

RU.KHPШ.00005-01 90 01

УТВЕРЖДЕН
RU. KHPШ.00005-01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС «ЗВЕЗДА-VDI»
RU.KHPШ.00005-01 90 01
Руководство администратора

Листов 192

2025

Инв. № подл.	Подп. и дата	Взам. Инв №	Инв. № дубл.	Подп. и дата

СОДЕРЖАНИЕ

Аннотация.....	5
1 Общие сведения об изделии	6
1.1 Назначение изделия.....	6
1.2 Функции изделия	6
1.3 Минимальный состав технических средств	8
1.4 Сведения о структуре программы.....	8
1.5 Архитектура платформы с VDI инфраструктурой	9
1.6 Компоненты VDI инфраструктуры	10
1.6.1 Сервер VDI.....	11
1.6.2 VDI Актор	11
1.6.3 Клиент VDI	12
1.7 Сведения о связях с другими программами	12
2 Установка программных компонентов VDI	14
2.1 Установка сервера VDI.....	14
2.2 Установка VDI Actor	14
2.2.1 Автономные виртуальные рабочие столы Windows	16
2.2.2 Создание виртуальных Linux машин	23
3 Управление VDI инфраструктурой.....	27
3.1 Поставщики услуг.....	29
3.1.1 Регистрация поставщика статических IP-машин	30
3.1.2 Поставщик ПК «Звезда».....	37
3.1.3 Поставщик «Иридиум»	44
3.1.4 Поставщик платформы RDS.....	50
3.2 Настройки аутентификации	60
3.2.1 Аутентификатор Active Directory.....	60
3.2.2 Базовый аутентификатор.....	63
3.2.3 IP Аутентификатор	69
3.2.4 Внутренняя база данных	71
3.2.5 Аутентификатор Kerberos	73
3.2.6 Аутентификатор Radius	74
3.2.7 Regex LDAP Аутентификатор	78

3.2.8 SAML-аутентификатор	83
3.2.9 Простой аутентификатор	89
3.2.10 Аутентификатор eDirectory	95
3.2.11 Настройка многофакторной аутентификации	97
3.2.12 Создание групп пользователей.....	116
3.2.13 Создание пользователя с ролью «Сотрудник»	118
3.2.14 Создание пользователя с ролью «Администратор»	120
3.2.15 Создание пользователя с ролью «Пользователь»	122
3.3 Настройка Менеджеров ОС.....	124
3.3.1 Создание менеджера ОС Linux.....	124
3.3.2 Linux со случайным паролем	126
3.3.3 RDS	129
3.3.4 Windows базовый менеджер ОС.....	130
3.3.5 Windows доменный менеджер	132
3.3.6 Windows со случайным паролем.....	137
3.4 Транспорт	139
3.4.1 Протокол RDP	140
3.4.1 RDS для виртуальных приложений (RDS for VApps).....	144
3.4.2 SPICE (прямой)	144
3.4.3 Добавление протокола СПЕКТР	147
3.4.4 X2Go (прямой)	149
3.4.1 Установка ограничений на авторизацию с устройства доступа пользователя.....	152
3.5 Сервис-пулы	154
3.5.1 Создание пула виртуальных машин Linux	154
3.5.2 Создание пула виртуальных машин Windows	155
3.5.3 Создание сессионного гостевого пула рабочих столов	156
3.5.1 Создание статического (персонализированного) пула рабочих столов	158
3.5.2 Доступ к календарям и запланированным задачам.....	160
3.5.3 Календари.....	160
3.5.4 Настройка разрешений.....	168
4 Параметры конфигурации VDI.....	172
4.1 Раздел «Конфигурация»	172
4.1.1 Вкладка «VDI»	172

4.1.2	Вкладка «Безопасность»	179
4.1.3	Вкладка «Администратор»	183
4.1.4	Вкладка «Пользовательский»	184
4.1	NX.....	186
4.2	Галерея	186
4.1	Отчеты.....	188

АННОТАЦИЯ

Программный комплекс «ЗВЕЗДА-VDI» RU.УГСФ.00005-01 90 01 (далее – «ЗВЕЗДА-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.

