Программный комплекс (ПК) «Иридиум»

Руководство администратора

RU.КНРШ.00009-01 90 01

Листов: 491

Москва 2023

Аннотация

Настоящее руководство является основным документом, описывающим порядок действий администратора при работе с комплексом программ «Иридиум». В руководстве приведены сведения, необходимые администратору для установки изделия в вычислительную технику на базе персональных электронных вычислительных машин (ПЭВМ), а также для настройки и эксплуатации изделия.

Содержание

Термины и определения

Термин	Определение
Watchdog	Сторожевые таймеры, основная задача которых - своевременный перезапуск «зависшего» оборудования с целью восстановления его работоспособности
Виртуализация	Группа технологий, основанных на преобразовании формата или параметров программных или сетевых запросов к компьютерным ресурсам. Технологии обеспечивают независимость процессов обработки информации от программной или аппаратной платформы информационной системы[1]
Виртуализация аппаратного обеспечения	Создание программных систем на основе существующих аппаратно-программных комплексов, зависящих или независящих от них
Виртуальная инфраструктура	Композиция иерархически взаимосвязанных групп виртуальных устройств обработки, хранения и/или передачи данных, а также группы необходимых для их работы аппаратных и/или программных средств
Виртуальная машина (ВМ)	Виртуальная вычислительная система, которая состоит из виртуальных устройств обработки, хранения и передачи данных и которая дополнительно может содержать ПО и пользовательские данные. На ВМ, как и на реальные, можно ставить операционные системы, причем на одном вычислительном узле может функционировать несколько ВМ
Виртуальная сеть	Группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов
Виртуальный диск (том)	Логическое устройство, с которым ВМ взаимодействует как с диском
Гипервизор	Программа, создающая среду функционирования других программ (в том числе других гипервизоров)

[1] ГОСТ Р 56938-2016 Защита информации. Защита информации при использовании технологий виртуализации. Общие положения

	за счет имитации аппаратных средств вычислительной техники, управления данными средствами и гостевыми операционными системами, функционирующими в данной среде
Гипервизор 1 (первого) типа	Гипервизор, устанавливаемый непосредственно на аппаратное обеспечение в качестве системного программного обеспечения
Гостевая операционная система	Операционная система, установленная в виртуальной машине
Кластер	Два или более вычислительных узла, соединенные в единую систему специальным программным и аппаратным обеспечением
Клонирование диска	Создание точной копии диска
Миграция	Перенос виртуальной машины/виртуального диска с одного вычислительного узла/хранилища на другой
Непостоянный (неперсистентный) образ диска	Тип виртуального диска, при подключении которого в ВМ создается копия исходного образа диска. После прекращения работы ВМ все изменения, сделанные на непостоянном диске, будут потеряны. Копия диска удаляется вместе с удалением ВМ
Образ виртуальной машины	Файл, содержащий информацию о конфигурации, настройках и состоянии виртуальной машины, а также хранящиеся в ней программы и данные
Плейбук	Сценарий, с помощью которого на удаленные серверы отправляются наборы команд
Постоянный (персистентный) образ диска	Тип виртуального диска, все изменения на котором сохраняются после прекращения работы с ним виртуальной машины
Пул хранения данных	Логическая группа физических дисков
Режим высокой доступности ВМ	Возможность автоматического перезапуска ВМ в случае сбоев
Сервер виртуализации (хост)	Аппаратная платформа с установленными программными компонентами серверной виртуализации
Система хранения данных	Комплексное программно-аппаратное решение по организации надёжного хранения информационных
	ресурсов и предоставления гарантированного доступа к ним

Снимок работающей ВМ	Контрольная точка состояния операционной системы виртуальной машины на уровне файловой системы, обеспечивающей возврат в произвольный момент вернуться к состоянию на момент создания контрольной точки
Средство защиты информации	Совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации
Суперпользователь	Пользователь, обладающий всеми правами
Технология высокой доступности (High Available)	Тип кластера, при использовании которого обеспечивается перезапуск виртуальных машин на резервном узле. Используется в случае выхода из строя основного. Обязательным условием для реализации данной технологии является наличие общего разделяемого хранилища на резервном и основном вычислительных узлах. Образ ВМ должен располагаться на этом хранилище и быть доступен на обоих узлах.
Хостинговая зона	Логическое объединение серверов виртуализации в группы по функциональному или иному признаку
Хостовая система	Система, предоставляющая аппаратные ресурсы и программное обеспечение
Шаблон виртуальной машины	Набор настроек, с которыми будут создаваться виртуальные машины

1 Введение

1.1 Область применения

Согласно приказам № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных», № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» ФСТЭК России (сертификат № 3723 от 21.03.2017 г.), изделие может использоваться в государственных информационных системах (ГИС) до 1 класса защищенности включительно, для обеспечения защищенности персональных данных в информационных системах персональных данных (ИСПДн) до 1 уровня включительно, автоматизированных системах управления технологическими процессами (АСУ ТП) до 1 класса защищенности включительно, значимых объектах критической информационной инфраструктуры (КИИ) до 1 категории включительно. Программное обеспечение «Терминал-Сервер» находится в едином реестре российских программ для электронных вычислительных машин и баз данных №2338 от 15.12.2016.

1.2 Краткое описание возможностей

ПК «Иридиум» предоставляет пользователям следующие возможности:

− поддержка графического установщика;

− установка непосредственно на аппаратное обеспечение без использования хостовой операционной системы (гипервизор 1 типа);

− создание и управление виртуальной средой на группе серверов (кластере);

− объединение физических серверов в кластер до 64 узлов, обеспечивающих постоянную доступность виртуальной машины с числом виртуальных процессоров не менее 4, даже в случае отказа физического сервера;

− обеспечение возможности использования в качестве гостевой ОС операционных систем семейств Linux, Windows;

− поддержка функции Multipathing;

− функционирование средств защиты информации:

− виртуальных систем обнаружения вторжения;

− межсетевых экранов;

− антивирусных средств;

− средств анализа защищенности;

− средств защиты информации от DDoS атак;

− средств корреляции событий безопасности;

− средств контроля утечки информации из информационной систем;

- наличие сертифицированной и несертифицированной версии изделия;
- создание виртуальных машин (ВМ), их образов и шаблонов с поддержкой 32 и 64-битных гостевых операционных систем;
- возможность управления конфигурацией ВМ с помощью графического и консольного интерфейсов;
- возможность создания ВМ из настраиваемых шаблонов с помощью графического и консольного интерфейсов;
- возможность группового создания ВМ из шаблонов;
- поддержка в ВМ до 240 виртуальных процессоров;
- включает в состав, программное обеспечение для управления виртуальными рабочими местами (VDI);
- поддержка различных сценариев виртуализации рабочих мест — с одним или несколькими брокерами (с балансировкой), внутри одного кластера или с выделенным кластером VDI;
- возможность изменения количества выделенных процессоров и размера оперативной памяти виртуальным машинам без завершения их функционирования;

- возможность подключения к ВМ устройств из состава аппаратных средств, на которых функционирует серверная часть изделия, включая устройства USB 3.0;
- возможность интеграции с внешними системами управления и мониторинга для сбора статистики производительности и контроля состояния (поддержка протоколов: SNMP, SSH, CLI, CIM, API и т.д.);
- возможность добавления виртуальных дисков в гостевую операционную систему и увеличение их размеров без остановки ВМ;
- поддержка открытого стандарта Open Virtualization Format (OVF);
- возможность подключения внешних хранилищ по протоколу FC;
- возможность клонирования ВМ;
- возможность создания кластеров высокой доступности, выполняющих перезапуск ВМ в случае выхода из строя узла кластера;
- возможность переноса ВМ между узлами кластера без прерывания трафика;
- обеспечение автоматического распределения сервером виртуализации ресурсов между работающими ВМ;
- миграция дисков работающих ВМ между хранилищами без их остановки;
- сервисный режим обслуживания узла с автоматическим перемещением работающих ВМ без их остановки;
- возможность централизованного управления кластерами, серверной частью изделия на всех узлах кластера высокой доступности, хранилищами и виртуальными коммутаторами;
- возможность мониторинга работоспособности и использования ресурсов ВМ;
- поддержка виртуальных коммутаторов с технологией VLAN (Virtual Local Area Network);
- подключение к ВМ по протоколу SPICE USB-устройств из состава аппаратных средств, на которых функционирует клиентская часть изделия;

- возможность ограничения для сетевого и дискового ввода-вывода ВМ на основе их групповых или индивидуальных настроек;
- поддержка механизмов оптимизации оперативной памяти:
- дедупликация страниц;
- динамическое распределение;
- выгрузка в файл подкачки, область подкачки, сформированную на постоянном накопителе, либо оперативной памяти;
- Memory Balooning;
- возможность создания динамически расширяющегося виртуального дискового пространства ВМ с обеспечением возможности выделения соответствующих аппаратных средств (физических дисков, блоков физических дисков) по мере заполнения виртуального дискового пространства ВМ;
- клиентское приложение с графическим интерфейсом для подключения к ВМ;
- поддержка работы с контейнерами;
- возможность работы с хранилищем LVM, а также использование технологии тонких томов LVM Thin Provision;
- поддержка создания программно-определяемой СХД;
- возможность параллельного доступа нескольких ВМ к одному виртуальному диску;
- возможность централизованного обновления с использованием штатных средств;
- возможность резервирования интерфейсов управления инфраструктурой виртуализации;
- возможность размещения контроллера на хосте (без использования дополнительного физического сервера);
- возможность создания снэпшотов ВМ;
- миграция ВМ из сред виртуализации, в том числе VMware;

- создание шаблона на базе существующей ВМ.
- поддержка Affinity Rule – размещение выбранных ВМ на одном хосте виртуализации и Anti-Affinity Rule – размещение выбранных ВМ на разных хостах виртуализации;
- обеспечение идентификации и аутентификации субъектов доступа (пользователей и администраторов) до предоставления доступа к функциям виртуализации и управления в том числе в режиме взаимодействия со средствами создания единого пространства пользователей;
- функционирование в условиях мандатного и/или дискреционного разграничения доступа при межпроцессном и сетевом взаимодействии, включая взаимодействие между ВМ по протоколам стека IPv4 в условиях мандатного разграничения доступа и доступ субъектов к файлам-образам и экземплярам функционирующих ВМ;
- запуск ВМ в виде отдельного процесса, функционирующего от имени учетной записи субъекта доступа (пользователя) с унаследованием его мандатных атрибутов;
- защита файлов-образов ВМ от модификации в процессе функционирования ВМ;
- регистрация событий с использованием средств централизованного протоколирования;
- регулярное обновление для нейтрализации угроз эксплуатации уязвимостей;
- управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;
- разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.
- интерфейс на русском языке с возможностью переключения на иностранный язык.

- наличие встроенного функционала резервного копирования, а также возможность интеграции с программным обеспечением для резервного копирования, выполняющим как агентное, так и безагентное резервное копирование и восстановление как самих ВМ, так и их шаблонов, образов и дисков в различных форматах (включая qcow2), на различных типах томов (включая lvm, ceph и S3-хранилища).

1.3 Структура ПК «Иридиум»

ПК «Иридиум» состоит из следующих основных компонентов:

Таблица 1.1

Обозначение изделия	Наименование изделия	Количество	Порядковый учетный номер	Примечание
RU.КНРШ.00009-01	1 Программный комплекс “Иридиум” в составе:			Примечание 5
МБРЦ.468313.001	1.1 Программно-аппаратный комплекс (ПАК) “Горизонт-ВС”			Примечание 6
RU.КНРШ.00007-01	1.2 Система хранения данных “Шторм”			
RU.КНРШ.00006-01	1.3 Программное обеспечение подсистемы VDI			Примечание 7
RU.КНРШ.000012-01	1.4 Программный комплекс «Система управления компонентами виртуализации»			
61649217.401200.003	1.5 Многофункциональный комплекс сетевой защиты «Diamond VPN/FW» (редакция для ПК «Иридиум»)			Примечание 8

Примечания

1 Количество и набор составных частей определяется по решению Заказчика спецификацией поставки.

2 Количество определяется спецификацией поставки.

3 Составные части ПК “Иридиум” поставляются на одном USB-носителе.

4 Программный комплекс “Иридиум” зарегистрирован в Реестре российского программного обеспечения (запись в реестре от 01.03.2023 №16819).

5 Права на ПАК «Горизонт-ВС» принадлежат ООО «Инновационный Центр «Баррикады», поставка лицензий осуществляется правообладателем. Комплекс программ “Терминал-Сервер” из состава ПАК “Горизонт-ВС” зарегистрирован в Реестре программ для ЭВМ (свидетельство о государственной регистрации № 2016618025 от 19.07.2016). Сертификат соответствия требованиям безопасности информации № 3723 выдан ФСТЭК России 21.03.2017, действителен до 21.03.2025.

6 Права на Систему хранения данных «Шторм» принадлежат АО «НПЦ «МАКС», поставка лицензий осуществляется правообладателем. Система хранения данных "Шторм" зарегистрирована в Реестре российского программного обеспечения (запись в реестре от 13.02.2023 №16626).

7 Права на Программное обеспечение подсистемы VDI принадлежат АО «НПЦ «МАКС» поставка лицензий осуществляется правообладателем.

8 Права на Многофункциональный комплекс сетевой защиты «Diamond VPN/FW» принадлежат ООО «ТСС», поставка лицензий осуществляется правообладателем. Сертификат ФСТЭК России № 4066 действителен до 24.01.2024, на соответствие требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ(Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ), Профиль защиты МЭ(В четвертого класса защиты. ИТ.МЭ.В4.ПЗ), Требования к СОВ, Профили защиты СОВ (сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ).

В изделии реализована возможность как локальной работы (на *сервере виртуализации*), так и на группе серверных платформ (*кластере*). Управление группой серверов виртуализации осуществляется при помощи системы группового управления (СГУ). Узлы под управлением СГУ разделяются на:

- серверы виртуализации, на которых выполняются ВМ;
- автоматизированные рабочие места (АРМ) управления виртуализацией (АРМ УВ), на которых выполняется СГУ.

Пример схемы стенда с установленными модулями Программный комплекс (ПК) «Иридиум» показан на рисунке ниже (Рисунок 1).

Для доступа к СГУ на стенде должно быть подключено АРМ Управления, представляющее собой ПЭВМ с установленной ОС (согласно требованиям п. 2.2.9), в среде которой функционирует браузер.

Локальная работа описана в разделе 3.1, работа в кластере с СГУ – в разделе 8 настоящего руководства.

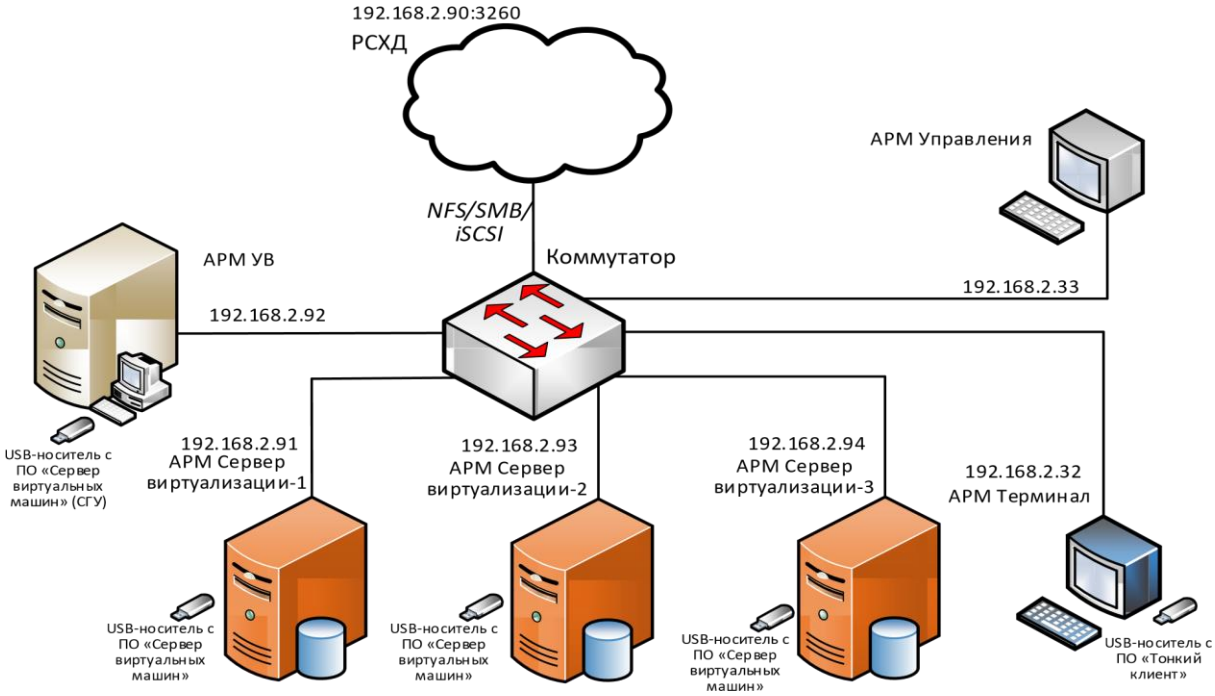


Рисунок 1 – Пример схемы стенда

1.4 Уровень подготовки персонала

Администраторы СГУ «Иридиум» должны иметь опыт работы с:

- персональным компьютером на уровне квалифицированного пользователя;
- стандартными приложениями на уровне свободного выполнения базовых операций;
- операционными системами:
  - Windows;
  - Unix-подобными ОС.

1.5 Перечень эксплуатационной документации, с которой необходимо ознакомиться администратору

Администратору «Иридиум» необходимо ознакомиться со следующими документами:

- Руководство пользователя. МБРЦ.468313.001.ИЗ.02.

- Руководство администратора. Часть 1. Описание и работа модуля идентификации и контроля доверенной среды (МИиКДС) «Шина». МБРЦ.468313.001.ИЗ.02-01;
- Руководство администратора. Часть 2. Описание и работа комплекса программ «Терминал-сервер». МБРЦ.468313.001.ИЗ.02-02.

2 Назначение и условия применения

2.1 Назначение изделия

Изделие предназначено для использования в клиент-серверных системах.

2.2 Условия применения изделия

ПК «Иридиум» поставляется на USB-носителе для установки на ПЭВМ, выполняющие функции *терминала*, *сервера виртуализации*. После получения необходимо сверить контрольные суммы носителей с указанными в формуляре МБРЦ.468313.001ФО.

После установки и настройки изделия должна быть исключена возможность бесконтрольного доступа к техническим средствам изделия, размещенным внутри системного блока ПЭВМ.

В изделии поддерживаются следующие роли безопасности: пользователи и администраторы средства доверенной загрузки (СДЗ).

Технические средства ПЭВМ, в которую устанавливается изделие, не должны содержать аппаратно-программных механизмов, ориентированных на целенаправленное нарушение правильности его функционирования.

Журнал регистрации событий, имеющих отношение к безопасности, должен иметь в своих записях точное указание даты и времени.

Администратор СДЗ должен раз в неделю производить резервное копирование виртуальных машин с помощью встроенной системы резервного копирования (п. 3.3).

В Программный комплекс (ПК) «Иридиум» реализованы:

- изолированная программная среда, в которой установлен проверенный КП «Терминал-Сервер», под управлением которого ведется работа;
- неизменность КП для определенного сеанса работы.

С целью предотвращения нарушения целостности замкнутой среды системы «Иридиум» на действия суперпользователя *root* накладываются ограничения. Администратор СДЗ с правами суперпользователя может выполнять следующие действия: 1) вносить изменения в конфигурационные файлы, расположенные в

директориях:

- /etc/auditd/;
- /etc/libvirt/

2) просматривать все файлы системы с использованием всех доступных системных утилит и средств фильтрации;

3) создавать учетные записи пользователей с использованием системной утилиты *useradd*. 4) изменять пароли пользователей и администраторов с использованием системной утилиты *passwd*. 5) использовать любые системные утилиты без внесения изменений в системные файлы и файлы конфигураций.

Внимание*! Действия, связанные с изменением конфигурационных файлов, не указанных в п.1, и запуском отключенных по умолчанию сервисов, запрещены.*

Технические характеристики Программный комплекс (ПК) «Иридиум»

Программный комплекс (ПК) «Иридиум» поддерживает работу в соответствии с показателями, приведенными в таблицах ниже (1 и Таблица 2).

Таблица 1 – Характеристики Программный комплекс (ПК) «Иридиум»

Характеристика	Показатель
Количество процессоров сервера виртуализации, поддерживаемых гипервизором	от 2 до 4096
Объем оперативной памяти сервера виртуализации, поддерживаемый гипервизором	от 4 Гб до 256 Тб
Объем жесткого диска сервера виртуализации	не менее 100 Гб
Количество процессорных сокетов	не менее 2
Суммарное количество физических ядер сервера виртуализации	не менее 4 до 2048
Количество виртуальных ЦПУ, поддерживаемых одной ВМ	от 2 до 256
Количество памяти, поддерживаемой ВМ	от 1 Гб до 32 Тб
Поддержка виртуальных накопителей в ВМ объёмом (максимальное значение ограничено аппаратными возможностями сервера виртуализации)	от 4 Гб
Количество виртуальных процессоров, поддерживаемых ВМ	от 2 до 2048
Возможность организации виртуальных сетевых интерфейсов со скоростями	до 10 Гбит/с
Возможность объединения физических серверов в кластер высокой доступности, с автоматическим перезапуском виртуальных машин в случае отказа физического сервера	до 200 узлов
Возможность создания в одной зоне Федерации или локации кластера высокой доступности из группы серверов	не менее чем 300 хостов суммарно
Основные поддерживаемые ОС семейства Windows	Windows Server 2016; Windows Server 2012 R2; Windows Server 2012; Windows Server 2008 R2 with Service Pack 1; Windows XP/7/10

Основные поддерживаемые ОС семейства Linux	AltLinux 8; AstraLinux 2.12; AstraLinux 1.5; AstraLinux 1.6; CentOS 8.x; CentOS 7.x; CentOS 6.x; Debian 10.x; Debian 9.x; Debian 8.x; Debian 7.x; Ubuntu 17.10; Ubuntu 16.04 LTS; Ubuntu 14.04 LTS; openSUSE 42.x; SLES 11; SLES 12; SLES 15; Oracle Linux 8.x; Oracle Linux 7.x; Oracle Linux 6.x; Oracle Linux 5.x; Oracle Enterprise Linux 4.x; Red Hat Enterprise Linux (RHEL), Oracle DB
Совместимое серверное оборудование	Hewlett Packard Enterprise, Huawei, Lenovo, Cisco, DellEMC, Fujitsu, IBM, Depo Computers, Аквариус, Булат, ТПлатформы.
Объем поддержки томов	Более 2 Тб
Поддержка ПО SAP	SAP, SAP ASE, SAP MaxDB
Поддержка систем управления реляционным базам данных	MS SQL, IBM DB2, PostgreSQL

Таблица 2 − Свойства, поддерживаемые в одной виртуальной среде

Поддерживаемое свойство	Минимальный показатель
Виртуальные центральные процессоры устройств (далее – ЦПУ)	64
Оперативная память	512 ГБ
Объем дисков в виртуальных машинах и контейнерах	16 ТБ

Процедура установки описана в Инструкции по установке

3 Описание операций

3.1 Настройки сервера виртуализации

В данном подразделе содержится описание настроек сервера виртуализации, выполняемых в командной строке и программе «Менеджер виртуальных машин».

3.1.1 Вход в систему

После загрузки Программный комплекс (ПК) «Иридиум» на экране появится окно аутентификации (Рисунок 2).

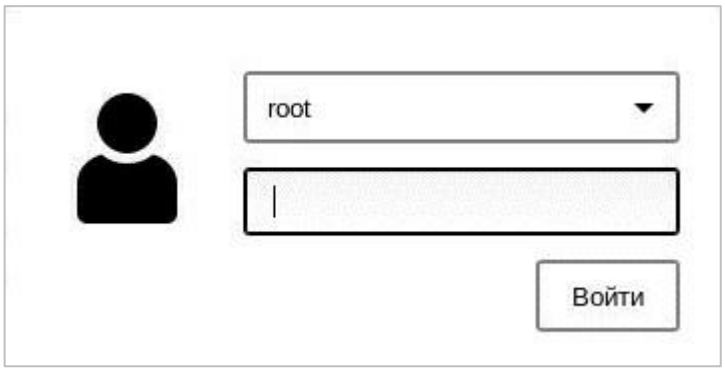


Рисунок 2 – Окно аутентификации

***Примечание**: по умолчанию для пользователя **root** установлен пароль **horizon**. Следует сменить пароль при первом запуске системы.* **Для входа в систему:**

1. Ввести имя администратора СДЗ и пароль.
2. Нажать клавишу **Enter** или кнопку **Войти**.

Загрузится рабочий стол ПК.

Пароль при вводе отображается в скрытом виде для защиты обратной связи при вводе аутентификационной информации.

3.1.2 Запуск сервера виртуализации

3.1.3 Первоначальные настройки сервера виртуализации

Работа Программный комплекс (ПК) «Иридиум» может осуществляться как в режимах:

- одиночного гипервизора;
- группы серверов виртуализации.

Порядок работы с группой гипервизоров при помощи системы группового управления описан в п. 3.2.

Для одиночного сервера виртуализации после установки Программный комплекс (ПК) «Иридиум» необходимо произвести следующие настройки от имени суперпользователя (пользователя, обладающего всеми правами) *root*:

1. При первом запуске обязательно сменить пароль суперпользователя root командой в консоли:

```
passwd <имя_пользователя>
```

2. Дважды корректно ввести новый пароль.

1. Перезапустить сервер виртуализации.

3.1.3.1 Развертывание хоста на сервере

После выполнения пункта по установке Программный комплекс (ПК) «Иридиум» (пункт **Ошибка! Источник ссылки не найден.**), следует в ыполнить данные действия:

1. Открыть доступ к серверу по **ssh,** отредактировав конфиг **/etc/ssh/sshd_config**. Изменить параметр **PermitBootLogin** на **yes** (предварительно следует раскоментировать его). Далее изменить параметр **PasswordAuthentication** на **yes.** Далее следует перезапустить службу **ssh** командой:

```
rc-service sshd restrart
```

2. Создать **bond** (описано в пункте **Ошибка! Источник ссылки не найден.**).

3. Далее следует создать на сервере виртуализации папку **/data/0/datastores** и назначить права **oneadmin**.
4. Прописать все хосты в **/etc/hosts**.
5. Далее следует загрузить СГУ на всех хостах (например, с помощью команды **scp**). Затем распаковать контейнер с помощью команды:

```
 docker load <
/mnt/hcs/....
```

Далее подписать **hvs_sign.**

6. В зависимости от типа хранилища, требуется та или настройка. Если подключена технология подключения узла сети хранения данных с использованием нескольких маршрутов (**multipathing**), то нужно заполнить конфиг **etc/multipath.conf:**

```
defaults {
        find_multipaths yes         user_friendly_names yes
}

blacklist {
}
```

Выполнить команды:

```
rc-service multipath start rc-service
multipathd start rc-update add
multipath default rc-update add
multipathd default
```

7. При использовании **Multipath -ll** найти диск (их название может быть, например, dm-1 и dm-2). Далее определяем **uuid** диск (путь, где его можно посмотреть по команде **|/dev/disk/by-id/**) и прописываем его в файле **/lvm/lvm.conf:**

```
global_filter = [ "a|/dev/disk/by-id/[uuid диск1]|",
"a|/dev/disk/by-id/[uuid диск2]|",  "r|.*|" ] use_lvmetad =
0 use_lvmlockd = 0 locking_type = 1
```

после выполнить команды:

```
rc-update del wdmd rc-
update del sanlock rc-
update del lvmlockd rc-
update del lvmetad
 rc-service wdmd stop rc-
service sanlock stop rc-
service lvmlockd stop
```

А также:

```
vgcreate -n VG0 |/dev/disk/by-id/[uuid диск1] vgcreate
-n VG1 |/dev/disk/by-id/[uuid диск2]
```

***Примечание**: имя VG0 и VG1 являются изменяемыми.*

8. Запустить на одном хосте:

```
docker run -d --name=hcs \
--network=host \
--restart=always \
--security-opt=seccomp:unconfined \
-v /var/tmp:/var/tmp \
-v hvol:/hvol \ --stop-timeout=90 \ hcs:latest
```

Дальнейшая настройка и подключение хоста производится в СГУ в данных пунктах руководства: 3.2.7 (создание и управление узлами (серверами виртуализации)), 3.2.14 (создание и управление хранилищами), 3.2.14 (создание и настройка виртуальных сетей).

3.1.4 Настройка сети

3.1.4.1 Настройка сетевых интерфейсов

Первоначальные настройки сетевых интерфейсов производятся на этапе установки системы (см. п. **Ошибка! Источник ссылки не найден.**).

Названия имен сетевых интерфейсов могут различаться, поэтому далее для примера будет рассмотрено имя **eth0**.

Для настройки сетевой карты необходимо создать символьную ссылки с net.lo на net.eth0 (или что-либо другое, в зависимости от названия сетевого интерфейса) в ***/etc/init.d*** следующими командами:

```
# cd /etc/init.d
# ln -s net.lo net.eth0
```

Конфигурация всех сетевых интерфейсов находится в файле ***/etc/conf.d/net***.

Пример настройки для использования DHCP или статических адресов:

```
# Для DHCP config_eth0=«dhcp»

# Статический IP-адрес, используется запись CIDR
config_eth0=«192.168.0.7/24»
routes_eth0=«default via 192.168.0.1»
dns_servers_eth0=«192.168.0.1 8.8.8.8»
# Статический IP-адрес, запись с маской подсети
config_eth0=«192.168.0.7 netmask 255.255.255.0»
routes_eth0=«default via 192.168.0.1»
dns_servers_eth0=«192.168.0.1 8.8.8.8»
```

Примечания:

1. *Если конфигурация для интерфейса не указывается, предполагается использование DHCP.*
2. *CIDR расшифровывается как Classless InterDomain Routing (бесклассовая междоменная маршрутизация). CIDR – это схема адресации, позволяющая одному IP-адресу обозначать множество*

IPадресов. IP-адрес CIDR выглядит как обычный IP-адрес с добавлением косой черты и числа; например, 192.168.0.0/16. CIDR описывается в RFC 1519.

Для запуска и остановки интерфейса выполнить команды:

```
# /etc/init.d/net.eth0 start
# /etc/init.d/net.eth0 stop
```

Для настройки запуска сетевого интерфейса при загрузке Программный комплекс (ПК) «Иридиум» выполнить команду:

```
# rc-update add net.eth0 default
```

Для установки MTU сетевого интерфейса выполнить команду:

```
set int eth0 mtu_request=1450
```

Для удаления конфигурации MTU и восстановления значения по умолчанию выполнить команду:

```
$ ovs-vsctl set int eth0 mtu_request=[]
```

3.1.4.2 Поддержка Jumbo Frames

Процесс настройки Jumbo Frames сводится к изменению настройки **MTU** на каждом устройстве до 9000 байт вместо 1500 байт по умолчанию командой **ovs-vsctl set Interface NAME mtu_request=9000** (на каждом хосте).

3.1.4.3 Поддержка группирования сетевых интерфейсов

Программный комплекс (ПК) «Иридиум»поддерживает группирование сетевых интерфейсов – teaming.

Для объединения сетевых интерфейсов в бонды выполнить команду**:**

```
ovs-vsctl add-bond nameOVS nameBOND eno1 eno2
```

3.1.4.4 Объединение физических сетевых интерфейсов в бонд

Рассмотрим создание бонда физических сетевых интерфейсов (Link Aggregation Group (LAG) группу) на примере объединения интерфейсов eth0 и eth1.

Для объединения сетевых интерфейсов в бонд:

1. Удалить порт eth0 из виртуального коммутатора командой:

```
# ovs-vsctl del-port hvssw0 eth0
```

2. Создать бонд из двух физических интерфейсов eth0, eth1 и добавить его в коммутатор Open vSwitch командой:

```
# ovs-vsctl add-bond hvssw0 bond0 eth0 eth1
```

3. Убедиться, что бонд был успешно создан, для чего набрать команду:

```
# ovs-vsctl show
```

Будет получен ответ следующего вида (Рисунок 3).

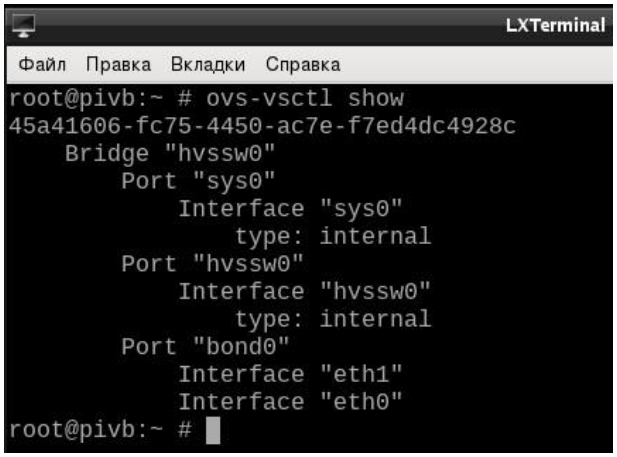


Рисунок 3 – Подтверждение создания бонда

3.1.5 Настройка мониторинга виртуальной среды

Для мониторинга виртуальной среды в изделии используются следующие средства:

– протокол SNMP (Simple Network Management Protocol — простой протокол сетевого управления), см. п. 3.1.5.1; – Zabbix, см. п. 3.1.5.2.

3.1.5.1 Настройка протокола SNMP

При использовании SNMP, один или более административных компьютеров (где функционируют программные средства, называемые менеджерами) выполняет отслеживание или управление группой хостов/устройств в компьютерной сети.

На каждой управляемой системе функционирует *агент* – постоянно запущенная программа, которая через SNMP передаёт информацию менеджеру.

На сервере виртуализации в директории ***/usr/share/snmp/mibs*** хранятся MIB-файлы, описывающие структуру управляемых данных на подсистеме устройства (Рисунок 4).

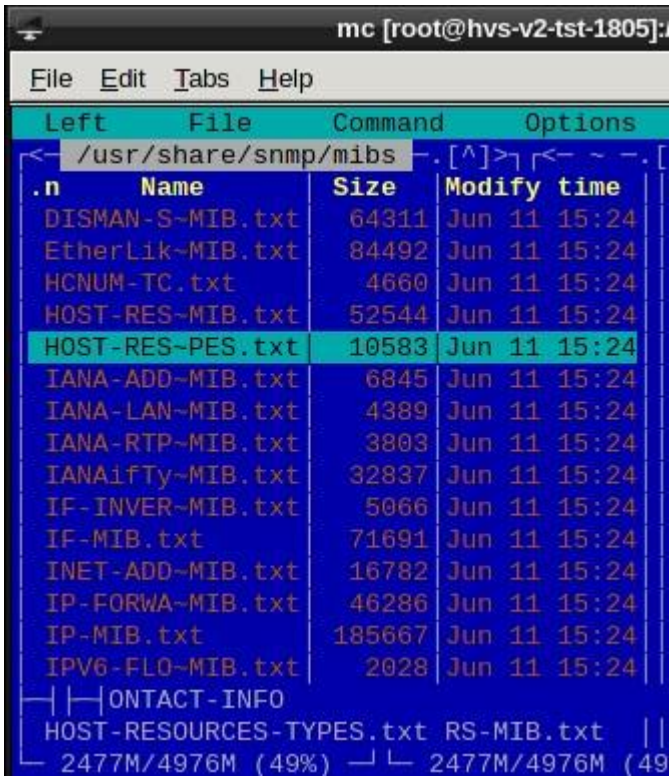


Рисунок 4 – MIB-файлы

3.1.5.2 Настройка Zabbix

Для запуска Zabbix агента и подключения к Zabbix серверу:

1. Отредактировать строки 112 и 153 конфигурационного файла /etc/zabbix/zabbix_agentd.conf:

```
server=ip-zabbixServer ServerActive=ip-zabbixServer
```

2. Запустить сервис zabbix-agentd:

```
rc-service zabbix-agentd start
```

3. Добавить сервис zabbix-agentd в автозагрузку:

```
rc-update add zabbix-agentd default
```

4. Зайти на сервер Zabbix и подключить узел с Программный комплекс (ПК) «Иридиум» согласно документации на сайте https://www.zabbix.com/manuals.

3.1.5.3 Настройка Sysklogd

Syslogd — журнал системных сообщений, утилита, которая считывает и регистрирует сообщения в консоле системы, файлы журналов, другие компьютеры и / или пользователей, как указано в ее файле конфигурации.

Syslogd поддерживает сообщения журнала в стиле RFC5424 и RFC3164 как для локального, так и для удаленного ведения журнала с использованием интернет-сокетов и доменных сокетов UNIX.

3.1.5.3.1 Установка Sysklogd

Следует воспользоваться USE-флагом **app-admin/sysklogd:**

- **Logger** — Создание программы-регистратора:
- **Logrotate** — использовать **app-admin/logrotate** для ротации журналов.

5. **Установка индексирования файлов**

Для индексации файлов следует использовать команду:

```
root #emerge --ask app-admin/sysklogd
```

***Примечание**: не рекомендуется запускать более одного системного регистратора на физическом хосте.*

6. **Установка файлов конфигурации**

- **/etc/conf.d/syslogd** — конфигурационный файл Gentoo для демона /etc/init.d/sysklogd. Для получения дополнительных опций требуется обратиться через **man syslogd.**

- **/etc/syslog.conf** — глобальный (общесистемный) конфигурационный файл. Для получения дополнительной информации следует обратиться через **syslog.conf.**

- **//etc/rsyslog.d/*.conf** — обычный подкаталог файлов .conf, считываемых syslogd.

- **/etc/syslog.d/10-remote-logging.conf** — обычное имя файла для дополнительных правил настройки.

7. **Установка OpenRC**

Для того чтобы добавить систему инициализации OpenRC, следует добавить демон системного журнала на уровень выполнения по умолчанию, чтобы ведение журнала начиналось при загрузке системы:

```
root #rc-update add sysklogd default
```

затем запустить **sysklogd** командой:

```
root #rc-service sysklogd start
```

после этого следует проверить файл **/var/log/messages** на наличие текущих записей системного журнала:

```
root #tail -f /var/log/messages
Mar  6 11:33:59 node syslogd[14000]: syslogd v2.3.0: restart.
```

```
runit
system
```

8. **Установка локального ведения журнала** Параметры запуска демона по умолчанию:

- **-m 0** — отключить интервал между отмеченными сообщениями;
- **-s** — работают в безопасном режиме, не регистрируют сообщения с удаленных компьютеров. Если указано дважды, сокет вообще не будет открыт, что также отключает поддержку ведения журнала на удаленных машинах.

В файле **/etc/conf.d/syslogd:**

```
# Config file for /etc/init.d/sysklogd

SYSLOGD="-m 0 -s -s"
```

В конфигурационном файле **syslog.conf** по умолчанию /etc/syslog.conf:

```
auth,authpriv.*                  /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
 kern.*                          -
/var/log/kern.log mail.*
-/var/log/mail.log

mail.err                         /var/log/mail.err

*.=info;*.=notice;*.=warn;\
auth,authpriv.none;\          cron,daemon.none;\
        mail,news.none           -/var/log/messages
*.=emerg                         *
 include
/etc/syslog.d/*.conf
```

На этом установка завершена, и все будет работать для локального ведения журнала событий.

3.1.5.3.2 Настройка удаленного ведения журнала

Настройка удаленного ведения журнала необязательна. В конфигурации по умолчанию демон **sysklogd** не будет отправлять или получать какие-либо сообщения системного журнала по IP. Файл конфигурации **/etc/conf.d/syslogd** необходимо настроить для сервера и клиента.

Настройки для сервера:

Чтобы сервер системного журнала мог прослушивать входящие сообщения системного журнала, следует отредактировать **/etc/conf.d/sysklogd** следующим образом:

```
# Config file for /etc/init.d/sysklogd

SYSLOGD="-m 0 -b 192.0.2.1:514
```

IP-адрес 192.0.2.1 — это интерфейс локального сервера, к которому sysklogd будет привязывать службу.

Перезапустите демон syslogd:

```
root #rc-service sysklogd restart
```

Следует проверить, запущена ли служба и привязана ли она к правильному интерфейсу, выполнив:

```
root #ss -tulpn | grep syslog udp   UNCONN 0      0
192.0.2.1:514      0.0.0.0:*
users:(("syslogd",pid=20175,fd=6))
```

Настройки клиента:

Чтобы разрешить клиенту системного журнала отправлять сообщения системного журнала, следует отредактировать /**etc/conf.d/sysklogd** следующим образом:

```
# Config file for /etc/init.d/sysklogd

SYSLOGD="-m 0"
```

Дополнительные файлы конфигурации клиента должны храниться в каталоге **/etc/rsyslog.d**/. Файлы, использующие суффикс ***.conf**, становятся активными после перезапуска демона syslogd. Следует создать файл **/etc/syslog.d/10-remote-logging.conf:**

```
*.*          @192.0.2.1                    ;RFC5424
```

Этот пример правила перенаправляет все сообщения на сервер системного журнала 2001:db8::1, используя форматирование системного журнала RFC 3164. Далее нужно создать файл **/etc/syslog.d/11-remote-ipv6logging.conf:**

```
*.*          @2001:db8::1                  ;RFC3164
```

Примечание: *Параметр системного журнала, формат ведения журнала RFC, который должен использоваться для отправки сообщений, задается с помощью* ***;RFC5424*** *или* ***;RFC3164.***

Затем требуется перезапустить демон **syslogd** на клиенте:

```
root #rc-server sysklogd restart
```

3.1.6 Настройка службы NTP

NTP (Network Time Protocol — протокол сетевого времени) — сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью.

Плейбук предназначен для настройки NTP. Поддерживается как обычная настройка с одним сервером времени, так и более сложные и многоуровневые варианты с перекрёстным опросом группы узлов, для соблюдения единого времени в случае отказа внешних источников.

Плейбук установлен в каталог ***/root/hvs-ansible*** и имеет следующую структуру:

```
group_vars/     ntp.yaml
roles/     hvs_ntp/
defaults/
main.yaml          files/
validate_conf.sh
tasks/              main.yaml
templates/
ntp.conf.j2 ansible.cfg
hosts.yaml ntp.yaml
```

Каталог *roles* содержит hvs_ntp, описывающую логику настройки NTP на отдельном узле.

Файл ***ntp.yaml***, является текстом плейбука и его точкой входа.

Файл ***ansible.cfg*** содержит конфигурационную информацию для решения ansible.

Следующие составные части являются структурами управляющими поведением, и подлежат кастомизации:

- каталог ***group_vars*** − должен содержать файлы с переменными плейбука, определяющими его поведение. Изначально содержит пример настройки.

- файл ***hosts.yaml*** – перечисление узлов организованных в группы (inventory файл).

Плейбук работает с узлами, внесёнными в группу с именем *ntp*.

Для каждого узла применяется роль *hvs_ntp*. Параметры роли могут быть указаны сразу для всех узлов, входящих в группу *ntp* или любым другим способом по-разному в разных подгруппах, индивидуально для некоторых узлов.

Пример содержимого ***group_vars/ntp.yaml*** из примера:

```
hvs_ntp_enabled: true

#hvs_ntp_upstreams: []
#hvs_ntp_pools: []
 hvs_ntp_peers:   -
192.168.213.208
- 192.168.213.209
- 192.168.213.210
```

- *hvs_ntp_enabled* отвечают за включение/выключение службы NTP на узле.
- параметры *hvs_ntp_upstreams, hvs_ntp_pools* и *hvs_ntp_peers* являются списками и конфигурируют службу NTP в соответствующем ключе:
- *hvs_ntp_upstreams* – создаёт одностороннюю клиентскую связь с указанным сервером;
- *hvs_ntp_pools* – создаёт одностороннюю клиентскую связь с указанным сервером или reference clock;
- *hvs_ntp_peers* – создаёт симметричную одноранговую связь с удалённым узлом.

После внесения изменений следует сделать текущим каталог с плейбуком (**/root/hvs-ansible/group_vars**) и запустить плейбук следующей командой:

```
ansible-playbook ntp.yaml
```

3.1.7 Управление томами данных

Logical Volume Manager (LVM) – это система управления томами с данными. Она позволяет создавать поверх физических разделов (или даже неразбитых жестких дисков) логические тома, которые в самой системе будут видны как обычные блочные устройства с данными (т.е. как обычные разделы).

Основные преимущества LVM:

- одну группу логических томов можно создавать поверх любого количества физических разделов;
- размер логических томов можно легко менять прямо во время работы.
- LVM поддерживает механизм снапшотов (снимки данных), копирование разделов «на лету» и зеркалирование, подобное RAID-1.

На каждом из дисков/разделов должен быть создан физический том (physical volume). Например, для LVM используются разделы sdb2 и sdb3:

```
# pvcreate /dev/sdb2 /dev/sdb3
```

Важно! *Чтобы команда* ***pvcreate /dev/sdb2 /dev/sdb3*** *была исполнена, необходимо в файле конфигурации* ***/etc/lvm/lvm.conf*** *заменить r на a (параметр* ***global_filter****)*.

```
global_filter = [ "a |.* ]
```

Для создания группы томов на разделах дисков необходимо выполнить команду:

```
# vgcreate vg_0 /dev/sdb2 /dev/sdb3
```

Отобразится сообщение об успешном создании группы томов:

«Volume group «vg_0» successfully created».

Для создания логических LVM разделов:

1. Выполнить команду:

```
# lvcreate -l 20 -n logical_vol1 vg_0
```

Отобразится сообщение об успешном создании раздела:

```
Logical volume «logical_vol1» created
```

2. Просмотреть список доступных логических разделов LVM командой:

```
# lvdisplay
```

3.1.8 Настройка кластеров

В данном пункте описываются операции по настройке кластеров Shared LVM на базе Sanlock.

Операции по настройке кластера выполняются при помощи плейбука, предназначенного для следующих действий:

- введение узлов в кластер:
  - включение службы Watchdog;
  - конфигурация LVM для работы с разделяемым блочным устройством;
  - включение механизма замков;
- удаление узла;
- первичное создание группы томов – volume group (VG).

Вывод узла из LVM кластера приводит к исходному состоянию узла, за исключением работы Watchdog демона. Его отключение приведёт к перегрузке сервера. После плановой перезагрузки служба Watchdog будет отключена.

***Примечание**. Для корректной работы кластера перед настройкой сконфигурировать службу NTP с помощью соответствующего плейбука (см. п. 3.1.6).*

Плейбук содержится в каталоге ***/root/hvs-ansible*** и имеет следующую структуру:

```
group_vars/
shared_lvm.yaml
sslvm_0.yaml
library/
kmodule.py roles/
    sanlock_shared_lvm/
defaults/
main.yaml         tasks/
disable.yaml
enable.yaml
main.yaml         templates/
lvm.conf.j2
lvmlocal.conf.j2
watchdog/         tasks/
            main.yaml
README.md ansible.cfg
hosts.yaml
lvm_sanlock_shared.yaml
lvm.yaml
```

- каталог ***roles*** содержит роли watchdog и sanlock_shared_lvm, необходимые для работы плейбука;
- файлы ***lvm_sanlock_shared.yaml*** и ***lvm.yaml*** являются текстом плейбука и его точкой входа соответственно;
- файл ***ansible.cfg*** содержит конфигурационную информацию для ansible.

Следующие составные части являются структурами, управляющими поведением, и подлежат кастомизации:

- каталог *group_vars* – должен содержать файлы с переменными плейбука, определяющими поведение. Изначально содержит пример настройки.

файл ***hosts.yaml*** – inventory, перечисление узлов организованных в группы.

Плейбук работает с узлами, внесёнными в группу с именем **shared_lvm**, при этом каждый отдельный кластер должен быть выделен в самостоятельную группу.

Пример содержимого ***hosts.yaml***:

```
all:
children:
    shared_lvm:
children:
sslvm_0:
    sslvm_0:
hosts:
        h110:
          ansible_host: host_ip_or_name
user: root         h109:           user: root
```

В группу *shared_lvm* включена группа с именем *sslvm_0*. В свою очередь, группа *sslvm_0* содержит описание узлов, составляющих отдельный кластер с общим ресурсом.

Файл ***shared_lvm.yaml*** в каталоге group_vars содержит параметры, определяющие работу плейбука в части описания отдельных кластеров:

```
#
# example inventory vars
#
sanlock_shared_lvm_groups:
- sslvm_0
 ansible_python_interpreter:
/usr/bin/python3
```

Параметр *sanlock_shared_lvm_groups* содержит список групп, определяющих отдельные кластера. остальное должно оставаться неизменным.

Каждый файл в каталоге *group_vars* с именами формата **имя_группы.yaml** должен содержать описание отдельного кластера.

Например, файл **sslvm_0.yaml**, содержащий параметры для группы sslvm_0:

```
wd_enabled: true
wd_module: softdog
#wd_module_args:
lvm_shared_vgs:   -
name: store0     pvs:
      - /dev/disk/by-id/scsi-36001405c3647f7263584fce9017278b5
# - name: store2
#   pvs:
#     - /dev/vdd sslvm_enabled:
true
```

Назначение параметров:

- *wd_enabled, wd_module* и *wd_module_args* определяют конфигурацию ядерной части службы Watchdog. В примере указано, что модуль *softdog* должен быть загружен (без дополнительных параметров).
- *sslvm_enabled* в состоянии **true** указывает, что нужно ввести узлы в состав кластера.
- *lvm_shared_vgs* является перечислением разделяемых ресурсов, которыми являются группы томов LVM. Каждая группа представляется именем **name** и списком физических томов **pvs**.

  Имена томов должны совпадать на всех узлах кластера.

Для вывода отдельных узлов из состава кластера:

1. Создать каталог ***host_vars.***
2. Скопировать в созданный каталог файл с параметрами группы.
3. Переименовать файл в соответствии с именем узла в файл inventory (например, *sslvm_0.yaml → h110.yaml*).
4. Произвести изменения, отражающие отличия конкретно взятого узла.

Для вывода отдельных узлов из состава кластера в файле параметров узла:

1. Не меняя других параметров, изменить *wd_enabled u sslvm_enabled* на **false**.

После внесения изменений следует сделать текущим каталог с плейбуком (***/root/hvs-ansible***) и запустить плейбук следующей командой:

```
ansible-playbook lvm.yaml
```

3.1.9 Поддержка работы с кластерной файловой системой

3.1.9.1 Настройка гипервизоров

Для настройки гипервизоров:

1. Настроить гипервизоры на использование статических IPv4 адресов.
2. Привести файл /etc/conf.d/net к следующему виду:

```
config_eth0=«null»
rc_net_eth0_provide=«net»
 config_sys0=«ip адрес/ «битовая маска»
routes_sys0=«default via «сетевой шлюз»
rc_net_sys0_need=«ovs-vswitchd»
```

3. На всех гипервизорах, использующих gfs2, прописать соответствие имен и Ip-адресов в файле **/etc/hosts:**

```
192.168.2.144 node1
192.168.2.145 node2
```

3.1.9.2 Настройка кластерного программного обеспечения

Для настройки кластерного ПО:

1. На всех гипервизорах создать файл **/etc/corosync/corosync.conf** со следующим содержимым:

```
# Totem Protocol Configuration
totem {   version: 2
cluster_name: mycluster
secauth: off
  bindnetaddr: ip адрес гипервизора
transport: udpu
}

# Nodelist - Server List nodelist {
```

```
  node {
ring0_addr: node1
nodeid: 1
  }   node {
ring0_addr: node2
nodeid: 2
  }   node {
ring0_addr: node3
nodeid: 3
  }
}

# Quorum configuration quorum {
provider: corosync_votequorum
two_node: 0
}

# Corosync Log configuration logging {
to_logfile: yes   logfile:
/var/log/corosync/corosync.log
to_syslog: yes   debug: on   timestamp:
on
}
service {
}
```

2. На всех гипервизорах создать директорию для записи журналов:

```
mkdir -p /var/log/corosync/
```

3. Включить и добавить сервисы в автозагрузку на всех узлах:

```
rc-service corosync start rc-service
pacemaker start rc-update add
pacemaker default
```

4. Отключить и удалить из автозагрузки **iscsid** на всех узлах:

```
rc-service iscsid stop rc-update
del iscsid
```

Важно! *Отключение и удаление протокола* ***iscsid*** *необходимо произвести только в том случае, если диски содержат протокол* ***iscsid.*** *Если присутствуют диски с протоколом* ***Fibre Channel (FC)****, то отключение и удаление из автозагрузки не требуется.*

3.1.9.3 Форматирование и монтирование файловой системы

Для форматирования и монтирования GFS2:

1. Собрать кластер через **crmsh**. на одном из гипервизоров запуском следующие команды:

```
crm crm(live)# configure crm(live)configure# primitive
st-null stonith:null params hostlist=«node1 node2 node3»
```

2. Настроить тестовый фенсинг:

Примечание*. На аппаратной платформе разных вендоров настройки различаются.*

a. Выполнить команды:

```
crm(live)configure# clone fencing st-null crm(live)configure#
commit
```

a. Настроить **dlm lock** и его запуск на всех гипервизорах для возможности монтирования **gfs2**:

```
crm  crm(live)# configure crm(live)configure# primitive
dlm ocf:pacemaker:controld \
   >          op monitor interval=30s on-fail=fence \
>                params  allow_stonith_disabled=true
crm(live)configure# clone dlm_c dlm \    >        meta
interleave=true    ordered=true    targetrole=Started
crm(live)configure# commit
```

3. Подключить диски по **ISCSI** с использованием кластерного ПО.
4. Настроить этот запуск на всех гипервизорах.

Если хранилище будет настроено следующим образом, то:

5. Настроить подключение командами:

```
crm(live)configure#  primitive disk0 iscsi params
portal=192.168.2.108:3260 target=iqn.2020-
04.bkd.hpiscsi:dfd42696a8b5 crm(live)configure# clone
clonedisk0 disk0 meta interleave=true ordered=true
crm(live)configure# commit
```

Вывод команды **lsblk** должен показывать следующее:

```
lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT sda
8:0    0 97,7G  0 disk
```

6. Проверить наличие файловых систем на устройстве:

```
wipefs /dev/sda
DEVICE OFFSET  TYPE UUID                                 LABEL
sda         0x10000  gfs2  57ad91e0-a701-40ad-8b8f-1f6f50f88c6b
mycluster:web
```

7. При наличии файловых систем, очистить устройство:

```
sda    0x10000 gfs2 57ad91e0-a701-40ad-8b8f-1f6f50f88c6b
mycluster:web hor-gfs-4 ~ # wipefs -a /dev/sda
/dev/sda: 4 bytes were erased at offset 0x00010000 (gfs2): 01 16
19 70
```

8. Форматировать устройство в файловую систему **gfs2**:

   a. Выбрать протокол блокировок **lock_dlm**.

б. Завести журналы по количеству узлов (**-j3**).

в. Настроить имя в таблице блокировок, где **mycluster** — имя кластера:

```
mkfs.gfs2 -p lock_dlm -j 3  -t mycluster:0 /dev/sda
This will destroy any data on /dev/sda
Are you sure you want to proceed? [y/n] y
Discarding device contents (may take a while on large devices):
Done
Adding journals: Done
Building resource groups: Done
Creating quota file: Done
Writing superblock and syncing: Done
Device:                    /dev/sda
Block size:                4096
Device size:               97,66 GB (25600000 blocks)
Filesystem size:           97,66 GB (25599996 blocks)
Journals:                  3
Journal size:              128MB
Resource groups:           393
Locking protocol:          «lock_dlm»
Lock table:                «mycluster:0»
UUID:                      ce2eb2f0-e94b-40eb-
b9b60bb3b767f9be
```

г. Создать точки монтирования на всех гипервизорах:

```
mkdir -p /data/100
```

GFS2 должен монтироваться с помощью кластера.

9. Монтировать и настроить запуск монтирования на всех узлах:

```
crm
crm(live)# configure
crm(live)configure# primitive gfs0 Filesystem params
device=«/dev/sda» directory=«/data/100» fstype=gfs2
options=noatime op monitor depth=0 timeout=60 interval=10s
onfail=restart
crm(live)configure# clone clonegfs gfs0 meta interleave=true
target-role=Started crm(live)configure# commit
```

10. Настроить порядок выполнения действий при перезагрузке узлов:

```
crm
crm(live)# configure
```

```
crm(live)configure# order clonediskorder Mandatory: dlm_c
clonedisk0
crm(live)configure# order clonegfsorder Mandatory: dlm_c
clonedisk0 clonegfs crm(live)configure# commit
```

Если операции завершились успешно, то вывод команды **crm_resource** будет следующий:

```
 Clone Set: fencing [st-null]
     Started: [ node1 node2 node3 ]  Clone Set: dlm_c [dlm]
     Started: [ node1 node2 node3 ]
 Clone Set: clonedisk0 [disk0]
     Started: [ node1 node2 node3 ]  Clone Set: clonegfs [gfs0]
     Started: [ node1 node2 node3 ]
```

В выводе команды **df** будет видно, что все подключено.

3.1.9.4 Остановка и удаление ресурсов

Для остановки и удаления ресурсов выполнить команду:

```
hor-gfs-4 ~ #   crm resource stop gfs0 hor-gfs-4
~ # crm configure delete gfs0
```

Важно*! При удалении зависимых ресурсов вышестоящая настройка также будет изменяться.*

3.1.10 Кэш-логические тома

Программный комплекс (ПК) «Иридиум» обеспечивает полную поддержку логических томов кэша LVM.

Кэш-логический том использует небольшой логический том, состоящий из быстрых блочных устройств (например, накопителей SSD). Кэш-логический том повышает производительность более объемного и медленного логического тома путем хранения часто используемых блоков на более узком логическом томе меньшего размера.

Все эти связанные логические тома должны находиться в одной группе томов.

Кэш-память LVM использует следующие типы логических томов LVM:

6) ***Логический том исходный (origin)*** – большой, медленный логический том.

Для создания исходного тома выполнить команду:

```
# lvcreate -L 4G -n lv VG /dev/sde1
```

В данном примере создается исходный том с именем lv размера 4G и состоит из ***/dev/sde1*** медленного физического тома

2) ***Логический том пула кэша*** – небольшой, быстрый логический том, который состоит из двух устройств: логического тома данных кэша и логического тома метаданных кэша.

Для создания логического тома пула кэша необходимо создать группу томов, содержащую медленный физический том и быстрый физический том, выполнив команду:

```
# pvcreate /dev/sde1
# pvcreate /dev/sdf1
# vgcreate VG /dev/sde1 /dev/sdf1
```

В данном примере ***/dev/sde1*** является медленным устройством и ***/dev/sdf1*** является быстрым устройством, и оба устройства содержатся в группе томов VG.

3) ***Логический том данных кэша*** – логический том, содержащий блоки данных для логического тома пула кэша.

Для создания логического тома данных кэша выполнить команду:

```
# lvcreate -L 2G -n lv_cache VG /dev/sdf1
```

Созданный логический том будет содержать блоки данных из тома источника. Размер этого логического тома – это размер кэша и будет отображаться как размер логического тома пула кэша.

В данном примере создается объем данных кэша lv_cache. Кэш имеет размер 2G и содержится на быстром устройстве ***/dev/sdf1***, являющимся частью группы томов VG.

4) ***Логический том метаданных кэша*** – логический том, содержащий метаданные для логического тома пула кэша. Содержит учетную информацию, которая указывает, где хранятся блоки данных (например, на логическом томе источника или логическом томе данных кэша).

Для создания логического тома метаданных кэша выполнить команду:

```
# lvcreate -L 12M -n lv_cache_meta VG /dev/sdf1
```

В данном примере создается тома метаданных кэша ***lv_cache_meta***. Он имеет размер 12M и также содержится на быстром устройстве ***/dev/sdf1***, которое является частью группы томов VG.

Созданный логический том будет содержать метаданные пула кэша. Его объем должен быть примерно в 1000 раз меньше логического тома данных кэша с минимальным размером 8 Мбайт.

5) **Логический том кэша** – логический том, содержащий логический том источника и логический том пула кэша. Это результирующее пригодное для использования устройство, которое инкапсулирует различные компоненты тома кэш-памяти.

Для создания логического тома пула кэша выполнить команду:

```
# lvconvert --type cache-pool --cachemode writethrough -
poolmetadata VG/lv_cache_meta VG/lv_cache
```

```
  WARNING: Converting logical volume VG/lv_cache and
VG/lv_cache_meta to pool's data and metadata volumes.
  THIS WILL DESTROY CONTENT OF LOGICAL VOLUME (filesystem etc.)
  Converted VG/lv_cache to cache pool.
# lvs -a -o +devices
  LV                VG  Attr        LSize   Pool Origin Data%
Meta% Cpy%Sync Devices   lv              VG  -wi-a-----   4.00g
/dev/sde1(0)     lv_cache              VG   Cwi---C---     2.00g
lv_cache_cdata(0)
  [lv_cache_cdata] VG  Cwi-------   2.00g
/dev/sdf1(0)
  [lv_cache_cmeta] VG  ewi-------  12.00m
/dev/sdf1(512)
  [lvol0_pmspare]  VG  ewi-------  12.00m
       /dev/sde1(1024)
```

Создается логический том пула кэша. Данные кэша и логические тома метаданных кэша объединяются в логический том типа cache-pool. На этом шаге можно установить поведение пула кэша.

В данном примере аргумент **cachemode** установлен **writethrough**. Это указывает на то, что запись считается завершенной только тогда, когда она была сохранена как в логическом томе пула кэша, так и в логическом томе источника.

При выполнении этой команды, логический том данных кэша переименовывается с **_cdata** добавлением к исходному имени логического тома данных кэша, а логический том метаданных кэша переименовывается с **_cmeta** добавлением к исходному имени логического тома данных кэша; оба этих тома становятся скрытыми.

3.1.11 Настройка дедупликации

В Программный комплекс (ПК) «Иридиум» поддерживается ***Btrfs*** – новая файловая система с принципом копирования при записи (CoW), направленная на реализацию дополнительных функций, отказоустойчивость, восстановление и простоту администрирования.

Дедупликация времени записи будет записывать только одну копию дублированных данных на диск. Такое поведение может значительно сэкономить емкость хранилища.

Запуск дедупликации осуществляется командой:

```
# btrfs dedup enable /<точка_монтирования>
```

Также поддерживается дедупликация виртуальных дисков формата *.qcow2.

Для проверки данного функционала:

1. Создать виртуальный диск формата *.qcow2.
2. Подключить виртуальный диск к ВМ с установленной гостевой ОС типа Linux.
3. Произвести форматирование виртуального диска и установку файловой системы, например, ext4.
4. Создать заполненный нулями файл на диске при помощи команды:

```
# dd if=/dev/zero of=/<точка_монтирования> count=1024 bs=1M
```

5. Убедиться в наличии файла.
6. Выключить ВМ.
7. Определить размер *.qcow2 файла образа виртуального диска.
8. Выполнить команду:

```
# qemu-img convert -o qcow2 original_image.qcow2
deduplicate_image.qcow2
```

9. Включить ВМ с диском и убедиться в наличии файла, заполненного нулями.
10. Убедиться, что размер файла ***deduplicate_image.qcow2*** значительно меньше original_image.qcow2.

3.1.11.1 Создание и настройка кластера высокой доступности

3.1.11.1.1 Предварительные настройки

Выполнить предварительные настройки:

11. Создать общее внешнее хранилище или РСХД объемом не менее 15 ГБ.
12. Выполнить команды:

```
vgcreate VG0 /dev/sdX
lvcreate -L 2G -n hcs VG0
mkfs.xfs /dev/VG0/hcs
mkdir -p /data/hcs/hvol
```

где:

- sdX − имя устройства;
- VG0−имя новой LV группы

13. На каждом хосте развернуть docker-контейнер нужной версии:

```
docker load < $PATH_TO_IMAGES hvs_sign
```

14. Для создания необходимых директорий в папке ***/data/0/docker/volumes/hvol/_data,*** запустить контейнер на одном из хостов с помощью команд:

```
docker run -d --name=hcs \
--network=host \
--restart=always \
--security-opt=seccomp:unconfined \
-v /var/tmp:/var/tmp \
-v hvol:/hvol \ --stop-
timeout=90 \ hcs:latest
```

15. Проверить работу веб-интерфеса.
16. Остановить и удалить контейнер:

```
docker rm -f hcs
```

17. Перенести в директорию ***/data/hcs/hvol*** служебные папки dockerконтейнера из директории ***/data/0/docker/volumes/hvol/_data*** с сохранением прав на них:

```
cp -a /data/0/docker/volumes/hvol/_data/* /data/hcs/hvol
```

18. Папку ***/data/0/docker/volumes/hvol/_data*** перенести на директорию выше.

3.1.11.1.2 Настройка кластерного по

Для настройки кластерного ПО:

19. На всех гипервизорах создать конфигурационный файл ***/etc/corosync/corosync.conf /corosync.conf.***
20. На всех гипервизорах создать директорию для вывода записей журнала (логов):

```
mkdir -p /var/log/corosync/
```

21. Включить и добавить сервисы в автозагрузку на всех узлах:

```
rc-service corosync start rc-service
pacemaker start rc-update add
pacemaker default
```

22. Выложить в папку ***/usr/lib/python3.8/site-packages***/ два файла:

− /easy-install.pth;

− /parallax-1.0.6-py3.8.egg

23. Собрать кластер через **crmsh**.

Для создания кластера:

д. На одном из гипервизоров запустить **crm**.

е. Проверить серверы на доступность (настроить фенсинг):

```
crm crm(live)# configure crm(live)configure# primitive
st-null stonith:null params hostlist="node1 node2 node3"
crm(live)configure# clone fencing st-null
```

ж. Активировать том LVM:

```
crm(live)configure# primitive hcs_lvm LVM params
volgrpname=VG0 op monitor timeout=30 interval=10
```

з. Примонтировать файловую систему:

```
crm(live)configure# primitive fs_work Filesystem params
device="/dev/VG0/hcs" directory="/data/hcs" fstype=xfs op
monitor interval=10s
```

***Примечание**. На каждом хосте сервис docker должен быть запущен и добавлен в автозагрузку с помощью команд:*

```
rc-service docker start rc-update
add docker default
```

и. Запустить контейнер:

```
crm(live)configure# primitive docker_start docker params
image="hcs:latest" name=hcs run_opts="--network=host -
restart=always --security-opt=seccomp:unconfined -v
/var/tmp:/var/tmp -v /data/hcs/hvol:/hvol --stop-timeout=90"
meta target-role=Started
```

к. Назначить адрес на порт (порт создать заранее в ovs hvssw0):

```
crm(live)configure# primitive vip_sgu IPaddr2 params
ip=${FLOAT_IP} cidr_netmask=${FLOAT_NETMASK} nic={FLOAT_NIC}
op monitor interval=10 timeout=20
```

л. Запустить группы ресурсов:

```
crm(live)configure# group hcs hcs_lvm fs_work docker_start
vip_sgu
```

м. Завершить настройку:

```
crm(live)configure# commit
```

3.1.11.2 Использование кластера на базе Pacemaker

Pacemaker представляет собой полноценный менеджер ресурсов, который позволяет управлять любыми сервисами в распределённой кластерной системе. Pacemaker рекомендуется использовать совместно с программным обеспечением Corosync.

Pacemaker состоит из универсального набора утилит для управления распределением ресурсов кластера. Его основными свойствами являются:

- обнаружение и восстановление сбоев на уровне узлов и сервисов;
- независимость от подсистемы хранения: общий диск не требуется;
- независимость от типов ресурсов: все что может быть заскриптовано, может быть кластеризовано;
- поддержка STONITH (Shoot-The-Other-Node-In-The-Head)
- поддержка кластеров любого размера;
- поддержка практически любой избыточной конфигурации;
- автоматическая репликация конфигураций на все узлы кластера;
- возможность задания порядка запуска ресурсов, а также их совместимости на одном узле;
- поддержка расширенных типов ресурсов: клонов (запущен на множестве узлов) и с дополнительными состояниями (master/slave и т.п.);
- единый кластерный шелл (crm), унифицированный и управляемый скриптами.

3.1.11.2.1 Настройка распределённого реплицируемого блочного устройства

DRBD (Distributed Replicated Block Device — распределённое реплицируемое блочное устройство) — это блочное устройство, предназначенное для построения отказоустойчивых кластерных систем.

DRBD предназначено для создания зеркалируемого устройства хранения данных с функцией синхронной репликации. Репликация между основным и резервным устройством DRBD-кластера осуществляется по сети.

DRBD может функционировать в двух режимах: Active/Passive и Active/Active.

В режиме ***Active/Passive*** одно из локальных хранилищ, входящих в кластер, находится в режиме read-write, а другое − read-only. В этом случае не требуется дополнительных методов синхронизации записи на хранилище, так как операции записи и чтения разрешены на дисковой подсистеме только одного из хостов.

В режиме ***Active/Active*** все локальные хранилища, входящие в кластер, находится в режиме read-write. В этом случае требуется установка дополнительных средств поверх виртуального блочного устройства DRBD, обеспечивающих целостность данных на уровне файловых систем, при одновременной работе в режиме read-write на обоих хостах, входящих в кластер.

Для настройки DRBD:

1. Файл, расположенный в директории ***/etc/drbd.d/global_common.conf***, заполнить следующим образом:

```
# DRBD is the result of over a decade of development by
LINBIT.
  # In case you need professional services for DRBD or have
  # feature requests visit http://www.linbit.com
global {       usage-count no;
      disable-ip-verification;
      # minor-count dialog-refresh disable-ip-verification
# cmd-timeout-short 5; cmd-timeout-medium 121; cmdtimeout-
long 600;
  }   common {
handlers {
                  # These are EXAMPLE handlers only.
                  # They may have severe implications,
                  # like hard resetting the node under certain
circumstances.
                  # Be careful when chosing your poison.

                  pri-on-incon-degr «/usr/lib/drbd/notify-
prion-incon-degr.sh; /usr/lib/drbd/notify-emergency-reboot.sh;
echo b > /proc/sysrq-trigger ; reboot -f»;
pri-lost-after-sb «/usr/lib/drbd/notify-prilost-after-sb.sh;
/usr/lib/drbd/notify-emergency-reboot.sh; echo b >
/proc/sysrq-trigger ; reboot -f»;
                  local-io-error «/usr/lib/drbd/notify-
ioerror.sh; /usr/lib/drbd/notify-emergency-shutdown.sh; echo o
> /proc/sysrq-trigger ; halt -f»;
```

```
                  #      fence-peer      «/usr/lib/drbd/crm-
fencepeer.sh»;                                    split-brain
«/usr/lib/drbd/notify-splitbrain.sh                    root»;
initial-split-brain      «/usr/lib/drbd/notifysplit-brain.sh
root»;                     out-of-sync «/usr/lib/drbd/notify-
out-ofsync.sh root»;
                  # before-resync-target
«/usr/lib/drbd/snapshot-resync-target-lvm.sh -p 15 -- -c 16k»;
                  # after-resync-target
/usr/lib/drbd/unsnapshot-resync-target-lvm.sh;
          }
           startup
{
                  #   wfc-timeout   degr-wfc-timeout   outdated-
wfctimeout wait-after-sb
          }
           options
{
                  # cpu-mask on-no-data-accessible
          }
           disk {
fencing dont-care;
                  # on-io-error call-local-io-error;
                  # disk-drain md-flushes resync-rate
resyncafter al-extents                    c-plan-ahead 150;
# c-delay-target                    c-fill-target 40M;
c-max-rate 700M;                    c-min-rate 4M;
# disk-timeout                    on-io-error detach;
          }
           net
{
                  protocol C;
# timeout                     max-epoch-
size 8192;                     max-
buffers 12000;                      #
unplug-watermark
```

```
                # connect-int ping-int
sndbuf-size 2097152;                rcvbuf-size
2097152;
                # ko-count
                #      allow-two-primaries      cram-hmac-alg
sharedsecret after-sb-0pri
                # after-sb-1pri after-sb-2pri always-asbp rr-
conflict
                # ping-timeout
data-integrity-alg sha1;                  #
tcp-cork on-congestion
                # congestion-fill congestion-extents
csums-alg sha1;
                # verify-alg                  # use-
rle                 after-sb-0pri discard-zero-changes;
after-sb-1pri discard-secondary;                after-
sb-2pri violently-as0p;          }  }
```

2. На обоих узлах репликации выполнить команду в консоли:

```
dd if=/dev/zero of=/var/lib/drbd/one-drbd bs=1M count=10000
```

3. После завершения выполнения на обоих узлах репликации выполнить команду в консоли:

```
losetup /dev/loop255 /var/lib/drbd/one-drbd
```

4. На обоих узлах репликации отредактировать файл, расположенный в директории ***/etc/init.d/drbd***. В секцию start перед строчкой log_daemon_msg добавить строку:

```
losetup /dev/loop255 /var/lib/drbd/one-drbd
```

5. Создать новый файл ресурса в директории ***/etc/drbd.d/one.res***, описывающий реплицируемые блочные устройства и узлы, участвующие в процессе, и заполнить его следующим образом:

```
resource one {
      on <node_name_A> {
# device to create
device    /dev/drbd1;            #
low-level device           disk
/dev/loop255;

          # unique replication uri
address   <IP_address_A>:7789;
meta-disk internal;
      }        on <node_name_B> {
device   /dev/drbd1;         disk
/dev/loop255;
           address
<IP_address_B>:7789;           meta-disk
internal;
      }
  }
```

где в секции *<node_name_XX> {…}* на каждом из узлов будут применены настройки, соответствующие имени узла (информацию об узле можно узнать командой ***uname -n***):

- параметр *address* содержит IP-адрес данного узла;
- параметр *device* указывает устройство, создаваемое подсистемой DRBD, доступное для использования в системе и обеспечивающее репликацию записываемых данных.
- параметр *disk* – блочное устройство, подлежащее репликации; при активации подсистемы DRBD перестаёт быть доступным для операций чтения/записи.

6. После заполнения конфигурационные файлы ***global_common.conf*** и ***/one.res*** скопировать на второй узел репликации командой в консоли:

```
# scp -r /etc/drbd.d/* <ip|имя второго узла>:/etc/drbd.d
```

7. На каждом узле выполнить команду в консоли для создания метаданных реплицируемого ресурса:

```
# drbdadm create-md <RESOURCE NAME>
```

8. Включить ресурс на каждом узле выполнением команды в консоли:

```
# drbdadm up <RESOURCE NAME>
```

9. Запустить начальную синхронизацию:

```
# drbdadm primary --force <RESOURCE NAME>
```

За ходом синхронизации можно следить с помощью команды

```
# cat /proc/drbd или watch -n1 cat /proc/drbd.
```

3.1.11.2.2 Настройка кластера Pacemaker/Corosync

На всех серверах виртуализации, являющимися узлами кластера, должна быть возможность получить IP-адрес по имени узла. Для этого: либо DNS, либо IP-адреса и имена всех узлов должны быть прописаны в файле ***/etc/hosts*** единым образом на всех узлах кластера.

На всех узлах кластера необходимо остановить и удалить из автозагрузки службы *corosync-notifyd* и *pacemaker_remote*:

```
# service corosync-notifyd stop
# service pacemaker_remote stop
# chkconfig --del corosync-notifyd
# chkconfig --del pacemaker_remote
```

3.1.11.2.3 Настройка Corosync

Corosync служит транспортным уровнем кластера. На этом уровне обеспечивается кворум. Данный уровень может быть сконфигурирован двумя различными способами.

Первый способ предусматривает использование ***multicast*** протокола и при большом количестве узлов может быть менее эффективным. Указание IP-адресов узлов, и, следовательно, переконфигурация, в случае изменения последних, не требуется.

Второй способ использует ***unicast*** протокол и требует перечисления в конфигурации corosync всех узлов кластера.

Для настройки corosync:

1. На одном из узлов кластера создать конфигурационный файл ***/etc/corosync/corosync.conf***.

– для multicast протокола. Содержимое можно взять из файла ***/etc/corosync/corosync.conf.example***. Должно получиться следующее содержимое файла:

```
totem {          version:2          crypto_cipher: none
crypto_hash: none       cluster_name: Name interface {
               ringnumber:0               bindnetaddr:<net_address>
mcastaddr:239.255.1.1               mcastport:5405
ttl:1
      }
} logging {       fileline: off       to_stderr:no
to_logfile:yes
      logfile:
/var/log/cluster/corosync.log
to_syslog:yes        debug: off
timestamp: on       logger_subsys {
subsys: QUORUM               debug: off
      }
} quorum {
provider: corosync_votequorum
two_node: 1 expected_votes:
1
}
```

Секция *totem.interface* определяет интерфейс, используемый узлами для служебного трафика кластера, в случае резервирования каналов связи таких секций может быть несколько. Их идентификация и приоритет использования определяется параметром *totem.interface.ringnumber*, который должен принимать значения, начиная с 0, и инкрементироваться на 1. Он должен совпадать для соответствующих сетей у всех узлов кластера.

- параметр *totem.interface.bindnetaddr* должен соответствовать адресу сети, к которой подключен интерфейс;
- параметр *totem.interface.mcastaddr* – выделенный multicast-адрес для кластера;
- параметр *totem.interface.mcastport* – выделенный multicast-порт для кластера;
- параметр *quorum.two_nodes* контролирует возможность создания кластера из двух узлов.

***Примечание**. Параметр quorum.expected_votes должен отражать необходимое количество запущенных узлов для начальной инициализации кластера.*

- для unicast протокола содержимое можно взять из файла ***/etc/corosync/corosync.conf.example.udpu***. Должно получиться следующее содержимое файла:

```
totem {        version:2
crypto_cipher:       none
crypto_hash:         none
cluster_name:        Name
interface {
              ringnumber:0
bindnetaddr:<net_address>
mcastport:5405               ttl:1
      }
transport: udpu
}     logging     {
fileline:        off
to_stderr:no
to_logfile:yes
      logfile:
/var/log/cluster/corosync.log
to_syslog:yes       debug: off
timestamp: on       logger_subsys {
subsys: QUORUM               debug: off
      }
}    nodelist    {    node{                        ring0_addr:
<node_ip_addr_in_ring0_interface_network>       nodeid: 1
  }
} quorum {
provider: corosync_votequorum two_node:
1
}
```

Внести следующие изменения:

- удалить параметр totem.interface.mcastaddr;
- параметр totem.transport – установить в значение udpu;
- удалить quorum.expected_votes;
- должна присутствовать секция nodelist с подсекциями nodelist.node для каждого узла кластера;
- для каждого узла кластера должен быть указан его IP-адрес в параметре nodelist.node.ring<X>_addr: <IP_address> соответствующий одному из интерфейсов кластера

сконфигурированному в секции totem.interface с параметром ringnumber равным <X>;

- для каждого узла кластера параметр nodelist.node.nodeid должен быть уникален.

2. Скопировать созданный конфигурационный файл на все узлы кластера.
3. Запустить на всех узлах кластера службу corosync командой:

```
# rc-service corosync start
```

4. Проконтролировать работу транспортного уровня командой:

```
# corosync-quorumtool
```

В выводе команды должны присутствовать все узлы кластера.

3.1.11.2.4 Настройка Pacemaker

Для настройки Pacemaker:

1. Запустить на всех узлах кластера службу pacemaker командой

```
# rc-service pacemaker start
```

2. Проконтролировать состояние кластера командой

```
# crm status
```

В выводе команды должны присутствовать все узлы кластера, и полное отсутствие выполняемых ресурсов.

3.1.11.2.5 Настройка высокой доступности сервера

Для запуска сервера в режиме высокой доступности:

1. Настроить кластер Pacemaker в соответствии с п. 3.1.11.2.2.
2. Остановить и удалить из автозагрузки на всех узлах кластера службы one следующими командами:

```
# service one stop
# chkconfig --del one
```

3. На двух узлах выделить под реплицируемое хранилище диск или раздел.
4. Настроить и запустить для них репликацию в соответствии с п.3.1.11.2.1.
5. Задать имя DRBD-ресурса – *hcs*.
6. Остановить и убрать из автозагрузки на обоих узлах службу drbd командами:

```
# service drbd stop
# chkconfig --del drbd
```

7. На обоих узлах отключить DRBD-ресурс командой:

```
# drbdadm down hcs
```

8. Настроить DRBD-ресурс.
   Для настройки DRBD-ресурса:

   а. На одном из узлов войти в оболочку управления ресурсами кластера Pacemaker, в раздел конфигурации:

```
# crm configure
```

   б. Отключить фенсинг:

```
# property stonith-enabled=false
```

   в. Создать примитив DRBD:

```
primitive drbd_hcs ocf:linbit:drbd \
params drbd_resource=hcs \   op monitor
interval=«29s» role=«Master» \   op
monitor interval=«30s» role=«Slave»
```

г. Указать для данного примитива конфигурацию Master/Slave:

```
ms ms_drbd_hcs drbd_hcs \   meta master-
max=«1» master-node-max=«1» \
clone-max=«2» clone-node-max=«1» \
notify=«true»
```

д. Актуализировать изменения конфигурации кластера:

```
# commit
```

е. Выйти из оболочки управления ресурсами:

```
# bye
```

9. Проверить состояние кластера и определить узел, на котором запущен мастер DRBD-ресурса командой:

```
# crm status
```

10. На узле, обслуживающем мастер DRBD-ресурс, создать файловую систему на требуемом ресурсе:

```
# mkfs.ext4 /dev/drbd1
```

11. Скопировать базу настроечных параметров СГУ, на узле, обслуживающем мастер DRBD-ресурс:

а. Смонтировать хранилище в каталог ***/mnt:***

```
# mount /dev/drbd1 /mnt
```

б. Скопировать данные:

```
# cp -a /var/lib/one/. /mnt
```

в. Отмонтировать хранилище:

```
# umount /mnt
```

12. Настроить ресурсы хранилища, виртуального адреса и СГУ. Связать их с DRBD-ресурсом:

а. На одном из узлов войти в оболочку управления ресурсами кластера Pacemaker, в раздел конфигурации, командой:

```
# crm configure
```

б. Создать примитив виртуального IP:

```
primitive ip_hcs ocf:heartbeat:IPaddr2 params
ip=«192.168.2.94» nic=«sys0»
```

в. Создать примитив точки монтирования:

```
primitive fs_hcs ocf:heartbeat:Filesystem \
  params device=«/dev/drbd1» \
        directory=«/var/lib/one» fstype=«ext4»
```

г. Создать примитив запуска СГУ, заполнив файл в директории **/usr/bin/one-res** (Рисунок 5) и в раздел stop добавить строку ***pkill lighttpd***.

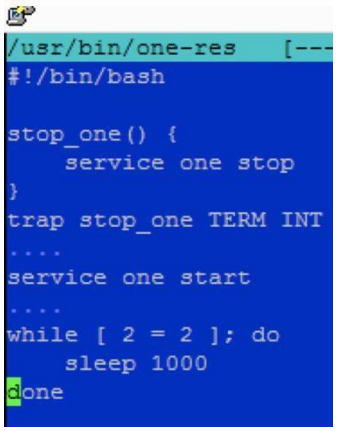


Рисунок 5 – Создание примитива запуска СГУ

д. Создать примитив запуска СГУ:

```
primitive hcs ocf:heartbeat:anything \     params
binfile=«/bin/sh» \
            cmdline_options=«-f /bin/one-res»
```

е. Создать группу ресурсов:

```
group g_hcs fs_hcs ip_hcs hcs
```

ж. Указать порядок запуска (сначала DRBD-ресурс, потом остальные):

```
order o_hcs inf: ms_drbd_hcs:promote g_hcs:start
```

з. Указать условия размещения (все ресурсы, связанные с СГУ должны быть размещены на том же узле, что и DRBD-ресурс):

```
colocation cl_hcs inf: g_hcs ms_drbd_hcs:Master
```

и. Актуализировать изменения конфигурации кластера:

```
commit
```

к. Выйти из оболочки управления ресурсами:

```
bye
```

13. Проконтролировать состояние ресурсов кластера можно командой:

```
crm status
```

3.1.12 Настройка брокера подключения тонких клиентов

Брокер подключений – это служба, являющаяся посредником при подключении тонкого клиента VDI к серверу, позволяющая организовать балансировку нагрузки среди независимых серверов.

Для запуска брокера подключений на каждом сервере с установленной СГУ:

1. Выполнить команду:

```
docker exec -it hcs bash
```

2. Редактором в файле ***/etc/squid/squid.conf*** указать сеть гипервизоров:

```
acl SPICE_HOSTS src 192.168.0.0/16
```

3. Перезагрузить брокер подключений и выйти:

```
pkill squid
/usr/sbin/squid
exit
```

Балансировка нагрузки брокера подключений осуществляется в момент подключения тонкого клиента на стороне сервера виртуализации при помощи алгоритма Power-of-two-choices. Балансировка реализуется путем выдачи оптимально загруженного экземпляра брокера подключений. Балансировщик имеет точки балансировки на каждом гипервизоре группы. Дополнительных настроек его в процессе работы не требуется.

3.1.13 Управление информационными потоками между компонентами виртуальной инфраструктуры

Программный комплекс (ПК) «Иридиум» обеспечивает управление потоками информации между компонентами виртуальной инфраструктуры:

- фильтрацию;
- маршрутизацию;
- контроль соединения.

Создание виртуальных сетей описано в главе **Ошибка! Источник ссылки не найден.** настоящего руководства. Более подробное описание функций сетевого управления приведено ниже.

3.1.13.1 Фильтрация сетевого трафика

Для организации фильтрации сетевого трафика для виртуальных сетей используются правила iptables. На сервере виртуализации в консоли необходимо набрать команду следующего вида:

```
iptables –A INPUT –d ip-адрес –j DROP,
```

где *ip-адрес* – адрес виртуальной сети, в которую будет запрещена передача пакетов.

3.1.13.2 Автоматическое изменение маршрутов передачи сетевых пакетов

Для настройки автоматического изменения маршрутов передачи сетевых пакетов между компонентами виртуальной инфраструктуры:

1. На сервере виртуализации включить маршрутизацию командой в консоли:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

2. При создании новой виртуальной сети выбрать опцию **Перенаправлять в физическую сеть** (Рисунок 6).
3. В поле **Режим** выбрать **Маршрутизированная.**

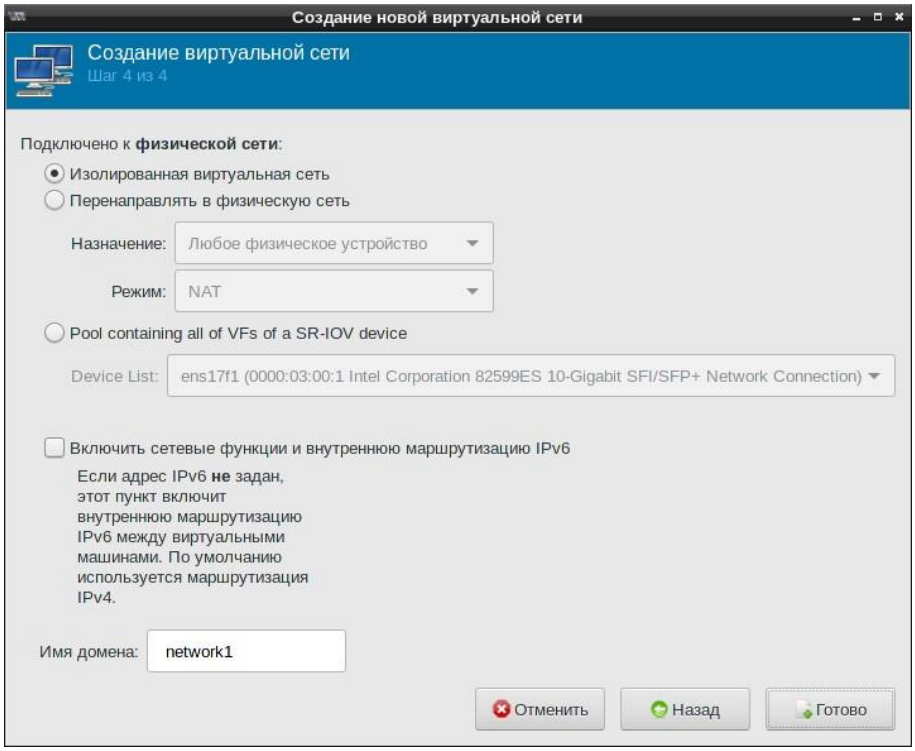


Рисунок 6 – Подключение к физической сети

4. Назначить виртуальную сеть ВМ на сервере виртуализации (см. п. **Ошибка! Источник ссылки не найден.**).

5. В ОС, установленной в ВМ, настроить статический IP-адрес из адресного пространства, и маршрутизацию по умолчанию, например, командой:

```
route add default gw ip-адрес,
```

где *ip-адрес* – адрес виртуальной сети из назначенного адресного пространства.

3.1.13.3 Отключение неиспользуемых сетевых протоколов

Для отключения неиспользуемых сетевых протоколов:

1. При создании новой виртуальной сети выбрать опцию **Перенаправлять в физическую сеть** (Рисунок 6).
2. В поле **Режим** выбрать **NAT**.
3. Назначить виртуальную сеть ВМ на сервере виртуализации.
4. В ОС, установленной в ВМ, настроить статический IP-адрес из назначенного адресного пространства.
5. Настроить маршрутизацию по умолчанию командой:

```
route add default gw ip-адрес
```

где *ip-адрес* – адрес виртуальной сети из назначенного адресного пространства.

6. В консоли сервера виртуализации создать правило через команду iptables, запрещающую все исходящие соединения (например, на порт http (80)):

```
iptables –A INPUT –i eth1 –p tcp –dport 80 –j DROP
```

3.1.13.4 Обеспечение изоляции потоков данных

Изоляция потоков данных обеспечивается настройкой типа подключения к физической сети – **Изолированная виртуальная сеть** при создании виртуальной сети (Рисунок 6).

В режиме изолированной сети виртуальные машины, подключенные к виртуальному коммутатору, могут взаимодействовать друг с другом и с хостом. Тем не менее, их трафик не будет выходить за пределы хоста. Виртуальные машины не могут получать сетевой трафик за пределами хоста.

При выборе изолированной сети, можно получить доступ к шлюзу по умолчанию командой:

```
route add default gw ip-адрес (в большинстве гостевых ОС)
```

где *ip-адрес* – адрес виртуальной сети из назначенного адресного пространства.

Для полной изоляции сети на консоли необходимо набрать команду следующего вида:

```
iptables –I FORWARD –s ip-адрес –j DROP
```

где *ip-адрес* – адрес виртуальной сети из назначенного адресного пространства.

3.1.13.5 Обеспечение фильтрации ARP-пакетов

Для защиты от атак на протокол ARP в локальной сети, где установлены серверы и терминалы Программный комплекс (ПК) «Иридиум» необходимо использовать коммутаторы с встроенными средствами защиты от подмены адресов (ARP-spoofing) с возможностью настройки фильтрации пакетов используя списки контроля доступа (packet filtering ACL).

На коммутаторах сети следует настроить следующие функции, согласно инструкции к этим устройствам:

- фильтрацию всех ARP-пакетов на всех пользовательских портах, у которых в адресе протокола отправителя (SPA) содержится IP-адрес шлюза. Серверы и терминалы Программный комплекс (ПК) «Иридиум» будут защищаться от подмены адреса шлюза;

- фильтрацию всех ARP-пакетов на каждом из пользовательских портов, у которых адрес устройства отправителя (SHA) и адрес протокола отправителя (SPA) не совпадают с известными заранее MAC и IPадресами пользователя этого порта. Тем самым серверы и терминалы Программный комплекс (ПК) «Иридиум» будут защищаться от всех ARP-атак: от подмены адреса шлюза и адреса другого пользователя.

В случае отсутствия встроенных средств защиты от подмены адресов, в коммутаторах сети, к которой подключены компоненты Программный комплекс (ПК) «Иридиум» терминалы и серверы Программный комплекс (ПК) «Иридиум» должны коммутироваться в изолированном VLAN или сегменте, в котором не допускается подключение недоверенных сетевых устройств.

3.1.14 Объединение маршрутов ввода/вывода

Устройства множественного ввода/вывода (Device Mapper Multipathing, DM-Multipath) предоставляют возможность объединять несколько маршрутов ввода/вывода между сервером и системой хранения данных в единый канал. Это позволяет рассматривать доступный по нескольким путям массив как одно мета-устройство.

Например, если сервер с двумя двух-портовыми Fibre Channel картами Host Bus Adapter (HBA) подключен к одному и тому же массиву, то на сервере будет обнаруживаться четыре устройства, например, /dev/sd{a,b,c,d}. При помощи модуля ядра dm-multipath можно собрать из них мета-устройство

хранения данных, агрегирующее все четыре пути /dev/dm-N. Это обеспечивает прозрачную для гипервизора, ВМ и приложений отказоустойчивую конфигурацию. В случае выхода из строя HBA, кабеля или коммутатора (если каждый HBA подключен через свой коммутатор) разрыва связи с системой хранения данных (СХД) не происходит.

Для проверки доступа по нескольким путям, в консоли сервера виртуализации ввести команду:

```
# multipath -ll
```

Выводом команды является дерево подключений устройств множественного ввода/вывода. Оно содержит:

- объединенные устройства и их специализированное системное наименование wwn;
- устройства, из которых собираются объединенные устройства множественного ввода/вывода.

3.1.15 Подсистема регистрации событий

При помощи подсистемы регистрации событий можно получить подробную информацию о всех системных событиях. В КП «ТерминалСервер» осуществляется регистрация следующих событий:

- запрос на доступ к защищаемому ресурсу (ВМ);
- создание и уничтожение виртуальных машин;
- действия по изменению правил разграничения доступа.

Сведения о события представлены в общесистемном журнале СГУ (см. п. 3.2.32).

Для настройки отображения всех событий:

1. В консоли ввести ряд команд:

```
docker exec –it hcs bash
```

2. В редакторе vim или mcedit внести изменения в файл

   /etc/one/oned.conf, установив значение параметра DEBUG_LEVEL=3.

3. Сохранить конфигурационный файл.
4. Перезапустить службу командами:

```
su –
oneadmin
one restart
exit  exit
```

После перезапуска в системе будут регистрироваться все события и выводиться в общий журнал.

3.1.16 Инсталляция и защищённое исполнение контейнеров «Иридиум» со сторонним программным обеспечением

В системном окружении гипервизора Программный комплекс (ПК) «Иридиум» возможно защищённое исполнение контейнеров «Иридиум». Контейнеры в окружении «Иридиум» исполняются с предопределёнными администратором безопасности мандатными и дискреционными правами, в ограниченном контексте исполнения (Рисунок 7).

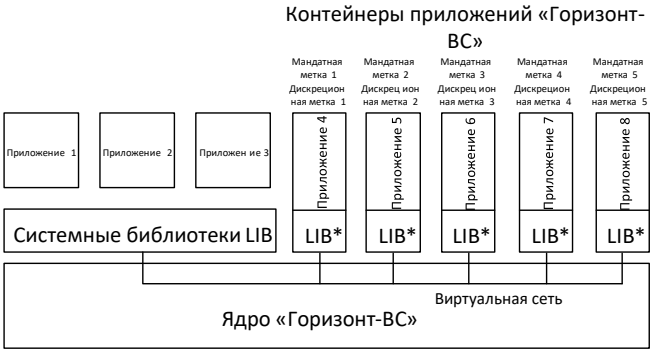


Рисунок 7 – Контейнеры приложение «Иридиум»

Контейнер «Иридиум» представляет собой chroot образ, включающий системные библиотеки «Иридиум» и сервисное программное обеспечение.

Также возможно защищённое исполнение произвольного контейнера, состав системных библиотек которого отличается от состава системных библиотек «Иридиум».

Взаимодействие защищённых контейнеров в рамках гипервизора и с внешними субъектами и объектами осуществляется через виртуальные сетевые соединения с использованием мандатных меток.

Возможно подключение к контейнерам изолированных, либо разделяемых хранилищ, представленных в виде точек монтирования гипервизора Программный комплекс (ПК) «Иридиум». Доступ к файлам на подключаемых хранилищах определяется дискреционными и мандатными правами контейнера.

3.1.16.1 Настройка прав исполнения контейнера

Права исполнения контейнера задаются в файле ***/etc/gvscontainers/gvscpolicy.conf:***

```
# Container 1 name=«Имя_контейнера1»
dac=«Имя_пользователя1»
mac=«Мандатная метка1»

# Container 2 name=«Имя_контейнера2»
dac=«Имя_пользователя2» mac=«Мандатная метка2»
```

3.1.16.2 Инсталляция контейнера

После установки Программный комплекс (ПК) «Иридиум» необходимо установить контейнер.

Для установки контейнера:

1. Отредактировать 947-ю строку файла ***/etc/lvm/lvm.conf***

```
use_lvmlockd = 0
```

2. Расширить менеджер логических томов (lvm) командой в консоли:

```
lvresize -l +100%FREE /dev/sdX
```

где *sdX* диск, на который произведена установка. Можно посмотреть командой **cat /proc/partitions**.

```
resize2fs /dev/HVS/data
```

3. Скопировать образ контейнера и скрипт установки с предварительно примонтированного USB-накопителя:

```
mount /dev/sdY /mnt
```

можно посмотреть командой cat /proc/partitions.

```
cp /mnt/hcs-* /data/0/
```

4. Запустить docker и добавить в автозагрузку:

```
rc-service docker start rc-update
add docker default
```

5. Загрузить образ контейнера:

```
cd /data/0/
./hcs-run.sh «Имя_контейнера»
```

6. Проверить доступ к контейнеру (curl опции ссылка), IP-адрес и порт ссылки заданные в процессе инсталляции контейнера.

3.1.17 Интеграция со службой каталогов Microsoft Active Directory

Для подключения к службе каталогов Microsoft Active Directory (MS AD) используется надстройка LDAP Authentication, которая позволяет пользователям иметь те же учетные данные, что и в MS AD.

Это дополнение не устанавливает сервер LDAP и не осуществляет его настроек, не создает, удаляет или изменяет какие-либо записи на сервере LDAP, к которому он подключается. СГУ подключается к уже работающему серверу LDAP, выполняет успешную операцию ldapbind и предоставляет возможность выполнять поиск пользователей.

Файл конфигурации для модуля аутентификации находится по адресу ***/etc/one/auth/ldap_auth.conf***.

Для подключения LDAP-аутентификации:

1. Внести следующие значения в поля файла конфигурации:

Пример поля	Описание
: rfc2307bis : true	Разрешение на использование MS AD
: user : Administrator@win.gorizont-vs.ru	Пользователь MS AD с разрешениями на чтение в дереве пользователей плюс домен (*например, администратор в домене win.gorizont-vs.ru указывается как Administrator@win.gorizont-vs.ru*)
: password : qwerty	Пароль пользователя
: host : localhost	Имя хоста или IP-адрес контроллера домена
: base : 'dc = domain'	Базовое DN для поиска пользователей. Необходимо разложить полное доменное имя и использовать каждую часть как компонент DN. *Например, для win.gorizont-vs.ru получим базовое DN: DN = win, DN = gorizont-vs, DN = ru*.
:user_field: ‘ sAMAccountName ‘	Поле в LDAP, содержащее имя пользователя
: user_group_field: 'dn'	Поле пользователя, которое находится в группе group_field
: group_field: 'member'	Имя поля для членства в группе

2. Включить в СГУ возможность внешней аутентификации, добавив в файл ***/etc/one/oned.conf*** строку:

```
DEFAULT_AUTH  =  «ldap»
```

3. В ситуации когда нужно провести поиск пользователя на нескольких серверах LDAP, необходимо обратиться к специальному ключу «**:order».**

Элементы «**:order»** - это имена серверов или вложенные массивы имен серверов, представляющие группу доступности. Элементы в «**:order»** обрабатываются один за другим до тех пор, пока пользователь не пройдет успешную аутентификацию или не будет достигнут конец списка. Внутри группы доступности запрашивается только самый первый сервер, к которому можно успешно подключиться. Любой сервер, неуказанный в **«:order**», запрашиваться не будет. пример:

:order:

-server 1

-server 2

3.1.18 Сквозная аутентификация на основе протокола Kerberos

Чтобы использовать проверку подлинности Kerberos, пользователям необходимо настроить общедоступный драйвер. При этом аутентификация пользователей через интерфейс XML-RPC будет недоступна, для них будет предоставлен доступ только Sunstone.

Для обновления существующих пользователей для использования проверки подлинности Kerberos необходимо изменить драйвер на общедоступный и обновить пароль командой:

```
oneuser chauth new_user public «new_user @ DOMAIN»
```

Новые пользователи с этим методом аутентификации должны создаваться следующим образом:

```
oneuser create new_user «new_user @ DOMAIN» --driver public
```

Чтобы включить метод входа в систему по Kerberos, следует установить в файле ***/etc/one/sunstone-server.conf*** значение *remote* для параметра *auth*:

```
: auth :  remote
```

На экране входа в систему больше не будут отображаться поля имени пользователя и пароля, так как вся информация будет браться из сервера Kerberos или службы удаленной аутентификации.

3.1.19 Настройка подключения хранилищ по протоколу Fibre Channel

Для обнаружения HBA карты на сервере:

1. Ввести команду в консоли:

```
lspci -nn | grep -i hba
```

4. Найти WWN портов командой:

```
systool -c fc_host -v | grep port_name
port_name           = «0x21000024ff53e456»
port_name           = «0x21000024ff53e457»
```

5. Определить статус портов:

```
systool -c fc_host -v | grep port_state
port_state          = «Online»
port_state          = «Online»
```

6. Если статус Online и настроен доступ на СХД, то можно перезагрузить модуль адаптера и получить доступ к LUN:

```
rmmod qla2xxx modprobe
qla2xxx lsscsi -s
```

где xxx – версия драйвера QLE.

3.2 Работа в Системе группового управления

3.2.1 Общие сведения

Система группового управления (СГУ) Программный комплекс (ПК) «Иридиум» представляет собой графический веб-интерфейс, предназначенный для: – конечных пользователей; – администраторов.

При помощи СГУ осуществляется удаленное создание и управление виртуальной инфраструктурой на базе универсальных серверных платформ и облаков.

СГУ обеспечивает создание и управление виртуальной инфраструктурой как на серверной платформе, так и на группе серверных платформ (кластере).

Узлы под управлением СГУ разделяются на:

- вычислительные узлы – серверы виртуализации, на которых выполняются ВМ;
- контроллеры (основной и резервный) – вычислительные узлы, которые обеспечивают выполнение ВМ и запуск менеджера конфигурации.

Добавление вычислительных узлов в кластер и их удаление обеспечивается без необходимости полной переконфигурации (первоначальной настройки) виртуальной инфраструктуры. В момент добавления нового узла в кластер выполняется его автоматическая настройка.

СГУ позволяет управлять полным жизненным циклом виртуальных машин с возможностью их клонирования и миграции. Для работы СГУ используется MySQL — свободная реляционная система управления базами данных.

СГУ позволяет производить интеграцию внешних систем с Программный комплекс (ПК) «Иридиум»по XML-RPC. Описание REST-API

приведено в приложении к данному документу (ПРИЛОЖЕНИЕ В). **3.2.2 Вход в Систему группового управления**

Для подключения к СГУ:

1. Ввести в адресной строке браузера IP-адрес узла, на котором установлена СГУ (*например*, 192.168.2.1), либо доменное имя.
2. В открывшемся окне аутентификации ввести имя пользователя и пароль (Рисунок 8).

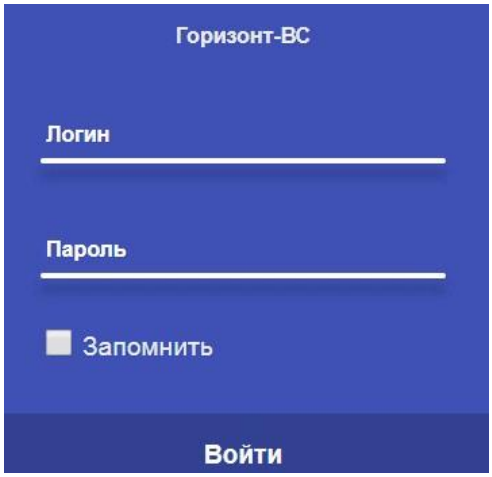


Рисунок 8 – Окно аутентификации

***Примечание**. По умолчанию имя пользователя и пароль «admin/admin». При первом запуске необходимо обязательно сменить пароль администратора в разделе **Система** → **Пользователи** (п. 3.2.9.4). После смены необходимо поменять его в контейнере в файле **/var/lib/one/.one/one_auth**.*

Пароль при вводе отображается в скрытом виде, таким образом осуществляется защита обратной связи при вводе аутентификационной информации.

3.2.2.1 Описание веб-интерфейса Системы группового управления

3.2.2.2 Главное окно СГУ

После успешной аутентификации отобразится главное окно СГУ – **Информационная панель** (Рисунок 9).

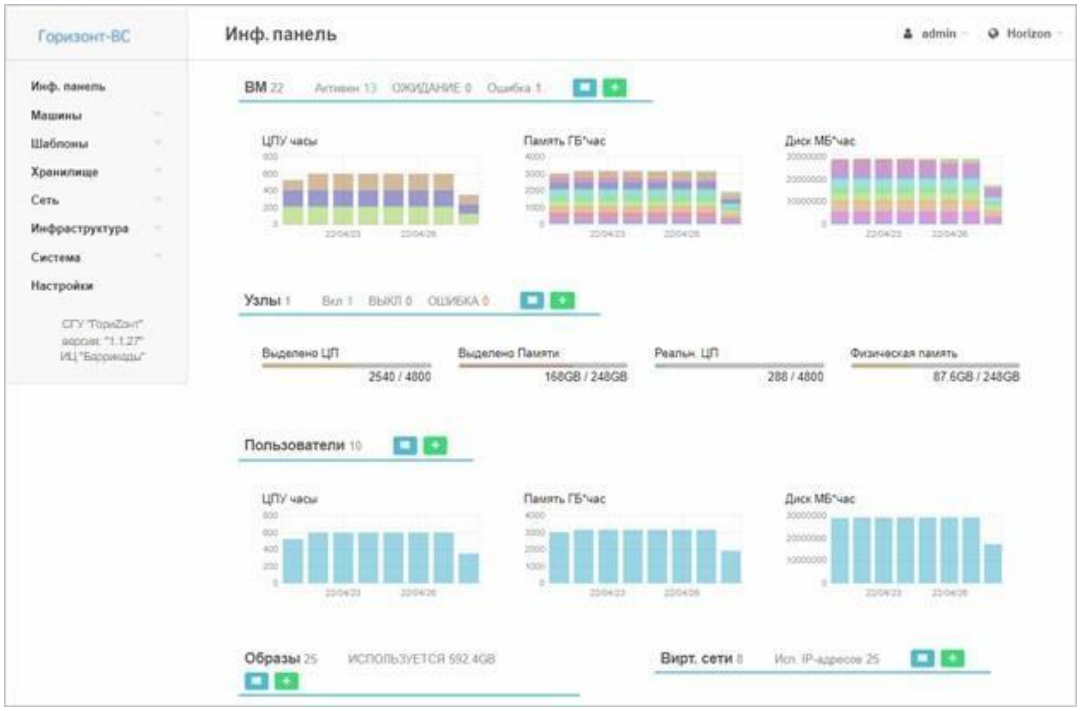


Рисунок 9 – Веб-интерфейс СГУ. Главное окно

В левой колонке размещено меню управления системой. В верхней части – название текущего меню, имя пользователя и наименование ведущей хостинговой зоны (зоны управления).

Раздел **ВМ** содержит информацию о количестве:

- созданных ВМ;
- функционирующих (активных) ВМ;
- размещаемых в данный момент времени ВМ в системе (режим ожидания);
- сообщений об ошибках.

На диаграммах представлена статистика о загрузке ЦПУ, оперативной памяти и дискового пространства как по всем ВМ, размещенных в системе, так и по каждой ВМ в отдельности (Рисунок 10).

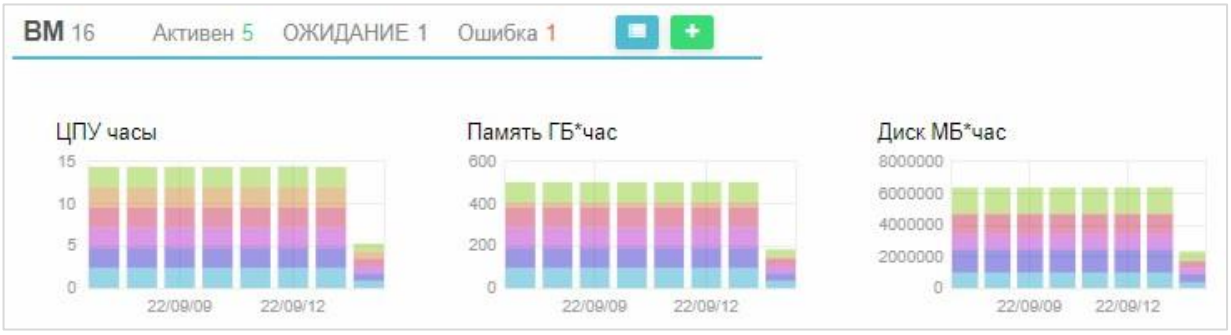


Рисунок 10 – Сведения о ВМ

Раздел **Узлы** (Рисунок 11) содержит следующую информацию:

- в верхней части – статистику по серверам:
  - количество физических серверных узлов, зарегистрированных в системе;
  - количество функционирующих и отключенных узлов;
  - количество сообщений об ошибках.
- в нижней части – мониторинг суммарного использования (Рисунок 11):
  - процессорной мощности в системе со всех хостов;
  - выделенных ресурсов ЦП для ВМ;
  - реальной процессорной мощности в системе;
  - объем оперативной памяти в системе.

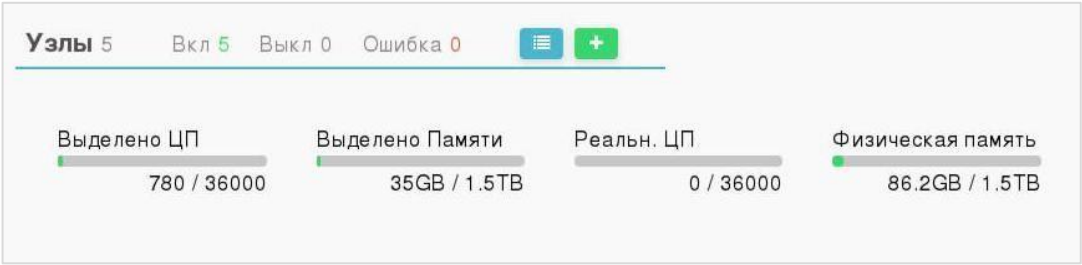


Рисунок 11 – Статистика узлов системы

Раздел **Пользователи** содержит информацию о количестве зарегистрированных пользователей и администраторов в системе. На рисунке ниже (Рисунок 12) представлен мониторинг суммарного использования ресурсов (ЦПУ, пространства в СХД, оперативной памяти) каждым пользователем.

Рисунок 12 – Статистика пользователей

Раздел **Образы ВМ** содержит информацию о количестве созданных образов в зоне управления и используемый объем жесткого диска (Рисунок 13).

Раздел **Виртуальные сети** содержит информацию о количестве созданных виртуальных сетей и используемых в зоне управления IP-адресов (Рисунок 13).

Рисунок 13 – Образы ВМ и Виртуальные сети

В каждом разделе с помощью кнопок и предусмотрен переход на соответствующую страницу СГУ или создания виртуального ресурса:

- машины/ВМ;
- инфраструктура/узлы;
- система/пользователи;
- хранилище/образы ВМ;
- сеть/виртуальные сети.

3.2.2.3 Описание основных элементов интерфейса

Информация в рабочей области разделов представлена в виде таблицы (Рисунок 14). Состав колонок индивидуален для каждого раздела.

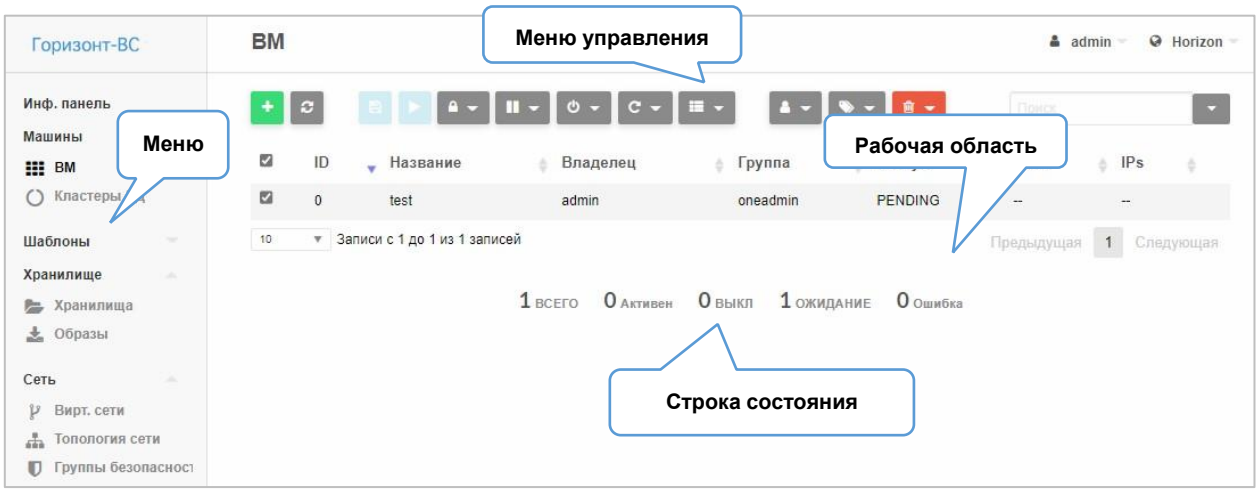
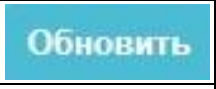


Рисунок 14 – Пример интерфейса раздела

Под таблицей содержится строка состояния, в которой отображается общее количество строк в таблице и количество виртуальных ресурсов в разных состояниях.

Над таблицей располагается меню управления. Каждый раздел содержит индивидуальный набор элементов управления. В таблице ниже (Таблица 3) приведено описание элементов управления, общих для большинства разделов:

Таблица 3 – Общие команды управления

Опция	Функция	Описание
	Создание нового ресурса	Открывает страницу интерфейса создания нового ресурса
	Обновление текущей страницы (активна всегда)	После внесения каких-либо изменений в работу виртуального ресурса или его конфигурацию необходимо выполнить обновление страницы, чтобы увидеть изменения
	Удалить	Удаление ресурса
	Изменение конфигурации	Открывается страница изменения конфигурации ресурса
	Выпадающее меню:	

	Администрирование	Разрешение специальных операций. Данные операции должны назначаться только пользователям с ролью администратора
	Управление	Разрешение на работу, при котором операции могут изменять ресурс
	Пользование	Разрешение на работу с ресурсом, при котором операции не изменяют ресурс
Опция	**Функция**	**Описание**
	Unlock	Разблокирование всех возможных операций с ресурсом
	Выпадающее меню:	
	Приостановить работу	Приостановка (Пауза) работы ресурса
	Остановить	Полная остановка работы ресурса
	Выпадающее меню:	
	Сменить владельца	Позволяет сменить пользователя ВМ
	Сменить группу	Позволяет сменить группу пользователей
	Добавить метку	Для удобства управления ресурсом в системе группового управления предусмотрены метки, которые позволяют группировать и выводить списки ресурсов по их типу или функциональному предназначению. *Например: ВМ бухгалтерии, ВМ отдела АСУ и т.д.*
	Назад	Возвращает назад к списку. Кнопка доступна в окне информации о ресурсе

При нажатии на строку таблицы открывается окно просмотра и редактирования данных выбранного ресурса (Рисунок 15):

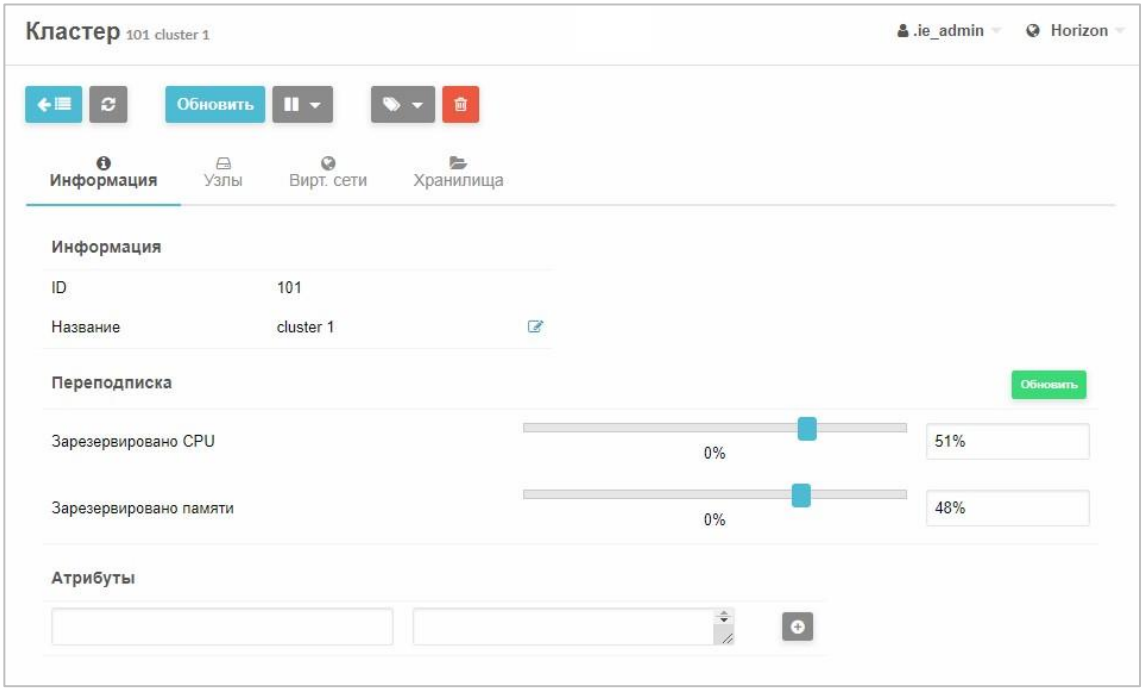


Рисунок 15 – Окно просмотра и редактирования информации о виртуальном ресурсе

3.2.3 Поддержка защищённых протоколов доступа к Системе группового управления

В Программный комплекс (ПК) «Иридиум» реализован защищенный доступ к СГУ с помощью ssh.

Для настройки защищенного подключения к СГУ требуется:

1. Зайти по ssh на сервер управления, где расположен СГУ.
2. Зайти в контейнер, выполнив команду:

```
docker exec -it hcs bash
```

3. Перейти в каталог: ***/etc/lighttpd***.
4. Отредактировать файл***: lighttpd.conf***.
5. Отредактировать файл: ***/etc/one/sunstone-server.conf.***
6. Отредактировать нужные пункты:

```
:vnc_proxy_port: 29876
:vnc_proxy_support_wss: no
:vnc_proxy_cert:
:vnc_proxy_key:
# :vnc_proxy_support_wss: yes
# :vnc_proxy_cert: /etc/lighttpd/server.pem
# :vnc_proxy_key: /etc/lighttpd/server.pem
:vnc_proxy_ipv6: false
:vnc_request_password: false
```

7. Выйти из контейнера и перезапустить:

```
docker restart hcs
```

3.2.4 Конфигурация учетной записи администратора

Федерация будет иметь уникальную учетную запись администратора (oneadmin). Это необходимо для выполнения вызовов API через зоны. Нельзя использовать эту учетную запись непосредственно в рабочей среде и создавать учетную запись в группе «oneadmin» для каждого администратора зоны.

Если необходимы дополнительные ограничения доступа, администратор федерации может создать специальную административную группу с полными разрешениями только для одной зоны.

После установки СГУ в системе по умолчанию регистрируется ведущая зона управления с конечной точкой ***http://адрес ядра системы группового управления зоной:2633/RPC2***.

В верхнем правом углу страницы отображается значок глобуса рядом с названием зоны, которая используется. При нажатии на пиктограмму открывается раскрывающийся список со всеми зонами, к которым у пользователя есть доступ (Рисунок 16).

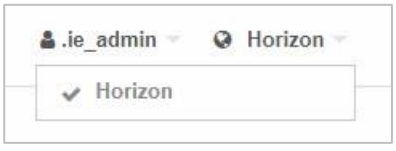


Рисунок 16 – Доступные администратору зоны управления

При нажатии на любую из зон в раскрывающемся списке пользователь попадает в выбранную зону.

3.2.5 Создание и конфигурация зон управления

3.2.5.1 Структура федерации СГУ

Зона управления – это логическое объединение серверов виртуализации в группы по функциональному или иному признаку.

СГУ позволяет объединять несколько различных инфраструктур в единую федерацию. Каждая инфраструктура в федерации СГУ называется зоной (zone). Федерация строится по схеме ведущий-ведомый (master-slave) – одна главная зона и несколько управляемых зон. Любые другие конфигурации федерации (например, более глубокая иерархия ведущийведомый) не поддерживаются.

В подобной тесно связанной интеграции все облачные инфраструктуры имеют единую базу пользователей, а управление всей федерацией осуществляется централизованно с главной зоны. Подобная схема интеграции удобна для объединения территориально разнесенных облачных инфраструктур одной организации (например, ее подразделений), но не подходит для объединения инфраструктур разных организаций ввиду присущей данному подходу централизованного управления, а в случае использования организациями разных платформ – невозможна. Все зоны будут иметь одинаковые настройки учетных записей пользователей, групп и разрешений. Можно определить политику доступа по всей федерации, чтобы пользователи имели ограниченный доступ к определенным зонами или конкретным кластерам внутри зоны.

Конечные пользователи могут использовать ресурсы независимо от того, где они находятся. Интеграция является бесшовной, то есть пользователь, зарегистрированный в веб-интерфейсе, выбирает зону, в которой хочет работать.

Главная зона (мастер-зона) отвечает за обновление объединенной информации и репликацию обновлений в управляемых зонах. Объединенная информация, разделяемая всеми зонами, включает пользователей, группы, виртуальные ЦОД (VDC), ACL-правила и зоны.

Управляемые зоны имеют доступ только для чтения к локальной копии объединенной информации. Операции записи в управляемых зонах перенаправляются в главную зону. В открытом для чтения файле локальной копии могут быть неактуальные данные, пока обновленные (актуальные) данные реплицируются от главной зоны к управляющим. Этот подход обеспечивает последовательную согласованность между зонами (каждая зона будет тиражировать операции в том же порядке) без какого-либо влияния на скорость действий только для чтения.

Репликация объединенной информации реализуется с помощью журнала, который включает в себя последовательность операторов SQL, применяемых к общим таблицам. Этот журнал реплицируется и используется в базе данных каждой зоны. Такая модель репликации допускает отказы при подключении и выключения зоны, при этом отсутствует влияние на федерацию.

3.2.5.2 Конфигурация федерации СГУ

В данном пункте описано, как настроить две (и более) зоны СГУ для работы по схеме ведущий-ведомый. Данный процесс может применяться при новых инсталляциях или уже имеющихся экземплярах СГУ.

Сервер главной зоны СГУ реплицирует изменения базы данных в управляемых зонах с использованием журнала. Журнал содержит команды SQL, которые должны применяться во всех зонах.

***Примечание**: Главный и управляемые серверы должны взаимодействовать друг с другом через **API XML-RPC**.*

Шаг 1. Выбор главной зоны федерации

Настройка главной зоны федерации СГУ начинается с выбора главной зоны федерации. Главная зона будет отвечать за обновление общей информации по всем зонам и репликацию обновлений на управляемые устройства.

Можно начать с существующей установки или с новой.

Примечание. *При установке новой главной зоны с нуля необходимо запустить СГУ, по крайней мере, один раз, чтобы правильно загрузить базу данных.*

Для установки главной зоны:

1. **Master (главная зона)**. Отредактировать конечную точку главной зоны. Это можно сделать через веб-интерфейс или с помощью команды **onezone**. Необходимо записать эту конечную точку, чтобы использовать ее позже при настройке управляемых зон.

```
$ onezone update 0
ENDPOINT = http://<master-ip>:2633/RPC2
```

Примечание*. При установке высокой доступности master-ip должен быть установлен на плавающий IP-адрес. В зонах с одним сервером используется IPадрес сервера.*

2. **Master**: Обновить файл в директории ***/etc/one/oned.conf*** для изменения режима работы.

```
FEDERATION=[
MODE=«MASTER»,
ZONE_ID= 0
]
```

3. **Master**: Перезагрузить СГУ.

Теперь можно добавлять управляемые зоны.

<u>Шаг 2. Добавление управляемой зоны</u> Для добавления управляемой зоны:

1. **Slave**: Установить СГУ на рабочую станцию, и запустить хотя бы один раз.
2. **Slave**: Остановить СГУ.
3. **Master**: Создать зону для управления и записать новый идентификатор зоны. Это можно сделать через веб-интерфейс или с помощью команды **onezone**:

```
$ vim /tmp/zone.tmpl
NAME     = slave-name
ENDPOINT = http://<slave-zone-ip>:2633/RPC2
$onezone create /tmp/zone.tmpl
ID: 100
$onezone list
   ID NAME
0OpenNebula
100slave-name
```

***Примечание**: в настройках высокой доступности необходимо использовать плавающий IP-адрес для slave-zone-ip, в зонах с одним сервером использовать IP-адрес сервера.*

4. **Master**: Сделать снимок объединенных таблиц следующей командой:

```
$ onedb backup --federated -s /var/lib/one/one.db
Sqlite database backup of federated tables stored in
/var/lib/one/one.db_federated_2017-6-15_8:52:51.bck Use
'onedb restore' to restore the DB.
```

5. **Master**: скопировать снимок базы данных в управляемую зону.
6. **Master**: скопировать только выбранные файлы из каталога ***/var/lib/one/.one*** в управляемую зону. Этот каталог и его содержимое должны иметь только одного администратора в качестве владельца. Заменять только следующие файлы:

```
ls -1 /var/lib/one/.one
ec2_auth one_auth
oneflow_auth
onegate_auth
sunstone_auth
```

7. **Slave**: Обновить ***/etc/one/oned.conf,*** чтобы изменить режим на управляемый, установить URL-адрес главной зоны и ZONE_ID, полученный при создании главной зоны:

```
FEDERATION = [
MODE        = «SLAVE»,
ZONE_ID     = 100,
MASTER_ONED = «http://<master-ip>:2633/RPC2» ]
```

8. **Slave**: Восстановить снимок базы данных:

```
onedb restore --federated -s /var/lib/one/one.db
/var/lib/one/one.db_federated_2017-6-14_16:0:36.bck Sqlite
database backup restored in one.db
```

9. **Slave**: Запустить СГУ.

Зона настроена и готова к использованию.

Шаг 3 [Опциональный]. Добавление режима высокой доступности в управляемую зону

Теперь можно добавлять больше серверов в управляемую зону для высокой доступности.

Процедура аналогична описанной для автономных зон в руководстве по установке высокой доступности (см. п. **Ошибка! Источник ссылки не н айден.** «**Ошибка! Источник ссылки не найден.**»).

В этом случае репликация работает многоуровневым способом. Мастер реплицирует изменение базы данных на один из серверов зон. Затем этот сервер реплицирует изменение на других серверах зон.

Важно*! Дважды проверить, работает ли федерация, до добавления серверов высокой доступности в зону, так как будут обновляться метаданные зоны – они являются объединенной информацией.*

3.2.5.3 Импорт существующих зон СГУ

Виртуальные ресурсы: хранилища данных, виртуальные машины, сети и т.д., за исключением существующих пользователей и групп, сохраняются автоматически.

Автоматическая процедура для импорта существующих пользователей и групп в запущенную федерацию отсутствует.

Для импорта пользователей и групп:

1. **Slave**: Создать резервные копии данных пользователей, групп и виртуальных ЦОД (VDC), которые необходимо воссоздать в федеративной среде.
2. **Slave**: Остановить СГУ. Если зона запущена как кластер высокой доступности, остановить все серверы и выбрать один из них, чтобы добавить зону в федерацию. Поместить этот сервер в соло-режим, установив SERVER_ID в значение «-1» в файле ***/etc/one/oned.conf***.
3. **Master, Slave**: повторить процедуру, описанную в шаге 2, чтобы добавить новую зону.
4. **Slave**: создать любого пользователя, группу или ЦОД, которые необходимо сохранить в федеративной среде.

Теперь зона готова к использованию. Если необходимо добавить больше серверов высокой доступности, следует повторить процедуру.

3.2.6 Создание и управление кластерами

Кластер – группа компьютеров, объединённых высокоскоростными каналами связи, представляющая с точки зрения пользователя единый аппаратный ресурс.

Раздел СГУ **Инфраструктура** → **Кластеры** позволяет создать необходимое количество серверных кластеров и распределить между ними

зарегистрированные в системе узлы, в зависимости от исполняемых на них задач и их функционального назначения (Рисунок 17).

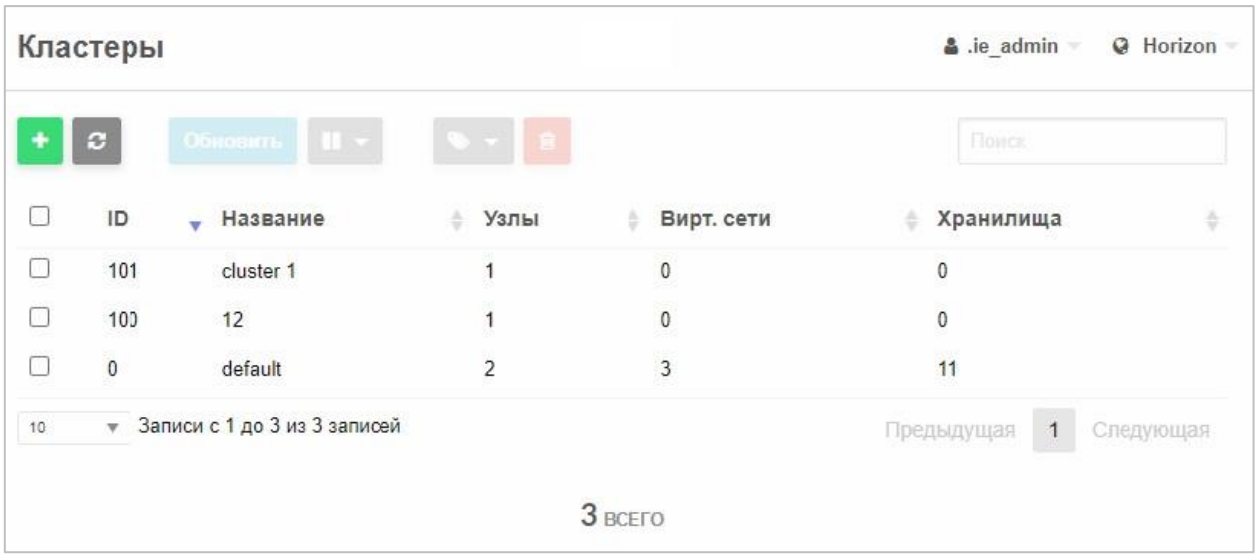


Рисунок 17 – Раздел «Кластеры»

Для создания кластера:

1. Нажать кнопку  в верхнем левом углу.

   Откроется окно **Создать кластер** (Рисунок 18).
2. Ввести имя кластера в поле **Название**, выбрать узлы (не менее двух) для подсоединения к кластеру (Рисунок 18).

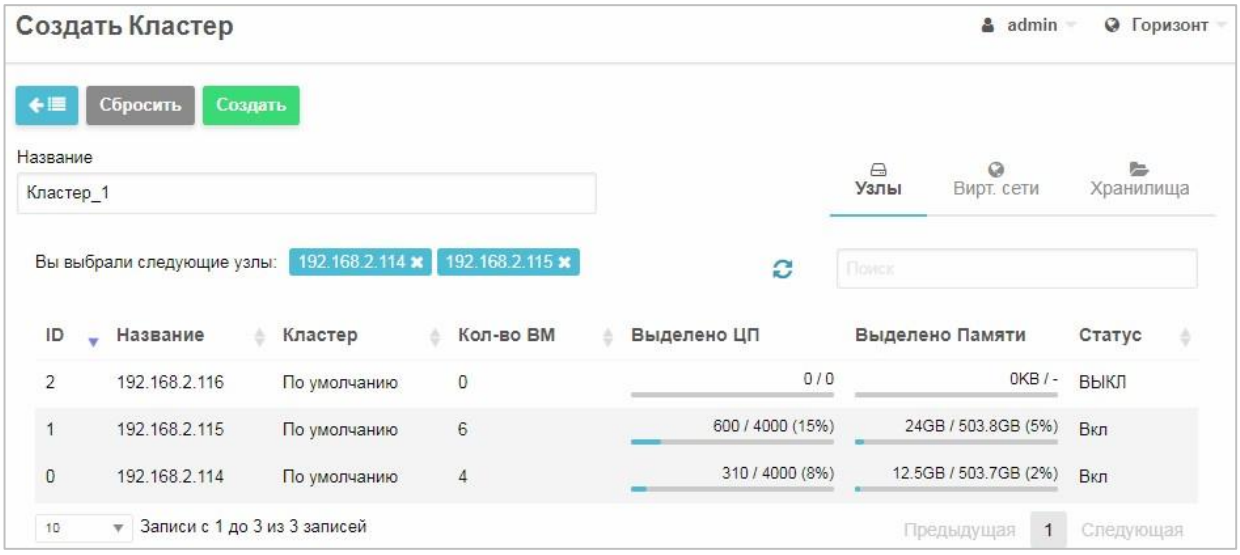


Рисунок 18 – Создание кластера. Выбор узлов

3. На вкладке **Вирт. сети** выбрать виртуальные сети (Рисунок 19).

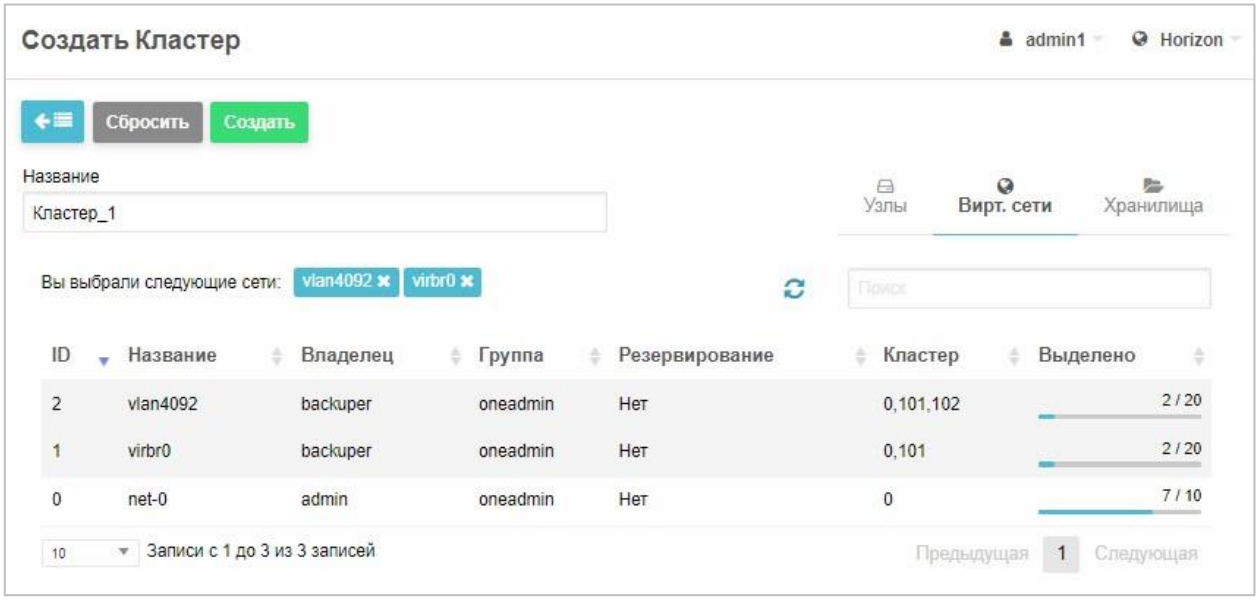


Рисунок 19 – Создание кластера. Выбор виртуальных сетей

4. На вкладке **Хранилища** выбрать хранилища (Рисунок 20).

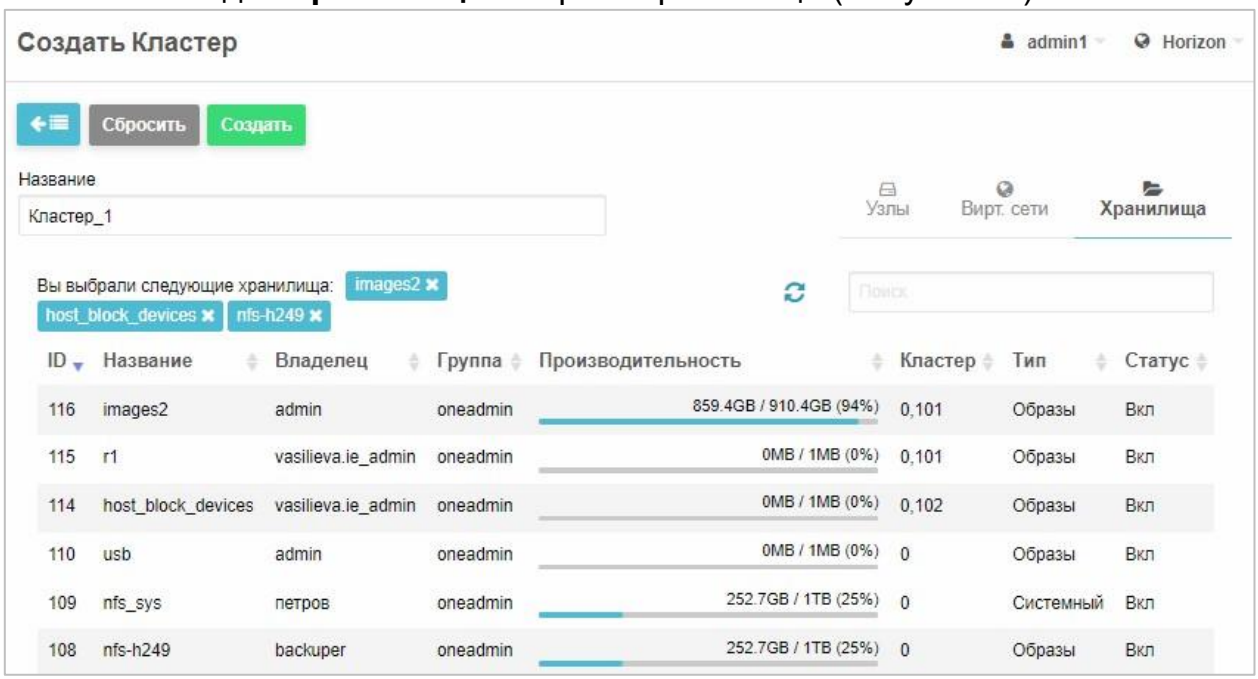


Рисунок 20 – Создание кластера. Выбор хранилищ

5. Нажать кнопку Создать.

