайт свободного места в хранилище сразу после своего создания.

- Тонкое резервирование разреженного типа.

Тонкое резервирование разреженного типа даёт возможность администратору определить общий объём места в хранилище, выделяемого виртуальной машине, но это место выделяется только при необходимости. Логический том тонкого резервирования размером в 20 Гбайт займёт при создании 0 Гбайт. После установки операционной системы размер диска будет равен размеру установленных файлов и будет увеличиваться до максимального размера в 20 Гбайт по мере добавления данных.

Просмотреть **ID** (идентификатор) виртуального диска можно в меню **Хранилище → Диски**. Этот идентификатор служит для обозначения виртуального диска, поскольку название устройства (например, `/dev/vda0`) может поменяться, что приведёт в свою очередь к повреждению диска. Также просмотреть ID виртуального диска можно в `/dev/disk/by-id`.

Просмотреть **Виртуальный размер** диска можно в меню **Хранилище → Диски** и на вкладке **Диски** области подробного просмотра для доменов хранилищ, ВМ и шаблонов. Виртуальный размер — это общий объём дискового пространства, который может использовать ВМ. Таким образом это число, которое администратор указывает в поле **Размер (Гбайт)** при создании или изменении параметров виртуального диска.

Просмотреть **Фактический размер** диска можно на вкладке **Диски** области подробного просмотра доменов хранилищ и шаблонов. Фактический размер — это объём дискового пространства, выделенный виртуальной машине на текущий момент. Предварительно зарезервированные диски показывают одинаковое значение как для **Виртуального размера**, так и для **Фактического размера**. Диски разрежённого типа как правило показывают различные значения **Виртуального** и **Фактического размера**, в зависимости от того, сколько места было реально выделено диску в хранилище.

Примечание — при создании виртуального диска Cinder, формат и тип диска обрабатывается внутренними процессами Cinder, а не системой виртуализации ROSA Virtualization.

В Табл. 13.1 описываются возможные сочетания форматов и типов, разрешённые для хранилищ в системе виртуализации ROSA Virtualization.

Табл. 13.1. Сочетания форматов и типов, разрешённые для хранилищ

Хранилище	Формат	Тип	Примечание
NFS	raw	Предварительное резервирование	Файл без форматирования, начальный размер которого равен объёму, определённому

Хранилище	Формат	Тип	Примечание
			для виртуального диска
NFS	raw	Разрежённый	Файл без форматирования, начальный размер которого близок к нулю
NFS	QCOW2	Разрежённый	Файл в формате QCOW2, начальный размер которого близок к нулю
SAN	raw	Предварительное резервирование	Блочное устройство без форматирования, начальный размер которого равен объёму хранилища, выделенного для виртуального диска
SAN	QCOW2	Разрежённый	Блочное устройство, начальный размер которого намного меньше, чем размер, определённый для виртуального диска (на данный момент — 1 Гбайт). Выделяемое по мере необходимости пространство форматируется как QCOW2 (на данный момент шаг выделения — 1 Гбайт)

13.3. Очистка после удаления для виртуальных дисков

Активация флага `wipe_after_delete`, представленного на Портале администрирования в виде флажка **Забить нулями после удаления**, заменяет старые данные нулями при удалении виртуального диска. При указанном значении «*неверно*» (по умолчанию флаг деактивирован) во время удаления диска блоки будут освобождены для повторного использования, но данные не будут стёрты. Следовательно, эти данные потенциально можно восстановить, так как блоки не были забиты нулями.

Флаг `wipe_after_delete` эффективен только для блочных хранилищ. В применении к файловому хранилищу, например NFS, этот параметр не имеет смысла, так как файловая система обеспечивает полное удаление данных.

Активация флага `wipe_after_delete` для виртуальных дисков является дополнительной защитой и рекомендуется в том случае, если на виртуальных дисках хранятся любые сведения конфиденциального характера.

Данная операция требует более интенсивных вычислительных затрат, чем операция стандартного удаления, и система может испытывать снижение производительности и необходимость в увеличенном времени для выполнения операции очистки после удаления.

Примечание — функциональность замены данных нулями не является аналогом защищённого удаления и не даёт гарантии того, что данные будут удалены из хранилища, но гарантирует то, что новые диски, созданные в том же хранилище, не предоставят доступ к предыдущим данным.

Значение по умолчанию для флага `wipe_after_delete` можно изменить на `true` во время процесса настройки или с помощью утилиты `engine-config` в виртуализированном ЦУ.

Примечание — изменение значения по умолчанию для флага `wipe_after_delete` не влияет на значение параметра **Забить нулями после удаления** для уже существующих дисков.

Установка значения по умолчанию **`true`** для параметра **`SANWipeAfterDelete`** **с помощью утилиты настройки виртуализированного ЦУ**

1. Запустите утилиту `engine-config` с опцией `--set` и указанным значением `true` для параметра `SANWipeAfterDelete`:

```
# engine-config --set SANWipeAfterDelete=true
```

2. Перезапустите службу `ovirt-engine` для применения изменений:

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

Информация о выполнении операций очистки после удаления виртуальных дисков журналируется в файле `/var/log/vdsm/vdsm.log` на хосте.

В случае удачного заполнения нолями блоков диска журнал будет содержать следующую запись:

`id_домена_хранилища/id_тома` `was zeroed and will be deleted`

Например:

```
        a9cb0625-d5dc-49ab-8ad1-722e82b0bf/a49351a7-15d8-4932-8d67-
    51a36f9d61 was zeroed and will be deleted
```

При неудачном заполнении нолями блоков диска журнал будет содержать следующую запись:

```
        zeroing id_домена_хранилища/id_тома failed
        Zero and remove this volume manually
```

В случае удачного удаления диска журнал будет содержать следующую запись:

`finished with VG:` *`id_домена_хранилища`* `LVs:` *`список_id_томов`*`, img:` *`id_образа`*

Например:

```
        finished    with    VG:    a9cb0625-d5dc-49ab-8ad1-72722e82b0bf    LVs:
    {'a49351a7-15d8-4932-8d67-512a369f9d61':    ImgsPar(imgs=['11f8b3be-fa96-
    4f6a-bb83-14c9b12b6e0d'],                parent='00000000-0000-0000-0000-
    000000000000')}, img: 11f8b3be-fa96-4f6a-bb83-14c9b12b6e0d
```

При неудачном удалении диска журнал будет содержать следующую запись:

```
        Remove failed for some of VG: id_домена_хранилища zeroed volumes:
    список_id_томов
```

13.4. Разделяемые диски

Некоторым приложениям необходимо, чтобы хранилище было общим хранилищем серверов. Система виртуализации ROSA Virtualization даёт возможность пометить жёсткие диски ВМ флажком **Может быть общим** и присоединять эти диски к ВМ. Таким образом один виртуальный диск может использоваться несколькими гостями с поддержкой кластеров.

Разделяемые диски не должны использоваться во всех ситуациях. Общие диски рекомендуются для таких применений как серверы баз данных, собранные в кластеры. Но присоединение общего диска ко многим гостям, не имеющим поддержки кластера, скорей всего вызовет повреждение данных, поскольку их операции чтения и записи на диск не скоординированы.

Для общего диска нельзя создать снимок. Виртуальные диски со сделанными снимками нельзя пометить как общие.

Установить флажок **Может быть общим** для диска возможно либо во время его создания, либо во время изменения параметров диска.

13.5. Диски с доступом только для чтения

Некоторым приложениям необходимо, чтобы разделяемые администраторами данные были доступны только для чтения. Данная возможность реализуется при создании или изменении параметров диска, присоединённого к ВМ, на вкладке **Диски** области подробного просмотра ВМ с помощью флажка **Только для чтения**. Таким образом один диск может читаться несколькими гостями с поддержкой кластера, а привилегии на запись остаются только у администратора.

Во время работы ВМ нельзя сменить состояние диска с установленным параметром **Только для чтения**.

Примечание — монтирование журналируемой файловой системы требует доступа на чтение и запись. Использование параметра **Только для чтения** не является желательным для виртуальных дисков, содержащих такие файловые системы (например EXT3, EXT4 или XFS).

13.6. Работа с виртуальными дисками

13.6.1. Создание виртуального диска

Процесс создания дисков с типом **Образ** полностью управляется виртуализированным ЦУ. Диски с **Прямыми LUN** требуют уже существующих подготовленных внешних целей. Дискам **Cinder** необходим доступ к экземпляру тома OpenStack, который должен быть предварительно добавлен в окружение виртуализации ROSA Virtualization с помощью окна **Внешние поставщики**.

Создание виртуального диска, присоединённого к конкретной ВМ

1. Нажмите **Ресурсы → Виртуальные машины**.

2. Нажмите на имя ВМ, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Диски**.
4. Нажмите **Добавить**.
5. Перейдите на соответствующую вкладку, чтобы создать виртуальный диск с типом **Образ**, виртуальный диск с **Прямыми LUN** или виртуальный диск **Cinder** (Рис. 153).
6. Выберите параметры, требуемые для виртуального диска. Параметры изменяются в зависимости от выбранного типа диска.
7. Нажмите **OK**.

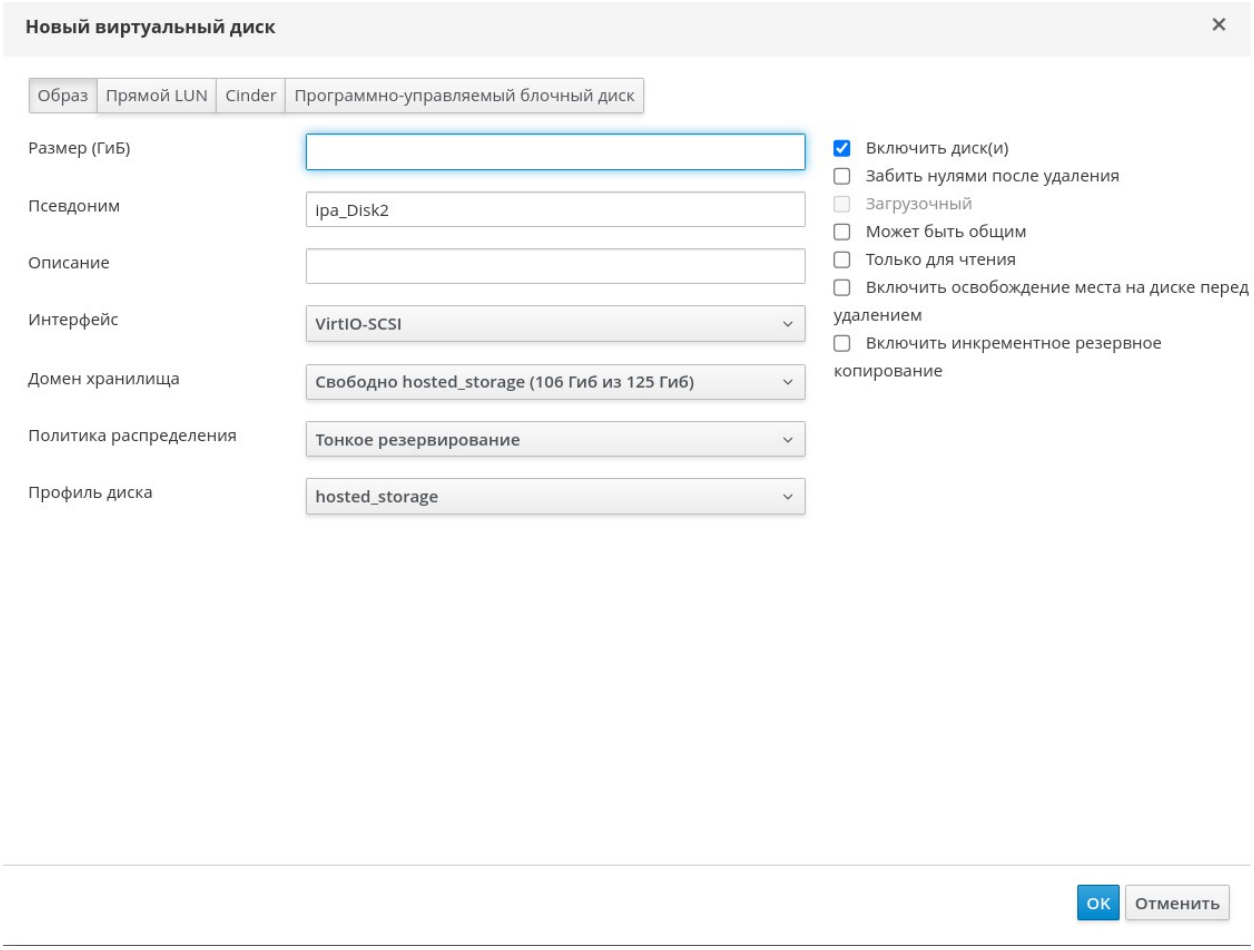

Рис. 153. Создание нового виртуального диска

Создание «плавающего» виртуального диска

При необходимости можно создать «плавающий» виртуальный диск, не принадлежащий ни одной ВМ. Этот диск можно присоединить к одной ВМ или к нескольким, а также этот диск может быть общим. При создании «плавающего» виртуального диска некоторые параметры будут недоступны (см. п. 13.6.2. Параметры виртуального диск).

1. Нажмите **Хранилище → Диски**.
2. Нажмите **Добавить**.

3. Нажмите на соответствующую кнопку, чтобы указать, будет ли виртуальный диск **Образом**, **Прямым LUN** или диском **Cinder**.
4. Выберите параметры, требуемые для виртуального диска. Параметры изменяются в зависимости от выбранного типа диска.
5. Нажмите **OK**.

13.6.2. Параметры виртуального диска

13.6.2.1. Параметры образа виртуального диска

В Табл. 13.2 описываются параметры образа виртуального диска в окнах Новый виртуальный диск и **Параметры виртуального диска**.

Табл. 13.2. Параметры образа виртуального диска

Поле	Описание
Размер (ГиБ)	Размер нового виртуального диска в Гбайт
Псевдоним	Название виртуального диска (ограничение — 40 символов)
Описание	Описание виртуального диска (необязательное, но рекомендуемое для заполнения поле)
Интерфейс	Виртуальный интерфейс, предоставляемый диском виртуальной машине (параметр доступен только при создании присоединённого диска). Тип интерфейса можно обновлять после остановки всех ВМ, к которым присоединён диск. Интерфейс **VirtIO** более быстрый, но требует специальных драйверов. В ОС семейства ROSA эти драйверы присутствуют. В ОС семейства Windows драйверы отсутствуют, но их можно установить с образа гостевых утилит или с виртуальной дискеты. Устройствам **IDE** специальные драйверы не требуются
Дата-центр	Дата-центр, в котором будет использоваться виртуальный диск (параметр доступен только при создании плавающих дисков)
Домен хранения	Домен хранения, в котором будет храниться виртуальный диск. В выпадающем списке показаны все домены хранилищ, доступные в указанном дата-центре, а также отображается общий объём хранилища в домене и объём, доступный на данный момент
Политика распределения	Политика распределения для нового виртуального диска. Для выбора доступны следующие значения: • Предварительное резервирование. Во время создания виртуального диска в домене хранилища выделяется весь объём диска. Виртуальный и

Поле	Описание
	зарезервированный размеры равны. На создание предварительно зарезервированного виртуального диска затрачивается больше времени, чем на создание виртуального диска тонкого резервирования, но они имеют лучшие показатели чтения и записи. Предварительно зарезервированные виртуальные диски рекомендуются для размещения серверов и других ВМ с интенсивными процессами ввода-вывода. Если ВМ в процессе работы записывает более 1 Гбайт каждые 4 секунды, при возможности используйте предварительно зарезервированные диски. • Тонкое резервирование. Во время создания виртуального диска выделяется 1 Гбайт хранилища и настраивается максимальный предел размера, до которого может вырасти диск. Виртуальный размер диска является максимальным пределом, а фактический размер — место, выделенное на данный момент. Диски тонкого резервирования создаются быстрее предварительно зарезервированных дисков и позволяют использовать превышенное выделение ресурсов хранилища. Виртуальные диски тонкого резервирования рекомендуются для рабочих столов.
Профиль диска	Профиль диска, присвоенный виртуальному диску. Профили дисков определяют максимальную пропускную способность и максимальный уровень операций ввода-вывода для виртуального диска в домене хранения. Профили дисков определяются на уровне домена хранения на основании записей о качестве обслуживания хранилищ, созданных для дата-центров
Включить диск(и)	Немедленная активация виртуального диска после создания (параметр доступен только при создании присоединённого диска)
Забить нулями после удаления	Параметр даёт возможность включить повышенную защиту в виде удаления конфиденциальной информации при удалении виртуальных дисков
Загрузочный	Параметр даёт возможность пометить виртуальный диск как загрузочный (параметр доступен только при создании присоединённого диска)
Может быть общим	Параметр даёт возможность присоединить виртуальный диск к нескольким виртуальным машинам одновременно
Только для чтения	Параметр даёт возможность предоставить доступ к виртуальному диску только для чтения (параметр доступен

Поле	Описание
	только при создании присоединённого диска). Один и тот же диск может быть доступен только для чтения для одной ВМ, но доступен для записи для другой ВМ
Освободить блоки	Параметр даёт возможность сжать диск тонкого резервирования во время работы ВМ (параметр доступен только при создании присоединённого диска). Если параметр включён, команды SCSI UNMAP, вызванные гостевой ВМ, передаются QEMU в базовое хранилище для освобождения неиспользуемого пространства. Базовое устройство блочного хранилища должно поддерживать вызовы discard, а параметр не может использоваться вместе с параметром **Забить нулями после удаления**, если только базовое хранилище не поддерживает свойство discard_zeroes_data. Для файлового хранилища соответствующая базовая файловая система и блочное устройство должны поддерживать вызовы discard
Включить инкрементное резервное копирование	Технологический параметр, который не используется (игнорируется) в процессе пользовательской настройки

13.6.2.2. Параметры виртуального диска с прямыми LUN

Параметр **Прямой LUN** может присутствовать либо в меню **Таргеты > LUN**, либо в меню **LUN > Таргеты**. Меню **Таргеты > LUN** сортирует доступные номера LUN согласно хостам, на которых обнаружены LUN, в то время как меню **LUN > Таргеты** отображает одиночный список LUN.

Для обнаружения целевого сервера заполните поля в разделе **Обнаружение таргетов** и нажмите кнопку **Обнаружить**. Далее нажмите кнопку **Выполнить вход для всех** для получения списка всех доступных LUN на целевом сервере, после чего с помощью переключателей рядом с каждым LUN, выберите добавляемые LUN.

Прямое использование LUN в качестве образов дисков ВМ удаляет слой абстракции между виртуальными машинами и данными.

При использовании прямых LUN в качестве образов жёстких дисков ВМ необходимо учитывать следующие особенности:

- Динамическая миграция прямых LUN в виде образов жёстких дисков в хранилище не поддерживается.
- Диски в виде прямых LUN не включаются в экспорт ВМ.
- Диски в виде прямых LUN не включаются в снимки ВМ.

В Табл. 13.3 описываются параметры виртуального диска с прямыми LUN в окнах **Новый виртуальный диск** и **Параметры виртуального диска**.

Табл. 13.3. Параметры виртуального диска с прямыми LUN

Поле	Описание
Псевдоним	Название виртуального диска (ограничение — 40 символов)
Описание	Описание виртуального диска (необязательное, но рекомендуемое для заполнения поле). По умолчанию в поле присутствует 4 последних символа LUN ID. Поведение по умолчанию можно настроить, выставив соответствующее значение ключа `PopulateDirectLUNDiskDescriptionWithLUNId` с помощью команды `engine-config`. Ключ может иметь значение `-1` для использования полного идентификатора LUN, или `0`, чтобы эта возможность игнорировалась. При указании положительного целого числа описание заполняется соответствующим числом символов идентификатора LUN
Интерфейс	Виртуальный интерфейс, предоставляемый диском виртуальной машине (параметр доступен только при создании присоединённого диска). Тип интерфейса можно обновлять после остановки всех ВМ, к которым присоединён диск. Интерфейс **VirtIO** более быстрый, но требует специальных драйверов. В ОС семейства ROSA эти драйверы присутствуют. В ОС семейства Windows драйверы отсутствуют, но их можно установить с образа гостевых утилит или с виртуальной дискеты. Устройствам **IDE** специальные драйверы не требуются
Дата-центр	Дата-центр, в котором будет использоваться виртуальный диск (параметр доступен только при создании плавающих дисков)
Хост	Хост, на котором будет смонтирован LUN. Можно выбрать любой хост в дата-центре
Тип хранилища	Тип добавляемых внешних LUN. Для выбора доступны значения **iSCSI** или **Оптоволокно**
Обнаружение целей	При использовании внешних LUN iSCSI и выбранном меню **Таргеты > LUN**, в разделе **Обнаружение целей** будут доступны следующие поля: • **Адрес** — имя хоста или IP-адрес целевого сервера. • **Порт** — порт, с которого будет выполняться подключение к целевому серверу. Номер порта по умолчанию — 3260. • **Аутентификация пользователя** — установите этот флажок для аутентификации пользователя на сервере iSCSI.

Поле	Описание
	• **Имя пользователя CHAP** — имя пользователя, имеющего полномочия входа в систему на LUN. Это поле становится видимым при отмеченном пункте **Аутентификация пользователя**. • **Пароль CHAP** — пароль пользователя, имеющего полномочия входа в систему на LUN. Это поле становится видимым при отмеченном пункте **Аутентификация пользователя**.
Активировать диск(и)	Немедленная активация виртуального диска после создания (параметр доступен только при создании присоединённого диска)
Загрузочный	Параметр даёт возможность пометить виртуальный диск как загрузочный (параметр доступен только при создании присоединённого диска)
Может быть общим	Параметр даёт возможность присоединить виртуальный диск к нескольким виртуальным машинам одновременно
Только для чтения	Параметр даёт возможность предоставить доступ к виртуальному диску только для чтения (параметр доступен только при создании присоединённого диска). Один и тот же диск может быть доступен только для чтения для одной ВМ, но доступен для записи для другой ВМ
Включить освобождение блоков	Параметр даёт возможность сжать диск тонкого резервирования во время работы ВМ (параметр доступен только при создании присоединённого диска). Если параметр включён, команды SCSI UNMAP, вызванные гостевой ВМ, передаются QEMU в базовое хранилище для освобождения неиспользуемого пространства
Включить сквозной доступ к SCSI	Параметр доступен только при создании присоединённого диска и в случае, когда для параметра **Интерфейс** указано значение **VirtIO-SCSI**. Выбор этого флажка включает сквозной доступ виртуального диска к физическому устройству SCSI. Интерфейс VirtIO-SCSI с включённым сквозным доступом к SCSI автоматически включает в себя поддержку освобождения блоков. Если этот флажок отмечен, параметр **Только для чтения** не поддерживается. Если этот параметр не отмечен, виртуальное устройство использует эмулируемое устройство SCSI. Для эмулируемых дисков VirtIO-SCSI поддерживается параметр **Только для чтения**

Поле	Описание
Включить привилегированный ввод-вывод SCSI	Параметр доступен только при создании присоединённого диска и при выбранном параметре **Включить сквозной доступ к SCSI**. Выбор этого параметра включает доступ SCSI Generic I/O (SG_IO) без фильтрации, разрешая привилегированные команды SG_IO для диска. Этот параметр требуется для постоянного резервирования
Использует резервирование SCSI	Параметр доступен только при создании присоединённого диска и при выбранных параметрах **Включить сквозной доступ к SCSI** и **Включить привилегированный ввод-вывод SCSI**. Выбор этого параметра отключает возможность миграции для любой ВМ, использующей этот диск, с целью предотвращения потери доступа к диску со стороны ВМ, использующих резервирование SCSI

13.6.2.3. Параметры виртуального диска Cinder

Для виртуальных дисков Cinder требуется доступ к экземпляру тома OpenStack, который был добавлен в окружение виртуализации ROSA Virtualization с помощью окна **Внешние поставщики**.

При отсутствии доступных доменов хранения томов OpenStack, для которых имеются разрешения на создание дисков в соответствующих дата-центрах, интерфейс настройки параметров виртуальных дисков Cinder будет недоступен.

В Табл. 13.4 описываются параметры виртуального диска Cinder в окнах **Новый виртуальный диск** и **Параметры виртуального диска**.

Табл. 13.4. Параметры виртуального диска Cinder

Поле	Описание
Размер (Гбайт)	Размер нового виртуального диска в Гбайт
Псевдоним	Название виртуального диска (ограничение — 40 символов)
Описание	Описание виртуального диска (необязательное, но рекомендуемое для заполнения поле)
Интерфейс	Виртуальный интерфейс, предоставляемый диском виртуальной машине (параметр доступен только при создании присоединённого диска). Тип интерфейса можно обновлять после остановки всех ВМ, к которым присоединён диск. Интерфейс **VirtIO** более быстрый, но требует специальных драйверов. В ОС семейства ROSA эти драйверы присутствуют. В ОС семейства Windows драйверы отсутствуют, но их можно установить с образа гостевых утилит или с виртуальной

Поле	Описание
	дискеты. Устройствам **IDE** специальные драйверы не требуются
Дата-центр	Дата-центр, в котором будет использоваться виртуальный диск (параметр доступен только при создании плавающих дисков)
Домен хранения	Домен хранения, в котором будет располагаться виртуальный диск. В выпадающем списке показываются все домены хранилищ, доступные в указанном дата-центре, а также отображается общий объём хранилища в домене и объём, доступный на данный момент
Тип тома	Тип тома виртуального диска. В выпадающем списке показываются все доступные типы томов. Тип тома будет управляться и настраиваться в OpenStack Cinder
Активировать диск(и)	Немедленная активация виртуального диска после создания (параметр доступен только при создании присоединённого диска)
Загрузочный	Параметр даёт возможность пометить виртуальный диск как загрузочный (параметр доступен только при создании присоединённого диска)
Может быть общим	Параметр даёт возможность присоединить виртуальный диск к нескольким виртуальным машинам одновременно
Только для чтения	Параметр даёт возможность предоставить доступ к виртуальному диску только для чтения (параметр доступен только при создании присоединённого диска). Один и тот же диск может быть доступен только для чтения для одной ВМ, но доступен для записи для другой ВМ

13.6.3. Обзор процесса динамической миграции между хранилищами

Существует возможность выполнения миграции виртуальных дисков из одного домена хранения в другой во время работы ВМ, к которой эти диски присоединены. Этот процесс называется динамической миграцией. При миграции диска, присоединённого к выполняющейся ВМ, в исходном домене хранения создаётся снимок цепочки образа этого диска, и вся эта цепочка образа реплицируется в целевом домене. Поэтому необходимо убедиться в том, что в доменах хранения (исходном и целевом) существует свободное дисковое пространство для размещения цепочки образа диска и снимка. При каждой попытке динамической миграции между хранилищами создаётся новый снимок, даже если эта попытка будет неудачной.

При использовании динамической миграции между хранилищами учитывайте следующие особенности процесса:

- Динамическая миграция может осуществляться для нескольких дисков одновременно.
- Несколько дисков одной ВМ могут располагаться более, чем в одном домене хранилищ, но цепочки образов каждого диска должны располагаться в одном домене.
- Динамическая миграция может проводиться между двумя любыми доменами хранения в одном дата-центре.
- Не поддерживается динамическая миграция образов жёстких дисков с прямыми LUN или общих дисков.

13.6.4. Перемещение виртуальных дисков

В следующей последовательности действий описывается процесс перемещения виртуального диска, присоединённого к ВМ или «плавающего» виртуального диска из одного домена хранения в другой.

При перемещении виртуальных дисков поддерживается динамическая миграция, таким образом диски, присоединённые к выполняющейся ВМ, также можно перемещать, или как вариант, завершите работу ВМ перед началом миграции.

При перемещении виртуальных дисков учитывайте следующие особенности процесса:

- Возможно перемещение нескольких виртуальных дисков одновременно.
- Диски могут перемещаться между двумя любыми доменами хранения одного дата-центра.
- Если виртуальный диск присоединён к ВМ, созданной на базе шаблона с использованием тонкого резервирования пространства в хранилище, необходимо скопировать диски, на базе которых был создан шаблон, в тот же домен хранения, что и виртуальный диск.

Перемещение виртуального диска

1. Нажмите **Хранилище** → **Диски** и выберите один или несколько виртуальных дисков для перемещения.
2. Нажмите **Переместить**.
3. В списке **Таргет** выберите домен хранения, в который будет перемещён виртуальный диск.
4. При необходимости в списке **Профиль диска** выберите профиль диска.
5. Нажмите **OK**.

В результате выбранные виртуальные диски будут перемещены в целевой домен хранения. Во время процесса перемещения в столбце **Статус** будет отображаться надпись `Заблокировано`, а ход процесса будет показан в виде индикатора прогресса.

13.6.5. Изменение типа интерфейса диска

После создания диска пользователь может изменить тип интерфейса диска. Это даёт возможность присоединить уже существующий диск к ВМ, требующей другого типа интерфейса. Например диск, использующий интерфейс `VirtIO`, можно присоединить к

ВМ, требующей интерфейс `VirtIO-SCSI` или `IDE`. Эта возможность предоставляет гибкость в осуществлении миграции дисков в целях создания и восстановления резервных копий или восстановления после сбоев. Тип интерфейса общих дисков также можно обновлять для каждой из ВМ. Это означает, что каждая ВМ, использующая разделяемые диски, может использовать различные типы интерфейсов.

Перед изменением типа интерфейса диска, работа всех ВМ, использующих этот диск, должна быть остановлена.

Изменение типа интерфейса диска

1. Нажмите **Ресурсы → Виртуальные машины** и остановите работу необходимых ВМ.
2. Нажмите на имя ВМ, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Диски** и выберите диск.
4. Нажмите **Изменить**.
5. Из выпадающего списка **Интерфейс** выберите новый тип интерфейса.
6. Нажмите **ОК**.

Также диск можно присоединять к различным ВМ, требующим другого типа интерфейса.

Присоединение диска к ВМ, использующим другой тип интерфейса

1. Нажмите **Ресурсы → Виртуальные машины** и остановите работу соответствующих ВМ.
2. Нажмите на имя ВМ, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Диски** и выберите диск.
4. Нажмите **Удалить**, затем нажмите **ОК**.
5. Вернитесь в меню **ВМ** и нажмите на имя новой ВМ, к которой будет присоединён диск.
6. Перейдите на вкладку **Диски**, затем нажмите **Присоединить**.
7. Выберите диск в окне **Присоединить виртуальные диски** и выберите соответствующий интерфейс из выпадающего списка **Интерфейс**.
8. Нажмите **ОК**.

13.6.6. Копирование виртуальных дисков

Виртуальный диск можно скопировать из одного домена хранения в другой. После чего скопированный диск можно присоединять к виртуальным машинам.

Копирование виртуального диска

1. Нажмите **Хранилище → Диски** и выберите один или несколько виртуальных дисков.
2. Нажмите **Копировать**.
3. Опционально введите новое имя в поле **Псевдоним**.
4. В списке **Таргет** выберите домен хранения, в который будут скопированы виртуальные диски.

5. При необходимости в списке **Профиль диска** выберите профиль диска.
6. Нажмите **OK**.

В результате выбранные виртуальные диски будут скопированы в целевой домен хранения. Во время процесса копирования в столбце **Статус** будет отображаться надпись `Заблокировано`, а ход процесса будет показан в виде индикатора прогресса.

13.6.7. Шифрование виртуальных дисков

В целях обеспечения защиты информации пользователь может создавать и использовать в работе шифрованные виртуальные диски в дополнение к обычным виртуальным дискам.

Примечание — для поддержки функции шифрования виртуальных дисков должны быть установлены дополнительные пакеты в окружение виртуализации ROSA Virtualization.

13.6.7.1. Установка дополнительных пакетов

Установка дополнительных пакетов осуществляется пользователем на всех хостах (физических серверах), входящих в состав ROSA Virtualization, а также в виртуализированном ЦУ (ВМ СУСВ).

Установка пакета `rv-vm-disks-encoding-host` на хосте

Перед установкой пакета `rv-vm-disks-encoding-host` вставьте носитель с дистрибутивом ROSA Virtualization в привод DVD и выполните в консоли хоста следующую команду для монтирования носителя:

```
# mount /dev/cdrom/ /mnt/
```

Для установки дополнительных пакетов выполните в консоли хоста следующие команды в указанной последовательности:

```
# dnf config-manager --set-enabled DVD
# dnf swap -y vdsm-python vdsm-python-crypto
# dnf install -y rv-vm-disks-encoding-host
# systemctl restart vdsmd
```

Установка пакета `rv-vm-disks-encoding-engine` в виртуализированном ЦУ (ВМ СУСВ)

Для установки дополнительного пакета выполните в консоли ВМ СУСВ следующие команды:

```
# dnf -y install rv-vm-disks-encoding-engine
# systemctl enable --now rosa-disk-encoding-daemon.service
# systemctl restart httpd
```

13.6.7.2. Создание шифрованных виртуальных дисков

Создание шифрованного диска осуществляется пользователем через интерфейс Портала администрирования.

Создание шифрованного диска

1. Нажмите **Дополнения → Шифрование дисков**.

2. Введите наименование диска в поле **Псевдоним**, пробелы в названии диска использовать не допускается.
3. Укажите **Размер** диска в Гбайт.
4. Выберите **Дата-центр** и **Домен хранения**.
5. Задайте **Пароль** для шифрования диска.

Примечание — в случае утери пароля, работа на другом хосте с диском или перенесенной копией этого диска будет невозможна.

6. Выберите **Алгоритм** и **Режим** шифрования диска.
7. Нажмите **Создать диск**.