1 ОБЩИЕ СВЕДЕНИЯ ОБ ИЗДЕЛИИ

1.1 Назначение изделия

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

1.2 Функции изделия

VDI-ЗВЕЗДА 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 «горячего» подключения клавиатуры и мыши (для тонких клиентов)
- 34) 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 ВРМ
- 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.

1.4 Сведения о структуре программы

Общая схема функционирования VDI представлена на рисунке 1.

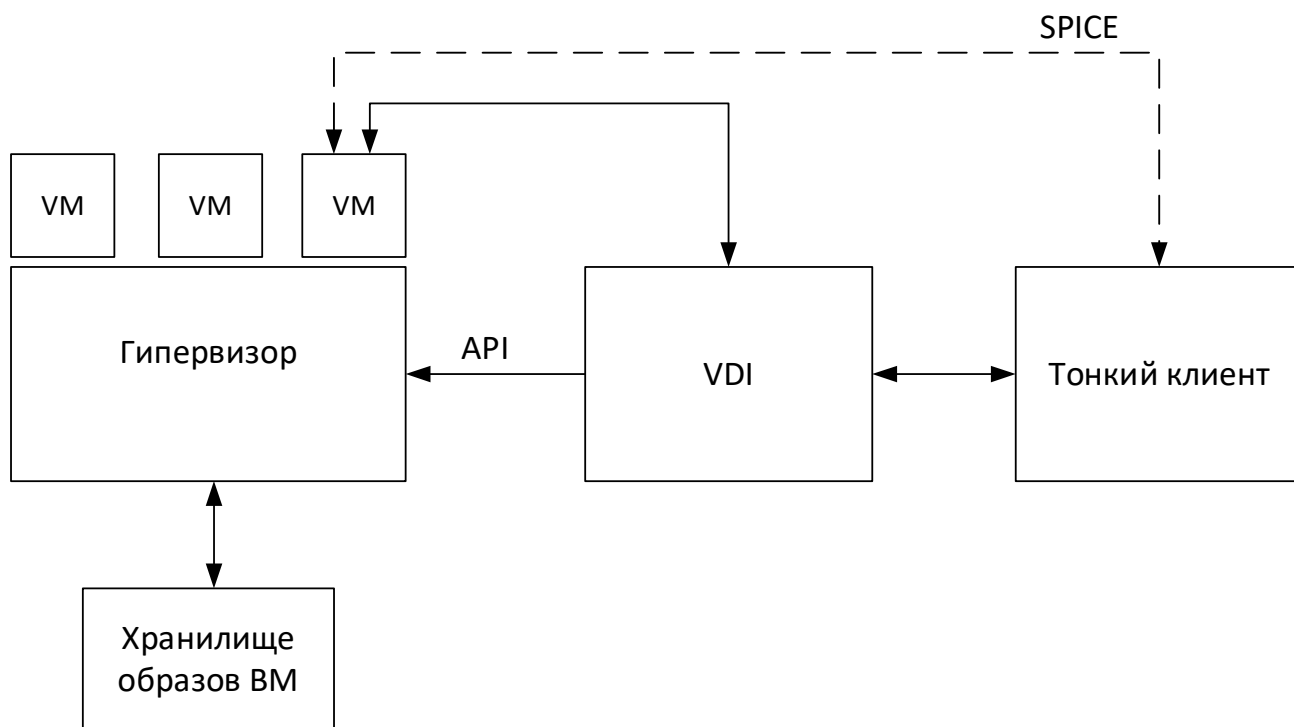


Рисунок 1 – Структура VDI инфраструктуры

1.5 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», ПК «Звезда», VMware vSphere, KVM (oVirt, RHEV, Proxmox, OpenStack).
- **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.

1.6 Компоненты VDI инфраструктуры

VDI состоит из трех элементов, взаимодействующих друг с другом.

- VDI брокер: устанавливается как Docker-контейнер.
- VDI актер: 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.

1.6.1 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 «Звезда» входит защищенная платформа виртуализации – средство виртуализации «Звезда» RU.КНПШ.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.

1.6.2 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.

1.6.3 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.