Созданный кластер будет добавлен в список.

Для изменения конфигурации кластера: 1.

Нажать на кластер в таблице (Рисунок 17).

Откроется окно **Кластер**, содержащее информацию о выбранном кластере (Рисунок 21).

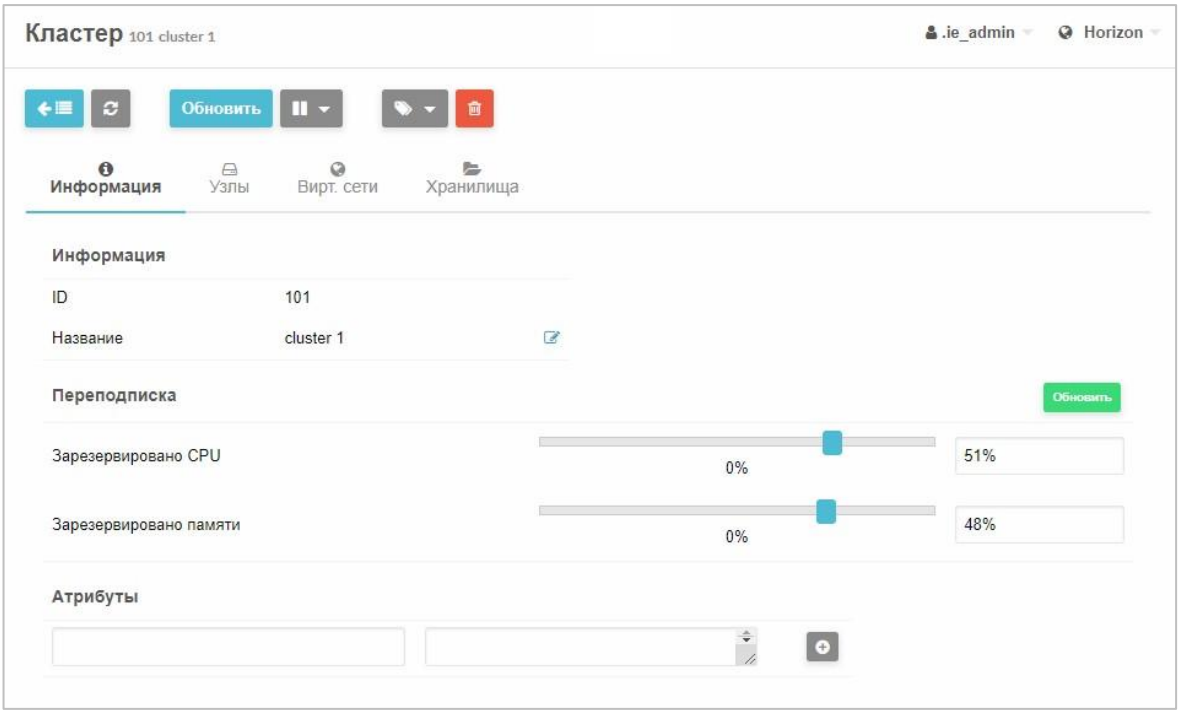


Рисунок 21 – Окно «Кластер»

2. Нажать кнопку Обновить.

Откроется окно **Обновить кластер** (Рисунок 22).

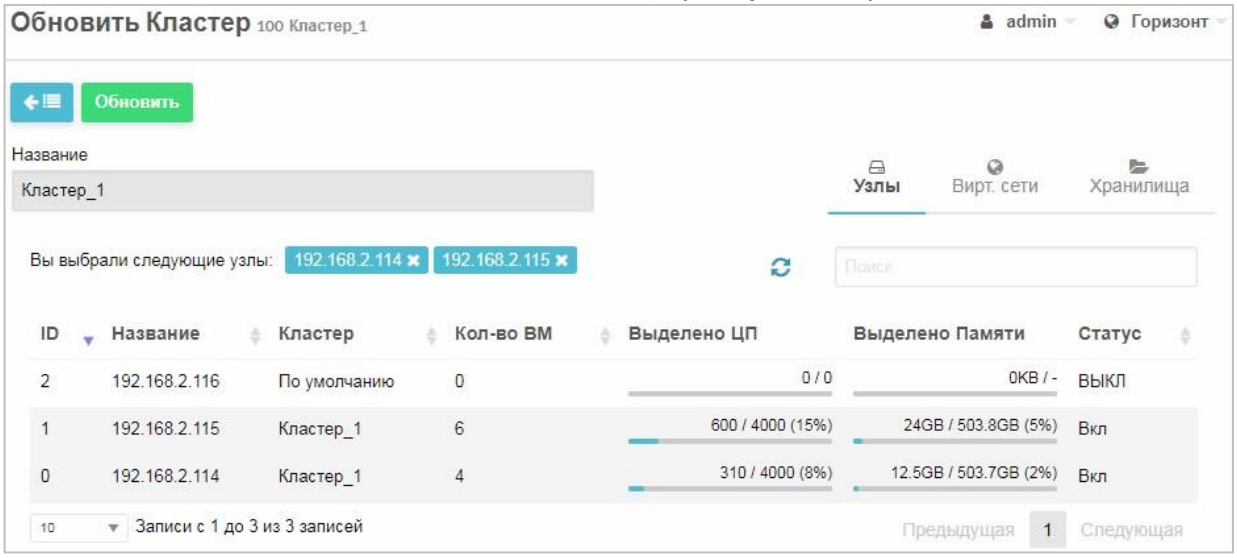


Рисунок 22 – Обновление конфигурации кластера.

Подключение/отключение узлов

3. На вкладке **Узлы** подключить дополнительные хосты нажатием на соответствующую строку в таблице.

   Названия подключаемых узлов отобразятся справа от надписи **Вы выбрали следующие узлы** и будут выделены синим цветом (Рисунок 22).

   Для удаления узла нажать на крестик справа от его названия ( ).

4. На вкладке **Виртуальные сети** добавить/удалить виртуальные сети (Рисунок 23) по аналогии с подключением/отключением узлов на шаге 3.

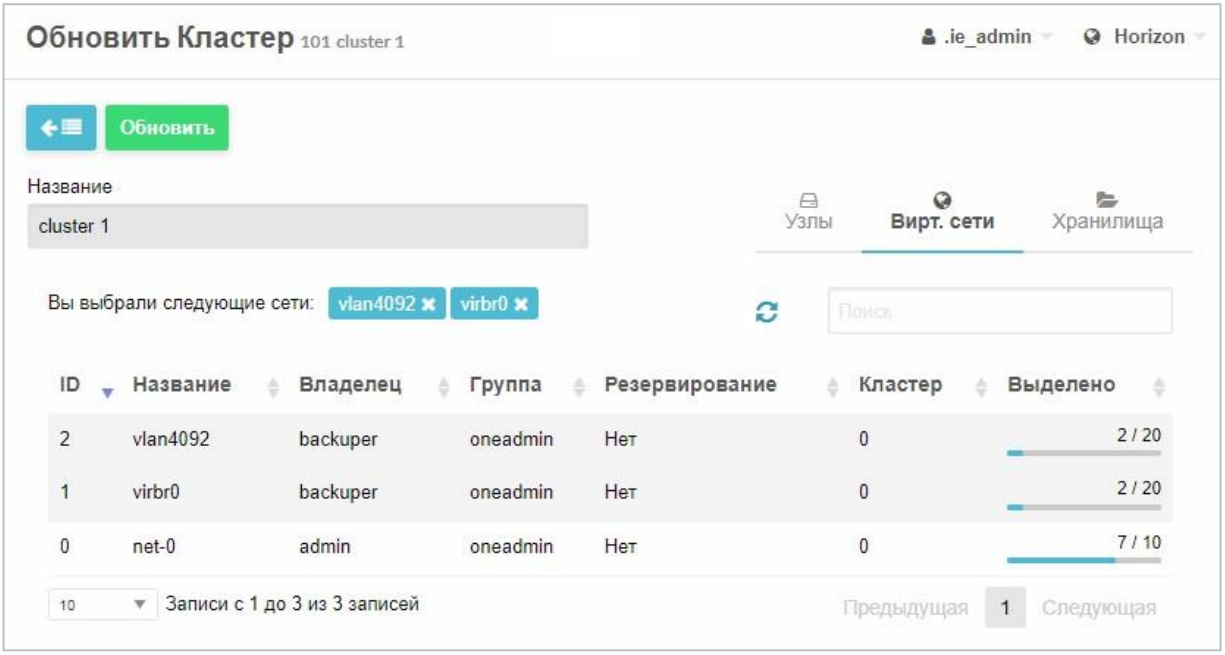


Рисунок 23 – Подключение/отключение виртуальных сетей

5. На вкладке **Хранилища** добавить/удалить хранилища (Рисунок 24) по аналогии с подключением/отключением узлов на шаге 3.

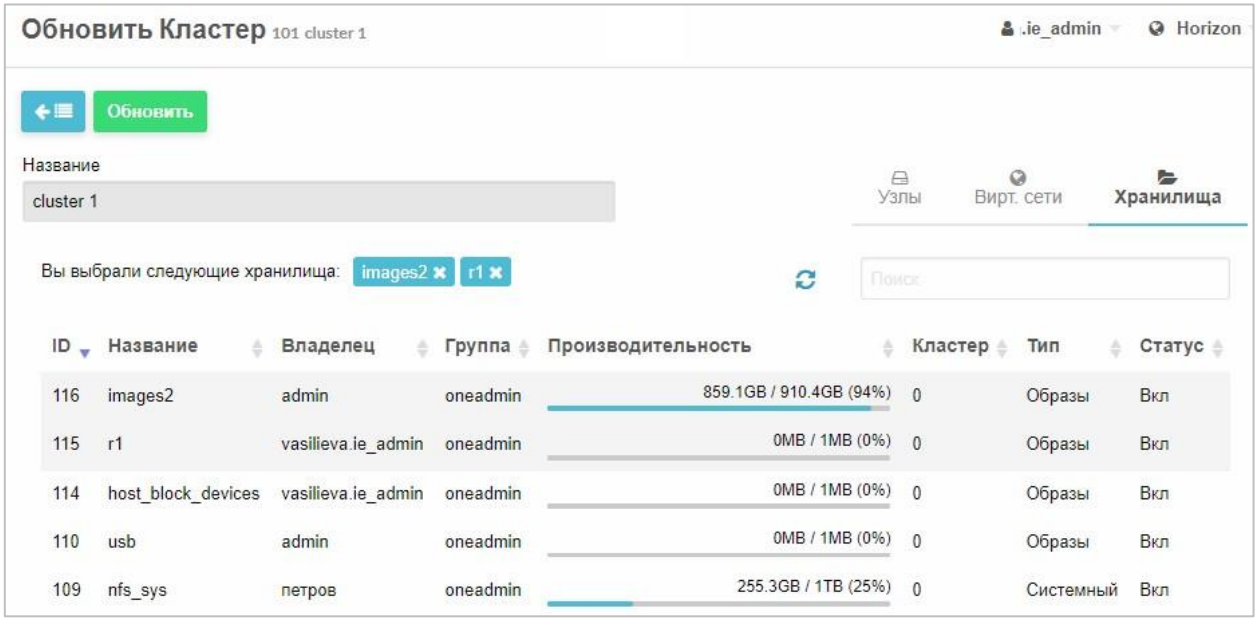


Рисунок 24 – Подключение/отключение хранилищ

6. Нажать кнопку Обновить.

Для удаления кластера:

1. Выбрать кластер.
2. Нажать кнопку Обновить (Рисунок 21).
3. Удалить из него все ресурсы на вкладках Узлы, Вирт. сети, Хранилища нажатием кнопки справа от ресурса.
4. Нажать кнопку Обновить.

   Откроется список кластеров.
5. Выделить данный кластер, установив флаг слева от его названия.
6. Нажать кнопку .
7. В открывшемся окне подтвердить удаление нажатием кнопки OK (Рисунок 25).

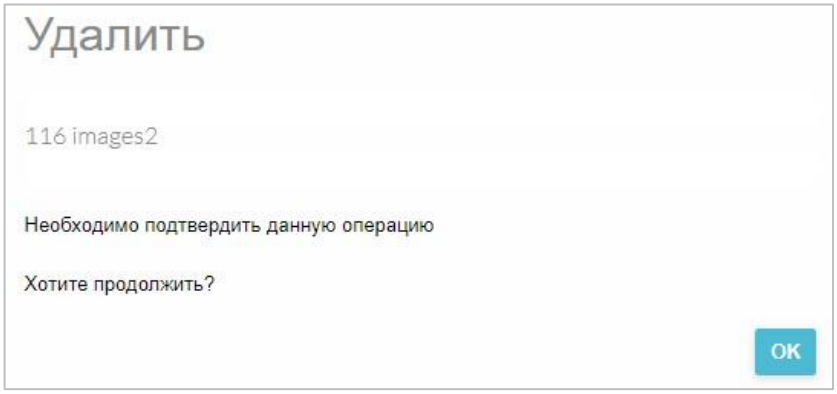


Рисунок 25 – Удаление кластера

***Внимание**! При попытке удалить кластер, содержащий виртуальные ресурсы (узлы, сети, и/или хранилища) появится сообщение об ошибке (Рисунок 26).*

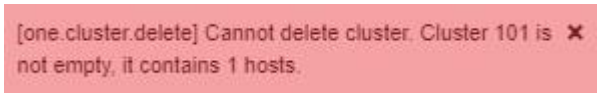


Рисунок 26 – Ошибка удаления кластера

3.2.7 Создание и управление узлами (серверами виртуализации)

Для добавления сервера виртуализации (узла):

1. Зайти в раздел **Инфраструктура** → **Узлы**.

   Откроется окно **Узлы** (Рисунок 27).

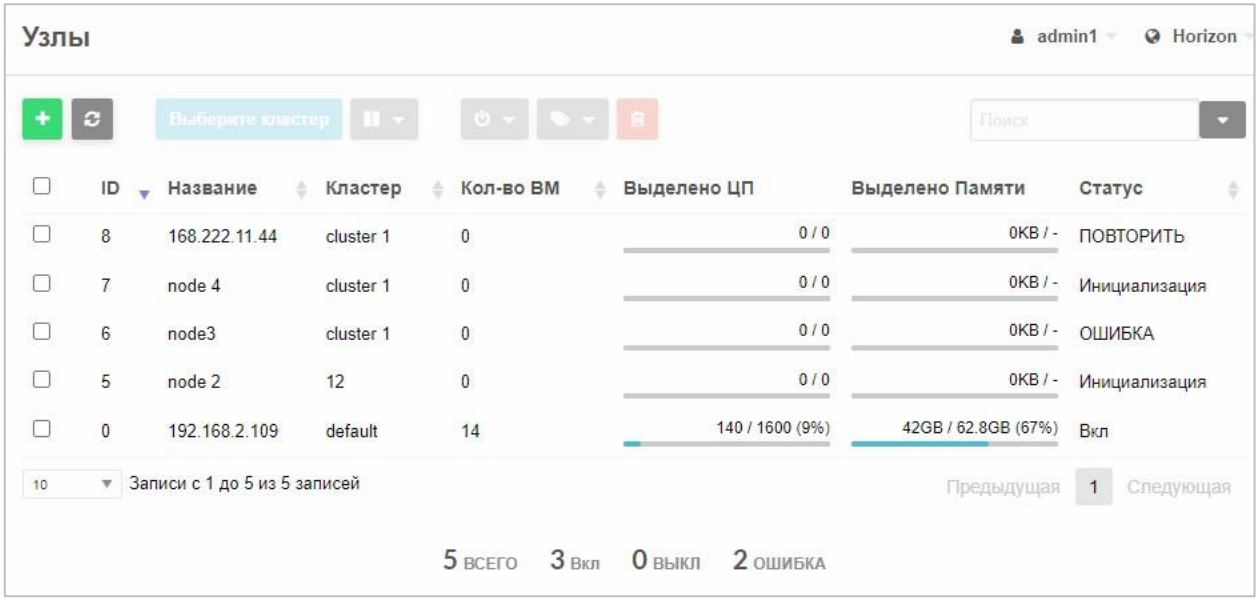


Рисунок 27 – Раздел «Инфраструктура → Узлы»

2. Нажать кнопку  в верхнем левом углу.

   На экране появится окно регистрации нового узла (Рисунок 28).

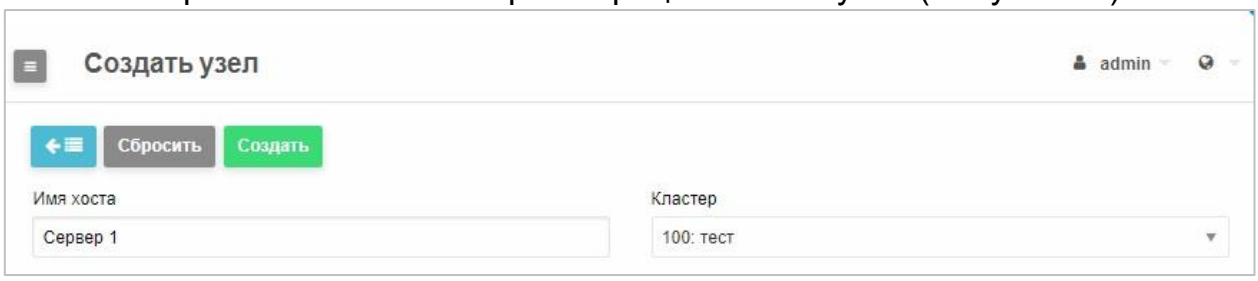


Рисунок 28 – Создание узла

3. В поле **Кластер** выбрать наименование кластера, к которому будет подключаться новый узел. Узел по умолчанию добавляется как **0:default**.
4. В поле **Имя хоста** ввести IP-адрес или доменное имя подключаемого узла (см. п. 3.1.4.1).
5. Нажать кнопку **Создать**.

   Новый узел добавится в список со статусом **Инициализация**.

Начнется процесс инициализации нового узла в зоне управления и размещение его в выбранном кластере.

Система запрашивает о ресурсах на данном узле.

Для того чтобы узнать, инициализировался ли узел, выбрать узел, установив флаг слева, и нажать кнопку **Обновить**. Если узел инициализировался, его статус изменится на **вкл**.

Для смены кластера узла:

1. Выбрать узел, установив флаг слева (Рисунок 29).

   Станет доступна кнопка 

.

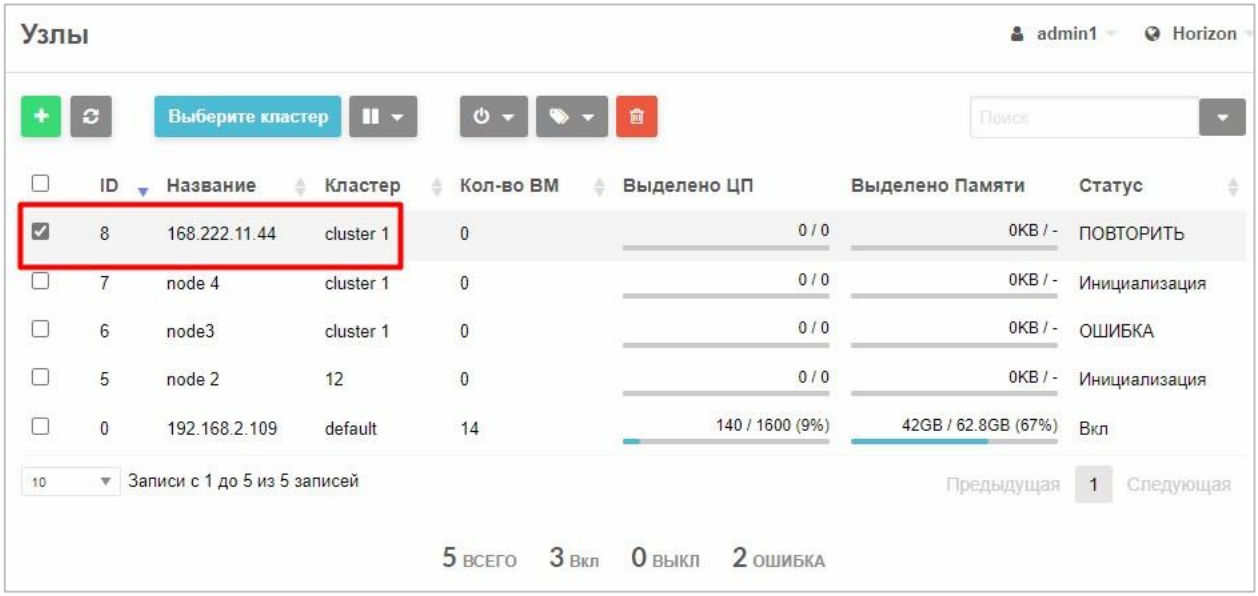


Рисунок 29 – Выбор узла из списка

2. Нажать кнопку **Выберите кластер**.

   Откроется окно **Выберите кластер** (Рисунок 30).

3. Выбрать кластер нажатием и нажать кнопку **OK** в нижнем правом угла.

   В колонке **Кластер** таблицы **Узлы** отобразится новый кластер.

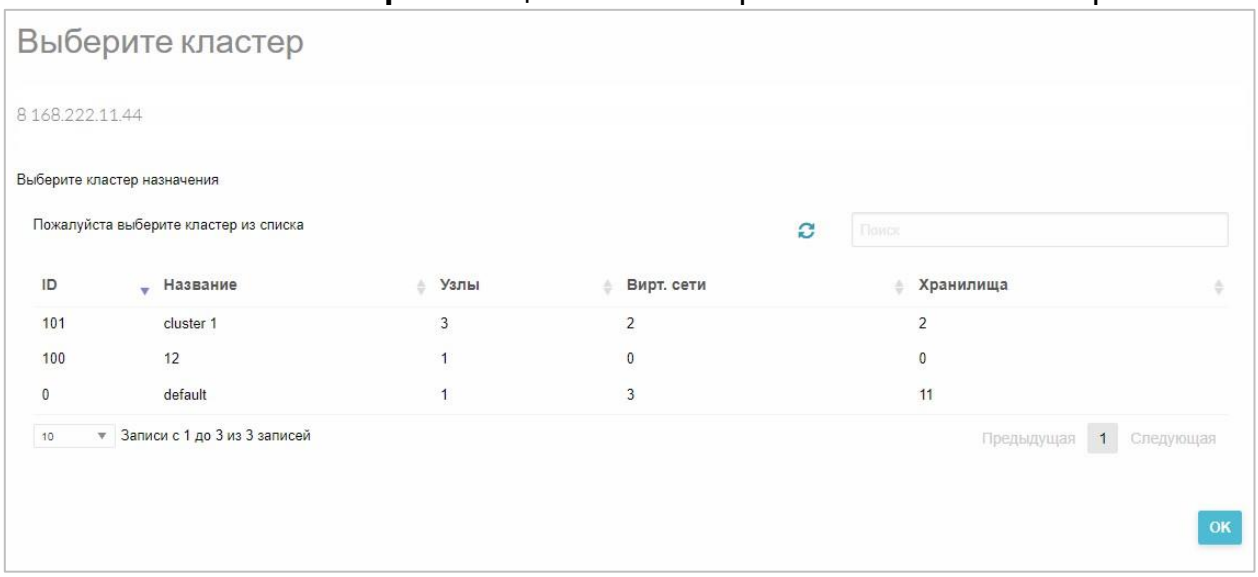


Рисунок 30 – Выбор кластера

3.2.8 Создание и управление хранилищами

Для создания и управления хранилищами следует зайти в СГУ **Хранилище** → **Хранилища.** Откроется окно, в котором в виде списка представлены хранилища, уже существующие в системе (Рисунок 31).

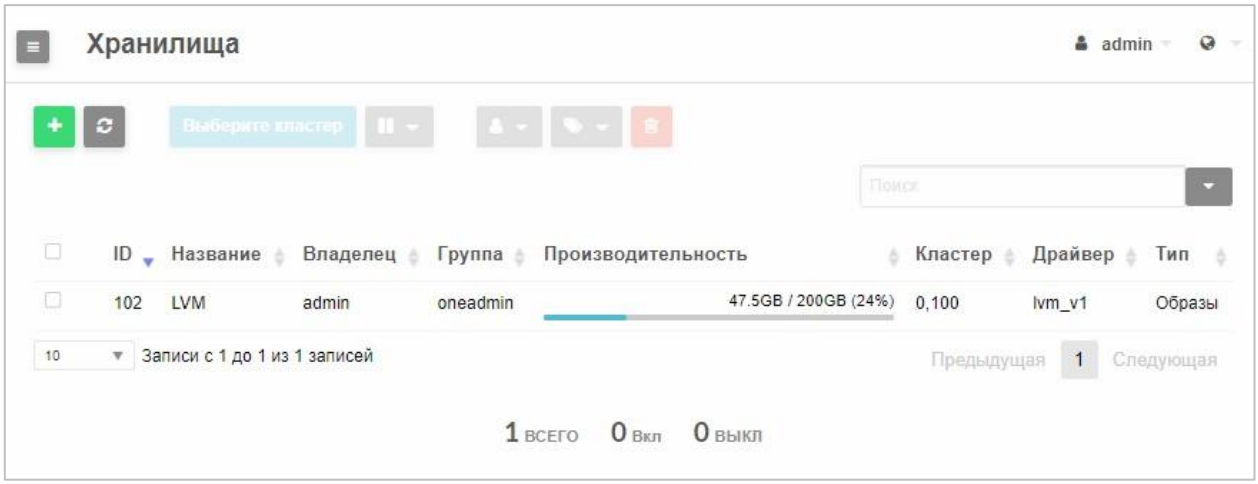


Рисунок 31 – Менеджер хранилищ

Для управления хранилищами предназначено меню, активирующееся при выборе флагом одного или нескольких хранилищ из списка (Таблица 4).

Таблица 4 – Команды меню управления хранилищами

Опция	Функция	Описание
+	Создание нового хранилища (всегда активна)	Открывается страница создания нового хранилища
	Обновление текущей страницы (активна всегда)	После внесения каких-либо изменений в работу хранилища необходимо выполнить обновление страницы, чтобы увидеть изменения.
Выберите кластер	Открывается окно со списком кластеров	Позволяет выбрать кластер, в который будет входить хранилище
Опция	**Функция**	**Описание**
	Выпадающее меню:	
	Сменить владельца	Позволяет сменить пользователя хранилища

	Сменить группу	Позволяет сменить группу пользователей хранилища
	Редактировать метку	Для удобства управления ресурсом в системе группового управления предусмотрены метки, которые позволяют группировать и выводить списки ресурсов по их типу или функциональному предназначению. *Например: БД бухгалтерии*
	Удаление	Удаление хранилища из системы

Для создания нового хранилища:

1. Нажать кнопку  в управляющем меню (Рисунок 31).

   Откроется окно **Создать хранилище** (Рисунок 32).

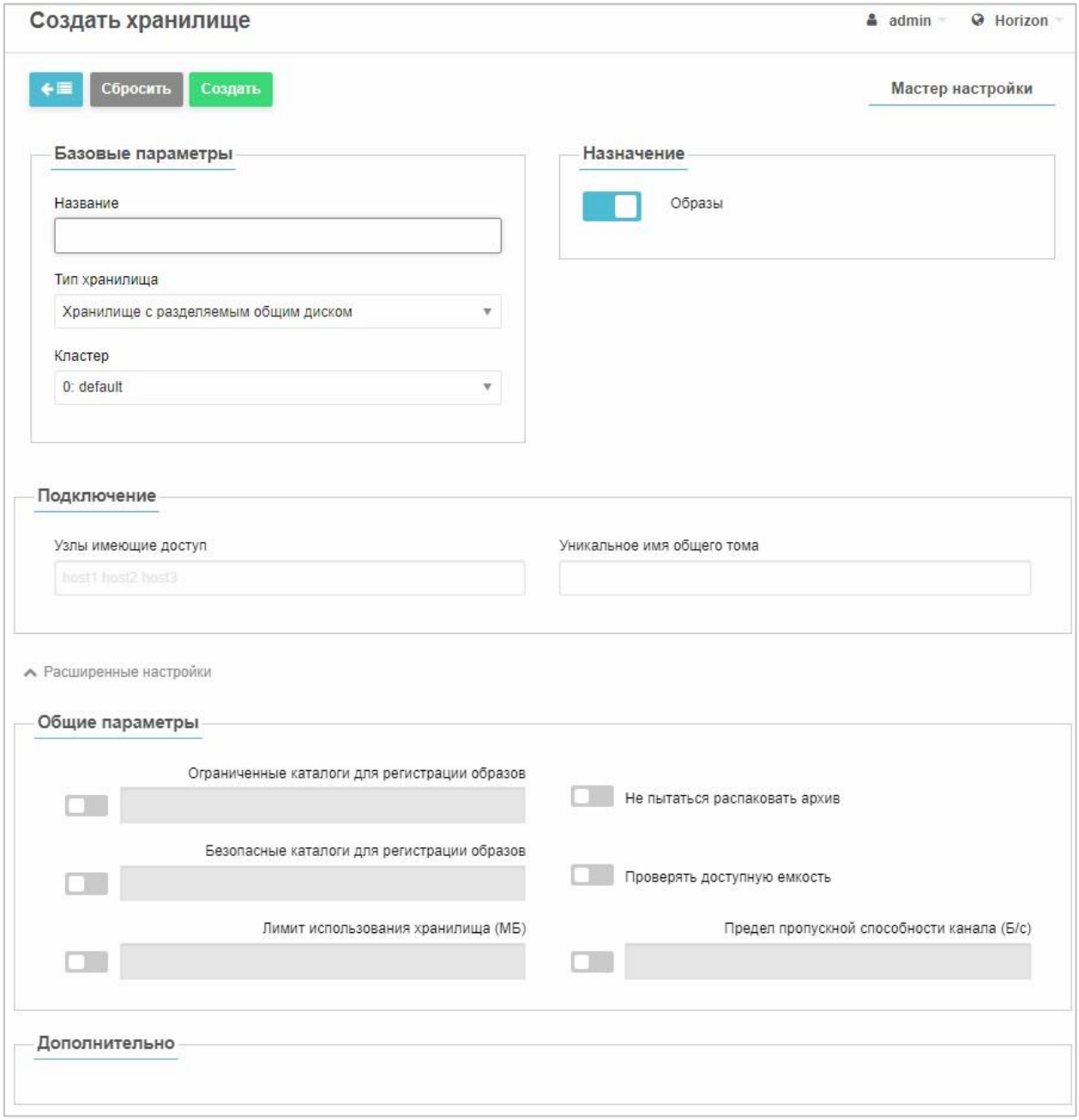


Рисунок 32 – Создание хранилища

2. В области **Базовые параметры** заполнить поля:

– ввести название хранилища;

– выбрать кластер, в котором оно будет расположено. – из раскрывающегося списка **Тип хранилища** выбрать тип хранилища (Рисунок 33). Атрибуты хранилища зависят от выбранного типа хранилища.

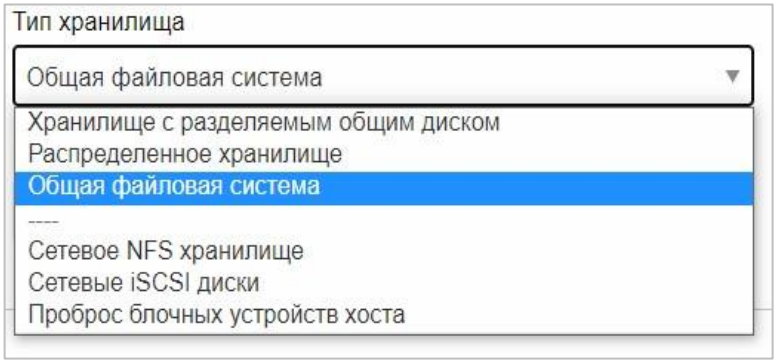


Рисунок 33 – Протоколы для подключения хранилища

3. В области **Подключения** указать, какие хосты имеют доступ к данному хранилищу.
4. Поля области **Подключения** зависят от выбранного типа хранилища.
5. После заполнения всех необходимых полей нажать кнопку **Создать**. Новое хранилище появится в списке.
6. При необходимости, установить расширенные настройки создаваемого хранилища. Данные настройки зависят от типа выбранного хранилища. (Рисунок 34).

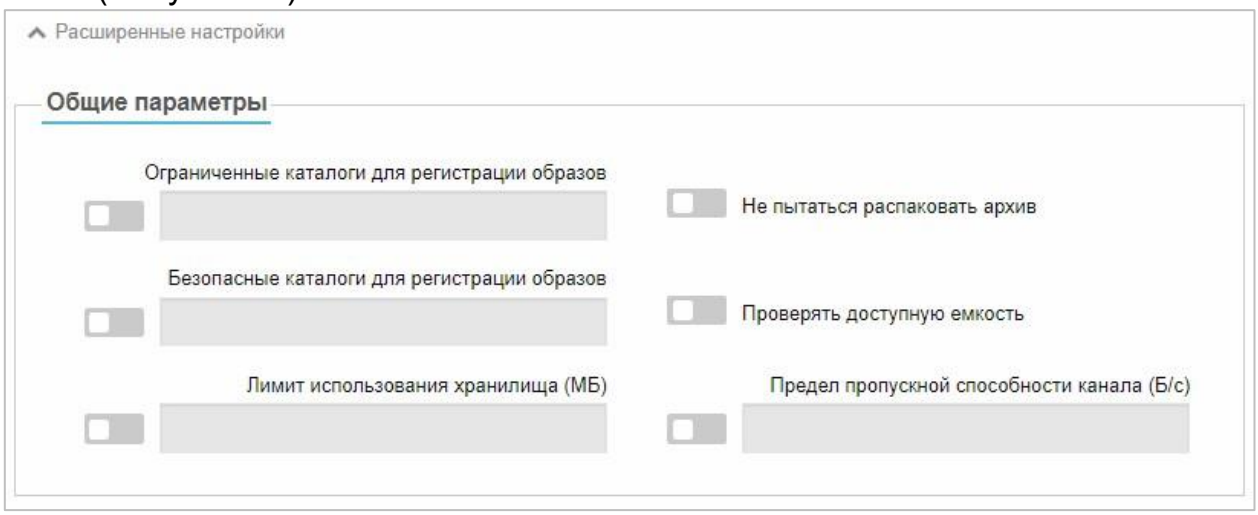


Рисунок 34 – Расширенные настройки хранилища с разделяемым общим диском

3.2.8.1.1 iSCSI хранилище

Для подключения iSCSI хранилища:

1. В разделе **Хранилища** → **Хранилище** нажать кнопку  в управляющем меню (Рисунок 31).

   Откроется окно **Создать хранилище** (Рисунок 32)
2. Из раскрывающегося списка **Тип хранилища** выбрать тип **Сетевые iSCSI диски** (Рисунок 33).
3. Заполнить поля, как показано на рисунке ниже (Рисунок 35):

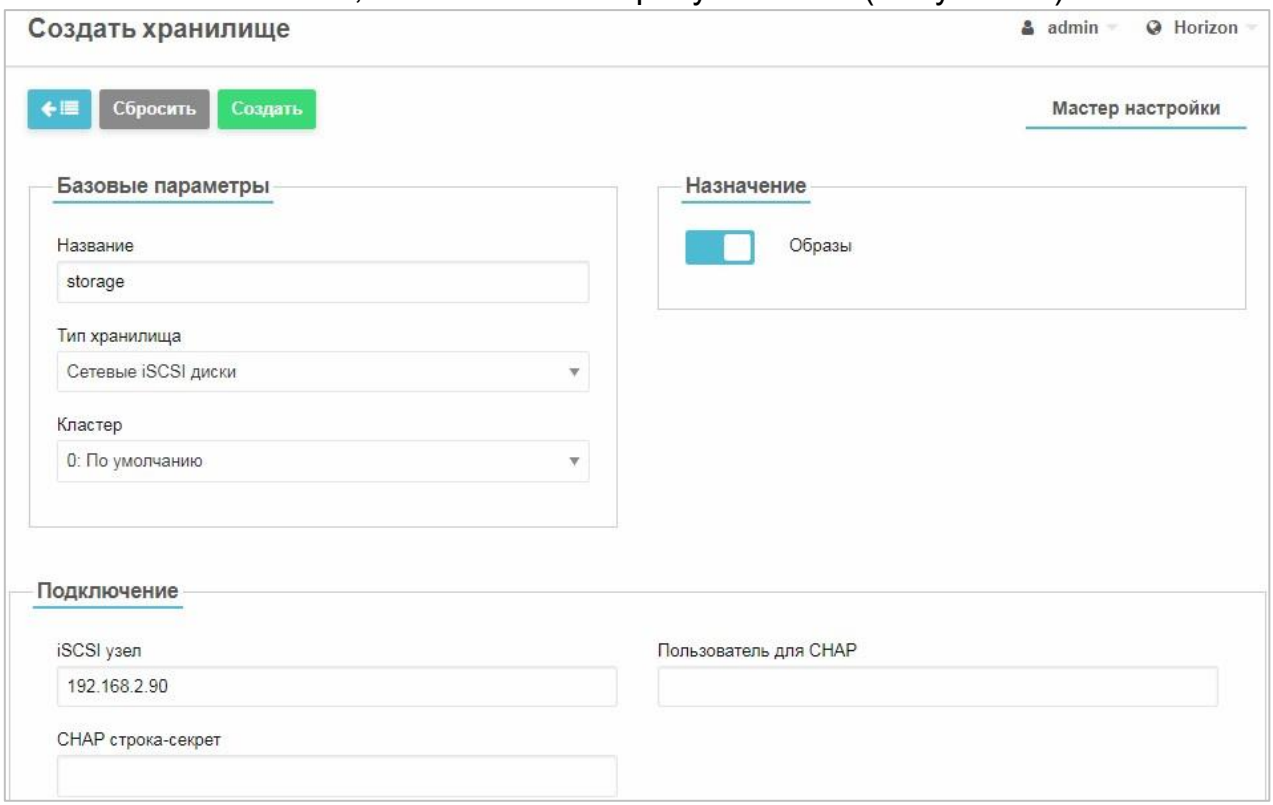


Рисунок 35 – iSCSI хранилище

- в поле **Название** ввести имя хранилища;
- в поле Тип хранилища оставить значение *Сетевые iSCSI диски*;
- в поле **Кластер** выбрать из списка кластер, в котором будет размещено хранилище;
- в поле **iSCSI узел** ввести IP-адрес iSCSI хранилища;
- если будет использоваться аутентификация CHAP, то заполнить поля **CHAP строка-секрет** и **CHAP имя пользователя**.

4. Нажать кнопку **Создать**.

   Новое хранилище появится в списке.

5. Перейти в раздел СГУ **Хранилище** → **Образы** и создать образ хранилища.

   Для создания образа iSCSI хранилища:

   a. Нажать кнопку  в управляющем меню (Рисунок 36).

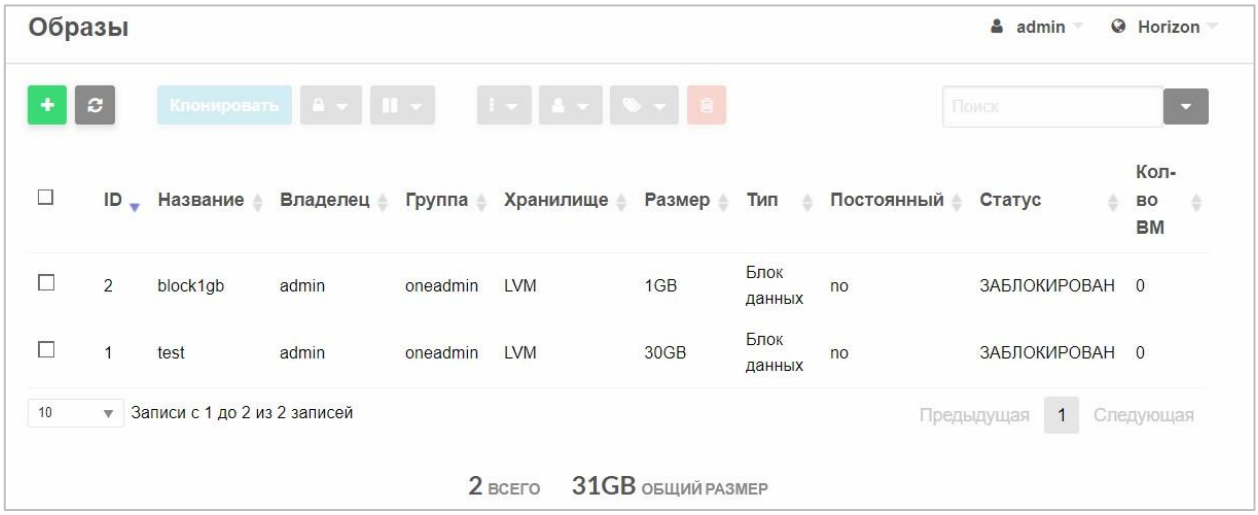


Рисунок 36 – Раздел «Хранилище» → «Образы»

6. В открывшемся окне (Рисунок 37) заполнить поля:

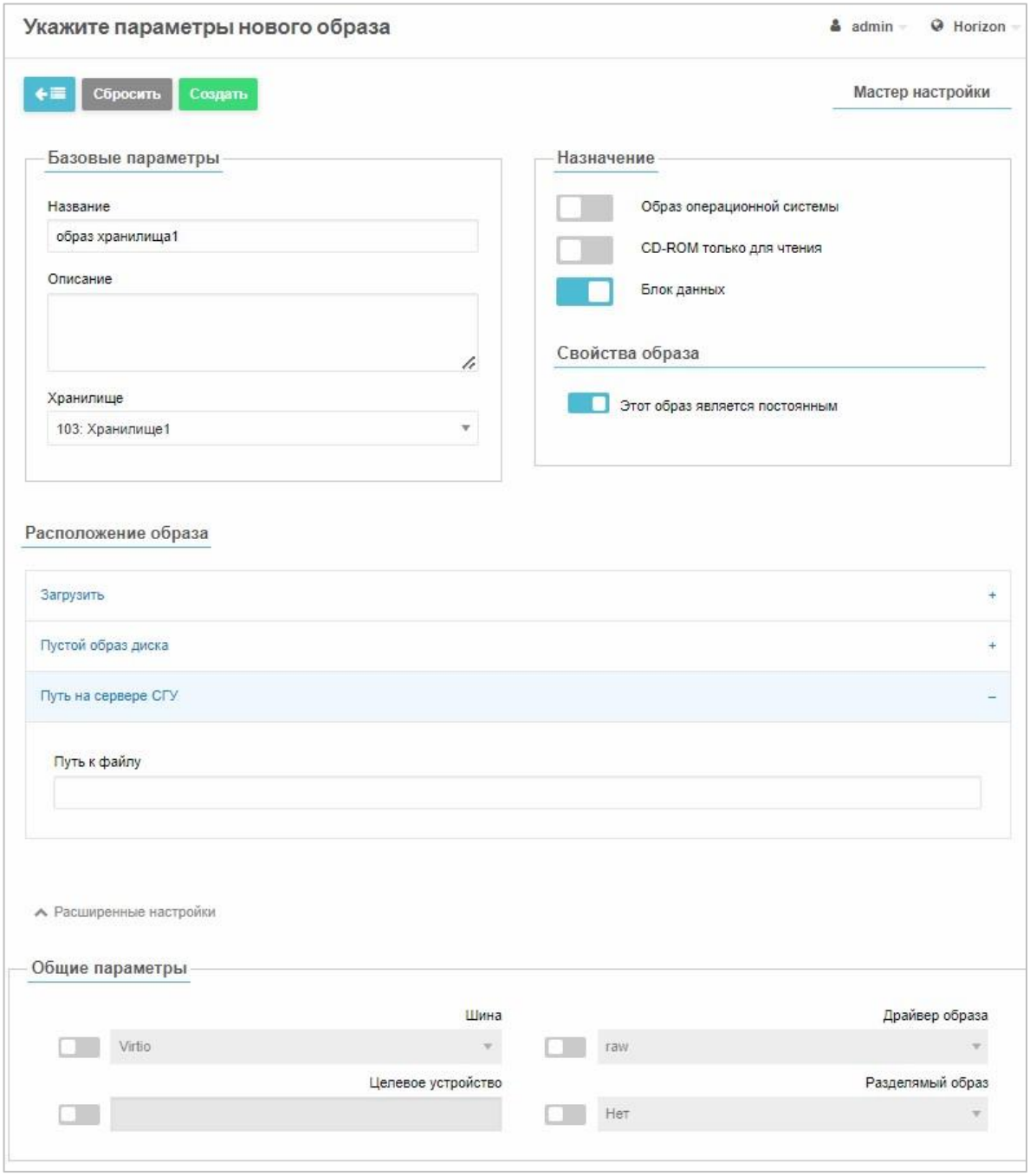


Рисунок 37 – Установка параметров нового образа

- название образа;
- передвинуть переключатель **Блок данных** вправо;
- в поле **Хранилище** выбрать имя хранилища типа iSCSI, созданное ранее;
- выбрать пункт **Путь на сервере СГУ** и в поле **Путь к файлу** указать путь к LUN на общем хранилище (Рисунок 37).

- при необходимости, настроить **Общие параметры**.

7. Нажать кнопку **Создать**.

   Новый образ появится в списке.

3.2.8.1.2 NFS хранилище

Для создания NFS хранилища:

1. В разделе **Хранилища** → **Хранилище** нажать кнопку  в управляющем меню (Рисунок 31).
2. В открывшемся окне **Создать хранилище** (Рисунок 32) выбрать тип **Сетевые NFS хранилище**.
3. Заполнить поля (Рисунок 38).

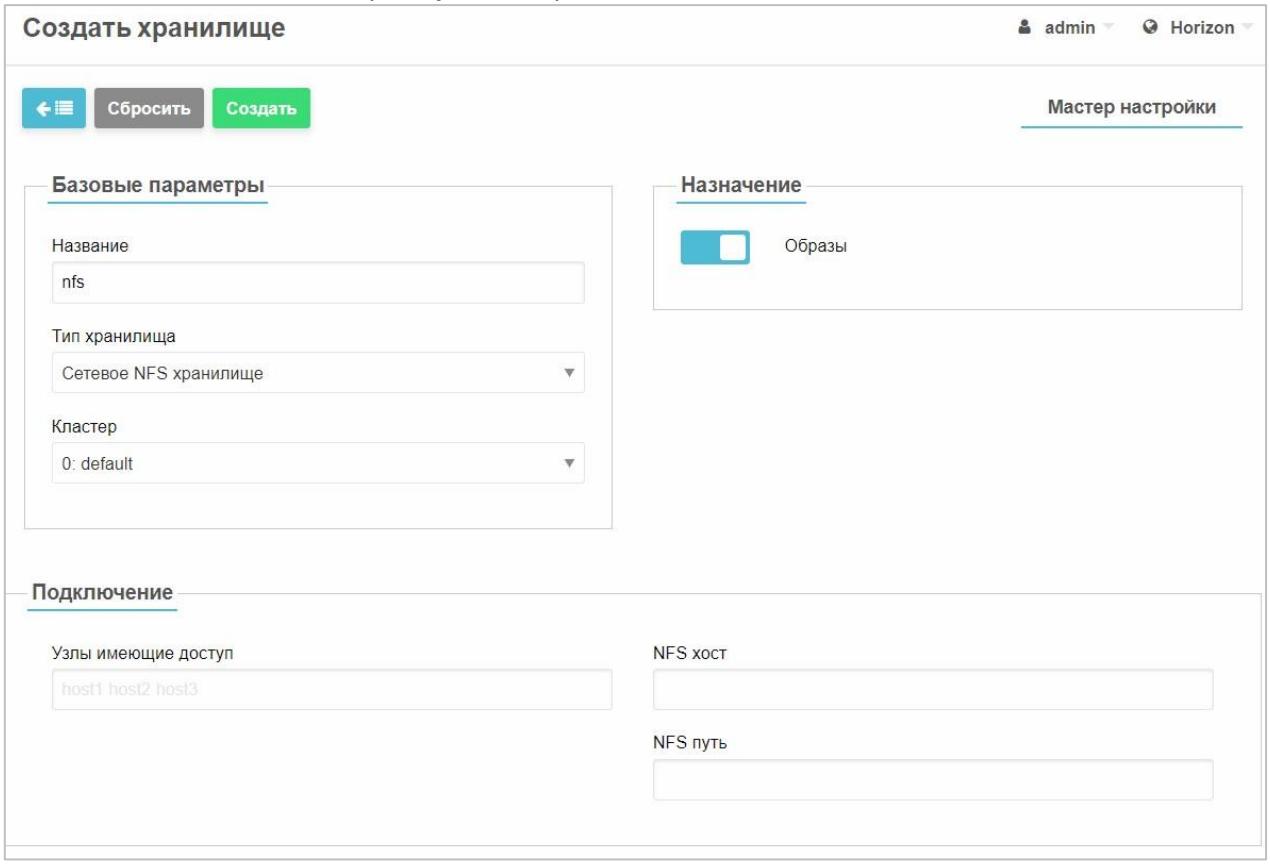


Рисунок 38 – Создание хранилища

– в поле **Название** ввести имя хранилища;
– из раскрывающегося списка **Тип хранилища** оставить значение **Сетевое NFS хранилище**;

- в поле **Кластер** выбрать из списка кластер, в котором будет размещено хранилище;
- в поле **Узлы имеющие доступ** ввести адрес серверов виртуализации, для которых доступно создаваемое хранилище. Поле обязательно для заполнения при создании хранилища для размещения образов ВМ, входящих в кластер высокой доступности. В этом случае необходимо через пробел ввести адреса всех серверов, входящих в кластер высокой доступности;
- в поле **NFS хост** ввести IP-адрес узла;
- в поле **NFS путь** указать директорию на общем хранилище для хранения файлов.

4. Нажать кнопку **Создать**.

   Новое хранилище появится в списке.

3.2.8.1.3 Распределенное хранилище

Перед подключением распределенного хранилища к СГУ необходимо произвести предварительные настройки на сервере виртуализации:

1. Убедиться в наличии директории ***etc/ceph*** на каждом сервере виртуализации. При её отсутствии создать командой в консоли:

```
$ mkdir /etc/ceph
```

2. Перейти в консоль кластера Ceph (на узлы, где развернуто хранилище) и произвести следующие настройки от имени суперпользователя: а. Создать пул для хранилищ данных СГУ командой в консоли:

```
$ ceph osd pool create one 128
```

   где one – название обязательное, 128 – параметр хранилища (количество плэйсмент групп для пула, в котором будут храниться образы).

б. Определить пользователя Ceph для доступа к пулу хранилища данных, который также будет использоваться службой libvirt для доступа к образам дисков ВМ:

```
$ ceph auth get-or-create client.libvirt mon 'profile rbd'
osd 'profile rbd pool=one'
```

в. Получить копию ключа этого пользователя:

```
$ ceph auth get client.libvirt > ceph.client.libvirt.keyring
$ ceph auth get-key client.libvirt | tee client.libvirt.key
$ ceph auth get client.libvirt -o ceph.client.libvirt.keyring
```

г. Скопировать файлы конфигурации хранилища на гипервизоры

```
$ scp /etc/ceph/ceph.conf <имя_сервера>:/etc/ceph
$ scp ceph.client.libvirt.keyring <имя_сервера>:/etc/ceph
```

где **<*имя_сервера*>** - имя или IP-адрес сервера виртуализации.

д. Скопировать файл ключа на узел с СГУ в домашний каталог пользователя oneadmin командой (пароль пользователя oneadmin по умолчанию – oneadmin):

```
$ scp client.libvirt.key oneadmin@<имя_сервера_СГУ>:
```

3. На узле с СГУ ввести в консоли:

```
cat > secret.xml <<EOF
<secret ephemeral='no' private='no'>
  <uuid>$(uuidgen) </uuid>
  <usage type='ceph'>
          <name>client.libvirt secret</name>
  </usage>
</secret> EOF
```

4. Войти в режим работы из-под пользователя oneadmin, набрав команду:

```
$ su oneadmin
```

5. На все серверы виртуализации скопировать файлы secret.xml и client.libvirt.key в домашний каталог пользователя oneadmin:

```
$ scp secret.xml oneadmin@<имя_сервера>:
$ scp client.libvirt.key oneadmin@<имя_сервера>:
```

где **<*имя_сервера*>** - имя или IP-адрес сервера виртуализации.

6. Перейти на сервер виртуализации и на каждом из них выполнить следующую команду из-под пользователя oneadmin:

```
virsh -c qemu:///system secret-define secret.xml
```

а. Скопировать UUID из файла secret.xml и ввести команду:

```
virsh -c qemu:///system secret-set-value --secret <UUID> -
base64 $(cat cli-ent.libvirt.key)
```

б. Удалить файл ключей командой:

```
rm client.libvirt.key
```

Для создания распределенного хранилища:

1. В разделе **Хранилища** → **Хранилище** нажать кнопку  в управляющем меню (Рисунок 31).
2. В открывшемся окне **Создать хранилище** (Рисунок 32) выбрать тип **Распределенное хранилище**.
3. Заполнить поля так, как показано на рисунке ниже (Рисунок 39).

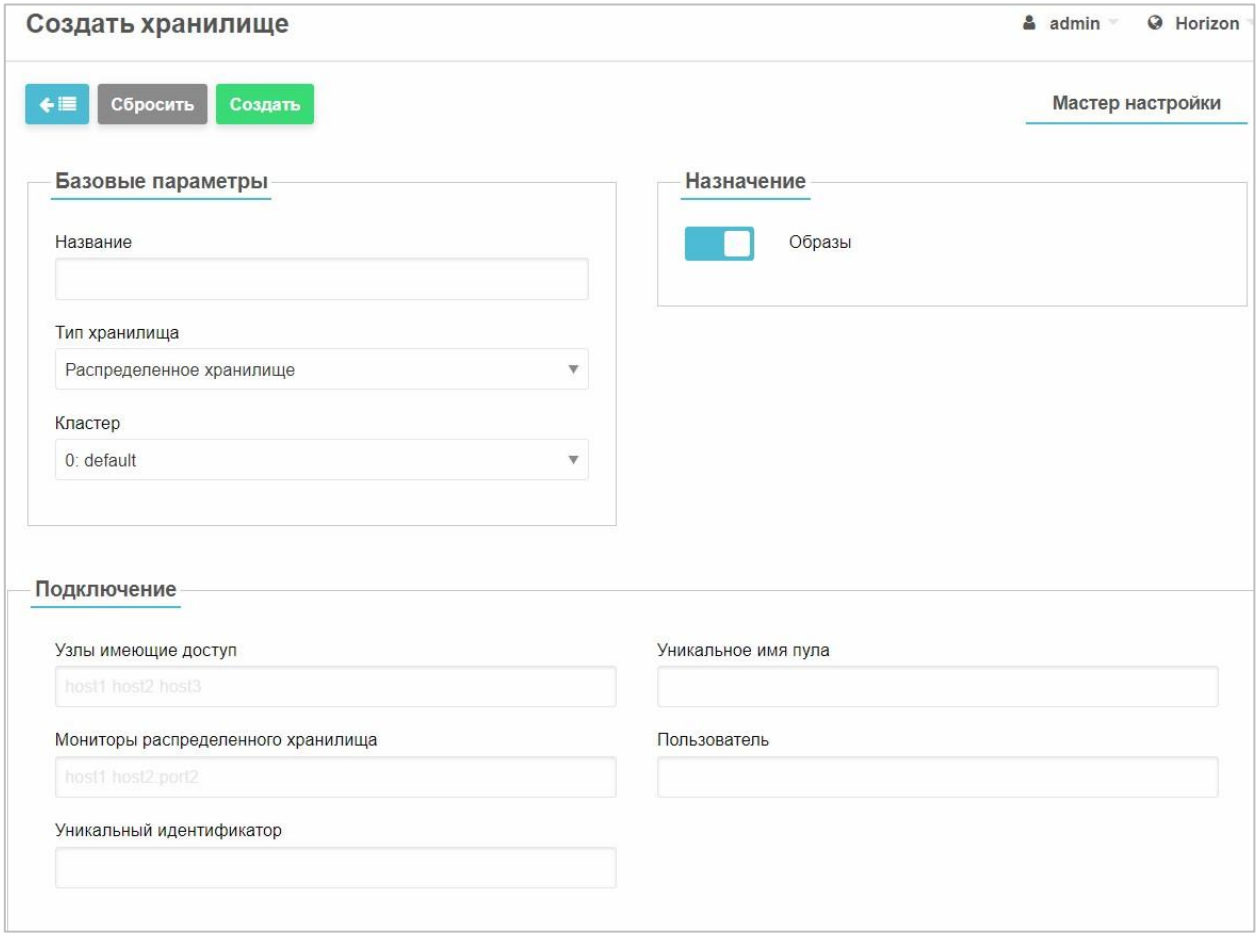


Рисунок 39 – Создание распределенного хранилища. Заполнение полей

- в поле **Название** ввести имя хранилища;
- из раскрывающегося списка **Тип хранилища** выбрать значение **Распределенное хранилище**;
- в поле **Кластер** выбрать из списка кластер, в котором будет размещено хранилище;
- в поле **Узлы имеющие доступ** ввести адреса серверов виртуализации, для которых доступно создаваемое хранилище;
- в поле **Уникальное имя пула** указать название пула (one);
- в поле **Мониторы распределенного хранилища** перечислить список мониторов, разделенных пробелами, с указанием порта 6789;
- в поле **Пользователь** ввести имя пользователя libvirt, созданного на узле;

– в поле **Уникальный идентификатор** ввести UUID из файла «secret.xml».

4. Нажать кнопку **Создать**.

   Новое хранилище появится в списке.

5. При необходимости, выполнить расширенные настройки создаваемого хранилища, представленные ниже на рисунке (Рисунок 40).

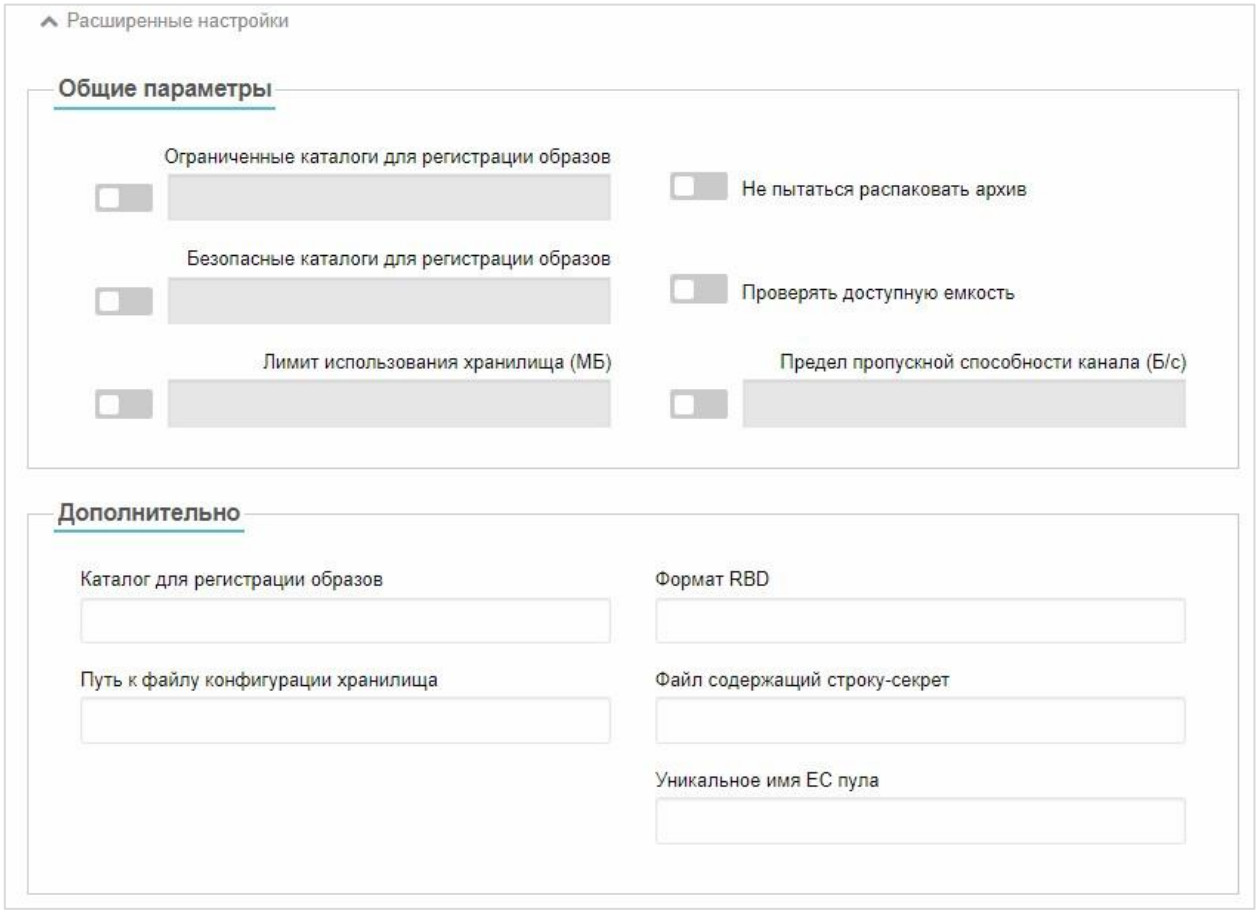


Рисунок 40 – Расширенные настройки распределенного хранилища

3.2.8.1.4 Создание хранилища с пробросом блочных устройств хоста

Для создания хранилища с пробросом блочных устройств хоста:

1. Подключить в терминале внешний топ хранения
2. В разделе **Хранилища** → **Хранилище** нажать кнопку  в управляющем меню (Рисунок 31).

3. В открывшемся окне **Создать хранилище** (Рисунок 32) выбрать тип **Проброс блочных устройств хоста.**
1. Нажать кнопку **Создать**. Новое хранилище появится в списке.
2. Перейти в раздел **Хранилища** → **Образы,** нажать кнопку  в управляющем меню (Рисунок 41).
3. В поле **Хранилище** выбрать имя хранилища с типом проброса блочных устройств хоста, созданное ранее.
4. Выбрать пункт **Путь на сервере СГУ.** Указать путь на сервере СГУ в виде *#/dev/имя_диска*, как он отображается в консоли гипервизора в выводе команды **lsblk.**
5. Нажать кнопку **Создать**.

После того, как диск будет доступен для одной ВМ, им можно пользоваться.

3.2.9 Управление образами виртуальных машин

Образ ВМ – файл, содержащий информацию о конфигурации, настройках и состоянии виртуальной машины, а также хранящиеся в ней программы и данные.

Образы ВМ могут быть операционными системами или дисками с данными, которые используются при создании или в работе виртуальных машин. Эти образы могут использоваться несколькими ВМ одновременно. В системе есть два типа образов ВМ: постоянные и непостоянные.

Постоянный (персистентный, persistent) образ диска – тип виртуального диска, все изменения на котором сохраняются после прекращения работы виртуальной машины.

Непостоянный (неперсистентный, non-persistent) образ диска – тип виртуального диска, при подключении которого в ВМ, создается копия

исходного образа диска. После удаления ВМ все изменения, сделанные на непостоянном диске, будут потеряны. Данный диск удаляется вместе с ВМ.

Различные типы виртуальных дисков могут использоваться, в том числе и для создания *эталонных* («золотых») образов ВМ.

Для создания эталонного образа ВМ:

1. Установить гостевую ОС на диск, являющийся персистентным.
2. Произвести все необходимые настройки внутри ОС.
3. Изменить тип диска на неперсистентный, и затем использовать диск для создания ВМ из эталонного образа.

Для работы с образами необходимо перейти в раздел **Хранилище** → **Образы**, после чего будет доступен список образов (Рисунок 41).

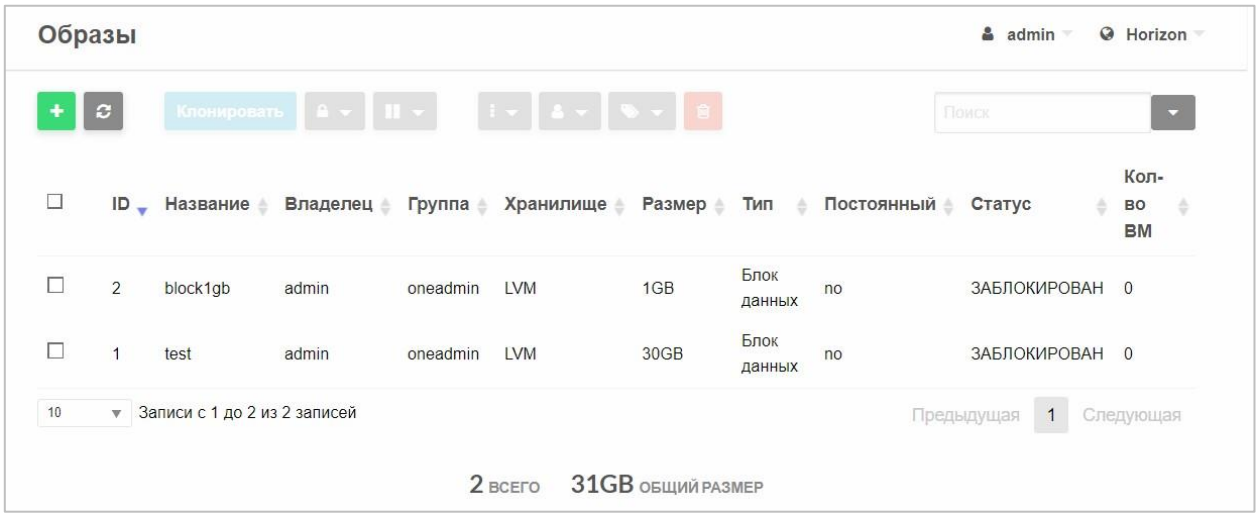


Рисунок 41 – Список образов ВМ

Для управления образами предназначено меню, активирующееся при выборе флагом одного или нескольких образов из списка (Таблица 5).

Таблица 5 – Команды меню управления образами

Опция	Функция	Описание
	Создание нового образа (всегда активна)	Открывается страница создания нового образа
	Обновление текущей страницы (активна всегда)	Обновление страницы, чтобы увидеть изменения

Клонировать	Открывается окно управления клонированием	Позволяет выбрать хранилище для клонированного диска (подробнее см. п. 3.2.9.4)
	Выпадающее меню:	
	Администрирование	Разрешение специальных операций (например, изменение параметров образа). Данные операции должны назначаться только пользователям с ролью администратора
	Управление	Разрешение на работу с образом, при котором

Опция	Функция	Описание
		операции могут изменять ресурс (например, изменение атрибута образа виртуального диска на «постоянный»)
	Пользование	Разрешение на работу с образом, при котором операции не изменяют ресурс
	Unlock	Разблокирование всех возможных операций с ресурсом
		
	Выпадающее меню:	
	Включить	Образ активен для СГУ. Статус образа изменяется на «Вкл»
	Отключить	Образ отключается от СГУ. Статус образа изменяется на «Выкл»
	Сделать постоянным	Образ становится постоянным (персистентным)
	Сделать непостоянным	Образ становится непостоянным (неперсистентным)

	Выпадающее меню:	
	Сменить владельца	Позволяет сменить пользователя образа
	Сменить группу	Позволяет сменить группу пользователей образа
	Добавить метку	Метки позволяют группировать и выводить списки образов по их типу или функциональному предназначению.
Опция	**Функция**	**Описание**
	Удаление	Удаление образа из системы

3.2.9.1 Создание установочного образа диска виртуальной машины

Для создания установочного образа диска гостевой ОС:

1. Перейти в раздел **Хранилище** → **Образы.**
2. Нажать кнопку  .

Откроется окно установки параметров нового образа (Рисунок 42).

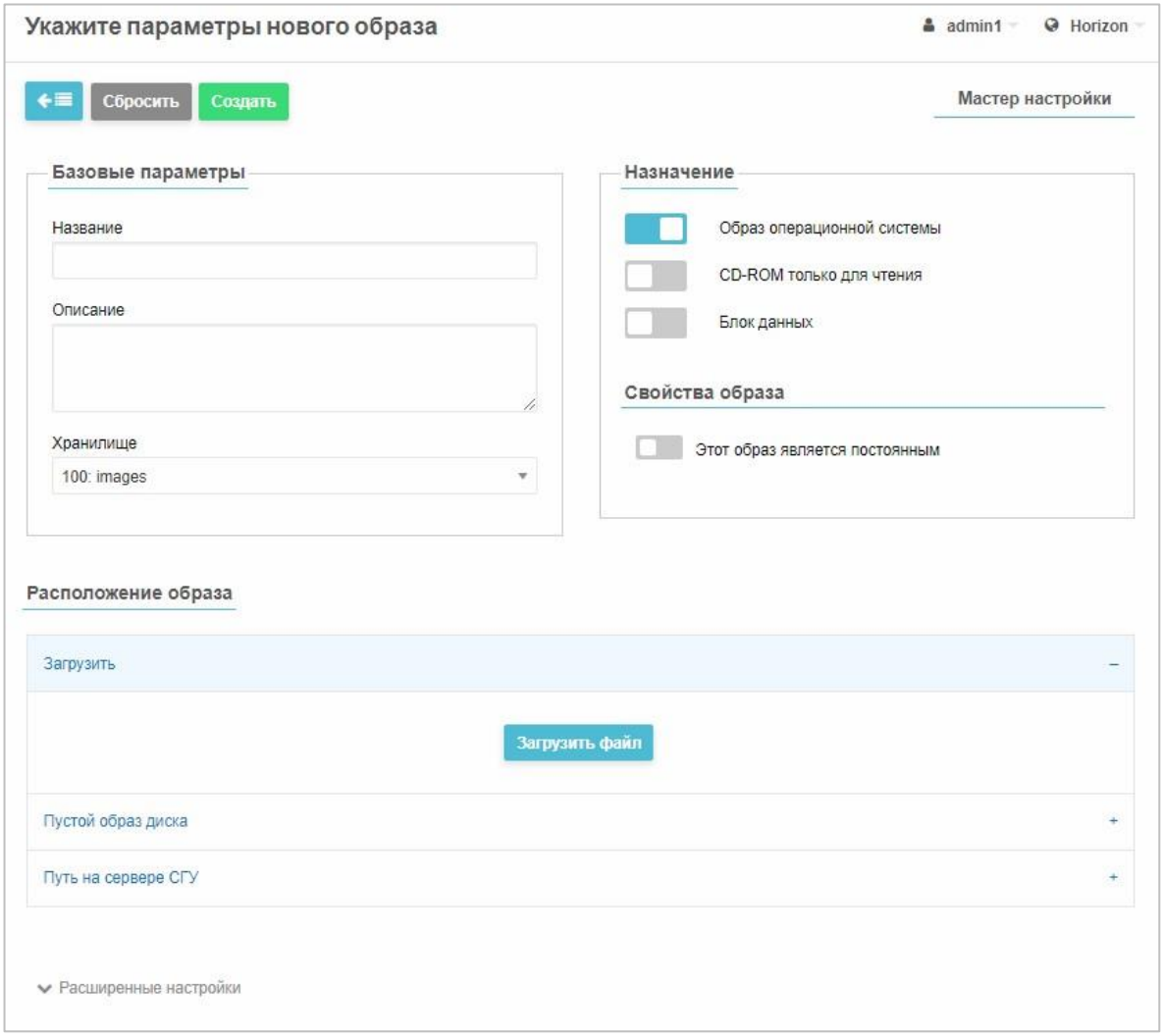


Рисунок 42 – Создание установочного образа диска ВМ

3. В поле **Название** указывается наименование образа диска.
4. В области **Назначение** выбрать один из вариантов:

– **Образ операционной системы** – для подключения готовых образов загрузочных дисков, т.е. то, что импортируется из других гипервизоров;

– **CD-ROM только для чтения** – для установки системы с диска или ISO образа;

– **Блок данных** – для создания пустого диска.

***Примечание**. В каждом шаблоне ВМ можно подключить только один образ данного типа.*

5. В поле **Свойства образа** можно установить, будет образ постоянным или непостоянным. Применимо для типов **Образ операционной системы** и **Блок данных.**

   Если образ является постоянным, то можно запустить одну ВМ из этого образа, и все изменения ВМ будут сразу же вноситься в этот файл. Если образ непостоянный, то каждый раз будет производиться полная копия ВМ, назависимо от базового образа.

6. В поле **Хранилище** указывается тип хранилища, в котором будет храниться образ.
7. В поле **Описание** вносится дополнительная информация о содержащейся на образе ОС.
8. В поле **Расположение образа** нажать кнопку 

и с помощью кнопки **Выберите файл** выбрать необходимый iso-образ установочного диска.

   В поле **Путь к файлу** можно указать вручную путь к хранилищу: полный путь и имя образа.

9. В дополнительных настройках (группа полей **Расширенные настройки**), которые активируются нажатием заполнить поля:

– в поле **Драйвер образа** указать выходной формат образа диска:

- **raw** – «сырые» данные и объем данного образа в поле **Размер. Хранилище займет** место, указаннае в поле **Размер;**
- **qcow2** – создается файл на 1–1,5 КБ, который будет занимать стольто места, сколько будут занимать производящиеся записи в этот файл. В поле **Размер** задать размер, которого этот файл может достичь;

– указать, разделяемый образ или нет:
  - если образ **неразделяемый**, то его можно примонтировать только к одной ВМ;
  - если образ **разделяемый**, то его можно примонтировать только к двум ВМ одновременно; две ВМ займут один диск, который был создан ранее (например, это нужно для корзины ОС Windows);

– в поле **Шина** из раскрывающегося списка выбрать интерфейс подключения жесткого диска внутри ОС: VirtIO, SCSI или Parallel ATA (IDE). В зависимости от поддерживаемойго типа гостевой ОС и поддерживаемых шин.

***Примечания**:*

1. *Если предполагается осуществлять миграцию виртуального диска, следует установить флажок «Этот образ является постоянным».*
2. *Если предполагается создавать снимки ВМ, то в поле Драйвер образа необходимо указать формат qcow2.*

10. Нажать кнопку Создать.

После завершения процесса копирования файла образ диска будет создан и размещен в хранилище. Возможные состояния образов перечислены в приложении (ПРИЛОЖЕНИЕ Б).

3.2.9.2 Создание дисковых разделов

Для создания в хранилище дисковых разделов, которые будут использованы для создания гостевой ОС и хранения данных:

1. Перейти в раздел **Хранилище** → **Образы** и нажать кнопку +.

Откроется окно установки параметров нового образа (Рисунок 43).

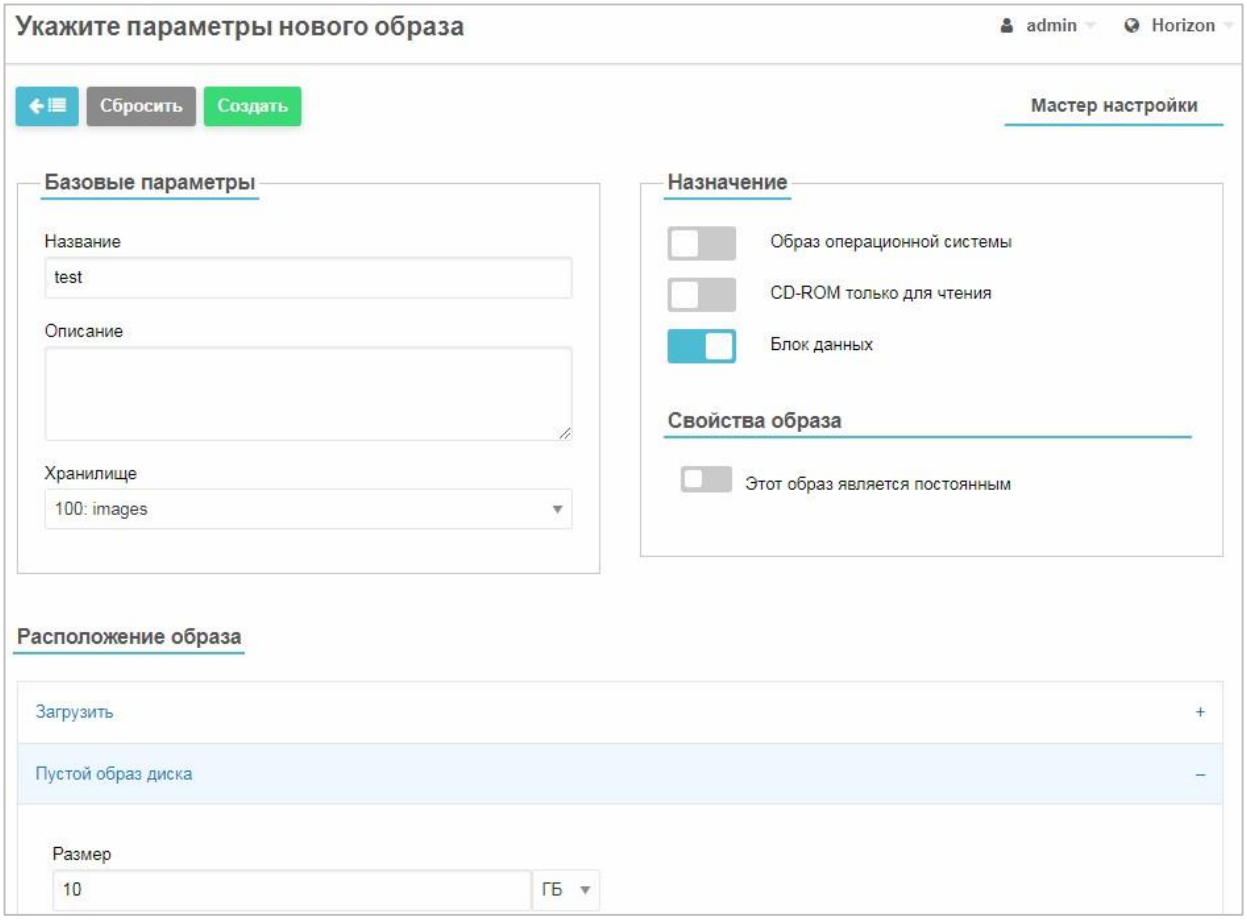


Рисунок 43 – Окно установки параметров нового образа

2. В поле **Название** ввести наименование диска.
3. В поле **Назначение** включить опцию **Блок данных,** передвинув переключатель вправо.
4. В поле **Хранилище** указать хранилище, где будет храниться образ.
5. В поле **Совйства образа** выбрать, является ли образ постоянным или непостоянным.

– для создания *постоянного* образа передвинуть вправо переключатель **Этот образ является постоянным** в секции **Свойства образа**.

– для создания *непостоянного* образа переключатель **Этот образ является постоянным** оставить неактивным.

6. В секции **Пустой образ диска** в поле **Размер** указать размер виртуального жесткого диска ВМ в ГБ или МБ (выбрать из списка).
7. В секции **Расширенные настройки** в поле **Драйвер образа** передвинуть переключатель вправо и указать формат **qcow2**.

   Виртуальный диск, созданный в данном формате, будет являться «тонким» (свободное дисковое пространство представлено общим пулом, из которого любой том может брать ёмкости при необходимости). Убедиться в этом можно, зайдя на сервер, на котором исполняется ВМ, к которой будет подключен диск (информацию о сервере можно получить в разделе **Узлы** → **ВМ**).
8. На сервере виртуализации найти директорию с размещенной ВМ и с помощью команды ***ls –l*** убедиться в том, что размер созданного файла диска *.qcow значительно меньше объявленного размера при его создании.

   Примечания.

   1. *Если предполагается осуществлять миграцию виртуального диска, следует установить флажок **Этот образ является постоянным**.*
   2. *Если предполагается создавать снимки ВМ, то в поле **Драйвер образа** необходимо указать формат **qcow2**.*
   3. *После этого нажать кнопку **Создать** и дождаться размещения образа ВМ в хранилище.*
   4. *Возможные состояния образов перечислены в приложении (ПРИЛОЖЕНИЕ Б).*

3.2.9.3 Миграция виртуальных дисков

Миграция виртуальных дисков – перенос их на другое хранилище.

Миграция виртуальных дисков возможна как с приостановкой обслуживания (выключенной ВМ), так и без приостановки обслуживания (включенной ВМ).

Примечания.

1. *Миграция доступна только для персистентных дисков (при создании необходимо активировать переключатель* ***Этот образ является постоянным*** *(Рисунок 42, 43).*
2. *Миграция возможна только между хранилищами NFS-NFS.*

Для осуществления миграции виртуальных дисков ВМ:

1. В разделе **Хранилище** выбрать подраздел **Образы.**
2. Выбрать из списка диск, который необходимо мигрировать и нажать кнопку Мигрировать диск

   Откроется окно списка хранилищ для миграции диска ( ).

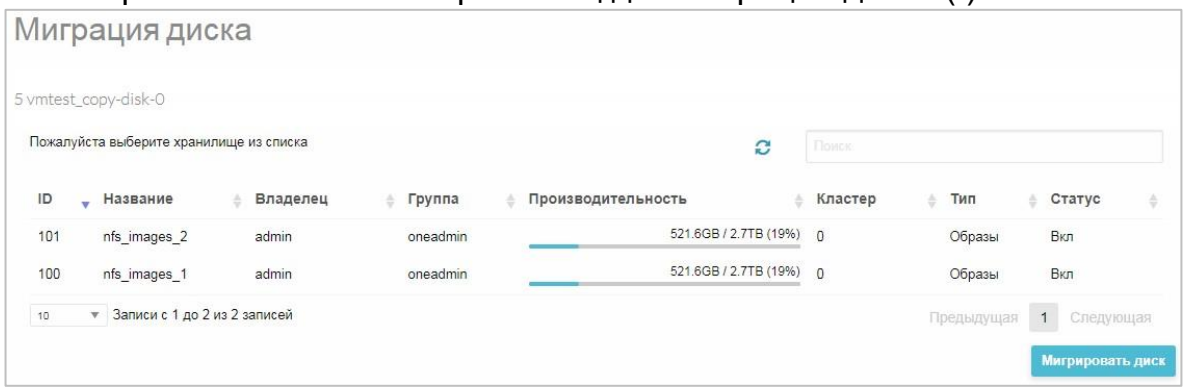


Рисунок 44 – Миграция дисков

3. Выбрать целевое хранилище из списка и нажать кнопку Мигрировать диск в нижнем правом углу.

   Запустится процесс миграции.

3.2.9.4 Клонирование образов

Клонирование диска – это создание точной копии диска.

Существующие образы можно клонировать в новые. Это может применяться для создания резервной копии образа перед его изменением или для получения копии образа, предоставленного другим пользователем.

Внимание*! Постоянные образы со снимками клонировать нельзя.* Для клонирования виртуальных дисков ВМ:

1. В разделе **Хранилище** выбрать подраздел **Образы ВМ**.

2. Выбрать из списка диск, который необходимо клонировать и нажать кнопку Клонировать в верхней части окна.

   Откроется окно с настройками параметров клонирования (Рисунок 45).

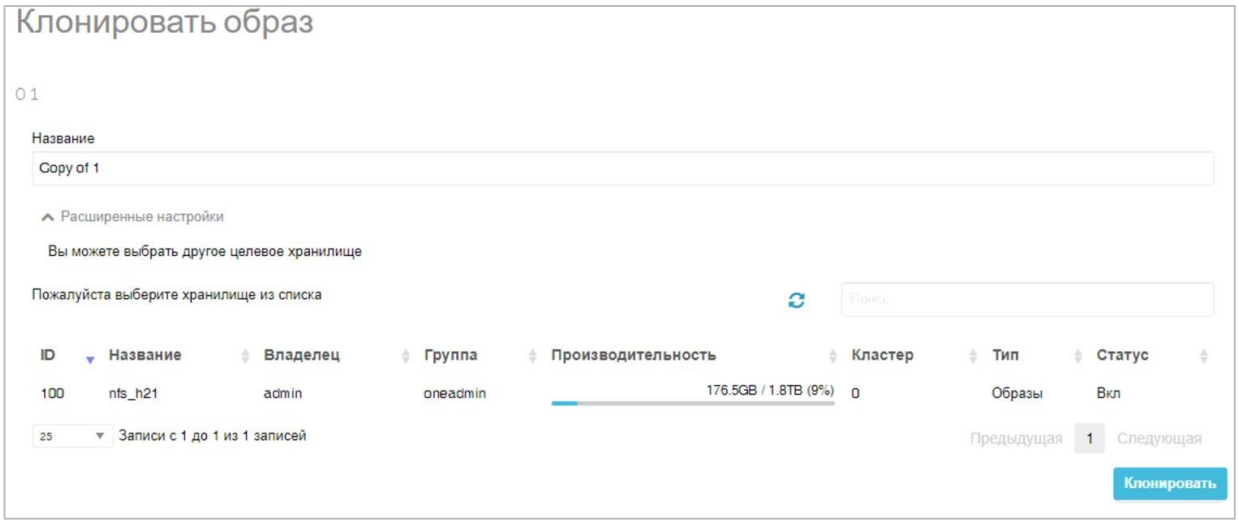


Рисунок 45 – Клонирование образа

3. Указать название нового диска, из списка выбрать целевое хранилище.
4. Нажать кнопку Клонировать в нижнем правом углу.

   Запустится процесс клонирования.

3.2.9.5 Настройка общего диска для нескольких ВМ

Для настройки общего диска для нескольких виртуальных машин:

1. В меню **Хранилище** → **Образы** добавить образ с назначением **Блок Данных** (см. п. 3.2.9.2).
2. Перейти в раздел **Машины** → **ВМ**.
3. При «горячем» подключении диска к ВМ (при включенной ВМ), нажать на нужную ВМ.

   Откроется окно информации о ВМ.
4. Перейти на вкладку **Хранилище** (Рисунок 46).

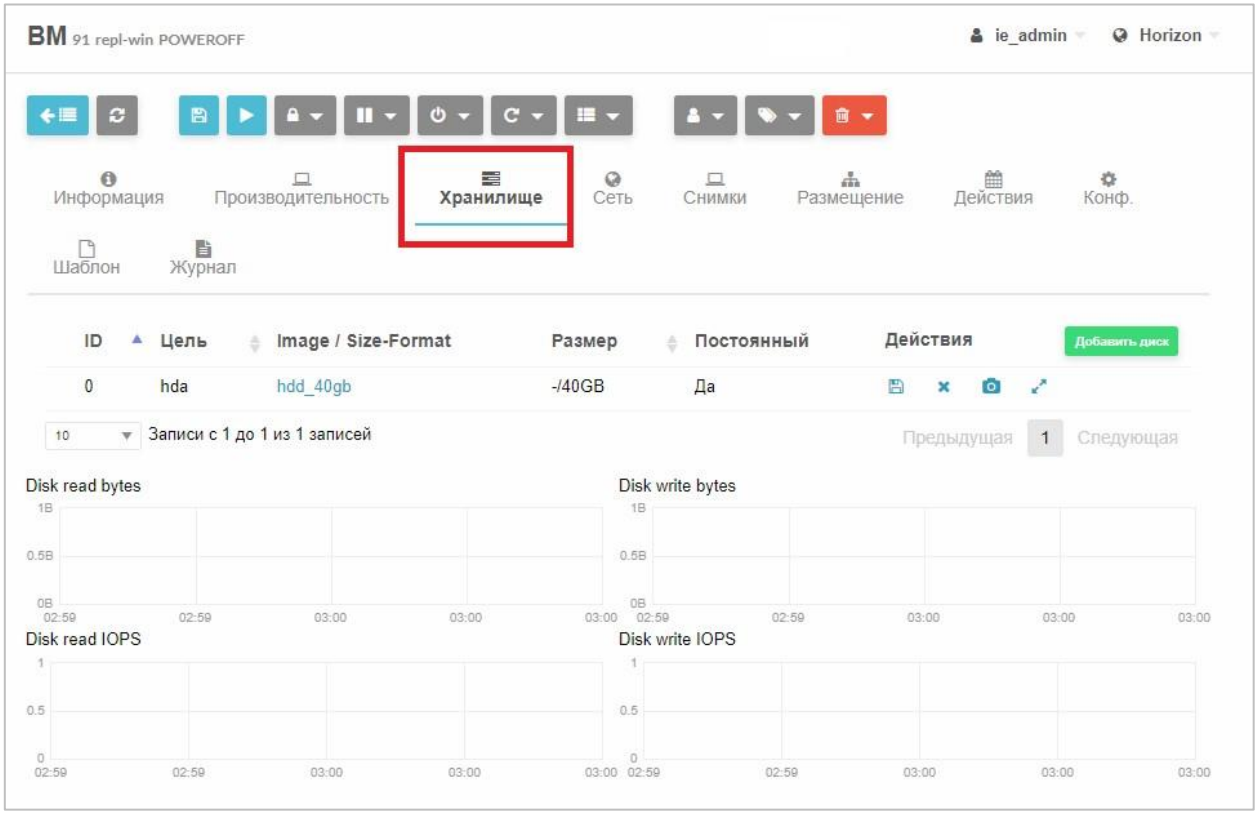


Рисунок 46 – Раздел «ВМ → Хранилище»

5. Нажать на кнопку **Добавить диск.**
6. В открывшемся окне **Присоединить диск** (Рисунок 47) выбрать диск, созданный на шаге 1.

***Внимание**! Для «горячего» подключения доступны только диски с шиной virtio. Для проверки шины диска перейти в раздел **Хранилища** → **Образы**, выбрать образ нажатием, в области **Общие параметры** в поле **Шина** должно быть значение **Virtio**.*

7. Нажать на кнопку **Присоединить** в нижнем правом углу.

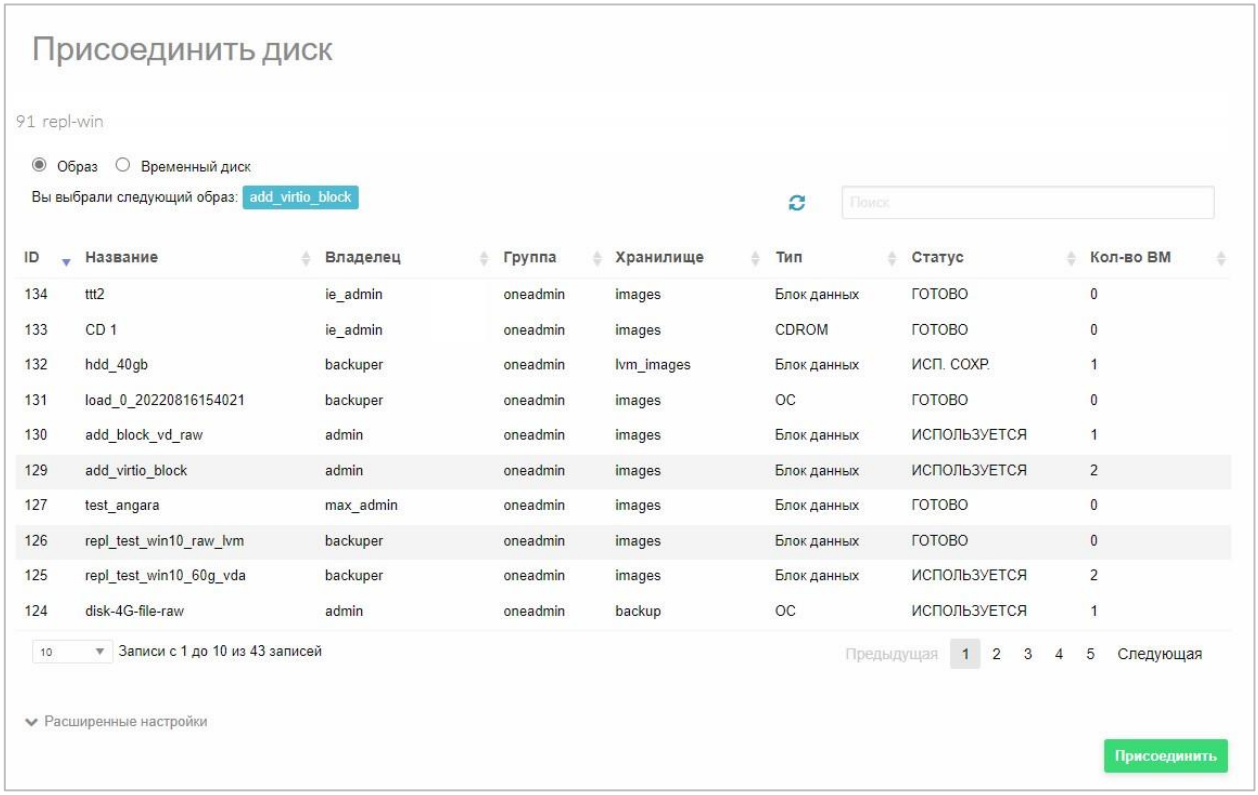


Рисунок 47 – Присоединение диска

8. Убедиться, что диск подключен к ВМ/ **Для проверки подключения диска в ВМ:** а. Подключиться к ВМ.

   ***Примечание**. Далее описаны действия для ОС Windows 10.* б.

   Нажать **Пуск** правой кнопкой мыши.

   в. В открывшемся списке выбрать **Управление дисками**.

   Появится диалог, предлагающий инициализировать диски и выбрать стиль разделов: Master Boot Record (MBT) или GUID (Рисунок 48).

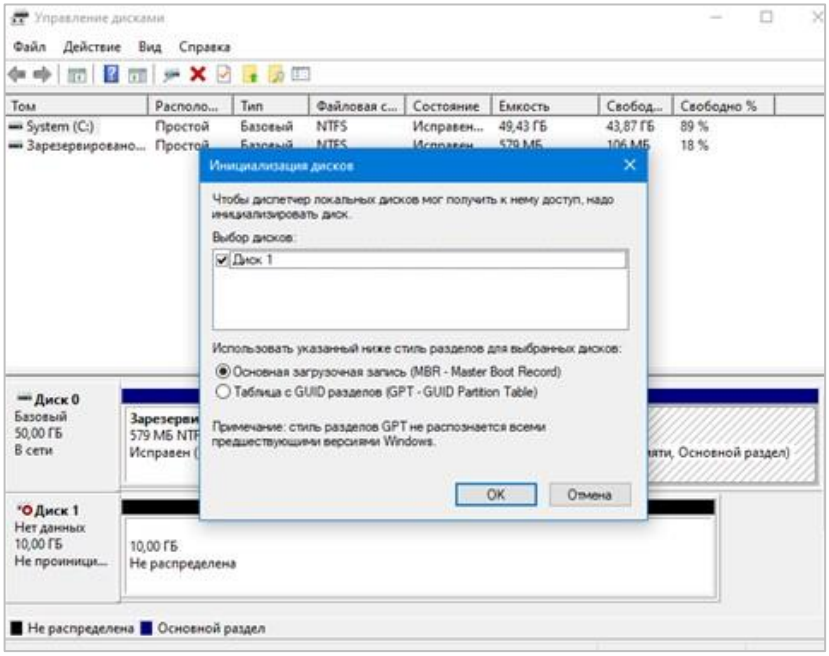


Рисунок 48 – Инициализация дисков

г. Выполнить инициализацию диска и выбрать стиль разделов.

Диск будет доступен для работы.

3.2.10 Создание, удаление, смена пароля пользователя

Работа с пользователями виртуальных машин осуществляется в подразделе **Система** → **Пользователи** (Рисунок 49).

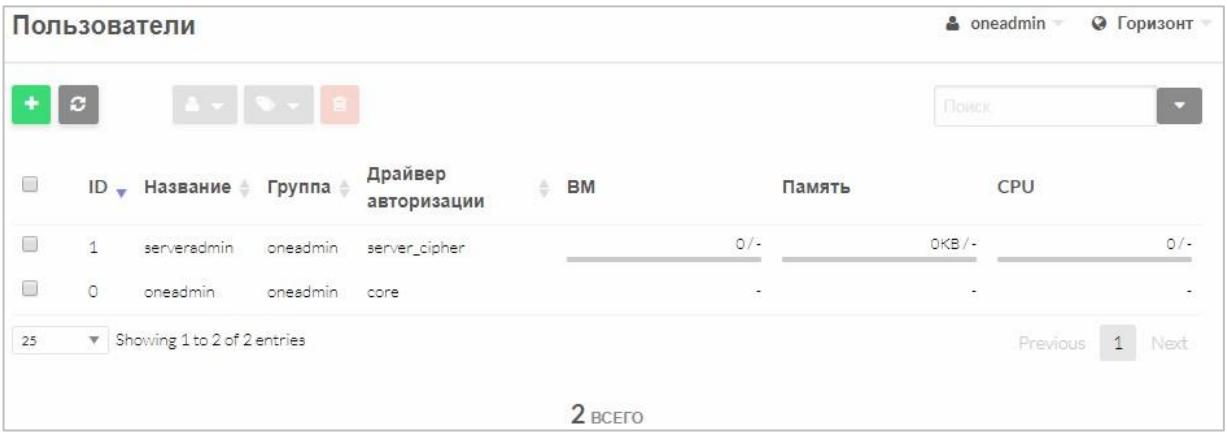


Рисунок 49 – Менеджер пользователей ВМ **Для создания нового пользователя:**

1. Нажать кнопку  в управляющем меню

Откроется окно **Создать пользователя** (Рисунок 50).

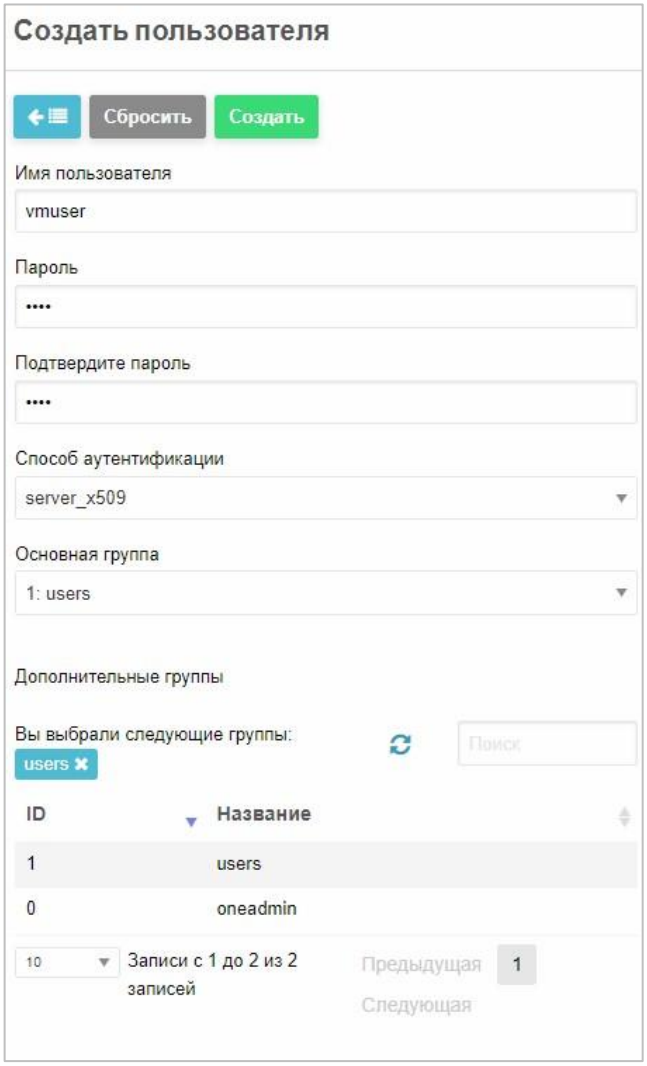


Рисунок 50 – Новый пользователь ВМ

2. В открывшемся окне заполнить поля:

- **Имя пользователя** – имя пользователя, как оно будет отображаться в системе;
- **Пароль** и **подтвердить пароль** – пароль пользователя;
- из раскрывающегося списка выбрать способ аутентификации (Рисунок 51) (для доступа через веб-интерфейс необходимо выбрать «ядро»);

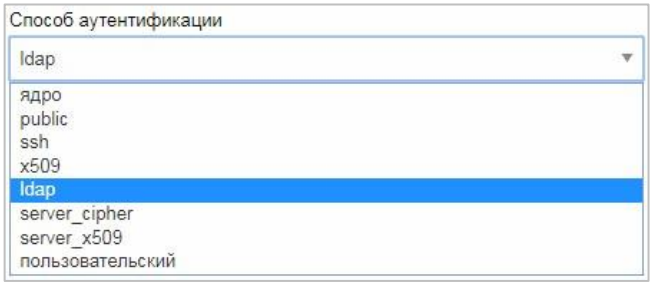


Рисунок 51 – Выбор способа аутентификации

– выбрать основную группу, в которую будет входить пользователь.

После заполнения всех полей нужно нажать кнопку **Создать** (Рисунок 50), и в главном окне (Рисунок 49) в списке появится новый пользователь.

***Примечания**:*

1. Если не все поля будут заполнены, то на экране появится предупреждающее сообщение (Рисунок 52).

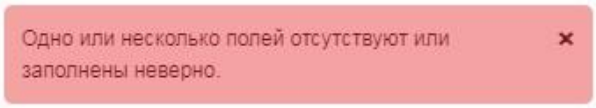


Рисунок 52 – Сообщение (1)

2. Имя пользователя должно быть уникальным. Если будет введено имя, уже существующее в системе, то на экране появится предупреждающее сообщение (Рисунок 53).

Рисунок 53 – Сообщение (2)

Для удаления пользователя:

1. Выбрать пользователя из списка (Рисунок 49)
2. Нажать кнопку  в управляющем меню
3. Подтвердить удаление пользователя в открывшемся окне нажатием

кнопки OK (Рисунок 54).

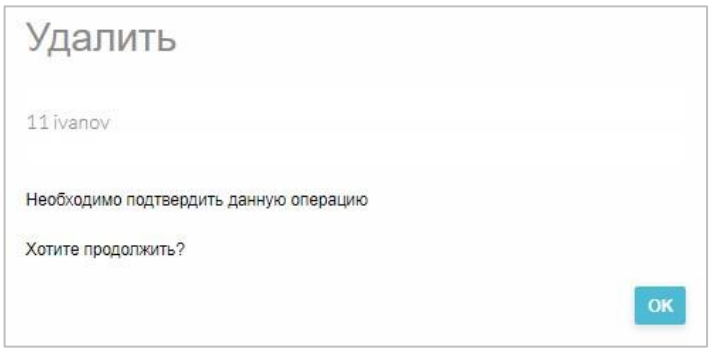


Рисунок 54 – Предупреждающее сообщение

Для изменения пароля пользователя:

1. Выбрать пользователя из списка (Рисунок 49) пользователя.
2. В открывшемся окне перейти на вкладку **Аутентификация** (Рисунок 55).

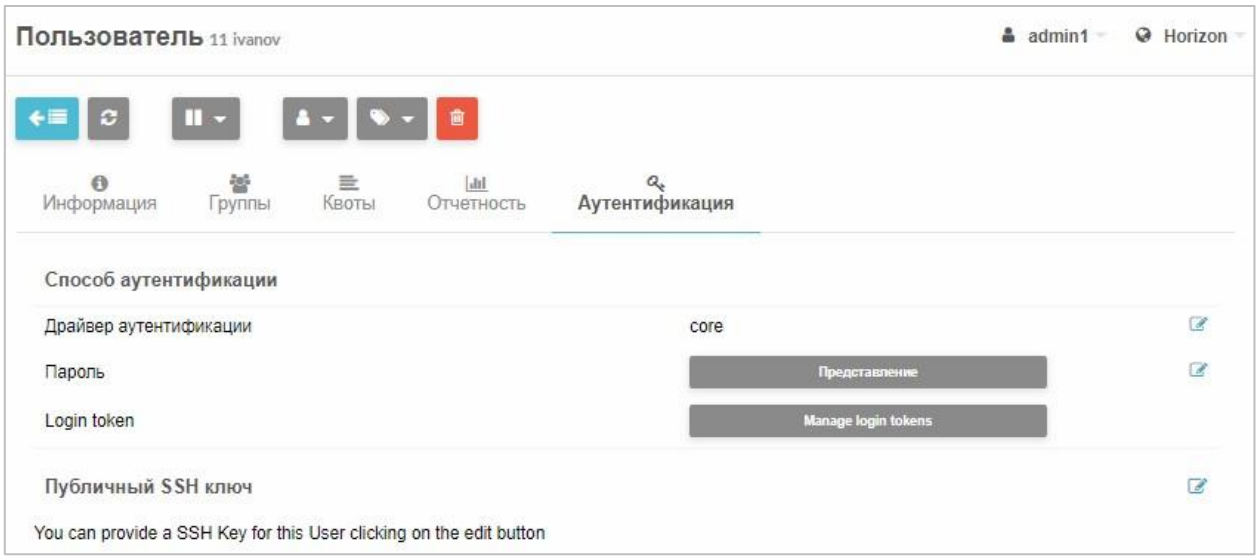


Рисунок 55 – Вкладка «Аутентификация»

3. В строке **Пароль** нажать кнопку редактирования .
4. В открывшемся окне **Обновить пароль** (Рисунок 56) дважды ввести

новый пароль и нажать кнопку Сменить (Рисунок 56).

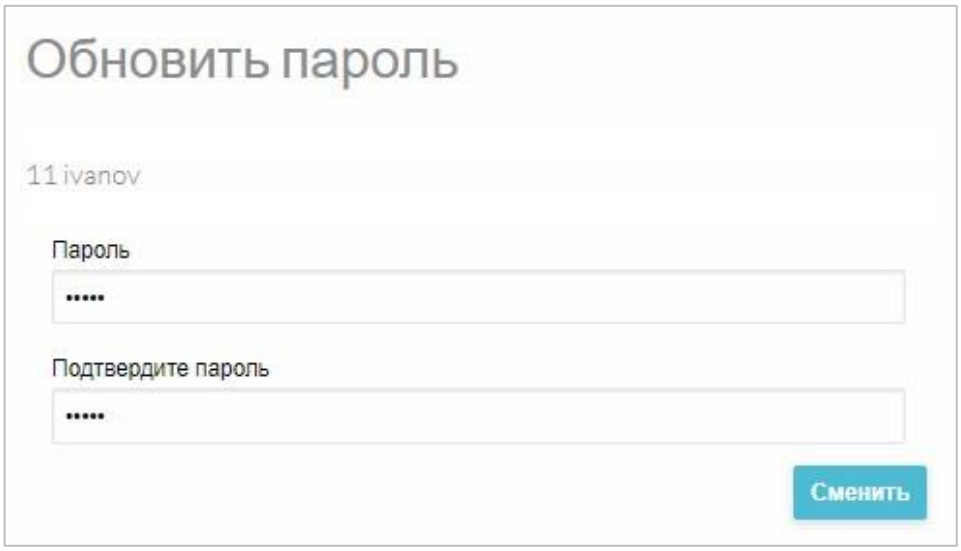


Рисунок 56 – Смена пароля пользователя

***Примечание**. По умолчанию имя пользователя и пароль «admin/admin». При первом запуске необходимо обязательно сменить пароль администратора. После смены пароля администратора необходимо поменять его в контейнере в файле **/var/lib/one/.one/one_auth**.*

3.2.11 Назначение пользователям права доступа на виртуальные машины

Для предоставления доступа к ВМ пользователю системы:

5. Зайти в СГУ **Машины** → **ВМ**,
6. Выделить флажком выключенную ВМ.
7. Нажать кнопку в управляющем меню и выбрать в меню пункт **Сменить владельца** (Рисунок 57).

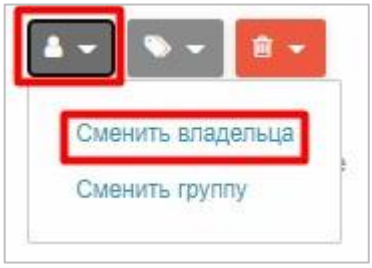


Рисунок 57 – Опция «Сменить владельца»

Откроется окно со списком пользователей (Рисунок 58).

8. Выбрать пользователя, которому будет предоставлен доступ к ВМ и нажать кнопку **ОК** (Рисунок 58).

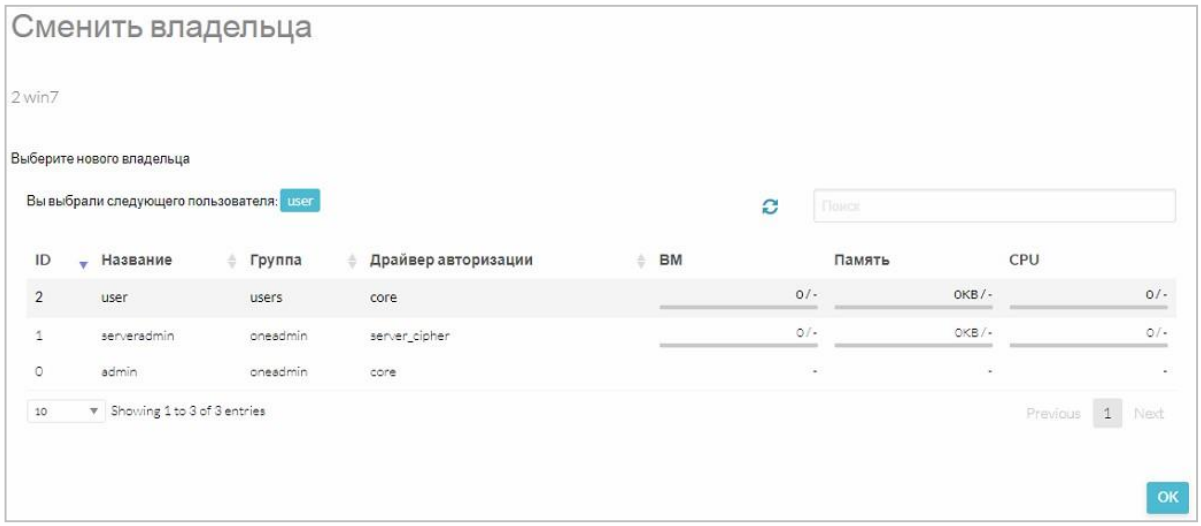


Рисунок 58 – Назначение нового пользователя ВМ

После назначения прав ВМ будет запускаться от имени указанного пользователя.

***Внимание**! Одному пользователю, согласно указаниям по эксплуатации (Формуляр МБРЦ.468313.001ФО, п. 6.4), назначается <u>только одна</u> виртуальная машина.*

3.2.12 Создание групп пользователей

Для разграничения прав в «Иридиум», для каждого ресурса, помимо пользователей, определены группы. Также как и пользователь, группа обладает правам доступа к тем или иным каталогам, файлам, ВМ и т.д. Группы объединяют пользователей для предоставления одинаковых полномочий на какие-либо действия.

Принадлежность пользователя к группе устанавливается администратором.

Работа с группами пользователей виртуальных машин осуществляется в разделе **Система** → **Группы**. В рабочей области раздела содержится список зарегистрированных в системе групп (Рисунок 59).

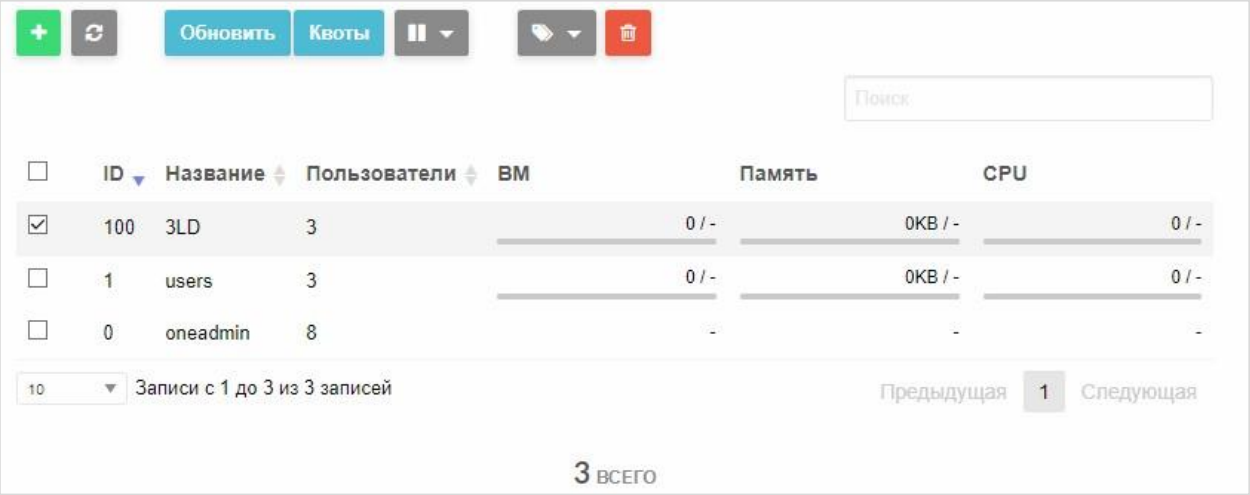


Рисунок 59 – Группы пользователей

Для создания новой группы:

1. Нажать кнопку  .

   Откроется окно **Создать группу** на вкладке **Общие** (Рисунок 60).

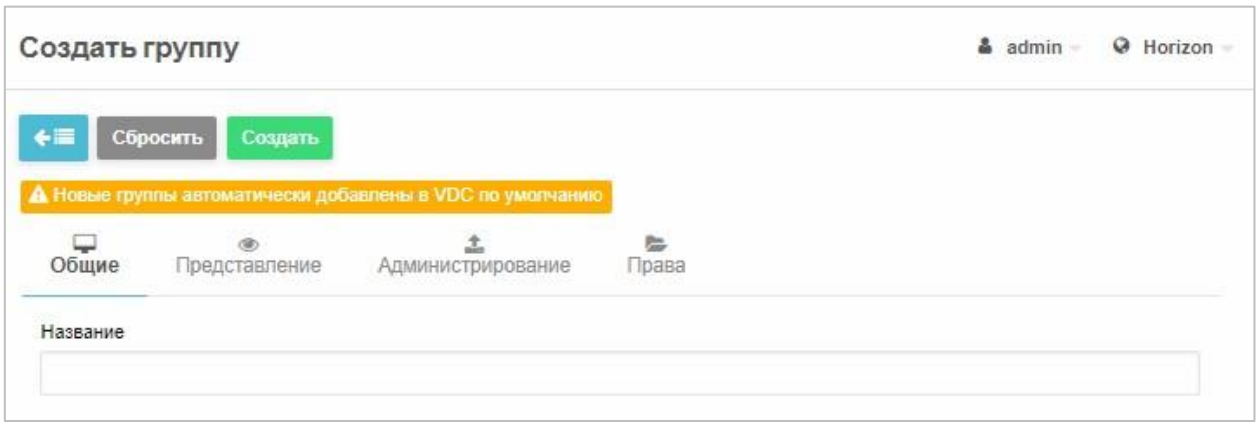


Рисунок 60 – Создание группы. Вкладка «Общие»

2. В поле **Название** ввести имя группы, как оно будет отображаться в системе.
3. На вкладке **Представление** указать стандартный пользовательский и административный интерфейсы, а также установить флажками

представление группы в качестве группы пользователей или администраторов (Рисунок 61).

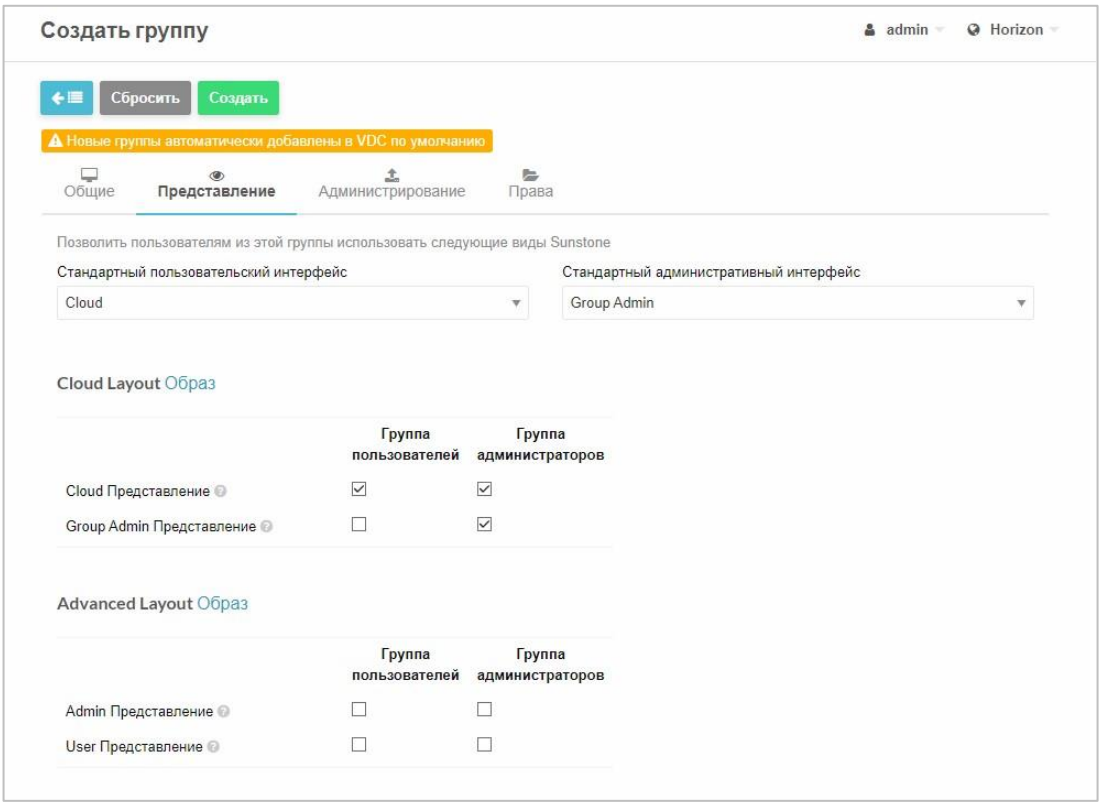


Рисунок 61 – Создание группы. Вкладка «Представление»

4. На вкладке **Администрирование** можно создать пользователя группы с административными правами. Для этого следует установить соответствующий флажок, после чего станут активными поля **Имя пользователя**, **Пароль**, **Подтвердите пароль** и **Способ аутентификации**, которые необходимо заполнить (Рисунок 62).

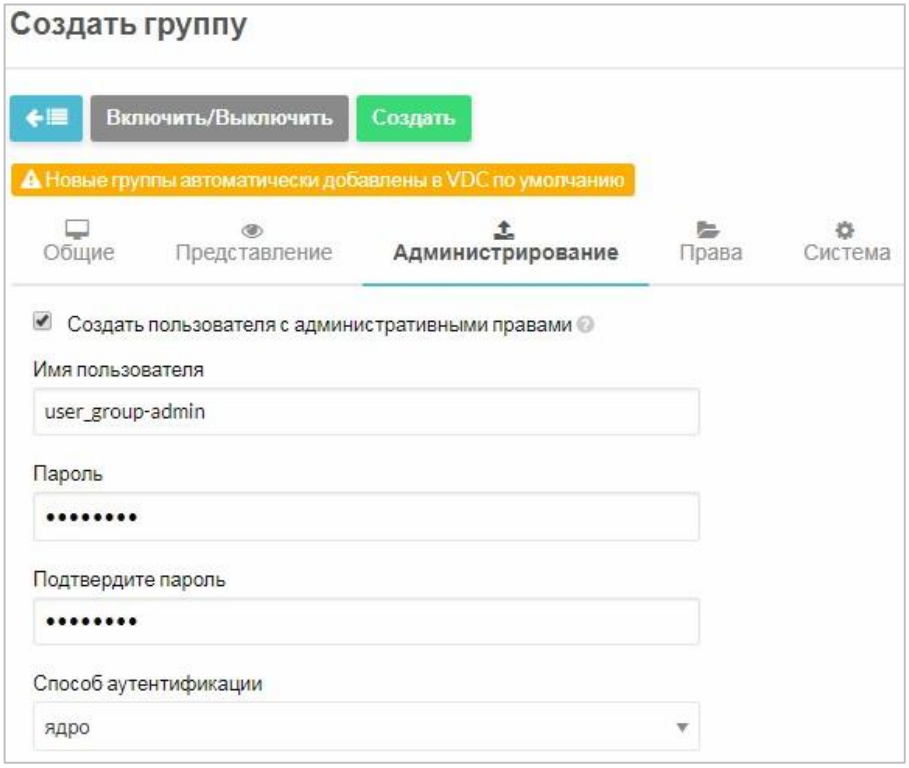


Рисунок 62 – Создание группы. Вкладка «Администрирование»

5. На вкладке **Права** устанавливаются разрешения на создание ресурсов для пользователей группы (Рисунок 63). Разрешенные ресурсы отмечаются флажками.

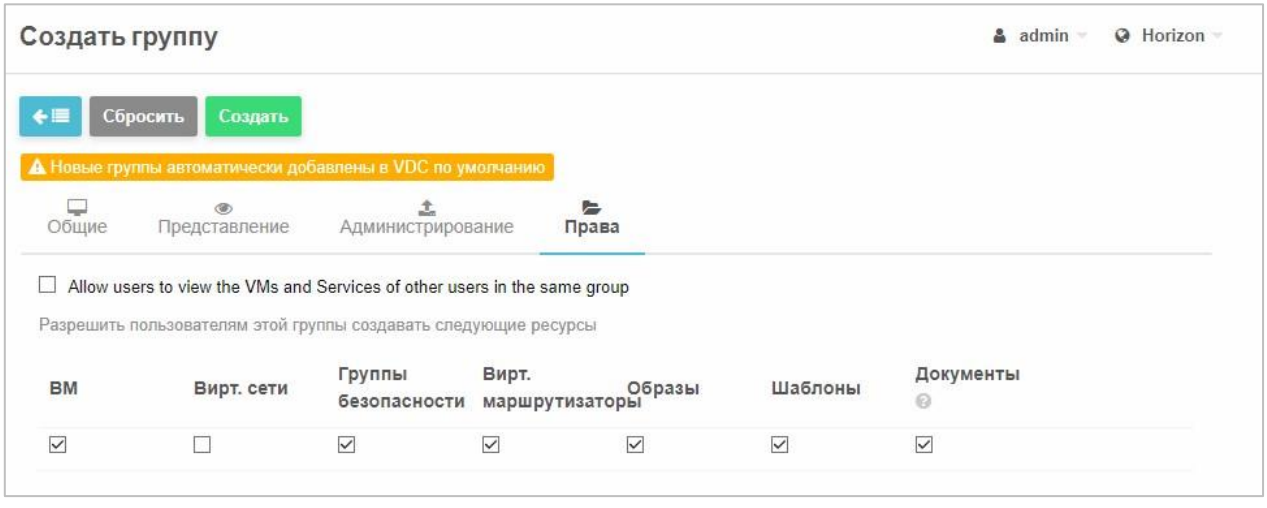


Рисунок 63 – Создание группы. Вкладка «Права»

6. Нажать кнопку Создать в управляющем меню.

   Новая группа появится в списке (Рисунок 59).

3.2.12.1 Назначение дискреционных прав доступа к ресурсам

Дискреционный принцип контроля доступа позволяет осуществлять настройку разрешенных операций для любого пользователя или группы пользователей. При попытке доступа происходит проверка списков контроля доступа, по результатам которой запрос разрешается или отклоняется. Настройка правил контроля доступа может производиться как для отдельных пользователей, так и для групп пользователей.

Для назначения дискреционных прав доступа:

1. Перейти в раздел **Система** → **Списки контроля**, после чего на экране откроются зарегистрированные в системе списки контроля доступа (Рисунок 64).

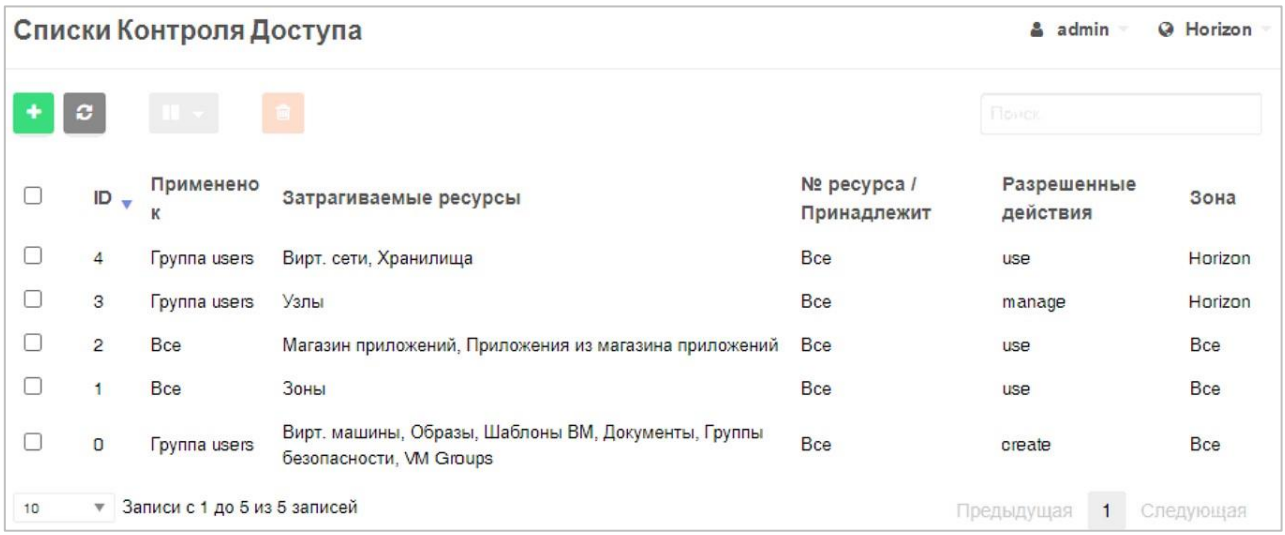


Рисунок 64 – Списки контроля доступа

В таблице указаны:

- ID (идентификатор) списка;
- к чему применен список – пользователю или группе;
- перечень ресурсов, разрешенных операций с ресурсами;
- разрешенные действия;
- в какой зоне применяется правило контроля доступа.

Для создания нового правила:

1. Нажать кнопку  в управляющем меню.
   Откроется окно **Создать правило контроля** (Рисунок 65).

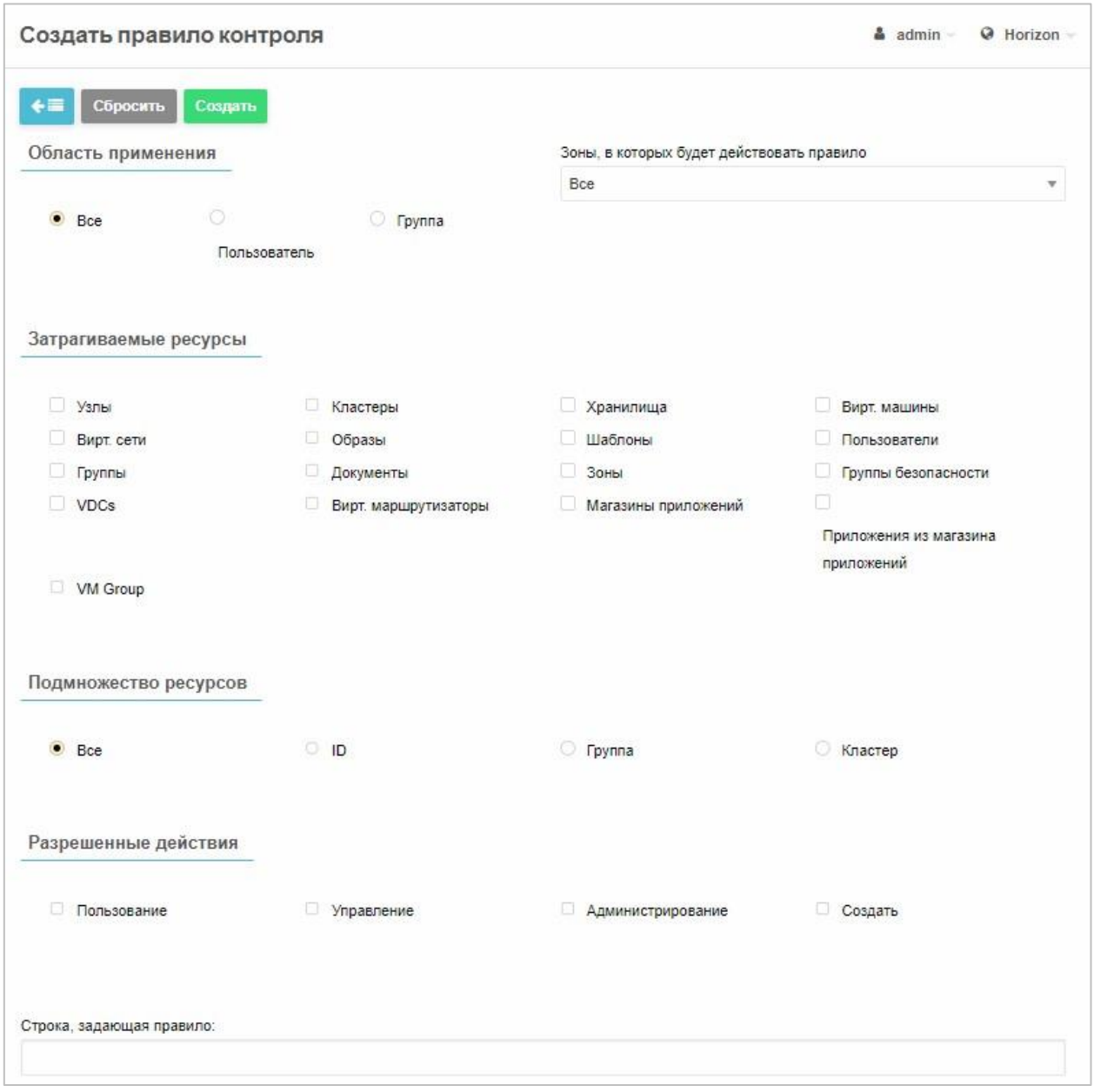


Рисунок 65 – Создать правило контроля доступа

2. В секции **Область применения** указать, для кого будут назначаться права, при помощи переключателей **Все**, **Пользователь** и **Группа**.
   При выборе **Пользователь** или **Группа** появится раскрывающийся список пользователей/групп (Рисунок 66).

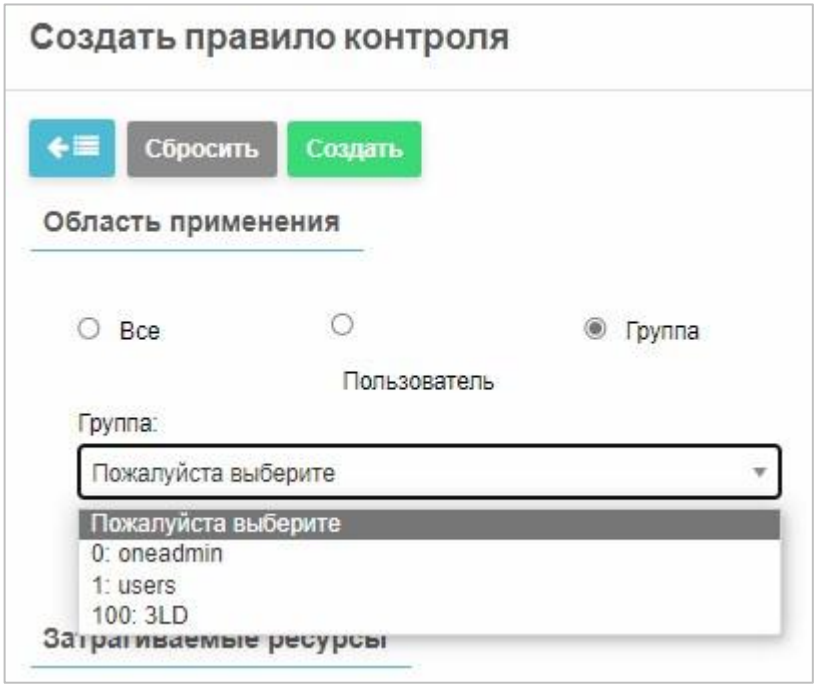


Рисунок 66 – Список групп пользователей

3. Выбрать пользователя/группу.
4. Выбрать зону, в которой будет действовать правило.
5. В секции **Затрагиваемые ресурсы** установить один или несколько флажков у перечисленных ресурсов («Узлы», «Кластеры» и т.д.), таким образом, предоставляя пользователю доступ к выбранным ресурсам.
6. В секции **Подмножество ресурсов** выбрать соответствующую опцию.
7. В секции **Разрешенные действия** необходимо определить доступные операции для выбранных ресурсов:

- **Пользование** – данные операции не изменяют ресурс (например, использование образа или виртуальной сети);
- **Управление** – операции, изменяющие ресурс (например, остановка ВМ, изменение атрибута образа виртуального диска на «постоянный» и т.д.);
- **Администрирование** – специальные операции (например, создание/удаление ролей, изменение параметров узлов и кластеров).

Данные операции должны назначаться только пользователям с ролью администратора;

– **Создать** – операции создания нового ресурса.

8. Нажать кнопку Создать (Рисунок 65).

Новое правило доступа появится в списке (Рисунок 64).

3.2.13 Перераспределение прав доступа к объектам инфраструктуры виртуализации

Система позволяет переназначать владельца (пользователя и группы пользователей) следующих виртуальных ресурсов:

– хранилищ; –
ВМ.

Для разных владельцев можно назначить разные права по управлению ресурсом.

3.2.13.1 Перераспределение прав доступа к хранилищам

Для назначения нового владельца хранилища:

1. Зайти в раздел **Хранилище** → **Хранилища**.
2. Выбрать хранилище из текущего списка двойным нажатием. Откроется окно информации о хранилище (Рисунок 67).

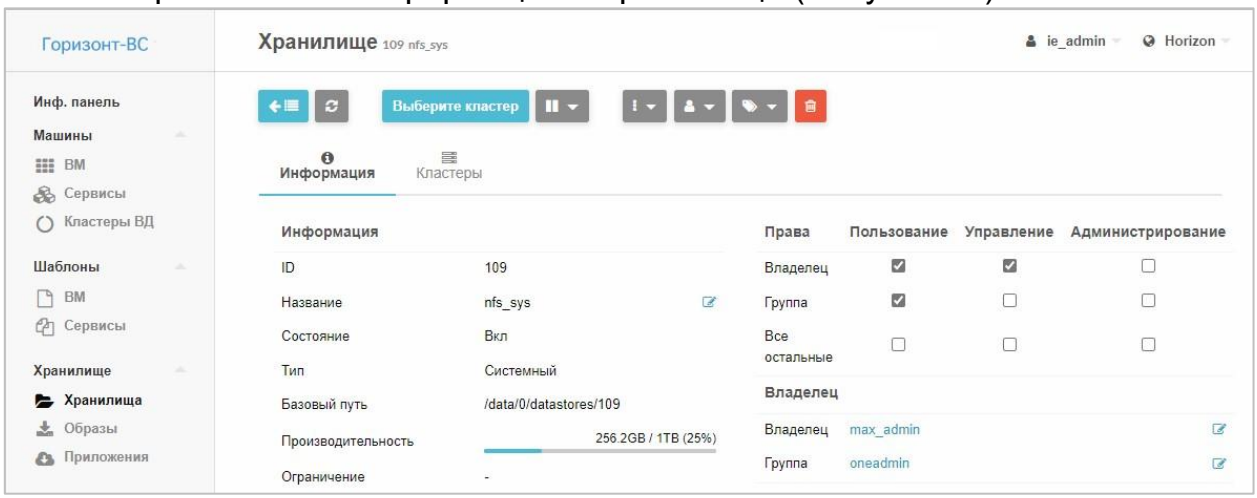


Рисунок 67 – Окно информации о хранилище

3. Выбрать нового владельца.

   Данную операцию можно выполнить двумя способами:

   Способ 1.

   а. В секции информации о владельце нажать на кнопку в строке «Владелец» (Рисунок 68).

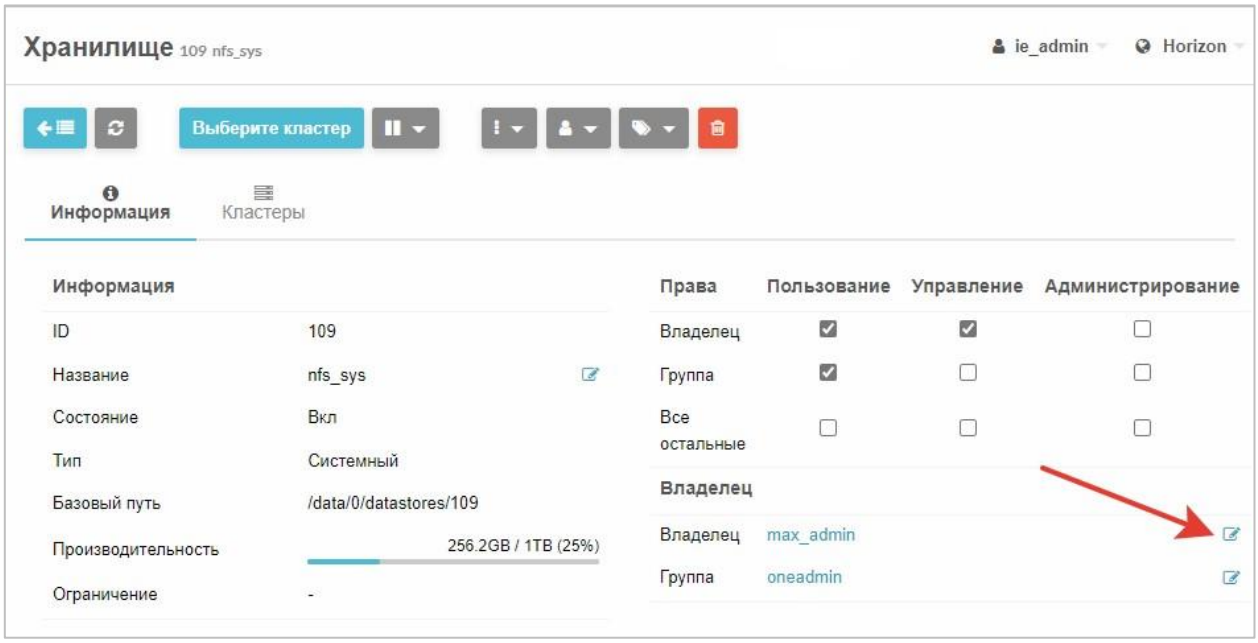


Рисунок 68 – Кнопка в строке «Владелец»

Появится раскрывающийся список пользователей (Рисунок 69).

б. Выбрать пользователя (Рисунок 70).

