

АО «Научно-производственный центр «МАКС»

Программный комплекс (ПК) «Звезда»

Руководство администратора

RU.КНРШ.00008-01 90 01

Листов: 931

Москва 2024

АННОТАЦИЯ

Настоящее руководство является основным документом, описывающим порядок действий администратора при работе с комплексом программ «Звезда». 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

1	Введение	15
1.1	Область применения	15
1.2	Краткое описание возможностей	15
1.4	Уровень подготовки персонала	27
2	Назначение и условия применения	28
2.1	Назначение изделия	28
2.2	Условия применения изделия	28
3	Работа ПК «Звезда»	33
3.1	Настройки сервера виртуализации	33
3.1.12	Настройка высокой доступности сервера виртуализации	67
3.2	Работа в Системе группового управления	113
3.3	Операции с Системой резервного копирования	272
3.4	Обновление версии Системы группового управления	310
4	Настройка и работа СХД «Шторм»	313
4.1	Информационная панель	313
4.2	Управление пулами	319
4.3	Конфигурация stormwind	322
4.4	Управление узлами	326
4.5	Управление iscsi дисками	331
4.6	Управление репликацией	333
4.7	Управление rbd	340
4.8.	Управление cifs	341
4.9	Управление nfs	345
4.10	Обслуживание	348
4.11	Управление пользователями	348
4.12	Настройки дедупликации	351
4.13	Обновление	351
4.14	Поддержка thin provisioning	353
4.15	Замена компонентов СХД	354

5	Настройка Программного обеспечения подсистемы VDI	356
5.1	Установка VDI Server	356
5.2	Установка VDI на VMware vSphere	356
5.3	Установка и настройки VDI Actor	357
5.4	Статические настольные ПК Linux	374
5.5	Установка и настройка RDS (Remote Desktop Service).....	383
6	Инструкция по настройке многофункционального комплекса сетевой защиты	543
6.1	Установка ключевой информации	543
6.2	Установка корневого сертификата	543
6.3	Установка ключевой пары	545
6.4	Просмотр ключевой информации.....	548
6.5	Настройка VPN сервиса	549
6.5.1	Управление VPN сервисом	549
6.5.2	Настройка VPN сервиса, режим сервера.....	549
6.5.3	Настройка VPN сервиса, режим мультисервер.....	551
6.5.4	Настройка VPN сервиса, режим клиента	552
6.5.5	Просмотр информации о VPN сервисе.....	554
6.6	Настройка резервирования.....	557
6.6.1	Настройка соединения P2P	558
6.6.2	Настройка соединения P2M.....	559
6.6.3	Настройка L3overVPN.....	559
6.6.4	Настройка L2overVPN.....	559
6.6.5	Настройка VPN сервиса для удаленных пользователей	559
6.7	Инструкция по настройке межсетевого экрана	561
6.7.1	Настройка правил фильтрации	561
	Настройка межсетевого экранирования на уровне L3	561
6.2	Настройка фильтрации по сетевому интерфейсу.....	563
6.3	Настройка фильтрации по общей длине сетевого пакета	565
6.4	Настройка фильтрации по физическому адресу (MAC адрес)	565
6.5	Настройка фильтрации по типу протокола канального уровня	566

6.6	Настройка фильтрации по полю CoS (Class of Service)	570
6.7	Настройка Фильтрации по метке VLAN ID	571
6.8	Настройка фильтрации по ip-адресу источника	572
6.9	Настройка фильтрации по IP-адресу назначения.....	574
6.10	Настройка фильтрации по метке DSCP.....	576
6.11	Настройка фильтрации по биту ECN	577
6.12	Настройка фильтрации по полю длина пакета (Packet Length)	579
6.13	Настройка фильтрации по полю время жизни пакета (TTL)	580
6.14	Настройка фильтрации по биту фрагментации	581
6.15	Настройка фильтрации по протоколу TCP	583
6.16	Настройка фильтрации по протоколу UDP.....	584
6.17	Настройка фильтрации по протоколу ICMP	584
6.18	Настройка фильтрации протоколов, инкапсулируемых в IP	585
6.19	Настройка фильтрации по типу соединения	586
6.20	Настройка фильтрации произвольных данных.....	587
6.7.2	Настройка межсетевого экранирования на уровне L2	588
7.10	Настройка фильтрации по сетевому интерфейсу	593
7.11	Настройка фильтрации по общей длине сетевого пакета.....	594
7.12	Настройка фильтрации по физическому адресу (MAC адрес)	595
7.13	Настройка фильтрации по типу протокола канального уровня	596
7.14	Настройка фильтрации по полю CoS (Class of Service) ...	597
7.15	Настройка фильтрации по метке VLAN ID.....	599
7.16	Фильтрация по IP-адресу источника	600
7.17	Фильтрация по ip-адресу назначения	602
7.18	Фильтрация по метке DSCP.....	605
7.19	Настройка межсетевого экранирования по расписанию	606
7.20	Настройка межсетевого экранирования по доменному имени	610

7.21	Настройка логирования правил фильтрации	612
7.22	Создание группы ip-адресов	614
7.23	Создание правила фильтрации на основе группы ip-адресов	617
7.24	Создание группы сетевых портов	620
7.25	Создание правила фильтрации на основе группы сетевых портов	624
7.26	Настройка счетчика пакетов для правила фильтрации ...	627
7.27	Настройка комментария для правила фильтрации	630
6.7.3	Синхронизация правил фильтрации	632
8.1	Настройка устройства в режиме Master	633
8.2	Настройка устройства в режиме Slave	633
8.3	Создание группы с правилами фильтрации	634
8.4	Управление подчиненными устройствами	637
8.5	Правило фильтрации по умолчанию	640
6.7.4	Сценарий применения межсетевого экрана	642
6.8	Фильтрация доступа к устройству по протоколу https и ssh	642
6.9	Фильтрация защищенного соединения	650
9.3	Фильтрация по IP-адресу	656
9.4	Фильтрация протокола UDP	660
9.5	Фильтрация протокола TCP	662
9.6	Фильтрация по расписанию.	665
9.7	Логирование правил фильтрации	669
9.8	Фильтрация на уровне L2 в таблице Bridge	672
9.9	Фильтрация на основе VLAN ID	676
6.8	Аварийные ситуации	682
7.	Введение в ПК “Защищенный проксирующий сервер управления виртуальной инфраструктурой”	684
7.1	Структура ПК “Защищенный проксирующий сервер управления виртуальной инфраструктурой”	684
7.2	Системные требования	684
7.3	Развертывание изделия	684
7.3.1	Подготовка к работе	684

7.3.2 Установка Squid в Альт	685
7.4 Начало работы	686
7.4.1 Настройка прокси-сервера Alterator-squid	686
7.4.2 Настройки политики доступа пользователей во внешнюю сеть.....	690
7.4.3 Просмотр статистики работы прокси-сервера	693
7.5 Централизованный выход в Интернет через один сервер в сети (проxy) ...	694
7.5.1 Обычный доступ.....	694
7.5.2 Анонимизирующий доступ	695
7.5.3 Прозрачный” доступ.....	695
7.5.4 Фильтрация доступа	696
7.5.5 Авторизация доступа.....	697
7.6 Локальное хранение данных, которые уже запрашивались пользователями (cache).....	697
7.6.1 Обычное кеширование	698
7.6.2 Выборочное кеширование	701
7.6.3 Иерархия серверов.....	701
7.7 Обратное проксирование и кеширование внутренних серверов (accelerate).....	702
7.7.1 Обычное обратное проксирование (один сервер)	702
7.7.2 Множественное проксирование.....	702
7.8 Сбор статистики и ограничение полосы доступа	703
7.9 Кеширование DNS-запросов.....	704
8 Подсистема мониторинга «Горизонт-ВС»	705
8.1 Назначение Подсистемы.....	705
8.2 Назначение документа	705
8.3 Требования к квалификации администратора	705
8.4 Вход в Веб-интерфейс Подсистемы мониторинга	706
8.4.1 Требования к рабочему месту	706
8.4.2 Аутентификация пользователя	706
8.4.3 Смена временного пароля	708
8.4.4 Стартовая страница Веб-интерфейса Подсистемы мониторинга.....	711

8.5 Особенности использования пробной версии Подсистемы мониторинга ..	711
8.5.1 Работа в пробной версии Подсистемы мониторинга	711
8.5.2 Активация лицензии по завершению работы с пробной версией Подсистемы мониторинга	713
8.6 Подключение Подсистемы мониторинга к Системе виртуализации «Горизонт-ВС»	715
8.7 Веб-интерфейс Подсистемы мониторинга. Функции администратора	722
8.7.1 Общие данные о веб-интерфейсе Подсистемы мониторинга	722
8.7.2 Перечень функций администратора в веб-интерфейсе Подсистемы мониторинга «Горизонт-ВС»	725
8.7.3 Управление пользователями	727
8.7.3.1 Доступ к функции. Назначение и состав подраздела «Пользователи»	727
8.7.3.2 Список пользователей.....	728
8.7.3.3 Добавление нового пользователя.....	729
8.7.3.4 Удаление пользователя	730
8.7.3.5 Просмотр и редактирование данных пользователя	731
8.7.3.6 Смена временного пароля	733
8.7.4 Настройка мониторинга оборудования «Горизонт-ВС»	736
8.7.4.1 Доступ к функции	736
8.7.4.2 Настройка мониторинга оборудования «Горизонт-ВС» в разделе интерфейса «Администрирование»	736
8.7.4.3 Подключение оборудования из раздела интерфейса «Состояния»	744
8.7.5 Настройка системы рассылки уведомлений	746
8.7.5.1 Доступ к функции. Назначение и состав	746
8.7.5.2 Управление группами адресатов рассылки.....	748
8.7.5.3 Управление рассылками	754
8.7.6 Настройка триггеров	758
8.7.6.1 Доступ к функции. Назначение и состав.....	758
8.7.6.2 Список триггеров.....	760
8.7.6.3 Сортировки записей в списке триггеров по значениям полей	761
8.7.6.4 Создание нового триггера	762
8.7.6.5 Удаление триггера	765

8.7.6.6	Просмотр и редактирование параметров триггера.....	766
8.7.7	Настройка подключения к почтовому серверу Подсистемы мониторинга	768
8.7.7.1	Доступ к функции. Назначение и состав.....	768
8.7.7.2	Подключение почтового сервера после установки Подсистемы мониторинга	769
8.7.7.3	Корректировка данных при подключении сервера	772
8.7.7.4	Редактирование настроек почтового сервера.....	773
8.7.7.5	Проверка работы почтового сервера.....	774
8.7.8	Настройка взаимодействия с системой мониторинга Zabbix.....	775
8.7.8.1	Доступ к функции. Назначение и состав.....	775
8.7.8.2	Настройка взаимодействия с системой Zabbix после установки Подсистемы мониторинга	777
8.7.8.3	Редактирование настроек взаимодействия с Zabbix.....	779
8.7.9	Настройка отправки зафиксированных Подсистемой мониторинга событий на сторонние syslog-серверы.....	780
8.7.9.1	Доступ к функции. Назначение и состав.....	780
8.7.9.2	Настройка отправки зафиксированных событий на syslog-серверы после установки Подсистемы мониторинга	782
8.7.9.3	Редактирование настроек взаимодействия с syslog-серверами	785
8.7.9.4	Управление списком syslog-серверов.....	785
8.7.10	Настройка отправки зафиксированных событий в виде SNMP trap-сообщений на сторонние ресурсы	787
8.7.10.1	Доступ к функции. Назначение и состав.....	787
8.7.10.2	Настройка отправки зафиксированных событий в виде SNMP trap-сообщений после установки Подсистемы мониторинга.....	789
8.7.10.3	Редактирование настроек взаимодействия со сторонними ресурсами с использованием SNMP trap-сообщений	792
8.7.10.4	Управление списком ресурсов для приема SNMP trap-сообщений	793
8.7.11	Изменение УЗ, используемой для подключения к СГУ	794
8.7.11.1	Доступ к функции	794
8.7.11.2	Ввод данных новой учетной записи	795

8.7.12 Изменение ключа SSH, используемого для подключения к гипервизору	796
8.7.12.1 Доступ к функции	796
8.7.10.2 Замена ключа SSH	797
8.7.12 Импорт конфигураций Подсистемы мониторинга	798
8.7.12.1 Доступ к функции	798
8.7.13.2 Импорт файлов с конфигурациями	799
8.7.13 Экспорт конфигураций Подсистемы мониторинга	800
8.7.13.1 Доступ к функции	800
8.7.12.2 Экспорт конфигураций	801
8.7.13 Отключение Подсистемы мониторинга от СГУ	801
8.7.13.1 Доступ к функции	801
8.7.13.2 Отключение от СГУ	802
8.7.14 Управление мониторингом объектов «Горизонт-ВС»	804
8.7.14.1 Доступ к функции. Назначение и состав	804
8.7.14.2 Список сборщиков данных	806
8.7.14.3 Приостановка/Запуск опроса всех сборщиков данных объекта мониторинга	807
8.7.14.4 Приостановка/Запуск отдельного сборщика данных	810
8.7.14.5 Настройка временного интервала опроса	811
8.7.15 Формирование диагностических отчётов	814
8.7.15.1 Доступ к функции	814
8.7.15.2 Формирование, выгрузка и просмотр диагностического отчета	817
8.7.16 Переход в СГУ Системы виртуализации «Горизонт-ВС»	822
9 Первоначальные настройки в средстве виртуализации “Звезда”	824
9.1 Смена пароля пользователя root	824
9.2 Обновление СВ “Звезда”	827
9.3 Защита среды виртуализации	834
9.4 Создание и удаление пользователей	835
9.5 Управление ролевым доступом	836
9.6 Резервное копирование с использованием файловой системы Overlayfs	867

9.7 Централизованное управление образами контейнеров и контейнерами...	873
9.8 Работа с виртуальными машинами.....	881
9.9 Создание снимков системы	890
ПРИЛОЖЕНИЯ.....	898
Приложение А. Особенности формирования списков пользователей при создании (редактировании) групп адресатов рассылки	898
Приложение Б. Особенности формирования рассылки	902
ПРИЛОЖЕНИЕ А	911
ПРИЛОЖЕНИЕ Б	913
ПРИЛОЖЕНИЕ В	915
Описание XML-RPC API (справочное)	915

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

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

Виртуальный диск (том)	Логическое устройство, с которым ВМ взаимодействует как с диском
Гипервизор	Программа, создающая среду функционирования других программ (в том числе других гипервизоров)
	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 Состав 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 «Звезда» предоставляет пользователям следующие возможности:

- Поддержка интеграцию с внешними системами контроля версионности;

- 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);

Поддержка режима работы узлов, при котором Control, Compute, Storage компоненты расположены исключительно на разных серверах

Поддержка предоставления аппаратного обеспечения в монопольное использование какой-либо сетевой функции (предоставление bare metal);

Поддержка работы узлов в режиме гиперконвергенции, т.е. Control, Compute, Storage компоненты расположены на одном сервере;

Поддержка вынесения аппаратных ресурсов за пределы ЦОД (edge ноды) с сохранением управления этими ресурсами с единой системы управления Платформой;

Поддержка защиты виртуальных машин от паразитного трафика (трафик, не предназначенный конкретной виртуальной машине должен быть отброшен на виртуальном порту на входном направлении и не попасть в сетевой стек виртуальной машины);

Поддержка подключения серверного оборудования, на базе которого разворачивается платформа, должно выполняться по отказоустойчивой схеме (подключение к двум физическим коммутаторам с использованием протоколов агрегации портов LACP в режиме Active-Active);

Поддержка использования для хранения виртуальных жестких дисков виртуальных машин (блочное хранилище) локальные диски вычислительных узлов Платформы;

Поддержка наличия документированного API для администрирования и управления системой хранения (разворачивание новых узлов, настройка кластера, обслуживание, мониторинг статуса);

Поддержка технологии Virtio-net Multi-Queue на уровне ОС, драйверов NIC, а также виртуальных коммутаторов (при их наличии в решении);

Поддержка контейнерной инфраструктуры Docker;

- Поддержка изменения параметров контейнеров (увеличение vCPU/RAM) без влияния на работу контейнеров;

- Поддержка изменения параметров виртуальных машин (увеличение vCPU/RAM);

- Поддержка изменения параметров контейнеров (добавление сетевых портов, виртуальных дисков) без влияния на работу контейнеров;

- Поддержка изменения параметров контейнеров (уменьшение vCPU/RAM);

- Поддержка изменения параметров контейнеров (удаление сетевых портов, виртуальных дисков);

- 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;

- поддержка HyperThreading;

- поддержка интерфейсов VNFM, VNFO;

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

- поддержка технологии huge pages;

- поддержка средства автоматизации ansible;

- подключение к транспортной сети осуществляется с использованием резервирования;

- поддержка функции Multipathing;

- поддержка CPU pinning;
- поддержка maintenance mode;
- Программный комплекс базируется на программном обеспечении с открытым программным кодом – OpenNebula, qemu, KVM;
- Поддержка интеграции с DLP (в том числе с использованием протокола ICAP);
- Поддержка управления службой каталогов LDAP (в том числе LDAPS);
- - обеспечивается работа ядра в реальном времени;
- функционирование средств защиты информации:
- виртуальных систем обнаружения вторжения;
- межсетевых экранов;
- поддержка зон доступности;
- поддержка технологии ускорения DPDK
- антивирусных средств;
- Поддержка образов гипервизора от производителя с интегрированными драйверами и сервисами;
- 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;
- ограничение и приоритезация ресурсов для ВМ;
- поддержка протокола Corba;
- поддержка объектных хранилищ;
- поддержка коммутации и маршрутизации трафика между сетями функций;

- Поддержка нескольких портов одной ВМ;
- поддержка резервируемого подключения ко внешней сети с использованием списков контроля;
- создание виртуальных машин (ВМ), их образов и шаблонов с поддержкой 32 и 64-битных гостевых операционных систем;
- Поддержка протокола XML;
- Поддержка протоколов FTP, SFTP, SCP;
- Поддержка traceroute, ICMP, udp ping, tcpdump;
- возможность управления конфигурацией ВМ с помощью графического и консольного интерфейсов;
- возможность увеличения количества хостов без остановки работы других хостов;
- поддержка
- Поддержка резервирования ресурсов для виртуальной машины;
- 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;

Поддержка разделения виртуализированных ресурсов на изолированные ресурсные зоны;

- Поддержка изоляции служб и процессов;

- Поддержка изолированного внутреннего репозитория;

- Поддержка протоколирования событий, связанных с безопасностью;

- Поддержка RBAC с возможностью интеграции с внешними контроллерами доменов (AD) Заказчика по протоколу LDAP;

- Поддержка единого журнала событий

- Поддержка выгрузки журнала событий на внешний лог сервер;

Поддержка фильтрации трафика с помощью ACL на уровнях L3-L4;

Поддержка служб SELinux и iptables для защиты Платформы от несанкционированного доступа, как из внешней сети, так и с виртуальных машин, контейнеров, выделенных в монопольное использование серверов;

Поддержка шифрования подключений к программному комплексу (через GUI, CLI, API);

- Поддержка записи в журнал сбора системных логов и уведомлений все подключения к Платформе и совершаемые пользователями (включая m2m)

действия и команды, выполняемые/исполняемые через любой канал управления Платформой (GUI/CLI/API);

- Поддержка хранения журнала лога в открытом формате (.log/.txt) с глубиной не менее 7 дней, и в архивном формате (.gz,.rar,.gz,.zip) с глубиной не менее 30 дней;

- Поддержка опправки сообщений журнала лога на внешние лог серверы (работа с не менее чем 2-мя внешними syslog серверами);

- Поддержка списков контроля доступа (ACL) на исходящем направлении трафика для всех уровней сетевой связности (порт/IP/протокол);

- Поддержка механизмов контроля целостности пакетов ПО, плейбуков, темплейтов, используемых для развертывания, обновления, расширения;

- Поддержка m2m пользователей, используемых для внутреннего взаимодействия между службами/процессами;

- Поддержка внутреннего DNS сервера для разрешения доменных имен служб и процессов при взаимодействии внутренних компонент между собой;

- 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;

- поддержка более чем 48 вычислительных нод;

- поддержка статической маршрутизации между сетями;

- поддержка overlay тоннелей на программных коммутаторах;

- 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, приоритизации и резервирования 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 Ballooning;

- обеспечивается предоставление ресурсов без переподписки;

- 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 снимков 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.
 - поддержка обновлений системы;
- 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, serph и S3-хранилища).

1.3 Структура ПК «Звезда»

ПК «Звезда» состоит из следующих основных компонентов:

Таблица 1.1

Обозначение изделия	Наименование изделия	Количество	Порядковый	Примечание

			учетный номер	
RU.КНРШ.00008-01	1 Программный комплекс “Звезда” в составе:			Примечание 3
МБРЦ.468313.001	1.1 Программно- аппаратный комплекс (ПАК) “Горизонт- ВС”			Примечание 4,5
RU.КНРШ.00014-01	1.2 Средство виртуализации “Звезда”			Примечание 5
RU.КНРШ.00007-01	1.3 Система хранения данных “Шторм”			Примечание 6
RU.КНРШ.00006-01	1.4 Программное обеспечение подсистемы VDI			
61649217.401200.003	1.5 Многофункциональный комплекс сетевой защиты «Diamond VPN/FW» (редакция для ПК «Звезда»)			Примечание 7

Примечания

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

2 Составные части ПК “Звезда” поставляются на одном USB-носителе.

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

4 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.

5 В состав ПК “Звезда” может опционально входить в качестве гипервизора либо ПАК “Горизонт-ВС”, либо гипервизор СВ “Звезда”.

6 Система хранения данных “Шторм” зарегистрирована в Реестре российского программного обеспечения (запись в реестре от 13.02.2023 №16626).

7 Права на Многофункциональный комплекс сетевой защиты «Diamond VPN/FW» принадлежат ООО «ТСС». 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) «Звезда» 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.

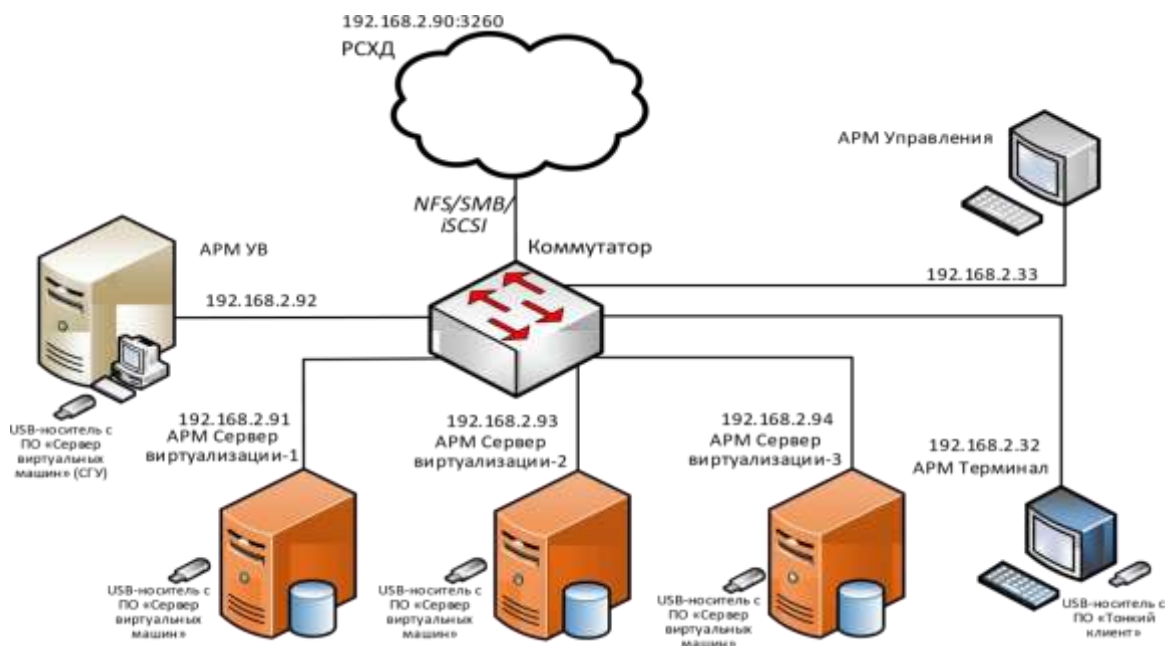


Рисунок 1 - Пример схемы стенда

1.4 Уровень подготовки персонала

Администраторы СГУ «Звезда» 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.

2 Назначение и условия применения

2.1 Назначение изделия

Изделие предназначено для использования в клиент-серверных системах.

2.2 Условия применения изделия

ПК «Звезда» 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) «Звезда» 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 «Звезда» 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) «Звезда»

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

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

Характеристика	Показатель
Количество процессоров сервера виртуализации, поддерживаемых гипервизором	от 2 до 4096
Объем оперативной памяти сервера	от 4 Гб до 256 Тб

виртуализации, поддерживаемый гипервизором	
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 40 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
Совместимость с процессорами	x86_64
Поддержка TLS	TLS_AES_128_GCM_SHA256; TLS_AES_256_GCM_SHA384; TLS_CHACHA20_POLY1305_SHA256; TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256; TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256; TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256; TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384; TLS_DHE_RSA_WITH_AES_128_GCM_SHA256; TLS_DHE_RSA_WITH_AES_256_GCM_SHA384.
Количество блочных устройств, поддерживаемых гипервизором (по протоколам FC, iSCSI)	- 2048 для iSCSI; - 4096 для FC;
Поддерживаемое гипервизором число блочных устройств,	До 512

подключенных по протоколам iSCSI и FC	
Количество поддерживаемых путей к каждому блочному устройству, подключенным с помощью протоколов FC и iSCSI	16 и более
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; ПЕД ОС; 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

3 Работа ПК «Звезда»

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) «Звезда» на экране появится окно аутентификации (Рисунок 2).

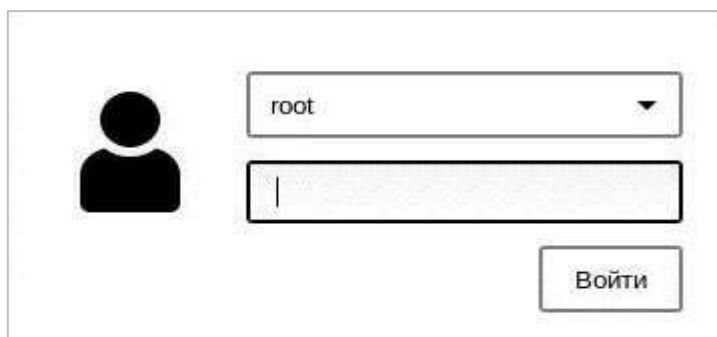


Рисунок 2 - Окно аутентификации

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) «Звезда» 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) «Звезда» 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) «Звезда», следует выполнить данные действия:

1. Открыть доступ к серверу по **ssh**, отредактировав конфиг

`/etc/ssh/sshd_config`. Изменить параметр `PermitBootLogin` на `yes`

(предварительно следует раскомментировать его). Далее изменить параметр **PasswordAuthentication** на **yes**. Далее следует перезапустить службу **ssh** командой:

```
rc-service sshd
restart
```

2. Создать **bond**.

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  
rcupdate del sanlock rcupdate  
del lvmlockd rcupdate del  
lvmetad rc-service wdmd stop  
rcservice sanlock stop  
rcservice 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.

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

Для настройки сетевой карты необходимо создать символическую ссылку 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 IP-адресов. 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) «Звезда» 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) «Звезда» 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 hvsw0 eth0
```

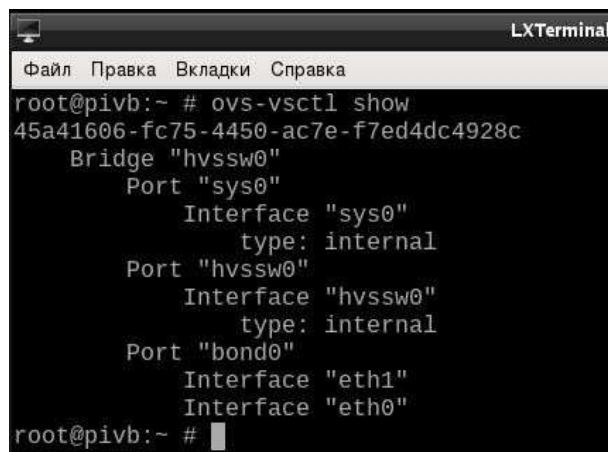
2. Создать бонд из двух физических интерфейсов eth0, eth1 и добавить его в коммутатор Open vSwitch командой:

```
# ovs-vsctl add-bond hvsw0 bond0 eth0 eth1
```

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

```
# ovs-vsctl show
```

Будет получен ответ следующего вида (**Рисунок 3**).



```
root@pivb:~ # ovs-vsctl show
45a41606-fc75-4450-ac7e-f7ed4dc4928c
    Bridge "hvssw0"
        Port "sys0"
            Interface "sys0"
                type: internal
        Port "hvssw0"
            Interface "hvssw0"
                type: internal
        Port "bond0"
            Interface "eth1"
            Interface "eth0"
```

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.
- поддерживается возможность управления мониторингом с помощью API.

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. Поддерживаются версии SNMPv2, SNMPv3.

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) «Звезда» 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/syslogd. 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-remoteipv6logging.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
sslv 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* и *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.

- а. Выполнить команды:

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

- а. 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:

```

h108 ~ # targetcli ls
o- / ..... [..]
| o- backstores ..... [..]
| | o- block ..... [Storage Objects: 1]
| | | o- dc1-0 ..... [/dev/loop0 (97.7GiB) write-thru activated]
| | | | o- alua ..... [ALUA Groups: 1]
| | | | | o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
| | o- fileio ..... [Storage Objects: 0]
| | o- pscsi ..... [Storage Objects: 0]
| | o- ramdisk ..... [Storage Objects: 0]
| o- iscsi ..... [Targets: 1]
| | o- iqn.2020-04.bkd.hp-iscsi:dfd42696a8b5 ..... [TPGs: 1]
| | | o- tpg1 ..... [gen-acls, no-auth]
| | | | o- acls ..... [ACLs: 0]
| | | | o- luns ..... [LUNs: 1]
| | | | | o- lun0 ..... [block/dc1-0 (/dev/loop0) (default_tg_pt_gp)]
| | | | o- portals ..... [Portals: 1]
| | | | | o- 0.0.0.0:3260 ..... [OK]
| o- loopback ..... [Targets: 0]
| o- whost ..... [Targets: 0]
| o- non-persistent ..... [Targets: 0]
h108 ~ #

```

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**:

а. 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-40ebb9b60bb3b767f9be
```

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 clon diskorder Mandatory: dlm_c
clon disk0
crm(live)configure# order clonegfsorder Mandatory: dlm_c
clon disk0 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: clon disk0 [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) «Звезда» 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 12М 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)
```

```
[lv010_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) «Звезда» 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 hvsw0*):

```
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
```

3.1.12 Настройка высокой доступности сервера виртуализации

Для обеспечения высокой доступности сервера предусмотрено две возможности:

использование механизма RAFT, встроенного в сервер (см. п. 0). В этом случае должно быть обеспечено внешнее хранилище или база данных (mysql) со своими механизмами обеспечения высокой доступности.

использование кластера на базе Pacemaker (см. п. 0).

Для этого необходимо создать общее хранилище, доступное для узлов. путем использования:

внешнего хранилища, подключаемого через NFS или iSCSI/Fiber Channel LUN; подсистемы DRBD, которая позволяет реплицировать локальные для узлов кластера блочные устройства.

Использование механизма RAFT

Для обеспечения отказоустойчивости и восстановления виртуальных машин предусмотрен механизм создания кластера высокой доступности – алгоритм RAFT. Данный алгоритм выполняет функции:

- перезапуск ВМ на рабочем узле кластера в случае аварии;
- безопасная и эффективная реализация конечного автомата поверх кластерной вычислительной системы.

Алгоритм перезапуска ВМ обладает следующими особенностями:

- чёткое разделение фаз. RAFT предлагает декомпозицию задачи управления кластером на несколько, слабо связанных, подзадач. Основные подзадачи: выбор лидера (голосование) и репликация протоколов. Каждая из этих задач допускает более детальное разделение.

- на кластере всегда существует явно выделенный лидер. Только этот лидер отправляет новые записи на другие узлы кластера. Остальные узлы следуют за лидером и не взаимодействуют между собой (за исключением фазы голосования). Если внешний клиент подключается к кластеру через обычный узел, то все его запросы перенаправляются лидеру и только оттуда поступают на узлы.

- протоколы работы не могут содержать пропусков. Записи добавляются строго последовательно.

- изменение размера кластера. RAFT позволяет легко менять конфигурацию кластера, не останавливая работы: добавлять или удалять узлы;

основной и резервный узлы подключаются к общему сетевому хранилищу, используемому как разделяемое блочное устройство. На нем размещаются образы ВМ, для которых требуется организовать режим высокой доступности. Конфигурационные файлы ВМ также размещаются на общем хранилище и доступны на обоих вычислительных узлах. В случае выхода из строя основного узла после наступления таймаута, заданного администратором системы, которое обычно составляет 10-15 секунд, на резервном узле автоматически начинается загрузка виртуальных машин.

Каждый узел может находиться в одном из 3-х состояний:

лидер (Leader);

кандидат (Candidate);

ведомый (Follower).

Управление кластером четко разделено на две фазы:

1) Выборы лидера (голосование);

Репликация (передача данных протокола).

Настройка Системы группового управления в режиме RAFT

Для настройки СГУ в режиме RAFT необходимо развернуть СГУ минимум на трех серверах:

1. Загрузить на один гипервизор архив с СГУ ***hcs-<версия>.tar.gz*** в директорию ***/data/0***.

Перейти в директорию ***/ansible/raft*** и в файле ***hosts.yaml*** ввести IP-адреса всех серверов виртуализации, которые будут введены в режим RAFT.

В файле ***group_vars/all.yaml*** заполнить следующие данные:

IP-адреса (лидера, последователей и всех серверов в пуле);

load_path (указать путь к директории, где лежит образ СГУ, например ***/data/0***);

image (указать версию СГУ, например, ***hcs:1.0.28***);

floating_ip (ввести плавающий IP-адрес, выделенный в той же сети).

Если необходимо обновить версию СГУ, разослать архив с СГУ командой:

```
ansible stand1 -m shell -a «scp <IP- сервера>:<директория с образом СГУ>»
```

Загрузить новую версию СГУ командой:

```
ansible-playbook raft_sgu.yaml
```

Запустить развёртывание СГУ (контейнер уже загружен в Docker и подписан) командой:

```
ansible-playbook raft_sgu.yaml -v --tags start_HCS
```

Проверить корректность выполнения:

```
ansible all -m shell -a «docker exec hcs cat  
/etc/one/oned.conf | grep SERVER_ID»
```

Убедиться, что все цифры **SERVER_ID** разные.

Если есть одинаковые цифры, то выполнить команду:

```
ansible-playbook raft_sgu.yaml --tags conf
```

и повторить пункт 5.

Настройки при уже развернутой Системе группового управления

Для выполнения настроек при наличии уже развернутой СГУ:

1. Перейти в директорию **/ansible/raft** и в файле **group_vars/all.yaml** установить значение **leader_ip** = IP-адрес работающего СГУ.

В файле **hosts.yaml**:

Изменить IP-адрес в группе **leader** на IP-адрес работающей СГУ.

Установить значение **follower_ip u sgu_host_ips** на все IP-адреса, которые войдут в режим RAFT.

Запустить команду:

```
ansible-playbook convert_solo_to_raft_sgu.yaml
```

и дождаться ее завершения.

Обновление версии Системы группового управления

1. Перейти в директорию **/ansible/raft** и в файле **group_vars/all.yaml** заполнить следующие данные:

load_path (указать путь к директории, где лежит новая версия СГУ, например **/data/0**);

image (указать новую версию СГУ, например, **hcs:1.0.28**);

Запустить процесс обновления командой:

```
ansible-playbook update_sgu_version.yaml
```

Объединение контейнеров в отказоустойчивую систему

1. Выбрать сервер виртуализации с СГУ, в котором нужно сохранить данные. В файлах *hosts.yaml* и *group_vars/all.yaml* изменить IP-адрес в группе leader на IP-адрес сервера с работающей СГУ.

Установить значение `follower_ip` и `sgu_host_ips` на все IP-адреса.

Запустить процесс объединения командой:

```
ansible-playbook convert_solo_toRAFT_sgu.yaml
```

Добавление и удаление серверов в HA-кластере

Для добавления/удаления серверов из HA-кластера:

1. В файлах *hosts.yaml* и *group_vars/all.yaml* изменить IP-адреса серверов виртуализации (добавить или удалить из кластера).

Запустить процесс обновления состава серверов в HA-кластере:

```
ansible-playbook raft_sgu.yaml
```

Описание тегов *raft_sgu.yaml*:

«start_HCS»: разворачивание RAFT из уже загруженного контейнера;

«sign»: подпись контейнеров;

«conf»: изменение конфигурационного файла OpenNebula:

 `LISTEN\_ADDRESS`;

 `Hooks`;

«conf_server_id»: изменение `SERVER\_ID` в конфигурационном файле;

«back»: создание резервной копии БД на лидере;

«rec»: восстановление БД на последователях из резервной копии лидера;

«add»: добавление узлов в кластер, если их там еще нет;

«reboot»: перезагрузка всех узлов кластера.

Описание тегов «destrukt_RAFT_all.yaml»:

«no_del_volume»: разбор кластера без удаления volume (сохраняет БД).

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.

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

```

# fence-peer «/usr/lib/drbd/crm-fence-
peer.sh»;;
split-brain «/usr/lib/drbd/notify-split-
brain.sh root»;;
initial-split-brain
«/usr/lib/drbd/notify-split-brain.sh root»;;
out-of-sync «/usr/lib/drbd/notify-out-
of-sync.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-
wfc-timeout 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
resync-after 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
shared-secret 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;
    } }

```

На обоих узлах репликации выполнить команду в консоли:

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

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

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

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
```

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.

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

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

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

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

Включить ресурс на каждом узле выполнением команды в консоли:

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

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.
```

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
```

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.

Скопировать созданный конфигурационный файл на все узлы кластера.

Запустить на всех узлах кластера службу `corosync` командой:

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

Проконтролировать работу транспортного уровня командой:

```
# corosync-quorumtool
```

в выводе которой должны присутствовать все узлы кластера.

Настройка Pacemaker

Для настройки Pacemaker:

1. Запустить на всех узлах кластера службу `pacemaker` командой

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

Проконтролировать состояние кластера командой

```
# crm status
```

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

Настройка высокой доступности сервера

Для запуска сервера в режиме высокой доступности:

1. Настроить кластер Pacemaker в соответствии с п. 0.

Остановить и удалить из автозагрузки на всех узлах кластера службы `one` следующими командами:

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

На двух узлах выделить под реплицируемое хранилище диск или раздел.

Настроить и запустить для них репликацию в соответствии с п.0. Задать имя DRBD-ресурса – `hcs`.

Остановить и убрать из автозагрузки на обоих узлах службу `drbd` командами:

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

На обоих узлах отключить DRBD-ресурс командой:

```
# drbdadm down hcs
```

Настроить DRBD-ресурс:

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

```
# crm configure
```

Отключить фенсинг:

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

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»
```

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»
```

Актуализировать изменения конфигурации кластера:

```
# commit
```

Выйти из оболочки управления ресурсами:

```
# bye
```

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

```
# crm status
```

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

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

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

Смонтировать хранилище в каталог **/mnt**:

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

Скопировать данные:

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

Отмонтировать хранилище:

```
# umount /mnt
```

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

На одном из узлов войти в оболочку управления ресурсами кластера Расетакер, в раздел конфигурации, командой:

```
# crm configure
```

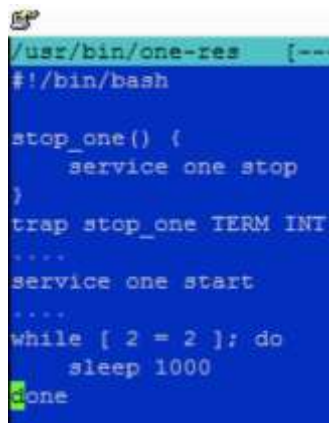
Создать примитив виртуального IP:

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

Создать примитив точки монтирования:

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

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



```
/usr/bin/one-res {--  
#!/bin/bash  
  
stop_one() {  
    service one stop  
}  
trap stop_one TERM INT  
....  
service one start  
....  
while [ 2 = 2 ]; do  
    sleep 1000  
done
```

Рисунок 5 – Создание примитива запуска СГУ

Создать примитив запуска СГУ:

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

Создать группу ресурсов:

```
group g_hcs fs_hcs ip_hcs hcs
```

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

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

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
```

Актуализировать изменения конфигурации кластера:

```
commit
```

Выйти из оболочки управления ресурсами:

```
bye
```

Проконтролировать состояние ресурсов кластера можно командой:

```
crm status
```

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 закриптовано, 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, находятся 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; cmdtimeoutlong 600;
          }  common {
handlers {
                                # These are EXAMPLE handlers
only.
                                # They may have severe
implications,
                                # like hard resetting the node
under certain circumstances.
                                # Be careful when choosing your
poison.

                                pri-on-incon-degr
«/usr/lib/drbd/notifyprion-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/crmfencepeer.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/notifyout-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
outdatedwfctimeout 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-epochsize 8192;

```

```
maxbuffers 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 rrconflict
                                # ping-timeout
data-integrity-alg sha1;                                #
tcp-cork on-congestion
                                # congestion-fill congestion-
extents                                csums-alg sha1;
                                # verify-alg
# userle                                after-sb-0pri discard-
zero-changes;                                after-sb-1pri discard-
secondary;                                aftersb-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 `Расетакер`, 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  
mastermax=«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 Расетакер, 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 ***pskill lighttpd***.

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) «Звезда» обеспечивает управление потоками информации между компонентами виртуальной инфраструктуры:

- фильтрацию;
- маршрутизацию;
- контроль соединения.

Создание виртуальных сетей описано в главе **Ошибка! Источник с 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**.

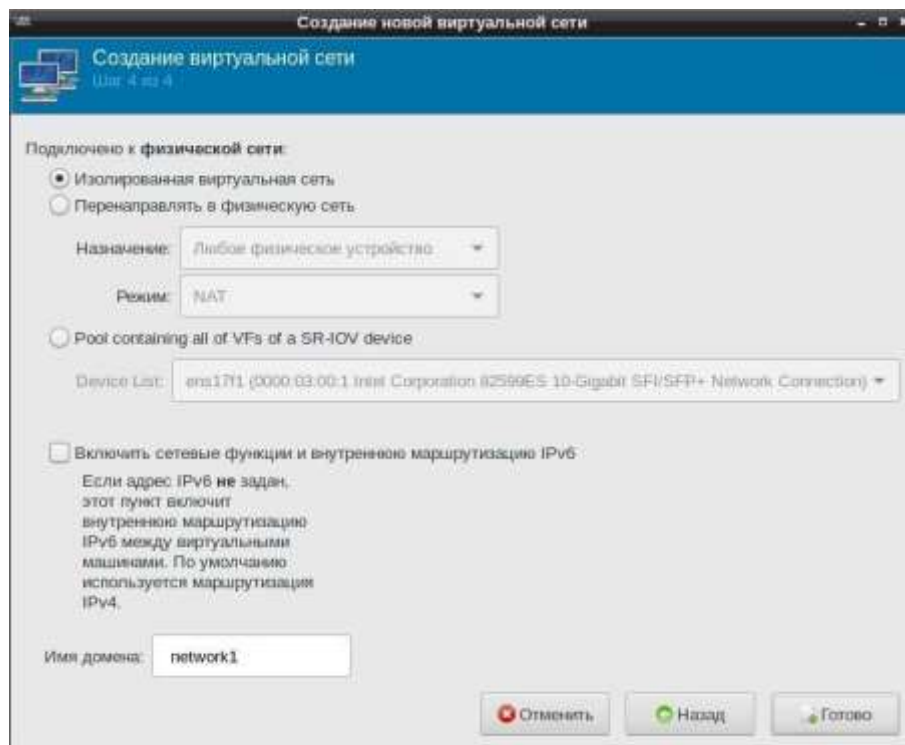


Рисунок 6 - Подключение к физической сети

4. Назначить виртуальную сеть VM на сервере виртуализации.

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) «Звезда» 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) «Звезда» 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 IP-адресами пользователя этого порта. Тем самым серверы и терминалы Программный комплекс (ПК) «Звезда» 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) «Звезда» терминалы и серверы Программный комплекс (ПК) «Звезда» 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 НВА, кабеля или коммутатора (если каждый НВА 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 событиях 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

«Звезда» со сторонним программным обеспечением

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

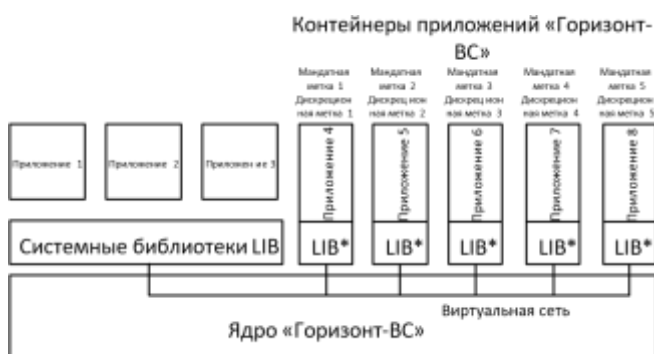


Рисунок 7 - Контейнеры приложение «Звезда»

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

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

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) «Звезда». 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/gvsccontainers/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) «Звезда» 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/
```

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

	<i>Administrator@win.gorizont-vs.ru)</i>
: 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 <i>win.gorizont-vs.ru</i> получим базовое DN: <i>DN = win, DN = gorizont-vs, DN = ru.</i>
: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

```
./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:

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) «Звезда» 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) «Звезда» 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).

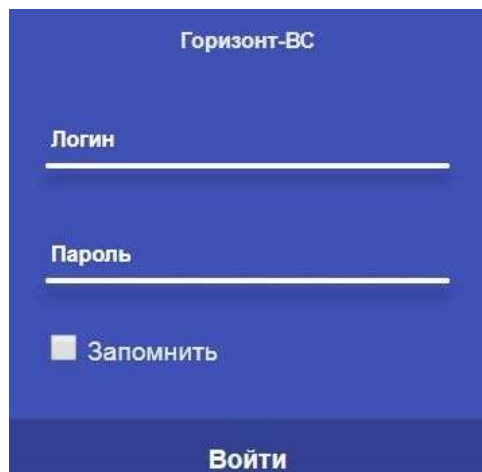


Рисунок 8 - Окно аутентификации

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).

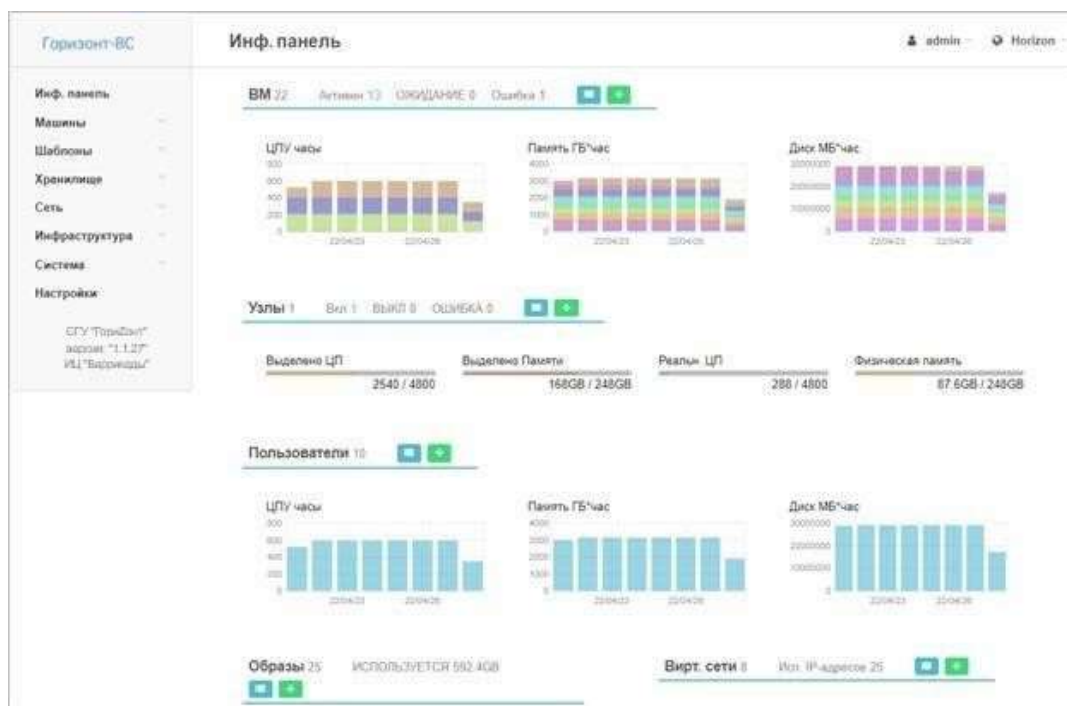


Рисунок 9 - Веб-интерфейс СГУ. Главное окно

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.

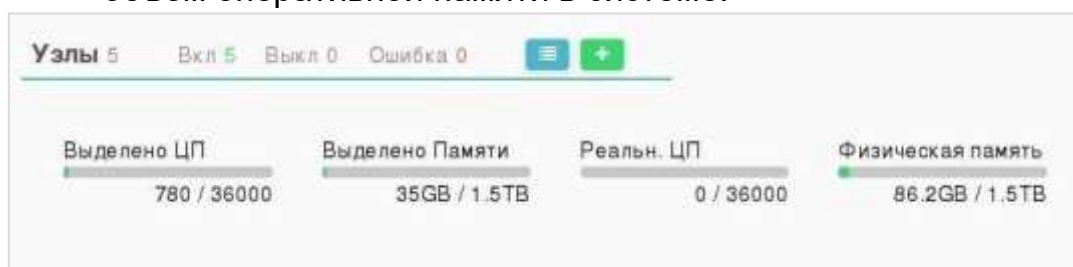


Рисунок 11 - Статистика узлов системы

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.

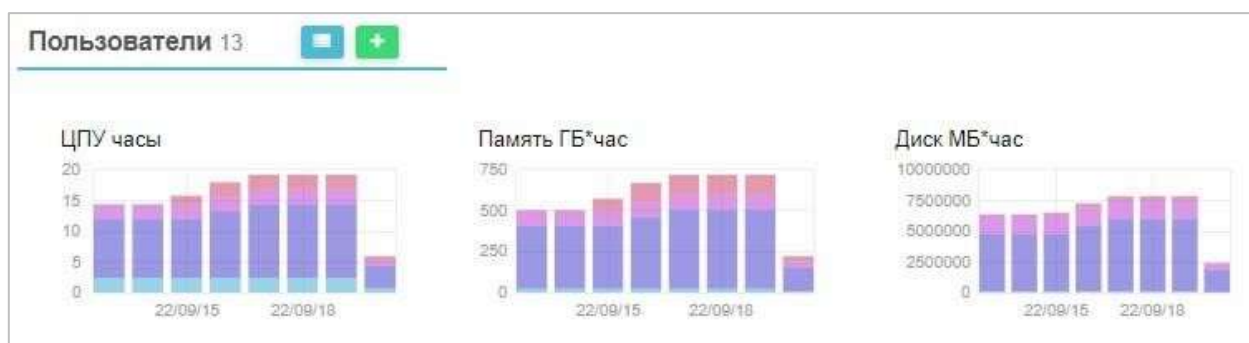


Рисунок 12 - Статистика пользователей

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).

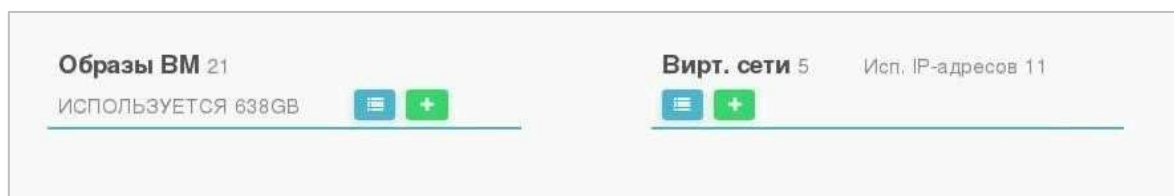


Рисунок 13 - Образы ВМ и Виртуальные сети

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.

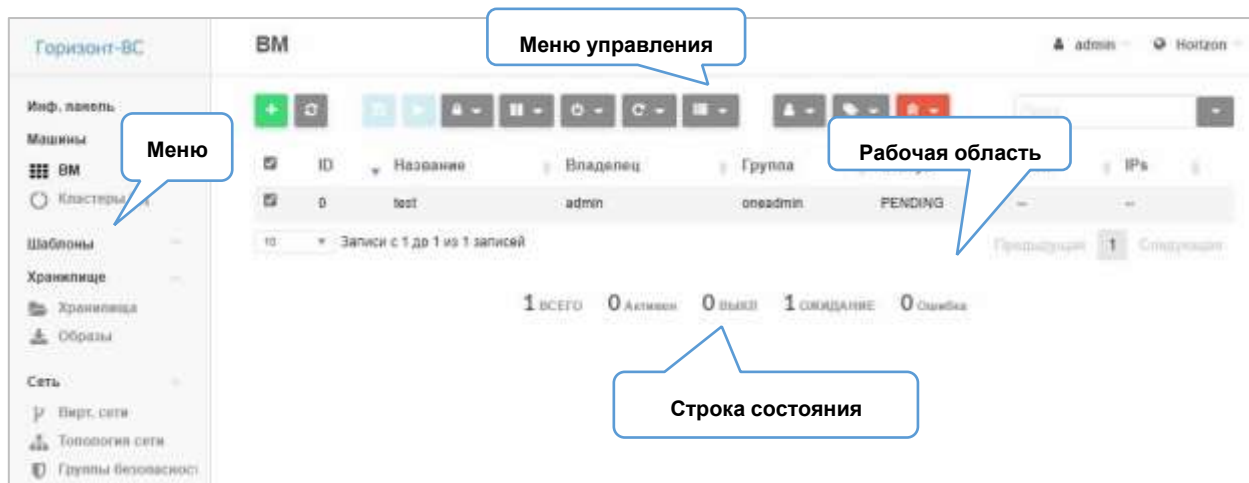


Рисунок 14 - Пример интерфейса раздела

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 VM
	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 назначению. <i>Например: VM бухгалтерии, VM отдела АСУ и т.д.</i>
	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) «Звезда» 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).

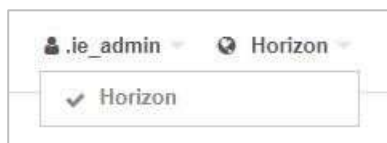


Рисунок 16 - Доступные администратору зоны управления

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 ведущий-ведомый) 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 IP-адрес 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. **Шаг 2.**

Добавление управляемой зоны 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
    0 OpenNebula
    100 slave-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 -l /var/lib/one/.one
ec2_auth one_auth oneflow_auth
onегate_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 найден.** «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.

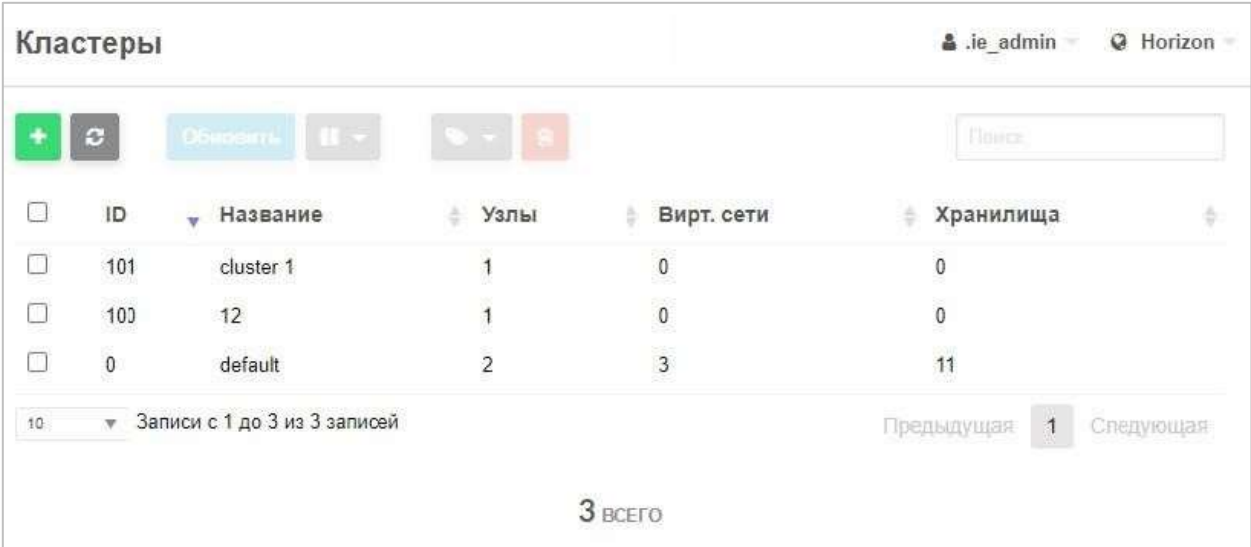
4. **Slave:** создать любого пользователя, группу или ЦОД, которые необходимо сохранить в федеративной среде.

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).



☐	ID	Название	Узлы	Вирт. сети	Хранилища
☐	101	cluster 1	1	0	0
☐	103	12	1	0	0
☐	0	default	2	3	11

10 ▼ Записи с 1 до 3 из 3 записей

Предыдущая 1 Следующая

3 ВСЕГО

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 подключения к кластеру (Рисунок 18).

Создать Кластер

admin | Горизонт

Название: Кластер_1

Вы выбрали следующие узлы: 192.168.2.114 x 192.168.2.115 x

ID	Название	Кластер	Кол-во ВМ	Выделено ЦП	Выделено Памяти	Статус
2	192.168.2.116	По умолчанию	0	0 / 0	0KB / -	ВЫКЛ
1	192.168.2.115	По умолчанию	6	600 / 4000 (15%)	24GB / 503.8GB (5%)	Вкл
0	192.168.2.114	По умолчанию	4	310 / 4000 (8%)	12.5GB / 503.7GB (2%)	Вкл

10 | Записи с 1 до 3 из 3 записей

Предыдущая | 1 | Следующая

Рисунок 18 - Создание кластера. Выбор узлов

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

Создать Кластер

admin1 | Horizon

Название: Кластер_1

Вы выбрали следующие сети: vian4092 x virbr0 x

ID	Название	Владелец	Группа	Резервирование	Кластер	Выделено
2	vian4092	backuper	oneadmin	Нет	0,101,102	2 / 20
1	virbr0	backuper	oneadmin	Нет	0,101	2 / 20
0	net-0	admin	oneadmin	Нет	0	7 / 10

10 | Записи с 1 до 3 из 3 записей

Предыдущая | 1 | Следующая

Рисунок 19 - Создание кластера. Выбор виртуальных сетей

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

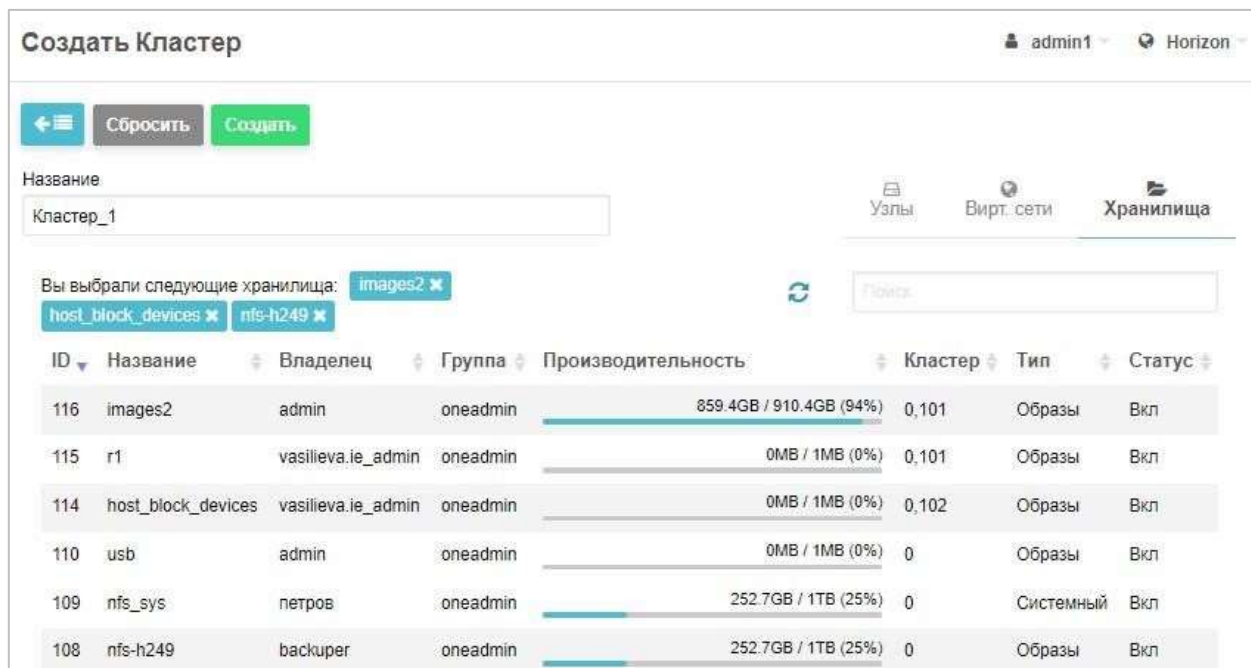


Рисунок 20 - Создание кластера. Выбор хранилищ

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).

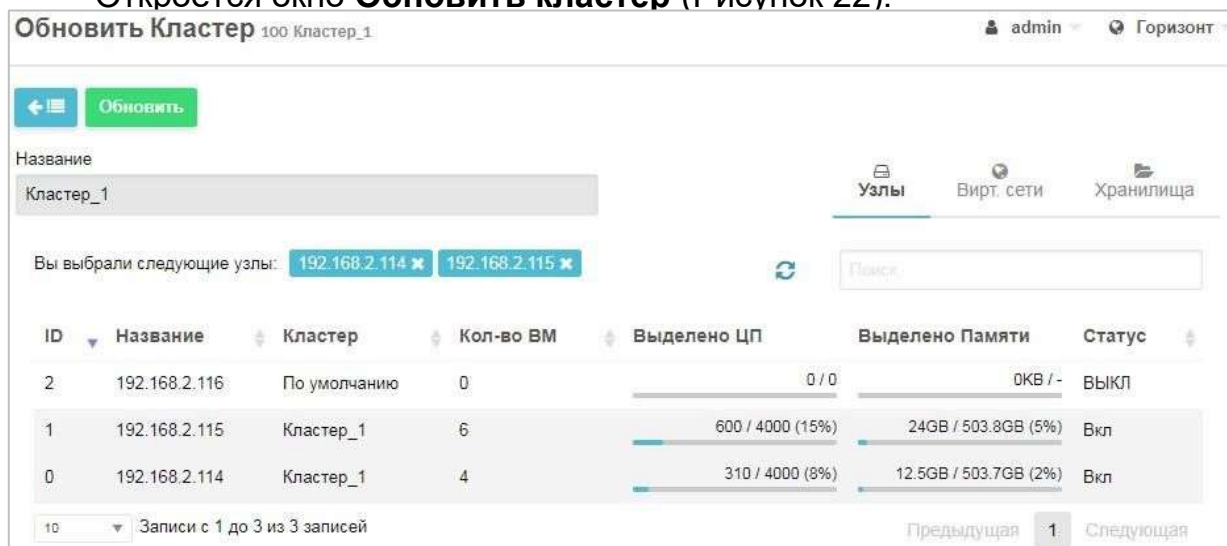


Рисунок 21 - Окно «Кластер»

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.

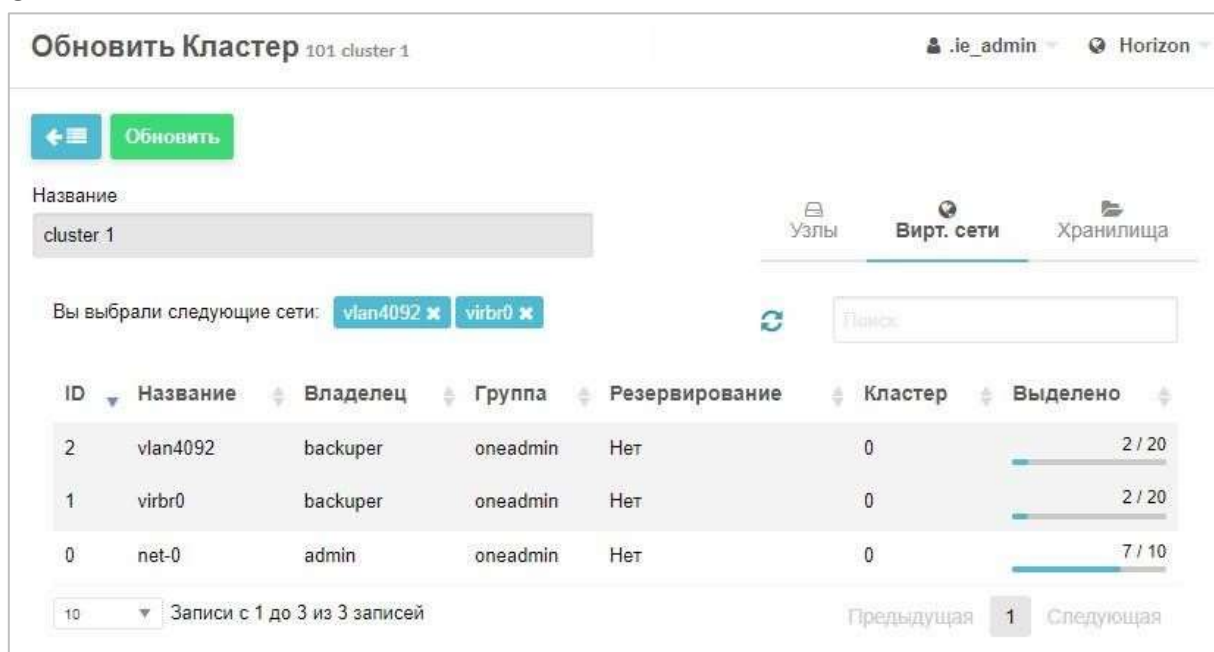


Рисунок 23 - Подключение/отключение виртуальных сетей

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

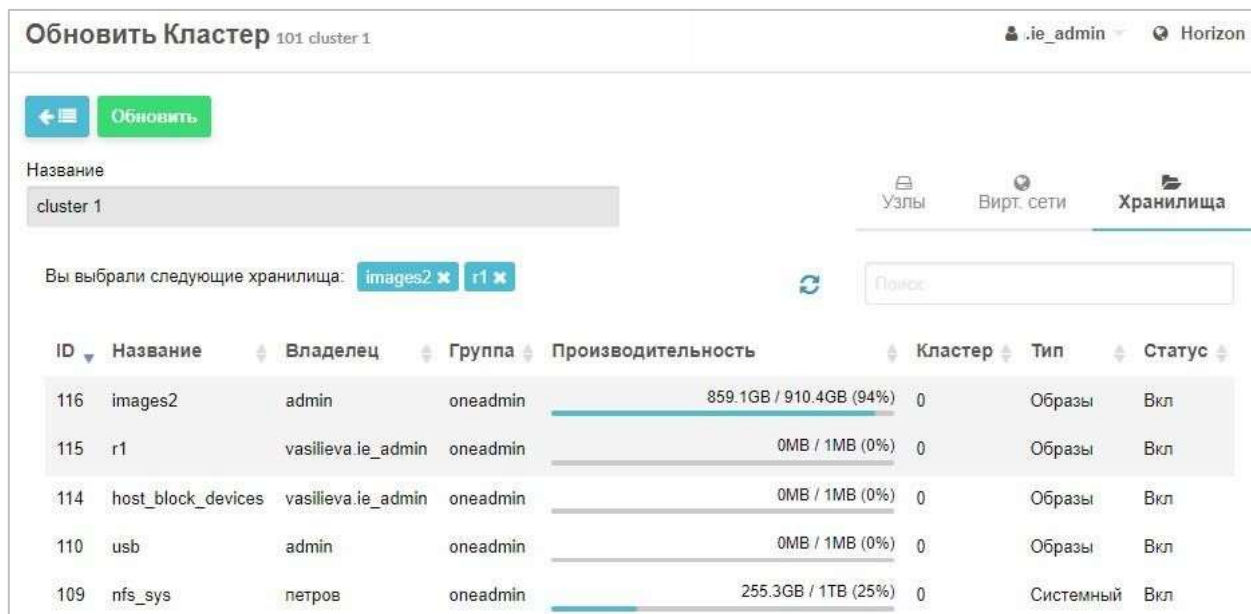


Рисунок 24 - Подключение/отключение хранилищ

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 **x** справа от ресурса.

4. Нажать кнопку **Обновить**.

Откроется список кластеров.

5. Выделить данный кластер, установив флаг слева от его названия.

6. Нажать кнопку **Удалить**.

7. В открывшемся окне подтвердить удаление нажатием кнопки **ОК**

(Рисунок 25).

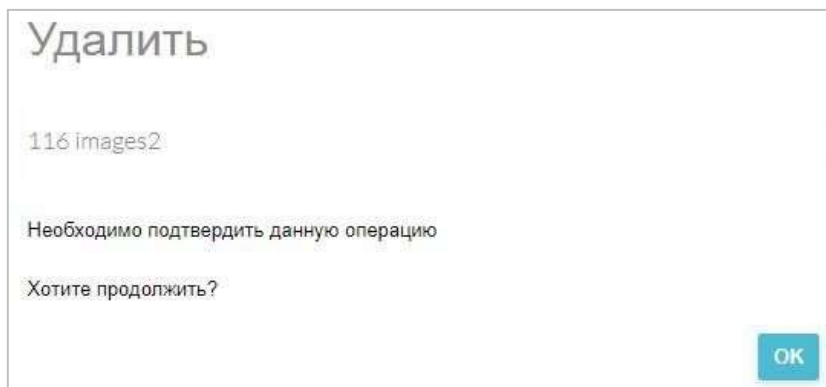


Рисунок 25 – Удаление кластера

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).

Узлы

admin1 Horizon

Выберите кластер

ID	Название	Кластер	Кол-во VM	Выделено ЦП	Выделено Памяти	Статус
8	168.222.11.44	cluster 1	0	0 / 0	0KB / -	ПОВТОРИТЬ
7	node 4	cluster 1	0	0 / 0	0KB / -	Инициализация
6	node3	cluster 1	0	0 / 0	0KB / -	ОШИБКА
5	node 2	12	0	0 / 0	0KB / -	Инициализация
0	192.168.2.109	default	14	140 / 1600 (9%)	42GB / 62.8GB (67%)	Вкл

Записи с 1 до 5 из 5 записей

5 ВСЕГО 3 Вкл 0 ВЫКЛ 2 ОШИБКА

Рисунок 27 - Раздел «Инфраструктура → Узлы»

- Нажать кнопку  в верхнем левом углу.

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

Создать узел

admin

Сбросить Создать

Имя хоста: Сервер 1

Кластер: 100: тест

Рисунок 28 - Создание узла

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

☐	ID	Название	Кластер	Кол-во VM	Выделено ЦП	Выделено Памяти	Статус
☒	8	168.222.11.44	cluster 1	0	0 / 0	0KB / -	ПОВТОРИТЬ
☐	7	node 4	cluster 1	0	0 / 0	0KB / -	Инициализация
☐	6	node3	cluster 1	0	0 / 0	0KB / -	ОШИБКА
☐	5	node 2	12	0	0 / 0	0KB / -	Инициализация
☐	0	192.168.2.109	default	14	140 / 1600 (9%)	42GB / 62.8GB (67%)	Вкл

10 Записи с 1 до 5 из 5 записей

5 ВСЕГО 3 Вкл 0 ВЫКЛ 2 ОШИБКА

Рисунок 29 – Выбор узла из списка

2.Нажать кнопку

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

3. Выбрать кластер нажатием и нажать кнопку **ОК** в нижнем правом углу.

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

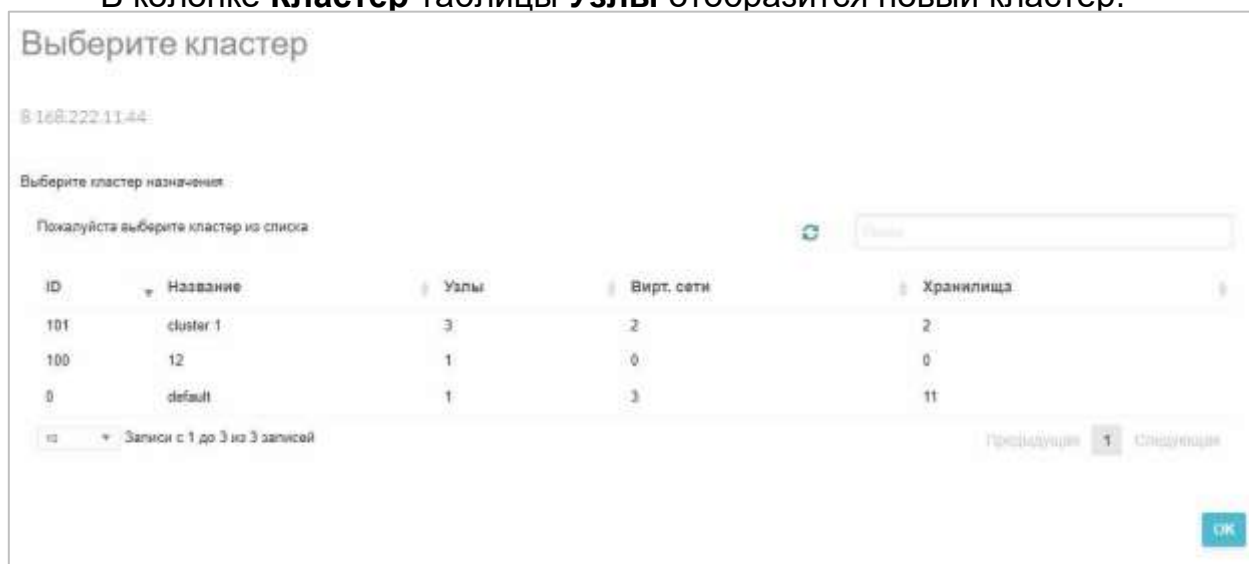


Рисунок 30 - Выбор кластера

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).

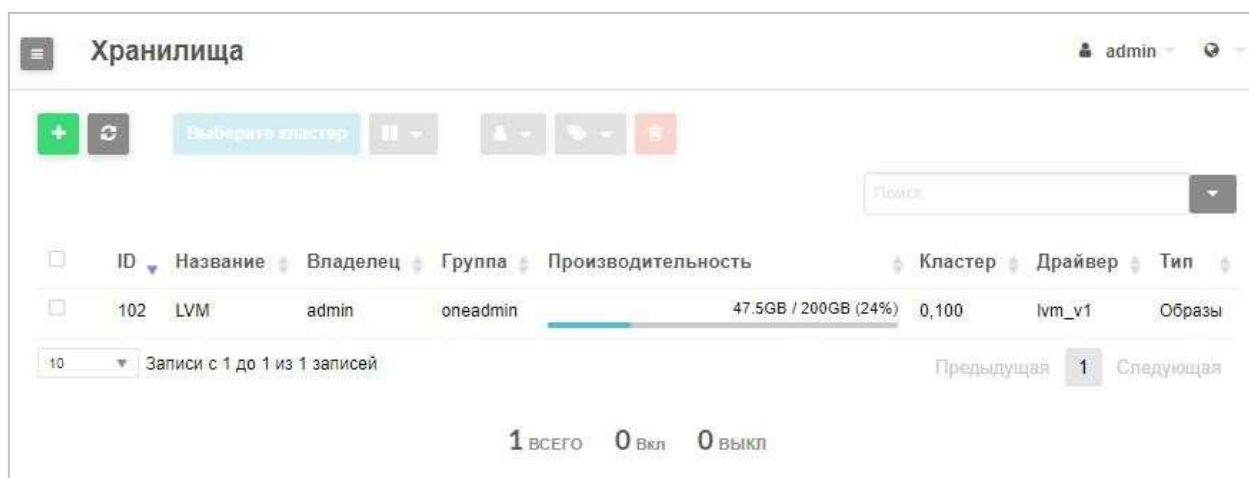


Рисунок 31 - Менеджер хранилищ

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.
	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 назначению.

		<i>Например: БД бухгалтерии</i>
	Удаление	Удаление хранилища из системы

Для создания нового хранилища:

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

Откроется окно **Создать хранилище** (Рисунок 32 **Ошибка! Источник ссылки не найден.**).

Создать хранилище

admin Horizon

← Сбросить Создать

Мастер настройки

Базовые параметры

Название

Тип хранилища

Хранилище с разделяемым общим диском

Кластер

0: default

Назначение

☒

Образы

Подключение

Узлы имеющие доступ

host1 host2 host3

Уникальное имя общего тома

Расширенные настройки

Общие параметры

☐

Ограниченные каталоги для регистрации образов

☐

Не пытаться распаковать архив

☐

Безопасные каталоги для регистрации образов

☐

Проверять доступную емкость

☐

Лимит использования хранилища (МБ)

☐

Предел пропускной способности канала (Б/с)

Дополнительно

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.

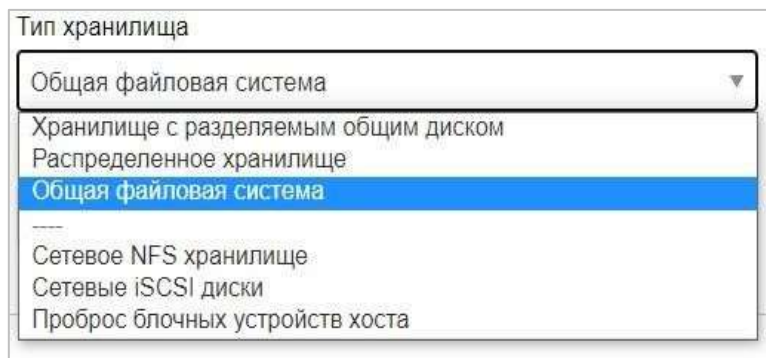


Рисунок 33 - Протоколы для подключения хранилища

3. В области **Подключения** указать, какие hosts 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).

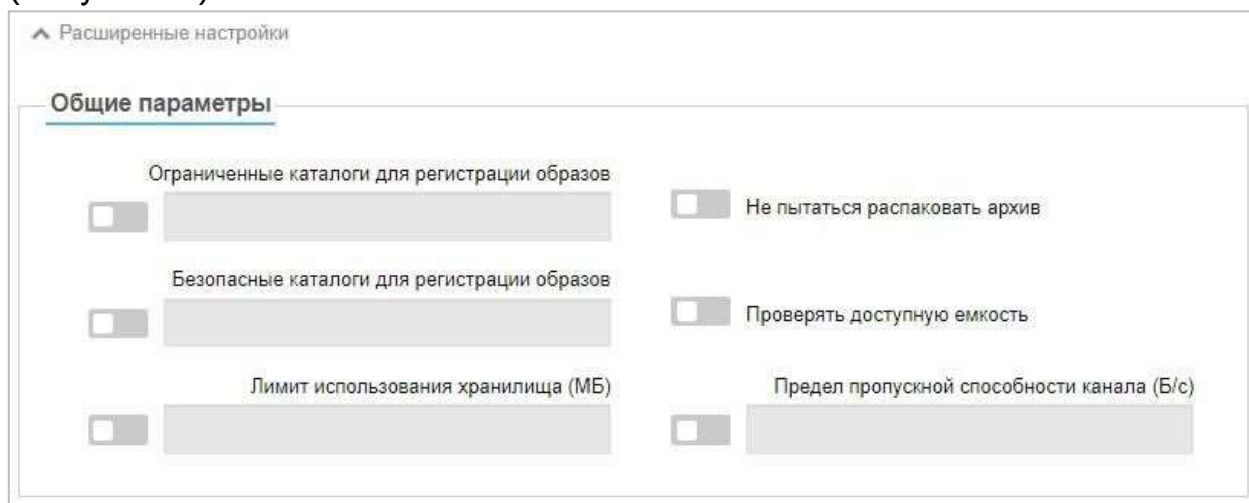


Рисунок 34 - Расширенные настройки хранилища с разделяемым общим диском

3.2.8.1.1 iSCSI хранилище

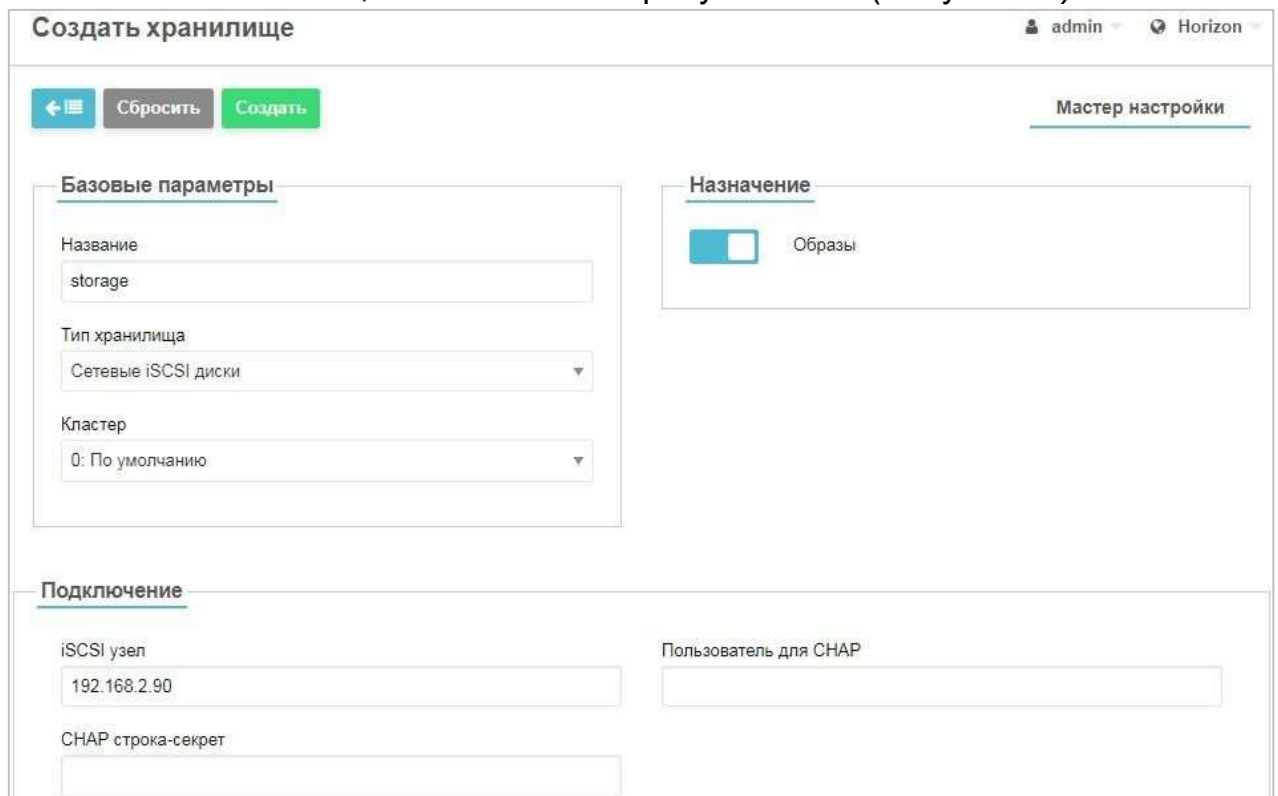
Для подключения iSCSI хранилища:

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):



Создать хранилище

admin Horizon

Мастер настройки

← Сбросить Создать

Базовые параметры

Название
storage

Тип хранилища
Сетевые iSCSI диски

Кластер
0: По умолчанию

Назначение

☒ Образы

Подключение

iSCSI узел
192.168.2.90

Пользователь для CHAP

CHAP строка-секрет

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:

- а. Нажать кнопку  в управляющем меню (Рисунок 36).

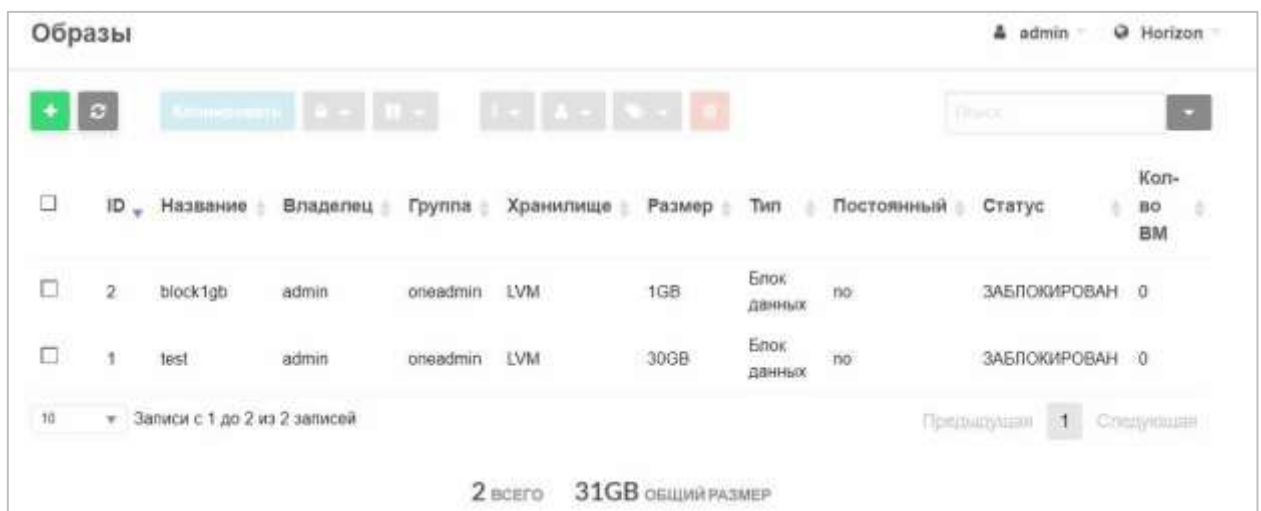


Рисунок 36 - Раздел «Хранилище» → «Образы»

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

Укажите параметры нового образа admin Horizon

← Сбросить Создать Мастер настройки

Базовые параметры

Название
образ хранилища1

Описание

Хранилище
103: Хранилище1

Назначение

☐ Образ операционной системы

☐ CD-ROM только для чтения

☒ Блок данных

Свойства образа

☒ Этот образ является постоянным

Расположение образа

Загрузить +

Пустой образ диска +

Путь на сервере СГУ -

Путь к файлу

⤴ Расширенные настройки

Общие параметры

Шина
☐ Virtio

Целевое устройство
☐

Драйвер образа
☐ raw

Разделяемый образ
☐ Нет

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).

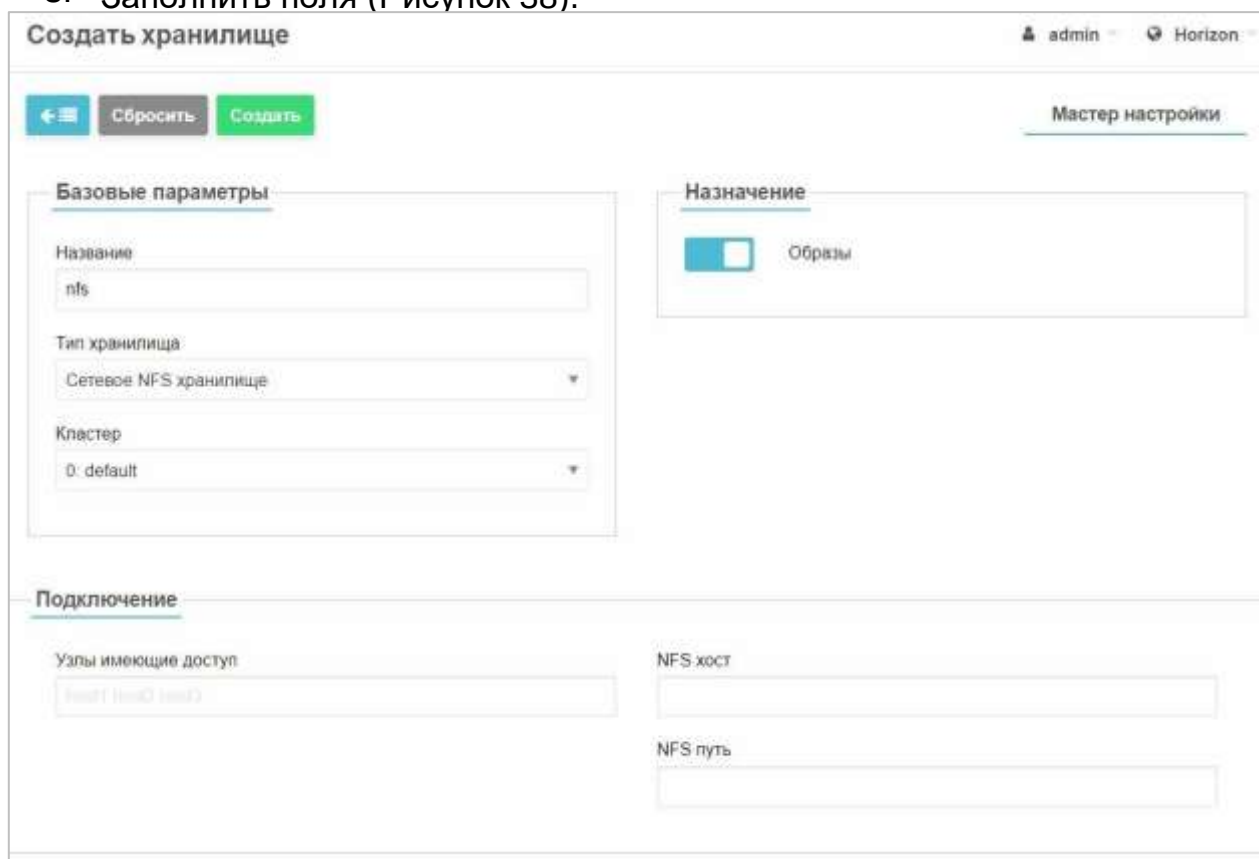


Рисунок 38 – Создание хранилища

- 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 VM:

```
$ 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 client.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).

Расширенные настройки

Общие параметры

☐ Ограниченные каталоги для регистрации образов	☐ Не пытаться распаковать архив
☐ Безопасные каталоги для регистрации образов	☐ Проверять доступную емкость
☐ Лимит использования хранилища (МБ)	☐ Предел пропускной способности канала (Б/с)

Дополнительно

Каталог для регистрации образов	Формат RBD
Путь к файлу конфигурации хранилища	Файл содержащий строку-секрет
	Уникальное имя ЕС пула

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.

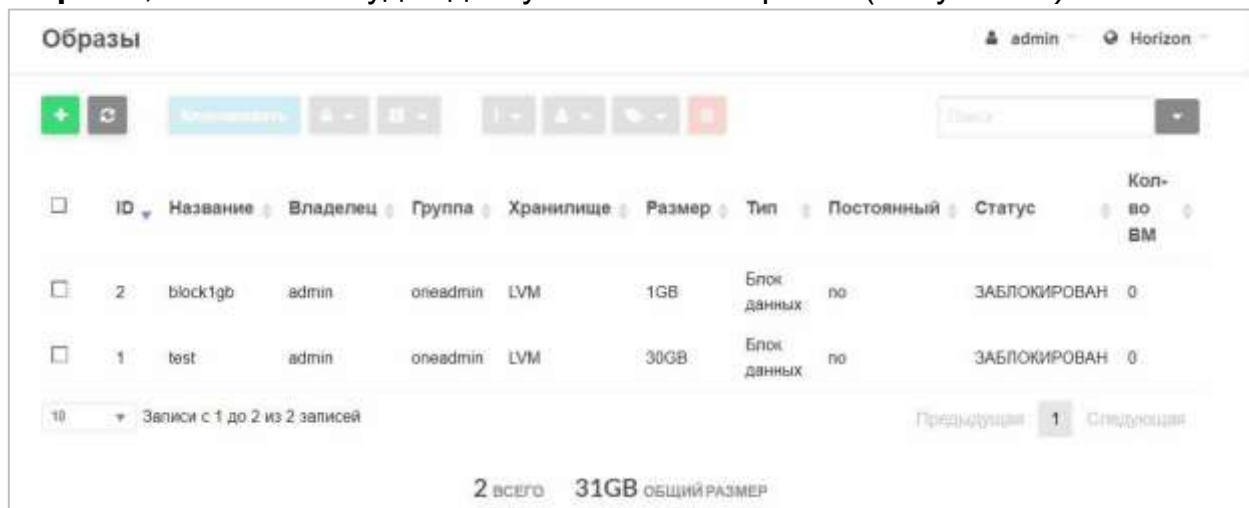
Различные типы виртуальных дисков могут использоваться, в том числе и для создания *эталонных* («золотых») образов ВМ.

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).



☐	ID	Название	Владелец	Группа	Хранилище	Размер	Тип	Постоянный	Статус	Кол-во ВМ
☐	2	block1gb	admin	oneadmin	LVM	1GB	Блок данных	no	ЗАБЛОКИРОВАН	0
☐	1	test	admin	oneadmin	LVM	30GB	Блок данных	no	ЗАБЛОКИРОВАН	0

10 Записи с 1 до 2 из 2 записей

2 всего 31GB ОБЩИЙ РАЗМЕР

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
	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»)
	Пользовани е	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 назначению.
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).

Укажите параметры нового образа admin1 Horizon

← Сбросить Создать Мастер настройки

Базовые параметры

Название

Описание

Хранилище
100: images

Назначение

☒ Образ операционной системы

☐ CD-ROM только для чтения

☐ Блок данных

Свойства образа

☐ Этот образ является постоянным

Расположение образа

Загрузить

Загрузить файл

Пустой образ диска

Путь на сервере СГУ

Расширенные настройки

Рисунок 42 - Создание установочного образа диска VM

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 VM 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, независимо 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 ручную 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, указанное в поле **Размер;**

- **qcow2** – создается файл на 1–1,5 КБ, который будет занимать столько 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 .

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 44).

Укажите параметры нового образа

admin Horizon

Сбросить Создать

Мастер настройки

Базовые параметры

Название

test

Описание

Хранилище

100: images

Назначение

☐ Образ операционной системы

☐ CD-ROM только для чтения

☒ Блок данных

Свойства образа

☐ Этот образ является постоянным

Расположение образа

Загрузить +

Пустой образ диска -

Размер

10 ГБ

Рисунок 43

Рисунок 44 - 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 **Свойства 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 VM 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 выполняется VM, к которой будет подключен диск (информацию о сервере можно получить в разделе **Узлы → VM**).

8. На сервере виртуализации найти директорию с размещенной VM 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 VM, то в поле **Драйвер образа** необходимо указать формат **qcow2**.

3. После этого нажать кнопку **Создать** и дождаться размещения образа VM 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 VM), так и без приостановки обслуживания (включенной VM).

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 VM:

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 45).

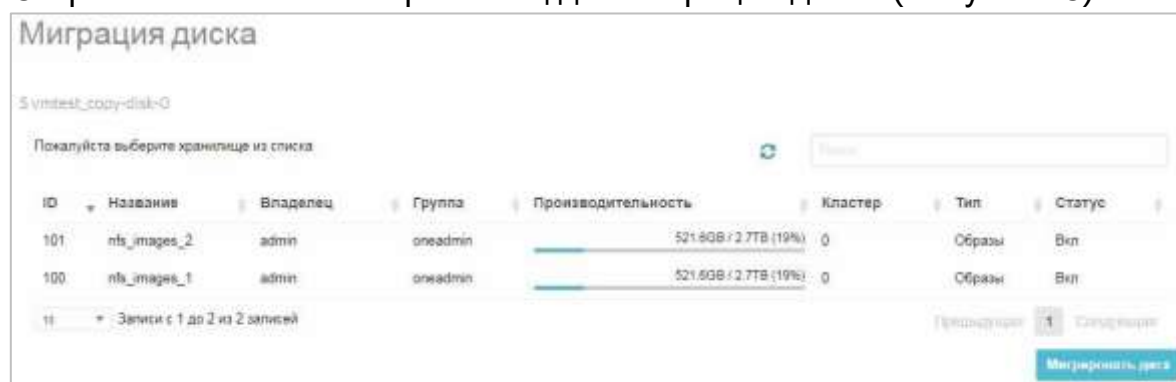


Рисунок 45 - Миграция дисков

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 VM:

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).

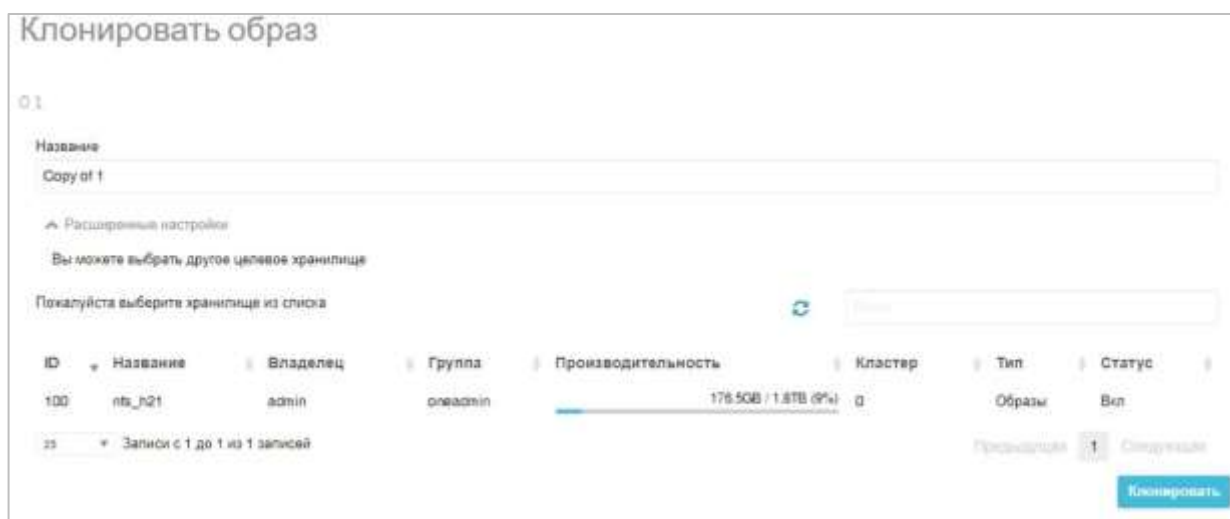


Рисунок 46 - Клонирование образа

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 47).

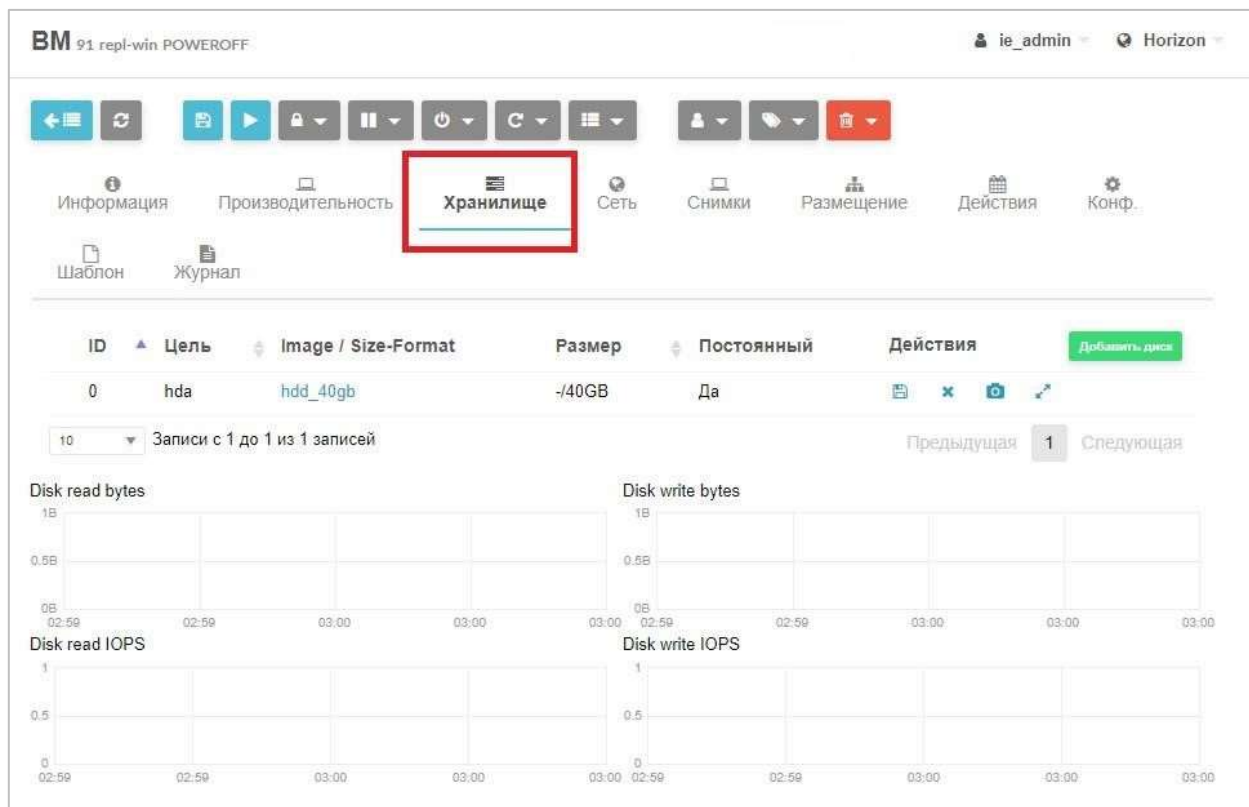


Рисунок 47 - Раздел «BM → Хранилище»

5. Нажать на кнопку **Добавить диск**.

6. В открывшемся окне **Присоединить диск** (Рисунок 48) 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.

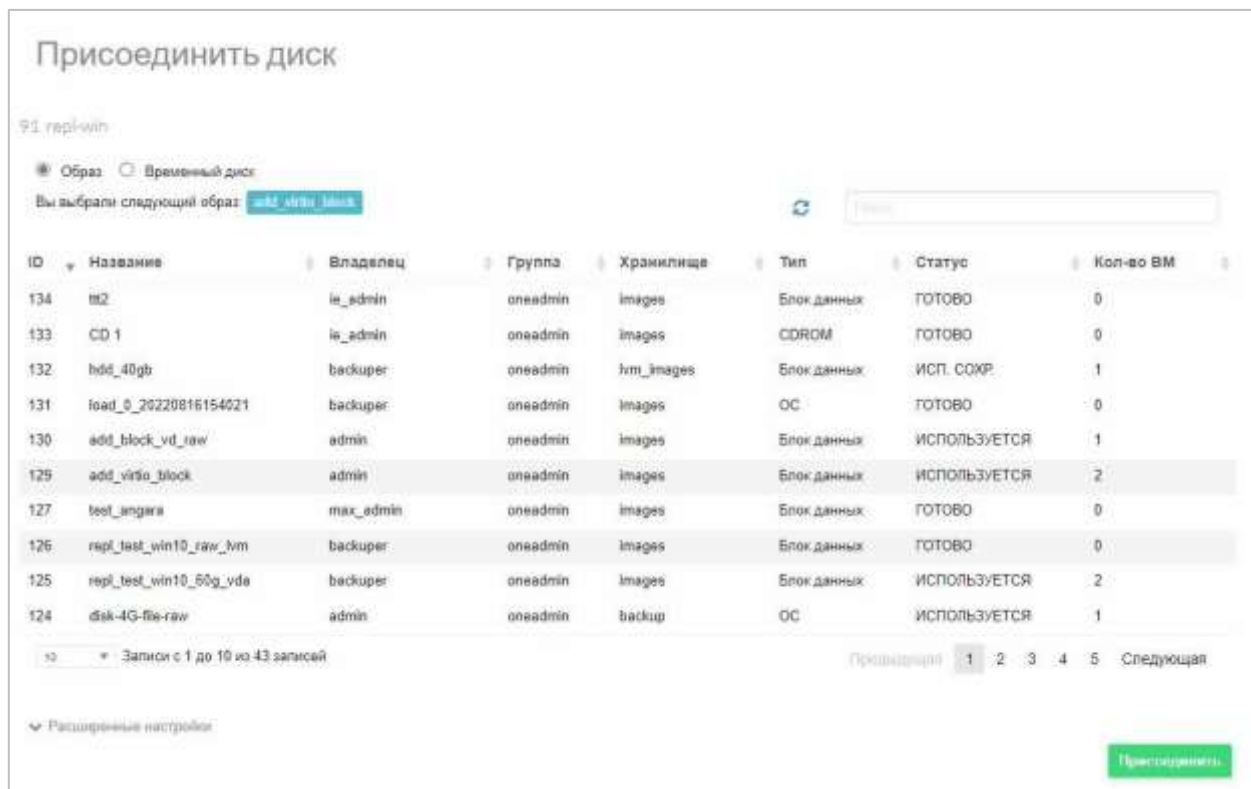


Рисунок 48 - Присоединение диска

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 49).

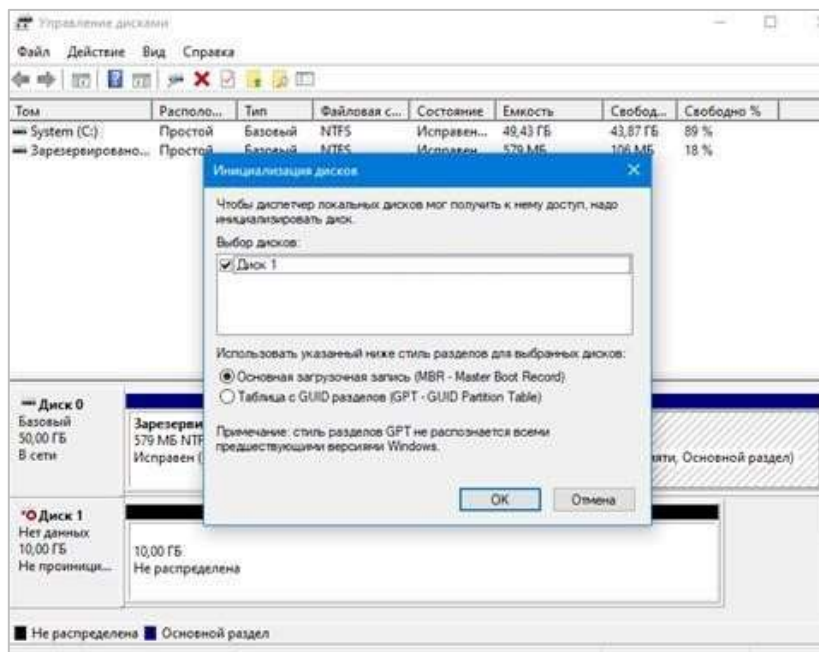


Рисунок 49 - Инициализация дисков

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 50).

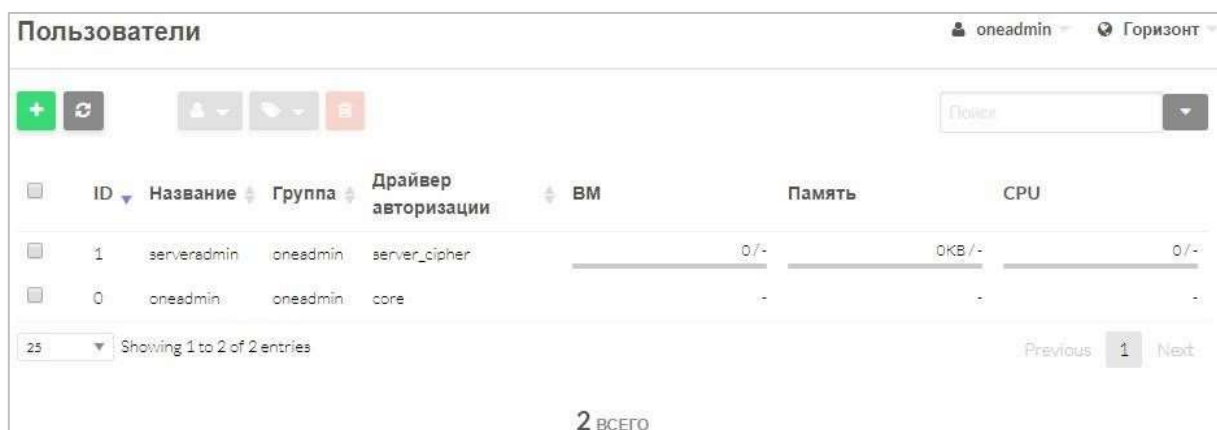


Рисунок 50 - Менеджер пользователей ВМ

Для создания нового пользователя:

1. Нажать кнопку  в управляющем меню. Откроется окно **Создать пользователя** (Рисунок 51).

Создать пользователя

← Сбросить Создать

Имя пользователя
vmuser

Пароль
....

Подтвердите пароль
....

Способ аутентификации
server_x509

Основная группа
1: users

Дополнительные группы

Вы выбрали следующие группы:

users ✕

ID	Название
1	users
0	oneadmin

10 Записи с 1 до 2 из 2 записей

Предыдущая 1 Следующая

Рисунок 51 - Новый пользователь VM

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 52) (для доступа через веб-интерфейс необходимо выбрать «ядро»);

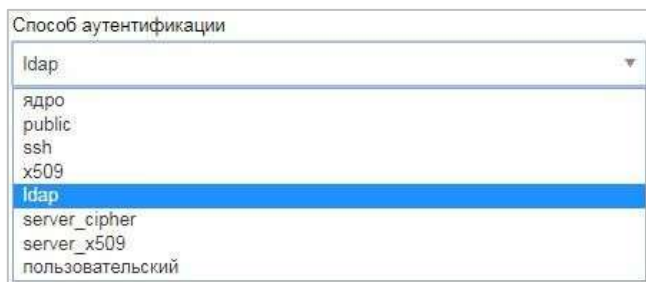


Рисунок 52 - Выбор способа аутентификации

– 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 53).

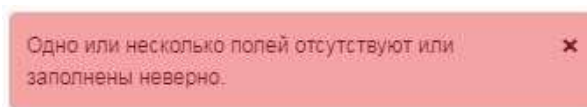


Рисунок 53 - Сообщение (1)

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

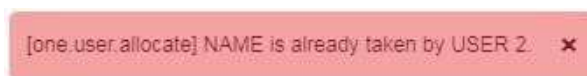


Рисунок 54 - Сообщение (2)

Для удаления пользователя:

1. Выбрать пользователя из списка (Рисунок 50)
2. Нажать кнопку  в управляющем меню
3. Подтвердить удаление пользователя в открывшемся окне нажатием

кнопки  (Рисунок 54).



Рисунок 55 - Предупреждающее сообщение

Для изменения пароля пользователя:

1. Выбрать пользователя из списка (Рисунок 50) пользователя.
2. В открывшемся окне перейти на вкладку

Аутентификация (Рисунок 55).

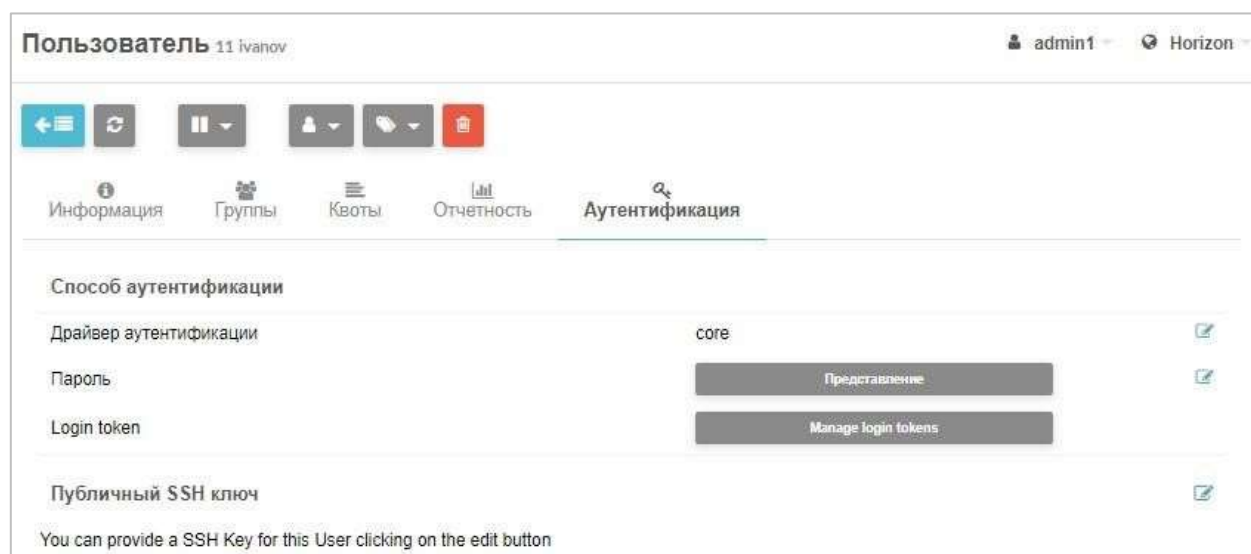
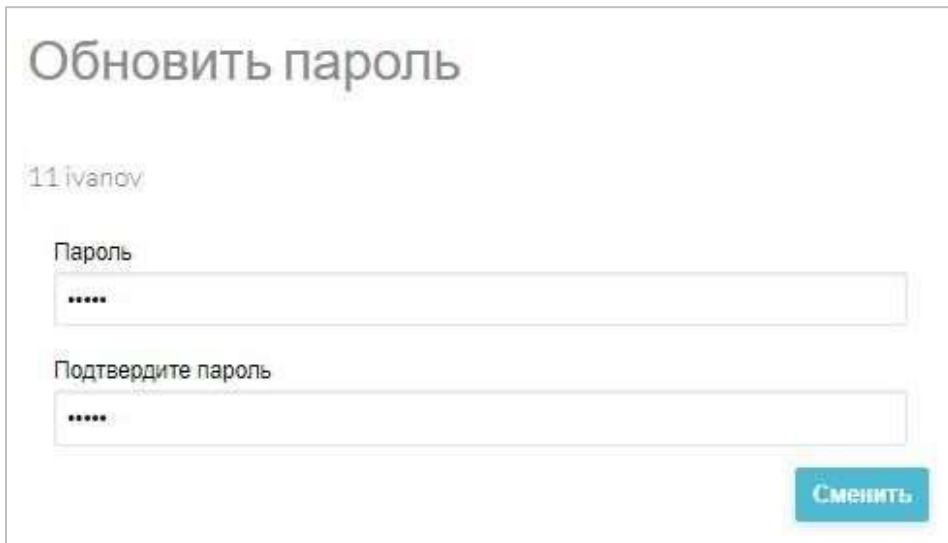


Рисунок 56 - Вкладка «Аутентификация»

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

новый пароль и нажать кнопку  (Рисунок 56).



Обновить пароль

11 ivanov

Пароль

Подтвердите пароль



Рисунок 57 - 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 58).

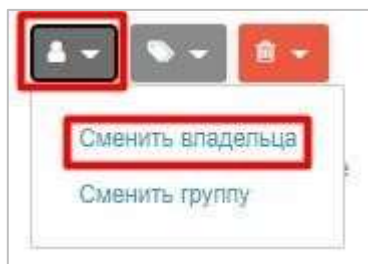


Рисунок 58 - Опция «Сменить владельца»

Откроется окно со списком пользователей (Рисунок 58).

8. Выбрать пользователя, которому будет предоставлен доступ к ВМ и нажать кнопку **ОК** (Рисунок 59).

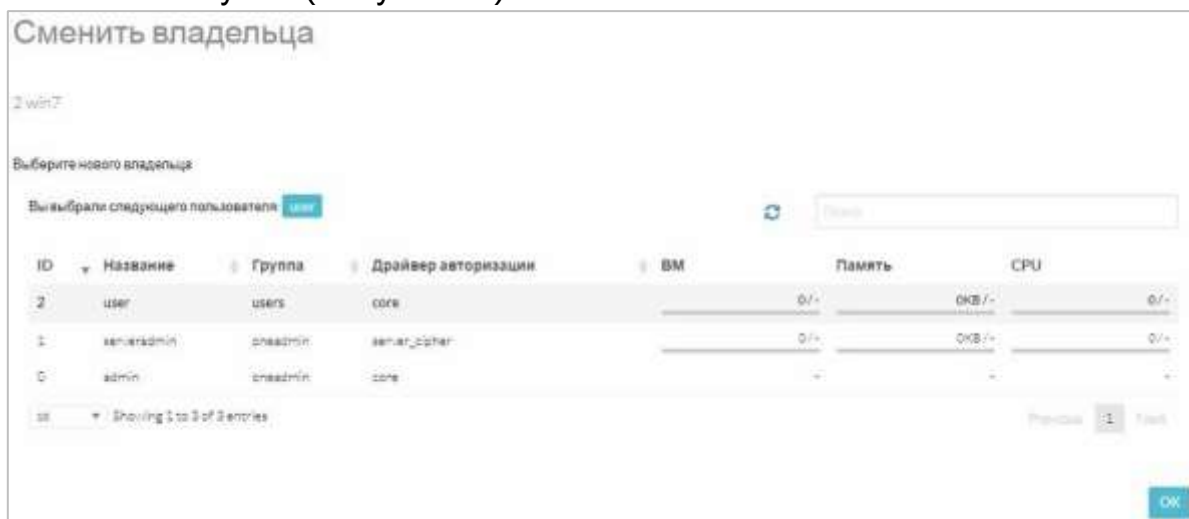


Рисунок 59 - Назначение нового пользователя ВМ

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 только одна виртуальная машина.*

3.2.12 Создание групп пользователей

Для разграничения прав в «Звезда», 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).

☐	ID	Название	Пользователи	ВМ	Память	CPU
☒	100	3LD	3		0 / -	0КВ / -
☐	1	users	3		0 / -	0КВ / -
☐	0	oneadmin	8		-	-

10 Записи с 1 до 3 из 3 записей

Предыдущая 1 Следующая

3 ВСЕГО

Рисунок 60 - Группы пользователей

Для создания новой группы

1. Нажать кнопку .

Откроется окно **Создать группу** на вкладке **Общие** (Рисунок 61).

Рисунок 61 - 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 62).

	Группа пользователей	Группа администраторов
Cloud Представление	☒	☒
Group Admin Представление	☐	☒

	Группа пользователей	Группа администраторов
Admin Представление	☐	☐
User Представление	☐	☐

Рисунок 62 - 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 63).

Создать группу

← Включить/Выключить Создать

⚠ Новые группы автоматически добавлены в VDC по умолчанию

Общие Представление **Администрирование** Права Система

☒ Создать пользователя с административными правами ⓘ

Имя пользователя
user_group-admin

Пароль
.....

Подтвердите пароль
.....

Способ аутентификации
ядро ▼

Рисунок 63 - Создание группы. Вкладка «Администрирование»

5. На вкладке **Права** устанавливаются разрешения на создание ресурсов для пользователей группы (Рисунок 64). Разрешенные ресурсы отмечаются флажками.

ВМ	Вирт. сети	Группы безопасности	Вирт. маршрутизаторы	Образы	Шаблоны	Документы
☒	☐	☒	☒	☒	☒	☒

Рисунок 64 - Создание группы. Вкладка «Права»

- Нажать кнопку **Создать** в управляющем меню.

Новая группа появится в списке (Рисунок 60).

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:

- Перейти в раздел **Система** → **Списки контроля**, после чего на экране откроются зарегистрированные в системе списки контроля доступа (Рисунок 65).

Списки Контроля Доступа						
+ ↺ ↻ + admin Horizon						
10 Записи с 1 до 5 из 5 записей Предыдущая 1 Следующая						
☐	ID	Применено к	Затрагиваемые ресурсы	№ ресурса / Принадлежит	Разрешенные действия	Зона
☐	4	Группа users	Вирт. сети, Хранилища	Все	use	Horizon
☐	3	Группа users	Узлы	Все	manage	Horizon
☐	2	Все	Магазин приложений, Приложения из магазина приложений	Все	use	Все
☐	1	Все	Зоны	Все	use	Все
☐	0	Группа users	Вирт. машины, Образы, Шаблоны VM, Документы, Группы безопасности, VM Groups	Все	create	Все

Рисунок 65 - 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 66).

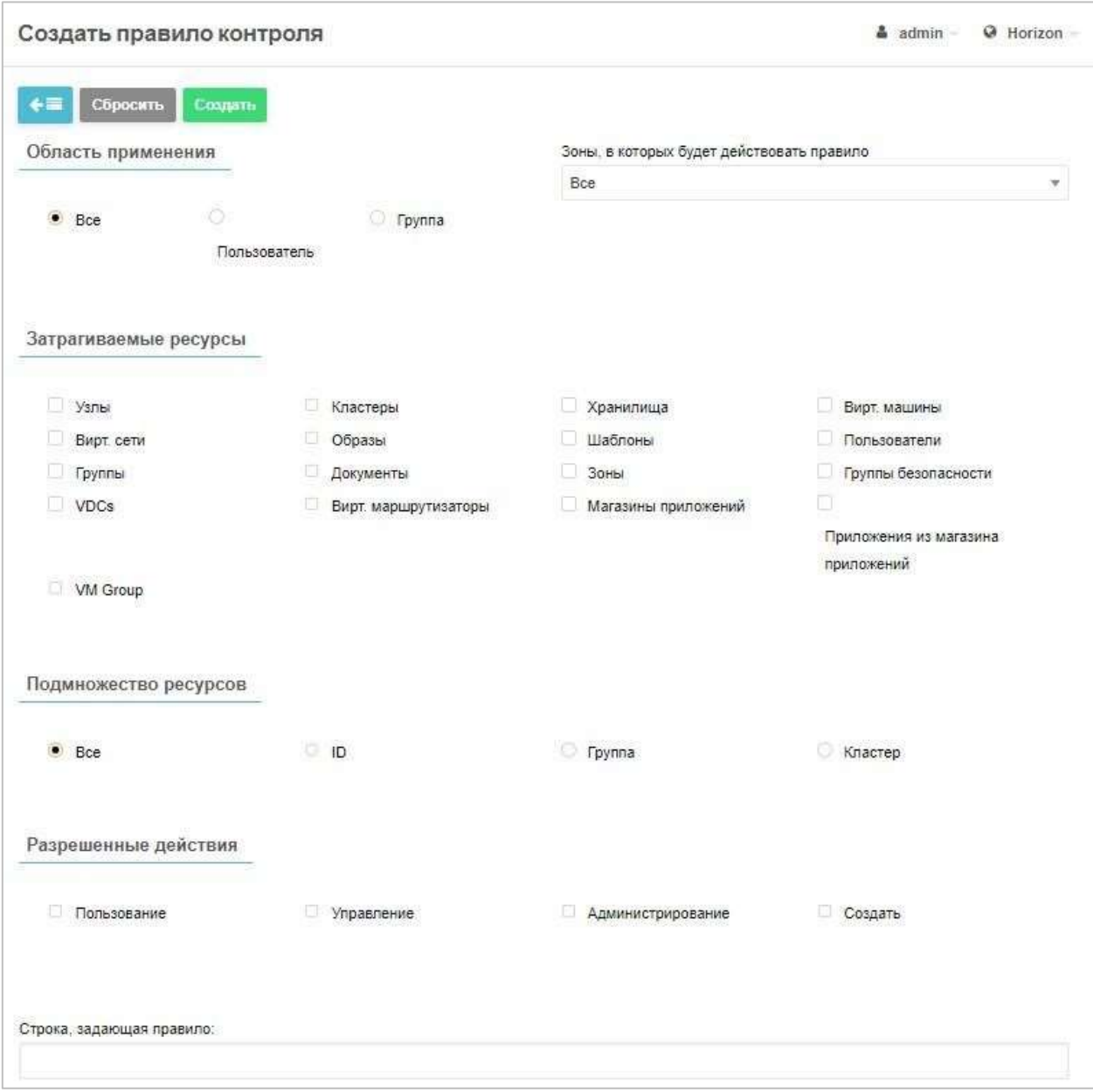


Рисунок 66 - Создать правило контроля доступа

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 67).

Создать правило контроля

← Сбросить Создать

Область применения

☐ Все ☐ Пользователь ☒ Группа

Группа:

Пожалуйста выберите

Пожалуйста выберите

0: oneadmin

1: users

100: 3LD

Затрагиваемые ресурсы

Рисунок 67 - 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  (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 68).

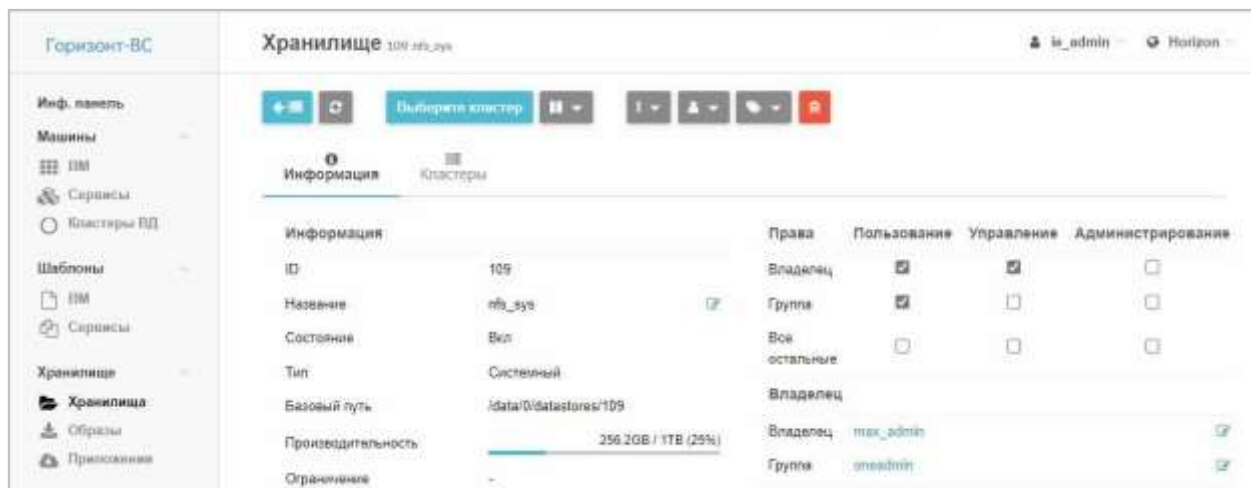


Рисунок 68 - Окно информации о хранилище

3. Выбрать нового владельца.

Данную операцию можно выполнить двумя способами:

Способ 1.

а. В секции информации о владельце нажать на кнопку в строке «Владелец» (**Ошибка! Источник ссылки не найден.**).

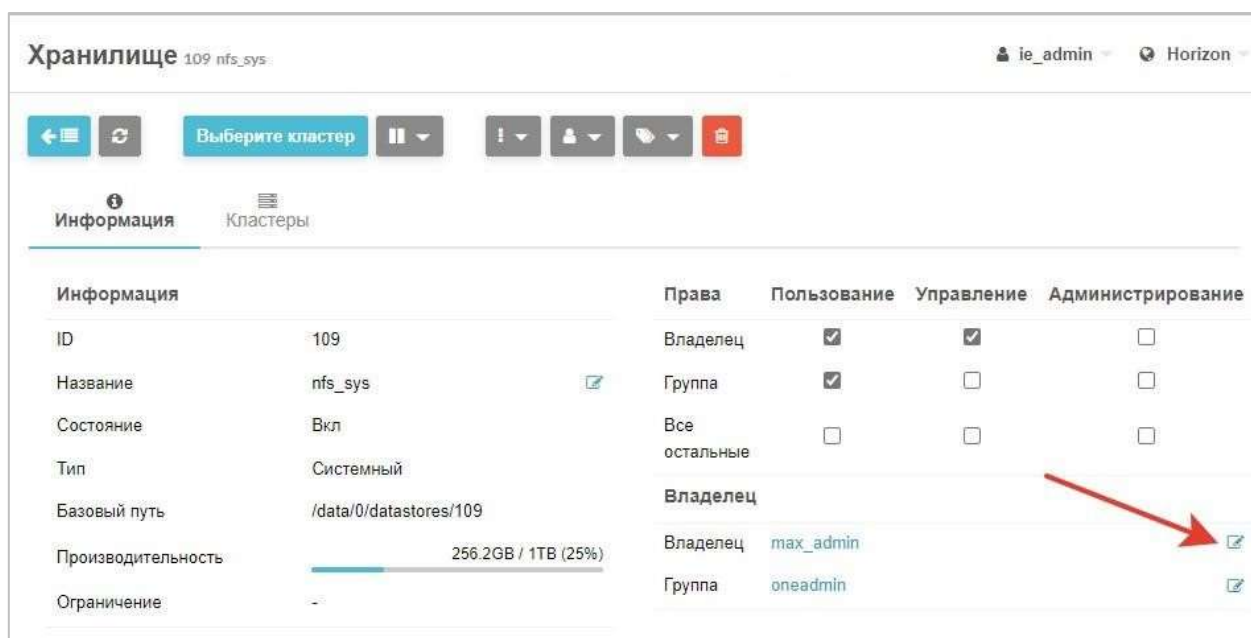


Рисунок 69 - Кнопка в строке «Владелец»

Появится раскрывающийся список пользователей (Рисунок 69)

б. Выбрать пользователя (Рисунок 70).

Права	Пользование	Управление	Администрирование
Владелец	☒	☒	☐
Группа	☒	☐	☐
Все остальные	☐	☐	☐

Владелец

Владелец	9: max_admin	
Группа	0: admin 1: serveradmin 4: backupер 5: 3LD-admin 6: 3LD-user 7: cl_user1 8: cl_admin1 9: max_admin 10: vasilieva.ie_admin 11: ivanov 12: петров	

Рисунок 70 - Выбор пользователя Способ 2.

в. Нажать кнопку

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



на панели управления.

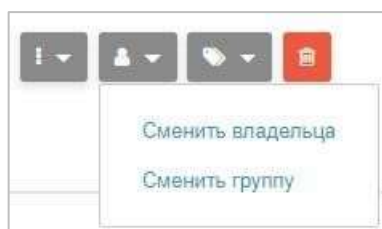


Рисунок 71 - «Сменить владельца»

Откроется окно «Сменить владельца» (Рисунок 72).

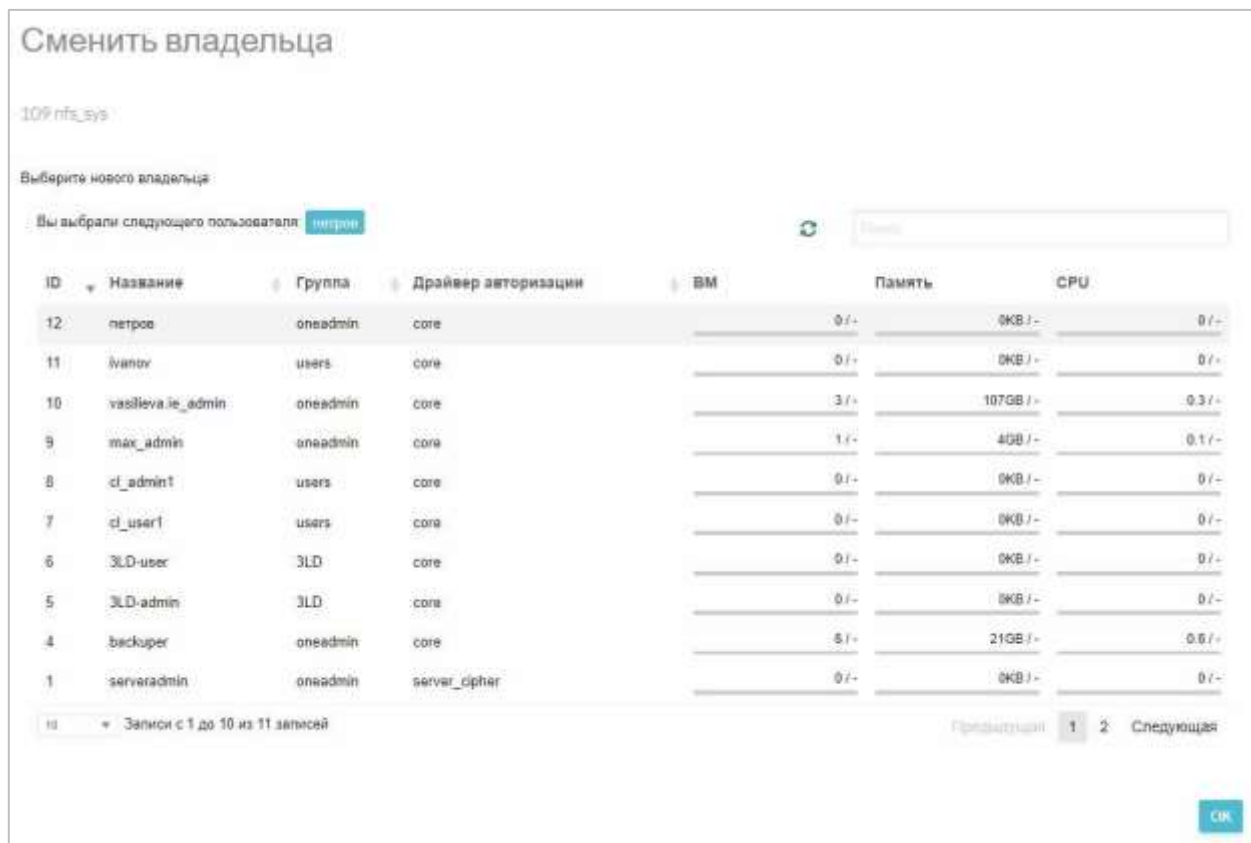


Рисунок 72 - Окно «Сменить владельца»

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 73).

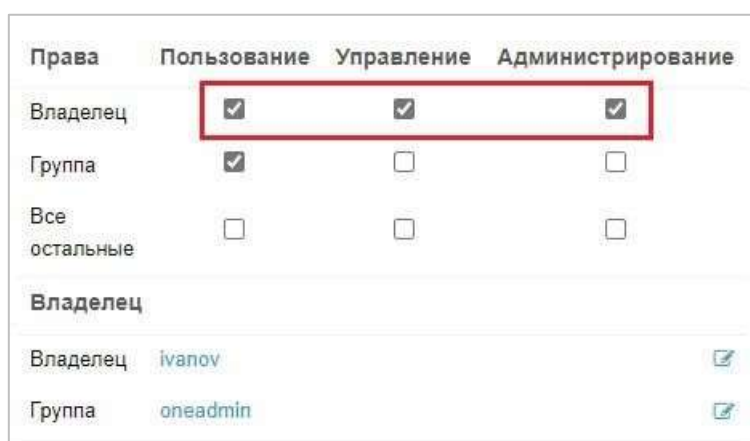


Рисунок 73 - Настройка прав для нового владельца

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 74) и выполнить действия, аналогичные шагам 3 – 5 в описании назначения нового владельца хранилища (стр. 158).

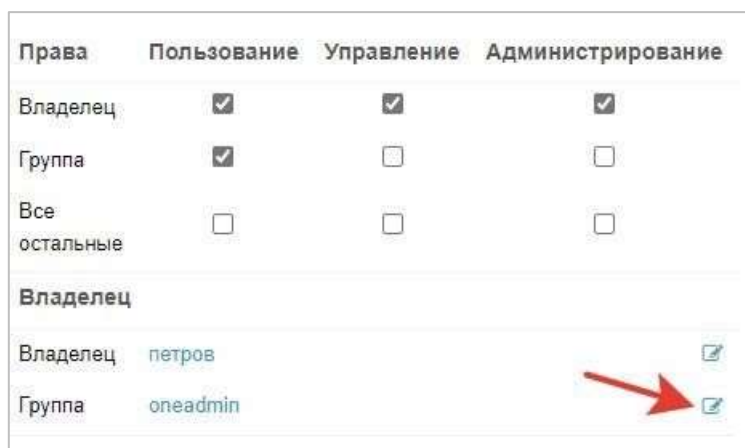


Рисунок 74 - Кнопка в строке «Владелец»

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 75).

Создать Виртуальную сеть

admin | Горизонт

← Сбросить Создать

Мастер настройки

Общие Конф. Адреса Безопасность QoS Контекст

Название
network1

Описание

Рисунок 75 - Создание виртуальной сети. Вкладка «Общие»

3. На вкладке **Общие** необходимо ввести имя сети в поле **Название** и описание в поле **Описание** (Рисунок 75).

4. На вкладке **Конф.**:

– в поле **Интерфейс сет. моста** ввести название виртуального коммутатора, созданного в разделе 3.1.4 (Рисунок 76).

Значение по умолчанию – **hvssw0**.

Создать Виртуальную сеть

admin | Horizon

← Сбросить Создать

Мастер настройки

Общие Конф. Адреса Безопасность QoS Контекст

Интерфейс сет. моста
hvssw0

Режим работы сети
Open vSwitch

☐ MAC spoofing filter
☐ IP spoofing filter

VLAN ID
No VLAN network

Рисунок 76 - Создание новой виртуальной сети. Вкладка «Конф.»

5. Из раскрывающегося списка выбрать режим работы сети



Рисунок 77 - Режимы работы виртуальной сети

Режимы работы:

- **Open vSwitch** – виртуальный коммутатор, открытый проект, виртуальный коммутатор с возможностью фильтровать трафик 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 ebttables (на L3);
- **Bridged with ebttables VLAN** – сетевой мост, который связан группами пользователей, который включает в себя ebttables для L2 изоляции виртуальных сетей;
- **802.1QVLAN** – стандартный VLAN, сеть с поддержкой стандарта 802.1q. В Программный комплекс (ПК) «Звезда» реализована поддержка 802.1q на уровне ВМ и гипервизора;
- **VXLAN** – для поддержки OpenFlow;

- установить флаги **MAC spoofing filter** (защита от подмены MAC-адреса) 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:

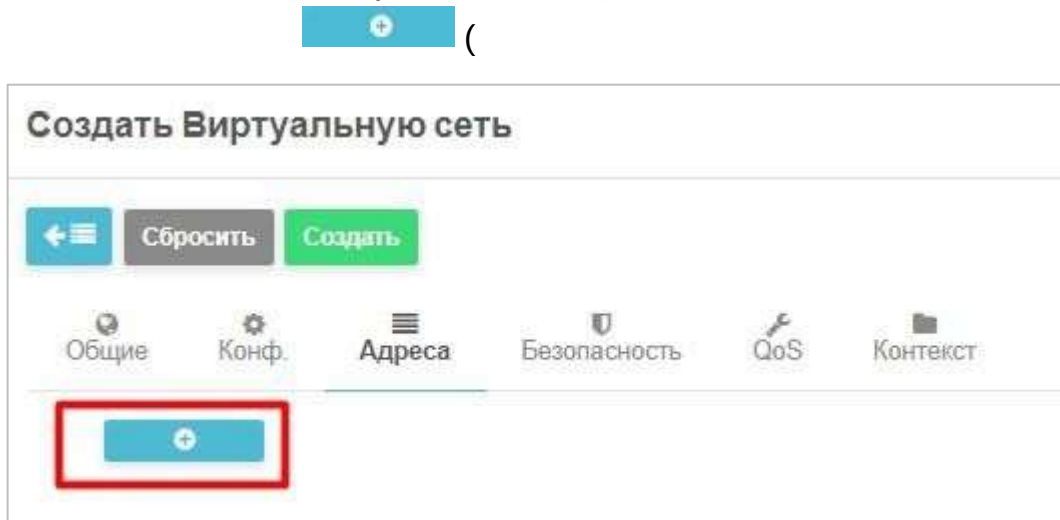


Рисунок 78 - Создание новой виртуальной сети. Вкладка «Адреса» Откроется окно настройки диапазона адресов

Вкладка «Адреса» Откроется окно настройки диапазона адресов (Рисунок 79).

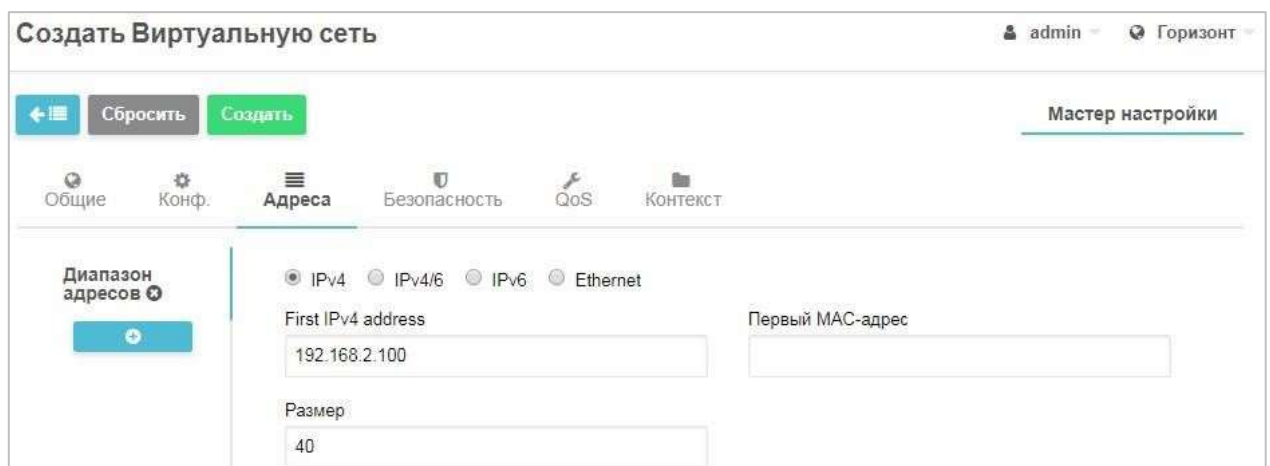


Рисунок 79 - Установка диапазона адресов виртуальной сети

- 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 79).

7. На вкладке **Безопасность** выбрать из списка одну из групп безопасности (Рисунок 80).

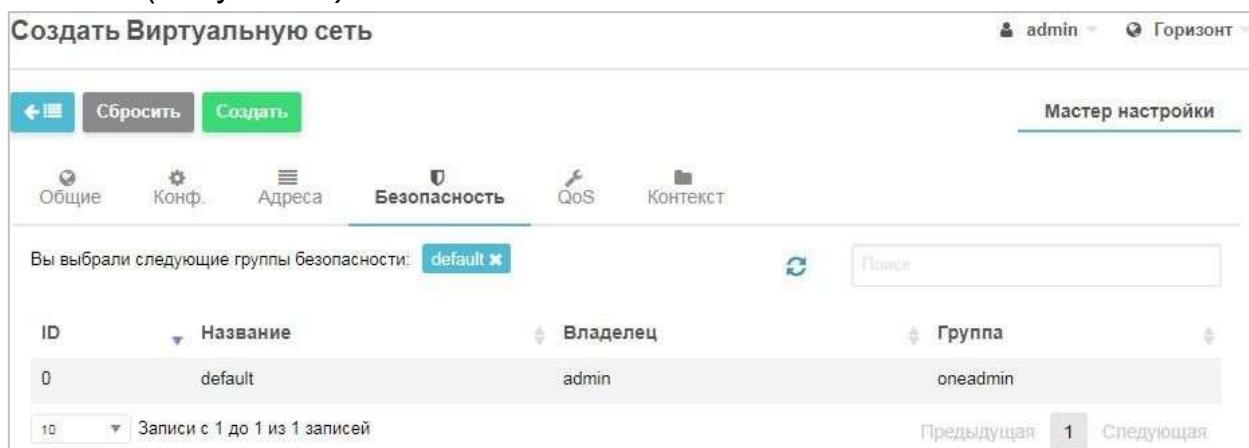


Рисунок 80 - Создание новой виртуальной сети. Вкладка «Безопасность»

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 81);

Создать Виртуальную сеть

admin Горизонт

Сбросить Создать

Мастер настройки

Общие Конф. Адреса Безопасность QoS Контекст

Входящий трафик

Average bandwidth (KBytes/s)
100

Сохранить шаблон виртуального маршрутизатора здесь

Peak burst (KBytes)

Исходящий трафик

Average bandwidth (KBytes/s)
150

Сохранить шаблон виртуального маршрутизатора здесь

Peak burst (KBytes)

Рисунок 81 - 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 VM во время загрузки. Эти атрибуты контекстуализации могут включать в себя, например, сетевые маски, DNS-серверы или шлюзы.

Создать Виртуальную сеть

oneadmin | Горизонт

Включить/Выключить | **Создать**

Мастер настройки | Расширенный

Общие | Conf | Адреса | Безопасность | QoS | **Контекст**

Адрес сети:

Маска подсети:

Шлюз:

Шлюз IPv6:

DNS:

MTU of the Guest interfaces:

Пользовательские атрибуты

Ключ	Значение

[+](#)

Рисунок 82 - 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 **Сеть** → **Вирт. сети**.

12. Выбрать из списка сеть установкой флажка.

13. Нажать 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 83).

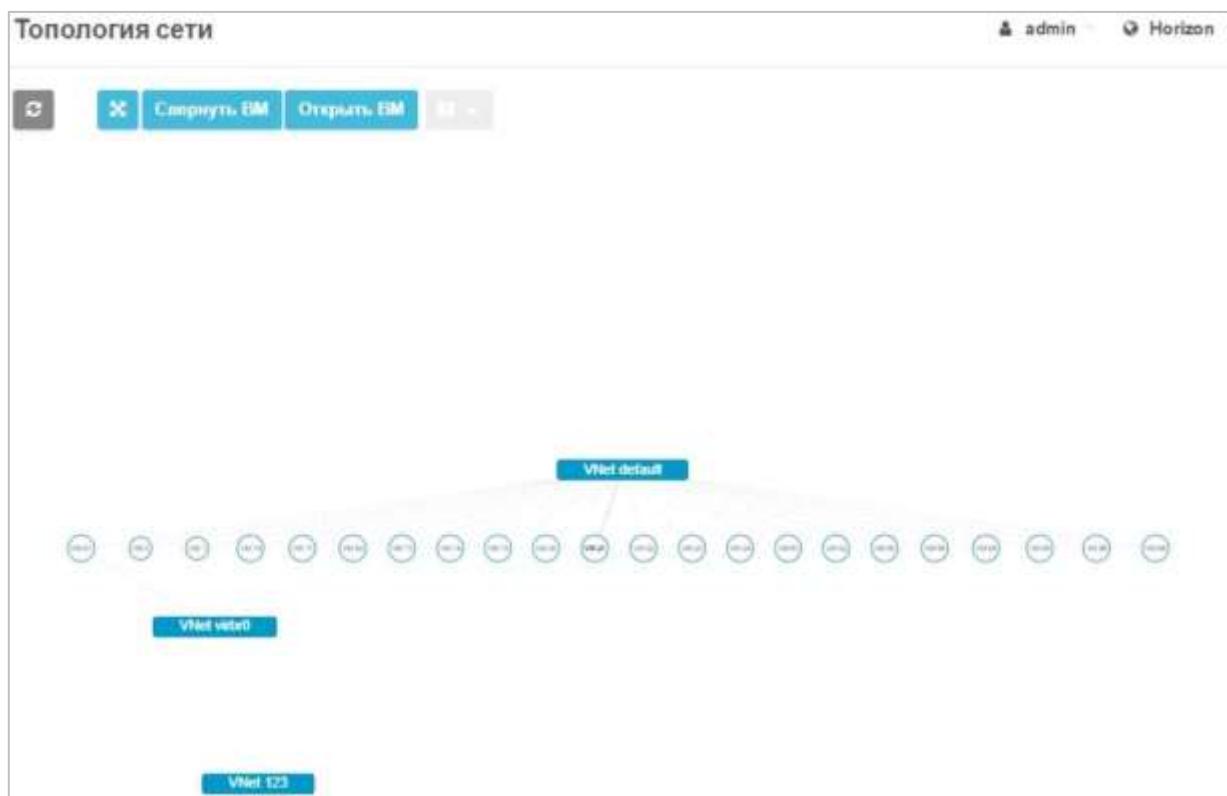


Рисунок 83 - Топология сетей

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 дополнительных 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 84).

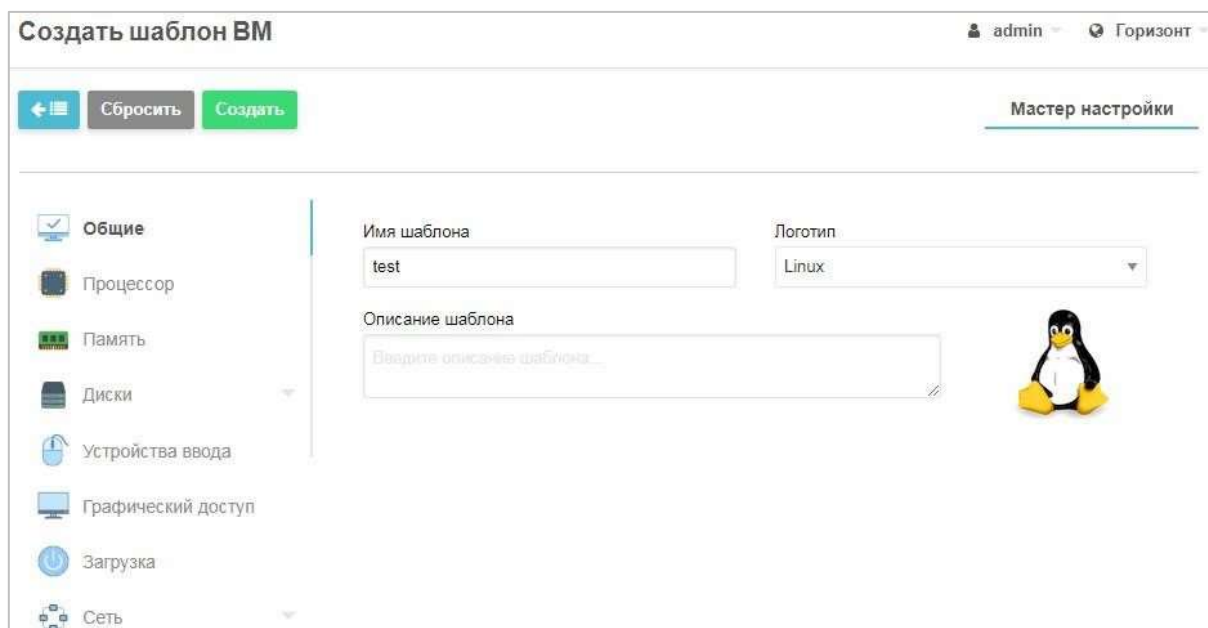


Рисунок 84 - Мастер настройки шаблона ВМ. Вкладка «Общие»

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 84).

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 85).

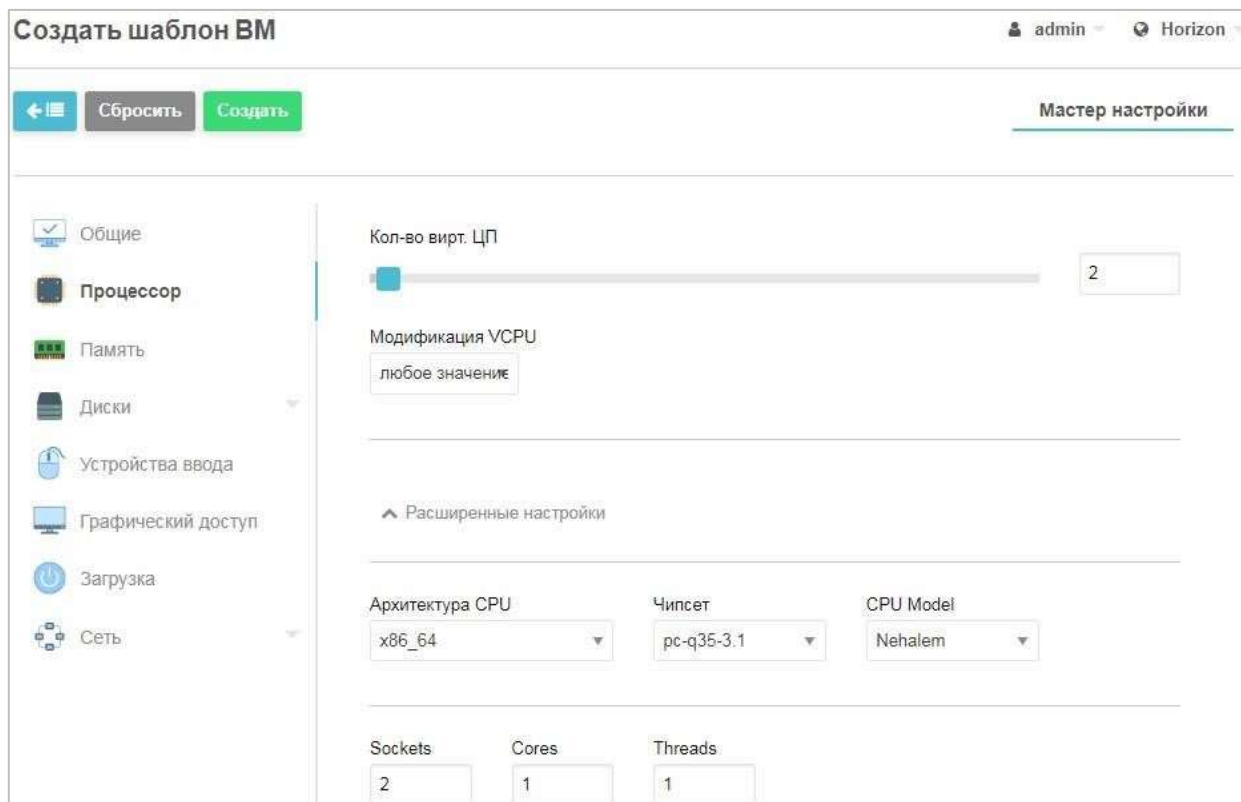


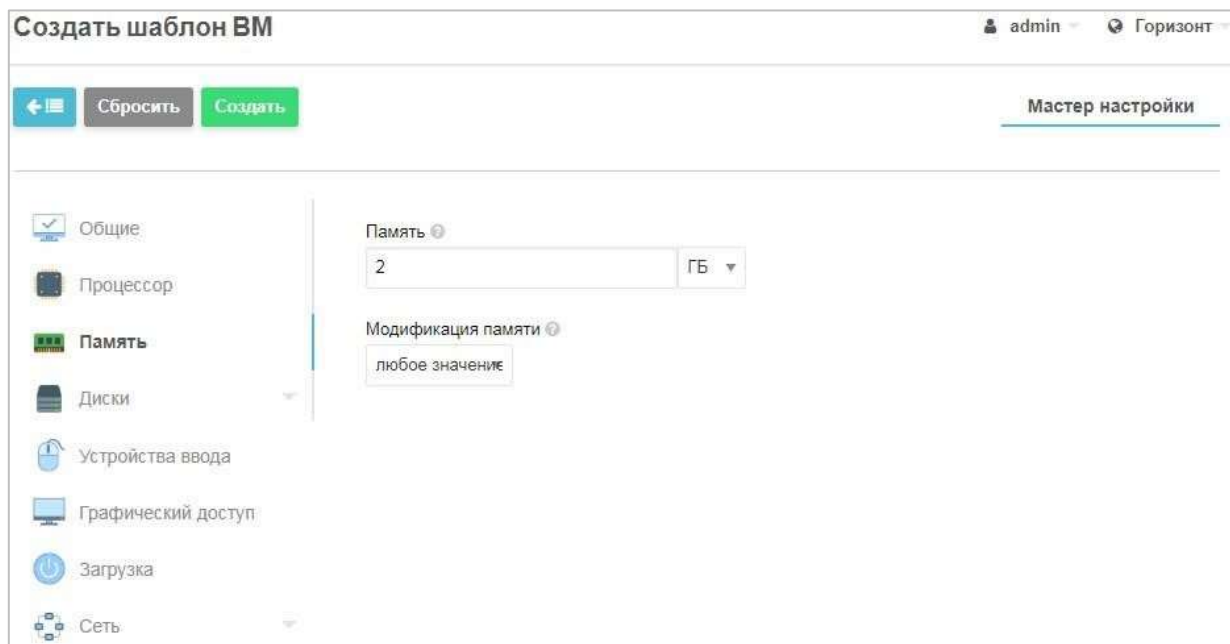
Рисунок 85 - Мастер настройки шаблона VM. Вкладка «Процессор»

- в поле **Кол-во вирт. ЦП** с помощью ползунка или записью значения в поле установить количество виртуальных процессоров, необходимых для VM. 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 VM (для использования процессора хоста выбрать значение *host-model*, если нужна вложенная виртуализация – *host-passthrough*).

Примечание: для обеспечения возможности миграции VM 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 86).



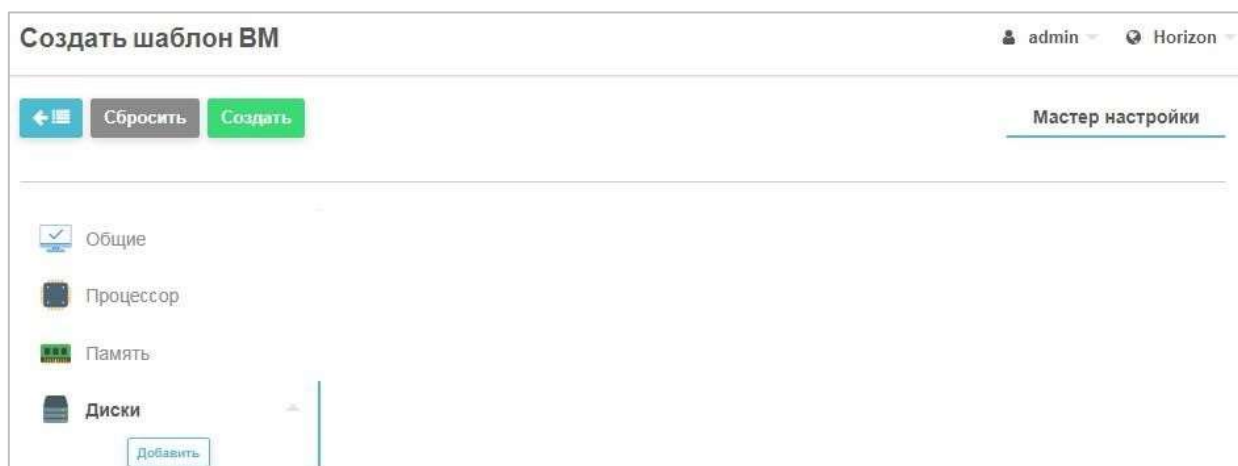
The screenshot shows the 'Создать шаблон ВМ' (Create VM Template) wizard in the 'Мастер настройки' (Configuration Wizard) step. The left sidebar lists configuration categories: 'Общие' (General), 'Процессор' (Processor), 'Память' (Memory), 'Диски' (Disks), 'Устройства ввода' (Input Devices), 'Графический доступ' (Graphic Access), 'Загрузка' (Boot), and 'Сеть' (Network). The 'Память' tab is selected. The main area shows the 'Память' (Memory) field set to '2' GB, with a unit dropdown set to 'ГБ'. Below it, the 'Модификация памяти' (Memory Modification) field is set to 'любое значение' (any value).

Рисунок 86 - 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 87) к шаблону ВМ подсоединяются образы виртуальных дисков или загрузочных дисков с гостевой ОС или другим ПО.



The screenshot shows the 'Создать шаблон ВМ' (Create VM Template) wizard in the 'Мастер настройки' (Configuration Wizard) step, with the 'Диски' (Disks) tab selected. The left sidebar shows the same configuration categories as in the previous screenshot. The 'Диски' tab is highlighted. A 'Добавить' (Add) button is visible at the bottom of the 'Диски' section.

Рисунок 87 - 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 подключаемого диска (Рисунок 88).

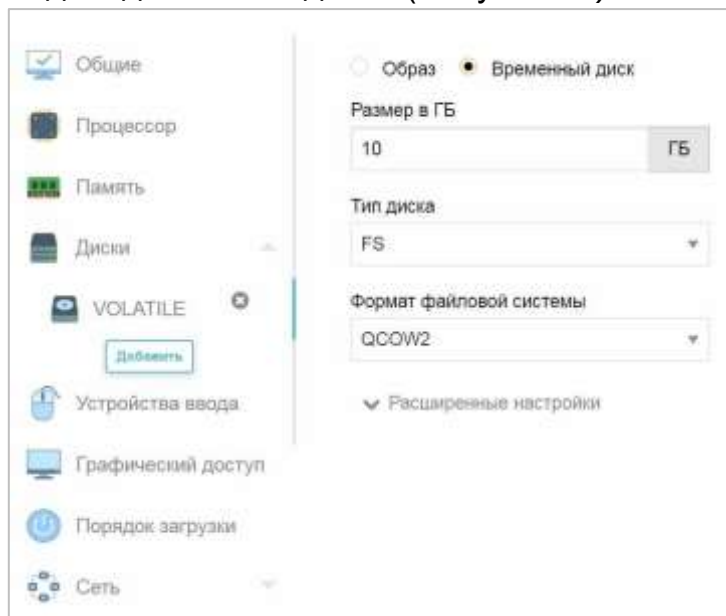


Рисунок 88 - Мастер настройки шаблона VM. Параметры дисков

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

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

- 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 подключаемого 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).

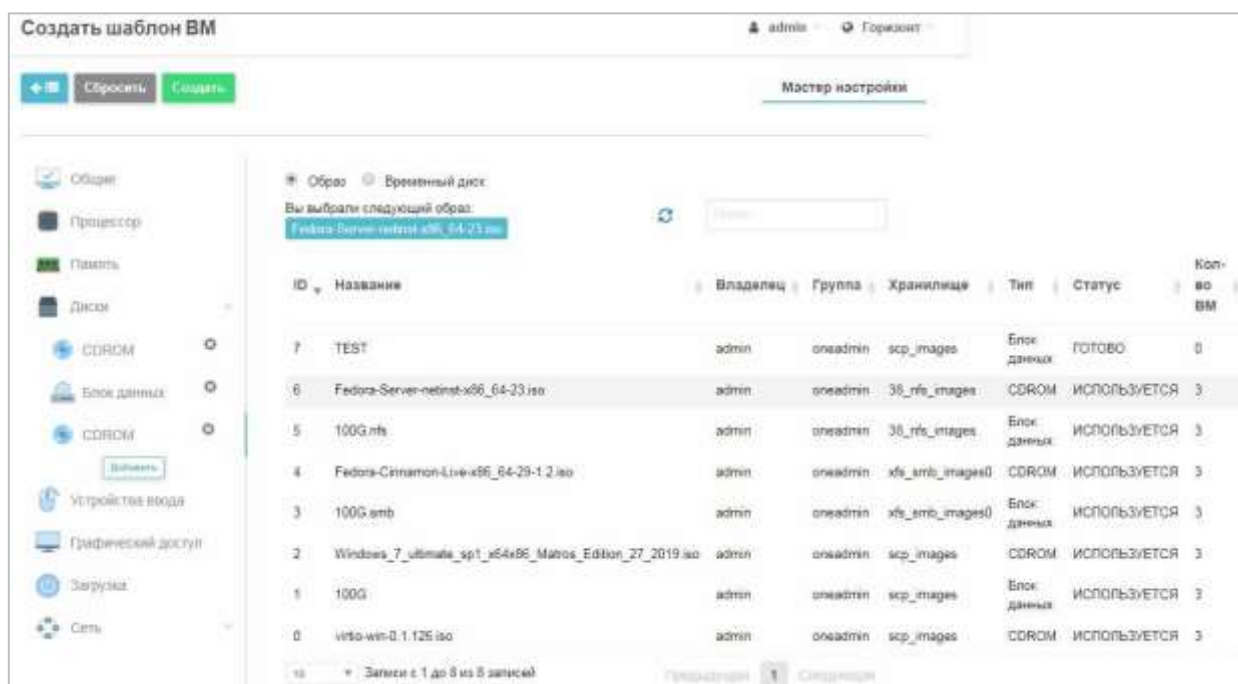


Рисунок 89 - Мастер настройки шаблона VM. Выбор образа диска

- при выборе образа диска типа **Блок данных** (в колонке **Тип**) вкладка

второго уровня примет вид  **Блок данных** (Рисунок 89

);

- при выборе типа образа **CD-ROM** с установочным диском гостевой ОС или другим ПО вкладка второго уровня примет

вид  **CDROM**;

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

вид  .

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**;

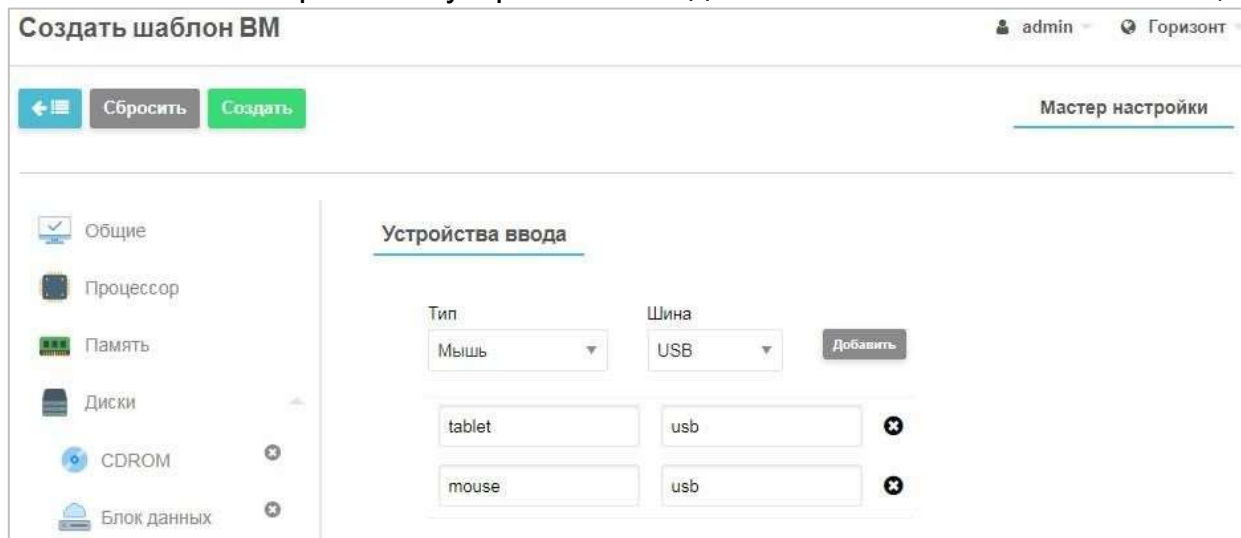


Рисунок 90 - Мастер настройки шаблона VM. Вкладка «Устройства ввода»

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

– после ввода всех данных следует нажать кнопку **Добавить** - на экране отобразится подсоединенное к VM устройство ввода (Рисунок 90).

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

8. На вкладке **Графический доступ** указывается средства графического доступа к консоли VM: доступ отсутствует, **VNC** или **SPICE** (Рисунок 254).

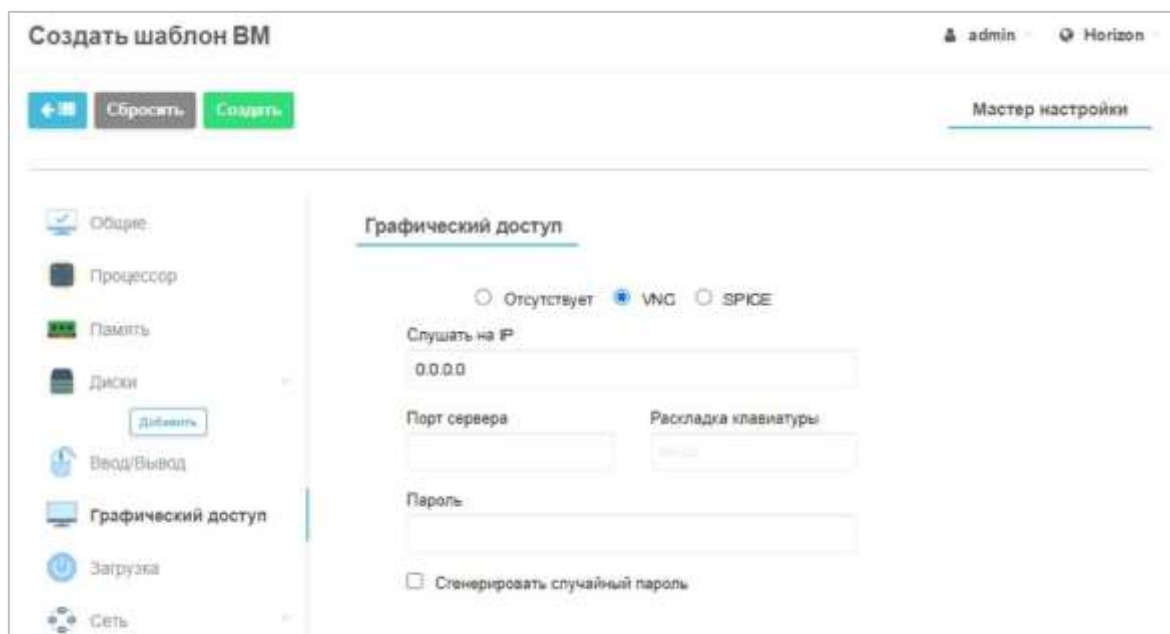


Рисунок 90 – Мастер настройки шаблона VM. Вкладка «Графический доступ»

Для подключения тонких клиентов через терминалы к VM необходимо устанавливать протокол **SPICE**. Для администрирования VM 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**.

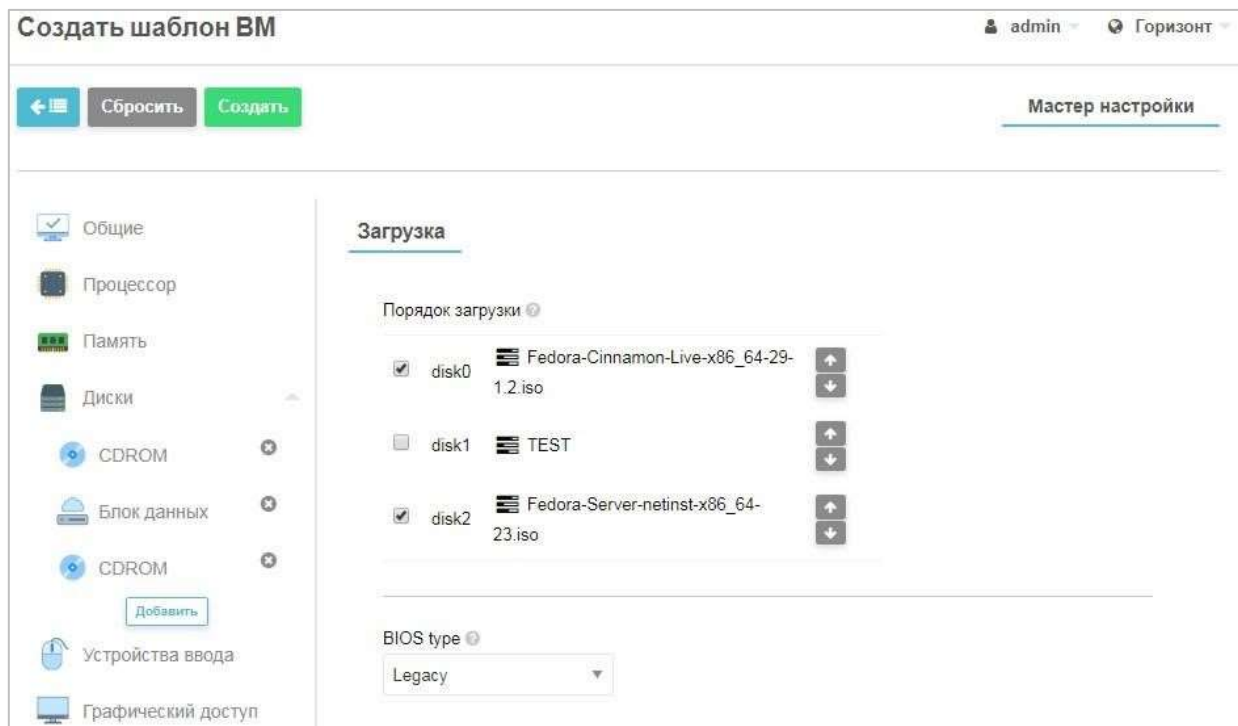


Рисунок 91 - Мастер настройки шаблона ВМ. Вкладка «Загрузка ОС»

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).

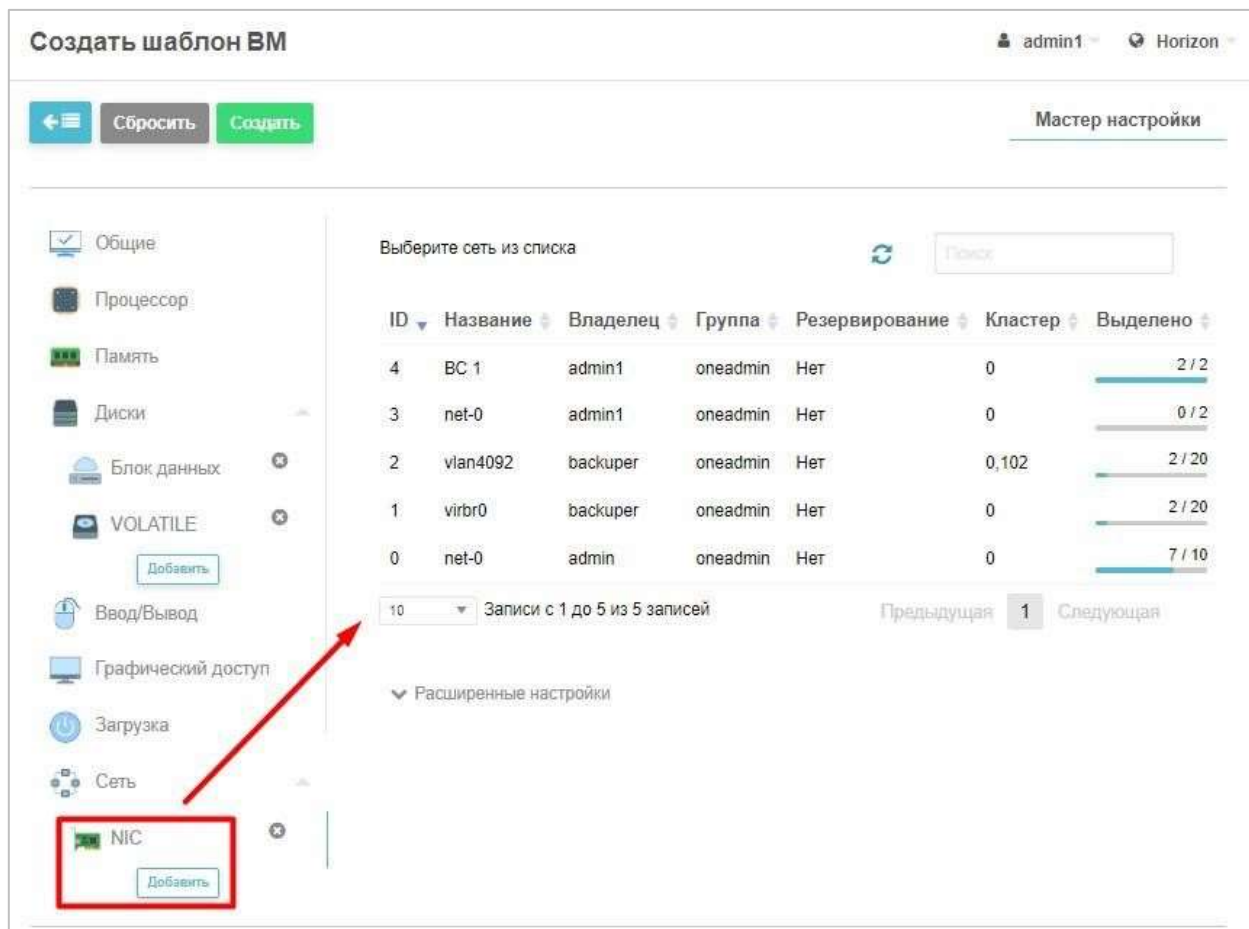


Рисунок 92 - Мастер настройки шаблона VM. Вкладка «Сеть»

При необходимости можно присоединить шаблон VM 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 VM;

– **Override Network Inbound Traffic QoS** и **Override Network Outbound Traffic QoS** задать пропускную способность VM;

– **Аппаратное обеспечение** позволяет «пробросить» внутрь VM 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

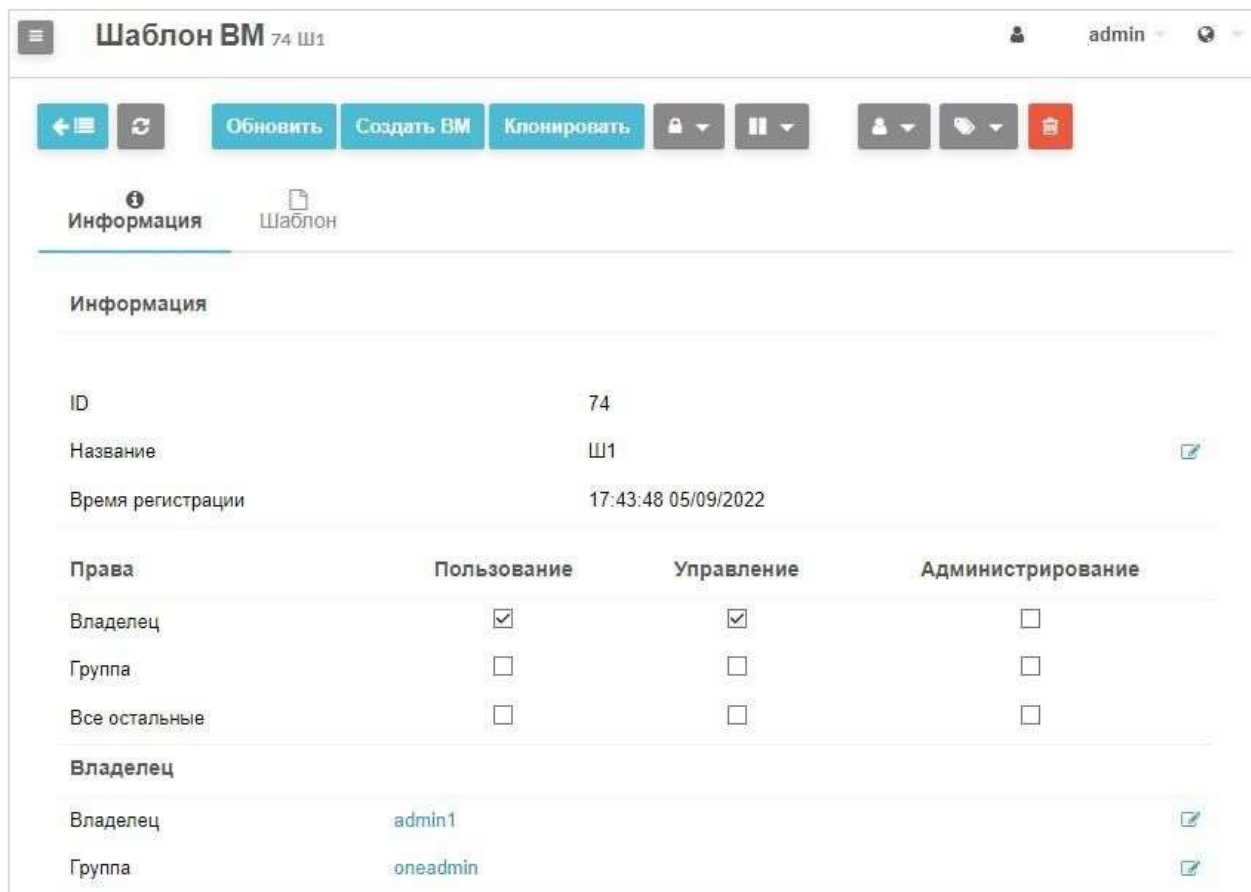


Рисунок 93 - Окно параметров шаблона VM

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

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



Рисунок 94 - Панель управления конфигурацией шаблона VM

С помощью панели управления шаблоном VM пользователь может создать VM на базе этого шаблона VM, 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

Виртуальные машины являются изолированными процессами от процессов друг друга, в том числе и от процессов гипервизора. Изоляция процессов ВМ обеспечена на уровне qemu.

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.

Укажите параметры виртуальной машины admin Horizon

[←](#) [Сбросить](#) [Создать](#)

Вы выбрали следующий Шаблон: **шаблон1** [↻](#)

ID	Название	Владелец	Группа	Время регистрации
2	шаблон1	admin	oneadmin	13/12/2022 10:28:48
1	test_win	admin	oneadmin	12/12/2022 13:05:36

10 Записи с 1 до 2 из 2 записей [Предыдущая](#) **1** [Следующая](#)

Имя ВМ Количество экземпляров ☐ Не размещать

шаблон1

[Производительность](#) [Диски](#)

Память

Диск 0: Copy of 1

CPU Кол-во вирт. ЦП

[Сеть](#)

▼ Интерфейс [+](#)

[Сетевой интерфейс](#)

▲ Расширенные настройки

[Узел](#)

Пожалуйста выберите из списка не менее одного узла [↻](#)

ID	Название	Кол-во ВМ	Реальн. ЦП	Реально Памяти	Выделено Памяти	Статус

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) «Звезда» поддерживается динамическое распределение ВМ по серверам виртуализации. Например, при высокой загрузке 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).

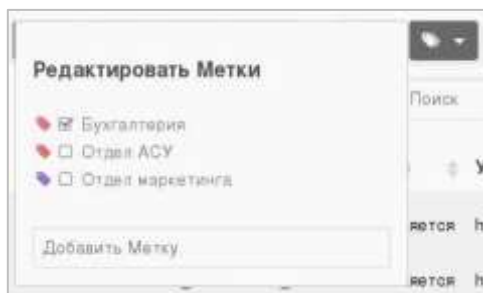


Рисунок 96 - Метки VM

Для работы с VM в отдельной вкладке браузера следует нажать на иконку , откроется окно рабочего стола VM (Рисунок 97).

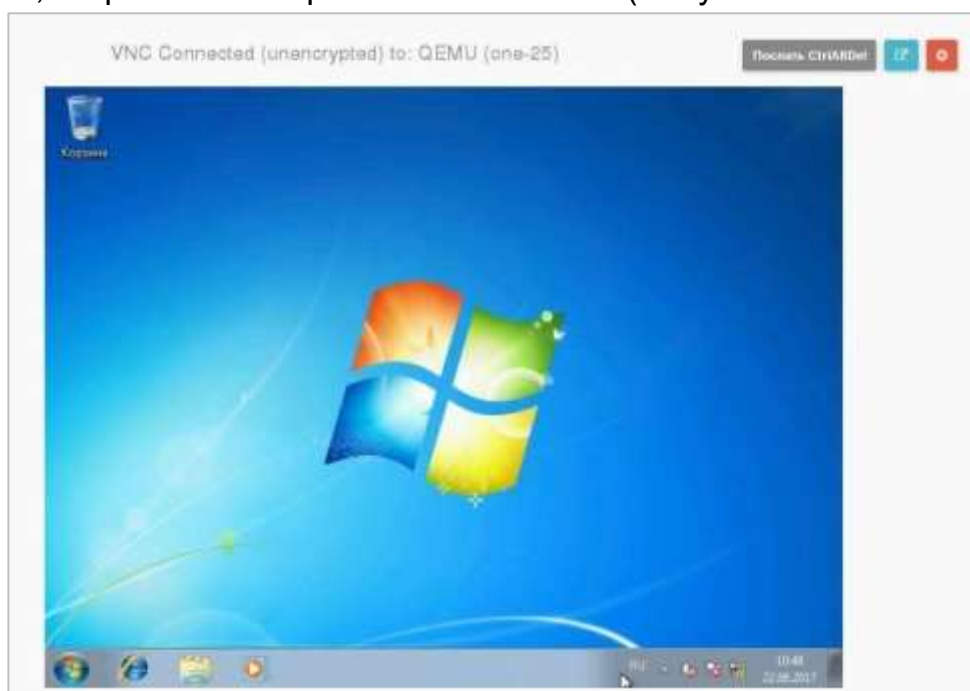


Рисунок 97 - Вид рабочего стола гостевой ОС

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 VM на любой стадии функционирования обеспечивается за счет использования в VM 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 VM

Кнопка	Функция	Описание
	Создание новой VM (активна всегда)	Открывается страница интерфейса создания новой VM.
	Обновление текущей страницы (активна всегда)	После внесения каких-либо изменений в работу VM или ее конфигурацию необходимо выполнить обновление страницы, чтобы увидеть изменения.
	Создание шаблона VM на базе существующей VM	Позволяет создать шаблон с параметрами и конфигурацией существующей VM. Примечание. VM во время создания шаблона должна быть выключена.
	Запуск VM	На VM 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 VM, 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 VM	Работа VM приостанавливается. VM может быть запущена в любой момент времени с текущего состояния до приостановки работы VM.
	Остановить	Работа VM останавливается. Оперативная память записывается на жесткий диск. Работа VM может быть запущена в любой момент времени с текущего состояния до остановки VM.
	Выпадающее меню:	
	Отключить питание	Корректное выключение VM из системы группового управления
	Отключить питание жесткий	Принудительное отключение питания VM. Отключение питания VM из системы группового управления (аналогично некорректному выключению физической машины посредством отключения питания из сети).
	Отменить размещение	VM снимается с узла и сохраняется в хранилище в виде файла-образа VM с возможностью восстановления. Восстановление VM осуществляется непосредственно размещением ее на серверном узле или нажатием кнопки запуска VM (в этом случае

		происходит автоматическое размещение VM на узле)
	Отменить размещение жесткий	VM снимается с узла и сохраняется на физическом сервере в виде файла-образа VM с возможностью

		восстановления. Восстановление VM происходит так, как будто она создается заново. Происходит ее размещение на узле.
	Выпадающее меню:	
	Перезагрузка	Корректная перезагрузка гостевой ОС на VM (аналогична перезагрузки из меню «Пуск»)
	Перезагрузка жесткий	Принудительная перезагрузка гостевой ОС на VM (аналогична перезагрузке через кнопку «reset»)
	Выпадающее меню:	
	Разместить на узле	Ручное размещение VM на узле с возможностью выбора узла размещения.
	Перенести VM с приостановкой	При миграции VM будет остановлена
	Перенести VM без приостановки	Горячая миграция VM между узлами
	Запретить размещение	Запретить размещать VM на узле

	Восстановить	новление VM. При выборе о пункта отрывается окно с выпадающим списком 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 VM из системы; – удалить и создать повторно – удаляет VM из системы, а затем корректно
		развертывает в системе аналогичную VM.
	Выпадающее меню:	
	Сменить владельца	Позволяет сменить пользователя VM
	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 назначению. <i>Например: ВМ бухгалтерии, ВМ отдела АСУ и т.д.</i>
	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.

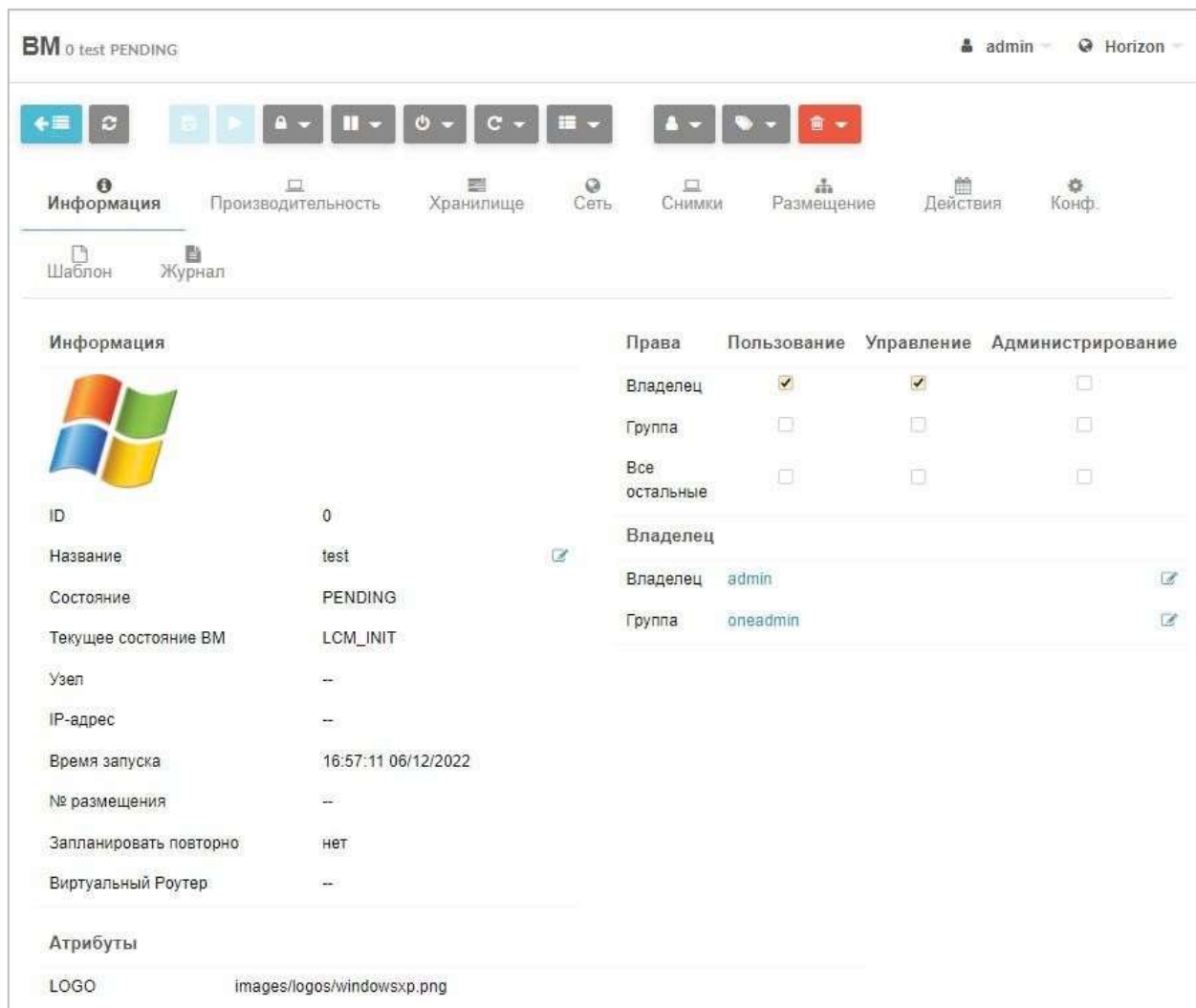


Рисунок 100 – Вкладка «Информация»

3.2.22.1 Вкладка «Информация»

На вкладке **Информация** выводятся общие данные о работе VM: логотип ОС, номер VM в системе (поле ID), состояние, текущее состояние VM, IP-адрес узла размещения, IP-адрес VM, время запуска, запланирован ли повторный запуск, адрес виртуального роутера; информация о владельце VM и права пользователей – для отключённой VM.

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

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).

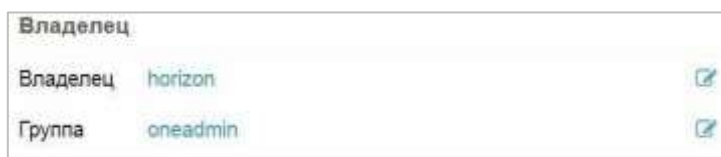


Рисунок 102 - Раздел «Владелец»

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 VM.

Примечание: Виртуальная машина во время изменения базовых характеристик должна быть выключена.

Для изменения характеристик производительности VM:

1. Нажать на кнопку **Изменить**.

Откроется окно **Изменить базовые характеристики** (Рисунок 104).

2. Внести новые параметры VM: объем оперативной памяти, процент процессорного времени ЦП, количество виртуальных ЦП, сокеты, ядра, потоки;

3. Нажать кнопку **Изменить**.

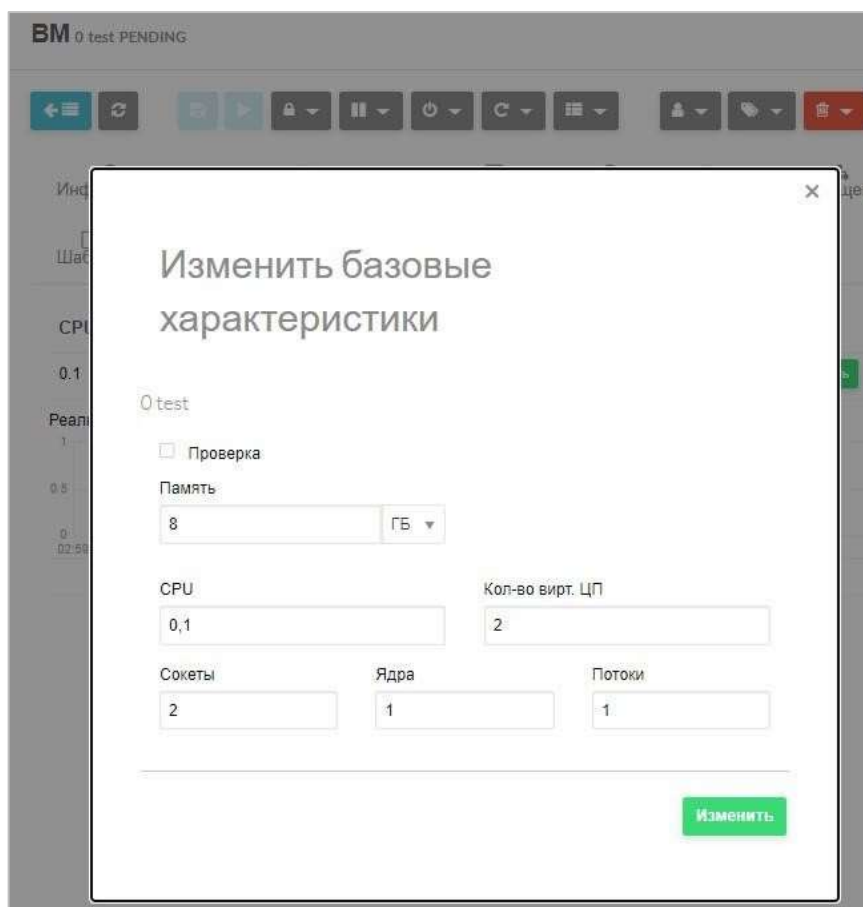


Рисунок 104 - Изменение базовых характеристик

3.2.22.3 Вкладка «Хранилище»

На вкладке **Хранилище** представлены подключенные к MB ресурсы (пустые образы жестких дисков, CDROM-образы, образы ОС, временные диски).

В нижней части вкладки **Хранилище** в виде графика представлен мониторинг взаимодействия VM 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).

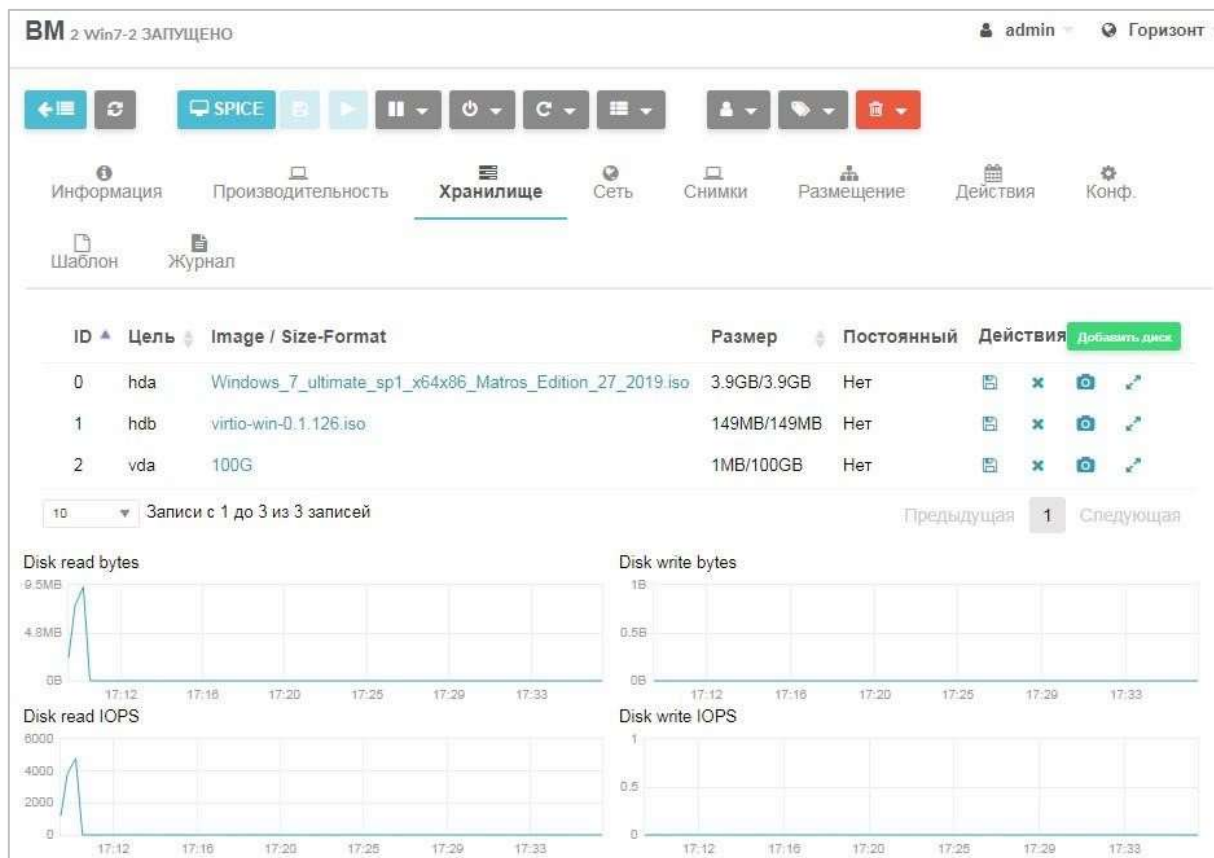


Рисунок 105 - Вкладка «Хранилище»

Пользователь может добавлять, удалять, редактировать ресурсы.

Для присоединения дополнительного ресурса:

1. Нажать кнопку **Добавить диск**.
2. В открывшемся окне **Присоединить диск** (Рисунок 106).

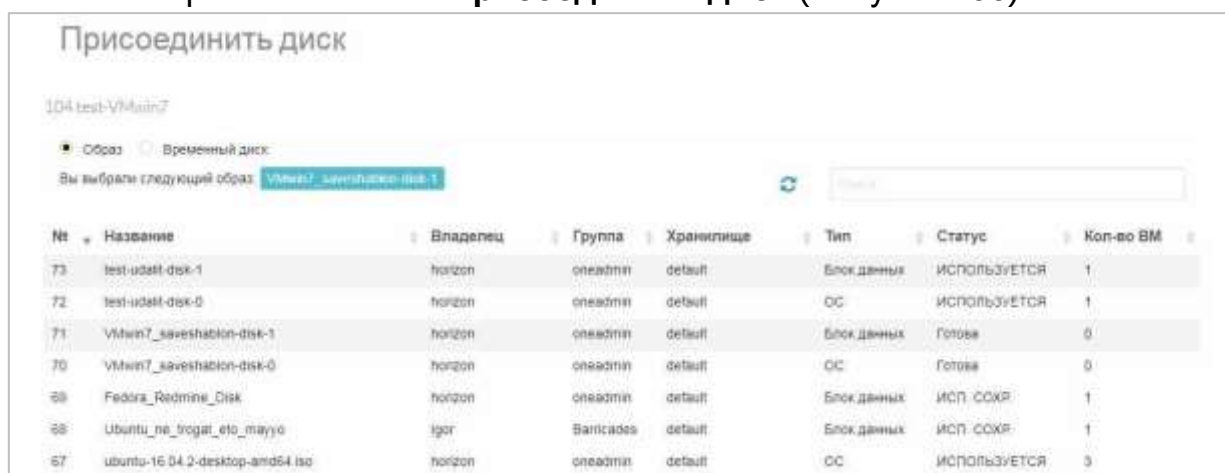


Рисунок 106 - Присоединить диск к VM

3. Выбрать образ из списка.

4. Нажать кнопку **Присоединить**.

5. Нажать Расширенные настройки:

– В секции IO throttling (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 VM необходимо в столбце **Действия** (Рисунок 105) выбрать одну из опций:

–  – создание образа диска из одного из ресурсов VM (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 VM.

3.2.22.3.1 Создание образа диска из одного из ресурсов VM

Для создания образа диска из одного из исполняемых жестких дисков VM:

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**.

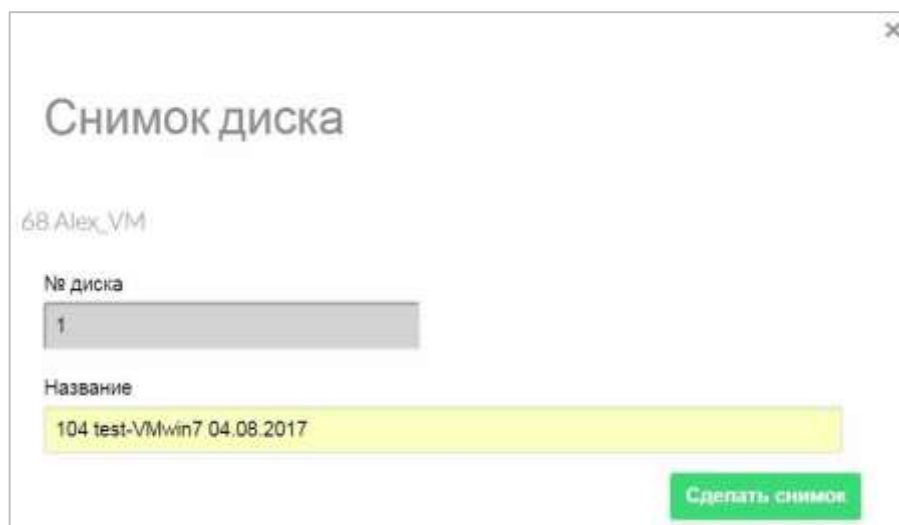
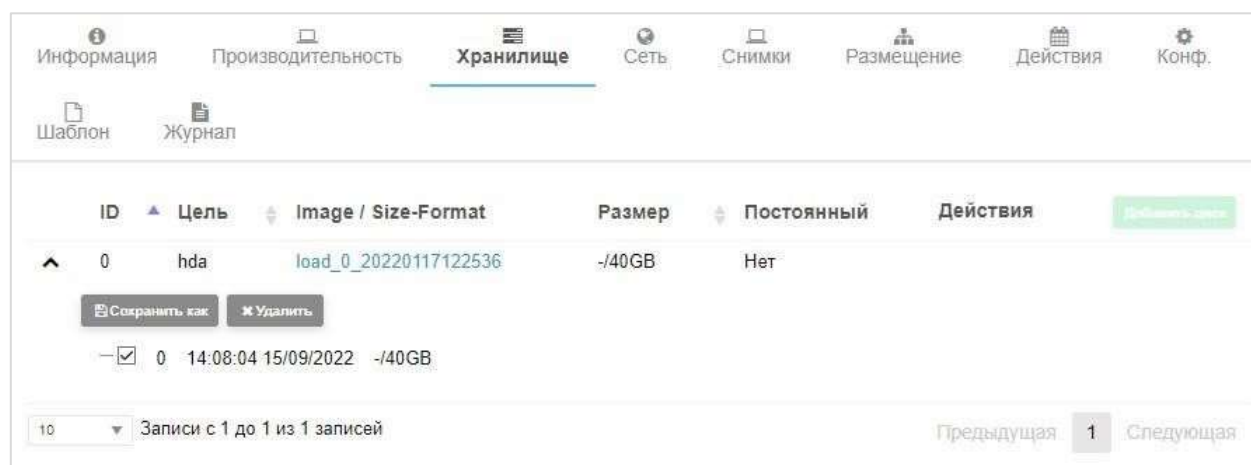


Рисунок 108 - Снимок диска

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).



ID	Цель	Image / Size-Format	Размер	Постоянный	Действия
0	hda	load_0_20220117122536	-/40GB	Нет	

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**.

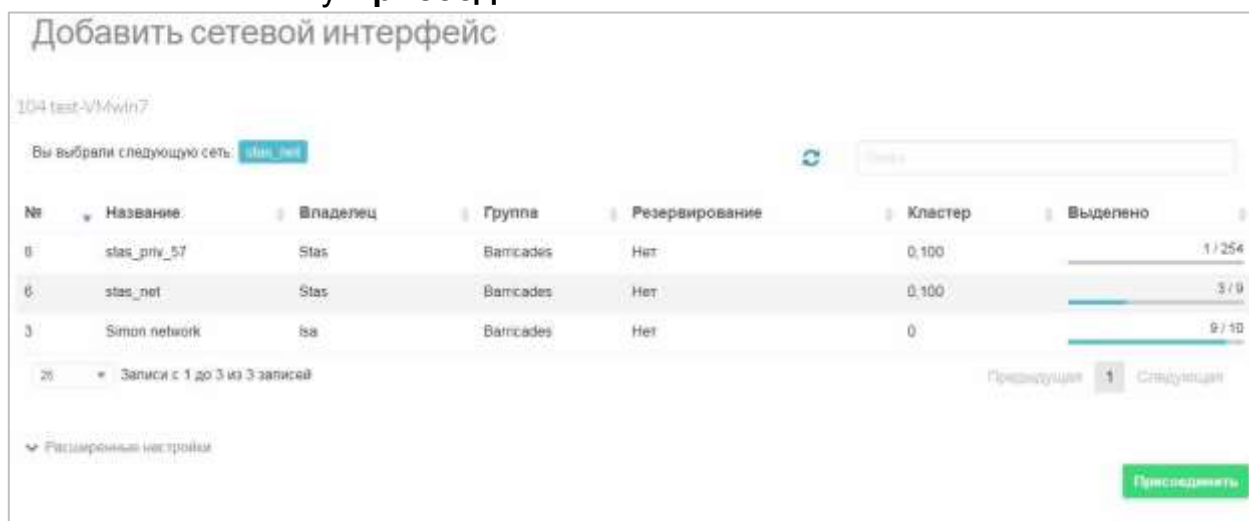


Рисунок 112 - Добавить сетевой интерфейс в VM

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).

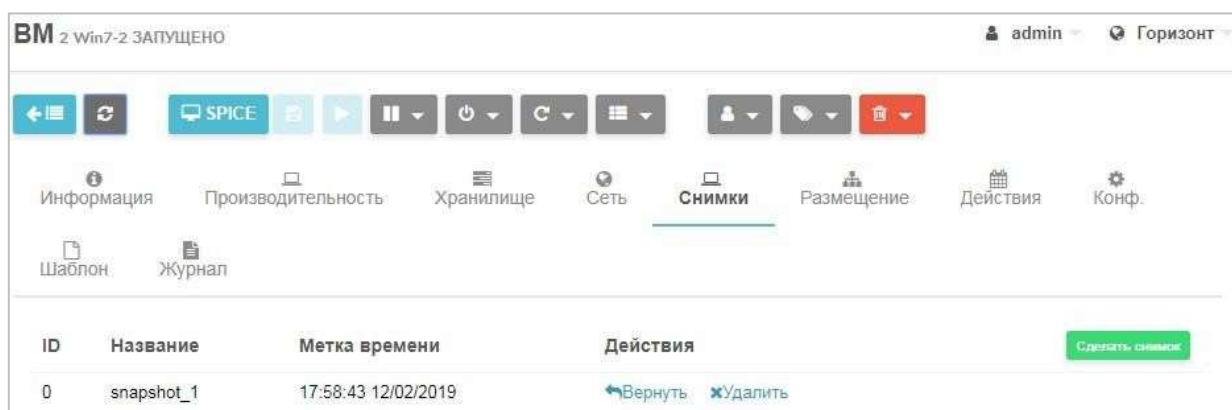
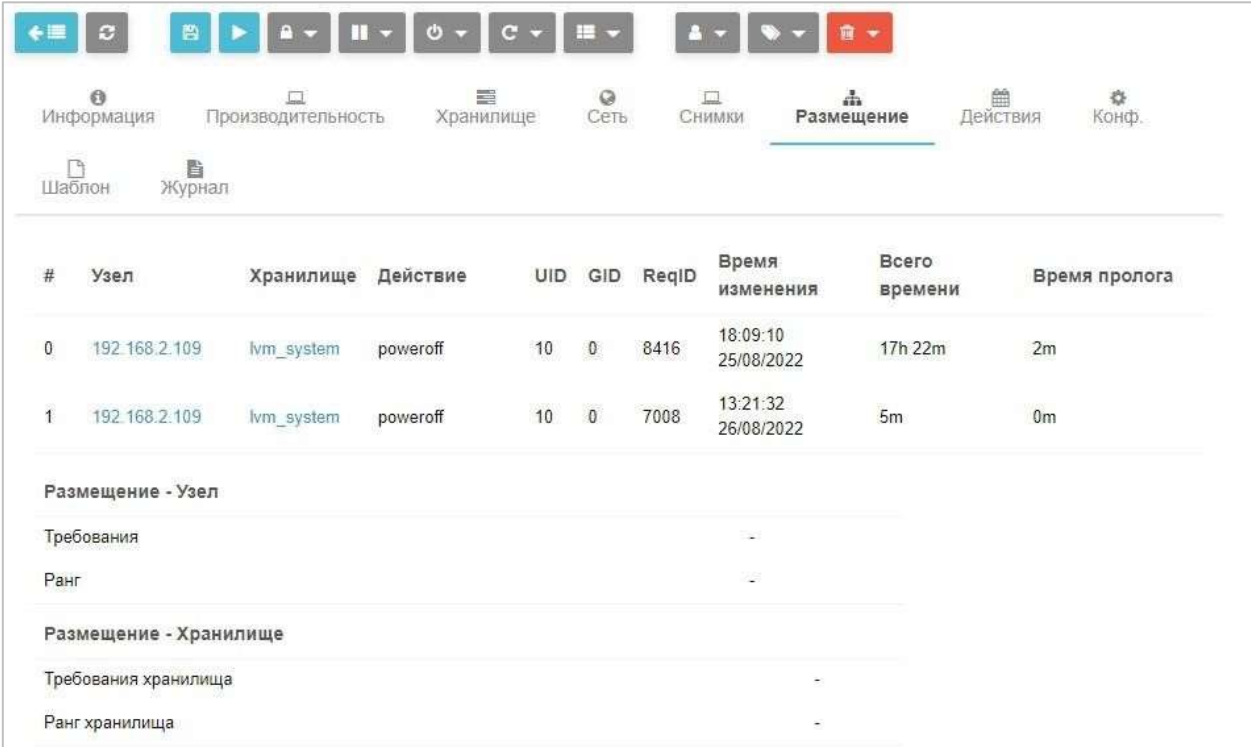


Рисунок 113 - Создание снимков ВМ

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.



#	Узел	Хранилище	Действие	UID	GID	ReqID	Время изменения	Всего времени	Время пролога
0	192.168.2.109	lvm_system	poweroff	10	0	8416	18:09:10 25/08/2022	17h 22m	2m
1	192.168.2.109	lvm_system	poweroff	10	0	7008	13:21:32 26/08/2022	5m	0m

Размещение - Узел

Требования: -

Ранг: -

Размещение - Хранилище

Требования хранилища: -

Ранг хранилища: -

»

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).

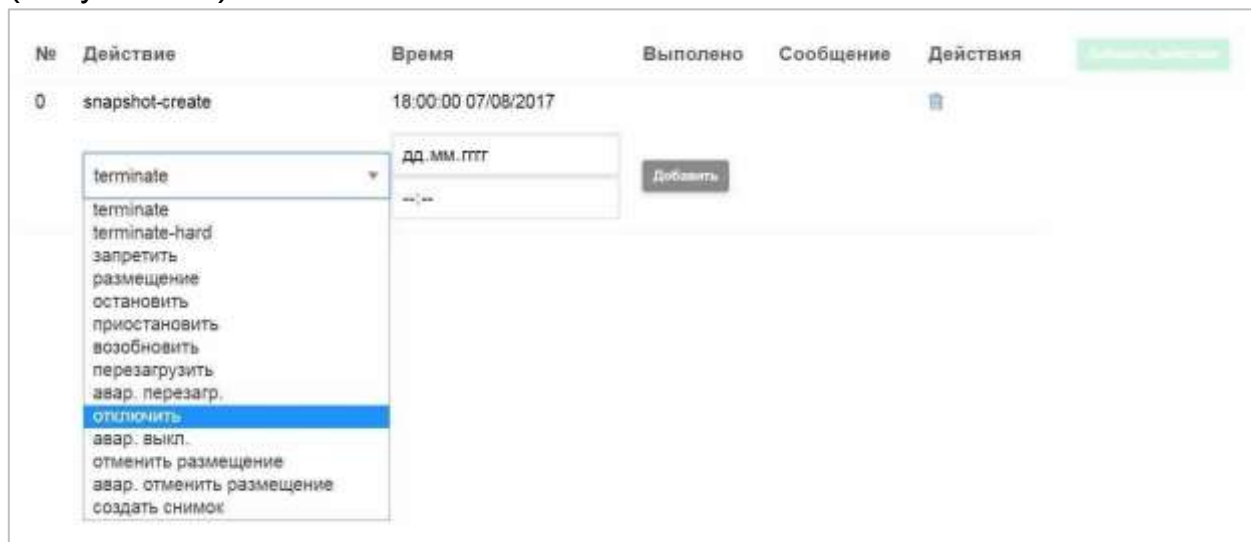


Рисунок 115 - Добавление действий

14. Выбрать требуемое действие, установить дату и время его выполнения.

15. Нажать кнопку **Добавить**.

На странице появится запись о запланированном действии и времени его исполнения (Рисунок 116).

№	Действие	Время	Выполнено	Сообщение	Действия	Добавить действие
0	snapshot-create	18:00:00 07/08/2017				
1	poweroff	18:30:00 07/08/2017				

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 VM должна быть выключена.

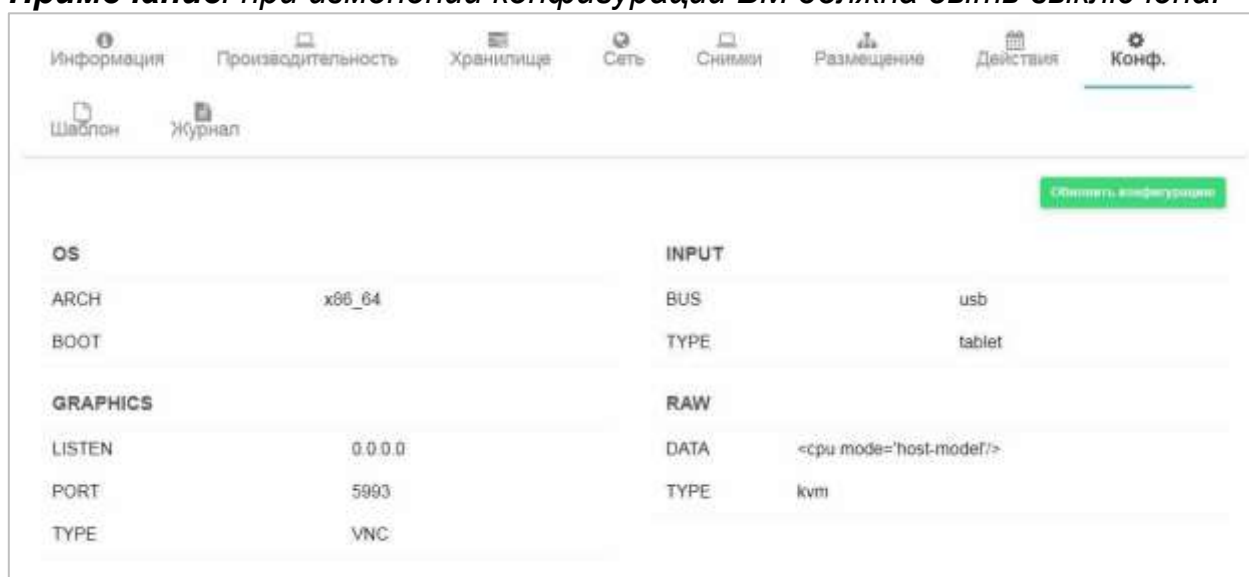


Рисунок 117 – Вкладка «Конфигурация»

Для изменения конфигурации VM:

16. Нажать на кнопку **Обновить конфигурацию** (Рисунок 117).

Откроется мастер настройки изменения конфигурации VM

(Рисунок 118).

The screenshot shows the 'Обновить конфигурацию ВМ' (Update VM Configuration) wizard for a VM named '0 test'. The user is 'admin' and the environment is 'Horizon'. The 'Мастер настройки' (Configuration Wizard) is active. The 'Загрузка ОС' (OS Load) tab is selected, showing various settings for the OS load configuration. The settings are organized into sections: 'Архитектура CPU' (CPU Architecture) with a dropdown set to 'x86_64'; 'Тип BIOS' (BIOS Type) with a dropdown set to 'Legacy'; 'Чипсет' (Chipset) with a dropdown set to 'pc-q35-3.1'; 'Меню загрузки' (Boot Menu) with a dropdown set to 'NO'; 'Root устройство' (Root Device) with a dropdown set to 'sda1'; 'CPU Model' with a dropdown set to 'Nehalem'; 'USB контроллер' (USB Controller) with a dropdown set to 'xHCI'; 'Порядок загрузки' (Boot Order) with a checkbox for 'p1s0' and a radio button for 'Ручные настройки' (Manual Settings); 'Параметры загрузки ядра' (Kernel Load Parameters) with a text field containing 'to console=0x1'; and 'Путь к исполняемому файлу загрузчика' (Path to the bootable file) with an empty text field.

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).

Обновить конфигурацию VM 4 Strelec

admin Horizon

← Обновить

Мастер настройки

Загрузка ОС Ввод/Выход Все остальные

Графический доступ

☐ Отсутствует ☐ VNC ☒ SPICE

Слушать на IP: 0.0.0.0

Раскладка клавиатуры: ru

Пароль:

Устройства ввода

Тип: [выбор] Шина: [выбор] Добавить

tablet usb +

Рисунок 119 - Изменение конфигурации VM. Ввод/Выход

19. На вкладке **Все остальные** можно «пробросить» (подключить напрямую) внутрь VM какие-либо PCI-устройства (Рисунок 120).

Обновить конфигурацию VM 19 test_centos-19

admin Horizon

← Обновить

Мастер настройки

Загрузка ОС Ввод/Выход Все остальные

Ввести параметры вручную

Тип: kvm

Данные:

```
<devices>
<hostdev mode='subsystem' type='pci' managed='yes'>
<source>
<address domain='0x0000' bus='0x1a' slot='0x00' function='0x0'>
</source>
<address type='pci' domain='0x0000' bus='0x1a' slot='0x00' function='0x0'>
</address>
</hostdev>
</devices>
```

Рисунок 120 - Обновление конфигурации VM. 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 выполняется ВМ, а также внесенные пользователем в код изменения и коррективы (Рисунок 121).



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).

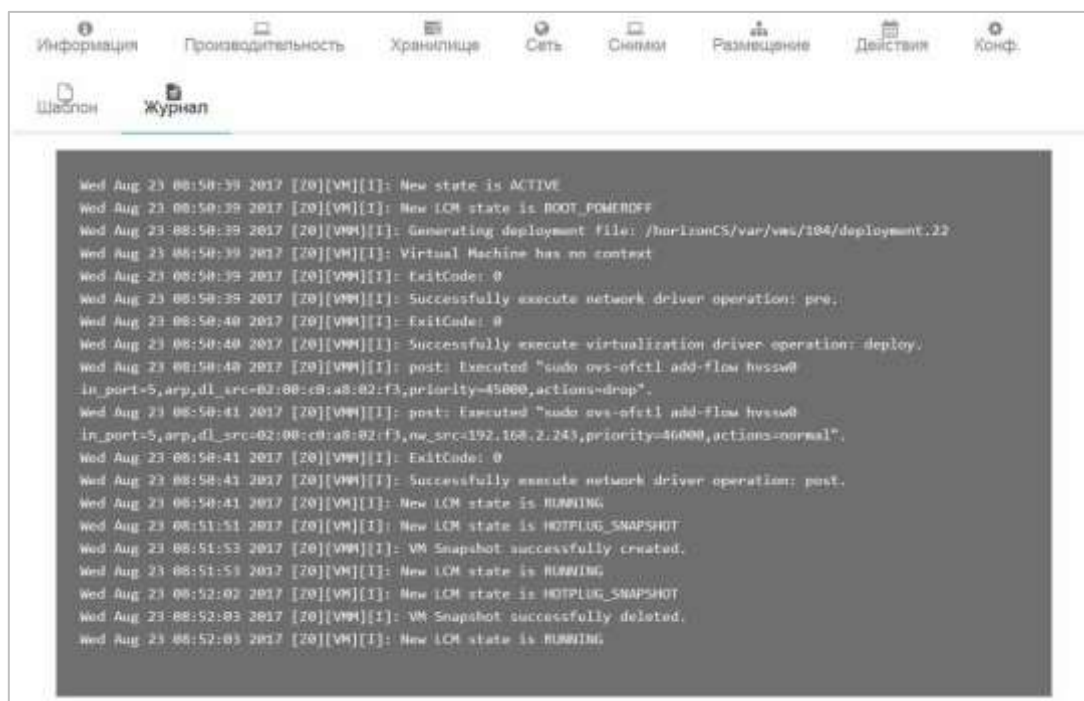


Рисунок 122 - Вкладка «Журнал»

В журнале отображаются следующие события (Таблица 7): Таблица 7 – События журнала VM

Событие	Запись в журнале
Время создания VM	Дата и время строки с состоянием «BOOT»
Запуск VM	Строка с состоянием «RUNNING»
Уничтожение VM	Строка с состоянием «EPILOG»
Миграция VM	Строка с состоянием «MIGRATE»
Создание/удаление снимка VM	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 VM.

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).

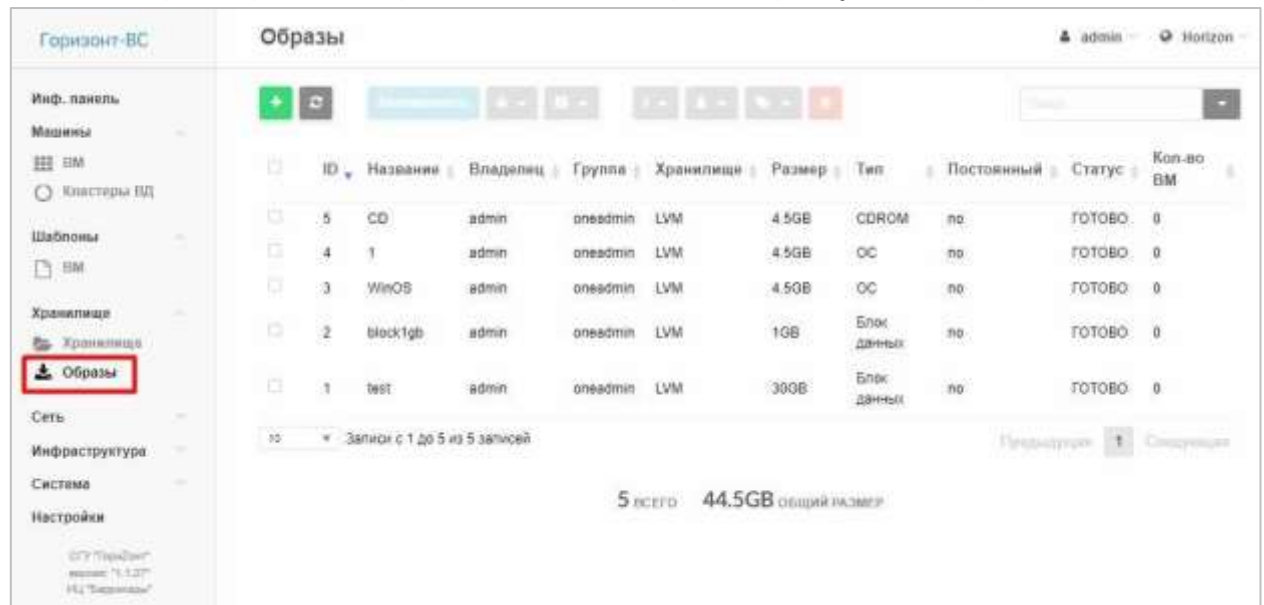


Рисунок 123 - Раздел «Хранилище → Образы»

4. Нажать кнопку добавления образа – .

Откроется окно создания образа (Рисунок 124).

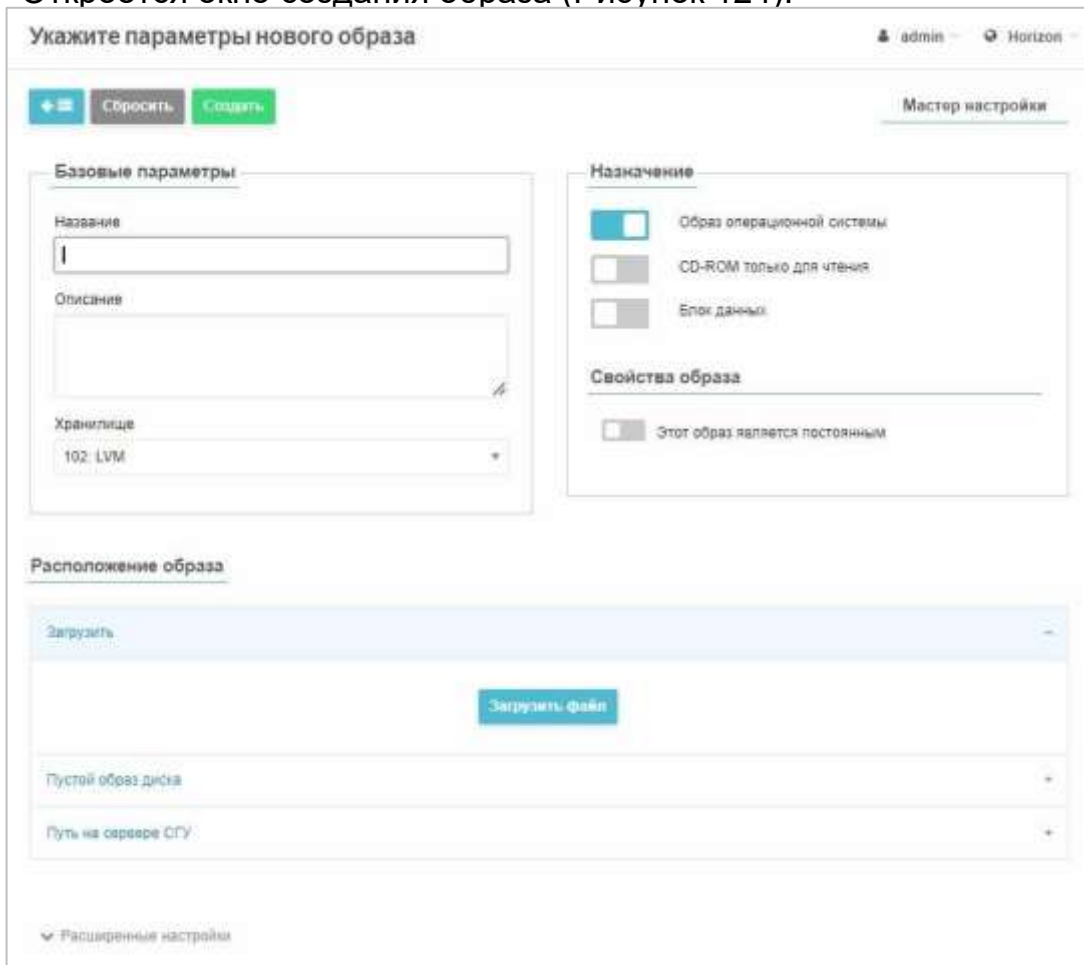


Рисунок 124 - Окно создания образа хранилища

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**.

Укажите параметры нового образа le_admin Horizon

[←](#) [Сбросить](#) [Создать](#) Мастер настройки

Базовые параметры

Название
образ 1

Описание

Хранилище
115: r1

Назначение

☐ Образ операционной системы

☐ CD-ROM только для чтения

☒ Блок данных

Свойства образа

☒ Этот образ является постоянным

Расположение образа

Загрузить	+
Пустой образ диска	*
Путь на сервере СГУ	-
Путь к файлу /dev/sdd	

Расширенные настройки

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).

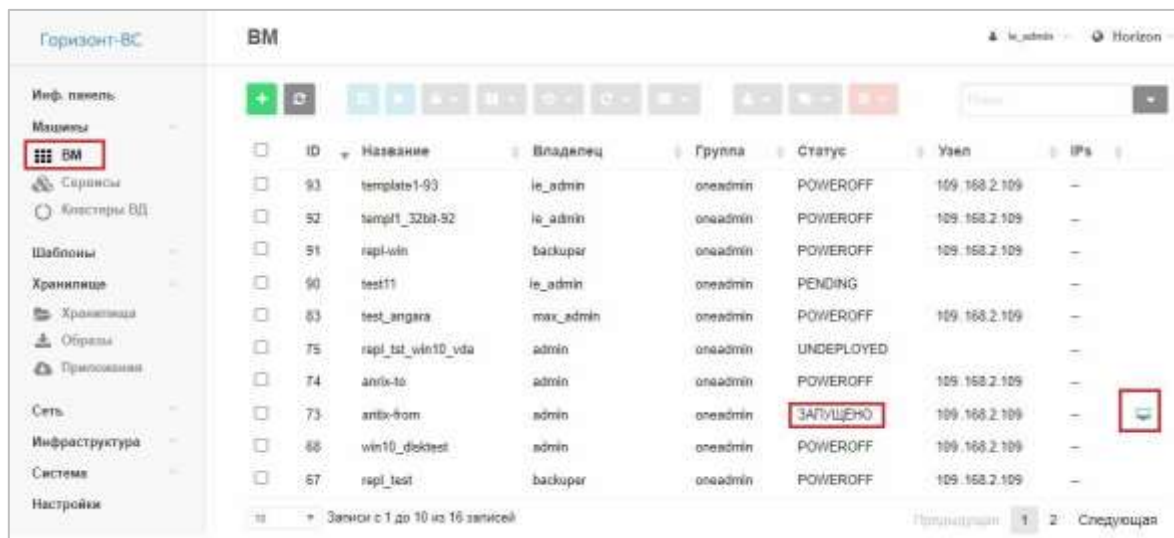


Рисунок 126 - Выбор VM для подключения тома СХД

8. Перейти на вкладку **Хранилище** (Рисунок 127).

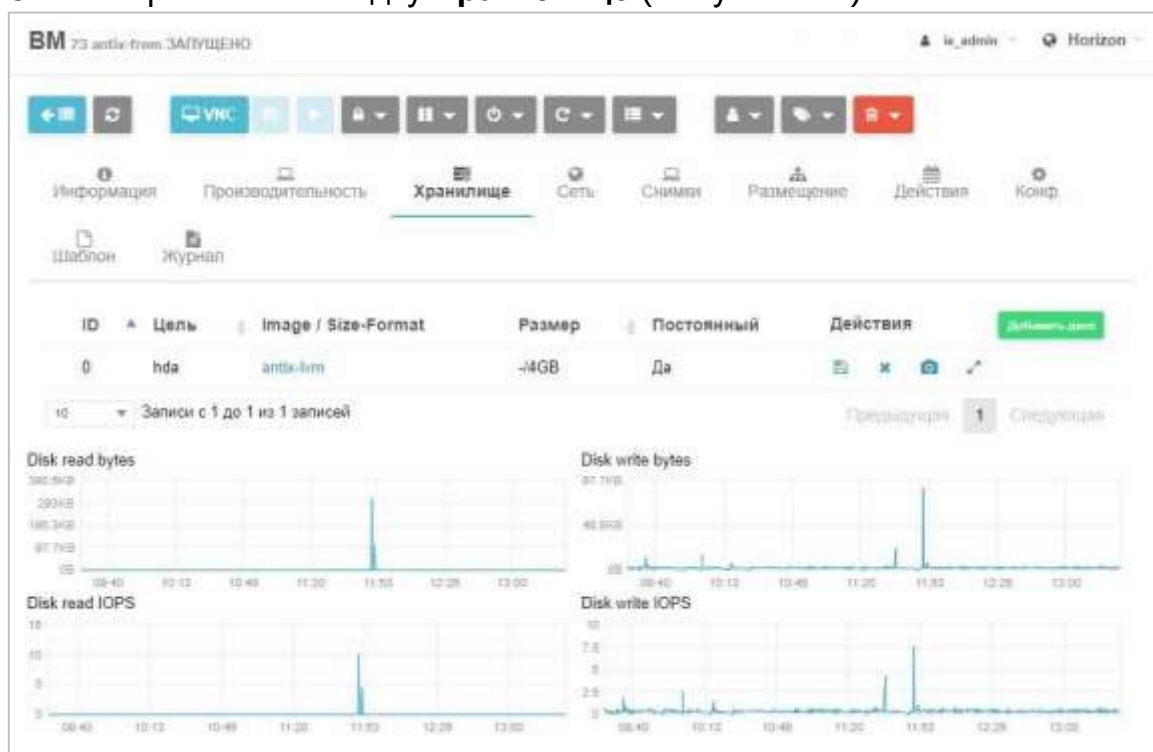


Рисунок 127 - Информация о VM. Вкладка хранилище

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).

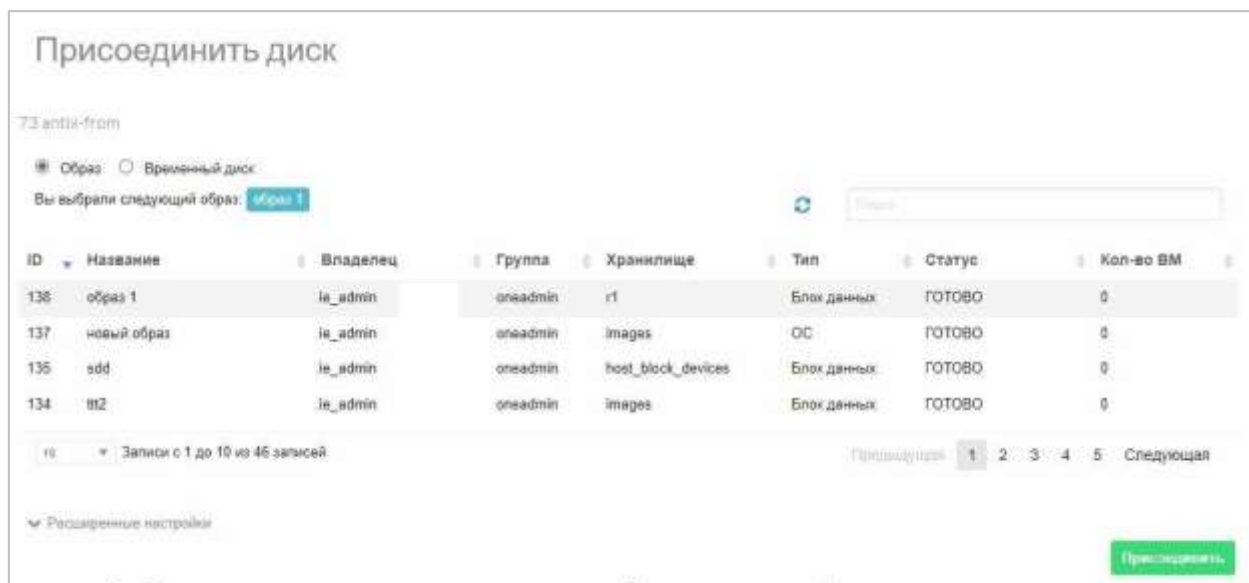


Рисунок 128 - Подключение тома СХД к ВМ

Добавленный ТОМ СХД появится в списке хранилищ, подключенных к данной ВМ (Рисунок 129).

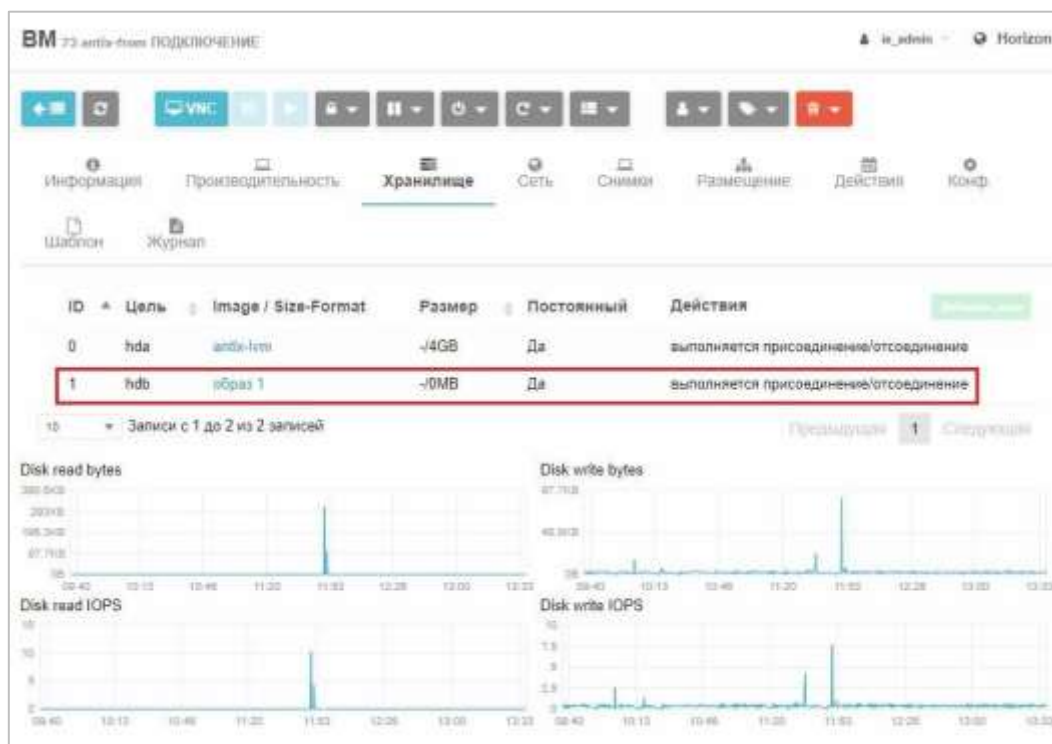


Рисунок 129 - Том СХД подключен к ВМ

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).

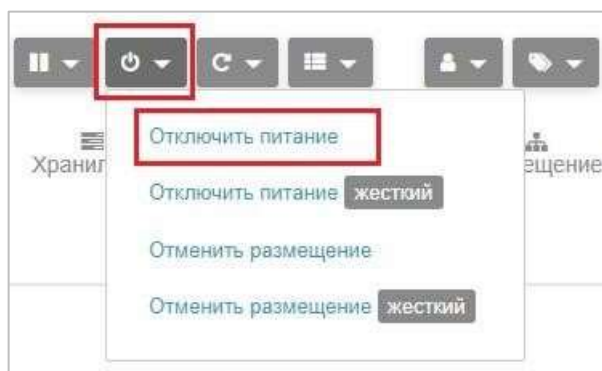


Рисунок 130 – Отключение питания ВМ

3. Перейти на вкладку **Конф.**
4. Нажать кнопку **Обновить конфигурацию** (Рисунок 131).

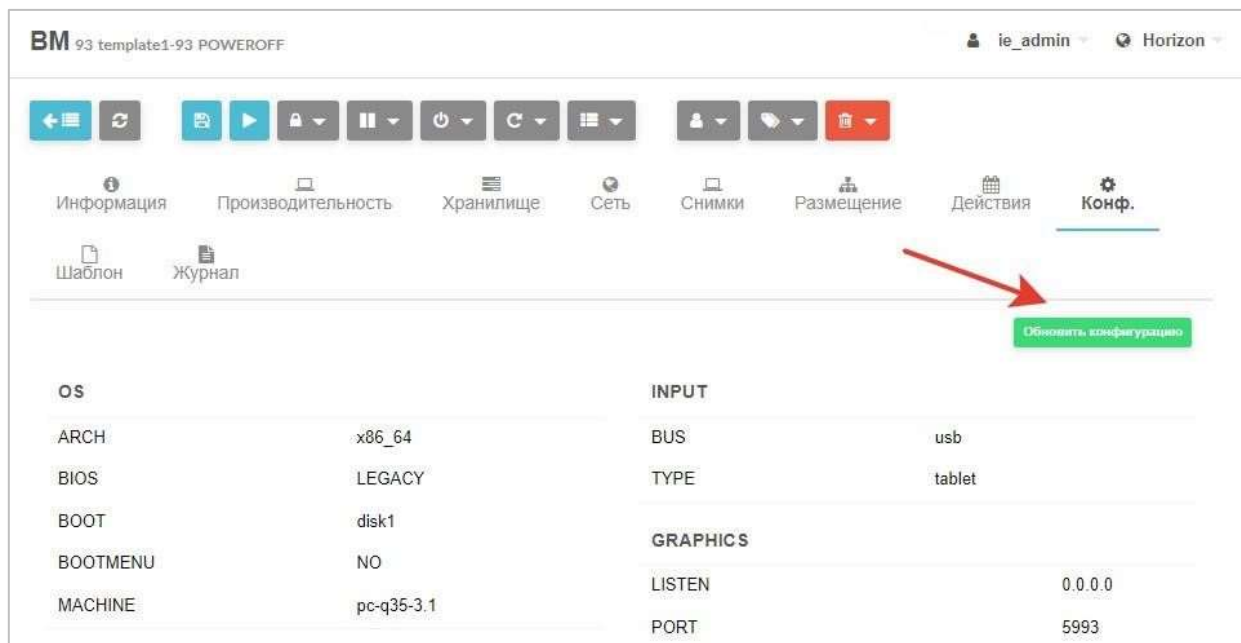


Рисунок 131- Кнопка «Обновить конфигурацию»

Откроется окно **Обновить конфигурацию ВМ** (Рисунок 132).

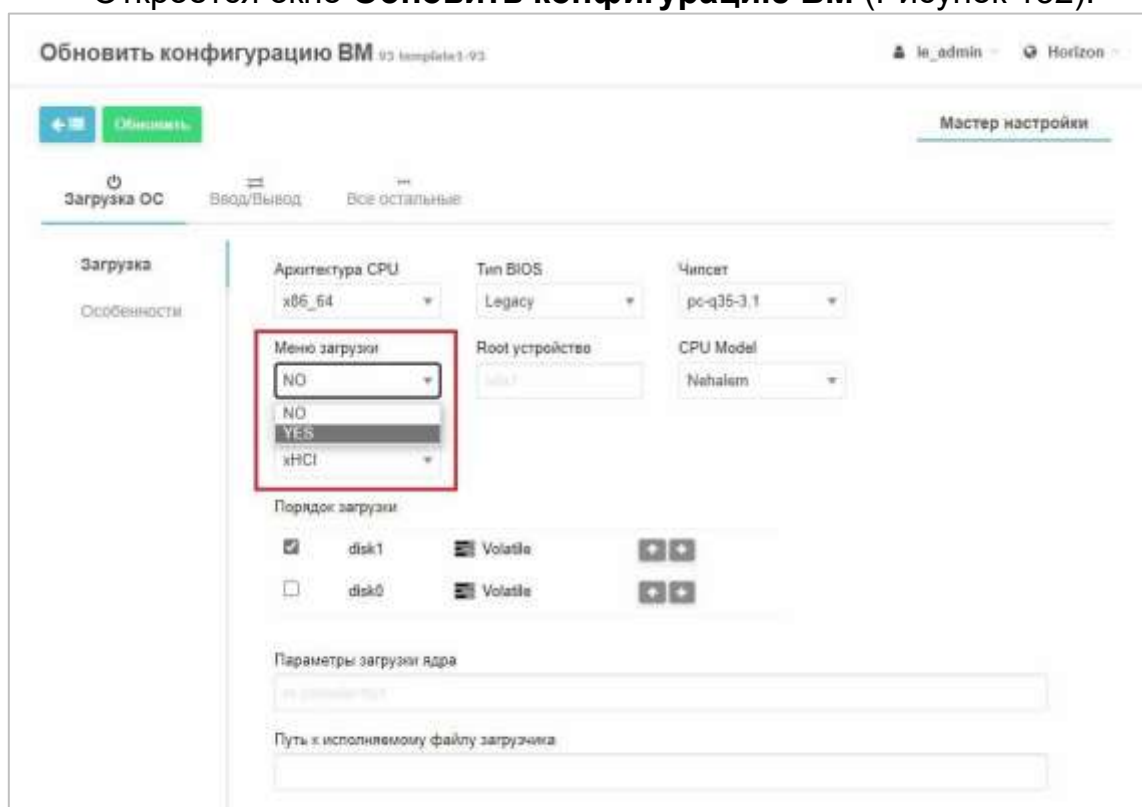


Рисунок 132 - Окно «Обновить конфигурацию ВМ»

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) «Звезда» 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) «Звезда» 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) «Звезда» 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 отчетности и информация по использованию ресурсов центрального процессора (Рисунок 134).

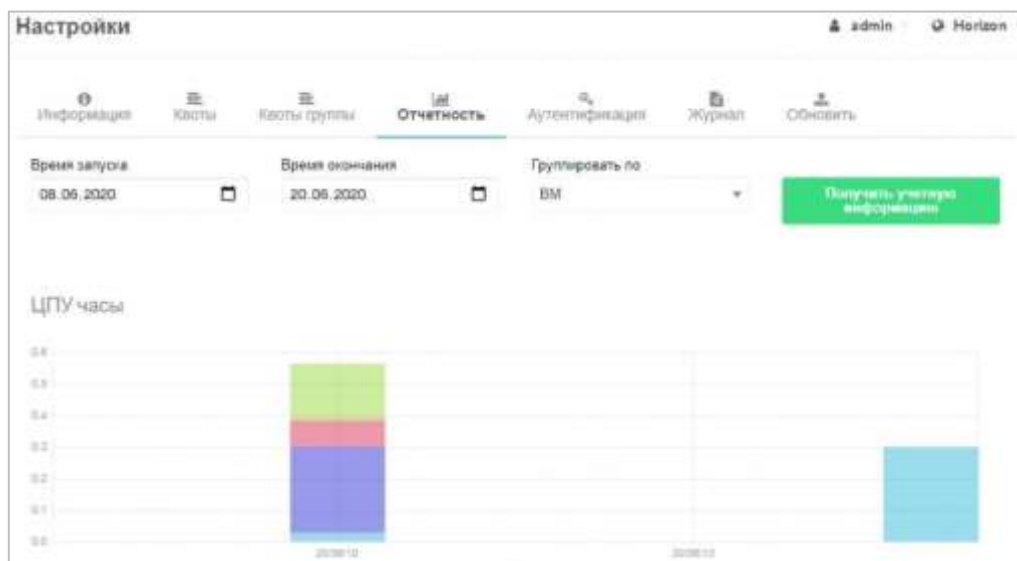


Рисунок 134 - Получение статистической информации об использовании ресурсов системы

7. Ввести промежуток времени для получения отчета.
8. В поле **Группировать по** выбрать параметр, по которому необходимо вывести статистику: ВМ, пользователь, группа (Рисунок 135).

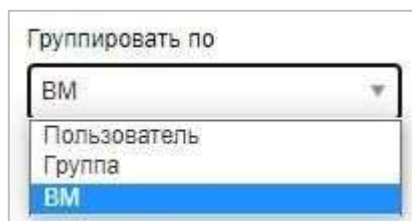


Рисунок 135 - Получение статистической информации об использовании ресурсов системы

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).

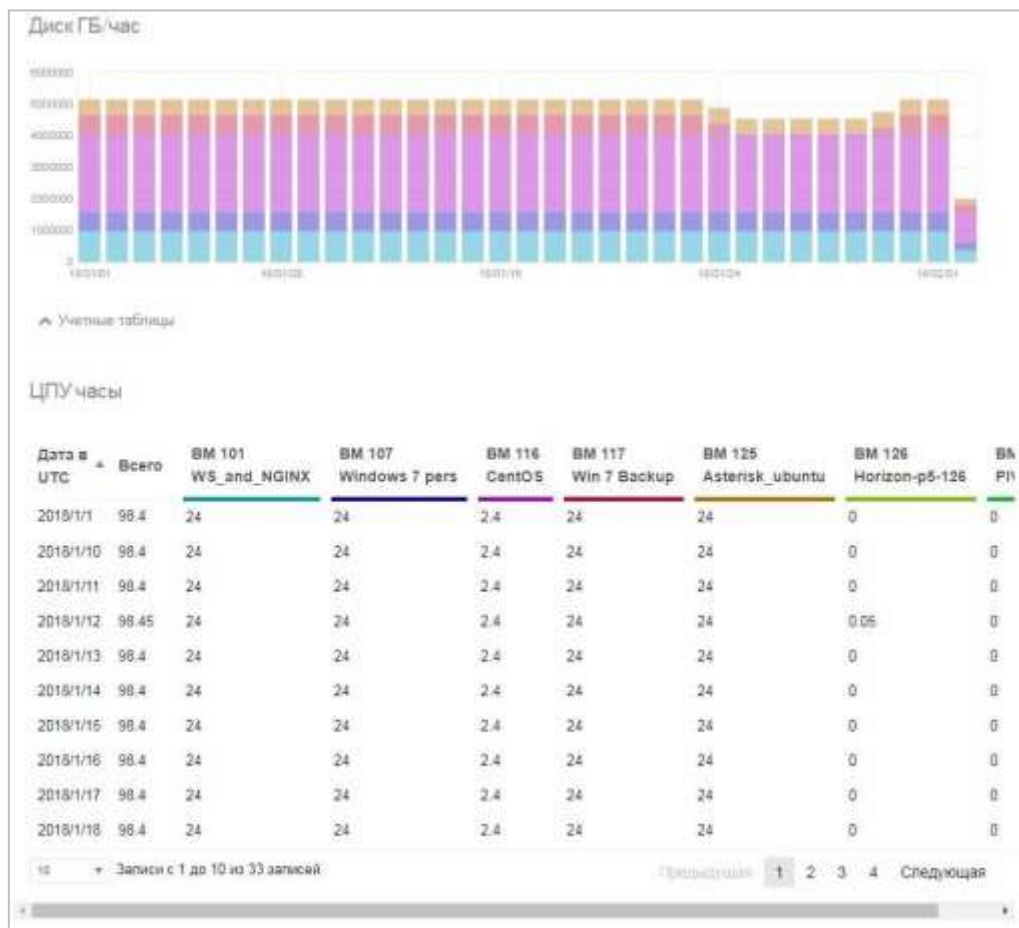


Рисунок 136 – Статистика использования ресурсов виртуальных машин

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).

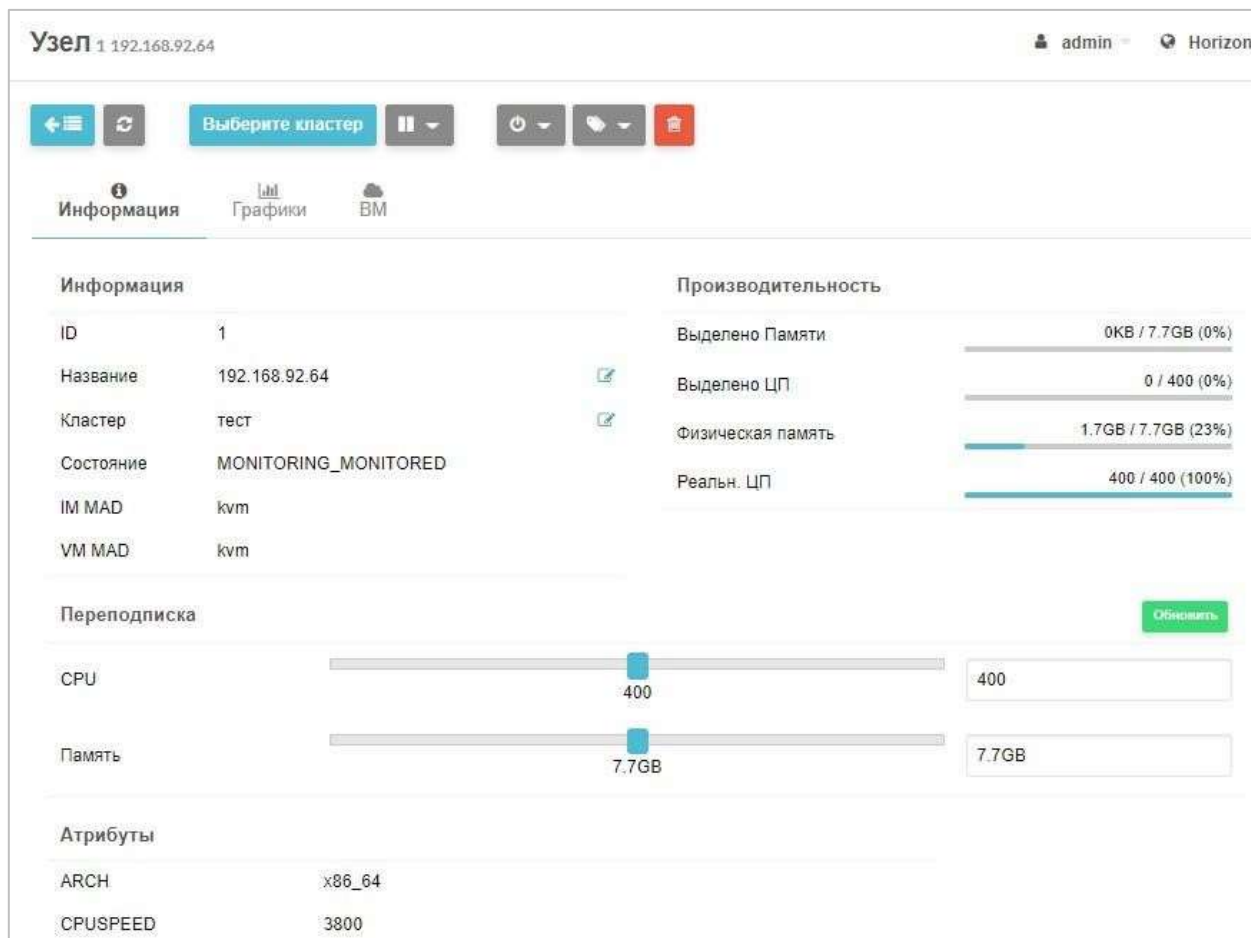


Рисунок 137 - Окно информации о выбранном узле (сервере)

12. Перейти на вкладку **Графики**.

Отобразится информация об использовании ресурсов процессора и памяти ВМ, на которой установлен сервер (Рисунок 138).

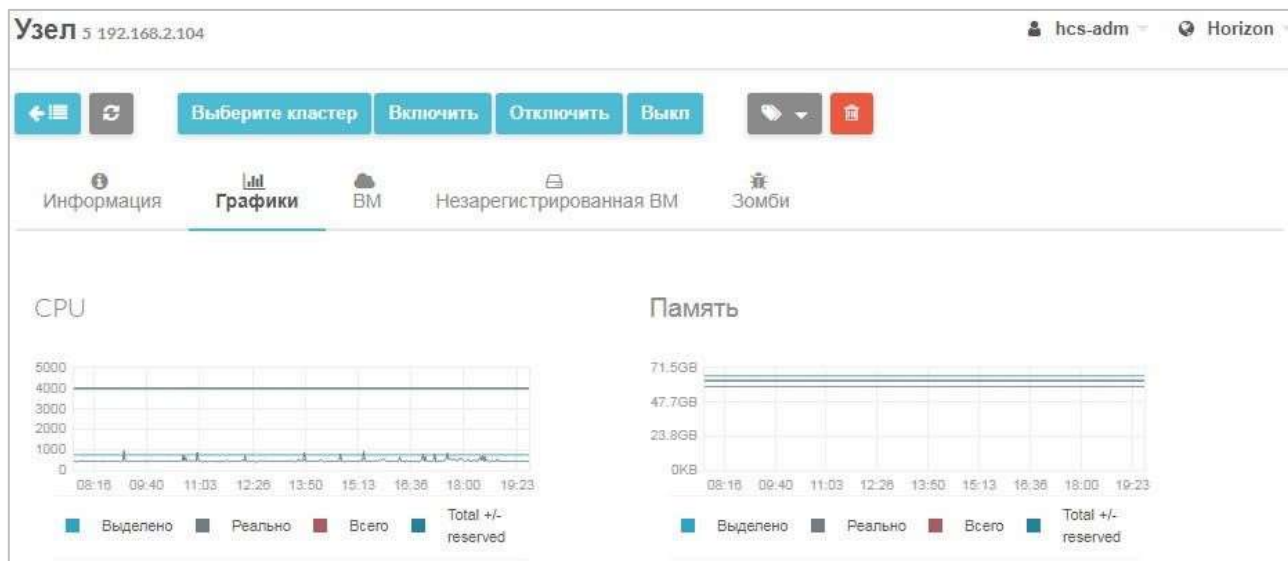


Рисунок 138 - Графики

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 (Рисунок 139).

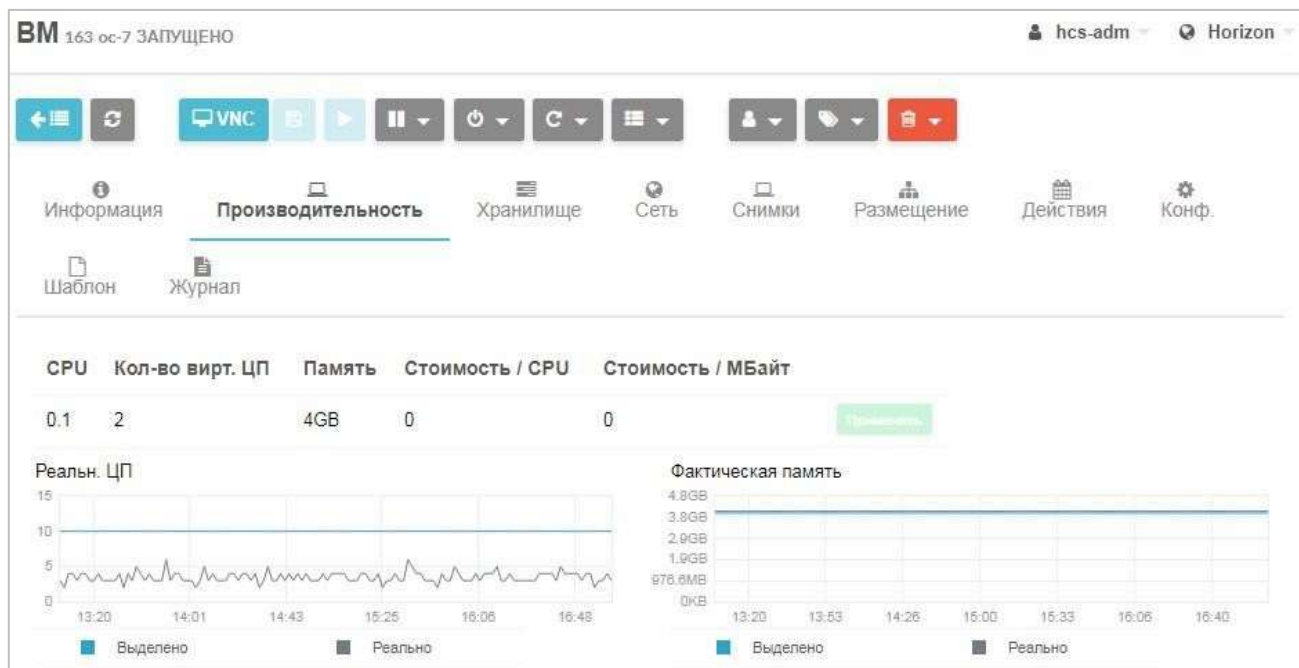


Рисунок 139 - Производительность ВМ

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.

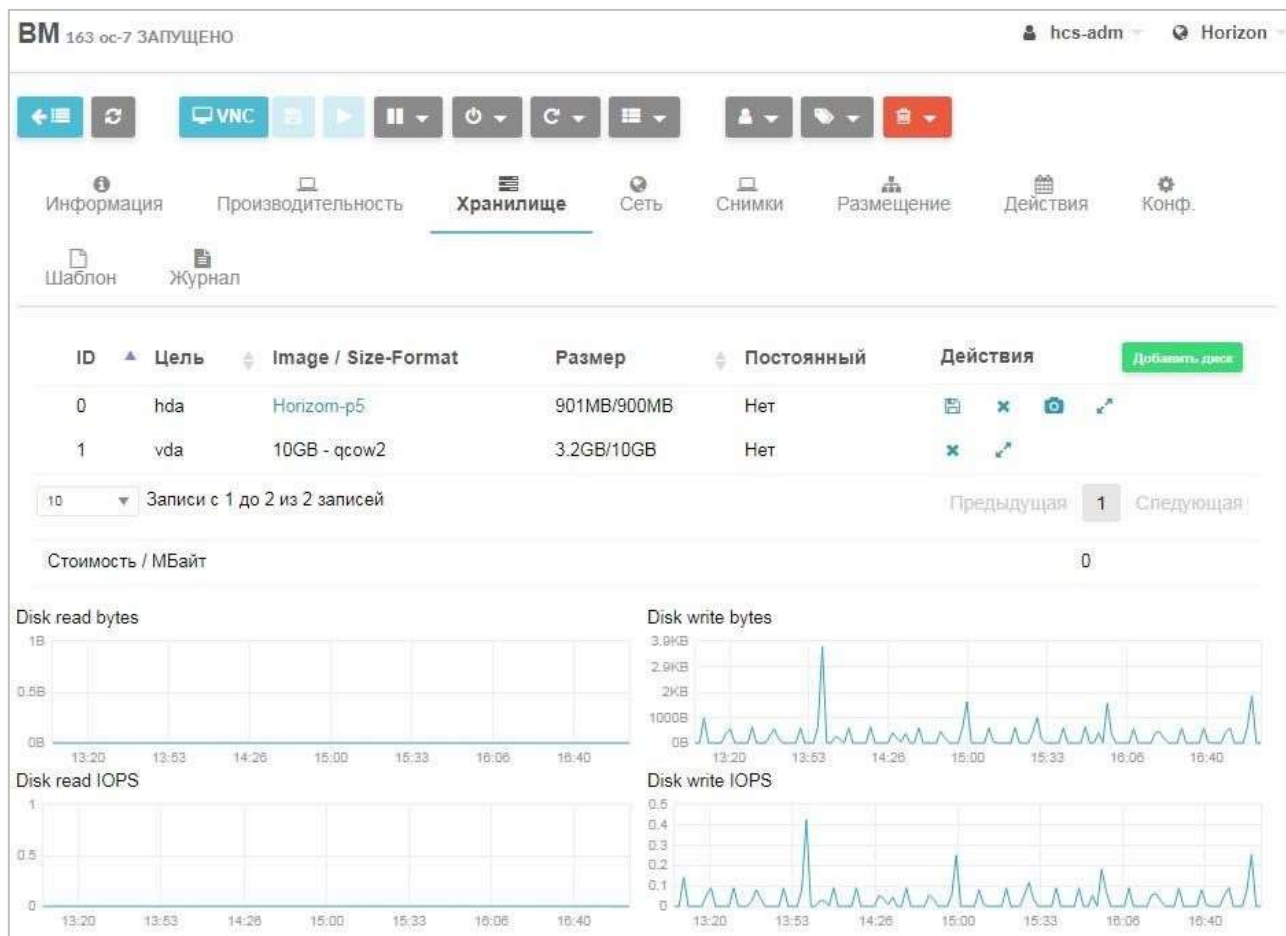


Рисунок 140 - Отчетная информация о хранилищах VM

17. Для просмотра информации о виртуальных сетях той же VM перейти на вкладку **Сеть** (Рисунок 141).

Отобразится информация о виртуальных сетях, к которым подключенна данная VM, и ниже – статистика их использования в виде графика.

Для отключения VM от сети нажать кнопку .

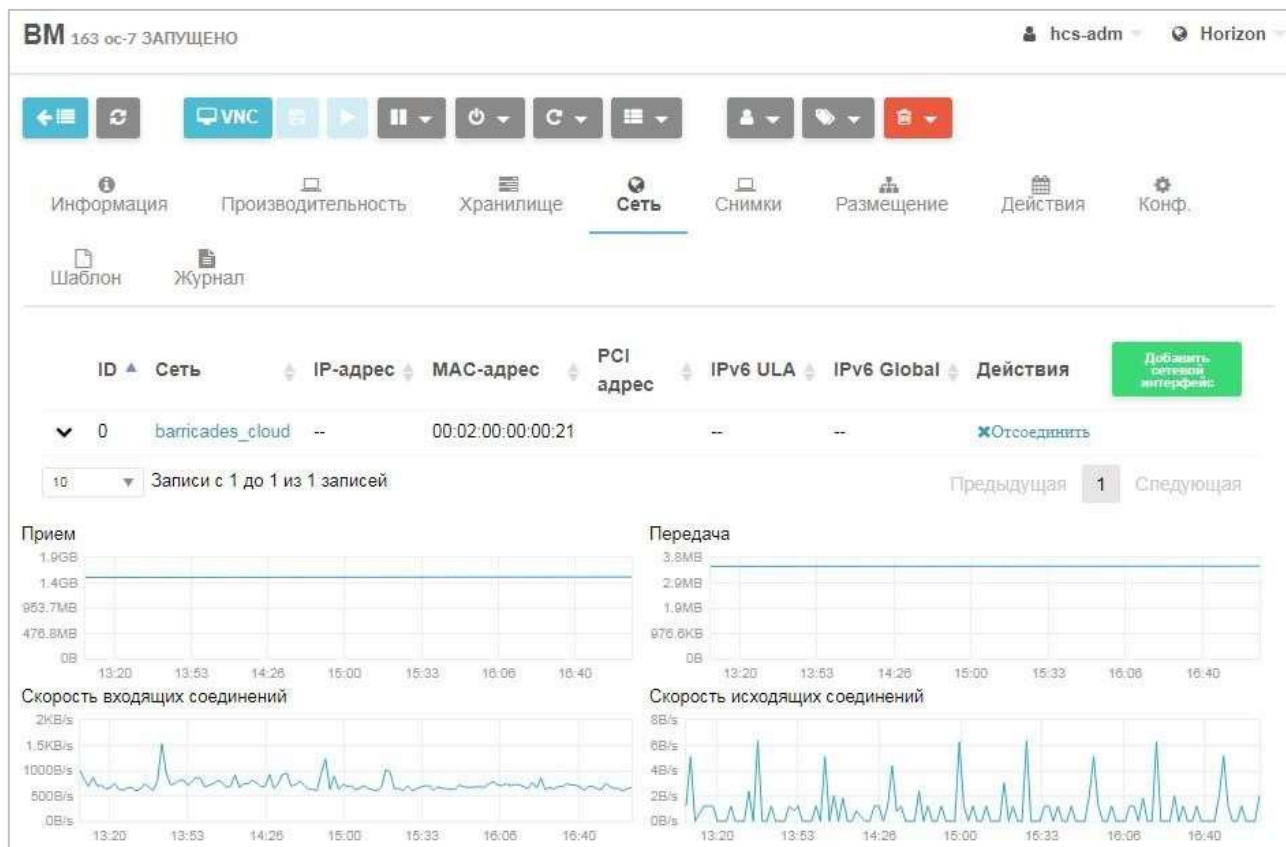


Рисунок 141 - Отчетная информация о сетях, к которым подключена ВМ

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:

- е. 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 производится 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:

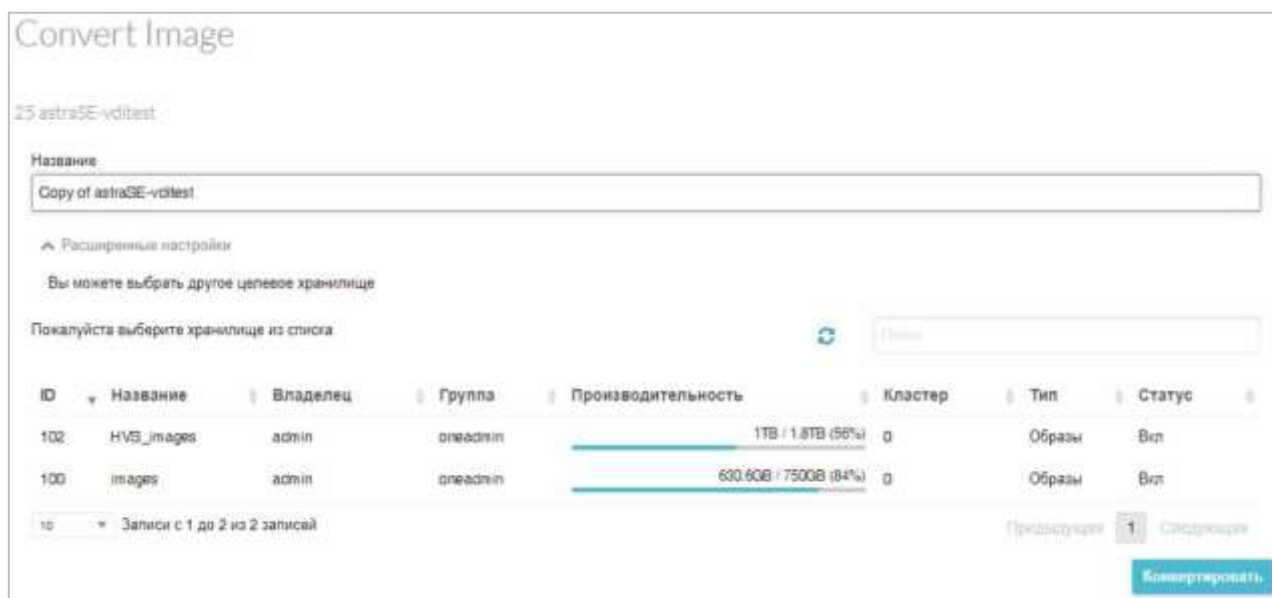
6. Загрузить в СГУ образ диска для конвертации.

Для загрузки образа диска:

н. Перейти в раздел **Хранилище** → **Образы ВМ**.

о. Нажать кнопку .

).



ID	Название	Владелец	Группа	Производительность	Кластер	Тип	Статус
102	HVS_images	admin	oneadmin	1TB / 1.8TB (56%)	0	Образы	Вкл
100	images	admin	oneadmin	630.6GB / 750GB (84%)	0	Образы	Вкл

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 access) и механизмы оптимизации использования оперативной памяти. Для этого 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.

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 hvsw5
```

где *hvsw5* – имя моста; *eth7*

– порт;

в. добавить физический порт в мост командой:

```
ovs-vsctl  
add-port hvsw5 eth7
```

где *hvsw5* – 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).

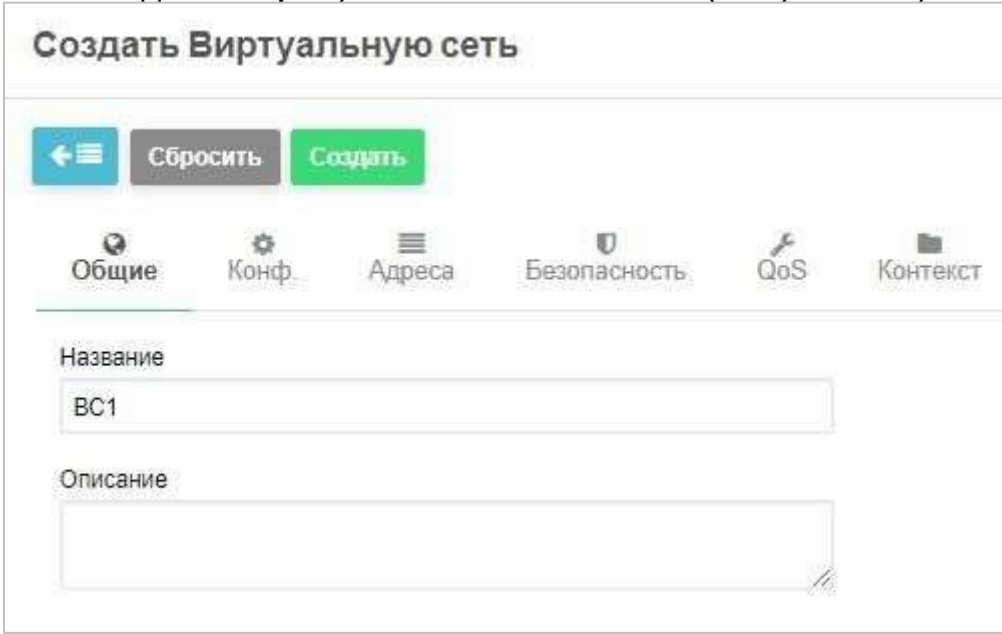


Рисунок 143 - Создание виртуальной сети. Вкладка «Общие»

- 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**;

Создать Виртуальную сеть

← Сбросить Создать

Общие Конф. Адреса Безопасность QoS Контекст

Интерфейс сет. моста
hvsw5

Режим работы сети
Open vSwitch

☐ MAC spoofing filter
☐ IP spoofing filter

VLAN ID
No VLAN network

Рисунок 144 - Создание виртуальной сети. Вкладка «Конф.»

г. На вкладке **Адреса** выбрать Ethernet и в поле Первый 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).

Создать Виртуальную сеть admin1 Horizon

← Сбросить Создать Мастер настройки

Общие Конф. Адреса Безопасность QoS Контекст

Диапазон адресов +

☐ IPv4 ☐ IPv4/6 ☐ IPv6 ☒ Ethernet

Первый MAC-адрес
12:34:56:78:90:12

Размер

▼ Расширенные настройки

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 VM.

а. В разделе **ВМ** → **Машины** выбрать VM двойным нажатием.

б. Перейти на вкладку **Сеть**.

в. Нажать кнопку **Добавить сетевой интерфейс** (Рисунок 146).

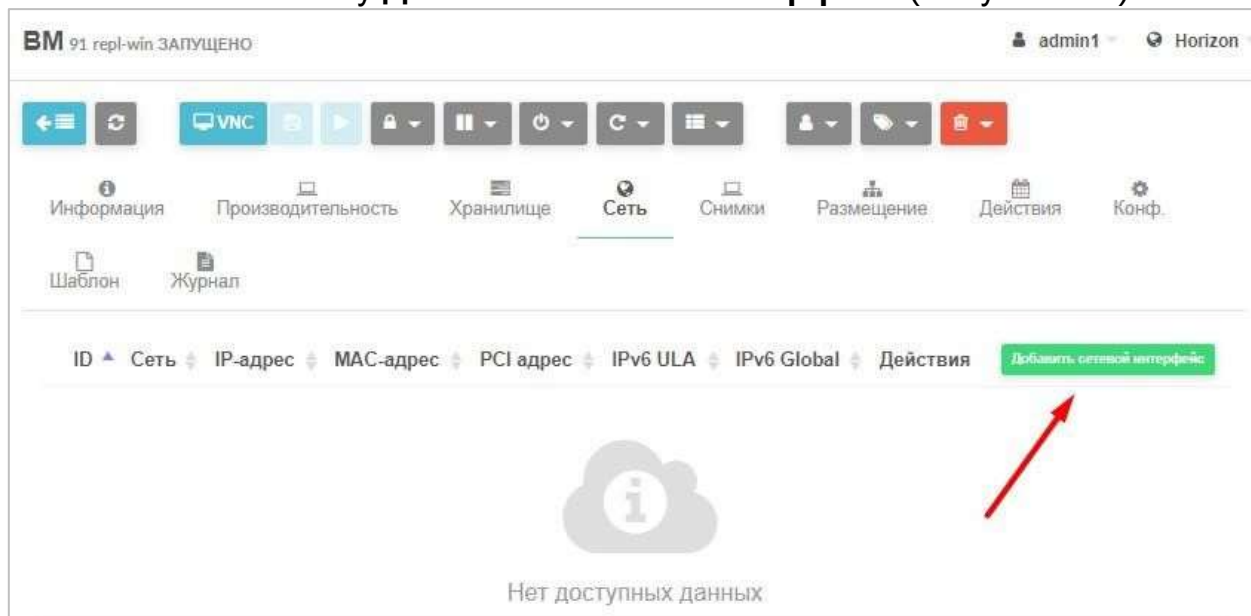


Рисунок 146 - ВМ. Вкладка «Сети»

Откроется список доступных сетей (Рисунок 147).

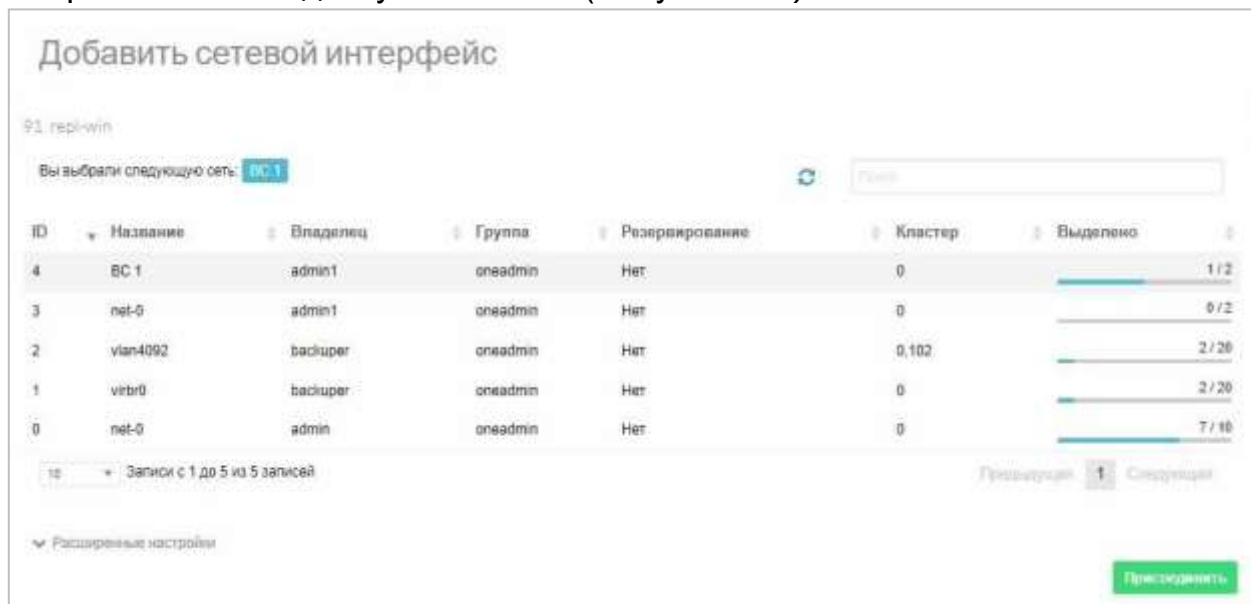


Рисунок 147 - Добавление сети в конфигурацию ВМ

г. Выбрать созданную сеть (в данном примере – ВС 1) и нажать кнопку **Присоединить**.

Добавленная сеть отобразится в списке (Рисунок 148).

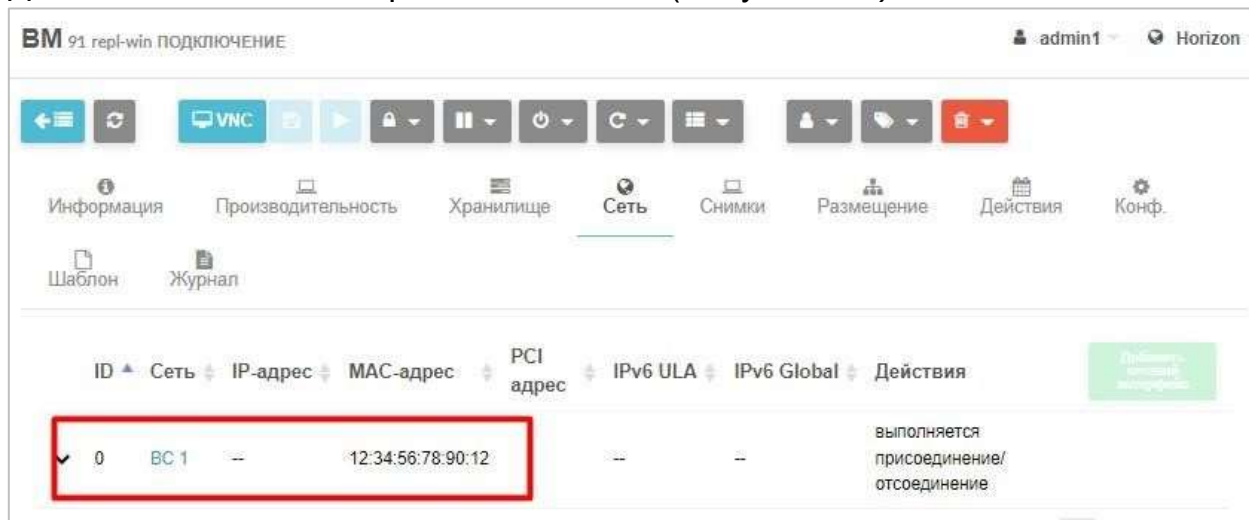


Рисунок 148 - Сеть добавлена в конфигурацию VM

5. Подключить виртуальную сеть с назначенным VLAN ко второй VM по аналогии с шагом 4.

Для проверки моста между двумя VM выполнить команду:

```
ovs-vsctl show
```

При наличии моста на экране отобразятся результаты, как на рисунке ниже (Рисунок 149)

```
h109 ~ # ovs-vsctl show
f58d8ebd-a9c1-4563-a25b-3c95edefabca
Bridge hvsw5
  Port one-67-1
    tag: 6
    Interface one-67-1
  Port hvsw5
    Interface hvsw5
      type: internal
  Port one-91-0
    tag: 6
    Interface one-91-0
```

Рисунок 149 - Мост между двумя VM создан

Для проверки соединения между VM1 и VM2:

1. Подключиться VM1, нажав кнопку  или  в зависимости от настроек подключения к VM (Рисунок 148).
2. В командной строке выполнить команду:

```
ping IP-адрес VM2
```

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 VM.

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 VM;

<count> – количество добавляемых ядер.

Примечание. Количество добавляемых ядер не должно превышать лимит, установленный при создании шаблона VM 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 VM 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**.

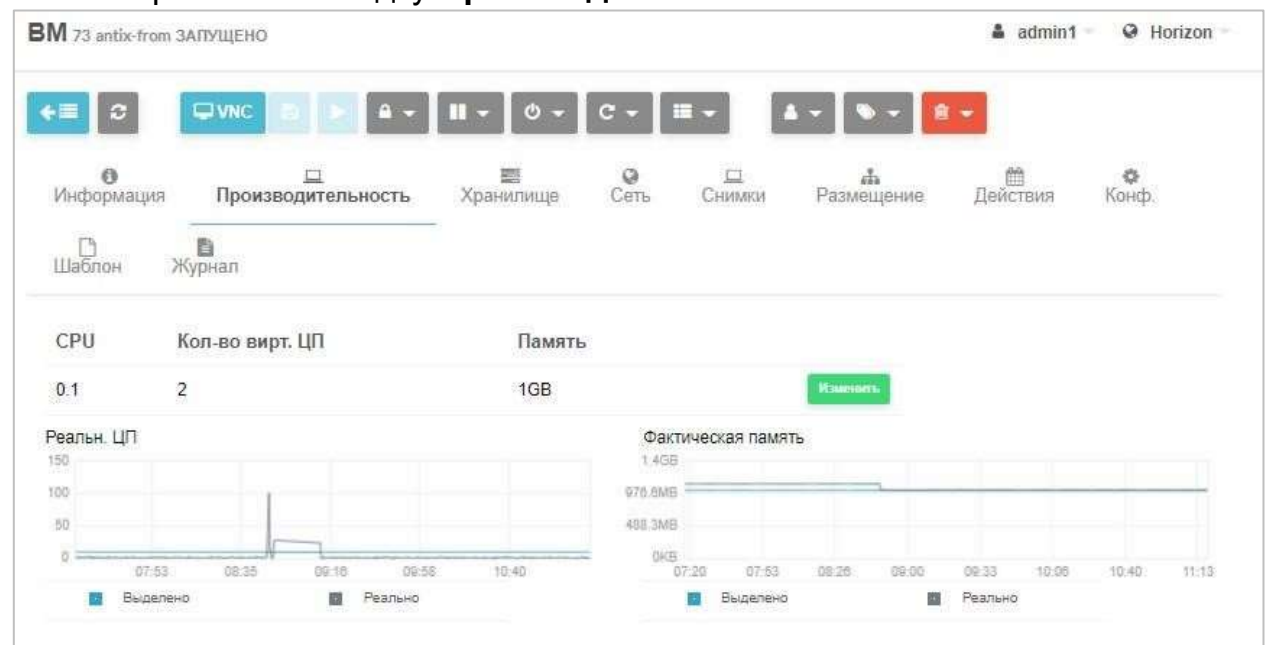


Рисунок 150 - Параметры производительности ВМ

3. Нажать кнопку **Изменить** (Рисунок 150).

Откроется окно «Базовые характеристики» (Рисунок 151).

4. Изменить значения полей и нажать кнопку **Изменить**.

Изменить базовые характеристики

91 repl-win

☐ Проверка

Память

4 ГБ

CPU

0,1

Кол-во вирт. ЦП

2

Сокеты

2

Ядра

1

Потоки

1

Изменить

Рисунок 151 - Изменение параметров производительности VM
VM Для добавления дисков:

1. В разделе **Машины** → **VM** выбрать VM нажатием.
- Откроется окно информации о VM.
2. Перейти на вкладку **Хранилище**.
3. Нажать кнопку **Добавить диск** (Рисунок 152).



Рисунок 152 - Список хранилищ, подключенных к MB

Откроется окно со списком доступных дисков (Рисунок 153).

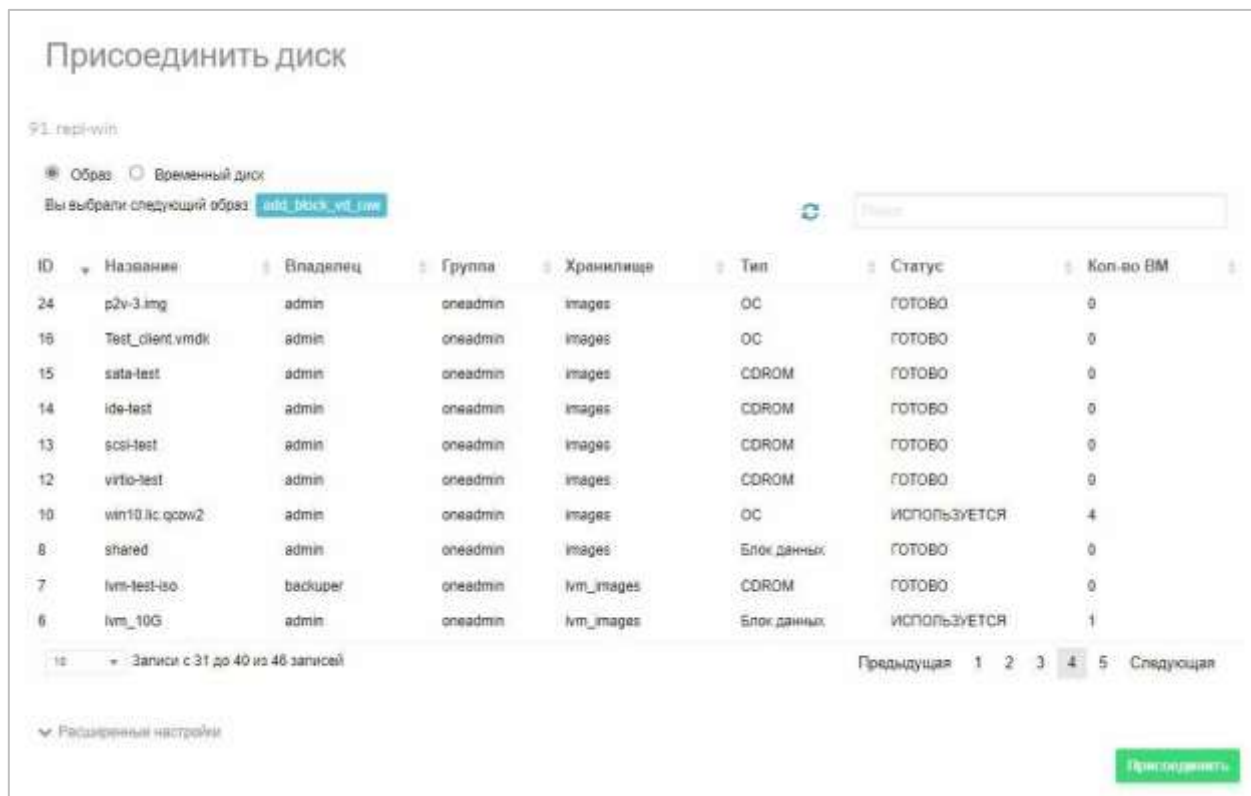


Рисунок 153 - Добавление диска к VM

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 «Звезда» 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).

Кластеры ВД

admin

Горизонт

Создать кластер ВД

ID	Владелец	Группа	Название	Статус	Узел	В кластере
9	admin	oneadmin	TEST	POWEROFF	192.168.2.114	
8	admin	oneadmin	Server-2	POWEROFF	192.168.2.114	
7	admin	oneadmin	Server-1	POWEROFF	192.168.2.114	
6	admin	oneadmin	Server-0	POWEROFF	192.168.2.114	
5	admin	oneadmin	Fedora-2	POWEROFF	192.168.2.114	

Рисунок 154 - Кластеры НА

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).

Настроить кластер ВД

ВМ 6 Server-0 в настоящее время запущено на Узле 192.168.2.114

Выбрать узел

Хосты в кластере ВД: 192.168.2.114 192.168.2.115

ID	Название	Кластер	Кол-во ВМ	Выделено ЦП	Выделено Памяти	Статус
2	192.168.2.116	По умолчанию	0	0 / 0	0KB / -	ВЫКЛ
1	192.168.2.115	По умолчанию	0	0 / 0	0KB / -	ВЫКЛ
0	192.168.2.114	По умолчанию	10	910 / 4000 (23%)	36.5GB / 503.7GB (7%)	Вкл

10 Записи с 1 до 3 из 3 записей

Hosts that won't be included in HA Cluster

1 Предыдущая Следующая

Setup

Рисунок 155 - Конфигурирование кластера ВД

После окончания конфигурирования кластера в списке ВМ (**Рисунок 155**) 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).

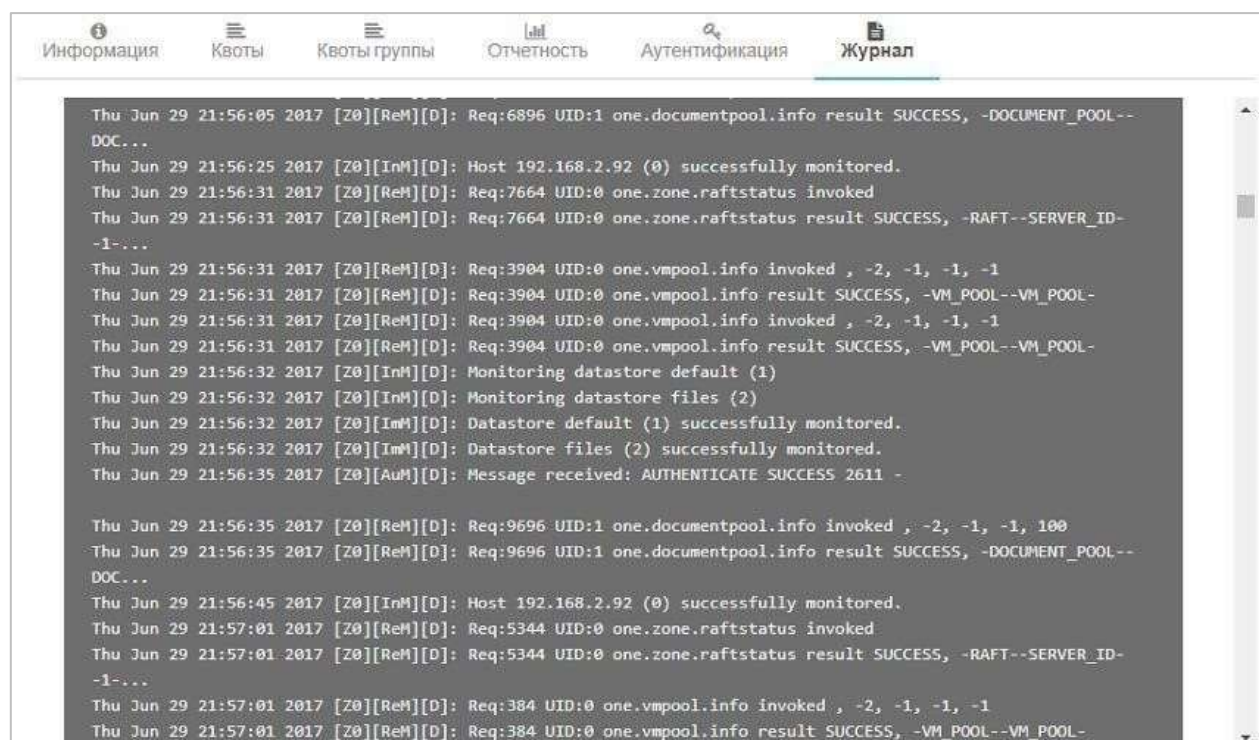


Рисунок 156 - Общесистемный журнал событий

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 VM	reason=saved vm=<имя_VM>
Клонирование VM	vm=<имя_VM>-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 VM	VM <ID_VM>	ID VM, соответствующий отображаемому в списке VM в СГУ
terminate	сведения об удалении VM	UID:<ID_VM> USER:<имя пользователя>	
one.vm.action	сведения о запросах на доступ к VM	UID:<имя пользователя запустившего VM>	
chown	сведения об изменении правил разграничения доступа пользователей к VM		

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 VM.

- сети, чтобы ограничить количество IP-адресов, которые пользователь / группа может получить из данной сети.

- образов, для ограничения количества экземпляров VM от определенного пользователя / группы, использующих данный образ. Можно

воспользоваться этой квотой, если образ содержит расходные ресурсы (например, лицензии на ПО).

Примечание: при использовании хранилища Serp 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).

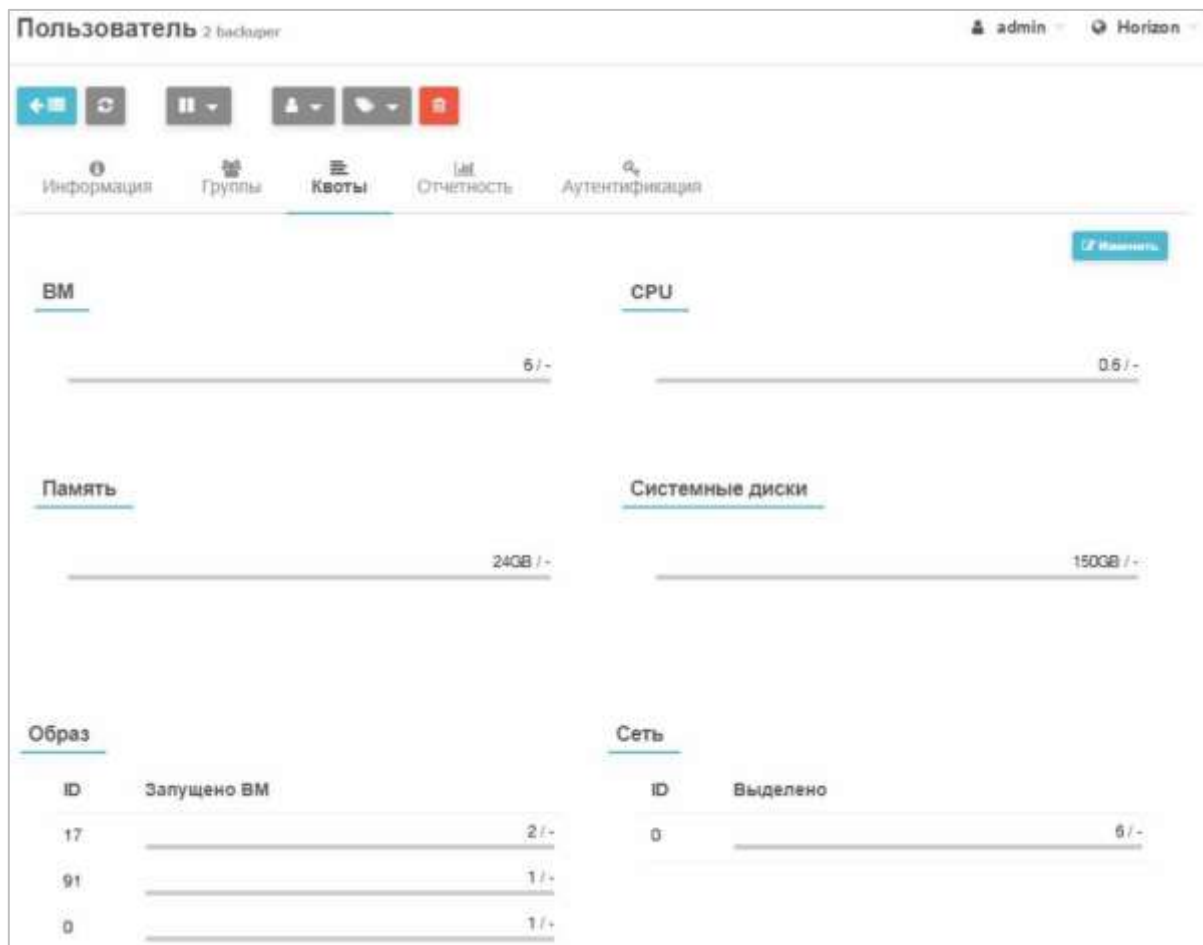


Рисунок 157 - Управление квотами

4. Нажать кнопку **Изменить** в правом верхнем углу.

Станут доступны параметры для редактирования (Рисунок 158).

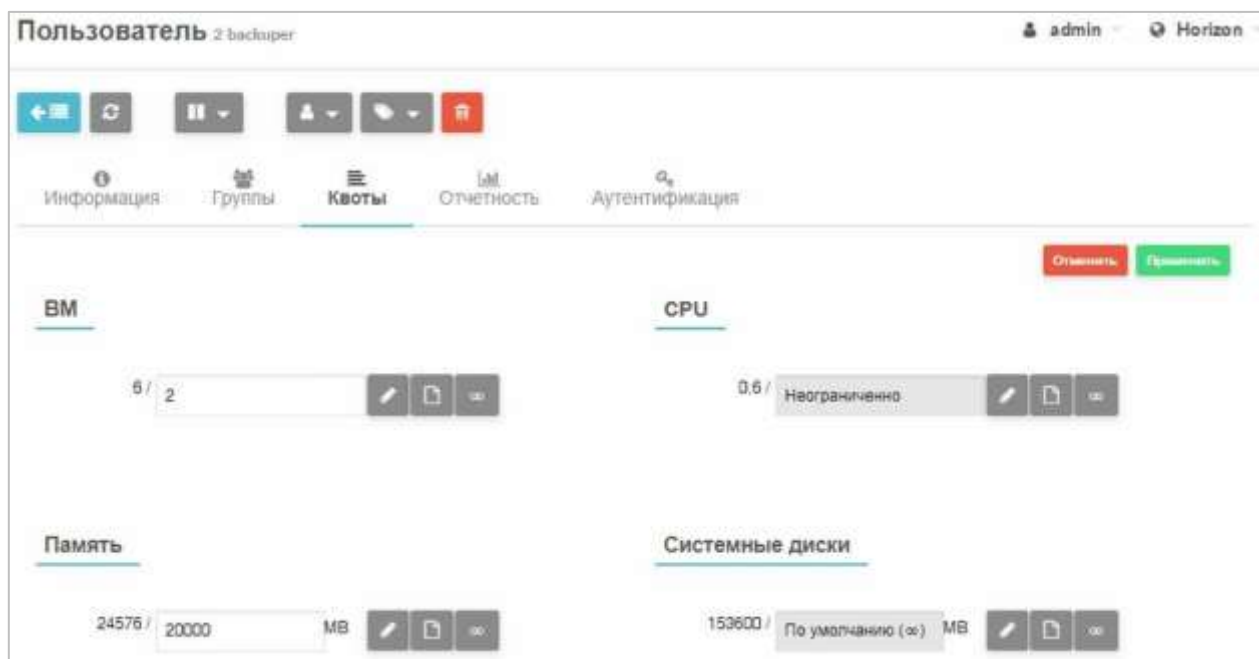


Рисунок 158 - Редактирование квот

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_RESCHEDULE	Выполнять миграцию при перенастройке виртуальной машины	1 – «горячая» миграция ВМ; 0 – «холодная» миграция ВМ
DEFAULT_SCHEDULE	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 «Звезда» (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 «Звезда». 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 «Звезда».

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
Звезда
// по умолчанию = Звезда app_name=Звезда
//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 Звездаа (кластера)
gorizont_host=192.168.2.4
//Пользователь ssh По умолчанию - oneadmin
sshuser=oneadmin //максимальное время выполнения 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 - backupper
onerpcuser=backupper
// - таймаут (сек) 5..60, по умолчанию -5 onetimeout=10
// - порт, по умолчанию - 2634
onerport=2634
// - использование https для взаимодействие с СГУ?
// Использовать https для взаимодействие с СГУ, по
умолчанию =no и
// onerport 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 использования 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 Звезда):

```
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).

Конфигурационный файл

Название модуля

Выводить ли отладочные сообщения в log?

Количество дней хранения файлов-резервов

Настройка веб интерфейса бэкапа - порт

- маска подсети

Интервал запуска планировщика копирования, сек

Хост Горизонта (для взаимодействия по ssh)

Пользователь ssh

Взаимодействие с opennebula по xmb пре - хост

- порт

- URL

- пользователь

- таймаут (сек)

- использование https?

взаимодействие с агентами копирования - порт

- таймаут (сек)

Максимальное время сохранения СГУ (сек)

время на остановку VM (сек)

размер снимка IVM в Mb или %

СГУ идентификатор serh

процент использования процессоров backup при восстановлении VM

доступные языки

текущий язык

Сохранить конфигурацию

И обязательно выйти

/usr/local/backup/backup.conf

Порт веб-ФС

Нет

30

2033

0.0.0.0

60

192.168.2.4

oneadmin

192.168.2.4

2033

/RPC2

backupet

10

Нет

9000

5

100

60

5%

libvirt

30

en,ru

ru

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).

Горизонт-ВС

Резервное
копирование
[192.168.2.110]

Имя пользователя СГУ

Пароль

Войти

Версия 2.6.22-э
СГУ "Горизонт"
ИЦ "Баррикады"

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 ().

3.3.4 Общие настройки резервного копирования

Данные настройки СРК сохраняются для всех компонент резервного копирования и состоят из следующих полей ().

Горизонт-ВС

Резервное копирование [192.168.2.110]

Общие настройки

Копирование ВМ ▾

Восстановление ВМ

Загрузка ВМ

Репликация ВМ ▾

Сохранение СГУ

Log-файлы

Назад

Версия 2.6.22-я

СГУ "Горизонт"

ИЦ "Баррикады"

Общие настройки резервного копирования

Сохранить

Тайм-аут ожидания копирования ВМ (мин)

30

Количество копий ВМ по умолчанию

1

Хранилище резервных копий по умолчанию (fs,nfs)

nfs ▾

Количество повторов при ошибке

3

Время ожидания между повторами (мин)

5

Время, отводимое на остановку ВМ (сек)

720

Использовать программу сжатия

lbzip2 ▾

Процент использования CPU при сжатии

25

Степень сжатия (1=min)

2

Файлы журналов отправлять по почте?

☐

Почтовый сервер для отправки файлов журналов

Номер порта

Адрес(а) получателя

Адрес отправителя

Пароль отправителя

Использовать TLS

Нет ▾

Число секунд, отводимое на отправку

5

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

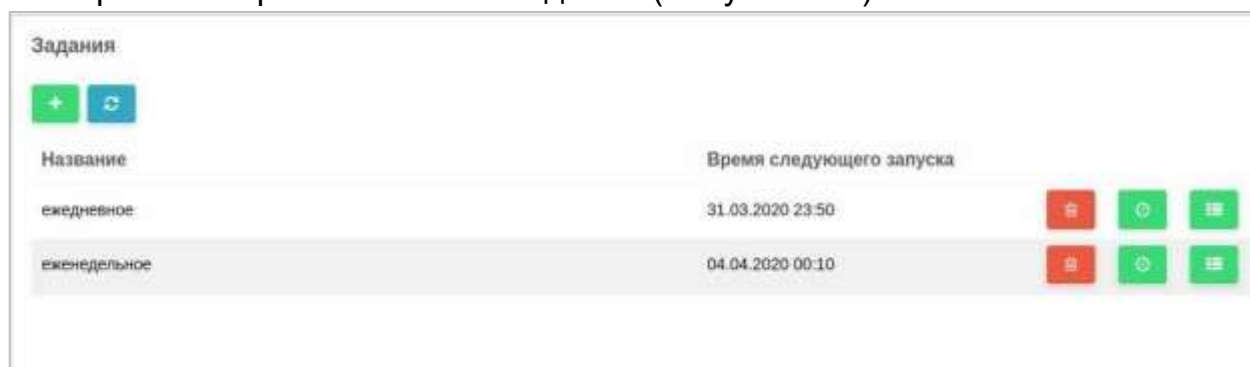
Данный раздел позволяет пользователю выполнять следующие функции:

- просматривать список заданий на копирование ВМ;
- создавать задания на копирование ВМ;
- просматривать состояния компонентов копирования на всех узлах гипервизора «Звезда» 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).



Задания	Название	Время следующего запуска	
	ежедневное	31.03.2020 23:50	  
	еженедельное	04.04.2020 00:10	  

Рисунок 162 - Список заданий на копирование

Администратор может задать произвольное число заданий на резервное копирование.

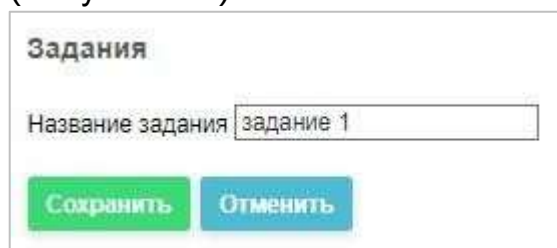
3.3.5.1.1 Создание задания

Для создания задания:

1. Нажать кнопку  в верхнем левом углу (Рисунок 162).
2. В открывшемся окне указать название задания и нажать кнопку



(Рисунок 163).



Задания

Название задания

Рисунок 163 – Название задания

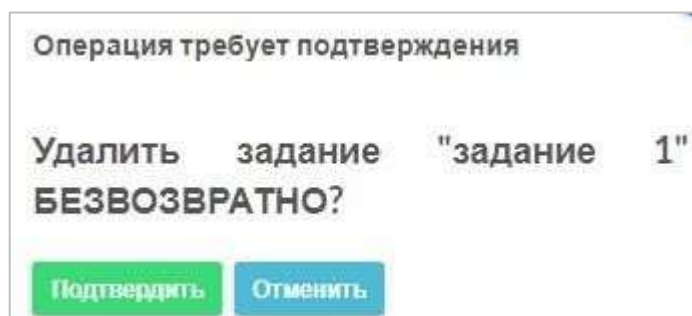
Задание будет добавлено в список.

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 VM

Для удаления задания нажать кнопку  и подтвердить действие в открывшемся окне (Рисунок 164).



Операция требует подтверждения

Удалить задание "задание 1"
БЕЗВОЗВРАТНО?

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).

Расписание резервного копирования

задание : задание 1

Назад Сохранить

☒ отключено

☐ ежедневно

☐ еженедельно

☐ ежемесячно

☐ периодически

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).

Расписание резервного копирования

Задание: ежедневное

Назад Сохранить

☐ отключено ☒ ежедневно ☐ еженедельно ☐ ежемесячно ☐ периодически

В 23:50

каждый день

Следующее копирование в 31.03.2020 23:50

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**).

Список сохраняемых ВМ

Задание: ежедневное

Назад + - В

☐	ID	Виртуальная машина	Таймаут	Хранилище	Тип копии	Копий	стоп ВМ	Приоритет	Диски
☐	0	win10	30		полный	2	с ост.	99	

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 VM из списка нажатием.
 4. Задать параметры копирования (Рисунок 168):
 - **приоритет при копировании** - задает последовательность копирования VM в рамках задания. Пока не завершено копирование одной VM, копирование следующей не запускается; **тип сохранения** – («полное» или «пропускается»); **тайм-аут ожидания копирования VM**
 - (мин) — см. п. 3.3.4; количество копий VM — см. п. 3.3.4; хранилище резервных копий — см. п. 3.3.4;
 - Время, отводимое на остановке VM (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 VM (выбираются из списка подключенных к VM дисков);
- порядок управления VM при копировании** (Рисунок 169).

Рисунок 168 -

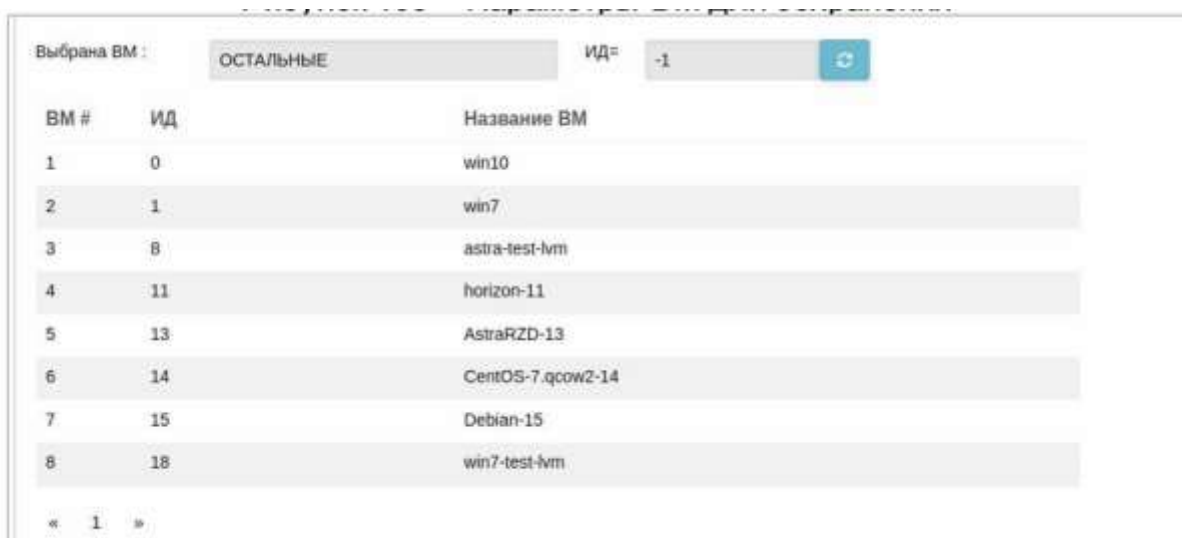


Рисунок 169 – Порядок управления VM при копировании

Порядок управления при копировании выбирается из выпадающего меню и может быть одним из следующих типов:

- без остановки (требуется qemu-guest-agent в VM — см. ниже).

Модуль копирования делает снимок (snapshot) дисков VM.

Целостность дисков обеспечивается при наличии установленного в VM специального агента. Виртуальная машина в этом режиме остается доступной все время, хотя и возможна потеря производительности. Существует ограничение – тип дисков VM

только qcow», тип хранилищ – LVM, rbd ceph;

- с остановкой. В данном случае модуль дает VM команду на завершение работы (если она работает) и после делает копию дисков. VM должна быть настроена так, чтобы запустить надлежащий механизм остановки работы при подаче сигнала завершения работы (ACPI) — см. ниже. После копирования модуль запустит VM, если она работала. Виртуальная машина в этом режиме будет недоступной все время копирования дисков;

- паузой и записью снимка памяти. В данном случае, если VM работает, делает снимок дисков и памяти VM, а затем восстанавливает виртуальную машину. Виртуальная машина в этом режиме будет недоступной только во время копирования памяти на диск. Вместо имени VM

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).

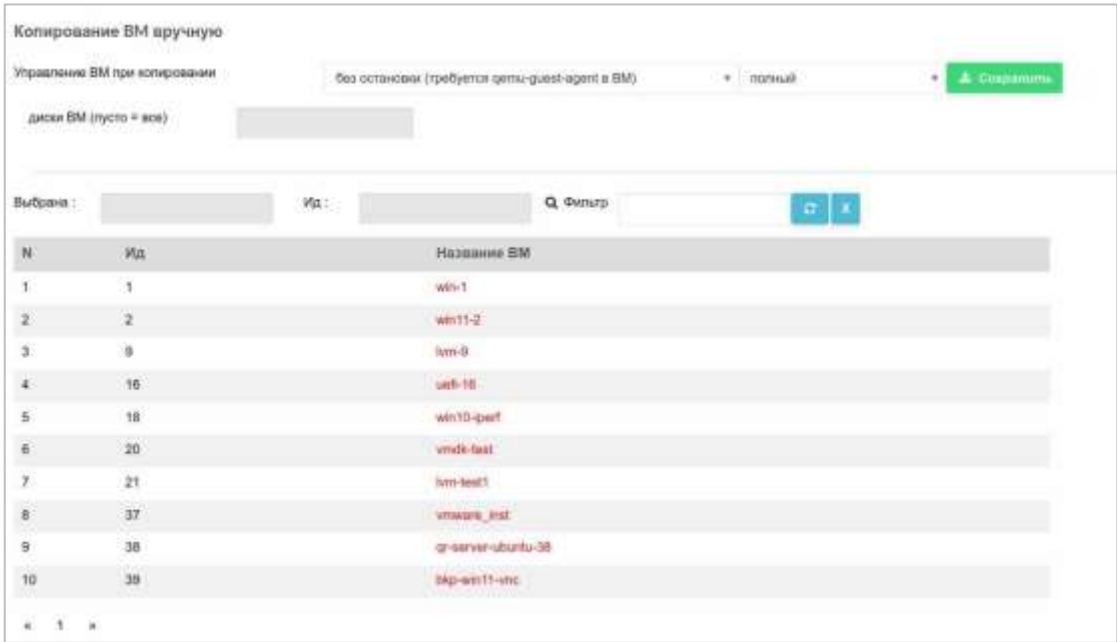


Рисунок 170 - Копирование ВМ вручную

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 **Звезда** и список выполняющихся заданий по сохранению ВМ (Рисунок 171).

Состояние процессов сохранения



Узел	Дата и время	Состояние агента
192.168.2.110	06.10.2022 14:45:55	ready

Выполняющиеся задания



Ид	ВМ	Коп.	Стадия	Узел	начато	Процент вып.
0	ubuntu	без ост.				

Рисунок 171 - Состояние выполнения заданий

Для удаления очереди копирования ВМ:

1. Нажать кнопку  справа от строки узла в секции **Узел**.

Подтвердить операцию в открывшемся диалоговом окне (Рисунок 172).

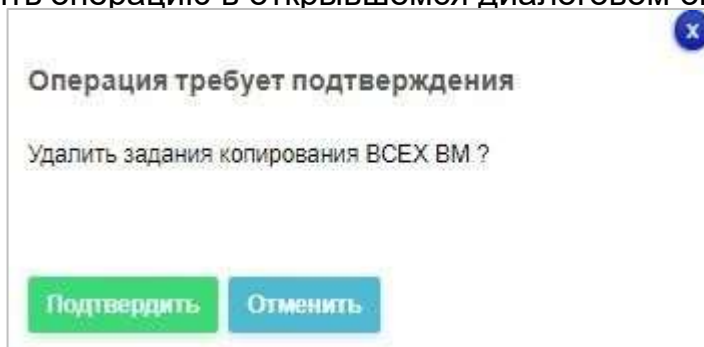


Рисунок 172 - Подтверждение удаления очереди копирования ВМ

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).

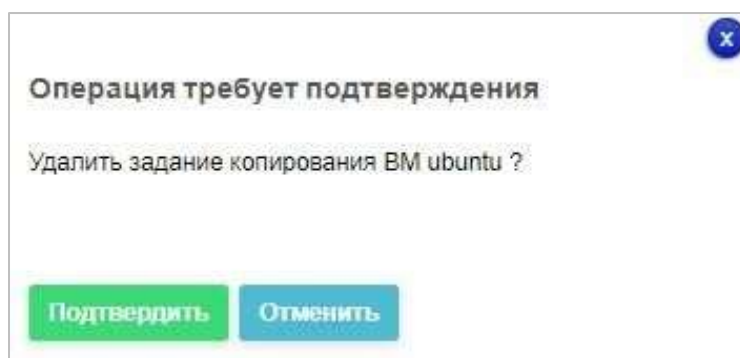


Рисунок 173 - Подтверждение удаления задания

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).

Выполняющиеся задания						
Задание уже запущено, невозможно удалить						
Ид	ВМ	Коп.	Стадия	Узел	начато	Процент вып.
5	hor-5	без ост.				

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.

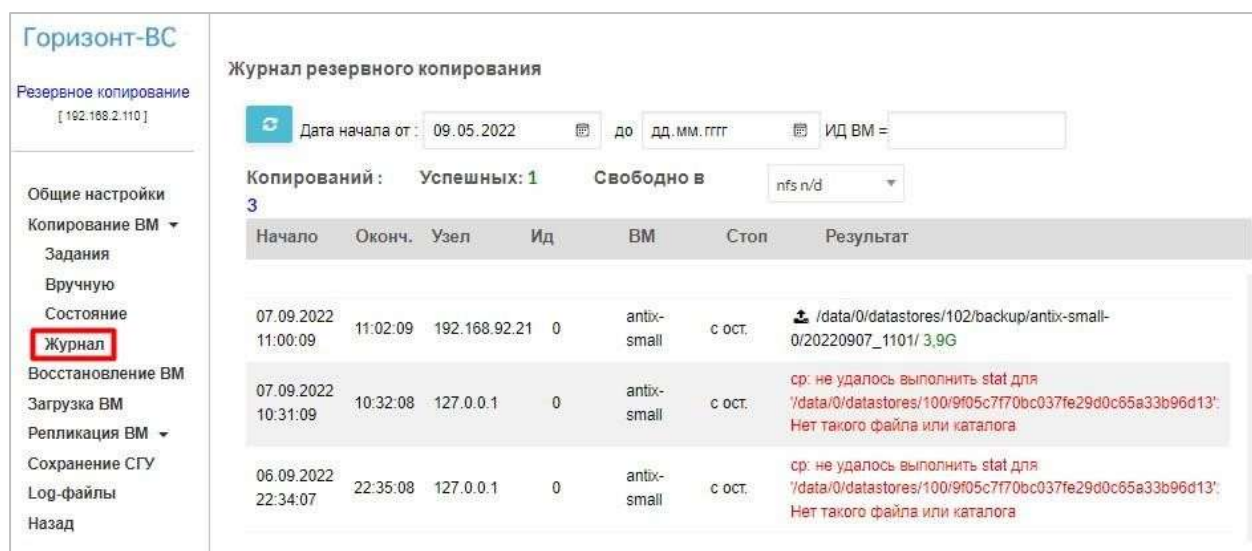


Рисунок 175 - Задания резервного копирования

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).

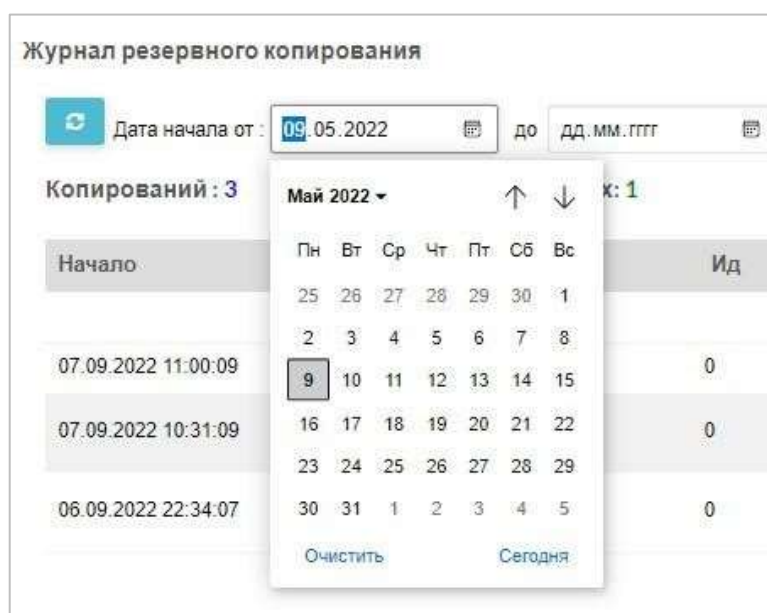


Рисунок 176 - Установка интервала, за который выводятся задания

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 этим заданием.

3.3.6 Состав папки резервной копии виртуальной машины Папка с резервными копиями содержит следующие файлы:

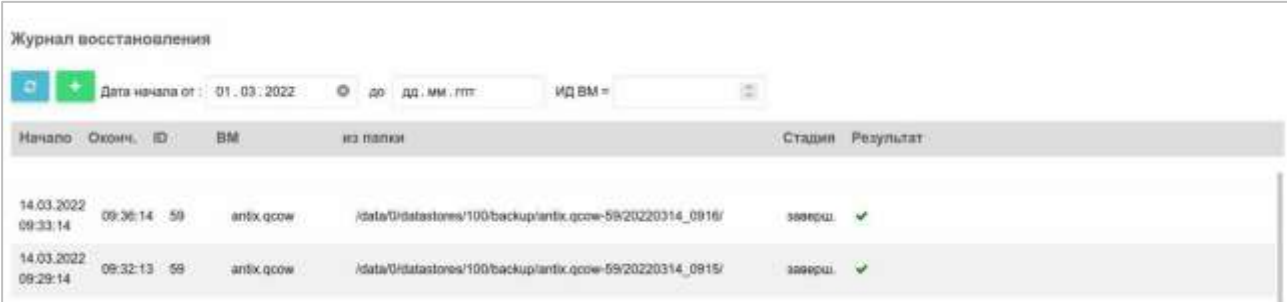
- файл(ы) дисков VM — **disks.#, *.img** – xml файл описания VM, полученный из СГУ «Звезда», - **one.xml**.

Если виртуальная машина была запущена после копирования, то дополнительно сохраняется xml файл описания VM, полученный средствами libvirt - **libvirt.xml**.

При сохранении VM 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 VM** отображается список VM, для которых были созданы резервные копии (Рисунок 177). Возможна фильтрация информации по диапазону дат и по ИД виртуальной машины.



Начало	Оконч.	ID	VM	из папки	Стадия	Результат
14.03.2022 09:33:14	09:36:14	59	antix.qcow	/data/01/datastores/100/backup/antix.qcow-59/20220314_0916/	заверш.	✓
14.03.2022 09:29:14	09:32:13	59	antix.qcow	/data/01/datastores/100/backup/antix.qcow-59/20220314_0915/	заверш.	✓

Рисунок 177 - Восстановление VM

Для восстановления VM из резервной копии следует выбрать VM и нажать кнопку **Показать список копий**.

Для выбранной VM появится список копий (Рисунок 178), из которого

необходимо выбрать нужную и нажать кнопку .



Рисунок 178 - Список копий VM

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 VM необходимо предварительно записать в файловую систему гипервизора, из физической машины или VM другого гипервизора (VMware, Hyper-V).

В рабочей области раздела представлен журнал ранее выполненных загрузок (Рисунок 179).



Начало	Оконч.	VM	из папки	Стадия	Результат
19.01.2022 08:40:34	08:42:35	xxxx	P2V: 192.168.2.175	заверш.	✓ (ИД шаблона = 40)
19.01.2022 08:28:34	08:30:35	xxxx	P2V: 192.168.2.175	заверш.	✓ (ИД шаблона = 39)

Рисунок 179 – Журнал загрузки

Для загрузки VM:

1. Нажать на кнопку .

2. Вставить путь к каталогу на файловой системе гипервизора, из которого требуется загрузить VM, в поле справа от надписи **Укажите папку с копией VM** (Рисунок 180).

Журнал загрузки		
из физической машины	Укажите хост с агентом импорта:	192.168.2.168
из копии VM Горизонта	Укажите папку с копией VM(192.168.2.4):	na/datasources/100/backup/bkp-astra-vm-60/20211025_2003/

Рисунок 180 - Путь к каталогу на файловой системе гипервизора, из которого требуется загрузить VM

Этот путь можно скопировать из:

- раздела Копирование VM → Журнал;
- физической машины;
- другого гипервизора (vmware, Hyper-V...) — требуется специальный агент p2v:

3. Нажать кнопку **Далее** (Рисунок 180)

Откроется окно редактирования шаблона выгружаемой VM (Рисунок 181).

Шаблон загружаемой VM

Имя шаблона виртуальной машины: antix-vm

Кол-во вирт. ЦП: 2 Кол-во ЦП: 0,1

Память, МБ: 1024

Диск(диски) (без CD-ROM): 0) Назначению hda Макс. размер 4096 Тип block Драйвер raw

Хранилище для загрузки: images

Графический доступ: Тип: VNC Слушать на IP: 0.0.0.0 Порт (был 5900): 0

Загрузка: Порядок загрузки: disk0 Тип BIOS: Legacy Меню загрузки: NO

Дополнительно: ACPI (управл. выключением): no GUEST_AGENT (агент qemu): no

Использовать сеть: [empty dropdown]

Графический адаптер: Модель: qxl Видео выходы: 1

Максимальное время загрузки VM (мин): 60

Максимальное время создания образа диска в СГУ (сек): 3000

Начать загрузку Назад

Рисунок 181 - Шаблон загружаемой VM

4. Отредактировать шаблон VM, 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 ID созданного в СГУ шаблона VM или ошибка.

3.3.9 Репликация виртуальной машины

Репликация – это перемещение состояния дисков VM (ведущей) с одного сервера на другой сервер (управляемый своим СГУ) в другую VM (ведомую).

Для возможности репликации VM необходимо выполнение требований:

- наличие канала связи между VM (возможно, небыстрого);
- ключи SSH на обоих площадках должны быть одинаковы;
- шаблоны дисков ведущей и ведомой VM 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 Звезда (сервера), т. е. из основной ВМ в запасную.

Репликация проводится следующим образом: 1) создается резервная копия ВМ на ведущем Звезде-ВС (не обязательно все диски);

2) копия в соответствии с предварительно заданным планом перемещается на ведомый Звезда 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 VM ID=** (Рисунок 183)

Рисунок 183 - План репликации копий VM

Рисунок 183 – План репликации копий VM

2. В поле Виртуальная машина нажать .

Откроется список доступных VM (Рисунок 184).

План репликации копий VM ID=

Сохранить Отменить

Виртуальная машина

Выбрана: Ид: Фильтр

N	Ид	Название VM
1	0	antix-small

« 1 »

Рисунок 184 - Выбор VM для репликации копий

3. Выбрать VM нажатием.

Для поиска VM, в поле **Фильтр** ввести ее номер или название полностью или частично и нажать кнопку .

Выбранная VM отобразится в поле **Выбрана** (Рисунок 185).

Выбрана: Ид: Фильтр

N	Ид	Название VM
1	0	antix-small

« 1 »

Рисунок 185 - Выбранная VM 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 VM, 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):

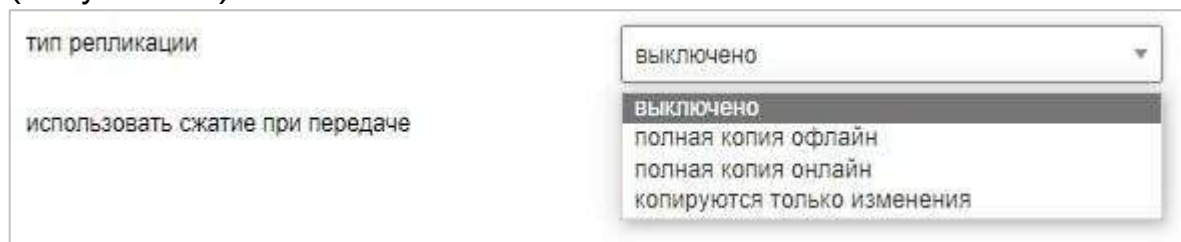


Рисунок 186 - Выбор типа репликации

- **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 передаче 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 использованием промежуточного файлового хранилища (ид=100) представлен на рисунке выше (Рисунок 187).

Сохранить Отменить

Виртуальная машина 0 antix-small

Выбрана antix-small Ид: 0 Фильтр

N	Ид	Название ВМ
1	0	antix-small

« 1 »

Диски hda

Ид	Имя	Образ	Размер
0	hda	antix	0G/3G

Хост СГУ для репликации 111.168.2.4

ID, имя целевой машины 2 wm-backup-serv

Диски

ID целевого хранилища 100

макс. время (мин.) 40

Время, отводимое на остановку ВМ (сек) 30

тип репликации полная копия офлайн

использовать сжатие при передаче ☒

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).

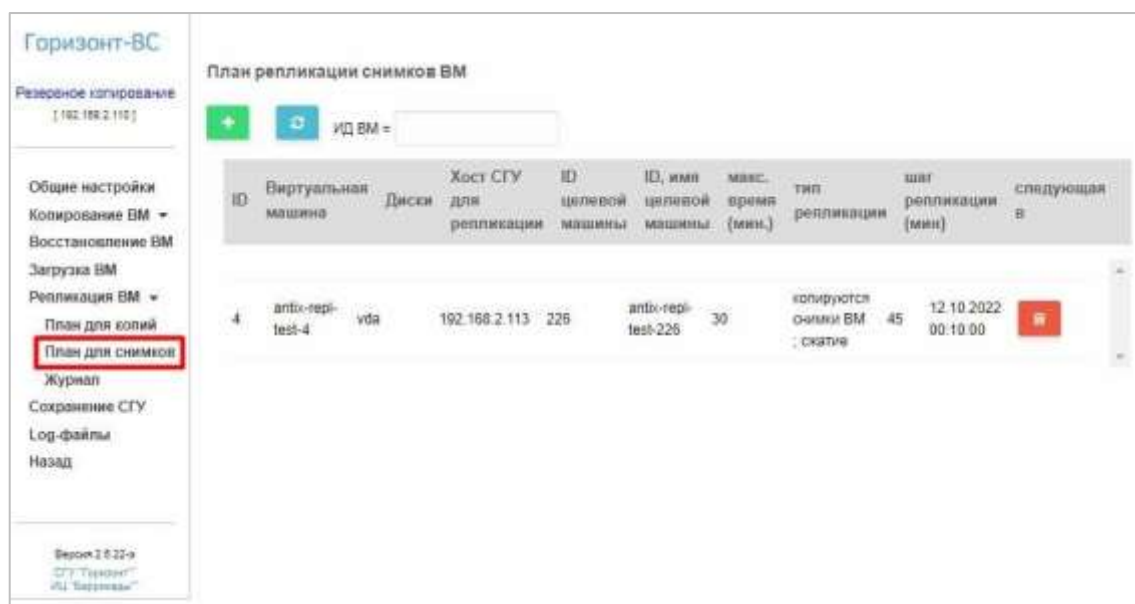


Рисунок 188 - План репликации для снимков VM

Для создания плана репликации снимков VM следует нажать кнопку  на панели управления и заполнить поля формы **План репликации снимков VM** (Рисунок 160).

Рисунок 189 - Создание плана репликации снимков VM

План репликации для снимков VM 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 завершения 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**.

Журнал репликации									
		Дата начала от: дд.мм.гггг		до: дд.мм.гггг	ИД ВМ =				
Начало	Оконч.	Ид	ВМ	Узел	Ид	ВМ	тип репликации	Результат	
08.09.2022 16:30:09	16:31:08	0	antix-small	192.168.92.127	1	repl-antix3	копируются изменения снимков	✓	
08.09.2022 16:00:08	16:01:09	0	antix-small	192.168.92.127	1	repl-antix3	копируются снимки ВМ	✓	
08.09.2022 15:30:08	15:31:09	0	antix-small	192.168.92.127	1	repl-antix3	копируются изменения снимков	✓	
08.09.2022 15:00:08	15:01:09	0	antix-small	192.168.92.127	1	repl-antix3	копируются снимки ВМ	✓	

Рисунок 190 - Журнал репликации

Строку журнала репликации можно посмотреть подробнее, нажав на соответствующую строку (Рисунок 191).

Репликация ВМ 41 antix-p2v	
Назад	
Начало	24.02.2022 09:40:14
Оконч.	24.02.2022 09:45:50
Диски	hda
Путь реплицируемой копии	/data/0/datastores/100/backup/antix-p2v-41/20220224_0900/
Узел	192.168.2.4
тип репликации	копируются только изменения
имя целевой машины	155 p2v-155
Время, отводимое на остановку ВМ (сек)	30
ID целевого хранилища	100
макс. время	40
Путь целевой копии	/var/lib/one//datastores/100/replications/p2v-155-155/
Стадия	заверш.
Результат	

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.

Журнал сохранения СГУ

Дата начала от :

дд : мм . гггг

до

дд . мм . гггг

Хранилище для копии

images

Сохранить

Отменить

Путь сохранения

Начало
Оконч.
стадия
Результат

/var/lib/one//datastores/100/backup/SGU/20200120_1350

20.01.2020

13:48:56

13:50:02

заверш.

✓

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).

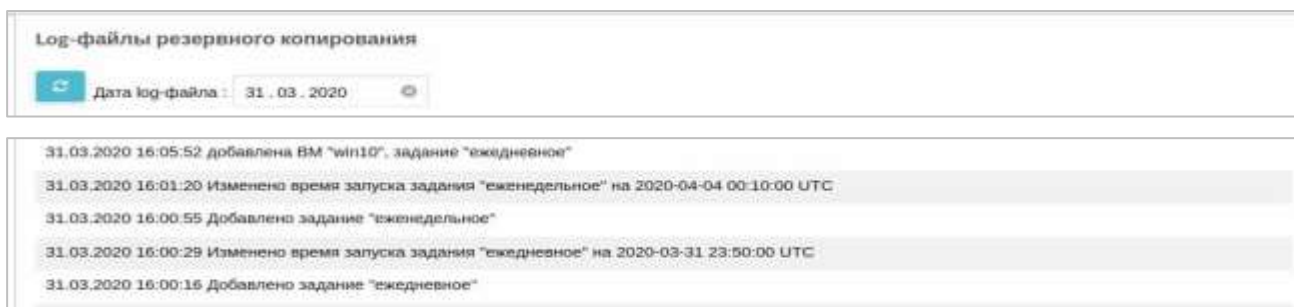


Рисунок 193 – Журнал СРК

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).

Обновить конфигурацию VM 93 template1-93 admin Horizon

← Обновить Мастер настройки

Загрузка ОС Ввод/Вывод Все остальные

Загрузка

Особенности

Архитектура CPU: x86_64

Тип BIOS: Legacy

Чипсет: pc-q35-3.1

Меню загрузки: YES

Root устройство: sda1

CPU Model: Nehalem

USB контроллер: xHCI

Порядок загрузки

☒	disk1	Volatile	↑ ↓
☐	disk0	Volatile	↑ ↓
☐	disk2	load_0_20220816154021	↑ ↓

Параметры загрузки ядра

re console=tty1

Путь к исполняемому файлу загрузчика

Рисунок 194 - Конфигурация VM

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 VM → Журнал;

е. Восстановление VM;

ж. Загрузка VM;

з. Репликация VM → 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, при 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:

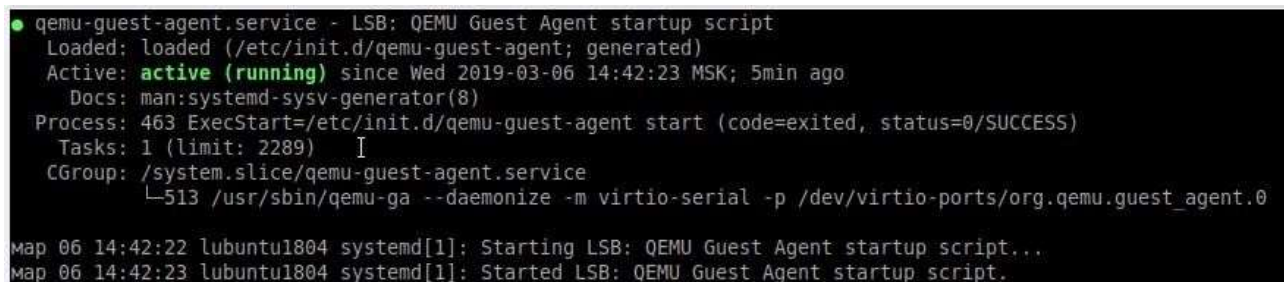
```
event=button/power action=/sbin/shutdown now
```

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).



```
● qemu-guest-agent.service - LSB: QEMU Guest Agent startup script
   Loaded: loaded (/etc/init.d/qemu-guest-agent; generated)
   Active: active (running) since Wed 2019-03-06 14:42:23 MSK; 5min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 463 ExecStart=/etc/init.d/qemu-guest-agent start (code=exited, status=0/SUCCESS)
    Tasks: 1 (limit: 2289)   I
   CGroup: /system.slice/qemu-guest-agent.service
           └─513 /usr/sbin/qemu-ga --daemonize -m virtio-serial -p /dev/virtio-ports/org.qemu.guest_agent.0

mar 06 14:42:22 lubuntu1804 systemd[1]: Starting LSB: QEMU Guest Agent startup script...
mar 06 14:42:23 lubuntu1804 systemd[1]: Started LSB: QEMU Guest Agent startup script.
```

Рисунок 195 - qemu-guest-agent запущен

Для ВМ с ОС семейства Windows загрузить в СГУ iso-образ virtio-win

<https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-virtio/virtio-win.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).

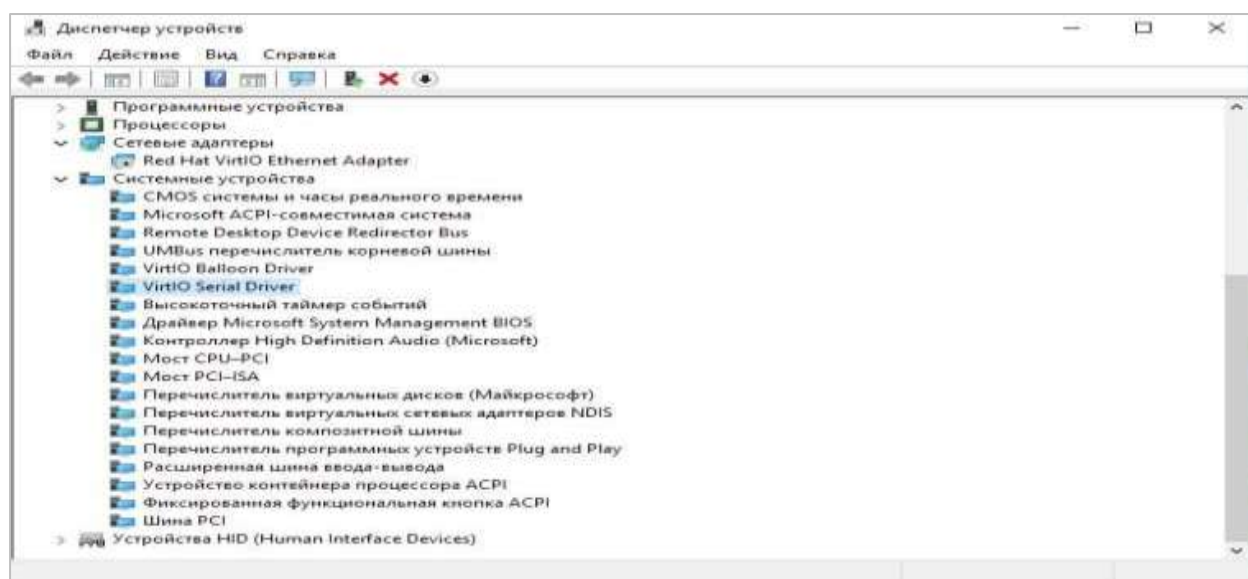


Рисунок 196 - Драйвер virtio-serial установлен

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).