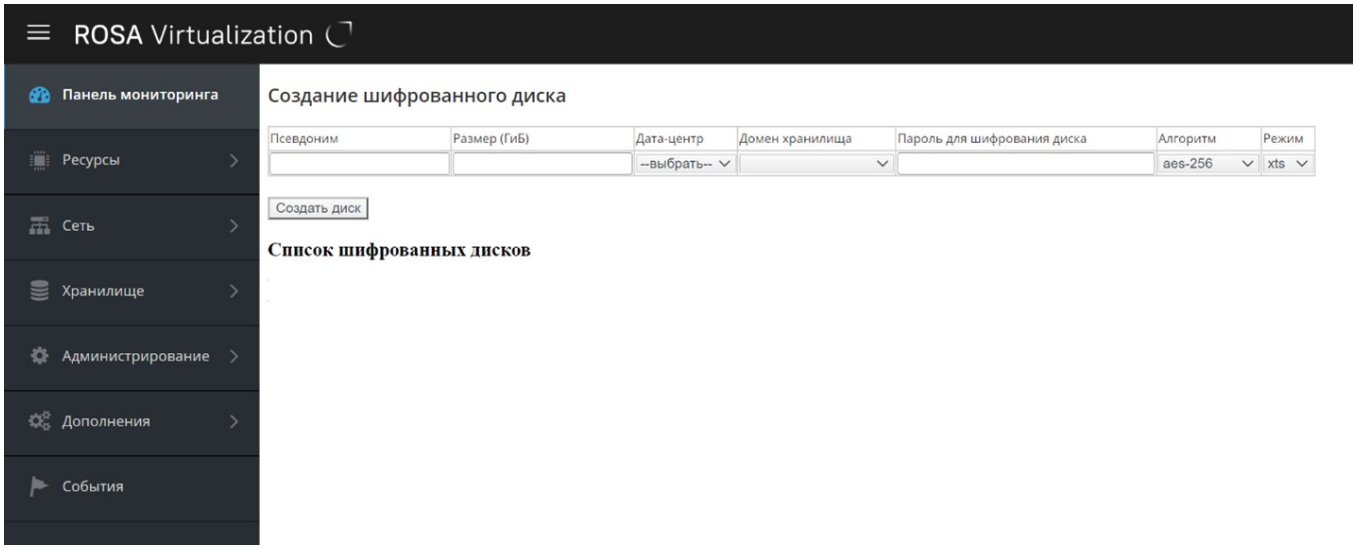

Рис. 154.Заполнение информации о создаваемом шифрованном диске

Создаваемый диск будет иметь статус: «**Идет создание диска…**».

Список шифрованных дисков

Название диска	uuid_disk	Присоединено к	Шифрование	Размер диска	Домен хранилища	Состояние
wizard						Идёт создание диска...

Рис. 155. Процесс создания шифрованного диска

Когда диск будет создан, статус в столбце «**Состояние**» поменяется на «ОК».

Список шифрованных дисков

Название диска	uuid_disk	Присоединено к	Шифрование	Размер диска	Домен хранилища	Состояние
wizard	5fc96c55-ecc5-4993-ba74-bf0c203e92da		aes-256/xts	20	hosted_storage	OK

Рис. 156. Завершение создания шифрованного диска

В результате созданный диск появится как в списке шифрованных дисков в меню **Дополнения → Шифрование дисков**, так и в общем списке виртуальных дисков в меню **Хранилище → Диски**.

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.

Обратите внимание, что создание снимков для шифрованных дисков не допускается, а ВМ с таким диском не запустится.

13.6.7.3. Создание копии шифрованного диска

После создания шифрованного диска он появляется не только в таблице шифрованных дисков, но и в общей таблице дисков.

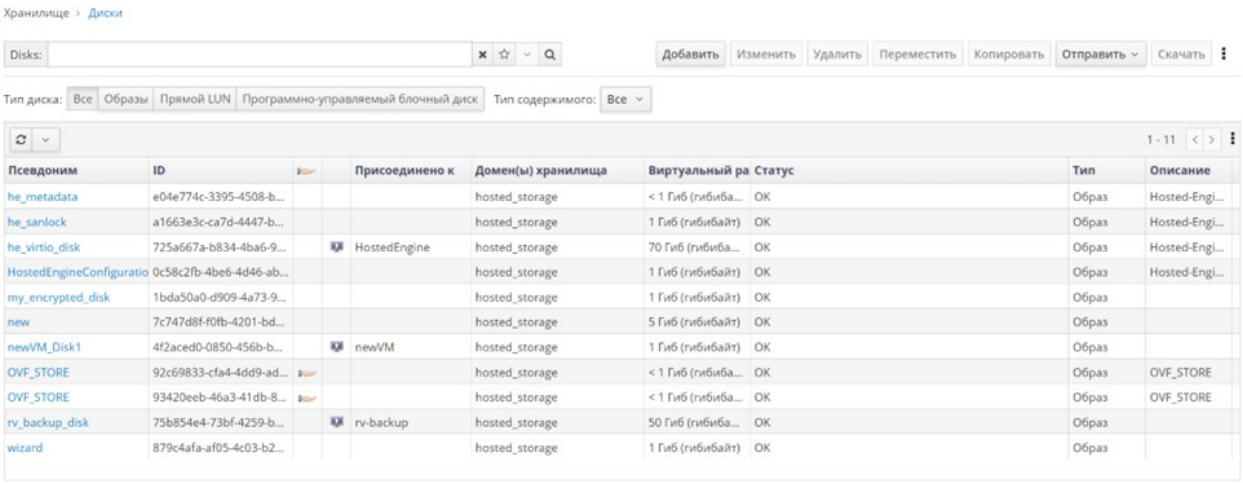

Рис. 157. Общий список дисков

Копия шифрованного диска производится стандартными средствами.

После создания копии диска он так же отобразиться в списке шифрованных дисков.

Список шифрованных дисков

Название диска	uuid_disk	Присоединено к	Шифрование	Размер диска	Домен хранилища	Состояние
wizard	5fc96c55-ecc5-4993-ba74-bf0c203e92da		aes-256/xts	20	hosted_storage	OK
wizard_copy	d4e52a05-75c5-43eb-ad74-aa095be7d181		aes-256/xts	20	hosted_storage	OK

Рис. 158. Список шифрованных дисков

13.6.7.4. Присоединение шифрованного диска к ВМ

Присоединение шифрованного диска к ВМ производится стандартными средствами. После того, как диск присоединён к ВМ, в таблице шифрованных дисков появится название ВМ, к которой присоединён диск.

Список шифрованных дисков

Название диска	uuid_disk	Присоединено к	Шифрование	Размер диска	Домен хранилища	Состояние
wizard	5fc96c55-ecc5-4993-ba74-bf0c203e92da	test_vm	aes-256/xts	20	hosted_storage	OK
wizard_copy	d4e52a05-75c5-43eb-ad74-aa095be7d181		aes-256/xts	20	hosted_storage	OK

Рис. 159. Список шифрованных дисков – указание ВМ, к которой присоединен диск

13.6.7.5. Удаление шифрованного диска

Удаление шифрованного диска происходит стандартными средствами на вкладке «**Хранилище**» → «**Диски**» через интерфейс Портала администрирования ВМ.

13.6.7.6. Скачивание шифрованного диска

Скачивание шифрованного диска происходит стандартными средствами на вкладке «**Хранилище**» → «**Диски**» через интерфейс Портала администрирования ВМ.

13.6.7.7. Установка шифрованного диска на другой хост

1. Файл диска, который был скачан с первого хоста, отправляется на новый хост стандартными средствами на вкладке «**Хранилище**» → «**Диски**» через интерфейс Портала администрирования ВМ.
2. После того, как диск будет отправлен в систему, он появится в таблице шифрованных дисков.
3. Установленный шифрованный диск с другого хоста будет требовать пароль, который был присвоен диску при создании. Если пароль утерян или были отправлены неверные данные, то работа с диском будет невозможна.

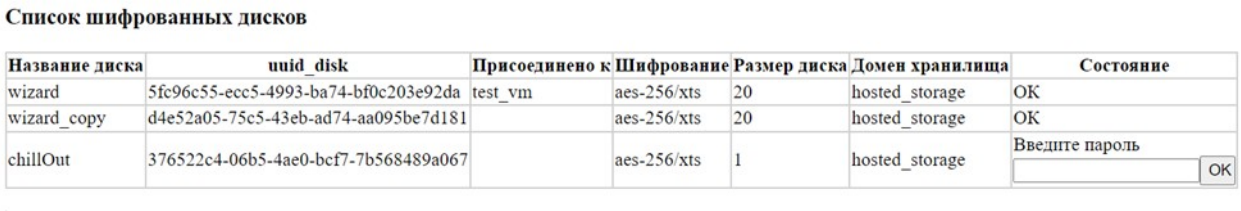

Рис. 160. Ввод пароля для переносимого диска

4. Для завершения установки диска на новый хост введите пароль. И нажмите кнопку **ОК**.

13.6.7.8. Ошибка при создании шифрованного диска

Если при создании шифрованного диска возникнут ошибки, то они будут отображаться в интерфейсе Портала администрирования ВМ.

Ниже предоставлен пример ошибки, когда при создании диска не был указан домен хранения.

Рис. 161: Ошибка при создании шифрованного диска

Примечания:

1. Создание снэпшотов для шифрованных дисков невозможно. Если создан снэпшот для шифрованного диска, то ВМ с таким диском запущена не будет.
2. При загрузке внешнего шифрованного диска на хост, убедитесь, что выключена опция инкрементного резервного копирования. В противном случае диск будет неработоспособным.

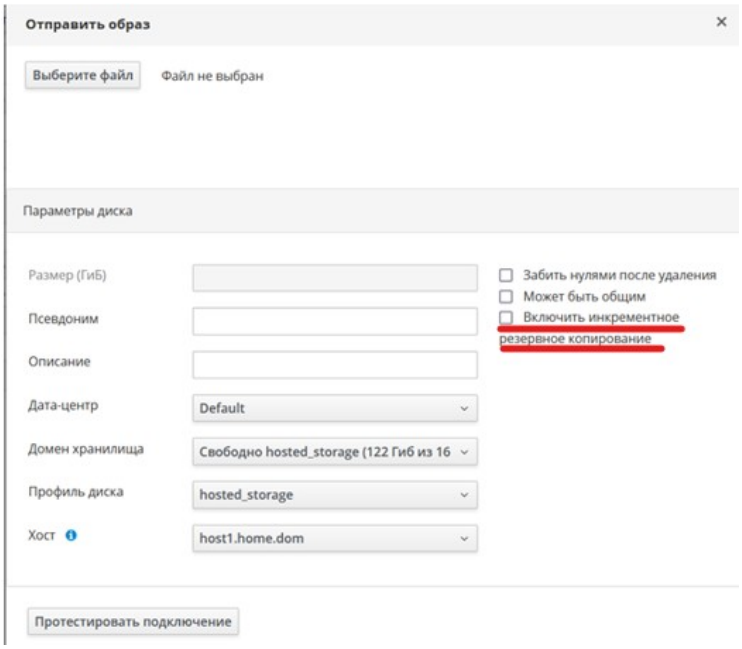

Рис. 162. Деактивированная опция инкрементного резервного копирования

13.6.8. Отправка образов в домен хранения данных

Отправить образы виртуальных дисков и образы ISO в домен хранения данных можно на Портале администрирования или с помощью REST API.

13.6.9. 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.

Импорт образа диска

1. Нажмите **Хранилище → Домены**.
2. Нажмите на имя импортированного домена хранения, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Импорт диска**.
4. Выберите один или несколько образов дисков и нажмите **Импортировать**.
5. Выберите соответствующий **Профиль диска** для каждого диска.
6. Нажмите **OK**.

13.6.10. Импорт незарегистрированного образа диска из импортированного домена хранения

«Плавающие» виртуальные диски, созданные вне окружения виртуализации ROSA Virtualization, не регистрируются виртуализированным ЦУ.

Выполните сканирование домена хранения для опознания незарегистрированных «плавающих» дисков для их последующего импорта.

Примечание — в виртуализированный ЦУ можно импортировать только диски, совместимые с QEMU.

Импорт незарегистрированного образа диска

1. Нажмите **Хранилище → Домены**.
2. Нажмите на имя импортированного домена хранения, чтобы перейти к подробному просмотру.
3. Нажмите **Больше действий** (⋮), затем нажмите **Сканирование дисков**, чтобы виртуализированный ЦУ идентифицировал незарегистрированные виртуальные диски.
4. Перейдите на вкладку **Импорт дисков**.
5. Выберите один или несколько образов дисков и нажмите **Импортировать**.
6. Выберите соответствующий **Профиль диска** для каждого диска.
7. Нажмите **ОК**.

13.6.11. 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.

Импорт виртуального диска из службы образов OpenStack

1. Нажмите **Хранилище → Домены.**
2. Нажмите на имя домена службы образов OpenStack, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Образы** и выберите образ.
4. Нажмите **Импорт**.
5. Выберите **Дата-центр**, в который будет импортирован образ.
6. Из выпадающего списка **Имя домена** выберите домен хранения, в котором будет храниться образ.
7. Опционально в списке **Квота** выберите квоту, применяемую к образу.
8. Нажмите **ОК**.

При необходимости после импорта виртуальный диск можно присоединить к ВМ.

13.6.12. 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.

Экспорт виртуального диска в службу образов OpenStack

1. Нажмите **Хранилище → Диски** и выберите один или несколько экспортируемых дисков.
2. Нажмите **Больше действий** (⋮), затем нажмите **Экспорт**.

3. Из выпадающего списка **Имя домена** выберите службу образов OpenStack, в которую будут экспортированы диски.
4. Опционально в списке **Квота** выберите квоту, применяемую к дискам.
5. Нажмите **OK**.

13.6.13. Возвращение хосту дискового пространства, ранее используемого виртуальными дисками

Виртуальные диски, использующие тонкое резервирование пространства в хранилище, не сжимаются автоматически после удаления файлов. Например, если фактический размер диска равен 100 Гбайт, и будет удалено 50 Гбайт файлов, выделенное пространство диска по-прежнему останется 100 Гбайт, а оставшиеся 50 Гбайт не возвращаются хосту и соответственно не могут использоваться виртуальными машинами.

Для того, чтобы вернуть хосту неиспользуемое дисковое пространство выполните процедуру разреживания диска ВМ, в результате которой свободное пространство переносится с образа диска на хост. При этом разреживать можно несколько дисков одновременно.

Рекомендуется выполнять разреживание диска перед клонированием ВМ, созданием шаблона на базе ВМ или очисткой пространства на диске в домене хранения.

Процедура разреживания диска имеет ряд следующих ограничений:

- Домены хранения NFS должны использовать версию NFS 4.2 или выше.
- Нельзя разреживать диск, использующий прямой LUN.
- Нельзя разреживать диск Cinder.
- Нельзя разреживать диск, использующий политику предварительного резервирования пространства в хранилище.

Примечание — при создании ВМ из шаблона выберите параметр **Тонкое** в поле **Резервирование хранилища**, или при выборе **Клонирования**, убедитесь в том, что шаблон основан на ВМ с тонким резервированием.

- Разреживать можно только активные снимки дисков.

Разреживание диска

1. Нажмите **Ресурсы → Виртуальные машины** и выключите необходимую ВМ.
2. Нажмите на имя ВМ, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Диски** и убедитесь в том, что диск имеет статус `OK`.
4. Нажмите **Больше действий** (⋮), затем нажмите **Разредить**.
5. Нажмите **OK**.

В процессе разреживания диска на вкладке **События** появится сообщение `Начало разреживания`, при этом статус диска изменится на значение `Заблокировано`.

После завершения разреживания диска на вкладке **События** появится сообщение `Разрежено успешно`, при этом статус диска изменится на значение `OK`.

В результате неиспользуемое дисковое пространство будет возвращено хосту и станет доступно для использования другими ВМ.

Часть III. Администрирование окружения

Глава 14. Администрирование виртуализированного ЦУ

14.1. Обслуживание виртуализированного ЦУ

14.1.1. Режимы обслуживания 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.

1. Активация локального режима обслуживания

Включение локального режима обслуживания останавливает работу агента высокой доступности на отдельном узле виртуализированного ЦУ.

Активация локального режима обслуживания с Портала администрирования:

1. Переводим узел виртуализированного ЦУ в локальный режим обслуживания:
   1.1. На Портале администрирования нажмите «**Ресурсы» → «Хосты»** и выберите узел виртуализированного ЦУ.
   1.2. Нажмите «**Управление» → «Обслуживание»** (Рис. 163) и дальше в открывшемся окне нажмите **ОК**. Опционально укажите причину перевода хоста в режим обслуживания (Рис. 164). Выбранный узел будет автоматически помещён в локальный режим обслуживания.

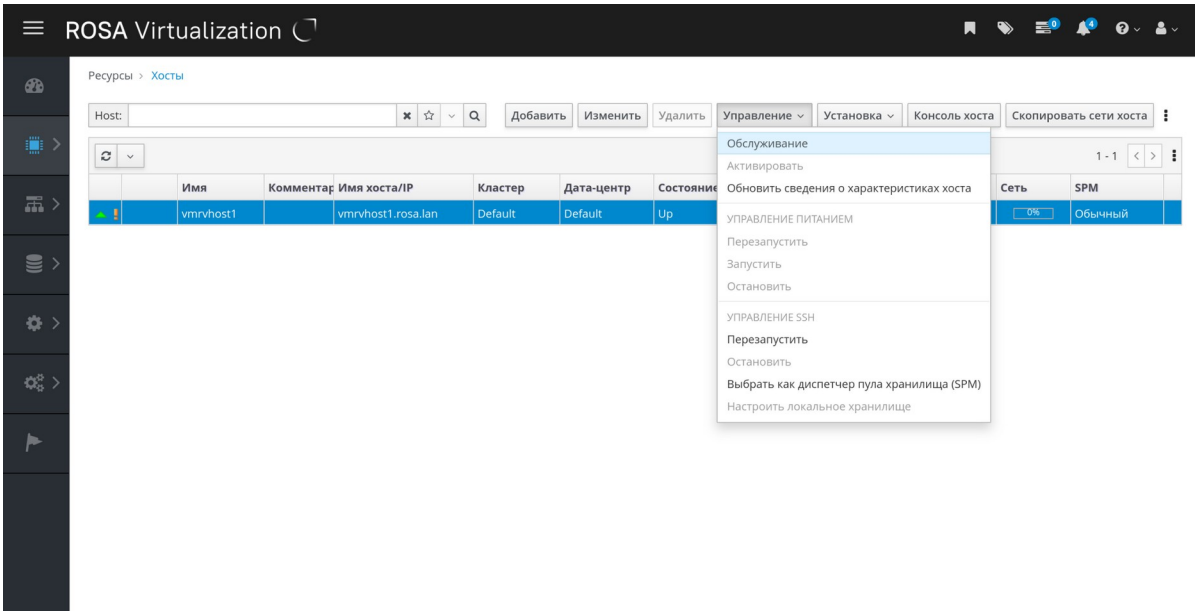

Рис. 163. Активация локального режима обслуживания хоста

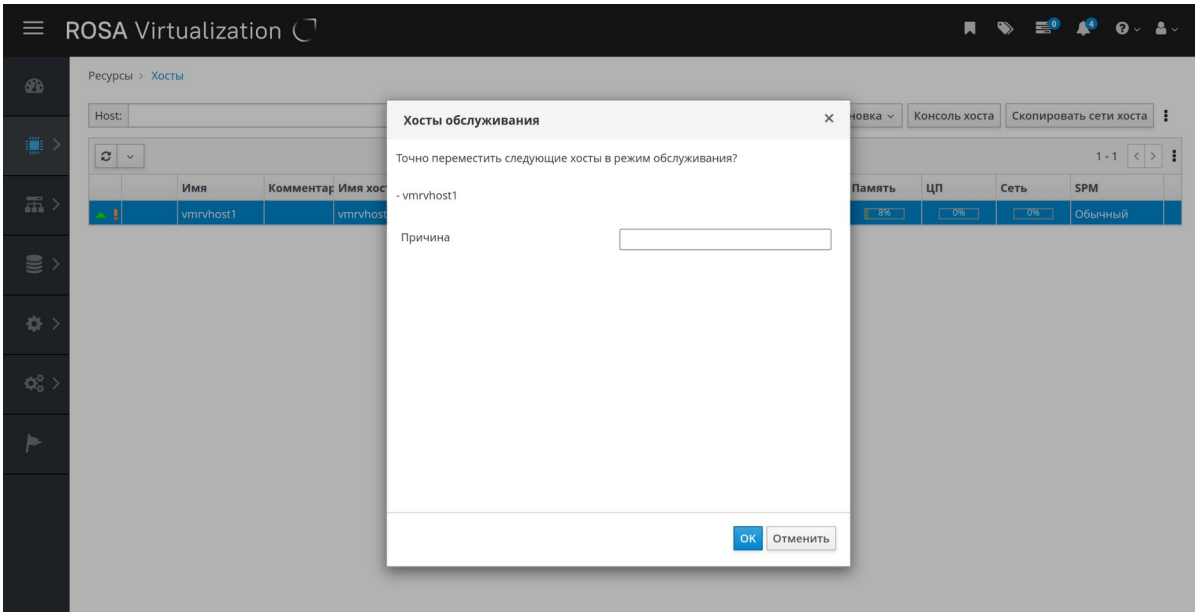

Рис. 164. Форма подтверждения перевода хоста в режим обслуживания

2. Выполнив необходимые задачи по обслуживанию, отключите режим обслуживания:
   2.1 На Портале администрирования нажмите «**Ресурсы**» → «**Хосты**» и выберите узел виртуализированного ЦУ.
   2.2 Нажмите «**Управление**» → «**Активировать**» для активации хоста, находящегося в режиме обслуживания (Рис. 165).

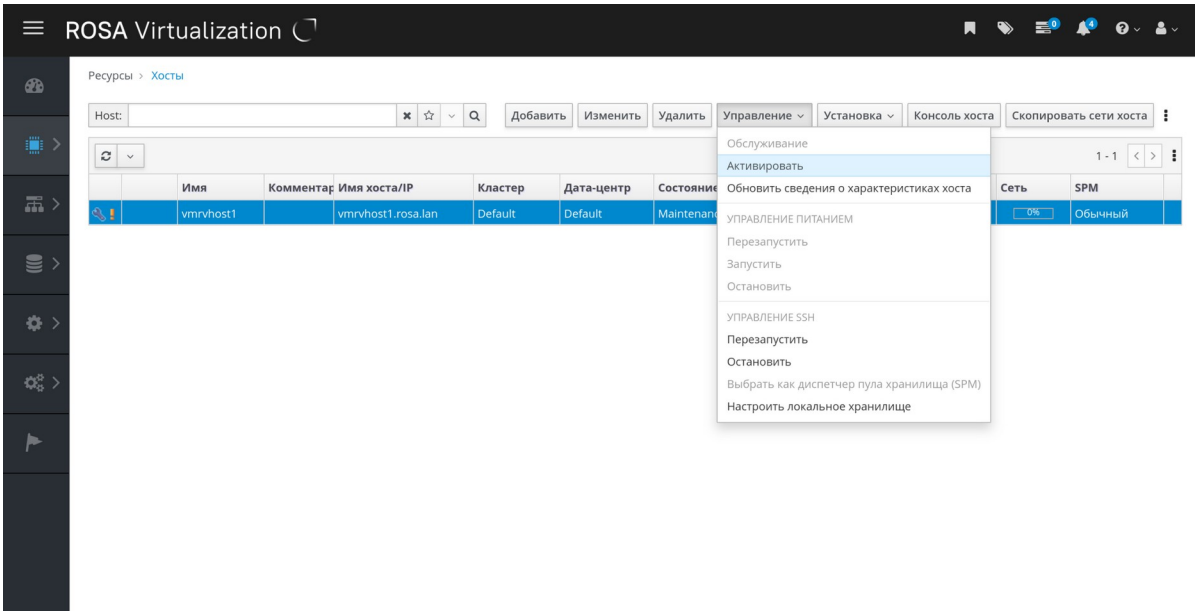

Рис. 165. Активация хоста, находящегося в режиме обслуживания

Активация локального режима обслуживания из командной строки:

1. Войдите в систему на узле виртуализированного ЦУ и переведите его в локальный режим обслуживания:

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

2. Выполнив необходимые задачи по обслуживанию, отключите режим обслуживания:

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

2. Активация глобального режима обслуживания

Включение глобального режима обслуживания останавливает работу агентов высокой доступности на всех узлах виртуализированного ЦУ в кластере.

Активация глобального режима обслуживания через интерфейс Портала администрирования:

1. Переведите все узлы виртуализированного ЦУ в глобальный режим обслуживания:
   1.1. На Портале администрирования нажмите «**Ресурсы**» → «**Хосты**» и выберите любой узел виртуализированного ЦУ.
   1.2. Нажмите значок «**Больше действий**» (⋮), затем нажмите «**Включить глобальное обслуживание высокой доступности**».

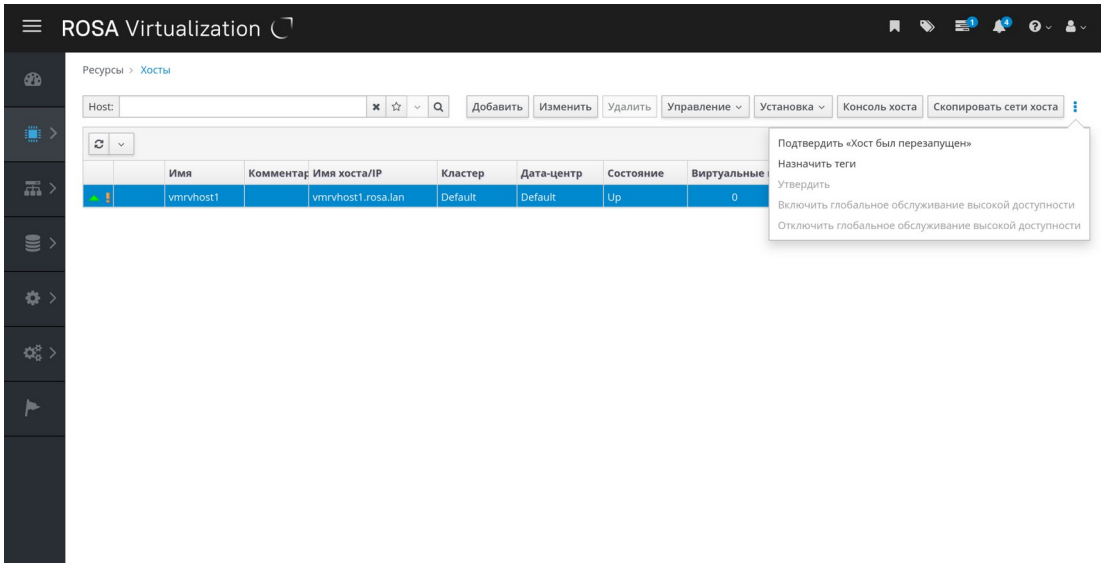

Рис. 166. Меню «Больше действий» в форме для управления хостами

2. Выполнив необходимые задачи по обслуживанию, отключите режим обслуживания:
   2.1 На Портале администрирования нажмите «**Ресурсы**» → «**Хосты**» и выберите любой узел виртуализированного ЦУ.
   2.2 Нажмите значок «**Больше действий**» (⋮), затем нажмите «**Отключить глобальное обслуживание высокой доступности**».

Активация глобального режима обслуживания из командной строки:

1. Войдите в систему на узле виртуализированного ЦУ и переведите его в глобальный режим обслуживания:

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

2. Выполнив необходимые задачи по обслуживанию, отключите режим обслуживания:

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

14.1.2. 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 выполните `hosted-engine --help`. Дополнительные сведения по отдельной команде можно просмотреть, выполнив

```
hosted-engine --<команда> --help.
```

1. Обновление конфигурации виртуализированного ЦУ

Для обновления конфигурации виртуализированного ЦУ используйте команду

```
# hosted-engine --set-shared-config.
```

Эта команда обновляет конфигурацию виртуализированного ЦУ в домене разделяемого хранилища после выполнения начального развёртывания.

Для просмотра значений текущей конфигурации используйте команду

```
# hosted-engine --get-shared-config.
```

Для получения списка всех доступных ключей конфигурации и их соответствующих типов введите следующую команду:

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

Где параметр `type` будет одним из указанных в Таблица 1.

Таблица 1. 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 новых значений перезапустите 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 развёрнуты после изменений конфигурации, использовали эти значения. Для активации новых значений на хосте разверните 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 перезапустите службу `ovirt-ha-broker`.

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 выполните следующие действия:

1. На узле виртуализированного ЦУ настройте желаемый адрес сервера SMTP для ключа `smtp-server`:

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

Примечание — для проверки обновлённых значений в конфигурации виртуализированного ЦУ выполните:

```
# hosted-engine --get-shared-config smtp-server --type=broker \
broker : smtp.example.com, type : broker
```

2. Проверьте конфигурация порта SMTP по умолчанию (порт 25):

```
# hosted-engine --get-shared-config smtp-port –type=broker
broker : 25, type : broker
```

3. Укажите 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
```

4. Укажите адрес, на котором будут приниматься почтовые уведомления. Для указания нескольких адресов используйте 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, измените состояние высокой доступности на узле виртуализированного ЦУ и проверьте, пришло ли почтовое уведомление. Изменить состояние, можно, например, переведя агента высокой доступности в режим обслуживания. Дополнительные сведения см. в разделе «Обслуживание виртуализированного ЦУ».

14.1.3. Настройка резервирования слотов памяти для виртуализированного ЦУ на дополнительных хостах

В случае, если СУСВ необходимо выключить, или выполнить её миграцию, объём 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 разделе «Добавление узлов виртуализированного ЦУ в СУСВ».

Настройка на дополнительных хостах слотов памяти, зарезервированных для виртуализированного ЦУ:

1. Нажмите **Ресурсы** → **Кластеры** и выберите кластер, в котором располагаются узлы виртуализированного ЦУ.
2. Нажмите **Изменить**.
3. Перейдите на вкладку «**Политика планирования**»
4. Нажмите + и выберите **HeSparesCount**.

5. Введите число дополнительных узлов виртуализированного ЦУ, на которых будет зарезервирован объём памяти, достаточный для запуска ВМ виртуализированного ЦУ.
6. Нажмите **OK**.

14.1.4. Добавление узлов виртуализированного ЦУ для СУСВ

Узлы виртуализированного ЦУ добавляются точно так же, как добавляются стандартные хосты, с дополнительным шагом по развёртыванию 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 минимум два узла 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, удалите существующую конфигурацию его виртуализированного ЦУ.

Порядок действий по добавлению узлов виртуализированного ЦУ для СУСВ

1. На портале администрирования нажмите **Ресурсы→Хосты**.
2. Нажмите **Добавить**.
3. Сведения по настройке параметров дополнительных хостов см. в Глава 10. Хосты.
4. В выпадающем списке выберите дата-центр и кластер хоста для нового хоста.
5. Введите **Имя** и **Адрес** нового хоста. Стандартный порт SSH, порт 22, будет автоматически введён в соответствующем поле.
6. Выберите метод аутентификации, который диспетчер будет использовать при доступе к хосту:
    - Для аутентификации по паролю введите пароль пользователя root.
    - Для аутентификации по открытому ключу, скопируйте ключ из поля **Открытый ключ SSH** в файл `/root/.ssh/authorized_keys` на хосте.
7. Перейдите на вкладку «**Виртуализированный ЦУ**».
8. Выберите **Развернуть**.
9. Нажмите **OK**.

14.1.5. 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, прикреплённые 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

1. Нажмите **Ресурсы → Хосты** и выберите хост.
2. Нажмите **Управление → Обслуживание** и нажмите **OK** для подтверждения перевода хоста в режим обслуживания (Рис. 164).
3. Нажмите **Установка → Переустановить**.
4. Перейдите на вкладку «**Виртуализированный ЦУ**» и в выпадающем списке выберите **Развернуть**.
5. Нажмите **OK**.

Хост будет переустановлен с конфигурацией виртуализированного ЦУ и затем будет помечен значком с короной на портале администрирования.

14.1.6. Загрузка СУСВ в режиме восстановления

В данном разделе описывается способ загрузки СУСВ в режим аварийного восстановления в случаях, когда ВМ не запускается.

1. Подключитесь к одному из узлов виртуализированного ЦУ (`host_address` — адрес хоста):

```
$ ssh root@host_address
```

2. Переведите виртуализированный ЦУ в глобальный режим обслуживания:

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

3. Проверьте наличие уже выполняющегося экземпляра ВМ диспетчера:

```
# hosted-engine --vm-status
```

4. Если экземпляр ВМ диспетчера уже выполняется, подключитесь к её хосту:

```
# ssh root@host_address
```

5. Выключите ВМ, выполнив в консоли команду:

```
# hosted-engine --vm-shutdown
```

Если ВМ не выключается, выполните следующую команду:

```
# hosted-engine --vm-poweroff
```

6. Запустите ВМ диспетчера в режиме паузы:

```
# hosted-engine  --vm-start-paused
```

7. Настройте временный пароль VNC:

```
# hosted-engine  --add-console-password
```

Данная команда выводит сведения, необходимые для выполнения входа на ВМ диспетчера с помощью консоли VNC.

1. Войдите в систему ВМ диспетчера с помощью VNC. ВМ диспетчера по-прежнему на паузе, поэтому кажется зависшей.
2. Возобновите работу ВМ диспетчера с помощью следующей команды, выполняемой на её хосте:

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

Примечание — 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, прочтите описание следующего шага по переходу в режим восстановления.

3. Загрузите ВМ диспетчера в режиме восстановления.
4. Отключите глобальный режим обслуживания

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

На СУСВ теперь можно выполнять работы по её восстановлению.

14.1.7. Удаление хоста из окружения виртуализированного ЦУ

Чтобы удалить узел виртуализированного ЦУ из окружения, переведите узел в режим обслуживания, сверните установку узла, и, опционально, удалите её. После остановки служб высокой доступности и удаления файлов конфигурации виртуализированного ЦУ узлом можно управлять, как обычным хостом.

Последовательность действий по удалению хоста из окружения виртуализированного ЦУ

1. На портале администрирования нажмите **Ресурсы → Хосты** и выберите узел виртуализированного ЦУ.
2. Нажмите **Управление → Обслуживание** и далее нажмите **OK**.
3. Нажмите **Установка → Переустановить**.
4. Перейдите на вкладку «**Виртуализированный ЦУ**» и в выпадающем списке выберите **Свернуть установку**. Данное действие останавливает работу служб **ovirt-ha-agent** и **ovirt-ha-broker** и удаляет файл конфигурации виртуализированного ЦУ.
5. Нажмите **OK**.
6. Опционально, нажмите **Удалить**. Будет запущено окно с подтверждением удаления хостов.

7. Нажмите **OK**.

14.1.8. Изменение полного доменного имени СУСВ в виртуализированном ЦУ

С помощью команды `ovirt-engine-rename` можно обновлять записи полного доменного имени (FQDN) диспетчера.

14.2. Резервные копии и миграция

В данной главе рассмотрен процесс создания резервных копий СУСВ и восстановление СУСВ из резервных копий.

14.2.1. Обзор: создание резервных копий СУСВ

Для регулярного резервного копирования СУСВ используйте утилиту **engine-backup**. Утилита создаёт резервные копии БД СУСВ и файлов конфигурации в одном файле, и утилиту можно запускать без прерывания работы службы **ovirt-engine**.

14.2.1.1 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 учётные данные для БД СУСВ. Полный список параметров и их назначение можно просмотреть, выполнив **engine-backup --help**.

Базовые параметры команды engine-backup:

`--mode`

Указывает, что выполняет команда: операцию создания резервной копии или операцию 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 рез. копия в режиме создания резервных копий, и из которого будут читаться данные в режиме восстановления. По умолчанию путь равен **/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 путь равен **/var/log/ovirt-engine-backup/** .

`--scope`

Указывает область данных, включаемых в создание или восстановление резервной копии. Есть 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

Следующие параметры доступны только при использовании команды **engine-backup** в режиме **restore**. Синтаксис параметров, указываемый ниже, применяется при восстановлении БД СУСВ. Те же параметры существуют для восстановления БД хранилища данных. Синтаксис параметров для хранилища данных см. в выводе `engine-backup -help`.

`--provision-db`

Создаёт БД PostgreSQL, в которую будет восстанавливаться резервная копия БД СУСВ. Этот параметр является обязательным при восстановлении из резервной копии на удалённом 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`

Создаёт БД для всех дампов памяти, включённых в архив. Если параметр включён, это является значением по умолчанию.

`--change-db-credentials`

Даёт возможность указать другие учётные данные при восстановлении БД СУСВ с учётными данными, отличными от сохранённых непосредственно в архиве. Дополнительные параметры, необходимые данному параметру, см. в выводе `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.

14.2.1.2 Создание резервных копий с помощью команды engine-backup

Создавать резервные копии СУСВ при активной СУСВ можно с помощью команды **engine-backup**.

Добавьте один из следующих аргументов к параметру **--scope** для указания, что именно требуется поместить в архив:

`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

Указывать параметр **--scope** можно несколько раз.

Команду **engine-backup** можно настроить на создание резервной копии для дополнительных файлов. При восстановлении эта команда восстанавливает все файлы из архива.

Примечание — 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 рез. копию файловой системы.

Примечание — Полные сведения о команде **engine-backup** можно получить в выводе **engine-backup --help** на машине диспетчера.

Последовательность действий для создания резервных копий с помощью команды engine-backup

1. Войдите в систему на машине СУСВ.
2. Создайте резервную копию:

```
# engine-backup
```

Следующие параметры применяются по умолчанию:

```
--scope=all
--mode=backup
```

Эта команда создаёт 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 используйте `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:

1. Создайте каталог для хранения специальных параметров конфигурации команды **engine-backup**:

```
# mkdir -p /etc/ovirt-engine-backup/engine-backup-config.d
```

2. Создайте 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"
```

3. При запуске команды **engine-backup** используйте **--scope=files**. В создание и восстановление из резервной копии входят **/etc/chrony.conf**, **/etc/ntp.conf** и **/etc/ovirt-engine-backup**.