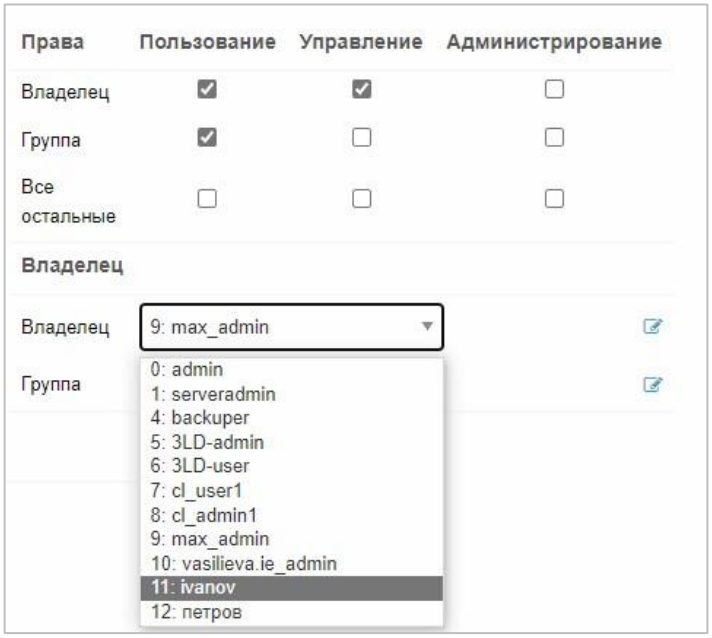


Рисунок 69 – Выбор пользователя

Способ 2.

в. Нажать кнопку  на панели управления.

г. Выбрать пункт **Сменить владельца** (Рисунок 70).

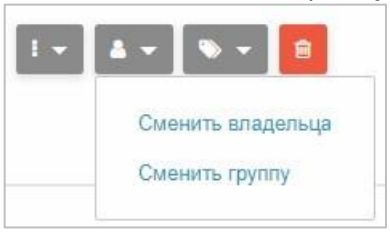


Рисунок 70 – «Сменить владельца»

Откроется окно «Сменить владельца» (Рисунок 71).

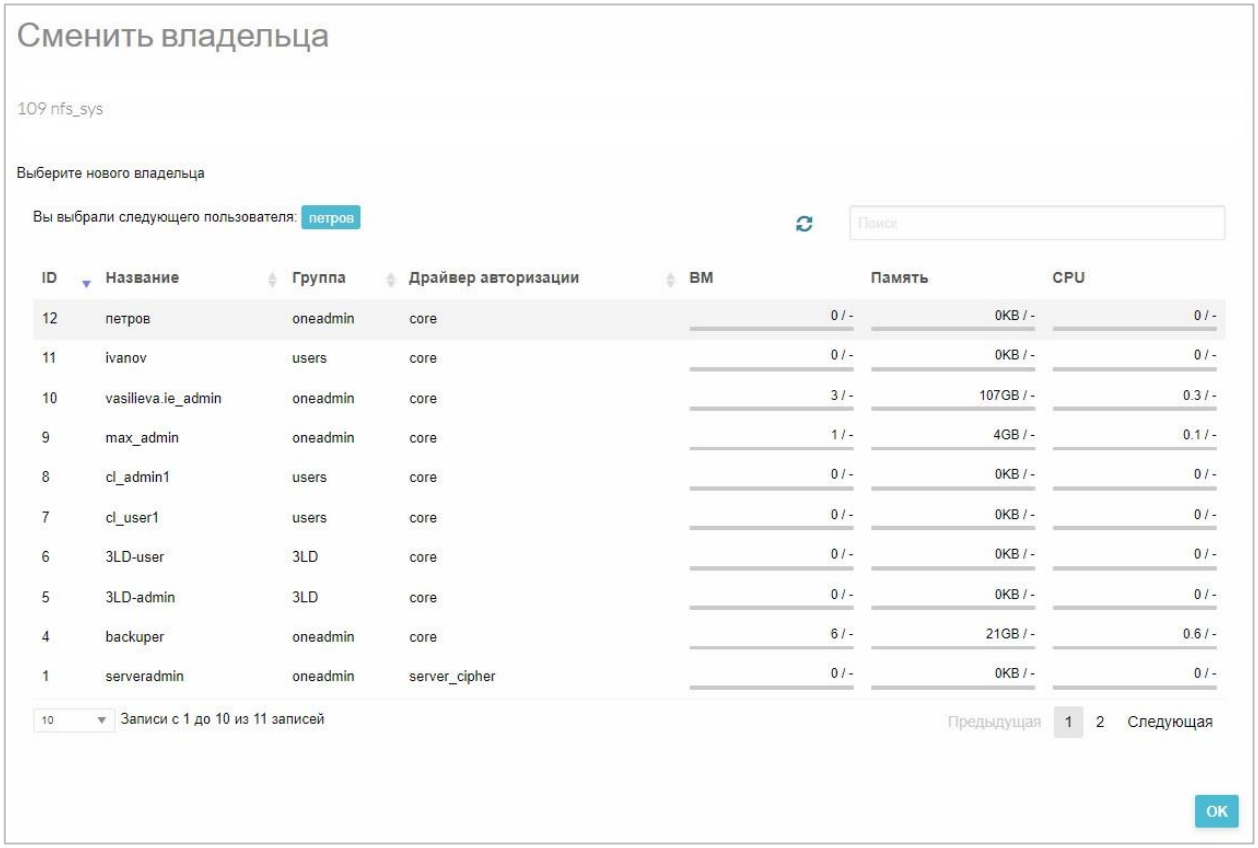


Рисунок 71 – Окно «Сменить владельца»

д. Выбрать нового владельца и нажать кнопку «ОК» в нижнем правом углу.

4. В секции настройки прав установить права для нового владельца: пользование, управление, администрирование (Рисунок 72).

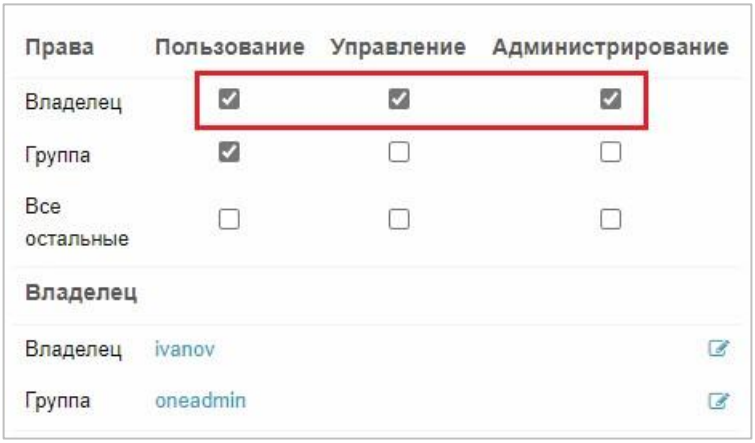


Рисунок 72 – Настройка прав для нового владельца

5. Нажать на кнопку «Обновить текущую страницу» на панели инструментов –  .

Для назначения новой группы пользователей хранилища необходимо нажать на кнопку в поле **Группа** в секции **Владелец** (Рисунок 73) и выполнить действия, аналогичные шагам 3 – 5 в описании назначения нового владельца хранилища (стр. 158).

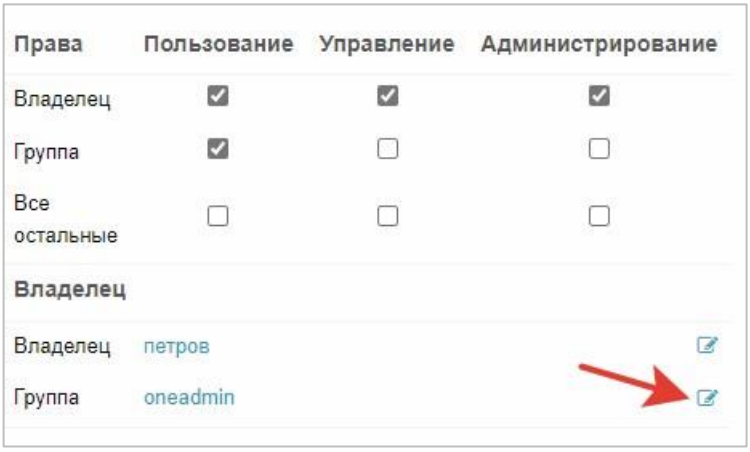


Рисунок 73 – Кнопка в строке «Владелец»

3.2.13.2 Перераспределение прав доступа к ВМ

Перераспределение прав доступа к ВМ осуществляется в разделе **Машины** → **ВМ** аналогично перераспределению прав доступа к хранилищам (см. п. 3.2.13.1).

3.2.14 Создание и настройка виртуальных сетей

Для создания сети:

1. Перейти в раздел СГУ **Сеть** → **Виртуальные сети.**
2. Нажать кнопку  на панели управления.

Откроется окно создания сети (Рисунок 74).

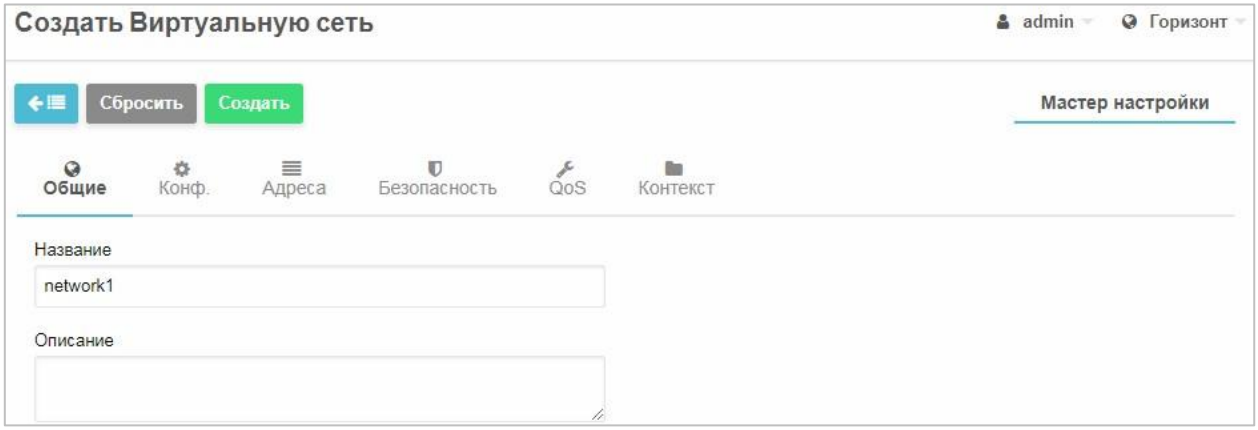


Рисунок 74 – Создание виртуальной сети. Вкладка «Общие»

3. На вкладке **Общие** необходимо ввести имя сети в поле **Название** и описание в поле **Описание** (Рисунок 74).
4. На вкладке **Конф.**:

– в поле **Интерфейс сет. моста** ввести название виртуального коммутатора, созданного в разделе 3.1.4 (Рисунок 75).

Значение по умолчанию – **hvssw0**.

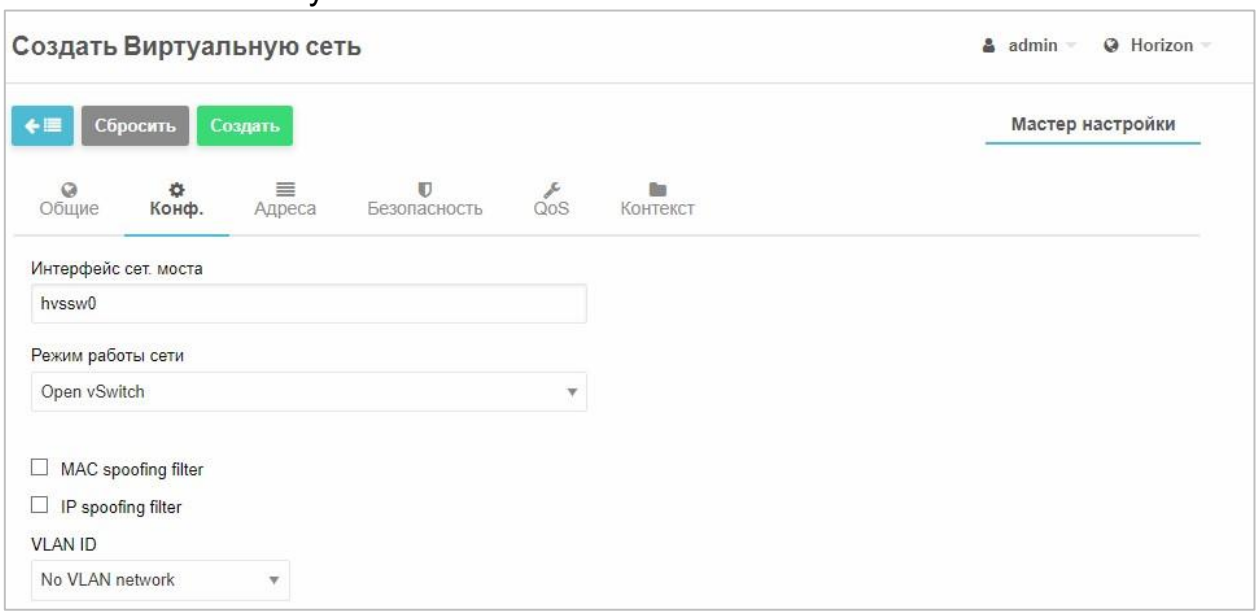


Рисунок 75 – Создание новой виртуальной сети. Вкладка «Конф.»

5. Из раскрывающегося списка выбрать режим работы сети

(Рисунок 76).

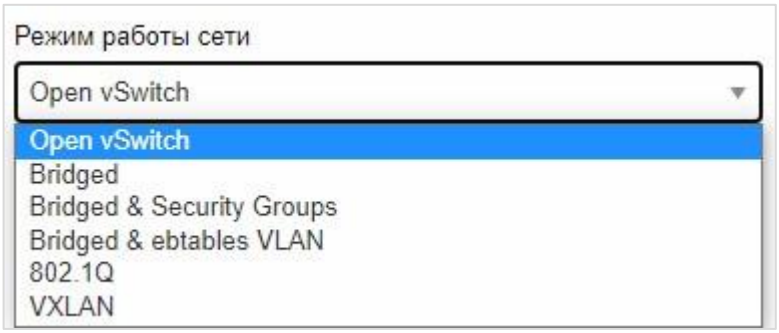


Рисунок 76 – Режимы работы виртуальной сети

Режимы работы:

- **Open vSwitch** – виртуальный коммутатор, открытый проект, виртуальный коммутатор с возможностью фильтровать график и более «умно» распределять нагрузку на сам коммутатор; При выборе **Open vSwitch** можно задать **VLAN ID** − выбрать способ формирования идентификатора сети.
- **Bridged** – стандартный сетевой мост Linux. Менее функциональный, чем **Open vSwitch**;
- **Bridged & Security Groups** – сетевой мост, который связан с группами пользователей. Данный режим работы устанавливается для реализации правил групп пользователей. Обладает функциональностью **Bridged** и дополнительно – межсетевой экран ebtables (на L3);
- **Bridged with ebtables VLAN** – сетевой мост, который связан группами пользователей, который включает в себя ebtables для L2 изоляции виртуальных сетей;
- **802.1QVLAN** – стандартный VLAN, сеть с поддержкой стандарта 802.1q. В Программный комплекс (ПК) «Иридиум» реализована поддержка 802.1q на уровне ВМ и гипервизора;
- **VXLAN** – для поддержки OpenFlow;

– установить флаги **MAC spoofing filter** (защита от подмены MACадреса) и **IP spoofing filter** (защита от подмены IP-адреса) – не обязательные поля;

– из выпадающего списка VLAN ID выбрать способ формирования идентификатора сети.

6. На вкладке **Адреса** установить параметры адресов:

– Нажать на кнопку  (Рисунок 77).

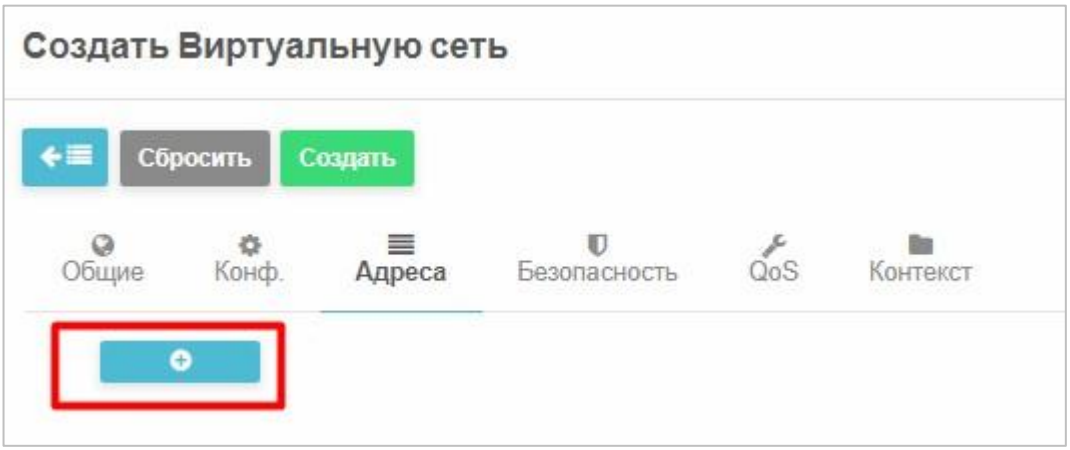


Рисунок 77 – Создание новой виртуальной сети. Вкладка «Адреса»

Откроется окно настройки диапазона адресов (Рисунок 78).

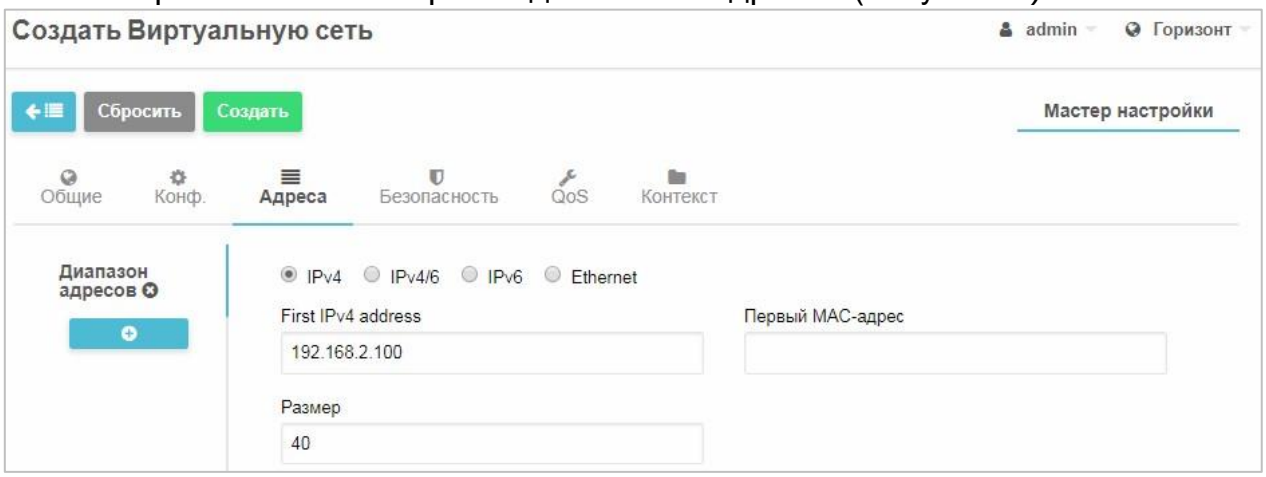


Рисунок 78 – Установка диапазона адресов виртуальной сети

– при помощи переключателей установить протокол сети (IPv4, IPv4/6, IPv6, Ethernet);

– в поле **Первый адрес IPv4** ввести первый адрес из адресного пространства;

– в поле **Размер** указать размер адресного пространства и в поле **Первый MAC-адрес** ввести MAC-адрес для виртуальной сети (Рисунок 78).

7. На вкладке **Безопасность** выбрать из списка одну из групп безопасности (Рисунок 79).

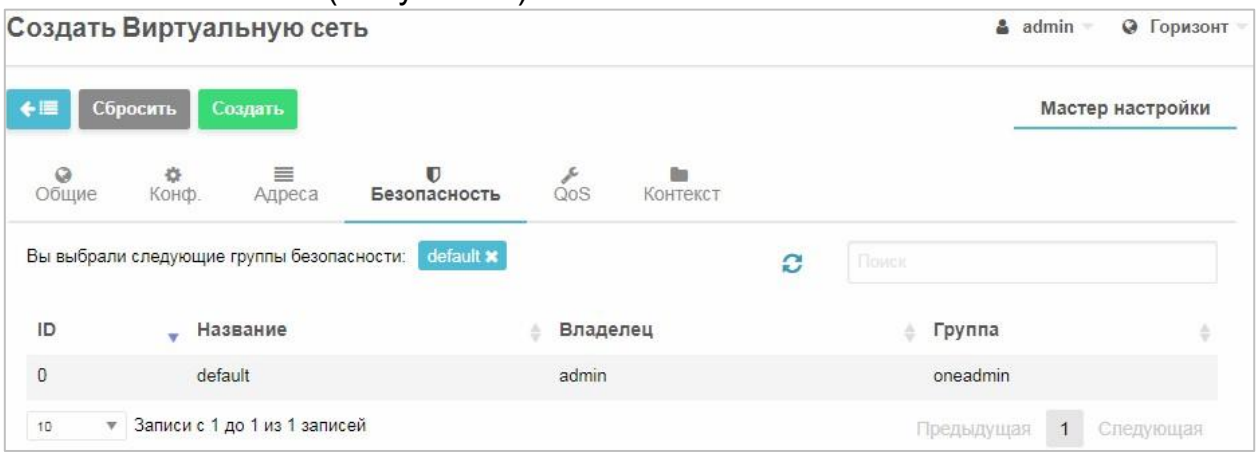


Рисунок 79 – Создание новой виртуальной сети. Вкладка «Безопасность»

8. На вкладке **QoS** можно настроить параметры обеспечения качества обслуживания (Quality of Service – QoS).

   QoS – полоса пропускания сети, способность сети обеспечить необходимый сервис заданному трафику в определенных технологических рамках.

   Для входящего и исходящего трафика можно задать среднюю пропускную способность в поле **Average bandwidth** (Кбайт/с) (Рисунок 80);

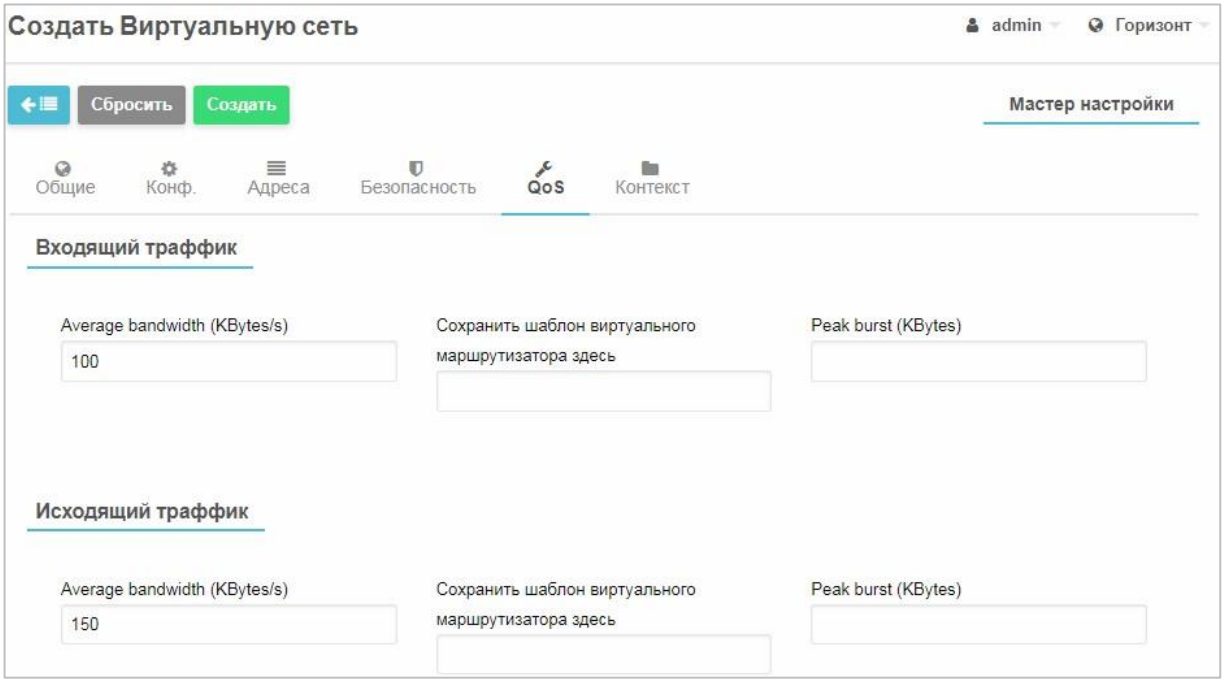


Рисунок 80 - Создание новой виртуальной сети. Вкладка «QoS»

9. Настроить дополнительные атрибуты контекстуализации на вкладке **Контекст** (Рисунок 81).

Для настройки гостевой сети виртуальная сеть может включать в себя дополнительную информацию, которая будет введена в ВМ во время загрузки. Эти атрибуты контекстуализации могут включать в себя, например, сетевые маски, DNS-серверы или шлюзы.

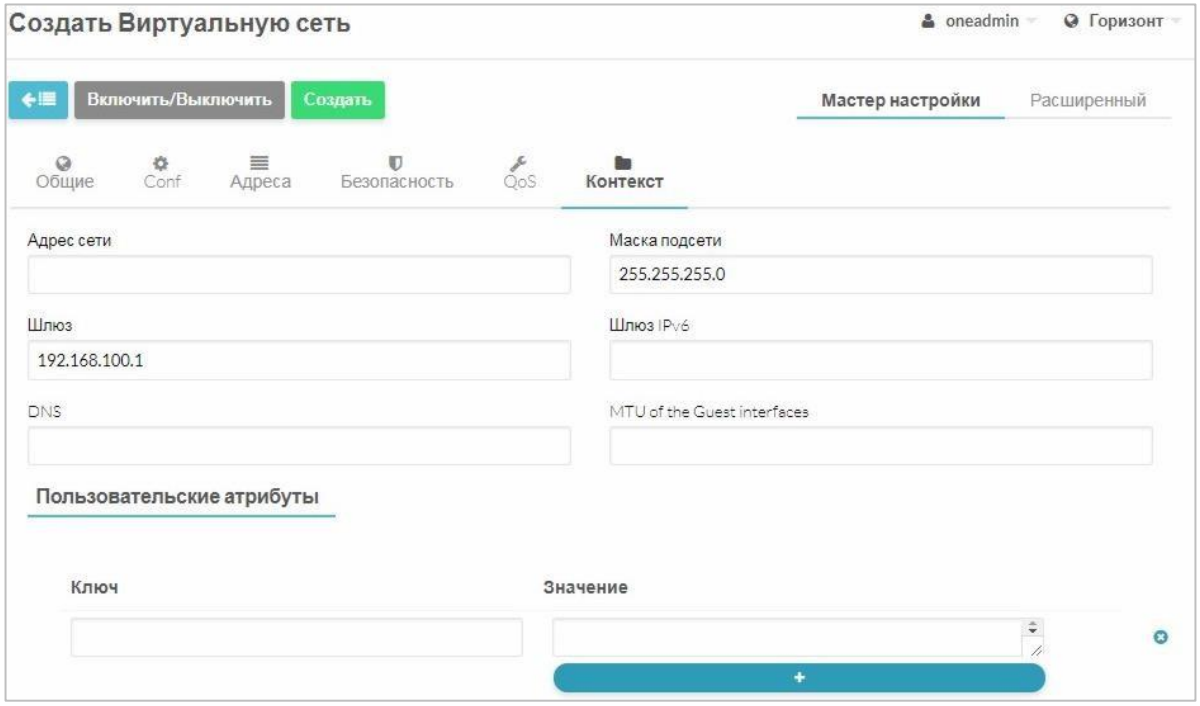


Рисунок 81 – Создание новой виртуальной сети. Вкладка «Контекст»

10. Нажать кнопку **Создать**.

В окне **Виртуальные сети** появится новая сеть.

Для изменения настроек виртуальной сети:

11. Перейти в раздел раздел **Сеть** → **Вирт. сети**.
12. Выбрать из списка сеть установкой флажка.
13. Ннажать кнопку **Обновить**.

1. Отредактировать параметры сети.

Подключение и отключение виртуальной сети к ВМ описано в разделе 3.2.22.4.

3.2.15 Топология сети

На вкладке **Топология** отображены все виртуальные сети и количество ВМ, работающих в тех или иных сетях.

Для обзора виртуальных сетей и маршрутизаторов необходимо в СГУ зайти в раздел **Сеть** → **Топология сети** (Рисунок 82).

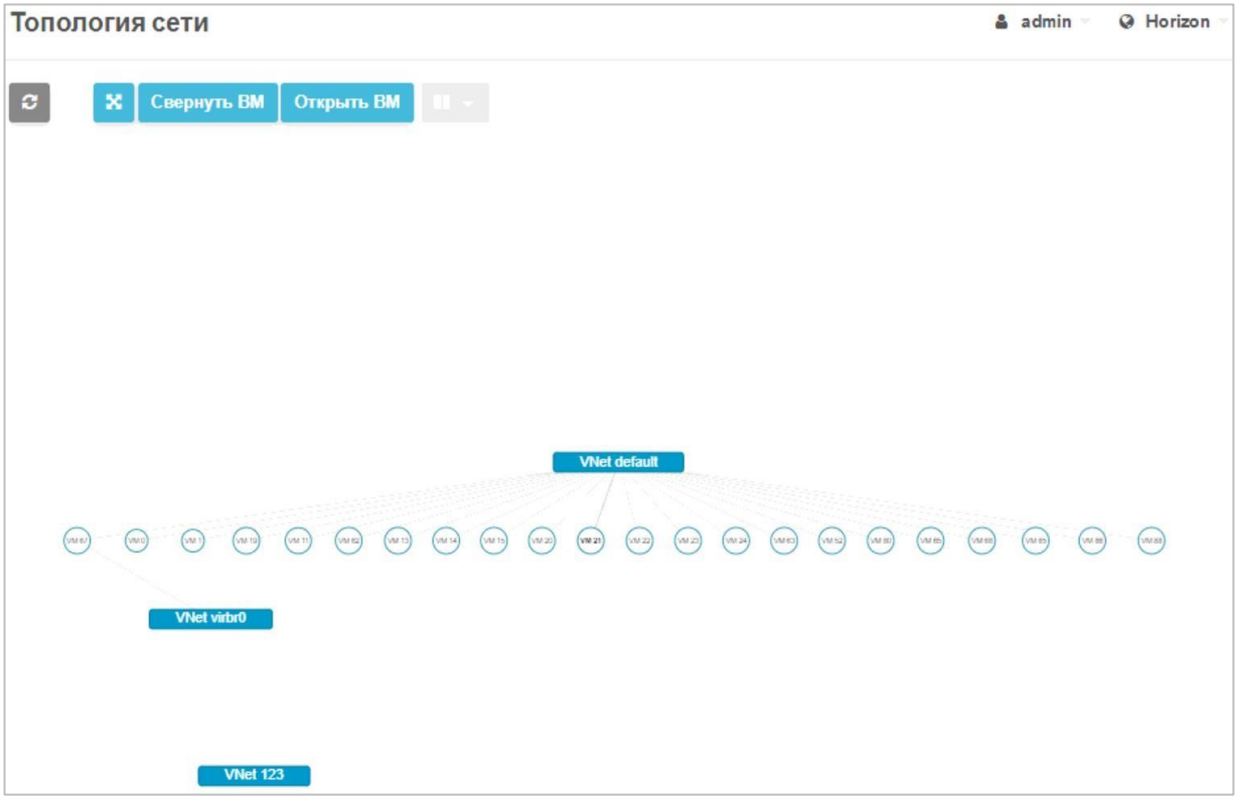


Рисунок 82 - Топология сетей

После того, как виртуальная сеть присоединена или отсоединена, устройства ВМ автоматически перенастраиваются, чтобы начать маршрутизацию к новому интерфейсу. Все изменения отображаются в разделе **Топология сети**.

Никаких дополнительный действий пользователя, например перезагрузки, не требуется.

3.2.16 Создание шаблонов виртуальных машин

Шаблоны ВМ – набор общих настроек для создания ВМ.

Для создания шаблона ВМ:

1. Перейти в раздел **Шаблоны → ВМ.**
2. На панели управления шаблонами ВМ нажать кнопку .

   На экране откроется страница с мастером настройки конфигурации шаблона ВМ (Рисунок 83).

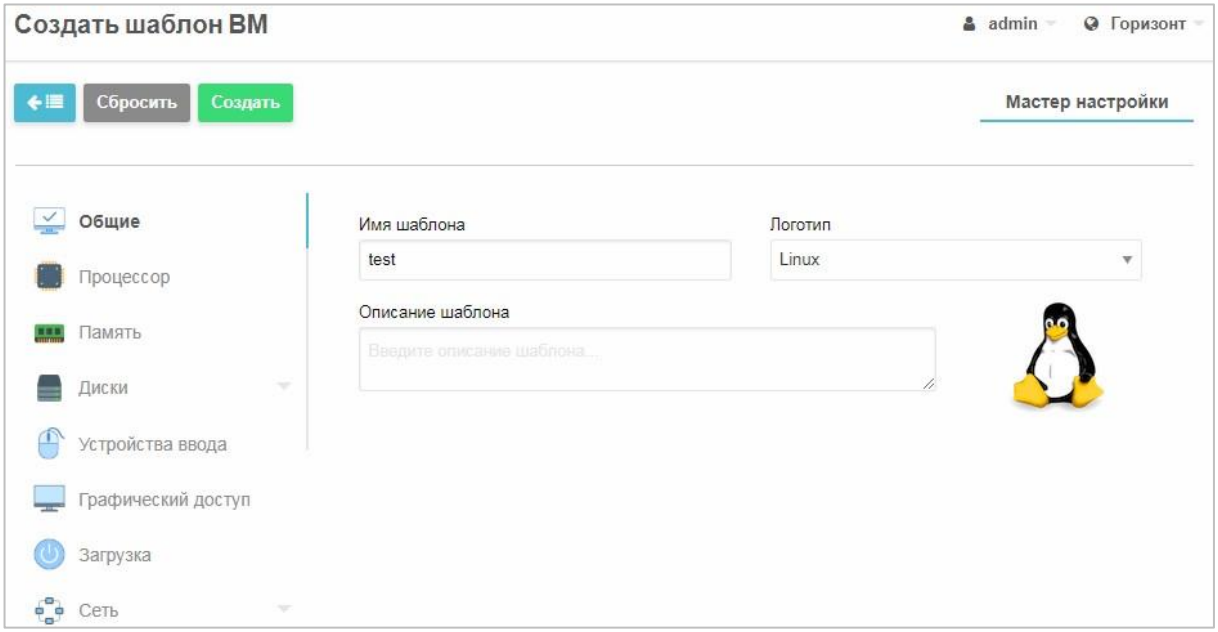


Рисунок 83 – Мастер настройки шаблона ВМ. Вкладка «Общие»

Мастер настройки представляет из себя систему вкладок, названия которых располагаются в левой части окна. Во вкладках предусмотрено моделирование конфигурации шаблона ВМ. По умолчанию открыта вкладка **Общие** (Рисунок 83).

3. На вкладке **Общие** настроить параметры:

– в поле **Имя шаблона** ввести наименование шаблона;

– в поле **Логотип** из выпадающего меню выбрать логотип устанавливаемой гостевой ОС;

– в поле **Описание** внести (опционально) дополнительное описание шаблона ВМ (пример: «ВМ отдела перспективных разработок. Базовое ПО, Win8, ОЗУ 8192 МБ, HardDisk 200 ГБ»).

4. На вкладке **Процессор** настроить конфигурацию и архитектуру ЦПУ (Рисунок 84).

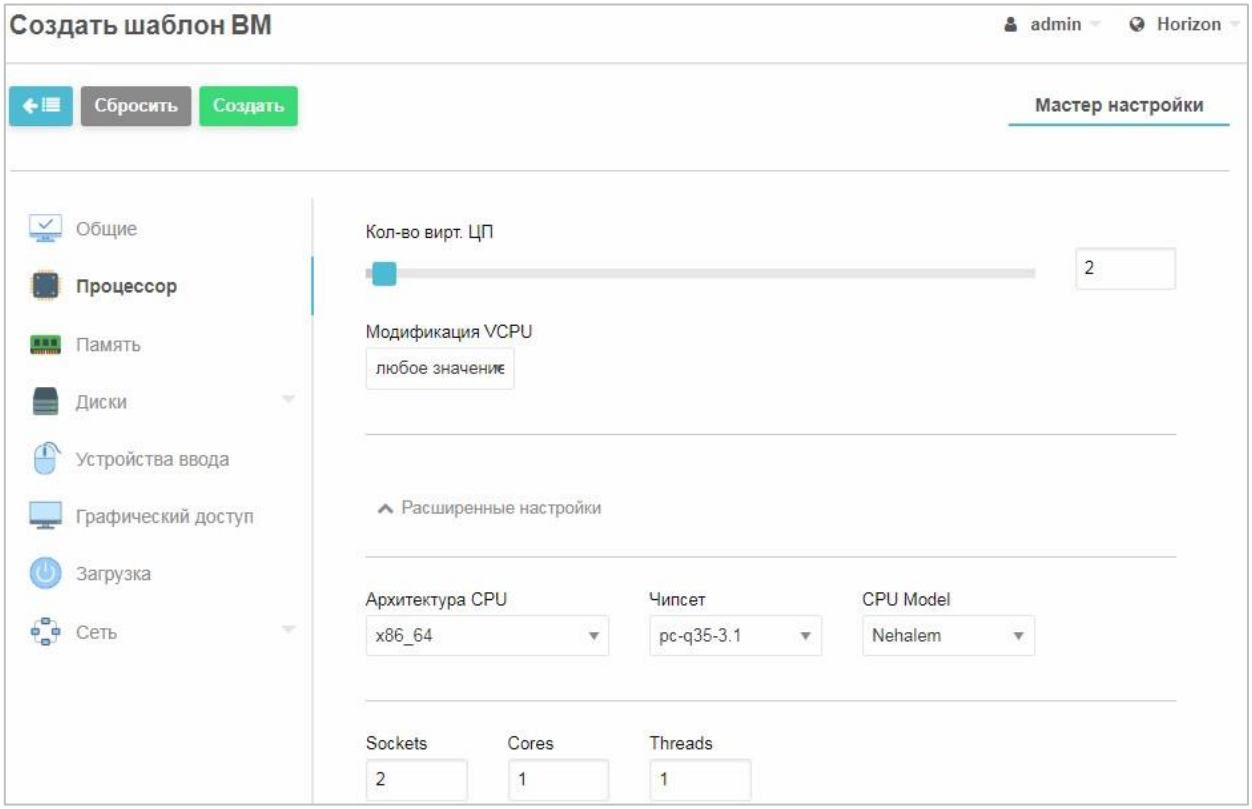


Рисунок 84 – Мастер настройки шаблона ВМ. Вкладка «Процессор»

- в поле **Кол-во вирт. ЦП** с помощью ползунка или записью значения в поле установить количество виртуальных процессоров, необходимых для ВМ. По умолчанию устанавливается два виртуальных ЦП;
- в поле **Модификация VCPU** можно выбрать тип и задать параметры;
- в поле **Архитектура CPU** из раскрывающегося меню выбрать тип архитектуры ЦПУ: *x86_64*;
- в поле **CPU Model** выбрать модель процессора для создаваемого шаблона ВМ (для использования процессора хоста выбрать значение *host-mode*, если нужна вложенная виртуализация – *host-passthrough*).

***Примечание**: для обеспечения возможности миграции ВМ между хостами с процессорами разных поколений, необходимо выбрать (вместо типа процессора «host-model») такой тип процессора, команды которого входят в множества команд всех используемых в кластере процессоров.*

5. На вкладке **Память** установить объем виртуальной оперативной памяти ВМ (Рисунок 85).

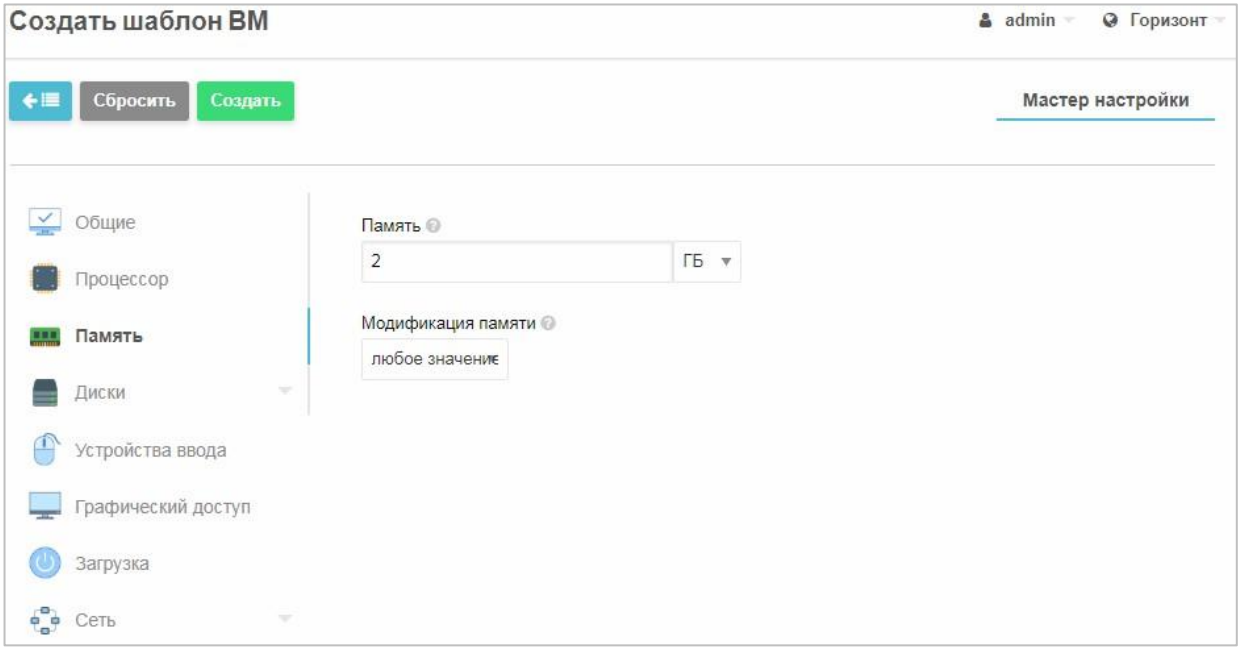


Рисунок 85 – Мастер настройки шаблона ВМ. Вкладка «Память»

– в поле **Память** устанавливается объем ОЗУ, необходимый для ВМ. Параметр вносится либо целым числом в ГБ, либо кратным 512 в МБ.

6. На вкладке **Диски** (Рисунок 86) к шаблону ВМ подсоединяются образы виртуальных дисков или загрузочных дисков с гостевой ОС или другим ПО.

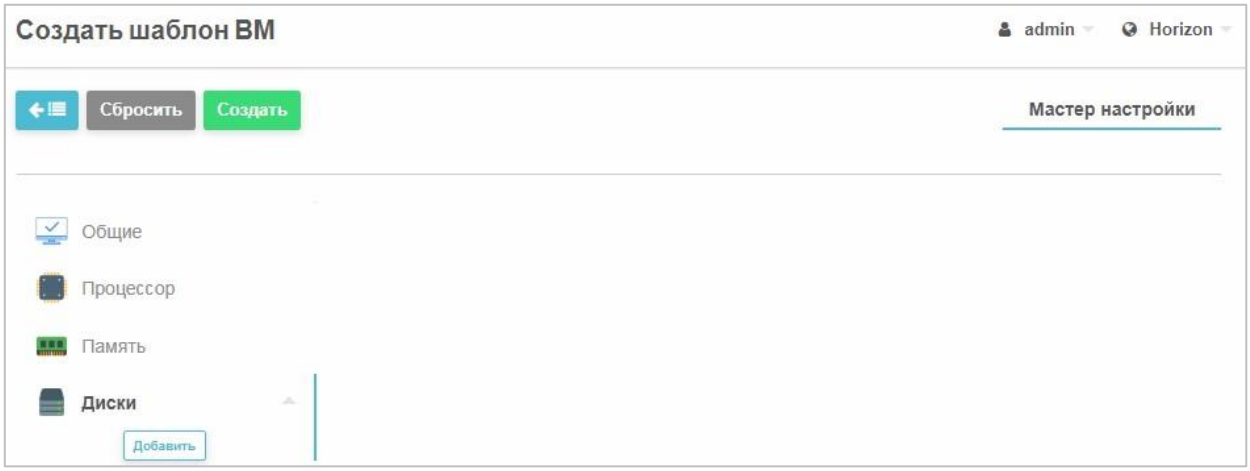


Рисунок 86 – Мастер настройки шаблона ВМ. Вкладка «Диски»

Для присоединения диска к ВМ необходимо нажать на кнопку **Добавить**.

На вкладке **Диски** появится вкладка второго уровня VOLATILE. При нажатии на нее откроется страница выбора и настройки подсоединяемого диска (Рисунок 87).

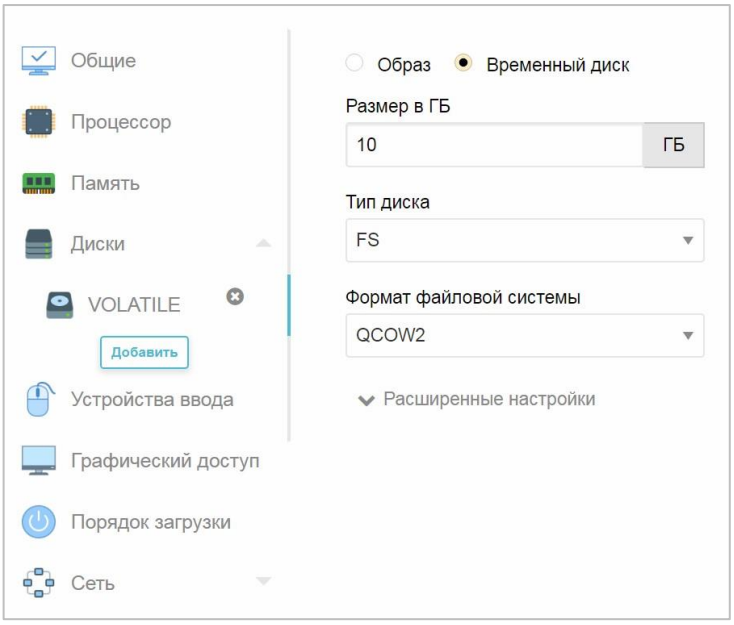


Рисунок 87 – Мастер настройки шаблона ВМ. Параметры дисков

К шаблону ВМ можно подключить уже созданный образ диска или временный диск.

Временные диски создаются «на лету» на целевом узле, где будет размещена ВМ, и удаляются вместе с ВМ. **Для подключения временного диска к ВМ**:

- установить переключатель **Временный диск**;
- в поле **Size in GB** (Размер в ГБ) указать необходимый размер жесткого диска в ГБ;
- в поле **Тип диска** выбирать тип файловой системы подсоединяемого диска: **FS** (Файловая система) или **SWAP**;
- в поле **Формат файловой системы** из раскрывающегося списка выбирается формат образа жесткого диска: **QCOW2** или **RAW** (Рисунок 87). Поддержка «тонких» томов для виртуальных жестких дисков и снимкой осуществляется при выборе в файловом

хранилище драйвера типа **QCOW2**. В таком случае диск становится «тонким»;

- в расширенных настройках возможно указать драйвер диска, шину и задать ограничения IOPS для записи и чтения данных.

Для подключения уже загруженного образа диска:

- установить переключатель **Образ** и из списка образов выбрать нужный файл (Рисунок 88).

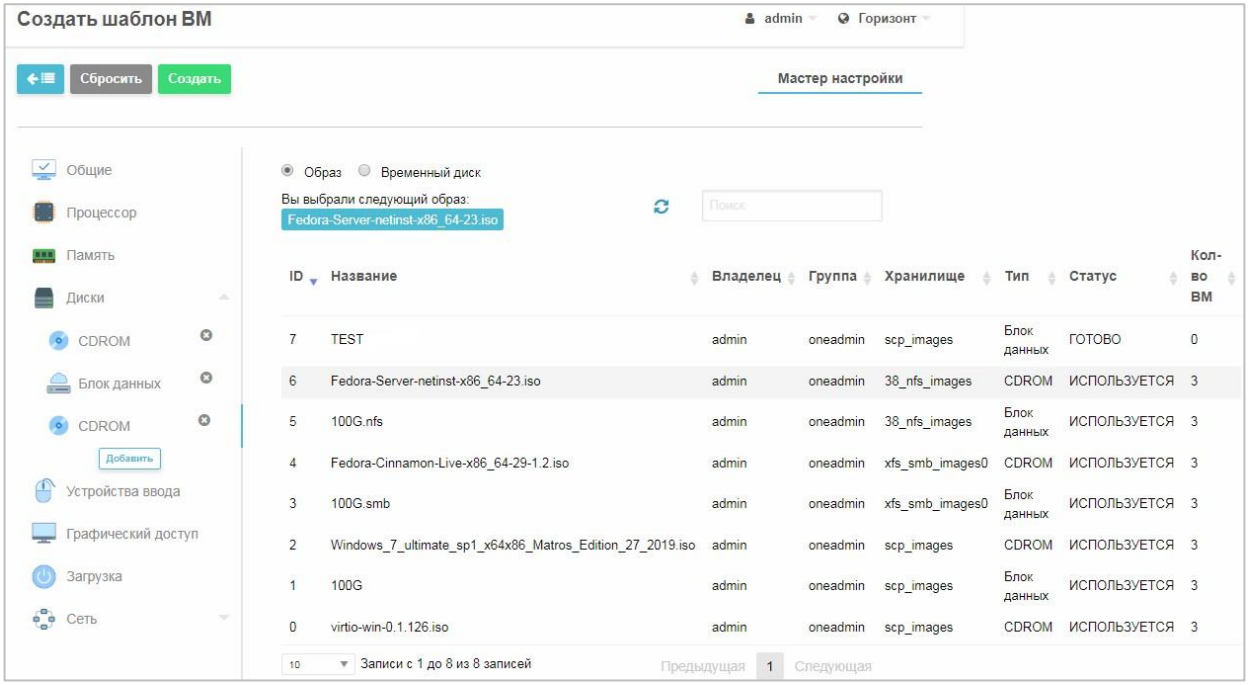


Рисунок 88 – Мастер настройки шаблона ВМ. Выбор образа диска

- при выборе образа диска типа **Блок данных** (в колонке **Тип**) вкладка второго уровня примет вид 

(Рисунок 88);
- при выборе типа образа **CD-ROM** с установочным диском гостевой ОС или другим ПО вкладка второго уровня примет вид 

;

- при выборе типа образа диска **ОС** (образа жесткого диска с установленной гостевой ОС) вкладка второго уровня примет вид ОС.

Выбранный образ отображается в строке **Вы выбрали следующий образ** (Рисунок 88).

7. На вкладке **Устройства ввода** (Рисунок 89)**:**

– в поле **Тип** выбрать тип устройства ввода: **Мышь** или **Планшетный ПК**;

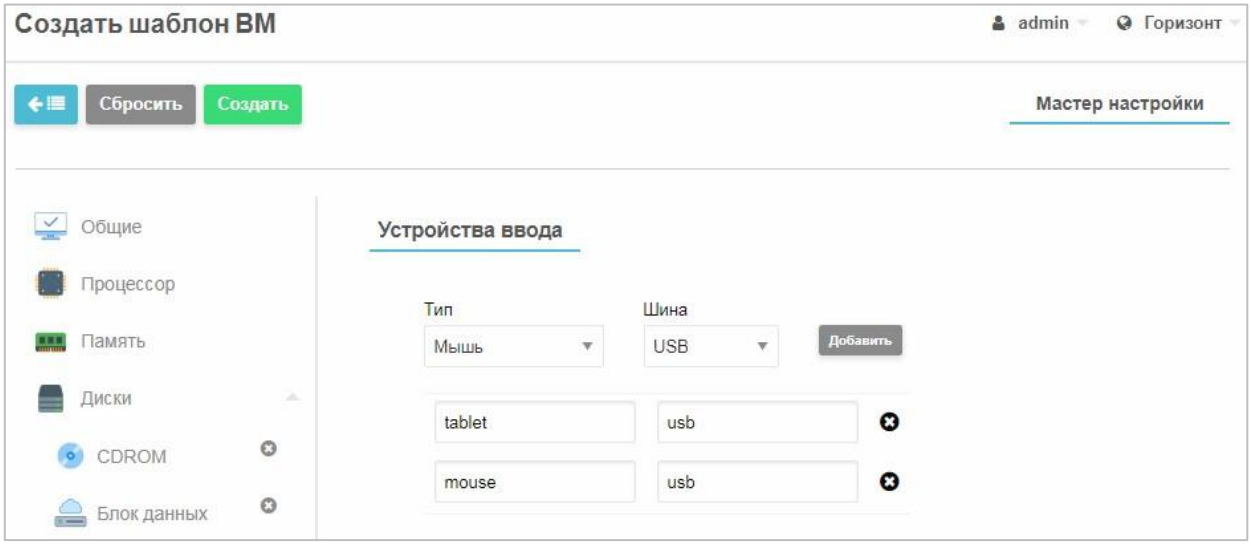


Рисунок 89 – Мастер настройки шаблона ВМ. Вкладка «Устройства ввода»

– в поле **Шина** выбрать тип подсистемы архитектуры ВМ для передачи данных: **USB** или **PS/2**;

– после ввода всех данных следует нажать кнопку **Добавить** - на экране отобразится подсоединенное к ВМ устройство ввода (Рисунок 89).

Примечание*. Рекомендуется для корректной работы манипулятора типа «мышь» на ВМ в поле* ***Тип*** *указать Планшетный ПК, в поле* ***Шина*** *– USB. После нажатия кнопки* ***Добавить*** *на экране появится подсоединенное к ВМ устройство ввода.*

8. На вкладке **Графический доступ** указывается средства графического доступа к консоли ВМ: доступ отсутствует, **VNC** или **SPICE** (Рисунок 90).

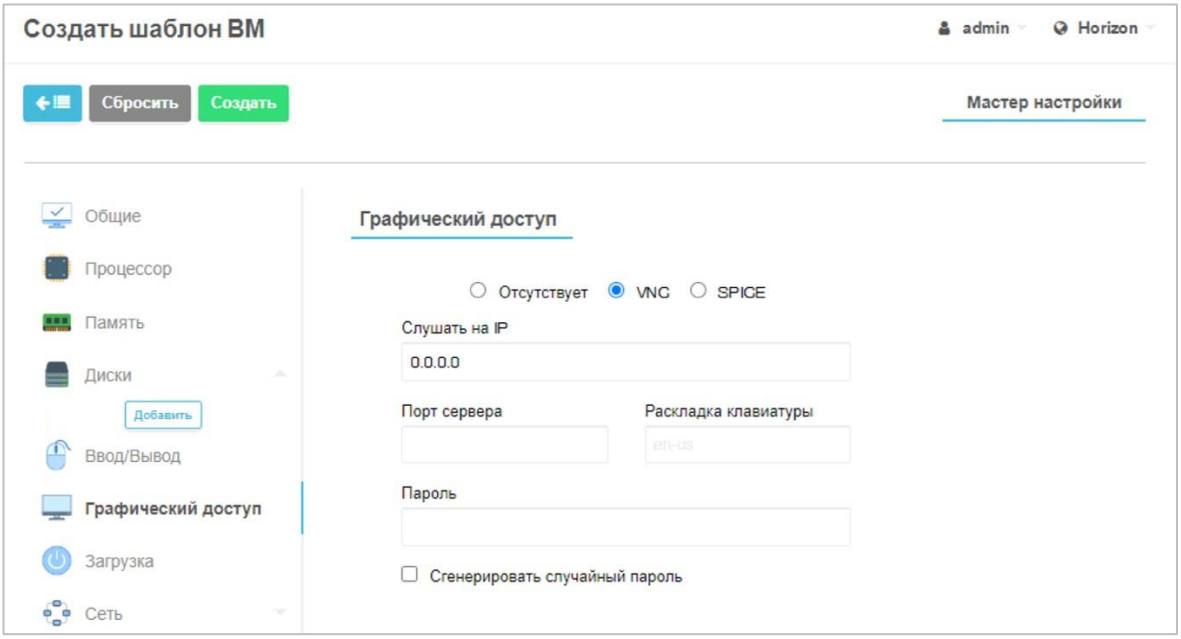


Рисунок 90 – Мастер настройки шаблона ВМ. Вкладка «Графический доступ»

Для подключения тонких клиентов через терминалы к ВМ необходимо устанавливать протокол **SPICE**. Для администрирования ВМ через вебинтерфейс СГУ желательно устанавливать протокол **VNC**.

9. На вкладке **Загрузка** (Рисунок 91) выбрать загрузочные устройства и их порядок загрузки:

- выбранные загрузочные устройства отметить флажком, а порядок их загрузки установить с помощью кнопок ;
- в поле **BIOS type** из раскрывающегося меню выбирается тип BIOS: **Legacy** или **UEFI**.

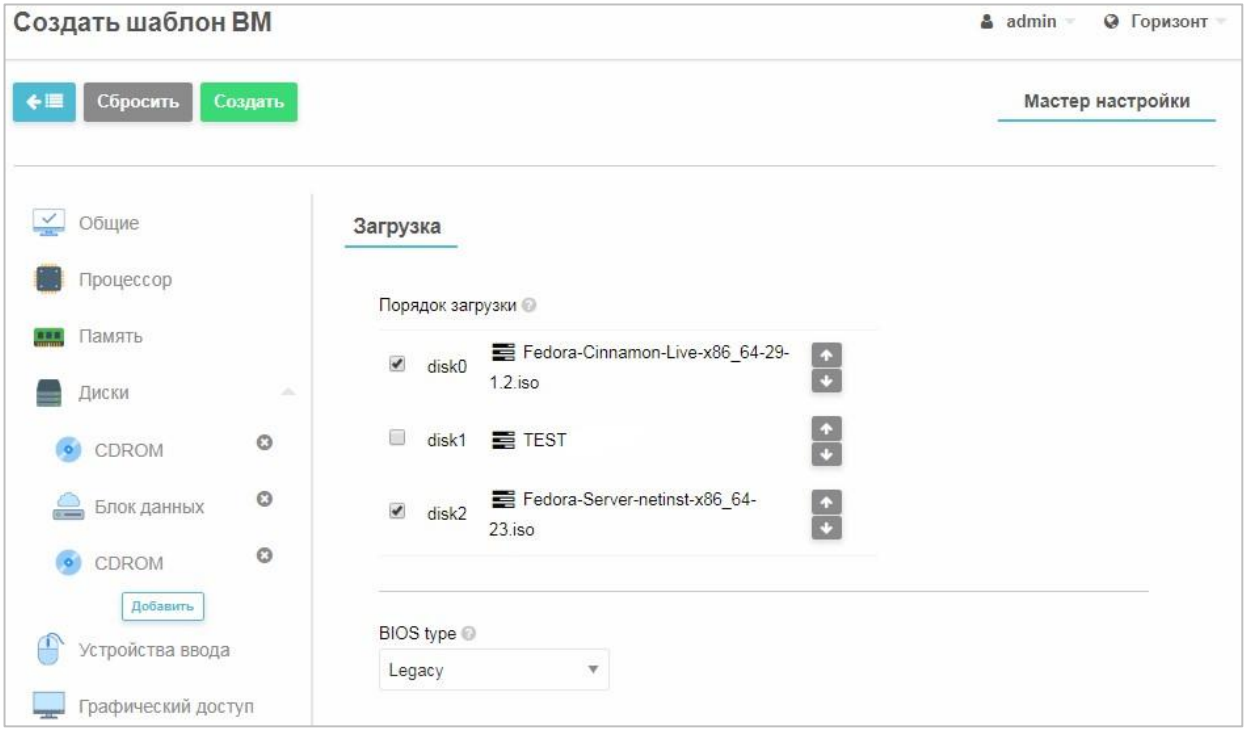


Рисунок 91 – Мастер настройки шаблона ВМ. Вкладка «Загрузка ОС»

10. На вкладке **Сеть** шаблон ВМ подключается к одной из виртуальных сетей (добавляются сетевые интерфейсы);

- нажать кнопку **Добавить**;
- нажать на появившуюся вкладку второго уровня **NIC**;
- выбрать интерфейс из созданных ранее виртуальных сетей (п. 3.2.13) (Рисунок 92).

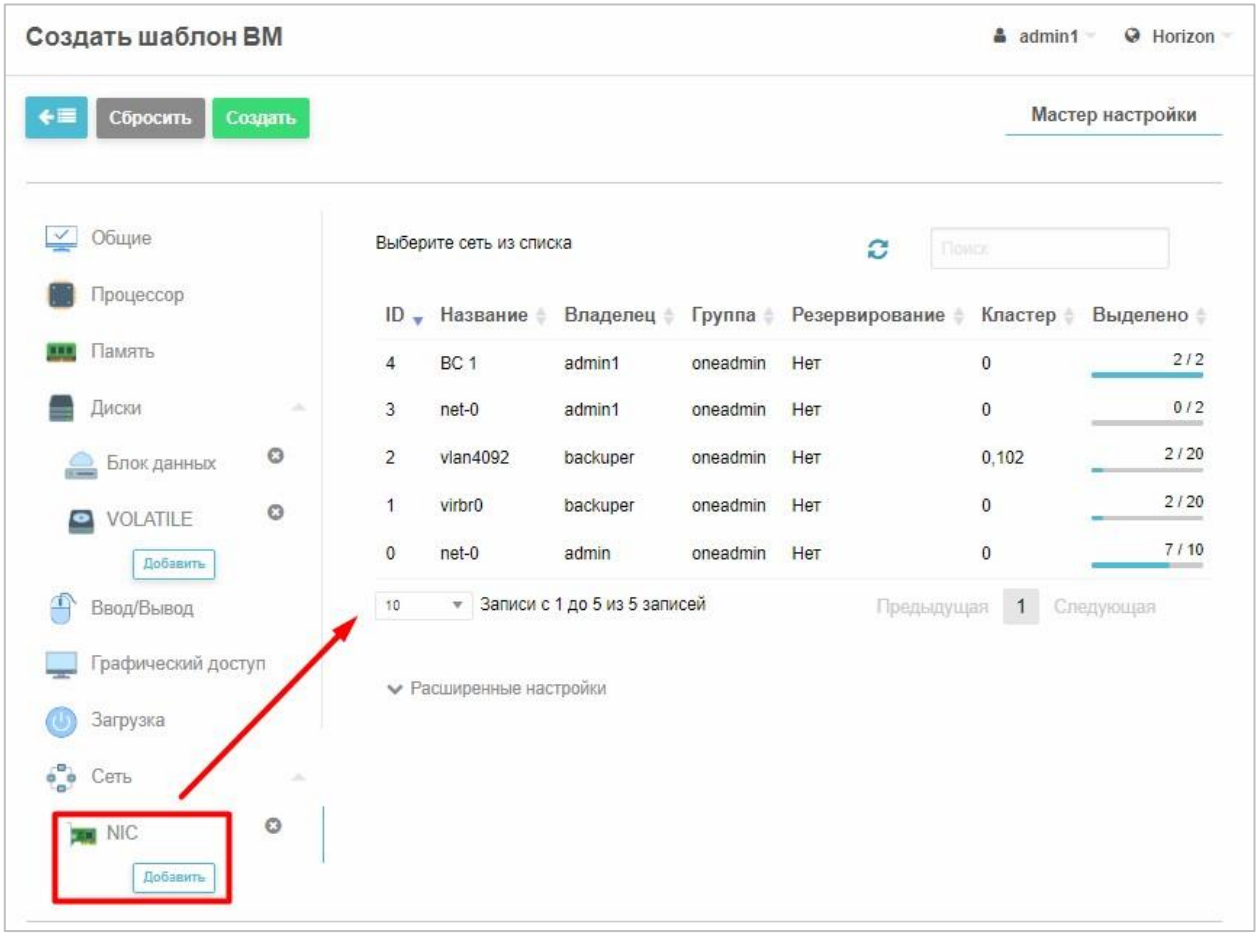


Рисунок 92 – Мастер настройки шаблона ВМ. Вкладка «Сеть»

При необходимости можно присоединить шаблон ВМ и к другим виртуальным сетям, созданным в системе. Для этого необходимо нажать кнопку **Добавить** и повторить процедуру выбора виртуальной сети.

Можно задать **Расширенные настройки**:

- выбрать дополнительную сеть;
- в области **Override Network Values IPv4** задать IP-адрес ВМ;
- **Override Network Inbound Traffic QoS** и **Override Network Outbound Traffic QoS** задать пропускную способность ВМ;
- **Аппаратное обеспечение** позволяет «пробросить» внутрь ВМ PCI устройство при установке флага PCI passthrough. Выбранный порт в поле **Имя устройства** будет браться из хостовой ОС и отображаться в гостевой ОС. Работа с этим портом будет осуществляться напрямую,

минуя среду виртуализации. Это нужно, чтобы для увеличения показателей полосы пропускания.

После этого можно создать шаблон ВМ, нажав на кнопку **Создать**.

3.2.17 Изменение конфигурации шаблонов виртуальных машин

Для изменения конфигурации шаблона ВМ необходимо в разделе **Шаблоны** → **ВМ** и выбрать нажатием шаблон.

Откроется информационное окно с параметрами шаблона ВМ (Рисунок 93).

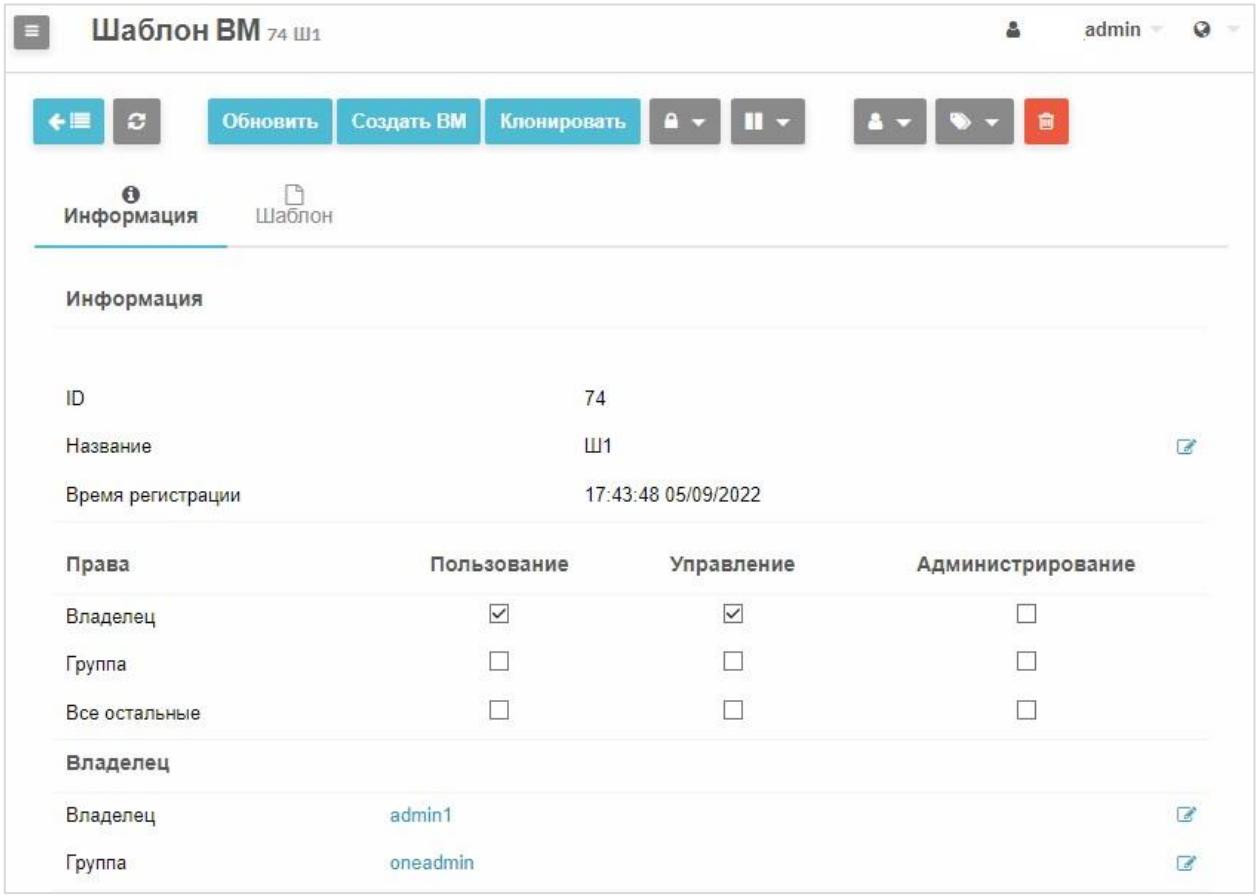


Рисунок 93 – Окно параметров шаблона ВМ

На вкладке **Информация** можно изменить название шаблона, права доступа, владельца шаблона, а также группу пользователей шаблоном.

Станет активной панель управления конфигурацией шаблона ВМ (Рисунок 94).

Рисунок 94 – Панель управления конфигурацией шаблона ВМ

С помощью панели управления шаблоном ВМ пользователь может создать ВМ на базе этого шаблона ВМ, клонировать шаблон (сделать копию шаблона), а также изменить конфигурацию шаблона.

После нажатия кнопки **Обновить** пользователь попадает в мастера изменения настройки шаблона ВМ, аналогичному мастеру создания шаблона ВМ, описанному в п. 3.2.16.

3.2.18 Создание виртуальных машин

Для создания новой ВМ необходимо наличие как минимум:

1) одного узла (проверяется в разделе **Инфраструктура** → **Узлы**).

Проверяется в разделе **Инфраструктура** → **Узлы**.

Создание узла описано в п. 3.2.7; 2) одной виртуальной сети (проверяется разделе **Сеть** → **Вирт. сети**); 3) хранилища (проверяется разделе **Инфраструктура** → **Узлы**) типа **Образы**.

Создание хранилищ описано в п. 3.2.8; 4) одной сети (в разделе **Сеть** → **Вирт. сети**).

Создание сетей описано в п. 3.2.14.

ВМ создается в разделе **Машины** → **ВМ** на основе шаблона.

Можно создать ВМ используя уже существующий шаблон (см. п. 3.2.19) или создать новый (см. п. 3.2.20).

3.2.19 Создание виртуальных машин на основе шаблона

Для создания ВМ:

1. Перейти раздел **Машины** → **ВМ**
2. Нажать кнопку  .
3. В открывшемся окне выбрать необходимый шаблон ВМ (создание шаблона описано в п. 3.2.16), на основе которого будет создана ВМ.
4. Заполнить обязательные поля:

- в поле **Имя ВМ** ввести название ВМ;
- в поле **Количество экземпляров** указать число создаваемых ВМ;

5. При необходимости, скорректировать параметры производительности и дисков.

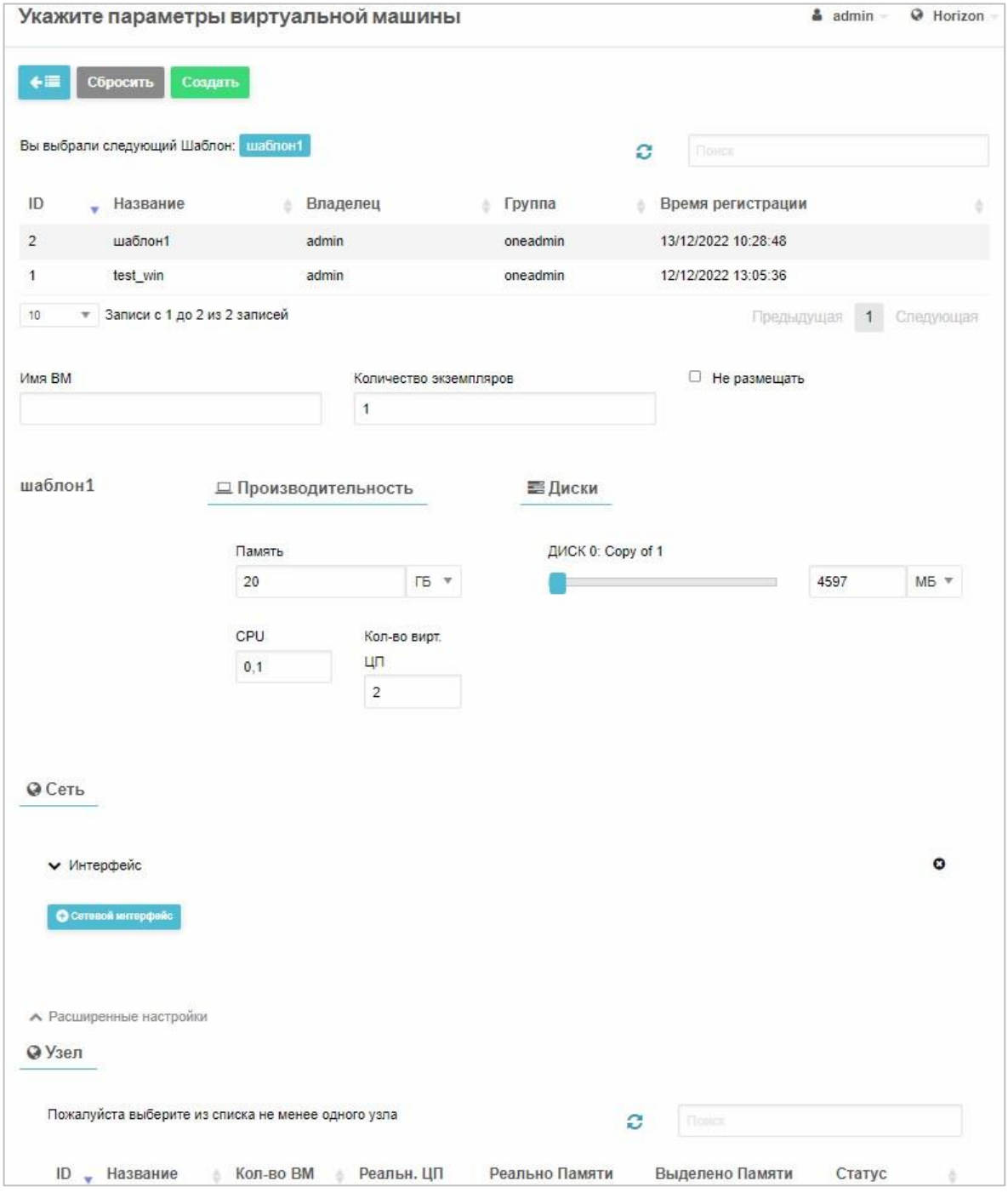


Рисунок 95 – Создание ВМ

***Примечание**. В поле **Имя ВМ** можно указать название ВМ в следующем формате: «name %i», чтобы система автоматически пронумеровала создаваемые экземпляры ВМ при количестве экземпляров больше 1.*

6. При необходимости, заполнить опциональные поля:

- **Не размещать:**

- если установлен флаг **Не размещать**, ВМ будет создана и не размещена ни на одном из серверов виртуализации. Разместить ВМ будет возможно вручную;
- если флаг **Не размещать** не установлен, то размещение ВМ на узле происходит автоматически, после чего у ВМ появится статус **Выполняется**.

***Примечание**: В Программный комплекс (ПК) «Иридиум»поддерживается динамическое распределение ВМ по серверам виртуализации. Например, при высокой загруженности одного сервера (порядка 80% объема вычислительной мощности), новая ВМ разместится на наименее загруженных узлах кластера.*

7. Если в шаблоне был указан порядок загрузки ОС с виртуального дисковода CD-ROM, то в ВМ начнется процесс установки гостевой ОС. После установки гостевой ОС на диск необходимо изменить порядок загрузки ВМ, установив первым пунктом загрузку с диска (см. п. 3.2.22.8).
8. Нажать кнопку **Создать** (Рисунок 95).

Дополнительно в разделе **Машины** → **ВМ**, панели управления можно указать метку для созданной ВМ (например, «*ВМ отдела маркетинга*») (Рисунок 96).

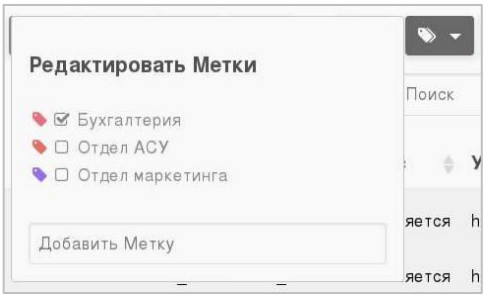


Рисунок 96 – Метки ВМ

Для работы с ВМ в отдельной вкладке браузера следует нажать на

иконку  , откроется окно рабочего стола ВМ (Рисунок 97).

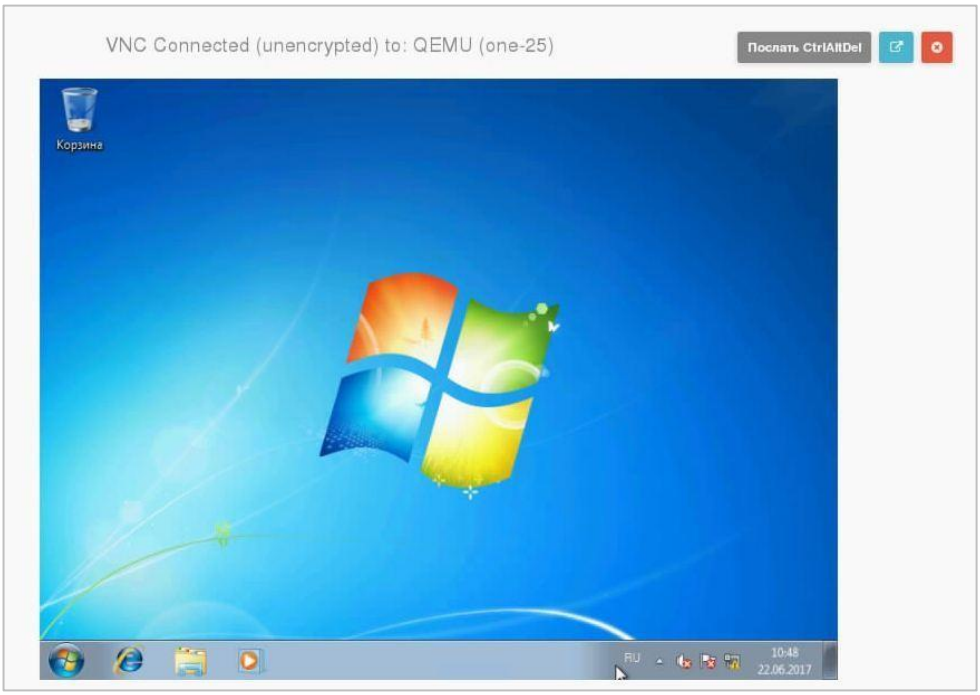


Рисунок 97 – Вид рабочего стола гостевой ОС

Подключение к экрану рабочего стола виртуального АРМ средствами СГУ обеспечивает возможность подключения сотрудников технической поддержки на любой стадии загрузки виртуальных АРМ. Возможность подключения к экрану ВМ на любой стадии функционирования обеспечивается за счет использования в ВМ виртуального видеоадаптера, вывод которого перенаправляется в виде потока протокола VNC или SPICE.

В гостевую ОС можно установить гостевые агенты для передачи информации о сбое гостевой ОС на гипервизор и последующего перезапуска:

– для гостевых ОС Debian и Ubuntu гостевые дополнения (Qemu Guest Additions) распространяются через сетевой репозиторий и устанавливаются с правами администратора root командой:

```
apt-get install qemu-guest-agent
```

– для гостевой ОС CentOS гостевые дополнения (Qemu Guest Additions)

распространяются также через сетевой репозиторий и устанавливаются с правами администратора root командой:

```
yum install qemu-guest-agent
```

– в гостевой ОС Windows запуск пакета установщика осуществляется запуском файла **qemu-ga-x86_64**. Далее следовать инструкциям «Мастера установки ПО».

3.2.20 Создание шаблона установленной виртуальной машины

После установки гостевой ОС можно создать шаблон ВМ с уже установленной ОС.

Для создания шаблона ВМ:

1. В разделе **Машины** → **ВМ** выбрать ВМ.

   Станут активными все кнопки панели управления.

2. Нажать кнопку  на панели управления ВМ.
3. В открывшемся окне ввести имя шаблона ВМ и нажать кнопку **Сохранить как шаблон** (Рисунок 98).

Рисунок 98 – Создание шаблона установленной ВМ

4. Новые образы присоединенных дисков можно сделать постоянными, установив соответствующий флаг.

***Примечания**:*

1. *При создании шаблона будут использованы текущие параметры ВМ, а не параметры базового шаблона данной ВМ.*
2. *Временные диски не могут быть сохранены, их текущее содержимое будет потеряно. Клонированный шаблон ВМ будет содержать определение пустого временного диска.*
3. *Диски и сетевые карты будут содержать только целевой образ/идентификатор сети. Если шаблон требует дополнительной настройки, то необходимо обновить его.*

3.2.21 Кнопки управления виртуальной машиной

При выборе одной и более ВМ (Рисунок 99) в разделе **Машины → ВМ** становится активной панель управления ВМ. Осуществлять управление возможно, как отдельной ВМ, так и предварительной выделенной группой ВМ.

Рисунок 99 – Панель управления ВМ

Подробно функционал описан в таблице ниже ().

Таблица 6 – Команды панели управления ВМ

Кнопка	Функция	Описание
	Создание новой ВМ (активна всегда)	Открывается страницу интерфейса создания новой ВМ.
	Обновление текущей страницы (активна всегда)	После внесения каких-либо изменений в работу ВМ или ее конфигурацию необходимо выполнить обновление страницы, чтобы увидеть изменения.
	Создание шаблона ВМ на базе существующей ВМ	Позволяет создать шаблон с параметрами и конфигурацией существующей ВМ. ***Примечание**. ВМ во время создания шаблона должна быть выключена.*
	Запуск ВМ	На ВМ инициализируется запуск гостевой ОС.
	Выпадающее меню:	

	Администрирование	Операции, которые не изменяют ресурс (например, использование образа или виртуальной сети). Подобные операции должны назначаться только пользователям с ролью администратора
	Управление	Операции, изменяющие ресурс (например, остановка ВМ, изменение атрибута образа виртуального диска на «постоянный» и т.д.);
	Пользование	Специальные операции (например, создание/удаление ролей, изменение параметров узлов и кластеров). Данные операции должны назначаться только пользователям с ролью администратора.
	Unlock	Разблокирование всех возможных операций с ресурсом
	**Выпадающее меню:**	
	Приостановить работу ВМ	Работа ВМ приостанавливается. ВМ может быть запущена в любой момент времени с текущего состояния до приостановки работы ВМ.
	Остановить	Работа ВМ останавливается. Оперативная память записывается на жесткий диск. Работа ВМ может быть запущена в любой момент времени с текущего состояния до остановки ВМ.
	**Выпадающее меню:**	
	Отключить питание	Корректное выключение ВМ из системы группового управления

	Отключить питание жесткий	Принудительное отключение питания ВМ. Отключение питания ВМ из системы группового управления (аналогично некорректному выключению физической машины посредством отключения питания из сети).
	Отменить размещение	ВМ снимается с узла и сохраняется в хранилище в виде файла-образа ВМ с возможностью восстановления. Восстановление ВМ осуществляется непосредственно размещением ее на серверном узле или нажатием кнопки запуска ВМ (в этом случае происходит автоматическое размещение ВМ на узле)
	Отменить размещение жесткий	ВМ снимается с узла и сохраняется на физическом сервере в виде файла-образа ВМ с возможностью

		восстановления. Восстановление ВМ происходит так, как будто она создается заново. Происходит ее размещение на узле.
	**Выпадающее меню:**	
	Перезагрузка	Корректная перезагрузка гостевой ОС на ВМ (аналогична перезагрузки из меню «Пуск»)
	Перезагрузка жесткий	Принудительная перезагрузка гостевой ОС на ВМ (аналогична перезагрузке через кнопку «reset»)
	**Выпадающее меню:**	
	Разместить на узле	Ручное размещение ВМ на узле с возможностью выбора узла размещения.
	Перенести ВМ с приостановкой	При миграции ВМ будет остановлена
	Перенести ВМ без приостановки	Горячая миграция ВМ между узлами
	Запретить размещение	Запретить размещать ВМ на узле

	Восстановить	ювление ВМ. При выборе) пункта отрывается окно с выпада писком с опциями: – повторить – сообщить СГУ о необходимости повторения предыдущей команды; – успешно – сообщить СГУ о корректности выполнения предыдущей команды; – не выполнено – сообщить СГУ о невыполнении предыдущей команды; – удалить – удаляет ВМ из системы; – удалить и создать повторно – удаляет ВМ из системы, а затем корректно
		развертывает в системе аналогичную ВМ.
	Выпадающее меню:	
	Сменить владельца	Позволяет сменить пользователя ВМ
	Сменить группу	Позволяет сменить группу пользователей

	Редактировать метки	Для удобства управления ВМ в системе группового управления предусмотрены метки, которые позволяют группировать и выводить списки виртуальных машин по их типу или функциональному предназначению. *Например: ВМ бухгалтерии, ВМ отдела АСУ и т.д.*
	**Выпадающее меню**	
	Terminate	Корректное удаление ВМ из системы
	Terminate жесткий	Принудительное удаление ВМ из системы
	Доступ к ВМ по протоколу SPICE (если настроен)	Доступны только в окне просмотра и редактирования ВМ
	Доступ к ВМ по протоколу VNC (если настроен)	

3.2.22 Просмотр и редактирование параметров виртуальной машины

Для изменения параметров ВМ необходимо перейти в раздел **Машины** → **ВМ** и выбрать ВМ нажатием.

Откроется окно со вкладками параметров, информацией и данными виртуальной машины (Рисунок 100), при этом останутся доступны элементы панели управления, описанной в п. 3.2.21.

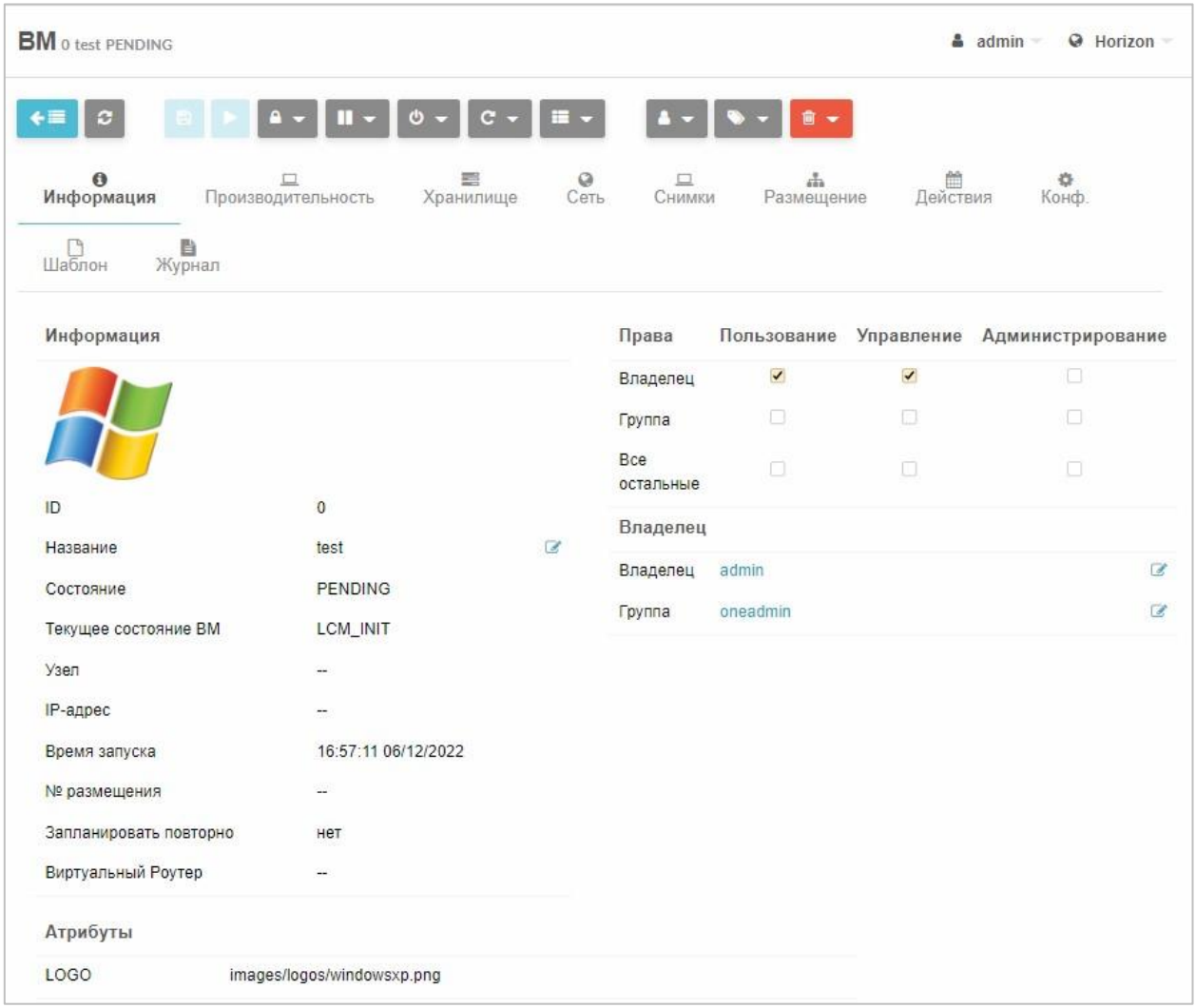


Рисунок 100 – Вкладка «Информация»

3.2.22.1 Вкладка «Информация»

На вкладке **Информация** выводятся общие данные о работе ВМ: логотип ОС, номер ВМ в системе (поле ID), состояние, текущее состояние ВМ, IP-адрес узла размещения, IP-адрес ВМ, время запуска, запланирован ли повторный запуск, адрес виртуального роутера; информация о владельце ВМ и права пользователей – для отклбченной ВМ.

Возможные состояния образов перечислены в приложении (ПРИЛОЖЕНИЕ Б).

На вкладке **Информация** можно изменить:

– название ВМ;

- права пользователей данной ВМ (для отключенной ВМ);
- владельца ВМ (для отключенной ВМ);
- группу пользователей (для отключенной ВМ).

Для изменения названия ВМ необходимо напротив параметра **Название** и нажать и в появившемся поле ввести новое название.

Для отключенной ВМ на вкладке **Информация** представлена матрица дискреционного разграничения прав доступа к ВМ: пользования, управления, администрирования.

Соответствующее право доступа может быть предоставлено:

- владельцу ВМ (**Владелец**);
- группе пользователей (**Группа**) всем пользователям, зарегистрированным в СГУ (**Все остальные**).

Для изменения прав доступа необходимо установить/снять флаг в соответствующем поле (Рисунок 101).

Права	Пользование	Управление	Администрирование
Владелец	☑	☑	☐
Группа	☐	☐	☐
Все остальные	☐	☐	☐

Рисунок 101 – Настройка прав доступа

Пользователям могут быть назначены следующие виды доступа к ресурсам:

- **пользование** – данные операции не изменяют ресурс (например, использование образа или виртуальной сети);
- **управление** – операции, изменяющие ресурс (например, остановка ВМ, изменение атрибута образа виртуального диска на «постоянный» и т.д.);
- **администрирование** – специальные операции (например, создание/удаление ролей, изменение параметров узлов и кластеров).

***Примечание**. Данные операции должны назначаться только пользователям с ролью администратора.*

В разделе **Владелец** представлен владелец ВМ и группа пользователей, которым могут быть назначены права доступа к ВМ. По умолчанию в поле **Группа** стоит название группы, к которой принадлежит пользователь (Рисунок 102).

Рисунок 102 – Раздел «Владелец»

Для изменения владельца ВМ или группы пользователей ВМ, необходимо нажать и выбрать из выпадающего списка новый параметр.

3.2.22.2 Вкладка «Производительность»

На вкладке **Производительность** в виде графика представлен мониторинг реального использования процента процессорного времени и оперативной памяти по сравнению с выделенными параметрами для работы ВМ и базовые характеристики ВМ: память, количество процессоров, процент процессорного времени ЦП (Рисунок 103).

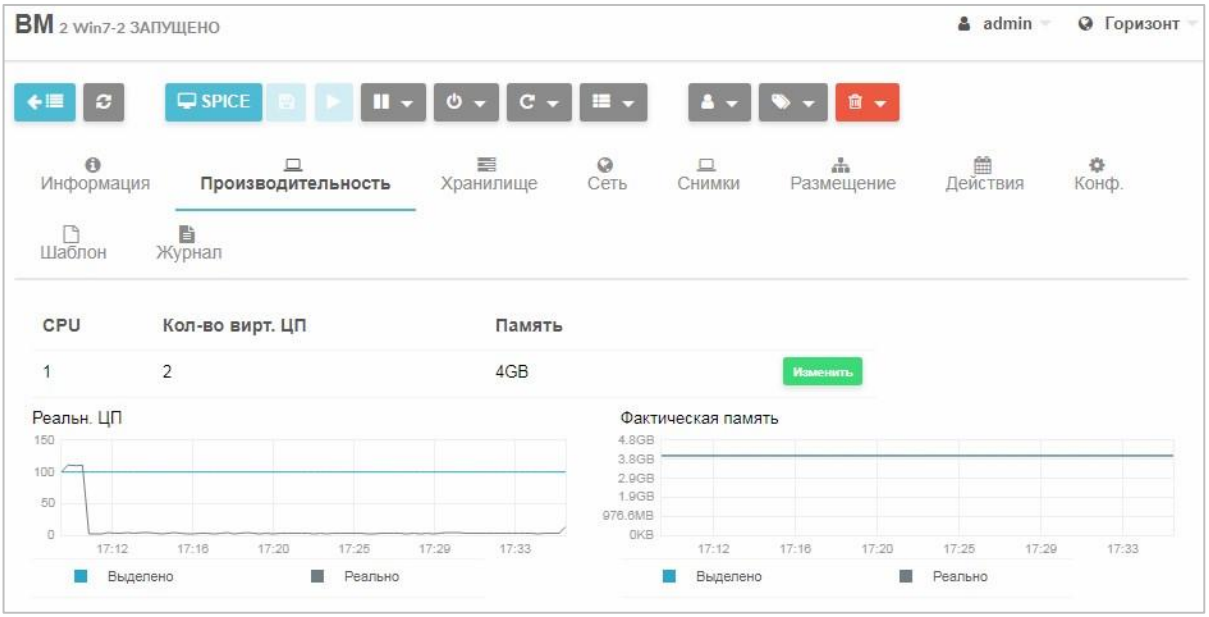


Рисунок 103 – Вкладка «Производительность»

Можно изменить базовые характеристики ВМ.

***Примечание**: Виртуальная машина во время изменения базовых характеристик должна быть выключена.*

Для изменения характеристик производительности ВМ:

1. Нажать на кнопку **Изменить**.

   Откроется окно **Изменить базовые характеристики** (Рисунок 104).
2. Внести новые параметры ВМ: объем оперативной памяти, процент процессорного времени ЦП, количество виртуальных ЦП, сокеты, ядра, потоки;
3. Нажать кнопку **Изменить**.

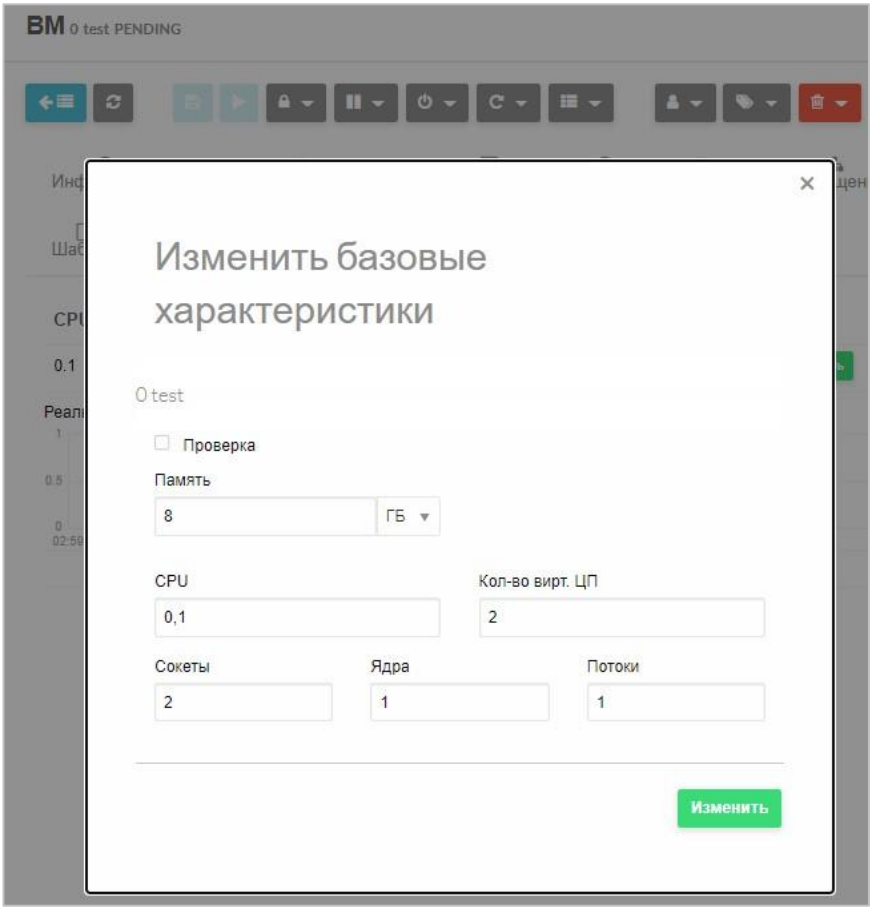


Рисунок 104 – Изменение базовых характеристик

3.2.22.3 Вкладка «Хранилище»

На вкладке **Хранилище** представлены подключенные к МВ ресурсы (пустые образы жестких дисков, CDROM-образы, образы ОС, временные диски).

В нижней части вкладки **Хранилище** в виде графика представлен мониторинг взаимодействия ВМ с дисковой подсистемой: скорость чтения (RDBytes) и записи (WRBytes) на жесткий диск байт в секунду и количество операций ввода/вывода в секунду (IOPS) при чтении (RDIOPS) и записи (WRIOPS) информации на жесткий диск (Рисунок 105).

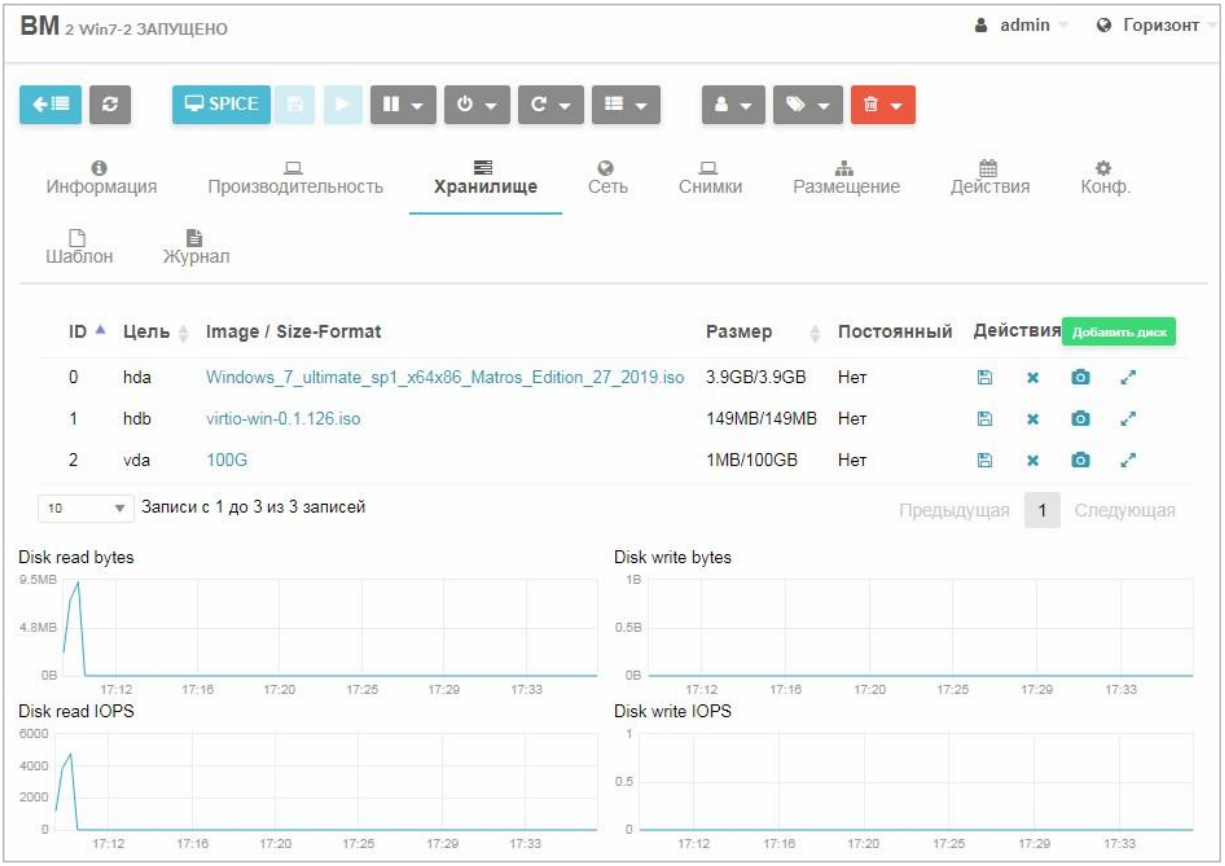


Рисунок 105 - Вкладка «Хранилище»

Пользователь может добавлять, удалять, редактировать ресурсы.

Для присоединения дополнительного ресурса:

1. Нажать кнопку **Добавить диск**.
2. В открывшемся окне **Присоединить диск** (Рисунок 106).

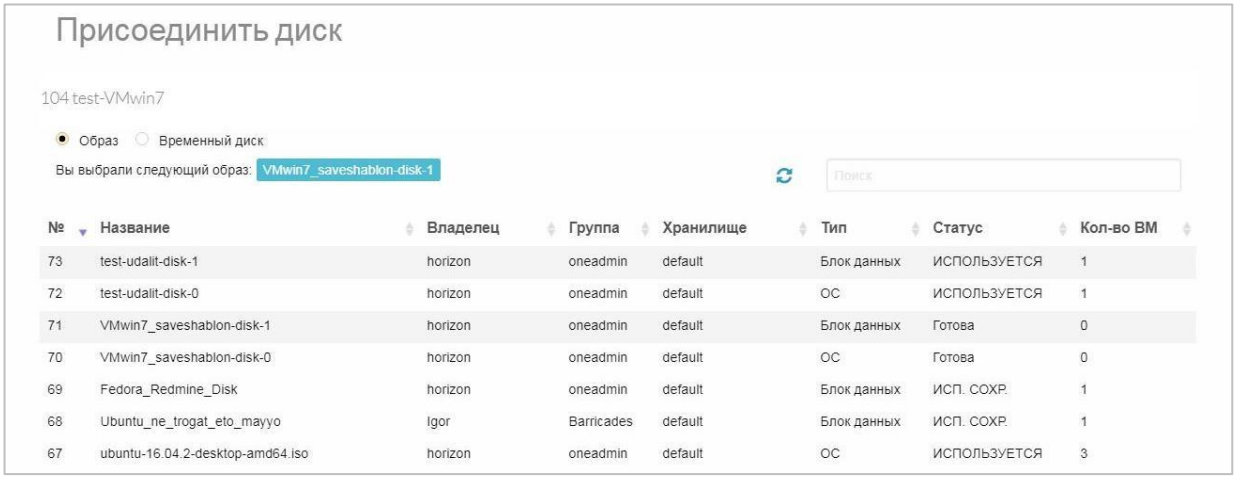


Рисунок 106 – Присоединить диск к ВМ

3. Выбрать образ из списка.
4. Нажать кнопку **Присоединить**.
5. Нажать Расширенные настройки:

– В секции **IO throttiling (IOPS)** можно заполнить поля **IOPS чтения** и **IOPS записи в сек** для обозначения максимальных значений потоков чтения и записи, выражаемых в IOPS и в байт/сек. Возможно задать как суммарные значения ограничений, так и значения ограничений для каждого потока в отдельности.

Для совершения дополнительных действий над присоединенными ресурсами к ВМ необходимо в столбце **Действия** (Рисунок 105) выбрать одну из опций:

– – создание образа диска из одного из ресурсов ВМ (подробнее см. п.3.2.22.3.1);

– – удаления диска; создание снимка из одного из дисков

– (подробнее см. п.3.2.22.3.2);

– – изменение объема дискового пространства (подробнее см. п. 3.2.22.3.3).

***Примечание**: опция активна только при выключенной ВМ.*

3.2.22.3.1 Создание образа диска из одного из ресурсов ВМ

Для создания образа диска из одного из исполняемых жестких дисков ВМ:

1. Активировать опцию  в строке исходного жесткого диска (Рисунок 105).

   Откроется окно создания образа (Рисунок 107).

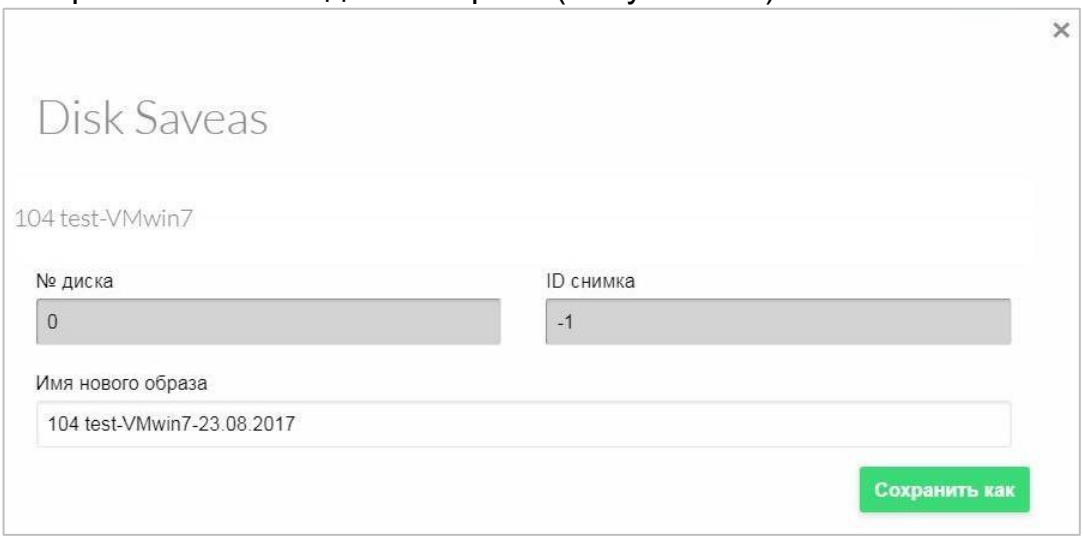


Рисунок 107 - Сохранение жесткого диска

2. Ввести имя нового образа диска.
3. Нажать кнопку **Сохранить как.**

В разделе СГУ **Хранилище** → **Образы ВМ** разместится новый образ жесткого диска.

3.2.22.3.2 Создание снимка диска ВМ

Для создания снимка диска ВМ

4. Перейти во вкладку **Хранилище**, а затем нажать кнопку  напротив диска, для которого нужно сделать снимок.

   На экране откроется окно **Снимок диска** (Рисунок 108).

5. Ввести имя снимка.

6. Нажать кнопку **Сделать снимок**.

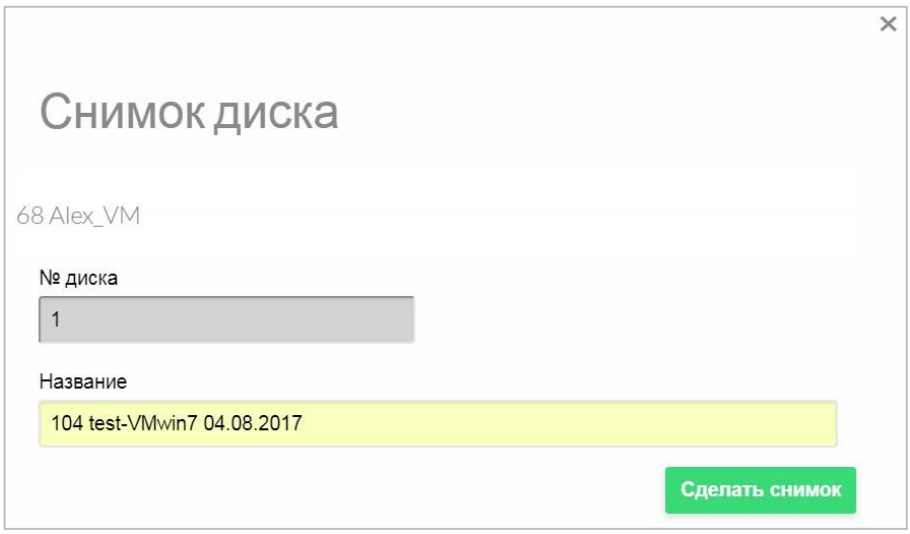


Рисунок 108 - Снимок диска

В таблице на вкладке **Хранилище** диск, с которого был сделан снимок, будет отмечен знаком .

Для просмотра информации о сделанном снимке нажать на диск (Рисунок 109).

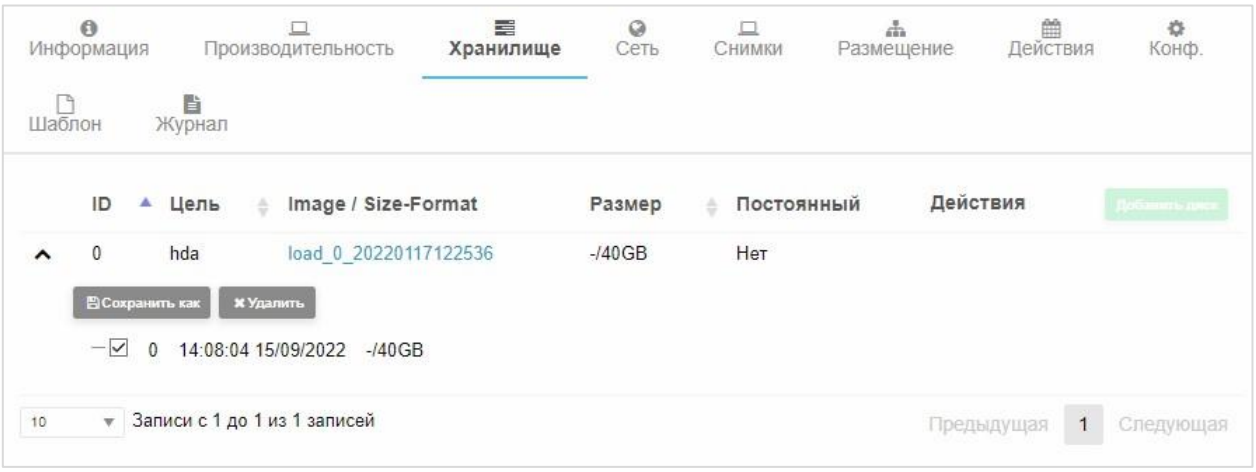


Рисунок 109 - Работа со снимком диска

Для сделанного снимка доступны следующие операции:

– сделать образ диска на основе снимка, нажав кнопку **Сохранить как**; – удалить снимок, нажав кнопку **Удалить**.

3.2.22.3.3 Изменение объема дискового пространства

Для изменения объема дискового пространства (*опция активна только при выключенной ВМ*):

7. Нажать  в строке изменяемого жесткого диска.

Откроется окно изменения дискового пространства (Рисунок 110). 8. С помощью ползунка установить размер диска и

9. Нажать кнопку **Применить**.

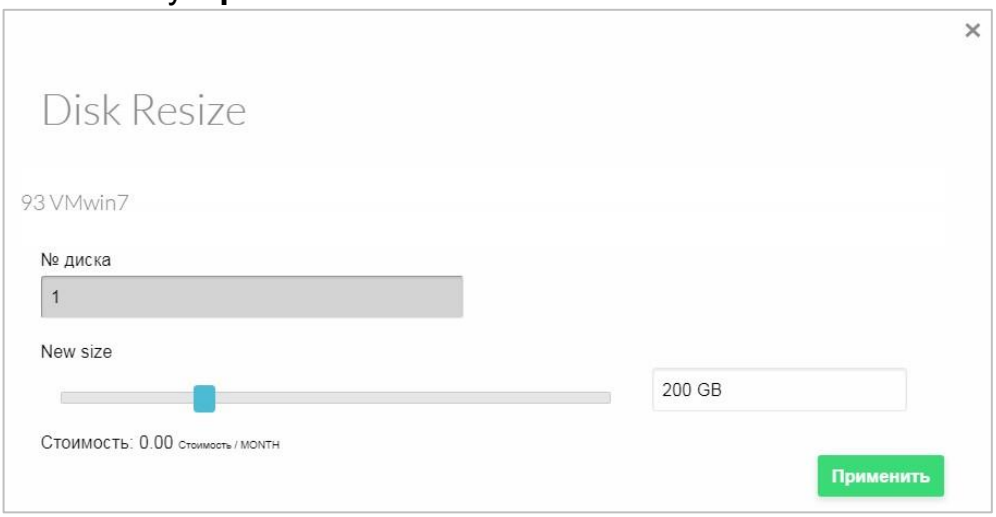


Рисунок 110– Окно изменения дискового пространства

На вкладке **Хранилище** может удостовериться, что у выбранного диска изменился объем согласно введенному параметру.

3.2.22.4 Вкладка «Сеть»

На вкладке **Сеть** возможно добавить или отсоединить сетевой интерфейс (Рисунок 111).

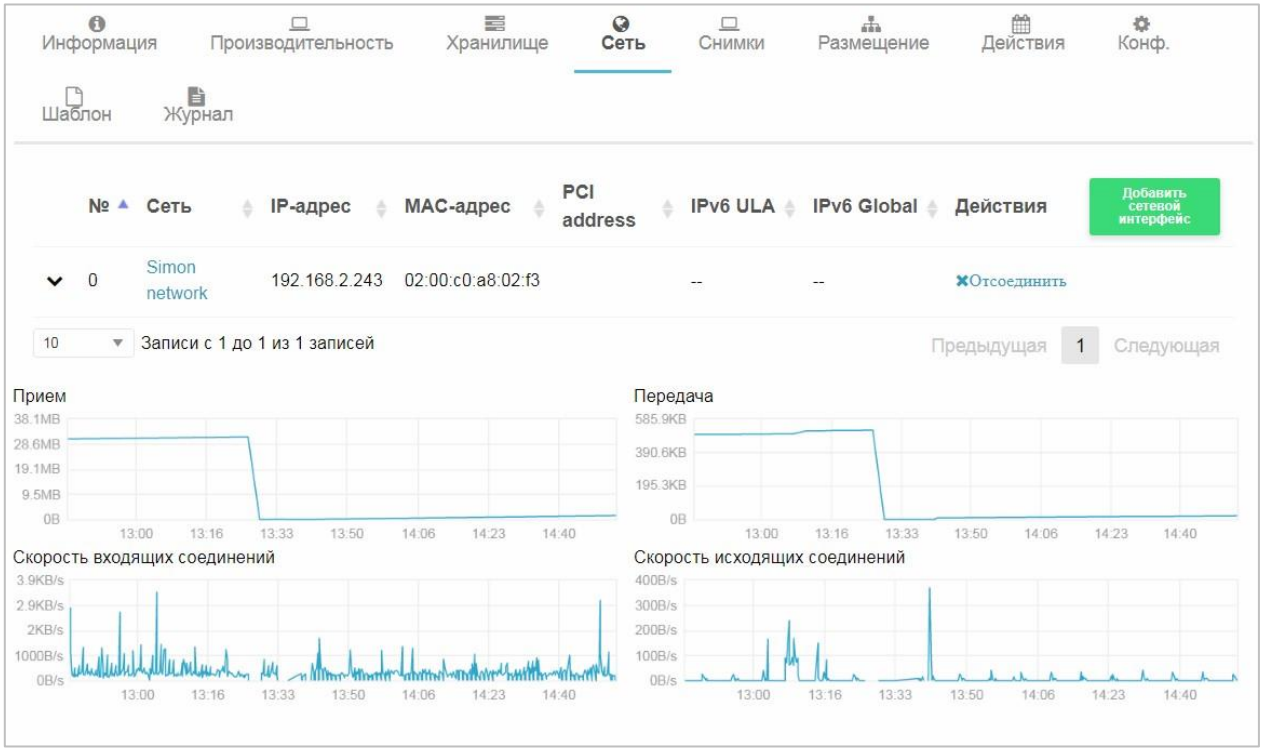


Рисунок 111– Вкладка «Сеть»

Для добавления нового сетевого интерфейса:

10. Нажать кнопку **Добавить сетевой интерфейс**.

    Откроется окно **Добавить сетевой интерфейс** (Рисунок 112).

11. Выбрать из списка не менее одного сетевого интерфейса.

12. Нажать кнопку **Присоединить**.

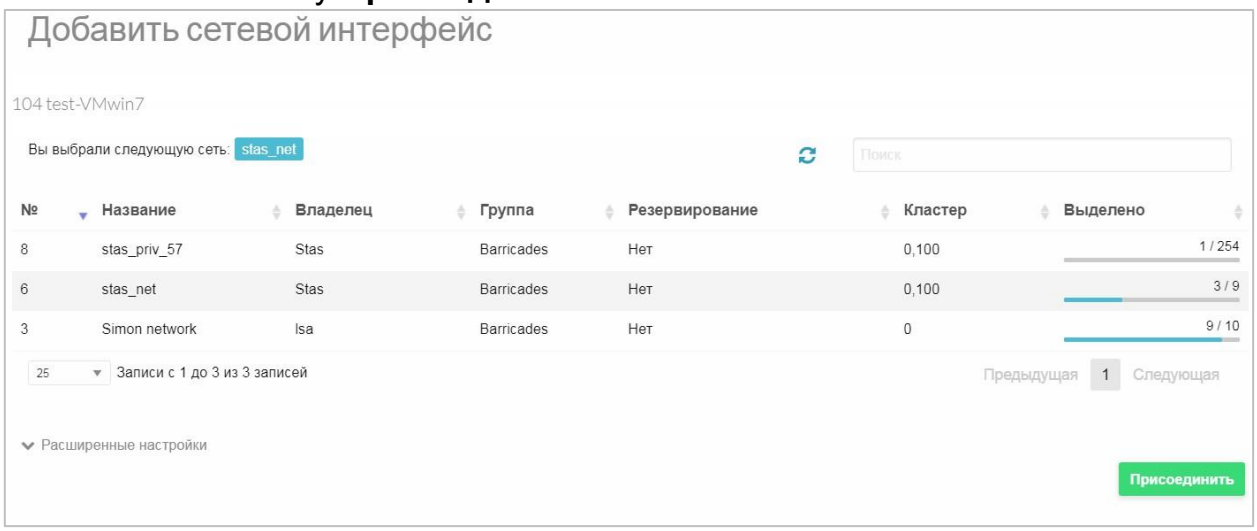


Рисунок 112 – Добавить сетевой интерфейс в ВМ

Для отсоединения сетевого интерфейса необходимо в столбце со списком присоединенных интерфейсов (Рисунок 111) выбрать опцию **Отсоединить**.

В нижней части вкладки **Сеть** в виде графика представлен мониторинг работы сети: прием и передача данных (KB, MB), скорость входящих и исходящих соединений (B/s).

3.2.22.5 Вкладка «Снимки»

На вкладке **Снимки** возможно создавать, удалять и восстанавливать снимки, или снапшоты работающих ВМ. Снимок будет содержать текущие диски и состояние памяти ВМ.

***Примечания**:*

1. *Снимки теряются, если выполняется какая-либо операция жизненного цикла ВМ, например, приостановить, перенести, удалить запрос.*
2. *Снимки доступны только в том случае, если все диски виртуальной машины используют драйвер qcow2.*

Для создания снимка ВМ необходимо нажать кнопку **Сделать снимок**, в открывшемся окне ввести имя снимка и дождаться, когда он будет размещен в системе (Рисунок 113).

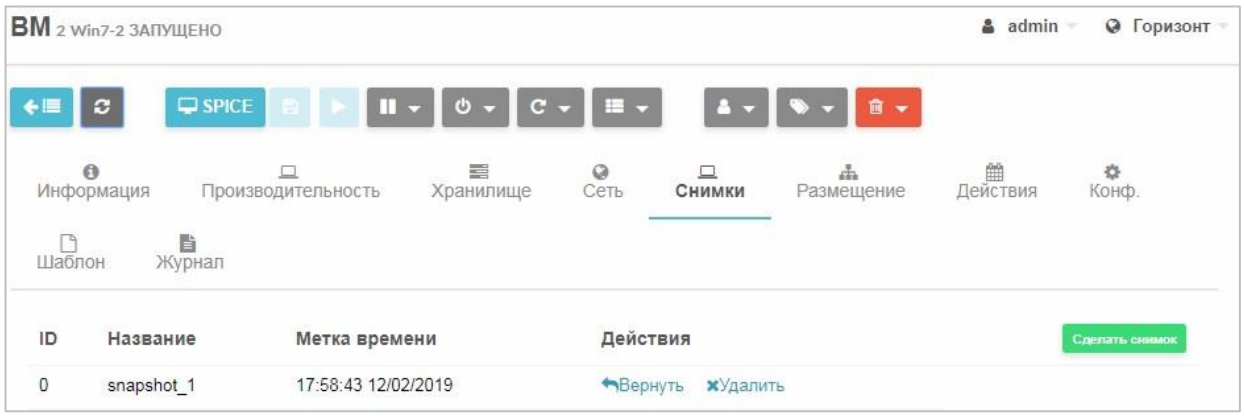


Рисунок 113 – Создание снимков ВМ

После этого будут доступен возврат ВМ к состоянию на момент создания снимка путем нажатия кнопки **Вернуть**. Для удаления снимка необходимо нажать кнопку **Удалить**.

3.2.22.6 Вкладка «Размещение»

На вкладке **Размещение** есть возможность просмотреть историю размещения ВМ на том или ином узле, какие действия были произведены с ВМ, указано в какое время было произведено изменение. Также доступно время пролога и общее время работы ВМ на данном узле.

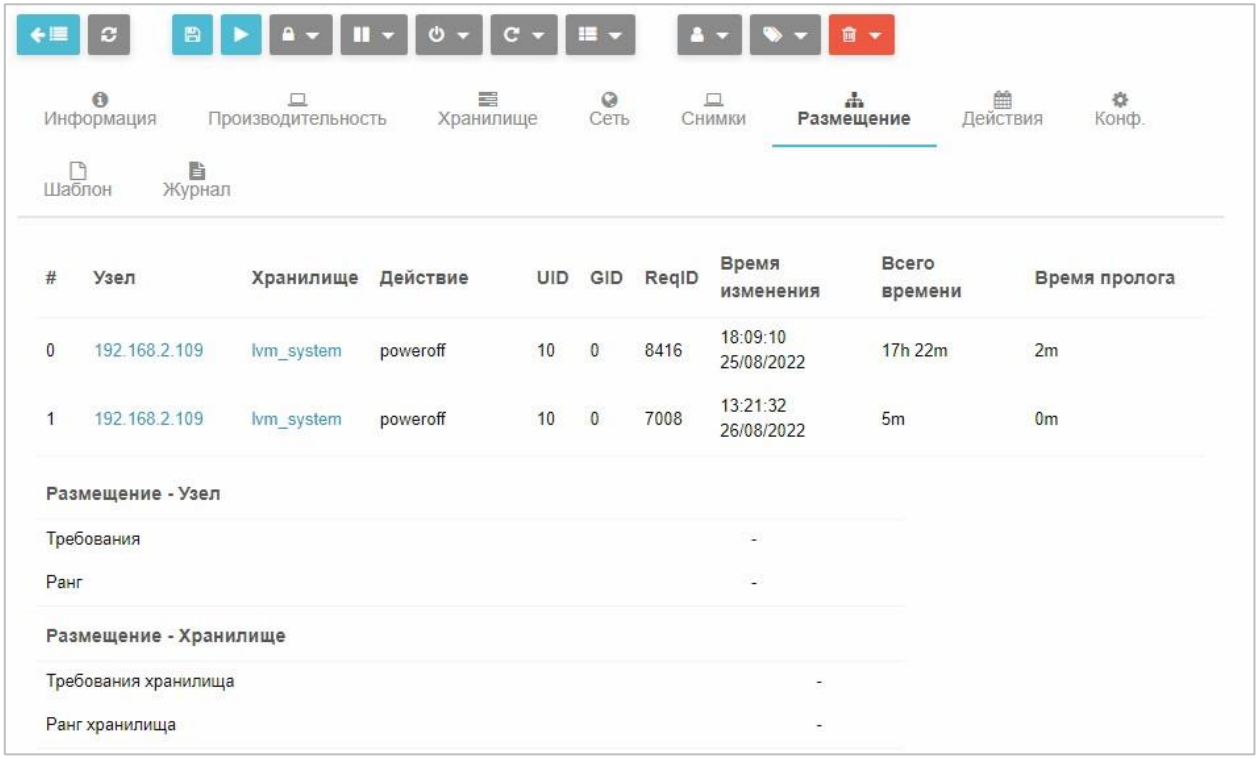


Рисунок 114 – Вкладка «Размещение»

3.2.22.7 Вкладка «Действия»

На вкладке **Действия** есть возможность запланировать ряд отложенных действий над ВМ, которые будут выполнены в автоматическом режиме.

Для планирования действия:

13. Нажать кнопку **Добавить действие**.

На экране появится выпадающее меню с выбором действий (Рисунок 115).

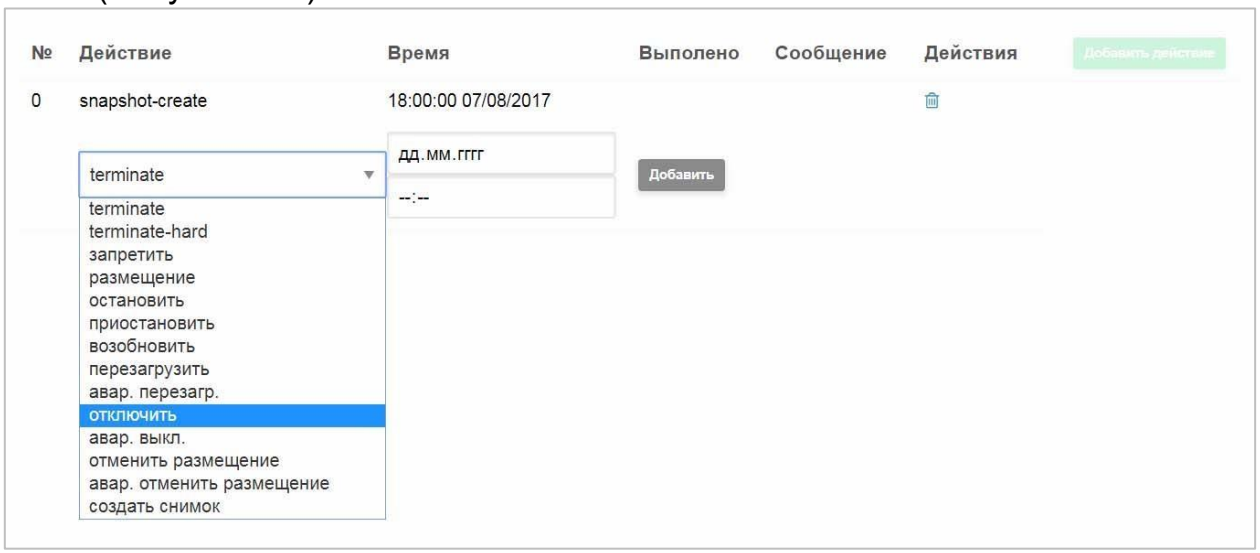


Рисунок 115 – Добавление действий

14. Выбрать требуемое действие, установить дату и время его выполнени.
15. Нажать кнопку **Добавить**.

    На странице появится запись о запланированном действии и времени его исполнения (Рисунок 116).

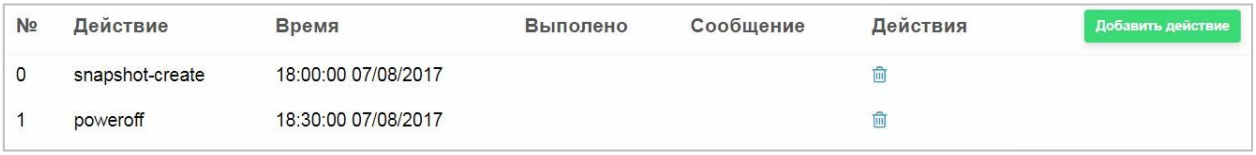


Рисунок 116 – Запись о запланированном действии и времени его исполнения

Для планирования нескольких действий необходимо повторить процедуру добавления действия.

3.2.22.8 Вкладка «Конфигурация»

На вкладке **Конф.** можно изменить конфигурацию ВМ (Рисунок 117).

***Примечание**: при изменении конфигурации ВМ должна быть выключена.*

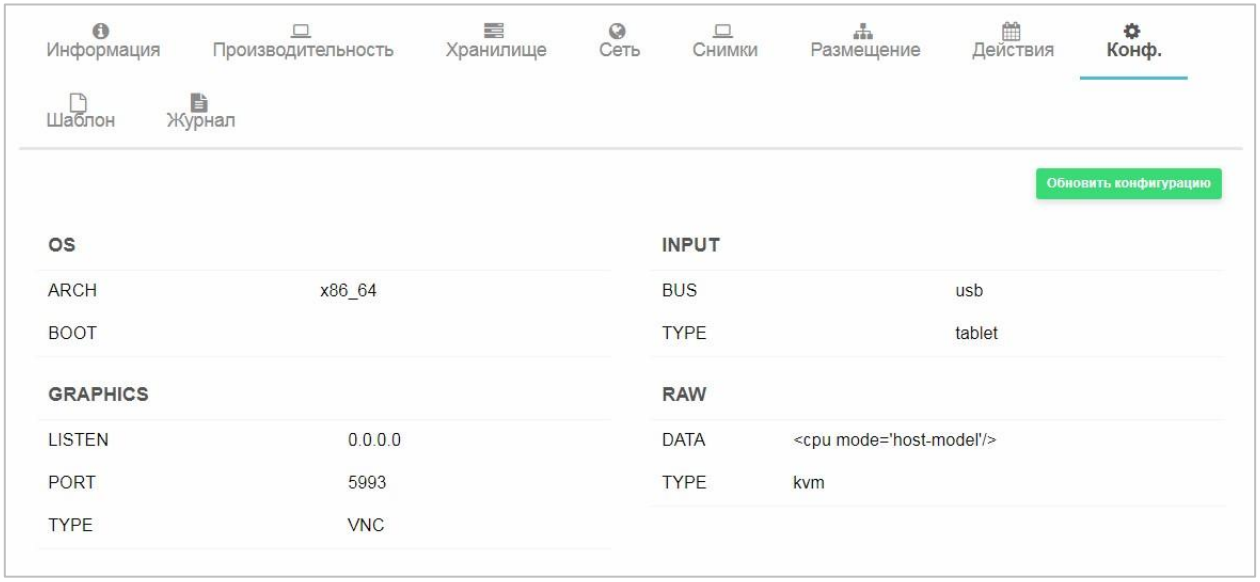


Рисунок 117 - Вкладка «Конфигурация»

Для изменения конфигурации ВМ:

16. Нажать на кнопку **Обновить конфигурацию** (Рисунок 117).

    Откроется мастер настройки изменения конфигурации ВМ (Рисунок 118).

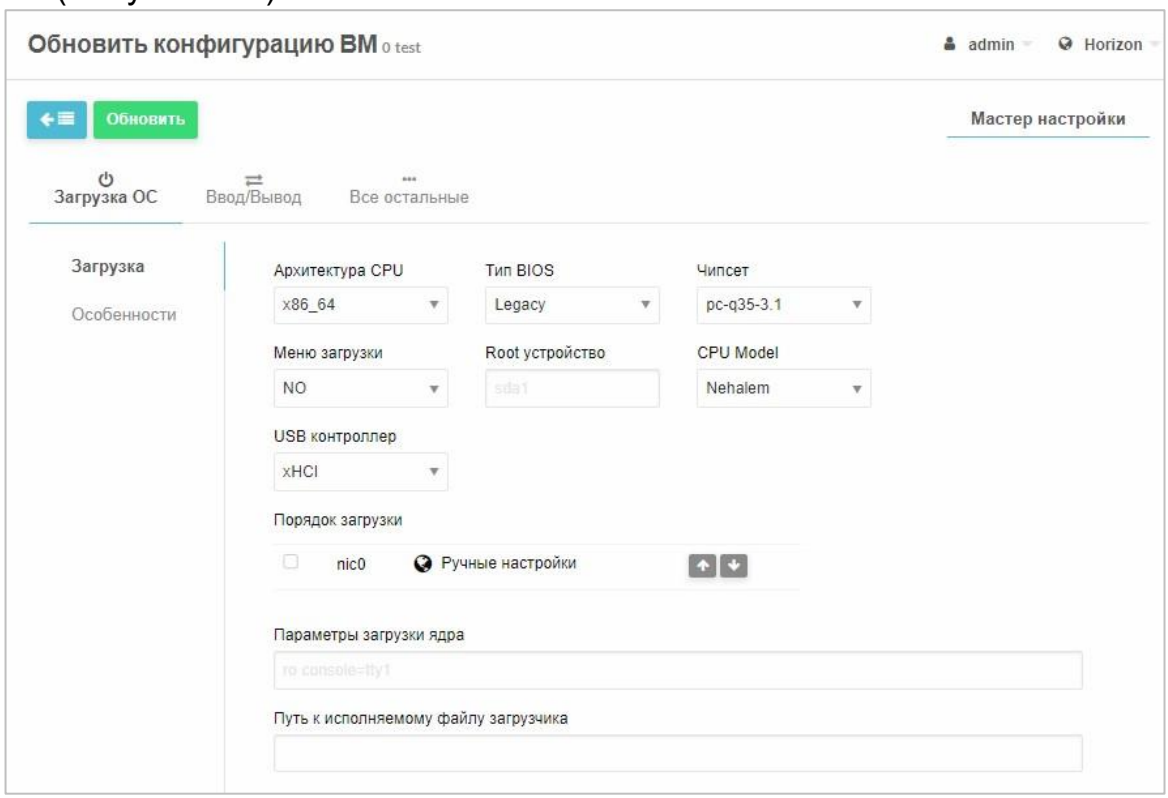


Рисунок 118 – Изменение конфигурации ВМ. Загрузка ОС

17. На вкладке **Загрузка ОС** можно поменять архитектуру CPU и изменить порядок загрузки (Рисунок 118).
18. На вкладке **Ввод/Вывод** поменять графический доступ и устройства ввода (Рисунок 119).

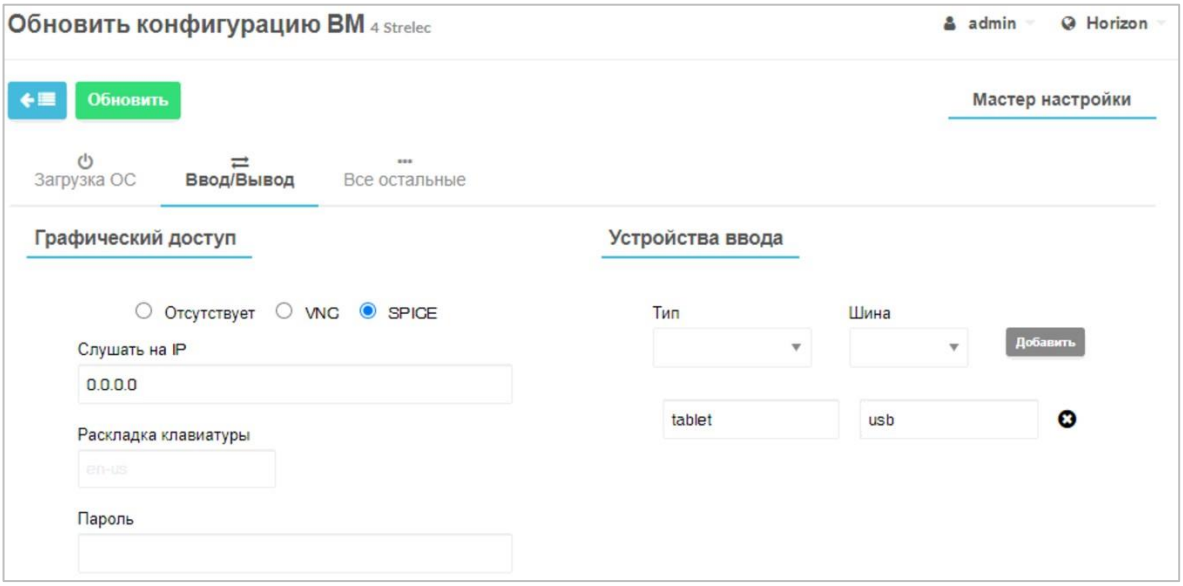


Рисунок 119 – Изменение конфигурации ВМ. Ввод/Вывод

19. На вкладке **Все остальные** можно «пробросить» (подключить напрямую) внутрь ВМ какие-либо PCI-устройства (Рисунок 120).

