УТВЕРЖДЕН

RU.УГСФ.00005-01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС «ИРИДИУМ».
ПРОГРАММНЫЙ КОМПЛЕКС «ИРИДИУМ-VDI»

RU.УГСФ.00005-01 90 01

Руководство администратора

Листов 215

2026

СОДЕРЖАНИЕ

АННОТАЦИЯ

Программный комплекс «ИРИДИУМ-VDI» RU.УГСФ.00005-01 90 01 (далее – «ИРИДИУМ-VDI» или изделие) предназначено для организации инфраструктуры виртуальных рабочих столов VDI (Virtual Desktop Infrastructure).

Руководство администратора программного обеспечения VDI содержит описание функций, возможностей и порядка администрирования программного обеспечения виртуальной инфраструктуры рабочих мест (VDI). Руководство предназначено для системных администраторов и специалистов по эксплуатации, обеспечивающих установку, настройку, управление и сопровождение комплекса.

Разработчик «ИРИДИУМ-VDI» осуществляет техническую поддержку, в том числе выпуск обновлений безопасности и своевременное устранение выявленных уязвимостей, в течении всего жизненного цикла системы.

1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1 Назначение программы

Программное обеспечение ИРИДИУМ-VDI предназначено для организации инфраструктуры виртуальных рабочих столов VDI (Virtual Desktop Infrastructure).

1.2 Функции программы

ИРИДИУМ-VDI обеспечивает следующие функциональные возможности:

1) Ролевая модель доступа к панели управления
2) Интеграция со службой каталогов LDAP через SSL (LDAPS). Добавление доменов аутентификации.
3) Настройка блокирования администратора по неуспешным попыткам авторизации
4) Поддержка различных поставщиков ресурсов (сред виртуализаций)
5) Добавление параметров гостевой ОС (Windows, Linux) с последующим вводом в домен
6) Поддержка различных протоколов доставки (RDP, SPICE)
7) Поддержка протокола LoudPlay (протокола доставки рабочего стола СПЕКТР)
8) Возможность создания сессионного (гостевого) пула рабочих столов
9) Возможность создания статического (персонализированного) пула рабочих столов
10) Возможность управления питанием виртуальных рабочих столов
11) Обновление шаблона виртуальных рабочих столов в сессионном пуле
12) Ограничение на прямое подключение к виртуальному рабочему столу
13) Установка запрета на авторизацию с устройства доступа пользователя
14) Возможность принудительного закрытия активных сессий (отключение пользователей)
15) Отправка пользователям информационного сообщения
16) Делегирование прав на управление пулом виртуальных машин

17) Наличие полного комплекта эксплуатационной документации

18) Отказоустойчивость и горизонтальное масштабирование. Возможность построения кластеров с балансировкой нагрузки

19) Мониторинг состояния компонентов системы

20) Логирование и аудит действий администраторов и пользователей системы

21) Просмотр журналов регистрации событий

22) Создание отчетов

23) Возможность установки запрета многократного запуска Клиента

24) Одновременное подключение к нескольким виртуальным рабочим столам

25) Изменение пароля пользователя через Клиент

26) Сбор и отправка диагностических логов с клиентского устройства

27) Сквозной проброс USB устройств (в т.ч. смарт-карт, токенов, веб камеры, МФУ) на удаленный рабочий стол, с возможностью выбора целевых USB-портов для проброса (пробрасывать не все, а выборочно).

28) Проброс устройств передачи и воспроизведения звука на удаленный рабочий стол

29) Проброс (перенаправление) каталога с пользовательской рабочей станции на удаленный рабочий стол

30) Поддержка буфера обмена между рабочей станцией и удаленным рабочим столом

31) Поддержка нескольких мониторов

32) Поддержка vGPU (работа с графикой)

33) Возможность настройки масштабирования

34) Возможность «горячего» подключения клавиатуры и мыши (для тонких клиентов)

35) Поддержка работы ПО для унифицированных коммуникаций (UCS) для организации аудио/видео конференций, чатов, демонстрации экрана рабочего стола/приложений и других возможностей UCS.

36) Поддержка русского и английского языка в интерфейсе изделия.

37) Реализацию следующих требований безопасности:

- Требования к идентификации и аутентификации пользователей
- Требования к управлению идентификаторами и средствами аутентификации
- Требования к защите обратной связи при вводе аутентификационной информации
- Требования к управлению учетными записями пользователей
- Требования к ролевому управлению и правам доступа пользователей и групп
- Требования к ограничению неуспешных попыток доступа к Изделию
- Требования к блокированию сеанса пользователя при бездействии
- Требования к регистрации действий пользователей (событий безопасности), подлежащих регистрации
- Требования к доступу пользователей к терминальным серверам
- Требования к доступу пользователей к BPM
- Требования к управлению терминальными серверами и приложениями

1.3 Минимальный состав технических средств

Для выполнения VDI необходима ПЭВМ, подключенная к локальной вычислительной сети (ЛВС), в конфигурации:

- процессор класса x86;
- оперативная память не менее 2 Гбайт;
- жесткий диск не менее 100 Мбайт;
- наличие USB не ниже v2.0 (при работе с токенами);
- монитор, клавиатура, мышь;
- сетевой адаптер, обеспечивающий взаимодействие по ЛВС в соответствии с протоколом TCP/IP.

В случае недоступности сервера лицензирования изделие поддерживает работу 14 дней без ограничения функционала.

1.4 Требования к пользователю

Системный программист должен обладать практическими навыками работы с пользовательским интерфейсом операционной системы, установленной на компьютере.

1.5 Структура программы

1.6 Сведения о структуре программы

Общая схема функционирования VDI представлена на рисунке 1.

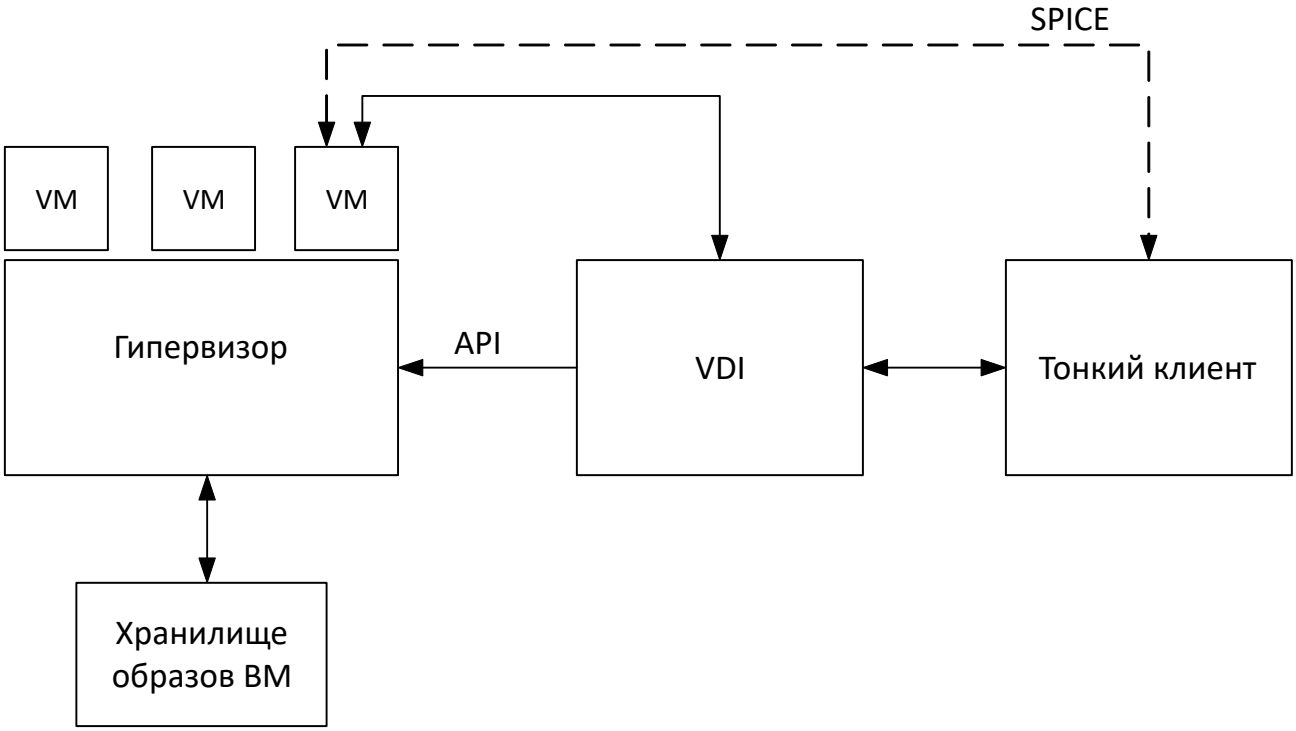


Рисунок 1 – Структура VDI инфраструктуры

1.7 Архитектура платформы с VDI инфраструктурой

Основными элементами, составляющими архитектуру с VDI, являются:

1. **Клиенты подключения** — устройства, с которых пользователи работают с виртуальными рабочими столами и приложениями:
   - тонкие клиенты;
   - нулевые клиенты;
   - персональные компьютеры;
   - мобильные устройства.

2. **Сервер VDI** — центральный узел системы. Он обеспечивает:
   - хранение информации о среде (база данных);
   - управление жизненным циклом виртуальных рабочих мест (брокер подключений);
   - взаимодействие с гипервизорами и внешними сервисами.
3. **Службы аутентификации** — отвечают за управление доступом пользователей. Поддерживаются Microsoft Active Directory, OpenLDAP, eDirectory и другие решения. В системе может применяться один или несколько аутентификаторов.
4. **Поставщики услуг**:
   - **Платформа гипервизора** — выполняет создание, запуск и удаление виртуальных рабочих мест по командам брокера. Поддерживаются: ПК «Иридиум», VMware vSphere, KVM (oVirt, RHEV, Proxmox, OpenStack, ПК «Звезда»).
   - **RDS-приложения** — позволяют публиковать и запускать приложения Windows в среде VDI.
5. **Подсистема хранения** — хранит:
   1. образы виртуальных рабочих мест;
   2. приложения;
   3. вспомогательные сервисы платформы.

При выборе хранилища необходимо учитывать требования к производительности и надежности, исходя из количества пользователей и характера нагрузки.

1.8 Компоненты VDI инфраструктуры

VDI состоит из трех элементов, взаимодействующих друг с другом.

- VDI брокер: устанавливается как Docker-контейнер.

– VDI актор: устанавливается как служба в виртуальной машине, которая будет использоваться в качестве шаблона для развертывания групп рабочих столов и на серверах приложений RDS для предоставления виртуализированных приложений.

– VDI клиент: устанавливается на клиентский компьютер для подключения к службам рабочего стола.

1.8.1 Сервер VDI

Требования к инфраструктуре, необходимые для развертывания VDI:

– Платформа виртуализации. Она будет отвечать за размещение серверов VDI, созданных виртуальных рабочих столов и серверов приложений. В состав ПК «Иридиум» входит защищенная платформа виртуализации – средство виртуализации «Звезда» RU.КНРШ.00014-01 (сертификат соответствия ФСТЭК России № 4934 от 05.05.2025).

– Имя пользователя и пароль менеджера платформы виртуализации с правами администратора.

– DNS-сервер. Эта служба необходима как для правильной работы виртуальной платформы, так и для развертывания среды виртуальной платформы VDI.

– DHCP-сервер. DHCP-сервер, позволяющий назначать IP-адреса группам виртуальных рабочих столов, созданным VDI.

Требования к сети

Для настройки сети VDI необходимо иметь в наличии:

– Маска сети;

– IP-адрес DNS-сервера;

– IP-адрес шлюза;

– Доменное имя (если таковое имеется);

– IP-адрес менеджера платформы виртуализации.

1.8.2 VDI Актор

VDI-Актор — это программный компонент, обеспечивающий взаимодействие между VDI-Сервером и виртуальными рабочими столами или службами удалённых приложений. Он выполняет функции:

– передачи служебной информации (состояние виртуального рабочего стола, имя машины и др.);
– управления процессом связи между VDI-Сервером и рабочими столами/сессиями;
– интеграции со службами удалённых рабочих столов (RDS) для предоставления виртуализированных приложений и сессий.

Актор устанавливается как служба на:

– шаблонных виртуальных машинах, используемых для создания пулов виртуальных рабочих столов на основе связанных клонов;
– серверах RDS, обеспечивающих виртуализированные приложения и удалённые сессии.

Требования:

– .Net Framework 3.5 SP1 (Windows машин);
– Python 3.6 (Linux машины);
– Доступ до IP VDI сервера.

1.8.3 Клиент VDI

Клиент VDI — это программное обеспечение, обеспечивающее подключение пользователей к виртуальным рабочим столам и приложениям с использованием поддерживаемых протоколов удалённого доступа.

Программа устанавливается на пользовательские устройства, с которых осуществляется доступ к службам виртуальных рабочих столов.

Поддерживаемые операционные системы:

– Windows: Windows 11, Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2.

– Linux: ОС Альт, Astra Linux (Смоленск), Debian, Ubuntu, CentOS, Fedora, OpenSUSE и др.

– macOS: начиная с версии 10.5.

– Android.

1.9 Сведения о связях с другими программами

Программное обеспечение VDI взаимодействует с гипервизором и с программным обеспечение тонкого клиента.

Необходимо включить следующие порты связи между различными элементами, составляющими платформу VDI (таблица 1).

Таблица 1 – Сетевые соединения

Источник	Место назначения	Порт
Сервер VDI	vCenter	443
Сервер VDI	Аутентификатор	389, 636, XXX
Сервер VDI	Виртуальные рабочие столы	3389 (RDP), 22 (NX), XXX
Сервер VDI (Actor)	Виртуальные рабочие столы	43910
Виртуальные рабочие столы	Сервер VDI (Actor)	80/443
Пользователи	Сервер VDI	80/443
Пользователи (LAN – локальная сеть)	Виртуальные рабочие столы	3389 (RDP), 22 (NX), XXX
Сервер VDI	VDI MySQL	3306
Сервер VDI	Туннель VDI	80
Туннель VDI	Сервер VDI	80
Туннель VDI	Виртуальные рабочие столы	3389(RDP), 22(NX), XXX
Пользователи	Туннель VDI	443
Пользователи	Туннель VDI (HTML5)	10443

2 УСТАНОВКА СЕРВЕРА VDI

1. В консоли платформы виртуализации перейти в директорию, где находится образ «star.vdi».
2. Загрузить образ: `docker load < star.vdi.0.0.3.tar.bz2`
3. 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
```

Рисунок 2

4. Запустить контейнер:

```
docker run -d --name=star.vdi -p 2637:2637 --restart=always -v svdi.vol:/svol
star.vdi:0.0.3
```

3 УСТАНОВКА 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 актор для каждой платформы (Windows, Linux и vApps).

Для этого необходимо:

– Подключиться к брокеру VDI через веб-браузер и использовать учетные данные пользователя с правами администратора для доступа к загрузкам (рисунки 3).

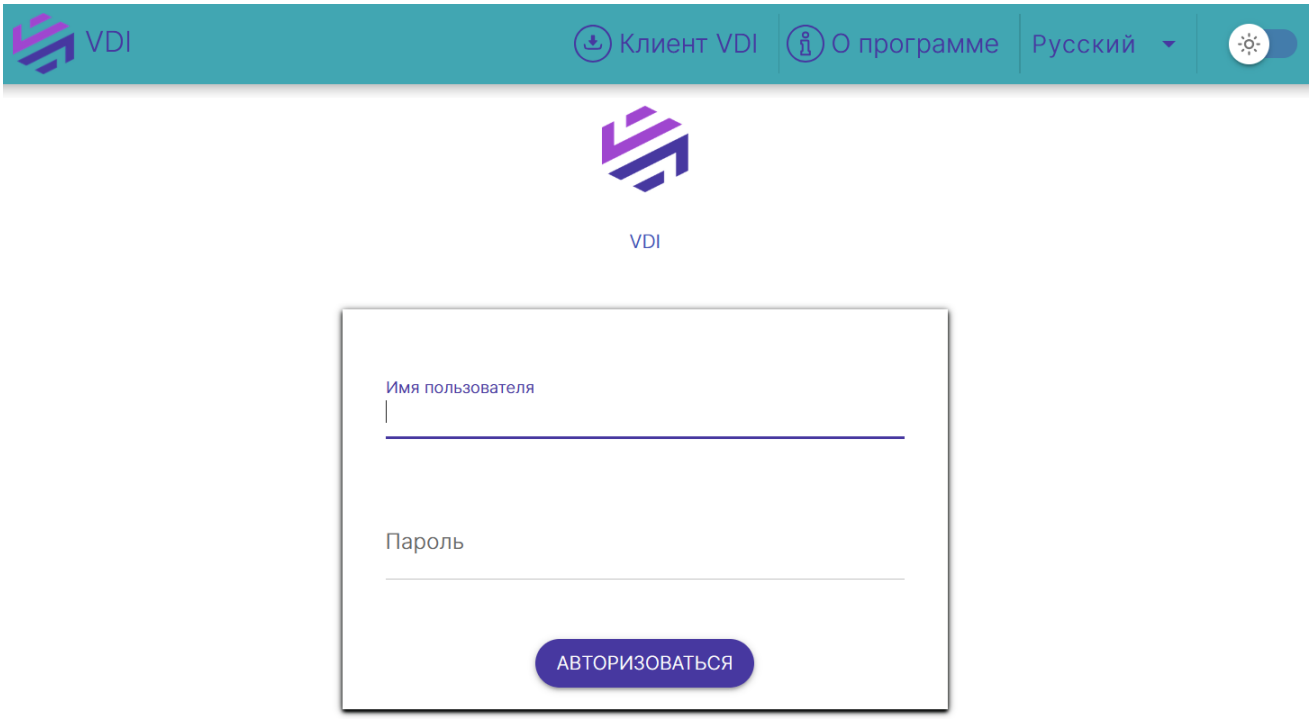


Рисунок 3

– Нажать на страницу **Загрузки**.

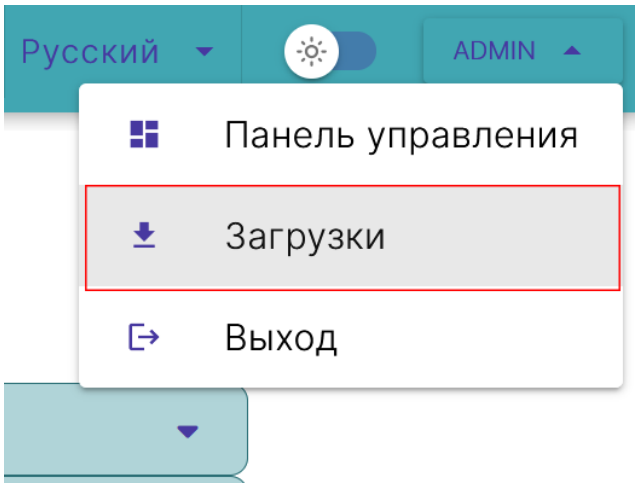


Рисунок 4

Выбрать Actor соответствующей операционной системы и службы, установленной в базовом шаблоне или сервере приложений, на котором будут развернуты службы рабочего стола (Рисунок 5):

– Альт Линукс;
– РЕД ОС;
– Windows 10/11;
– Астра Линукс.

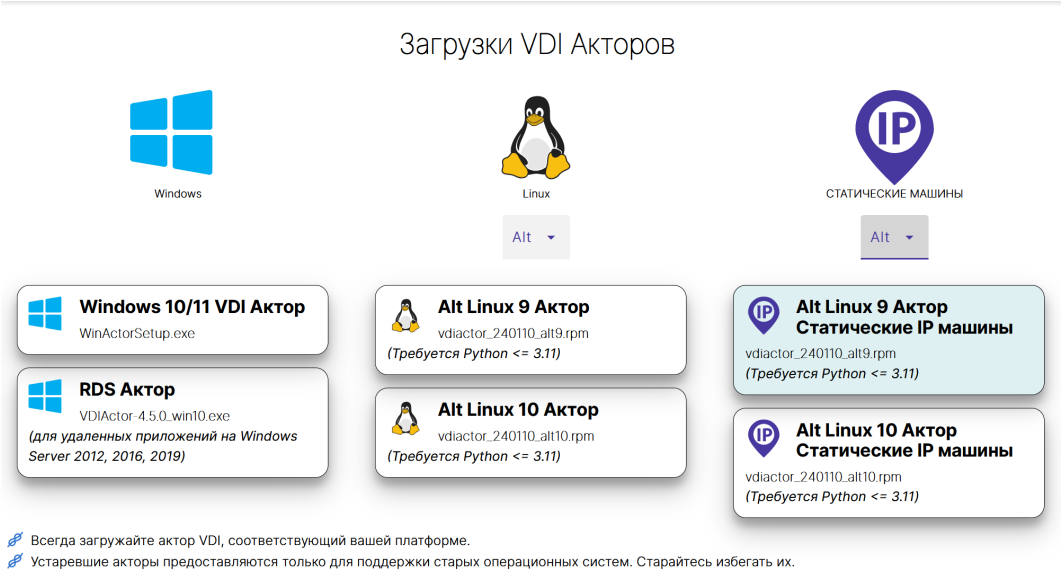


Рисунок 5

3.1.1 Автономные виртуальные рабочие столы Windows

Для управления жизненным циклом виртуальных машин Windows, самостоятельно создаваемых VDI, необходимо, чтобы на шаблонной машине, на которой они будут основаны, был установлен VDI Actor.

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:

1. Выбрать директорию, в которую необходимо установить VDI Actor (Рисунок 6).

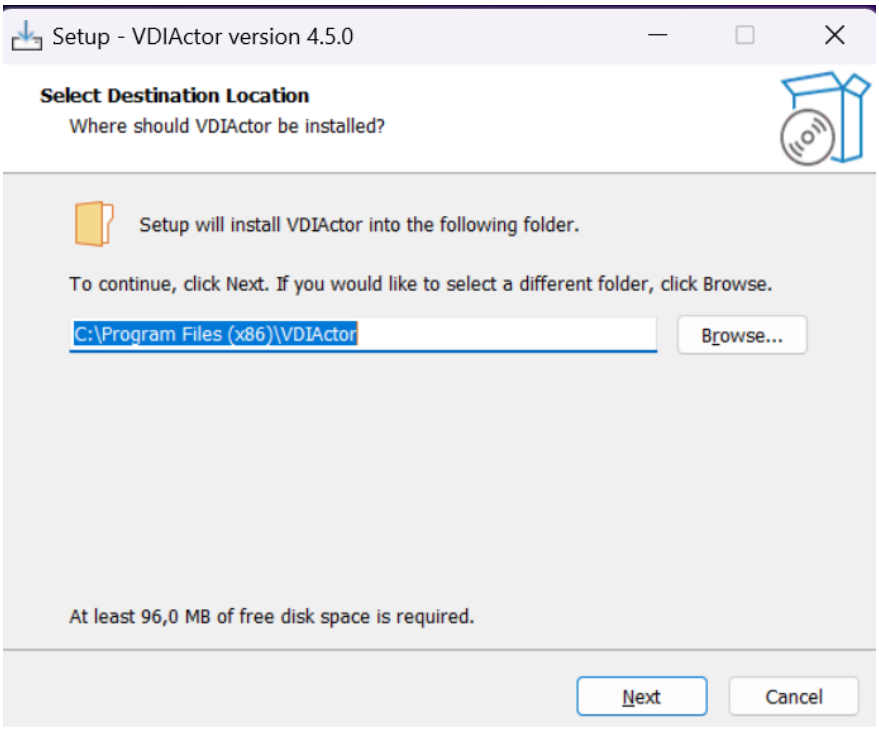


Рисунок 6

2. Указать директорию в меню «Пуск», в которой будут созданы ярлыки программы. (Рисунок 7). Для выбора папки нажать кнопку «Обзор».

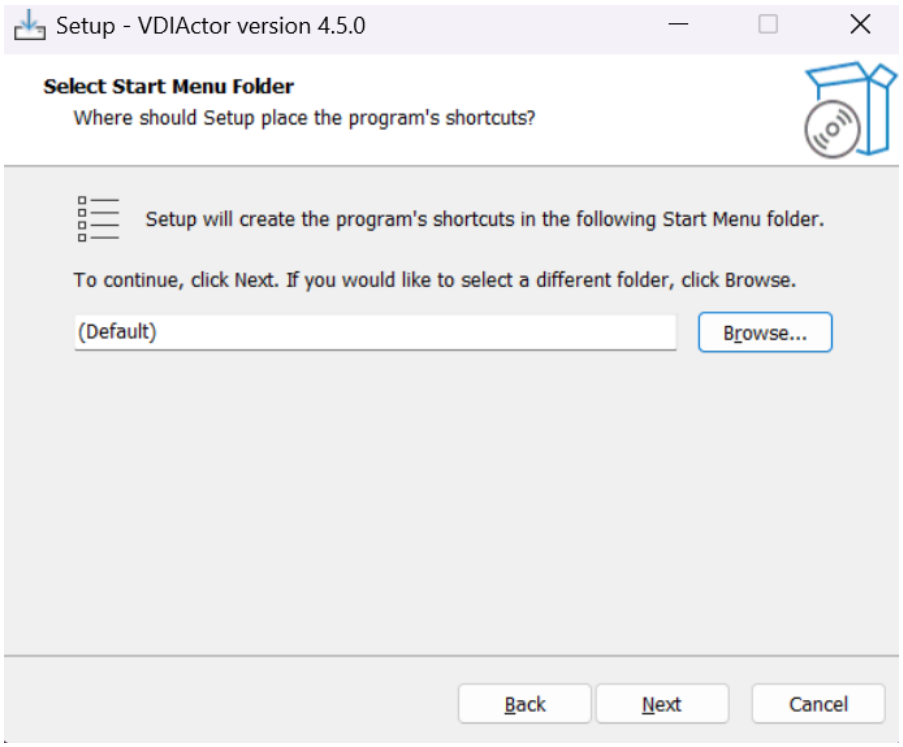


Рисунок 7

3. В следующем шаге установки доступно добавление ярлыка на рабочем столе, а также в меню быстрого доступа. (Рисунок 8).

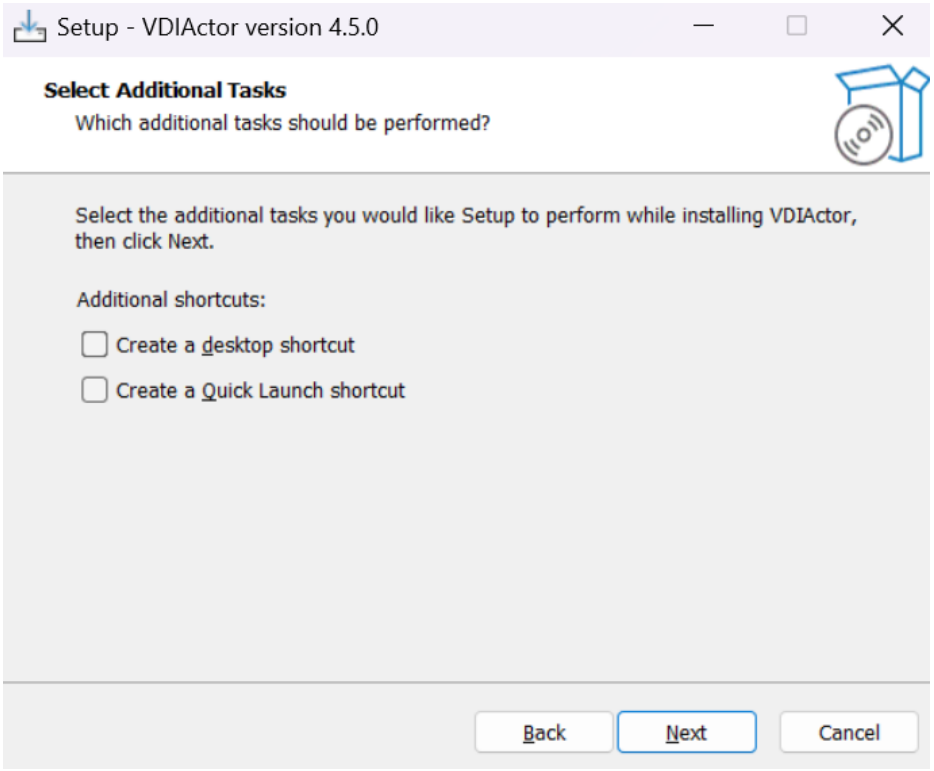


Рисунок 8

4. Далее доступен обзор параметров установки. Для продолжения нажать кнопку **Установить (**Рисунок 9**).**

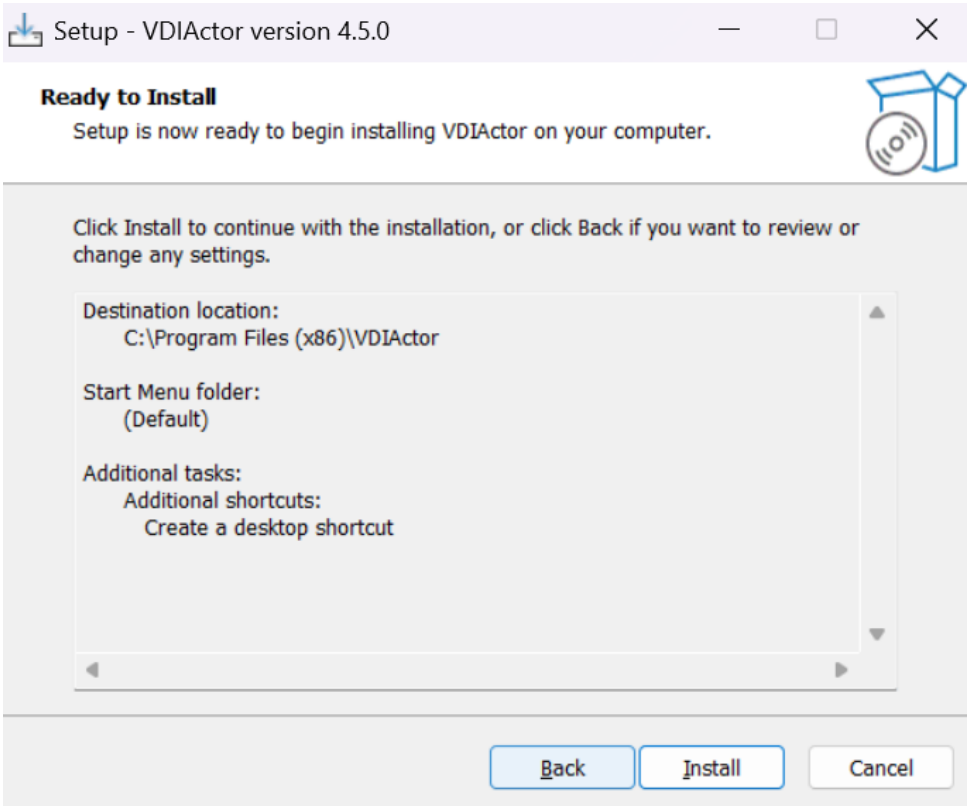


Рисунок 9

5. Установка завершена (Рисунок 10).

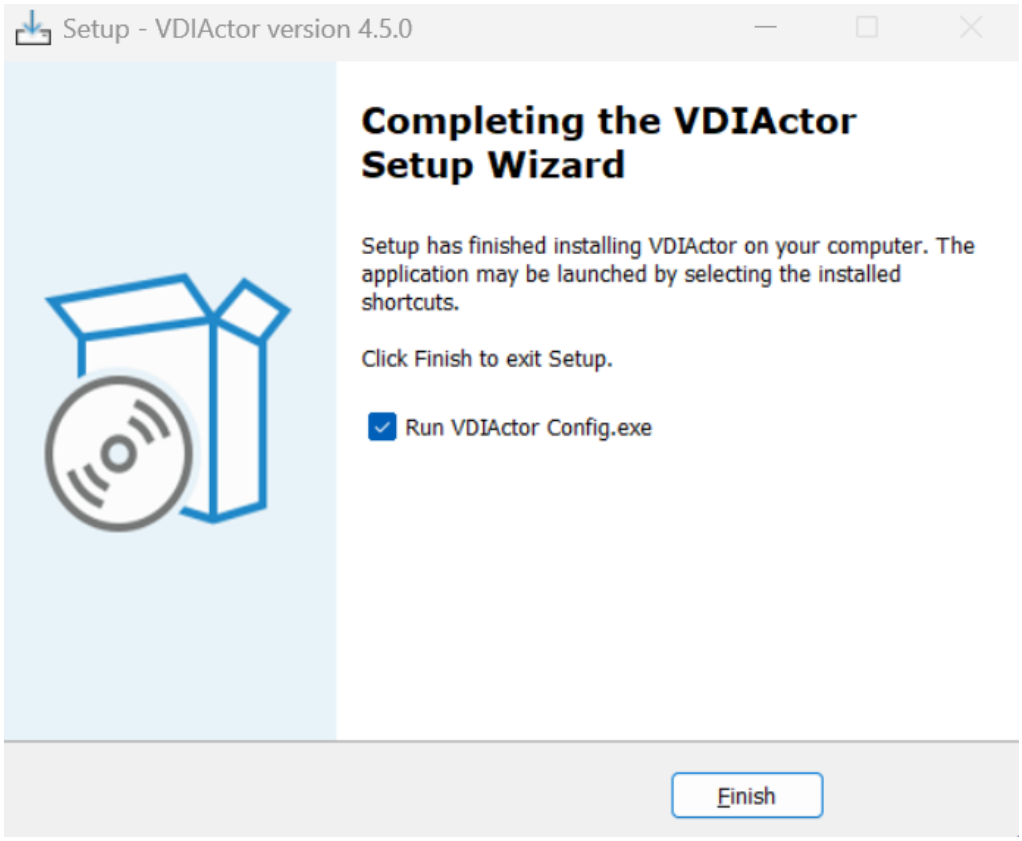


Рисунок 10

На вкладке VDI Server нужно зарегистрировать Actor в экземпляре VDI, указав следующие параметры (Рисунок 11):

1. Проверка SSL: игнорировать сертификат\верификационный сертификат
2. Сервер VDI : имя или IP-адрес VDI-сервера и порт.
3. 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).

– Имя пользователя с полномочиями администратора.
– Пароль пользователя администратора.

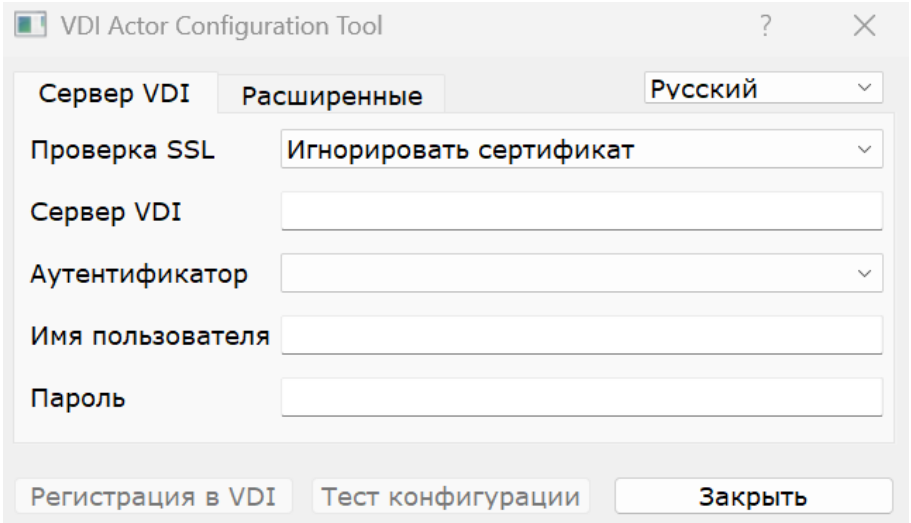


Рисунок 11

4. После ввода этих данных нажать кнопку **Регистрация в VDI** (Рисунок 12).

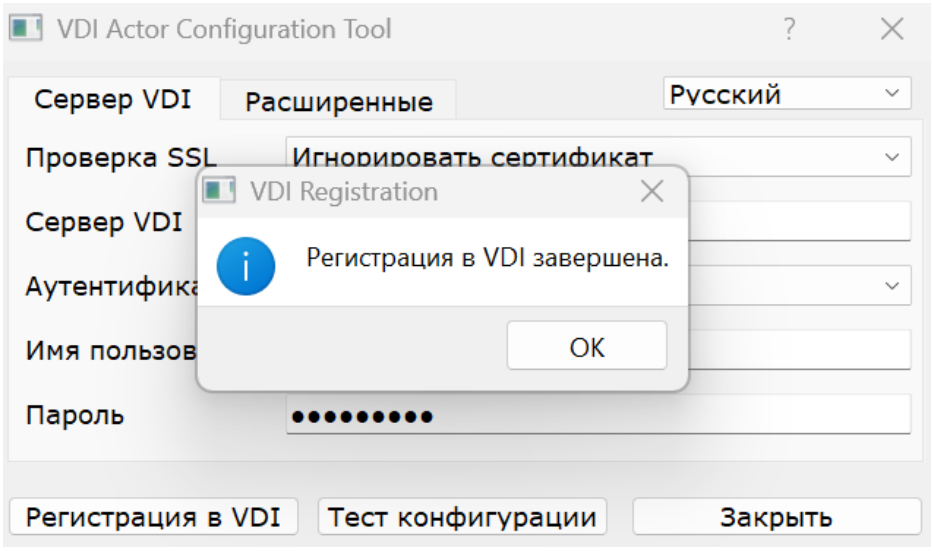


Рисунок 12

Можно выполнить тест, нажав кнопку **Тест конфигурации** для проверки правильности подключения к серверу VDI (Рисунок 13).

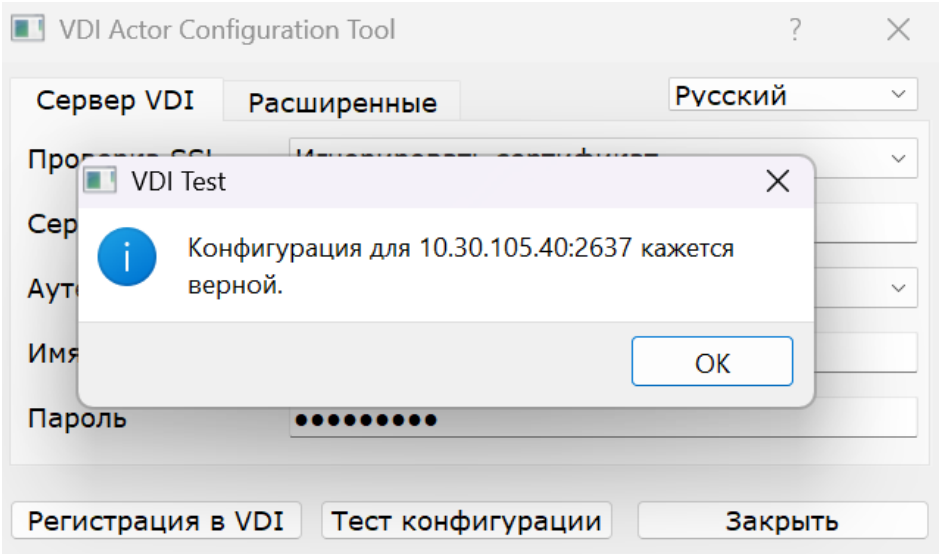


Рисунок 13

На вкладке **Расширенные** можно указать следующие дополнительные параметры (Рисунок 14).

- Предподключение: запуск сценария непосредственно перед тем, как разрешить пользователю подключение к виртуальному рабочему столу.

VDI автоматически передает следующие параметры, которые могут использоваться в сценарии:

имя пользователя, протокол (rdp, nx, pcoip…), IP (IP, распознанный на клиенте (SRC IP)), имя хоста (SRC Host).

– Запустить один раз: 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.

– Постконфигурация: 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.

– Уровень лога: 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).

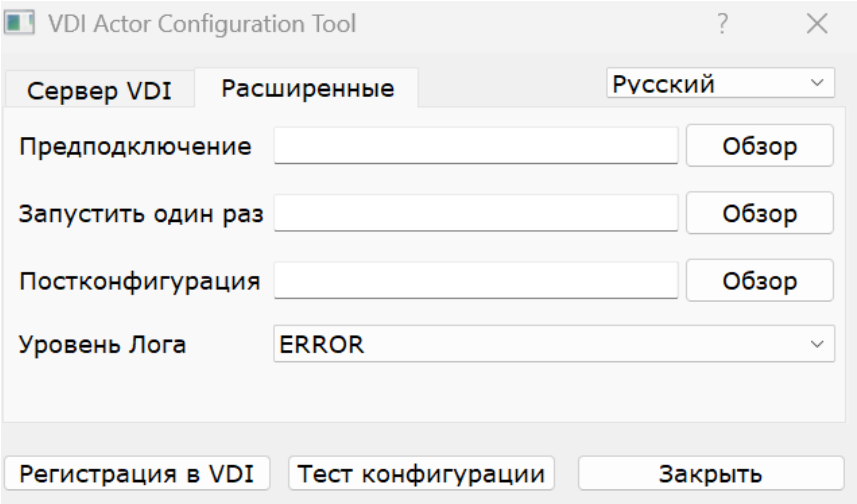


Рисунок 14

Очень важно отметить, что для применения значений вкладки **Расширенные** всегда необходимо выполнить процесс регистрации позже, так как необходимо добавить какой-либо сценарий или изменить уровень журнала, и Actor не был зарегистрирован снова, то изменения 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.).

3.1.2 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:

- vdiactor_240110_alt9.rpm - VDI Actor для Alt Linux 9 (Требуется python >= 3.6);
- vdiactor_240110_r7.3.2.rpm - VDI Actor для RedOS 7 (Требуется python >= 3.8);
- vdiactor_240110_ub22.deb - VDI Actor для Ubuntu 22 (Требуется python >= 3.7);
- vdiactor_240110_alt10.rpm - VDI Actor для Alt Linux 10 (Требуется python >= 3.8);

- vdiactor_240217_astra1.7se.deb - VDI Actor для Astra Linux 1.7 (Требуется python >= 3.7).

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:

```
sudo apt-get update
sudo apt-get install -f
sudo apt-get install vdiactor
```

После установки необходимых зависимостей запустить конфигурацию VDI Actor. На вкладке VDI Server можно зарегистрировать Actor, указав следующие параметры (Рисунок 15).

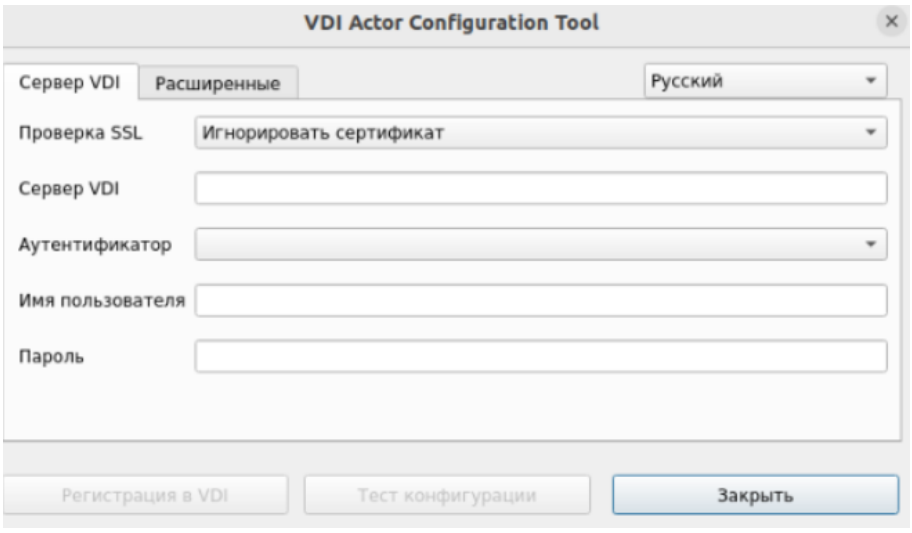


Рисунок 15

- Адрес сервера VDI: IP-адрес с указанием порта (например, 10.x.x.x:xxxx);
- Проверка SSL: выбрать вариант "Игнорировать сертификат";
- Аутентификатор: выбрать нужный тип (например, "Administration");

- Имя пользователя: указать имя учётной записи;
- Пароль: ввести соответствующий пароль.

После указания этих данных нажать кнопку «Регистрация в VDI» (Рисунок 16).

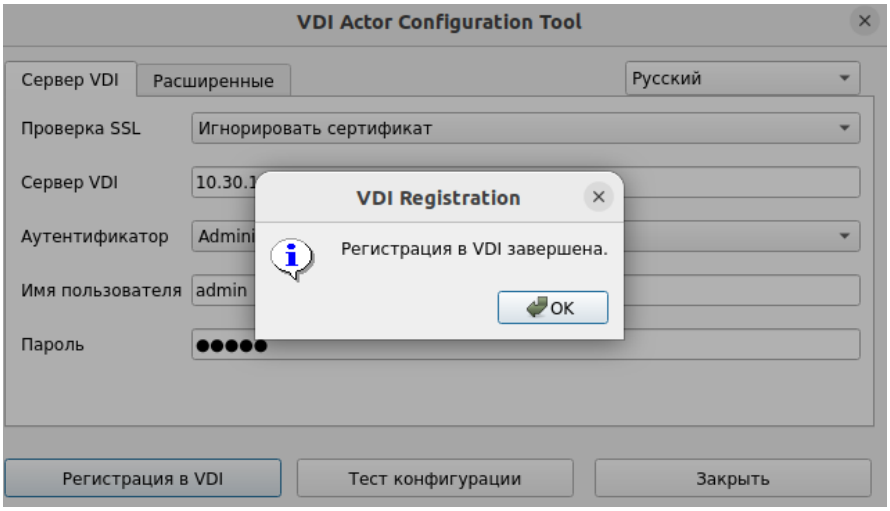


Рисунок 16

Можно выполнить тест, нажав кнопку «Тест конфигурации», чтобы проверить правильность подключения к серверу VDI (Рисунок 17).

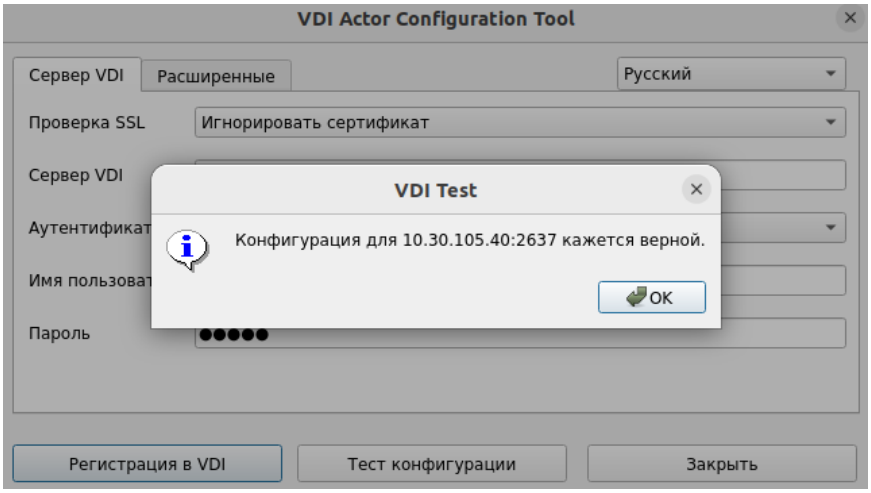


Рисунок 17

На вкладке «Расширенные» можно указать следующие дополнительные параметры (Рисунок 18).

- Предподключение: 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, pcoip…), IP (IP, распознанный на клиенте (SRC IP)), имя хоста (SRC Host).

- Запустить один раз: 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 Actor, что не позволит ему перейти в состояние «Действительно» при администрировании VDI.

- Постконфигурация: 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.

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

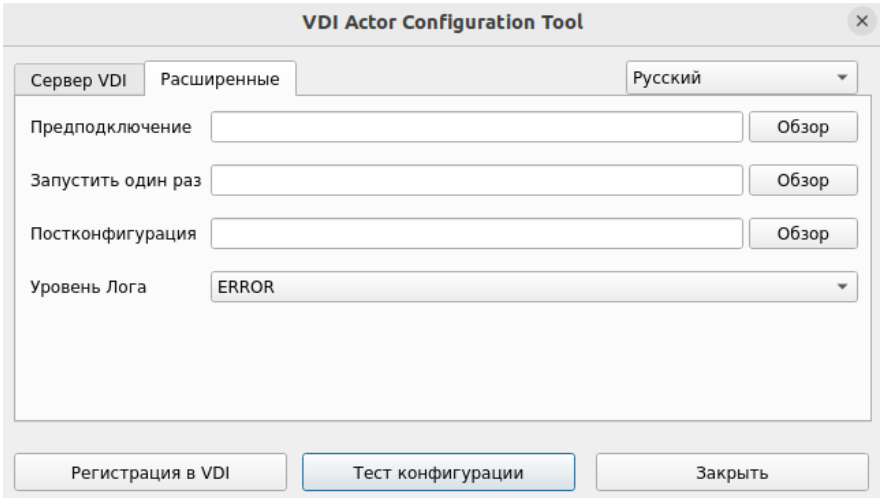


Рисунок 18

Очень важно отметить, что для применения значений вкладки **Расширенные** необходимо 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.).

4 УСТАНОВКА И НАСТРОЙКА RDS (REMOTE DESKTOP SERVICE)

Установка службы удаленных рабочих столов (RDS) осуществляется следующим образом: «Диспетчер серверов» – «Управление» – «Добавить роли и компоненты» (Рисунок 19).

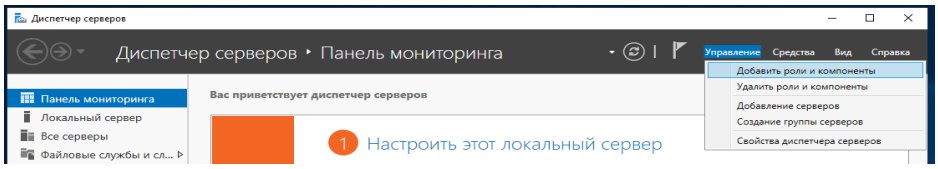


Рисунок 19

В мастере выполнить следующие действия:

1) Тип установки: «Установка служб удаленных рабочих столов» (Рисунок 20).

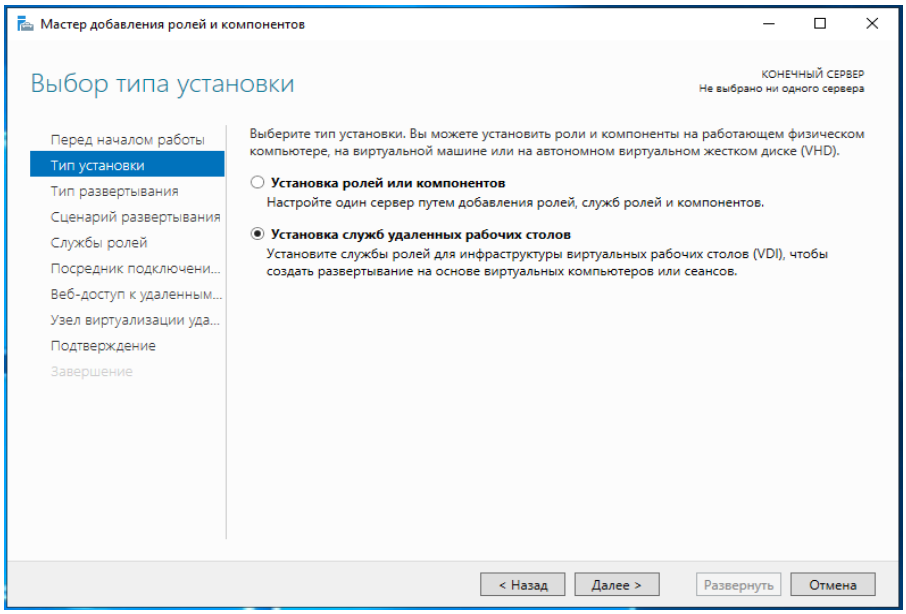


Рисунок 20

2) Тип развертывания: «Стандартное развертывание» (Рисунок 21).

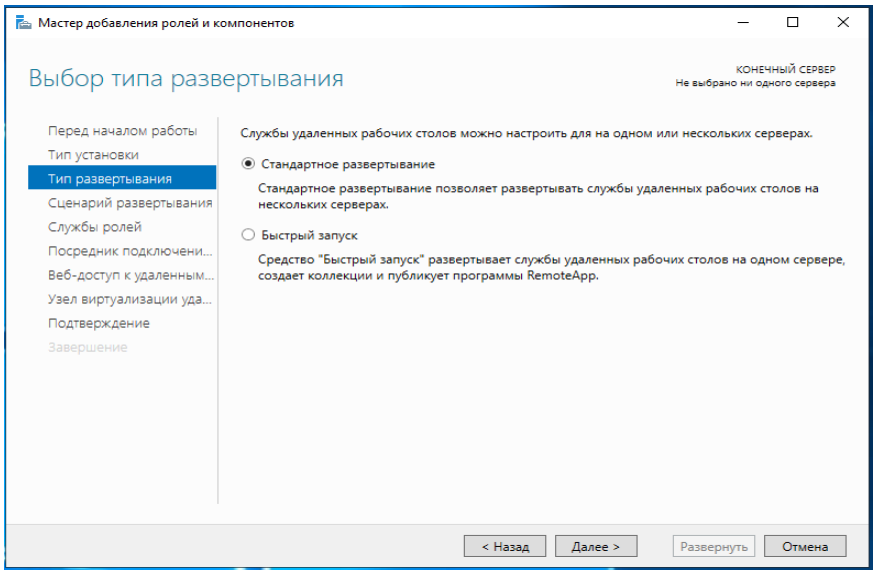


Рисунок 21

3) Сценарий развертывания: «Развертывание рабочих столов на основе сеансов» (Рисунок 22).

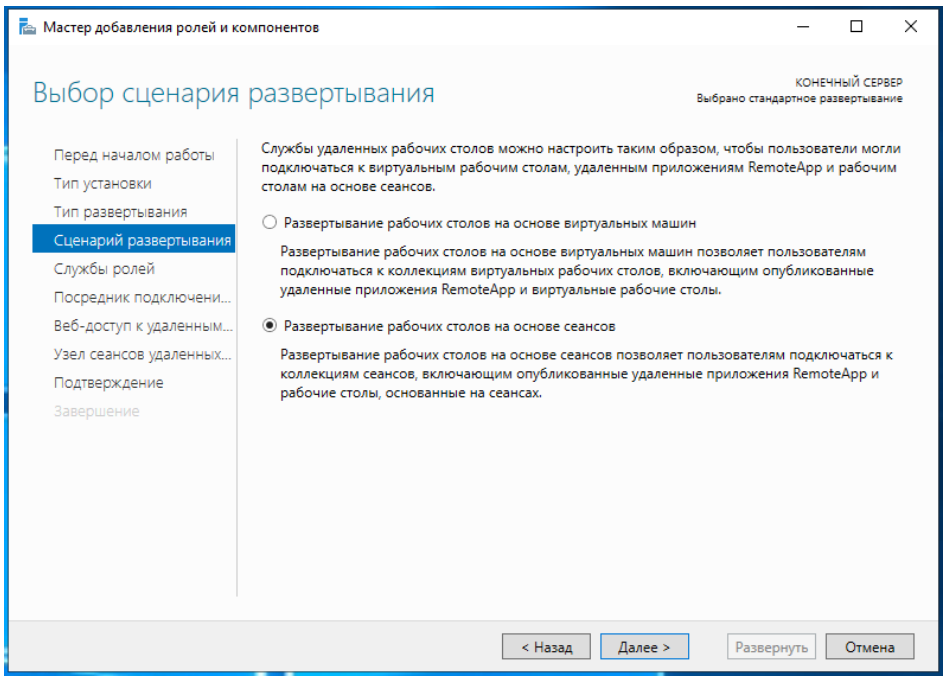


Рисунок 22

4) Появится сводная информация о том, что будет установлено (Рисунок 23)

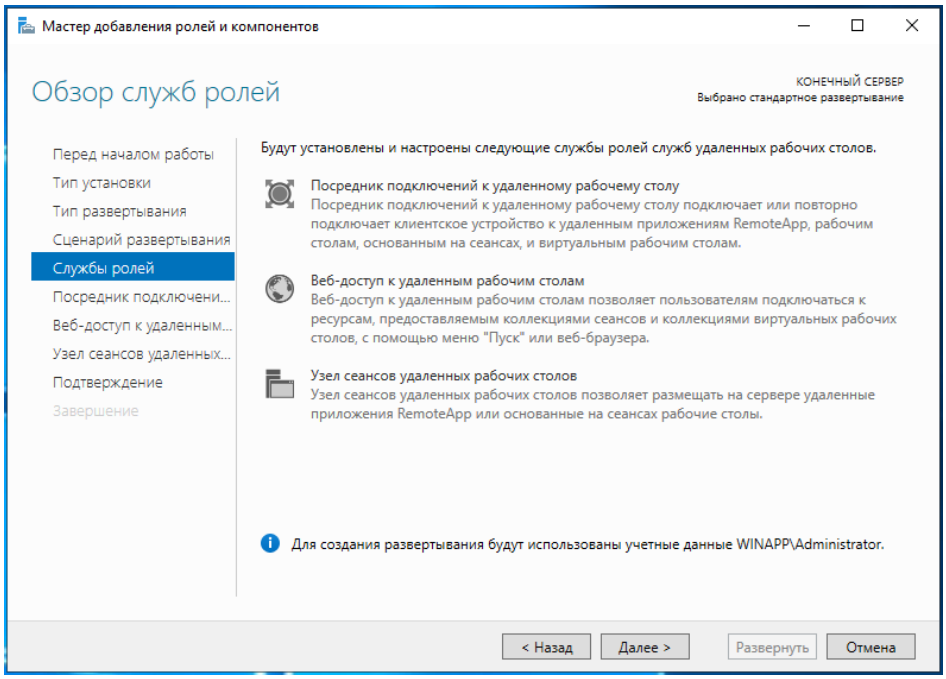


Рисунок 23

5) Должен быть указан сервер, на котором будет установлен каждый элемент (рисунки 24 - 26).

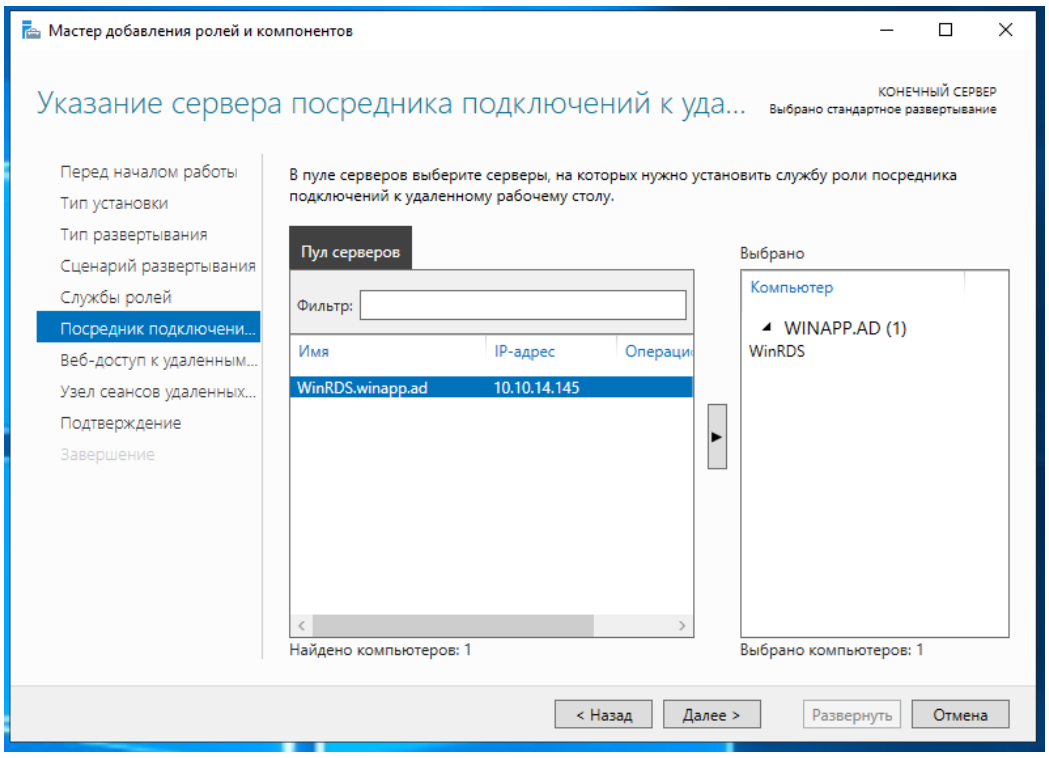


Рисунок 24

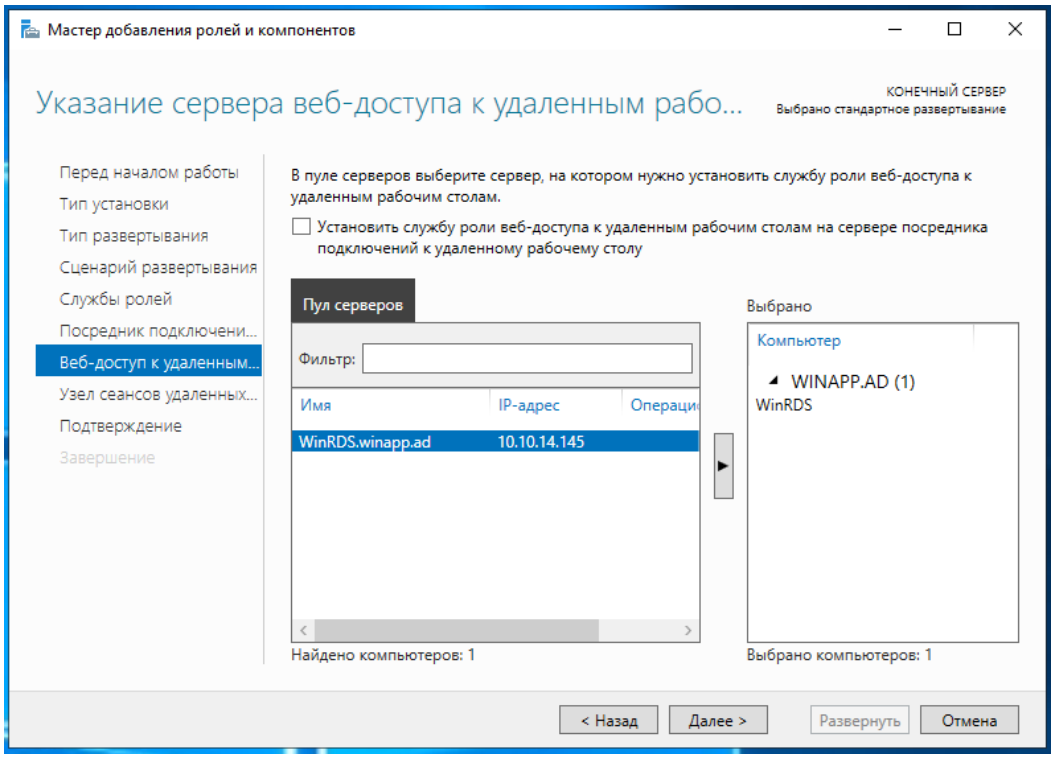


Рисунок 25

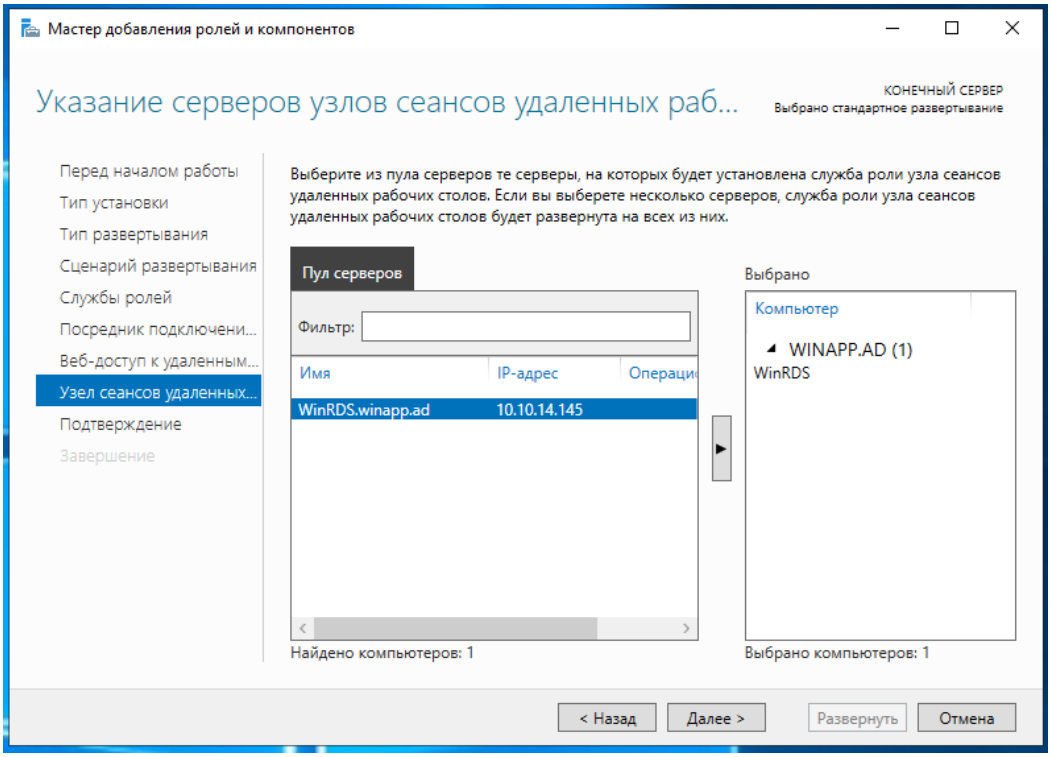


Рисунок 26

6) Установка подтверждается и выполняется ее развертывание (Рисунок 27):

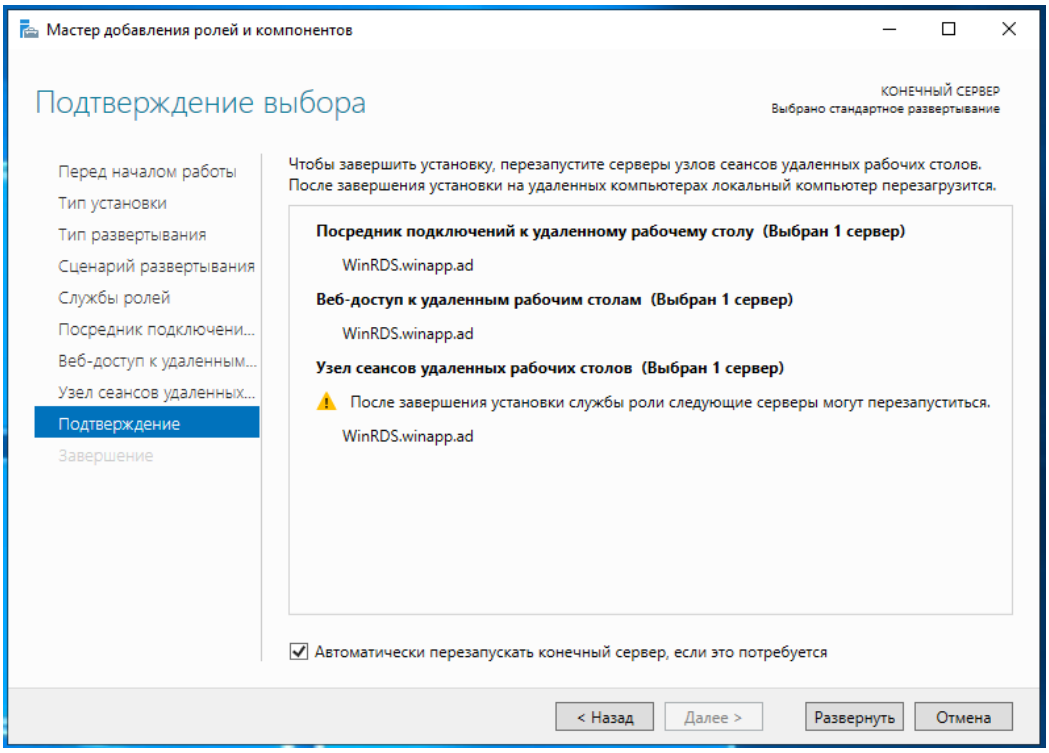


Рисунок 27

7) Сервер будет перезапущен автоматически (если вы это указали), и установка завершится (Рисунок 28).

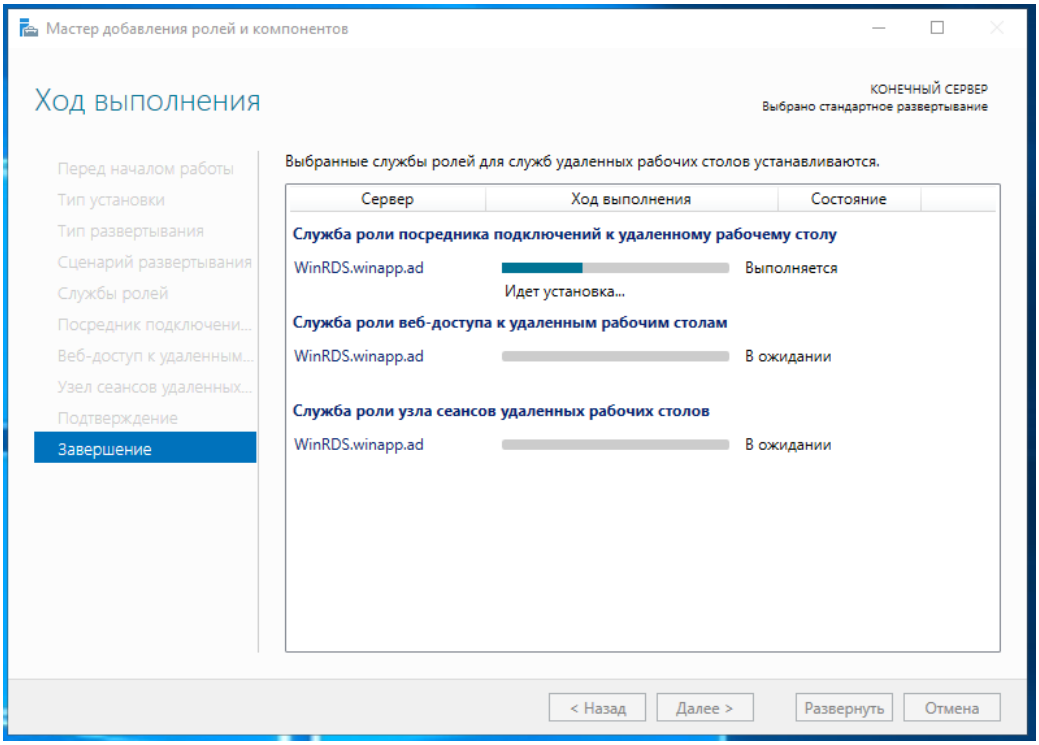


Рисунок 28

4.1.1 Настройка RDS с VDI

После установки роли RDS и перезапуска сервера продолжить создание новой коллекции RDS. Для этого выбрать «Создание коллекций сеансов» или открыть раздел «Коллекции» и выбрать «Создать коллекцию сеансов» (Рисунок 29).

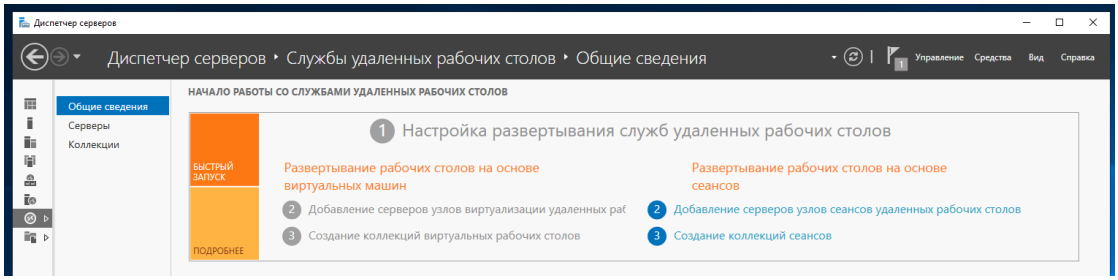


Рисунок 29

В мастере создания следует указать следующие данные. Указать имя для новой коллекции (Рисунок 30).

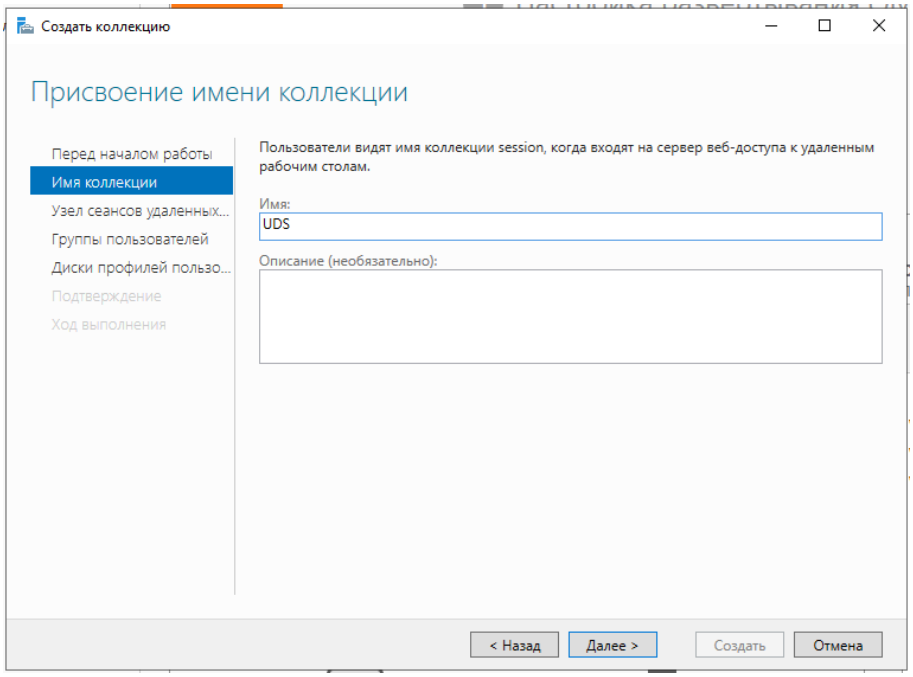


Рисунок 30

Добавить сервер в «Узел сеансов удаленных рабочих столов» (Рисунок 31):

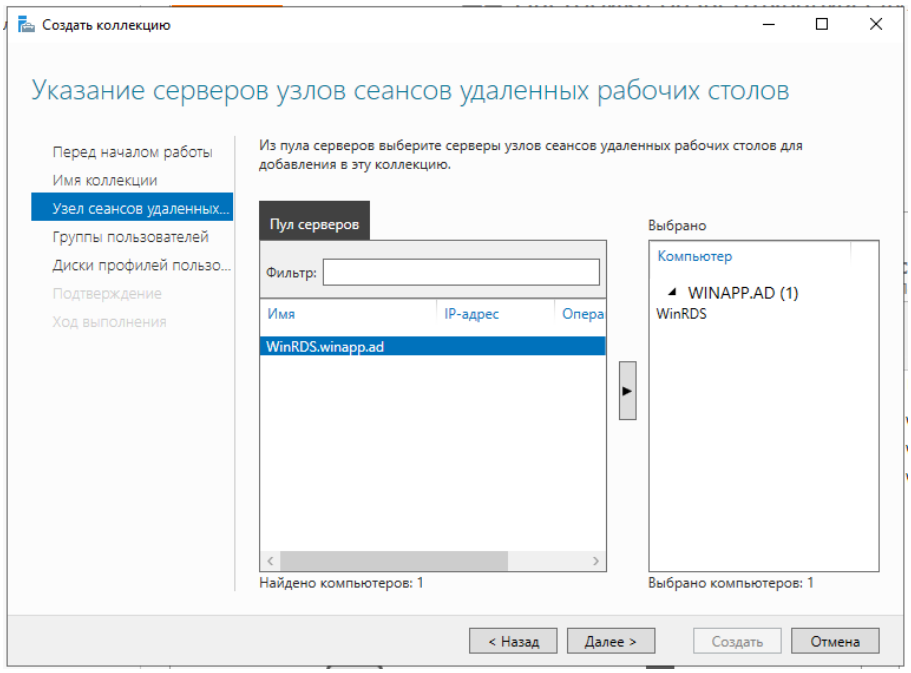


Рисунок 31

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 32).

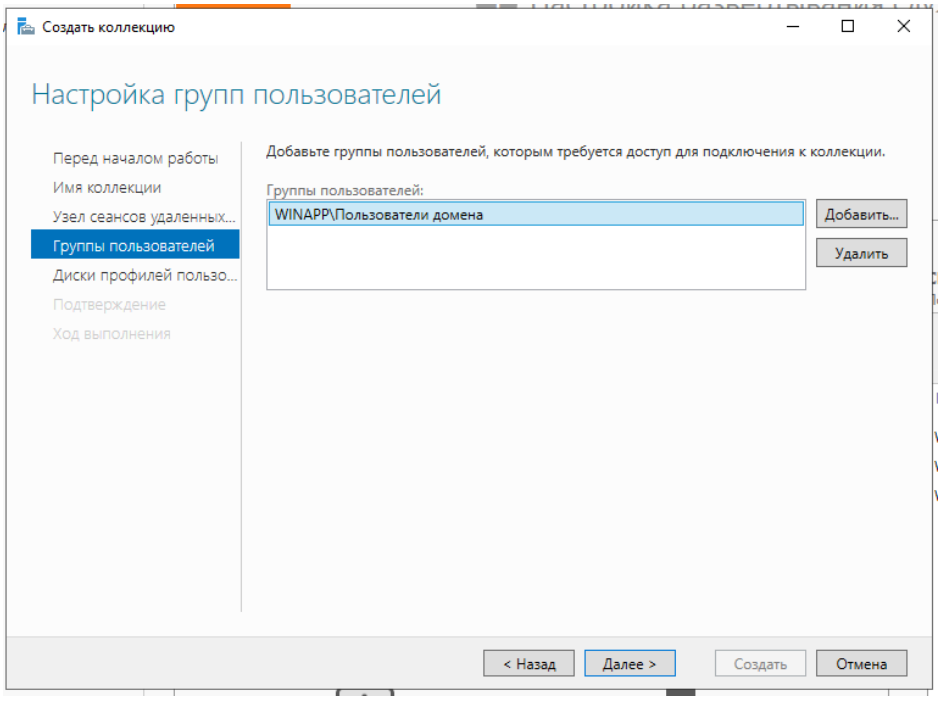


Рисунок 32

Указать, где будет храниться профиль пользователя. Если не указать, будет создан временный профиль, который будет удален при отключении пользователя (Рисунок 33).

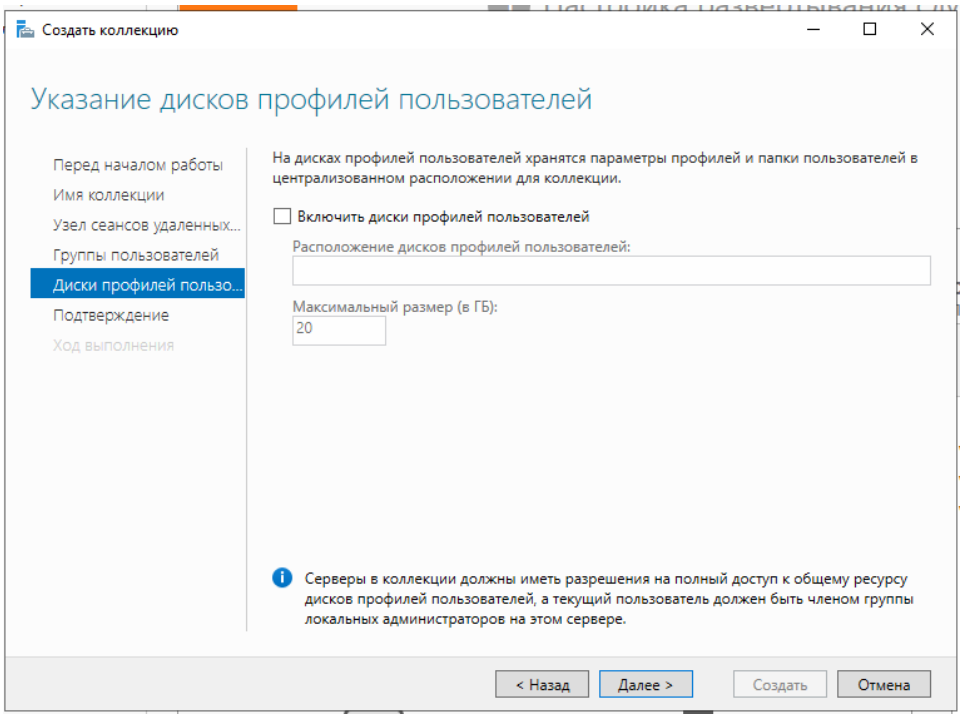
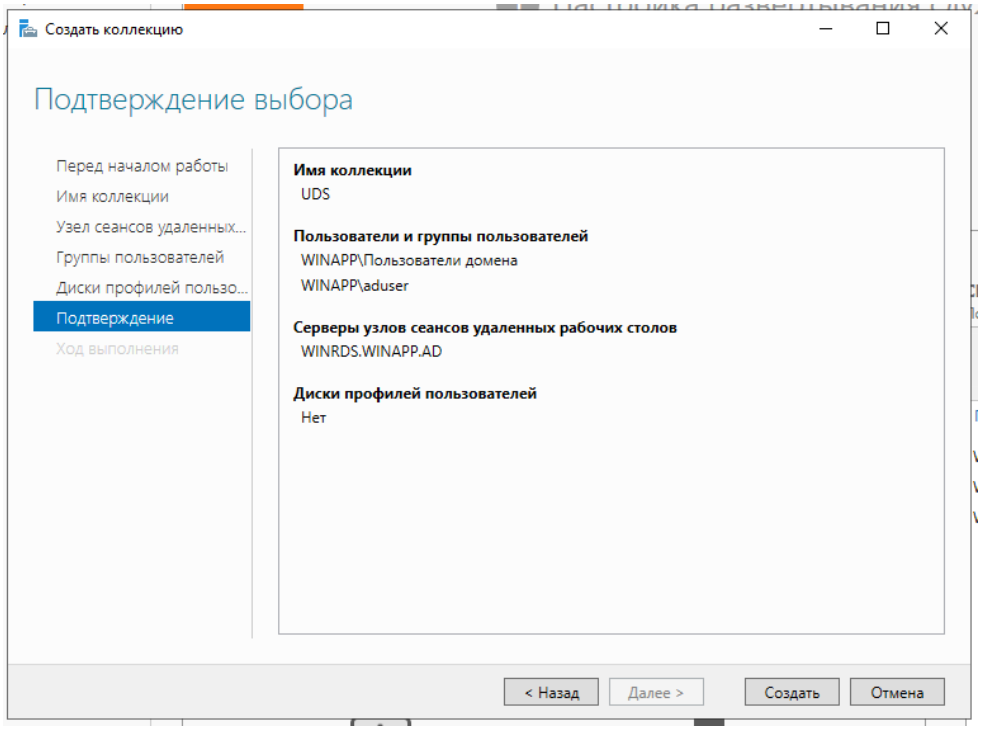


Рисунок 33

Подтвердить и создать коллекцию (Рисунок 34).



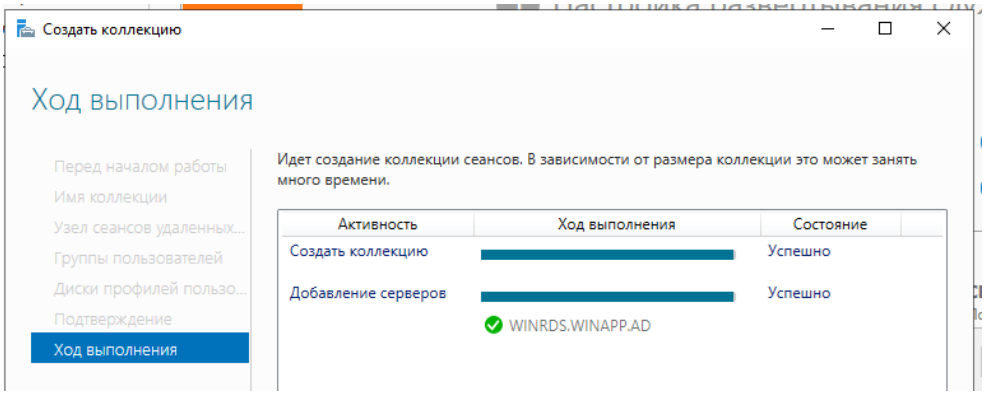


Рисунок 34

Публикация RDS Actor на RDS сервере. После создания коллекции выбрать «Опубликовать удаленные приложения RemoteApp» (Рисунок 35).

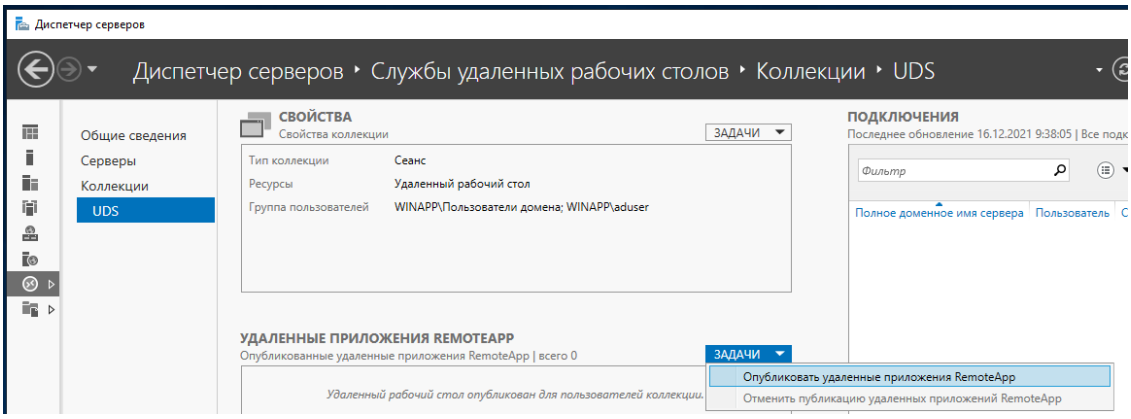


Рисунок 35

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 36):

C:\Program Files\RDSActor\RDSActor.exe

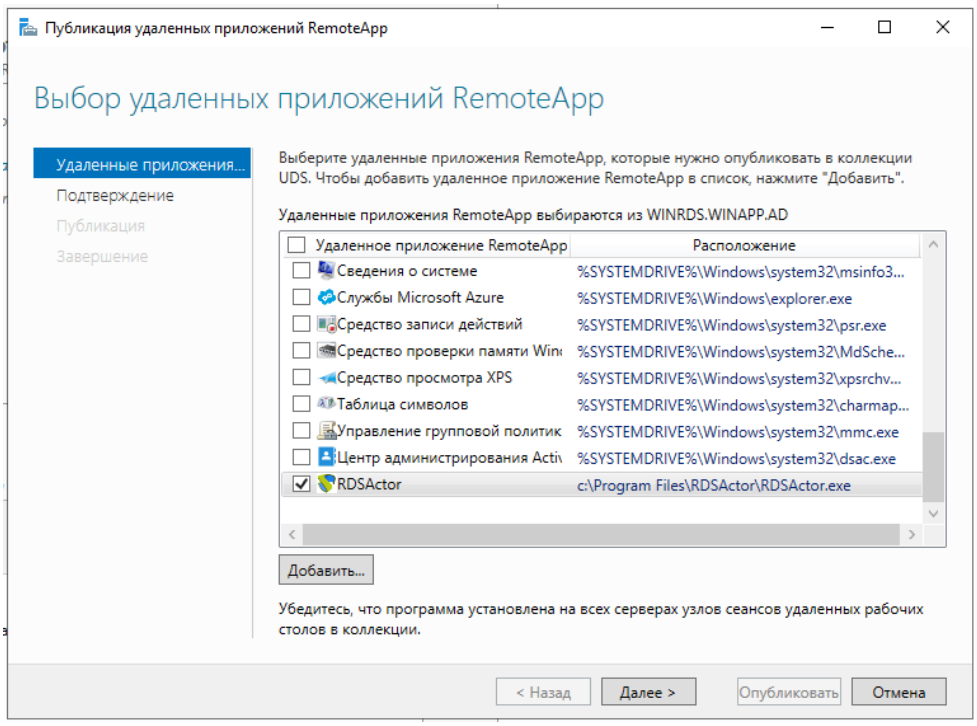


Рисунок 36

Подтвердить публикацию, нажать «Опубликовать» (Рисунок 37).

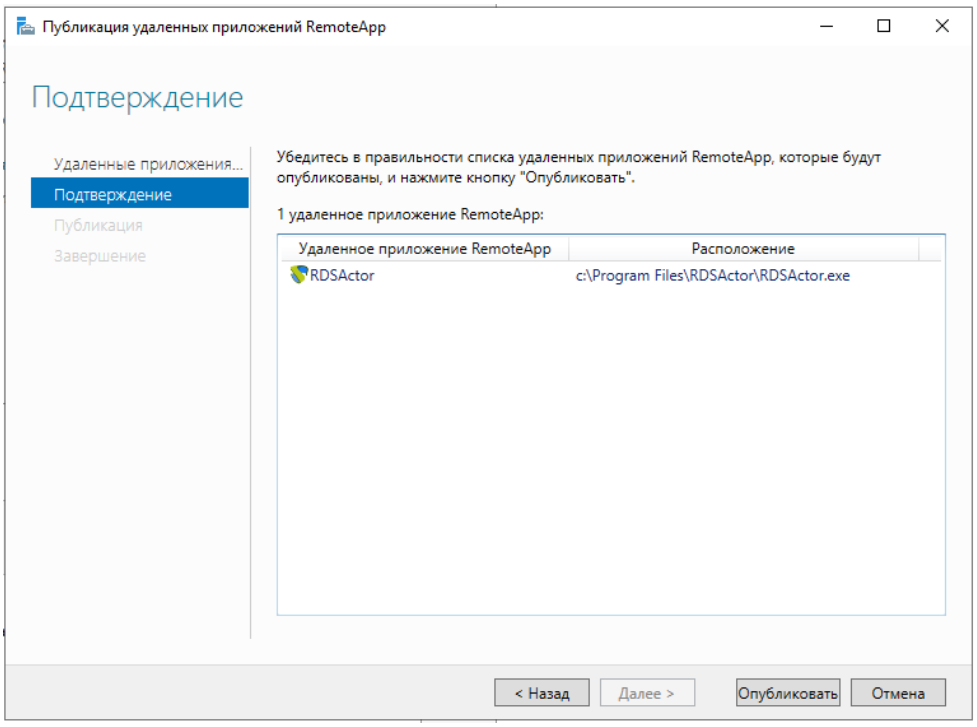


Рисунок 37

После создания отредактировать его свойства (Рисунок 38).

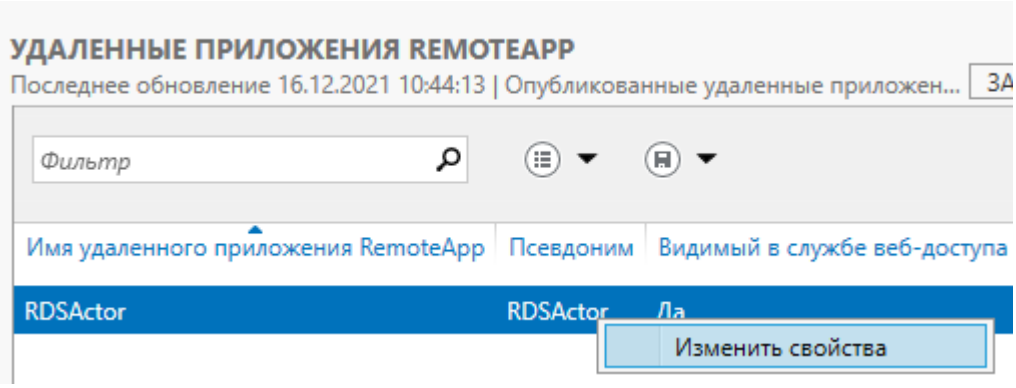


Рисунок 38

В разделе «Общие» отметить «Нет» в разделе «Показать удаленное приложение RemoteApp в веб-доступе к удаленным рабочим столам» (Рисунок 39).

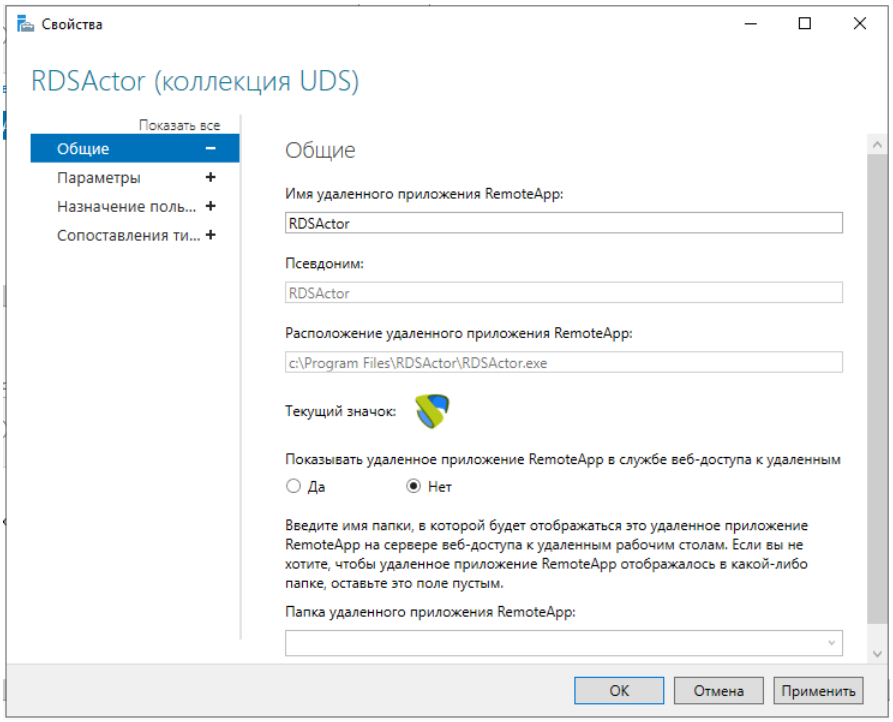


Рисунок 39

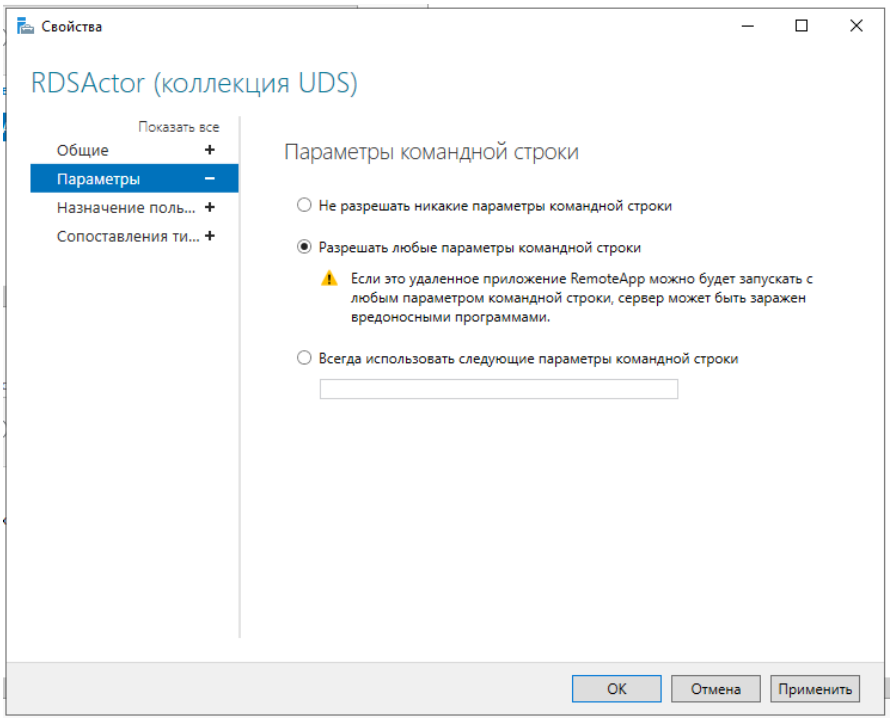


Рисунок 40

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 41):

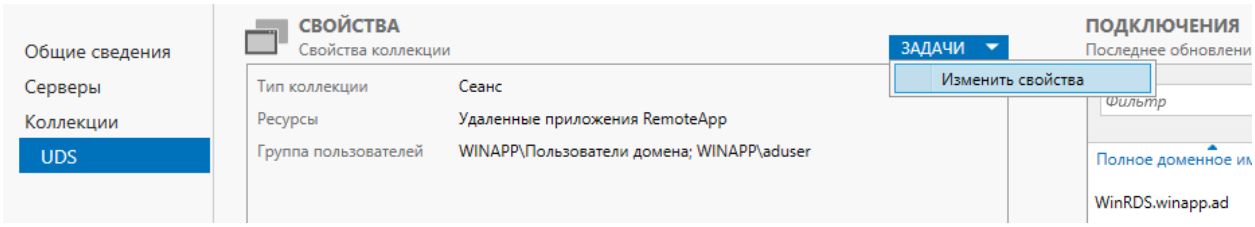


Рисунок 41

В разделе «Сеансы» указать минимальное время для «Окончание разъединенного сеанса» (Рисунок 42).

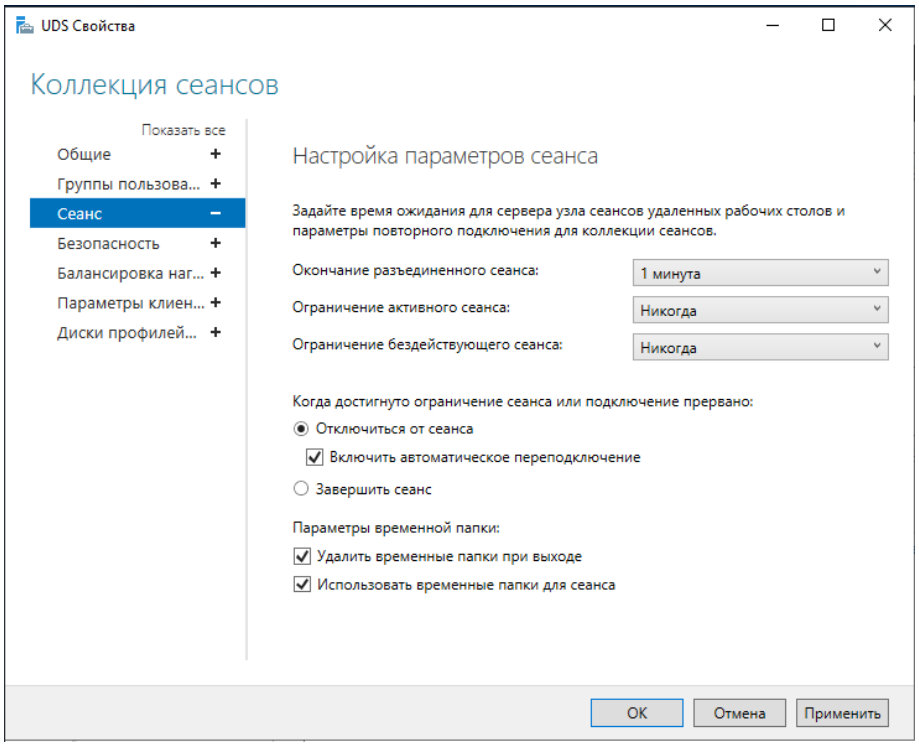


Рисунок 42

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

5 УПРАВЛЕНИЕ VDI ИНФРАСТРУКТУРОЙ

После установки компонентов платформы VDI система готова к настройке. Необходимо в браузере ввести IP-адрес и порт (по умолчанию: 3030) или имя сервера VDI (брокера) через **https-доступ** (Рисунок 43) (например, https://10.10.10.10:3030).

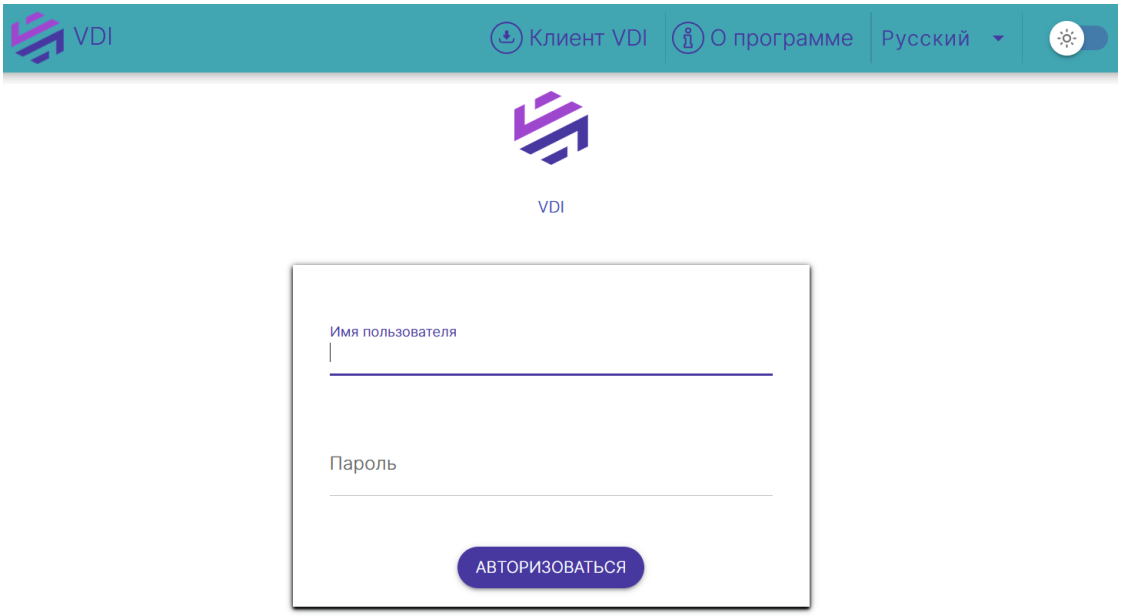


Рисунок 43

1. Для входа в панель администрирования VDI необходимо войти с помощью пользователя и пароля администратора. (По умолчанию: admin/admin).
2. После доступа к панели администрирования можно изменить пароль и создать или выбрать новых пользователей для входа в панель администрирования.
3. 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).
4. 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.

5. В меню пользователя выбрать **Панель управления**, чтобы войти в администрирование VDI (Рисунок 44).

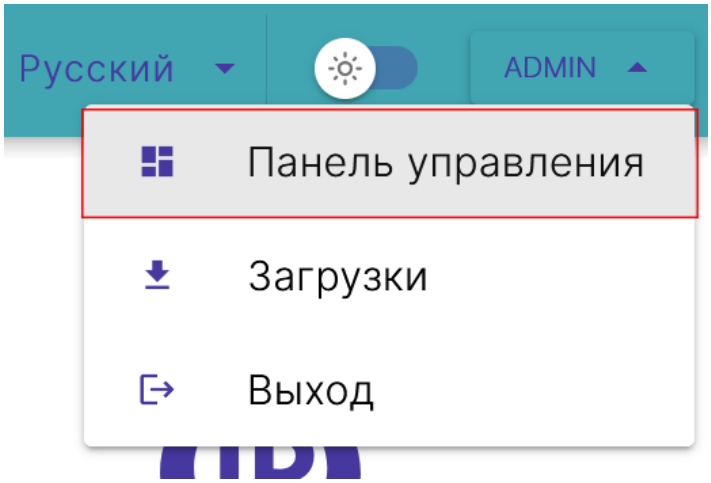


Рисунок 44

6. После входа в администрирование VDI необходимо выполнить 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 45) 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 5.2;

– *список сервис-пулов* по кнопке **Просмотр пулов услуг**. Создание пула услуг позволяет использовать настольные сервисы или виртуальные приложения, которые будут доступны различным группам пользователей (см. пункт 5.4.1).

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

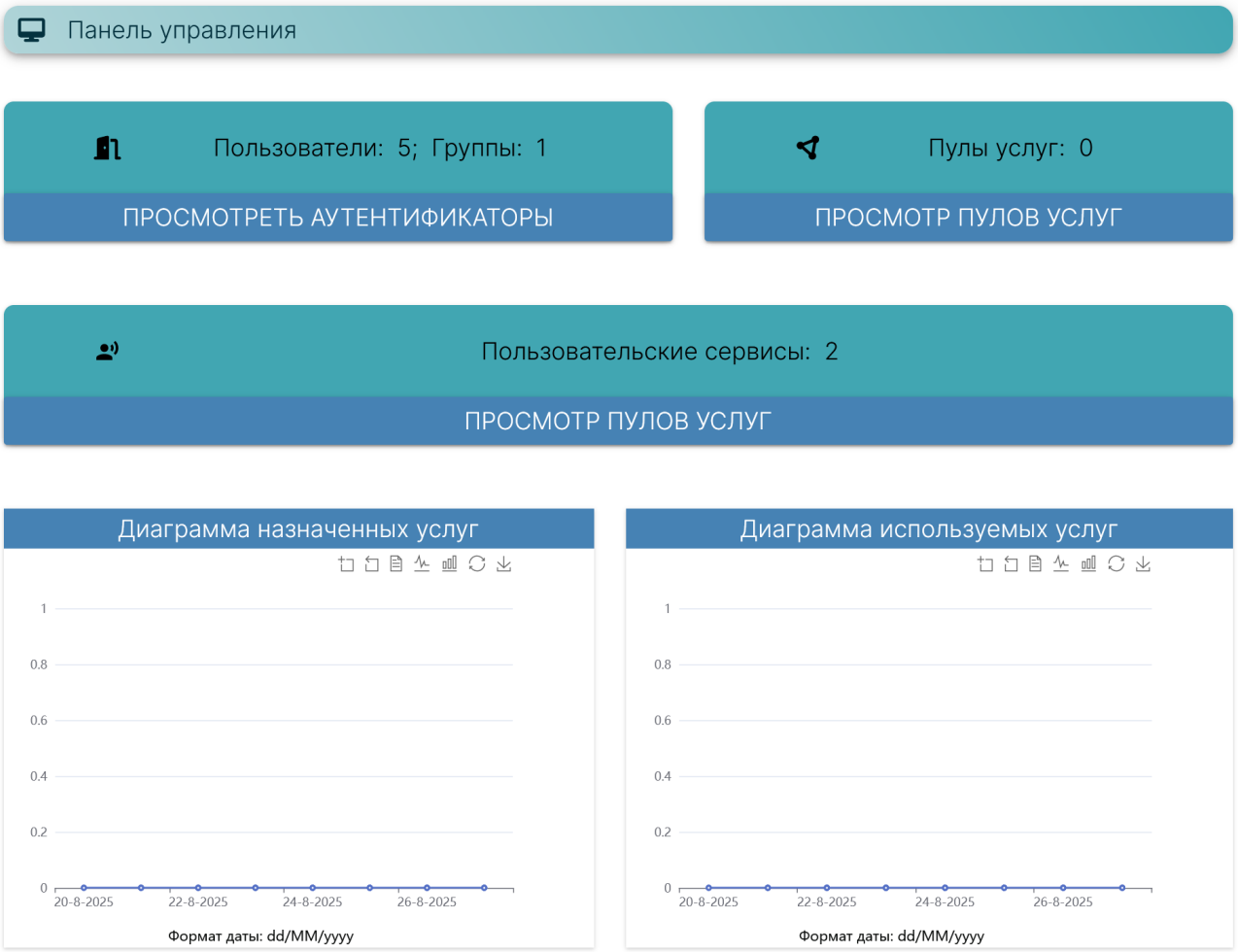


Рисунок 45

5.1 Поставщики услуг

Поставщик услуг — это компонент, отвечающий за предоставление IP-услуг в рамках системы VDI.

Услуги, предоставляемые через VDI, могут включать:

– виртуальные рабочие столы по требованию;

– приложения по требованию;

– постоянные физические или виртуальные рабочие столы, назначаемые конкретным пользователям с использованием механизма назначения IP.

Для формирования пула служб и публикации виртуальных рабочих столов и приложений необходимо наличие хотя бы одного поставщика услуг.

Система VDI поддерживает одновременную работу нескольких поставщиков услуг, что обеспечивает масштабируемость и гибкость при организации сервисов.

В настоящее время VDI поддерживает следующих поставщиков услуг:

– Поставщик статических IP-машин;

– Поставщик платформы Иридиум;

– Поставщик платформы RDS.

5.1.1 Регистрация поставщика статических IP-машин

Примечание: для использования указанного поставщика на сервере VDI должна быть развернута хотя бы одна ВМ.

Для создания **поставщика статических IP-машин** необходимо:

1. Нажать **Новый** и выбрать **Поставщик статических IP-машин** (Рисунок 46).
2. Откроется окно добавления поставщика.

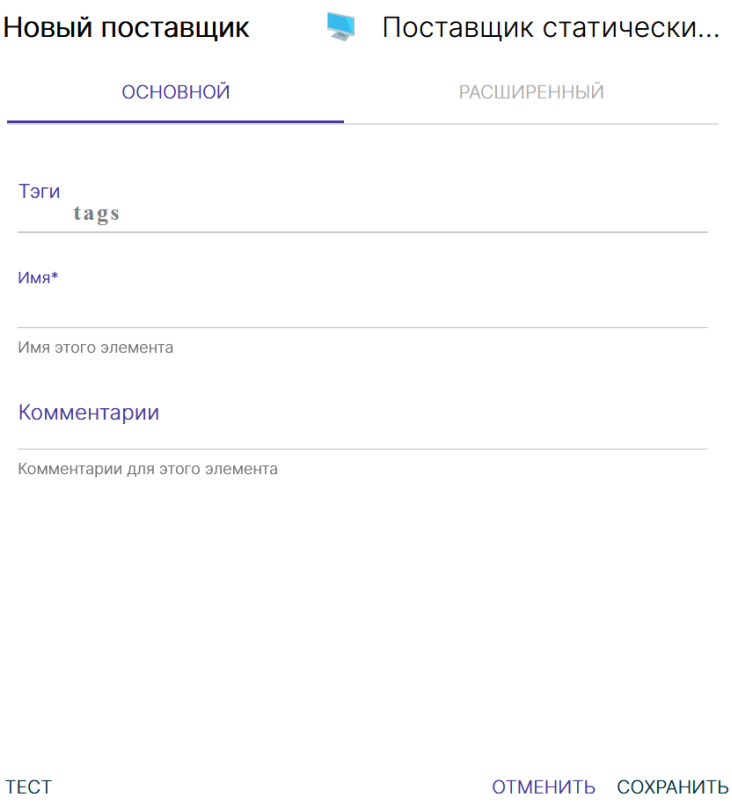


Рисунок 46

3. В поле **Поставщик машин статистических IP** необходимо указать описательное имя поставщика услуг.
4. Нажать кнопку **Сохранить**.
5. Поставщик появится в списке. Для регистрации базовых служб необходимо дважды щелкнуть по созданному поставщику услуг или щелкнуть правой кнопкой мыши и выбрать в меню **Подробности** (Рисунок 47).

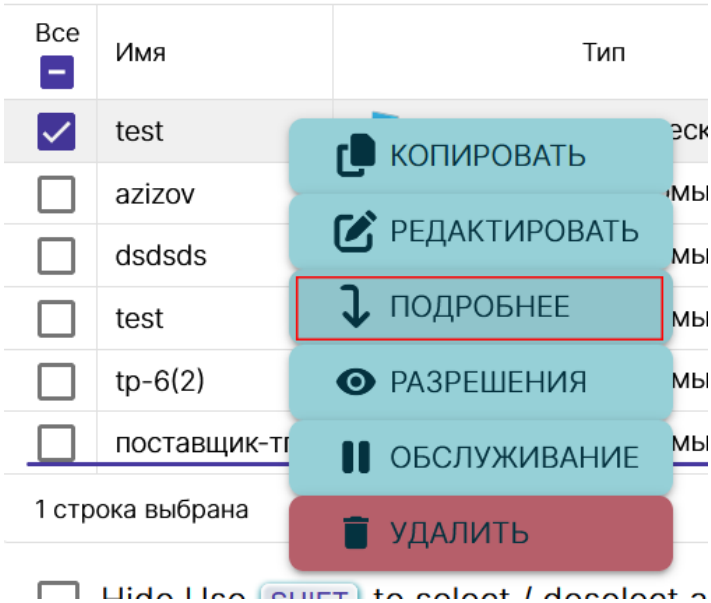


Рисунок 47

5.1.1.1 *Конфигурирование служб на основе статической множественной IP-адресации*

Данный тип службы предназначен для организации доступа пользователей к отдельным компьютерам (физическим или виртуальным), закреплённым за ними по принципу «один пользователь — один компьютер». Каждому пользователю назначается уникальный IP-адрес из заданного пула, что обеспечивает постоянное и индивидуальное соединение с конкретным ресурсом.

Для создания службы на основе **Статического множественного IP-адреса** необходимо:

1. Выбрать поставщика услуг **Поставщик статических IP-машин**.
2. Двойным нажатием нажать на выбранного поставщика.
3. Нажать на кнопку **Новый.**
4. Выбрать **Статический множественный IP-адрес.**

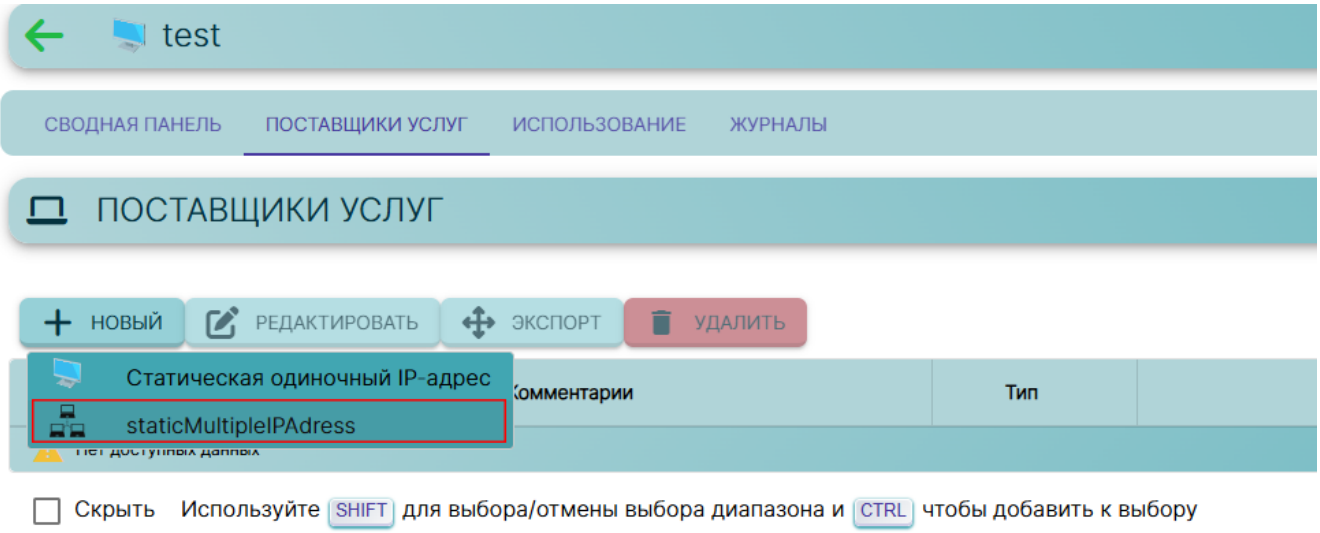


Рисунок 48

5. Откроется окно создания службы (Рисунок 49).

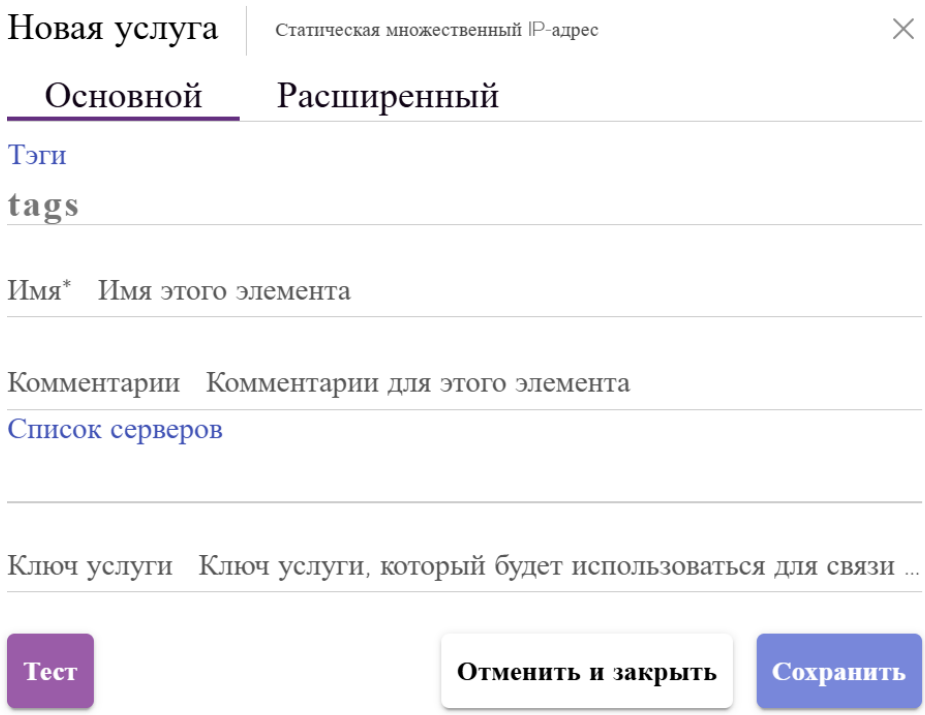


Рисунок 49

Необходимо заполнить следующие поля:

– **Имя**. название службы;

– **Список серверов**. IP-адреса компьютеров, к которым будут подключаться пользователи.

– Ввести различные IP-адреса, разделенные запятыми, и нажать **Добавить** (Рисунок 50).

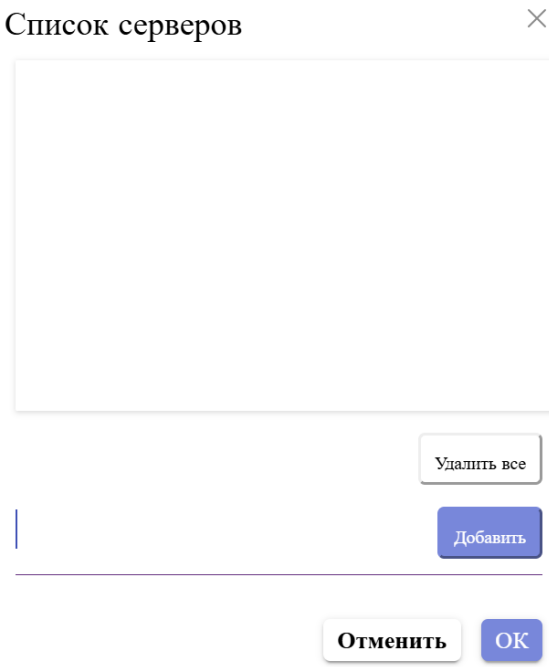


Рисунок 50

– **Ключ услуги** (Рисунок 51). это уникальный идентификатор, по которому платформа узнаёт конкретный сервис и связывает его с пулами и пользователями. При указании ключа необходимо, чтобы указанные компьютеры имели установленные VDI Actor, управляющий статическими машинами.

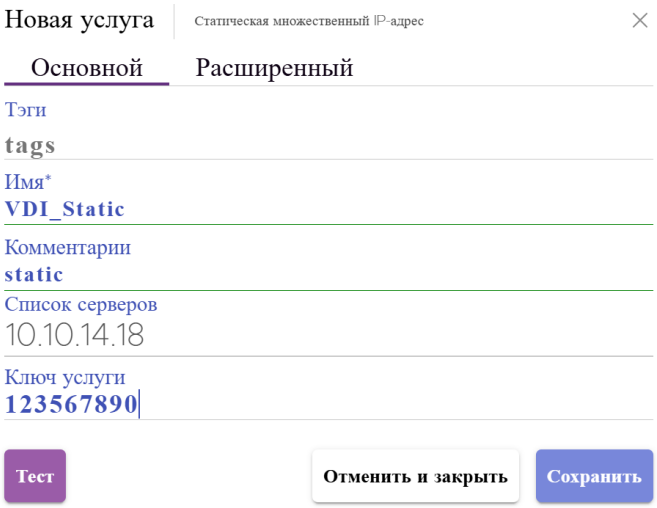


Рисунок 51

6. Вкладка **Расширенные настройки** (Рисунок 52):

– **Время ожидания**. Данное поле определяет, сколько секунд система ждет ответа от хоста при проверке его доступности. Если хост не отвечает в течение указанного времени, проверка считается проваленной. По умолчанию указано 0 – проверка отключена;

– **Проверка порта**. Позволяет задать порт, на котором проверяется доступность сервиса. Если указать 0, проверка по порту не выполняется (будет использоваться только ICMP или другой базовый метод).

– **Максимальное количество сеансов для машины**. Лимит одновременно активных подключений (сессий) к одной машине. По умолчанию значение 0 – количество сессий не ограничено.

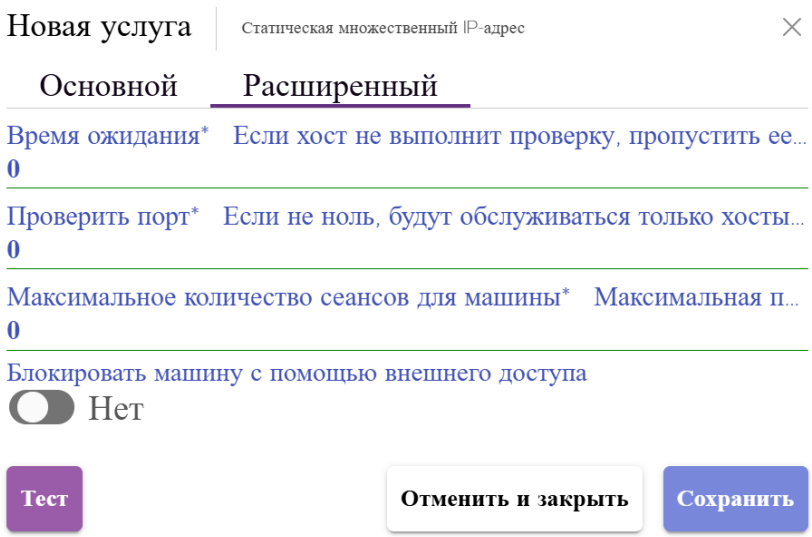


Рисунок 52

7. Нажать кнопку **Сохранить.**

8. Созданный сервис будет доступен в списке.

5.1.1.2 *Конфигурирование службы на основе статической одиночной IP-адресации*

Данный тип службы позволяет нескольким пользователям подключаться к одному и тому же компьютеру (физическому или виртуальному). При этом каждому

пользователю предоставляется отдельный сеанс работы на этом компьютере, при условии, что он сконфигурирован для многопользовательского доступа.

Для создания базовой службы типа на основе **Статического одиночного IP-адреса:**

1. Перейти к списку поставщиков услуг.
2. Выбрать поставщика статических IP-машин.
3. Нажать на него двойным щелчком.
4. Нажать кнопку **Новый -> Статический одиночный IP-адрес.**
5. Откроется окно добавления услуги (Рисунок 53).

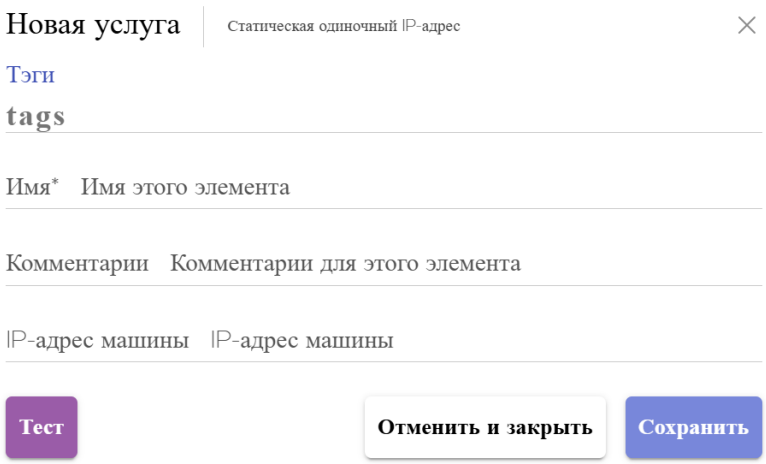


Рисунок 53

Заполнить следующие поля:

– **Имя**. Название службы.

– **IP адрес машины**: IP-адрес компьютера, с которым соединятся пользователи. Компьютер должен разрешить доступ через различные пользовательские сеансы.

6. Нажать кнопку **Сохранить.**

5.1.2 Поставщик платформы Горизонт-ВС

Для добавления поставщика Горизонт-ВС:

1. В разделе **Поставщики услуг** нажать кнопку **Новый.**
2. Выбрать **Поставщик платформы HVS.**

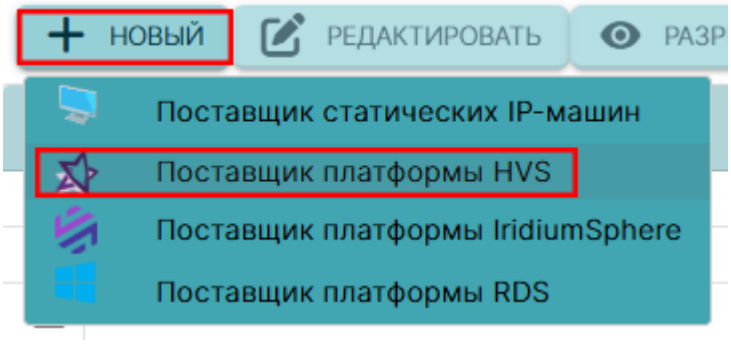


Рисунок 54

3. Откроется окно добавления поставщика, в котором нужно заполнить:
   - Имя;
   - Хост;
   - Имя пользователя;
   - Пароль.

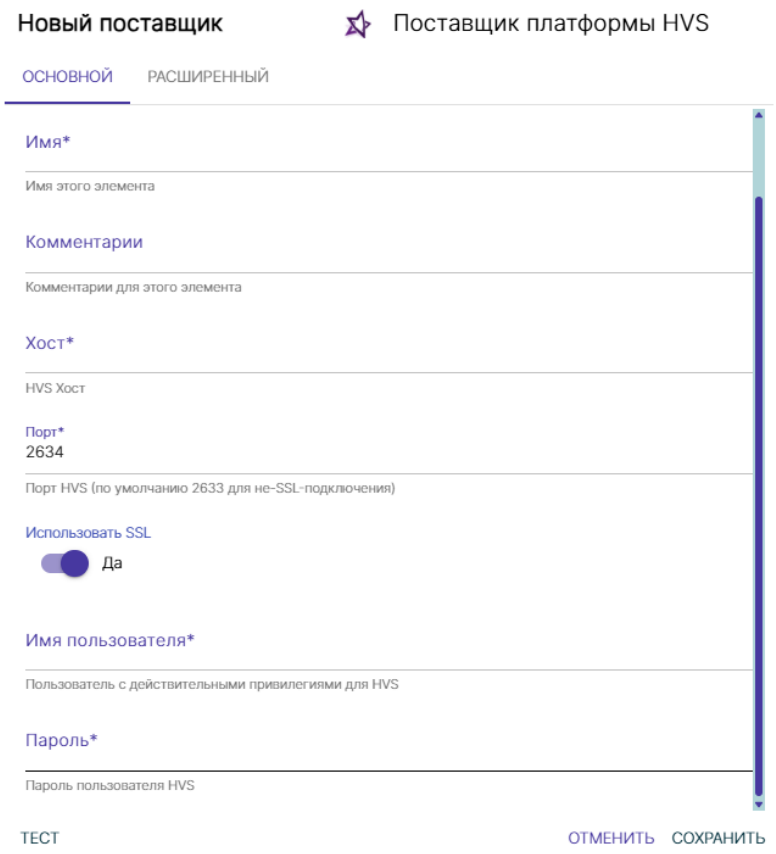


Рисунок 55

4. На вкладке **Расширенный** возможна настройка дополнительных параметров, таких как Максимальное количество одновременно создаваемых виртуальных машин, максимальное количество одновременно удаляемых виртуальных машин, время ожидания подключения к HVS в секундах.

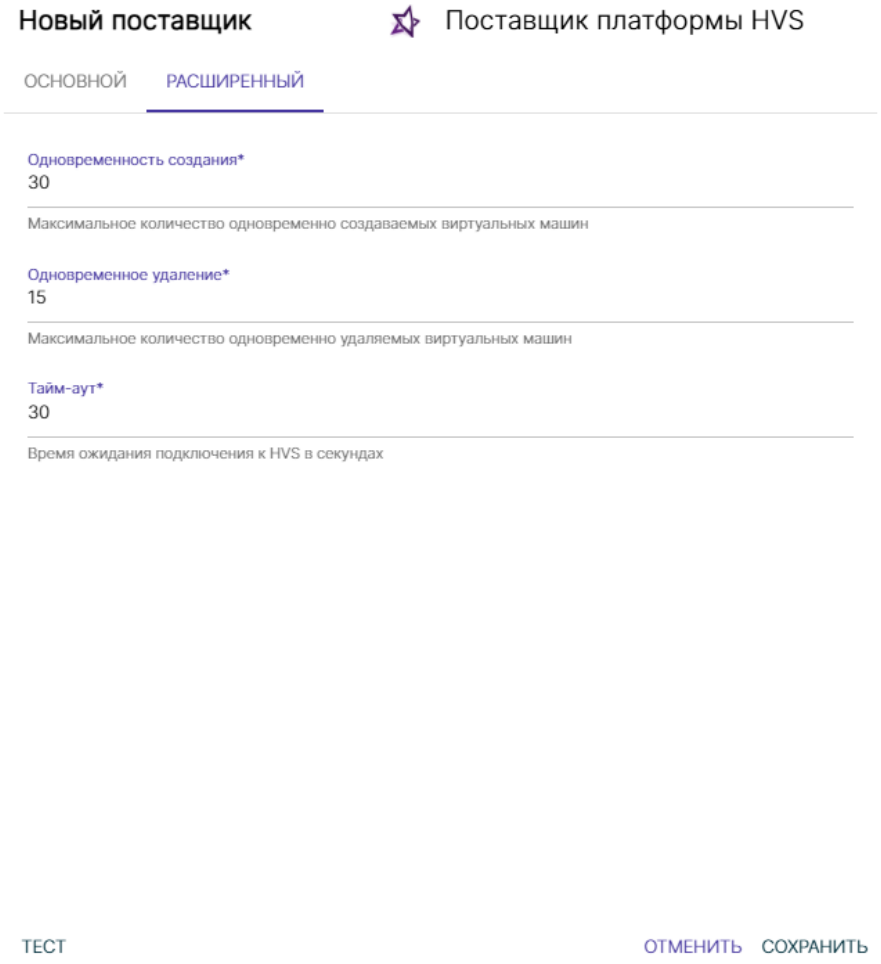


Рисунок 56

5. Нажать кнопку **Сохранить.**
6. Поставщик будет доступен в списке.

5.1.2.1 *Создание службы на основе поставщика Горизонт-ВС*

1. Дважды нажать на созданный ранее поставщик.
2. Выбрать кнопку **Подробнее**.

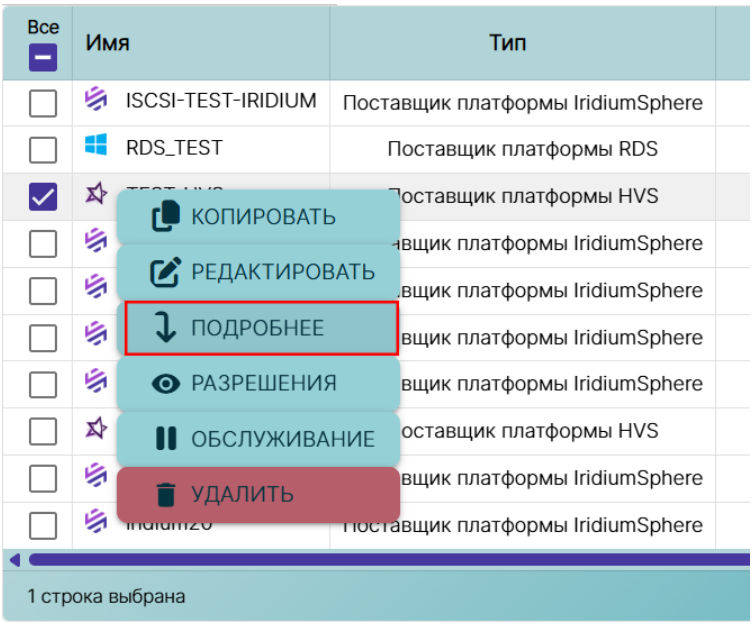


Рисунок 57

3. Нажать кнопку **Новый** -> **Действующие образы HVS**.

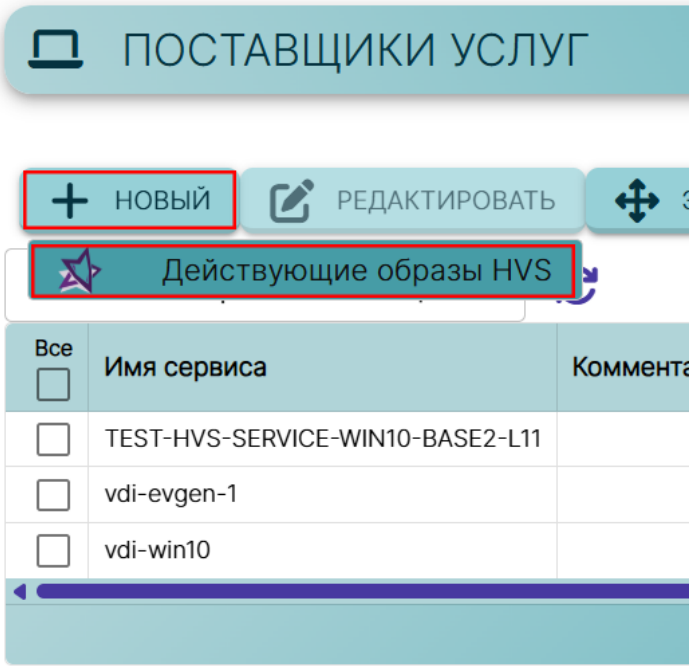


Рисунок 58

4. Вписать имя сервиса, выбрать Хранилище во вкладке **Основной**.

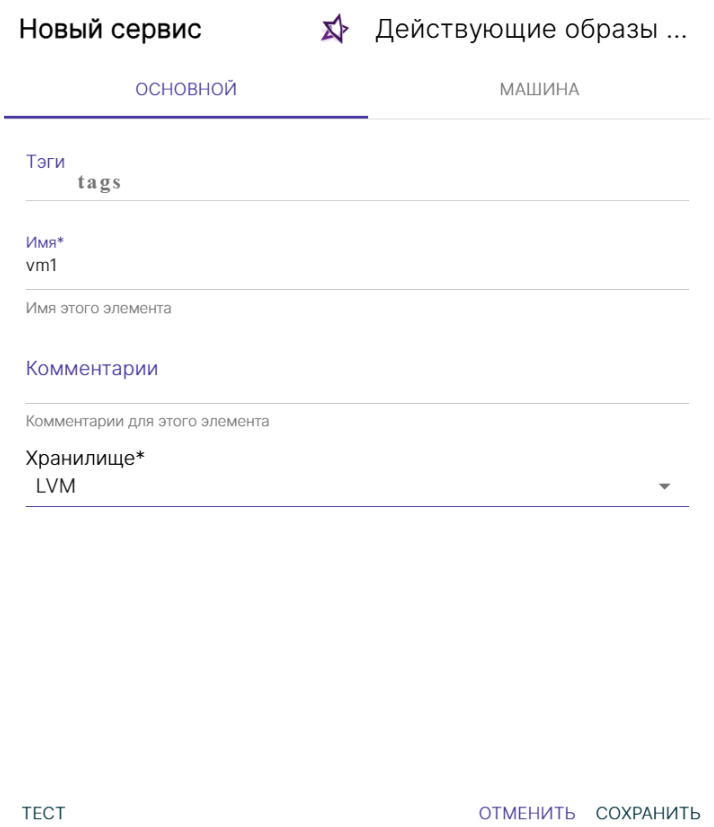


Рисунок 59

5. Во вкладке **Машина** выбрать шаблон ВМ, ввести имя для клонов этой ВМ и длину имени (размер числовой части названий этих машин).

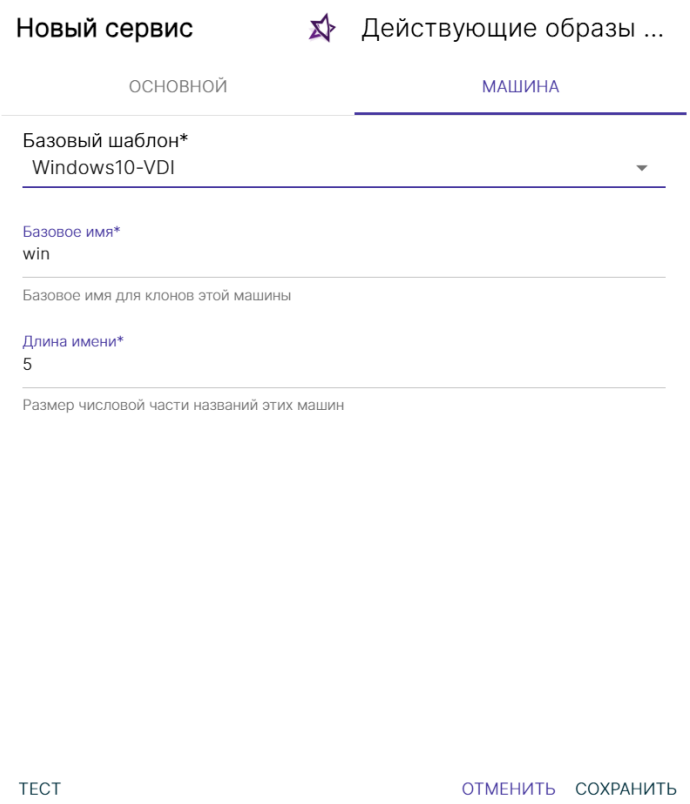


Рисунок 60

6. Нажать кнопку **Сохранить**.

5.1.3 Поставщик «Иридиум»

Для добавления поставщика «Иридиум»:

1. В разделе **Поставщики услуг** нажать кнопку **Новый**.
2. В списке выбрать **IridiumSphere.**

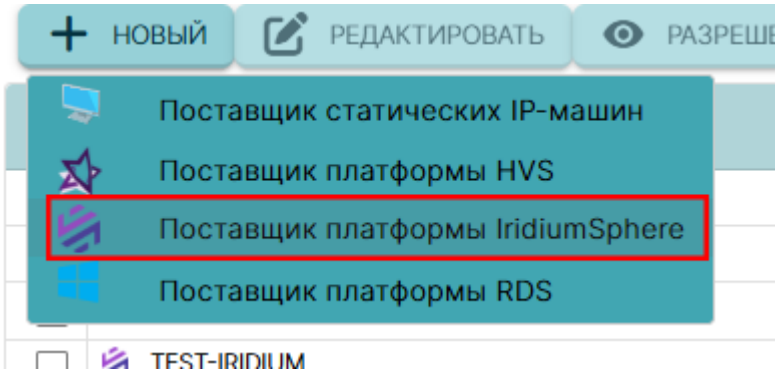


Рисунок 61

3. Откроется окно добавления поставщика.
4. Заполнить следующие поля:

- **Имя;**
- **Хост;**
- **Порт;**
- **Имя пользователя (с действительными привилегиями);**
- **Пароль от учетной записи пользователя.**

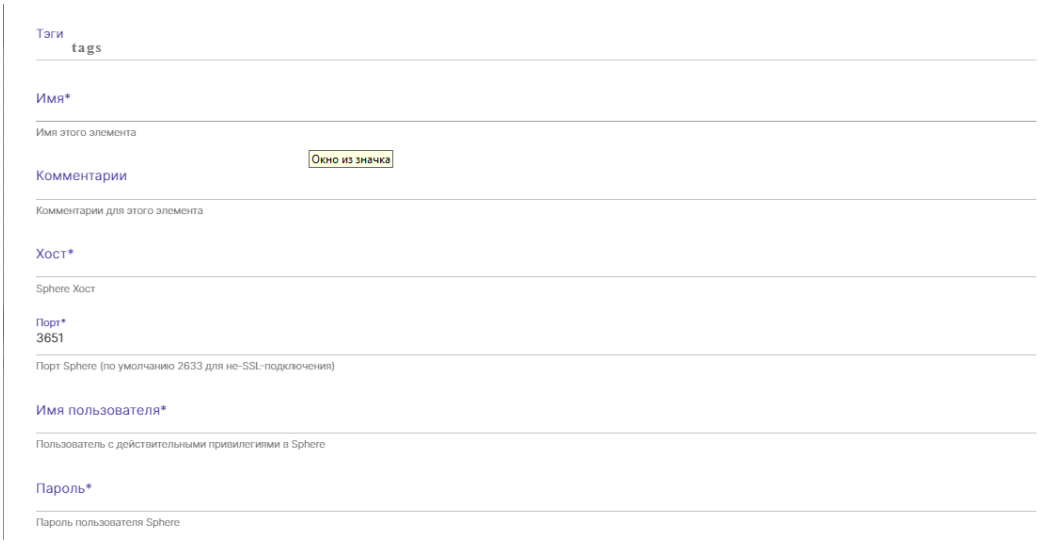


Рисунок 62

5. Нажать кнопку **Тест** для тестирования подключения к поставщику.
6. Нажать кнопку **Сохранить.**
7. Поставщик будет отображен в списке.

Все	Имя	Тип
☐	ISCSI-TEST-IRIDIUM	Поставщик платформы IridiumSphere
☐	RDS_TEST	Поставщик платформы RDS
☐	TEST-HVS	Поставщик платформы HVS
☐	TEST-IRIDIUM	Поставщик платформы IridiumSphere
☐	dont_tp6	Поставщик платформы IridiumSph Окно из значка
☐	dont_tp6	Поставщик платформы IridiumSphere
☐	dont_tp6	Поставщик платформы IridiumSphere
☐	hvs35	Поставщик платформы HVS
☐	iridium160	Поставщик платформы IridiumSphere
☐	iridium20	Поставщик платформы IridiumSphere

Рисунок 63

5.1.3.1 *Изменение параметров поставщика Иридиум*

Для изменения настроек поставщика:

1. Выбрать созданный ранее поставщик.

2. Нажать кнопку **Редактировать.**

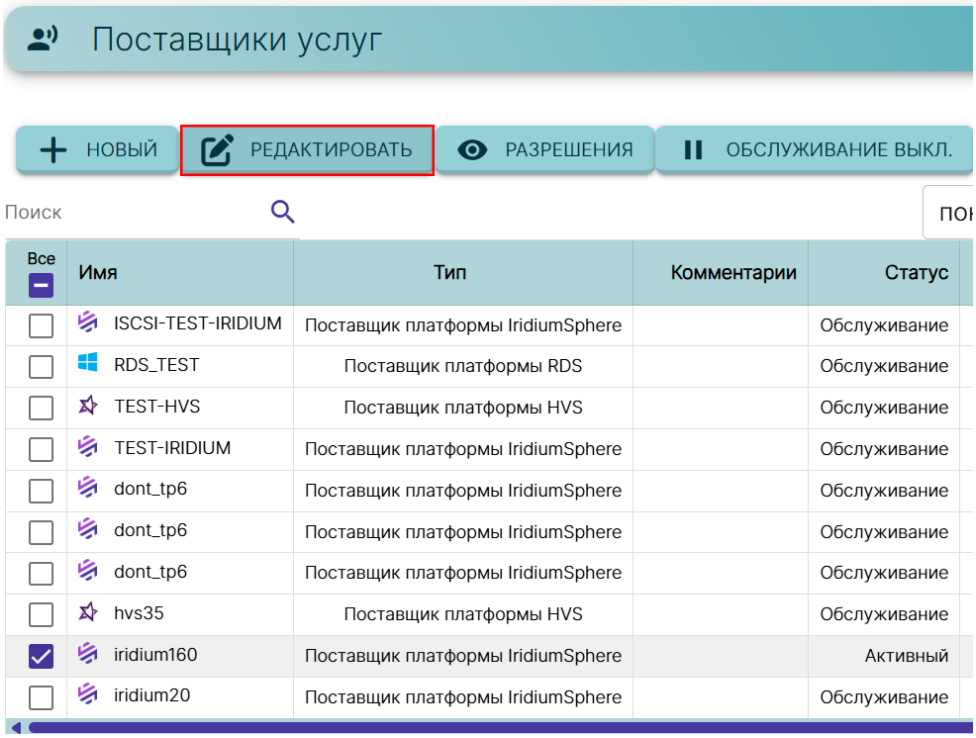


Рисунок 64

3. Откроется окно редактирования поставщика.

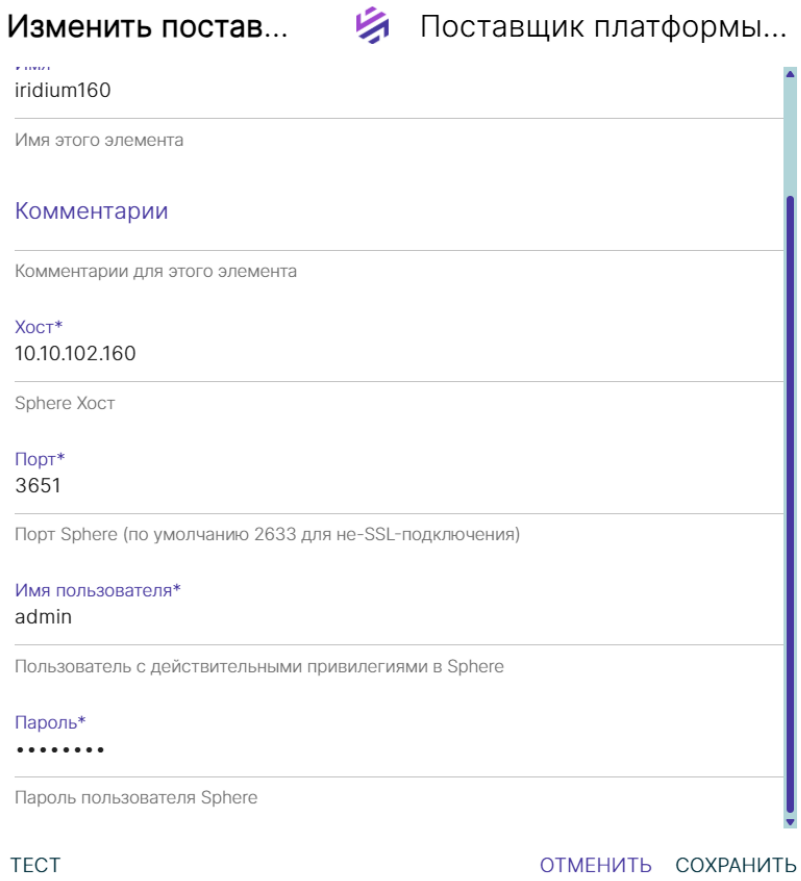


Рисунок 65

4. Нажать кнопку **Сохранить.**

5.1.3.2 *Создание службы на основе поставщика Иридиум*

1. Дважды нажать на созданный ранее поставщик.
2. Выбрать кнопку **Подробнее.**