1.7 Сведения о связях с другими программами

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

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

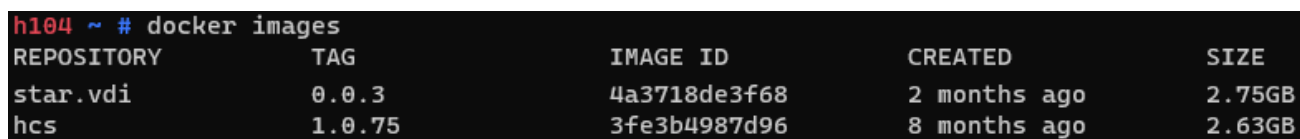
Таблица 1 – Сетевые соединения

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 ПРОГРАММНЫХ КОМПОНЕНТОВ VDI

2.1 Установка сервера VDI

1. В консоли платформы виртуализации перейти в директорию, где находится образ «star.vdi».
2. Выполнить команду `apply-ima <директория, в которой находится образ VDI>`.
3. Загрузить образ: `docker load < star.vdi.0.0.3.tar.bz2`
4. Посмотреть версию контейнера: `docker images` (пример: `star.vdi:0.0.3`)



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

5. Запустить контейнер:

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

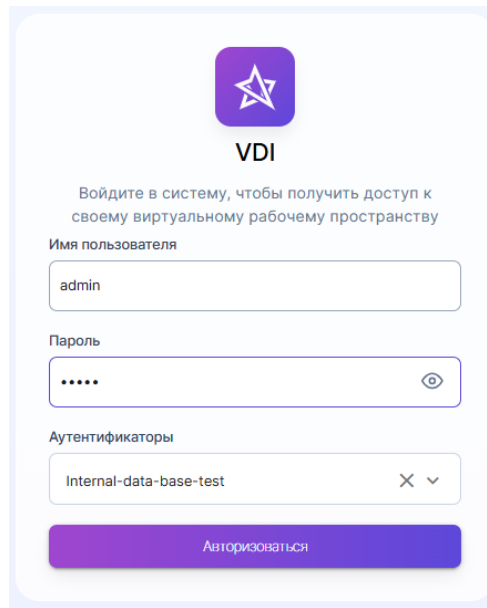
2.2 Установка VDI Actor

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 актер 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).



The image shows a login interface for a VDI system. At the top is a purple square icon with a white star. Below it, the text "VDI" is centered. A message in Russian asks the user to log in to access their virtual workspace. There are three input fields: "Имя пользователя" (Username) with the value "admin", "Пароль" (Password) with masked characters "....." and an eye icon, and "Аутентификаторы" (Authenticators) with the value "Internal-data-base-test" and a dropdown arrow. A large purple button at the bottom is labeled "Авторизоваться" (Log in).

Рисунок 3

- Нажать на страницу **Загрузки**.

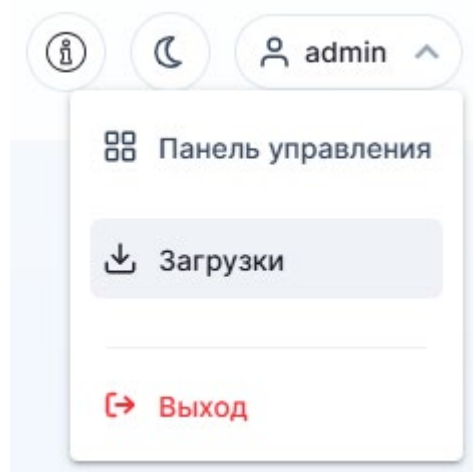


Рисунок 4

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

- Windows;
- Linux;
- Статические IP-машины.