14.2.1.3 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 ROSA Virtualization, поверх уже имеющейся установки ROSA Virtualization, а также использовать локальные или удалённые БД.

14.2.1.4 Восстановление из резервной копии в свежую установку

Команду `engine-backup` можно использовать для восстановления из резервной копии в свежую установку диспетчера ROSA Virtualization. Нижеописанная процедура должна выполняться на машине с установленной хост-системой, но где ещё 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:

1. Выполните вход в систему на машине диспетчера. Если восстанавливается БД СУСВ на удалённый хост, то необходимо также войти в систему на этом хосте и выполнить там требуемые действия. Аналогичным образом, при восстановлении БД хранилища данных на удалённый хост, на этом хосте необходимо войти в систему и выполнить требуемые действия.
2. Выполните полное восстановление, либо только восстановление резервной копии БД.

a. 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, укажите дополнительную БД:

```
# engine-backup --mode=restore --file=file_name \
--log=log_file_name --provision-db -- provision-dwh-db
```

b. При восстановлении резервной копии только БД восстановите 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.
```

3. Для создания конфигурации восстановленного диспетчера запустите команду и следуйте подсказкам:

```
# engine-setup
```

СУСВ был восстановлен в версии, сохранённой в резервной копии.

14.2.1.5 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, внесённые 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

1. Войдите в систему на машине СУСВ.

2. Удалите файлы конфигурации и очистите 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.

3. Восстановление полной резервной копии или резервной копии только БД. Нет необходимости создавать новую БД или указывать учётные записи, т.к. пользователи и БД уже существуют.

a. Восстановление из полной резервной копии:

```
# engine-backup --mode=restore --file=file_name \
--log=log_file_name --restore- permissions
```

b. 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.
```

4. Повторная настройка диспетчера:

```
# engine-setup
```

14.2.1.6 Восстановление из резервной копии с использованием других учётных данных

Команда **engine-backup** может восстановить резервную копию на машину, где СУСВ уже ранее была установлена и настроена, в ситуации, когда данные учётных 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 её из системы и не удаляет пользователей-владельцев этой БД. Поэтому нет необходимости создавать новую БД или указывать данные учётных записей. Тем не менее, если данные учётной 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 учётных данных:

1. Выполните вход в систему на машине СУСВ.
2. Для удаления файлов конфигурации диспетчера и очистки БД СУСВ запустите следующую команду и следуйте подсказкам:

```
# engine-cleanup
```

3. Смените пароль владельца БД engine, если данные его учётной записи неизвестны:

a. Войдите в командную строку postgresql:

```
# su - postgres -c 'psql'
```

b. Смените пароль пользователя-владельца БД engine:

```
postgres=# alter role user_name encrypted password 'new_password';
```

В случае необходимости повторите эти действия для пользователя-владельца БД **ovirt_engine_history**.

4. Восстановите полный архив или архив только с БД с параметром `--change-db-credentials` для передачи учётных 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 защищённой передачи паролей утилите `engine-backup` без необходимости вводить пароли в интерактивном запросе командной строки.

Восстановите полную резервную копию:

```
# engine-backup --mode=restore --file=file_name --log=log_file_name \
--change-db- credentials --db-host=database_location –db \
name=database_name --db-user=engine --db-password  --no-restore-permissions
```

Если в составе полного восстановления также восстанавливается БД хранилища данных, то необходимо включить данные учётных 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 выполните следующую команду:

```
# engine-setup
```

14.2.1.7 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. Выполняйте эти действия для таких задач, как миграция окружений в новые домены хранилищ виртуализированного ЦУ с другими типами хранилищ.

При указании файла резервной копии во время развёртывания архив восстанавливается на новой СУСВ с новым доменом хранилища виртуализированного ЦУ. Старый диспетчер удаляется, а старый домен хранилища переименовывается и может быть удалён вручную после проверки корректности работы нового окружения. Настоятельно рекомендуется выполнять развёртывание на свежем хосте; если в архиве резервной копии окружения присутствовал хост, использованный для развёртывания, он будет удалён из восстановленной БД для избегания конфликтов в новом окружении. При развёртывании на новом хосте новому хосту нужно присвоить новое имя. Повторное использование имени существующего хоста, включённого в резервную копию, может привести к конфликтам в новом окружении.

Создание резервной копии виртуализированного ЦУ

Последовательность действий по созданию и восстановлению резервной копии включает в себя следующие ключевые шаги:

1. Создайте резервную копию исходной СУСВ с помощью утилиты engine-backup.
2. Разверните новый виртуализированный ЦУ и восстановите СУСВ из резервной копии.
3. Подключите репозитории СУСВ на новой СУСВ.
4. Переустановите узлы виртуализированного ЦУ для обновления их конфигурации.
5. Удалите домен хранилищ старого виртуализированного ЦУ.

Данная процедура предполагает, что у администратора есть доступ к исходному диспетчера и права на внесение изменений.

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 обновлённой 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 ещё не является диспетчером пула хранилища, передайте 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:

1. Удалите конфигурацию виртуализированного ЦУ на узле (но не удаляйте узел из окружения). См. раздел **Удаление хоста из виртуализированного ЦУ**.
2. Добавьте новый обычный хост. См. раздел **Добавление стандартных хостов СУСВ**.

14.2.1.7.1 Создание резервной копии исходной СУСВ

Создайте резервную копию исходной СУСВ с помощью команды **engine-backup** и скопируйте файл архива резервной копии в отдельное местоположение, чтобы к нему сохранялся доступ в любой момент работы.

Дополнительные сведения о параметрах **engine-backup --mode=backup** смотрите в разделе **Создание и восстановление резервных копий СУСВ** в *Руководстве администратора*.

Последовательность действий по созданию резервной копии исходной СУСВ

1. Выполните вход в систему на одном из узлов виртуализированного ЦУ и поместите окружение в глобальный режим обслуживания:

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

2. Выполните вход в систему на исходной СУСВ и остановите 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.

3. Выполните 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
```

4. Скопируйте 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/
```

5. Выполните вход в систему на одном из узлов виртуализированного ЦУ и выключите исходную СУСВ:

```
# hosted-engine --vm-shutdown
```

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

14.2.1.7.2 Восстановление резервной копии в новом виртуализированном ЦУ

Запустите сценарий **hosted-engine** на новом хосте и используйте параметр **--restore-from-file=*path/to/file_name*** для восстановления резервной копии диспетчера во время развёртывания.

Примечание — Если используется хранилище iSCSI, и цель iSCSI фильтрует подключения согласно списку управления доступом (ACL) инициатора, то развёртывание может закончиться неудачно с ошибкой **STORAGE_DOMAIN_UNREACHABLE**. Для предотвращения этой ошибки необходимо обновить конфигурацию iSCSI до начала развёртывания виртуализированного ЦУ:

- Если выполняется повторное развёртывание 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 отображённым на цель iSCSI, либо необходимо его обновить до нового IQN, если это применимо.

- При развёртывании на свежем хосте необходимо обновить конфигурацию цели iSCSI для принятия подключений с этого хоста.

Обратите 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

1. Скопируйте 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/
```

2. Войдите в систему на новом хосте.

3. Чтобы избежать обрыва сеанса в случае неполадок с сетью или терминалом, для запуска сценария используйте оконный менеджер **tmux**.
   Запустите **tmux**, используя следующую команду в консоли:

```
# tmux
```

4. Запустите 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 развёртывание в любой момент, используйте **CTRL+D**.

5. Чтобы начать развёртывание, выберите Yes.
6. Настройте сеть. Сценарий обнаружит сетевые контроллеры, пригодные для использования в качестве моста управления окружением.
7. При необходимости использовать настраиваемое программно-аппаратное устройство для установки ВМ, укажите путь к архиву OVA. В противном случае оставьте поле пустым.
8. Введите пароль root для СУСВ.
9. Введите открытый ключ SSH, с помощью которого можно будет выполнить вход в систему диспетчера в качестве пользователя root, и укажите, нужно ли разрешать доступ с использованием SSH для root.
10. Введите конфигурацию памяти и ЦП для ВМ.
11. Укажите адрес MAC для ВМ диспетчера, или примите случайно созданный адрес. Если ВМ должна получать адрес IP с помощью DHCP, убедитесь в наличии действительного зарезервированного DHCP для этого адреса MAC. Сценарий развёртывания не настраивает сервер DHCP.
12. Укажите сетевые параметры ВМ. При указании статического IP укажите 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).

13. Укажите, нужно ли добавлять запись ВМ диспетчера и запись базового хоста в файл **/etc/hosts** на ВМ. Убедитесь в разрешаемости имён хостов.
14. Укажите имя и номер порта TCP сервера SMTP, почтовый адрес для отсылки уведомлений и список адресов-получателей этих сообщений, через запятую.
15. Укажите пароль пользователя **admin@internal** для доступа к порталу администрирования. Сценарий создаст ВМ.

Примечание — Если в связи с отсутствующей требуемой сетью или аналогичной проблемой хост перейдёт в нерабочее состояние, процесс развёртывания 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 даёт возможность администратору:

- Подключиться к порталу администрирования с помощью предоставленного URL.

- Оценить ситуацию, понять, почему хост в нерабочем состоянии и исправить всё, что необходимо исправить. Если, например, данное развёртывание 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 всё будет починено, и хост получит статус «работоспособен», удалите временный файл блокировки, указанный в системном сообщении, приведённом выше.

16. Настройте тип используемого хранилища:
    - Для NFS укажите версию, полный адрес и путь до хранилища, а также любые параметры монтирования.

Примечание — Не используйте точку монтирования старого домена хранилища виртуализированного ЦУ для нового домена хранилища, т.к. присутствует риск потери данных.

- Укажите сведения о портале для iSCSI и выберите цель и LUN из списка автоматически обнаруженных. Во время развёртывания 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 развёртывания виртуализированного ЦУ.

- Для хранилища Gluster укажите полный адрес и путь до хранилища, вместе с любыми параметрами монтирования.

Примечание — Не используйте точку монтирования строго домена хранилища виртуализированного ЦУ для нового домена хранилища, т.к. присутствует риск потери данных ВМ.

Примечание — 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 выберите 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 разделе «Повторное использование LUN» Руководства администратора.

17. Укажите размер диска диспетчера.

Сценарий продолжит своё выполнение до завершения развёртывания.

18. В процессе развёртывания будут изменены ключи SSH диспетчера. Чтобы разрешить клиентским машинам доступ к новому диспетчеру без ошибок, связанных с SSH, удалите запись исходного диспетчера из файла **.ssh/known_hosts** на любой из клиентских машин, ранее имевших доступ к исходному диспетчеру.

После завершения развёртывания выполните вход в систему на ВМ новой СУСВ и подключите необходимые репозитории.

14.2.1.7.3 Повторная установка хостов

Переустановите хосты ROSA Virtualization на портале администрирования. Эти действия 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, прикреплённые 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, переустанавливайте хост в момент его относительно низкой нагрузки.
- Убедитесь в том, что объём 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 выключите некоторые или все ВМ.

- Перед началом переустановки убедитесь в том, что в кластере находится более одного хоста. Не пытайтесь начать переустановку всех хостов одновременно. Один хост всегда должен быть доступен для выполнения задач диспетчера пула хранилища (SPM).

Последовательность действий по повторной установка хостов

1. Нажмите **Ресурсы → Хосты** и выберите хосты.
2. Нажмите **Управление → Обслуживание** и **OK**.
3. Нажмите **Установка → Переустановить**. Будет открыто окно **Установить хост**.
4. Перейдите на вкладку «**Виртуализированный ЦУ**» и в выпадающем списке выберите **Развернуть**.
5. Для переустановки хоста нажмите **OK**.

После окончания процесса переустановки хоста, когда статус хоста снова будет равен «Работоспособен», можно выполнить миграцию ВМ обратно на хост.

Примечание — После выполнения регистрации хоста ROSA Virtualization в СУСВ статус этого хоста на портале администрирования может ошибочно показывать «Сбой установки». Нажмите **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 удалён на случай, если при восстановлении случится сбой. После подтверждения того, что окружение работает нормально, старый домен можно удалить.

14.2.1.7.4 Удаление домена хранилища

В ЦОД имеется домен хранилища, который необходимо удалить из виртуализированного окружения.

Последовательность действий по удалению домена хранилища

1. Нажмите **Хранилище → Домены**.
2. Переведите домен хранилища в режим обслуживания и отсоедините его:
   a. Нажмите на имя домена хранилища. Будет открыт подробный просмотр.
   b. Перейдите на вкладку **«Дата-центр»**.
   c. Нажмите **Обслуживание**, затем нажмите **OK**.
   d. Нажмите **Отсоединить**, затем нажмите **OK**.
3. Нажмите **Удалить**.
4. Опционально, выберите **Форматировать домен, т.е. содержимое хранилища будет потеряно** и поставьте галочку для удаления содержимого домена.
5. Нажмите **OK**.

Домен хранилища будет навсегда удалён из окружения.

14.2.1.7.5 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 развёртывания 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 развёртывание на свежем хосте; если хост, используемый для развёртывания, существовал в окружении, для которого создавалась резервная копия, то он будет удалён из восстановленной БД для избежание конфликтов в новом окружении. Если развёртывание выполняется на новом хосте, этому хосту необходимо присвоить уникальное имя. Повторное использование имени хоста, включённого в резервную копию, может привести к конфликтам в новом окружении.

Последовательность восстановления виртуализированного ЦУ состоит из следующих ключевых действий:

1. Развёртывание нового виртуализированного ЦУ и восстановление резервной копии.
2. Подключение репозиториев СУСВ на новой ВМ СУСВ.
3. Переустановка узлов виртуализированного ЦУ для обновления их конфигурации.
4. 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.

14.2.1.7.6 Восстановление из резервной копии на новом виртуализированном ЦУ

Запустите на новом хосте сценарий **hosted-engine** и с помощью параметра **--restore-from-file=*path/to/file_name*** восстановите диспетчер из резервной копии во время развёртывания.

Примечание — Если используется хранилище iSCSI, и цель iSCSI фильтрует подключения согласно списку управления доступом (ACL) инициатора, то развёртывание может закончиться неудачно с ошибкой **STORAGE_DOMAIN_UNREACHABLE**. Для предотвращения этой ошибки необходимо обновить конфигурацию iSCSI до начала развёртывания виртуализированного ЦУ:

- Если выполняется повторное развёртывание 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 отображённым на цель iSCSI, либо необходимо его обновить до нового IQN, если это применимо.
- При развёртывании на свежем хосте необходимо обновить конфигурацию цели iSCSI для принятия подключений с этого хоста.

Обратите 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

1. Скопируйте 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/
```

2. Выполните вход в систему на новом хосте.
3. Чтобы избежать обрыва сеанса в случае неполадок с сетью или терминалом, для запуска сценария используйте оконный менеджер tmux. Запустите tmux командой:

```
# tmux
```

4. Запустите 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 развёртывание в любой момент, используйте **CTRL+D**.

5. Чтобы начать развёртывание, выберите **Yes**.
6. Настройте сеть. Сценарий обнаруживает сетевые контроллеры, пригодные к использованию в качестве моста для управления окружением.
7. При необходимости использовать настраиваемое программно-аппаратное устройство для установки ВМ, укажите путь к архиву OVA. В противном случае оставьте поле пустым.
8. Введите пароль root для диспетчера.
9. Введите открытый ключ SSH, с помощью которого можно будет выполнить вход в систему диспетчера в качестве пользователя root, и укажите, нужно ли разрешать доступ с использованием SSH для root.
10. Введите конфигурацию памяти и ЦП для ВМ.
11. Укажите адрес MAC для ВМ диспетчера, или примите случайно созданный адрес. Если ВМ должна получать адрес IP с помощью DHCP, убедитесь в наличии действительного зарезервированного DHCP для этого адреса MAC. Сценарий развёртывания не настраивает сервер DHCP.
12. Укажите сетевые параметры ВМ. При указании статического IP укажите 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).

13. Укажите, нужно ли добавлять запись ВМ диспетчера и запись базового хоста в файл `/etc/hosts` на ВМ. Убедитесь в разрешаемости имён хостов.
14. Укажите имя и номер порта TCP сервера SMTP, почтовый адрес для отсылки уведомлений и список адресов-получателей этих сообщений, через запятую.
15. Укажите пароль пользователя admin@internal для доступа к порталу администрирования. Сценарий создаст ВМ.

Примечание — Если в связи с отсутствующей требуемой сетью или аналогичной проблемой хост перейдёт в нерабочее состояние, процесс развёртывания 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 даёт возможность администратору:

- Подключиться к порталу администрирования с помощью предоставленного URL.
- Оценить ситуацию, понять, почему хост в нерабочем состоянии и исправить всё, что необходимо исправить. Если, например, данное развёртывание 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 всё будет починено, и хост получит статус «работоспособен», удалите временный файл блокировки, указанный в системном сообщении, приведённом выше. Процесс развёртывания продолжается.

16. Выберите тип используемого хранилища:

a. Для NFS укажите версию, полный адрес и путь до хранилища, а также любые параметры монтирования.

Примечание — Не используйте точку монтирования старого домена хранилища виртуализированного ЦУ для нового домена, т.к. существует риск потери данных ВМ.

b. Укажите сведения о портале для iSCSI и выберите цель и LUN из списка автоматически обнаруженных. Во время развёртывания 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 развёртывания виртуализированного ЦУ.

c. Для хранилища Gluster укажите полный адрес и путь до хранилища, вместе с любыми параметрами монтирования.

Примечание — Не используйте точку монтирования старого домена хранилища виртуализированного ЦУ для нового домена, т.к. существует риск потери данных ВМ

Примечание — Поддерживаются только хранилища Gluster с типом replica 1 и replica 3. Убедитесь, что том настроен следующим образом:

```
  gluster volume set VOLUME_NAME group virt
  luster 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
```

d. Для Fibre Channel выберите LUN из списка автоматически обнаруженных. Адаптеры шины хоста должны быть заранее настроены и подключены, а LUN не должен содержать никаких существующих данных.

17. Укажите размер диска диспетчера.
    Сценарий продолжит своё выполнение до завершения развёртывания.
18. В процессе развёртывания будут изменены ключи SSH диспетчера. Чтобы разрешить клиентским машинам доступ к новому диспетчеру без ошибок, связанных с SSH, удалите запись исходного диспетчера из файла .ssh/known_hosts на любой из клиентских машин, ранее имевших доступ к исходному диспетчеру.

После завершения развёртывания выполните вход в систему на ВМ новой СУСВ и подключите необходимые репозитории.

14.2.1.7.7 Переустановка хостов

Переустановите хосты ROSA Virtualization на портале администрирования. Эти действия включают 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, переустанавливайте хост в момент его относительно низкой нагрузки.
- Убедитесь в том, что объём 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 выключите некоторые или все ВМ.
- Перед началом переустановки убедитесь в том, что в кластере находится более одного хоста. Не пытайтесь начать переустановку всех хостов одновременно. Один хост всегда должен быть доступен для выполнения задач диспетчера пула хранилища (SPM).

Последовательность действий по переустановке хостов:

1. Нажмите **Ресурсы → Хосты** и выберите хосты.
2. Нажмите **Управление → Обслуживание** и **ОК**.

3. Нажмите **Установка → Переустановить**. Будет открыто окно **Установить хост**.
4. Перейдите на вкладку «**Виртуализированный ЦУ**» и в выпадающем списке выберите **Развернуть**.
5. Для переустановки хоста нажмите **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 ROSA Virtualization в СУСВ статус этого хоста на портале администрирования может ошибочно показывать «Сбой установки». Нажмите «**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 удалён на случай, если при восстановлении случится сбой. После подтверждения того, что окружение работает нормально, старый домен можно удалить.

14.2.1.7.8 Удаление домена хранилища

В ЦОД имеется домен хранилища, который необходимо удалить из виртуализированного окружения.

Последовательность действий по удалению домена хранилища

1. Нажмите «**Хранилище» → «Домены»**.
2. Переведите домен хранилища в режим обслуживания и отсоедините его:
a. Нажмите на имя домена хранилища. Будет открыт подробный просмотр.
b. Перейдите на вкладку «**Дата-центр**».
c. Нажмите **Обслуживание**, затем нажмите **OK**.
d. Нажмите **Отсоединить**, затем нажмите **OK**.
3. Нажмите Удалить.
4. Опционально, выберите «**Форматировать домен**», т.е. содержимое хранилища будет потеряно и поставьте галочку для удаления содержимого домена.
5. Нажмите **OK**.

Домен хранилища будет навсегда удалён из окружения.

14.2.1.8 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).

Процесс восстановления виртуализированного ЦУ до предыдущего состояния состоит из следующих шагов:

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

Дополнительные сведения о параметрах **engine-backup --mode=restore** смотрите в разделе **Создание и восстановление виртуализированного ЦУ из резервной копии**.

14.2.1.8.1 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

1. Выполните вход в систему на одном из узлов виртуализированного ЦУ и поместите окружение в глобальный режим обслуживания:

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

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

```
# hosted-engine --vm-status
```

Должно появиться сообщение, указывающее, что окружение находится в глобальном режиме обслуживания.

14.2.1.8.2 Восстановление из резервной копии для перезаписи существующей установки

С помощью команды `engine-backup` можно восстановить резервную копию на машине, где виртуализированного 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, внесённые 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

1. Выполните вход в систему на ВМ СУСВ.
2. Удалите файлы конфигурации и очистите 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.

3. Восстановление полной резервной копии или резервной копии только БД. Нет необходимости создавать новую БД или указывать учётные записи, т.к. пользователи и БД уже существуют.
   a. Восстановление из полной резервной копии:

```
# engine-backup --mode=restore --file=file_name --log=log_file_name \
--restore- permissions
```

   b. 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.
```

4. Повторная настройка диспетчера:

```
# engine-setup
```

14.2.1.8.3 Отключение глобального режима обслуживания

Последовательность действий по отключению глобального режима обслуживания

1. Войдите в систему ВМ СУСВ и выключите её.
2. Войдите в систему на одном из узлов виртуализированного ЦУ и отключите 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.

3. Убедитесь 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"}
```

Примечание — Пока ВМ не начала работу и только загружается, ЦУ ещё не запущен и может иметь один из следующих статусов:

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

В этом случае подождите несколько минут и повторите попытку.

После того, как окружение снова начало работу, можно запустить все ранее остановленные ВМ и проверить корректность поведения ресурсов в окружении.

14.2.2. 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 её к существующей БД хранилища данных (**ovirt_engine_history**).
- Можно выполнить миграцию БД хранилища данных с машины СУСВ, а затем перенести службу Data Warehouse.

14.2.2.1. Миграция БД хранилища данных на отдельную машину

До начала миграции службы Data Warehouse перенесите БД хранилища данных (**ovirt_engine_history**). Для создания резервной копии БД и восстановления её на машине новой БД используйте команду **engine-backup**. Дополнительные сведения об engine-backup смотрите в выводе **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 выполните следующие действия:

1. Создайте 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
```

2. Скопируйте файл резервной копии с диспетчера на новую машину:

```
# scp /tmp/file_name root@new.dwh.server.com:/tmp
```

3. Установите engine-backup на новой машине:

```
# dnf install ovirt-engine-tools-backup
```

4. Установите пакет сервера PostgreSQL:

```
# dnf install postgresql-server postgresql-contrib
```

5. Инициализируйте БД PostgreSQL, запустите службу postgresql и настройте запуск этой службы при загрузке:

```
# su - postgres -c 'initdb'
# systemctl enable postgresql
# systemctl start postgresql
```

6. Восстановите БД хранилища данных на новой машине. Файл 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 выполните миграцию службы Data Warehouse.

14.2.2.2. 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.

Обратите 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, см. раздел **Миграция БД хранилища данных на отдельную машину**.

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 разделе **Миграция БД хранилища данных на отдельную машину**, то файл резервной копии содержит эти данные, т.к. они были созданы во время настройки БД на этой машине.

Инструкция состоит из нескольких шагов:

1. Настройка новой машины хранилища данных.
2. Остановка службы Data Warehouse на машине диспетчера.
3. Создание конфигурации на новой машине хранилища данных.
4. Отключение пакета Data Warehouse на машине диспетчера.

14.2.2.2.1 Остановка службы Data Warehouse на машине диспетчера

Последовательность действий по остановке службы Data Warehouse на машине диспетчера:

1. Остановка службы Data Warehouse:

```
# systemctl stop ovirt-engine-dwhd.service
```

2. Если БД размещается на удалённой машине, то необходимо предоставить доступ, вручную отредактировав файл postgres.conf. Измените строку listen_addresses в файле /var/lib/pgsql/data/postgresql.conf следующим образом:

```
listen_addresses = '*'
```

Если эта строка отсутствует или была закомментирована, добавьте её вручную.

Если БД размещается на машине диспетчера и была настроена во время чистой установки СУСВ, то доступ предоставляется по умолчанию.

3. Перезапустите службу postgresql:

```
# systemctl restart postgresql
```

14.2.2.2.2 Настройка новой машины хранилища данных

Порядок шагов, или параметры, представленные в данном разделе, могут отличаться, в зависимости от имеющегося окружения.

1. Если на одну и ту же машину переносится и БД **ovirt_engine_history** и служба Data Warehouse, выполните команду, указанную ниже. В противном случае переходите к следующему шагу.

```
# sed -i '/^ENGINE_DB_/d' \
/etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-database.conf
# sed -i \
-e 's;^\(OVESETUP_ENGINE_CORE/enable=bool\):True;\1:False;' \
-e '/^OVESETUP_CONFIG\/fqdn/d' \
/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

2. Удалите 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
```

3. Для начала создания конфигурации хранилища данных на машине запустите команду engine-setup:

```
# engine-setup
```

4. Нажмите Ввод для принятия автоматически определённого имени хоста, либо введите своё имя хоста и нажмите Ввод:

```
          Host fully qualified DNS name of this server [autodetected host name]:
```

5. Для автоматической настройки межсетевого экрана нажмите Ввод, либо введите **No** и нажмите Ввод 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]:
```

Если была выбрана автоматическая настройка межсетевого экрана, но активные диспетчеры межсетевых экранов отсутствуют, то будет предложено выбрать диспетчер из списка поддерживаемых возможностей. Введите имя диспетчера межсетевого экрана и нажмите **Ввод**. Это применимо и в тех случаях, когда доступен только один диспетчер межсетевых экранов.

6. Введите полное доменное имя и пароль диспетчера. Для принятия значений по умолчанию в каждом из других полей, нажмите **Ввод**:

```
          Host fully qualified DNS name of the engine server []: engine-fqdn
          Setup needs to do some actions on the remote engine server. Either
    automatically, using ssh as root to access it, or you will be prompted to
    manually perform each such action.
          Please choose one of the following:
          - 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
```

7. Укажите полное доменное имя и пароль машины БД диспетчера. Для принятия значений по умолчанию в каждом из других полей, нажмите **Ввод**:

```
          Engine database host []: manager-db-fqdn
```

```
        Engine database port [5432]:
        Engine database secured connection (Yes, No) [No]: Engine database name
    [engine]:
        Engine database user [engine]: Engine database password: password
```

8. Подтвердите параметры установки:

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

Теперь служба Data Warehouse настроена на удалённой машине. Приступайте к отключению службы Data Warehouse на машине диспетчера.

14.2.2.2.3 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:

1. Перезапустите диспетчер на машине диспетчера:

```
# service ovirt-engine restart
```

2. Для изменения файла `/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf` и указания параметра `False`, выполните 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
```

3. Отключите службу Data Warehouse:

```
# systemctl disable ovirt-engine-dwhd.service
```

4. Удалите 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.

14.2.3. Создание и восстановление ВМ из резервных копий с использованием домена хранения резервных копий

14.2.3.1. 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 резервный копий. Домен хранения резервных копий отличается от других доменов тем, что все ВМ в домене хранения резервных копий находятся в выключенном состоянии. В домене хранения резервных копий виртуальные машины выполняться не могут.

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

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

Как и в случае других типов доменов хранения, домены хранения резервных копий можно присоединять к 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.

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

- В дата-центре может существовать несколько доменов хранения резервных копий, но только один домен экспорта. Домен хранения резервных копий можно выделить для создания резервных копий и восстановления в аварийных ситуациях.
- 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:

- Диски любых ВМ или шаблонов, располагающихся в домене хранения резервных копий, должны размещаться в этом же домене.
- Все ВМ в домене хранения должны быть выключены перед тем, как этот домен можно будет сделать доменом хранения резервных копий.
- ВМ, хранящуюся в домене хранения резервных копий, нельзя запустить, так как при этом будет выполняться обработка дисковых данных.

- Домены хранения резервных копий не предназначены для томов памяти, так как тома памяти поддерживаются только активными ВМ.
- В домене хранения резервных копий нельзя выполнить предварительный просмотр ВМ.
- Динамическая миграция ВМ в домен хранения резервных копий невозможна.
- Домен хранения резервных копий не может быть **главным** доменом.
- Домен виртуализированного ЦУ нельзя сделать доменом хранения резервных копий.
- Не используйте домен хранилищ по умолчанию в качестве домена хранения резервных копий.

14.2.3.2. 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:

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

Домен стал доменом хранения резервных копий.

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

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

Последовательность действий: создание резервной копии виртуальной машины:

1. Создайте домен хранения резервных копий. См. раздел **Настройка домена хранения данных в качестве домена хранения резервных копий**.
2. Создайте новую ВМ на основе ВМ, для которой нужно создать резервную копию:
   a. Для создания резервной копии снимка, сначала на базе этого снимка создайте ВМ.
   b. Для создания резервной копии ВМ, машину сначала нужно клонировать. И перед тем, как продолжить, убедитесь в том, что

клон выключен.

3. Экспортируйте новую ВМ в домен хранения резервных копий.
4. Последовательность действий: восстановление ВМ из резервной копии
5. Убедитесь в том, что домен хранения резервных копий, в котором хранится резервная копия ВМ, присоединён к дата-центру.
6. Импортируйте ВМ из домена хранения резервных копий.

14.3. Обновление сертификатов до истечения срока их действия

В системе ROSA Virtualization до версии 3.0 срок действия всех сертификатов равнялся 398 дням. Начиная с ROSA Virtualization версии 3.0, срок жизни самоподписанных внутренних сертификатов между гипервизорами и диспетчером будет равняться 10 годам.

Примечание — Не пропускайте сроков обновления сертификатов. Просроченный сертификат приводит к тому, что диспетчер и хосты перестают отвечать, а процесс восстановления занимает время и не защищён от ошибок.

Последовательность действий по обновлению сертификатов:

1. Обновление сертификатов хоста:
   a. На портале администрирования нажмите «**Ресурсы**» → «**Хосты**».
   b. Нажмите «**Управление**» → «**Обслуживание**» и **ОК**. ВМ должны автоматически мигрировать с хоста. В случае прикреплённых ВМ, или других причин для невозможности миграции, их необходимо выключить вручную.
   c. Когда на хосте не останется ВМ и после помещения хоста в режим обслуживания, нажмите «**Установка**» → «**Регистрация сертификата**».
   d. После завершения регистрации нажмите «**Управление**» → «**Активировать**».
2. Обновите сертификаты диспетчера:
   a. Только для виртуализированного ЦУ: войдите в систему на хосте и переведите его в глобальный режим обслуживания.

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

   b. Виртуализированный ЦУ и отдельно размещённый диспетчер: войдите в систему на диспетчере и выполните engine-setup.

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

Сценарий **engine-setup** задаст вопросы по конфигурации. Отвечайте согласно вашей ситуации, либо используйте файл с ответами.

   c. Введите Yes после нижеследующего вопроса engine-setup:

```
        Renew certificates? (Yes, No) [Yes]:
```

   d. Только для виртуализированного ЦУ: войдите в систему на хосте и отключите глобальный режим обслуживания:

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

14.4. Автоматизация задач конфигурирования с помощью Ansible

Ansible — это средство автоматизации, используемое при настройке систем, развёртывании ПО и выполнения последовательных обновлений. В ROSA Virtualization включена ограниченная версия Ansible для автоматизации таких задач пост-установки, как установка и настройка дата-центров, управление пользователями или действия с виртуальными машинами.

По сравнению с различными REST API и SDK, Ansible предоставляет более простой способ автоматизации конфигурирования системы ROSA Virtualization

Различные варианты установки Ansible, а также сведения по работе с Ansible смотрите в документации Ansible.

14.5. Пользователи и роли

14.5.1. Что такое пользователи

В системе ROSA Virtualization существует два типа доменов пользователей: локальный домен и внешний домен. Во время процесса установки виртуализированного ЦУ создаётся 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**. Учётные записи, создаваемые в локальных доменах, называются «локальными пользователями». Также к окружению ROSA Virtualization можно присоединять внешние серверы каталогов, такие, как Active Directory, OpenLDAP и многие другие поддерживаемые серверы, и использовать их в качестве внешних доменов. Учётные 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, как, например, кластеры и дата-центры.

14.5.2. Введение в серверы каталогов

Во время установки СУСВ создаёт пользователя `admin` в домене `internal`. Этот пользователь также называется **admin@internal**. Назначение этой учётной 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, учётную запись **admin@internal** можно отключить, если она больше не нужна. 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

Примечание — Если в качестве сервера каталогов используется Active Directory, а в создании шаблонов и ВМ планируется использовать sysprep, то в этом случае пользователю-администратору системы ROSA Virtualization должен быть делегирован контроль над:

- Присоединением компьютеров к домену
- Изменением членства в группах

14.5.3. Настройка внешнего поставщика LDAP

14.5.3.1. Создание конфигурации внешнего поставщика LDAP (интерактивная установка)

Расширение `ovirt-engine-extension-aaa-ldap` даёт 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 разделе **Настройка внешнего поставщика LDAP**.

Пример для Active Directory смотрите в разделе **Присоединение Active Directory**.

Предварительные условия для настройка внешнего поставщика LDAP

- Должно быть известно доменное имя сервера DNS или сервера LDAP.
- Для настройки защищённого соединения между сервером LDAP и диспетчером убедитесь в том, что был подготовлен сертификат удостоверяющего центра в формате PEM.

– Необходимо иметь как минимум одну пару «имя учётной записи-пароль» для выполнения поисковых запросов и запросов по входам в систему в Active Directory.

Последовательность действий по созданию конфигурации внешнего поставщика LDAP:

1. Для начала интерактивной установки запустите команду `ovirt-engine-extension-aaa-ldap-setup`:

```
#  ovirt-engine-extension-aaa-ldap-setup
```

2. Выберите тип LDAP, введя соответствующий номер. Если схема сервера LDAP неизвестна, выберите стандартную схему для имеющегося типа сервера LDAP. Для Active Directory следуйте 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:
```

3. Для принятия значений по умолчанию и конфигурации разрешения доменного имени для имени сервера LDAP нажмите Ввод:

```
        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]:
```

4. Выберите метод для политики DNS:

– Для варианта 1, серверы DNS, перечисленные в `/etc/resolv.conf` используются для разрешения адреса IP. Убедитесь в том, что файл `/etc/resolv.conf` обновлён до корректных значений серверов DNS.