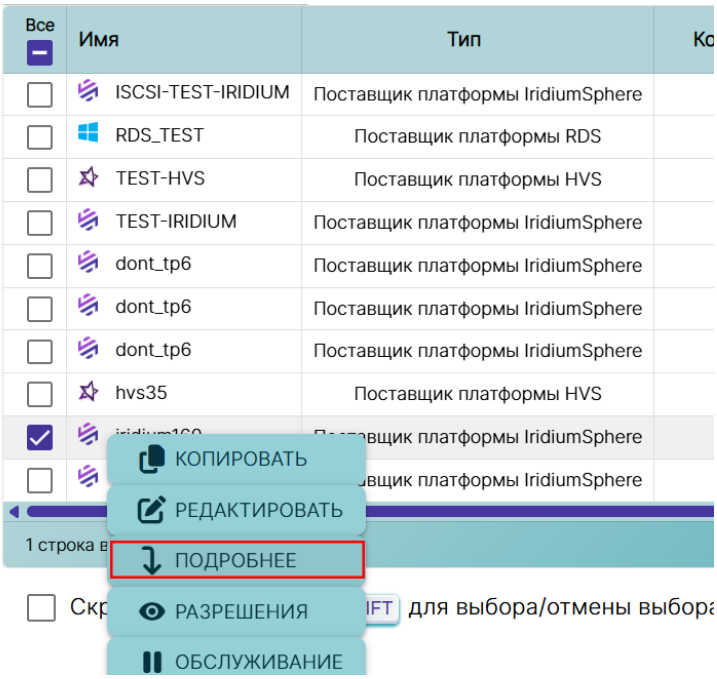


Рисунок 66

3. Нажать кнопку **Новый -> Действующий образ Iridium**.

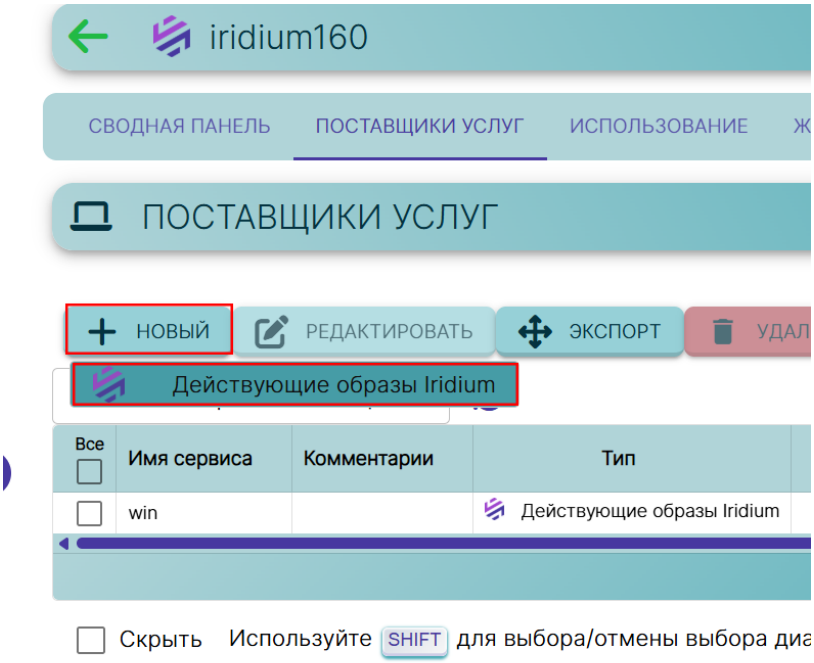


Рисунок 67

4. Вписать имя сервиса, выбрать **Хранилище** во вкладке **Основной.**

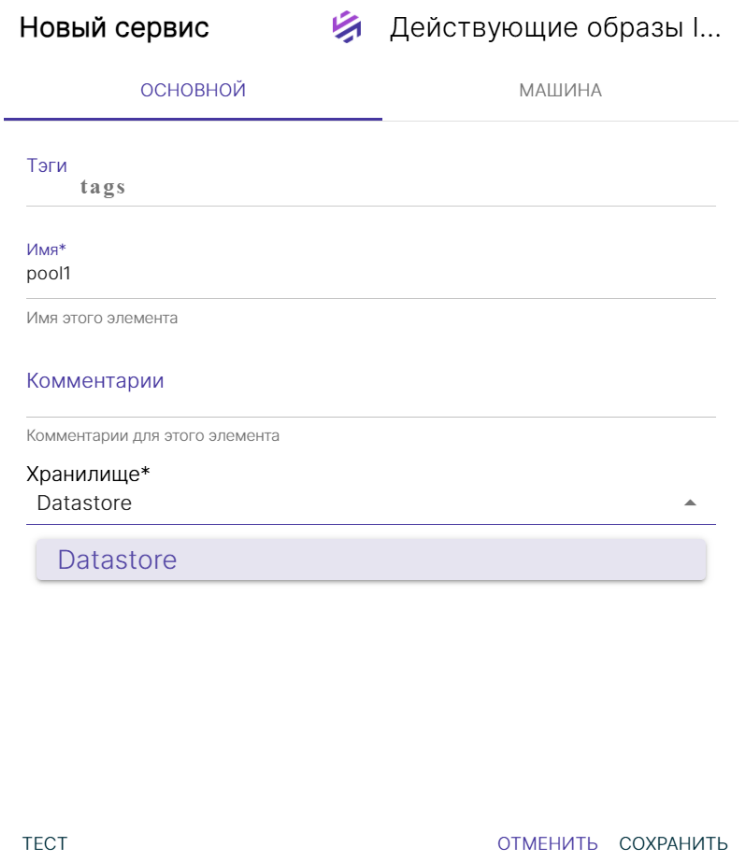


Рисунок 68

5. Во вкладке **Машина** выбрать шаблон ВМ, ввести имя для клонов этой ВМ и длину имени (размер числовой части названий этих машин).

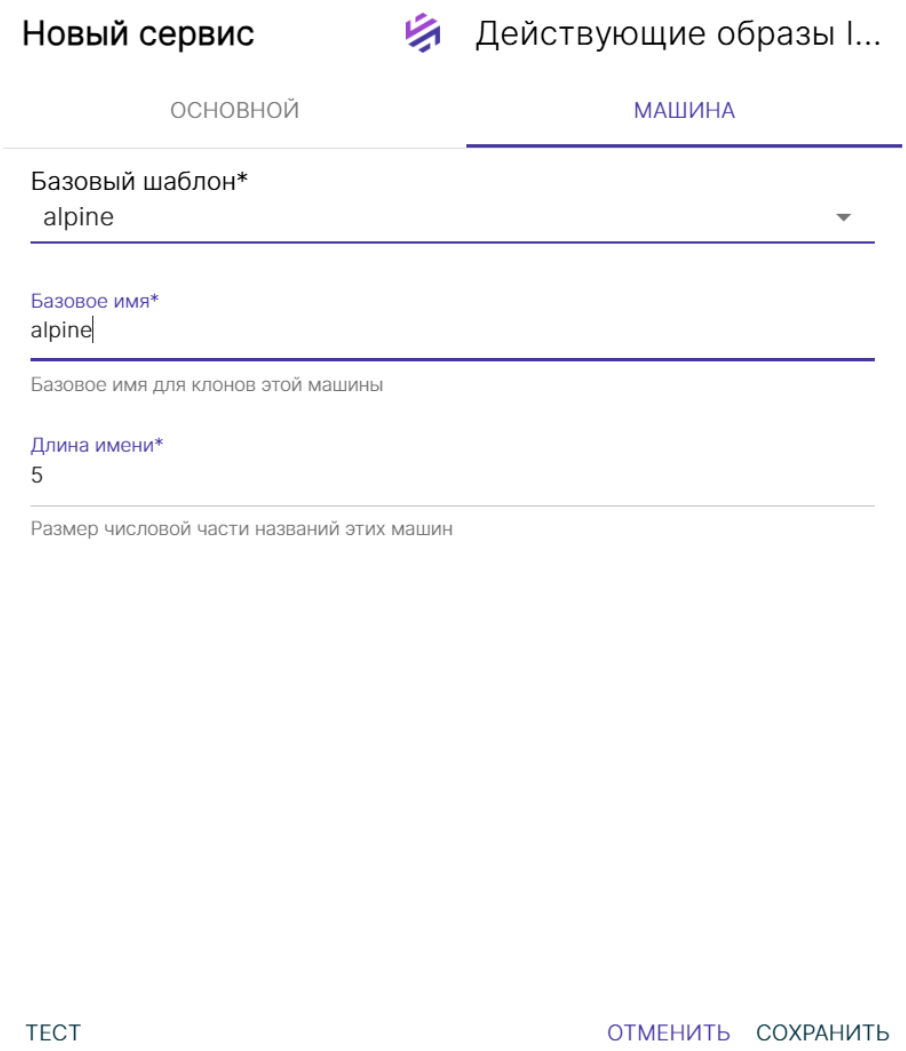


Рисунок 69

6. Нажать кнопку **Сохранить.**

5.1.4 Поставщик платформы RDS

Данный тип поставщика услуг предназначен для организации сеансов виртуальных приложений с использованием служб удалённых рабочих столов Microsoft (RDS).

Функциональные возможности включают предоставление доступа пользователям, прошедшим аутентификацию в системе, отличной от Active Directory.

Для обеспечения доступа требуется сопоставление учетных записей пользователей. Сопоставление может выполняться двумя способами:

– использование заранее созданных учетных записей в выделенном домене Active Directory, предназначенном для среды VDI;

– автоматическое создание учетных записей в существующем сервере Active Directory средствами подсистемы VDI.

Для добавления поставщика платформы RDS необходимо выполнить следующие действия:

1. Перейти в раздел **Поставщики услуг.**
2. Нажать **Новый** и выбрать **Поставщик платформы RDS** (Рисунок 70):

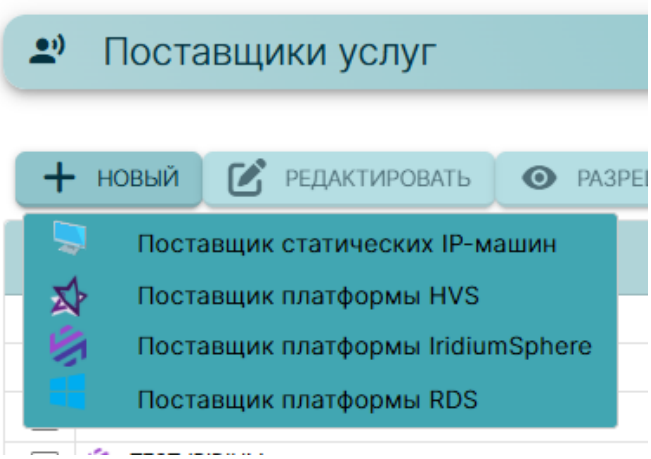


Рисунок 70

3. Заполнить следующие поля (Рисунок 71):

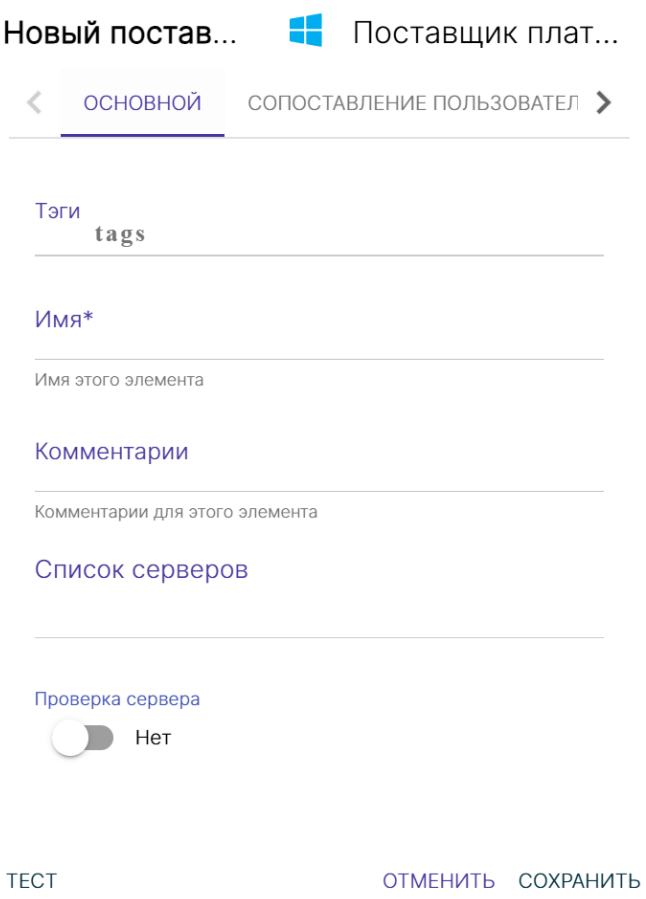


Рисунок 71

- **Тэги** (опционально);
- **Имя;**
- **Комментарии** (опционально);
- **Список серверов**. Указываются адреса серверов (RDS/VDI-брокеров), через которые будет работать данный поставщик услуг. При нажатии открывается окно, в которой необходимо ввести адрес сервера, затем нажать **Добавить**.

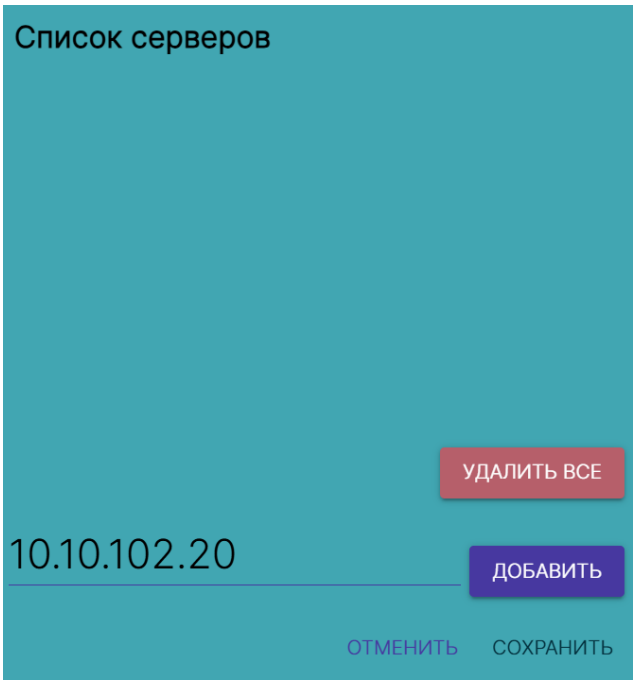


Рисунок 72

– **Проверка сервера.** Система периодически или при сохранении проверяет, доступен ли сервер (например, отвечает ли на сетевые запросы, корректно ли установлено соединение). Если выключено — серверы считаются «как есть», и система не делает проверок.

Примечание: одна и таже служба RDS может иметь несколько IP-адресов, соединяющих различные существующие серверы RDS, что обеспечивает высокую доступность приложений. Кроме того, при указании нескольких IP-адресов необходимо отметить флажок «Сервер проверяется».

4. Вкладка **Сопоставление пользователей** (Рисунок 74) нужна для того, чтобы связать чётные записи пользователей из внешней системы аутентификации (например, не-AD) с учётными записями, которые будут использоваться в среде VDI. При выключенном положении будет использоваться пользователи портала VDI для доступа к приложениям (в этом случае, это должен быть пользователь AD).

5. Для включения сопоставления пользователей необходимо включить его в положение **включено** (переместить ползунок вправо) и заполнить следующие поля:

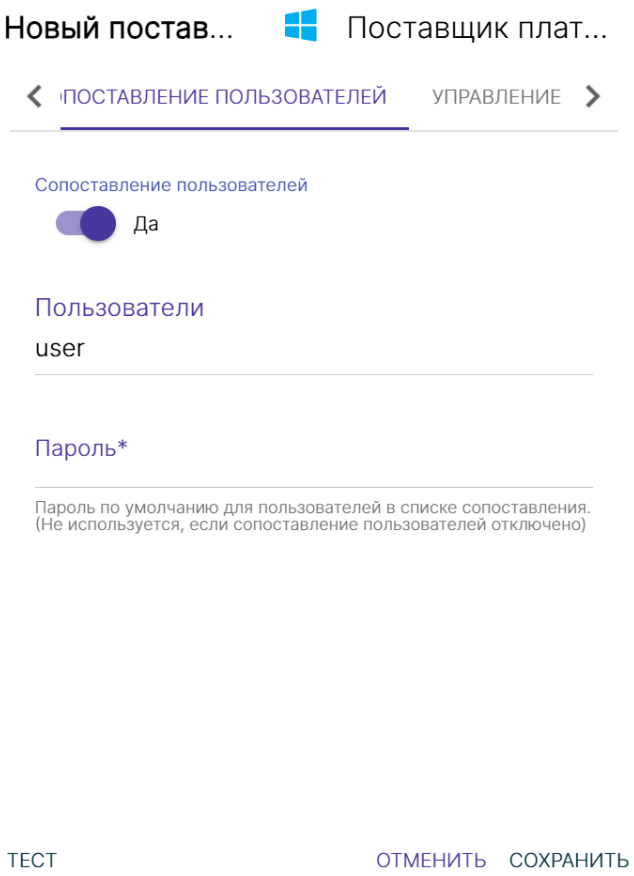


Рисунок 73

– Необходимо нажать на поле **Пользователи**, ввести имя пользователя (Рисунок 74);
– нажать кнопку **Добавить**;
– Нажать кнопку **Сохранить**.
– Поле **Пароль.** Пароль по умолчанию для пользователей в списке сопоставления. Все пользователи сопоставления должны иметь одинаковый пароль.

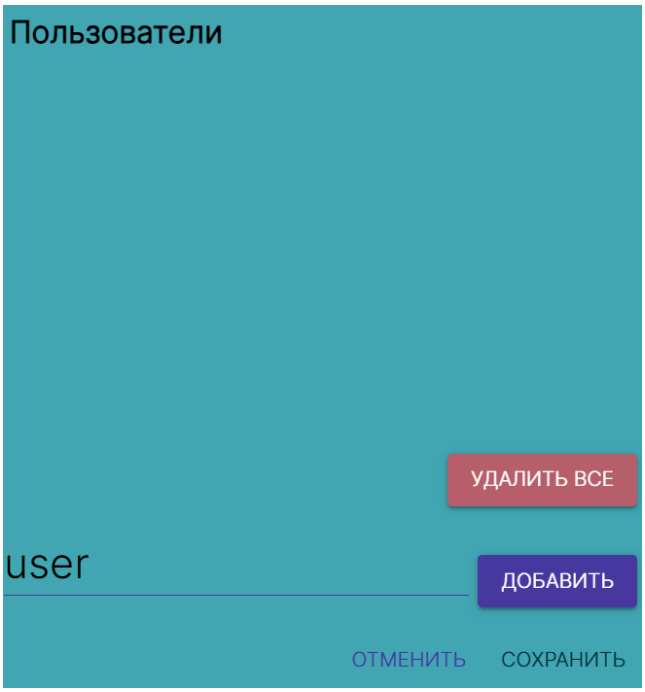


Рисунок 74

*Примечание: следует активировать **Сопоставление пользователей**» только в том случае, если нужно указать общих пользователей домена AD.*

6. Вкладка **Управление пользователями AD** позволяет включить автоматическое создание пользователей в AD в том случае, если нужно указать пользователей из домена AD (Рисунок 75). Эти пользователи будут автоматически созданы VDI.

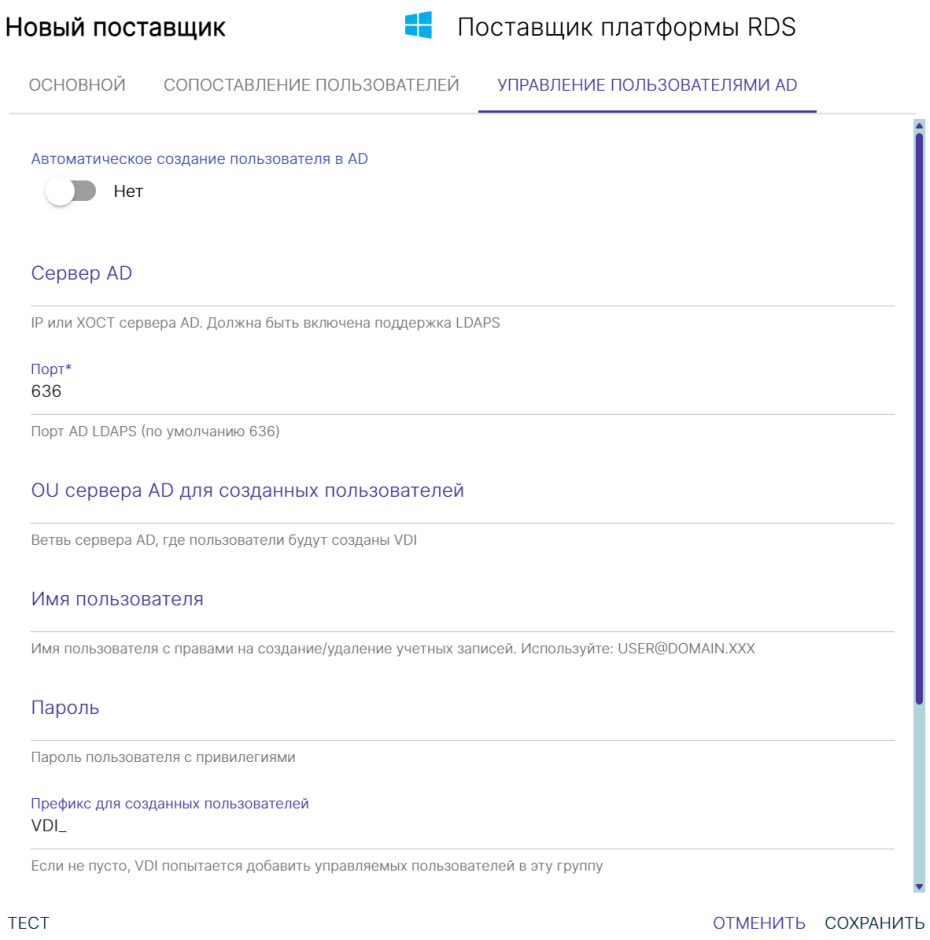


Рисунок 75

– Включенная функция означает, что для доступа к приложениям будут использоваться определенные пользователи, автоматически созданные VDI в AD;

– Выключенная функция означает, будет использовать пользователя портала входа VDI для доступа к приложениям (в этом случае это должен быть пользователь AD);

– В поле **Сервер AD** необходимо ввести IP-адрес или имя сервера Active Directory, на котором будут создаваться новые пользователи (на сервере должно быть включено подключение через LDAPS);

– В **поле Порт** вводится значение, используемое в соединении.

– Поле **OU сервера AD для созданных пользователей**. Это контейнер в структуре Active Directory, в котором хранятся учётные записи

пользователей, компьютеров и групп. Здесь указывается путь к OU, в которую VDI будет помещать вновь созданных пользователей. Это нужно для того, чтобы пользователи создавались не в корне домена, а в заранее определённом месте, где администратору проще управлять правами и политиками;

- **Имя пользователя**. учётная запись администратора домена, которая имеет права создавать и удалять пользователей. В формате: user@domain.xxx;
- **Пароль**. Пароль от указанной выше учётной записи;
- **Префикс для созданных пользователей**. Строка, которая автоматически добавляется к имени всех пользователей, создаваемых VDI**.** Формат: префикс+имя_пользователя;
- **Домен AD**. Домен Active Directory, в котором будут создаваться пользователи.
- **Группа AD.** Имя существующей группы в AD, куда будут добавляться все новые пользователи, созданные VDI.

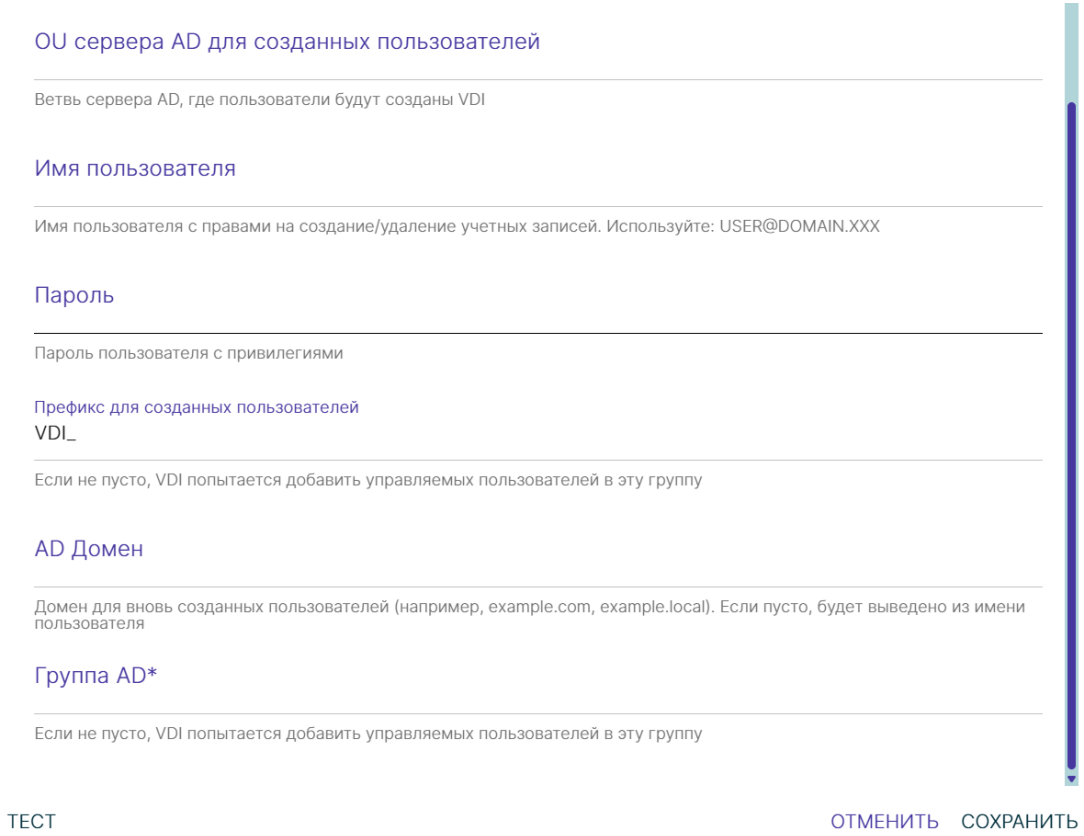


Рисунок 76

Примечание: для сопоставления пользователей можно активировать только один из двух методов: ***Сопоставление пользователей*** *или* ***Автоматическое создание пользователей в AD****.*

8. С помощью кнопки **Тест** производится успешность подключения.
9. Для сохранения конфигурации нажать кнопку **Сохранить.**

5.1.4.1 *Изменение параметров RDP*

1. Для изменения любого параметра в существующем **Поставщике услуг**, выбрать его и нажать **Изменить**.
2. С помощью кнопки **Войти в режим обслуживания** приостанавливаются 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.

5.1.4.2 *Создание служб на основе поставщика RDS*

Для создания базовых служб необходимо:

1. Дважды щелкнуть по созданному провайдеру услуг или в меню провайдера и выбрать **Подробнее** (Рисунок 77).

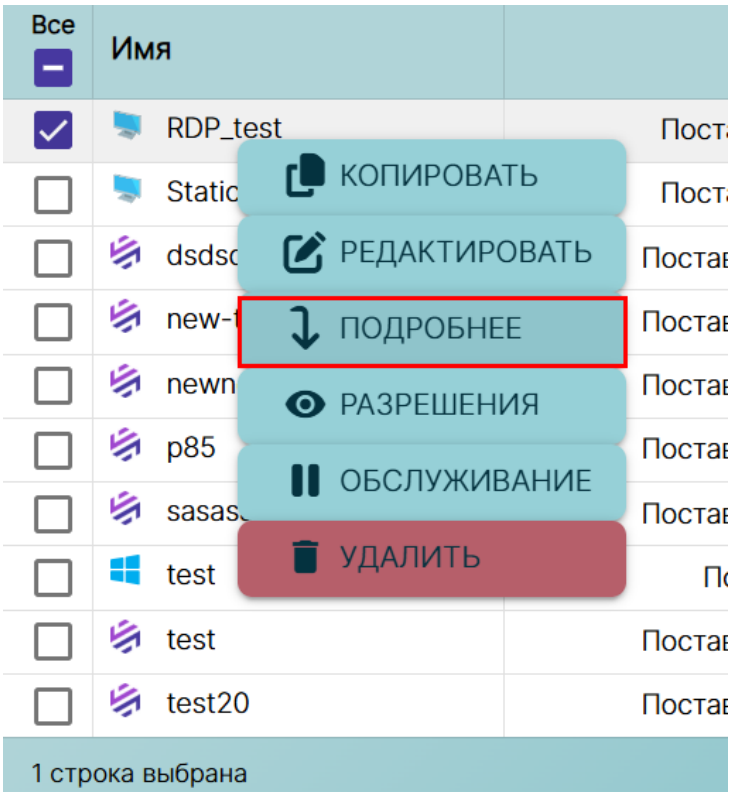


Рисунок 77

2. Нажать кнопку **Новый**.
3. Откроется окно выбора типа службы: на основе статической одиночной IP-адресации или на основе множественной IP- адресации (Рисунок 78).

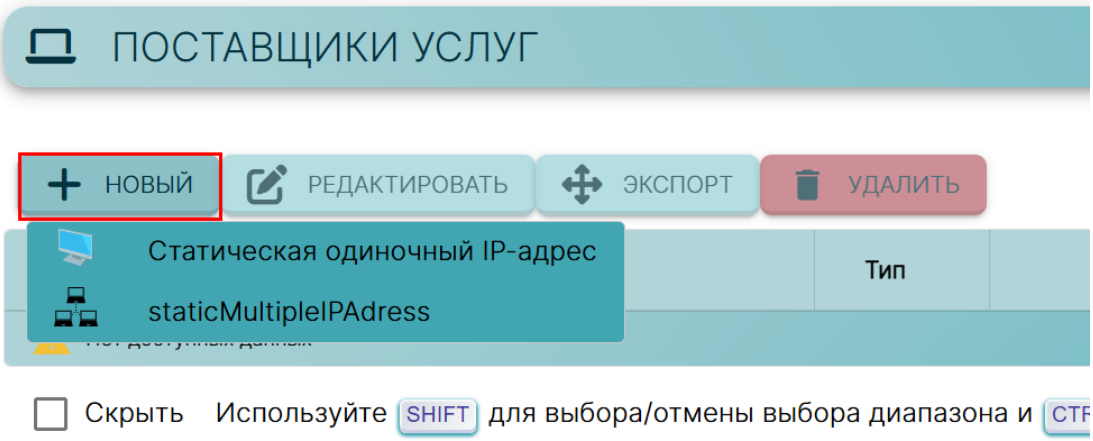


Рисунок 78

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).

Минимальные параметры для настройки в этом типе службы (Рисунок 79):

- 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).

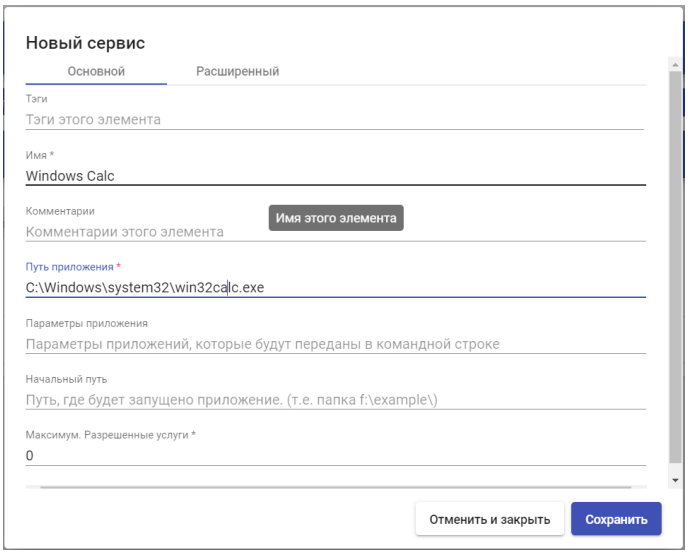


Рисунок 79

- Дополнительно (Рисунок 80):

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

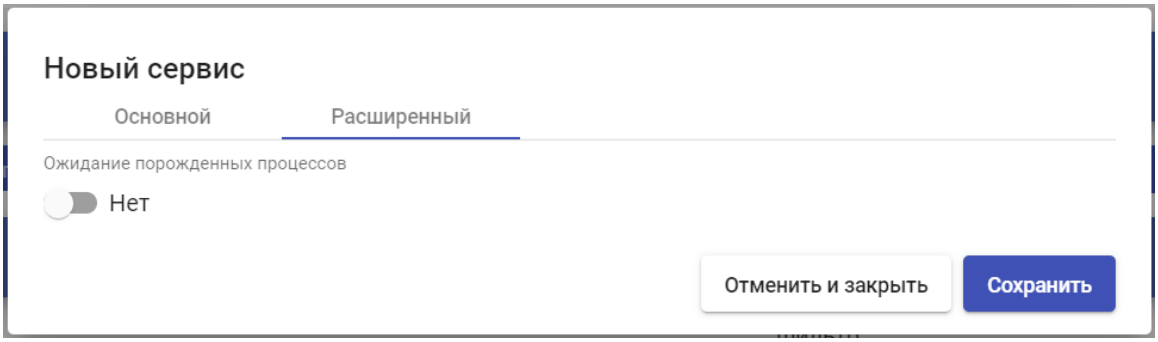


Рисунок 80

5.2 Настройки аутентификации

5.2.1 Аутентификатор Active Directory

Этот внешний аутентификатор обеспечивает доступ к виртуальным рабочим столам и приложениям для пользователей и групп пользователей, принадлежащих Active Directory (Рисунок 81).

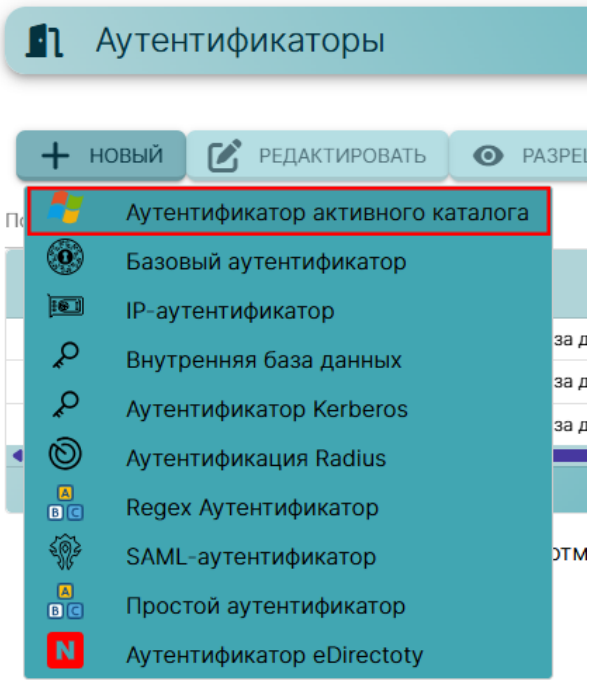


Рисунок 81

Для настройки аутентификатора Active Directory необходимо:

1. Перейти в раздел **Аутентификаторы.**
2. Нажать кнопку **Новый.**
3. Откроется окно добавления аутентификатора, **Основная вкладка** (Рисунок 82) в котором необходимо заполнить следующие поля:
   - **Тэги** (опционально). Поле для присвоения тэгов (меток);
   - **Имя.** Уникальное имя для поставщика аутентификации;
   - **Комментарии (**опционально). Необязательное поле для добавления заметок;
   - **Приоритет.** Числовое поле для указания порядка, в котором система будет пытаться использовать этого поставщика, если их настроено несколько;
   - **Метка.** Используется для группировки транспортов в механизме Metapool;

– **Хост**. Обязательное поле для ввода имени или IP-адреса сервера Active Directory;

– **Использование SSL.** Чекбокс для указания, необходимо ли использовать шифрованное соединение для обмена данными с контроллером домена;

– **Совместимость.** Чекбокс, необходимый для выбора версии совместимости с версиями Windows (доступны WindowsNT и Windows 2000 и позже);

– **Тайм-аут**. Максимальное количество времени в секундах, в течение которого система будет ожидать ответа от сервера при попытке установить соединение.

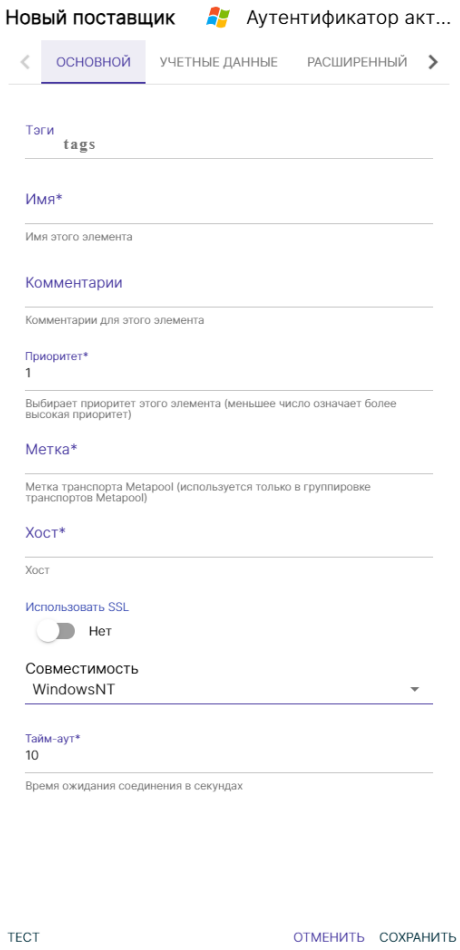


Рисунок 82

4. Вкладка **Учетные данные** (Рисунок 83). Заполнить поля **Имя пользователя** и **Пароль**.

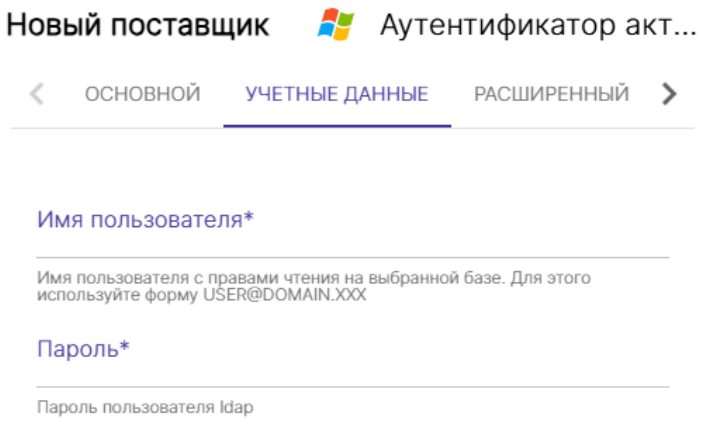


Рисунок 83

5. Вкладка **Расширенный** (Рисунок 84)**.** Поле **Переопределить базу** позволяет вручную указать «базу поиска» (Search Base) для LDAP-запросов к домену Active Directory.
   - начение должно быть в формате LDAP Distinguished Name (DN). Это иерархическая строка, которая однозначно идентифицирует местоположение в каталоге;
   - Пример для корня домена: **DC=mycompany, DC=local;**
   - Пример для конкретного подразделения (**OU): OU=Users, OU=Moscow, DC=mycompany, DC=local.**

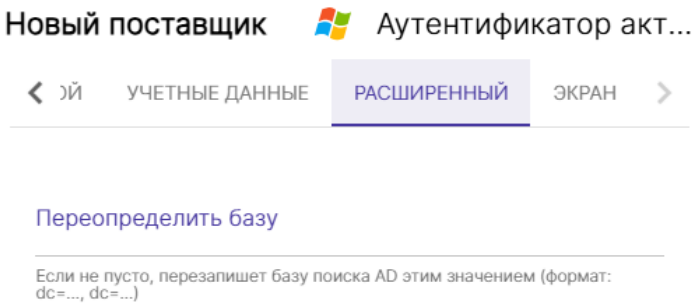


Рисунок 84

6. Вкладка **Экран**. Опция **Видимые** определяет, будет ли этот конкретный поставщик аутентификации отображен в списке доступных методов входа для конечного пользователя.
7. Нажать кнопку **Сохранить.** Аутентификатор будет отображен в списке.

5.2.2 Базовый аутентификатор

Базовый аутентификатор – это универсальный и гибкий инструмент для интеграции VDI с любыми внешними системами аутентификации или базами данных, для которых нет готового специализированного модуля.

Для создания базового аутентификатора необходимо:

1. Выбрать его из списка аутентификаторов (Рисунок 85).

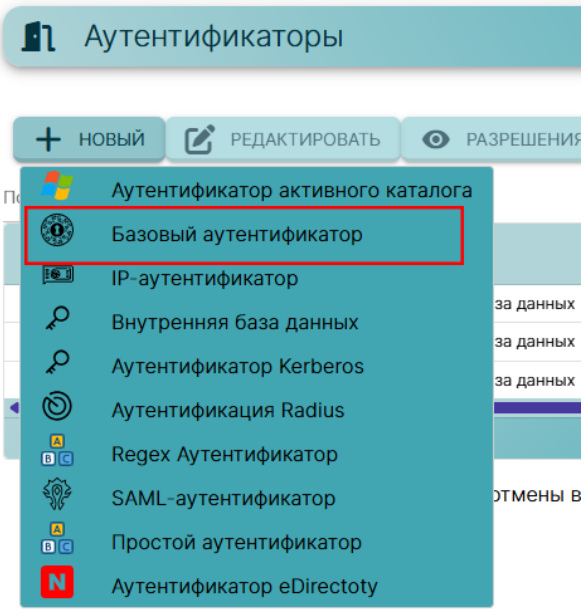


Рисунок 85

2. Откроется окно добавления базового аутентификатора, в котором необходимо заполнить поля во вкладках **Основной. Сервер, Расширенный, Атрибуты, Экран.** * означает, что поле обязательно для заполнения. Во вкладке **Основной** (Рисунок 86):

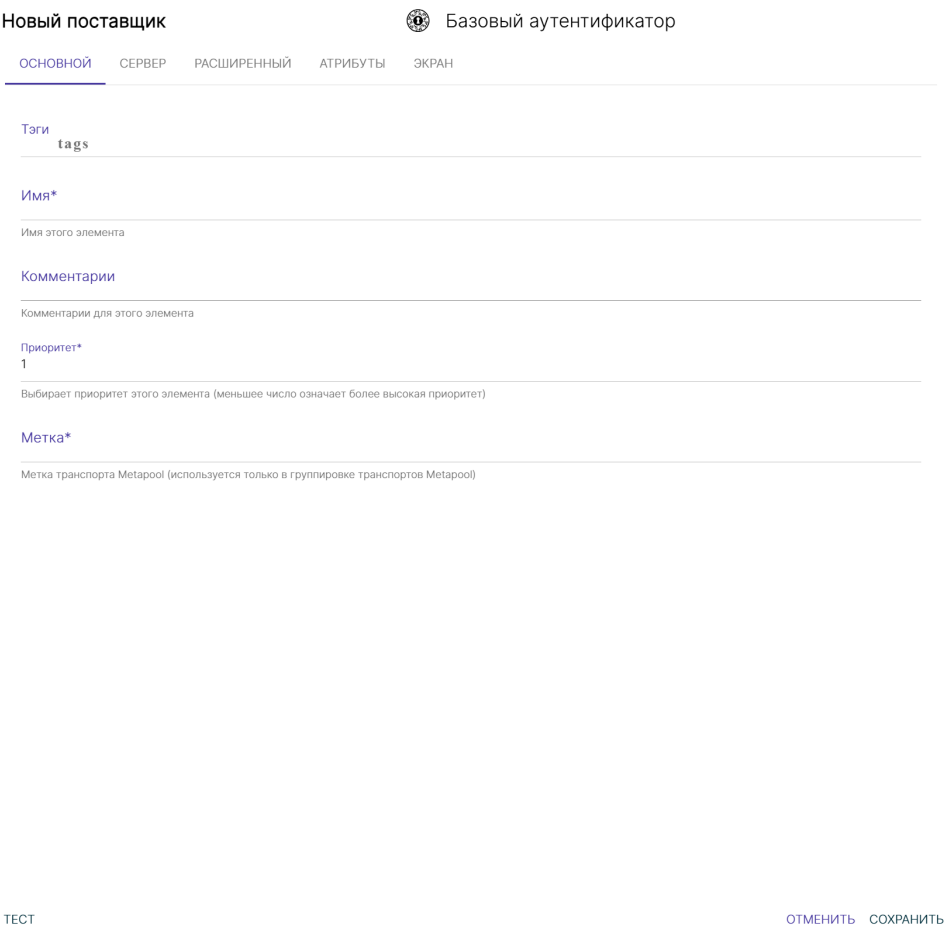


Рисунок 86

- **Тэги** (опционально). Поле для присвоения меток аутентификатору;
- **Имя.** Уникальное имя для аутентификатора;
- **Комментарии** (опционально)**.** Необязательное многострочное текстовое поле для заметок;
- **Приоритет.** Числовое поле для указания порядка, в котором система будет пытаься использовать этого поставщика аутентификации;
- **Метка.** Поле необходимо для группировки в механизме Metapool.

3. Вкладка **Сервер** (Рисунок 87)**:**

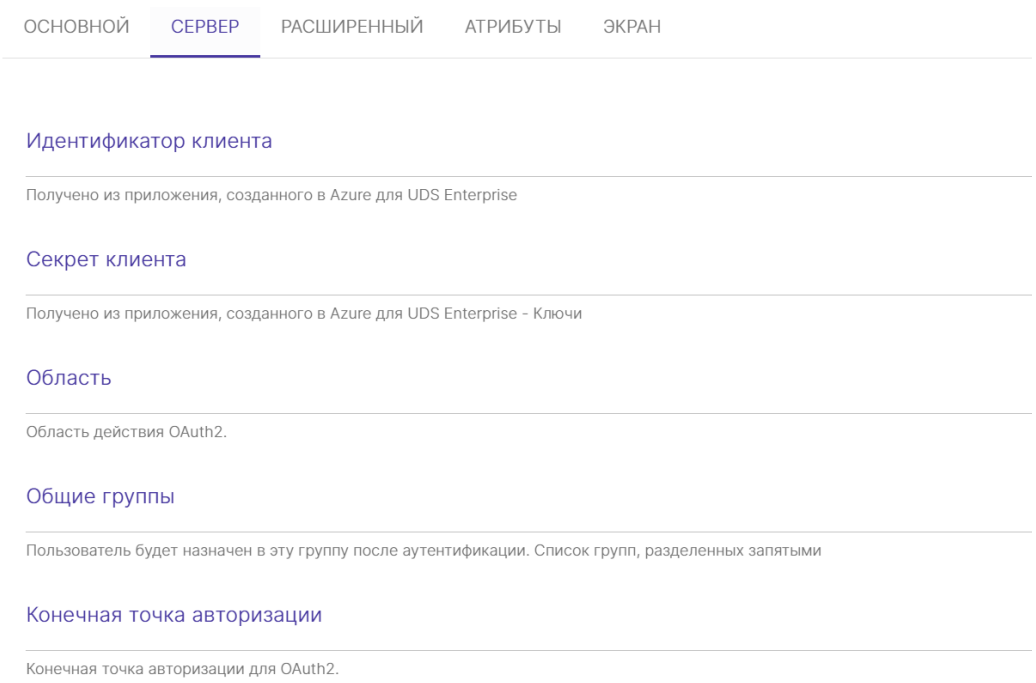


Рисунок 87

- **Идентификатор клиента.** Уникальный идентификатор приложения;
- **Секрет клиента.** Секретный клюс для приложения. Доказывает, что запрос на аутентификацию корректен;
- **Область.** Определяет уровень доступа, который запрашивает VDI у пользователя;
- **Общие группы.** Позволяет автоматически назначить всех пользователей, успешно аутентифицировавшихся через этого провайдера, в одну или несколько групп внутри VDI;
- **Конечная точка авторизации.** URL-адрес, на который VDI будет перенаправлять браузер пользователя для ввода его учетных данных.

4. Вкладка **Расширенный** (Рисунок 88)**.** Вкладка настраивает аутентификацию по протоколу OAuth 2.0.

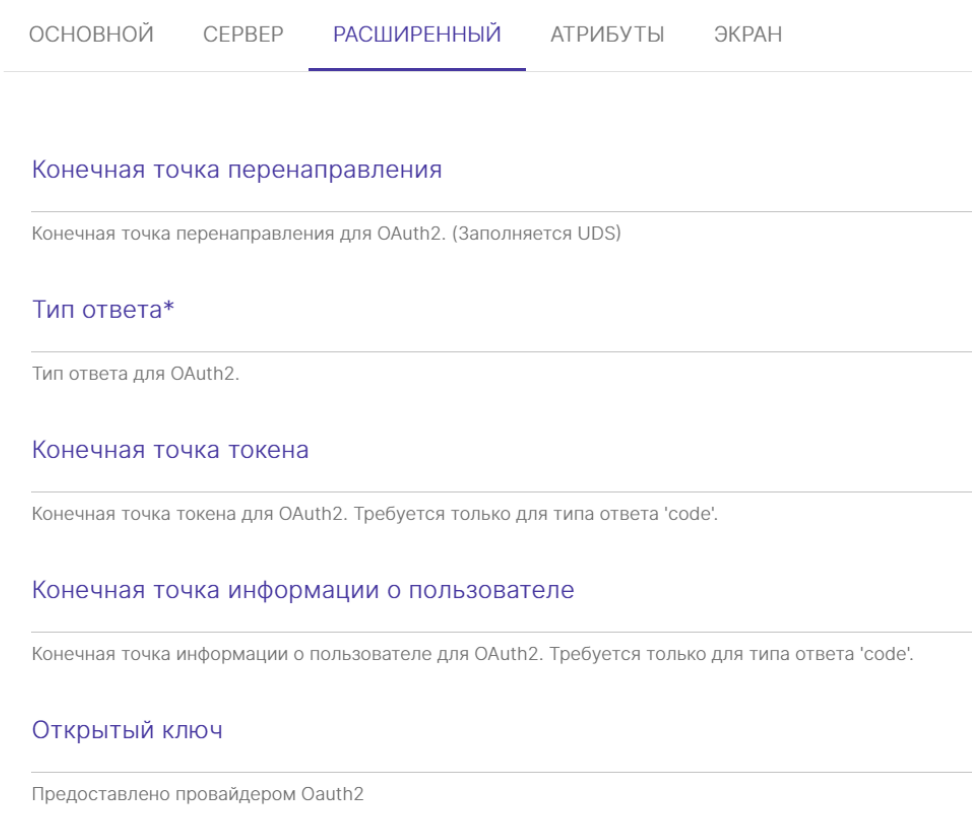


Рисунок 88

- **Конечная точка перенаправления.** Это URL внутри сервера VDI, на котором провайдер OAuth 2.0 будет перенаправлять браузер пользователя после успешного ввода учетных данных;
- **Тип ответа.** Определяет, как тип учетных данных VDI запрашивает у провайдера на первом этапе аутентификации;
- **Конечная точка токена**. URL-адрес провайдера, который VDI использует для обмена authorization code на access token и id token;
- **Конечная точка информации о пользователе**. URL-адрес API провайдера OAuth 2.0, который возвращает claims (утверждения) о аутентифицированном пользователе;
- **Открытый ключ.** Ключ или адрес для получения набора ключей (JWKS), которые используются для проверки подписи на id token, полученном от провайдера.

5. Вкладка **Атрибуты** (Рисунок 89) отвечает за извлечение конкретных данных о пользователе из полученных токенов или ответов API после успешной аутентификации через OAuth2:
   - **Атрибуты имени пользователя**. Определяет, из каких полей в структуре данных (например, в JWT id_token или ответе от userinfo endpoint) система должна извлечь логин пользователя;
   - **Атрибут имени группы.** Определяет, из какого поля в данных брать названия групп, членом которых является пользователь;
   - **Атрибут настоящего имени.** Определяет, из каких полей в данных извлекать отображаемое имя (ФИО) пользователя.

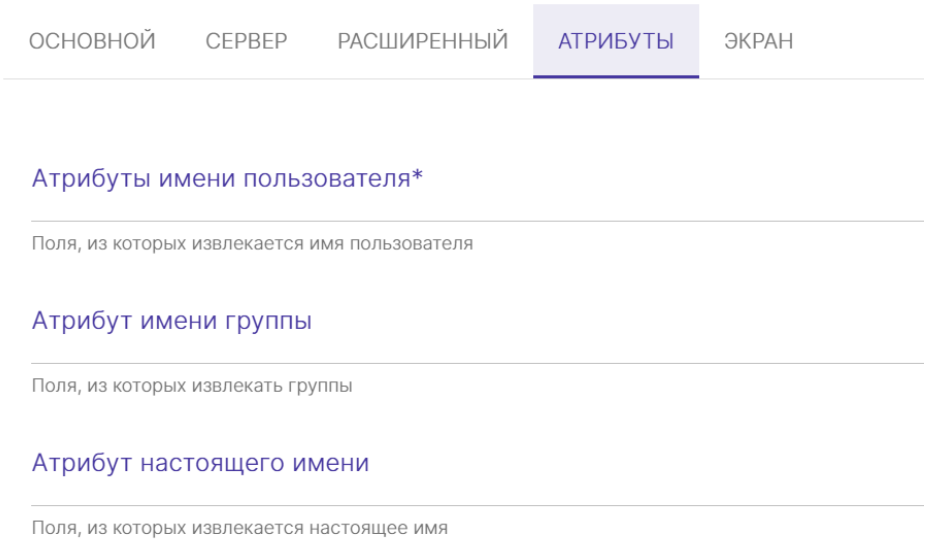


Рисунок 89

6. Вкладка **Экран** (Рисунок 90)**.** Настраивает видимость аутентификатора для пользователя.

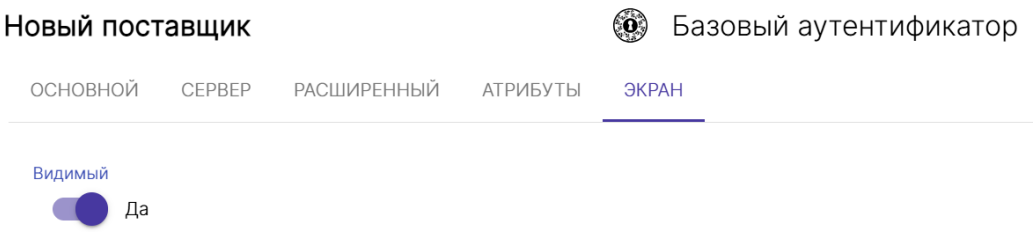


Рисунок 90

7. Для сохранения настроек нажать кнопку **Сохранить.**
8. Созданные аутентификатор будет отображен в списке.

5.2.3 IP Аутентификатор

Этот способ входа позволяет автоматически предоставлять доступ к рабочим столам и приложениям пользователям, которые подключаются с определенных IP-адресов, без необходимости вводить логин и пароль.

Для добавления IP-аутентификатора:

1. Перейти в раздел **Аутентификаторы**.
2. Нажать кнопку **Новый.**
3. Выбрать **IP**-аутентификатор. (Рисунок 91).

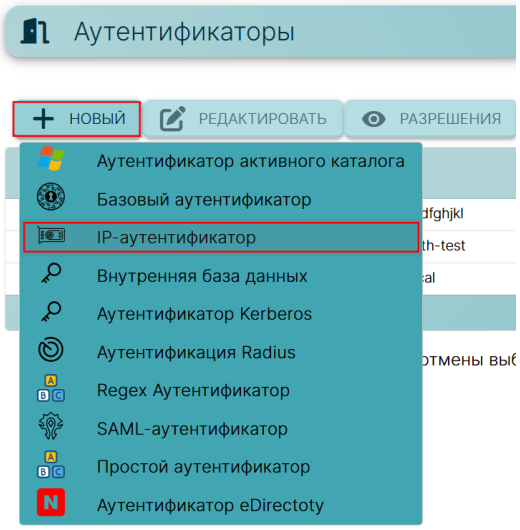


Рисунок 91

4. Откроется окно добавления поставщика. На вкладке **Основной** необходимо заполнить следующие поля:
   - **Тэги** (опционально). Метка для легкого поиска и фильтрации;
   - **Имя.** Уникальное имя для аутентификатора;
   - **Комментарии** (опционально). Необязательное текстовое поле для добавления информации;
   - **Приоритет.** Числовое поле для указания порядка, в котором система будем пытаться использовать этого поставщика;
   - **Метка.** Специфическая метка, используемая для группировки в механизме Metapool.
5. Вкладка **Расширенный.** Содержит настройки, которые непосредственно управляют логикой проверки Ip-адресов и видимостью аутентификатора в зависимости от сети, из которой пришел пользователь:
   - Опция **Принять прокси**. Если эта включена, VDI будет проверять специальные заголовки HTTP, которые прокси-серверы добавляют в запрос, чтобы передать реальный IP-адрес конечного пользователя;

– **Видно только из этих сетей.** Это поле позволяет ограничить видимость и саму попытку аутентификации через этот провайдер только для запросов, поступающих из определенных IP-сетей.

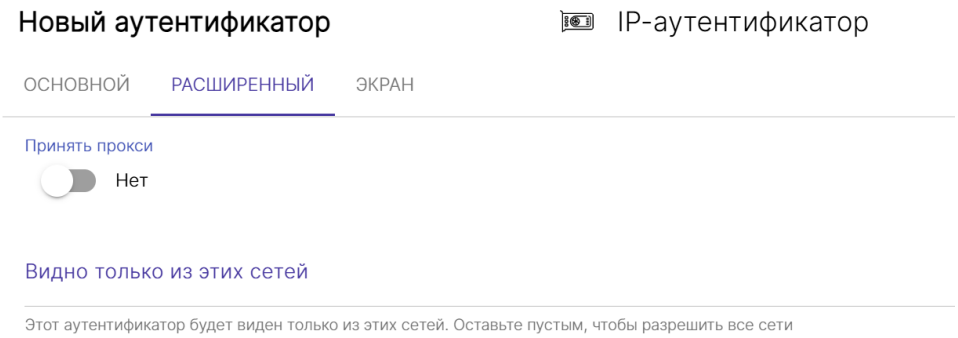


Рисунок 92

6. Вкладка **Экран** (Рисунок 93) управялет видимостью аутентификатора при выборе способа аутентификации в систему.

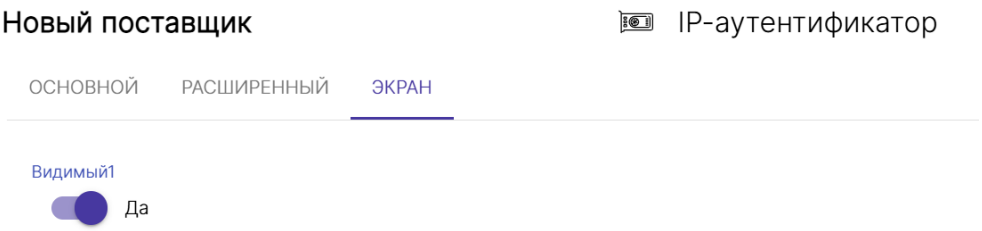