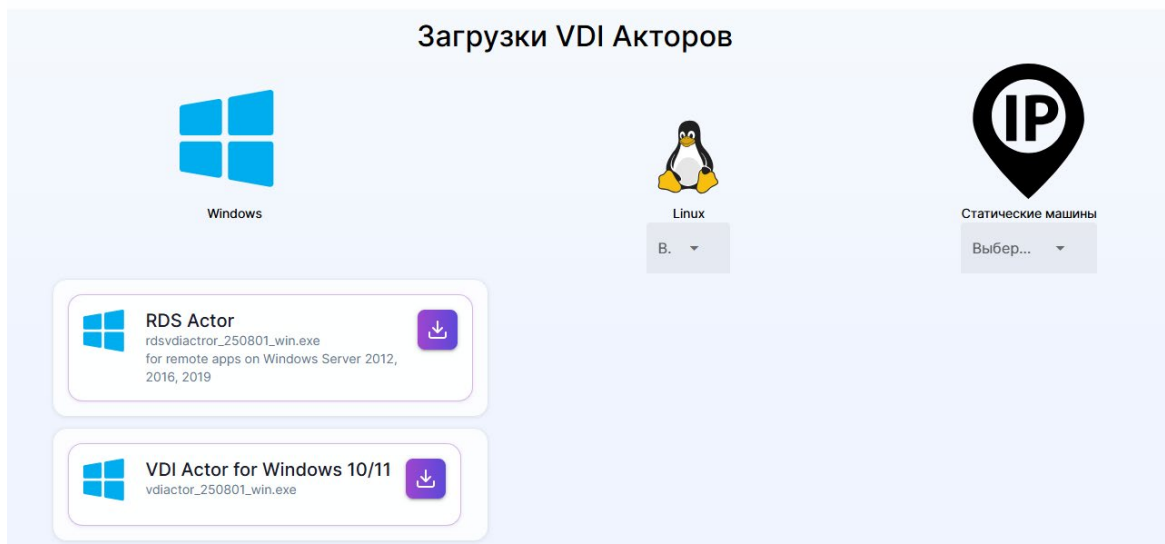


Рисунок 5

2.2.1 Автономные виртуальные рабочие столы Windows

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

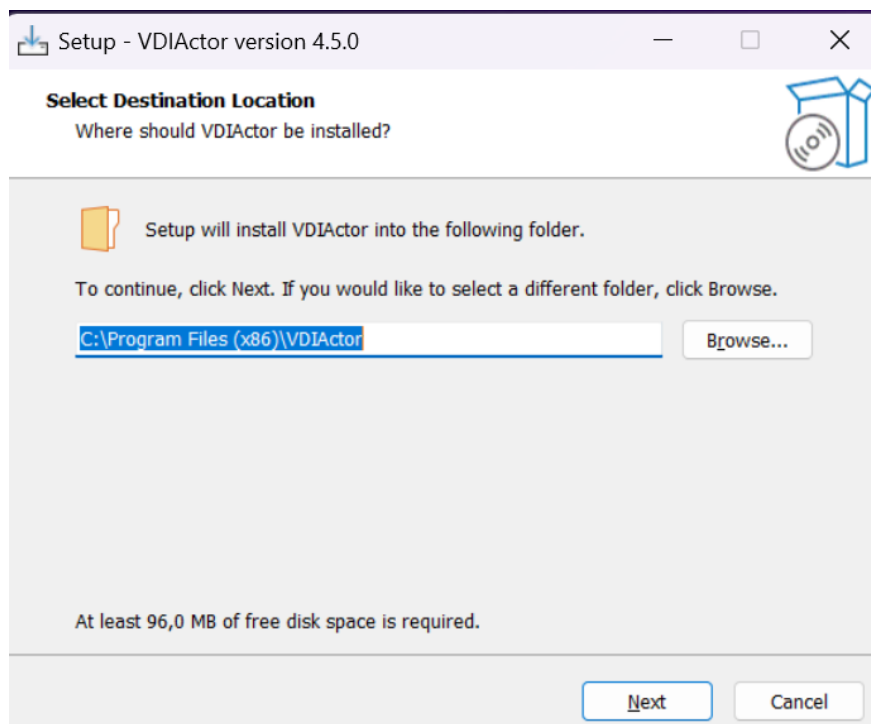


Рисунок 6

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