– Для варианта 2 введите полное доменное имя (FQDN) или адрес IP 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 введите список серверов LDAP, разделённых пробелами используйте 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 укажите список серверов LDAP, разделённых пробелами. Используйте либо полное доменное имя серверов, либо их адреса IP. 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:
```

5. Выберите метод защищённого соединения, поддерживаемый имеющимся сервером LDAP, и укажите этот метод для получения сертификата ЦС в формате PEM:

– **File** даёт возможность указать полный путь до сертификата.
– **URL** даёт возможность указать адрес URL сертификата.
– **Inline** даёт возможность вставить содержимое сертификата в терминал.
– **System** даёт возможность указать местоположение по умолчанию для всех файлов ЦС.
– **Insecure** пропускает проверку сертификата, но подключение по-прежнему шифруется с использованием TLS 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 защищённый протокол LDAP (Lightweight Directory Access Protocol Over Secure Socket Links). Для подключений SSL выбирайте параметр **ldaps**.

6. Введите 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 нажмите клавишу Ввод.

```
     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:
```

7. Введите отличительное имя базы:

```
Please enter base DN (dc=example,dc=ru) [dc=example,dc=ru]:
ou=department- 1,dc=example,dc=ru
```

8. Если для ВМ планируется настроить единый вход, выберите `Yes`. Обратите 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 раздела Настройка единого входа для ВМ в Руководстве по управлению ВМ.

```
Are you going to use Single Sign-On for Virtual Machines (Yes, No)
[Yes]:
```

9. Укажите 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, отредактируйте атрибут **ovirt.engine.aaa.authn.profile.name** в файле **/etc/ovirt-engine/extensions.d/example.ru.-authn.properties**. Для применения изменений перезапустите службу **ovirt-engine**.

```
Please specify profile name that will be visible to users: example.ru
```

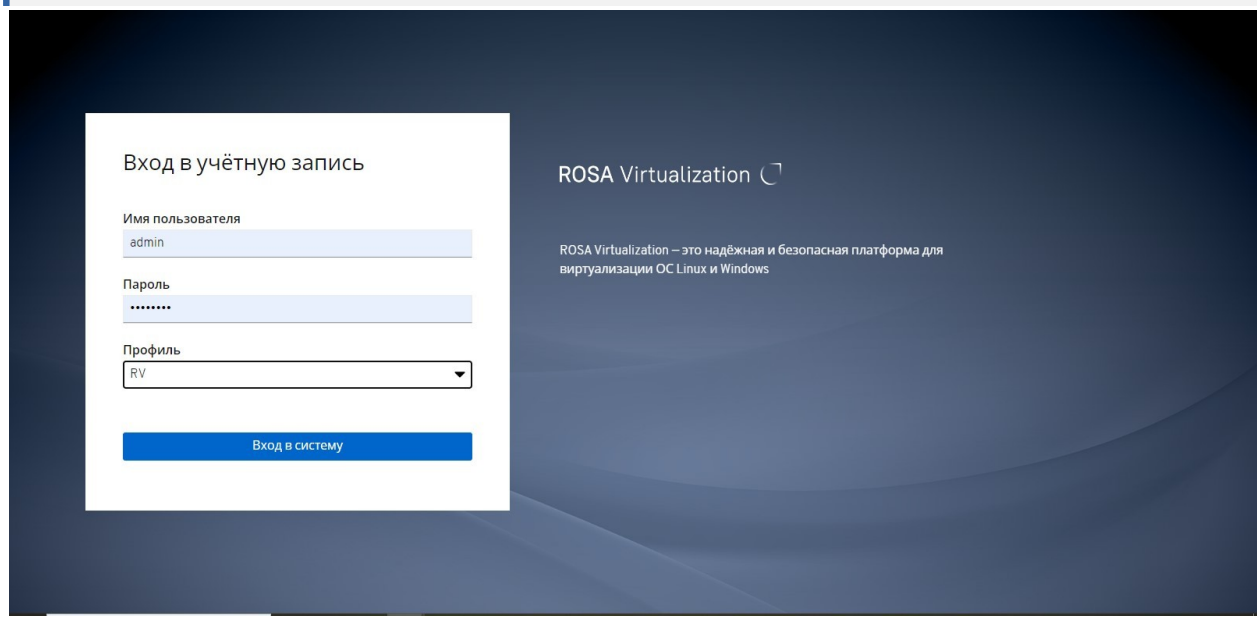

Рис. 167. Страница входа в систему на портале администрирования

Примечание — Пользователь, впервые выполняющий вход в систему, должен выбрать профиль в выпадающем списке. Эта информация сохранится в файлах cookie браузера и будет автоматически указана в следующий раз.

10. Протестируйте возможность входа в систему, чтобы убедиться в том, что сервер LDAP корректно подключён к ROSA Virtualization. В запросе на вход укажите 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
```

11. Проверьте корректность информации пользователя. Если она неверна, выберите `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]:
```

12. Рекомендуется вручную протестировать функционал поиска. Для создания запроса выберите **Principal** для учётных записей пользователей или **Group** для учётных записей групп. Если также должна выводиться информация об учётной записи группы пользователя, выберите 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]:
```

13. Для завершения настройки выберите `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
```

14. Перезапустите службу ovirt-engine. Созданный профиль теперь доступен на страницах входа в систему Портала администрирования и Портала ВМ. Чтобы присвоить пользовательской учётной записи на сервере LDAP соответствующие роли и полномочия, например, для входа в систему на Портале ВМ, обратитесь к сведениям в разделе Администрирование задач пользователей.

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

Примечание — Дополнительную информацию смотрите в файле README расширения для аутентификации и авторизации в LDAP по пути `/usr/share/doc/ovirt-engine-extension-aaa-ldap-`*`версия`*.

14.5.3.2. 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 защищённого соединения между сервером LDAP и машиной диспетчера убедитесь в том, что был подготовлен сертификат ЦС в формате PEM. Подробности см. в разделе Настройка подключений SSL или TLS между диспетчером и сервером LDAP.
- 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. Запишите отличительное имя (DN) этого пользователя. Не используйте 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 учётной записи - пароль**»
- Если при развёртывании Active Directory охватывается несколько доменов, ознакомьтесь с ограничениями, указанными в файле `/usr/share/ovirt-engine-extension-aaa-ldap/profiles/ad.properties`.

Последовательность действий по присоединению к серверу Active Directory:

1. Для начала интерактивной установки запустите команду `ovirt-engine-extension-aaa-ldap-setup`:

```
#  ovirt-engine-extension-aaa-ldap-setup
```

2. Выберите тип LDAP, введя соответствующий номер. Вопросы, касающиеся LDAP, 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
```

3. Укажите имя леса Active Directory. Если DNS диспетчера виртуализации не разрешает имя леса, сценарий предложит указать список имён 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
```

4. Выберите метод защиты соединения, поддерживаемый сервером LDAP, а также укажите способ получения сертификата центра сертификации в формате PEM. Вариант File даёт возможность указать полный путь до сертификата. Вариант URL даёт возможность указать адрес URL сертификата. Вариант Inline используется для вставки содержимого сертификата в консольную строку. Вариант System даёт возможность указать путь до местоположения всех файлов центра сертификации. Вариант Insecure даёт возможность использовать startTLS в незащищённом 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 защищённый протокол LDAP (Lightweight Directory Access Protocol Over Secure Socket Links). Для подключений SSL выбирайте параметр **ldaps**.

5. Введите 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 нажмите клавишу Ввод.

```
     Enter search user DN (empty for anonymous):
cn=user1,ou=Users,dc=test,dc=ru
      Enter search user password:
```

6. Укажите, нужно ли использовать единый вход для ВМ планируется. Эта возможность используется по умолчанию, но её 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 раздела Настройка единого входа для ВМ в Руководстве по управлению ВМ.

```
     Are you going to use Single Sign-On for Virtual Machines (Yes, No)
[Yes]:
```

Укажите 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
```

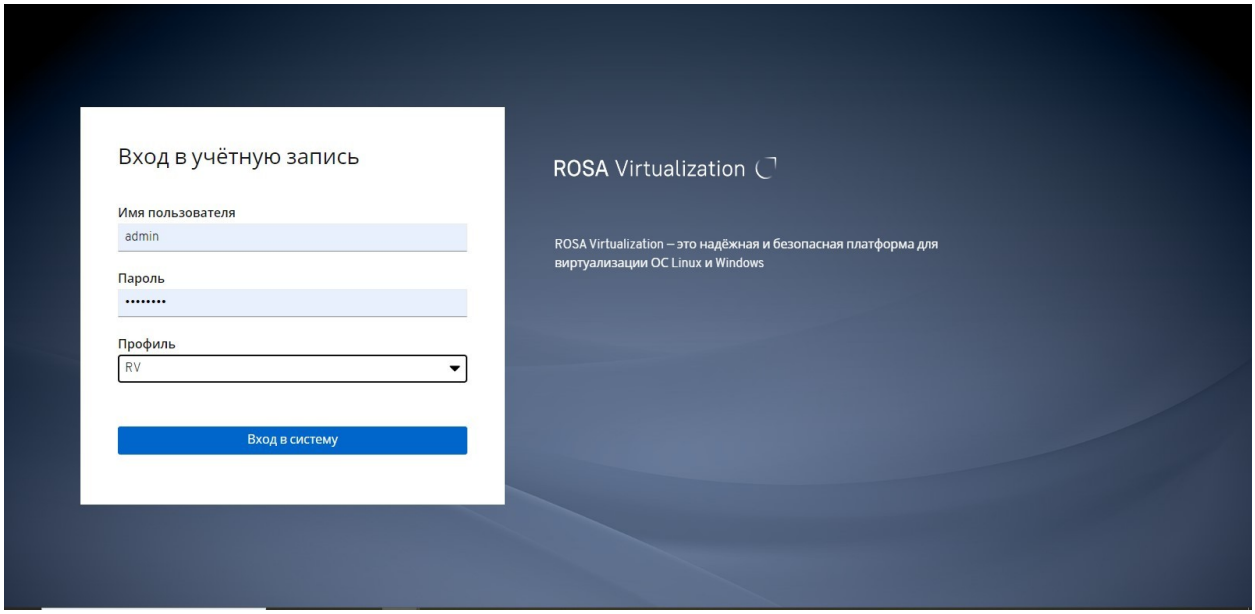

Рис. 168. Страница входа в систему на портале администрирования

Примечание — Пользователь, впервые выполняющий вход в систему, должен выбрать профиль в выпадающем списке. Эта информация сохранится в файлах cookie браузера и будет автоматически указана в следующий раз.

7. Протестируйте возможность входа в систему и поиск, чтобы убедиться в том, что сервер LDAP корректно подключён к окружению ROSA Virtualization. В запросе на вход в систему укажите имя пользователя и пароль. Для создания запроса выберите Principal для учётных записей пользователей или Group для учётных записей групп. Если также должна выводиться информация об учётной записи группы пользователя, выберите значение Yes для пункта Resolve Groups. Для завершения настройки выберите 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
```

8. Созданный профиль теперь доступен на страницах входа в систему Портала администрирования и Портала ВМ. Чтобы присвоить пользовательской учётной записи на сервере LDAP соответствующие роли и полномочия, например, для входа в систему на Портале ВМ, обратитесь к сведениям в разделе Управление пользовательскими задачами на диспетчере.

Примечание — Дополнительные сведения смотрите в файле README расширения аутентификации и авторизации LDAP по пути `/usr/share/doc/ovirt-engine-extension-aaa-ldap-`*`версия`*.

14.5.3.3. 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 разделе 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:

1. Установите пакет расширения LDAP на диспетчере ROSA Virtualization:

```
# dnf install ovirt-engine-extension-aaa-ldap
```

2. Скопируйте 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
```

3. Переименуйте 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
```

4. Измените 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. 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, получите сертификат ЦС для сервера LDAP и с его помощью создайте файл открытого ключа. Раскомментируйте строки, указанные ниже, и укажите полный путь к открытому ключу и паролю доступа к файлу.

Примечание — Дополнительные сведения о создании файла хранения открытого ключа смотрите в разделе **Настройка подключения SSL или TSL между диспетчером и сервером LDAP**.

Пример. 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
```

5. Просмотрите 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. 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
```

6. 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. 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
```

7. Установите соответствующие права доступа и укажите владельца файла профиля:

```
# chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties
# chmod 600 /etc/ovirt-engine/aaa/example.properties
```

8. Перезапустите службу engine:

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

9. Созданный профиль example теперь доступен на страницах входа в систему Портала администрирования и Портала ВМ. Чтобы присвоить пользовательской учётной записи на сервере LDAP соответствующие роли и полномочия, например, для входа в систему на Портале ВМ, обратитесь к сведениям в разделе Управление пользовательскими задачами на диспетчере.

Примечание — Дополнительную информацию смотрите в файле README расширения для аутентификации и авторизации в LDAP по пути **`/usr/share/doc/ovirt-engine-extension-aaa-ldap-`*`версия`***.

14.5.3.4. Удаление внешнего поставщика LDAP

В данной последовательности показывается процесс удаления настроенного внешнего поставщика LDAP и его пользователей.

Последовательность действий по удалению внешнего поставщика LDAP

1. Удалите 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
```

2. Перезапустите службу `ovirt-engine`:

```
# systemctl restart ovirt-engine
```

3. Во вкладке **Пользователи** Портала администрирования выберите пользователей этого поставщика (пользователи со значением profile1-authz для параметра Поставщик авторизации) и нажмите **Удалить.**

14.5.4. Настройка единого входа для LDAP и Kerberos

Механизм единого входа даёт возможность пользователям войти в систему на Портале ВМ или Портале администрирования без повторного ввода пароля. Данные учётной записи для аутентификации получаются с сервера Kerberos. Для настройки единого входа на Портале администрирования необходимо настроить два расширения: o`virt-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 она 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 порталу нет необходимости принимать пароль, 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:

- На сервере KDC
  a. На машине диспетчера ROSA Virtualization создайте принципала службы и файл keytab для службы Apache.
- На диспетчере ROSA Virtualization
  a. Установите пакеты расширений аутентификации и авторизации, а также модуль аутентификации Kerberos для Apache.
  b. Настройте файлы расширений

14.5.4.1 Настройка Kerberos для службы Apache

1. На сервере KDC используйте 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
```

2. Создайте файл keytab для службы Apache. В этом файле 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, убедитесь, что для него была создана и восстановлена резервная копия.

```
kadmin> ktadd -k /tmp/http.keytab HTTP/fqdn-of-rhevm@REALM.COM
kadmin> quit
```

3. Скопируйте файл keytab с сервера KDC на машину диспетчера виртуализации:

```
# scp /tmp/http.keytab root@rhevm.example.com:/etc/httpd
```

Настройка единого входа для Портала ВМ или Портала администрирования

4. На машине диспетчера виртуализации установите соответствующие права доступа и укажите владельца файла таблицы ключей:

```
# chown apache /etc/httpd/http.keytab
# chmod 400 /etc/httpd/http.keytab
```

Установите 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
```

5. Скопируйте 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
```

6. Переместите 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, убедитесь, что для него была создана и восстановлена резервная копия.

```
# mv /etc/ovirt-engine/aaa/ovirt-sso.conf /etc/httpd/conf.d
```

7. Просмотрите 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. 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>
```

8. Переименуйте 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
```

9. Измените 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. 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, получите сертификат корневого центра сертификации для сервера LDAP и с его помощью создайте файл открытого ключа. Раскомментируйте строки, указанные ниже, и укажите полный путь к открытому ключу и паролю доступа к файлу.

Примечание — Дополнительные сведения о создании файла хранения открытого ключа смотрите в разделе **Настройка подключения SSL или TLS между диспетчером и сервером LDAP**.

Пример. 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
```

10. Просмотрите 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. 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
```

11. Просмотрите 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. 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
```

12. Просмотрите 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. 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}
```

13. Установите соответствующие права доступа и укажите 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
```

14. Перезапустите службу Apache и службу ovirt-engine:

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

14.5.5. Авторизация пользователей

14.5.5.1 Модель авторизации пользователей

Управление авторизацией в системе ROSA Virtualization базируется на сочетании трёх составляющих:

- Пользователь, выполняющий действие
- Тип этого выполняемого действия
- Объект, над которым выполняется это действие

14.5.5.2 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 целевой домен хранения. Пользователь, выполняющий это действие, должен иметь полномочия на все объекты, подпадающие под влияние этого действия.

14.5.6. Администрирование задач пользователей на Портале администрирования

14.5.6.1. Окно «Параметры учётной записи»

В окне «**Администрирование**» → «**Параметры учётной записи**» можно просматривать или редактировать следующие параметры пользователя Портала администрирования:

- Вкладка «**Общее**»:
  a. Имя пользователя (только для чтения)
  b. E-mail (только для чтения).
  c. Домашняя страница:
     d. По умолчанию - **#dashboard-main**.
     e. Настраиваемая домашняя страница: введите только последнюю часть URL, включая символ #. Например: **#vms-snapshots;name-testVM**.
  f. Последовательная консоль
  g. Открытый ключ пользователя — введите открытый ключ SSH, используемый для доступа к диспетчеру с помощью последовательной консоли.
  h. Таблицы
  i. Параметры сохранения состояния сетки — сохранение параметров столбцов сетки на сервере.
- Вкладка «**Подтверждения**»:
  a. Показывать диалог подтверждения при заморозке ВМ — включение показа диалога подтверждения заморозки ВМ.

14.5.6.2. Добавление пользователей и присвоение полномочий для работы на Портале виртуальных машин

Роли и полномочия можно присваивать только ранее созданным пользователям. Роли и полномочия, присваиваемые в данном процедуре, дают пользователям права на выполнение входа в систему на Портале ВМ и на создание виртуальных машин. Процедура также применима и для учётных записей групп.

Последовательность действий по добавлению пользователей и присвоению полномочий для работы на Портале виртуальных машин:

1. На панели заголовков нажмите «**Администрирование**» → «**Настроить**», чтобы открыть окно «**Параметры**».
2. Нажмите «**Системные полномочия**».
3. Нажмите «**Добавить**», откроется окно «**Добавить системные полномочия пользователю**».
4. В разделе «**Поиск**» выберите профиль. Профиль — это домен, в котором нужно выполнить поиск. В поле поиска введите имя или часть имени и нажмите «**Выполнить**». Как вариант, нажмите «**Выполнить**», чтобы просмотреть список всех пользователей и групп.
5. Отметьте галочками нужных пользователей или нужные группы.
6. В списке «**Присваиваемая роль**» выберите подходящую роль. Роль **UserRole** даёт учётной записи пользователя полномочия на выполнения входа в систему на Портале ВМ.
7. Нажмите **ОК**.

Выполните вход в систему на Портале ВМ, чтобы убедиться, что у пользователя есть полномочия на вход.

14.5.6.3. Просмотр сведений о пользователе

Последовательность действий по просмотру сведений о пользователе:

1. Нажмите «**Администрирование**» → «**Пользователи**», чтобы просмотреть список авторизованных пользователей.
2. Нажмите на имя пользователя, чтобы перейти к подробному просмотру, обычно это вкладка «**Общее**», где показываются такие сведения, как имя домена, почтовый адрес и статус пользователя.
3. В других вкладках можно просмотреть группы, полномочия, квоты и события пользователя.

Чтобы, например, просмотреть группы, к которым принадлежит пользователь, перейдите на вкладку **Группы каталогов**.

14.5.6.4. Просмотр полномочий пользователя для работы с ресурсами

Администратор может присваивать пользователям полномочия на работу с конкретными ресурсами или иерархией ресурсов. Для каждого ресурса можно просмотреть присвоенных пользователей и их полномочия.

Последовательность действий по просмотру полномочий пользователя для работы с ресурсами:

1. Найдите и нажмите на имя ресурса, чтобы перейти к подробному просмотру
2. Перейдите на вкладку **Полномочия**, чтобы просмотреть список присвоенных пользователей, их роли, а также наследуемые полномочия на выбранные ресурсы.

14.5.6.5. Удаление пользователей

Если учётная запись пользователя больше не нужна, удалите её из системы ROSA Virtualization.

Последовательность действий по удалению пользователей:

1. Нажмите «**Администрирование**» → «**Пользователи**», чтобы просмотреть список авторизованных пользователей.
2. Выберите удаляемого пользователя. Убедитесь в том, что от имени пользователя не выполняются никакие ВМ.
3. Нажмите «**Удалить**», затем нажмите «ОК».

Пользователь будет удалён из системы ROSA Virtualization, но не с внешнего каталога.

14.5.6.6. Просмотр пользователей, выполнивших вход в систему

Администратор может просматривать пользователей, на текущий момент выполнивших вход в систему, а также время длительности их сеанса и другие подробности. Нажмите **Администрирование → Активные сеансы пользователей**, чтобы просмотреть **ID сеанса в БД**, **Имя пользователя**, **Поставщика авторизации**, **ID пользователя**, **IP источника**, **Время начало сеанса** и **Активное время последнего сеанса** каждого из пользователей, выполнивших вход в систему.

14.5.6.7. Завершение сеанса работы пользователя

Администратор может завершать сеансы работы пользователей, выполнивших вход в систему.

Завершение сеанса работы пользователя

1. Нажмите «**Администрирование**» → «**Активные сеансы**» пользователей.
2. Выберите сеанс пользователя, который необходимо завершить.
3. Нажмите «**Завершить сеанс**».
4. Нажмите «**ОК**».

14.5.7. Администрирование задач пользователей в консольном режиме

С помощью утилиты `ovirt-aaa-jdbc-tool` можно управлять учётными записями пользователей во внутреннем домене. Изменения, внесённые при помощи этой утилиты, применяются мгновенно и не требуют перезапуска службы **ovirt-engine**. Полный список параметров для работы с пользователями можно просмотреть в выводе **ovirt-aaa-jdbc-tool user --help**. Примеры наиболее часто встречающихся случаев использования предлагаются в данном разделе.

Примечание — Администратор должен выполнить вход в систему на машине СУСВ.

14.5.7.1. Создание нового пользователя

Администратор может создавать учётные записи новых пользователей. Дополнительный параметр `--attribute` передаёт подробности. Чтобы просмотреть полный список параметров, выполните `ovirt-aaa-jdbc-tool user add --help`.

```
# 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. Подробности см. в разделе **Добавление пользователей**.

14.5.7.2. Настройка пароля пользователя

Администратор может создавать пароли. Необходимо указать значение параметру **--password-valid-to**, в противном случае время истечения действия пароля по умолчанию равно текущему времени.

- Формат 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 используйте значение **Z**.
- Дополнительные параметры см. в выводе **`ovirt-aaa-jdbc-tool user password-reset --help`**.

```
# 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
```

Примечание — По умолчанию, политика паролей для учётных 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, выполните **`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 ROSA Virtualization продолжит использовать старый пароль. Для внесения нового пароля в **`ovirt-provider-ovn`**, выполните следующие действия:

1. На портале администрирования нажмите **Администрирование** → **Поставщики**.
2. Выберите `ovirt-provider-ovn`.
3. Нажмите **Изменить** и введите новый пароль в поле **Пароль**.
4. Нажмите **Проверить**, чтобы протестировать успешность аутентификации с предоставленными данными учётной записи.
5. В случае успешности проверки нажмите **ОК**.

14.5.7.3. Настройка интервала истечения времени ожидания сеанса пользователя

Администратор может настроить интервал истечения времени ожидания сеанса пользователя:

```
# engine-config --set UserSessionTimeOutInterval=integer
```

14.5.7.4. 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.

1. Выполните следующую 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
```

2. С помощью сценария ovirt-aaa-jdbc-tool с параметром --encrypted укажите новый пароль:

```
# ovirt-aaa-jdbc-tool user password-reset test1 \
--password-valid-to="2025-08-01 12:00:00- 0800" --encrypted
```

3. Введите и подтвердите зашифрованный пароль:

```
Password:
Reenter password:
updating user test1...
user updated successfully
```

14.5.7.5. Просмотр информации о пользователях

Администратор может просматривать подробные сведения об учётных записях пользователей:

```
# ovirt-aaa-jdbc-tool user show test1
```

Указанная команда выводит больше сведений, чем можно получить на экране «**Администрирование**» → «**Пользователи**» на Портале администрирования.

14.5.7.6. 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
```

14.5.7.7. Удаление пользователей

Администратор может удалять учётные записи пользователей:

```
# ovirt-aaa-jdbc-tool user delete test1
```

Удалите пользователя с Портала администрирования. Подробности см. в разделе **Удаление пользователей**.

14.5.7.8. 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` убедитесь в том, что в окружении имеется ещё как минимум один пользователь с полными административными полномочиями.

Последовательность действий по отключению внутреннего пользователя-администратора:

1. Выполните вход в систему на машине с установленным диспетчером виртуализации.
2. Убедитесь в том, что в окружение был добавлен ещё один пользователь с ролью `SuperUser`. Подробности см. в разделе **Добавление пользователей**.
3. Отключите изначального пользователя `admin`:

```
# ovirt-aaa-jdbc-tool user edit admin --flag=+disabled
```

Примечание — Чтобы включить отключённого пользователя, выполните команду:

```
# ovirt-aaa-jdbc-tool user edit username --flag=-disabled
```

14.5.7.9. Управление группами

С помощью утилиты ovirt-aaa-jdbc-tool можно управлять учётными записями групп во внутреннем домене. Управление учётными записями групп аналогично управлению учётными записями пользователей. Полный список возможностей для групп смотрите в выводе ovirt-aaa-jdbc-tool group --help. В данном разделе приводятся общие примеры.

Создание группы пользователей

Данная последовательность действий объясняет, как создать группу пользователей, добавить пользователей в группу и просматривать сведения о группе.

1. Выполните вход в систему на машине с установленным диспетчером виртуализации.
2. Создайте новую группу:

```
# ovirt-aaa-jdbc-tool group add group1
```

3. Добавьте пользователей в группу. Эти пользователи должны уже быть созданы ранее.

```
# ovirt-aaa-jdbc-tool group-manage useradd group1 --user=test1
```

Примечание — Полный список параметров управления группами см. в выводе **`ovirt-aaa-jdbc-tool group- manage --help`**.

4. Просмотрите сведения об учётной записи группы:

```
# ovirt-aaa-jdbc-tool group show group1
```

5. Добавьте только что созданную группу на Портале администрирования и выделите группе необходимые роли и полномочия. Пользователи-участники группы наследуют роли и полномочия группы. Подробности см. в разделе Добавление пользователей.

Создание вложенных групп

Данная процедура объясняет, как создать группу внутри группы.

1. Выполните вход в систему на машине с установленным диспетчером виртуализации.
2. Создайте новую группу:

```
# ovirt-aaa-jdbc-tool group add group1
```

3. Создайте вторую группу:

```
# ovirt-aaa-jdbc-tool group add group1-1
```

4. Добавьте вторую группу к первой:

```
# ovirt-aaa-jdbc-tool group-manage groupadd group1 --group=group1-1
```

5. Добавьте первую группу на Портале администрирования и присвойте группе необходимые роли и полномочия. Подробности смотрите в разделе Добавление пользователей.

14.5.7.10. Запрос сведений о группах и пользователях

Модуль **query** даёт возможность запросить сведения о пользователях и группах. Полный список параметров можно посмотреть в выводе `ovirt-aaa-jdbc-tool query --help`.

Просмотр сведений об учётных записях всех пользователей или групп

Данная последовательность действий объясняет, как можно просмотреть информацию обо всех учётных записях.

1. Выполните вход в систему на машине с установленным диспетчером виртуализации.
2. Получите список сведений об учётных записях

Учётные записи всех пользователей:

```
# ovirt-aaa-jdbc-tool query --what=user
```

Учётные записи всех групп:

```
# ovirt-aaa-jdbc-tool query --what=group
```

Получение списка учётных записей с применением фильтра

Данная процедура объясняет, как применять фильтры при получении списка сведений об учётных записях.

1. Выполните вход в систему на машине с установленным диспетчером виртуализации.
2. Примените фильтр к информации об учётной записи с помощью параметра **--pattern**.

Получите список учётных записей с именами, начинающимися с символа ***j***.

```
# ovirt-aaa-jdbc-tool query --what=user --pattern="name=j*"
```

Получить список групп, со значением ***marketing*** атрибута department:

```
# ovirt-aaa-jdbc-tool query --what=group --pattern="department=marketing"
```

14.5.7.11. Управление параметрами учётных записей

Для изменения исходных параметров учётной записи используйте модуль **`ovirt-aaa-jdbc-tool settings`**.

Обновление информации о параметрах учётной записи

Данная последовательность действий объясняет, как изменить изначальные параметры учётной записи.

1. Выполните вход в систему на машине с установленным диспетчером виртуализации.
2. Для просмотра всех доступных параметров выполните следующую команду:

```
# ovirt-aaa-jdbc-tool settings show
```

3. Измените необходимые параметры:
   a. В данном примере изначальное значение длительности сеанса пользователя (10080 минут) изменяется на 60 минут для всех учётных записей пользователей.

```
# ovirt-aaa-jdbc-tool settings set --name=MAX_LOGIN_MINUTES --value=60
```

   b. В данном примере изменяется значение числа неудачных попыток входа в систему, которые может выполнить пользователь до того, как его учётная запись будет заблокирована. Значение по умолчанию: 5.

```
# ovirt-aaa-jdbc-tool settings set --name=MAX_FAILURES_SINCE_SUCCESS \
--value=3
```

Примечание — Для разблокирования учётной записи пользователя выполните **ovirt-aaa-jdbc-tool user unlock *test1***.

14.5.8. 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 системы ROSA Virtualization, после выходов следующих версий эти домены необходимо будет обновлять вручную. Дополнительные сведения о создании дополнительных локальных доменов и об обновлении версий этих доменов смотрите в файле README, расположенном по пути **`/usr/share/doc/ovirt-engine-extension-aaa-jdbc-`*`версия`*`/README.admin`**.

14.6. Квоты и политика соглашения об уровне обслуживания

14.6.1. Что такое Quota

Quota — это утилита ограничения ресурсов, предоставляемая системой ROSA Virtualization. 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 ROSA Virtualization ограничивать доступ пользователей к памяти, ЦП и хранилищам. Quota определяет объём 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:

1. Quota времени выполнения. Эта квота ограничивает потребление ресурсов времени выполнения, таких, как ЦП и память.
2. Quota хранилища. Эта квота ограничивает доступный объём хранилища

У Quota, как и у SELinux, есть три режима, они представлены на Таблица 2. Режимы квот.

Таблица 2. 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.
Отключён	Этот режим отключает ограничения времени выполнения и ограничения на использования хранилища, установленные квотой.

При попытке пользователя запустить ВМ, спецификации этой ВМ 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, определённую квотой, то в этом случае диспетчер виртуализации откажется запускать машину.

При создании нового диска пользователем, запрошенный размер диска добавляется к общему объёму дисков, покрываемых применимой квотой. Ели общий объём, включая объём нового диска, превышает объём, разрешённый квотой, то диск не будет создан.

Quota допускает разделение ресурсов одного аппаратного обеспечения. Есть поддержка мягкого и жёсткого 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 приведёт 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 даёт 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 создаётся этот шаблон.

14.6.2. 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 Тбайт в хранилище, а один из этих десяти пользователей заполнит весь этот объём, 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.