Рисунок 93

7. Нажать кнопку **Сохранить**.
8. Аутентификатор будет отображен в списке.

5.2.4 Внутренняя база данных

Аутентификатор **Внутреняя база данных** является встроенным и автономным способом управления пользователями.

Для создания аутентификатора необходимо:

1. Перейти в раздел **Аутентификаторы.**

2. Нажать кнопку **Новый.**

3. В списке выбрать **Внутренняя база данных** (Рисунок 94).

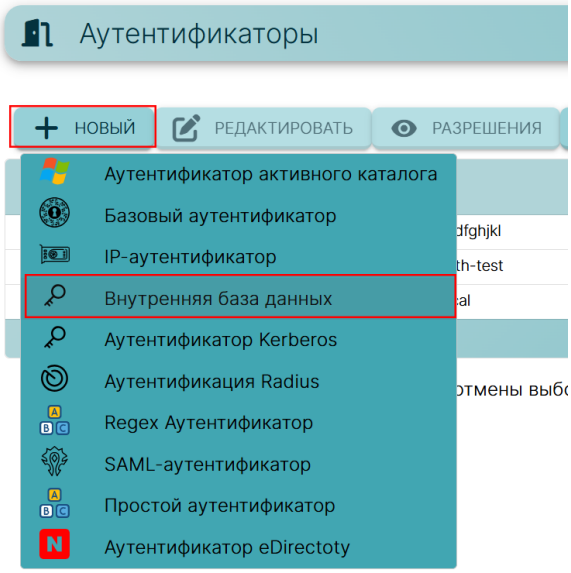


Рисунок 94

4. Откроется окно создания аутентификатора. Во вкладке **Основной** необходимо заполнить следующие поля:
   - **Тэги** (опционально). Поле для присвоения тэгов (меток) аутентификатору;
   - **Имя.** Уникальное имя для аутентификатора;
   - **Комментарии** (опционально). Необязательное текстовое поле для информации;
   - **Приоритет.** Числовое поле для указания порядка, в котором система будет пытаться использовать этого поставщика аутентификации;
   - **Метка.** Специфическая метка, используемая для группировки в механизме Metapool.
5. Вкладка **Расширенный** содержит дополнительные параметры:
   - **Разные пользователи для каждого хоста.** Опция определяет, создавать ли уникального пользователя для каждого отдельного IP-адреса или использовать одного общего пользователя для целого диапазона;

- **Обратный DNS.** Опция включает попытку преобразования IP-адреса подключившегося устройства в его сетевое имя (hostname) через службу обратного DNS-запроса;
- **Принять прокси.** Если опция включена, система будет проверять стандартные HTTP-заголовки (например, X-Forwarded-For), которые прокси-серверы используют для передачи реального IP-адреса конечного пользователя.

6. Для сохранения настроек нажать кнопку **Сохранить.**
7. Созданный аутентификатор будет отображен в списке.

5.2.5 Аутентификатор Kerberos

Аутентификатор Kerberos предназначен для интеграции с инфраструктурой Kerberos, которая является основой безопасности в доменах Active Directory. Он обеспечивает единый вход (Single Sign-On, SSO) для пользователей Windows.

Для создания:

1. Перейти в раздел **Аутентификаторы.**
2. Нажать кнопку **Новый.**
3. В списке выбрать **Аутентификатор Kerberos**.

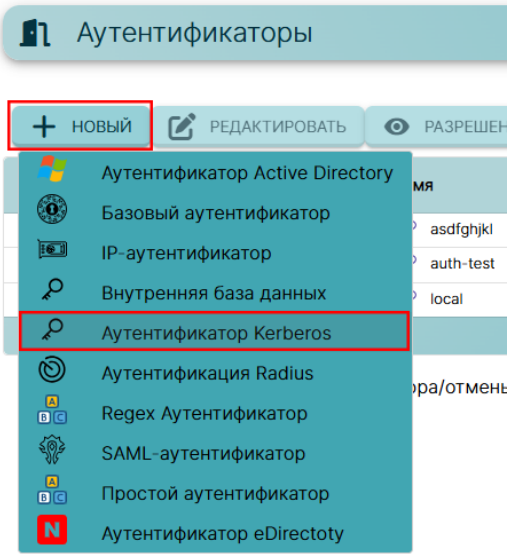


Рисунок 95

4. Откроется окно создания нового аутентификатора, вкладка **Основной**, где необходимо заполнить следующие поля:
   - **Тэги** (опционально). Поле для присвоения тэгов (меток) аутентификатору;
   - **Имя.** Уникальное имя аутентификатора;
   - **Комментарии** (опционально)**.** Необязательное текстовое поле для информации;
   - **Приоритет.** Числовое поле для указания порядка, в котором система будет пытаться использовать этого поставщика аутентификации;
   - **Метка.** Специфическая метка, используемая для группировки в механизме Metapool.
   - **SPN (Service Principal Name).**Уникальный идентификатор службы в домене Kerberos. SPN имеет строгий формат: HTTP/полное.имя.сервера.vdi@DOMAIN.LOCAL;
   - **Keytab в Base64.** Это файл, содержащий пароль (ключ) службы UDS в зашифрованном виде. Он используется для расшифровки билетов Kerberos, которые присылают пользователи;
   - **Хост.** IP-адрес или DNS-имя контроллера домена Active Directory (KDC - Key Distribution Center);
   - **Тайм-аут.** Максимальное время (в секундах), которое VDI будет ждать ответа от контроллера домена;
   - **Опция Использовать SSL.** Включает шифрование всего обмена данными между VDI и контроллером домена.
5. Вкладка **LDAPinfo** содержит параметры, которые сообщают VDI, как искать и идентифицировать пользователей и группы в структуре каталога Active Directory или другого LDAP-сервера. Настраиваемые параметры:
   - **Поле База (Search Base / Base DN).** Определяет стартовую точку (корень) в дереве LDAP, с которой VDI начнет поиск пользователей и групп. Формат: `DC=domain, DC=local` или `OU=Users, OU=Moscow, DC=domain, DC=local`;

5.2.6 Аутентификатор Radius

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

Для добавления аутентификатора Radius:

1. Перейти в раздел **Аутентификация -> Аутентификаторы.**
2. Нажать кнопку **Новый.**
3. Выбрать **Аутентификатор Radius.**

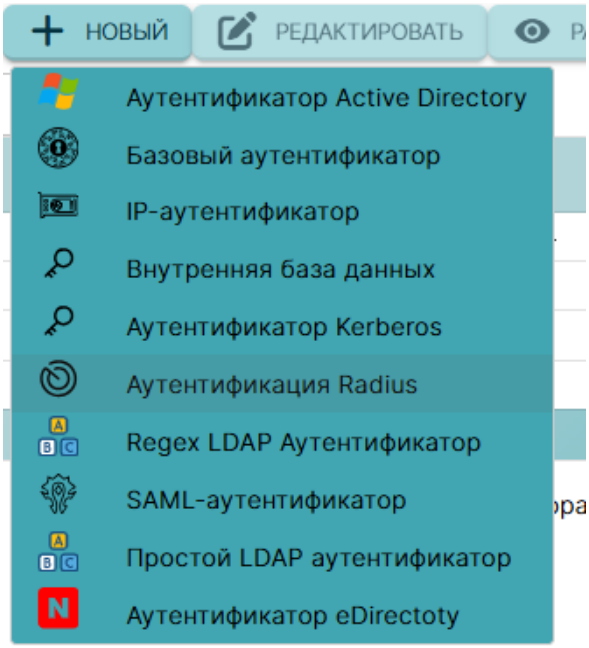


Рисунок 96

4. В открывшемся окне заполнить поля:
   - Имя;
   - Приоритет;
   - Метка;
   - Хост. IP-адрес или имя RADIUS-сервера;
   - Порт (по умолчанию 1812) порт связи с RADIUS-сервером;
   - Секрет. Строка проверки для RADIUS-сервера (определена на самом RADIUS-сервере).

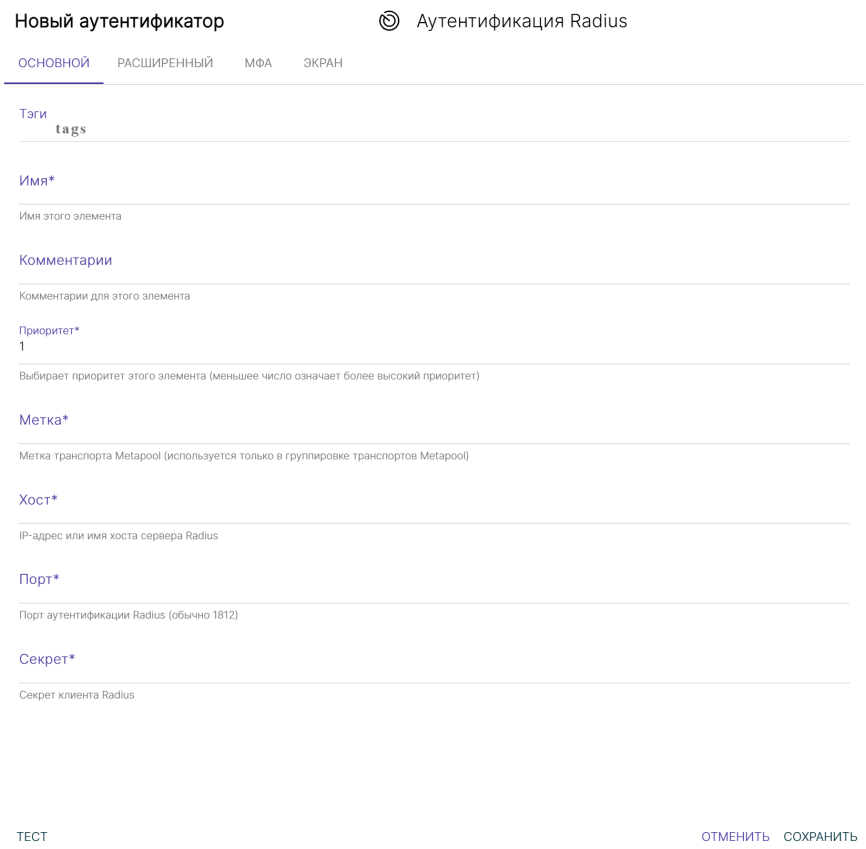


Рисунок 97

5. На вкладке **Расширенный** (Рисунок 98):

– **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).

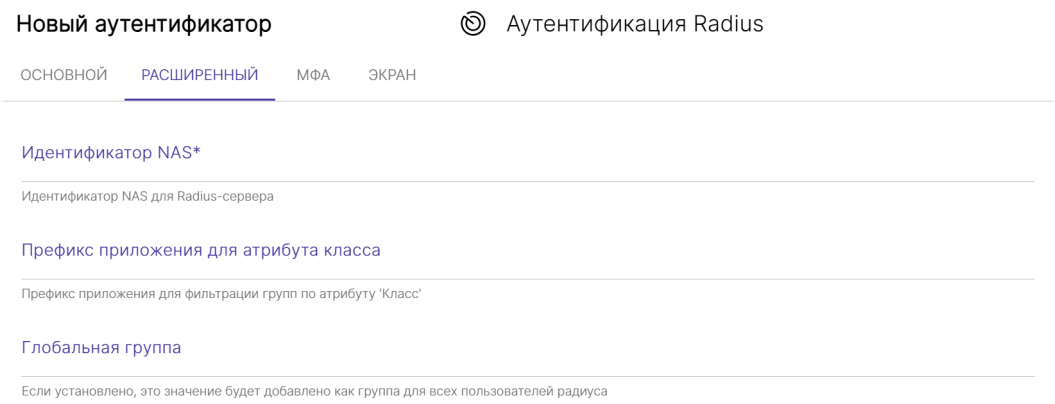


Рисунок 98

ПРИМЕЧАНИЕ:

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

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

6. На вкладке **МФА** (Рисунок 99):

– **Поставщик МФА**. Поле заполняется при настройке многофакторной аутентификации.

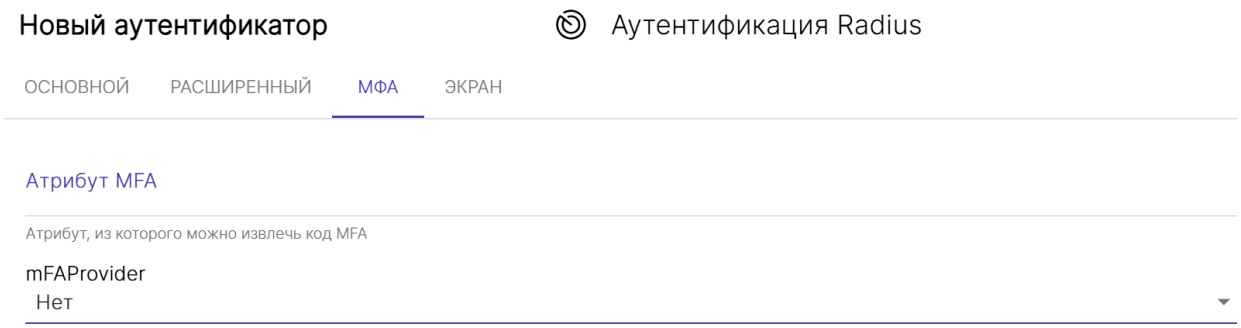


Рисунок 99

7. На вкладке «**Экран.** (Рисунок 100):

– **Видимый**. При включении аутентификатор не будет отображаться на странице входа в VDI.

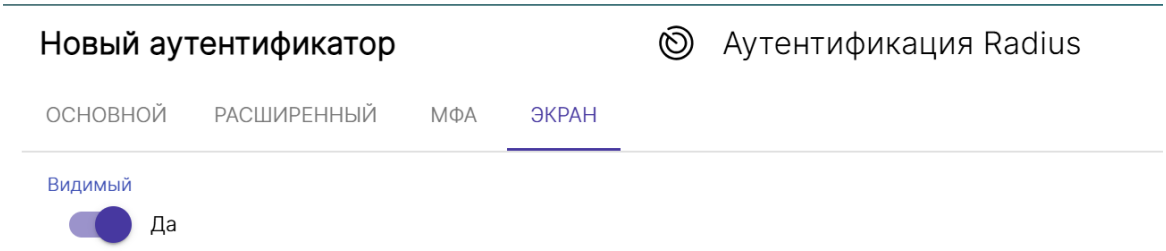


Рисунок 100

8. Нажать кнопку **Сохранить.**
9. Аутентификатор доступен в списке.

5.2.7 Regex LDAP Аутентификатор

Данный аутентификатор предназначен для интеграции с LDAP-серверами, имеющими нестандартную структуру каталога или атрибутов, когда стандартные методы поиска и фильтрации не подходят.

Для добавления аутентификатор Regex:

1. Перейти в **Аутентификация -> Аутентификаторы.**
2. Нажать кнопку **Новый.**

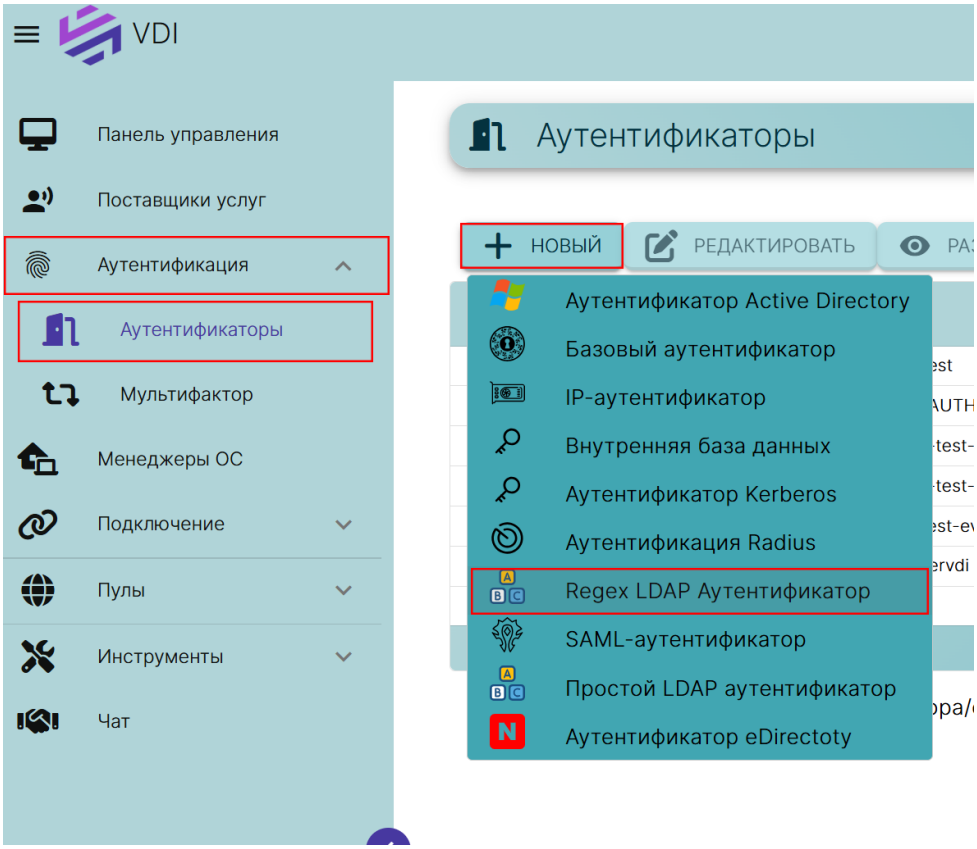


Рисунок 101

3. На вкладке **Основной** заполнить поля:

- **Имя***: Имя этого элемента.
- **Приоритет***: Определяет порядок попытки аутентификации (меньшее число означает более высокий приоритет).
- **Метка***: Метка транспорта Metapool (используется только для группировки транспортов в Metapool).
- **Хост***: IP-адрес или имя хоста сервера LDAP.
- **Порт***: Порт для подключения к серверу LDAP (по умолчанию 389).
- **Использовать SSL**: Опция для шифрования соединения (по умолчанию "Нет").
- **Тэги**: Произвольные теги для категоризации элемента.

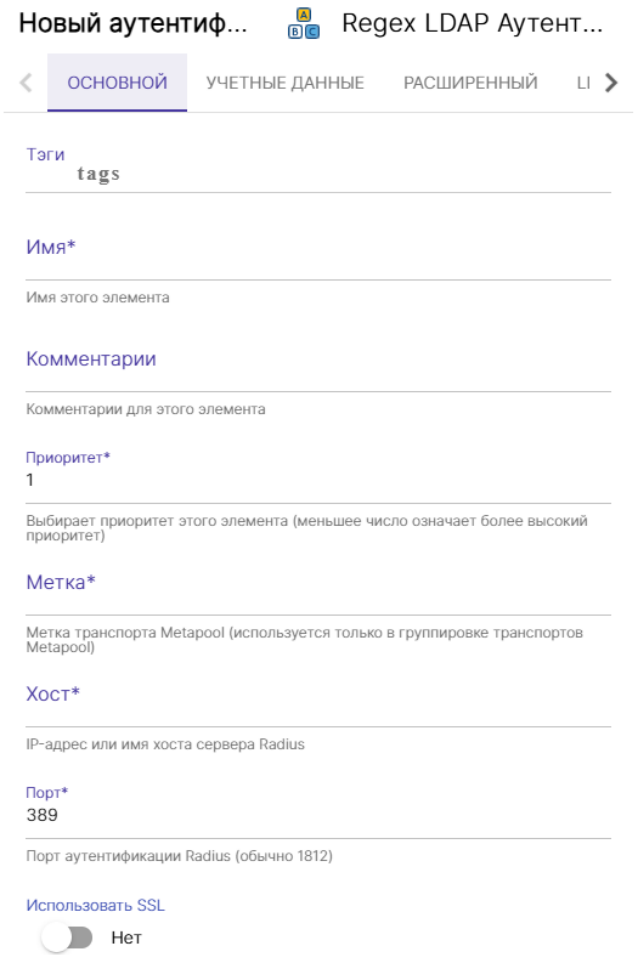


Рисунок 102

4. На вкладке **Учетные данные** заполнить поля:

- **Имя пользователя**: Учетная запись пользователя с правами чтения в LDAP. Необходимо использовать формат USER@DOMAIN.XXX.
- **Пароль**: Пароль для указанного пользователя LDAP.

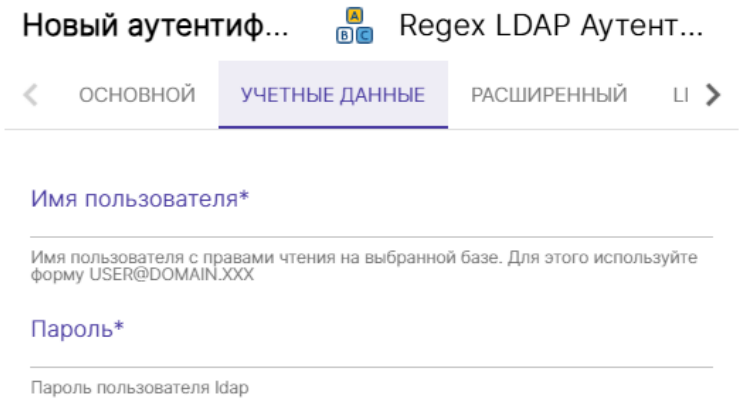


Рисунок 103

5. На вкладке **Расширенный** заполнить поля:

- **Тайм-аут**: Время ожидания подключения к серверу LDAP в секундах (по умолчанию 10).
- **Проверить сертификат**: Опция для проверки SSL-сертификата сервера (по умолчанию "Нет").
- **Сертификат**: Поле для загрузки сертификата, используемого для проверки SSL-подключения.
- **Альтернативный класс**: Дополнительный класс объектов LDAP, который также будет проверяться для извлечения групп (обычно не заполняется).

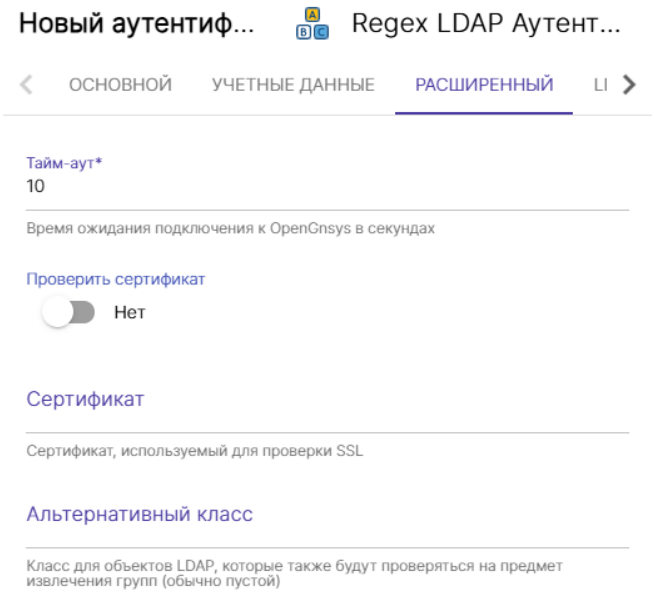


Рисунок 104

6. На вкладке **LDAPINFO** указать:

- **База***: Общая база поиска (Distinguished Name), используемая для поиска пользователей и групп.
- **Класс пользователя***: Класс LDAP, к которому относятся объекты-пользователи (обычно user или person).
- **Атрибут идентификатора пользователя***: Атрибут LDAP, содержащий уникальный идентификатор пользователя (например, sAMAccountName).

- **Атрибуты имени пользователя***: Поля LDAP, из которых извлекается отображаемое имя пользователя (например, displayName).
- **Атрибут имени группы***: Поле LDAP, из которого извлекаются названия групп.

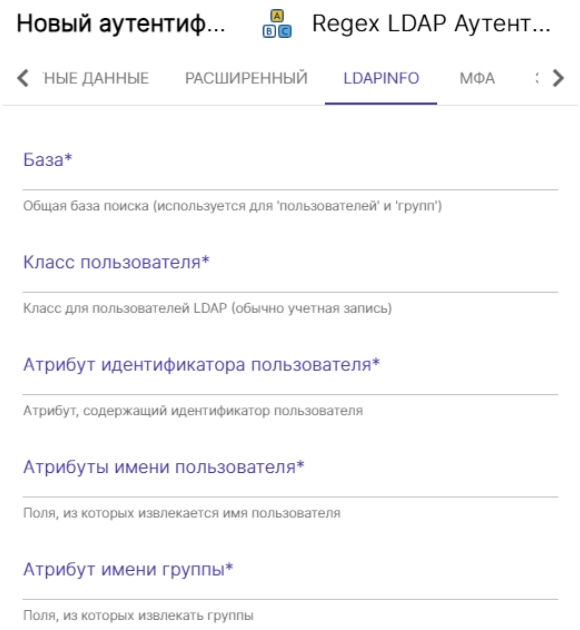


Рисунок 105

7. На вкладке **МФА** заполнить поля:

- **Атрибут MFA**: Атрибут LDAP, из которого можно извлечь код многофакторной аутентификации.
- **Поставщик МФА**: Выбор провайдера для настройки многофакторной аутентификации.

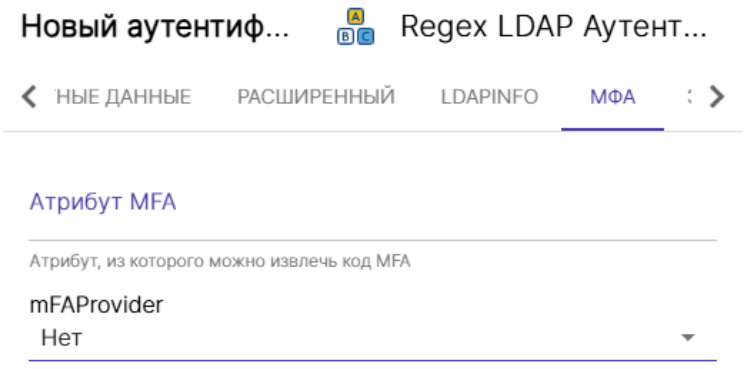


Рисунок 106

8. На вкладке **Экран** задать настройки видимости:

– **Видимый**: Если опция включена, аутентификатор не будет отображаться на странице входа в VDI.

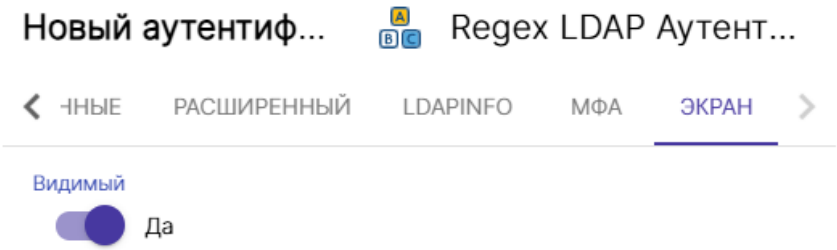


Рисунок 107

9. Нажать кнопку **Сохранить**.
10. Аутентификатор станет доступен в общем списке аутентификаторов.

5.2.8 SAML-аутентификатор

Внешний аутентификатор позволяет предоставлять доступ к виртуальным рабочим столам и приложениям для пользователей, используя протокол безопасности SAML (Security Assertion Markup Language) для федеративной аутентификации.

Для добавления SAML-аутентификатора:

1. Перейти в раздел **Аутентификация -> Аутентификаторы**.
2. Нажать кнопку **Новый**.
3. Выбрать **SAML-аутентификатор**.

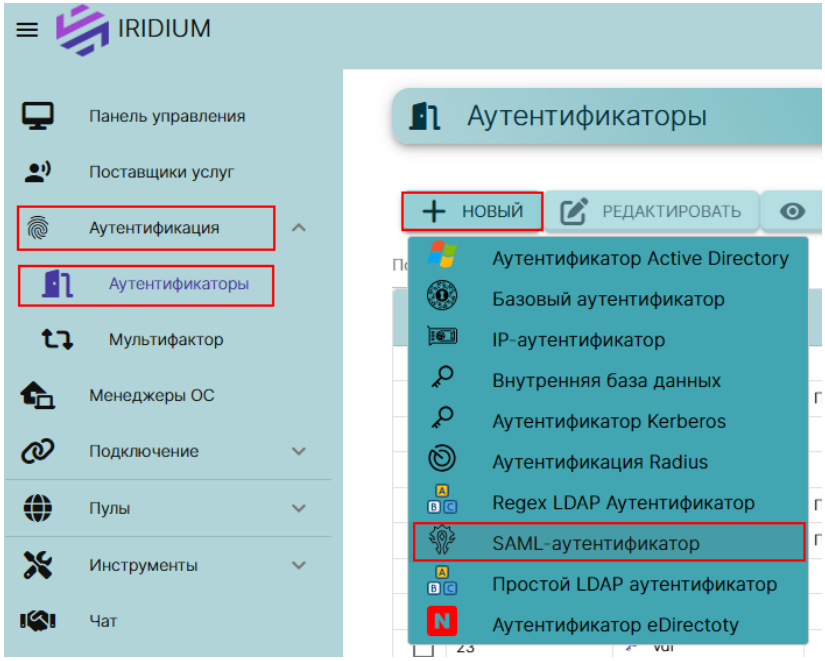


Рисунок 108

4. На вкладке **Основной** заполнить поля:
   - **Имя**: Имя этого элемента.
   - **Приоритет**: Определяет порядок попытки аутентификации (меньшее число означает более высокий приоритет).
   - **Метка**: Метка транспорта Metapool (используется только для группировки транспортов в Metapool).
   - **Тэги**: Произвольные теги для категоризации элемента.
   - **Комментарии**: Комментарии для этого элемента.

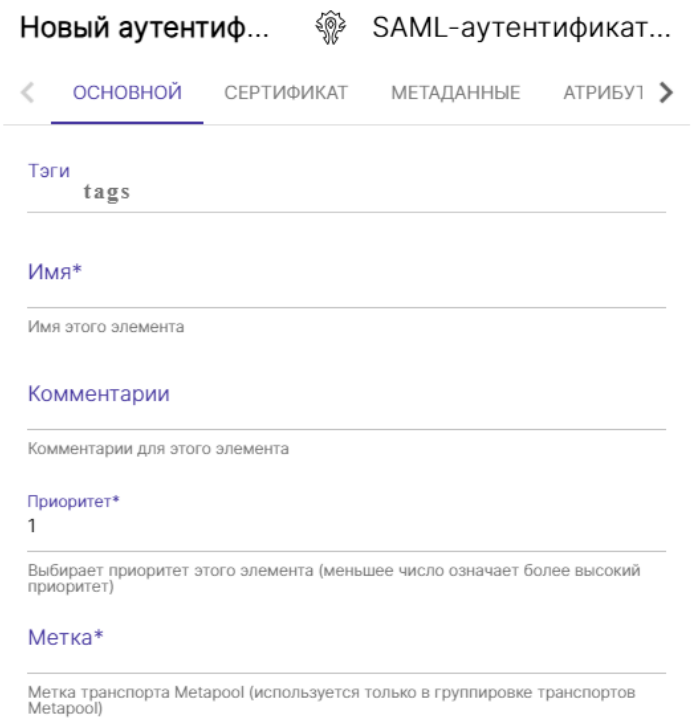


Рисунок 109

5. На вкладке **Сертификат** заполнить поля:
   - **Закрытый ключ**: Закрытый ключ, используемый для подписи и шифрования запросов, в формате Base64.
   - **Сертификат**: Сертификат сервера (поставщика услуг, SP), используемый в SAML, в формате Base64.

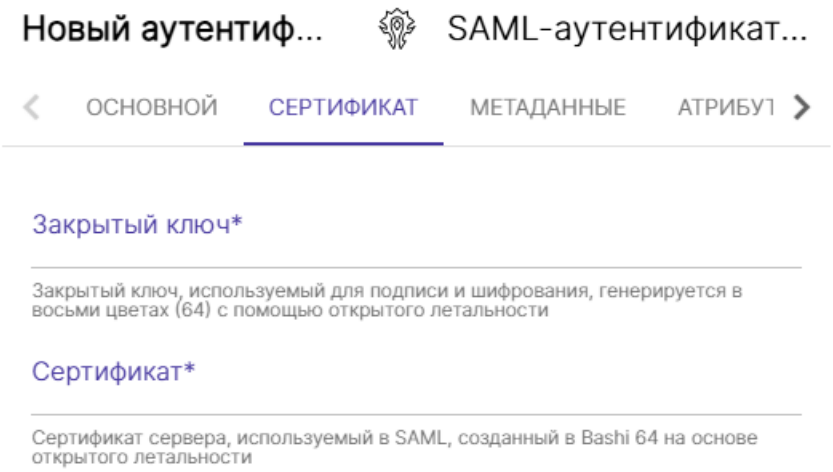


Рисунок 110

6. На вкладке **Метаданные** заполнить поля:

- **Метаданные IDP**: Можно ввести URL, по которому доступны метаданные поставщика удостоверений (IdP), или непосредственно XML-содержимое метаданных.
- **Идентификатор сущности**: Идентификатор сущности IdP (обычно указывается в метаданных).
- **Срок действия MetaData**: Срок действия метаданных в днях. Значение 0 означает значение по умолчанию (десять лет).
- **Длительность кэширования MetaData**: Длительность кэширования метаданных в днях. Значение 0 означает значение по умолчанию (десять лет).

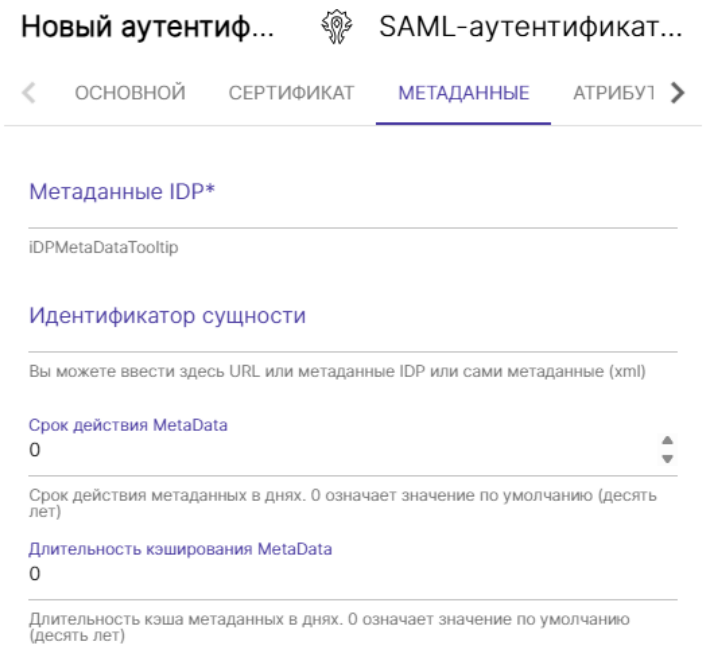


Рисунок 111

7. На вкладке **Атрибут** заполнить поля:
   - **Атрибуты имени пользователя**: Названия атрибутов (полей) из утверждения SAML, из которых извлекается логин пользователя.
   - **Атрибут имени группы**: Название атрибута из утверждения SAML, из которого извлекаются группы пользователя.
   - **Атрибут настоящего имени**: Названия атрибутов из утверждения SAML, из которых извлекается отображаемое имя (ФИО) пользователя.

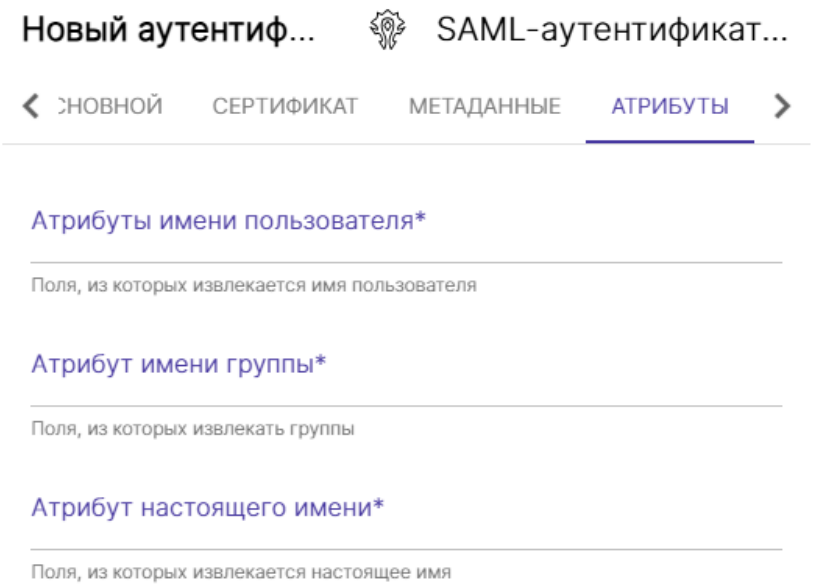


Рисунок 112

8. На вкладке **Расширенный** настроить дополнительные параметры:
   - **Глобальный выход**: При включении обеспечивает выход из всех приложений при выходе из VDI.
   - **Совместимость с ADFS**: Опция для включения специальных настроек совместимости с Microsoft Active Directory Federation Services.

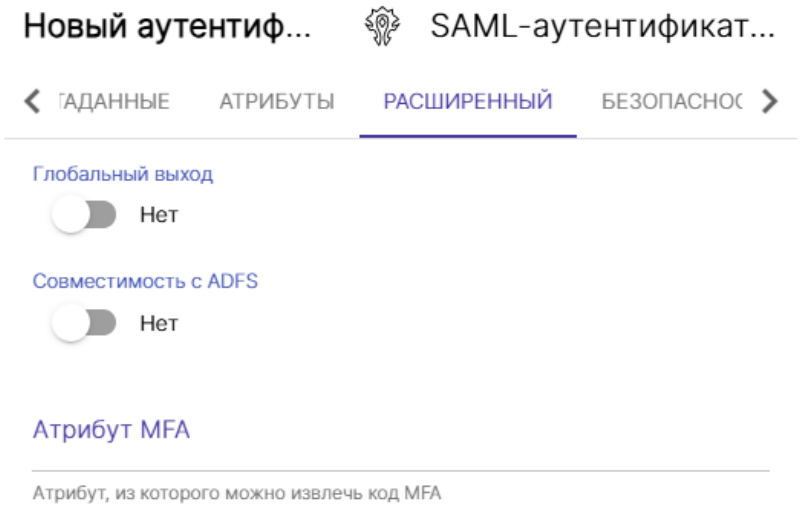


Рисунок 113

9. На вкладке **Безопасность** настроить параметры подписи и шифрования (все опции по умолчанию отключены):
   - **Зашифрованный идентификатор имени;**

- **Запросы аутентификации подписаны;**
- **Запрос на выход подписан;**
- **Ответы на выход подписаны;**
- **Подписать метаданные;**
- **Хочу, чтобы сообщения были подписаны;**
- **Хочу, чтобы утверждения были подписаны;**
- **Хотите зашифровать утверждения;**
- **Хочу зашифровать NameID;**
- **Запрошенный контекст аутентификации;**
- **Разрешить устаревшие алгоритмы подписи;**
- **Проверить SSL-сертификат.**

10. На вкладке **Организация** заполнить информацию для метаданных поставщика услуг (SP):
    - **Название организации**: Название организации для использования в метаданных SAML SP.
    - **Отображаемое имя организации**: Отображаемое имя организации для использования в метаданных SAML SP.
    - **URL организации**: URL-адрес организации для использования в метаданных SAML SP.

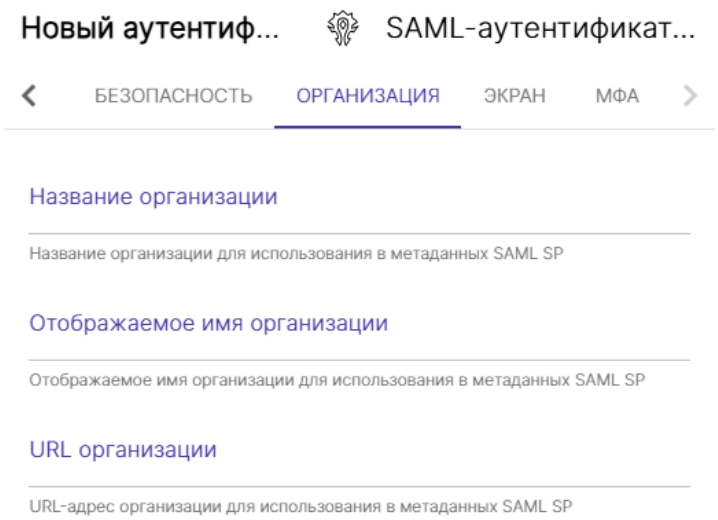


Рисунок 114

11. На вкладке **Экран** задать настройки видимости:

– **Видимый**: Если опция включена, аутентификатор не будет отображаться на странице входа в VDI.

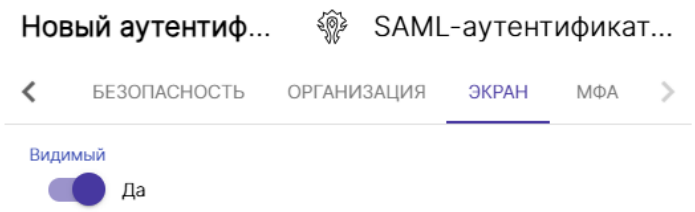


Рисунок 115

12. На вкладке **МФА** заполнить поля:
    – **Поставщик МФА**: Выбор провайдера для настройки многофакторной аутентификации.

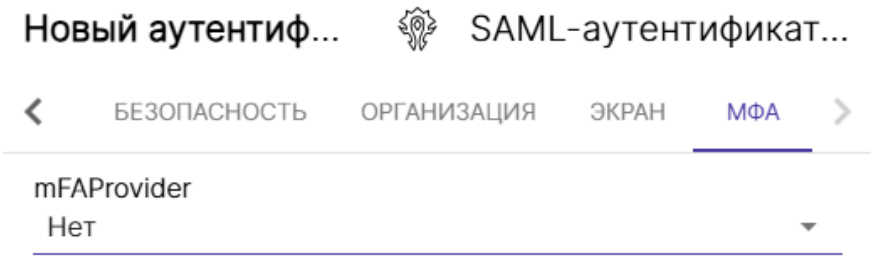


Рисунок 116

13. Нажать кнопку **Сохранить**.
14. Аутентификатор станет доступен в общем списке аутентификаторов.

5.2.9 Простой аутентификатор

Этот внешний аутентификатор позволяет предоставлять доступ к виртуальным рабочим столам и приложениям для пользователей, проходящих проверку подлинности на сервере LDAP, используя упрощенную конфигурацию.

Для добавления простого LDAP аутентификатора:

1. Перейти в раздел **Аутентификация -> Аутентификаторы**.
2. Нажать кнопку **Новый**.
3. Выбрать **Простой LDAP аутентификатор**.

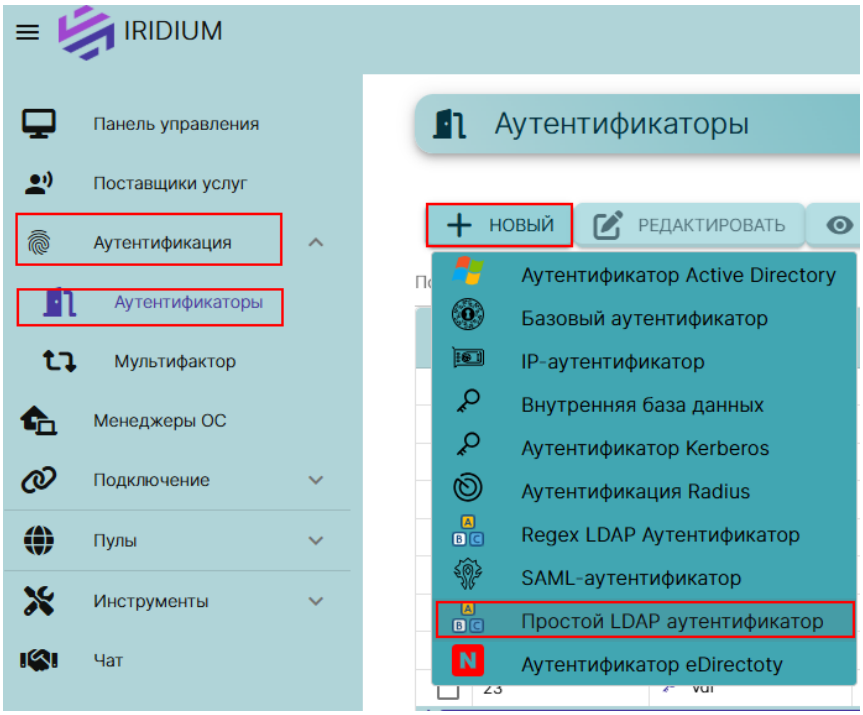


Рисунок 117

4. На вкладке **Основной** заполнить поля:

– **Имя**: Имя этого элемента.
– **Приоритет**: Определяет порядок попытки аутентификации (меньшее число означает более высокий приоритет).
– **Метка** Метка транспорта Metapool (используется только для группировки транспортов в Metapool).
– **Хост** IP-адрес или имя хоста сервера LDAP.
– **Порт** Порт для подключения к серверу LDAP (обычно 389 для не-SSL и 636 для SSL).
– **Использовать SSL**: Опция для шифрования соединения.
– **Тэги**: Произвольные теги для категоризации элемента.
– **Комментарии**: Комментарии для этого элемента.

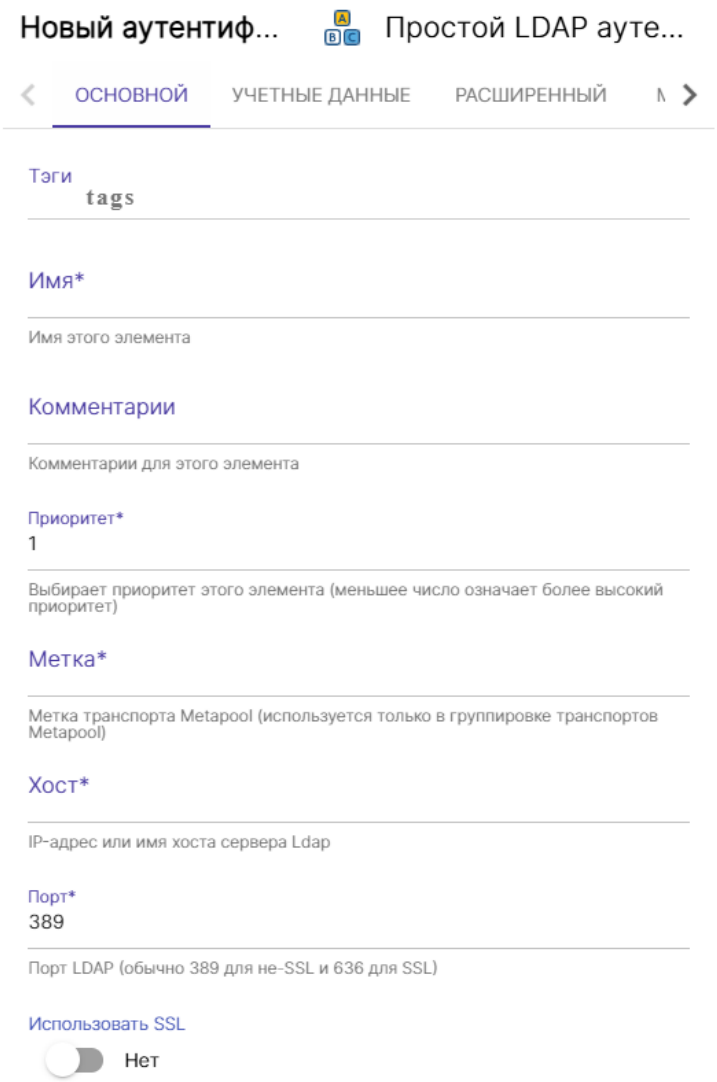


Рисунок 118

5. На вкладке **Учетные данные** заполнить поля:

– **Имя пользователя**: Учетная запись пользователя с правами чтения в LDAP. Необходимо использовать формат `USER@DOMAIN.XXX`.
– **Пароль**: Пароль для указанного пользователя LDAP.

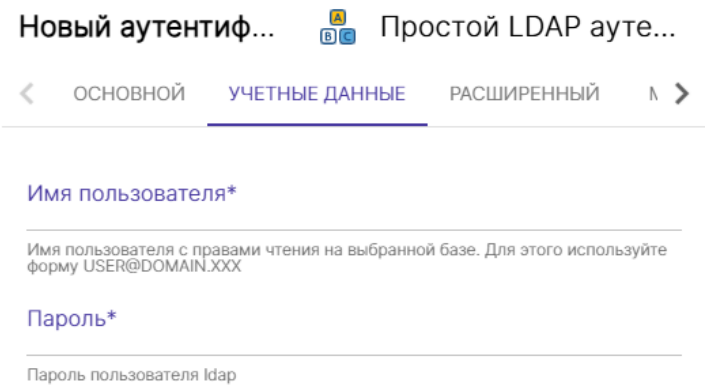


Рисунок 119

6. На вкладке **Расширенный** заполнить поля:

– **Тайм-аут**: Время ожидания подключения к серверу LDAP в секундах (по умолчанию 10).
– **Проверить сертификат**: Опция для проверки SSL-сертификата сервера (по умолчанию "Нет").
– **Сертификат**: Поле для загрузки сертификата, используемого для проверки SSL-подключения.

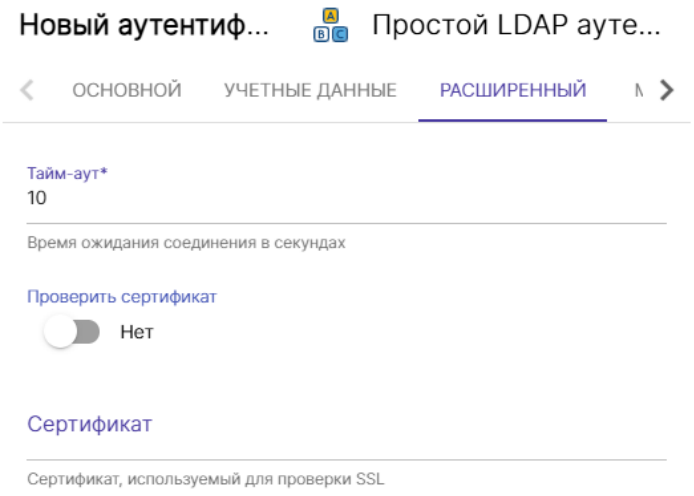
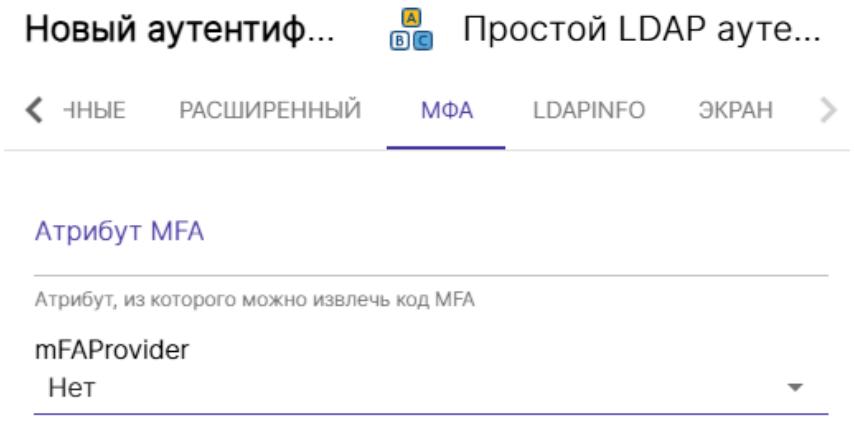


Рисунок 120

7. На вкладке **МФА** заполнить поля:

– **Атрибут MFA**: Атрибут LDAP, из которого можно извлечь код многофакторной аутентификации.

– **Поставщик МФА**: Выбор провайдера для настройки многофакторной аутентификации.



8. На вкладке **LDAPINFO** заполнить поля для связи с объектами в LDAP:

– **База**: Общая база поиска (Distinguished Name), используемая для поиска пользователей и групп.