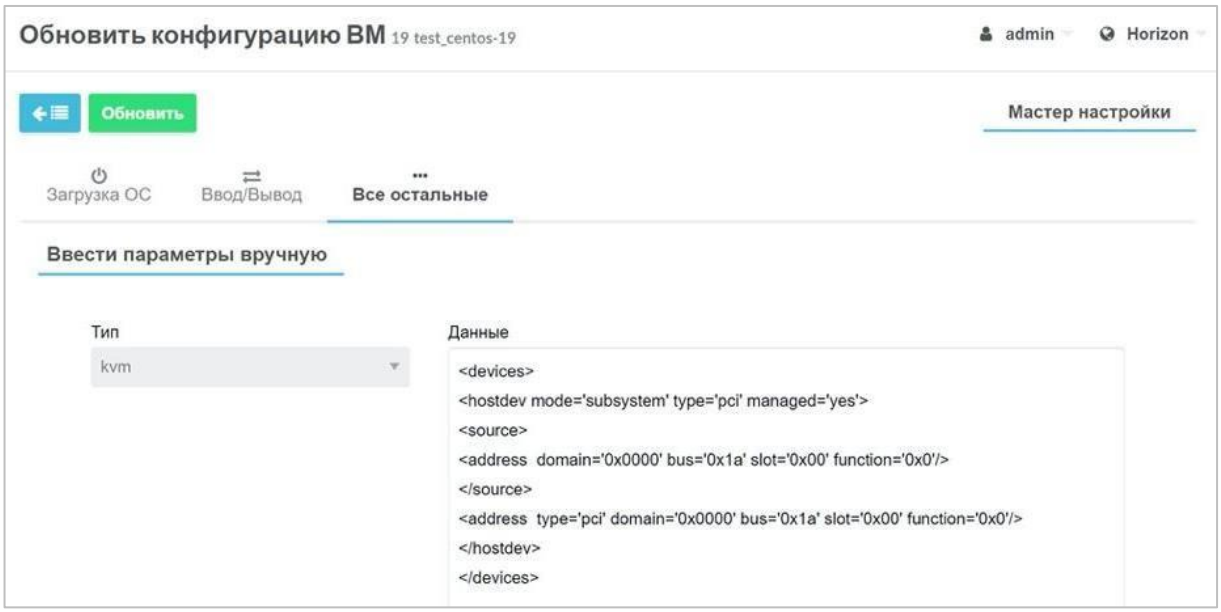


Рисунок 120 – Обновление конфигурации ВМ. Проброс PCI-устройства

Для «проброса» PCI-устройства, в поле **Данные** ввести информацию об устройстве в следующем формате:

```
<devices>
<hostdev mode='subsystem' type='pci' managed='yes'>
      <source>
        <address domain='0x0000' bus='0x04' slot='0x00'
function='0x0'/>
      </source>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x08'
function='0x0'/>
    </hostdev>
</devices>
```

Для получения необходимых сведений ввести команду в консоли:

```
 lspci -mmnn
```

Примечание*: существуют зарезервированные адреса PCI, список их доступен по адресу https://libvirt.org/pci-addresses.html#reserved-addresses.*

20. После внесения всех изменений в конфигурацию ВМ нажать кнопку **Обновить** для обновления и сохранения конфигурации ВМ.

3.2.22.9 Вкладка «Шаблон»

На вкладке **Шаблон** представлен код шаблона ВМ, на базе которого исполняется ВМ, а также внесенные пользователем в код изменения и коррективы (Рисунок 121 – Вкладка «Шаблон»

).

Рисунок 121 – Вкладка «Шаблон»

3.2.22.10 Вкладка «Журнал»

На вкладке **Журнал** представлена история исполнения ВМ и внесенных изменений в работу ВМ (Рисунок 122).

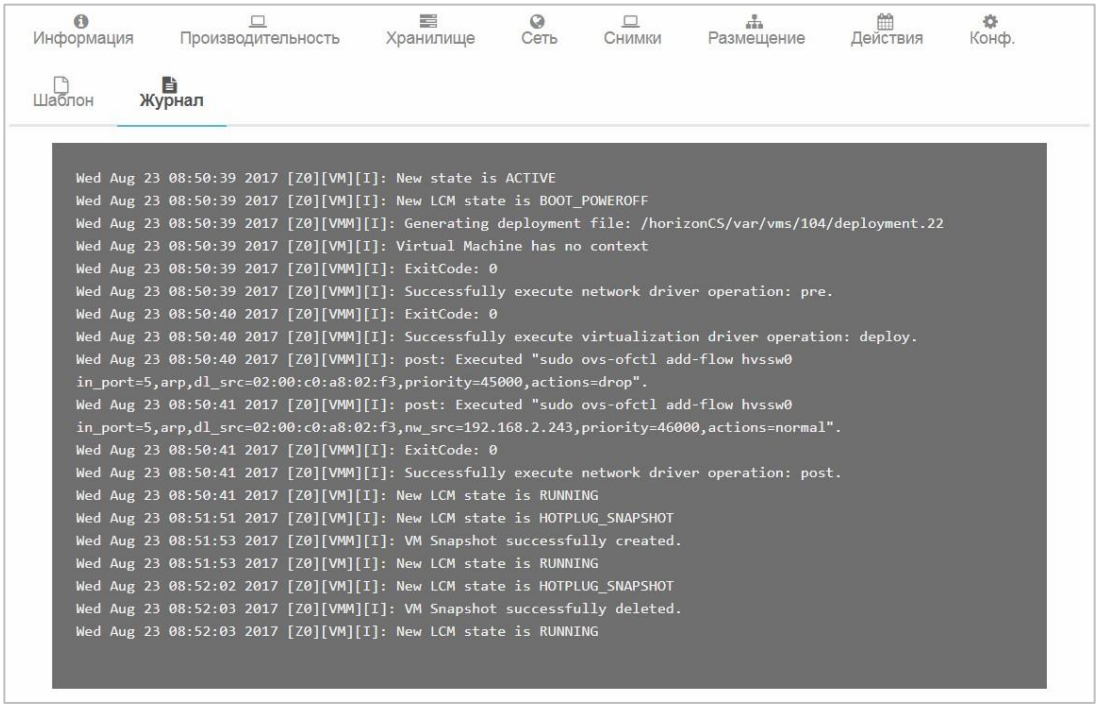


Рисунок 122 – Вкладка «Журнал»

В журнале отображаются следующие события (Таблица 7): Таблица 7 – События журнала ВМ

Событие	Запись в журнале
Время создания ВМ	Дата и время строки с состоянием «BOOT»
Запуск ВМ	Строка с состоянием «RUNNING»
Уничтожение ВМ	Строка с состоянием «EPILOG»
Миграция ВМ	Строка с состоянием «MIGRATE»
Создание/удаление снимка ВМ	Строка со состоянием «HOTPLUG_SNAPSHOT»

3.2.23 Подключение внешнего тома системы хранения к виртуальной машине

***Внимание**! Том системы хранения может быть подключен только к одной ВМ.*

Для подключения тома системы хранения в ВМ:

1. Подключить внешний том системы хранения в терминале.
2. Создать распределенное хранилище (подробно см. п. 3.2.8.1.3).
3. Открыть раздел **Хранилище** → **Образы** (Рисунок 123).

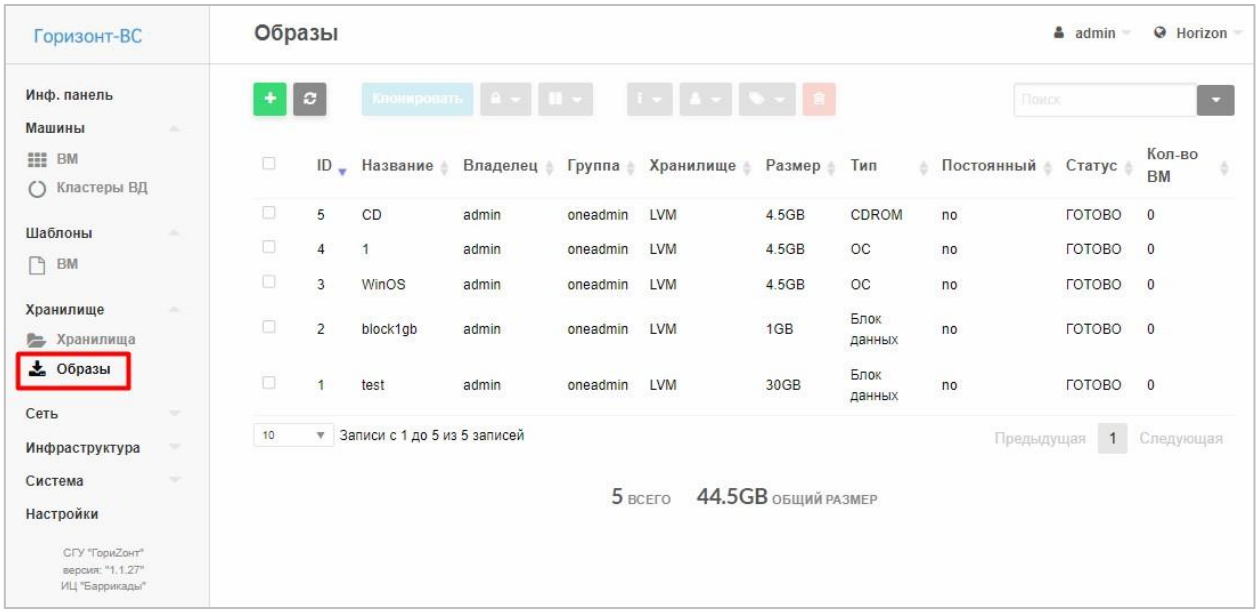


Рисунок 123 – Раздел «Хранилище → Образы»

4. Нажать кнопку добавления образа –  .

   Откроется окно создания образа (Рисунок 124).

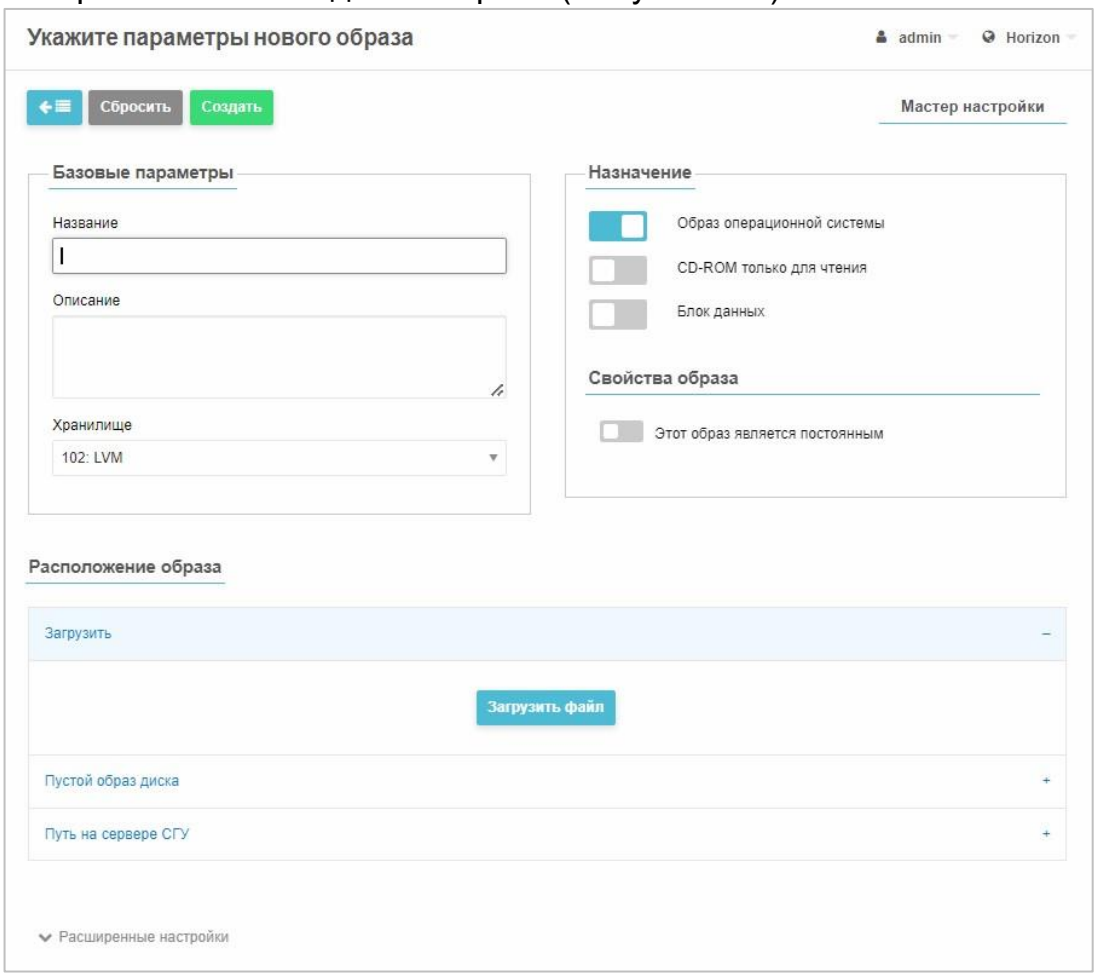


Рисунок 124 – Окно создания образа хранилища

5. Установить обязательные параметры образа диска:

– в секции **Базовые параметры** в поле **Название** ввести название образа;

– из выпадающего списка **Хранилище** выбрать хранилище, созданное на шаге 2.

– В секции **Назначение** установить значение **Блок данных**, передвинув соответствующий переключатель вправо.

– в секции **Расположение образа** нажать на поле **Путь на сервере СГУ** указать путь на сервере СГУ в виде **#/dev/имя диска**.

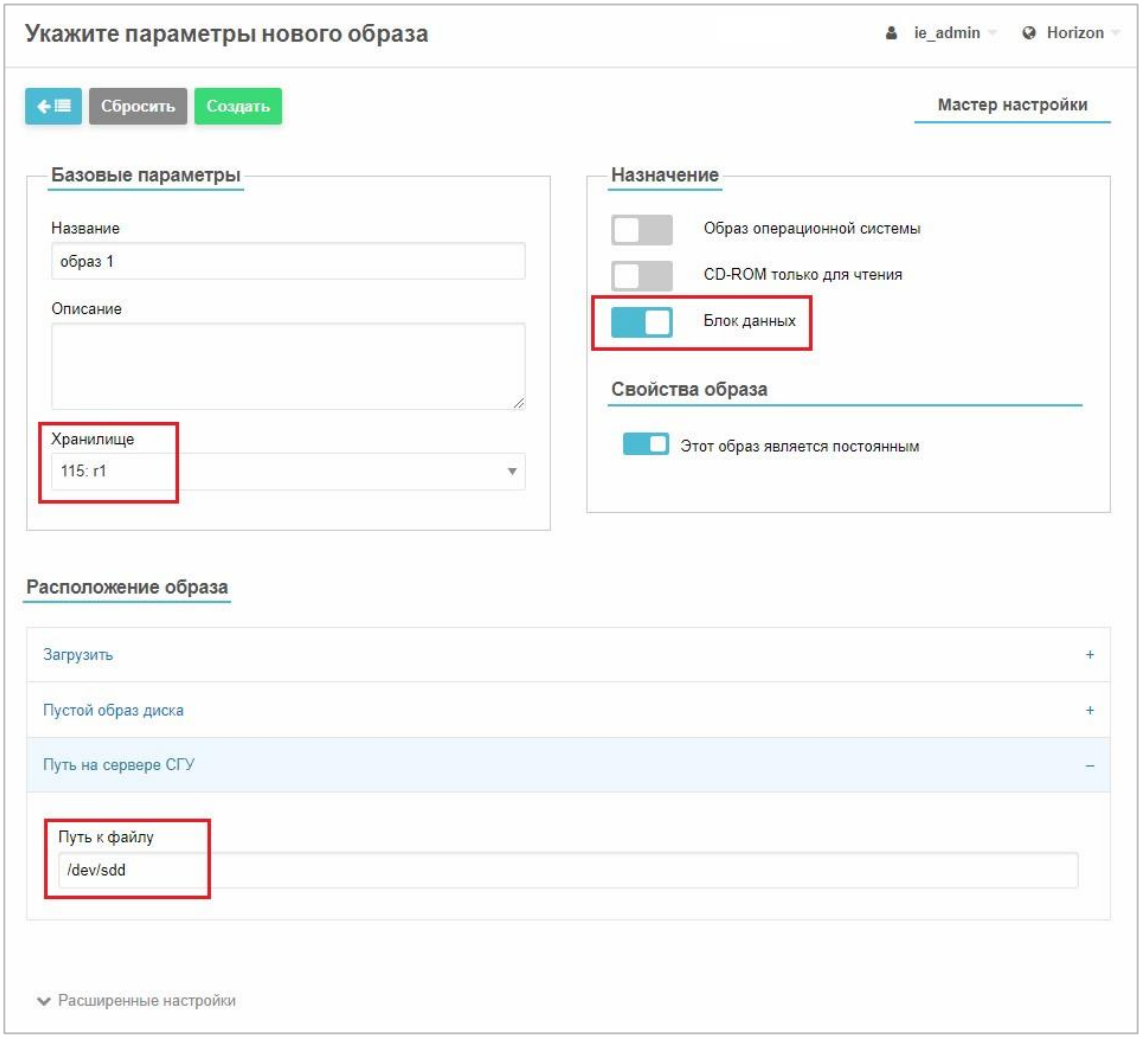


Рисунок 125 – Создание образа диска

6. Нажать кнопку Создать.

   Созданный образ хранилища будет добавлен в список.

7. В разделе **Машины → ВМ выбрать ВМ**, к которой необходимо подключить том СХД и дважды нажать на нее.

   ***Внимание**! Машина должна быть запущена.*

   Откроется окно информации ВМ (Рисунок 126).

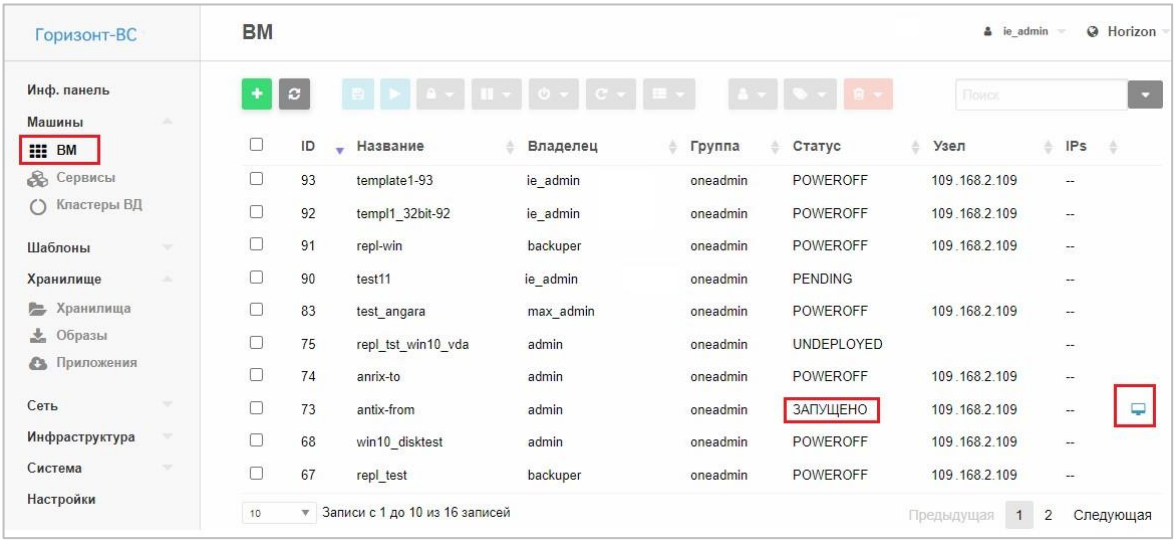


Рисунок 126 – Выбор ВМ для подключения тома СХД

8. Перейти на вкладку **Хранилище** (Рисунок 127).

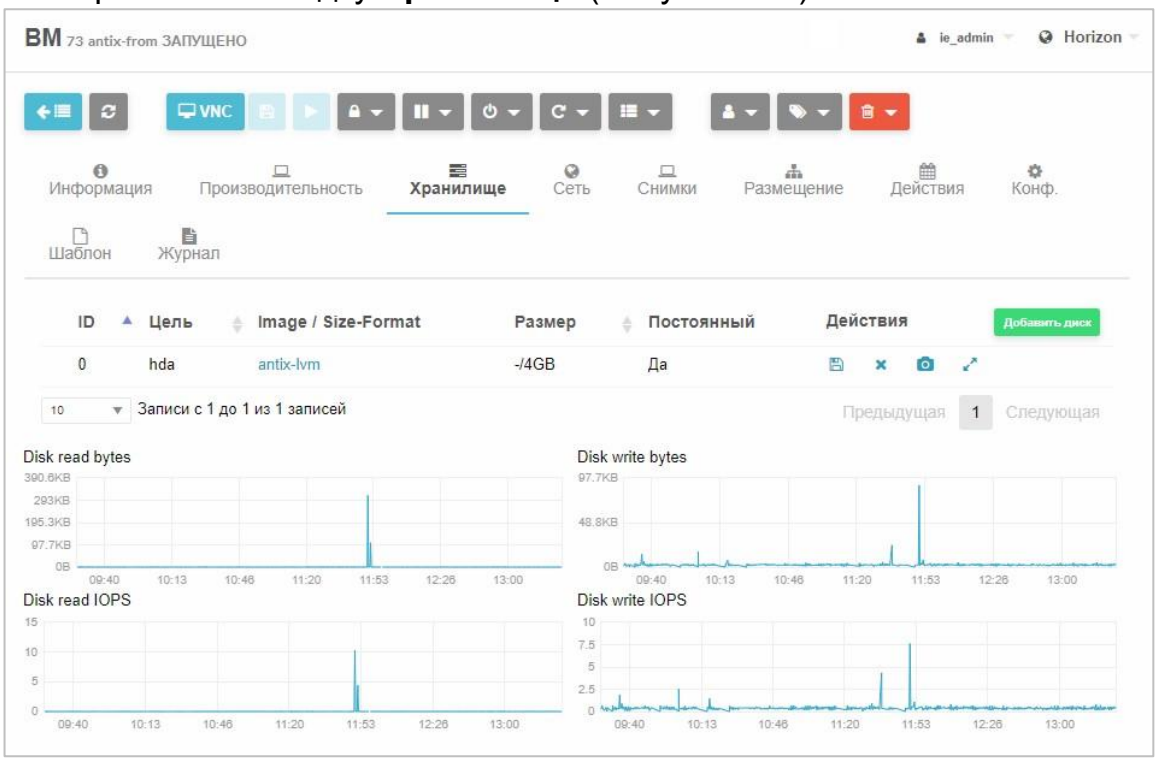


Рисунок 127 – Информация о ВМ. Вкладка хранилище

9. Нажать кнопку Добавить диск.
   Откроется окно **Выбрать диск** (Рисунок 128).

10. Выбрать опцию Образ, выбрать образ хранилища, созданный на шагах

3 – 7, и нажать кнопку Присоединить в нижнем правом углу (Рисунок 128).

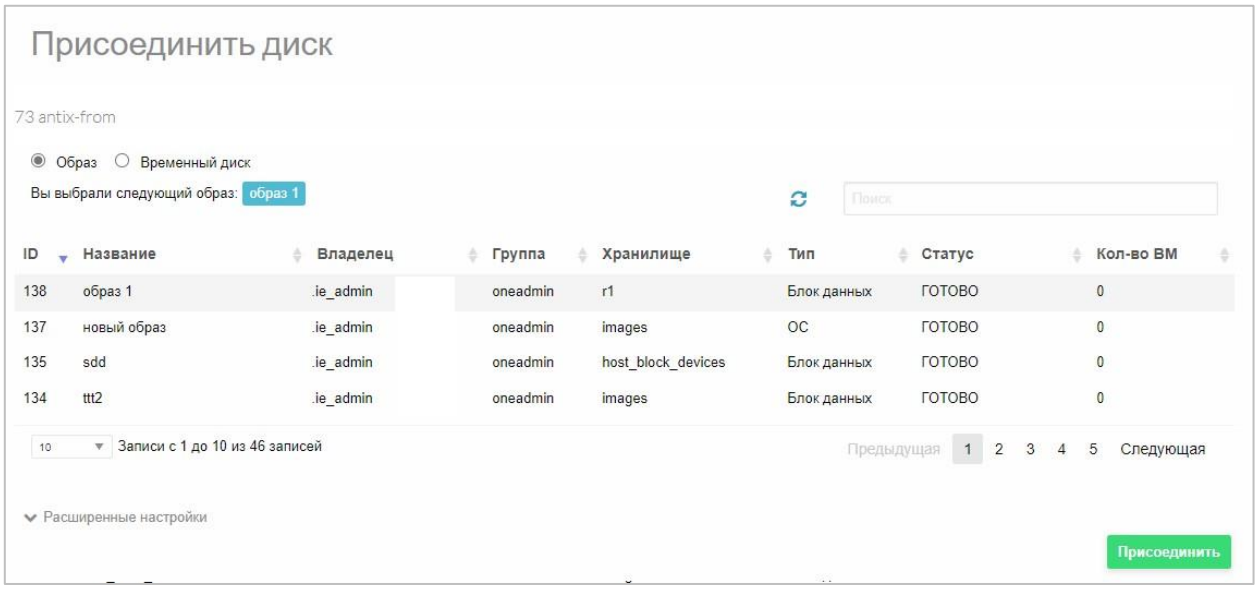


Рисунок 128 – Подключение тома СХД к ВМ

Добавленный ТОМ СХД появится в списке хранилищ, подключенных к данной ВМ (Рисунок 129).

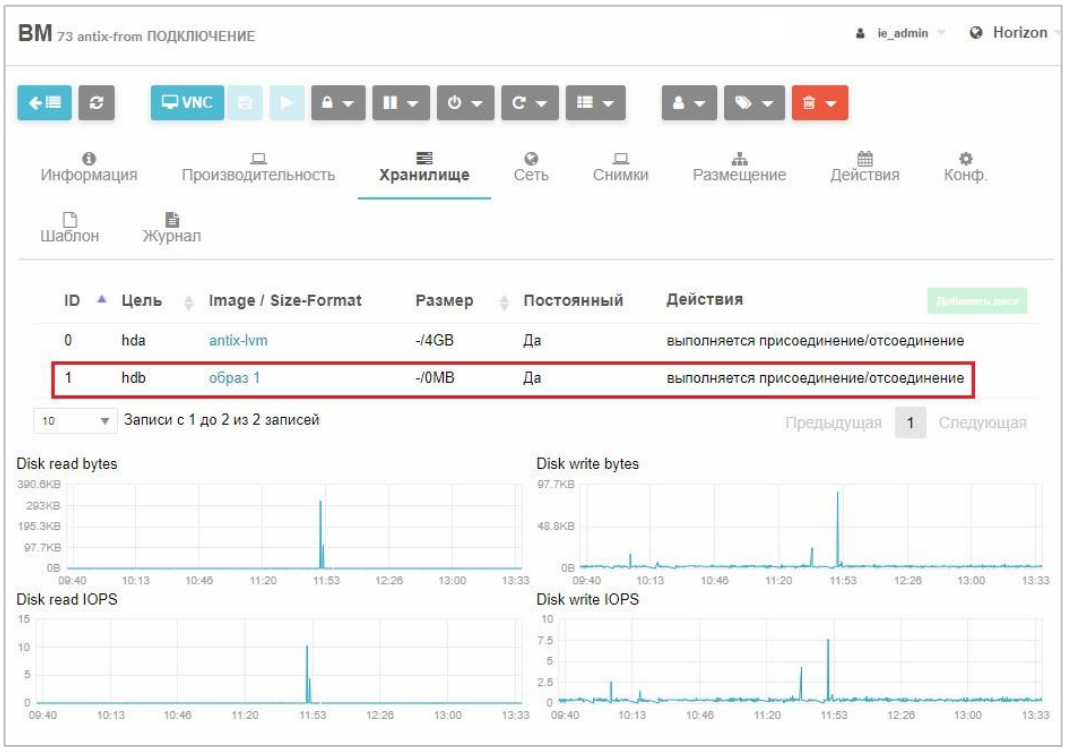


Рисунок 129 – Том СХД подключен к ВМ

3.2.24 Настройка включения автоматической загрузки виртуальной машины в БИОС

Для настройки включения загрузки виртуальной машины в БИОС:

1. В меню **Машины** → **ВМ** нажать на строку ВМ, которую необходимо изменить.

   Откроется окно информации о данной ВМ.

2. Нажать на кнопку **Отключить питание** на панели управления и выбрать пункт **Отключить питание** (Рисунок 130).

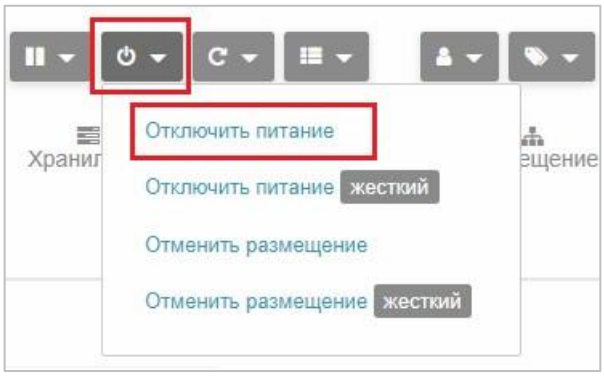


Рисунок 130 – Отключение питания ВМ

3. Перейти на вкладку **Конф**.
4. Нажать кнопку **Обновить конфигурацию** (Рисунок 131).

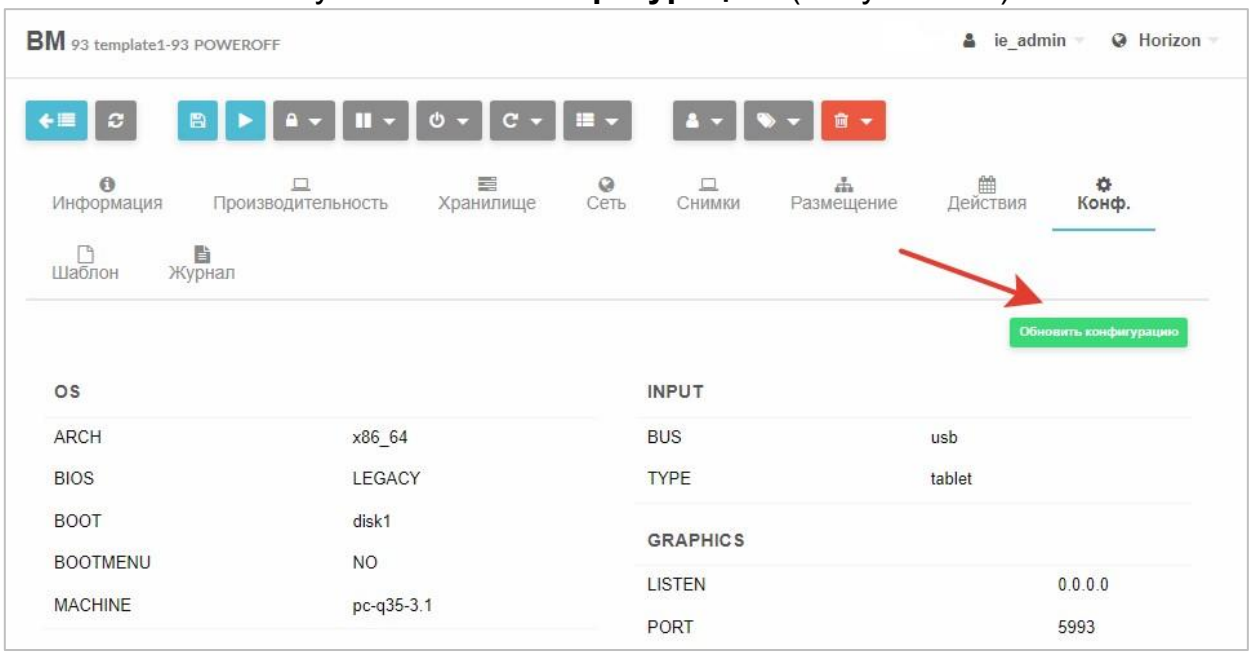


Рисунок 131 – Кнопка «Обновить конфигурацию»

Откроется окно **Обновить конфигурацию ВМ** (Рисунок 132).

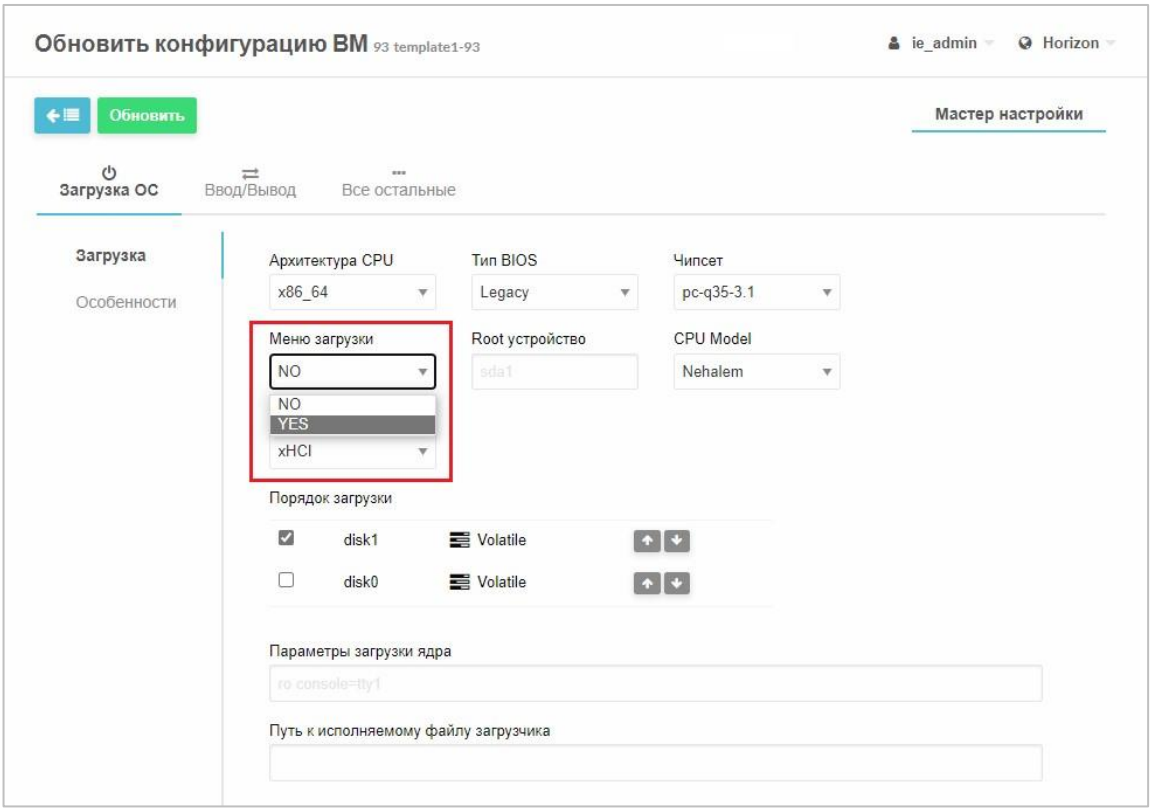


Рисунок 132 – Окно «Обновить конфигурацию ВМ»

5. В выпадающем списке **Меню загрузки** выбрать **YES** (Рисунок 132).
6. Нажать на кнопку **Обновить** в верхнем левом углу окна.

   Откроется окно информации о ВМ.

7. Включить ВМ нажатием кнопки  на панели управления.

   Станет доступна кнопка  на панели управления.

8. Нажать кнопку  .

   Откроется окно с надписью **VNC Connected** (Рисунок 133).

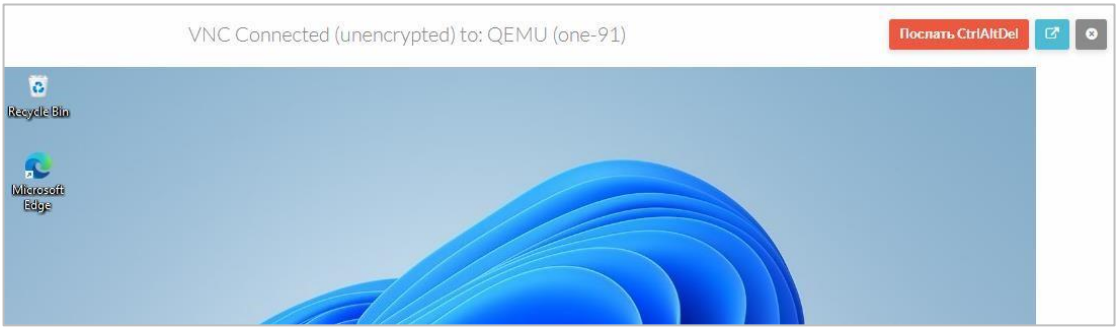


Рисунок 133 – ВМ с измененными настройками загрузилась в BIOS

***Примечание**. При включенной ВМ кнопка «Обновить конфигурацию» недоступна.*

3.2.25 Миграция виртуальных машин

В Программный комплекс (ПК) «Иридиум»поддерживается миграция ВМ.

Миграция ВМ – это перемещение ВМ с одного сервера СГУ на другой.

Поддерживаются два типа миграции ВМ:

- миграция с остановкой ВМ;
- *живая миграция* (Live migration) – перенос виртуальной машины с одного физического сервера на другой без прекращения работы ВМ и остановки сервисов. Живая миграция необходима в проектах, работу которых нежелательно прерывать: сервисы обслуживания магистральных и провайдерских сетей (например, DNS), крупные сервисы электронной почты.

Для осуществления миграции ВМ:

9. Перейти в раздел СГУ **Машины→ВМ.**
10. Выбрать из списка ВМ те, которые необходимо мигрировать.
11. В выпадающем меню нажать кнопку  .
1. Выбрать способ миграции:

- **Перенести ВМ с приостановкой** (миграция с приостановкой работы ВМ);

– **Перенести ВМ без остановки** (живая миграция ВМ между узлами).

2. В открывшемся окне выбрать узел, на который необходимо мигрировать ВМ.
3. Нажать кнопку **Перенести ВМ.**

   Запустится процесс миграции, статус ВМ изменится на **Миграция**. После окончания переноса в списке ВМ значение в столбце **Узел** изменится на выбранное в процессе миграции.

Программный комплекс (ПК) «Иридиум»также обеспечивает возможность живой миграции функционирующих ВМ между хостами с процессорами разных поколений.

При создании кластера из узлов виртуализации на аппаратных платформах с процессорами разных поколений, необходимо, в целях обеспечения возможности миграции ВМ между хостами, выбрать для всех создаваемых ВМ в шаблоне вместо типа процессора «host-model». Команды процессора данного типа входят в качестве подмножества в множество команд всех используемых в кластере процессоров (см. п. 3.2.16).

3.2.26 Статистика использования ресурсов системы

В Программный комплекс (ПК) «Иридиум» доступен сбор и просмотр статистики об использовании различных ресурсов системы и представление ее в графическом виде по запросу пользователя.

Для просмотра статистики по использованию ресурсов СГУ:

4. Запустить СГУ.
5. Перейти в раздел **Настройки.**
6. Выбрать вкладку **Отчетность**.

Отобразится строка настроек для вывода отчетсности и информация по использованию ресурсов центрального процессора (Рисунок 134).

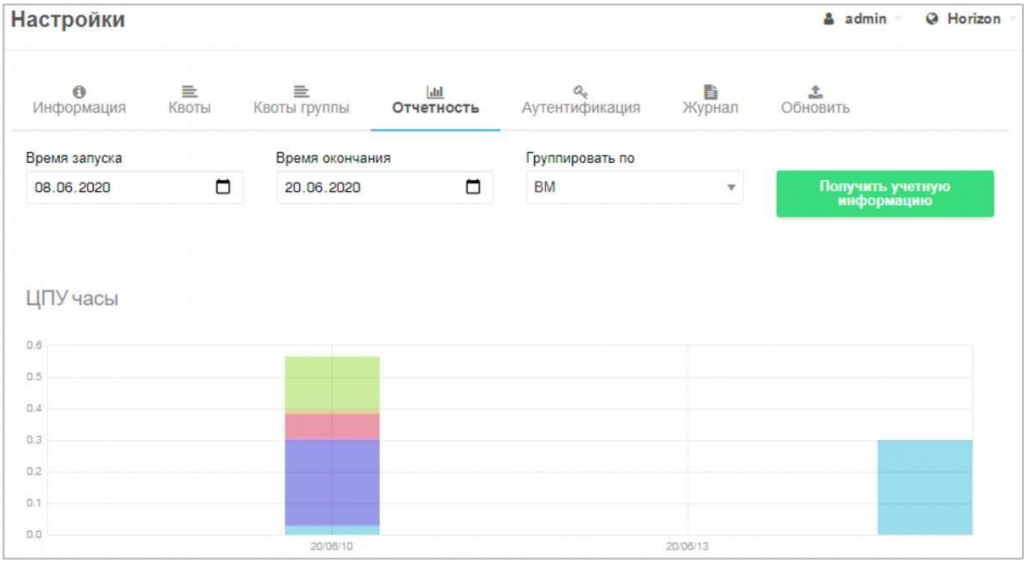


Рисунок 134 – Получение статистической информации об использовании ресурсов системы

7. Ввести промежуток времени для получения отчета.
8. В поле **Группировать по** выбрать параметр, по которому необходимо вывести статистику: ВМ, пользователь, группа (Рисунок 135).

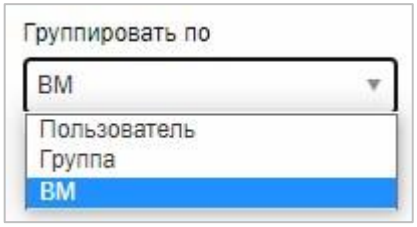


Рисунок 135 – Настройка параметров для вывода статистики

9. Нажать кнопку **Получить учетную информацию** (Рисунок 134). Отобразятся статистические данные по всем виртуальным машинам/пользователям/группам пользователей, зарегистрированными в СГУ, за указанный период (Рисунок 136).

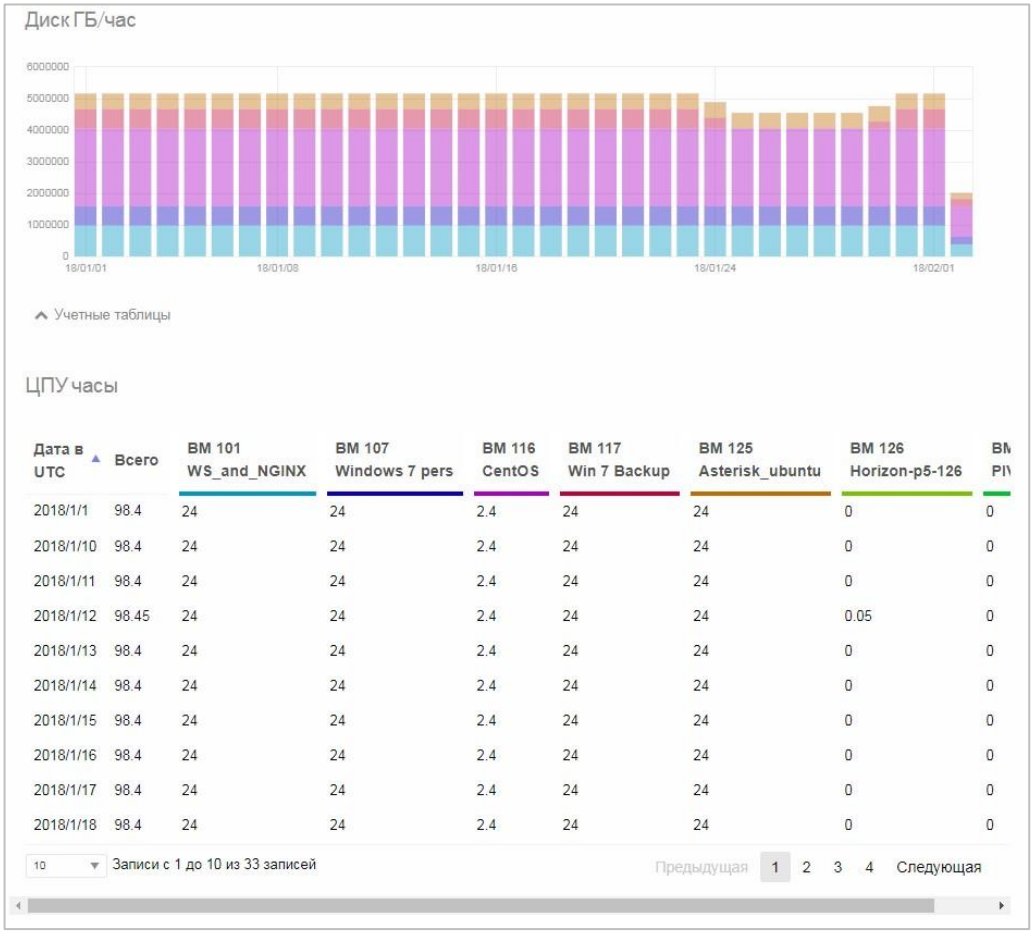


Рисунок 136 – Статистика использования ресурсов виртуальных машин

Для просмотра статистики по использованию CPU и памяти узла:

10. Перейти в раздел СГУ **Инфраструктура** → **Узлы**.
11. Выбрать из списка узел и нажать на него.

Откроется окно информации о выбранном узле (Рисунок 137).

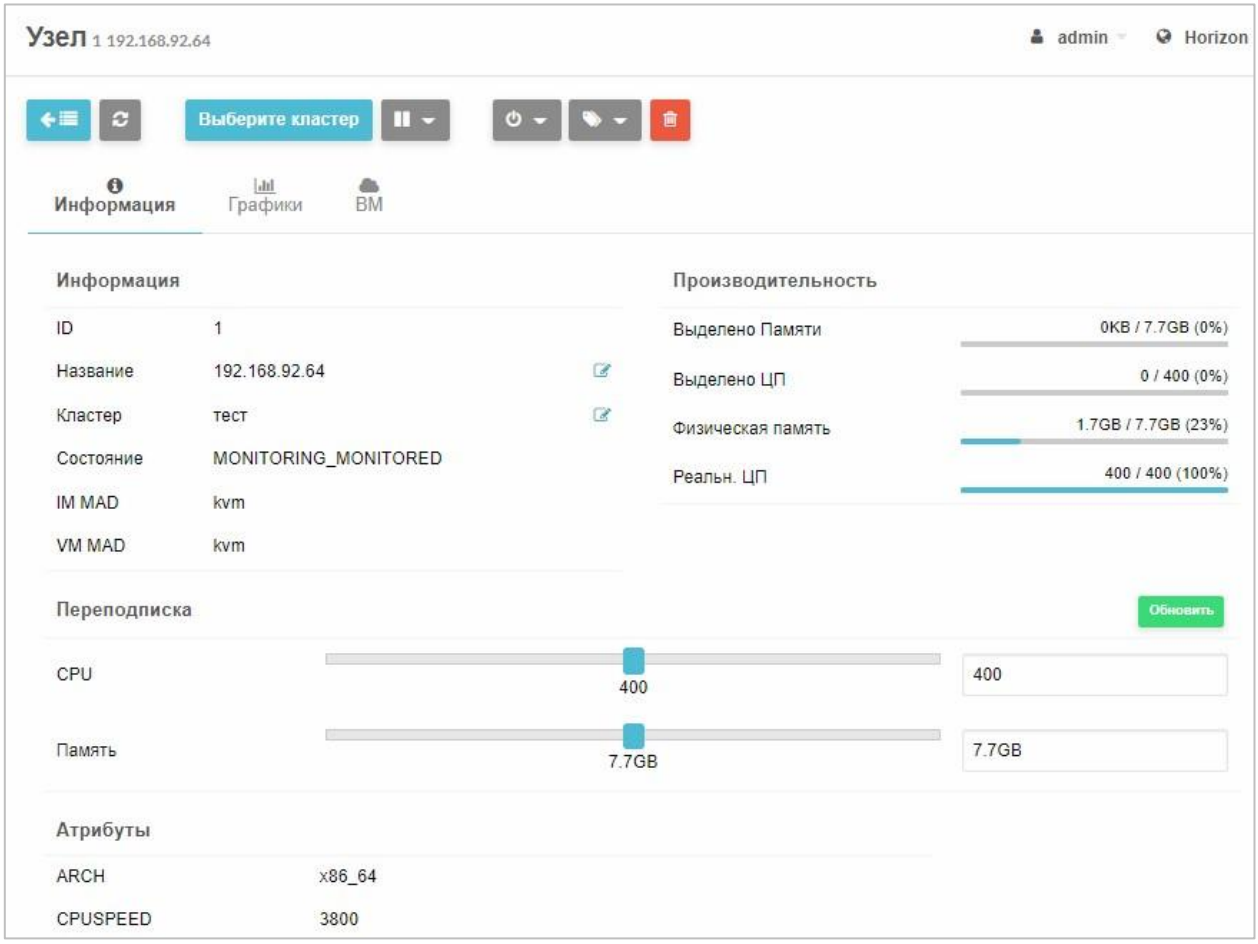


Рисунок 137 – Окно информации о выбранном узле (сервере)

12. Перейти на вкладку **Графики**.

    Отобразится информация об использовании ресурсов процессора и памяти ВМ, на которой установлен сервер (Рисунок 138).

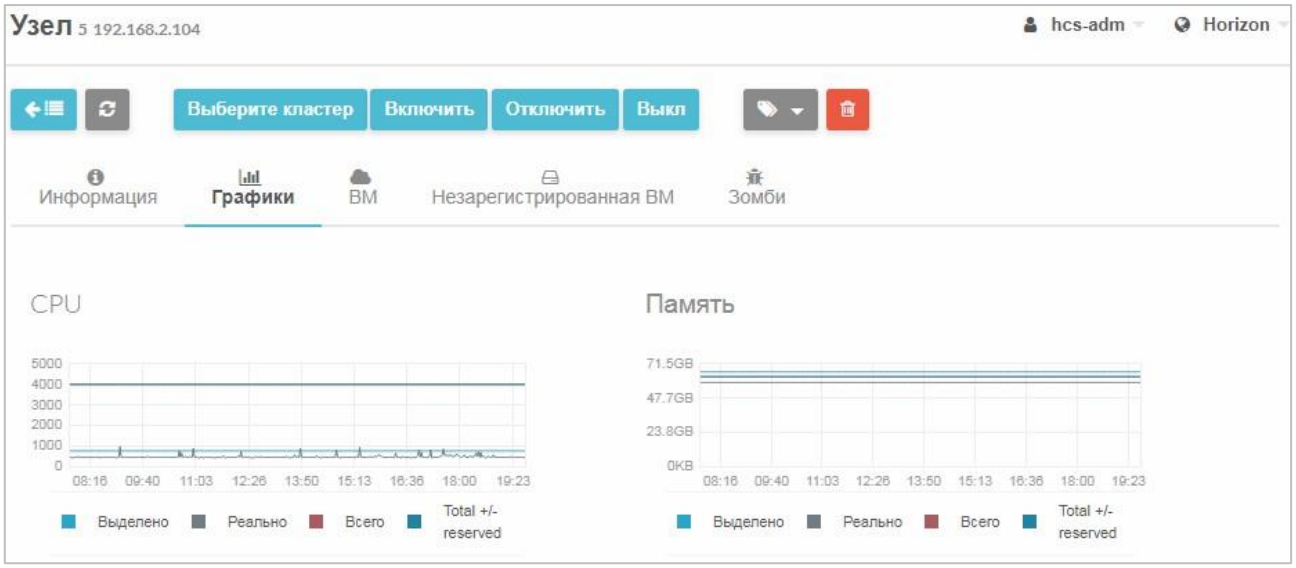


Рисунок 138 – Графики

Для просмотра информации о CPU и памяти ВМ и статистики их использования:

13. Перейти в раздел СГУ **Машины** → **ВМ**.
14. Выбрать из списка ВМ нажатием.

    Откроется окно информации о ВМ
15. Перейти на вкладку **Производительность.**

    Отобразится информация об CPU и памяти выбранной ВМ и ниже – статистика их использования в виде графика (139).

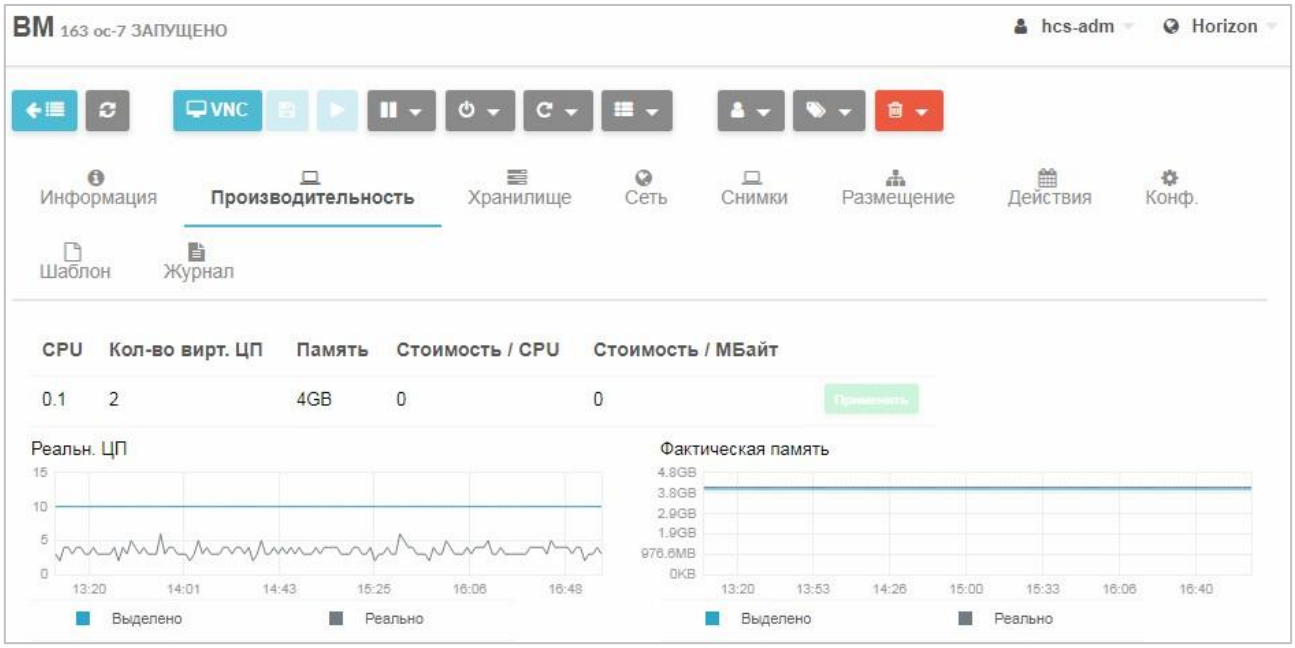


Рисунок 139 – Производительность ВМ

16. **Для просмотра информации о хранилищах той же ВМ и его статистике** перейти на вкладку **Хранилище** (Рисунок 140).

    Отобразится информация о хранилищах, подключенных к данной ВМ, и ниже – статистика их использования в виде графика.

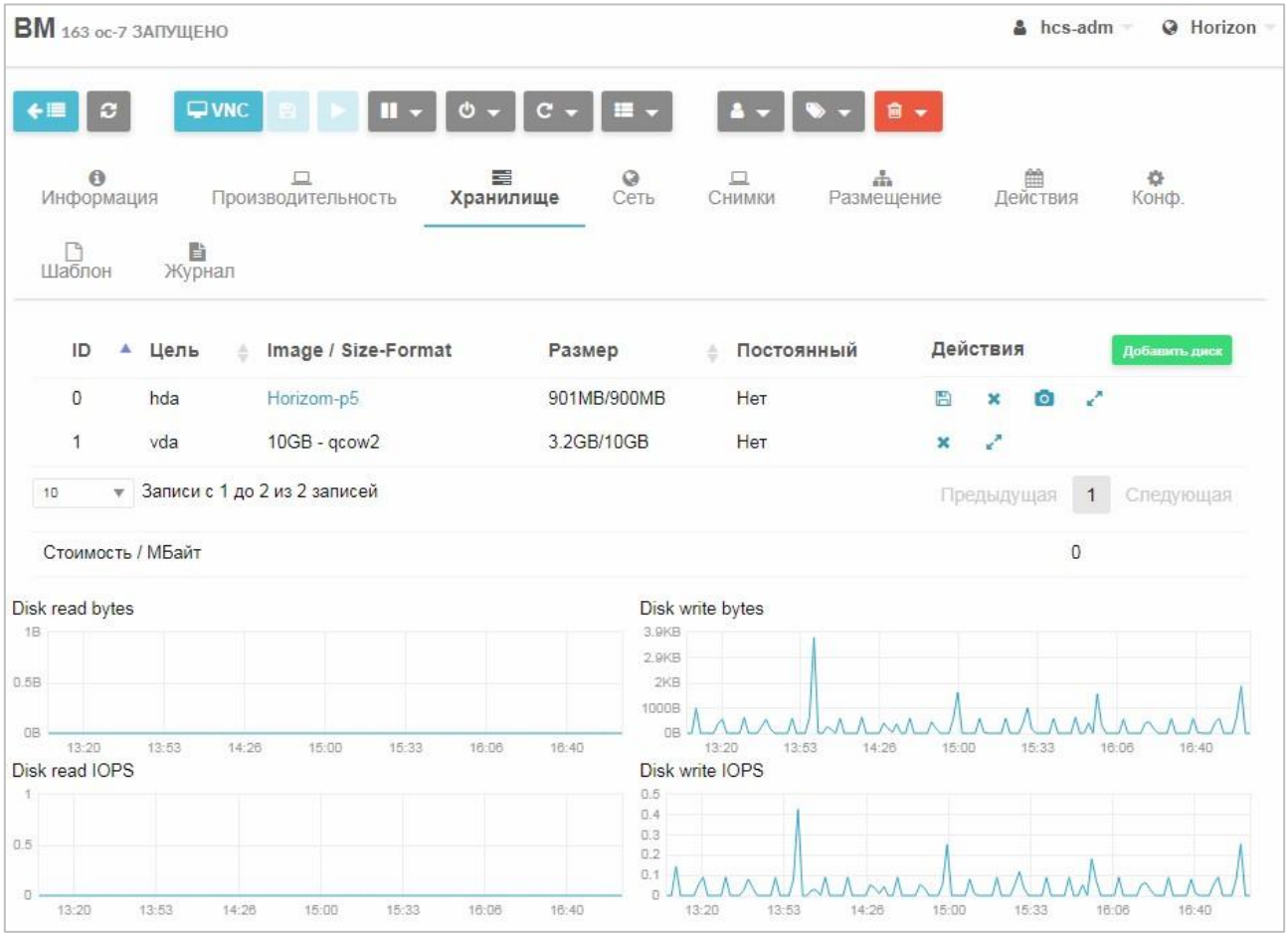


Рисунок 140 – Отчетная информация о хранилищах ВМ

17. **Для просмотра информации о витруальных сетях той же ВМ** перейти на вкладку **Сеть** (Рисунок 141).

    Отобразится информация о виртуальных сетях, к которым подключенна данная ВМ, и ниже − статистика их использования в виде графика.

    Для отклюбчения ВМ от сети нажать кнопку Отсоединить.

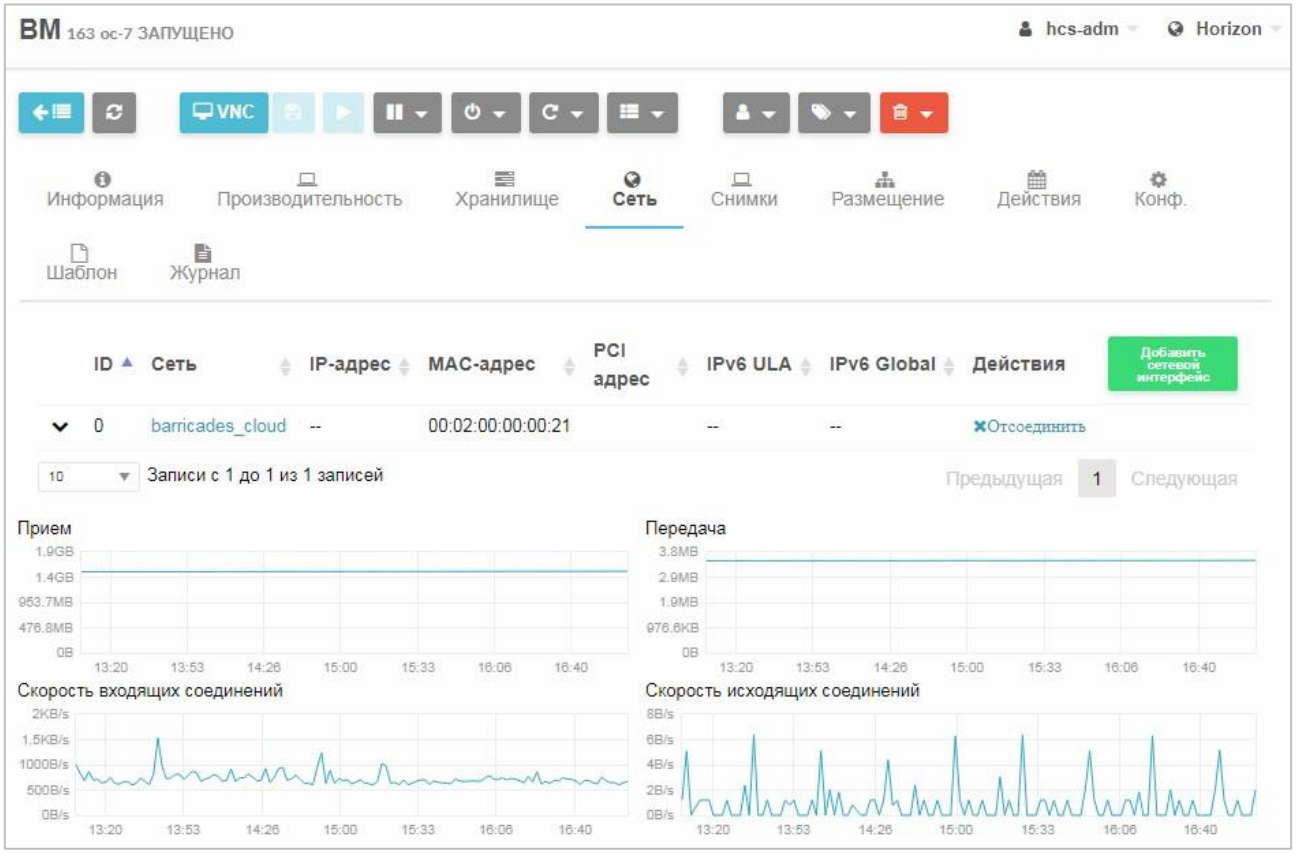


Рисунок 141 – Отчетная информация о сетях, к которым подключена ВМ

3.2.27 Конвертация виртуальных машин

Конвертация ВМ – это перенос ВМ в СГУ из внешней системы.

Поддерживаются два типа конвертации ВМ в виртуальную среду:

- из физических серверов x86 с установленной ОС (см. п. 3.2.27.1);
- из сред виртуализации, например VMWare, Hyper-V и т. д. (см. п. 3.2.27.2).

3.2.27.1 Конвертация ВМ из физического сервера

Для конвертации в виртуальную среду из физических серверов x86 с установленной ОС:

1. Предварительно подготовить образ системы.
   Для подготовки образа системы:
   e. Загрузить физический сервер с загрузочного live USB-накопителя (например, с ОС Fedora).

ж. Войти в систему под пользователем root.

з. Запустить консоль.

и. Установить отформатированный USB-накопитель, на который будет производится запись образа.

к. Определить обозначение дисков при помощи команды:

```
#cat /proc/partitions
```

л. Смонтировать накопитель, на который будет производиться запись образа, командой:

```
# mount /dev/sdb /mnt
```

м. Создать образ системы, установленной на физическом сервере, при помощи команды:

```
dd if=/dev/sda of=/mnt/image.img /conf.img bs=8M
conv=sync,noerror
```

где **sda** − диск физического сервера, **sdb** − диск накопителя, **image.img** – образ сервера.

2. После окончания создания образа извлечь накопитель с образом командой:

```
# umount /mnt
```

3. Установить накопитель с образом физического сервера в АРМ УВ.
4. Создать образ ВМ, как описано в разделе 3.2.18.
5. После окончания загрузки образа создать шаблон и ВМ с подготовленным образом, согласно п. 3.2.16 и 3.2.18.

3.2.27.2 Конвертация виртуальной машины из сред виртуализации

Для конвертации виртуальной машины из сред виртуализации:

6. Загрузить в СГУ образ диска для конвертации.

Для загрузки образа диска:

н. Перейти в раздел **Хранилище** → **Образы ВМ.**

о. Нажать кнопку  .

Откроется окно (рисунок 42).

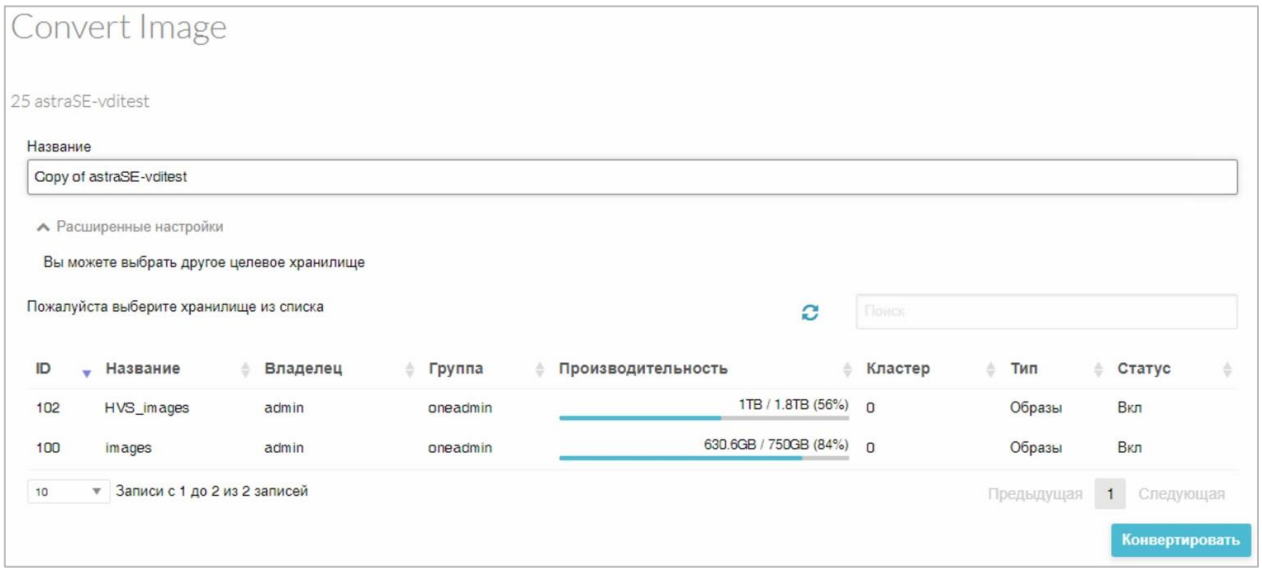


Рисунок 142 – Конвертация образа ВМ

п. Заполнить поля:

- в поле **Название** указать наименование образа диска;
- в поле **Тип** из раскрывающегося списка выбрать **Образ операционной системы**;
- в поле **Свойства образа** можно установить, будет образ постоянным или непостоянным;
- в поле **Хранилище** указать тип хранилища, в котором будет храниться образ;
- в поле **Расположение образа** выбрать пункт **Закачать**;
- с помощью кнопки **Выберите файл** выбрать необходимый образ диска.

р. Нажать кнопку **Создать**.

После завершения процесса копирования файла образ диска будет создан и размещен в хранилище.

7. Выделить образ в списке флажком и нажать кнопку **Конвертировать** в управляющем меню.

   Откроется окно конвертации образа (**Ошибка! Источник ссылки не найден.**).
8. В окне конвертации ввести название образа, выбрать хранилище и нажать кнопку **Конвертировать**.
9. После окончания конвертации образа создать шаблон и ВМ с подготовленным образом, согласно п. 3.2.16 и 3.2.18.

3.2.28 Одновременное применение технологии NUMA и механизмов оптимизации использования оперативной памяти сервера

СГУ предоставляет возможность одновременно использовать технологию неравномерного доступа к памяти (NUMA − Non-Uniform Memory ccess) и механизмы оптимизации использования оперативной памяти. Для этго необходимо выполнить следующие действия:

1. Подключиться к серверу системы управления гипервизорами посредством браузера под учетной записью администратора.
2. Выбрать один сервер для проверки отказоустойчивости кластера,
3. Убедиться, что режим высокой доступности для ВМ, размещенных на данном сервере, включен.

   Для проверки подключения режима высокой доступности ВМ:

   с. Перейти в раздел **Машины** → **Кластеры ВД**.

   т. Убедиться в наличии флага слева от ВМ в списке.

***Примечание**. Режим высокой доступности ВМ − возможность автоматического перезапуска ВМ в случае сбоев.*

4. Запустить созданную ВМ и запустить встроенные в ОС приложения.

5. Выполнить отключение сервера.
6. Посредством консоли системы управления гипервизорами продемонстрировать перезапустить ВМ на других серверах.
7. Выборочно проверить работоспособность виртуальных машин (посредством команды ping и открытия консоли ОС).

3.2.29 Создание изолированных виртуальных сетей между виртуальными машинами

Для создания изолированных виртуальных сетей:

1. Подключиться к серверу системы управления гипервизорами посредством браузера под учетной записью администратора:

```
ssh ondeadmin@XXX.XXX.XX.X
```

2. Создать виртуальный коммутатор. **Для создания виртуального коммутатора:**

а. командной строке зайти на виртуальный сервер под учетной записью администратора;

б. создать мост командой:

```
ovs-vsctl add-br hvssw5
```

где *hvssw5* – имя моста; *eth7* – порт;

в. добавить физический порт в мост командой:

```
ovs-vsctl add-port hvssw5 eth7
```

где *hvssw5* – имя моста; *eth7* – порт;

3. В веб-приложении СГУ создать виртуальную сеть, подключенную к интерфейсу виртуального коммутатора:

а. В разделе **Сеть** → **Виртуальные сети** нажать кнопку .

б. На вкладке **Общие** указать название сети (Рисунок 143).

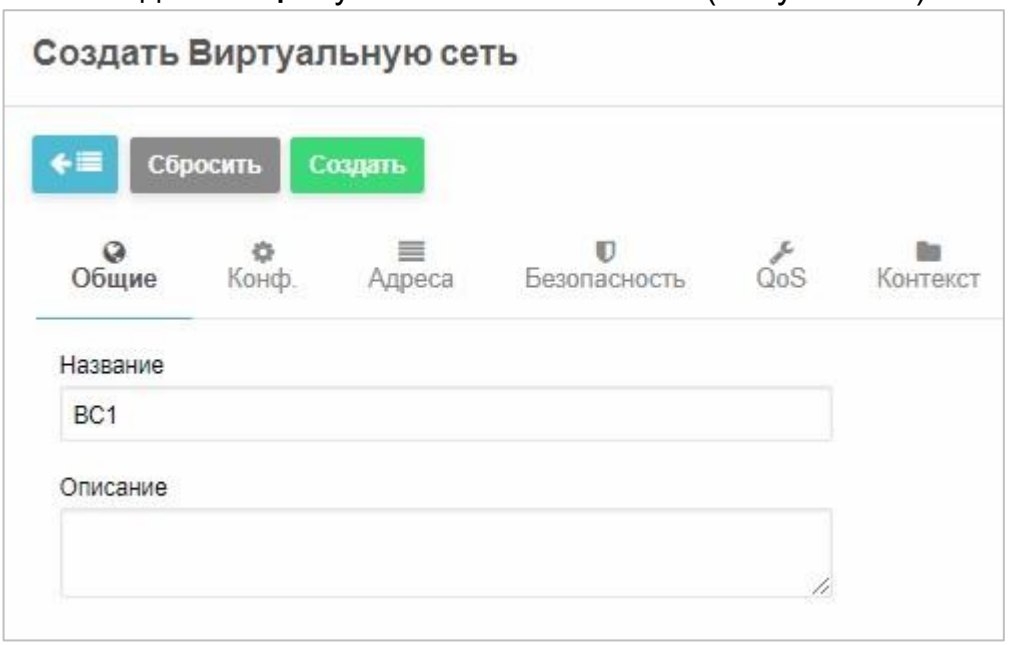


Рисунок 143 – Создание виртуальной сети. Вкладка «Общие»

в. Заполнить поля на вкладке **Конф**.(Рисунок 144):

- в поле **Интерфейс сет. моста** указать имя созданного моста (в данном примере – *hvssw5*);
- из выпадающего списка **Режим работы сети** выбрать **Open vSwitch**;

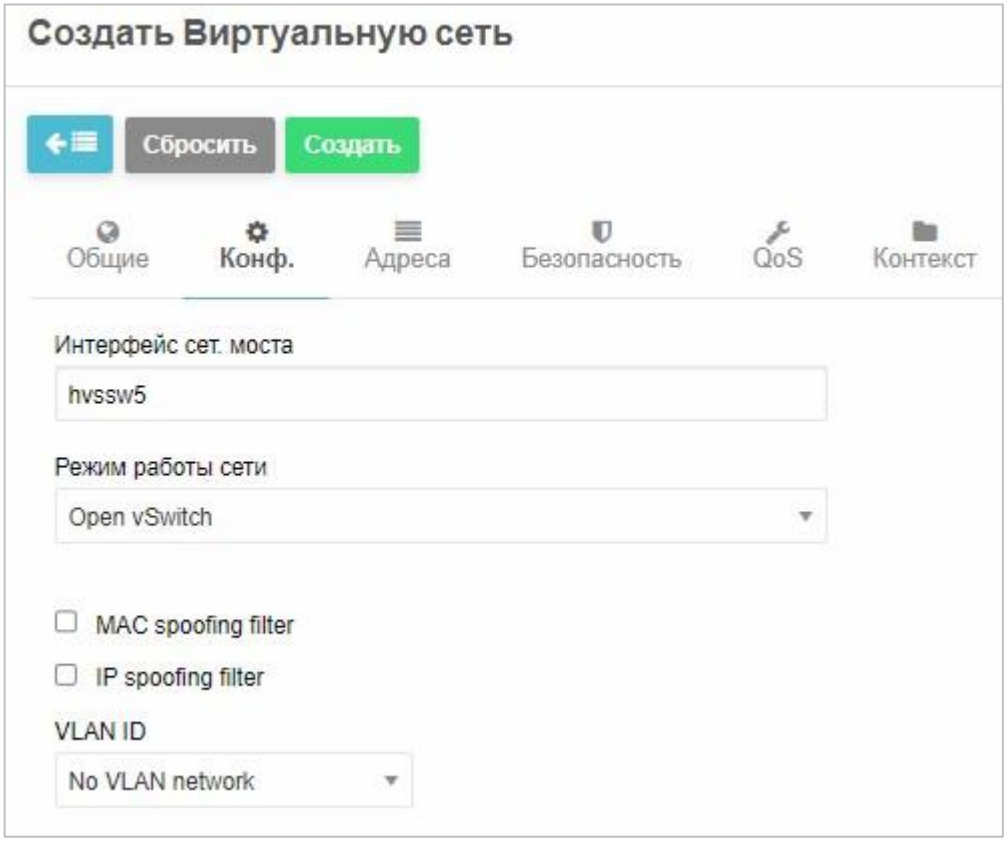


Рисунок 144 – Создание виртуальной сети. Вкладка «Конф.»

г. На вкладке **Адреса** выбрать Ethernet и в поле Первы MAC-адрес указать MAC-адрес сети из 12 цифр в 16х системе, по две цифры с разделителем «:», *например*: 52:54:77:ab:cd:ef (Рисунок 145).

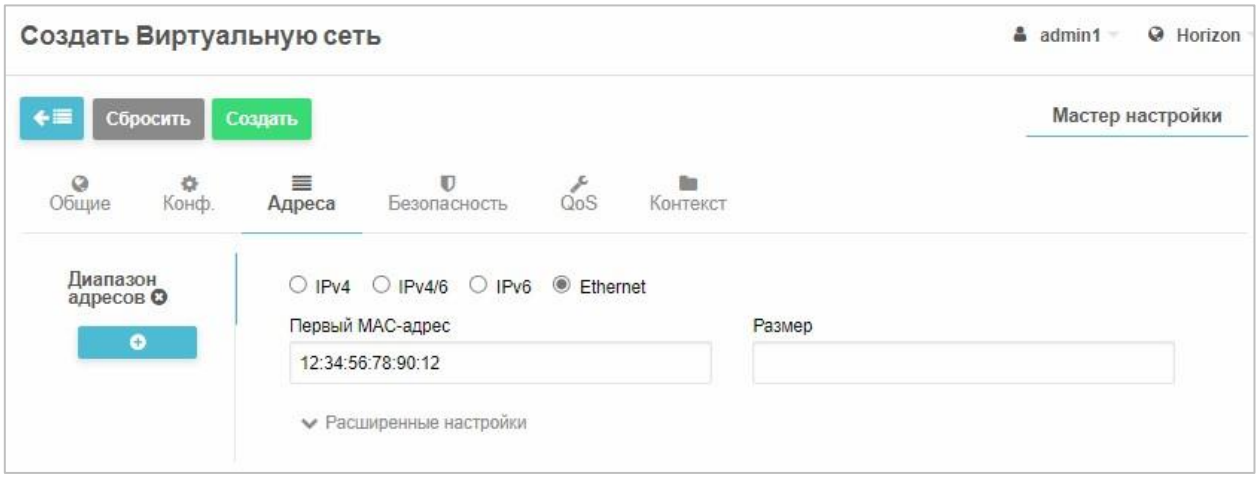


Рисунок 145 – Создание виртуальной сети. Вкладка «Адреса»

д. Нажать кнопку Создать.

Созданная сеть будет добавлена в список.

4. Подключить виртуальную сеть с назначенным VLAN к первой ВМ.

а. В разделе **ВМ** → **Машины** выбрать ВМ двойным нажатием.

б. Перейти на вкладку **Сеть**.

в. Нажать кнопку **Добавить сетевой интерфейс** (Рисунок 146).

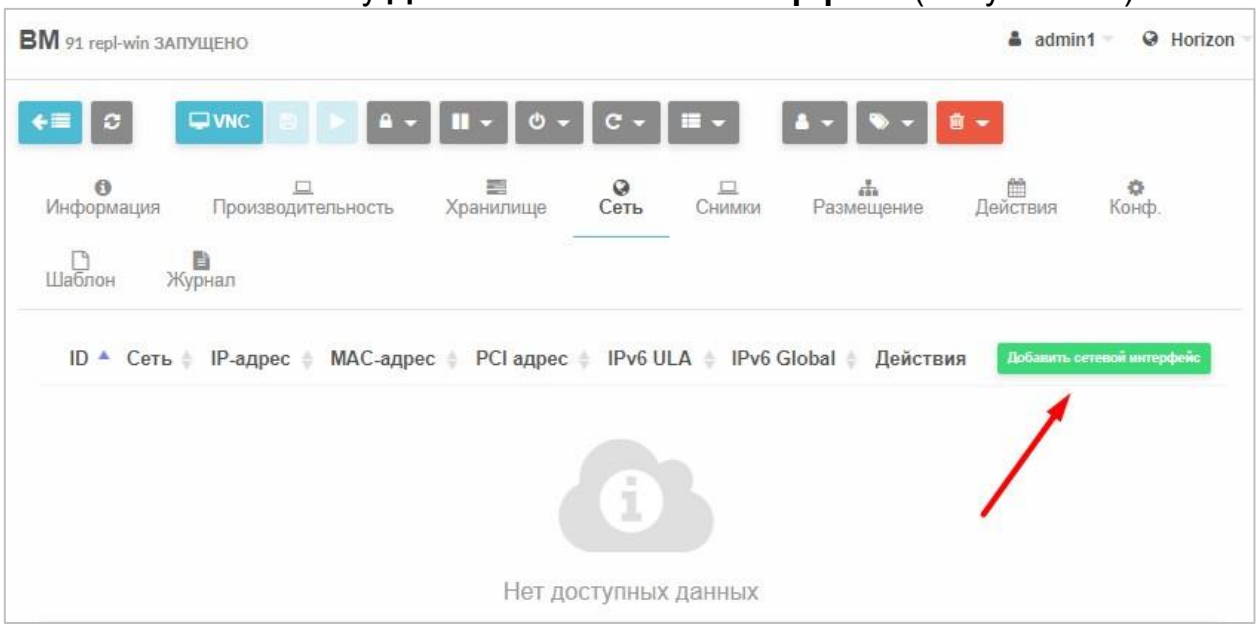


Рисунок 146 – ВМ. Вкладка «Сети»

Откроется список доступных сетей (Рисунок 147).

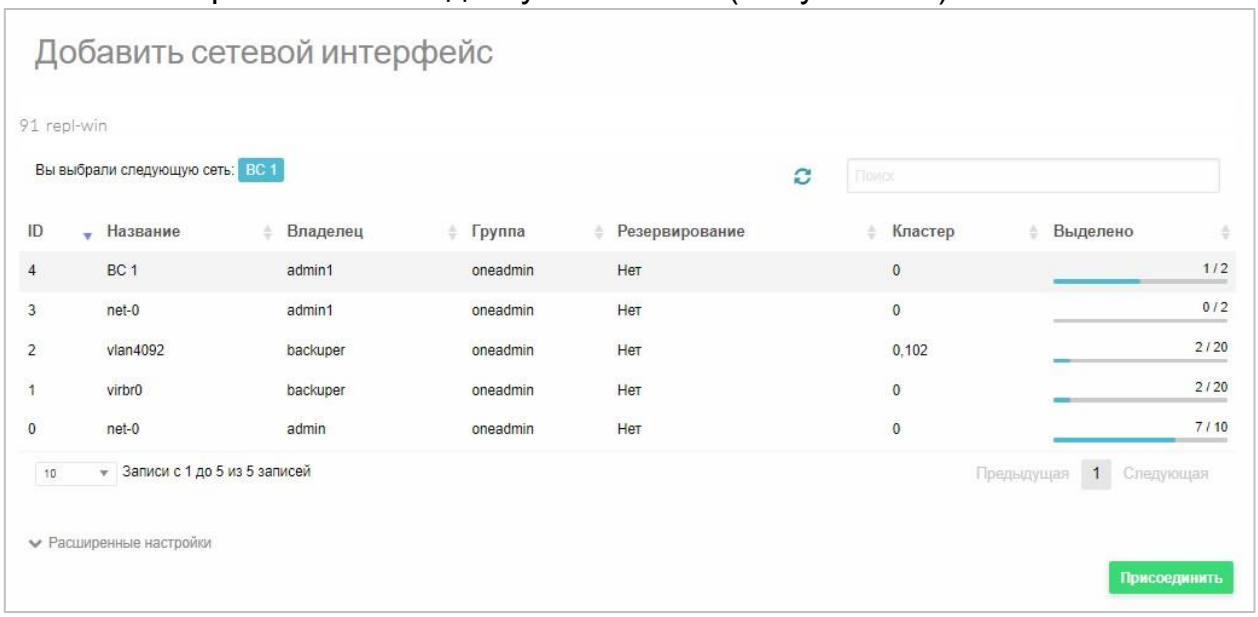


Рисунок 147 – Добавление сети в конфигурацию ВМ

г. Выбрать созданную сеть (в данном примере – ВС 1) и нажать кнопку **Присоединить**.

Добавленная сеть отобразится в списке (Рисунок 148).

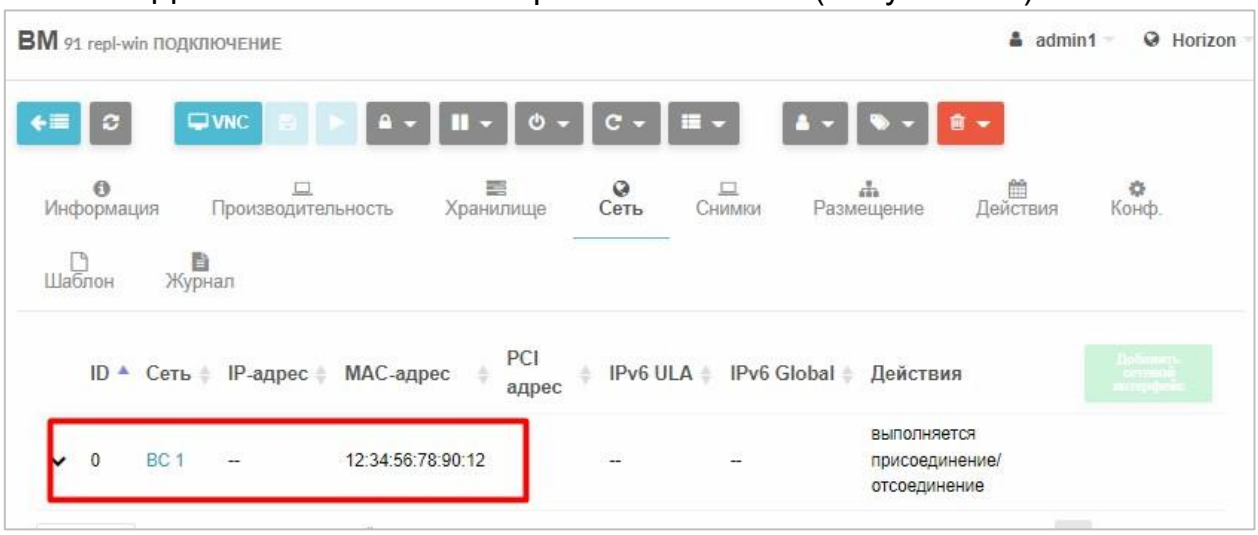


Рисунок 148 – Сеть добавлена в конфигурацию ВМ

5. Подключить виртуальную сеть с назначенным VLAN ко второй ВМ по аналогии с шагом 4.

Для проверки моста между двумя ВМ выполнить команду:

```
ovs-vsctl show
```

При наличии моста на экране отобразятся результаты, как на рисунке ниже (Рисунок 149)

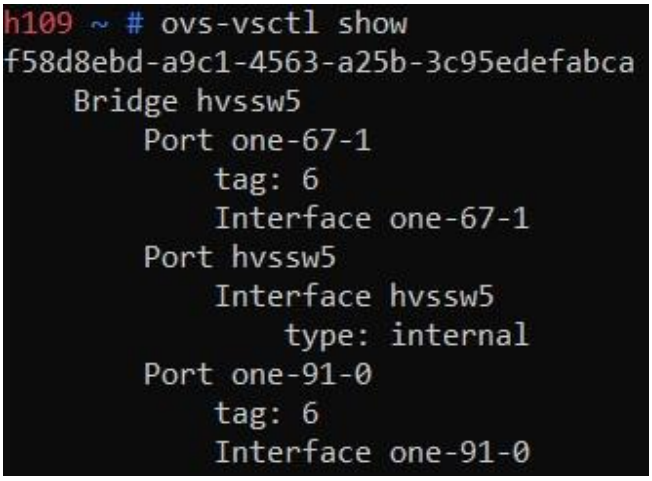


Рисунок 149 – Мост между двумя ВМ создан

Для проверки соединения между ВМ1 и ВМ2:

1. Подключиться ВМ1, нажав кнопку VNC или SPICE в зависимости от настроек подключения к ВМ (Рисунок 148).
2. В командной строке выполнить команду:

```
ping IP-адрес ВМ2
```

3.2.30 «Горячее» добавление процессоров, оперативной памяти и виртуальных дисков для работающей гостевой ОС

В СГУ реализована возможность добавления ядер процессоров, оперативной памяти и виртуальных дисков для работающей гостевой ОС без остановки работы ВМ.

Изменить количество ядер, памяти и дисков можно с помощью команд и в консоли СГУ.

Для добавления ядер выполнить команду на сервере виртуализации:

```
virsh setvcpus <name><count>
```

где:
<name> – ID ВМ;

<count> – количество добавляемых ядер.

***Примечание**. Количество добавляемых ядер не должно превышать лимит, установленный при создании шаблона ВМ в СГУ.*

Для добавления оперативной памяти выполнить команду на сервере виртуализации:

```
virsh setmem --size <размер> --domain <имя>
```

где:

<размер> – размер добавляемой памяти в МБ. Допускается указывать в ГБ: <размер>G;

<имя> – имя в формате one-N, где N - ID в СГУ. *Например*, если в СГУ ID ВМ 73, то он записывается как one-73.

***Примечание**. Размер добавляемой памяти не должен превышать лимит в 1095 МБ.*

Диск добавляется в консоли СГУ.

Для добавления количества ядер и/или объема оперативной памяти в СГУ:

1. В разделе **Машины** → **ВМ** выбрать ВМ нажатием.

   Откроется окно информации о ВМ.

2. Перейти на вкладку **Производительность**.

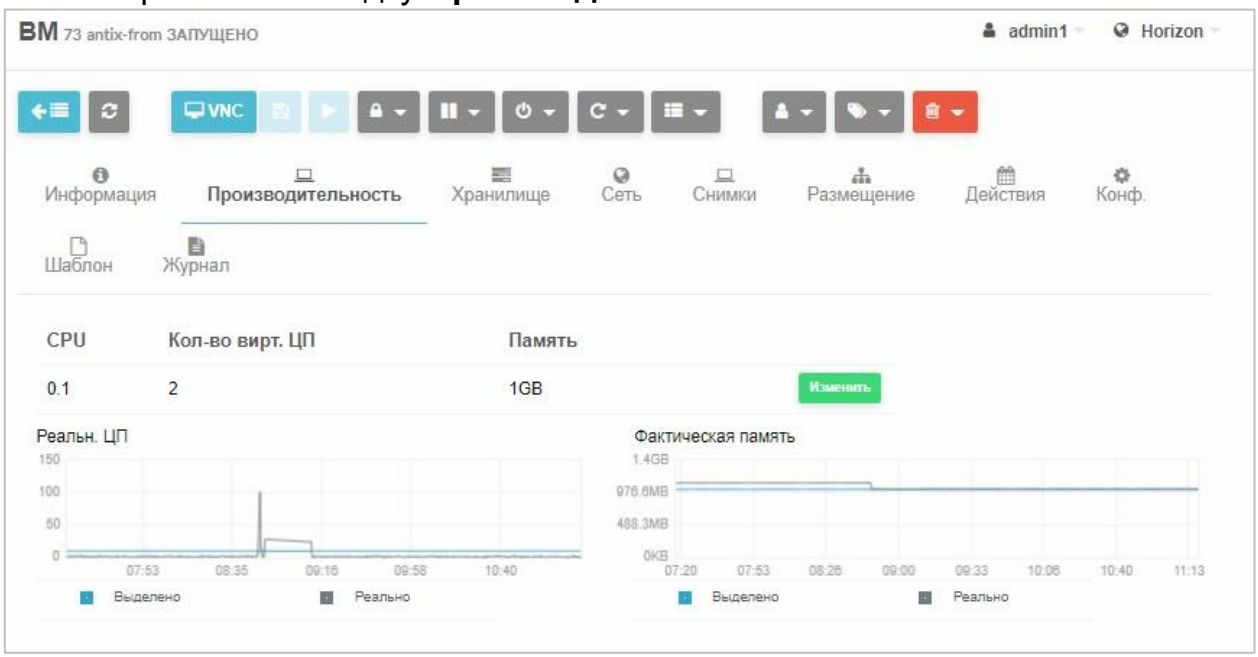


Рисунок 150 – Параметры производительности ВМ

3. Нажать кнопку Изменить (Рисунок 150).

   Откроется окно «Базовые характеристики» (Рисунок 151).

4. Изменить значения полей и нажать кнопку Изменить.

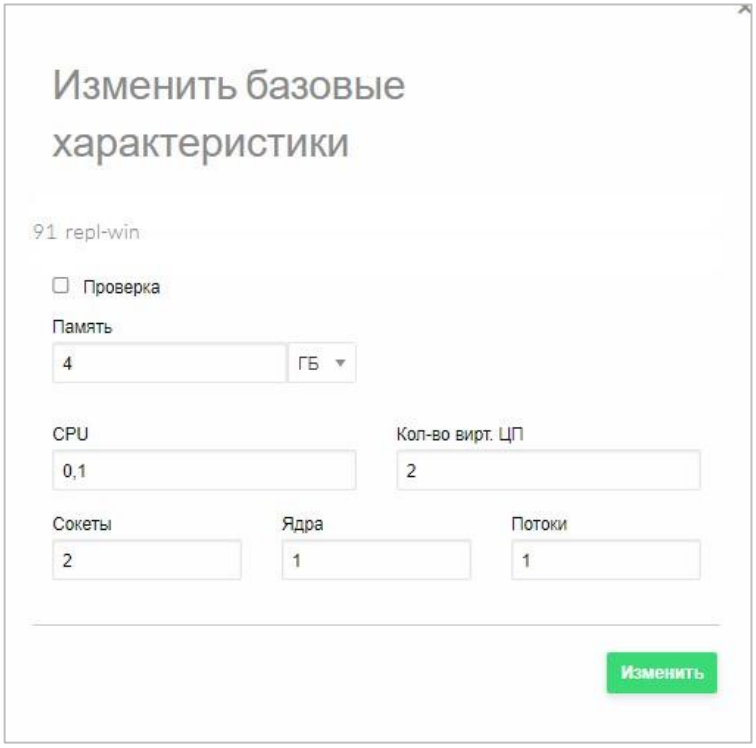


Рисунок 151 – Изменение параметров производительности ВМ **Для добавления дисков:**

1. В разделе **Машины** → **ВМ** выбрать ВМ нажатием. Откроется окно информации о ВМ.
2. Перейти на вкладку **Хранилище**.
3. Нажать кнопку Добавить диск (Рисунок 152).

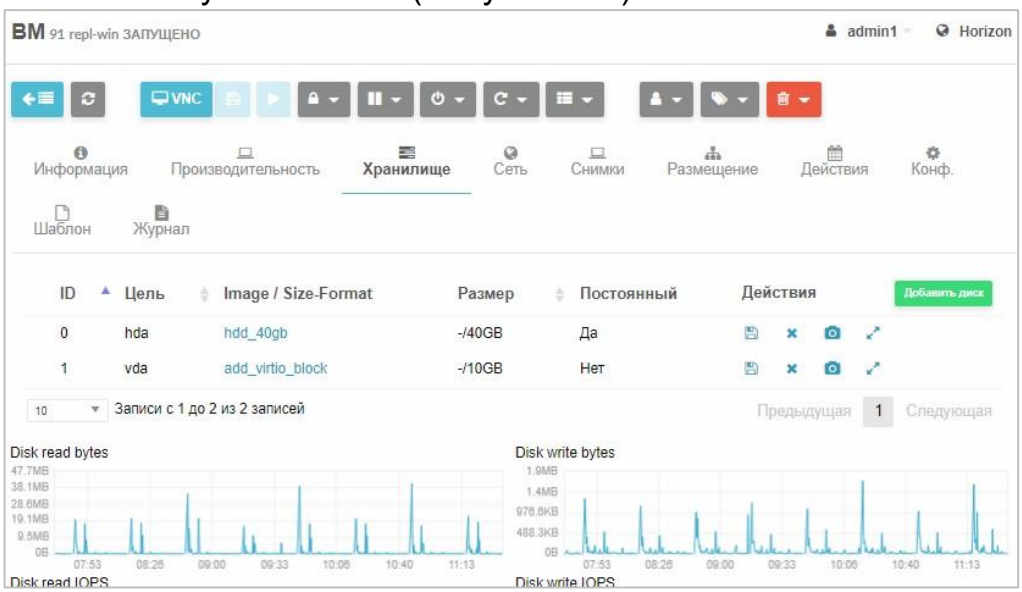


Рисунок 152 – Список хранилищ, подключенных к МВ Откроется окно со списком доступных дисков (Рисунок 153).

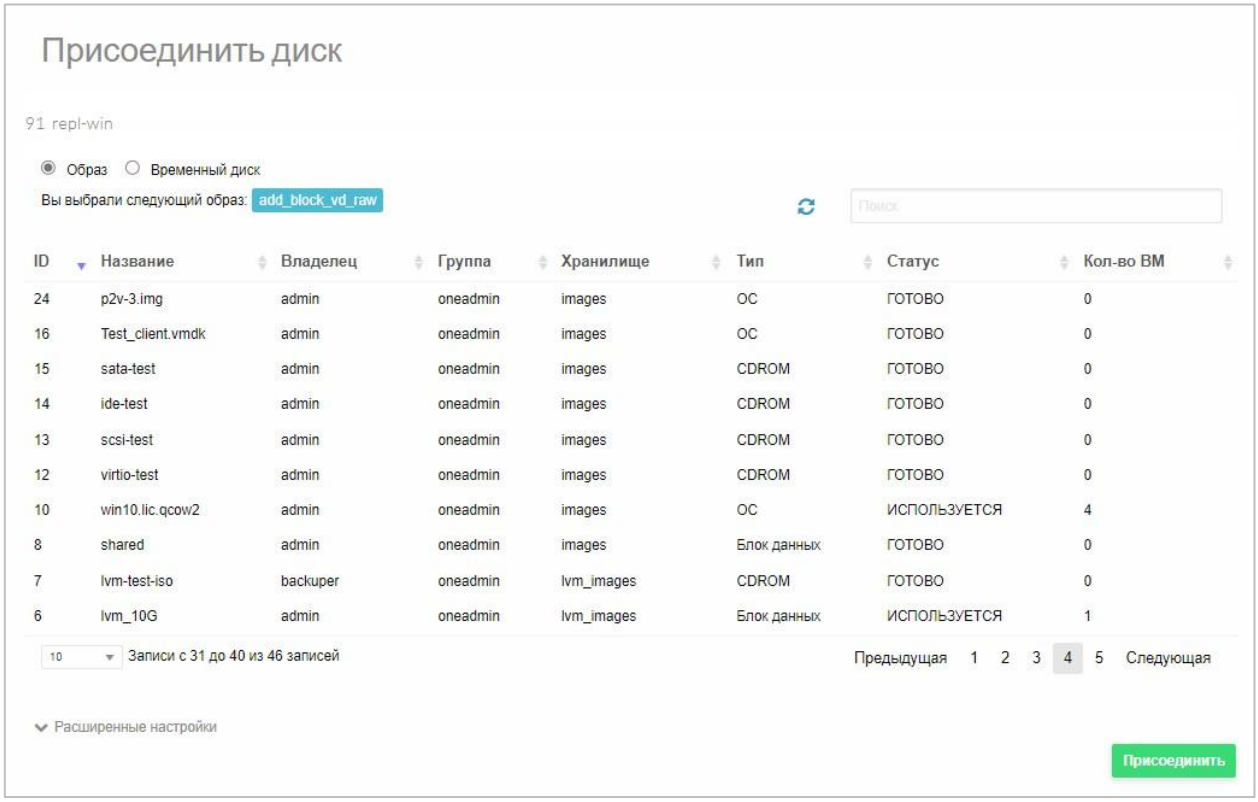


Рисунок 153 – Добавление диска к ВМ

4. Выбрать диск и нажать кнопку Присоединить.

3.2.31 Создание кластера высокой доступности

Кластер – это две или более самостоятельные системы, соединенные в единую систему высокого уровня доступности посредством специального программного и аппаратного обеспечения и представляющие с точки зрения пользователя единый аппаратный или программный ресурс.

Задача создания кластера заключается в обеспечении согласованной работы всех узлов для достижения поставленной цели. Целью может быть:

- высокая устойчивость, или доступность (HA, High Availability);
- высокая вычислительная способность (HP, High Performance);
- параллельное вычисление;
- параллельное обслуживание запросов.

Отказоустойчивый кластер (High-Availability, HA) — кластер (группа серверов), спроектированный в соответствии с методиками обеспечения

высокой доступности и гарантирующий минимальное время простоя за счёт аппаратной избыточности.

Без кластеризации сбой сервера приводит к тому, что поддерживаемые им приложения или сетевые сервисы оказываются недоступны до восстановления его работоспособности.

Отказоустойчивая кластеризация исправляет эту ситуацию, перезапуская приложения на других узлах кластера без вмешательства администратора в случае обнаружения аппаратных или программных сбоев. Процесс перезапуска известен как *аварийное переключение*. В рамках этого процесса ПО кластеризации может дополнительно настроить узел перед запуском приложения на нём (например, импортировать и смонтировать соответствующие файловые системы, переконфигурировать сетевое оборудование или запустить какие-либо служебные приложения).

Для создания HA-кластера (кластера высокой доступности):

1. Подключить к «Иридиум» общее хранилище типа **Образы** и в разделе **Хосты имеющие доступ** указать IP-адреса серверов виртуализации (минимум два) (см. п. 3.2.7);
2. Загрузить образ ВМ на общее хранилище типа **Образы**.
3. Создать образ пустого диска на общем хранилище типа **Образы** (п. 3.2.9.2);
4. Создать ВМ как описано в п. 3.2.18.
5. Перейти в раздел **Машины** → **Кластеры ВД**, установить флажок у ВМ, которую планируется запустить в режиме высокой доступности, и нажать кнопку **Создать кластер ВД** (Рисунок 154).

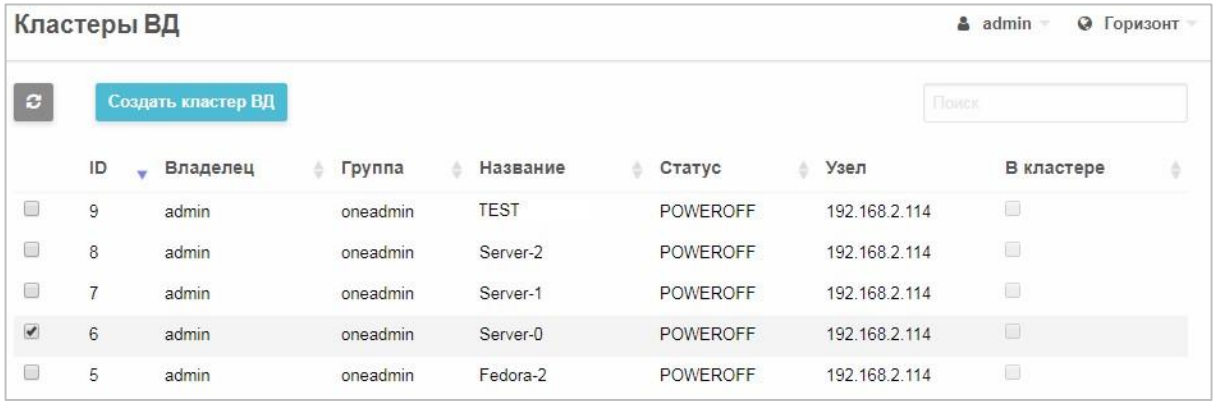


Рисунок 154 – Кластеры HA

Откроется окно **Настроить кластер ВД** (Рисунок 155).

6. В окне **Настроить кластер ВД** выделить не менее двух узлов, на которых сможет работать ВМ в составе кластера, и нажать кнопку **Создать** (Рисунок 155).

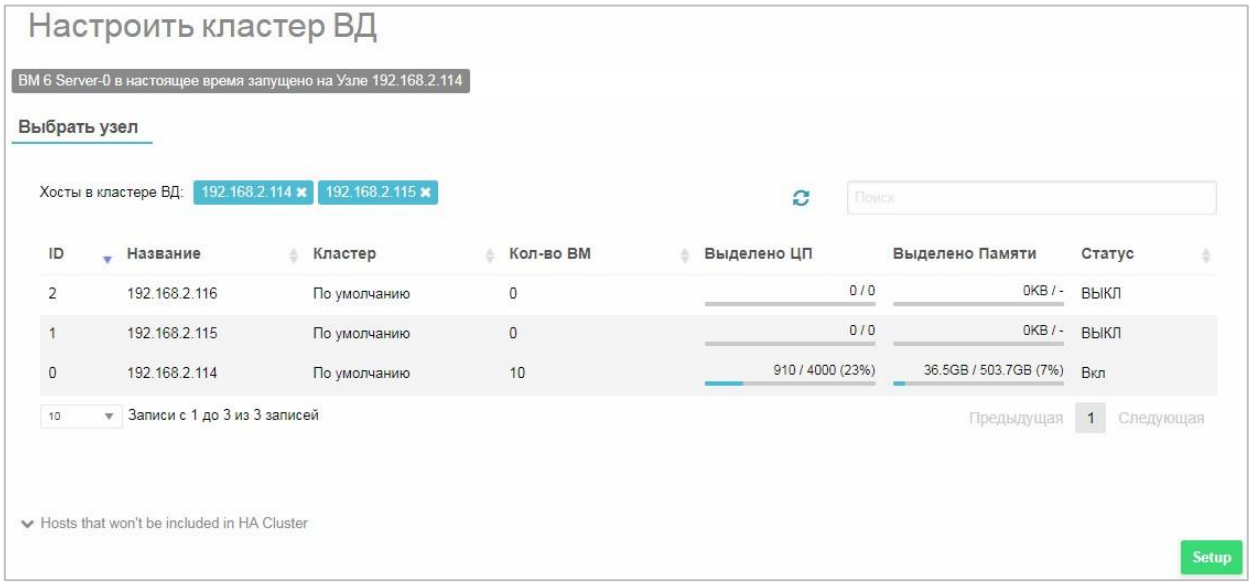


Рисунок 155 – Конфигурирование кластера ВД

После окончания конфигурирования кластера в списке ВМ (Рисунок 154) напротив настроенной ВМ в столбце **ВД кластер** появится флажок, подтверждающий перевод ВМ на работу в режиме высокой доступности.

3.2.32 Общесистемный журнал событий

Для просмотра общесистемного журнала событий следует перейти в раздел **Настройки** и затем на вкладку **Журнал** (Рисунок 156).

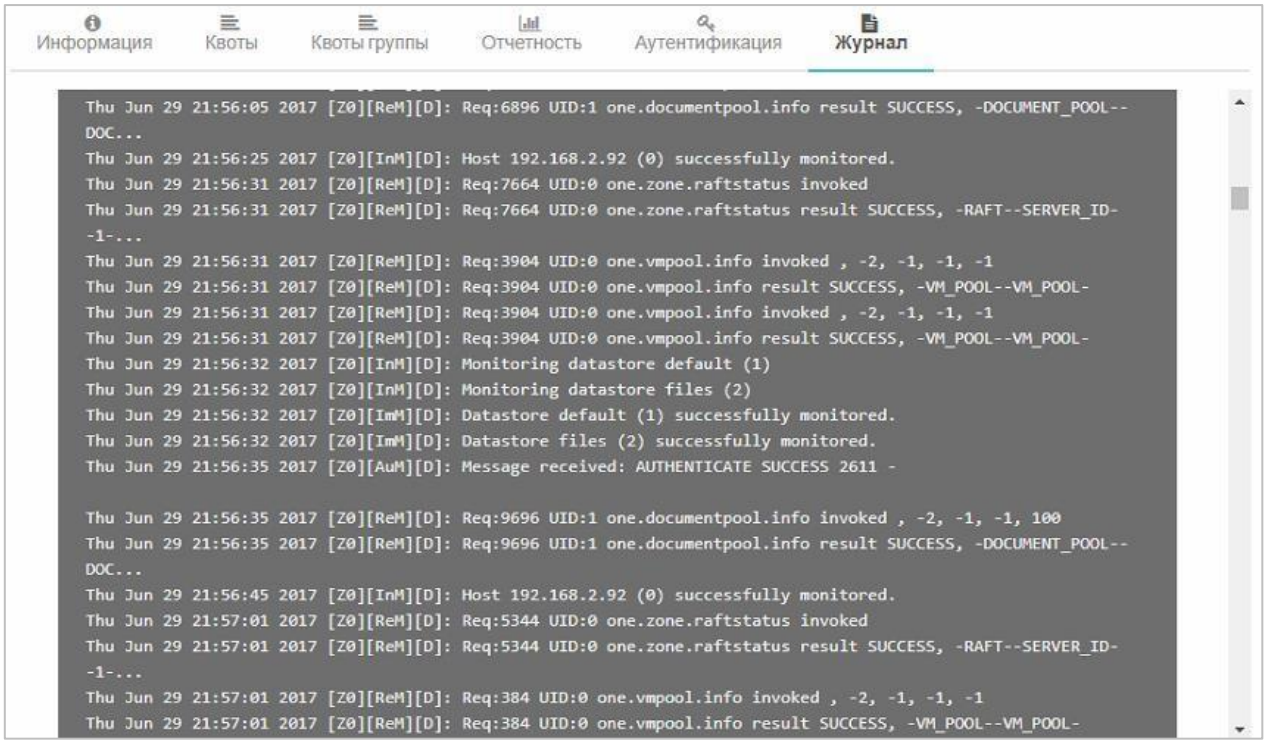


Рисунок 156 – Общесистемный журнал событий

В журнал заносятся:

- события, перечисленные в таблице ниже (Таблица 8).

Таблица 8 – События системного журнала

Событие	Запись в журнале
Авторизация пользователя/администратора в интерфейсе управления	Login: User: <имя_пользователя> GROUP:<имя_группы>
Ошибки аутентификации пользователя	RUNNING
Запуск контроллера	Oned started in solo mode
Событие	**Запись в журнале**
Изменения состояния вычислительного модуля	Host <имя_вычислительного_модуля> successfully monitored

Добавления нового вычислительного модуля	User: <имя_пользователя> one.cluster.addhost , <№_вычислительного_модуля>
Удаление вычислительного модуля	User:<имя_пользователя> one.host.delete , <№_вычислительного_модуля>
Создание снимка состояния ВМ	reason=saved vm=<имя_ВМ>
Клонирование ВМ	vm=<имя_ВМ>-clone… res=succes

– данные аудита функций безопасности.

Для получения записей аудита функций безопасности необходимо нажать сочетание клавиш **Ctrl+F** и ввести соответствующее ключевое слово из левой колонки таблицы ниже (Таблица 9).

Таблица 9 – События аудита безопасности

Обозначение события в журнале	Событие аудита безопасности	Запись в журнале	Комментарий
PROLOG	сведения о создании ВМ	VM <ID_ВМ>	ID ВМ, соответствующий отображаемому в списке ВМ в СГУ
terminate	сведения об удалении ВМ	UID:<ID_ВМ> USER:<имя пользователя>	
one.vm.action	сведения о запросах на доступ к ВМ	UID:<имя пользователя запустившего ВМ>	
chown	сведения об изменении правил разграничения доступа пользователей к ВМ		
finalized	данные о завершении функции аудита		
Обозначение события в журнале	**Событие аудита безопасности**	**Запись в журнале**	**Комментарий**

[AUTH]	данные об авторизации пользователей и администраторов		

3.2.33 Управление ограничениями на использование ресурса

Система квот отслеживает использование системных ресурсов пользователями и группами и позволяет администратору устанавливать ограничения на использование этих ресурсов. Лимиты квот могут быть установлены для:

- пользователей, чтобы индивидуально ограничить использование данным пользователем.
- группы, чтобы ограничить общее использование всеми пользователями в данной группе.

Система квот позволяет отслеживать и ограничивать использование:

- хранилищ, чтобы контролировать объем хранилища, выделяемый каждому пользователю / группе для каждого хранилища данных.
- памяти/CPU, чтобы ограничить общую память, ЦП или количество экземпляров ВМ.
- сети, чтобы ограничить количество IP-адресов, которые пользователь / группа может получить из данной сети.
- образов, для ограничения количества экземпляров ВМ от определенного пользователя / группы, использующих данный образ. Можно воспользоваться этой квотой, если образ содержит расходные ресурсы (например, лицензии на ПО).

***Примечание**: при использовании хранилища Ceph в режиме гиперконвергентности используется только размер хранилища данных, системные диски в этом случае не будут затронуты. В хранилищах данных такого типа используется одно и то же пространство для системы и для образов, поэтому СГУ не знает, какое пространство используется в каждом случае.*

Для установки квот пользователя:

1. Перейти в раздел **Система** → **Пользователи**.
2. Выбрать пользователя нажатием.
3. Перейти на вкладку **Квоты.**

   Откроется окно информации об ограничениях (Рисунок 157).

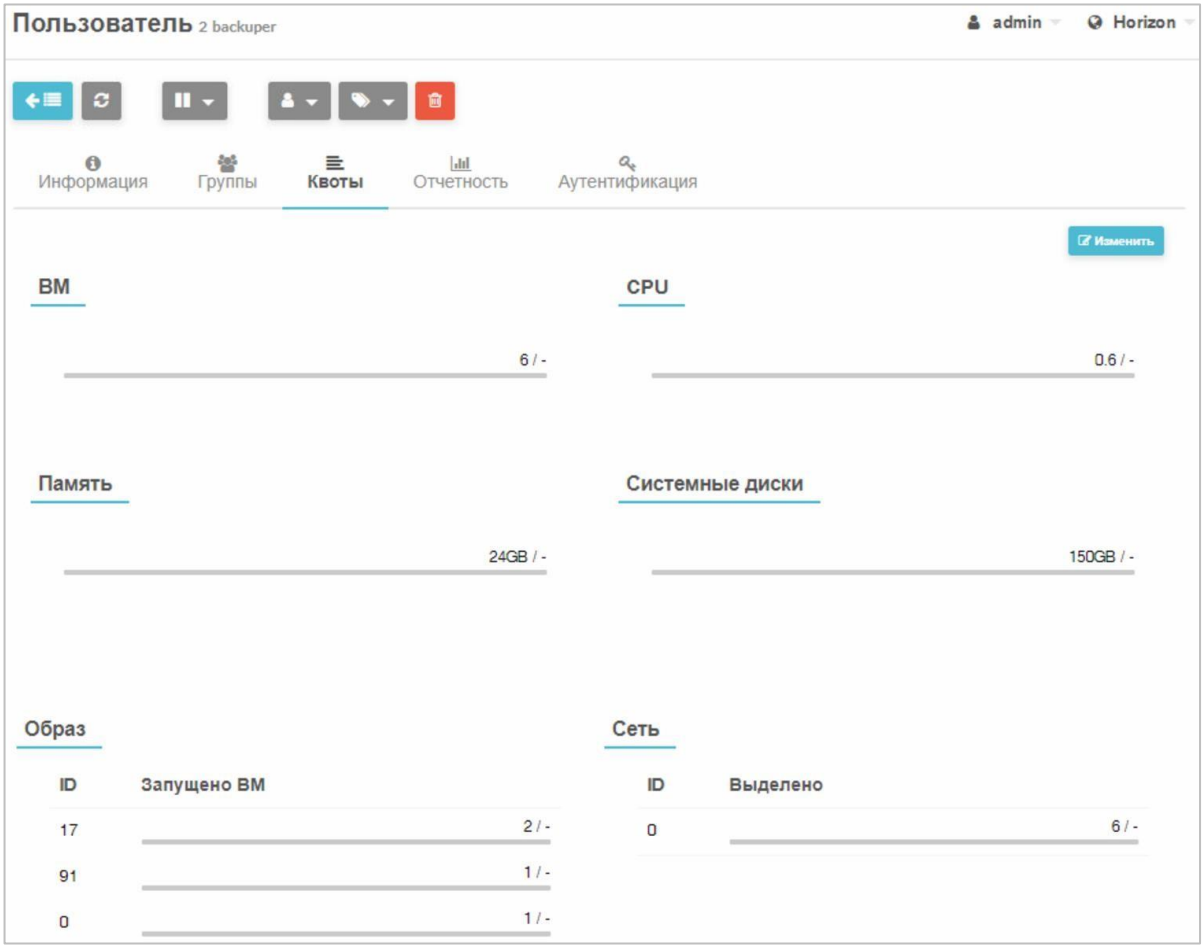


Рисунок 157 – Управление квотами

4. Нажать кнопку **Изменить** в правом верхнем углу.

   Станут доступны параметры для редактирования (Рисунок 158).

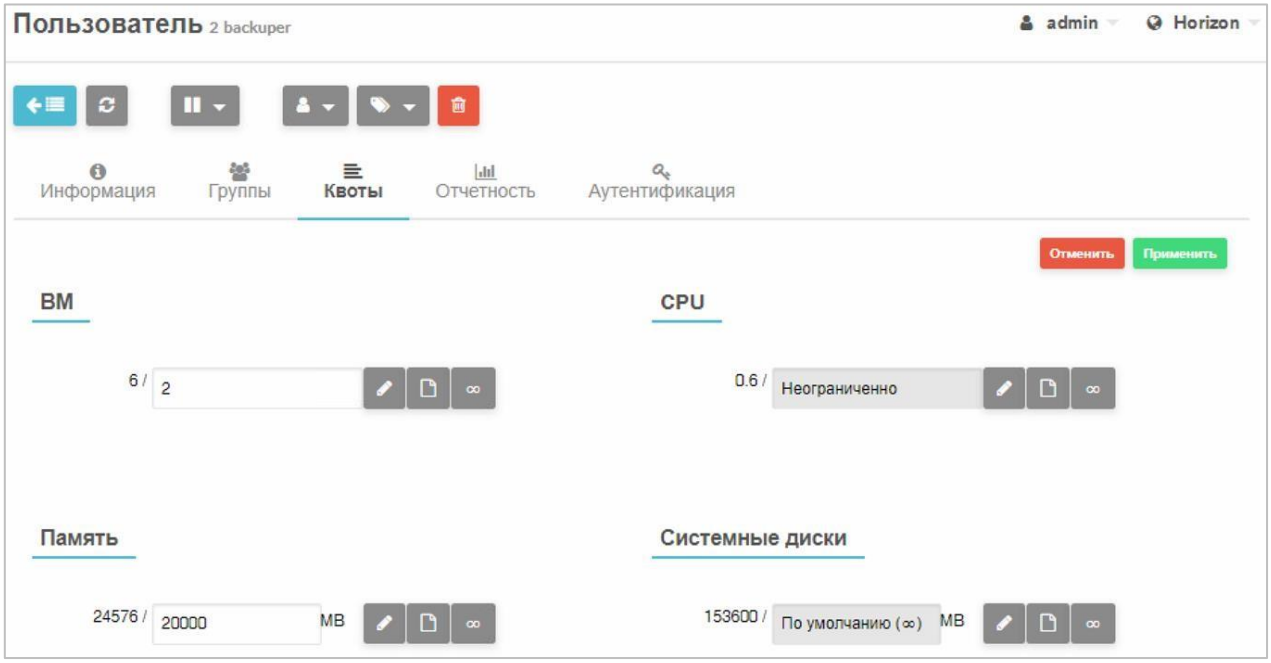


Рисунок 158 – Редактирование квот

5. Задать квоты на ресурсы в соответствующих полях (Таблица 10).

Таблица 10 – Ресурсы, на которые устанавливаются ограничения

Поле	Значение
ВМ	максимальное количество ВМ, которое можно создать
CPU	максимальная мощность ЦП, которую могут запросить ВМ пользователя
Память	максимальный объем памяти в МБ, который может быть запрошен ВМ пользователя
Системные диски	максимальный размер (в МБ) системных дисков, который может запрашиваться ВМ пользователя
Образ	максимальное количество ВМ, которые могут использовать этот образ одновременно
Сеть	максимальное количество IP-адресов, которые можно арендовать из сети

Для задания квоты на ресурс воспользоваться кнопками справа от ресурса (Таблица 11).

Таблица 11 – Кнопки задания ограничений на использование ресурса

Кнопка	Назначение
	Задание значения вручную
	Установка значения по умолчанию
	Разрешение на неограниченное использование

6. Нажать кнопку **Применить** (**Ошибка! Источник ссылки не найден.**).

Для установки квот на группу пользователей:

7. Перейти в раздел **Система** → **Группы**.
8. Выбрать необходимую группу нажатием.
9. Открыть вкладку **Квоты.**
1. Дальнейшие настройки аналогичны установке ограничений для пользователей.

3.2.34 Планировщик

Планировщик СГУ отвечает за назначение между ожидающими виртуальными машинами и известными серверами виртуализации.

Алгоритм работает следующим образом:

– каждый диск запущенной ВМ требует хранилище из хранилища образов. ВМ, которые требуют больше пространства, чем доступно в настоящее время, отфильтровываются и остаются в состоянии «pending»;
– те узлы, которые не соответствуют требованиям ВМ или не имеют достаточного количества ресурсов (доступный процессор и память) для запуска ВМ, отфильтровываются;

– драйверы управления формируют ранг для узлов и хранилищ;
– ресурсы с более высоким рангом используются сначала для размещения ВМ.

Настройки планировщика расположены в директории ***/etc/one/sched.conf***.

Для настройки планировщика необходимо задать параметры в соответствии с таблицей ниже (Таблица 12).

Таблица 12 – Параметры конфигурации планировщика

Параметр	Назначение	Значение по умолчанию
MESSAGE_SIZE	Размер буфера в байтах для ответов XML-RPC	
ONE_XMLRPC	URL-адрес для подключения к службе oned	http://localhost:2633/RPC2
SCHED_INTERVAL	Время между двумя действиями планирования в секундах	30
MAX_VM	Максимальное количество виртуальных машин, запланированных в каждом планировании	5000 Использовать 0 для планирования всех ожидающих виртуальных машин каждый раз
MAX_DISPATCH	Максимальное количество виртуальных машин, фактически отправленных на хост в каждом планировании	30
MAX_HOST	Максимальное количество виртуальных машин, отправленных на данный узел в каждом планировании	10
LIVE_RESCHEDS	Выполнять миграцию при перенастройке виртуальной машины	1 – «горячая» миграция ВМ; 0 – «холодая» миграция ВМ
DEFAULT_SCHED	Определение алгоритма планирования по умолчанию	
Параметр	**Назначение**	**Значение по умолчанию**
RANK	Арифметическое выражение для ранжирования подходящих хостов на основе их атрибутов	

POLICY	Предопределенная политика: 0 – Packing. Минимизируется количество используемых хостов, размещая ВМ на узлах, чтобы уменьшить фрагментацию ВМ; 1 – Striping: Максимизируются ресурсы, доступные для ВМ, путем распространения ВМ на хостах 2 – Load-aware: максимизируются ресурсы, доступные для ВМ, путем использования узлов с меньшей нагрузкой 3 – Custom: используется пользовательский рейтинг (RANK) 4 – Fixed: Серверы будут ранжироваться в соответствии с атрибутом	
DEFAULT_DS_SCHED	Определение алгоритма планирования хранения по умолчанию	

Оптимальные значения параметров планировщика зависят от гипервизора, подсистемы хранения и количества физических хостов. Значения могут быть получены путем определения максимального количества виртуальных машин, которые могут быть запущены в системе без ошибок, связанных с гипервизором.

3.3 Операции с Системой резервного копирования

3.3.1 Назначение и условия применения Системы резервного копирования

Система резервного копирования «Иридиум» (СРК) предназначена для выполнения операций по защите данных в виртуальной среде. СРК осуществляет резервное копирование данных с целью их последующего восстановления в случае аварийных ситуаций.

СРК интегрирована с СГУ «Иридиум». Разграничение прав пользователей на запуск СРК осуществляется средствами СГУ.

СРК состоит из трех основных компонент:

- веб-интерфейс управления;
- компонент обработки заданий;
- исполнительный компонент («агент»).

Все три компонента работают асинхронно.

***Примечания**:*

1. В процессе выполнения заданий копирования и восстановления требуется остановка ВМ. Каждая ВМ должна быть настроена так, чтобы запустить надлежащий механизм остановки работы при подаче сигнала завершения работы ACPI (см. п. 3.3.13).

2. Для копирования без остановки при использовании типа дисков qcow2, в ВМ необходимо добавить специальное программное обеспечение — qemu-guestagent. Необходимо также произвести настройку ВМ в СГУ (см. п. 3.3.12).

3.3.2 Запуск Системы резервного копирования

Модуль размещается в контейнере **docker** и запускается или внутри специальной виртуальной машины с **docker** или внутри «Иридиум».

Для запуска СРК:

1. Скопировать образ какой-либо каталог, например: /data/0/.
2. Если образ заархивирован, разархивировать командой: unzip имя_архива.zip.
3. Загрузить образ контейнера на хосте:

```
docker load < /data/0/bus.tar.bz2
```

4. Подписать образа контейнера:

```
hvs_sign
```

5. Создать папки для хранения журналов (логов) и БД модуля, например:

```
mkdir -p /home/backuplogs
```

6. Создать в указанной папке файл конфигурации **backup.conf**, например:

```
//отображаемое название модуля для систем, встраивающих Иридиум
// по умолчанию = Иридиум app_name=Иридиум
//Выводить ли отладочные сообщения в log? По умолчанию - no
debug=yes
//Количество дней хранения файлов-протоколов, по умолчанию -30
logcount=45
//Настройки веб интерфейса бэкапа - порт
backup_port=2635 // - маска подсети
backup_bind=0.0.0.0
// - использовать https (нужны файлы backup.key, backup.crt).
// По умолчанию - no
backup_https=yes
//Интервал запуска планировщика копирования, сек — в диапазоне
30..180
// По умолчанию - 60 interval=60
//Хост Иридиума (кластера)
gorizont_host=192.168.2.4
//Пользователь ssh По умолчанию - oneadmin sshuser=oneadmin
//максимальное время выпонения команд ssh (сек) 5..300, по
умолчанию -120 ssh_timeout=120
//Взаимодействие с СГУ по xml rpc -хост  СГУ (кластера)
//  По умолчанию = gorizont_host
onerpchost=192.168.2.4 // - URL
, по умолчанию /RPC2
oneurl=/RPC2
// - пользователь , по умолчанию - backuper onerpcuser=backuper
// - таймаут (сек) 5..60, по умолчанию -5 onetimeout=10
// - порт, по умолчанию - 2634
oneport=2634
// - использование https для взаимодействие с СГУ?
// Использовать https для взаимодействие с СГУ, по умолчанию
=no и
// oneport д.б. 2633 onerpcssl=yes
//взаимодействие с агентами копирования - порт, по умолчанию -
9000 agentport=9000
```

```
// - Таймаут (сек) ожидания ответа агентов копирования , по
умолчанию 5 agenttimeout=5
//Максимальное время сохранения СГУ (сек), по умолчанию - 300
save_sgu_time_max=300
//время на остановку ВМ (сек), если не задано, по умолчанию -
60
shutdown_timeout=60
      // Размер снимка LVM в Мб или %
      // зависит от интенсивности изменения тома LVM во время
копирования
      // объем изменений не должен превышать указанный, иначе
будет ошибка
      // по умолчанию — 5%
lvm_backup_size=5%
//СГУ идентификатор ceph— должен совпадать с указанным при
установке
// ceph, по умолчанию - libvirt ceph_id=libvirt
//процент использоватия процессоров lbzip2 при восстановлении
ВМ
// по умолчанию -10 unzip_proc=10
//языковые настройки — список языков, в данной версии —
русский,
// английский (ru,en)  — не менять, требуется изменение
программы! locales=en,ru
//выбрать язык, по умолчанию — русский (ru) current_locale=ru
// Настройки агента Qemu для fsfreeze в ВМ (для версий 2.6.18 и
выше) qga_count=3  // от 1 до 5  = число попыток  qga_sleep=15
// от 15 до 60= интервал между попытками при ошибке секунд$
```

При использовании протокола https для работы СРК, необходимо в этот же каталог записать ключ (backup.key) и сертификат (backup.crt).

7. Создать в СГУ служебного пользователя **backuper** — как указано в конфигурационном файле (с паролем – backuper), в группе администраторов для доступа к СГУ.
8. Запустить модуль, где x.x.x – номер версии:

```
docker run -itd --net=host  -v
/home/backuplogs:/var/log/one/backup --name bus
--restart=always bus:XXX /bin/bash /opt/backup/start
Проверяем наличие ключа ssh  docker exec bus ls
root/.ssh/id_rsa
-rw------- 1 root root 1675 Apr 23  2019 /root/.ssh/id_rsa И
меняем права на ключ ssh, если они отличаются от указанных
docker exec bus chmod 0600 /root/.ssh/id_rsa
```

9. Для запоминания в контейнере пароля пользователя *backuper* набрать команду в адресной строке браузера:

```
http://адрес_машины_модуля:2635
```

или в зависимости от настроек (backup_https)

```
https://адрес_машины_модуля:2635
```

10. Войти в СРК под учетной записью пользователя **backuper**.
11. В СГУ в разделе **Общие настройки** задать параметры **Хранилище** и **Количество копий**, и нажать кнопку **Сохранить**.
12. Если контейнер не запускается, то посмотреть возможные ошибки запуска модулей в контейнере можно путем выполнения команд внутри ВМ (или Иридиум):

```
cat /home/backuplogs/error.log      //для компонента интерфейса  cat /home/backuplogs/ag-error.log   //для компонента агента копирования
```

13. Просмотреть и отредактировать загруженный конфигурационный файл можно путем выполнения команды

```
docker exec bus /opt/backup/editconf <порт>
```

по умолчанию порт- 8081.

14. Набрать в браузере:

```
http://адрес_машины_модуля:<порт>
```

Вид окна редактирования конфигурации представлен на рисунке ниже (Рисунок 159).

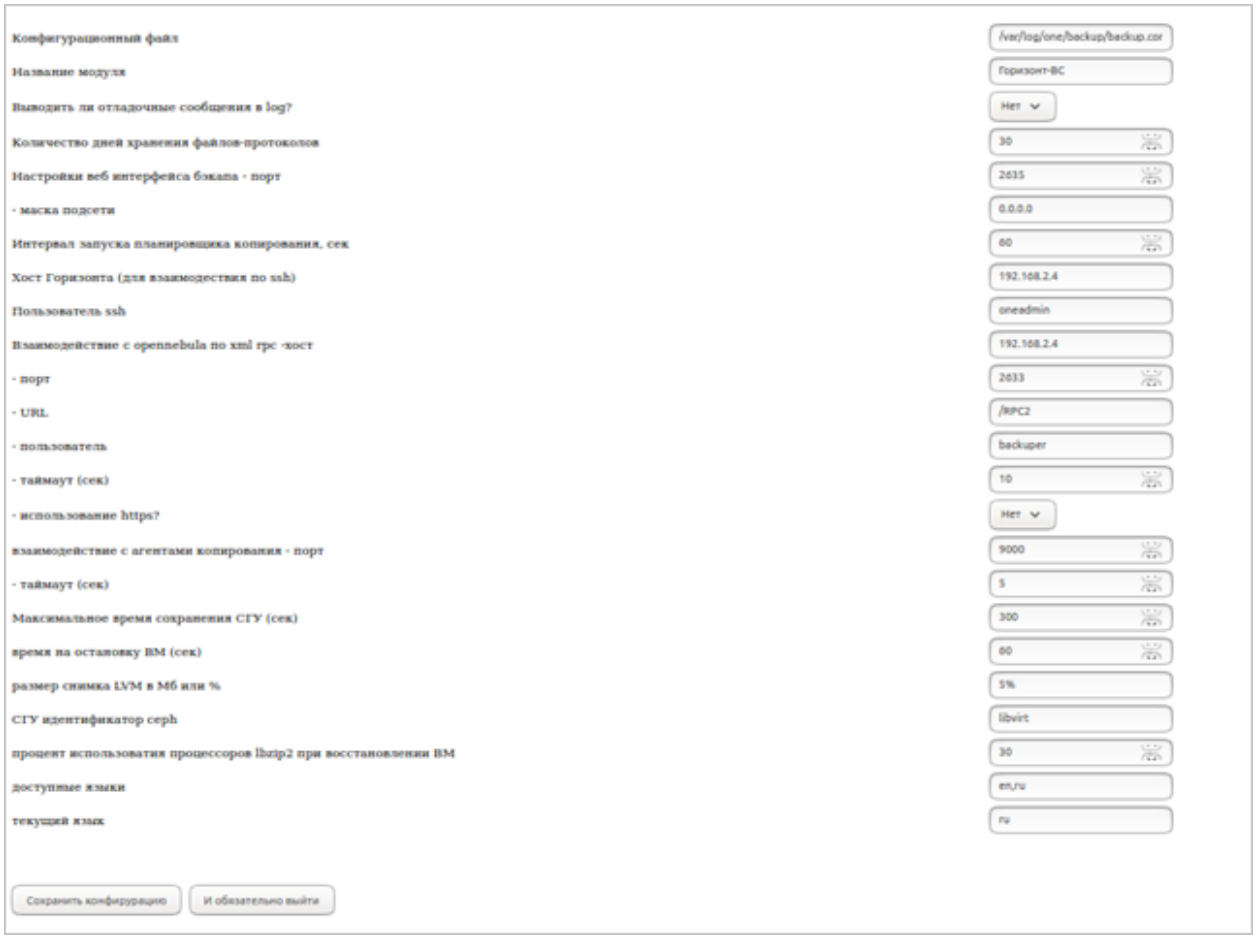


Рисунок 159 – Окно конфигурации

15. Нажать кнопку Сохранить конфигурацию.
16. Нажать **Выйти**.

    Новый файл конфигурации будет сохранен, а старый переименован.
17. Чтобы применить изменения, необходимо перезапустить контейнер командой:

```
docker container restart bus
```

Для остановки и удаления контейнера при необходимости перезапуска выполнить команды:

```
docker container stop bus
docker container rm bus
```

Для удаления образа контейнера для переустановки и обновления подписи (п.1.1.) выполнить команду, где x.x.x – номер версии образа:

```
docker image rm bus:x.x.x
```

3.3.3 Подключение и вход в Систему резервного копирования

Для подключения к СРК ввести в адресной строке браузера IP-адрес виртуальной машины, на которой установлена СРК, и порт 2635:

http://адрес_виртуальной_машины_срк:2635 или (в

зависимости от настроек при запуске):

https://адрес_виртуальной_машины_срк:2635

Появится приглашение ввода имени пользователя

и

В открывшемся окне аутентификации ввести имя пользователя и пароль (Рисунок 160).

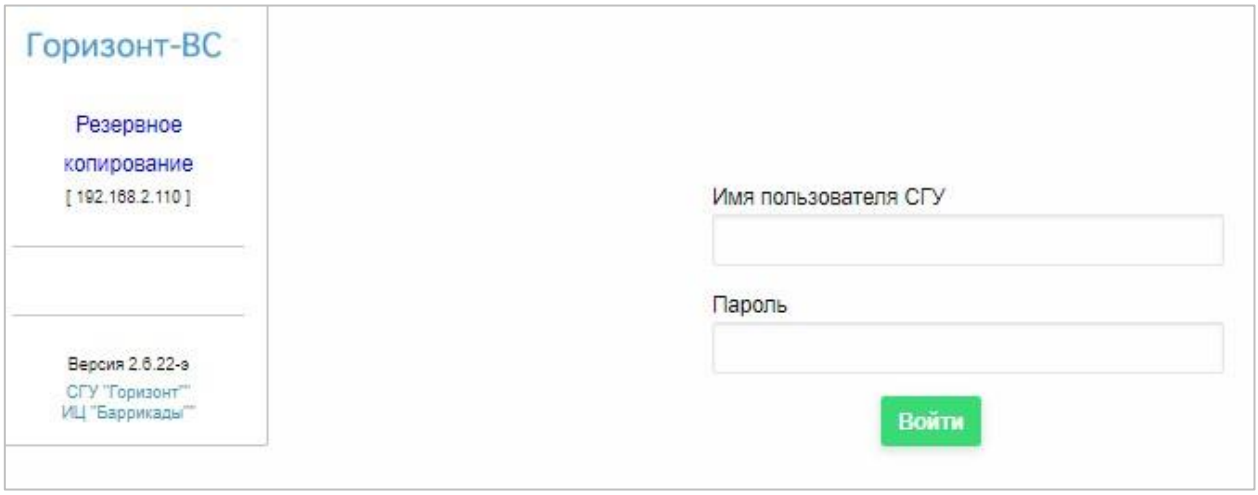


Рисунок 160 – Авторизация в СРК

***Примечание**. Имя пользователя и пароля задаются администратором СГУ.*

После успешной авторизации пользователя ему становится доступна панель управления резервным копированием.

В левой части основного содержится меню, в правой – область просмотра информации и поля для настроек (Рисунок 161).

3.3.4 Общие настройки резервного копирования

Данные настройки СРК сохраняются для всех компонент резервного копирования и состоят из следующих полей (Рисунок 161).

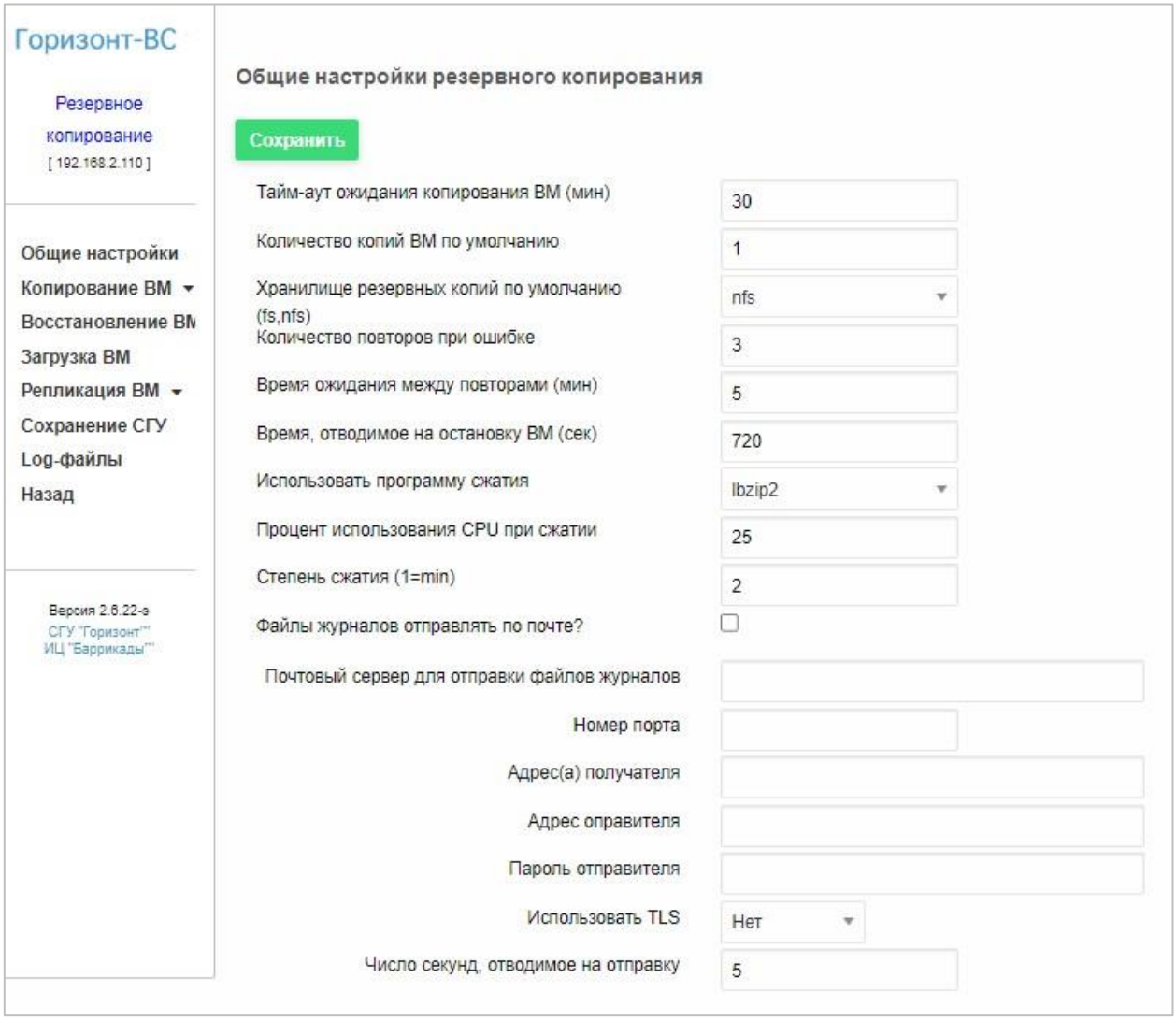


Рисунок 161 – Общие настройки резервного копирования

- **Тайм-аут ожидания копирования виртуальных машин ВМ (мин)** – задает максимальную длительность операции резервного копирования для одной виртуальной машины (ВМ). При превышении этого времени копирование прерывается;

- **Количество копий ВМ по умолчанию** — задает число одновременно существующих копий ВМ. Старые копии автоматически удаляются;
- **Хранилище резервных копий по умолчанию** — хранилище СГУ, в которое будут копироваться ВМ. В указанном хранилище создается папка **backup,** в ней папки с **именами ВМ**, а в папке ВМ - папки вида **ГГГГММДД_ЧЧММ —** по дате и времени окончания резервного копирования;

- **Количество повторов при ошибке** — задает число попыток повтора резервного копирования при ошибках;
- **Время ожидания между повторами (мин)** — задает число минут задержки между повторными попытками копирования;
- **Время, отводимое на остановку ВМ (сек)** — задает число секунд на остановку ВМ;
- **Использовать программу сжатия** — выбирается из списка (lbzip2);
- Процент использования CPU при сжатии;
- **Степень сжатия (1=мин)** − параметр программы сжатия, число от 1 до 9. 1 означает малое сжатие, но быстрое, 9 − максимальное сжатие, но медленное;
- **Файлы журналов отправлять по почте**? — при установке флага файлы журналов резервного копирования будут автоматически передаваться по e-mail администратору (или нескольким).