14.6.3. Расчёт квот

При назначенной пользователю или ресурсу квоте, каждое действие этого потребителя или действие с ресурсом, включающее 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 расчёта квоты

Пользователь запустил ВМ с 1 виртуальным ЦП и 1024 Мбайт памяти. Это действие потребляет 1 виртуальный ЦП и 1024 Мбайт квоты, выделенной этому пользователю. После остановки этой ВМ, 1 вЦП и 1024 Мбайт ОЗУ возвращаются обратно в квоту, присвоенную этому пользователю. Потребление квоты времени выполнения считается только во время фактического времени выполнения потребителя.

Пользователь создаёт виртуальный диск тонкого резервирования размером в 10 Гбайт. Фактическое потребление дискового объёма может указывать, что используется только 3 Гбайт. Но потребление квоты, тем не менее, будет составлять 10 Гбайт, т.е. максимальный потенциал роста этого диска.

14.6.4. 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, выполните вход на Портал администрирования.

Для тестирования квоты и проверки, что её выполнения отвечает ожиданиям, используйте режим **Аудит**. Для создания или изменения квоты режим Аудит необязателен.

Последовательность действий по включению и изменению режима квот в дата-центре:

1. Нажмите «**Ресурсы**» → «**Дата-центры**» и выберите дата-центр.
2. Нажмите «**Изменить**».
3. В выпадающем списке Режим квоты измените режим на «**Принудительный**».

4. Нажмите **ОК**.

Если во время тестирования установить режим **«Аудит»**, то для того, чтобы параметры квоты вступили в силу, режим необходимо сменить на **«Принудительный»**.

14.6.5. Создание новых политик квотирования

Администратор включил режим квоты, либо в режиме **Аудит** либо в режиме **Принудительный**, и теперь необходимо настроить политику квоты для управления потреблением ресурсов в дата-центре.

Последовательность действий по созданию новых политик квотирования

1. Нажмите **«Администрирование» → «Квота»**.
2. Нажмите **«Добавить»**.
3. Заполните поля **«Название** и **Описание»**.
4. Выберите **«Дата-центр»**.
5. В разделе **«Память и ЦП»** с помощью зелёного бегунка настройте **«Порог кластера»**.
6. В разделе **«Память и ЦП»** с помощью голубого бегунка настройте Льготу кластера.
7. Активируйте переключатель **«Все кластеры»** или переключатель **«Конкретные кластеры»**. При выборе переключателю Конкретные кластеры отметьте кластеры, для которых нужно добавить политику квоты.
8. Нажмите **Изменить**, чтобы открыть окно **Изменить квоту**.
   a. В поле **«Память»** активируйте либо переключатель **«Без ограничений** (чтобы не ограничивать использование ресурсов памяти в кластере), либо активируйте переключатель **«Ограничить до»**, чтобы указать объём памяти, установленный для этой квоты. При выборе переключателя **Ограничить до** указывайте объём памяти в мегабайтах (Мбайт) в поле **Мбайт**.
   b. В поле **«ЦП»** активируйте либо переключатель **«Без ограничений»**, либо переключатель **«Ограничить до»**, чтобы указать объём ЦП, установленный для этой квоты. При выборе переключателя **Ограничить до** указывайте число виртуальных ЦП в поле **вЦП**.
   c. Нажмите **ОК** в окне **«Изменить квоту»**.
9. В разделе **«Хранилище** с помощью зелёного бегунка настройте **«Порог хранилища»**.
10. В разделе **«Хранилище»** с помощью голубого бегунка настройте **«Льготу хранилища**.
11. Активируйте переключатель **«Все домены хранилищ»** или **«Конкретные домены хранилищ»**. При выборе переключателя **«Конкретные домены хранилищ»** отметьте домены хранения, для которых нужно добавить политику квоты.
12. Нажмите **«Изменить»**, чтобы открыть окно **«Изменить квоту»**.

a. В поле «**Квота хранилища**» активируйте либо переключатель «**Без ограничений**» (чтобы не ограничивать использование ресурсов хранилища), либо активируйте переключатель «**Ограничить до**», чтобы указать объём хранилища, до которого пользователи будут ограничены квотой. При выборе переключателя «**Ограничить до**» указывайте объём размера квоты на хранилище в гигабайтах (Гбайт) в поле **Гбайт**.
b. Нажмите **OK** в окне «**Изменить квоту**».

13. Нажмите **OK** в окне «**Новая квота**».

14.6.6. Объяснение параметров порога квоты

Параметры квот представлены в Таблица 3 Пороги и льготы квот.

Таблица 3 Пороги и льготы квот

Параметр	Определение
Порог кластера	Объём ресурсов кластера, доступный для каждого из дата-центров.
Льгота кластера	Объём ресурсов кластера, доступный дата-центру после исчерпания объёма, указанного значением порога кластера дата-центра.
Порог хранилища	Объём ресурсов хранилища, доступный для каждого из дата-центров.
Льгота хранилища	Объём ресурсов хранилища, доступный дата-центру после исчерпания объёма, указанного значением порога хранилища.

При квоте, установленной в 100 Гбайт со льготой в 20%, потребителям будет запрещено использование хранилища после того, как используемый ими объём хранилища достигнет 120 Гбайт. Если та же самая квота имеет значение порога в 70%, тогда потребителям выводится предупреждение в момент, когда используемый ими объём превысит 70 Гбайт (но остаётся возможность потреблять хранилище до тех пор, пока потребляемый объём не достигнет 120 Гбайт).

Как значение «Порога», так и значение «Льготы» настраиваются относительно значения квоты. «Порог» можно представить как «мягкий предел», и при его превышении выводится предупреждение. «Льготу» можно представить как «жёсткое ограничение», и при его превышении дальнейшее потребление ресурсов хранилища становится невозможным.

14.6.7. Присвоение квот объектам

Присвоение квот виртуальным машинам

1. Нажмите «**Ресурсы**» → «**ВМ**» и выберите виртуальную машину.
2. Нажмите «**Изменить**».
3. В выпадающем списке «**Квота**» выберите квоту, которую будет потреблять выбранная ВМ.
4. Нажмите **ОК**.

Присвоение квоты диску

1. Нажмите «**Ресурсы**» → «**ВМ**».
2. Нажмите на имя ВМ, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку **Диски** и выберите диск, который планируется связать с квотой.
4. Нажмите «**Изменить**».
5. В выпадающем списке «**Квота**» выберите квоту, которую будет потреблять выбранный виртуальный диск.
6. Нажмите **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 выдаёт при этом диспетчер виртуализации, является очень общей, что затрудняет нахождение её 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.

14.6.8. Использование квот для ограничения потребления ресурсов пользователем

Данная последовательность действий объясняет, как с помощью квот ограничить доступные пользователю ресурсы.

Последовательность действий по использованию квот для ограничения потребления ресурсов пользователем

1. Нажмите «**Администрирование**» → «**Квота**».
2. Нажмите на название целевой квоты, чтобы перейти к подробному просмотру.
3. Перейдите на вкладку «**Потребители**».
4. Нажмите «**Добавить**».
5. В поле «**Поиск**» введите имя пользователя, которого нужно связать с квотой.
6. Нажмите «**Выполнить**».
7. Поставьте галочку рядом с именем пользователя.
8. Нажмите **ОК**.

Через некоторое время пользователь появится во вкладке «Потребители».

14.6.9. Редактирование квот

Данная последовательность действий объясняет, как изменять существующие квоты.

Последовательность действий по редактированию квот

1. Нажмите «**Администрирование**» → «**Квота**» и выберите квоту.
2. Нажмите «**Изменить**».
3. Внесите необходимые изменения.
4. Нажмите **ОК**.

14.6.10. Удаление квот

Данная последовательность действий объясняет, как удалять квоты.

Последовательность действий по удалению квот

1. Нажмите «**Администрирование**» → «**Квота**» и выберите квоту.
2. Нажмите «**Удалить**».
3. Нажмите **ОК**.

14.6.11. Принудительное применение политики соглашения об уровне обслуживания

Данная последовательность действий объясняет, как настроить параметры ЦП согласно соглашению об уровне обслуживания.

Последовательность действий по принудительному применению политики соглашения об уровне обслуживания

1. Нажмите «**Ресурсы**» → «**ВМ**».
2. Нажмите «**Создать**» или выберите ВМ и нажмите «**Изменить**».
3. Перейдите на вкладку «**Выделение ресурсов**».
4. Укажите **Ресурсы ЦП**. Возможные значения: **Низкое**, **Среднее**, **Высокое**, **Пользовательское** и **Отключено**. Виртуальные машины, для которых указано **Высокое** значение, получают в два раза больше ресурсов, чем ВМ, для которых указано **Среднее** значение, а ВМ со **Средним** значением получают в два раза больше ресурсов, чем ВМ, для которых указано **Низкое** значение. Значение **Отключено** указывает, что для расчёта 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.

14.7. Уведомления о событиях

14.7.1. Настройка уведомлений о событиях на Портале администрирования

При возникновении конкретных событий в окружении, управляемом диспетчером системы ROSA Virtualization, диспетчер может послать почтовое сообщение

предварительно назначенным пользователям с уведомлением об этом событии. Чтобы использовать эту возможность, необходимо настроить агент пересылки сообщений. На Портале администрирования можно настроить только почтовые уведомления. Ловушки SNMP настраиваются на машине СУСВ.

Последовательность действий по настройке уведомлений о событиях:

1. Убедитесь в том, что имеется доступ на почтовый сервер, который может принимать автоматизированные сообщения из виртуализированного ЦУ и доставлять их по списку адресатов.
2. Нажмите **Администрирование → Пользователи** и выберите пользователя.
3. Нажмите на Имя пользователя, чтобы перейти на страницу подробного просмотра.
4. На вкладке **Уведомления о событиях** нажмите **Управление событиями**.
5. Для просмотра событий используйте кнопку **Развернуть** все или отдельные кнопки развёртывания по темам.
6. Отметьте галочками необходимые элементы.
7. В поле **Получатель почты** введите почтовый адрес.
8. Нажмитее **ОК**.

Примечание — Почтовый адрес может быть адресом для отправления СМС (например, ***1234567890@carrierdomainname.com***) или почтовым адресом группы, включающий в себя как обычные почтовые адреса, так и почтовые адреса для отправления СМС.

9. На машине диспетчера скопируйте `ovirt-engine-notifier.conf` в новый файл с именем 90-email-notify.conf:

```
  # cp /usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-
notifier.conf /etc/ovirt- engine/notifier/notifier.conf.d/90-email-notify.conf
```

10. Отредактируйте файл `90-email-notify.conf`, удалив всё, кроме раздела `EMAIL Notifications`.
11. Укажите 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`.

12. Для применения внесённых изменений активируйте и перезапустите 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 ROSA Virtualization. Выбранные события будут показываться во вкладке **Уведомления о событиях** этого пользователя.

14.7.2. Отмена уведомлений о событиях на Портале администрирования

Пользователь ранее настроил ненужные почтовые уведомления и хочет их отменить

Последовательность действий по отмене уведомлений о событиях на Портале администрирования:

1. Нажмите **Администрирование → Пользователи**.
2. Нажмите на **Имя пользователя**, чтобы перейти к подробному просмотру.

3. Перейдите на вкладку «**Уведомления о событиях**», чтобы просмотреть события, для которых пользователь ранее настроил получение почтовых уведомлений.
4. Нажмите **Управление событиями**.
5. Для просмотра событий используйте кнопку **Развернуть все** или отдельные кнопки развёртывания по темам.
6. Снимите соответствующие галочки для отмены уведомлений по этим событиям.
7. Нажмите **OK**.

14.7.3. 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`.

Таблица 4. 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-engine`	Местоположение каталога etc, 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 удалённой

		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 счётчик 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 N_THRESHOLD	30	Число неудачных запросов, после которых будет послано почтовое 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, укажите 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) ${FILTER}
MAIL_SERVER	`нет`	Адрес почтового сервера SMTP. Требуемое значение.
MAIL_PORT	`25`	Порт, используемый для связи. Возможные значения: 25 для простого SMTP, 465 for SMTP с SSL и 587 для SMTP с TLS.
MAIL_USER	`нет`	Эту переменную необходимо настроить, если для аутентификации пользователей используется SSL. Также эта переменная используется для указания почтового адреса пользователя-отправителя, если переменная MAIL_FROM не настроена. Некоторые почтовые адреса не поддерживают этот функционал. Адрес указывается в формате RFC822.
SENSITIVE_KEYS	`${SENSITIVE_KEYS}, MAIL_PASS WORD`	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 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	Адреса IP 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. Обратите внимание, что изменение ловушки по умолчанию делает невозможным её 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, подключённого с помощью SNMP.
SNMP_USERNAME	нет	(SNMPv3) Имя пользователя, используемого для ловушек SNMPv3.
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 убедитесь, 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 выполнить мониторинг машины диспетчера за указанный интервал после неудачной попытки.
IS_HTTPS_PROTOCOL	false	Если JBoss выполняется в защищённом режиме, данная переменная должна иметь значение true.
SSL_PROTOCOL	TLS	Протокол, используемый коннектором конфигурации JBoss при включённом SSL.
SSL_IGNORE_CERTIFICATE_ERR ORS	false	Данная переменная должна иметь значение true, если JBoss выполняется в защищённом режиме, а ошибки SSL должны будут игнорироваться.
SSL_IGNORE_HOST_VERIFICATI ON	false	Данная переменная должна иметь значение true, если JBoss выполняется в защищённом режиме, а ошибки верификации имени хоста должны будут игнорироваться.
REPEAT_NON_RESPONSIVE_NO TIFICATION	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.

14.7.4. Настройка отправки ловушек SNMP из диспетчера ROSA Virtualization

Настройте отправку ловушек протокола SNMP (Simple Network Management Protocol, «простой протокол сетевого управления ») из диспетчера ROSA Virtualization на один или несколько внешних диспетчеров SNMP. Ловушки SNMP содержат сведения о системных событиях; они используются для наблюдения за окружением системы ROSA Virtualization. Число и тип ловушек, отправляемых диспетчеру SNMP, можно настроить на диспетчере виртуализации.

Система ROSA Virtualization 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:

- На одном или более внешних диспетчерах SNMP настраивается получение ловушек.
- Адреса IP или полные доменные имена машин, которые будут выполнять роль диспетчеров SNMP. Опционально, настройте порт, на котором диспетчер будет получать уведомления от ловушек. Порт по умолчанию: порт UDP, 162.
- 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. Комьюнити по умолчанию: **public**.
- Идентификатор объектов ловушек для уведомлений. Диспетчер ROSA Virtualization 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. Обратите внимание, что изменение ловушки по умолчанию отменяет соответствие создаваемых ловушек требованиям базы MIB диспетчера.
- Имя пользователя SNMP, для SNMP версии 3 и уровням защиты 1,2 и 3.
- Парольная фраза SNMP, для SNMP версии 3 и уровням защиты 2 и 3.
- Закрытая парольная фраза, для SNMP версии 3 и уровня защиты 3.

Примечание — Диспетчер ROSA Virtualization предоставляет базы MIB в файлах **`/usr/share/doc/ovirt-engine/mibs/OVIRT-MIB.txt`.** Загрузите базы в диспетчер SNMP до того, как продолжить.

Значение конфигурации SNMP по умолчанию присутствуют 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 редактируйте файл напрямую, т.к. такие системные изменения, как обновления, могут в дальнейшем изменить его значения. Для редактирования файла создайте 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 ROSA Virtualization

1. Создайте 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 — Скопируйте 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.

2. Укажите диспетчеров SNMP, комьюнити SNMP (только для SNMP версии 2), и OID в формате, приведённом 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
```

3. Укажите используемую версию SNMP: версию 2 (по умолчанию), или 3:

```
SNMP_VERSION=3
```

4. Укажите значение SNMP_ENGINE_ID. Например:

```
SNMP_ENGINE_ID="80:00:00:00:01:02:05:05"
```

5. Для SNMP версии 3 укажите 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
```

6. Укажите, какие события отправляются на диспетчер SNMP:

Примеры событий:

a. Отправлять все события на профиль SNMP по умолчанию:

```
FILTER="include:*(snmp:) ${FILTER}"
```

b. Отправлять все события с уровнем серьёзности ERROR или ALERT на профиль SNMP по умолчанию:

```
FILTER="include:*:ERROR(snmp:)  ${FILTER}"
FILTER="include:*:ALERT(snmp:)  ${FILTER}"
```

c. Отправлять события VDC_START на указанный почтовый адрес:

```
FILTER="include:VDC_START(snmp:mail@example.com) ${FILTER}"
```

d. 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 отключён, 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, фильтруйте журнальные сообщения в рамках диспетчера SNMP.

7. Сохраните файл.
8. Запустите службу ovirt-engine-notifier и настройте запуск этой службы при загрузке:

```
# systemctl start ovirt-engine-notifier.service
# systemctl enable ovirt-engine-notifier.service
```

Проверьте 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.

Пример файла конфигурации SNMP:

Данный примерный файл конфигурации базируется на параметрах файла **ovirt-engine-notifier.conf**. Файл конкретной конфигурации SNMP, как указанный ниже, перезаписывает параметры общего файла **ovirt-engine-notifier.conf**.

Примечание — Скопируйте значения SNMP по умочанию из файла конфигурации демона уведомлений о событиях по пути **/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf** в файл **/etc/ovirt-engine/notifier/notifier.conf.d/<_целое_число_>-snmp.conf**, где **<_ целое_число _>** — это число, указывающее приоритет, с которым должен запускаться файл. В этом файле есть построковые комментарии для всех параметров.

/etc/ovirt-engine/notifier/notifier.conf.d/20-snmp.conf

14.8. Служебные программы

14.8.1. Утилита oVirt Engine Rename

14.8.1.1 Утилита oVirt Engine Rename

При запуске команды **engine-setup** в чистом окружении, команда создаёт 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 имён для доступа к веб-интерфейсу диспетчера.

1. Убедитесь в том, что выбранные имена разрешаются на адрес IP машины диспетчера, для этого добавьте соответствующие записи на сервер DNS или в **/etc/hosts** (для проверки используйте **`ping enginename`** или **getent hosts enginename**).
2. Выполните 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 адрес IP машины диспетчера. Но использование адресов IP вместо имён DNS не является лучшей практикой.

Примечание — Несмотря на то, что команда **`ovirt-engine-rename`** создаёт 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 ROSA Virtualization более ранних версий. Соответственно, везде, где возможно, рекомендуется изменять полное доменное имя диспетчера с помощью команд **`engine-cleanup`** и **`engine-setup`**.

Примечание — 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,
```

добавьте старое имя хоста в файл `/etc/hosts`, запустите утилиту oVirt Engine Rename и затем удалите старое имя хоста из `/etc/hosts`.

14.8.1.2 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]`

Даёт возможность указать новое полное доменное имя диспетчера без необходимости действий со стороны пользователей

`--log=[file]`

Даёт возможность указать путь и имя файла, в который будет записываться журнал операции переименования.

`--config=`*`[file]`*

Даёт возможность указать путь и имя файла конфигурации для использования во время операции переименования.

`--config-append=`*`[file]`*

Даёт возможность указать путь и имя файла конфигурации для добавления во время операции переименования. С помощью этого параметра можно указать путь и имя существующего файла с ответами для автоматизации операции переименования.

`--generate-answer=`*`[file]`*

Даёт возможность указать путь и имя файла, в котором записаны ответы и значения, изменённые командой **`ovirt-engine-rename`**.

14.8.1.3 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. Если да, то перед тем, как продолжать, утилита предлагает пользователю извлечь, выключить или перевести в режим обслуживания любые ВМ или домены хранения, подключённые 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:

1. Подготовьте все DNS и другие записи, необходимые для нового FQDN.
2. Обновите конфигурацию сервера DHCP, в случае, если используется DHCP.
3. Обновите имя хоста на СУСВ.
4. Выполните следующую команду:

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

5. По запросу команды нажмите **Ввод** для остановки службы engine:

```
During execution engine service will be stopped (OK, Cancel) [OK]:
```

6. По запросу команды введите новый FQDN для СУСВ:

```
New fully qualified server name:new_engine_fqdn
```

Команда **ovirt-engine-rename** обновляет записи FQDN СУСВ.

Для виртуализированного ЦУ выполните следующие дополнительные шаги:

1. На каждом из существующих узлов виртуализированного ЦУ выполните 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.

2. На каждом из узлов виртуализированного ЦУ выполните 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 удалённых машинах хранилища данных. Смена имени на этих машинах должна выполняться вручную.

Для развёртываний в удалённых хранилищах данных выполните следующие шаги на удалённой машине (не на машине диспетчера):

1. Удалите следующие файлы PKI:

```
/etc/pki/ovirt-engine/apache-ca.pem/etc/pki/ovirt-engine/apache-
grafana- ca.pem/etc/pki/ovirt-engine/certs/*/etc/pki/ovirt-engine/keys/*
```

2. Обновите 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
```

3. Выполните engine-setup с переключателем --offline для исключения выполнения обновлений в это время:

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

14.8.2. Утилита Engine Configuration

14.8.2.1 Утилита Engine Configuration

Утилита «engine configuration» является консольной утилитой для настройки глобальных параметров окружения ROSA Virtualization. Утилита взаимодействует со списком отображений «ключ-значение», которые хранятся в базе данных диспетчера виртуализации, и даёт возможность получить список всех ключей и значений, доступных для настройки. Кроме того, для каждого из уровней настройки системы ROSA Virtualization 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**.

14.8.2.2 Синтаксис команды engine-config

Утилиту engine configuration можно запускать на машине, на которой установлен диспетчер виртуализации. Для получения подробных сведений об использовании просмотрите 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, замените ИМЯ_КЛЮЧА на имя нужного ключа. Для указания версии конфигурации получаемого значения используйте параметр --cver. Если версия не указывается, выводятся значения для всех существующих версий.

– Настроить значение ключа конфигурации

```
# engine-config --set ИМЯ_КЛЮЧА=ЗНАЧЕНИЕ_КЛЮЧА --cver=ВЕРСИЯ
```

Замените *ИМЯ_КЛЮЧА* на имя конкретного настраиваемого ключа, и замените *ЗНАЧЕНИЕ_КЛЮЧА* на настраиваемое значение. В окружениях с несколькими версиями конфигурации необходимо указать *ВЕРСИЮ*.

– Для загрузки изменений перезапустите службу ovirt-engine

Для применения изменений необходимо перезапустить службу **ovirt-engine**.

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

14.8.3. Утилита Log Collector

14.8.3.1 Log Collector

Утилита для сбора файлов журналов Log Collector включена в состав ПО СУСВ. С её помощью можно легко собрать необходимые файлы журналов в окружении ROSA Virtualization, например, для создания сводки при обращении в техподдержку.

По умолчанию утилита не установлена. Для установки выполните в консоли СУСВ команду

```
# dnf install ovirt-log-collector
```

Исполняемая команда сборщика: **`ovirt-log-collector`**. Для её запуска необходимо выполнить вход в систему в качестве пользователя `root` и предоставить административные полномочия в окружении виртуализации. Команда **`ovirt-log-collector -h`** показывает сведения о её применении, включая список всех действительных параметров команды **ovirt-log-collector**.

14.8.3.2 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** и **collect**.

– Параметр **list** выводит список хостов, кластеров или дата-центров, присоединённых к диспетчеру виртуализации . Можно выполнять фильтрацию на основе списка объектов.

– Параметр **collect** 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.

В 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.

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. Используйте этот параметр 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.

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**.

--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 имён 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 имён 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 имён хостов, полных доменных имён или адресов IP. Также принимаются шаблоны для совпадения.

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.

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, используйте параметр **pg-dbhost**. Для сбора удалённых файлов журналов используйте дополнительный параметр **pg-host-key**. Для успешного сбора удалённых файлов журналов на сервере базы данных должно быть установлено расширение PostgreSQL SOS.

--no-postgresql

Отключает сбор с базы данных. Сборщик журналов подключится к базе данных PostgreSQL диспетчера виртуализации и включит эти данные в отчёт 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 используется **postgres**.

--pg-dbname= *ИМЯ_БД*

Указывает ИМЯ_БД в качестве имени базы данных для подключения к серверу баз данных. По умолчанию используется **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.

14.8.3.3 Базовое использование Log Collector

При запуске без дополнительных параметров команда **`ovirt-log-collector`** по умолчанию собирает все файлы журналов с диспетчера виртуализации и его присоединённых 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 трёх присоединённых хостов.

Пример. Использование Log Collector

```
  # 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
```

14.8.4. Утилита Engine Vacuum

14.8.4.1 Утилита 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 её параметрах смотрите в документации PostgreSQL.

Исполняемая команда утилиты: **`engine-vacuum`**. Для её запуска необходимо выполнить вход в систему в качестве пользователя root и предоставить административные полномочия в окружении ROSA Virtualization.

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.

14.8.4.2 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 объём свободного пространства, ранее используемого таблицей.

Full vacuum сжимает таблицы, записывая новые копии файлов таблиц, освобождённых от беиспользуемого пространства, тем самым давая возможность ОС получить это пространство. Работа в этом режиме занимает значительный объём 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.

14.8.4.3 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.

Общие параметры команды engine-vacuum

-h --help

Выводит сведения об использовании команды **engine-vacuum**.

-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.

```
# engine-vacuum -f -v -t vm_dynamic -t vds_dynamic
```

14.8.5. Утилита отображения имён VDSM на имена сетей

14.8.5.1 Отображение имён VDSM на имена логических сетей

Если имя логической сети состоит боле чем из 15 символов или содержит символы не в кодировке ASCII, система автоматически создаёт 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 имён логических сетей и их автоматически созданных сетевых имён, используйте утилиту **`VDSM-to-Network-Name Mapping`**, расположенную в каталоге **`/usr/share/ovirt-engine/bin/`**.

Последовательность действий по отображению имён VDSM на имена логических сетей:

1. Во время первого запуска утилиты настройте переменную среды PASSWORD, являющуюся паролем пользователя базы данных с правами на чтение базы данных диспетчера виртуализации. Например, выполните:

```
# export PASSWORD=DatabaseUserPassword
```

2. Запустите 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 имён логических сетей, отображённых на их соответствующие идентификаторы на хосте.

Дополнительные флаги

Утилиту можно запустить со следующими флагами:

--host — имя хоста/адрес IP 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 защищённое соединение с базой данных. По умолчанию, утилита выполняется с незащищённым соединением.

Глава 15. Сбор сведений об окружении

15.1 Мониторинг и наблюдаемость

В этой главе предлагается несколько способов настроить мониторинг системы ROSA Virtualization и получать системные метрики и журналы. В числе этих методов:

- Мониторинг ROSA Virtualization с помощью хранилища данных и Grafana
- Отсылка метрик на удалённый экземпляр Elasticsearch

15.1.1. Мониторинг систем ROSA Virtualization с помощью хранилища данных и Grafana

15.1.1.1 Обзор Grafana

Grafana — это веб-утилита с графическим интерфейсом для создания отчётов на базе данных, собранных в БД PostgreSQL хранилища данных oVirt с именем `ovirt_engine_history`. Подробности о доступных сводных панелях отчётов смотрите в разделе **Панели мониторинга Grafana** и Grafana website - dashboards.

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, сохранённых за 24 часа, почасовых данных за 1 месяц, для ежедневных данных выборки не сохраняются.
- **Full** (рекомендуется): выборки данных, сохранённых 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.

15.1.1.2 Установка Grafana

Интеграция Grafana включается и устанавливается по умолчанию при выполнении **engine-setup** для СУСВ в отдельной установке диспетчера, а также при установке виртуализированного ЦУ.

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 создаёт пользователей автоматически. Новых пользователей нужно создать (пункт **Invite** в графическом интерфейсе Grafana) и подтвердить, только после этого они могут входить в систему.

1. Настройте почтовый адрес пользователя на диспетчере, если он ещё не настроен.
2. Выполните вход в систему Grafana для существующего пользователя `admin` (изначально настроенный `admin`).
3. Нажмите **Configuration → Users** и выберите **Invite**.
4. Введите почтовый адрес и имя, затем выберите **Роль**.
5. Пошлите приглашение, используя одну из следующих возможностей:
   - Выберите **Send invite mail** и нажмите **Submit**. Для этой возможности необходимо иметь рабочий локальный почтовый сервер, настроенный на машине с Grafana.
   - Выберите **Pending Invites**
   - Найдите нужную запись
   - Выберите **Copy invite**
   - Скопируйте ссылку и используйте её для создания учётной записи, либо скопировав напрямую в адресную строку браузера, либо отослав её 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 в Портал мониторинга с этой учётной записью:

1. Выполните вход на приветственной странице веб-администрирования ROSA Virtualization с помощью учётной записи с этим почтовым адресом.
2. Чтобы перейти на панель мониторинга Grafana, выберите **Портал мониторинга**.
3. Выберите **Вход с помощью oVirt Engine Auth**.

15.1.1.3 Встроенные панели мониторинга Grafana

В начальной установке Grafana доступны следующие панели мониторинга со сводками из ЦОД, кластера, хоста и ВМ:

Таблица 5. Встроенные панели мониторинга Grafana

Тип панели мониторинга	Содержимое
Панели оперативных отчётов	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 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 отчёта: 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, объём памяти, дата создания, дата удаления, подробные аппаратные сведения для выбранных хостов, согласно свежим конфигурациям. Инвентарная панель доменов хранилищ: тип домена, тип хранилища, доступный объём на дисках, используемое место на дисках, общий объём дисков, дата создания и дата удаления для выбранных

	доменов хранилищ за указанный период. Инвентарная панель ВМ: имя шаблона, ОС, ядра ЦП, объём 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 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 приём/передача для сетей) для выбранных хостов за указанный период. Панель тенденций для ВМ: потребление ресурсов (число ВМ, ЦП, память, приём/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, приём/передача для сетей) для выбранных хостов за указанный период. Панель потребления ресурсов ВМ — ежедневное и ежечасное потребление ресурсов (ЦП, память, приём/передача для сетей, ввод-вывод для дисков) для выбранных ВМ за указанный период.

Примечание — На панелях Grafana присутствуют прямые ссылки на Портал администрирования ROSA Virtualization, что позволяет быстро просмотреть дополнительные сведения л кластерах, хостах и ВМ.

15.1.1.4 Настраиваемые панели Grafana

Панели Grafana можно копировать и изменять, а также создавать пользовательские панели согласно требованиям отображения сводок отчётов.

Примечание — Встроенные панели нельзя перенастроить.

15.1.2. Отправка метрик и журналов на удалённый экземпляр Elasticsearch

Примечание — Для развёртывания данной возможности необходимо иметь опыт работы по настройке и обслуживанию Elasticsearch.

На диспетчере и хостах ROSA Virtualization можно настроить отправку данных метрик и журналов на существующий экземпляр Elasticsearch.

Для этого запустите 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.

15.1.2.1 Установка collectd и rsyslog

Развёртывание **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

1. Выполните вход на машине диспетчера с помощью SSH.
2. Скопируйте **/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
```

3. Измените параметры ovirt_env_name и elasticsearch_host в config.yml и сохраните файл. В файл можно добавить 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`** укажите значение true.

Для отключения журналирования или метрик используйте параметры **`rsyslog_elasticsearch_usehttps_metrics`** и/или **`rsyslog_elasticsearch_usehttps_logs`**.

4. Разверните 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 развёртывания и настройки **rsyslog** на хосте. **rsyslog** собирает метрики из **collectd** и отправляет их в Elasticsearch.

15.1.2.2 Схема журналирования и анализ журналов

Для интерактивного просмотра данных, собранных в системе ROSA Virtualization, используйте страницу **Обнаружение**. Каждый набор собранных данных представляется в виде документа. Документы составляются из следующих файлов журналов:

- **engine.log** - содержит сведения о всех аварийных сбоях графич. 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.

Таблица 6. 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 серьёзности журнальной записи: 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`	Адрес IP 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**.

15.2 Файлы журналов

15.2.1. Файлы журналов процесса установки диспетчера виртуализации

Таблица 7. 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 ROSA Virtualization к изначальным параметрам. Журнал создаётся 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 создаёт отчётную БД ovirt_engine_history. Журнал создаётся 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-*гггггммддччммсс*.log	Журнал команды **engine-setup**. Журнал создаётся при каждом запуске команды. Дата и время запуска команды используется в имени файла для возможности одновременного существования нескольких журналов.

15.2.2. Файлы журналов диспетчера ROSA Virtualization

Таблица 8. Активность служб

Файл журнала	Описание
/var/log/ovirt-engine/engine.log	Отображает все аварийные сбои в GUI диспетчера ROSA Virtualization, поиск в Active Directory, проблемы в БД и другие события.
/var/log/ovirt-engine/host-deploy	Файлы журналов хостов, развёрнутых с помощью диспетчера виртуализации.
/var/lib/ovirt-engine/setup-history.txt	Отслеживание установок и обновлений пакетов, связанных с диспетчером ROSA Virtualization.
/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.

15.2.3. Файлы журналов SPICE

Файлы журналов SPICE удобны в ситуациях поиска и решения проблем с подключениями SPICE. Для начала запуска журналирования SPICE смените уровень журналирования на **debugging**. Затем укажите 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`**, используйте команду **`remote-viewer`**.

15.2.3.1 Журналы SPICE для серверов SPICE гипервизора

Таблица 9. 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 выполните 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, не на уровне кластера.

15.2.3.2 Журналы SPICE для гостевых машин

Таблица 10. 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

15.2.3.3 Журналы SPICE для клиентов, запущенных с помощью console.vv

Для клиентских машин на Linux:

1. Включите отладку SPICE, выполнив команду **remote-viewer** с параметром **--spice-debug**. По запросу команды введите URL подключения, например, spice:*//virtual_machine_IP:port*.

```
# remote-viewer --spice-debug
```

2. Для запуска клиента SPICE с параметром debug и для передачи ему файла `.vv`, скачайте файл `console.vv`, запустите команду `remote-viewer` с параметром `--spice-debug` и укажите полный путь до файла `console.vv`.