```
Mon Feb 10 15:19:15 MSK 2020
Обновление СГУ
Остановка контейнера СГУ
hcs
Удаление текущего контейнера СГУ
Остановка службы контейнеров
* Stopping docker ...Подпись нового контейнера СГУ
Signing recursively in /var/lib/docker
Запуск службы контейнеров
* Starting docker ... [ ok ]
Запуск нового контейнера СГУ hcs:1.0.25

Обновление СГУ успешно завершено
Mon Feb 10 15:31:13 MSK 2020
```

Рисунок 199 - Журнал системы автоматического обновления СГУ

4 Настройка и работа СХД «Шторм»

4.1 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 Серв»). Модель состояний системы состоит из следующих значений:

- **Значок «ОК»** 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 Серв»). 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 «

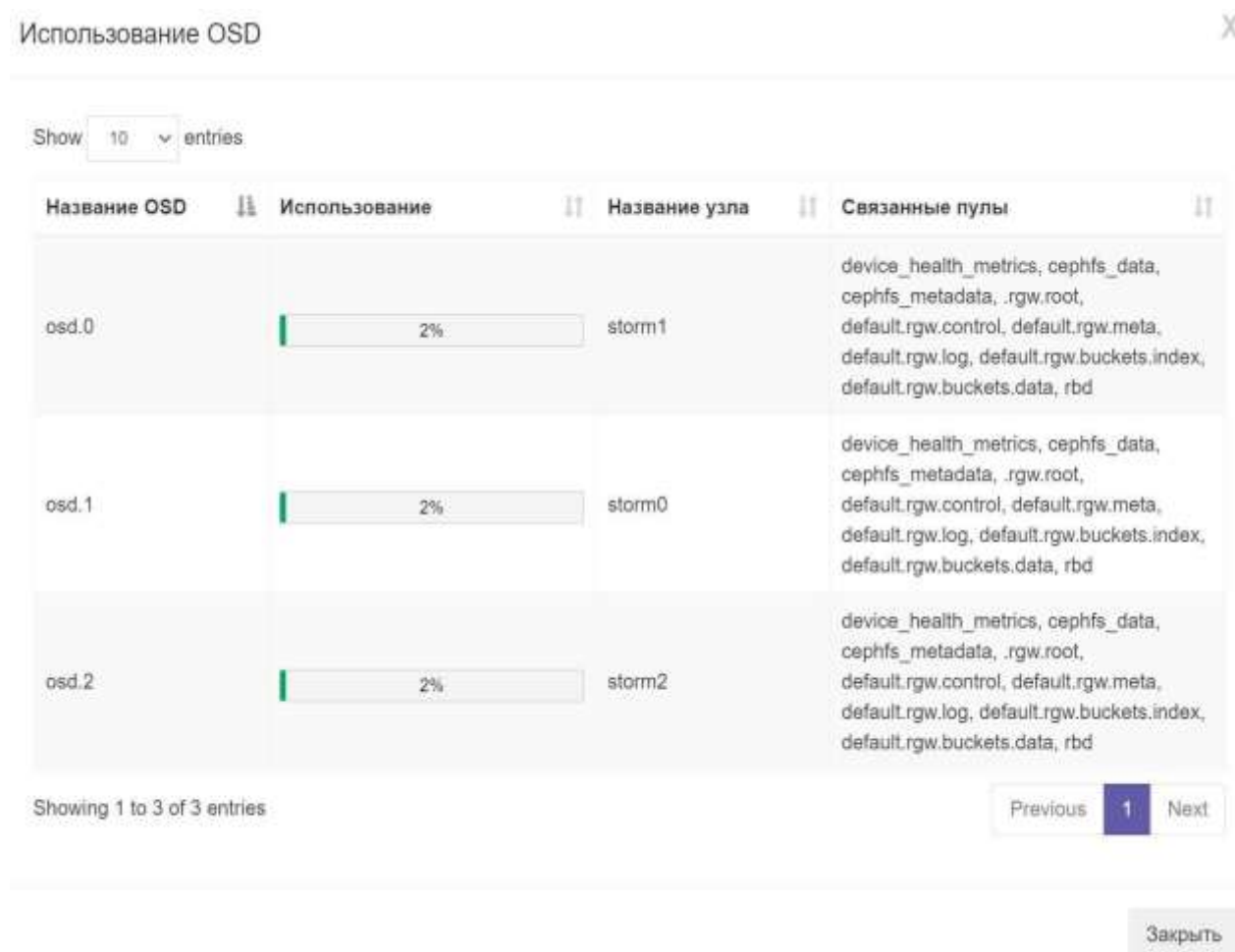


Рисунок 202 - Детализированная информация о дисках хранилища
» (Рисунок 202):

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.

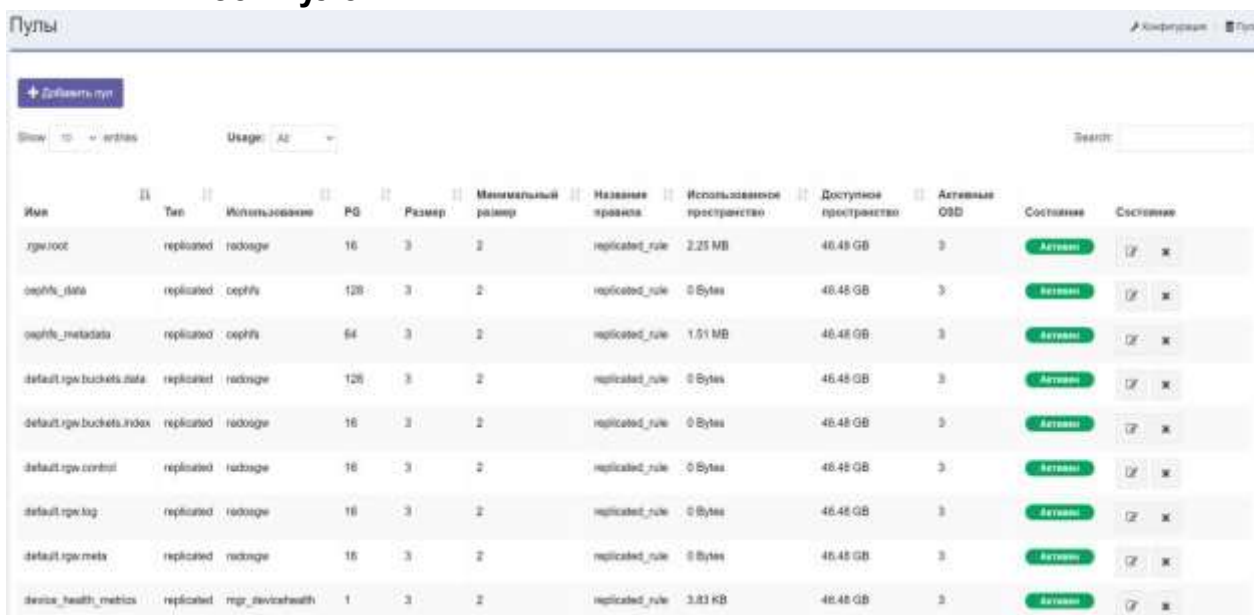
- **Температура диска.** Температура диска считывается с помощью SMART Tools.

- **Использование сети.** Использование сети в процентах показывает, насколько заняты интерфейсные карты.

- **Пропускная способность сети.** Скорость передачи чтения/ записи сети.

4.2 Управление пулами

4.2.1 Список пулов



Имя	Тип	Использование	PG	Размер	Минимальный размер	Название правила	Использованное пространство	Доступное пространство	Активные OSD	Состояние	Состояние
rgw.root	replicated	radosgw	16	3	2	replicated_rule	2.25 MB	46.48 GB	3	Активно	🔄 ✖
cephfs_data	replicated	cephfs	128	3	2	replicated_rule	0 Bytes	46.48 GB	3	Активно	🔄 ✖
cephfs_metadata	replicated	cephfs	64	3	2	replicated_rule	1.51 MB	46.48 GB	3	Активно	🔄 ✖
default.rgw.buckets.data	replicated	radosgw	128	3	2	replicated_rule	0 Bytes	46.48 GB	3	Активно	🔄 ✖
default.rgw.buckets.index	replicated	radosgw	16	3	2	replicated_rule	0 Bytes	46.48 GB	3	Активно	🔄 ✖
default.rgw.control	replicated	radosgw	16	3	2	replicated_rule	0 Bytes	46.48 GB	3	Активно	🔄 ✖
default.rgw.log	replicated	radosgw	16	3	2	replicated_rule	0 Bytes	46.48 GB	3	Активно	🔄 ✖
default.rgw.meta	replicated	radosgw	16	3	2	replicated_rule	0 Bytes	46.48 GB	3	Активно	🔄 ✖
device_health_metrics	replicated	mgr_devicehealth	1	3	2	replicated_rule	3.83 KB	46.48 GB	3	Активно	🔄 ✖

Рисунок 203 - Список пулов

При нажатии в меню Конфигурация -> Пулы, система отобразит список существующих пулов (Рисунок 203).

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 ЕС: 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.

4.2.2 Добавить пул

Добавить пул

Конфигурация > Пулы > Добавить пул

Название пула*

Тип*

☒ Реплицируемый ☐ EC

Использование:*

Количество PG:*

Размер:*

Минимальный размер*

Сжатие:

☐ Включено ☒ Отключено

Название правила:*

Отменить Сохранить

Рисунок 204 - Форма добавления пула

При нажатии меню на Конфигурация -> Пулы-> Добавить пул, система откроет форму добавления пула (Рисунок 204).

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 ЕС.** Появляется в случае пула ЕС, чтобы можно было выбрать профиль ЕС
- **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 ЕС: 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 ЕС: 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.

4.3 Конфигурация stormwind

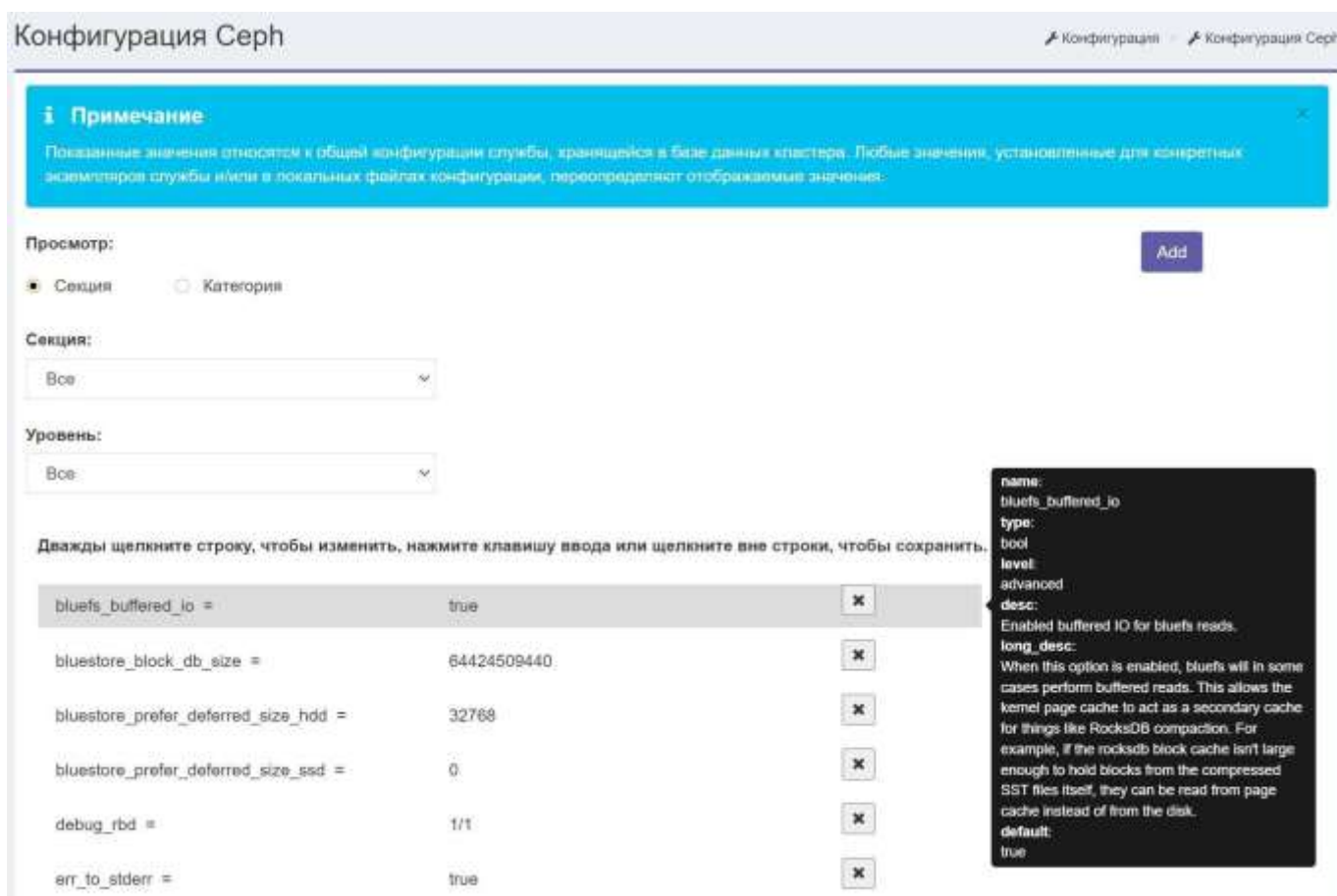
4.3.1 Просмотр конфигурации stormwind

При нажатии меню на Конфигурация -> Конфигурация Серв, можно просмотреть ключи конфигурации, которые сохранены в общей 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.

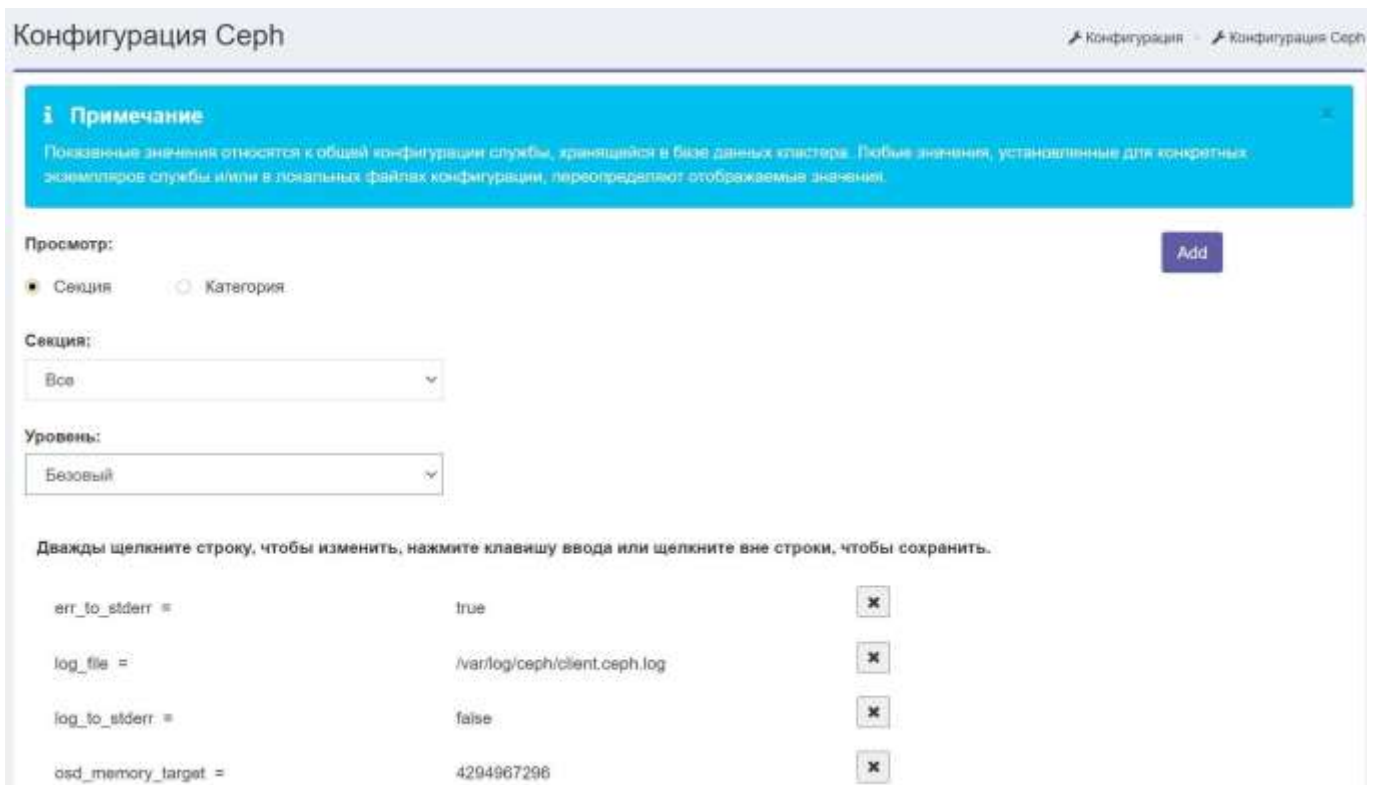
При наведении курсора мыши на любую клавишу система отображает справочное описание этой клавиши (Рисунок 205Рисунок 205 –).



Можно фильтровать ключи по:

- **Секция.** Доступные варианты текущих разделов:
 - все
- Рисунок 205 – Описаний клавиш
- 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.
- **Категория.** Текущие параметры категорий ():
- Recovery (Восстановление)

Рисунок 206 – Выбрать конфигурацию

Конфигурация Serph

Конфигурация · Конфигурация Serph

Просмотр:

☐ Секция ☒ Категория

Категория:

recovery

Дважды щелкните строку, чтобы изменить, нажмите клавишу ввода или щелкните вне строки, чтобы сохранить.

osd_max_backfills =	1	x
osd_recovery_max_active =	1	x
osd_recovery_op_priority =	1	x
osd_recovery_priority =	1	x
osd_recovery_sleep =	0.100000	x
osd_scrub_during_recovery =	false	x

- Scrubbing (Очистка).

Добавить конфигурацию serph

Ключ:*

Секция:*

Значение:*

Закреть Добавить

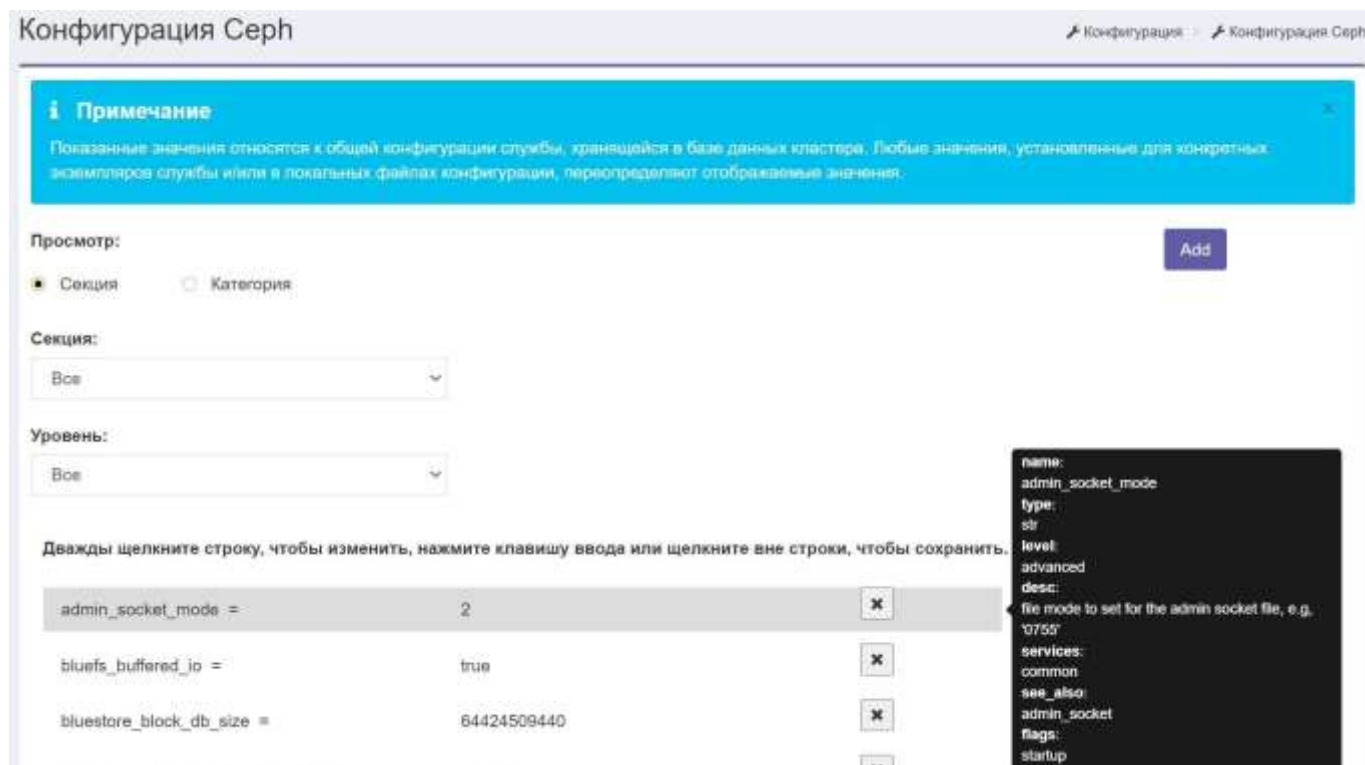
4.3.2 Добавить ключ конфигурации stormwind

Доступно добавление нового ключа конфигурации StormWind (Рисунок 208).

- **Ключ.** Из списка доступных ключей можно выбрать имя ключа, которое необходимо добавить.

Рисунок 207 – Добавление ключа конфигурации

- **Секция.** Выберите раздел, в который хотите добавить ключ.



- **Значение.** Введите значение выбранного ключа.

4.3.3 Удалить значение ключа конфигурации stormwind

Можно удалить один из существующих ключей конфигурации StormWind, по нажатию кнопки «» в строке с ключом (Рисунок 209).

4.4 Управление узлами

4.4.1 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).

В списке узлов отображается следующая информация о каждом узле:

- **Имя** – имя хоста узла.

Рисунок 209 – Удаление ключа конфигурации

- **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.

Рисунок 210 – Список узлов кластера

Имя	Тип	Управление IP-адресами	Версия	Состояние	Состояние
storm0	Управление	10.10.101.50	22.07	Вкл	[Иконки]
storm1	Управление	10.10.101.51	22.07	Вкл	[Иконки]
storm2	Управление	10.10.101.52	22.07	Выкл	[Иконки]

Showing 1 to 3 of 3 entries

- **Задание роли узла.** Открывает форму «Управление ролями». Кнопка

Рисунок 211 - Список физических дисков узла

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.

4.4.2 Список физических дисков узла

В системе управления отображается список локальных дисков для определенного узла (Рисунок 211).

дисков узла отображается следующая информация о каждом диске:

- **Имя** – имя локального диска.
- **Размер** – размер диска.
- **Список физических дисков узла SSD** – в этом столбце указывается,

Имя	Размер	SSD	Серия	SMART тест	Использование	Состояние	Связанные устройства	Использование OSD	Состояние
		Нет			OSD1	Вкл			
dm-0	10 GB	Нет	Not Detected		Пусто				+ i
dm-1	10 GB	Нет	Not Detected		Пусто				+ i
dm-2	29 GB	Нет	Not Detected		Пусто				+ i

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:

Рисунок 212 – Список физических дисков

- 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 213).

Добавить устройство хранения



Физический диск:

dm-0

Добавить как:

OSD

Внешний журнал:

Отключено

Внешний кэш:

Отключено

Примечания:

- Устройства SSD должны быть корпоративного класса с PLP, высоким DWPD и обеспечивать высокую производительность записи синхронизации/FUA.
- Память, необходимая для каждого OSD, по умолчанию составляет 4 ГБ + дополнительные 2%% от размера раздела кэша при использовании кэша записи.

Заккрыть

Добавить

Рисунок 213 - 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.

4.4.3 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 214).



Рисунок 214 – Назначение ролей для узла

4.4.4 Просмотр журнала

Система позволяет просматривать системный журнал узла (Рисунок 215).

Для просмотра последних записей журнала использовать кнопку «Обновить».



Рисунок 215 - Журнал ошибок

4.5 Управление iSCSI дисками

4.5.1 Список iSCSI дисков

При переходе в пункт меню *Управление iSCSI дисками* -> *iSCSI диски* отображается список iSCSI дисков системы (Рисунок 216).

В списке iSCSI дисков отображается следующая информация о каждом диске:

- **ID диска** – идентификатор диска
- **Размер** – размер диска
- **Имя** – имя диска



Рисунок 216 - Список iSCSI дисков

- **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 с ссылки не найден..**

4.5.2 Список назначенных путей

Пункт меню Управление iSCSI дисками -> Назначение пути (Рисунок 217):



Рисунок 217 - Список назначенных путей

4.6 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.

4.6.1 СПИСОК ЗАДАЧ РЕПЛИКАЦИИ

Для отображения списка задач репликации необходимо перейти в пункт меню

Управление iSCSI дисками -> Репликация -> Задачи (Рисунок 218 **Ошибка! Источник ссылки не найден.**).

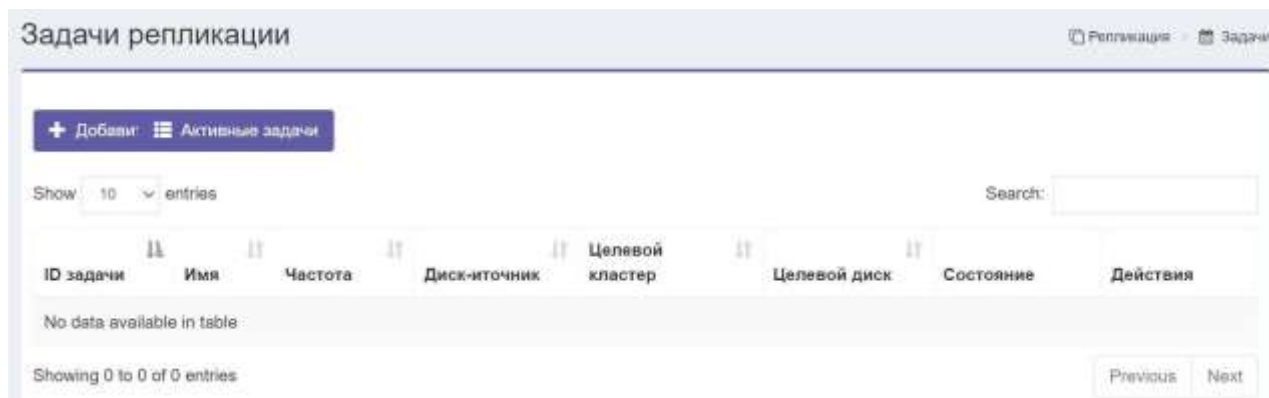
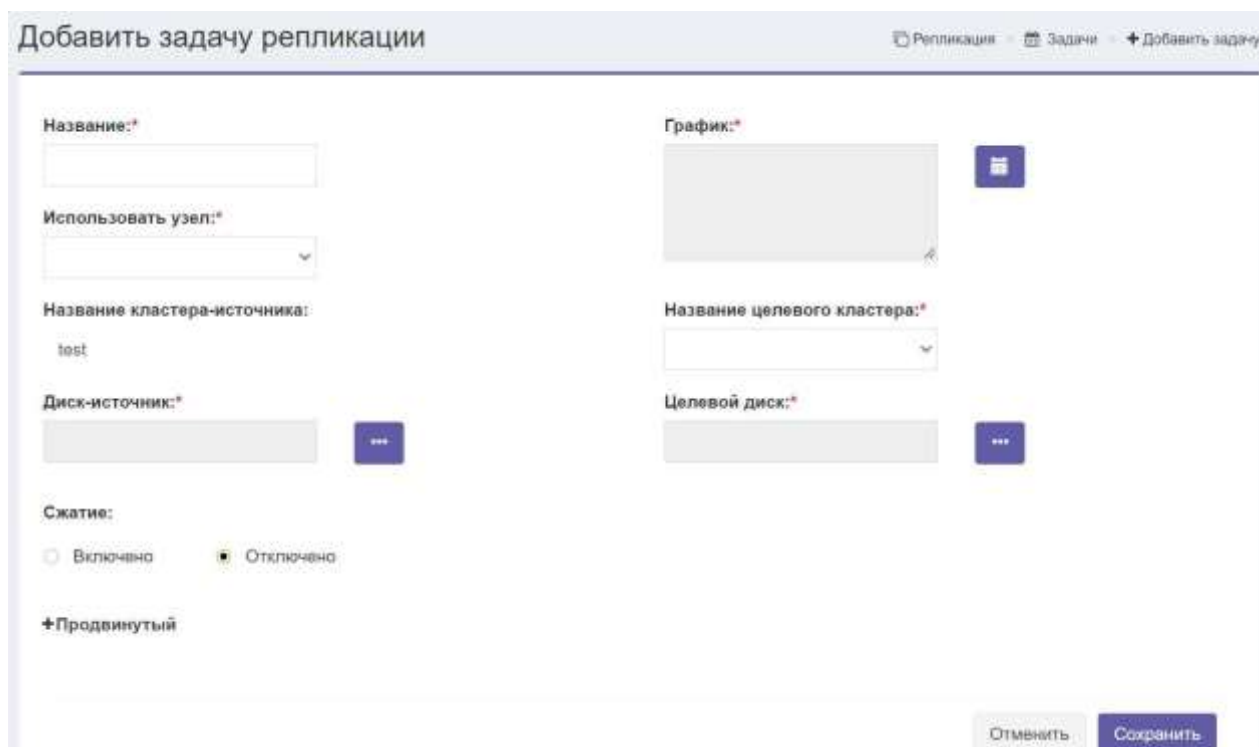


Рисунок 218 - Список задач репликации

4.6.2 Создание задания репликации

Доступно добавление задания репликации в исходный кластер (кнопка «Добавить задачу репликации») (Рисунок 219).



The screenshot shows a web form titled "Добавить задачу репликации" (Add replication task). The form is divided into two main columns. The left column contains fields for "Название:" (Name), "Использовать узел:" (Use node), "Название кластера-источника:" (Source cluster name) with the value "test", and "Диск-источник:" (Source disk). The right column contains a "График:" (Schedule) field with a calendar icon, "Название целевого кластера:" (Target cluster name), and "Целевой диск:" (Target disk). Below these fields are radio buttons for "Сжатие:" (Compression) with options "Включено" (Enabled) and "Отключено" (Disabled). At the bottom left is a link "+Продвинутый" (+Advanced). At the bottom right are "Отменить" (Cancel) and "Сохранить" (Save) buttons. The top right of the form has navigation links: "Репликация" (Replication), "Задачи" (Tasks), and "+ Добавить задачу" (+ Add task).

Рисунок 219 - 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 220).

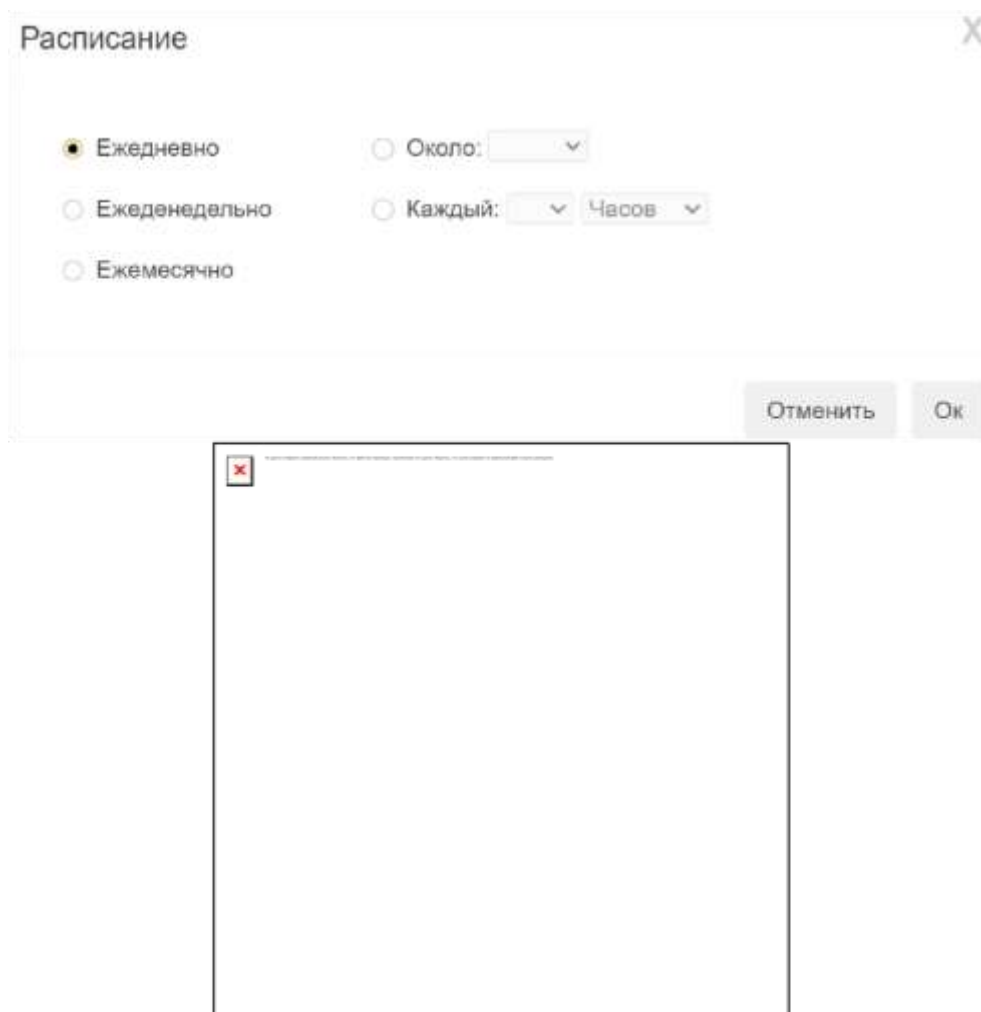


Рисунок 220 - Настройка расписания выполнения задания

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 221):

Рисунок 221 - – Настройка еженедельного расписания

- **По.** Вы можете выбрать дни недели, в которые будет выполняться задание.

- **Около.** Работа будет выполняться ежедневно в определенный час.

- о **Ежемесячно** (Рисунок 222):

Рисунок 222 - 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.

Добавить задачу репликации

Репликация | Задачи | + Добавить задачу

Название:*

Использовать узел:*

Название кластера-источника:
test

Диск-источник:*

График:*

Название целевого кластера:*

Целевой диск:*

Сжатие:
☐ Включено ☒ Отключено

—Продвинутый

URL скрипта предварительного снимка: ⓘ

URL скрипта итогового снимка: ⓘ

URL после выполненной задачи: ⓘ

Отменить Сохранить

Рисунок 223 - Добавление задачи репликации в продвинутом формате

Расширенная форма дополнена следующей информацией (Рисунок 223):

- **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.

4.6.3 СПИСОК АКТИВНЫХ ЗАДАНИЙ

В системе доступен список текущих работ.

4.6.4 СПИСОК ПОЛЬЗОВАТЕЛЕЙ РЕПЛИКАЦИИ

Для отображения списка пользователей репликации необходимо перейти в пункт меню Управление iSCSI дисками -> Репликация -> Пользователи (Рисунок 224).

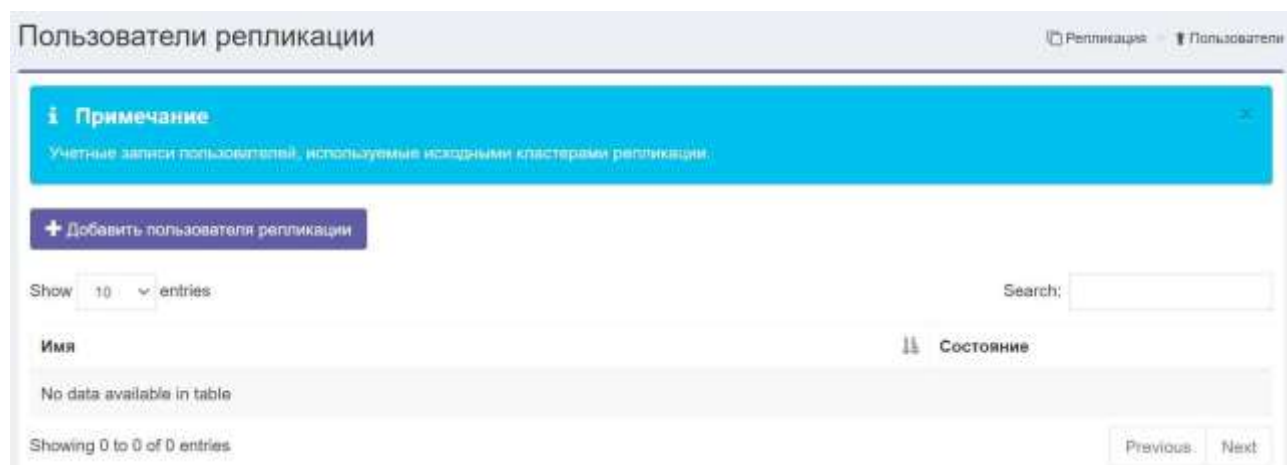


Рисунок 224 - Список пользователей репликации

Добавление пользователя репликации (Рисунок 225).

The screenshot shows a web interface for adding a replication user. The title is 'Добавить пользователя репликации'. The breadcrumb trail is 'Репликация > Пользователи > + Добавить пользователя'. The form contains three fields: 'Имя пользователя:' (User Name) with an asterisk, 'Авторизованные пулы:' (Authorized Pools) with an asterisk and an information icon, and 'Закрытый ключ пользователя:' (User Secret Key). The 'Авторизованные пулы' dropdown menu is open, showing 'rbd'. At the bottom right, there are 'Отменить' (Cancel) and 'Сохранить' (Save) buttons.

Рисунок 225 - Добавление пользователя репликации

4.6.5 СПИСОК ЦЕЛЕВЫХ КЛАСТЕРОВ

Для отображения списка целевых кластеров необходимо перейти в пункт меню Управление iSCSI дисками -> Репликация -> Целевые кластеры (Рисунок 226).

The screenshot shows a web interface for target clusters. The title is 'Целевые кластеры'. The breadcrumb trail is 'Репликация > Целевые кластеры'. There is a '+ Добавить целевой кластер' (Add Target Cluster) button. Below it, there is a 'Show 10 entries' dropdown and a 'Search:' input field. The table has three columns: 'Название кластера' (Cluster Name), 'Удалённый IP-адрес' (Remote IP Address), and 'Действия' (Actions). The table is currently empty, with the message 'No data available in table'. At the bottom, it says 'Showing 0 to 0 of 0 entries' and has 'Previous' and 'Next' buttons.

Рисунок 226 - Список целевых кластеров

Добавление целевого кластера (Рисунок 227).

Рисунок 227 - Добавление целевого кластера

4.7 Управление rbd

4.7.1 Список rbd

При переходе в пункт меню *Управление RBD* -> *Список RBD* отображается список RBD системы (Рисунок 228).

Рисунок 228 - 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**

4.7.2 Добавление rbd диска

При нажатии на кнопку «Добавить RBD» открывается форма добавления нового RBD диска (Рисунок 229).

Рисунок 229 - Добавление RBD диска

4.8. Управление cifs

4.8.1 Просмотр ресурсов cifs

Система отображает список существующих общих ресурсов, в котором отображаются следующие столбцы (Рисунок 230)

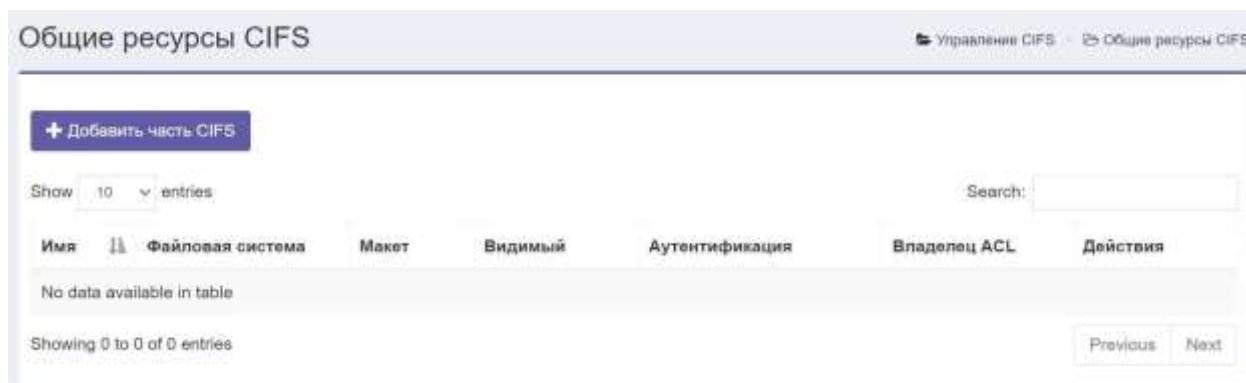


Рисунок 230 - Список общих ресурсов

- **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.

4.8.2 Добавить общий ресурс cifs

Система открывает форму CIFS Share (Рисунок 231).



Рисунок 231 - 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.

4.8.3 Просмотр статуса cifs

Доступен просмотр текущего статуса CIFS (Рисунок 232 **Рисунок 232**).

Node Name	Status	Assigned IPs
VM00R-01	On	10.0.4.101 10.0.4.103 10.0.4.105 10.0.4.107 10.0.4.109 10.0.4.111 10.0.4.113 10.0.4.115 10.0.4.117 10.0.4.119
VM00R-03	On	10.0.4.100 10.0.4.102 10.0.4.104 10.0.4.106 10.0.4.108 10.0.4.110 10.0.4.112 10.0.4.114 10.0.4.116 10.0.4.118 10.0.4.120

Рисунок 232 - 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

4.8.4 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

4.9 Управление nfs

4.9.1 Просмотр nfs exports

Для просмотра выводится список существующих NFS Exports, содержащий следующие столбцы (Рисунок 233):

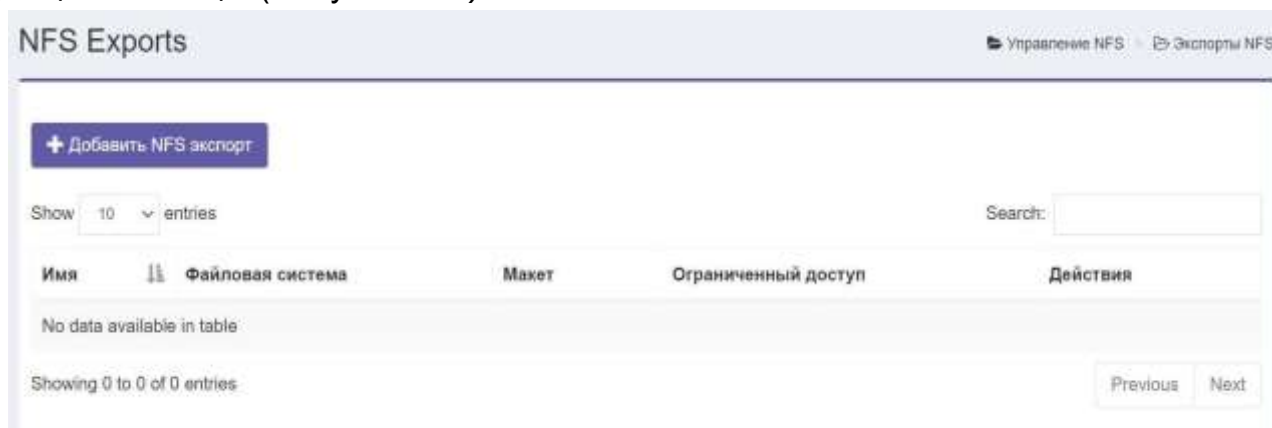


Рисунок 233 - NFS Exports

- **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.

4.9.2 Добавление nfs exports

Система открывает форму для создания NFS Exports (Рисунок 234).

Add NFS Export

Manage NFS - NFS Exports - Add NFS Export

Name: Slow

File System:

Layout: default

Cancel Save

Рисунок 234 - Создание NFS Экспорт

Форма добавления NFS Exports содержит следующие поля:

- **Имя** – имя экспорта.
- **Файловая система** – файловая система, в которой будет создан экспорт.
- **Действия:**
- *Сохранить* – сохраняет добавленный экспорт.

4.9.3 Просмотр статуса nfs

Возможно просмотреть текущий статус NFS (Рисунок 235).

NFS Status

Manage NFS - NFS Status

Node Name	Status	Assigned IPs	Number Of Connections
node-01	Up	192.168.50.100 192.168.50.102	2
node-02	Up	192.168.50.101 192.168.50.103 192.168.50.104	0

Рисунок 235 - 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.

4.9.4 Просмотр подключений

Доступен просмотр соединений для выбранного серверного узла (Рисунок 236).

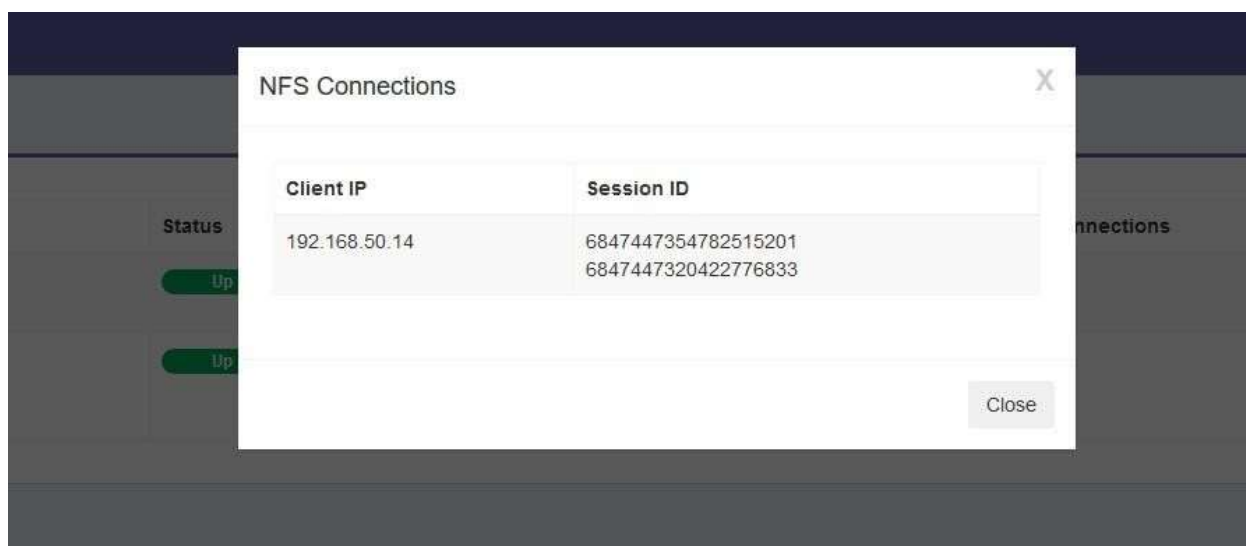


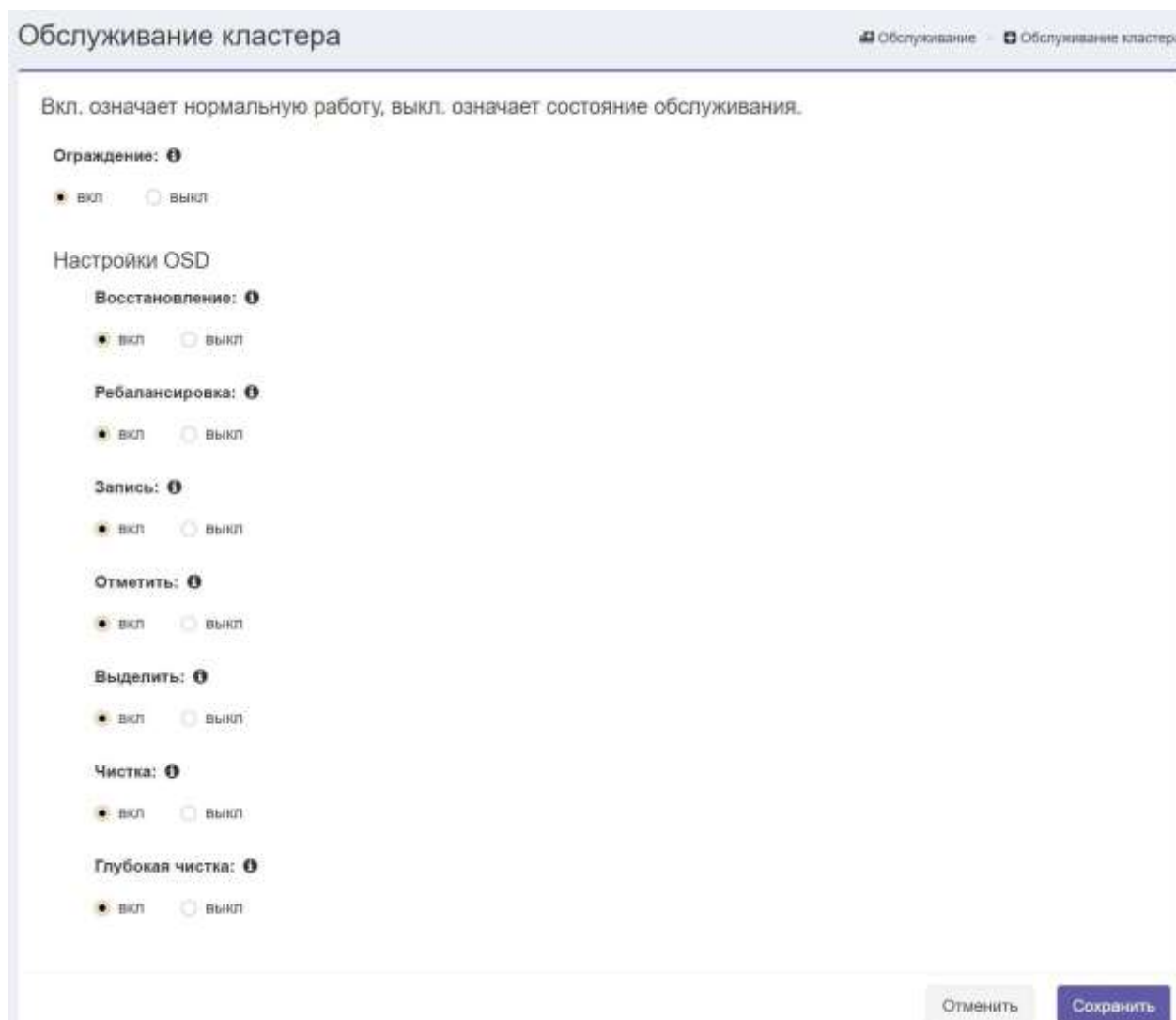
Рисунок 236 - Соединения для выбранного серверного узла

В системе отображаются следующие столбцы для каждого активного соединения:

- **Клиентский IP** – IP-адрес подключенного клиента.
- **Идентификатор сеанса** – идентификатор сеанса подключенного клиента.

4.10 Обслуживание

4.10.1 Обслуживание кластера С помощью формы обслуживания кластера можно отключить один или несколько параметров обслуживания (Рисунок 237).



Обслуживание кластера

Обслуживание Обслуживание кластера

Вкл. означает нормальную работу, выкл. означает состояние обслуживания.

Ограждение: ⓘ

☒ вкл ☐ выкл

Настройки OSD

Восстановление: ⓘ

☒ вкл ☐ выкл

Ребалансировка: ⓘ

☒ вкл ☐ выкл

Запись: ⓘ

☒ вкл ☐ выкл

Отметить: ⓘ

☒ вкл ☐ выкл

Выделить: ⓘ

☒ вкл ☐ выкл

Чистка: ⓘ

☒ вкл ☐ выкл

Глубокая чистка: ⓘ

☒ вкл ☐ выкл

Отменить Сохранить

Рисунок 237 - Настройка параметров обслуживания кластера

4.11 Управление пользователями

4.11.1 Добавление пользователя

Для добавления пользователя используется следующая форма (Рисунок 237).

Рисунок 238 - 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».

4.11.2 Просмотр списка пользователей

Система позволяет просматривать всех пользователей в системе с помощью страницы списка пользователей (Рисунок 239).



Рисунок 239 - Страница списка пользователей

Действия

Система позволяет выполнять следующие действия для каждого пользователя:

Редактировать - обновлять информацию о пользователе, кроме имени пользователя (Рисунок 240);



Рисунок 240 - Форма редактирования информации о пользователе

Удалить - удалить любого пользователя, кроме администратора по умолчанию.

4.11.3 Изменение пароля пользователя

Система позволяет любому пользователю изменить свой пароль



Рисунок 241 - Форма изменения пароля

4.12 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.

4.13 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 242):



Рисунок 242 - Загрузиться с носителя

2. Повторить настройки узла. Ввести hostname (Рисунок 243):

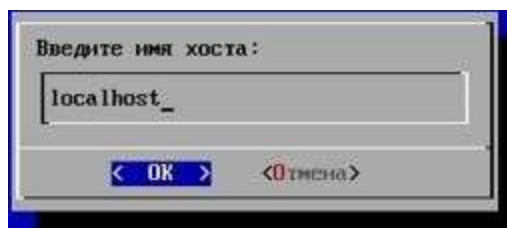


Рисунок 243 - Ввести hostname

3. Выбрать сетевой интерфейс (Рисунок 244):

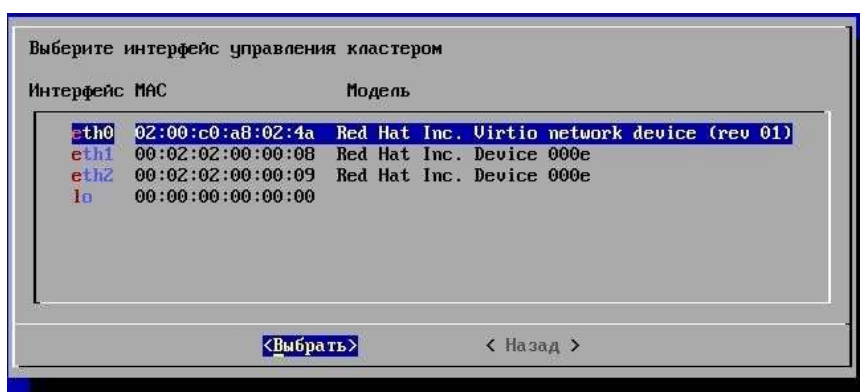


Рисунок 244 - 3. Выбрать сетевой интерфейс

4

- Настроить сеть (Рисунок 245):

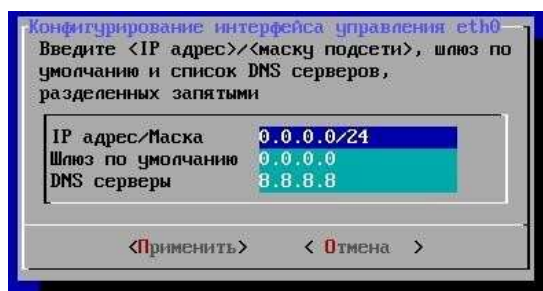


Рисунок 245 - Настроить сеть

5. Выбрать диск для обновления системы (Рисунок 246):

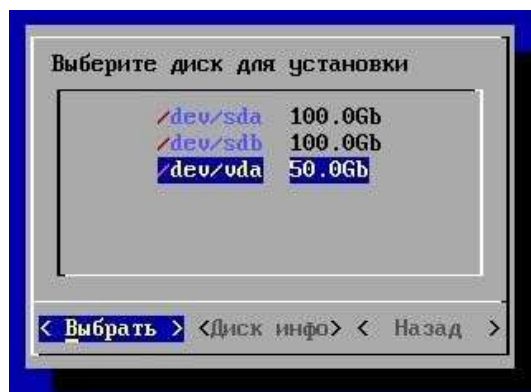


Рисунок 246 - Выбрать диск для обновления системы

6. После обновления выбрать необходимое действие (Рисунок 246):



Рисунок 247 - Выбрать необходимое действие

4.14 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).

4.15 Замена компонентов СХД

Замена компонентов СХД производится в следующем порядке:

1. Отключить одну ноду (Рисунок 248):



Рисунок 248 - Отключить одну ноду

2. Посмотреть выключенные OSD (Рисунок 249):



Рисунок 249 - Посмотреть выключенные OSD

3. Заменить один диск на другой (Рисунок 250):

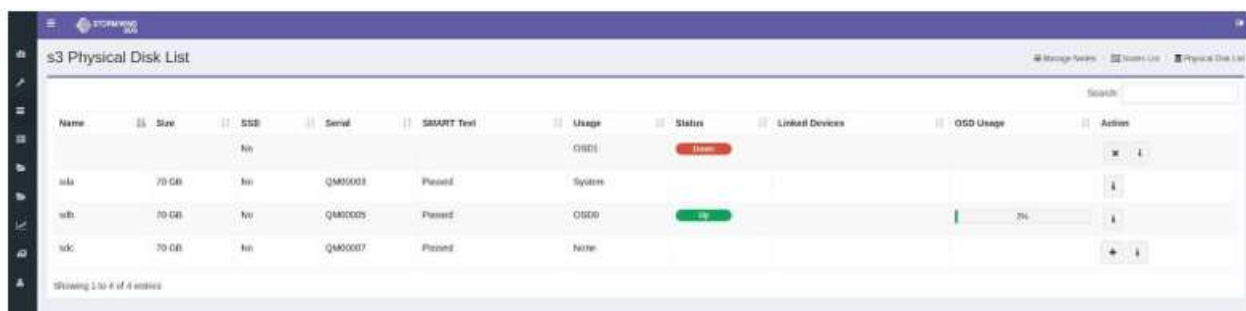


Рисунок 250 – Заменить диск

4. Активировать новый диск (Рисунок 251)

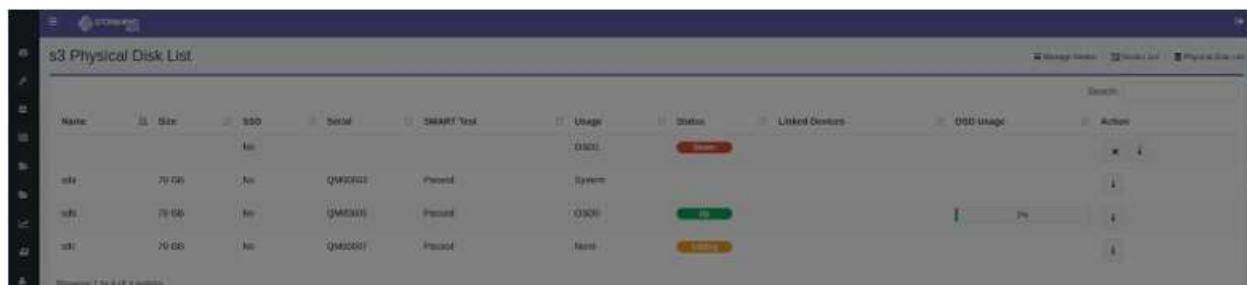


Рисунок 251 – Активировать новый диск

5. Убедиться, что после активации статус изменился (Рисунок 252):

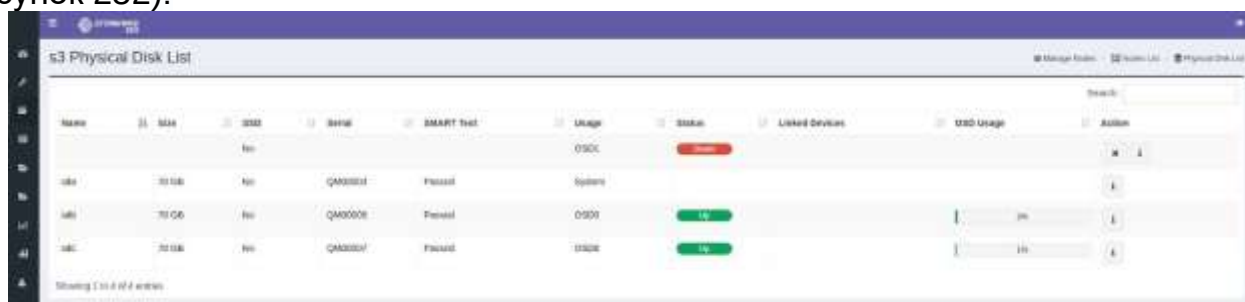


Рисунок 252 - Статус

5 Настройка Программного обеспечения подсистемы VDI

5.1 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`

5.2 Установка VDI на VMware vSphere

Требования к виртуальной платформе

Подсистема VDI может быть размещена на платформе виртуализации VMware vSphere, версии 6.5 или выше.

VMware vSphere, на которой будет развернута подсистема VDI, должна соответствовать следующим требованиям:

- Для установки сервера VDI и создания виртуальных рабочих столов, необходим по крайней мере один сервер VMware ESXi с действующей лицензией.
- VMware vSphere должна администрироваться vCenter с действующей лицензией.

- Для возможности VDI интегрировать и отправлять запросы в vCenter, чтобы их можно было выполнять, необходимо иметь *учетные данные пользователя с правами администрирования* на платформе VMware vSphere, на которой будут развернуты виртуальные рабочие столы и приложения.
- Необходимо определить хотя бы одну Группу виртуальных локальных сетей для виртуальной машины, к которой будут подключены виртуальные серверы платформы VDI.
- Необходимо определить хотя бы одну Группу виртуальных локальных сетей для виртуальной машины, к которой будут подключены различные виртуальные рабочие столы, управляемые VDI.
- Для размещения виртуальных серверов, составляющих VDI, необходимо не менее 43 ГБ свободного дискового пространства и не менее 5ГБ свободной оперативной памяти.

5.3 Установка и настройки VDI Actor

VDI Actor устанавливается в ОС Windows или Linux (золотой образ) для использования при развертывании виртуальных рабочих столов. Также необходимо, чтобы серверы приложений RDS имели установленный VDI Actor, чтобы иметь возможность представлять пользователям виртуальные сессии приложений.

Для установки VDI 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 (Рисунок 253 Рисунок 254).



Рисунок 253

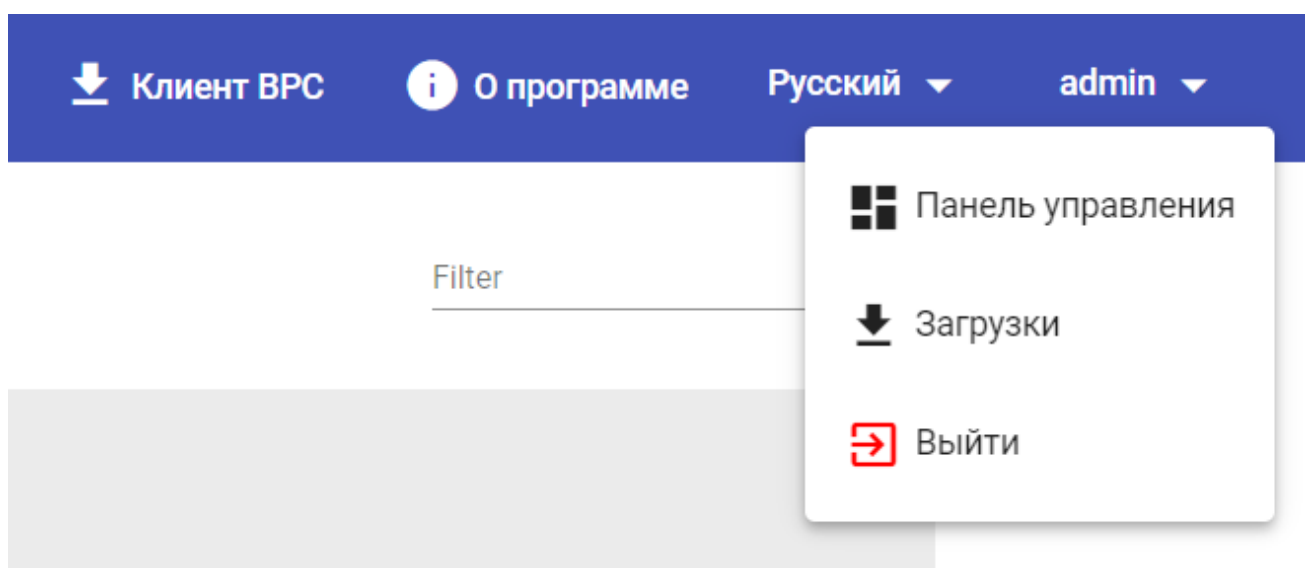


Рисунок 254

Выбрать Actor соответствующей операционной системы и службы, установленной в базовом шаблоне или сервере приложений, на котором будут развернуты службы рабочего стола.

- VDIactor_3.0.0_all.deb: VDI Actor для шаблона машин Linux (золотой образ) на основе дистрибутивов Debian, таких как: Ubuntu, Xubuntu и т.д.

- **VDIactor-3.0.0-1.noarch.rpm:** VDI Actor для шаблона машин Linux (золотой образ) на основе дистрибутивов Red Hat, таких как: CentOS, Fedora и т.д.

- **VDIactor-opensuse-3.0.0-1.noarch.rpm:** VDI Actor для шаблона машин Linux (золотой образ) на основе дистрибутивов на базе Suse, таких как: OpenSuse и т.д.

- **VDIactor-2.2.0_legacy.deb:** VDI Actor версии 2.2 для шаблона машин Linux (золотой образ) на основе дистрибутивов Debian, таких как: Ubuntu, xUbuntu и т.д.

- **VDIactor-unmanaged_3.0.0_all.deb:** VDI Actor для управления сеансами машин на основе Debian от поставщика услуг «Поставщик статических IP-машин», таких как: Ubuntu, xUbuntu и т.д.

- **RDSActorSetup-3.0.0.exe:** VDI Actor для серверов приложений Windows Server 2012 R2, 2016, 2019 или 2022 с настроенной ролью RDS.

- **VDIActorUnmanagedSetup-3.0.0.exe:** VDI Actor для управления сеансами компьютеров Windows от поставщика услуг «Поставщик статических IP-машин».

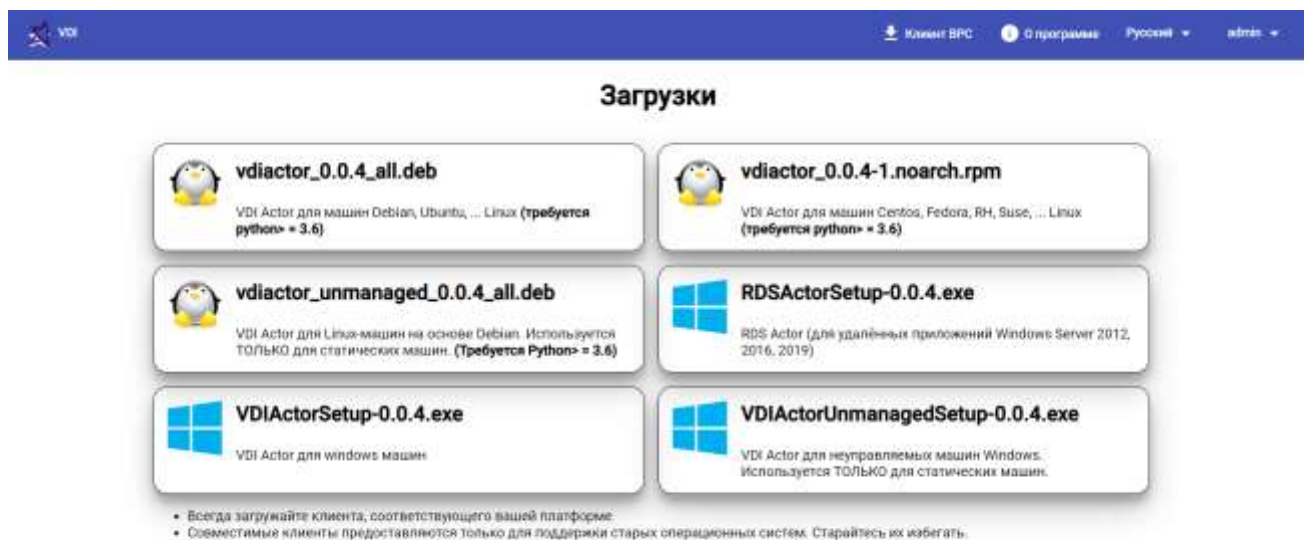


Рисунок 255

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 VDI Actor: VDIActorSetup-3.0.0.exe.

Примечание: перед установкой VDI 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 VDI Actor для Windows и переноса его на компьютер-шаблона запустить его, чтобы продолжить установку.

Выбрать язык программы установки и нажать кнопку «ОК» (Рисунок 256).

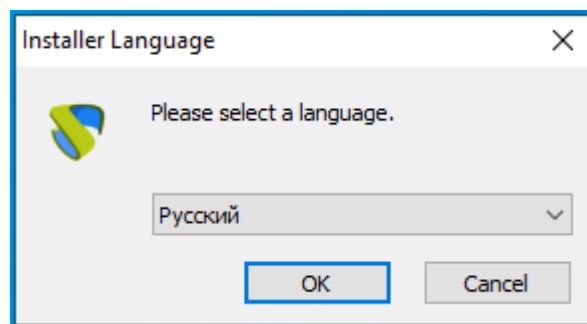


Рисунок 256 -Выбор языка программы

Указать путь установки элемента VDI (Рисунок 257).

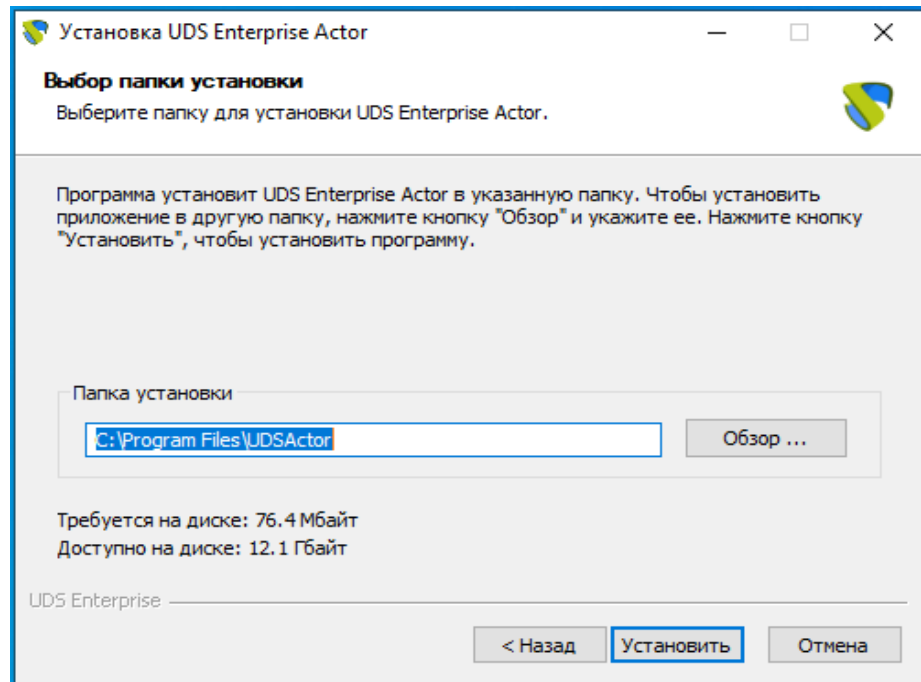


Рисунок 257

После завершения установки перейти к конфигурированию элемента VDI (Рисунок 258).

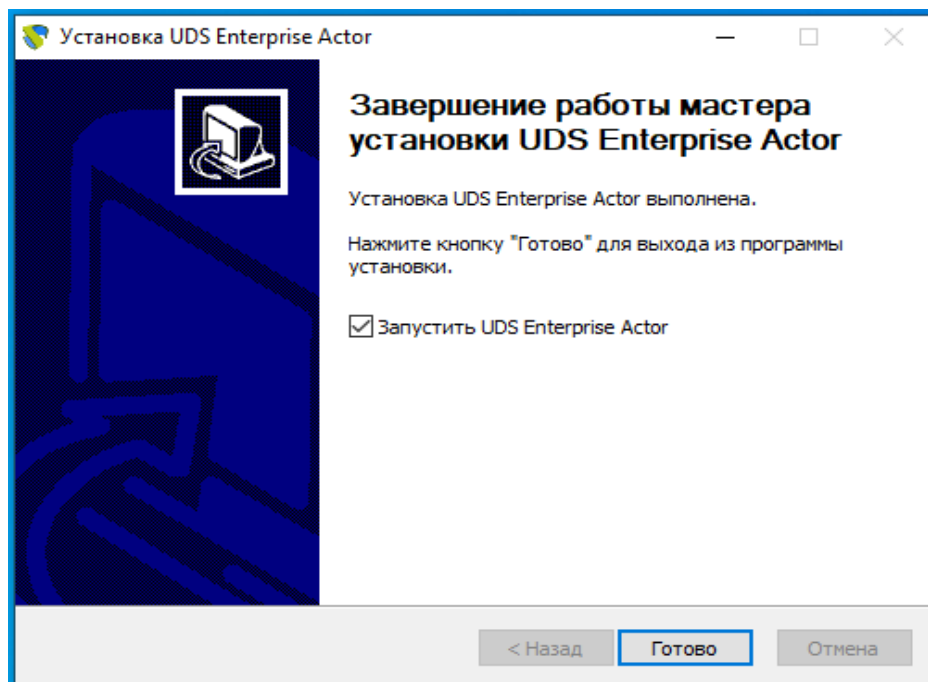


Рисунок 258

На вкладке VDI Server нужно зарегистрировать Actor в экземпляре VDI, указав следующие параметры (Рисунок 260):

- SSL Validation: игнорировать сертификат\верификационный сертификат
- VDI Server: имя или IP-адрес VDI-сервера и порт.
- Authenticator: Аутентификатор, к которому принадлежит указанный пользователь-администратор для регистрации VDI 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.

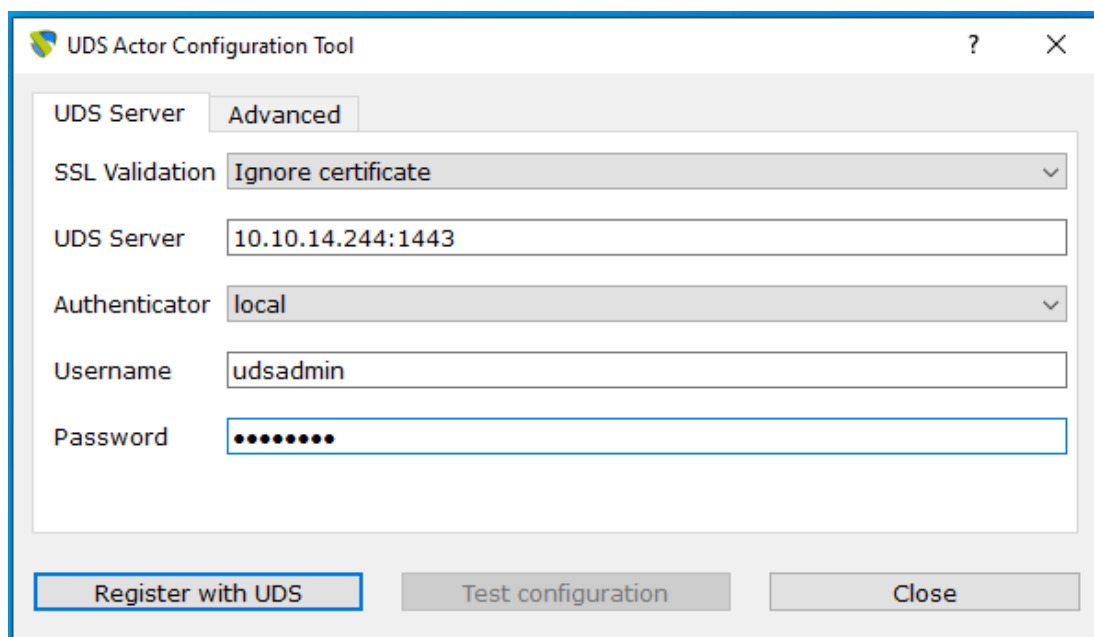


Рисунок 259

После ввода этих данных нажать кнопку «Register with VDI» (Регистрация в VDI).

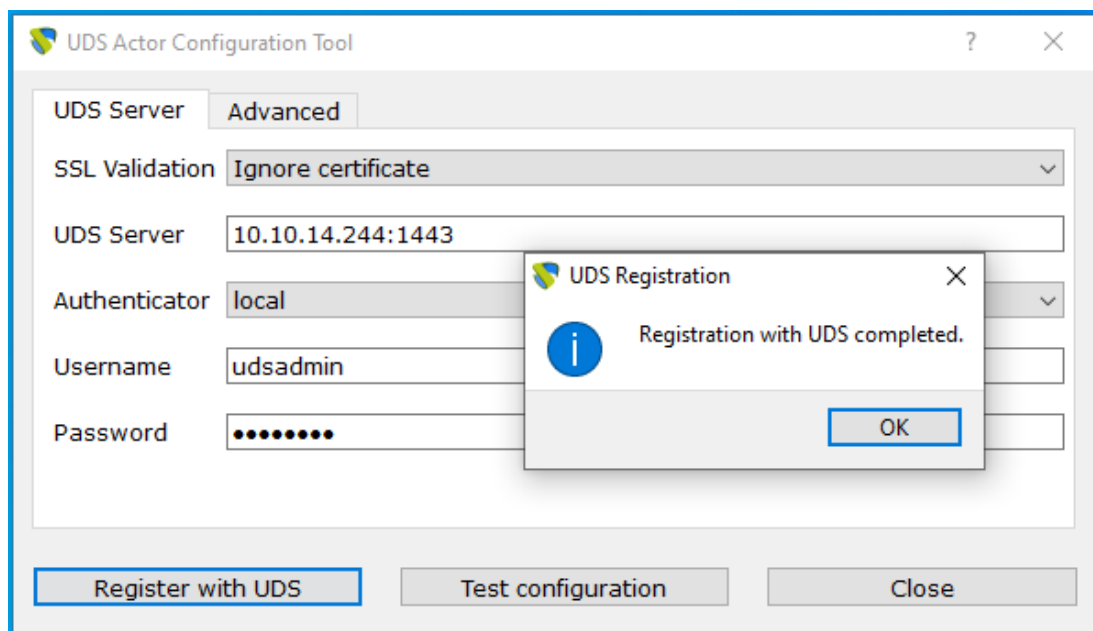


Рисунок 260

Можно выполнить тест, нажав кнопку «Test configuration», для проверки правильности подключения к серверу VDI (Рисунок 261).

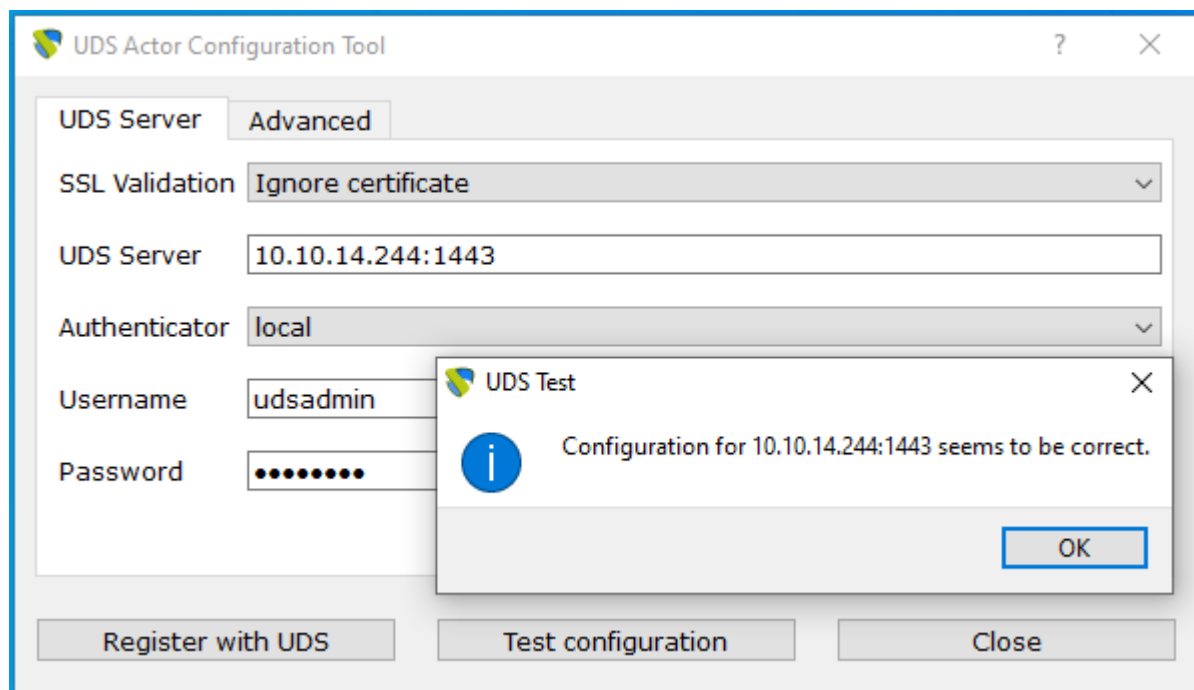


Рисунок 261
363

На вкладке «Advanced» можно указать следующие дополнительные параметры (Рисунок 262).

- 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, rsoip...), IP (IP, распознанный на клиенте (SRC IP)), имя хоста (SRC Host).

- Runonce: сценарий, который выполняется только один раз и до того, как VDI 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 Actor, 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 VDI Actor, таких как копирование файлов из локальной сети, выполнение конфигураций и т.д.

- Log Level: типы журналов, которые должны отображаться в файлах журнала VDI Actor. Эти файлы журнала (VDIactor.log) будут располагаться в

путях: %temp% (путь временных файлов пользователя) и C:\Windows\Temp (путь временных файлов системы).

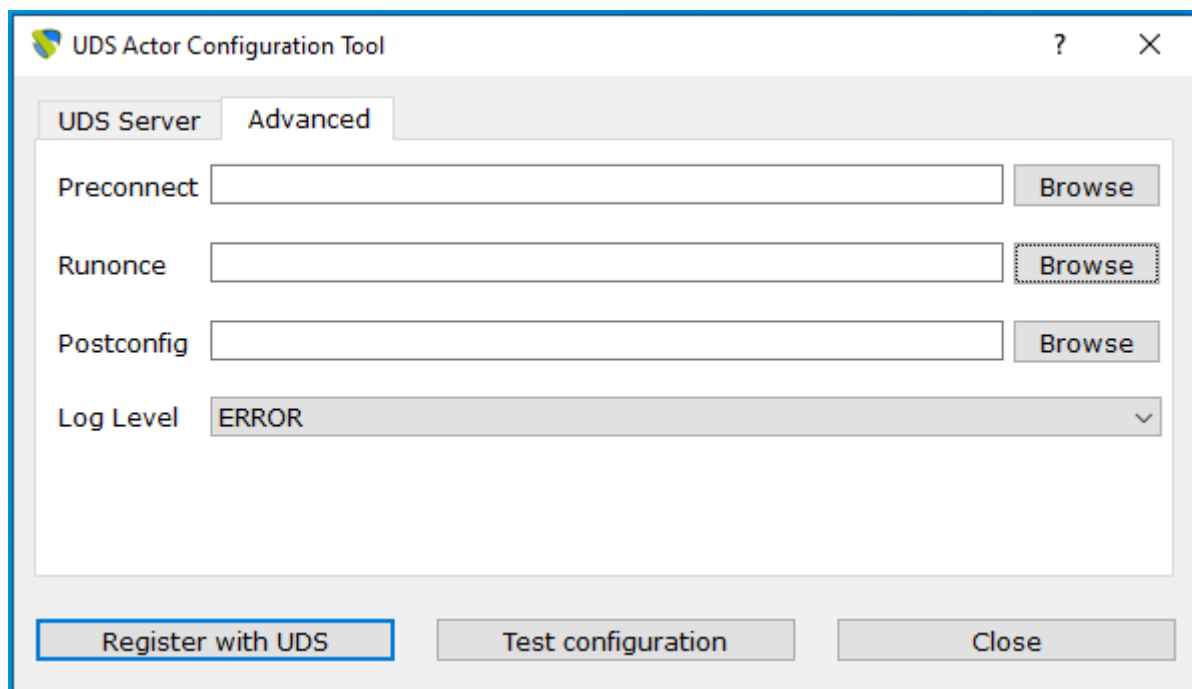


Рисунок 262

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 VDI Actor шаблонная машина теперь может быть отключена и будет доступна для использования VDI для самогенерированных виртуальных рабочих столов.

Примечание: помимо установки VDI Actor, необходимо включить протокол подключения для подключения к создаваемым рабочим столам (например, включить удаленный рабочий стол, установить клиент PCoIP и т.д.).

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 VDI Actor: VDIActorUnmanagedSetup-3.0.0.exe.

Если на этих машинах не установлен VDI 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 263Рисунок 263).

Рисунок 263

Примечание: перед установкой VDI Actor необходимо зарегистрировать IP-адрес или имя VDI-сервера и ключ «Ключ услуги» в службе типа «Статистический множественный IP-адрес» в «Поставщик статистических IP машин».

Установка VDIActorUnmanagedSetup-3.0.0 осуществляется следующим образом. Выбрать язык программы установки (Рисунок 264).

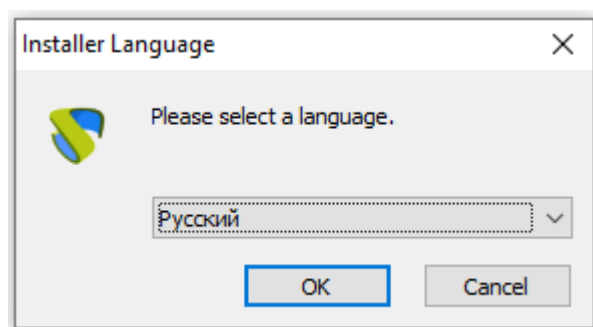


Рисунок 264

Указать путь установки VDI Actor и нажать кнопку «Установить» (Рисунок 265).

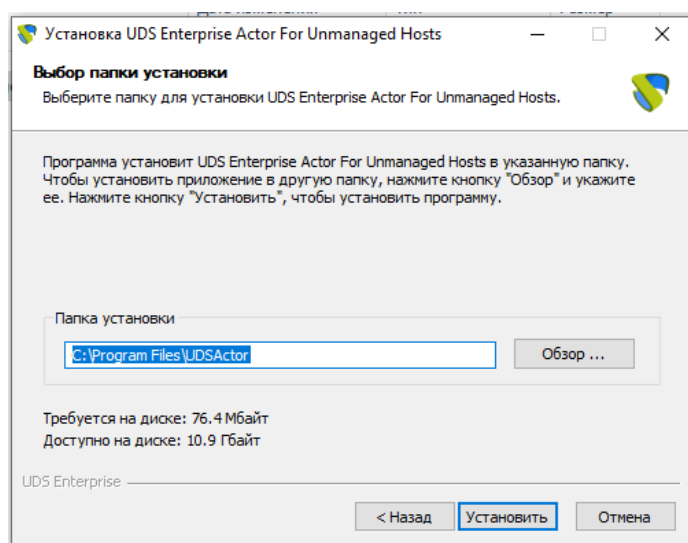


Рисунок 265

После завершения установки перейти к регистрации Actor на сервере VDI, указав следующие параметры:

- **SSL Validation:** игнорировать сертификат\верификационный сертификат.
- **VDI Server:** имя или IP-адрес VDI-сервера.

- **Service Token:** код, созданный в администрировании VDI, в типе «Статистический множественный IP-адрес» в рамках поставщика «Поставщик статистических IP машин»
- **Log Level:** типы журналов, которые должны отображаться в файлах журнала VDI Actor. Эти файлы журнала (VDIactor.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 266).

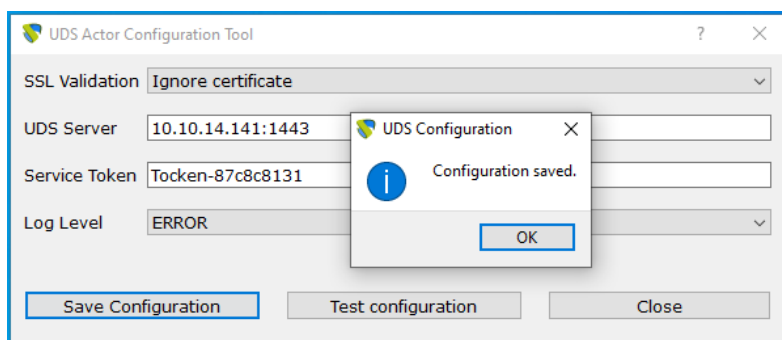


Рисунок 266

Необходимо выполнить конфигурационный тест для проверки правильности указанных данных и наличия подключения к серверу VDI (Рисунок 267).

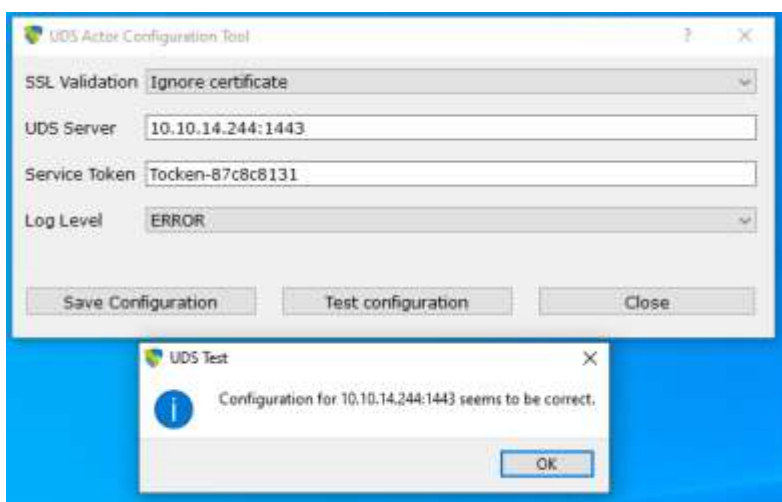


Рисунок 267

После завершения установки и конфигурирования элемента VDI машина будет доступна для назначения VDI и управления пользовательскими сеансами.

Примечание: в дополнение к установке VDI Actor, необходимо включить протокол подключения для подключения к сгенерированным рабочим столам (например, включить удаленный модуль записи и т.д.).

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 VDI Actor для различных дистрибутивов Linux:

- Дистрибутивы на основе Debian: VDIactor_3.0.0_all.deb
- Дистрибутивы на основе Red Hat: VDIactor-3.0.0-1.noarch.rpm
- Дистрибутивы на основе Suse: VDIactor-opensuse-3.0.0-1.noarch.rpm

Примечание: перед установкой VDI 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 VDI Actor для выбранного дистрибутива Linux будет загружен и перенесен на машину-шаблон, выполнить его, чтобы продолжить установку.

Настоятельно рекомендуется выполнять установку VDI Actor через командную строку:

```
user@ubuntu:~/Downloads$ sudo dpkg -i udsactor_3.0.0_all.deb
```

Если получена ошибка из-за отсутствия зависимостей, можно воспользоваться командой исправления зависимостей: “sudo apt-get install -f” (Рисунок 268).

```
user@ubuntu:~/Downloads$ sudo dpkg -i udsactor 3.0.0 all.deb
[sudo] password for user:
Selecting previously unselected package udsactor.
(Reading database ... 146861 files and directories currently installed.)
Preparing to unpack udsactor_3.0.0_all.deb ...
Unpacking udsactor (3.0.0) ...
dpkg: dependency problems prevent configuration of udsactor:
 udsactor depends on python3-pyqt5 (>= 4.9); however:
  Package python3-pyqt5 is not installed.
 udsactor depends on xscreensaver; however:
  Package xscreensaver is not installed.

dpkg: error processing package udsactor (--install):
 dependency problems - leaving unconfigured
Processing triggers for gnome-menus (3.13.3-1ubuntu1.1) ...
Processing triggers for desktop-file-utils (0.23-1ubuntu3.18.04.2) ...
Processing triggers for mime-support (3.60ubuntu1) ...
Errors were encountered while processing:
 udsactor
user@ubuntu:~/Downloads$ sudo apt-get install -f
```

```
Need to get 19.1 MB of archives.
After this operation, 90.8 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Рисунок 268

После установки необходимых зависимостей запустить конфигурацию VDI Actor. На вкладке VDI Server можно зарегистрировать Actor, указав следующие параметры (Рисунок 269).

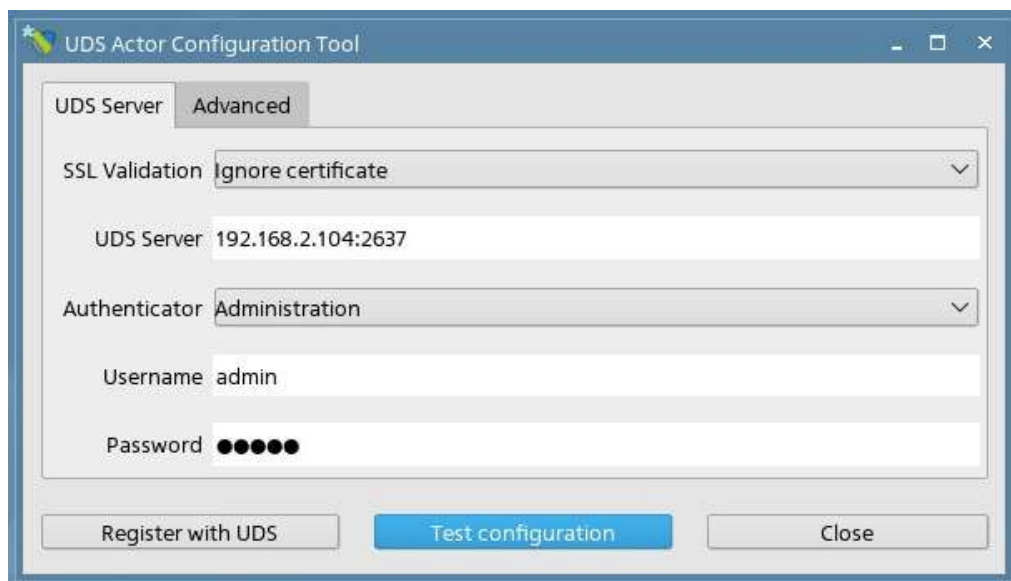


Рисунок 269

- SSL Validation: игнорировать сертификат\верификационный сертификат.
- VDI Server: имя или IP-адрес VDI сервера и порт (по умолчанию: 2637).
- Authenticator: Аутентификатор, 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 VDI» (Рисунок 270).



Рисунок 270

Можно выполнить тест, нажав кнопку «Test configuration», чтобы проверить правильность подключения к серверу VDI (Рисунок 271).

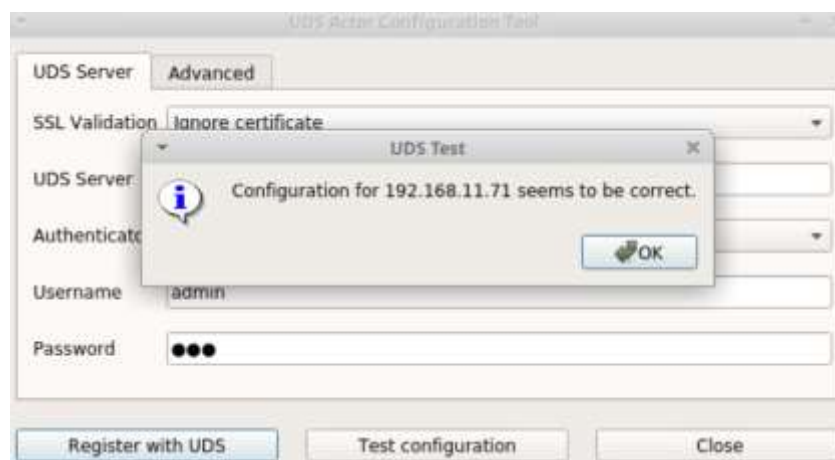


Рисунок 271

На вкладке «Advanced» можно указать следующие дополнительные параметры (Рисунок 272).

- Preconnect: Сценарий должен быть запущен непосредственно перед тем, как разрешить пользователю подключиться к виртуальному рабочему столу.

VDI автоматически передает следующие параметры, которые могут использоваться в сценарии: имя пользователя, протокол (rdp, nx, rsoip...), IP (IP, распознанный на клиенте (SRC IP)), имя хоста (SRC Host).

- Runonce: Сценарий, который выполняется только один раз и до того, как исполнитель VDI 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 VDI.

- Postconfig: Сценарий, который выполняется после того, как VDI 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 VDI Actor, например, копирование файлов из локальной сети, выполнение конфигураций и т.д.

- Log Level: типы журналов, которые должны отображаться в файлах журнала VDI Actor. Эти файлы журнала (VDIactor.log) будут расположены по пути `:/var/log/`

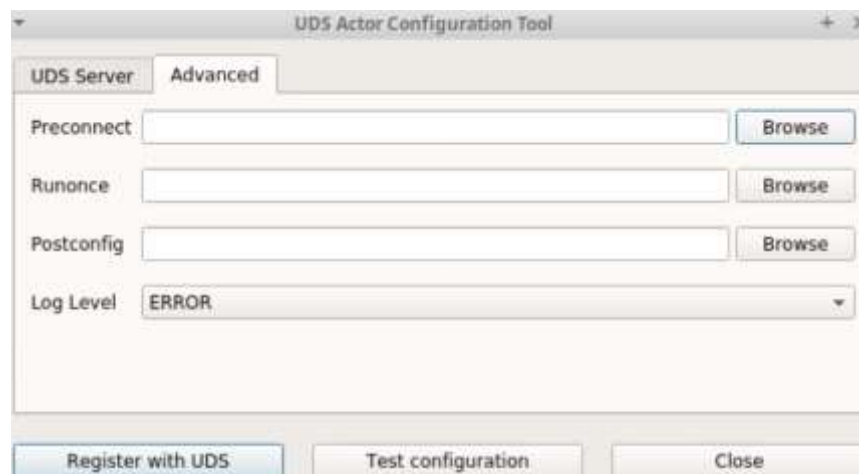


Рисунок 272

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 VDI Actor на шаблонной машине (золотой образ) теперь может быть отключена и будет доступна для использования VDI для самостоятельного создания виртуальных рабочих столов.

Примечание: в дополнение к установке VDI Actor, необходимо включить протокол подключения для подключения к сгенерированным рабочим столам (например, установить и включить XRDP, X2Go Server и т.д.).

5.4 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 VDI Actor: `VDIactor-unmanaged_3.0.0_all.deb`.

Если на этих машинах не установлен компонент VDI, 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.

Примечание: перед установкой VDI Actor необходимо зарегистрировать IP-адрес или имя сервера VDI и ключ «Ключ услуги» в службе типа «Статистический множественный IP-адрес» в поставщике услуг «Поставщик статистических IP машин».

После загрузки VDI 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 VDI Actor через консоль:

```
user@ubuntu:~/Downloads$ sudo dpkg -i udsactor-unmanaged_3.0.0_all.deb
```