  Настройка передачи по почте осуществляется в нижней части экрана:

  • в поле **Почтовый сервер для отправки файлов журнала** указывается адрес почтового сервера;
  - в поле **Номер порта** указывается номер порта подключения почтового сервера;
  - в поле **Адрес(а) получателя** указываются через «;» адреса, на которые будут приходить файлы журналов;
  - в поле **Адрес отправителя** указывается e-mail, с которого будут отправляться файлы журналов;
  - в поле **Пароль отправителя** задается пароль отправителя;
  - **Использовать TLS** − включение/отключение шифрования TLS;
  - в поле **Число секунд, отводимое на отправку** задается таймаут на отправку файлов журнала.

3.3.5 Копирование виртуальной машины

Данный раздел позволяет пользователю выполнять следующие функции:

- просматривать список заданий на копирование ВМ;
- создавать задания на копирование ВМ;
- просматривать состояния компонентов копирования на всех узлах гипервизора «Иридиум» и список выполняющихся заданий по сохранению ВМ;
- просматривать журнал резервного копирования.

3.3.5.1 Задания

Для просмотра списка и создания заданий на резервное копирование ВМ перейти в подраздел **Копирование ВМ → Задания.**

На экране отобразится список заданий (Рисунок 162).

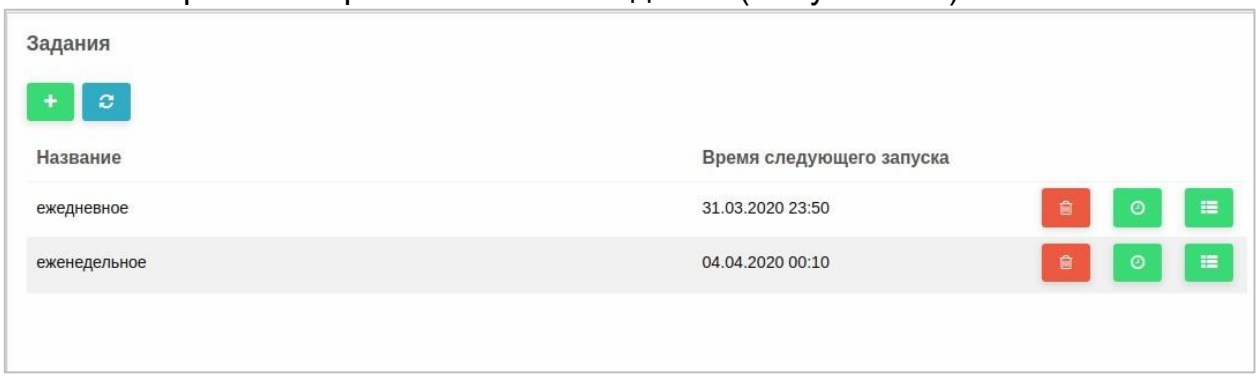


Рисунок 162 – Список заданий на копирование

Администратор может задать произвольное число заданий на резервное копирование.

3.3.5.1.1 Создание задания

Для создания задания:

1. Нажать кнопку + в верхнем левом углу (Рисунок 162).
2. В открывшемся окне указать название задания и нажать кнопку Сохранить (Рисунок 163).

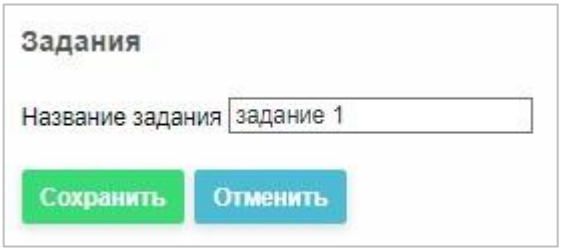


Рисунок 163 – Название задания

Задание будет добавлено в список.

Для управления заданием предназначены кнопки справа от его названия (Таблица 13).

Таблица 13 – Кнопки управления заданиями

Кнопка	Назначение
	Удаление задания
	Установка расписания задания
	Переход к списку сохраняемых ВМ

Для удаления задания нажать кнопку и подтвердить действие в открывшемся окне (Рисунок 164).

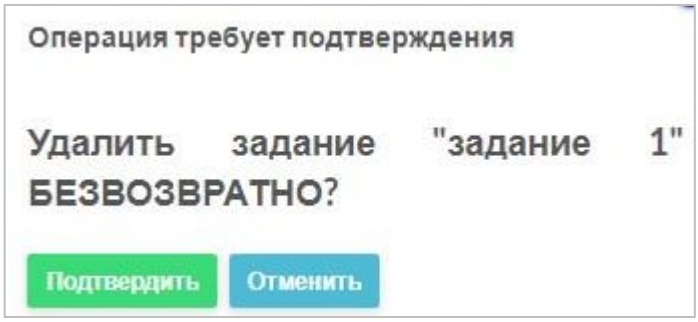


Рисунок 164 – Подтверждение удаления задания

3.3.5.1.2 Расписание резервного копирования

Для просмотра и редактирования задания на копирование, нажать  справа от задания (Рисунок 162).

Откроется окно, представленное на рисунке ниже (Рисунок 165).

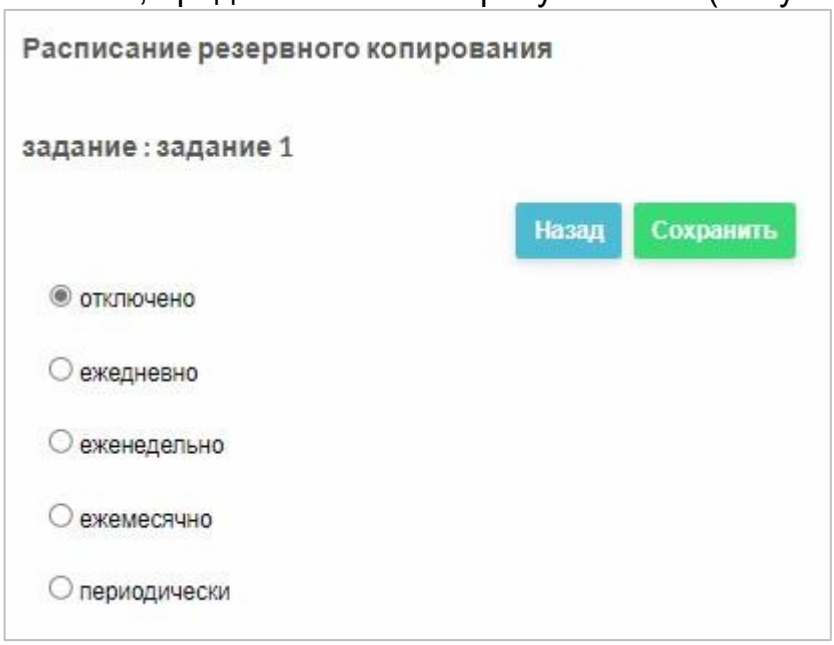


Рисунок 165 – Расписание резервного копирования

Для задания на копирование может быть определено одно из расписаний его исполнения, которые задается установкой соответствующего флажка (Рисунок 165 и Рисунок 166):

- отключено (для сохранения и последующего использования);
- выполнятся ежедневно (каждый день, по рабочим дням, по выходным дням);
- выполняется еженедельно в заданный день недели;
- выполняется ежемесячно в заданный день заданной недели;
- выполняться периодически с интервалом в заданное число часов (дней, недель, месяцев).

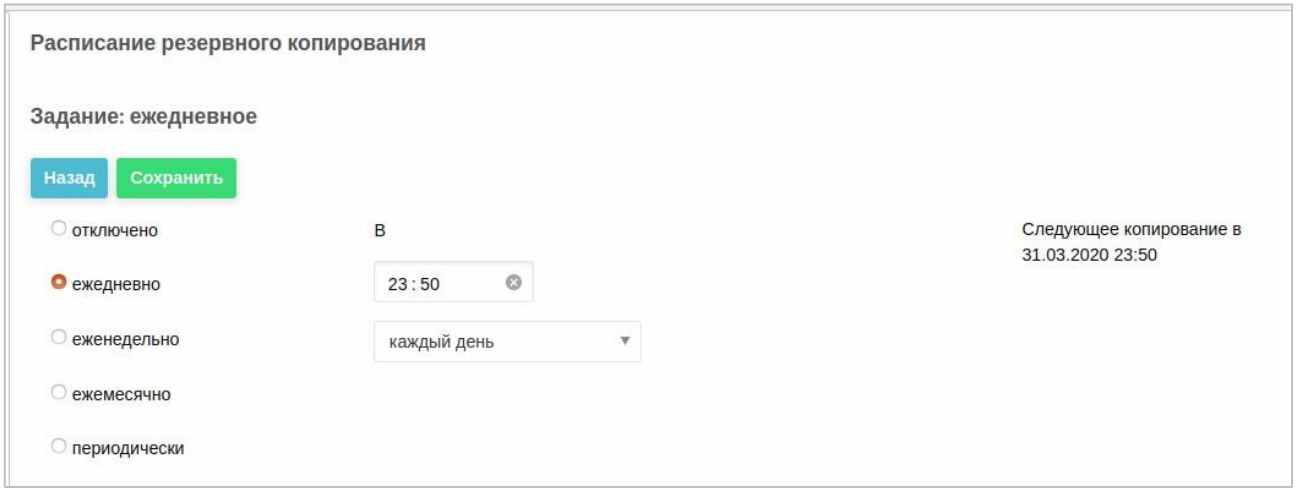


Рисунок 166 – Расписание заданий

Для сохранения расписания нажать кнопку Сохранить.

3.3.5.1.3 Список сохраняемых виртуальных машин

Для просмотра и управления списка сохраняемых ВМ, нажать кнопку  справа от задания.

Откроется окно, представленное на рисунке ниже (Рисунок 167).

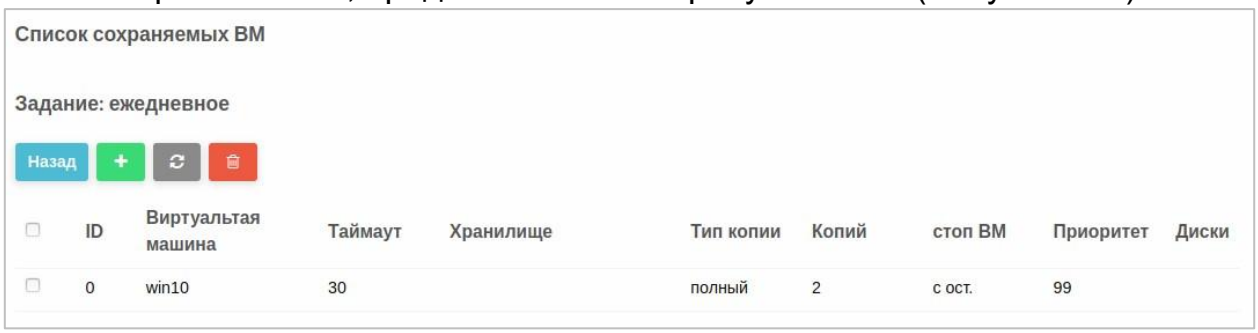


Рисунок 167 – Список сохраняемых ВМ

ВМ можно добавлять, удалять и редактировать.

Для редактирования ВМ нажать на ВМ в списке.

3.3.5.1.4 Задание параметров виртуальной машины для сохранения

Для установки параметров ВМ для сохранения:

1. Зайти в подраздел **Копирование ВМ** → **Задания**.
2. Нажать кнопку  справа от задания

   Откроется список сохраняемых ВМ (Рисунок 167)
3. Выбрать ВМ из списка нажатием.
4. Задать параметры копирования (Рисунок 168):

- **приоритет при копировании** - задает последовательность копирования ВМ в рамках задания. Пока не завершено копирование одной ВМ, копирование следующей не запускается; **тип сохранения**
- («полное» или «пропускается»); **тайм-аут ожидания копирования ВМ**
- **(мин)** — см. п. 3.3.4; **количество копий ВМ** — см. п. 3.3.4; **хранилище**
- **резервных копий** — см. п. 3.3.4;
- Время, отводимое на остановке ВМ (сек);
- **Использовать программу сжатия** — выбор программы, отвечающей
- за сжатие;

  Процент использования CPU при сжатии — задает процент
- использования центрального процессора;

  Степень сжатия (1=min) — степень сжатия при копировании;
- диски ВМ (выбираются из списка подключенных к ВМ дисков);
  порядок управления ВМ при копировании (Рисунок 169).
-
-

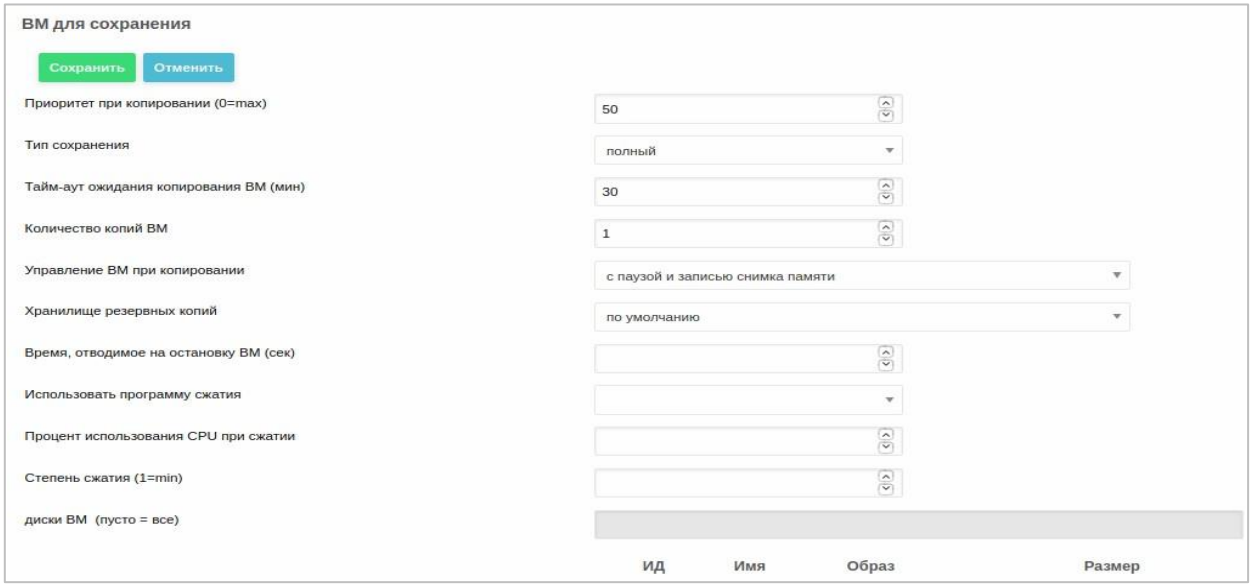


Рисунок 168 – Параметры ВМ для сохранения

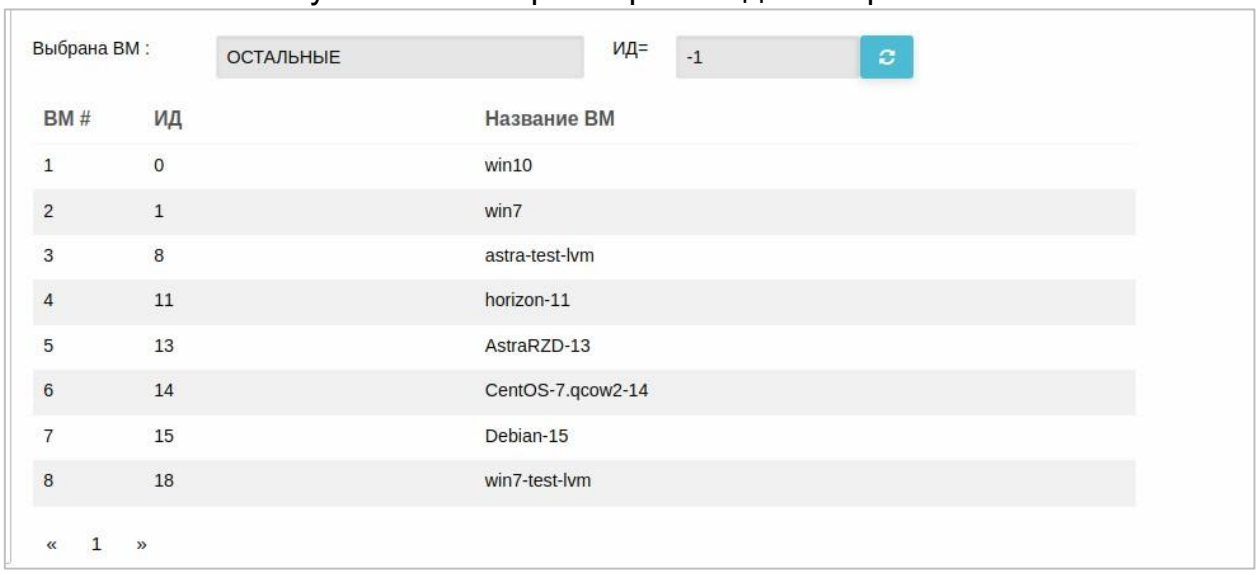


Рисунок 169 — Порядок управления ВМ при копировании

Порядок управления при копировании выбирается из выпадающего меню и может быть одним из следующих типов:

- без остановки (требуется qemu-guest-agent в ВМ — см. ниже). Модуль копирования делает снимок (snapshot) дисков ВМ.

  Целостность дисков обеспечивается при наличии установленного в ВМ специального агента. Виртуальная машина в этом режиме остается доступной все время, хотя и возможна потеря

производительности. Существует ограничение – тип дисков ВМ только qcow», тип хранилищ – LVM, rbd ceph;

- с остановкой. В данном случае модуль дает ВМ команду на завершение работы (если она работает) и после делает копию дисков. ВМ должна быть настроена так, чтобы запустить надлежащий механизм остановки работы при подаче сигнала завершения работы (ACPI) — см. ниже. После копирования модуль запустит ВМ, если она работала. Виртуальная машина в этом режиме будет недоступной все время копирования дисков;
- паузой и записью снимка памяти. В данном случае, если ВМ работает, делает снимок дисков и памяти ВМ, а затем восстанавливает виртуальную машину. Виртуальная машина в этом режиме будет недоступной только во время копирования памяти на диск. Вместо имени ВМ можно выбрать специальную строку «остальные», что позволяет не указывать весь список существующих ВМ, копирование будет проводиться для таких ВМ в порядке их ИД СГУ.

3.3.5.2 Запуск сохранения виртуальной машины вручную

В подразделе **Копирование ВМ → Вручную** можно запустить сохранение одиночной виртуальной машины немедленно при необходимости (Рисунок 170).

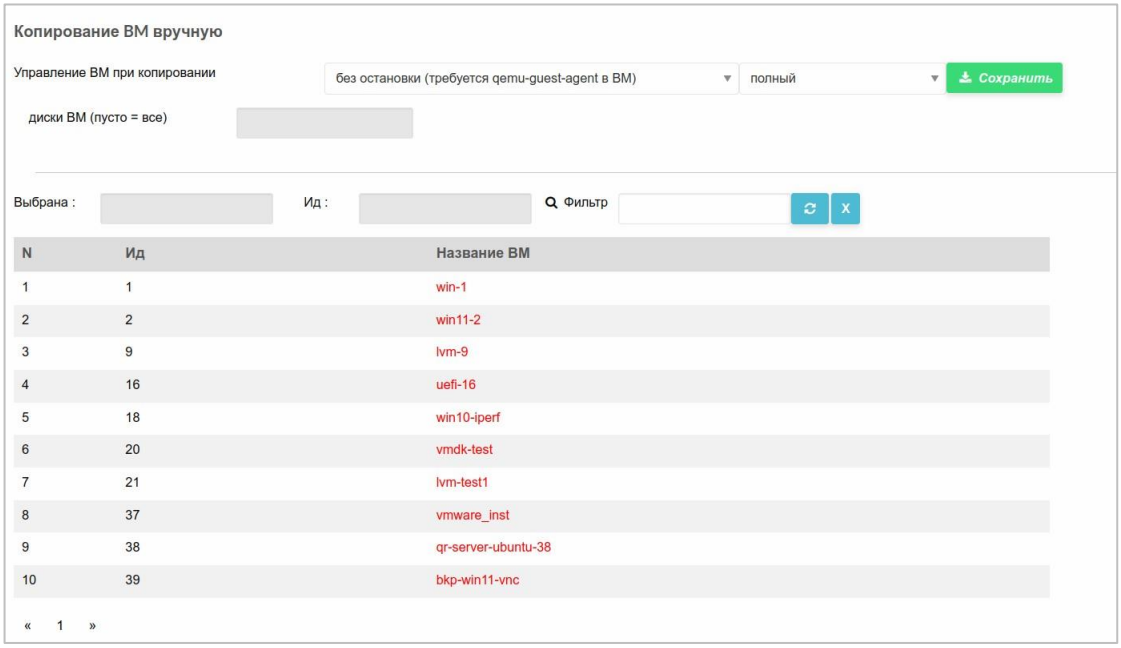


Рисунок 170 – Копирование ВМ вручную

В поле **управление ВМ при копировании** из выпадающего меню следует выбрать порядок работы с ВМ (возможные значения аналогичны приведенным в п. 3.3.5.1.4).

Далее следует выбрать ВМ и нажать кнопку Сохранить.

3.3.5.3 Состояние

На данной вкладке отображается состояние компонентов копирования на всех узлах **Иридиум** и список выполняющихся заданий по сохранению ВМ (Рисунок 171).

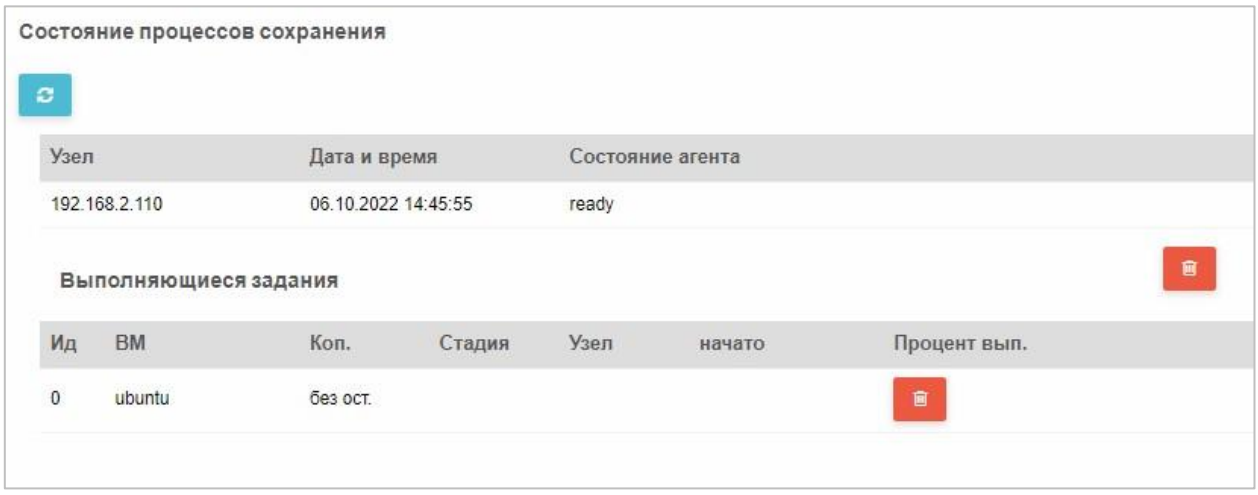


Рисунок 171 – Состояние выполнения заданий **Для удаления очереди копирования ВМ:**

1. Нажать кнопку справа от строки узла в секции **Узел.**
2. Подтвердить операцию в открывшемся диалоговом окне (Рисунок 172).

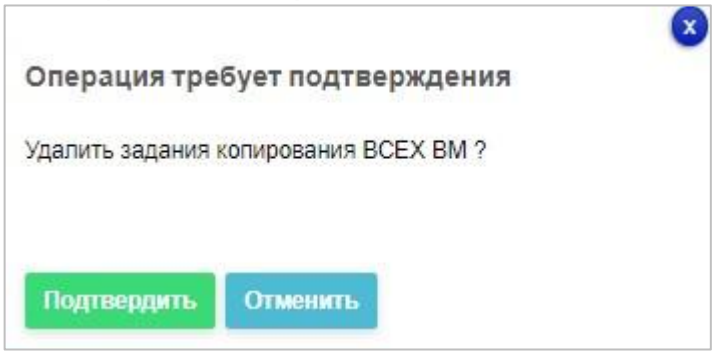


Рисунок 172 – Подтверждение удаления очереди копирования ВМ

Для удаления задания:

1. Нажать кнопку справа от строки ВМ в секции **Выполняющиеся задания.**
2. Подтвердить операцию нажатием кнопки в открывшемся диалоговом окне (Рисунок 173).

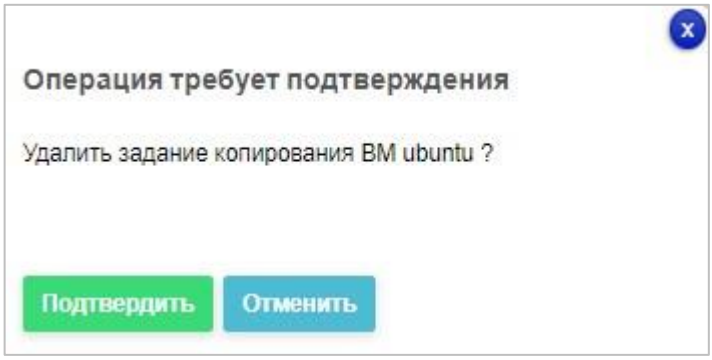


Рисунок 173 – Подтверждение удаления задания

Операция по удалению задания может занимать до 60 секунд. В этом случае на месте значка отобразится крестик. Когда задание будет удалено, крестик и строка задания исчезнут.

***Примечание**. Запущенное задание удалить невозможно. При попытке удаления такого задания появляется сообщение (Рисунок 174).*

Рисунок 174 – Сообщение о невозможности удаления запущенного задания

3.3.5.4 Журнал

На данной вкладке отображаются результаты резервного копирования ВМ (Рисунок 175). Возможна фильтрация информации по диапазону дат и по ИД виртуальной машины.

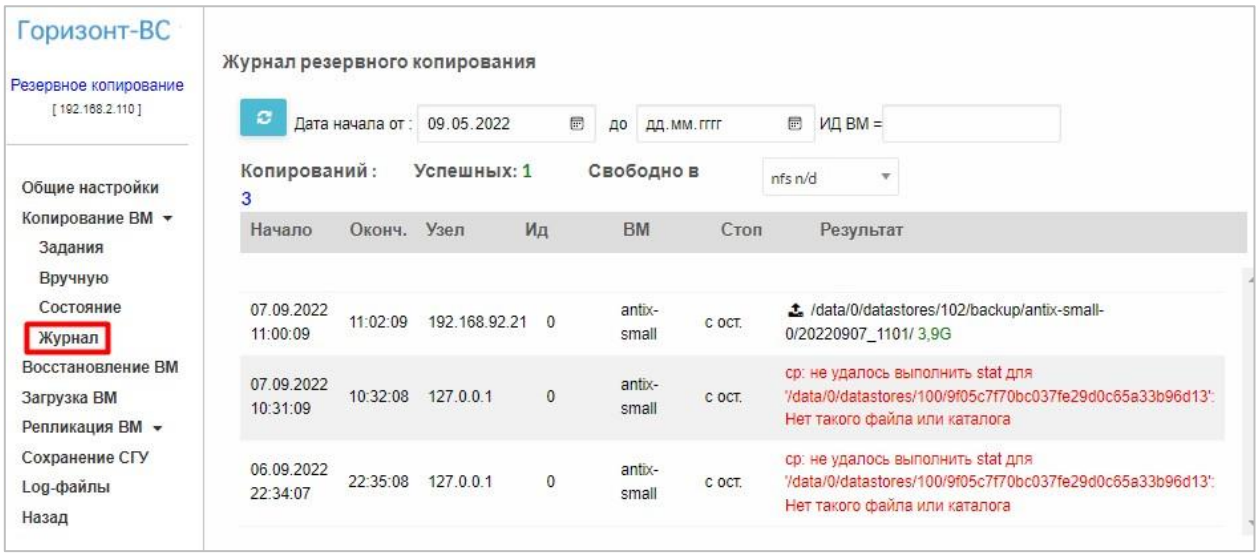


Рисунок 175 – Задания резервного копирования

Для выбора интервала, за который необходимо просмотреть задания, выбрать даты начала и конца временного интервала из календарей в верхней части окна и нажать кнопку  (Рисунок 176).

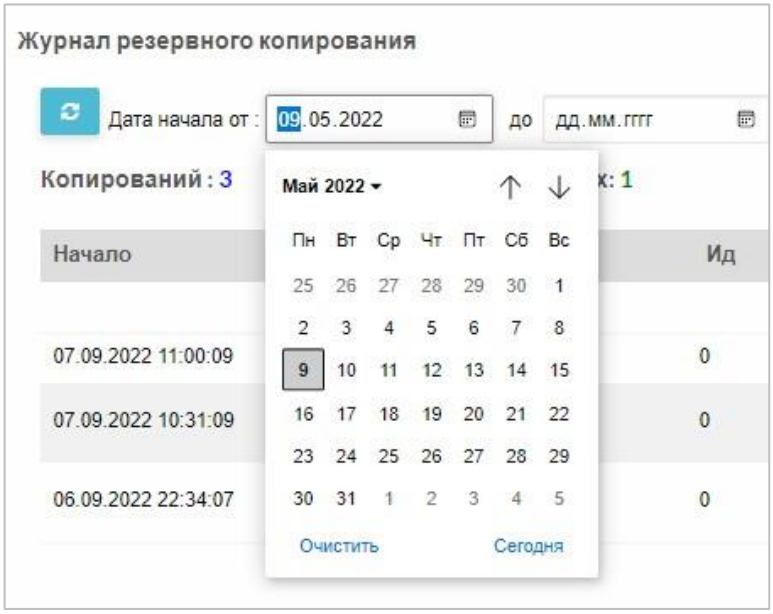


Рисунок 176 – Установка интервала, за который выводятся задания

Для поиска заданий по определенной ВМ, указать ее идентификатор в поле **ИД ВМ=** и нажать кнопку .

Для каждого задания задаются следующие характеристики:

- имя;
- расписание запуска;
- список виртуальных машин, которые сохраняются эти заданием.

3.3.6 Состав папки резервной копии виртуальной машины

Папка с резервными копиями содержит следующие файлы:

- файл(ы) дисков ВМ — **disks.#, *.img**
- xml файл описания ВМ, полученный из СГУ «Иридиум», - **one.xml**.

Если виртуальная машина была запущена после копирования, то дополнительно сохраняется xml файл описания ВМ, полученный средствами libvirt - **libvirt. xml**.

При сохранении ВМ в режиме «с паузой и записью снимка памяти» папка дополнительно содержит файл снимка памяти **memory.dump** и файл(ы) снимка(снимков) дисков **disks.#.bus, *-bus.img**.

3.3.7 Восстановление виртуальной машины из резервной копии

В разделе **Восстановление ВМ** отображается список ВМ, для которых были созданы резервные копии (Рисунок 177). Возможна фильтрация информации по диапазону дат и по ИД виртуальной машины.

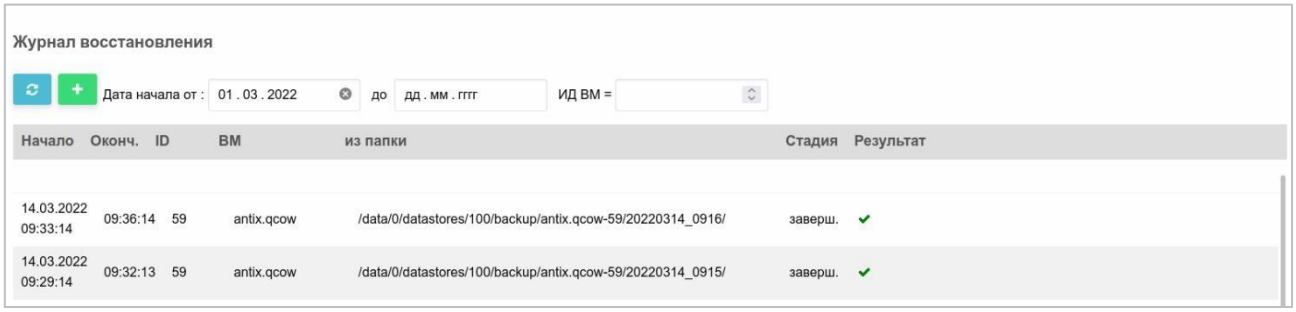


Рисунок 177 - Восстановление ВМ

Для восстановления ВМ из резервной копии следует выбрать ВМ и нажать кнопку **Показать список копий**.

Для выбранной ВМ появится список копий (Рисунок 178), из которого необходимо выбрать нужную и нажать кнопку  .

Рисунок 178 – Список копий ВМ

Для удаления резервной копии следует нажать кнопку  .

3.3.8 Загрузка виртуальной машины

Данный режим предназначен для загрузки (импорта) отсутствующей в СГУ виртуальной машины из копии. Копию ВМ необходимо предварительно

записать в файловую систему гипервизора, из физической машины или ВМ другого гипервизора (VMware, Hyper-V).

В рабочей области раздела представлен журнал ранее выполненных загрузок (Рисунок 179).

Рисунок 179 – Журнал загрузки

Для загрузки ВМ:

1. Нажать на кнопку  .
2. Вставить путь к каталогу на файловой системе гипервизора, из которого требуется загрузить ВМ, в поле справа от надписи **Укажите папку с копией ВМ** (Рисунок 180).

Рисунок 180 – Путь к каталогу на файловой системе гипервизора, из которого требуется загрузить ВМ

Этот путь можно скопировать из:

- раздела Копирование ВМ → Журнал;
- физической машины;
- другого гипервизора (vmware, Hyper-V…) — требуется специальный агент p2v:

3. Нажать кнопку **Далее** (Рисунок 180)

   Откроется окно редактирования шаблона выгружаемой ВМ (Рисунок 181).

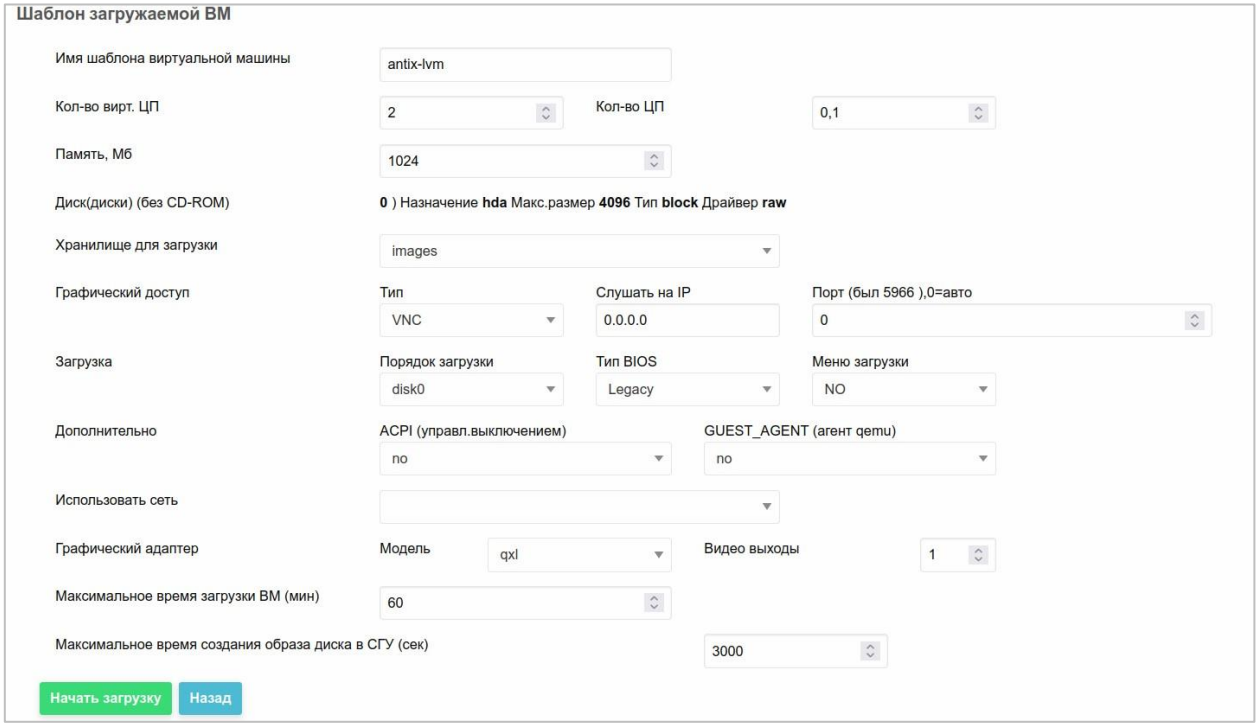


Рисунок 181 – Шаблон загружаемой ВМ

4. Отредактировать шаблон ВМ, выставляя необходимые параметры. При выборе номера порта графического доступа равным нулю, в СГУ он будет устанавливаться автоматически.
5. Нажать кнопку **Начать загрузку** (Рисунок 181).

Начнется процесс загрузки, в результате которого отобразится ИД созданного в СГУ шаблона ВМ или ошибка.

3.3.9 Репликация виртуальной машины

Репликация – это перемещение состояния дисков ВМ (ведущей) с одного сервера на другой сервер (управляемый своим СГУ) в другую ВМ (ведомую).

Для возможности репликации ВМ необходимо выполнение требований:

- наличие канала связи между ВМ (возможно, небыстрого);
- ключи SSH на обоих площадках должны быть одинаковы;
- шаблоны дисков ведущей и ведомой ВМ должны быть идентичны.

- в СГУ на хосте для репликации должен быть создан пользователь с таким же именем и паролем, под которым выполняется вход в СРК.

Возможна репликация ВМ в пределах одного Иридиум (сервера), т. е. из основной ВМ в запасную.

Репликация проводится следующим образом: 1) создается резервная копия ВМ на ведущем Иридиуме-ВС (не обязательно все диски);

2) копия в соответствии с предварительно заданным планом перемещается на ведомый Иридиум в промежуточное хранилище;

3) производится актуализация дисков ведомой (реплицируемой) ВМ; Предусмотрены следующие режимы перемещения:

- перенос вручную на внешнем носителе (для первоначального выравнивания дисков ВМ);
- полное копирование всех файлов резервной копии (используется утилита **rsync**);
- копирование только измененных частей файлов (используется утилита rsync).

План репликации описывает соответствие ведущей и ведомой ВМ. Для каждой реплицируемой ВМ должен быть подготовлен план репликации.

План репликации отдельно составляется для:

- копий ВМ;
- для снимков ВМ.

Возможна репликация в несколько мест. При этом для каждой ведомой копии должна быть заготовлена строка в плане.

3.3.9.1 План для копий

План репликации для копий ВМ представлен в разделе **Репликация ВМ → План для копий** (Рисунок 182).

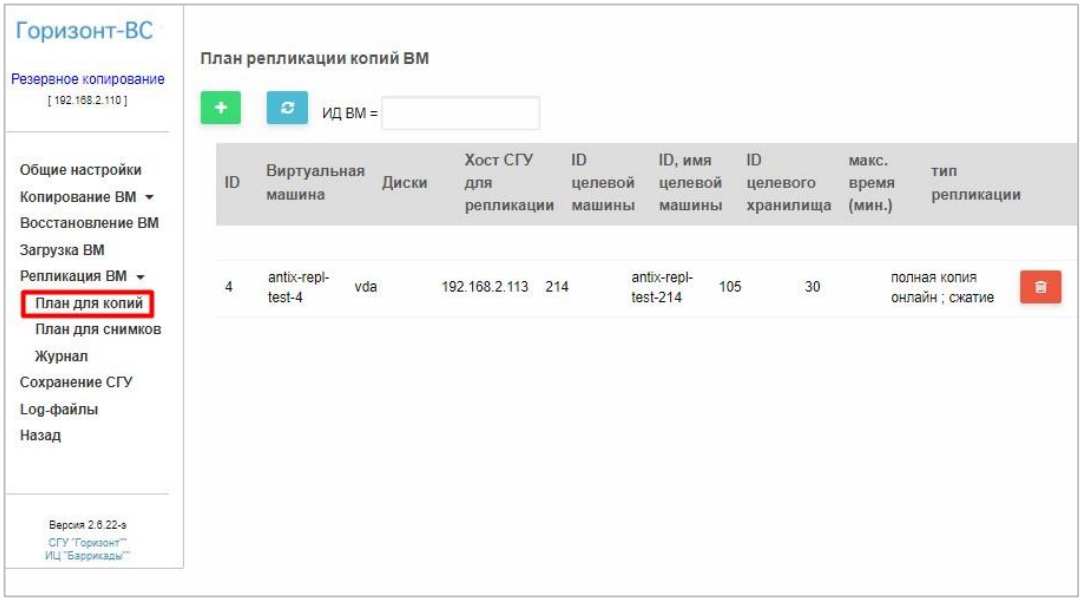


Рисунок 182 – План репликации

Для добавления строки плана:

1. Нажать кнопку + на панели управления.

Откроется окно **План репликации копий ВМ ID=** (Рисунок 183)

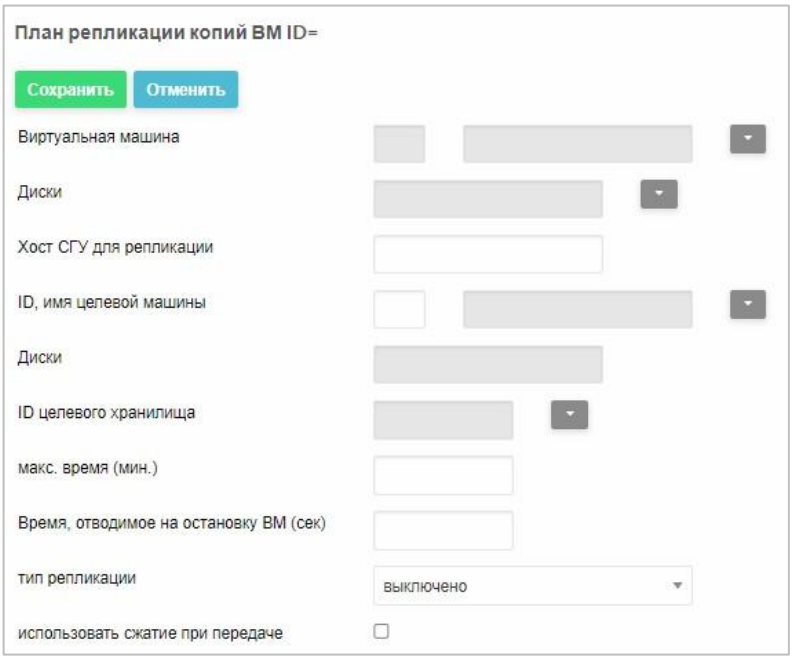


Рисунок 183 – План репликации копий ВМ

2. В поле Виртуальная машина нажать .

Откроется список доступных ВМ (Рисунок 184).

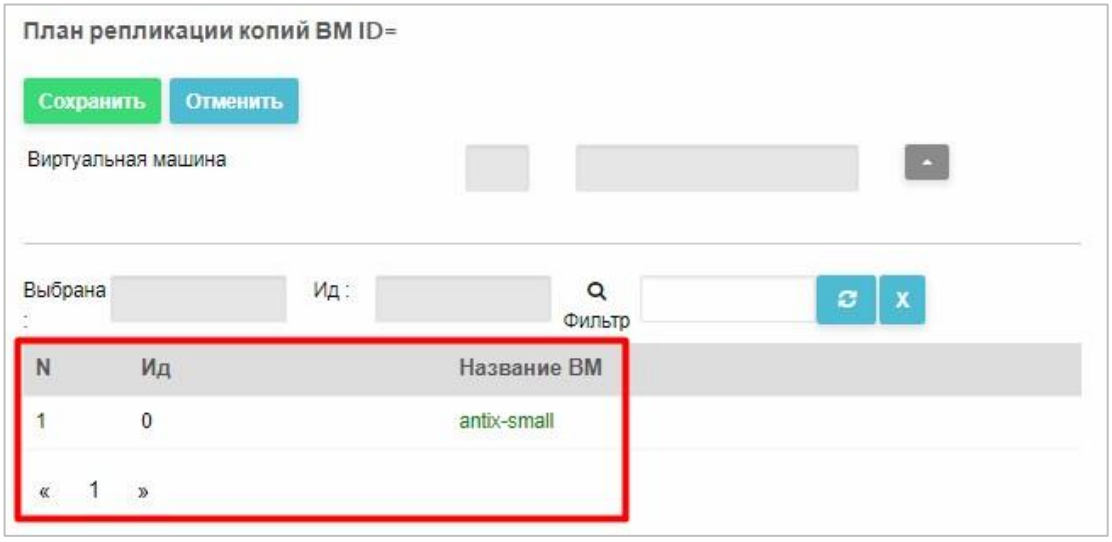


Рисунок 184 – Выбор ВМ для репликации копий

3. Выбрать ВМ нажатием.
   Для поиска ВМ, в поле **Фильтр** ввести ее номер или название полностью или частично и нажать кнопку .
   Выбранная ВМ отобразится в поле **Выбрана** (Рисунок 185).

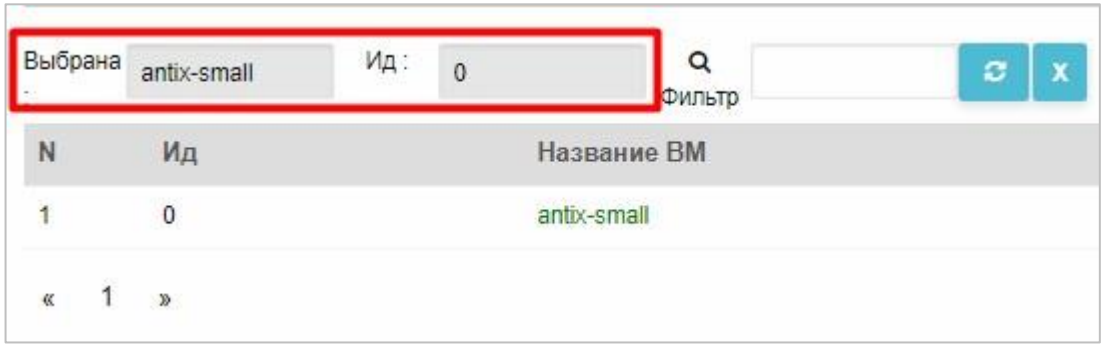


Рисунок 185 – Выбранная ВМ для репликации копий

4. В поле **Диски** нажать и выбрать диск.
5. В поле **Хост СГУ для репликации** указать IP-адрес хоста, на который осуществляется репликация.
6. В поле **ID целевой машины** нажать и выбрать ВМ, на которую выполняется репликация.
7. В полях **Диски** и **ID целевого хранилища** выбрать диски и хранилища, куда будет осуществляется репликация.

8. В поле **макс. Время (мин.)** задать таймаут на выполнение репликации. По истечении установленного значения операция отменяется.
9. В поле **Время, отводимое на остановку ВМ (сек)** указать таймаут, в течение которого нужно остановить ВМ.
10. Из выпадающего списка **Тип репликации** выбрать значение (Рисунок 186):

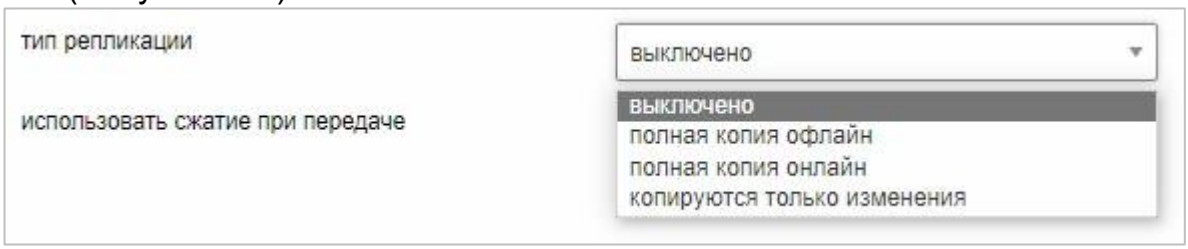


Рисунок 186 – Выбор типа репликации

- **выключено** – репликация не производится. Для запуска репликации необходимо открыть форму с заданными параметрами и выбрать другой тип репликации;
- **полная копия офлайн** – будет периодически сканироваться целевая копия и сравниваться наличие и размеры файлов до их полного совпадения (или завершения максимального отведенного времени);
- **полная копия онлайн** – перенесутся все копии;
- **копируются только изменения** – будут скопированы только изменения целевой ВМ по сравнению с копируемой.

11. Для сжатия данных при передачи установить флаг использовать сжатие **при передаче**.
12. Нажать кнопку Сохранить в верхнем левом углу и подтвердить действие в открывшемся окне.

Пример плана репликации для копий одного диска ВМ «antix-small» (ид=0) в ВМ «wm-backup-serv» (ид 2) на хост 111.168.2.4 с использование

промежуточного файлового хранилища (ид=100) представлен на рисунке выше (Рисунок 187).

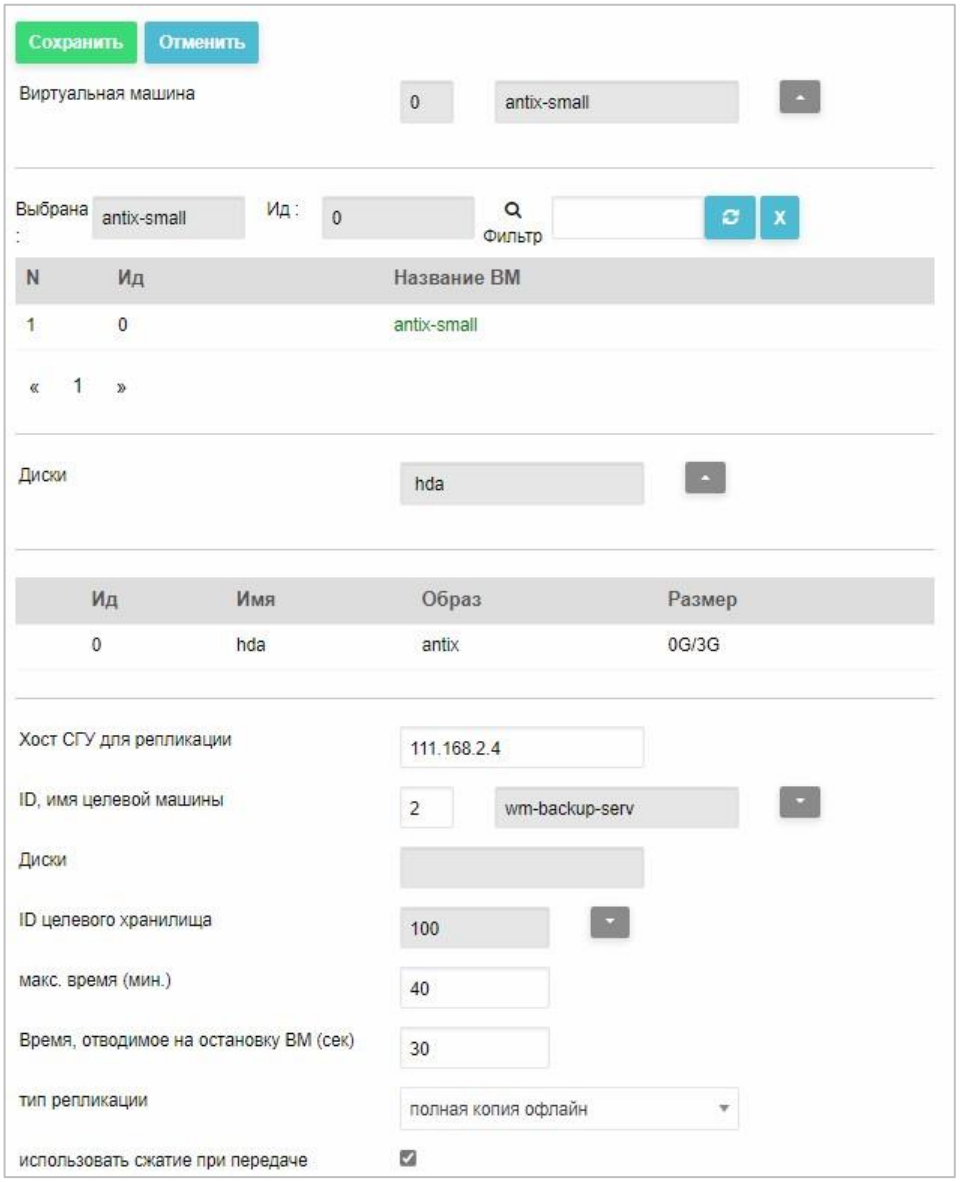


Рисунок 187 – Пример плана репликации для копий

Важно! *Основная и ведомая ВМ должны иметь диски одинакового типа (raw, qcow2), совпадающего размера и с одинаковыми именами.*

3.3.9.2 План для снимков

План репликации для снимков ВМ представлен в разделе **Репликация ВМ → План для снимков** (Рисунок 188).

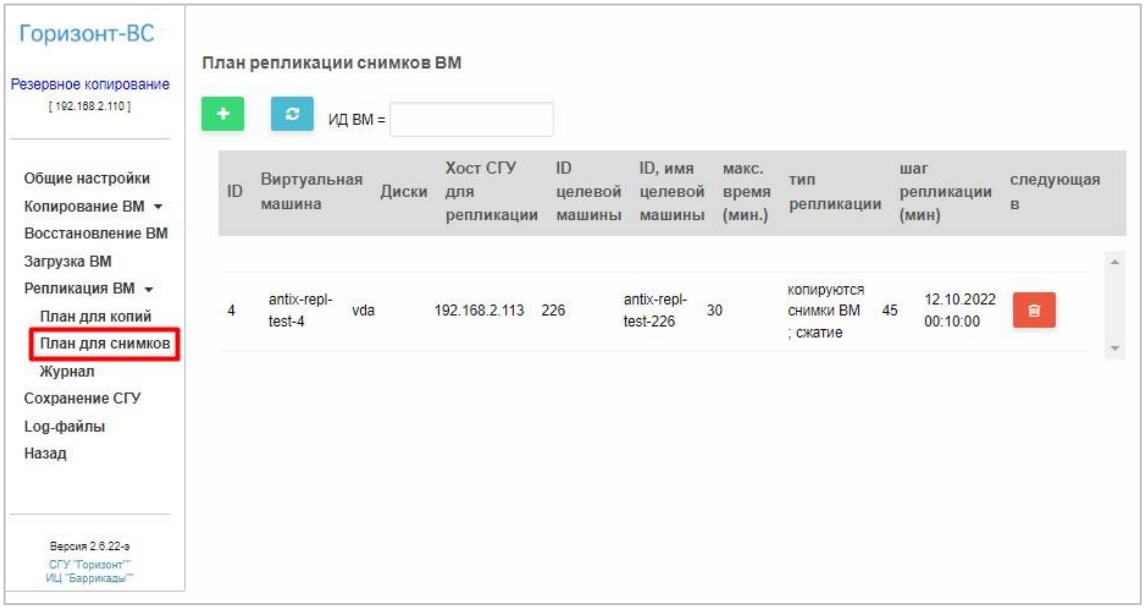


Рисунок 188 – План репликации для снимков ВМ

Для создания плана репликации снимков ВМ следует нажать кнопку + на панели управления и заполнить поля формы **План репликации снимков ВМ** (Рисунок 160).

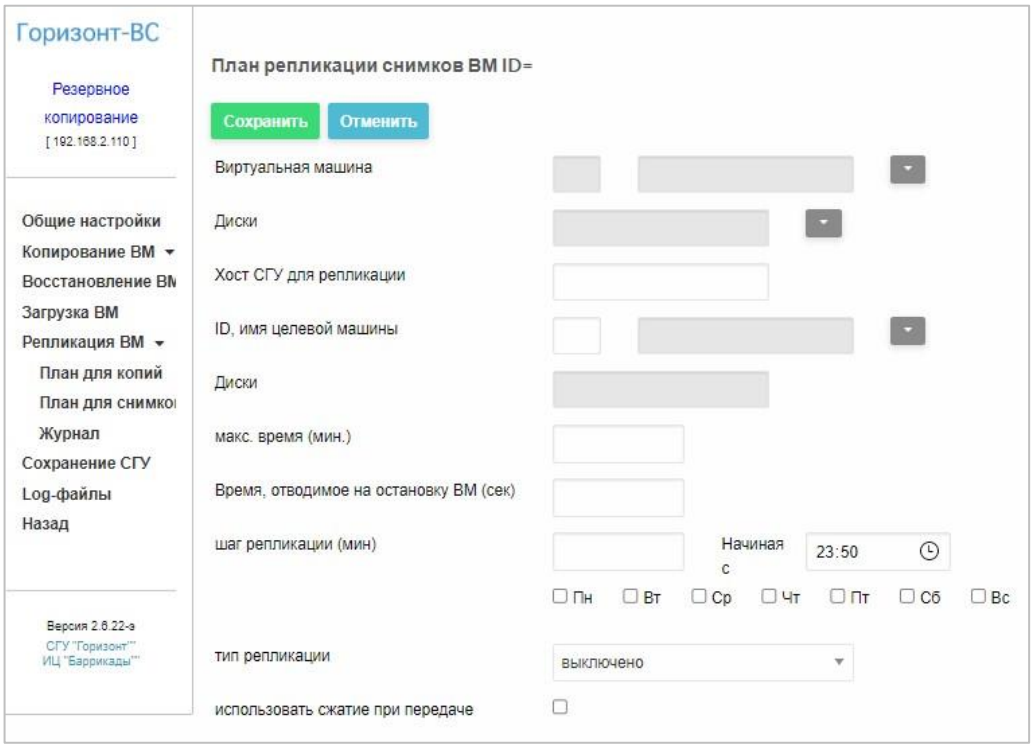


Рисунок 189 – Создание плана репликации снимков ВМ

План репликации для снимков ВМ создается по аналогии с планом репликации для копий (см. п. 3.3.9.1).

***Примечание**. Шаг репликации – промежуток времени между снимками.*

3.3.9.3 Журнал репликации

После завершении процесса резервного копирования любой ВМ, просматривается план репликации. При наличии в плане соответствующей строки производится заполнения журнала и запускается процесс репликации.

Для просмотра журнала репликации (Рисунок 190) необходимо зайти в раздел **Репликация ВМ → Журнал**.

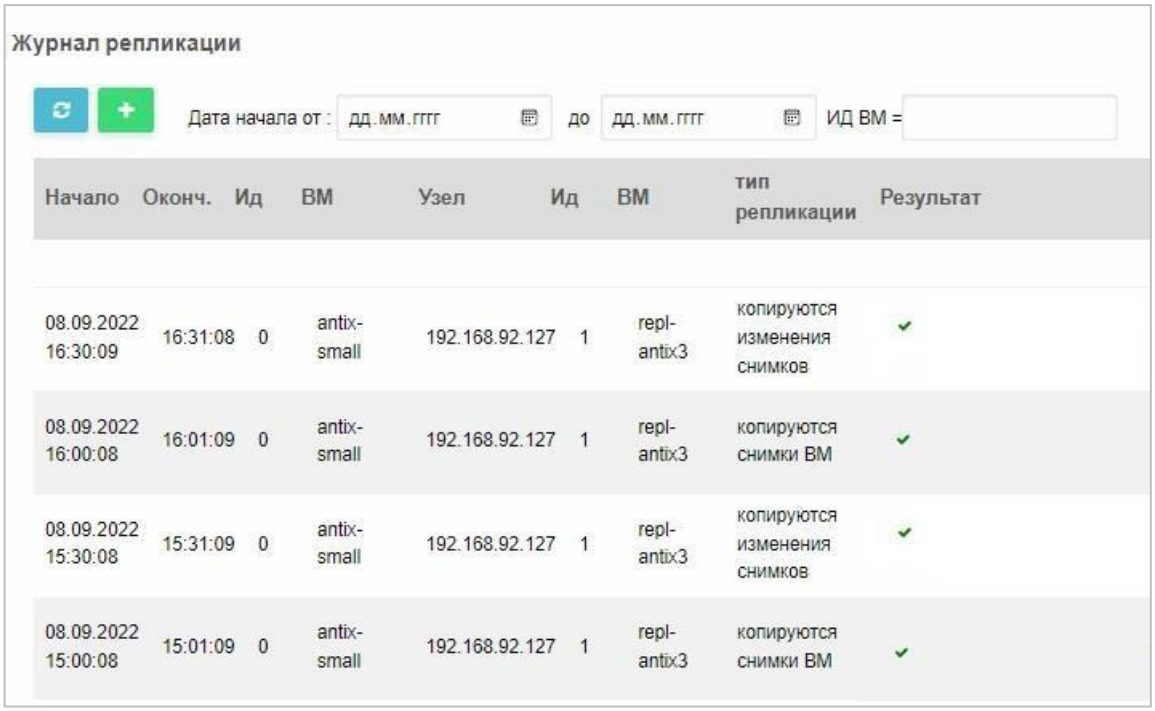


Рисунок 190 – Журнал репликации

Строку журнала репликации можно посмотреть подробней, нажав на соответствующую строку (Рисунок 191).

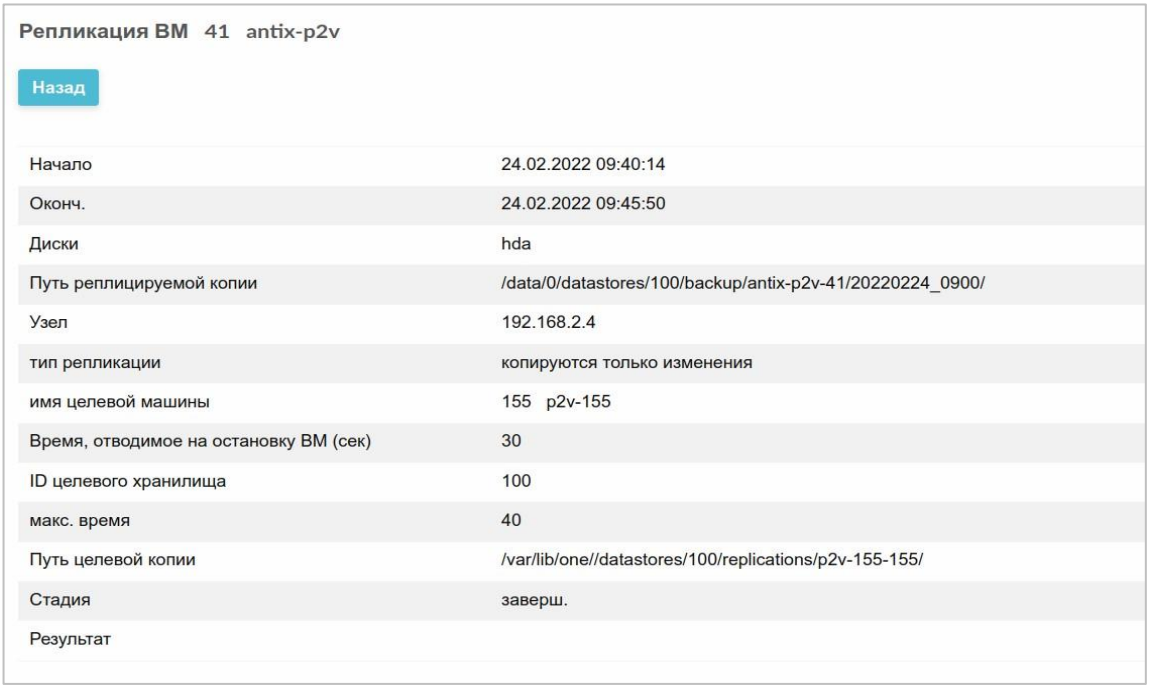


Рисунок 191 – Просмотр журнала репликации

3.3.10 Сохранение Системы резервного копирования

Данная вкладка предназначена для сохранения настроек и базы данных СГУ.

В поле **Хранилище для копии** следует выбрать хранилище для сохранения СГУ и нажать кнопку **Сохранить** (Рисунок 192). Созданные копии появятся в списке.

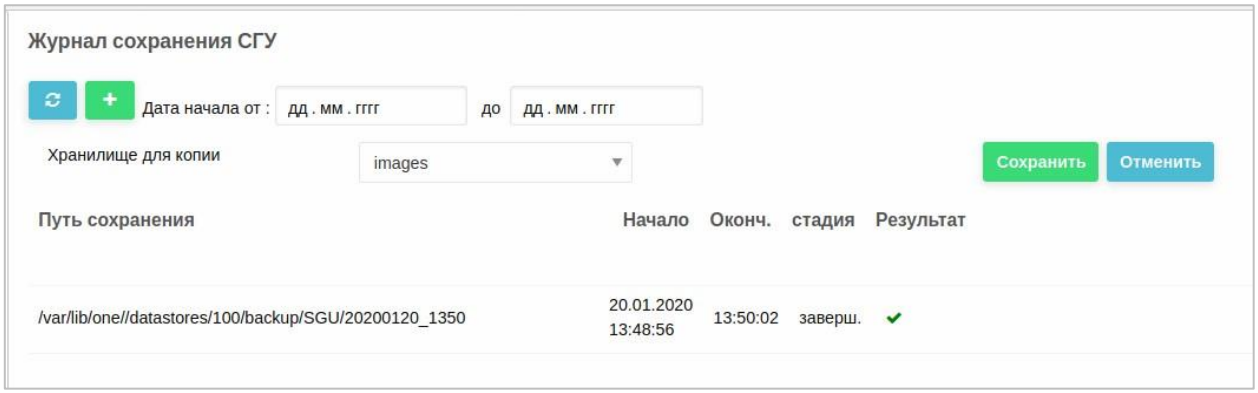


Рисунок 192 - Сохранение СГУ

3.3.11 Log-файлы резервного копирования

На данной вкладке отображаются log-файлы работы СРК обработки заданий копирования за выбранную дату (Рисунок 193).

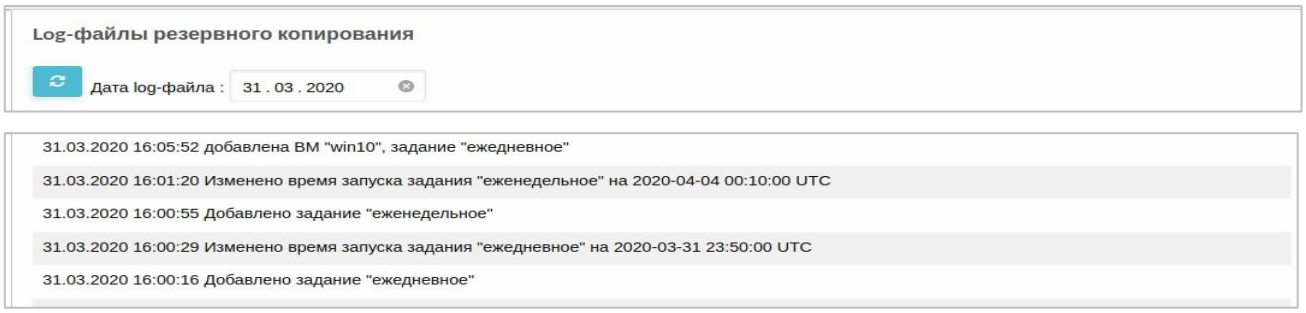


Рисунок 193 – Журнал СРК

3.3.12 Установка и настройка виртуальной машины

Настройки ВМ предназначены для:

- корректного выключения ВМ (ACPI);
- получения снимков дисков qcow2 без выключения ВМ (агент qemu-guest-agent).

В СГУ для каждой ВМ обновить конфигурацию (см. п. 3.2.22.8), установив значение **Да** в полях **ACPI** и **Гостевой агент QEMU** (Рисунок 194).

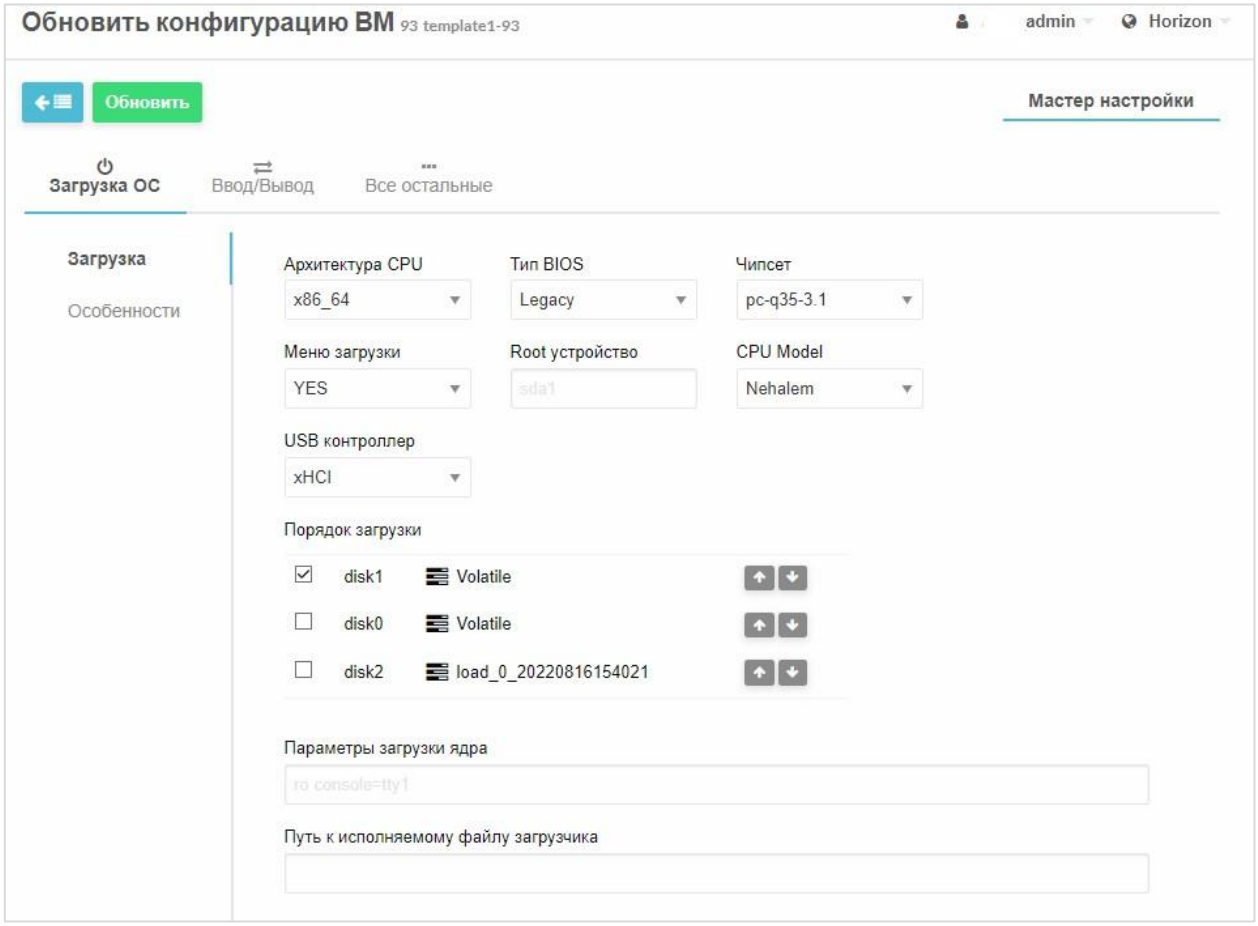


Рисунок 194 – Конфигурация ВМ

3.3.13 Репликация в обратном направлении

Для того чтобы данная операция была выполнена значительно проще, можно развернуть дополнительный экземпляр СРК, предварительно остановив основной, по следующему алгоритму:

13. Для начала следует убедиться, что СРК в данный момент не выполняет никаких операций. Для этого необходимо проверить следующие разделы web-интерфейса СРК:

    д. Копирование ВМ → Журнал;

    е. Восстановление ВМ;

    ж. Загрузка ВМ;

    з. Репликация ВМ → Журнал;

    и. Сохранение СГУ.

14. Остановить контейнер СРК следующей командой:

```
horizon ~ # docker stop bus
```

где bus - имя контейнера СРК.

15. Создать рабочий каталог для дополнительного экземпляра СРК, затем скопируйте в него файлы конфигурации, а в случае использования HTTPS - ключевые файлы:

```
horizon ~ # mkdir /home/restorelogs horizon ~ # cd
/home/restorelogs horizon /home/restorelogs # cp
../backuplogs/backup.conf . horizon /home/restorelogs # cp
../backuplogs/backup.crt . horizon /home/restorelogs # cp
../backuplogs/backup.key .
```

16. Далее следует заменить в конфигурационном файле дополнительного экземпляра IP-адрес СГУ основной площадки на адрес резервной площадки. Данный адрес указывается в директиве **gorizont-host.** Для этого следует:

к. Открыть конфигурационный файл в текстовом редакторе

```
horizon ~ # mcedit /home/restorelogs/backup.conf
```

л. Найти в файле строку, начинающуюся с **gorizont-host=,** в которой должен быть указан IP-адрес СГУ основной площадки. Удалить этот адрес и ввести вместо него адрес резервной площадки.

м. Сохранить конфигурационный файл и завершить работу редактора.

17. Запустить контейнер дополнительного экземпляра СРК:

```
horizon ~ # docker run -itd --net=host -v
/home/restorelogs:/var/log/one/backup --name bus2 --
restart=unless-stopped bus:2.6.18 /bin/bash /opt/backup/start
```

18. После этого следует выполнить конфигурацию дополнительного экземпляра:

н. Для этого следует выполнить вход под технологической учетной записью СРК (backuper), созданной в СГУ резервной площадки, пи отсутствии учетной записи – следует ее создать.

о. Далее следует заполнить параметры раздела **Общие настройки** дополнительного экземпляра аналогично основному. В поле **Хранилище резервных копий по умолчанию** должен отобразиться перечень хранилищ резервной площадки.

19. После этого необходимо выполнить следующие операции:

п. Создать правило репликации в разделе **Репликация → План копий**, указав экземпляр ВМ на резервной площадке в качестве исходного, экземпляр на основной площадке – в качестве целевого. В **поле Хост СГУ для репликации** указать адрес СГУ основной площадки.

р. Запустить операцию создания копии в разделе **Копирование ВМ → Вручную**. По завершении создания копии, операция репликации должна запуститься автоматически (см. раздел **Репликация ВМ → Журнал).**

***Примечание**. Если в журнале репликации отсутствует запись о запущенной операции, следует запустить ее вручную с помощью кнопки зеленого цвета с изображением знака «плюс» в вышеупомянутом разделе. После нажатия кнопки **Показать список копий** выберите вновь созданную резервную копию.*

20. Следует дождаться окончания операции репликации.
21. Убедиться, что дополнительный экземпляр СРК не выполняет никаких операций.
22. После этого следует остановить контейнер дополнительного экземпляра, затем запустить контейнер основного экземпляра:

```
horizon ~ # docker stop bus2 horizon ~ # docker start bus
```

3.3.14 Настройка ACPI

В ОС семейства Linux следует установить агент ACPI и настроить файл **/etc/acpi/events/powerbtn** указав там реакцию на выключение:

event=button/power action=/sbin/shutdown

now

В ОС семейства Windows также необходимо настроить реакцию на выключение.

Например, в Windows 10 в строке поиска набрать слово «*питание*», в результатах выбрать пункт **Электропитание** и в открывшемся окне **Системные параметры** найти пункт **Действие при нажатии кнопки питания**. Открыть окно, выбрать опцию **Завершение работы** и нажать кнопку **Сохранить изменения**.

3.3.15 Настройка qemu-guest-agent

Для ВМ с ОС семейства Linux установить qemu-guest-agent и убедиться, что он запущен – значение *active* (Рисунок 195).

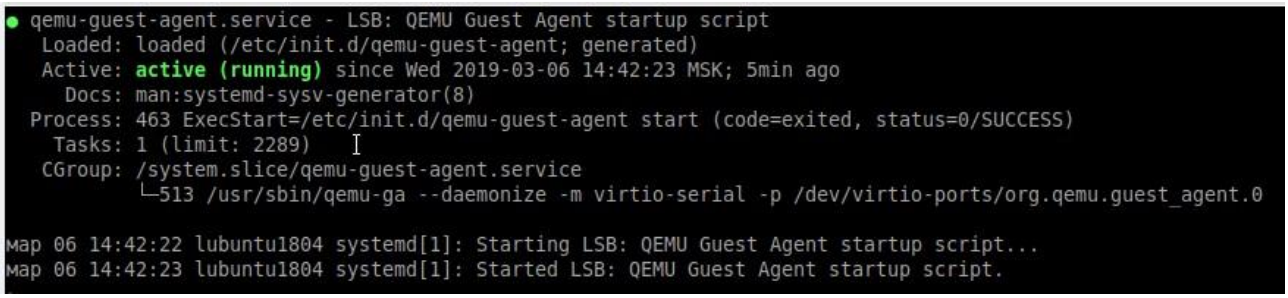


Рисунок 195 – qemu-guest-agent запущен

Для ВМ с ОС семейства Windows закачать в СГУ iso-образ virtio-win https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-virtio/virtiohttps://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-

virtio/virtio-win.isowin.iso и добавить его в хранилище каждой ВМ как cdrom (см. п. 3.2.22.3).

Внутри ВМ с ОС Windows произвести установку qemu-ga. После установки убедиться, что служба Qemu Guest Agent запущена.

Установить драйвер virtio-serial, находящийся на подключенном диске virtio-win и убедиться, что он был установлен (Рисунок 196).

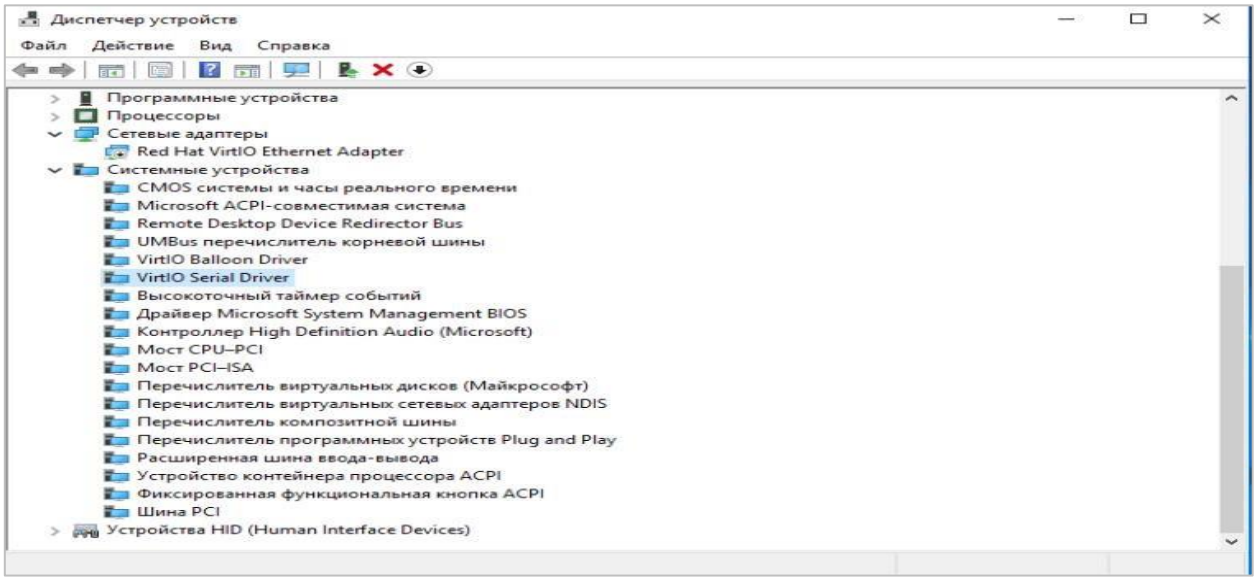


Рисунок 196– Драйвер virtio-serial установлен

3.4 Обновление версии Системы группового управления

Для автоматического обновления версии СГУ:

23. Авторизоваться в системе от имени администратора.
24. В интерфейсе СГУ перейти в меню **Настройки**.
25. Открыть вкладку **Обновить**.
26. Нажать кнопку **Загрузить** (Рисунок 197).

Откроется меню выбора файла обновления.

Рисунок 197 – Интерфейс раздела обновления СГУ

27. Выбрать файл обновления.

Запустится процедура автоматического обновления (Рисунок 198).

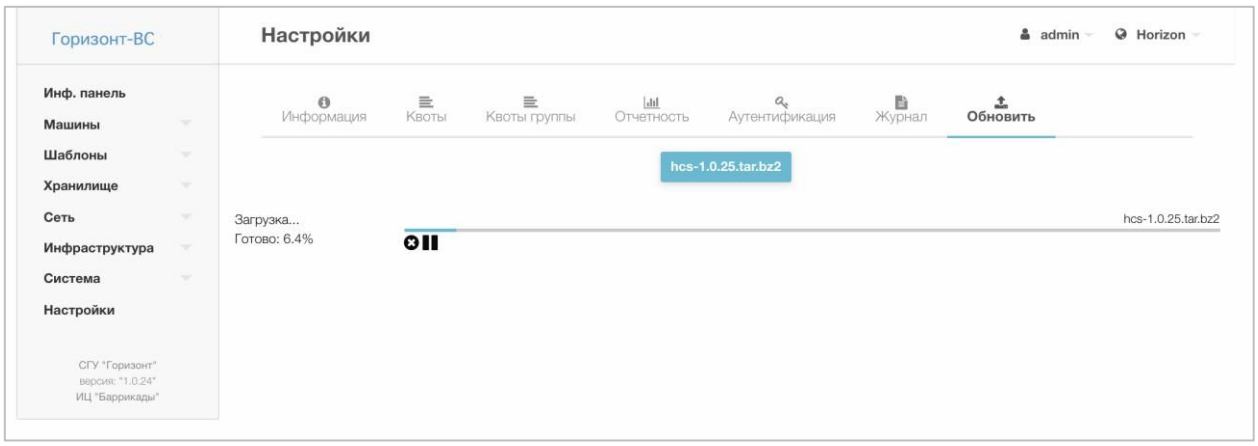


Рисунок 198 – Загрузка новой версии СГУ

После завершения загрузки новой версии система будет недоступна около 10 минут.

Журнал системы обновления СГУ доступен по пути ***/var/tmp/hcs_update.log*** (Рисунок 199).

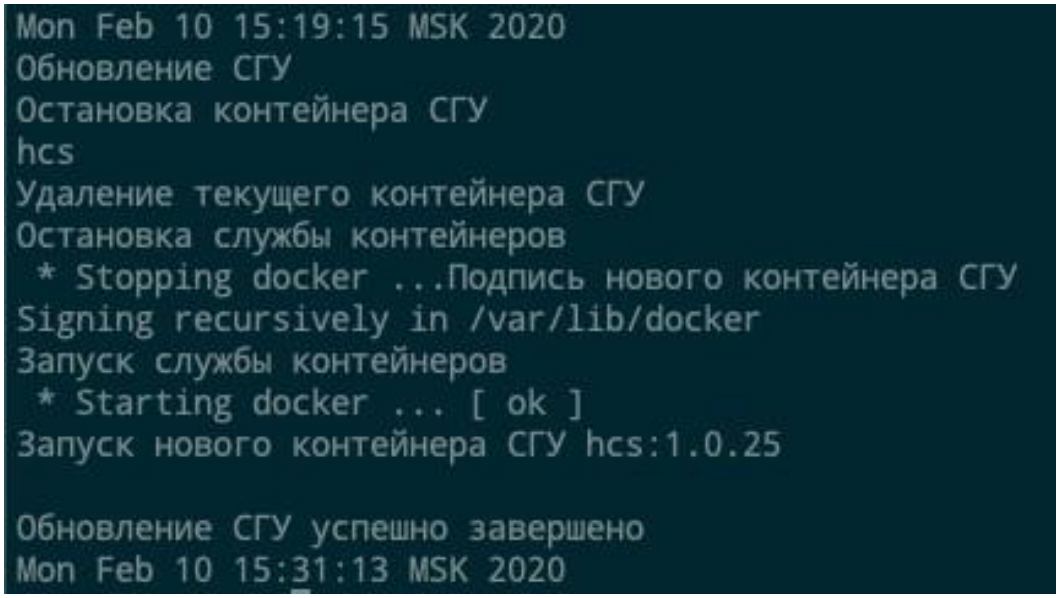


Рисунок 199 – Журнал системы автоматического обновления СГУ

3.5 Настройка и работа СХД «Шторм»

3.5.1 Информационная панель

Для перехода на страницу мониторинга необходимо в браузере перейти по ссылке на любой из первых трех узлов, например: https://10.10.10.100. Далее в окне авторизации (Рисунок 200) указывается имя пользователя «admin», и пароль по умолчанию «password». Открывается информационная панель (

Рисунок **201**), которая также является домашней страницей

Системы.

Рисунок 200 – Авторизация в Системе

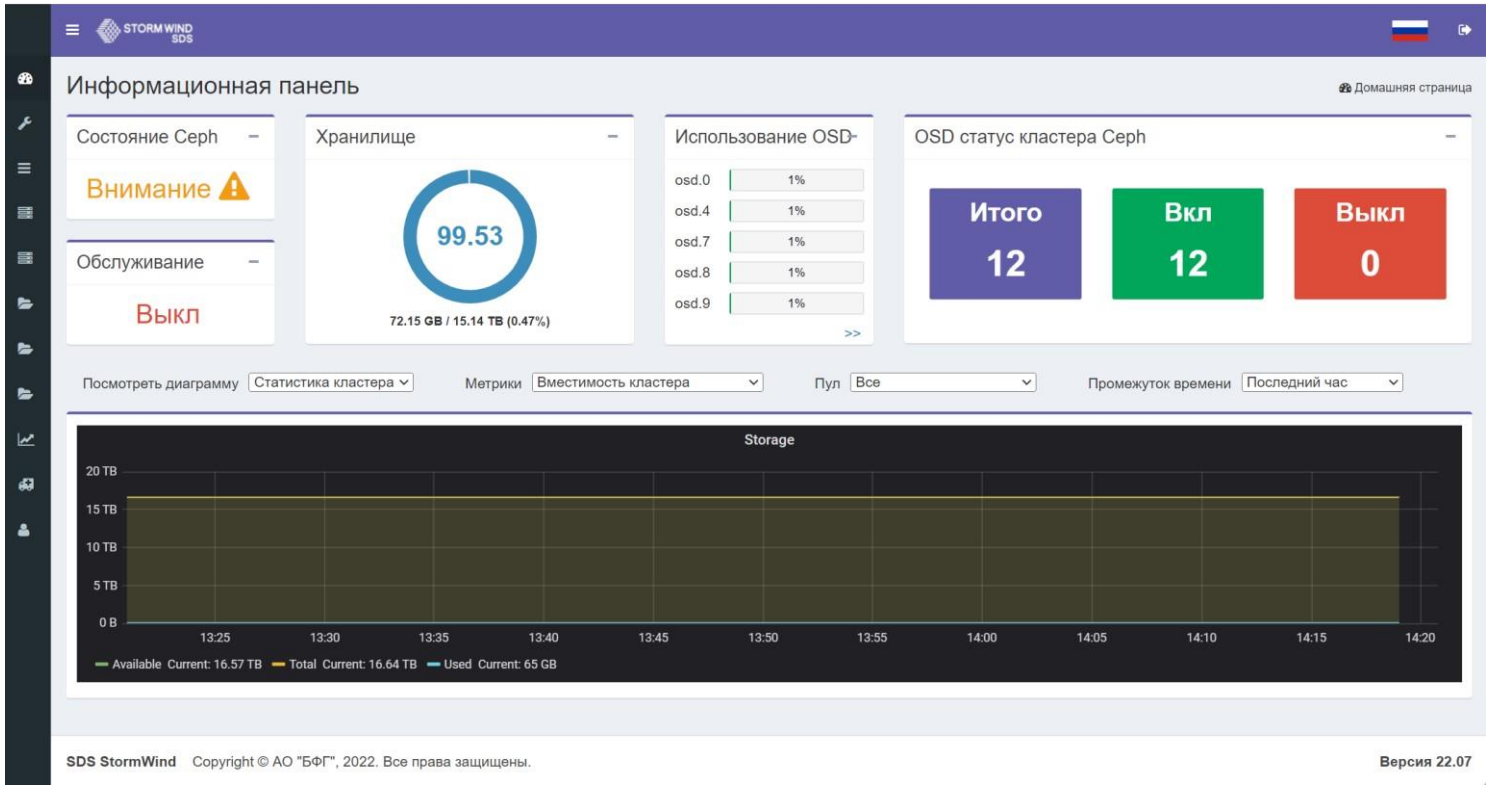
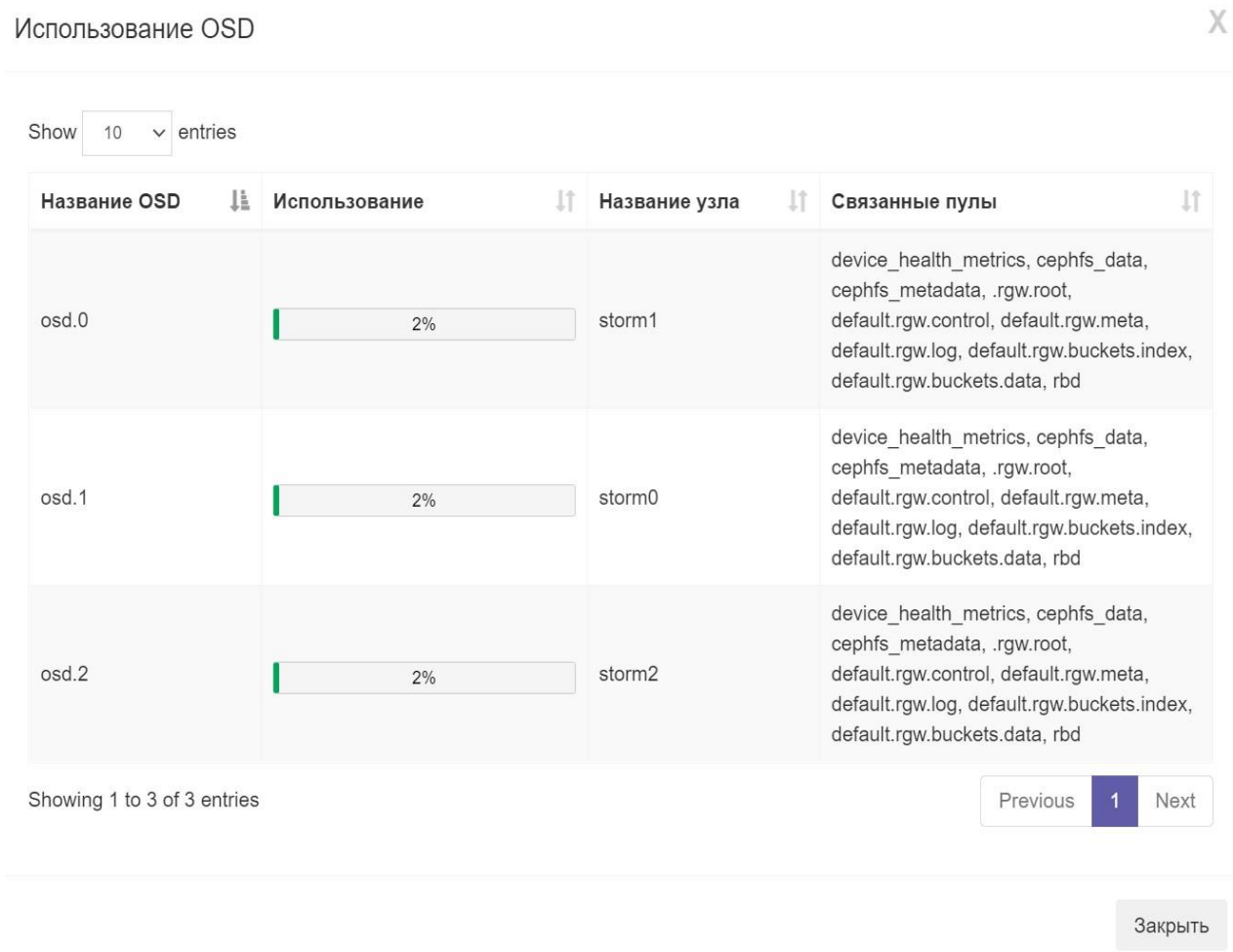


Рисунок 201 – Страница информационной панели– Страница информационной панели

На информационной панели отображается текущее состояние системы «StormWind». Это позволяет администратору вести мониторинг следующих данных:

- **Объем кластера** (окно «Хранилище»). На диаграмме отображается общий объем дискового пространства и объем свободного дискового пространства, доступного в кластере (в числовых значениях и процентом соотношении).
- **Состояние кластера** (окно «Состояние Ceph»). Модель состояний системы состоит из следующих значений:
- Значок «OK» отображается, когда кластер исправен.
- Внимание – в кластере есть предупреждения, которые можно просмотреть, щелкнув значок.
- Ошибка – в кластере есть ошибки, которые можно просмотреть, нажав на значок.
- **Техническое обслуживание** (окно «Обслуживание»). Раздел обслуживания показывает, находится ли система на обслуживании или нет. Система находится на обслуживании, если какие-либо настройки обслуживания отключены.
- **Состояние экранного меню** (окно «OSD статус кластера Ceph»). На приборной панели отображается следующая информация об OSD системы «StormWind»:
- Итого – общее количество OSD в кластере.
- Включенные – количество запущенных экранных меню.
- Выключенные – количество отключенных экранных меню. Можно просмотреть список отключенных экранных меню и узлов, на которых они размещены.

- **Реестр OSD дисков** (окно «Использование OSD»). Чтобы просмотреть детализацию по подключенным к хранилищу OSD дискам нажимается кнопка « >> »:



(Рисунок 202):

Рисунок 202 – Детализированная информация о дисках хранилища

Доступен просмотр диаграмм, объединенных в группу «Статистика кластера». В этой группе объединены графики, отображающие различные показатели кластера (во временном диапазоне, начиная от одного часа и заканчивая одним годом):

- **Вместимость хранилища**. Эта диаграмма представляет собой использованное и доступное бесплатное хранилище.

- **Пропускная способность**. На этой диаграмме представлена пропускная способность чтения/ записи для выбранного пула.
- **IOPS**. Эта диаграмма представляет количество операций чтения / записи в секунду для выбранного пула.
- **Статус монитора**. На этой диаграмме представлено количество узлов монитора StormWind и их состояние.
- **Состояние OSD**. Эта диаграмма представляет количество OSD StormWind и их статус.
- **Фиксированная задержка OSD**. На этой диаграмме представлена задержка во время операций фиксации OSD.
- **Примененная задержка OSD**. На этой диаграмме представлена задержка во время операций применения OSD.
- **Состояние PG**. На этой диаграмме показано количество PG StormWind и их состояние.
- **Использование OSD**.

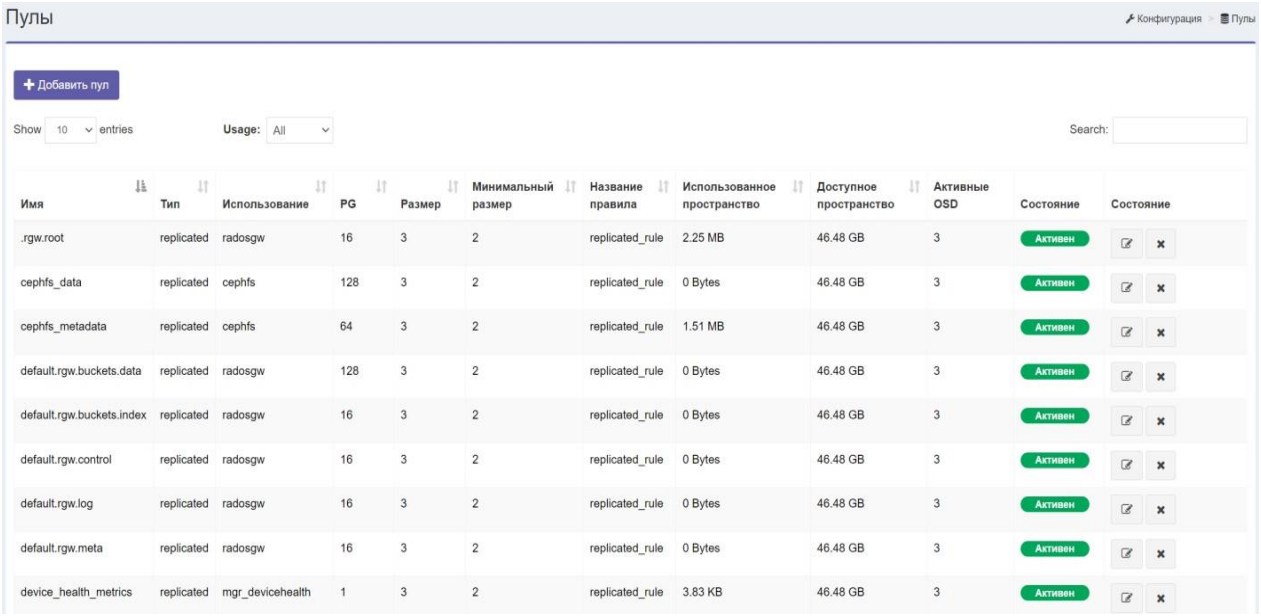
Доступен просмотр диаграмм, объединенных в группу «Статистика узла». Выбрать узел, для которого необходимо просмотреть статистику, а затем выбрать диаграмму, которую хотите просмотреть, из одного из следующих вариантов:

- **Центральная память (ЦП)**. Общая процентная загрузка ЦП для узла.
- **Память**. Общее процентное использование ОЗУ для узла.
- **Использование диска**. Использование диска в процентах, показывает, насколько заняты ваши диски.
- **Дисковая пропускная способность**. Скорость чтения / записи диска.

- **IOPS диска**. Общее количество операций с диском в секунду.
- **Перераспределенные сектора на диске**. Перераспределение секторов на диске с помощью SMART Tools.
- **Питание диска в часах**. Количество часов работы диска, считанное с помощью SMART Tools.
- **Температура диска**. Температура диска считывается с помощью SMART Tools.
- **Использование сети**. Использование сети в процентах показывает, насколько заняты интерфейсные карты.
- **Пропускная способность сети**. Скорость передачи чтения/ записи сети.

3.5.2 Управление пулами

3.5.2.1 Список пулов



При нажатии в меню Конфигурация -> Пулы, система отобразит список существующих пулов (Рисунок 203).

Рисунок 203 – Список пулов

В списке пулов отображается следующая информация для каждого пула:

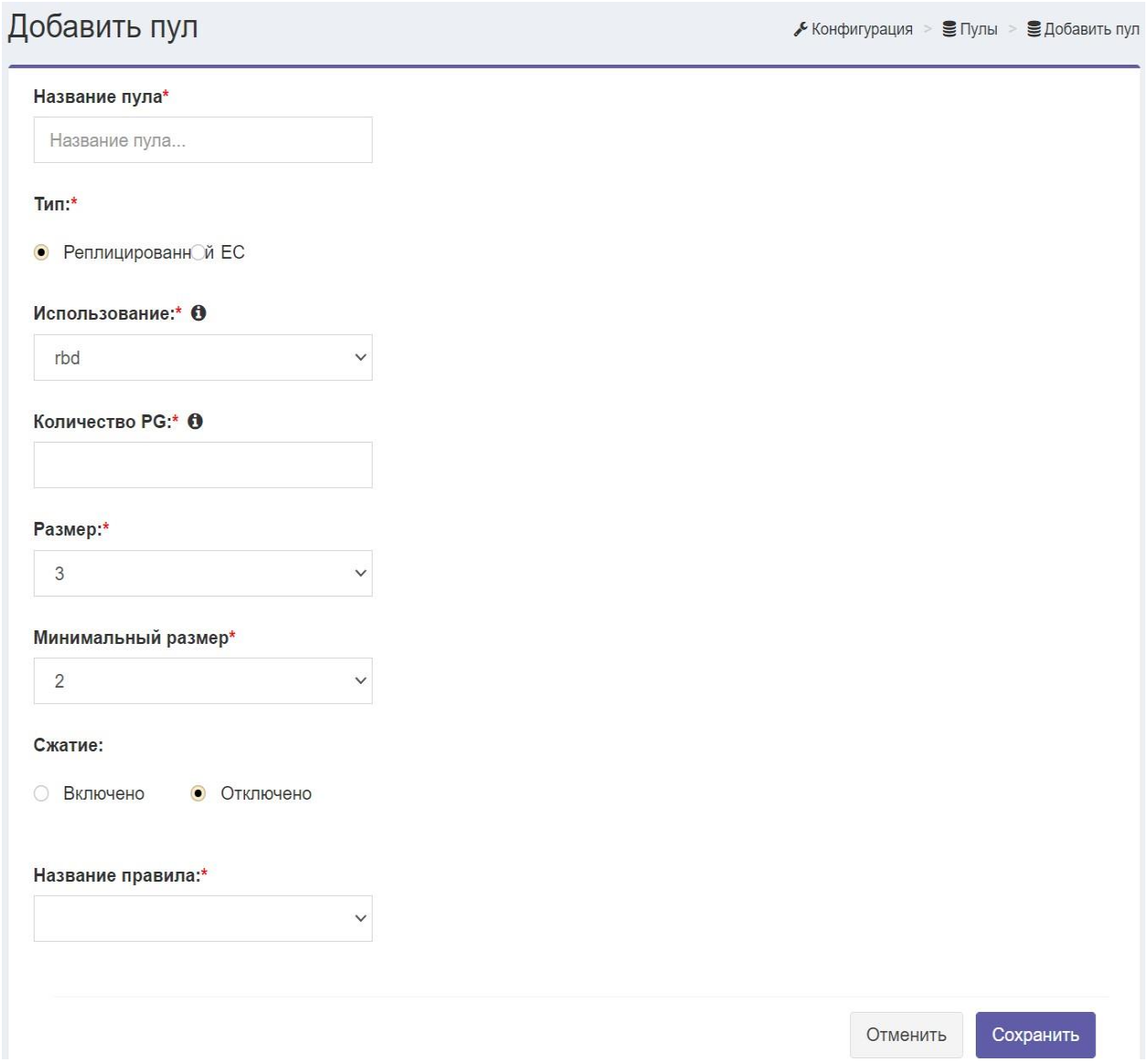
- **Имя** – название пула.
- **Тип**. Тип пула: Replicated или EC.
- **Использование**. Назначение пула: rbd, cephfs, radosgw, mgr_devicehealth.
- **PG** – количество PG в пуле.
- **Размер**:
- В случае реплицированного пула: количество реплик на объект.
- В случае пула EC: количество блоков на объект
- **Минимальный размер**:
- В случае реплицированного пула: минимальное количество реплик, необходимое для сохранения пула.
- В случае пула EC: минимальное количество блоков, необходимых для того, чтобы пул оставался активным и продолжал обслуживать клиентские запросы ввода-вывода.
- **Название правила**. Правило, используемое для распространения реплик.
- **Использованное пространство**. Объем памяти, который занимает пул.
- **Доступное пространство**. Общий объем доступной памяти.
- **Активные OSD**. Отображается количество активных OSD дисков.
- **Состояние**. Отображает текущий статус пула, который может быть одним из следующих:
- Активен – пул может обслуживать клиентские запросы ввода-вывода.
- Неактивен – пул не может обслуживать клиентские запросы ввода-вывода.

- Удален – пул удаляется.

ПРИМЕЧАНИЕ:

При удалении пула будут удалены все сохраненные в нем данные.

3.5.2.2 Добавить пул



При нажатии меню на Конфигурация -> Пулы-> Добавить пул, система откроет форму добавления пула (Рисунок 204).

Рисунок 204 – Форма добавления пула

Окно «Добавить пул» содержит следующие поля:

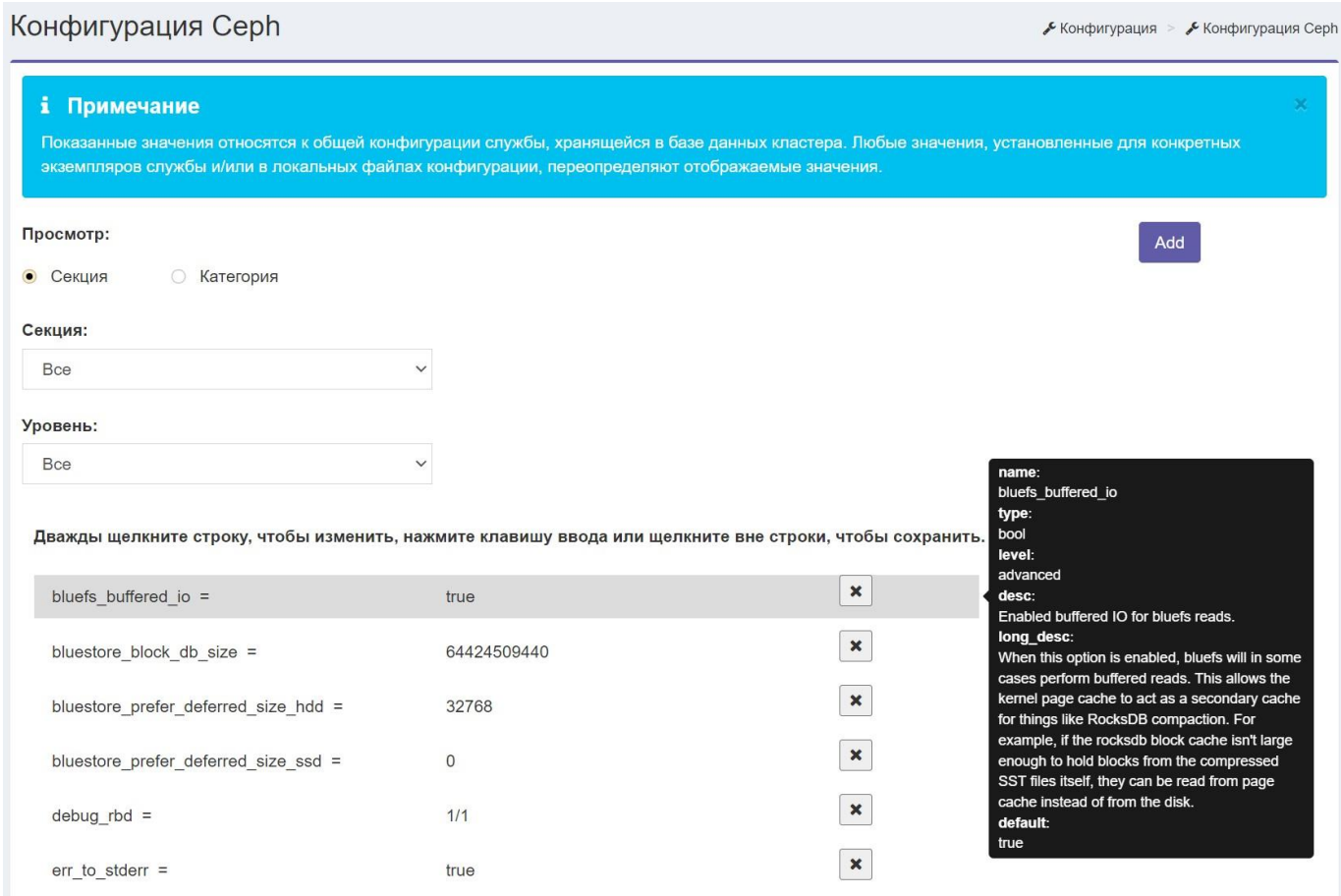
- **Название пула**. Имя пула, имя не может содержать пробелов.
- **Тип пула** – реплицируемый или EC.
- **Использование**. Для ISCSi используется rbd, для CIFS и NFS – cephfs, для S3 – radosgw.
- **Профиль EC**. Появляется в случае пула EC, чтобы можно было выбрать профиль EC
- **Количество PG**. Количество PG в пуле, вы должны выбрать это значение, чтобы каждый OSD обрабатывал общее количество PG примерно 100 PG (включая реплики) во всех его пулах.
- **Размер**:
- В случае реплицированного пула: количество реплик в пуле.
- В случае пула EC: общее количество блоков на объект. Что равно K + M, где K – это количество блоков данных, а M – количество блоков четности.
- **Минимальный размер**:
- В случае реплицированного пула: минимальное количество реплик, необходимое для пула для его активности и продолжения обслуживания клиентских запросов ввода-вывода
- В случае пула EC: минимальное количество блоков, необходимое для того, чтобы пул оставался активным и продолжал обслуживать клиентские запросы ввода-вывода.
- **Сжатие**. Для включения сжатия, выбрать «Включено».
- **Алгоритм сжатия**. Если включено сжатие, выбрать используемый алгоритм сжатия.

- **Название правила**. Правило использования, которое определяет, как распределяются сохраненные данные.

3.5.3 Конфигурация stormwind

3.5.3.1 Просмотр конфигурации stormwind

При нажатии меню на Конфигурация -> Конфигурация Ceph, можно просмотреть ключи конфигурации, которые сохранены в общая кластерной базе данных. Они применяются ко всем экземплярам сервисов, таких как OSD, мониторы, MDS и т.д., однако, они будут отменены любыми настройками, установленными для



конкретных экземпляров, а также любыми настройками, определенными в локальных файлах конфигурации.

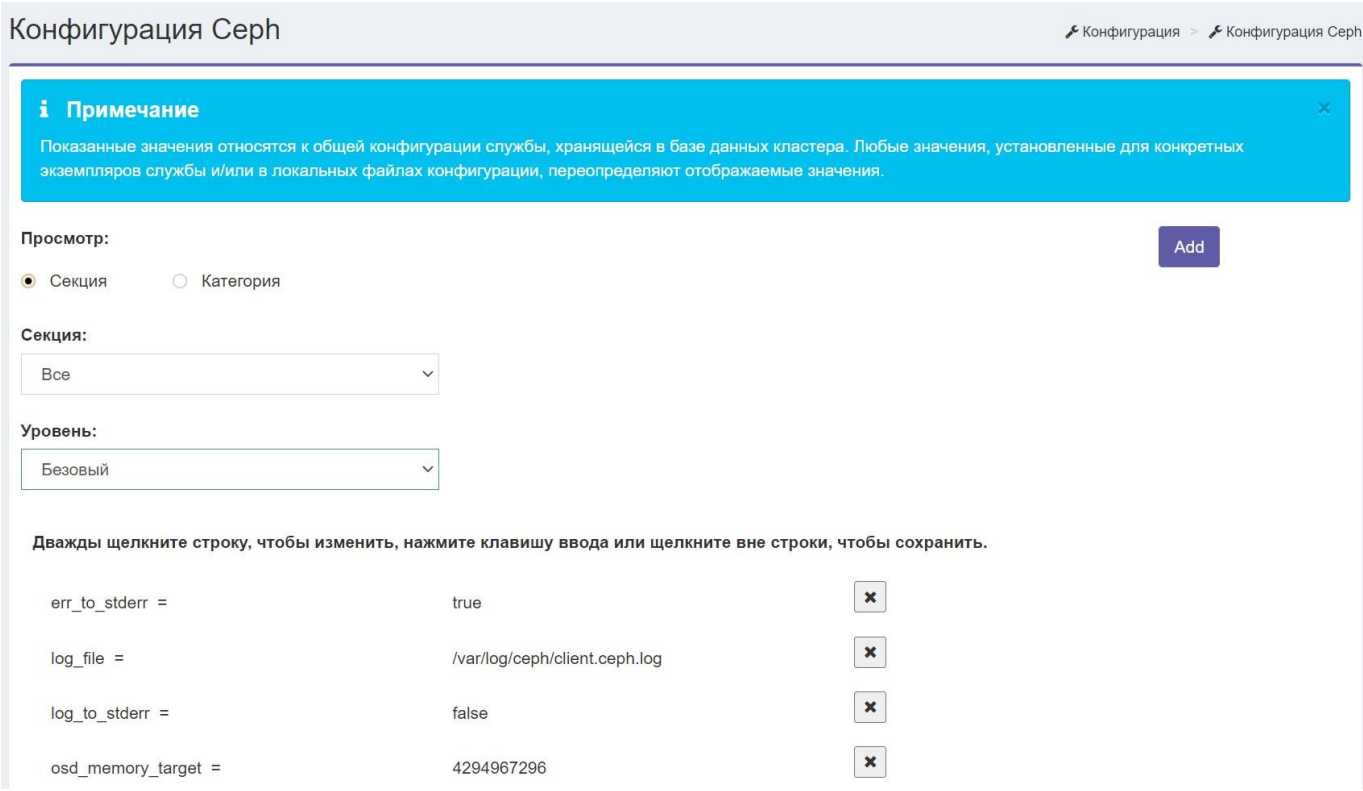
При наведении курсора мыши на любую клавишу система отображает справочное описание этой клавиши (Рисунок 205).

Рисунок 205 – Просмотр информации по ключам конфигурации

Можно фильтровать ключи по:

- **Секция**. Доступные варианты текущих разделов:
- все
- общее
- osd – демон хранилища
- mon – демон монитора
- mgr
- mds – сервер метаданных
- клиент.
- **Уровень**. По умолчанию система будет работать на всех уровнях, или можно выбрать уровень конфигурации из одного из следующих значений (**Рисунок 206**):
- Все
- Базовый • Продвинутый
- Разработчик.

Рисунок 206 – Выбор уровня конфигурации

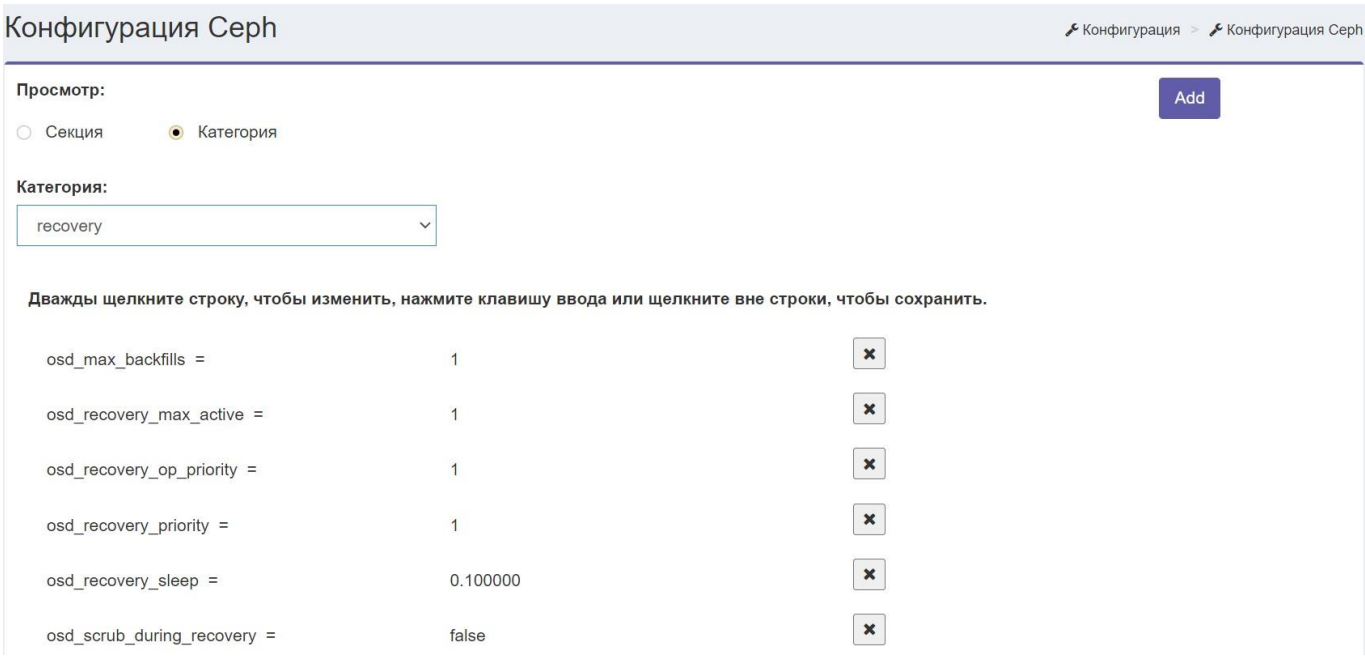


- **Категория**. Текущие параметры категорий (**Рисунок 207**):
- Recovery (Восстановление)
- Scrubbing (Очистка).

Рисунок 207 – Выбор категории вместе с параметрами

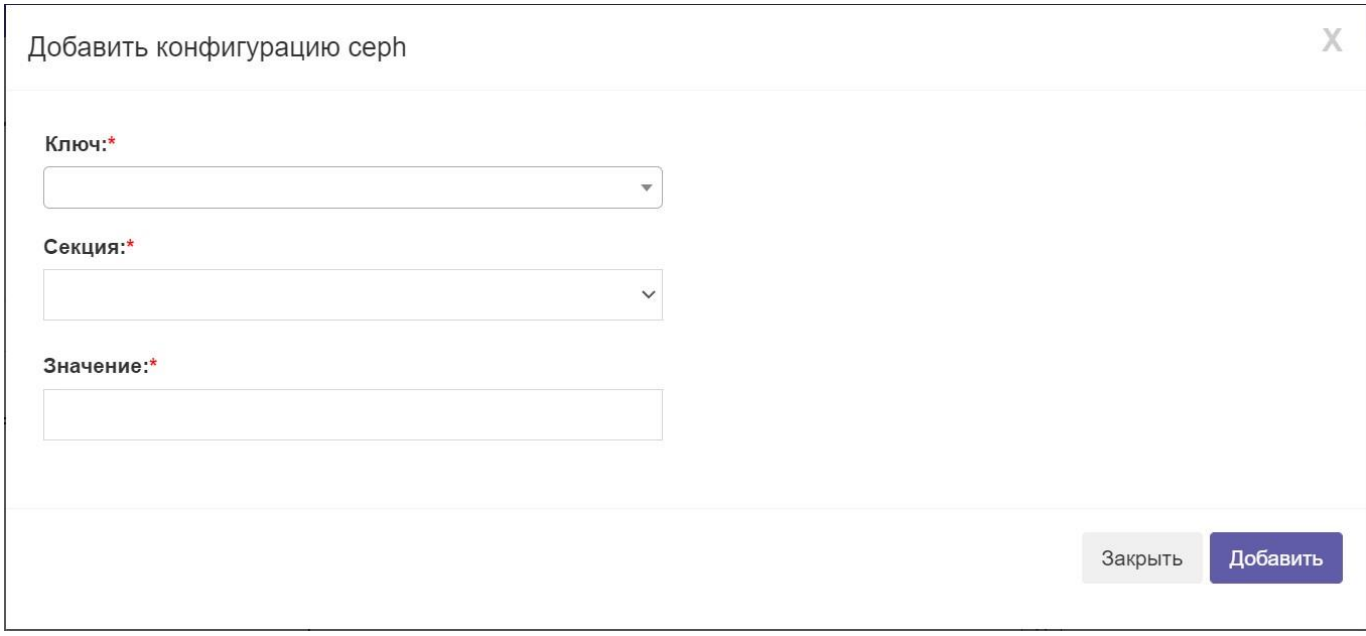
3.5.3.2 Добавить ключ конфигурации stormwind

Доступно добавление нового ключа конфигурации StormWind (Рисунок 208).



- **Ключ**. Из списка доступных ключей можно выбрать имя ключа, которое необходимо добавить.
- **Секция**. Выберите раздел, в который хотите добавить ключ.
- **Значение**. Введите значение выбранного ключа.

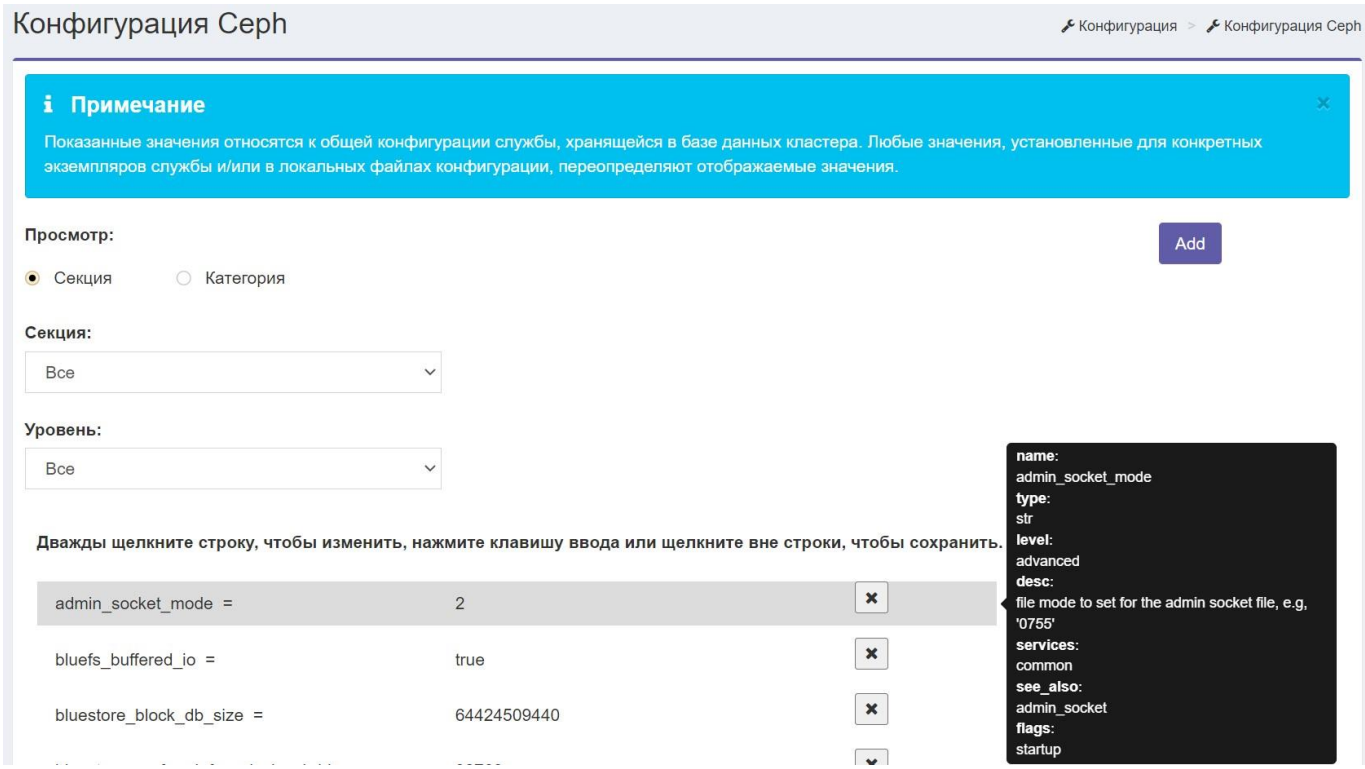
Рисунок 208 – Добавление ключа конфигурации



3.5.3.3 Удалить значение ключа конфигурации stormwind

Можно удалить один из существующих ключей конфигурации StormWind, по нажатию кнопки «✖» в строке с ключом (Рисунок 209).

Рисунок 209 – Удаление ключа конфигурации



3.5.4 Управление узлами

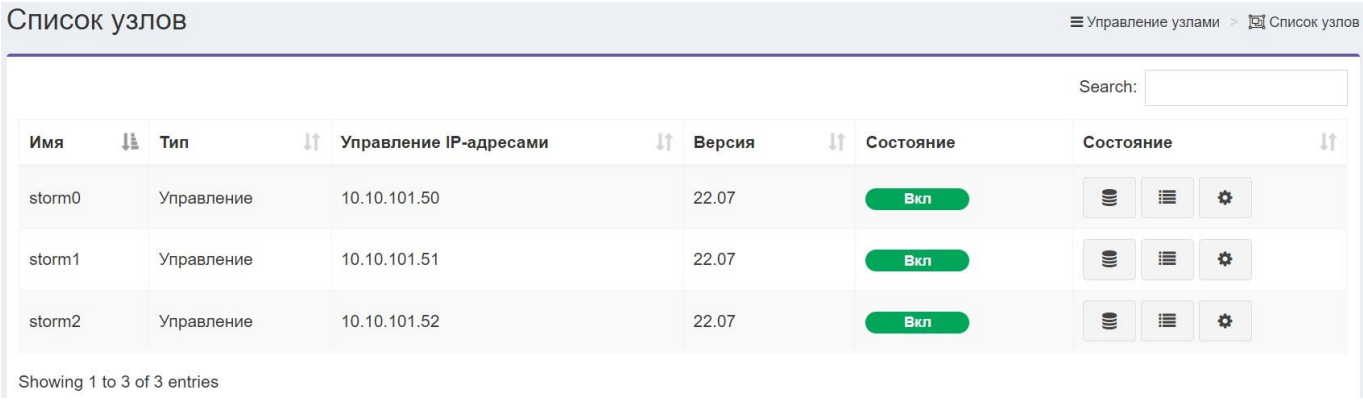
3.5.4.1 Список узлов

Система управления позволяет просматривать список узлов кластера и управлять ими. Для этого необходимо перейти в пункт меню Управление узлами –> Список узлов (Рисунок 210).

Рисунок 210 – Список узлов кластера

В списке узлов отображается следующая информация о каждом узле:

- **Имя** – имя хоста узла.
- **Тип** – тип узла, который может быть «Управление» или «Хранилище».
- **Управление IP-адресами** – IP-адреса управления узлом.



- **Состояние** – статус узла, работает он или нет.
- **Действие**. Система отображает действия, которые можно выполнять на узле, в зависимости от его типа и статуса:
- Список *физических дисков*. Показывает список локальных дисков для узла и позволяет управлять ими. Кнопка будет доступна только для запущенных узлов.
- *Показать лог* – системный журнал узла. Кнопка будет доступна только для запущенных узлов.
- *Задание роли узла*. Открывает форму «Управление ролями». Кнопка будет доступна только для запущенных узлов.

▪ Удалить

Позволяет удалить неработающий узел хранения, который удалит узел из кластера и все его OSD. Кнопка будет доступна для узлов типа «Хранилище» и только когда они отключены. *ПРИМЕЧАНИЕ:*

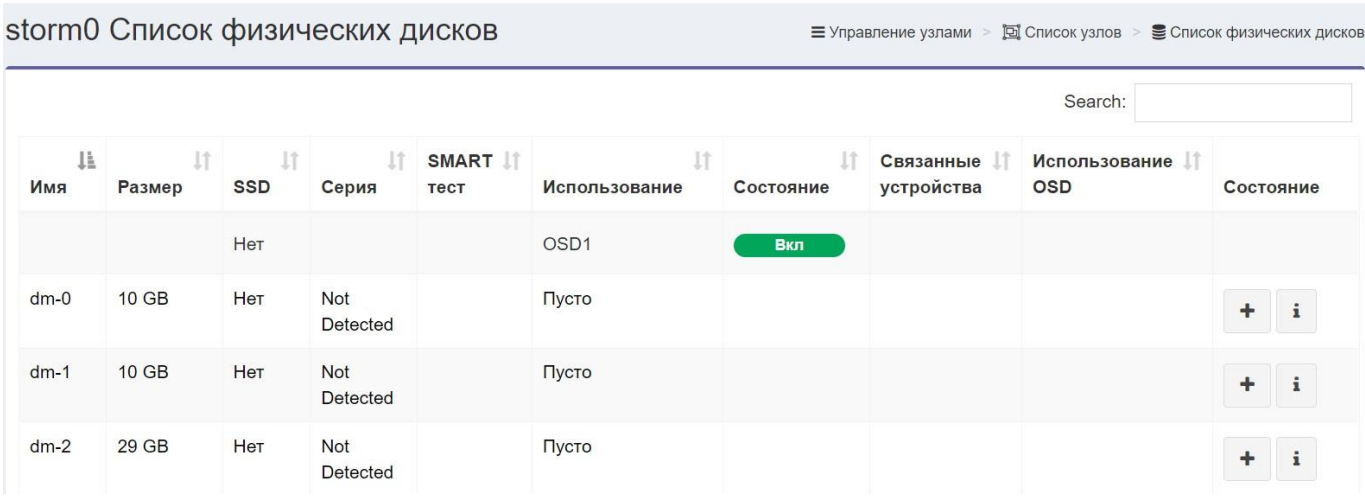
Если есть неработающий узел хранения, можно повторно использовать его OSD, переместив их на другие узлы перед удалением узла.

3.5.4.2 Список физических дисков узла

В системе управления отображается список локальных дисков для определенного узла (Рисунок 211).

Рисунок 211 – Список физических дисков узла В списке локальных дисков узла отображается следующая информация о каждом диске:

- **Имя** – имя локального диска.
- **Размер** – размер диска.
- **SSD** – в этом столбце указывается, является ли диск SSD или нет.



- **Серия** – серийный номер диска.
- **SMART тест**.
- **Использование**. В этом столбце показано, используется ли диск в кластере и каково его использование. Использование диска может быть одним из следующих значений:
- Система – означает, что диск используется как системный.
- Журнал – означает, что диск используется как журнал WAL / DB.

- OSD – означает, что диск используется как диск для хранения OSD StormWind. Система отображает свое количество OSD.
- Пусто – это означает, что диск не используется в кластере.
- Установленный – означает, что диск не используется в кластере, но он смонтирован.
- **Состояние** – отображается состояние узла (вкл./ выкл.).
- **Связанные устройства**.
- **Использование OSD** – процент использования диска.
- **Действие**. Система отображает действия, которые можно выполнять с диском, в зависимости от его типа и статуса.
- *Добавить устройство*. Добавляет локальный диск в качестве OSD, журнала, кэша. Он доступен, только если диск не используется или не смонтирован (**Рисунок 212**).

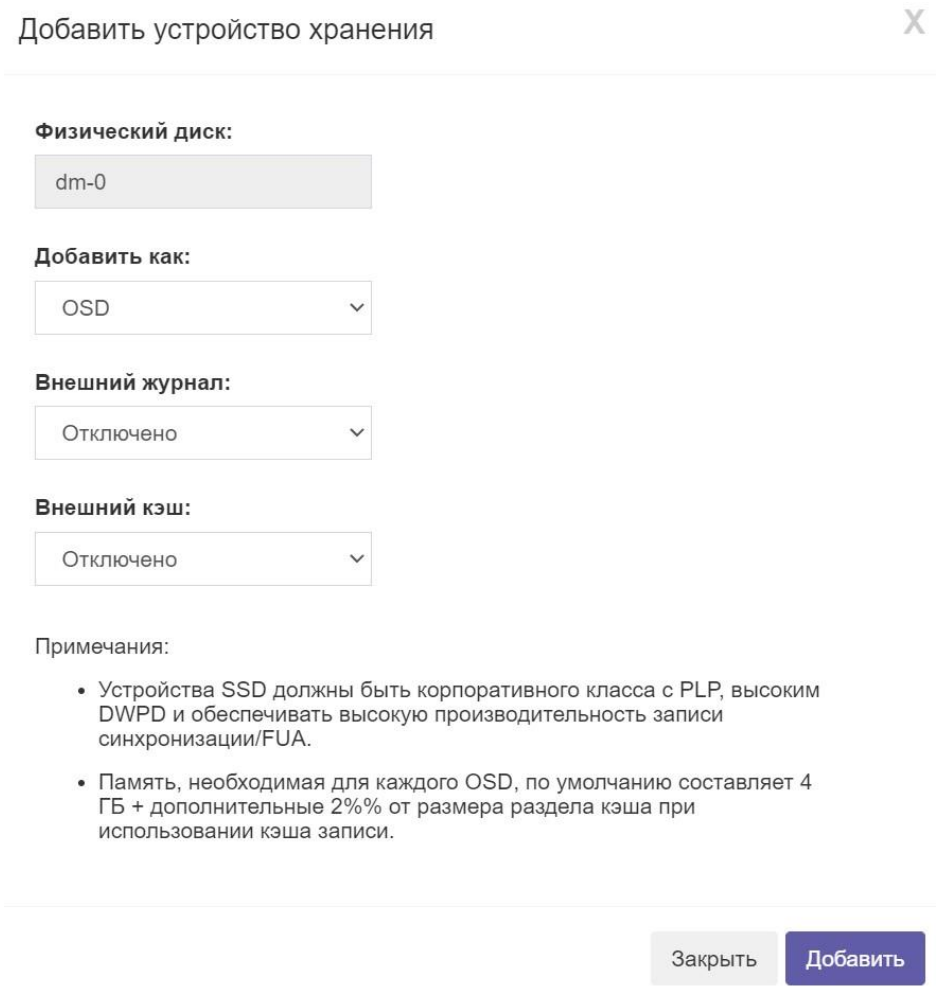


Рисунок 212 – Добавление устройства

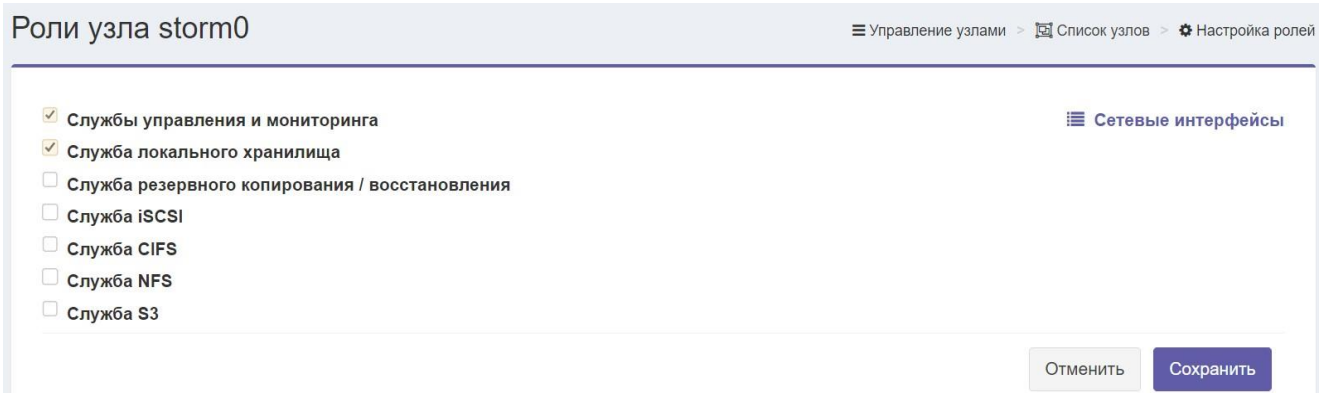
ПРИМЕЧАНИЕ:

Вы не сможете добавить диск в качестве OSD или журнала, если его узел не имеет Local Служба хранения, назначенная ее ролям, сначала необходимо обновить роли узлов с помощью Форма управления ролями.

3.5.4.3 Управление ролями

Система показывает роли, назначенные на данный момент узлу, и позволяет добавлять дополнительные роли или удалить существующие роли с помощью формы управления ролями (Рисунок 213).

Рисунок 213 – Назначение ролей для узла



3.5.4.4 Просмотр журнала

Система позволяет просматривать системный журнал узла (Рисунок 214).

Рисунок 214 – Журнал ошибок

Для просмотра последних записей журнала использовать кнопку «Обновить».

3.5.5 Управление iscsi дисками

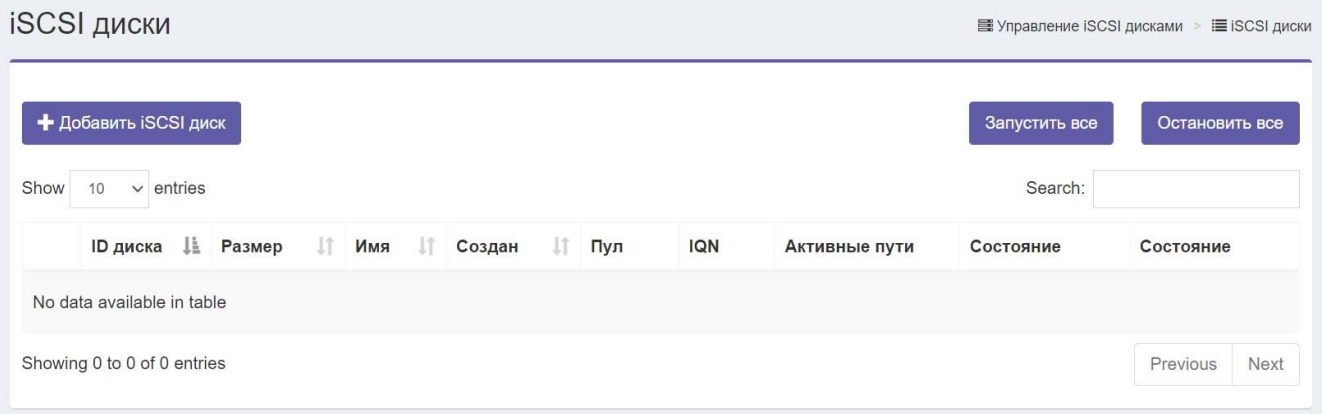
3.5.5.1 Список iscsi дисков

При переходе в пункт меню *Управление iSCSI дисками -> iSCSI диски* отображается список iSCSI дисков системы (**Рисунок 215**).

Рисунок 215 – Список iSCSI дисков

В списке iSCSI дисков отображается следующая информация о каждом диске:

- **ID диска** – идентификатор диска
- **Размер** – размер диска
- **Имя** – имя диска



- **Создан** – дата создания диска
- **Пул** – пул, который развернут на диске
- **IQN** (с англ. iSCSI Qualified Name) – уникальный идентификатор устройства
- **Активные пути**
- **Состояние** – отображается состояние диска (вкл./ выкл.)
- **Действие**

Страница списка дисков включает функцию поиска, которая может выполнять поиск и фильтрацию дисков по нескольким критериям, таким как имя и размер диска.