```
# remote-viewer --spice-debug /path/to/console.vv
```

Для клиентских машин на Windows:

1. В версиях `virt-viewer 2.0-11.el7ev` и более поздних, файл `virt-viewer.msi` устанавливает `virt-viewer` и `debug-viewer.exe`.
2. Запустите команду `remote-viewer` с аргументом `spice-debug` и направьте команду на путь до консоли:

```
remote-viewer --spice-debug path\to\console.vv
```

3. Для просмотра журналов подключитесь к ВМ, чтобы увидеть приглашение командной строки с выполняющимся GDB со стандартным выводом и стандартные ошибки для remote-viewer.

15.2.4. Файлы журналов хостов

Таблица 11. Файлы журналов хостов

Файл журнала	Описание
`/var/log/messages`	Файл журнала, используемый **libvirt**. Для просмотра журнала используйте **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.
`/var/log/vdsm/vdsm.log`	Файл журнала VDSM, агента диспетчера на хостах.
`/tmp/ovirt-host-deploy-`*`Date`*`.log`	Журнал развёртывания хоста, который после удачного развёртывания 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.

15.2.5. Настройка отладочного уровня журналирования для служб ROSA Virtualization

Примечание — Указание отладочного уровня для журналирования может открыть доступ к такой конфиденциальной информации, как пароли или внутренние данные ВМ. Убедитесь, что у недоверенных или неавторизованных пользователей не будет доступа к журналам отладки.

Отладочный уровень журналов следующих служб ROSA Virtualization можно настроить, отредактировав файл **sysconfig** каждой из служб.

Таблица 12. Службы ROSA Virtualization и пути до файлов sysconfig

Сервис	Путь файла
ovirt-engine.service	/etc/sysconfig/ovirt-engine
ovirt-engine-dwhd.service	/etc/sysconfig/ovirt-engine-dwhd
ovirt-fence-kdump-listener.service	/etc/sysconfig/ovirt-fence-kdump-listener
ovirt-websocket-proxy.service	/etc/sysconfig/ovirt-websocket-proxy

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.

Убедитесь в существовании файла **sysconfig**, который необходимо изменить. Создайте его при необходимости.

Последовательность действий для настройки отладочного уровня журналирования для служб ROSA Virtualization:

1. Добавьте следующее содержимое в файл sysconfig службы:

```
OVIRT_SERVICE_DEBUG=1
```

2. Перезапустите службу:

```
# systemctl restart <service>
```

Уровень файла журнала **sysconfig** службы теперь отладочный.

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**.

15.2.6. Основные файлы конфигураций служб ROSA Virtualization

В дополнение к файлам **sysconfig**, для каждой службы системы ROSA Virtualization существует ещё один файл конфигурации, используемый гораздо чаще.

Таблица 13. Службы и конфигурационные файлы системы ROSA Virtualization

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

15.2.7. 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 ROSA Virtualization.

Последовательность действий по настройке сервера журналирования хоста:

1. Проверьте, разрешён ли трафик на порте UDP 514, и открыт ли он для трафика службы syslog:

```
# firewall-cmd --query-service=syslog
```

При выводе **no**, разрешите трафик на порте **UDP 514** с помощью:

```
# firewall-cmd --add-service=syslog --permanent
# firewall-cmd --reload
```

2. Создайте новый файл .conf на сервере syslog, например, **/etc/rsyslog.d/from_remote.conf**, и добавьте 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")
```

3. Перезапустите службу `rsyslog`:

```
# systemctl restart rsyslog.service
```

4. Выполните вход в систему на гипервизоре и добавьте следующую строку в `/etc/rsyslog.conf`:

```
        *.info;mail.none;authpriv.none;cron.none  @<syslog-FQDN>:514
```

5. Перезапустите службу rsyslog на гипервизоре.

```
# systemctl restart rsyslog.service
```

Централизованный сервер теперь настроен на получение, хранение и обеспечение защиты для файлов журналов хостов виртуализации.

15.2.8. Включение использования SyslogHandler для передачи журналов диспетчера ROSA Virtualization на удалённый 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.

Выполните следующую последовательность действий 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 раздел **Настройка сервера журналирования хоста**.

Настройка реализации SyslogHandler

1. В каталоге `/etc/ovirt-engine/engine.conf.d` создайте файл `90-syslog.conf` со следующим содержимым:

```
        SYSLOG_HANDLER_ENABLED=true
        SYSLOG_HANDLER_SERVER_HOSTNAME=localhost
        SYSLOG_HANDLER_FACILITY=USER_LEVEL
```

2. Разрешите трафик rsyslog в SELinux.

```
# semanage port -a -t syslogd_port_t -p udp 514
```

3. Создайте 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")
```

4. Перезапустите службу rsyslog.

```
# systemctl restart rsyslog.service
```

5. Если межсетевой экран включён и активен, выполните следующую команду для добавления необходимых правил для открытия портов `rsyslog в Firewalld`:

```
# firewall-cmd --permanent --add-port=514/udp
# firewall-cmd --reload
```

6. Перезапустите диспетчер ROSA Virtualization.

```
# systemctl restart ovirt-engine
```

7. Сервер syslog теперь может получать и хранить файлы `engine.log`.

Часть IV. Дополнительные настройки

Глава 16. Настройка двухфакторной аутентификации

16.1. Двухфакторная аутентификация для SSH с использованием «Рутокен ЭЦП»

Рассмотрим пример настройки двухфакторной аутентификации с использованием «Рутокен ЭЦП».

Настройка двухфакторной аутентификации для SSH

Для примера настройки двухфакторной аутентификации для SSH консоли используется хост с гипервизором под управлением ROSA Virtualization 3.0. В качестве токена для аутентификации используется ранее подготовленный USB Рутокен ЭЦП 2.0 для двухфакторной аутентификации на web-портале ROSA Virtualization 3.0 для пользователя **`ovirtadmin`**. С процедурой подготовки токена можно ознакомиться в соответствующем разделе документации.

Подключите токен к USB порту компьютера, на котором ранее выполнялась подготовка этого токена и с помощью консольной команды проверьте 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        : 6/32
```

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>
Private Key Object; RSA
  label:      login_ovirtadmin
  ID:         10
  Usage:      decrypt, sign
  Access:     sensitive
Certificate Object; type = X.509 cert
  label:      login_ovirtadmin
  subject:    DN: O=EXAMPLE.COM, CN=ovirtadmin
  ID:         10
```

Создайте публичный ключ для SSH консоли на основе пользовательского сертификата, хранящегося на подключенном USB токене:

```
$ ssh-keygen -D /usr/lib64/librtpkcs11ecp.so -I 0:10 > ovirtadmin_key.pub
```

Используя утилиту **ssh-copy-id** скопируйте полученный публичный ключ **ovirtadmin_key.pub** на хост, на котором требуется настроить двухфакторную аутентификацию для SSH консоли:

```
$ ssh-copy-id -f -i ovirtadmin_key.pub root@rosa-virt01.example.com
```

Для включения двухфакторной аутентификации для SSH консоли на хосте с гипервизором требуется отредактировать конфигурационный файл SSH сервера **/etc/ssh/sshd_config**, изменив или добавив соответствующие строки как показано ниже:

```
        PubkeyAuthentication yes
        AuthorizedKeysFile .ssh/authorized_keys
        PasswordAuthentication yes
        PermitEmptyPasswords no
        UsePAM yes
        AuthenticationMethods publickey,password
```

Такая конфигурация SSH сервера будет требовать обязательной аутентификации по ssh ключу и паролю, что приведёт к нарушению работы между виртуальной машиной СУСВ и хостом. Чтобы предотвратить такую ситуацию, необходимо в самом конце файла **/etc/ssh/sshd_config** добавить строки:

```
        Match Address 192.168.1.164
                AuthenticationMethods publickey password
```

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.

Перезапустите сервис sshd:

```
# systemctl restart sshd
```

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>
```

16.2. Двухфакторная аутентификация для web-портала ROSA Virtualization 3.0

Двухфакторная аутентификация на web-портале ROSA Virtualization основана на USB токене с приватным ключом и клиентским сертификатом, имени пользователя и его пароле. Для этого потребуется полная замена корневого сертификата системы управления средой виртуализации (СУСВ).

Примечание — 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 её 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 ROSA Virtualization и всех сертификатов, подписанных им.

1. Новый корневой сертификат и приватный ключ будет взят из файла **`/root/cacert.p12`** который создаётся в процессе установки IPA сервера. Файл защищён паролем о чём свидетельствует скриншот, полученный в процессе установки IPA:

```
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
```

Рис. 169. 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 необходимо 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 фай **ovirt_hosts** в той директории из которой предполагается запускать скрипт, к примеру, в директории /**root**. В этом файле должны быть прописаны все хосты, подключенные к системе управления средой виртуализации. 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.

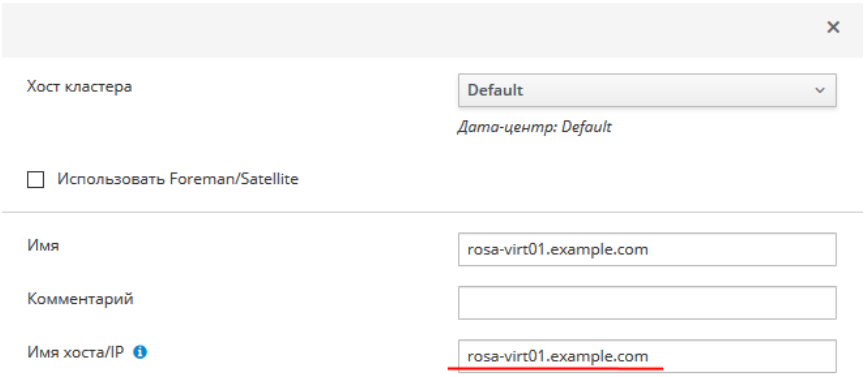

Рис. 170. Параметр «Имя хоста» при добавлении хоста в систему

Согласно этим данным заполнить файл **ovirt_hosts**. В конце файла, после всех введённых данных 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
```

На любом из активных хостов системы виртуализации, который был настроен для запуска и миграции виртуализированного ЦУ, включить режим глобального обслуживания выполнив команду в консоли хоста:

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

Для замены сертификата 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
```

--name - это общая часть в именах новых файлов корневого сертификата и ключа, в нашем случаи ipa-ca от файлов `ipa-ca.pem` и `ipa-ca.key`.

--new-key - указывает на необходимость пересоздать приватные ключи для сертификатов.

--domain - домен локальной сети в котором находятся подключенные хосты.

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 ROSA Virtualization в раздел "**Администрирование**" → "**Поставщики**", выбрать строку **ovirt-provider-ovn** и нажать кнопку "**Изменить**".

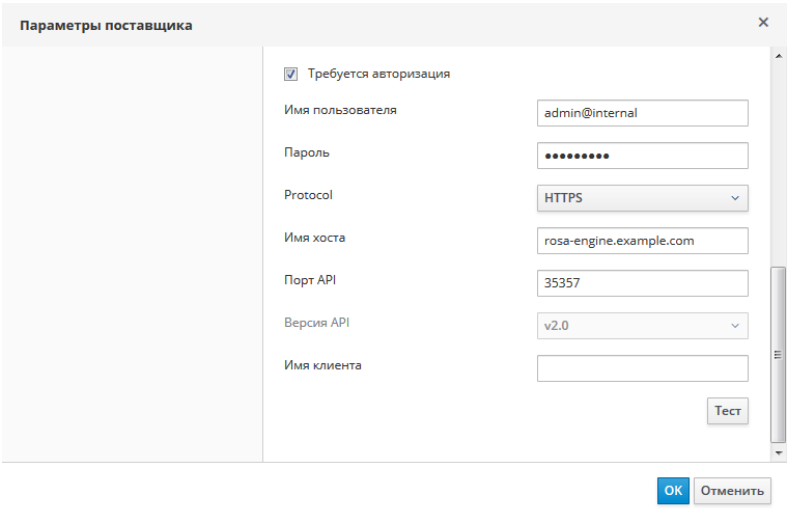

Рис. 171. Окно «Параметры поставщика»

В открывшемся окне ввести пароль для пользователя **`admin@internal`** (учётная запись администратора во внутреннем домене СУСВ). Нажать кнопку "**Тест**" и согласиться импортировать сертификат. После удачного завершения теста нажать кнопку "**ОК**".

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 делается 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. Перевести хост в режим обслуживания, нажав "**Управление**" → "**Обслуживание**". Запустить переустановку хоста, нажав "**Установка**" → "**Переустановить**". Хост с виртуальной машиной **HostedEngine** переустанавливается в последнюю очередь.

На данном этапе процесс замены корневого сертификата СУСВ считается завершённым и можно отключить режим глобального обслуживания, выполнив в консоли хоста, с которого он был включен, команду:

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

2. 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, к примеру, `ovirtadmin`. Для этого в консоли IPA сервера выполнить команды:

```
# kinit admin
# ipa user-add ovirtadmin --first=ovirtadmin --last=ovirtadmin
```

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'
```

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 web-порталу ROSA Virtualization, создаются аналогичным способом.

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 завершённым.

3. В качестве аппаратного хранилища приватного ключа и сертификата в данном примере будет использован USB «Рутокен ЭЦП» 2.0.

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. 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 тут: **`/usr/lib64/librtpkcs11ecp.so`**.

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
```

Подключить Рутокен к USB порту компьютера и выполнить его форматирование:

```
$ ./rtadmin -f -q -z /usr/lib64/librtpkcs11ecp.so \
-a <PIN-код администратора> -u <PIN-код пользователя>
```

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>
```

Если для подготовки токена используется операционная система 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 тут **`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>
```

Открыть панель управления Рутокен, перейти на вкладку **"Сертификаты",** выбрать токен и нажать на кнопку **"Импорт"**.

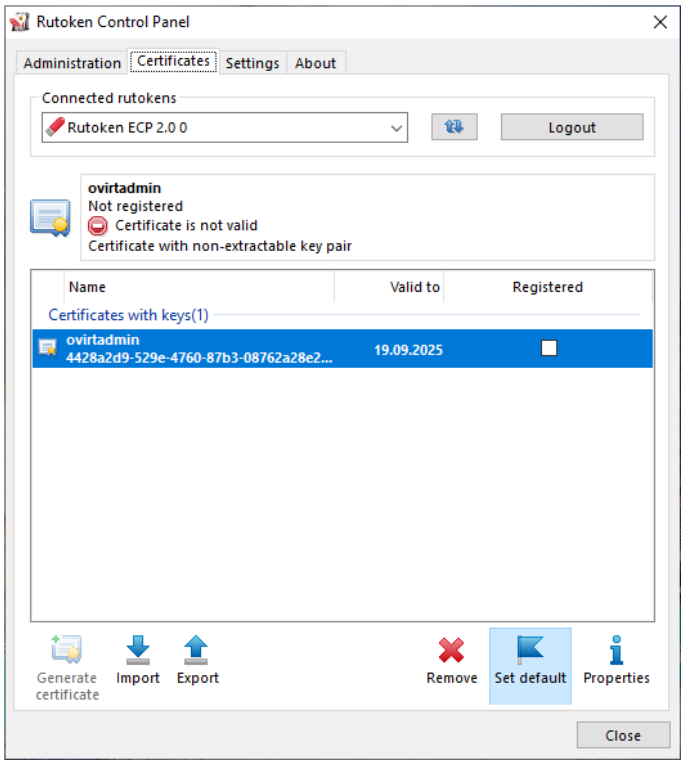

Рис. 172. Контрольная панель Рутокен – вкладка Сертификаты

Указать путь к ранее подготовленному файлу `ovirtadmin.p12`, ввести пароль который был задан при его создании и нажать на кнопку **"Импорт"**.

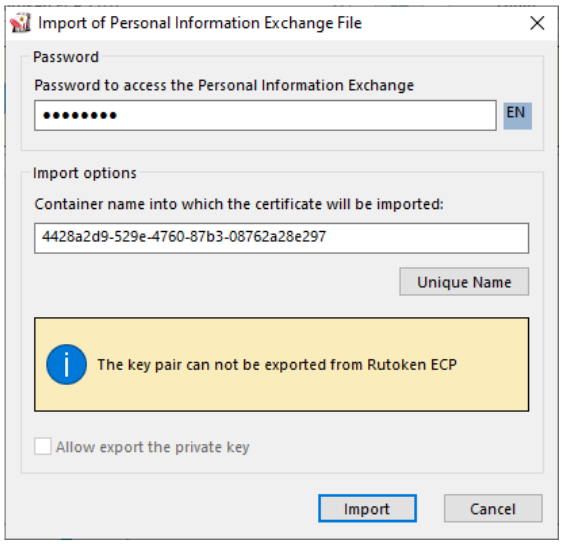

Рис. 173. Ввод пароля для файла

Ввести пин код пользователя для подключенного токена. В результате приватный ключ и сертификат пользователя из файла `ovirtadmin.p12` будут импортированы на устройство Рутокен.

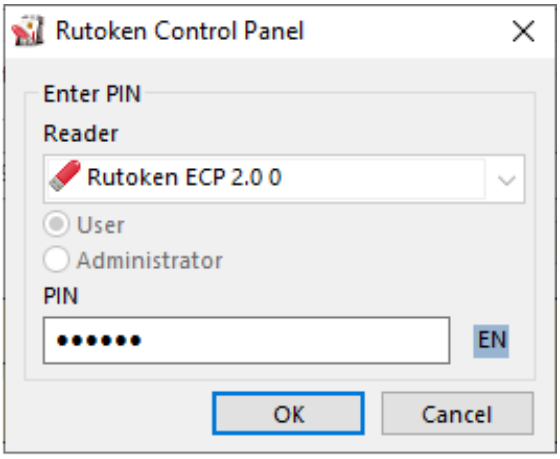

Рис. 174. Ввод пин кода для «Рутокен ЭЦП»

4. Для включения двухфакторной аутентификации на web-портале ROSA Virtualization необходимо 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>
```

Отредактировать файл `/etc/ovirt-engine/engine.conf.d/60-ovirt-2fa.conf`, установив для переменной `TWO_FACTOR_AUTHENTICATION` значение `true`:

```
        TWO_FACTOR_AUTHENTICATION=true
```

Для переменной **OVIRT_ADMIN_LOGIN** установить значение **ovirtadmin** (логин учётной записи на IPA сервере сертификат от которой будет сопоставлен с внутренней учётной записью **admin** системы управления средой виртуализации):

```
        OVIRT_ADMIN_LOGIN=ovirtadmin
```

Перезапустить сервис httpd:

```
# systemctl restart httpd
```

5. При необходимости контроля отозванных сертификатов требуется дополнительная настройка httpd сервера. Контроль может осуществляться с помощью сервиса OCSP, предоставляемого IPA сервером, либо с помощью CRL.

5.1. 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.

5.2. Вариант контроля отозванных сертификатов на основе CRL более сложен в реализации и требует больше настроек. 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`. 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
```

Далее 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>
```

В независимости от того какой вариант контроля отозванных сертификатов был выбрал, 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).

6. Пример настройки браузера Firefox для работы с USB «Рутокен ЭЦП 2.0».

В адресной строке браузера ввести **about:preferences#privacy** или перейти по вкладкам меню **«Tools» → «Settings» → «Privacy & Security»**.

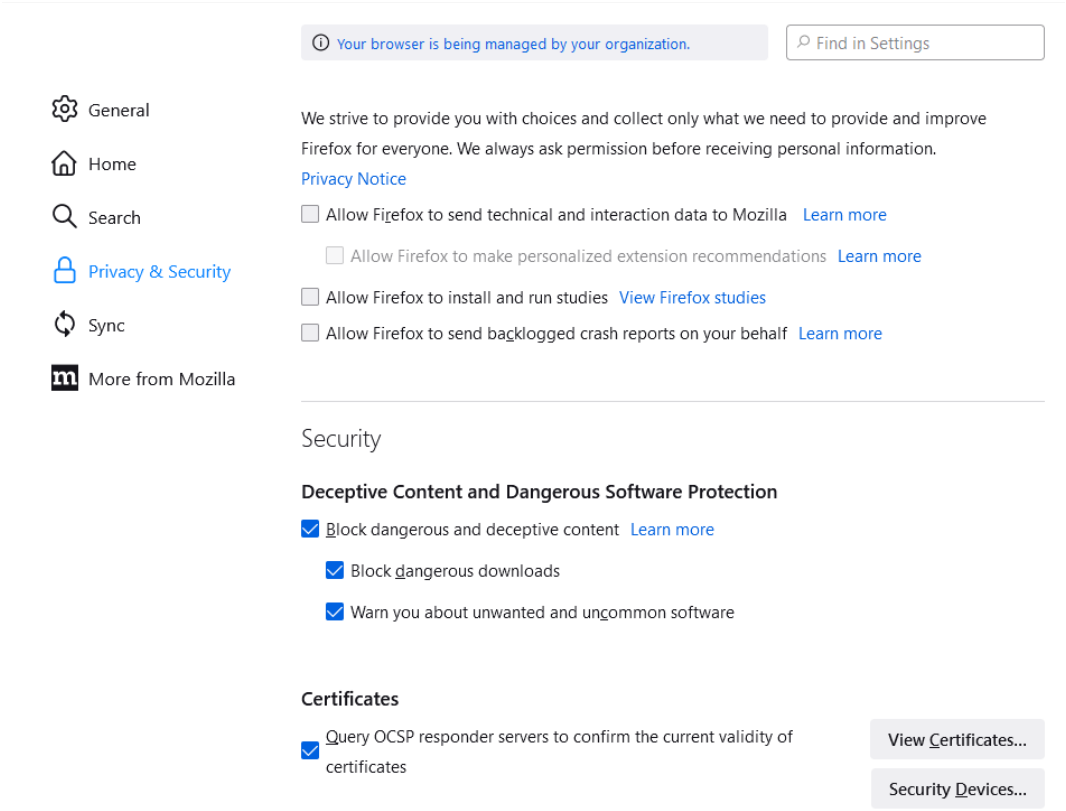

Рис. 175. Настройки браузера Firefox

Нажать кнопку **Security Devices**, в окне **Device Manager** нажать **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).

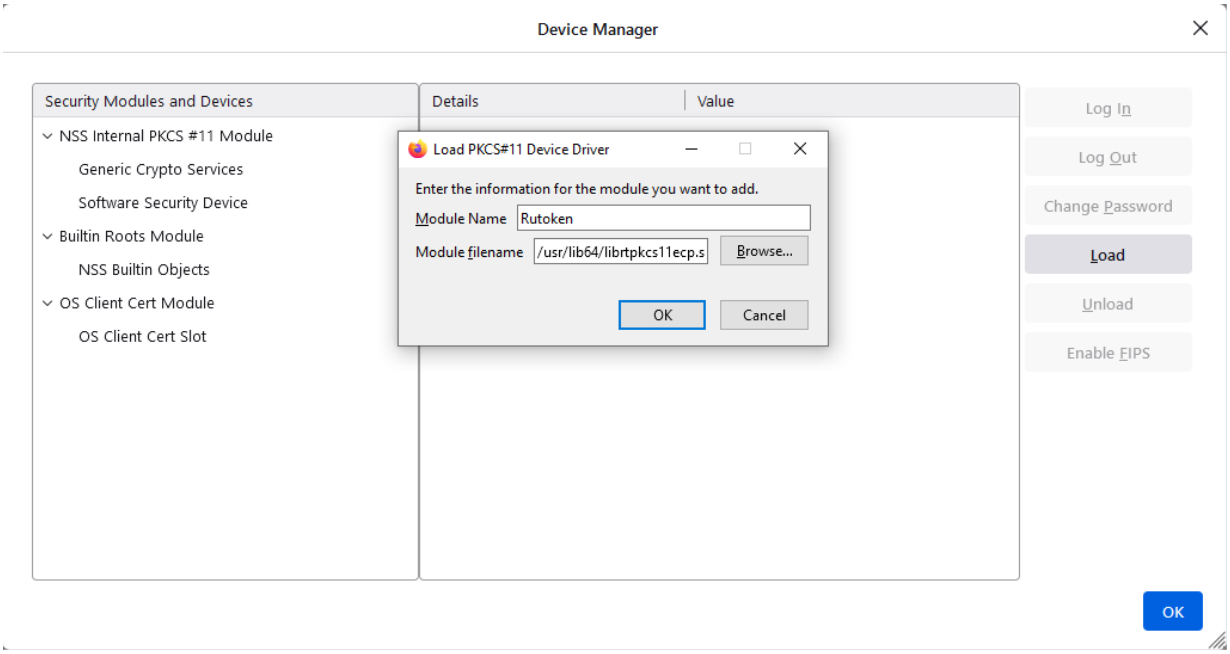

Рис. 176. Настройки браузера с библиотеками библиотекой PKCS#11

16.3. Двухфакторная аутентификация в локальной консоли с использованием «Рутокен ЭЦП»

Все действия по настройки двухфакторной аутентификации для локальной консоли выполняются на хосте с гипервизором под управлением ROSA Virtualization 3.0.

1. Необходимо убедиться, что на хосте установлены следующие пакеты и если они отсутствуют, то установить: `opensc`, `pcsc-lite`, `pcsc-lite-ccid`, `pam_pkcs11`, `nss-tools`. Установить библиотеку PKCS#11 для операционных систем GNU/Linux x64 https://www.rutoken.ru/support/download/pkcs/.

После установки пакета PKCS#11, необходимая для работы с токеном, библиотека будет находиться тут **`/usr/lib64/librtpkcs11ecp.so`**. В качестве токена для аутентификации используется ранее подготовленный USB «Рутокен ЭЦП 2.0» для двухфакторной аутентификации на web-портале ROSA Virtualization 3.0 для пользователя **ovirtadmin**.

С процедурой подготовки токена можно ознакомиться в соответствующем разделе документации. 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         : 6/32
```

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>
  Private Key Object; RSA
    label:      login_ovirtadmin
    ID:         10
    Usage:      decrypt, sign
    Access:     sensitive
  Certificate Object; type = X.509 cert
    label:      login_ovirtadmin
    subject:    DN: O=EXAMPLE.COM, CN=ovirtadmin
    ID:         10
```

2. Следующий этап - настройка модуля `pam_pkcs11`. Создать структуру каталогов и установить необходимые права доступа:

```
  # mkdir /etc/pam_pkcs11/{nssdb,cacerts,crls}
  # chmod 0644 /etc/pam_pkcs11/{nssdb,cacerts,crls}
```

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
```

Создать пустую базу данных для сертификатов и импортировать в неё 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
```

Присутствие корневого сертификата в базе данных можно проверить командой:

```
  # certutil -L -d /etc/pam_pkcs11/nssdb

  Certificate Nickname                                         Trust Attributes
                                                               SSL,S/MIME,JAR/XPI

  ipa-ca                                                       CT,C,C
```

Сделать резервную копию существующего файла **`/etc/pam_pkcs11/pam_pkcs11.conf`**:

```
  # mv /etc/pam_pkcs11/pam_pkcs11.conf \
  /etc/pam_pkcs11/pam_pkcs11.conf.default
```

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;
        }
      }
```

Для сопоставления сертификата, хранящегося на токене, и учётной записи пользователя **root**, под которой будет осуществляться локальный вход в систему, необходимо 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
```

Получить строку **`"CN=ovirtadmin,O=EXAMPLE.COM"`** для добавления в файл можно 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 учётной записью для которой сопоставлен сертификат в файле **/etc/pam_pkcs11/subject_mapping**.

3. Следующий этап настройки – включение двухфакторной аутентификации для локальной консоли. Для этого требуется внести соответствующие изменения в систему PAM, отредактировав файл `/etc/pam.d/system-auth`, как показано ниже:

```
[root@rosa-virt03 ~]# cat /etc/pam.d/system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authselect is run.
auth        required      pam_env.so
auth        required      pam_unix.so try_first_pass nullok
auth        [success=done ignore=ignore default=die] pam_pkcs11.so nodebug wait_for_card
auth        required      pam_deny.so

account     required      pam_unix.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so try_first_pass use_authtok nullok sha512 shadow
password    required      pam_deny.so
```

Рис. 177. Редактирование файла /etc/pam.d/system-auth

В файле необходимо 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 **PIN** код к подключенному USB токену.

```
rosa-virt03 login: root
Password:
Smart card found.
Welcome Rutoken!
Smart card PIN:
verifying certificate
Checking signature
Last login: Wed Sep 20 16:31:26 on tty1
[root@rosa-virt03 ~]# _
```

Рис. 178. Ввод пин кода для «Рутокен ЭЦП»

В случаи отсутствия USB токена аутентификация будет прервана.

В консоль будет выведено сообщение:

```
        Smartcard authentication cancelled
```

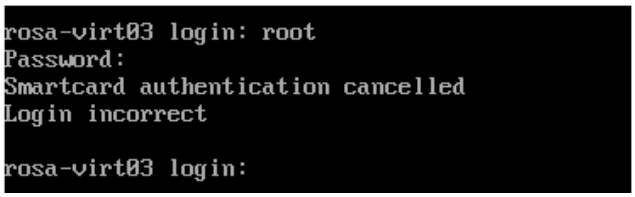

Рис. 179. Сбой аутентификации «Рутокен ЭЦП»

Глава 17. Настройка vGPU

В данном руководстве описывается процесс настройки vGPU на примере NVIDIA RTX A6000.

Для настройки vGPU воспользуйтесь следующей инструкцией:

17.1. 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 системе управления средой виртуализации.

1. Отредактировать в файле `/etc/default/grub` строку `GRUB_CMDLINE_LINUX`, добавив параметры загрузки ядра
   `"rdblacklist=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 rdblacklist=nouveau intel_iommu=on
loglevel=4"
```

2. 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
```

3. Для установки драйверов требуется включить репозиторий DVD и смонтировать диск в директорию /mnt:

```
# dnf config-manager --set-enabled DVD
# mount -t iso9660 -o ro /dev/sda1 /mnt
```

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
```

Далее необходимо перезагрузить хост.

4. Проверьте с какими параметрами загрузилось ядро. Это действие можно выполнить с помощью команд:

```
# dmesg | grep "Command line"
# cat /proc/cmdline
```

Проверьте какие модули ядра используются для vGPU с помощью команд:

```
# 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 | 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                                                 |
+-----------------------------------------------------------------------------+
```

Далее создайте 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
```

После чего перезагрузите хост. Если всё 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)
```

5. Подключите хост к СУСВ стандартным способом, используя **Портал Администрирования**.

17.2. Установка драйвера vGPU

На следующем шаге настройки необходимо создать виртуальную машину и установить гостевую ОС стандартным способом. Выключить ВМ и на портале администрирования в разделе "**Ресурсы**" → "**Виртуальные машины**" открыть окно со свойствами настраиваемой ВМ нажав мышкой на ссылку в поле "**Имя**". Далее перейти на вкладку "**Устройства хоста**" и нажать кнопку "**Управление vGPU**". В открывшемся окне выбрать vGPU которое будет подключено к виртуальной машине. Перевести переключатель

"**Вторичный видеоадаптер для VNC**" в положение "**Выкл.**", нажать кнопку "**Сохранить**".

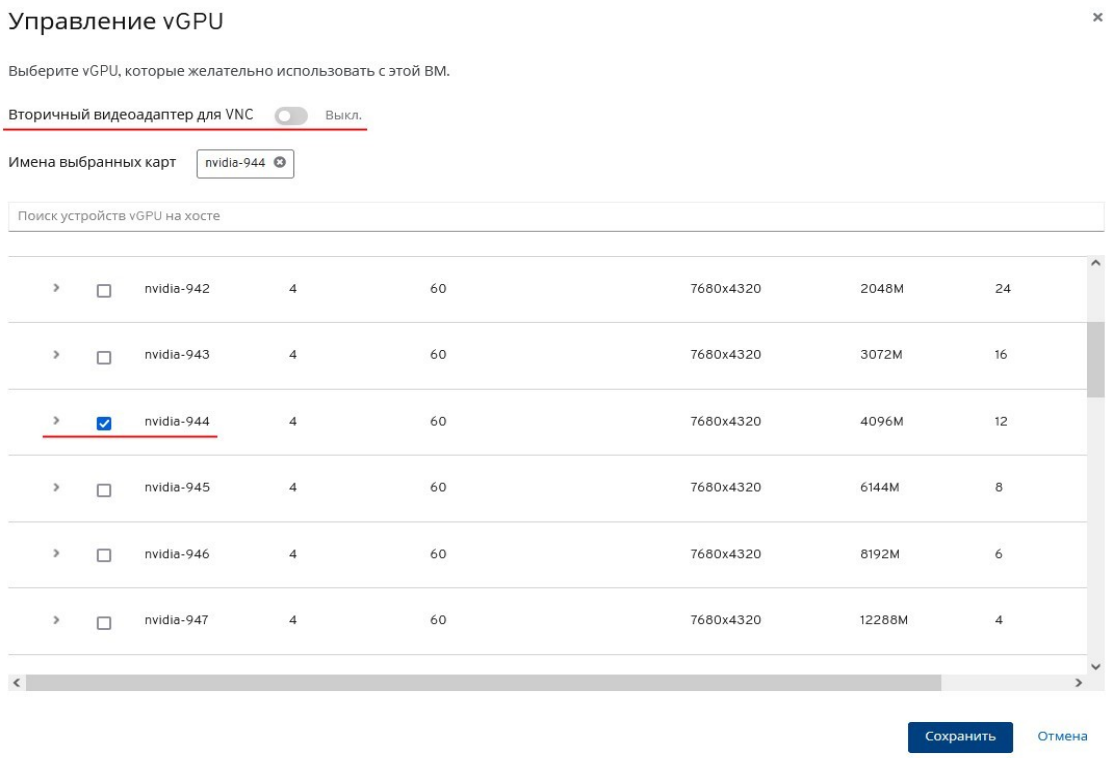

Рис. 180. Настройка vGPU

Далее запустите ВМ и подключитесь к SPICE консоли для установки vGPU драйвера. Диспетчер устройств до установки драйвера не будет отображать подключенных видеоадаптеров, как указано на рисунке ниже.