Если получена ошибка из-за отсутствия зависимостей, можно воспользоваться командой исправления зависимостей: “sudo apt-get install -f” (Рисунок 273).

```
user@ubuntu:~/Downloads$ sudo dpkg -i udsactor-unmanaged_3.0.0_all.deb
[sudo] password for user:
Selecting previously unselected package udsactor-unmanaged.
(Reading database ... 146861 files and directories currently installed.)
Preparing to unpack udsactor-unmanaged_3.0.0_all.deb ...
Unpacking udsactor-unmanaged (3.0.0) ...
dpkg: dependency problems prevent configuration of udsactor-unmanaged:
 udsactor-unmanaged depends on python3-pyqt5 (>= 4.9); however:
  Package python3-pyqt5 is not installed.
 udsactor-unmanaged depends on xscreensaver; however:
  Package xscreensaver is not installed.

dpkg: error processing package udsactor-unmanaged (--install):
 dependency problems - leaving unconfigured
Processing triggers for gnome-menus (3.13.3-1ubuntu1.1) ...
Processing triggers for desktop-file-utils (0.23-1ubuntu3.18.04.2) ...
Processing triggers for mime-support (3.60ubuntu1) ...
Errors were encountered while processing:
 udsactor-unmanaged
user@ubuntu:~/Downloads$ sudo apt-get install -f
```

```
Need to get 19.1 MB of archives.  
After this operation, 90.8 MB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

Рисунок 273

После установки необходимых зависимостей будет выполнена конфигурация VDI Actor, следует указать следующие параметры (Рисунок 274).

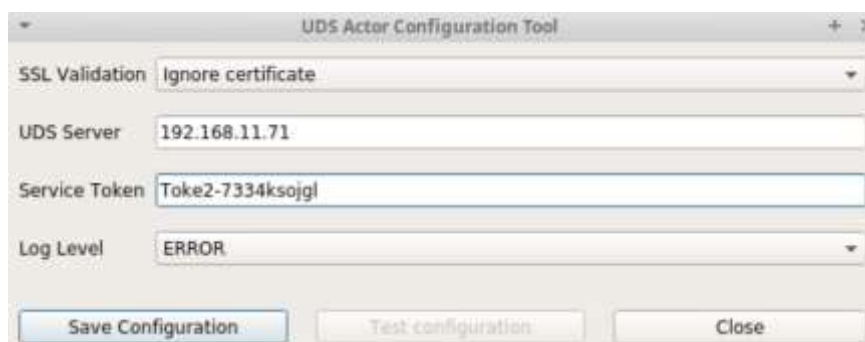


Рисунок 274

- SSL Validation: игнорировать сертификат\верификационный сертификат.
- VDI Server: имя или IP-адрес VDI-сервера.
- Service Token: код, созданный в администрировании VDI, 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 VDI Actor. Эти файлы журнала (VDIactor.log) будет располагаться по пути `:/var/log/`

После ввода этих данных нажать кнопку «Save Configuration» (сохранить конфигурацию) (Рисунок 275).



Рисунок 275

Необходимо выполнить конфигурационный тест для проверки правильности указанных данных и наличия подключения к серверу VDI (Рисунок 276).



Рисунок 276

После завершения установки и конфигурирования элемента VDI машина будет доступна для назначения VDI и управления пользовательскими сеансами.

Примечание: в дополнение к установке VDI Actor необходимо включить протокол подключения для подключения к сгенерированным рабочим столам (например, установить и включить XRDP).

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 VDI Actor.

На странице загрузки выбрать и загрузить Actor для серверов RDS (RDS VDI Actor) (Рисунок 277).

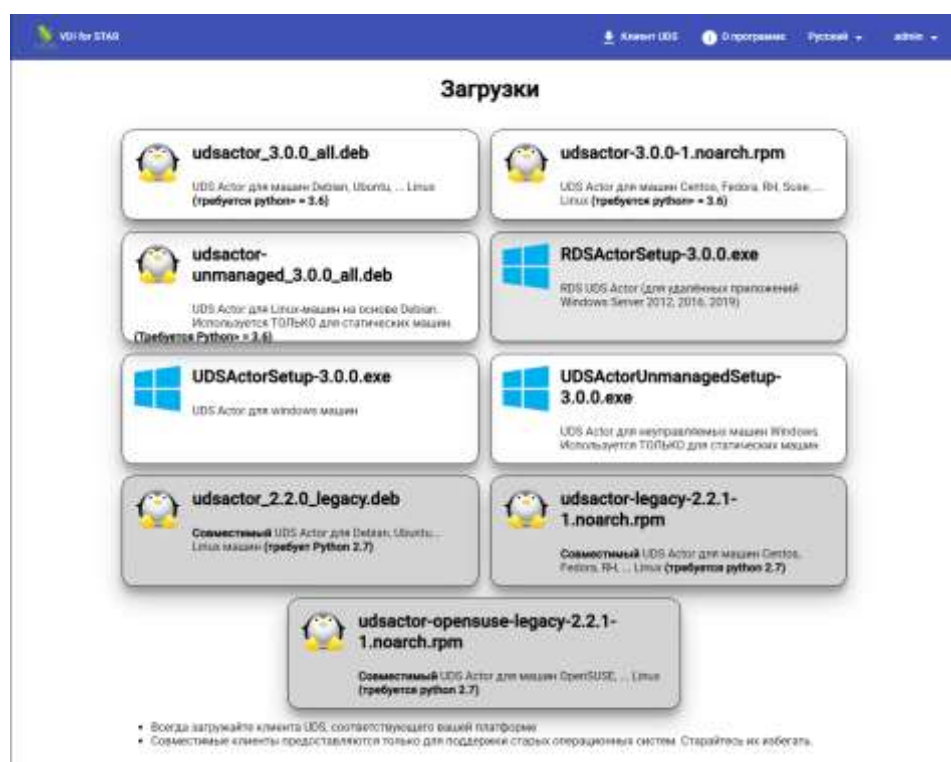


Рисунок 277

Он будет установлен на сервере Windows (Рисунок 278).

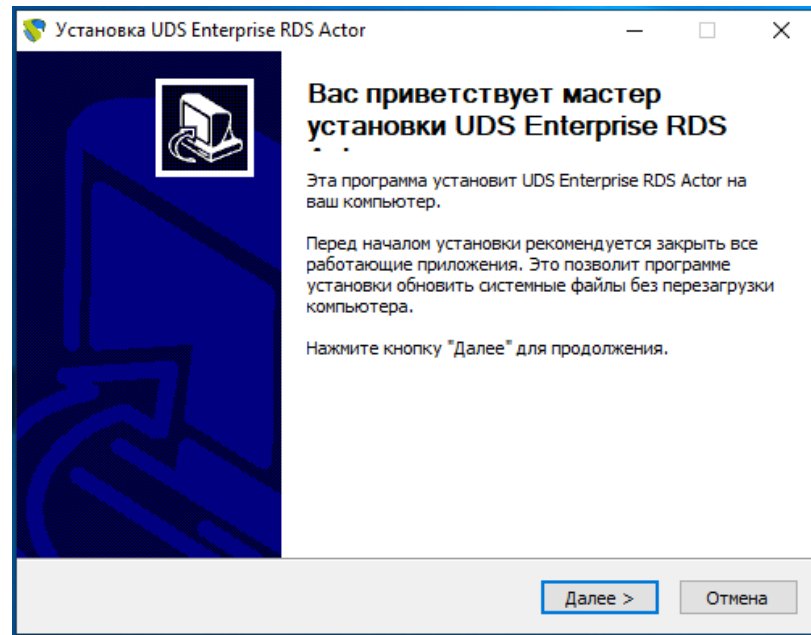


Рисунок 278

Необходимо принять Лицензионное соглашение (Рисунок 279).

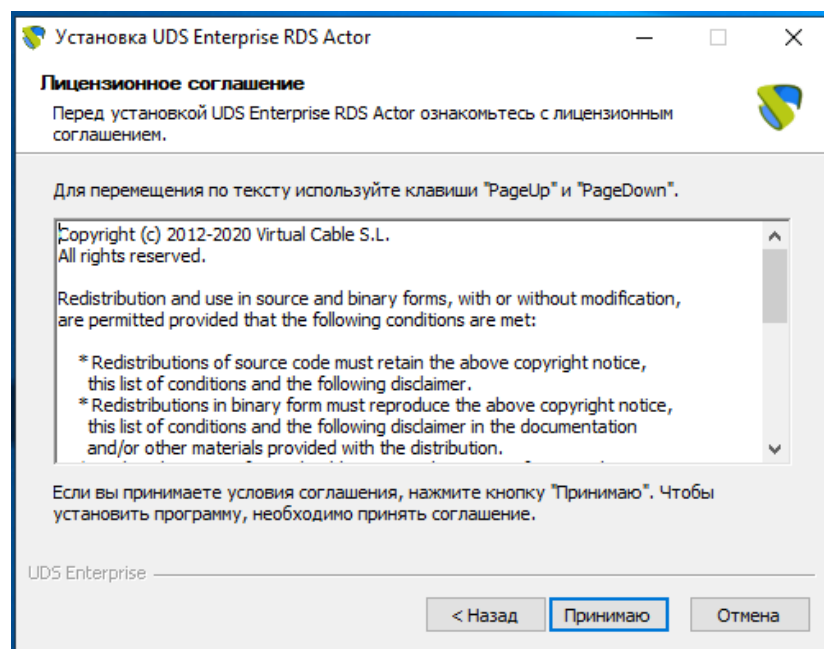


Рисунок 279

Выбрать место установки (Рисунок 280).

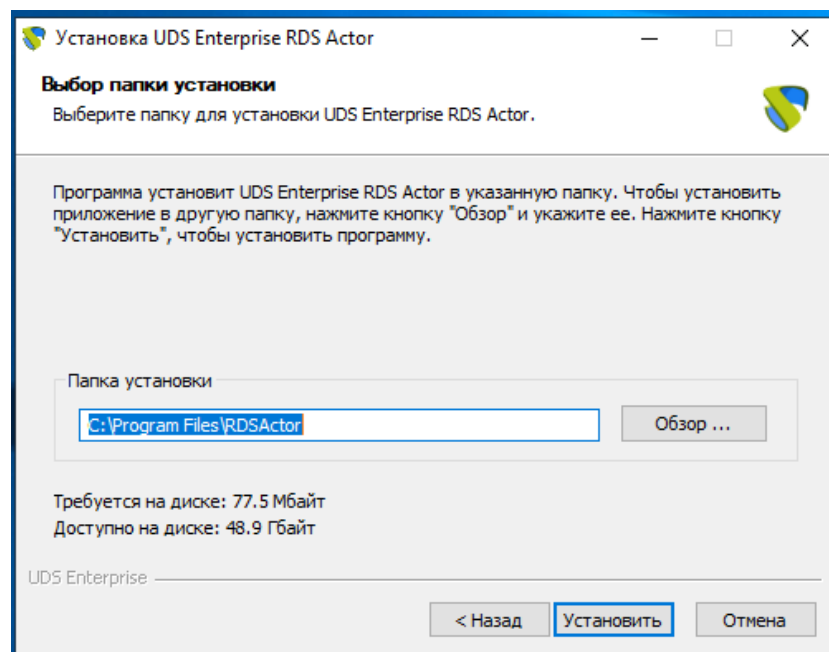


Рисунок 280

После завершения установки запустить VDI Actor (Рисунок 281).

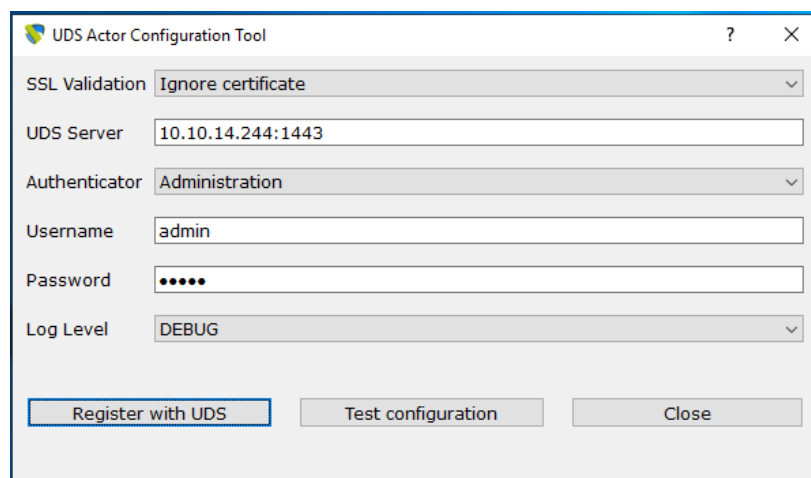


Рисунок 281

Зарегистрировать актера на сервере VDI, указав следующие параметры:

- SSL Validation: игнорировать сертификат \ верификационный сертификат.

- VDI Server: имя или IP-адрес VDI - сервера и порт (по умолчанию: 2637).
- Authenticator: Аутентификатор, 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 VDI Actor. Эти файлы журнала (VDIactor.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 VDI», чтобы зарегистрировать Actor на сервере VDI (Рисунок 282).

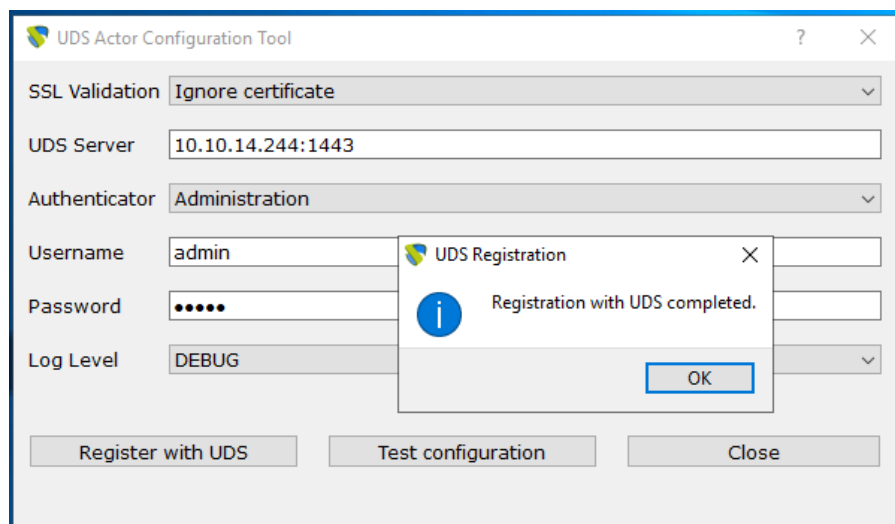


Рисунок 282

Нажать кнопку «Test configuration» для подтверждения правильности всех данных (Рисунок 283).

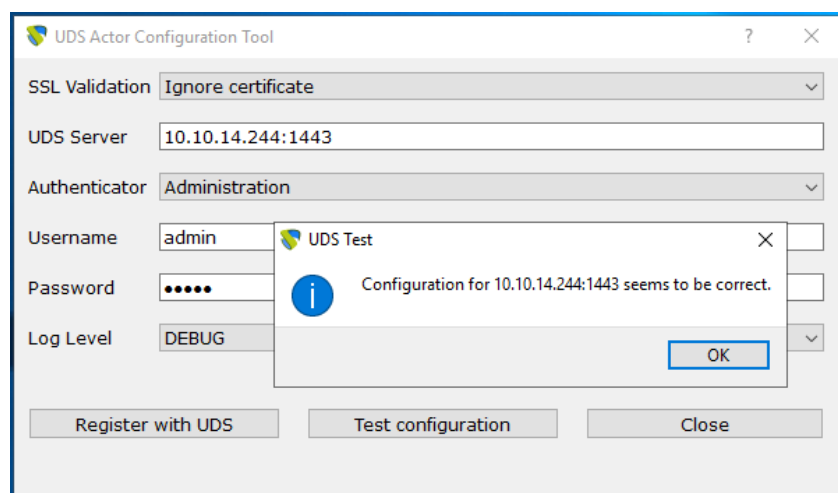


Рисунок 283

После установки участника VDI для серверов Windows RDS продолжить установку и настройку служб удаленных рабочих столов (Майкрософт).

Примечание: необходимо, чтобы в среде VDI был хотя бы один аутентификатор.

5.5 Установка и настройка RDS (Remote Desktop Service)

Установка службы удаленных рабочих столов (RDS) осуществляется следующим образом: «Диспетчер серверов» – «Управление» – «Добавить роли и компоненты» (Рисунок 284).

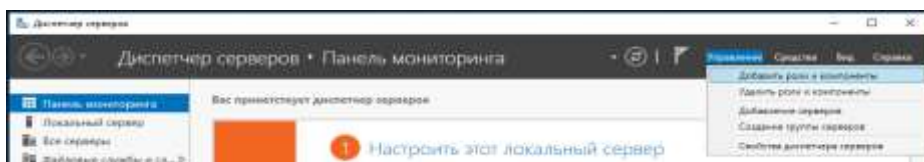


Рисунок 284

В мастере выполнить следующие действия:

- 1) Тип установки: «Установка служб удаленных рабочих столов» (Рисунок 285).

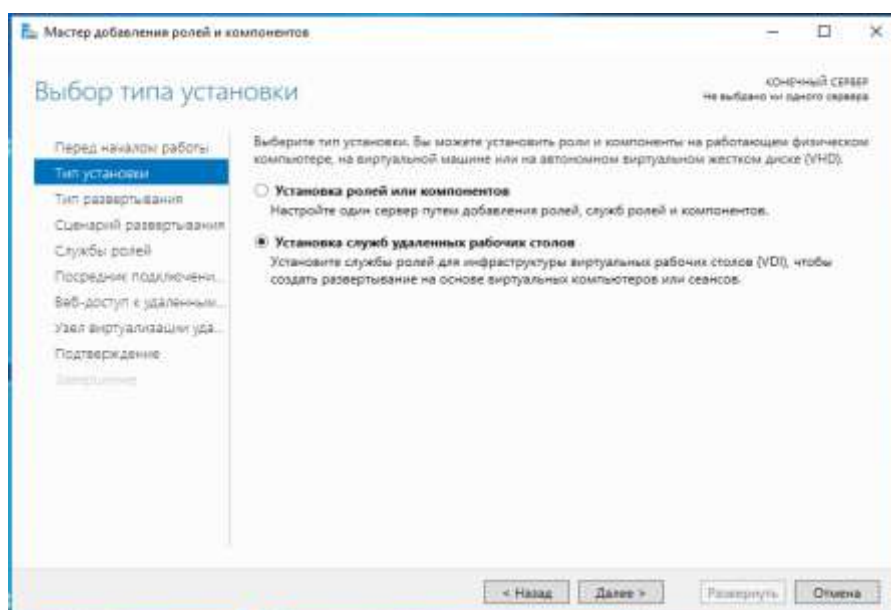


Рисунок 285

- 2) Тип развертывания: «Стандартное развертывание» (Рисунок 286).

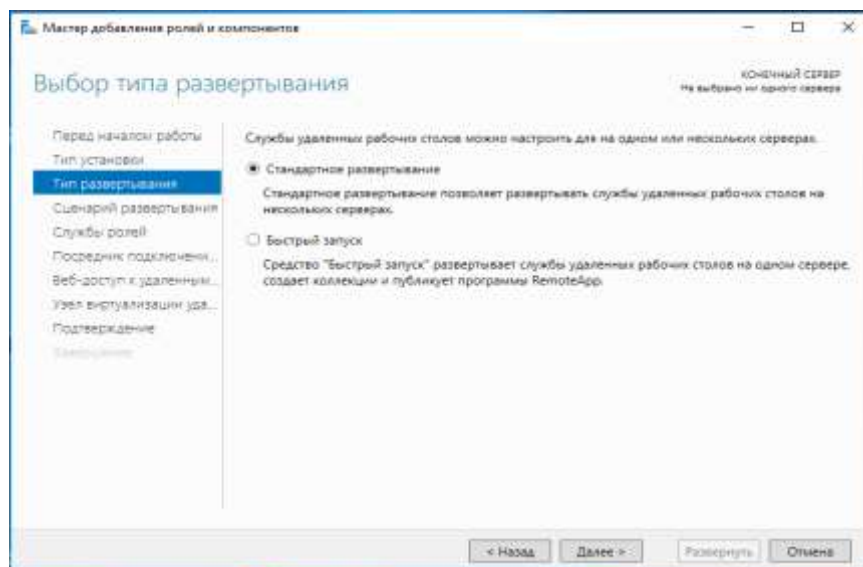


Рисунок 286

3) Сценарий развертывания: «Развертывание рабочих столов на основе сеансов» (Рисунок 287).

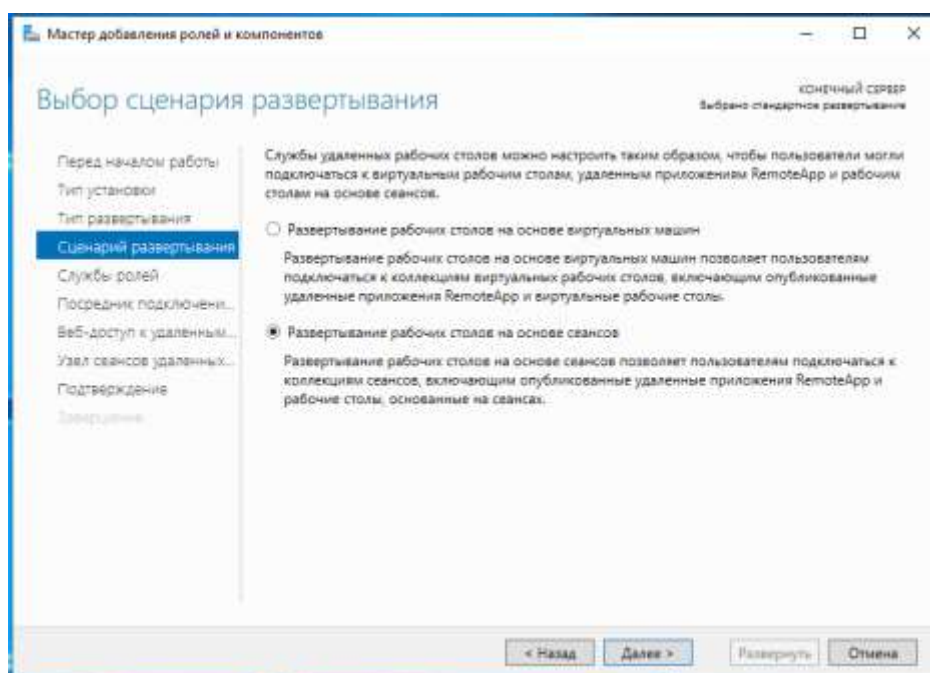


Рисунок 287

4) Появится сводная информация о том, что будет установлено (Рисунок 288)

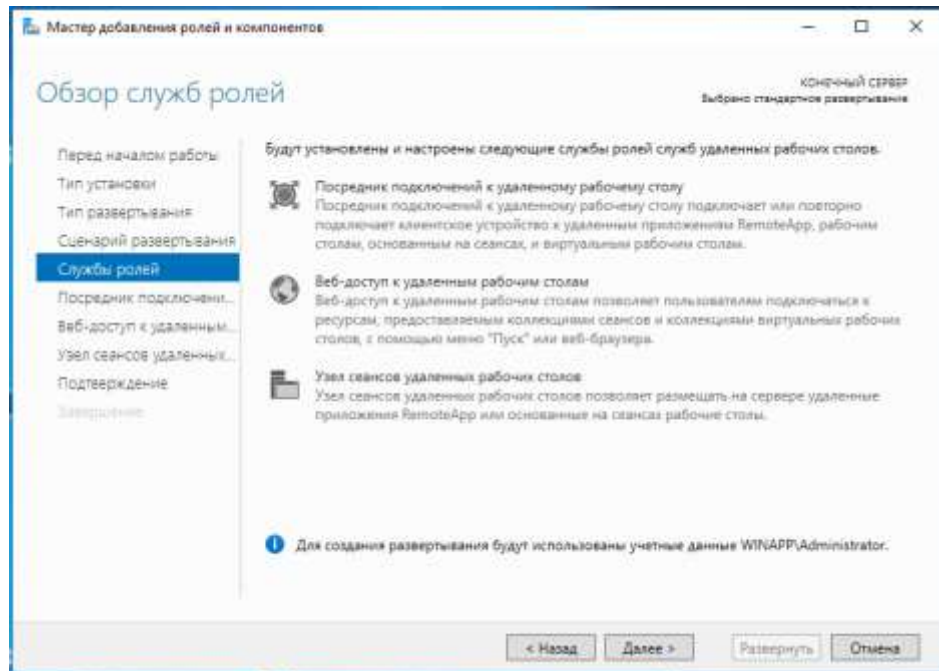


Рисунок 288

5) Должен быть указан сервер, на котором будет установлен каждый элемент (Рисунок 289).

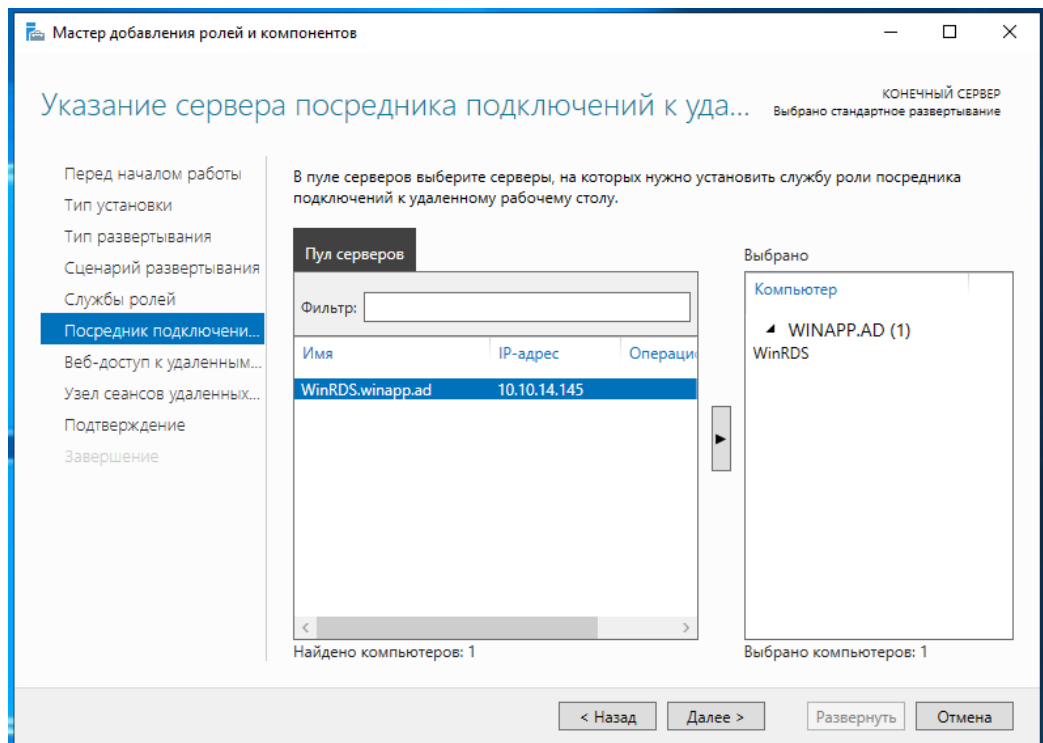


Рисунок 289

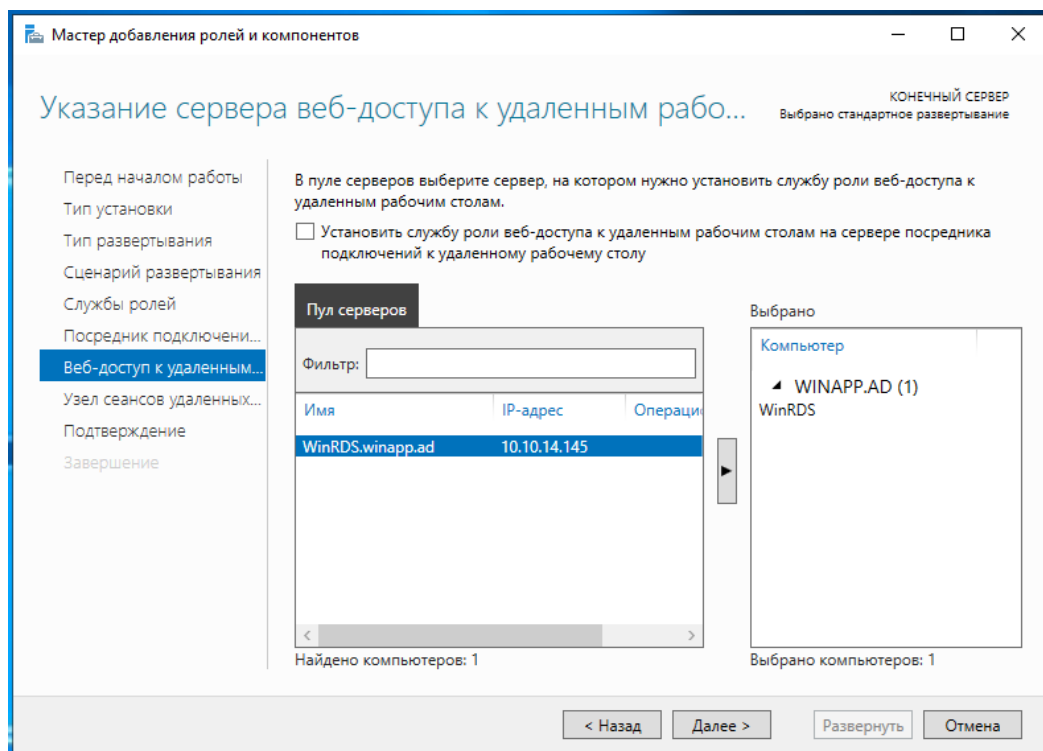


Рисунок 290

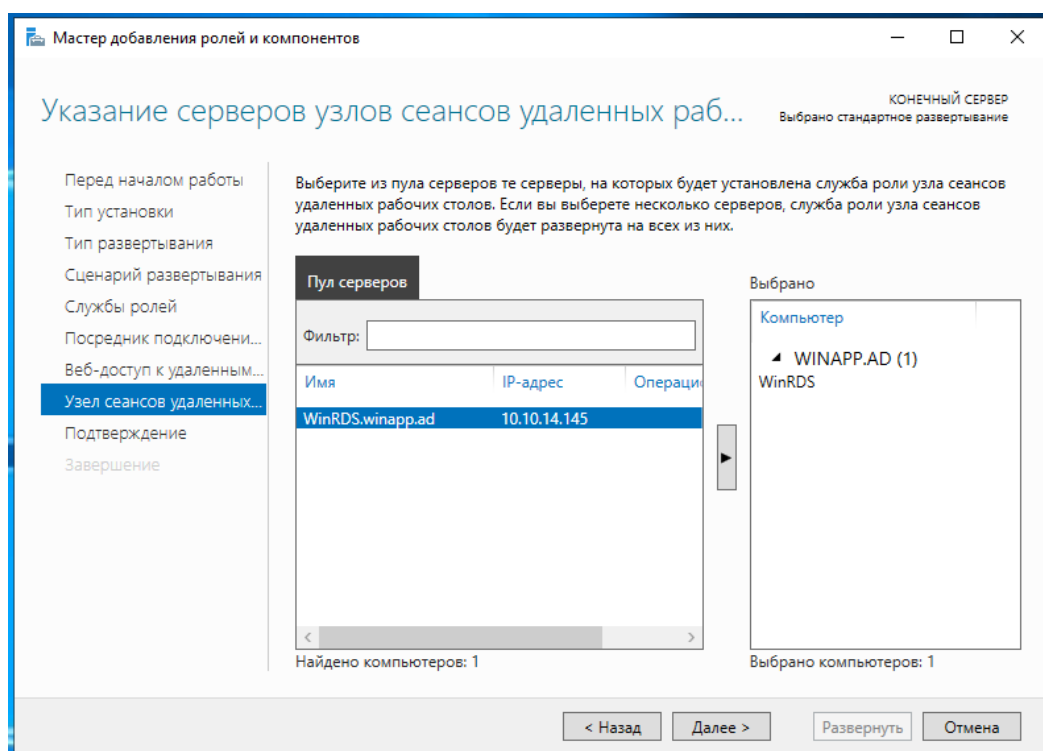


Рисунок 291

6) Установка подтверждается и выполняется ее развертывание (Рисунок 292):

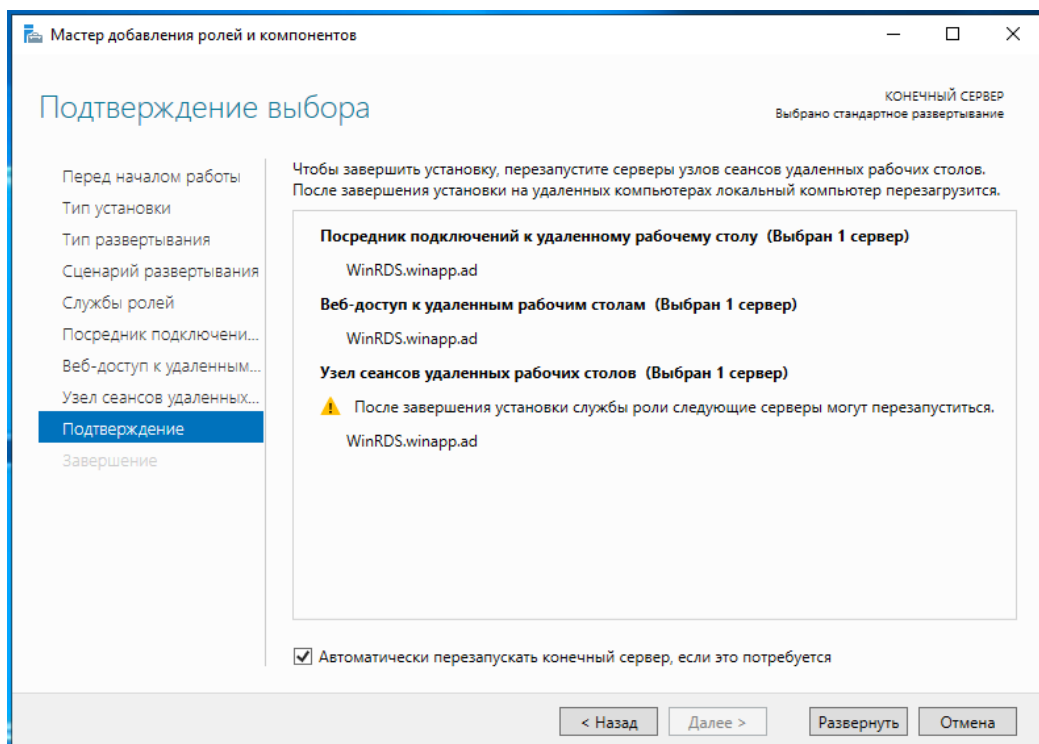


Рисунок 292

7) Сервер будет перезапущен автоматически (если вы это указали), и установка завершится (Рисунок 293).

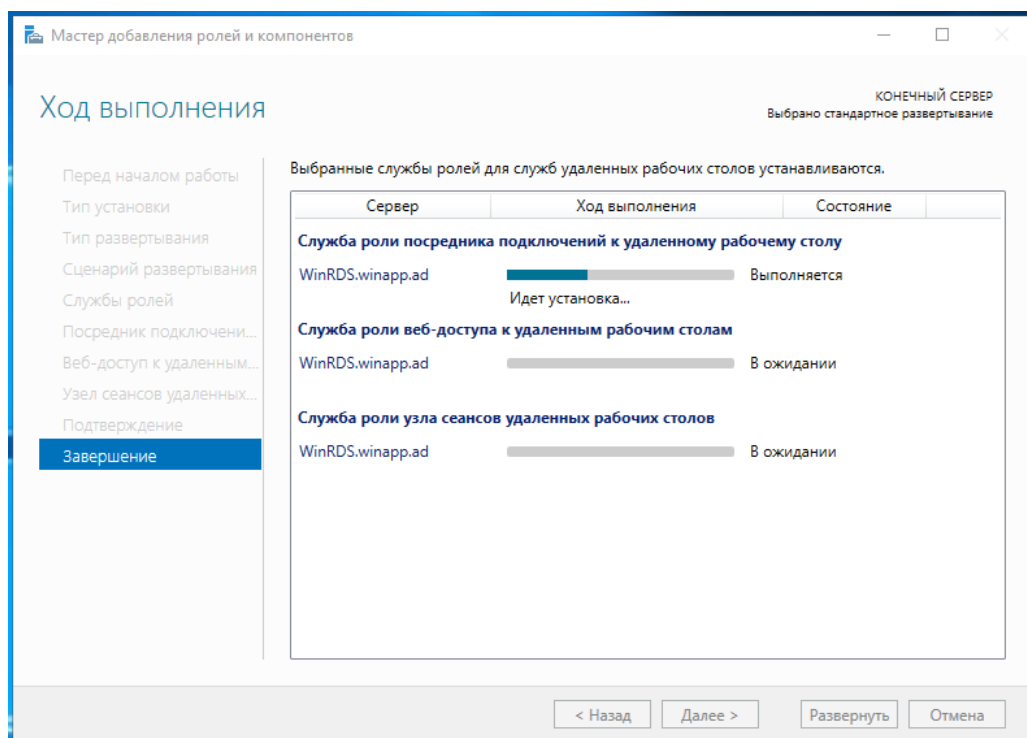


Рисунок 293

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 294).

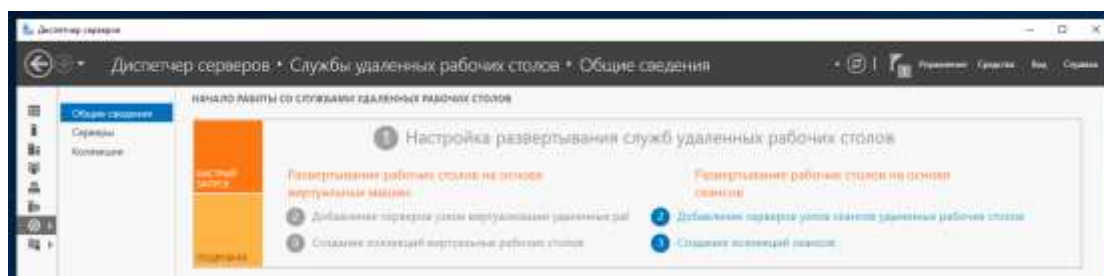


Рисунок 294

В мастере создания следует указать следующие данные. Указать имя для новой коллекции (Рисунок 295).

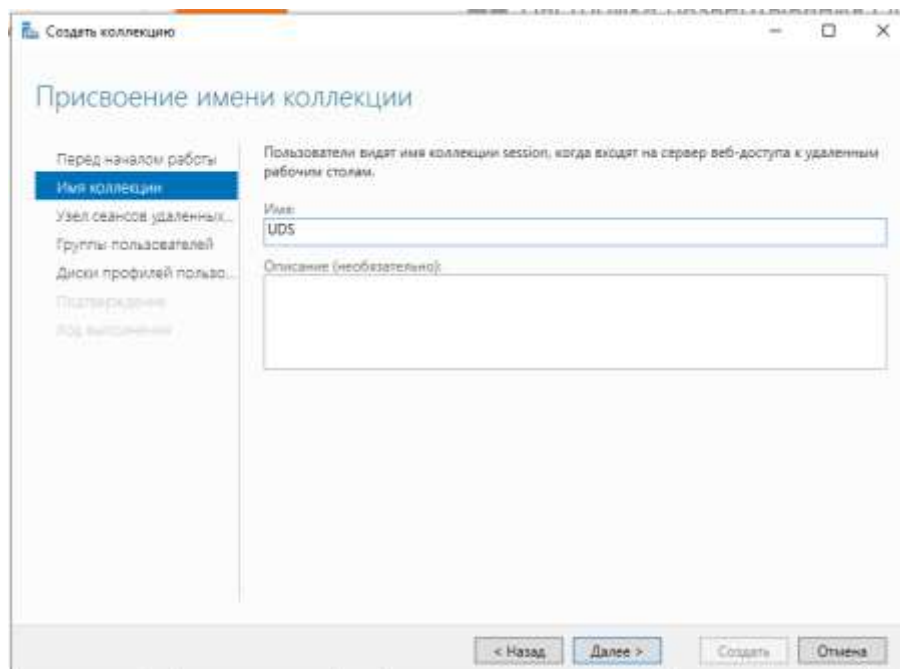


Рисунок 295

Добавить сервер в «Узел сеансов удаленных рабочих столов» (Рисунок 296):

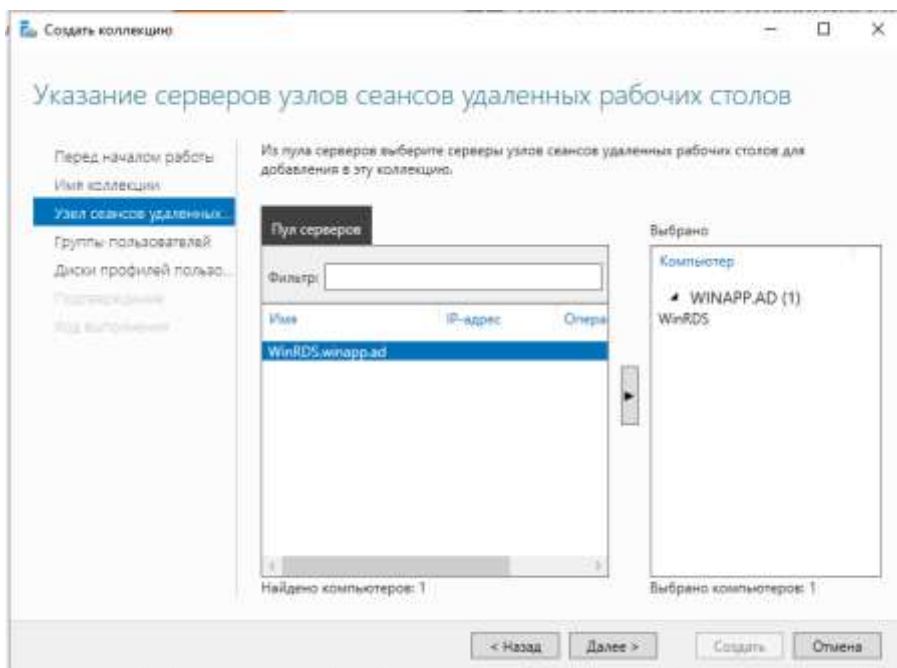


Рисунок 296

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 297).

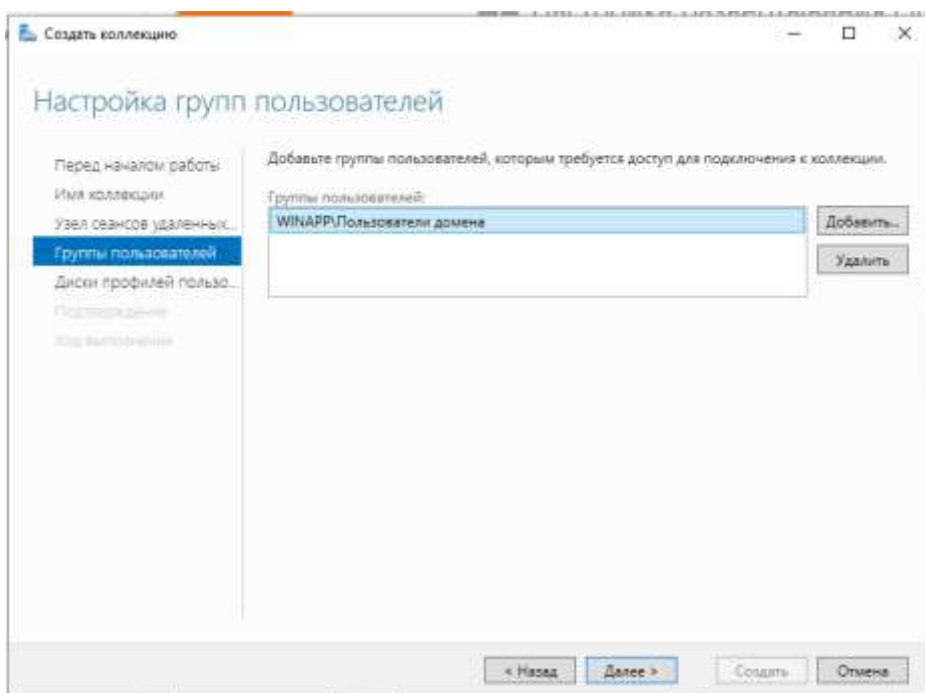


Рисунок 297

Указать, где будет храниться профиль пользователя. Если не указать, будет создан временный профиль, который будет удален при отключении пользователя (Рисунок 298Рисунок 298).

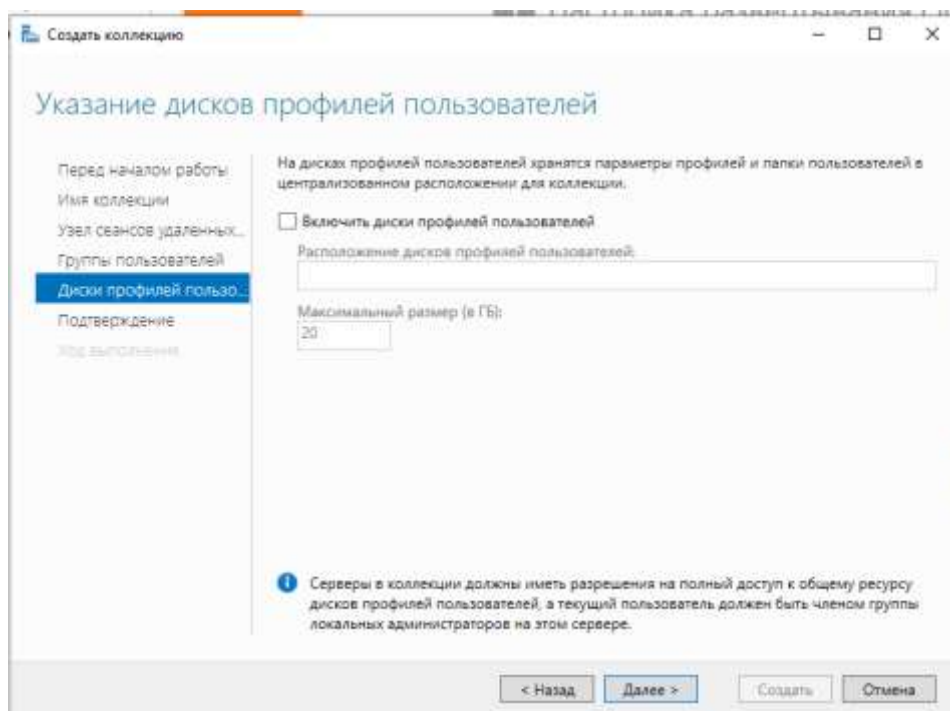


Рисунок 298

Подтвердить и создать коллекцию (Рисунок 299).

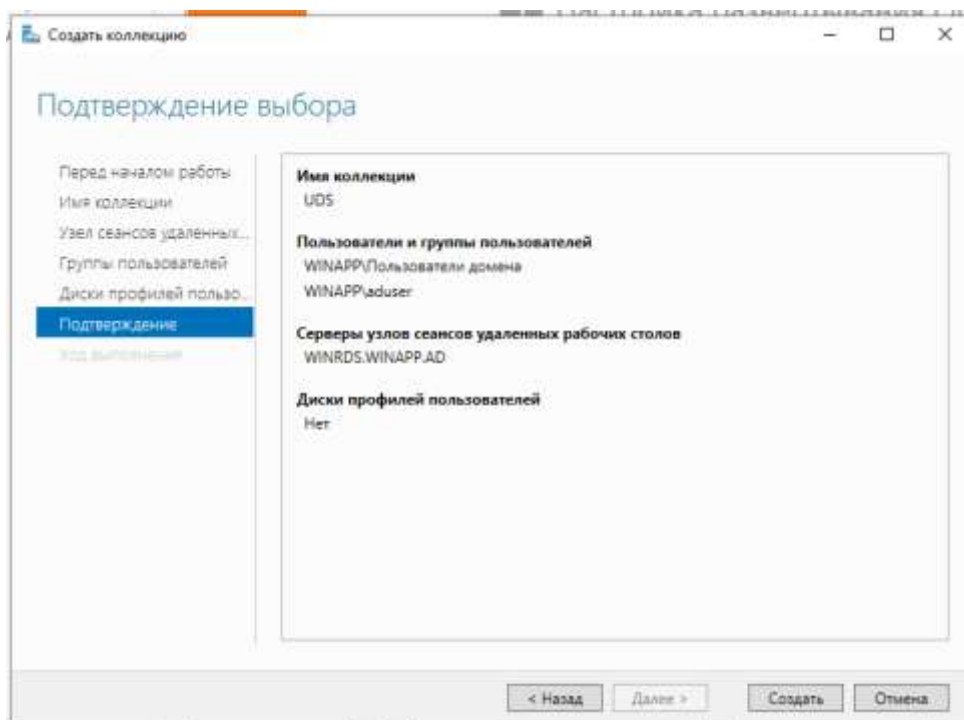


Рисунок 299

Публикация RDS Actor на RDS сервере. После создания коллекции выбрать «Опубликовать удаленные приложения RemoteApp» (Рисунок 300).

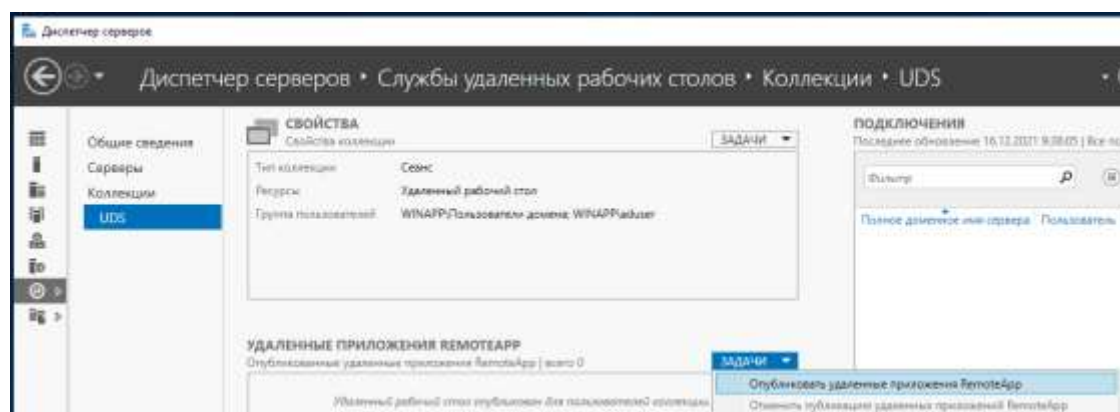


Рисунок 300

Необходимо добавить и выбрать исполнителя служб удаленных рабочих столов в списке «Удаленные приложения RemoteApp». Для этого необходимо предварительно установить VDI Actor для RDS.

Нажать кнопку «Добавить» и выбрать VDI Actor по пути (Рисунок 301)

C:\Program Files\RDSAActor\RDSAActor.exe

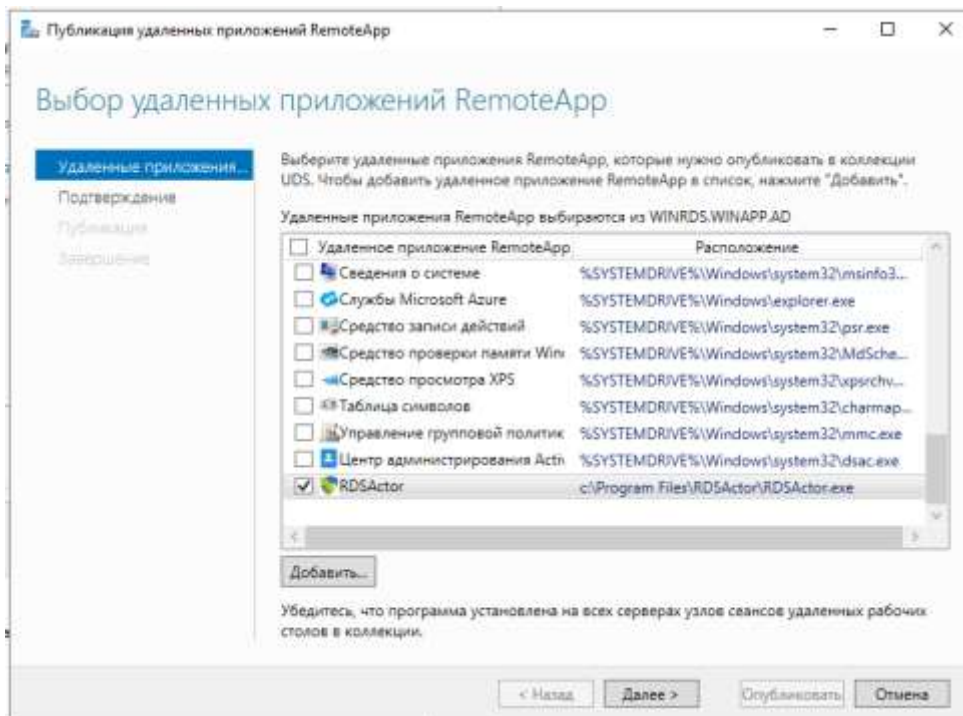


Рисунок 301

Подтвердить публикацию, нажать «Опубликовать» (Рисунок 302).

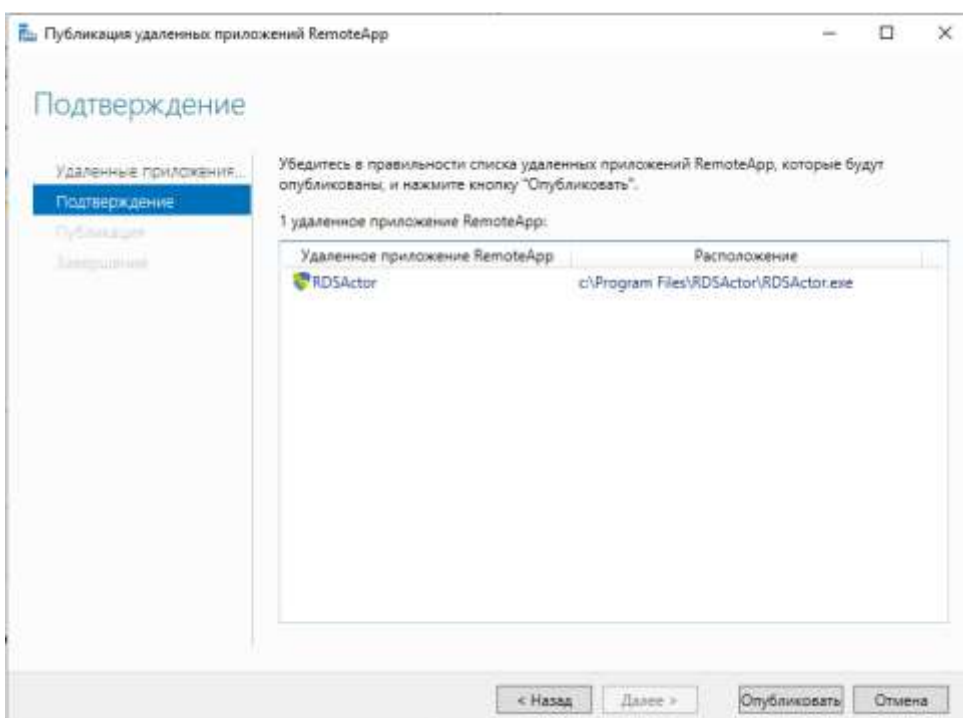


Рисунок 302

После создания отредактировать его свойства (Рисунок 303).

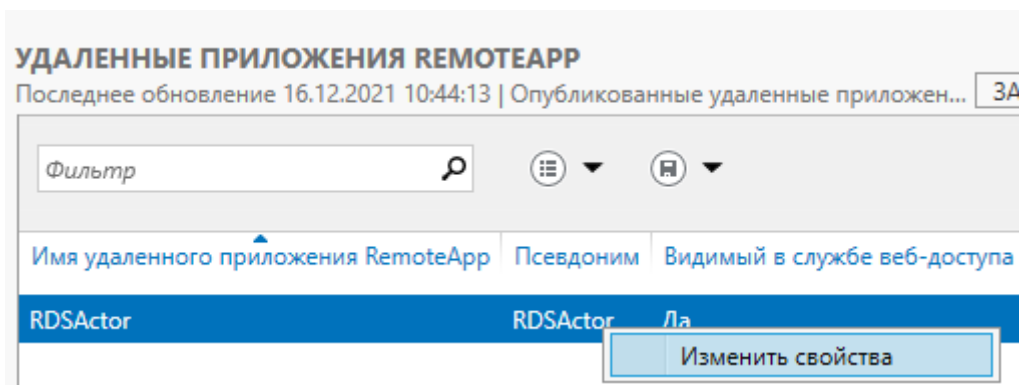


Рисунок 303

В разделе «Общие» отметить «Нет» в разделе «Показать удаленное приложение RemoteApp в веб-доступе к удаленным рабочим столам» (Рисунок 304Рисунок 304).

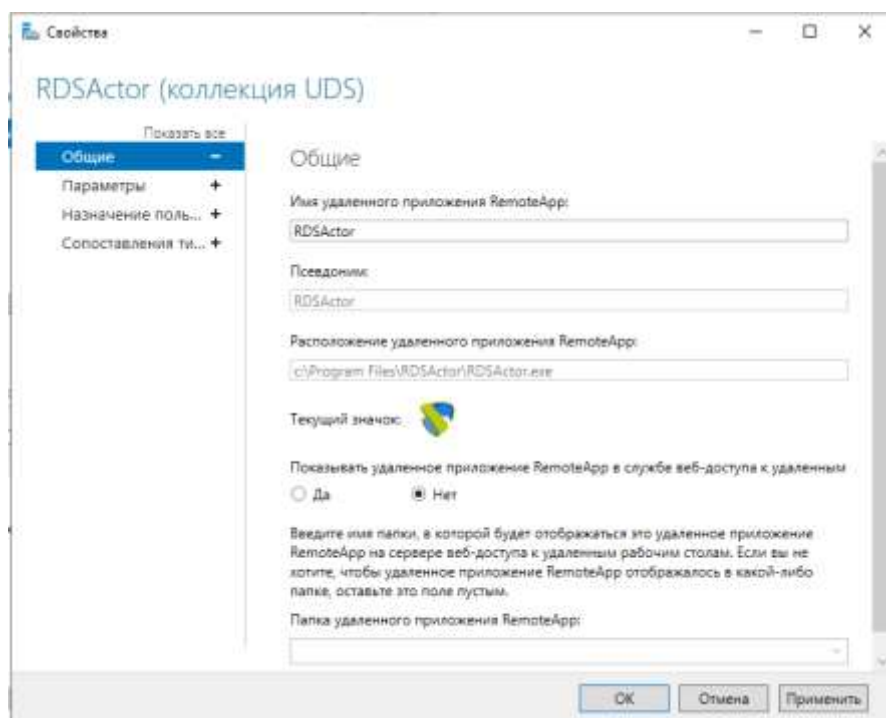


Рисунок 304

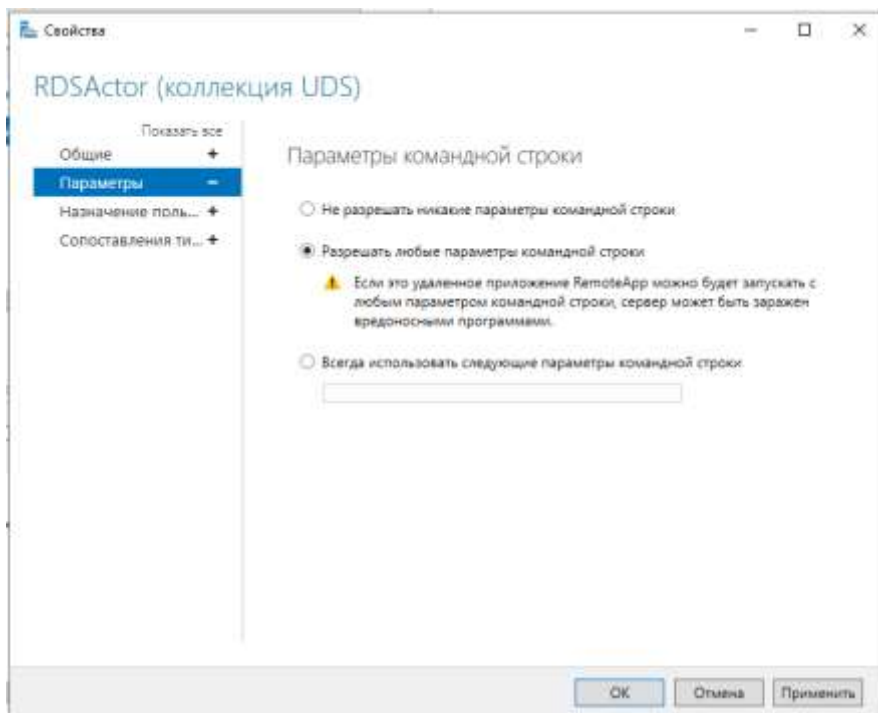


Рисунок 305

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 306):

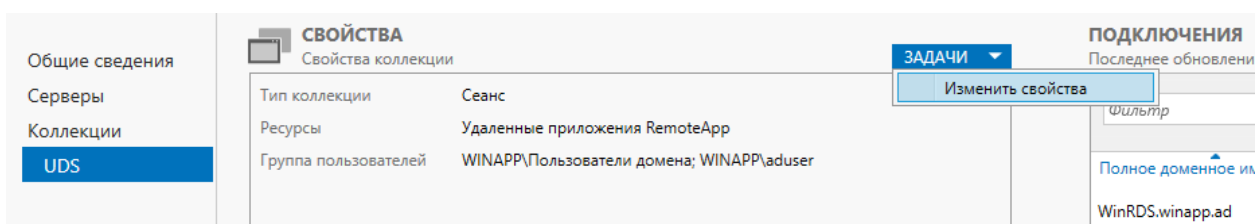


Рисунок 306

В разделе «Сеансы» указать минимальное время для «Окончание разъединенного сеанса» (Рисунок 307).

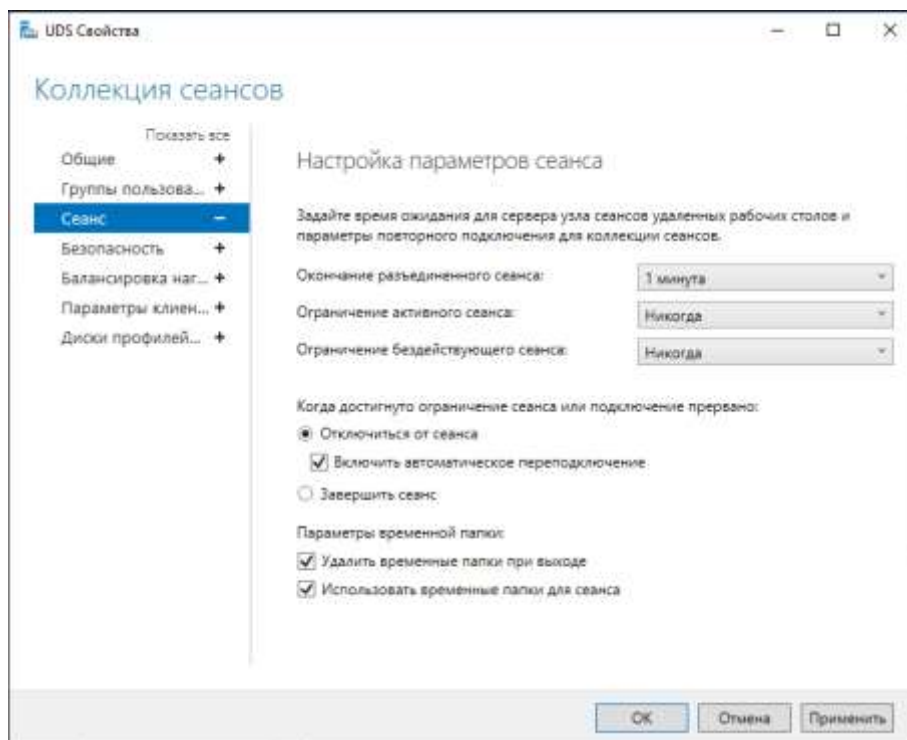


Рисунок 307

После выполнения всех этих шагов будет создан допустимый сервер RDS для подключения к серверу VDI и публикации виртуальных приложений для пользователей VDI.

3.6.7 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 308).



VDI

Имя пользователя *

Пароль

Аутентификатор

ad

Авторизоваться

Рисунок 308

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 309).

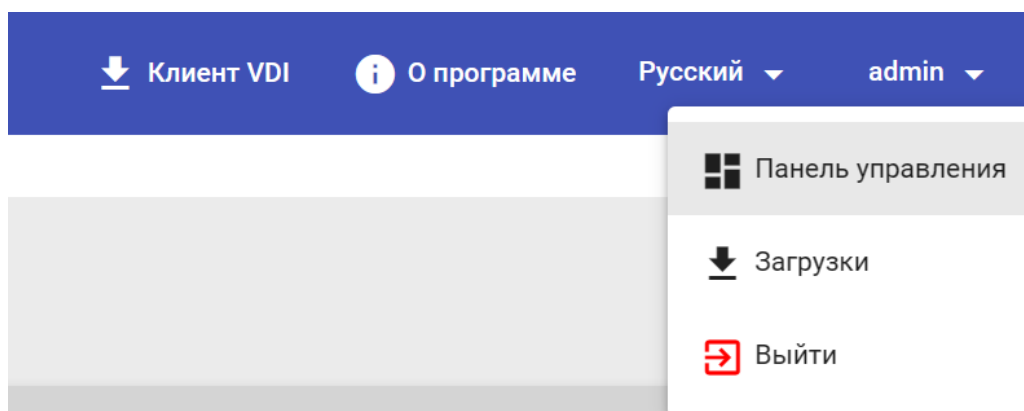


Рисунок 309

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.).

С главной страницы (Рисунок 310) осуществляется быстрый переход к следующим настройкам:

-*список аутентификаторов* по кнопке «Посмотреть аутентификаторы». VDI позволяет зарегистрировать несколько типов аутентификаторов, которые проверяют подлинность пользователя и предоставляют ему право на подключение к виртуальным столам и службам. Аутентификаторы бывают как внешние (OpenLDAP и т.д), так и внутренние (внутренняя база данных, IP-адрес аутентификация), подробнее о каждом из них написано в пункте 0;

-*список сервис-пулов* по кнопке «Просмотр пулов услуг». Создание пула услуг позволит развертывать настольные сервисы или виртуальные приложения, которые будут доступны различным группам пользователей (см. пункт 0).

Также на главной странице отображаются два графика – с таблицей назначенных услуг и таблицей используемых услуг.

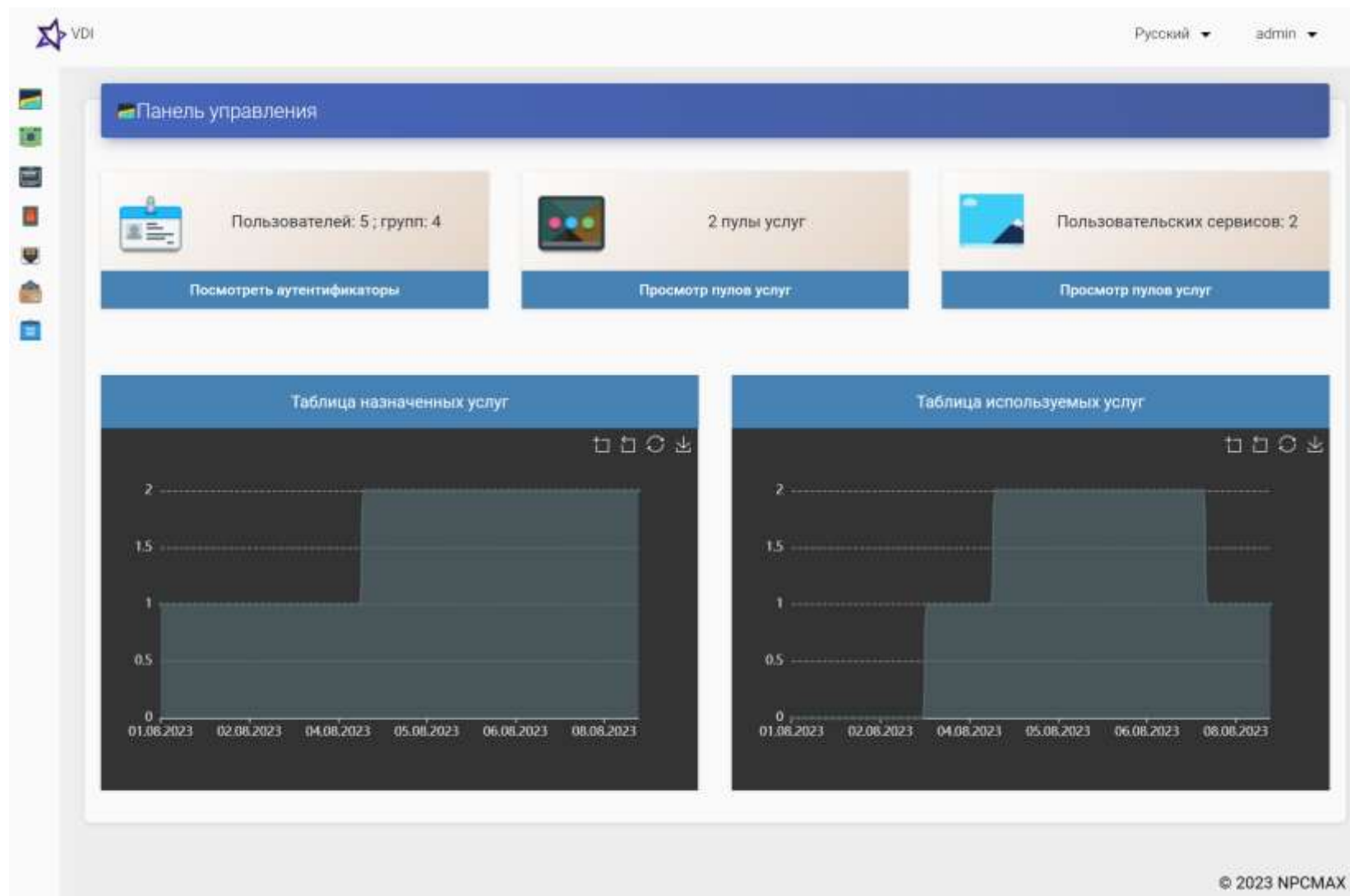


Рисунок 310

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 (Горизонт-ВС);

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 311).

Рисунок 311

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 312).

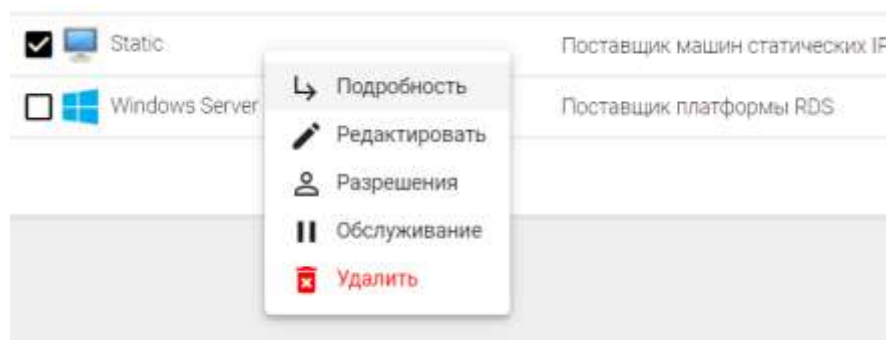


Рисунок 312

Конфигурирование службы на основе «Статистический множественный IP-адрес»

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 IP-адрес», выбрать вкладку «Поставщики услуг», нажать «Новый» и выбрать «Статистический множественный IP-адрес» (Рисунок 313).

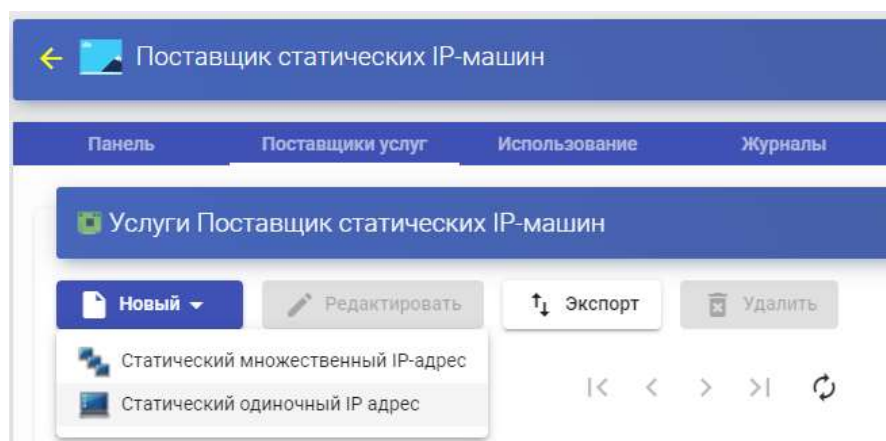


Рисунок 313

Откроется окно параметров настроек (Рисунок 314).

Рисунок 314

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 315).

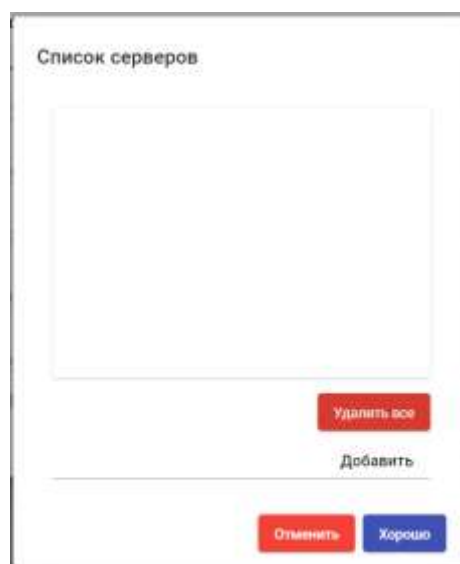


Рисунок 315

Ключ услуги (Рисунок 316) 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 VDI Actor, управляющий статическими машинами («VDIActorUnmanagedSetup-»....).

Новый сервис

Основной Расширенный

Тип
Тип этого элемента

Тип *

Static VDI

Комментарий
Комментарий этого элемента

Список серверов
10.10.14.18, 10.10.14.19

Ключ услуги
1234567890

Отменить и закрыть Сохранить

Рисунок 316

▪ Расширенный (Рисунок 317):

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.

Новый сервис

Основной Расширенный

Пропустить время *

15

Проверьте порт *

3389

Отменить и закрыть Сохранить

Рисунок 317

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 получают 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 318).

Рисунок 318

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 получают доступ к IP указанного устройства, начав новый сеанс.

Поставщик платформы VMware vSphere

Позволяет развёртывать виртуальные рабочие столы, созданные VDI самостоятельно, в инфраструктуре виртуализации VMware vSphere.

Нажать «новый» и выбрать «поставщик платформы VMware vCenter» (Рисунок 319)

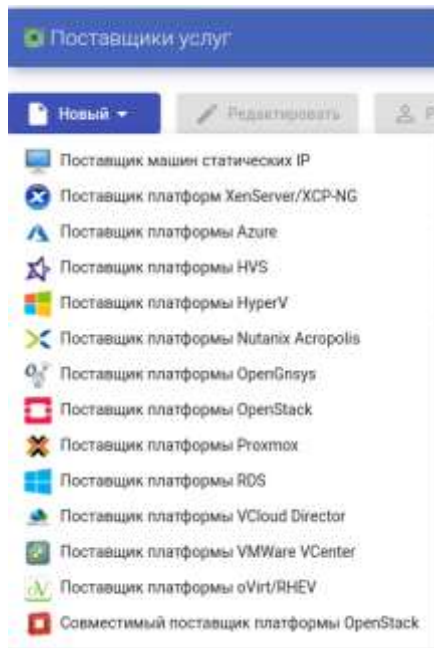


Рисунок 319

В «Поставщике платформы VMware vCenter» необходимо настроить следующие минимальные параметры в разделе «Основной» (Рисунок 320) и «Расширенный» (Рисунок 320):

Имя: имя поставщика услуг.

Хост: IP-адрес сервера vCenter.

Порт: порт подключения к центру.

Имя пользователя, пароль.

Новый поставщик

Основной Расширенный

Тип

Имя *

vs

Комментарий

Хост *

10.10.10.17

Порт *

443

Имя пользователя *

Administrator@vs.ipromax.ru

Пароль *

Проверить Отменить и закрыть Сохранить

Рисунок 320

Одновременное создание: Количество одновременных задач по созданию рабочего стола.

Одновременное удаление: Количество одновременных задач удаления с рабочего стола.

Таймаут: «Тайм-аут» для соединения с vCenter.

Максимальный диапазон: Диапазон MAC-адресов, используемых VDI для создания виртуальных рабочих столов.

Новый поставщик

Основной **Расширенный**

Одновременное создание *

15

Одновременное удаление *

8

Таймаут *

30

Максимальный диапазон *

00:50:56:10:00:00-00:50:56:3F:FF:FF

Включите виртуальные машины на кэше L2

☐ Нет

Проверить Отменить и закрыть Сохранить

Рисунок 321

Нажав «Проверить», можно протестировать и убедиться, что соединение прошло успешно. После сохранения конфигурации будет создан сервис «Поставщики услуг» чтобы начать регистрацию базовых сервисов платформы VMware vSphere.

Для изменения параметров в уже существующем сервисе «поставщики услуг», нужно выбрать необходимый сервис и нажать «редактировать». Выбрав «Войти в режим обслуживания», можно приостановить все операции выполняемые VDI Broker для данного поставщика услуг. Рекомендуется переводить поставщика услуг в режим обслуживания при разрыве соединения или для прекращения обслуживания.

Как только платформа VMware vSphere будет интегрирована в VDI, могут быть созданы различные типы базовых сервисов. Для этого нужно нажать правой кнопкой мыши на созданный поставщик услуг и выбрать «Подробность» в меню провайдера (Рисунок 322).

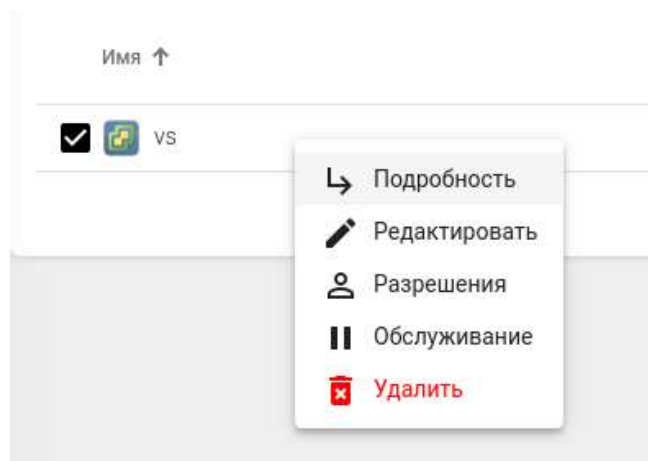


Рисунок 322

Будут доступны следующие типы базовых услуг (Рисунок 323):

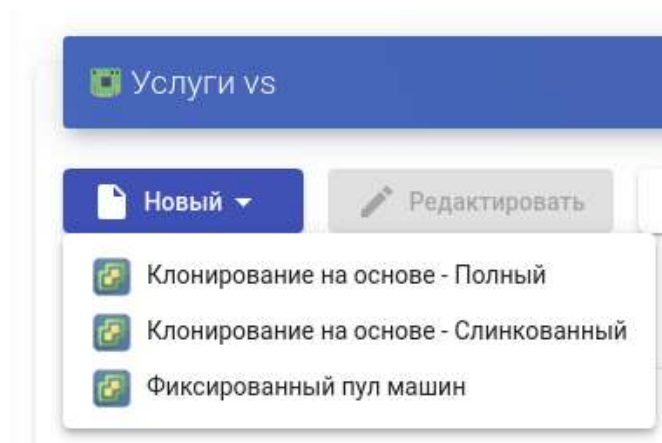


Рисунок 323

Примечание: для создания любой из базовых служб, поддерживаемых VDI, вам потребуется выбрать минимум одну виртуальную локальную сеть для подключения виртуальных машин, хранилище данных для хранения публикаций и виртуальных рабочих столов, а также папку в «Виртуальные машины и шаблоны». Если нет одного из этих элементов можно получить следующую ошибку (Рисунок 324):

Error handling your request

Error 500: VMWare services needs that vCenter contains at least one folder, one network and one datastore.

Close

Рисунок 324

Настройка через сервис «Клонирование на основе - Полный»

Этот тип сервиса позволит создать в рамках виртуальной инфраструктуры полноценные виртуальные рабочие столы, независимые от активной публикации.

Для создания базовых сервисов типа «Клонирование на основе — Полный» нужно перейти в «Поставщики услуг», далее правой кнопкой мыши нажать по нужной «услуге», перейти в «Подробности», нажать «Новый» и выбрать «Клонирование на основе — Полный» (Рисунок 325).

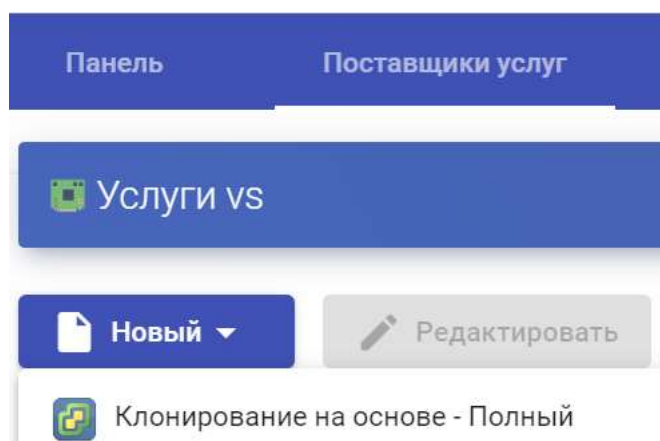


Рисунок 325

В «Клонировании на основе — Полный» необходимо настроить следующие минимальные параметры в разделах “Основной” (Рисунок 326), “Машина” (Рисунок 327) и “Расширенный” (Рисунок 328):

Имя: название службы.

Центр обработки данных: центр обработки данных среды VMware vSphere для размещения службы.

Продолжить при ошибке: при активации система игнорирует все ошибки доступа к службе.

Публичный пул ресурсов: местоположение, в котором будет храниться служебная публикация. Можно выбрать одно, несколько или все доступные хранилища данных. В случае выбора нескольких, система всегда будет размещать новые публикации в хранилище данных, в котором больше свободного места.

Удалить найденные дубликаты: если эта опция активирована (значение по умолчанию), когда VDI обнаружит виртуальный рабочий стол с тем же именем (и созданный VDI), что и рабочий стол, который запланировано создать, он удалит его

(рекомендуется его использование, чтобы избежать существования «потерянных» виртуальных машин в инвентаре vCenter).

Рисунок 326

Новый сервис

Основной Машина Расширенный

Тип

Теги этого элемента

Имя *

Имя этого элемента

Комментарий

Комментарий этого элемента

Центр обработки данных *

Datacenter

Публичный пул ресурсов *

e0.vtmw.acbfg.ru

Публичная вилка *

Хранилище данных, где размещать публикации

Продолжить

☐ Нет

☒ Да

Удалить найденные дубликаты

Отменить и закрыть Сохранить

Пул ресурсов: пул ресурсов vCenter, в котором находится шаблон виртуальной машины (золотой образ), который будет использоваться службой.

Базовая машина: шаблон виртуальной машины (золотой образ), используемый системой VDI для развертывания виртуальных рабочих столов.

Память: объем памяти в Мб, который будет назначен созданным виртуальным «Полным клоном».

Основная сеть: сеть связи участника VDI с сервером VDI. Она так же определит сетевой интерфейс для изменения в созданных виртуальных рабочих столах.

Публичная сеть: сеть, к которой будут подключаться виртуальные рабочие столы.

Папка клонов: папка, в которой новые виртуальные рабочие столы будут добавлены в «Виртуальные машины и шаблоны».

Хранилища данных ВМ: место, где будут храниться виртуальные рабочие столы. Можно выбрать одно, несколько или все хранилища данных. В случае выбора нескольких, система всегда будет размещать новые виртуальные рабочие столы в хранилище данных, где больше свободного места.

Имена машин: корневые имена всех виртуальных рабочих столов «Полных клонов», которые будут развернуты в этой службе.

Длина имени: количество цифр счётчика, прикрепленного к корню имени рабочего стола (например, длина имени = 3. Конечным именем сгенерированных рабочих столов будет: Win10-full000, Win-full001...Win-full999).

Новый сервис

Основной Машина Расширенный

Путь ресурса *
e0.vmmw.sobfg.ru

Имя машины *
Astra1.7

Емкость (МБ) *
512

Основная сеть *

Публичная сеть

Путь клонов *
/Discovered virtual machine

Хранилище данных ВМ *
Хранилища, которые используются машинами

Имя машины *
Базовое имя для клонов этой машины

Длина имени *
3

Отменить и закрыть Сохранить

Рисунок 327

Зарезервированное место: когда в хранилище данных меньше свободного места чем указано в этом параметре (в Гб), VDI не будет использовать его для размещения публикаций или виртуальных рабочих столов.



Новый сервис

Основной Машина Расширенный

Зарезервированное место *

32

Отменить и закрыть Сохранить

Рисунок 328

Сохранение конфигурации в последствии создает услугу «Клонирование на основе — Полный» на платформе VMware vCenter (Рисунок 329).

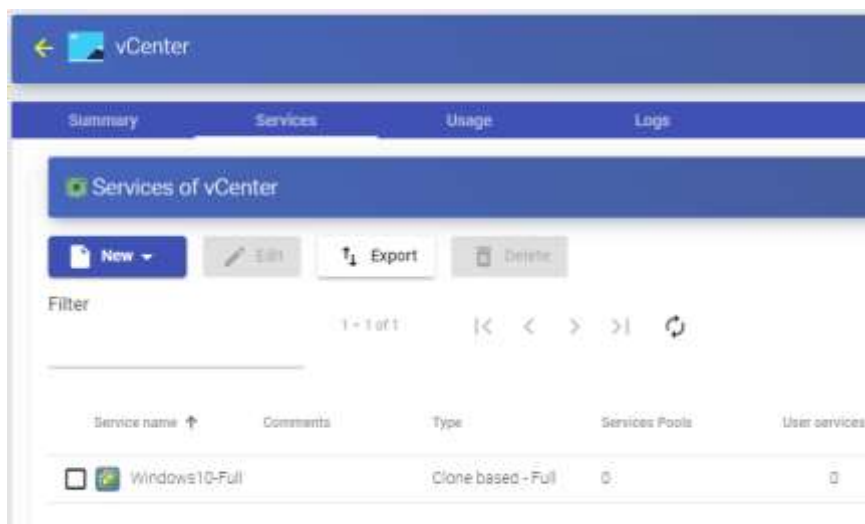


Рисунок 329

Как только будет настроена полная среда VDI (службы, средства аутентификации, менеджеры ОС и транспорт) и первый «Сервисный пул» можно будет наблюдать, как виртуальные рабочие столы, основанные на связанных клонах VMware, развертываются на сервере vCenter.

Первой задачей, которую выполнит vCenter, будет создание базового компьютера (этот компьютер будет создаваться каждый раз, когда делается

публикация сервиса), который будет клоном шаблона, выбранного при регистрации сервиса, с размером жесткого диска и функциями указанным в шаблоне. Как только процесс клонирования базовой машины будет завершён, его виртуальные рабочие столы автоматически создаются в vCenter.

Примечание: дисковое пространство, которое будут занимать виртуальные рабочие столы («Полные клоны») такие же, как и на компьютере с шаблоном.

Настройка через сервис «Клонирование на основе - Слинкованный»

Этот тип сервиса создаст в виртуальной инфраструктуре виртуальные рабочие столы в режиме связанного клонирования в зависимости от активной публикации.

Для создания базовых сервисов типа «Клонирование на основе — Слинкованный» перейдите в раздел «Поставщики услуг», выберите «Услуги» перейдите в неё и нажмите на «Новый» и выберите «Клонирование на основе - Слинкованный»:

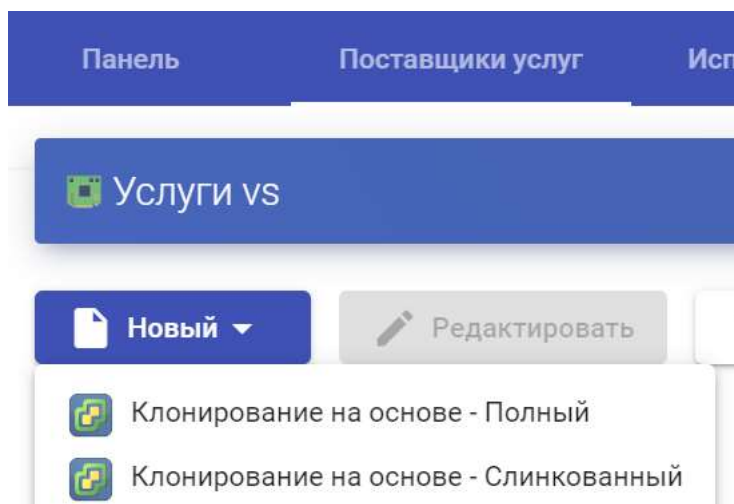


Рисунок 330

В режиме «Клонирование на основе — Слинкованный» минимальными параметрами, которые необходимо настроить, являются:

На вкладке «Основной» (см. Рисунок 331Рисунок 331):

- **Имя:** название службы.
- **Центр обработки данных:** центр обработки данных среды VMware vSphere для размещения службы.
- **Публичный пул ресурсов:** пул ресурсов vCenter, в котором будут размещены публикации и виртуальные рабочие столы (если пулы недоступны в инфраструктуре VMware, они будут созданы в корневом каталоге).
- **Публичные хранилища:** местоположения, в котором будут храниться служебные публикации. Вы можете выбрать одно, несколько или все доступные хранилища данных. В случае выбора нескольких, система всегда будет размещать новые публикации в хранилище данных, в котором будет больше свободного места.
- **Продолжайте:** при активации система игнорирует все ошибки доступа к службе.
- **Удалить найденные дубликаты:** если эта опция активирована (значение по умолчанию), когда VDI обнаружит виртуальный рабочий стол с тем же именем что и рабочий стол, который вы собираетесь создать, он удалит его.

Новый сервис

Основной	Машина	Расширенный
Теги		
Теги этого элемента		
Имя *		
Имя этого элемента		
Комментарии		
Комментарии этого элемента		
Центр обработки данных *		
Datacenter		
Публичный пул ресурсов *		
e2.vmw.aobfg.ru		
Публичные хранилища *		
Хранилища данных, где размещать публикации		
Продолжайте		
☐ Нет		
Удалить найденные дубликаты		
☒ Да		
Отменить и закрыть		Сохранить

Рисунок 331

На вкладке «Машина»:

- **Пул ресурсов:** пул ресурсов vCenter, в котором находится шаблон виртуальной машины (золотой образ), который будет использоваться службой.
- **Базовая машина:** шаблон виртуальной машины используемый VDI для развертывания виртуальных рабочих столов.
- **Память:** объем памяти в Мб, который будет назначен созданным виртуальным «Full clones».
- **Основная сеть:** ...

- **Публичная подсеть:** сеть, к которой будут подключаться виртуальные рабочие столы.
- **Папка клонов:** папка, в которой будут новые виртуальные рабочие столы будут зарегистрированы в «Виртуальные машины и шаблоны».
- **Inc.Datastores:** место, где будут храниться созданные виртуальные рабочие столы. Вы можете выбрать одно, несколько или все хранилища данных. В случае выбора нескольких, система будет размещать новые виртуальные рабочие столы в том хранилище данных, где больше места.
- **Имена машин:** корневые имена всех связанных виртуальных рабочих столов клонов, которые будут развернуты в этой службе.
- **Длина имени:** количество цифр счётчика, прикрепленного к корню имени рабочего стола (например, длина имени = 3. Конечным именем сгенерированных рабочих столов будет: Win10-full000, Win10-full001...Win10-full999).

Новый сервис

Основной	Машина	Расширенный
Пул ресурсов *		
e2.vmw.aobfg.ru		▼
Базовая машина *		
VMware vCenter Server		▼
Память (Мб) *		
512		
Основная сеть *		
		▼
Публичная подсеть		
		▼
Папка клонов *		
/Discovered virtual machine		▼
Inc.Datastores *		
Хранилища данных, где добавлены инкременты		▼
Имена машин *		
Базовое имя для клонов этой машины		
Длина имени *		
3		

Отменить и закрытьСохранить

Рисунок 332

На вкладке «Расширенный»:

- **Зарезервированное место:** когда в хранилище данных меньше свободного места чем указано в этом параметре (в Гб), VDI не будет использовать его для размещения публикаций или виртуальных рабочих столов.

Новый сервис

Основной

Машина

Расширенный

Зарезервированное место *

32

Отменить и закрыть

Сохранить

Рисунок 333

Сохраните конфигурацию и у вас будет создан сервис «Клонирование на основе - Слинкованный» на платформе VMware vCenter:

Панель

Поставщики услуг

Использование

Журналы

Услуги vs

Новый

Редактировать

Экспорт

Удалить

Фильтр

1 - 2 of 2

Имя сервиса	Комментарии	Тип	Сервисные пулы	Сервисы пользователя
☐ test		Клонирование на основе - Полный	0	0
☐ Windows10-Full		Клонирование на основе - Слинкованный	0	0

Рисунок 334

Как только будет настроена полная среда VDI (службы, средства аутентификации, менеджеры ОС и транспорт) и первый «Сервисный пул», вы сможете наблюдать, как виртуальные рабочие столы, основанные на связанных клонах VMware, развертываются на сервере vCenter. Первой задачей, которую выполнит vCenter, будет создание базового компьютера (этот компьютер будет создаваться каждый раз, когда вы делаете публикацию сервиса), который будет клоном шаблона, выбранного при регистрации сервиса, с размером жесткого диска

и функциями, указанным в шаблоне. Как только процесс клонирования базовой машины будет завершён, его виртуальные рабочие столы автоматически создаются в vCenter.

Примечание: дисковое пространство, которое будут занимать виртуальные рабочие столы («Слинкованные клоны») такое же, как и на компьютере с шаблоном.

Конфигурация сервиса, основанного на «Фиксированный пул машин»

Этот тип сервиса позволит напрямую подключать пользователей к существующим виртуальным машинам в среде VMware vSphere.

Для создания сервиса «Фиксированный пул машин» необходимо перейти в «Поставщики услуг», выбрать услугу и перейти в её детализацию. Далее нажать «Новый» и выбрать «Фиксированный пул машин»:

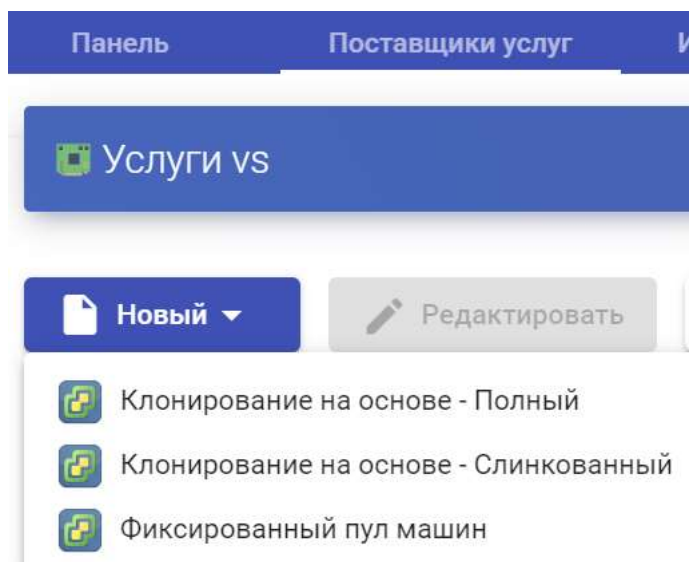
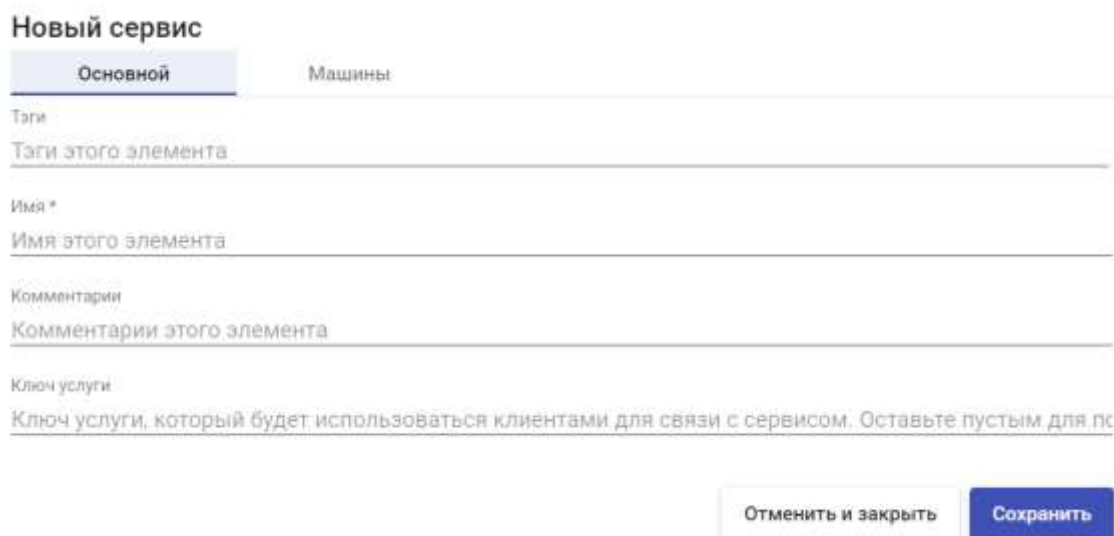


Рисунок 335

В фиксированном пуле машин минимальными параметрами, которые необходимо настроить, являются:

На вкладке «Основной» (см.Рисунок 336):

- **Имя:** название службы.
- **Ключ услуги:** если требуется, чтобы VDI распознала “вход” и “выход из системы” пользователя, который обращается к сервису этого типа (чтобы при “выходе из системы” VDI автоматически освобождала компьютер и делала его доступным для другого пользователя), необходимо будет заполнить это поле буквенно-цифровыми символами. Если поле оставить пустым, VDI навсегда назначит компьютер пользователю (до тех пор, пока администратор вручную не отключит службу).



Новый сервис

Основной Машины

Тэги
Тэги этого элемента

Имя *
Имя этого элемента

Комментарии
Комментарии этого элемента

Ключ услуги
Ключ услуги, который будет использоваться клиентами для связи с сервисом. Оставьте пустым для пс

Отменить и закрыть Сохранить

Рисунок 336

На вкладке «Машины» (см. Рисунок 337Рисунок 337):

- **Центр обработки данных:** центр обработки данных среды vSphere, где размещены виртуальные машины, которыми мы хотим управлять и назначать пользователям.
- **Пул ресурсов:** пул ресурсов, в котором расположены виртуальные машины, которыми мы хотим управлять и которые мы хотим назначать пользователям.
- **Машины:** виртуальные машины, существующие в указанном выше пуле ресурсов, которые будут управляться VDI и к которым доступ может быть предоставлен разным пользователям. Вы можете выборочно выбирать машины.
- **Использовать моментальные снимки:** если этот параметр включен, VDI создаст снимок на виртуальной машине перед подключением пользователя. Как только его назначение будет удалено (путем автоматического обнаружения выхода пользователя из системы или удаления вручную администратором), снимок будет восстановлен, чтобы компьютер находился в том же состоянии, в котором он был до подключения пользователя. Если этот параметр не активирован, VDI не восстановит предыдущее состояние компьютера при удалении назначения пользователю.

Новый сервис

Основной Машины

Центр обработки данных *

Datcenter

Пул ресурсов *

e2.vmw.aobfg.ru

Машины *

dev0.aobfg.ru, dev1.aobfg.ru

Использовать моментальные снимки

☐ Нет

Отменить и закрыть Сохранить

Рисунок 337

Сохраните конфигурацию, и у вас будет создан «Фиксированный пул машин» на платформе VMware vCenter. Вы сможете зарегистрировать все необходимые вам услуги «Фиксированный пул машин».

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 338Рисунок 338):

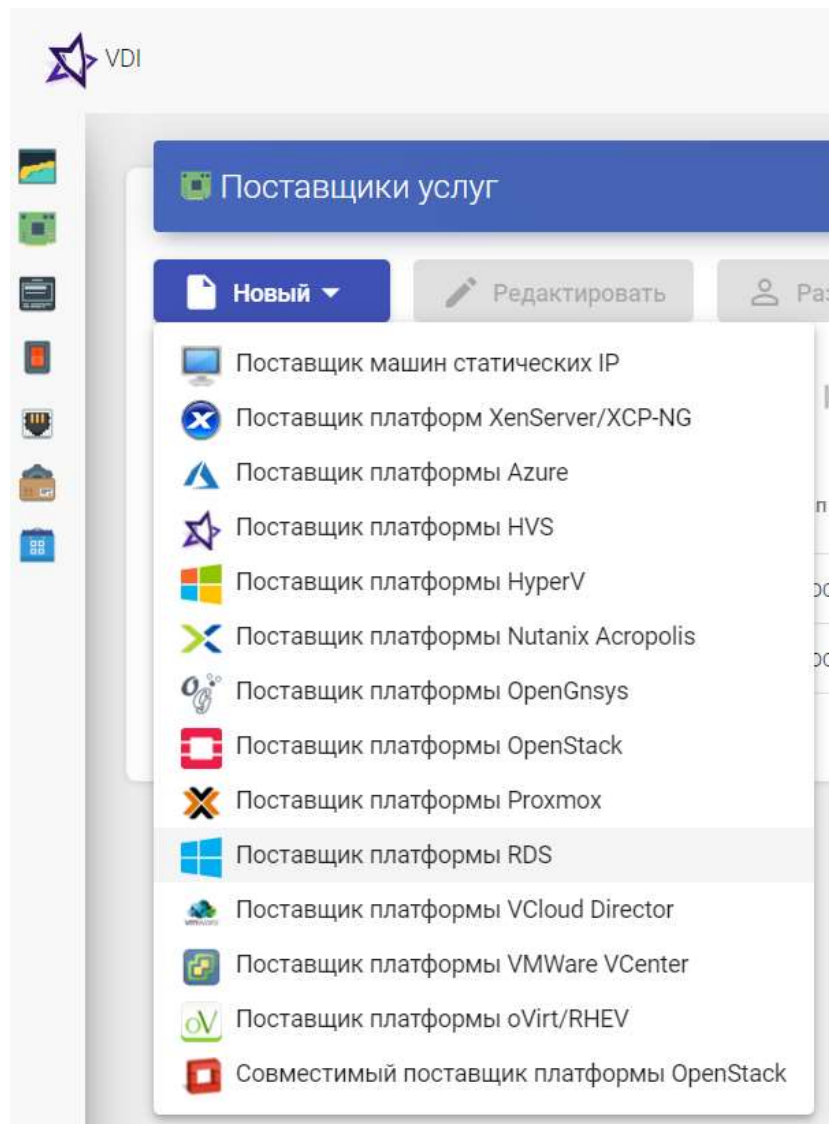


Рисунок 338

В «Поставщике платформы RDS» необходимо настроить следующие минимальные параметры (Рисунок 339):

Рисунок 339

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 340):

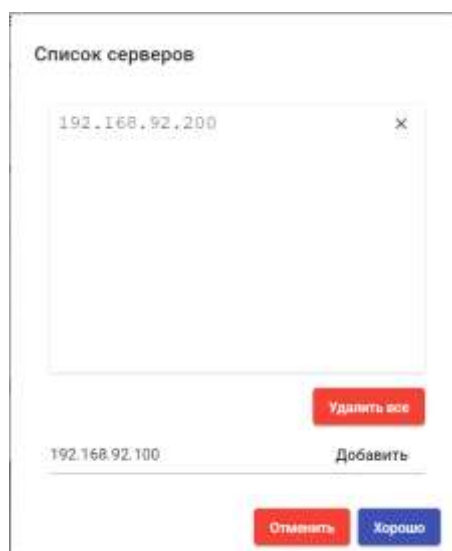


Рисунок 340

Примечание: одна и та же 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 341):

Рисунок 341

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 VDI 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 VDI 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 342).

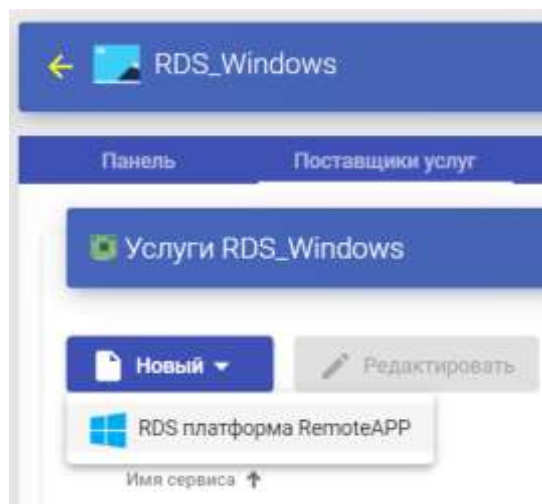


Рисунок 342

Минимальные параметры для настройки в этом типе службы (Рисунок 343):

- 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 343

- Дополнительно (Рисунок 344):

Ожидание порожденных процессов: ожидает завершения всех процессов, производных от приложения, прежде чем считать приложение отключенным.

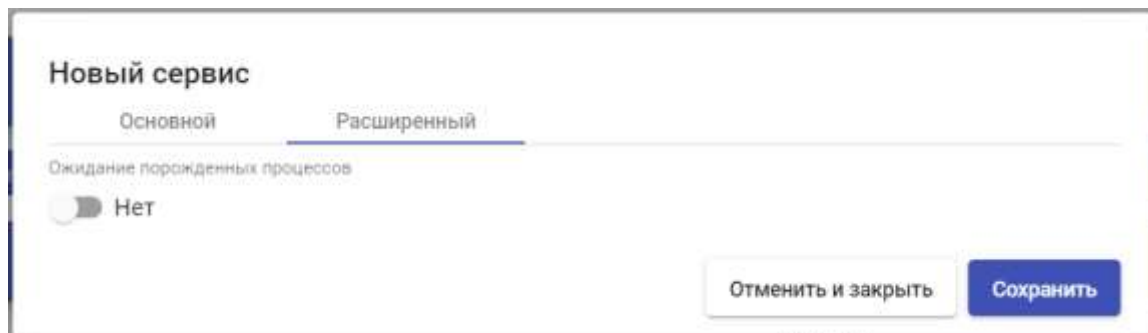


Рисунок 344

Настройки аутентификации

Active Directory

Этот внешний аутентификатор обеспечивает доступ к виртуальным рабочим столам и приложениям для пользователей и групп пользователей, принадлежащих Active Directory (Рисунок 345).

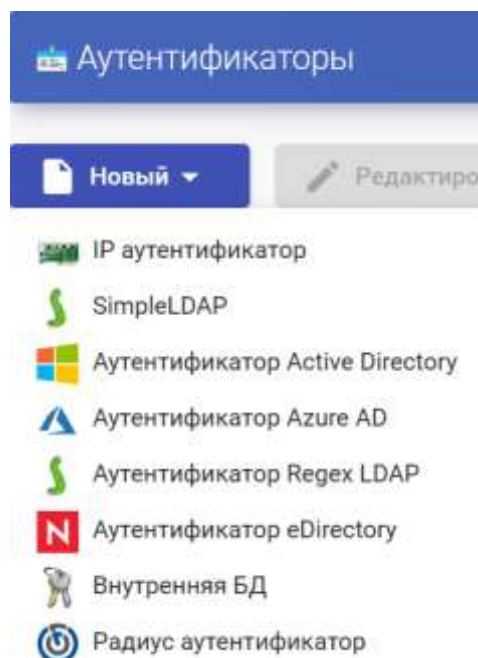


Рисунок 345

В «Active Directory аутентификаторе» настраиваются следующие минимальные параметры (Рисунок 346):

Рисунок 346

- 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 347):

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 347

▪ Учетные данные (Рисунок 348):

Пользователь: пользователь с привилегиями на чтения (формат: user@domain)

Пароль: пароль пользователя

Новый Аутентификатор

Основной Расширенный **Учетные данные** Экран/Дисплей

Пользователь *

Имя пользователя с привилегиями на чтение (используйте форму USER@DOMAIN.DOM)

Пароль *

Пароль пользователя LDAP

Проверить

Отменить и закрыть Сохранить

Рисунок 348

- Экран/Дисплей (Рисунок 349):

Видимый: Если параметр отключен, средство проверки подлинности не будет отображаться.

Новый Аутентификатор

Основной Расширенный Учетные данные **Экран/Дисплей**

Видимый

Да

Проверить

Отменить и закрыть Сохранить

Рисунок 349

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 350).

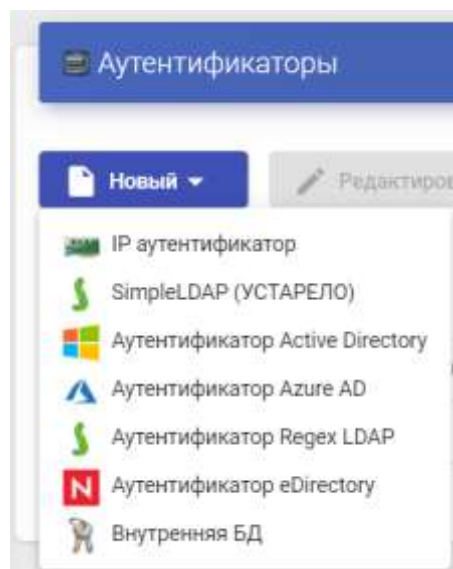


Рисунок 350

В разделе «Внутренняя база данных» настраиваются следующие минимальные параметры (Рисунок 351):

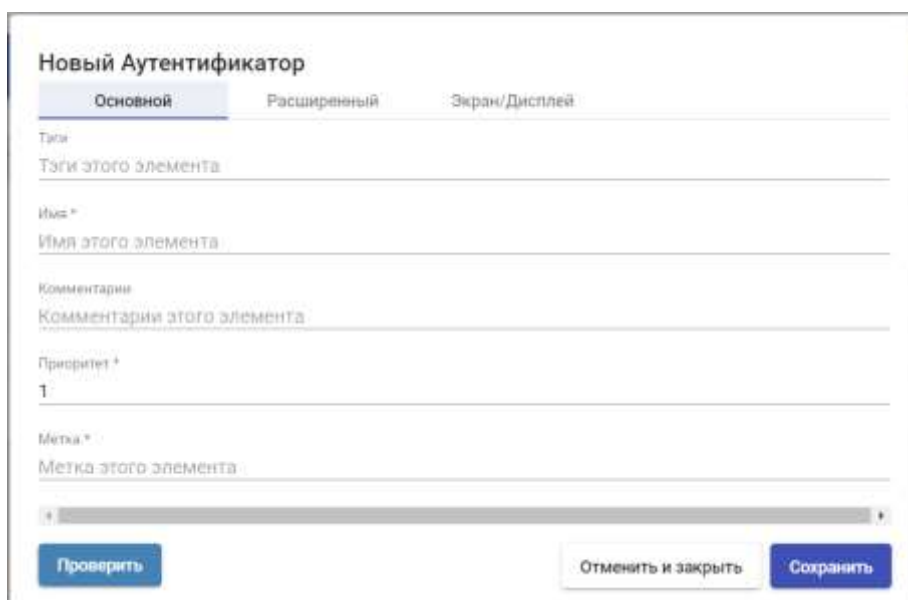


Рисунок 351

- 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 352):

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.

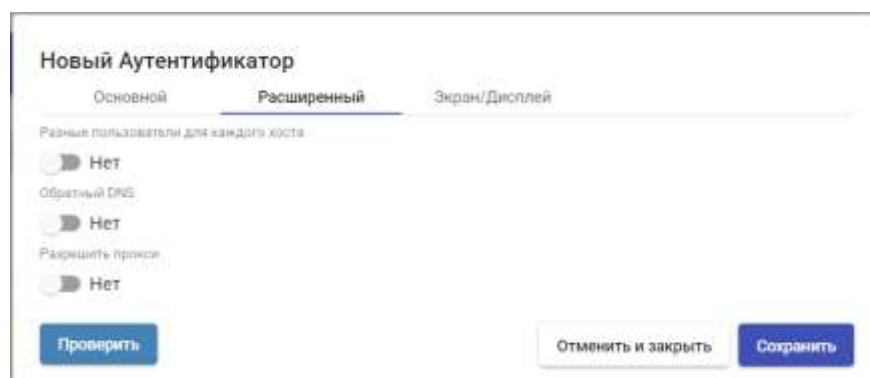


Рисунок 352

▪ Экран/Дисплей (Рисунок 353):

Видимый: Если параметр отключен, средство проверки подлинности не будет отображаться как доступное на странице входа в VDI.

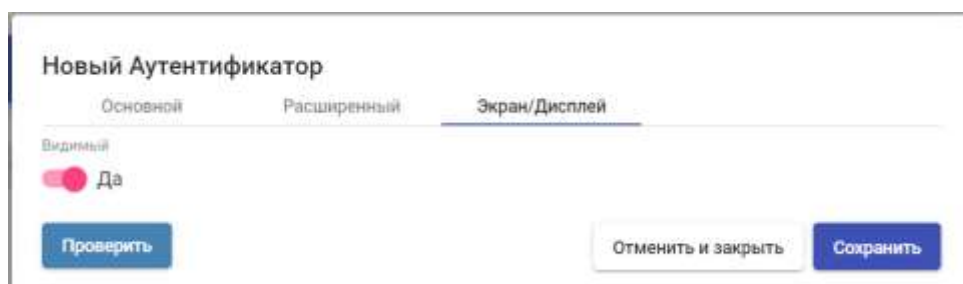


Рисунок 353

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 IP-адресов (Рисунок 354).

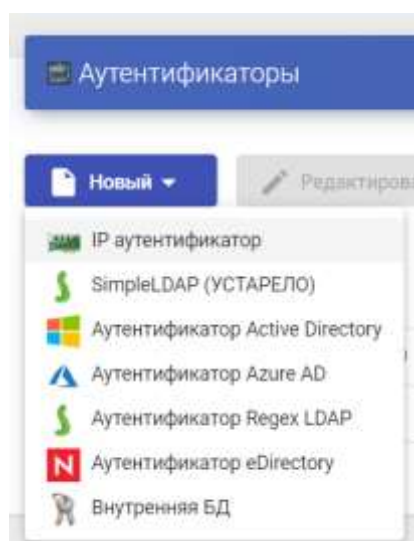


Рисунок 354

В «IP Аутентификатор» настраиваются следующие минимальные параметры (Рисунок 355):

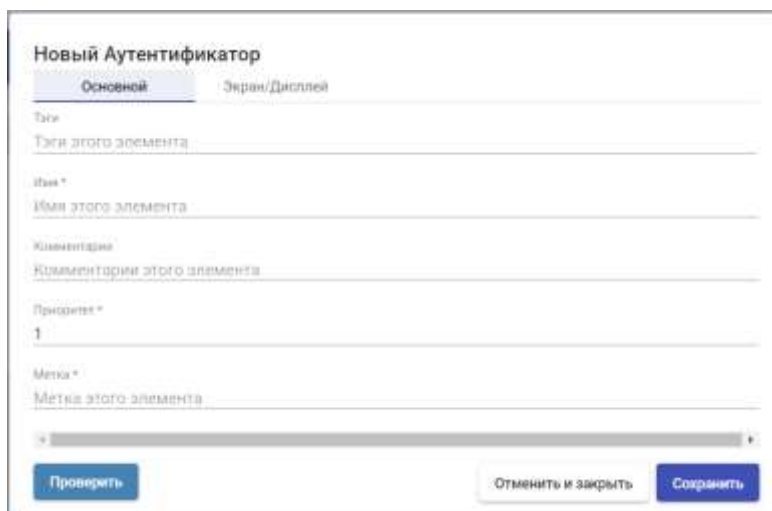


Рисунок 355

- 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 356)

Видимый: Если параметр отключен, средство проверки подлинности не будет отображаться как доступное на странице входа в VDI.

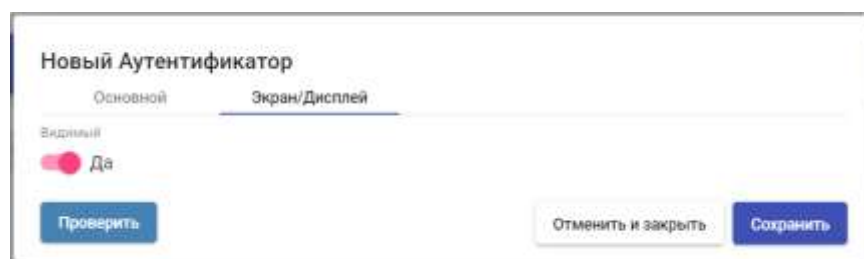


Рисунок 356

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 VDI 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 VDI страница.

Кнопка «Test» позволяет проверить успешность подключения.

Радиус аутентификатор

Этот внешний аутентификатор, который позволяет предоставлять доступ к виртуальным рабочим столам и приложениям для пользователей и групп пользователей, участвующим в аутентификации на основе RADIUS.

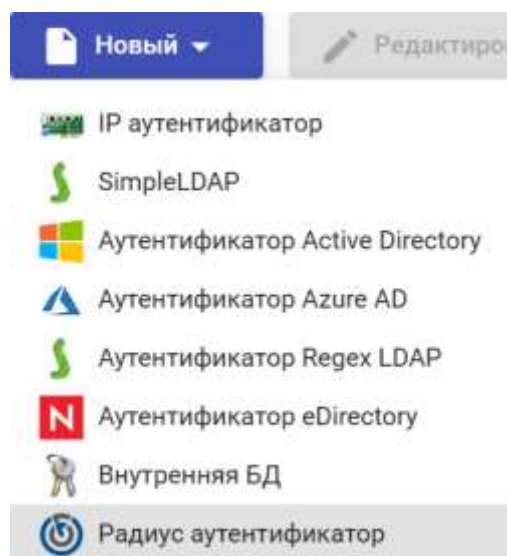


Рисунок 357

В Радиус аутентификаторе минимальными параметрами для настройки являются:

- на вкладке «Основной» (Рисунок 358):

Имя – имя аутентификатора.

Приоритет – приоритет, который будет иметь этот аутентификатор. Если имеется несколько аутентификаторов, то чем ниже его приоритет, тем выше он будет отображаться в списке доступных аутентификаторов на портале входа в систему VDI. Это поле допускает отрицательные значения.

Метка. Включает прямую проверку подлинности в этом средстве проверки подлинности. Это позволяет пользователю выполнять проверку с помощью указанного средства проверки подлинности, хотя в среде VDI имеется больше средств проверки подлинности. Чтобы сделать это, вам нужно будет получить доступ к экрану входа в систему VDI в следующем формате:

Сервер WDS/wds/страница/логин/метка (например:
https://VDIServer/vdi/page/login/Radi).

Хост – IP-адрес или имя RADIUS-сервера.

Порт – порт связи с RADIUS-сервером.

Секрет – строка проверки для RADIUS-сервера (определена на самом RADIUS-сервере).

Новый аутентификатор

Основной	Расширенный	МФА	Экран/Дисплей
Тэги			
Тэги этого элемента			
Имя *			
Имя этого элемента			
Комментарии			
Комментарии этого элемента			
Приоритет *			
1			
Метка *			
Метка этого элемента			
Хост *			
IP-адрес или имя хоста Radius Server			
Порт *			
1812			
Секрет *			
Секрет клиента Radius			
Проверить		Отменить и закрыть	
		Сохранить	

Рисунок 358

- на вкладке «Расширенный» (Рисунок 359):

Идентификатор NAS. Идентифицирует использование на сервере RADIUS, позволяя при необходимости выполнять фильтрацию.

Префикс приложения для атрибутов класса. Позволяет фильтровать, какие группы мы получаем из атрибута «class» сервера RADIUS.

Глобальная группа. Позволяет принудительно присоединить всех пользователей к группе. Это позволяет серверу RADIUS (который по-прежнему является «простым» средством аутентификации), не содержащему групп, иметь

возможность назначать всех пользователей группе (даже если он также содержит группы).

The screenshot shows a web interface for configuring a new authenticator. The title is 'Новый аутентификатор'. There are four tabs: 'Основной', 'Расширенный' (which is selected), 'МФА', and 'Экран/Дисплей'. The 'Расширенный' tab contains the following fields:

- 'Идентификатор NAS *': vdi-server
- 'Префикс приложения для атрибутов класса':
- 'Префикс приложения для фильтрации групп по атрибуту "Класс"':
- 'Глобальная группа':
- A note below the 'Глобальная группа' field: 'Если установлено, это значение будет добавлено как группа для всех пользователей радиуса.'

At the bottom, there are three buttons: 'Проверить' (blue), 'Отменить и закрыть' (white), and 'Сохранить' (blue).

Рисунок 359

ПРИМЕЧАНИЕ:

По умолчанию VDI извлекает из атрибута Radius «Class» элементы, имеющие вид «group=...».

Если мы определим в «Префиксе приложения для атрибутов класса», например «лаборатория», VDI будет искать только атрибуты «класса», которые имеют вид «лабораторная группа=...».

- на вкладке «МФА» (Рисунок 360):

Поставщик МФА. Заполняется, если настраивается многофакторная аутентификация.

Новый аутентификатор

Основной	Расширенный	МФА	Экран/Дисплей

Атрибут многофакторной идентификации

Поставщик МФА

Нет

Проверить

Отменить и закрыть

Сохранить

Рисунок 360

- на вкладке «Экран/Дисплей» (Рисунок 361):

Видимый. Если он отключен, средство проверки подлинности не будет отображаться как доступное на странице входа в VDI.

Новый аутентификатор

Основной	Расширенный	МФА	Экран/Дисплей

Видимый

☒ Да

Проверить

Отменить и закрыть

Сохранить

Рисунок 361

Настройка многофакторной аутентификации

Многофакторная аутентификация (далее – МФА) добавляет уровень защиты к процессу входа в систему.

При доступе к учетной записи или приложению пользователи должны пройти дополнительную проверку личности.

VDI изначально поддерживает несколько систем многофакторной аутентификации:

- Многофакторная электронная почта;

- Вызов Radius OTP;
- SMS по протоколу HTTP;
- МИД на базе TOTP,

и он также поддерживает другие МФА, интегрированные в сам аутентификатор, так что, когда аутентификатор встроен в VDI, МФА включается автоматически. В VDI вы можете выполнить двойную аутентификацию пользователей изначально, используя различные методы, описанные ниже.

Чтобы настроить многофакторную аутентификацию необходимо перейти в пункт меню «Аутентификация» - «Многофакторный». Далее нажать кнопку «Новый», и выбрать из списка нужную строку:

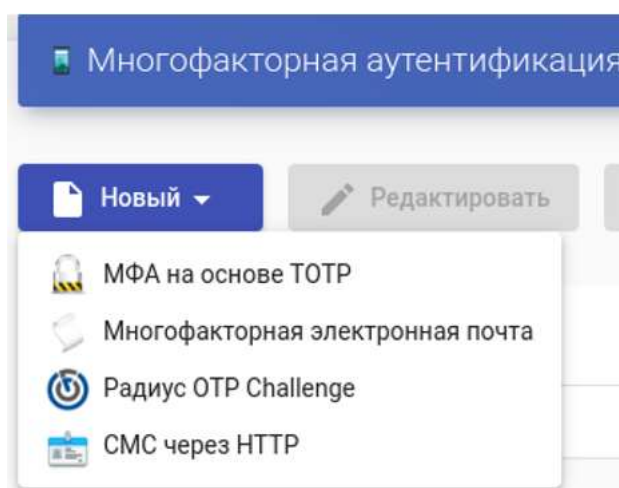


Рисунок 362

«Многофакторная» конфигурация не является необходимым компонентом для создания «Пула услуг».

Многофакторная электронная почта

С помощью этого метода пользователь сначала аутентифицируется под своим именем пользователя и паролем, а затем перенаправляется на второй процесс аутентификации, где он получит электронное письмо с необходимым кодом для окончательной аутентификации на своей платформе VDI.

В «многофакторном электронном письме» минимальными параметрами для настройки являются:

- на вкладке «Основной» (Рисунок 363):

Имя – название, под которым будет указан товар.

Кэширование устройства – время в часах для кэширования устройства, чтобы МФА больше не требовался.

Срок действия кода МФА – время в минутах, необходимое для разрешения использования кода МФА.

Новая МФА

Основной SMTP-сервер Конфигурация

Тэги
Тэги этого элемента

Имя *
Имя этого элемента

Комментарии
Комментарии этого элемента

Кэширование устройства
0

Срок действия кода МФА
5

Отменить и закрыть Сохранить

Рисунок 363

- на вкладке «SMTP-сервер» (Рисунок 364):

SMTP-хост – имя хоста или IP-адрес SMTP-сервера.

Безопасность – используемый протокол безопасности.

Имя пользователя и пароль – учетные данные пользователя, имеющего доступ к SMTP-серверу. Рекомендации безопасного использования – пароли должны быть достаточной длины и содержать заглавные и строчные буквы, цифры и специальные символы.

Новая МФА

Основной SMTP-сервер Конфигурация

SMTP-хост *

IP-адрес или имя хоста SMTP-сервера. Если используется нестандартный порт, следует указать его после двоеточия,

Безопасность *

TLS

Имя пользователя

Пользователь с доступом к SMTP-серверу

Пароль

Пароль пользователя с доступом к SMTP-серверу

Отменить и закрыть Сохранить

Рисунок 364

- на вкладке «Конфигурация» (Рисунок 365):

Предмет – тема электронного письма, которое будет отправлено пользователям.

Из электронной почты – адрес электронной почты, который будет использоваться в качестве отправителя.

Политика для пользователей без поддержки МФА – политика, которая будет использоваться с теми пользователями, у которых не настроена поддержка МФА.

Текст сообщения – текст, который будет отображаться в отправленном письме.

Новая МФА

Основной	SMTP-сервер	Конфигурация

Предмет *

Verification Code

Из электронной почты *

Адрес электронной почты, который будет использоваться в качестве отправителя

Включить HTML

☐ Нет

Политика для пользователей без поддержки MFA *

Разрешить вход пользователя

Почтовые сети OTP

Сети для проверки подлинности электронной почты OTP

Текст сообщения *

Почтовый HTML

Отменить и закрытьСохранить

Рисунок 365

Radius OTP Challenge

С помощью этого метода пользователь сначала аутентифицируется под своим именем пользователя и паролем, а затем перенаправляется ко второму процессу аутентификации, где он должен ввести соответствующий код, предоставленный его radius-сервером, чтобы окончательно пройти аутентификацию на своей платформе VDI.

- вкладка «Основной» (Рисунок 366):

Имя – имя, которое будет указано элементу.

Хост – имя хоста или IP-адрес сервера Radius.

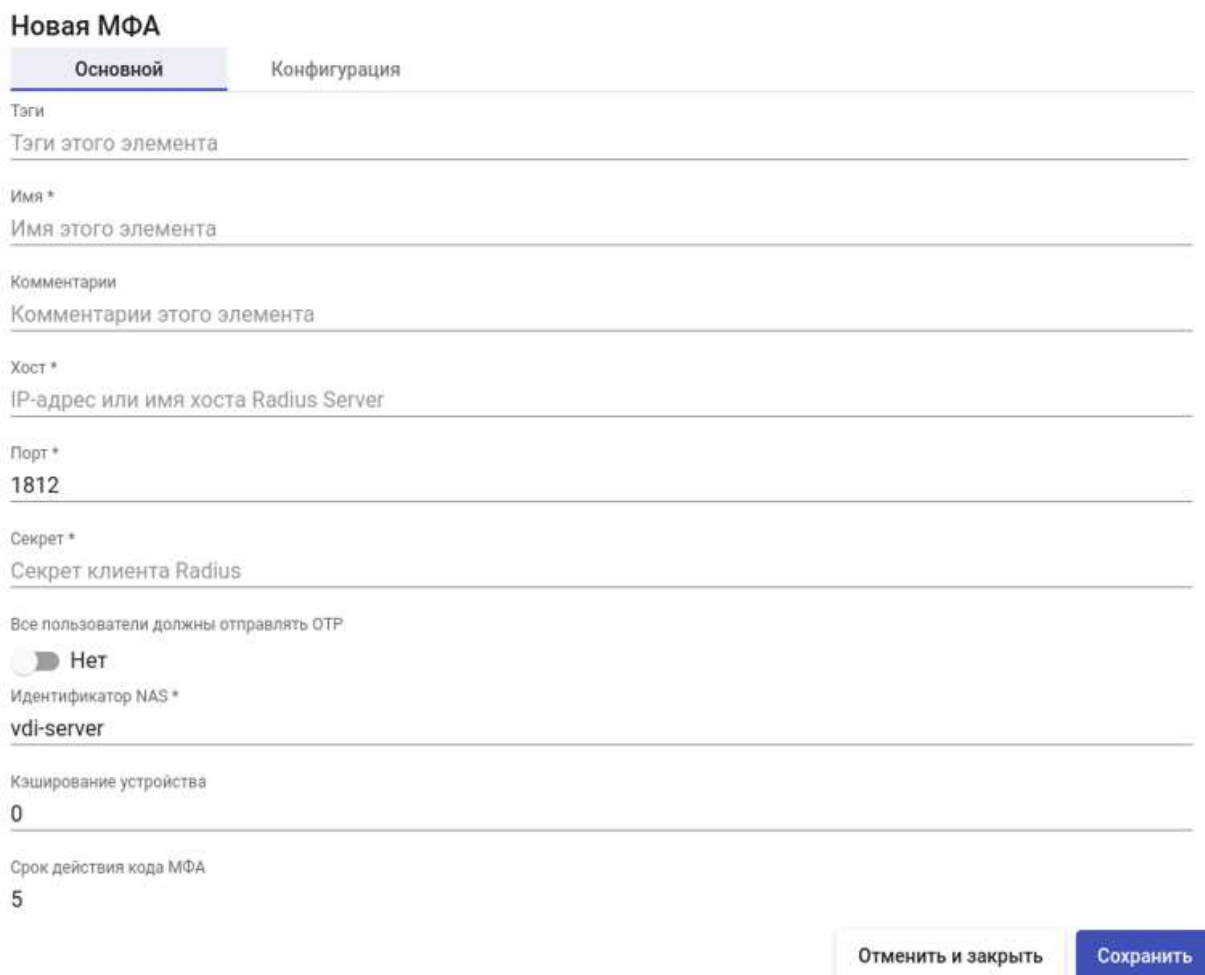
Порт – порт аутентификации Radius.

Секрет – секрет клиента Radius.

Идентификатор NAS – идентификатор NAS для Radius-сервера.

Кэширование устройства – время в часах для кэширования устройства, чтобы МФА больше не требовался.

Срок действия кода МФА – время в минутах, необходимое для разрешения использования кода МФА.



Новая МФА

Основной Конфигурация

Тэги
Тэги этого элемента

Имя *
Имя этого элемента

Комментарии
Комментарии этого элемента

Хост *
IP-адрес или имя хоста Radius Server

Порт *
1812

Секрет *
Секрет клиента Radius

Все пользователи должны отправлять OTP:
☐ Нет

Идентификатор NAS *
vdi-server

Кэширование устройства
0

Срок действия кода МФА
5

Отменить и закрыть Сохранить

Рисунок 366

- вкладка «Конфигурация» (Рисунок 367Рисунок 367):

Действие при ошибке связи Radius OTP – действие, которое должно быть выполнено сервером Radius в случае ошибки.

Радиусные OPT-сети – сети для аутентификации Radius OTP.

Пользователи без определенного OTP на сервере – политика, которая будет использоваться с теми пользователями, у которых не настроен МФА.

The screenshot shows a web interface for configuring a new Multi-Factor Authentication (MFA) policy. The title is 'Новая МФА'. There are two tabs: 'Основной' (Main) and 'Конфигурация' (Configuration), with the latter being active. The configuration section contains three rows, each with a label and a dropdown menu:

- Label: 'Действие при ошибке связи Radius OTP *' (Action in case of Radius OTP connection error *). Dropdown: 'Разрешить вход пользователя' (Allow user login).
- Label: 'Радиусные OTP-сети' (Radius OTP networks). Dropdown: 'Сети для OTP-аутентификации Radius' (Radius networks for OTP authentication).
- Label: 'Пользователь без определенного OTP на сервере *' (User without a specific OTP on the server *). Dropdown: 'Разрешить вход пользователя' (Allow user login).

At the bottom right, there are two buttons: 'Отменить и закрыть' (Cancel and close) and 'Сохранить' (Save).

Рисунок 367

СМС через HTTP

С помощью этого метода пользователь сначала аутентифицируется под своим именем пользователя и паролем, а затем перенаправляется на второй процесс аутентификации, где он получит SMS-сообщение с необходимым кодом для окончательной аутентификации на своей платформе VDI.

- вкладка «Основной»:

Имя – название, под которым будет указан товар.

Кэширование устройства – время в часах для кэширования устройства, чтобы МФА больше не требовался.

Срок действия кода МФА – время в минутах, необходимое для разрешения использования кода МФА.

HTTP-сервер

Новая МФА

Основной

HTTP-сервер

HTTP-аутентификация

HTTP-ответ

Конфигурация

Таги

Таги этого элемента

Имя *

Имя этого элемента

Комментарии

Комментарии этого элемента

Кодирование устройства

0

Срок действия кода МФА

5

Отменить и закрыть

Сохранить

Рисунок 368

- вкладка «HTTP-сервер»:

Шаблон URL-адреса для отправки SMS – шаблон URL-адреса для отправки SMS. Он может содержать следующие переменные:

- * {код} – код для отправки
- * {телефон/+phone} – номер телефона
- * {username} – имя пользователя
- * {* {просто имя пользователя} – имя пользователя без @.

Способ отправки SMS – метод, который будет использоваться для отправки SMS.

Кодировка SMS – шифрование, которое будет использоваться для отправки SMS.

Новая МФА

Основной	HTTP-сервер	HTTP-аутентификация	HTTP-ответ	Конфигурация
Шаблон URL для отправки SMS *				
Шаблон URL для отправки SMS. Он может содержать следующие переменные: * {code} - код для отправки * {phone/+7}				
Игнорировать ошибки сертификата				
☐ Нет				
Способ отправки СМС *				
GET				
Параметры для отправки SMS POST/PUT				
Заголовки для SMS-запросов				
Кодировка SMS *				
utf-8				
				Отменить и закрыть
				Сохранить

Рисунок 369

- вкладка «HTTP-аутентификация»:

Метод SMS-аутентификации.

Пользователь или токен SMS-аутентификации.

Пароль для аутентификации по SMS.

Новая МФА

Основной	HTTP-сервер	HTTP-аутентификация	HTTP-ответ	Конфигурация
Метод аутентификации по SMS *				
Нет				
Пользователь или токен SMS-аутентификации				
Пользователь или токен для SMS-аутентификации				
SMS-пароль аутентификации				
Пароль для SMS-аутентификации				
				Отменить и закрыть
				Сохранить

Рисунок 370

- вкладка «Конфигурация»:

Действие при ошибке ответа на SMS – действие, которое должно быть предпринято сервером в случае ошибки.

Пользователь без политики МФА – действие, выполняемое для пользователей без настроенной политики МФА.

The screenshot shows a web interface for configuring MFA. The title is 'Новая МФА'. There are five tabs: 'Основной', 'HTTP-сервер', 'HTTP-аутентификация', 'HTTP-ответ', and 'Конфигурация' (which is active). The 'Конфигурация' tab contains three sections, each with a dropdown menu:

- Section: 'Действие при ошибке ответа SMS *'. Dropdown: 'Разрешить вход пользователя'.
- Section: 'SMS-сети'. Dropdown: 'Сети для SMS-аутентификации'.
- Section: 'Пользователь без политики MFA *'. Dropdown: 'Разрешить вход пользователя'.

At the bottom right, there are two buttons: 'Отменить и закрыть' (light blue) and 'Сохранить' (dark blue).

Рисунок 371

МФА на основе TOTP

С помощью этого метода пользователь сначала аутентифицируется под своим именем пользователя и паролем, а затем перенаправляется на второй процесс аутентификации, где он должен ввести код TOTP, генерируемый время от времени в нашем приложении, таком как Google authenticator, Microsoft и т.д. чтобы иметь возможность, пройти аутентификацию на вашей корпоративной платформе VDI.

- вкладка «Основной»:

Имя – название, под которым будет указан предмет.

Эмитент – OTP-эмитент, после создания он не может быть изменен.

Кэширование устройства – время в часах для кэширования устройства, чтобы MFA больше не требовался.

Срок действия кода МФА – время в минутах, необходимое для разрешения использования кода МФА.

The screenshot shows the 'Новая МФА' (New MFA) configuration window with the 'Основной' (Main) tab selected. The 'Конфигурация' (Configuration) tab is also visible. The form contains the following fields:

- Тэги (Tags): Тэги этого элемента (Tags of this element)
- Имя * (Name *): Имя этого элемента (Name of this element)
- Комментарии (Comments): Комментарии этого элемента (Comments of this element)
- Эмитент * (Issuer *): VDI Authenticator
- Кэширование устройства (Device caching): 0
- Срок действия кода МФА (MFA code validity period): 5

At the bottom right, there are two buttons: 'Отменить и закрыть' (Cancel and close) and 'Сохранить' (Save).

Рисунок 372

- вкладка «Конфигурация»:

Действительное окно – количество кодов, которые будут действительны до и после текущего.

TOTP-сети. У пользователя, добавленного в эти сети, не будет запрашиваться ОТР.

The screenshot shows the 'Новая МФА' (New MFA) configuration window with the 'Конфигурация' (Configuration) tab selected. The 'Основной' (Main) tab is also visible. The form contains the following fields:

- Действительное окно * (Valid window *): 1
- TOTP-сети (TOTP networks): У пользователей из этих сетей не будет запрашиваться одноразовый пароль (Users from these networks will not be prompted for a one-time password)

At the bottom right, there are two buttons: 'Отменить и закрыть' (Cancel and close) and 'Сохранить' (Save).

Рисунок 373

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 portalу входа в VDI 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 «Сервис-пулу».

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 374).

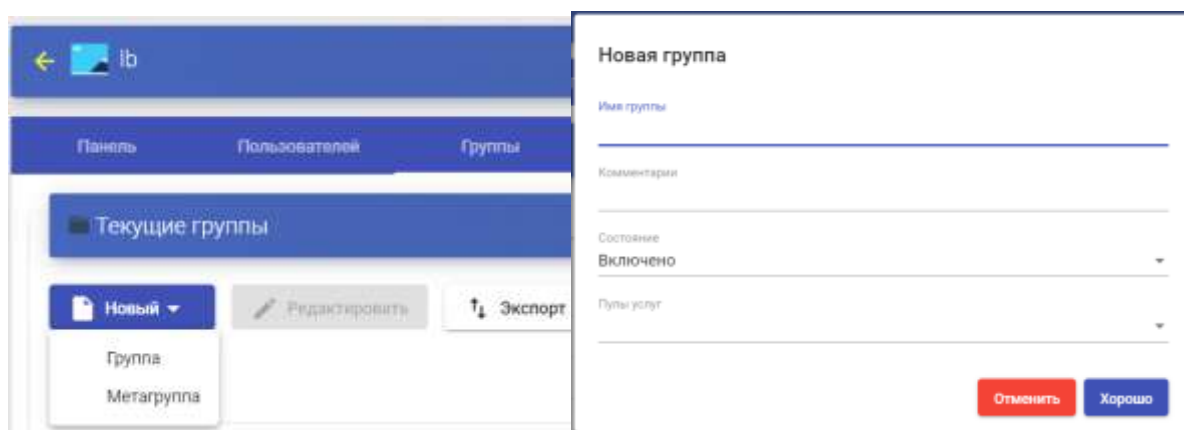


Рисунок 374

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 375).

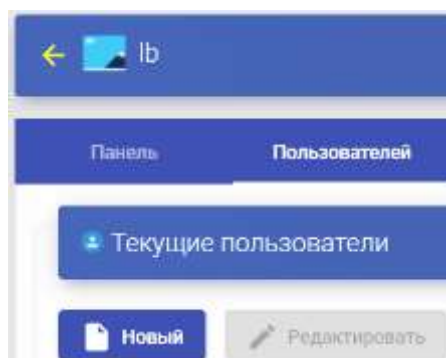


Рисунок 375

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 376).

Рисунок 376

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 377).

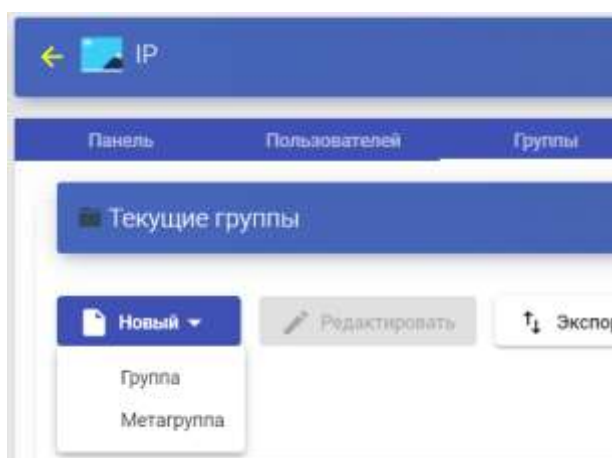


Рисунок 377

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 378).

Рисунок 378

Когда пользователь выбирает этот аутентификатор на портале входа в VDI (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 379).

Рисунок 379

Как только пользователь будет проверен на портале входа в систему VDI, его IP-адрес будет автоматически зарегистрирован на вкладке «Пользователи» (Рисунок 380).



Рисунок 380

Если нужно изменить его статус (включен или отключен) или уровень доступа (поле «Роль»), выбрать его и нажать «Редактировать» (Рисунок 381).

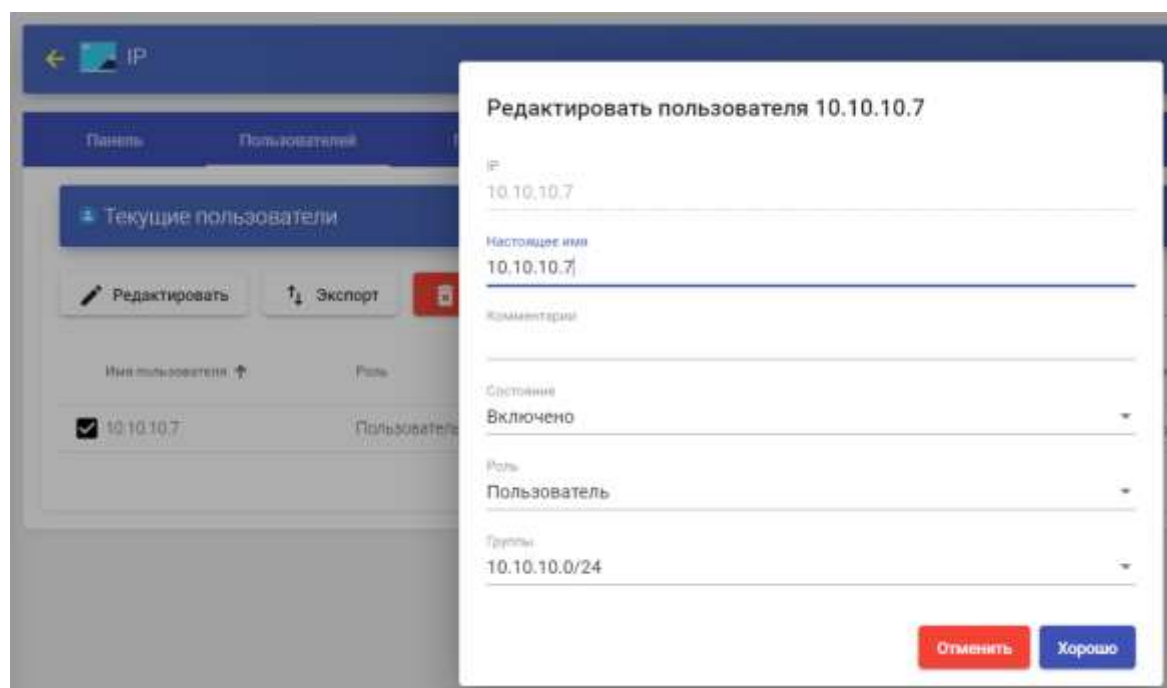


Рисунок 381

Настройка «Менеджер ОС»

«Менеджер ОС» запускает ранее настроенный тип службы.

VDI 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 382).

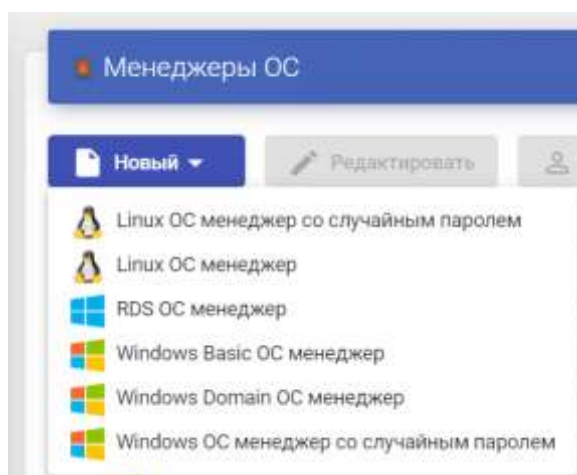


Рисунок 382

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 383):

Рисунок 383

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 VDI 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 384):

Рисунок 384

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 VDI 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 385).

Минимальные параметры, которые необходимо настроить в «RDS ОС менеджер», следующие (Рисунок 385).

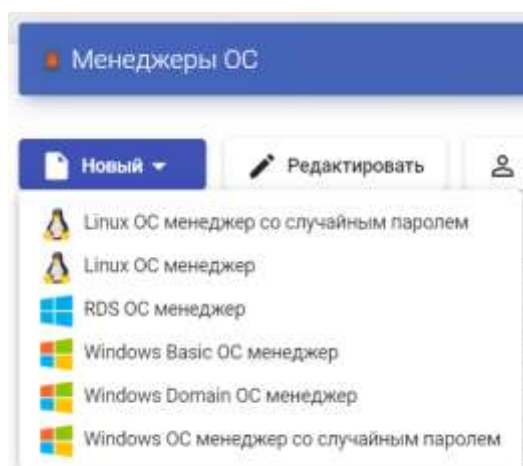


Рисунок 385

Имя: Имя «Менеджер ОС».

Максимальное время сессии: максимальное время, в течение которого сессия будет оставаться открытым, в часах (0 = не ограничено).

Рисунок 386

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 387):

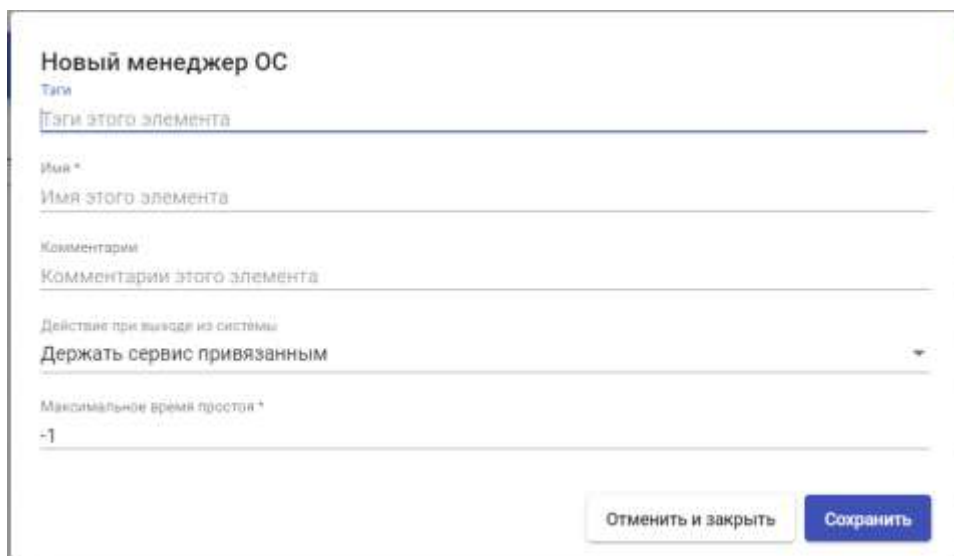


Рисунок 387

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 VDI 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 388):

- Основной:

Рисунок 388

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 389).

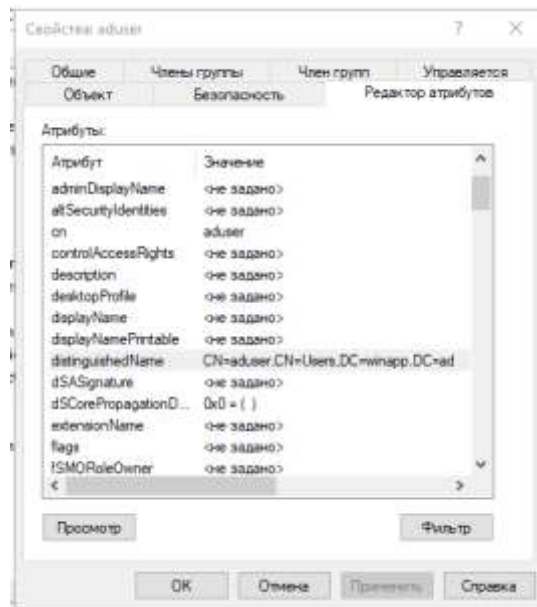


Рисунок 389

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 VDI Actor автоматически закроет сеанс. Отрицательные значения и менее 300 секунд отключают эту опцию.

- Расширенный (Рисунок 390):

The screenshot shows a web-based configuration interface titled 'Новый менеджер ОС'. It has two tabs: 'Основной' (Basic) and 'Расширенный' (Advanced), with the latter being selected. The 'Расширенный' tab contains four configuration sections, each with a radio button and a 'Да' (Yes) selection:

- Группа машин:** A text input field with a placeholder: «Группа, к которой добавляются машины при создании. Если пусто, на одну группу не будет использоваться». (Обязательное)
- Убрать машину:** A radio button set to 'Да'.
- Предпочтения серверов:** A text input field with a placeholder: «В случае нескольких серверов AD, какой из них предпочтительнее».
- Использовать VDI:** A radio button set to 'Да'.

At the bottom right, there are two buttons: 'Отменить и закрыть' (Cancel and close) and 'Сохранить' (Save).

Рисунок 390

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 391):

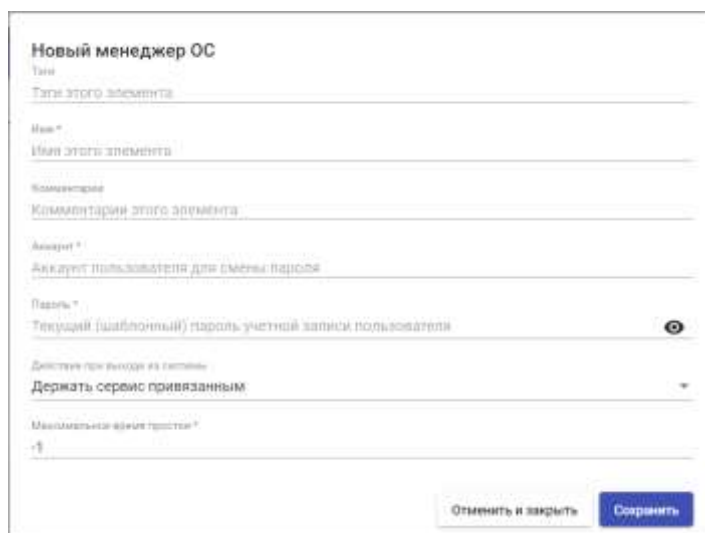


Рисунок 391

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 VDI Actor автоматически закрывает сеанс. Отрицательные значения и менее 300 секунд отключают эту опцию.

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 392):

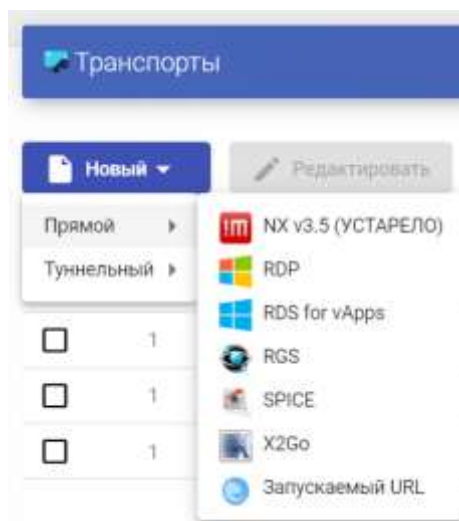


Рисунок 392

- 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 393):

Рисунок 393

Имя: Имя транспорта.

Приоритет: приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортных средств для службы. Транспорт с наименьшим приоритетом будет использоваться по умолчанию при нажатии на изображение сервиса.

Порт прослушивания: порт прослушивания программного обеспечения NX.

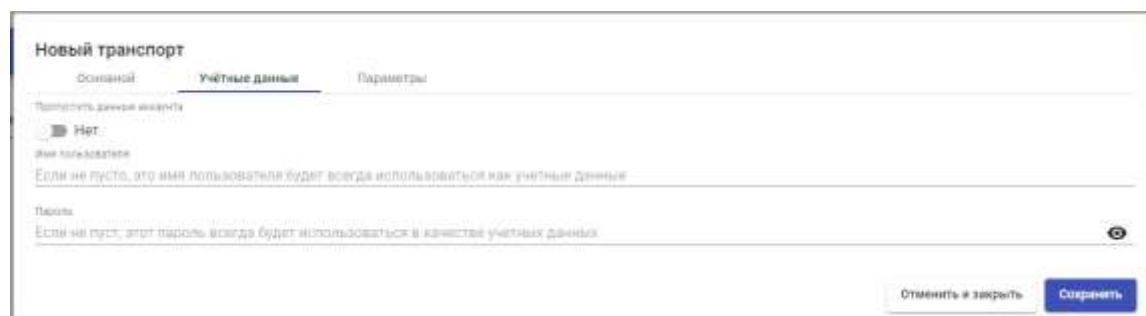
Доступ к сети: разрешает или запрещает доступ пользователя к службе в зависимости от сети, из которой он осуществляет доступ, и сети, указанной в поле «Сети».

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 394):



The screenshot shows a web form titled 'Новый транспорт' (New Transport) with three tabs: 'Созданой' (Created), 'Учётные данные' (Account Data), and 'Параметры' (Parameters). The 'Учётные данные' tab is active. It contains a section 'Подобрать данные аккаунта' (Select account data) with a radio button labeled 'Нет' (No) selected. Below this is a text input field for 'Имя пользователя' (Username) with a hint: 'Если не пусто, это имя пользователя будет всегда использоваться как учетные данные' (If not empty, this username will always be used as account data). Below the username field is a password input field for 'Пароль' (Password) with a hint: 'Если не пусто, этот пароль всегда будет использоваться в качестве учетных данных' (If not empty, this password will always be used as account data). At the bottom right, there are two buttons: 'Отменить и закрыть' (Cancel and Close) and 'Сохранить' (Save).

Рисунок 394

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 395):

The screenshot shows a web-based configuration interface titled 'Новый транспорт' (New Transport). It has three tabs: 'Основной' (Main), 'Учетные данные' (Credentials), and 'Параметры' (Parameters), with 'Параметры' being the active tab. The interface contains several configuration items, each with a label, a value, and a dropdown arrow:

- Подключение** (Connection): modem
- Сессия** (Session): gnome
- Дисковый кэш** (Disk cache): 0 Mb
- Кэш памяти** (Memory cache): 4 Mb
- Размер экрана** (Screen size): Полный экран (Full screen)

At the bottom right, there are two buttons: 'Отменить и закрыть' (Cancel and close) and 'Сохранить' (Save).

Рисунок 395

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 396):

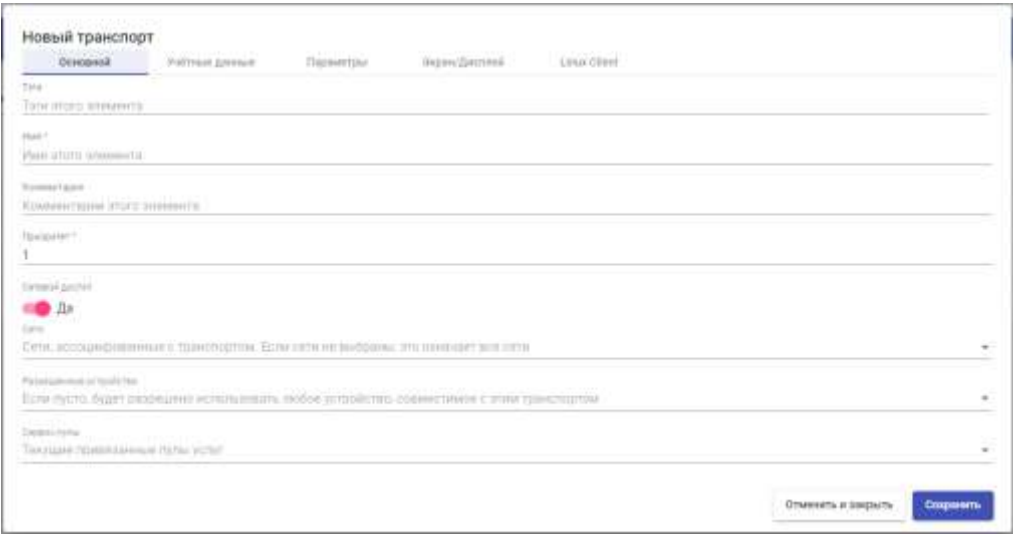


Рисунок 396

Имя: Имя транспорта.

Приоритет: приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортных средств 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 397):

Рисунок 397

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 398):

Рисунок 398

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 399)

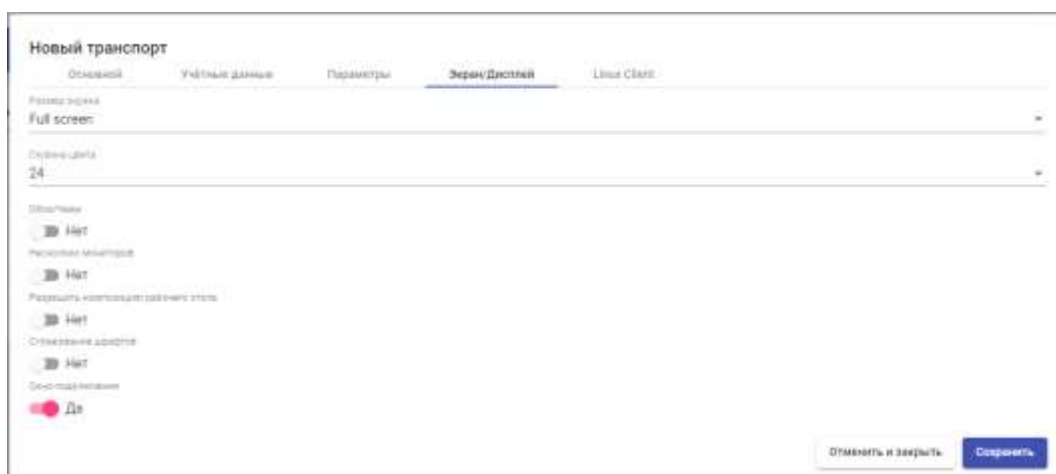


Рисунок 399

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 400):

Рисунок 400

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 401):

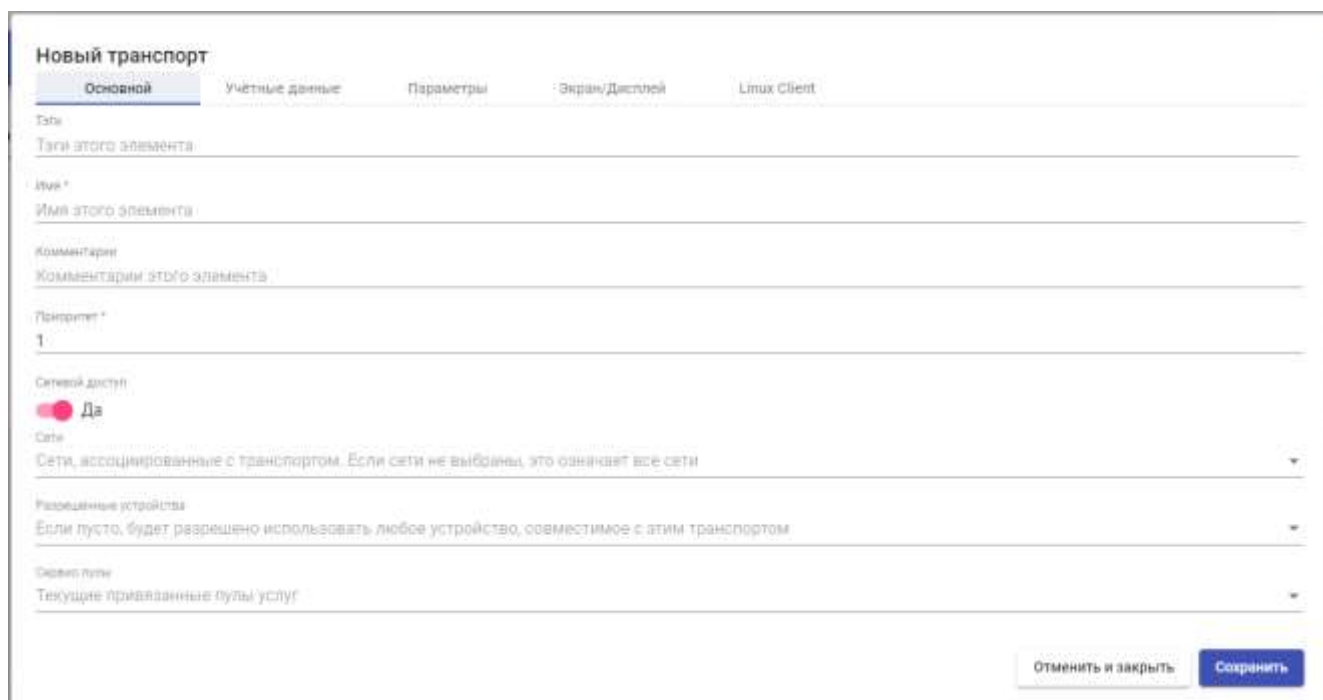


Рисунок 401

Имя: Имя транспорта.

Приоритет: приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортных средств 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 402):



The screenshot shows a web interface for creating a new transport. The title is 'Новый транспорт' (New Transport). There are five tabs: 'Основной' (Main), 'Учетные данные' (Account Data), 'Параметры' (Parameters), 'Экран/Дисплей' (Screen/Display), and 'Linux Shell'. The 'Учетные данные' tab is active. It contains three sections: 'Пропустить данные входа' (Skip login data) with a 'Нет' (No) button, 'Без домена' (No domain) with a 'Нет' (No) button, and 'Домен' (Domain) with a text input field. Below the input field is a note: 'Если это не пусто, этот домен всегда будет использоваться в качестве учетных данных (используется как DOMAIN\user)'. At the bottom right are two buttons: 'Отменить и закрыть' (Cancel and Close) and 'Сохранить' (Save).

Рисунок 402

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 403):

Рисунок 403

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 404)



Рисунок 404

Глубина цвета: указывает глубину цвета.

Сглаживание шрифтов: активирует сглаживание шрифта.

▪ Клиент Linux (Рисунок 405):

The screenshot shows the 'Linux Client' configuration window. It has a title bar 'Новый транспорт' and four tabs: 'Основной', 'Учетные данные', 'Параметры', and 'Linux Client'. The 'Linux Client' tab is active. It contains several settings, each with a checkbox and a 'Нет' (None) button. The settings are: 'Execute as shell', 'Мультимедийная синхронизация', 'Использовать alsa', 'Перенаправить домашнюю папку', and 'Страна принтера'. Below these are two text fields: 'Если принтер установлен, строка принтера, используемая с клиентом xfreerdp' and 'Если установлена строка smbd-адреса, строка smbd-адреса, используемая с клиентом xfreerdp'. At the bottom, there is a text field for 'Пользовательские параметры' and two buttons: 'Отменить и закрыть' and 'Сохранить'.

Рисунок 405

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 406):

Рисунок 406

Имя: Имя транспорта.

Приоритет: приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортных средств 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 407):



The screenshot shows a web interface for creating a new transport. The title is 'Новый транспорт' (New Transport). There are three tabs: 'Общая' (General), 'Учетные данные' (Credentials), and 'Параметры' (Parameters). The 'Учетные данные' tab is active. It contains a section 'Требуется ли аутентификация?' (Authentication required?) with a radio button set to 'Нет' (No). Below this, there are three input fields: 'Имя пользователя:' (Username:), 'Пароль:' (Password:), and 'Домен:' (Domain:). Each field has a placeholder text indicating that if left empty, it will be used as the default. At the bottom right, there are two buttons: 'Отменить и закрыть' (Cancel and Close) and 'Сохранить' (Save).

Рисунок 407

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 408):

Рисунок 408

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 Горизонт-ВС.

В транспорте «SPICE» (прямом) минимальные параметры для настройки:

- Основное (Рисунок 409Рисунок 409):

Рисунок 409

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 410Рисунок 410):

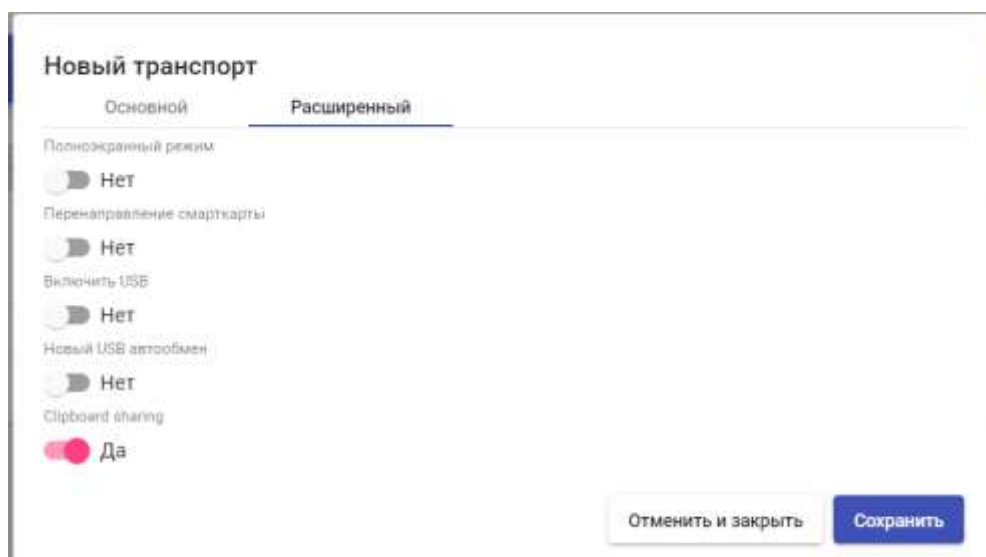


Рисунок 410

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 411):

The screenshot shows a web-based configuration interface for a 'Новый транспорт' (New Transport) window. The interface has four tabs: 'Основной' (Basic), 'Учётные данные' (Credentials), 'Параметры' (Parameters), and 'Расширенный' (Advanced). The 'Основной' tab is active. It contains several input fields and a toggle switch. The 'Имя' (Name) field is required and contains the text 'Имя этого элемента'. The 'Комментарий' (Comment) field is optional and contains 'Комментарий этого элемента'. The 'Приоритет' (Priority) field is required and contains the value '1'. The 'Сетевой доступ' (Network access) toggle switch is turned on, labeled 'Да'. The 'Сети' (Networks) dropdown menu is set to 'Сети, ассоциированные с транспортом. Если сети не выбраны, это означает все сети'. The 'Разрешение устройств' (Device permission) dropdown menu is set to 'Если пусто, будет разрешено использовать любое устройство, совместимое с этим транспортом'. The 'Сервис пулы' (Service pools) dropdown menu is set to 'Текущие привязанные пулы услуг'. At the bottom right, there are two buttons: 'Отменить и закрыть' (Cancel and close) and 'Сохранить' (Save).

Рисунок 411

Имя: Имя транспорта.

Приоритет: приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортных средств 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 412):

Имя пользователя: имя пользователя, которое будет использоваться для входа в виртуальный рабочий стол.



The screenshot shows a web interface for creating a new transport. The title is 'Новый транспорт' (New Transport). There are four tabs: 'Основной' (Main), 'Учетные данные' (Account Information), 'Параметры' (Parameters), and 'Расширенный' (Advanced). The 'Учетные данные' tab is currently selected. Below the tabs, there is a label 'Имя пользователя' (Username) and a text input field. A note below the field states: 'Если не пусто, это имя пользователя будет всегда использоваться как учетные данные' (If not empty, this username will always be used as account information). At the bottom right, there are two buttons: 'Отменить и закрыть' (Cancel and Close) and 'Сохранить' (Save).

Рисунок 412

- Параметры (Рисунок 413):



Рисунок 413

Размер экрана: Разрешение окна подключения.

Экран: выбор менеджера рабочего стола (xfce, Mate, Gnome и т. д.) или виртуализация приложений Linux (VDI vAPP).

vAPP: Путь выполнения приложения для виртуализации (применяется только в том случае, если для параметра «Рабочий стол» выбрано «VDI vAPP»).

Включить звук: включает звук в соединении.

Перенаправить домашнюю папку: перенаправляет пользователя из /home.

Скорость: Оптимизация соединения.

▪ Дополнительно (Рисунок 414):

Звук: Выбор типа звукового сервера.

Клавиатура: Язык клавиатуры.

Новый транспорт

Основной Учётные данные Параметры Расширенный

Зерк
Pulse

Клавиатура
Раскладка клавиатуры (ru, us, ...)

Реск
16m-jpeg

Качество *
6

Отменить и закрыть Сохранить

Рисунок 414

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 415):

Рисунок 415

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 416):



Рисунок 416

Видимый: если этот параметр отключен, «Пул служб» не будет отображаться как доступный для пользователей на странице служб VDI («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 417):

Рисунок 417

Разрешить удаление пользователями: если этот параметр включен, пользователи могут удалять назначенные им службы. Если сервис представляет собой виртуальный рабочий стол, автоматически сгенерированный VDI, 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 VDI).

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 418):

Рисунок 418

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 можете полностью удалить «Сервис-пул», а с помощью «Редактировать» вы можете изменить его (Рисунок 419).



Рисунок 419

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 420).

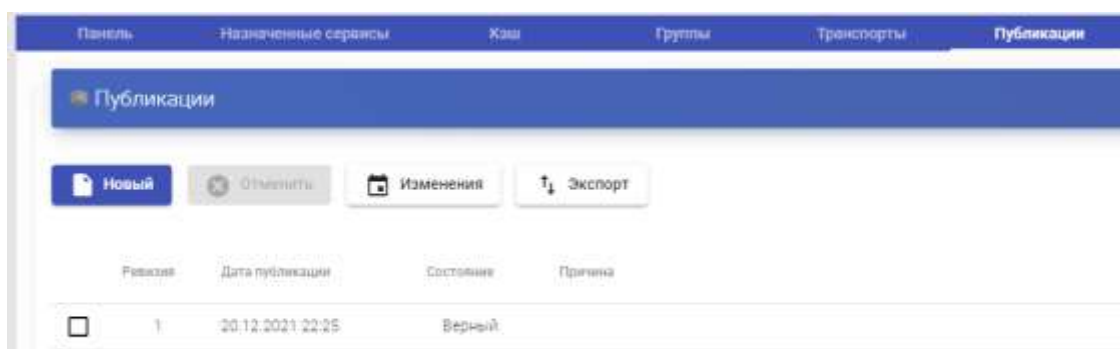


Рисунок 420

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, MAC-адрес сетевой карты VM, DNS и IP-имя виртуального рабочего стола, статус рабочего стола, если он используется, имя и IP-адрес клиента подключения, владелец машины и версия VDI Actor, установленного на машине-шаблоне (Рисунок 421).

- 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 425).

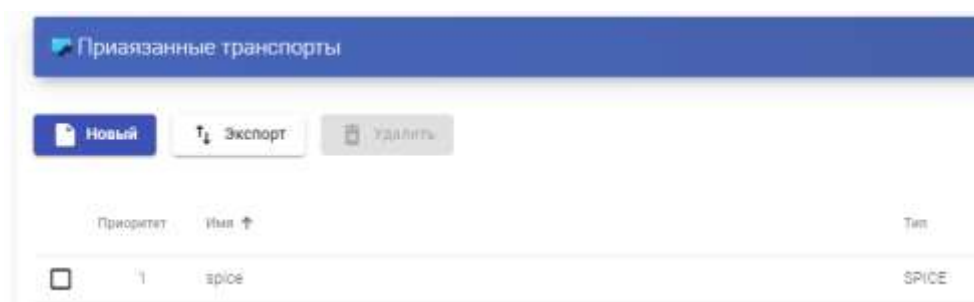


Рисунок 425

Выбрать «Транспорт», который нужно использовать в этом «пуле услуг», и сохранить (Рисунок 426).

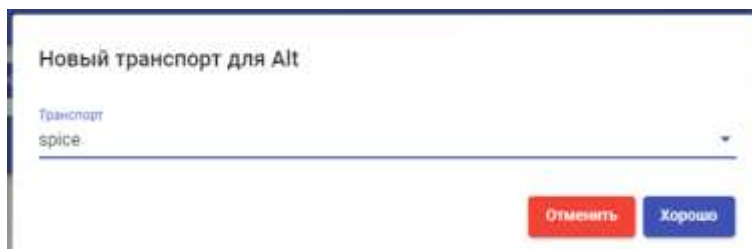


Рисунок 426

- 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 427).

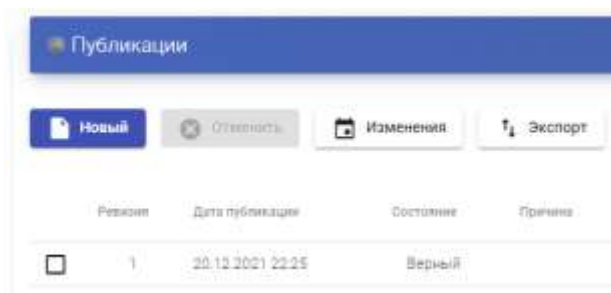


Рисунок 427

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.

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 428).

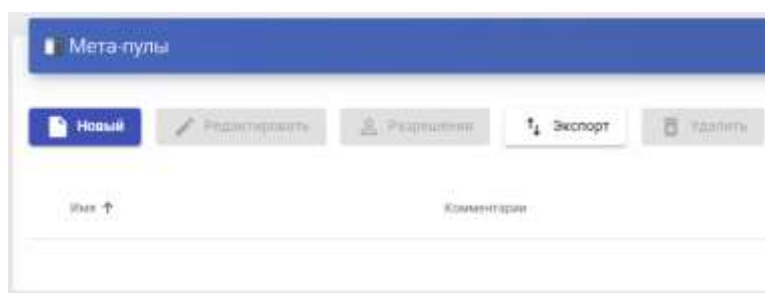


Рисунок 428

Для настройки «Метапула» необходимо будет указать:

- Основное (Рисунок 429):

Рисунок 429

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».

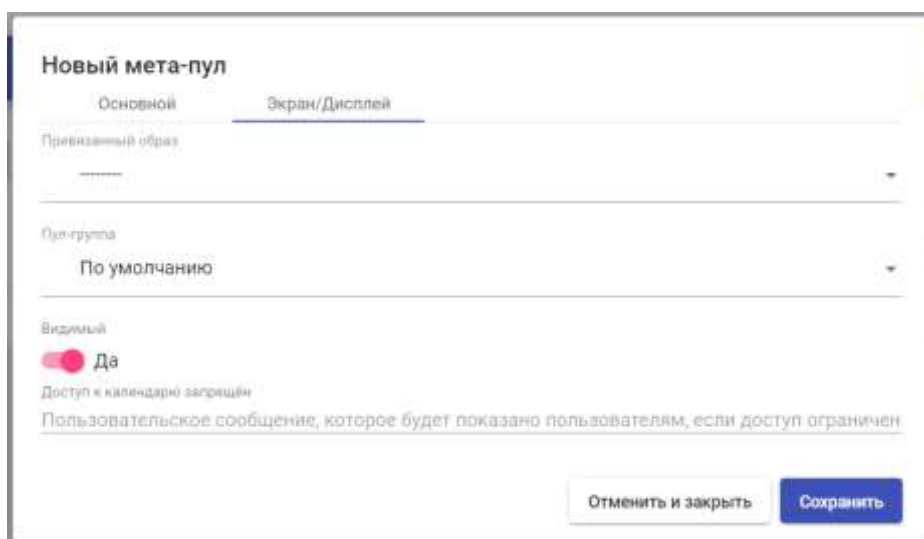
Политика: Политика, которая будет применяться при создании сервисов в «Пулах сервисов», являющихся частью «Метапула».

- 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 430Рисунок 430):



Новый мета-пул

Основной Экран/Дисплей

Привязанный образ

Оп-группа

По умолчанию

Видимый

Да

Доступ к календарю запрещён

Пользовательское сообщение, которое будет показано пользователям, если доступ ограничен

Отменить и закрыть Сохранить

Рисунок 430

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 VDI («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 431):

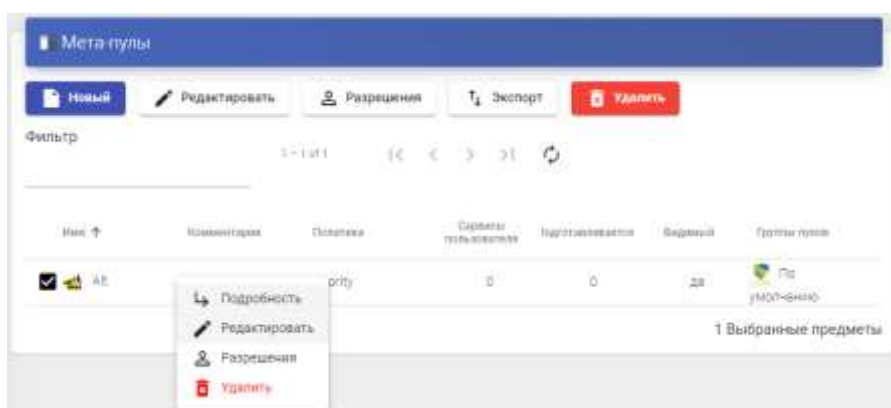


Рисунок 431

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 432).

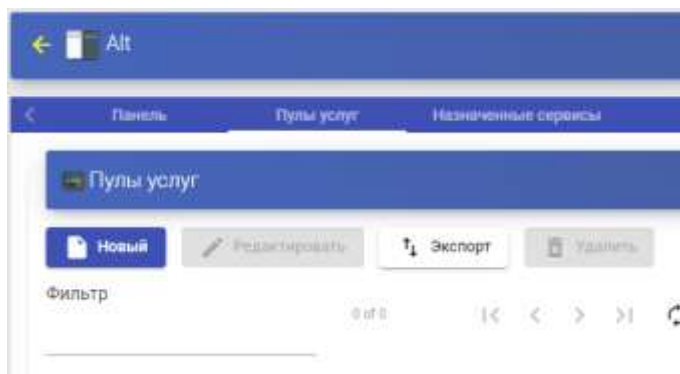


Рисунок 432

Для добавления «Сервисного пула» необходимо указать следующие параметры (Рисунок 433):

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».

Новый пул участников

Приоритет
0

Пул услуг
IE

Включено?
☒ да

Отменить Хорошо

Рисунок 433

Можно добавить столько, сколько нужно, комбинируя службы, размещенные на разных платформах виртуализации (VMware, KVM, Azure и т. д.), серверах приложений и статических устройствах (Рисунок 334).

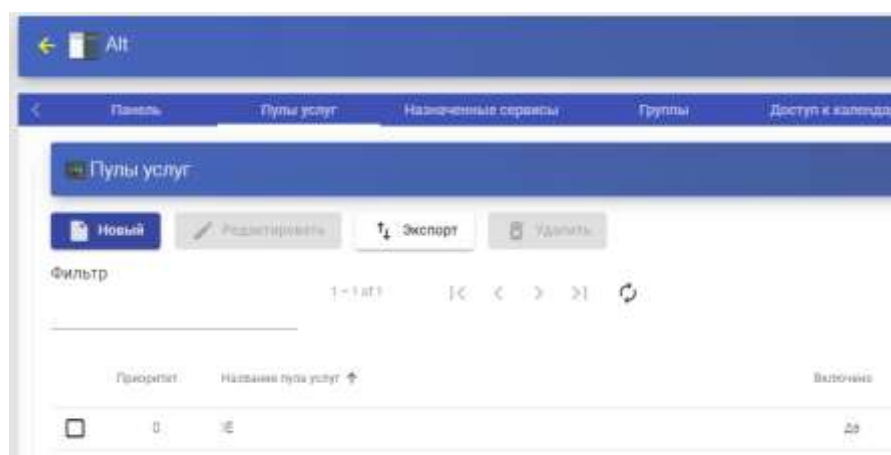


Рисунок 434

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».

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 435).

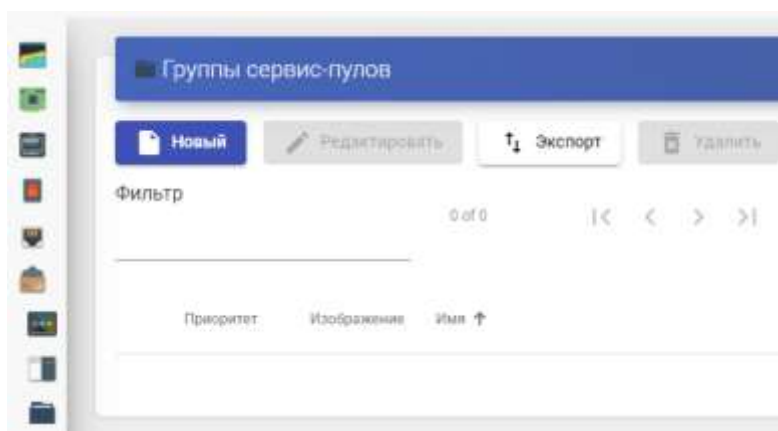


Рисунок 435

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 436):

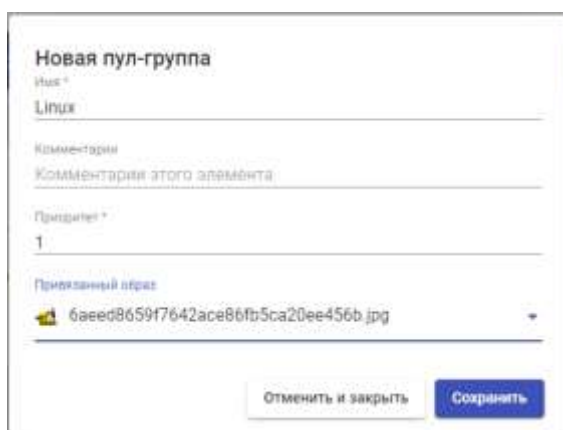


Рисунок 436

После создания он будет доступен для назначения в «Сервисный пул» (Рисунок 437).

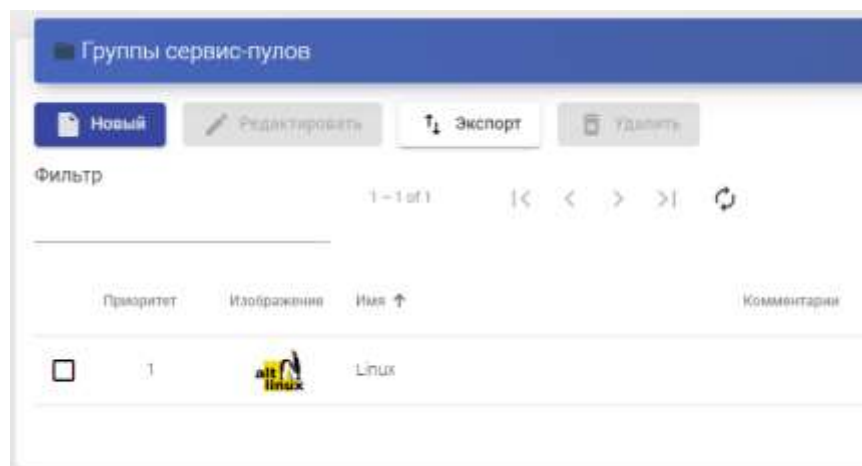


Рисунок 437

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 438).

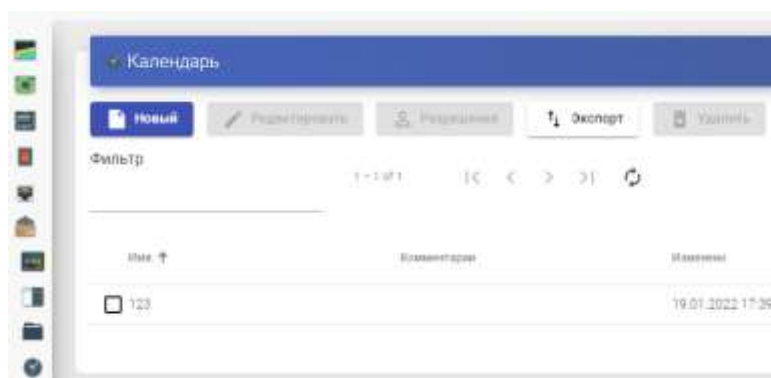


Рисунок 438

Указать описательное имя для идентификации календаря (Рисунок 439).

Рисунок 439

Сохранить, и будет действующий календарь, чтобы начать создавать правила, которые позже можно применить к сервису через «Сервис-пулов» (Рисунок 440).

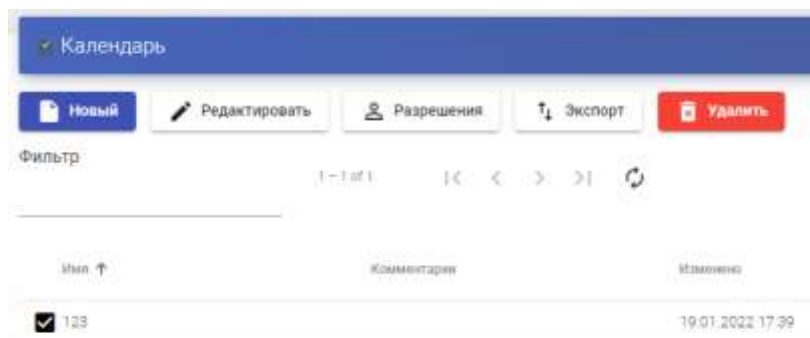


Рисунок 440

В «Календаре» можно зарегистрировать различные типы правил, чтобы запланировать доступность услуг в определенное время.

Чтобы создать правило, открыть календарь и нажать «Создать» (Рисунок 441Рисунок 441).



Рисунок 441

Минимальные параметры для настройки в «Правило» (Рисунок 442):

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.

Новое правило

Имя

Комментарии

Событие

Время начала: 00:00 | Продолжительность: 0 | Единицы длительности: Минуты

Repetition

Дата начала: 04.02.2022 | Повторять до даты: Навсегда

Частота: Ежедневно | Повторять каждый: 1 день

Панель

Это правило будет действовать каждый 1 день, от 04.02.2022 далее, начиная с 00:00 без длительности

Отменить | Хорошо

Рисунок 442

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 443):

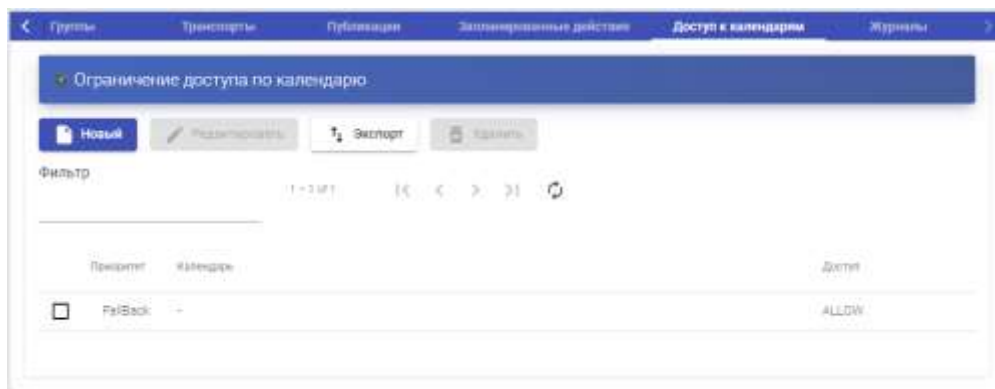


Рисунок 443

Указать приоритет доступа, выбрать существующий календарь и отметить действие, которое будет применяться при доступе к сервису (Рисунок 444).

The form is titled 'Новое правило доступа для Alt'. It contains three input fields: 'Приоритет' with a dropdown menu showing 'Q', 'Календарь' with a dropdown menu, and 'Действие' with a dropdown menu showing 'ALLOW'. At the bottom right of the form are two buttons: 'Отменить' (red) and 'Хорошо' (blue).

Рисунок 444

После сохранения «Пул услуг» будет с настроенным календарем доступа (Рисунок 445).

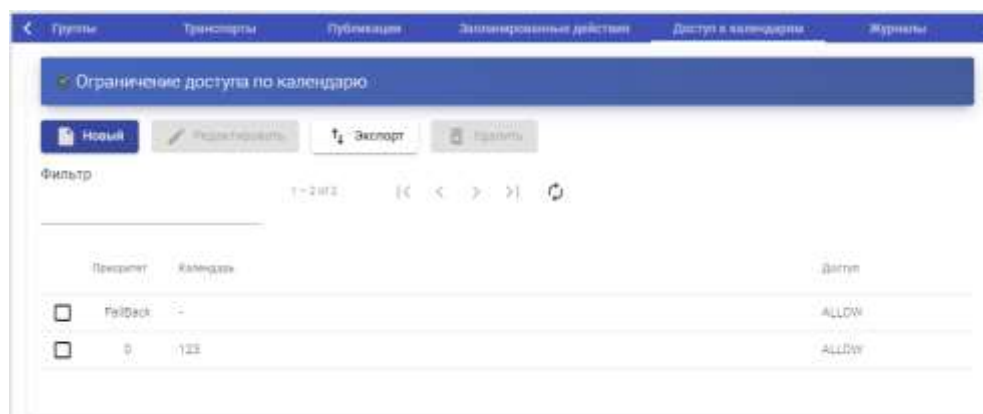


Рисунок 445

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 446Рисунок 446).

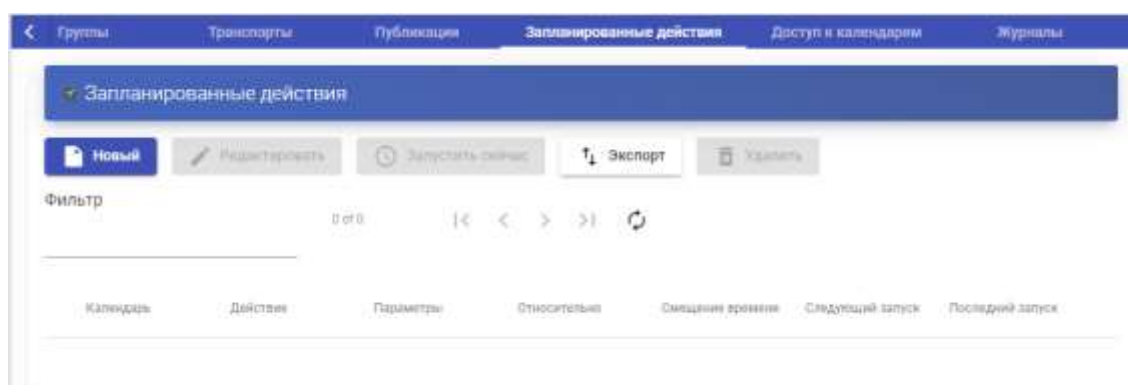


Рисунок 446

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 447).

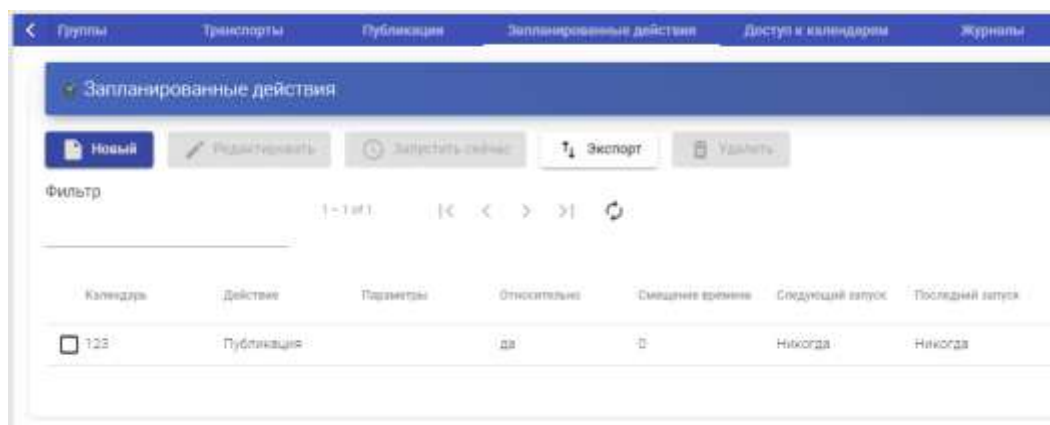


Рисунок 447

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 448):

Редактировать пользователя vdiadmin

Имя пользователя
vdiadmin

Пароль
vdiadmin

Комментарий

Состояние
Включено

Роль
Штатный сотрудник

Пароль

Пароль
admin

Отменить Хорошо

Рисунок 448

Чтобы включить разрешения в различных элементах администрирования, выбрать элемент и нажать «Разрешения». Например, в «Поставщик услуг» (Рисунок 449).



Рисунок 449

В окне разрешений нажать «Новое разрешение...» для групп и пользователей и выбрать аутентификатор и группу/пользователя, к которым будет применяться разрешение (Рисунок 450).

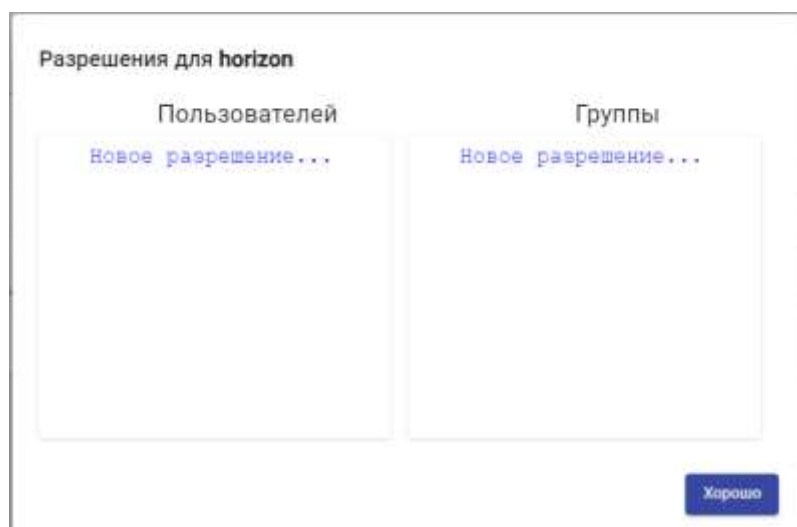


Рисунок 450

Нужно указать, будет ли этот пользователь или группа иметь доступ для чтения к элементу («Только чтение») или полный доступ («Полный доступ») (Рисунок 451).

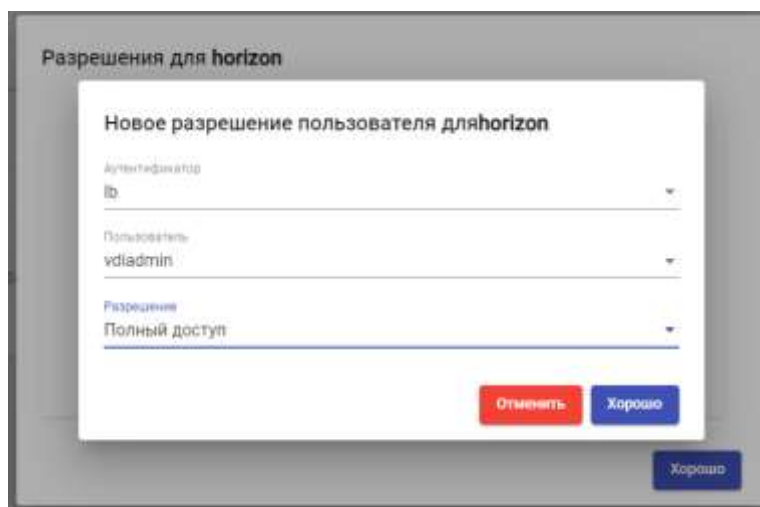


Рисунок 451

После применения пользователи, у которых включена опция «Сотрудник», смогут получить доступ к этому элементу администрирования с назначенными разрешениями (Рисунок 452).

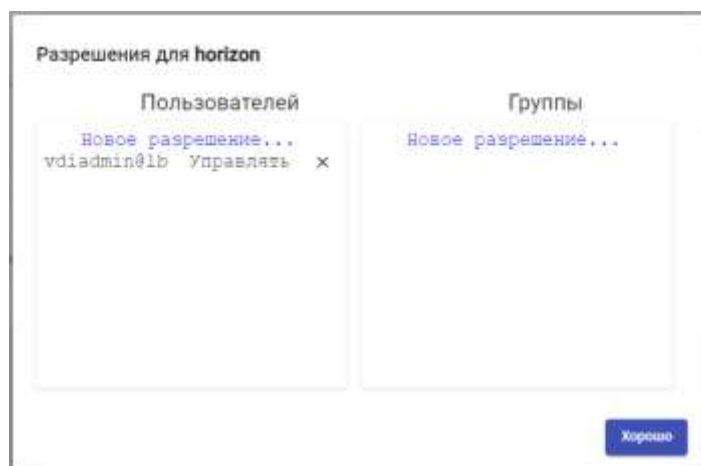


Рисунок 452

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.).

Галерея

VDI 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 VDI, перейти в раздел «Инструменты» и выбрать «Галерея» (Рисунок 453):

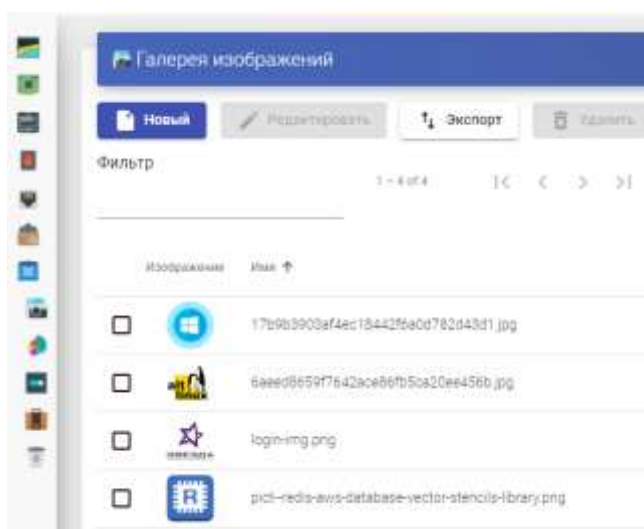


Рисунок 453

Выбрать «Новый», чтобы добавить новый образ в репозиторий. Необходимо указать имя и с помощью кнопки «Выбрать изображение» найти образ, который нужно загрузить (Рисунок 454Рисунок 454).

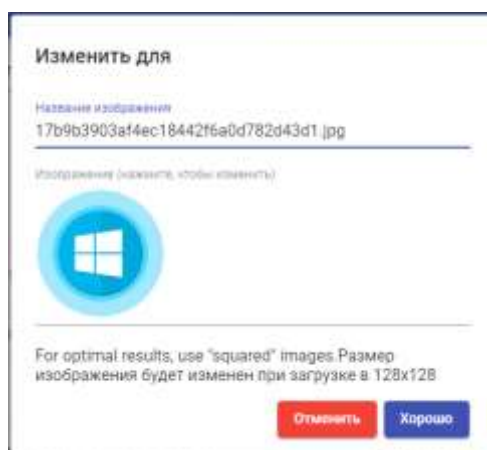


Рисунок 454

После того как образ будет сохранен, он будет доступен для назначения в «Сервисный пул» или «Группу пулов».

Отчеты

VDI позволяет автоматически генерировать отчеты по различным элементам платформы.

Чтобы получить доступ к отчетам, войти в раздел «Инструменты» и выбрать «Отчеты» (Рисунок 455).

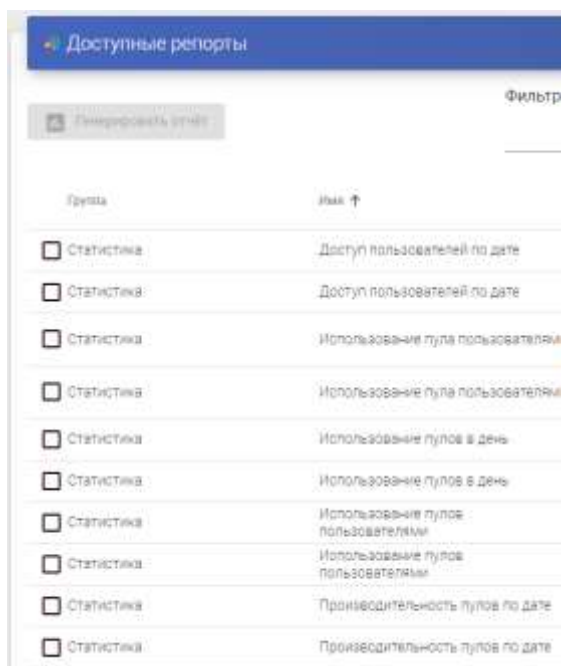


Рисунок 455

В VDI можно генерировать различные отчеты:

- Список пользователей: создает отчет со всеми пользователями, принадлежащими аутентификатору. Выбрать аутентификатор и нажать «Сохранить» (Рисунок 456).

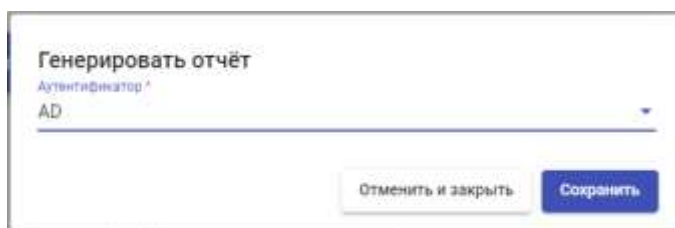
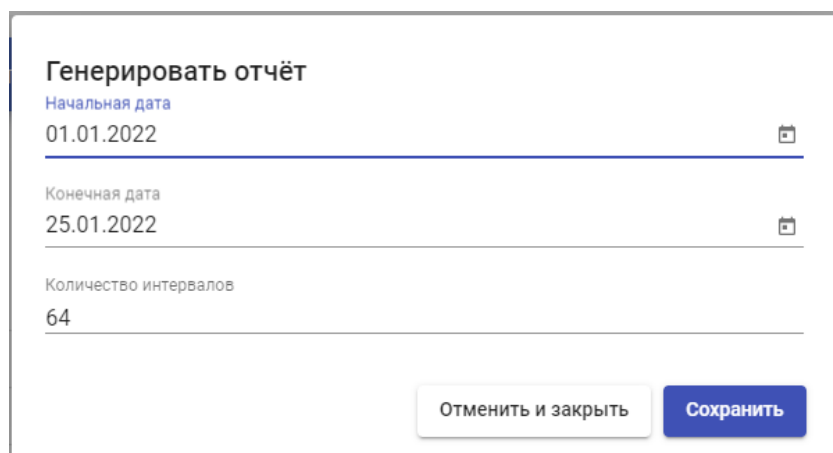


Рисунок 456

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 457):



Генерировать отчёт

Начальная дата
01.01.2022

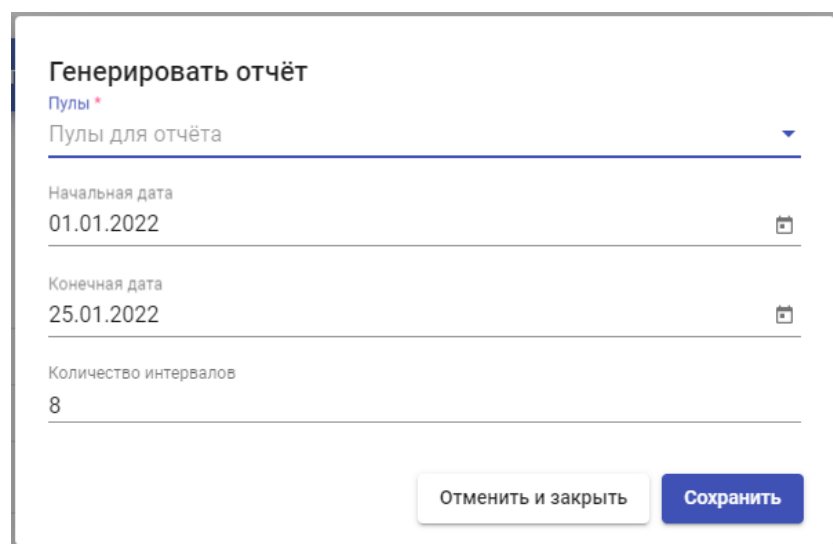
Конечная дата
25.01.2022

Количество интервалов
64

Отменить и закрыть Сохранить

Рисунок 457

▪ 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 458):



Генерировать отчёт

Пулы *
Пулы для отчёта

Начальная дата
01.01.2022

Конечная дата
25.01.2022

Количество интервалов
8

Отменить и закрыть Сохранить

Рисунок 458

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 VDI необходимо перезапустить сервер VDI, чтобы изменения вступили в силу.

Чтобы получить доступ к параметрам расширенной конфигурации VDI, перейти в раздел «Инструменты» и выбрать «Конфигурация» (Рисунок 459):

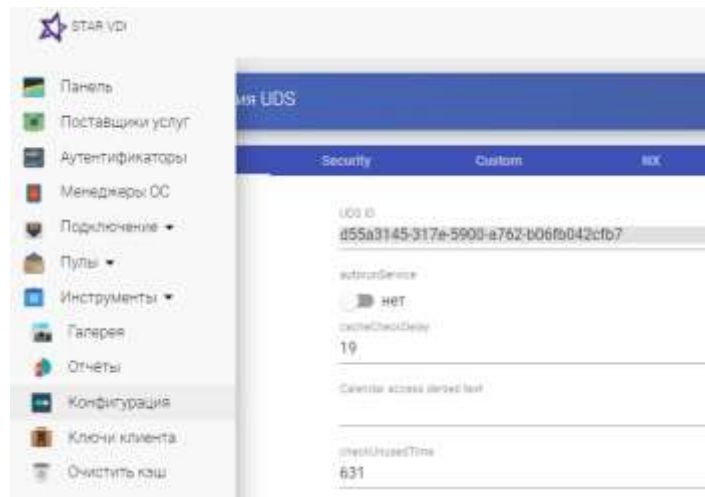


Рисунок 459

VDI

VDI 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.

Безопасность

Описаны параметры, связанные с безопасностью системы VDI:

AllowRootWebAccess: позволяет суперпользователю войти в систему (пользователю, созданному в мастере настройки VDI-сервера) на портале входа VDI.

Изменение этой переменной не повлияет на доступ пользователя root через консоль ОС Linux.

По умолчанию: да.

Behind a proxy: указывает системе, что серверы VDI находятся «за» прокси-сервером (например, среда VDI в режиме высокой доступности с прокси-сервером 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 VDI 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 VDI-Server.

SuperUser: имя суперпользователя, созданное в мастере настройки VDI-Server.

Trusted Hosts: хосты, которые VDI считает безопасными. Эти хосты могут делать «чувствительные» запросы к VDI, такие как туннели.

По умолчанию: "*" (все разрешено), допускает значения диапазона адресов.

Пользовательский

Описаны параметры, связанные с графической настройкой VDI (портал входа и обслуживания пользователей):

CSS: поддерживает код для изменения страниц стиля VDI 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.

NX

Описаны параметры, относящиеся к «Транспорту» NX:

DownloadUrl: веб-адрес для загрузки программного обеспечения NX.

DownloadUrlMACOS: веб-адрес загрузки программного обеспечения NX для MAC.

PCoIP

Описаны параметры, относящиеся к Teradici PCoIP «Транспорт»:

DownloadUrl: адрес загрузки программного обеспечения клиента PCoIP.

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.

SAML

Описаны параметры, связанные с работой аутентификатора SAML:

Global logout on exit: указывает режим выхода из системы. Если этот параметр включен, при выходе VDI 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).

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: VDI.

Язык: язык устройства.

По умолчанию: us.

Привилегия: Уровень привилегии пользователя.

По умолчанию: НЕТ.

6 Инструкция по настройке многофункционального комплекса сетевой защиты

6.1 Установка ключевой информации

Для создания защищенного канала передачи данных на устройство МКСЗ «Горизонт-ВС VPN/FW» необходимо загрузить ключевую информацию. Ключевая информация состоит из корневого сертификата и ключевой пары. Корневой сертификат требуется для проверки ключевой пары. Ключевая пара представляет из себя контейнер, который содержит открытый и закрытый ключи. Сгенерировать ключевую информацию можно с помощью утилиты DmCrypt-Util.

6.2 Установка корневого сертификата

Чтобы загрузить на устройство МКСЗ «Горизонт-ВС VPN/FW» ключевую информацию, необходимо в главном меню выбрать пункт (см. **Рисунок 460 - Пункт меню «VPN – Сертификаты и ключи» и положение кнопки «Добавить новый объект ИОК»**) «VPN – Сертификаты и ключи» и нажать на кнопку **Добавить новый объект ИОК**.

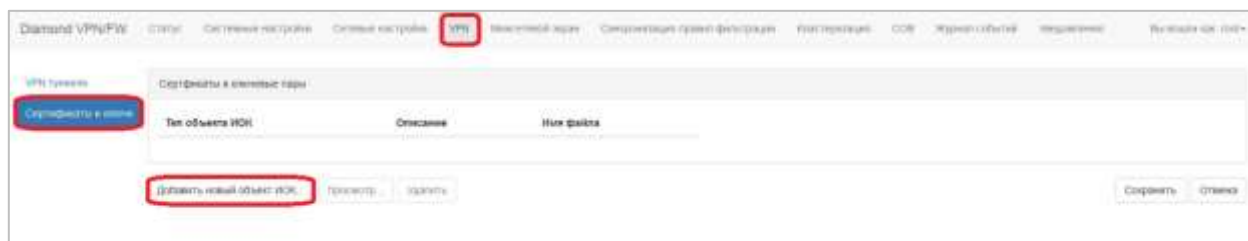


Рисунок 460 - Пункт меню «VPN – Сертификаты и ключи» и положение кнопки «Добавить новый объект ИОК»

Для загрузки на устройство МКСЗ «Горизонт-ВС VPN/FW» корневого сертификата, в новом окне необходимо нажать на кнопку **Загрузить новый объект ИОК** (Рисунок 461).



Рисунок 461 - Положение кнопки «Загрузить новый объект ИОК»

В окне **Загрузка нового сертификата или ключевой пары** необходимо нажать на кнопку **Обзор** и выбрать файл с корневым сертификатом. Файл с корневым сертификатом должен иметь расширение «*.crt» (Рисунок 462).

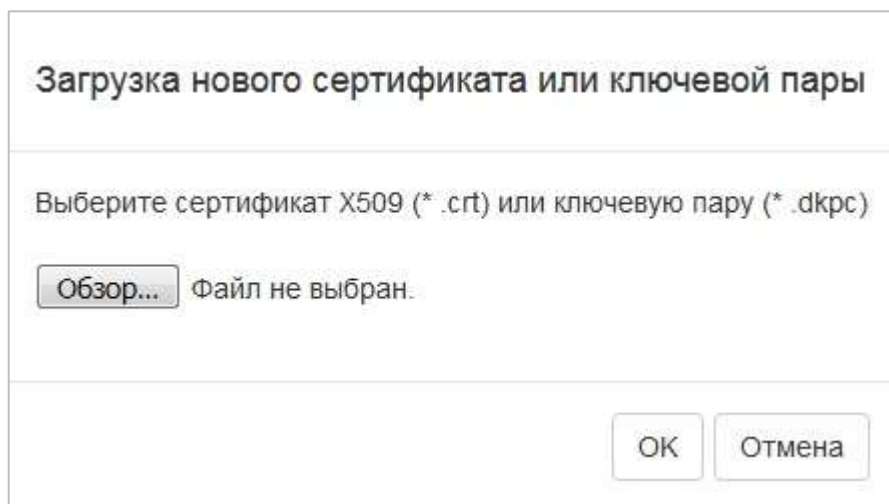


Рисунок 462- Выбор нового сертификата

После загрузки корневого сертификата, в окне **Загрузка нового сертификата или ключевой пары** появится сообщение **Сертификат X509 успешно загружен** (Рисунок 463).

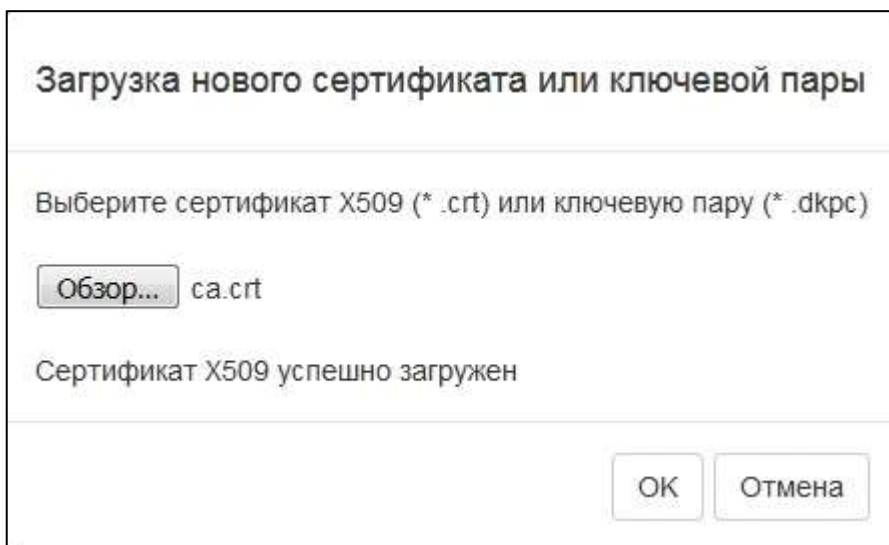


Рисунок 463 - Результат загрузки сертификата

Для продолжения необходимо нажать на кнопку **ОК**. В таблице **Добавление нового объекта ИОК** появится информация о корневом сертификате, которая включает в себя: тип объекта ИОК, издатель

сертификата, серийный номер сертификата, владелец сертификата, период действия сертификата. Для продолжения необходимо нажать на кнопку **ОК** (Рисунок 364).



Рисунок 464 - Информация о корневом сертификате

Для сохранения корневого сертификата необходимо нажать на кнопку **Сохранить** (Рисунок 465).



Рисунок 465 - Положение кнопки «Сохранить»

6.3 Установка ключевой пары

Чтобы загрузить на устройство МКСЗ «Горизонт-ВС VPN/FW» ключевую информацию, необходимо в главном меню выбрать пункт «VPN – Сертификаты и ключи» и нажать на кнопку **Добавить новый объект ИОК** (Рисунок 466).



Рисунок 466 - Пункт меню «VPN – Сертификаты и ключи» и положение кнопки «Добавить новый объект ИОК»

Для загрузки на устройство МКСЗ «Горизонт-ВС VPN/FW» ключевой пары, в новом окне необходимо нажать на кнопку «Загрузить новый объект ИОК» (Рисунок 467).



Рисунок 467 - Положение кнопки «Загрузить новый объект ИОК»

В окне **Загрузка нового сертификата или ключевой пары** необходимо нажать на кнопку **Обзор** и выбрать файл с ключевой парой. Файл с ключевой парой должен иметь расширение «*.dkrc» (Рисунок 468).

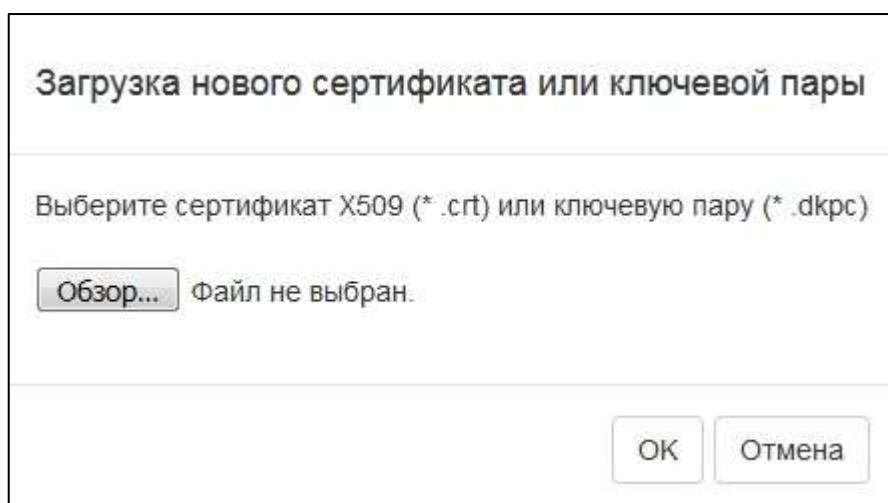


Рисунок 468 - Выбор новой ключевой пары

После загрузки ключевой пары, в окне **Загрузка нового сертификата или ключевой пары** появится сообщение **Ключевая пара успешно загружена. Введите пароль для ключевой пары** (Рисунок 469). Контейнер с ключевой парой защищен паролем, который задается при создании открытого и закрытого ключей.

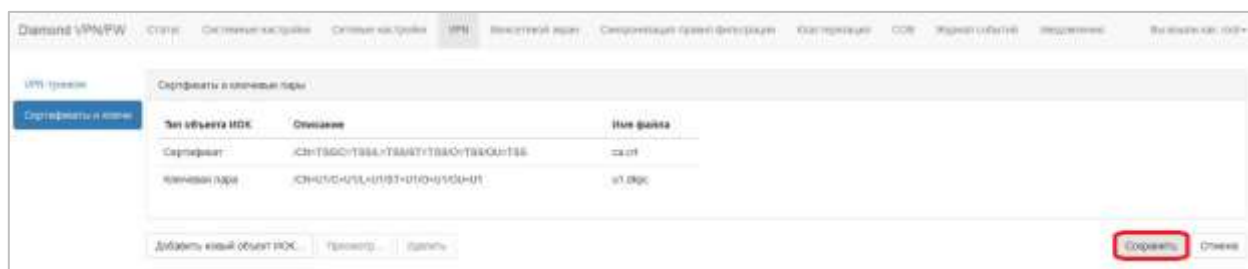


Рисунок 471 - Положение кнопки «Сохранить»

6.4 Просмотр ключевой информации

Для просмотра ключевой информации необходимо в главном меню МКСЗ Горизонт-ВС VPN/FW выбрать пункт **VPN – Сертификаты и ключи**. В таблице **Сертификаты и ключевые пары** необходимо выбрать объект ИОК, информацию о котором необходимо посмотреть и нажать на кнопку **Просмотр** (Рисунок 472).

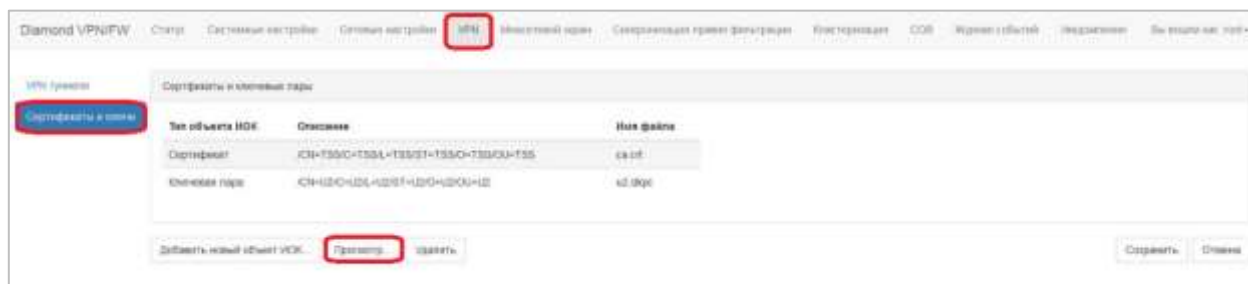


Рисунок 472 - Пункт меню «VPN – Сертификаты и ключи»

В таблице **Просмотр информации об объекте ИОК** представлена информация об объекте ИОК (Рисунок 473).



Рисунок 473 - Таблица просмотра информации об объекте ИОК

Для возвращения в предыдущие меню необходимо нажать на кнопку **Закреть**.

6.5 Настройка VPN сервиса

Для создания VPN сервиса необходимо в главном меню выбрать пункт **VPN – VPN туннели** и нажать на кнопку **Добавить туннель**. В таблице **Создание VPN туннеля** необходимо задать параметры VPN сервиса в зависимости от режима работы. После настройки VPN сервиса необходимо сохранить изменения и перевести сервис в состояние **Сервис работает**.

6.5.1 Управление VPN сервисом

Для запуска VPN сервиса необходимо в таблице **VPN туннели** выбрать сервис и нажать на кнопку **Запустить**. Состояние сервиса измениться на **Сервис работает**. Для сохранения настроек необходимо нажать на кнопку **Сохранить**.

Для удаления VPN сервиса необходимо в таблице **VPN туннели** выбрать сервис и нажать на кнопку **Остановить**. Состояние сервиса измениться на **Сервис остановлен**. После остановки VPN сервиса необходимо выбрать его и нажать на кнопку **Удалить**. Для сохранения настроек необходимо нажать на кнопку **Сохранить**.

Для редактирования VPN сервиса необходимо в таблице «VPN туннели» выбрать сервис и нажать на кнопку **Остановить**. Состояние сервиса измениться на **Сервис остановлен**. После остановки VPN сервиса необходимо выбрать его и нажать на кнопку **Редактировать**. В таблице **Создание VPN туннеля** необходимо внести изменения в настройки VPN сервиса и нажать на кнопку **ОК**. Для сохранения настроек необходимо нажать на кнопку **Сохранить**.

6.5.2 Настройка VPN сервиса, режим сервера

Для настройки сервиса в режиме сервера необходимо в главном меню выбрать пункт **VPN – VPN туннели** и нажать на кнопку **Добавить туннель**. В таблице **Создание VPN туннеля** необходимо задать параметры VPN сервиса (Рисунок 474).

Рисунок 474 - Окно «Создание VPN туннеля» и настройка режима сервера

Параметры, которые необходимо задать для настройки VPN сервиса, представлены в таблице (см. таблицу 1).

Таблица 1 – Параметры настройки VPN сервиса

Название поля	Описание
Режим работы	В поле необходимо выбрать режим работы «Сервер».
Описание	В поле необходимо задать название, которое может описывать объект, с которым связан данный сервис. Поле носит информационный характер.
Ключевая информация	В поле необходимо выбрать файл с ключевой информацией, который был загружен на устройство.
Название виртуального интерфейса	В поле необходимо задать название виртуального сетевого интерфейса, который появится в системе, после запуска сервиса.
MTU на виртуальном интерфейсе	В поле необходимо задать значение MTU на виртуальном сетевом интерфейсе.
Ip-адрес и маска подсети	В поле необходимо задать ip-адрес и маску подсети для виртуального сетевого интерфейса.
Сетевой порт для подключения	В поле необходимо задать сетевой порт для подключения других устройств МКСЗ «Горизонт-BC VPN/FW» или Клиента «Горизонт-BC VPN/FW».

6.5.3 Настройка VPN сервиса, режим мультисервер

Для настройки сервиса в режиме мультисервера необходимо в главном меню выбрать пункт «VPN – VPN туннели» и нажать на кнопку **Добавить туннель**. В таблице **Создание VPN туннеля** необходимо задать параметры VPN сервиса (см.Рисунок 475).

Рисунок 475 - Окно «Создание VPN туннеля» и настройка режима сервера

Параметры, которые необходимо задать для настройки VPN сервиса, представлены в таблице (см. таблицу 1).

Таблица 2 – Параметры настройки VPN сервиса

Название поля	Описание

Режим работы	В поле необходимо выбрать режим работы «Сервер для множества клиентов».
Описание	В поле необходимо задать название, которое может описывать объект, с которым связан данный сервис. Поле носит информационный характер.
Ключевая информация	В поле необходимо выбрать файл с ключевой информацией, который был загружен на устройство.
Ключевая информация	В поле необходимо выбрать файл с ключевой информацией, который был загружен на устройство.
Название виртуального интерфейса	В поле необходимо задать название виртуального сетевого интерфейса, который появится в системе, после запуска сервиса.
MTU на виртуальном интерфейсе	В поле необходимо задать значение MTU на виртуальном сетевом интерфейсе.
Ip-адрес и маска подсети	В поле необходимо задать ip-адрес и маску подсети для виртуального сетевого интерфейса.
Сетевой порт для подключения	В поле необходимо задать сетевой порт для подключения других устройств МКСЗ «Горизонт-BC VPN/FW» или Клиента «Горизонт-BC VPN/FW».

6.5.4 Настройка VPN сервиса, режим клиента

Для настройки сервиса в режиме клиента необходимо в главном меню выбрать пункт **VPN – VPN туннели** и нажать на кнопку **Добавить туннель**. В таблице **Создание VPN туннеля** необходимо задать параметры VPN сервиса (Рисунок 476).

Создание VPN туннеля

Основные параметры

Режим работы: Клиент

Описание:

Ключевая информация: 1C4-127C-42E1-122ST-12XC-122OU-122

Параметры виртуального интерфейса

Название виртуального интерфейса:

MTU на виртуальном интерфейсе: 9000

IP адрес/маска подсети: 10

Дополнительные параметры

Повторное подключение в случае разрыва: ☒

IP адрес сервера для подключения:

OK Отмена

Рисунок 476 - Меню «Создание VPN туннеля», режим клиент

Параметры, которые необходимо задать для настройки VPN сервиса, представлены в таблице (см. таблицу 3).

Таблица 3 – Параметры настройки VPN сервиса

Название поля	Описание

Режим работы	В поле необходимо выбрать режим работы «Клиент».
Описание	В поле необходимо задать название, которое может описывать объект, с которым связан данный сервис. Поле носит информационный характер.
Ключевая информация	В поле необходимо выбрать файл с ключевой информацией, который был загружен на устройство.
Название виртуального интерфейса	В поле необходимо задать название виртуального сетевого интерфейса, который появится в системе, после запуска сервиса.
MTU на виртуальном интерфейсе	В поле необходимо задать значение MTU на виртуальном сетевом интерфейсе.
Ip-адрес и маска подсети	В В поле необходимо задать ip-адрес и маску подсети для виртуального сетевого интерфейса.
Повторное подключение в случае разрыва	При установке флага в случае разрыва соединения устройство в автоматическом режиме будет пытаться восстановить подключение.
Ip-адрес сервера для подключения	В поле необходимо задать ip-адрес и сетевой порт сервера, с которым необходимо установить защищенное соединение. Данные необходимо задать в формате: ip-адрес: сетевой порт. Например, 192.168.1.100:1024, где 192.168.1.100 – это ip-адрес удаленного сервера, а 1024 сетевой порт для подключения.

6.5.5 Просмотр информации о VPN сервисе

Для просмотра информации о VPN сервисе необходимо в главном меню выбрать пункт **VPN – VPN туннели**. В таблице **VPN туннели** (см. таблицу 4) представлена информацию о текущих VPN сервисах. Для каждого сервиса отображается режим работы, название сервиса, название виртуального интерфейса, ip-адрес и состояние сервиса (Рисунок 477).

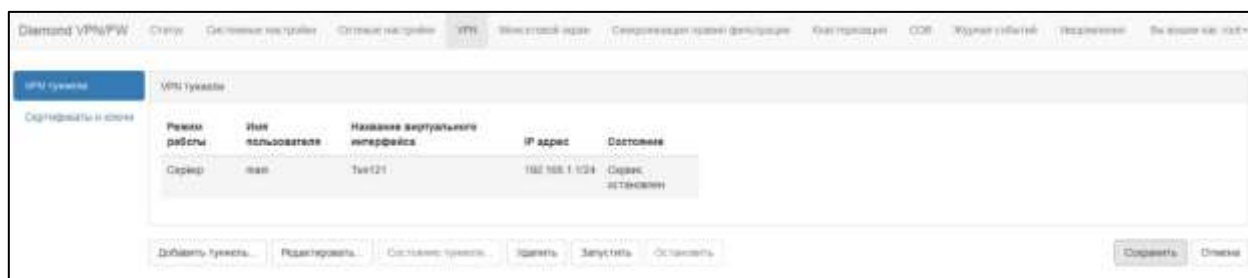


Рисунок 477 - Таблица информации о VPN сервисах

Таблица 4 - **VPN туннели**

Название поля	Описание
Режим работы	В поле необходимо выбрать режим работы «Клиент».
Название сервиса	Название может описывать объект, с которым связан данный сервис. Поле носит информационный характер.
Название виртуального интерфейса	В поле необходимо выбрать файл с ключевой информацией, который был загружен на устройство.
Название виртуального интерфейса	Название виртуального сетевого интерфейса, который появится в системе, после запуска сервиса.
Ip-адрес виртуального интерфейса	Ip-адрес и маска подсети, которые заданы на виртуальном сетевом интерфейсе.
Состояние сервиса	Сервис может находиться в двух состояниях: сервис работает и сервис остановлен.

Для получения дополнительной информации о VPN сервисе необходимо в таблице **VPN туннели** выбрать нужный VPN сервис и нажать на кнопку «Состояние туннеля». В таблице **Создание VPN туннеля** (см. таблицу 5) представлена информация о названии VPN сервиса, состоянии сервиса, времени начала работы, количество переданных и полученных байт, информация об удаленных клиентах (Рисунок 478).



Рисунок 478 - Таблица «Создание VPN туннеля»

Таблица 5 – Создание VPN туннеля

Название поля	Описание
Состояние	В поле отображается текущие состояние VPN сервиса.
Время начала работы VPN туннеля	В поле отображается время начала работы VPN сервиса.
Байт передано/получено	В поле отображается количество байт, которые были переданы и получены через защищенное соединение.
Удаленные клиенты	В поле отображается информация об удаленных клиентах, которые в настоящий момент подключены.

Для возвращения в предыдущие меню, необходимо нажать на кнопку **Заккрыть**.

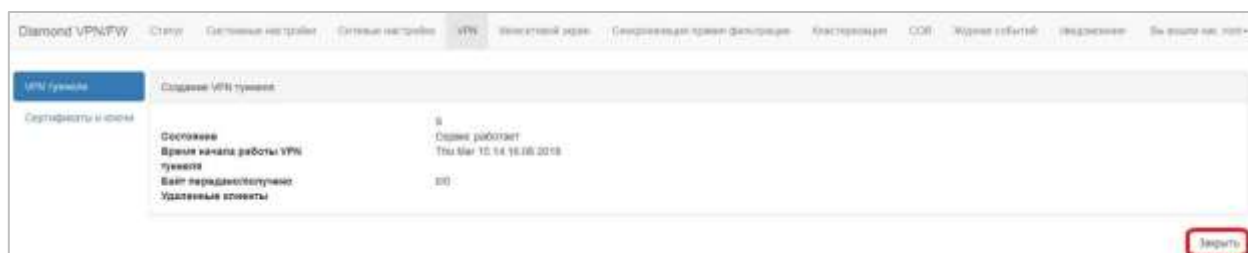


Рисунок 479 - Положение кнопки «Заккрыть»

6.6 Настройка резервирования

Для настройки механизма резервирования защищенного соединения необходимо в главном меню выбрать пункт **VPN – VPN туннели** и нажать на кнопку **Добавить туннель** (Рисунок 480).

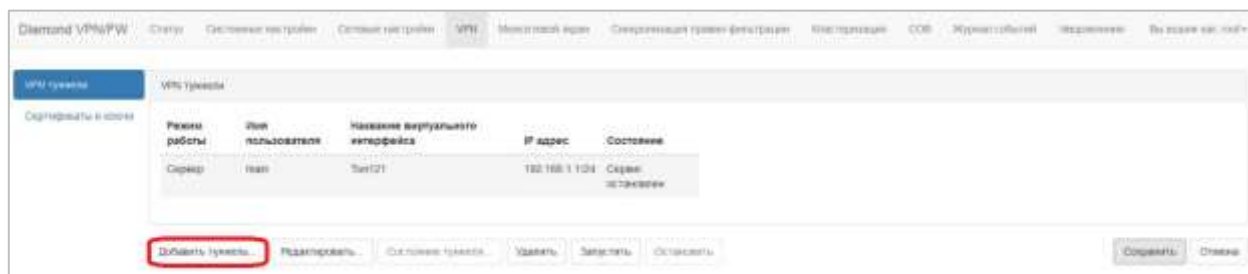


Рисунок 480 - Положение кнопки «Добавить туннель»

В таблице «Создание VPN туннеля» в поле «Режим работы» необходимо выбрать значение **Клиент**. В поле ip-адрес сервера для подключения необходимо задать ip-адрес и сетевой порт сервера, с которым необходимо установить защищенное соединения. Данные необходимо задать в формате: «ip-адрес: сетевой порт». Например, 192.168.1.100:1024, где 192.168.1.100 – это ip-адрес удаленного сервера, а 1024 сетевой порт для подключения (Рисунок 481).

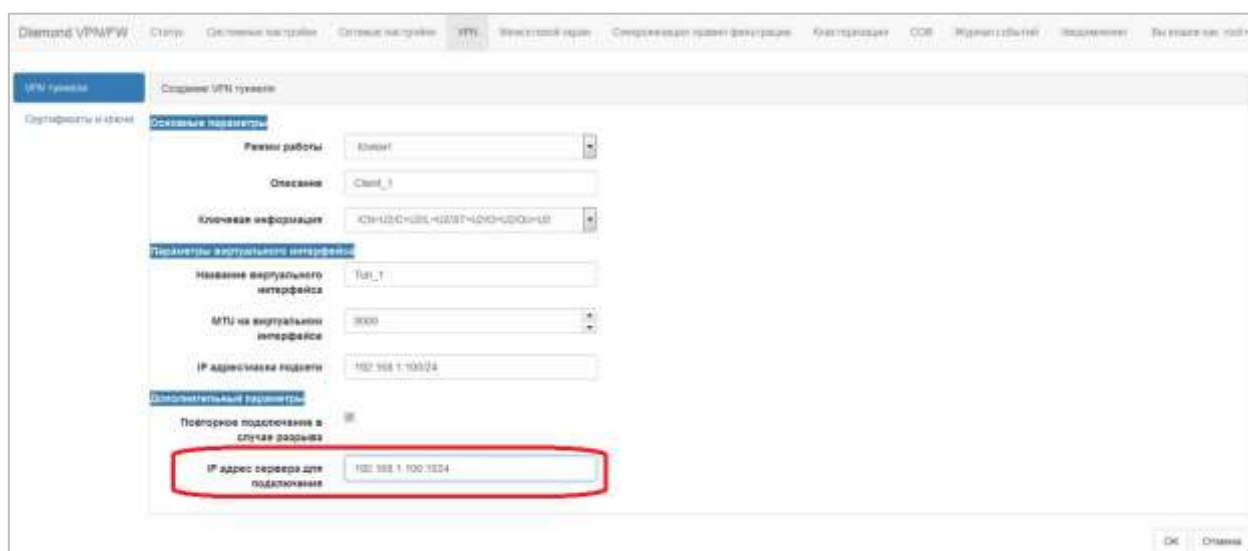


Рисунок 481 - Меню Создание VPN туннеля, режим клиент

6.6.2 Настройка соединения P2M

Защищенное соединение точка-мультиточка (P2M) можно установить между тремя и более устройствами МКСЗ «Горизонт-ВС VPN/FW». Одно из устройств необходимо настроить в режиме сервера, остальные устройства необходимо настроить в режиме клиента. Данная возможность позволяет настроить защищенные соединения между несколькими устройствами в одной ip подсети. Данный тип соединения позволяет осуществлять сетевое взаимодействие как между сервером и клиентом, так и между клиентами. Сетевое взаимодействие между сервером и клиентом, так и между клиентами осуществляется через устройство МКСЗ «Горизонт-ВС VPN/FW», которое работает в режиме сервера.

6.6.3 Настройка L3overVPN

Защищенное соединение в режиме L3overVPN позволяет установить защищенное соединение между двумя и более устройствами МКСЗ «Горизонт-ВС VPN/FW». Сетевой трафик, который проходит через защищенное соединение, участвует в процессе коммутации и маршрутизации, т.е. на втором и третьем уровнях стандартной сетевой модели.

6.6.4 Настройка L2overVPN

Защищенное соединение в режиме L2overVPN позволяет установить защищенное соединение между двумя и более устройствами МКСЗ «Горизонт-ВС VPN/FW». Сетевой трафик, который проходит через защищенное соединение, участвует только в процессе коммутации и не участвует в процессе маршрутизации. Данный режим позволяет связать два и более удаленных L2 сегмента сети в единый L2 сегмент с единой ip адресацией.

6.6.5 Настройка VPN сервиса для удаленных пользователей

Для настройки защищенного соединения между устройством МКСЗ «Горизонт-ВС VPN/FW» и удаленным клиентом необходимо настроить

устройство МКСЗ «Горизонт-ВС VPN/FW» в режиме сервера. Для настройки сервиса в режиме сервера необходимо в главном меню выбрать пункт **VPN – VPN туннели** и нажать на кнопку **Добавить туннель**. В таблице **Создание VPN туннеля** необходимо задать параметры VPN сервиса.

Параметры, которые необходимо задать для настройки VPN сервиса, представлены в таблице (см. таблицу 6).

Таблица 6 – Параметры настройки VPN сервиса

Название поля	Описание
Режим работы	В поле необходимо выбрать режим работы «Сервер» или режим работы Сервер для множества клиентов .
Описание	В поле необходимо задать название, которое может описывать объект, с которым связан данный сервис. Поле носит информационный характер.
Ключевая информация	В поле необходимо выбрать файл с ключевой информацией, который был загружен на устройство.
Название виртуального интерфейса	В поле необходимо задать название виртуального сетевого интерфейса, который появится в системе, после запуска сервиса.
MTU на виртуальном интерфейсе	В поле необходимо задать значение MTU на виртуальном сетевом интерфейсе.
Ip-адрес и маска подсети	В поле необходимо задать ip-адрес и маску подсети для виртуального сетевого интерфейса.
Сетевой порт для подключения	В поле необходимо задать сетевой порт для подключения других устройств МКСЗ «Горизонт-ВС VPN/FW» или Клиента Горизонт-ВС VPN.

После настройки сервиса в режиме сервера, необходимо настроить DHCP сервер, который будет выдавать сетевые настройки (ip-адрес, маску подсети и др.) удаленным пользователям. Для подключения удаленного пользователя необходимо задать ip-адрес удаленного сервера, сетевой порт для подключения и ключевую информацию.

6.7 Инструкция по настройке межсетевого экрана

6.7.1 Настройка правил фильтрации

Настройка межсетевого экранирования на уровне L3

Сетевые пакеты, которые проходят через устройство МКСЗ «Горизонт-ВС», обрабатываются межсетевым экраном. Правила фильтрации находятся в трех цепочках правил фильтрации: цепочка **«input»**, цепочка **forward** и цепочка **«output»**. В цепочку «input» попадают сетевые пакеты, в которых в поле ip-адрес пункта назначения указан ip-адрес одного из сетевых интерфейсов устройства МКСЗ «Горизонт-ВС». В цепочку **«output»** попадают сетевые пакеты, в которых в поле ip-адрес источника указан ip-адрес одного из сетевых интерфейсов устройства МКСЗ «Горизонт-ВС». В цепочку «forward» попадают сетевые пакеты, в которых в поле ip-адрес источника и ip-адрес назначения указаны ip-адреса, которые не принадлежат ни одному из сетевых интерфейсов устройства МКСЗ «Горизонт-ВС».

Для создания правила фильтрации необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила – таблицы/цепочки** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

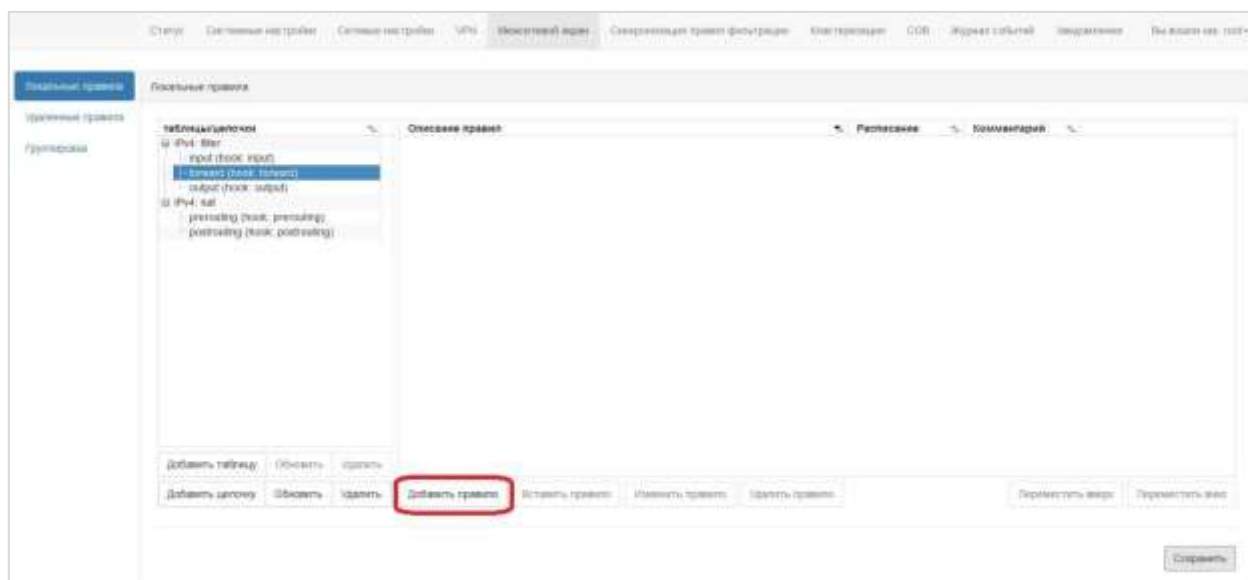


Рисунок 483 - Положение кнопки «Добавить правило»

В новом окне **Создание правила фильтрации** (Рисунок 484) необходимо задать параметры для фильтра и нажать на кнопку «ОК».

Рисунок 484 - Создание правила фильтрации

Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

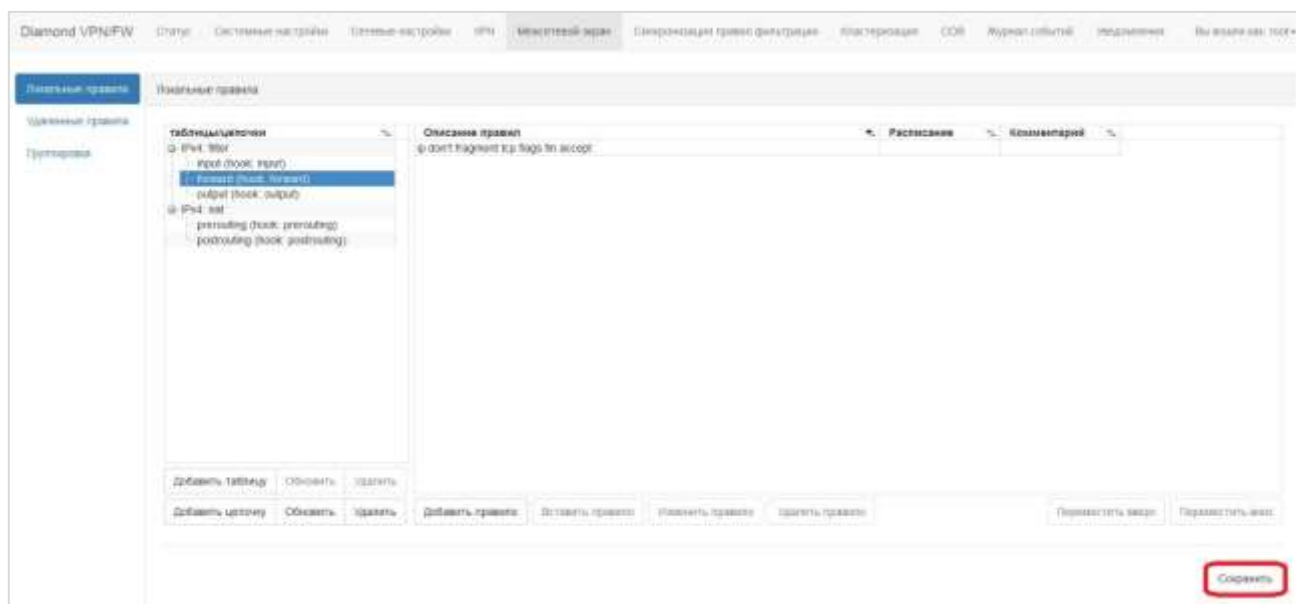


Рисунок 485 - Положение кнопки «Сохранить»

6.2 Настройка фильтрации по сетевому интерфейсу

Для создания правила фильтрации по сетевому интерфейсу необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило** (**Ошибка! Источник ссылки не найден.446**).

В новом окне **Создание правила фильтрации** необходимо выбрать пункт меню **Мета** (**Ошибка! Источник ссылки не найден.448**). В поле **Входящий интерфейс** или **Исходящий интерфейс** необходимо задать один из сетевых интерфейсов.

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Входящий интерфейс enp5s0s0

Исходящий интерфейс enp9s0s0

Общая длина пакета от 0 по 0

ОК Отмена

Рисунок 486 - Пункт меню «Мета»