– **Класс пользователя**: Класс LDAP, к которому относятся объекты-пользователи (обычно `account`).
– **Атрибут идентификатора пользователя**: Атрибут LDAP, содержащий уникальный идентификатор пользователя (например, `uid`).
– **Атрибуты имени пользователя**: Поля LDAP, из которых извлекается отображаемое имя пользователя.
– **Групповой класс**: Класс LDAP, к которому относятся объекты-группы (обычно `groupOfNames`).
– **Атрибут идентификатора группы**: Атрибут LDAP, содержащий уникальный идентификатор группы.
– **Атрибут членства в группе**: Атрибут группы, который содержит список членов (например, `member`).

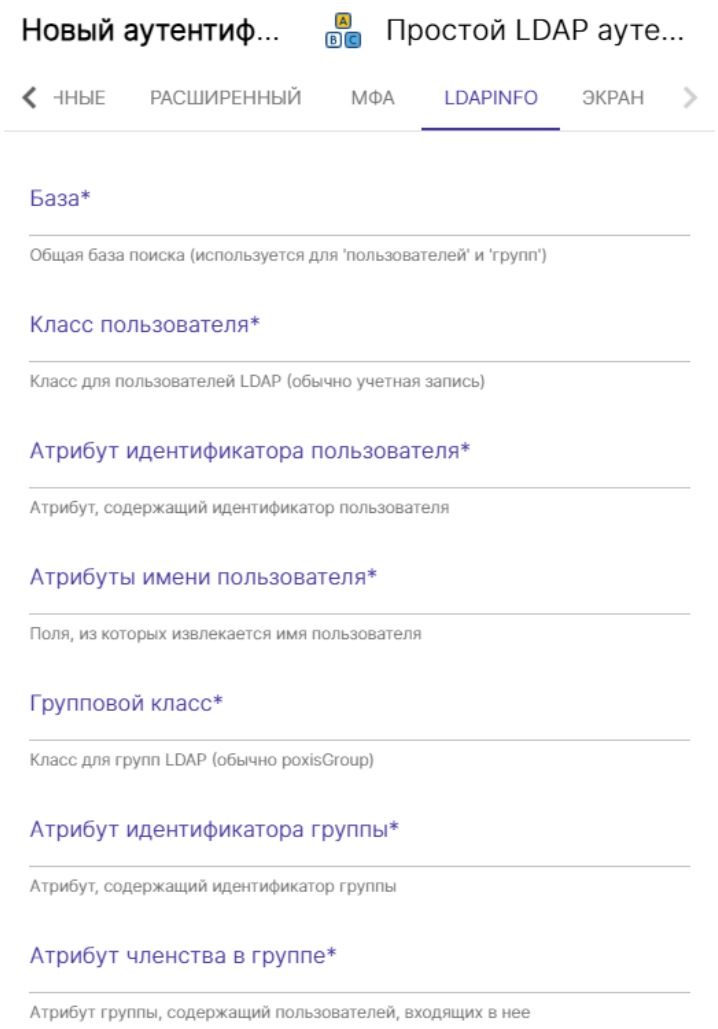


Рисунок 121

9. На вкладке **Экран** задать настройки видимости:

– **Видимый**: Если опция включена, аутентификатор не будет отображаться на странице входа в VDI.

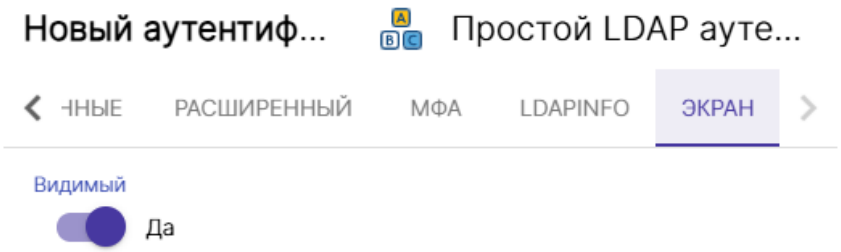


Рисунок 122

10. Нажать кнопку **Сохранить**.
11. Аутентификатор станет доступен в общем списке аутентификаторов.

5.2.10 Аутентификатор eDirectory

Этот внешний аутентификатор позволяет предоставлять доступ к виртуальным рабочим столам и приложениям для пользователей, проходящих проверку подлинности в службе Novell eDirectory.

Для добавления аутентификатора eDirectory:

1. Перейти в раздел **Аутентификация -> Аутентификаторы**.
2. Нажать кнопку **Новый**.
3. Выбрать **Аутентификатор eDirectory**.

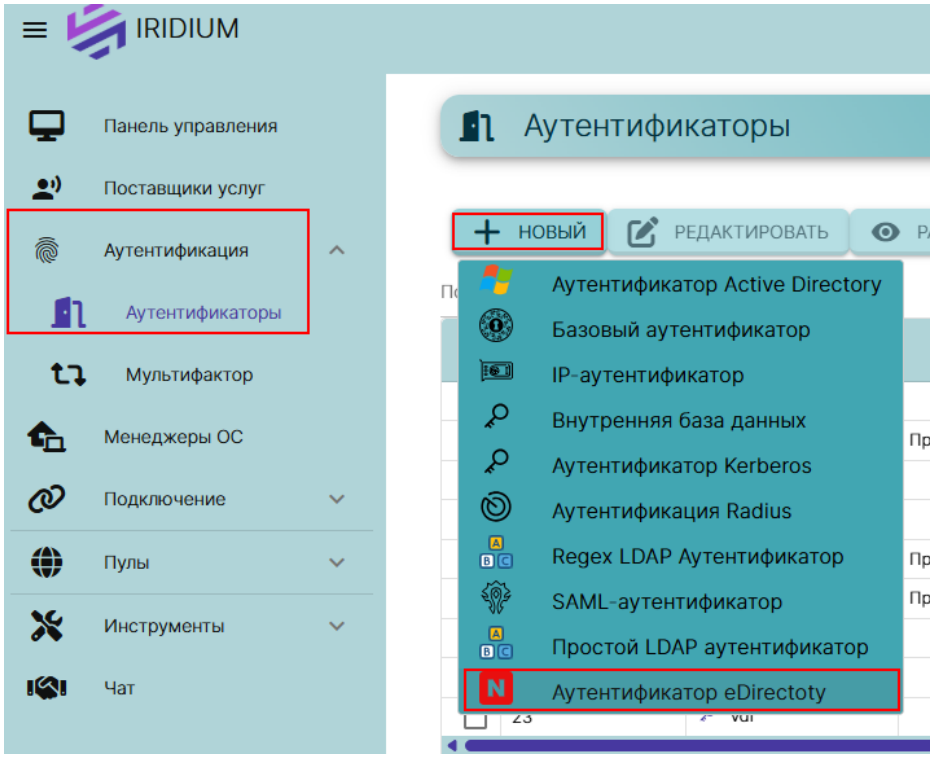


Рисунок 123

4. На вкладке Основной заполнить поля:

– **Имя**: Имя этого элемента.
– **Приоритет**: Определяет порядок попытки аутентификации (меньшее число означает более высокий приоритет).
– **Метка**: Метка транспорта Metapool (используется только для группировки транспортов в Metapool).

- **Хост**: IP-адрес или имя хоста сервера eDirectory.
- **Порт**: Порт для подключения к серверу eDirectory (обычно 389 для не-SSL и 636 для SSL).
- **Использовать SSL**: Опция для шифрования соединения (по умолчанию "Нет").
- **Тайм-аут**: Время ожидания подключения к серверу eDirectory в секундах (по умолчанию 10).
- **Тэги**: Произвольные теги для категоризации элемента.
- **Комментарии**: Комментарии для этого элемента.

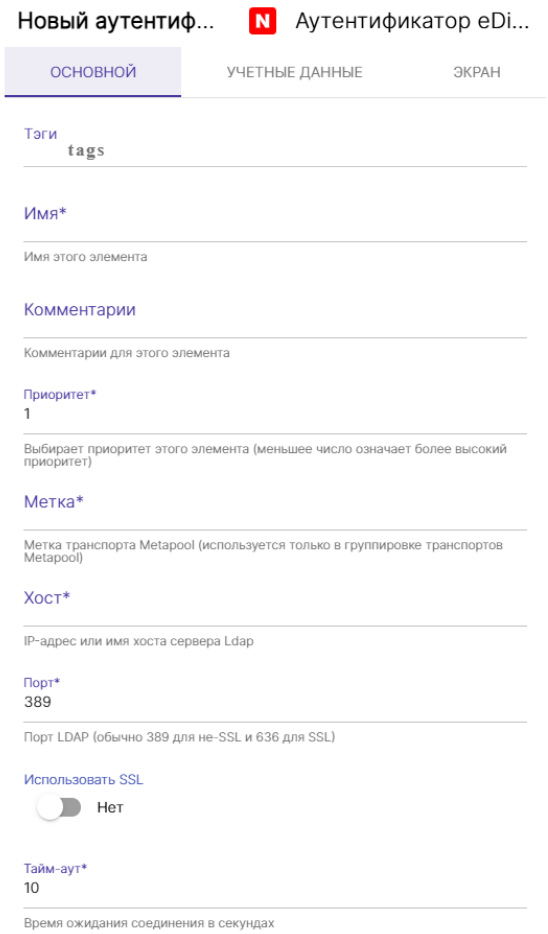


Рисунок 124

5. На вкладке **Учетные данные** заполнить поля:
   - **Имя пользователя**: Учетная запись пользователя с правами чтения в eDirectory.

– **Пароль**: Пароль для указанного пользователя eDirectory.

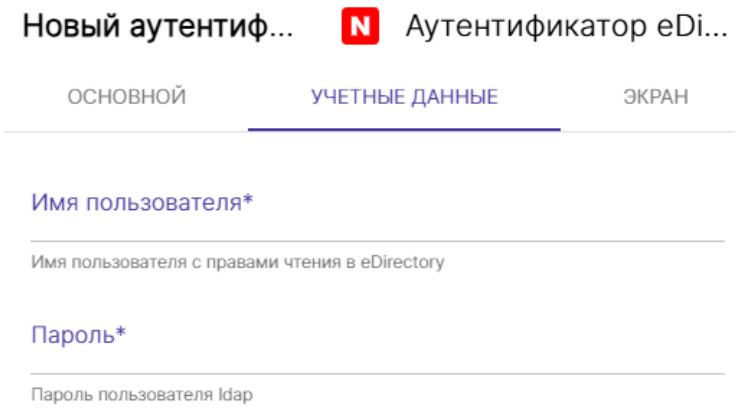


Рисунок 125

6. На вкладке **Экран** задать настройки видимости:
   – **Видимый**: Если опция включена, аутентификатор не будет отображаться на странице входа в VDI.

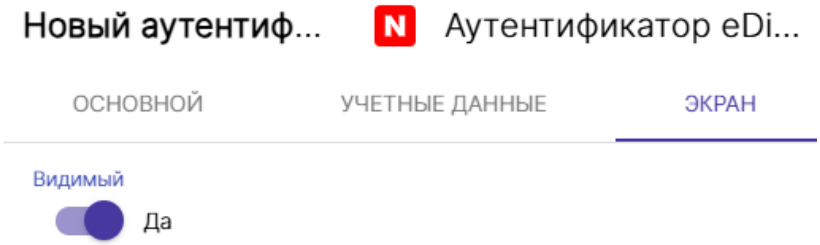


Рисунок 126

7. Нажать кнопку **Сохранить**.
8. Аутентификатор станет доступен в общем списке аутентификаторов.

5.2.11 Настройка многофакторной аутентификации

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

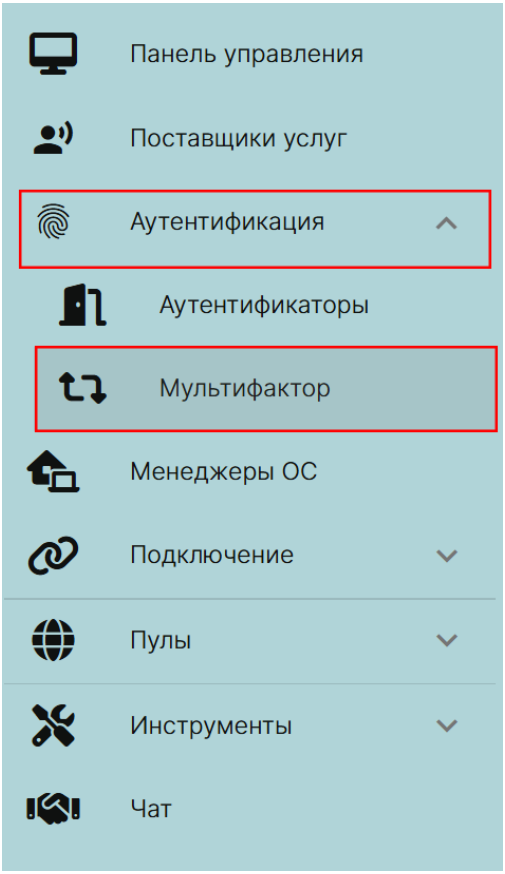


Рисунок 127

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

VDI изначально поддерживает несколько систем многофакторной аутентификации:

- Многофакторная электронная почта;
- Радиус OTP Challenge;
- Смс через HTTP;
- TOTP на основе MFA.

Чтобы настроить многофакторную аутентификацию необходимо:

1. перейти в пункт меню **Аутентификация - Многофакторный**.
2. Далее нажать кнопку **Новый**.
3. Выбрать из списка нужную строку.

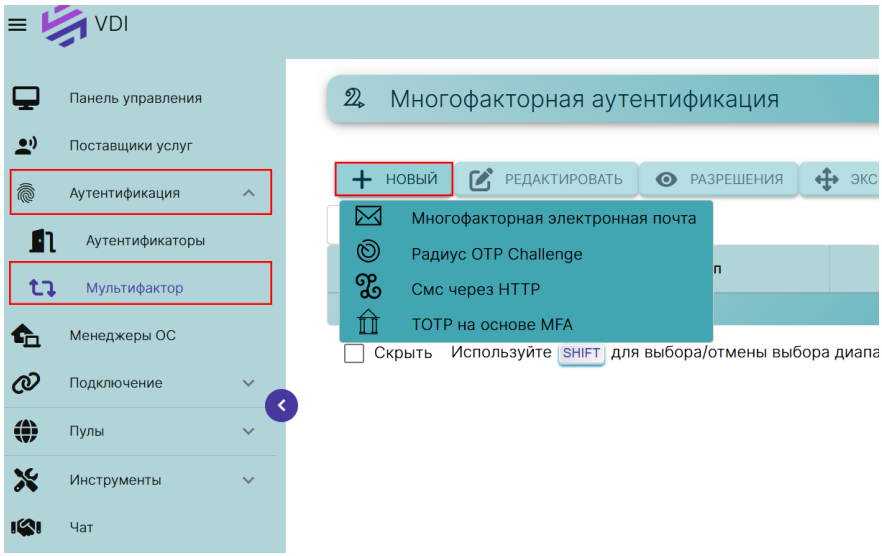


Рисунок 128

Многофакторная конфигурация не является необходимым компонентом для создания Пула услуг.

5.2.11.1 *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.

Для создания аутентификатора на основе многофакторной электронной почты необходимо:

1. В списке способов создания МФА нажать **Новый -> Многофакторная электронная почта.**

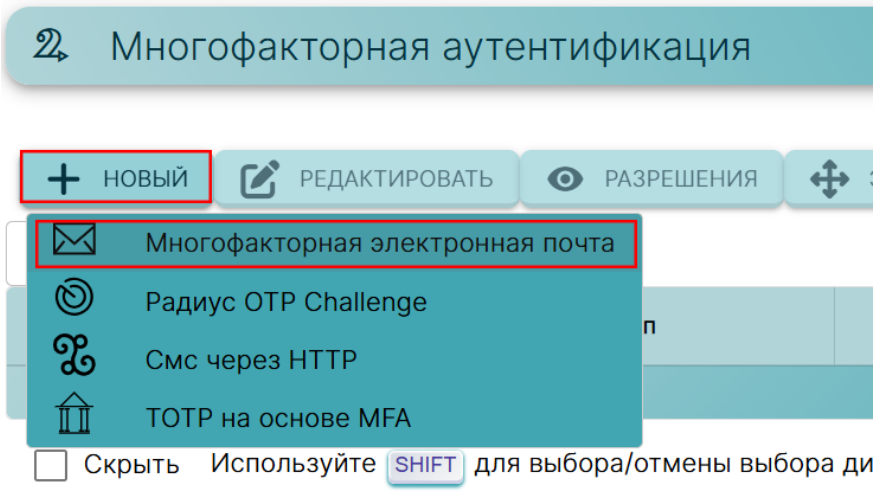


Рисунок 129

2. В открывшемся окне заполнить поля:
   - **Имя.** Обязательное поле для имени аутентификатора;
   - **Тэги.** Необязательное текстовое поле для тэгов;
   - **Комментарии.** Необязательное текстовое поле для заметок;
   - **Кэширование устройства.** Поле нужно для того, чтобы пользователю не приходилось проходить многофакторную аутентификацию заново каждый раз при входе на одном и том же доверенном устройстве.
   - **Действительность кода МФА.** Время в минутах, в течение которого можно использовать код MFA.

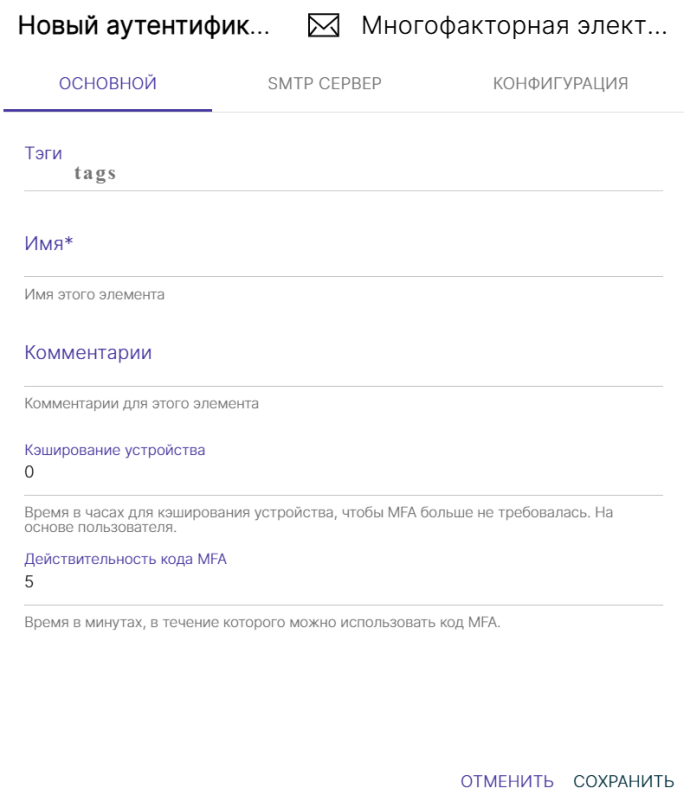


Рисунок 130

3. На вкладке **SMTP-сервер** (Рисунок 131) заполнить:

– **SMTP Хост**. Обязательное поле для ввода имени хоста или IP-адреса SMTP-сервера, через который будет отправляться многофакторная электронная почта.
– **Безопасность**. Выпадающий список для выбора типа безопасности соединения с SMTP-сервером (например, TLS).
– **Имя пользователя**. Поле для ввода имени пользователя, которое используется для аутентификации на SMTP-сервере.

– **Пароль**. Поле для ввода пароля пользователя с доступом к SMTP-серверу.

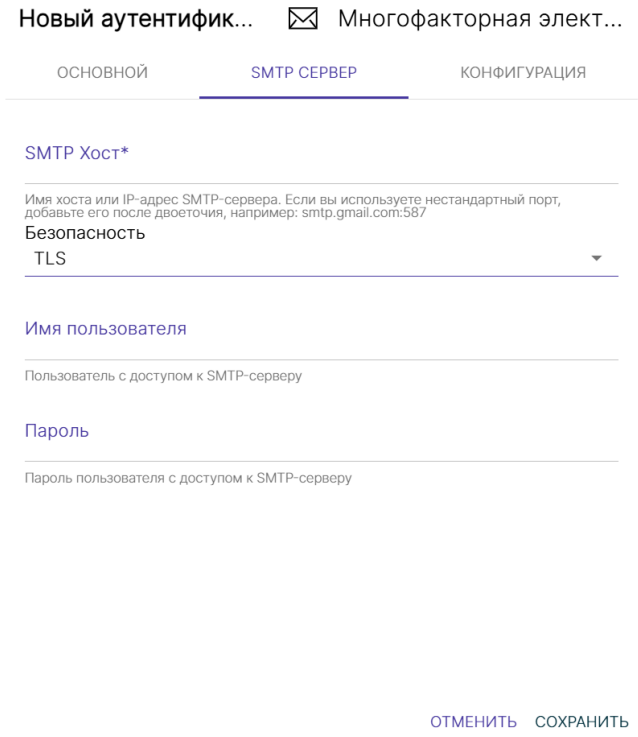


Рисунок 131

4. На вкладке «Конфигурация» (Рисунок 132):

– **Тема**. Обязательное поле для ввода темы письма, которое будет отправляться пользователю для многофакторной аутентификации.
– **Из электронной почты**. Обязательное поле для указания адреса электронной почты отправителя, который будет отображаться в письмах MFA
– **HTML режим**. Переключатель для выбора формата письма: если активирован, письмо будет отправляться в формате HTML, если выключен — в обычном текстовом формате.
– **Пользователь без политики MFA**. Обязательное поле для выбора пользователя, которому будет применяться данный механизм многофакторной аутентификации в случае отсутствия заданной политики MFA.
– **OTP Сети**. Выпадающий список для выбора сетей одноразовых паролей (OTP), которые будут использоваться данным аутентификатором.

– **Текст письма**. Обязательное поле для ввода основного текста письма. Если оставить пустым, будет использоваться текст по умолчанию.
– **Почта HTML**. Альтернативный HTML-шаблон письма. Если не заполнено, будет применяться стандартный HTML-текст по умолчанию.

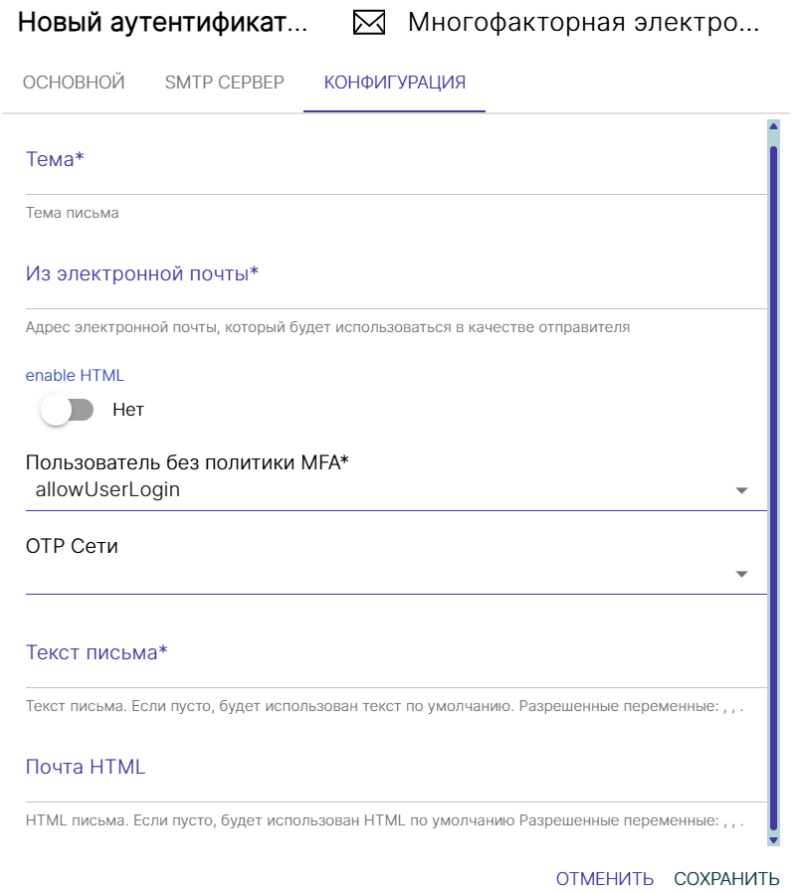


Рисунок 132

5. Нажать кнопку **Сохранить.**

5.2.11.2 *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.

Для создания аутентификатора Radius OTP Challenge:

1. Перейти в раздел **Аутентификация – Мультифактор**.

2. Нажать кнопку **Новый**, выбрать **Radius OTP Challenge.**

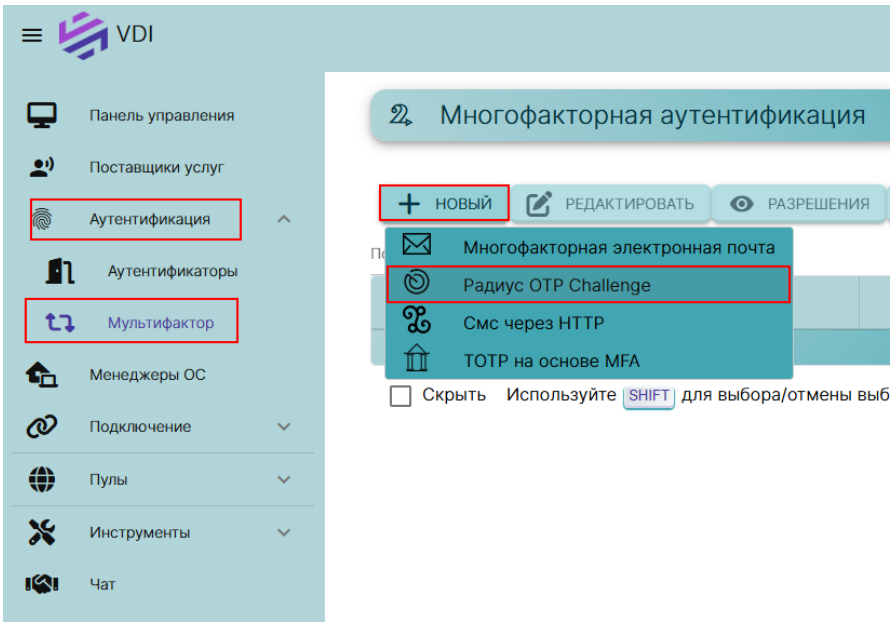


Рисунок 133

3. На вкладке **Основной** заполнить поля (Рисунок 134):

- **Тэги**. Используются для классификации и поиска настроек аутентификатора среди других элементов системы
- **Имя**. Обязательное поле для ввода уникального имени аутентификатора.
- **Комментарии**. Поле для внесения дополнительных пояснений или описания назначения аутентификатора.
- **Хост**. Обязательное поле для ввода IP-адреса или имени хоста сервера Radius, через который осуществляется аутентификация.
- **Порт**. Поле для ввода номера порта аутентификации Radius. По умолчанию используется порт 1812.
- **Секрет**. Обязательное поле для ввода общего секрета клиента Radius, необходимого для установления защищённого соединения.
- **Все пользователи должны отправить OTP**. Переключатель для активации обязательной отправки одноразового пароля (OTP) всеми пользователями при аутентификации через Radius.
- **Идентификатор NAS**. Обязательное поле для ввода идентификатора NAS (Network Access Server), который используется на стороне Radius-сервера.

– **Кэширование устройства**. Настройка времени (в часах), в течение которого устройство будет считаться доверенным без запроса повторной MFA.
– **Действительность кода MFA**. Установка срока действия одноразового кода многофакторной аутентификации в минутах.

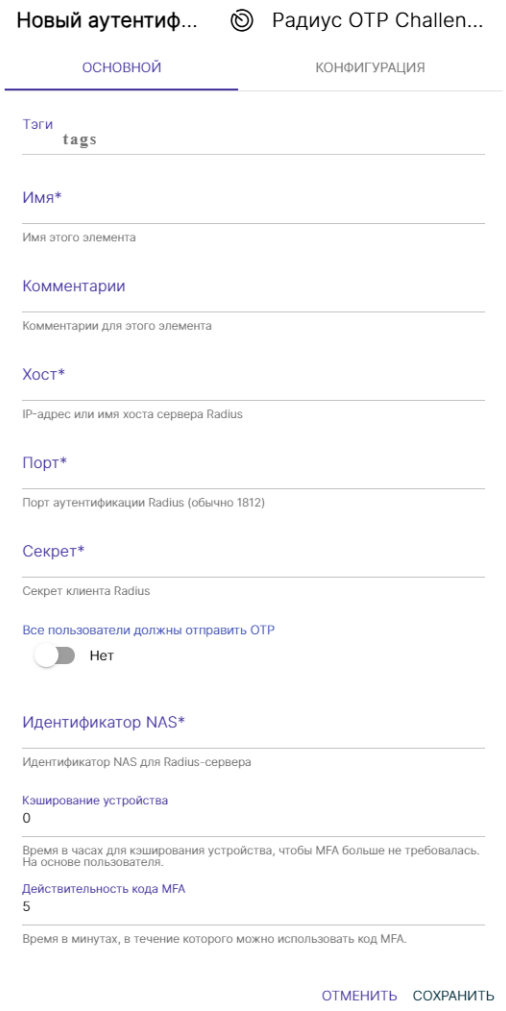


Рисунок 134

4. На вкладке **Конфигурация** заполнить поля (Рисунок 135):

– **Radius OTP — Действие при ошибке связи**. Обязательное поле для выбора действия в случае недоступности сервера Radius:
  - *Разрешить вход пользователю* — Пользователь будет допущен в систему без проверки через Radius.
  - *Запретить вход пользователя* — Вход пользователя будет запрещён.

- *Разрешить пользователю входить в систему, если его IP-адрес есть в списке сетей* — Пользователь сможет войти только при наличии его IP-адреса в разрешённых сетях.
- *Запретить пользователю вход в систему, если его IP-адрес есть в списке сетей* — Пользователь не сможет войти, если его IP-адрес находится в определённой сети.

– **Radius OTP Сети**. Поле для указания списка сетей, разрешённых для использования одноразовых паролей (OTP) при отправке через электронную почту. Здесь вводятся сети, к которым применяются правила Radius OTP.

– **Пользователь без политики MFA**. Обязательное поле для выбора поведения для пользователей без назначенной политики многофакторной аутентификации:

- *Разрешить вход пользователю* — Вход возможен без применения MFA.
- Запретить вход пользователя — Вход будет заблокирован без активной политики MFA.
- *Разрешить пользователю входить в систему, если его IP-адрес есть в списке сетей* — Вход возможен при совпадении IP-адреса с указанными сетями.
- *Запретить пользователю вход в систему, если его IP-адрес есть в списке сетей* — Вход будет запрещён при совпадении IP-адреса с указанными сетями.

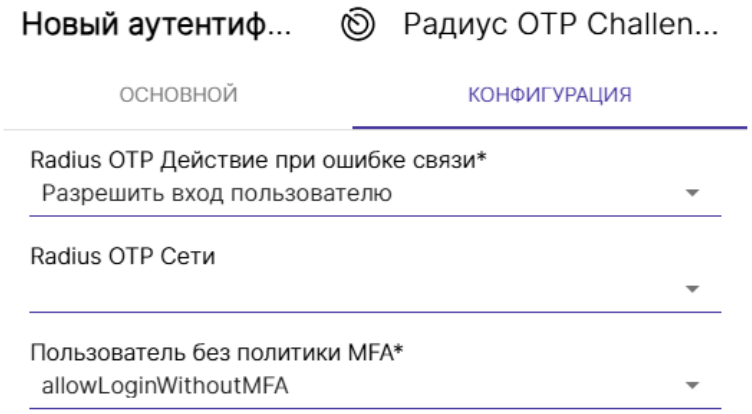


Рисунок 135

5. Нажать кнопку **Сохранить.**

5.2.11.3 *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.

Для создания аутентификатора СМС через HTTP:

1. Перейти в раздел **Аутентификация – Мультифактор**.
2. Нажать кнопку **Новый**, выбрать **СМС через HTTP.**

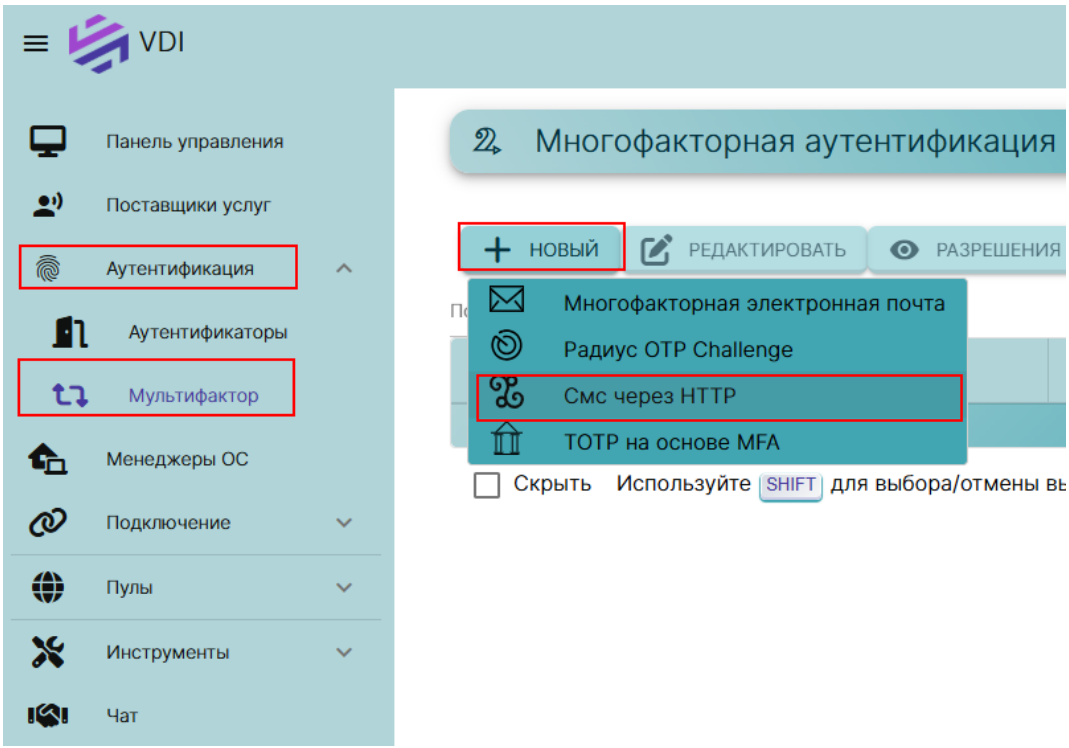


Рисунок 136

3. На вкладке **Основной** заполнить поля:

– **Тэги**. Используются для систематизации и упрощения поиска настроек аутентификатора среди других элементов.
– **Имя**. Обязательное поле для указания уникального имени аутентификатора.
– **Комментарии**. Поле для добавления произвольных примечаний или описания назначения аутентификатора.

– **Кэширование устройства**. Настройка времени (в часах), в течение которого устройство будет считаться доверенным, и пользователь сможет проходить аутентификацию без повторного ввода кода.
– **Действительность кода MFA**. Устанавливает срок действия одноразового кода многофакторной аутентификации в минутах.

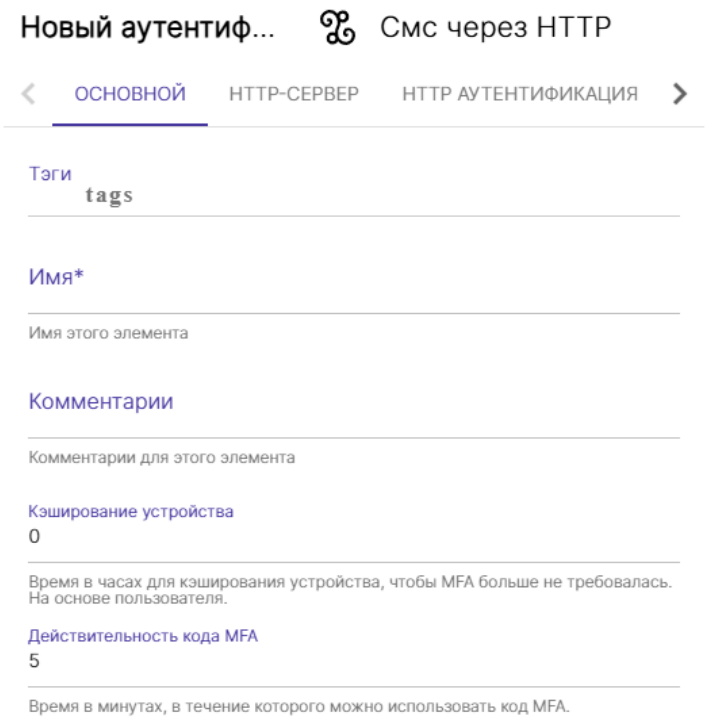


Рисунок 137

4. На вкладка **HTTP-сервер**:

– **Шаблон URL для отправки SMS**. Обязательное поле для указания шаблона URL, по которому будет отправляться SMS-сообщение. Шаблон может содержать переменные:
  a. `{code}` — код для отправки,
  b. `{phone}` или `{+phone}` — номер телефона пользователя,
  c. `{username}` — имя пользователя,
  d. `{justUsername}` — имя пользователя без доменной части.
– **Игнорировать ошибки сертификата**. Переключатель, позволяющий игнорировать ошибки SSL-сертификата при подключении к HTTP-серверу;

– **Метод отправки СМС**. Выпадающий список для выбора метода отправки HTTP-запроса: GET, POST, PUT;
– **Параметры для отправки SMS POST/PUT**. Поле для указания параметров тела запроса при использовании методов POST или PUT. Допустимо использование тех же переменных `{code}`, `{phone}`, `{username}`, `{justUsername}`.
– **Заголовки для SMS-запросов**. Поле для ввода HTTP-заголовков, которые будут добавлены к запросу. Формат заголовков: `ИмяЗаголовка: Значение`. Допускается использование переменных `{code}`, `{phone}`, `{username}`, `{justUsername}`.
– **Кодирование СМС**. Указывается кодировка данных при отправке запроса (например, `utf-8`).

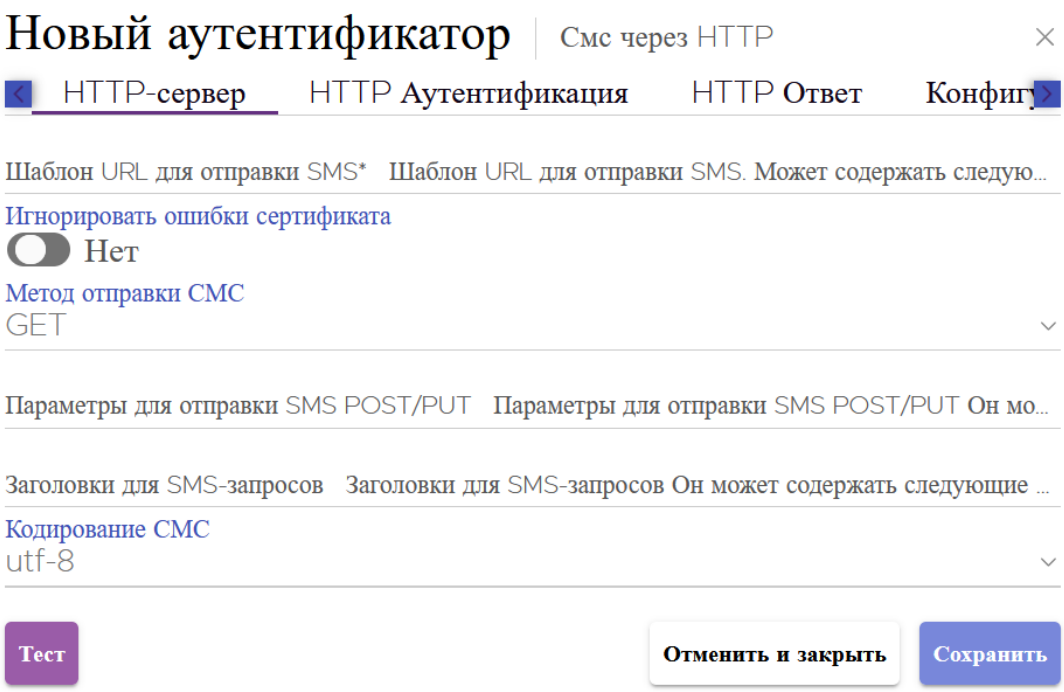


Рисунок 138

5. На вкладке **HTTP-аутентификация**:

– **Метод аутентификации SMS**. Обязательное поле для выбора способа аутентификации при отправке SMS:

  ○ **Нет** — аутентификация не используется. Запрос отправляется без указания пользователя и пароля.

- **Базовая HTTP-аутентификация** — используется стандартная Basic HTTP Authentication: имя пользователя и пароль передаются в заголовке запроса в кодировке Base64.
- **HTTP-дайджест-аутентификация** — используется более защищённая схема Digest Authentication, при которой данные о пароле не передаются в явном виде.

– **Пользователь или токен аутентификации SMS**. Поле для ввода имени пользователя или токена, который будет использоваться для авторизации при отправке SMS через HTTP.

– **Пароль аутентификации SMS**. Поле для ввода пароля пользователя или секрета, если выбран метод аутентификации, требующий пароль.

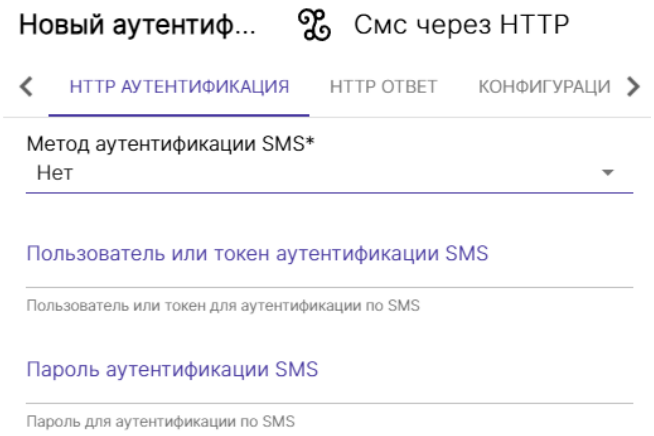


Рисунок 139

6. На вкладке **HTTP Ответ**:

   Регулярное выражение для ответа SMS OK. Поле для ввода регулярного выражения, которое будет применяться к ответу сервера для определения успешной отправки SMS. Если регулярное выражение задано, система проверяет текст ответа сервера на соответствие этому выражению. Если поле оставлено пустым, ответ считается успешным автоматически, если код HTTP-статуса равен 200.

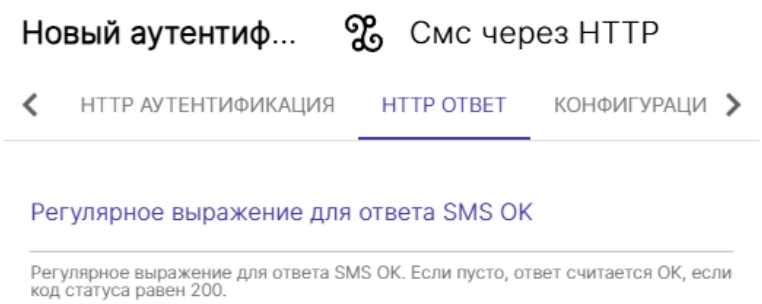


Рисунок 140

7. На вкладке **Конфигурация**:

– **Действие при ошибке ответа SMS**. Обязательное поле для выбора действия в случае ошибки или некорректного ответа от сервера при попытке отправки SMS:
  - *Разрешить вход пользователю* — пользователь сможет войти в систему несмотря на ошибку отправки SMS.
  - *Запретить вход пользователя* — пользователь не сможет войти при ошибке отправки SMS.
  - *Разрешить пользователю входить в систему, если его IP-адрес есть в списке сетей* — пользователь будет допущен, если его IP-адрес входит в разрешённые сети.
  - *Запретить пользователю вход в систему, если его IP-адрес есть в списке сетей* — вход будет запрещён, если IP-адрес пользователя входит в указанный список.
– **SMS Сети**. Поле для указания списка сетей, которые используются для применения специальных правил авторизации при ошибках SMS-отправки.
– **Пользователь без политики MFA**. Обязательное поле для выбора действия для пользователей, у которых не настроена политика многофакторной аутентификации:
  - *Разрешить вход пользователю* — вход без MFA будет разрешён.
  - *Запретить вход пользователя* — вход будет заблокирован без активной политики MFA.

- *Разрешить пользователю входить в систему, если его IP-адрес есть в списке сетей* — разрешение входа по IP.
- *Запретить пользователю вход в систему, если его IP-адрес есть в списке сетей* — запрет на вход по IP.

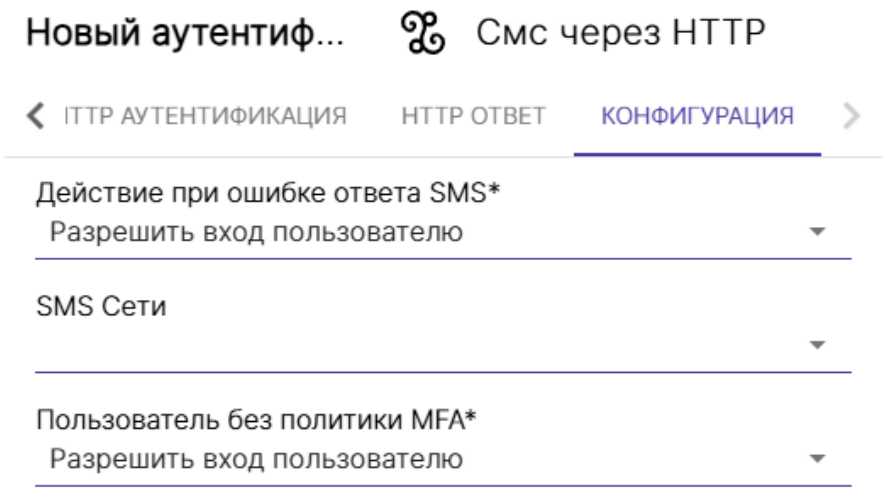


Рисунок 141

5.2.11.4 *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.

1. Перейти в раздел **Аутентификация – Мультифактор**.
2. Нажать кнопку **Новый**, выбрать **TOTP на основе MFA.**

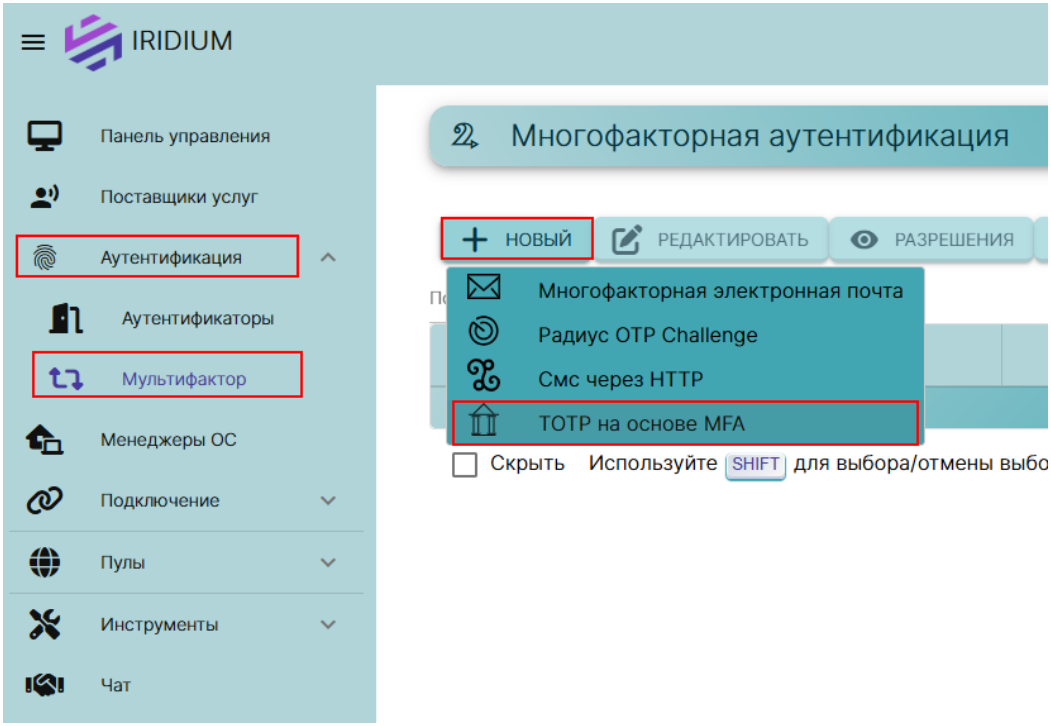


Рисунок 142

3. На вкладке **Основной** заполнить поля:

– **Тэги**. Используются для классификации аутентификатора и облегчения поиска среди других элементов системы.
– **Имя**. Обязательное поле для ввода уникального имени нового аутентификатора.
– **Комментарии**. Поле для добавления примечаний или описания назначения данного аутентификатора.
– **Эмитент**. Обязательное поле для указания эмитента OTP (One-Time Password). После создания аутентификатора значение изменить невозможно. Эмитент отображается в приложении для генерации кодов (например, Google Authenticator).
– **Кэширование устройства**. Время (в часах), в течение которого устройство будет считаться доверенным, что позволит пользователю временно не вводить код MFA.
– **Действительность кода MFA**. Устанавливает срок действия одноразового кода аутентификации в минутах.

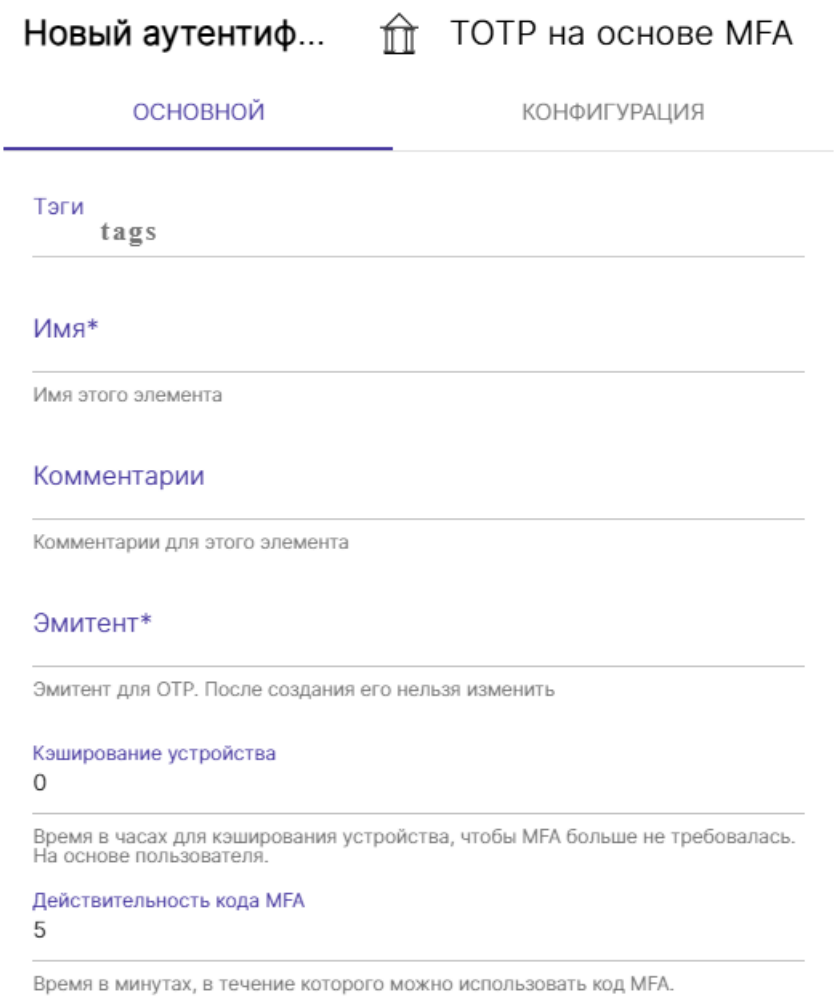


Рисунок 143

4. На вкладке **Конфигурация:**

– Действительное окно. Обязательное поле для ввода числа, определяющего диапазон допустимых кодов. Определяет количество допустимых TOTP-кодов до и после текущего момента времени. Например, значение 1 означает, что будет приниматься текущий код, один предыдущий и один следующий код (окно в три кода).
– Сети TOTP. Выбор сетей, в которых пользователям не будет предложено вводить одноразовый пароль. Пользователи, подключённые из указанных сетей, будут проходить аутентификацию без запроса кода TOTP.

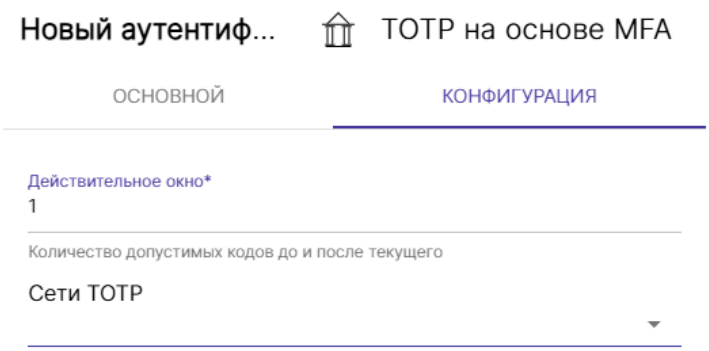


Рисунок 144

5. Нажать кнопку **Сохранить.**

5.2.12 Создание групп пользователей

1. Перейти в раздел **Аутентификация -> Аутентификаторы.** (Рисунок 145).

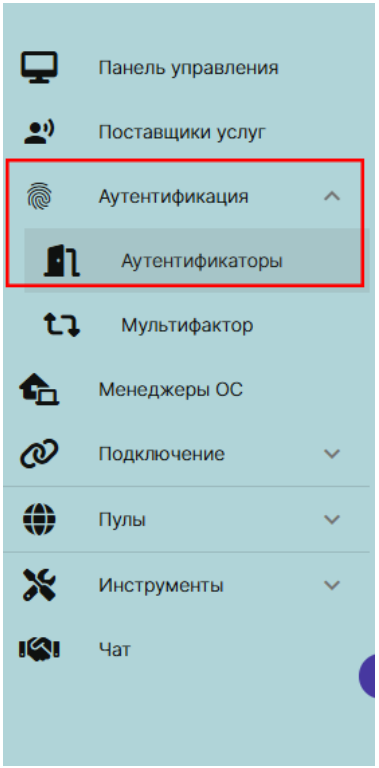


Рисунок 145

2. Выбрать созданный ранее аутентификатор.

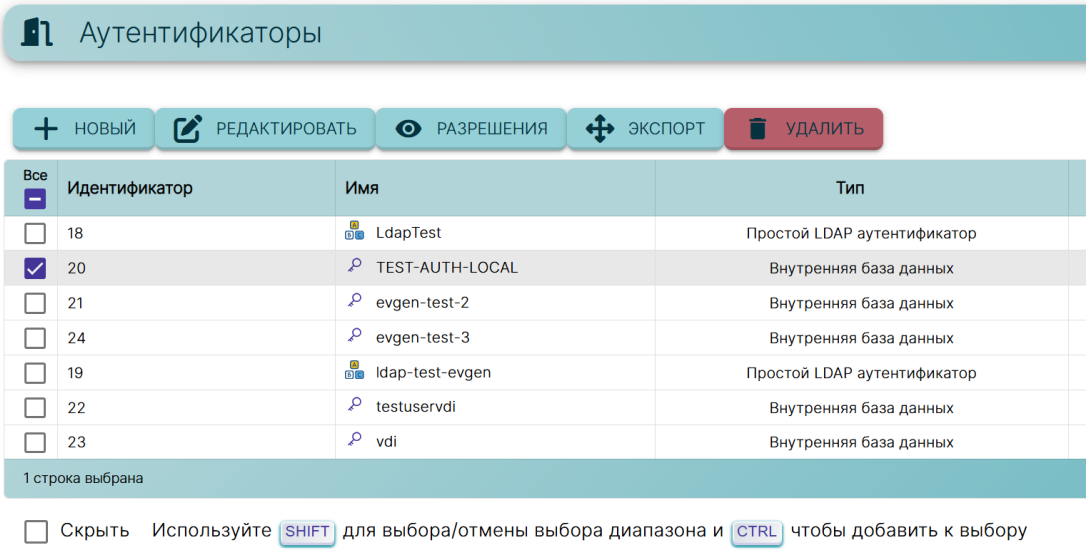


Рисунок 146

3. Дважды нажать на созданный ранее аутентификатор, либо правой кнопкой мыши -> **Подробнее**.

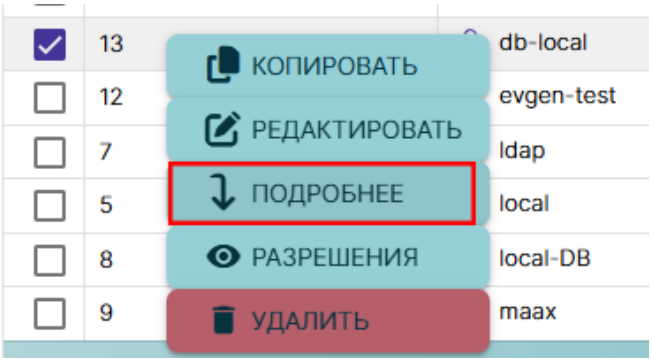


Рисунок 147

4. Перейти в раздел **Группы.**

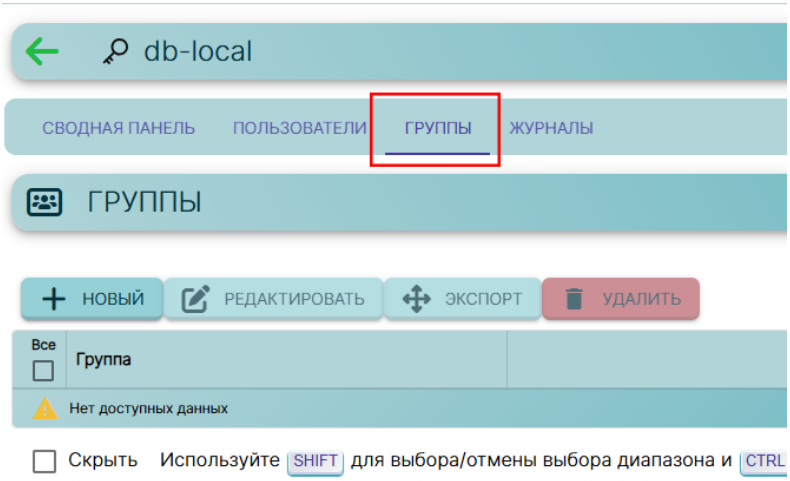


Рисунок 148

5. Нажать кнопку **Новый -> Группа**.

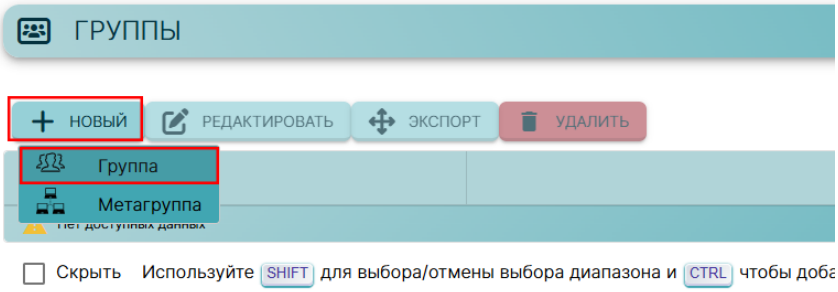


Рисунок 149

6. Откроется окно создания группы.
7. Ввести имя группы, состояние – включено, назначить пулы (опционально).

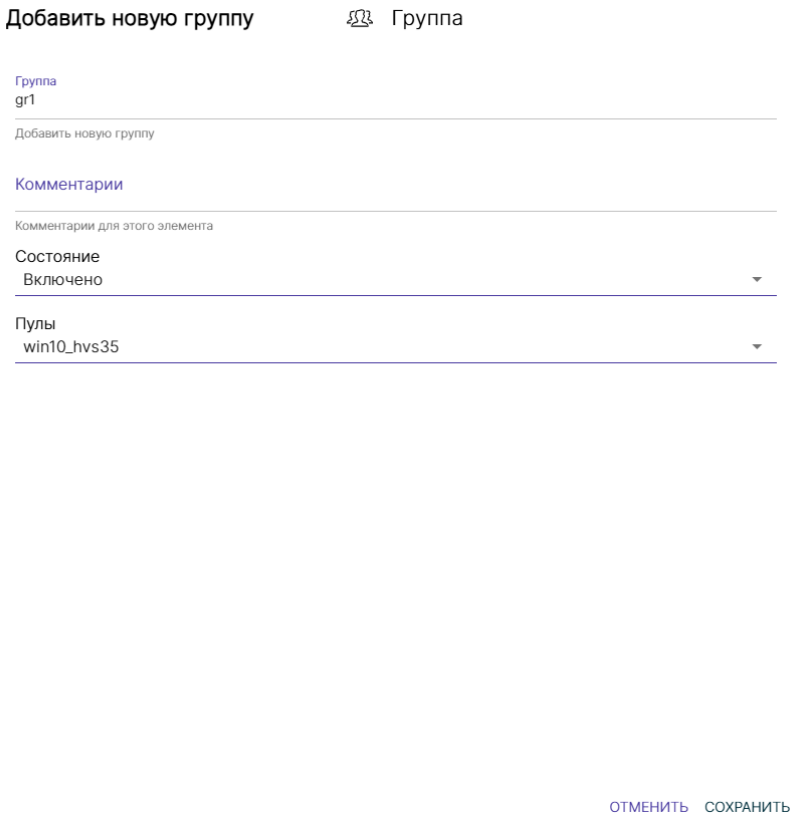


Рисунок 150

8. Нажать кнопку **Сохранить.**

5.2.13 Создание пользователя с ролью «Сотрудник»

1. Перейти в раздел **Пользователи.**

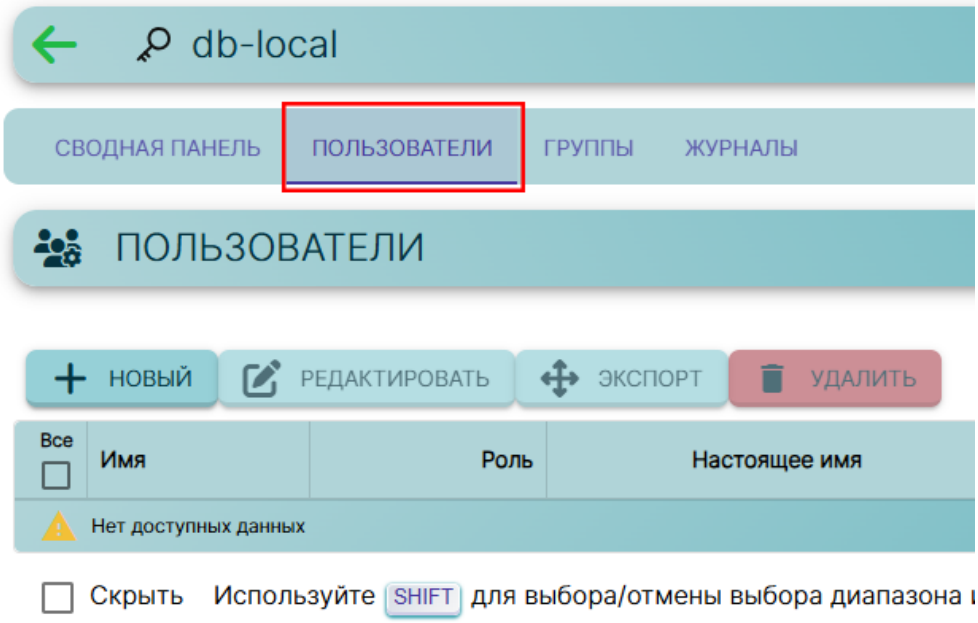


Рисунок 151

2. Нажать кнопку **Новый.**
3. Откроется окно создания нового пользователя. Необходимо заполнить поля:

– Имя пользователя;

– Пароль;

– Выбрать роль для пользователя **Сотрудник**.

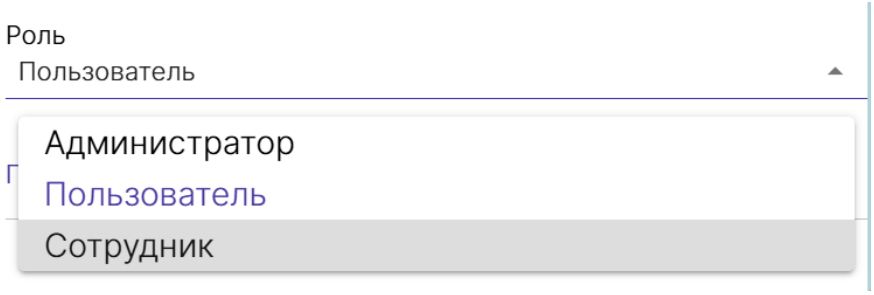


Рисунок 152

– Выбрать раннее созданную группу;

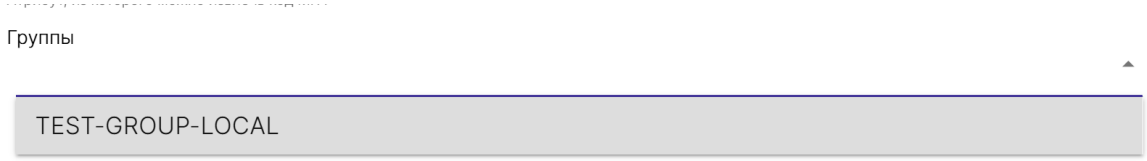


Рисунок 153

– При необходимости указать атрибут MFA.

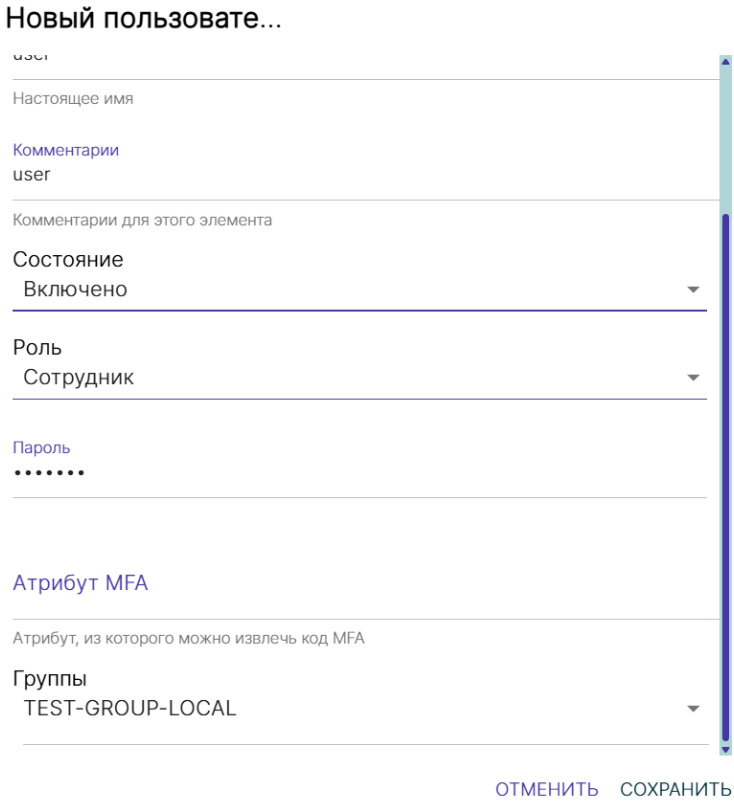


Рисунок 154

4. Нажать кнопку **Сохранить.**

5.2.14 Создание пользователя с ролью «Администратор»

1. Перейти в раздел **Пользователи.**

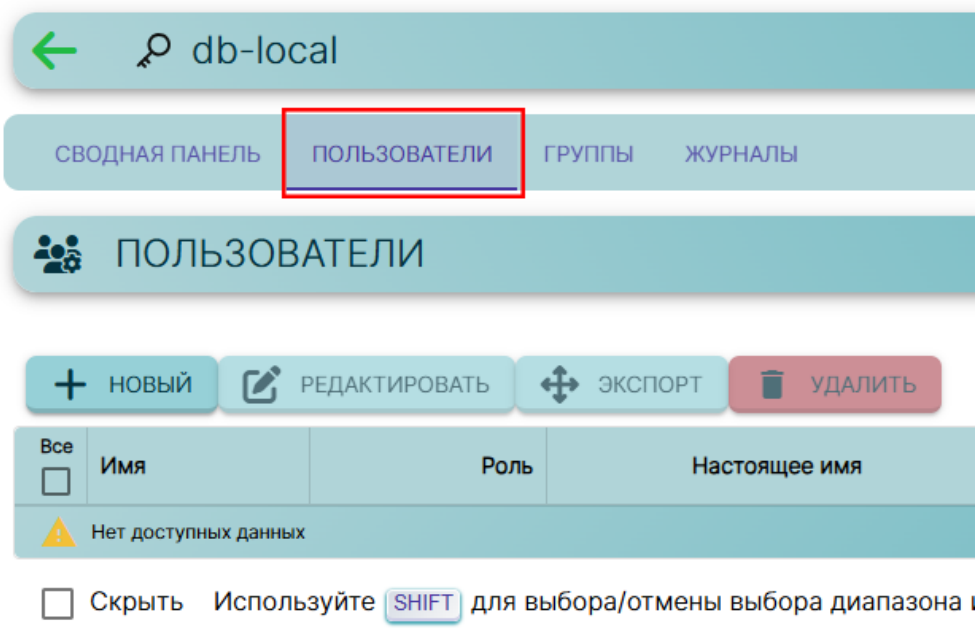


Рисунок 155

2. Нажать кнопку **Новый.**
3. Откроется окно создания нового пользователя. Необходимо заполнить поля:

– Имя пользователя;
– Пароль;
– Выбрать роль для пользователя **Администратор**;

Рисунок 156

– Выбрать раннее созданную группу;

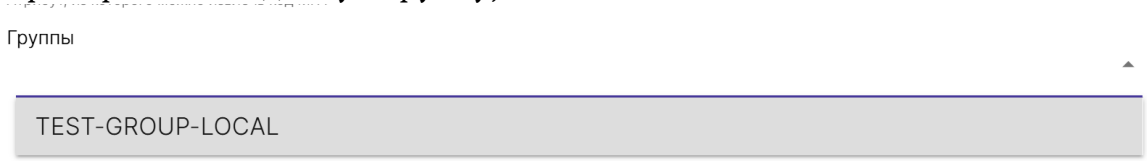


Рисунок 157

– При необходимости указать атрибут MFA.

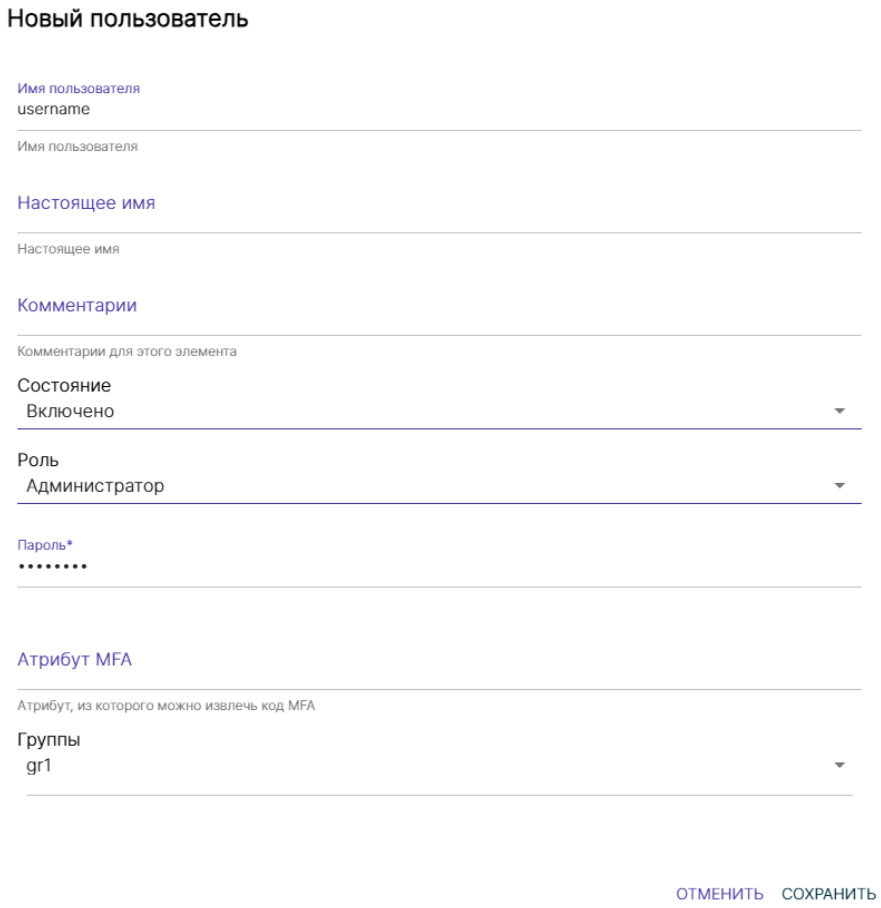


Рисунок 158

4. Нажать кнопку **Сохранить.**

5.2.15 Создание пользователя с ролью «Пользователь»

1. Перейти в раздел **Пользователи.**

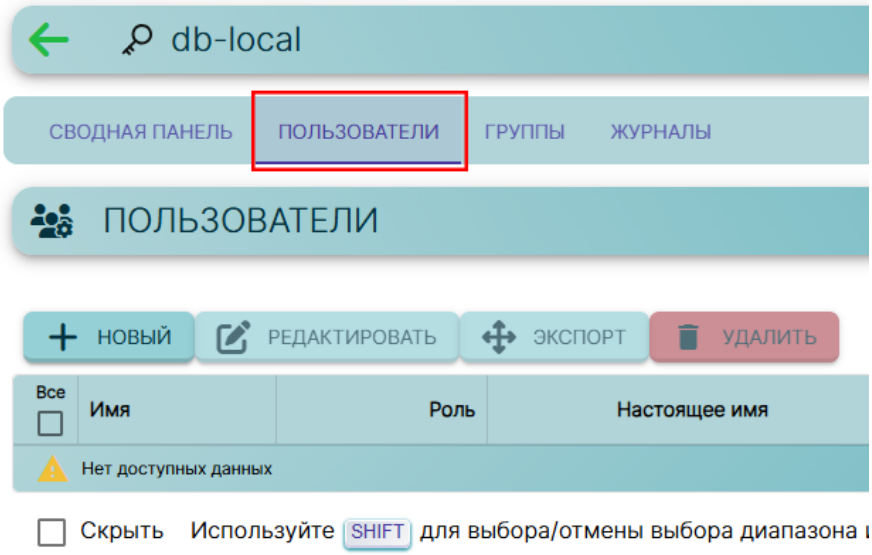


Рисунок 159

2. Нажать кнопку **Новый.**
3. Откроется окно создания нового пользователя. Необходимо заполнить поля:

– Имя пользователя;
– Пароль;
– Выбрать роль для пользователя. Доступно три роли:
  - Администратор;
  - Пользователь;
  - Сотрудник.

Рисунок 160

– Выбрать раннее созданную группу;

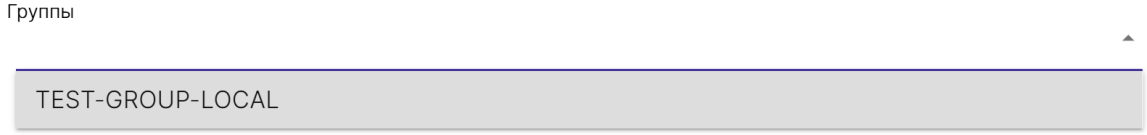


Рисунок 161

– При необходимости указать атрибут MFA.

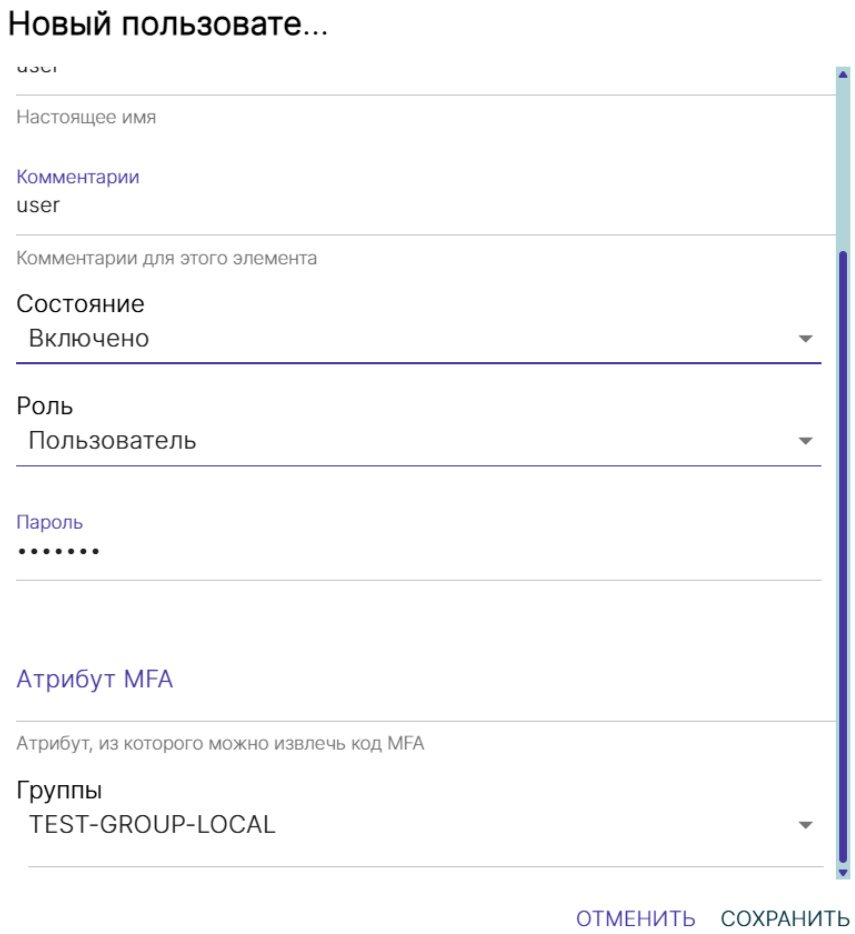


Рисунок 162

4. Нажать кнопку **Сохранить.**

5.3 Настройка Менеджеров ОС

Менеджер ОС — это компонент, который запускает предварительно настроенную службу для управления виртуальными рабочими местами.

5.3.1 Создание менеджера ОС Linux

Менеджер ОС для Linux — это специализированный компонент, который управляет виртуальными рабочими столами на базе операционных систем Linux.

Его основные задачи включают:

– Присвоение виртуальным машинам уникальных имен в соответствии с заданными правилами для удобства идентификации в пуле.

– Контроль за жизненным циклом пользовательских сеансов (запуск, завершение, отслеживание состояния) на виртуальных рабочих столах.

Для создание базового менеджера ОС:

1. Перейти в раздел **Менеджеры ОС.**
2. Нажать кнопку **Новый -> Linux ОС менеджер** (Рисунок 163):

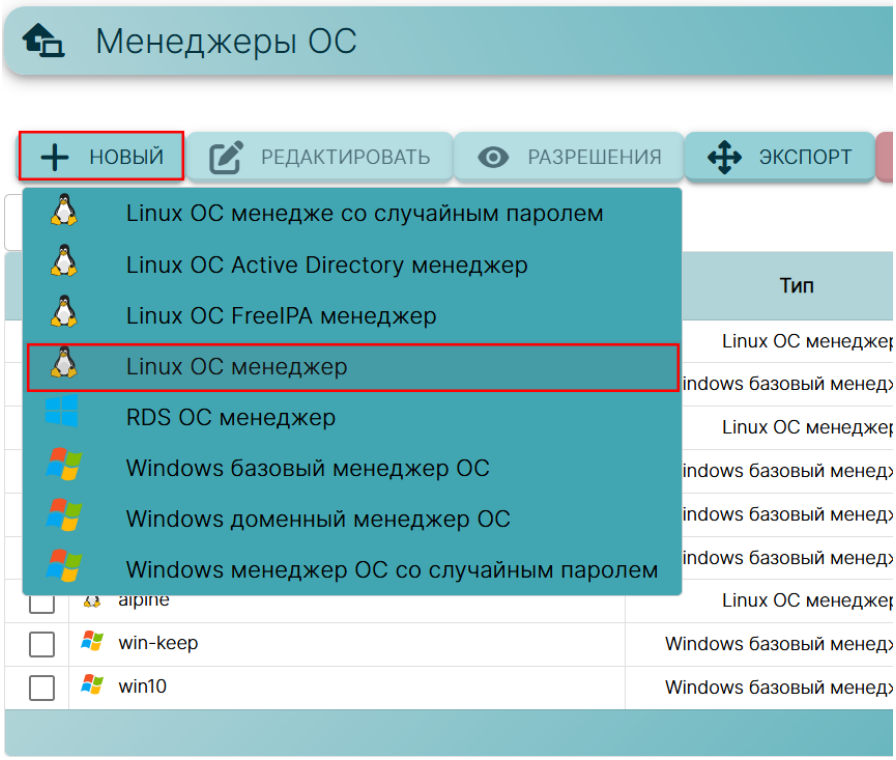


Рисунок 163

3. В открывшемся окне заполнить поле **Имя** Менеджера ОС.
4. При настройке виртуальных рабочих столов в VDI можно определить, что именно будет происходить с виртуальной машиной после завершения пользовательского сеанса. Доступны следующие варианты:

– **Держать сервис привязанным**.

  - При выходе пользователя из виртуального рабочего стола система не выполняет никаких действий.
  - При следующем подключении пользователю назначается тот же рабочий стол, с которым он работал ранее.

- Если администратор публикует новую версию «Сервисного пула», текущий рабочий стол пользователя будет удалён, и при следующем подключении ему будет предоставлен новый рабочий стол из обновлённого пула.
- **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.

5.3.2 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.

Для создания менеджера ОС Linux со случайным паролем:

1. Перейти в раздел **Менеджеры ОС.**

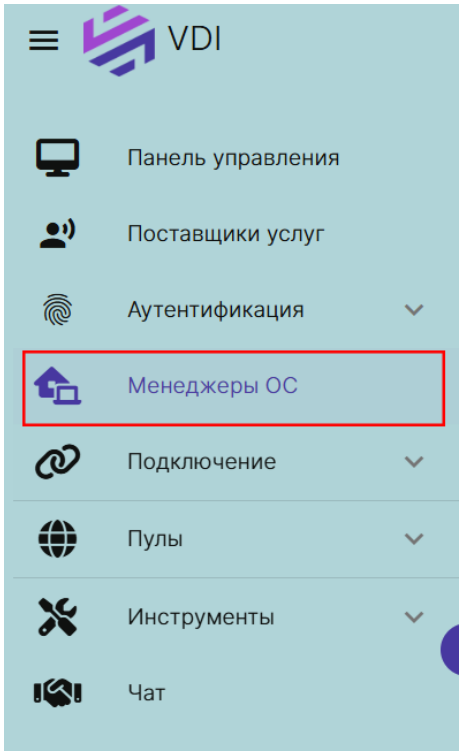
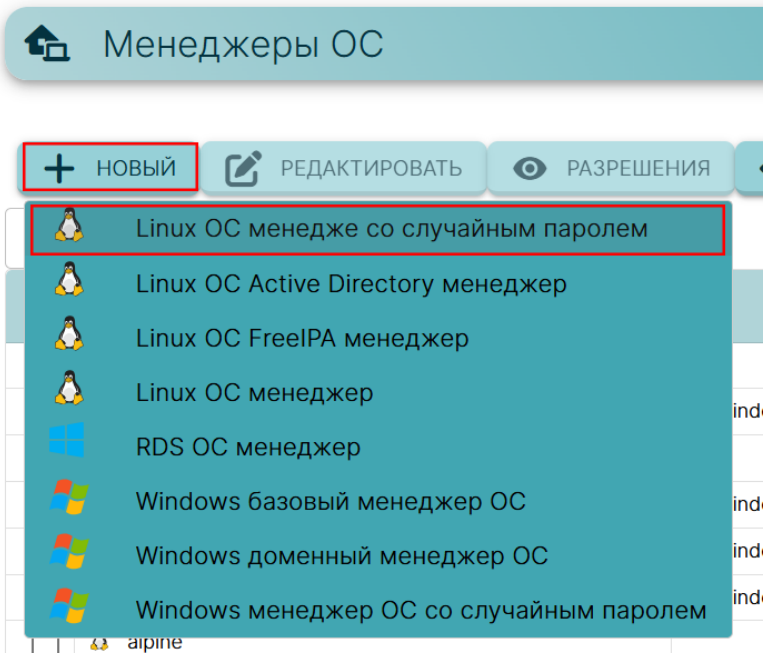


Рисунок 164

2. Нажать кнопку **Новый -> Linux ОС менеджер со случайным паролем.**



3. Заполнить поля:

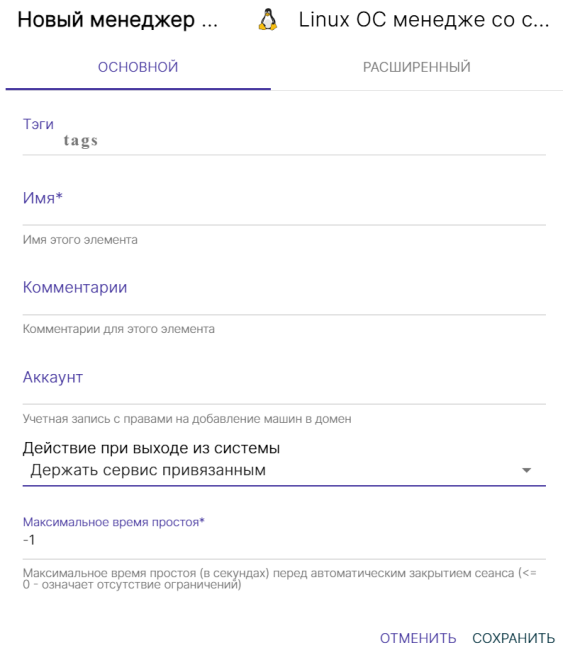


Рисунок 165

– **Имя;**

– Указать действия при выходе из системы;

  - При выходе пользователя из виртуального рабочего стола система не выполняет никаких действий.

- При следующем подключении пользователю назначается тот же рабочий стол, с которым он работал ранее.
- Если администратор публикует новую версию «Сервисного пула», текущий рабочий стол пользователя будет удалён, и при следующем подключении ему будет предоставлен новый рабочий стол из обновлённого пула.

– **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.

– В разделе **Расширенный** можно включить опцию завершения сессии пользователя по календарю.

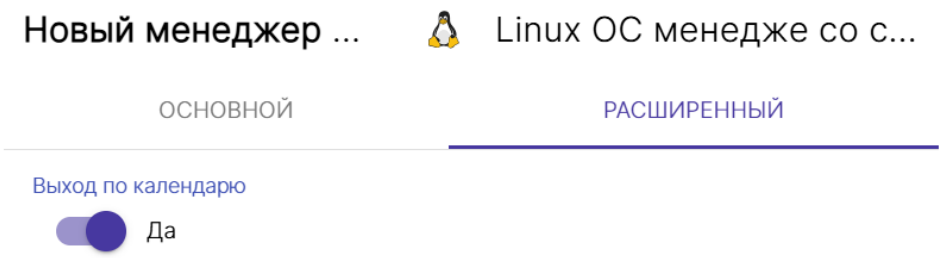


Рисунок 166

5.3.3 RDS

RDS ОС менеджер используется для настройки Сервис-пула, который предоставляет пользователям виртуальное приложение.

Для создания **RDS ОС менеджер** выполнить:

1. Переейти к разделу **Менеджеры ОС**, нажать **Новый**.
2. Выбрать **RDS ОС менеджер.**

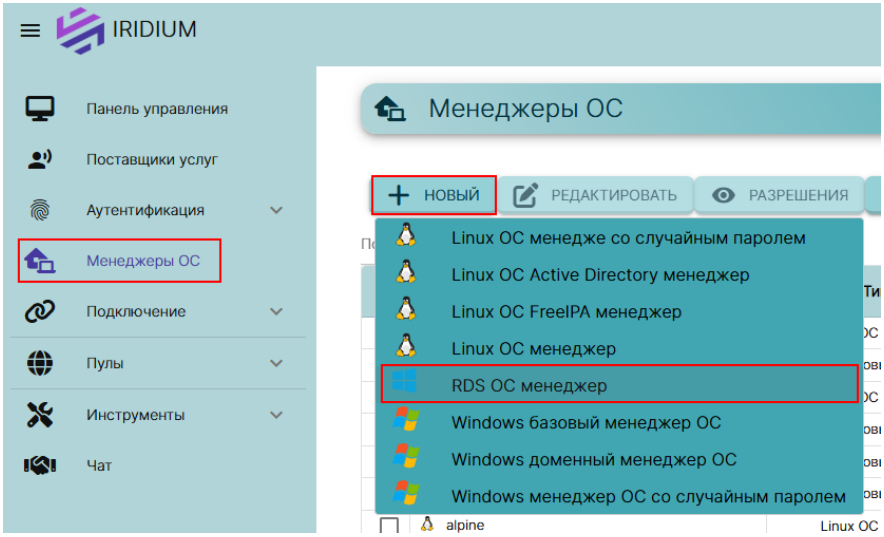


Рисунок 167

3. Заполнить поля:

– **Имя**;

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

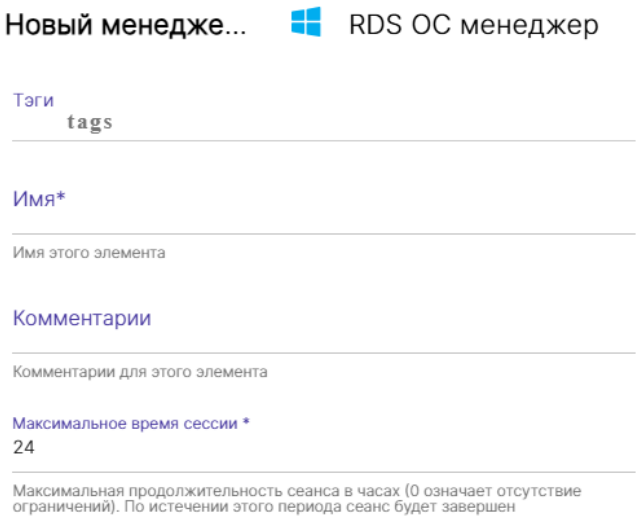


Рисунок 168

4. Нажать кнопку **Сохранить.**

5.3.4 Windows базовый менеджер ОС

Windows базовый менеджер ОС 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.

1. Перейти в **Менеджеры ОС.**
2. Нажать кнопку **Новый**.
3. Выбрать **Windows базовый менеджер ОС.**

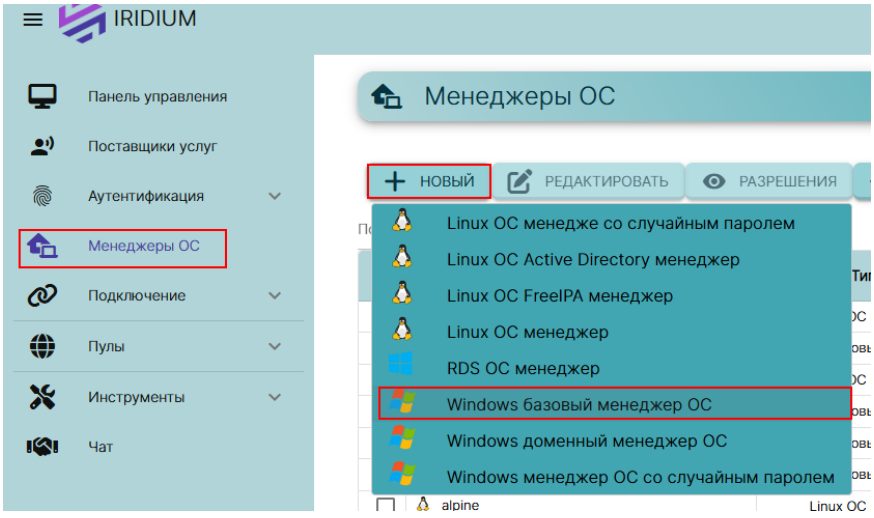


Рисунок 169

4. В открывшемся окне создания менеджера ОС заполнить поля:

– **Имя**;

– **Указать действия при выходе из системы**;

- При выходе пользователя из виртуального рабочего стола система не выполняет никаких действий.
- При следующем подключении пользователю назначается тот же рабочий стол, с которым он работал ранее.
- Если администратор публикует новую версию «Сервисного пула», текущий рабочий стол пользователя будет удалён, и при следующем подключении ему будет предоставлен новый рабочий стол из обновлённого пула.

– **Определить число максимального время простоя.** Максимальное время (указывается в секундах) бездействия на виртуальном рабочем столе;

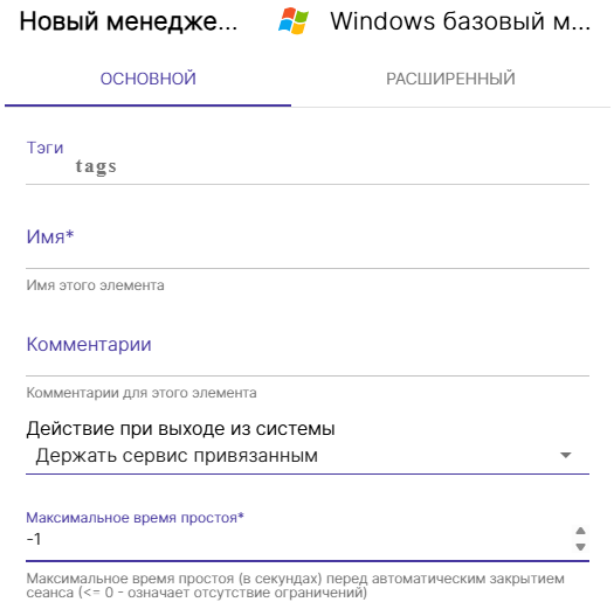


Рисунок 170

5. На вкладке **Расширенный** можно включить выход из сессии по календарю.

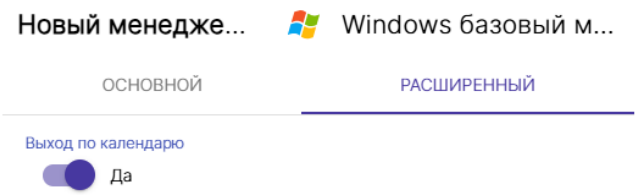


Рисунок 171

Нажать кнопку **Сохранить.**

5.3.5 Windows доменный менеджер

Windows доменный менеджер ОС 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.

Для создания Windows доменный менеджер:

1. Перейти в раздел **Менеджеры ОС.**

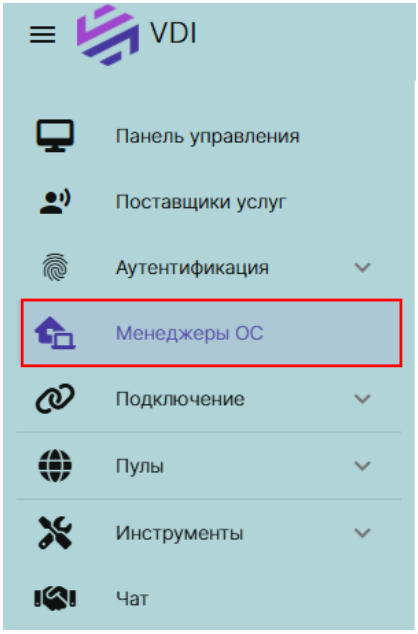


Рисунок 172

2. Нажать кнопку **Новый.**

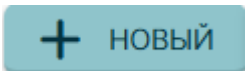


Рисунок 173

3. В списке выбрать **Windows доменный менеджер ОС**.

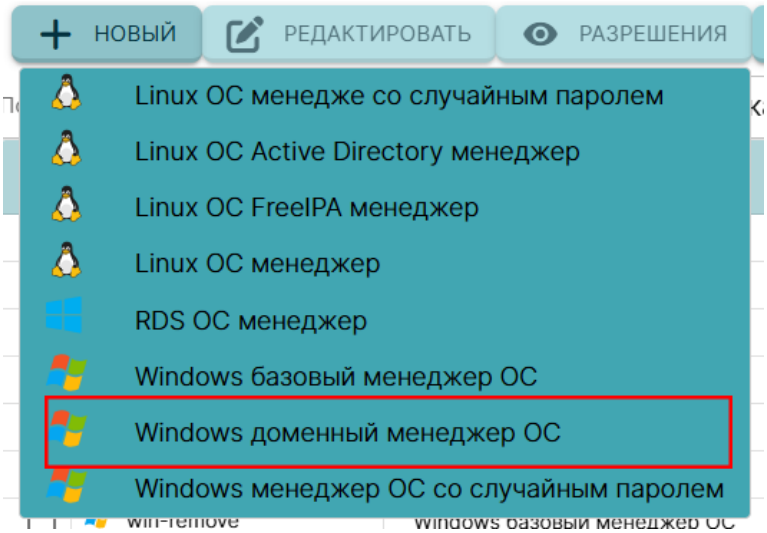


Рисунок 174

4. В открывшемся окне создания менеджера ОС заполнить поля:

– **Имя**;

– **Домен.** Имя домена AD, к которому будут присоединены виртуальные рабочие столы.;

– **Пароль**;

– **Указать действия при выходе из системы**;

- При выходе пользователя из виртуального рабочего стола система не выполняет никаких действий.

- При следующем подключении пользователю назначается тот же рабочий стол, с которым он работал ранее.
- Если администратор публикует новую версию «Сервисного пула», текущий рабочий стол пользователя будет удалён, и при следующем подключении ему будет предоставлен новый рабочий стол из обновлённого пула.

– **Определить число максимального время простоя.** Максимальное время (указывается в секундах) бездействия на виртуальном рабочем столе;

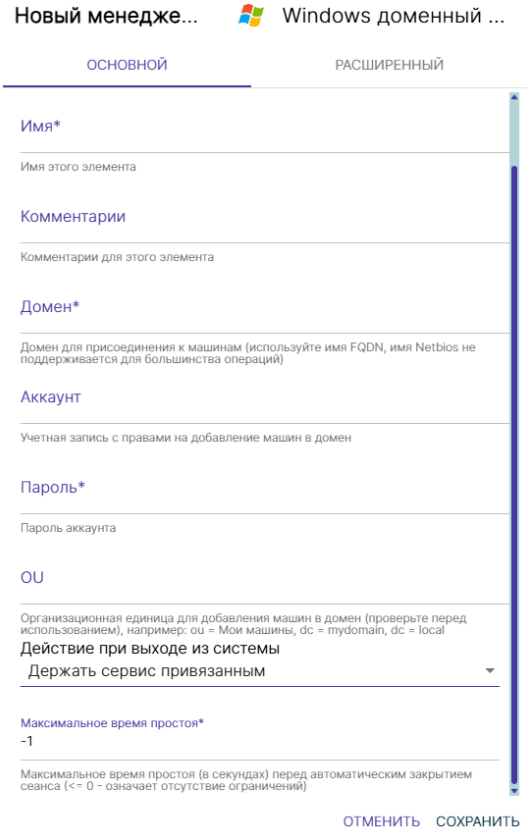


Рисунок 175

– **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 176).

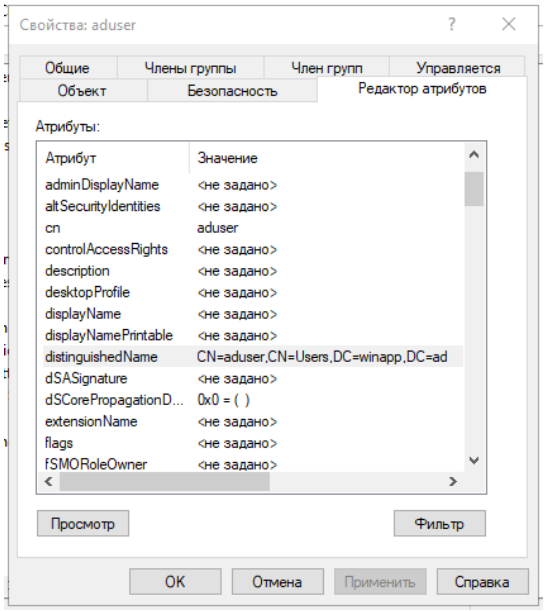


Рисунок 176

5. На вкладке **Расширенный** (Рисунок 177):

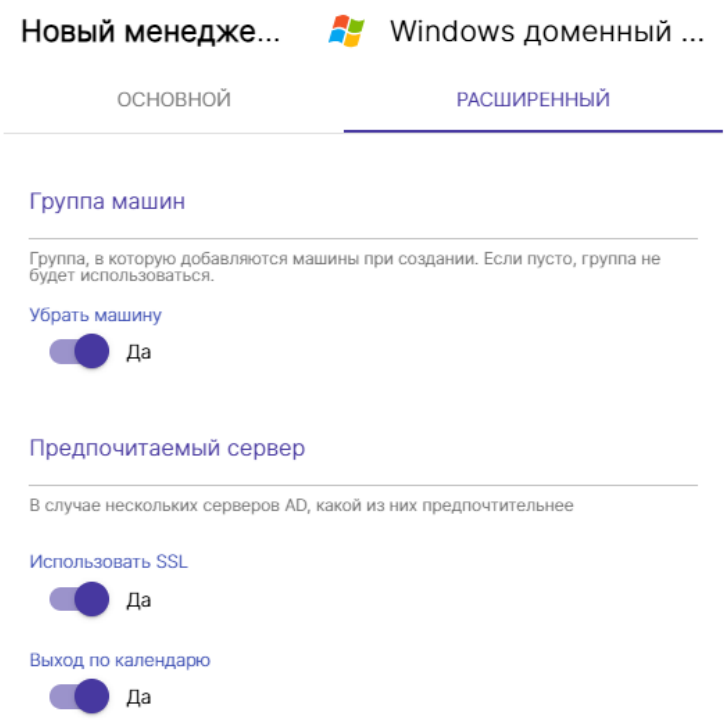


Рисунок 177

– **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.

6. Нажать кнопку **Сохранить**.

Рисунок 178

5.3.6 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.

Для создания Windows со случайным паролем необходимо выполнить следующие действия:

1. Перейти в **Менеджеры ОС.**
2. Нажать кнопку **Новый**.
3. Выбрать **Windows со случайным паролем.**

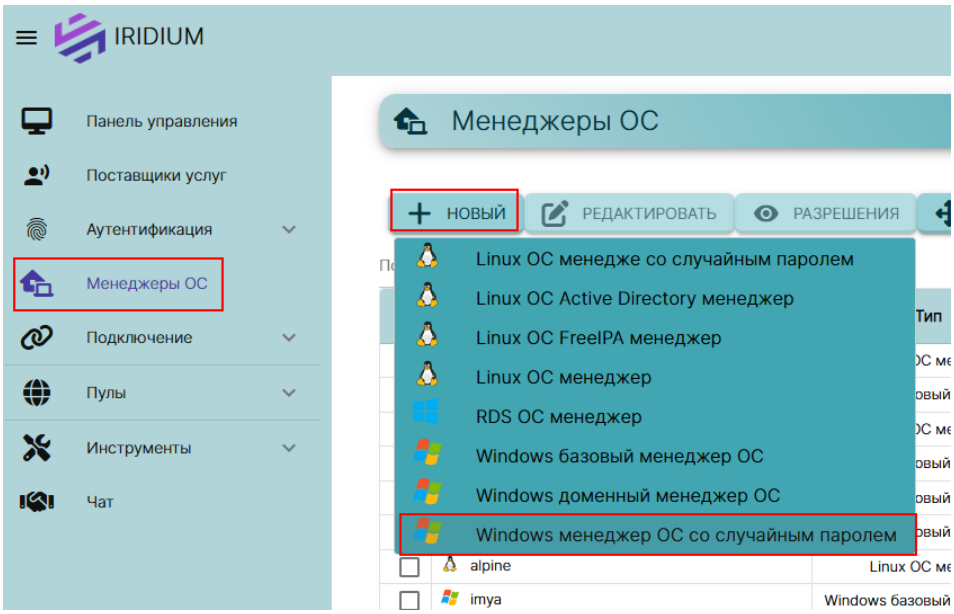


Рисунок 179

4. В открывшемся окне создания менеджера ОС заполнить поля:

– **Имя**;

– **Пароль**;

– **Указать действия при выходе из системы**;

- При выходе пользователя из виртуального рабочего стола система не выполняет никаких действий.
- При следующем подключении пользователю назначается тот же рабочий стол, с которым он работал ранее.
- Если администратор публикует новую версию «Сервисного пула», текущий рабочий стол пользователя будет удалён, и при следующем подключении ему будет предоставлен новый рабочий стол из обновлённого пула.

– **Определить число максимального время простоя.** Максимальное время (указывается в секундах) бездействия на виртуальном рабочем столе;

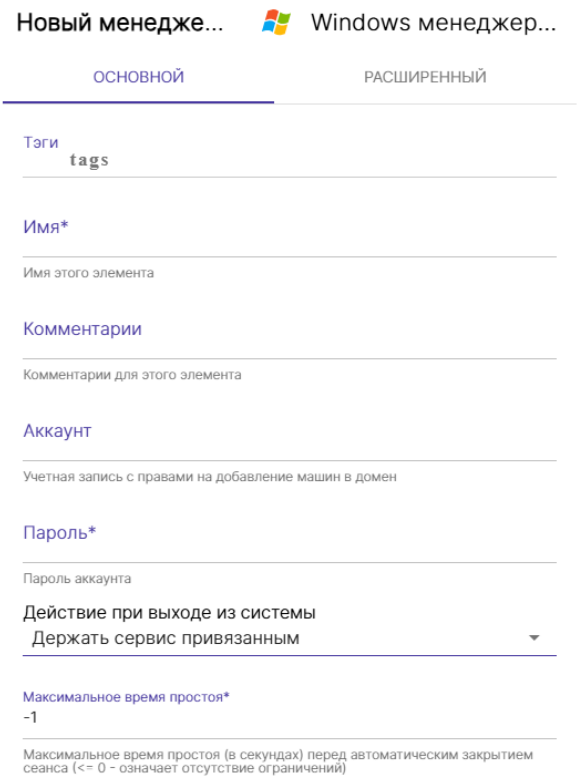


Рисунок 180

5. На вкладке **Расширенный** можно включить выход из сессии по календарю.

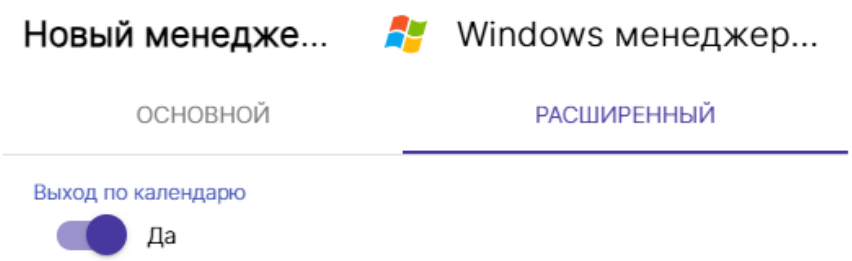


Рисунок 181

6. Нажать кнопку **Сохранить.**

5.4 Транспорт

Транспорты представляют собой клиентские модули, обеспечивающие установление защищенного соединения между рабочим местом пользователя и виртуальной средой (рабочим столом или приложением). Каждый транспорт

реализует определенный протокол подключения, определяющий способ передачи данных между клиентом и сервером.

Для корректной работы транспорта необходимо обеспечить поддержку выбранного протокола подключения как на стороне клиентского устройства, так и на стороне сервера виртуальных рабочих столов/приложений.

Для управления транспортами требуется:

1. Перейти в раздел администрирования **Подключение**.
2. Выбрать подраздел **Транспорт**.
3. Нажать кнопку **Новый.** В интерфейсе будет отображен список доступных для настройки типов транспортов.

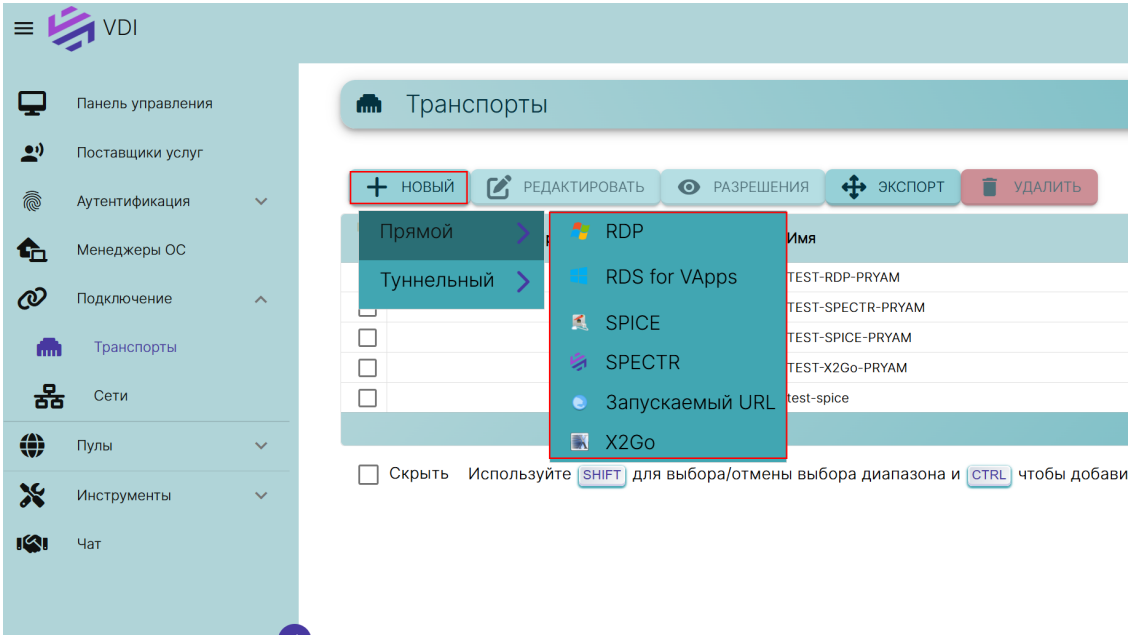


Рисунок 182

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.

5.4.1 Протокол RDP

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).

Для подключения протокола **RDP (прямой)**:

1. Перейти в **Подключение -> Транспорты.**

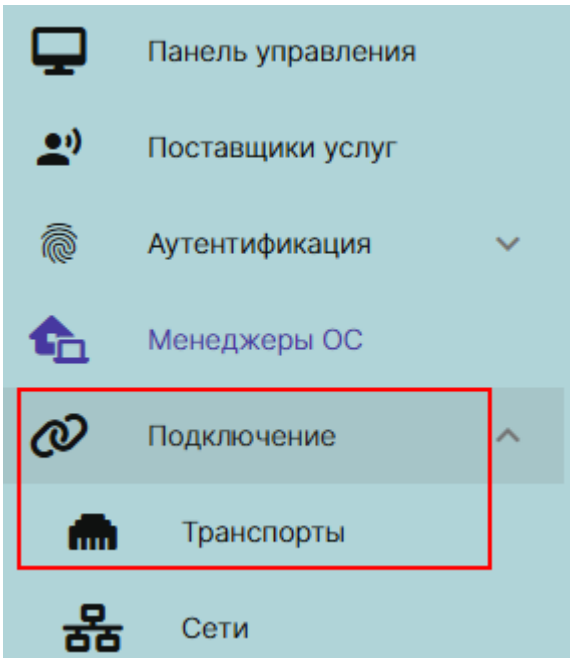


Рисунок 183

2. Нажать кнопку **Новый**.

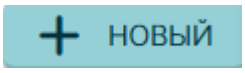


Рисунок 184

3. Выбрать **Прямой -> RDP**. Откроется окно добавления транспорта.

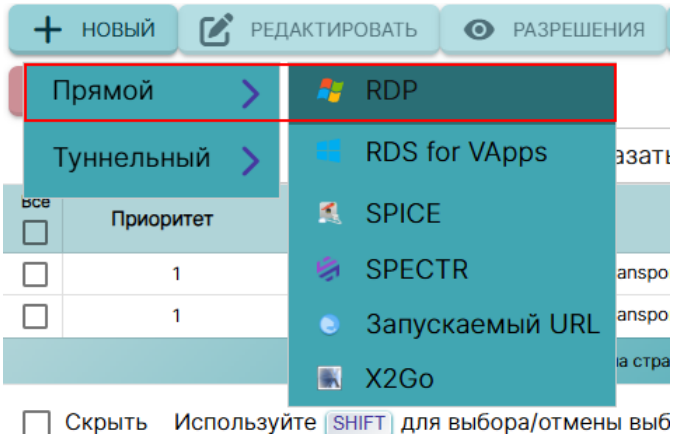
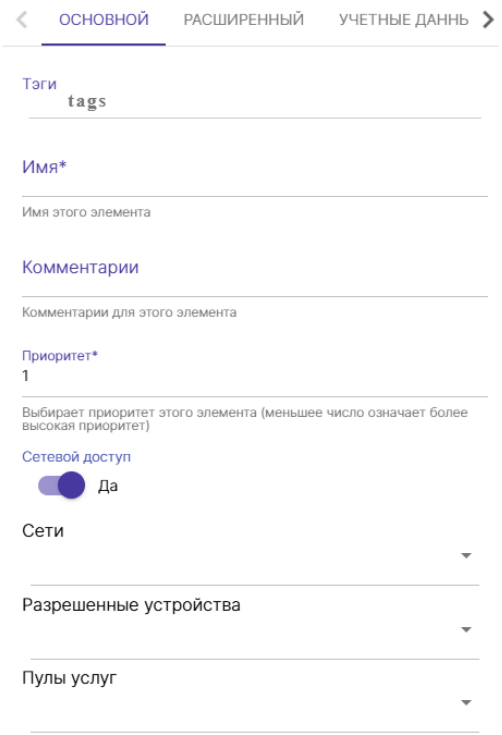


Рисунок 185

4. На вкладке **Основной** заполнить поля:

– **Имя**;

– **Приоритет.** Числовое поле для указания порядка, в котором система будет пытаться использовать этот транспорт, если для службы назначено несколько транспортов.



5. Нажать кнопку **Сохранить.**

Рисунок 186

6. Созданный транспорт будет отображен в списке.

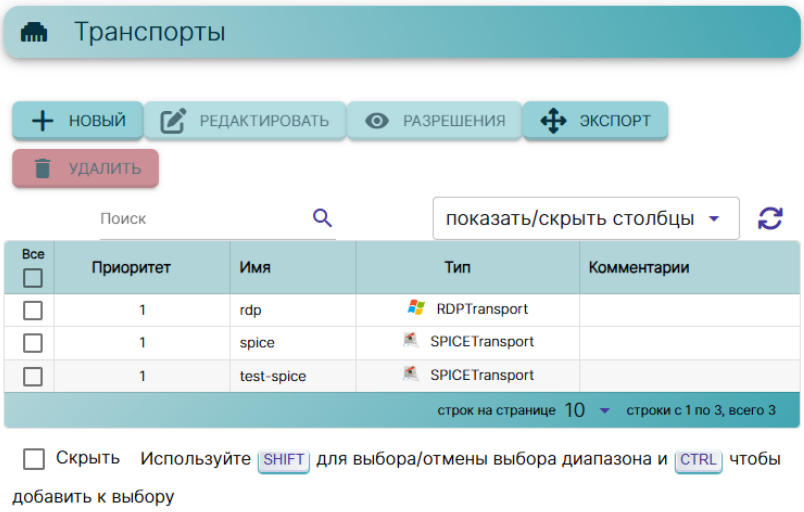


Рисунок 187

5.4.1 RDS для виртуальных приложений (RDS for VApps)

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.

5.4.2 SPICE (прямой)

Протокол 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).

Для добавления протокола Spice:

1. Перейти в раздел **Подключение** -> **Транспорты.**

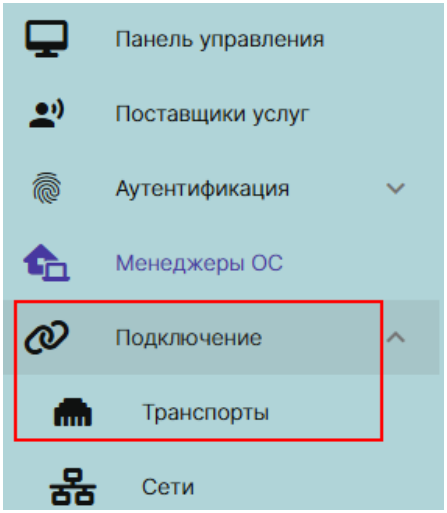


Рисунок 188

2. Нажать кнопку **Новый.**

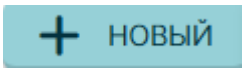


Рисунок 189

3. Выбрать Прямой -> SPICE. Откроется окно добавления транспорта.

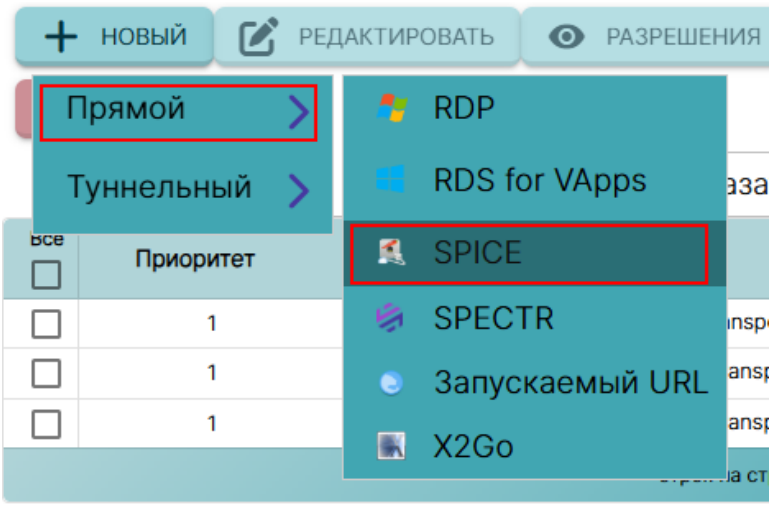


Рисунок 190

4. На вкладке **Основной** заполнить поля:

– **Имя**. Уникальное имя для SPICE-транспорта;

– **Приоритет**. Определяет порядок выбора транспорта, если их несколько. Меньшее число = высший приоритет;

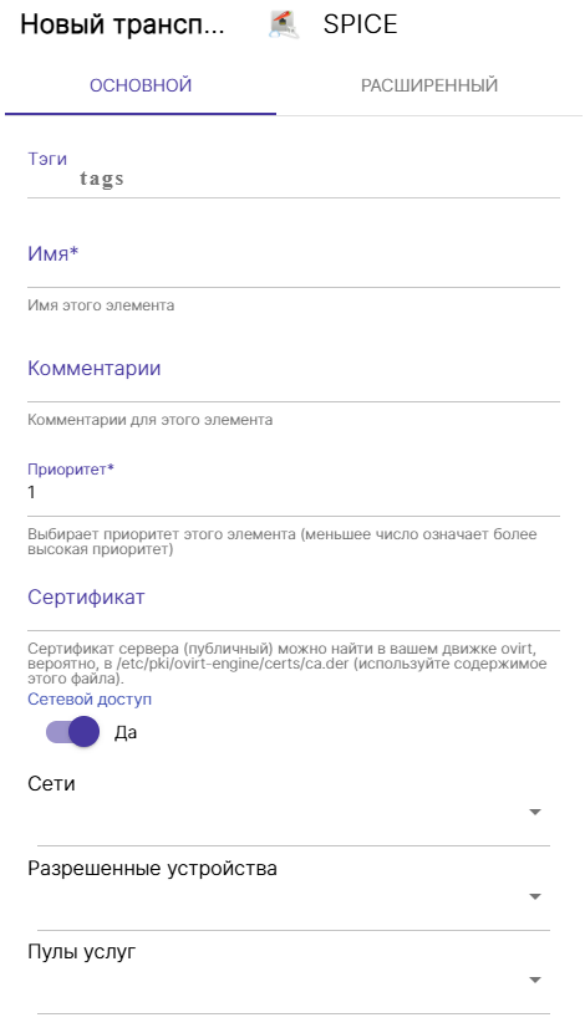


Рисунок 191

5. Нажать кнопку **Сохранить.**

Рисунок 192

6. Транспорт появится в списке.

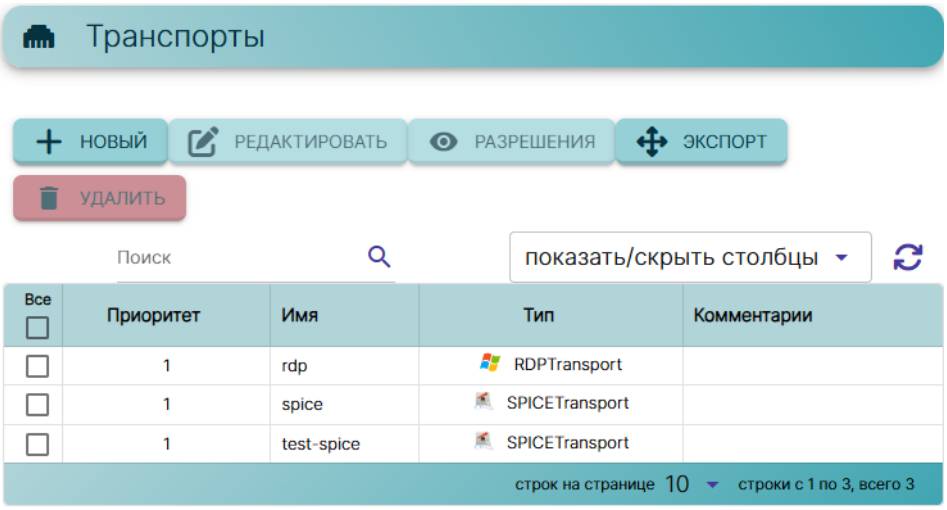


Рисунок 193

5.4.3 Добавление протокола СПЕКТР

Для добавления протокола СПЕКТР:

1. Перейти в раздел **Аутентификация -> Аутентификаторы**.

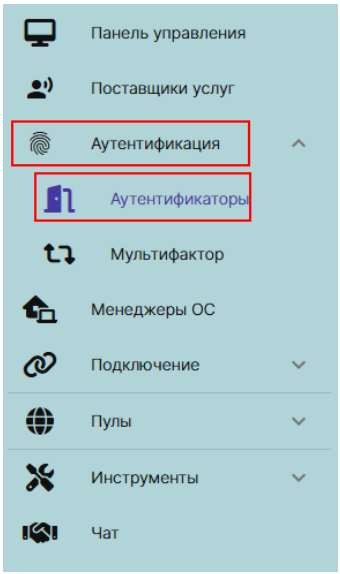


Рисунок 194

2. Нажать кнопку **Новый**.

3. Выбрать **Прямой -> SPECTR**.

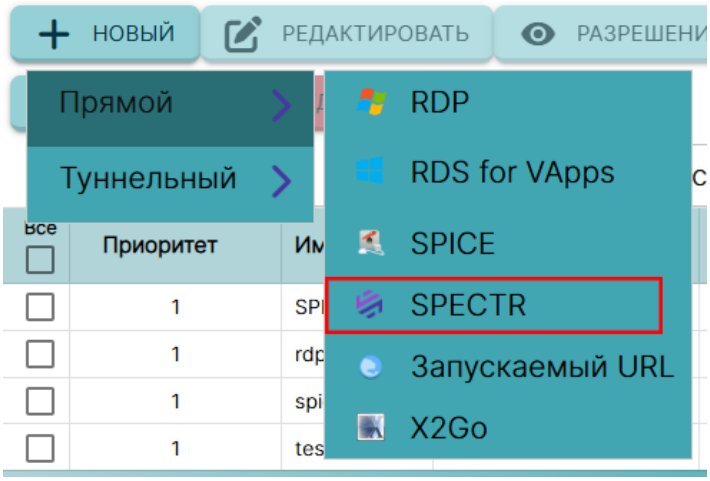


Рисунок 195

4. В открывшемся окне, вкладке Основной, заполнить поля:

– **Имя**;

– **Приоритет**;

– **Сети** (опционально);

– **Разрешенные устройства** (опционально);

– **Пулы услуг** (опционально).

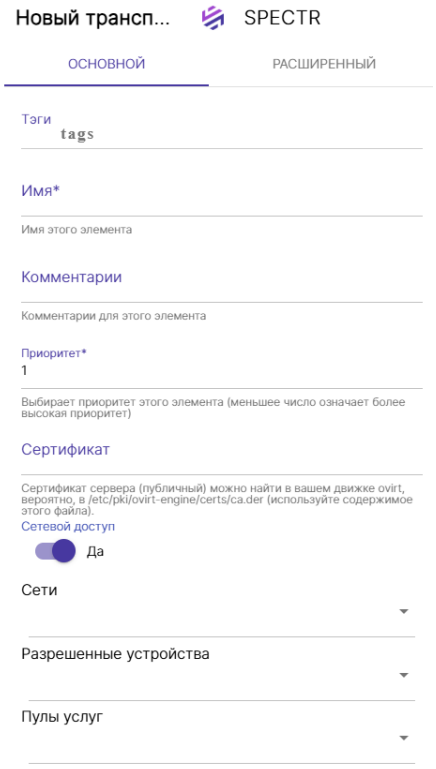


Рисунок 196

5. Нажать кнопку **Сохранить**.

Рисунок 197

6. Транспорт появится в списке.

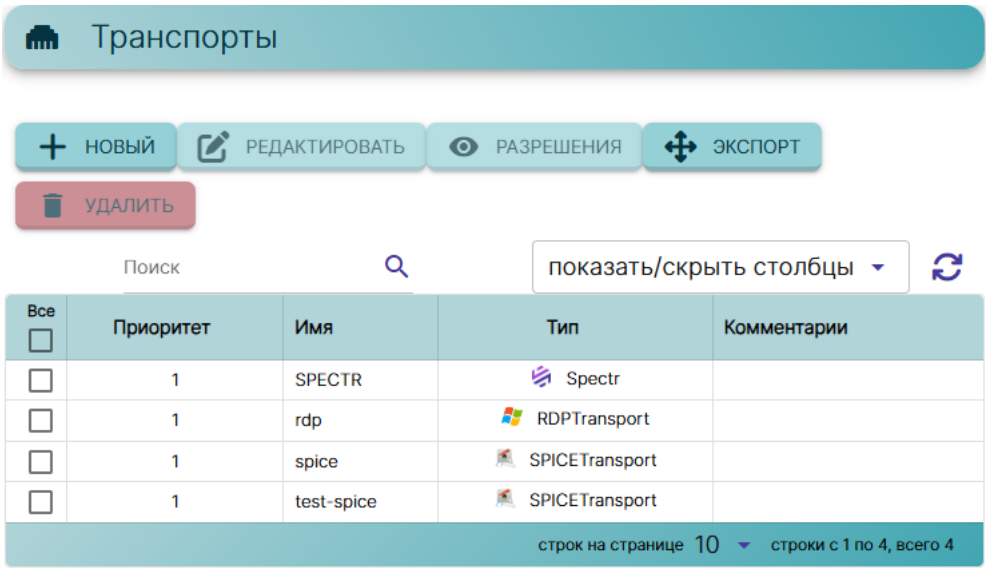


Рисунок 198

5.4.4 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**.

Для добавления транспорта:

1. Перейти в раздел **Подключение - > Транспорты -> Прямой -> X2Go**
2. Заполнить поля: (Рисунок 199):

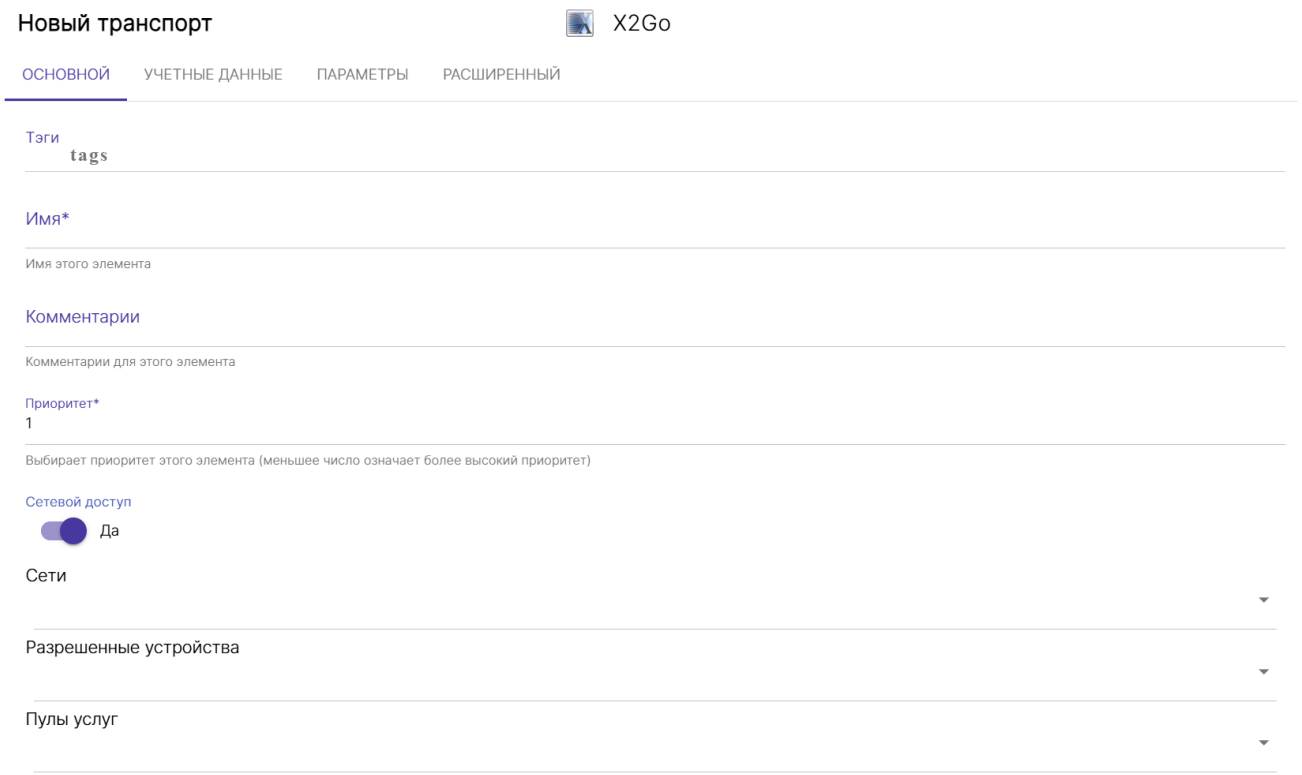


Рисунок 199

- **Имя: Имя транспорта.**
- **Приоритет**: приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортов для службы. Транспорт с наименьшим приоритетом будет использоваться по умолчанию при нажатии на изображение службы.
- **Сетевой доступ**: разрешает или запрещает доступ пользователя к службе в зависимости от сети, из которой осуществляется доступ, и сети, указанной в разделе **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.

– **Пулы услуг**: позволяет назначать этот транспорт непосредственно одному или нескольким ранее созданным «сервис-пулы».

3. В разделе **Учетные данные** (Рисунок 200):

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

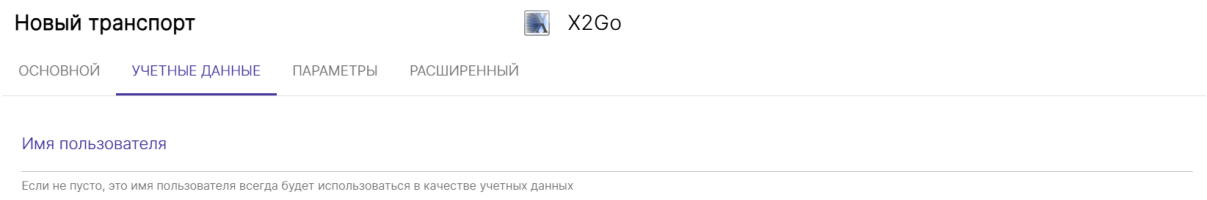


Рисунок 200

4. В разделе **Параметры** (Рисунок 201):

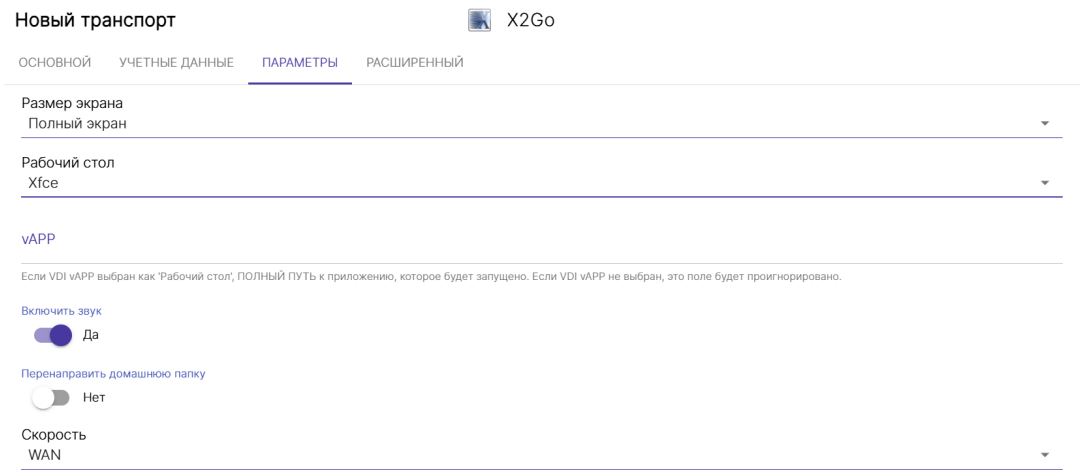


Рисунок 201

– **Размер экрана**: Разрешение окна подключения.

– **Рабочий стол**: 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.

5. В разделе **Расширенный** (Рисунок 202):

– **Звук**: Выбор типа звукового сервера.

– **Клавиатура**: Язык клавиатуры.

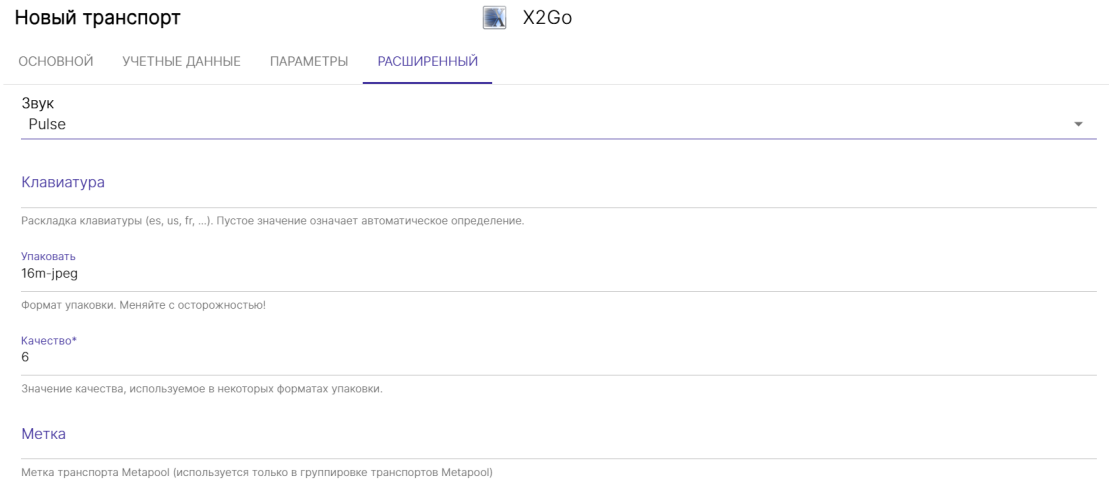


Рисунок 202

6. Нажать кнопку **Сохранить.**

5.4.1 Установка ограничений на авторизацию с устройства доступа пользователя

Для установки запрета на авторизацию с устройства пользователя необходимо:

1. Выбрать созданный ранее транспорт.

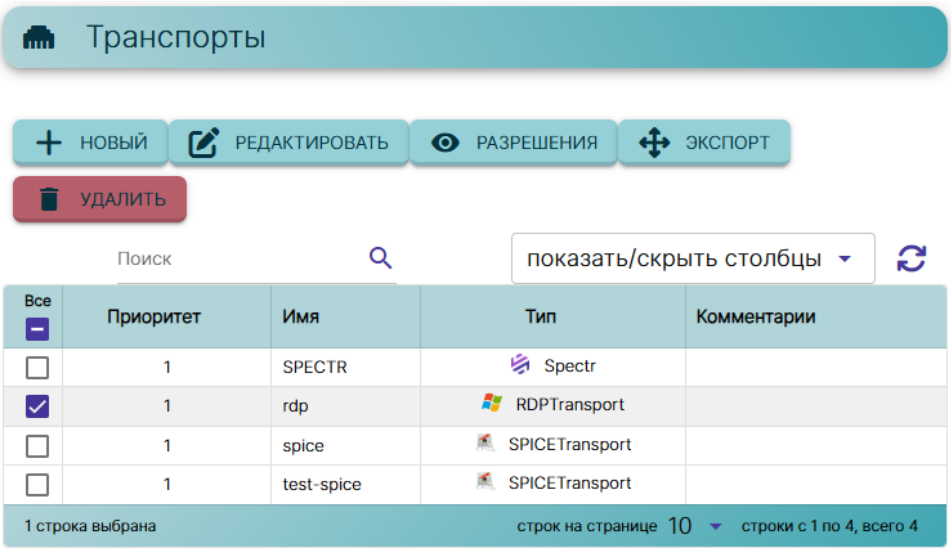
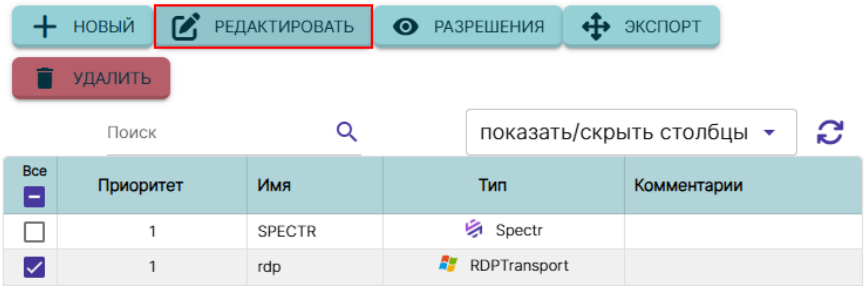
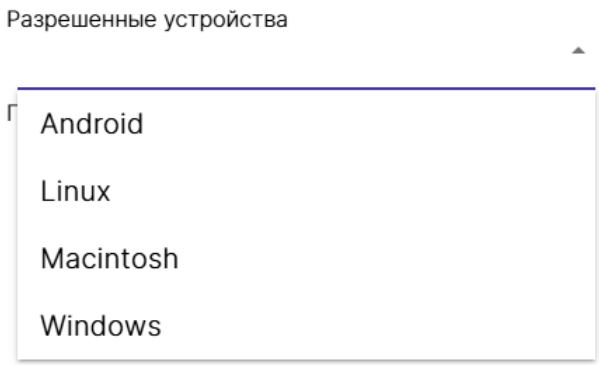


Рисунок 203

2. Нажать кнопку **Редактировать.**



3. Выбрать параметр **Разрешенные устройства.**
4. Выбрать, какое устройство разрешено для подключения.



5. Нажать кнопку **Сохранить.**

5.5 Сервис-пулы

Создание сервис-пула позволяет развернуть виртуальные рабочие столы или приложения и предоставить к ним доступ разным группам пользователей.

Для этого требуется:

- **Базовая служба** – включает поставщиков услуг и созданный в ней сервис.
- **Менеджер ОС** – отвечает за управление операционной системой в виртуальных машинах.

После создания сервис-пула необходимо назначить:

- одну или несколько групп пользователей, которым будет открыт доступ,
- один или несколько транспортов (способов подключения), через которые пользователи смогут заходить в систему.

5.5.1 Создание сессионного гостевого пула рабочих столов

1. Перед созданим гостевого пула необходимо убедиться, что был создан Менеджер ОС с политикой выхода – удаление (см п. 5.3).
2. Перейти в раздел **Пулы -> Пулы услуг**.

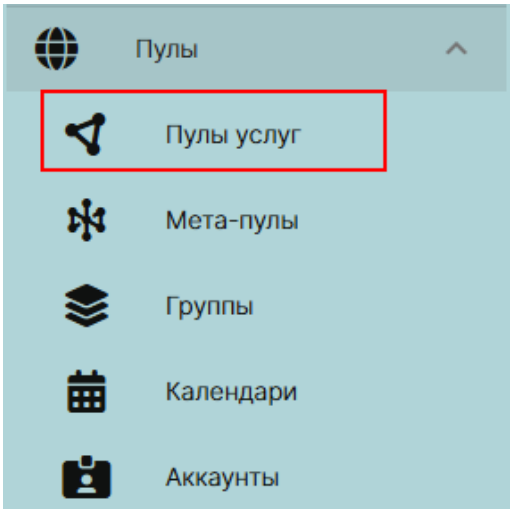


Рисунок 204

3. Нажать кнопку **Новый.**

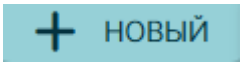


Рисунок 205

4. Откроется окно создания пула. На вкладке Основной заполнить поля:

- Имя;
- Короткое имя;
- Базовый сервис (поставщика услуг);
- Менеджер ОС;
- Опубликовать при создании – выключить.

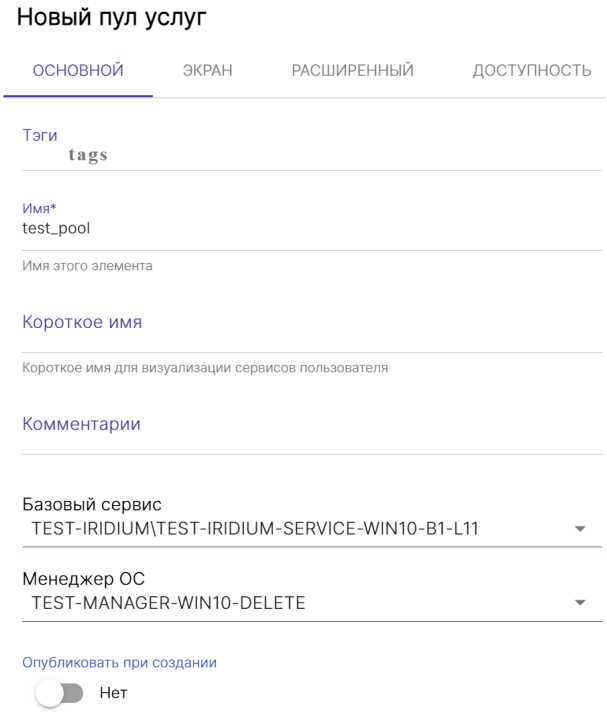


Рисунок 206

5. Перейти во вкладку **Доступность,** заполнить поля:

- Начальные доступные услуги: 1;
- Сервисы, хранящиеся в кеше: 1;
- Сервисы, хранящиеся в кеще L2: 0;
- Максимальное количество предоставляемые услуг:

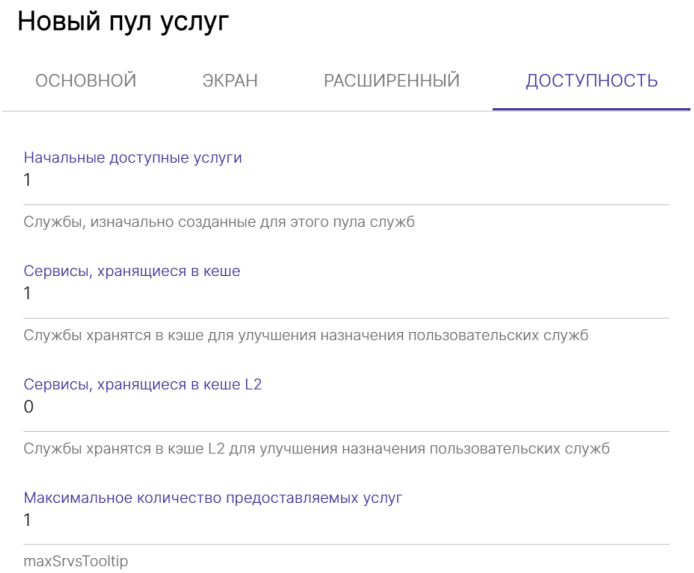


Рисунок 207

6. Нажать кнопку **Сохранить.**

Рисунок 208

7. После сохранения пул будет отображен в списке.

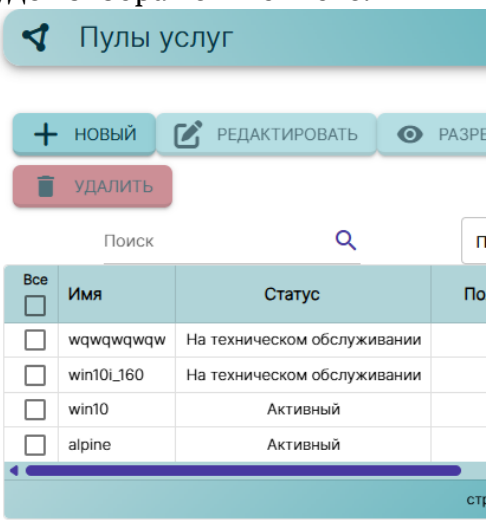


Рисунок 209

8. Нажать на созданный пул правой кнопкой мыши, затем нажать **Подробнее.**

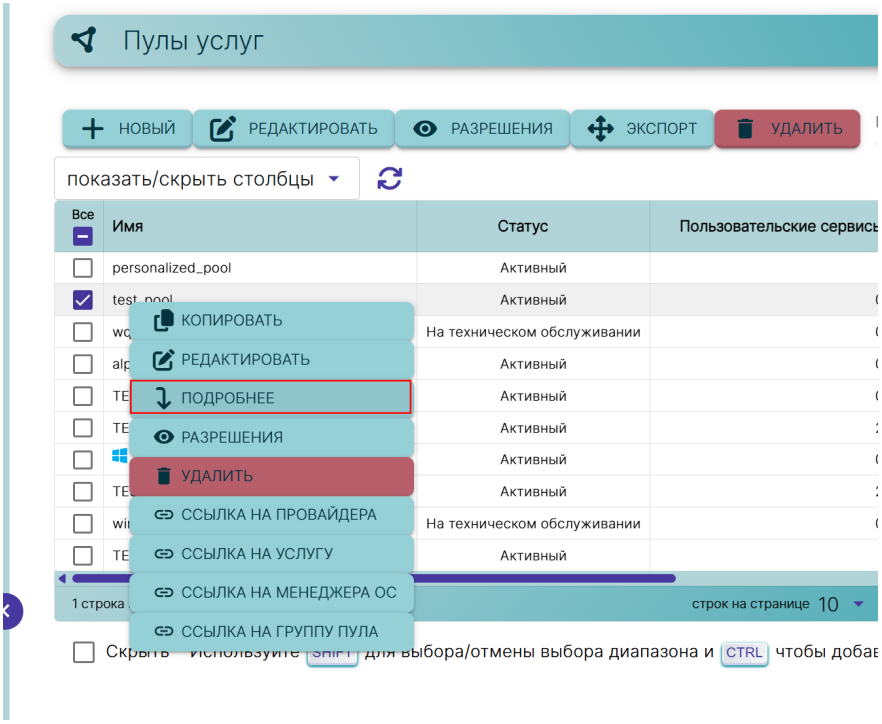


Рисунок 210

9. Перейти в раздел **Публикации**, нажать кнопку **Новый.**

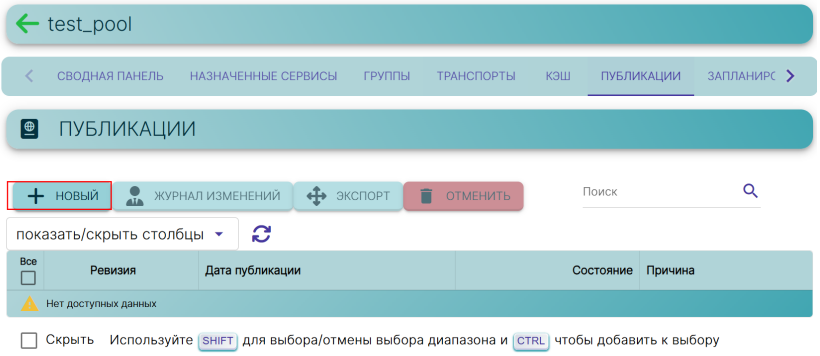


Рисунок 211

10. В открывшемся окне можно как внести текст, так и оставить поле пустым.
11. Нажать кнопку **Сохранить.**

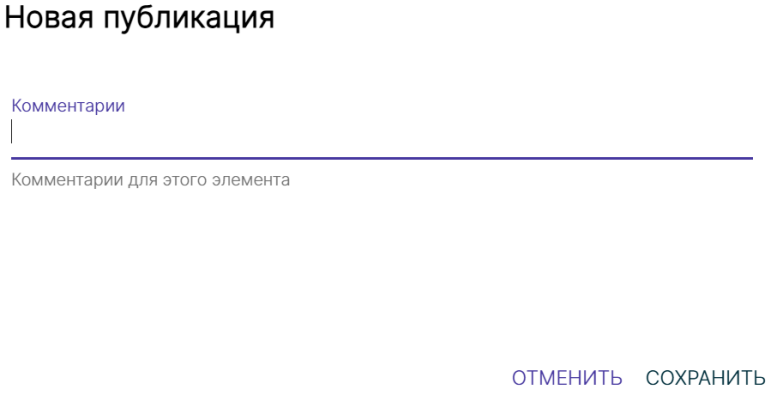


Рисунок 212

12. Пул будет создан.

5.5.1 Создание статического (персонализированного) пула рабочих столов

1. Необходимые требования к созданию статического пула:
   - Как минимум одна виртуальная машина на хосте;
   - Как минимум один поставщик статических IP-машин (см п. 5.1.1.2);
   - Как миниум один транспорт.
   - Как минимум один менеджер ОС с политикой при выходе из системы – **Сохранить назначенную услугу даже при новой публикации.**
2. Перейти в раздел **Пулы -> Пулы услуг.**

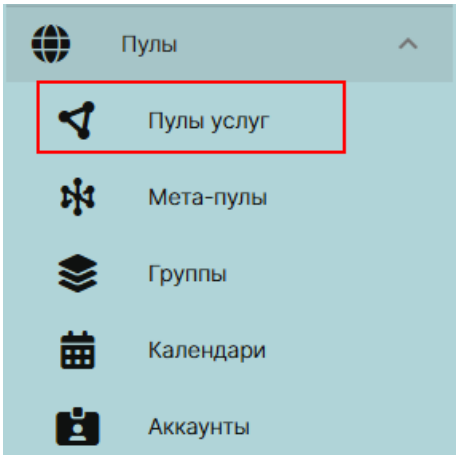


Рисунок 213

3. Нажать кнопку **Новый**.

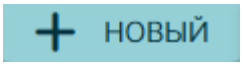


Рисунок 214

4. Откроется окно создания пула. На вкладке Основной заполнить поля:

– Имя;

– Базовый сервис (поставщика услуг);

– Менеджер ОС.

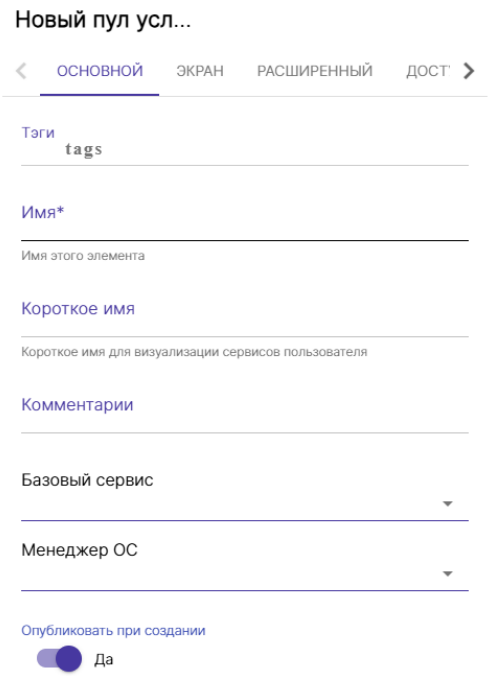


Рисунок 215

5. Нажать кнопку **Сохранить**.

Рисунок 216

6. После сохранения пул будет отображен в списке. ПО VDI начнет развертывание виртуальных машин согласно настройкам.

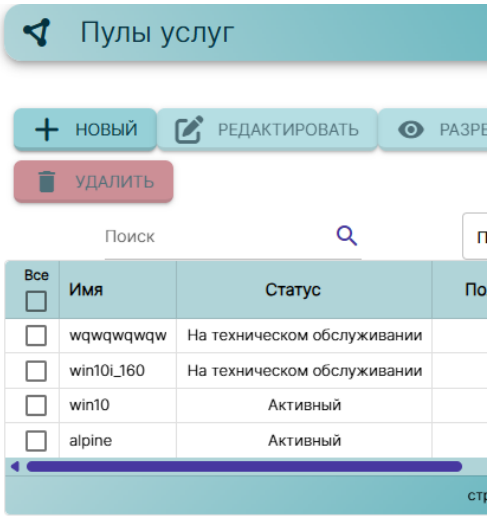


Рисунок 217

5.5.2 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 - Новый» (Рисунок 218).

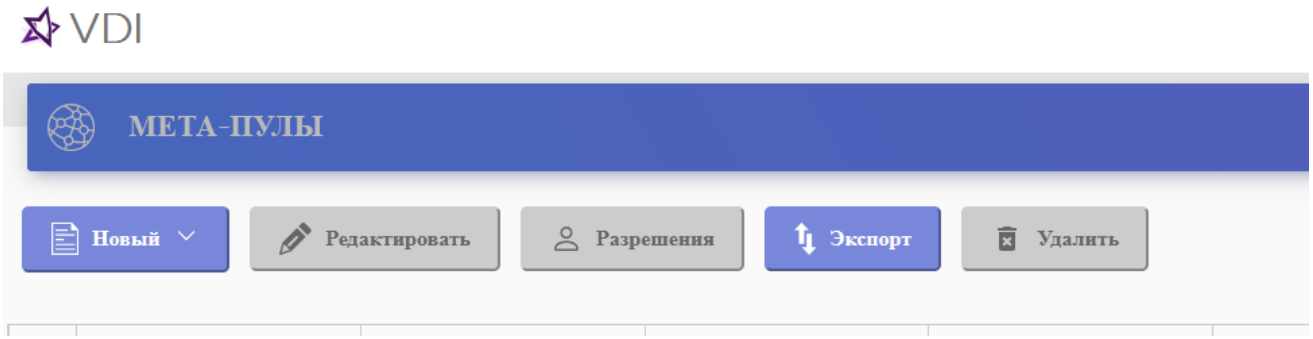


Рисунок 218

Для настройки «Метапула» необходимо будет указать:

- Основной (Рисунок 219):

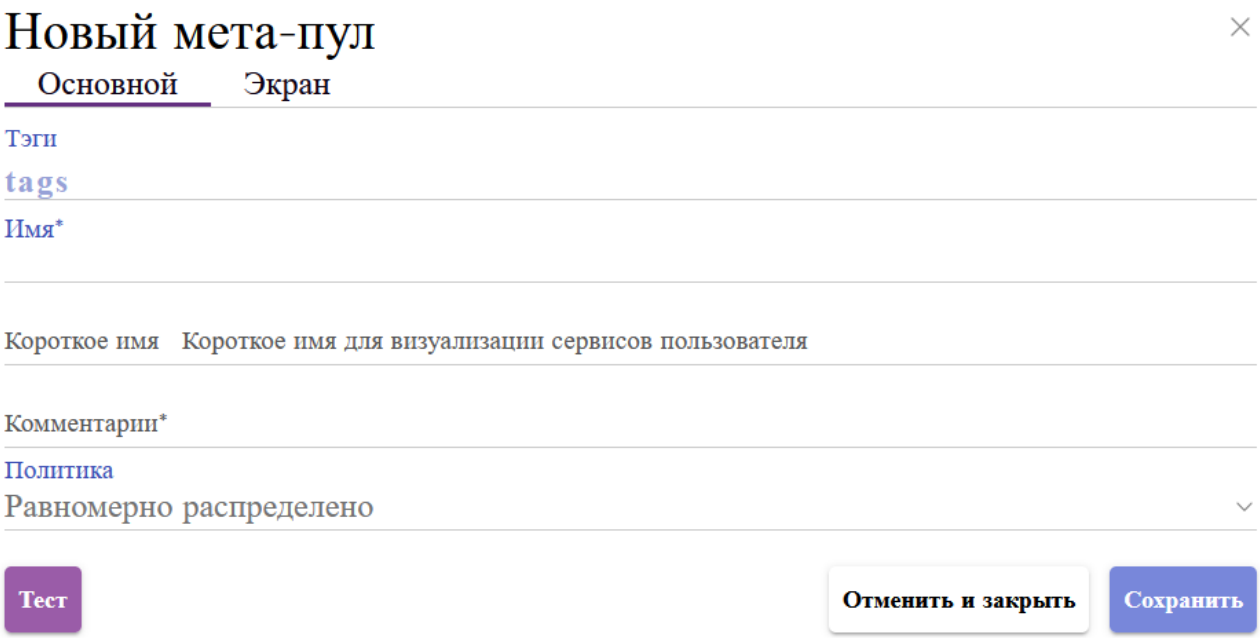


Рисунок 219

Тэги: дать мета-пулу тэг для удобства поиска.

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».

- Равномерно распределено: услуги будут создаваться и использоваться одинаково во всех «пулах услуг», составляющих «метапул».
- Приоритет: 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.
- Больший % доступно: службы будут создаваться и потребляться из «пула служб», который имеет самый высокий процент бесплатного использования.

- Экран (Рисунок 220):

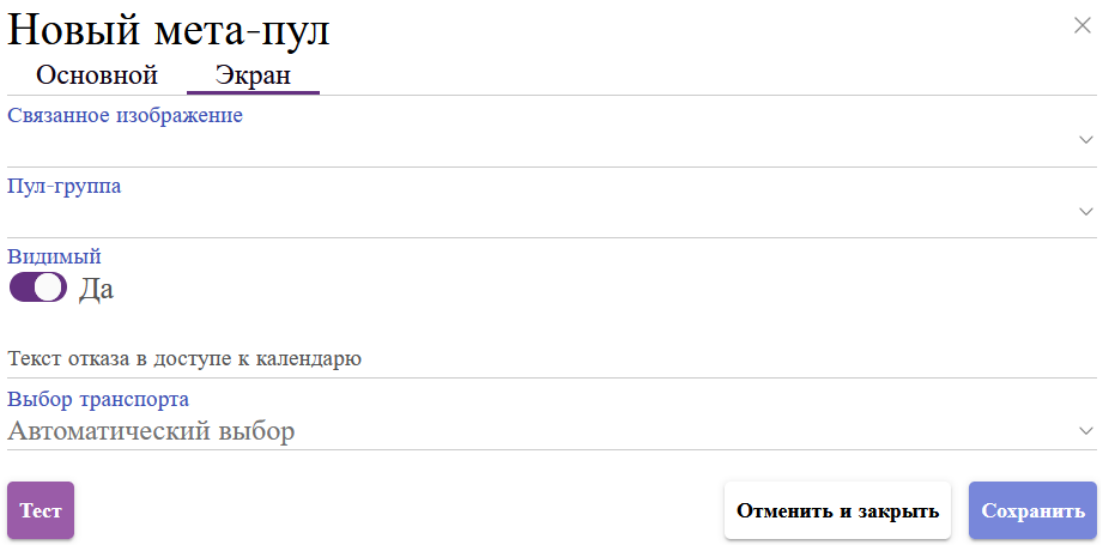


Рисунок 220

Связанное изображение: изображение, связанное с «метапулом». Он должен быть предварительно добавлен в хранилище изображений и доступен из раздела «Инструменты» — «Галерея».

Пул-группа: 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»).

Текст отказа в доступе к календарю: 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 221):

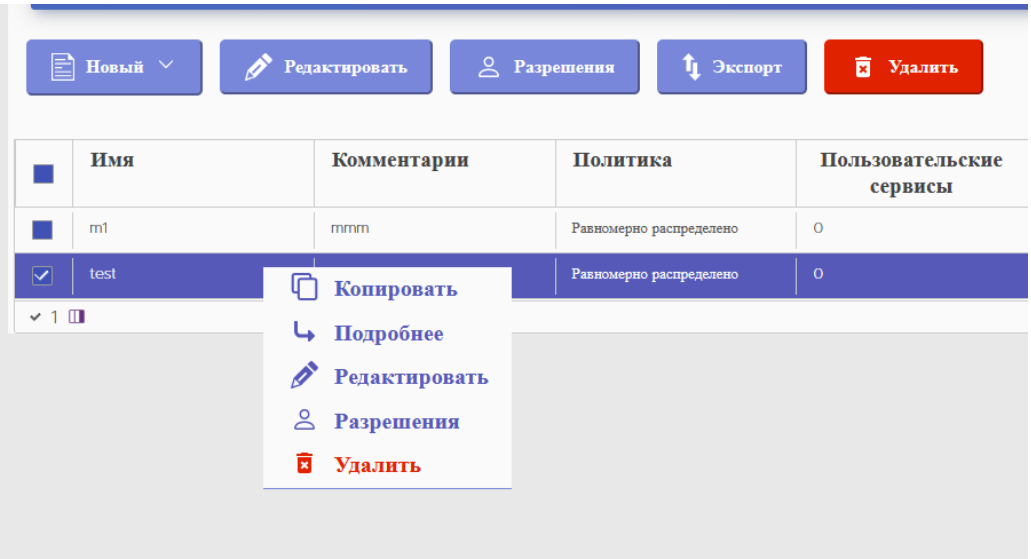


Рисунок 221

Нажать «Новый», 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 222).

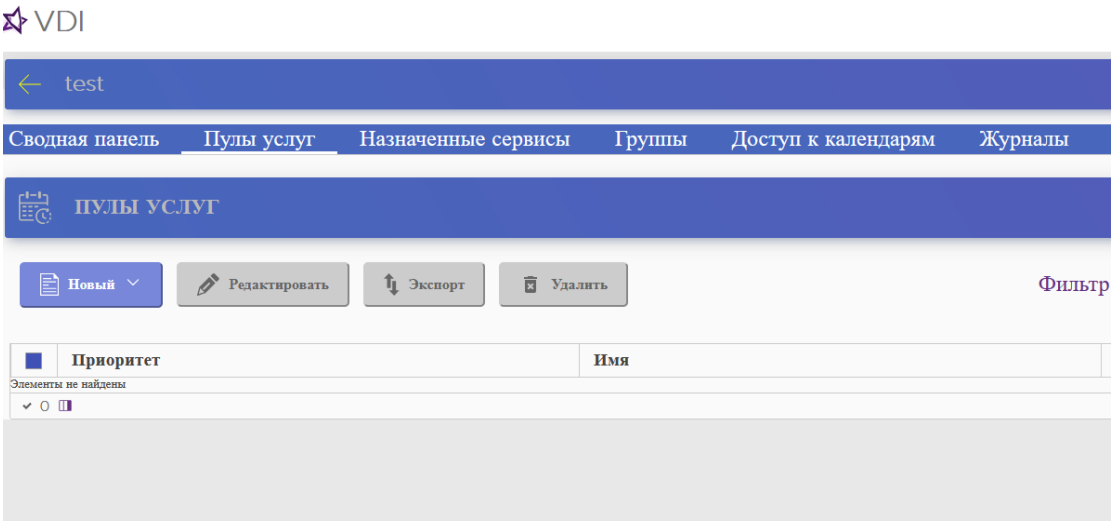


Рисунок 222

Для добавления «Сервисного пула» необходимо указать следующие параметры (Рисунок 223):

Приоритет: приоритет, который будет иметь «пул услуг» в «метапуле». Чем ниже значение, тем больший приоритет он имеет по отношению к остальным элементам.

Пул услуг: имя «пула услуг», который вы хотите добавить. Он должен быть предварительно создан.

Включено: Включает или отключает видимость «Метапула».

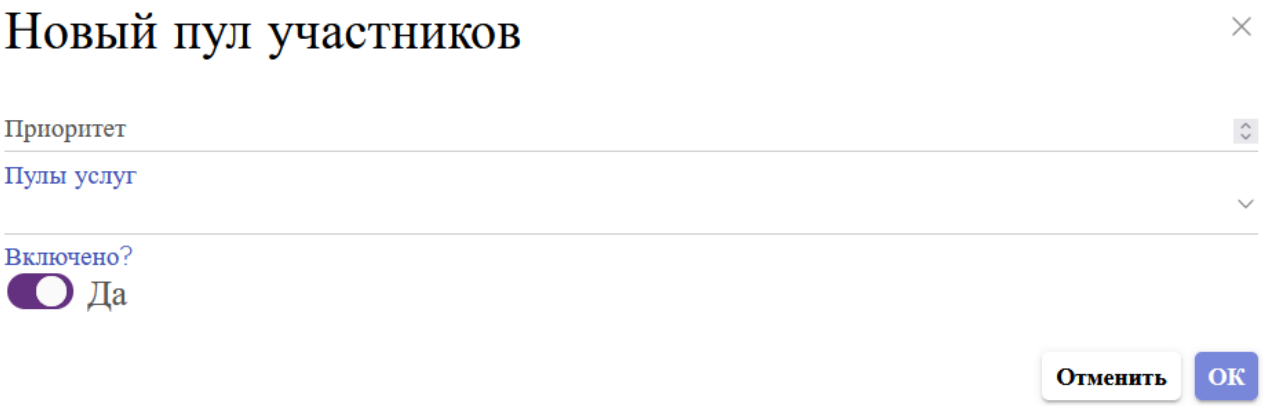


Рисунок 223

Можно добавить столько, сколько нужно, комбинируя службы, размещенные на разных платформах виртуализации (VMware, KVM, Azure и т. д.), серверах приложений и статических устройствах (Рисунок 224).

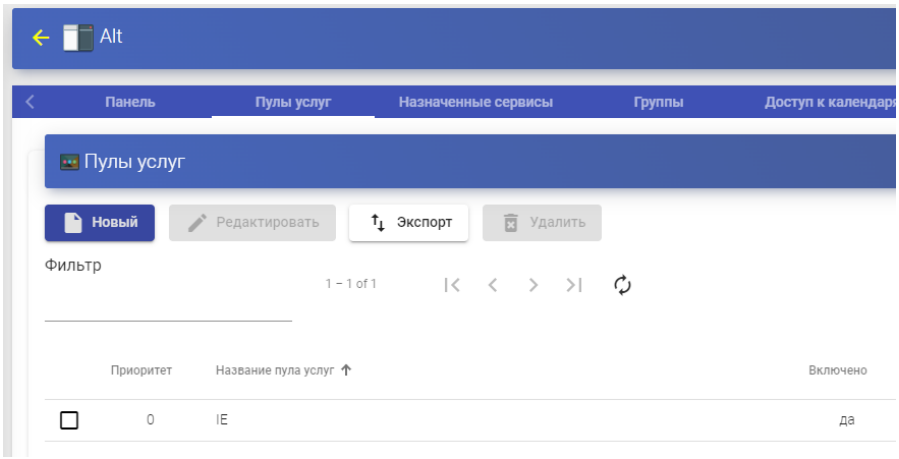


Рисунок 224

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.
- Доступ к календарям: позволяет применить ранее созданный календарь доступа.
- Журналы: Отображает все проблемы, возникшие в «Метапуле».

5.5.3 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 225).

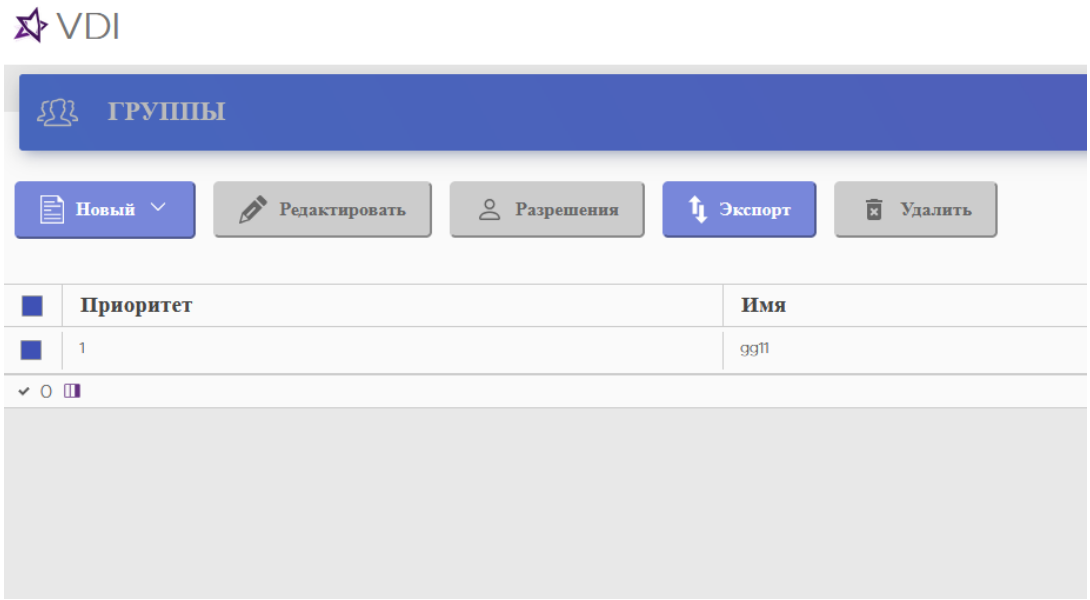


Рисунок 225

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 226):

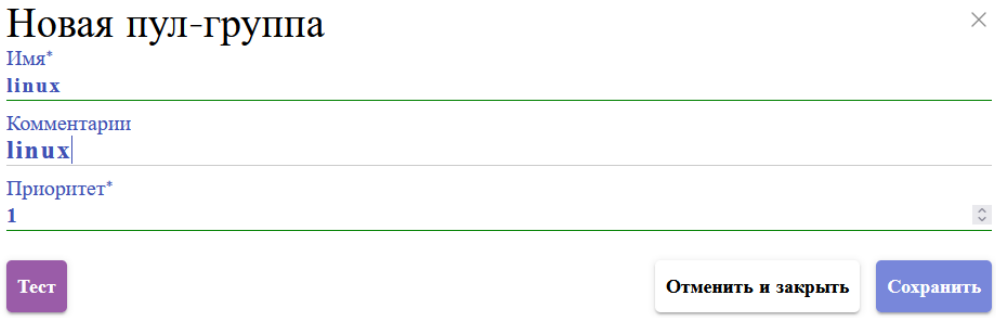


Рисунок 226

После создания он будет доступен для назначения в «Сервисный пул» (Рисунок 227).

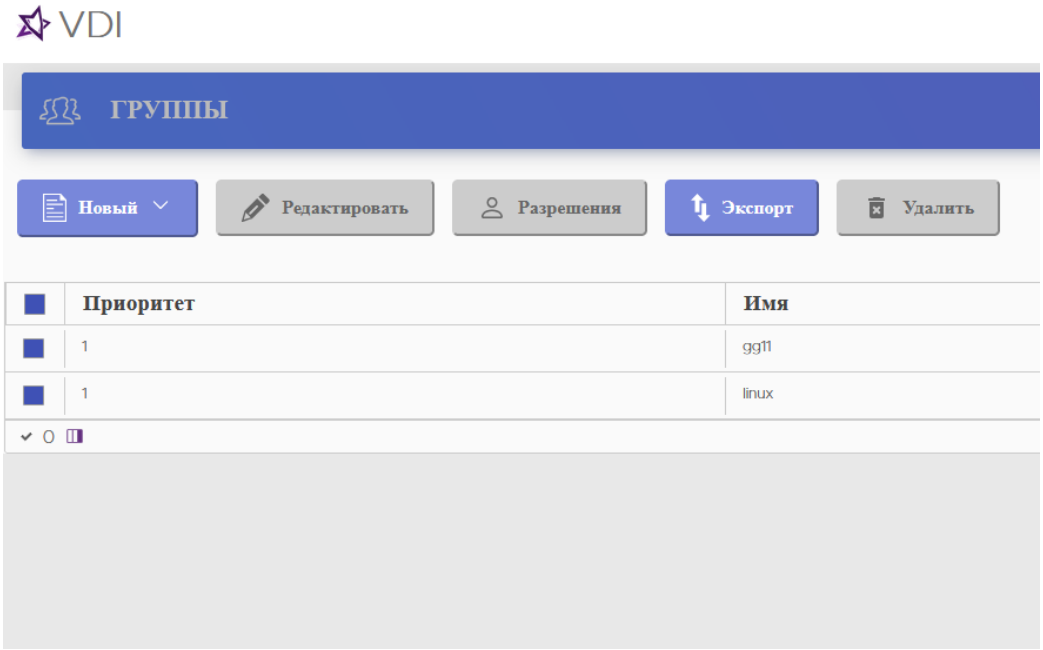


Рисунок 227

5.5.4 Доступ к календарям и запланированным задачам

VDI содержит встроенную систему календарей, которая позволяет управлять доступом пользователей к рабочим столам и виртуальным приложениям по датам и временным интервалам. С их помощью можно как разрешать, так и ограничивать использование сервисов.

Кроме того, календари позволяют автоматизировать задачи в рамках сервис-пула, например:

– публикацию новых версий,

– настройку параметров системного кэша,

– добавление или удаление групп пользователей и транспортов,

– изменение максимального числа доступных сервисов.

5.5.5 Календари

Для создания календаря:

1. Перейти в раздел **Пулы – Календари.**
2. Нажать кнопку **Новый.** (Рисунок 228).

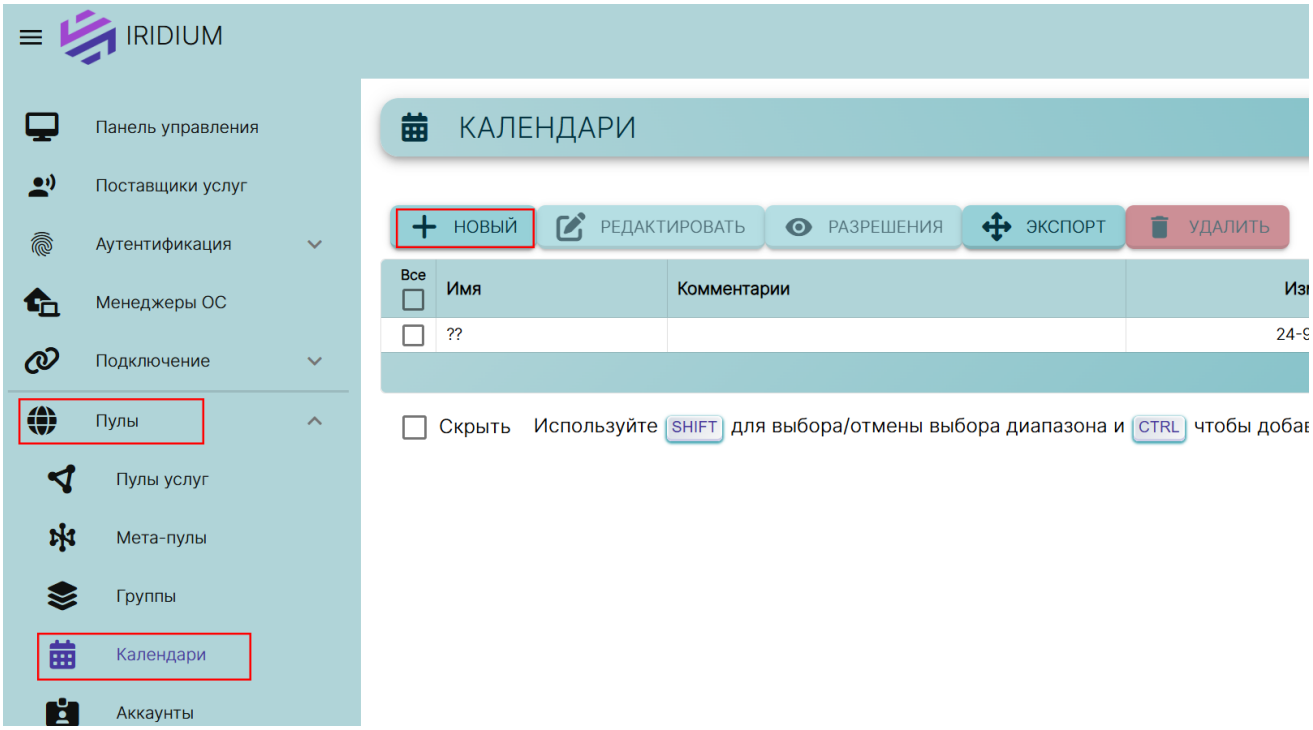


Рисунок 228

3. В открывшемся окне указать описательное имя для идентификации календаря (Рисунок 229).

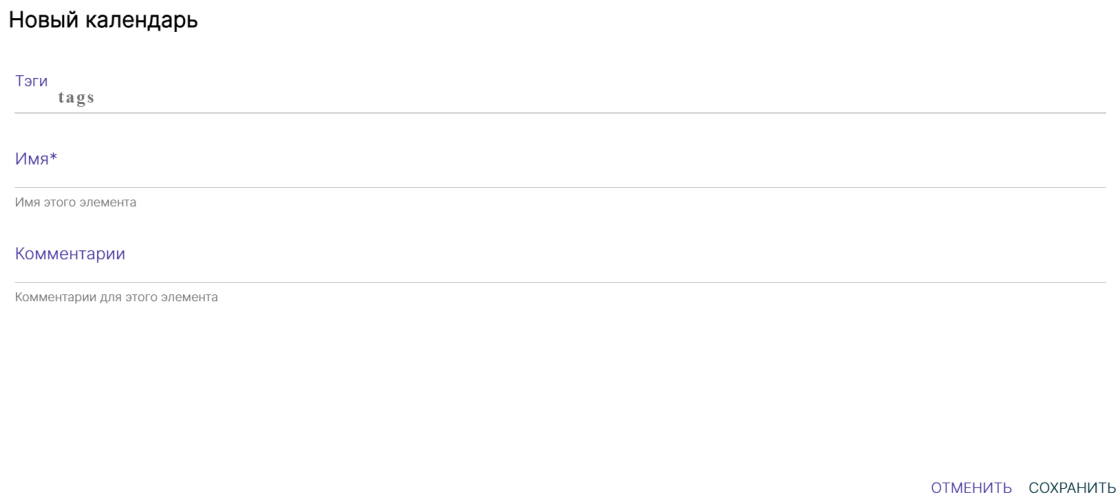


Рисунок 229

4. Нажать кнопку **Сохранить.** Календарь будет отображен в списке. (Рисунок 230).

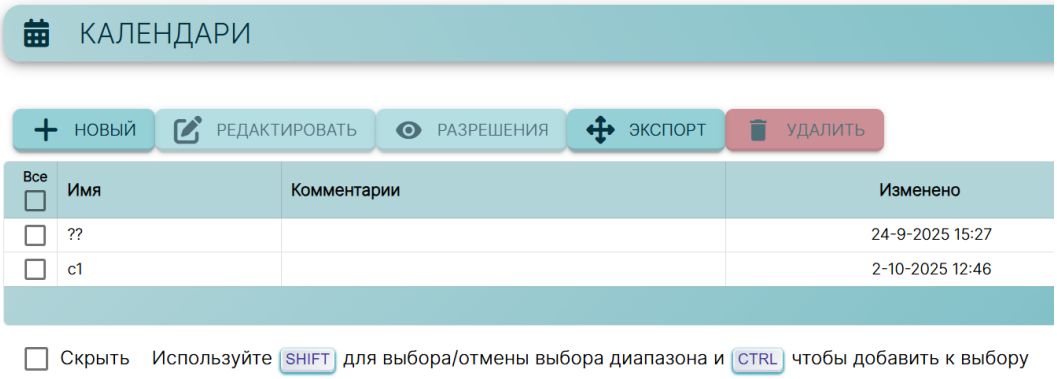


Рисунок 230

5.5.5.1 *Создание правил в календаре*

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

Для создания правила:

1. Нажать на календарь правой кнопкой мыши, выбрать **Подробнее.**

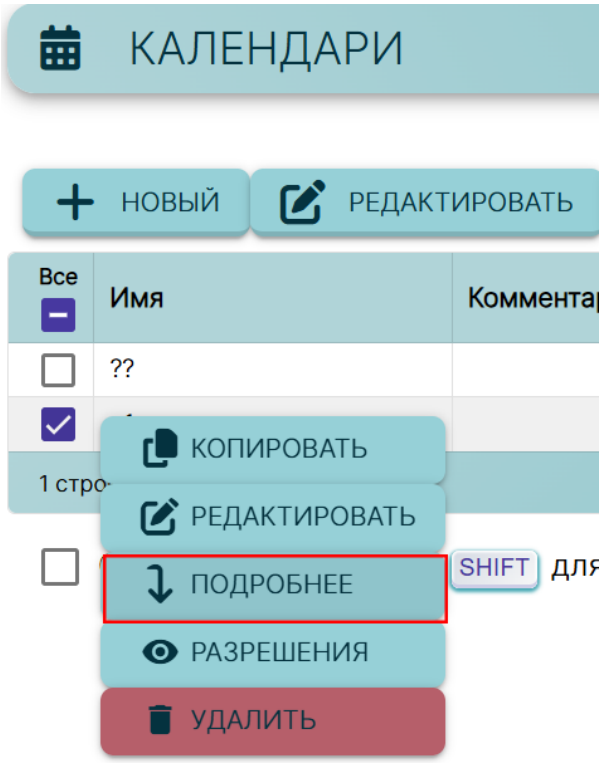


Рисунок 231

2. Нажать **Новый** (Рисунок 232).

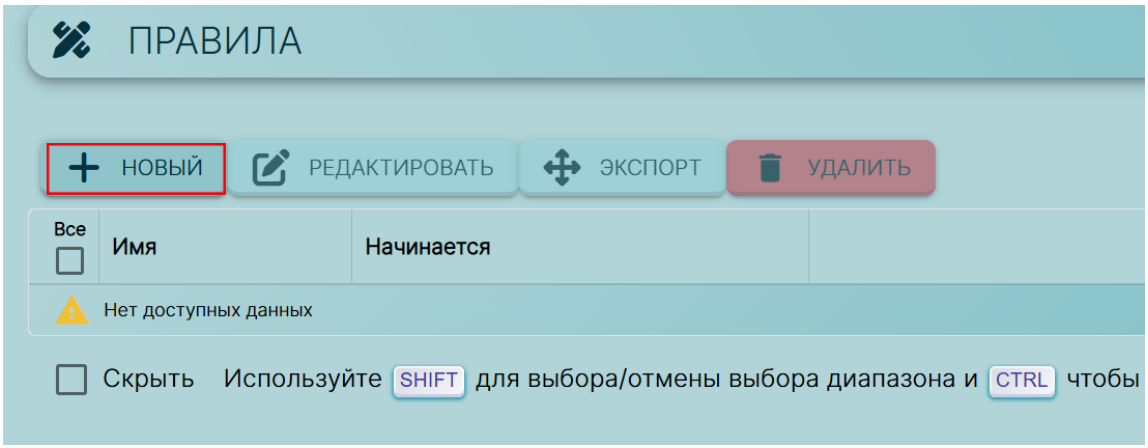


Рисунок 232

3. Заполнить поля:

– **Имя**: Имя правила.

– **Комментарии**: комментарии для нового правила.

– **Событие**: настройка периодов выполнения. Для этого указать время начала и продолжительность события (в минутах, часах, днях и месяцах).

– **Повторение**: в этом разделе можно настроить повторение правила в днях, неделях, месяцах, годах и даже позволяет указать рабочие дни.

– **Сводная панель**: показывает сводку всех ранее выполненных настроек.

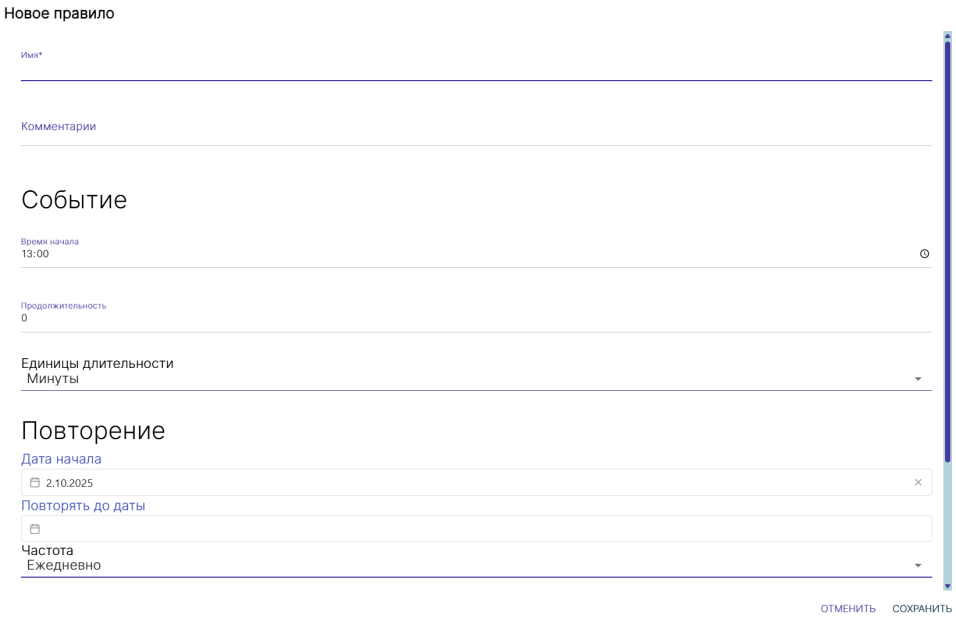


Рисунок 233

4. Нажать кнопку **Сохранить.** После сохранения действующее правило будет назначено Сервис-пулу (виртуальному рабочему столу и/или приложению).

5.5.5.2 *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.

Для этого необходимо:

1. Перейти в раздел **Пулы – Пулы услуг.**
2. Выбрать созданный ранее пул.

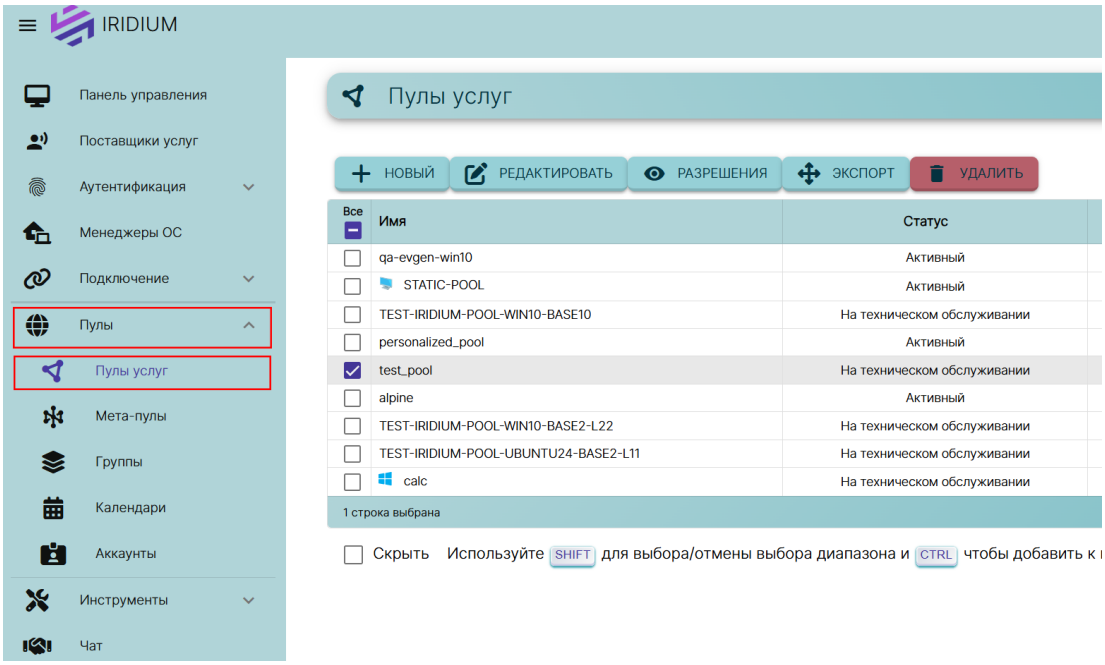


Рисунок 234

3. Нажать на пул правой кнопкой мыши, затем нажать **Подробнее.**

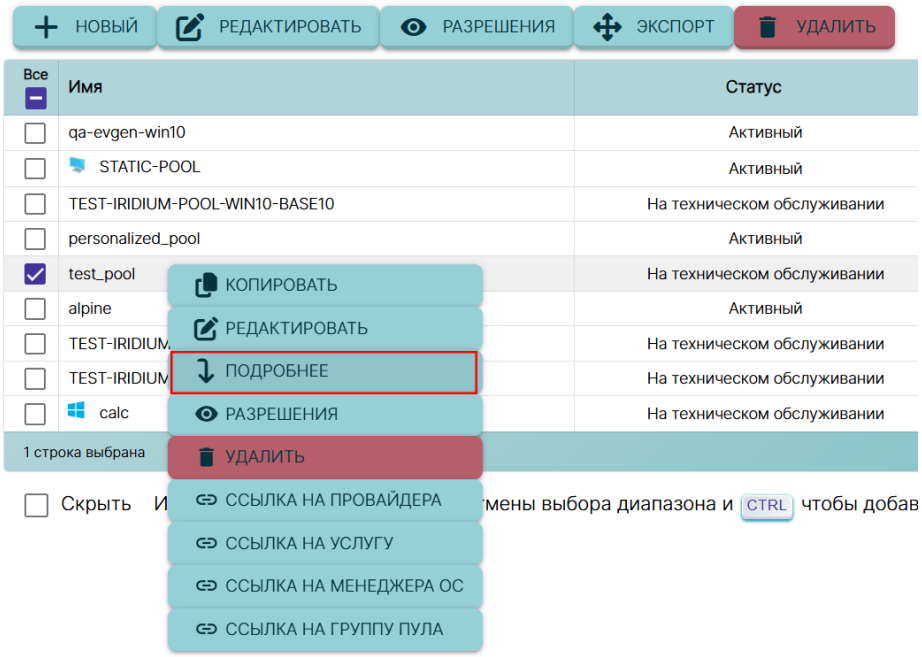


Рисунок 235

4. Перейти в раздел **Доступ к календарям.** Нажать кнопку **Новый.**

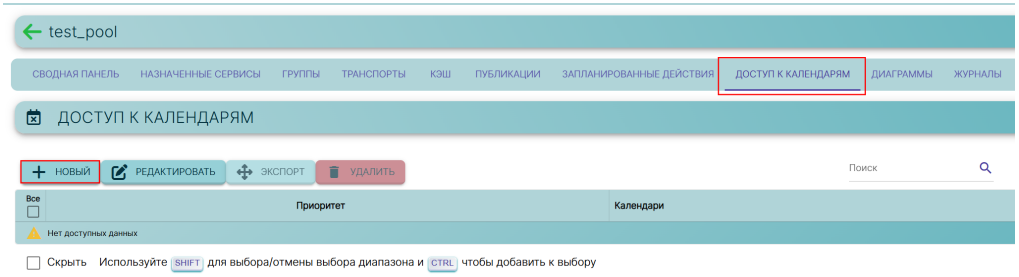


Рисунок 236

5. Указать приоритет доступа, выбрать существующий календарь и отметить действие, которое будет применяться при доступе к сервису (Рисунок 237).

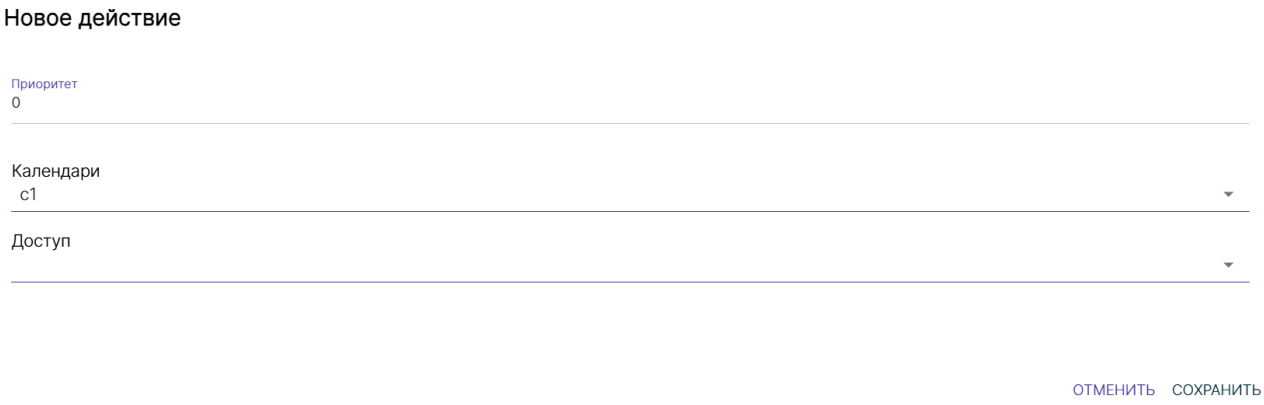


Рисунок 237

6. Нажать кнопку **Сохранить.** Календарь будет отображен в списке. (Рисунок 238).

Рисунок 238

5.5.5.3 *Запланированные действия*

После настройки правил в календарях можно использовать их для планирования определенных задач в пуле услуг.

Чтобы применить эти календари с их правилами:

1. Перейти в раздел **Пулы – Пулы услуг.**
2. Выбрать **Пул услуг**. Нажать правой кнопкой мыши, выбрать **Подробнее.**

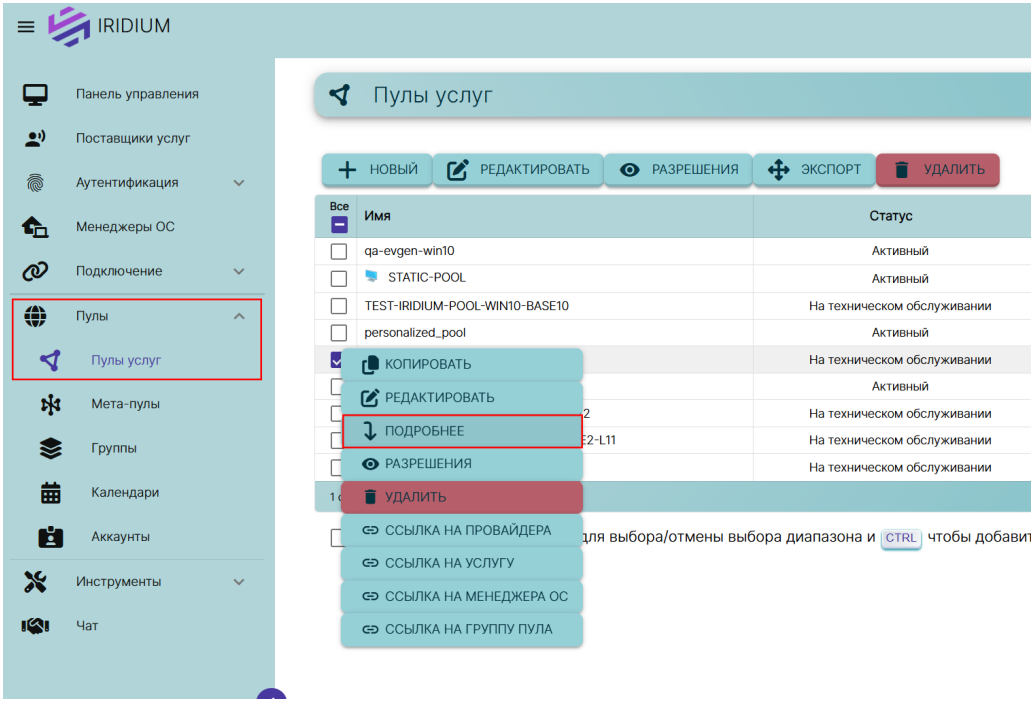


Рисунок 239

3. Перейти на вкладку **Запланированные действия** и нажать **Новый** (Рисунок 240).

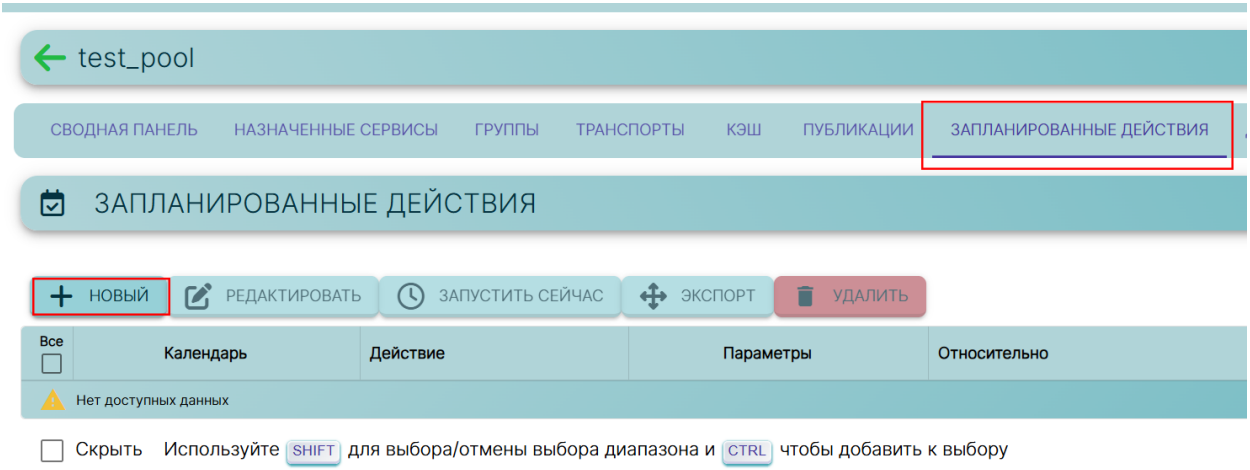


Рисунок 240

4. В поле **Календари** указать существующий календарь, время, в течение которого будет выполняться действие и выбрать действие, которое необходимо выполнить.
5. **Смещение событий**: в минутах указать периодичность события.
6. **В начале интервала**: выполнять действие в начале интервала.
7. Доступные запланированные действия:

– **Добавить транспорт**: добавляет существующий транспорт в Пул услуг.

– **Удалить транспорт**: удаляет транспорт из пула услуг.

– **Удалить все транспорты**: удалить все транспорты из пула услуг.

– **Добавить группу**: добавляет существующую группу в Пул услуг.

– **Удалить группу**: удаляет группу из пула услуг.

– **Удалить все группы**: удалиьь все группы из пула услуг.

– **Устанавливает игнорирование неиспользуемых**: устанавливает параметр Игнорировать неиспользуемые.

- **Удалить ВСЕ назначенные пользовательские службы**: удаляет все службы, назначенные пользователям в пуле служб.
- **Удалить СТАРЫЕ назначенные пользовательские службы**: удаление всех старых назначенных пользовательских слжуб в пуле служб.

8. После сохранения будет запланированная задача, которая выполняет определенное действие в пуле услуг.

5.5.6 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 241). Можно создать пользователя с нуля, а можно отредактировать существующего пользователя Для этого необходимо:

1. Перейти в **Аутентификация -> Аутентификаторы -> База данных -> Пользователь -> Редактировать**.
2. Выбрать роль – Сотрудник.

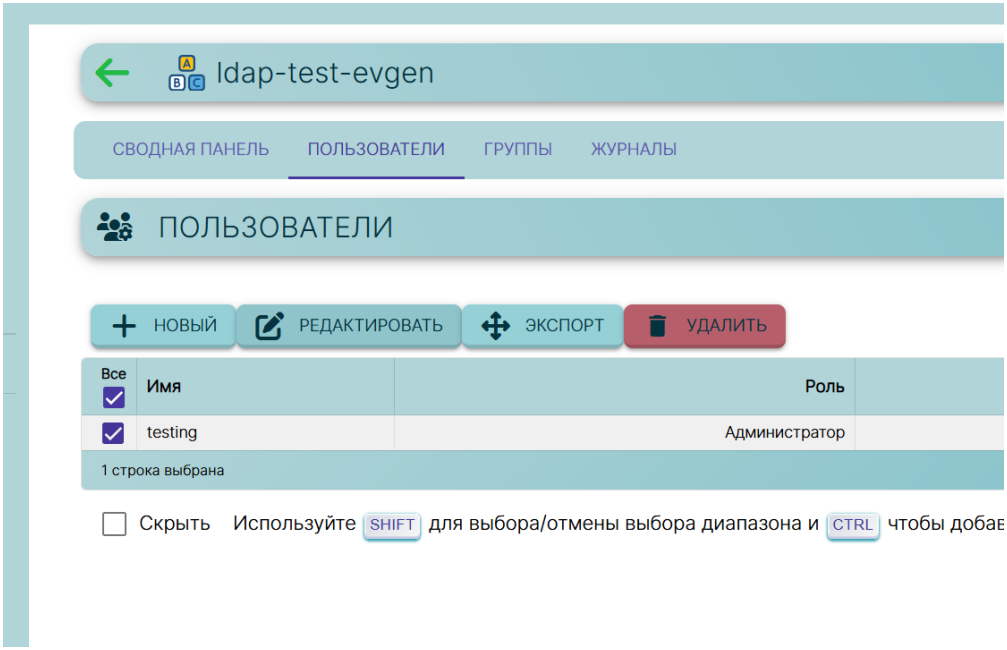


Рисунок 241

3. Далее необходимо перейти в элемент администрирования (Поставщики услуг, пулы услуг). Например, в **Поставщик услуг** (Рисунок 242).

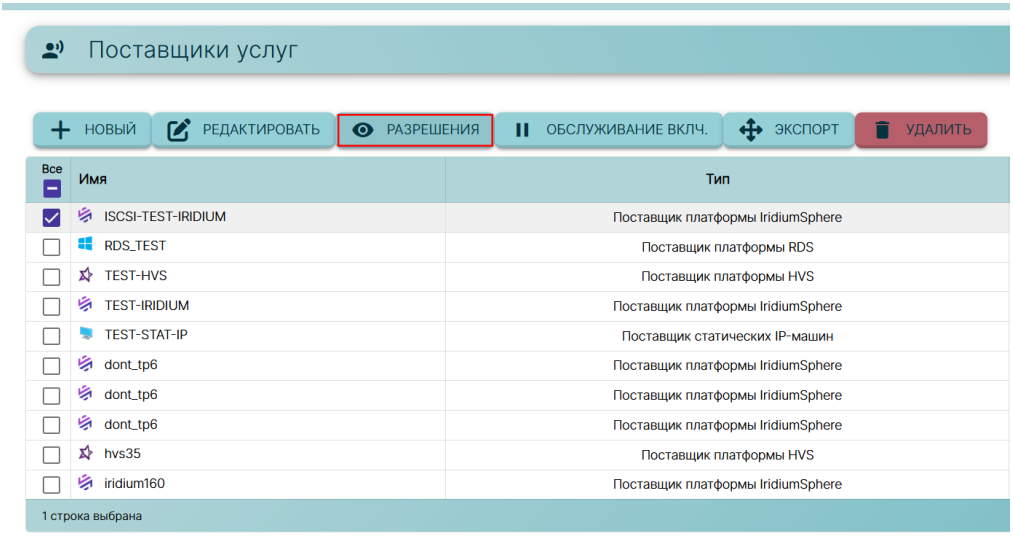


Рисунок 242

4. Нажать кнопку **Разрешения.** В окне разрешений нажать **Новое разрешение**… для групп и пользователей и выбрать аутентификатор и группу/пользователя, к которым будет применяться разрешение (Рисунок 243).

Рисунок 243

5. Нужно указать, будет ли этот пользователь или группа иметь доступ для чтения к элементу («Только чтение») или полный доступ («Полный доступ») (Рисунок 244).

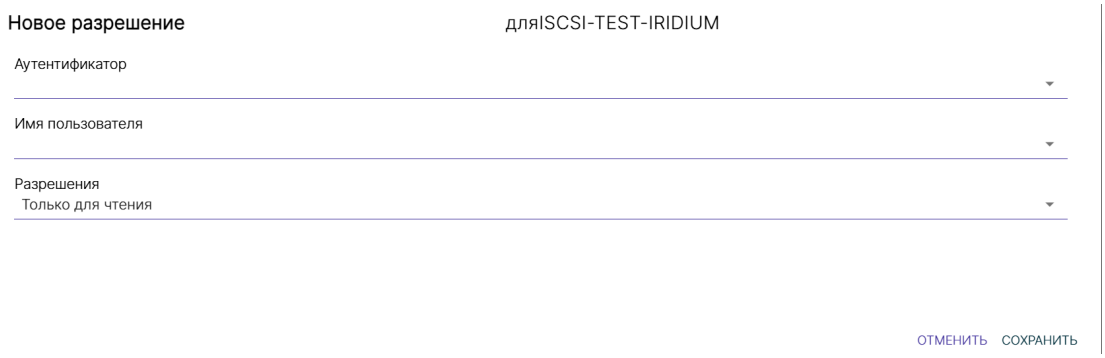


Рисунок 244

6. После применения пользователи, у которых включена опция «Сотрудник», смогут получить доступ к этому элементу администрирования с назначенными разрешениями (Рисунок 245).

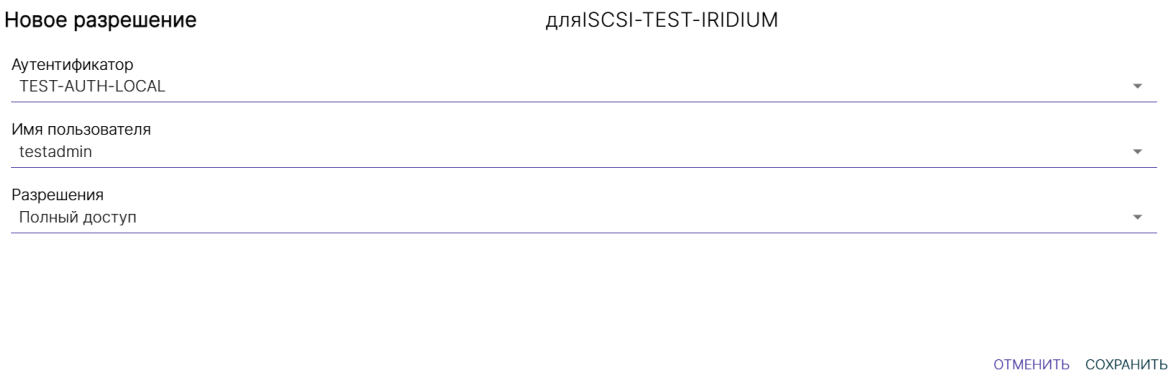


Рисунок 245

7. Нажать кнопку **Сохранить.**

6 ПАРАМЕТРЫ КОНФИГУРАЦИИ VDI

6.1 Раздел «Конфигурация»

В системе VDI существует набор параметров, управляющих её работой. Эти настройки отвечают за безопасность, режим функционирования, подключения, а также за взаимодействие между самой системой VDI и зарегистрированными в ней виртуальными платформами.

Примечание: после изменения значений любой из переменных расширенной конфигурации VDI необходимо перезапустить сервер VDI, чтобы изменения вступили в силу.

Для просмотра конфигурации необходимо перейти в раздел **Инструменты -> Конфигурация** (Рисунок 246):

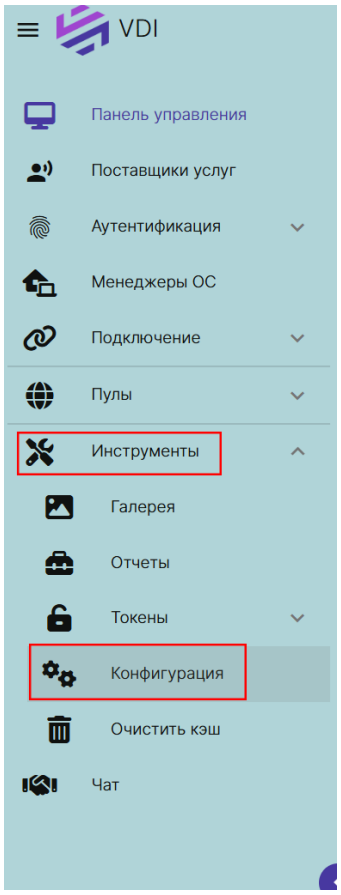


Рисунок 246

6.1.1 Вкладка «VDI»

Эта вкладка предназначена для централизованного управления параметрами безопасности, доступом и системными ограничениями в рамках административной панели.

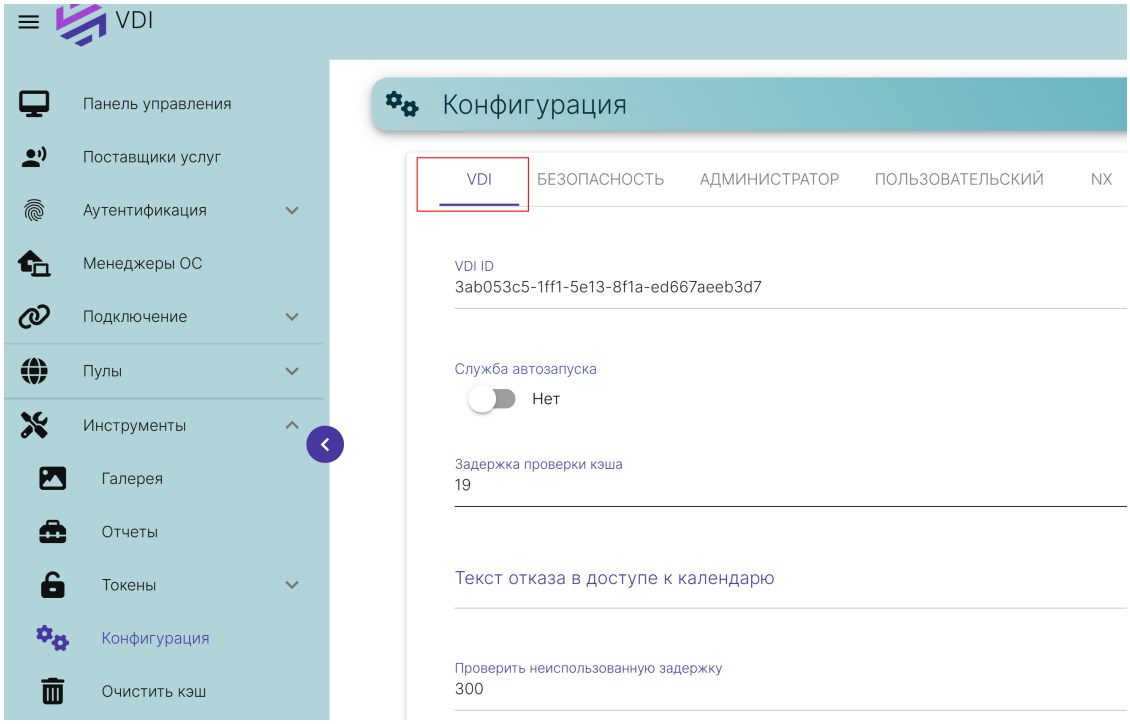


Рисунок 247

Настраиваемые параметры:

1. **VDI ID**. Это уникальный идентификатор установленного VDI.
2. **Служба автозапуска**. Флаг, определяющий, должна ли служба запускаться автоматически при старте системы. По умолчанию выключено.
3. **Задержка проверки кэша**. Временной интервал между проверками состояния кеша или его валидации. По умолчанию: 19
4. **Проверить неиспользованную задержку**. Период времени, по истечении которого система проверяет ресурсы, находящиеся в состоянии простоя. По умолчанию: 300.