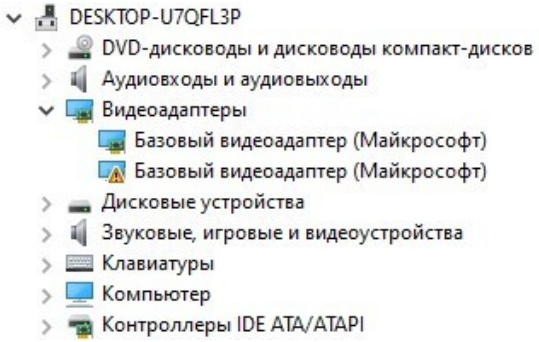

Рис. 181. Диспетчер устройств до установки vGPU драйвера

17.3. Настройка драйвера vGPU для ВМ

После установки драйвера необходимо выключить ВМ и вновь открыть окно "**Управление vGPU**" и перевести переключатель "**Вторичный видеоадаптер для VNC**" в положение "**Вкл.**"

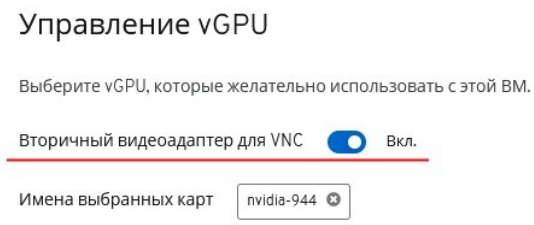

Рис. 182. Активация параметра "Вторичный видеоадаптер для VNC"

Запустите вновь виртуальную машину. В диспетчере устройств должен появиться соответствующий видео адаптер:

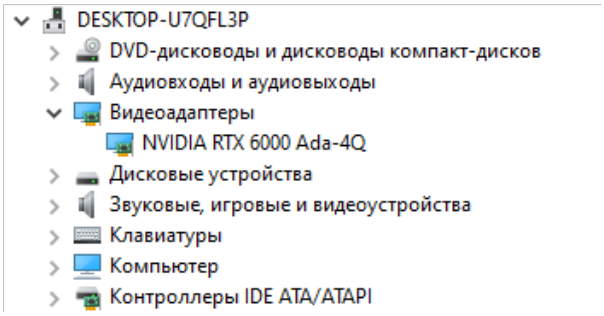

Рис. 183. Отображение подключенного видеоустройства в Диспетчере устройств

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 |
  +-----------------------------------------------------------------------------+
```

Глава 18. Развёртывание подсистемы мониторинга и отчётности Grafana

Grafana — это мультиплатформенное веб-приложение для аналитики и интерактивной визуализации.

Развёртывание Grafana

1. Переведите окружение в режим глобального обслуживания:

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

2. Войдите в систему, предназначенную для развёртывания Grafana, и выполните следующую команду:

```
# engine-setup --reconfigure-optional-components
```

3. При выводе следующих запросов нажмите клавишу `Enter`, чтобы установить Grafana:

```
        Configure Grafana on this host (Yes, No) [Yes]:
        Renew certificate (Yes, No) [Yes]:
```

4. Отключите глобальный режим обслуживания:

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

Для доступа к панелям управления Grafana нажмите **Портал мониторинга** на странице приветствия Портала администрирования, или перейдите по адресу `https://<доменное_имя/IP-адрес_виртуализированного_ЦУ>/ovirt-engine-grafana`.

Приложение А. VDSM и перехватчики событий

А.1. VDSM

Виртуализированный ЦУ использует службу VDSM (Virtual Desktop and Server Manager, служба 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 приложении А, используется Python.

Обратите внимание, что выполняются все сценарии, настроенные для события на хосте. Если необходимо, чтобы указанный перехватчик событий запускался только для определённого набора виртуальных машин, выполняемых на этом хосте, тогда необходимо, чтобы это обеспечивал сам сценарий с помощью оценки настраиваемых пользователем свойств ВМ (см. подраздел А.7. Настройка свойств, указываемых пользователем).

Предупреждение — перехватчики событий VDSM могут вмешиваться в работу системы виртуализации ROSA Virtualization. Программная ошибка перехватчика может потенциально привести к фатальному сбою в работе ВМ и к потере данных. Перехватчики событий VDSM должны быть реализованы разработчиками с осторожностью и тщательно тестироваться перед применением.

А.3. Расширение VDSM с помощью перехватчиков событий

В приложении А описывается как расширить VDSM с помощью перехватчиков, запускаемых при определённых событиях. Расширение VDSM с помощью перехватчиков событий является экспериментальной технологией, поэтому информация в приложении А предназначена для опытных разработчиков.

С помощью настраиваемых пользователем свойств ВМ, перехватчикам событий можно передавать дополнительные параметры, специфичные для данной ВМ.

A.4. Поддерживаемые события VDSM

В **Табл. A.1** описываются поддерживаемые события VDSM.

Табл. A.1. Поддерживаемые события VDSM

Название	Описание
`before_vm_start`	Перед запуском ВМ
`after_vm_start`	После запуска ВМ
`before_vm_cont`	Перед продолжением выполнения ВМ
`after_vm_cont`	После продолжения выполнения ВМ
`before_vm_pause`	Перед приостановкой работы ВМ
`after_vm_pause`	После приостановки работы ВМ
`before_vm_hibernate`	Перед входом ВМ в режим гибернации
`after_vm_hibernate`	После входа ВМ в режим гибернации
`before_vm_dehibernate`	Перед выходом ВМ из режима гибернации
`after_vm_dehibernate`	После выхода ВМ из режима гибернации
`before_vm_migrate_source`	Перед миграцией ВМ выполняются на исходном хосте, с которого осуществляется миграция
`after_vm_migrate_source`	После миграции ВМ выполняются на исходном хосте, с которого осуществляется миграция
`before_vm_migrate_destination`	Перед миграцией ВМ выполняются на целевом хосте, на который осуществляется миграция
`after_vm_migrate_destination`	После миграции ВМ выполняются на целевом хосте, на который осуществляется миграция
`after_vm_destroy`	После разрушения ВМ
`before_vdsm_start`	Перед запуском VDSM на хосте. Перехватчики событий before_vdsm_start

Название	Описание
	выполняются от имени суперпользователя `root` и не наследуют окружение процесса VDSM
`after_vdsm_stop`	После остановки VDSM на хосте. Перехватчики событий after_vdsm_stop выполняются от имени суперпользователя `root` и не наследуют окружение процесса VDSM
`before_nic_hotplug`	Перед горячим подключением сетевой карты к машине
`after_nic_hotplug`	После горячего подключения сетевой карты к машине
`before_nic_hotunplug`	Перед горячим отключением сетевой карты от машины
`after_nic_hotunplug`	После горячего отключения сетевой карты от машины
`after_nic_hotplug_fail`	После сбоя горячего подключения сетевой карты к машине
`after_nic_hotunplug_fail`	После сбоя горячего отключения сетевой карты от машины
`before_disk_hotplug`	Перед горячим подключением диска к машине
`after_disk_hotplug`	После горячего подключения диска к машине
`before_disk_hotunplug`	Перед горячим отключением диска от машины
`after_disk_hotunplug`	После горячего отключения диска от машины
`after_disk_hotplug_fail`	После сбоя горячего подключения диска к машине
`after_disk_hotunplug_fail`	После сбоя горячего отключения диска от машины
`before_device_create`	Перед созданием устройства,

Название	Описание
	поддерживающего настраиваемые пользователями свойства
`after_device_create`	После создания устройства, поддерживающего настраиваемые пользователями свойства
`before_update_device`	Перед обновлением устройства, поддерживающего настраиваемые пользователями свойства
`after_update_device`	После обновления устройства, поддерживающего настраиваемые пользователями свойства
`before_device_destroy`	Перед разрушением устройства, поддерживающего настраиваемые пользователями свойства
`after_device_destroy`	После разрушения устройства, поддерживающего настраиваемые пользователями свойства
`before_device_migrate_destination`	Перед миграцией устройства выполняются на целевом хосте, на который осуществляется миграция
`after_device_migrate_destination`	После миграции устройства выполняются на целевом хосте, на который осуществляется миграция
`before_device_migrate_source`	Перед миграцией устройства выполняются на исходном хосте, с которого осуществляется миграция
`after_device_migrate_source`	После миграции устройства выполняются на исходном хосте, с которого осуществляется миграция
`after_network_setup`	После настройки сети при запуске машины хоста
`before_network_setup`	Перед настройкой сети при запуске машины хоста

A.5. Окружение VDSM перехватчиков событий

Большинство сценариев перехватчиков событий выполняются от имени пользователя `vdsm` и наследуют окружение процесса VDSM.

Исключениями являются сценарии перехватчиков, запускаемых событиями `before_vdsm_start` и `after_vdsm_stop`. Сценарии перехватчиков, запускаемых этими событиями, выполняются от имени суперпользователя `root` и не наследуют окружение процесса VDSM.

A.6. Объект XML домена перехватчиков событий VDSM

При запуске сценариев перехватчиков событий к окружению добавляется переменная `_hook_domxml`, которая содержит путь до XML-представления домена `libvirt` соответствующей ВМ.

Исключениями являются следующие перехватчики событий, у которых переменная `_hook_domxml` содержит XML-представление сетевой карты, а не виртуальной машины:

- *_nic_hotplug_*
- *_nic_hotunplug_*
- *_update_device
- *_device_create
- *_device_migrate_*

Примечание — перехватчики событий `before_migration_destination` и `before_dehibernation` на данный момент получают XML домена исходного хоста (XML домена цели будет иметь некоторые отличия).

VDSM использует формат XML домена библиотеки `libvirt` для описания виртуальных машин. Сведения об этом формате можно найти по ссылке http://libvirt.org/formatdomain.html.

UUID виртуальной машины можно получить с помощью XML домена, а также в виде значения переменной окружения `vmId`.

A.7. Настройка свойств, указываемых пользователем

Настраиваемые пользователем свойства, принимаемые диспетчером виртуализации и, в свою очередь, передаваемые пользовательским перехватчикам событий определяются с помощью команды `engine-config`. Выполняйте эту команду с правами суперпользователя `root` на хосте, где установлен диспетчер виртуализации.

Конфигурационные ключи `UserDefinedVMProperties` и `CustomDeviceProperties` команды `engine-config` используются для хранения имён поддерживаемых пользовательских свойств виртуальной машины и устройства соответственно. В этих ключах также присутствуют регулярные выражения, определяющие действительные значения для каждого именованного пользовательского свойства.

Несколько пользовательских свойств разделяются точками с запятой без пробела. Обратите внимание, что при указании конфигурационного ключа, все уже содержащиеся в нём существующие значения перезаписываются. При указании новых и уже существующих пользовательских свойств в команду необходимо включать все пользовательские свойства, используемые для указания значения ключа.

После обновления ключа конфигурации необходимо перезапустить службу `ovirt-engine` для применения изменений.

Настройка пользовательского свойства `smartcard` (свойство ВМ)

1. Выполните следующую команду для проверки уже имеющихся пользовательских свойств ВМ, настроенных ключом конфигурации `UserDefinedVMProperties`:

```
# engine-config -g UserDefinedVMProperties
```

Из вывода ниже видно, что уже настроено пользовательское свойство `memory` (при этом регулярное выражение `^[0-9]+$` гарантирует, что пользовательское свойство `memory` будет содержать только числовые символы):

```
# engine-config -g UserDefinedVMProperties
UserDefinedVMProperties:  version: 3.6
UserDefinedVMProperties:  version: 4.0
UserDefinedVMProperties:  memory=^[0-9]+$ version: 4.0
```

2. Добавьте новое пользовательское свойство `smartcard` к уже настроенному пользовательскому свойству `memory`. При этом укажите, что новое свойство `smartcard` может принимать значения `true` или `false`:

```
# engine-config -s UserDefinedVMProperties='memory=^[0-9]+$; \
smartcard=^(true|false)$' --cver=4.0
```

3. Выполните следующую команду для проверки конфигурации пользовательских свойств `memory` и `smartcard`:

```
# engine-config -g UserDefinedVMProperties
UserDefinedVMProperties:  version: 3.6
UserDefinedVMProperties:  version: 4.0
UserDefinedVMProperties:  memory=^[0-9]+$;smartcard=^(true|false)$ version:
4.0
```

4. Для применения изменений в конфигурации пользовательских свойств ВМ перезапустите службу `ovirt-engine`:

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

Настройка пользовательского свойства `interface` (свойство устройства)

1. Выполните следующую команду для проверки уже имеющихся пользовательских свойств устройства, настроенных ключом конфигурации `CustomDeviceProperties`:

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

Из вывода ниже видно, что пользовательские свойства для устройства ещё не были настроены:

```
  # engine-config -g CustomDeviceProperties
  CustomDeviceProperties:  version: 3.6
  CustomDeviceProperties:  version: 4.0
```

2. Добавьте новое пользовательское свойство `interface`. При этом укажите, что значение параметра `prop` настраивается в диапазоне от 0 до 99999, а параметр `duplex` может принимать значения `full` или `half`:

```
  # engine-config -s CustomDeviceProperties="{type=interface;prop=
{speed=^([0-9]{1,5})$;duplex=^(full|half)$}}" --cver=4.0
```

3. Выполните следующую команду для проверки конфигурации пользовательского свойства `interface`:

```
  # engine-config -g CustomDeviceProperties
  UserDefinedVMProperties:  version: 3.6
  UserDefinedVMProperties:  version: 4.0
  UserDefinedVMProperties: {type=interface;prop={speed=^([0-9]{1,5})$;
duplex=^(full|half)$}} version: 4.0
```

4. Для применения изменений в конфигурации пользовательских свойств устройства перезапустите службу `ovirt-engine`:

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

A.8. Настраиваемые пользователем свойства ВМ

Как только пользовательские свойства были настроены в виртуализированном ЦУ, можно начинать настраивать их на виртуальных машинах. Пользовательские свойства настраиваются во вкладке **Настраиваемые пользователем свойства** окон **Новая ВМ** и **Параметры виртуальной машины** на Портале администрирования.

Пользовательские свойства также можно настроить в диалоговом блоке **Запуск ВМ**. Свойства, настраиваемые в этом блоке, применяются к ВМ только до следующего выключения этой ВМ.

Вкладка **Настраиваемые пользователем свойства** предоставляет возможность выбора из списка настроенных пользовательских свойств. После выбора ключа пользовательского свойства открывается дополнительное поле, в котором необходимо указать значение выбранного ключа. Добавляйте дополнительные пары «ключ-значение», нажимая на кнопку + (плюс), и удаляйте их с помощью кнопки – (минус).

A.9. Оценка пользовательских свойств ВМ в перехватчике событий VDSM

Во время вызова сценариев перехватчиков событий каждый ключ, указанный в поле **Настраиваемые пользователем свойства** виртуальной машины, добавляется в качестве переменной окружения. Хотя регулярные выражения, используемые для валидации полей **Настраиваемых пользователем свойств**, предоставляют некоторую защиту, необходимо обеспечить также оценку соответствия ввода значениям, ожидаемым регулярными выражениями.

Оценка настраиваемых пользователем свойств

Следующий пример, написанный на Python, проверят существование пользовательского свойства `key1`. Если свойство настроено, тогда его значение выводится в стандартных ошибках. Если пользовательское свойство `key1` не настроено, никаких действий не предпринимается.

```
#!/usr/bin/python

import os
import sys

if os.environ.has_key('key1'):
    sys.stderr.write('key1 value was : %s\n' % os.environ['key1'])
else:
    sys.exit(0)
```

A.10. Использование модуля перехватчиков событий VDSM

В составе VDSM поставляется модуль перехватчиков событий, написанный на Python, который предоставляет вспомогательные функции для сценариев перехватчиков событий VDSM. Данный модуль предоставляется в качестве примера, и относится только к перехватчикам VDSM, написанным на Python.

Модуль перехватчиков событий поддерживает чтение XML библиотеки `libvirt` виртуальной машины в объект DOM. Далее, сценарии перехватчиков событий управляют объектом с помощью Python, встроенного в библиотеку `xml.dom` (http://docs.python.org/release/2.6/library/xml.dom.html). Затем с помощью модуля перехватчиков изменённый объект можно снова сохранить в XML библиотеки `libvirt`.

В Табл. А.2 описываются функции модуля перехватчиков событий, предназначенные для поддержки разработки перехватчиков.

Табл. А.2. Функции модуля перехватчиков событий

Имя	Аргумент	Описание
`tobool`	строка	Преобразовывает строку «верно» или «ложно» в логическое значение
`read_domxml`		Читает XML библиотеки libvirt виртуальной машины в объект DOM

Имя	Аргумент	Описание
`write_domxml`		Записывает XML библиотеки libvirt виртуальной машины в объект DOM

A.11. Выполнение перехватчиков событий VDSM

Некоторые сценарии перехватчиков событий могут редактировать XML домена и изменять параметры VDSM виртуальной машины. Выполнять эти действия нужно с осторожностью. Сценарии перехватчиков событий потенциально могут нарушить работу VDSM, а сценарии с программными ошибками могут привести к перерывам в работе окружения системы виртуализации ROSA Virtualization. В частности, никогда не изменяйте UUID домена, и не пытайтесь удалять устройства из доменов без достаточного понимания процесса и последствий.

Как сценарий `before_vdsm_start`, так и сценарий `after_vdsm_stop` выполняются от имени суперпользователя `root`. Другие сценарии, которым необходим доступ `root`, должны писаться с использованием команды `sudo` для повышения привилегий. Для поддержки этого необходимо обновить информацию в файле `/etc/sudoers` так, чтобы пользователь `vdsm` мог использовать `sudo` без повторного введения пароля, так как сценарии перехватчиков событий выполняются без вмешательства со стороны пользователя.

Настройка `sudo` для сценариев перехватчиков событий VDSM

В следующем примере команда `sudo` будет настроена так, чтобы разрешить пользователю `vdsm` выполнять команду `/bin/chown` от имени суперпользователя `root`.

1. Выполните вход в систему хоста виртуализации с правами `root`.
2. Откройте файл `/etc/sudoers` в текстовом редакторе.
3. Добавьте в файл следующую строку:

```
vdsm ALL=(ALL) NOPASSWD: /bin/chown
```

В результате пользователь `vdsm` может запускать команду `/bin/chown` от имени суперпользователя `root`. Параметр `NOPASSWD` указывает, что при вызове `sudo` не будет предлагаться пользователю ввести пароль.

Таким образом после внесения этих изменений, в перехватчиках событий VDSM также можно использовать команду `sudo` для запуска `/bin/chown` от имени суперпользователя `root`.

В следующем коде на Python команда `sudo` используется для выполнения `/bin/chown` с правами суперпользователя `root` относительно файла `/my_file`:

```
  retcode = subprocess.call( ["/usr/bin/sudo", "/bin/chown", "root",
"/my_file"] )
```

Примечание — поток стандартных ошибок сценариев перехватчиков событий собирается в журнале VDSM. Эту информацию можно использовать при отладке сценариев перехватчиков событий.

A.12. Коды возврата перехватчиков событий VDSM

В Табл. А.3 описываются коды возврата сценариев перехватчиков событий. Коды возврата определяют, обрабатывает ли VDSM сценарий.

Табл. А.3. Коды возврата перехватчиков событий

Код	Описание
0	Сценарий перехватчика событий успешно завершил работу
1	Сценарий перехватчика событий завершился сбоем, нужно обрабатывать другие перехватчики
2	Сценарий перехватчика событий завершился сбоем, другие перехватчики обрабатывать не нужно
>2	Зарезервировано

A.13. Примеры перехватчиков событий VDSM

Примечание — все сценарии перехватчиков событий, устанавливаемые в систему администратором, вне зависимости от их происхождения, должны быть тщательно протестированы для конкретного окружения.

Тонкая настройка узла NUMA

Данный сценарий перехватчика событий даёт возможность отрегулировать выделение памяти на хосте NUMA с использованием настроенного пользователем свойства `numaset`:

```
        numaset=^(interleave|strict|preferred):[\^]?\d+(-\d+)?(,[\^]?\d+(-
    \d+)?)*$
```

Используемое регулярное выражение даёт возможность настроенному пользователем свойству `numaset` конкретной ВМ указать как режим распределения памяти (`interleave`, `strict`, `preferred`), так и используемый узел. При этом два значения разделяются двоеточием (`:`).

С помощью регулярного выражения можно указать `nodeset` как:

- Конкретный узел (например `numaset=strict:1` указывает, что будет использован только узел 1).
- Диапазон узлов (например `numaset=strict:1-4` указывает, что будут использоваться узлы с 1 по 4).
- Неиспользуемый узел (например `numaset=strict:^3` указывает, что узел 3 не будет использоваться).
- Любое сочетание вышеуказанных значений, через запятые (например `numaset=strict:1-4,6` указывает, что будут использоваться узлы с 1 по 4, а также узел 6).

Сценарий перехватчика событий `/usr/libexec/vdsm/hooks/before_vm_start/50_numa`:

```
#!/usr/bin/python

import os
import sys
import hooking
import traceback

'''
numa hook
=========
add numa support for domain xml:

<numatune>
    <memory mode="strict" nodeset="1-4,^3" />
</numatune>

memory=interleave|strict|preferred

numaset="1" (use one NUMA node)
numaset="1-4" (use 1-4 NUMA nodes)
numaset="^3" (don't use NUMA node 3)
numaset="1-4,^3,6" (or combinations)

syntax:
    numa=strict:1-4
'''

if os.environ.has_key('numa'):
    try:
        mode, nodeset = os.environ['numa'].split(':')

        domxml = hooking.read_domxml()

        domain = domxml.getElementsByTagName('domain')[0]
        numas = domxml.getElementsByTagName('numatune')

        if not len(numas) > 0:
            numatune = domxml.createElement('numatune')
            domain.appendChild(numatune)

            memory = domxml.createElement('memory')
            memory.setAttribute('mode', mode)
            memory.setAttribute('nodeset', nodeset)
            numatune.appendChild(memory)

            hooking.write_domxml(domxml)
        else:
            sys.stderr.write('numa: numa already exists in domain xml')
```

```
                sys.exit(2)
        except:
            sys.stderr.write('numa: [unexpected error]: %s\n' %
traceback.format_exc())
            sys.exit(2)
```

Приложение В. Свойства сетей, настраиваемые пользователем

В.1. Параметры bridge_opts

В **Табл. В.1** описываются параметры `bridge_opts`.

Табл. В.1. Параметры bridge_opts

Параметр	Описание
`forward_delay`	Временной интервал в децисекундах, во время которого мост слушает и получает информацию. Если за это время не будет обнаружена петля коммутации, мост войдёт в состояние передачи данных. Этот параметр даёт время на проверку трафика и структуры сети до начала обычной работы сети
`gc_timer`	Параметр указывает время сборки мусора в децисекундах, после которого база данных, данные для которой передаёт мост, проверяется и очищается от устаревших записей
`group_addr`	При отправке общего запроса значение параметра устанавливается на ноль. При отправке запроса, касающегося конкретной группы, а также запроса, касающегося группы и источника, значение параметра устанавливается на IP-адрес многоадресной рассылки
`group_fwd_mask`	Параметр даёт возможность мосту передавать локальные адреса групп каналов. Смена изначального значения параметра разрешает нестандартное поведение моста
`hash_elasticity`	Максимальная длина цепи, разрешённая в хэш-таблице. Значение параметра вступает в силу после добавления новой многоадресной группы. Если после повторного хэширования значение не может быть соблюдено, то происходит хэш-конфликт, и отслеживание отключается
`hash_max`	Максимальное число хэш-сегментов в таблице. Значение параметра должно быть степенью числа 2. Значение вступает в силу

Параметр	Описание
	немедленно, и это значение не может быть меньше текущего значения записей многоадресных групп
`hello_time`	Временной интервал в децисекундах между отправками сообщений 'hello', сообщающих о местоположении моста в сетевой топологии. Применяется, только если данный мост является корневым мостом связующего дерева
`hello_timer`	Время в децисекундах с последней отправки сообщения 'hello'
`max_age`	Максимальный промежуток времени в децисекундах, для получения сообщения 'hello' от другого корневого моста, после которого мост будет считаться «мёртвым» и начнётся процесс перехвата полномочий
`multicast_last_member_count`	Параметр указывает число запросов 'last member', посылаемых в многоадресную группу, после принятия сообщения 'leave group' от хоста
`multicast_last_member_interval`	Время в децисекундах между запросами 'last member'
`multicast_membership_interval`	Время в децисекундах, в течение которого мост ждёт ответа от участника многоадресной группы перед прекращением отправки многоадресного трафика на хост
`multicast_querier`	Параметр указывает, будет ли на мосту активно работать многоадресный опрашиватель или нет. При получении мостом запроса 'multicast host membership' от хоста в другой сети, этот хост отслеживается в течение таймера, основанного на времени получения запроса и времени интервала между многоадресными запросами. Если мост позднее попытается перенаправить трафик этого запроса на членство в многоадресной группе, или обменяется информацией с запрашивающим многоадресным роутером, то указанный таймер подтвердит действительность

Параметр	Описание
	опрашивателя. Если опрашиватель действителен, многоадресный трафик доставляется с помощью существующей многоадресной таблицы моста. Если опрашиватель не действителен, трафик посылается со всех портов моста. Для увеличения производительности в широковещательных доменах с существующим или ожидаемым многоадресным членством должен работать как минимум один многоадресный опрашиватель
multicast_querier_interval	Максимальный промежуток времени в децисекундах от последнего запроса 'multicast host membership', полученного от хоста, для подтверждения того, что хост действителен
multicast_query_use_ifaddr	Логическое значение. По умолчанию «0», и в этом случае опрашиватель в качестве адреса-источника для запросов IPv4 использует 0.0.0.0. При изменении значения по умолчанию, в качестве адреса-источника устанавливается IP-адрес моста
multicast_query_interval	Время в децисекундах между сообщениями запросов, посылаемых мостом для подтверждения действительности участия в многоадресных группах. В этом промежутке, а также если мост попросили отослать запрос на членство в этой многоадресной группе, мост проверяет состояние своего собственного опрашивателя, основываясь на времени получения запроса плюс значение multicast_query_interval. Если запрос был послан в рамках значения последнего интервала multicast_query_interval, то повторно он не посылается
multicast_query_response_interval	Промежуток времени в децисекундах, в течение которого мосту можно ответить на запрос после отправки. Значение должно быть меньше или равно значению multicast_query_interval

Параметр	Описание
`multicast_router`	Параметр даёт возможность включать или отключать порты с подключёнными мультивещательными маршрутизаторами. Порт с одним или несколькими мультивещательными маршрутизаторами получит весь многоадресный трафик. Параметр может принимать следующие значения: 0 — полностью отключает; 1 — система с помощью запросов автоматически определяет присутствие маршрутизаторов; 2 — активирует постоянное получение всего многоадресного трафика на портах
`multicast_snooping`	Параметр даёт возможность включать или отключать механизм отслеживания. Процесс отслеживания трафика позволяет мосту прослушивать трафик между маршрутизаторами и хостами для поддержания карты фильтрации многоадресного трафика на соответствующие каналы. Параметр даёт возможность пользователю повторно включить отслеживание, если оно было автоматически выключено из-за хэш-конфликта, но если хэш-конфликт не был разрешён, отслеживание включено не будет
`multicast_startup_query_count`	Параметр указывает число запросов, отправленных при запуске для определения информации о многоадресном членстве
`multicast_startup_query_interval`	Время в децисекундах между запросами, отправленными при запуске для определения информации о многоадресном членстве

B.2. Настройка использования команды ethtool в виртуализированном ЦУ

На Портале администрирования можно настроить свойства `ethtool` для сетевых карт хоста. По умолчанию ключ `ethtool_opts` недоступен, его необходимо добавить в виртуализированный ЦУ с помощью утилиты настройки ЦУ. Также на хостах необходимо установить дополнительный пакет перехватчиков событий для VDSM.

Добавление ключа ethtool_opts в виртуализированный ЦУ

1. Выполните следующую команду на машине виртуализированного ЦУ для добавления ключа `ethtool_opts`:

```
# engine-config -s UserDefinedNetworkCustomProperties=ethtool_opts=.* --
cver=4.0
```

2. Для применения изменений в конфигурации перезапустите службу `ovirt-engine`:

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

3. На тех хостах, где нужно настроить параметры `ethtool`, установите пакет с перехватчиками событий VDSM. По умолчанию пакет `vdsm-hook-ethtool-options` установлен на хостах виртуализации, а на стандартных хостах его необходимо установить дополнительно. Для этого выполните следующую команду:

```
# yum install vdsm-hook-ethtool-options
```

В результате на Портале администрирования станет доступен ключ `ethtool_opts`.

B.3. Настройка использования протокола FCoE в виртуализированном ЦУ

На Портале администрирования можно настроить параметры протокола FCoE для сетевых карт хоста. По умолчанию ключ `fcoe` недоступен, его необходимо добавить в виртуализированный ЦУ с помощью утилиты настройки ЦУ. Также на хостах необходимо установить дополнительный пакет перехватчиков событий для VDSM. В зависимости от типа карты FCoE на хосте, может потребоваться настройка дополнительных параметров.

Примечание — для проверки, был ли уже активирован ключ `fcoe`, выполните следующую команду:

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

Добавление ключа FCoE в виртуализированный ЦУ

1. Выполните следующую команду на машине виртуализированного ЦУ для добавления ключа `fcoe`:

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

2. Для применения изменений в конфигурации перезапустите службу `ovirt-engine`:

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

3. На тех хостах, где нужно настроить параметры FCoE, установите пакет с перехватчиками событий VDSM. По умолчанию пакет `vdsm-hook-fcoe`

установлен на хостах виртуализации, а на стандартных хостах его необходимо установить дополнительно. Для этого выполните следующую команду:

```
# yum install vdsm-hook-fcoe
```

В результате на Портале администрирования станет доступен ключ `fcoe`.

Приложение С. Модули пользовательского интерфейса

С.1. Модули пользовательского интерфейса

В системе виртуализации ROSA Virtualization существует поддержка модулей пользовательского интерфейса (модулей UI), что позволяет интегрировать Портал администрирования с другими системами. Каждый модуль UI представляет собой набор расширений UI, который можно поместить в пакет и распространять для использования в системе виртуализации.

Модули пользовательского интерфейса системы виртуализации ROSA Virtualization интегрируются в Портал администрирования напрямую на клиенте с помощью языка программирования JavaScript. Модули вызываются Порталом администрирования и выполняются во время выполнения JavaScript веб-браузера. Модули UI могут использовать язык JavaScript и его библиотеки.

Во время ключевых событий в течение времени их выполнения Портал администрирования вызывает отдельные модули с помощью функций обработки событий, представляющих собой обмен информацией между Порталом администрирования и модулем. Хотя Портал администрирования поддерживает множество функций обработки событий, модуль объявляет только те функции, которые представляют интерес для его реализации. Перед запуском в работу Порталом администрирования, каждый модуль должен зарегистрировать соответствующие функции обработки событий как часть последовательности программы самозагрузки модуля.

Для облегчения обмена информацией между модулем UI и Порталом администрирования открывается доступ к API модуля как к глобальному (верхнего уровня) объекту pluginApi, который может быть поглощён отдельными модулями. Каждый модуль получает отдельный экземпляр pluginApi, давая возможность Порталу администрирования контролировать вызовы функций API этого модуля со стороны каждого отдельного модуля с учётом жизненного цикла модуля.

С.2. Жизненный цикл модуля пользовательского интерфейса

С.2.1. Этапы жизненного цикла модуля пользовательского интерфейса

Базовый жизненный цикл модуля пользовательского интерфейса разделён на следующие этапы:

- Обнаружение модуля UI.
- Загрузка модуля UI.
- Самонастройка модуля UI.

С.2.2. Обнаружение модуля пользовательского интерфейса

Создание дескрипторов модуля — это первый шаг в процессе обнаружения модуля UI. Дескрипторы модуля содержат важные метаданные модуля и возможные конфигурации модуля UI.

Как часть обработки запросов страницы HTML Портала администрирования (`HTTP GET`), инфраструктура модуля UI пытается обнаружить и загрузить дескрипторы из локальной файловой системы. Для каждого дескриптора инфраструктура также пытается

загрузить соответствующие пользовательские конфигурации, используемые для переопределения параметров модуля по умолчанию (если такие есть) и настроить поведение модуля во время исполнения. Пользовательская конфигурация модуля является опциональной. После загрузки дескрипторов и соответствующих файлов пользовательских конфигураций, `oVirt Engine` собирает данные модуля UI и встраивает их в страницу HTML Портала администрирования для оценки во время исполнения.

По умолчанию дескрипторы модуля расположены в `$ENGINE_USR/ui-plug-ins` с отображением по умолчанию на `ENGINE_USR=/usr/share/ovirt-engine`, что настроено в локальной конфигурации `oVirt Engine`. Ожидается, что дескрипторы модуля отвечают требованиям спецификаций формата JSON, но в дескрипторах разрешаются комментарии в стиле Java/C++ (`/*` и `//`) в качестве дополнения к спецификациям JSON.

По умолчанию пользовательские конфигурации модуля расположены в `$ENGINE_ETC/ui-plug-ins`, с отображением по умолчанию на `ENGINE_USR=/usr/share/ovirt-engine`, что настроено в локальной конфигурации `oVirt Engine`. Ожидается, что пользовательские конфигурации модуля отвечают требованиям тех же спецификаций, что и дескрипторы.

Примечание — конфигурационные файлы модуля обычно следуют соглашению о наименованиях `<descriptorFileName>-config.json`.

C.2.3. Загрузка модуля пользовательского интерфейса

После обнаружения и встраивания данных модуля UI в страницу HTML Портала администрирования осуществляется загрузка модуля в составе запуска приложения (если только для модуля не была отключена такая загрузка).

Для каждого обнаруженного модуля Портал администрирования создаёт элемент HTML `iframe`, используемый для загрузки страницы хоста модуля. Страница хоста модуля необходима для начала процесса самонастройки, используемого для оценки кода модуля в контексте элемента `iframe` этого модуля. Инфраструктура модуля UI поддерживает обслуживание файлов ресурсов модуля (например, страница хоста модуля) из локальной файловой системы. Страница хоста модуля загружается в элемент `iframe`, и происходит оценка кода модуля. После оценки кода модуль UI обменивается информацией с Порталом администрирования с помощью API.

C.2.4. Самонастройка модуля пользовательского интерфейса

Процесс самонастройки модуля UI состоит из последовательного выполнения следующих шагов:

1. Получите экземпляр `pluginApi` для указанного модуля.
2. Опционально получите объект конфигурации модуля времени выполнения.
3. Зарегистрируйте функции соответствующего обработчика событий.
4. Сообщите инфраструктуре модуля UI, что можно инициализировать модуль.

Примечание — следующий отрывок кода демонстрирует процесс самонастройки модуля UI:

```
  // Access plug-in API using 'parent' due to this code being evaluated
within the context of an iframe element.
```

```
  // As 'parent.pluginApi' is subject to Same-Origin Policy, this will only
work when WebAdmin HTML page and plug-in
  // host page are served from same origin. WebAdmin HTML page and plug-in
host page will always be on same origin
  // when using UI plug-in infrastructure support to serve plug-in resource
files.
  var api = parent.pluginApi('MyPlugin');

  // Runtime configuration object associated with the plug-in (or an empty
object).
  var config = api.configObject();

  // Register event handler function(s) for later invocation by UI plug-in
infrastructure.
  api.register({
         // UiInit event handler function.
           UiInit: function() {
                      // Handle UiInit event.
                            window.alert('Favorite music band is ' +
config.band);
                                 }
  });