В окне **Создание правила фильтрации** необходимо выбрать пункт меню **Действие** (Ошибка! Источник ссылки не найден.) и в поле **Действие** необходимо задать один из доступных вариантов действий. Для подтверждения выбора необходимо нажать на кнопку **ОК**.

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

☐ Счетчик пакетов

☐ Логирование правила фильтрации

Действие: Accept

Drop

Reject

SetMark

ОК Отмена

Рисунок 487 - Положение пункта меню «Действие»

Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить** (Ошибка! Источник ссылки не найден.448).

6.3 Настройка фильтрации по общей длине сетевого пакета

Для создания правила фильтрации по общей длине сетевого пакета необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку «Добавить правило» (**Ошибка! Источник ссылки не найден.**).

В новом окне **Создание правила фильтрации** необходимо выбрать пункт «Мета». В поле **Общая длина пакета** (Рисунок 488) необходимо задать общую длину пакета с учетом всех заголовков.

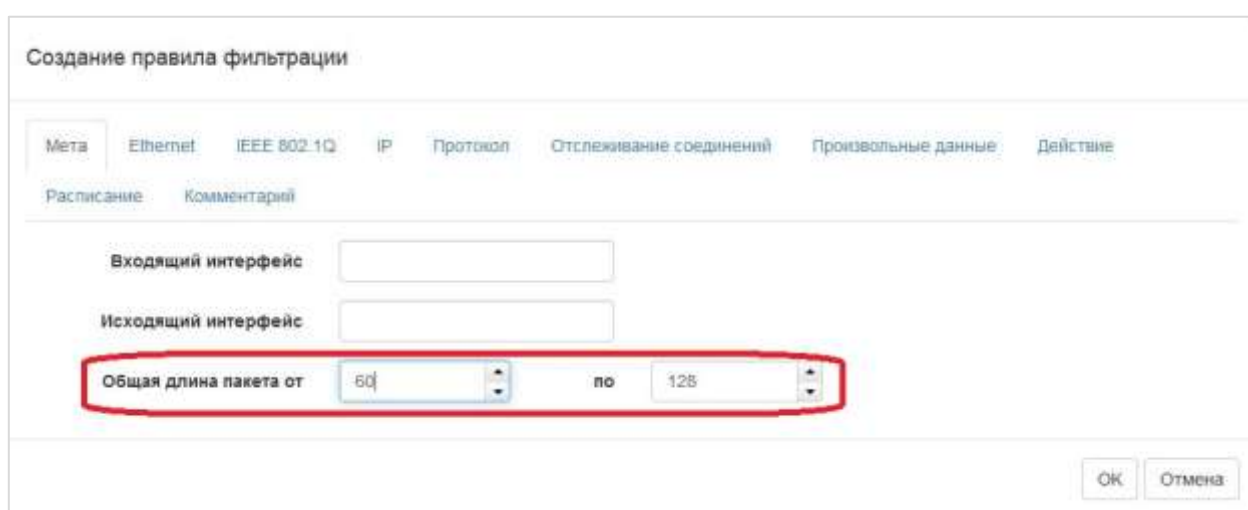
The image shows a web-based configuration window titled "Создание правила фильтрации". At the top, there are several tabs: "Мета", "Ethernet", "IEEE 802.1Q", "IP", "Протокол", "Отслеживание соединений", "Произвольные данные", and "Действие". The "Мета" tab is currently selected. Below the tabs, there are two input fields for "Входящий интерфейс" and "Исходящий интерфейс". Below these, there is a section for "Общая длина пакета" (Total packet length), which is highlighted with a red rectangle. This section contains two input fields: "от" (from) with the value "60" and "по" (to) with the value "128". At the bottom right of the window, there are two buttons: "ОК" and "Отмена".

Рисунок 488 - Положение поля «Общая длина пакета»

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** (**Ошибка! Источник ссылки не найден.**449) и в поле **Действие** необходимо задать один из доступных вариантов и нажать на кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

6.4 Настройка фильтрации по физическому адресу (MAC адрес)

Для создания правила фильтрации по физическому адресу (MAC адрес) необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

В новом окне «Создание правила фильтрации» необходимо выбрать пункт «Ethernet». В поле «Физический адрес источника» или «Физический адрес назначения» необходимо задать физический адрес устройства.

Создание правила фильтрации

Мета **Ethernet** IEEE 802.1Q IP Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Тип протокола [v]

Физический адрес источника 08:BC:17:AD:7E:A3

Физический адрес назначения xx:xx:xx:xx:xx:xx

ОК Отмена

Рисунок 489 - Положение пункта меню «Ethernet» и заполняемых полей

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** необходимо задать один из доступных вариантов и нажать на кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

6.5 Настройка фильтрации по типу протокола канального уровня

Для создания правила фильтрации по типу протокола канального уровня необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **«Добавить правило»**.

В новом окне «Создание правила фильтрации» необходимо выбрать пункт меню **Ethernet**. В поле «Тип протокола» необходимо выбрать тип протокола канального уровня.

Рисунок 490 - Пункт меню «Ethernet» и поле «Тип протокола»

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** необходимо задать один из доступных вариантов (Accept, Drop или Reject). Для подтверждения выбора необходимо нажать на кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

В поле **Тип протокола** можно выбрать наиболее распространенные протоколы: arp, rarp, ip, ipv6, vlan и lscr. Если нужного типа протокола нет в списке, то необходимо в поле «Тип протокола» выбрать пункт «other» и задать тип протокола в шестнадцатеричном формате. Перечень доступных протоколов представлен в таблице ниже .

Таблица 7 – Перечень доступных протоколов

Номер протокола	Название протокола
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x0842	Wake-on-LAN
0x22F3	IETF TRILL Protocol
0x22EA	Stream Reservation Protocol

Номер протокола	Название протокола
0x6003	DECnet Phase IV
0x8035	Reverse Address Resolution Protocol
0x809B	AppleTalk (Ethertalk)
0x80F3	AppleTalk Address Resolution Protocol (AARP)
0x8100	VLAN-tagged frame (IEEE 802.1Q) and Shortest Path Bridging IEEE 802.1aq with NNI compatibility
0x8137	IPX
0x8204	QNX Qnet
0x86DD	Internet Protocol Version 6 (IPv6)
0x8808	Ethernet flow control
0x8809	Ethernet Slow Protocols
0x8819	CobraNet
0x8847	MPLS unicast
0x8848	MPLS multicast
0x8863	PPPoE Discovery Stage
0x8864	PPPoE Session Stage
0x886D	Intel Advanced Networking Services
0x8870	Jumbo Frames (Obsoleted draft-ietf-isis-ext-eth-01)
0x887B	HomePlug 1.0 MME
0x888E	EAP over LAN (IEEE 802.1X)
0x8892	PROFINET Protocol
0x889A	HyperSCSI (SCSI over Ethernet)
0x88A2	ATA over Ethernet

Номер протокола	Название протокола
0x88A4	EtherCAT Protocol
0x88A8	Provider Bridging (IEEE 802.1ad) & Shortest Path Bridging IEEE 802.1aq
0x88AB	Ethernet Powerlink
0x88B8	GOOSE (Generic Object Oriented Substation event)
0x88B9	GSE (Generic Substation Events) Management Services
0x88BA	SV (Sampled Value Transmission)
0x88CC	Link Layer Discovery Protocol (LLDP)
0x88CD	SERCOS III
0x88DC	WSMP, WAVE Short Message Protocol
0x88E1	HomePlug AV MME
0x88E3	Media Redundancy Protocol (IEC62439-2)
0x88E5	MAC security (IEEE 802.1AE)
0x88E7	Provider Backbone Bridges (PBB) (IEEE 802.1ah)
0x88F7	Precision Time Protocol (PTP) over Ethernet (IEEE 1588)
0x88F8	NC-SI
0x88FB	Parallel Redundancy Protocol (PRP)
0x8902	IEEE 802.1ag Connectivity Fault Management (CFM) Protocol / ITU-T Recommendation Y.1731 (OAM)
0x8906	Fibre Channel over Ethernet (FCoE)
0x8914	FCoE Initialization Protocol
0x8915	RDMA over Converged Ethernet (RoCE)

Номер протокола	Название протокола
0x891D	TTEthernet Protocol Control Frame (TTE)
0x892F	High-availability Seamless Redundancy (HSR)
0x9000	Ethernet Configuration Testing Protocol
0x9100	VLAN-tagged (IEEE 802.1Q) frame with double tagging

6.6 Настройка фильтрации по полю CoS (Class of Service)

Для создания правила фильтрации по полю CoS (Class of Service) необходимо в главном меню выбрать пункт «Межсетевой экран – Локальные правила». В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

В новом окне **Создание правила фильтрации** необходимо выбрать пункт меню **Ethernet**. В поле «Тип протокола» необходимо выбрать тип протокола **vlan** (Ошибка! Источник ссылки не найден.).

Создание правила фильтрации

Мета **Ethernet** IEEE 802.1Q IP Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Тип протокола vlan

Физический адрес источника

Физический адрес назначения

OK Отмена

Рисунок 491 - Положение пункта меню «Ethernet» и поля «Тип протокола»

В окне **Создание правила фильтрации** необходимо выбрать пункт меню **IEEE 802.1Q** и в поле **Приоритет** необходимо выбрать одно из значений приоритета CoS (Class of Service).

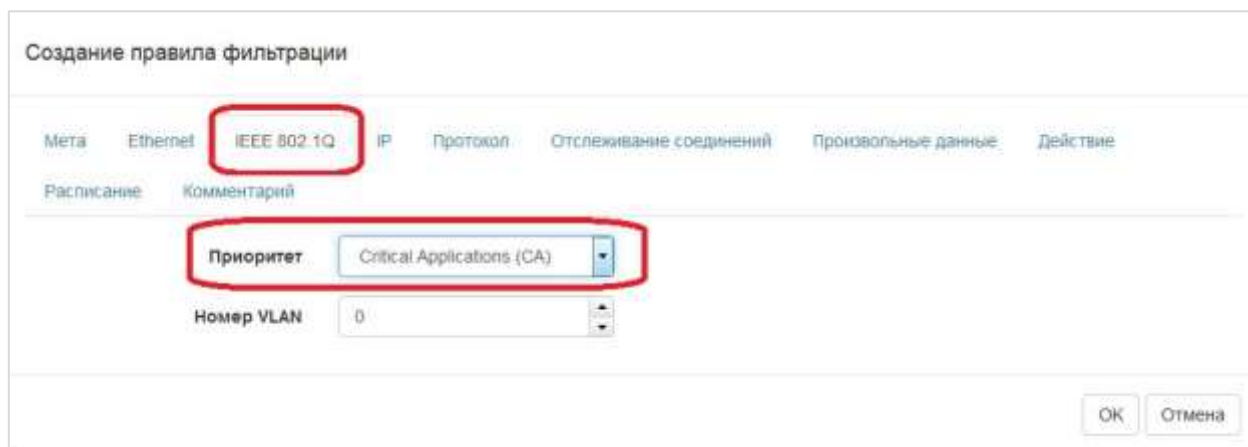


Рисунок 492 - Положение пункта меню «IEEE 802.1Q» и поля «Приоритет»

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать на кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

6.7 Настройка Фильтрации по метке VLAN ID

Для создания правила фильтрации по метке **VLAN ID** необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

В новом окне **Создание правила фильтрации** необходимо выбрать пункт **Ethernet**. В поле «Тип протокола» необходимо выбрать тип протокола **vlan**.

В окне **Создание правила фильтрации** необходимо выбрать пункт меню **IEEE 802.1Q** и в поле **Номер VLAN** необходимо задать номер VLAN ID.

Рисунок 493 - Пункт меню «IEEE 802.1Q» и поле «Номер VLAN»

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** необходимо задать один из доступных вариантов и нажать на кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

6.8 Настройка фильтрации по ip-адресу источника

Для создания правила фильтрации по ip-адресу источника необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку «Добавить правило».

В новом окне **Создание правила фильтрации** необходимо выбрать пункт **IP**. В поле **Адрес источника** необходимо задать ip-адрес источника. В поле **Маска подсети** необходимо задать маску подсети (Рисунок 494**Ошибка! Источник ссылки не найден.**).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q **IP** Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола ip4

Фильтрация по источнику Другое

Адрес источника 192.168.1.17 маска подсети 255.255.255.255

Доменное имя источника

Фильтрация по назначению Другое

Адрес назначения xxx.xxx.xxx.xxx маска подсети xxx.xxx.xxx.xxx

Доменное имя назначения

Метка DSCP N/A (0x00) Бит ECN Non-ECT (00)

Длина пакета от 0 по 0

Время жизни пакета (TTL) от 0 по 0

☐ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

ОК Отмена

Рисунок 494 - Пункт меню «IP» и заполняемые поля

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** (Рисунок 495) необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку **ОК**.

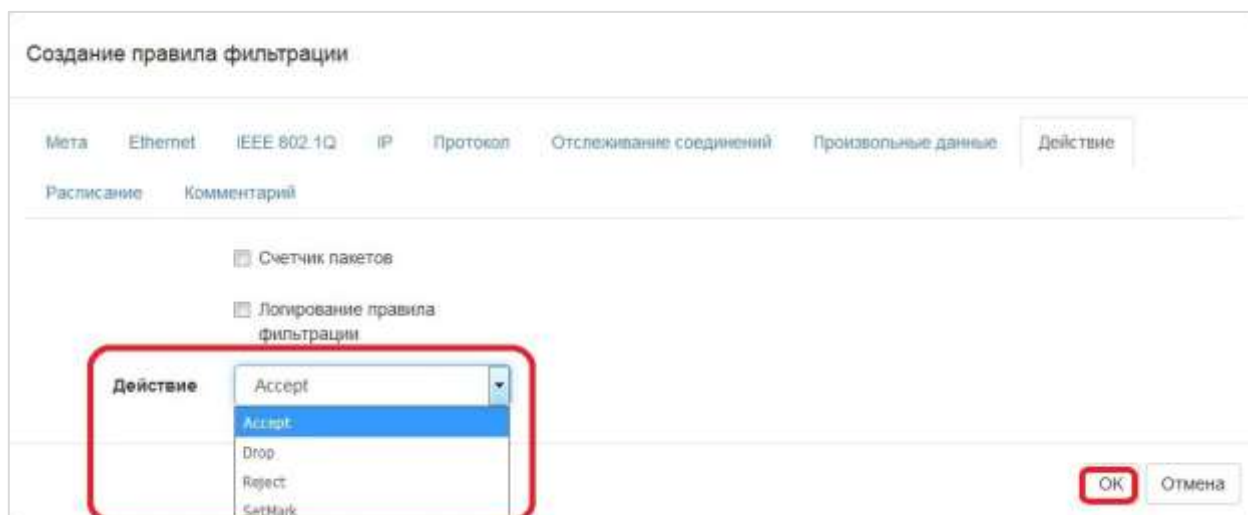


Рисунок 495 - Выбор действия

Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить** (Ошибка! Источник ссылки не найден.Рисунок 496).

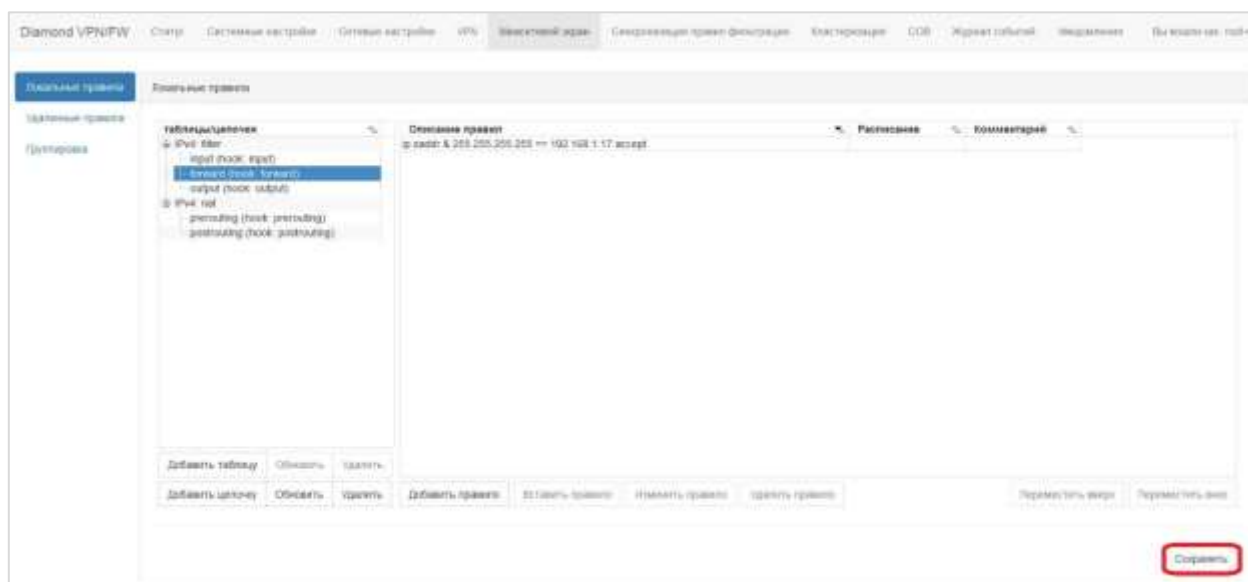


Рисунок 496 - Положение кнопки «Сохранить» для сохранения созданного правила

6.9 Настройка фильтрации по IP-адресу назначения

Для создания правила фильтрации по IP-адресу назначения необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В

таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

В новом окне «Создание правила фильтрации» необходимо выбрать пункт «IP». В поле «Адрес назначения» необходимо задать IP-адрес назначения. В поле «Маска подсети» необходимо задать маску подсети Рисунок 497.

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q **IP** Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола ip4

Фильтрация по источнику Другое

Адрес источника xxx.xxx.xxx.xxx маска подсети xxx.xxx.xxx.xxx

Доменное имя источника

Фильтрация по назначению Другое

Адрес назначения 10.18.192.0 маска подсети 255.255.255.0

Доменное имя назначения

Метка DSCP N/A (0x00) Бит ECN Non-ECT (00)

Длина пакета от 0 по 0

Время жизни пакета (TTL) от 0 по 0

☐ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

OK Отмена

Рисунок 497 - Пункт меню «IP» и заполняемые поля для правила фильтрации по адресу назначения

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** необходимо задать один из доступных вариантов.

Для подтверждения выбора необходимо нажать кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

6.10 Настройка фильтрации по метке DSCP

Для создания правила фильтрации по метке DSCP необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило** (Ошибка! Источник ссылки не найден.445).

В новом окне **Создание правила фильтрации** необходимо выбрать пункт меню **IP**. В поле **Метка DSCP** необходимо выбрать одно из значения метки (Рисунок 498).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q **IP** Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола ip4

Фильтрация по источнику Другое

Адрес источника xxx.xxx.xxx.xxx маска подсети xxx.xxx.xxx.xxx

Доменное имя источника

Фильтрация по назначению Другое

Адрес назначения xxx.xxx.xxx.xxx маска подсети xxx.xxx.xxx.xxx

Доменное имя назначения

Метка DSCP AF41 (0x22) Бит ECN Non-ECT (00)

Длина пакета от 0 по 0

Время жизни пакета (TTL) от 0 по 0

☐ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

ОК Отмена

Рисунок 498 - Пункт меню «IP» и положение поля «Метка DSCP»

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

6.11 Настройка фильтрации по биту ECN

Для создания правила фильтрации по биту ECN необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

В новом окне **Создание правила фильтрации** необходимо выбрать пункт **IP**. В поле **Бит ECN** необходимо выбрать одно из значения бита ECN (Рисунок 499).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q **IP** Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола ip4

Фильтрация по источнику Другое

Адрес источника xxx.xxx.xxx.xxx маска подсети xxx.xxx.xxx.xxx

Доменное имя источника

Фильтрация по назначению Другое

Адрес назначения xxx.xxx.xxx.xxx маска подсети xxx.xxx.xxx.xxx

Доменное имя назначения

Метка DSCP N/A (0x00) **Бит ECN ECT(1) (01)**

Длина пакета от 0 по 0

Время жизни пакета (TTL) от 0 по 0

☐ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

OK Отмена

Рисунок 499 - Пункт меню «IP» и положение поля «Бит ECN»

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

6.12 Настройка фильтрации по полю длина пакета (Packet Length)

Для создания правила фильтрации по полю длина пакета (Packet Length) необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

В новом окне **Создание правила фильтрации** необходимо выбрать пункт **IP**. В поле **Длина пакета** необходимо задать длину сетевого пакета без учета заголовка второго уровня .

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q **IP** Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола ip4

Фильтрация по источнику Другое

Адрес источника xxx.xxx.xxx.xxx маска подсети xxx.xxx.xxx.xxx

Доменное имя источника

Фильтрация по назначению Другое

Адрес назначения xxx.xxx.xxx.xxx маска подсети xxx.xxx.xxx.xxx

Доменное имя назначения

Метка DSCP N/A (0x00) Бит ECN Non-ECT (00)

Длина пакета от 120 по 1000

Время жизни пакета (TTL) от 0 по 0

☐ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

OK Отмена

Рисунок 500 - Положение пункта меню «IP» и положение поля

«Длина пакетов от № по №»

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие (Ошибка! Источник ссылки не найден.)** необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить (Ошибка! Источник ссылки не найден.)**.

6.13 Настройка фильтрации по полю время жизни пакета (TTL)

Для создания правила фильтрации по полю время жизни пакета (TTL) необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку «Добавить правило» (**Ошибка! Источник ссылки не найден.**).

В новом окне **Создание правила фильтрации** необходимо выбрать пункт **IP**. В поле **Время жизни пакета (TTL)** необходимо задать время жизни пакета (Рисунок 501).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q **IP** Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола ip4

Фильтрация по источнику Другое

Адрес источника 100.100.100.100 маска подсети 100.100.100.100

Доменное имя источника

Фильтрация по назначению Другое

Адрес назначения 100.100.100.100 маска подсети 100.100.100.100

Доменное имя назначения

Метка DSCP N/A (0x00) Бит ECN Non-ECT (00)

Длина пакета от 0 по 0

Время жизни пакета (TTL) от 50 по 100

☐ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

OK Отмена

Рисунок 501 - Пункт меню «IP» и положение поля
«Время

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** (Ошибка! Источник ссылки не найден.449) необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить** (Ошибка! Источник ссылки не найден.447).

6.14 Настройка фильтрации по биту фрагментации

Для создания правила фильтрации по биту фрагментации необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В

таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

В новом окне **Создание правила фильтрации** необходимо выбрать пункт **IP**. В поле **Установки бита фрагментации** необходимо задать флаг фрагментация запрещена или фрагментация разрешена (Рисунок 502).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q **IP** Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола ip4

Фильтрация по источнику Другое

Адрес источника 100.100.100.100 маска подсети 100.100.100.100

Доменное имя источника

Фильтрация по назначению Другое

Адрес назначения 100.100.100.100 маска подсети 100.100.100.100

Доменное имя назначения

Метка DSCP N/A (0x00) Бит ECN Non-ECT (00)

Длина пакета от 0 по 0

Время жизни пакета (TTL) от 0 по 0

☒ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

OK Отмена

Рисунок 502 – Пункт меню «IP» и положение полей «Установлен бит Фрагментация запрещена», «Установлен бит Фрагментация разрешена»

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

6.15 Настройка фильтрации по протоколу TCP

Для создания правила фильтрации по протоколу TCP необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

В новом окне «**Создание правила фильтрации**» необходимо выбрать пункт меню **Протокол**. В поле **Протокол** необходимо выбрать транспортный протокол TCP. В поле **Порт источника** необходимо задать диапазон сетевых портов источника. В поле **Порт назначения** необходимо задать диапазон сетевых портов назначения. В поле **Флаги** необходимо задать флаг протокола TCP (Рисунок 503).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP **Протокол** Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Протокол TCP (6)

Параметры TCP

Порт источника с 17 по 100

Порт назначения с 0 по 0

Флаги ☒ fin ☐ syn ☐ rst ☐ psh ☐ ack ☐ urg ☐ ecn ☐ cwr

ОК Отмена

Рисунок 503 - Пункт меню «Протокол» и заполняемые поля

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

6.16 Настройка фильтрации по протоколу UDP

Для создания правила фильтрации по протоколу UDP необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

В новом окне **Создание правила фильтрации** необходимо выбрать пункт **Протокол**. В поле **Протокол** необходимо выбрать транспортный протокол UDP. В поле **Порт источника** необходимо задать диапазон сетевых портов источника. В поле **Порт назначения** необходимо задать диапазон сетевых портов назначения (Рисунок 504).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP **Протокол** Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Протокол UDP (17)

Параметры UDP:

Порт источника с 18 по 23

Порт назначения с 74 по 105

OK Отмена

Рисунок 504 - Пункт меню «Протокол» и поля для ввода параметров

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

6.17 Настройка фильтрации по протоколу ICMP

Для создания правила фильтрации по протоколу ICMP необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В

таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

В новом окне **Создание правила фильтрации** необходимо выбрать пункт **Протокол**. В поле **Протокол** необходимо выбрать протокол ICMP. В поле **ICMP тип** необходимо выбрать тип сообщения. В поле **ICMP код** необходимо задать код сообщения ().

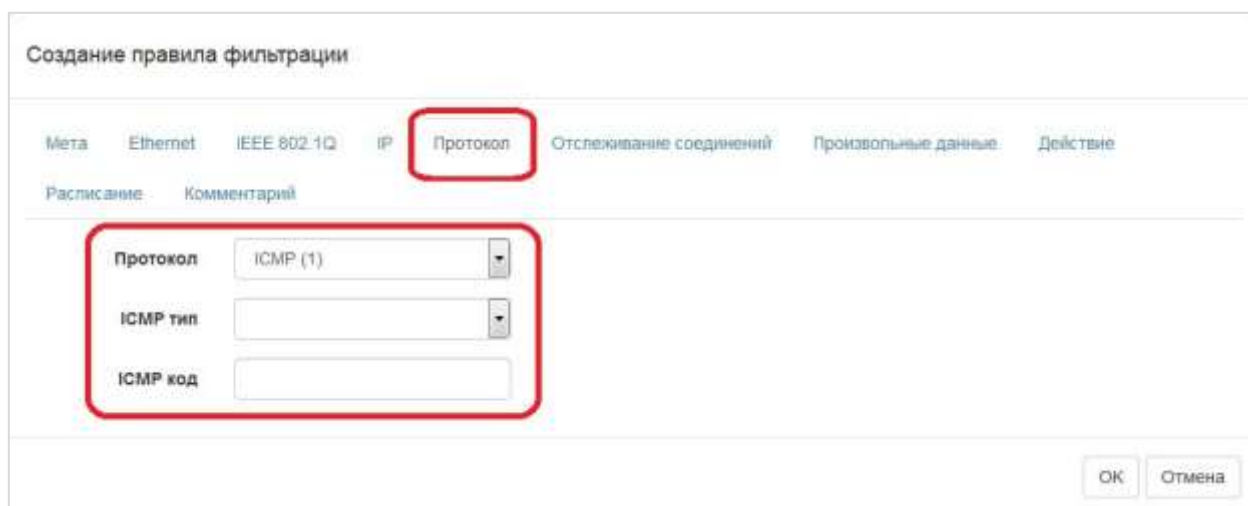


Рисунок 505 - Пункт меню «Протокол» и заполняемые поля

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку **ОК**. Для сохранения правила фильтрации необходимо нажать на кнопку **Сохранить**.

6.18 Настройка фильтрации протоколов, инкапсулируемых в IP

Для создания правила фильтрации по протоколу, инкапсулируемому в IP, необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

В новом окне **Создание правила фильтрации** необходимо выбрать пункт **Протокол**. В поле **Протокол** необходимо выбрать **Другой протокол**. В поле **ID протокола** задать ID номер протокола, инкапсулируемого в IP.

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP **Протокол** Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Протокол Другой протокол ID протокола

ОК Отмена

Рисунок 506 – Пункт меню «Протокол» и заполняемые поля

В окне **Создание правила фильтрации** необходимо выбрать пункт **Действие** и в поле **Действие** необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку «**ОК**». Для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**».

6.19 Настройка фильтрации по типу соединения

Для создания правила фильтрации по типу соединения, необходимо в главном меню выбрать пункт **Межсетевой экран – Локальные правила**. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **Добавить правило**.

В новом окне **Создание правила фильтрации** необходимо выбрать пункт **Отслеживание соединений** и установить флаг с типом соединения: новое соединение, установленное соединение или связанное соединение.

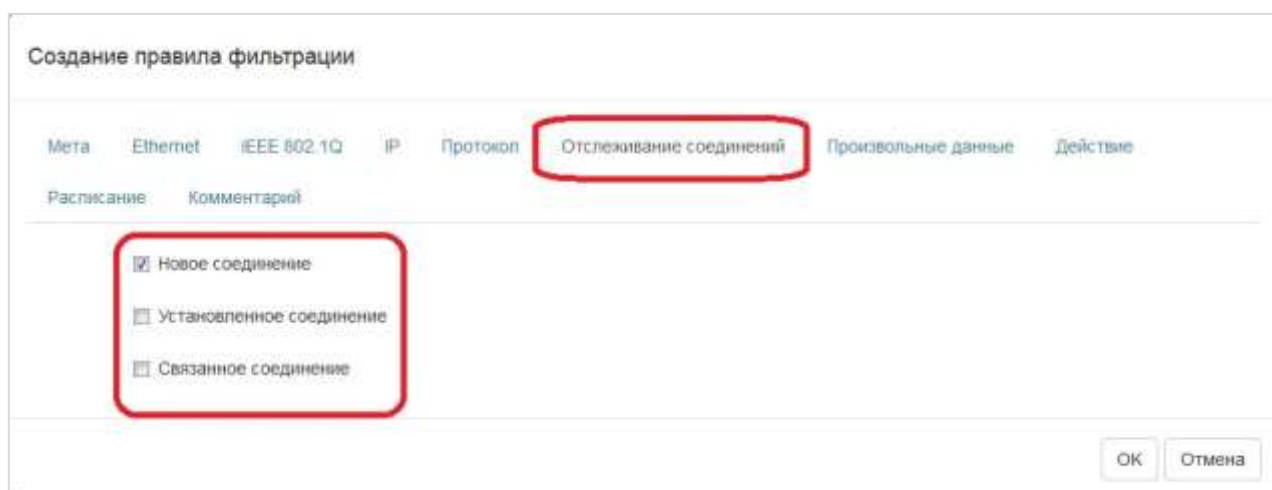


Рисунок 507 - Пункт меню «Отслеживание соединений» и положение полей «Новое соединение», «Установленное соединение» и «Связанное соединение».

В окне **«Создание правила фильтрации»** необходимо выбрать пункт **«Действие»** и в поле **«Действие»** (Ошибка! Источник ссылки не найден.) необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку **«ОК»**. Для сохранения правила фильтрации необходимо нажать на кнопку **«Сохранить»** (Ошибка! Источник ссылки не найден.).

6.20 Настройка фильтрации произвольных данных

Для создания правила фильтрации по произвольным данным, необходимо в главном меню выбрать пункт **«Межсетевой экран – Локальные правила»**. В таблице **«Локальные правила»** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **«Добавить правило»** (Ошибка! Источник ссылки не найден.).

В новом окне **«Создание правила фильтрации»** необходимо выбрать пункт **«Произвольные данные»**. В поле **«Номер байта»** необходимо задать адрес начала поиска в байтах. В поле **«Маска подсети»** необходимо задать маску для поиска произвольных данных. В поле **«Операция»** необходимо выбрать одну из доступных операций. В поле **«Результат»** необходимо задать результат операции.

Рисунок 508 – Пункт меню «Произвольные данные» и заполняемые поля

В окне «**Создание правила фильтрации**» необходимо выбрать пункт «**Действие**» и в поле «**Действие**» (449Ошибка! Источник ссылки не найден.) необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку «**ОК**». Для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**»

6.7.2 Настройка межсетевого экранирования на уровне L2

Сетевые пакеты, которые проходят через устройство МКС3 «Горизонт-ВС», обрабатываются межсетевым экраном. Правила фильтрации находятся в трех цепочках правил фильтрации: цепочка «input», цепочка «forward» и цепочка «output». В цепочку «input» попадают сетевые пакеты, в которых в поле ip-адрес пункта назначения указан ip-адрес одного из сетевых интерфейсов устройства МКС3 Горизонт-ВС. В цепочку «output» попадают сетевые пакеты, в которых в поле ip-адрес источника указан ip-адрес одного из сетевых интерфейсов

устройства МКСЗ «Горизонт-ВС». В цепочку «forward» попадают сетевые пакеты, в которых в поле ip-адрес источника и ip-адрес назначения указаны ip-адреса, которые не принадлежат ни одному из сетевых интерфейсов устройства МКСЗ «Горизонт-ВС».

Для создания правил фильтрации на втором уровне стандартной сетевой модели, необходимо на устройстве МКСЗ «Горизонт-ВС» перевести один или несколько сетевых интерфейсов в режим работы на втором уровне. В главном меню необходимо выбрать пункт **«Межсетевой экран – Локальные правила»**. В таблице **«Локальные правила – таблицы/цепочки»** необходимо нажать на кнопку **«Добавить таблицу»** (Ошибка! Источник ссылки не найден.Рисунок 509).

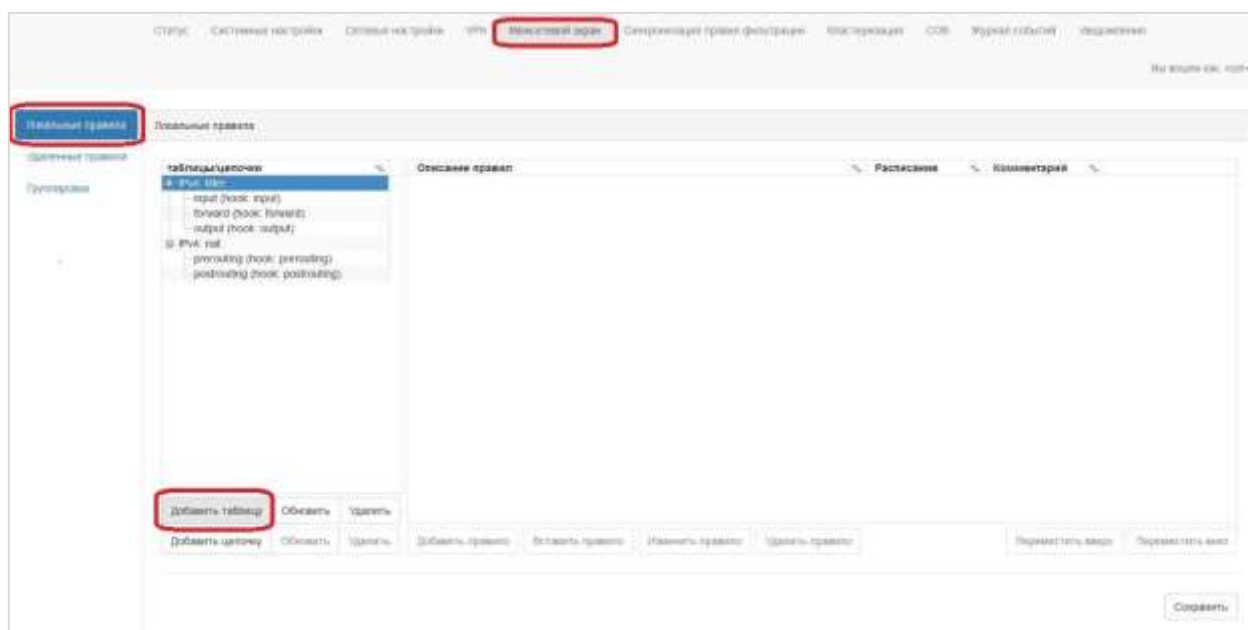
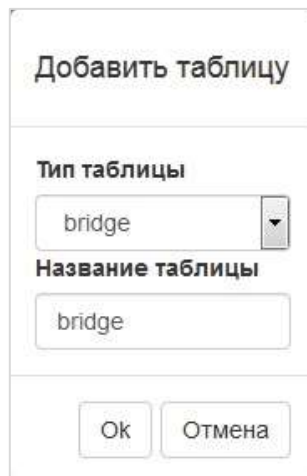


Рисунок 509 - Добавление таблицы локальных правил

В новом окне **«Добавить таблицу»** в поле **«Тип таблицы»** необходимо выбрать значение «bridge». В поле **«Название таблицы»** необходимо задать название таблицы и нажать на кнопку «ОК» (Рисунок 510Ошибка! Источник ссылки не найден.).



Добавить таблицу

Тип таблицы

bridge

Название таблицы

bridge

Ok Отмена

Рисунок 510 - Настройка названия и типа таблицы локальных правил

В новой таблице с типом «**Bridge**» необходимо создать цепочки для правил фильтрации. Для создания цепочки правил фильтрации необходимо выбрать таблицу с типом «**Bridge**» и нажать на кнопку «**Добавить цепочку**». В новом окне «**Добавить цепочку**» в поле «**Тип цепочки правил**» необходимо выбрать тип цепочки. В режиме фильтрации на втором уровне стандартной сетевой модели можно создать цепочку с типом «input» – для входящего трафика, с типом «**forward**» – для транзитного трафика и с типом «**output**» – для исходящего трафика. В поле «Название цепочки правил» необходимо задать название цепочки. Поле «**Приоритет**» и поле «**Политика**» необходимо оставить без изменения. После введения всех данных необходимо нажать на кнопку «ОК» (Рисунок 511 **Ошибка! Источник ссылки не найден.**).

Добавить цепочку

Тип цепочки правил

input

Название цепочки правил

input

Приоритет

0

Политика

Принять

Ok

Отмена

Рисунок 511 - Настройка параметров таблицы локальных правил

Для сохранения настроек необходимо нажать на кнопку **«Сохранить»** (Ошибка! Источник ссылки не найден.).

Аналогичным образом можно создать цепочку правил для исходящего трафика **«output»** и транзитного трафика **«forward»** (Рисунок 512Ошибка! Источник ссылки не найден.).

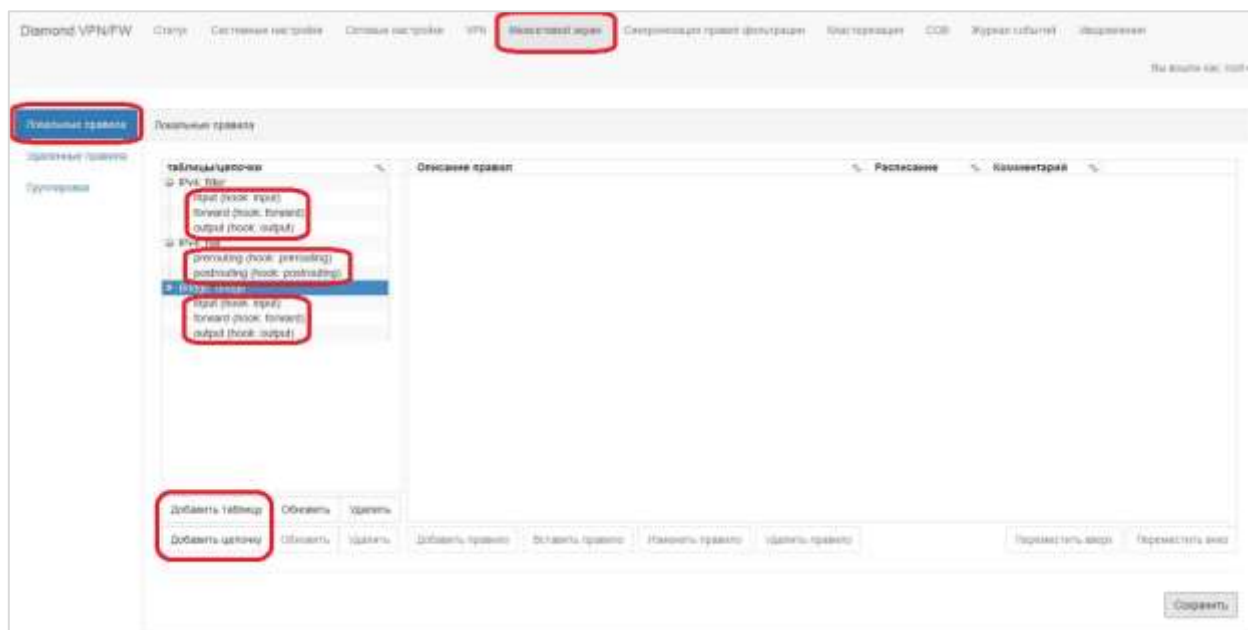


Рисунок 512 - Настраиваемые таблицы и цепочки правил

Для создания правила фильтрации на втором уровне стандартной сетевой модели необходимо в главном меню выбрать пункт **«Межсетевой экран – Локальные правила»**. В таблице **«Локальные правила – таблицы/цепочки»** необходимо выбрать цепочку правил фильтрации с типом **«Bridge»** и нажать на кнопку **«Добавить правило»** (Рисунок 513 **Ошибка! Источник ссылки не найден.**).

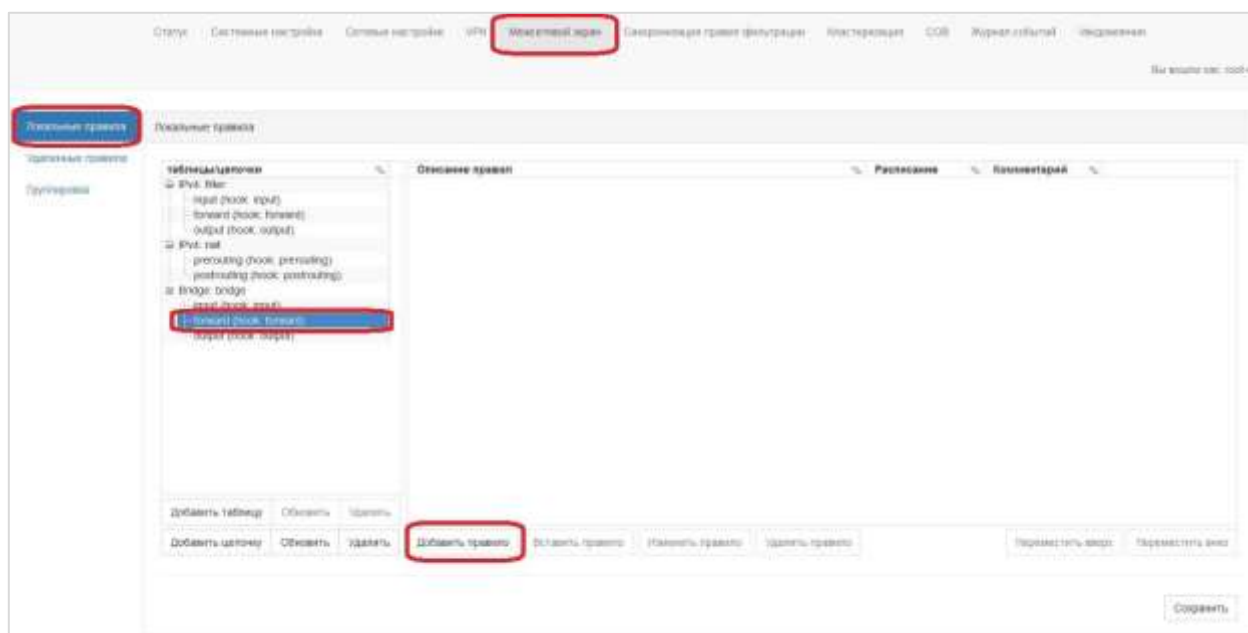


Рисунок 513 - Создание правила фильтрации с типом «Bridge»

В новом окне **«Создание правила фильтрации»** необходимо задать параметры для фильтра и нажать на кнопку **«ОК»** (Рисунок 514 **Ошибка! Источник ссылки не найден.**).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Входящий интерфейс

Исходящий интерфейс

Общая длина пакета от по

OK Отмена

Рисунок 514 - Окно «Создание правила фильтрации» и пункт меню «Мета»

Для сохранения правила фильтрации необходимо нажать на кнопку «Сохранить».

7.10 Настройка фильтрации по сетевому интерфейсу

Для создания правила фильтрации по сетевому интерфейсу необходимо в главном меню выбрать пункт «Межсетевой экран – Локальные правила». В таблице «Локальные правила» необходимо выбрать цепочку правил фильтрации с типом «Bridge» и нажать на кнопку «Добавить правило» (Рисунок 515).

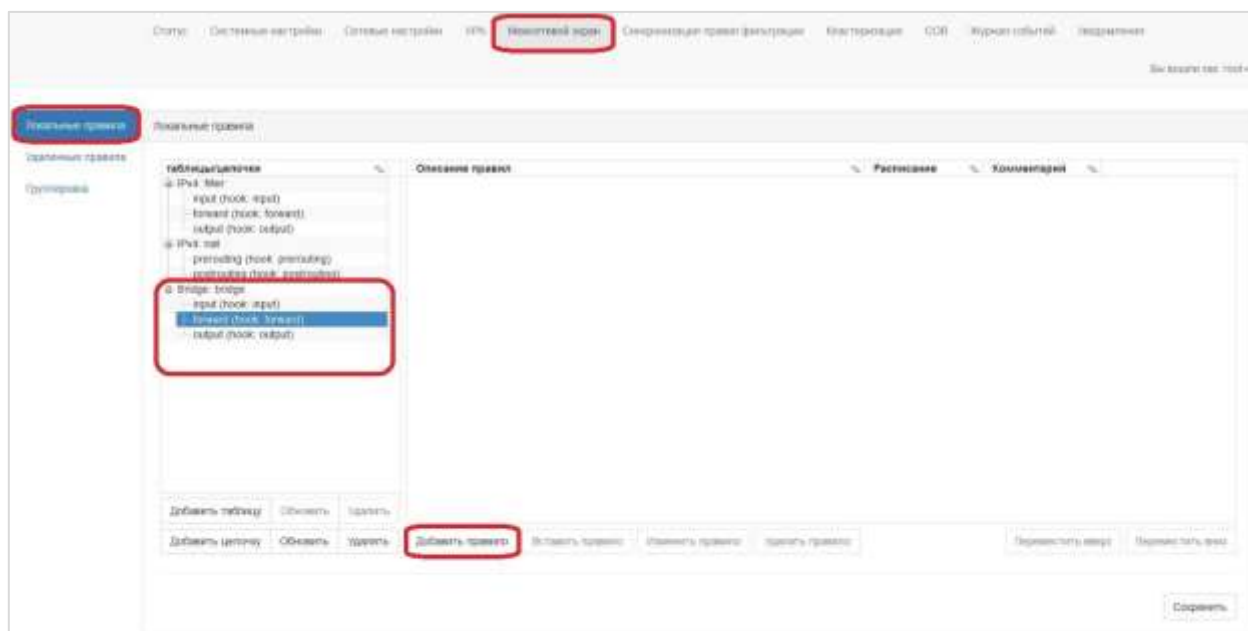


Рисунок 515 - Добавление правила фильтрации с типом «Bridge»

В новом окне «**Создание правила фильтрации**» необходимо выбрать пункт «**Мета**». В поле «**Входящий интерфейс**» или «**Исходящий интерфейс**» необходимо задать один из сетевых интерфейсов (Рисунок 516 **Ошибка! Источник ссылки не найден.**).

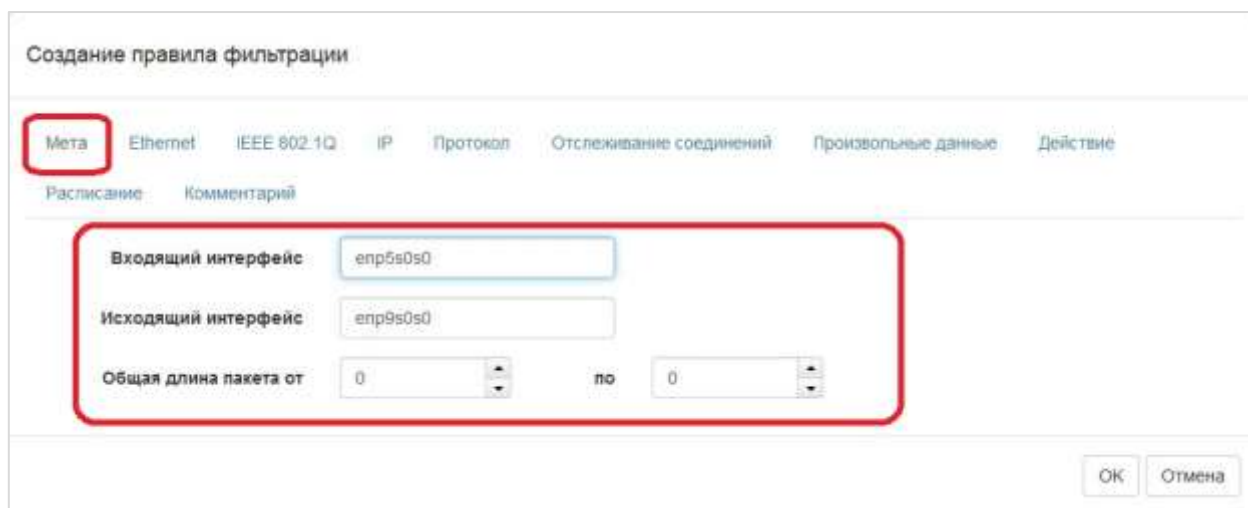


Рисунок 516 - Задание сетевых интерфейсов

В окне «**Создание правила фильтрации**» необходимо выбрать пункт «**Действие**» и в поле «**Действие**» (**Ошибка! Источник ссылки не найден.**)

необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку «ОК». Для сохранения правила фильтрации необходимо нажать на кнопку «Сохранить» (Ошибка! Источник ссылки не найден.).

7.11 Настройка фильтрации по общей длине сетевого пакета

Для создания правила фильтрации по общей длине сетевого пакета необходимо в главном меню выбрать пункт «Межсетевой экран – Локальные правила». В таблице «Локальные правила» необходимо выбрать цепочку правил фильтрации с типом «Bridge» и нажать на кнопку «Добавить правило» (475Ошибка! Источник ссылки не найден.).

В новом окне «Создание правила фильтрации» необходимо выбрать пункт «Мета». В поле «Общая длина пакета» необходимо задать общую длину пакета с учетом всех заголовков (Рисунок 517Ошибка! Источник ссылки не найден.).

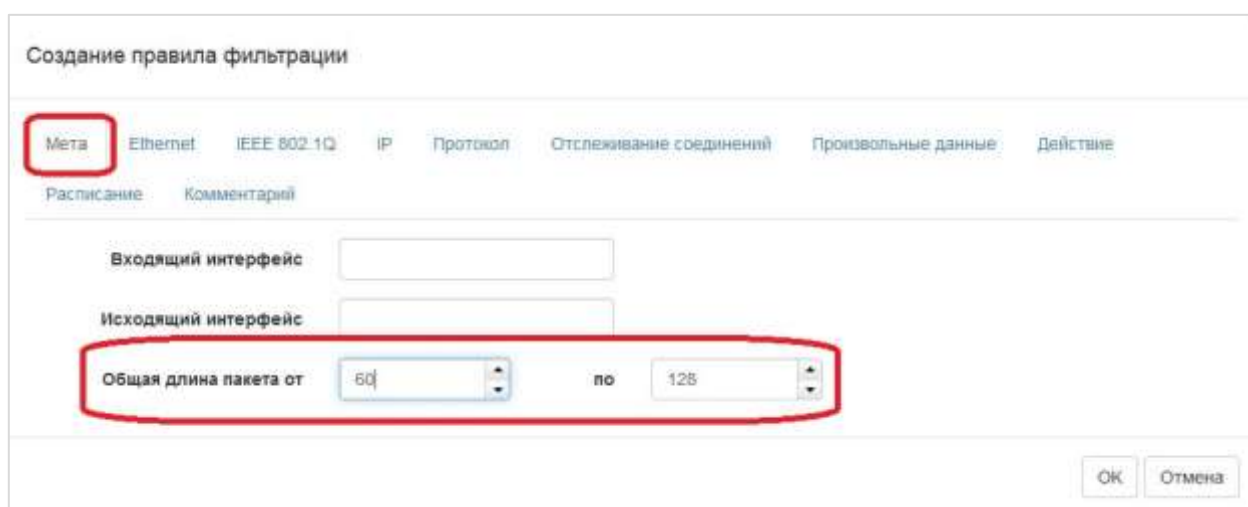


Рисунок 517 - Задание общей длины пакета от № по №

В окне «Создание правила фильтрации» необходимо выбрать пункт «Действие» и в поле «Действие» (449Ошибка! Источник ссылки не найден.) необходимо задать один из доступных вариантов. Для подтверждения выбора

необходимо нажать кнопку «**ОК**». Для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**».

7.12 Настройка фильтрации по физическому адресу (MAC адрес)

Для создания правила фильтрации по физическому адресу (MAC адрес) необходимо в главном меню выбрать пункт «**Межсетевой экран – Локальные правила**». В таблице «Локальные правила» необходимо выбрать цепочку правил фильтрации с типом «Bridge» и нажать на кнопку «**Добавить правило**».

В новом окне «**Создание правила фильтрации**» необходимо выбрать пункт меню «**Ethernet**». В поле «**Физический адрес источника**» или «**Физический адрес назначения**» необходимо задать физический адрес устройства (Рисунок 518 **Ошибка! Источник ссылки не найден.**).

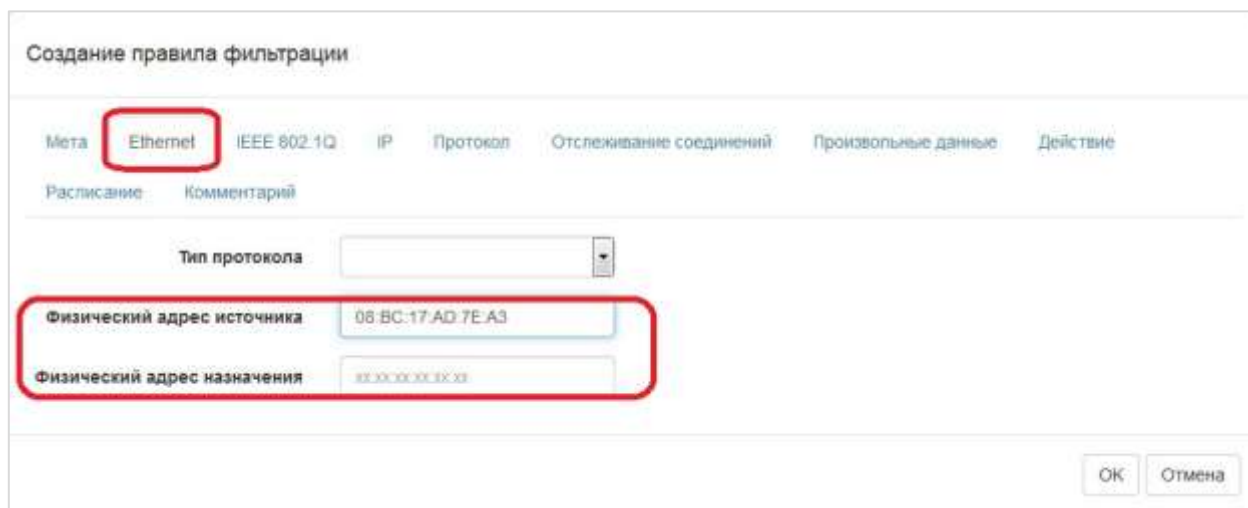


Рисунок 518 - Пункт меню «Ethernet» и поля «Физический адрес источника», «Физический адрес назначения»

В окне «**Создание правила фильтрации**» необходимо выбрать пункт «**Действие**» и в поле «**Действие**» (**Ошибка! Источник ссылки не найден.**) необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку «**ОК**». Для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**» (**Ошибка! Источник ссылки не найден.**).

7.13 Настройка фильтрации по типу протокола канального уровня

Для создания правила фильтрации по типу протокола канального уровня необходимо в главном меню выбрать пункт **«Межсетевой экран – Локальные правила»**. В таблице **«Локальные правила»** необходимо выбрать цепочку правил фильтрации с типом «Bridge» и нажать на кнопку **«Добавить правило»**.

В новом окне «Создание правила фильтрации» необходимо выбрать пункт «Ethernet». В поле «Тип протокола» необходимо выбрать тип протокола канального уровня (Рисунок 519).

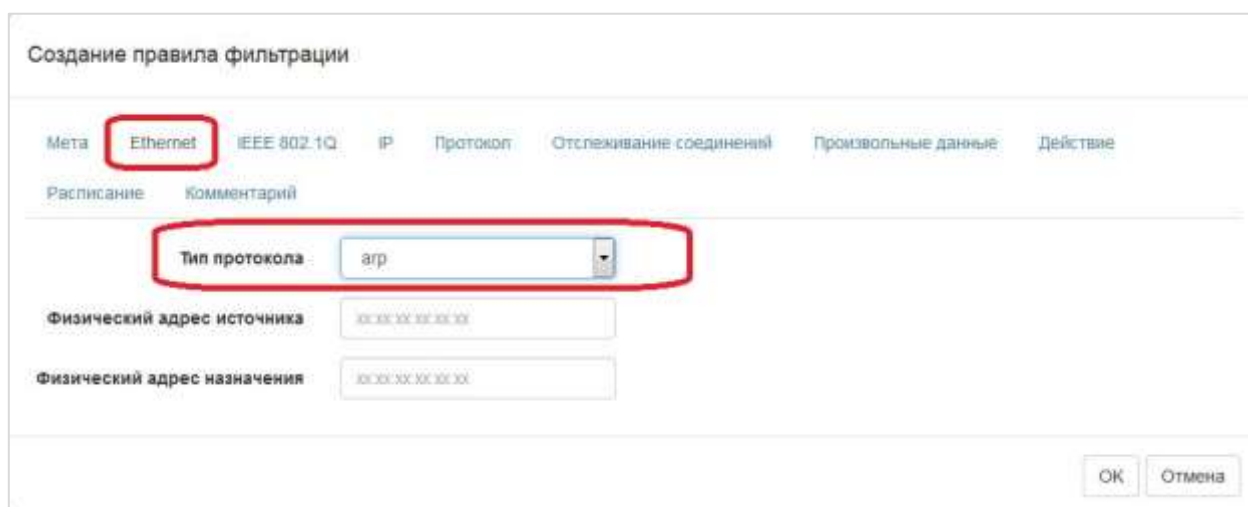


Рисунок 519 - Положение пункта меню «Ethernet» и положение поля «Тип протокола»

В окне **«Создание правила фильтрации»** необходимо выбрать пункт **«Действие»** и в поле **«Действие»** (**Ошибка! Источник ссылки не найден.**) необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку **«ОК»**. Для сохранения правила фильтрации необходимо нажать на кнопку **«Сохранить»** (**Ошибка! Источник ссылки не найден.**).

В поле **«Тип протокола»** можно выбрать наиболее распространенные протоколы, например, arp, rarp, ip, ipv6, vlan и l2cp. Если нужного типа протокола

нет в списке, то необходимо в поле «**Тип протокола**» выбрать пункт «**other**» и задать тип протокола в шестнадцатеричном формате. Перечень доступных протоколов представлен в таблице 7.

7.14 Настройка фильтрации по полю CoS (Class of Service)

Для создания правила фильтрации по полю CoS (Class of Service) необходимо в главном меню выбрать пункт «**Межсетевой экран – Локальные правила**». В таблице «**Локальные правила**» необходимо выбрать цепочку правил фильтрации с типом «**Bridge**» и нажать на кнопку «**Добавить правило**» (475Ошибка! Источник ссылки не найден.).

В новом окне «**Создание правила фильтрации**» необходимо выбрать пункт меню «**Ethernet**». В поле «**Тип протокола**» необходимо выбрать тип протокола «**vlan**» (Рисунок 520Ошибка! Источник ссылки не найден.).

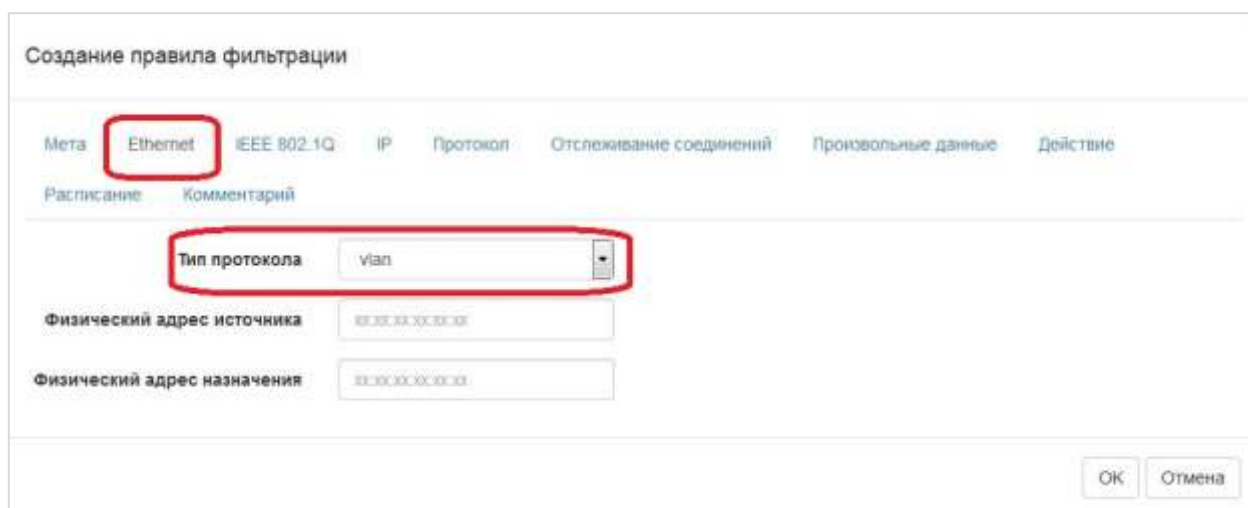


Рисунок 520 - Пункт меню «Ethernet» и поле «Тип протокола» vlan

В окне «**Создание правила фильтрации**» необходимо выбрать пункт меню «**IEEE 802.1Q**» и в поле «**Приоритет**» необходимо выбрать одно из значений приоритета CoS (Class of Service) (Рисунок 521Ошибка! Источник ссылки не найден.).

Создание правила фильтрации

Мета Ethernet **IEEE 802.1Q** IP Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Приоритет Critical Applications (CA)

Номер VLAN 0

ОК Отмена

Рисунок 521 - Пункт меню «IEEE 802.1Q» и поле «Приоритет»

В окне «**Создание правила фильтрации**» необходимо выбрать пункт «**Действие**» и в поле «**Действие**» (449Ошибка! Источник ссылки не найден.) необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку «**ОК**». Для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**» (447Ошибка! Источник ссылки не найден.).

7.15 Настройка фильтрации по метке VLAN ID

Для создания правила фильтрации по метке VLAN ID необходимо в главном меню выбрать пункт «**Межсетевой экран – Локальные правила**». В таблице «**Локальные правила**» необходимо выбрать цепочку правил фильтрации с типом «Bridge» и нажать на кнопку «**Добавить правило**» (Ошибка! Источник ссылки не найден.475).

В новом окне «**Создание правила фильтрации**» необходимо выбрать пункт «**Ethernet**». В поле «Тип протокола» необходимо выбрать тип протокола «**vlan**».

В окне «Создание правила фильтрации» необходимо выбрать пункт «**IEEE 802.1Q**» и в поле «**Номер VLAN**» необходимо задать номер VLAN ID (Рисунок 522).

Создание правила фильтрации

Мета Ethernet **IEEE 802.1Q** IP Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Приоритет

Номер VLAN

ОК Отмена

Рисунок 522 - Пункт меню «IEEE 802.1Q» и поле «Номер VLAN»

В окне «**Создание правила фильтрации**» необходимо выбрать пункт «**Действие**» и в поле «**Действие**» (449Ошибка! Источник ссылки не найден.) необходимо задать один из доступных вариантов. Для подтверждения выбора необходимо нажать кнопку «**ОК**». Для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**»

7.16 Фильтрация по IP-адресу источника

Для создания правила фильтрации по ip-адресу источника необходимо в главном меню выбрать пункт «**Межсетевой экран – Локальные правила**». В таблице «**Локальные правила**» необходимо выбрать цепочку правил фильтрации с типом «**Bridge**» и нажать на кнопку «**Добавить правило**» (Рисунок 523).

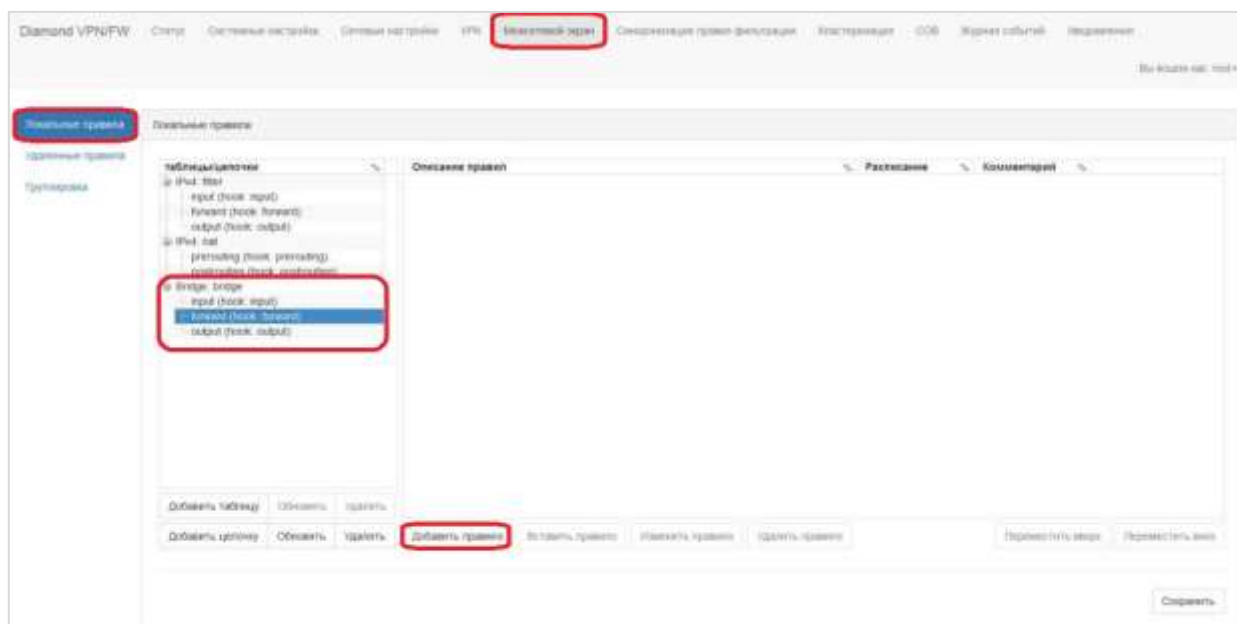


Рисунок 523 - Добавление правила фильтрации с типом «Bridge»

В новом окне «**Создание правила фильтрации**» необходимо выбрать пункт «**IP**». В поле «**Адрес источника**» необходимо задать IP-адрес источника. В поле «**Маска подсети**» необходимо задать маску подсети (Рисунок 524).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q **IP** Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола ip4

Фильтрация по источнику Другое

Адрес источника 192.168.1.17 маска подсети 255.255.255.255

Доменное имя источника

Фильтрация по назначению Другое

Адрес назначения xxx.xxx.xxx.xxx **маска подсети** xxx.xxx.xxx.xxx

Доменное имя назначения

Метка DSCP N/A (0x00) Бит ECN Non-ECT (00)

Длина пакета от 0 по 0

Время жизни пакета (TTL) от 0 по 0

☐ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

ОК Отмена

Рисунок 524 - Пункт «IP», и положение поля «Адрес назначения»,
«маска подсети»

В окне «Создание правила фильтрации» необходимо выбрать пункт «Действие» в поле «Действие» необходимо задать один из доступных вариантов и нажать на кнопку «ОК».

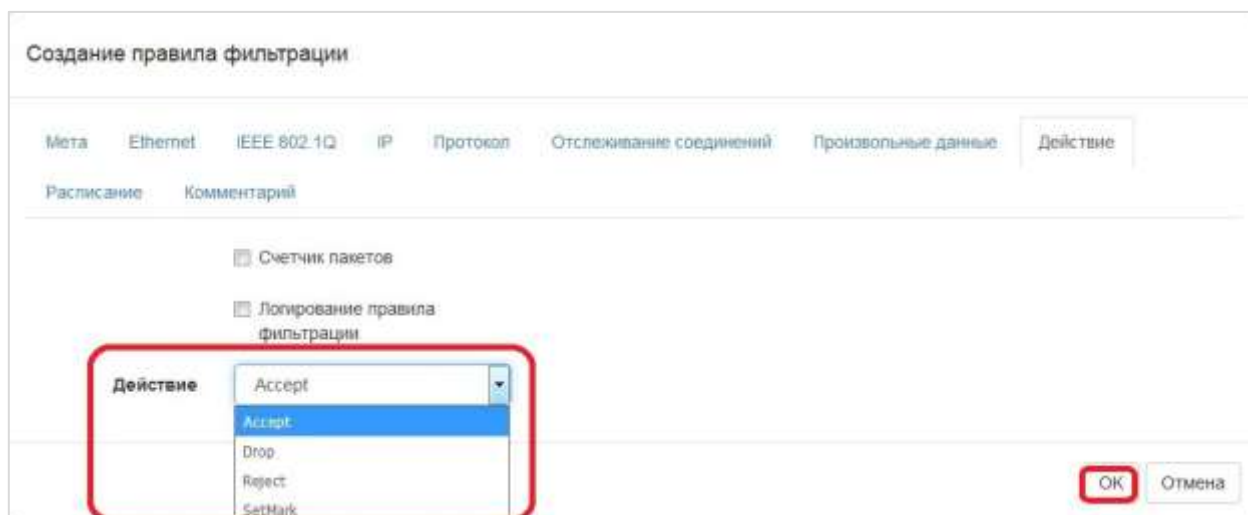


Рисунок 525 - Пункт меню «Создание правила фильтрации» и поле «Действие»

Для сохранения правила фильтрации необходимо нажать на кнопку «Сохранить».

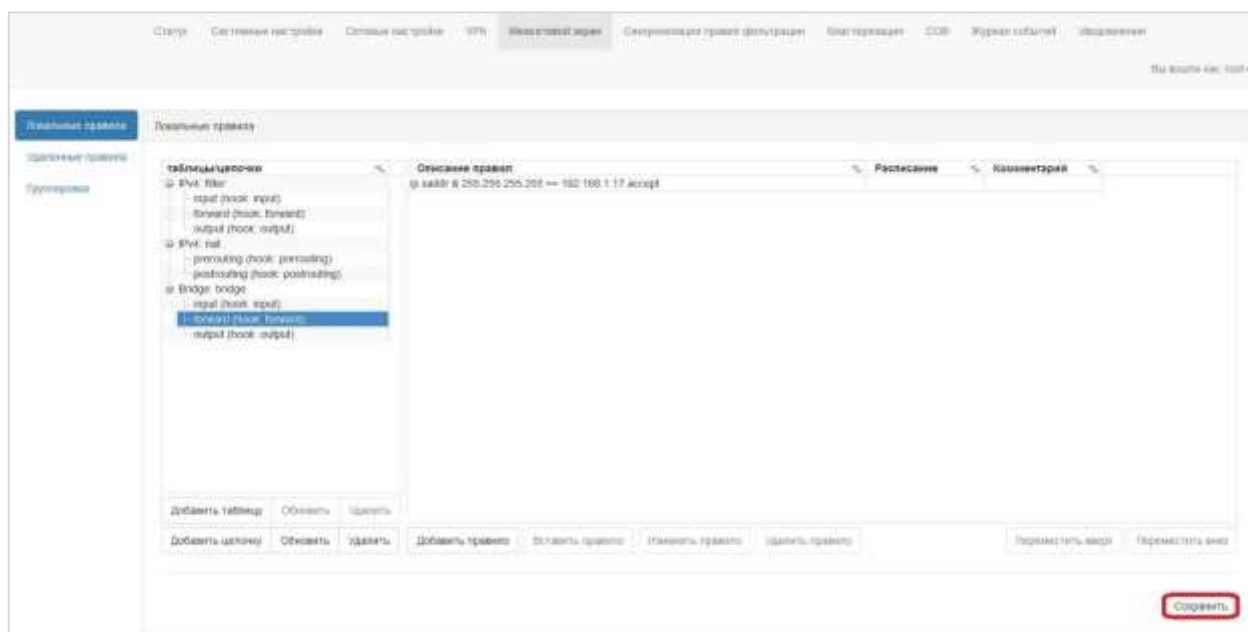


Рисунок 526 - Положения кнопки «Сохранить»

7.17 Фильтрация по ip-адресу назначения

Для создания правила фильтрации по ip-адресу назначения необходимо в главном меню выбрать пункт «Межсетевой экран – Локальные правила». В таблице «**Локальные правила**» необходимо выбрать цепочку правил

фильтрации с типом «**Bridge**» и нажать на кнопку «**Добавить правило**»
Рисунок 527.

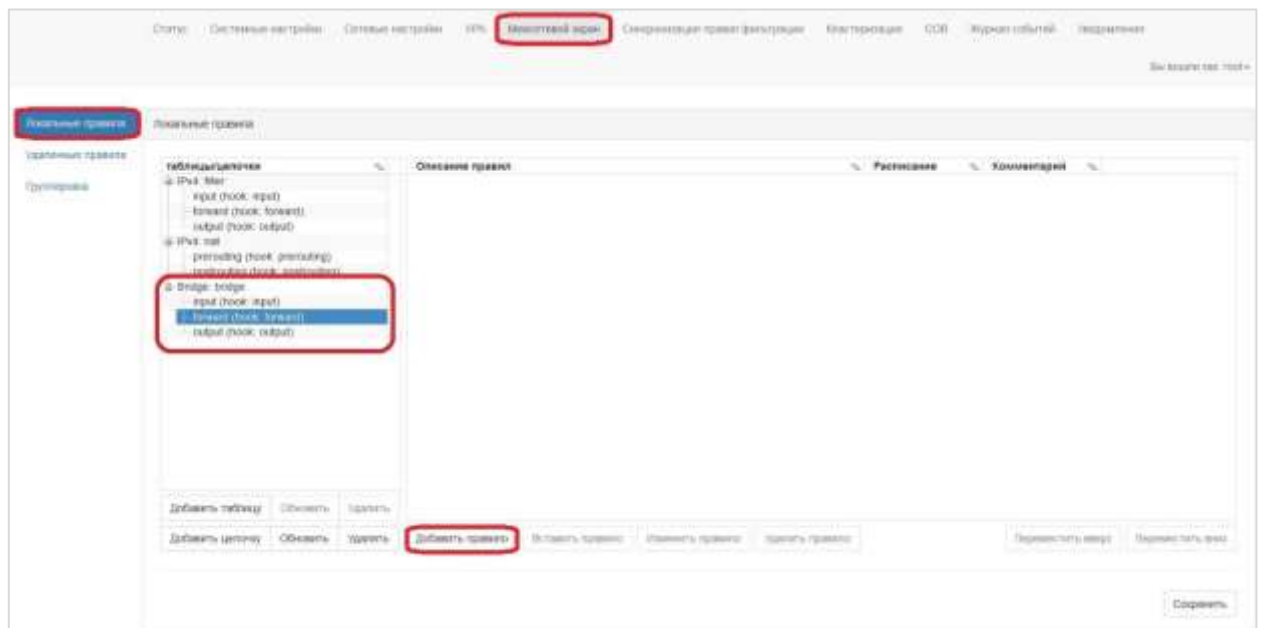


Рисунок 527 - Добавление правила фильтрации с типом «Bridge»

В новом окне «**Создание правила фильтрации**» необходимо выбрать пункт «**IP**» (**Ошибка! Источник ссылки не найден.**Рисунок 529). В поле «**Адрес назначения**» необходимо задать IP-адрес назначения. В поле «**Маска подсети**» необходимо задать маску подсети.

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q **IP** Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола ip4

Фильтрация по источнику Другое

Адрес источника маска подсети

Доменное имя источника

Фильтрация по назначению Другое

Адрес назначения 10.18.192.0 маска подсети 255.255.255.0

Доменное имя назначения

Метка DSCP N/A (0x00) Бит ECN Non-ECT (00)

Длина пакета от 0 по 0

Время жизни пакета (TTL) от 0 по 0

☐ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

ОК Отмена

Рисунок 528 - Пункт меню «IP» и положение поля «Адреса назначения», «маска подсети»

В окне «Создание правила фильтрации» необходимо выбрать пункт «Действие» и в поле «Действие» необходимо задать один из доступных вариантов и нажать на кнопку «ОК» (Рисунок 528Ошибка! Источник ссылки не найден.).

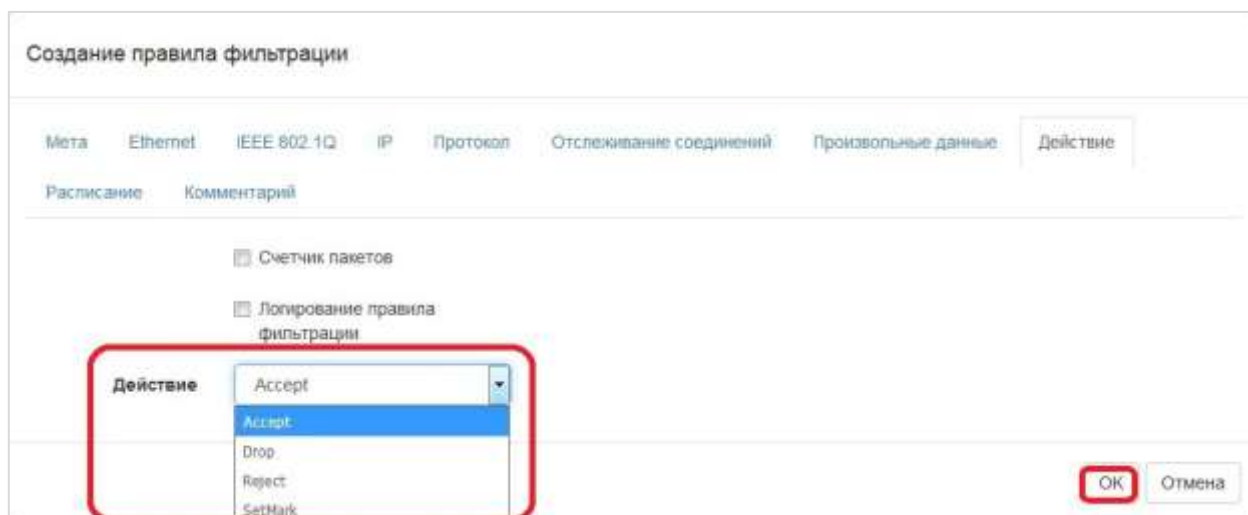


Рисунок 529 - Пункт «Действие», создание правила фильтрации

Для сохранения правила фильтрации необходимо нажать на кнопку «Сохранить».

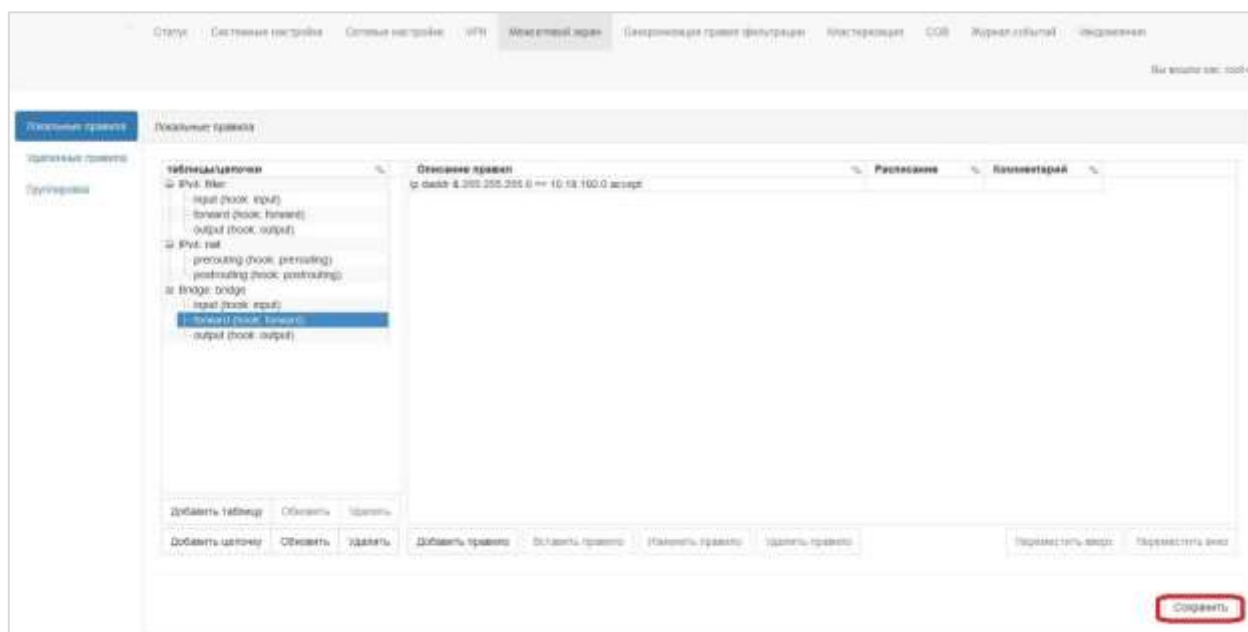


Рисунок 530 - Положения кнопки «Сохранить»

7.18 Фильтрация по метке DSCP

Для создания правила фильтрации по метке DSCP необходимо в главном меню выбрать пункт «**Межсетевой экран – Локальные правила**». В таблице «**Локальные правила**» необходимо выбрать цепочку правил фильтрации с

типом «**Bridge**» и нажать на кнопку «**Добавить правило**» (Ошибка! Источник ссылки не найден.).

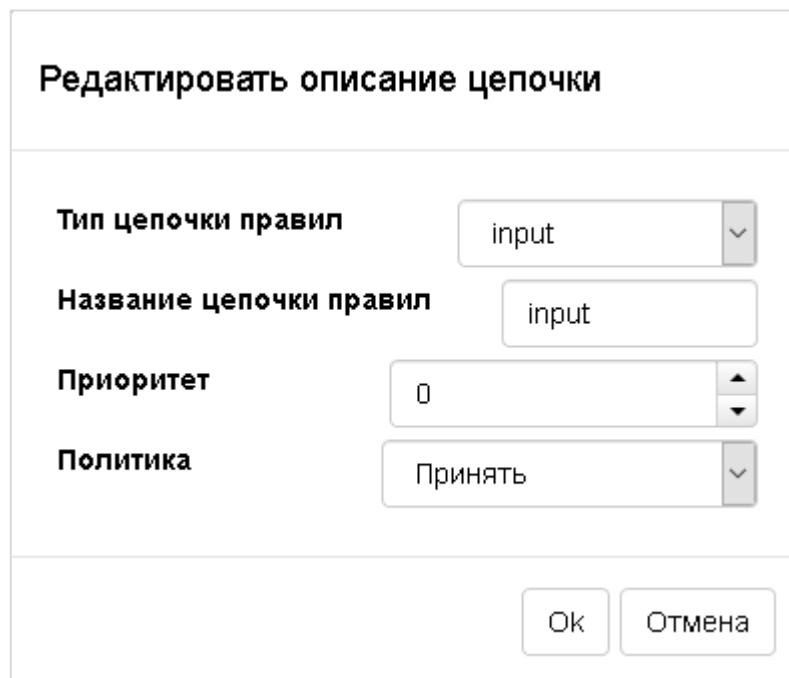


Рисунок 531

После задания политики по умолчанию необходимо нажать на кнопку «**ОК**». Для сохранения настроек необходимо нажать на кнопку «**Сохранить**».

7.19 Настройка межсетевого экранирования по расписанию

При настройке правил фильтрации на устройстве МКС3 Горизонт-ВС можно установить время действия правила фильтрации. Для задания расписания действия для правила фильтрации необходимо в главном меню выбрать пункт «**Межсетевой экран – Локальные правила**». В таблице «**Локальные правила**» необходимо выбрать цепочку правил фильтрации и нажать на кнопку «**Добавить правило**» (Рисунок 532)Ошибка! Источник ссылки не найден..

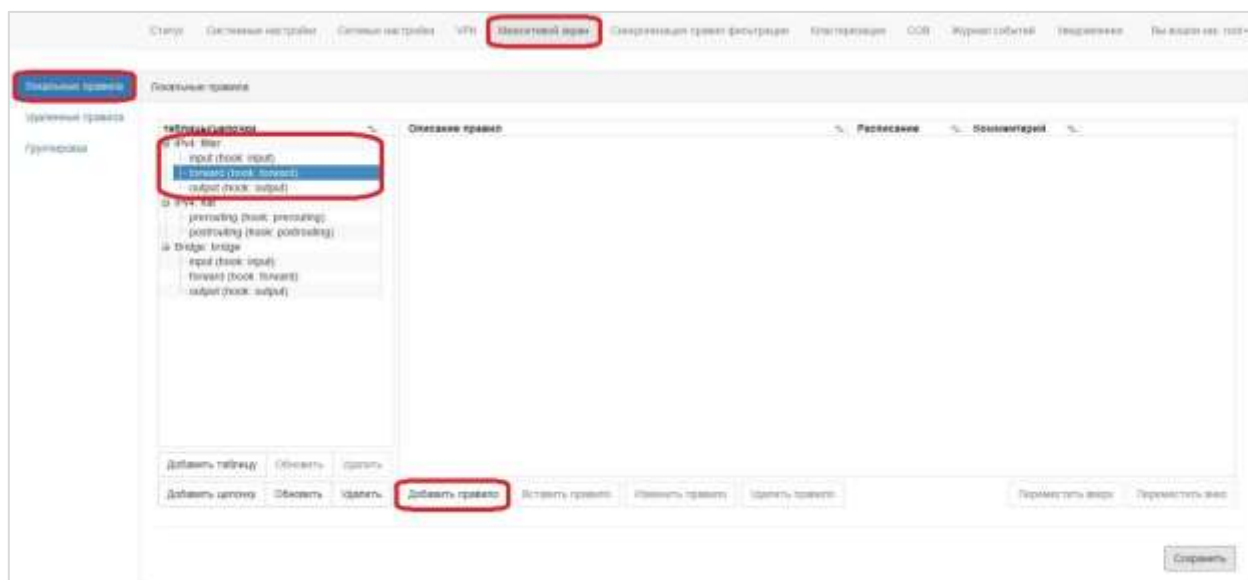


Рисунок 532 - Добавление правил фильтрации по расписанию

В новом окне «**Создание правила фильтрации**» необходимо выбрать пункт «**Расписание**». Для добавления нового расписания для правила фильтрации необходимо нажать на кнопку «**Добавить расписание**». Для изменения текущего расписания для правила фильтрации необходимо нажать на кнопку «**Обновить расписание**». Для удаления текущего расписания для правила фильтрации необходимо нажать на кнопку «**Удалить расписание**». При создании расписания для правила фильтрации доступны следующие поля: «**Временная зона**», «**Минуты**», «**Часы**», «**День**», «**Месяц**», «**Год**», флаг «**Дни недели**», флаг «**Диапазон**» (Рисунок 533 **Ошибка! Источник ссылки не найден.**).

Рисунок 533 - Пункт «Расписание» и поле установки времени

После установки точного времени необходимо нажать на кнопку «ОК»

(Рисунок 534Ошибка! Источник ссылки не найден.).

Рисунок 534 - Положение кнопки «ОК»

Для выхода в меню «**Локальные правила**» необходимо нажать на кнопку «ОК». Для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**» (Рисунок 535).

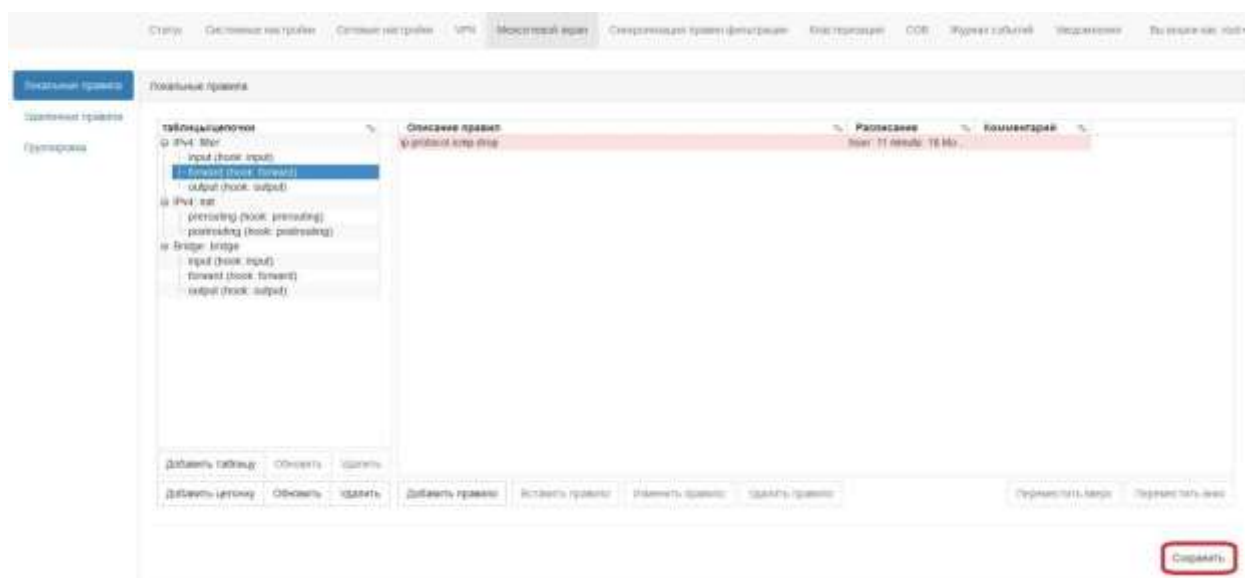


Рисунок 535 - Положение кнопки «Сохранить»

Неактивное правило фильтрации отмечено красным цветом. Если правило фильтрации неактивно, то оно не осуществляет фильтрацию сетевого трафика. Активное правило фильтрации отмечено белым цветом. Активное правило фильтрации осуществляет фильтрацию сетевого трафика (Рисунок 536).

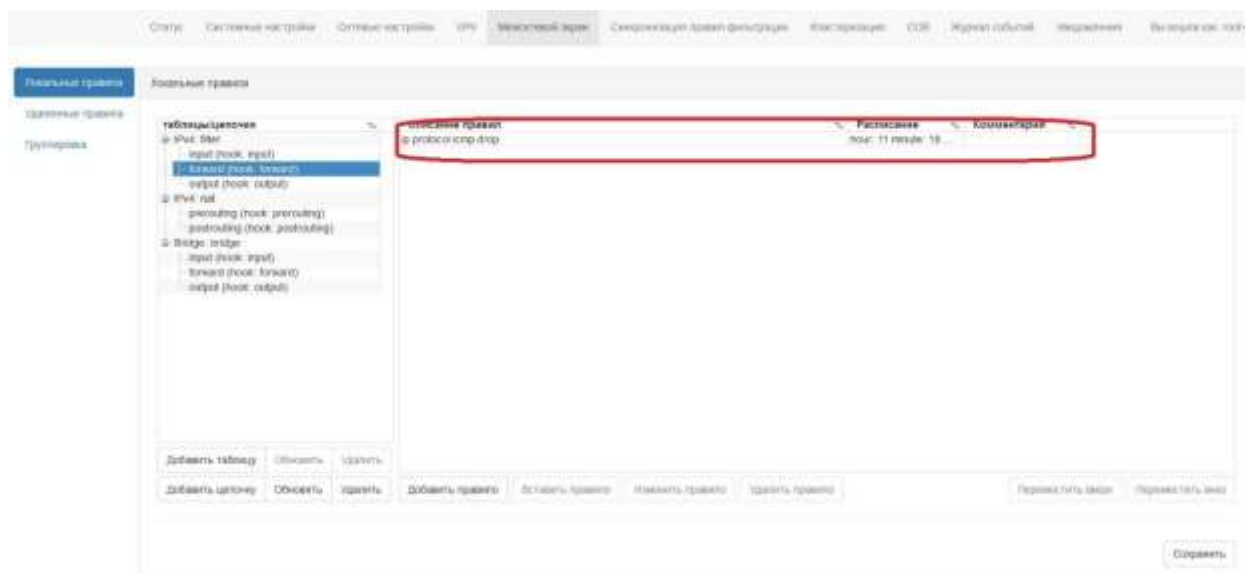


Рисунок 536 - Цвет активного правила фильтрации

При активации по времени, правило фильтрации появляется на позиции, на которой оно находится в общей таблице фильтрации.

7.20 Настройка межсетевого экранирования по доменному имени

Для создания правила фильтрации по доменному имени, необходимо в главном меню выбрать пункт «Межсетевой экран – Локальные правила». В таблице «Локальные правила» необходимо выбрать цепочку правил фильтрации и нажать на кнопку «Добавить правило» (Рисунок 537).

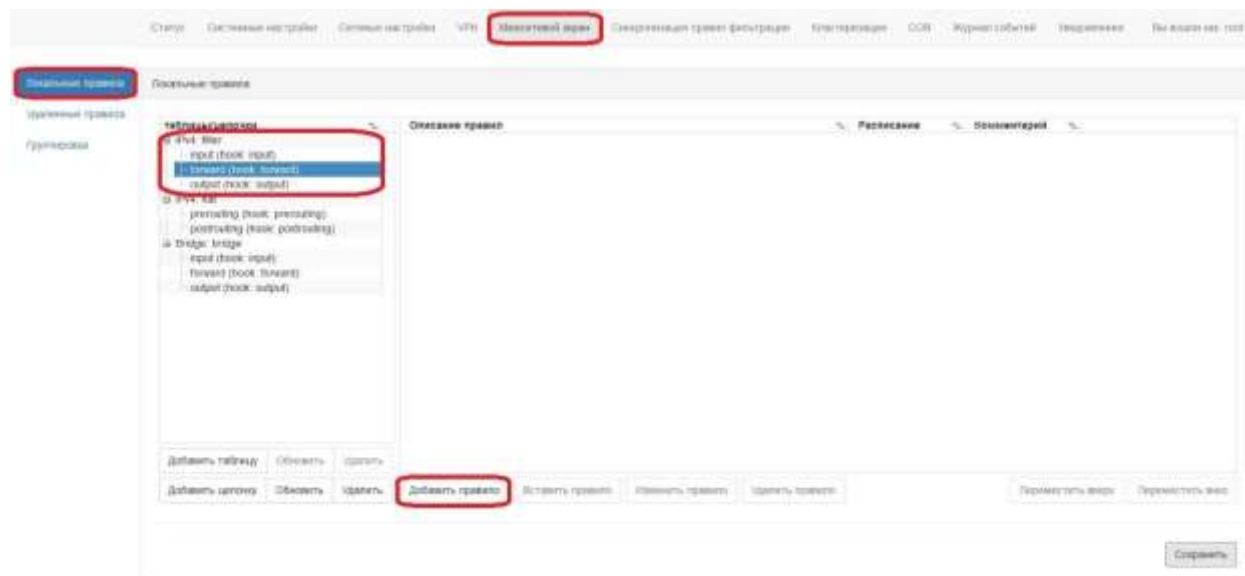


Рисунок 537 - Настройка фильтра IPv4

В новом окне «**Создание правила фильтрации**» необходимо выбрать пункт «**IP**». В поле «**Фильтрация по источнику**» или «**Фильтрация по назначению**» необходимо выбрать значение «**Доменное имя**». В поле «**Доменное имя источника**» или «**Доменное имя назначения**» задать доменное имя ресурса (Рисунок 538).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола ip4

Фильтрация по источнику Доменное имя

Адрес источника xxx.xxx.xxx.xxx маска подсети xxx.xxx.xxx.xxx

Доменное имя источника yandex.ru

Фильтрация по назначению Другое

Адрес назначения xxx.xxx.xxx.xxx маска подсети xxx.xxx.xxx.xxx

Доменное имя назначения

Метка DSCP N/A (0x00) Бит ECN Non-ECT (D0)

Длина пакета от 0 по 0

Время жизни пакета (TTL) от 0 по 0

☐ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

ОК Отмена

Рисунок 538 - Пункт «IP» и положение полей «Доменных имен»

В окне «Создание правила фильтрации» необходимо выбрать пункт «Действие» (Ошибка! Источник ссылки не найден.) и в поле «Действие» необходимо задать один из доступных вариантов и нажать на кнопку «ОК» (Рисунок 539).

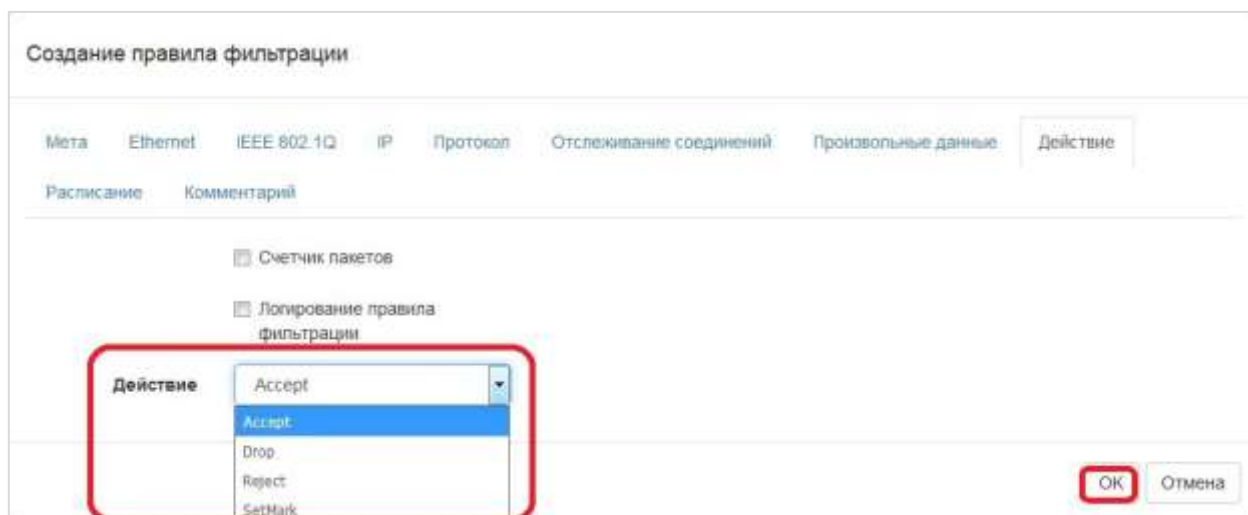


Рисунок 539 - Пункт меню «Создание правила фильтрации» и поле «Действие»

Для сохранения правила фильтрации необходимо нажать на кнопку «Сохранить» (Рисунок 540).

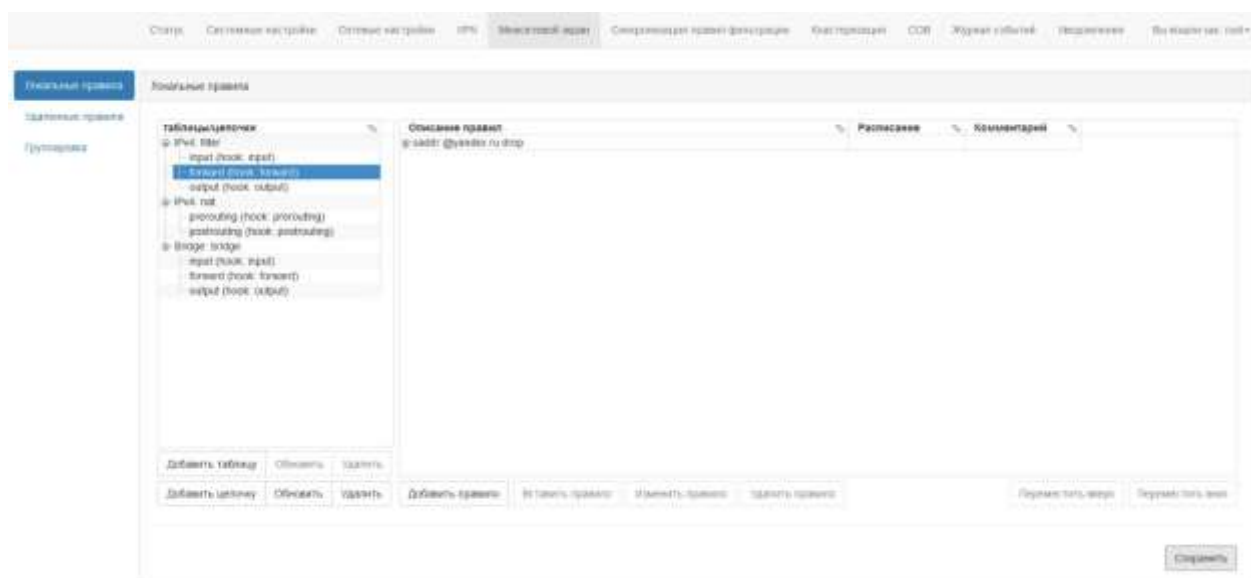


Рисунок 540 - Положение кнопки «Сохранить»

7.21 Настройка логирования правил фильтрации

Для создания правила фильтрации по доменному имени, необходимо в главном меню выбрать пункт **«Межсетевой экран – Локальные правила»**. В таблице **«Локальные правила»** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **«Добавить правило»** (Рисунок 541).

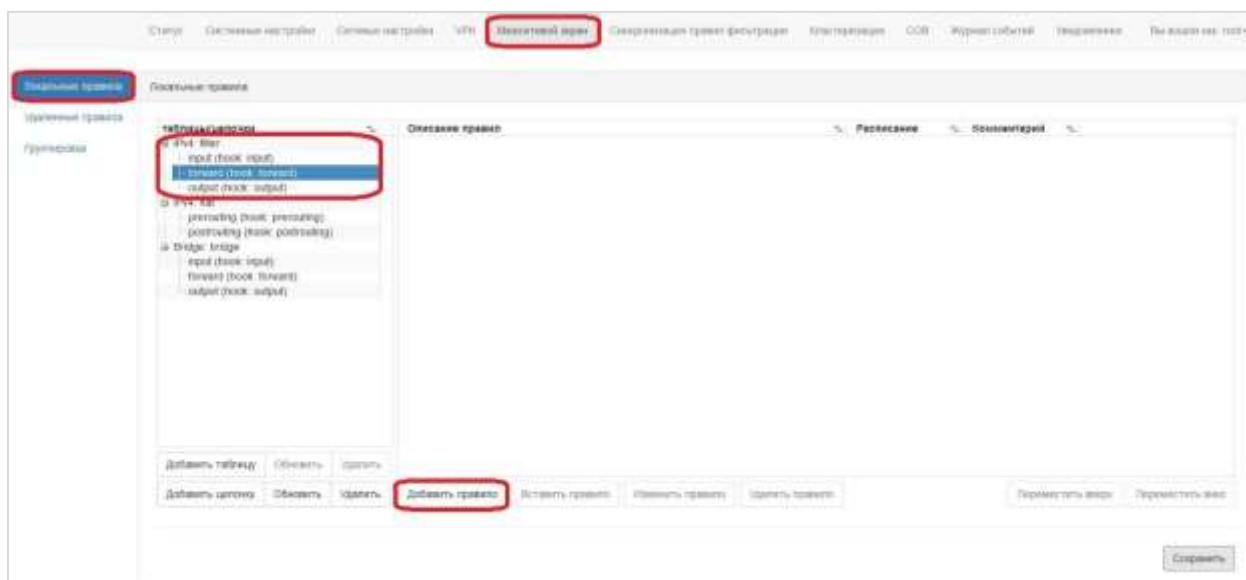


Рисунок 541 - Настройка фильтра IPv4

В новом окне «**Создание правила фильтрации**» необходимо выбрать пункт «**Действие**» и установить флаг «**Логирование правила фильтрации**». В поле «**Префикс**» необходимо задать название для записи в логах межсетевого экрана и нажать на кнопку «**ОК**» (Рисунок 542).

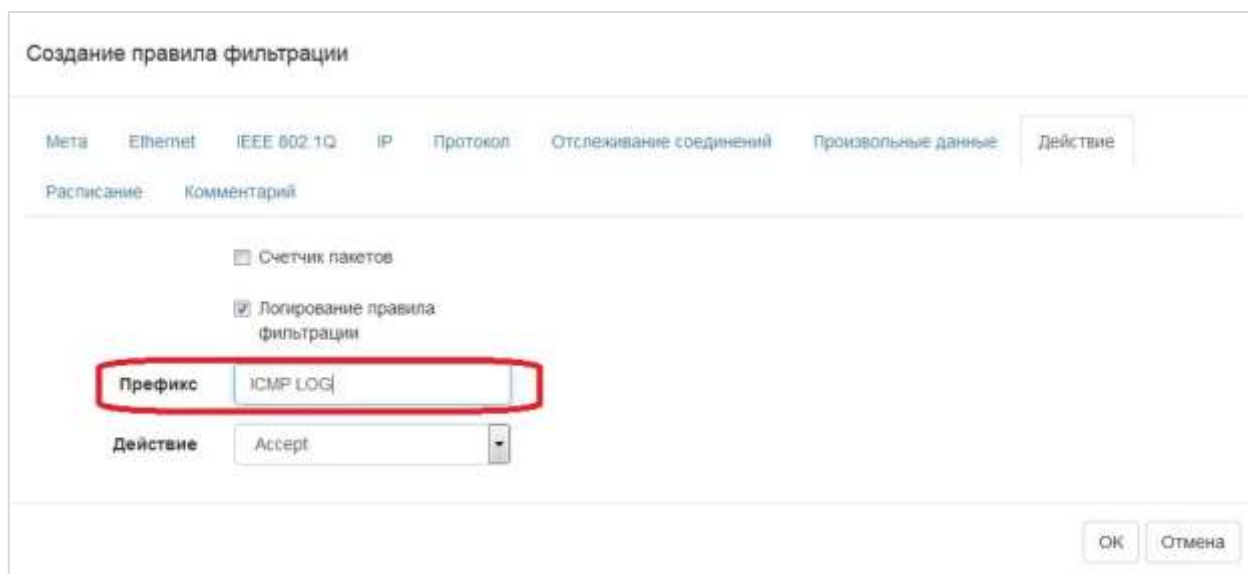


Рисунок 542 - Пункт «Действие» и положение поля «Префикс»

Для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**» (Рисунок 543).

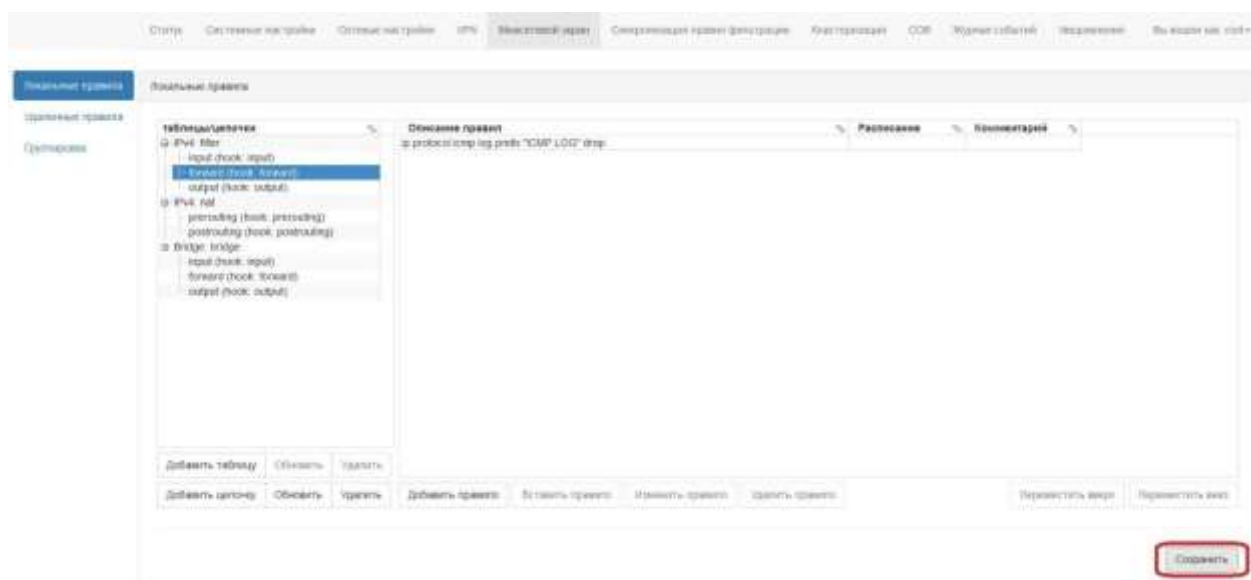


Рисунок 543 - Положение кнопки «Сохранить»

Логирование правила фильтрации очень трудоемкий процесс для устройства, который может отнимать большое количество ресурсов центрального процессора и оперативной памяти. Целесообразно использовать данный механизм только на этапе отладки.

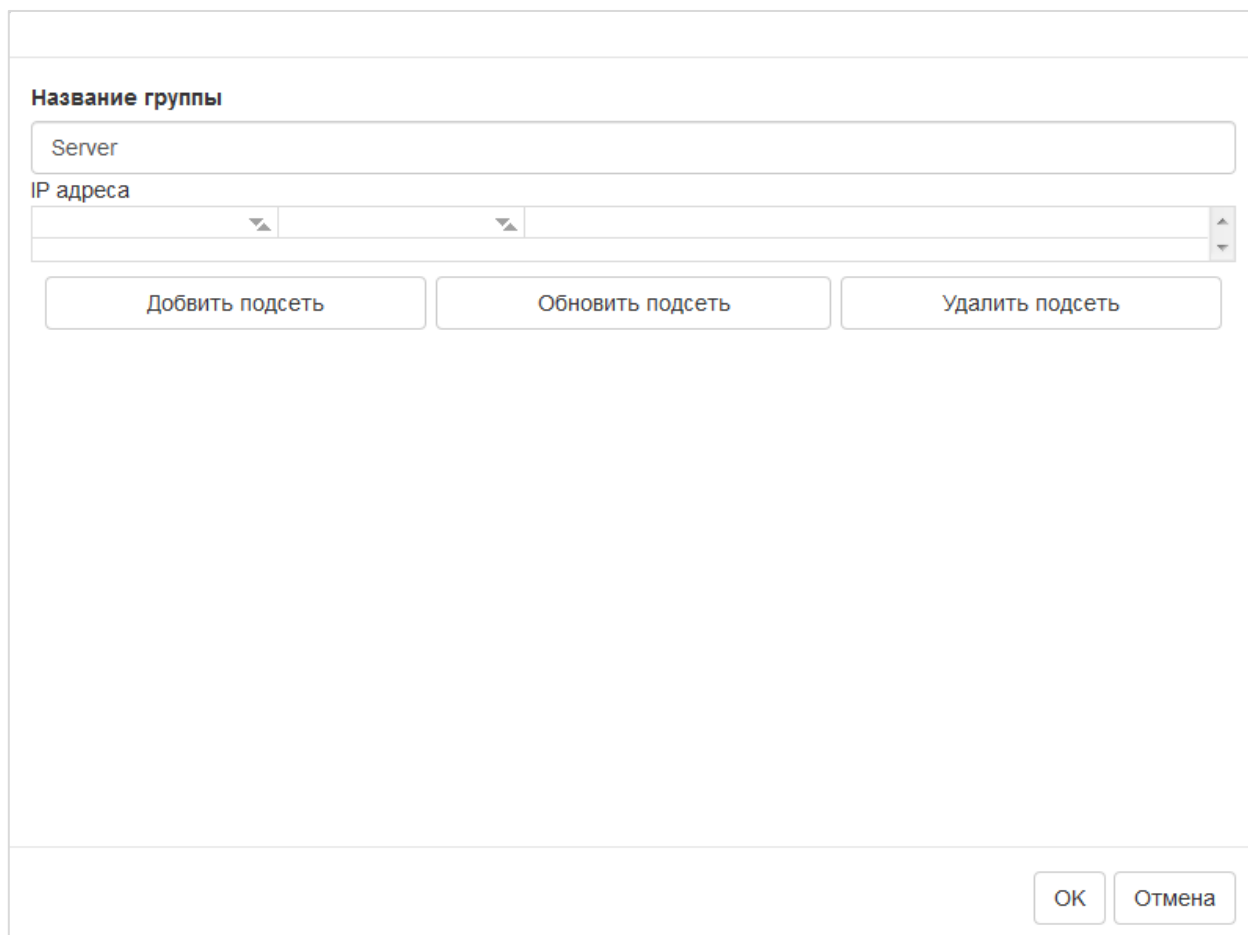
7.22 Создание группы ip-адресов

Для создания группы ip-адресов или диапазона ip адресов необходимо в главном меню выбрать пункт **«Межсетевой экран – Группировка»**. В таблице **«Группировка»** необходимо выбрать пункт **«IP-адреса»** и нажать на кнопку **«Добавить новую группу»**. Для изменения группы ip-адресов необходимо нажать на кнопку **«Изменить группу»**. Для удаления группы ip-адресов необходимо нажать на кнопку **«Удалить группу»** (Рисунок 544).



Рисунок 544 - Пункт «Группировка» и положение поля «IP-адреса»

В новом окне «**Создание группировки**» в поле «**название группы**» необходимо задать название для новой группы IP-адресов и нажать на кнопку «**Добавить подсеть**». Для изменения подсети необходимо нажать на кнопку «**Обновить подсеть**». Для удаления подсети необходимо нажать на кнопку «**Удалить подсеть**» (Рисунок 545).



The screenshot shows a window titled "Создание группировки". It contains a form with the following elements:

- A label "Название группы" above a text input field containing the text "Server".
- A label "IP адреса" above a container with three subnets, each represented by a text input field and a dropdown arrow. All three subnets are currently empty.
- Three buttons below the IP address fields: "Добвить подсеть" (note the typo), "Обновить подсеть", and "Удалить подсеть".
- At the bottom right, there are two buttons: "ОК" and "Отмена".

Рисунок 545 - Окно «Создание группировки» и поле «Название группы»

В новом окне необходимо выбрать параметр группы **Подсеть** или **Диапазон**, в поле **IP-адрес** необходимо задать IP-адрес хоста или подсети, в поле **Маска подсети** необходимо задать маску подсети и нажать на кнопку **ОК** (Рисунок 546).

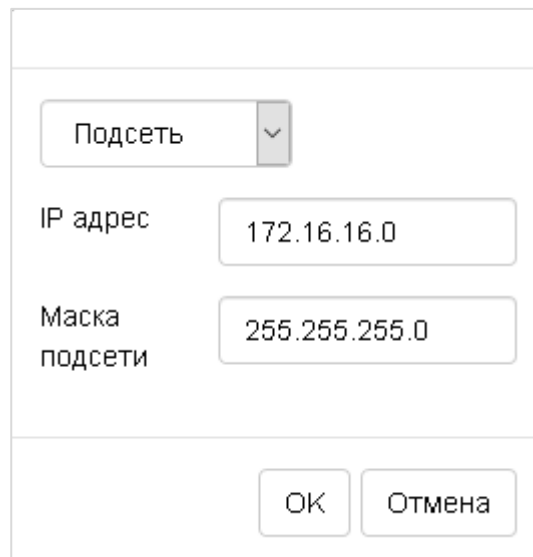


Рисунок 546 - Поле «IP-адрес» и поле «Маска подсети»

Для задания диапазона IP-адресов необходимо выбрать параметр **Диапазон**.

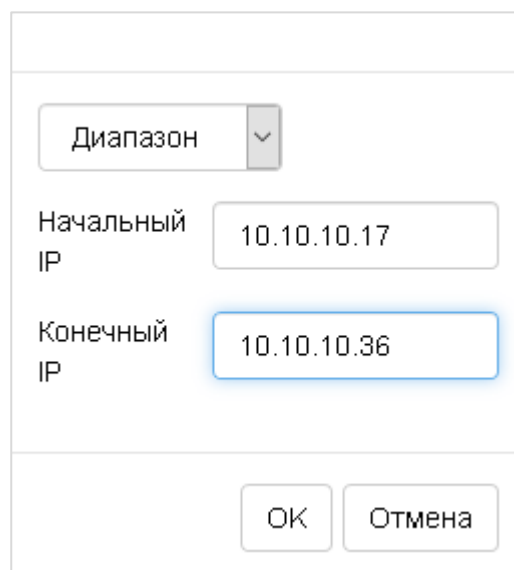
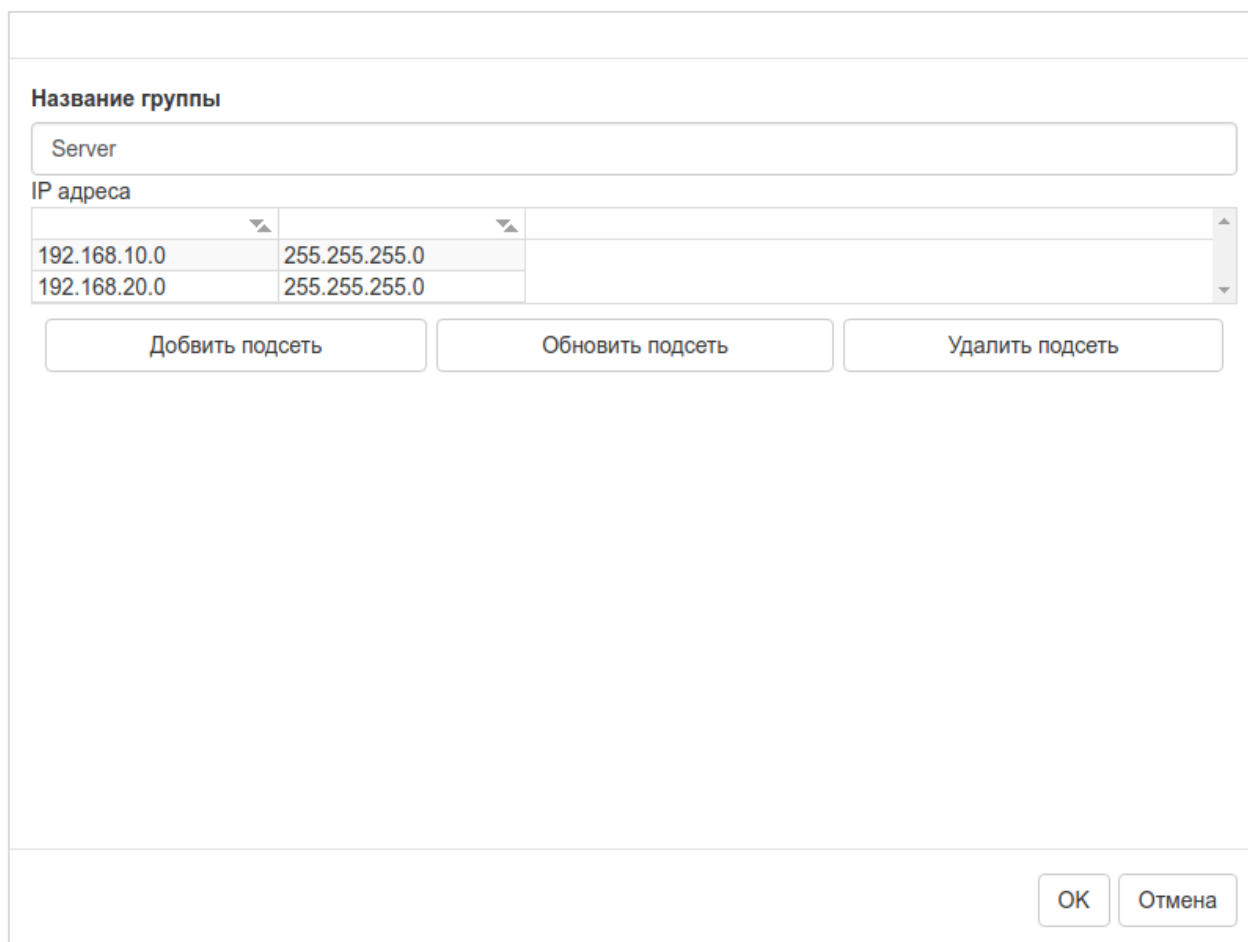


Рисунок 547

После добавления IP-адреса хоста или подсети необходимо нажать на кнопку «**ОК**» (Рисунок 547).



Название группы

Server

IP адреса

192.168.10.0	255.255.255.0
192.168.20.0	255.255.255.0

Добавить подсеть Обновить подсеть Удалить подсеть

OK Отмена

Рисунок 548 – Окно «Создание группировки» и поле «Название группы»

Для сохранения настроек необходимо нажать на кнопку **«Сохранить»** (Рисунок 549).

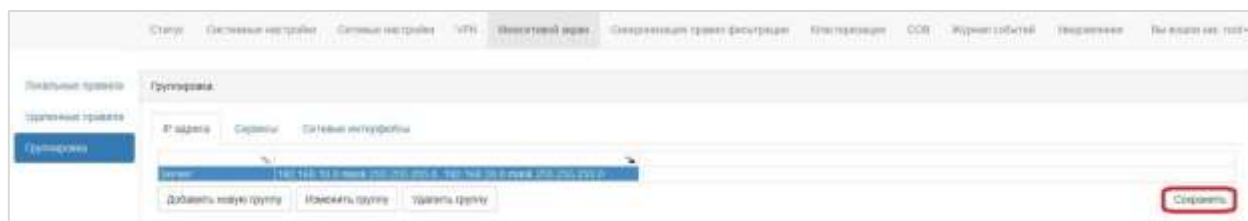


Рисунок 549 – Положение кнопки «Сохранить»

7.23 Создание правила фильтрации на основе группы ip-адресов

Для создания правила фильтрации на основе группы ip-адресов необходимо в главном меню выбрать пункт **«Межсетевой экран – Локальные**

правила. В таблице **Локальные правила** необходимо выбрать цепочку правил фильтрации и нажать на кнопку «Добавить правило» (Рисунок 550).

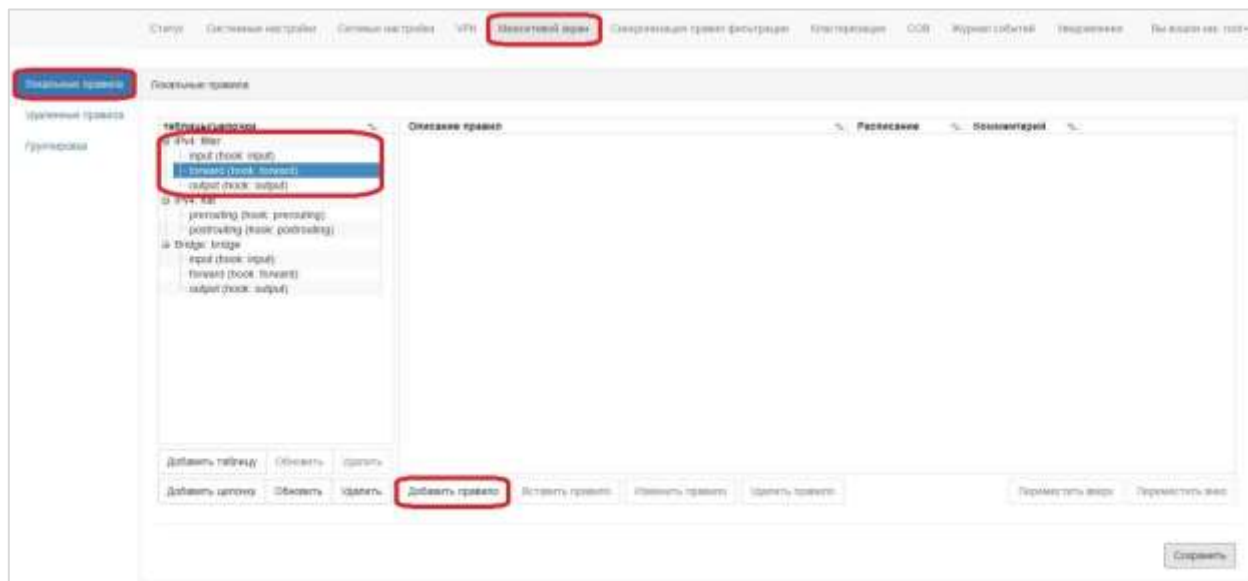


Рисунок 550 – Настройка фильтра IPv4

В новом окне **Создание правила фильтрации** необходимо выбрать пункт «IP». В поле «Фильтрация по источнику» или **Фильтрация по назначению** необходимо выбрать группу ip-адресов (Рисунок 551).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q **IP** Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола ip4

Фильтрация по источнику Server

Адрес источника xxx.xxx.xxx.xxx маска подсети xxx.xxx.xxx.xxx

Доменное имя источника

Фильтрация по назначению Другое

Адрес назначения xxx.xxx.xxx.xxx маска подсети xxx.xxx.xxx.xxx

Доменное имя назначения

Метка DSCP N/A (0x00) Бит ECN Non-ECT (00)

Длина пакета от 0 по 0

Время жизни пакета (TTL) от 0 по 0

☐ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

ОК Отмена

Рисунок 551 – Пункт «IP» и положение полей «Фильтрации»

В окне «**Создание правила фильтрации**» необходимо выбрать пункт «**Действие**» и в поле «**Действие**» необходимо задать один из доступных вариантов и нажать на кнопку «**ОК**» (Рисунок 552).

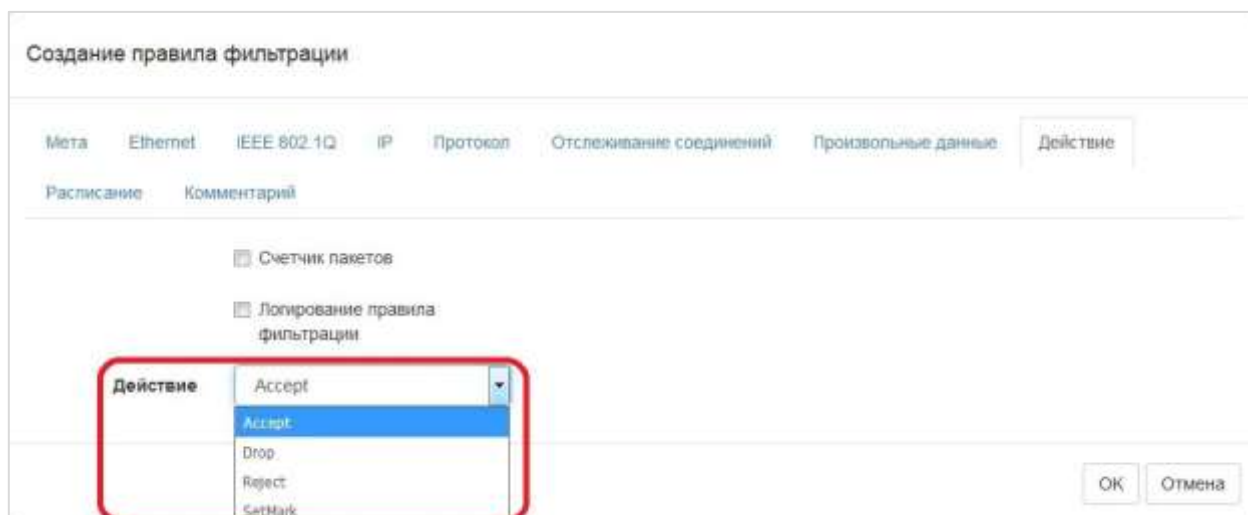


Рисунок 552 – Пункт меню «Создание правила фильтрации» и поле «Действие»

Для сохранения правила фильтрации необходимо нажать на кнопку «Сохранить» (Рисунок 553).

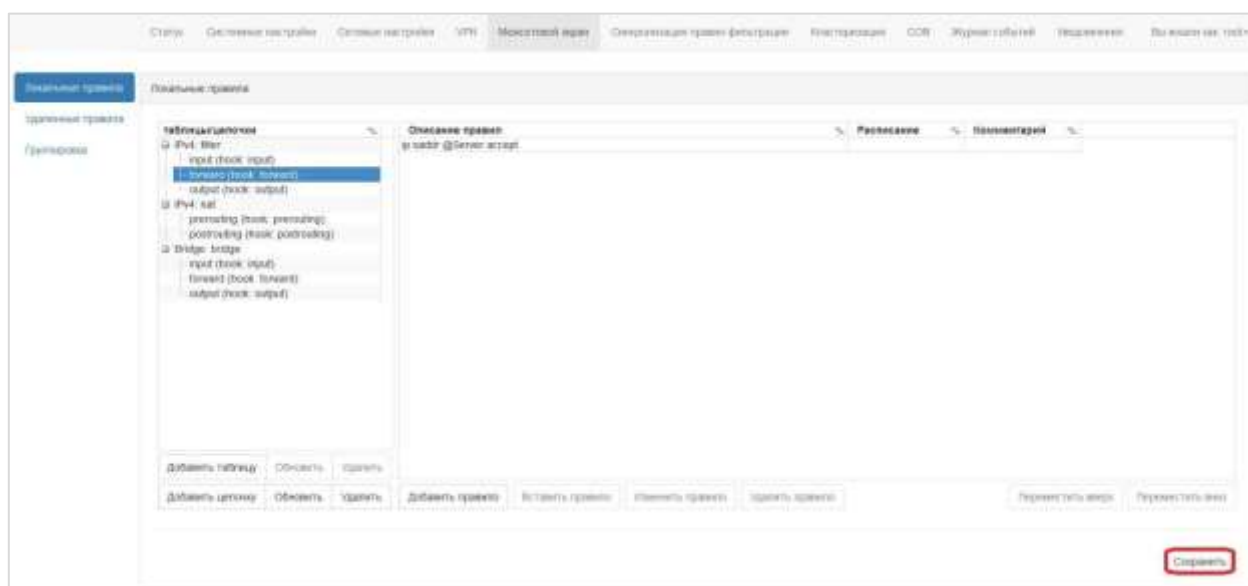


Рисунок 553 – Положение кнопки «Сохранить»

7.24 Создание группы сетевых портов

Для создания группы сетевых портов необходимо в главном меню выбрать пункт «Межсетевой экран – Группировка». В таблице «Группировка»

необходимо выбрать пункт «**Сервисы**» и нажать на кнопку «**Добавить новую группу**». Для изменения группы сетевых портов необходимо нажать на кнопку «**Обновить группу**». Для удаления группы сетевых портов необходимо нажать на кнопку «**Удалить группу**» (Рисунок 554).

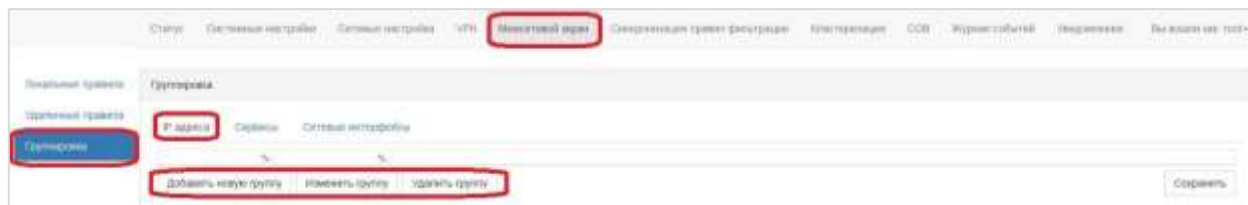


Рисунок 554 - Пункт «Группировка» и положение поля «IP-адреса»

В новом окне «**Создание группировки**» в поле «**название группы**» необходимо задать название для новой группы сетевых портов и нажать на кнопку «**Добавить сетевой порт**». Для изменения подсети необходимо нажать на кнопку «**Обновить сетевой порт**». Для удаления подсети необходимо нажать на кнопку «**Удалить сетевой порт**» (Рисунок 555).

Название группы

http

Серверы

Добавить сетевой порт Обновить сетевой порт Удалить сетевой порт

ОК Отмена

Рисунок 555 – Окно «Создание группировки»

В новом окне в поле «**Сетевой порт с**» необходимо задать сетевой порт для начала диапазона, в поле «до» необходимо задать сетевой порт для конца диапазона и нажать на кнопку «**ОК**» (Рисунок 556).

Сетевой порт с

80

до

80

OK Отмена

Рисунок 556 – Поле «Сетевой порт»

После добавления сетевого порта необходимо нажать на кнопку «ОК».

Название группы

Http

Сервисы

80	80
443	443

Добавить сетевой порт Обновить сетевой порт Удалить сетевой порт

OK Отмена

Рисунок 557 – Положение кнопки «ОК»

Для сохранения настроек необходимо нажать на кнопку **«Сохранить»** (Рисунок 558).

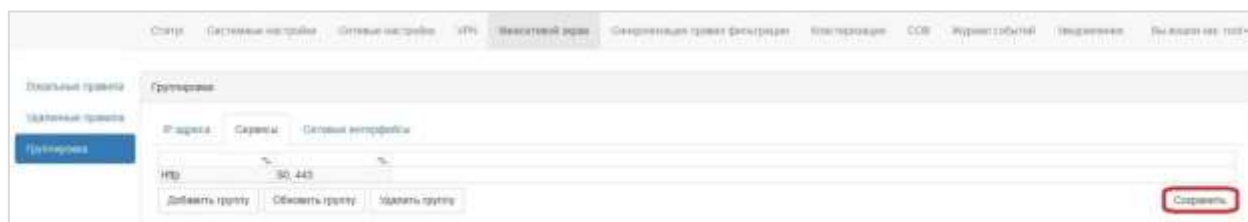


Рисунок 558 - Положение кнопки «Сохранить»

7.25 Создание правила фильтрации на основе группы сетевых портов

Для создания правила фильтрации на основе группы сетевых портов необходимо в главном меню выбрать пункт **«Межсетевой экран – Локальные правила»**. В таблице **«Локальные правила»** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **«Добавить правило»** (Рисунок 559).

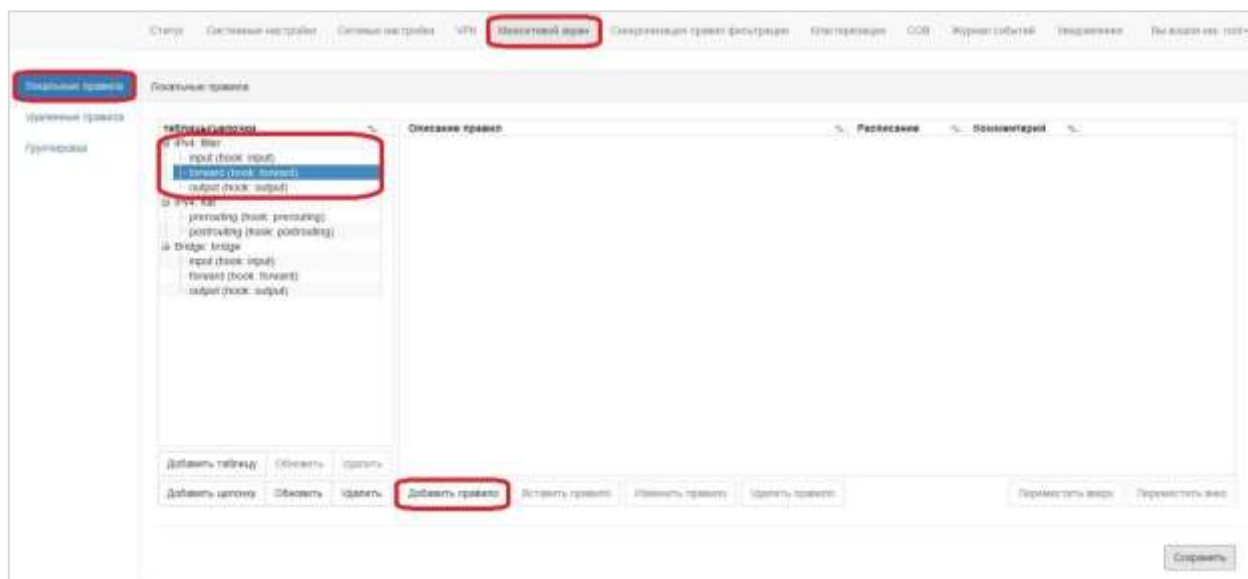


Рисунок 559 – Настройка фильтра IPv4

В новом окне **«Создание правила фильтрации»** необходимо выбрать пункт **«Протокол»**. В поле **«Протокол»** необходимо выбрать протокол TCP или протокол UDP. В поле **«Source service group»** или **«Destination service group»**

необходимо выбрать группу сетевых портов и нажать на кнопку «**ОК**» (Рисунок 560).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP **Протокол** Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Протокол TCP (6)

Параметры TCP

Source service group Http

Порт источника с 0 по 0

Destination service group Другое

Порт назначения с 0 по 0

Флаги ☐ fin ☐ syn ☐ rst ☐ psh ☐ ack ☐ urg ☐ ecn ☐ cwr

ОК Отмена

Рисунок 560 – Окно «Создание правила фильтрации» и положение поля «Протокол TCP»

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP **Протокол** Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Протокол UDP (17)

Параметры UDP:

Порт источника с 0 по 0

Source service group Http

Порт назначения с 0 по 0

Destination service group Другое

OK Отмена

Рисунок 561 – Окно «Создание правила фильтрации» и положение поля «Протокол UDP»

В окне «Создание правила фильтрации» необходимо выбрать пункт «Действие» (**Ошибка! Источник ссылки не найден.**) и в поле «Действие» необходимо задать один из доступных вариантов и нажать на кнопку «OK» (Рисунок 562).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP Протокол Отслеживание соединений Произвольные данные **Действие**

Расписание Комментарий

☐ Счетчик пакетов

☐ Логирование правила фильтрации

Действие Accept

Accept

Drop

Reject

SetMark

OK Отмена

Рисунок 562 – Окно «Создание правила фильтрации» и пункт «Действие»

Для сохранения правила фильтрации необходимо нажать на кнопку «Сохранить» (Рисунок 563).

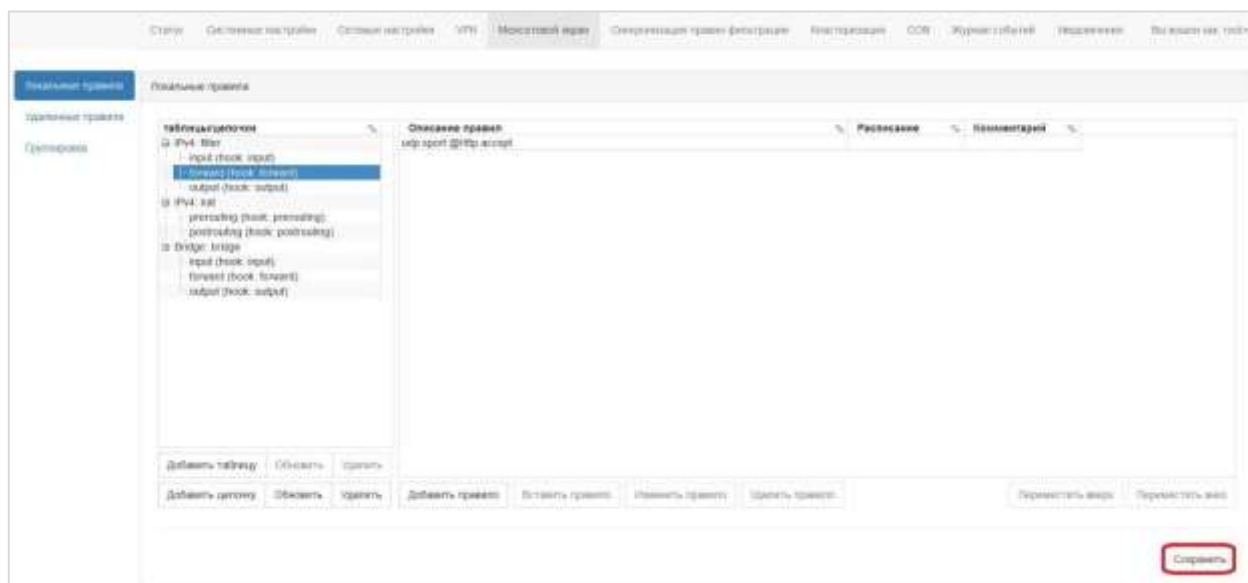


Рисунок 563 – Положение кнопки «Сохранить»

7.26 Настройка счетчика пакетов для правила фильтрации

Для настройки счетчика пакетов для правила фильтрации необходимо в главном меню выбрать пункт **«Межсетевой экран – Локальные правила»**. В таблице **«Локальные правила»** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **«Добавить правило»** (Рисунок 564).

необходимо задать один из доступных вариантов и нажать на кнопку «**ОК**» (Рисунок 566).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP Протокол Отслеживание соединений Произвольные данные **Действие**

Расписание Комментарий

☒ Счетчик пакетов

☐ Логирование правила фильтрации

Действие Ассерти

ОК Отмена

Рисунок 566 – Окно «Создание правила фильтрации» и пункт «Действие»

Для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**» (Рисунок 567).

Статус Системные настройки Сетевые настройки VPN Масштабный анализ Сериализация правил фильтрации Конфигурация СОФ Журнал событий Подключение

Вы вошли как: root

Локальные правила

Исходные правила

Правила

Название/описание Описание правила Расписание Комментарий

ip protocol tcp reset counter assert

Сохранить

Рисунок 567 – Положение кнопки «Сохранить»

7.27 Настройка комментария для правила фильтрации

Для настройки комментария для правила фильтрации необходимо в главном меню выбрать пункт **«Межсетевой экран – Локальные правила»**. В таблице **«Локальные правила»** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **«Добавить правило»** (Рисунок 568).

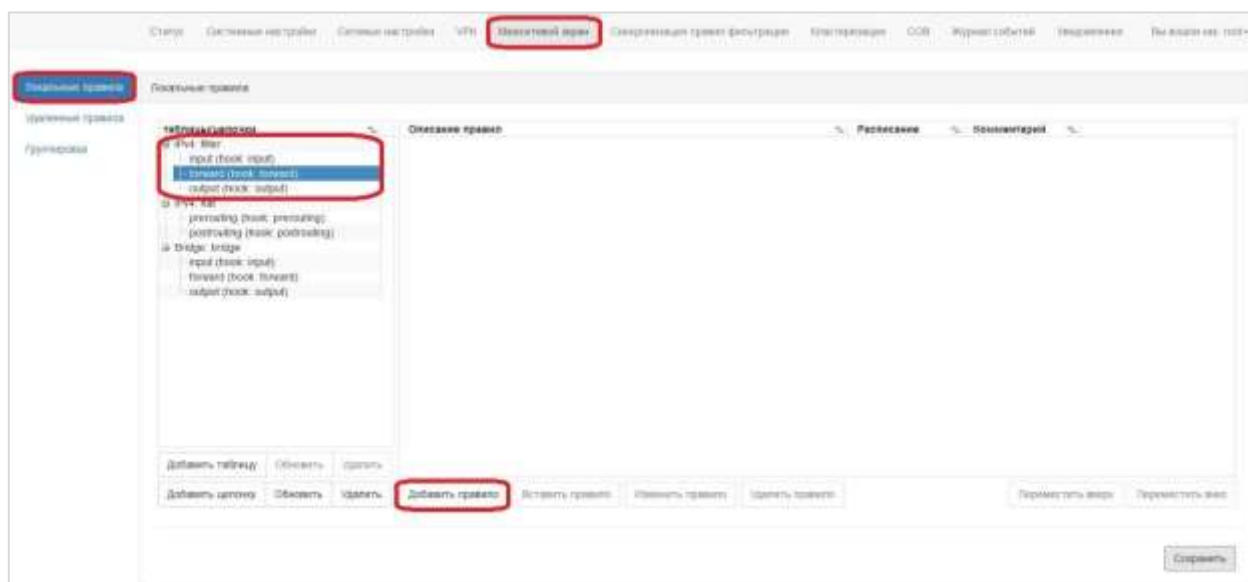


Рисунок 568 – Настройка фильтра «IPv4»

В новом окне **«Создание правила фильтрации»** необходимо задать параметры фильтрации. Для примера, создадим разрешающее правило для протокола ICMP (Рисунок 569).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP **Протокол** Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Протокол ICMP (1)

ICMP тип

ICMP код

OK Отмена

Рисунок 569 – Окно «Создание правила фильтрации» и поле «Протокол»

В окне «**Создание правила фильтрации**» необходимо выбрать пункт «**Действие**» и в поле «**Действие**» необходимо задать один из доступных вариантов и нажать на кнопку «**ОК**» (Рисунок 570/571).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP Протокол Отслеживание соединений Произвольные данные **Действие**

Расписание Комментарий

☐ Счетчик пакетов

☐ Логирование правила фильтрации

Действие Accept

OK Отмена

Рисунок 570 – Окно «Создание правила фильтрации» и пункт «Действие»

В окне «Создание правила фильтрации» необходимо выбрать пункт «Комментарий», задать комментарий к правилу фильтрации и нажать на кнопку «ОК» (Рисунок 571).

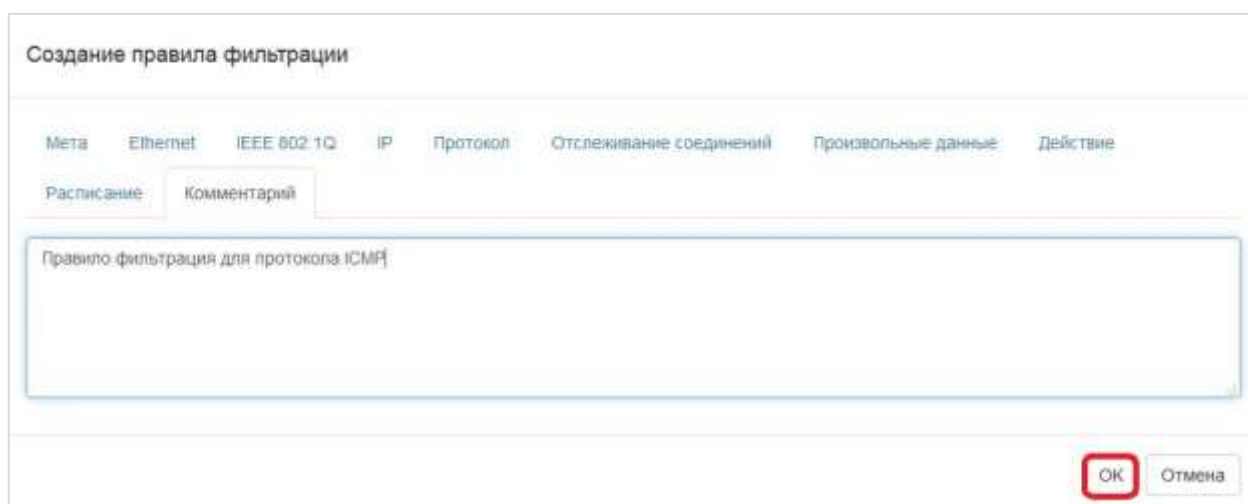


Рисунок 571 – Положение кнопки «ОК»

Для сохранения правила фильтрации необходимо нажать на кнопку «Сохранить». (Рисунок 572)

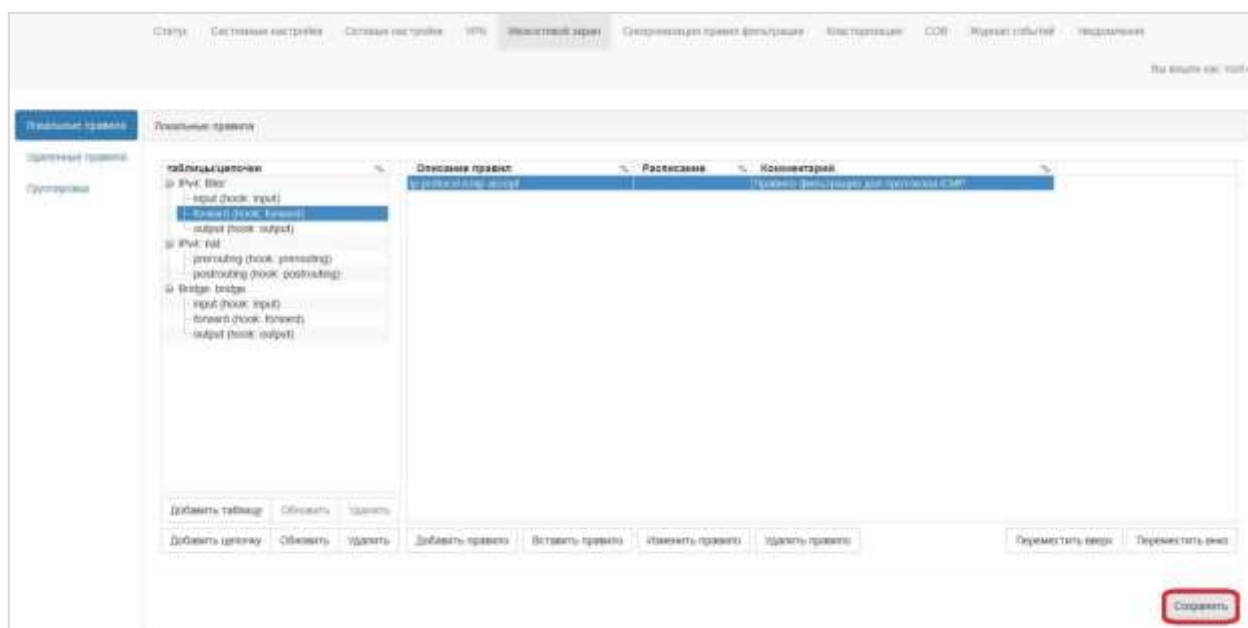


Рисунок 572 – Положение кнопки «Сохранить»

6.7.3 Синхронизация правил фильтрации

Синхронизация правил фильтрации позволяет централизованно создавать, изменять, удалять и управлять правилами фильтрации на подчиненных устройствах.

Устройство МКСЗ Горизонт-ВС может быть настроено в режиме работы главного устройства и подчиненного устройства. Главное устройство позволяет настраивать правила фильтрации для удаленных устройств, управлять группами.

8.1 Настройка устройства в режиме Master

Для настройки устройства в режиме «**Master**» необходимо в главном меню выбрать пункт «**Синхронизация правил фильтрации -- Статус**». В таблице «**Настройка режима работы**» необходимо установить флаг «**Главное устройство**». В поле «**IP-адрес для прослушивания**» необходимо задать ip-адрес одного из сетевых интерфейсов устройства, в поле «**Сетевой порт для прослушивания**» необходимо задать сетевой порт и нажать на кнопку «**Сохранить**» (Рисунок 573).

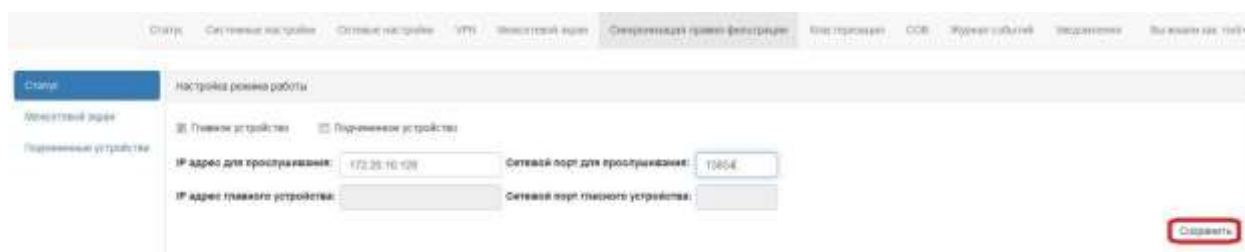


Рисунок 573 – Положение кнопки «Сохранить»

8.2 Настройка устройства в режиме Slave

Для настройки устройства в режиме «**Slave**» необходимо в главном меню выбрать пункт «**Синхронизация правил фильтрации -- Статус**». В таблице «**Настройка режима работы**» необходимо установить флаг «**Подчиненное устройство**». В поле «**IP-адрес для прослушивания**» необходимо задать ip-адрес одного из сетевых интерфейсов устройства, в поле «**Сетевой порт для прослушивания**» необходимо задать сетевой порт, в поле «**IP-адрес главного устройства**» необходимо ввести ip-адрес устройства, которое работает в режиме «**Master**», в поле «**Сетевой порт главного устройства**» необходимо задать сетевой порт для подключения к устройству, которое работает в режиме

«**Master**». Для сохранения настроек необходимо нажать на кнопку «**Сохранить**» (Рисунок 574).

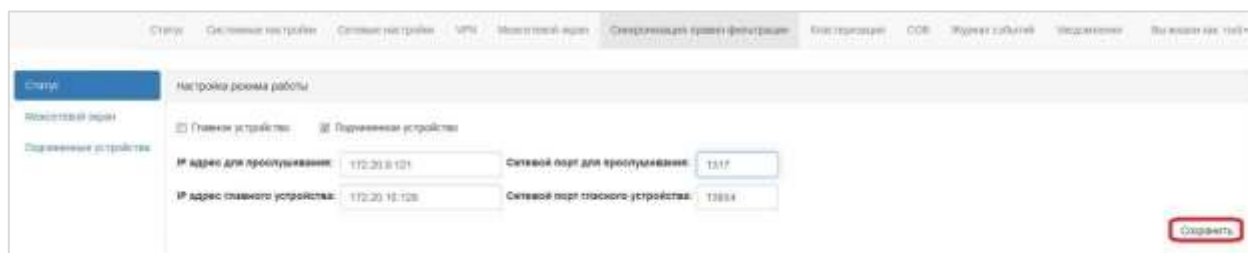


Рисунок 574 – Положение кнопки «Сохранить»

После успешного подключения к «**Главному устройству**», которое работает в режиме «**Master**», подчиненному устройству автоматически будет выдан номер «ID» (Рисунок 575).

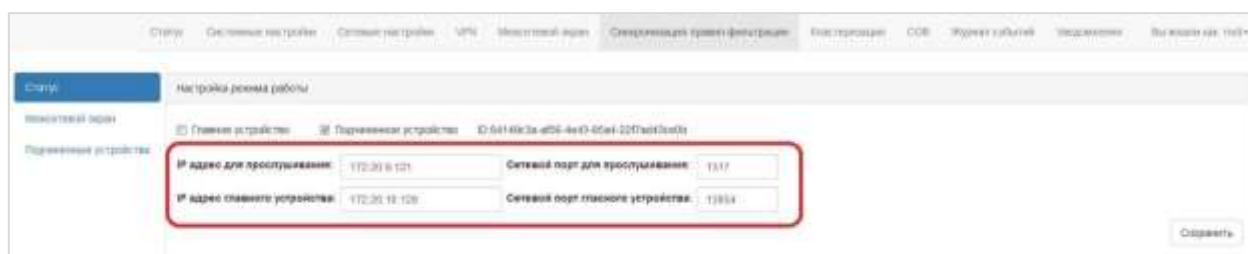


Рисунок 575 – Поле «Настройка режима работы»

8.3 Создание группы с правилами фильтрации

Для создания группы с правилами фильтрации необходимо в главном меню выбрать пункт «**Синхронизация правил фильтрации – Межсетевой экран**» и нажать на кнопку «**Добавить группу**» (Рисунок 576).

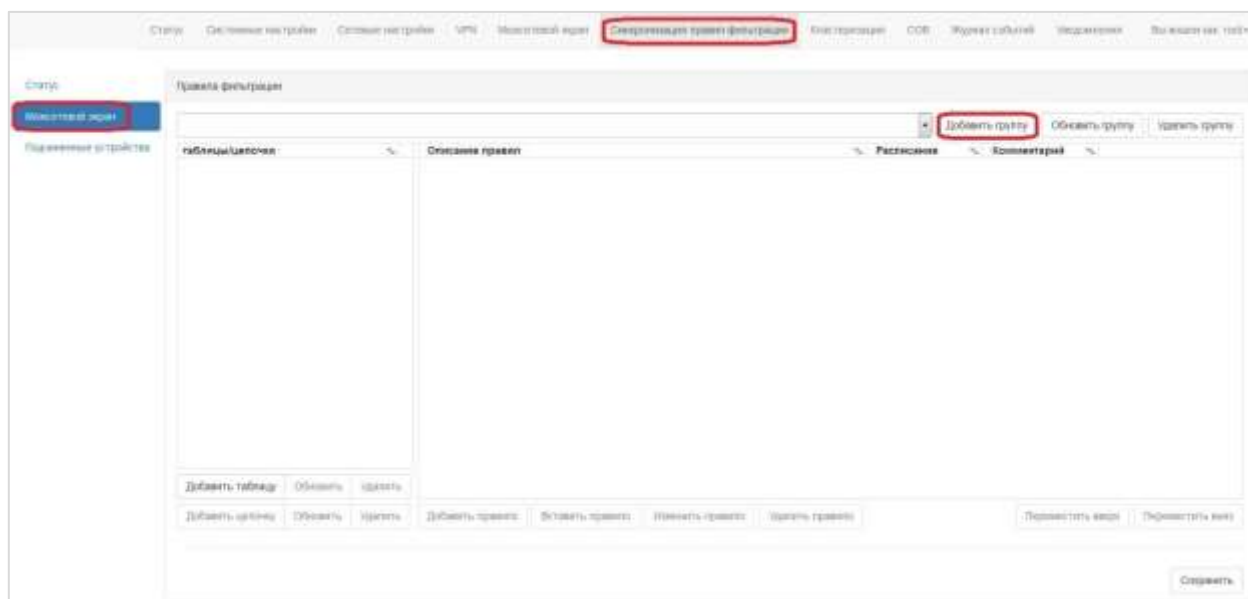


Рисунок 576 – Пункт «Синхронизация правил фильтрации – Межсетевой экран» и положение кнопки «Добавить группу»

В новом окне «**Добавить новую группу**» в поле «**Название группы**» необходимо ввести название группы с правилами фильтрации и нажать на кнопку «**ОК**» (Рисунок 577).

Добавить новую группу

Название группы

Ok Отмена

Рисунок 577 – Окно «Добавить новую группу»

В таблице «**Правила фильтрации**» необходимо выбрать группу «**Server**», в разделе «**таблицы/цепочки**» необходимо создать таблицу фильтрации и цепочки фильтрации для исходящего, входящего и транзитного трафика. Для

сохранения настроек необходимо нажать на кнопку «**Сохранить**» и нажать на кнопку «**ОК**» (Рисунок 478578).

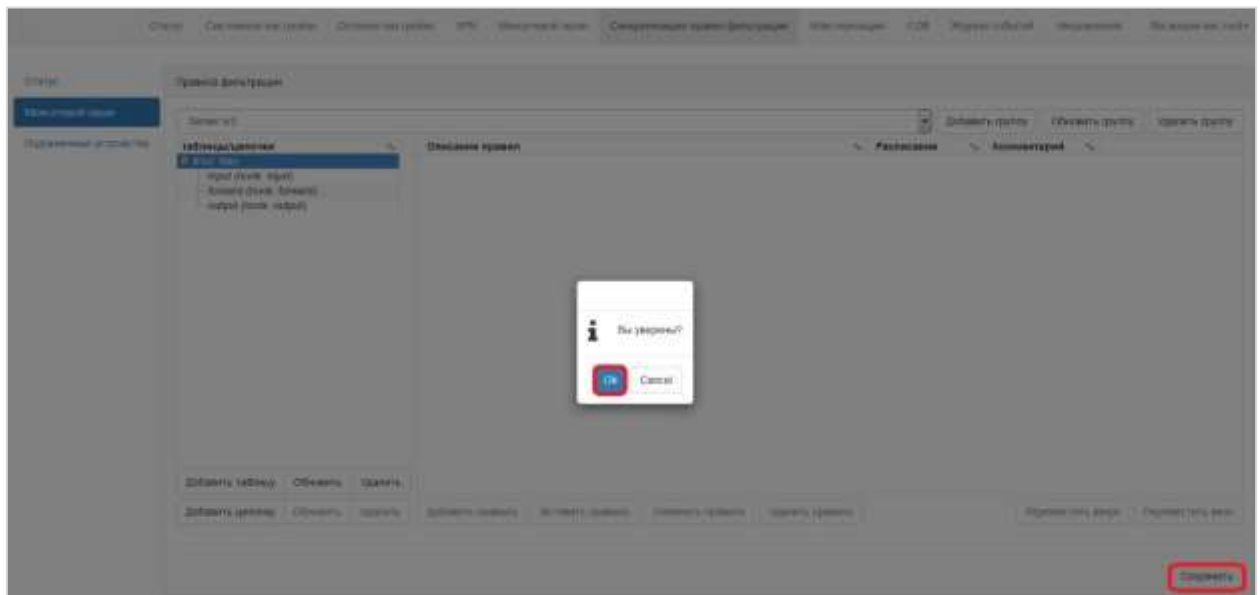


Рисунок 578 – Положение кнопок «Сохранить» и «ОК»

В одной из цепочек правил необходимо создать несколько правил фильтрации, которые мы хотим синхронизировать на другие устройства МКСЗ Горизонт-ВС. Создадим запрещающее правило фильтрации для протокола ICMP для транзитного трафика, запрещающее правило фильтрации для протокола TCP порт 80 для входящего трафика и сохраним настройки.

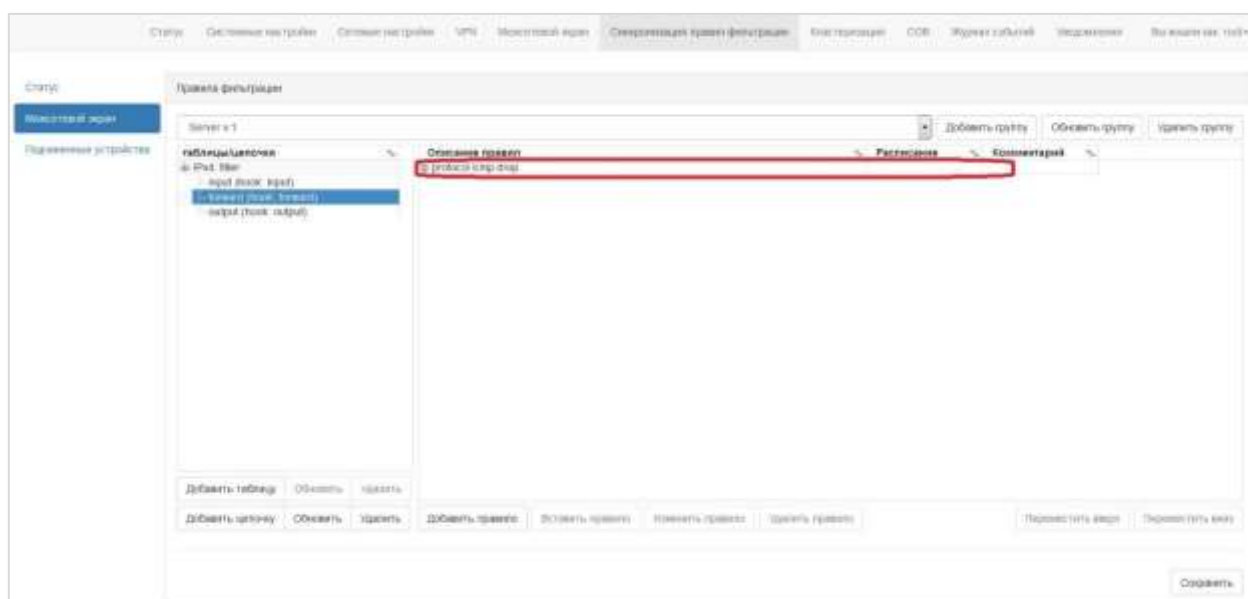


Рисунок 579 – Запрещающее правило фильтрации

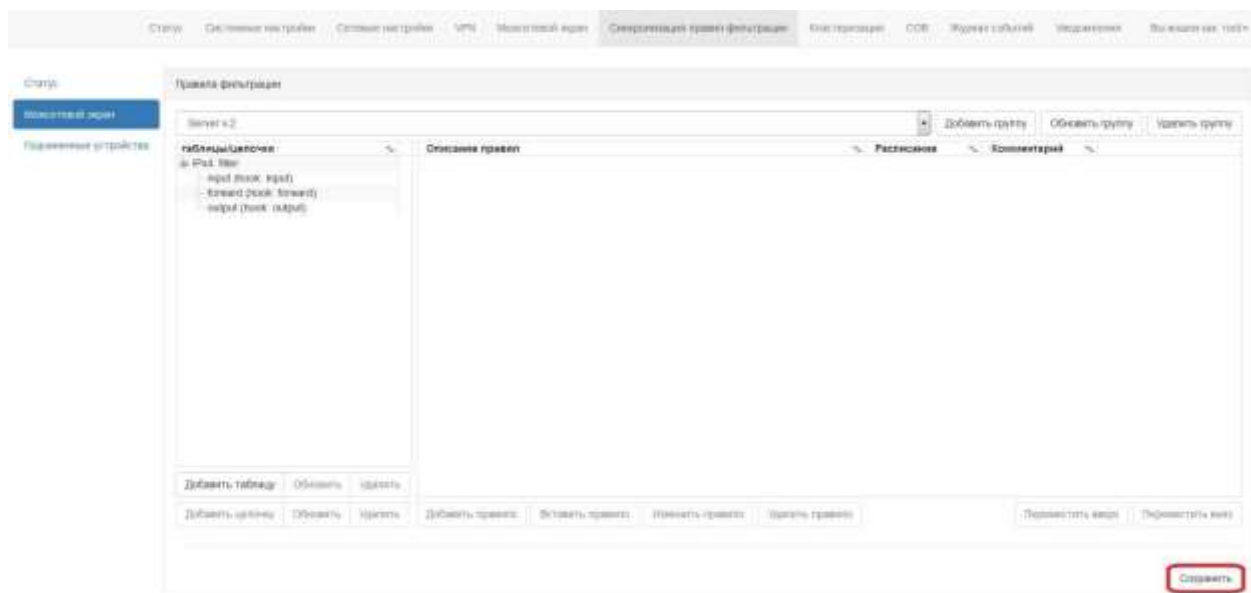


Рисунок 580 – Положение кнопки «Сохранить»

8.4 Управление подчиненными устройствами

По умолчанию все подчиненные устройства МКСЗ Горизонт-ВС попадают в группу «**Default**». Для просмотра подчиненного устройства в группе необходимо в главном меню выбрать пункт «**Синхронизация правил фильтрации – Подчиненные устройства**» (Рисунок 581), в таблице

«Управление подчиненными устройствами» в разделе «Название группы» выбрать группу «Default» (Рисунок 582). Ниже будут отображены «ID» подчиненных устройств. По умолчанию группа «Default» не имеет правил фильтрации.

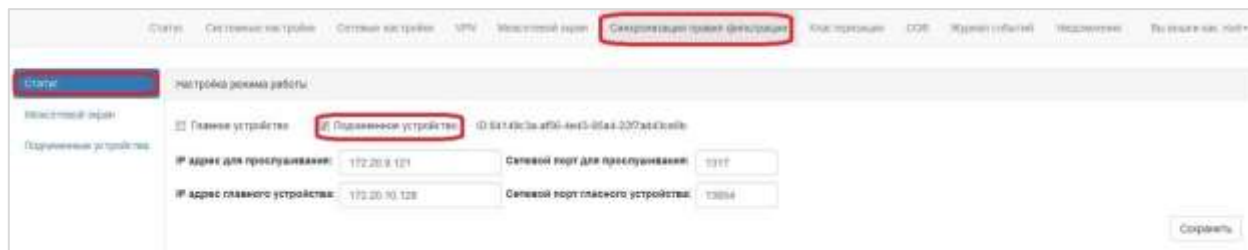


Рисунок 581 – Пункт меню «Синхронизация правил фильтрации» и пункт «Подчиненные устройства»

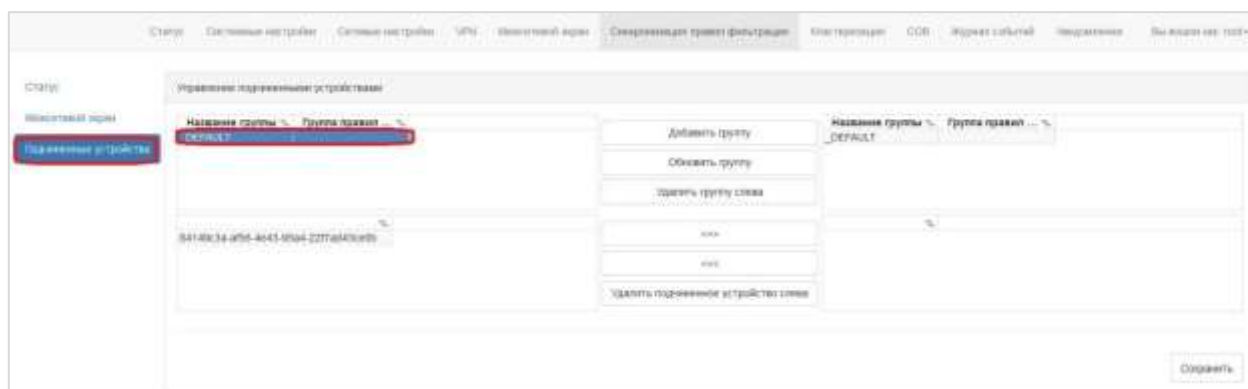


Рисунок 582 – Пункт «Подчиненные устройства» и выбор группы «Default»

Для добавления подчиненного устройства в новую группу необходимо в главном меню выбрать пункт «Синхронизация правил фильтрации – Подчиненные устройства», в таблице «Управление подчиненными устройствами» необходимо нажать на кнопку «Добавить группу». В поле «Название группы» необходимо задать название новой группы, в поле «Группа правил фильтрации» необходимо выбрать одну из доступных групп правил фильтрации и нажать на кнопку «ОК» (Рисунок 583). Для обновления группы необходимо нажать на кнопку «Обновить группу», для удаления группы необходимо нажать на кнопку «Удалить группу». Для удаления подчиненного

устройства необходимо выбрать «ID» устройства и нажать на кнопку «**Удалить подчиненное устройство**».

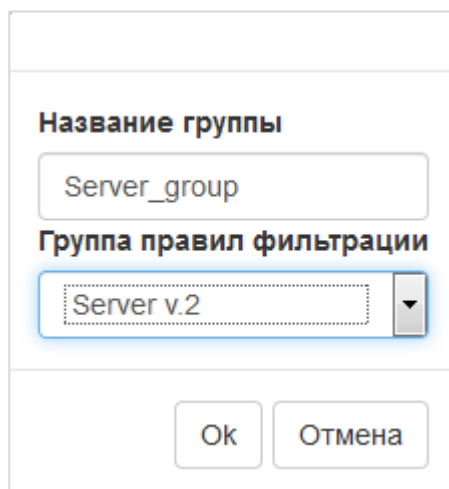


Рисунок 583 – Окно «Добавить группу»

Для сохранения настроек необходимо нажать на кнопку «**Сохранить**» (Рисунок 584).

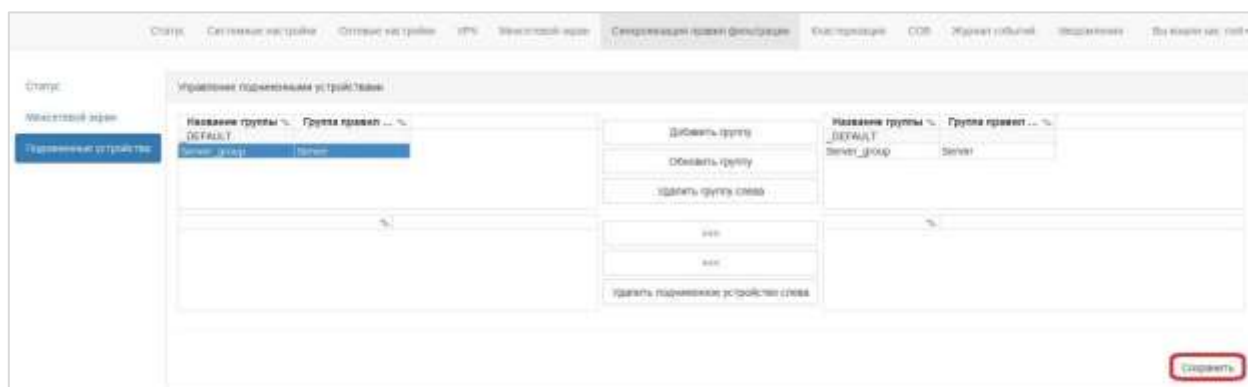


Рисунок 584 – Положение кнопки «Сохранить»

Для добавления устройства в новую группу «**Server_group**» необходимо в главном меню выбрать пункт «**Синхронизация правил фильтрации – Подчиненные устройства**», в таблице «**Управление подчиненными устройствами**» необходимо выбрать «ID» устройства в группе «**Default**» и группу, в которую необходимо переместить устройство «**Server_group**», и нажать на кнопку «>>>» (Рисунок 585).

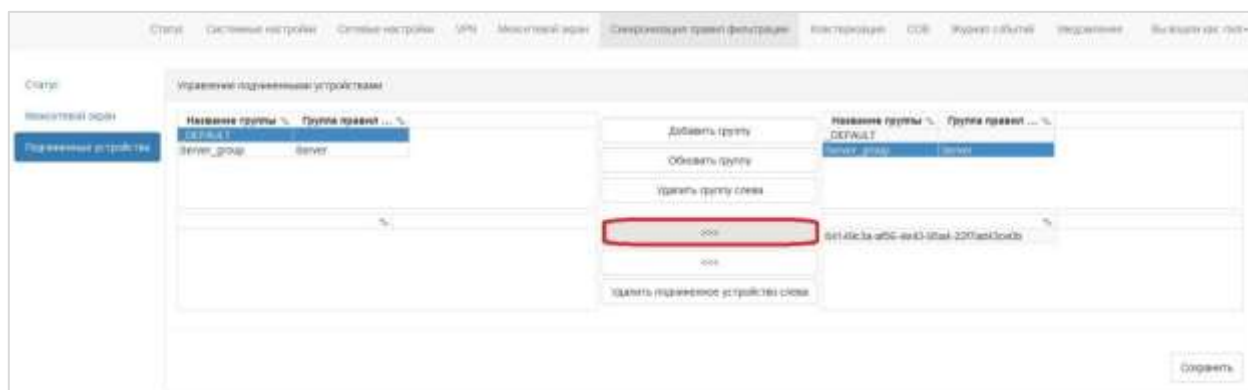


Рисунок 585 – Добавления устройства в новую группу «Server_group»

Для сохранения настроек необходимо нажать на кнопку «Сохранить» (Рисунок 586).

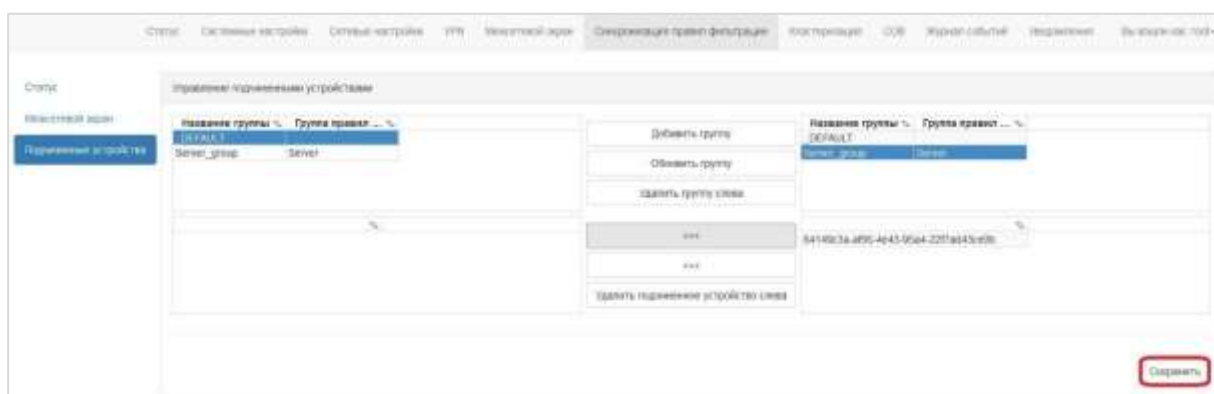


Рисунок 586 – Положение кнопки «Сохранить»

8.5 Правило фильтрации по умолчанию

Для задания правила фильтрации по умолчанию в текущей цепочке необходимо в главном меню выбрать пункт **«Синхронизация правил фильтрации – Локальные правила»**. В таблице **«Локальные правила»** необходимо выбрать цепочку правил фильтрации и нажать на кнопку **«Обновить»** (Рисунок 587).

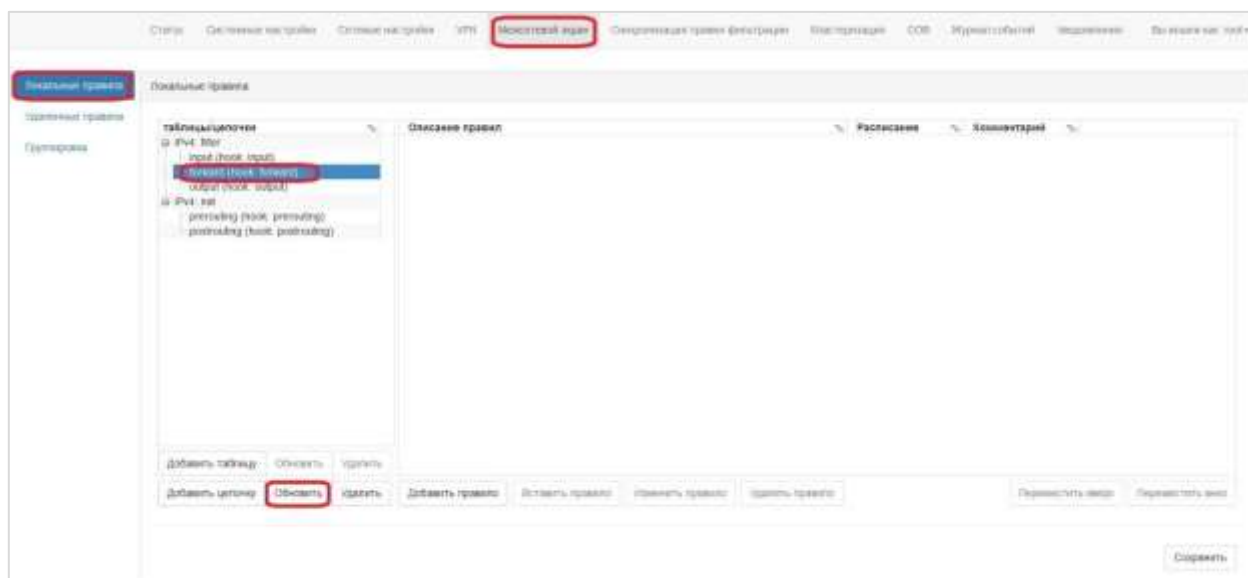


Рисунок 587 – Задание правила фильтрации по умолчанию

В новом окне «**Редактировать описание цепочки**» (Рисунок 589) в поле «**Политика**» необходимо задать действие по умолчанию, которое будет применяться ко всем сетевым пакетам, которые проходят через эту цепочку правил и нажать на кнопку «**ОК**». Правило по умолчанию находится в конце цепочки правил фильтрации. По умолчанию задана разрешающая политика.

Редактировать описание цепочки

Тип цепочки правил

forward

Название цепочки правил

forward

Приоритет

0

Политика

Принять

Ok

Отмена

Рисунок 588 – Окно «Редактировать описание цепочки»

Для сохранения настроек необходимо нажать на кнопку **«Сохранить»**.
Правило фильтрации по умолчанию не отображает в таблице **«Описание правил»**.

6.7.4 Сценарий применения межсетевого экрана

6.8 Фильтрация доступа к устройству по протоколу https и ssh

На рисунке представлена схема сети, на которой устройство МКСЗ Горизонт-ВС, администратор сети и пользователи находятся в одном сегменте (Рисунок 589). Необходимо ограничить доступ к устройству МКСЗ Горизонт-ВС по протоколу https и ssh для всех пользователей, кроме администратора.

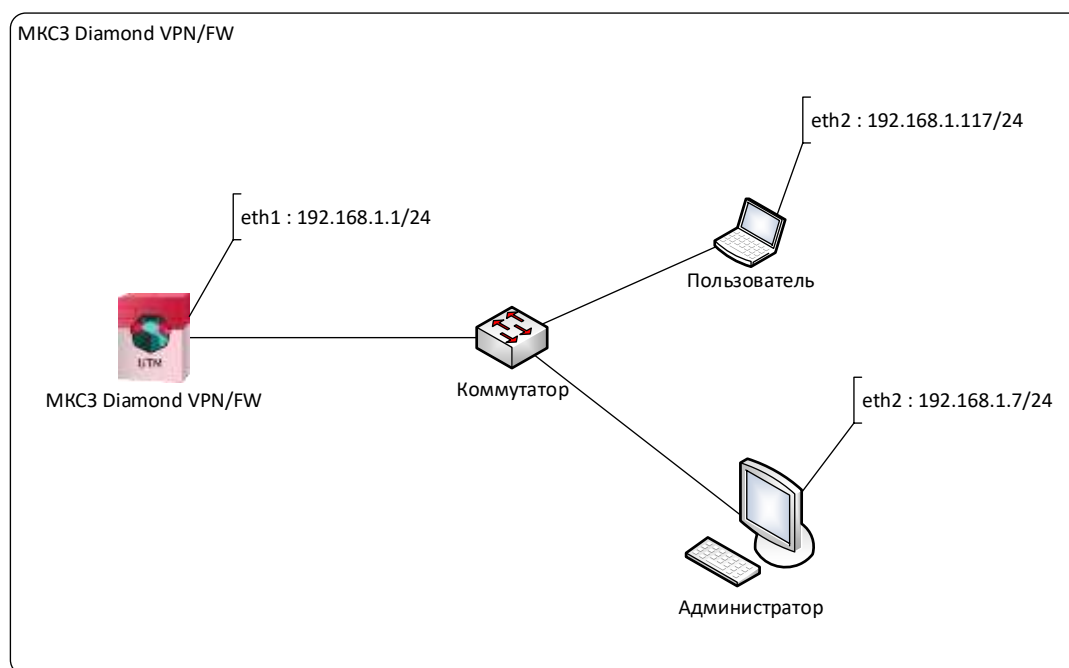


Рисунок 589 – Схема сети, где администратор сети и пользователи находятся в одном сегменте

Для настройки правила фильтрации для входящего и исходящего трафика необходимо добавить разрешающее правило для системного интерфейса **«I0»**.

Для настройки правила фильтрации для системного интерфейса **«I0»** необходимо в главном меню выбрать пункт **«Межсетевой экран»**. В таблице **«Локальные правила»** необходимо выбрать цепочку с правилами фильтрации

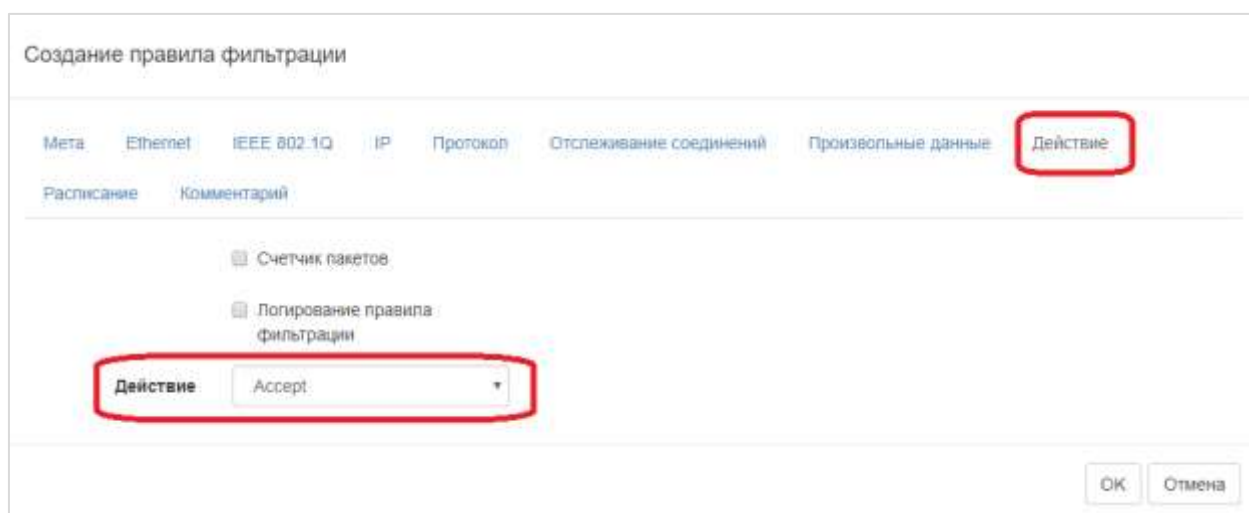


Рисунок 592 – Положение вкладки «Действие» и опции «Ассерпт»

После задания всех параметров необходимо нажать на кнопку «ОК», для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**» (Рисунок 593).

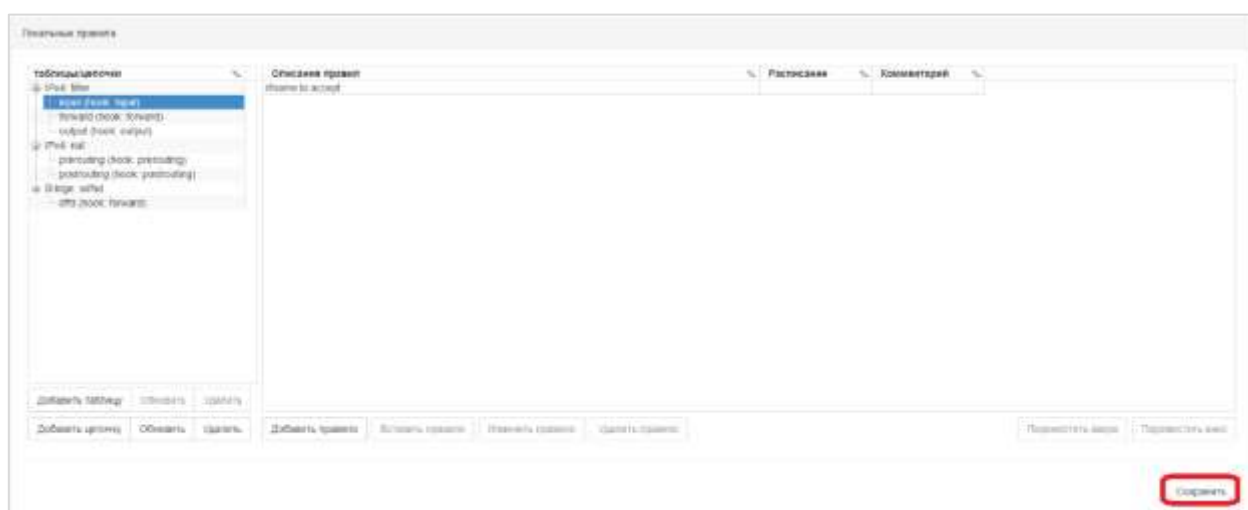


Рисунок 593 – Положение кнопки «Сохранить»

После создания правила фильтрации для системного интерфейса необходимо создать правило фильтрации для протокола https.

Для настройки правила фильтрации для протокола https или ssh необходимо в главном меню выбрать пункт «**Межсетевой экран**». В таблице «**Локальные правила**» необходимо выбрать цепочку с правилами фильтрации

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q **IP** Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола ip4

Фильтрация по источнику Другое

Адрес источника 192.168.11.7 маска подсети 255.255.255.255

Доменное имя источника

Фильтрация по назначению Другое

Адрес назначения 192.168.1.1 маска подсети 255.255.255.255

Доменное имя назначения

Метка DSCP N/A (0x00) Бит ECN Non-ECT (00)

Длина пакета от 0 по 0

Время жизни пакета (TTL) от 0 по 0

☐ Установлен бит фрагментация запрещена

☐ Установлен бит фрагментация разрешена

ОК Отмена

Рисунок 595 – Окно «Создание правил фильтрации» и положение вкладки «IP»

На вкладке «**Протокол**» в поле «**Протокол**» необходимо задать протокол «**TCP**», в поле «**Порт назначения**» необходимо задать порт номер 443 для протокола https

Рисунок 596

Рисунок 596 – Положение вкладки «Протокол»

На вкладке «**Отслеживание соединений**» необходимо установить флаг «**Новое соединение**», «**Установленное соединение**» и «**Связанное соединение**» (Рисунок 597).

Рисунок 597 – Положение флагов «Новое соединение», «Установленное соединение» и «Связанное соединение»

На вкладке «**Действие**» в поле «**Действие**» необходимо выбрать опцию «**Акцепт**» (Рисунок 598).

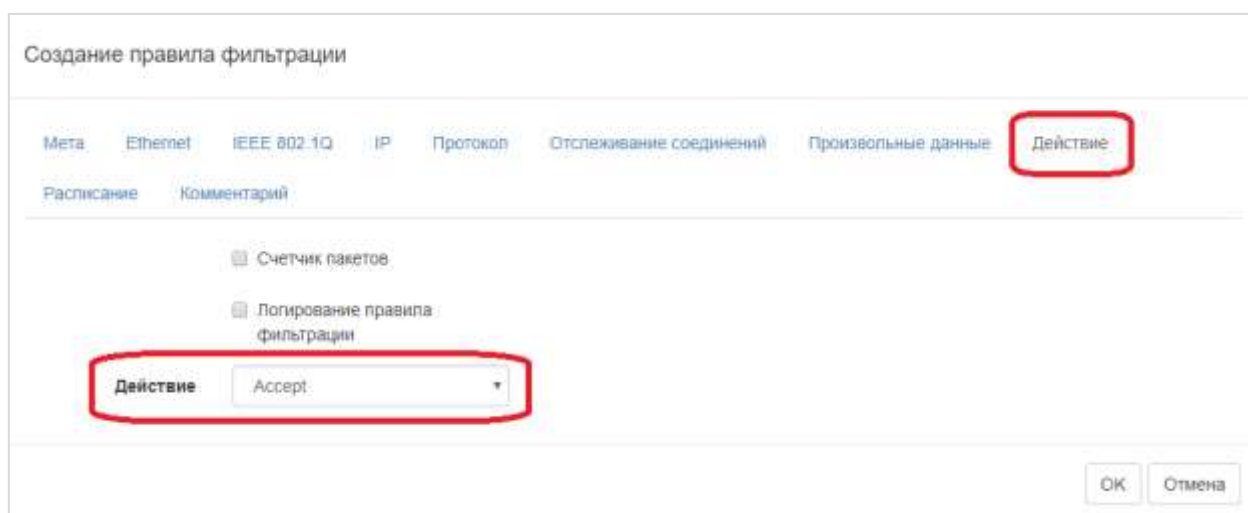


Рисунок 598 – Положение вкладки «Действие» и опции «Ассерти»

Чтобы проверить работу правила фильтрации можно использовать опцию **«Счетчик пакетов»** и **«Логирование правила фильтрации»**.

После задания все полей необходимо нажать на кнопку **«ОК»**, для сохранения правила фильтрации необходимо нажать на кнопку **«Сохранить»**.

Аналогичным образом необходимо создать правило фильтрации для протокола ssh – протокол TCP, сетевой порт назначения 22.



Рисунок 599 – Сохранение правил фильтрации

После задания разрешающих правил фильтрации необходимо создать запрещающее правило фильтрации для остального трафика.

Для создания запрещающего правила фильтрации необходимо в таблице «**Локальные правила**» необходимо выбрать цепочку с правилами фильтрации для входящего трафика «**input**» и нажать на кнопку «**Добавить правило**». На вкладке «**Действие**» в поле «**Действие**» необходимо выбрать действие «**Drop**» (Рисунок 600).

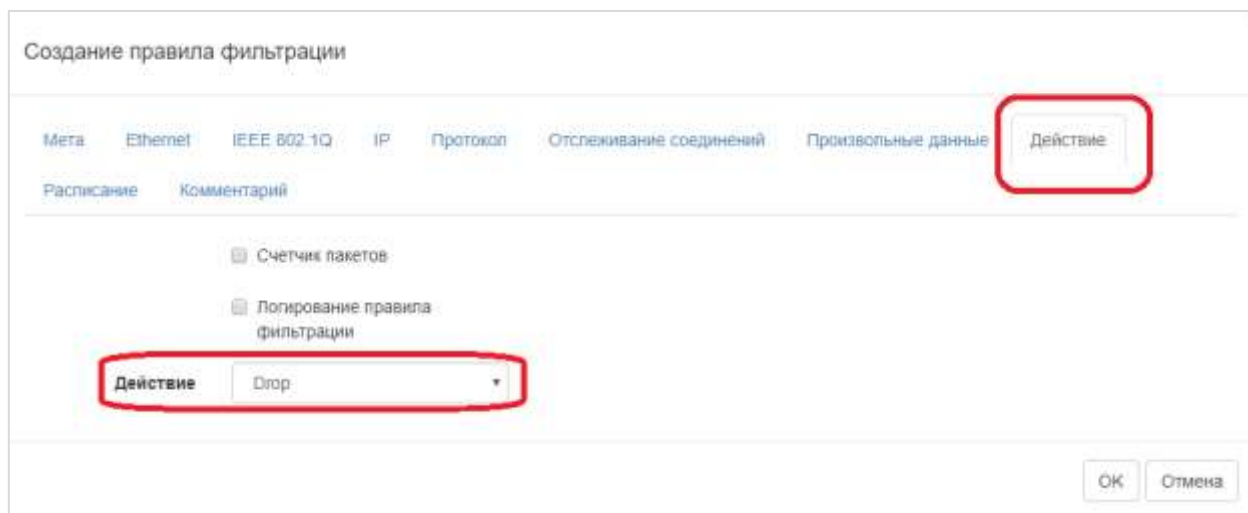


Рисунок 600 – Положение вкладки «Действие»

После задания все полей необходимо нажать на кнопку «**ОК**», для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**» (Рисунок 601).



Рисунок 601 – Сохранение правил фильтрации

Данный набор правил фильтрации разрешает сетевой трафик по протоколу https, ssh с рабочего места администратора с ip-адресом 192.168.1.7/32 к устройству МКС3 Горизонт-ВС с ip-адресом 192.168.1.1 и запрещает сетевой трафик к устройству МКС3 Горизонт-ВС от всех остальных рабочих мест.

6.9 Фильтрация защищенного соединения

При создании защищенного соединения одно устройство МКС3 Горизонт-ВС работает в режиме сервера и прослушивает сетевой порт на заданном сетевом интерфейсе. Второе устройство МКС3 Горизонт-ВС работает в режиме клиента инициализирует соединение на заданный адрес и сетевой порт (Рисунок 602).



Рисунок 602 – Схема фильтрации защищенного соединения

На сетевом интерфейсе «eth1» устройства МКС3 Горизонт-ВС, которое работает в режиме сервера, установлен ip-адрес 192.168.1.1. На сетевом интерфейсе «eth1» устройства МКС3 Горизонт-ВС, которое работает в режиме клиента, установлен ip-адрес 172.16.16.150/24. После установления защищенного соединения в логическом туннеле будет задана новая адресация. Для устройства МКС3 Горизонт-ВС, которое работает в режиме сервера, для логического интерфейса будет задан ip-адрес 10.10.10.1/24. Для

устройства, МКСЗ Горизонт-ВС, которое работает в режиме клиента, для логического интерфейса будет задан ip-адрес 10.10.10.2/24.

С помощью настроек необходимо реализовать сценарий, по которому на устройстве МКС3 Горизонт-ВС, которое работает в режиме сервера, будет настроено правило фильтрации, которое разрешает установление защищенного соединения от другого устройства МКС3 Горизонт-ВС и запрещает все новые соединения от других устройств.

Устройство МКС3 Горизонт-ВС – сервер прослушивает ip-адрес 192.168.1.1/24 и сетевой порт 12968 для протокола UDP.

Для создания разрешающего правила фильтрации для входящего соединения от устройства МКСЗ Горизонт-ВС – клиент необходимо в главном меню выбрать пункт «**Межсетевой экран**». Для добавления правила необходимо выбрать цепочку «input» и нажать на кнопку «**Добавить правило**» (Рисунок 603).



Рисунок 603 – Создание разрешающего правила фильтрации для входящего соединения

В новом окне «**Создание правила фильтрации**» на вкладке «**IP**» в поле «**Адрес источника**» необходимо задать ip-адрес 172.16.16.150, в поле маска подсети необходимо задать маску подсети 255.255.255.255, в поле

«Адрес назначения» необходимо задать ip-адрес 192.168.1.1, в поле маска подсети необходимо задать маску подсети 255.255.255.255 (Рисунок 604).

Создание правила фильтрации

Мета: Ethernet IEEE 802.1Q IP **Протокол** Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола: ip4

Фильтрация по источнику: Другое

Адрес источника: 172.16.16.150 маска подсети: 255.255.255.255

Доменное имя источника:

Фильтрация по назначению: Другое

Адрес назначения: 192.168.1.1 маска подсети: 255.255.255.255

Доменное имя назначения:

Метка DSCP: N/A (0x00) Бит ECN: Non-ECT (00)

Длина пакета от: 0 по: 0

Время жизни пакета (TTL) от: 0 по: 0

☐ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

OK Отмена

Рисунок 604 – Окно «Создание правила фильтрации»

На вкладке «Протокол» в поле «Протокол» необходимо выбрать протокол UDP, в поле «Порт назначения» необходимо задать сетевой порт 12968 (Рисунок 605).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP **Протокол** Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Протокол: UDP (17)

Параметры UDP:

Порт источника с: 0 по: 0

Порт назначения с: 12968 по: 12968

OK Отмена

Рисунок 605 – Настройка вкладки «Протокол»

На вкладке «**Отслеживание соединений**» необходимо установить флаг «**Новое соединение**», «**Установленное соединение**» и «**Связанное соединение**» (Рисунок 606).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP Протокол **Отслеживание соединений** Произвольные данные Действие

Расписание Комментарий

☒ Новое соединение

☒ Установленное соединение

☒ Связанное соединение

OK Отмена

Рисунок 606 – Положение флагов «Новое соединение», «Установленное соединение» и «Связанное соединение»

На вкладке «**Действие**» в поле «**Действие**» необходимо выбрать действие «**Асепт**» (Рисунок 607).

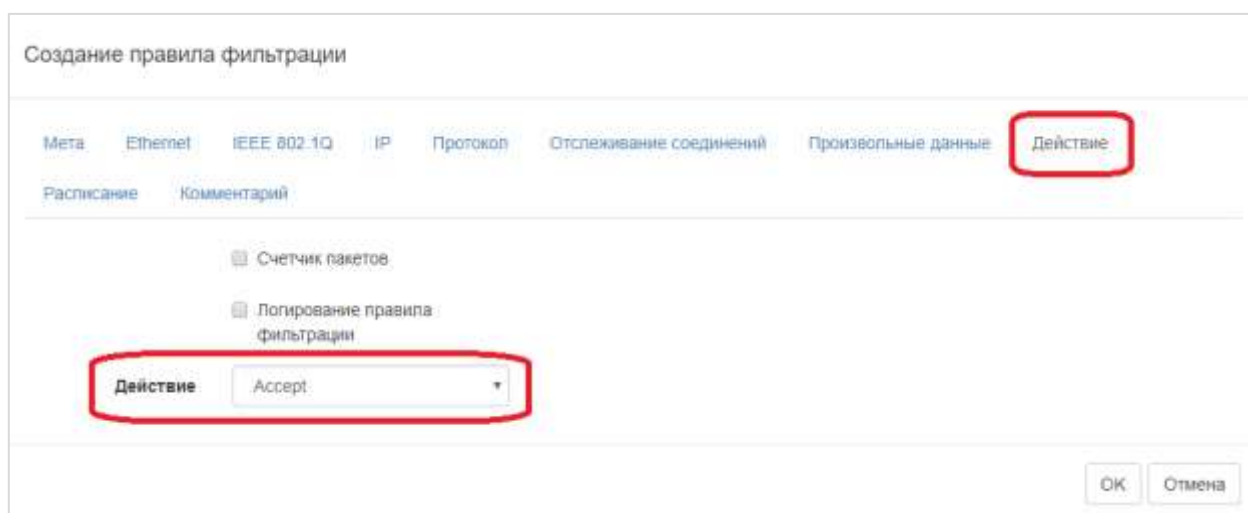


Рисунок 607 – Положение вкладки «Действие»

После задания всех параметров необходимо нажать на кнопку «**ОК**», для сохранения настроек необходимо нажать на кнопку «**Сохранить**» (Рисунок 608).



Рисунок 608 – Сохранение настроек

Чтобы проверить работу правила фильтрации можно использовать опцию «**Счетчик пакетов**» и «**Логирование правила фильтрации**».

После задания разрешающего правила фильтрации необходимо создать запрещающее правило фильтрации для остального трафика.

Для создания запрещающего правила фильтрации необходимо в таблице «**Локальные правила**» необходимо выбрать цепочку с правилами

фильтрации для входящего трафика «**input**» и нажать на кнопку «**Добавить правило**». На вкладке «**Действие**» в поле «**Действие**» необходимо выбрать действие «**Drop**» (Рисунок 609).

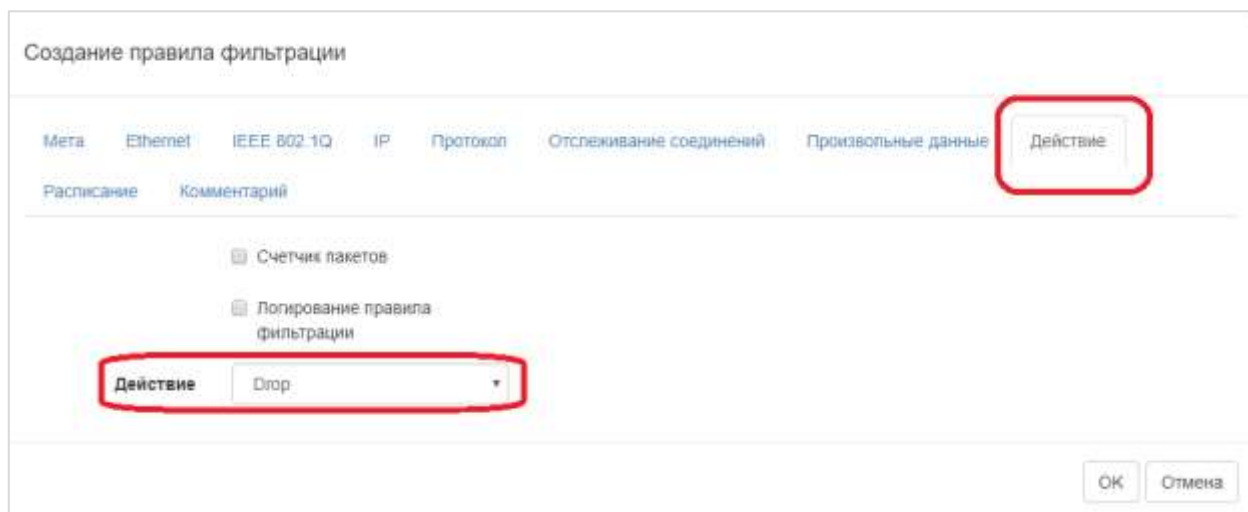


Рисунок 609 – Положение вкладки «Действие»

После задания все полей необходимо нажать на кнопку «**ОК**», для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**» (Рисунок 610).



Рисунок 610 – Сохранение правил фильтрации

Данный набор правил фильтрации разрешает сетевой трафик по протоколу UDP на порт номер 12968 с устройства МКС3 Горизонт-ВС с ip-

адресом 172.16.16.150/32 к устройству МКС3 Горизонт-ВС с ip-адресом 192.168.1.1/32 и запрещает весь сетевой трафик для остальных устройств.

9.3 Фильтрация по IP-адресу

С помощью настроек необходимо реализовать сценарий, по которому на устройстве МКС3 Горизонт-ВС, будет настроено правило фильтрации, которое запрещает весь трафик с устройства с ip-адресом 192.168.16.14/24 на устройство с ip-адресом 172.16.16.150/24 (Рисунок 611).

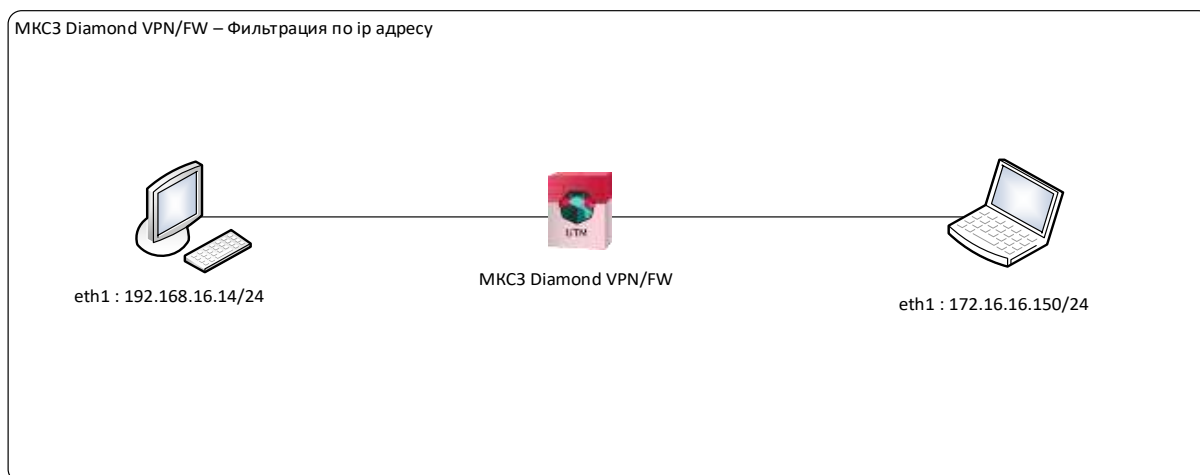


Рисунок 611 – Схема фильтрации по ip-адресу

Для создания правила фильтрации необходимо в главном меню выбрать пункт «Межсетевой экран», в окне «Локальные правила» необходимо выбрать цепочку «Forward» (Рисунок 612).



Рисунок 612 – Создание правила фильтрации

Для добавления правила фильтрации необходимо нажать на кнопку **«Добавить правило»**. В новом окне на вкладке **«IP»** в поле **«Адрес источника»** необходимо задать ip-адрес источника сетевого трафика 192.168.16.14, в поле маска подсети необходимо задать маску подсети 255.255.255.255, в поле **«Адрес назначения»** необходимо задать ip-адрес назначения сетевого трафика 172.16.16.150, в поле маска подсети необходимо задать маску подсети 255.255.255.255 (Рисунок 613).

Создание правила фильтрации

Meta Ethernet IEEE 802.1Q IP Протокол Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Версия протокола: ip4 *

Фильтрация по источнику: Другое *

Адрес источника: 192.168.16.14 маска подсети: 255.255.255.255

Доменное имя источника:

Фильтрация по назначению: Другое *

Адрес назначения: 172.16.16.150 маска подсети: 255.255.255.255

Доменное имя назначения:

Метка DSCP: N/A (0x00) Бит ECN: Non-ECT (00) *

Длина пакета от: 0 по: 0

Время жизни пакета (TTL) от: 0 по: 0

☐ Установлен бит Фрагментация запрещена

☐ Установлен бит Фрагментация разрешена

OK Отмена

Рисунок 613 – Окно «Создание правила фильтрации»

На вкладке «Действие» в поле «Действие» необходимо выбрать действие «**Drop**» (Рисунок 614).

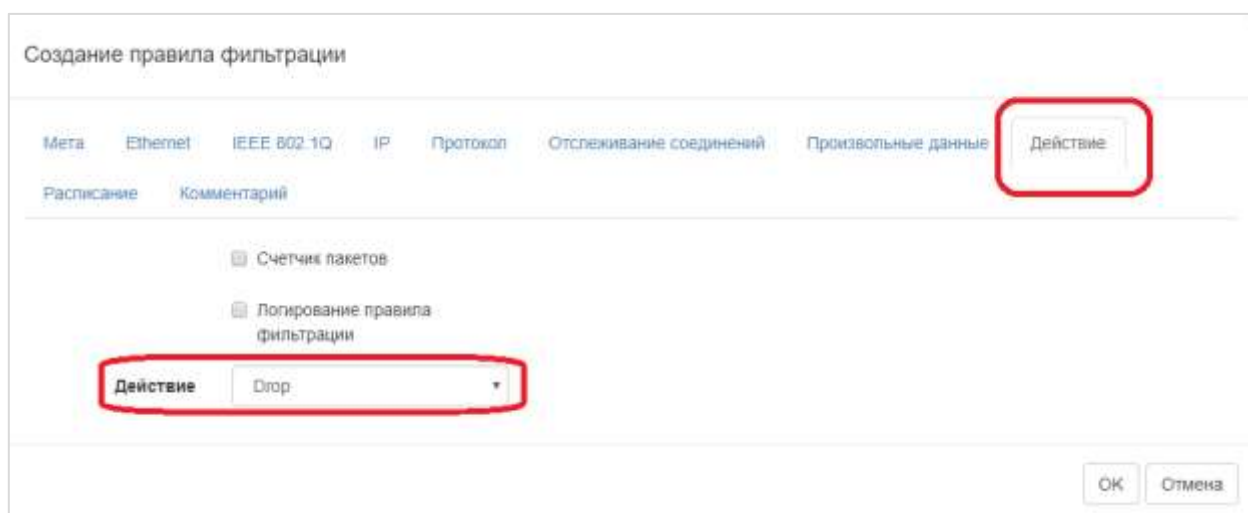


Рисунок 614 – Положение вкладки «Действие»

Чтобы проверить работу правила фильтрации можно использовать опцию «**Счетчик пакетов**» и «**Логирование правила фильтрации**».

После задания всех полей необходимо нажать на кнопку «**ОК**», для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**» (Рисунок 615).



Рисунок 615 – Сохранение правил фильтрации

Данное правило фильтрации запрещает весь сетевой трафик с устройства с ip-адресом 192.168.16.14/32 к устройству с ip-адресом 172.16.16.150/32.

9.4 Фильтрация протокола UDP

С помощью настроек необходимо реализовать сценарий, по которому на устройстве МКСЗ Горизонт-ВС, будет настроено запрещающее правило фильтрации для протокола UDP (Рисунок 616616).

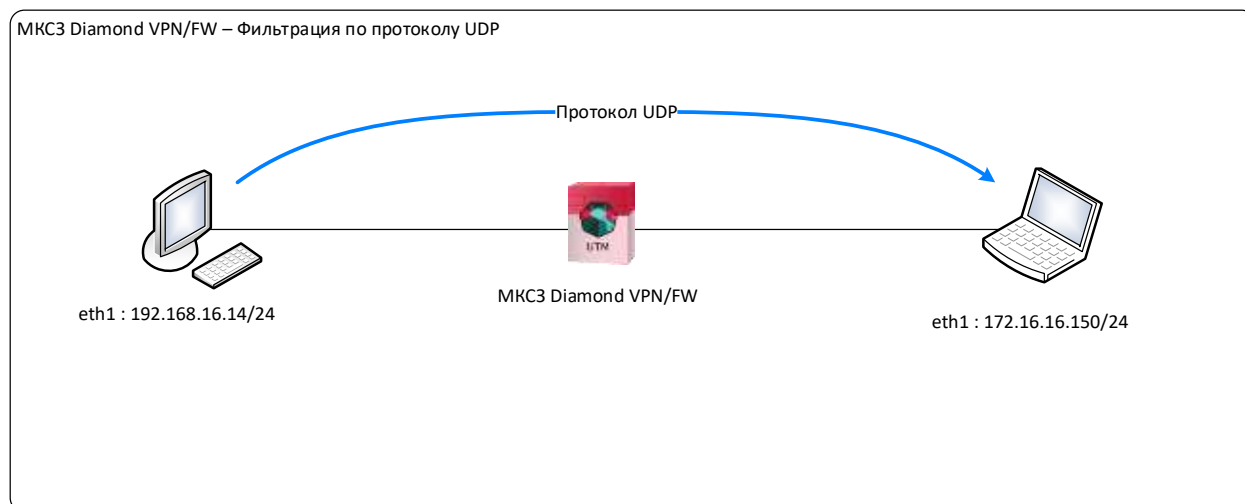


Рисунок 616 – Схема фільтрації по протоколу UDP

Для создания правила фильтрации необходимо в главном меню выбрать пункт «**Межсетевой экран**», в окне «**Локальные правила**» необходимо выбрать цепочку «**Forward**» (Рисунок 617).



Рисунок 617 – Создание правил фильтрации

Для добавления правила фильтрации необходимо нажать на кнопку «Добавить правило». В новом окне на вкладке «Протокол» в поле «Протокол» необходимо выбрать протокол UDP (618). При выборе типа протокола будут доступны дополнительные опции, которые поддерживает протокол. Для протокола UDP доступны следующие опции: сетевой порт источника и сетевой порт назначения.

The screenshot shows the 'Создание правила фильтрации' (Create Filter Rule) dialog box with the 'Протокол' (Protocol) tab selected. The 'Протокол' (Protocol) dropdown menu is set to 'UDP (17)'. Below it, the 'Параметры UDP:' (UDP Parameters) section contains two rows of port selection fields. The first row is for 'Порт источника с' (Source port from) and 'по' (to), both set to '0'. The second row is for 'Порт назначения с' (Destination port from) and 'по' (to), both set to '0'. At the bottom right, there are 'ОК' (OK) and 'Отмена' (Cancel) buttons.

Рисунок 618 – Добавление правил фильтрации

На вкладке «Действие» в поле «Действие» необходимо выбрать действие «Drop» (Рисунок 619).

The screenshot shows the 'Создание правила фильтрации' (Create Filter Rule) dialog box with the 'Действие' (Action) tab selected. The 'Действие' (Action) dropdown menu is set to 'Drop'. Above this, there are two checkboxes: 'Счетчик пакетов' (Packet counter) and 'Логирование правила фильтрации' (Logging of filter rule), both of which are unchecked. At the bottom right, there are 'ОК' (OK) and 'Отмена' (Cancel) buttons. Red rectangles highlight the 'Действие' tab and the 'Действие' dropdown menu.

Рисунок 619 – Положение поля «Действие»

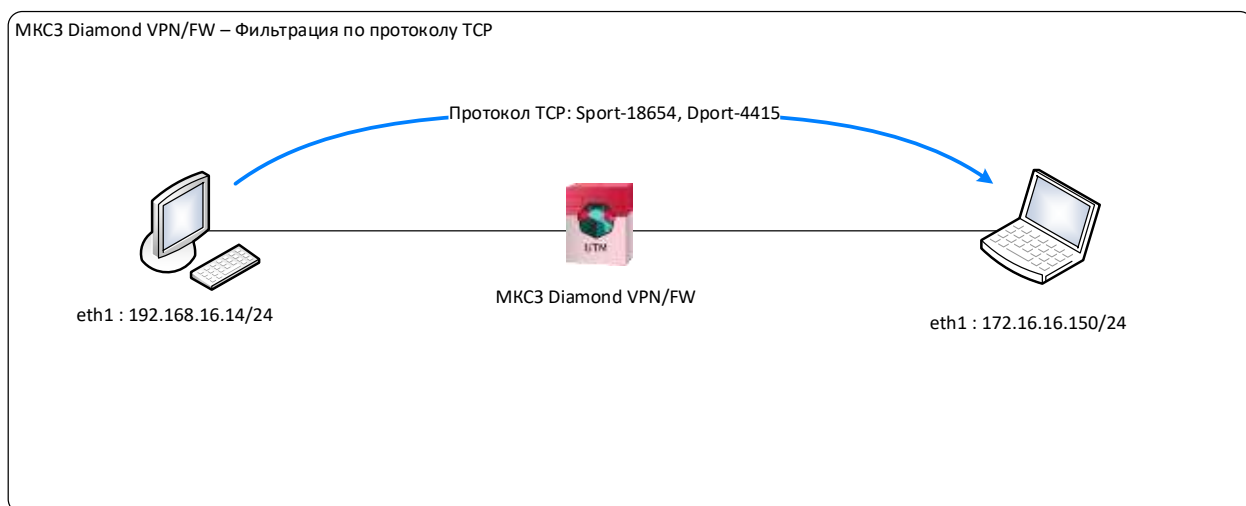


Рисунок 621 – Схема фильтрации по протоколу TCP

Для создания правила фильтрации необходимо в главном меню выбрать пункт **«Межсетевой экран»**, в окне **«Локальные правила»** необходимо выбрать цепочку **«Forward»** (Рисунок 622622).



Рисунок 622 – Создание правила фильтрации

Для добавления правила фильтрации необходимо нажать на кнопку **«Добавить правило»**. В новом окне на вкладке **«Протокол»** в поле **«Протокол»** необходимо выбрать протокол TCP, в поле **«Порт источника»** необходимо задать порт 18654, в поле **«Порт назначения»** необходимо задать 4415 порт, в поле **«Флаги»** необходимо установить флаг **«syn»**. При выборе типа протокола будут доступны дополнительные опции, которые поддерживает протокол. Для

протокола TCP доступны следующие опции: сетевой порт источника и сетевой порт назначения (Рисунок 623).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP **Протокол** Отслеживание соединений Произвольные данные Действие

Расписание Комментарий

Протокол TCP (6)

Параметры TCP

Порт источника с 18654 по 18654

Порт назначения с 4415 по 4415

Флаги ☐ fin ☒ syn ☐ rst ☐ psh ☐ ack ☐ urg ☐ ecn ☐ cwr

OK Отмена

Рисунок 623

На вкладке «**Действие**» в поле «**Действие**» необходимо выбрать действие «**Drop**» (Рисунок 624).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP Протокол Отслеживание соединений Произвольные данные **Действие**

Расписание Комментарий

☐ Счетчик пакетов

☐ Логирование правила фильтрации

Действие Drop

OK Отмена

Рисунок 624 – Положение вкладки «Действие»

Чтобы проверить работу правила фильтрации можно использовать опцию «**Счетчик пакетов**» и «**Логирование правила фильтрации**».

После задания всех полей необходимо нажать на кнопку «**ОК**», для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**» (Рисунок 625).

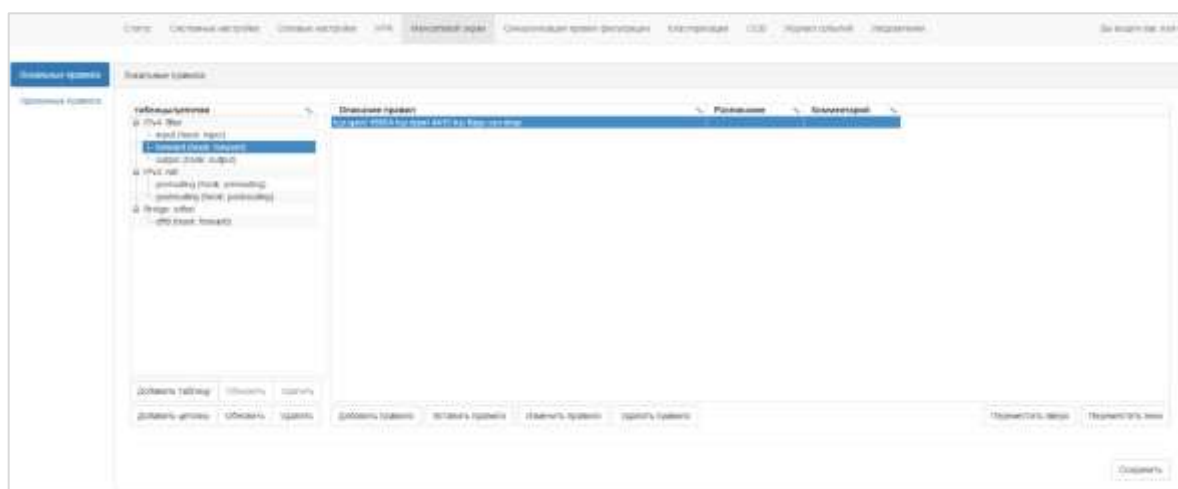


Рисунок 625 – Сохранение правила фильтрации

Данное правило фильтрации запрещает сетевой трафик по протоколу TCP с порта 18654 на порт 4415 с установленным битом «syn» с устройства с ip-адресом 192.168.16.14/32 к устройству с ip-адресом 172.16.16.150/32.

9.6 Фильтрация по расписанию.

С помощью настроек необходимо реализовать сценарий, по которому на устройстве МКС3 Горизонт-ВС, будет настроено правило фильтрации, которое запрещает трафик для протокола TCP на порт 80 с ip-адресом 192.168.16.14/24 к устройству с IP-адресом 172.16.16.150/24 с 9 до 18 часов по будням (Рисунок 626626).

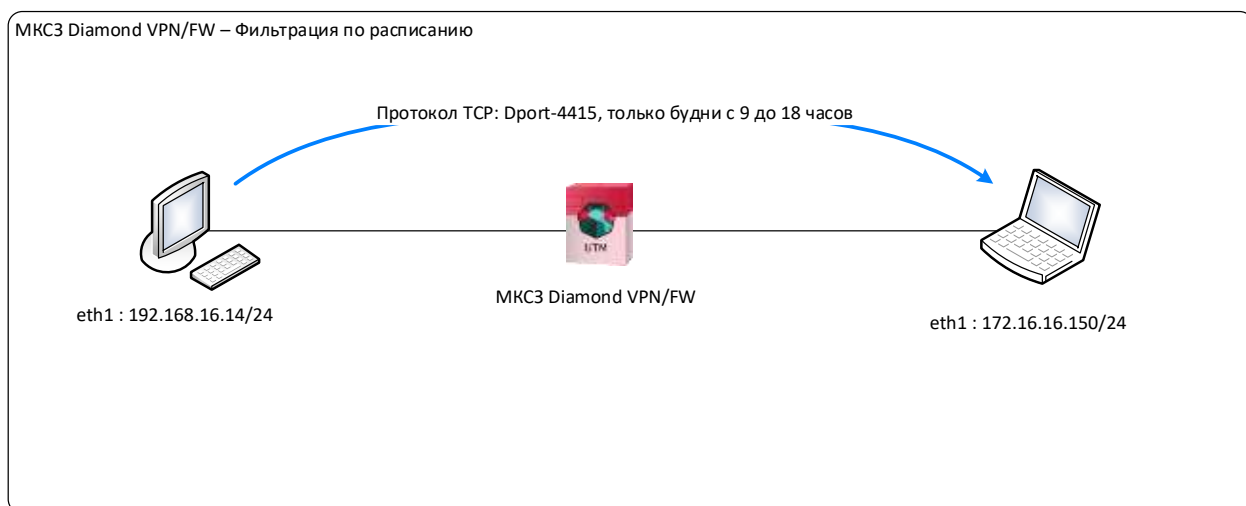


Рисунок 626 – Схема фильтрации по расписанию

Для создания правила фильтрации необходимо в главном меню выбрать пункт «**Межсетевой экран**», в окне «**Локальные правила**» необходимо выбрать цепочку «**Forward**» (Рисунок 627).



Рисунок 627 – Создание правила фильтрации

Для добавления правила фильтрации необходимо нажать на кнопку «**Добавить правило**». В новом окне на вкладке «**Протокол**» в поле «**Протокол**» необходимо выбрать протокол TCP, в поле «**Порт назначения**» необходимо задать 80 порт. На вкладке «**Расписание**» необходимо создать расписание для правила фильтрации. Для создания расписание необходимо нажать на кнопку «**Добавить расписание**» (Рисунок 628628).

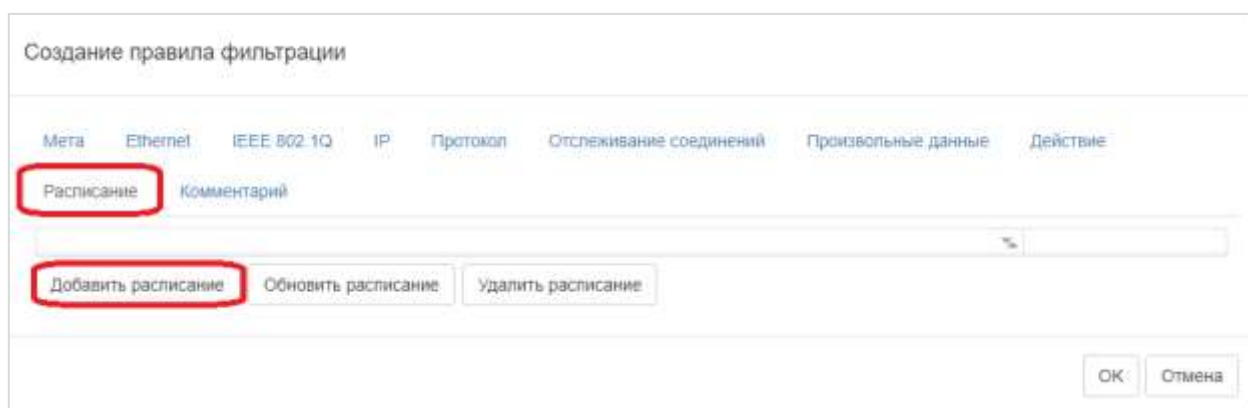


Рисунок 628 – Положение вкладки «Расписание» и кнопки «Добавить расписание»

В новом окне необходимо установить флаг **«Часы диапазон»**, в поле **«Часы»** необходимо задать время работы правила фильтрации и задать дни недели (Рисунок 629).

Рисунок 629 – Настройка расписания

После задания расписания его можно изменить или удалить с помощью дополнительных кнопок **«Обновить расписание»** и **«Удалить расписание»** (Рисунок 630630).

Рисунок 630 – Вкладка «Расписание»

На вкладке «**Действие**» в поле «**Действие**» необходимо выбрать действие «**Drop**» (Рисунок 631).

Рисунок 631 – Положение вкладки «Действие»

Чтобы проверить работу правила фильтрации можно использовать опцию «**Счетчик пакетов**» и «**Логиrowание правила фильтрации**».

После задания всех полей необходимо нажать на кнопку «ОК», для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**» (Рисунок 632).

задать префикс, который будет закреплен за данным правилом, в поле «**Действие**» необходимо выбрать действие «**Drop**» (Рисунок 635).

Создание правила фильтрации

Мета Ethernet IEEE 802.1Q IP Протокол Отслеживание соединений Произвольные данные **Действие**

Расписание Комментарий

☐ Счетчик пакетов

☒ Логирование правила фильтрации

Префикс TCP_s_18654_d_4415

Действие Drop

ОК Отмена

Рисунок 635 – Положение вкладки «Действие» и кнопки «Логирование правила фильтрации»

Чтобы проверить работу правила фильтрации можно использовать опцию «**Счетчик пакетов**». После задания всех полей необходимо нажать на кнопку «**ОК**», для сохранения правила фильтрации необходимо нажать на кнопку «**Сохранить**» (Рисунок 636636).

Правила фильтрации

Правила

Добавить правило Изменить правило Удалить правило

Рисунок 636 – Сохранение правила фильтрации

Данное правило фильтрации разрешает сетевой трафик для протокола TCP с порта 18654 на порт 4415 и запрещает весь остальной трафик. При срабатывании запрещающего правила фильтрации устройство регистрирует все сетевые пакеты в журнале событий.

Для просмотра журнала событий для межсетевого экрана необходимо в главном меню выбрать пункт «Журнал событий – Журнал межсетевого экрана» (Рисунок 637).



Рисунок 637 – Просмотр «Журнала событий»

9.8 Фильтрация на уровне L2 в таблице Bridge

С помощью настроек необходимо реализовать сценарий, по которому на устройстве MKC3 Горизонт-ВС будет настроено правило фильтрации для второго уровня стандартной сетевой модели. Сетевой трафик на втором уровне стандартной сетевой модели не участвует в процессе маршрутизации и в сетевых пакетах не происходит подмены MAC адресов. Для сторонних устройств MKC3 Горизонт-ВС будет прозрачным (Рисунок 638).

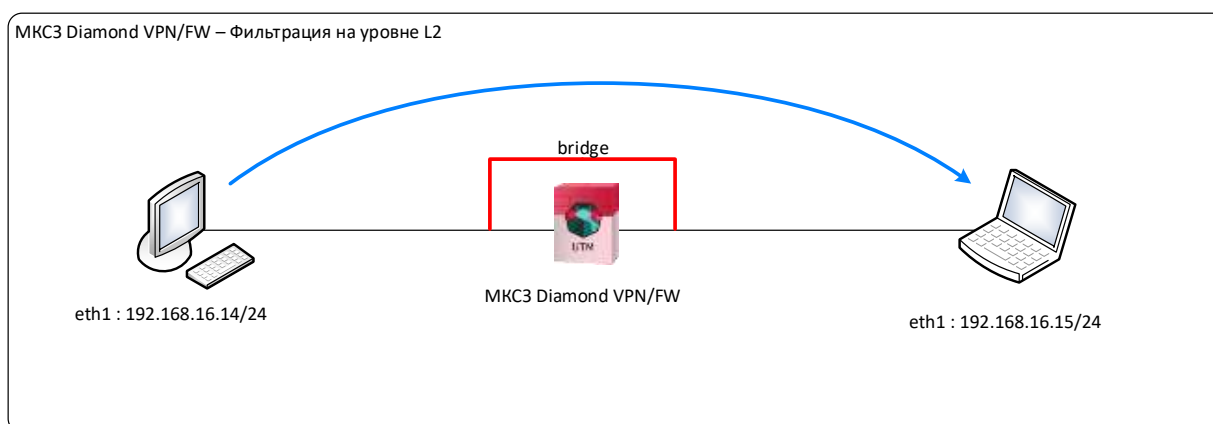


Рисунок 638 – Схема фильтрации на уровне L2

Для создания правила фильтрации на уровне L2 стандартной сетевой модели необходимо в главном меню выбрать пункт «Межсетевой экран – Локальные правила». В таблице «Локальные правила» необходимо нажать на кнопку «Добавить таблицу» (Рисунок 639).

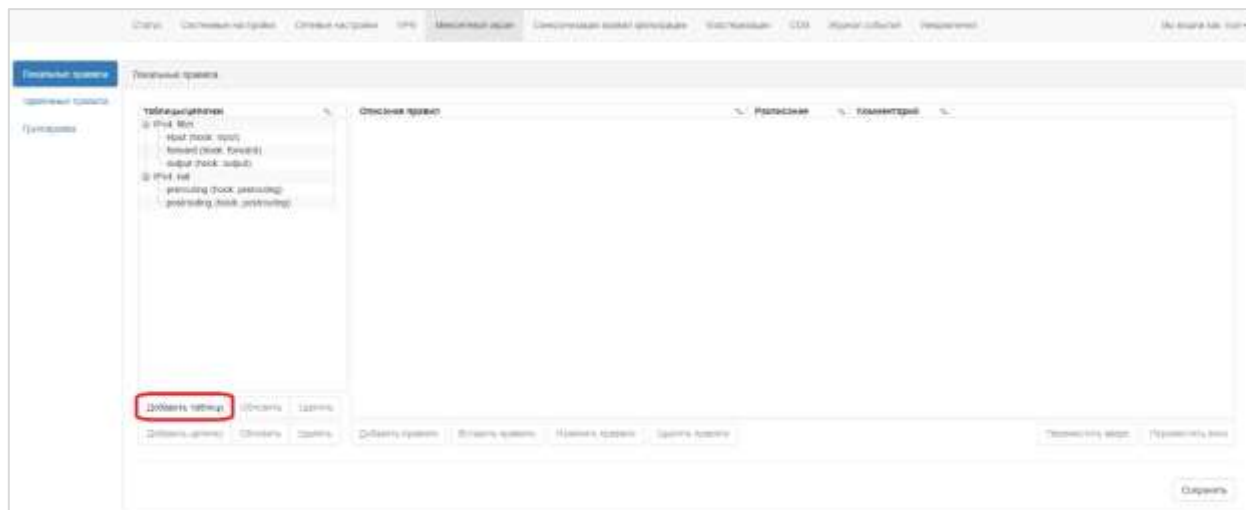


Рисунок 639 – Положение кнопки «Добавить таблицу»

В новом окне «Добавить таблицу» в поле «Тип таблицы» необходимо выбрать пункт «**bridge**», в поле «Название таблицы» необходимо задать название таблицы – «**bridge**» (Рисунок 640).

The image shows the 'Add Table' dialog box. It has a title bar 'Добавить таблицу'. Below it, there is a 'Тип таблицы' (Type of table) dropdown menu with 'bridge' selected. Below that is a 'Название таблицы' (Table name) text input field containing 'bridge'. At the bottom, there are 'Ok' and 'Отмена' (Cancel) buttons.

Рисунок 640 – Окно «Добавить таблицу»

Далее необходимо выбрать новую таблицу «**bridge**» и создать в ней цепочку для правил фильтрации. Для создания новой цепочки правил фильтрации необходимо нажать на кнопку «**Добавить цепочку**» (Рисунок 641641).

Рисунок 641 – Кнопка «Добавить цепочку»

Рисунок 642 – Окно добавить цепочку

После создания цепочки с типом «**forward**» необходимо создать правила фильтрации. Для создания правила фильтрации необходимо выбрать цепочку «**forward**» в таблице «**bridge**» и нажать на кнопку «**Добавить правило**» (Рисунок 543643).

Рисунок 643 – Создание правил фильтрации

В новом окне необходимо задать параметры фильтрации и нажать на кнопку «**ОК**». Для примера, создано запрещающее правило фильтрации для протокола ICMP (Рисунок 644).

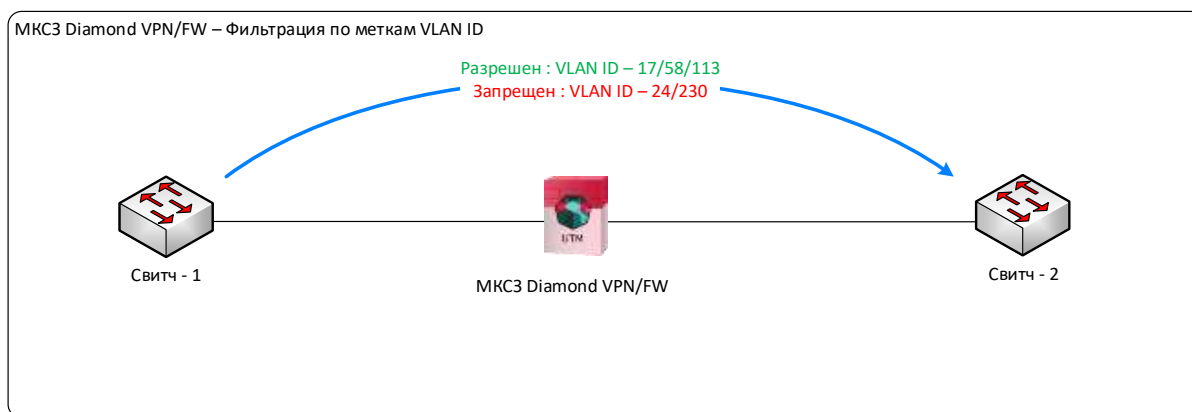


Рисунок 645 – Схема фильтрации по меткам VLAN ID

Для создания правила фильтрации для метки VLAN ID необходимо в главном меню выбрать пункт **«Межсетевой экран – Локальные правила»**. В таблице «Локальные правила» необходимо нажать на кнопку **«Добавить таблицу»** (Рисунок 546).

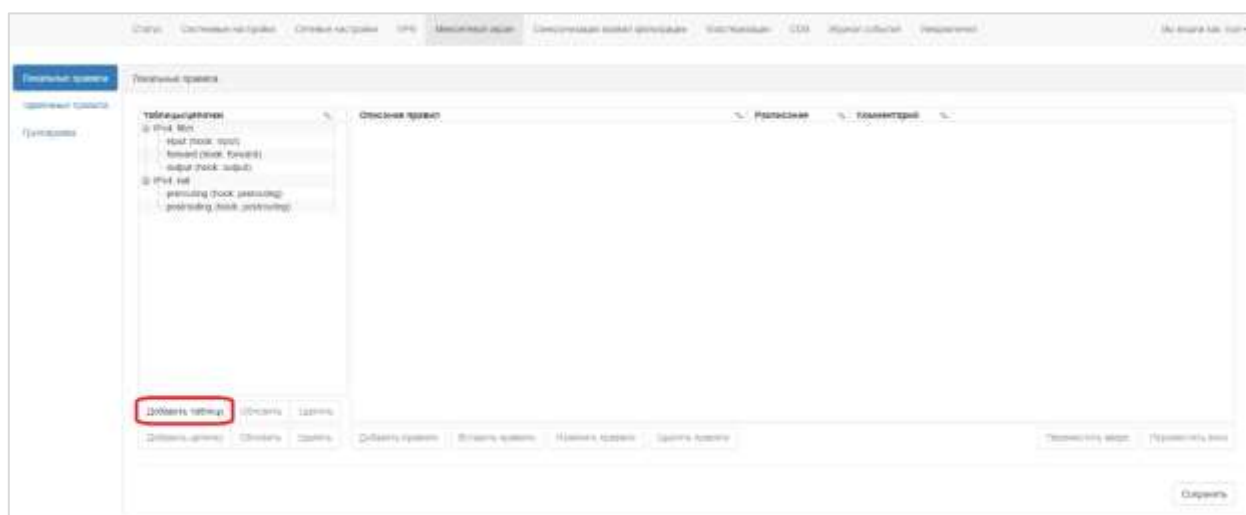


Рисунок 646 – Положение кнопки «Добавить таблицу»

В новом окне **«Добавить таблицу»** в поле **«Тип таблицы»** необходимо выбрать пункт **«bridge»**, в поле **«Название таблицы»** необходимо задать название таблицы – **«bridge»** (Рисунок 647).

Рисунок 647 – Окно «Добавить таблицу»

Далее необходимо выбрать новую таблицу «**bridge**» и создать в ней цепочку для правил фильтрации. Для создания новой цепочки правил фильтрации необходимо нажать на кнопку «**Добавить цепочку**» (Рисунок 648648).



Рисунок 648 – Положение кнопки «Добавить цепочку»

В новом окне «**Добавить цепочку**» в поле «**Тип цепочки правил**» необходимо выбрать тип «**forward**» для транзитного трафика, в поле «**Название цепочки правил**» необходимо задать название – «**forward**» и нажать на кнопку «**ОК**» (

).

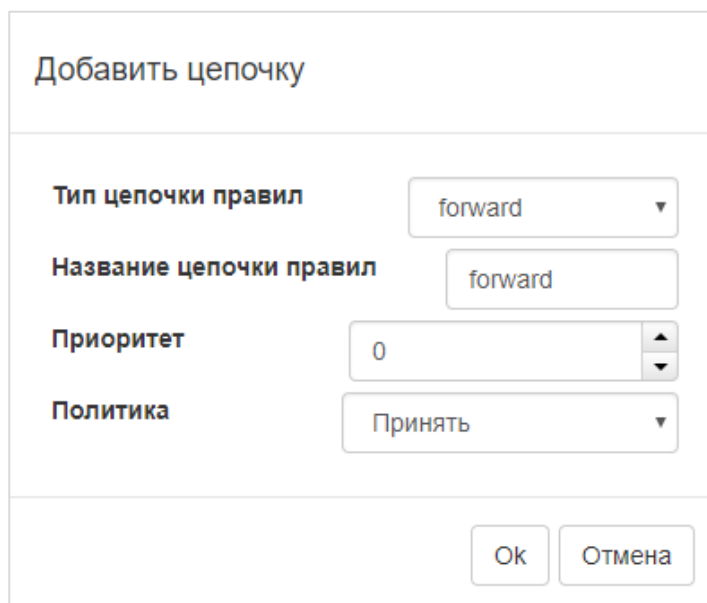


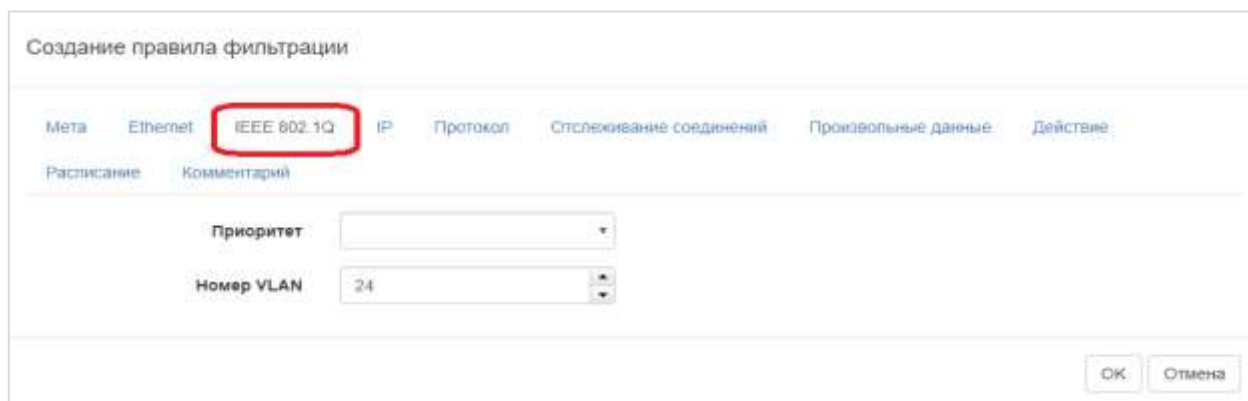
Рисунок 649 – Окно «Добавить цепочку»

После создания цепочки с типом «**forward**» необходимо создать правила фильтрации для метки VLAN ID. Для создания запрещающего правила фильтрации для метки VLAN ID 24 и 230 необходимо выбрать цепочку «**forward**» в таблице «**bridge**» и нажать на кнопку «**Добавить правило**» (650).



Рисунок 650 – Создание правила фильтрации

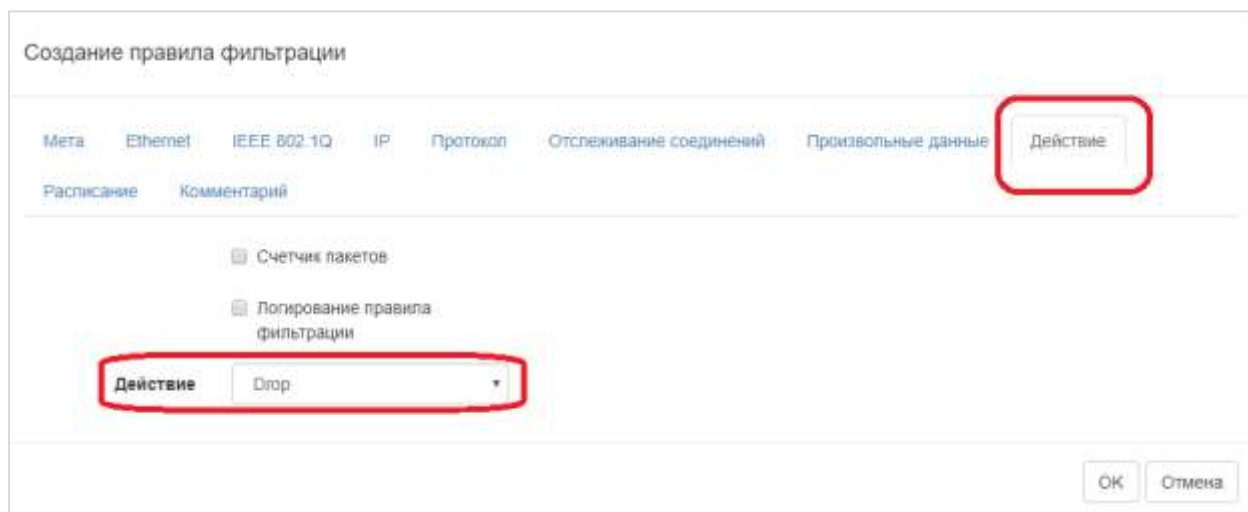
В новом окне на вкладке «**IEEE 802.1Q**» в поле «**Номер VLAN**» необходимо задать номер VLAN ID 24 (Рисунок 651).



The screenshot shows the 'Создание правила фильтрации' (Create filtering rule) window. The 'IEEE 802.1Q' tab is selected and highlighted with a red rectangle. Below the tabs, the 'Номер VLAN' (VLAN ID) field is set to 24. Other tabs include 'Мета', 'Ethernet', 'IP', 'Протокол', 'Отслеживание соединений', 'Произвольные данные', 'Действие', 'Расписание', and 'Комментарий'. At the bottom right are 'ОК' and 'Отмена' buttons.

Рисунок 651 – Положение вкладки «IEEE 802.1Q»

На вкладке «**Действие**» в поле «**Действие**» необходимо задать «**Drop**» (Рисунок 652).



The screenshot shows the 'Создание правила фильтрации' (Create filtering rule) window with the 'Действие' (Action) tab selected and highlighted with a red rectangle. In the 'Действие' field, 'Drop' is selected. Other tabs include 'Мета', 'Ethernet', 'IEEE 802.1Q', 'IP', 'Протокол', 'Отслеживание соединений', 'Произвольные данные', 'Действие', 'Расписание', and 'Комментарий'. Below the tabs, there are checkboxes for 'Счетчик пакетов' and 'Логирование правила фильтрации'. At the bottom right are 'ОК' and 'Отмена' buttons.

Рисунок 652 – Положение вкладки «Действие»

После задания параметров фильтрации необходимо нажать на кнопку «**ОК**». Для сохранения правил фильтрации необходимо нажать на кнопку «**Сохранить**» (Рисунок 653).

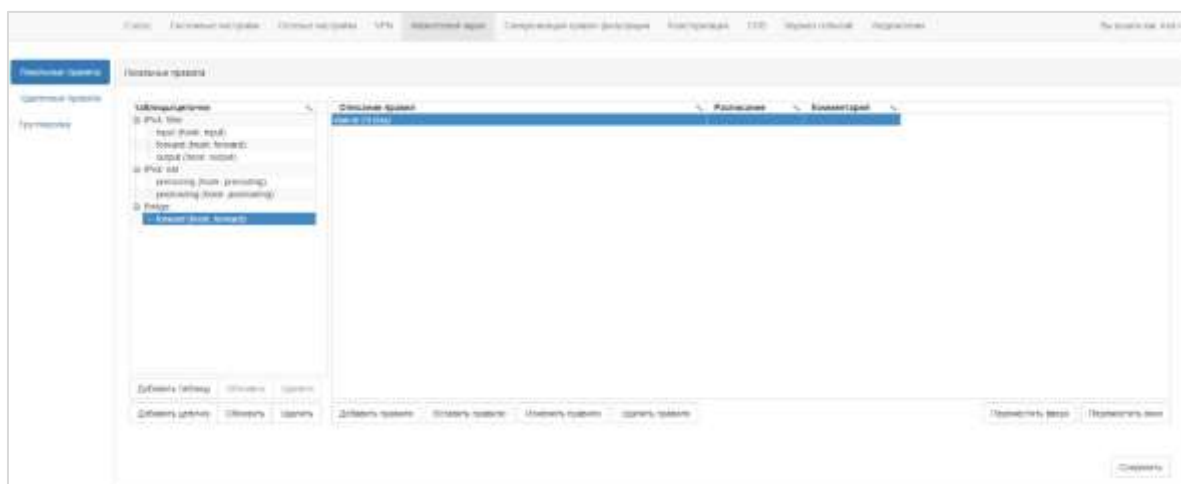


Рисунок 653 – Сохранение правила фильтрации

Аналогичным образом необходимо создать запрещающее правило фильтрации для метки VLAN ID 230 и разрешающее правило фильтрации для метки VLAN ID 17, 58 и 113 (Рисунок 654).

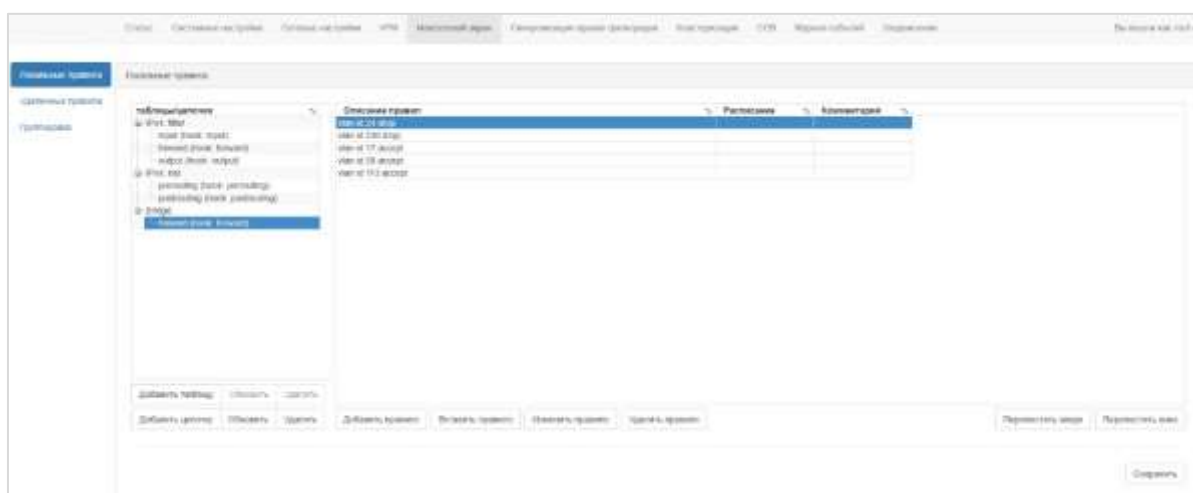


Рисунок 654 – Разрешающее правило фильтрации для метки VLAN ID 17, 58 и 113

6.8 Аварийные ситуации

Список сообщений об ошибках, выдаваемых пользователю, и рекомендации по устранению неисправности, 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 <i>'IPадрес сервера'</i>	1 По данному IP-адресу отсутствует сервер. 2 Отсутствует подключение терминала к локальной вычислительной сети (ЛВС)
2	Ошибка сервера <i>'IP-адрес сервера'</i> . Виртуальная машина <i>'Название VM'</i> не найдена	На сервере с данным IP-адресом отсутствует указанная виртуальная машина
3	Ошибка сервера <i>'IP-адрес сервера'</i> . Ошибка конфигурации виртуальной машины <i>'Название VM'</i>	1 В настройках конфигурации VM произошла ошибка. 2 При настройке VM неправильно сконфигурирован графический сервер Spice. Следует настроить Spice согласно настоящему руководству администратора

4	Ошибка сервера ' <i>IP-адрес сервера</i> '. Доступ к виртуальной машине ' <i>Название ВМ</i> ' запрещен администратором сервера	Неправильно настроен графический сервер Spice. Следует настроить Spice согласно настоящему руководству администратора
5	Ошибка сервера ' <i>IP-адрес сервера</i> '. Ошибка запуска виртуальной машины ' <i>Название ВМ</i> '	Потерян образ виртуальной машины
6	Неизвестный ключ или неавторизованный пользователь. Компьютер будет отключен	1 Ошибка работы с платой МИиКДС. 2 Ошибка в конфигурационном файле

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 предприятием-изготовителем.

7. Введение в ПК “Защищенный проксирующий сервер управления виртуальной инфраструктурой”

7.1 Структура ПК “Защищенный проксирующий сервер управления виртуальной инфраструктурой”

ПК “Защищенный проксирующий сервер управления виртуальной инфраструктурой” состоит из следующих компонентов:

- Виртуальная машина (ВМ), развернутая в ПК «Звезда»;
- Установленная в ВМ гостевая операционная система (ОС) Альт Рабочая станция 10 с развернутыми в ней пакетами:
 - Alterator-squid – модуль для конфигурирования прокси сервера Squid;
 - alterator-squidmill – модуль для просмотра статистики работы прокси-сервера;
 - Iptables – инструмент управления сетью.

7.2 Системные требования

Для корректной работы ПК “Защищенный проксирующий сервер управления виртуальной инфраструктурой” необходимо убедиться, что серверное оборудование отвечает минимальным требованиям к ПК “Звезда” RU.КНРШ.00008-01.

7.3 Развертывание изделия

7.3.1 Подготовка к работе

Для установки ПК “Защищенный проксирующий сервер управления виртуальной инфраструктурой” необходимо развернуть ПК “Звезда” RU.КНРШ.00008-01 согласно руководству администратора RU.КНРШ.00008-01 90 01 и создать виртуальную машину.

К виртуальной машине необходимо подключить готовый образ или установить Альт Рабочая станция 10.

7.3.2 Установка Squid в Альт

До начала всей установки необходимо перейти в режим администратора su. Для установки squid в терминале выполнить команду:

```
apt-get install squid
```

Настроить с помощью конфигурационного файла:

```
nano /etc/squid/squid.conf
```

Далее найти нужные строки и изменить их как приведено ниже. Необходимо еще учесть, что некоторые параметры могут быть закомментированы и не учитываться при запуске сервера. Строки комментируются знаком "#". Чтобы раскомментировать строку, необходимо удалить этот символ.

Указать, на какой порт необходимо обращаться к этому прокси серверу.

```
http_port 3128
```

Указать объем кеша, например для кеш 10ГБ, а 32 и 256 это 1-й и 2-ой уровни каталогов кеша.

```
cache_dir ufs /var/spool/squid/ 10000 32 256
```

Далее найти заголовок # INSERT YOUR OWN RULE(S) HERE TO ALLOW и после этого заголовка добавить правила, которые будут запрещать доступ к нежелательным сайтам:

acl	example	dstdomain	.example.com
http_access		allow	example
http_access		deny	example
acl	pool_blacklist	dstdomain	'/etc/squid/black.txt'
http_access	deny pool_blacklist		

Первый параметр запрещает обращаться к доменам example.com, а второй запрещает доступ к сайтам, которые находятся в /etc/squid/black.txt.

Также здесь можно добавить запреты на загрузку мультимедиа файлов:

```
acl music urlpath_regex -i \.mp3 \.wav \.ogg \.avi \.mpg \.mpeg \.wmf
http_access deny music
```

Далее необходимо найти строку и указать, сколько оперативной памяти будет использовать прокси сервер:

```
memory_pools_limit 100 MB
```

Сохраняем конфигурационный файл и выходим в терминал:

```
sudo /usr/sbin/squid -Z
sudo /etc/init.d/squid start
```

После этого можно настроить компьютеры, которые будут подключаться к прокси серверу. Для этого в них нужно использовать такие данные: сервер "ip компьютера, на котором установлен Squid", порт "3128".

7.4 Начало работы

7.4.1 Настройка прокси-сервера Alterator-squid

Модуль Прокси-сервер предназначен для конфигурирования прокси сервера Squid. Он доступен в веб-интерфейсе по адресу <https://ip-address:8080> (Ошибка! Источник ссылки не найден.).

Основные параметры
Основные параметры управления прокси-сервером

☐ Включить сервис прокси-сервера

Выберите режим проксирования: Прозрачный ▾

Выберите способ аутентификации: Без аутентификации ▾

Порт прокси-сервера:
(номер порта)

Разрешённые сети... Разрешённые протоколы...

Применить

Доступ к доменам
Для каждой из выбранной группы может быть задана политика разрешения или запрета на доступ к указанным в поле внизу доменам.

Все пользователи

Авторизованные пользователи

adm

_ahttpd

_alteratord

apache

apache2

asterisk

audio

auth

_autoipd

_avahi

Группа:
Политика доступа группы: Разрешить доступ ▾
Список суффиксов доменов:

(Список доменных суффиксов разделённых пробелами; каждый суффикс)

Сохранить

Рисунок 655 - Веб-интерфейс модуля Прокси-сервер

Несколько компьютеров, объединённых в локальную сеть могут быть подключены к глобальной сети (Интернет) через один общий канал. Такое решение имеет ряд преимуществ перед другими. В частности, если разместить в месте соединения двух сетей (шлюзе) прокси-сервер, полученные через него страницы попадут в кеш, и при повторном обращении к ним загрузка из внешней сети уже не потребуется. Это может существенно ускорить доступ к популярным сайтам и снизить потребляемый организацией трафик.

Прокси-сервер принимает запросы из локальной сети и, по мере необходимости, передаёт их во внешнюю сеть. Поступление запроса ожидается на определённом порту, который по умолчанию имеет стандартный номер 3128 (см. раздел 2). Если по каким-то причинам не желательно использовать данный порт, то можно поменять его значение на любое другое.

Перед тем как выполнить перенаправление запроса, прокси-сервер проверяет принадлежность сетевого адрес узла, с которого запрос был отправлен к группе внутренних сетевых адресов. Для того, чтобы запросы, отправленные из локальной сети, обрабатывались прокси-сервером, необходимо добавить соответствующую группу адресов (адрес подсети и адресную маску) в список внутренних сетей в разделе «Разрешённые сети» **Рисунок 656**).

Разрешённые сети

Запросы из указанных сетей будут обработаны. Запросы из других сетей будут проигнорированы.

192.168.7.0/24 (Network1)
<новая>

Сеть IP:
(IP-адрес/биты подсети)

Комментарий:

Применить **Вернуть**

Создать **Удалить**

Назад

Рисунок 656 - Редактирование списка внутренних сетей

Вторым условием передачи запроса является принадлежность целевого порта к разрешённому диапазону. Посмотреть и отредактировать список разрешённых целевых портов можно в разделе «Разрешённые протоколы» (Рисунок 657).

Разрешённые протоколы

Запросы из указанных сетей будут обработаны. Запросы из других сетей будут проигнорированы.

HTTP
GOPHER
SWAT
Filemaker
GSS-HTTP
CUPS
SNEWS (C)
FTP
Other ports
Multilingual HTTP
HTTPS (C)
HTTP-MGMT

С порта: 80 По порт: 80
(номер порта) (номер порта)

Способ соединения: Прокси
☒ Включить прозрачное перенаправление

Комментарий:
HTTP

Создать Назад Применить Вернуть Удалить

Рисунок 657 - Редактирование списка разрешенных протоколов

Прокси-сервер может работать в двух режимах: *стандартном* и *прозрачном*. Стандартный режим использования прокси-сервера требует изменения режима работы программ локальной сети, что может потребовать их ручной настройки. По этой причине другим популярным режимом использования прокси-сервера является прозрачный режим. В этом режиме все обращения из внутренней сети по зарегистрированным протоколам (портам) во внешнюю сеть автоматически перехватываются прокси-сервером при прохождении через шлюз. Программы в локальной сети при этом продолжают работать в обычном режиме, не требуя никакой специальной настройки. Недостатком прозрачного режима работы является невозможность идентификации пользователей — все запросы отправляются из локальной сети анонимно. Для указания портов, используемых в

режиме прозрачного проксирования, перейдите в раздел «Разрешённые протоколы», выберите из списка протокол и установите для этого протокола флажок «Включить прозрачное перенаправление».

Преимуществом непрозрачного режима работы, требующего перенастройки программ локальной сети, является возможность производить аутентификацию пользователей и контролировать их доступ во внешнюю сеть. Для того, чтобы включить аутентификацию, выберите способ аутентификации, отличный от Без аутентификации (Рисунок 658).

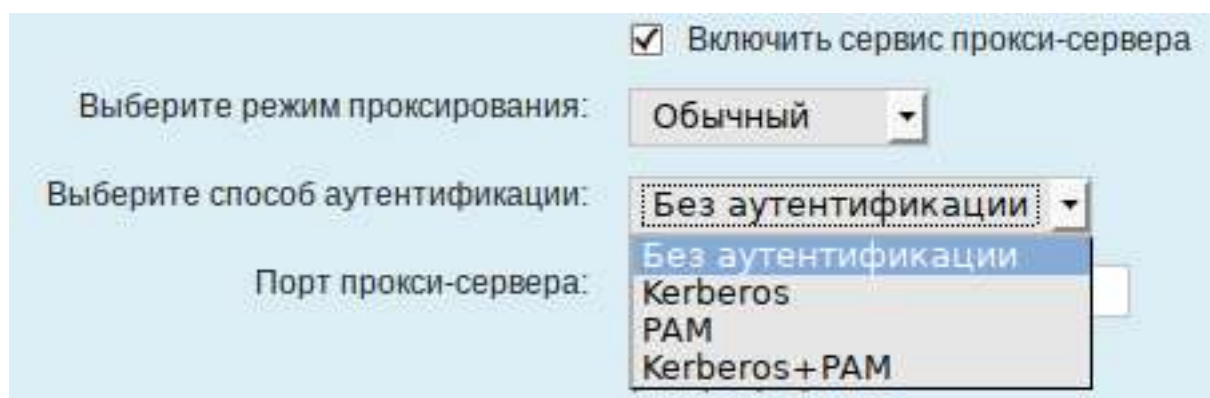


Рисунок 658 - Выбор способа аутентификации

7.4.2 Настройки политики доступа пользователей во внешнюю сеть

Политика доступа пользователей во внешнюю сеть формируется на основе групп пользователей и сетевых доменов в разделе Группы. Для каждой группы пользователей может быть сформирован список доменов, к которым разрешается, или наоборот, запрещается обращение. Внесение и исключение пользователей из групп производится с помощью общесистемного модуля «Пользователи/Группы». Политики доступа для специальных групп «Все пользователи» и «Авторизованные пользователи» обрабатываются несколько иначе, чем политики доступа для индивидуальных групп пользователей (Рисунок 659).

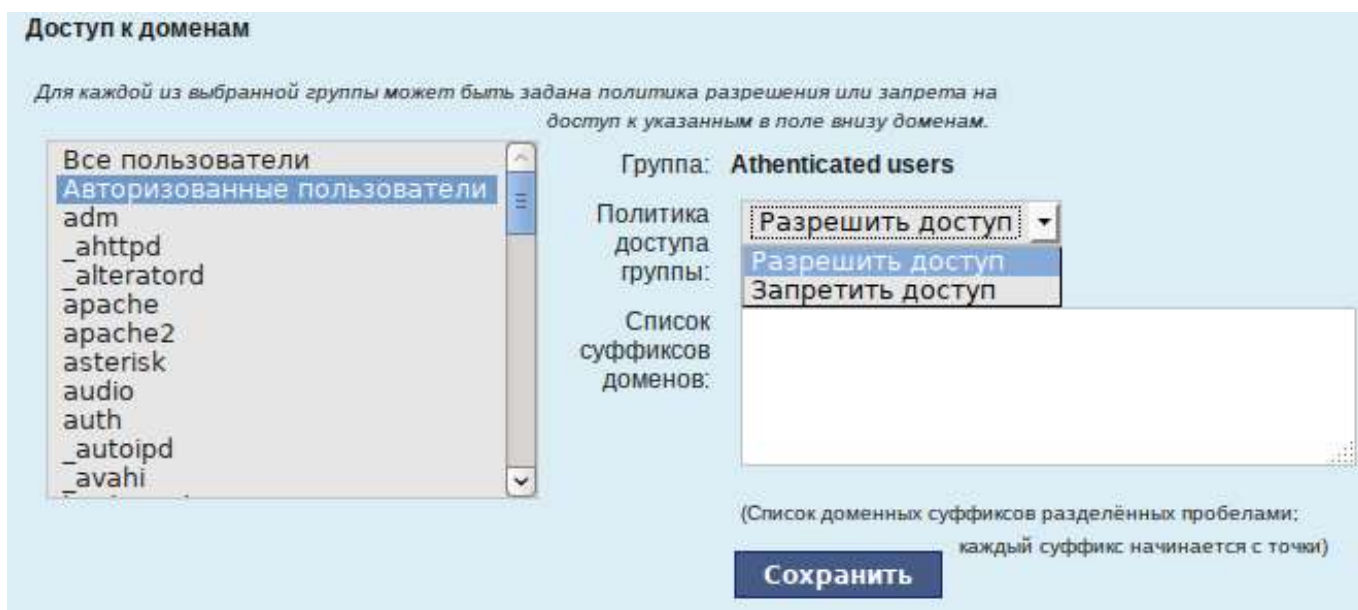


Рисунок 659 - Настройка политики доступа пользователей во внешнюю сеть

Индивидуальные политики для групп пользователей устанавливают точечные ограничения или разрешения: разрешение доступа к списку доменов не означает запрещение доступа для не вошедших в список доменов. Аналогично, запрещение доступа к списку доменов не означает разрешение доступа для не вошедших в список доменов. Имея самый высокий приоритет, они удобны для формирования исключений.

Разрешающая политика для группы «Все пользователи» определяет белый список доменов с более высоким приоритетом, чем аналогичная политика для группы «Аутентифицированные пользователи». Доступ к перечисленным доменам предоставляется всем пользователям, если индивидуальные политики не препятствуют этому. Разрешение доступа всем пользователям к определённому списку доменов удобно, когда вы совершенно не заботитесь об ограничении доступа к определённым сайтам, например, поисковым машинам. Однако в случае, если список доменов пуст, то по умолчанию доступ будет предоставлен ко всем сайтам без исключения, делая все политики с меньшим приоритетом бессмысленными.

Разрешающая политика для группы «Авторизованные пользователи» имеет более низкий по отношению к вышеописанной политике приоритет: доступ к перечисленным доменам предоставляется всем прошедшим аутентификацию пользователям, если индивидуальные политики не препятствуют этому. Разрешение доступа всем прошедшим аутентификацию пользователям к определённому списку доменов удобно, когда вы полагаете, что раз пользователь представился системе, то он может получить доступ к более широкому кругу сайтов, чем анонимные пользователи. Однако в случае, если список доменов пуст, таким пользователям по умолчанию будет предоставлен доступ ко всем сайтам без исключения. Такая установка удобна, когда вы хотите ограничить доступ в Интернет, главным образом, для анонимных пользователей.

Запрещающая политика для группы «Авторизованные пользователи» определяет чёрный список доменов с более высоким, чем аналогичная политика для группы «Все пользователи», приоритетом. Доступ к перечисленным сайтам будет запрещён для всех прошедших аутентификацию пользователей, если соответствующая индивидуальная политика или разрешающая политика группы «Все пользователи» не предоставляет его. Кроме того, доступ будет предоставлен ко всем не вошедшим в список сайтам. Такая политика удобна, когда для представившихся пользователей вы хотите ограничить доступ только к некоторому небольшому набору сайтов, оставив более масштабные ограничения для анонимных пользователей.

Запрещающая политика для группы «Все пользователи» определяет чёрный список доменов с наименьшим приоритетом. Доступ к перечисленным сайтам будет запрещён, если другие политики не препятствуют этому, в то время как доступ ко всем не вошедшим в список сайтам будет предоставлен. Такая политика удобна, когда по умолчанию вы хотите ограничить доступ только к некоторому небольшому набору сайтов.

7.4.3 Просмотр статистики работы прокси-сервера

Для просмотра статистики работы прокси-сервера предназначен модуль alterator-squidmill.

Включить сбор данных прокси-сервера: ☐ **Применить**

Общий объем трафика принятый за **сегодня**
всеми пользователями
со всех сайтов
составляет **0.00 Б**

Обновить

Список сайтов, набравших **любой объем** данных

UID/IP-адрес	Количество	Сайт/домен	Время последнего запроса

Рисунок 660 - Веб-интерфейс модуля alterator-squidmill

Пересылка каждого запроса во внешнюю сеть фиксируется прокси-сервером в специальном журнале. На основании этих данных автоматически формируются отчёты о статистике использования ресурсов сети, в том числе потраченного времени и количества переданных данных (трафика). Для включения сборки статистики работы прокси-сервера установите флажок «Включить сбор статистики», иначе новые данные об использовании сети не будет записываться в базу данных статистики.

Основное назначение модуля — это просмотр отчёта об объёме полученных из внешней сети данных. В зависимости от режима аутентификации пользователей при доступе к прокси-серверу, записи отчёта могут содержать как имена пользователей, так и адреса локальной сети.

Отчёт, выводимый на страницу не обновляется автоматически и поэтому может содержать устаревшие данные. Для обновления отчёта нажмите на кнопку «Обновить». При каждом обновлении учитываются параметры выборки, которые

можно определить над таблицей. Данные в таблице отсортированы по убыванию объёма полученных данных.

7.5 Централизованный выход в Интернет через один сервер в сети (proxy)

Для того чтобы разрешить только определённые методы доступа к Интернет (например, по протоколам HTTP и FTP) и определить права доступа абонентов на одном сервере, а самим абонентам разрешить только обращение к этому серверу по специальному прокси-протоколу (поддерживается всеми современными браузерами), можно использовать проксирующий сервер. Выделенная виртуальная машина с установленным изделием после определения прав доступа, будет транслировать (проксировать) приходящие на неё HTTP-запросы, направляя их адресатам. Допустим, несколько пользователей с нескольких компьютеров внутренней сети просматривают некоторый сайт. С точки зрения этого сайта их активность представляется потоком запросов от одного и того же компьютера.

7.5.1 Обычный доступ

Непосредственно после установки Squid уже поддерживает функции прокси, но принимает соединения только с того компьютера, на который установлен. Для того, чтобы можно было воспользоваться этим сервисом с других компьютеров, необходимо изменить т. н. таблицы управления доступом (Access Control Lists, далее ACL), находящиеся, как и большинство настроек Squid, в файле `/etc/squid/squid.conf`. Файл этот снабжён подробными комментариями и примерами по всем настройкам в виде комментариев, например, `# TAG: некоторая_настройка`. Таким же образом там описаны все значения, выставленные по умолчанию. В частности, для того, чтобы Squid принимал соединения из всей внутренней сети, необходимо раскомментировать две строки и подставить в них действительный диапазон адресов вашей сети:

```
acl our_networks src 192.168.1.0/24 192.168.2.0/24
```

```
http_access allow our_networks
```

Следует иметь в виду, что при обработке запроса на доступ к Squid все строки `http_access` файла `squid.conf` просматриваются последовательно сверху вниз до первой строки, соответствующей параметрам запроса. Это означает, что важен порядок следования строк `http_access`.

7.5.2 Анонимизирующий доступ

При использовании прокси-сервера остаётся некоторая угроза безопасности, связанная с тем, что топология внутренней сети и активность её абонентов не маскируются. Например, в протоколе HTTP используются т. н. заголовки (headers), значения которых заполняются броузерами при отправлении запроса. Squid умеет удалять опасные поля заголовка из запроса при помощи настройки `header_access` или подменять их значения на другие, заранее заданные, при помощи настройки `header_replace`.

Варианты использования этих настроек приведены в `squid.conf` в районе TAG: `header_access` и TAG: `header_replace` соответственно.

Примечание: из-за удаления и/или подмены полей заголовков может нарушиться связь с некоторыми системами, использующими значение этих полей для организации взаимодействия и авторизации.

7.5.3 Прозрачный” доступ

Можно вообще не сообщать пользователям сети, что в ней используется прокси-сервер. Если прокси-сервер — одновременно и маршрутизатор, весь сетевой трафик в любом случае его не обойдёт. При этом можно средствами межсетевого экрана все обычные HTTP-запросы к удалённым серверам перенаправлять на вход особым образом настроенного Squid. С внешней стороны это будет выглядеть обычным прокси-сервером, а со стороны пользователя —

ничем не будет отличаться от обычной работы в сети. Команда iptables, перенаправляющая HTTP-запросы к внешним серверам на порт Squid может, например, выглядеть так:

```
# iptables -t NAT -A PREROUTING -d ! адрес_самого_сервера \  
-i внутренний_сетевой_интерфейс -p tcp -m tcp --dport 80 \  
-j REDIRECT --to-ports 3128
```

Или так:

```
# iptables -t nat -A PREROUTING -p tcp -d 0/0 --dport www \  
-i внутренний_сетевой_интерфейс -j DNAT \  
--to локальный_адрес_на_котором_слушает_прокси:3128
```

Настройка squid.conf при этом использует обратное проксирование, описанное ниже. Для организации прозрачного прокси достаточно добавить в squid.conf строки

```
httpd_accel_host virtual  
httpd_accel_port 80  
httpd_accel_with_proxy on  
httpd_accel_uses_host_header on
```

7.5.4 Фильтрация доступа

В Squid существует гибкая схема фильтрации внешних ссылок. С её помощью, например, можно закрыть доступ к определённым сайтам и ресурсам на них, избавиться от навязчивой рекламы (banners), ссылок непристойного содержания и т. п. Содержимое фильтруется с помощью всё тех же ACL и настроек http_access deny, примеры которых приведены в squid.conf. Обратите внимание, что при задании фильтруемого URL или доменного имени сервера можно использовать регулярные выражения, таким образом в одной строке определяя фильтр для целого класса адресов или доменных имён. Подробнее о регулярных выражениях можно прочитать в руководстве regex(7). Запрет доступа к домену baddomain.com, например, можно оформить в виде строк

```
acl Bad dstdomain baddomain.com
http_access deny Bad
```

Примечание: `http_access deny Bad` следует помещать перед строками вида `http_access allow`, в этом случае доступ к любому сайту домена будет закрыт безусловно.

7.5.5 Авторизация доступа

В Squid есть возможность определять различные ACL разным пользователям и/или категориям пользователей. Если для определения того, какой именно пользователь подключается к серверу, недостаточно IP-адреса его компьютера, следует воспользоваться одной из многих схем авторизации, принятых в Squid. Авторизация конфигурируется с помощью тега TAG: `auth_param`. Посмотреть, какие схемы (программы) авторизации поддерживает Squid, вы можете в каталоге `/usr/lib/squid`.

Например, настройка авторизации в LDAP может выглядеть так:

```
auth_param basic program /usr/lib/squid/squid_ldap_auth -b
ou=People,dc=office,dc=lan -f (uid=%s) -h ldap.office.lan
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
```

7.6 Локальное хранение данных, которые уже запрашивались пользователями (cache)

Не менее важное свойство Squid состоит в том, что данные, полученные по запросам из сети Интернета, сохраняются в системе (кешируются). При повторных запросах данные будут предоставляться не из Интернет, а из сохранённой копии. Объекты кешируются до тех пор, пока не истечёт их “срок годности” или пока они не будут вытеснены другими, более часто используемыми. Например, если все пользователи внутренней сети одновременно работают с одним и тем же сайтом в сети, общий поток запросов от Squid будет несравненно меньше потока

пользовательских запросов, так как большинство ресурсов сайта уже будет закешировано.

7.6.1 Обычное кеширование

Непосредственно после установки сервера он уже выполняет кеширующие функции. Кеширование позволяет не только сэкономить на оплате трафика, но и уменьшить время доступа к ресурсам Интернет. Однако следует понимать, что снижение внешнего трафика возможно только если один и тот же ресурс был запрошен несколькими пользователями на протяжении некоторого промежутка времени. Если пользовательские запросы почти не пересекаются, снижение трафика может быть незначительным.

Кроме того, кеширование неэффективно в ситуации, когда повторный запрос на большинство объектов приходит уже после того, как эти объекты вытесняются из кеша более новыми. Если анализ статистики показывает, что происходит именно это, можно попробовать увеличить объём кешируемой информации. Настройки Squid, отвечающие за размер кеша, приведены в файле `squid.conf` в разделе, начинающемся словами `OPTIONS WHICH AFFECT THE CACHE SIZE`.

Наконец, кеширование входного потока данных делает невозможной “справедливую” оплату различными пользователями их собственного трафика. Например, если один пользователь посещает некие сайты по совету другого, то его трафик будет по большей части не выходить за пределы сервера, на котором ресурсы этих сайтов уже — по милости первого пользователя — закешированы.

Чтобы включить кеширование необходимо найти и раскомментировать следующую строку:

```
cache_dir ufs /var/spool/squid 100 16 256
```

100 здесь — размер буфера под кэш в Мб, его можно изменить, максимальное адекватное значение параметра 1/3 объема жесткого диска

Кэш будет храниться в `/var/spool/squid`. Необходимо убедиться в том, что каталог существует и SQUID имеет достаточно прав для того чтобы записывать в файлы, в нем размещающиеся информацию.

Останавливаем прокси командой

```
/etc/init.d/squid stop
```

Даем команду на создание дерева директорий

```
squid -z
```

Снова запускаем сервис

```
/etc/init.d/squid start  
du -sh /var/spool/squid
```

Если все сделано правильно вывод последней команды изначально должен показывать приблизительно 70 Мб, в дальнейшем размер каталога с кэшем, естественно, должен увеличиваться.

Чтобы изображения на сайтах, посещаемых пользователями, обновлялись несколько быстрее используем следующую директиву — в ее синтаксисе зададим форматы файлов, которые будут считаться изображениями и будут обновляться чаще

```
refresh_pattern -i \.{gif|png|jpg|jpeg|ico}$ 3600 90% 43200
```

Также в конфиге присутствуют настройки безопасных портов — `safe ports` — портов, с которыми будет производиться работа и SSL портов (настройка squid для работы по `https` является несколько более сложной задачей, чем разбираемая сейчас — она будет рассмотрена в рамках другой статьи). Настройки портов можно изменить.

```
acl SSL_ports port 443
```

Следующая директива запрещает доступ со всех портов, которые не определены в качестве безопасных

```
http_access deny !Safe_ports
```

Аналогично можно установить обязательность использования защищенного соединения — сейчас в тестовой среде директиву не применяем — здесь она приведена для примера

```
http_access deny CONNECT !SSL_ports
```

Разрешаем доступ служебному пользователю manager, это сделает возможным, в частности, для него читать статистику — доступ даем только к localhost

```
http_access allow localhost manager
http_access deny manager
http_access allow localhost
```

Если необходимо быстро дать приостановить использование прокси можно раскомментировать одну из следующих строк конфига, закомментировав при этом все строки с ограничивающими доступ правилами

```
#http_access allow localnet
#http_access allow all
```

Раскомментировав forwarded_for off мы спрячем ip адреса клиентов от Интернета — в лог файлах будет фигурировать адрес прокси сервера — используется в анонимайзерах, сейчас оставим знак комментария

```
#forwarded_for off
```

Ограничим возможность получения трафика с определенных сайтов указав их подряд разделяя имена пробелами

```
acl block_websites dstdomain .bad.com .yahoo.co
```


Активируем правило

```
http_access deny block_websites
```

7.6.2 Выборочное кеширование

Некоторые данные (например, очень большие файлы, автоматически изменяемые WWW-страницы, звуки и т. п.) кешировать невыгодно: вероятность повторного запроса в течение “срока годности” низкая, а других объектов вытесняется много. С другой стороны, содержимое некоторых сайтов может понадобиться кешировать в обязательном порядке (например, для ускорения доступа). Эти свойства управляются, как обычно, при помощи ACL и настроек `always_direct` (без кеширования) и `never_direct` (обязательное кеширование). Например, чтобы предотвратить кеширование файлов, получаемых по протоколу FTP (это, как правило, разумно), необходимо в соответствующем месте `squid.conf` раскомментировать строки

```
acl FTP proto FTP
always_direct allow FTP
```

7.6.3 Иерархия серверов

Если запрашиваемый ресурс не найден в локальном кеше Squid, он может попытаться запросить его у “вышестоящих” серверов или у “соседей” — вместо того, чтобы обращаться в Интернет. Таким вышестоящим сервером (`parent peer`) может быть сервер провайдера, а соседом (`sibling peer`) — сервер абонента, подключённого к тому же провайдеру. Правила передачи объектов кеша и формирования иерархии серверов описаны в документации. Раздел настроек, отвечающий за механизм обмена кешем, начинается словами `OPTIONS WHICH AFFECT THE NEIGHBOR SELECTION ALGORITHM`.

Необходимо знать, что обмен содержимым кеша требует непременно авторизации доступа между серверами (во избежание подлогов и другого вида атак). Все параметры соединения сервера с сервером (настройка `cache_peer`)

записываются в текстовом виде, включая пароли, так что следует строго ограничить доступ к файлу настройки squid.conf.

7.7 Обратное проксирование и кеширование внутренних серверов (accelerate)

Кеширующие и проксирующие способности Squid можно использовать и “в обратную сторону”, пропуская через сервер входящие запросы на внутренние серверы. Таким образом можно скрыть реальное расположение и структуру серверов, и уменьшить нагрузку на них.

7.7.1 Обычное обратное проксирование (один сервер)

В режиме accelerate сервер сам принимает извне HTTP-запросы, адресованные, как правило на 80-й порт. Кроме того, необходимо указать имя сервера и порт, на который будут проксироваться запросы. Это можно сделать, например, так

```
http_port 80
httpd_accel_host internal.www.com
httpd_accel_port 80
```

Если необходимо как-то ограничить доступ к внутреннему серверу, это легко сделать, применив соответствующие ACL.

7.7.2 Множественное проксирование

Для обратного проксирования нескольких внутренних серверов необходимо, чтобы внешние запросы на сайты с разными доменными именами попадали на вход Squid, который бы ставил в соответствие каждому имени действительный адрес сервера во внутренней сети и перенаправлял бы запрос туда. Делается это с помощью механизма виртуальных хостов. Вот как, например, можно организовать прокси для двух серверов, www1.foo.bar и www2.foo.bar, адреса которых в DNS указывают на машину со Squid-сервером (файл /etc/squid/squid.conf):

```
http_port 80
```

```
hosts_file /etc/squid/hosts
visible_hostname www1.foo.bar
httpd_accel_host virtual
httpd_accel_uses_host_header on
```

Настройка `visible_hostname` нужна серверу для заполнения HTTP-заголовков. Файл `/etc/squid/hosts`, формат которого аналогичен формату `/etc/hosts`, содержит адреса серверов во внутренней сети:

```
10.0.0.1 www1.foo.bar
10.0.0.2 www2.foo.bar
```

Множественное обратное проксирование имеет важный побочный эффект. В сетях, подключённых к Интернету постоянно, нередко случаи, когда недобросовестные администраторы внутренних сайтов регистрируют их в других доменах и используют их в качестве хостинг-платформ, часто с документами незаконного или нецензурного содержания. Допустим, сайт `www1.foo.bar` также зарегистрирован как `www.verycoolwarez.com`, и по этому адресу доступны пиратские версии программ и т. п. В обычном случае для обнаружения этого факта необходимо анализировать трафик, делать внушение администратору `www1.foo.bar` и т. д.

При использовании обратного проксирования такого вообще не может произойти без договорённости с администратором Squid, то есть без занесения в `/etc/squid/hosts`.

7.8 Сбор статистики и ограничение полосы доступа

В Squid входит утилита кеш-менеджер, служащая для отображения статистики и загрузки сервера. Кеш-менеджер представляет собой cgi-приложение и должен выполняться под управлением сконфигурированного HTTP-сервера. Все настройки кеш-менеджера также производятся в `/etc/squid/squid.conf`, строки, которые относятся к кеш-менеджеру, обычно включают `cachemgr`.

При помощи Squid можно ограничить полосу пропускания (“толщину канала”) для пользователей. За это отвечают параметры `delay_pools` и `delay_class`. Эта технология позволит вам снизить загрузку канала например mp3-файлами, и соответственно отдать полосу более приоритетному трафику. Один из примеров настройки можно найти на сайте www.atmsk.ru

7.9 Кеширование DNS-запросов

Squid содержит встроенный минисервер запросов DNS. Он выступает как посредник между Squid и внешними DNS-серверами. При запуске Squid производит начальное тестирование доступности DNS и интернет в целом. Это можно отключить, используя опцию `-D`. Время кеширования удачного DNS-запроса по умолчанию составляет шесть часов.

8 Подсистема мониторинга «Горизонт-ВС»

8.1 Назначение Подсистемы

Программное обеспечение «Подсистема мониторинга «Горизонт-ВС»» (далее Подсистема мониторинга) предназначена для обеспечения отображения текущего состояния Системы виртуализации «Горизонт-ВС» (далее «Горизонт-ВС»), производительности её работы и контроля её работоспособности.

8.2 Назначение документа

Данный документ предназначен: для пользователей Подсистемы мониторинга, осуществляющих функции администрирования данной Подсистемы.

Документ содержит перечень задач, выполняемых пользователем с правами администратора в процессе эксплуатации Подсистемы мониторинга.

Документ содержит краткие инструкции по выполнению данных задач в Веб-интерфейсе Подсистемы мониторинга.

Данный документ не содержит описание функций по установке и настройке ПО, не входящих в зону ответственности пользователей с ролью администратора Подсистемы мониторинга.

Внимание! Все функции, связанные с установкой и настройкой ПО Подсистемы мониторинга, приведены в отдельном документе: **«Подсистема мониторинга «Горизонт-ВС». Руководство по установке и настройке ПО»**.

8.3 Требования к квалификации администратора

Навыки администрирования ОС Linux. Работа с командной строкой и системой контейнеризации (docker, docker compose).

8.4 Вход в Веб-интерфейс Подсистемы мониторинга

8.4.1 Требования к рабочему месту

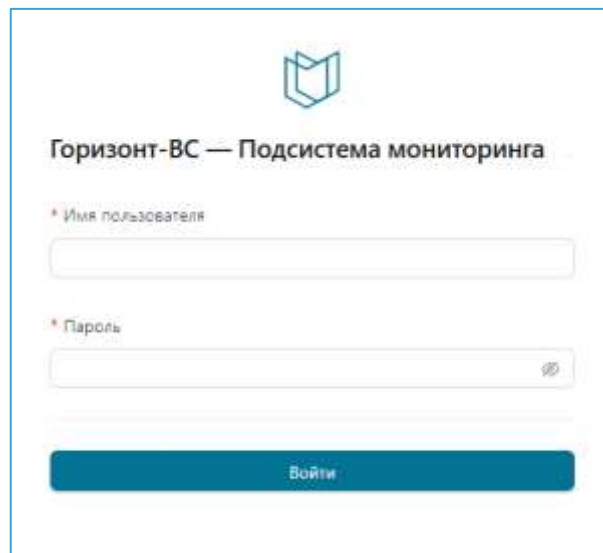
Для работы с Веб-интерфейсом Подсистемы мониторинга рекомендуется использовать один из следующих браузеров:

- Google Chrome — не ниже версии 97;
- Mozilla Firefox — не ниже версии 95;
- Safari — не ниже версии 14;
- Microsoft Edge — не ниже версии 97;
- Internet Explorer 11: полная поддержка для IE11;
- Яндекс Браузер — не ниже версии 21.

8.4.2 Аутентификация пользователя

Для входа в Веб-интерфейс Подсистемы мониторинга необходимо:

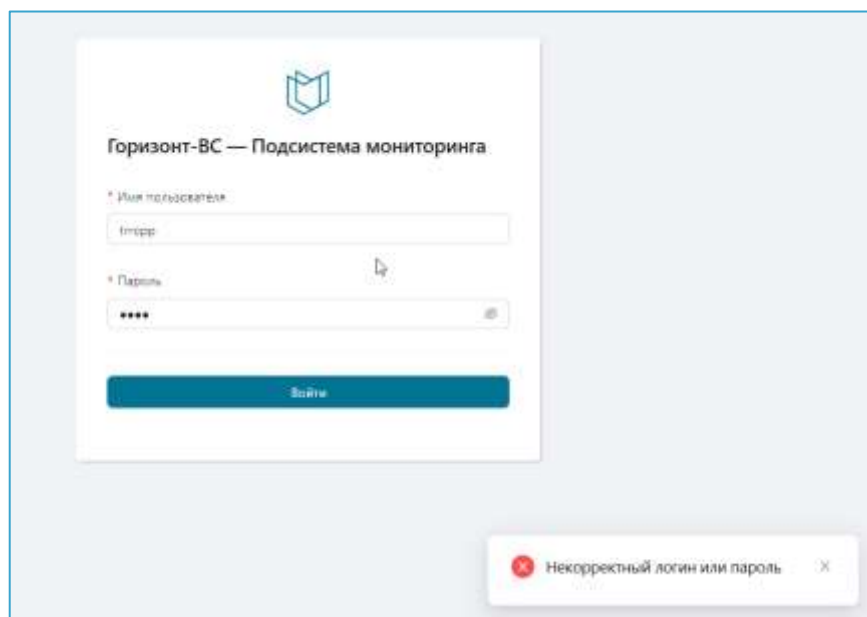
- 1) Ввести в браузере IP адрес Веб-сервера Подсистемы.
- 2) В открывшемся окне ввести логин и пароль пользователя, зарегистрированного в Подсистеме с ролью администратора (**Рисунок 661 - Аутентификация пользователя** Рисунок 661).
- 3) Нажать кнопку **Войти**.



The screenshot shows a login interface for 'Горизонт-ВС — Подсистема мониторинга'. At the top is a logo consisting of three blue geometric shapes. Below the logo is the title 'Горизонт-ВС — Подсистема мониторинга'. There are two input fields: the first is labeled 'Имя пользователя' (Username) and the second is labeled 'Пароль' (Password). The password field has a toggle icon on the right. Below the fields is a blue button labeled 'Войти' (Login).

Рисунок 661 - Аутентификация пользователя
в Подсистеме мониторинга

При попытке ввести неверные данные аутентификации Подсистема выдаст предупреждение (Рисунок 662).



This screenshot shows the same login form as Figure 661, but with an error message. The 'Имя пользователя' field contains the text 'lmprr' and the 'Пароль' field contains five asterisks. A blue 'Войти' button is at the bottom. In the bottom right corner, there is a red error message box that says 'Некорректный логин или пароль' (Incorrect login or password).

Рисунок 662 - Результат ввода неверных данных
аутентификации пользователя

Если аутентификация пользователя прошла успешно, то:

- 1) Если Подсистема **подключена** к Системе виртуализации «Горизонт-ВС» – на экране откроется основная страница веб-интерфейса Подсистемы мониторинга.
- 2) Если Подсистема **не подключена** к Системе виртуализации «Горизонт-ВС» – на экране откроется окно подключения к Системе (Рисунок 663). Для дальнейшей работы необходимо провести подключение Подсистемы мониторинга к Системе виртуализации «Горизонт-ВС» – см. п. 0.

Рисунок 663 - Окно подключения Подсистемы мониторинга к Системе виртуализации «Горизонт-ВС»

8.4.3 Смена временного пароля

При входе в Подсистему мониторинга под учетной записью с временным паролем:

- профиль пользователя отмечается оранжевой меткой в виде точки;
- на экране отображается всплывающее сообщение о необходимости сменить пароль.

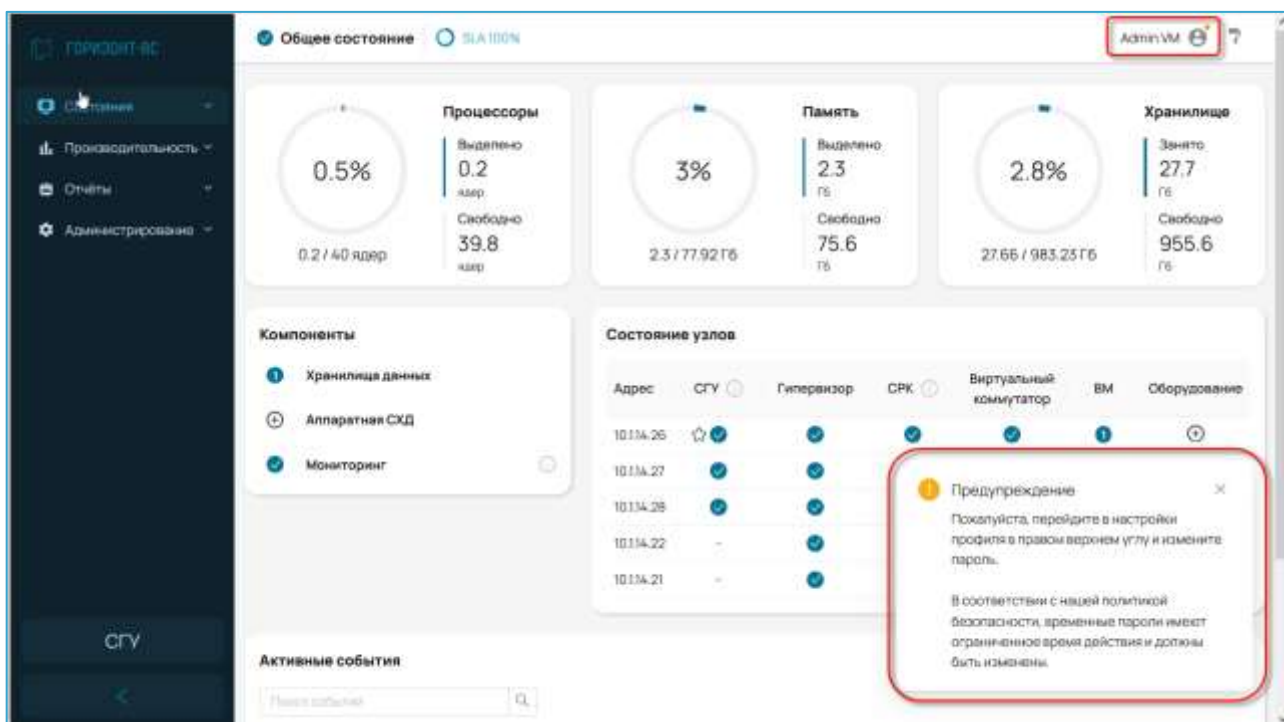


Рисунок 664 - Вход в Подсистему мониторинга под учетной записью с временным паролем

После первого входа в Подсистему желательно сменить временный пароль на постоянный.

Для смены пароля на постоянный, пользователю необходимо:

- 1) Зайти в профиль пользователя, выбрав в раскрывающемся меню строку **Профиль**.

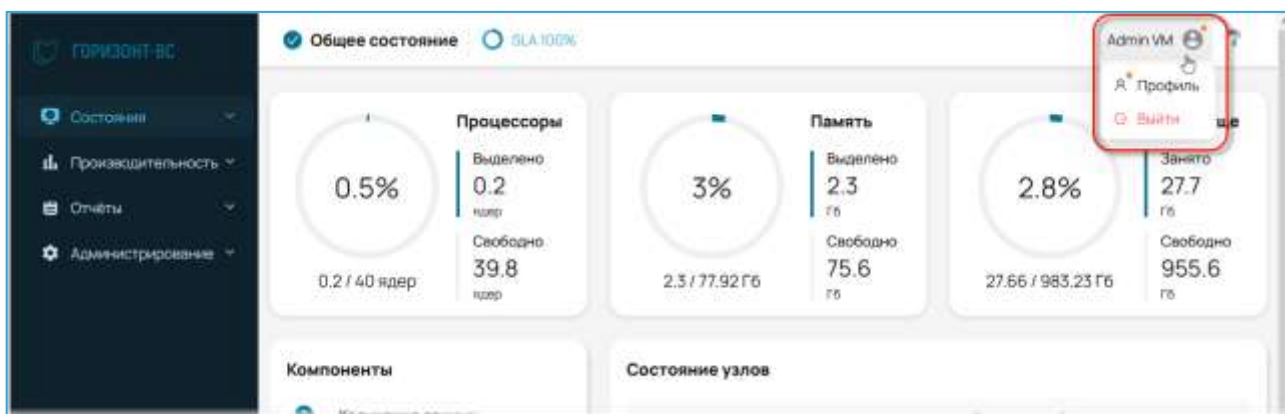


Рисунок 665 - Отображение в интерфейсе пользователя с временным паролем

2) В открывшемся окне профиля выбрать вкладку **Пароль** и указать новый пароль.

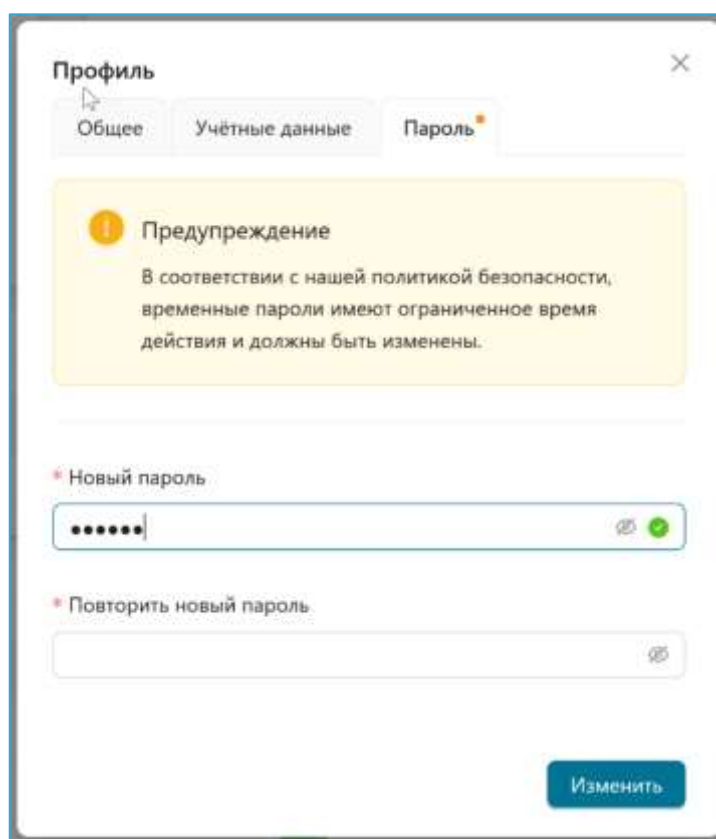


Рисунок 666 - Смена пароля

После смены временного пароля оранжевая метка возле данных пользователя будет удалена.

8.4.4 Стартовая страница Веб-интерфейса Подсистемы мониторинга

При первом входе в Веб-интерфейс открывается страница Подсистемы мониторинга – подраздел «Состояния» → «Платформа» (🖥️), который содержит сводную текущую информацию по объектам и компонентам Системы виртуализации «Горизонт-ВС».

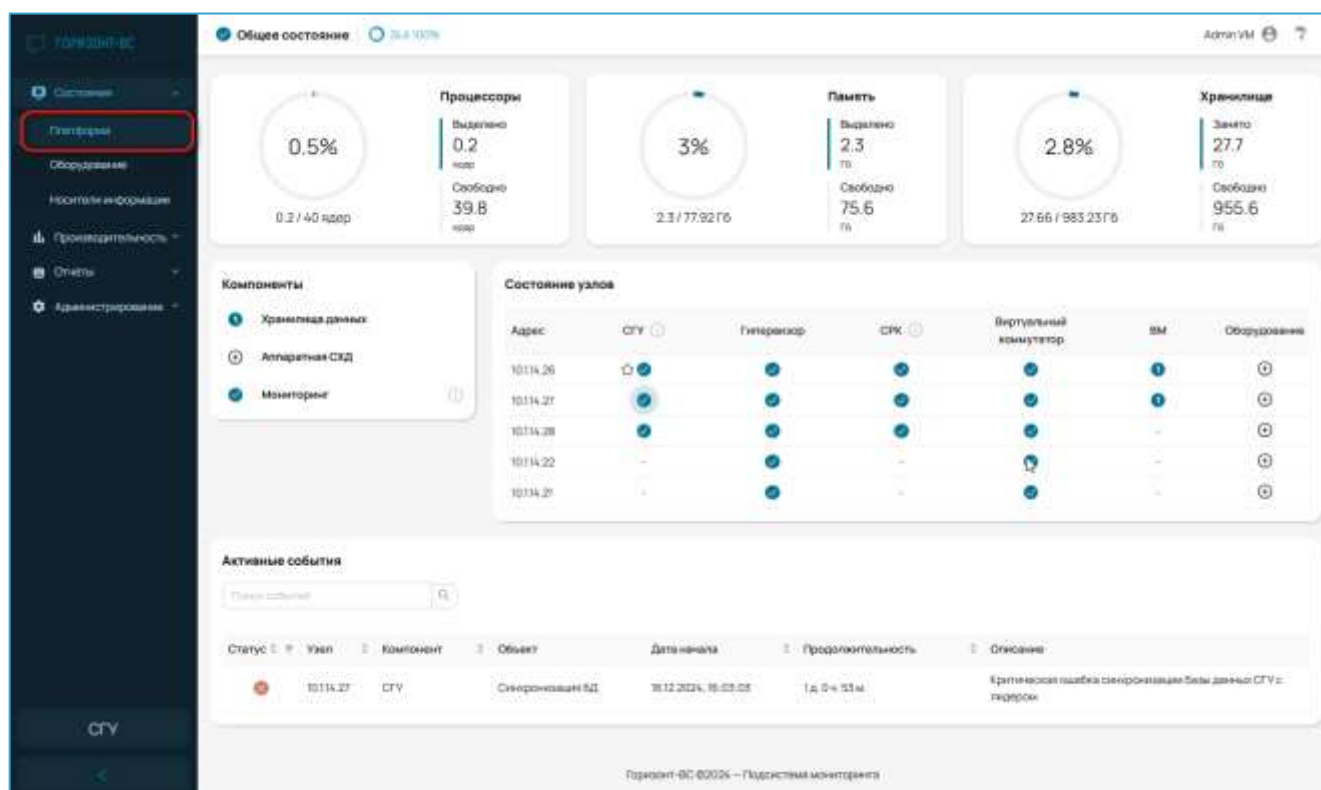


Рисунок 667 - Стартовая страница Веб-интерфейса Подсистемы мониторинга

8.5 Особенности использования пробной версии Подсистемы мониторинга

8.5.1 Работа в пробной версии Подсистемы мониторинга

В Подсистеме мониторинга «Горизонт-ВС» предусмотрена возможность однократной активации пробной версии ПО сроком на 30 дней. Подробно процесс активации пробной версии приведен в отдельном документе «Подсистема

мониторинга

«Горизонт-ВС». Руководство по установке и настройке ПО».

В случае работы пользователя с пробной версией Подсистемы мониторинга на экране открывается страница веб-интерфейса пробной версии Подсистемы мониторинга «Горизонт-ВС». Для пробной версии Подсистемы мониторинга в правом верхнем углу Веб-интерфейса указан параметр **Срок действия**, содержащий текущее время действия пробной версии. Данный информационный параметр доступен во всех разделах пробной версии интерфейса Подсистемы мониторинга.

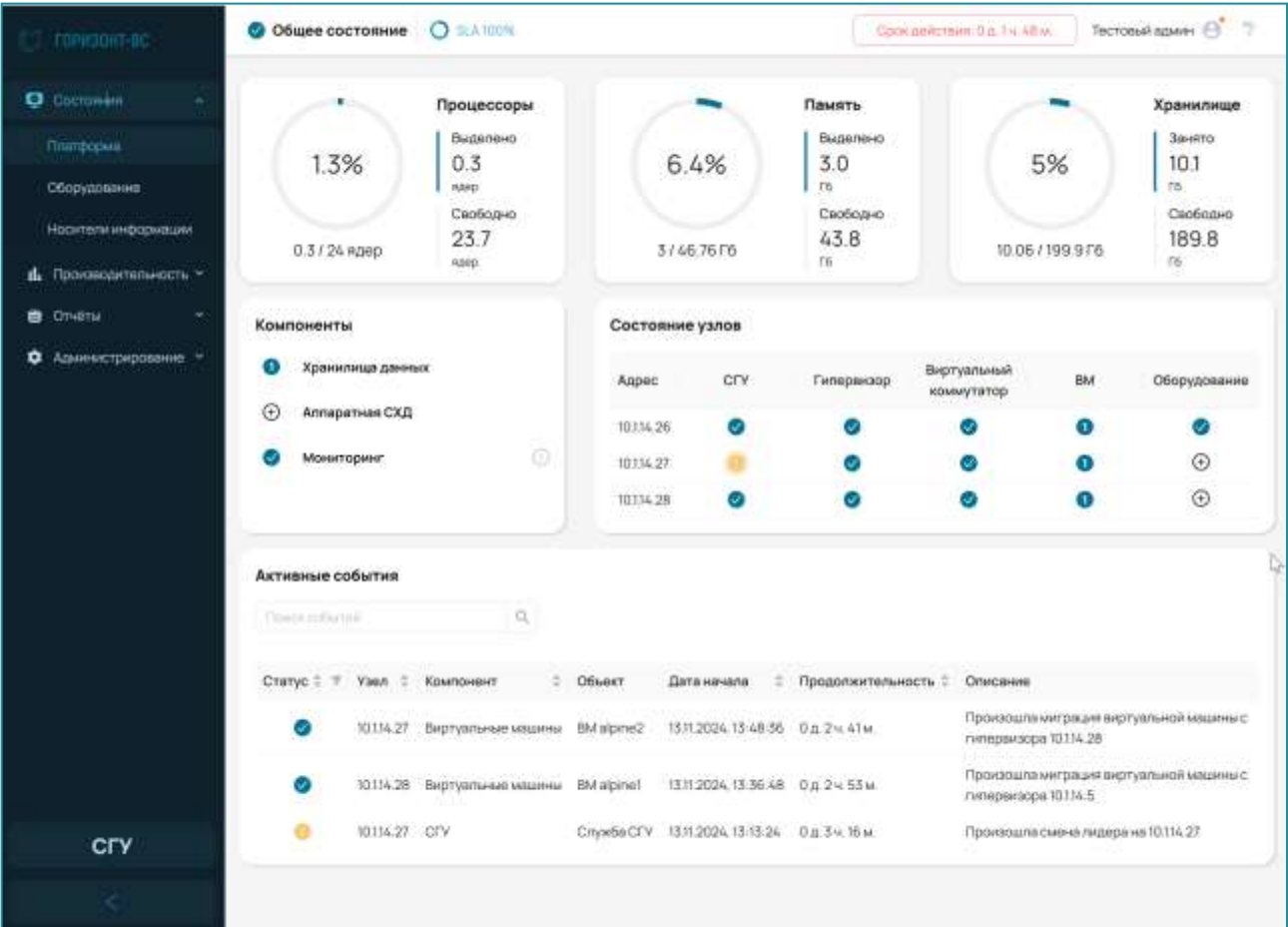


Рисунок 668 - Стартовая страница Веб-интерфейса Подсистемы мониторинга в режиме пробной версии

8.5.2 Активация лицензии по завершению работы с пробной версией Подсистемы мониторинга

Внимание! Пробную версию Подсистемы мониторинга «Горизонт-ВС» возможно активировать **только один раз**. Срок действия пробной версии 30 дней.

Завершение работы с пробной версией Подсистемы мониторинга может быть реализовано в следующих видах:

- 1) Переход на лицензионную версию ПО раньше окончания срока действия пробной версии.

Переход осуществляется с использованием функции интерфейса **Срок действия** – см. **Ошибка! Источник ссылки не найден..** Для перехода на лицензионную версию требуется активировать лицензию, следуя указаниям мастера активации. Алгоритм получения и активации лицензии подробно приведен в отдельном документе *«Подсистема мониторинга «Горизонт-ВС». Руководство по установке и настройке ПО»*.

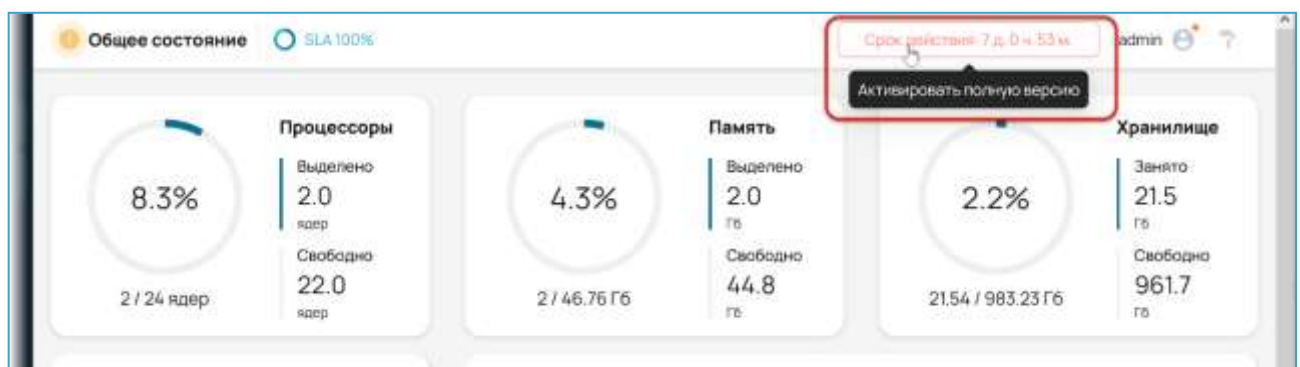


Рисунок 669 - Переход на лицензионную версию ПО

- 2) Переход на лицензионную версию ПО по окончании срока действия пробной версии.

По завершении срока действия пробной версии Подсистемы мониторинга на экране автоматически всплывает окно активации лицензии. Возврат к интерфейсу Подсистемы мониторинга невозможен. Для перехода на лицензионную версию требуется активировать лицензию, следуя указаниям мастера активации. Алгоритм получения и активации лицензии подробно приведен в отдельном документе «Подсистема мониторинга «Горизонт-ВС». Руководство по установке и настройке ПО».

Если лицензию не активировать, то Веб-интерфейс Подсистемы мониторинга «Горизонт-ВС» становится недоступным.

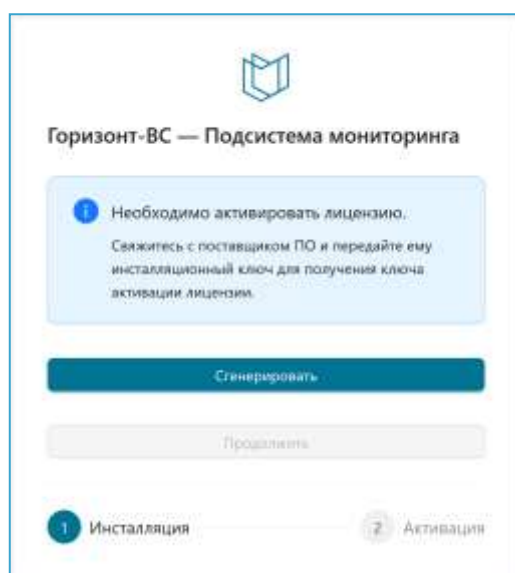


Рисунок 670 – 1 этап активации Подсистемы мониторинга:
получение инсталляционного ключа

При переходе на лицензионную версию:

- сохраняются настройки аутентификации пользователя, указанные в пробной версии ПО Подсистемы мониторинга;
- сохраняются настройки аутентификации пользователя;

- сохраняется подключение Подсистемы мониторинга к Системе виртуализации «Горизонт-ВС».

8.6 Подключение Подсистемы мониторинга к Системе виртуализации «Горизонт-ВС»

Подключение Подсистемы мониторинга к Системе виртуализации «Горизонт-ВС» проводится в следующих ситуациях:

- после активации временной лицензии, выполненной при первом входе в Подсистему мониторинга;
- после активации постоянной лицензии, выполненной при первом входе в Подсистему мониторинга, если временная лицензия не использовалась;
- после отключения от СГУ в разделе веб-интерфейса **«Администрирование»** → **«Настройки»** с целью сброса настроек и переподключения к иному СГУ.

Процесс подключения Подсистемы мониторинга к Системе виртуализации «Горизонт-ВС» состоит из двух этапов: **подключение** к «Горизонт-ВС» и **обнаружение** объектов мониторинга.

На этапе подключения к «Горизонт-ВС» необходимо выполнить следующие действия:

- 1) В открывшемся окне подключения ввести следующие данные:
 - адрес, на котором развернута СГУ;
 - порт, на котором «Горизонт-ВС» отвечает по XML-RPC. По умолчанию это порт 2634;
 - имя и пароль сервисного пользователя для доступа к «Горизонт-ВС» по XML-RPC (см. документ *«Подсистема мониторинга «Горизонт-ВС». Руководство по установке и настройке ПО»*).
- 2) Нажать кнопку **Подключить**.

Подключение к Горизонт-ВС

1 Для дальнейшей работы с системой мониторинга необходимо произвести подключение к Горизонт-ВС.

* Адрес

Порт

2634

* Имя пользователя

admin

* Пароль

Подключить

1 Подключение 2 Обнаружение

Рисунок 671 - Окно подключения Подсистемы мониторинга к Системе виртуализации «Горизонт-ВС»

Если какие-то данные введены неверно, то на экране откроется окно предупреждения:

- При вводе неверного адреса или порта «Горизонт-ВС» выводится сообщение **«СГУ не найден»**.
- При вводе неверного логина или пароля сервисного пользователя «Горизонт-ВС» выводится сообщение **«Некорректный логин или пароль»**.

Примечание. Для получения актуальных данных для подключения необходимо обратиться к администратору «Горизонт-ВС».

Если все данные введены верно, то автоматически начнется процесс обнаружения объектов мониторинга «Горизонт-ВС»: появится сообщение **«Запущен процесс обнаружения»** и в окне подключения отобразятся следующие шаги:

- «Горизонт-ВС найден, пожалуйста подождите»;
- «Запущен процесс обнаружения...».

Пройденные шаги отмечаются зеленым маркером, не пройденные – имеют синий маркер.

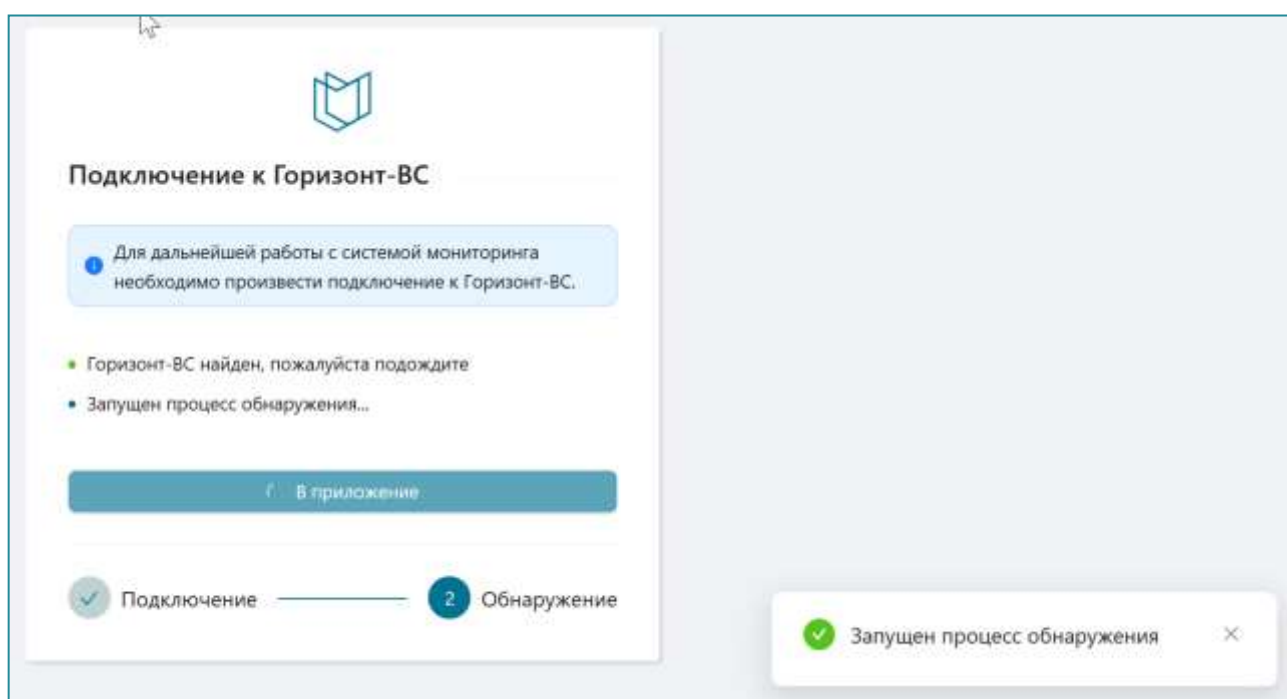


Рисунок 672 - Начало процесса обнаружения объектов

В процессе обнаружения открывается состав таких объектов «Горизонт-ВС» как:

- СГУ;
- гипервизоры;
- виртуальные рабочие столы (если есть в составе системы);
- СРК (если есть в составе системы);
- СХД/ РСХД (если есть в составе системы).

Зелеными и синими маркерами отмечаются соответственно обнаруженные и находящиеся в процессе обнаружения объекты (см. **Ошибка! Источник ссылки не найден.**).

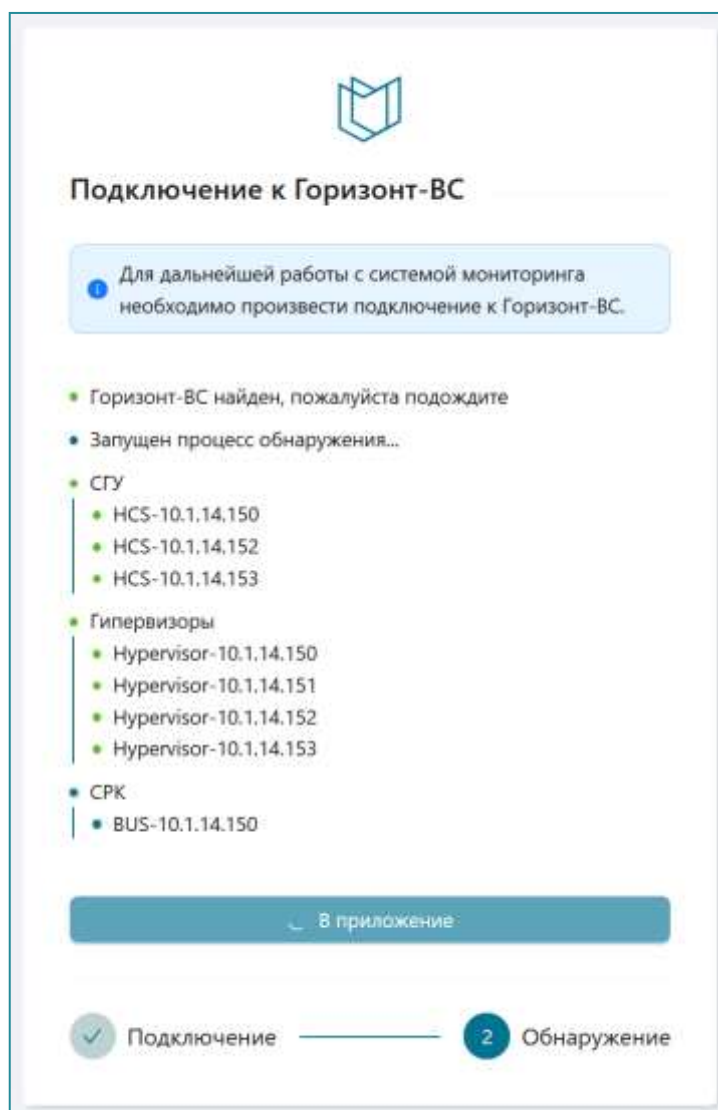


Рисунок 673 - Процесс обнаружения объектов «Горизонт-ВС»

После завершения процесса обнаружения:

- все шаги помечаются зеленым маркером;
- в список шагов добавляется новый пункт «**Горизонт-ВС успешно подключён!**»;

- второй этап «**Обнаружение**» отмечается флажком как пройденный;
- становится доступной кнопка **В приложение**.

Для перехода в веб-интерфейс Подсистемы мониторинга и начала работы нажать кнопку **В приложение**. На экране должна открыться основная страница веб-интерфейса Подсистемы мониторинга – раздел «**Состояния**» → «**Платформа**» .

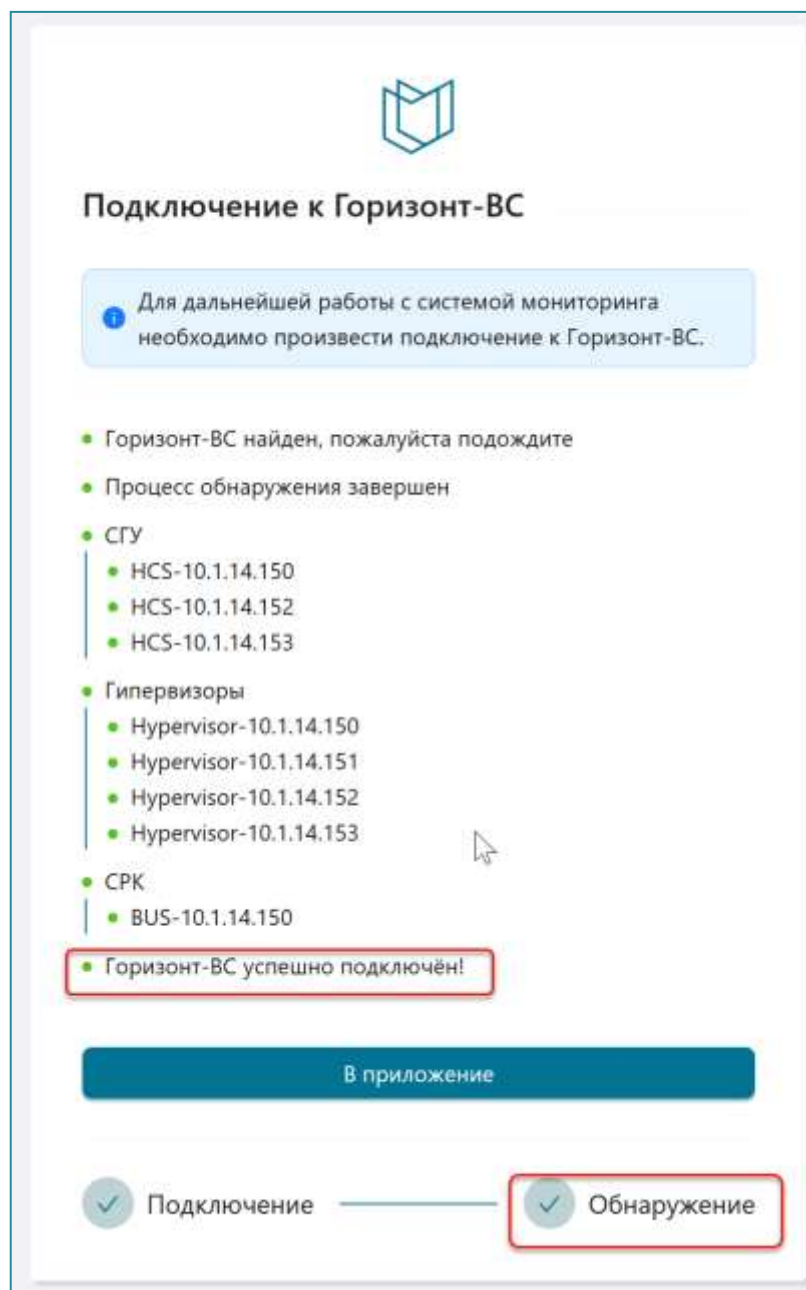


Рисунок 674 - Завершение процесса обнаружения объектов «Горизонт-ВС»

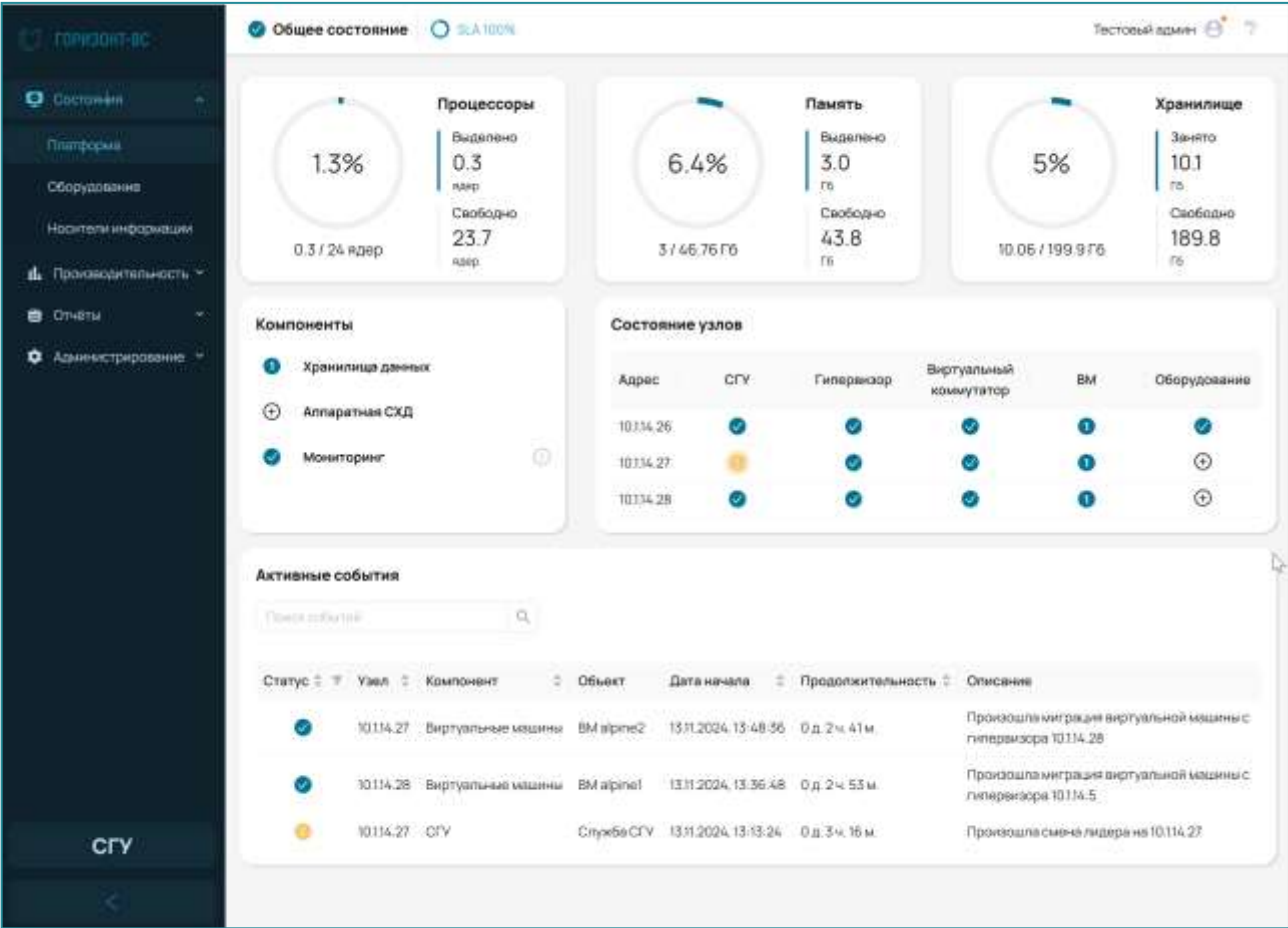


Рисунок 675 - Основная страница веб-интерфейса Подсистемы мониторинга для пользователя с ролью Администратор

8.7 Веб-интерфейс Подсистемы мониторинга. Функции администратора

8.7.1 Общие данные о веб-интерфейсе Подсистемы мониторинга

Веб-интерфейс Подсистемы мониторинга состоит из следующих разделов (см. **Ошибка! Источник ссылки не найден.**):

1) Раздел **«Состояния»** – состоит из следующих подразделов:

- **«Платформа»** – подраздел является стартовой страницей веб-интерфейса Подсистемы мониторинга. Представляет собой приборную панель и обеспечивает отображение сводной информации по объектам «Горизонт-ВС» в графическом виде (см. **Ошибка! Источник ссылки не найден.**).
- **«Оборудование»** – подраздел представляет собой приборную панель и предназначен для контроля работы различных типов оборудования в составе «Горизонт-ВС».
- **«Носители информации»** – подраздел представляет собой приборную панель и предназначен для контроля работы различных типов носителей информации, таких как: RAID массивы, жёсткие диски, флеш-накопители

2) Раздел **«Производительность»** – состоит из следующих подразделов:

- **«Платформа»** – предназначен для просмотра сводных данных о производительности платформы «Горизонт-ВС».
- **«Гипервизоры»** – предназначен для просмотра данных о работе гипервизоров на узлах платформы «Горизонт-ВС».
- **«Виртуальные машины»** – предназначен для просмотра данных о работе ВМ в составе платформы «Горизонт-ВС».

3) Раздел **«Отчёты»** – состоит из следующих подразделов:

- **«События»** – обеспечивает доступ пользователя к Журналу событий Подсистемы, в котором отображаются события со статусами **Критическая**

ошибка () и **Предупреждение** (), произошедшие на объектах «Горизонт-ВС»; информационные сообщения о произошедших в системе важных событиях, например, сообщения об успешном резервном копировании ВМ ().

- «**Производительность**» – предназначен для формирования и выгрузки из Подсистемы мониторинга отчетов о производительности таких объектов Системы виртуализации как платформа, гипервизоры, виртуальные машины.
- «**Статистика**» – предназначен для формирования и выгрузки из Подсистемы мониторинга отчётов по статистике работы Системы виртуализации и ее основных компонентов за указанный период времени.
- «**Диагностика**» – предназначен для формирования и выгрузки из Подсистемы мониторинга диагностических отчетов состояния Системы виртуализации «Горизонт-ВС» и входящих в состав компонентов в формате .txt. Отчеты предназначены для упрощения и более эффективного взаимодействия с службой технической поддержки Горизонт-ВС.

4) Раздел «**Администрирование**» предназначен для работы пользователя с правами администратора и включает следующие подразделы:

- «**Пользователи**» – предназначен для управления пользователями Подсистемы мониторинга.
- «**Оборудование**» – предназначен для настройки мониторинга оборудования «Горизонт-ВС» по протоколу IPMI;
- «**Уведомления**» – предназначен для настройки правил отправки уведомлений в Подсистеме мониторинга.
- «**Триггеры**» – предназначен для создания и настройки правил отслеживания (триггеров), позволяющих контролировать достижение

пороговых значений различных метрик Системы виртуализации «Горизонт-ВС».

- «**Настройки**» – предназначен для проведения настройки Подсистемы мониторинга, а также сброса системы и подключения к иному СГУ.
- «**Опрос**» – предназначен для настройки параметров опроса объектов мониторинга (частота, включение и отключение отдельных опросов).

Для пользователя с ролью администратор доступны все разделы веб-интерфейса Подсистемы мониторинга. Непосредственно для работы администратора предназначен раздел «**Администрирование**» и подраздел «**Отчёты**» → «**Диагностика**».

Подробное описание всех разделов веб-интерфейса Подсистемы мониторинга (кроме раздела «Администрирование») и правила работы приведены в документе «*Подсистема мониторинга «Горизонт-ВС». Руководство пользователя*».

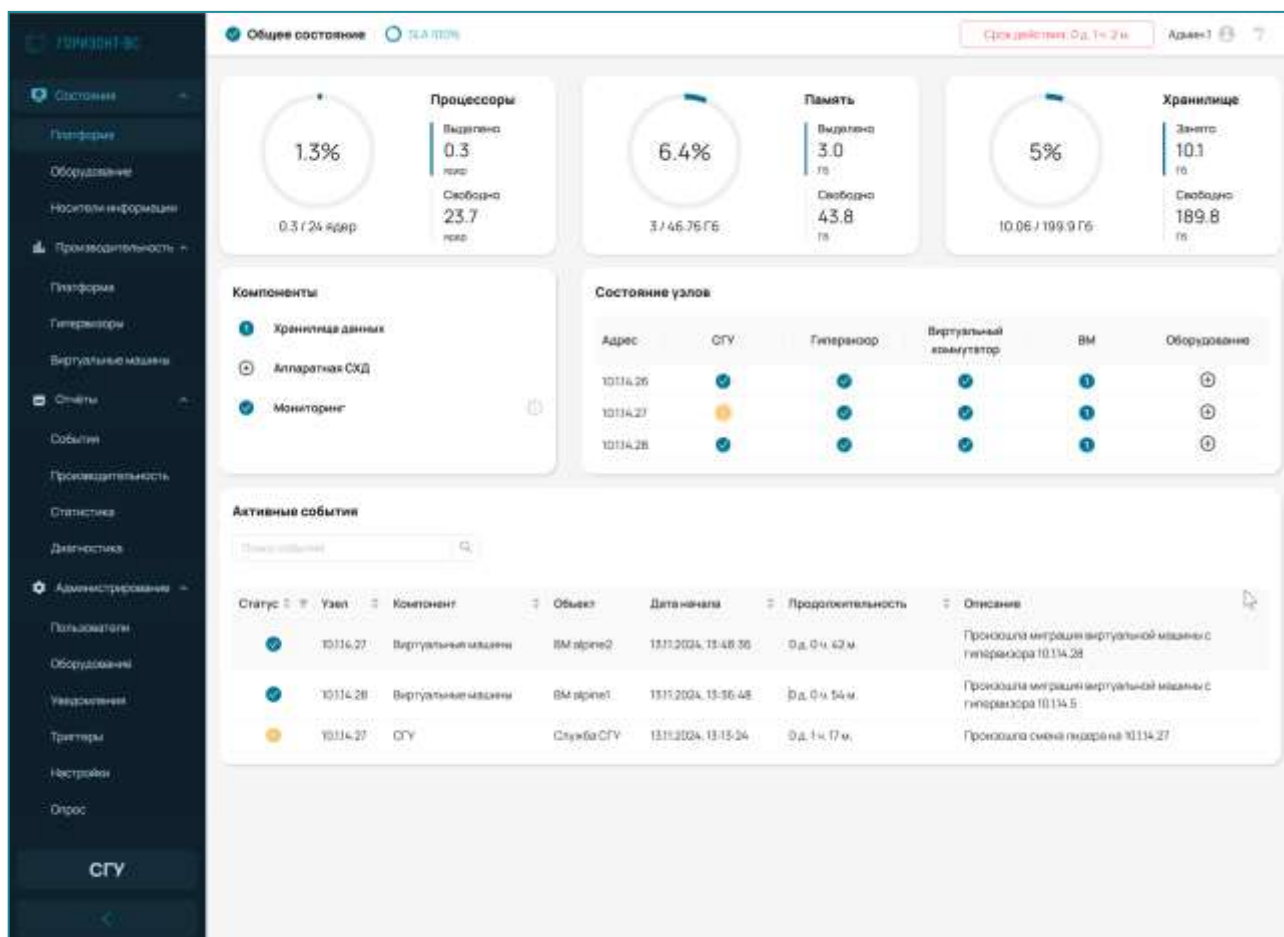


Рисунок 676 - Стартовая страница веб-интерфейса Подсистемы мониторинга (при использовании пробной версии ПО Подсистемы мониторинга)

8.7.2 Перечень функций администратора в веб-интерфейсе Подсистемы мониторинга «Горизонт-ВС»

Основные функции администратора при работе в Подсистеме мониторинга:

- 1) Управление пользователями Подсистемы мониторинга – подраздел **«Администрирование»** → **«Пользователи»**.
- 2) Настройка мониторинга состояния оборудования «Горизонт-ВС» по протоколу IPMI или с использованием Ping – подраздел **«Администрирование»** → **«Оборудование»**.

- 3) Настройка правил отправки пользователям уведомлений о событиях, произошедших в Подсистеме мониторинга – подраздел **«Администрирование» → «Уведомления»**.
- 4) Создание и настройка правил отслеживания, позволяющих контролировать достижение пороговых значений различных метрик Системы виртуализации «Горизонт-ВС» – подраздел **«Администрирование» → «Триггеры»**.
- 5) Настройка подключения к почтовому серверу Подсистемы мониторинга – подраздел **«Администрирование» → «Настройки»**.
- 6) Настройка интеграции с системой мониторинга Zabbix – подраздел **«Администрирование» → «Настройки»**.
- 7) Настройка отправки зафиксированных событий по протоколу Syslog – подраздел **«Администрирование» → «Настройки»**.
- 8) Настройка отправки зафиксированных событий в виде SNMP trap сообщений – подраздел **«Администрирование» → «Настройки»**.
- 9) Изменение учётной записи (УЗ), используемой для подключения к СГУ – подраздел **«Администрирование» → «Настройки»**.
- 10) Замена SSH ключа для подключения к гипервизорам – подраздел **«Администрирование» → «Настройки»**.
- 11) Быстрое восстановление настроек Подсистемы мониторинга в случае полной переустановки или сброса существующих настроек путем импорта сохранённых ранее конфигураций Подсистемы мониторинга – подраздел **«Администрирование» → «Настройки»**.
- 12) Экспорт конфигураций Подсистемы мониторинга в файлы формата .json – подраздел **«Администрирование» → «Настройки»**.
- 13) Отключение Подсистемы мониторинга от СГУ для сброса настроек и переподключения к иному СГУ – подраздел **«Администрирование» → «Настройки»**.

- 14) Управление опросом объектов мониторинга – настройка параметров частоты опроса, запуск/остановка мониторинга объектов в составе системы виртуализации – подраздел **«Администрирование»** → **«Опрос»**.
- 15) Формирование и выгрузка диагностических отчётов состояния Системы виртуализации «Горизонт-ВС» и входящих в её состав компонентов – **«Отчёты»** → **«Диагностика»**.

8.7.3 Управление пользователями

8.7.3.1 Доступ к функции. Назначение и состав подраздела «Пользователи»

Управление пользователями Подсистемы мониторинга «Горизонт-ВС» осуществляет в подразделе **«Администрирование»** → **«Пользователи»**.

В подразделе отображается следующая информация:

- табличный список пользователей, зарегистрированных в Подсистеме мониторинга «Горизонт-ВС»;
- функция добавления нового пользователя в подсистему мониторинга;
- функция удаления пользователя из Подсистемы;
- функция просмотра и редактирования данных пользователя.

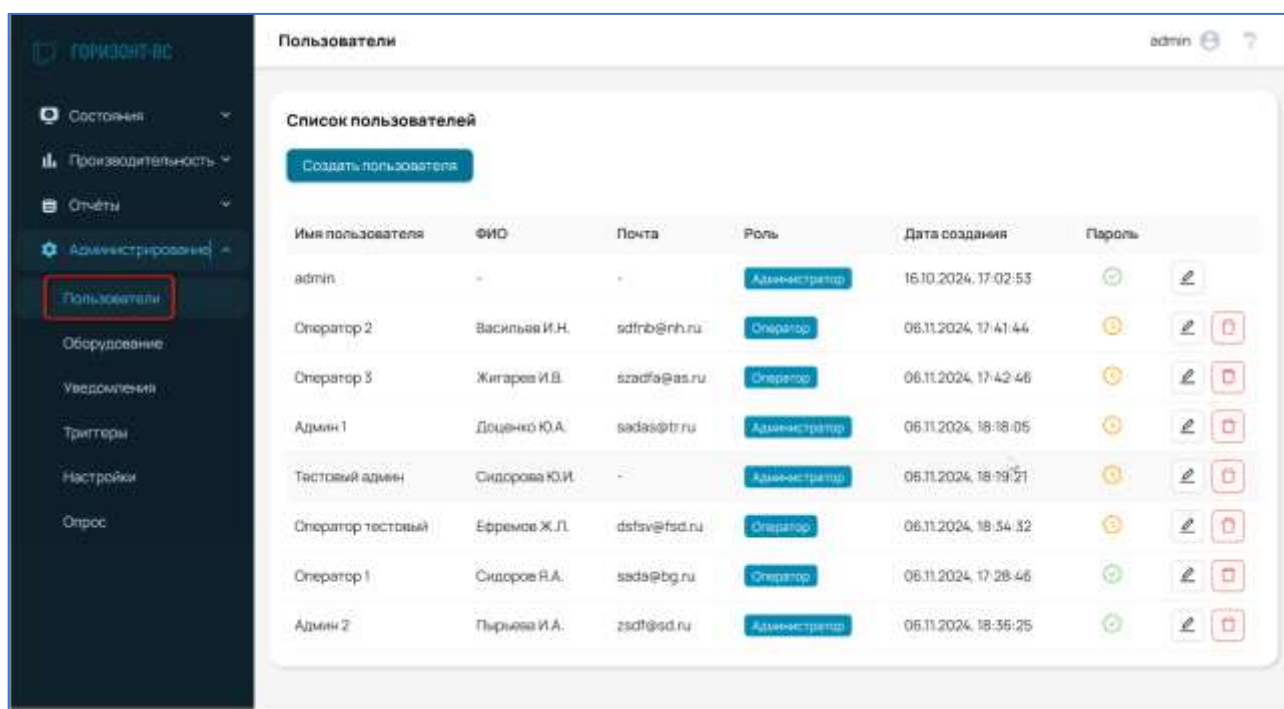


Рисунок 677 - Список пользователей Подсистемы мониторинга

8.7.3.2 Список пользователей

Список пользователей представляет собой табличный список, в котором для каждого пользователя указываются следующие параметры:

- **Имя пользователя** – логин пользователя в Подсистеме мониторинга;
- **ФИО** – фамилия, имя, отчество зарегистрированного пользователя;
- **Почта** – электронная почта пользователя;
- **Роль** – роль пользователя при работе с Подсистемой мониторинга – Администратор/Оператор;
- **Дата создания** – дата создания пользователя в Подсистеме мониторинга в формате: «дд.мм.гггг, чч:мм:сс»;
- **Пароль** – статус пароля пользователя:
 - 🟢 – постоянный;
 - 🟡 – временный (требуется смена пароля);

-  – функция просмотра данных пользователя и редактирования роли пользователя;
-  – функция удаления пользователя.

8.7.3.3 Добавление нового пользователя

Для добавления нового пользователя в Подсистему мониторинга необходимо выполнить следующие действия:

- 1) Щелкнуть по функции **Создать пользователя**.
- 2) В открывшейся форме «Создание пользователя» указать следующие данные нового пользователя (см. **Ошибка! Источник ссылки не найден.**):
 - **Имя пользователя** – имя пользователя в Подсистеме мониторинга (логин).
 - **Роль** – роль пользователя, определяющая права пользователя при работе в Подсистеме мониторинга: Администратор/Оператор. Выбирается из раскрывающегося списка.
 - **Пароль** – временный пароль нового пользователя для входа в Подсистему мониторинга (не менее 6 символов).
 - **Повторите пароль** – подтверждение временного пароля.
 - **ФИО** – фамилия, имя и отчество нового пользователя (необязательное поле).
 - **Почта** – электронная почта пользователя (необязательное поле).
- 3) Нажать кнопку **Создать** для создания в Подсистеме мониторинга пользователя с указанными данными.

На экране должно появиться всплывающее сообщение об успешном создании пользователя. Новый пользователь должен отобразиться в списке пользователей.

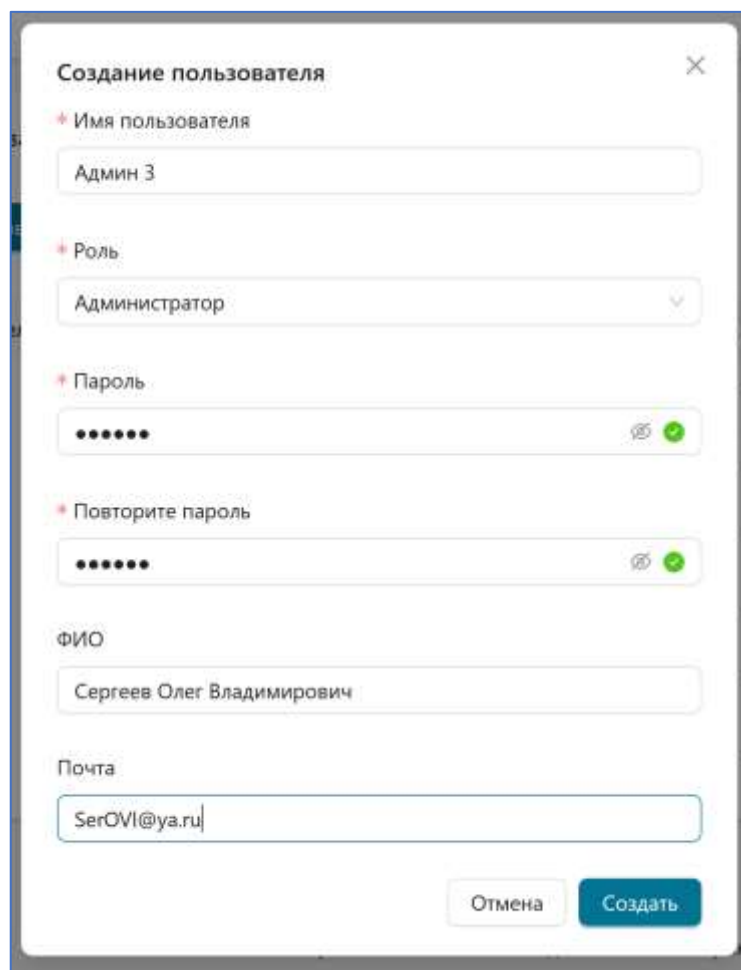


Рисунок 678 - Список пользователей Подсистемы мониторинга

8.7.3.4 Удаление пользователя

Для удаления пользователя из Подсистемы мониторинга необходимо:

- 1) В списке пользователей щелкнуть по значку  в строке удаляемого пользователя.
- 2) В открывшемся окне подтверждения щелкнуть **Подтверждаю**.

Должно появиться всплывающее сообщение об успешном удалении пользователя. Строка данного пользователя должна быть удалена из списка пользователей Подсистемы мониторинга.

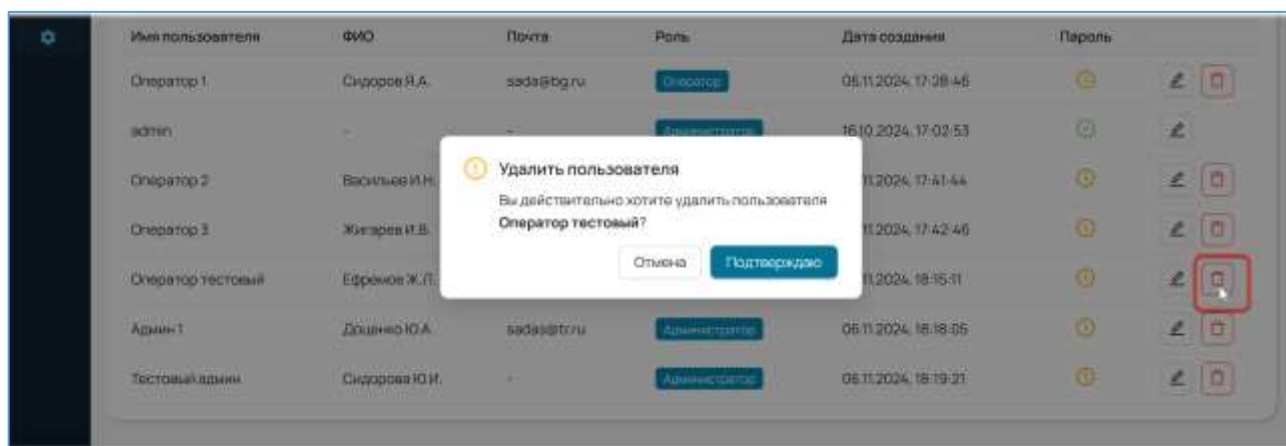


Рисунок 679 - Удаление пользователя

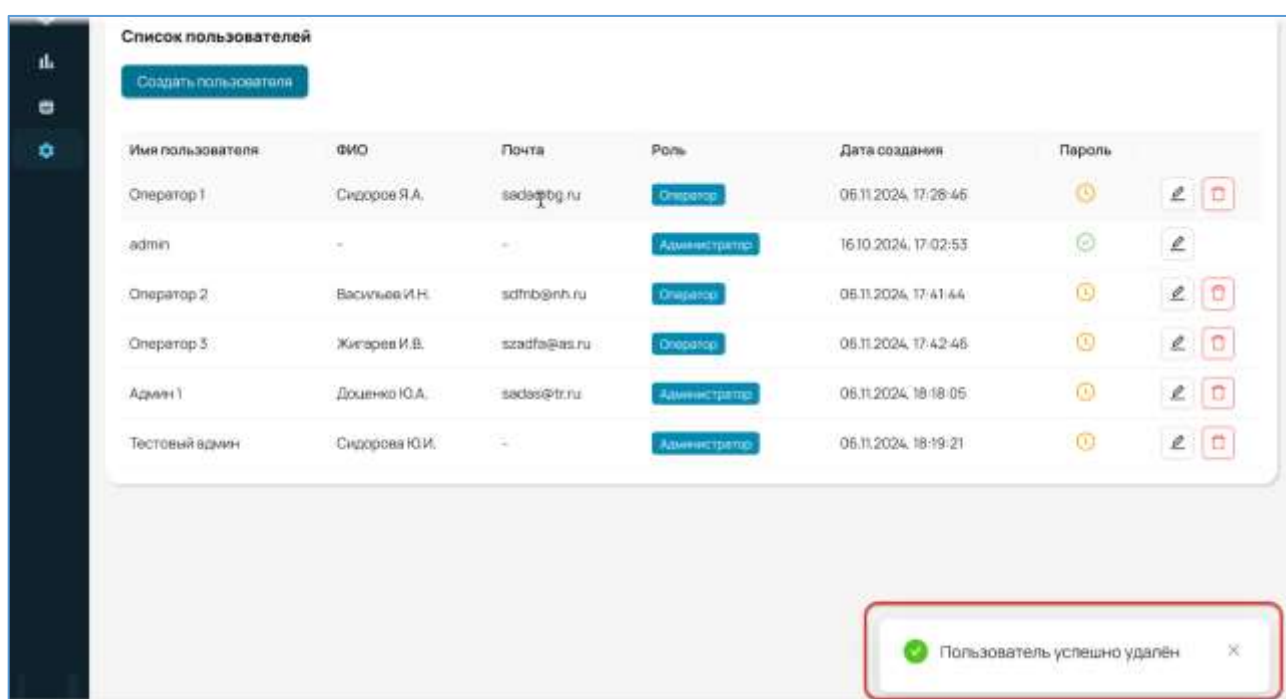


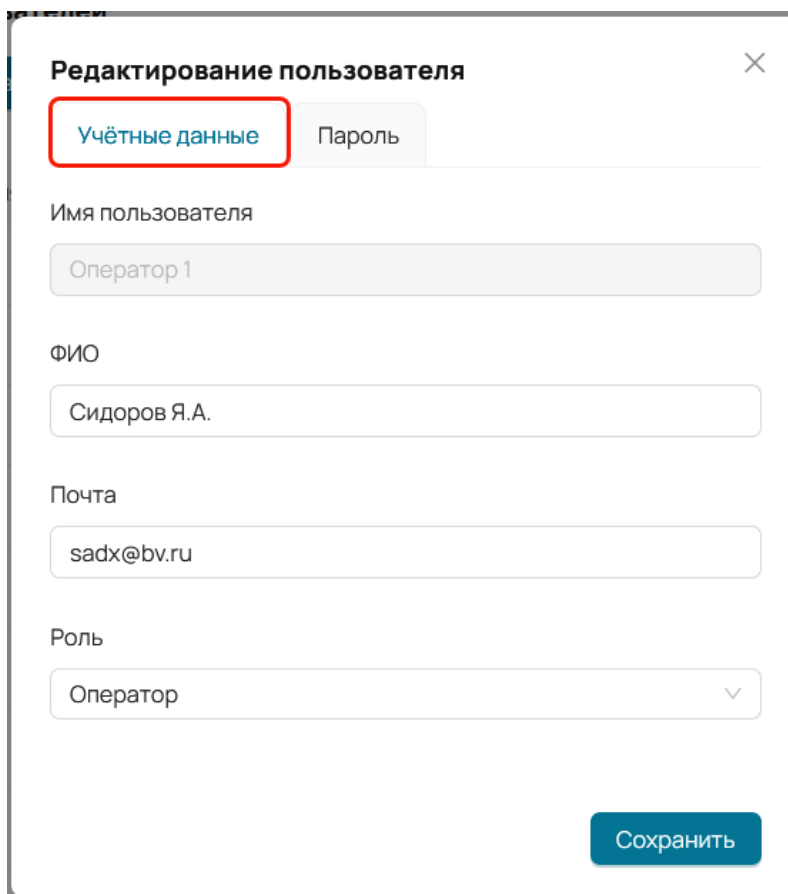
Рисунок 680 - Сообщение об удалении пользователя

8.7.3.5 Просмотр и редактирование данных пользователя

При необходимости просмотра и редактирования данных пользователя надо в списке пользователей Подсистемы мониторинга щелкнуть по значку  в строке интересующего пользователя. Откроется окно **«Редактирование пользователя»** состоящее из двух вкладок: **Учётные данные** и **Пароль**.

Вкладка **Учётные данные** предназначена для редактирования параметров учётной записи выбранного пользователя. На данной вкладке администратор может отредактировать такие параметры пользователя как **ФИО**, **Почта**, выбрать новую роль в списке **Роль**. Параметр **Имя пользователя** является неизменяемым. Для сохранения сделанных изменений в учётной записи пользователя нажать кнопку **Сохранить**.

Вкладка **Пароль** предназначена для смены пароля у выбранного пользователя. Используется стандартный алгоритм смены пароля. Для сохранения нового пароля пользователя нажать кнопку **Сохранить**.



The image shows a modal window titled "Редактирование пользователя" (Edit User) with a close button (X) in the top right corner. It contains two tabs: "Учётные данные" (Account Data), which is selected and highlighted with a red rectangle, and "Пароль" (Password). The "Учётные данные" tab contains the following fields:

- Имя пользователя** (Username): A text input field with the value "Оператор 1".
- ФИО** (Full Name): A text input field with the value "Сидоров Я.А."
- Почта** (Email): A text input field with the value "sadx@bv.ru".
- Роль** (Role): A dropdown menu with the value "Оператор" and a downward arrow.

A blue button labeled "Сохранить" (Save) is located at the bottom right of the dialog.

Рисунок 681 - Редактирование учётных данных пользователя

Рисунок 682 - Редактирование пароля пользователя

8.7.3.6 Смена временного пароля

Вновь созданному пользователю не зависимо от роли присваивается временный пароль. В списке пользователей временный статус пароля отображается оранжевым значком — 🕒 .

При входе в Подсистему мониторинга под учетной записью с временным паролем:

- профиль пользователя отмечается оранжевой меткой в виде точки;
- на экране отображается во всплывающем окне предупреждение о временном пароле и необходимости его смены.

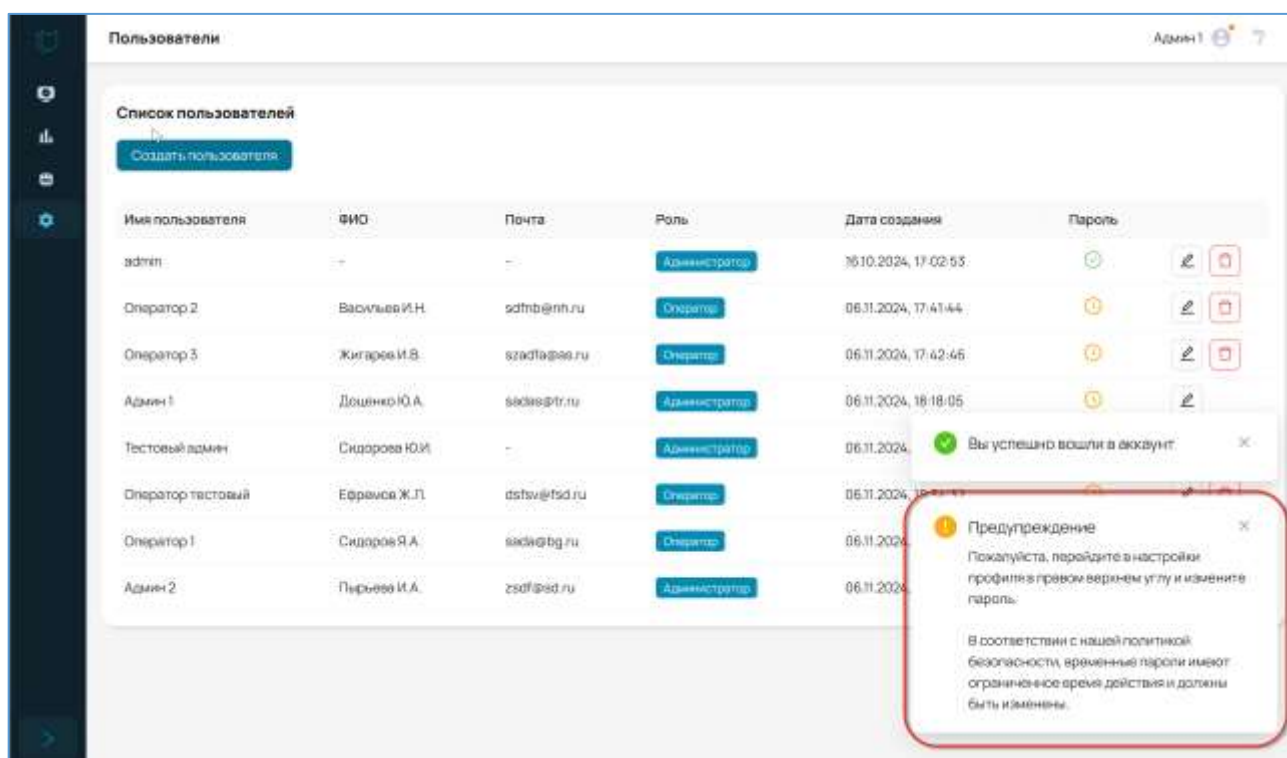


Рисунок 683 - Отображение в интерфейсе пользователя с временным паролем

Для смены пароля с временного на постоянный, пользователю необходимо:

- 1) Зайти в Подсистему мониторинга под своей учетной записью (имеющей временный пароль).
- 2) Зайти в профиль пользователя, выбрав в раскрывающемся меню строку **Профиль**.



Рисунок 684- Профиль временного пользователя

- 3) В открывшемся окне профиля выбрать вкладку **Пароль** и указать новый пароль.

Профиль

Общее Учётные данные Пароль

Предупреждение

В соответствии с нашей политикой безопасности, временные пароли имеют ограниченное время действия и должны быть изменены.

* Новый пароль

.....

* Повторить новый пароль

.....

Сохранить

Рисунок 685 - Смена пароля

После смены временного пароля оранжевая метка возле данных пользователя будет удалена.

В веб-интерфейсе администратора в списке пользователей («Администрирование» → «Пользователи») данный пользователь будет отображаться как пользователь с постоянным паролем – в поле **Пароль** будет отображаться зелёный значок .

Так же при необходимости изменить временный пароль пользователя может администратор, используя функцию редактирования данных пользователя – см. п.0.

8.7.4 Настройка мониторинга оборудования «Горизонт-ВС»

8.7.4.1 Доступ к функции

Настройки мониторинга оборудования «Горизонт-ВС» доступны:

- В подразделе интерфейса **«Администрирование»** → **«Оборудование»**:
 - просмотр списка подключенного оборудования;
 - подключение нового оборудования к Подсистеме мониторинга;
 - отключение оборудования от Подсистемы мониторинга;
 - редактирование параметров подключённого оборудования.
- В подразделе **«Состояния»** → **«Платформа»**: подключение оборудования к подсистеме мониторинга.

Функция предназначена для постановки на мониторинг следующего типа оборудования, используемого для размещения объектов «Горизонт-ВС»: **Серверы и аппаратная СХД**.

8.7.4.2 Настройка мониторинга оборудования «Горизонт-ВС» в разделе интерфейса «Администрирование»

Назначение и состав подраздела

Подраздел **«Администрирование»** → **«Оборудование»** содержит следующие данные:

- табличный список оборудования, подключенного к Подсистеме мониторинга на текущий момент времени;
- функция подключения нового оборудования к Подсистеме мониторинга;
- функция просмотра и редактирования параметров подключения оборудования;
- функция отключения оборудования от Подсистемы мониторинга;

- функция отображения пароля, по которому происходит подключение к оборудованию.

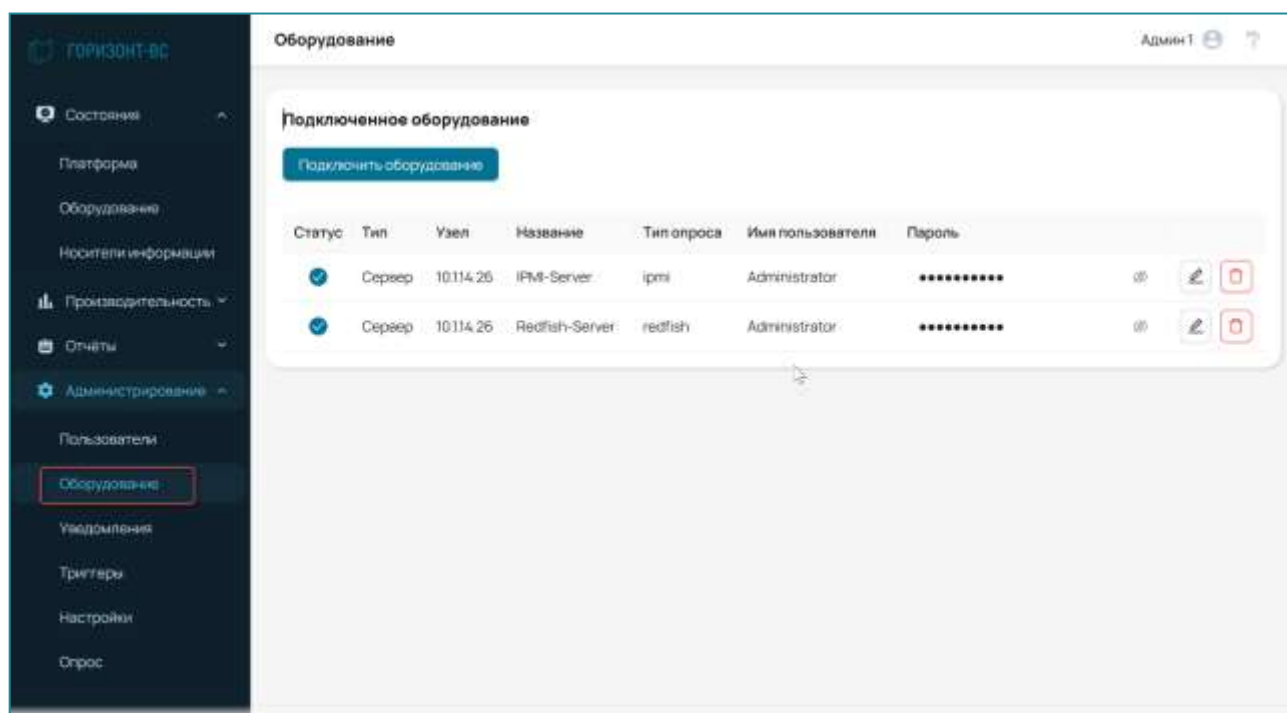


Рисунок 686 - Раздел интерфейса для настройки подключения оборудования

Список оборудования, подключенного к Подсистеме мониторинга

Список оборудования, подключённого к Подсистеме мониторинга, представляет собой табличный список, в котором для каждого объекта указываются следующие параметры:

- **Статус** – цветовой маркер текущего состояния объекта.
- **Тип** – тип оборудования: Сервер или аппаратная СХД.
- **Узел** – IP-адрес или доменное имя гипервизора, размещенного на данном оборудовании. Для СХД не указывается.
- **Название** – уникальное название оборудования в Подсистеме мониторинга.
- **Тип опроса** – используемый тип опроса: Ping или IPMI.

- **Имя пользователя** – логин пользователя для доступа к оборудованию при использовании IPMI.
- **Пароль** – пароль пользователя для доступа к оборудованию при использовании IPMI.
-  – функция визуализации пароля пользователя для доступа к оборудованию при использовании IPMI.
-  – функция просмотра и редактирования параметров подключения оборудования;
-  – функция отключения оборудования от Подсистемы мониторинга.

Если объект был подключен с использованием нескольких протоколов, то в списке подключений для каждого подключения объекта будут созданы свои строки.

Подключение нового оборудования

Для подключения нового оборудования к Подсистеме мониторинга необходимо выполнить следующие действия:

- 1) Щелкнуть по функции **Подключить оборудование**.
- 2) В открывшемся бланке «Подключение оборудования» указать следующие параметры нового подключения (см. **Ошибка! Источник ссылки не найден.**):
 - **Название** – указать уникальное название оборудования, которое будет отображаться в веб-интерфейсе Подсистемы мониторинга.
 - **Тип оборудования** – в раскрывающемся списке выбрать тип оборудования. Доступны следующие типы: Сервер, Аппаратная СХД.
 - **Узел** – выбрать из раскрывающегося списка IP-адрес или доменное имя гипервизора, размещенного на подключаемом оборудовании. Для СХД данный параметр не указывается.

- **Адрес** – указать адрес для проведения опроса по Ping/ IPMI/ Redfish.
- **Опрос** – в раскрывающемся списке выбрать тип опроса оборудования. Доступны следующие значения: Ping, IPMI и Redfish.
- **Частота опроса** – в раскрывающемся списке выбрать период опроса. Доступны следующие значения: 1 мин., 2 мин., 5 мин., 10 мин., 15 мин, 20 мин., 25 мин. и 30 мин.
- **Имя пользователя** – указать логин пользователя для доступа к оборудованию по IPMI или Redfish.
- **Пароль** – указать пароль пользователя для доступа к оборудованию по IPMI или Redfish.

3) Нажать кнопку **Подключить** для создания в Подсистеме мониторинга нового подключения оборудования.

На экране должно появиться всплывающее сообщение об успешном подключении оборудования. Новый объект должен отобразиться в списке оборудования, подключенного к Подсистеме мониторинга.

Подключение оборудования

* Название
Сервер 1

* Тип оборудования
Сервер

* Узел
10.114.26

* Адрес
Укажите адрес для опроса по ipmi/ping

* Опрос
Redfish

* Частота опроса
5 мин.

* Имя пользователя
Админ 1
Имя пользователя для IPMI/Redfish

* Пароль
.....
Пароль для IPMI/Redfish

Отмена Подключить

Рисунок 687 - Форма для создания нового подключения оборудования к Подсистеме мониторинга «Горизонт-ВС» на примере сервера

В результате подключения оборудования в подразделе **«Состояния»** → **«Оборудование»** отобразятся данные мониторинга этого оборудования .

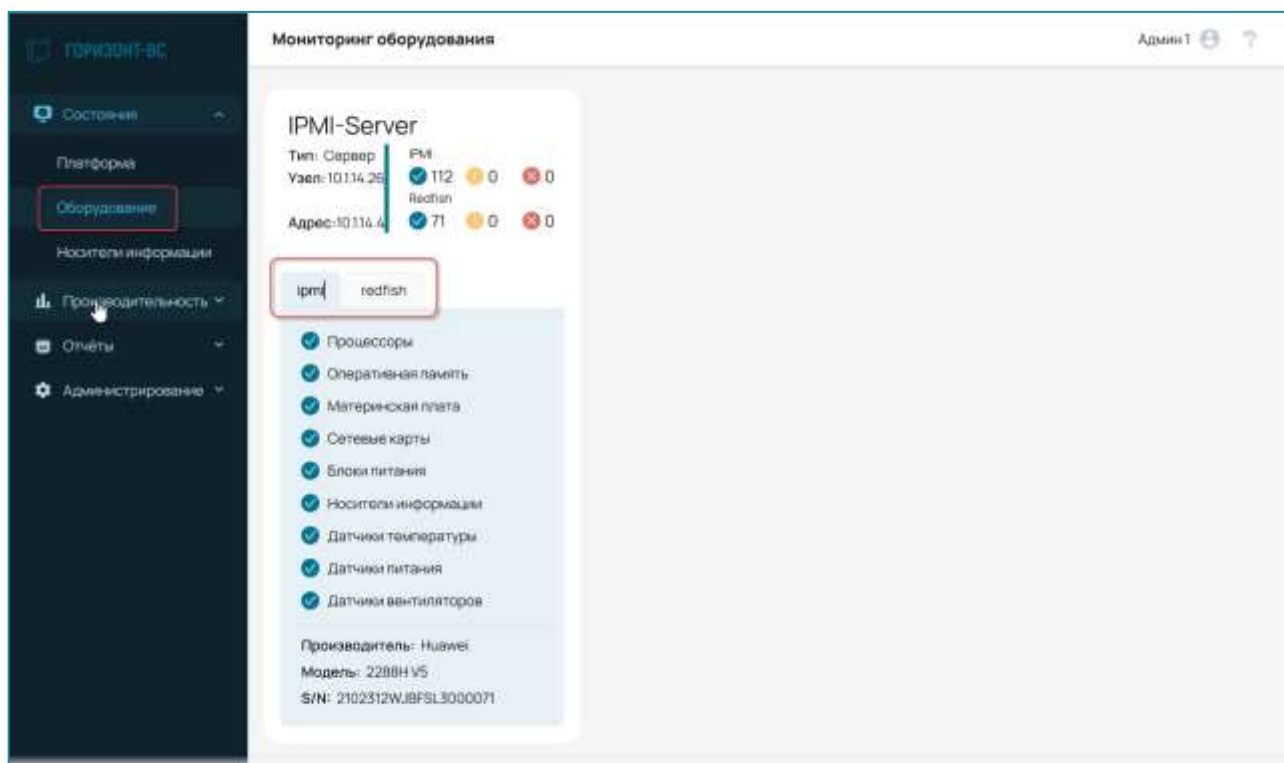


Рисунок 688 - Пример мониторинга сервера по протоколам IPMI и Redfish

Отключение оборудования от Подсистемы мониторинга

Для отключения оборудования от Подсистемы мониторинга необходимо выполнить следующие действия:

- 1) В списке подключённого оборудования щелкнуть по значку  в строке оборудования, которое требуется отключить.
- 2) В открывшемся окне подтверждения щелкнуть **Подтверждаю**.

Должно появиться всплывающее сообщение об успешном отключении оборудования: «Оборудование успешно снято с мониторинга».

Строка параметров данного оборудования должна быть удалена из списка оборудования, подключённого к Подсистеме мониторинга.

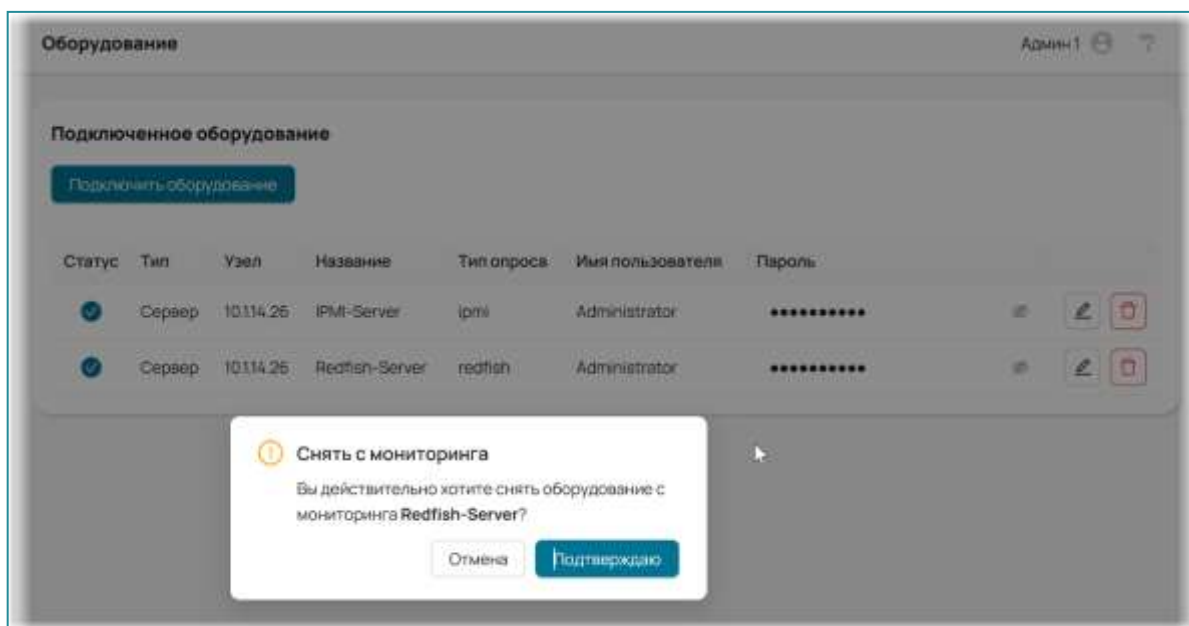


Рисунок 689 - Отключение оборудования от Подсистемы мониторинга

Просмотр и редактирование параметров подключения оборудования

При необходимости просмотра и редактирования параметров подключения оборудования необходимо выполнить следующие действия:

- 1) В списке подключённого оборудования щелкнуть по значку  в строке интересующего объекта. Откроется окно **«Редактирование подключения»** (см. **Ошибка! Источник ссылки не найден.**).
- 2) Внести необходимые корректировки в параметры подключения.

Для корректировки доступны все параметры кроме (см. **Ошибка! Источник ссылки не найден.**): **Название** (название объекта в Подсистеме мониторинга), **Тип оборудования**, **Узел** (только для объектов типа Сервер) и **Опрос**.

- 3) Для сохранения изменений нажать кнопку **Сохранить**.

Если изменения в параметры подключения были внесены правильно, то на экране должно отобразиться окно подтверждения сохранения новых данных подключения.



The image shows a dialog box titled "Редактирование подключения" (Edit connection) with a close button (X) in the top right corner. The dialog contains several form fields, each preceded by a red square icon:

- Название** (Name): A text input field containing "IPMI-Server".
- Тип оборудования** (Equipment type): A dropdown menu with "Сервер" (Server) selected.
- Узел** (Node): A dropdown menu with "10.114.25" selected.
- Адрес** (Address): A text input field containing "10.114.4" with a cursor at the end.
- Опрос** (Query): A dropdown menu with "IPMI" selected.
- Имя пользователя** (Username): A text input field containing "Administrator". Below this field is the text "Имя пользователя для IPMI/Redfish".
- Пароль** (Password): A password input field with masked characters (dots) and a toggle icon on the right. Below this field is the text "Пароль для IPMI/Redfish".

At the bottom right of the dialog are two buttons: "Отмена" (Cancel) and "Сохранить" (Save).

Рисунок 690 - Редактирование параметров подключения

8.7.4.3 Подключение оборудования из раздела интерфейса «Состояния»

Пользователь с правами администратора может совершить подключение оборудования к Подсистеме мониторинга из раздела «Состояния» → «Платформа»¹.

На данной странице реализованы следующие функции подключения оборудования:

- Подключение серверов – реализовано в области «Состояние узлов» в поле **Оборудование** в виде функционального значка . Подключенное оборудование обозначено значком .
- Подключение аппаратной СХД – реализовано в области «Компоненты» в строке **Аппаратная СХД** в виде функционального значка . Если СХД уже подключено, то в строке СХД будет стоять значок .

¹ Данная функция недоступна для пользователей с правами оператора Подсистемы мониторинга

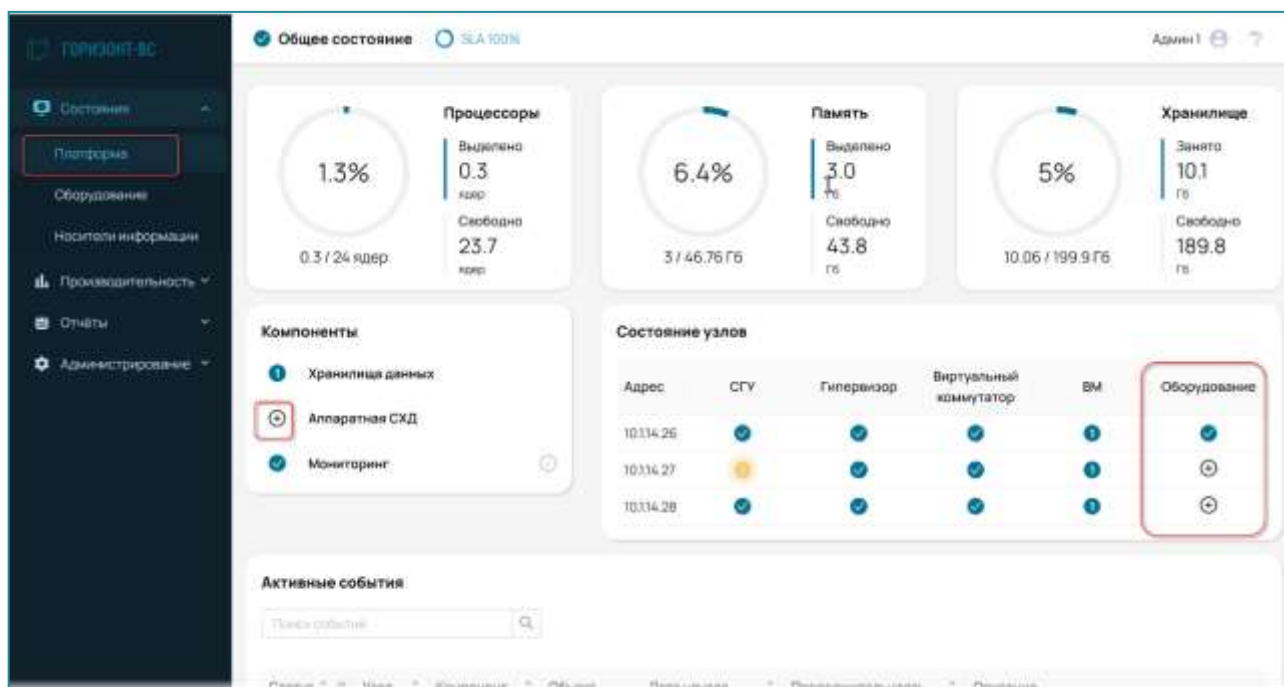


Рисунок 691 - Функции подключения оборудования на странице интерфейса «Состояния» → «Платформа»

Для подключения нового оборудования к Подсистеме мониторинга необходимо:

- 1) Щёлкнуть по значку  в строке узла или компонента аппаратного СХД, у которого необходимо подключить оборудование. На экране откроется бланк подключения оборудования, аналогичный бланку подключения в разделе интерфейса «Администрирование» → «Оборудование».
- 2) Указать параметры подключения. Подробное описание установки параметров приведено в п.0.
- 3) Нажать кнопку **Подключить**.

В строке узла или компонента с подключаемым оборудованием значок  должен измениться на . Подключенное оборудование должно отобразиться в разделе **«Состояния» → «Оборудование»**.

Примечание. Функция отключения оборудования от Подсистемы мониторинга и функция редактирования параметров подключения оборудования в данном подразделе интерфейса недоступны.

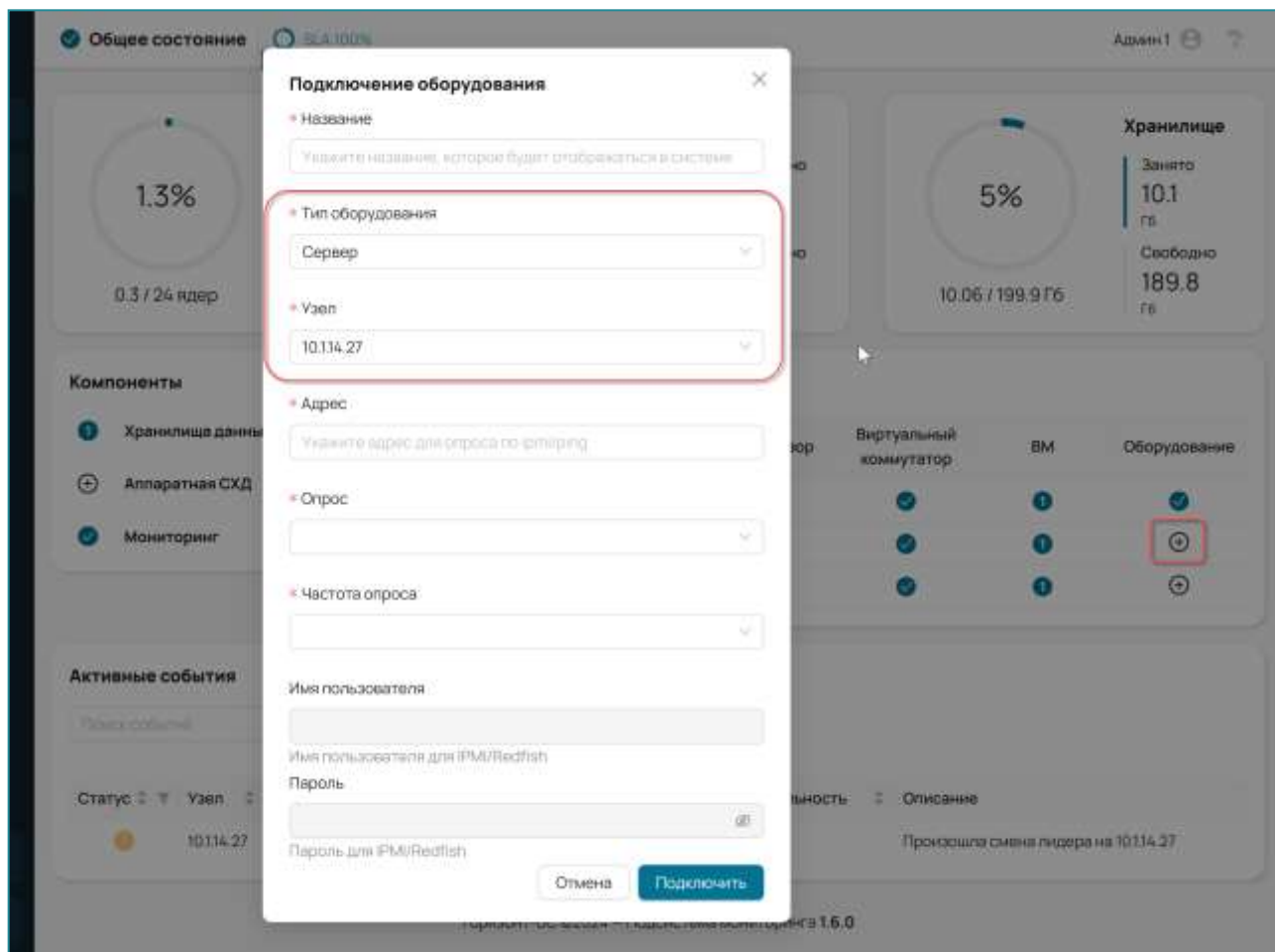


Рисунок 692 - Бланк подключения оборудования

8.7.5 Настройка системы рассылки уведомлений

8.7.5.1 Доступ к функции. Назначение и состав

Настройки системы рассылки уведомлений Подсистемы мониторинга доступны в подразделе интерфейса **«Администрирование»** → **«Уведомления»**. Раздел состоит из двух областей:

- 1) «**Группы адресатов**» – область предназначена для формирования групп пользователей адресатов для той или иной рассылки уведомлений. Включает в себя табличный список групп адресатов рассылки, функции создания, редактирования и удаления групп адресатов рассылки.
- 2) «**Рассылки**» – область предназначена для формирования системы уведомлений для рассылки. Включает в себя табличный список текущих рассылок, функции создания, редактирования и удаления рассылок.

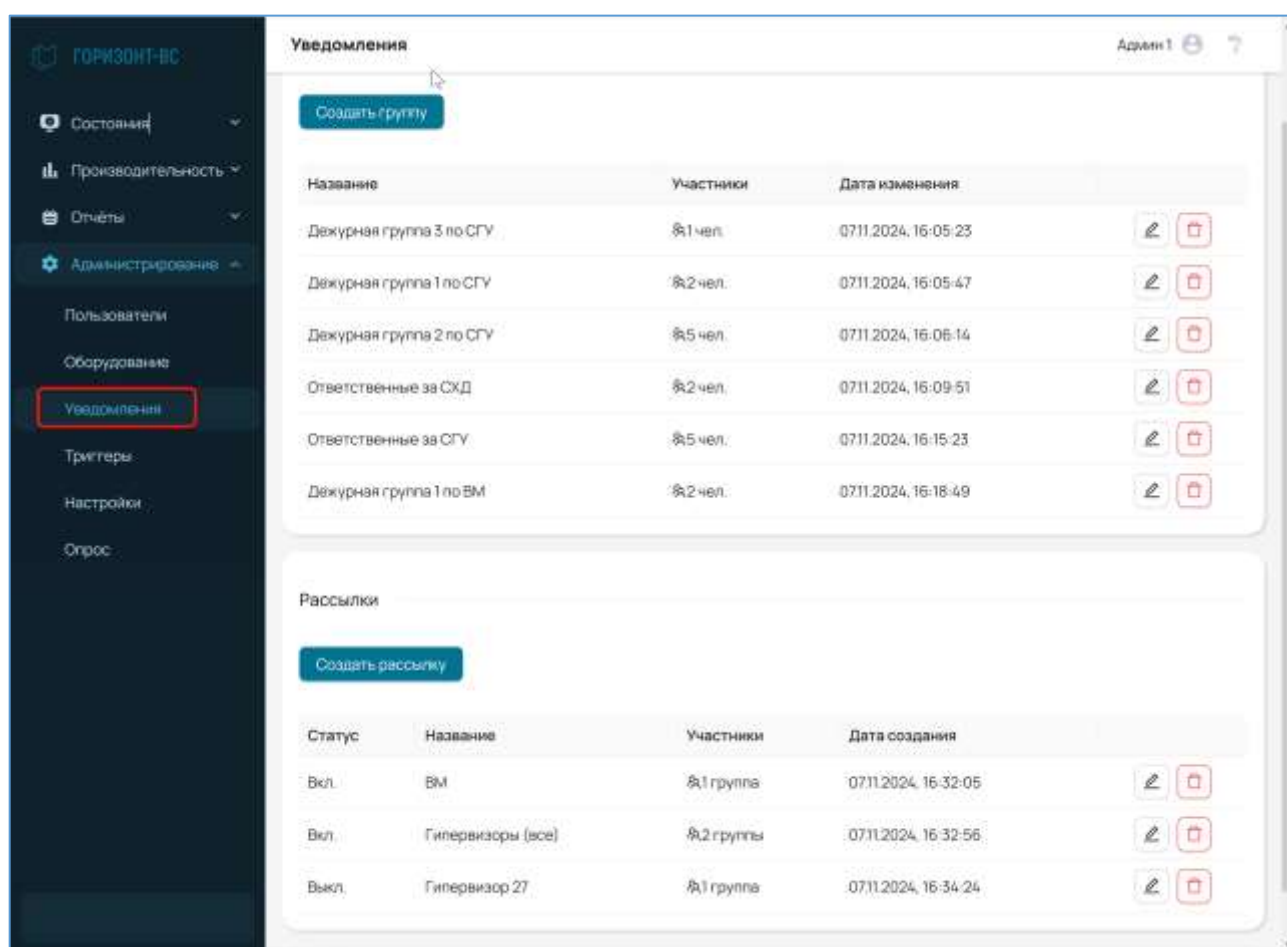


Рисунок 693 - Раздел интерфейса для настройки системы рассылки уведомлений

8.7.5.2 Управление группами адресатов рассылки

Список групп адресатов рассылки

Список групп адресатов рассылки представляет собой табличный список, в котором для каждой группы указываются следующие параметры:

- **Название** – название группы адресатов рассылки в Подсистеме мониторинга;
- **Участники** – количество участников в группе;
- **Дата изменения** – дата последнего изменения параметров группы в Подсистеме мониторинга в формате: «дд.мм.гггг, чч:мм:сс»;
-  – функция просмотра и редактирования данных группы;
-  – функция удаления группы.

Создание новой группы адресатов рассылки

Для создания новой группы адресатов рассылки необходимо выполнить следующие действия:

- 1) Нажать кнопку **Создать группу**. Откроет форма для формирования новой группы адресатов рассылки – «Создание группы».
- 2) В открывшейся форме в поле **Название** ввести название группы.
- 3) В области «Доступно», содержащей список доступных пользователей Подсистемы мониторинга, установить флажки возле пользователей, которые должны войти в состав группы.

Более подробно работа со списками пользователей в областях «Доступно» и «Выбрано» приведена в Приложении А.

Создание группы

Название

Доступно

2/7 элем.

Поиск

Имя пользователя	Почта	Роль
☐ test	-	Администратор
☒ Оператор 1	-	Оператор
☒ Админ 2	-	Администратор
☐ iv	wdeaq@ghcf.ru	Оператор
☐ Админ 3	SerOVI@ya.ru	Администратор
☐ Adm	mda04B00903@ya.ru	Администратор
☐ admin	asdfa@sva.com	Администратор

Выбрано

0 элем.

Поиск

Имя пользователя Почта Роль

Нет данных

Отмена Создать

Рисунок 694 - Форма для создания новой группы адресатов рассылки

- 4) Нажать значок , расположенный между областями «Доступно» и «Выбрано». Выбранные в области «Доступно» пользователи будут перенесены в область «Выбрано».
- 5) Для завершения формирования группы адресатов рассылки нажать кнопку **Создать**.

На экране должно появиться всплывающее сообщение об успешном создании группы. Новая группа должна отобразиться в списке групп адресатов рассылки.

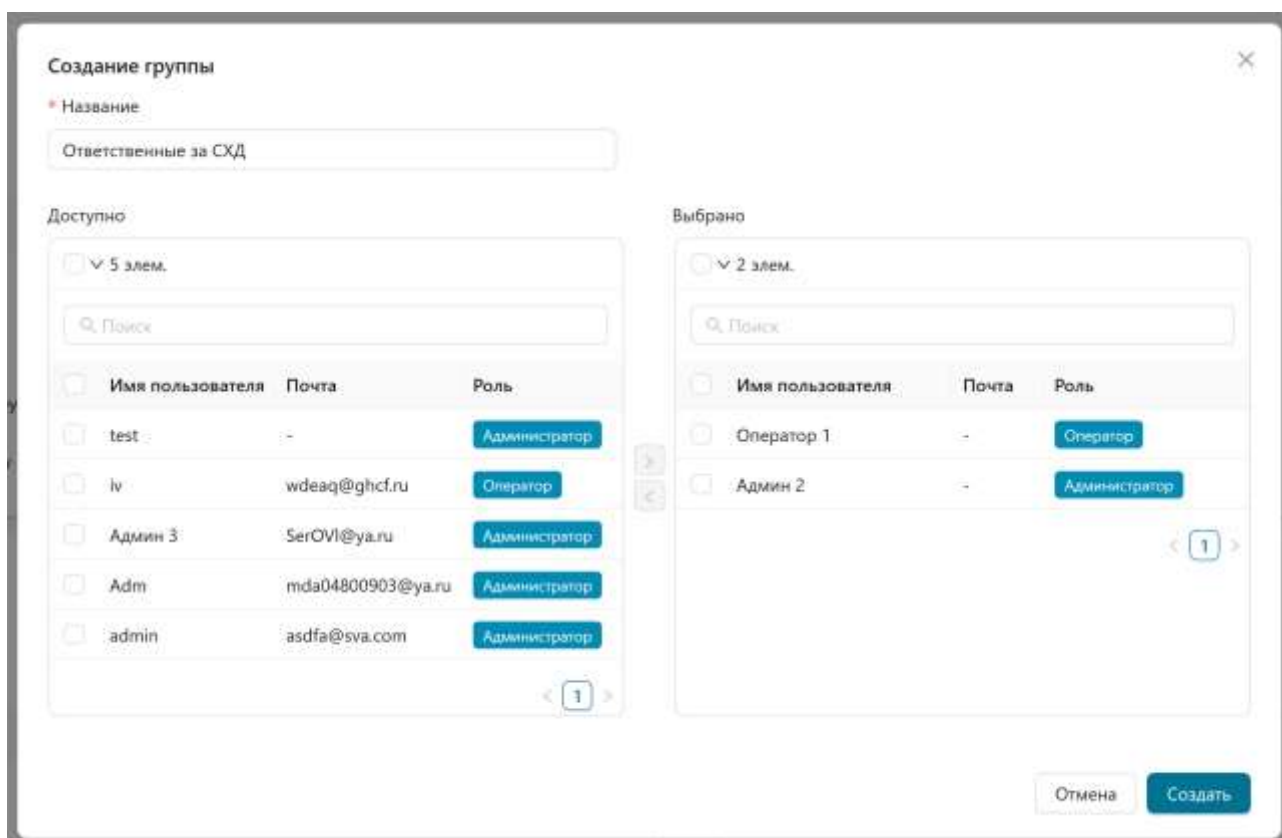


Рисунок 695 - Создание списка пользователей для новой группы адресатов рассылки

Редактирование данных группы адресатов рассылки

При необходимости для группы адресатов рассылки возможно отредактировать состав участников.

Для редактирования состава участников группы необходимо щелкнуть по значку  в строке данной группы. В результате действий откроется форма для редактирования состава группы, аналогичная форме создания группы. Имя группы в поле **Название** для редактирования недоступно.

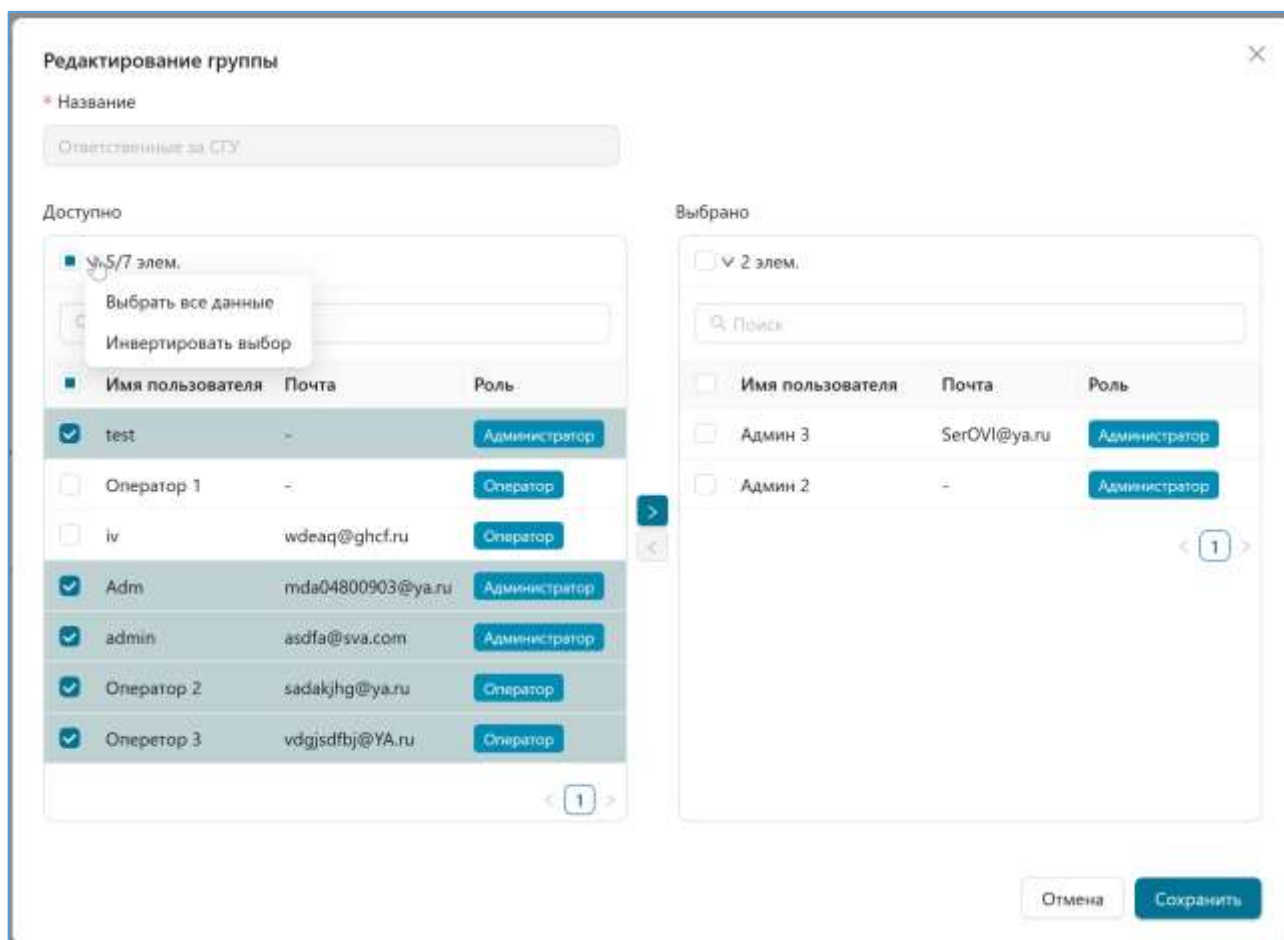


Рисунок 696 - Редактирование состава группы

Для **добавления новых пользователей** в редактируемую группу необходимо:

- 1) В области «Доступно» отметить нужных пользователей флажками (см. **Ошибка! Источник ссылки не найден.**). После чего станет доступным значок переноса  выбранных пользователей в список пользователей группы в области «Выбрано» (подробное описание областей со списками – см. Приложение А).
- 2) Нажать значок . Выбранные в области «Доступно» пользователи будут перенесены в область «Выбрано».
- 3) Для сохранения сделанных изменений нажать кнопку **Сохранить**.

В результате проведенных действий на экране должно появиться всплывающее сообщение об успешном изменении группы. В списке групп у

отредактированной группы в поле **Участники** должно отобразиться новое количество участников.

Для **удаления пользователей** из редактируемой группы необходимо:

- 1) В области «Выбрано» отметить удаляемых пользователей флажками. После чего станет доступным значок переноса  выбранных пользователей из списка группы в общий список пользователей в области «Доступно» (подробное описание областей со списками – см. Приложение А).
- 2) Нажать значок . Указанные в области «Выбрано» пользователи будут перенесены в область «Доступно».
- 3) Для сохранения сделанных изменений нажать кнопку **Сохранить**.

В результате проведенных действий на экране должно появиться всплывающее сообщение об успешном изменении группы. В списке групп у отредактированной группы в поле **Участники** должно отобразиться новое количество участников.

Удаление группы адресатов рассылки

Для удаления группы адресатов рассылки из Подсистемы мониторинга необходимо:

- 1) В списке групп щелкнуть по значку  в строке удаляемой группы.
- 2) В открывшемся окне подтверждения щелкнуть **Подтверждаю**.

Должно появиться всплывающее сообщение об успешном удалении группы адресатов рассылки.

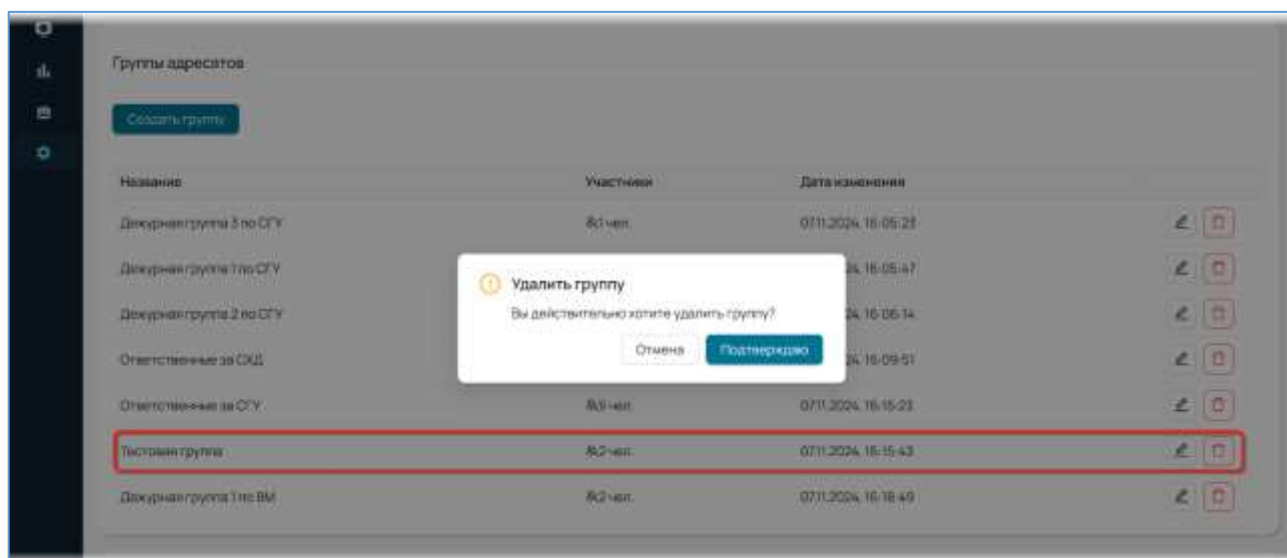


Рисунок 697 - Удаление группы адресатов рассылки

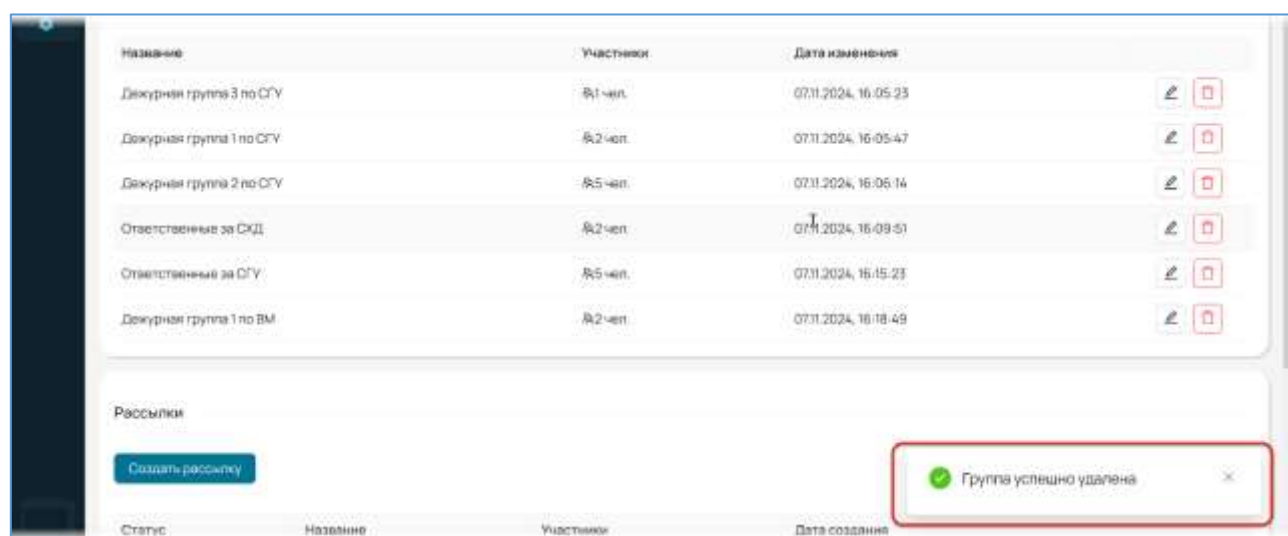


Рисунок 698 - Подтверждение удаления группы адресатов рассылки

8.7.5.3 Управление рассылками

Список рассылок

Список рассылок уведомлений представляет собой табличный список, в котором для каждой рассылки указываются следующие параметры (см. **Ошибка! Источник ссылки не найден.**):

- **Статус** – текущий статус рассылки: **вкл/выкл.**;
- **Название** – название рассылки в Подсистеме мониторинга;
- **Участники** – перечень адресатов рассылки: группы и отдельные пользователи;
- **Дата создания** – дата создания рассылки в формате: «дд.мм.гггг, чч:мм:сс»;
-  – функция просмотра и редактирования данных рассылки;
-  – функция удаления рассылки.

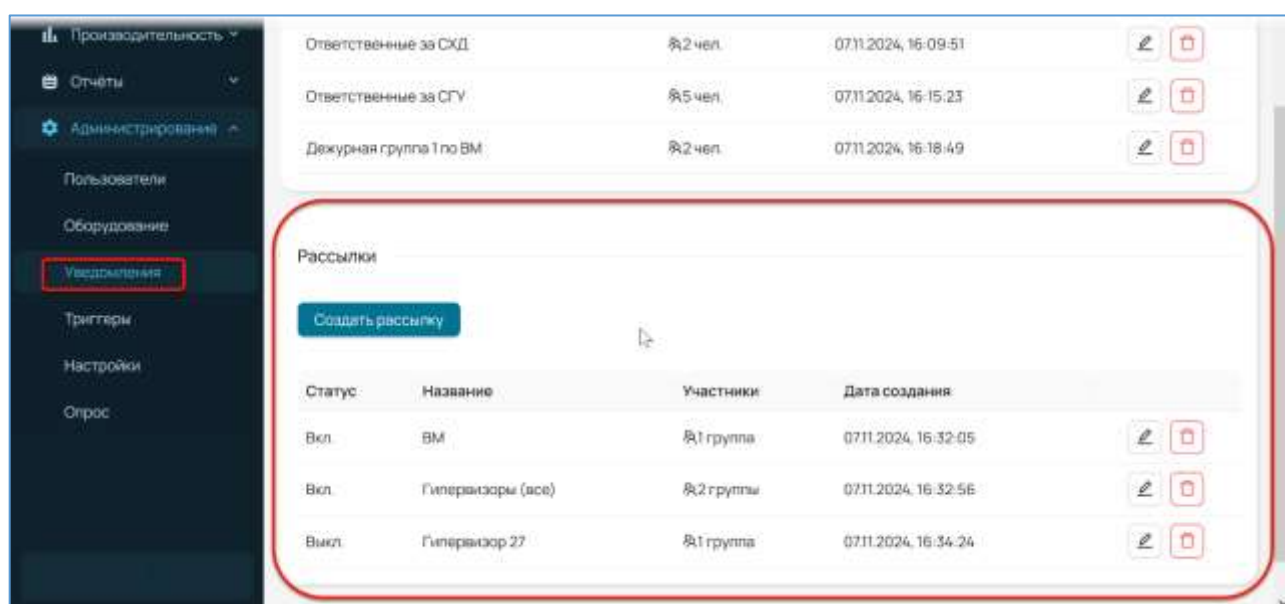


Рисунок 699 - Область «Рассылки»

Создание новой рассылки

Для создания новой рассылки необходимо выполнить следующие действия:

- 1) Нажать кнопку **Создать рассылку**. Откроет форма для создания новой рассылки уведомлений «Создание рассылки».
- 2) В открывшейся форме в поле **Название** ввести название новой рассылки уведомлений.
- 3) Из раскрывающегося списка **Объекты** выбрать объекты мониторинга, уведомления от которых будут участвовать в создаваемой рассылке (более подробно про выбор объектов приведено в Приложении Б).
- 4) Из раскрывающегося списка **Участники** выбрать группу(-ы) адресатов рассылки и/или отдельных пользователей, которым будут приходить уведомления, составляющие данную рассылку (более подробно про выбор участников приведено в Приложении Б).
- 5) В поле **Критичность события** установить от событий с каким статусом, уведомления будут попадать в рассылку – возможны статусы **Предупреждение** и/или **Критическая ошибка**.
- 6) Из раскрывающегося списка **Мин. длительность** выбрать время задержки отправки уведомлений, входящих в рассылку (более подробно про выбор времени приведено в Приложении Б).
- 7) При необходимости активировать рассылку, установив тумблер **Активировать рассылку** в положение **Вкл**.
- 8) При необходимости включить уведомление о закрытии рассылки, установив тумблер **Уведомлять о закрытии** в положение **Вкл**.
- 9) Для завершения создания рассылки нажать кнопку **Создать**.

Создание рассылки

* Название
Гипервизор 28

* Объекты ?
10.1.14.28 ×

* Участники ?
Дежурная группа 2 по СГУ ×

* Критичность события
Предупреждение Критическая ошибка

* Метод отправки
Почта

Мин. длительность ?
0 сек.

* Активировать рассылку Уведомлять о закрытии
Вкл Выкл

Отмена Создать

Рисунок 700 - Форма для создания новой рассылки

Редактирование данных рассылки

При необходимости параметры рассылки возможно отредактировать, щелкнув по значку  в строке интересующей рассылки. В результате действий откроется форма для редактирования параметров рассылки, аналогичная форме создания рассылки. Имя рассылки в поле **Название** для редактирования недоступно.

Возможно отредактировать следующие параметры рассылки:

- В поле **Объекты** изменить список объектов, чьи уведомления входят в рассылку.
- В поле **Участники** изменить список пользователей, которым предназначена рассылка.
- В поле **Критичность события** изменить список статусов событий, по которым формируются уведомления рассылки.
- В поле **Мин. длительность** изменить время задержки отправки уведомлений в рассылке.
- Изменить состояние тумблеров **Активировать рассылку** и **Уведомлять о закрытии**.

Б. Более подробное описание работы с полями формы приведено в Приложении

Удаление рассылки

Для удаления рассылки из Подсистемы мониторинга необходимо:

- 1) В списке рассылок щелкнуть по значку  в строке удаляемой рассылки.
- 2) В открывшемся окне подтверждения щелкнуть **Подтверждаю**.

Если удаление произошло удачно, то в интерфейсе должно появиться всплывающее сообщение об успешном удалении рассылки.

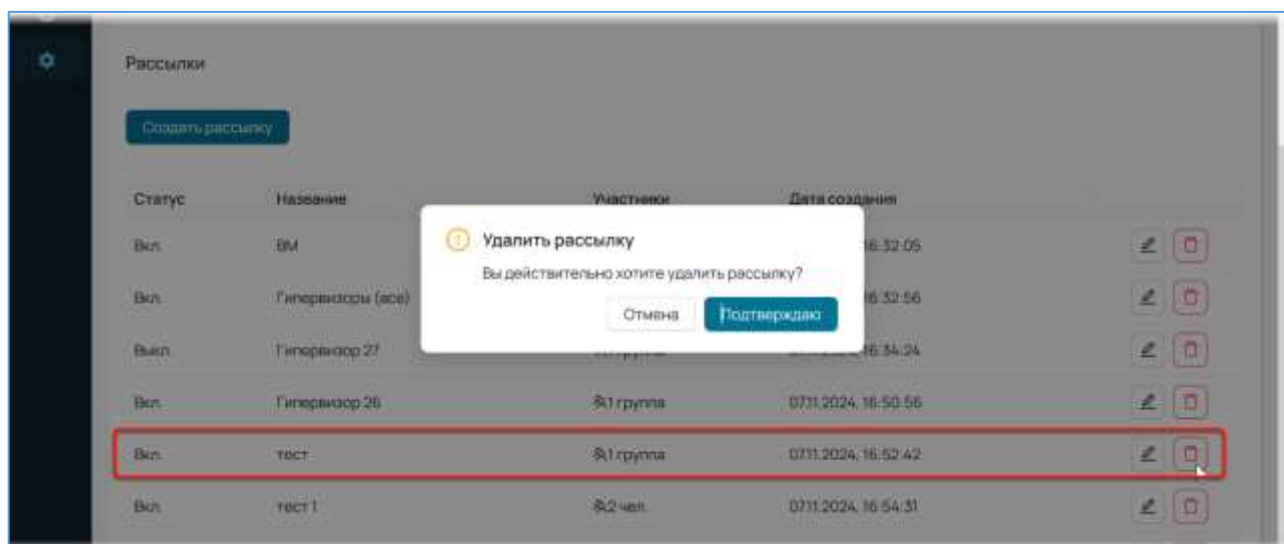


Рисунок 701 - Удаление рассылки

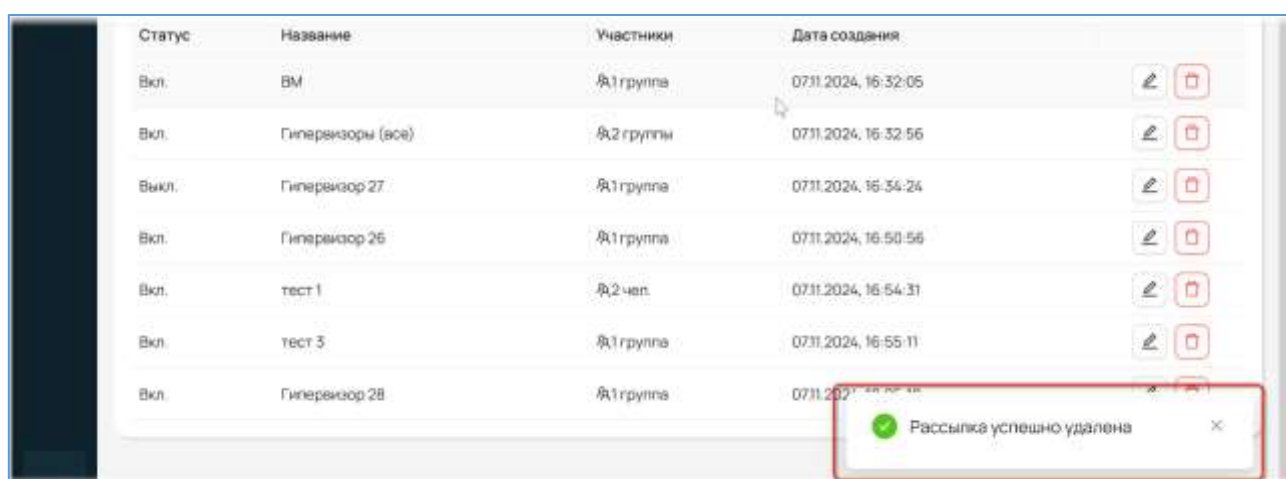


Рисунок 702 - Подтверждение удаления рассылки

8.7.6 Настройка триггеров

8.7.6.1 Доступ к функции. Назначение и состав

Создание и настройка правил отслеживания (триггеров), позволяющих контролировать достижение пороговых значений различных метрик Системы виртуализации «Горизонт-ВС» доступно в подраздел интерфейса **«Администрирование» → «Триггеры»**.

Функция предназначена для создания пороговых значений для следующих элементов Системы виртуализации «Горизонт-ВС»:

- Платформа;
- Гипервизор;
- Виртуальная машина;
- СРК;
- VDI;
- Хранилища данных.

Подраздел содержит следующие данные:

- табличный список триггеров, созданных в Подсистеме мониторинга на текущий момент времени;
- функции сортировки триггеров по значениям полей списка;
- функция создания нового триггера для объектов Системы виртуализации «Горизонт-ВС», подключенных к Подсистеме мониторинга;
- функция просмотра и редактирования триггера;
- функция удаления триггера.

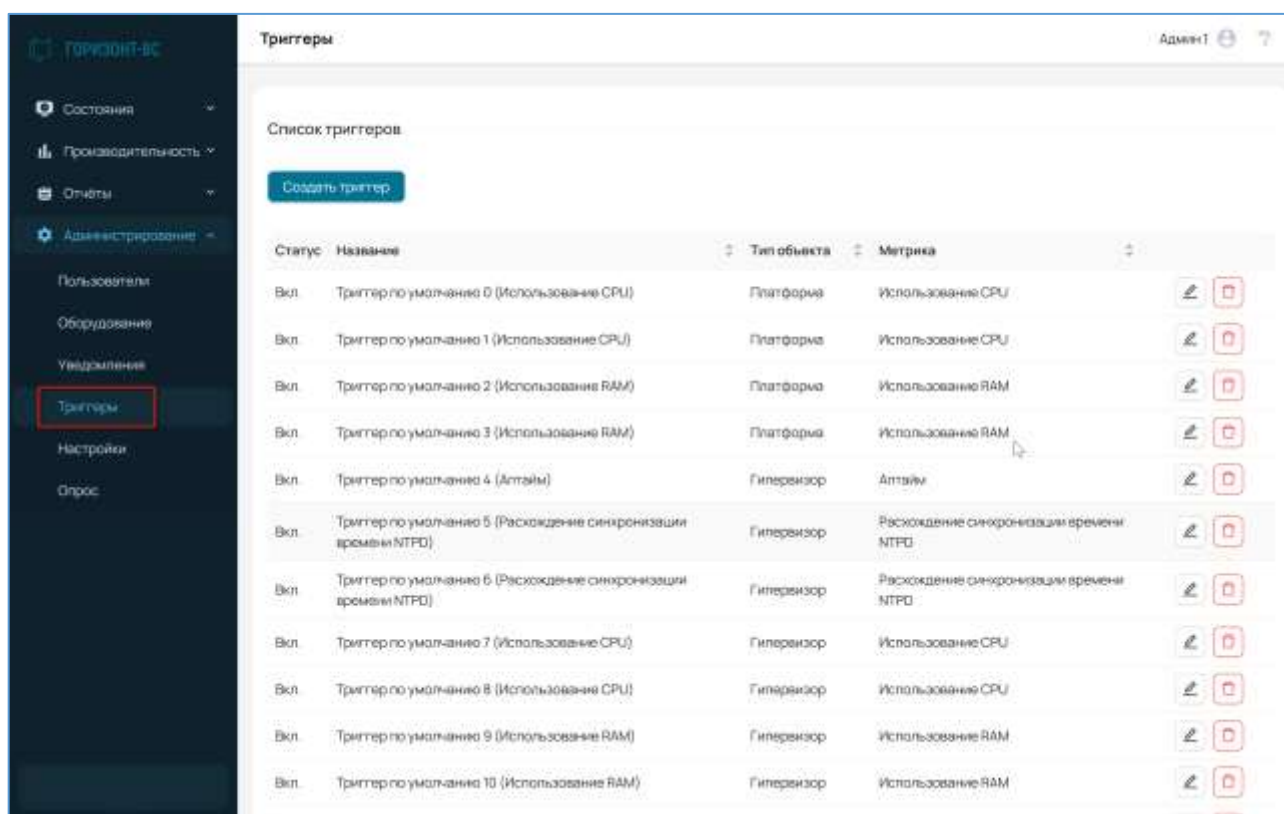


Рисунок 703 - Раздел интерфейса для работы с триггерами

8.7.6.2 Список триггеров

Перечень триггеров, созданных в Подсистеме мониторинга, представляет собой табличный список, в котором для каждого триггера указываются следующие параметры:

- **Статус** – отображает используется или нет в данный момент триггер. Возможные значения **Вкл./Выкл** – соответственно активен/неактивен.
- **Название** – уникальное название триггера в Подсистеме мониторинга.
- **Тип объекта** – тип объекта Системы виртуализации «Горизонт-ВС» для которого создан данный триггер.
- **Метрика** – метрика по которой сделан триггер.
-  – функция просмотра и редактирования параметров триггера;

-  – функция удаления триггера из Подсистемы мониторинга.

8.7.6.3 Сортировки записей в списке триггеров по значениям полей

Сортировка записей в списке триггеров осуществляется по значениям следующих полей:

- **Название** – прямая/обратная сортировка строк по алфавиту по уникальному названию триггера;
- **Тип объекта** – прямая/обратная сортировка строк по алфавиту по названию типа объекта Системы виртуализации «Горизонт-ВС» для которого созданы триггеры (платформа, гипервизор, СРК и т.д.).
- **Метрика** – прямая/обратная сортировка строк по алфавиту по названию метрики для которой сделан триггер.

Поля, по которым возможна сортировка строк списка, отмечены стандартным значком сортировки строк . При щелчке мышкой по названию поля, отмеченного данным значком, предоставляются следующие возможности сортировки:

- **Подсказка Нажмите для сортировки по возрастанию** – список триггеров будет сформирован согласно расположению значений указанного поля по алфавиту А→Я.
- **Подсказка Нажмите для сортировки по убыванию** – список триггеров будет сформирован согласно расположению значений указанного поля в обратном порядке Я→А.
- **Подсказка Нажмите, чтобы отменить сортировку** – список триггеров будет возвращен в исходное состояние (по времени создания записей).

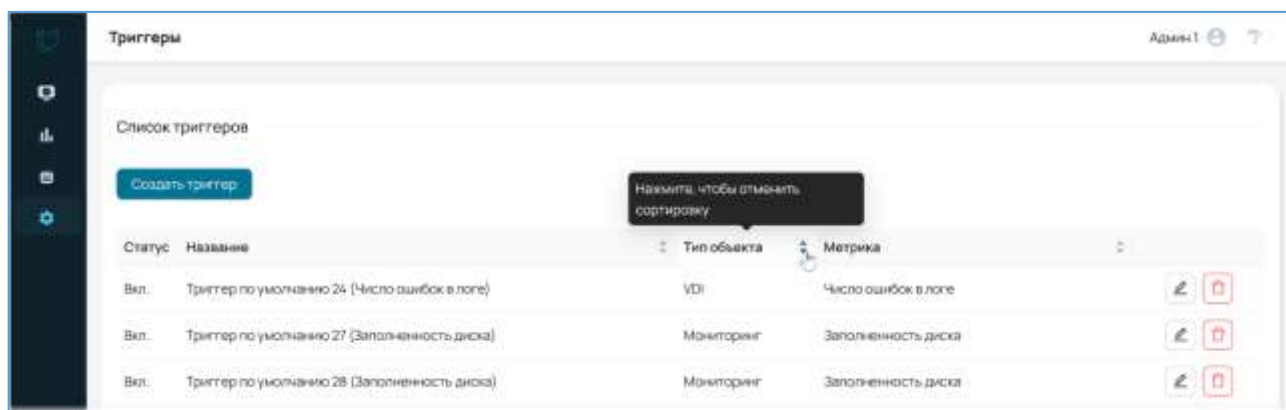


Рисунок 704 - Сортировка списка триггеров

8.7.6.4 Создание нового триггера

Для создания нового триггера в Подсистеме мониторинга необходимо выполнить следующие действия:

- 1) Щелкнуть по функции **Создать триггер**.
- 2) В открывшемся бланке «Создание триггера» указать следующие параметры нового правила отслеживания:
 - **Название** – указать уникальное название триггера, которое будет отображаться в веб-интерфейсе Подсистемы мониторинга.
 - **Тип объекта** – в раскрывающемся списке выбрать тип объекта из состава «Горизонт-ВС».
 - **Объекты** – выбрать из раскрывающегося списка один или несколько объектов, для которых будет создаваться триггер.
 - **Метрика** – выбрать из раскрывающегося списка метрику, по которой будет устанавливаться пороговое значения триггера.
 - **Условие** – в раскрывающемся списке выбрать условие срабатывания порога.
 - **Значение** – в раскрывающемся списке выбрать значение порога.
 - **Критичность события** – в раскрывающемся списке выбрать критичность события срабатывания порога.

- **Мин. длительность** – в раскрывающемся списке выбрать время задержки срабатывания триггера и отправки сообщения о событии по превышению порога.
- **Активировать триггер** – установить тумблер в положение **Вкл.** для активации триггера сразу после сохранения настроек. Установить тумблер в положение **Выкл.** для сохранения триггера без его использования при мониторинге системы.

3) Нажать кнопку **Создать** для создания в Подсистеме мониторинга нового триггера для объектов «Горизонт-ВС».

На экране должно появиться всплывающее сообщение об успешном создании нового триггера. Новый триггер должен отобразиться в списке триггеров Подсистемы мониторинга.

Создание триггера

✕

✱ Название

Гипервизор 150. Ошибки сетевого интерфейса

✱ Тип объекта

Гипервизор

✱ Объекты

10.114.150

✱ Метрика

Ошибки на сетевом интерфейсе

✱ Условие

>

✱ Значение

5

%

✱ Критичность события

Предупреждение

✱ Мин. длительность ?

2 мин.

✱ Активировать триггер

Вкл

Отмена

Создать

Рисунок 705 - Форма для создания в Подсистеме мониторинга нового триггера для объектов «Горизонт-ВС»

8.7.6.5 Удаление триггера

Для удаления триггера из Подсистемы мониторинга необходимо выполнить следующие действия:

- 1) В списке триггеров щелкнуть по значку  в строке триггера, который требуется удалить.
- 2) В открывшемся окне подтверждения щелкнуть **Подтверждаю**.

Должно появиться всплывающее сообщение об успешном удалении триггера. Строка данного триггера должна быть удалена из списка триггеров Подсистемы мониторинга.

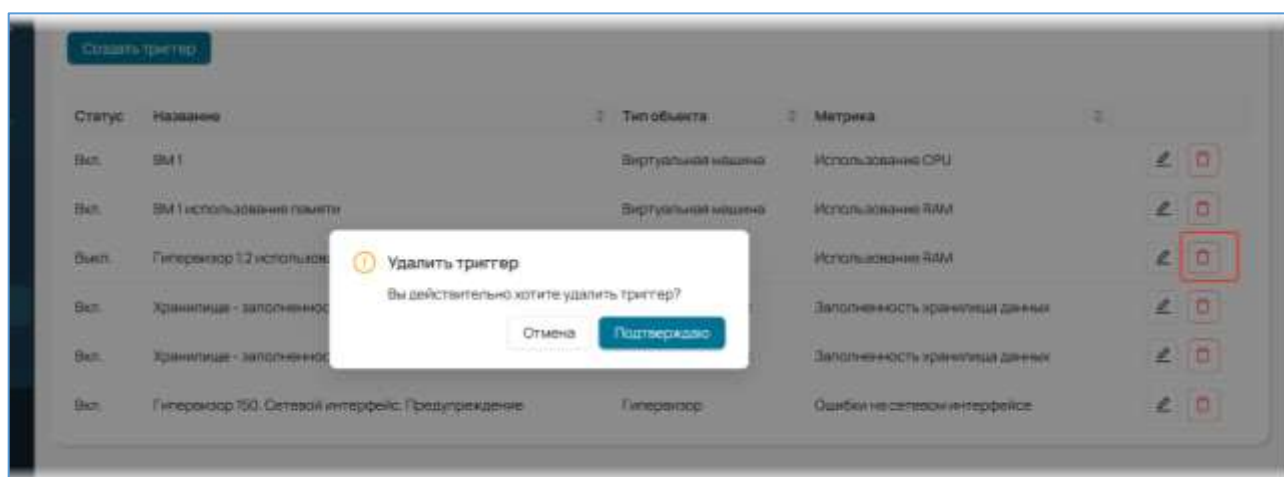


Рисунок 706 - Удаление триггера

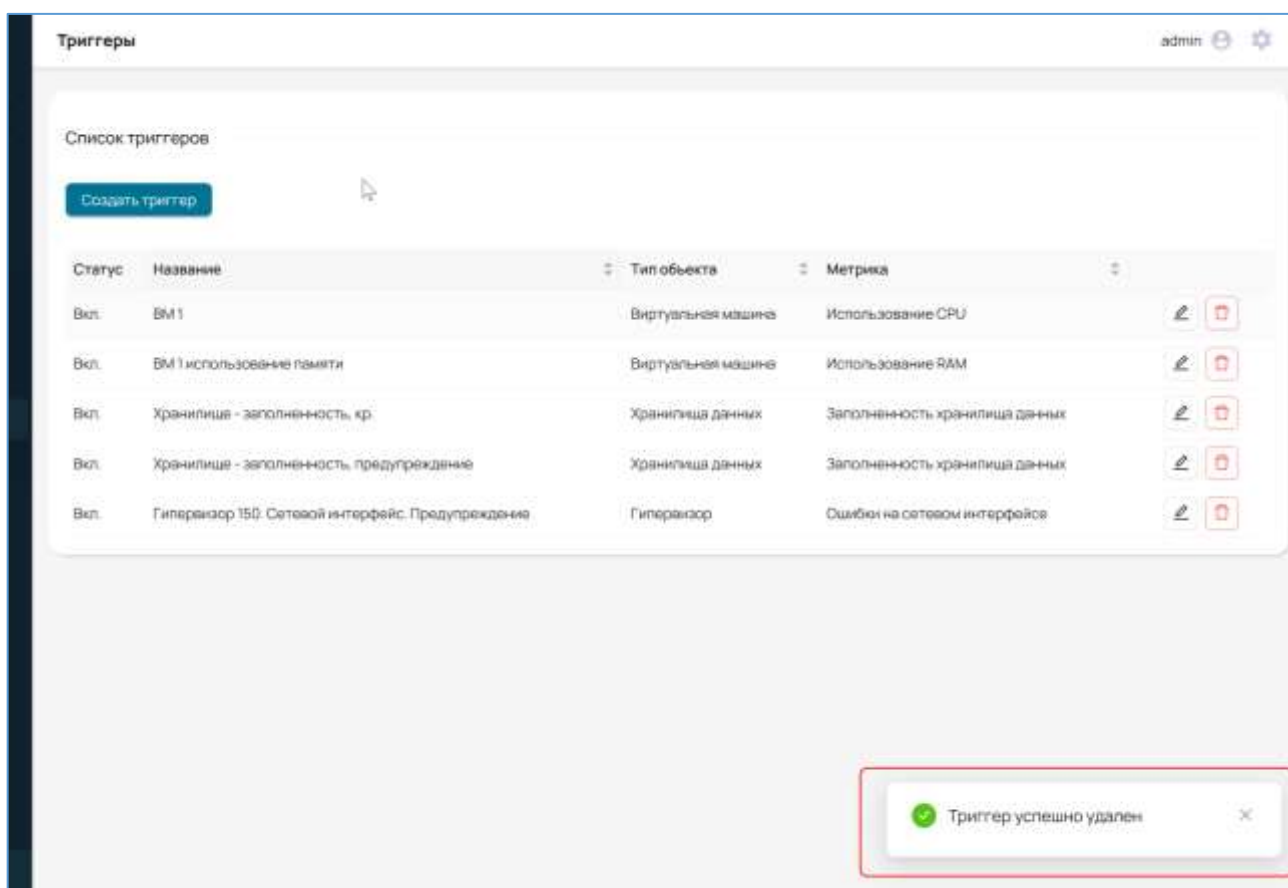


Рисунок 707 - Сообщение об удалении триггера из Подсистемы мониторинга

8.7.6.6 Просмотр и редактирование параметров триггера

При необходимости просмотра и редактирования параметров триггера необходимо выполнить следующие действия:

1) В списке триггеров щелкнуть по значку в строке интересующего триггера. Откроется окно **«Редактирование триггера»** (Рисунок 708).

2) Внести необходимые корректировки в параметры триггера.

Для корректировки доступны все параметры кроме (Рисунок 708) поля **Название** (название триггера в Подсистеме мониторинга).

3) Для сохранения изменений нажать кнопку **Сохранить**.

Если изменения в параметры триггера были внесены правильно, то на экране должно отобразиться окно подтверждения успешного изменения триггера.

The image shows a dialog box titled "Редактирование триггера" (Editing trigger) with a close button (X) in the top right corner. The dialog contains several form fields for configuring a trigger:

- Название** (Name): A text field containing "Триггер по умолчанию 25 (Заполненность хранилища)" (Default trigger 25 (Storage fullness)).
- Тип объекта** (Object type): A dropdown menu with "Хранилища данных" (Data stores) selected.
- Объекты** (Objects): A dropdown menu with "Все" (All) selected.
- Метрика** (Metric): A dropdown menu with "Заполненность хранилища данных" (Data store fullness) selected.
- Условие** (Condition): A dropdown menu with ">" selected.
- Значение** (Value): A text field with "75" and a percentage sign "%".
- Критичность события** (Event criticality): A dropdown menu with "Предупреждение" (Warning) selected.
- Мин. длительность** (Min. duration): A dropdown menu with "0 сек." (0 sec.) selected.
- Активировать триггер** (Activate trigger): A toggle switch currently set to "Вкл" (On).

At the bottom right of the dialog are two buttons: "Отмена" (Cancel) and "Сохранить" (Save).

Рисунок 708 - Редактирование параметров триггера

8.7.7 Настройка подключения к почтовому серверу Подсистемы мониторинга

8.7.7.1 Доступ к функции. Назначение и состав

Функция настройки почтового сервера Подсистемы мониторинга доступна в подразделе интерфейса **«Администрирование»** → **«Настройки»** (Рисунок 709). Функция реализована в области **«Настройка почтового сервера»** и предназначена для:

- подключения почтового сервера после установки Подсистемы мониторинга;
- смены текущих настроек почтового сервера при необходимости (кнопка **Редактировать**);
- проверки работы почтового сервера (кнопка **Проверить**).

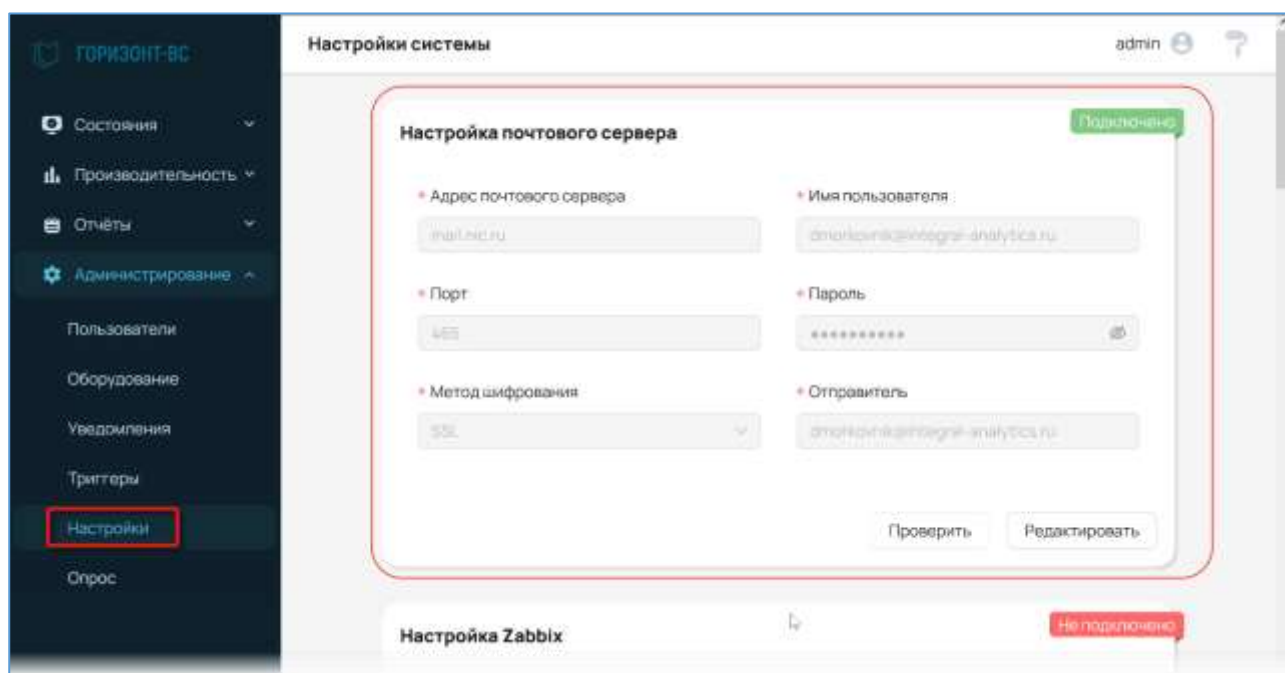


Рисунок 709 - Область настроек почтового сервера

Область настроек почтового сервера содержит следующие параметры (поля):

- **Адрес почтового сервера** – ip-адрес или доменное имя почтового сервера.
- **Порт** – порт для подключения к почтовому серверу.
- **Метод шифрования** – раскрывающийся список методов шифрования сообщений. Доступны следующие методы SSL, TLS, STARTTLS.
- **Имя пользователя** – имя для авторизации на почтовом сервере.
- **Пароль** – пароль для авторизации на почтовом сервере.
- **Отправитель** – электронный адрес, с которого буду рассылаться уведомления от Подсистемы мониторинга.

8.7.7.2 Подключение почтового сервера после установки Подсистемы мониторинга

После установки Подсистемы мониторинга в области «**Настройка почтового сервера**» отобразятся пустые поля настройки и статус почтового сервера **Не подключено** (Рисунок 710).

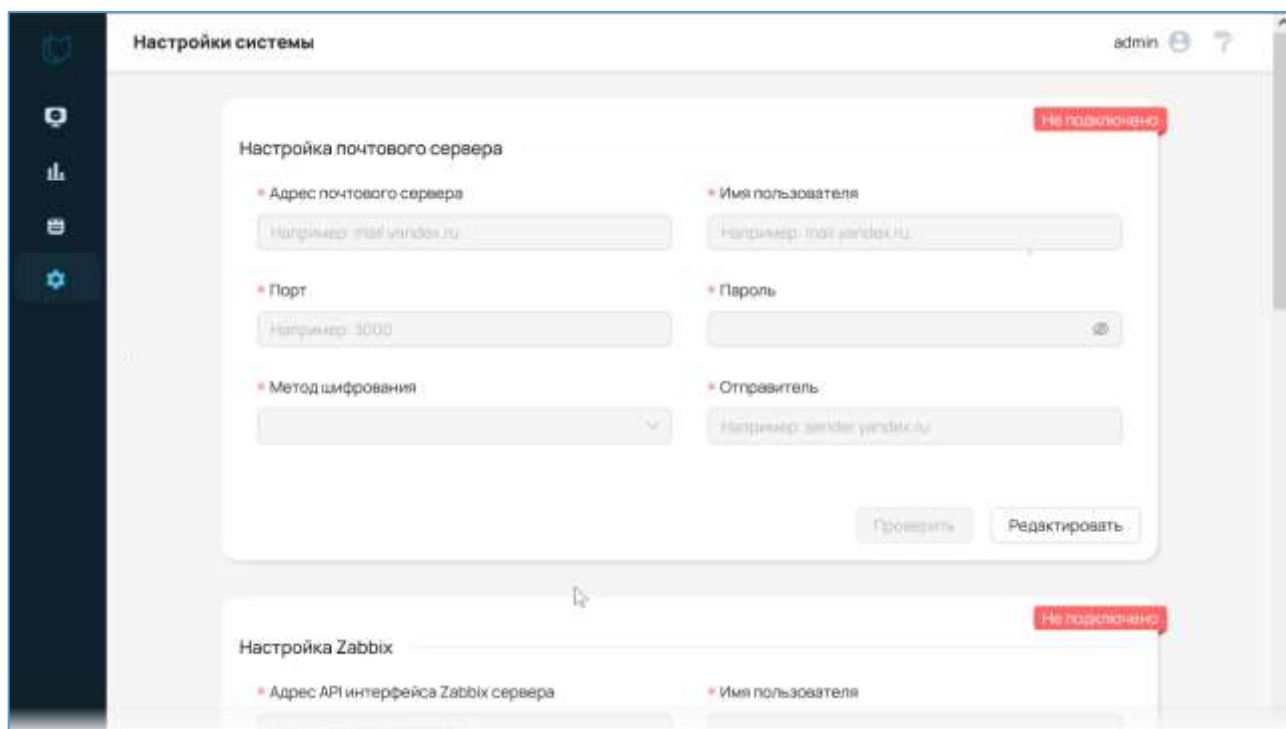


Рисунок 710 - Область настройки почтового сервера после установки Подсистемы мониторинга

Для настройки почтового сервера необходимо выполнить следующие действия:

- 1) Нажать кнопку **Редактировать** (Рисунок 710). Поля станут доступны для ввода данных. Назначение кнопки **Редактировать** изменится на **Подключить**.
- 2) В соответствующих полях ввести параметры почтового сервера (все поля обязательны для заполнения). Описание полей – см. п.0.
- 3) Для подключения почтового сервера нажать кнопку **Подключить** (Рисунок 711).

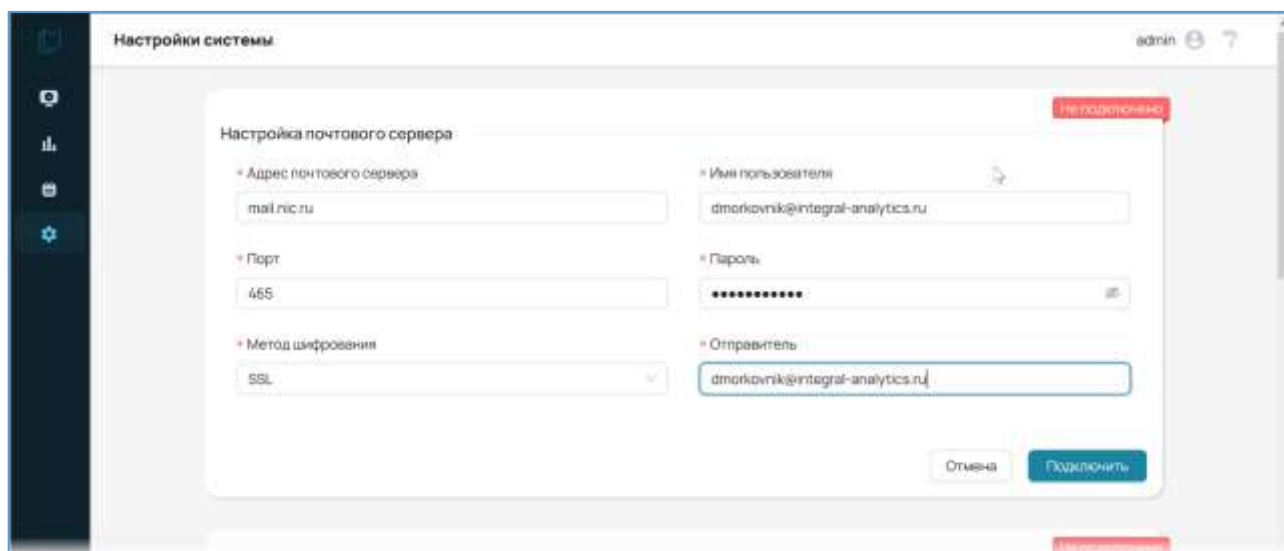


Рисунок 711 - Ввод данных и подключение почтового сервера

Если все данные были введены без ошибок, то:

- на экране должно отобразиться всплывающее сообщение «Почтовый сервер успешно подключен»;
- статус почтового сервера должен измениться на **Подключено** на зеленом фоне (Рисунок 712);
- данные, введенные в полях, станут недоступными для изменения;
- станут доступны кнопки **Проверить** и **Редактировать**.

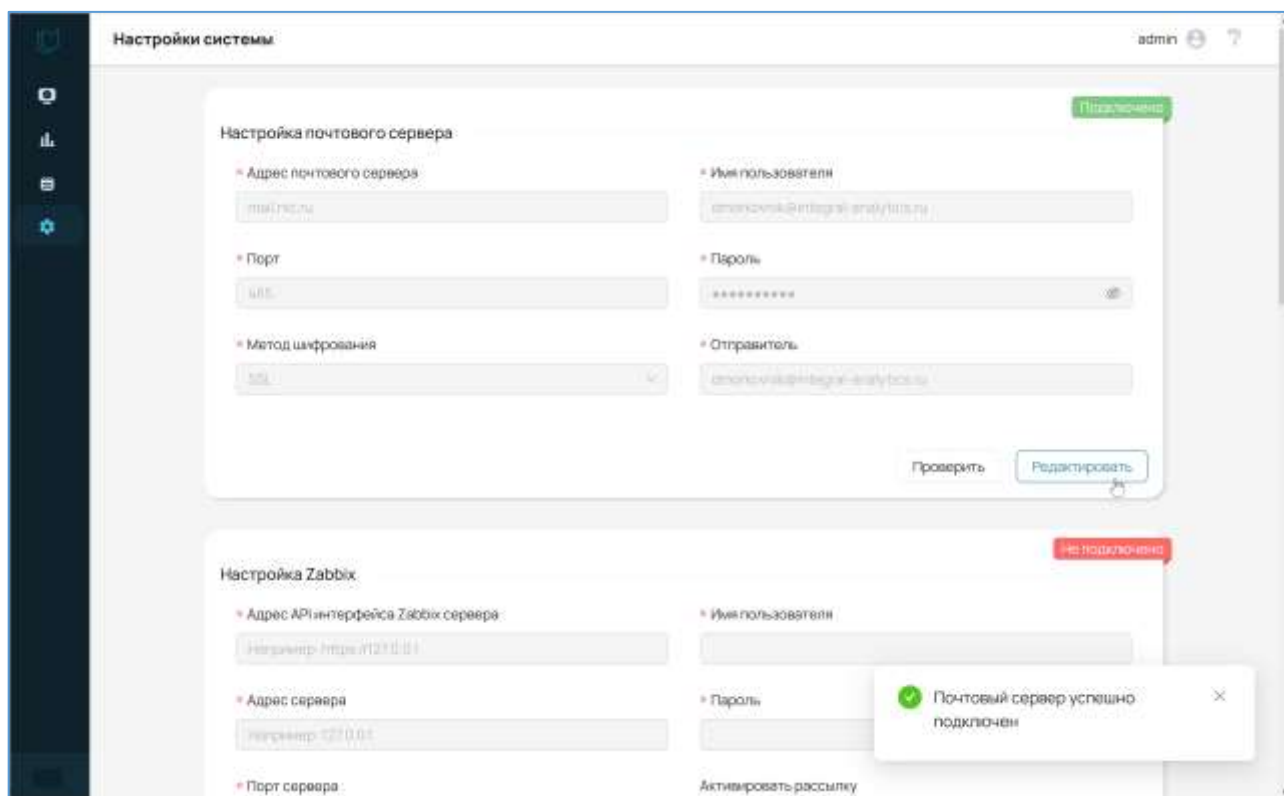


Рисунок 712 - Почтовый сервер подключен

8.7.7.3 Корректировка данных при подключении сервера

Если в процессе подключения были введены неверные данные, то после нажатия кнопки **Подключить** появится всплывающее сообщение об ошибке введенных данных (см. **Ошибка! Источник ссылки не найден.**).

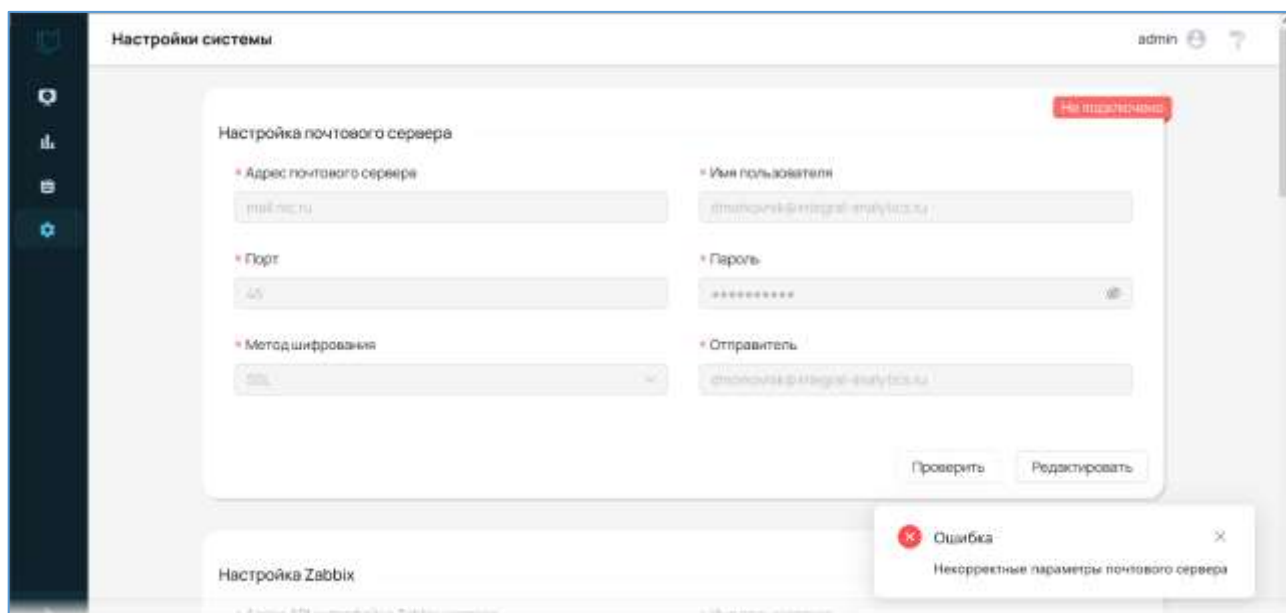


Рисунок 713 - Попытка подключения почтового сервера при указании неверных данных

Для корректировки данных выполнить следующие действия:

- 1) Нажать кнопку **Редактировать**. Поля станут доступными для редактирования. Назначение кнопки **Редактировать** изменится на **Подключить**.
- 2) Провести необходимую корректировку данных.
- 3) Нажать кнопку **Подключить**.

8.7.7.4 Редактирование настроек почтового сервера

В случае смены настроек почтового сервера их так же необходимо отредактировать в области «**Настройка почтового сервера**» в веб-интерфейсе Подсистемы мониторинга. Редактирование настроек уже подключенного сервера происходит аналогично корректировке параметров почтового сервера при первом подключении.

8.7.7.5 Проверка работы почтового сервера

После подключения почтового сервера желательно проверить его работоспособность. Для этого необходимо выполнить следующие действия:

- 1) Нажать кнопку **Проверить**.
- 2) В открывшемся окне ввести электронный адрес, на который почтовым сервером Подсистемы мониторинга будет отправлено тестовое письмо, и нажать кнопку **Отправить** (Рисунок 714).

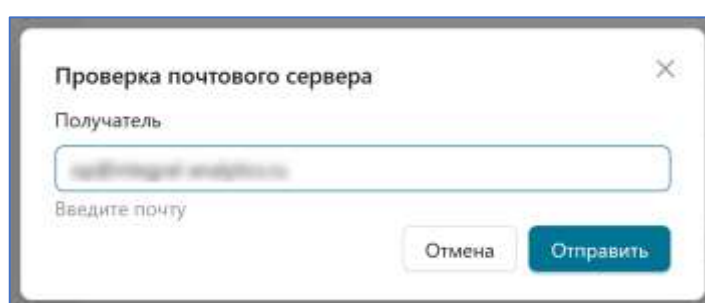


Рисунок 714 - Отправка тестового письма

Если отправка тестового письма прошла успешно, то появится всплывающее сообщение об успешной отправке письма.

На электронную почту, указанную в качестве получателя тестового письма, должно прийти сообщение со следующими параметрами:

- заголовок сообщения – «[Горизонт-ВС] Тестовое письмо»;
- текст сообщения – «Проверка параметров почтового сервера»;
- адрес отправителя – электронный адрес, указанный в настройках почтового сервера в поле **Отправитель**.

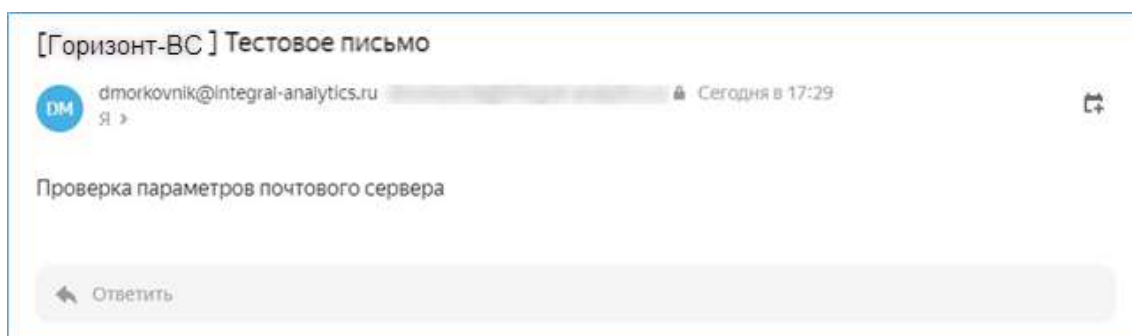


Рисунок 715 - Образец тестового письма от почтового сервера
Подсистемы мониторинга

8.7.8 Настройка взаимодействия с системой мониторинга Zabbix

8.7.8.1 Доступ к функции. Назначение и состав

При необходимости можно настроить процесс передачи данных о состоянии «Горизонт-ВС» из Подсистемы мониторинга «Горизонт-ВС» в систему мониторинга Zabbix, расположенную в корпоративной сети.

Интеграция Подсистемы Мониторинга с Zabbix происходит автоматически и не требует дополнительных настроек в Zabbix. Подсистема мониторинга автоматически создает внутри Zabbix ряд объектов на основании своих внутренних шаблонов:

- хост-группа: **HCS cluster**;
- темплейты внутри хост-группы: **hcs-cluster**, **hcs-node**, **hcs-hypervisor**, **hcs-vm**, **hcs-vdi**, **hcs-bus**, внутри каждой из которых определяются параметры для мониторинга;
- конкретные хосты с указанными выше темплейтами, по которым будут передаваться данные мониторинга.

Наличие перечисленных выше объектов проверяется каждый раз при запуске контейнера **monitor**.

Функция настройки взаимодействия Подсистемы мониторинга «Горизонт-ВС» со сторонней системой мониторинга Zabbix доступна в подразделе интерфейса **«Администрирование»** → **«Настройки»**. Функция реализована в области **«Настройка Zabbix»** и предназначена для:

- интеграции с системой мониторинга Zabbix после установки Подсистемы мониторинга «Горизонт-ВС»;
- смены текущих настроек интеграции при необходимости (кнопка **Редактировать**);
- включение/выключение передачи данных при наличии настроенной интеграции (тумблер **Активировать рассылку**).

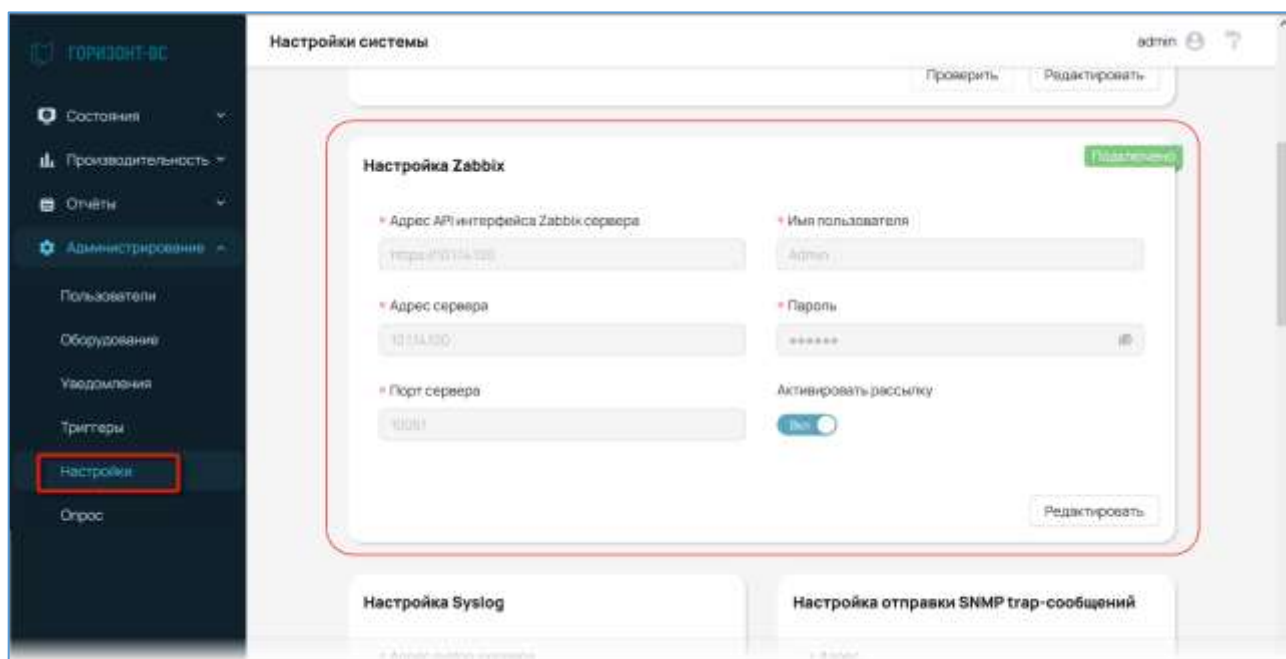


Рисунок 716 - Область настроек интеграции с Zabbix

Область настроек Zabbix содержит следующие параметры (поля):

- **Адрес API интерфейса Zabbix сервера;**
- **Имя пользователя и Пароль** – логин и пароль для доступа к API интерфейсу Zabbix сервера;

- **Адрес сервера и Порт сервера** – параметры Zabbix траппера для получения данных мониторинга.

8.7.8.2 Настройка взаимодействия с системой Zabbix после установки Подсистемы мониторинга

После установки Подсистемы мониторинга в области «**Настройка Zabbix**» отобразятся пустые поля настройки и статус **Не подключено** (см. **Ошибка! Источник ссылки не найден.**).

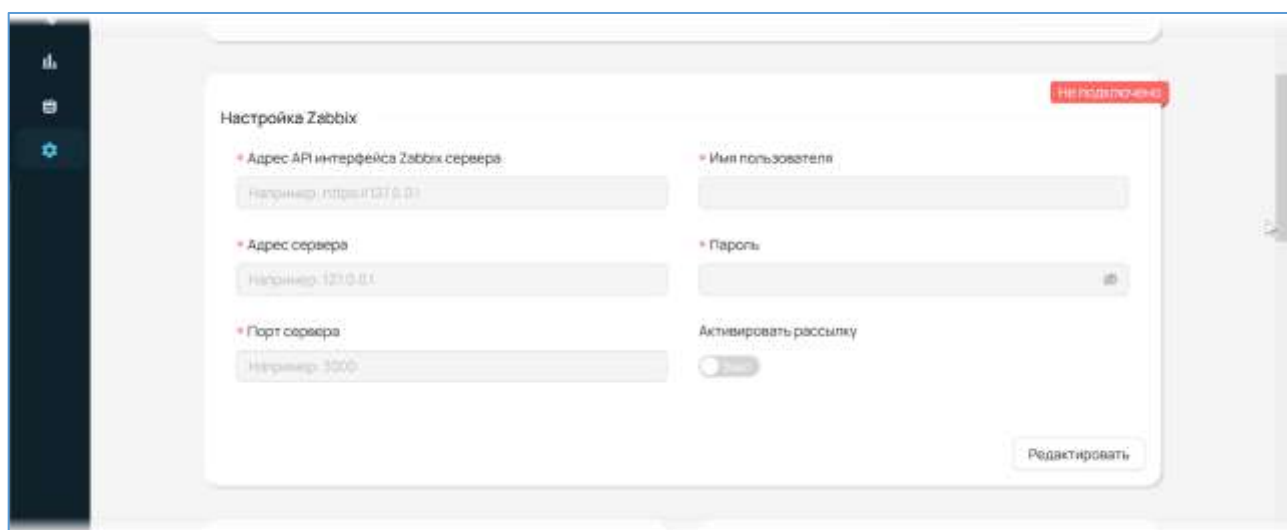


Рисунок 717 - Область настройки взаимодействия с системой мониторинга Zabbix после установки Подсистемы мониторинга

Для настройки интеграции с Zabbix необходимо выполнить следующие действия:

- 1) Нажать кнопку **Редактировать**. Поля станут доступны для ввода данных. Назначение кнопки **Редактировать** изменится на **Подключить**.
- 2) В советующих полях ввести данные сервера Zabbix (все поля обязательны для заполнения). Описание полей – см. п.0.
- 3) Установить тумблер **Активировать рассылку** в положение **Вкл.** для начала передачи данных в Zabbix сразу после сохранения настроек. Установить

тумблер в положение **Выкл.** для сохранения настроек интеграции без осуществления передачи данных.

- 4) Для сохранения настроек интеграции Подсистемы мониторинга «Горизонт-ВС» с системой Zabbix нажать кнопку **Подключить**.

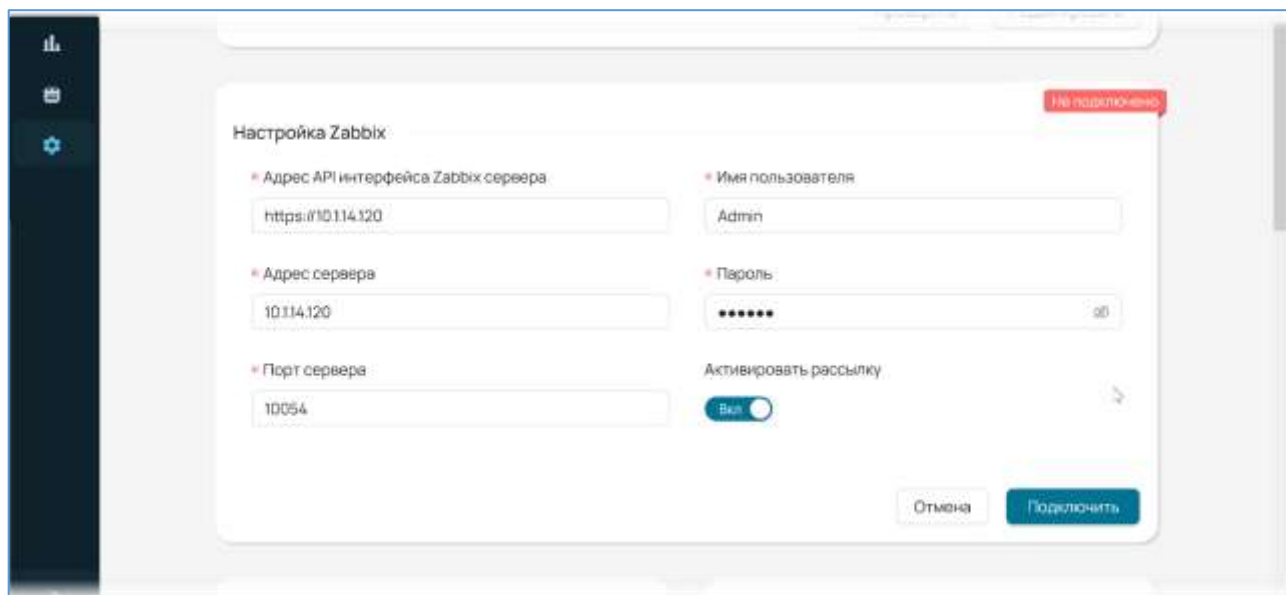


Рисунок 718 - Ввод данных для интеграции с Zabbix

Если все данные были введены без ошибок, то:

- на экране должно отобразиться всплывающее сообщение «Настройки интеграции с Zabbix успешно сохранены»;
- статус интеграции с Zabbix должен измениться на **Подключено** на зеленом фоне ;
- данные, введенные в полях, станут недоступными для изменения;
- станет доступна кнопка **Редактировать**.

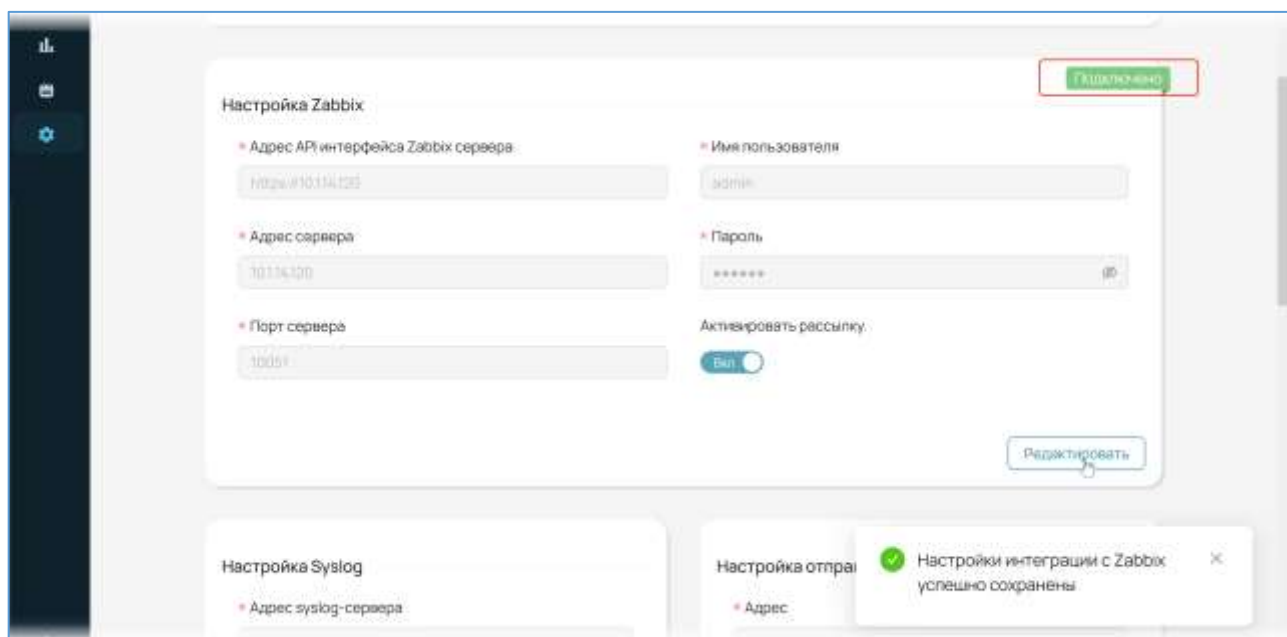


Рисунок 719 - Взаимодействие с системой мониторинга Zabbix настроено и активировано

8.7.83 Редактирование настроек взаимодействия с Zabbix

В случае смены параметров системы мониторинга Zabbix, данные параметры так же необходимо отредактировать в области «**Настройка Zabbix**» в веб-интерфейсе Подсистемы мониторинга.

Для корректировки данных выполнить следующие действия:

- 1) Нажать кнопку **Редактировать**. Поля станут доступными для редактирования. Назначение кнопки **Редактировать** изменится на **Подключить**.
- 2) Провести необходимую корректировку данных.
- 3) Нажать кнопку **Подключить**.

8.7.9 Настройка отправки зафиксированных Подсистемой мониторинга событий на сторонние syslog-серверы

8.7.9.1 Доступ к функции. Назначение и состав

При необходимости можно настроить процесс передачи данных о событиях, зафиксированных Подсистемой мониторинга «Горизонт-ВС», на syslog-серверы, расположенные в корпоративной сети.

Функция настройки отправки зафиксированных событий на syslog-серверы доступна в подразделе интерфейса **«Администрирование»** → **«Настройки»** (). Функция реализована в области **«Настройка Syslog»** и предназначена для:

- настройки взаимодействия с одним или несколькими syslog-серверами для отправки событий, зафиксированных Подсистемой мониторинга «Горизонт-ВС»;
- включения/выключения передачи данных о зафиксированных событиях при наличии настроенного взаимодействия с syslog-серверами (тумблер **Активировать рассылку**).

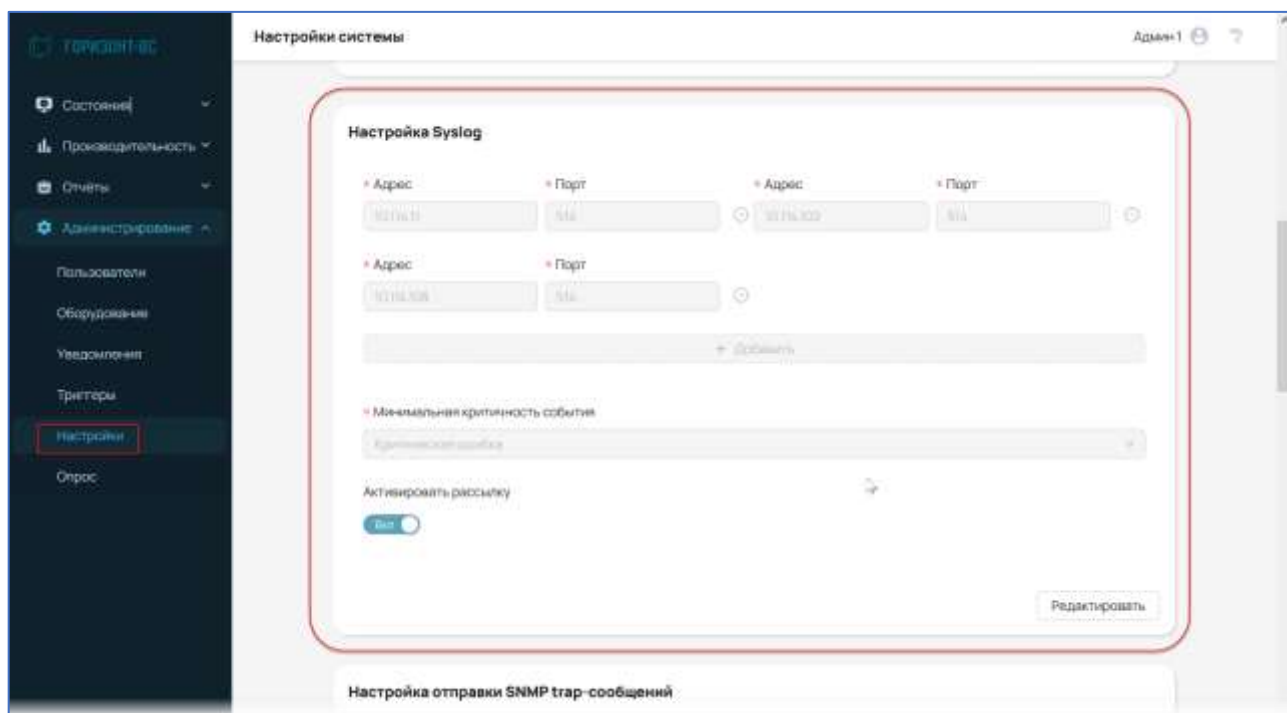


Рисунок 720 - Область настройки взаимодействия Подсистемы мониторинга «Горизонт-ВС» с syslog-сервером корпоративной сети

Область «Настройка Syslog» содержит следующие параметры и функции:

- список syslog-серверов для рассылки сообщений в формате:
 - **Адрес** – ip-адрес syslog-сервера в корпоративной сети;
 - **Порт** – порт, через который поступает информация на syslog-сервер.
- **+Добавить** – функция добавления в список нового syslog-сервера.
- **⊖** – функция удаления сервера из списка syslog-серверов.
- **Минимальная критичность события** – список критичности событий Подсистемы мониторинга для создания фильтра отправляемых на syslog-сервер событий. Если статус события, зафиксированного Подсистемой мониторинга, выше или равен установленному порогу минимальной критичности, то данные о событии передаются на syslog-сервер, если ниже – не передаются. Список содержит следующие позиции:
 - Информирование;

- Предупреждение;
 - Критическая ошибка;
 - Неизвестная ошибка.
- **Редактировать / Подключить** – функции редактирования/ подключения списка серверов.

8.7.9.2 Настройка отправки зафиксированных событий на syslog-серверы после установки Подсистемы мониторинга

После установки Подсистемы мониторинга в области «**Настройка Syslog**» отобразятся пустые поля настройки для одного syslog-сервера (Рисунок 721).

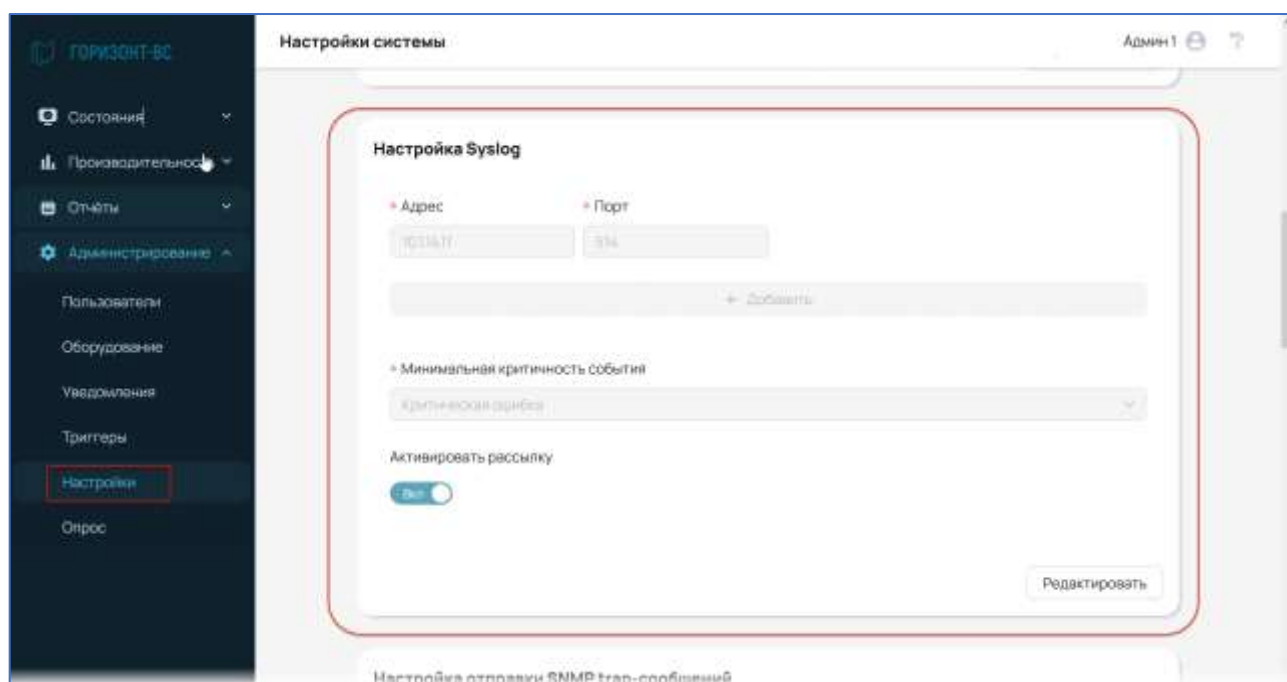


Рисунок 721 - Область настройки отправки зафиксированных событий на syslog-серверы после установки Подсистемы мониторинга

Для настройки отправки событий, зафиксированных Подсистемой мониторинга на один или несколько сторонних syslog-серверов необходимо выполнить следующие действия:

- 1) Нажать кнопку **Редактировать** (см. **Ошибка! Источник ссылки не найден.**). Поля станут доступны для ввода данных. Назначение кнопки **Редактировать** изменится на **Подключить**.
- 2) В советующих полях ввести ip-адрес syslog-сервера и номер порта (все поля обязательны для заполнения). Подробное описание полей – см. п.0.
- 3) Если для отправки сообщений необходимо настроить еще один syslog-сервер, то нажать функцию **+Добавить**. Появятся поля **Адрес** и **Порт** для ввода параметров и подключения еще одного syslog-сервера.
- 4) Ввести в поля **Адрес** и **Порт** данные нового syslog-сервера (Рисунок 722).
Повторить п. 3) и 4) данного алгоритма столько раз, сколько syslog-серверов необходимо подключить для получения событий от Системы мониторинга.

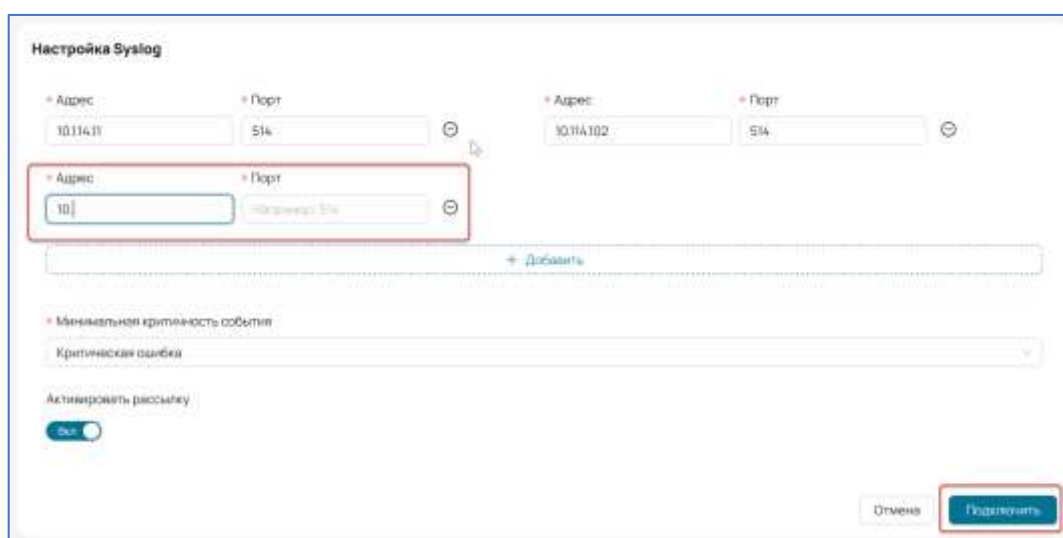


Рисунок 722 - Ввод параметров нового syslog-сервера

- 5) Выбрать в раскрывающемся списке **Минимальная критичность события** необходимое значение порога критичности (Рисунок 722). Подробное описание списка.

Критичность события устанавливается единая для всех заявленных syslog-серверов.

- 6) Установить тумблер **Активировать рассылку** в положение **Вкл.** для начала передачи данных о событиях, зафиксированных Подсистемой мониторинга, на syslog-серверы сразу после сохранения настроек (см. **Ошибка! Источник ссылки не найден.**). Установить тумблер в положение **Выкл.** для сохранения настроек без осуществления передачи данных.

Активация режима рассылки устанавливается для всех заявленных syslog-серверов.

- 7) Для сохранения настроек отправки зафиксированных событий на syslog-серверы нажать кнопку **Подключить**.

Рисунок 723 - Выбор минимальной критичности для отправки зафиксированных событий на заявленные syslog-сервера

Если все данные были введены без ошибок, то:

- на экране должно отобразиться всплывающее сообщение «Настройки отправки уведомлений Syslog успешно сохранены»;

- данные, введённые в полях, станут недоступными для изменения;
- станет доступна кнопка **Редактировать**.

8.7.9.3 Редактирование настроек взаимодействия с syslog-серверами

Доступны следующие изменения настроек:

- редактирование параметров syslog-сервера (адрес и порт);
- изменение списка syslog-серверов – удаление серверов из списка или добавление новых серверов;
- редактирование минимального уровня критичности отправляемых сообщений;
- активировать или деактивировать рассылку.

Для корректировки параметров взаимодействия выполнить следующие действия:

- 1) Нажать кнопку **Редактировать**. Поля станут доступными для редактирования. Назначение кнопки **Редактировать** изменится на **Подключить**.
- 2) Провести необходимую корректировку данных.
- 3) Нажать кнопку **Подключить**.

Если все новые данные были введены без ошибок, то:

- на экране должно отобразиться всплывающее сообщение «Настройки отправки уведомлений Syslog успешно сохранены»;
- данные, введённые в полях, станут недоступными для изменения;
- станет доступна кнопка **Редактировать**.

8.7.9.4 Управление списком syslog-серверов

В список syslog-серверов можно добавить новые адреса рассылки, либо удалить из списка существующие.

Для **добавления** нового syslog-сервера в список адресов рассылки сообщений от Подсистемы мониторинга необходимо выполнить следующие действия:

- 1) Нажать кнопку **Редактировать**. Поля станут доступными для редактирования. Назначение кнопки **Редактировать** изменится на **Подключить**.
- 2) Нажать функцию **+Добавить**. Появятся поля **Адрес** и **Порт** для ввода параметров нового syslog-сервера.
- 3) Ввести в поля **Адрес** и **Порт** данные нового syslog-сервера.

Повторить пункты 2) и 3) данного алгоритма столько раз, сколько syslog-серверов необходимо подключить для получения событий от Системы мониторинга.

- 4) Для подключения нового списка серверов нажать кнопку **Подключить**.

Для **удаления** syslog-сервера из списка адресов рассылки сообщений от Подсистемы мониторинга необходимо выполнить следующие действия:

- 1) Нажать кнопку **Редактировать**. Поля станут доступными для редактирования. Назначение кнопки **Редактировать** изменится на **Подключить**.
- 2) Нажать функцию  справа от параметров сервера, который необходимо удалить.

Поля с параметрами указанного сервера будут удалены из списка.

- 3) Для подключения нового списка серверов нажать кнопку **Подключить**.

8.7.10 Настройка отправки зафиксированных событий в виде SNMP trap-сообщений на сторонние ресурсы

8.7.10.1 Доступ к функции. Назначение и состав

При необходимости можно настроить процесс передачи на ресурсы корпоративной сети данных о событиях, зафиксированных Подсистемой мониторинга «Горизонт-ВС», в виде SNMP trap-сообщений.

Функция настройки отправки зафиксированных событий в виде SNMP trap-сообщений доступна в подразделе интерфейса

«Администрирование» → **«Настройки»** (Рисунок 724). Функция реализована в области **«Настройка отправки SNMP trap-сообщений»** и предназначена для:

- настройки отправки на сторонние ресурсы зафиксированных Подсистемой мониторинга «Горизонт-ВС» событий в виде SNMP trap-сообщений;
- включение/выключение передачи данных о зафиксированных событиях при наличии настроенного взаимодействия со сторонними ресурсами посредством SNMP trap-сообщений (тумблер **Активировать рассылку**).

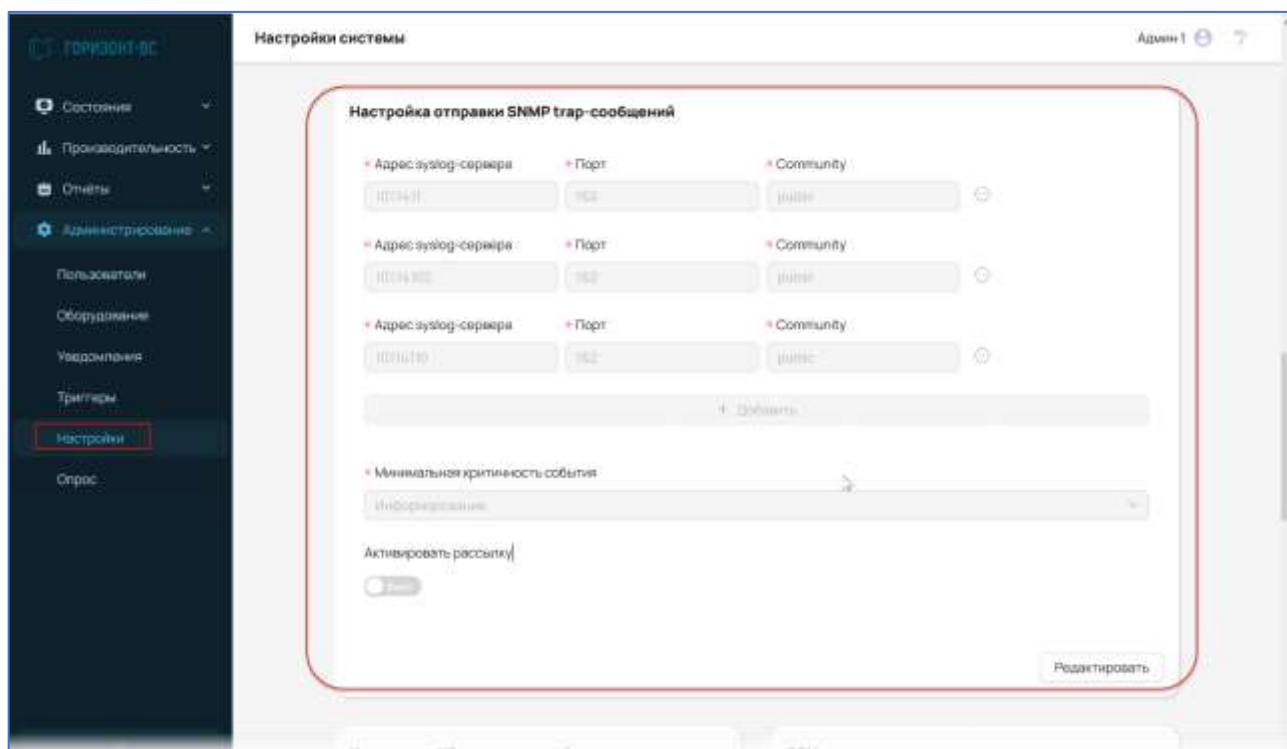


Рисунок 724 - Область настройки отправки зафиксированных событий в виде SNMP trap-сообщений

Область «**Настройка отправки SNMP trap-сообщений**» содержит следующие параметры и функции:

- список syslog-серверов для рассылки trap-сообщений в формате:
 - **Адрес syslog-сервера** – ip-адрес ресурса в корпоративной сети, на который будут передаваться зафиксированные события в виде SNMP trap-сообщений (используется syslog-сервер);
 - **Порт** – порт ресурса, на который будут приходить SNMP trap-сообщения от Подсистемы мониторинга.
 - **Community** – имя сообщества для взаимодействия по протоколу SNMP.
- **+Добавить** – функция добавления в список нового ресурса.
- **⊖** – функция удаления сервера из списка ресурсов.

- **Минимальная критичность события** – список критичности событий Подсистемы мониторинга для создания фильтра отправляемых на сторонние ресурсы событий. Если статус события, зафиксированного Подсистемой мониторинга, выше или равен установленному порогу минимальной критичности, то данные о событии передаются на сторонние ресурсы в виде SNMP trap-сообщений, если ниже – не передаются. Список содержит следующие позиции:
 - Информирование;
 - Предупреждение;
 - Критическая ошибка;
 - Неизвестная ошибка.
- Редактировать / Подключить – функции редактирования/подключения списка серверов.

8.7.10.2 Настройка отправки зафиксированных событий в виде SNMP trap-сообщений после установки Подсистемы мониторинга

После установки Подсистемы мониторинга в области «**Настройка отправки SNMP trap-сообщений**» отобразятся пустые поля настройки (Рисунок 725).

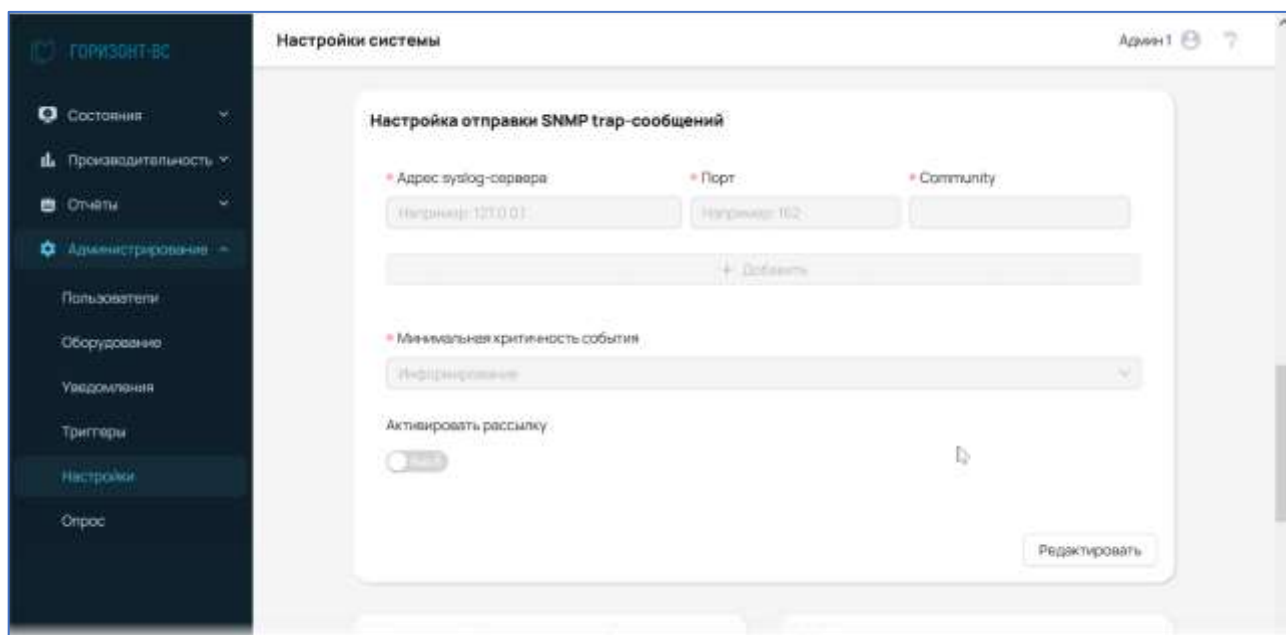


Рисунок 725 - Область настройки отправки зафиксированных событий в виде SNMP trap-сообщений после установки Подсистемы мониторинга

Для настройки отправки зафиксированных событий в виде SNMP trap-сообщений необходимо выполнить следующие действия:

- 1) Нажать кнопку **Редактировать**. Поля станут доступны для ввода данных. Назначение кнопки **Редактировать** изменится на **Подключить**.
- 2) В соответствующих полях ввести ip-адрес стороннего ресурса, номер порта на ресурсе и имя сообщества (community) для взаимодействия по протоколу SNMP (все поля обязательны для заполнения). Подробное описание полей – см. п.0.
- 3) Если для приема отправленных сообщений необходимо настроить еще один ресурс, то нажать функцию **+Добавить**. Появятся поля **Адрес syslog-сервера**, **Порт** и **Community** для ввода параметров и подключения еще одного ресурса для отправки SNMP trap-сообщений.
- 4) Ввести в поля **Адрес syslog-сервера**, **Порт** и **Community** данные нового ресурса.

Повторить п. 3) и 4) данного алгоритма столько раз, сколько ресурсов необходимо подключить для получения trap-сообщений от Системы мониторинга.

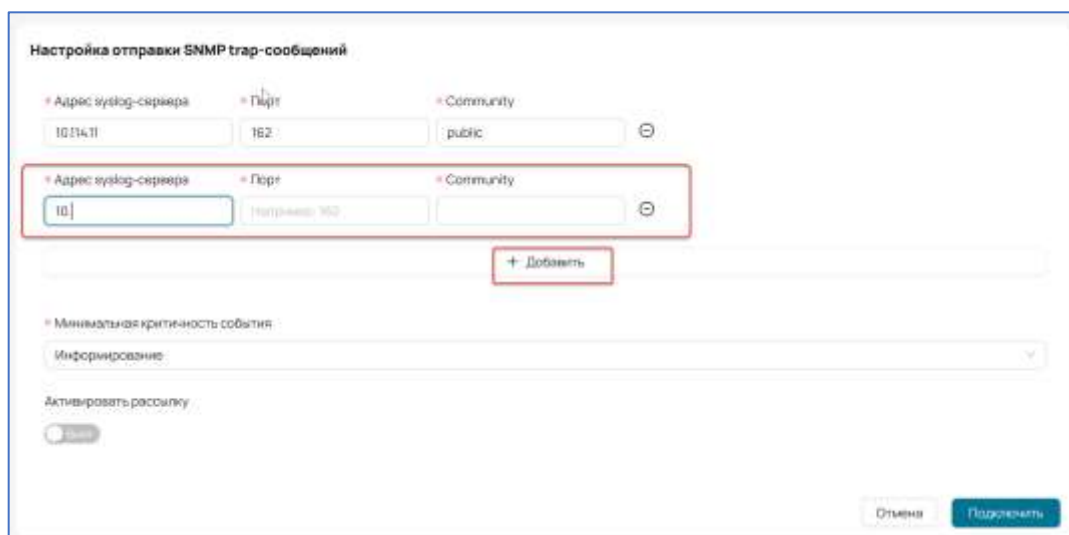


Рисунок 726 - Ввод параметров нового ресурса

- 5) Выбрать в раскрывающемся списке **Минимальная критичность события** необходимое значение порога критичности. Подробное описание списка.

Критичность события устанавливается единая для всех заявленных ресурсов.

- 6) Установить тумблер **Активировать рассылку** в положение **Вкл.** для начала передачи на ресурсы данных о событиях, зафиксированных Подсистемой мониторинга, в виде SNMP trap-сообщений сразу после сохранения настроек. Установить тумблер в положение **Выкл.** для сохранения настроек без осуществления передачи данных.

Активация режима рассылки устанавливается для всех заявленных ресурсов.

- 7) Для сохранения настроек отправки зафиксированных событий в виде trap-сообщений нажать кнопку **Подключить**.

Рисунок 727 - Ввод данных для настройки отправки зафиксированных событий в виде SNMP trap-сообщений

Если все данные были введены без ошибок, то:

- на экране должно отобразиться всплывающее сообщение «Настройки отправки уведомлений SNMP успешно сохранены»;
- данные, введенные в полях, станут недоступными для изменения;
- станет доступна кнопка **Редактировать**.

8.7.10.3 Редактирование настроек взаимодействия со сторонними ресурсами с использованием SNMP trap-сообщений

Доступны следующие изменения настроек отправки SNMP trap-сообщений:

- редактирование параметров ресурсов (адрес syslog-сервера, порт и сообщество);
- изменение списка ресурсов – удаление серверов из списка или добавление новых серверов;
- редактирование минимального уровня критичности отправляемых сообщений;

- активировать или деактивировать рассылку.

Для корректировки параметров взаимодействия выполнить следующие действия:

- 1) Нажать кнопку **Редактировать**. Поля станут доступными для редактирования. Назначение кнопки **Редактировать** изменится на **Подключить**.
- 2) Провести необходимую корректировку данных.
- 3) Нажать кнопку **Подключить**.

Если все новые данные были введены без ошибок, то:

- на экране должно отобразиться всплывающее сообщение «Настройки отправки уведомлений SNMP успешно сохранены»;
- данные, введенные в полях, станут недоступными для изменения;
- станет доступна кнопка **Редактировать**.

8.7.10.4 Управление списком ресурсов для приема SNMP trap-сообщений

В список ресурсов можно добавить новые адреса рассылки, либо удалить из списка существующие.

Для **добавления** нового syslog-сервера как ресурса для приема trap-сообщений, в список адресов рассылки сообщений от Подсистемы мониторинга необходимо выполнить следующие действия:

- 1) Нажать кнопку **Редактировать**. Поля станут доступными для редактирования. Назначение кнопки **Редактировать** изменится на **Подключить**.
- 2) Нажать функцию **+Добавить**. Появятся поля **Адрес syslog-сервера**, **Порт** и **Community** для ввода параметров нового ресурса.

- 3) Ввести в поля **Адрес syslog-сервера**, **Порт** и **Community** данные нового ресурса.

Повторить пункты 2) и 3) данного алгоритма столько раз, сколько ресурсов необходимо подключить для получения событий от Системы мониторинга.

- 4) Для подключения нового списка серверов нажать кнопку **Подключить**.

Для **удаления** ресурса из списка адресов рассылки сообщений от Подсистемы мониторинга необходимо выполнить следующие действия:

- 1) Нажать кнопку **Редактировать**. Поля станут доступными для редактирования. Назначение кнопки **Редактировать** изменится на **Подключить**.
- 2) Нажать функцию ⊖ справа от параметров сервера, который необходимо удалить.

Поля с параметрами указанного сервера будут удалены из списка.

- 3) Для подключения нового списка ресурсов нажать кнопку **Подключить**.

8.7.11 Изменение УЗ, используемой для подключения к СГУ

8.7.11.1 Доступ к функции

Функция изменения УЗ, используемой для подключения к СГУ, доступна в подразделе интерфейса **«Администрирование»** → **«Настройки»** (см. **Ошибка! Источник ссылки не найден.**).

Смена учетной записи, используемой для подключения к СГУ, требуется в случае изменения в Системе виртуализации «Горизонт-ВС» параметров сервисной учетной записи. Создание сервисной учетной записи приведено в отдельном документе *«Подсистема мониторинга «Горизонт-ВС». Руководство по установке и настройке ПО»*. Данные о смене параметров предоставляются администраторами Системы виртуализации «Горизонт-ВС». После смены учетной записи Подсистема мониторинга будет

подключаться к СГУ с помощью новой учетной записи для получения информации о компонентах «Горизонт-ВС».

Функция реализована в области «**Изменение УЗ, используемой для подключения СГУ**». Область содержит следующие параметры (поля): **Имя пользователя** и **Пароль** – соответственно логин и пароль сервисного пользователя Системы виртуализации «Горизонт-ВС», который осуществляет подключение «Горизонт-ВС» к подсистеме мониторинга.

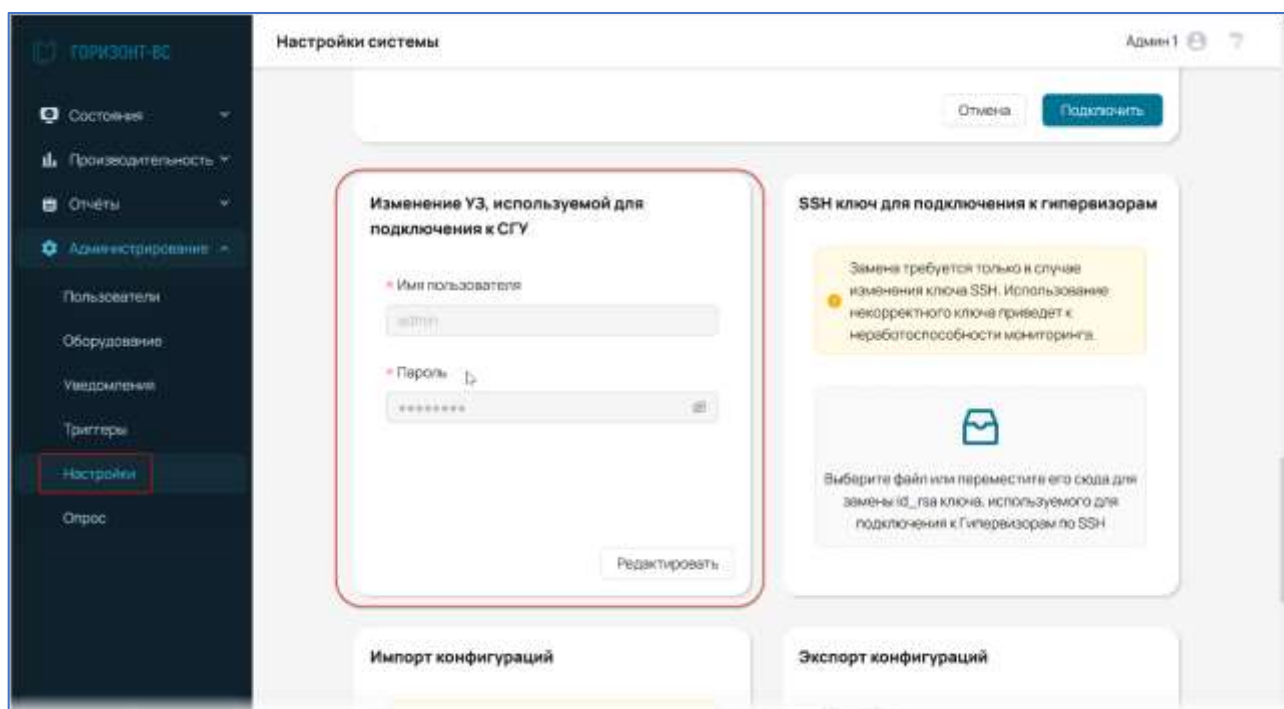


Рисунок 728 - Изменение данных учетной записи, используемой для подключения к СГУ

8.7.11.2 Ввод данных новой учетной записи

Для смены учетной записи необходимо выполнить следующие действия:

- 1) Нажать кнопку **Редактировать**. Поля станут доступны для ввода данных. Назначение кнопки **Редактировать** изменится на **Сохранить**.

- 2) Ввести в полях **Имя пользователя** и **Пароль** новые данные учетной записи для подключения к СГУ.
- 3) Нажать кнопку **Сохранить**.

8.7.12 Изменение ключа SSH, используемого для подключения к гипервизору

8.7.12.1 Доступ к функции

В случае изменения SSH ключа, используемого для подключения к гипервизорам «Горизонт-ВС», требуется загрузить в Подсистему мониторинга новый ключ **id_rsa** через веб-интерфейс Подсистемы мониторинга. Данный ключ используется для опроса Подсистемой мониторинга параметров гипервизора с помощью Linux-команд с предварительным подключением по SSH.

Функция изменения ключа SSH, используемого для подключения к гипервизору, доступна в подразделе интерфейса **«Администрирование»** → **«Настройки»** (Рисунок 729). Функция реализована в области **«SSH ключ для подключения к гипервизорам»**, которая содержит поле загрузки файла нового ключа.

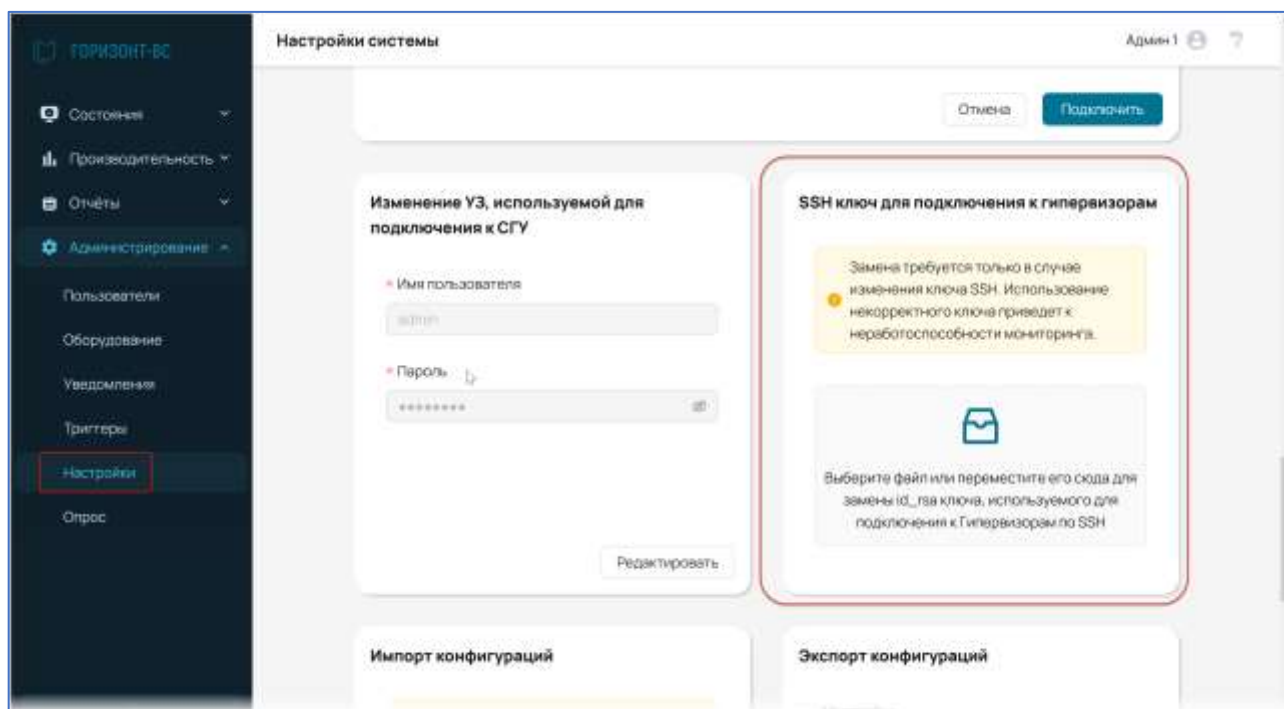


Рисунок 729 - Функция замены SSH ключа для подключения к гипервизорам

8.7.10.2 Замена ключа SSH

Загрузить новый SSH ключ в Подсистему мониторинга можно двумя стандартными способами.

- В области «SSH ключ для подключения к гипервизору» щелкнуть по зоне загрузки файла. В открывшемся стандартном окне проводника выбрать нужную директорию и файл с ключом и нажать кнопку **Открыть**.
- Одновременно с разделом **«Администрирование»** → **«Настройки»** веб-интерфейса Подсистемы мониторинга открыть на экране директорию, в которой находится файл нового SSH ключа. Перетащить мышкой файл ключа из директории в веб-интерфейс Подсистемы мониторинга в зону загрузки файла области «SSH ключ для подключения к гипервизору».

8.7.12 Импорт конфигураций Подсистемы мониторинга

8.7.12.1 Доступ к функции

Функция импорта конфигураций Подсистемы мониторинга доступна в подразделе интерфейса **«Администрирование»** → **«Настройки»** (Рисунок 730) и обеспечивает загрузку в Подсистему мониторинга ранее сохранённых в формате .json конфигураций Подсистемы. Функция предназначена:

- для быстрого восстановления произведённых настроек Подсистемы в случае полной переустановки или при ручном сбросе существующей конфигурации;
- для возврата к более ранним настройкам Подсистемы при необходимости.
- для копирования и переноса настроек между разными экземплярами Подсистемы

Функция реализована в области **«Импорт конфигураций»**, которая содержит поле загрузки файла в формате .json с сохранёнными ранее конфигурациями Подсистемы мониторинга.

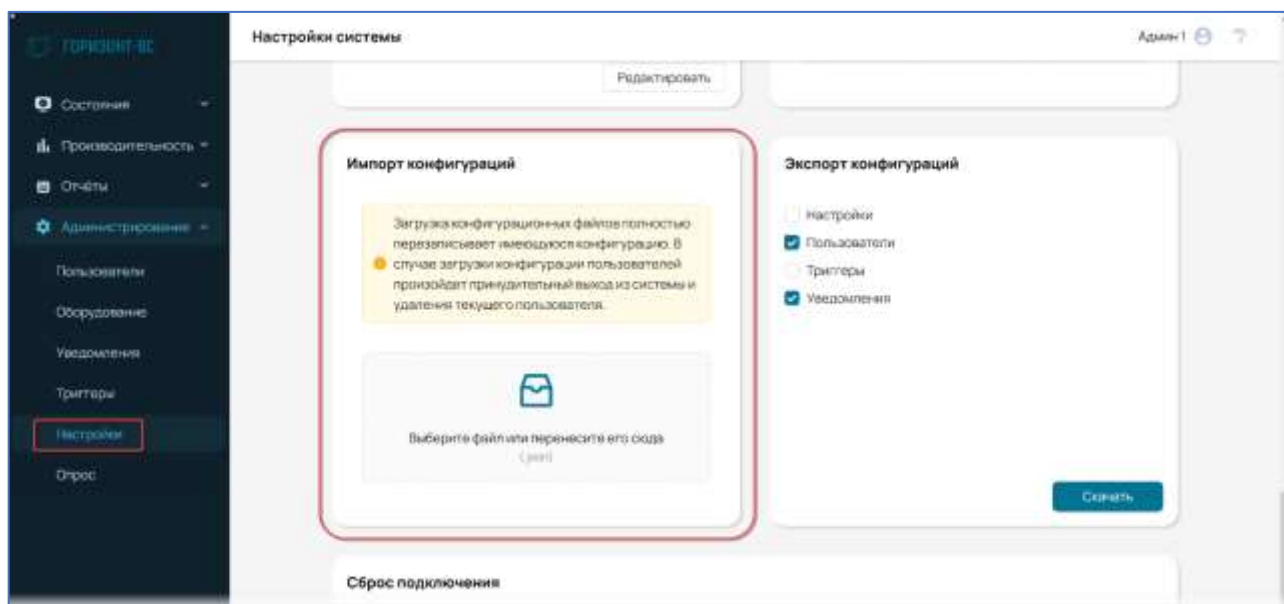


Рисунок 730 - Импорт конфигураций

8.7.13.2 Импорт файлов с конфигурациями

Загрузить конфигурации в Подсистему мониторинга можно двумя стандартными способами.

- В области «Импорт конфигураций» щелкнуть по зоне загрузки файла (см. **Ошибка! Источник ссылки не найден.**). В открывшемся стандартном окне проводника выбрать нужную директорию и файл .json с конфигурацией, далее нажать кнопку **Открыть**.
- Одновременно с разделом **«Администрирование» → «Настройки»** веб-интерфейса Подсистемы мониторинга открыть на экране директорию, в которой находятся файлы конфигураций. Перетащить мышкой нужный файл конфигурации из директории в веб-интерфейс Подсистемы мониторинга в зону загрузки файла области «Импорт конфигураций».

После выбора файла дождаться конца процесса загрузки и появления сообщения **«Конфигурация успешно загружена»**.

8.7.13 Экспорт конфигураций Подсистемы мониторинга

8.7.13.1 Доступ к функции

Функция экспорта конфигураций Подсистемы мониторинга доступна в подразделе интерфейса **«Администрирование»** → **«Настройки»** (см. Рисунок 0.731) и предназначена для формирования и выгрузки из Подсистемы мониторинга текущих конфигураций в виде файлов формата .json. Экпортируемые параметры конфигураций предназначены:

- для быстрого восстановления произведенных настроек Подсистемы в случае полной переустановки или при ручном сбросе существующей конфигурации;
- для возврата к более ранним настройкам Подсистемы при необходимости.
- для копирования и переноса настроек между разными экземплярами Подсистемы

Поддерживается экспорт следующих конфигураций:

- Настройки;
- Пользователи;
- Триггеры;
- Уведомления.

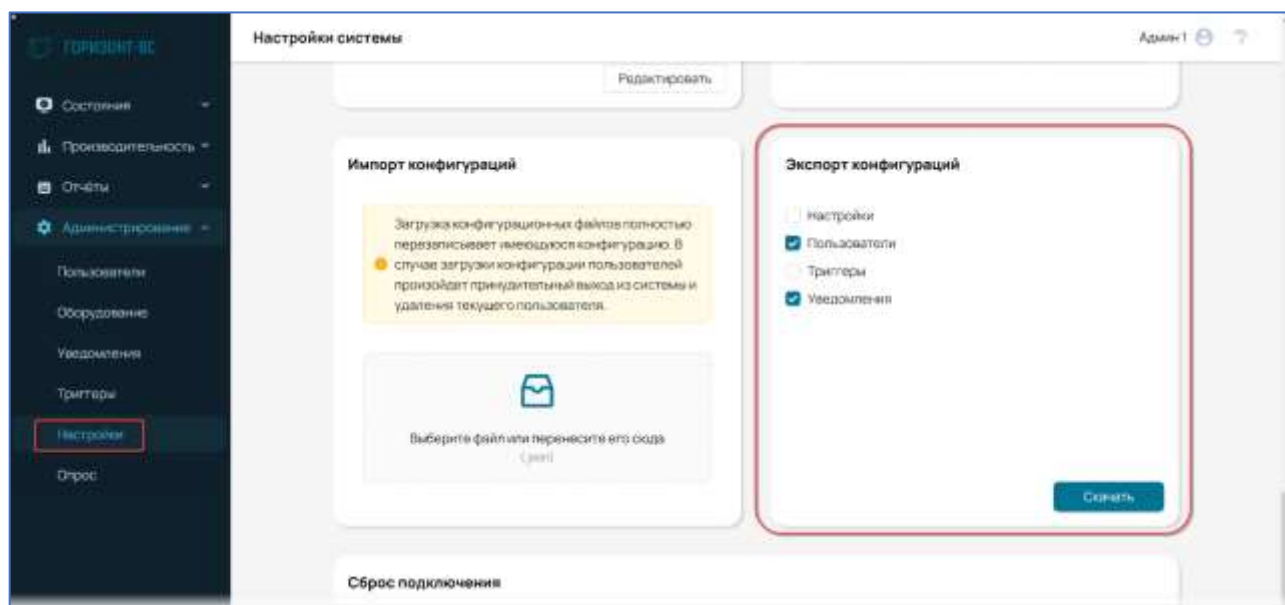


Рисунок 0.731 – Экспорт конфигураций

8.7.12.2 Экспорт конфигураций

Для текущих конфигураций Подсистемы мониторинга необходимо:

- 1) Выбрать в списке одну или несколько интересующих конфигураций, установив соответствующие флажки (см. Рисунок 0.731).
- 2) Нажать кнопку **Скачать**.
- 3) В открывшемся стандартном окне сохранения файла указать директорию, в которую будет помещён json-файл с конфигурациями, и нажать кнопку **Сохранить**.

Все выбранные для экспорта конфигурации скачиваются в виде единого json-файла в указанную директорию (см. Рисунок 0.732). При необходимости можно скачивать конфигурации каждую отдельно.

По умолчанию устанавливается следующее название json-файла:

<Горизонт-ВС_конфигурации_приложения_дд-мм-гггг_чч-мм>

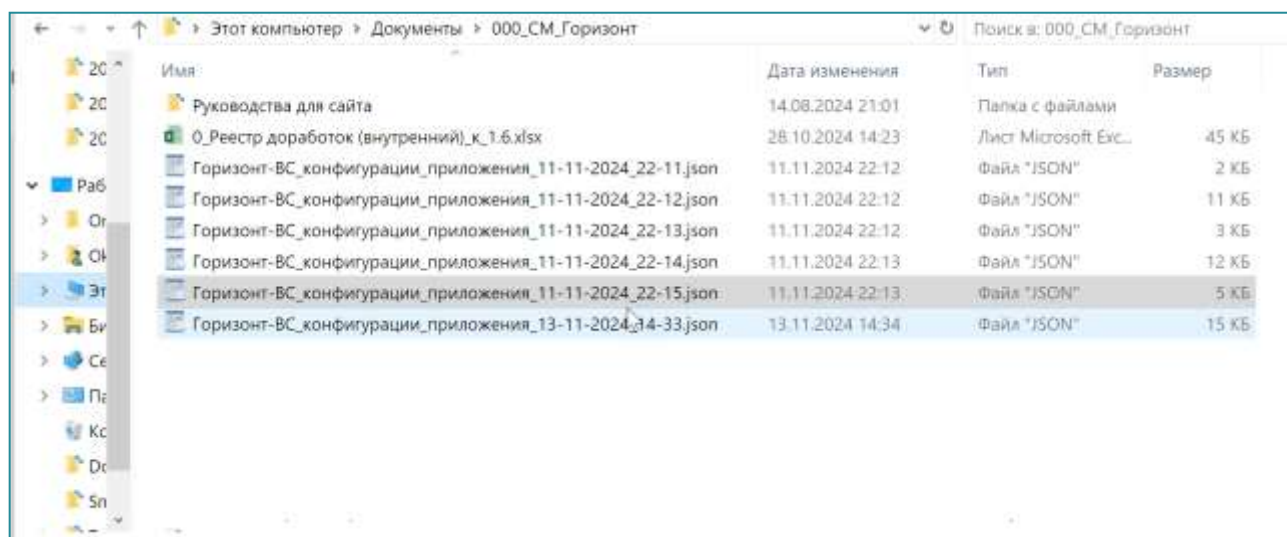


Рисунок 0.732 – Пример экспортированных конфигураций Подсистемы мониторинга

8.7.13 Отключение Подсистемы мониторинга от СГУ

8.7.13.1 Доступ к функции

Функция отключения Подсистемы мониторинга от СГУ доступна в подразделе интерфейса **«Администрирование»** → **«Настройки»** (Рисунок 733) и

предназначена для отключения Подсистемы мониторинга от СГУ, для сброса настроек и переподключения к иному СГУ.

Функция реализована в области «**Сброс подключения**» как предупреждение о последствиях отключения и кнопки **Сброс**.

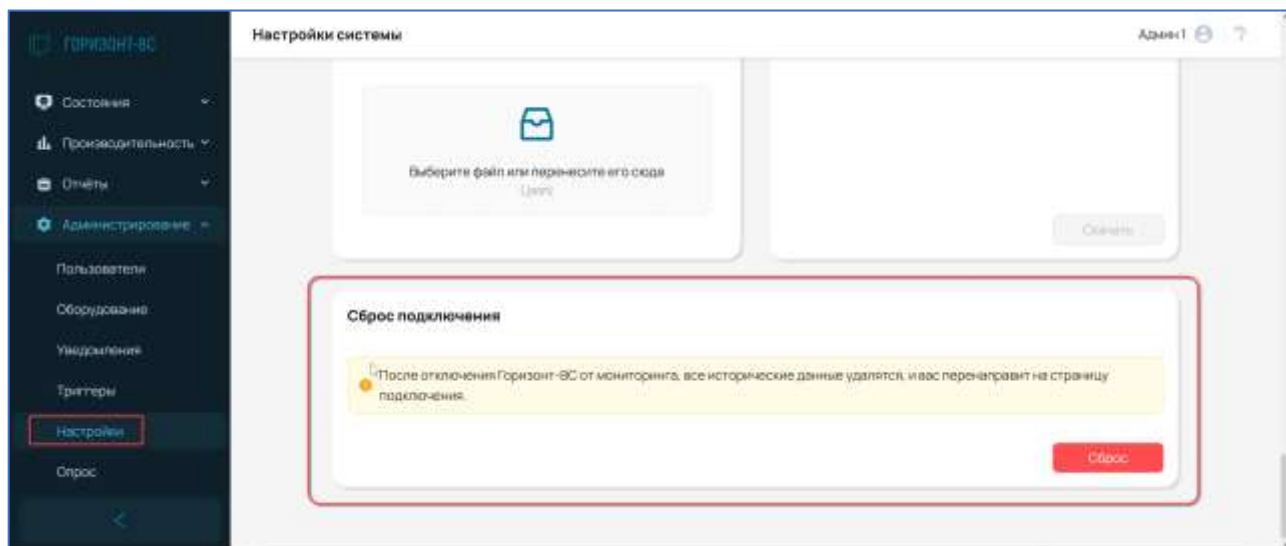


Рисунок 733 - Сброс подключения к СГУ

8.7.13.2 Отключение от СГУ

Для сброса подключения Подсистемы мониторинга к СГУ необходимо выполнить следующие действия:

- 1) В области «Сброс подключения» нажать кнопку **Сброс**.
- 2) В открывшемся окне подтверждения нажать **Подтверждаю** (Рисунок 734).

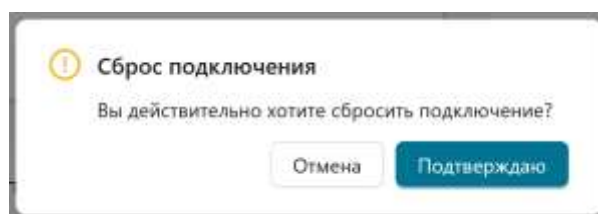


Рисунок 734 - Окно подтверждения сброса подключения к СГУ

Текущее подключение к СГУ будет сброшено. На экране автоматически откроется окно подключения Подсистемы мониторинга к СГУ. Подробно процесс подключения к СГУ приведен в п.0.

Подключение к Горизонт-ВС

1

Для дальнейшей работы с системой мониторинга необходимо произвести подключение к Горизонт-ВС.

* Адрес

Порт

2634

* Имя пользователя

admin

* Пароль

•••••

Подключить

1

Подключение

2

Обнаружение

Рисунок 735

8.7.14 Управление мониторингом объектов «Горизонт-ВС»

8.7.14.1 Доступ к функции. Назначение и состав

Функция управления опросом объектов мониторинга Системы виртуализации «Горизонт-ВС» доступна в подразделе интерфейса

«Администрирование» → «Опрос» (см. **Ошибка! Источник ссылки не найден.**).

Функция предназначена для:

- настройки параметров частоты опроса объектов мониторинга,
- включения/отключения опроса мониторинга объектов.

Подраздел «Опрос» состоит из следующих вкладок:

- Платформа;
- Мониторинг;
- СГУ;
- Гипервизоры;
- ВМ;
- Оборудование.

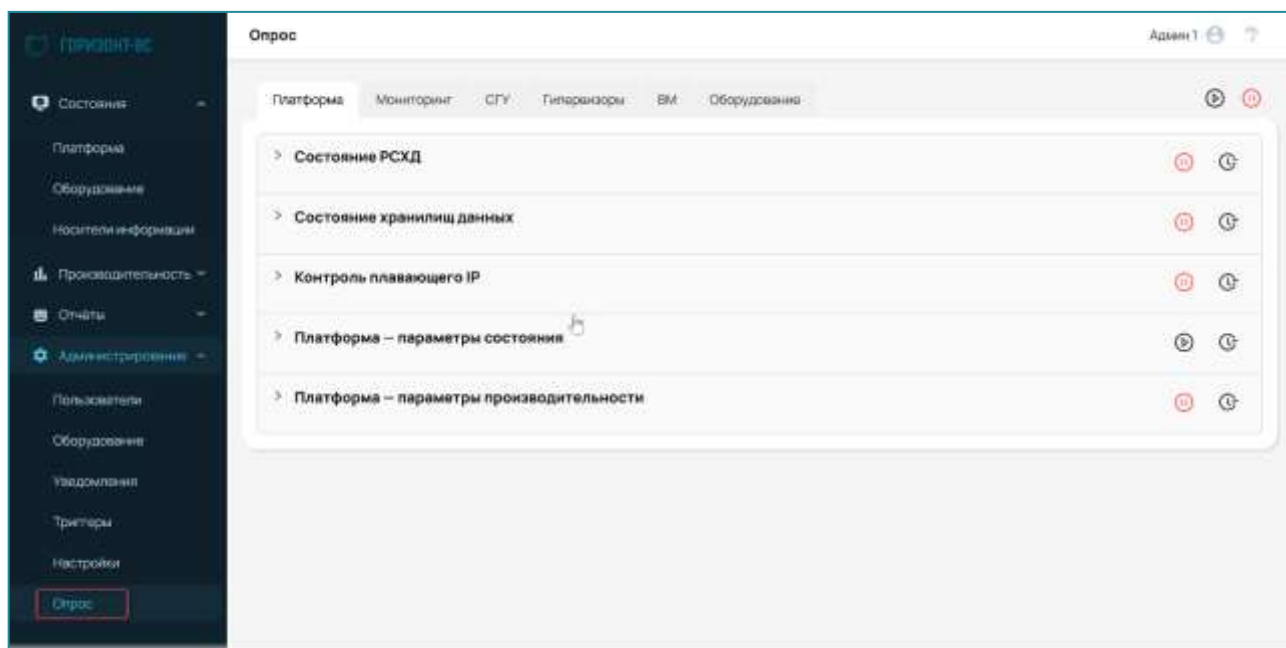


Рисунок 736 - Подраздел «Опрос»

Каждая вкладка подраздела содержит следующие данные:

- список сборщиков данных (соответствующие объекту на вкладке), которые можно установить на мониторинг;
-  – значок, расположенный в правом верхнем углу: «Возобновить работу всех сборщиков данных». Функция возобновляет работу всех сборщиков, указанных на выбранной вкладке.
-  – значок, расположенный в правом верхнем углу: «Приостановить работу всех сборщиков данных». Функция останавливает работу всех сборщиков, указанных на выбранной вкладке.
-  /  – значки в строке сборщика в таблице сборщиков данных: соответственно «Возобновить работу сборщика данных»/ «Приостановить работу сборщика данных».
-  – значок в строке сборщика данных в таблице сборщиков – функция выбора временного интервала для опроса.

8.7.14.2 Список сборщиков данных

Ниже в Таблице 5.1 приведен список опрашиваемых Подсистемой мониторинга сборщиков данных Системы виртуализации «Горизонт-ВС».

Таблица 0.1 – Список сборщиков данных, опрашиваемых Подсистемой мониторинга

№	Вкладка	Сборщики данных
1	Платформа	Состояние РСХД Состояние хранилищ данных Контроль плавающего IP Платформа – параметры состояния Платформа – параметры производительности
2	Мониторинг	Свободное место на диске
3	СГУ	Состояние базы данных СГУ Состояние веб-интерфейса СГУ Проверка синхронности БД Состояние серверной части СГУ
4	Гипервизоры	Состояние дисков и RAID массивов Проверка синхронности СГУ и Гипервизоров Параметры производительности Гипервизоров Состояние служб Open vSwitch Состояние служб Libvirt Состояние гипервизора Проверка синхронности системного времени Гипервизоров Состояние интерфейса sys0 Использование дисков Аптайм гипервизора
5	ВМ	Данные по QEMU Состояние виртуальной машины

№	Вкладка	Сборщики данных
6	Оборудование	Опрос параметров по IPMI Материнская плата Процессоры Сетевые карты Оперативная память Датчики питания Носители информации Датчики температуры Блоки питания Датчики вентиляторов

8.7.14.3 Приостановка/Запуск опроса всех сборщиков данных объекта мониторинга

В Подсистеме мониторинга реализована возможность Приостановить / Запустить одновременно все сборщики данных на выбранной вкладке. Для этого используются значки  и , расположенные в правом верхнем углу.

Для приостановки всех сборщиков данных необходимо:

- 1) Нажать значок  в правом верхнем углу экрана.

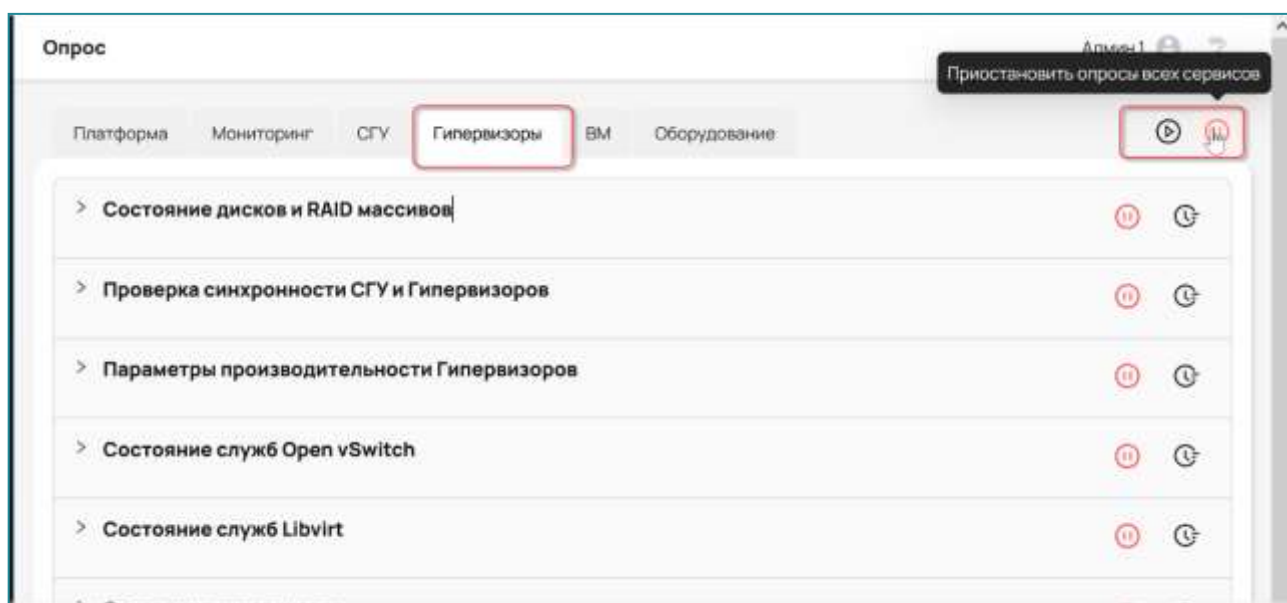


Рисунок 737- Функции Приостановить/Запустить опросы всех сборщиков данных гипервизоров

- 2) Нажать кнопку **Подтверждаю** в открывшемся окне подтверждения приостановки.

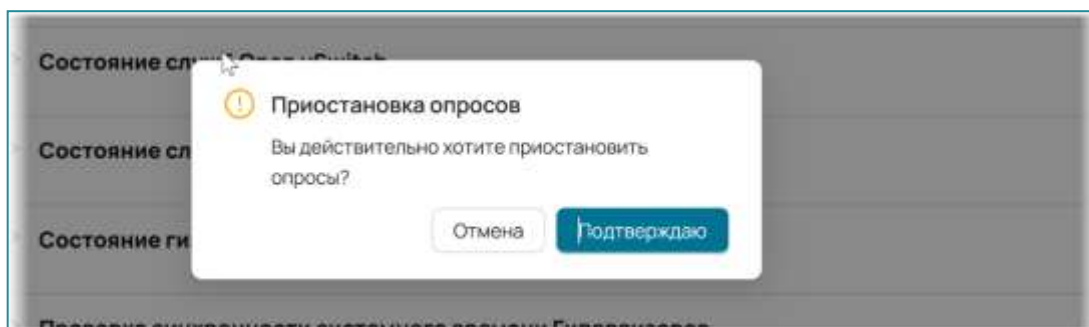


Рисунок 738 - Окно подтверждения приостановки опроса

- 3) Дождаться окончания процесса применения изменений и появления сообщения «Изменения успешно применены».

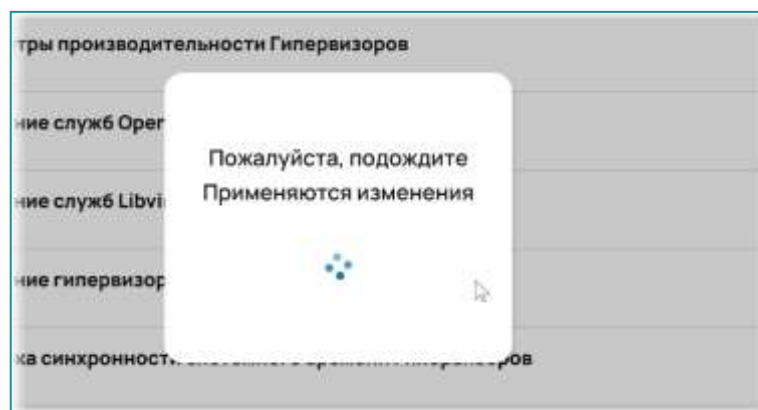


Рисунок 739 - Ожидание завершения процесса применения

В результате проведенного изменения все сборщики данных будут отмечены как приостановленные.

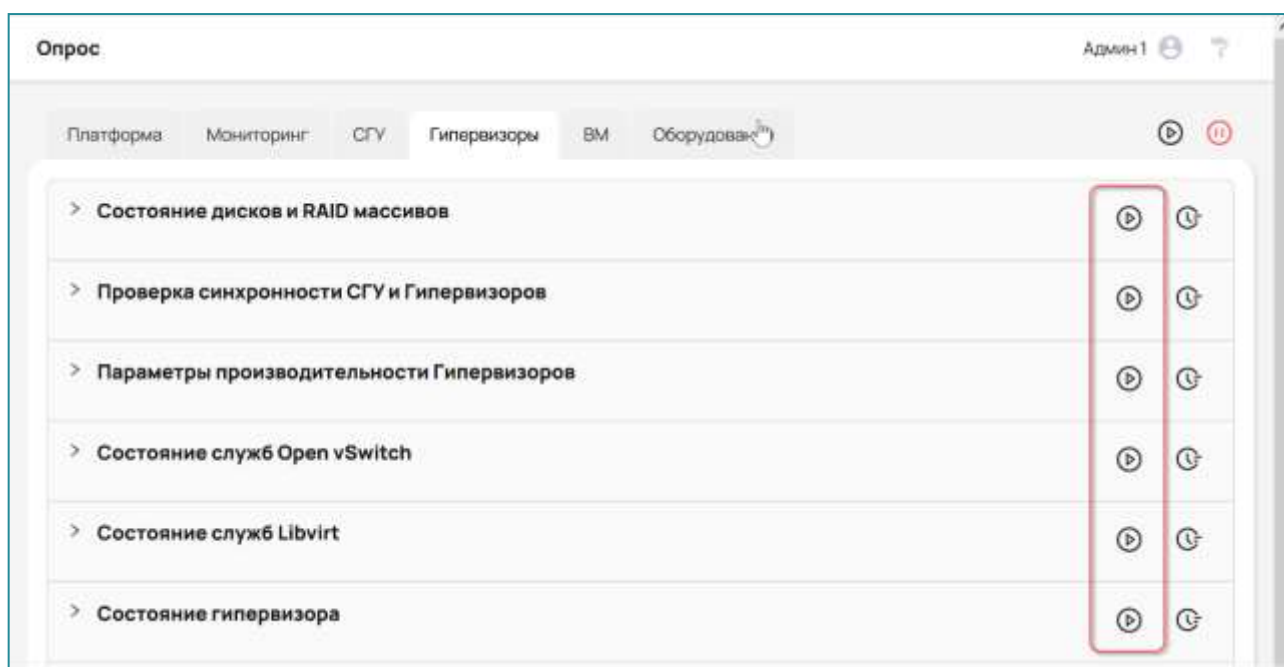


Рисунок 740 - Пример приостановки опроса на всех сборщиках данных гипервизоров

Для возобновления опроса всех сборщиков данных используется значок  (Возобновить опросы всех сборщиков данных) в правом верхнем углу экрана.

Для возобновления опроса проводятся действия, аналогичные действиям для приостановки опроса (см. алгоритм выше).

8.7.14.4 Приостановка/Запуск отдельного сборщика данных

В Подсистеме мониторинга реализована возможность Приостановить / Запустить отдельный сборщик данных на выбранной вкладке. Для этого используется значок-маркер состояния сборщика данных

 / , расположенный в строке сборщика данных справа.

Для приостановки сборщика данных необходимо нажать значок  в строке останавливаемого сборщика данных. При этом значок изменится на .

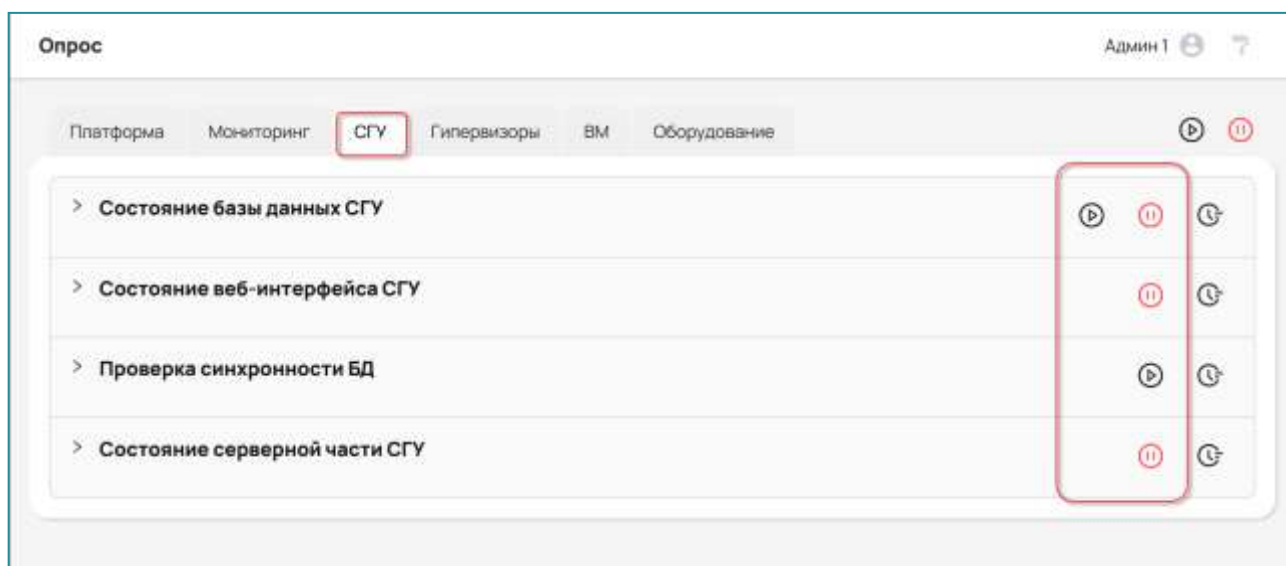


Рисунок 741 - Пример приостановки опроса на отдельно взятом сборщике данных

Если сборщик данных работает на нескольких узлах, то возможно приостановить /запустить сборщик на отдельно взятом узле. При этом в строке сборщика данных будут отображаться оба значка  и  одновременно .

Для этого необходимо:

- 1) Раскрыть список узлов сборщика данных, щелкнув по стрелке слева от названия сборщика. Откроется список узлов, на которых работает данный сборщик данных .
- 2) Для приостановки/запуска сборщика данных на выбранном узле использовать тумблер **Активность** – соответствующие положения Выкл./Вкл.
- 3) Подтвердить внесенные изменения в окне подтверждения и дождаться окончания процесса применения изменений.

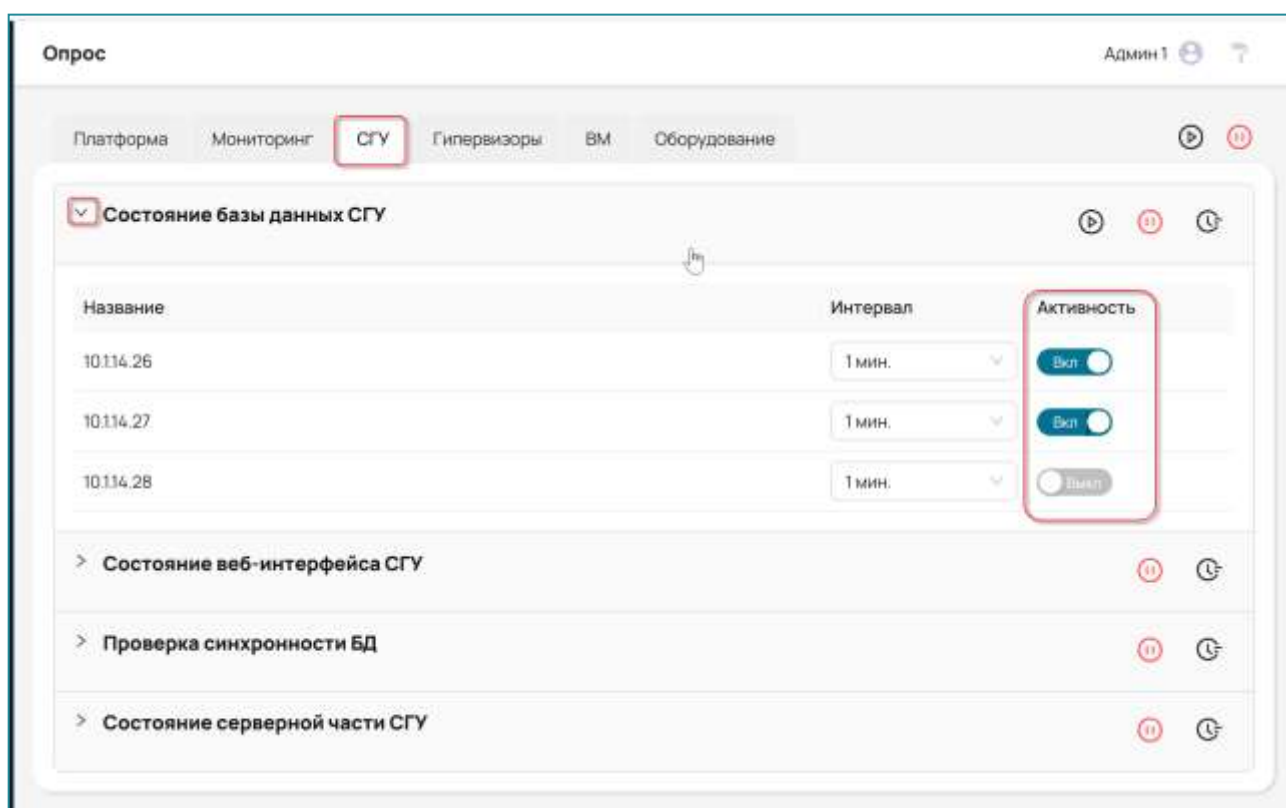


Рисунок 742 - Приостановка / Запуск сборщика данных на разных узлах

8.7.14.5 Настройка временного интервала опроса

Подсистема мониторинга позволяет настроить интервал времени для опроса:

- для отдельного сборщика данных;

- для сборщика данных, работающего на конкретном узле.

Для установки нового временного интервала опроса для сборщика данных необходимо выполнить следующие действия:

- 1) Подвести курсор мыши к значку , расположенному в строке интересующего сборщика данных.

На экране откроется список возможных временных интервалов опроса.

- 2) Выбрать в списке новый интервал опроса.
- 3) Подтвердить внесённые изменения в окне подтверждения и дождаться окончания процесса применения изменений.

Если сборщик данных работает на нескольких узлах, то заданный таким образом новый интервал опроса будет установлен для всех узлов.

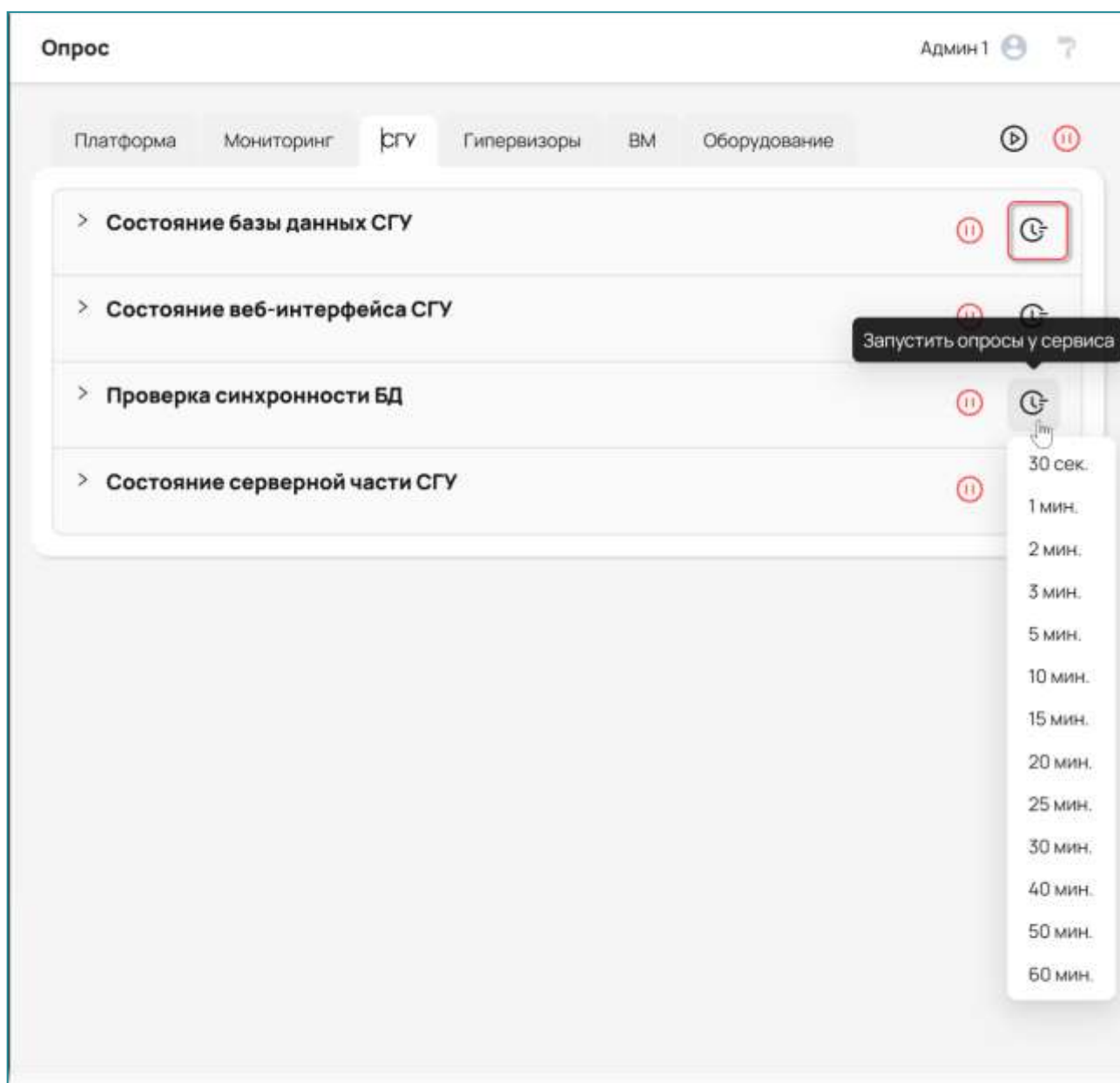


Рисунок 743 - Выбор временного интервала для сбора данных

Для установки нового временного интервала опроса для сборщика данных, работающего на конкретном узле, необходимо выполнить следующие действия:

- 1) Раскрыть список узлов сборщика данных, щелкнув по стрелке слева от названия сборщика. Откроется список узлов, на которых работает данный сборщик.

- 2) Выбрать новый временной интервал опроса для сборщика данных на выбранном узле в раскрывающемся списке **Интервал** (список возможных временных интервалов опроса).
- 3) Подтвердить внесенные изменения в окне подтверждения и дождаться окончания процесса применения изменений.

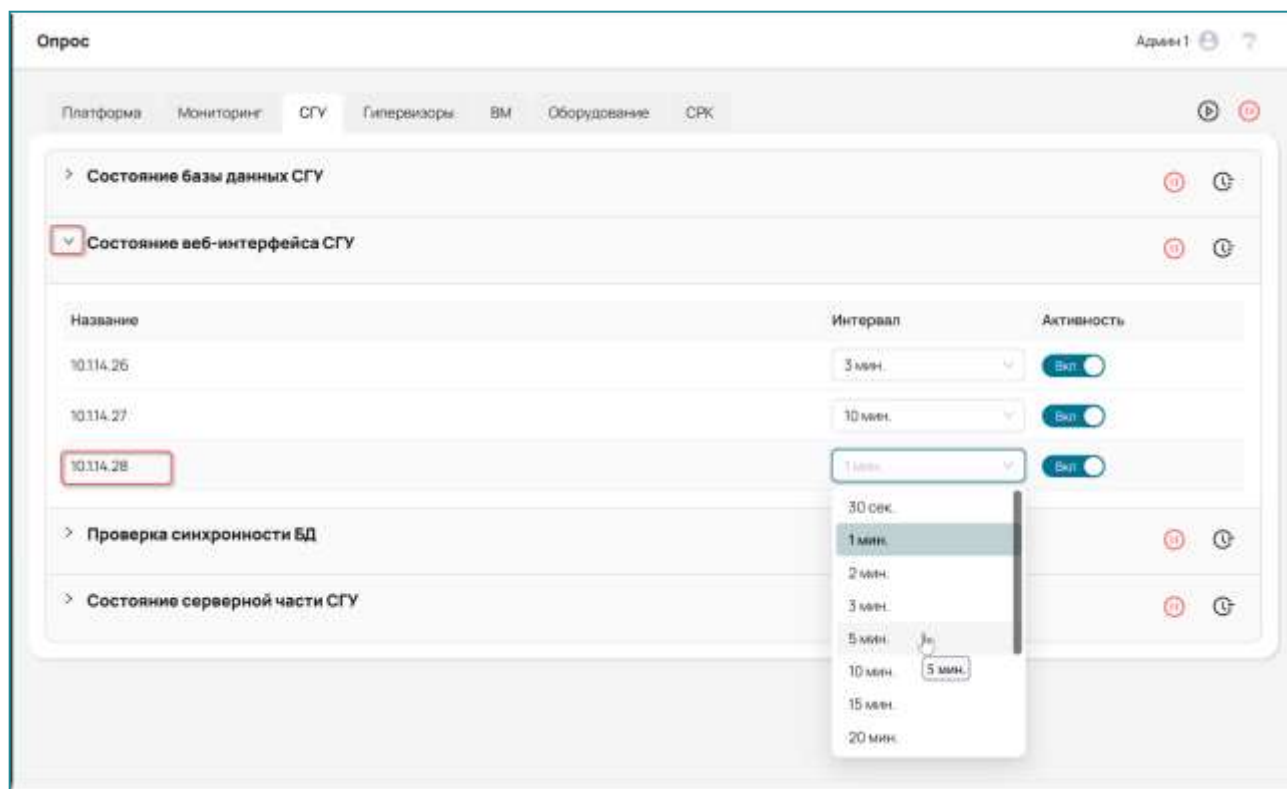


Рисунок 744 - Выбор временного интервала для сборщика данных, работающего на конкретном узле

8.7.15 Формирование диагностических отчётов

8.7.15.1 Доступ к функции

Функция формирования диагностических отчётов доступна в подразделе интерфейса «Отчёты» → «Диагностика» и предназначена для формирования и выгрузки из Подсистемы мониторинга диагностических отчетов состояния Системы

виртуализации «Горизонт-ВС» и входящих в состав компонентов в формате .txt. Диагностические отчеты предназначены для упрощения и более эффективного взаимодействия с службой технической поддержки Горизонт-ВС в случае выявления неполадок.

Поддерживаются следующие виды диагностических отчетов:

- Гипервизоры;
- Лог-файлы гипервизоров;
- СГУ;
- Лог-файлы СГУ;
- Хранилища данных;
- Оборудование (ipmi).

Диагностические отчеты выгружаются в виде архивного файла в формате .zip, содержащего набор диагностических txt-файлов по указанному объекту.

Примечание. Работа с отчётами в подразделах **«События»** и **«Производительность»** приведена в документе *«Подсистема мониторинга «Горизонт-ВС». Руководство пользователя»*.

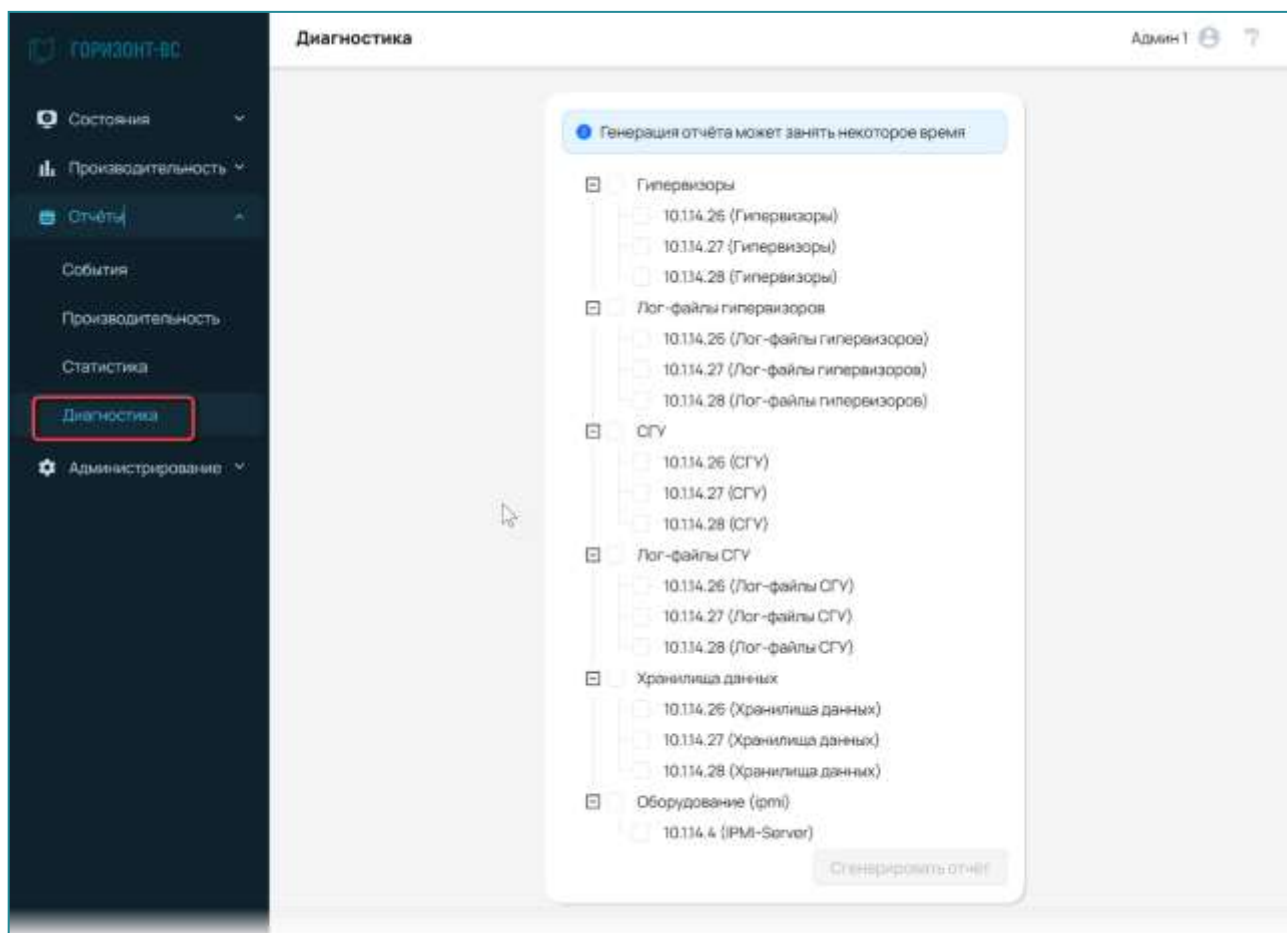


Рисунок 745 - Область формирования и выгрузки диагностических отчетов по объектам СГУ

8.7.15.2 Формирование, выгрузка и просмотр диагностического отчета

Для формирования и выгрузки диагностического отчета необходимо:

- 1) Выбрать в списке один или несколько интересующих объектов (см. Рисунок 0.746).

Генерация отчёта может занять некоторое время

- ☒ Гипервизоры
 - ☒ 10.114.26 (Гипервизоры)
 - ☒ 10.114.27 (Гипервизоры)
 - ☒ 10.114.28 (Гипервизоры)
- ☐ Лог-файлы гипервизоров
 - ☐ 10.114.26 (Лог-файлы гипервизоров)
 - ☐ 10.114.27 (Лог-файлы гипервизоров)
 - ☐ 10.114.28 (Лог-файлы гипервизоров)
- ☒ СГУ
 - ☒ 10.114.26 (СГУ)
 - ☒ 10.114.27 (СГУ)
 - ☒ 10.114.28 (СГУ)
- ☐ Лог-файлы СГУ
 - ☐ 10.114.26 (Лог-файлы СГУ)
 - ☐ 10.114.27 (Лог-файлы СГУ)
 - ☐ 10.114.28 (Лог-файлы СГУ)
- ☐ Хранилища данных
 - ☐ 10.114.26 (Хранилища данных)
 - ☐ 10.114.27 (Хранилища данных)
 - ☐ 10.114.28 (Хранилища данных)
- ☐ Оборудование (ipmi)
 - ☐ 10.114.4 (IPMI-Server)

Сгенерировать отчёт

Рисунок 0.746 – Выбор объектов СГУ для формирования и выгрузки диагностических отчетов

2) Нажать кнопку **Сгенерировать отчёт**.

Должно появиться сообщение об успешной отправке запроса на генерацию отчета (см. Рисунок 0.747). При успешном создании отчёта в Подсистеме мониторинга назначение кнопки **Сгенерировать отчёт** должно поменяться на **Скачать отчёт** (см. Рисунок 0.748).

Внимание! Формирование диагностического отчёта может занимать несколько минут, в зависимости от количества объектов указанных для диагностического отчета. Необходимо дождаться появления кнопки **Скачать отчёт**.

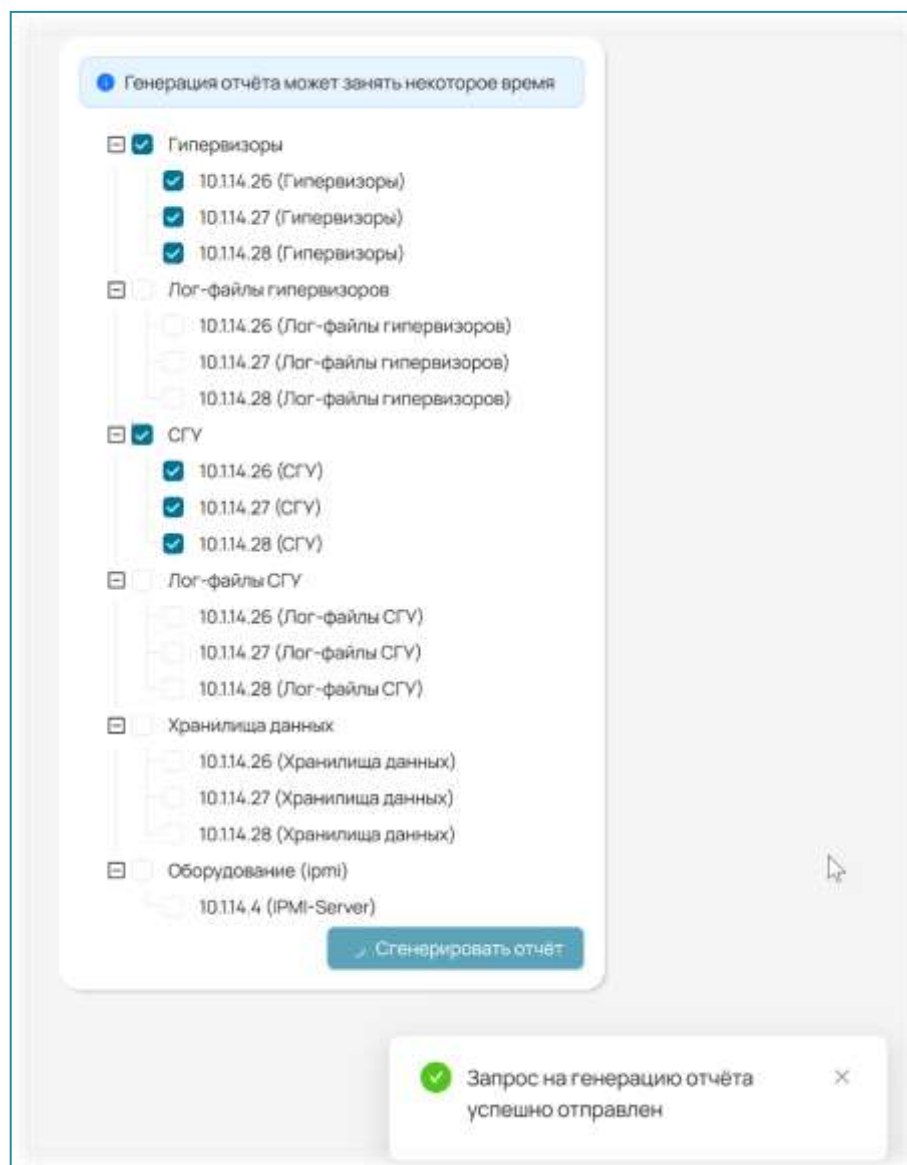


Рисунок 0.747 – Сообщение об успешном запросе на формирование диагностических отчетов по указанным объектам

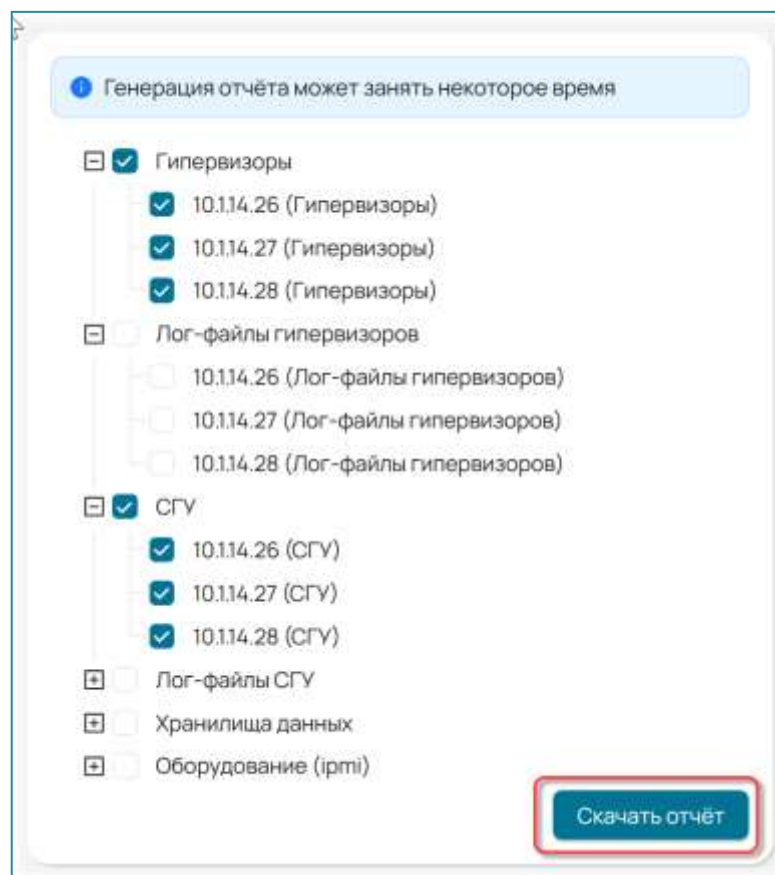


Рисунок 0.748 – Кнопка выгрузки сформированного отчёта

3) Нажать кнопку **Скачать отчёт** (см. Рисунок 0.748).

4) В открывшемся стандартном окне сохранения файла указать директорию, в которую будет помещён zip-файл отчёта, и нажать кнопку **Сохранить**.

По умолчанию устанавливается следующее название zip-файла:

<Горизонт-ВС_отчёт_диагностики_дд-мм-гггг_чч-мм>

Для просмотра диагностических отчётов зайти в директорию, куда был выгружен zip-файл, и открыть архив. Архив содержит набор txt-файлов с диагностикой по объектам (см. Рисунок 0.749 и Рисунок 0.750).

Имя	Тип	Сжатый размер	Защищён п...	Размер	Сжатие	Дата изменения
hcs_diagnostic_10.1.14.26_docker_exec_hcs_oneynet_show_0.txt	Текстовый документ	1 КБ	Нет	1 КБ	0%	13.11.2024 14:15
hcs_diagnostic_10.1.14.26_docker_ps_a.txt	Текстовый документ	1 КБ	Нет	1 КБ	0%	13.11.2024 14:14
hcs_diagnostic_10.1.14.26_for_id_in__docker_exec_hcs_oneynet_show_0.txt	Текстовый документ	3 КБ	Нет	3 КБ	0%	13.11.2024 14:15
hcs_diagnostic_10.1.14.26_for_id_in__docker_exec_hcs_oneynet_list.txt	Текстовый документ	1 КБ	Нет	5 КБ	0%	13.11.2024 14:15
hcs_diagnostic_10.1.14.26_for_id_in__docker_exec_hcs_oneynet_list.txt	Текстовый документ	15 КБ	Нет	15 КБ	0%	13.11.2024 14:15
hcs_diagnostic_10.1.14.26_for_id_in__docker_exec_hcs_oneynet_list.txt	Текстовый документ	2 КБ	Нет	2 КБ	0%	13.11.2024 14:15
hcs_diagnostic_10.1.14.27_docker_exec_hcs_oneynet_show_0.txt	Текстовый документ	1 КБ	Нет	1 КБ	0%	13.11.2024 14:15
hcs_diagnostic_10.1.14.27_docker_ps_a.txt	Текстовый документ	1 КБ	Нет	1 КБ	0%	13.11.2024 14:15
hcs_diagnostic_10.1.14.27_for_id_in__docker_exec_hcs_oneynet_show_0.txt	Текстовый документ	3 КБ	Нет	3 КБ	0%	13.11.2024 14:15
hcs_diagnostic_10.1.14.27_for_id_in__docker_exec_hcs_oneynet_list.txt	Текстовый документ	5 КБ	Нет	5 КБ	0%	13.11.2024 14:15
hcs_diagnostic_10.1.14.27_for_id_in__docker_exec_hcs_oneynet_list.txt	Текстовый документ	15 КБ	Нет	15 КБ	0%	13.11.2024 14:15
hcs_diagnostic_10.1.14.27_for_id_in__docker_exec_hcs_oneynet_list.txt	Текстовый документ	2 КБ	Нет	2 КБ	0%	13.11.2024 14:15
hcs_diagnostic_10.1.14.28_docker_exec_hcs_oneynet_show_0.txt	Текстовый документ	1 КБ	Нет	1 КБ	0%	13.11.2024 14:15

Рисунок 0.749 – Пример архива с диагностическими отчётами