5. **Проверить неиспользованное время**. Максимально допустимое время неактивности ресурса перед выполнением проверки или его освобождением. По умолчанию: 631.

6. **Проверка очистки**. По умолчанию: 3607. Интервал времени (в секундах), через который выполняется задача очистки временных файлов или устаревших данных.
7. **Потоки отложенных задач**. Количество параллельных потоков обработки для выполнения фоновых или отложенных заданий. По умолчанию: 4.
8. **Запретить глобальный вход**. Флаг, активация которого блокирует возможность входа в систему с нескольких устройств одновременно под одной учетной записью. Может быть использовано при техническом обслуживании. По умолчанию выключено.
9. **Экспериментальные функции**. Флаг, разрешающий или запрещающий доступ к нестабильным функциональным возможностям, находящимся в стадии тестирования По умолчанию выключено.
10. **Игнорировать ограничения**. По умолчанию: Нет. Если включено — обходит системные лимиты (может применяться в режиме отладки или в чрезвычайных ситуациях).

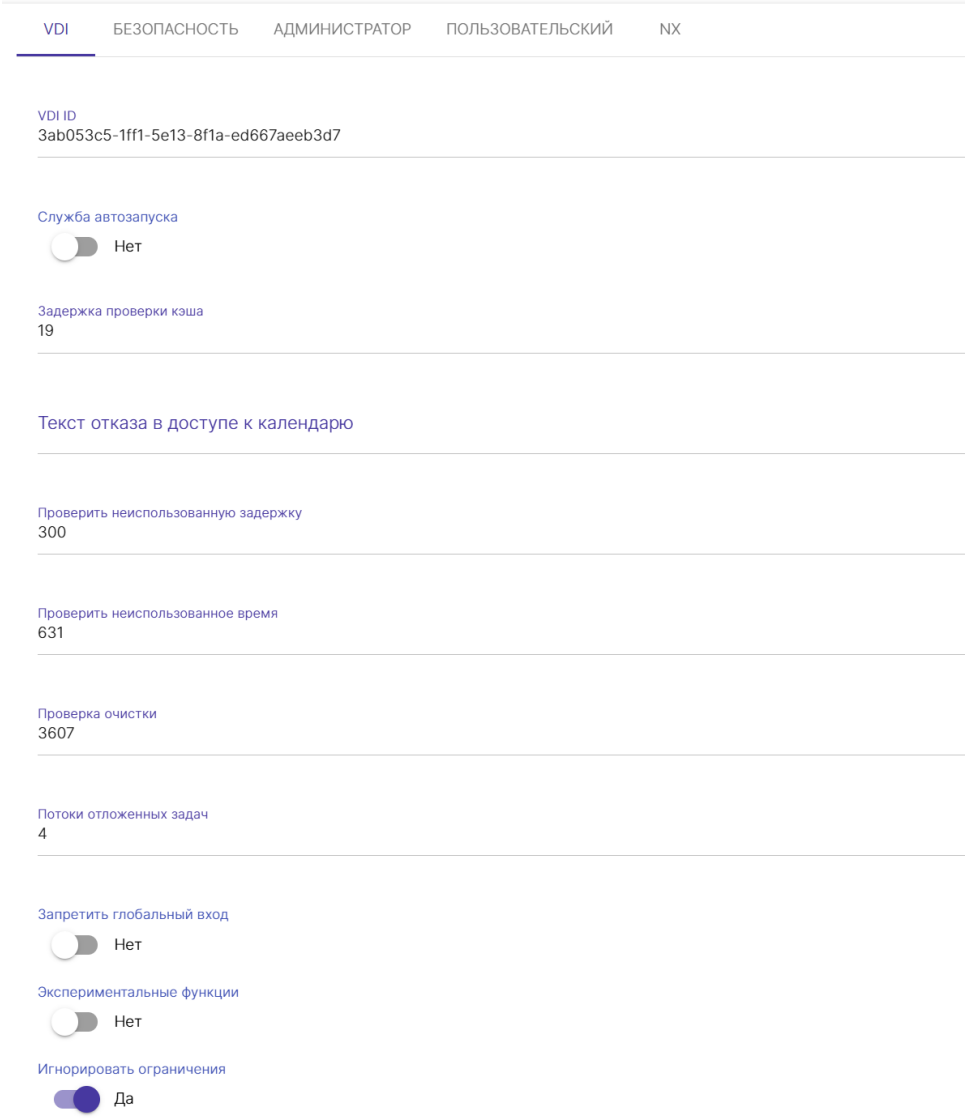


Рисунок 248

11. **Сохранять информацию о времени**. Период времени (в секундах), в течение которого система хранит детальную временную метаинформацию о событиях или операциях. По умолчанию: 14401.
12. **Максимальное время инициализации**. Максимально допустимое время (в секундах) для полной инициализацииVDI-сессии. По умолчанию: 3601.
13. **Максимальный журнал на элемент**. Ограничение на количество записей журнала, хранящихся для одного объекта системы. По умолчанию: 100.
14. **Максимальное количество услуг по подготовке**. Лимит количества сервисов, которые могут подготавливаться к работе одновременно. По умолчанию: 15.

15. **Максимальное время удаления**. Предельное время, отведенное системе на выполнение операции удаления сложного объекта или группы данных. По умолчанию: 14400.
16. **Максимальное количество услуг по удалению**. Лимит количества сервисов, которые могут быть удалены в рамках одной операции. По умолчанию: 15

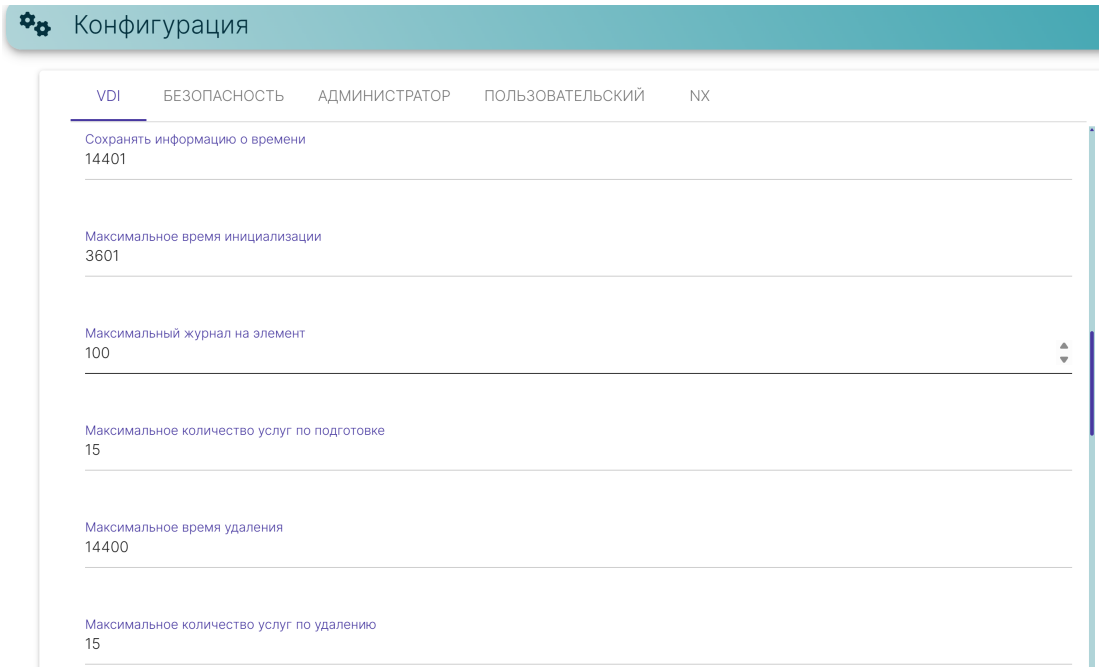


Рисунок 249

17. **Новое максимальное ограничение**. Флаг активации альтернативной логики ограничения доступа или ресурсов, используется при внедрении новых политик. По умолчанию выключено.
18. **Уведомить о новой публикации**. Флаг, определяющий, будут ли пользователи уведомленны о появлении новых публикаций пула. По умолчанию выключено.
19. **Время перезагрузки страницы**. Интервал (в секундах), через который клиентская часть интерфейса автоматически обновляет данные с сервера. По умолчанию: 300.
20. **Перенаправить на Https**.. Флаг, принудительно перенаправляющий все HTTP-запросы на защищенное HTTPS-соединение. По умолчанию включено.

21. **Проверка удаления**. Период (в секундах) между циклами проверки успешности удаления. Каждые 31 секунду система проверяет, что помечено на удаление, и окончательно уничтожает эти данные, освобождая место. По умолчанию: 31 сек.
22. **Ограничить количество**. По умолчанию: 3. Задает лимит на количество сущностей или операций.
23. **Ограничить количество.** По умолчанию: 600. Аналогично предыдущему параметру, но используется для другого ресурса или уровня доступа.

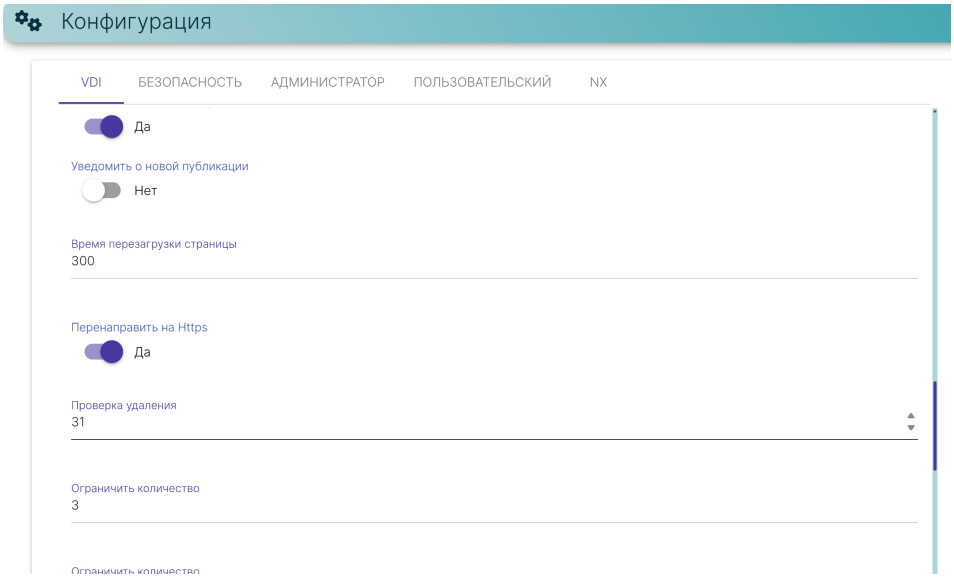


Рисунок 250

24. **Потоки планировщика**. Количество потоков, обрабатывающих задачи, связанные с планированием (scheduler workers). По умолчанию: 3.
25. **Время истечения сеанса**. Максимальная продолжительность (в минутах) для пользовательской сессии, после которого потребуется повторная авторизация. По умолчанию: 24
26. **Частота накопления статистики**. Интервал (в секундах) между циклами сбора и агрегации системной статистики. По умолчанию: 14400
27. **Максимальное время накопления статистики**. Период (в днях), в течение которого собираются детальные данные для статистики перед их архивацией или агрегацией.

28. **Длительность статистики**. Срок (в днях), в течение которого статистические данные хранятся в системе перед окончательным удалением. По умолчанию: 365.

29. **Номер очистки службы пользователя**. Идентификатор или порядковый номер задачи, отвечающей за очистку данных, связанных с неактивными пользовательскими службами. По умолчанию: 8.

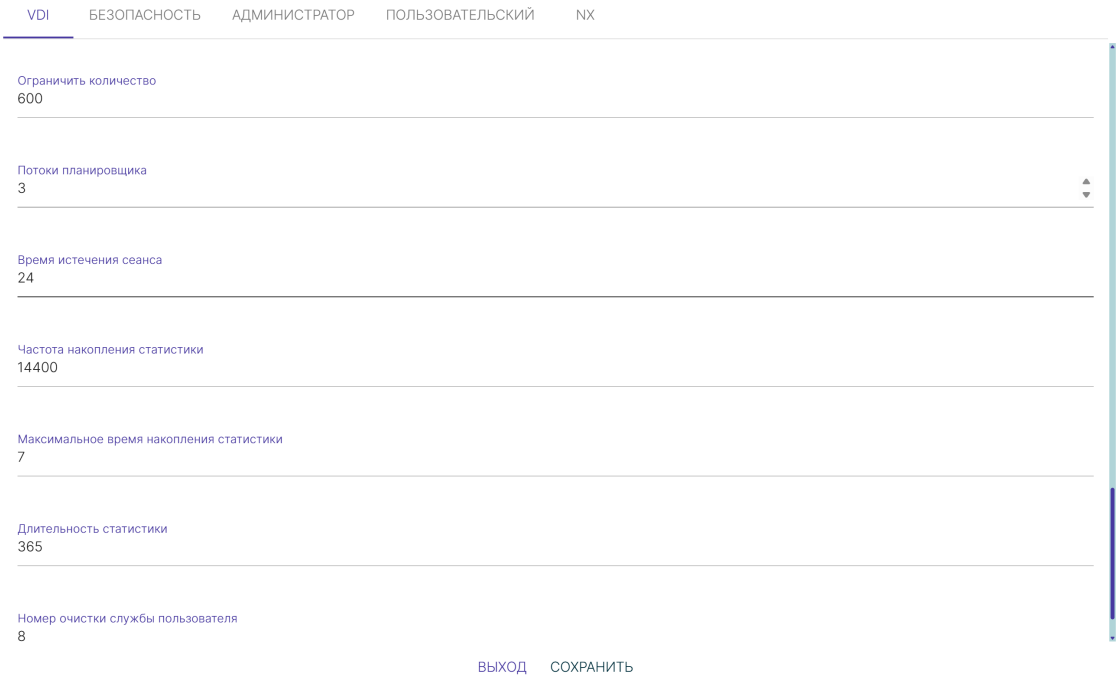


Рисунок 251

6.1.2 Вкладка «Безопасность»

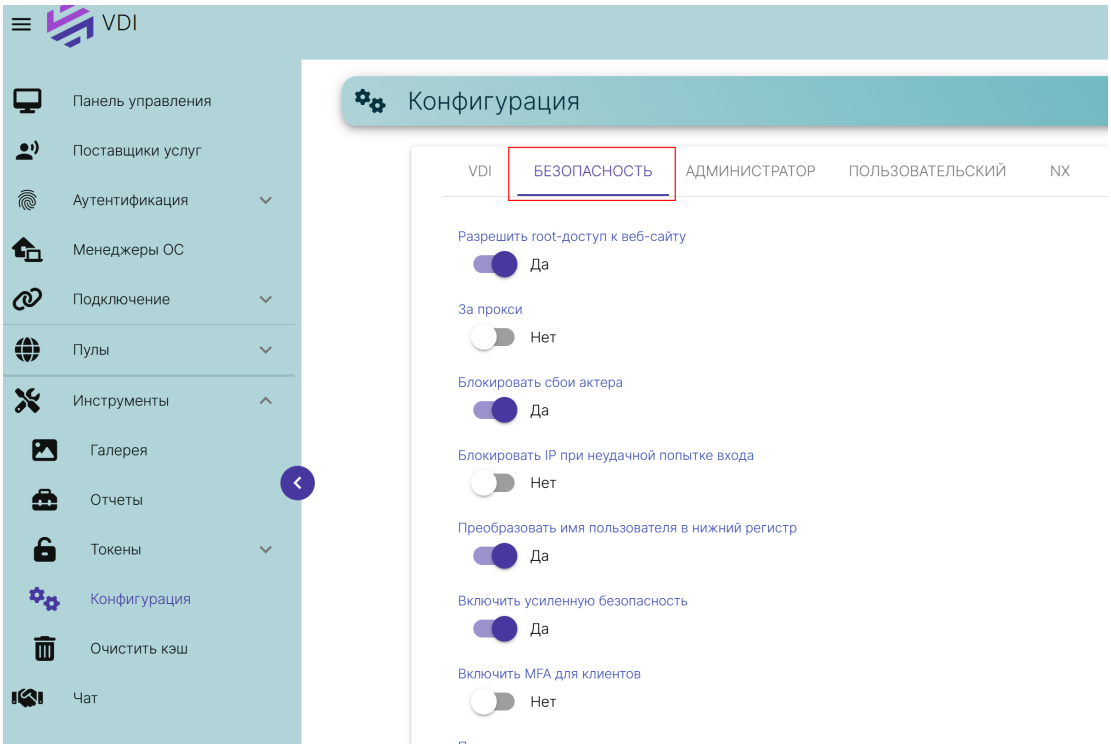


Рисунок 252

Описаны параметры, связанные с безопасностью системы VDI. Настраиваются следующие параметры:

1. **Разрешить root-доступ к веб-сайту.** Флаг, разрешающий аутентификацию в веб-интерфейсе с использованием учетной записи с максимальными привилегиями (root/admin). **Значение по умолчанию: Да**
2. **Работа за прокси-сервером.** Указывает системе, что она находится за обратным прокси-сервером. Это необходимо для корректного определения реальных IP-адресов клиентов. **Значение по умолчанию: Нет**
3. **Блокировать сбои актора.** Активирует блокировку учетной записи или процесса при обнаружении множественных аномальных или ошибочных действий. **Значение по умолчанию: Нет**
4. **Блокировать IP при неудачной попытке входа.** Включает функцию автоматической блокировки IP-адреса, с которого поступило несколько неудачных попыток входа в систему подряд. **Значение по умолчанию: Нет.**

5. **Преобразовать имена пользователей в нижний регистр.** Все вводимые логины автоматически преобразуются в нижний регистр для устранения неоднозначности. **Значение по умолчанию: Да.**
6. **Включить усиленную безопасность.** Активирует дополнительные уровни защиты, такие как строгая политика паролей, проверка заголовков HTTP. **Значение по умолчанию: Да.**
7. **Включить MFA для клиентов.** Требует от всех пользователей использовать многофакторную аутентификацию для входа в систему. **Значение по умолчанию: Нет.**
8. **Применить режим нулевого доверия.** Включает политику безопасности, при которой каждый запрос к системе проверяется, независимо от его источника внутри или снаружи сети. **Значение по умолчанию: Нет.**

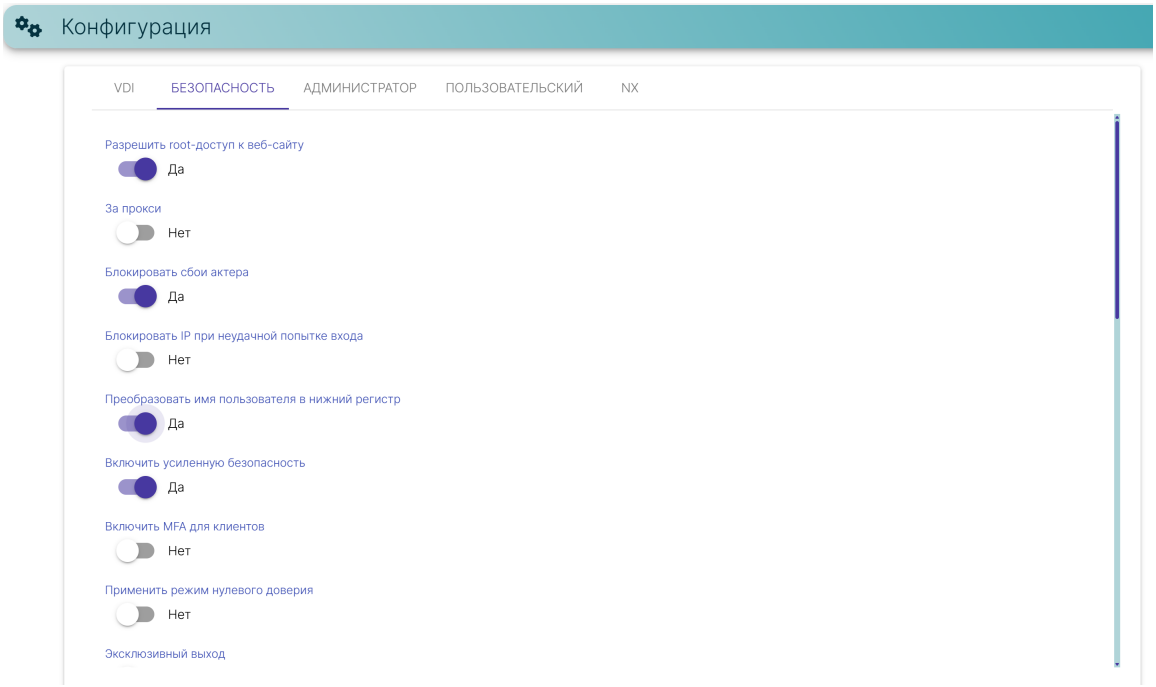


Рисунок 253

9. **Эксклюзивный выход.**При включении выход из системы на одном устройстве завершает все остальные активные сеансы этого пользователя. **Значение по умолчанию: Нет**

10. **Учитывать IP-адрес клиента для уведомлений.** Отправляет уведомление о подключении клиента с новым IP-адресом. **Значение по умолчанию: Нет.**
11. **Время блокировки входа.** Продолжительность (в секундах), на которую блокируется возможность входа после превышения лимита попыток. **Значение по умолчанию: 300**
12. **Мастер-ключ.** Криптографический ключ, используемый системой для защиты критически важных данных.
13. **Максимальная продолжительность журналов аудита.** Период хранения записей журналов безопасности (в днях). **Значение по умолчанию: 365**
14. **Максимальное количество попыток входа.** Количество разрешенных последовательных неудачных попыток аутентификации перед срабатыванием блокировки. **Значение по умолчанию: 5.**
15. **Ограничение времени сеанса RDS.** Максимальная продолжительность (в секундах) сеанса служб удаленных рабочих столов перед его принудительным завершением. **Значение по умолчанию: 86400.**

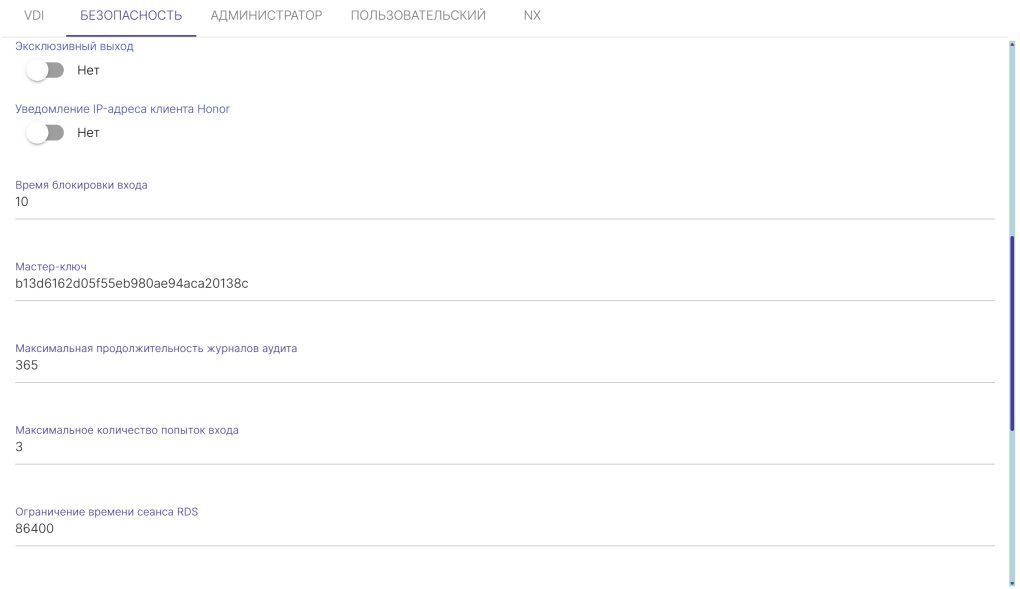


Рисунок 254

16. **Пароль root.** Пароль для учетной записи суперпользователя. Значение задаётся вручную.

17. **Время ожидания сеанса для администратора.** Время неактивности (в минутах), после которого сеанс администратора автоматически разрывается. **Значение по умолчанию: 14400.**
18. **Время ожидания сеанса для пользователя.** Время неактивности (в минутах), после которого сеанс обычного пользователя автоматически разрывается. **Значение по умолчанию: 14400**
19. **Суперпользователь.** Имя учетной записи, обладающей неограниченными правами в системе. **Значение по умолчанию: admin.**
20. **Доверенные хосты.** Список IP-адресов или сетей, с которых разрешен доступ к системе. Знак * разрешает подключения с любых адресов.

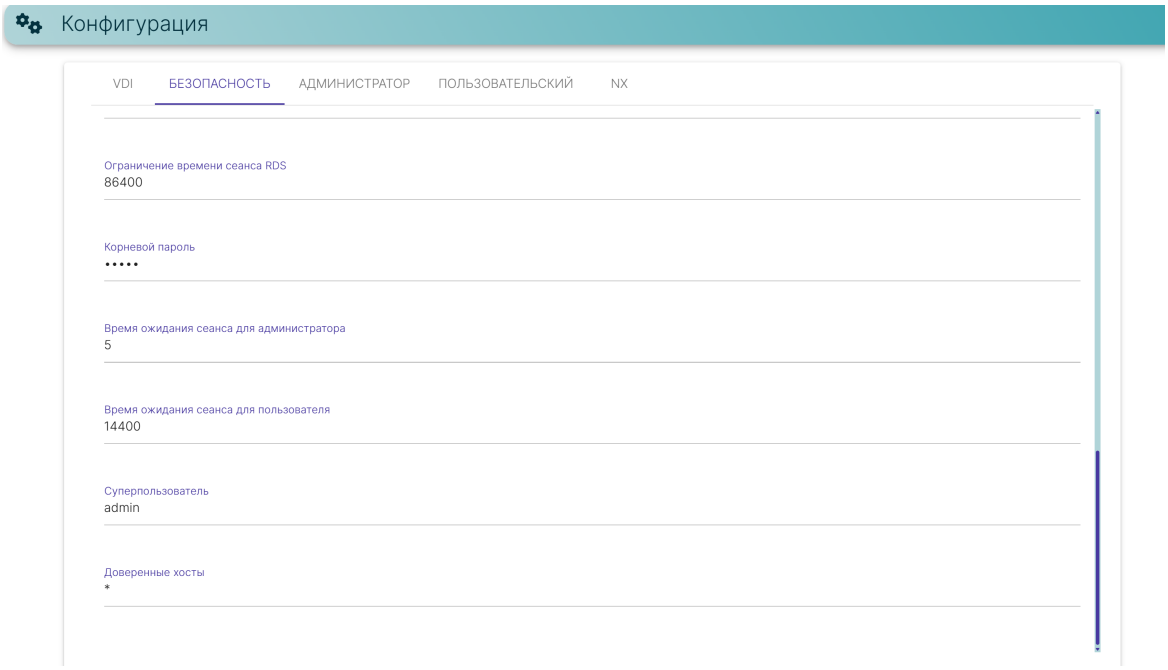


Рисунок 255

6.1.3 Вкладка «Администратор»

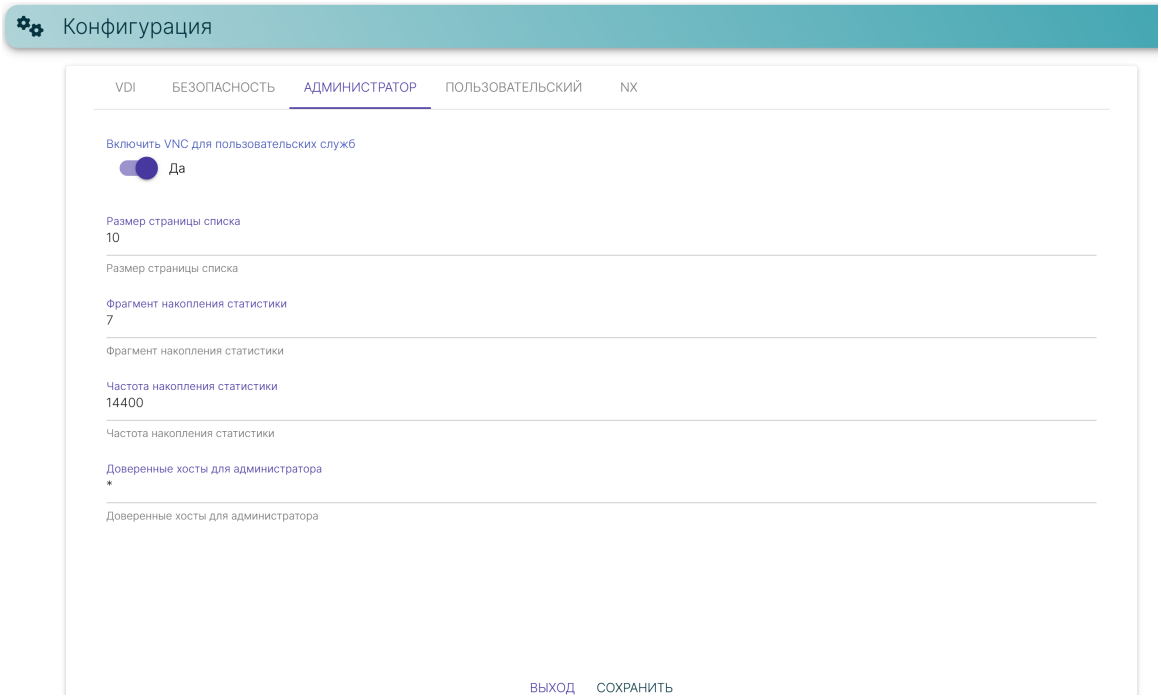


Рисунок 256

- **Включить VNC для пользовательских служб**. Активирует использование протокола VNC для подключения к виртуальным рабочим столам пользователей. Позволяет удаленно управлять сеансами. **По умолчанию включено**.
- **Размер страницы списка**. Определяет количество элементов, отображаемых на одной странице в таблицах и списках интерфейса администратора.
- **Фрагмент накопления статистики**. Задает временной интервал (в секундах или минутах) для сбора "сырых" данных перед их агрегацией. Это "окно", за которое система накапливает данные для последующего анализа.
- **Частота накопления статистики**. Определяет, как часто система выполняет финальную агрегацию и сохранение статистических отчетов на основе собранных "фрагментов".
- **Доверенные хосты для администратора**. Ограничивает IP-адреса или подсети, с которых разрешен доступ к административной панели управления. Повышает безопасность.

6.1.4 Вкладка «Пользовательский»

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

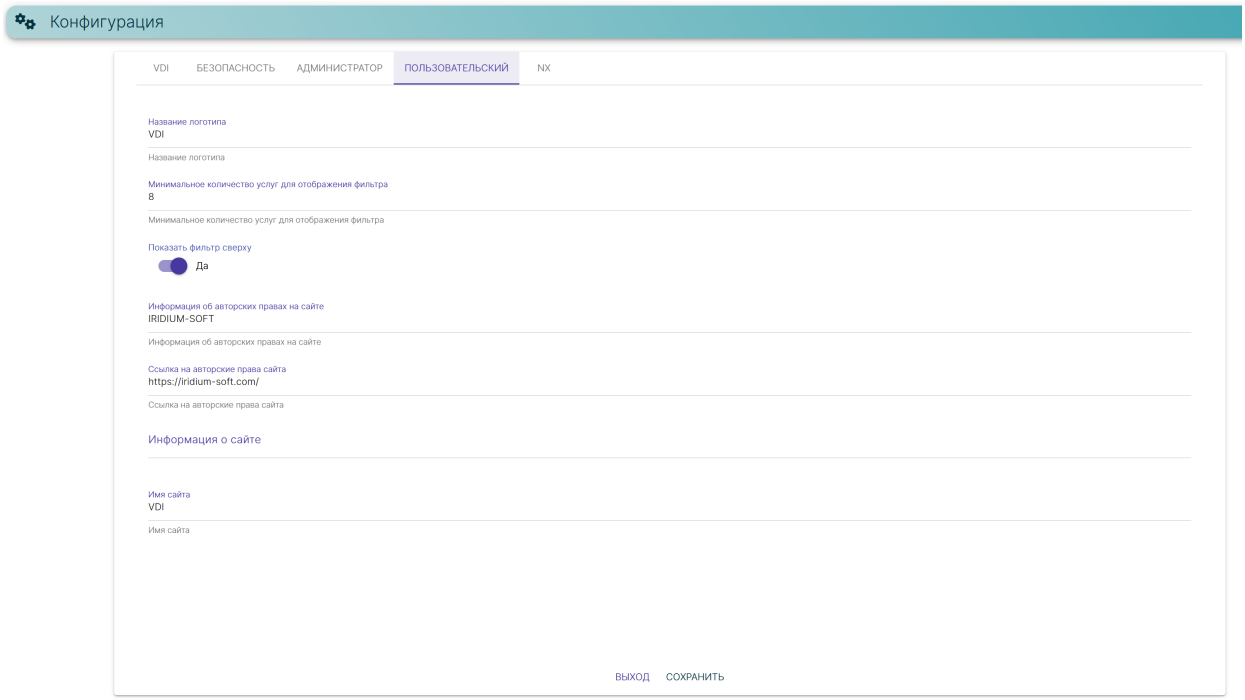


Рисунок 257

Название логотипа. Значение по умолчанию: VDI. Определяет текстовое значение, отображаемое в качестве логотипа системы на пользовательском интерфейсе. Может быть заменено на имя организации или проекта.

1. **Минимальное количество услуг для отображения фильтра.** Устанавливает минимальное количество элементов (услуг), при превышении которого отображается панель фильтрации. Используется для оптимизации отображения при большом числе объектов. **Значение по умолчанию: 8.**
2. **Показать фильтр сверху.** Если параметр включён, панель фильтров отображается в верхней части интерфейса вместо стандартного положения. **Значение по умолчанию: выключено.**
3. **Информация об авторских правах на сайте.** Строка с информацией о правообладателе, отображаемая в нижней части сайта. Может содержать наименование юридического лица или проекта.

4. **Ссылка на авторские права сайта.** Гиперссылка на внешний ресурс с описанием авторских прав или пользовательского соглашения.
5. **Информация о сайте.** Пояснительный текст или описание назначения сайта. Может быть отображено на стартовой или информационной странице системы.
6. **Имя сайта. Значение по умолчанию: VDI.** Определяет название сайта, отображаемое в заголовке окна браузера и других элементах интерфейса.

6.1 NX

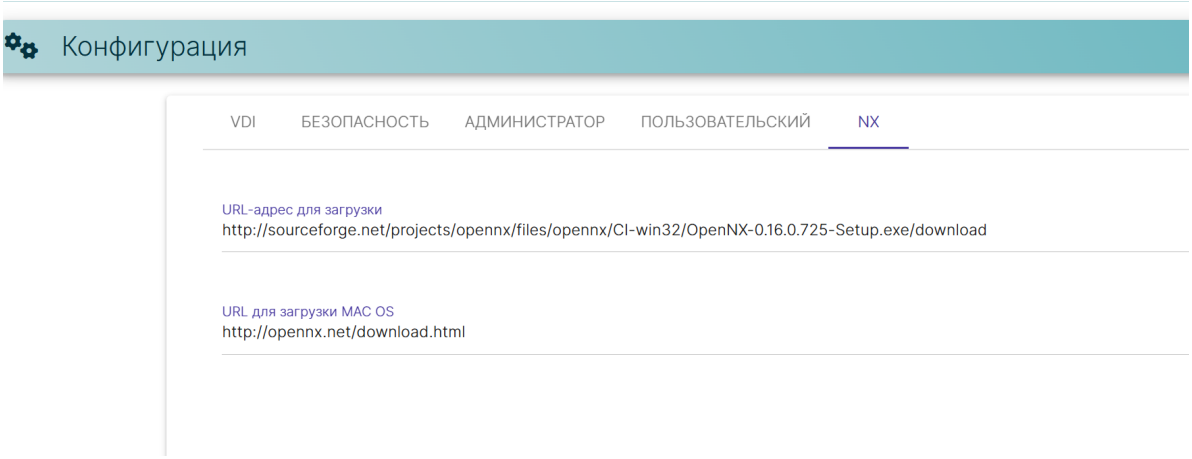


Рисунок 258

Описаны параметры, относящиеся к **Транспорту** Транспорту NX:

DownloadUrl: веб-адрес для загрузки программного обеспечения NX.

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

6.2 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:

1. Перейти в раздел **Инструменты** и выбрать **Галерея** (Рисунок 259):

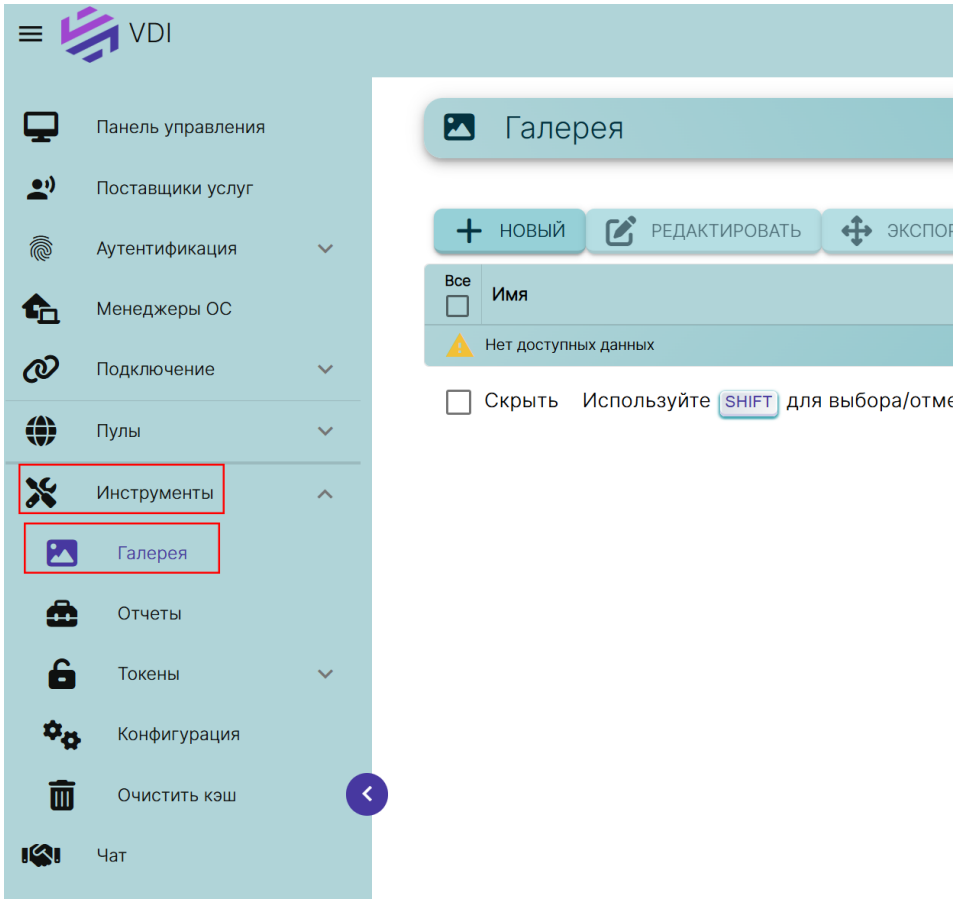


Рисунок 259

2. Нажать кнопку **Новый**, чтобы добавить новый образ в репозиторий.

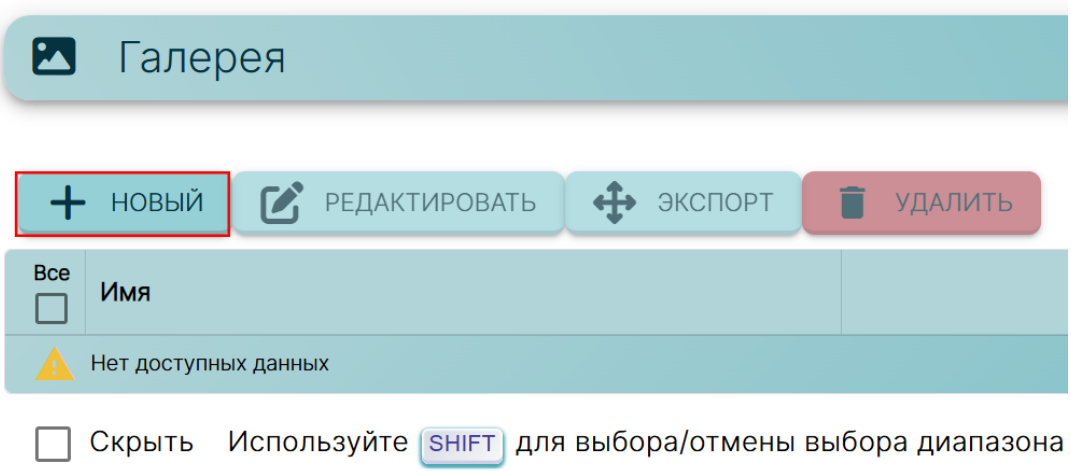


Рисунок 260

3. В открывшемся окне необходимо указать имя и с помощью кнопки **Выбрать изображение** найти образ, который нужно загрузить (Рисунок 261).

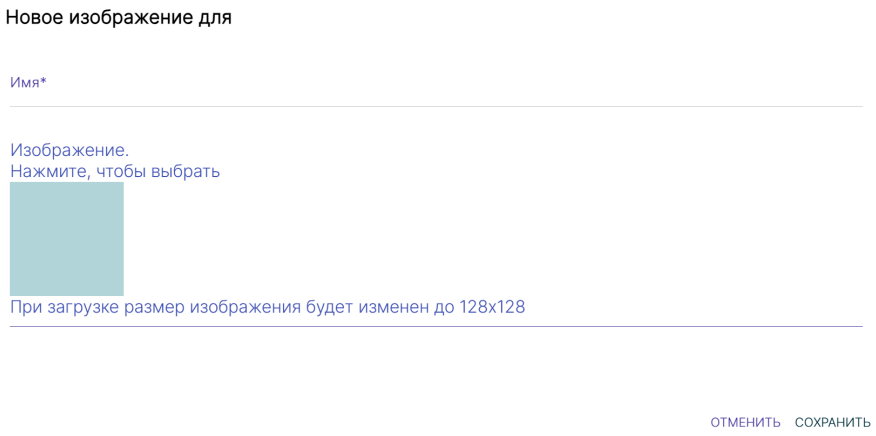


Рисунок 261

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

6.1 Отчеты

VDI позволяет автоматически генерировать отчеты по различным элементам платформы.

Чтобы получить доступ к отчетам:

1. Войти в раздел **Инструменты** и выбрать **Отчеты** (Рисунок 262).

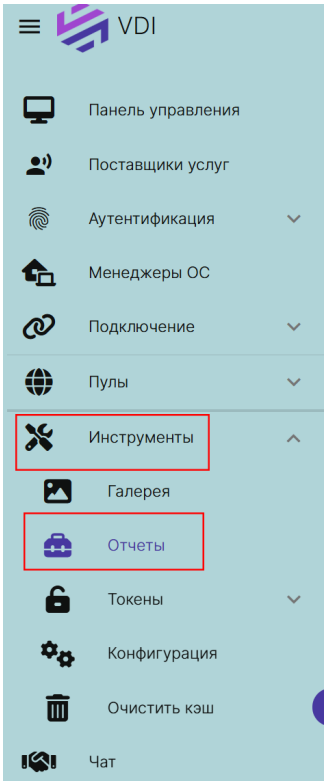


Рисунок 262

2. В VDI можно генерировать различные отчеты

– **Список пользователей**. Выбрать отчет из списка, нажать **Сгенерировать отчет.**

Рисунок 263

В открывшемся окне, в выпадающем списке выбрать аутентификатор, нажать кнопку **Сохранить**. (Рисунок 264).

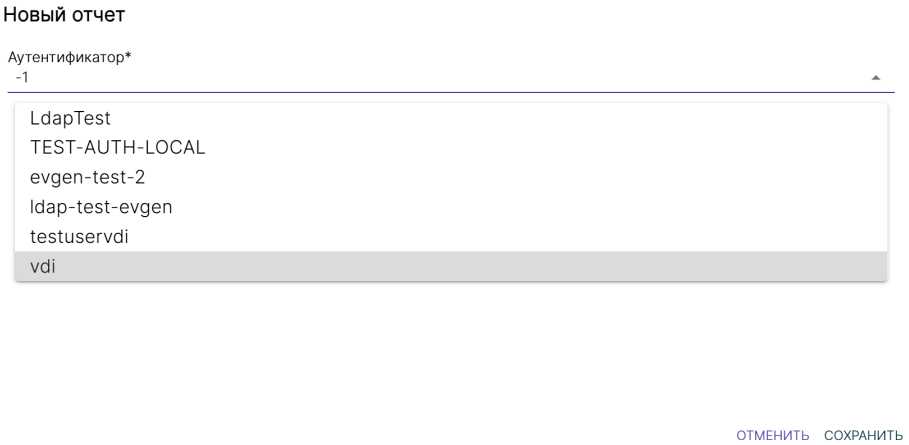


Рисунок 264

После создания будет список всех пользователей, принадлежащих этому аутентификатору.

– **Отчет о доступе пользователей по дате.** Выбрать отчет, нажать кнопку **Сгенерировать отчет.**

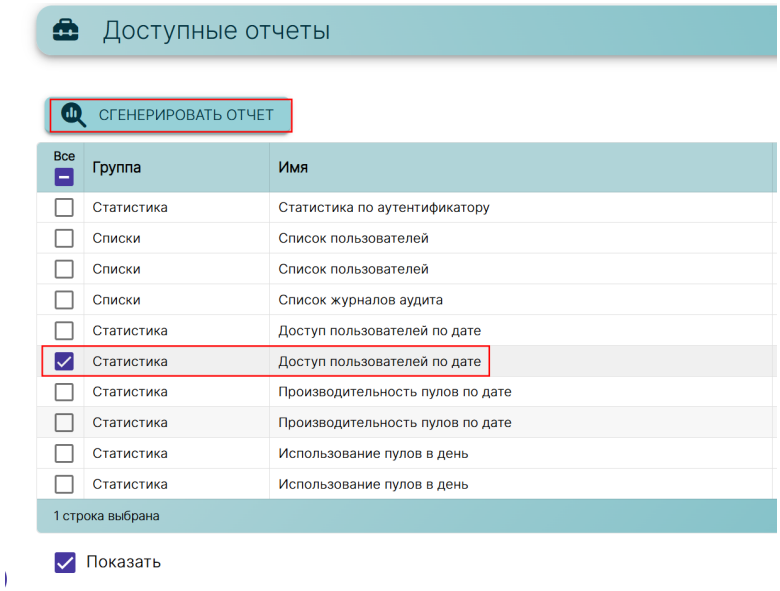


Рисунок 265

Создает отчет со всеми доступами пользователей к системе в указанном диапазоне дат. указать диапазон дат и количество интервалов.

Рисунок 266Рисунок 266

– **Производительность пулов по дате**. Выбрать отчет, нажать кнопку **Сгенерировать отчет.**

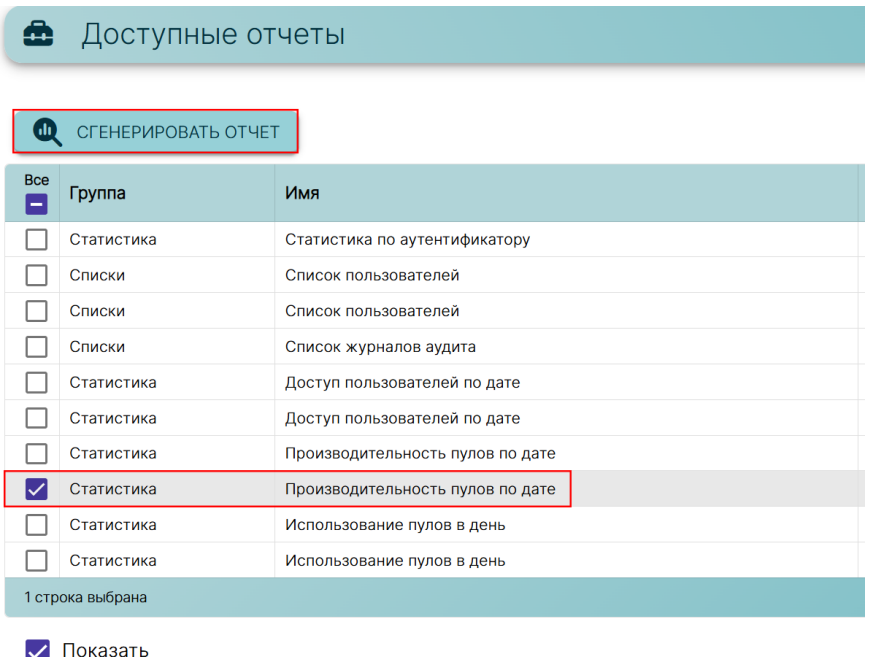


Рисунок 267

Указать пул, по которому нужно сформировать отчет, диапазон дат и количество интервалов (Рисунок 268), нажать кнопку **Сохранить.**

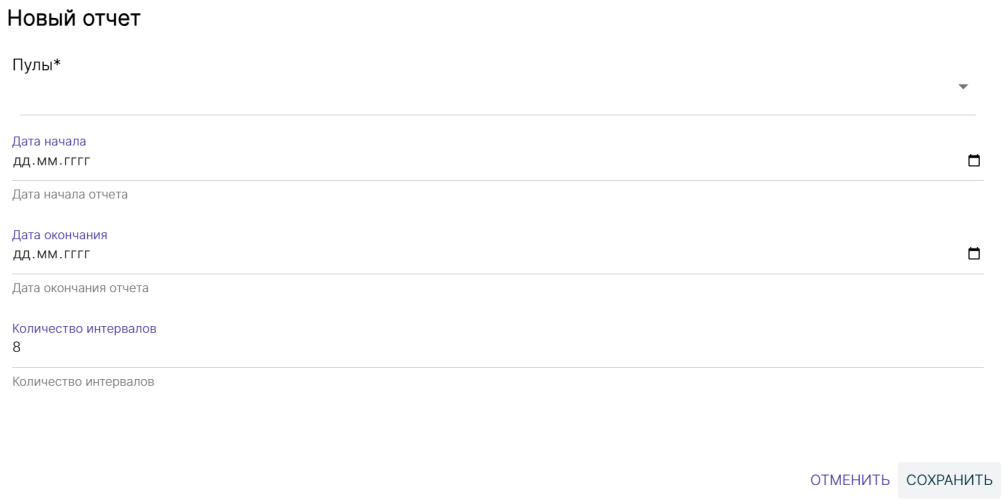


Рисунок 268

6.2 Завершение работы

Для завершения работы необходимо в правом верхнем углу системы нажать на имя пользователя и в меню выбрать пункт **Выйти**.

7 ПРОВЕРКА ПРОГРАММЫ

Проверка корректности функционирования VDI проводится на основании Технического задания на разработку и согласно Техническим условиям.

8 СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

В процессе выполнения программы могут появляться предупреждения и сообщения об ошибках.

ПЕРЕЧЕНЬ ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

Гостевая операционная система	операционная система, установленная в виртуальной машине
Виртуальная машина (ВМ)	виртуальная вычислительная система, которая состоит из виртуальных устройств обработки, хранения и передачи данных и которая дополнительно может содержать программное обеспечение и пользовательские данные. На ВМ, как и на реальные, можно ставить операционные системы, причем на одном вычислительном узле может функционировать несколько ВМ
Шаблон виртуальной машины	набор настроек, с которыми будут создаваться виртуальные машины
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
Инфраструктура виртуальных рабочих столов (ВРС)	форма виртуализации настольных систем, в которой все элементы рабочего стола пользователя размещены в центре обработки данных. Пользователь удаленно подключается к своему рабочему столу с какого-либо клиентского устройства; при этом ни рабочий стол пользователя, ни приложения, ни данные на его устройстве локально не хранятся
ПАК	программно-аппаратный комплекс
СГУ	система группового управления
VDI	Virtual Desktop Infrastructure

ПЕРЕЧЕНЬ ССЫЛОЧНЫХ ДОКУМЕНТОВ

1) ГОСТ 19.103-77 ЕСПД. Обозначение программ и программных документов

2) ГОСТ 19.104-78 ЕСПД. Основные надписи

3) ГОСТ 19.106-78 ЕСПД. Общие требования к программным документам, выполненным печатным способом

4) ГОСТ 19.604-78 ЕСПД. Правила внесения изменений в программные документы, выполненные печатным способом

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

	Номера листов (страниц)				*Всего листов (страниц) в докум.*	*№ документа*	*Входящий номер доп. Документа и дата*	*Подп.*	*Дата*
Изм.	*измененных*	*замененных*	*новых*	*аннулированных*					