  // Notify UI plug-in infrastructure to proceed with plug-in initialization.
  api.ready();
```

C.3. Файлы модуля пользовательского интерфейса

В **Табл. C.1** описываются файлы модуля UI, а также указывается расположение этих файлов в системе.

Табл. C.1. Файлы модуля UI

Файл	Расположение	Примечания
Файлы дескриптора модуля (метаданные)	`/usr/share/ovirt-engine/ui-plugins/my-plugin.json`	
Пользовательские файлы конфигурации модуля	`/etc/ovirt-engine/ui-plugins/my-plugin-config.json`	
Файлы ресурсов модуля	`/usr/share/ovirt-engine/ui-plugins/<resourcePath>/PluginHostPage.html`	`<resourcePath>` настраивается с помощью соответствующего атрибута дескриптора модуля

C.4. Пример развёртывания модуля пользовательского интерфейса

В следующей пошаговой инструкции описывается процесс создания модуля UI, запускающего программу `Hello World!` при выполнении входа в систему на Портале администрирования виртуализированного ЦУ.

Развёртывание модуля `Hello World!`

1. Создайте следующий дескриптор модуля в виде файла `/usr/share/ovirt-engine/ui-plugins/helloWorld.json` в виртуализированном ЦУ:

```
{
    "name": "HelloWorld",
    "url": "/ovirt-engine/webadmin/plugin/HelloWorld/start.html",
    "resourcePath": "hello-files"
}
```

2. Создайте следующую страницу хоста модуля в виде файла `/usr/share/ovirt-engine/ui-plugins/hello-files/start.html` в виртуализированном ЦУ:

```
<!DOCTYPE html><html><head>
<script>
    var api = parent.pluginApi('HelloWorld');
    api.register({
  UiInit: function() { window.alert('Hello world'); }
    });
    api.ready();
</script>
</head><body></body></html>
```

В случае успешной реализации модуля `Hello World!` следующая заставка (Рис. 184. Заставка модуля Hello World!) появится при выполнении входа в систему на Портале администрирования виртуализированного ЦУ.

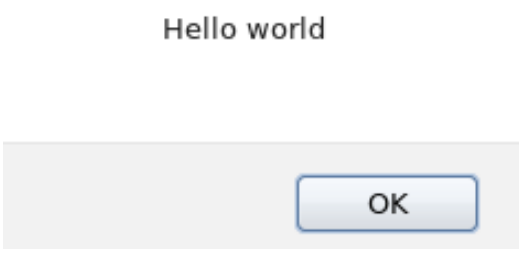

Рис. 184. Заставка модуля Hello World!

Приложение D. Система виртуализации и шифрование связи

D.1. Замена сертификата ЦС виртуализированного ЦУ

Идентификацию пользователей виртуализированного ЦУ, подключающихся с использованием протокола HTTPS, можно выполнять с помощью сертификата стороннего Центра сертификации (ЦС) организации.

Примечание — использование сертификата стороннего ЦС для подключений по протоколу HTTPS не влияет на сертификат, используемый для аутентификации между виртуализированным ЦУ и хостами, так как в последнем случае используется самоподписанный сертификат, созданный виртуализированным ЦУ.

Перед выполнением процедуры замены сертификата ЦС виртуализированного ЦУ убедитесь в наличии и характеристиках следующих информационных объектов:

- Сертификат стороннего ЦС. Цепочка сертификатов должна отслеживаться вплоть до корневого сертификата. В процедуре подразумевается, что сертификат стороннего ЦС находится в `/tmp/3rd-party-ca-cert.pem`.
- Закрытый ключ, который планируется для использования с Apache httpd, не должен содержать пароль. В процедуре подразумевается, что закрытый ключ находится в `/tmp/apache.key`.
- Сертификат ключа, выпущенный сторонним ЦС. В процедуре подразумевается, что сертификат ключа находится в `/tmp/apache.cer`.

Предупреждение — не изменяйте владельца и права доступа к каталогу `/etc/pki` и его подкаталогам. Права доступа для каталогов `/etc/pki` и `/etc/pki/ovirt-engine` должны оставаться правами по умолчанию, то есть `755`.

Если закрытый ключ и сертификат ключа были получены из стороннего ЦС в виде файла с расширением `*.p12`, извлеките их с помощью следующей инструкции, в которой подразумевается, что полученный файл находится в `/tmp/apache.p12`. В случае других форматов файла свяжитесь со сторонним ЦС для консультации.

Извлечение сертификата и закрытого ключа из файла с расширением `*.p12`

Примечание — внутренний ЦС системы хранит закрытый ключ и сертификат ключа в файле `/etc/pki/ovirt-engine/keys/apache.p12`.

1. Создайте резервную копию текущего файла `apache.p12`:

```
# cp -p /etc/pki/ovirt-engine/keys/apache.p12 \
/etc/pki/ovirt-engine/keys/apache.p12.bck
```

2. Замените текущий файл на файл, полученный из стороннего ЦС:

```
# cp /tmp/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

3. Извлеките закрытый ключ и сертификат ключа в необходимое местоположение (если файл защищён паролем, добавьте параметр `-passin pass:_password_`, где замените *password* текущим паролем):

```
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 \
-nocerts -nodes > /tmp/apache.key
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 \
-nokeys > /tmp/apache.cer
```

Замена сертификата ЦС виртуализированного ЦУ для Apache

1. Переведите окружение в режим глобального обслуживания:

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

2. Добавьте сертификат стороннего ЦС в хранилище доверенных сертификатов хоста:

```
# cp /tmp/3rd-party-ca-cert.pem /etc/pki/ca-trust/source/anchors
# update-ca-trust
```

3. Удалите символьную ссылку `/etc/pki/ovirt-engine/apache-ca.pem` на `/etc/pki/ovirt-engine/ca.pem`, настроенную в виртуализированном ЦУ по умолчанию:

```
# rm /etc/pki/ovirt-engine/apache-ca.pem
```

4. Сохраните сертификат ЦС как `/etc/pki/ovirt-engine/apache-ca.pem`:

```
# cp /tmp/3rd-party-ca-cert.pem /etc/pki/ovirt-engine/apache-ca.pem
```

5. Создайте резервную копию закрытого ключа и сертификата ключа:

```
  # cp /etc/pki/ovirt-engine/keys/apache.key.nopass
/etc/pki/ovirt-engine/keys/apache.key.nopass.bck
  # cp /etc/pki/ovirt-engine/certs/apache.cer
/etc/pki/ovirt-engine/certs/apache.cer.bck
```

6. Скопируйте закрытый ключ в необходимое местоположение:

```
# cp /tmp/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
```

7. Укажите суперпользователя `root` в качестве владельца закрытого ключа и настройте права доступа `0640`:

```
# chown root:ovirt  /etc/pki/ovirt-engine/keys/apache.key.nopass
# chmod 640 /etc/pki/ovirt-engine/keys/apache.key.nopass
```

8. Скопируйте сертификат в необходимое местоположение:

```
# cp /tmp/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

9. Перезапустите веб-сервер Apache:

```
# systemctl restart httpd.service
```

10. Создайте новый файл конфигурации `/etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf` для хранилища доверенных сертификатов со следующими параметрами:

```
ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

11. Скопируйте файл `/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf`, переименуйте этот файл с применением для индекса номера больше 10 (например, `99-setup.conf`) и добавьте в новый переименованный файл следующие параметры:

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/certs/apache.cer
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```

12. Перезапустите службу `ovirt-websocket-proxy`:

```
# systemctl restart ovirt-websocket-proxy.service
```

13. Если файл `/etc/ovirt-provider-ovn/conf.d/10-setup-ovirt-provider-ovn.conf` был отредактирован вручную убедитесь, что в виртуализированном ЦУ в качестве источника сертификата по-прежнему используется `/etc/pki/ovirt-engine/apache-ca.pem`.

14. Для включения в `engine-backup` возможности обновления при восстановлении создайте новый файл `/etc/ovirt-engine-backup/engine-backup-config.d/update-system-wide-pki.sh` со следующими строками:

```
BACKUP_PATHS="${BACKUP_PATHS}
```

```
        /etc/ovirt-engine-backup"
        cp -f /etc/pki/ovirt-engine/apache-ca.pem
        /etc/pki/ca-trust/source/anchors/3rd-party-ca-cert.pem
        update-ca-trust
```

15. Перезапустите службу `ovirt-provider-ovn`:

```
# systemctl restart ovirt-provider-ovn.service
```

16. Перезапустите службу `ovirt-engine`:

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

17. Отключите глобальный режим обслуживания:

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

В результате при подключении пользователей к Порталу администрирования и Порталу ВМ не будет появляться предупреждение о подлинности сертификата, используемого для шифрования трафика HTTPS.

D.2. Настройка шифрованного соединения между виртуализированным ЦУ и сервером LDAP

Для настройки шифрованного соединения между виртуализированным ЦУ и сервером LDAP получите корневой сертификат ЦС сервера LDAP, скопируйте этот сертификат на машину виртуализированного ЦУ и создайте сертификат ЦС в кодировке PEM.

Тип файла ключа может быть любым типом, поддерживаемым Java. В приведенной ниже процедуре используется файл ключа с расширением `*.jks` в формате Java KeyStore.

Примечание — дополнительные сведения о создании сертификатов ЦС в кодировке PEM, а также об импортировании сертификатов можно посмотреть в разделе `X.509 CERTIFICATE TRUST STORE` файла `README` в каталоге `/usr/share/doc/ovirt-engine-extension-aaa-ldap-`*`версия`*.

Создание сертификата ЦС в кодировке PEM

1. На машине виртуализированного ЦУ скопируйте корневой сертификат ЦС сервера LDAP в каталог `/tmp` и импортируйте корневой сертификат с применением команды `keytool` для создания сертификата ЦС в кодировке PEM:

```
$ keytool -importcert -noprompt -trustcacerts -alias myrootca \
-file /tmp/myrootca.pem -keystore /etc/ovirt-engine/aaa/myrootca.jks \
-storepass password
```

Приведенная команда импортирует корневой сертификат ЦС в файл */tmp/myrootca.pem* и создаёт сертификат ЦС в кодировке PEM *myrootca.jks* в каталоге */etc/ovirt-engine/aaa/*.

2. Обновите информацию о сертификате в файле `/etc/ovirt-engine/aaa/profile1.properties` с использованием startTLS (рекомендуемый способ) или SSL:

- С использованием **startTLS**:

```
# Create keystore, import certificate chain and uncomment
pool.default.ssl.startTLS = true
pool.default.ssl.truststore.file = ${local:_basedir}/myrootca.jks
pool.default.ssl.truststore.password = password
```

- С использованием **SSL**:

```
# Create keystore, import certificate chain and uncomment
pool.default.serverset.single.port = 636
pool.default.ssl.enable = true
pool.default.ssl.truststore.file = ${local:_basedir}/myrootca.jks
pool.default.ssl.truststore.password = password
```

Примечание — `${local:_basedir}` является каталогом, в котором расположен файл конфигурации LDAP `property`, который указывает на каталог `/etc/ovirt-engine/aaa`. Если сертификат ЦС в кодировке PEM был создан в другом каталоге, замените `${local:_basedir}` на полный путь до сертификата.

D.3. Настройка шифрования соединений VDSM вручную

Шифрование соединений VDSM с виртуализированным ЦУ и с другими экземплярами VDSM можно настроить вручную.

Ручная настройка требуется только для хостов в кластерах с уровнем кластера 3.6, 4.0 и 4.1. Стойкое шифрование на хостах в кластерах с уровнем 4.2 настраивается автоматически во время переустановок хостов. При наличии кластеров 3.6, 4.0 или 4.1 с хостами виртуализации версии 4.2 используйте стойкое шифрование.

Настройка шифрования соединений VDSM вручную

1. Нажмите **Ресурсы → Хосты** и выберите хост.
2. Нажмите **Управление → Обслуживание**, чтобы открыть окно подтверждения Хосты на обслуживании.
3. Нажмите **OK**, чтобы запустить режим обслуживания.
4. Создайте на хосте файл `/etc/vdsm/vdsm.conf.d/99-custom-ciphers.conf` со следующим параметром:

```
[vars]
ssl_ciphers = HIGH
```

5. Перезапустите службу VDSM:

```
# systemctl restart vdsm
```

6. Нажмите **Ресурсы → Хосты** и выберите хост.
7. Нажмите **Управление → Активировать**, чтобы повторно активировать хост.

Приложение Е. Прокси

Е.1. Прокси-сервер SPICE

Е.1.1. Обзор SPICE Proxy

SPICE Proxy — это утилита, используемая для подключения клиентов SPICE к ВМ, когда клиенты SPICE находятся вне сети, соединяющей гипервизоры. Настройка SPICE Proxy состоит из установки на машине прокси-сервера `Squid` и настройки межсетевого экрана для разрешения трафика прокси. Процесс включения SPICE Proxy состоит из запуска на виртуализированном ЦУ утилиты `engine-config` для настройки значения ключа `SpiceProxyDefault`, состоящего из имени и порта прокси. Процесс выключения SPICE Proxy состоит из запуска на виртуализированном ЦУ утилиты `engine-config` для удаления ранее настроенного значения ключа `SpiceProxyDefault`.

Примечание — утилиту SPICE Proxy можно использовать только в сочетании с одиночным клиентом SPICE и нельзя использовать для подключения к ВМ, использующим noVNC.

Е.1.2. Настройка машины SPICE Proxy

В следующей последовательности действий описывается как настроить машину в качестве SPICE Proxy. SPICE Proxy делает возможным подключение извне к сети системы виртуализации ROSA Virtualization. Для предоставления служб прокси используется `Squid`.

Установка прокси-сервера `Squid`

1. Установите `Squid` на машине прокси, выполнив команду:

```
# yum install squid
```

2. В конфигурационном файле `/etc/squid/squid.conf` в строке `http_access deny CONNECT` замените значение `!SSL_ports` на значение `!Safe_ports`.

3. Запустите службу `squid` и включите автоматический запуск этой службы в процессе загрузки системы:

```
# systemctl enable squid.service --now
```

4. Разрешите исходящие запросы на службу `squid` в зоне по умолчанию межсетевого экрана `firewalld`:

```
# firewall-cmd --permanent --add-service=squid
```

5. Для применения изменений в конфигурации перезапустите службу межсетевого экрана `firewalld`:

```
# firewall-cmd --reload
```

В результате данная машина будет настроена для протокола SPICE в качестве прокси.

Активируйте (включите) прокси перед тем, как подключаться извне к сетям системы виртуализации ROSA Virtualization.

E.1.3. Включение SPICE Proxy

В следующей последовательности действий описывается как активировать (включить) прокси для протокола SPICE.

Активация SPICE Proxy

1. На машине виртуализированного ЦУ выполните следующую команду с применением утилиты `engine-config` для настройки прокси:

```
# engine-config -s SpiceProxyDefault=someProxy
```

2. Перезапустите службу `ovirt-engine`:

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

В результате SPICE Proxy будет активирован (включён), предоставляя возможность подключения извне к сетям системы виртуализации ROSA Virtualization через прокси-сервер для протокола SPICE.

Запись прокси должна быть в формате:

```
protocol://[host]:[port].
```

Примечание — поддержка прокси HTTPS доступна только для клиентов SPICE, поставляемых в составе системы виртуализации ROSA Virtualization. Клиенты в более ранних версиях ОС поддерживают только HTTP. Если указать HTTPS для клиентов более ранних версий, клиент проигнорирует настройку прокси и будет пробовать прямое подключение к хосту.

E.1.4. Выключение SPICE Proxy

В следующей последовательности действий описывается как выключить (деактивировать) прокси для протокола SPICE.

Выключение SPICE Proxy

1. На машине виртуализированного ЦУ выполните следующую команду для очистки прокси SPICE:

```
# engine-config -s SpiceProxyDefault=""
```

2. Перезапустите службу `ovirt-engine`:

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

В результате SPICE Proxy будет деактивирован (выключен) и подключение извне к сетям системы виртуализации ROSA Virtualization через прокси-сервер для протокола SPICE станет невозможным.

E.2. Прокси-сервер Squid

E.2.1. Установка и настройка Squid

В данном подразделе объясняется как установить и настроить прокси-сервер Squid для Портала ВМ.

Прокси-сервер Squid используется в качестве ускорителя передачи данных за счет кэширования часто просматриваемого содержимого, что повышает пропускную способность и снижает время откликов.

Настройка прокси-сервера Squid

1. Получите в установленном порядке закрытый ключ и сертификат ключа для порта HTTPS прокси-сервера Squid в виде файлов `proxy.key` и `proxy.cer` соответственно.

2. Установите Squid на машине прокси:

```
# yum install squid
```

3. Переместите полученные файлы `proxy.key` и `proxy.cer` с закрытым ключом и сертификатом ключа в каталог машины прокси (например, `/etc/squid`).

4. Установите права на чтение файлов `proxy.key` и `proxy.cer` для пользователя `squid`:

```
# chgrp squid /etc/squid/proxy.*
# chmod 640 /etc/squid/proxy.*
```

5. Squid должен верифицировать сертификат ЦС, используемый виртуализированным ЦУ. Для этого скопируйте с виртуализированного ЦУ сертификат ЦС `/etc/pki/ovirt-engine/ca.pem` на машину прокси в каталог `/etc/squid`, и установите права на чтение файла сертификата `ca.pem` для пользователя `squid`:

```
# chgrp squid /etc/squid/ca.pem
```

```
# chmod 640 /etc/squid/ca.pem
```

6. Для принудительного режима SELinux измените контекст порта 443, тем самым разрешив Squid использовать порт 443:

```
# yum install policycoreutils-python
# semanage port -m -p tcp -t http_cache_port_t 443
```

7. Замените текущий файл конфигурации Squid `/etc/squid/squid.conf` следующим содержимым:

```
https_port 443 key=/etc/squid/proxy.key cert=/etc/squid/proxy.cer ssl-bump
defaultsite=engine.example.com
cache_peer engine.example.com parent 443 0 no-query originserver ssl
sslcafile=/etc/squid/ca.pem name=engine login=PASSTHRU
cache_peer_access engine allow all
ssl_bump allow all
http_access allow all
```

8. Перезапустите службу прокси-сервера Squid:

```
# systemctl restart squid.service
```

Примечание — для увеличения интервала времени простоя Squid перед разрывом соединения (по умолчанию 15 минут простоя) настройте параметр `read_timeout` в файле конфигурации Squid `/etc/squid/squid.conf` (например, следующее значение `read_timeout 10 hours` увеличивает интервал времени простоя до 10 часов).

E.3. Прокси-сервер WebSocket

E.3.1. Обзор прокси-сервера WebSocket

Прокси-сервер WebSocket даёт возможность пользователям подключаться к ВМ с помощью консоли noVNC. Клиент noVNC использует веб-сокеты для передачи данных VNC, но сервер VNC в QEMU не поддерживает технологию веб-сокетов, поэтому между клиентом и сервером VNC необходимо расположить прокси WebSocket. При этом прокси WebSocket может выполняться на любой машине, имеющей доступ к сети, включая машину виртуализированного ЦУ.

Примечание — прокси-сервер WebSocket и консоль noVNC являются экспериментальными технологиями. Экспериментальные возможности не поддерживаются соглашениями об уровне обслуживания, могут иметь неполную функциональность и не рекомендуются к использованию на производстве, но предоставляют ранний доступ к будущим возможностям продукта, давая клиентам средство протестировать функциональность и предоставить отзывы, полезные для разработчиков.

Прокси-сервер WebSocket можно установить и настроить на машине виртуализированного ЦУ во время начального создания конфигурации ЦУ или на отдельной машине. Также можно провести миграцию WebSocket с машины виртуализированного ЦУ на отдельную машину.

E.3.2. Миграция WebSocket на отдельную машину

По соображениям безопасности или производительности прокси-сервер WebSocket может выполняться на отдельной машине. Действия по переносу WebSocket с машины виртуализированного ЦУ на отдельную машину включают в себя удаление конфигурации WebSocket с машины виртуализированного ЦУ, а затем установку прокси на отдельной машине.

Удаление WebSocket с машины виртуализированного ЦУ

1. Для удаления конфигурации прокси-сервера WebSocket запустите утилиту `engine-cleanup` на машине виртуализированного ЦУ:

```
# engine-cleanup
```

2. При запросе на удаление всех компонентов введите `No`:

```
   Do you want to remove all components? (Yes, No) [Yes]: No
```

3. При запросе на удаление виртуализированного ЦУ (`engine`) введите `No`:

```
   Do you want to remove the engine? (Yes, No) [Yes]: No
```

4. При запросе на удаление прокси-сервера WebSocket введите `Yes`:

```
   Do you want to remove the WebSocket proxy? (Yes, No) [No]: Yes
```

5. При запросах на удаление любых других компонентов введите `No`.

Установка WebSocket на отдельной машине

1. Установите прокси-сервер WebSocket:

```
# yum install ovirt-engine-websocket-proxy
```

2. Запустите утилиту `engine-setup` для настройки конфигурации прокси-сервера WebSocket:

```
# engine-setup
```

Примечание — если в системе ранее был установлен пакет `rhvm`, то при выводе запроса о необходимости настройки виртуализированного ЦУ на этом хосте введите `No`.

3. При выводе следующего запроса нажмите клавишу `Enter` для запуска процесса настройки конфигурации прокси-сервера WebSocket на данной машине:

```
Configure WebSocket Proxy on this machine? (Yes, No) [Yes]:
```

4. При выводе следующего запроса нажмите клавишу `Enter`, чтобы принять автоматически определённое имя хоста, или введите альтернативное имя хоста (обратите внимание, что при использовании виртуальных хостов автоматически определённое имя хоста может быть неправильным):

```
Host fully qualified DNS name of this server [host.example.com]:
```

5. При выводе следующего запроса нажмите клавишу `Enter`, чтобы утилита `engine-setup` автоматически настроила межсетевой экран и открыла порты, необходимые для внешних соединений (в противном случае, нужные порты необходимо будет открыть вручную):

```
Setup can automatically configure the firewall on this system.
Note: automatic configuration of the firewall may overwrite current settings.
Do you want Setup to configure the firewall? (Yes, No) [Yes]:
```

6. При выводе следующего запроса введите полное доменное имя (FQDN) машины виртуализированного ЦУ:

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

7. При выводе следующего запроса нажмите клавишу `Enter`, чтобы утилита `engine-setup` автоматически выполнила необходимые настройки на машине виртуализированного ЦУ, или введите цифру 2, чтобы выполнить эти настройки вручную:

```
Setup will need to do some actions on the remote engine server. Either
automatically, using ssh as root to access it, or you will be prompted to
manually perform each such action.
Please choose one of the following:
1 - Access remote engine server using ssh as root
2 - Perform each action manually, use files to copy content around
(1, 2) [1]:
```

Настройка вручную:

a. При выводе следующего запроса нажмите клавишу `Enter`, чтобы принять номер порта SSH по умолчанию, или укажите номер порта SSH машины виртуализированного ЦУ:

```
ssh port on remote engine server [22]:
```

b. Укажите пароль суперпользователя `root` для выполнения входа в систему на машине виртуализированного ЦУ:

```
root password on remote engine server engine_host.example.com:
```

8. При выводе следующего запроса введите `Yes` для просмотра правил `iptables` на предмет их отличия от текущих параметров:

```
Generated iptables rules are different from current ones.
Do you want to review them? (Yes, No) [No]:
```

9. При выводе ранее настроенных параметров нажмите клавишу `Enter`, чтобы подтвердить текущую конфигурацию:

```
--== CONFIGURATION PREVIEW ==--

Firewall manager                          : iptables
Update Firewall                           : True
Host FQDN                                 : host.example.com
Configure WebSocket Proxy                 : True
Engine Host FQDN                          : engine_host.example.com

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

Ознакомьтесь со следующими инструкциями для использования настроенного прокси-сервера WebSocket на машине виртуализированного ЦУ:

```
Manual actions are required on the engine host in order to enroll certs for this
host and configure the engine about it.

Please execute this command on the engine host:
   engine-config -s WebSocketProxy=host.example.com:6100
and than restart the engine service to make it effective
```

10. Осуществите вход в систему на машине виртуализированного ЦУ и выполните следующие команды для завершения настройки:

```
# engine-config -s WebSocketProxy=host.example.com:6100
# systemctl restart ovirt-engine.service
```

Приложение F. Системные учётные записи

F.1. Системные записи пользователей виртуализированного ЦУ

Во время установки пакета `rhevm` создаются следующие системные учётные записи пользователей с соответствующими идентификаторами (UID) для поддержки системы виртуализации ROSA Virtualization:

- Пользователь **`vdsm`** (UID `36`), предназначенный для поддержки работы инструментов монтирования и доступа к доменам хранения NFS.
- Пользователь **`ovirt`** (UID `108`).
- Пользователь **`ovirt-vmconsole`** (UID `498`), предназначенный для гостевой последовательной консоли.

F.2. Группы виртуализированного ЦУ

Во время установки пакета `rhevm` создаются следующие системные учётные записи групп пользователей с соответствующими идентификаторами (GID) для поддержки системы виртуализации ROSA Virtualization:

- Группа **`kvm`** (GID `36`). В группу входит пользователь `vdsm`.
- Группа **`ovirt`** (GID `108`). В группу входит пользователь `ovirt`.
- Группа **`ovirt-vmconsole`** (GID `498`). В группу входит пользователь `ovirt-vmconsole`.

F.3. Системные записи пользователей хостов виртуализации

Во время установки пакетов `vdsm` и `qemu-kvm-rhev` на хостах виртуализации создаются следующие системные учётные записи пользователей с соответствующими идентификаторами (UID):

- Пользователь **`vdsm`** (UID `36`).
- Пользователь **`qemu`** (UID `107`).
- Пользователь **`sanlock`** (UID `179`).
- Пользователь **`ovirt-vmconsole`** (UID `498`).

Примечание — назначенные идентификаторы пользователей (UID) и идентификаторы групп (GID) могут отличаться от системы к системе. Для пользователя **`vdsm`** зафиксировано значение UID `36`, а для группы **`kvm`** зафиксировано значение GID `36`. Если UID `36` или GID `36` уже используются другой учётной записью в системе, во время установки пакетов `vdsm` и `qemu-kvm-rhev` возникнет конфликт.

F.4. Группы хостов виртуализации

Во время установки пакетов `vdsm` и `qemu-kvm-rhev` на хостах виртуализации создаются следующие системные учётные записи групп пользователей с соответствующими идентификаторами (GID):

- Группа **`kvm`** (GID `36`). В группу входят пользователи `qemu` и `sanlock`.
- Группа **`qemu`** (GID `107`). В группу входят пользователи `vdsm` и `sanlock`.

- Группа **ovirt-vmconsole** (GID 498). В группу входит пользователь ovirt-vmconsole.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ВМ	—	виртуальная машина
ВЦОД	—	виртуальный центр обработки данных
ОЗУ	—	оперативное запоминающее устройство
ОС	—	операционная система
ПО	—	программное обеспечение
СУСВ	—	система управления средой виртуализации
ФС	—	файловая система
ФСТЭК	—	федеральная служба по техническому и экспортному контролю
ЦОД	—	центр обработки данных
ЦП	—	центральный процессор
ЦС	—	центр сертификации (удостоверяющий центр)
ЦУ	—	центр управления
API (Application Programming Interface)	—	программный интерфейс приложения
ARP (Address Resolution Protocol)	—	протокол разрешения адресов
BIOS (Basic Input/Output System)	—	базовая система ввода-вывода
CA (Certification Authority)	—	центр сертификации (удостоверяющий центр)
CD (Compact Disc)	—	компакт-диск
CHAP (Challenge Handshake Authentication Protocol)	—	протокол аутентификации с косвенным согласованием
CIDR (Classless Inter-Domain Routing)	—	бесклассовая IP-адресация
CIFS (Common Internet File System)	—	единая файловая система сети интернет
CRL (Certificate Revocation List)	—	Список отозванных сертификатов
DHCP (Dynamic Host Configuration Protocol)	—	протокол динамической настройки хоста
DNS (Domain Name System)	—	система доменных имён
DVD (Digital Versatile Disc)	—	цифровой многоцелевой диск
FC (Fibre Channel)	—	оптоволоконный канал
FCoE (Fibre Channel over Ethernet)	—	протокол FC, работающий поверх Ethernet
FCP (Fibre Channel Protocol)	—	транспортный протокол FC
FIPS (Federal Information Processing Standards)	—	федеральные стандарты обработки информации
FQDN (Fully Qualified Domain Name)	—	полное доменное имя хоста
GID (Group Identifier)	—	идентификатор группы
GPU (Graphics Processing Unit)	—	графический ускоритель (процессор)
GRUB (Grand Unified Bootloader)	—	унифицированный загрузчик ОС

HTML (HyperText Markup Language)	—	язык гипертекстовой разметки
HTTP (HyperText Transfer Protocol)	—	протокол передачи гипертекста
HTTPS (HyperText Transfer Protocol Secure)	—	безопасная версия протокола HTTP
ID (Identification Data)	—	идентификатор
IDE (Integrated Drive Electronics)	—	параллельный интерфейс подключения накопителей к компьютеру
IOMMU (Input/Output Memory Management Unit)	—	блок управления памятью для операций ввода-вывода
IP (Internet Protocol)	—	межсетевой протокол
IPA (Identity, Policy and Audit)	—	система идентификации и аутентификации пользователей, задания политик доступа и аудита
iSCSI (Internet Small Computer System Interface)	—	версия протокола SCSI, базирующаяся на TCP/IP
ISO (International Organization for Standardization)	—	международная организация, занимающаяся выпуском стандартов
IT (Information Technology)	—	информационные технологии
JSON (JavaScript Object Notation)	—	текстовый формат обмена данными, основанный на JavaScript
KSM (Kernel Shared Memory)	—	объединение одинаковых страниц памяти ядром ОС
LAN (Local Area Network)	—	локальная вычислительная сеть
LDAP (Lightweight Directory Access Protocol)	—	протокол доступа к каталогам
LKM *(Loadable Kernel Module)*	—	загружаемый модуль ядра ОС
LLDP *(Link Layer Discovery Protocol)*	—	канальный протокол (протокол обнаружения уровня связи)
LUN *(*Logical Unit Number*)*	—	номер логического устройства
LVM *(*Logical Volume Management*)*	—	менеджер логических томов
MAC (Media Access Control)	—	уникальный идентификатор сетевого оборудования
MoM (Memory Overcommit Manager)	—	диспетчер превышенного выделения памяти
MTU (Maximum Transmission Unit)	—	максимальная единица передачи данных
NAT (Network Address Translation)	—	преобразование сетевых адресов
NFS (Network File Sharing)	—	сетевая файловая система
NIC (Network Interface Controller)	—	сетевой адаптер
NUMA (Non-Uniform Memory Access)	—	неравномерный доступ к памяти
OCSP (Online Certificate Status Protocol)	—	протокол проверки статуса сертификата
OOM (Out of Memory)	—	уничтожитель перерасхода памяти

OVF (Open Virtualization Format)	—	формат образа виртуальной машины
OVN (Open Virtual Network)	—	виртуальная сеть с поддержкой OVS
OVS (Open vSwitch)	—	виртуальный коммутатор
PAM (Pluggable Authentication Modules)	—	подключаемые модули аутентификации
PCI (Peripheral Component Interconnect)	—	межсетевое соединение периферийных компонентов
PEM (Privacy-Enhanced Mail)	—	формат файлов для сертификатов
PF (Physical Function)	—	физическая функция PCI Express (PCIe) в SR-IOV
PIN (Personal Identification Number)	—	персональный идентификационный номер (код)
PKCS (Public Key Cryptography Standards)	—	стандарты (спецификации, протоколы) криптографии с открытым ключом
POSIX (Portable Operating System Interface)	—	переносимый интерфейс операционных систем
QCOW (QEMU Copy on Write)	—	формат образа виртуального диска
QEMU (Quick Emulator)	—	эмулятор аппаратного обеспечения различных платформ
QoS (Quality of Service)	—	качество обслуживания
RAC (Remote Access Card)	—	карта удалённого доступа
RDMA (Remote Direct Memory Access)	—	удалённый прямой доступ к памяти
RPC (Remote Procedure Call)	—	вызов удаленных процедур
SAN (Storage Area Network)	—	сеть хранения данных
SCSI (Small Computer System Interface)	—	системный интерфейс
SELinux (Security Enhanced Linux)	—	система контроля доступа, реализованная на уровне ядра ОС
SMT (Symmetric Multiprocessing)	—	синхронная многопоточность (гиперпоточность)
SPICE (Simple Protocol for Independent Computing Environments)	—	протокол удалённого доступа (простой протокол для независимых вычислительных сред)
SPM (Storage Pool Manager)	—	диспетчер пула хранилища
SR-IOV (Single Root Input/Output Virtualization)	—	виртуализация ввода-вывода с единым корнем
SSH (Secure Shell)	—	защищённая оболочка
SSL (Secure Sockets Layer)	—	уровень защищённых сокетов
STP (Spanning Tree Protocol)	—	канальный протокол (протокол связующего дерева)
TCP (Transmission Control Protocol)	—	протокол управления передачей данных
TLS (Transport Layer Security)	—	протокол безопасности транспортного уровня
TLV (Tag (Type) Length Value)	—	метод записи данных в файлах и протоколах
TSC (Time Stamp Counter)	—	счётчик метки времени
UCS (Unified Computing	—	система унифицированных вычислений

System)		компании Cisco
UEFI (Unified Extensible Firmware Interface)	—	объединённый интерфейс расширяемой прошивки
UI (User Interface)	—	пользовательский интерфейс
UID (User Identifier)	—	идентификатор пользователя
URL (Uniform Resource Locator)	—	сетевой адрес ресурса
USB (Universal Serial Bus)	—	универсальная последовательная шина
UUID (Universally Unique Identifier)	—	уникальный идентификатор элемента
VDSM (Virtual Desktop and Server Manager)	—	служба для управления виртуальными и физическими хостами, хранилищами хостов, ресурсами памяти и ресурсами сетей
VF (Virtual Function)	—	виртуальная функция PCI Express (PCIe) в SR-IOV
VFS (Virtual File System)	—	виртуальная файловая система
VGPU (Virtual Graphics Processing Unit)	—	виртуальный графический ускоритель (процессор)
VLAN (Virtual Local Area Network)	—	виртуальная локальная вычислительная сеть
VNC (Virtual Network Computing)	—	система (протокол) удалённого доступа в виртуальных сетях
VNIC (Virtual Network Interface Controller)	—	виртуальный сетевой адаптер
XML (eXtensible Markup Language)	—	расширяемый язык разметки
XOR (eXclusive OR)	—	исключающее «ИЛИ» (логическая операция)

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводит. докум. и дата	Подп.	Дата
Изм.	измененных	замененных	новых	аннулированных					