Есть также несколько действий, которые мы можем выполнить с диском, такие как запуск / остановка, редактирование, удаление диска, а также присоединение и отсоединение. При отключении удаляются параметры iSCSI из метаданных диска, но не удаляется образ диска.

Чтобы просмотреть пути для нашего диска, в столбце «Активные пути» щелкните число показанных путей. Это покажет IP-адреса, используемые карты Ethernet и их текущие назначения узлов.

Информацию по добавлению iSCSI диска см. в пункте **Ошибка! Источник ссылки не найден.**.

3.5.5.2 Список назначенных путей

Пункт меню Управление iSCSI дисками -> Назначение пути (Рисунок 216):

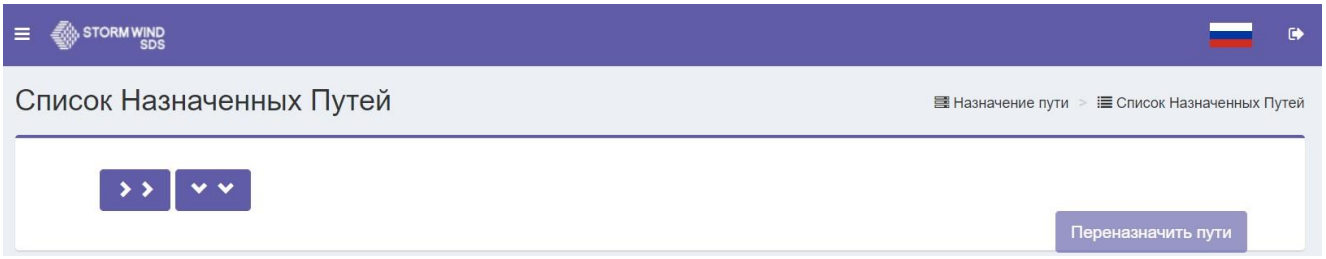


Рисунок 216 – Список назначенных путей

3.5.6 Управление репликацией

Данная функция позволяет реплицировать данные с исходного диска на целевой диск в другом кластере.

Репликация включается путем создания задания репликации в исходном кластере. Первый раз выполняется задание репликации, оно переносит все данные с исходного диска на целевой диск, последующие задания экземпляры будут передавать только изменения / различия, сделанные с момента предыдущего экземпляра репликации.

3.5.6.1 СПИСОК ЗАДАЧ РЕПЛИКАЦИИ

Для отображения списка задач репликации необходимо перейти в пункт меню Управление iSCSI дисками -> Репликация -> Задачи (**Рисунок 217**).

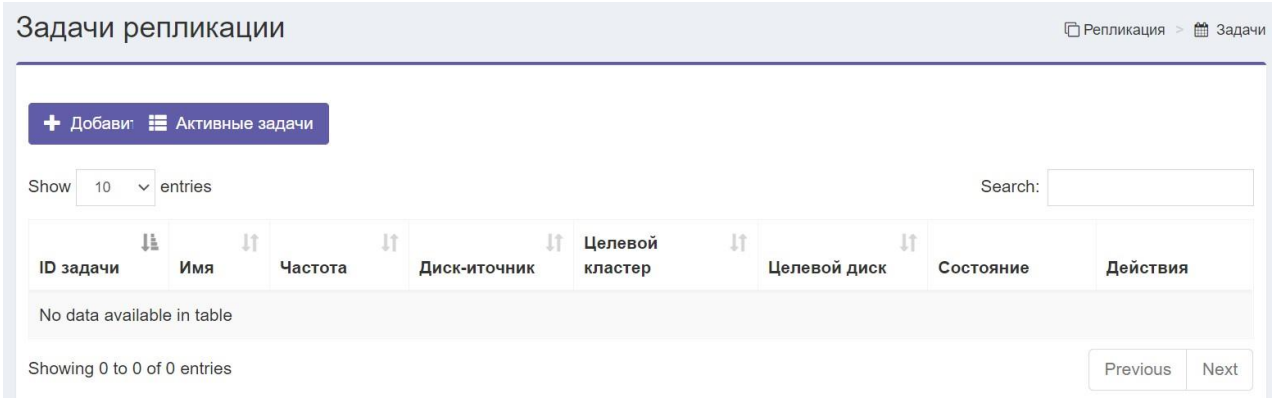


Рисунок 217 – Список задач репликации

3.5.6.2 Создание задания репликации

Доступно добавление задания репликации в исходный кластер (кнопка «Добавить задачу репликации») (Рисунок 218).

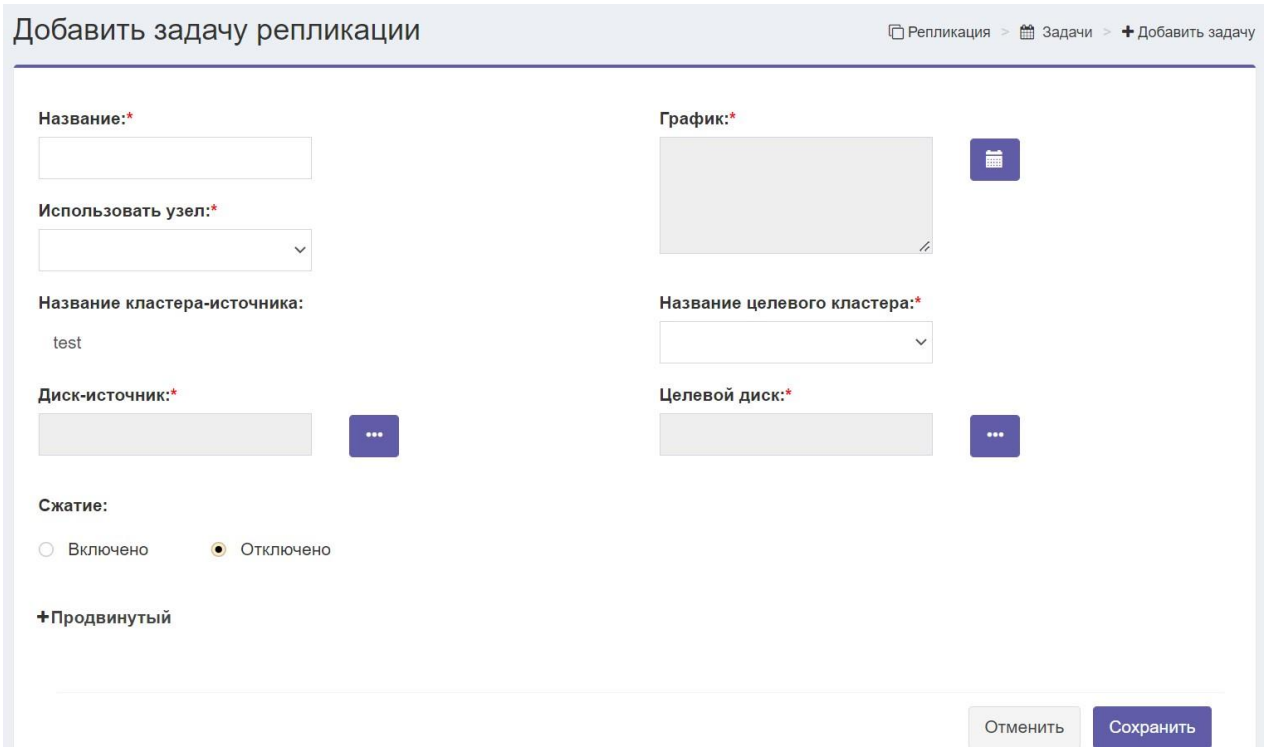


Рисунок 218 – Добавление задачи репликации

Форма требует следующей информации:

- **Название**. Название задания репликации
- **Использовать узел**. Узел, который будет использоваться для запуска задания репликации в исходном кластере, для выбора предоставляются узлы из списка резервного копирования / репликации.
- **График**. Устанавливает, как часто будет выполняться задание (**Рисунок 219**).

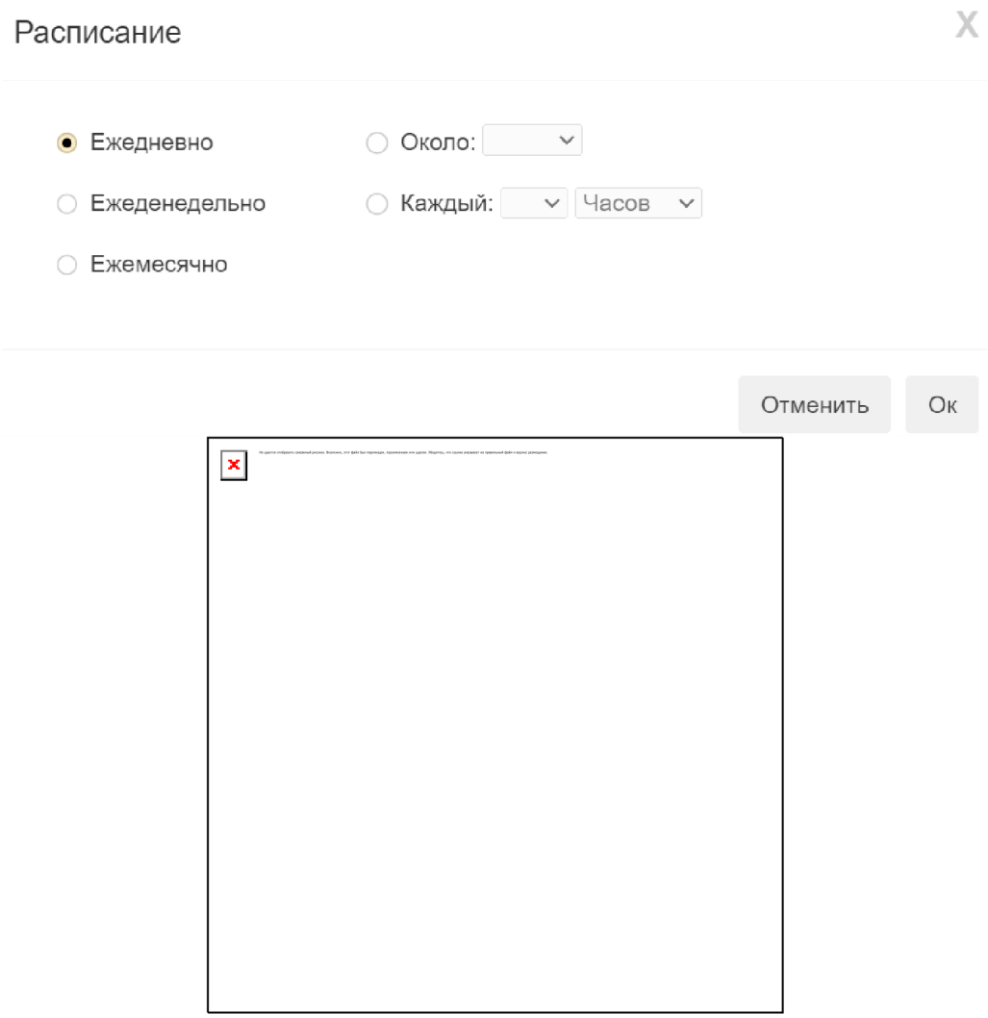


Рисунок 219 – Настройка расписания выполнения задания

Сначала вы должны выбрать частоту работы из одного из следующих вариантов: о

Ежедневно

▪ **Около**. Работа будет выполняться ежедневно в определенный час, вы выбираете час в 24-часовом формате.

▪ **Каждый**. Задание будет выполняться каждые x минут или x часов. о

Еженедельно (**Рисунок 220**):

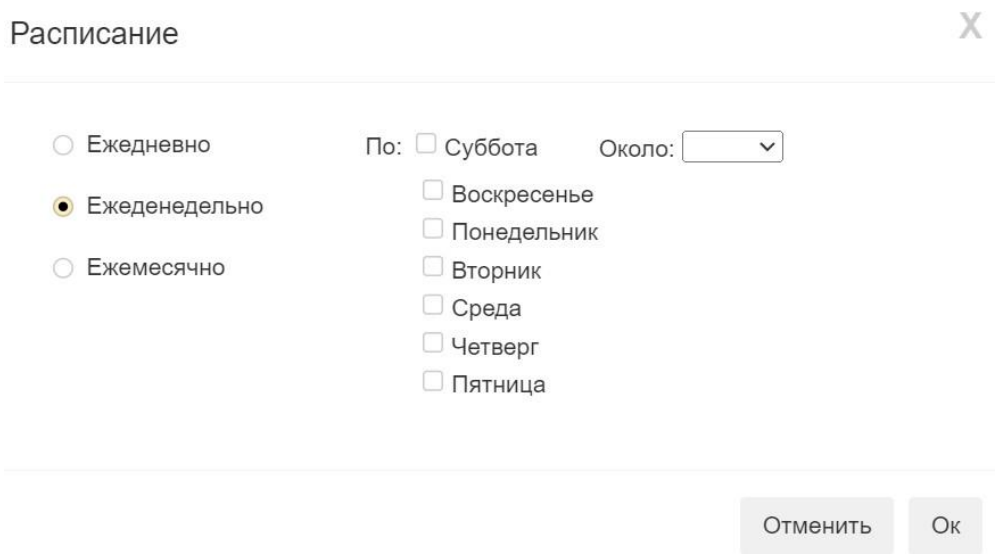


Рисунок 220 – Настройка еженедельного расписания

▪ **По**. Вы можете выбрать дни недели, в которые будет выполняться задание.

▪ **Около**. Работа будет выполняться ежедневно в определенный час.

o **Ежемесячно** (**Рисунок 221**):

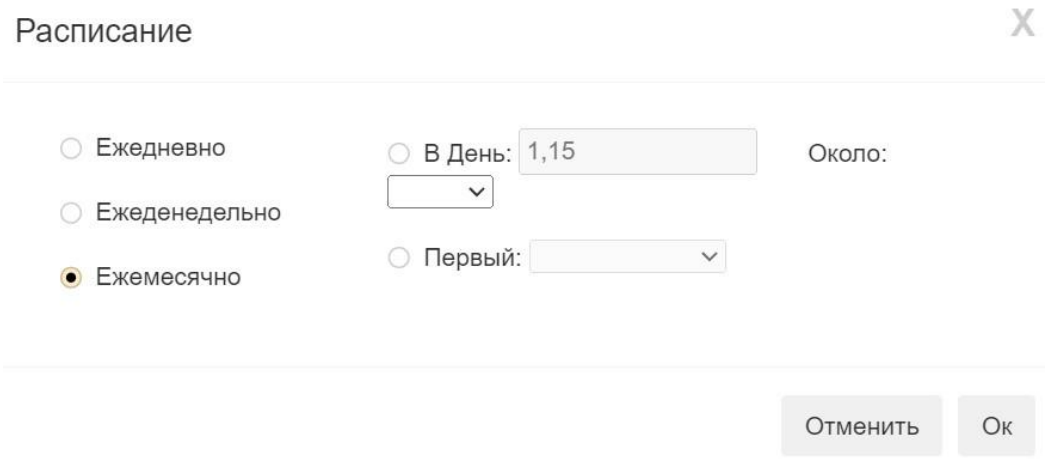


Рисунок 221 – Настройка ежемесячного расписания

▪ **В день**. Вы можете выбрать день (дни) для запуска задания репликации.

▪ **Первый**. Работа может выполняться в первое воскресенье, понедельник месяца.

▪ **Около**. Работа будет запущена в определенный час.

• **Название кластера-источника**. Имя исходного кластера (имя текущего кластера).

- **Диск-источник**. Система позволяет выбрать диск iSCSI из списка дисков в исходном кластере.
- **Название целевого кластера**. Имя целевого кластера можно выбрать из целевых кластеров, которые определены ранее.
- **Целевой диск**. Система позволяет выбрать диск iSCSI из списка целевых дисков репликации на целевой кластер.
- **Сжатие**. Если необходимо включить сжатие во время передачи данных.

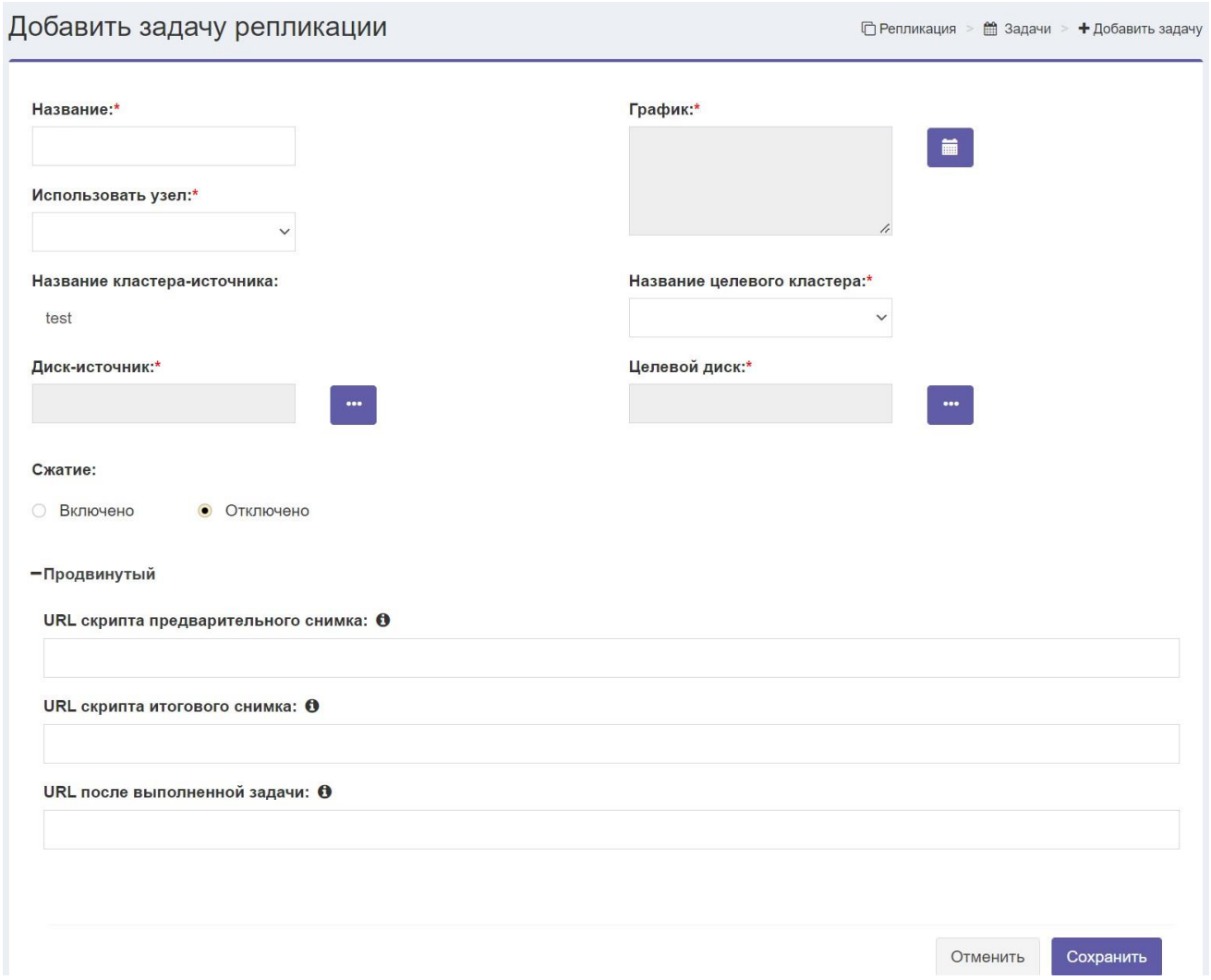


Рисунок 222 – Добавление задачи репликации в продвинутом формате

Расширенная форма дополнена следующей информацией (**Рисунок 222**):

- **URL скрипта предварительного снимка**. Необязательный URL-адрес настраиваемого сценария, который вы хотите запустить до того, как задание репликации сделает снимок из исходного диска.
- **URL скрипта итогового снимка**. Необязательный URL-адрес настраиваемого сценария, который вы хотите запустить после того, как задание репликации сделает снимок из исходного диска.
- **URL после выполненной задачи**. Необязательный URL-адрес настраиваемого сценария, который нужно запустить после создания снимка с исходного диска.

4.5.6.3 СПИСОК АКТИВНЫХ ЗАДАНИЙ

В системе доступен список текущих работ.

4.5.6.4 СПИСОК ПОЛЬЗОВАТЕЛЕЙ РЕПЛИКАЦИИ

Для отображения списка пользователей репликации необходимо перейти в пункт меню Управление iSCSI дисками -> Репликация -> Пользователи (**Рисунок 223**).

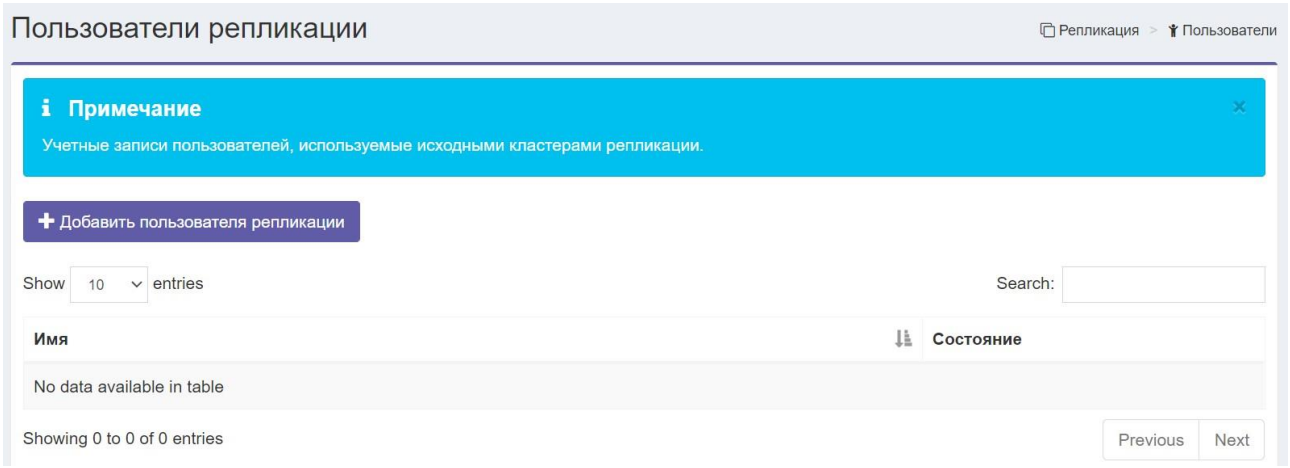


Рисунок 223 – Список пользователей репликации Добавление пользователя репликации (**Рисунок 224**).

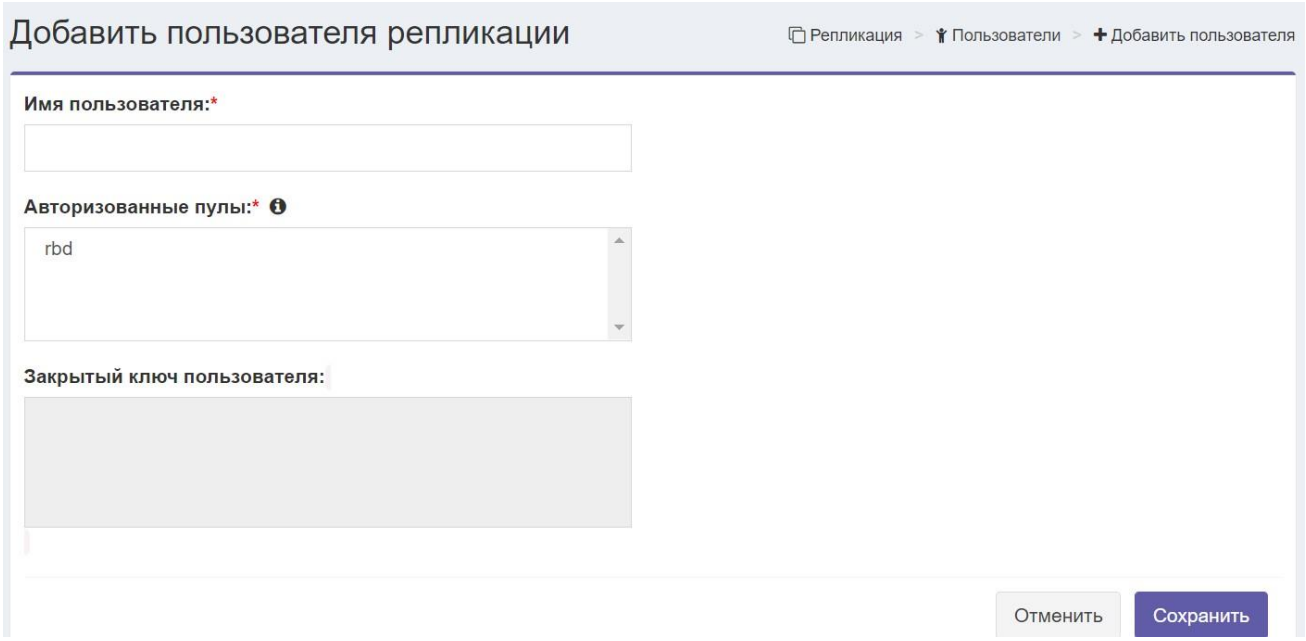


Рисунок 224 – Добавление пользователя репликации

3.5.6.5 СПИСОК ЦЕЛЕВЫХ КЛАСТЕРОВ

Для отображения списка целевых кластеров необходимо перейти в пункт меню Управление iSCSI дисками -> Репликация -> Целевые кластеры (**Рисунок 225**).

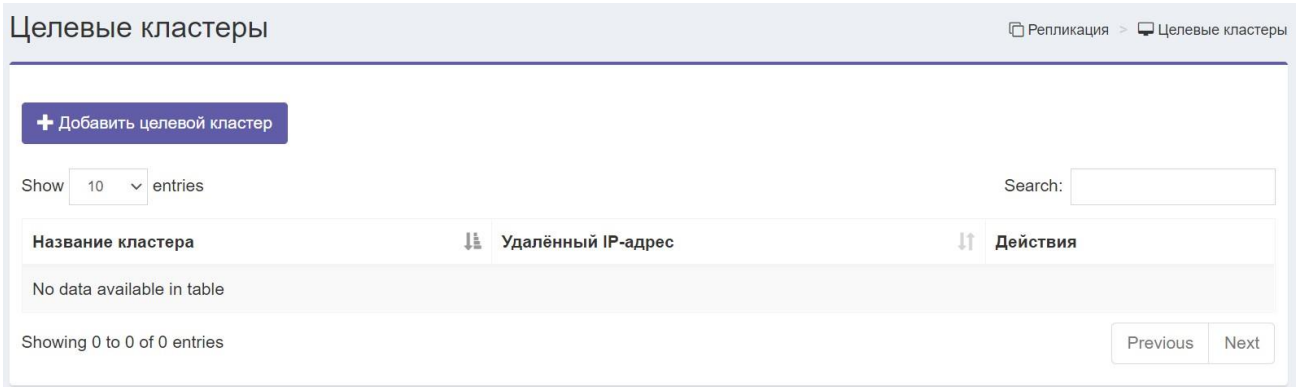


Рисунок 225 – Список целевых кластеров

Добавление целевого кластера (**Рисунок 226**).

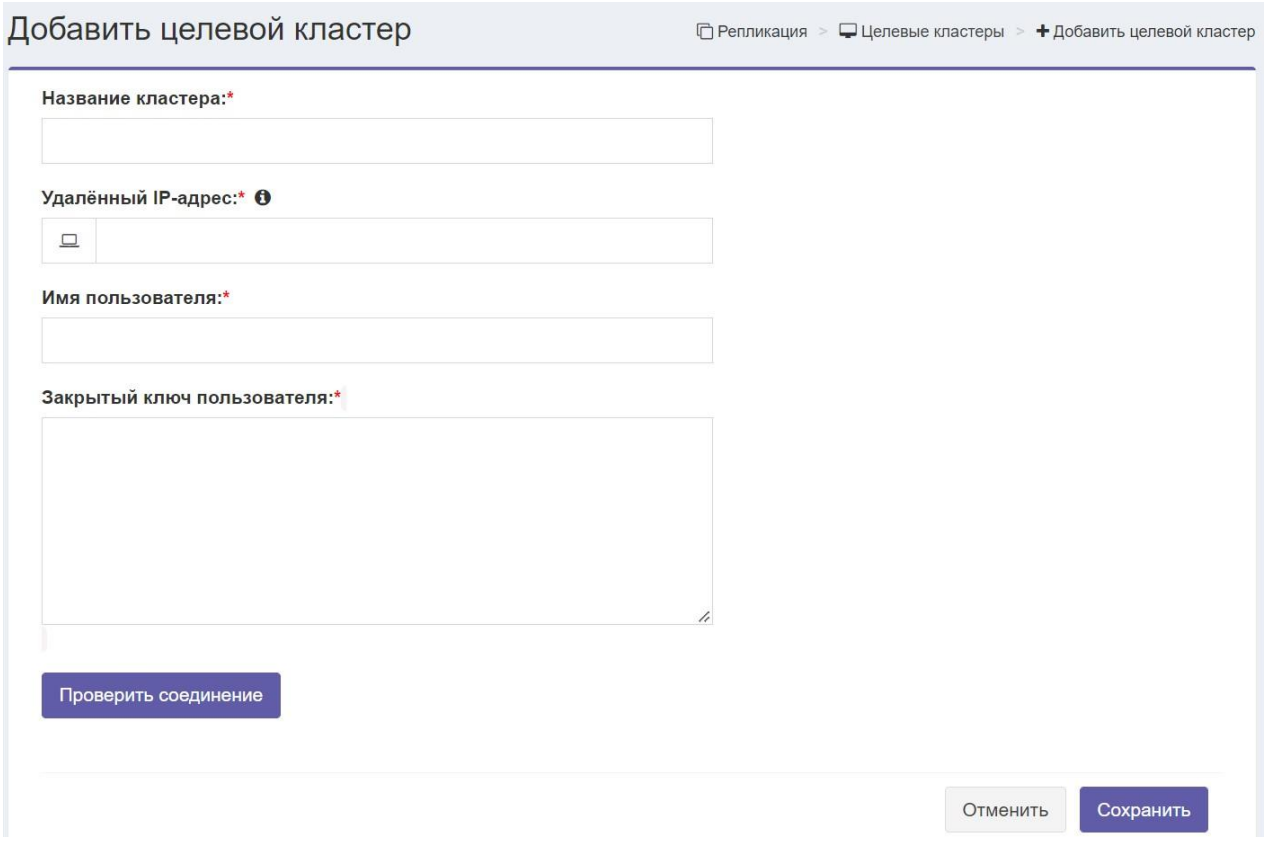


Рисунок 226 – Добавление целевого кластера

3.5.7 Управление rbd

3.5.7.1 Список rbd

При переходе в пункт меню *Управление RBD -> Список RBD* отображается список RBD системы (**Рисунок 227**).

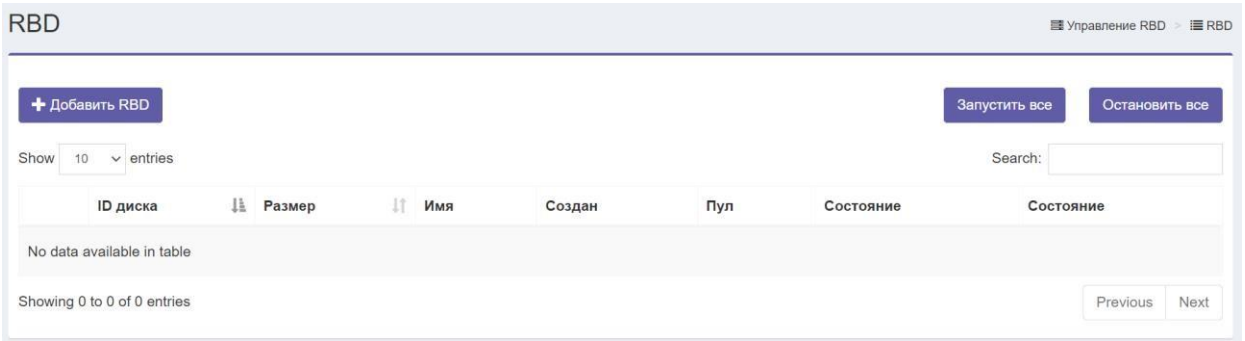


Рисунок 227 – Список RBD

В списке RBD отображается следующая информация:

- **ID диска** – идентификатор диска
- **Размер** – размер диска
- **Имя** – имя диска
- **Создан** – дата создания диска
- **Пул** – пул, который развернут на диске
- **Состояние** – отображается состояние диска (вкл./ выкл.)
- **Действие**

3.5.7.2 Добавление rbd диска

При нажатии на кнопку «Добавить RBD» открывается форма добавления нового RBD диска (**Рисунок 228**).

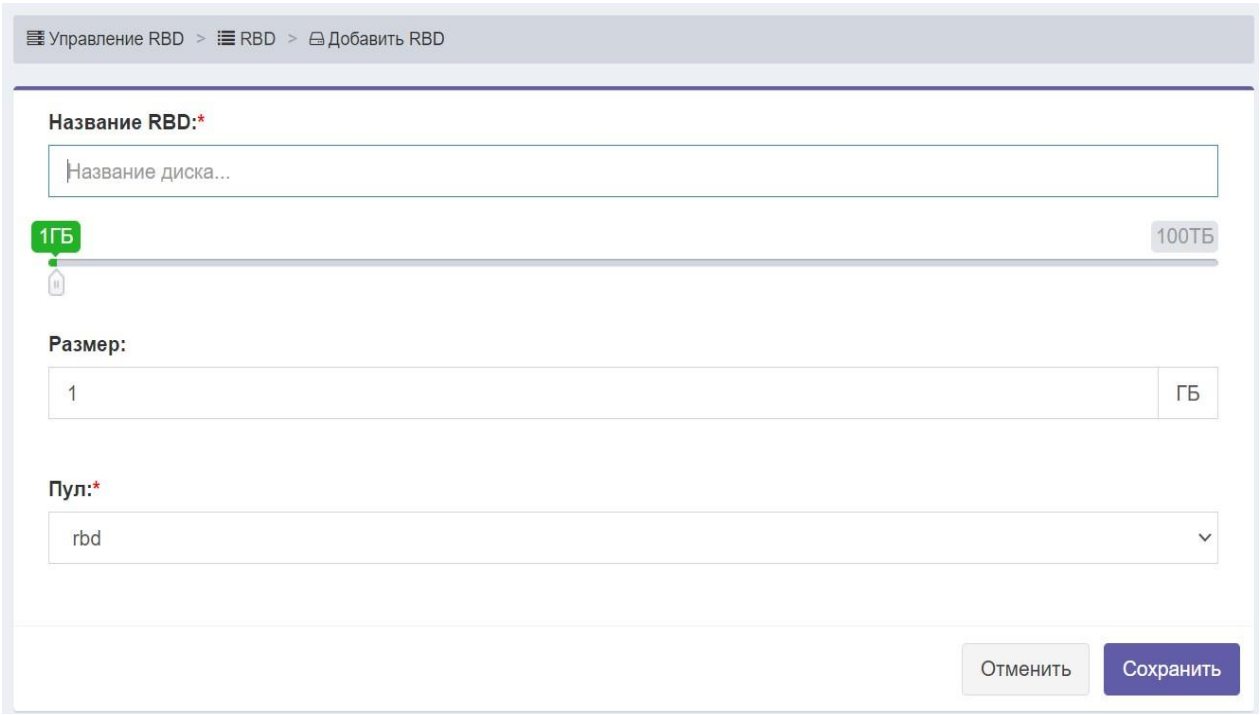


Рисунок 228 – Добавление RBD диска

3.5.8. Управление cifs

3.5.8.1 Просмотр ресурсов cifs

Система отображает список существующих общих ресурсов, в котором отображаются следующие столбцы (**Рисунок 229**)

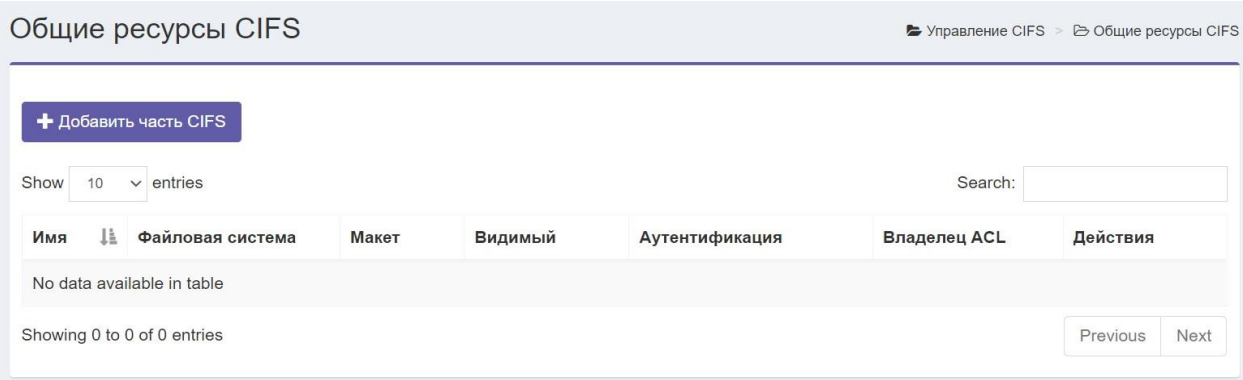


Рисунок 229 – Список общих ресурсов

- **Имя** – поделиться именем
- **Файловая система** – файловая система, в которой создается общий ресурс.
- **Макет** – макет, в котором создается общий ресурс.
- **Видимый** – показывает, доступна ли общая папка для просмотра клиентам.
- **Аутентификация** – показывает, требуется ли аутентификация для доступа к общему ресурсу.
- **Владелец ACL** – владелец ACL, это пользователь, который может назначать другим права доступа к общему ресурсу.
- **Действия**:
- *Добавить* – открывает новую форму публикации.
- *Удалить* – удалить текущую общую папку, включая все сохраненные данные.

3.5.8.2 Добавить общий ресурс cifs

Система открывает форму CIFS Share (Рисунок 230).

Рисунок 230 – Добавление части CIFS

Форма CIFS Share содержит следующие поля:

- **Имя** – имя общего ресурса.
- **Файловая система** – файловая система, в которой будет создан общий ресурс.
- **Макет** – макет, в котором будет создан общий ресурс.
- **Возможность просмотра** – указывает, доступна ли общая папка для просмотра клиентам.
- **Аутентификация** – вы можете выбрать без аутентификации или AD. Если вы выбрали AD, вам потребуется ввести владельца ACL.
- **Действия**
- *Сохранить* – сохраняет добавленную долю.

3.5.8.3 Просмотр статуса cifs

Доступен просмотр текущего статуса CIFS (Рисунок 231).

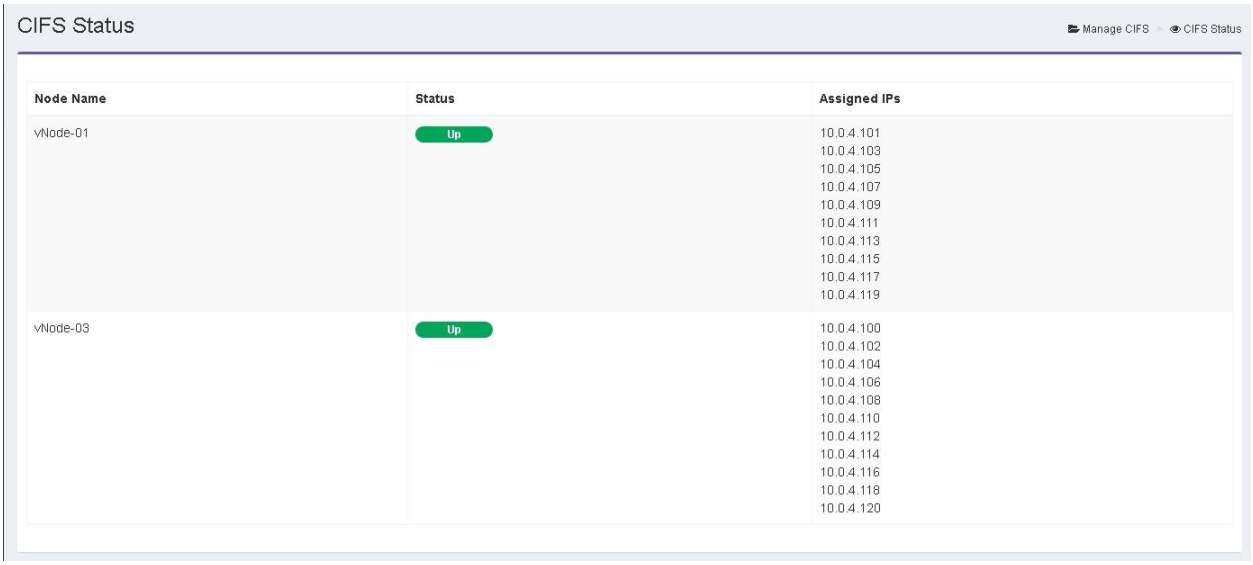


Рисунок 231 – Статус CIFS

В системе отображаются следующие столбцы:

- **Имя узла** – имя узла сервера CIFS
- **Статус –** статус узла, включен или выключен
- **Назначенные IP-адреса**. IP-адреса, назначенные каждому узлу
- **Количество подключений**. Количество активных клиентских подключений

3.5.8.4 Просмотр подключений

Для просмотра каждого активного соединения выводятся следующие данные:

- **Имя пользователя** – имя пользователя подключенного клиента
- **Название группы** – имя группы подключенного клиента
- **Клиентский IP** – IP подключенного клиента
- **Поделиться именем** – ресурсы, к которым подключен клиент

3.5.9 Управление nfs

3.5.9.1 Просмотр nfs exports

Для просмотра выводится список существующих NFS Exports, содержащий следующие столбцы (Рисунок 232):

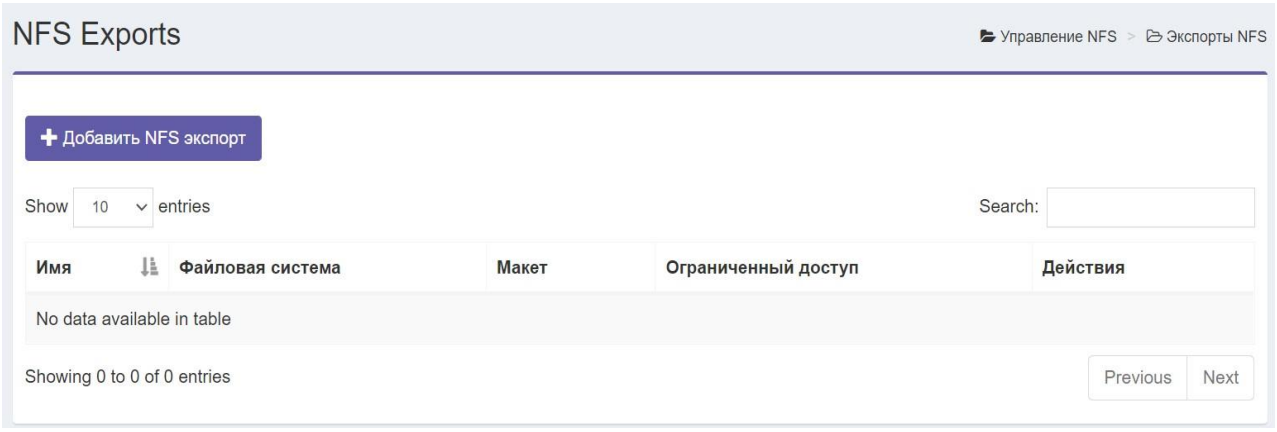


Рисунок 232 – NFS Exports

- **Имя** – имя NFS Export.
- **Файловая система**. Файловая система, в которой создается NFS Export.
- **Макет**. Макет, в котором создается NFS Export.
- **Действия**
  - *Добавить* – открывает новую форму NFS Export.
  - *Удалить* – удаляет текущий экспорт, включая все сохраненные данные.

3.5.9.2 Добавление nfs exports

Система открывает форму для создания NFS Exports (Рисунок 233).

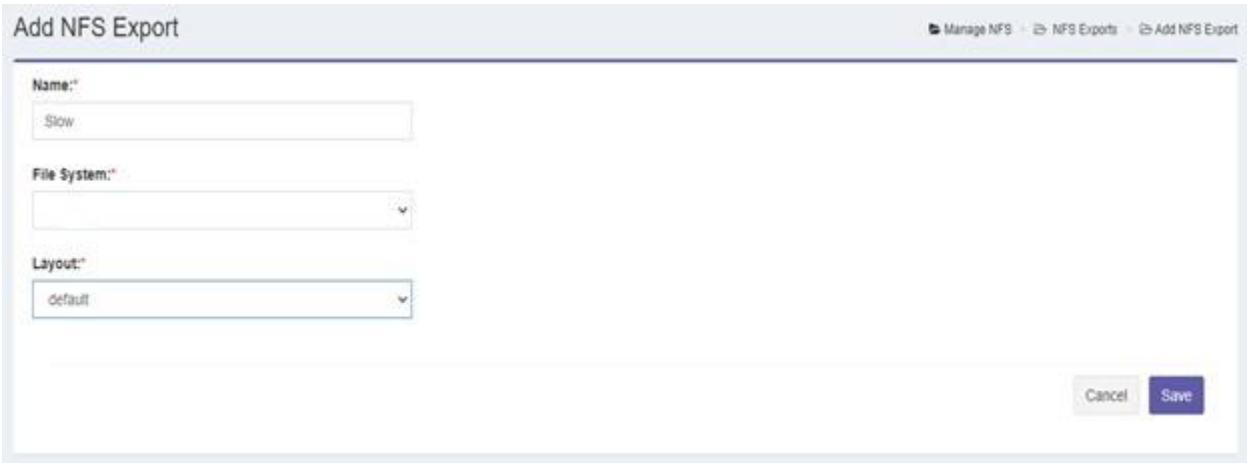


Рисунок 233 – Создание NFS Export

Форма добавления NFS Exports содержит следующие поля:

- **Имя** – имя экспорта.
- **Файловая система** – файловая система, в которой будет создан экспорт.
- **Действия**:
- *Сохранить* – сохраняет добавленный экспорт.

3.5.9.3 Просмотр статуса nfs

Возможно просмотреть текущий статус NFS (Рисунок 234).

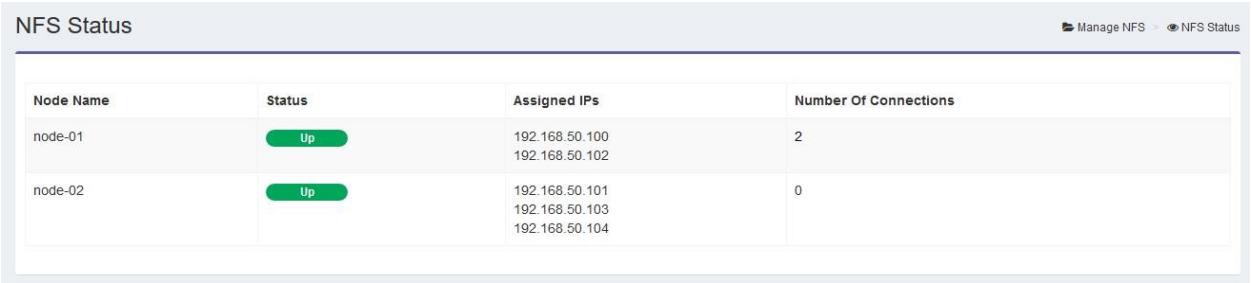


Рисунок 234 – Статус NFS

В системе отображаются следующие столбцы:

- **Имя узла** – имя узла сервера NFS.
- **Статус**. Статус узла: активен, не работает или в льготном режиме, где в льготном режиме означает, что узел не может принимать новые клиентские соединения.
- **Назначенные IP-адреса**. Отображаются IP-адреса, назначенные каждому узлу.
- **Количество подключений** – количество активных клиентских подключений.

3.5.9.4 Просмотр подключений

Доступен просмотр соединений для выбранного серверного узла (Рисунок 235).

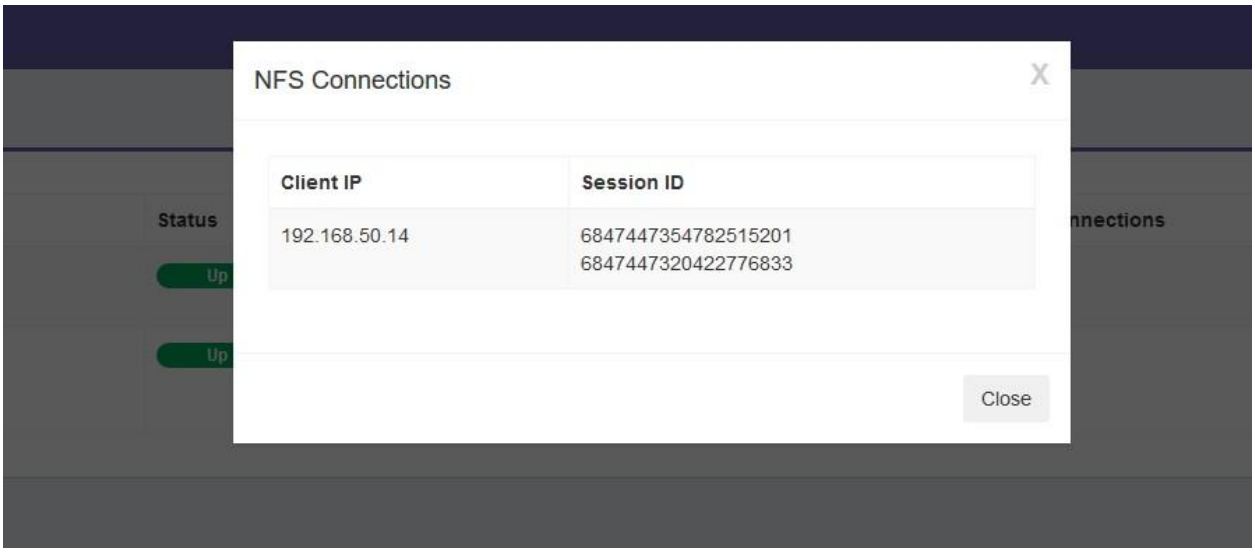


Рисунок 235 – Соединения для выбранного серверного узла

В системе отображаются следующие столбцы для каждого активного соединения:

- **Клиентский IP** – IP-адрес подключенного клиента.
- **Идентификатор сеанса** – идентификатор сеанса подключенного клиента.

3.5.10 Обслуживание

3.5.10.1 Обслуживание кластера С помощью формы обслуживания кластера можно отключить один или несколько параметров обслуживания (Рисунок 236).

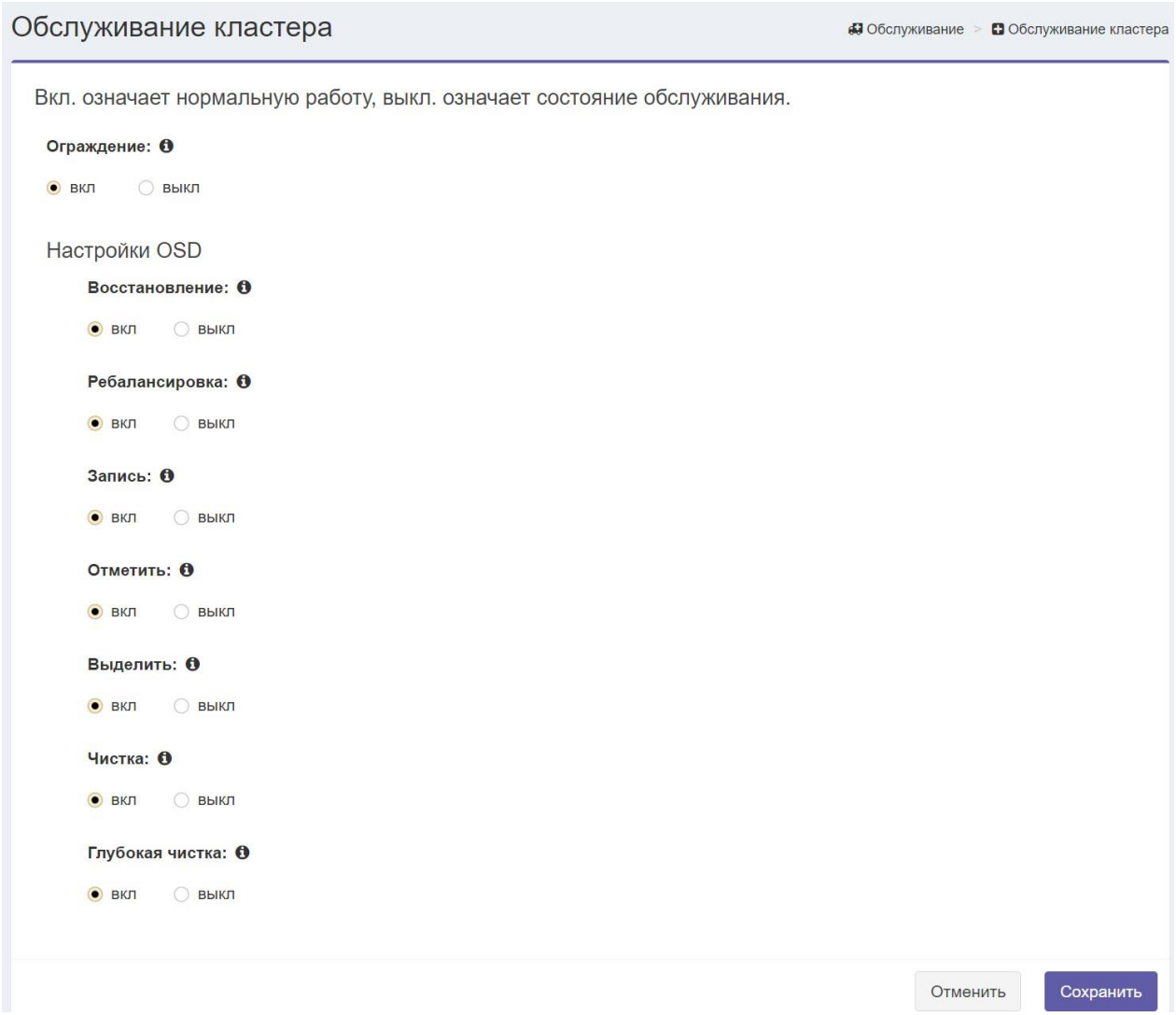


Рисунок 236 – Настройка параметров обслуживания кластера

3.5.11 Управление пользователями

3.5.11.1 Добавление пользователя

Для добавления пользователя используется следующая форма (Рисунок 237).

Рисунок 237 – Форма добавления пользователя

Форма требует следующей информации:

• **Имя**

Имя пользователя

• **Имя пользователя**

Имя пользователя, которое будет использоваться для входа

• **Пароль / подтверждение пароля**

Пароль пользователя и его подтверждение

• **Роль**

Роль пользователя, которая может быть:

«Администратор» позволяет пользователю получить доступ ко всем системным страницам.

«Пользователь» позволяет пользователю контролировать кластер с помощью панели мониторинга.

• **Электронная почта**

Если необходимо, чтобы пользователь получал уведомление по электронной почте, следует ввести адрес электронной почты пользователя и отметить опцию «Получать уведомление».

3.5.11.2 Просмотр списка пользователей

Система позволяет просматривать всех пользователей в системе с помощью страницы списка пользователей (Рисунок 238).

Рисунок 238 - Страница списка пользователей

Действия

Система позволяет выполнять следующие действия для каждого пользователя:

Редактировать - обновлять информацию о пользователе, кроме имени пользователя (Рисунок 239);

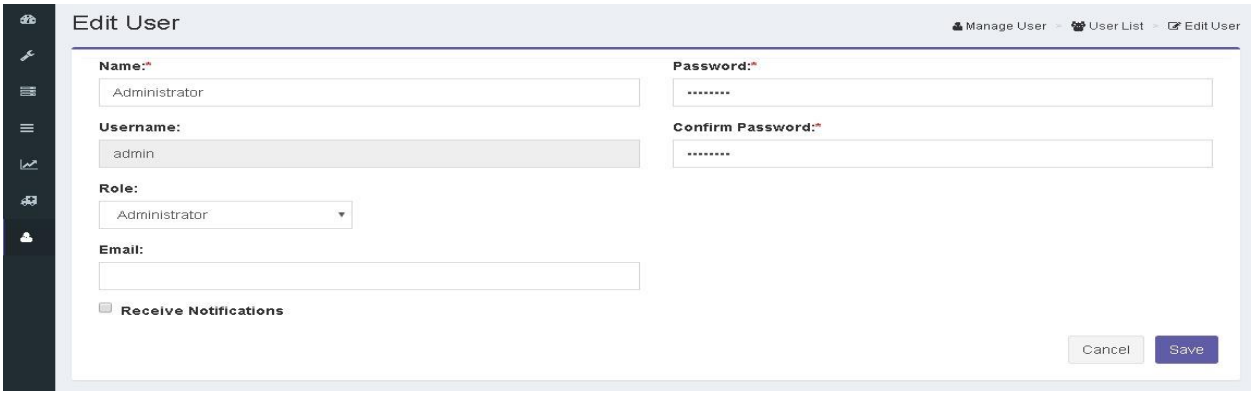


Рисунок 239 – Форма редактирования информации о пользователе

Удалить - удалить любого пользователя, кроме администратора по умолчанию.

3.5.11.3 Изменение пароля пользователя

Система позволяет любому пользователю изменить свой пароль (Рисунок 240).

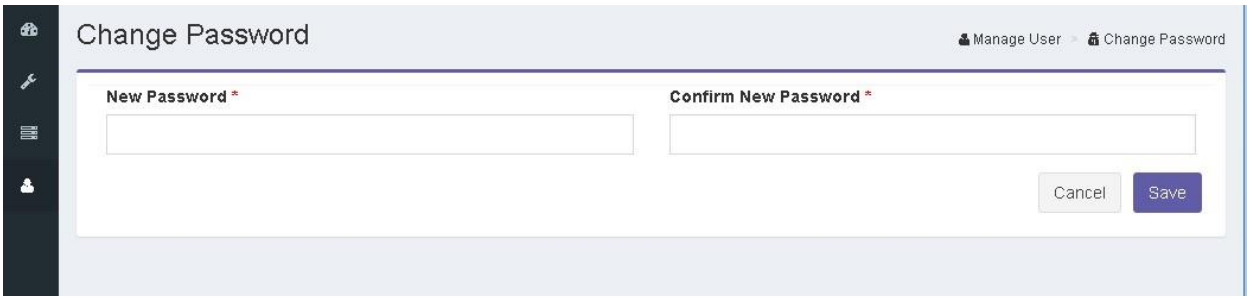


Рисунок 240 – Форма изменения пароля

3.5.12 Настройки дедупликации

Для включения функции дедупликации, перед формированием пула необходимо подготовить физические устройства, которые войдут в состав пула с помощью команды из командной строки set_osd_pool_dedup </dev/xxx /dev/yyy /...> с перечислением всех этих устройств.

3.5.13 Обновление

Убедиться в актуальности ПО поставляемого образца. По необходимости произвести обновление ПО из официальных источников производителя согласно инструкции.

Произвести обновление через графический инсталлятор.

1. Загрузиться с носителя (Рисунок 241):

Рисунок 241

2. Повторить настройки узла. Ввести hostname (Рисунок 242):

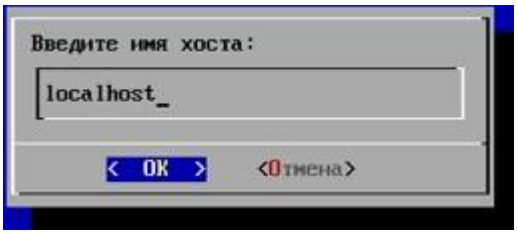


Рисунок 242

3. Выбрать сетевой интерфейс (Рисунок 243):

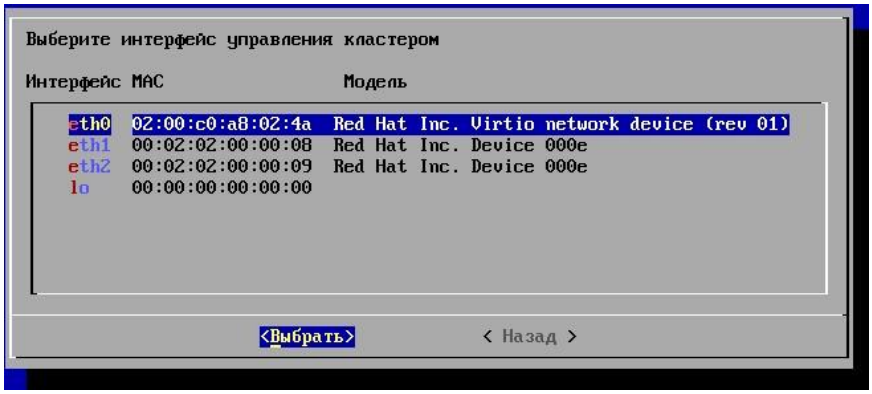


Рисунок 243 4.

Настроить сеть (Рисунок 244):

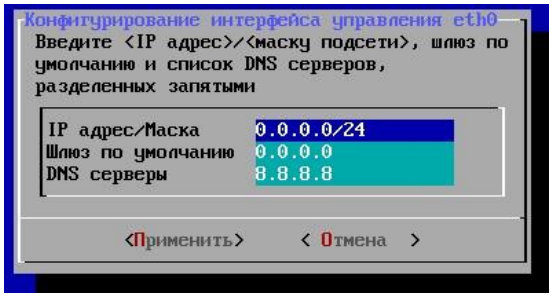


Рисунок 244

5. Выбрать диск для обновления системы (Рисунок 245):

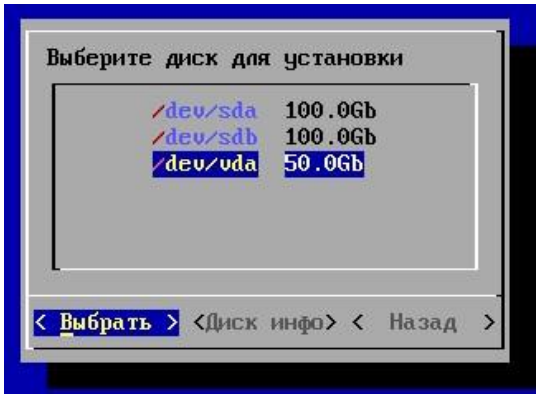


Рисунок 245

6. После обновления выбрать необходимое действие (Рисунок 246):

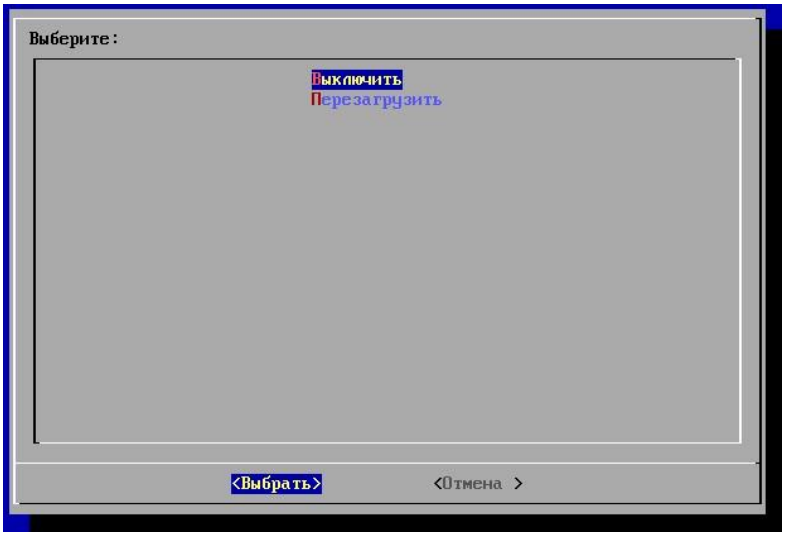


Рисунок 246

3.5.14 Поддержка thin provisioning

Образы блочных устройств СХД «Шторм» поддерживают Thin Provisioning. Они фактически не используют какое-либо физическое хранилище, пока в них не сохранены какие-либо данные.

Однако у них есть максимальная емкость, которая устанавливается с помощью опции --size. Если необходимо увеличить (или уменьшить) максимальный размер образа блочного устройства, необходимо выполнить следующие команды:

rbd resize --size 2048 foo (для увеличения) rbd resize --
size 2048 foo --allow-shrink (для уменьшения).

3.5.15 Замена компонентов схд

Замена компонентов СХД производится в следующем порядке:

1. Отключить одну ноду (Рисунок 247):

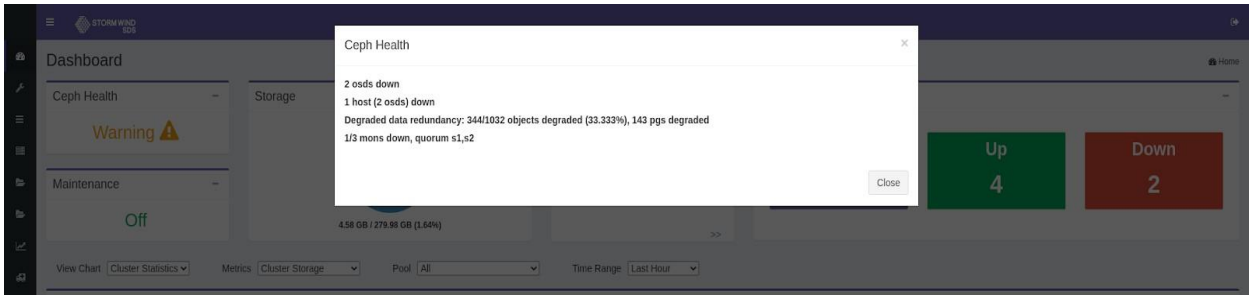


Рисунок 247

2. Посмотреть выключенные OSD (Рисунок 248):

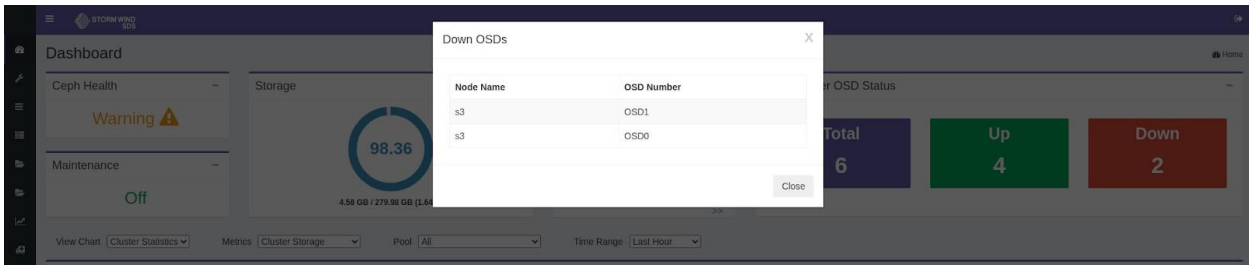


Рисунок 248

3. Заменить один диск на другой (Рисунок 249):

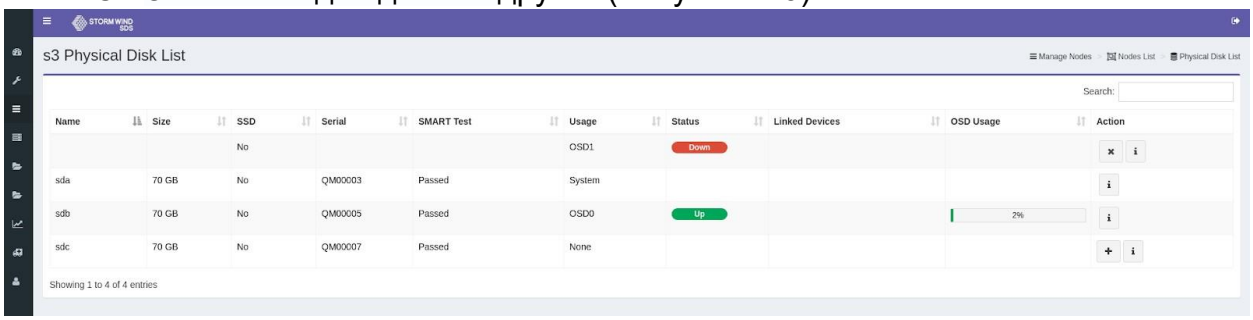


Рисунок 249

4. Активировать новый диск (Рисунок 250):

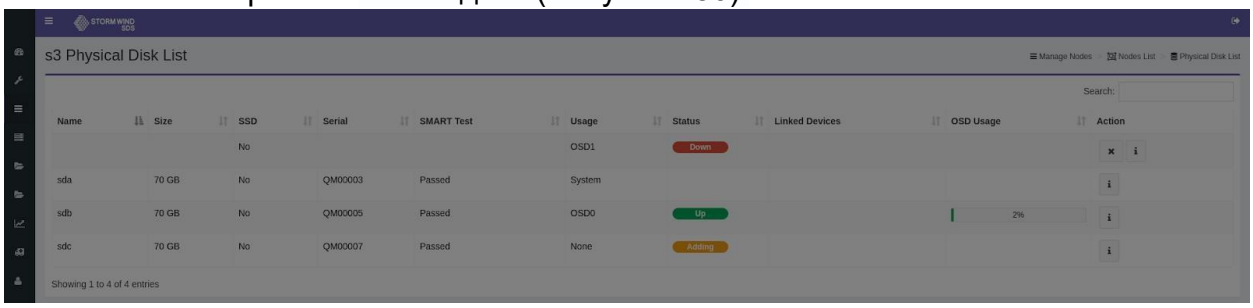


Рисунок 250

5. Убедиться, что после активации статус изменился (Рисунок 251):

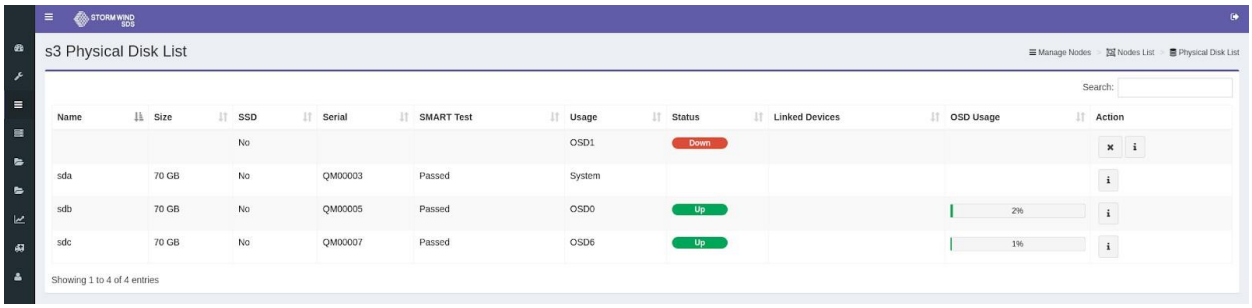


Рисунок 251

3.6 Настройка программы

3.6.1 Установка VDI Server

Перейти в директорию, где находится образ «star.vdi»
Загрузить образ: docker load < star.vdi.0.0.3.tar.bz2

Подписать контейнер: hvs_sign

Посмотреть версию контейнера: docker images (пример: star.vdi:0.0.3)

```
h104 ~ # docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
star.vdi            0.0.3               4a3718de3f68        2 months ago        2.75GB
hcs                 1.0.75              3fe3b4987d96        8 months ago        2.63GB
```

Запустить контейнер:

docker run -d --name=star.vdi -p 2637:2637 --restart=always -v svdi.vol:/svol star.vdi:0.0.3

3.6.2 Установка и настройки UDS Actor

UDS Actor устанавливается в ОС Windows или Linux (золотой образ) для использования при развертывании виртуальных рабочих столов. Также необходимо, чтобы серверы приложений RDS имели установленный UDS Actor, чтобы иметь возможность представлять пользователям виртуальные сессии приложений.

Для установки UDS Actor необходимо предварительно загрузить из брокера VDI подходящий Actor для каждой платформы (Windows, Linux и vApps).

Для этого следует подключиться к брокеру VDI через веб-браузер и использовать учетные данные пользователя с правами администратора для доступа к загрузкам (рисунки Рисунок 252, Рисунок 253).

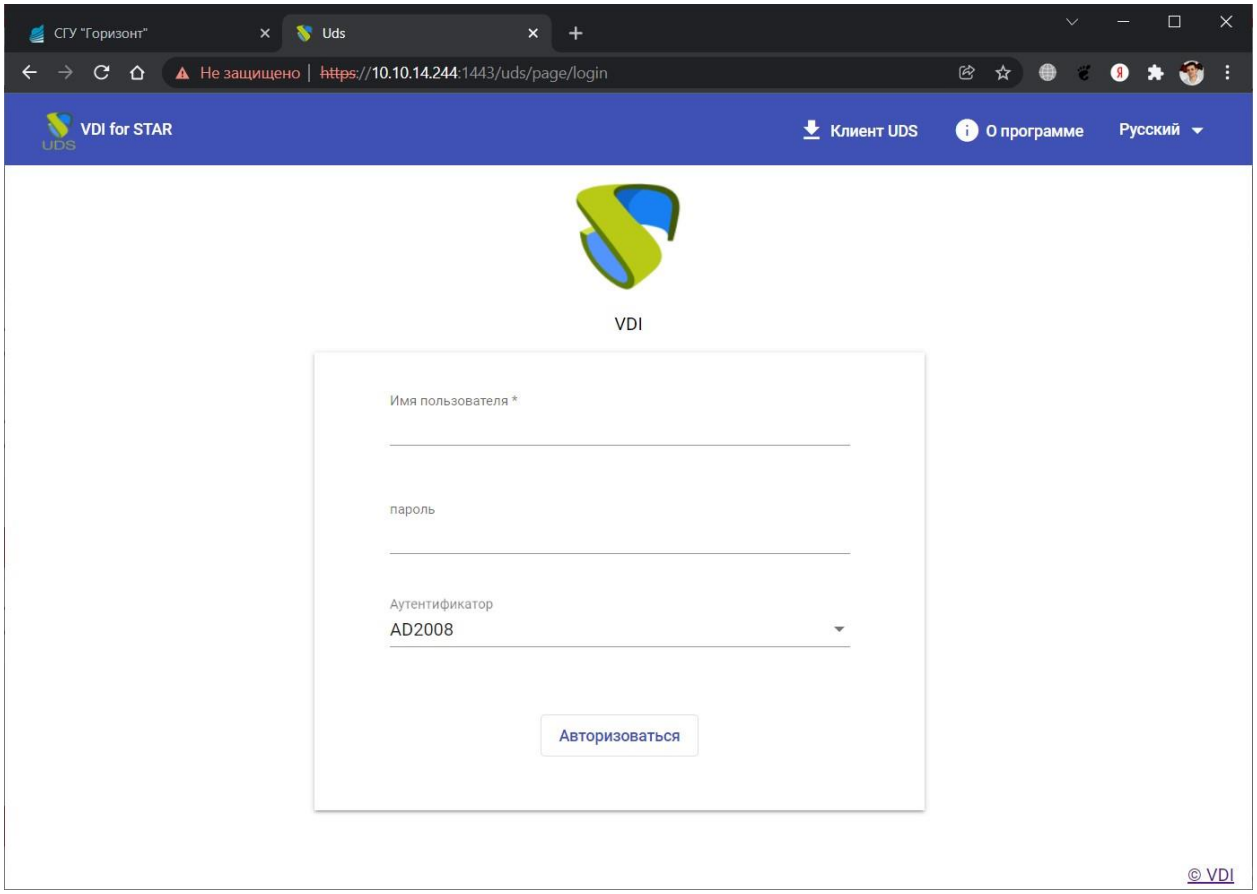


Рисунок 252

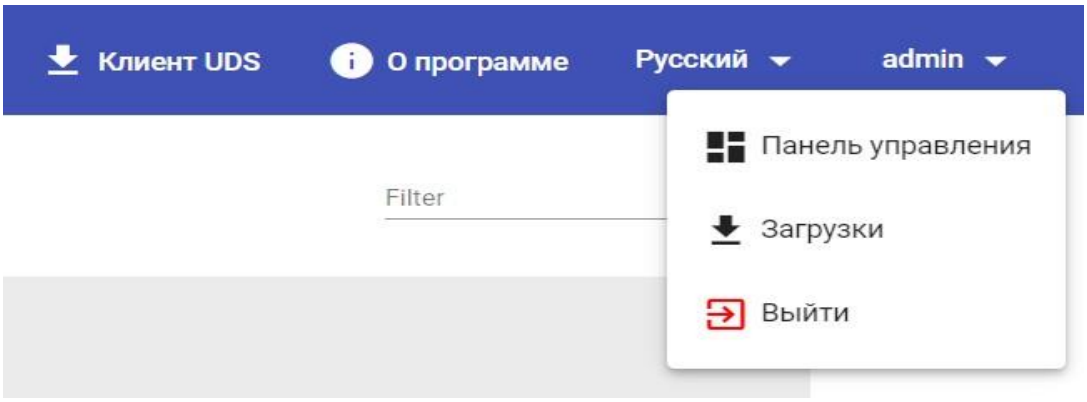


Рисунок 253

Выбрать Actor соответствующей операционной системы и службы, установленной в базовом шаблоне или сервере приложений, на котором будут развернуты службы рабочего стола (Рисунок 254):

▪ udsactor_3.0.0_all.deb: UDS Actor для шаблона машин Linux (золотой образ) на основе дистрибутивов Debian, таких как: Ubuntu, Xubuntu и т.д.

▪ udsactor-3.0.0-1.noarch.rpm: UDS Actor для шаблона машин Linux (золотой образ) на основе дистрибутивов Red Hat, таких как: CentOS, Fedora и т.д.

▪ udsactor-opensuse-3.0.0-1.noarch.rpm: UDS Actor для шаблона машин Linux (золотой образ) на основе дистрибутивов на базе Suse, таких как: OpenSuse и т.д.

▪ udsactor-2.2.0_legacy.deb: UDS Actor версии 2.2 для шаблона машин Linux (золотой образ) на основе дистрибутивов Debian, таких как: Ubuntu, xUbuntu и т.д.

▪ udsactor-unmanaged_3.0.0_all.deb: UDS Actor для управления сеансами машин на основе Debian от поставщика услуг «Поставщик статических IPмашин», таких как: Ubuntu, xUbuntu и т.д.

▪ RDSActorSetup-3.0.0.exe: UDS Actor для серверов приложений Windows Server 2012 R2, 2016, 2019 или 2022 с настроенной ролью RDS.

▪ UDSActorUnmanagedSetup-3.0.0.exe: UDS Actor для управления сеансами компьютеров Windows от поставщика услуг «Поставщик статических IPмашин».

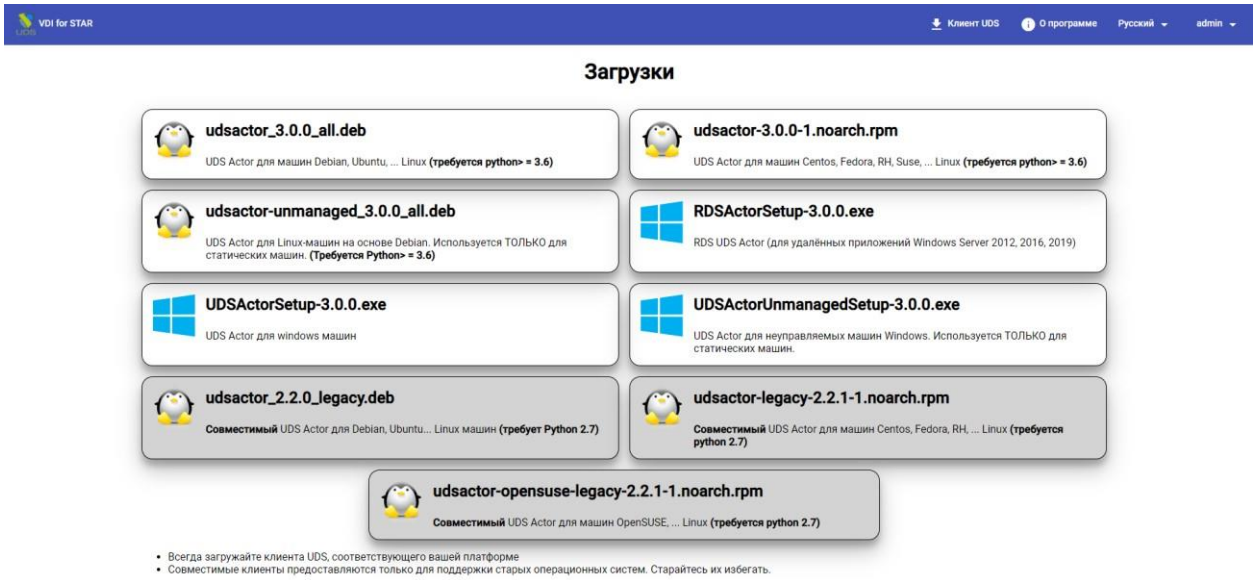


Рисунок 254

3.6.2.1 Автономные виртуальные рабочие столы Windows

Для управления жизненным циклом виртуальных машин Windows, самостоятельно создаваемых VDI, необходимо, чтобы на шаблонной машине, на которой они будут основаны, был установлен UDS Actor: UDSActorSetup-3.0.0.exe.

Примечание: перед установкой UDS Actor необходимо иметь IP-адрес или имя сервера VDI, учетные данные пользователя с административными разрешениями в среде VDI и хотя бы один аутентификатор, зарегистрированный в системе.

После загрузки UDS Actor для Windows и переноса его на компьютер шаблона запустить его, чтобы продолжить установку.

Выбрать язык программы установки и нажать кнопку «ОК» (Рисунок 255).

Рисунок 255

Указать путь установки элемента UDS (Рисунок 256).

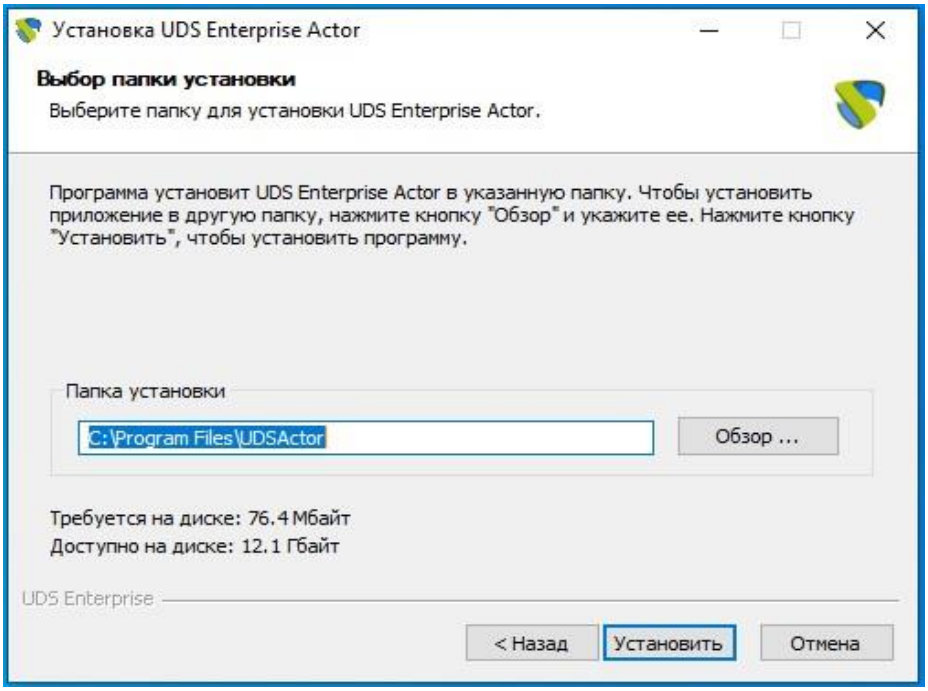


Рисунок 256

После завершения установки перейти к конфигурированию элемента UDS (Рисунок 257).

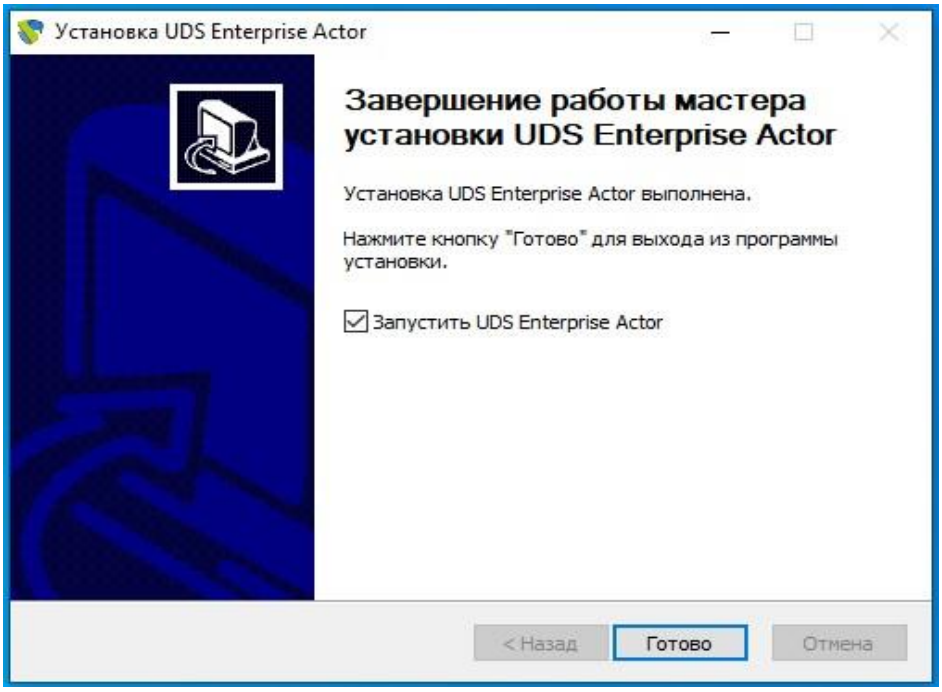


Рисунок 257

На вкладке UDS Server нужно зарегистрировать Actor в экземпляре VDI, указав следующие параметры (Рисунок 258):

SSL Validation: игнорировать сертификат\верификационный сертификат UDS Server: имя или IP-адрес VDI-сервера и порт.

Authenticator: Аутендификатор, к которому принадлежит указанный пользователь-администратор для регистрации UDS Actor.

Для отображения различных аутентификаторов связь с VDI-сервером должна быть успешной. В администрировании VDI должен быть зарегистрирован хотя бы один (аутентификатор «Администрирование» соответствует суперпользователю, созданному в мастере настройки сервера VDI).

Username: Имя пользователя с полномочиями администратора.

Password: Пароль пользователя администратора.

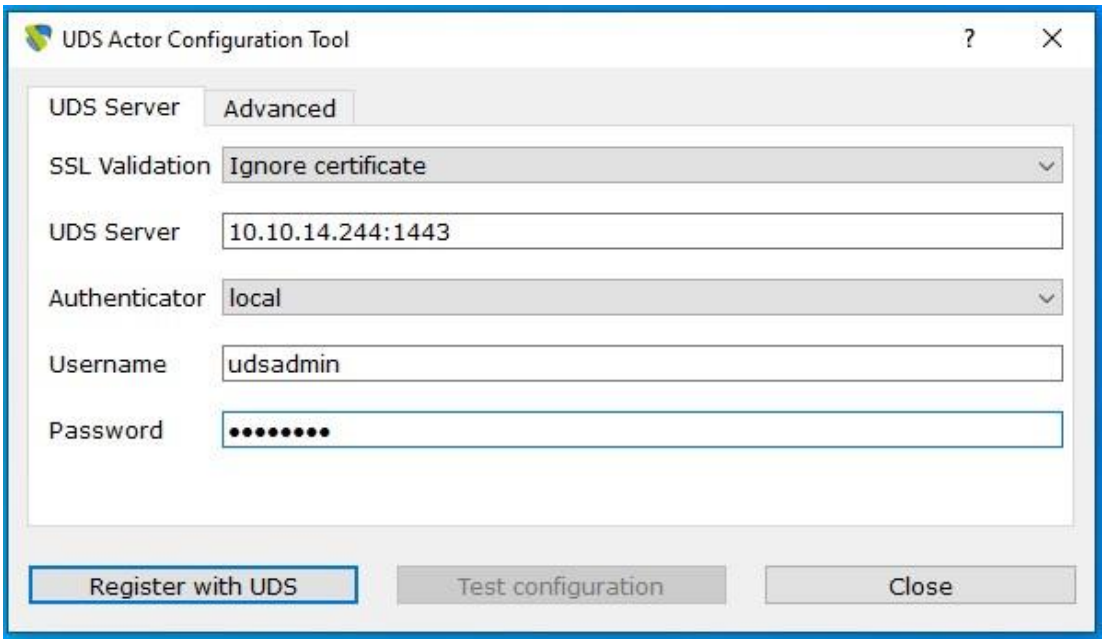


Рисунок 258

После ввода этих данных нажать кнопку «Register with UDS» (Регистрация в VDI) (Рисунок 259).

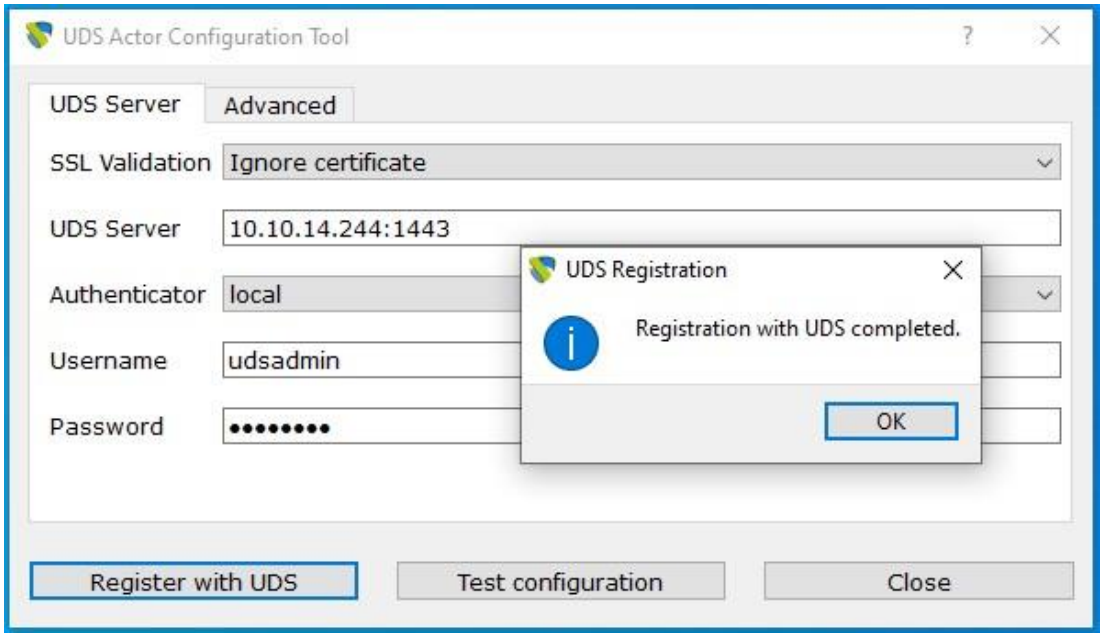


Рисунок 259

Можно выполнить тест, нажав кнопку «Test configuration», для проверки правильности подключения к серверу VDI (Рисунок 260).

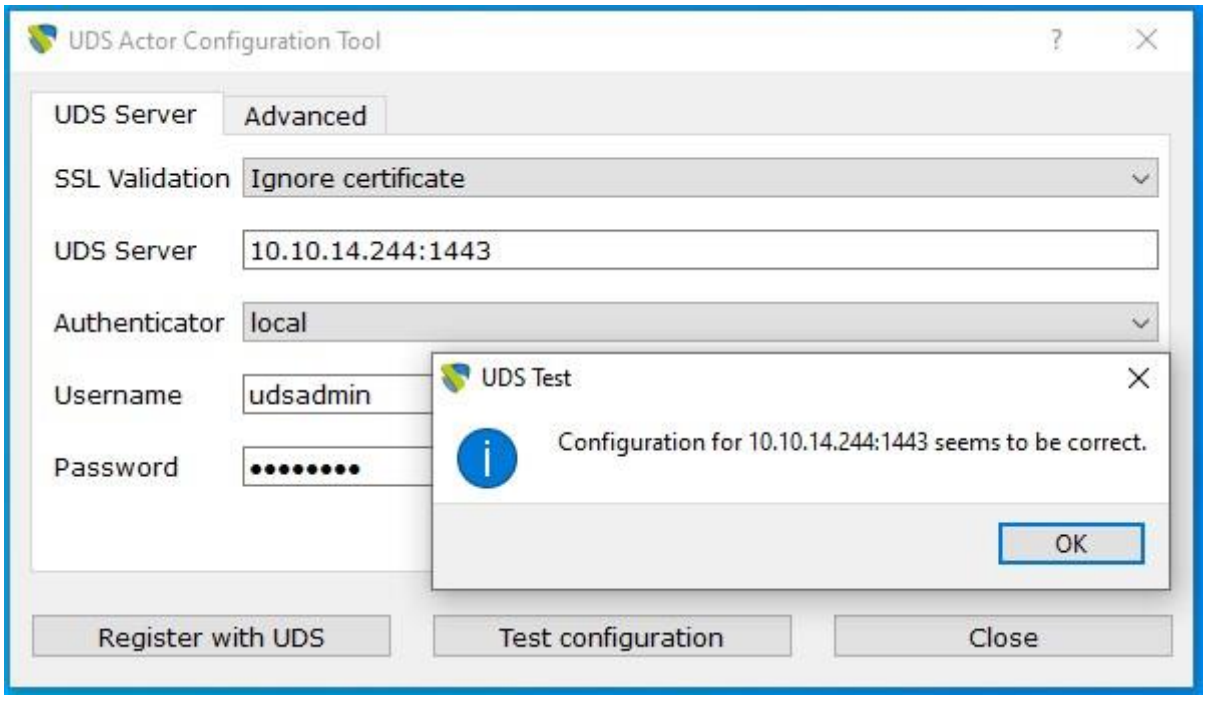


Рисунок 260

На вкладке «Advanced» можно указать следующие дополнительные параметры (Рисунок 261).

Preconnect: запуск сценария непосредственно перед тем, как разрешить пользователю подключение к виртуальному рабочему столу.

VDI автоматически передает следующие параметры, которые могут использоваться в сценарии: имя пользователя, протокол (rdp, nx, pcoip...), IP (IP, распознанный на клиенте (SRC IP)), имя хоста (SRC Host).

Runonce: сценарий, который выполняется только один раз и до того, как UDS Actor применит свои параметры. После его выполнения он удаляется из конфигурации. Параметры могут передаваться непосредственно в него.

Выполняемый сценарий должен быть завершен перезапуском виртуального рабочего стола. В противном случае рабочий стол никогда не будет применять параметры Acter, препятствуя переходу в состояние «Действительно» при администрировании VDI.

Postconfig: сценарий, который запускается после завершения настройки VDI Actor. Параметры могут передаваться непосредственно в него.

Сценарий запускается только один раз, но в отличие от режима «Runonce» перезапустить виртуальный рабочий стол не требуется. Этот сценарий полезен для добавления некоторых «собственных» элементов в конфигурацию, созданную UDS Actor, таких как копирование файлов из локальной сети, выполнение конфигураций и т.д.

Log Level: типы журналов, которые должны отображаться в файлах журнала UDS Actor. Эти файлы журнала (udsactor.log) будут располагаться в

путях: %temp% (путь временных файлов пользователя) и C:\Windows\Temp (путь временных файлов системы).

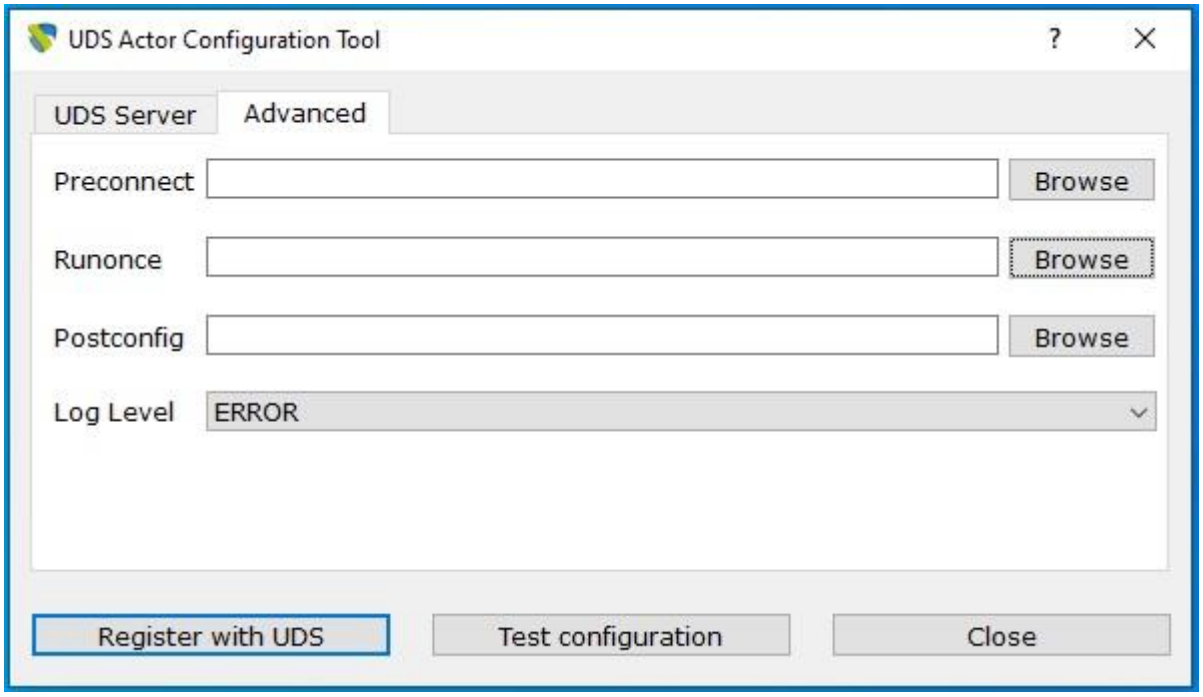


Рисунок 261

Очень важно отметить, что для применения значений вкладки «Advanced» всегда необходимо выполнить процесс регистрации позже, так как если вы добавляете какой-либо сценарий или изменяете уровень журнала, и вы не зарегистрировали Actor снова, то они не будут применены.

После установки и настройки UDS Actor шаблонная машина теперь может быть отключена и будет доступна для использования VDI для самогенерированных виртуальных рабочих столов.

Примечание: помимо установки UDS Actor, необходимо включить протокол подключения для подключения к создаваемым рабочим столам (например, включить удаленный рабочий стол, установить клиент PCoIP и т.д.).

3.6.2.2 Статические Windows машины

Для управления пользовательскими сеансами (вход в систему и выход из системы) компьютера, настроенного в рамках поставщика «Поставщик статистических IP машин», необходимо, чтобы на нем был установлен UDS Actor: UDSActorUnmanagedSetup-3.0.0.exe.

Если на этих машинах не установлен UDS Actor и они являются частью службы типа «Статистический множественный IP-адрес», VDI не сможет управлять выходом пользователя из системы и, следовательно, не сможет освободить его, чтобы сделать его доступным другому пользователю (Рисунок 262).

Рисунок 262

Примечание: перед установкой UDS Actor необходимо зарегистрировать IPадрес или имя VDI-сервера и ключ «Ключ услуги» в службе типа «Статистический множественный IP-адрес» в «Поставщик статистических IP машин».

Установка UDSActorUnmanagedSetup-3.0.0 осуществляется следующим образом. Выбрать язык программы установки (Рисунок 263).

Рисунок 263

Указать путь установки UDS Actor и нажать кнопку «Установить» (Рисунок 264).

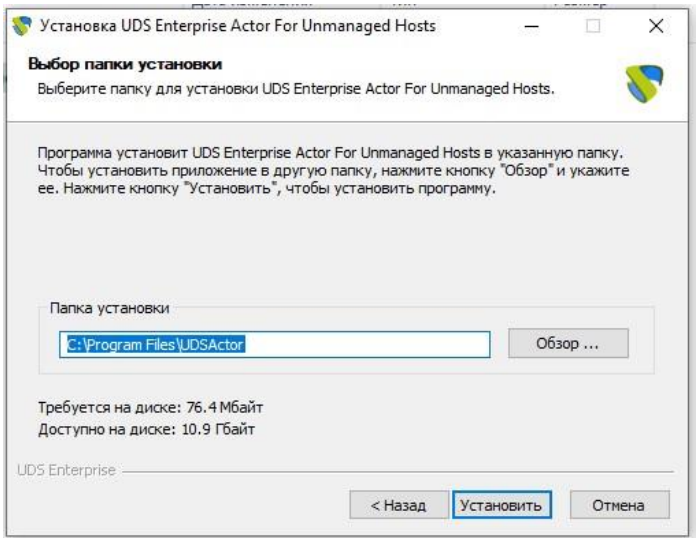


Рисунок 264

После завершения установки перейти к регистрации Actor на сервере UDS, указав следующие параметры:

SSL Validation: игнорировать сертификат\верификационный сертификат.

UDS Server: имя или IP-адрес UDS-сервера.

Service Token: код, созданный в администрировании UDS, в типе «Статистический множественный IP-адрес» в рамках поставщика «Поставщик статистических IP машин»

Log Level: типы журналов, которые должны отображаться в файлах журнала UDS Actor. Эти файлы журнала (udsactor.log) будут располагаться по путям: %temp% (путь временных файлов пользователя) и C:\Windows\Temp (путь временных файлов O.S.)

После ввода этих данных нажать кнопку «Save Configuration» (сохранить конфигурацию) (Рисунок 265).

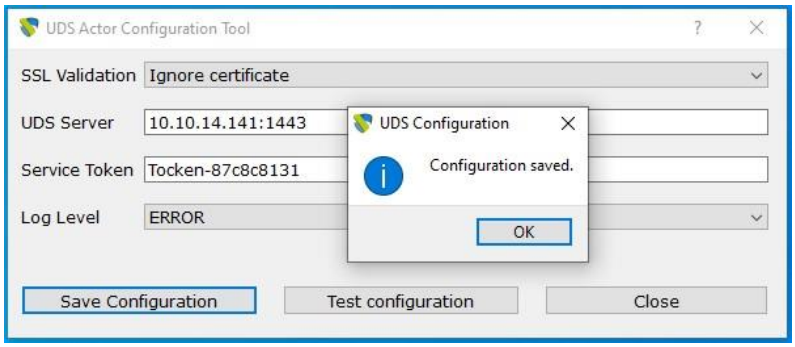


Рисунок 265

Необходимо выполнить конфигурационный тест для проверки правильности указанных данных и наличия подключения к серверу VDI (Рисунок 266).

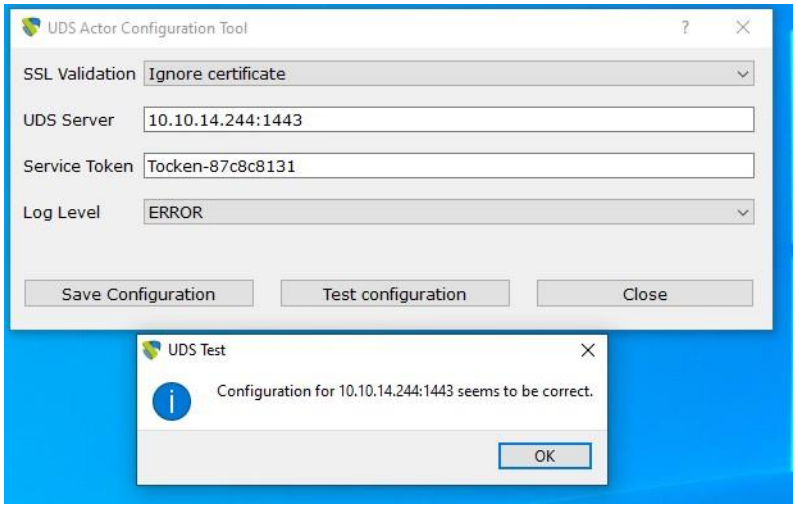


Рисунок 266

После завершения установки и конфигурирования элемента VDI машина будет доступна для назначения VDI и управления пользовательскими сеансами.

Примечание: в дополнение к установке UDS Actor, необходимо включить протокол подключения для подключения к сгенерированным рабочим столам (например, включить удаленный модуль записи и т.д.).

4.6.2.3 Создание виртуальных Linux машин

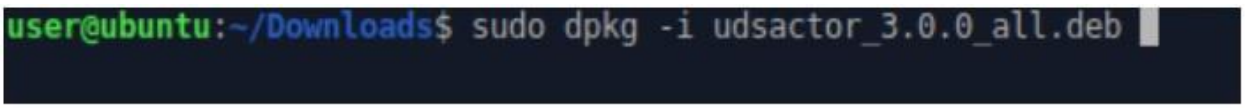
Для управления жизненным циклом виртуальных рабочих столов Linux, самостоятельно генерируемых VDI, на шаблонной машине, на которой они будут основаны, должен быть установлен UDS Actor для различных дистрибутивов Linux:

- Дистрибутивы на основе Debian: udsactor_3.0.0_all.deb
- Дистрибутивы на основе Red Hat: udsactor-3.0.0-1.noarch.rpm
- Дистрибутивы на основе Suse: udsactor-opensuse-3.0.0-1.noarch.rpm

Примечание: перед установкой UDS Actor необходимо иметь IP-адрес или имя сервера VDI, учетные данные пользователя с правами администратора в среде VDI и хотя бы один аутентификатор, зарегистрированный в системе.

Как только UDS Actor для выбранного дистрибутива Linux будет загружен и перенесен на машину-шаблон, выполнить его, чтобы продолжить установку.

Настоятельно рекомендуется выполнять установку UDS Actor через командную строку:



Если получена ошибка из-за отсутствия зависимостей, можно воспользоваться командой исправления зависимостей: “sudo apt-get install f” (Рисунок 267).

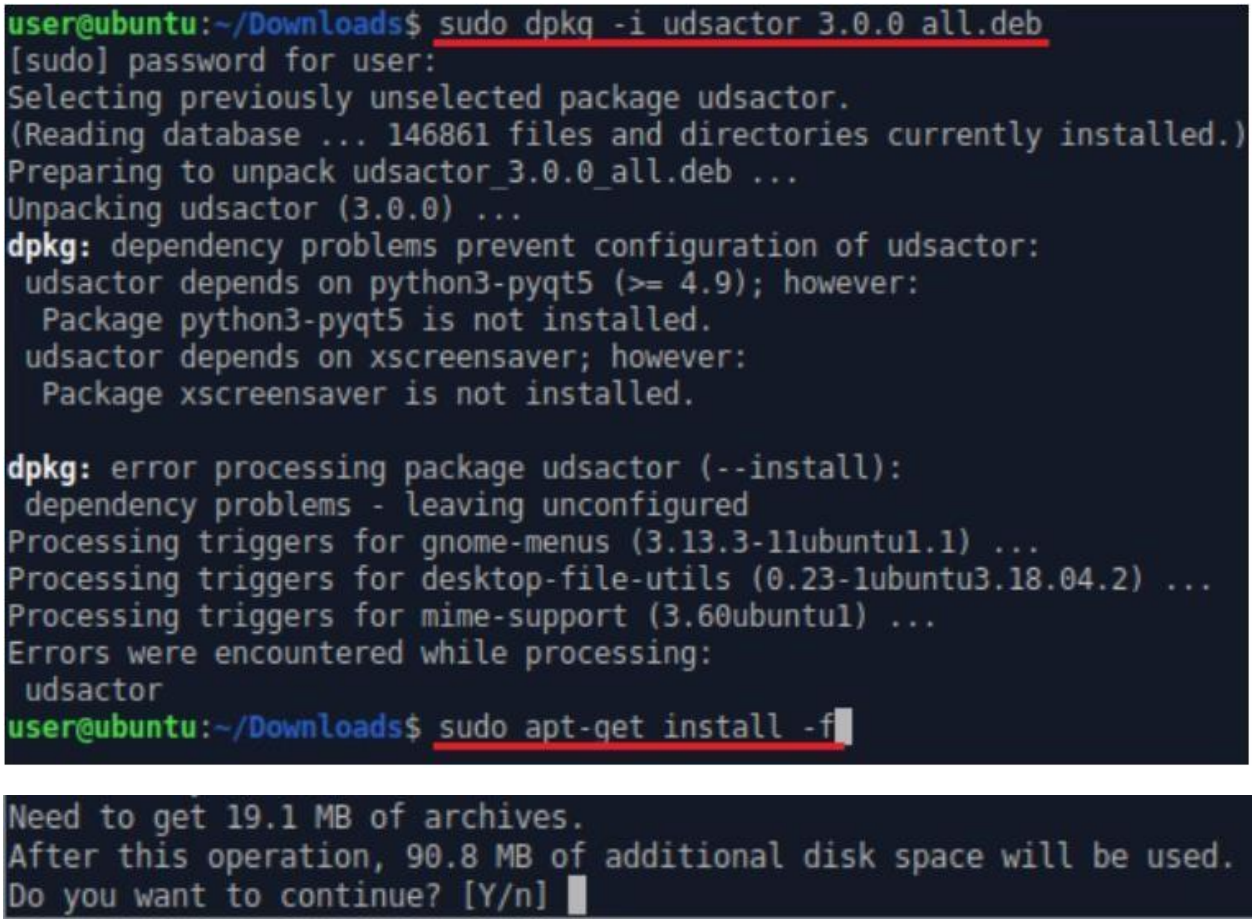


Рисунок 267

После установки необходимых зависимостей запустить конфигурацию UDS Actor. На вкладке UDS Server можно зарегистрировать Actor, указав следующие параметры (Рисунок 268).

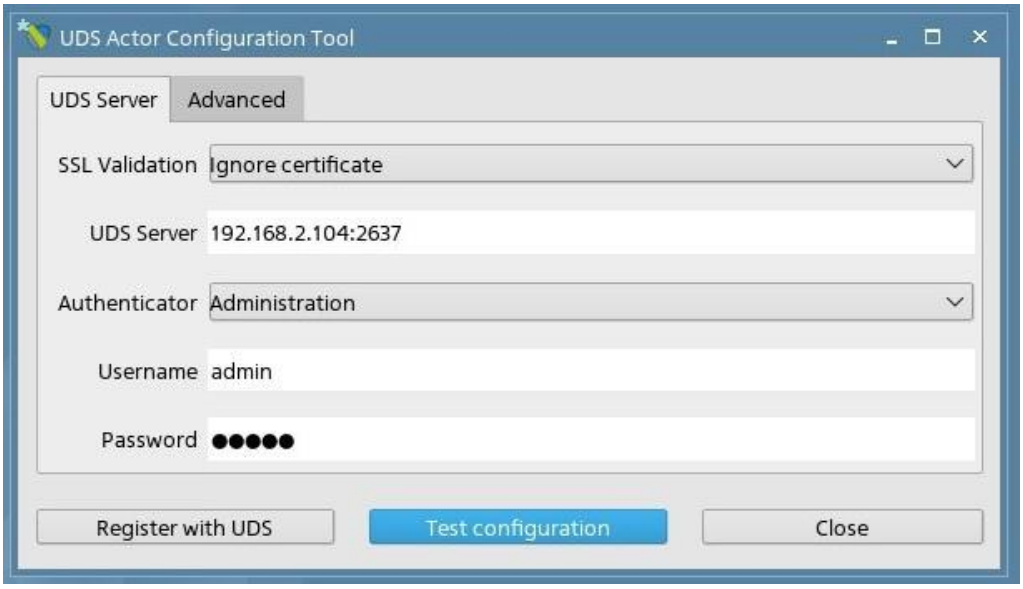


Рисунок 268

SSL Validation: игнорировать сертификат\верификационный сертификат.

UDS Server: имя или IP-адрес VDI сервера и порт (по умолчанию: 2637).

Authenticator: Аутендификатор, к которому принадлежит указанный пользователь-администратор для регистрации участника VDI.

Для отображения различных аутентификаторов связь с VDI -сервером должна быть успешной. В администрировании VDI должен быть зарегистрирован хотя бы один (аутентификатор «Администрирование» соответствует суперпользователю, созданному в мастере настройки сервера VDI).

Username: Имя пользователя с разрешением администрации в окружающей среде VDI.

Password: Пароль администратора.

После указания этих данных нажать кнопку «Register with UDS» (Рисунок 269).

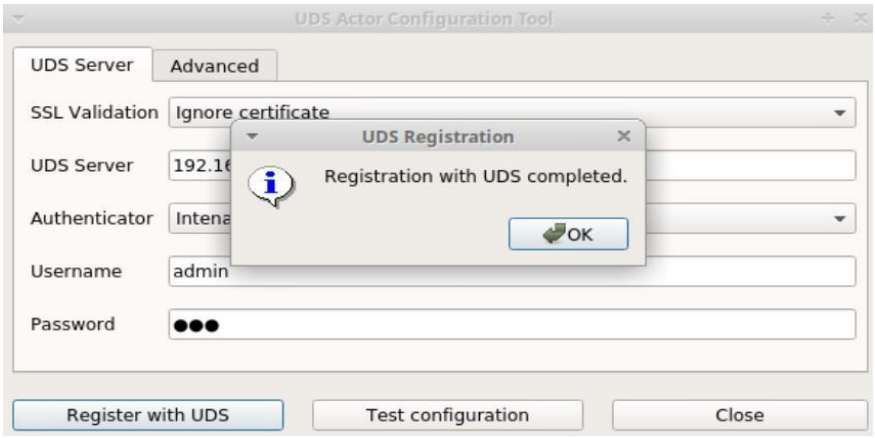


Рисунок 269

Можно выполнить тест, нажав кнопку «Test configuration», чтобы проверить правильность подключения к серверу VDI (Рисунок 270).

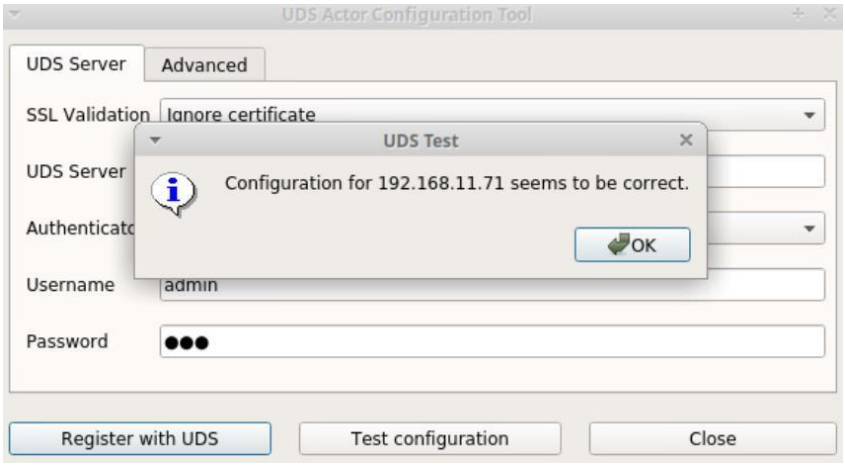


Рисунок 270

На вкладке «Advanced» можно указать следующие дополнительные параметры (Рисунок 271).

Preconnect: Сценарий должен быть запущен непосредственно перед тем, как разрешить пользователю подключиться к виртуальному рабочему столу.

UDS автоматически передает следующие параметры, которые могут использоваться в сценарии: имя пользователя, протокол (rdp, nx, pcoip...), IP (IP, распознанный на клиенте (SRC IP)), имя хоста (SRC Host).

Runonce: Сценарий, который выполняется только один раз и до того, как исполнитель UDS применит свои параметры.

После выполнения он удаляется из конфигурации. Параметры могут передаваться непосредственно в него. Выполняемый сценарий должен быть завершен перезапуском виртуального рабочего стола. В противном случае рабочий стол никогда не будет применять параметры актера, что не позволит ему перейти в состояние «Действительно» при администрировании UDS.

Postconfig: Сценарий, который выполняется после того, как UDS Actor закончит настройку. Параметры могут передаваться непосредственно в него.

Сценарий запускается только один раз, но в отличие от режима «Runonce» ему не нужно перезагружать виртуальный рабочий стол. Этот сценарий полезен для добавления некоторого «собственного» элемента в конфигурацию, созданную UDS Actor, например, копирование файлов из локальной сети, выполнение конфигураций и т.д.

Log Level: типы журналов, которые должны отображаться в файлах журнала

UDS Actor. Эти файлы журнала (udsactor.log) будут расположены по пути :/var/log/

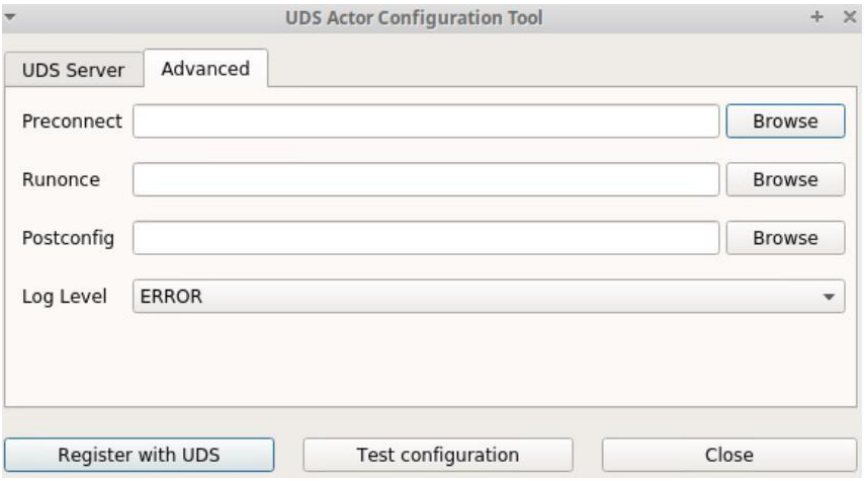


Рисунок 271

Очень важно отметить, что для применения значений закладки «Advanced» всегда необходимо будет выполнить процесс регистрации позже. Если добавлен какой-либо сценарий или изменен уровень журнала, и не зарегистрирован Actor снова, они не будут применены.

После установки и настройки UDS Actor на шаблонной машине (золотой образ) теперь может быть отключена и будет доступна для использования UDS для самостоятельного создания виртуальных рабочих столов.

Примечание: в дополнение к установке UDS Actor, необходимо включить протокол подключения для подключения к сгенерированным рабочим столам (например, установить и включить XRDP, X2Go Server и т.д.).

3.6.2.4 Статические настольные ПК Linux

Для управления пользовательскими сеансами (вход в систему и выход из системы) компьютера, настроенного в рамках поставщика «Поставщик

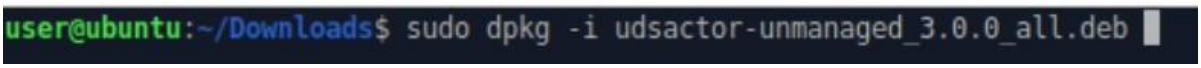
статистических IP машин», необходимо, чтобы на нем был установлен UDS Actor: udsactor-unmanaged_3.0.0_all.deb.

Если на этих машинах не установлен компонент UDS, и они являются частью службы типа «Статистический множественный IP-адрес», UDS не сможет управлять выходом пользователя из системы и, следовательно, не сможет освободить его, чтобы сделать его доступным другому пользователю.

Примечание: перед установкой UDS Actor необходимо зарегистрировать IPадрес или имя сервера UDS и ключ «Ключ услуги» в службе типа «Статистический множественный IP-адрес» в поставщике услуг «Поставщик статистических IP машин».

После загрузки UDS Actor for Linux O.S. и передачи его на машину, к которой необходимо подключить пользователей (физических или виртуальных), его следует запустить, чтобы продолжить его установку.

Настоятельно рекомендуется выполнять такое выполнение UDS Actor через консоль:



Если получена ошибка из-за отсутствия зависимостей, можно воспользоваться командой исправления зависимостей: “sudo apt-get install f” (Рисунок 272).

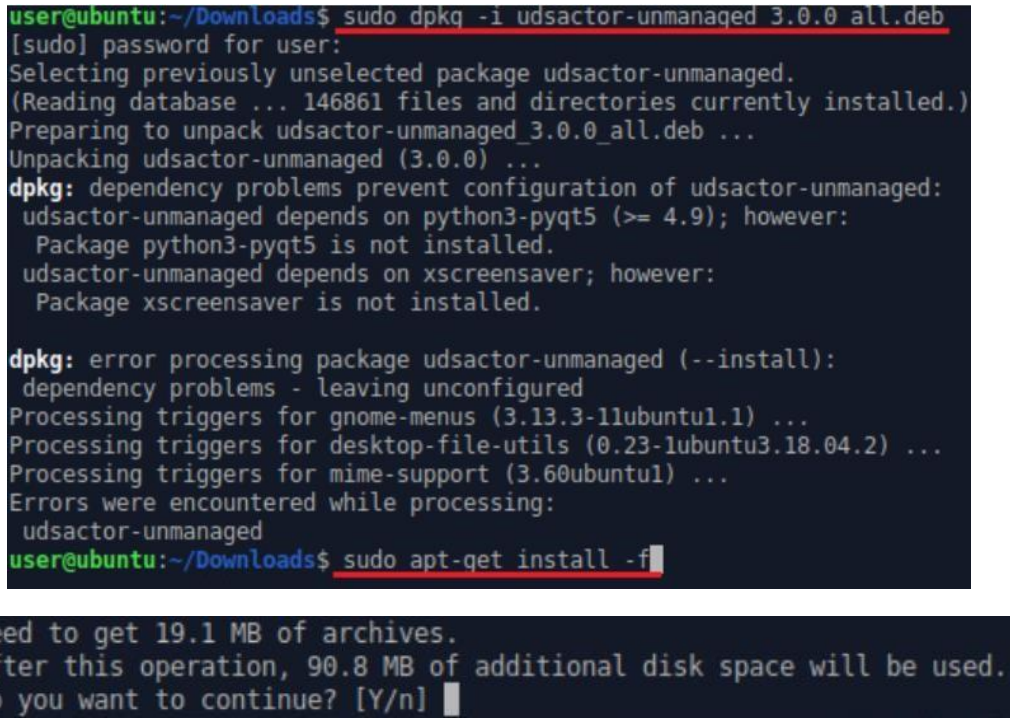


Рисунок 272

После установки необходимых зависимостей будет выполнена конфигурация UDS Actor, следует указать следующие параметры (Рисунок 273).

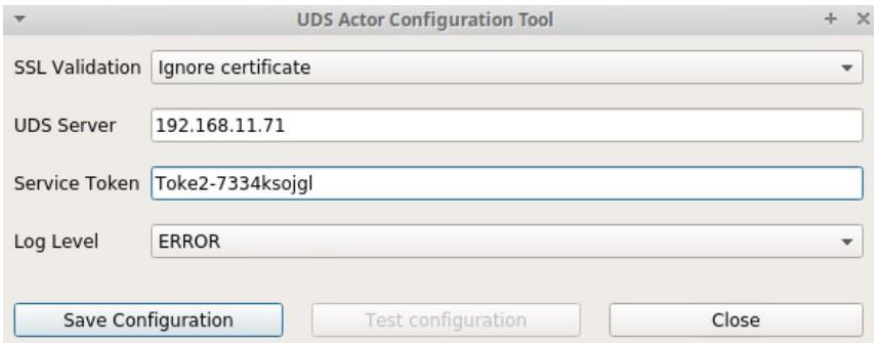


Рисунок 273

SSL Validation: игнорировать сертификат\верификационный сертификат.

UDS Server: имя или IP-адрес UDS-сервера.

Service Token: код, созданный в администрировании UDS, в типе службы "Static IP Machines Provider" в рамках поставщика услуг" Поставщик статических IP-машин ".

Log Level: типы журналов, которые должны отображаться в файлах журнала

UDS Actor. Эти файлы журнала (udsactor.log) будет располагаться по пути

:/var/log/

После ввода этих данных нажать кнопку «Save Configuration» (сохранить конфигурацию) (Рисунок 274).

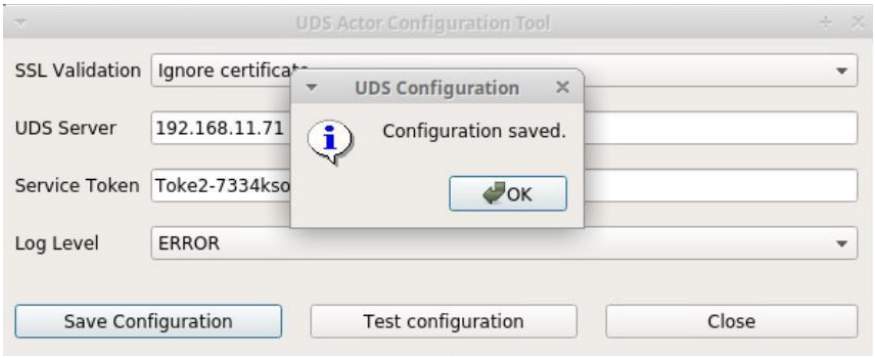


Рисунок 274

Необходимо выполнить конфигурационный тест для проверки правильности указанных данных и наличия подключения к серверу UDS (Рисунок 275).

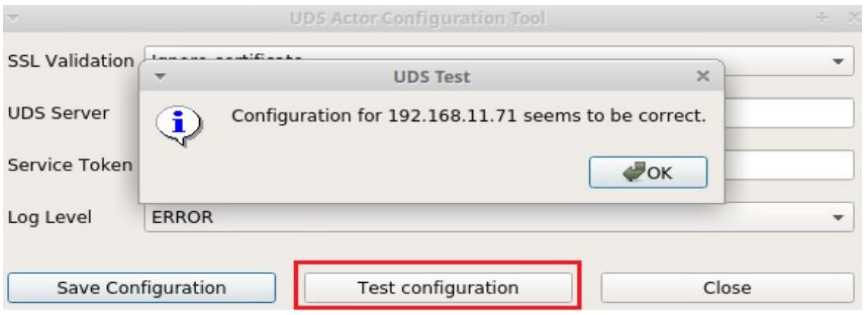


Рисунок 275

После завершения установки и конфигурирования элемента UDS машина будет доступна для назначения UDS и управления пользовательскими сеансами.

Примечание: в дополнение к установке UDS Actor необходимо включить протокол подключения для подключения к сгенерированным рабочим столам (например, установить и включить XRDP).

3.6.2.5 Виртуализация приложений Windows с помощью VDI

Должны быть выполнены следующие требования:

Обновлена ОС Windows Server 2012 R2, 2016,2019 или 2022 (установлена и настроена).

Иметь IP брокера, а также администратора его пользователя.

Сервер должен иметь фиксированный IP-адрес.

Сервер должен быть частью домена.

Перед установкой и настройкой RDS необходимо установить UDS Actor.

На странице загрузки выбрать и загрузить Actor для серверов RDS (RDS UDS Actor) (Рисунок 276).

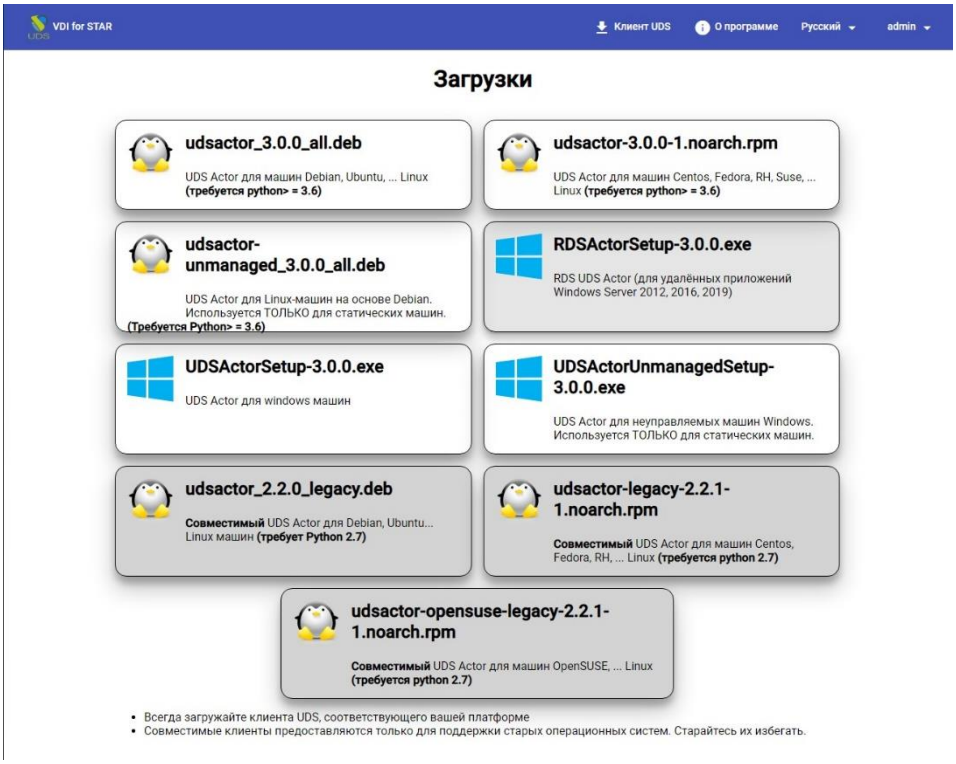


Рисунок 276

Он будет установлен на сервере Windows (Рисунок 277).

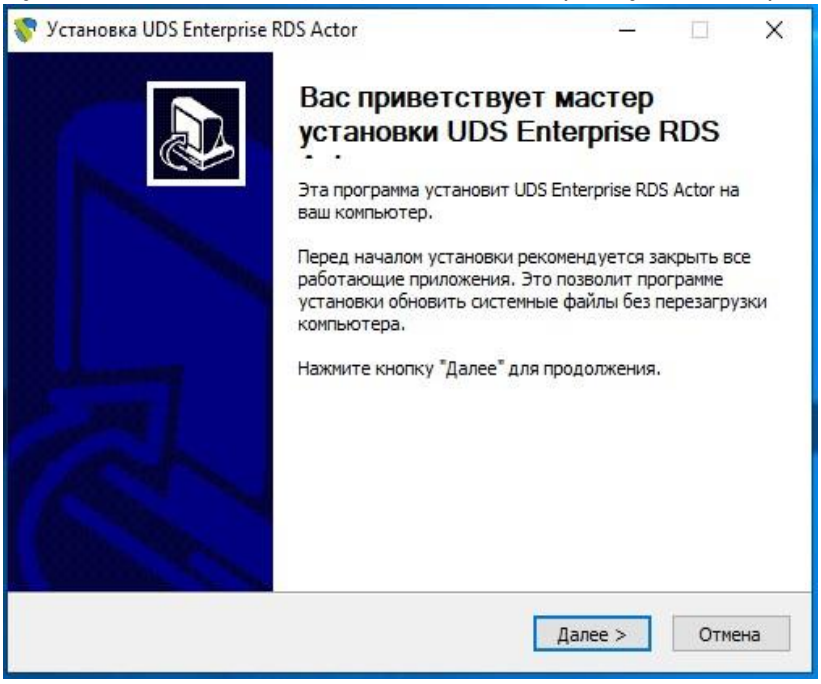


Рисунок 277

Необходимо принять Лицензионное соглашение (Рисунок 278).

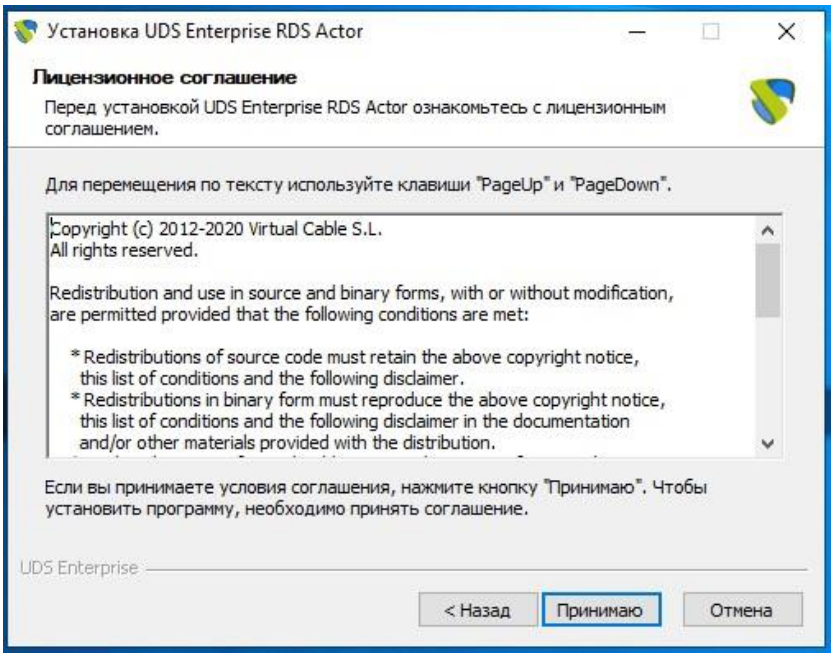


Рисунок 278

Выбрать место установки (Рисунок 279).

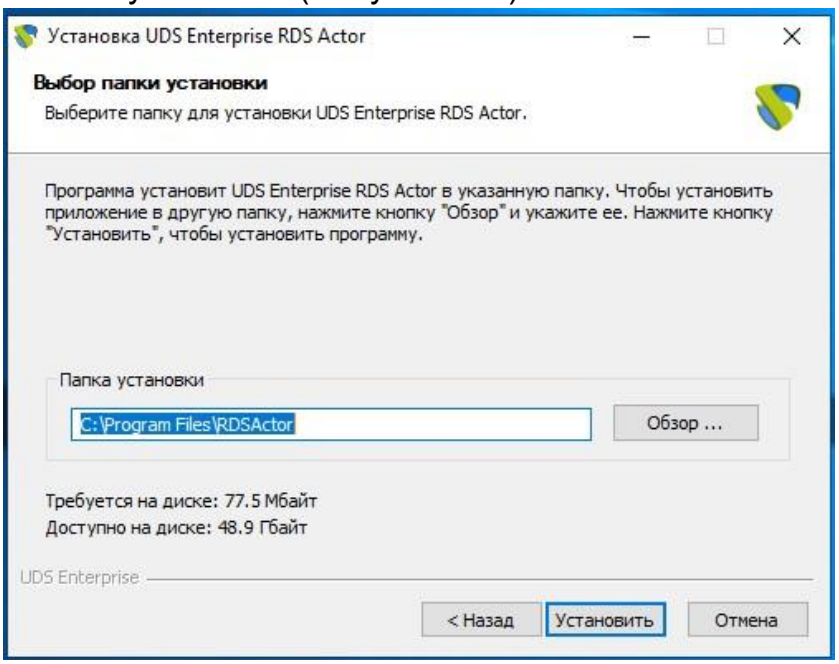


Рисунок 279

После завершения установки запустить UDS Actor (Рисунок 280).

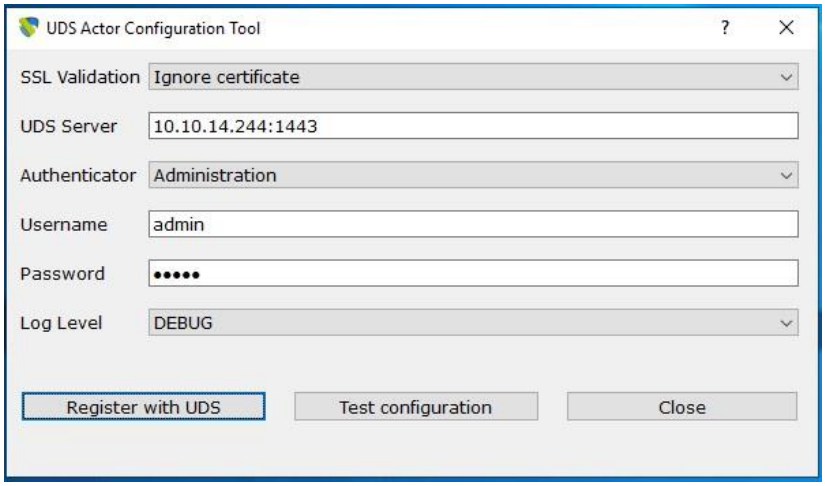


Рисунок 280

Зарегистрировать актера на сервере UDS, указав следующие параметры:

SSL Validation: игнорировать сертификат \ верификационный сертификат.

UDS Server: имя или IP-адрес VDI - сервера и порт (по умолчанию: 2637).

Authenticator: Аутендификатор, к которому принадлежит указанный пользователь-администратор для регистрации участника VDI.

Для отображения различных аутентификаторов связь с VDI -сервером должна быть успешной. В администрировании VDI должен быть зарегистрирован хотя бы один (аутентификатор «Администрирование» соответствует суперпользователю, созданному в мастере настройки сервера VDI).

Username: Имя пользователя с разрешением администрации в окружающей среде VDI.

Password: Пароль администратора.

Log Level: типы журналов, которые должны отображаться в файлах журнала UDS Actor. Эти файлы журнала (udsactor.log) будут располагаться по путям:

%temp% (путь временных файлов пользователя) и

C:\Windows\Temp (путь временных файлов O.S.)

Как только все данные будут указаны, нажать кнопку «Register with UDS», чтобы зарегистрировать Actor на сервере VDI (Рисунок 281).

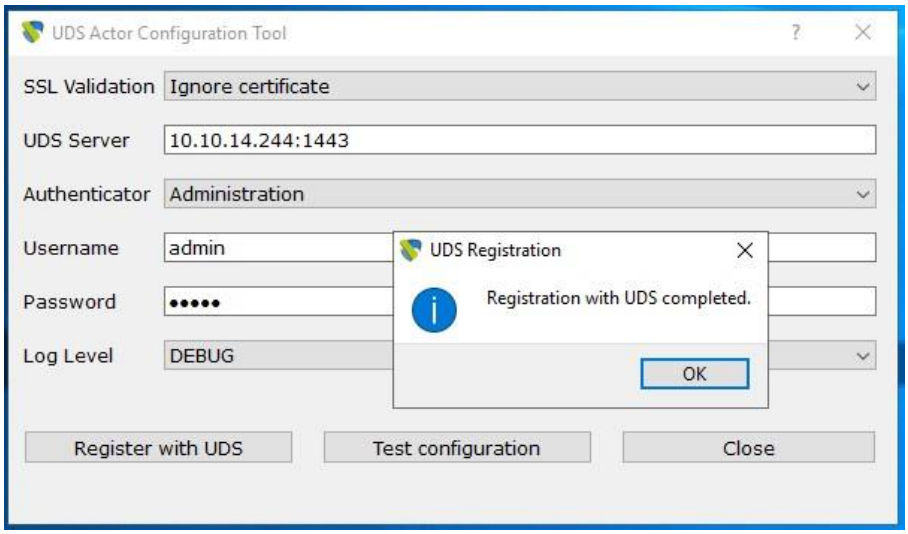


Рисунок 281

Нажать кнопку «Test configuration» для подтверждения правильности всех данных (Рисунок 282).