```

hcs_diagnostic_10.1.14.27_for_id_in__docker_exec_hcs_oneynet_list.txt - Блокнот
Файл Правка Формат Вид Справка
Command: for id in $(docker exec hcs_oneynet list | awk 'NR > 1 {print $1}'); do docker exec hcs_oneynet show $id

VIRTUAL NETWORK 0 INFORMATION
ID                : 0
NAME              : net-0
USER              : admin
GROUP             : onedadmin
LOCK              : None
CLUSTERS          : 0
BRIDGE            : hvsw0
VN_MAD            : ovswitch
USED LEASES       : 3

PERMISSIONS
OWNER             : um-
GROUP             : ---
OTHER             : ---

VIRTUAL NETWORK TEMPLATE
BRIDGE="hvsw0"
PHYDEV=""
SECURITY_GROUPS="0"
VN_MAD="ovswitch"

ADDRESS RANGE POOL
AR 0
SIZE              : 254
LEASES            : 3

RANGE             FIRST                LAST
MAC               02:00:22:1b:0e:c2    02:00:22:1b:0f:bf

LEASES
AR  OWNER          MAC                IP        IP6
0   V:0            02:00:22:1b:0e:c2    -         -
0   V:1            02:00:22:1b:0e:c3    -         -
0   V:2            02:00:22:1b:0e:c4    -         -

VIRTUAL ROUTERS
  
```

Рисунок 0.750 – Пример диагностического отчёта

8.7.16 Переход в СГУ Системы виртуализации «Горизонт-ВС»

Для того чтобы перейти из Подсистемы мониторинга непосредственно в интерфейс СГУ Системы виртуализации «Горизонт-ВС» необходимо:

- 1) Нажать функцию **СГУ**, расположенную в нижней части зоны основного меню.

В результате проведенного действия на экране на новой странице браузера откроется окно аутентификации пользователя в СГУ «Горизонт-ВС» .

- 2) Для входа в СГУ ввести логин и пароль пользователя Системы виртуализации «Горизонт-ВС».

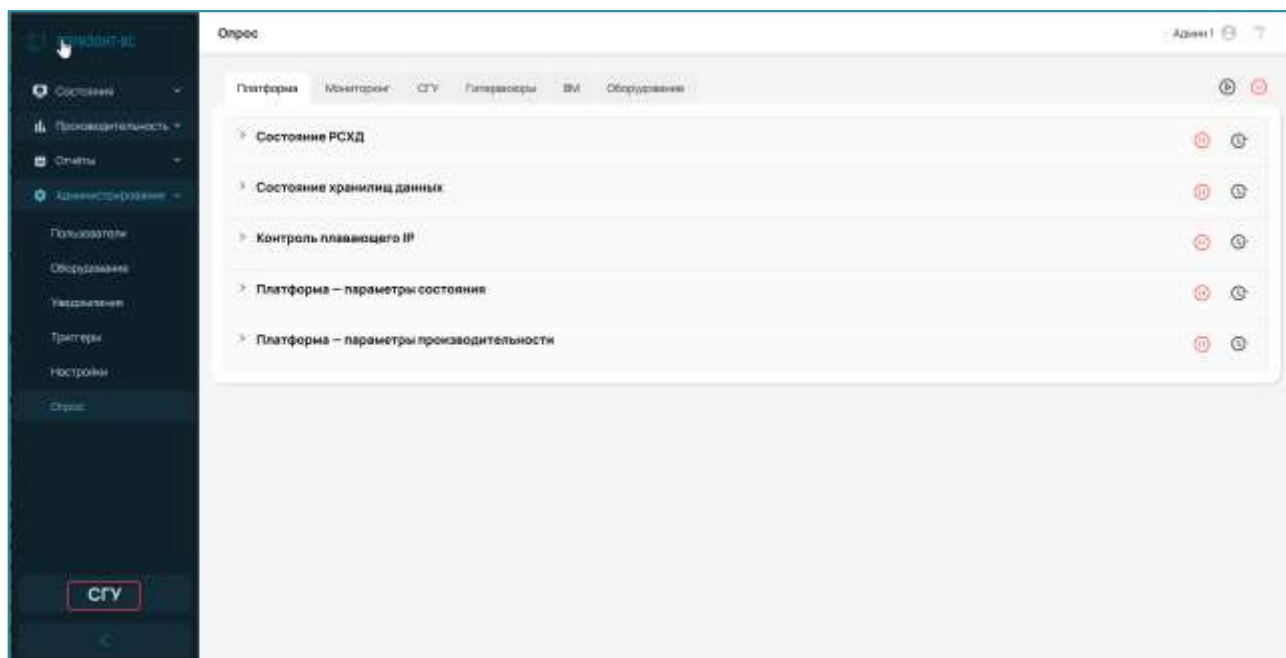


Рисунок 751 - Функция возврата в СГУ Системы виртуализации «Горизонт-ВС»

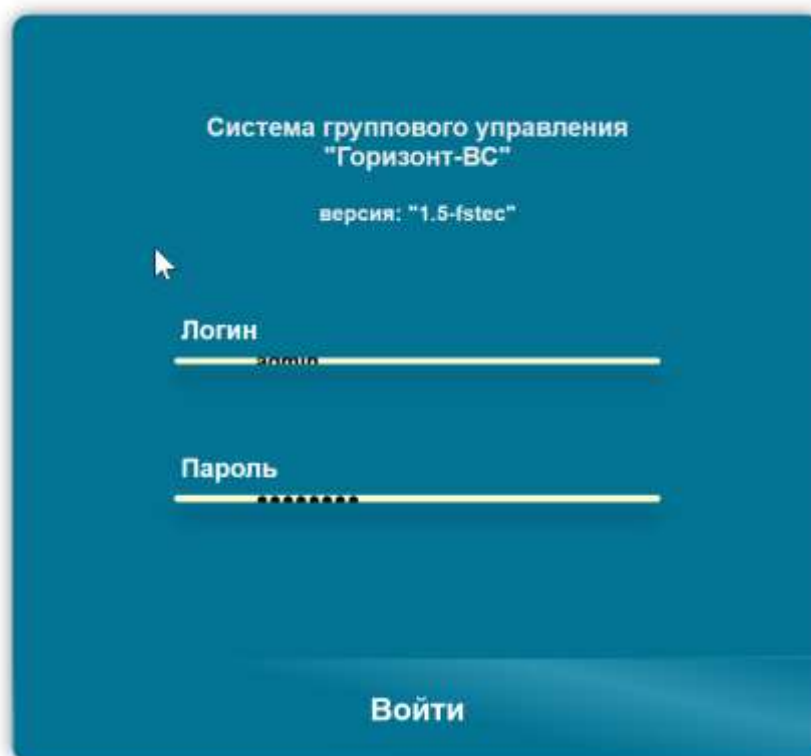


Рисунок 752 - Окно аутентификации СГУ «Горизонт-ВС»

9 Первоначальные настройки в средстве виртуализации “Звезда”

После установки СВ “Звезда” необходимо:

- Сменить пароль от имени пользователя root;
- подключить дополнительное хранилище для резервных копий и снимков;
- создать пользователей системы в соответствии с ролевым доступом.

9.1 Смена пароля пользователя root

Для смены пароля:

- 1) Выполнить команду в консоли:
`passwd <имя_пользователя>`
- 2) Дважды корректно ввести новый пароль.
- 3) Перезапустить сервер виртуализации.

Парольная политика

Для настройки парольной политики необходимо выполнить следующее:

- 1) Открыть файл `passwdqc.conf` для редактирования:

```
sudo nano /etc/security/passwdqc.conf
```

Настройки по умолчанию включают в себя следующие параметры:

min=disabled,24,11,8,7

- Задаёт минимальные требования к длине пароля: - disabled – запрещает использование односимвольных паролей. - 24 – минимальная длина пароля для самого слабого пароля (который не соответствует никаким требованиям сложности). - 11 – минимальная длина для пароля, который соответствует минимальным требованиям сложности. - 8 – минимальная длина для более сложного пароля. - 7 – минимальная длина для самого сложного пароля.

max=72

- Ограничивает максимальную длину пароля до 72 символов.

passphrase=3

- Требуется минимум 3 уникальных символа в пароле.

match=4

- Проверяет наличие 4 совпадающих символов в строках с ранее использованными паролями. Если совпадение есть, пароль считается слабым.

similar=deny

- Запрещает использование паролей, которые похожи на текущее или предыдущее значение.

random=47

- Определяет минимальную длину для автоматически сгенерированных паролей. Это полезно, если используются случайные пароли.

enforce=none

- Не требует обязательного применения политики паролей ко всем пользователям.

retry=3

- Задаёт количество попыток ввода пароля при смене или установке нового.

2) Настроить параметры в файле:

min=disabled,8,8,8,8

passphrase=70

— min=disabled,8,8,8,8 – устанавливает минимальную длину пароля в 8 символов для разных категорий паролей (от простых до сложных). Значение disabled означает, что односимвольные пароли не принимаются.

— passphrase=70 – задаёт минимальное количество уникальных символов (алфавита) в пароле.

3) Сохранить изменения и закрыть файл.

4) Применить изменения. Перезагрузка сервера или перезапуск сервисов не требуется, так как настройки применяются при каждом изменении пароля.

Подключение хранилища для резервных копий и снимков

После “чистой” установки СВ “Звезда” рекомендуется подключить дополнительное хранилище для резервных копий и снимков. В роли такого хранилища может выступать любое отформатированное в поддерживаемой файловой системе блочное устройство. Список поддерживаемых файловых систем можно получить командой:

```
grep -v nodev /proc/filesystems
```

Хранилище для резервных копий и снимков определяется специальной точкой монтирования:

```
/var/backups
```

Для подключения блочного устройства необходимо выполнить следующие действия:

1) Отформатировать блочное устройство в поддерживаемой файловой системе:

```
mkfs.ext4 /dev/sdb
```

2) Добавить строку в /etc/fstab:

```
/dev/sdb /var/backups auto defaults 0 0
```

3) Выполнить команду:

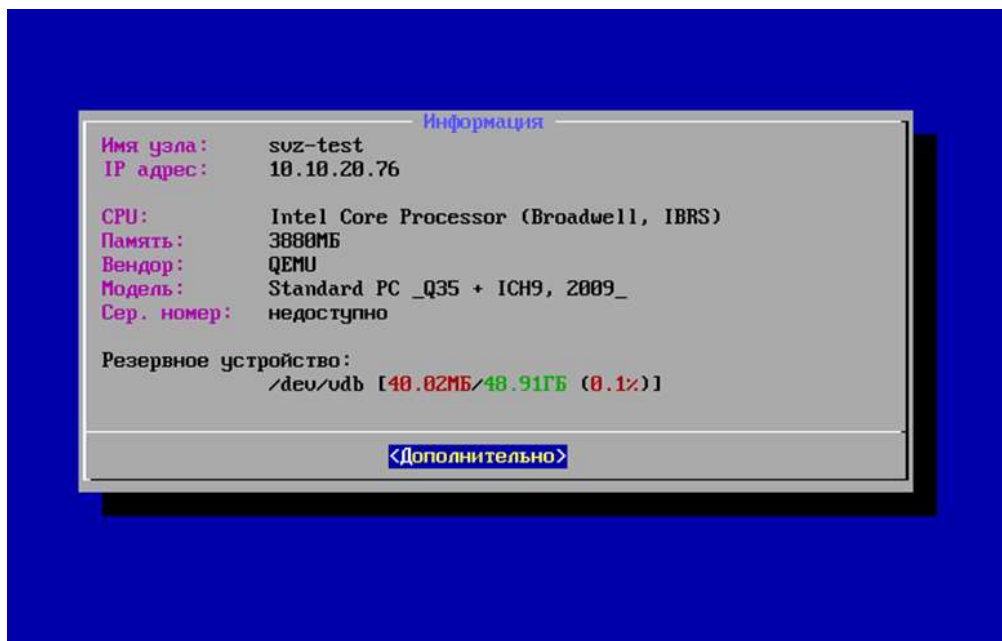
```
systemctl daemon-reload
```

4) Далее необходимо выполнить монтирование с созданием точки монтирования:

```
mount --mkdir /var/backups/
```

5) Перейти в консоль TUI, затем выбрать **Обслуживание**.

- 6) После подключения резервного копирования в TUI будет отображено следующее сообщение:



9.2 Обновление СВ "Звезда"

Необходимо выполнить пункты 1-4 установки СВ "Звезда". Если была обнаружена ранее установленная версия СВ "Звезда", то меню выбора целевого диска будет выглядеть следующим образом:

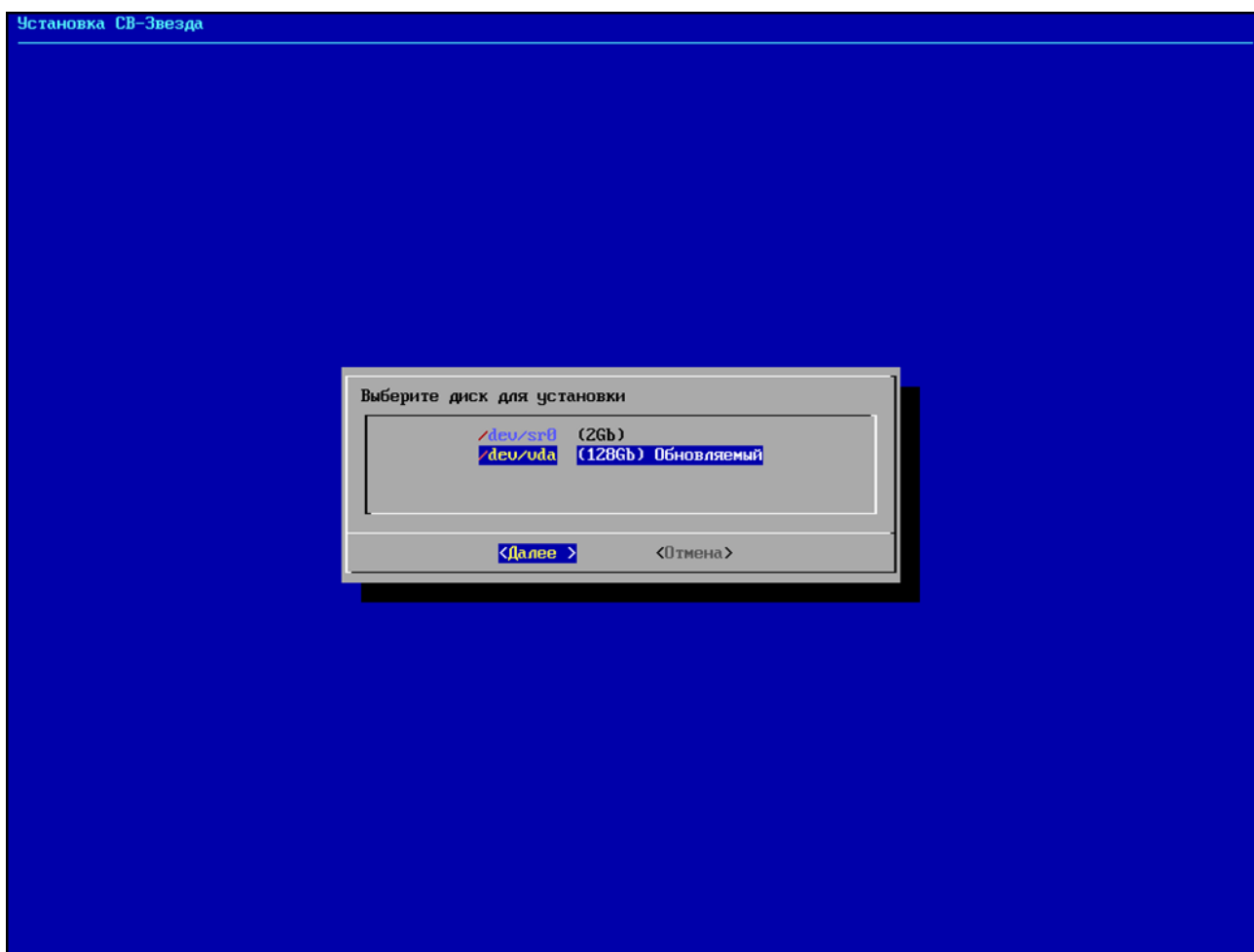


Рисунок 753 – Выбор диска

Отметка **Обновляемый** означает, что на данном целевом диске уже есть установленное средство виртуализации “Звезда”, ее можно обновить. После нажатия на данный диск будет доступен выбор:

- **Обновить**. Осуществляет безопасное обновление (с сохранением состояния системы);
- **Чистая установка**. Форматирует блочное устройство с установленным СВ “Звезда”, что приводит к полному удалению системы и произведенных изменений.

При выборе первого варианта система запросит подтверждения выполняемых действий.

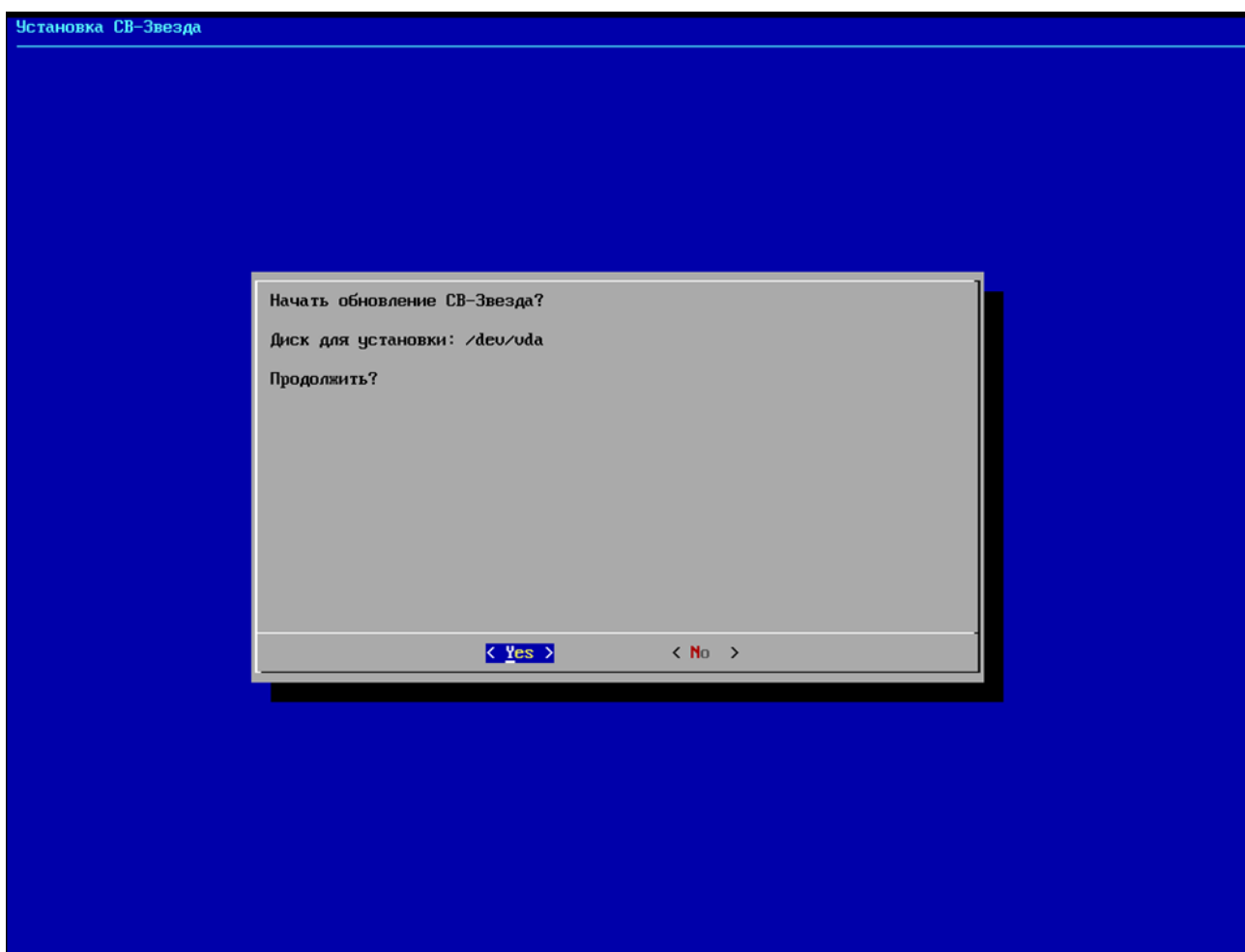


Рисунок 754 – Подтверждение обновления
Необходимо дождаться обновления системы.

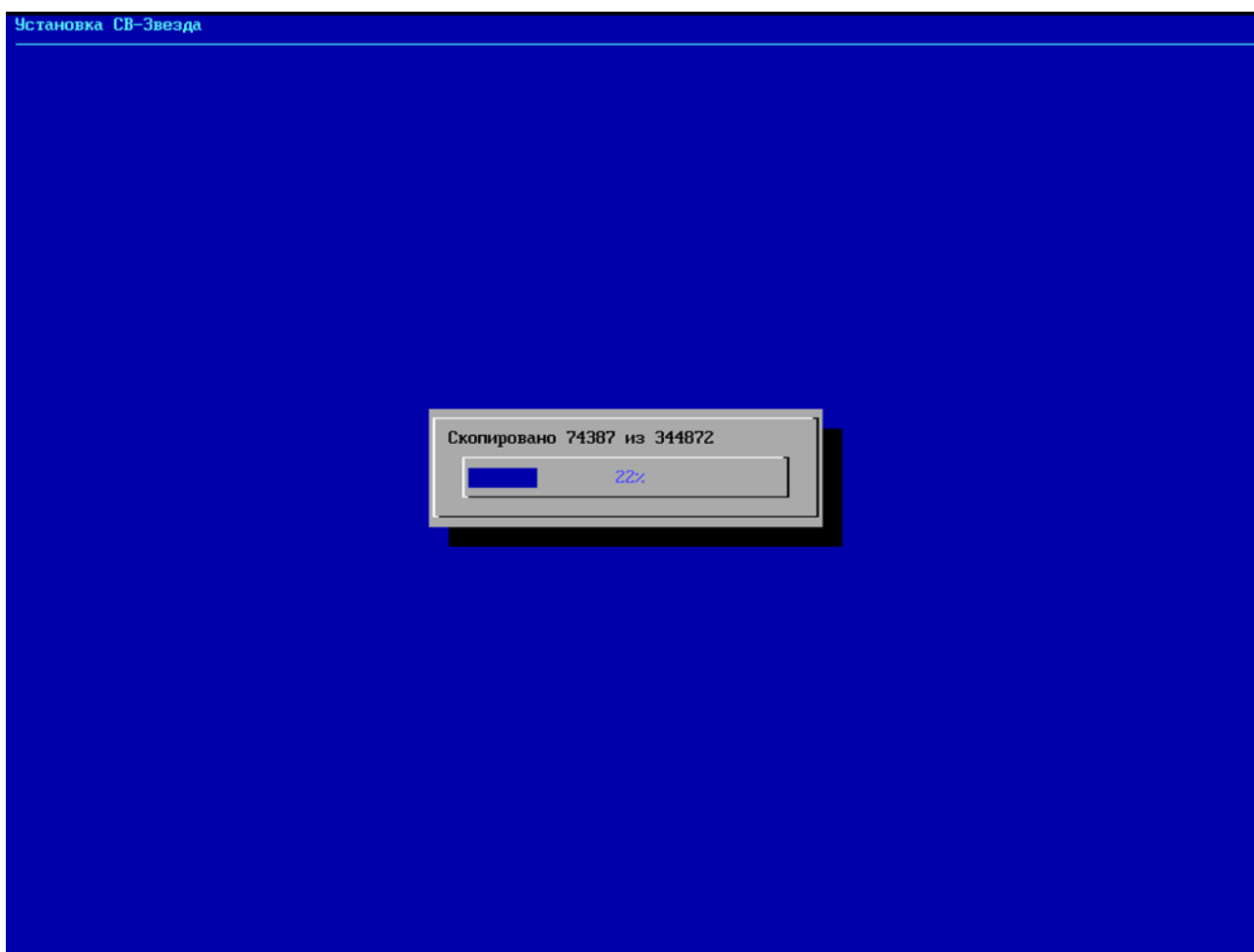


Рисунок 755 – Обновление системы

После окончания обновления, необходимо перезагрузить систему.

Откат к предыдущей версии

Для отката к предыдущей версии и состоянию до обновления необходимо войти в TUI СВ “Звезда”, после чего выбрать **Дополнительно > Обслуживание > Обновления**.

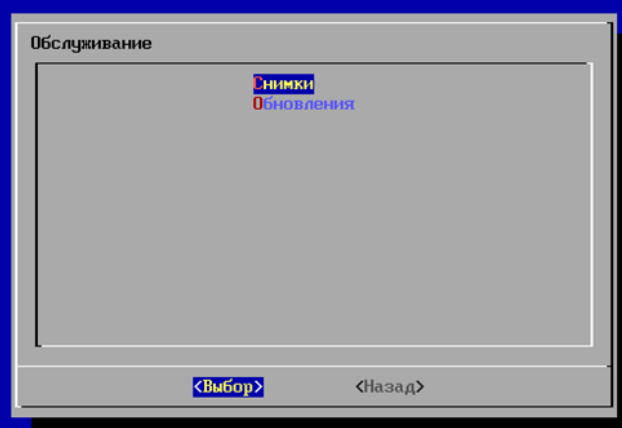


Рисунок 756 – Обслуживание

Выбрать версию, к которой нужно совершить откат.

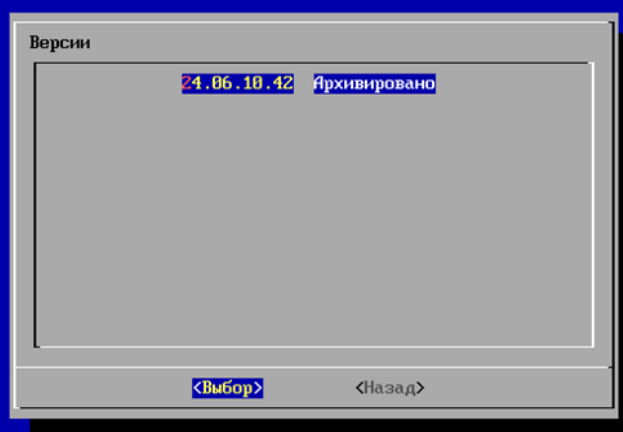


Рисунок 757 – Выбор версии

Для отката необходимо нажать **Выполнить откат версии**, для удаления версии - **Удалить версию**.

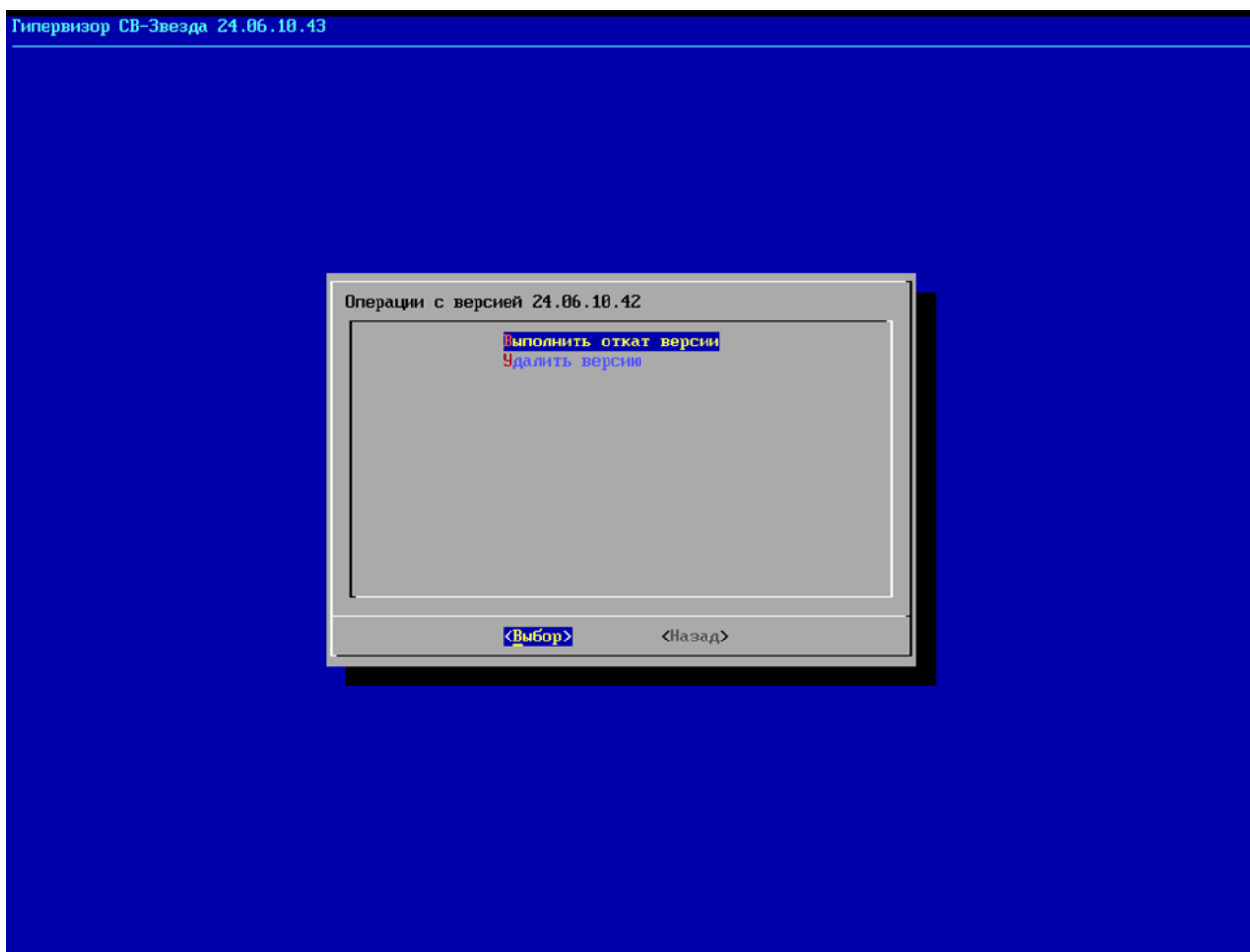


Рисунок 758 – Операции с версией

Изменение сетевых настроек

Для изменения IP-адреса необходимо выполнить следующие действия:

1) Открыть файл:

```
vim /etc/systemd/network/[наименование_интерфейса]
```

2) Отредактировать необходимые строчки. Пример содержания файла:

[Match]

Name=sys0

[Network]

Address=10.10.105.20/24

Gateway=10.10.105.1

DNS=10.10.105.1

3) Выполнить перезагрузку СВ “Звезда”.

9.3 Защита среды виртуализации

Контроль целостности

В СВ “Звезда” реализован механизм изоляции программной среды. Все исполняемые файлы подписываются, запуск измененных файлов невозможен. Система производит динамический контроль целостности, при обнаружении изменений в директории /usr производится автоматическое восстановление файлов к исходной версии, созданной при инсталляции системы.

Для вычисления контрольной суммы директории (или директорий) необходимо выполнить команду:

```
gostsum-dir <путь к директории>
```

Идентификация и аутентификация пользователей

Создание пользователей и паролей для них осуществляется администратором. Администратор уполномочен устанавливать уникальное имя и идентификатор для пользователя. При вводе неправильного логина или пароля, система отобразит информацию о том, что вход не выполнен, будет предложено ввести правильные значение повторно. Учетная запись пользователя автоматически блокируется при достижении заданного количества неудачных попыток аутентификации с возможностью разблокировки администратором средства виртуализации или с возможностью автоматической разблокировки по истечении временного интервала, устанавливаемого администратором средства виртуализации (настройки приведены в п. [4.3.1](#)). Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 4.

Аутентификация осуществляется с помощью локальной базы данных пользователей.

9.4 Создание и удаление пользователей

Запрещено создавать пользователей, не принадлежащих ни одной роли (п.4.3). 1. Для добавления пользователя необходимо войти в СВ “Звезда” с использованием прав администратора (root). 2. Ввести команду:

```
useradd [имя_пользователя]
```

Далее необходимо настроить пароль созданного пользователя, введя команду `passwd [имя_пользователя]`.

Запрещено устанавливать одинаковые идентификаторы и пароли для разных пользователей. Пароль пользователя средства виртуализации должен содержать не менее 8 символов:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры от 0 до 9;
- специальные символы, не принадлежащие алфавитно-цифровому набору (например, *_@);
- в пароле должны отсутствовать повторяющиеся символы;
- пароль не должен иметь смысловой нагрузки.
- Для создания пользователя с уникальным идентификационным номером (ID) необходимо выполнить команду:

```
useradd -u 1000 [имя_пользователя]
```

где 1000 - это ID, который необходимо добавить пользователю.

- Если необходимо добавить учетную запись с истекающим сроком действия, необходимо выполнить команду:

```
useradd -e 2020-05-30 [имя_пользователя]
```

- Для добавления пользователя с комментарием, необходимо выполнить следующую команду:

```
useradd -s "комментарий" [имя_пользователя]
```

- 3) Для удаления пользователя, необходимо ввести команду:

`userdel -r имя_пользователя`

удалить домашнюю директорию и все связанные с пользователем файлы:

`rm -rf /home/имя_пользователя`

`rm -f /var/spool/mail/имя_пользователя`

Проверить, удалены ли данные пользователя:

`cat /etc/passwd | grep имя_пользователя`

`ls /home | grep имя_пользователя`

Создание групп пользователей, добавление пользователя в группу

- 1) Для создания групп пользователей используется команда `groupadd [опции] [имя группы]`.

Доступные опции:

- `-f` - если группа уже существует, то утилита возвращает положительный результат операции;
- `-g` - установить значение идентификатора группы GID вручную;
- `-K` - изменить параметры по умолчанию автоматической генерации GID;
- `-o` - разрешить добавление группы с неunikальным GID;
- `-p` - задаёт пароль для группы;
- `-r` - указывает, что группа системная;
- `-R` - позволяет изменить корневой каталог

- 2) Для того чтобы добавить пользователя в группу, необходимо ввести команду `usermod` с ключами `-a` и `-G группа`.

`usermod -a -G groupname username.`

- 3) Для удаления пользователя из группы, необходимо ввести команду `gpasswd -d username groupname`.

9.5 Управление ролевым доступом

В издании поддерживаются следующие роли безопасности:

- разработчик виртуальной машины;
- администратор безопасности средства виртуализации;

- администратор средства виртуализации;
- администратор виртуальной машины;
- разработчик образов контейнеров;
- администратор безопасности средства контейнеризации;
- администратор информационной (автоматизированной) системы.

Порядок настройки ролей пользователей приведен в подразделах ниже.

Создание роли администратора средств виртуализации

Администратор безопасности средства виртуализации имеет права на следующие действия:

- создавать учетные записи пользователей средства виртуализации;
- управлять учетными записями пользователей средства виртуализации;
- назначать права доступа пользователям средства виртуализации к виртуальным машинам;
- создавать и удалять виртуальное оборудование средства виртуализации;
- изменять конфигурации виртуального оборудования средства виртуализации;
- управлять доступом виртуальных машин к физическому и виртуальному оборудованию;
- управлять квотами доступа виртуальных машин к физическому и виртуальному оборудованию;
- управлять перемещением виртуальных машин; Добавить команды миграции в конфиг файл для пользователя;
- удалять виртуальные машины;
- запускать и останавливать виртуальные машины;
- создавать снимки состояния виртуальных машин, включающих файл конфигурации виртуальной машины, образа виртуальной машины и образа памяти виртуальной машины.

Для создания роли администратора средства виртуализации необходимо выполнить следующие шаги:

1) Войти в СВ “Звезда” под учетной записью root.

2) Создать пользователя:

```
useradd adm_sv
```

3) Создать пароль для пользователя:

```
passwd
```

adm_sv

<ввести пароль для пользователя>

4) Открыть файл protector_rgate.conf:

```
nano /etc/protector_rgate.conf
```

5) Добавить строки:

```
adm_sv:useradd
```

*

```
adm_sv:userdel
```

*

```
adm_sv:scp
```

*

```
adm_sv:virsh
```

*

```
adm_sv:nano
```

```
/etc/protector_rgate.conf
```

```
adm_sv:virsh
```

```
destroy
```

*

```
adm_sv:virsh
```

```
undefine
```

*

```
adm_sv:virsh
```

```
edit
```

*

```
adm_sv:passwd *
```

6) Сохранить изменения и закрыть файл.

Создание роли разработчика ВМ

Разработчик виртуальной машины имеет права на следующие действия:

— создавать виртуальные машины;

— изменять конфигурации виртуальных машин.

Для создания роли разработчика виртуальной машины необходимо выполнить следующие шаги:

1) Войти в СВ “Звезда” под учетной записью администратора средства виртуализации.

2) Создать пользователя командой:

rgate useradd dev_vm

- 3) Создать пароль для пользователя. Необходимо, чтобы пароль содержал не менее 8 символов при алфавите пароля не менее 70 символов. Выполнить команду:

```
rgate                                passwd                                dev_vm
<ввести пароль для пользователя>
```

- 3) Открыть файл protector_rgate.conf:

```
rgate nano /etc/protector_rgate.conf
```

- 4) Добавить строки:

```
dev_vm:virsh                                create                                *
dev_vm:virsh                                define                                *
dev_vm:virsh                                undefine                               *
dev_vm:nano                                  *
dev_vm:qemu-img create *
```

- 5) Сохранить изменения и закрыть файл.

Создание роли администратора безопасности средства виртуализации

Администратор безопасности имеет права на следующие действия:

- иметь доступ на чтение к журналу событий безопасности средства виртуализации;
- формировать отчеты с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности средства виртуализации.

Для создания роли администратора безопасности необходимо выполнить следующие шаги:

- 1) Войти в СВ “Звезда” под учетной записью администратора средства виртуализации.

- 2) Создать пользователя командой:

```
rgate useradd adm_sec
```

3) Создать пароль для пользователя. Необходимо, чтобы пароль содержал не менее 8 символов при алфавите пароля не менее 70 символов. Выполнить команду:

```
rgate                                passwd                                adm_sec
<ввести пароль для пользователя>
```

3) Открыть файл protector_rgate.conf:

```
rgate nano /etc/protector_rgate.conf
```

4) Добавить строки:

```
sec_adm:aureport
sec_adm:cat                                /var/log/protector/protector.log
sec_adm:cat                                /var/log/audit/audit.log
sec_adm:cat                                /var/log/protector/rgate.log
sec_adm:tail                                -f                                /var/log/protector/protector.log
sec_adm:tail                                -f                                /var/log/protector/rgate.log
sec_adm:journalctl                                *
sec_adm:journalctl
sec_adm:cat                                /var/log/auth.log
sec_adm:cat /var/log/boot.log
```

5) Сохранить изменения и закрыть файл.

Создание роли администратора виртуальной машины

Роль администратора виртуальной машины позволяет осуществлять доступ к виртуальной машине. Администратор виртуальной машины является единственным пользователем, который имеет доступ к подключению ВМ по протоколу spice. Любая передача сведений о способах подключения к ВМ сторонним лицам запрещена.

Создание виртуальной машины описано в разделе [6.1](#).

Для создания роли администратора виртуальной машины необходимо выполнить следующие действия:

1) Войти в СВ “Звезда” под учетной записью администратора средства виртуализации.

2) Создать пользователя командой:

```
rgate useradd adm_vm
```

3) Создать пароль для пользователя. Необходимо, чтобы пароль содержал не менее 8 символов при алфавите пароля не менее 70 символов. Выполнить команду:

```
rgate                                passwd                                adm_vm
```

<ввести пароль для пользователя>

3) Предоставить администратору виртуальной машины необходимой информацией о ВМ для обеспечения административных функций (IP-адрес, порт, способ подключения, созданная учетная запись для администратора внутри ВМ).

Создание роли разработчика образов контейнеров

Разработчик образов контейнеров имеет права на следующие действия:

- менять установленный администратором безопасности средства контейнеризации для разработчика пароль;
- создавать, модифицировать и удалять образы контейнеров.

Для создания роли администратора безопасности необходимо выполнить следующие шаги:

1) Войти в СВ “Звезда” под учетной записью администратора средства виртуализации.

2) Создать пользователя командой:

```
rgate useradd dev_img_docker
```

3) Создать пароль для пользователя. Необходимо, чтобы пароль содержал не менее 8 символов при алфавите пароля не менее 70 символов. Выполнить команду:

rgate passwd dev_img_docker

<ввести пароль для пользователя>

3) Открыть файл protector_rgate.conf:

```
rgate nano /etc/protector rgate.conf
```

4) Добавить строки:

dev_img_docker:passwd dev_img_docker

```
dev img docker:docker import *
```

dev img docker:nano Dockerfile

dev img docker:docker rmi *

```
dev img docker:docker rm *
```

dev img docker:docker images

dev img docker:docker image *

```
dev img docker:apply-ima
```

dev img docker:docker build *

```
dev img docker:docker update *
```

5) Сохранить изменения и закрыть файл.

Создание роли администратора информационной системы

Роль администратора информационной (автоматизированной) системы позволяет:

- менять установленный администратором безопасности средства контейнеризации для администратора информационной (автоматизированной) системы пароль;

- запускать и останавливать контейнеры.

Для создания роли администратора безопасности необходимо выполнить следующие шаги:

- 1) Войти в СВ “Звезда” под учетной записью администратора средства виртуализации.

2) Создать пользователя командой:

```
rqgate useradd adm ias
```

- 3) Создать пароль для пользователя. Необходимо, чтобы пароль содержал не менее 8 символов при алфавите пароля не менее 70 символов. Выполнить команду:

```
rgate                                passwd                                adm_ias  
<ввести пароль для пользователя>
```

- 3) Открыть файл protector_rgate.conf:

```
rgate nano /etc/protector_rgate.conf
```

- 4) Добавить строки:

```
adm_ias:passwd                                adm_ias  
adm_ias:docker                                run  
adm_ias:docker stop *
```

- 5) Сохранить изменения и закрыть файл.

Создание роли администратора безопасности средства контейнеризации

Роль администратора безопасности средства контейнеризации позволяет:

- назначать права доступа пользователям средства контейнеризации к образам контейнеров;
- создавать учетные записи пользователей средства контейнеризации;
- управлять учетными записями пользователей средства контейнеризации;
- иметь доступ на чтение к журналу событий безопасности средства контейнеризации (rgate journalctl –no-pager | awk ‘/container/’);
- формировать отчеты с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности средства контейнеризации.

Для создания роли администратора безопасности средства контейнеризации необходимо выполнить следующие шаги:

- 1) Войти в СВ “Звезда” под учетной записью администратора средства виртуализации.

- 2) Создать пользователя командой:

```
rgate useradd adm_sec_docker
```


3) Создать пароль для пользователя. Необходимо, чтобы пароль содержал не менее 8 символов при алфавите пароля не менее 70 символов. Выполнить команду:

```
rgate                                passwd                                adm_sec_docker
<ввести пароль для пользователя>
```

3) Открыть файл protector_rgate.conf:

```
rgate nano /etc/protector_rgate.conf
```

4) Добавить строки:

```
adm_sec_docker:docker                                logs                                *
adm_sec_docker:journalctl                            *
adm_sec_docker:useradd                                *
adm_sec_docker:passwd                                *
adm_sec_docker:nano                                    /etc/protector_rgate.conf
adm_sec_docker:docker                                    events
adm_sec_docker:cat                                    /var/log/protector/protector.log
adm_sec_docker:cat                                    /var/log/protector/rgate.log      *
adm_sec_docker:docker                                    inspect                            *
adm_sec_docker:cat /var/log/protector/rgate.log
```

5) Сохранить изменения и закрыть файл.

Журналирование фактов изменения ролевой модели

Факты изменения ролевой модели пользователя фиксируются в файле protector.log. Для просмотра журнала, администратор безопасности средства виртуализации должен ввести следующую команду:

```
rgate cat /var/log/protector/protector.log
```

Администратору доступна информация о пользователе, который изменил ролевую модель, время, дата, какие именно изменения были внесены.

Журналирование фактов создания, модификации и удаления образов контейнеров

Для просмотра фактов создания, модификации и удаления образов контейнеров, администратору информационной системы необходимо выполнить следующие действия:

```
rgate cat /var/log/protector/rgate.log
```

В журнале будут доступны записи о фактах создания, модификации и удаления образов контейнеров.

Журналирование неуспешных попыток аутентификации пользователей средства контейнеризации

Для просмотра фактов неуспешных попыток аутентификации пользователей средства контейнеризации, администратору информационной системы необходимо выполнить следующие действия:

```
rgate cat /var/log/protector/rgate.log
```

В журнале будут доступны записи о фактах неуспешных попыток аутентификации пользователей средства контейнеризации.

Журналирование запуска и остановки контейнеров

Для просмотра фактов запусков и остановок контейнеров, администратору информационной системы необходимо выполнить следующие действия:

```
rgate cat /var/log/protector/rgate.log
```

В журнале будут доступны записи о фактах запусков и остановок контейнеров.

Журналирование модификаций запускаемых контейнеров

Для просмотра фактов модификаций запускаемых контейнеров, администратору информационной системы необходимо выполнить следующие действия:

```
rgate cat /var/log/protector/rgate.log
```

В журнале будут доступны записи о фактах модификаций запускаемых контейнеров.

Журналирование успешных и неуспешных попыток аутентификации

Для просмотра журнала успешных и неуспешных попыток аутентификации необходимо ввести команду:

```
rgate cat /var/log/auth.log
```

Администратору безопасности будет доступна информация о всех успешных и неуспешных попыток аутентификации.

Журналирование доступа пользователей средства виртуализации к виртуальным машинам

Просмотр журнала доступа пользователей к ВМ осуществляется с помощью команды:

```
rgate cat /var/log/libvirt/qemu/<имя_ВМ>.log
```

Журналирование создания и удаления виртуальных машин

Для просмотра журнала создания и удаления ВМ, администратору безопасности необходимо выполнить команду:

```
rgate cat /var/log/protector/rgate.log
```

Администратору будет доступна информация о том, какой пользователь выполнял команду создания и удаления ВМ.

Журналирование запуска и остановки средства виртуализации

Для просмотра журнала запуска и остановки средства виртуализации, администратору безопасности необходимо выполнить команду:

```
rgate cat /var/log/boot.log
```

Администратору будет доступна информация о запуске и остановке средства виртуализации.

Журналирование запуска и остановки ВМ

Для просмотра журнала запуска и остановки ВМ, администратору безопасности необходимо выполнить команду:

```
rgate cat /var/log/protector/rgate.log
```

Администратору будет доступна информация о том, какой пользователь выполнял команду запуска и остановки ВМ.

Журналирование изменения конфигурации средства виртуализации

Для просмотра журнала изменения конфигурации средства виртуализации выполнить команду:

```
rgate journalctl -k | grep -E 'sd[a-z]|block|disk'
```

Для дополнительной информации выполнить команду:

```
rgate journalctl -k -f
```

Журналирование изменения конфигурации ВМ

Для просмотра изменений конфигурации ВМ администратор безопасности должен ввести команду:

```
rgate cat /var/log/protector/protector.log
```

Администратору доступна информация о пользователе, который изменил конфигурацию ВМ, время, дата, какие именно изменения были внесены.

Журналирование фактов нарушения целостности объектов контроля

Для просмотра фактов нарушения целостности объектов контроля администратор безопасности должен ввести команду:

```
rgate cat /var/log/protector/protector.log
```

Администратору доступна информация о том, какие именно изменения были внесены.

Журналирование доступа к образам контейнеров

Для просмотра журнала доступа к образам контейнеров, администратору безопасности необходимо выполнить команду:

```
rgate cat /var/log/protector/rgate.log
```

Администратору будет доступна информация о доступе к образам контейнеров.

Управление потоками информации

Средство виртуализации “Звезда” поддерживает управление потоками информации с помощью технологии локальных сетей (VLAN). Используются следующие механизмы:

- 1) Изоляция трафика виртуальной машин.
- 2) Маскировка исходящего трафика ВМ во внешнюю сеть.
- 3) Маршрутизация сети.

Изоляция сетей осуществляется с помощью многоуровневого коммутатора Open vSwitch, который позволяет фильтровать трафик сети. Для настройки изолированной сети необходимо настроить bridge с помощью консоли управления. СВ “Звезда” поддерживает инструменты iptables для настройки и управления правилами фильтрации пакетов. Основные параметры и команды для настройки правил фильтрации:

1) **Просмотр текущих правил:**

```
iptables -L
```

2) **Добавление правила для блокировки входящих пакетов от определенного IP-адреса:**

```
iptables -A INPUT -s 192.168.1.100 -j DROP
```

3) **Разрешение входящих SSH соединений:**

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

4) **Удаление правила:**

```
iptables -D INPUT -s 192.168.1.100 -j DROP
```

- iptables-save: Сохраняет текущие правила в файл.
- iptables-restore: Восстанавливает правила из файла.
- iptables -F: Очищает все правила в таблице.

Регистрация событий безопасности

Использование auditd

В СВ “Звезда” реализована регистрация событий безопасности. В качестве инструмента используется auditd (Linux Audit Daemon).

Для настройки параметров auditd необходимо выполнить следующие действия:

1) **Перейти к файлу конфигурации:**

```
cd /etc/audit/auditd.conf
```

Файл конфигурации будет иметь следующий вид:

local_events	=	yes
write_logs	=	yes

log_file	=	/var/log/audit/audit.log
log_group	=	root
log_format	=	ENRICHED
flush	=	INCREMENTAL_ASYNC
freq	=	50
max_log_file	=	8
num_logs	=	5
priority_boost	=	4
name_format	=	NONE
##name	=	mydomain
max_log_file_action	=	ROTATE
space_left	=	75
space_left_action	=	SYSLOG
verify_email	=	yes
action_mail_acct	=	root
admin_space_left	=	50
admin_space_left_action	=	SUSPEND
disk_full_action	=	SUSPEND
disk_error_action	=	SUSPEND
use_libwrap	=	yes
##tcp_listen_port	=	60
tcp_listen_queue	=	5
tcp_max_per_addr	=	1
##tcp_client_ports	=	1024-65535
tcp_client_max_idle	=	0
transport	=	TCP
krb5_principal	=	auditd
##krb5_key_file	=	/etc/audit/audit.key

```

distribute_network                =                no
q_depth                          =                2000
overflow_action                   =                SYSLOG
max_restarts                     =                10
plugin_dir                       =                /etc/audit/plugins.d
end_of_event_timeout = 2

```

В таблице представлены события аудита безопасности.

Таблица 4.1 – События аудита безопасности

№	Тип сообщения	Описание
1	USER_LOGIN	Запись о входе пользователя в систему
2	USER_LOGOUT	Запись о выходе пользователя из системы
3	LOGIN	Запись о попытке входа пользователя
4	SERVICE_START	Запись о запуске службы
5	SERVICE_STOP	Запись о остановке службы
6	SYSCALL	Запись о вызове системной функции
7	PROCTITLE	Запись о заголовке процесса, содержащая информацию о процессе
8	USER_MODIFY	Запись об изменении информации о пользователе (например, изменение пароля)
9	USER_CREATE	Запись о создании нового пользователя
10	USER_DELETE	Запись о удалении пользователя
11	FILE_ACCESS	Запись о доступе к файлу (чтение или запись)
12	FILE_MODIFY	Запись о модификации файла
13	FILE_CREATE	Запись о создании файла

14	FILE_DELETE	Запись о удалении файла
15	CONFIG_CHANGE	Запись об изменениях в конфигурации системы
16	LOGIN_FAILURE	Запись о неудачной попытке входа
17	NETWORK_ACCESS	Запись о доступе к сети (например, попытка подключения к удаленному хосту)
18	DEVICE_ACCESS	Запись о доступе к устройствам системы
19	MODULE_LOAD	Запись о загрузке модуля ядра
20	MODULE_UNLOAD	Запись об выгрузке модуля ядра
21	SETUID_EXEC	Запись о выполнении программы с установленным битом setuid
22	SETGID_EXEC	Запись о выполнении программы с установленным битом setgid
23	FILE_RENAME	Запись о переименовании файла
24	FILE_RESTORE	Запись о восстановлении файла
25	CAPABILITY_CHANGE	Запись об изменении привилегий (capabilities) процесса
26	SYSTEM_BOOT	Запись о загрузке системы
27	SYSTEM_SHUTDOWN	Запись о завершении работы системы

log_file

Для изменения каталога хранения файлов журнала аудита, необходимо изменить строку `log_file = /var/log/audit/audit.log`.

max_log_file

Параметр **max_log_file** указывает максимальный размер одного файла журнала аудита, который должен быть установлен для полного использования доступного

пространства на разделе, где хранятся файлы журнала аудита. Данный параметр определяет максимальный размер файла в мегабайтах. Указанное значение должно быть числовым.

max_log_file_action

Параметр **max_log_file_action** определяет, какое действие будет выполнено после достижения установленного предела в параметре **max_log_file**; его следует установить на **keep_logs**, чтобы предотвратить перезапись файлов журнала аудита.

space_left

Данный параметр определяет объем свободного места на диске. При достижении лимита объема диска срабатывает действие, установленное в параметре **space_left_action**. Необходимо указать число, которое дает администратору время для освобождения дискового пространства. Значение **space_left** зависит от темпа генерации файлов аудита. Если значение **space_left** указано как целое число, оно интерпретируется как абсолютный размер в мегабайтах (MiB). Если значение указано как число от 1 до 99, за которым следует знак процента (например, 5%), демон аудита вычисляет абсолютный размер в мегабайтах на основе размера файловой системы, содержащей файл журнала.

space_left_action

Рекомендуется установить параметр **space_left_action** на значение **email** или **exec** с соответствующим методом уведомления.

admin_space_left

Данный параметр определяет абсолютное минимальное количество свободного места, при достижении которого срабатывает действие, установленное в параметре **admin_space_left_action**. Это значение должно быть установлено так, чтобы осталось достаточно места для регистрации действий, выполняемых администратором. Числовое значение для этого параметра должно быть меньше значения параметра **space_left**. Вы также можете добавить знак процента

(например, 1%) к числу, чтобы демон аудита вычислил число на основе размера раздела диска.

admin_space_left_action

Должен быть установлен в значение single, чтобы перевести систему в однопользовательский режим и позволить администратору освободить диск.

disk_full_action

Параметр определяет действие, которое срабатывает, когда на разделе, где хранятся файлы журнала аудита, нет свободного места. Должен быть установлен в значение halt или single. Это обеспечивает остановку системы или переход в однопользовательский режим, когда аудит больше не может регистрировать события.

disk_error_action

Параметр определяет действие, которое срабатывает в случае обнаружения ошибки на разделе, где хранятся файлы журнала аудита. Должен быть установлен в значение syslog, single или halt в зависимости от местных политик безопасности относительно обработки неисправностей оборудования.

flush

Параметр должен быть установлен в значение incremental_async. Он работает в сочетании с параметром freq, который определяет, сколько записей может быть отправлено на диск перед принудительной синхронизацией с жестким диском. Параметр freq должен быть установлен на 100. Эти параметры гарантируют, что данные событий аудита синхронизируются с файлами журнала на диске, сохраняя при этом хорошую производительность для всплесков активности.

Запуск сервиса auditd

После конфигурации файла необходимо запустить сервис. Для запуска сервиса auditd необходимо ввести команду:

```
systemctl start auditd.service
```

Статус сервиса можно проверить, введя команду:

```
systemctl status auditd.service
```

Убедиться, что сервис работает исправно, перейдя к log-файлам. Каталог хранения файлов журнала аудита указан в конфигурационном файле `log_file = /var/log/audit/audit.log`:

```
vim /var/log/audit/audit.log
```

Убедившись, что логи записываются, выйти из файла.

Команды управления сервисом `auditd`:

Важно! Необходимо просмотреть файл `/usr/lib/systemd/system/auditd.service` и убедиться, что параметр `RefuseManualStop` имеет значение `no`. После изменения параметра необходимо перезапустить демон командой `systemctl daemon-reload`.

— Для остановки сервиса:

```
systemctl stop auditd.service
```

— Для перезапуска сервиса:

```
systemctl restart auditd.service
```

— Для перезагрузки и принудительной перезагрузки конфигурационного файла:

```
systemctl reload auditd.service и systemctl force-reload auditd.service
```

Формирование отчетов

Для формирования отчета на основе журнала аудита (`audit.log`) используется утилита **aureport**. Она входит в состав пакета **auditd**, который отвечает за ведение журнала аудита безопасности системы.

В СВ “Звезда” реализован контроль доступа к файлу `audit.log`. Попытки доступа и формирования отчета заносятся в файле `protector.log`.

Примеры команд для формирования отчетов из `audit.log`:

1) Общий отчет по событиям аудита:

```
aureport
```

2) Отчет по событиям, связанным с пользователями:

```
aureport --user
```

3) Отчет по событиям входа в систему:

aureport --login

4) Отчет по событиям файловой системы:

aureport --file

5) Отчет по командам, выполненным пользователями:

aureport --command

6) Отчет по результатам попыток аутентификации:

aureport --auth

7) Отчет по сетевым событиям:

aureport --network

8) Формирование отчета в определенный период (например, за последние 24 часа):

aureport --start today --end now

9) Формирование отчета по конкретному типу события (например, события создания файлов):

aureport --summary --type file

Дополнительные опции: - Можно сохранить отчет в файл, используя перенаправление вывода:

aureport --user > user_report.txt

Утилита **aureport** помогает агрегировать данные из журнала audit.log и выводить их в читаемом формате для анализа.

Использование Logrotate

Утилита Logrotate позволяет управлять журналами автоматизированно. Таким образом, можно задать необходимые условия и правила для выполнения действий, связанных с журналом. Например, доступна архивация журналов или передача их на другой сервер при достижении определенного размера, возраста или других критериев. Проверка условий может быть настроена для выполнения ежедневно, еженедельно или ежемесячно.

Настройка logrotate

Для настройки logrotate необходимо перейти в конфигурационный файл logrotate.conf: vim /etc/logrotate.conf. Пример открытого файла конфигурации:

```
# Default logrotate(8) configuration file for Gentoo Linux.
# See "man logrotate" for details.

# rotate log files weekly.
weekly
#daily

# keep 4 weeks worth of backlogs.
rotate 4

# create new (empty) log files after rotating old ones.
create

# use date as a suffix of the rotated file.
dateext

# compress rotated log files.
compress

notifempty
nomail
noolddir

# packages can drop log rotation information into this directory.
include /etc/logrotate.d
```

```
# no packages own wtmp and btmp -- we'll rotate them here.
/var/log/wtmp {
    monthly
    create          0664          root          utmp
    minsize         1M
    rotate          1
}
/var/log/btmp {
    missingok
    monthly
    create          0600          root          utmp
    rotate          1
}
```

system-specific logs may also be configured here.

Переменные, с помощью которых осуществляется управление логами:

1) Периодичность выполнения проверок совпадения условий:

- hourly - каждый час;
- daily - каждый день;
- weekly - каждую неделю;
- monthly - каждый месяц;
- yearly - каждый год.

2) Основные инструменты:

- rotate - указывает сколько старых логов нужно хранить, в параметрах передается количество;
- create - указывает, что необходимо создать пустой лог файл после перемещения старого;
- dateext - добавляет дату ротации перед заголовком старого лога;

- compress - указывает, что лог необходимо сжимать;
- delaycompress - не сжимать последний и предпоследний журнал;
- extension - сохранять оригинальный лог файл после ротации, если у него указанное расширение;
- mail - отправлять Email после завершения ротации;
- maxage - выполнять ротацию журналов, если они старше, чем указано;
- missingok - не выдавать ошибки, если лог файла не существует;
- olddir - перемещать старые логи в отдельную папку;
- postrotate/endscript - выполнить произвольные команды после ротации;
- start - номер, с которого будет начата нумерация старых логов;
- size - размер лога, когда он будет перемещен.

Каждый лог, который подлежит ротации, описывается следующим образом:

```
адрес_файла_лога                                     {
директивы
}
```

Настройки для ротации лога

Для примера будет использован файл rsyslog.conf, который был создан в папке /etc/logrotate.d/. Важно создать файл messages в директории log. Далее необходимо поместить в данный файл настройки ротации данного лога:

```
/var/log/messages                                     {
daily
rotate                                                3
size                                                  10M
compress
delaycompress
}
```

Данные настройки отображают следующее:

- daily - ротация журналов будет производиться ежедневно;

- rotate 3 - будут храниться три последних журнала, более старые копии будут удалены;
- size 10M минимальный размер для ротации - 10 мегабайт, ротация не будет выполнена;
- compress - будет использовано сжатие;
- delaycompress - сжатие будет использовано для всех журналов, кроме последнего и предпоследнего.

По такому принципу возможно настроить ротацию логов для любого из журналов.

Для проверки необходимо ввести следующую команду:

```
logrotate -d /etc/logrotate.d/rsyslog.conf
```

В выводе команды должен быть отображен файл лога.

Работа с журналом journald

Настройка journald включает редактирование конфигурационных файлов, чтобы изменить параметры ведения журналов. Основным конфигурационным файлом для journald является /etc/systemd/journal.conf. Основные шаги и параметры для настройки journald:

1) Открыть файл конфигурации:

```
nano /etc/systemd/journal.conf
```

2) Основные параметры конфигурации:

- Storage – определяет, где хранятся журналы. Возможные значения:
 - volatile – журналы хранятся в оперативной памяти и исчезают при перезагрузке.
 - persistent – журналы сохраняются на диске и сохраняются между перезагрузками.
 - auto – по умолчанию. Если директория /var/log/journal/ существует, журналы хранятся на диске, иначе – в оперативной памяти.
 - none – отключает ведение журналов.

Storage=persistent

- `Compress` – указывает, должны ли сжиматься журналы. Значение `yes` включает сжатие, `no` – отключает.

`Compress=yes`

- `RateLimitInterval` и `RateLimitBurst` – параметры, контролирующие ограничение скорости записи сообщений. Например, следующие настройки ограничивают до 200 сообщений каждые 10 секунд:

`RateLimitInterval=10s`

`RateLimitBurst=200`

- `SystemMaxUse` – максимальное пространство на диске, которое может использовать `journal` для хранения журналов.

`SystemMaxUse=500M`

- `MaxFileSec` – максимальное время хранения файлов журналов. Например, чтобы хранить журналы не более 1 месяца:

`MaxFileSec=1month`

- `ForwardToSyslog` – отправлять ли журналы в `syslog`. Значение `yes` включает пересылку, `no` – отключает.

`ForwardToSyslog=yes`

3) **Применение изменений:**

После внесения изменений необходимо перезапустить службу `systemd-journal`:

`systemctl restart systemd-journal`

4) **Дополнительные параметры:**

Полный список параметров можно найти в руководстве по конфигурации `journal`:

`man journal.conf`

Включение ротации в journal

В `systemd-journal` ротация журналов осуществляется автоматически в зависимости от параметров конфигурации. Однако, возможна настройка параметров, которые контролируют ротацию и очистку старых журналов. Важно правильно установить такие параметры, как максимальный размер использования дискового

пространства, максимальный размер отдельных файлов журналов и максимальное время их хранения. Для этого:

1) **Открыть конфигурационный файл:**

```
nano /etc/systemd/journald.conf
```

2) **Настроить параметры ротации и хранения:**

В файле `/etc/systemd/journald.conf` вы можно настроить следующие параметры:

- `SystemMaxUse` – максимальное пространство на диске, которое может использовать `journald` для хранения журналов. Например, чтобы ограничить до 500 MB:

```
SystemMaxUse=500M
```

- `SystemKeepFree` – минимальное свободное пространство на диске, которое должно быть оставлено. Это полезно для предотвращения заполнения диска журналами. Например, чтобы оставлять минимум 100 MB свободного пространства:

```
SystemKeepFree=100M
```

- `SystemMaxFileSize` – максимальный размер одного файла журнала. Например, чтобы ограничить до 50 MB на файл:

```
SystemMaxFileSize=50M
```

- `MaxFileSec` – максимальное время хранения файлов журналов. Например, чтобы хранить журналы не более 1 месяца:

```
MaxFileSec=1month
```

- `SystemMaxFiles` – максимальное количество файлов журналов. Например, чтобы ограничить до 100 файлов:

```
SystemMaxFiles=100
```

3) **Сохранить файл и закрыть редактор.**

4) **Перезапустить службу `systemd-journald` для применения изменений:**

```
systemctl restart systemd-journald
```

Эти параметры будут автоматически регулировать ротацию и удаление старых журналов, основываясь на данных настройках. `journalld` автоматически начнет удалять старые файлы журналов, когда суммарный объем будет превышать указанные лимиты или файлы станут старше указанного времени.

Для получения дополнительной информации о параметрах конфигурации `journalld`, можно использовать команду:

```
man journald.conf
```

Это откроет руководство, где подробно описаны все доступные параметры и их использование.

Система мониторинга системного журнала `journald-monitor`

Общие сведения

Название: `journald-monitor`

Назначение: мониторинг системного журнала (`journald`) для обнаружения ошибок и отправки уведомлений администратору.

Зависимости:

- Утилита `journalctl` для чтения системного журнала.
- Утилита `mail` для отправки электронной почты.
- Файл конфигурации `/etc/sysconfig/journald-monitor`.

Основные функции

- 1) Автоматический мониторинг системного журнала на наличие ошибок.
- 2) Хранение текущего состояния курсора журнала в файле `/var/tmp/journal_cursor`.
- 3) Отправка уведомлений с ошибками по электронной почте.
- 4) Поддержка настройки через файл конфигурации.

Настройка `ssmtp`

Используется лёгкий почтовый сервер `ssmtp` для отправки писем через SMTP.

Конфигурация ssmtp

Основной файл конфигурации: /etc/ssmtp/ssmtp.conf.

Открыть файл для редактирования:

```
sudo nano /etc/ssmtp/ssmtp.conf
```

Настроить файл для работы с SMTP-сервером:

```
hostname=localhost
```

```
FromLineOverride=YES
```

```
AuthUser=example@yandex.ru
```

```
AuthPass=example-pass
```

```
mailhub=smtp.yandex.ru:587
```

```
rewriteDomain=yandex.ru
```

```
UseTLS=YES
```

```
UseSTARTTLS=YES
```

Установка прав доступа к конфигурации

Установить права доступа:

```
sudo chmod 600 /etc/ssmtp/ssmtp.conf
```

Настройка файла aliases

Создать или отредактировать файл /etc/ssmtp/revalias:

```
sudo nano /etc/ssmtp/revalias
```

Добавить запись:

```
root:example@yandex.ru:smtp.yandex.ru:587
```

Тестирование отправки писем

Проверить работоспособность:

```
echo "Тестовое сообщение" | mail -s "Тестовая тема" -r example@yandex.ru  
example@yandex.ru
```

Настройка journald-monitor

Убедиться, что параметр MAIL_FROM в /etc/sysconfig/journald-monitor соответствует настройкам ssmtp. Пример:

MAIL_FROM=example@yandex.ru

Файл конфигурации *journald-monitor*

Создать или отредактировать файл /etc/sysconfig/journald-monitor:

Email администратора для получения уведомлений

ADMIN_EMAIL=admin@domain.com

Email отправителя

MAIL_FROM=example@yandex.ru

Интервал мониторинга (в секундах)

INTERVAL=10

Настройка *systemd*

Активировать сервис:

systemctl enable journald-monitor.service

systemctl start journald-monitor.service

Управление сервисом

Запустить сервис:

systemctl start journald-monitor

Остановить сервис:

systemctl stop journald-monitor

Проверить статус:

systemctl status journald-monitor

Просмотр логов

Получить логи работы:

journalctl -u journald-monitor.service

Принцип работы

- 1) Загрузка конфигурации из файла /etc/sysconfig/journald-monitor.
- 2) Проверка состояния курсора в файле /var/tmp/journal_cursor.

- 3) Получение новых ошибок через journalctl.
- 4) Отправка уведомлений с ошибками по электронной почте.
- 5) Обновление состояния курсора.

Решение проблем

Отсутствие файла конфигурации: необходимо проверить наличие файла /etc/sysconfig/journald-monitor и корректность его параметров.

Не отправляются уведомления: необходимо убедиться в установке и настройке утилиты mail.

Сервис не запускается: проверить логи:

```
journalctl -u journald-monitor.service
```

Резервное копирование журналов

Возможность резервного копирования журналов systemd-journald реализуется путем копирования файлов журналов в безопасное место. Файлы журналов хранятся в формате бинарных файлов и обычно находятся в следующих директориях:

- /var/log/journal/ (если настроено хранение журналов на диске)
- /run/log/journal/ (если журналы хранятся в оперативной памяти и исчезают при перезагрузке)

Для настройки резервного копирования журналов используется overlayfs, которая создает резервную копию всей файловой системы.

Настройка поля вывода

В systemd-journald можно настроить вывод определенных полей, используя утилиту journalctl. Это особенно полезно, когда нужно фильтровать или форматировать журналы для более удобного анализа. Для этого:

1) Фильтрация по определенным полям

Можно использовать ключ -o (или --output) в сочетании с форматом json или json-pretty, чтобы получить вывод в формате JSON. Затем, используя утилиты обработки JSON (например, jq), выбрать конкретные поля. Пример:

```
journalctl -o json | jq '.MESSAGE, .PRIORITY'
```

2) **Использование формата short-monotonic**

Формат short-monotonic показывает только основные поля, включая метки времени, которые будут полезны при анализе.

```
journalctl -o short-monotonic
```

3) **Использование формата short-full**

Формат short-full показывает основные поля, включая метки времени, приоритет и идентификаторы:

```
journalctl -o short-full
```

4) **Создание пользовательского формата**

journalctl позволяет указать, какие поля отображать, используя формат verbose, но это может быть слишком подробным. Можно использовать awk или другие утилиты для обработки вывода journalctl и выбора конкретных полей. Пример:

```
journalctl -o json | jq ' . | {timestamp: .__REALTIME_TIMESTAMP, message: .MESSAGE}'
```

5) **Фильтрация по конкретным критериям**

Можно фильтровать вывод journalctl по конкретным полям прямо в командной строке. Например, чтобы отфильтровать сообщения от конкретного сервиса или с определенным приоритетом:

```
journalctl _SYSTEMD_UNIT=sshd.service
```

Или по приоритету (например, только ошибки и критические сообщения):

```
journalctl -p err
```

6) **Использование --output-fields**

С версии systemd 246, можно использовать --output-fields для вывода только определенных полей:

```
journalctl --output-fields=MESSAGE,PRIORITY,_PID
```

Примеры использования

Пример 1: Выводить только сообщения и приоритеты

```
journalctl -o json | jq ' . | {message: .MESSAGE, priority: .PRIORITY}'
```

Пример 2: Выводить сообщения только от определенного сервиса с указанием времени

```
journalctl _SYSTEMD_UNIT=sshd.service -o json | jq '. | {time:
.__REALTIME_TIMESTAMP, message: .MESSAGE}'
```

Использование protector.log

Журнал protector.log осуществляет журналирование попыток входа в защищенные директории, входящие в программный модуль libprotector. Ниже представлен формат записи:

```
<unique_id> <timestamp> <username> <process_name> attempted to <action>
protected resource <pathname>
```

9.6 Резервное копирование с использованием файловой системы Overlayfs

В основе работы с бэкапами лежит Overlayfs (Overlay Filesystem), которая представляет собой наложенную файловую систему, позволяющую объединять два отдельных каталога (нижнюю и верхнюю директории) в одну единую файловую систему.

После монтирования содержимое нижней и верхней директорий будет доступно через объединенную точку монтирования /mnt/overlay. Любые изменения в этой директории будут записаны в верхнюю директорию, в то время как нижняя директория останется неизменной.

Подробное описание слоев

Overlayfs функционирует посредством объединения двух директорий в слои:

1) Нижний слой (lowerdir):

- Является неизменяемым и содержит исходные данные.
- Этот слой может быть общей директорией, доступной для чтения нескольким файловым системам Overlayfs.
- Может быть использован в различных сценариях, таких как предоставление базовой файловой системы, на которую накладываются изменения.

2) **Верхний слой (upperdir):**

- Является изменяемым и содержит все изменения, вносимые в файловую систему.
- Если файл изменяется или создается в объединенной точке монтирования, он будет записан в верхнюю директорию.
- Если файл в нижнем слое изменяется или удаляется, верхний слой содержит соответствующую информацию для обработки этих изменений.

3) **Рабочая директория (workdir):**

- Используется для внутренних операций Overlayfs.
- Эта директория необходима для того, чтобы верхний слой функционировал корректно.
- Рабочая директория должна находиться на том же файловом разделе, что и верхняя директория.

4) **Промежуточные слои (read-only layers):**

- Overlayfs поддерживает использование нескольких промежуточных слоев, которые являются неизменяемыми.
- Эти слои располагаются между нижней директорией и верхней директорией.
- Промежуточные слои позволяют создавать более сложные структуры файловых систем с множеством уровней неизменяемых данных.
- Пример монтирования с промежуточными слоями:

```
mount -t overlay overlay -o  
lowerdir=/mnt/lower:/mnt/lower2:/mnt/lower3,upperdir=/mnt/upper,workdir=/mnt/  
work /mnt/overlay
```

Резервные копии виртуальных машин

Создание резервной копии

Для настройки резервного копирования виртуальных машин необходимо выполнить следующие действия:

- 1) Настроить директорию для хранения резервных копий. По умолчанию установлена директория **/var/backups/[имя_VM]**
- 2) По умолчанию, таймер для создания копий VM установлен на 00 ч., 00 мин., 0 сек. Для изменения расписания необходимо перейти в директорию **/usr/lib/systemd/system/backup-all-vms.timer**, затем после внесенных изменений выполнить команду:

```
systemctl daemon-reload
```

Для создания резервной копии VM необходимо выполнить команду:

```
systemctl start backup-all-vms.service &
```

По умолчанию, при отсутствии копии VM, создается полная резервная копия.

Восстановление виртуальной машины

Прежде чем начать восстановление, важно убедиться, что были соблюдены все условия:

- была создана резервная копия диска VM;
- доступно хранилище для восстановления копий VM.

Если диск виртуальной машины, который необходимо восстановить, все еще работает или существует, нужно остановить VM и удалить текущий диск:

```
virsh shutdown имя_виртуальной_машины
```

Удаление диска (если необходимо):

```
virsh vol-delete имя_диска --pool имя_пула
```

Для восстановления виртуальной машины необходимо использовать команду **virtbdrestore**. Эта команда восстановит данные с NBD-устройства на диск виртуальной машины.

Пример команды:

```
virtbdrestore -i (ПУТЬ_К_БЕКАПУ) -o (КУДА_СОХРАНИТЬ_ОБРАЗЫ)
```

Убедиться, что диск был восстановлен.

Защита памяти

Для предотвращения доступа субъекта к остаточной информации в СВ “Звезда” реализована функция очистки памяти.

При создании образа диска на сервере виртуализации согласно условиям по безопасности создается дисковое пространство, заполненное нулями. Очистка осуществляется посредством перезаписи каждого байта создаваемого образа диска ВМ нулями. Очистка памяти используется при создании и удалении виртуальных машин (при создании образа диска для ВМ), таким образом предотвращается доступ субъектов к остаточной информации, а также после переполнения журнала событий.

Управление и защита контейнеров

Подпись контейнера

Для подписи контейнера необходимо выполнить следующие действия:

1) Импортировать образ контейнера в docker с помощью команды:

```
docker import [название_контейнера].tag.xz [имя_контейнера]
```

2) Применить IMA-подписи:

```
apply-ima
```

3) Запустить образ с помощью команды:

```
docker run --detach --privileged --cap-add=ALL --network=host --name [имя_контейнера]  
--entrypoint "" [имя_контейнера] /bin/bash -c "while true; do sleep 60; done"
```

4) Войти в контейнер:

```
docker exec -it [имя_контейнера] bash
```

Внимание! Неподписанные контейнеры не будут запущены.

Для запуска docker необходимо предварительно загрузить образ для контейнера, затем запустить контейнер с помощью команды `docker run [имя контейнера]`. Для того чтобы убедиться, что контейнер запущен, необходимо ввести команду `docker ps`. С помощью данной команды можно просмотреть список всех запущенных контейнеров.

Создание образов контейнеров

Для создания образа контейнера разработчик образов контейнеров должен выполнить следующие действия:

- 1) Войти в СВ “Звезда”.
- 2) Создать предварительно директорию /var/tmp/template/cache с помощью команды mkdir.
- 3) Загрузить полученные от разработчика СВ “Звезда” образ с шаблонами контейнеров с помощью утилиты scp в СВ “Звезда”:

```
scp /место/расположения/шаблонов/  
dev_img_docker@10.10.102.102:/var/tmp/template/cache
```

В поле после “@” необходимо ввести IP-адрес СВ “Звезда”.

- 4) Создать bash-сценарий. Ниже представлен пример bash-сценария:

```
#!/bin/bash
```

```
##### Set Variables #####
```

```
hostname="pve01"
```

```
container_name="container104"
```

```
template_path="/var/tmp/template/cache"
```

```
network="custom_bridge"
```

```
ip="192.168.0.93"
```

```
subnet="192.168.0.0/24"
```

```
nameserver="8.8.8.8"
```

```
ram="1024m"
```

```
rootpw="password"
```

```
gateway="192.168.0.1"
```

```
bridge="vmbr0"
```

```
##### Select Template #####
```

```
echo "Выберите шаблон:"
```

```
options=("alpine" "alt" "debian" "fedora" "ubuntu")
```

```

select          distro          in          "${options[@]}";          do
    if          [[          -n          "$distro"          ]];          then
        template="${distro}-signed.tar.xz"
        image_name="${distro}-container"
        break
    else
        echo          "Некорректный          выбор.          Попробуйте          снова."
    fi
done

#####          Create          Network          if          Not          Exists          #####
if  [[  !  "$(docker          network          ls  |  grep          $network)"  ]];  then
    echo          "Создаётся          сеть          $network..."
    docker          network          create          --subnet=$subnet          $network
fi

#####          Load          from          Template          #####
if  [[  !  "$(docker          images          -q          $image_name          2>/dev/null)"  ]];  then
    echo          "Импорт          шаблона          из          $template_path/$template..."
    cat  "$template_path/$template"  |  docker          import          -  "$image_name"  /bin/sh
fi

#####          Sign          Container          #####
echo          "Подписываю          контейнер          $image_name..."
apply-ima

#####          Run          Container          #####
docker          run          -d          \

```

```

--name                $container_name          \
--hostname            $hostname                \
--memory              $ram                     \
--net                 $network                 \
--ip                  $ip                      \
--dns                 $nameserver              \
--env                 "ROOT_PASSWORD=$rootpw"  \
--restart              unless-stopped           \
"$image_name" /bin/sh -c "while true; do sleep 3600; done"

```

echo "Контейнер \$container_name (\$distro) создан и подписан успешно."

9.7 Централизованное управление образами контейнеров и контейнерами

Для просмотра списка всех контейнеров, которые были запущены, можно использовать команду `docker ps -a`.

```

$ docker ps -a
CONTAINER ID   IMAGE          COMMAND                  CREATED          STATUS          PORTS          NAMES
305297d7a235   image1         "uptime"                11 minutes ago   Exited (0) 11 minutes ago   distracted_goldstine
ff0a5c3750b9   image2         "sh"                    12 minutes ago   Exited (0) 12 minutes ago   elated_ramanujan

```

Для запуска более одной команды в `docker` необходимо запустить контейнер с флагом `-it`, который подключает интерактивный `tty` в контейнер.

Для централизованного хранения образов контейнера используется локальный реестр образов, который позволяет контролировать доступ в него. Данный реестр настраивается с помощью Docker CLI: `docker run -d -p 5000:5000 --name registry registry:2`. Так же можно тегировать образ для локального реестра с помощью

команды `docker tag <image_id> localhost:5000/<repository>:<tag>`. Для загрузки образа в локальный реестр необходимо ввести команду `docker push localhost:5000/<repository>:<tag>`. Для загрузки образа из локального реестра необходимо ввести команду `docker pull localhost:5000/<repository>:<tag>`.

Ограничение прав на использование вычислительных ресурсов контейнера

Для ограничения использования объема оперативной памяти в контейнере необходимо запустить контейнер со следующими параметрами:

```
docker run -d --name test_container --memory=512m ubuntu /bin/bash
```

Регистрация событий безопасности в контейнере

Для просмотра журнала контейнера, необходимо ввести команду `docker logs`. Необходимый контейнер должен быть запущен в этот момент. Далее необходимо узнать container ID с помощью команды:

```
docker ps
```

После этого можно посмотреть логи данного контейнера: `docker logs -f ff0a5c3750b9`. Журналы содержат данные выходного потока с отметкой времени. Приведенная выше команда не содержит непрерывный вывод журнала. Чтобы просмотреть непрерывный вывод журнала контейнера, нам нужно использовать параметр `-follow` в команде `docker logs`.

По умолчанию Docker хранит файлы журнала в выделенном каталоге на хосте с помощью драйвера журнала `json-file`. Каталог файла журнала — `/var/lib/docker/containers/<container_id>` на хосте, на котором запущен контейнер.

Для очистки журнала Docker необходимо выполнить команду:

```
truncate -s 0 /var/lib/docker/containers/*/*-json.log
```

Данная команда не удалит файл журнала, но удалит его содержимое.

Изоляция контейнеров

Основные механизмы для обеспечения изоляции и управления ресурсами в контейнерах включают `namespaces` и `cgroups`. Технологии `namespaces` и `cgroups`

вместе обеспечивают изоляцию и контроль ресурсов для контейнеров, что позволяет запускать приложения в безопасной и управляемой среде.

Использование Docker для настройки Namespaces и Cgroups

В Docker namespaces и cgroups автоматически настраиваются при создании контейнеров, но можно задавать параметры вручную через флаги командной строки. Ниже приведены шаги по проверке корректной изоляции пространств имен контейнеров.

Изоляция пространств имен для пользователей и групп контейнеров

1) Создать пользователя dockremap:

```
sudo useradd -r -s /usr/sbin/nologin dockremap
```

Флаг `-r` создаёт системного пользователя. `-s /usr/sbin/nologin` запрещает вход в систему.

2) Проверить, что пользователь создан:

```
id dockremap
```

3) Добавить диапазоны UID/GID

```
echo "dockremap:100000:65536" | sudo tee -a /etc/subuid
```

```
echo "dockremap:100000:65536" | sudo tee -a /etc/subgid
```

4) Проверить изменения:

```
cat /etc/subuid | grep dockremap
```

```
cat /etc/subgid | grep dockremap
```

5) Вывод должен содержать:

```
dockremap:100000:65536
```

6) Перезапустить Docker:

```
systemctl restart docker
```

7) Запустите контейнер:

```
docker run -it --rm alpine sh
```

8) Проверьте user namespace:

```
lsns -t user
```


Ожидаемый результат — новый namespace для контейнера.

Изоляция пространств имен хостов и доменов контейнеров

Изоляция имен хостов контейнеров подразумевает существование разных hostname для каждого контейнера:

- 1) Запустить контейнер №1:

```
docker run -it --entrypoint "" ubuntufortest /bin/bash -c "while true; do sleep 60; done"
```

- 2) Войти в него:

```
docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS        NAMES
ab3e560b4de4   ubuntufortest "/bin/bash -c 'while... 6 seconds ago   Up 6 seconds   interesting_mccarthy
svz102         ~                                     #
svz102 ~ # docker exec -it ab3e560b4de4 bash
```

- 3) Ввести команду hostname:

```
root@ab3e560b4de4:/# hostname
ab3e560b4de4
root@ab3e560b4de4:/#
```

- 4) Hostname был отображен. Выполнить шаги 1-4 для контейнера №2 и убедиться, что hostname для каждого контейнера уникальны.

Изоляция сетевых пространств имен контейнеров

- 1) Войти в контейнера №1 и №2, ввести команду ifconfig.

- 2) Выводы команд должны отличаться MAC-адреса.

Изоляция пространств имен для иерархии каталогов контейнеров

Каталоги контейнеров находятся в директории /var/lib/docker/containers/имя_контейнера. Изоляция обеспечена существованием для каждого контейнера идентификационным номером, тем самым изменения в контейнере №1 никак не влияют на каталог контейнера №2.

Изоляция представлена на изображениях ниже.

Изоляция пространств имен для иерархии каталогов контейнеров

Рисунок 5.1 – Изоляция пространств имен для иерархии каталогов контейнеров



Рисунок 5.2 – Изоляция пространств имен для иерархии каталогов контейнеров

Аппаратная изоляция контейнеров

1) **Пример запуска контейнера с ограничением использования памяти и процессора:**

```
docker run -d --name my_container --memory=256m --cpus=0.5 my_image
```

Этот пример создаёт контейнер с лимитом в 256MB памяти и ограничением использования процессора до 50%.

Технологии namespaces и cgroups вместе обеспечивают изоляцию и контроль ресурсов для контейнеров, что позволяет запускать приложения в безопасной и управляемой среде.

— Ограничение I/O:

```
docker run --device-write-bps /dev/sda:1mb nginx
```

- Ограничение путем назначения разных VLAN - необходимо настроить и назначить контейнерам разные VLAN:

1) Создать контейнер с VLAN1, предварительно необходимо создать для контейнера сеть:

```
svz ~ # docker network create -d macvlan \
--subnet=10.10.106.0/24 \
```

--gateway=10.10.106.1 \

-o parent=eno49.10 eno49_10_net

2) Запустить контейнер:

```
docker run --rm --detach --name ubuntu-eno49.10 --network eno49_10_net --entrypoint ""  
ubuntu /bin/bash -c "while true; do sleep 60; done"  
3c152d0f5b3d1467bd9e5def0139f89093fc5309dbf3dff5b192a34304e151e5
```

3) Создать сеть для второго контейнера:

```
docker network create -d macvlan \  
--subnet=10.10.107.0/24 \  
--gateway=10.10.107.1 \  
-o parent=eno49.20 eno49_20_net
```

4) Запустить контейнер №2:

```
docker run --rm --detach --name ubuntu-eno49.20 --network eno49_20_net --entrypoint ""  
ubuntu /bin/bash -c "while true; do sleep 60; done"
```

5) Запустить на первом контейнере iperf3 для проверки соединения:

```
Docker exec -it ubuntu-eno49.20 iperf3 -c 10.10.106.2
```

6) Необходимо убедиться, что связи между контейнерами нет.

— Ограничение скорости сети. В примере приводятся ограничения до 100 Мбит/с и 1 Гбит/с:

1) **Пример ограничения сети до 100 Мбит/с:**

Используется команду `tc` для создания ограничения сетевой пропускной способности на уровне Docker. Например, интерфейс контейнера называется `eth0`.

Выполнить следующие команды для ограничения до 100 Мбит/с:

— Необходимо узнать PID процесса контейнера:

```
docker inspect --format '{{.State.Pid}}' limited-memory-ubuntu
```

— Выполнить команду `tc` для ограничения скорости (подставьте PID процесса контейнера в путь):

```
nsenter -t <PID> -n tc qdisc add dev eth0 root tbf rate 100mbit burst 32kbit latency 400ms
```

2) Измерение скорости с помощью iperf3:

Теперь можно измерить скорость передачи данных через iperf3. На хосте выполнить команду:

— На хосте запустить сервер iperf3:

```
iperf3 -s
```

— В контейнере запустить клиент iperf3:

```
docker exec -it limited-memory-ubuntu iperf3 -c <ip-хоста>
```

Это измерит скорость передачи данных между контейнером и хостом с учетом ограничения 100 Мбит/с.

3) Установка пропускной способности до 1 Гбит/с:

Для установки пропускной способности до 1 Гбит/с повторить команду с новым значением:

```
nsenter -t <PID> -n tc qdisc change dev eth0 root tbf rate 1gbit burst 32kbit latency 400ms
```

Монтирование корневой файловой системы хоста в контейнер в режиме “только для чтения”

Выполнить команды:

— Создать папку, например, testdirectory:

```
mkdir /root/testdirectory
```

— Выполнить команду:

```
docker run --rm -it --mount type=bind,source="$root/testdirectory",target=/app,readonly  
ubuntu /bin/bash
```

Выявление уязвимостей в образах контейнеров

Выявление уязвимостей в образах контейнеров проводится администратором средства контейнеризации при создании, запуске и перезагрузке контейнера. При обнаружении уязвимостей дальнейшее использование образа запрещено.

Разработчик образов контейнеров должен не реже одного раза в неделю осуществлять проверку уязвимостей в образах контейнеров сертифицированным ФСТЭК России средством (например, программным изделием «Средство

обеспечения безопасности информационных систем MaxPatrol»). При появлении информации о новых уязвимостях в банке данных угроз безопасности информации производитель контейнера проводит с помощью сертифицированных средств проверку незамедлительно. Запрещено создание образов контейнеров, содержащих известные уязвимости критического и высокого уровня опасности.

Контроль целостности контейнеров и их образов

В изделии невозможен запуск неподписанных контейнеров. Проверка целостности происходит автоматически при загрузке и запуске образа.

Идентификация и аутентификация пользователей

Процесс идентификации пользователей происходит через встроенную систему аутентификации. Пароль и логин пользователя задает администратор системы, он же уполномочен изменить данные пользователя, а также удалить его.

Монтирование USB-устройства в контейнер

Для монтирования устройства необходимо выполнить следующие действия:

- 1) Подключить USB-устройство к хосту.
- 2) Убедиться, что устройство подключено, выполнив команду:
lsblk
- 3) Создать директорию, куда будет монтироваться устройство:
mkdir -p /mnt/usb
- 4) Монтировать устройство:

```
mount /dev/sde1 /mnt/usb0
```

Важно отметить, что вместо sde1 может быть другое название.

- 5) Проверить, смонтировано ли устройство:

```
lsblk
```

Пример вывода команды:

sda		8:0		0	745,2G	0	disk
—sda1	8:1	0	128M	0	part	/boot/grub	
—sda2	8:2	0	32G	0	part	/run/initramfs/container	

└─sda3	8:3	0	713,1G	0	part	/var
sdb	8:16	0	745,2G	0	disk	
sdc	8:32	0	745,2G	0	disk	
sdd	8:48	0	745,2G	0	disk	
sde	8:64	1	116,2G	0	disk	
└─sde1	8:65	1	116,2G	0	part	/mnt/usb

6) Запустить контейнер:

```
docker run -v /mnt/usb:/usb-data -it <имя_контейнера> /bin/bash
```

7) Убедиться, что устройство было примонтировано, запустив команду **lsblk**, затем перейти в **usb-data** (директория, в которое было смонтировано устройство), убедиться что данные устройства присутствуют.

8) Создать текстовый файл в устройстве:

```
touch test.txt
```

9) Убедиться, что файл появился в устройстве, выполнив команду:

```
ls
```

Просмотр журнала событий контейнера

Для просмотра журнала событий необходимо использовать команду:

```
docker events
```

Для импорта записей о событиях необходимо дополнить команду:

```
docker events > docker_journal.log
```

9.8 Работа с виртуальными машинами

Создание виртуальной машины

Для работы с виртуальными машинами необходимо убедиться, что сервис **libvirtd.service** запущен. Для этого необходимо ввести команду **systemctl status libvirtd.service**.

Для создания виртуальной машины необходимо выполнить следующие действия:

Создание диска

- 1) Необходимо создать диск формата qcow2, для этого необходимо выполнить команду:

```
qemu-img create -f qcow2 ubuntu.qcow2 10G
```

Где 10G - размер диска.

- 2) Загрузить ISO-образ ОС в СВ “Звезда”.
- 3) Создать .xml файл в директории /etc/libvirt/qemu для ВМ, в которой будут указана конфигурация виртуальной машины: virsh create vm1.xml.

Пример XML-файла:

```
<domain type='kvm'>
  <name>test_vm</name>
  <memory unit='KiB'>1048575</memory>
  <currentMemory unit='KiB'>1048576</currentMemory>
  <vcpu placement='static'>1</vcpu>
  <os>
    <type arch='x86_64' machine='pc-q35-3.1'>hvm</type>
    <loader type='rom'>/usr/share/OVMF/OVMF.fd</loader>
    <boot dev='hd'>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
  <clock offset='localtime'>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>destroy</on_crash>
  <devices>
```

```

<disk                                type='file'                                device='disk'>
  <driver                            name='qemu'                                type='qcow2'>
    <source                          file='/etc/libvirt/qemu/ubuntu.qcow2'>
      <target                        dev='vda'                                bus='virtio'>
    </target>
  </driver>
</disk>

```

```

<disk                                type='file'                                device='cdrom'>
  <driver                            name='qemu'                                type='raw'>
    <source                          file='/etc/libvirt/qemu/ubuntu-22.04.4-live-server-amd64.iso'>
      <target                        dev='sda'                                bus='sata'>
    </target>
    <readonly/>
  </driver>
</disk>

```

```

<interface                          type="bridge">
  <mac                              address="02:00:45:d6:7b:15">
  <source                          bridge="ovs-br0">
  <virtualport                      type="openvswitch">
    <parameters                    interfaceid='63940821-5b8a-4ce6-b32a-9699de8d92bd'>
  </virtualport>
  <target                          dev="br2">
  <model                            type="virtio">
</interface>

```

```

<graphics type='spice' port='5900' autoport='no' listen='0.0.0.0' keymap='en-us'>
  <listen                          type='address'                          address='0.0.0.0'>
</graphics>
</devices>
</domain>

```


Добавление пароля для подключения по протоколу spice

Для добавления пароля для подключения по протоколу spice необходимо в конфигурации VM изменить строчку graphics следующим образом:

```
<graphics type='spice' port='5910' autoport='no' listen='0.0.0.0' keymap='en-us'
passwd='P@ssw0rd'>
    <listen                                type='address'                        address='0.0.0.0'/>
</graphics>
```

passwd='P@ssw0rd' - пароль, который необходимо ввести при подключении по протоколу spice.

Добавление диска к VM

Для добавления диска к VM необходимо добавить строчку **disk**:

```
<disk                                type='file'                                device='cdrom'>
<source                                file='/home/createvm/image.iso'/>
<target dev='sda' bus='ide'/>
```

В строчке **type** необходимо указать тип диска, **device** - тип устройства, в строчке **source file** расположение диска, строчка **bus** - тип шины. В примере указано добавление CD-ROM диска.

1) Далее необходимо создать виртуальную машину на основе ранее созданного шаблона .xml:

```
virsh define vm1.xml
```

Где setup.xml - название шаблона .xml.

2) Удостовериться в успешном создании машины с помощью команды virsh list --all.

3) Далее необходимо запустить виртуальную машину:

```
virsh start test_vm
```

Где **test_ubuntu** - имя VM, которое было указано в шаблоне .xml.

Операционная система была установлена.

Далее необходимо осуществить запуск и вход в операционную систему. Перед этим необходимо выполнить следующие действия:

- 4) Закрывать и удалять XML-файл, созданный для установки ВМ, перед этим необходимо выключить ВМ:

```
virsh shutdown test_vm
```

```
virsh undefine test_vm
```

- 5) Создать новый XML-файл для изменения запускаемого диска в файле с CD-ROM на жесткий диск. Остальные параметры можно оставить прежними.
- 6) Необходимо использовать подготовленный образ и конфигурационный XML-файл для создания и запуска виртуальной машины:

```
virsh define vm1.xml
```

```
virsh start test_vm
```

Подключение ВМ к сети

Для подключения ВМ к сети необходимо отредактировать параметр **interface**:

```
<interface type="bridge">
<mac address="02:00:45:d6:7b:15"/>
<source bridge="ovs-br0"/>
<virtualport type="openvswitch">
<parameters interfaceid="6154375c-a99b-4bc7-b528-9a082c1ab565"/>
</virtualport>
<target dev="test_ubuntu2"/>
<model type="virtio"/>
<address type="pci" domain="0x0000" bus="0x0c" slot="0x01" function="0x0"/>
</interface>
```

А именно:

- interface type - тип подключения (в данном случае представлен bridge);
- mac adress - создается пользователем;

- source bridge - здесь необходимо ввести имя сети. Можно узнать с помощью команды `ovs-vsctl show`;
- virtualport type - тип виртуального порта;
- parameters interfaceid - уникальный номер интерфейса, который необходимо узнать с помощью команды `ovs-vsctl show`;
- target dev - имя сети ВМ, которое будет отображаться при выводе команды `ovs-vsctl show`;
- model type - тип шины;
- address type - тип устройства.

Необходимо добавить созданный порт ВМ в bridge. Для этого:

- 1) Выполнить команду `ip a`.
- 2) Найти в списке интерфейс ВМ.

```
svz1406 ~ # ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master ovs-system state UP group default qlen 1000
    link/ether 02:00:71:81:08:75 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::71ff:fe81:875/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
3: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 92:ef:28:85:0d:d1 brd ff:ff:ff:ff:ff:ff
4: sys0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 0e:4d:bb:ea:b4:31 brd ff:ff:ff:ff:ff:ff
    inet 10.10.105.20/24 brd 10.10.105.255 scope global sys0
        valid_lft forever preferred_lft forever
    inet6 fe80::c4d:bbff:feea:b431/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
5: ovs-br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 0e:2e:ce:13:ff:49 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::c2e:ceff:fe13:ff49/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
6: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:2c:2e:86 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
        valid_lft forever preferred_lft forever
11: alpine: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master ovs-system state UNKNOWN group default qlen 1000
    link/ether fe:00:45:d6:7b:15 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::fc00:45ff:fed6:7b15/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
```

Рисунок 759 – Интерфейс ВМ

- 3) Убедиться, что bridge существует. При необходимости - создать его. По умолчанию, bridge создан в СВ “Звезда”(ovs-br0). Для создания bridge выполнить следующие действия:

```

ovs-vsctl                                                    show
ovs-vsctl                                                    add-br          br1
ovs-vsctl add-br br2

```

- 4) Выполнить команду `ovs-vsctl add-port br0 test_ubuntu2`, где **test_ubuntu2** - название интерфейса ВМ, br0 - bridge.
- 5) Необходимо настроить сеть в ВМ, после чего будет получен доступ в интернет.

Редактирование ВМ

Для изменения параметров виртуальной машины необходимо отредактировать исходный файл формата .xml.

- 1) Для изменения названия ВМ отредактировать строку `<name>test_ubunt3</name>`.

- 2) Для изменения настроек сети отредактировать строки:

```

<interface                                                    type='bridge'>
  <virtualport                                                type='openvswitch'>
    <source                                                    bridge='br1'>
      <mac                                                      address='02:00:71:81:18:01'>
        <target                                                dev='br1-1'>
          <model                                                type='virtio'>
        </model>
      </target>
    </source>
  </virtualport>
</interface>

```

- 3) Для изменения дисковых параметров необходимо отредактировать следующие строки:

```

<disk                                                         type='file'          device='disk'>
  <driver                                                       name='qemu'          type='qcow2'>
    <source                                                       file='/fed1.qcow2'>
      <target                                                     dev='sda'            bus='sata'>
        <address          type='drive'          controller='0'      bus='0'      target='0'      unit='0'>
      </address>
    </target>
  </driver>
</disk>

```

Для помещения VM в 2000 VLAN необходимо выполнить команду `ovs-vsctl set port br1-1 tag=2000`. Таким образом, виртуальная машина не будет получать сетевые пакеты.

Снимки состояния VM

Создание снимка состояния VM

Для создания снимка состояния VM необходимо выполнить следующие действия:

1) Выполнить команду:

```
virsh snapshot-create-as <VM_name> <snapshot_name> --description  
"<snapshot_description>"
```

Где:

— это имя вашей виртуальной машины. — это имя создаваемого снимка. — это описание снимка (необязательное поле).

2) Снимок VM был создан. Убедиться, что снимок был сделан, ввести команду:

```
virsh snapshot-list <VM_name>
```

3) Созданный снимок отображен в списке.

Если необходимо сохранить не только диск, но и текущее состояние памяти VM, нужно добавить флаг `--live`:

```
virsh snapshot-create-as ubuntu-vm snapshot1 --description "Snapshot before update" --  
live
```

Восстановление VM с помощью снимка состояния VM

Для восстановления VM выполнить следующие действия:

1) Выполнить команду:

```
virsh snapshot-revert <VM_name> <snapshot_name>
```

2) Убедиться, что VM восстановилась, просмотрев список VM с помощью команды:

```
virsh list --all
```

Удаление снимка VM

Для удаления снимка VM ввести команду:

```
virsh snapshot-delete <VM_name> <snapshot_name>
```

Миграция VM с хоста на хост

Для перемещения виртуальных машин (VM) и их образов с сохранением конфигурации и настроек используется инструмент `virsh`.

Для выполнения миграции необходимо выполнить следующие действия:

- 1) Остановить виртуальную машину (если она запущена):

```
virsh shutdown имя_виртуальной_машины
```

— Проверить статус VM:

```
virsh list --all
```

- 2) Экспортировать конфигурацию VM в файл XML:

```
virsh dumpxml имя_виртуальной_машины > /path/to/имя_виртуальной_машины.xml
```

— Этот файл сохранит всю конфигурацию виртуальной машины.

- 3) Скопировать образ диска VM на новый сервер:

— Найти расположение дискового файла образа:

```
virsh domblklist имя_виртуальной_машины
```

— Скопировать образ на новый сервер с помощью `scp` или `rsync`:

```
scp /path/to/диск.qcow2 user@новый_сервер:/path/to/
```

Или:

```
rsync -av /path/to/диск.qcow2 user@новый_сервер:/path/to/
```

- 4) Скопировать XML-файл конфигурации на новый сервер:

```
scp /path/to/имя_виртуальной_машины.xml user@новый_сервер:/path/to/
```

- 5) Импортировать конфигурацию VM на новом сервере:

— На новом сервере выполнить команду для определения VM:

```
virsh define /path/to/имя_виртуальной_машины.xml
```

— Проверить, что VM определена:

```
virsh list --all
```

- 6) Запустить виртуальную машину на новом сервере:

```
virsh start имя_виртуальной_машины
```

- 7) VM перенесена на новый сервер с сохранением всех настроек и конфигураций.

9.9 Создание снимков системы

Снимки в СВ “Звезда” - это резервные копии текущего состояния системы. Текущее состояние системы — это изменения, внесенные пользователем в процессе работы и сохраненные в системе. Эти изменения в силу архитектуры overlaysfs сохраняются в отдельной директории, и при необходимости могут быть безопасно восстановлены. Безопасность архивирования/восстановления гарантируется тем, что происходит до момента сборки/монтажа системы, на этапе initramfs.

Необходимо убедиться, что дополнительное хранилище для снимков системы было подключено.

Для создания снимка необходимо выполнить следующие действия:

- 1) Перейти в TUI СВ “Звезда”.
- 2) Выбрать **Обслуживание**.
- 3) Выбрать **Снимки**.

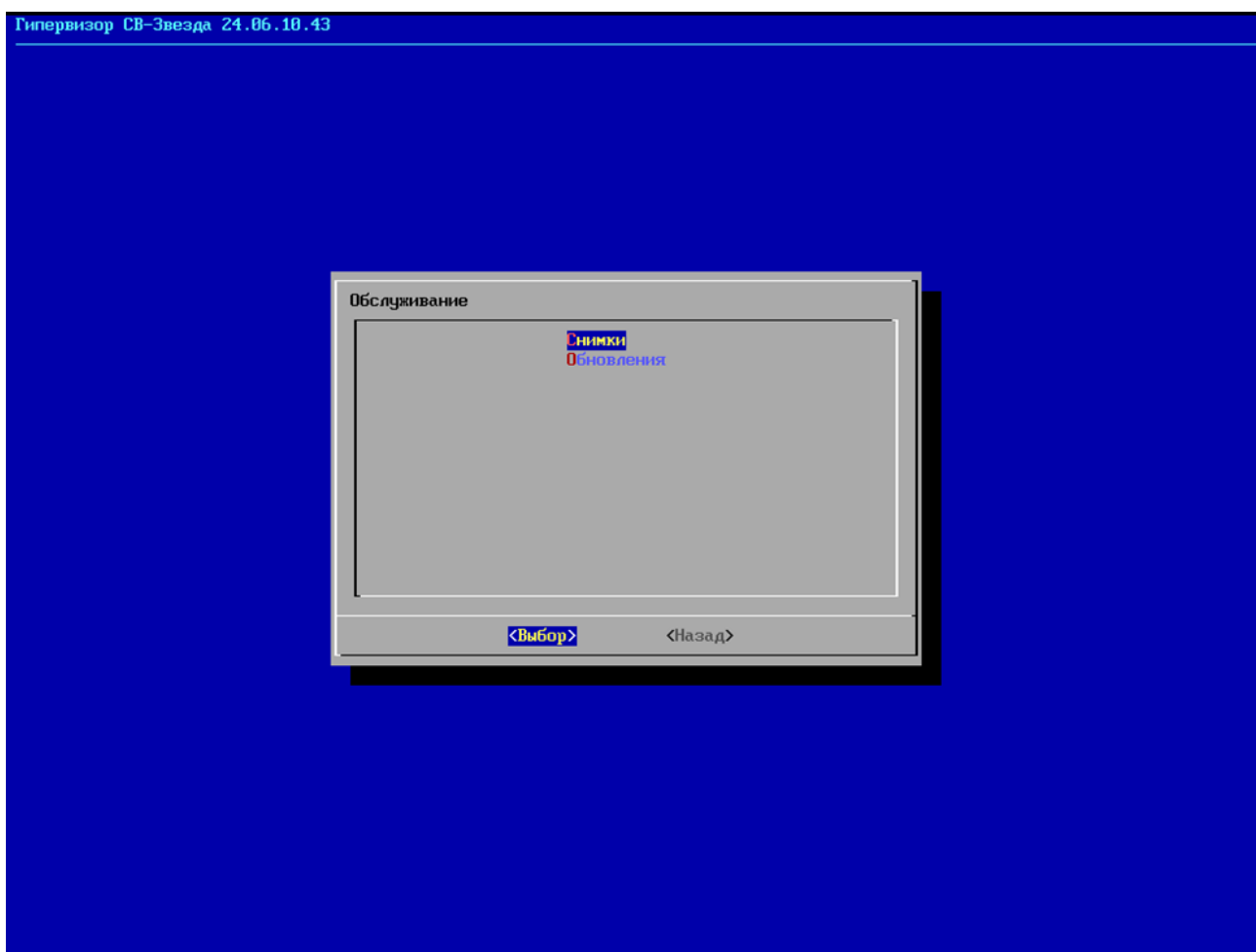


Рисунок 760 – Обслуживание

Будет доступен выбор: - Создать снимок; - Применить снимок; - Удалить снимок.

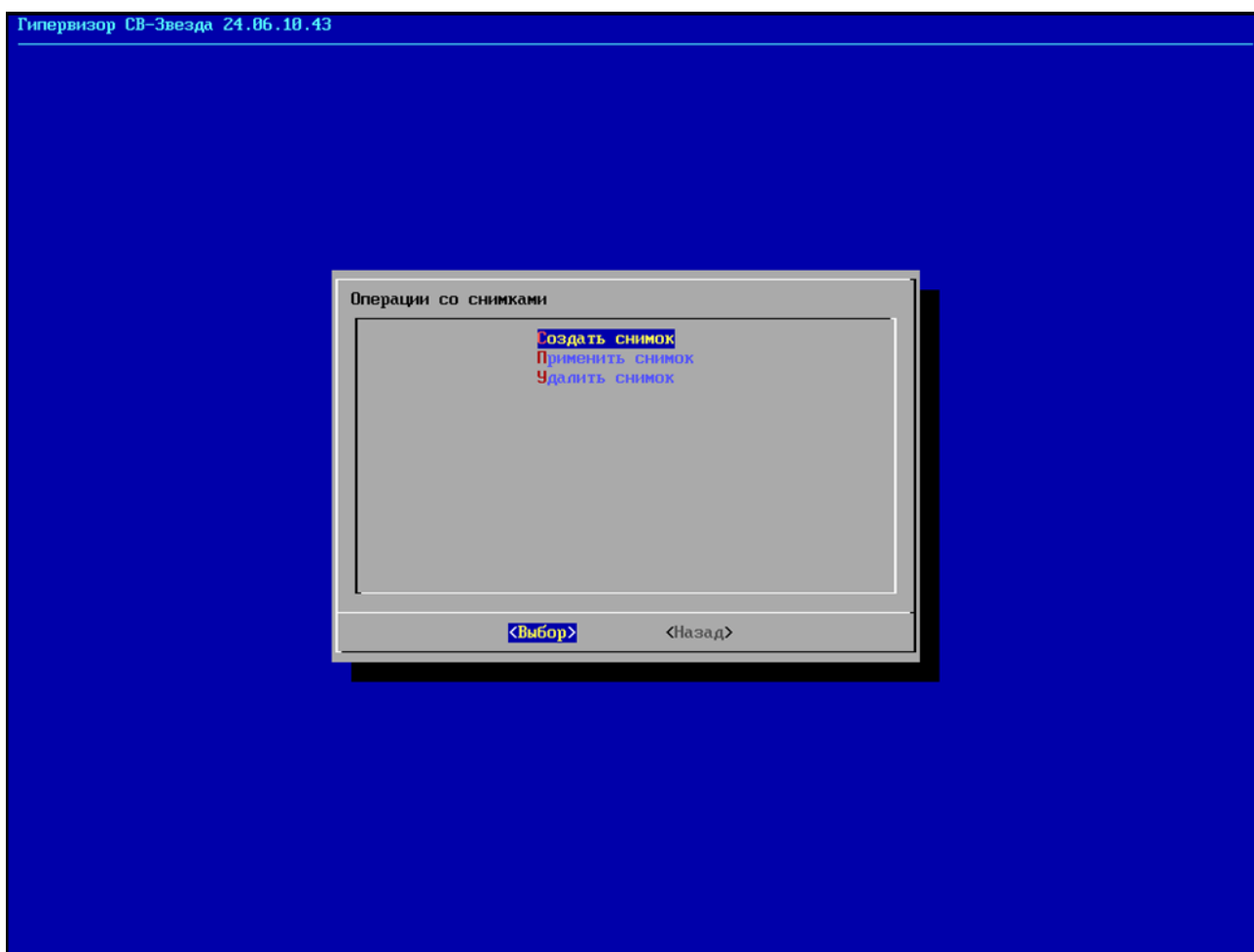


Рисунок 761 – Операции со снимками

При выборе **Создать снимок** создается скрипт, который выполняется при следующей загрузке и архивирует текущее состояние системы. После выбора **Создать снимок** средство виртуализации можно либо выключить, либо перезагрузить. После перезагрузки в меню **Обслуживание - Снимки - Применить снимок** будет доступен список снимков. При выборе нужного снимка TUI создаст скрипт, который при следующей загрузке восстановит состояние системы. Также после выбора снимка система спросит, нужно ли сохранить текущее состояние системы. Если подтвердить, то в снимках после перезагрузки появится соответствующий пункт.

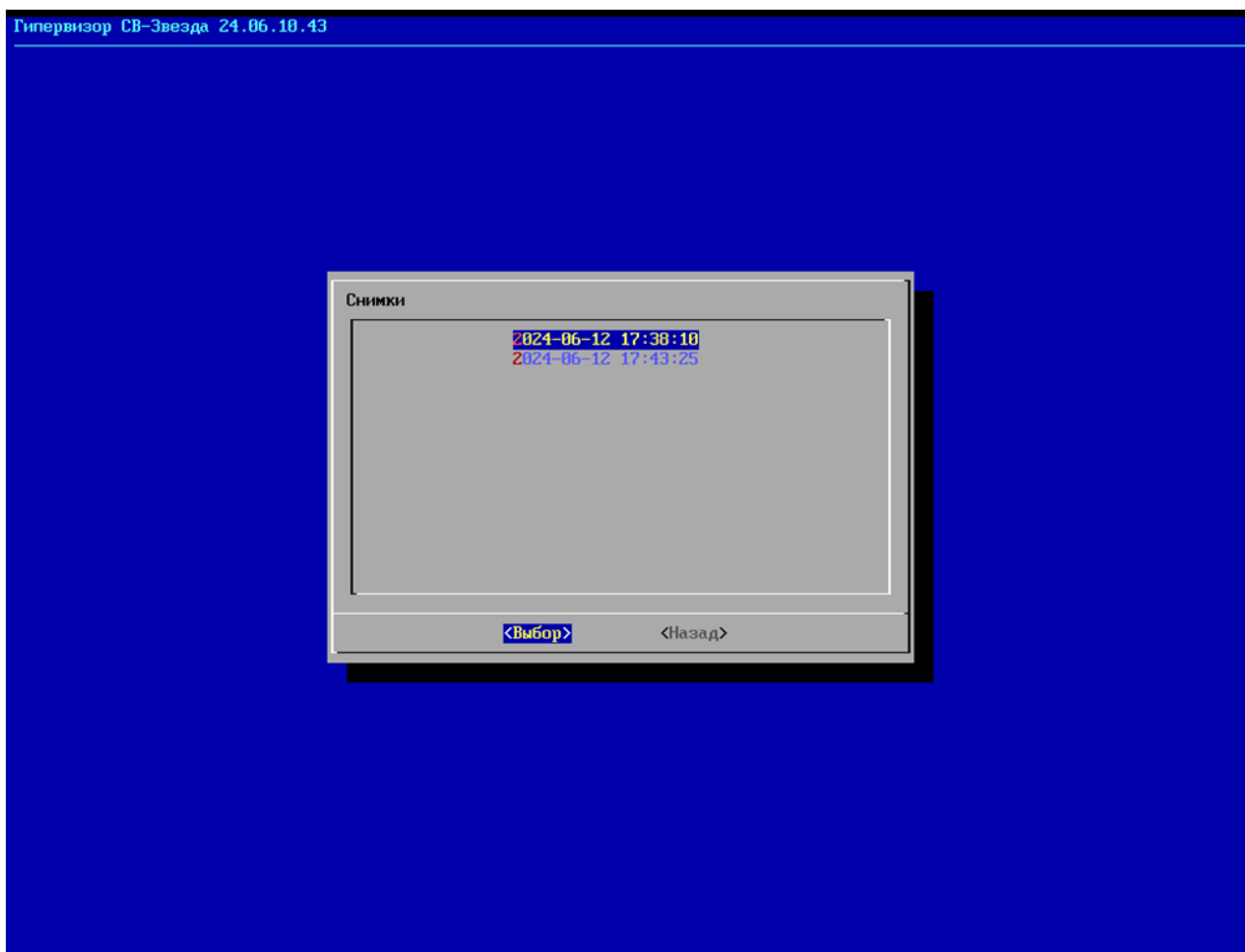


Рисунок 762 – Выбор снимка

Установка приложений

Для установки приложений необходимо выполнить следующие действия:

- 1) Загрузить приложение в необходимую директорию.
- 2) Перейти в TUI СВ “Звезда”.
- 3) Выбрать **Дополнительно**.
- 4) Выбрать **Обслуживание**.
- 5) Выбрать раздел **Приложения**.

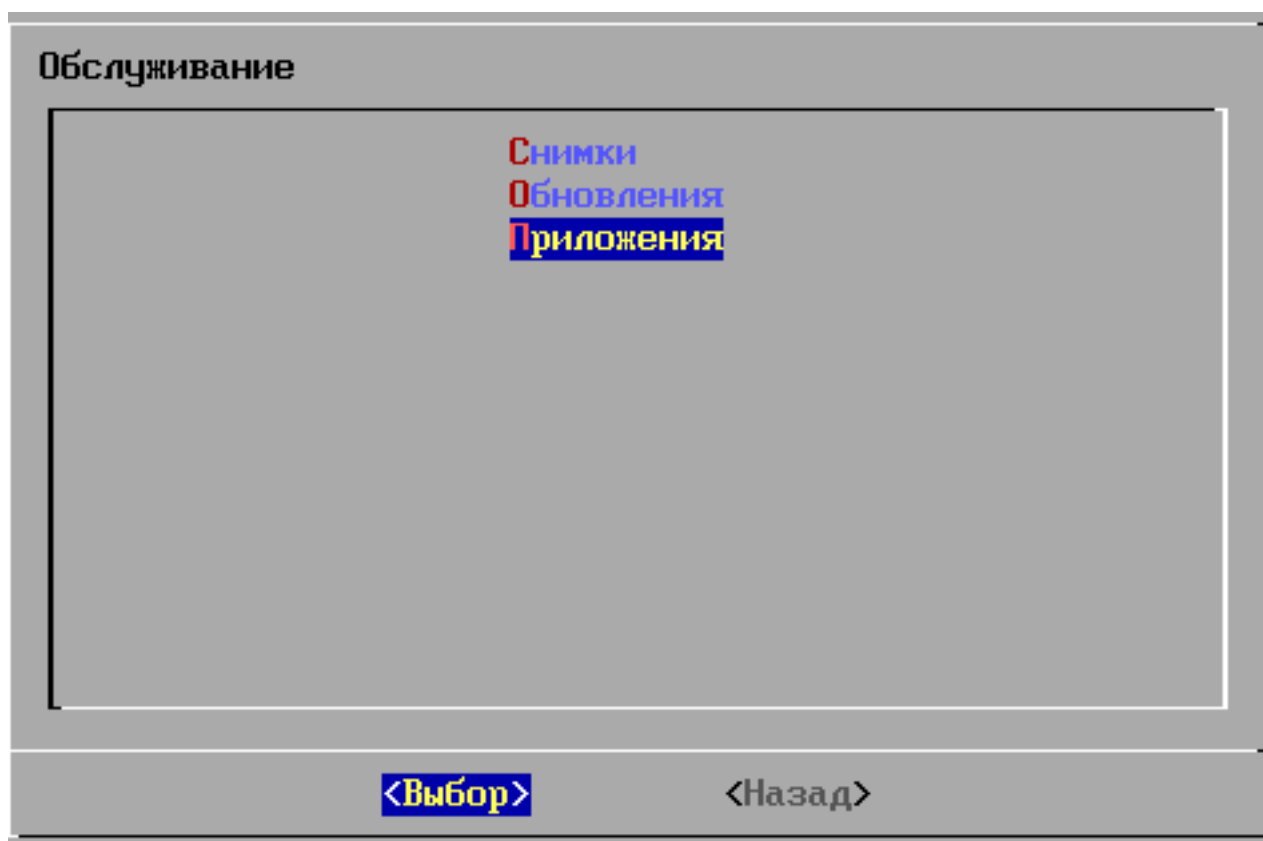


Рисунок 763 – Приложения

- 6) в разделе **Приложения** выбрать директорию, куда были загружены предварительно приложения.

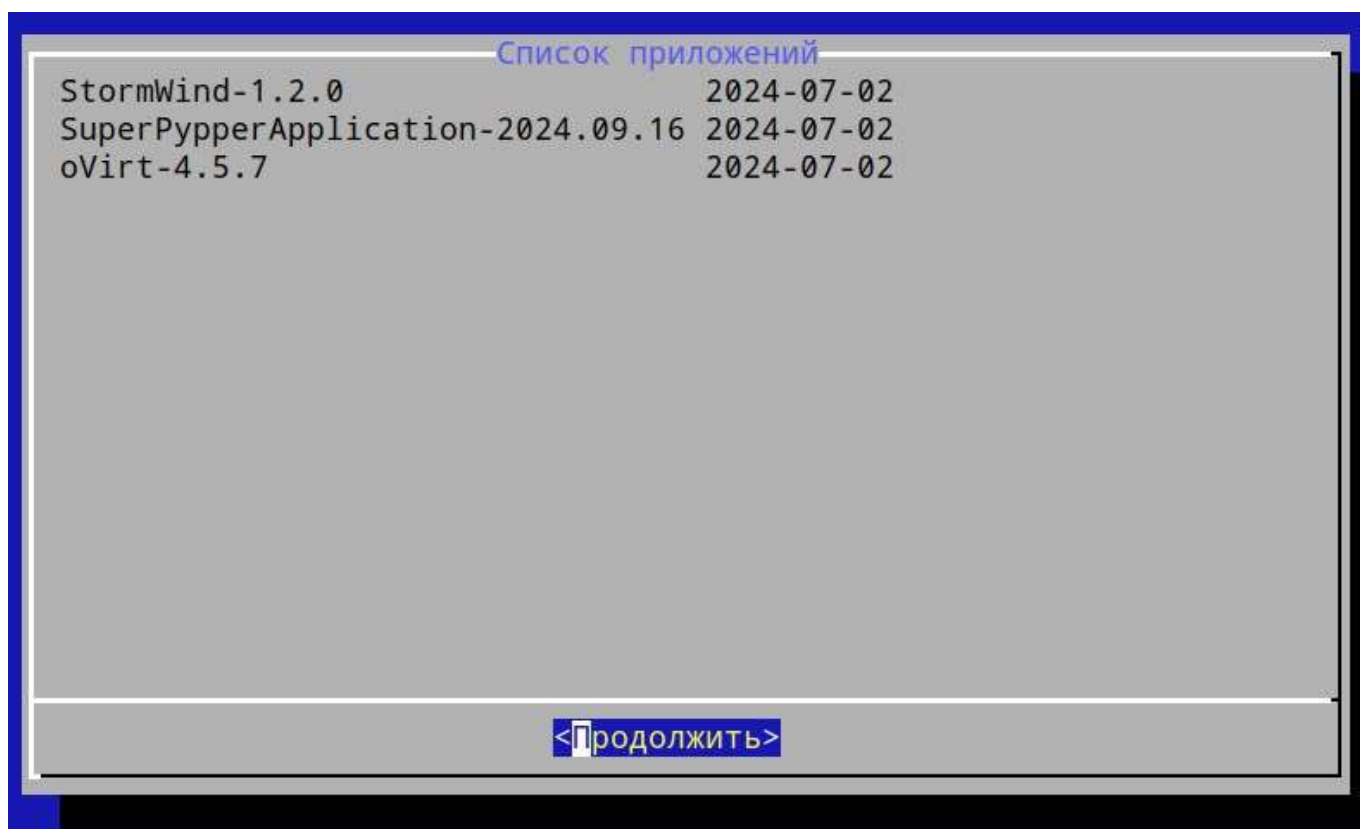


Рисунок 764 – Список доступных приложений

- 7) Нажать на приложение.
- 8) Начнется расшифровка приложения.

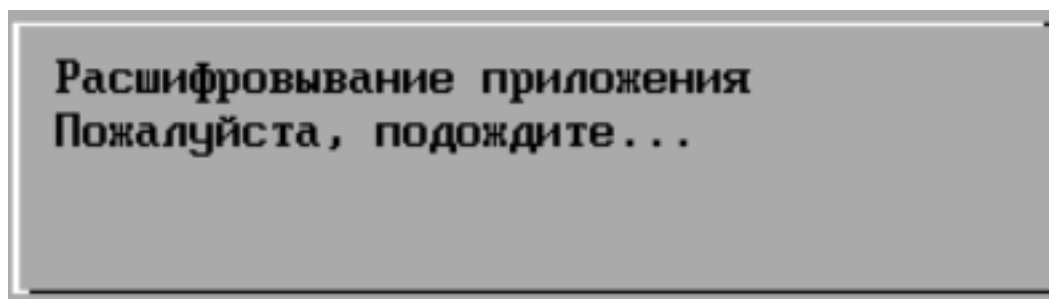


Рисунок 765 – Расшифровка приложения

- 9) Далее система предложит установить приложение.

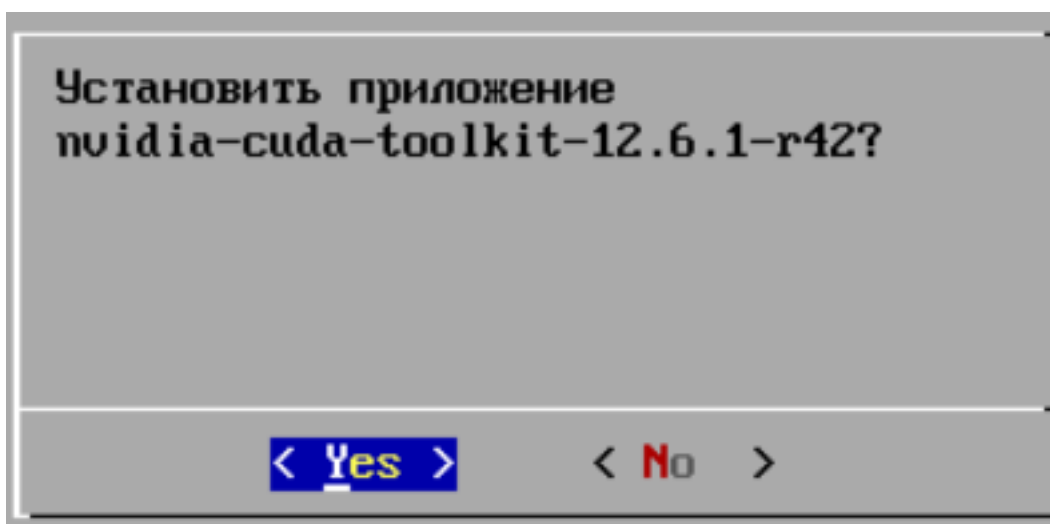


Рисунок 766 – Установка приложений

- 10) Дождаться распаковки и установки приложения.
- 11) После установки необходимо перезагрузить систему.

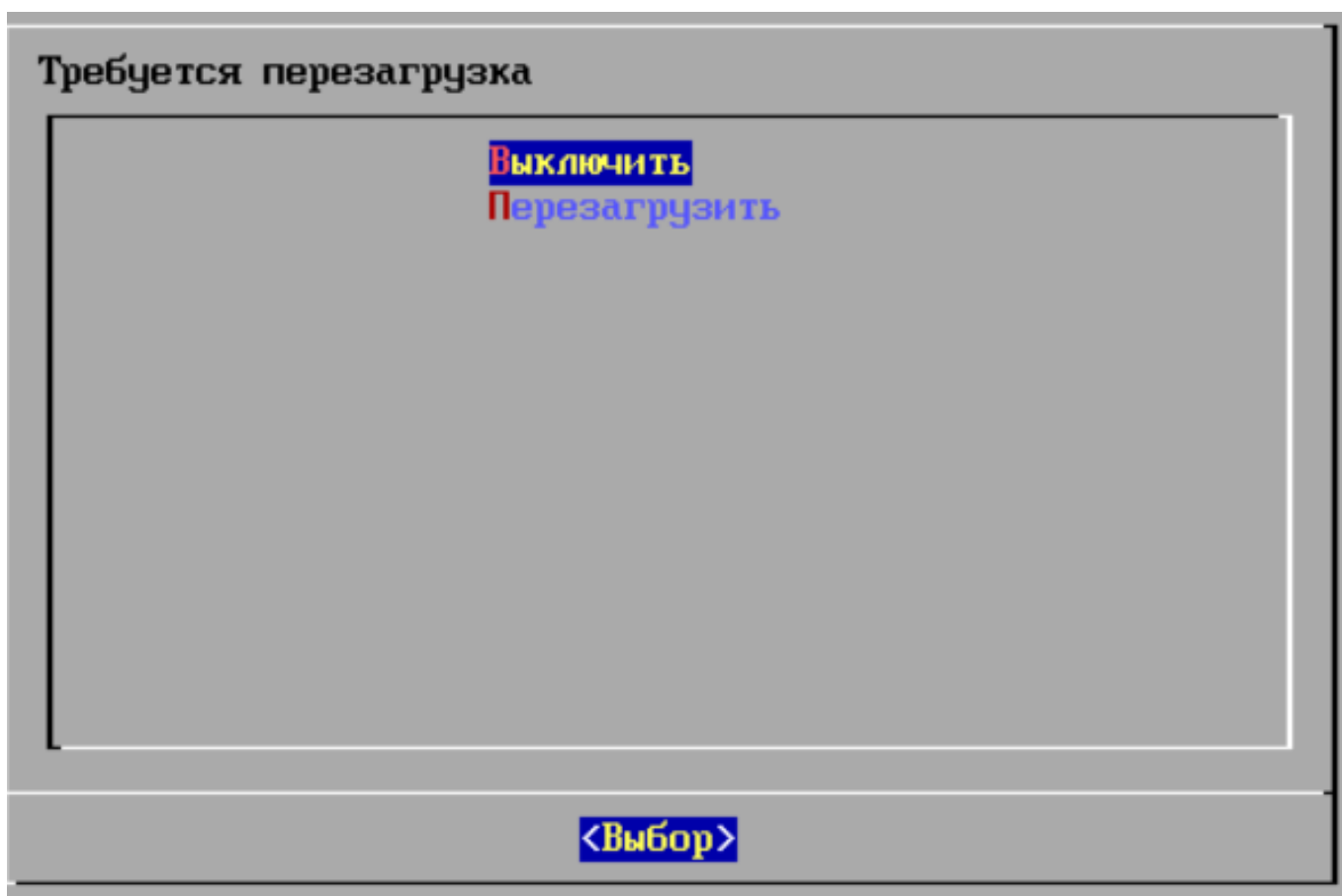


Рисунок 767 – Приложение установлено

Для удаления приложений необходимо выбрать **Удалить** в менеджере приложений. Появится список приложений, для удаления нажать кнопку **Выбор**.

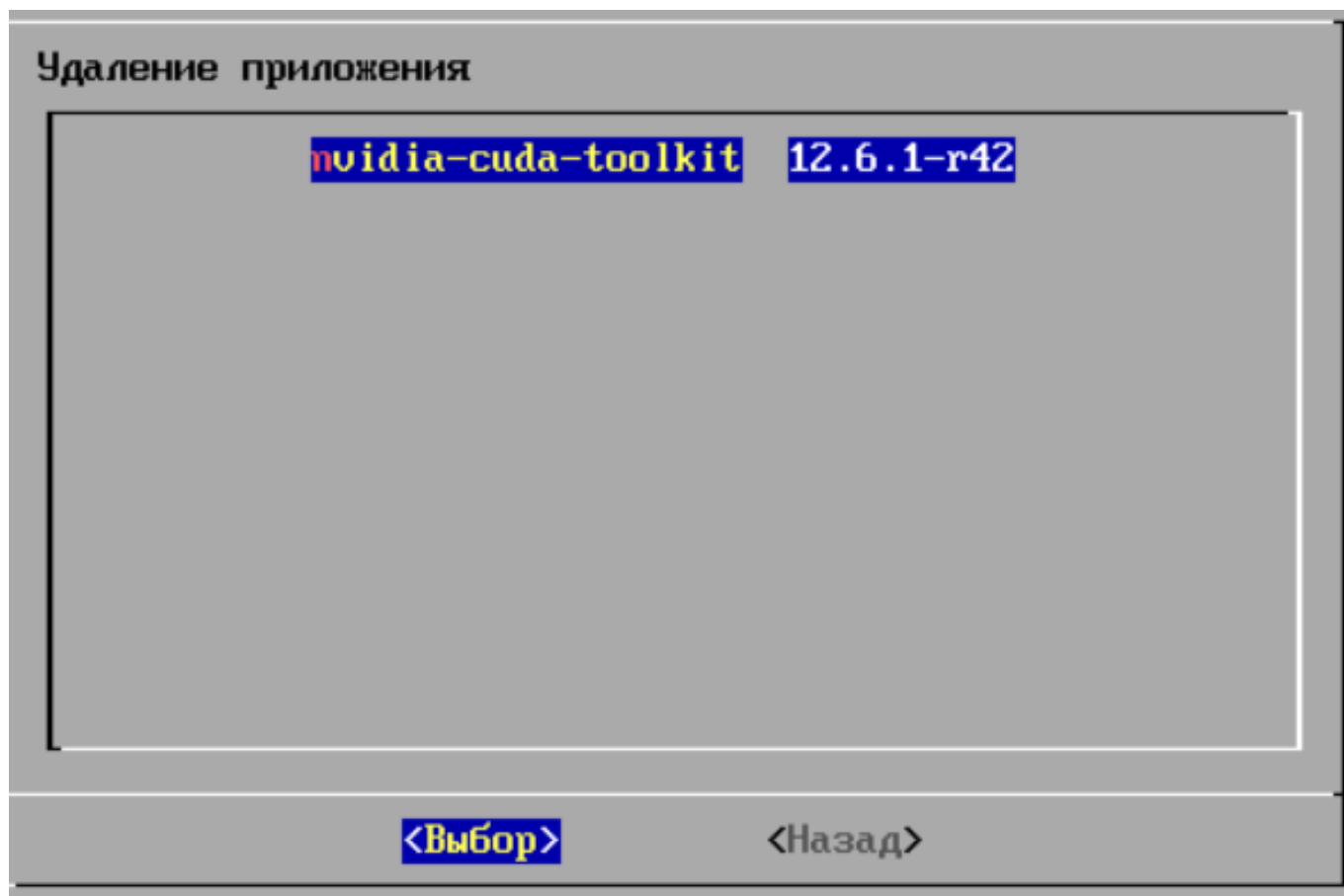


Рисунок 768 – Удаление приложения

После удаления приложения необходимо выполнить перезагрузку системы.

ПРИЛОЖЕНИЯ

Приложение А. Особенности формирования списков пользователей при создании (редактировании) групп адресатов рассылки

Формирование списков пользователей для групп адресатов рассылки проводится при настройке системы рассылки уведомлений Подсистемы мониторинга и доступно в подразделе интерфейса

«Администрирование» → «Уведомления», область «Группы адресатов» (см. Рисунок А.1).

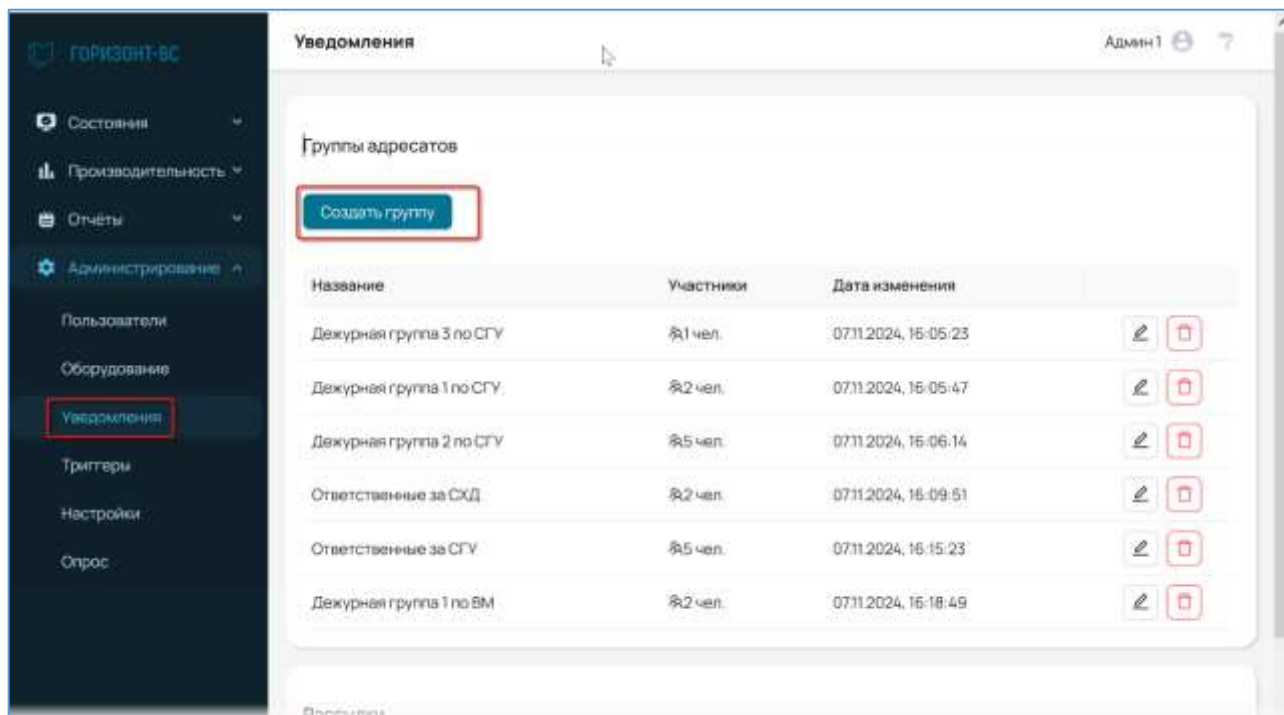


Рисунок А.1 – Группы адресатов рассылки уведомлений от Подсистемы мониторинга

При использовании функций **Создать группу** или значка редактирования группы  (см. Рисунок А.1) на экране открывается форма для создания/ редактирования группы рассылки уведомлений (см. Рисунок А.2).

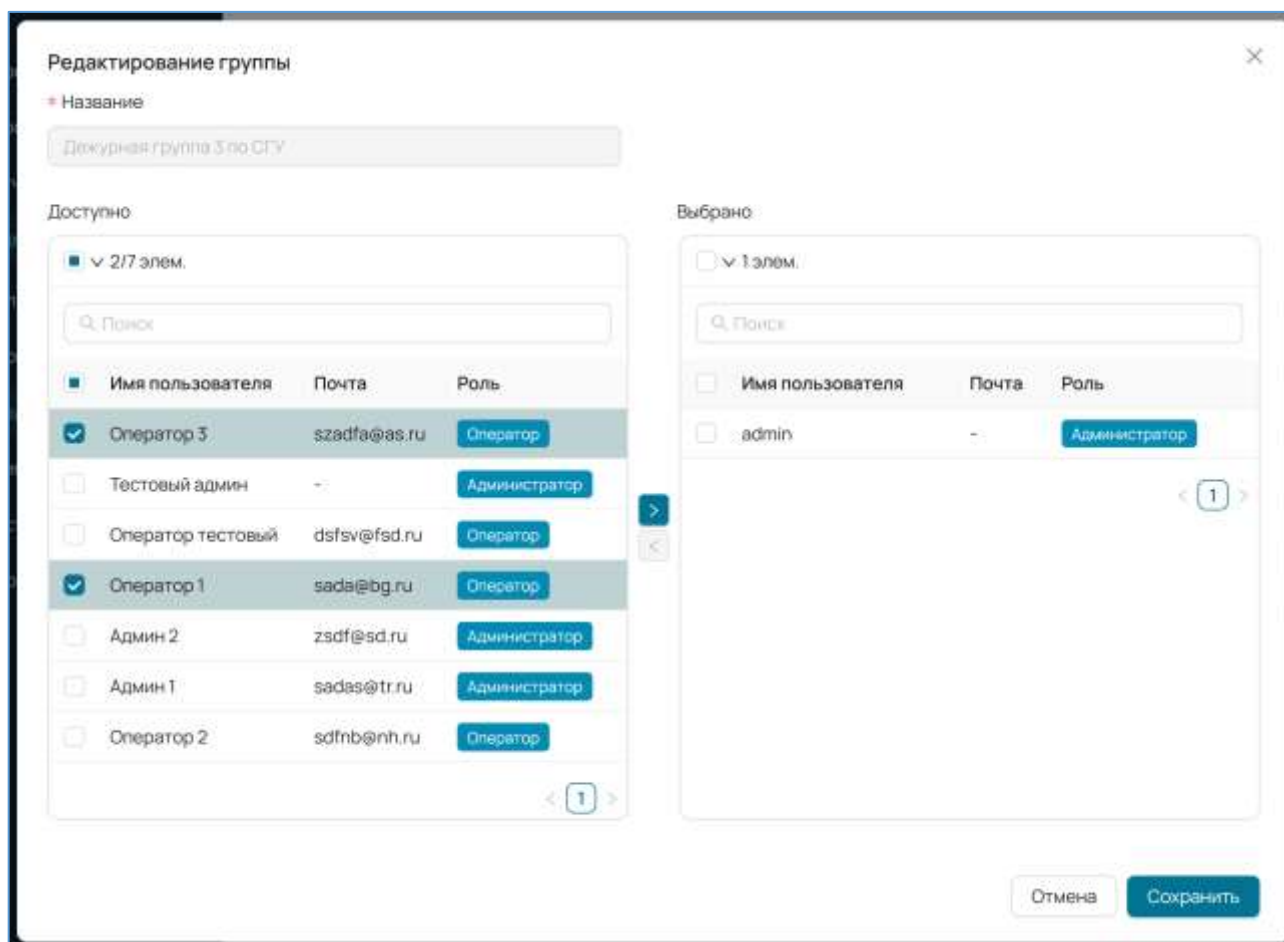


Рисунок А.2 – Редактирование состава группы

Область «Доступно»

Область содержит список пользователей, не вошедших в группу, и, соответственно, доступных для добавления в редактируемую группу. При создании новой группы область «Доступно» содержит список всех пользователей, зарегистрированных на тот момент в Подсистеме мониторинга.

Список пользователей включает следующие поля: поле выбора строки (☐/ ☒) , **Имя пользователя**, **Почта** и **Роль** (см. Рисунок А.2).

В верхней части области расположены (см. Рисунок А.3).

- счетчик элементов таблицы формата: **<выбрано>/<всего> элем.**;
- стандартное флаговое поле выбора/отмены всех элементов списка ☐/ ☒/ ☐ – соответственно *не выбрано/ выбрано все/ выбраны отдельные элементы*;

- раскрывающийся список функций **Выбрать все данные** и **Инвертировать выбор**.

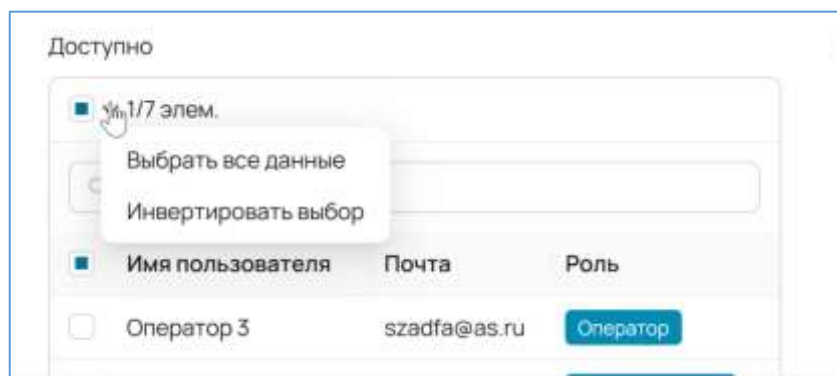


Рисунок А.3 – Счетчик элементов таблицы и функции выбора элементов

Так же в верхней части области расположено поле поиска в списке пользователей по текстовой строке (см. Рисунок А.4). Поиск проводится с учетом регистра по полям **Имя пользователя** и **Роль**.

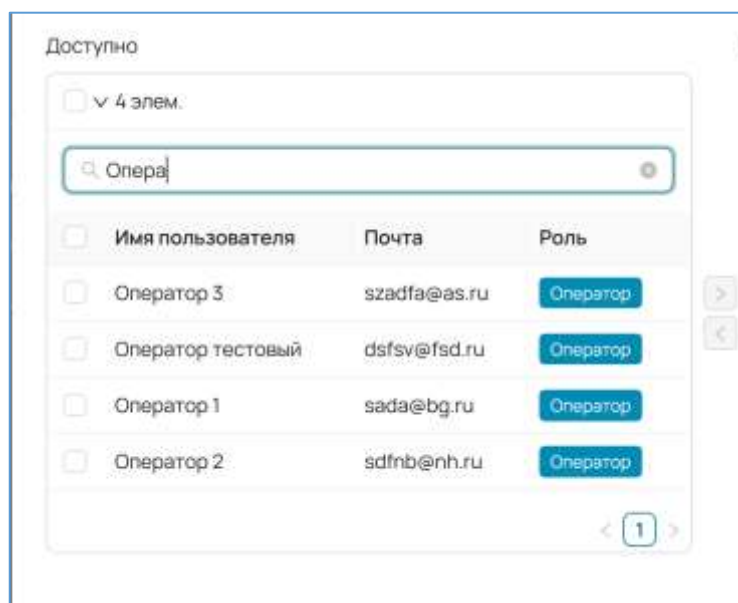


Рисунок А.4 – Пример использования функции поиска

Область «Выбрано»

Область содержит список пользователей указанной группы. При создании новой группы область «Выбрано» пустая.

Функционал данной области аналогичен функционалу области «Доступно».

Стрелки переноса

Стрелки между областями «Доступно» и «Выбрано» служат для переноса выбранных элементов в соответствующую область:

-  – перенос указанных пользователей из списка «Доступно» в список «Выбрано», реализация добавления пользователей в группу. Стрелка активизируется только при выборе пользователя в списке «Доступно».
-  – перенос указанных пользователей из списка «Выбрано» в список «Доступно», реализация удаления пользователей из группы. Стрелка активизируется только при выборе пользователя в списке «Выбрано».

Приложение Б. Особенности формирования рассылки

Создание рассылок проводится при настройке системы рассылки уведомлений Подсистемы мониторинга и доступно в подразделе интерфейса **«Администрирование»**

→ **«Уведомления»**, область **«Рассылки»** (см. Рисунок Б.1).

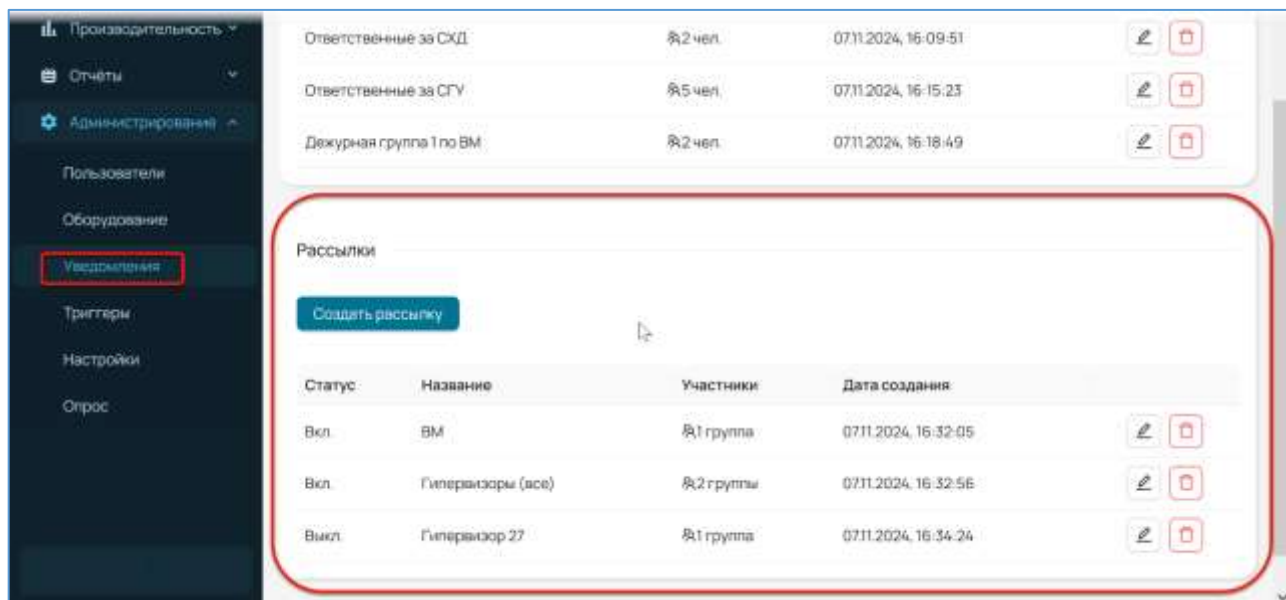


Рисунок Б.1 – Список рассылок уведомлений от Подсистемы мониторинга

При использовании функций **Создать рассылку** или значка редактирования рассылки (см. Рисунок Б.1) на экране открывается форма для создания (редактирования) группы рассылки уведомлений (см. Рисунок Б.2).

Создание рассылки

Название

Объекты

Участники

Критичность события

Предупреждение Критическая ошибка

Метод отправки

Почта

Мин. длительность

0 сек.

Активировать рассылку Уведомлять о закрытии

Вкл. Выкл.

Отмена Создать

Рисунок Б.2 – Пустая форма для создания новой рассылки

Поле **Название** – допускается ввод любых символов, кроме восклицательного знака (!)

Раскрывающийся список **Объекты** – предназначен для выбора объектов мониторинга, уведомления от которых должны входить в рассылку. Список содержит все объекты системы виртуализации «Горизонт-ВС», поставленные на мониторинг (см. Рисунок Б.3). Слева от каждого объекта расположено флаговое поле выбора.

Объекты, объединенные в группы, можно выбирать сразу всей группой, установив флажок в названии группы. Например, для включения в рассылку уведомлений от всех виртуальных машин необходимо установить флажок слева от названия группы «Виртуальные машины» (см. Рисунок Б.3). В результате все виртуальные машины будут включены как источники данной рассылки.

Выбранные элементы последовательно отображаются в поле **Объекты** (см. Рисунок Б.3).

Для того чтобы просто убрать ненужный объект из списка, нужно в поле **Объекты** щёлкнуть по значку **×** справа от названия объекта (см. Рисунок Б.3).

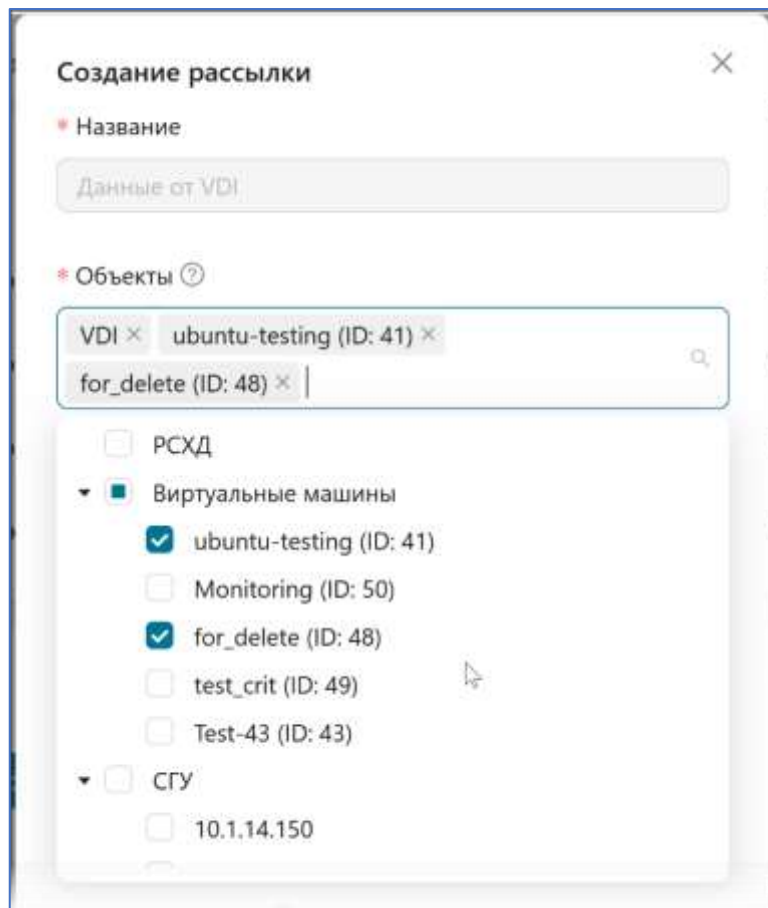


Рисунок Б.3 – Выбор объектов мониторинга, источников уведомлений в рассылке

Раскрывающийся список **Участники** – предназначен для выбора адресатов для получения уведомлений из рассылки (см. Рисунок Б.4). Список содержит:

- блок **Группы**, содержащий текущий список групп адресатов рассылок
- блок **Пользователи**, содержащий текущий список всех пользователей Подсистемы мониторинга.

Слева от каждого элемента списка расположено флаговое поле выбора. Для рассылки можно выбирать как готовые группы пользователей, так и отдельных пользователей.

Для выбора всех групп необходимо установить флажок у элемента **Группы** (см. Рисунок Б.4). В результате все группы пользователей будут включены как адресаты данной рассылки. Аналогично можно выбрать всех пользователей в блоке **Пользователи**.

Выбранные элементы последовательно отображаются в поле **Участники** (см. Рисунок Б.4).

Для того чтобы просто убрать ненужную группу или пользователя из списка, нужно в поле **Участники** щёлкнуть по значку **×** справа от названия группы или пользователя (см. Рисунок Б.4).

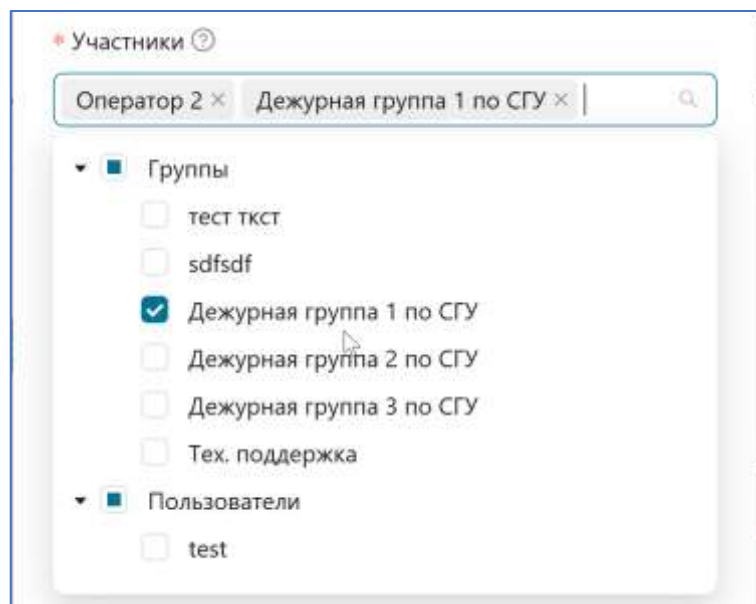


Рисунок Б.4 – Выбор адресатов рассылки

Раскрывающийся список **Критичность события** – предназначен для отбора в рассылку уведомлений по статусу события, сгенерировавшего уведомление (см. Рисунок Б.5). По умолчанию в рассылку включены уведомления о событиях со статусами **Предупреждение** и **Критическая ошибка**. Изменить набор статусов можно, выбрав в разрывающемся списке нужный статус (см. Рисунок Б.5).

Для того чтобы просто убрать статус из списка, нужно в поле **Критичность события** щёлкнуть по значку  () справа от названия ненужного статуса (см. Рисунок Б.5).

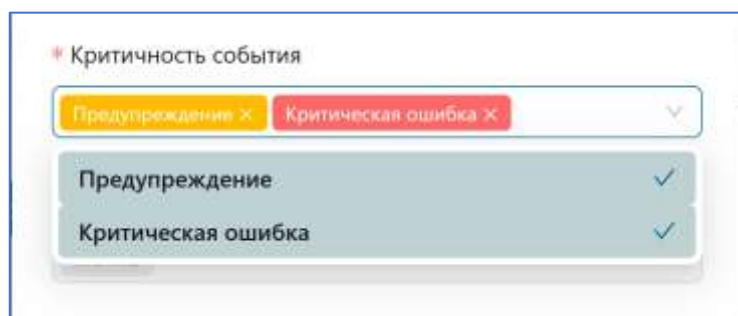


Рисунок Б.5 – Отбор уведомлений по статусу событий

Раскрывающийся список **Мин. длительность** – предназначен для установки времени задержки отправки уведомлений, входящих в рассылку (см. Рисунок Б.6). Данный параметр определяет, спустя какое время будет отправлено уведомление, если проблема на объекте мониторинга не прекратится.



Рисунок Б.6 – Выбор времени задержки отправки уведомления

Тумблер **Активировать рассылку** (см. Рисунок Б.7):

- положение **Вкл.** – рассылка действует;
- положение **Выкл.** – рассылка создана, но находится в архивном состоянии (не действует).

Данный тумблер позволяет в любой момент отключить действующую рассылку или активировать архивную.

Тумблер **Уведомлять о закрытии**:

- положение **Вкл.** – пользователям приходит уведомление о закрытии рассылки, на которую они подписаны;
- положение **Выкл.** – пользователям не приходит уведомление о закрытии рассылки, на которую они подписаны.

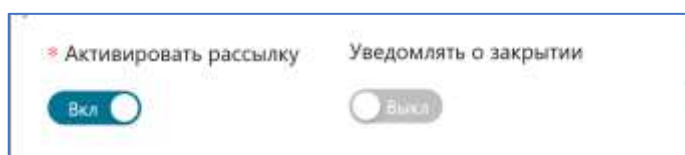


Рисунок Б.7 – Функции активации рассылки и включения уведомлений о закрытии

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. VM 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	VM работает (этот этап включает в себя этапы загрузки и включения внутренней виртуальной машины). В этом состоянии драйвер виртуализации будет периодически отслеживать ее.
Migrate	VM 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 <code>onevm recover --recreate</code>
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 <code>onevm show</code>

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:

$$\text{sig} = \text{md5}(\text{uid} + \text{params} + \text{private\_key})$$

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:

$$\text{sig} = \text{md5}(\text{params} + \text{secret\_key})$$

В данном приложении описываются XML-RPC методы,

использующиеся СГУ. Каждое описание состоит из 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/AD MIN>
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
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	Only 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:<MANAG E ADMIN> /
Enable disable	one.datastore.enable	DATASTORE:MANAGE
list	one.datastorepool.inf o	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 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

[illegible]