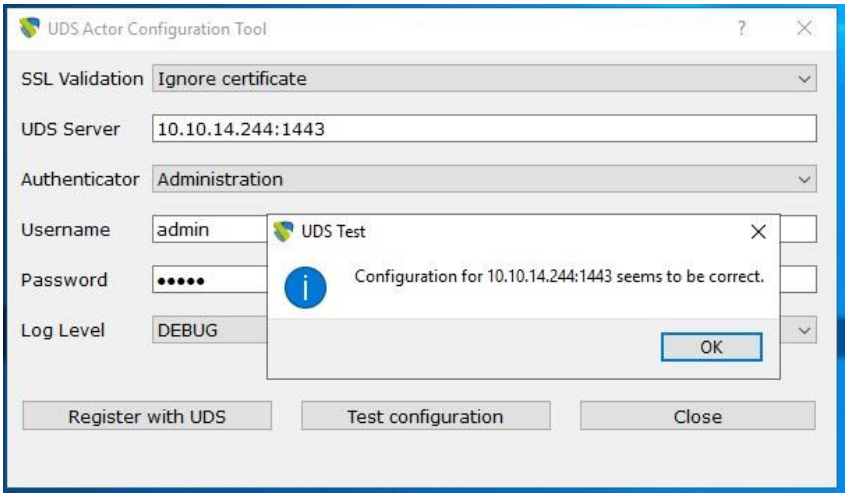


Рисунок 282

После установки участника UDS для серверов Windows RDS продолжить установку и настройку служб удаленных рабочих столов (Майкрософт).

Примечание: необходимо, чтобы в среде UDS был хотя бы один аутентификатор.

3.6.3 Установка и настройка RDS (Remote Desktop Service)

Установка службы удаленных рабочих столов (RDS) осуществляется следующим образом: «Диспетчер сервисов» – «Управление» – «Добавить роли и компоненты» (Рисунок 283).

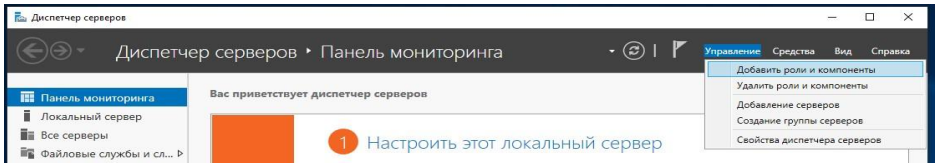


Рисунок 283

В мастере выполнить следующие действия:

Тип установки: «Установка служб удаленных рабочих столов» (Рисунок 284).

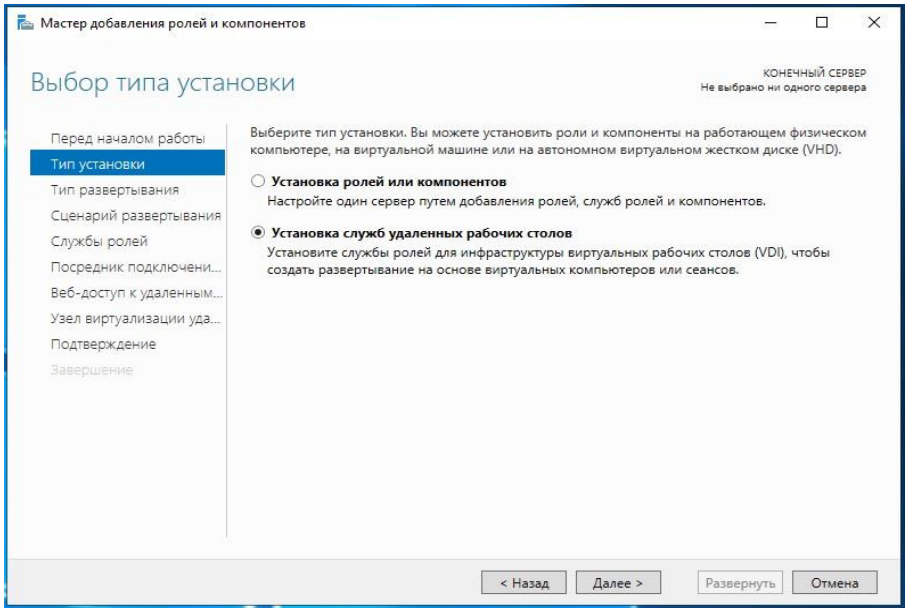


Рисунок 284

Тип развертывания: «Стандартное развертывание» (Рисунок 285).

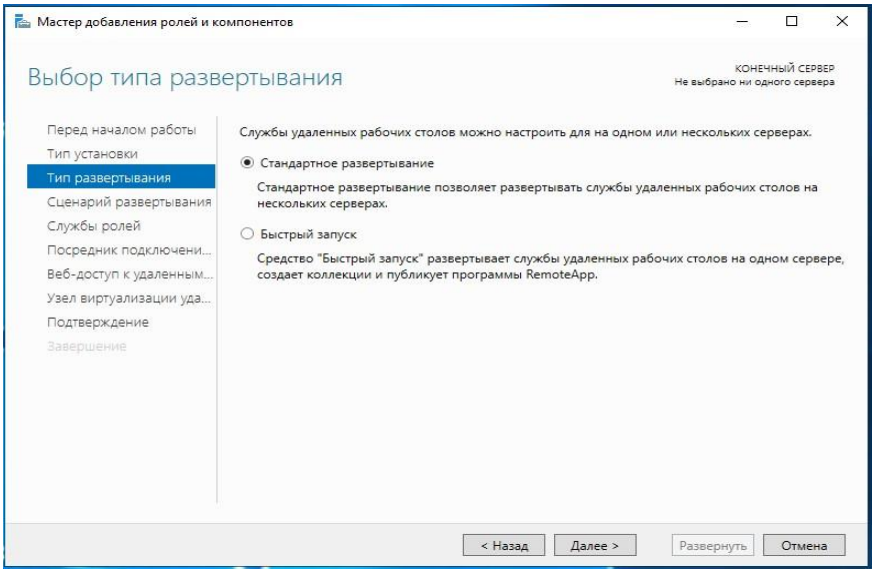


Рисунок 285

Сценарий развертывания: «Развертывание рабочих столов на основе сеансов» (Рисунок 286).

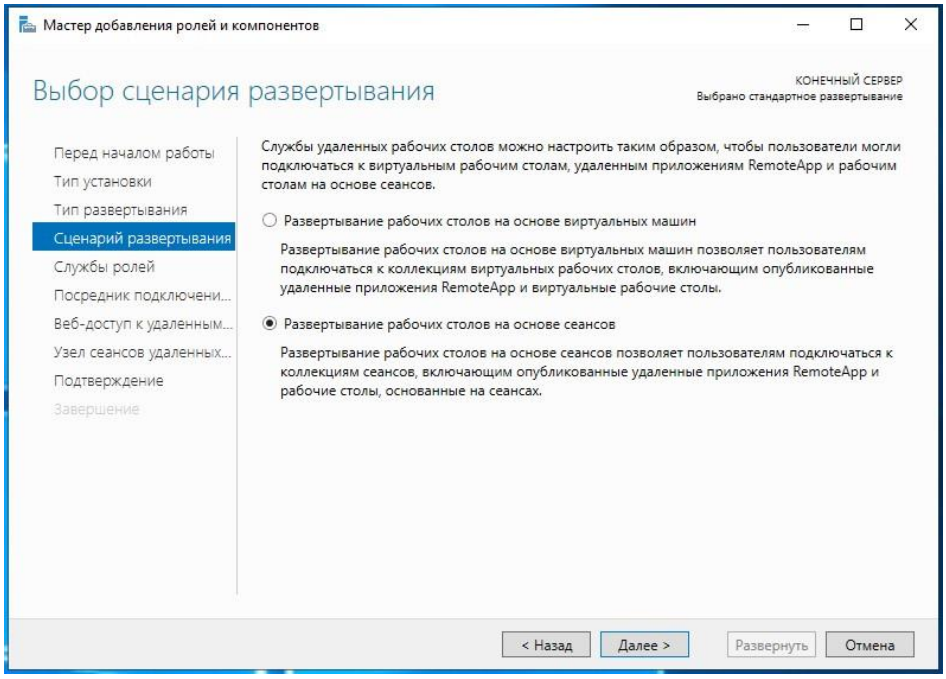


Рисунок 286

Появится сводная информация о том, что будет установлено (Рисунок 287)

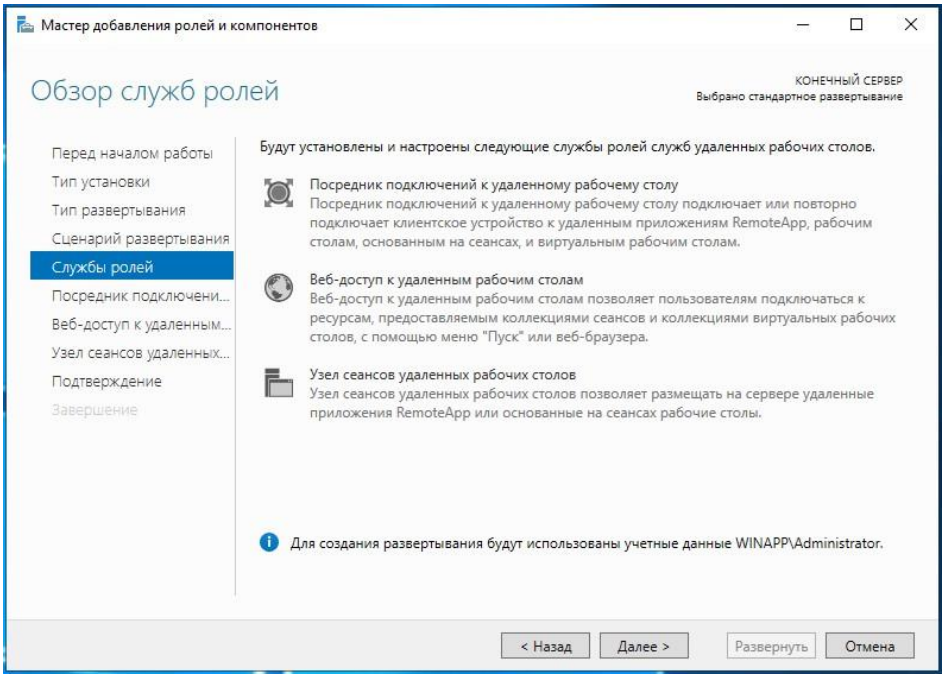


Рисунок 287

Должен быть указан сервер, на котором будет установлен каждый элемент (рисунки Рисунок 288 - Рисунок 290).

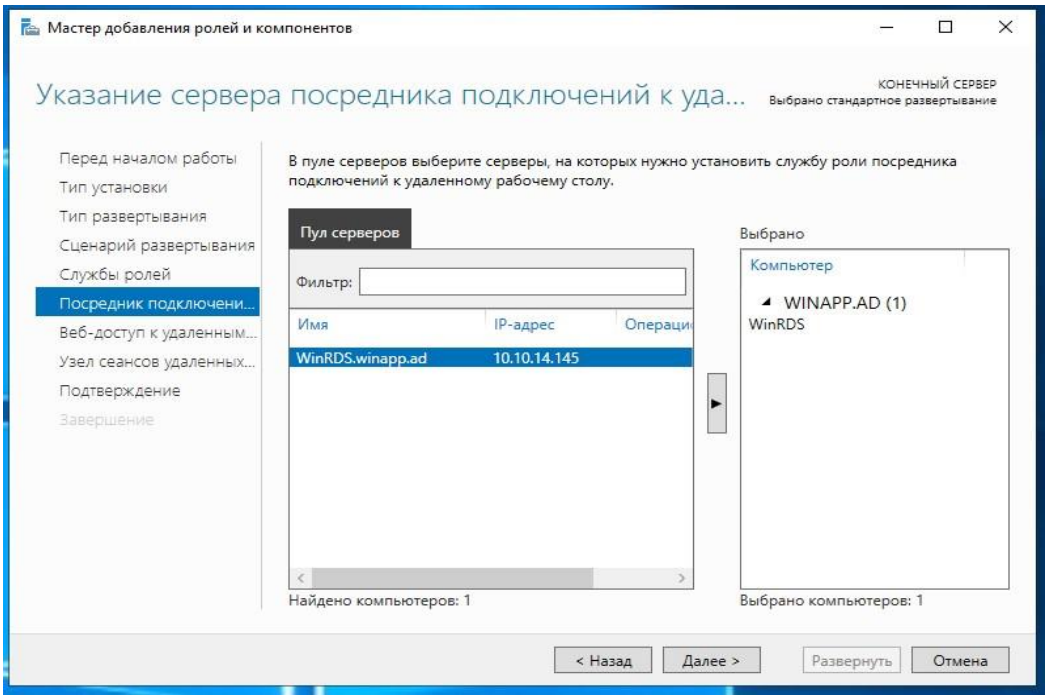


Рисунок 288

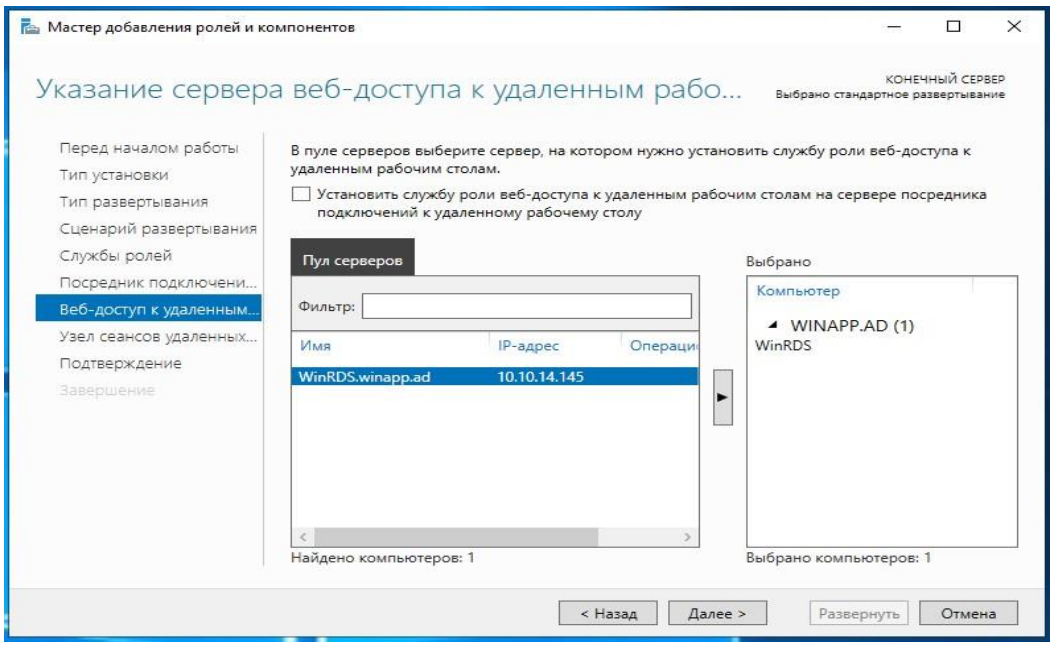


Рисунок 289

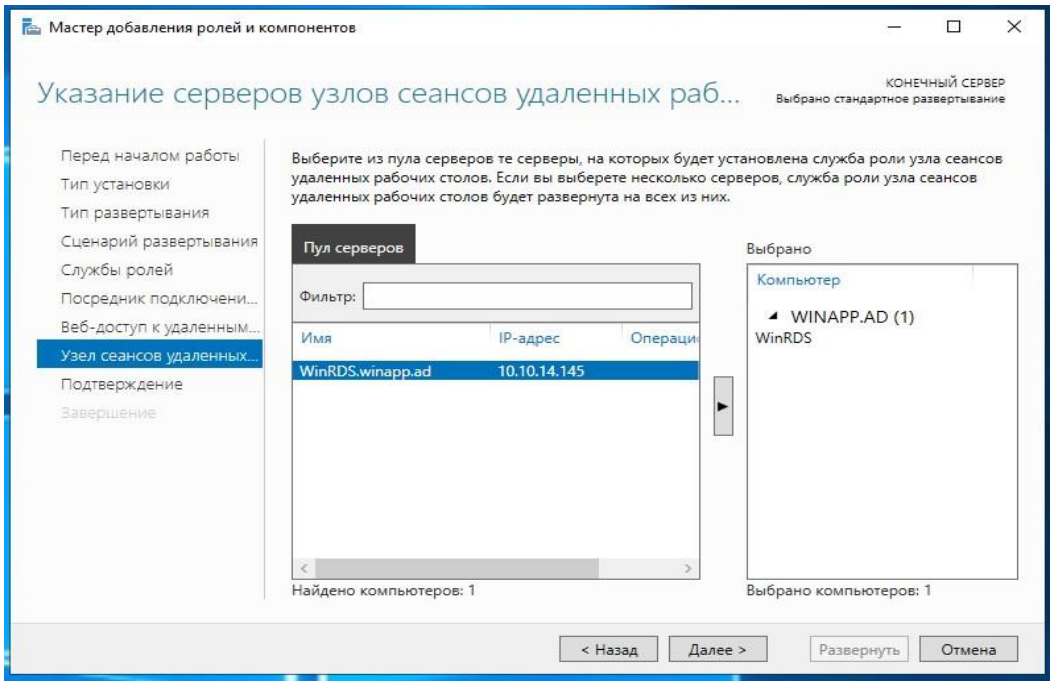


Рисунок 290

Установка подтверждается и выполняется ее развертывание (Рисунок 291):

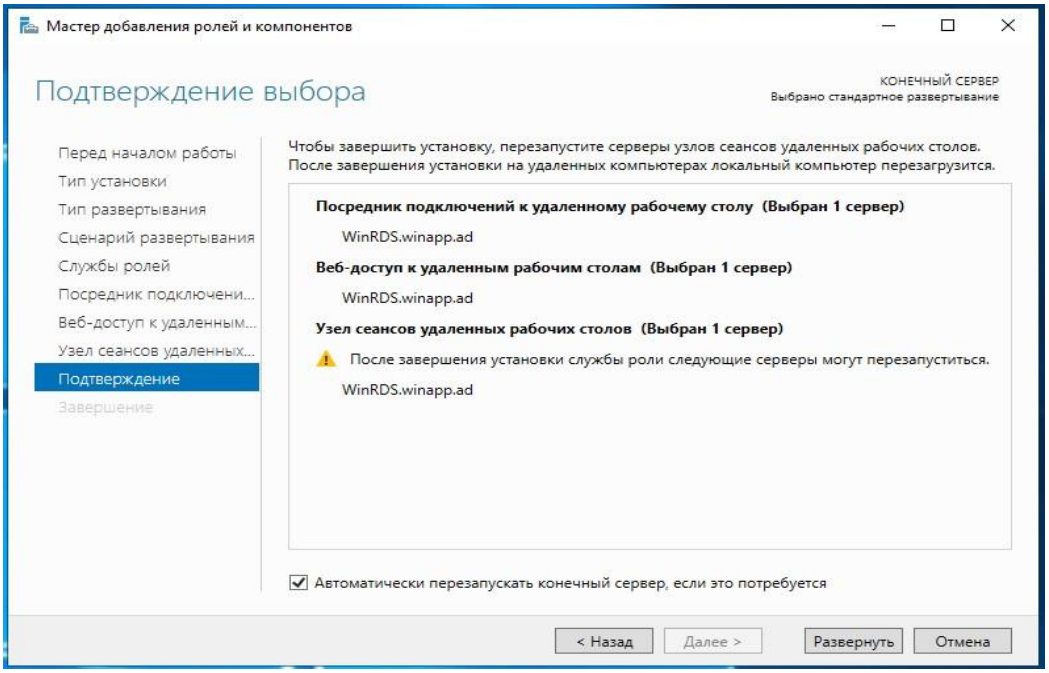


Рисунок 291

Сервер будет перезапущен автоматически (если вы это указали), и установка завершится (Рисунок 292).

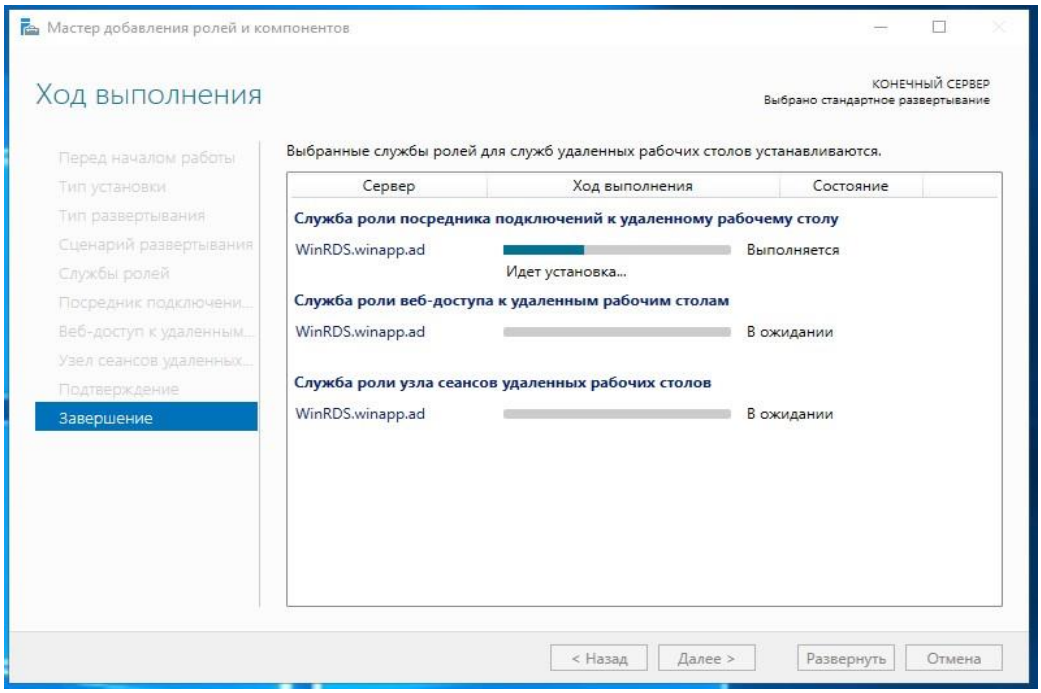


Рисунок 292

3.6.3.1 Настройка RDS с VDI

После установки роли RDS и перезапуска сервера продолжить создание новой коллекции RDS. Для этого выбрать «Создание коллекций сеансов» или открыть раздел «Коллекции» и выбрать «Создать коллекцию сеансов» (Рисунок 293).

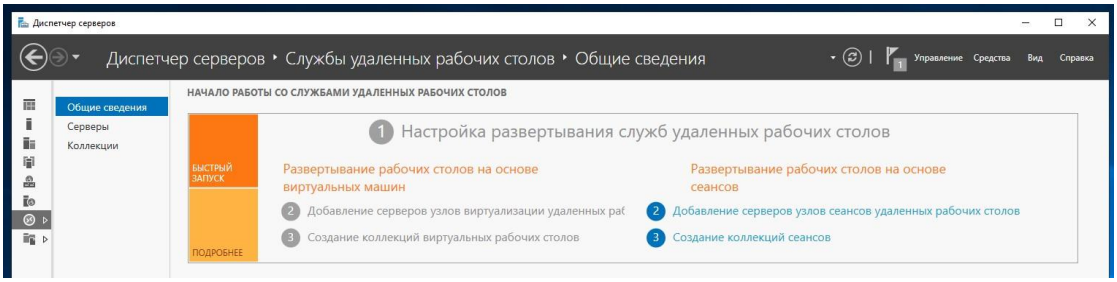


Рисунок 293

В мастере создания следует указать следующие данные. Указать имя для новой коллекции (Рисунок 294).

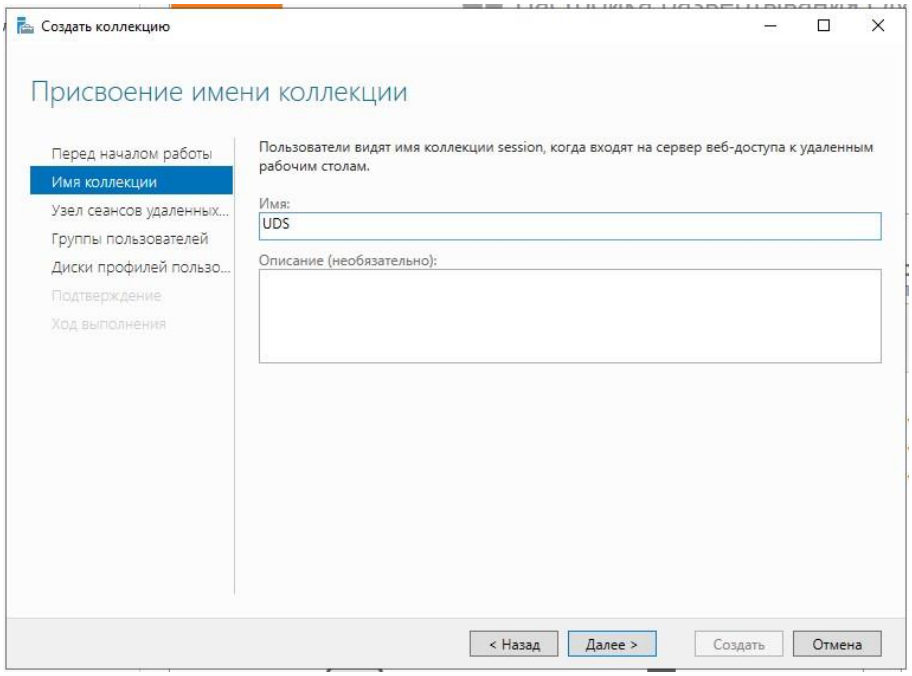


Рисунок 294

Добавить сервер в «Узел сеансов удаленных рабочих столов» (Рисунок 295):

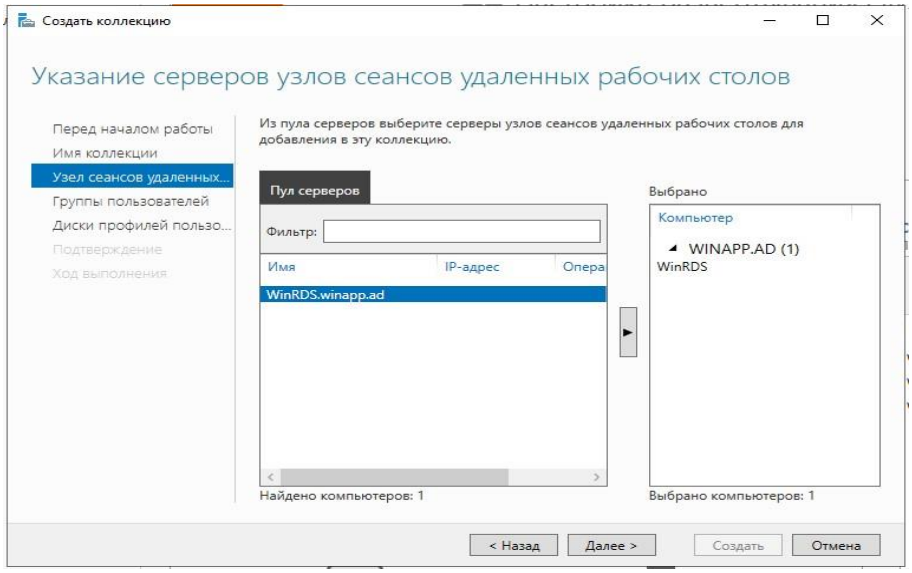


Рисунок 295

Выбрать группы пользователей, которые смогут получить доступ к коллекции. Оставьте группу «Пользователи домена» по умолчанию, чтобы разрешить всем пользователям и выполнить групповую фильтрацию из администрирования VDI (Рисунок 296).

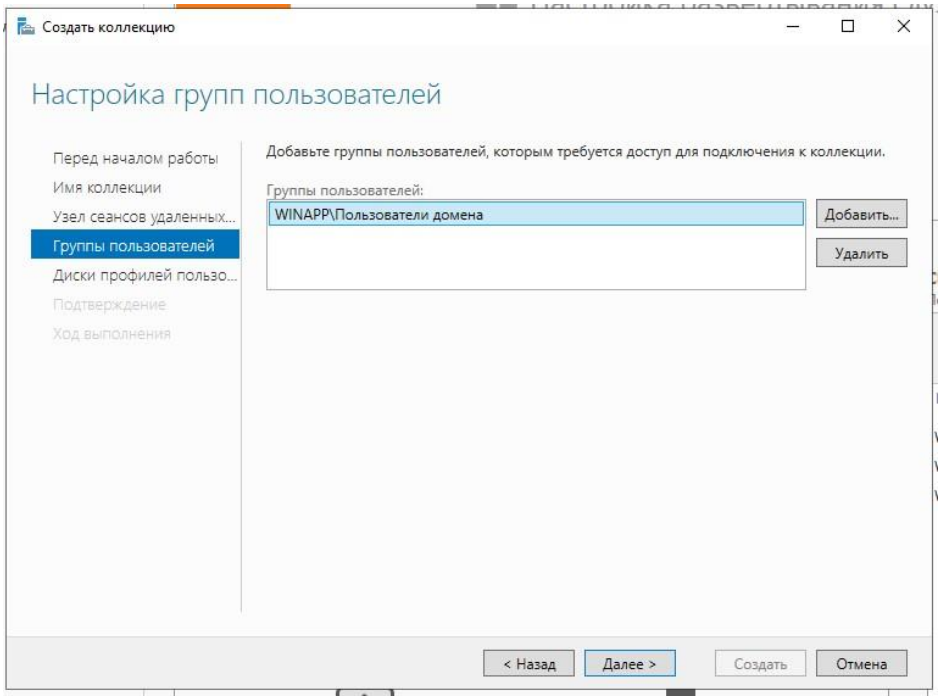


Рисунок 296

Указать, где будет храниться профиль пользователя. Если не указать, будет создан временный профиль, который будет удален при отключении пользователя (Рисунок 297).

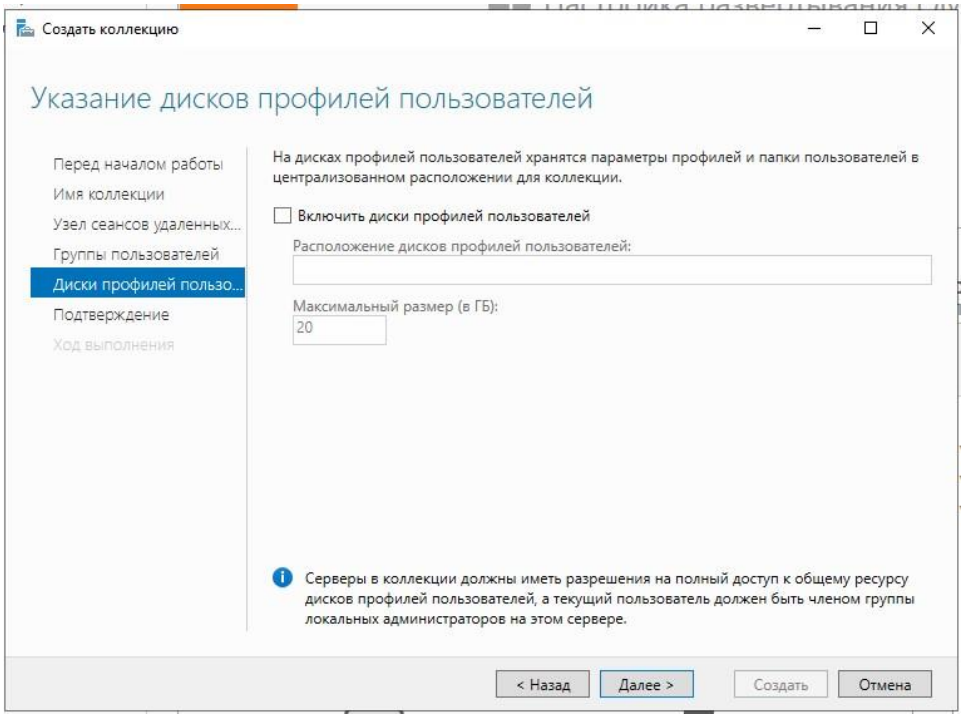
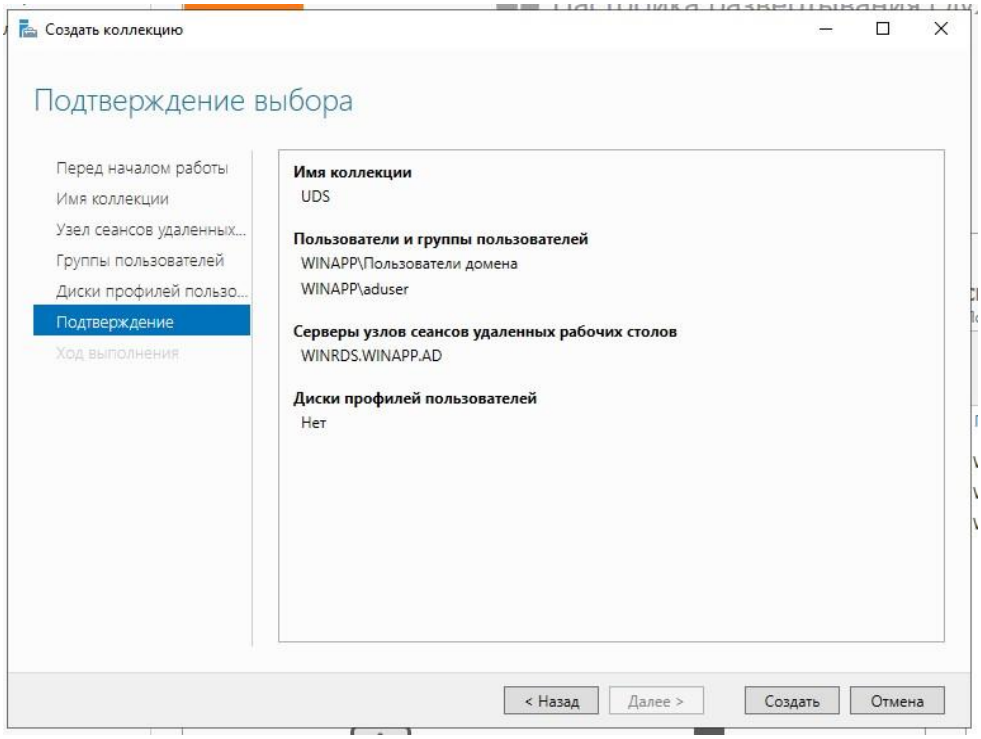


Рисунок 297

Подтвердить и создать коллекцию (Рисунок 298).



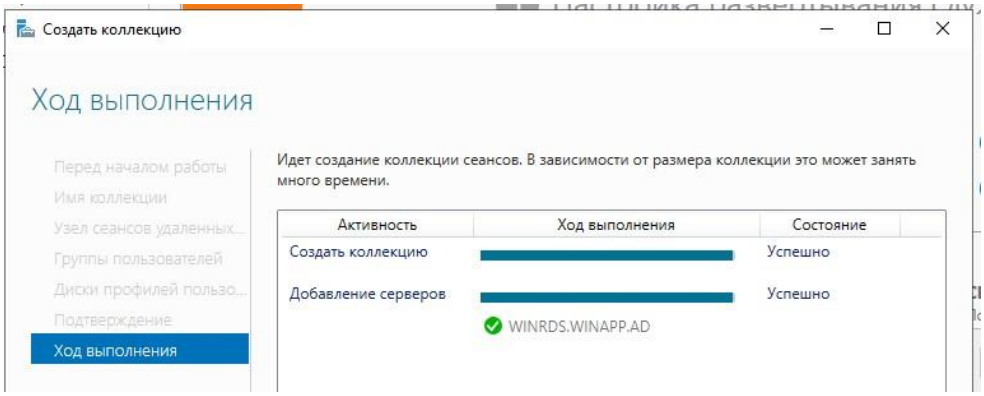


Рисунок 298

Публикация RDS Actor на RDS сервере. После создания коллекции выбрать «Опубликовать удаленные приложения RemoteApp» (Рисунок 299).

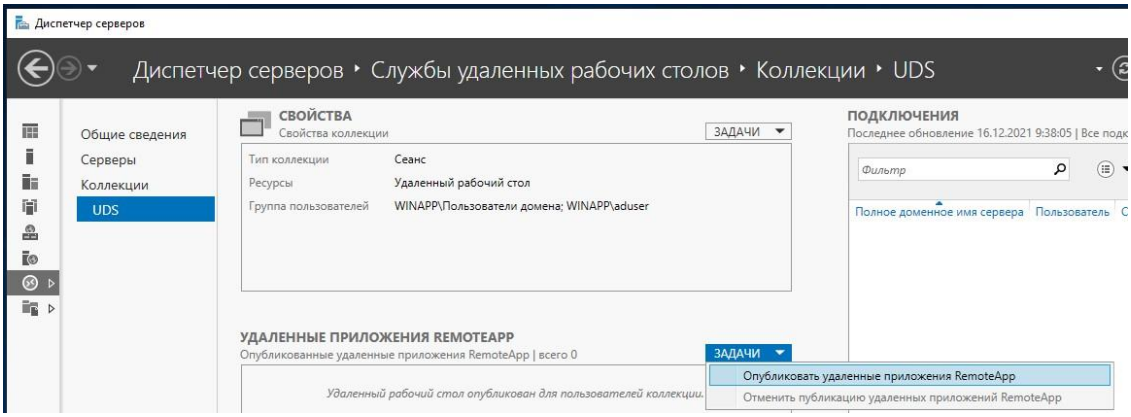


Рисунок 299

Необходимо добавить и выбрать исполнителя служб удаленных рабочих столов в списке «Удаленные приложения RemoteApp». Для этого необходимо предварительно установить UDS Actor для RDS.

Нажать кнопку «Добавить» и выбрать UDS Actor по пути (Рисунок 300):

C:\Program Files\RDSActor\RDSActor.exe

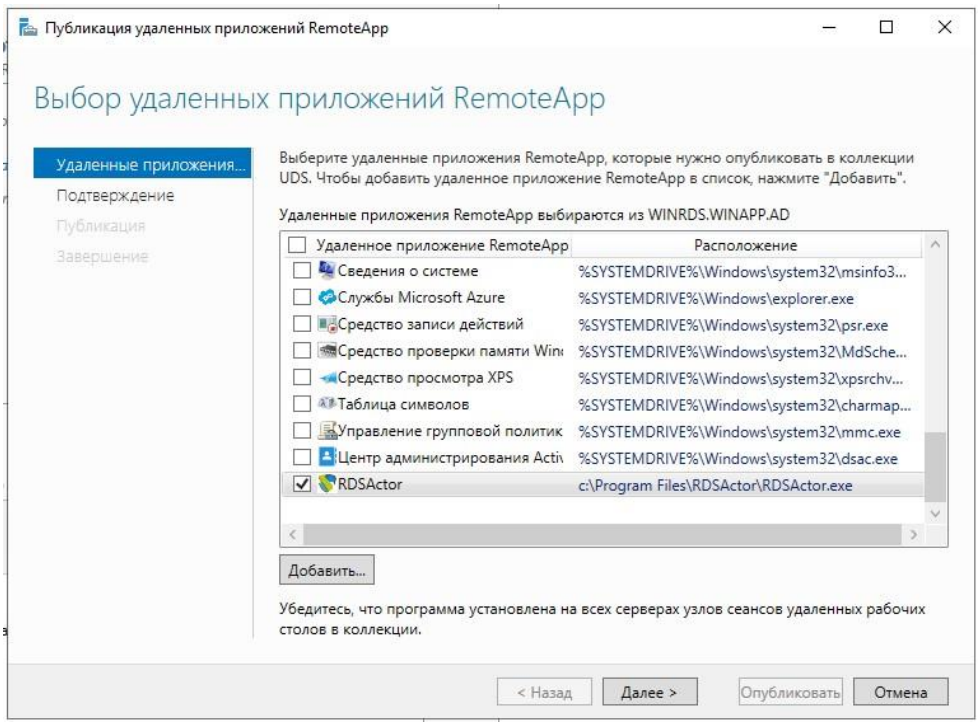


Рисунок 300

Подтвердить публикацию, нажать «Опубликовать» (Рисунок 301).

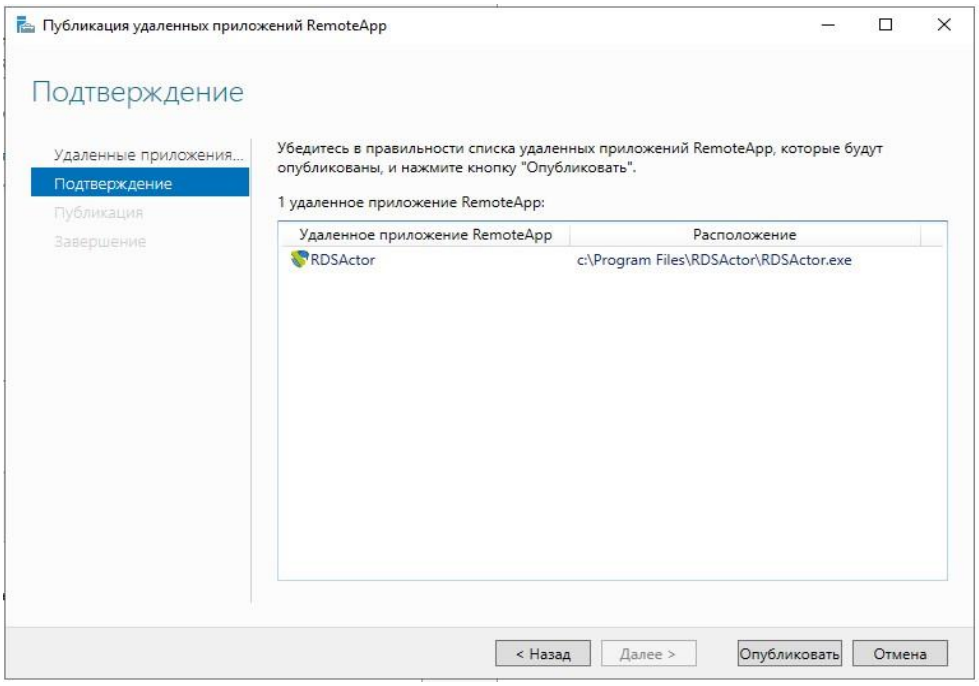


Рисунок 301

После создания отредактировать его свойства (Рисунок 302).

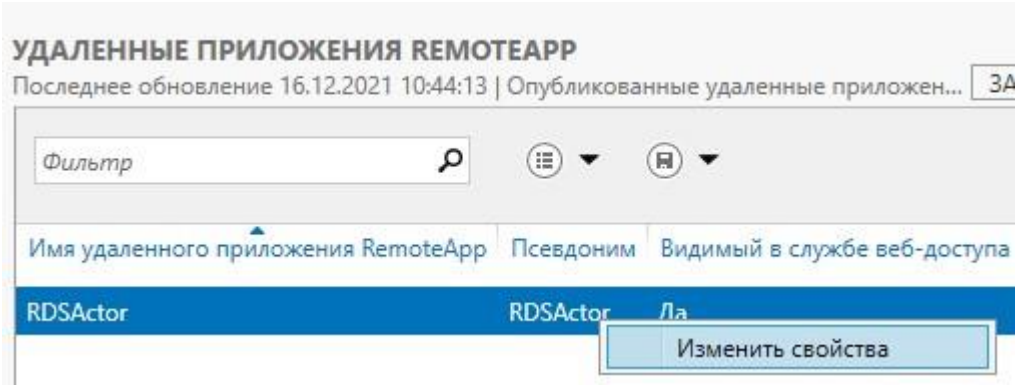


Рисунок 302

В разделе «Общие» отметить «Нет» в разделе «Показать удаленное приложение RemoteApp в веб-доступе к удаленным рабочим столам» (Рисунок 303).

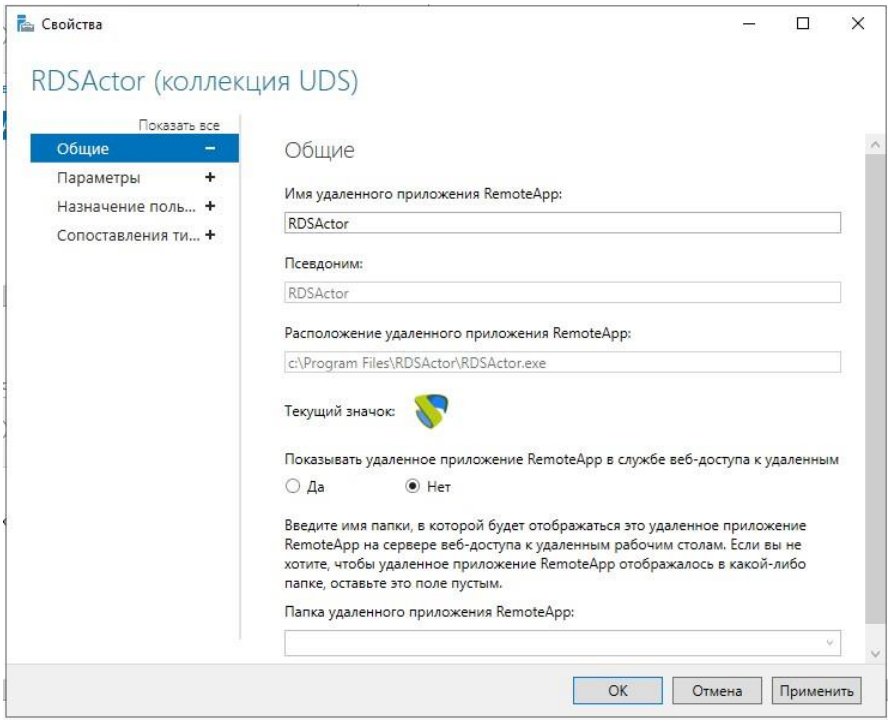


Рисунок 303

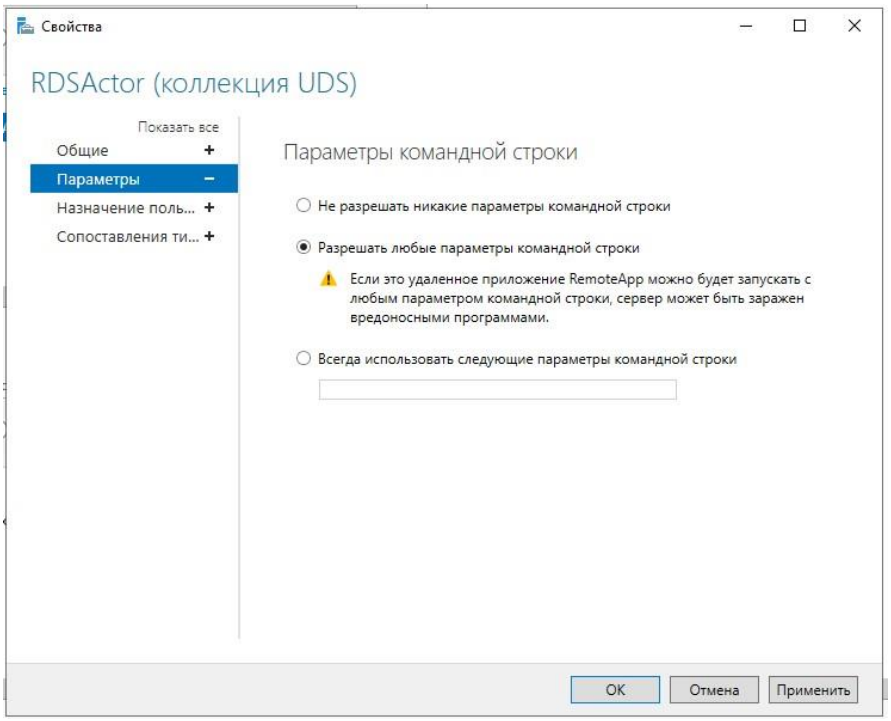


Рисунок 304

В разделе «Параметры» выбрать «Разрешать любые параметры командной строки» и применить изменения. Рекомендуется указать время окончания сеансов отключенных пользователей. Таким образом, пользователи и их лицензии будут освобождены при отключении от виртуального приложения.

Для этого изменить свойства коллекции (Рисунок 305):

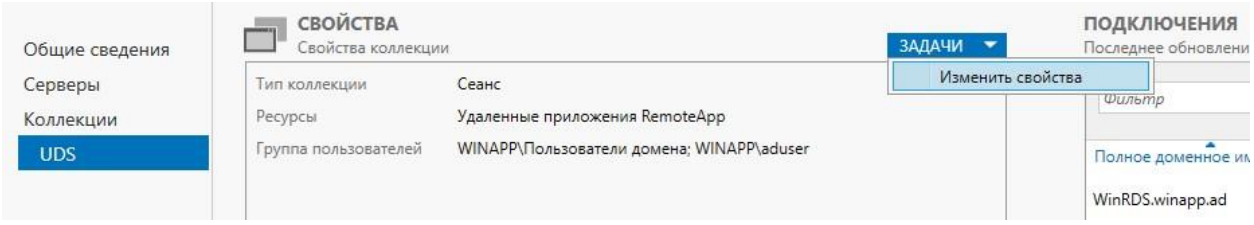


Рисунок 305

В разделе «Сеансы» указать минимальное время для «Окончание разъединенного сеанса» (Рисунок 306).

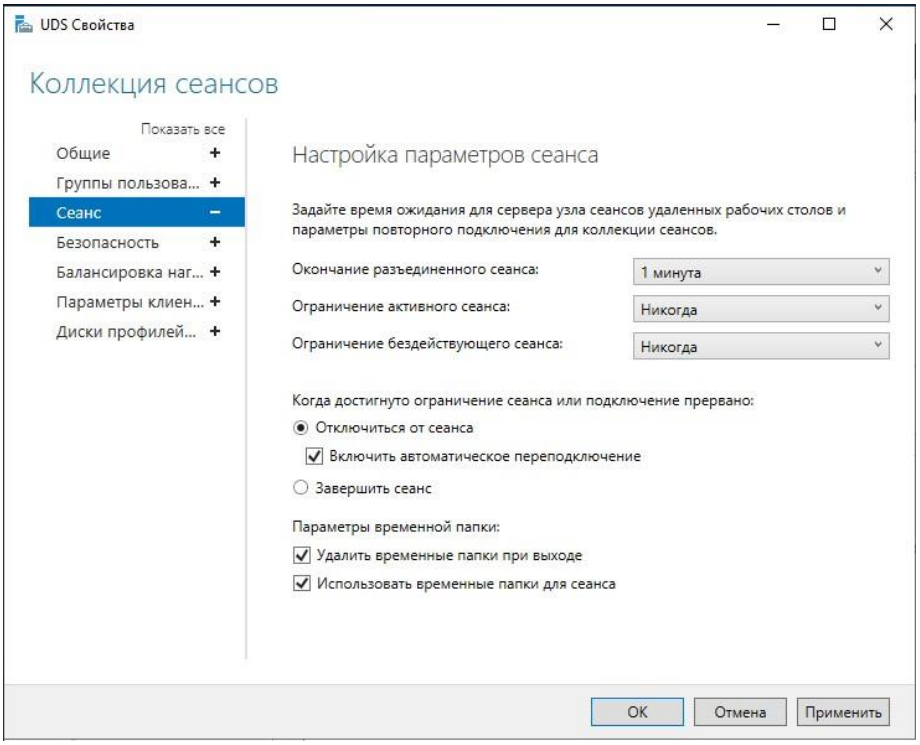


Рисунок 306

После выполнения всех этих шагов будет создан допустимый сервер RDS для подключения к серверу VDI и публикации виртуальных приложений для пользователей VDI.

3.6.4 Управление

После установки компонентов платформы VDI система готова к настройке. Введите IP-адрес и порт (по умолчанию: 2637) или имя сервера VDI (брокера) через https-доступ (Рисунок 307).

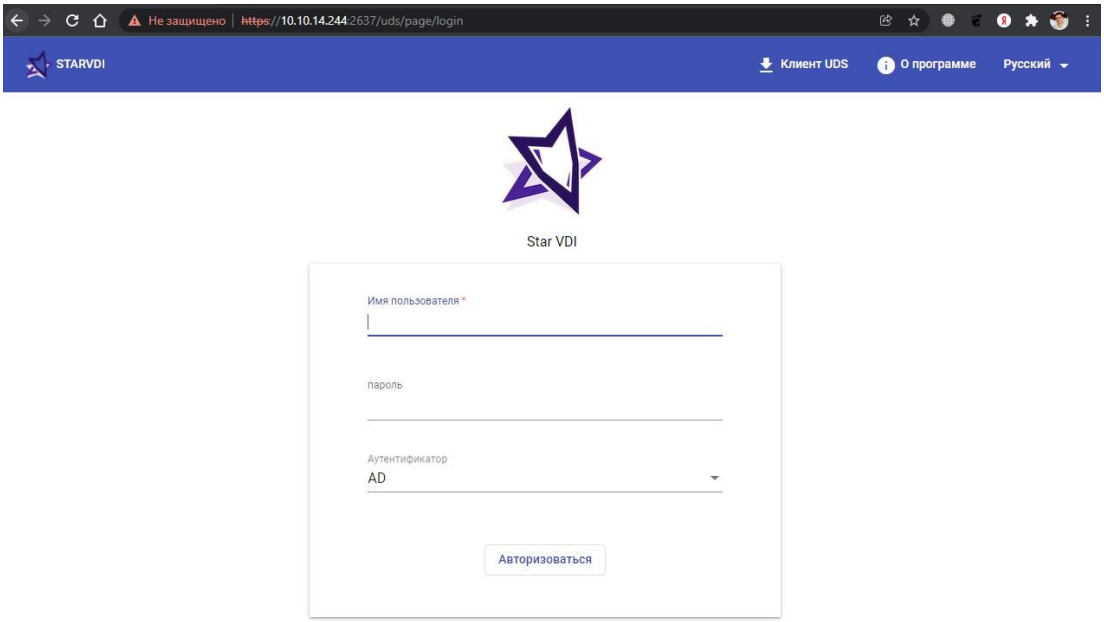


Рисунок 307

Для входа в панель администрирования VDI необходимо войти с помощью пользователя и пароля администратора. (По умолчанию: admin/admin)

После доступа к панели администрирования можно изменить пароль и создать или выбрать новых пользователей для входа в панель администрирования.

В случае, если уже есть пользователь с правами администратора на платформе VDI, ввести пользователя и пароль, а также выбрать аутентификатор, с которым пользователь будет проверять подлинность (только в случае наличия нескольких аутентификаторов).

Если к VDI-платформе подключено более одного аутентификатора и требуется получить доступ к панели администрирования под стандартным администратором VDI, выбранный аутентификатор не будет использоваться, поскольку этот пользователь не будет проверен на подлинность.

В меню пользователя выбрать «Панель управления», чтобы войти в администрирование VDI (Рисунок 308).

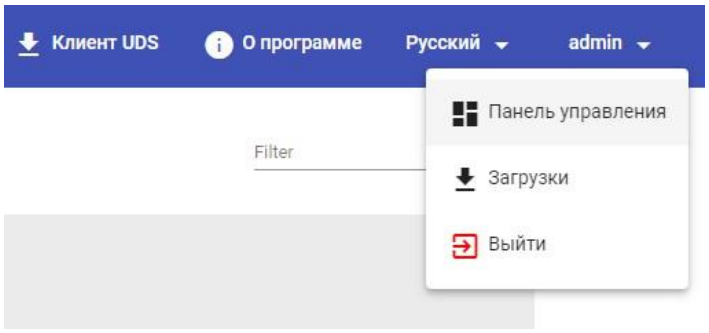


Рисунок 308

После входа в администрирование VDI выполните начальные конфигурации компонентов, которые образуют «сервис пулы». Это позволит развертывать и подключать различные службы, поддерживаемые VDI (виртуальные рабочие столы, сессии виртуальных приложений, и т.д.)

3.6.4.1 Поставщики услуг

«Поставщик услуг» отвечает за предоставление IP-услуг.

Услуги, предлагаемые VDI, будут представлять собой виртуальные рабочие столы или приложения по требованию, предоставляемые платформой виртуализации или постоянными физическими/виртуальными рабочими столами, назначенными определенным пользователям посредством назначения IP.

Чтобы построить «Пул служб» и опубликовать виртуальные рабочие столы и приложения, необходимо создать хотя бы одного «Поставщика услуг». VDI поддерживает одновременное выполнение нескольких «поставщиков услуг».

В настоящее время VDI поддерживает следующих «Поставщиков услуг»:

Поставщик статических IP-машин;
Поставщик платформы XenServer/XCP-NG;

Поставщик платформы Azure;

Поставщик платформы HVS (Иридиум);

Поставщик платформы HyperV;

Поставщик платформы Nutanix Acropolis;

Поставщик платформы OpenGnsys

Поставщик платформы OpenStack

Поставщик платформы Proxmox

Поставщик платформы RDS

Поставщик платформы VCloud Director

Поставщик платформы VMWare VCenter

Поставщик платформы oVirt/RHEV

Совместимый поставщик платформы OpenStack

Регистрация поставщика услуг «Поставщик статических IP-машин»

Нажать «Новый» и выбрать «Поставщик машин статистических IP» (Поставщик статических IP-машин) (Рисунок 309).

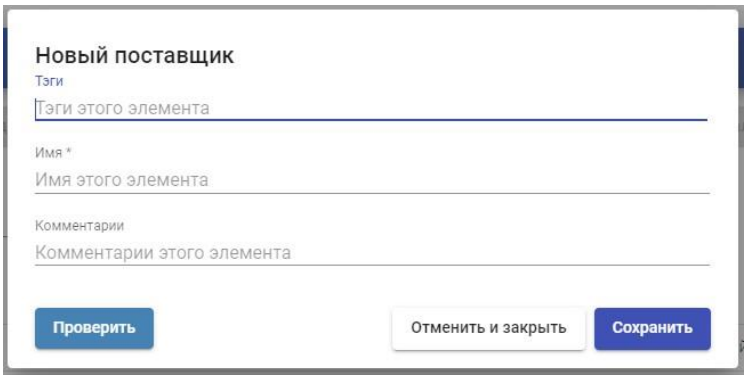


Рисунок 309

В поле «Поставщик машин статистических IP» необходимо указать описательное имя поставщика услуг.

Сохранить конфигурацию, и будет зарегистрирован действительный «Поставщик услуг», чтобы начать регистрацию базовых служб в поставщике типа «Поставщик статических IP-машин».

Для этого дважды щелкнуть по созданному поставщику услуг или щелкнуть правой кнопкой мыши и выбрать в меню «Подробность» (Рисунок 310).

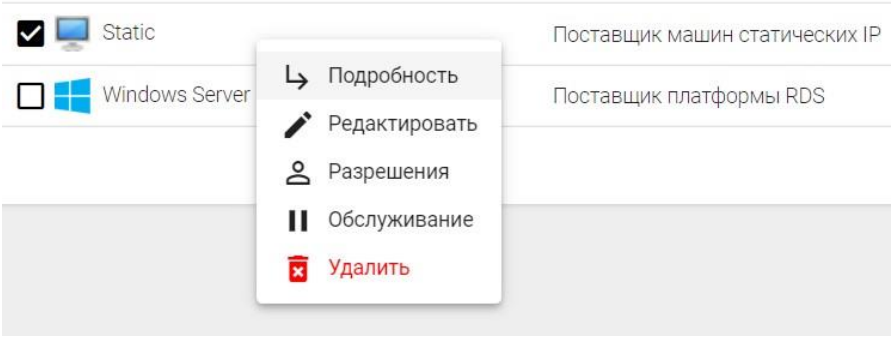


Рисунок 310

Конфигурирование службы на основе «Статистический множественный IPадрес»

Этот тип службы позволит пользователям получать доступ к различным компьютерам (физическим или виртуальным). Соединение всегда будет выполняться один к одному, то есть один пользователь к одному компьютеру.

Чтобы создать базовые службы типа «Статистический множественный IPадрес», выбрать вкладку «Поставщики услуг», нажать «Новый» и выбрать «Статистический множественный IP-адрес» (Рисунок 311).

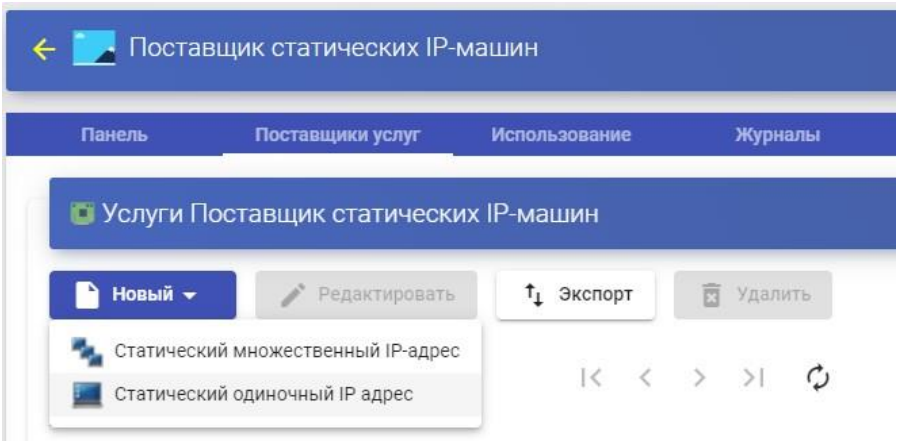


Рисунок 311

Откроется окно параметров настроек (Рисунок 312).

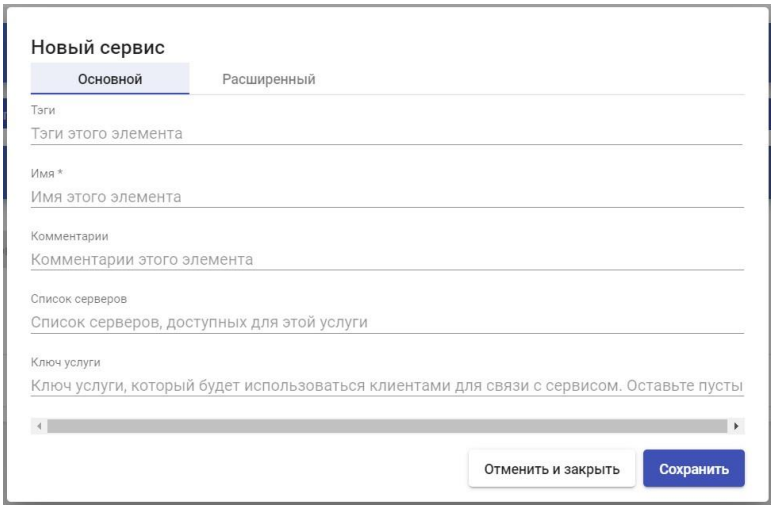


Рисунок 312

Минимальные параметры для настройки в этом типе службы:

▪ Основные:

Имя: Название службы.

Список серверов: IP-адреса компьютеров, к которым будут подключаться пользователи.

Ввести различные IP-адреса, разделенные запятыми, и нажать «Добавить» (Рисунок 313).

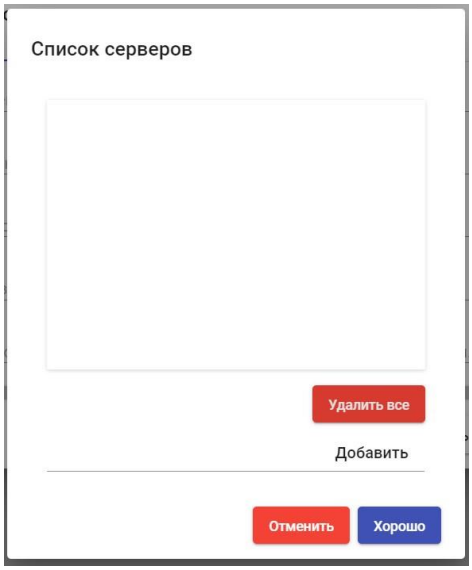


Рисунок 313

Ключ услуги (Рисунок 314): если в этом поле не указан маркер (пустой), система не будет управлять сеансами пользователей на компьютерах. Поэтому при назначении компьютера пользователю это назначение будет поддерживаться до тех пор, пока администратор не удалит его вручную. При наличии маркера сеансы пользователей будут управляться.

Когда пользователи выйдут из системы, они будут освобождены, чтобы снова стать доступными для других пользователей.

При указании ключа необходимо, чтобы указанные компьютеры (посредством их IP-адреса) установили UDS Actor, управляющий статическими машинами («UDSActorUnmanagedSetup-»....).

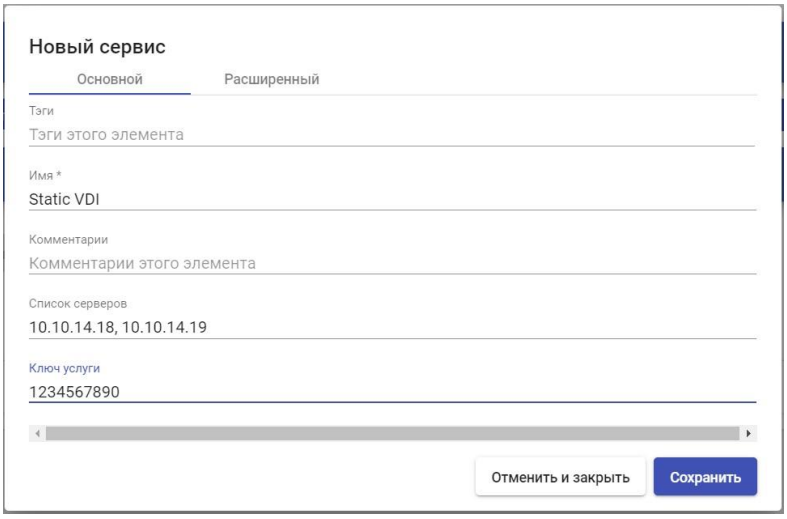


Рисунок 314 ▪

Расширенный (Рисунок 315):

Пропустить время: если порт указан в поле «Проверьте порт» и машина недоступна, можно указать время, которое предотвратит новую проверку этой машины. Если указано значение 0, машины всегда будут проверены. По умолчанию индицируется 15 (этот параметр указывается в минутах).

Проверьте порт: если вы указываете порт, то перед назначением услуги пользователю система проверяет доступность компьютера. Если он недоступен через указанный порт, система назначает следующую доступную машину в списке. Если порт не указан, доступ к машинам не проверяется и назначается независимо от их состояния.

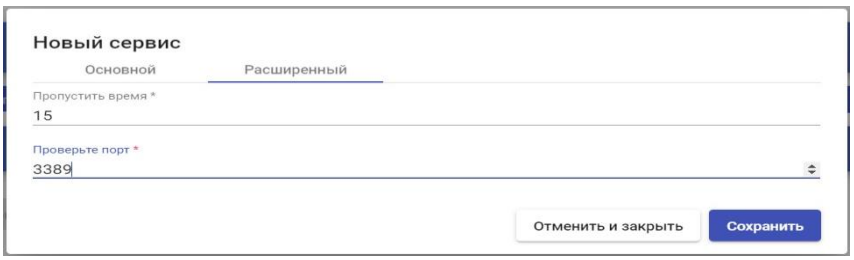


Рисунок 315

Сохранить конфигурацию, и будет действительный «Статистический множественный IP-адрес». Можно зарегистрировать все необходимые услуги типа «Статистический множественный IP-адрес».

После настройки полной среды VDI (служб, аутентификаторов и транспортов) и создания первого «пула служб» пользователи получат доступ к IP-адресам различных компьютеров, зарегистрированных в службе.

Из «Сервис-пула» можно также выполнить выборочное назначение, указывающее, какое устройство назначено каждому пользователю.

Конфигурирование службы на основе «Статический одиночный IP-адрес»

Этот тип службы позволит разным пользователям получать доступ к одному и тому же компьютеру (физическому или виртуальному). Каждый пользователь запускает новый сеанс на компьютере, пока он настроен для этой цели.

Для создания базовой службы типа «Статический одиночный IP-адрес» перейдите к «Поставщики услуг», выбрать вкладку «Поставщики услуг», нажать «Новый» и выбрать «Статический одиночный IP-адрес» (Рисунок 316).

Рисунок 316

Минимальные параметры для настройки в этом типе службы:

Имя: Название службы.

IP адрес машины: IP-адрес компьютера, с которым соединятся пользователи. Компьютер должен разрешить доступ через различные пользовательские сеансы.

Сохранить конфигурацию и введите допустимый «Статический одиночный IP-адрес». Можно зарегистрировать все необходимые услуги типа «Статический одиночный IP-адрес».

После настройки полной среды VDI (служб, аутентификаторов и транспортов) и создания первого «Сервис пула» пользователи получат доступ к IP указанного устройства, начав новый сеанс.

Поставщик платформы RDS

Этот тип «поставщика услуг» позволяет развертывать сеансы виртуальных приложений и подключаться к ним через службы удаленных рабочих столов Microsoft (RDS).

Через этого провайдера пользователи, прошедшие проверку в системе аутентификации, отличной от «Active Directory», также смогут получить доступ к сеансам приложений. Необходимо будет использовать сопоставление пользователей, которые могут быть как ранее созданы в AD (выделенном для среды VDI) или чтобы VDI автоматически создавал этих пользователей на существующем сервере AD.

Нажать «Новый» и выбрать «Поставщик платформы RDS» (Рисунок 317):

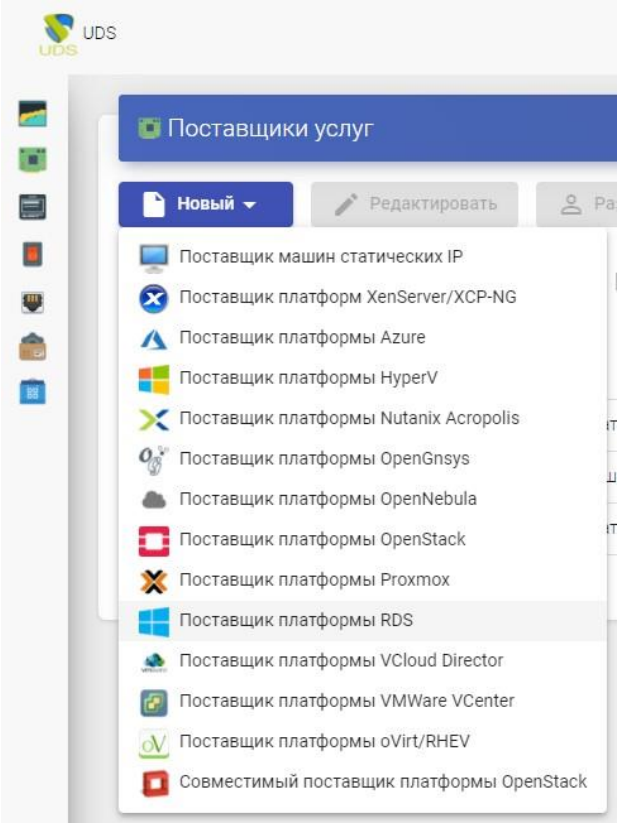


Рисунок 317

В «Поставщике платформы RDS» необходимо настроить следующие минимальные параметры (Рисунок 318):

Рисунок 318

Имя: имя службы.

Список серверов: список серверов приложений Microsoft RDS, доступных для публикации приложений. В случае указания более одного сервера соединения пользователей будут распределяться между разными серверами.

Введите разные IP-адреса, разделенные запятыми, и нажать «Добавить» (Рисунок 319):

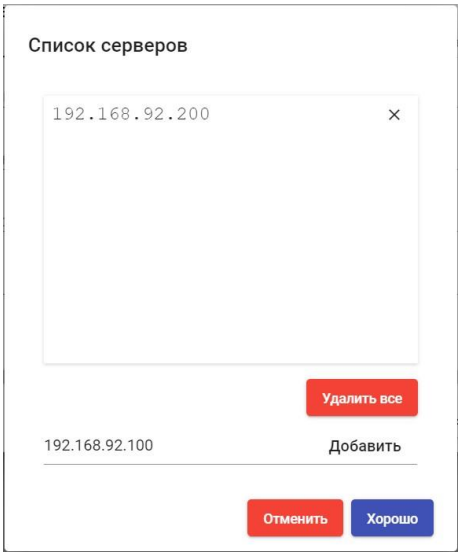


Рисунок 319

Примечание: одна и таже служба RDS может иметь несколько IP-адресов, соединяющих различные существующие серверы RDS, что обеспечивает высокую доступность приложений. Кроме того, при указании нескольких IP адресов необходимо отметить флажок «Сервер проверяется».

Сервер проверяется: проверяет, доступен ли сервер приложений RDS каждый раз, когда поступает запрос от пользователя. В случае невозможности подключения к первому серверу в списке VDI будет искать следующий доступный сервер для предоставления услуги.

Сопоставление пользователей (Рисунок 320):

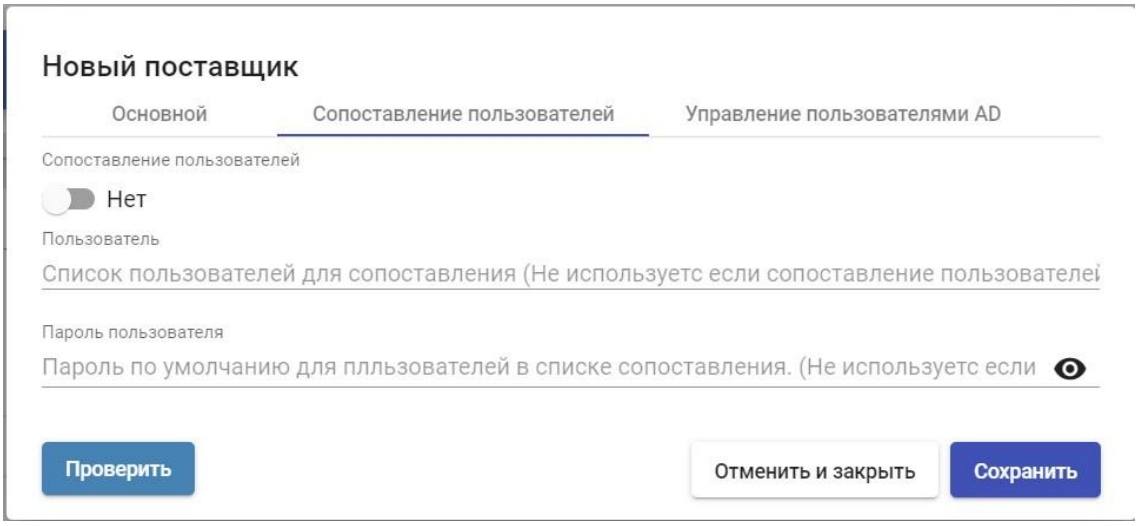


Рисунок 320

Примечание: следует активировать «Сопоставление пользователей» только в том случае, если нужно указать общих пользователей домена AD.

Если пользователь не находится в журнале Active Directory (AD) в «Аутентификаторы» VDI, необходимо определить следующие параметры на вкладке «Сопоставление пользователей»:

Переключатель в положении «Да»: указывает, что для доступа к приложениям будут использоваться определенные пользователи (указанные в разделе «Пользователь»).

Переключатель в положении «Нет»: будет использоваться пользователи портала входа VDI для доступа к приложениям (в этом случае, это должен быть пользователь AD).

«Пользователь»: применяется только в том случае, если «Сопоставление пользователей» имеет значение «Да». Они будут сопоставлять пользователей, принадлежащих Active Directory, которые

смогут входить на серверы приложений RDS и которые будут использоваться VDI только для выполнения сеанса приложения.

«Пароль пользователя»: пароль всех пользователей, указанных в предыдущем разделе. Все пользователи сопоставления должны иметь одинаковый пароль.

Управление пользователями AD:

Примечание: следует включать «Автоматическое создание пользователей в AD» только в том случае, если нужно указать пользователей из домена AD. Эти пользователи будут автоматически созданы VDI.

Автоматическое создание пользователей в AD:

«Да» означает, что для доступа к приложениям будут использоваться определенные пользователи, автоматически созданные VDI в AD.

«Нет» будет использовать пользователя портала входа VDI для доступа к приложениям (в этом случае это должен быть пользователь AD).

Сервер AD: IP или имя сервера Active Directory, на котором будут создаваться новые пользователи (на сервере должно быть включено подключение через LDAPS)

Порт: порт, используемый в соединении.

OU сервера AD для созданных пользователей: Организационная единица, в которой будут созданы новые пользователи.

Имя пользователя: пользователь домена с правами на создание и удаление пользователей. В формате: user@domain.xxx

Пароль: Пароль указанного пользователя

Префикс для созданных пользователей: Префикс, который будет добавлен к имени пользователя, созданного в AD. Окончательное имя созданного пользователя будет таким: префикс+имя_пользователя

Домен AD: имя домена, в котором будут зарегистрированы новые пользователи. Если не указано, будет использоваться домен поля: «Имя пользователя».

Группа AD: имя группы (должно существовать), в которую VDI будет добавлять новых пользователей.

Примечание: для сопоставления пользователей можно активировать только один из двух методов: «Сопоставление пользователей» или «Автоматическое создание пользователей в AD».

С помощью кнопки «Тест» вы проверите успешность подключения.

Сохраните конфигурацию, и у вас будут действительные «поставщики услуг», чтобы начать регистрацию сеансов виртуальных приложений.

Примечание: если необходимо создать новые серверы приложений, можно зарегистрировать всех необходимых вам «Поставщиков услуг» типа «Поставщик платформы RDS».

Чтобы изменить любой параметр в существующем «Поставщике услуг», выбрать его и нажать «Изменить».

С помощью кнопки «Войти в режим обслуживания» можно приостановить все операции, выполняемые VDI-сервером на поставщике услуг. Рекомендуется переводить поставщика услуг в режим обслуживания в тех случаях, когда связь с этим поставщиком услуг потеряна или планируется отключение обслуживания.

После интеграции серверов приложений в UDS можно создавать базовые службы. Для этого дважды щелкнуть по созданному провайдеру услуг или в меню провайдера и выбрать «Подробность».

Настройте службу на основе «Поставщик платформы RDS»

После интеграции серверов приложений в VDI и установки соответствующего UDS Actor необходимо создать базовые службы типа «Поставщик платформы RDS».

Там указать приложение для виртуализации.

Чтобы создать базовые службы типа «Поставщик платформы RDS», откройте созданного «Поставщик платформы RDS», выбрать вкладку «Поставщики услуг», нажать «Новый» и выбрать «RDS платформа RemoteAPP» (В этом примере калькулятор Windows) (Рисунок 321).

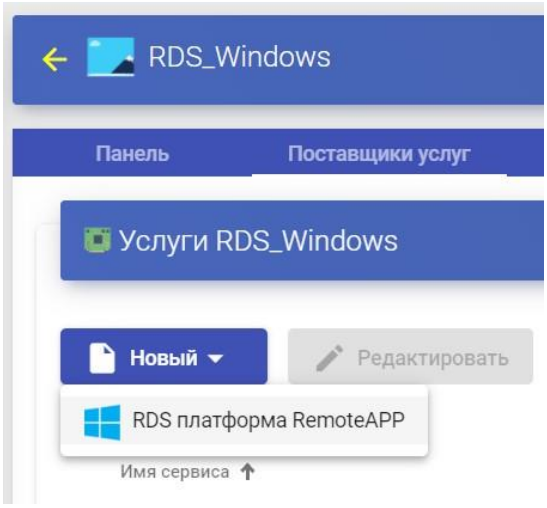


Рисунок 321

Минимальные параметры для настройки в этом типе службы (Рисунок 322):

▪ Основной:

Имя: Имя службы.

Путь приложения: путь выполнения виртуализируемого приложения, размещенного на серверах RDS.

Параметры приложения: параметры могут быть переданы любому приложению в этом поле, чтобы настроить выполнение приложения.

Начальный путь: путь, по которому будет выполняться приложение.

Максимум. Разрешенные услуги: максимальное количество сеансов приложений (0 = неограниченно).

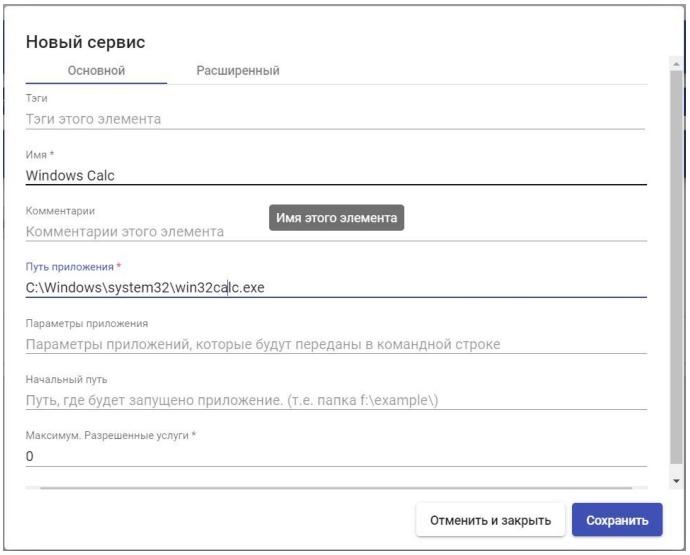


Рисунок 322

▪ Дополнительно (Рисунок 323):

Ожидание порожденных процессов: ожидает завершения всех процессов, производных от приложения, прежде чем считать приложение отключенным.

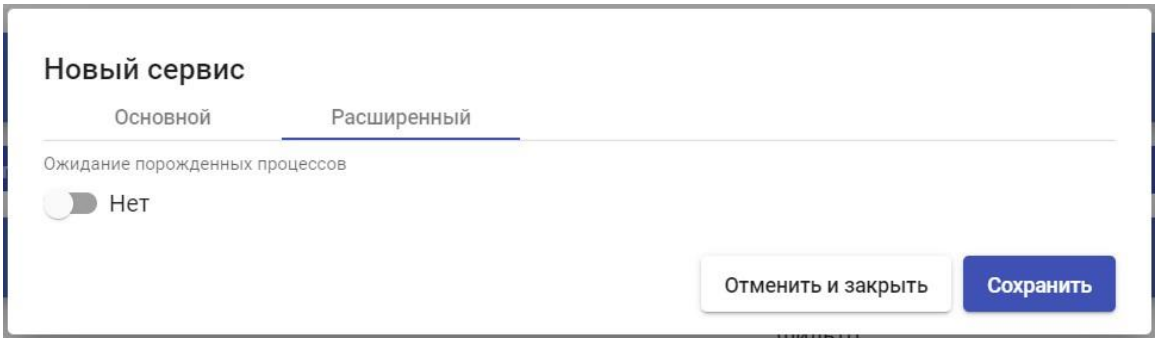


Рисунок 323

3.6.4.2 Настройки аутентификации

Active Directory

Этот внешний аутендификатор обеспечивает доступ к виртуальным рабочим столам и приложениям для пользователей и групп пользователей, принадлежащих Active Directory (Рисунок 324).

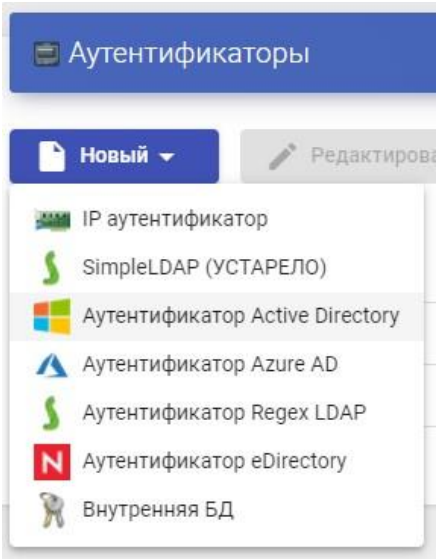


Рисунок 324

В «Active Directory аутендификаторе» настраиваются следующие минимальные параметры (Рисунок 325):

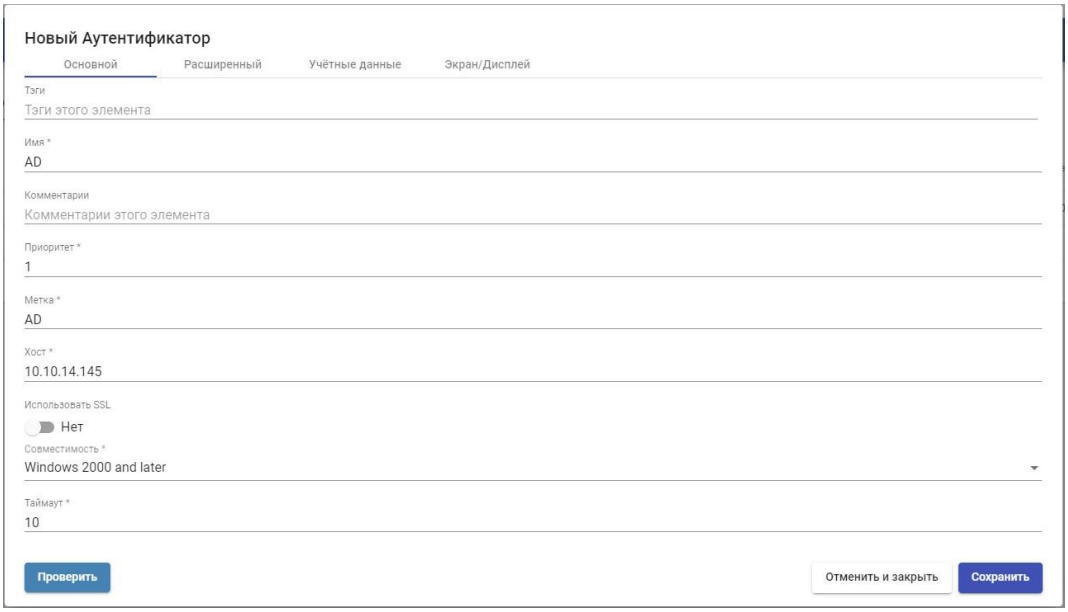


Рисунок 325 ▪

Основной:

Имя: Имя аутентификатора

Приоритет: Приоритет, который будет иметь этот аутентификатор. Если аутентификаторов несколько, чем ниже его приоритет, тем выше он появится в списке аутентификаторов, доступных на портале входа в VDI. Это поле поддерживает отрицательные значения.

Метка: включает прямую проверку подлинности в средстве проверки подлинности. Это позволяет пользователю быть проверенным в портале входа с указанным аутентификатором, даже если среда VDI имеет больше аутентификаторов.

Хост: IP-адрес или имя сервера Active Directory.

Используйте SSL: если включено, SSL-соединение будет использоваться для проверки подлинности.

Совместимость: выбрать уровень совместимости средства проверки подлинности Active Directory.

Тайм-аут: «Тайм-аут» для подключения к аутентификатору.

▪ Расширенный (Рисунок 326):

Переопределение базы: это поле позволяет использовать базу поиска, отличную от используемой по умолчанию (база поиска по умолчанию извлекается из пользователя, указанного в поле «Пользователь» раздела «Учетные данные»). Заполните это поле только в том случае, если необходимо указать определенную базу поиска пользователя (например: dc = vdi2, dc = local).

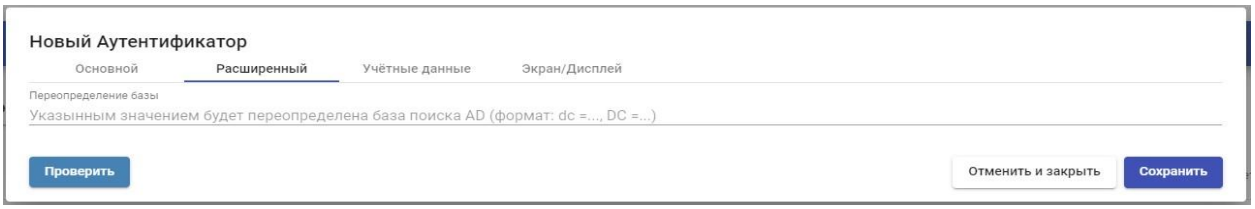


Рисунок 326

▪Учетные данные (Рисунок 327):

Пользователь: пользователь с привилегиями на чтения (формат: user@domain)

Пароль: пароль пользователя

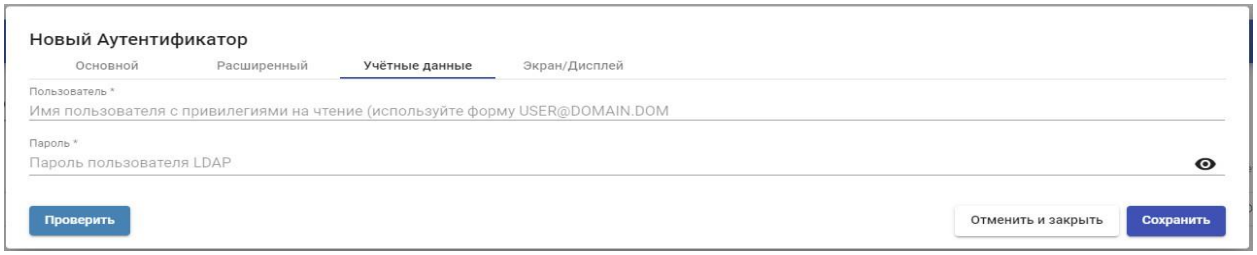


Рисунок 327

▪ Экран/Дисплей (Рисунок 328):

Видимый: если параметр отключен, средство проверки подлинности не будет отображаться.

Рисунок 328

С помощью кнопки «Проверить» Вы убедитесь, что соединение с аутентификатором успешно установлено.

Внутренняя база данных

В средах, где отсутствует внешний аутентификатор, можно использовать аутентификатор «Внутренняя база данных». Этот аутентификатор позволяет создавать пользователей и группы вручную для доступа к различным службам рабочего стола и виртуальным приложениям, предоставляемым платформой VDI.

Все пользовательские и групповые данные хранятся в базе данных, к которой подключен сервер VDI (Рисунок 329).

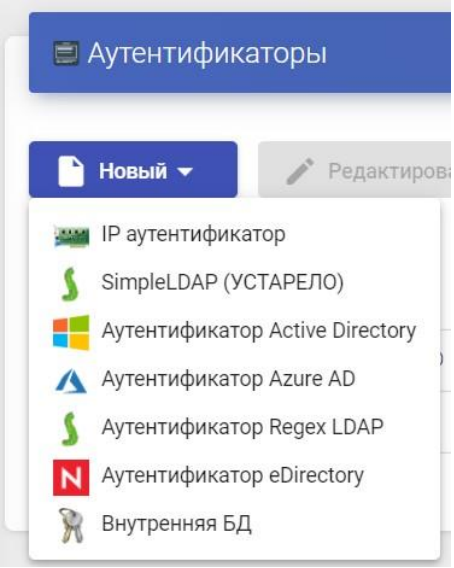


Рисунок 329

В разделе «Внутренняя база данных» настраиваются следующие минимальные параметры (Рисунок 330):

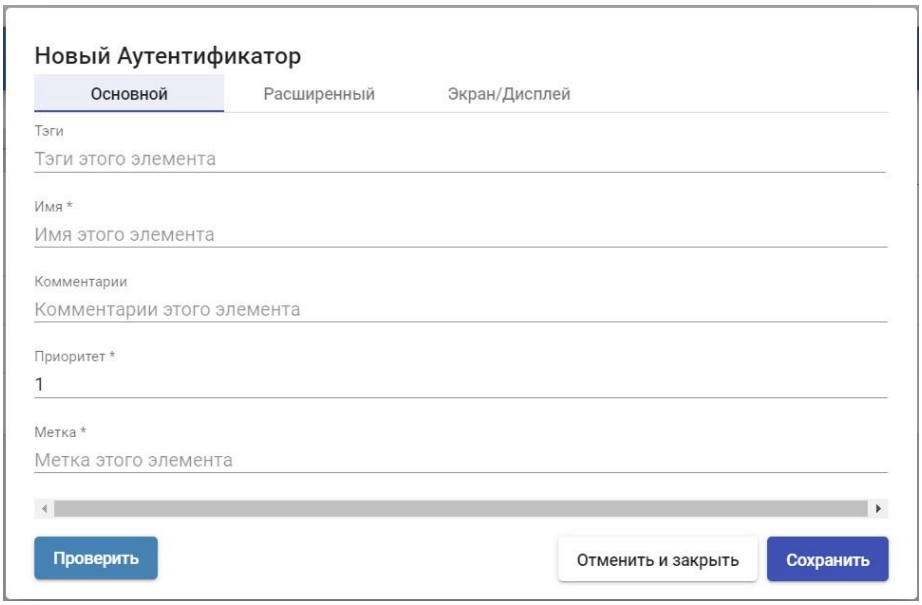


Рисунок 330

▪ Основные:

Имя: Имя аутентификатора.

Приоритет: Приоритет, который будет иметь этот аутентификатор. Чем ниже этот приоритет, тем выше он будет отображаться в списке аутентификаторов, доступных в окне доступа пользователя. В этом поле допускаются отрицательные значения.

Метка: включает прямую проверку в этом средстве проверки подлинности. Это позволяет пользователю проверять подлинность с помощью указанного аутентификатора, хотя среда VDI имеет больше аутентификаторов.

▪ Расширенный (Рисунок 331):

Различные пользователи для каждого хоста: эта опция позволяет подключаться к виртуальным рабочим столам с помощью одного пользователя подключения, добавляя корень к имени существующего пользователя во время подключения к виртуальному рабочему столу. Этот корень является IP-адресом клиента подключения или его DNS-именем.

Новое созданное имя пользователя имеет следующую структуру:

IP-адрес пользователя клиентского общего соединения

Обратный DNS: Он ведет себя точно так же, как параметр «Разные пользователи для каждого хоста», но корень, добавленный к пользователю, является DNS-именем клиента подключения. Требуется правильное разрешение DNS. В противном случае будет использован IP-адрес.

Созданный новый пользователь имеет следующую структуру:

Общее имя клиента подключения пользователя

Разрешить прокси: этот параметр должен быть включен, если перед доступом к серверу VDI имеется компонент, например балансировщик нагрузки.

По умолчанию VDI автоматически определяет IP-адрес клиента подключения. В средах, где сконфигурированы балансировщики нагрузки или другие подобные элементы, это обнаружение выполняется неправильно, так как обнаруженный IP-адрес соответствует этим балансировщикам.

Включив этот параметр, вы получите правильное IP-обнаружение.

В средах, где используется параметр «Разные пользователи для каждого хоста» и имеются балансировщики нагрузки, необходимо включить этот параметр.

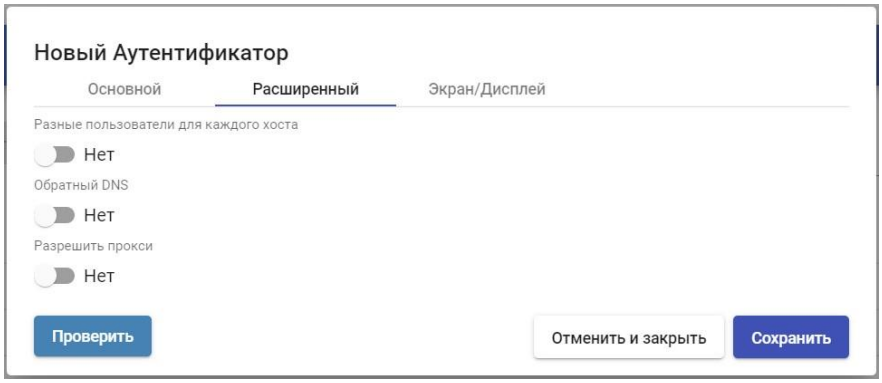


Рисунок 331

▪ Экран/Дисплей (Рисунок 332):

Видимый: если параметр отключен, средство проверки подлинности не будет отображаться как доступное на странице входа в VDI.

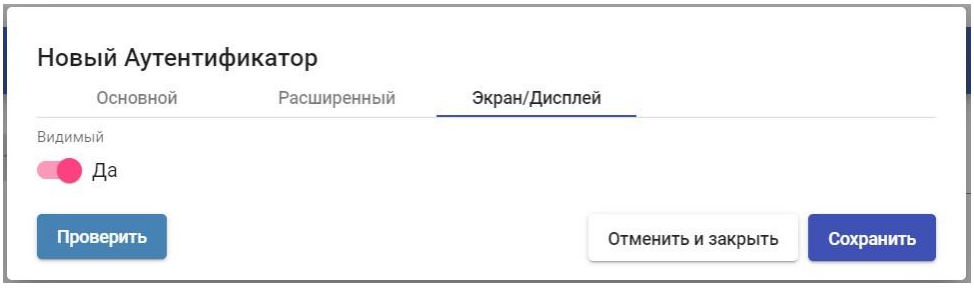


Рисунок 332

IP Аутентификатор

Этот внутренний аутентификатор обеспечивает прямой доступ к клиентам подключения (Single Sign-On) через их IP-адрес к рабочим столам и виртуальным приложениям.

IP-адреса работают как пользователи других аутентификаторов, что позволяет осуществлять прямую проверку клиентов соединения на портале входа в VDI. Группы пользователей в «IP Аутентификатор» могут быть от определенных диапазонов сети до полных подсетей или определенных IPадресов (Рисунок 333).

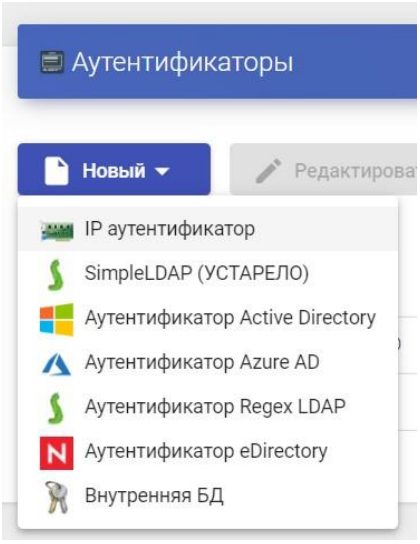


Рисунок 333

В «IP Аутентификатор» настраиваются следующие минимальные параметры (Рисунок 334):

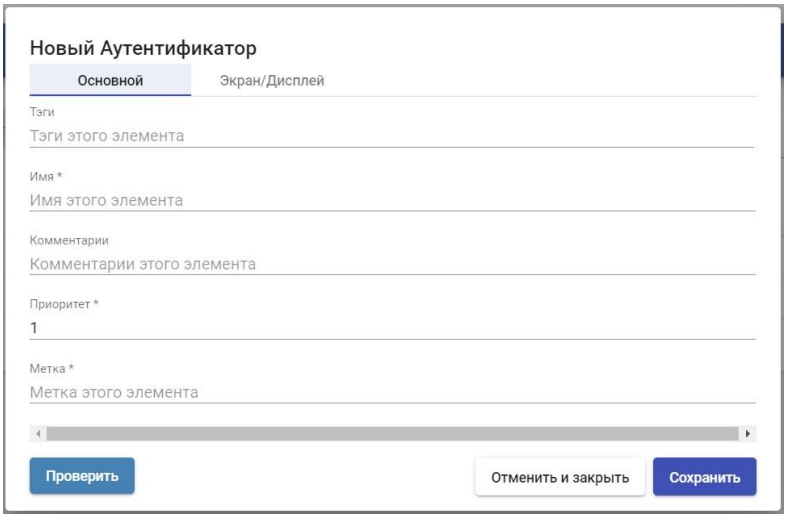


Рисунок 334

▪ Основной:

Имя: Имя аутентификатора.

Приоритет: приоритет, который будет иметь этот аутентификатор. Чем ниже этот приоритет, тем выше он будет отображаться в списке аутентификаторов, доступных в окне доступа пользователя. В этом поле допускаются отрицательные значения.

Метка: включает прямую проверку в этом средстве проверки подлинности. Это позволяет пользователю проверять подлинность с помощью указанного аутентификатора, хотя среда VDI имеет больше аутентификаторов.

▪ Экран/Дисплей (Рисунок 335)

Видимый: если параметр отключен, средство проверки подлинности не будет отображаться как доступное на странице входа в VDI.

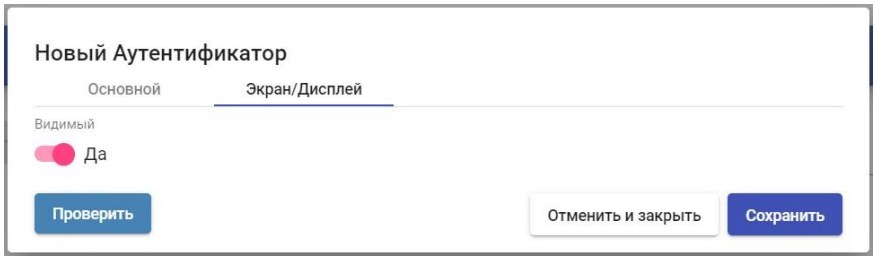


Рисунок 335

Regex LDAP

Этот аутентификатор позволяет пользователям и группам пользователей, принадлежащим практически любому аутентификатору на основе LDAP, получать доступ к виртуальным рабочим столам и приложениям.

В «Regex LDAP Authenticator» минимальными параметрами для настройки являются:

▪ Основной:

Имя: Имя аутентификатора.

Приоритет: Приоритет, который будет иметь этот аутентификатор. Чем ниже этот приоритет, тем выше он будет отображаться в списке аутентификаторов, доступных в окне доступа пользователя. В этом поле допускаются отрицательные значения.

Метка: включает прямую проверку в этом средстве проверки подлинности. Это позволяет пользователю проверять подлинность с помощью указанного аутентификатора, хотя среда VDI имеет больше аутентификаторов.

Хост: IP-адрес или имя сервера LDAP.

Используйте SSL: если включено, SSL-соединение будет использоваться для проверки подлинности.

Тайм-аут: «Тайм-аут» для подключения к аутентификатору.

▪ Учетные данные:

Пользователь: Пользователь с разрешениями на чтение аутентификатора.

Формат: uid =..., ou =...., dc =..., dc =...

Пароль: пароль пользователя.

▪ Сведения о LDAP:

База: Поиск в каталоге, где система будет находить группы и пользователей для проверки в система.

Класс пользователя: общий класс, который должны иметь все пользователи.

Имя пользователя Attr: атрибут LDAP, определяющий имя пользователя для входа в UDS портал доступа.

Attr имени группы: атрибут LDAP, который определяет членство пользователя в группе. Для определения различных атрибутов группы (по одному в каждой строке) могут быть указаны различные атрибуты. Это также позволяет использовать регулярные выражения для извлечения или составления определенных значений.

▪ Дополнительно:

Alt. class: можно указать больше видов объектов для поиска пользователей и групп пользователей.

▪ Отображение:

Visible: Если параметр отключен, средство проверки подлинности не будет отображаться как доступное при входе в UDS страница.

Кнопка «Test» позволяет проверить успешность подключения.

3.6.4.3 Настройка пользователей, групп и метагрупп пользователей

После настройки аутентификатора или аутентификаторов необходимо настроить группы пользователей, содержащие пользователей, которым должен быть предоставлен доступ к службам рабочего стола. Также возможно создание метагрупп, которые будут использоваться для объединения нескольких групп.

Чтобы добавить группы или метагруппы в средство проверки подлинности, выбрать его и дважды щелкните его или выбрать пункт «Подробно» в меню поставщика:

Находясь внутри аутентификатора, перейдите на вкладку «Группы» и в разделе «Создать» выбрать «Группа»:

Имя группы указывается в поле «Group» вместе с ее состоянием (включено или отключено). Кроме того, ее можно непосредственно присвоить одному или нескольким «пулам услуг».

В некоторых средствах проверки подлинности, таких как «Active Directory», будет выполняться автоматический поиск:

В других, таких как «Regex LDAP», «SAML», «eDirectory»... необходимо будет указать его вручную.

Примечание: для внутренних аутентификаторов типа, таких как «Внутренняя база данных» и «IP Authenticator», необходимо будет создавать

группы вручную, так как они не подключаются к какой-либо внешней системе аутентификации.

Доступ к порталу входа в UDS будет предоставлен всем пользователям, входящим в группу (определенного аутентификатора)

Создание групп и пользователей «Внутренняя база данных»

В аутентификаторе типа «Внутренняя база данных» необходимо будет вручную создать группы пользователей, которых вы назначите «Сервиспулу».

Перейдите в ранее созданный аутентификатор «Внутренняя база данных» и на вкладку «Группы» и нажать «Новый» - >«Группа». Указать имя новой группы, ее состояние (включено или отключено), а также назначить ее непосредственно одному или нескольким «пулам услуг» (Рисунок 336).

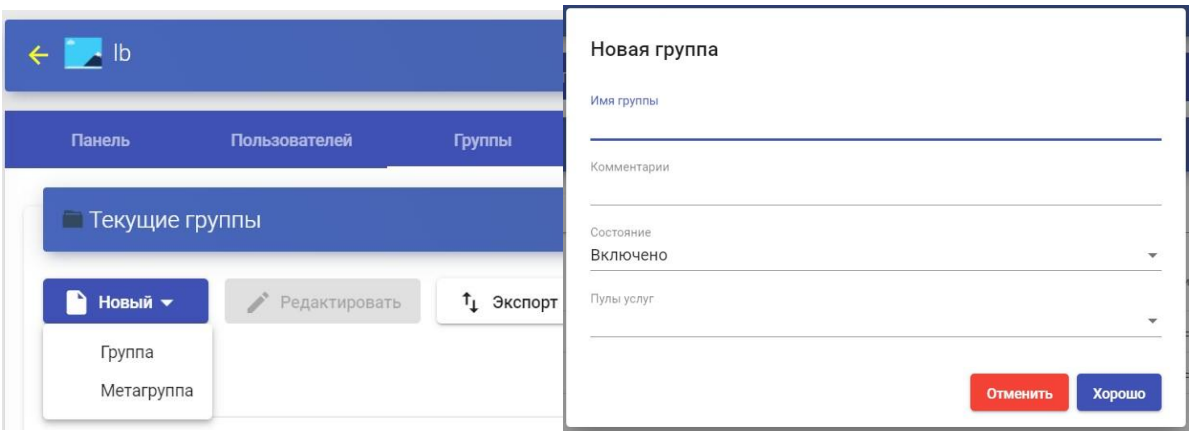


Рисунок 336

Выполнить ту же процедуру, если нужно создать метагруппу.

После того, как создана группа, зарегистрировать пользователей и назначить их одной или нескольким группам. Перейти на вкладку «Пользователи» и нажать «Новый» (Рисунок 337).

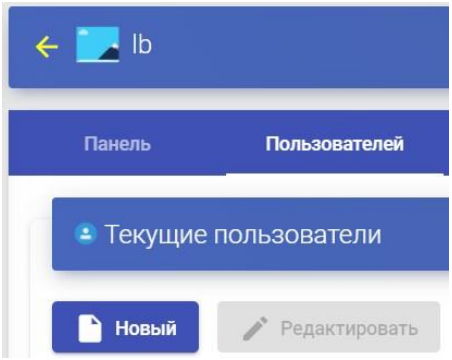


Рисунок 337

Ввести имя нового пользователя, его состояние (включено или отключено), уровень доступа (поле «Роль») и пароль. В поле «Группы» указать, к каким группам он будет принадлежать (можно выбрать одну или несколько из существующих групп) (Рисунок 338).

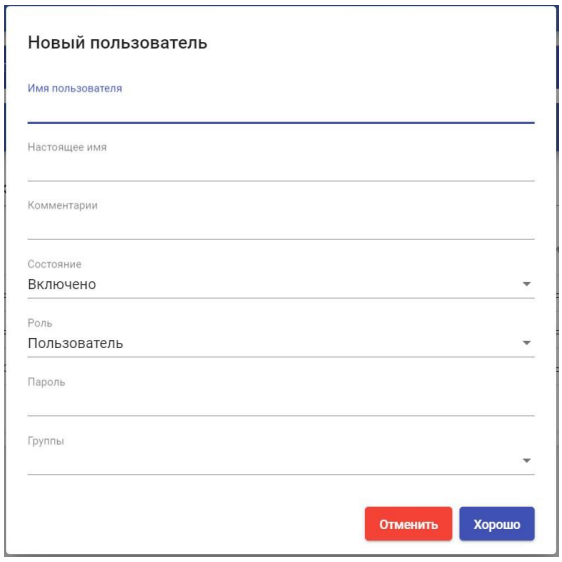


Рисунок 338

Создание групп и пользователей «IP аутентификатор»

В «IP аутентификатор» необходимо вручную создать группы пользователей. В этом случае группа это будет диапазон IP-адресов, полная подсеть или один IP-адрес. В каждом случае использовать следующий формат:

- Уникальный IP-адрес: xxx.xxx.xxx.xxx (например: 192.168.11.33,192.168.11.50)
- Полная подсеть: xxx.xxx.xxx.xxx/x (например: 192.168.11.0/24)
- Диапазон IP-адресов: xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx (Например: 192.168.11.1-192.168.11.155)

Перейти к ранее созданному аутентификатору «IP аутентификатор» и на вкладке «Группы» нажать «Новый» - «Группа» (Рисунок 339).

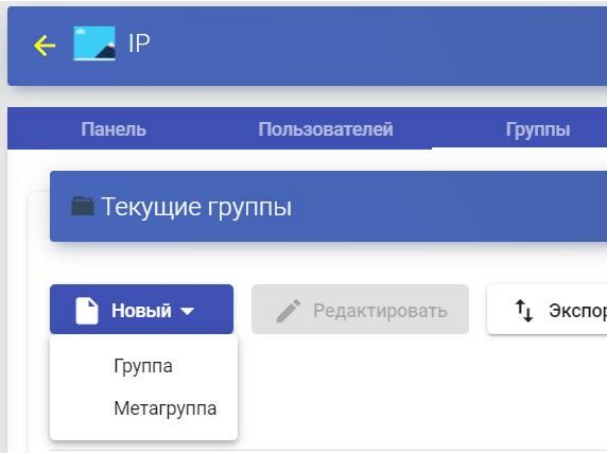


Рисунок 339

Ввести диапазон IP-адресов, полную подсеть или IP-адреса, разделенные запятыми (поле «Диапазон IP»), и их статус (включен или отключен). Можно назначить его непосредственно одному или нескольким «пулам услуг» (Рисунок 340).

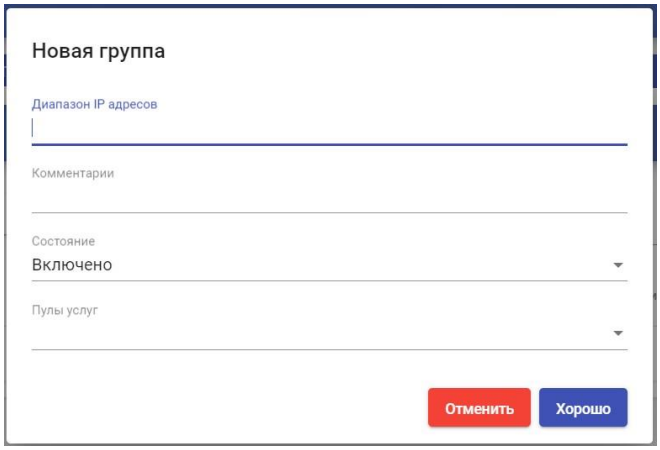


Рисунок 340

Когда пользователь выбирает этот аутентификатор на портале входа в UDS (то есть аутентификатор по умолчанию), система проверяет IP-адрес его клиента подключения. Если этот адрес находится в диапазоне, указанном в группе (поле «Диапазон IP»), пользователь будет автоматически проверен (Рисунок 341).

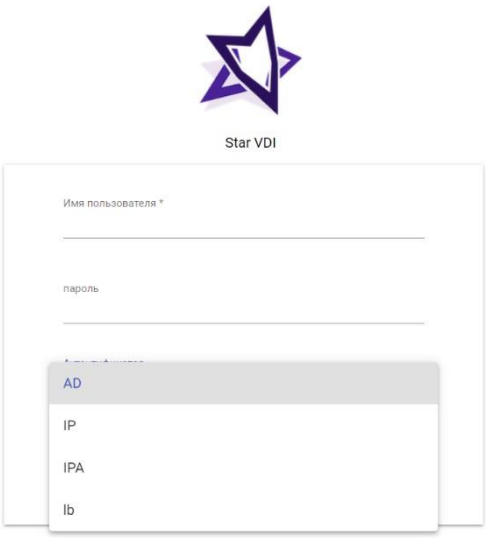


Рисунок 341

Как только пользователь будет проверен на портале входа в систему VDI, его IP-адрес будет автоматически зарегистрирован на вкладке «Пользователи» (Рисунок 342).

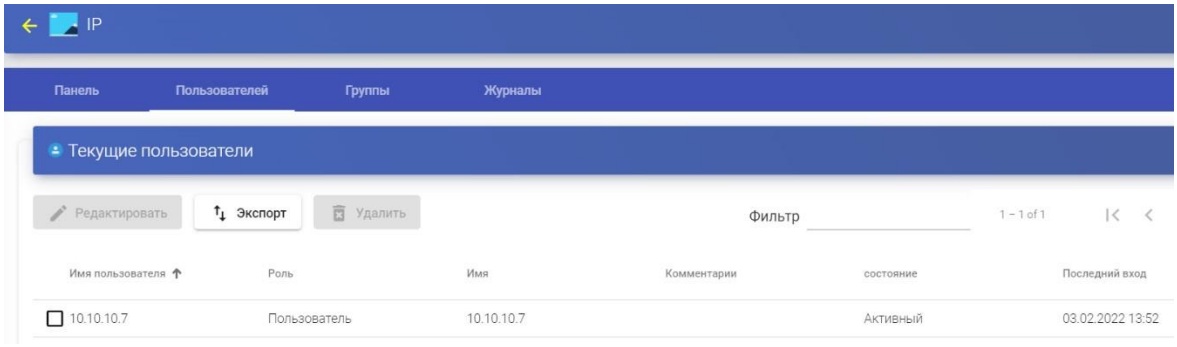


Рисунок 342

Если нужно изменить его статус (включен или отключен) или уровень доступа (поле «Роль»), выбрать его и нажать «Редактировать» (Рисунок 343).

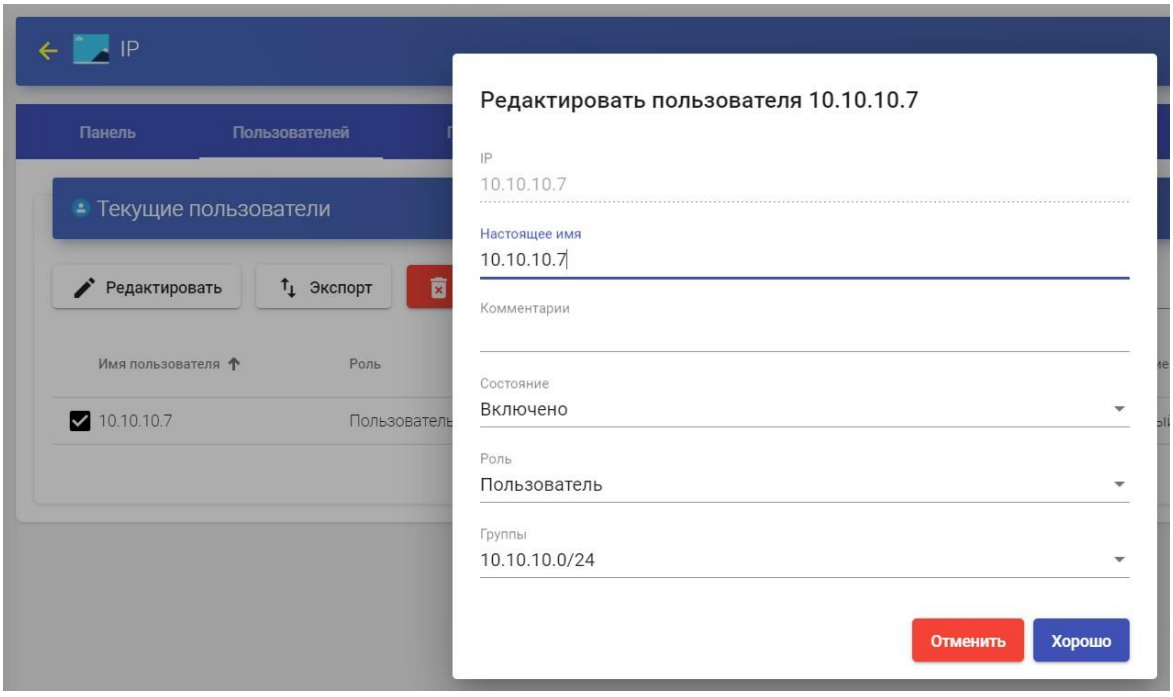


Рисунок 343

3.6.4.4 Настройка «Менеджер ОС»

«Менеджер ОС» запускает ранее настроенный тип службы.

UDS Actor, размещенный на виртуальном рабочем столе или сервере приложений, отвечает за взаимодействие между ОС и сервером VDI на основе выбранных конфигураций или типа «Менеджер ОС».

Можно зарегистрировать столько «Менеджеров ОС», сколько вам нужно на платформе VDI. Можно выбрать различные типы в зависимости от потребностей развертываемых служб (Рисунок 344).

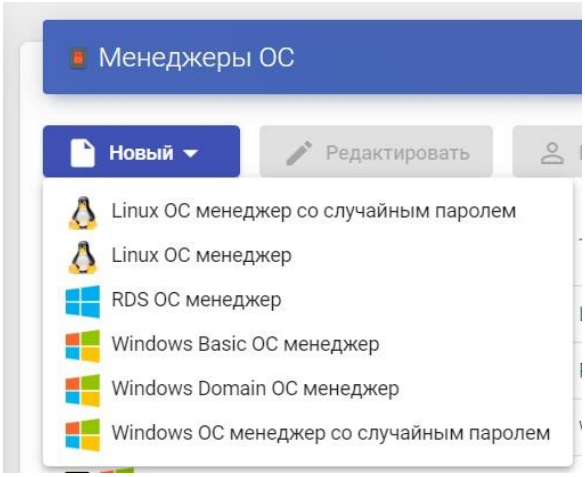


Рисунок 344

Примечание: для любого типа службы, развернутой в VDI, потребуется «Менеджер ОС», за исключением случаев, когда используется провайдер «Поставщик статических IP-машин».

Linux

«Linux ОС менеджер» используется для виртуальных рабочих столов на базе систем Linux. Он выполняет задачи переименования и управления сеансами виртуальных рабочих столов.

Минимальные параметры, которые необходимо настроить в «Linux ОС менеджер», следующие (Рисунок 345):

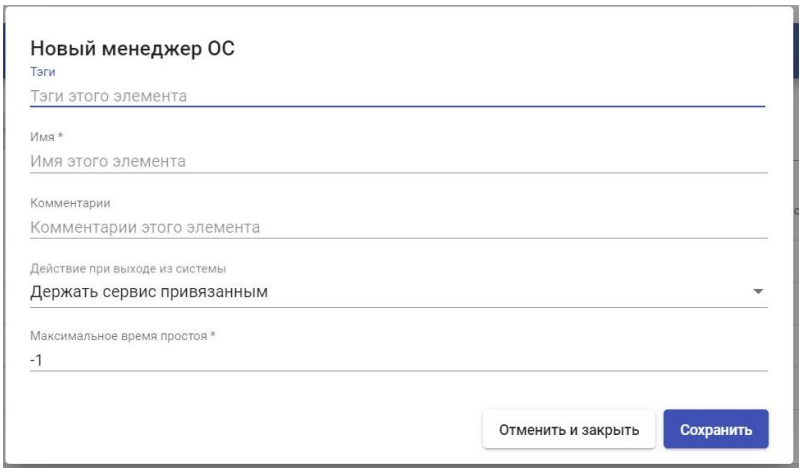


Рисунок 345 Имя:

Имя «Менеджера ОС».

Действие при выходе из системы: указать действие, которое VDI будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя:

▪ Держать сервис привязанным: когда пользователь выходит из виртуального рабочего стола, система не предпринимает никаких действий. При повторном подключении вам будет назначен тот же рабочий стол, с которым вы работали ранее. Если будет произведена новая публикация «Сервисного пула», при выходе пользователя из системы его виртуальный рабочий стол будет удален, и он подключится к новому, сгенерированному в новой версии.

▪ Удалить службу (непостоянная виртуальная машина): когда пользователь выходит из системы, система уничтожает рабочий стол. Если

тот же пользователь снова запросит виртуальную машину в системе, система предоставит новый виртуальный рабочий стол.

▪ Держать сервис привязанным в новой публикации (постоянный виртуальный рабочий стол): когда пользователь выходит из виртуального рабочего стола, система не предпринимает никаких действий. При повторном подключении ему будет назначен тот же рабочий стол, с которым он работал ранее. Если производится новая публикация «Сервис-пула», при выходе пользователя из системы его виртуальный рабочий стол останется назначенным и будет удален только тогда, когда на это укажет администратор.

▪ Максимальное время простоя: Максимальное время (указывается в секундах) бездействия на виртуальном рабочем столе. По истечении этого времени бездействия UDS Actor автоматически закроет сеанс.

Отрицательные значения и менее 300 секунд отключают эту опцию.

Linux со случайным паролем

«Linux ОС менеджер со случайным паролем» используется для виртуальных рабочих столов на базе систем Linux и требует более высокого уровня безопасности при доступе пользователей. Он выполняет задачи по переименованию, управлению сеансом и изменению пароля существующего локального пользователя на виртуальных рабочих столах.

Благодаря его использованию существующему локальному пользователю при настройке каждого нового развернутого виртуального рабочего стола назначается случайный пароль, что обеспечивает более высокий уровень безопасности доступа.

В «Linux ОС менеджер со случайным паролем» минимальные параметры для настройки (Рисунок 346):

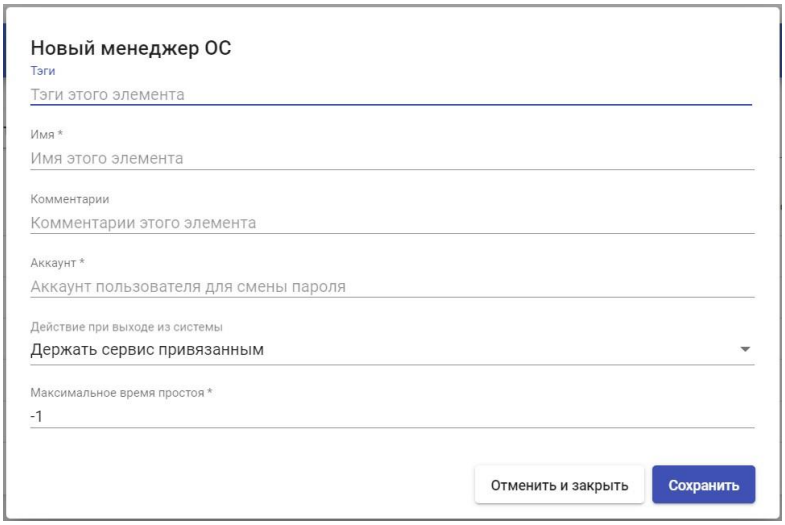


Рисунок 346 Имя:

Имя «Менеджер ОС».

Учетная запись: имя существующего локального пользователя на виртуальном рабочем столе, которому VDI изменит пароль на самостоятельно сгенерированный случайный пароль.

Действие при выходе из системы: вы укажете действие, которое VDI будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя:

▪ Держать сервис привязанным: когда пользователь выходит из виртуального рабочего стола, система не предпринимает никаких действий. При повторном подключении вам будет назначен тот же рабочий стол, с которым вы работали ранее. Если будет произведена новая публикация «Сервисного пула», при выходе пользователя из системы его виртуальный рабочий стол будет удален, и он подключится к новому, сгенерированному в новой версии.

▪ Удалить службу (непостоянная виртуальная машина):Когда пользователь выходит из системы, система уничтожает рабочий стол. Если тот же пользователь снова запросит виртуальную машину в системе, система предоставит новый виртуальный рабочий стол.

▪ Держать сервис привязанным в новой публикации (постоянный виртуальный рабочий стол): когда пользователь выходит из виртуального рабочего стола, система не предпринимает никаких действий. При повторном подключении ему будет назначен тот же рабочий стол, с которым он работал ранее. Если производится новая публикация «Сервис-пула», при выходе пользователя из системы его виртуальный рабочий стол останется назначенным и будет удален только тогда, когда на это укажет администратор.

▪ Максимальное время простоя: Максимальное время (указывается в секундах) бездействия на виртуальном рабочем столе. По истечении этого времени бездействия UDS Actor автоматически закроет сеанс.

Отрицательные значения и менее 300 секунд отключают эту опцию.

RDS

«RDS ОС менеджер» используется для настройки «Сервис-пула», который предоставляет пользователям виртуальное приложение (Рисунок 347).

Минимальные параметры, которые необходимо настроить в «RDS ОС менеджер», следующие (Рисунок 348).

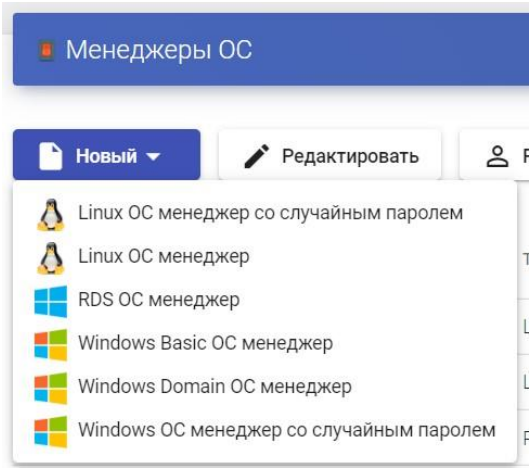


Рисунок 347 Имя:

Имя «Менеджер ОС».

Максимальное время сессии: максимальное время, в течение которого сессия будет оставаться открытым, в часах (0 = не ограничено).

Рисунок 348

Windows Basic ОС менеджер

«Windows Basic ОС менеджер» используется для виртуальных рабочих столов на основе систем Windows, которые не являются частью домена AD. Он выполняет задачи переименования и управления сеансом виртуальных рабочих столов.

Минимальные параметры, которые необходимо настроить в «Windows Basic ОС менеджер», следующие (Рисунок 349):

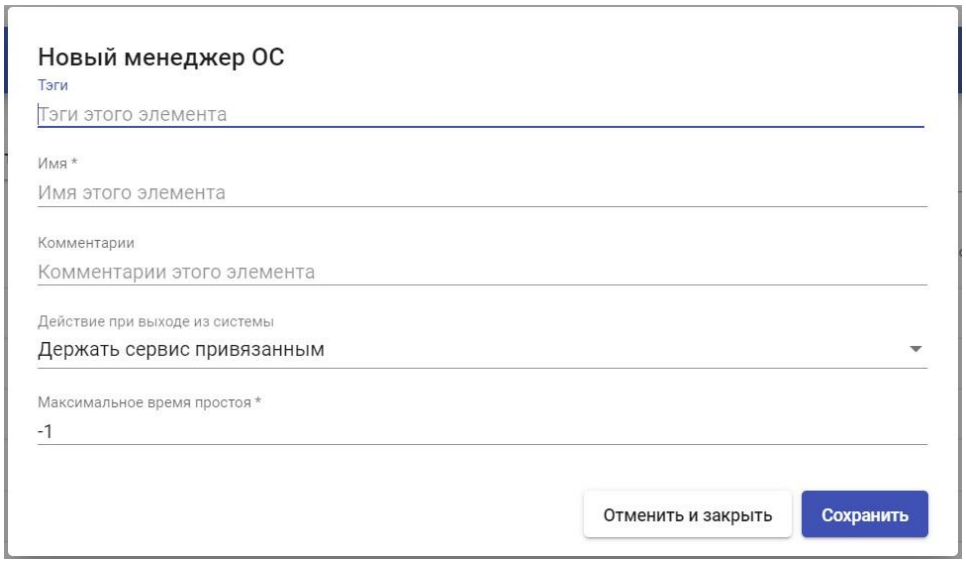


Рисунок 349 Имя:

Имя «Менеджер ОС».

Учетная запись: имя существующего локального пользователя на виртуальном рабочем столе, которому VDI изменит пароль на самостоятельно сгенерированный случайный пароль.

Действие при выходе из системы: указать действие, которое VDI будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя:

▪ Держать сервис привязанным: когда пользователь выходит из виртуального рабочего стола, система не предпринимает никаких действий. При повторном подключении будет назначен тот же рабочий стол, с которым работал ранее. Если будет произведена новая публикация «Сервисного пула», при выходе пользователя из системы его виртуальный рабочий стол будет удален, и он подключится к новому, сгенерированному в новой версии.

▪ Удалить службу (непостоянная виртуальная машина): Когда пользователь выходит из системы, система уничтожает рабочий стол. Если тот же пользователь снова запросит виртуальную машину в системе, система предоставит новый виртуальный рабочий стол.

▪ Держать сервис привязанным в новой публикации (постоянный виртуальный рабочий стол): когда пользователь выходит из виртуального рабочего стола, система не предпринимает никаких действий. При повторном подключении ему будет назначен тот же рабочий стол, с которым он работал ранее. Если производится новая публикация «Сервис-пула», при выходе пользователя из системы его виртуальный рабочий стол останется назначенным и будет удален только тогда, когда на это укажет администратор.

▪ Максимальное время простоя: Максимальное время (указывается в секундах) бездействия на виртуальном рабочем столе. По истечении этого времени бездействия UDS Actor автоматически закроет сеанс.

Отрицательные значения и менее 300 секунд отключают эту опцию.

Windows Domain менеджер

«Windows Domain ОС менеджер» используется для виртуальных рабочих столов на основе систем Windows, которые являются частью домена AD. Он выполняет переименование, регистрацию домена AD и управление сеансом на виртуальных рабочих столах.

В «Windows Domain ОС менеджер» необходимо настроить следующие минимальные параметры (Рисунок 350):

▪ Основной:

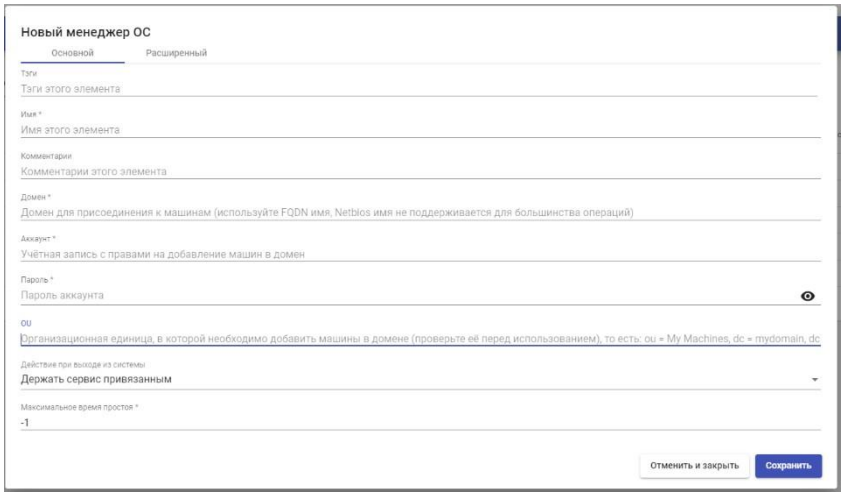


Рисунок 350 Имя:

Имя «Менеджер ОС».

Домен: имя домена AD, к которому будут присоединены виртуальные рабочие столы.

Учетная запись: имя пользователя с правами на добавление машин в домен. Пароль: Пароль пользователя в поле «Учетная запись».

OU: Организационная единица, в которой будут зарегистрированы виртуальные рабочие столы (если ничего не указано, рабочие столы будут зарегистрированы в организационной единице по умолчанию «Компьютеры»). Формат поддерживаемой OU:

OU=name_OU_last_level,… OU=name_OU_first_level, DC=name_domain, DC=extension_domain

Во избежание ошибок при введении формата рекомендуется сверяться с полем «distinguishedName» в свойствах атрибута OU (Рисунок 351).

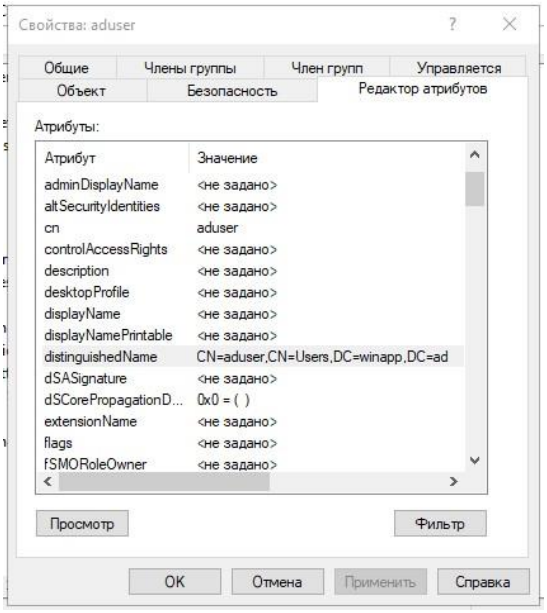


Рисунок 351

Действие при выходе из системы: указать действие, которое VDI будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя:

▪ Держать сервис привязанным: когда пользователь выходит из виртуального рабочего стола, система не предпринимает никаких действий. При повторном подключении будет назначен тот же рабочий стол, с которым работал ранее. Если будет произведена новая публикация «Сервисного пула», при выходе пользователя из системы его виртуальный рабочий стол будет удален, и он подключится к новому, сгенерированному в новой версии.

▪ Удалить службу (непостоянная виртуальная машина): Когда пользователь выходит из системы, система уничтожает рабочий стол. Если тот же пользователь снова запросит виртуальную машину в системе, система предоставит новый виртуальный рабочий стол.

▪ Держать сервис привязанным в новой публикации (постоянный виртуальный рабочий стол): когда пользователь выходит из виртуального рабочего стола, система не предпринимает никаких действий. При повторном подключении ему будет назначен тот же рабочий стол, с которым он работал ранее. Если производится новая публикация «Сервис-пула», при выходе пользователя из системы его виртуальный рабочий стол останется назначенным и будет удален только тогда, когда на это укажет администратор.

▪ Максимальное время простоя: Максимальное время (указывается в секундах) бездействия на виртуальном рабочем столе. По истечении этого времени бездействия UDS Actor автоматически закроет сеанс.

Отрицательные значения и менее 300 секунд отключают эту опцию. ▪ Расширенный (Рисунок 352):

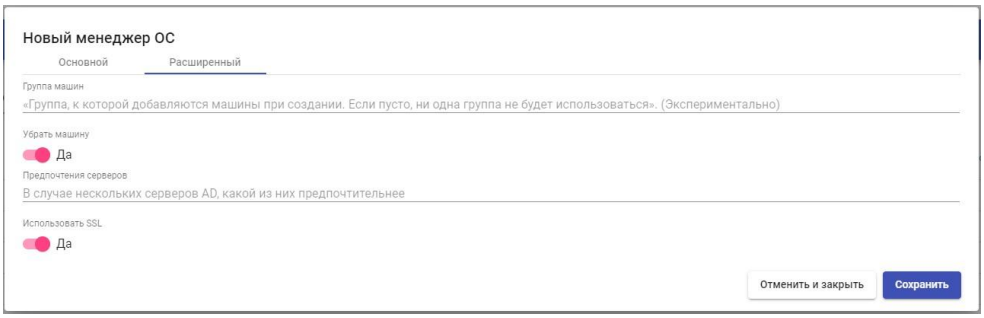


Рисунок 352

Группа машин: указывает, к какой группе машин AD будут добавлены виртуальные рабочие столы, созданные VDI.

Убрать машину: если этот параметр включен, VDI удалит записи виртуальных рабочих столов в указанном подразделении после удаления рабочего стола.

Предпочтения серверов: если серверов AD несколько, будет указано, какой из них использовать предпочтительнее.

Использовать SSL: если этот параметр включен, SSL-соединение будет использоваться для сервера AD.

Windows со случайным паролем

«Windows ОС менеджер со случайным паролем» используется для виртуальных рабочих столов на базе систем Windows и требует более высокого уровня безопасности при доступе пользователей. Он выполняет задачи по переименованию, управлению сеансом и изменению пароля существующего локального пользователя на виртуальных рабочих столах.

Благодаря его использованию существующему локальному пользователю при настройке каждого нового развернутого виртуального рабочего стола назначается случайный пароль, что обеспечивает более высокий уровень безопасности доступа.

Минимальные параметры, которые необходимо настроить в Windows ОС менеджер со случайным паролем (Рисунок 353):

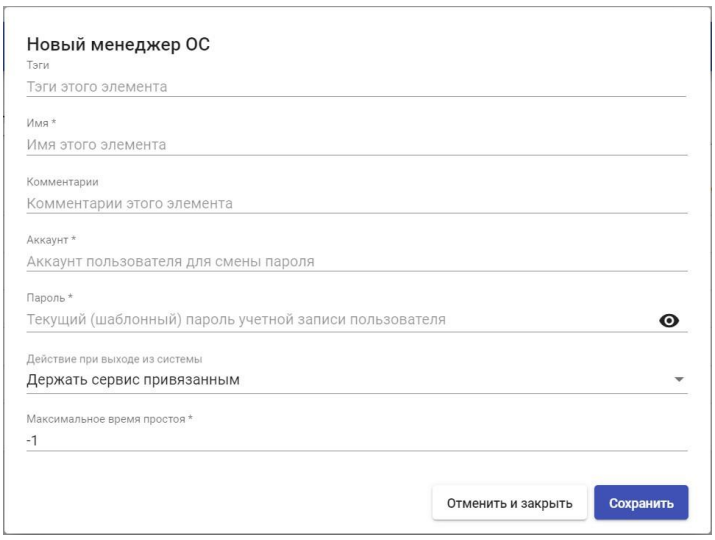


Рисунок 353

Имя: Имя «Менеджер ОС».

Учетная запись: имя существующего локального пользователя на виртуальном рабочем столе, которому VDI изменит пароль на самостоятельно сгенерированный случайный пароль.

Действие при выходе из системы: указать действие, которое VDI будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя:

Пароль: Пароль пользователя в поле «Учетная запись».

▪ Держать сервис привязанным: когда пользователь выходит из виртуального рабочего стола, система не предпринимает никаких действий. При повторном подключении будет назначен тот же рабочий стол, с которым работал ранее. Если будет произведена новая публикация «Сервисного пула», при выходе пользователя из системы его виртуальный рабочий стол будет удален, и он подключится к новому, сгенерированному в новой версии.

▪ Удалить службу (непостоянная виртуальная машина): Когда пользователь выходит из системы, система уничтожает рабочий стол. Если тот же пользователь снова запросит виртуальную машину в системе, система предоставит новый виртуальный рабочий стол.

▪ Держать сервис привязанным в новой публикации (постоянный виртуальный рабочий стол): когда пользователь выходит из виртуального рабочего стола, система не предпринимает никаких действий. При повторном подключении ему будет назначен тот же рабочий стол, с которым он работал ранее. Если производится новая публикация «Сервис-пула», при выходе пользователя из системы его виртуальный рабочий стол останется

назначенным и будет удален только тогда, когда на это укажет администратор.

▪ Максимальное время простоя: Максимальное время (указывается в секундах) бездействия на виртуальном рабочем столе. По истечении этого времени бездействия UDS Actor автоматически закроет сеанс.

Отрицательные значения и менее 300 секунд отключают эту опцию.

3.6.4.5 Транспорт

Для подключения к виртуальным рабочим столам и приложениям необходимо создать «Транспорты». Это приложения, которые будут выполняться на клиенте подключения и будут отвечать за предоставление доступа к реализованной службе.

В зависимости от типа виртуального рабочего стола, который настраивается, местоположения и устройства, используемого для подключения к виртуальным рабочим столам, потребуется создать различные типы транспорта.

Клиент соединения и сервер рабочего стола/приложений должны установить протокол соединения (клиент-сервер), используемый в транспорте, чтобы транспорт работал правильно.

Для доступа к разделу «Транспорт» перейти в раздел «Подключение» и выбрать «Транспорт». В настоящее время доступны следующие (Рисунок 354):

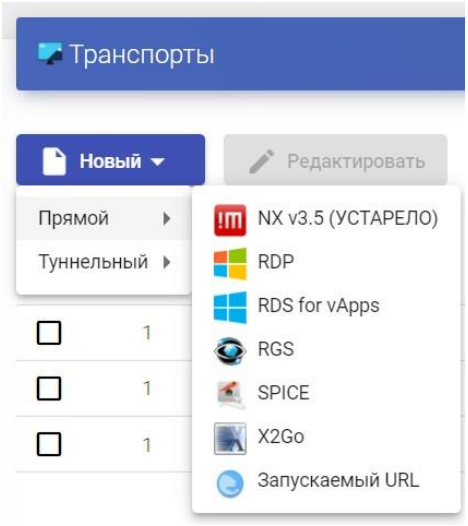


Рисунок 354 ▪

Прямой:

«Транспорты», указанные как «Прямой», будут использоваться для доступа пользователей к виртуальным рабочим столам и приложениям из внутренней локальной сети, VPN, расширения локальной сети и т. д.

NX v3.5 (прямой)

Транспорт «NX v3.5» позволяет пользователям получать доступ к виртуальным рабочим столам Linux с помощью программного обеспечения NX (как клиенты подключения, так и виртуальные рабочие столы должны иметь установленную версию NX 3.5).

Загрузку программного обеспечения NX 3.5 следует запросить в службе поддержки.

Минимальные параметры для настройки транспорта "NX v3.5":

▪ Основное (Рисунок 355):

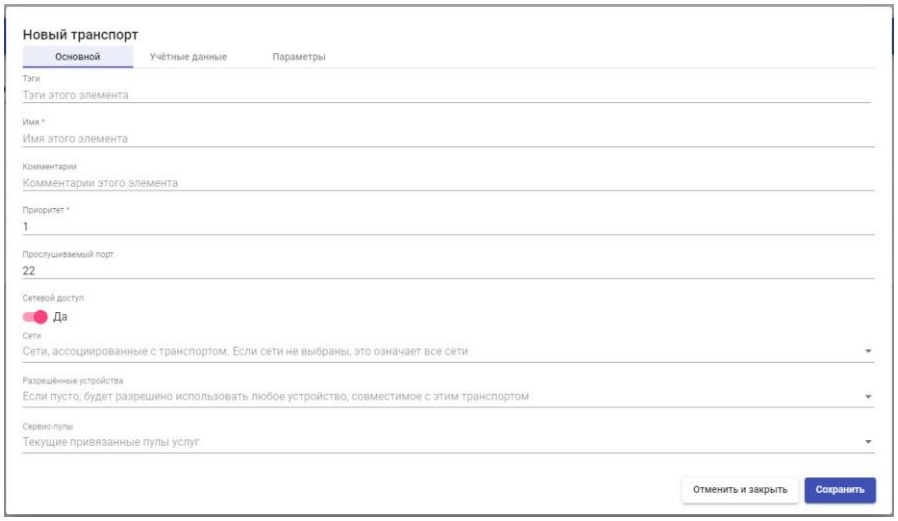


Рисунок 355 Имя:

Имя транспорта.

Приоритет: приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортов для службы. Транспорт с наименьшим приоритетом будет использоваться по умолчанию при нажатии на изображение сервиса.

Порт прослушивания: порт прослушивания программного обеспечения NX.

Доступ к сети: разрешает или запрещает доступ пользователя к службе в зависимости от сети, из которой он осуществляет доступ, и сети, указанной в поле «Сети».

Сети: диапазоны сетей, подсети или IP-адреса, указанные в разделе «Сети» раздела «Подключение». Он используется вместе с полем «Доступ к сети», чтобы разрешить или запретить доступ пользователя к службе в зависимости от его местоположения в сети.

Разрешенные устройства: разрешает доступ к услуге только с выбранных устройств. Если ничего не выбрано, фильтрация не выполняется.

Сервисные пулы: позволяет назначать этот транспорт непосредственно одному или нескольким ранее созданным «сервисным пулам».

▪ Учетные данные (Рисунок 356):

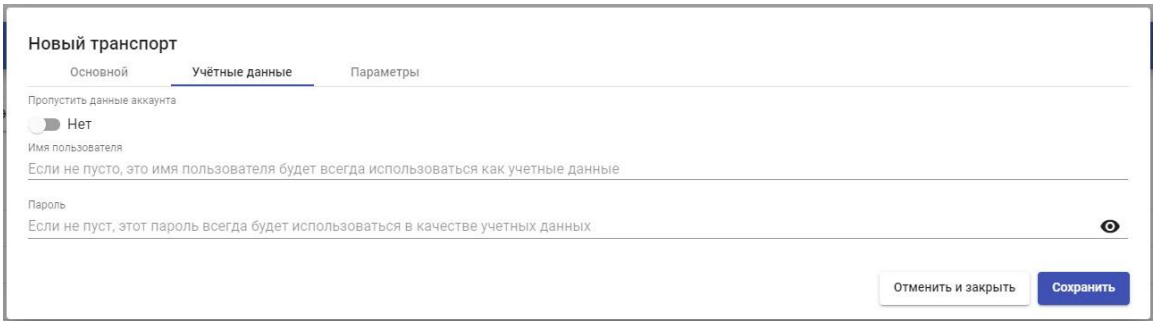


Рисунок 356

Пустые учетные данные: если для него установлено значение «Да», при подключении к службе будут запрашиваться учетные данные для доступа к виртуальному рабочему столу. Если установлено значение «Нет», учетные данные, введенные на портале входа в VDI, будут перенаправлены. Имя пользователя: имя пользователя, которое будет использоваться для входа на рабочий стол (пользователь должен существовать на рабочем столе). Если это поле пусто, будет предпринята попытка использовать пользователя для входа в портал VDI, если в поле «Пустые учетные данные» установлено значение «Нет», или будут запрошены учетные данные, чтобы указать их вручную, если установлено значение «Да».

Пароль: пароль пользователя в поле «Имя пользователя».

▪ Параметры (Рисунок 357):

Рисунок 357 Подключение:

Качество соединения.

Сессия: сеанс рабочего стола по умолчанию.

Дисковый кэш: размер кэша, хранящегося на диске.

Кэш памяти: размер кэша, хранящегося в памяти.

Размер экрана: Размер окна соединения.

RDP (прямой)

Транспорт «RDP» (прямой) позволяет пользователям получать доступ к виртуальным рабочим столам Windows/Linux с помощью протокола удаленного рабочего стола (RDP). Как клиенты подключения, так и виртуальные рабочие столы должны иметь установленный и включенный протокол RDP (для виртуальных рабочих столов Linux необходимо использовать XRDP).

В «RDP» (прямом) транспорте минимальные параметры для настройки:

▪ Основное (Рисунок 358):

Рисунок 358 Имя:

Имя транспорта.

Приоритет: приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортов для службы. Транспорт с наименьшим приоритетом будет использоваться по умолчанию при нажатии на изображение сервиса.

Сетевой доступ: разрешает или запрещает доступ пользователя к службе в зависимости от сети, из которой он осуществляет доступ, и сети, указанной в поле «Сети».

Сети: диапазоны сетей, подсети или IP-адреса, указанные в разделе «Сети» раздела «Подключение». Он используется вместе с полем «Доступ к сети», чтобы разрешить или запретить доступ пользователя к службе в зависимости от его местоположения в сети.

Разрешенные устройства: разрешает доступ к услуге только с выбранных устройств. Если ничего не выбрано, фильтрация не выполняется.

Сервис-пулы: позволяет назначать этот транспорт непосредственно одному или нескольким ранее созданным «сервис-пулам».

▪ Учетные данные (Рисунок 359):

Рисунок 359

Пропустить данные аккаунта: если для него установлено значение «Да», при подключении к службе он запросит у вас учетные данные для доступа к виртуальному рабочему столу. Если установлено значение «Нет», учетные данные, введенные на портале входа в VDI, будут перенаправлены.

Имя пользователя: имя пользователя, которое будет использоваться для входа на рабочий стол (пользователь должен существовать на рабочем столе). Если это поле пусто, будет предпринята попытка использовать пользователя для входа в портал VDI, если в поле «Пустые учетные данные» установлено значение «Нет», или будут запрошены учетные данные, чтобы указать их вручную, если установлено значение «Да».

Пароль: пароль пользователя в поле «Имя пользователя».

Без домена: указывает, перенаправляется ли имя домена вместе с пользователем.

Домен: имя домена, которое будет отправлено с учетными данными пользователя.

▪ Параметры (Рисунок 360):

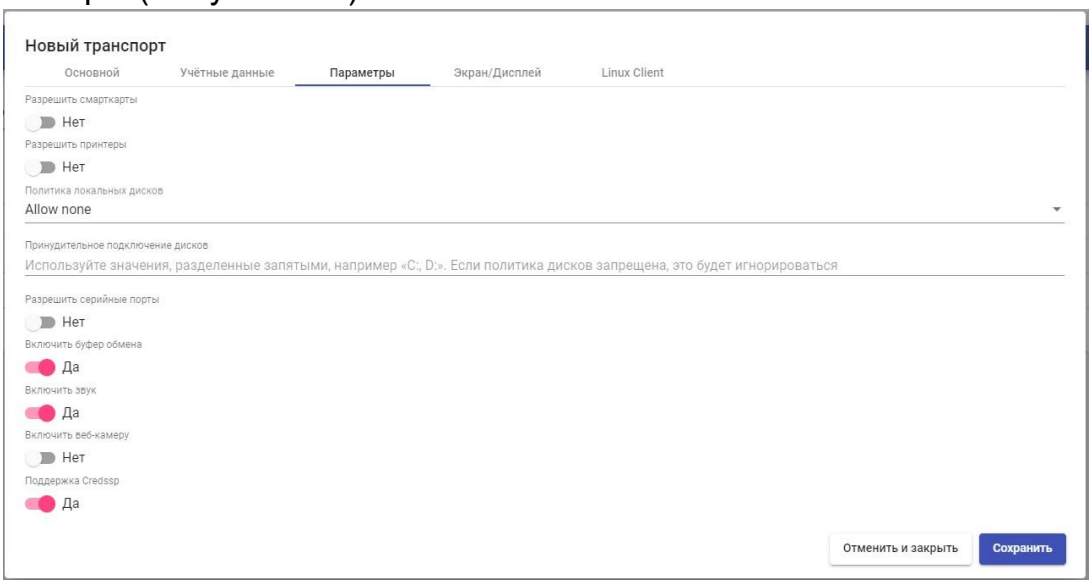


Рисунок 360

Разрешить смарт-карты: включает перенаправление смарт-карт.

Разрешить принтеры: включает перенаправление принтеров.

Политика локальных дисков: включает перенаправление дисков:

▪ Allow none: ни один диск не перенаправляется.

▪ Allow PnP drives: во время активного сеанса перенаправляются только подключенные диски.

▪ Allow any drive: Все диски перенаправляются.

Принудительное подключение дисков: принудительно перенаправляет определенные диски. Можно указать несколько через запятую. (Пример: F:, G:).

Разрешить серийные порты: включить перенаправление последовательного порта.

Включить буфер обмена: если он активирован, он позволит копировать/вставлять между клиентом подключения и рабочим столом.

Включить звук: если он активирован, это позволит перенаправить звук с рабочего стола на клиент подключения.

Включить веб-камеру: если эта функция включена, это позволит перенаправлять веб-камеры между клиентом подключения и рабочим столом.

Поддержка Credssp: если он активирован, он будет использовать «Поставщика поддержки безопасности учетных данных».

▪ Дисплей (Рисунок 361)

Рисунок 361

Размер экрана: определяет размер окна рабочего стола.

Глубина цвета: указывает глубину цвета.

Обои/тема: отображает фон рабочего стола.

Несколько мониторов: позволяет использовать несколько мониторов.

Разрешить композицию рабочего стола: Включает «Композицию рабочего стола».

Сглаживание шрифтов: активирует сглаживание шрифта.

Окно подключения: позволяет включать или отключать панель подключения.

▪ Клиент Linux (Рисунок 362):

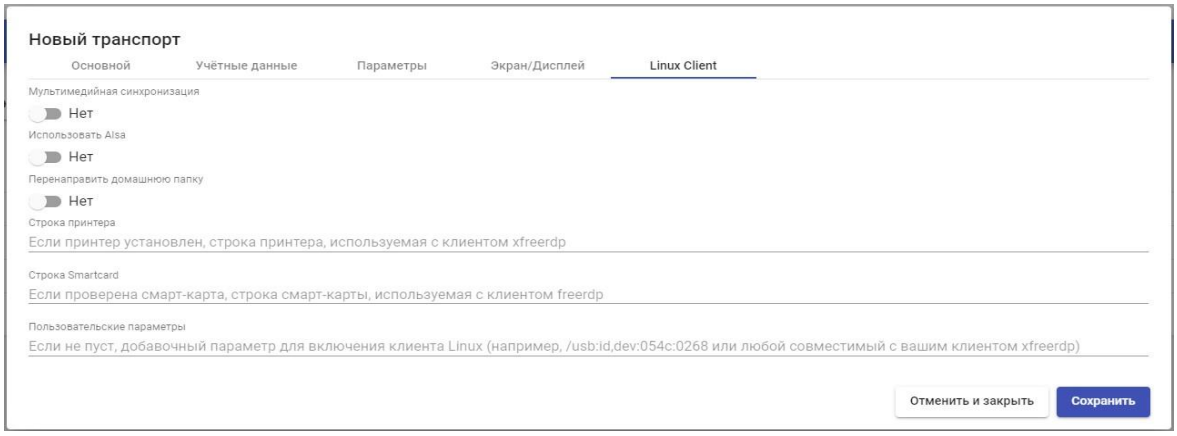


Рисунок 362

Синхронизация мультимедиа: включает параметр мультимедиа в клиенте FreeRDP.

Использовать Alsa: позволяет использовать аудио через Alsa.

Перенаправить домашнюю папку: если она активна, домашняя страница пользователя клиента подключения будет перенаправлена на виртуальный рабочий стол.

Строка принтера: пример: "Zebra", "ZDesigner TM400 200 dpi (ZPL)" ("Zebra" — имя локального принтера, "ZDesigner TM400 200 dpi (ZPL)" — точное имя драйвера принтера в Windows).

Строка смарт-карты: Пример: «Gemalto PC Twin Reader 00 00» («Gemalto PC Twin Reader 00 00» — это название смарт-карты).

Пользовательские параметры: вы можно указать любой параметр, поддерживаемый клиентом FreeRDP. Они будут применяться при подключении к виртуальному рабочему столу.

RDS для виртуальных приложений (прямое)

Транспорт «RDS для vAPP» (прямой) позволяет пользователям получать доступ к виртуальным приложениям Windows с помощью RemoteAPP.

Клиентами подключения могут быть Windows или Linux.

Клиент подключения Windows должен иметь RemoteAPP для открытия виртуальных приложений. Клиент подключения Linux должен иметь пакет freerdp2 для открытия виртуальных приложений.

В транспорте «RDS для vAPP» (прямом) минимальные параметры для настройки:

▪ Основное (Рисунок 363):

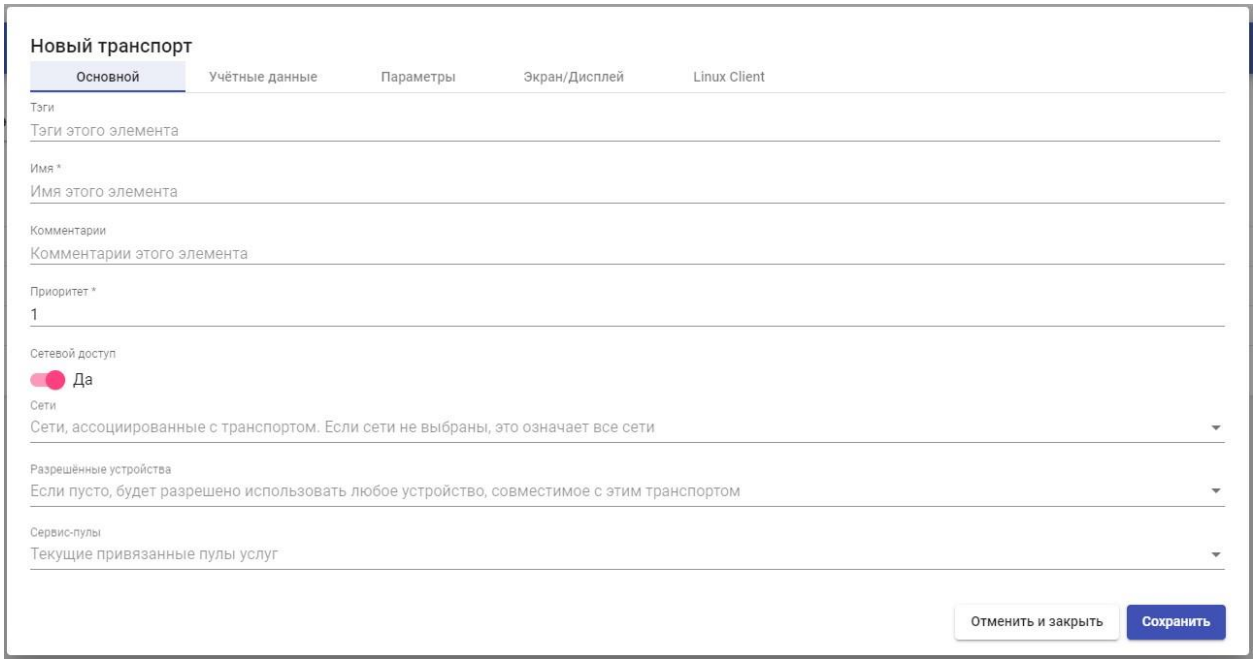


Рисунок 363 Имя:

Имя транспорта.

Приоритет: приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортов для службы. Транспорт с наименьшим приоритетом будет использоваться по умолчанию при нажатии на изображение сервиса.

Сетевой доступ: разрешает или запрещает доступ пользователя к службе в зависимости от сети, из которой он осуществляет доступ, и сети, указанной в поле «Сети».

Сети: диапазоны сетей, подсети или IP-адреса, указанные в разделе «Сети» раздела «Подключение». Он используется вместе с полем «Доступ к сети», чтобы разрешить или запретить доступ пользователя к службе в зависимости от его местоположения в сети.

Разрешенные устройства: разрешает доступ к услуге только с выбранных устройств. Если ничего не выбрано, фильтрация не выполняется.

Сервис-пулы: позволяет назначать этот транспорт непосредственно одному или нескольким ранее созданным «сервис-пулам».

▪ Учетные данные (Рисунок 364):

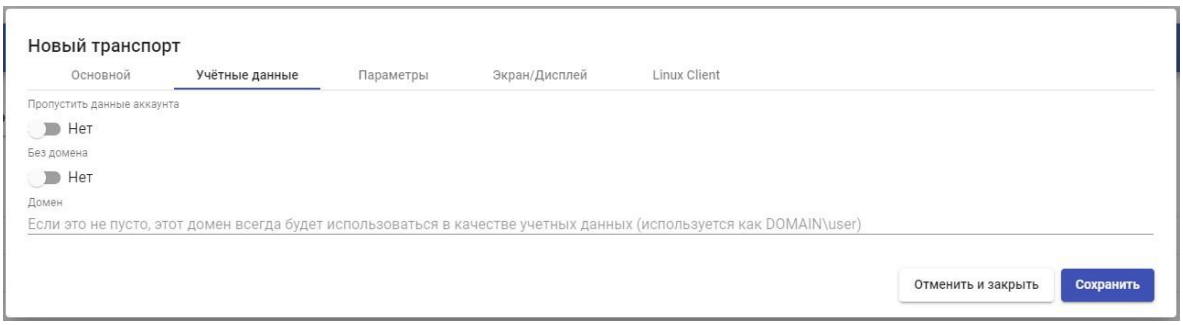


Рисунок 364

Пропустить данные аккаунта: если для него установлено значение «Да», при подключении к службе он запросит у вас учетные данные для доступа к виртуальному рабочему столу. Если установлено значение «Нет», учетные данные, введенные на портале входа в VDI, будут перенаправлены.

Без домена: указывает, перенаправляется ли имя домена вместе с пользователем.

Домен: имя домена, которое будет отправлено с учетными данными пользователя.

▪ Параметры (Рисунок 365):

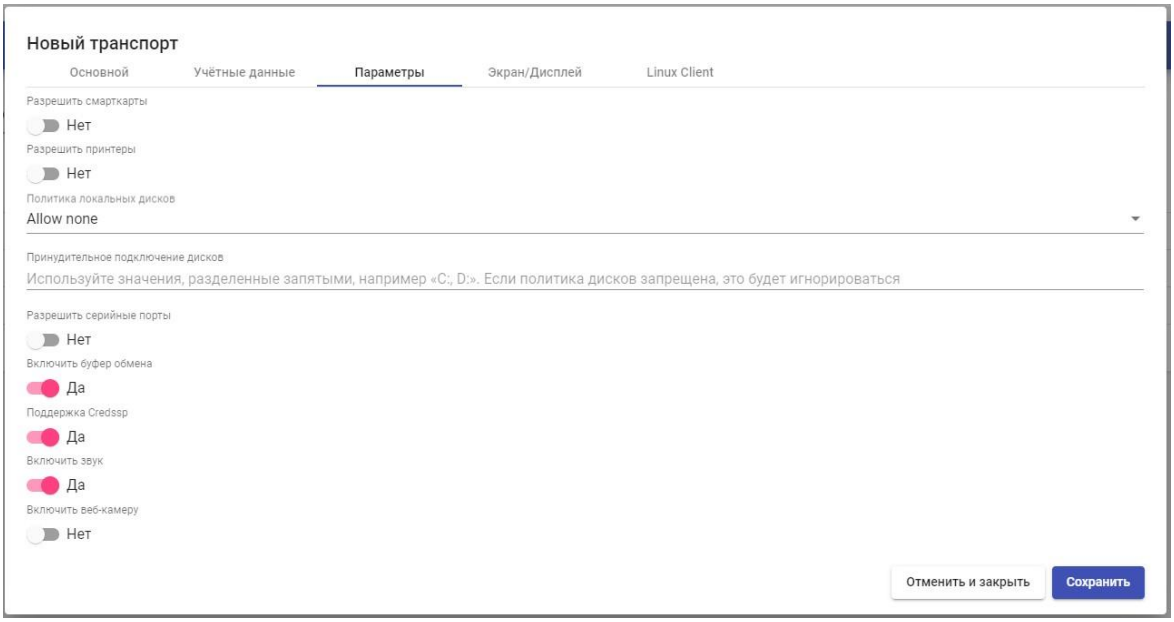


Рисунок 365

Разрешить смарт-карты: Включает перенаправление смарт-карт.

Разрешить принтеры: включает перенаправление принтеров.

Политика локальных дисков: Включает перенаправление дисков:

▪ Allow none: Ни один диск не перенаправляется.

▪ Allow PnP drives: во время активного сеанса перенаправляются только подключенные диски.

▪ Allow any drive: Все диски перенаправляются.

Принудительное подключение дисков: Принудительно перенаправляет определенные диски. Можно указать несколько через запятую. (Пример: F:, G:).

Разрешить серийные порты: включить перенаправление последовательного порта.

Включить буфер обмена: если он активирован, он позволит копировать/вставлять между клиентом подключения и рабочим столом.

Поддержка Credssp: если он активирован, он будет использовать «Поставщика поддержки безопасности учетных данных».

Включить звук: если он активирован, это позволит перенаправить звук с рабочего стола на клиент подключения.

Включить веб-камеру: если эта функция включена, это позволит перенаправлять веб-камеры между клиентом подключения и рабочим столом.

▪ Дисплей (Рисунок 366)

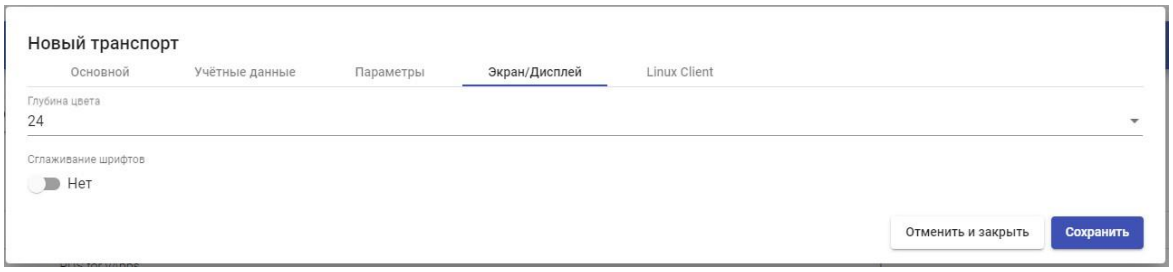


Рисунок 366 Глубина

цвета: указывает глубину цвета.

Сглаживание шрифтов: активирует сглаживание шрифта.

▪ Клиент Linux (Рисунок 367):

Рисунок 367

Execute as shell: если флажок установлен, клиент Linux будет выполнять приложение в сеансе вместо удаленного приложения.

Мультимедийная синхронизация: включает параметр мультимедиа в клиенте FreeRDP.

Использовать Alsa: позволяет использовать аудио через Alsa.

Перенаправить домашнюю папку: если она активна, домашняя страница пользователя клиента подключения будет перенаправлена на виртуальный рабочий стол.

Строка принтера: пример: "Zebra", "ZDesigner TM400 200 dpi (ZPL)" ("Zebra" — имя локального принтера, "ZDesigner TM400 200 dpi (ZPL)" — точное имя драйвера принтера в Windows).

Строка смарт-карты: Пример: «Gemalto PC Twin Reader 00 00» («Gemalto PC Twin Reader 00 00» — это название смарт-карты).

Пользовательские параметры: вы можно указать любой параметр, поддерживаемый клиентом FreeRDP. Они будут применяться при подключении к виртуальному рабочему столу.

RGS (прямой)

Транспорт «RGS» (прямой) позволяет пользователям получать доступ к виртуальным рабочим столам Windows/Linux с помощью протокола Remote Graphics Software (RGS). Как на клиентах подключения, так и на виртуальных рабочих столах должно быть установлено и включено программное обеспечение RGS.

В транспорте «RGS» (прямом) минимальные параметры для настройки:

▪ Основное (Рисунок 368):

Рисунок 368 Имя:

Имя транспорта.

Приоритет: приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортов для службы. Транспорт с наименьшим приоритетом будет использоваться по умолчанию при нажатии на изображение службы.

Сетевой доступ: разрешает или запрещает доступ пользователя к службе в зависимости от сети, из которой он осуществляет доступ, и сети, указанной в поле «Сети».

Сети: диапазоны сетей, подсети или IP-адреса, указанные в разделе «Сети» раздела «Подключение». Он используется вместе с полем «Доступ к сети», чтобы разрешить или запретить доступ пользователя к службе в зависимости от его местоположения в сети.

Разрешенные устройства: разрешает доступ к услуге только с выбранных устройств. Если ничего не выбрано, фильтрация не выполняется.

Сервисные пулы: позволяет назначать этот транспорт непосредственно одному или нескольким ранее созданным «сервисным пулам».

▪ Учетные данные (Рисунок 369):

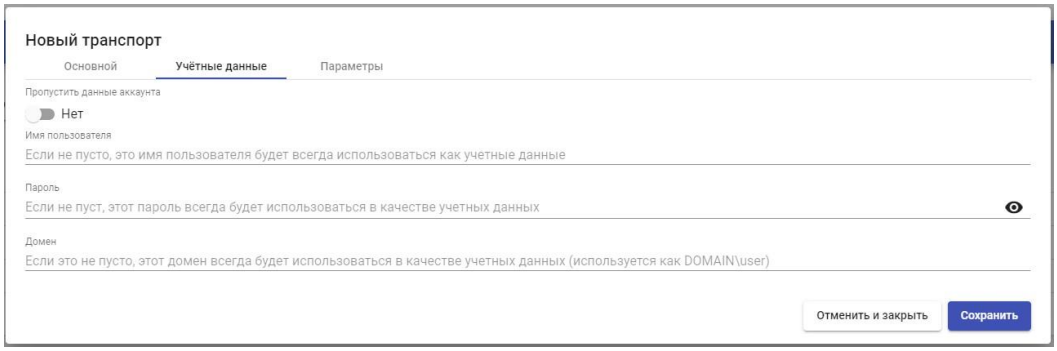


Рисунок 369

Пустые учетные данные: если для него установлено значение «Да», при подключении к службе он запросит у вас учетные данные для доступа к

виртуальному приложению. Если установлено значение «Нет», учетные данные, введенные на портале входа в VDI, будут перенаправлены.

Имя пользователя: имя пользователя, которое будет использоваться для входа на рабочий стол (пользователь должен существовать на рабочем столе). Если это поле пусто, будет предпринята попытка использовать логин портала VDI пользователя, если в поле «Пустые учетные данные» установлено значение «Нет», или запросит учетные данные, чтобы указать их вручную, если установлено значение «Да».

Пароль: пароль пользователя в поле «Имя пользователя».

Домен: доменное имя, которое будет отправлено вместе с учетными данными пользователя.

▪ Параметры (Рисунок 370):

Рисунок 370

Качество изображения: качество изображения в диапазоне от 0 до 100.

Регулируемое качество: если эта функция включена, качество изображения будет автоматически доступная пропускная способность в сети.

Мин. Регулируемое качество: минимальное качество изображения.

Регулируемая частота кадров: коэффициент автонастройки изображения.

Соответствие локальному разрешению: регулирует разрешение экрана клиента и сервера.

Перенаправление USB: если включено, перенаправляет устройство, подключенное через USB в клиенте подключения, на виртуальный рабочий стол.

Перенаправление аудио: если этот параметр включен, звук перенаправляется с клиента подключения на виртуальный рабочий стол.

Перенаправление микрофона: если этот параметр включен, микрофон клиента подключения перенаправляется на виртуальный рабочий стол.

SPICE (прямой)

Транспорт «SPICE» (прямой) позволяет пользователям получать доступ к виртуальным рабочим столам Windows/Linux с использованием протокола

«SPICE». На клиентах подключения должен быть установлен клиент SPICE (Virt-Manager).

Транспорт «SPICE» может использоваться с поставщиком услуг Иридиум.

В транспорте «SPICE» (прямом) минимальные параметры для настройки:

▪ Основное (Рисунок 371):

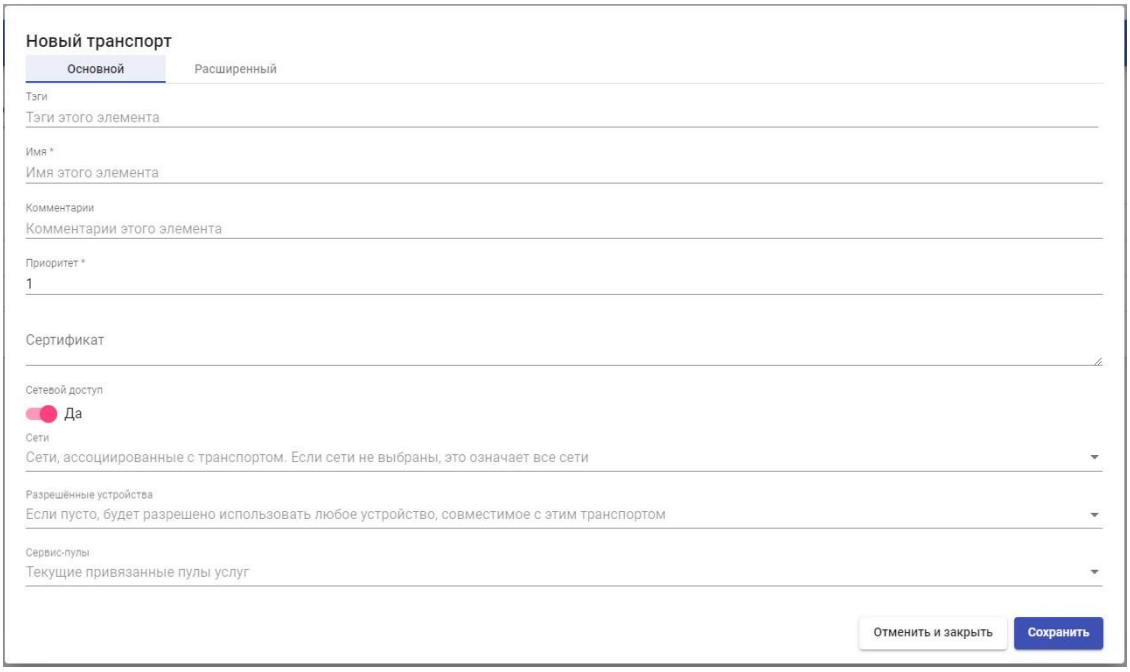


Рисунок 371

Имя: Имя транспорта.

Приоритет: приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортов для службы. Транспорт с наименьшим приоритетом будет использоваться по умолчанию при нажатии на изображение службы.

Сертификат: сертификат, сгенерированный в ovirt-engine/rhev-manager или в OpenNebula. Требуется для подключения к виртуальным рабочим столам (обычно размещенным в /etc/pki/ovirtengine/certs/ca.cer).

Сетевой доступ: разрешает или запрещает доступ пользователя к службе в зависимости от сети, из которой осуществляется доступ, и сети, указанной в поле «Сети».

Сети: диапазоны сетей, подсети или IP-адреса, указанные в разделе «Сети» раздела «Подключение». Он используется вместе с полем «Доступ к

сети», чтобы разрешить или запретить доступ пользователя к службе в зависимости от его местоположения в сети.

Разрешенные устройства: разрешает доступ к услуге только с выбранных устройств. Если ничего не выбрано, фильтрация не выполняется.

Сервис-пулы: позволяет назначать этот транспорт непосредственно одному или нескольким ранее созданным «сервис-пулам».

▪ Дополнительно (Рисунок 372):

Рисунок 372

Полноэкранный режим: включает полноэкранный режим виртуального рабочего стола.

Перенаправление смарт-карт: включает перенаправление смарт-карт на виртуальном рабочем столе.

Включить USB: разрешает перенаправление устройств, подключенных к порту USB.

Новый USB автообмен: позволяет перенаправлять PnP-устройства, подключенные к USB-порту.

X2Go (прямой)

Транспорт «X2Go» (прямой) позволяет пользователям получать доступ к виртуальным рабочим столам Linux с помощью программного обеспечения «X2Go».

Как на клиентах подключения (клиент), так и на виртуальных рабочих столах (сервер) должен быть установлен и включен «X2Go».

В транспорте «X2Go» (прямом) минимальные параметры для настройки:

▪ Основное (Рисунок 373):

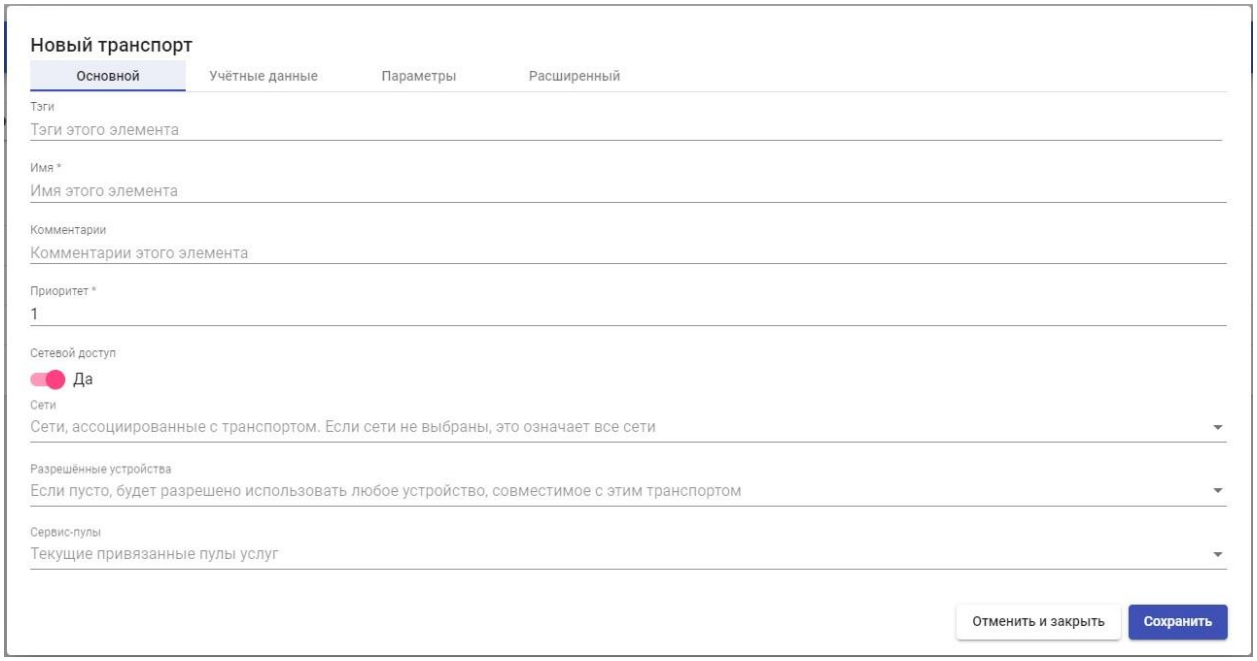


Рисунок 373 Имя:

Имя транспорта.

Приоритет: приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортов для службы. Транспорт с наименьшим приоритетом будет использоваться по умолчанию при нажатии на изображение службы.

Сетевой доступ: разрешает или запрещает доступ пользователя к службе в зависимости от сети, из которой осуществляется доступ, и сети, указанной в поле «Сети».

Сети: диапазоны сетей, подсети или IP-адреса, указанные в разделе «Сети» раздела «Подключение». Он используется вместе с полем «Доступ к сети», чтобы разрешить или запретить доступ пользователя к службе в зависимости от его местоположения в сети.

Разрешенные устройства: разрешает доступ к услуге только с выбранных устройств. Если ничего не выбрано, фильтрация не выполняется.

Сервис-пулы: позволяет назначать этот транспорт непосредственно одному или нескольким ранее созданным «сервис-пулы».

▪ Учетные данные (Рисунок 374):

Имя пользователя: имя пользователя, которое будет использоваться для входа в виртуальный рабочий стол.

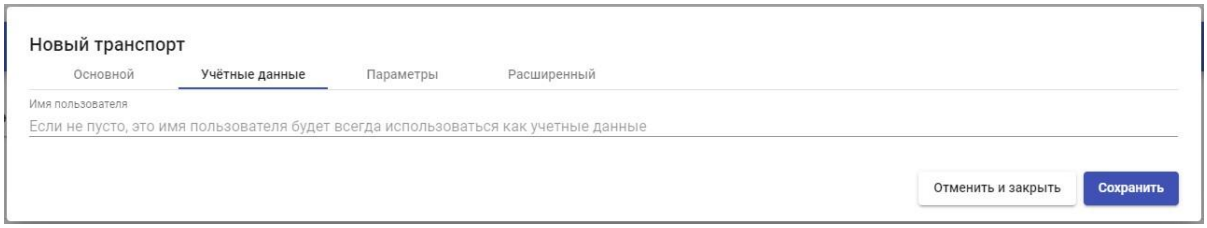


Рисунок 374 ▪

Параметры (Рисунок 375):

Рисунок 375

Размер экрана: Разрешение окна подключения.

Экран: выбор менеджера рабочего стола (xfce, Mate, Gnome и т. д.) или виртуализация приложений Linux (UDS vAPP).

vAPP: Путь выполнения приложения для виртуализации (применяется только в том случае, если для параметра «Рабочий стол» выбрано «UDS vAPP»).

Включить звук: включает звук в соединении.

Перенаправить домашнюю папку: перенаправляет пользователя из /home.

Скорость: Оптимизация соединения.

▪ Дополнительно (Рисунок 376):

Звук: Выбор типа звукового сервера.

Клавиатура: Язык клавиатуры.

Рисунок 376

3.6.4.6 Сервис-пулы

Создание «Сервис-пула» позволит развертывать десктопные сервисы или виртуальные приложения, которые будут доступны для доступа различным группам пользователей.

Необходимыми элементами для создания «Пулов услуг» являются «Базовая служба» (состоящая из «Поставщиков услуг» + служба, созданная в ней) и «Менеджер ОС». После создания вам нужно будет назначить одну или несколько групп пользователей и один или несколько транспортов, чтобы разрешить доступ пользователей.

Чтобы создать «Пул услуг», перейдите в раздел «Пулы» и выбрать «Пул услуг».

Для настройки «Сервисного пула» необходимо будет указать:

▪ Основной (Рисунок 377):

Рисунок 377

Имя: имя «пула услуг» (это имя будет показано пользователю для доступа к его рабочему столу или виртуальному приложению).

Короткое имя: если указано, это будет имя службы, которое будет показано пользователю. При наведении на него появится содержимое поля «Имя».

Базовый сервис: используемая базовая служба (виртуальный рабочий стол или приложение). Он состоит из поставщика услуг и базовой службы, предварительно настроенной в разделе «Услуги».

ОС менеджер: ранее созданный «ОС менеджер», конфигурация которого будет применяться к каждому из созданных виртуальных рабочих столов. В случае публикации сервиса vAPP он также потребуется. Но если вы используете услугу типа «Статический IP», это поле использоваться не будет.

Публиковать при создании: если этот параметр включен, при сохранении пула сервисов система автоматически запустит первую

публикацию. Если установлено «Нет», необходимо будет запустить публикацию сервиса вручную (из вкладки «Публикации»).

▪ Дисплей (Рисунок 378):

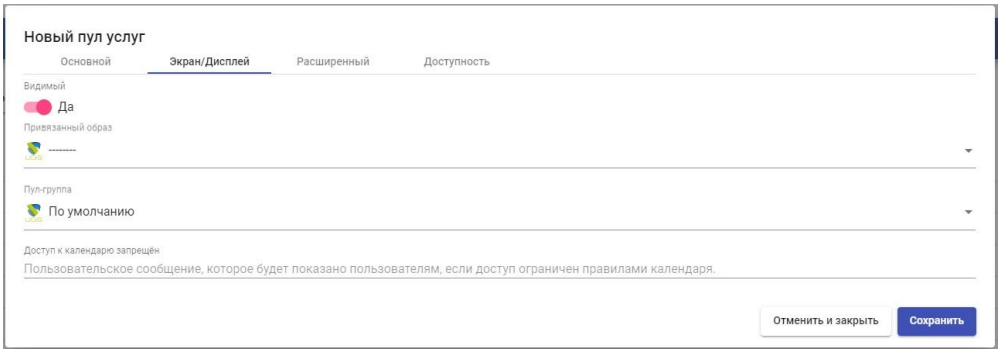


Рисунок 378

Видимый: если этот параметр отключен, «Пул служб» не будет отображаться как доступный для пользователей на странице служб UDS («Режим пользователя»).

Привязанный образ: изображение, связанное с сервисом. Его необходимо предварительно добавить в хранилище изображений, доступное из раздела «Инструменты» — «Галерея».

Пул-группа: позволяет группировать различные услуги. Для назначения

«Группы пула» ее необходимо предварительно создать в разделе «Пулы» — «Группы».

Доступ к календарю запрещён: текст, который будет отображаться, когда доступ к службе запрещен приложением календаря доступа.

▪ Дополнительно (Рисунок 379):

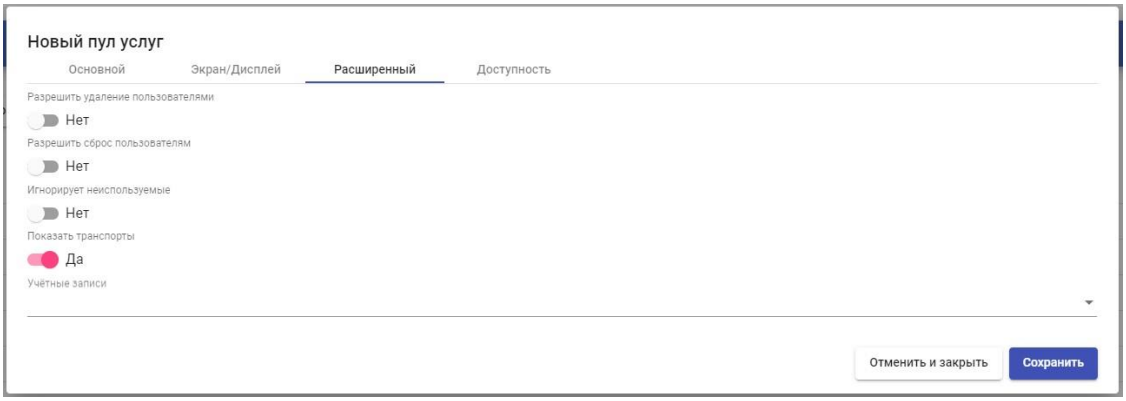


Рисунок 379

Разрешить удаление пользователями: если этот параметр включен, пользователи могут удалять назначенные им службы. Если сервис представляет собой виртуальный рабочий стол, автоматически сгенерированный UDS, он будет удален, и при следующем подключении ему будет назначен новый. Если это другой тип сервиса (vAPP / статический IP), назначение будет только удалено, а новое будет назначено на следующее подключение.

Разрешить сброс пользователями: если он активирован, пользователь сможет перезапускать или сбрасывать назначенные ему службы (относится только к виртуальным рабочим столам, автоматически созданным UDS).

Игнорирует неиспользуемые: если этот параметр включен, непостоянные пользовательские службы, которые не используются, не будут удалены.

Показать транспорты: если эта опция активирована, будут отображаться все транспорты, назначенные услуге. Если он не активирован, будет отображаться только транспорт по умолчанию с наивысшим приоритетом (наименьшее число в поле «приоритет» транспорта).

Учетные записи: назначение услуги ранее созданным «Аккаунтам» («Пулы»

— «Аккаунты»)

▪ Доступность (Рисунок 380):

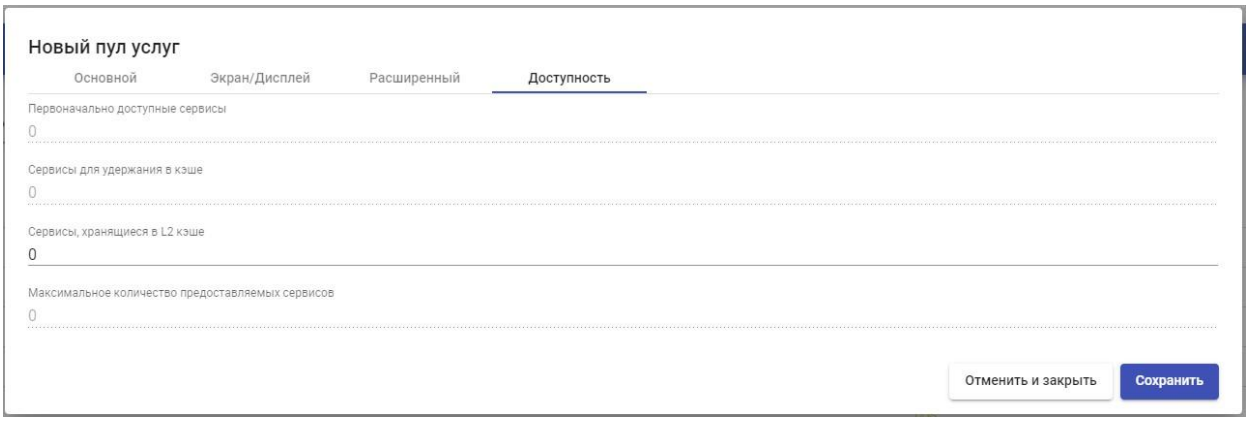


Рисунок 380

Первоначально доступные сервисы: минимальное количество виртуальных рабочих столов, созданных, настроенных и назначенных/доступных для службы.

Сервисы для удержания в кэше: количество доступных виртуальных рабочих столов. Они всегда будут настроены и готовы к назначению пользователю (они будут генерироваться автоматически, пока не будет достигнуто максимальное количество машин, указанное в поле «Максимальное количество услуг для предоставления»).

Сервисы, хранящиеся в L2 кэше: количество виртуальных рабочих столов в спящем или выключенном состоянии. Эти рабочие столы будут настроены и готовы к размещению, когда системе потребуются новые кэшированные рабочие столы. Виртуальные рабочие столы, сгенерированные на уровне кэша L2, будут помещены в кэш, как только

система потребует их. Они никогда не будут напрямую назначены пользователям.

Максимальное количество предоставляемых сервисов: максимальное количество виртуальных рабочих столов, созданных системой в «пуле сервисов» (рабочие столы, созданные в кэше L2, не будут учитываться).

Сохраните «Сервис-пул», и система начнет генерировать виртуальные рабочие столы на основе настроенного кеша (вкладка «Availability»).

С помощью кнопки «Удалить» вы можно полностью удалить «Сервис-пул», а с помощью «Редактировать» вы можно изменить его (Рисунок 381).

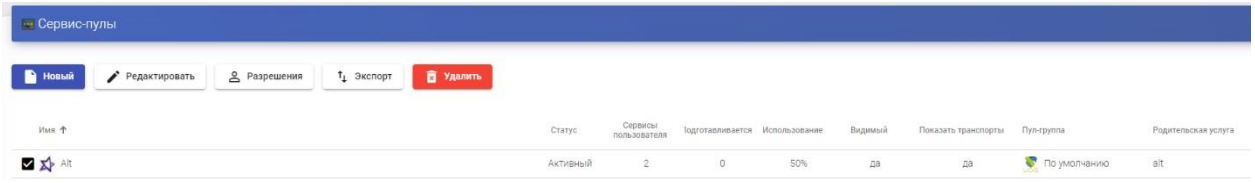


Рисунок 381

Перейти в созданный «Сервис-пул», в разделе «Публикации» (если вы отметили опцию «Публикация при создании»), система запустится с публикацией службы, создающей базовую машину, на которой будут основаны виртуальные рабочие столы (Рисунок 382).

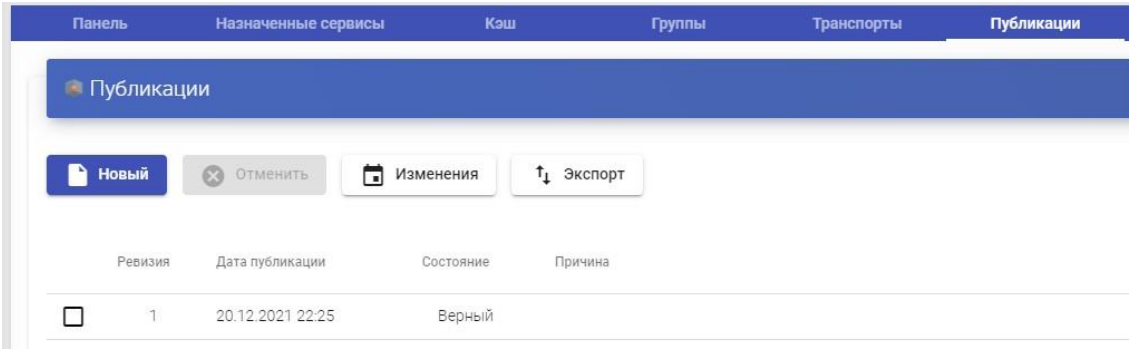


Рисунок 382

После того, как создан «Сервис-пул», при доступе к нему есть следующие меню управления и настройки:

▪ Назначенные сервисы: виртуальные рабочие столы, назначенные пользователям. Отображает информацию о дате создания рабочего стола, номере ревизии (или публикации), на которой создан рабочий стол, MACадрес сетевой карты ВМ, DNS и IP-имя виртуального рабочего стола, статус рабочего стола, если он используется, имя и IP-адрес клиента подключения, владелец машины и версия UDS Actor, установленного на машине-шаблоне (Рисунок 383).

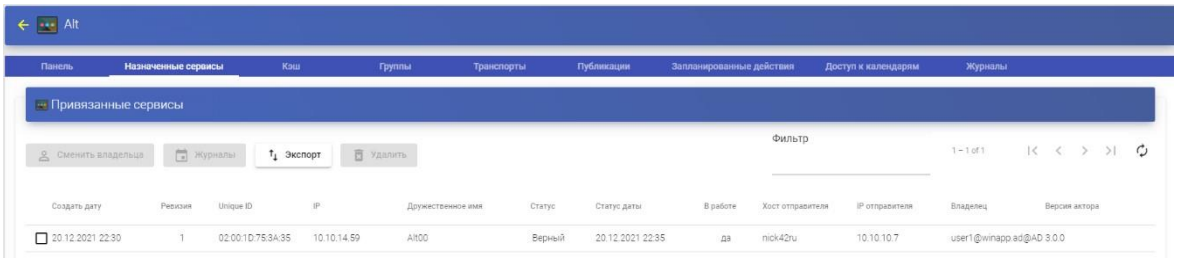


Рисунок 383

Выбрав виртуальный рабочий стол и нажав «Сменить владельца», можно изменить пользователя, назначенного рабочему столу.

Нажав «Удалить», можно удалить его вручную, а в «Журналах» сохранится вся информация, сообщенная «UDS Actor», установленного на рабочем столе.

▪ Кэш: виртуальные рабочие столы, доступные для подключения пользователя (включая кэш-машины L2). Эти рабочие столы будут проходить через разные состояния (Рисунок 384):

o В процессе подготовки: в этом состоянии виртуальные рабочие столы создаются на платформе виртуализации.

o Ожидание ОС: В этом состоянии виртуальные рабочие столы настраиваются с параметрами, указанными в «Менеджер ОС» (смена имени, включение в домен и т.д..).

o Действителен: когда виртуальный рабочий стол находится в этом состоянии, это означает, что он доступен для доступа пользователей.

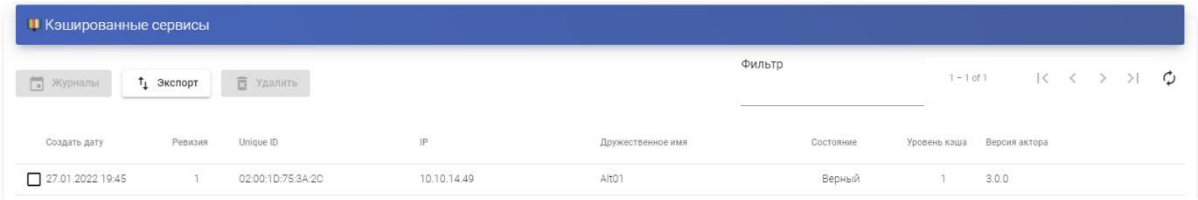


Рисунок 384

▪ Группы: чтобы пользователи могли подключаться, необходимо назначить группы доступа или метагруппы. Эти группы или метагруппы должны быть созданы в разделе «Аутентификаторы», и можно назначить одну или несколько групп доступа или метагрупп для каждого «Сервис-пула» (Рисунок 385).

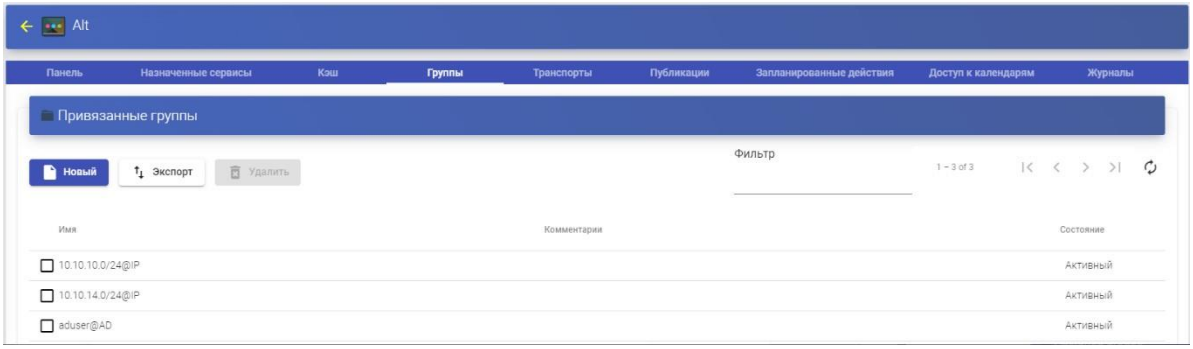


Рисунок 385

Выбрать «Аутентификатор» и «Имя группы» (Рисунок 386).

Рисунок 386

▪ Транспорты: будут указаны «Транспорты» для подключения к виртуальному рабочему столу (ранее добавленные в разделе «Транспорты»). «Транспорты» с самым низким приоритетом будут настроены системой по умолчанию. Чтобы использовать остальные транспорты, пользователь должен будет открыть раскрывающееся меню на экране доступа к виртуальному рабочему столу и выбрать соответствующий (Рисунок 387).

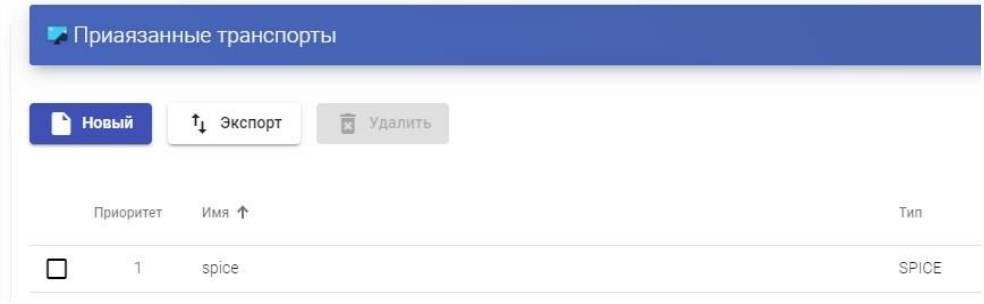


Рисунок 387

Выбрать «Транспорт», который нужно использовать в этом «пуле услуг», и сохранить (Рисунок 388).

Рисунок 388

▪ Публикации: из этого меню можно создать новую публикацию службы (например, если обновлен базовый компьютер новыми приложениями или исправлениями ОС и нужно, чтобы все виртуальные рабочие столы приняли эти изменения). После завершения процесса публикации весь системный кеш будет перегенерирован с новыми рабочими столами на основе этой последней публикации (Рисунок 389).

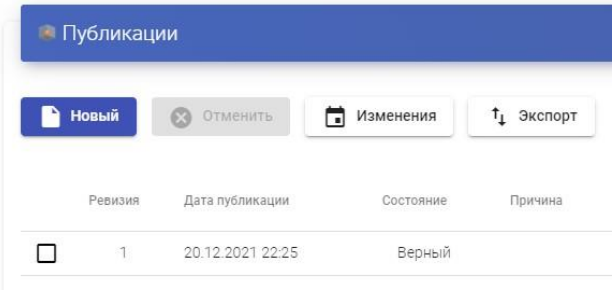


Рисунок 389

Если будет сделана новая публикация, будет создана новая базовая машина, и, как только она станет доступной, система продолжит удаление виртуальных рабочих столов предыдущей версии и создаст новые на основе новой публикации.

3.6.4.7 Метапулы

Создание «Метапула» позволит получить доступ к настольным сервисам или виртуальным приложениям, состоящим из разных «пулов сервисов». Эти пулы будут работать вместе, предоставляя различные услуги абсолютно прозрачным для пользователей способом.

«Пулы услуг», образующие «Метапул», будут работать в соответствии с политикой, которая позволит предоставлять услуги в соответствии с потребностями пула. В настоящее время поддерживаемые политики будут определяться приоритетами, емкостью платформы и использованием.

Чтобы создать «Метапул», перейдите в раздел «Пулы» и выбрать «Метапулы» (Рисунок 390).

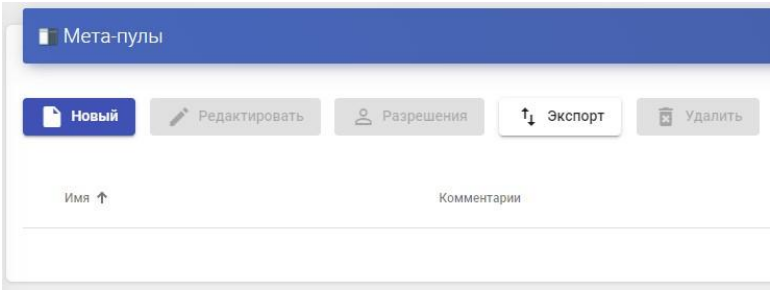


Рисунок 390

Для настройки «Метапула» необходимо будет указать:

▪ Основное (Рисунок 391):

Рисунок 391

Имя: Имя «Метапула» (это имя будет отображаться пользователю для доступа к его службе: виртуальному рабочему столу или приложению).

Короткое имя: если указано, это будет имя службы, которое будет показано пользователю. При наведении на него появится содержимое поля «Имя».

Политика: Политика, которая будет применяться при создании сервисов в «Пулах сервисов», являющихся частью «Метапула».

▪ Evenly distributed: услуги будут создаваться и использоваться одинаково во всех «пулах услуг», составляющих «метапул».

▪ Priority: услуги с наивысшим приоритетом будут создаваться и потребляться из «пула услуг» (приоритет определяется полем «приоритет». Чем ниже значение этого поля, тем выше приоритет будет у элемента). Когда «Сервисный пул» достигает максимального количества сервисов, будут потребляться сервисы следующего.

▪ Greater % available: службы будут создаваться и потребляться из «пула служб», который имеет самый высокий процент бесплатного использования.

▪ Дисплей (Рисунок 392):

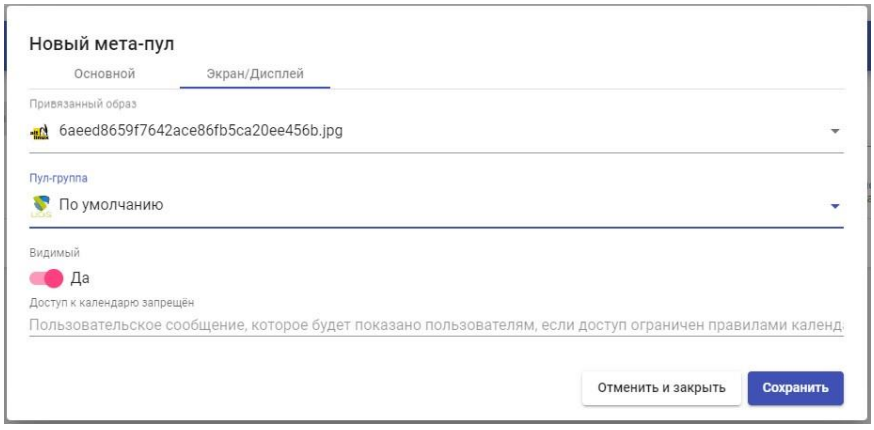


Рисунок 392

Связанное изображение: изображение, связанное с «метапулом». Он должен быть предварительно добавлен в хранилище изображений и доступен из раздела «Инструменты» — «Галерея».

Группа пулов: позволяет группировать различные «метапулы» для назначения «группы пулов». Его необходимо предварительно создать в разделе «Пулы» — «Группы».

Видимый: если этот параметр отключен, «Метапул» не будет отображаться как доступный для пользователей на странице услуг UDS («Режим пользователя»).

Доступ к календарю запрещен: текст, который будет отображаться, когда доступ к метапулу запрещен приложением календаря доступа.

Сохраните конфигурацию, и у вас будет действующий «Метапул», чтобы начать регистрацию «Сервис-пулов».

Чтобы изменить любой параметр в существующем «Метапуле», выбрать его и нажать «Редактировать».

После создания необходимо добавить «Пулы сервисов». Для этого дважды кликните по созданному «Метапулу» или выбрать «Подробнее» в меню провайдера (Рисунок 393):

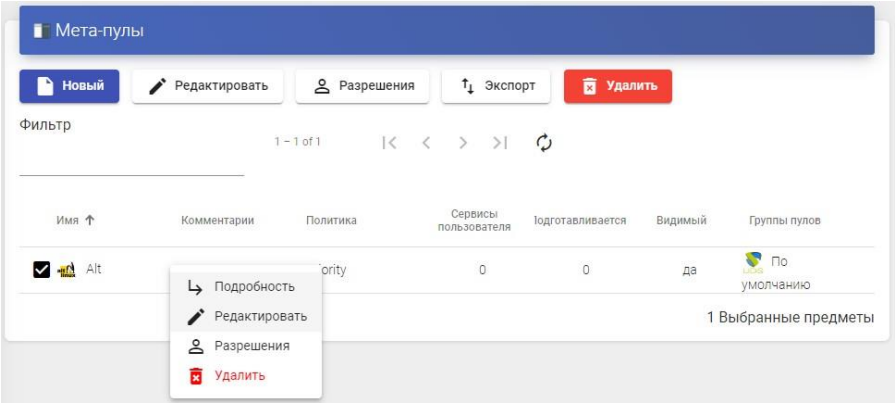


Рисунок 393

Нажать «Создать», чтобы добавить все «Пулы сервисов», которые будут содержаться в «Метапуле». Вы можно добавить столько, сколько вам

нужно, комбинируя службы, размещенные на разных платформах виртуализации (VMware, KVM, Azure и т. д.), серверах приложений и статических устройствах (Рисунок 394).

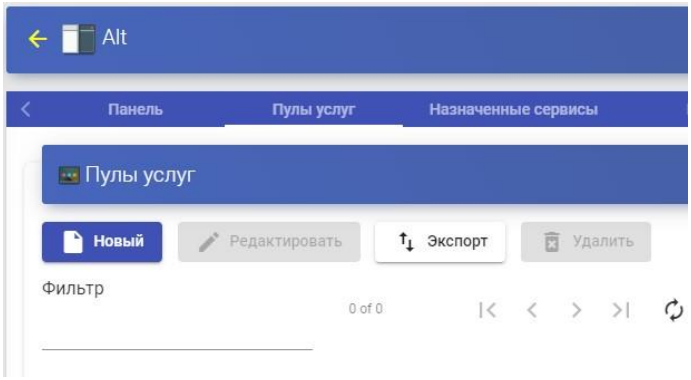


Рисунок 394

Для добавления «Сервисного пула» необходимо указать следующие параметры (Рисунок 395):

Приоритет: приоритет, который будет иметь «пул услуг» в «метапуле». Чем ниже значение, тем больший приоритет он имеет по отношению к остальным элементам.

Пул услуг: имя «пула услуг», который вы хотите добавить. Он должен быть предварительно создан.

Включено: включает или отключает видимость «Метапула».

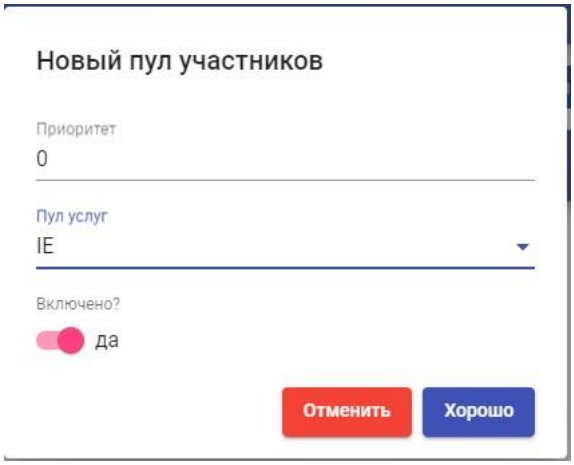


Рисунок 395

Можно добавить столько, сколько нужно, комбинируя службы, размещенные на разных платформах виртуализации (VMware, KVM, Azure и т. д.), серверах приложений и статических устройствах (Рисунок 396).

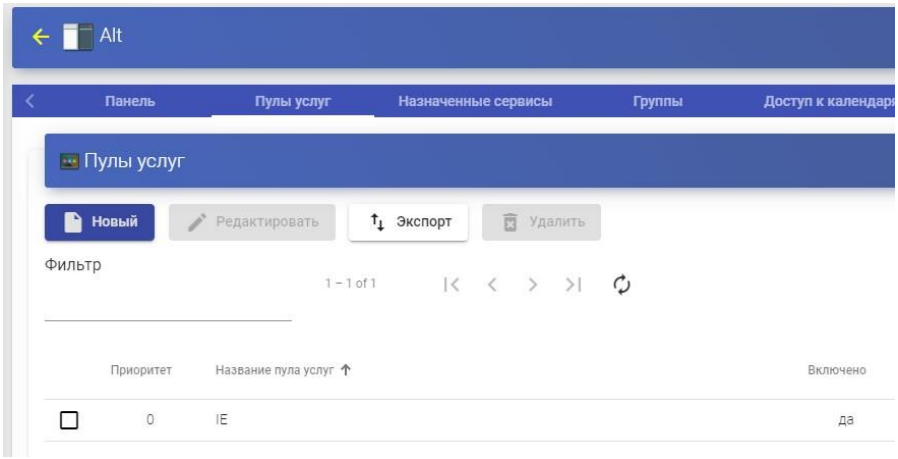


Рисунок 396

Как и в «Сервисном пуле», здесь есть следующие вкладки с информацией и конфигурацией:

- Назначенные службы: отображает службы, назначенные пользователям, что позволяет вручную удалить их и переназначить другому пользователю.

▪ Группы: указывает, какие группы пользователей различных аутентификаторов, зарегистрированных в системе, будут иметь доступ к услуге.

▪ Календари доступа: позволяет применить ранее созданный календарь доступа.

▪ Журналы: отображает все проблемы, возникшие в «Метапуле».

3.6.4.8 Группы

VDI позволяет группировать сервисы, чтобы облегчить их доступ и расположение. Кроме того, каждой группе услуг можно присвоить имя и изображение. Если «Группы» не определены, службы будут расположены на сайте по умолчанию, созданном системой.

Чтобы создать «Группы», перейти в раздел «Пулы» и выбрать «Группы» (Рисунок 397).

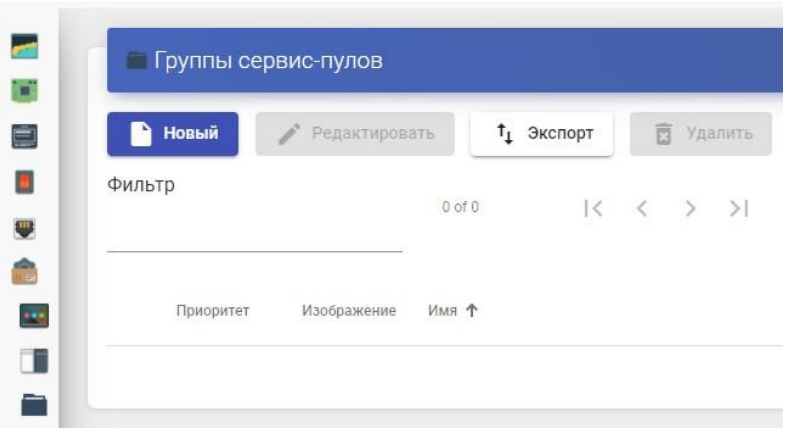


Рисунок 397

Выбрать «Новый» и указать описательное имя. Назначить приоритет группе пула (чем ниже значение, тем выше приоритет по отношению к остальным элементам) и привязать образ (Рисунок 398):

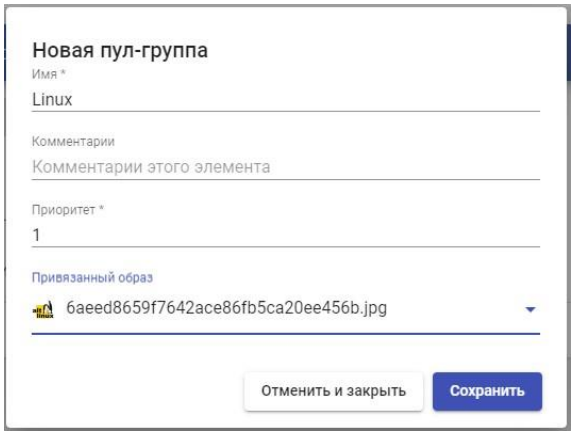


Рисунок 398

После создания он будет доступен для назначения в «Сервисный пул» (Рисунок 399).

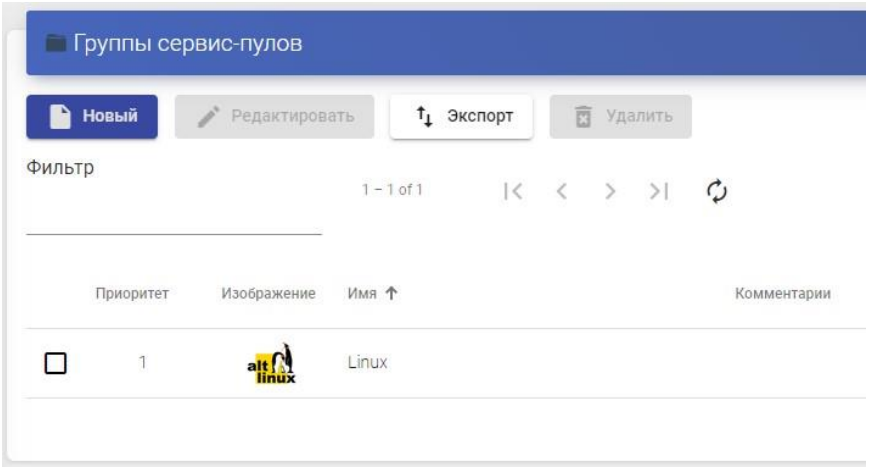


Рисунок 399

3.6.4.9 Доступ к календарям и запланированным задачам

VDI включает систему, позволяющую разрешать или запрещать доступ через календари. Они позволяют разрешать или ограничивать доступ пользователей к настольным службам и виртуальным приложениям по датам и временным интервалам.

С помощью календарей также можно планировать и автоматизировать определенные задачи в «Сервис-пул», такие как создание новых публикаций, настройка значений системного кэша, добавление или удаление групп и транспортов или изменение максимального количества услуг.

Календари

Чтобы создать «Календари», перейти в раздел «Пулы» и выбрать «Календари» (Рисунок 400).

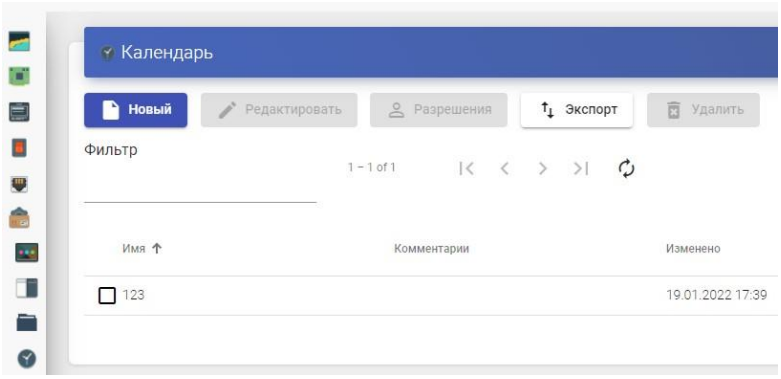


Рисунок 400

Указать описательное имя для идентификации календаря (Рисунок 401).

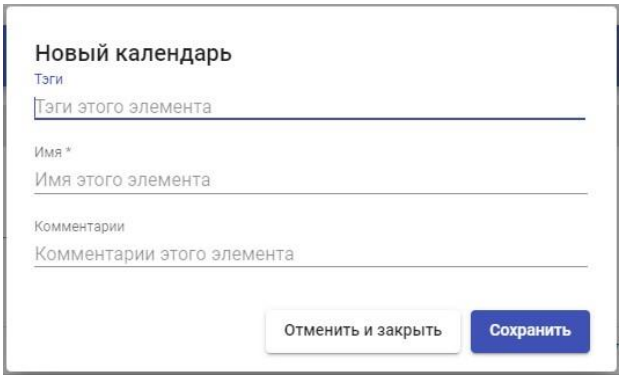


Рисунок 401

Сохранить, и будет действующий календарь, чтобы начать создавать правила, которые позже можно применить к сервису через «Сервис-пулов» (Рисунок 402).

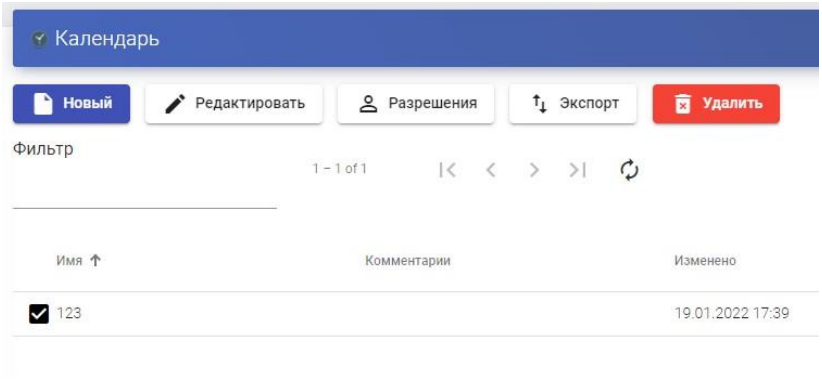


Рисунок 402

В «Календаре» можно зарегистрировать различные типы правил, чтобы запланировать доступность услуг в определенное время.

Чтобы создать правило, открыть календарь и нажать «Создать» (Рисунок 403).

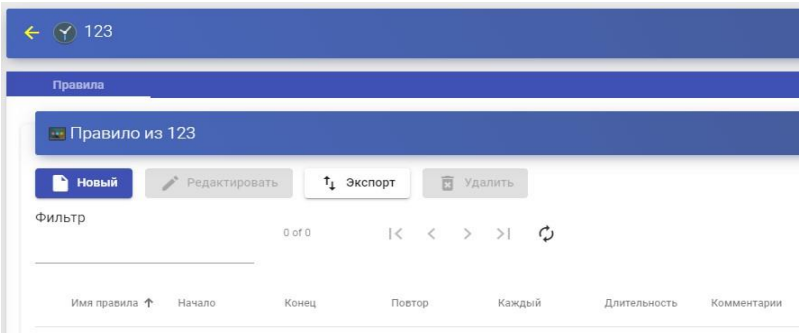


Рисунок 403

Минимальные параметры для настройки в «Правило» (Рисунок 404):

Имя: Имя правила.

Событие: настройка периодов выполнения. Для этого указать время начала и продолжительность события (в минутах, часах, днях и месяцах).

Повтор: в этом разделе можно настроить повторение правила в днях, неделях, месяцах, годах и даже позволяет указать рабочие дни. Наконец, можно указать интервалы повторения в день.

Сводка: показывает сводку всех ранее выполненных настроек.

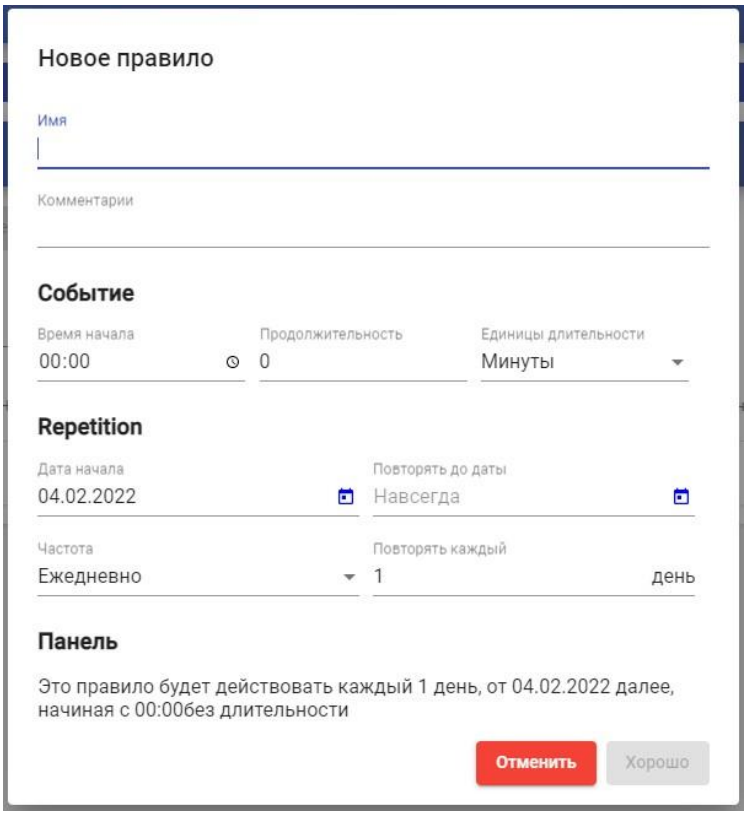


Рисунок 404

После сохранения будет действующее правило, которое будет назначено «Сервис-пулу» (виртуальному рабочему столу и/или приложению).

4.10.1.1 Разрешить или запретить доступ пользователя

После настройки правил в календарях можно использовать их, чтобы разрешить или запретить доступ пользователей к службам рабочего стола и виртуальным приложениям.

Чтобы применить эти календари с их правилами, выбрать «Пул услуг», перейти на вкладку «Доступ к календарям» и нажать «Создать» (Рисунок 405):

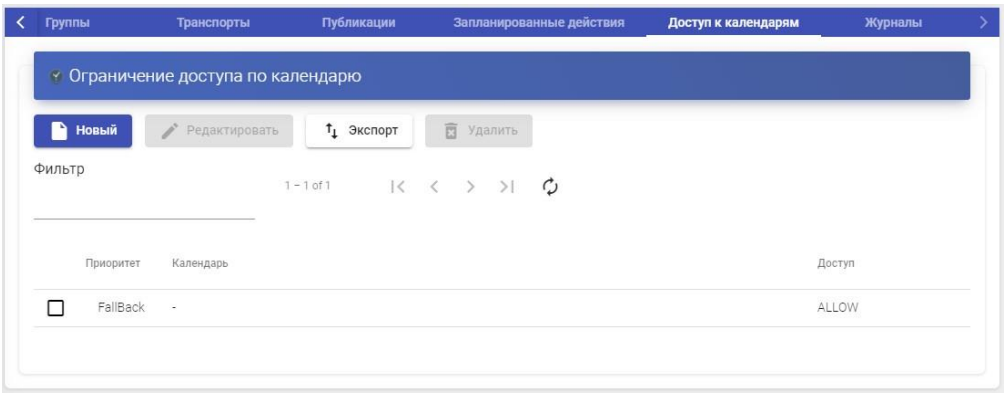


Рисунок 405

Указать приоритет доступа, выбрать существующий календарь и отметить действие, которое будет применяться при доступе к сервису (Рисунок 406).

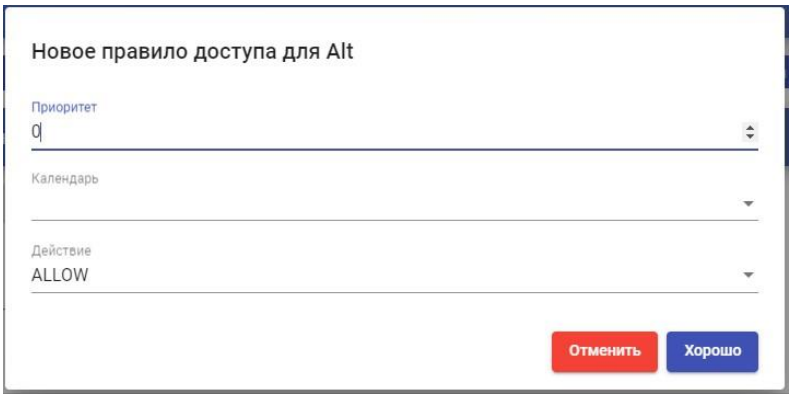


Рисунок 406

После сохранения у будет «Пул услуг» с настроенным календарем доступа (Рисунок 407).

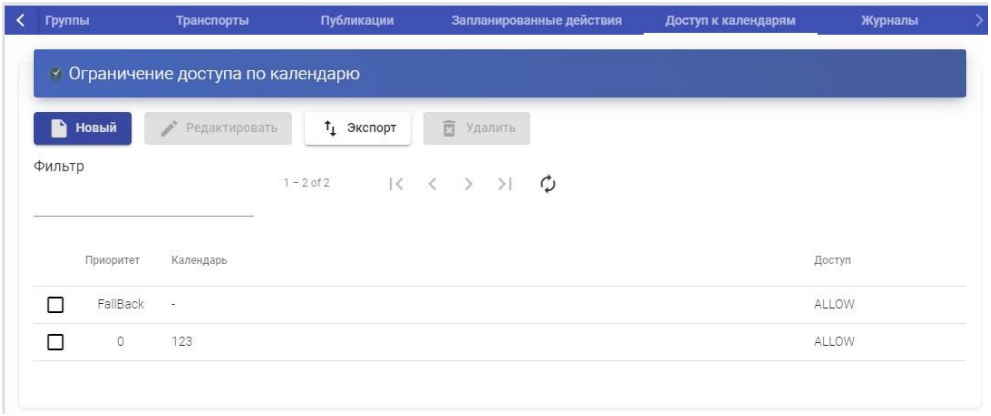


Рисунок 407

Примечание: необходимо настроить правило по умолчанию «FallBack» в зависимости от потребностей службы, чтобы разрешить или запретить доступ к службе, когда календарь не применяется.

Запланированные действия

После настройки правил в календарях можно использовать их для планирования определенных задач в «пуле услуг».

Чтобы применить эти календари с их правилами, выбрать «Пул услуг», перейти на вкладку «Запланированные действия» и нажать «Создать» (Рисунок 408).

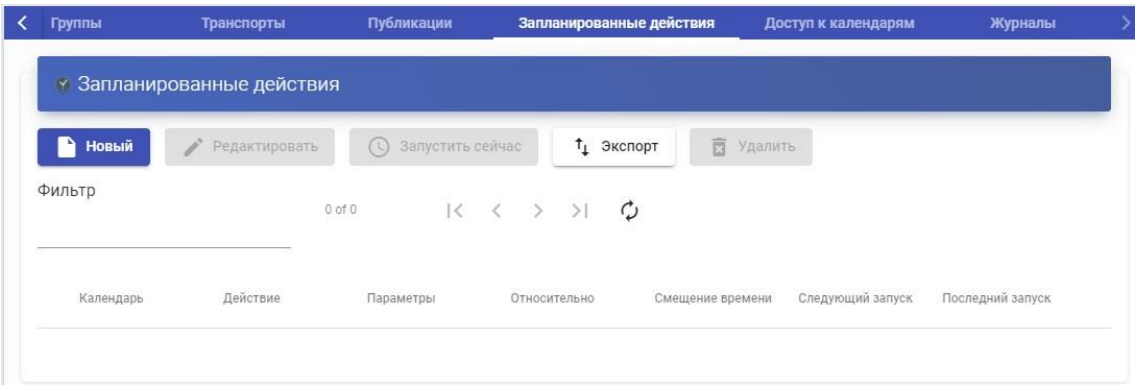


Рисунок 408

Указать существующий календарь, время, в течение которого будет выполняться действие и выбрать действие, которое необходимо выполнить:

Установить начальные службы: сбрасывает минимальное количество созданных и настроенных виртуальных рабочих столов.

Установить размер кеша: сбрасывает виртуальные рабочие столы, доступные в системном кеше. Эти рабочие столы будут настроены и готовы к назначению пользователю.

Установить максимальное количество служб: изменяет максимальное количество виртуальных рабочих столов в «пуле служб».

Публикация: создание новой публикации в «пуле услуг».

Добавить транспорт: добавляет существующий транспорт в «Пул услуг».

Удалить транспорт: удаляет транспорт из «пула услуг».

Добавить группу: добавляет существующую группу в «Пул услуг».

Удалить группу: удаляет группу из «пула услуг».

Устанавливает игнорирование неиспользуемых: устанавливает параметр «Игнорировать неиспользуемые».

Удалить ВСЕ назначенные пользовательские службы: удаляет все службы, назначенные пользователям в «пуле служб».

После сохранения будет запланированная задача, которая выполняет определенное действие в «пуле услуг» (Рисунок 409).

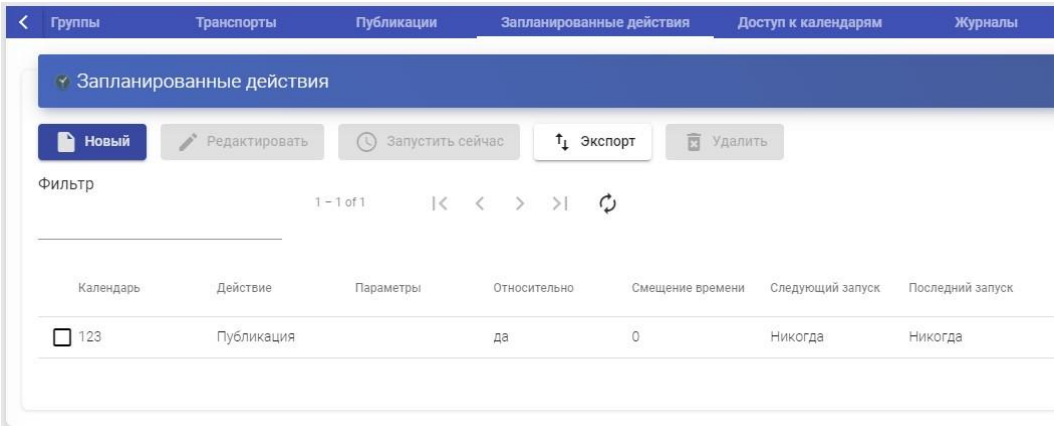


Рисунок 409

3.6.4.10 Настройка разрешений

В рамках администрирования VDI можно назначать права доступа и управления различным элементам, пользователям и группам пользователей. Разрешения будут назначены непосредственно для каждого элемента, а также будут применяться к его подэлементам.

Чтобы позволить пользователю получить доступ к администрированию и подать заявку на эти разрешения, у пользователя должна быть включена опция «Сотрудник» (Рисунок 410):

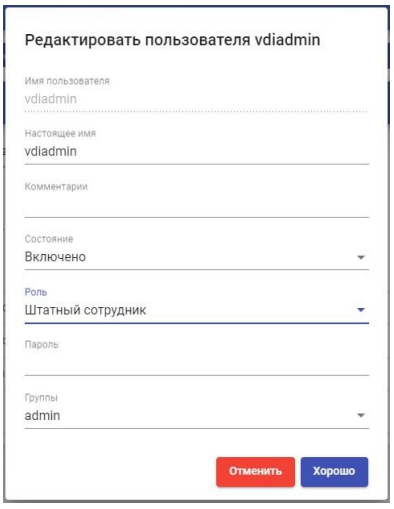


Рисунок 410

Чтобы включить разрешения в различных элементах администрирования, выбрать элемент и нажать «Разрешения». Например, в «Поставщик услуг» (Рисунок 411).

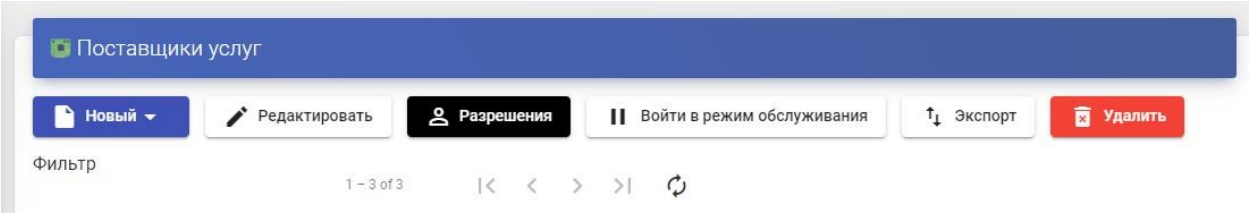


Рисунок 411

В окне разрешений нажать «Новое разрешение…» для групп и пользователей и выбрать аутентификатор и группу/пользователя, к которым будет применяться разрешение (Рисунок 412).

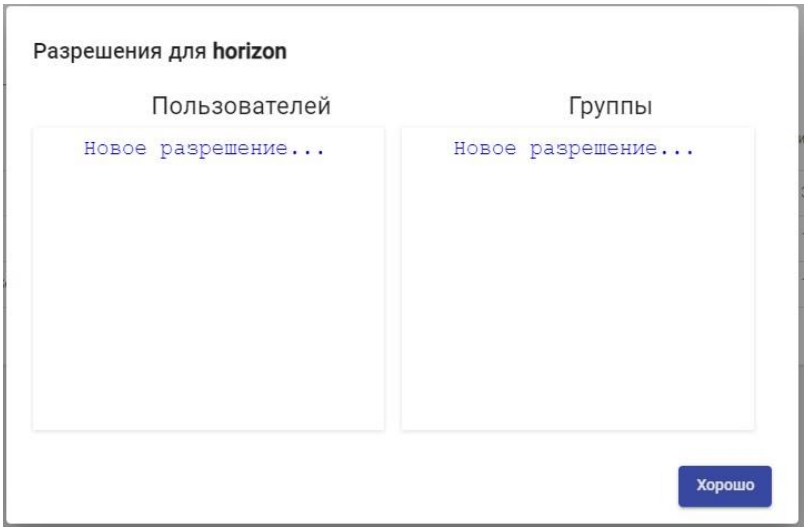


Рисунок 412

Нужно указать, будет ли этот пользователь или группа иметь доступ для чтения к элементу («Только чтение») или полный доступ («Полный доступ») (Рисунок 413).

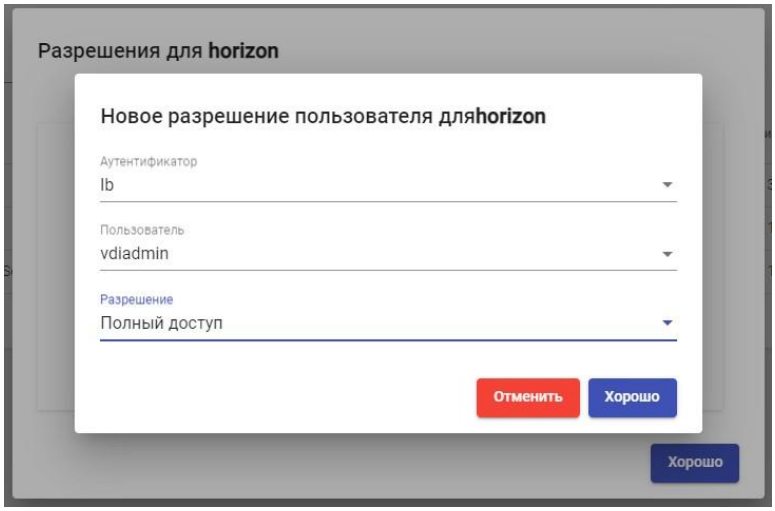


Рисунок 413

После применения пользователи, у которых включена опция «Сотрудник», смогут получить доступ к этому элементу администрирования с назначенными разрешениями (Рисунок 414).

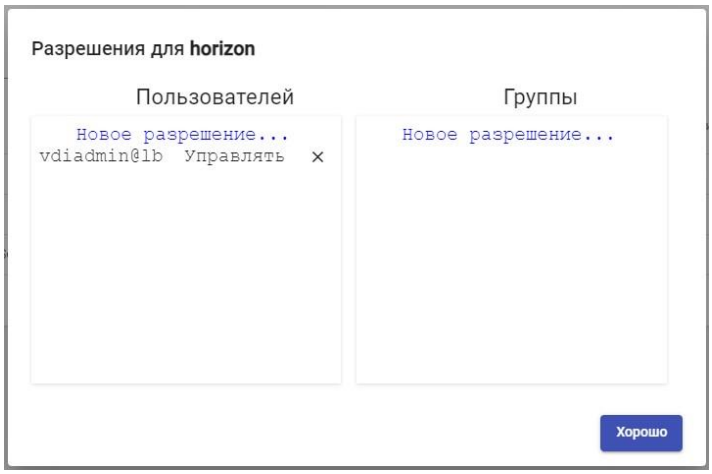


Рисунок 414

Чтобы удалить разрешения для группы или пользователя, нажать «X».

Разрешения типа «Полный доступ» («Управление») могут применяться только к элементам, имеющим второй уровень («Сервисы», «Календари», «Сервисные пулы» и т. д.).

3.6.5 Галерея

UDS имеет репозиторий образов, которые можно связать с «пулом услуг» или «группой пулов», чтобы облегчить идентификацию виртуального рабочего стола. Допустимые форматы: PNG, JPEG и GIF. Если размер изображения больше 128x128, он будет изменен до этих значений.

Чтобы получить доступ к галерее изображений UDS, перейти в раздел «Инструменты» и выбрать «Галерея» (Рисунок 415):

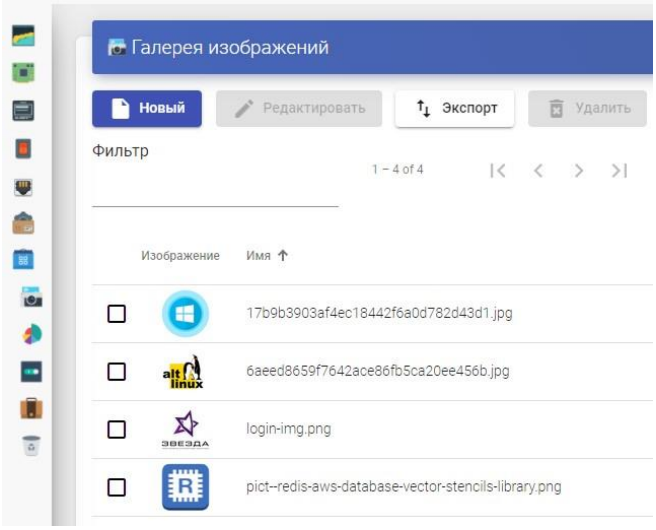


Рисунок 415

Выбрать «Новый», чтобы добавить новый образ в репозиторий. Необходимо указать имя и с помощью кнопки «Выбрать изображение» найти образ, который нужно загрузить (Рисунок 416).

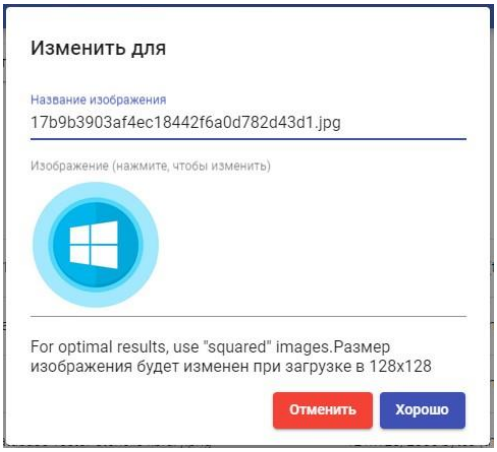


Рисунок 416

После того как образ будет сохранен, он будет доступен для назначения в «Сервисный пул» или «Группу пулов».

3.6.6 Отчеты

VDI позволяет автоматически генерировать отчеты по различным элементам платформы.

Чтобы получить доступ к отчетам, войти в раздел «Инструменты» и выбрать «Отчеты» (Рисунок 417).

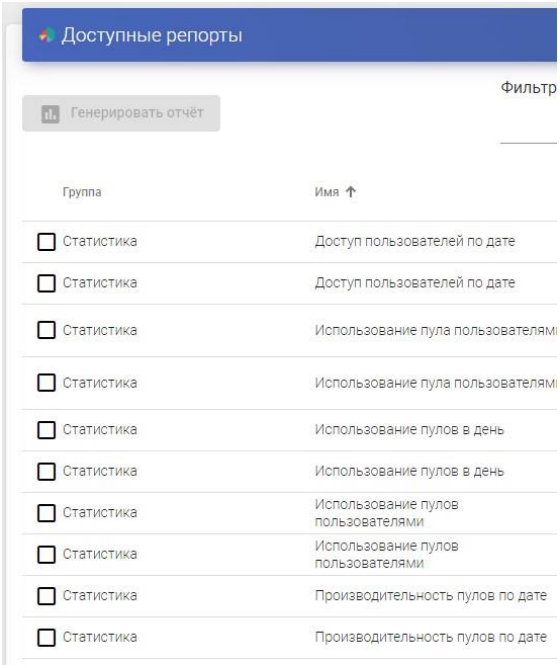


Рисунок 417

В VDI можно генерировать различные отчеты:

▪ Список пользователей: создает отчет со всеми пользователями, принадлежащими аутентификатору. Выбрать аутентификатор и нажать «Сохранить» (Рисунок 418).

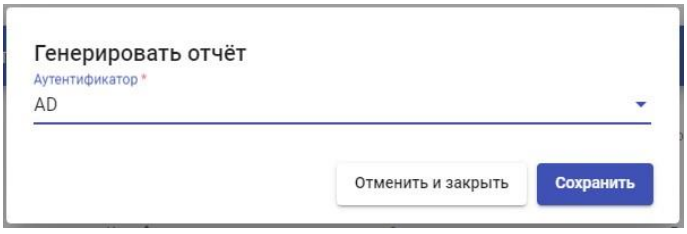


Рисунок 418

После создания будет список всех пользователей, принадлежащих этому аутентификатору:

▪ Отчет о доступе пользователей по дате: создает отчет со всеми доступами пользователей к системе в указанном диапазоне дат. Можно указать диапазон дат и количество интервалов (Рисунок 419):

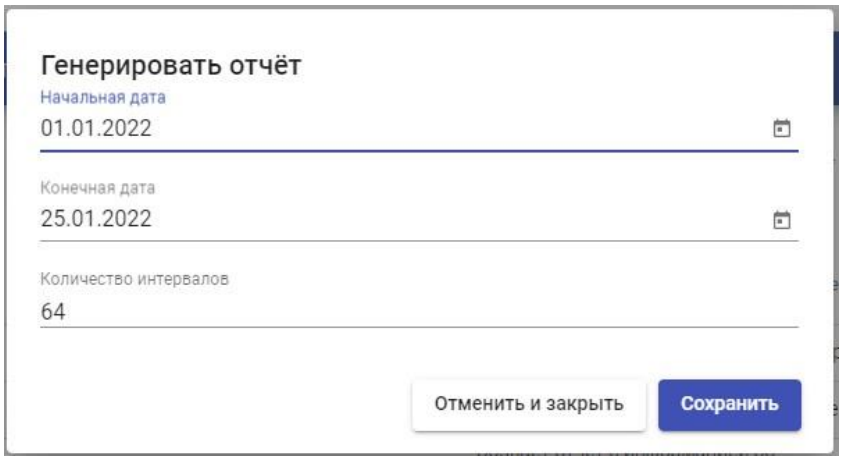


Рисунок 419

▪ Производительность пулов по дате: создает отчет об использовании пула услуг в указанном диапазоне дат. Вы можно указать пул, по которому нужно сформировать отчет, диапазон дат и количество интервалов (Рисунок 420):

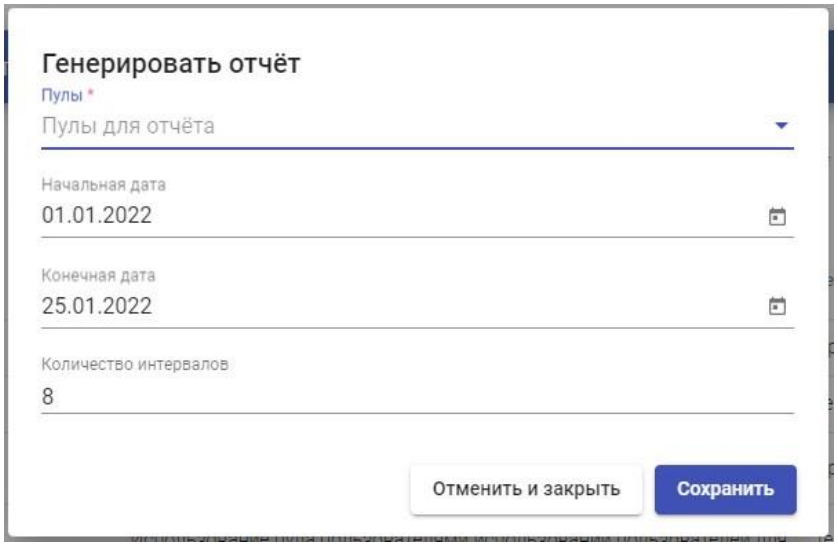


Рисунок 420

3.6.7 Конфигурация

VDI предоставляет ряд параметров, которые будут определять работу системы. Эти параметры будут отвечать за определение таких аспектов, как безопасность, режим работы, подключение и т. д. как самой системы VDI, так и ее связи с виртуальными платформами, зарегистрированными в VDI.

В данном руководстве показаны только некоторые системные переменные, которые считаются наиболее полезными для управления виртуальными рабочими столами.

В остальных переменных рекомендуется не изменять значения по умолчанию, так как некоторые из них указывают системе, как она должна работать (количество одновременных задач, время выполнения задач, плановые проверки и т. изменение параметра может привести к полной остановке системы или неправильной работе.

Примечание: после изменения значений любой из переменных расширенной конфигурации UDS необходимо перезапустить сервер UDS, чтобы изменения вступили в силу.

Чтобы получить доступ к параметрам расширенной конфигурации UDS, перейти в раздел «Инструменты» и выбрать «Конфигурация» (Рисунок 421):

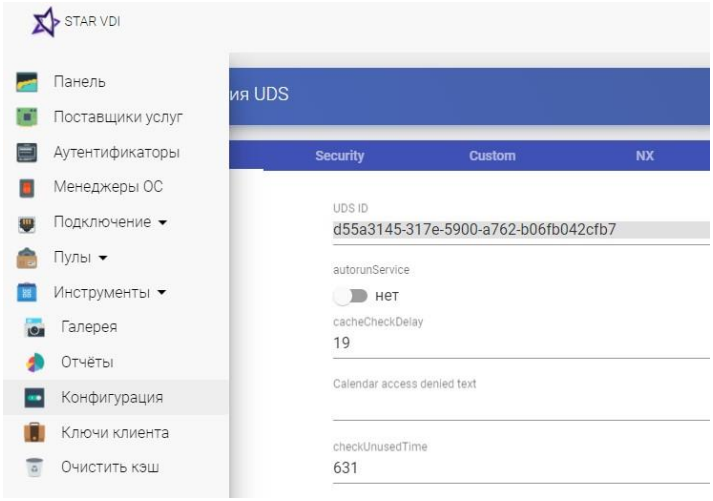


Рисунок 421

3.6.7.1 UDS

UDS ID: Идентификация установки VDI.

AutorunService: выполняет прямой доступ к службе пользователя, если пользователю назначена только одна служба. Активировав этот параметр, пользователи, которым назначен один сервис, будут подключаться к нему напрямую, скрывая экран выбора сервиса и используя предварительно настроенный «Транспорт».

По умолчанию: нет.

DisallowGlobalLogin: если этот параметр включен, глобальный список аутентификаторов не отображается. Если включено, пользователи будут проверяться на аутентификаторе «по умолчанию» или с более высоким приоритетом. Для проверки с помощью других аутентификаторов и предоставления пользователю доступа к системе необходимо будет использовать «метку» в URL-адресе доступа (определенном в аутентификаторе).

По умолчанию: нет.

KeepInfoTime: определяет время, в течение которого завершенные события

«пула услуг» остаются видимыми. Выражается в секундах

По умолчанию: 14401 секунд (4 часа)

RedirectToHttps: автоматически перенаправляет доступ к ПО с http на https.

По умолчанию: нет

SessionExpireTime: указывает максимальное время, в течение которого пользовательский сеанс будет открыт после создания новой публикации. По истечении этого времени система закроет сеанс пользователя и продолжит удаление службы. Если у службы есть диспетчер ОС с «Сохранить назначение службы даже при новой публикации» в качестве политики сохранения на виртуальном рабочем столе, это не будет применяться.

По умолчанию: 24 часа.

StatsDuration: время, в течение которого система будет хранить статистику.

По умолчанию: 365 дней.

3.6.7.2 Безопасность

Описаны параметры, связанные с безопасностью системы UDS:

AllowRootWebAccess: позволяет суперпользователю войти в систему (пользователю, созданному в мастере настройки UDS-сервера) на портале входа UDS.

Изменение этой переменной не повлияет на доступ пользователя root через консоль ОС Linux.

По умолчанию: да.

Behind a proxy: указывает системе, что серверы UDS находятся «за» проксисервером (например, среда UDS в режиме высокой доступности с проксисервером HA типа балансировщика нагрузки).

По умолчанию: нет.

Block ip on login failure: Включает блокировку пользователя, который несколько раз ошибался на портале входа, также блокирует IP-адрес его клиента подключения.

По умолчанию: нет.

LoginBlockTime: Время, в течение которого пользователь будет заблокирован (в секундах) после неправильного ввода пароля, время, указанное в переменной «maxLoginTries».

По умолчанию: 300 секунд (5 минут).

Мастер-ключ: защитный код для UDS Actor (применяется только к предыдущим версиям VDI).

MaxLoginTries: количество попыток, которые пользователь должен будет ввести свой пароль, прежде чем система заблокирует его.

RootPass: Пароль суперпользователя, созданный в мастере настройки VDIServer.

SuperUser: имя суперпользователя, созданное в мастере настройки VDIServer.

Trusted Hosts: хосты, которые UDS считает безопасными. Эти хосты могут делать «чувствительные» запросы к UDS, такие как туннели.

По умолчанию: "*" (все разрешено), допускает значения диапазона адресов.

3.6.7.3 Пользовательский

Описаны параметры, связанные с графической настройкой UDS (портал входа и обслуживания пользователей):

CSS: поддерживает код для изменения страниц стиля UDS по умолчанию.

Logo name: текст, который отображается рядом с верхним левым изображением строки пользовательского меню.

Show Filter on Top: позволяет изменить расположение панели поиска служб на странице пользовательских служб (режим пользователя).

Site copyright info: текст, который будет отображаться в нижней правой части страницы входа и пользовательских услуг.

Site copyright link: Веб-адрес в тексте раздела «Информация об авторских правах на сайт».

Site information: HTML-код для частичной настройки страницы входа в VDI.

Введенный код появится под полем входа пользователя на портале входа

VDI.

Site name: текст, который будет отображаться в верхней части поля входа пользователя на портале входа VDI.

3.6.7.4 NX

Описаны параметры, относящиеся к «Транспорту» NX:

DownloadUrl: веб-адрес для загрузки программного обеспечения NX.

DownloadUrlMACOS: веб-адрес загрузки программного обеспечения NX для MAC.

3.6.7.5 PCoIP

Описаны параметры, относящиеся к Teradici PCoIP «Транспорт»:

DownloadUrl: адрес загрузки программного обеспечения клиента PCoIP.

3.6.7.6 RGS

Описаны параметры, связанные с работой РГС «Транспорт»:

DownloadUrl: веб-адрес для загрузки программного обеспечения RGS.

TunnelOpenedTime: максимальное время, в течение которого туннель будет ожидать открытия соединения RGS.

Если за время, указанное в этой переменной, соединение не будет установлено, оно будет отменено и потребуется установить соединение заново (в случае соединения с очень медленными клиентами рекомендуется увеличить это значение).

По умолчанию: 30 секунд.

3.6.7.7 SAML

Описаны параметры, связанные с работой аутентификатора SAML: Global logout on exit: указывает режим выхода из системы. Если этот параметр включен, при выходе UDS из системы также выполняется SAML.

По умолчанию: нет.

IDP Metadata Cache: время хранения кэшированных метаданных IDP.

По умолчанию: 86400 секунд (24 часа).

Organization Display Name: отображается название организации.

Organization Name: Название организации.
Organization URL: веб-адрес организации.

User cleanup: указывает, как часто задача очистки пользователя будет выполняться без активности.

Если пользователь остается без активности в течение времени, указанного в этой переменной, система приступит к его устранению.

По умолчанию: 2592000 секунд (30 дней).

3.6.7.8 WYSE

Описаны параметры, связанные с подключением к клиентам Wyse:

Автоподключение: разрешает автоматическое подключение устройства.

По умолчанию: нет.

Цвета: определяет качество цветов, предлагаемых во время соединения.

По умолчанию: Высокий.

DefaultUser: пользователь по умолчанию, перенаправленный на устройство.

По умолчанию: UDS.

Язык: язык устройства.

По умолчанию: us.

Привилегия: Уровень привилегии пользователя.

По умолчанию: НЕТ.

Подробнее об этих параметрах см. в официальной документации Wyse или в этом справочном руководстве:

4 Аварийные ситуации

Список сообщений об ошибках, выдаваемых пользователю, и рекомендации по устранению неисправностью, приведены в таблице ниже (Таблица 14).

Таблица 14 – Перечень сообщений об ошибках, выдаваемых пользователю.

№ п/п	Сообщение	Пояснения и рекомендации
1	Ошибка подключения к серверу ‘*IPадрес сервера*'	1 По данному IP-адресу отсутствует сервер. 2 Отсутствует подключение терминала к локальной вычислительной сети (ЛВС)
2	Ошибка сервера ‘*IP-адрес сервера*'. Виртуальная машина ‘*Название ВМ’* не найдена	На сервере с данным IP-адресом отсутствует указанная виртуальная машина
3	Ошибка сервера ‘*IP-адрес сервера*'. Ошибка конфигурации виртуальной машины ‘*Название ВМ’*	1 В настройках конфигурации ВМ произошла ошибка. 2 При настройке ВМ неправильно сконфигурирован графический сервер Spice. Следует настроить Spice согласно настоящему руководству администратора (п. **Ошибка! Источник ссылки не н айден.**)
4	Ошибка сервера ‘*IP-адрес сервера*'. Доступ к виртуальной машине ‘*Название ВМ’* запрещен администратором сервера	Неправильно настроен графический сервер Spice. Следует настроить Spice согласно настоящему руководству администратора (п. **Ошибка! Источник ссылки не н айден.**)
5	Ошибка сервера ‘*IP-адрес сервера*'. Ошибка запуска виртуальной машины ‘*Название ВМ’*	Потерян образ виртуальной машины
6	Неизвестный ключ или неавторизованный пользователь. Компьютер будет отключен	1 Ошибка работы с платой МИиКДС. 2 Ошибка в конфигурационном файле

5 Порядок внесения изменений

Изменения, не влияющие на технические характеристики и условия эксплуатации, вносятся в документацию в соответствии с ГОСТ 2.503.

Изменения, в том числе и программного обеспечения (затрагивающие технические данные изделия или влекущие за собой изменение условий эксплуатации изделия), могут быть внесены только предприятиемизготовителем.

Перечень принятых сокращений

Сокращение	Расшифровка
LG	Logical Group
LVM	Logical Volume Manager – система управления томами с данными. Позволяет создавать поверх физических разделов или даже неразбитых жестких дисков логические тома, которые в самой системе будут видны как обычные блочные устройства с данными (т.е. как обычные разделы)
NTP	Network Transfer Protocol. Сетевой протокол для синхронизации часов в компьютерных системах по сетям передачи данных с коммутацией пакетов и переменной задержкой (латентностью)
VNC	Virtual Network Computing. Система удалённого доступа к рабочему столу компьютера, использующая протокол RFB. Управление осуществляется путём передачи нажатий клавиш на клавиатуре и движений мыши с одного компьютера на другой и ретрансляции содержимого экрана через компьютерную сеть
АБИ	Компонент «Администратор безопасности»
АГ	Административная группа
АРМ	Автоматизированное рабочее место
ВД	Высокая доступность
ВМ	Виртуальная машина
ГИС	Государственная информационная система
ДСП	Для служебного пользования
К	Конфиденциально
КП	Комплекс программ

КС	Комплект серверный
КТ	Комплект терминальный

ЛД	Лазерный диск
МИиКДС	Модуль идентификации и контроля доверенной среды
НС	Несекретно
НСД	Несанкционированный доступ
ОО	Объект оценки
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПРД	Правила разграничения доступа
ПЭВМ	Персональная электронная вычислительная машина
РД	Руководящий документ
СВТ	Средство вычислительной техники
СГУ	Система группового управления
СДЗ	Средства доверительной загрузки
СРК	Система резервного копирования
СС	Совершенно секретно

ФСТЭК России	Федеральная служба по техническому и экспортному контролю России
ЦОД	Центр обработки данных
ЭК	Электронный ключ

ПРИЛОЖЕНИЕ А

Перечень состояний виртуальных машин (справочное)

Перечень состояний виртуальных машин:

Состояние	Описание
Pending	По умолчанию виртуальная машина запускается в состоянии ожидания, ожидая запуска. Она будет оставаться в этом состоянии до тех пор, пока планировщик не решит развернуть его или пользователь не развернет ее вручную
Hold	Владелец «удержал» виртуальную машину, и она не будет планироваться до ее освобождения. ВМ можно развернуть вручную.
Cloning	Виртуальная машина ожидает, пока один или несколько образов дисков завершат первоначальное копирование в хранилище (образ находится в состоянии «Заблокирован»)
Prolog	Система передает файлы виртуальной машины (образы дисков и файл восстановления) на хост, на котором будет работать виртуальная машина.
Boot	СГУ ожидает гипервизора для создания виртуальной машины.
Running	ВМ работает (этот этап включает в себя этапы загрузки и выключения внутренней виртуальной машины). В этом состоянии драйвер виртуализации будет периодически отслеживать ее.

Migrate	ВМ мигрирует с одного ресурса на другой. Это может быть «живая» или миграция с приостановкой (виртуальная машина сохраняется, а файлы виртуальной машины переносятся на новый ресурс).

Состояние	Описание
Hotplug	Процесс присоединения / отсоединения диска и виртуальной сети.
Snapshot	Создание «снимка» ВМ.
Save	Система сохраняет файлы ВМ после миграции, остановки или приостановки работы.
Epilog	На этом этапе система очищает узел, используемый для ВМ, и дополнительно образы дисков, которые необходимо сохранить, копируются обратно в системное хранилище данных.
Shutdown	СГУ отправила ВМ сигнал ACPI о завершении работы и ожидает его завершения. Если по истечении времени ожидания ВМ не исчезнет, СГУ будет предполагать, что гостевая ОС проигнорировала сигнал, и состояние виртуальной машины будет изменено на Running, а не Done.
Stopped	ВМ остановлена. Состояние виртуальной машины было сохранено и передано обратно вместе с образами дисков в системное хранилище данных.
Suspended	То же самое, что остановлено, но файлы остаются на хосте для последующего возобновления работы виртуальной машины (т.е. нет необходимости перепланировать виртуальную машину).

PowerOff	То же, что и приостановлено, но файл контрольных точек не создается. Файлы остаются на хосте для последующей загрузки там виртуальной машины. Когда гостевая ОС выключена, СГУ переведет виртуальную машину в это состояние.
Undeployed	ВМ выключена. Диски ВМ передаются в системное хранилище данных. ВМ может быть возобновлена позже.
Failed	Неуспешная операция с ВМ.

Состояние	Описание
Unknown	Не удалось связаться с ВМ, она находится в неизвестном состоянии.
Cleanup-resubmit	ВМ ждет, когда драйверы очистят узел после действия onevm recover --recreate
Done	ВМ готова. Виртуальные машины в этом состоянии не отображаются, но хранятся в базе данных с целью учета. Можно получить информацию о них с помощью команды onevm show

ПРИЛОЖЕНИЕ Б

Перечень состояний образов виртуальных машин (справочное)

Перечень состояний образов виртуальных машин:

Состояние	Описание
Заблокирован	Образ копируется или создается в хранилище
LOCKED_USED	Образ копируется или создается в хранилище, а ВМ ожидают завершения операции
LOCKED_USED_PERS	Постоянный образ копируется или создается в хранилище, а ВМ ожидают завершения операции
Готово	Образ готов к использованию
Используется	Непостоянный образ, подключенный как минимум к одной ВМ. Он также может использоваться другими ВМ.
Исп. сохр.	Постоянный образ используется ВМ. Он не может быть подключен к другим ВМ.
Отключен	Образ отключен владельцем. Он не может быть подключен к новым ВМ.
Ошибка	Ошибка, операция не удалась.
DELETE	Образ удаляется из хранилища
CLONE	Образ клонируется

ПРИЛОЖЕНИЕ В

Описание XML-RPC API (справочное)

Описание XML-RPC API

REST API определяет набор функций, к которым разработчики могут совершать запросы и получать ответы. Взаимодействие происходит по протоколу HTTP. Преимуществом такого подхода является широкое распространение протокола HTTP, поэтому REST API можно использовать практически из любого языка программирования.

Для запросов с веб-клиентов – клиентской части социального приложения или от сайта – существуют JS API и Flash-библиотека, которые более удобны и просты в использовании.

Все вызовы методов API – это GET или POST HTTP-запросы к URL с некоторым набором параметров. Кодировка результата – UTF-8.

Данные запроса могут передаваться в виде query-строки (после знака «?») при использовании метода GET, либо в теле POST-запроса. В случае GET-запроса, параметры должны быть закодированы с помощью URL encoding.

На данный момент, API не делает различий между GET– и POST–запросами. Тем не менее, существует ограничение на длину URL запроса – 2048 символов.

В каждом запросе должен присутствовать набор обязательных параметров. Также для каждой функции в ее документации определены дополнительные параметры, нужные только для этой функции. Текстовые значения параметров должны быть переданы в кодировке UTF-8.

Одинаковые для всех функций параметры перечислены в таблице ниже (Таблица 15).

Таблица 15 − Параметры функций

Имя	Тип	Описание
method	string	Название вызываемого метода, например, users.getinfo; обязательный параметр
app_id	int	Идентификатор приложения; обязательный параметр
sig	string	Подпись запроса; обязательный параметр
session_key	string	Сессия текущего пользователя
uid	uint64	Идентификатор пользователя, для которого вызывается метод; данный аргумент должен быть указан, если не указан session_key
secure	bool	Флаг, обозначающий, что запрос идет по защищенной схеме «сервер-сервер»; возможные значения: 1 или 0; по-умолчанию 0
format	string	Формат выдачи ответа API; возможные значения: xml или json; по умолчанию json

Параметры session_key и uid отвечают за авторизацию, то есть от лица какого пользователя происходит запрос. В зависимости от этого одна и та же функция в одном и том же приложении может возвращать немного разные результаты, например, когда один пользователь имеет доступ к различным закрытым данным, а другой нет. session_key используется для выполнения запросов по схеме «клиент-сервер», а uid − по схеме «сервер-сервер».

Сессия (session_key) получается при каждом новом сеансе работы пользователя с вашим приложением или сайтом. При последующих заходах

того же пользователя это значение будет другим, поэтому сохранять его не надо. Значение session_key получается в зависимости от того, как используется REST API. Если используется API в клиенте социального приложения, session_key приходит в параметрах запроса, если интегрируются API для сайтов, сессия получается в процессе логина. В любом случае, после получения session_key, можно передать это значение на сервер, чтобы осуществлять вызовы функций API с сервера от лица текущего пользователя.

Схема клиент−сервер предназначена для случаев, когда REST API используется из клиента социального приложения, клиентского кода сайта или отдельного мобильного или desktop − приложения.

Если используется схема клиент−сервер, то в параметрах запроса secure=0 и sig рассчитывается по следующему алгоритму:

sig = md5(uid + params + private_key)

Значение params − это конкатенация пар «имя=значение» отсортированных в алфавитном порядке по «имя», где «имя» − это название параметра, передаваемого в функцию API, «значение» − значение параметра. Разделитель в конкатенации не используется. Параметр sig при расчете подписи не учитывается, все остальные параметры запроса должны учитываться при расчете.

Значение uid − идентификатор текущего пользователя приложения. Значение private_key можно взять из настроек приложения.

Схема сервер−сервер является более надежной. Некоторые запросы, которые подразумевают согласие пользователя, можно выполнить только по

схеме клиент−сервер. В случае невозможности выполнения запроса по схеме сервер-сервер, вернется соответствующая ошибка.

Схема сервер−сервер использует отдельный ключ secret_key. При использовании схемы сервер−сервер, в параметрах запроса параметр secure=1 и значение параметра sig рассчитывается следующим образом:

sig = md5(params + secret_key)

В данном приложении описываются XML-RPC методы, использующиеся СГУ. Каждое описание состоит их имени метода и его входных и выходных значений.

Все ответы XML-RPC имеют общую структуру, приведенную в таблице ниже (Таблица 16).

Таблица 16 − Структура ответов XML-RPC

Данные	Тип данных	Описание
Вывод	Boolean	True или false в случае успешного или неуспешного завершения.
Вывод	String	Если возникает ошибка, выводится сообщение об ошибке
Вывод	Int	Код ошибки

Вывод всегда состоит из трёх значений. Первое и третье являются фиксированными, второе содержит сообщение об ошибке только в случае сбоя. Код ошибки содержит одно из значений, приведенных в таблице ниже (Таблица 17).

Таблица 17 − Коды ошибок

Значение	Код	Описание
0x0000	SUCCESS	Успешный ответ

0x0100	AUTHENTICATION	Пользователь не может быть аутентифицирован.
0x0200	AUTHORIZATION	Пользователь не имеет права выполнять запрошенное действие
0x0400	NO_EXISTS	Запрошенный ресурс не существует.
0x0800	ACTION	Ошибка состояния для выполнения действия.
0x1000	XML_RPC_API	Неверные параметры, например, параметр должен быть «1» или «2», а получено значение «3».
0x2000	INTERNAL	Внутренняя ошибка, например, ресурс не может быть загружен из БД.

А.1. Запросы авторизации

СГУ имеет интерфейс, который упаковывает запросы XML-RPC. Для каждого запроса XML-RPC аутентифицируется токен сеанса, и после этого диспетчер запросов генерирует запрос авторизации, который может включать более одной операции. В таблицах ниже описаны эти запросы из разных команд интерфейса (Таблица 18 – Таблица 29).

Таблица 18 – Команда Onevm

Команда onevm	XML-RPC метод	Запрос
deploy	one.vm.deploy	VM:ADMIN HOST:MANAGE
boot terminate suspend hold stop resume release poweroff reboot	one.vm.action	VM:MANAGE
resched unresched	one.vm.action	VM:ADMIN
migrate	one.vm.migrate	VM:ADMIN HOST:MANAGE
disk-saveas	one.vm.disksaveas	VM:MANAGE IMAGE:CREATE
disk-snapshot-create	one.vm.disksnapshotcreate	VM:MANAGE IMAGE:MANAGE
disk-snapshot-delete	one.vm.disksnapshotdelete	VM:MANAGE IMAGE:MANAGE
disk-snapshot-revert	one.vm.disksnapshotrevert	VM:MANAGE
disk-attach	one.vm.attach	VM:MANAGE IMAGE:USE
disk-detach	one.vm.detach	VM:MANAGE
disk-resize	one.vm.diskresize	VM:MANAGE
nic-attach	one.vm.attachnic	VM:MANAGE NET:USE
nic-detach	one.vm.detachnic	VM:MANAGE
create	one.vm.allocate	VM:CREATE IMAGE:USE NET:USE
show	one.vm.info	VM:USE

chown chgrp	one.vm.chown	VM:MANAGE [USER:MANAGE]
Команда onevm	**XML-RPC метод**	**Запрос**
		[GROUP:USE]
chmod	one.vm.chmod	VM:<MANAGE/ADMIN>
rename	one.vm.rename	VM:MANAGE
snapshot-create	one.vm.snapshotcreate	VM:MANAGE
snapshot-delete	one.vm.snapshotdelete	VM:MANAGE
snapshot-revert	one.vm.snapshotrevert	VM:MANAGE
resize	one.vm.resize	VM:MANAGE
update	one.vm.update	VM:MANAGE
recover	one.vm.recover	VM:ADMIN
save	– (ruby method)	VM:MANAGE IMAGE:CREATE TEMPLATE:CREATE
updateconf	one.vm.updateconf	VM:MANAGE
list top	one.vmpool.info	VM:USE
–	one.vm.monitoring	VM:USE

Таблица 19 – Команда Onetemplate

Команда onetemplate	XML-RPC метод	Запрос
update	one.template.update	TEMPLATE:MANAGE
instantiate	one.template.instantiate	TEMPLATE:USE [IMAGE:USE] [NET:USE]
create	one.template.allocate	TEMPLATE:CREATE
clone	one.template.clone	TEMPLATE:CREATE TEMPLATE:USE
delete	one.template.delete	TEMPLATE:MANAGE
show	one.template.info	TEMPLATE:USE
chown chgrp	one.template.chown	TEMPLATE:MANAGE [USER:MANAGE] [GROUP:USE]
chmod	one.template.chmod	TEMPLATE:<MANAGE/ADMIN>
rename	one.template.rename	TEMPLATE:MANAGE
list top	one.templatepool.info	TEMPLATE:USE

Таблица 20 – Команда Onehost

Команда onehost	XML-RPC метод	Запрос
enable disable offline	one.host.status	HOST:ADMIN
update	one.host.update	HOST:ADMIN
create	one.host.allocate	HOST:CREATE [CLUSTER:ADMIN]
delete	one.host.delete	HOST:ADMIN
rename	one.host.rename	HOST:ADMIN
show	one.host.info	HOST:USE
list top	one.hostpool.info	HOST:USE

Таблица 21 – Команда onecluster

Команда onecluster	XML-RPC метод	Запрос
create	one.cluster.allocate	CLUSTER:CREATE
delete	one.cluster.delete	CLUSTER:ADMIN
update	one.cluster.update	CLUSTER:MANAGE
addhost	one.cluster.addhost	CLUSTER:ADMIN HOST:ADMIN
delhost	one.cluster.delhost	CLUSTER:ADMIN HOST:ADMIN
adddatastore	one.cluster.adddatastore	CLUSTER:ADMIN DATASTORE:ADMIN
deldatastore	one.cluster.deldatastore	CLUSTER:ADMIN DATASTORE:ADMIN
addvnet	one.cluster.addvnet	CLUSTER:ADMIN NET:ADMIN
delvnet	one.cluster.delvnet	CLUSTER:ADMIN NET:ADMIN
rename	one.cluster.rename	CLUSTER:MANAGE
show	one.cluster.info	CLUSTER:USE
list	one.clusterpool.info	CLUSTER:USE

Таблица 22 – Команда onegroup

Команда onegroup	XML-RPC метод	Запрос
create	one.group.allocate	GROUP:CREATE
delete	one.group.delete	GROUP:ADMIN
show	one.group.info	GROUP:USE
update	one.group.update	GROUP:MANAGE
addadmin	one.group.addadmin	GROUP:MANAGE USER:MANAGE

deladmin	one.group.deladmin	GROUP:MANAGE USER:MANAGE
quota	one.group.quota	GROUP:ADMIN
list	one.grouppool.info	GROUP:USE
–	one.groupquota.info	–
Команда onegroup	**XML-RPC метод**	**Запрос**
defaultquota	one.groupquota.update	Только для пользователей из группы «oneadmin»

Таблица 23 – Команда onevdc

Команда onevdc	XML-RPC метод	Запрос
create	one.vdc.allocate	VDC:CREATE
rename	one.vdc.rename	VDC:MANAGE
delete	one.vdc.delete	VDC:ADMIN
update	one.vdc.update	VDC:MANAGE
show	one.vdc.info	VDC:USE
list	one.vdcpool.info	VDC:USE
addgroup	one.vdc.addgroup	VDC:ADMIN GROUP:ADMIN
delgroup	one.vdc.delgroup	VDC:ADMIN GROUP:ADMIN
addcluster	one.vdc.addcluster	VDC:ADMIN CLUSTER:ADMIN ZONE:ADMIN
delcluster	one.vdc.delcluster	VDC:ADMIN CLUSTER:ADMIN ZONE:ADMIN
addhost	one.vdc.addhost	VDC:ADMIN HOST:ADMIN ZONE:ADMIN
delhost	one.vdc.delhost	VDC:ADMIN HOST:ADMIN ZONE:ADMIN

adddatastore	one.vdc.adddatastore	VDC:ADMIN DATASTORE:ADMIN ZONE:ADMIN
deldatastore	one.vdc.deldatastore	VDC:ADMIN DATASTORE:ADMIN ZONE:ADMIN
addvnet	one.vdc.addvnet	VDC:ADMIN NET:ADMIN
Команда onevdc	**XML-RPC метод**	**Запрос**
		ZONE:ADMIN
delvnet	one.vdc.delvnet	VDC:ADMIN NET:ADMIN ZONE:ADMIN

Таблица 24 – Команда onevnet

Команда onevnet	XML-RPC метод	Запрос
addar	one.vn.add_ar	NET:ADMIN
rmar	one.vn.rm_ar	NET:ADMIN
free	one.vn.free_ar	NET:MANAGE
reserve	one.vn.reserve	NET:USE
updatear	one.vn.update_ar	NET:MANAGE
hold	one.vn.hold	NET:MANAGE
release	one.vn.release	NET:MANAGE
update	one.vn.update	NET:MANAGE
create	one.vn.allocate	NET:CREATE [CLUSTER:ADMIN]
delete	one.vn.delete	NET:MANAGE

show	one.vn.info	NET:USE
chown chgrp	one.vn.chown	NET:MANAGE [USER:MANAGE] [GROUP:USE]
chmod	one.vn.chmod	NET:<MANAGE/ADMIN>
rename	one.vn.rename	NET:MANAGE
Команда onevnet	**XML-RPC метод**	**Запрос**
list	one.vnpool.info	NET:USE
lock	one.vn.lock	NET:MANAGE
unlock	one.vn.unlock	NET:MANAGE

Таблица 25 – Команда oneuser

Команда oneuser	XML-RPC метод	Запрос
create	one.user.allocate	USER:CREATE
delete	one.user.delete	USER:ADMIN
show	one.user.info	USER:USE
passwd	one.user.passwd	USER:MANAGE
login	one.user.login	USER:MANAGE
update	one.user.update	USER:MANAGE
chauth	one.user.chauth	USER:ADMIN
quota	one.user.quota	USER:ADMIN

chgrp	one.user.chgrp	USER:MANAGE GROUP:MANAGE
addgroup	one.user.addgroup	USER:MANAGE GROUP:MANAGE
delgroup	one.user.delgroup	USER:MANAGE GROUP:MANAGE
encode	–	–
Команда oneuser	**XML-RPC метод**	**Запрос**
list	one.userpool.info	USER:USE
–	one.userquota.info	–
defaultquota	one.userquota.update	Ony for users in the oneadmin group

Таблица 26 – Команда onedatastore

Команда onedatastore	XML-RPC метод	Запрос
create	one.datastore.allocate	DATASTORE:CREATE [CLUSTER:ADMIN]
delete	one.datastore.delete	DATASTORE:ADMIN
show	one.datastore.info	DATASTORE:USE
update	one.datastore.update	DATASTORE:MANAGE
Rename	one.datastore.rename	DATASTORE:MANAGE
Chown chgrp	one.datastore.chown	DATASTORE:MANAGE [USER:MANAGE] [GROUP:USE]
chmod	one.datastore.chmod	DATASTORE:<MANAGE / ADMIN>

Enable disable	one.datastore.enable	DATASTORE:MANAGE
list	one.datastorepool.info	DATASTORE:USE

Таблица 27 – Команда oneimage

Команда oneimage	XML-RPC метод	Запрос
persistent nonpersistent	one.image.persistent	IMAGE:MANAGE
enable disable	one.image.enable	IMAGE:MANAGE
chtype	one.image.chtype	IMAGE:MANAGE
snapshot-delete	one.image.snapshotdelete	IMAGE:MANAGE
snapshot-revert	one.image.snapshotrevert	IMAGE:MANAGE
snapshot-flatten	one.image.snapshotflatten	IMAGE:MANAGE
update	one.image.update	IMAGE:MANAGE
create	one.image.allocate	IMAGE:CREATE DATASTORE:USE
clone	one.image.clone	IMAGE:CREATE IMAGE:USE DATASTORE:USE
delete	one.image.delete	IMAGE:MANAGE
show	one.image.info	IMAGE:USE
chown chgrp	one.image.chown	IMAGE:MANAGE [USER:MANAGE] [GROUP:USE]

chmod	one.image.chmod	IMAGE:<MANAGE / ADMIN>
rename	one.image.rename	IMAGE:MANAGE
list top	one.imagepool.info	IMAGE:USE
Команда oneimage	**XML-RPC метод**	**Запрос**
lock	one.image.lock	IMAGE:MANAGE
unlock	one.image.unlock	IMAGE:MANAGE

Таблица 28 – Команда onemarket

Команда onemarket	**XML-RPC метод**	**Запрос**
update	one.market.update	MARKETPLACE:MANAGE
create	one.market.allocate	MARKETPLACE:CREATE
delete	one.market.delete	MARKETPLACE:MANAGE
show	one.market.info	MARKETPLACE:USE
chown chgrp	one.market.chown	MARKETPLACE:MANAGE [USER:MANAGE] [GROUP:USE]
chmod	one.market.chmod	MARKETPLACE:<MANAGE / ADMIN>
rename	one.market.rename	MARKETPLACE:MANAGE
enable disable	one.market.enable	MARKETPLACE:MANAGE
list	one.marketpool.info	MARKETPLACE:USE

Таблица 29 – Команда onemarketapp

Команда onemarketapp	XML-RPC метод	Запрос
create	one.marketapp.allocate	MARKETPLACEAPP:CREATE MARKETPLACE:USE
export	(ruby method)	MARKETPLACEAPP:USE IMAGE:CREATE DATASTORE:USE [TEMPLATE:CREATE]
download	(ruby method)	MARKETPLACEAPP:USE
enable disable	one.marketapp.enable	MARKETPLACEAPP:MANAGE
update	one.marketapp.update	MARKETPLACEAPP:MANAGE
delete	one.marketapp.delete	MARKETPLACEAPP:MANAGE
show	one.marketapp.info	MARKETPLACEAPP:USE
chown chgrp	one.marketapp.chown	MARKETPLACEAPP:MANAGE [USER:MANAGE] [GROUP:USE]
chmod	one.marketapp.chmod	MARKETPLACEAPP:<MANAGE / ADMIN>
rename	one.marketapp.rename	MARKETPLACEAPP:MANAGE
lock	one.marketapppool.info	MARKETPLACEAPP:USE
list	one.marketapp.lock	MARKETPLACEAPP:MANAGE
unlock	one.marketapp.unlock	MARKETPLACEAPP:MANAGE

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	Аннулированных					