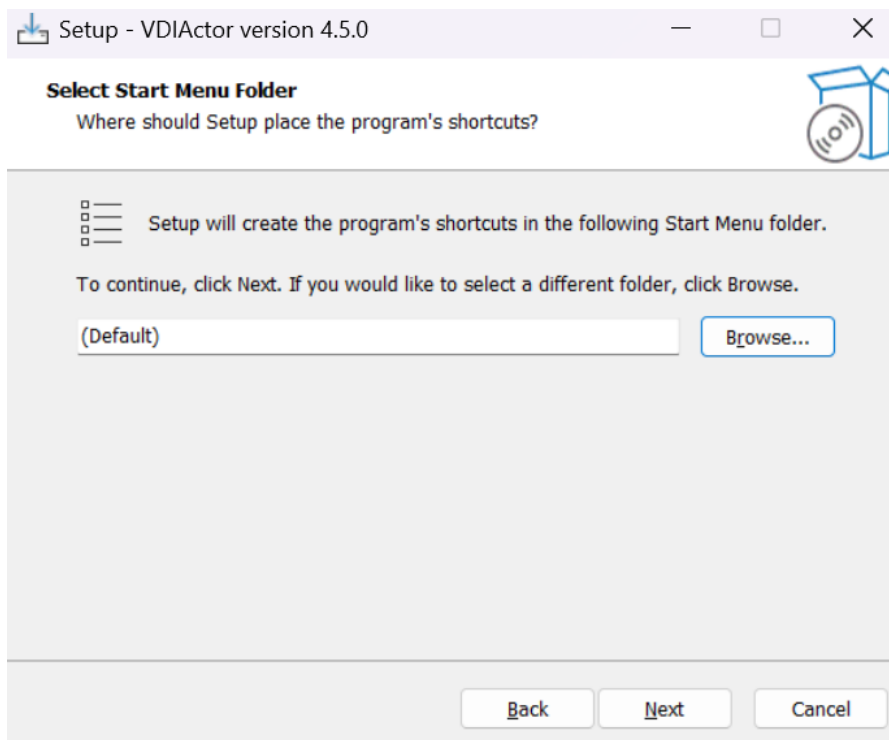


Рисунок 7

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

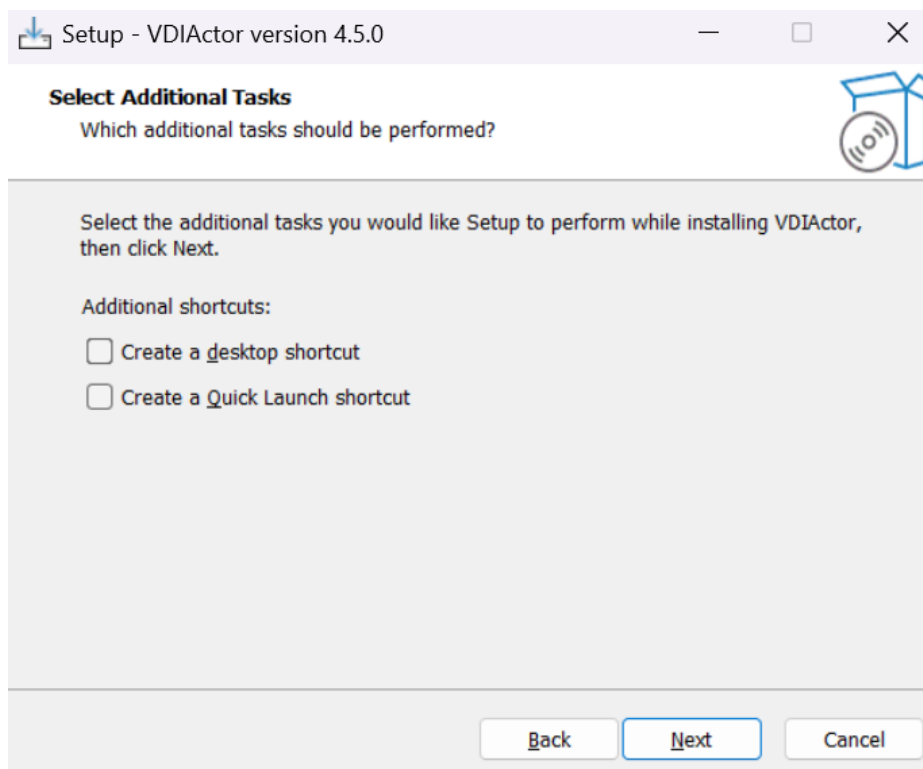


Рисунок 8

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

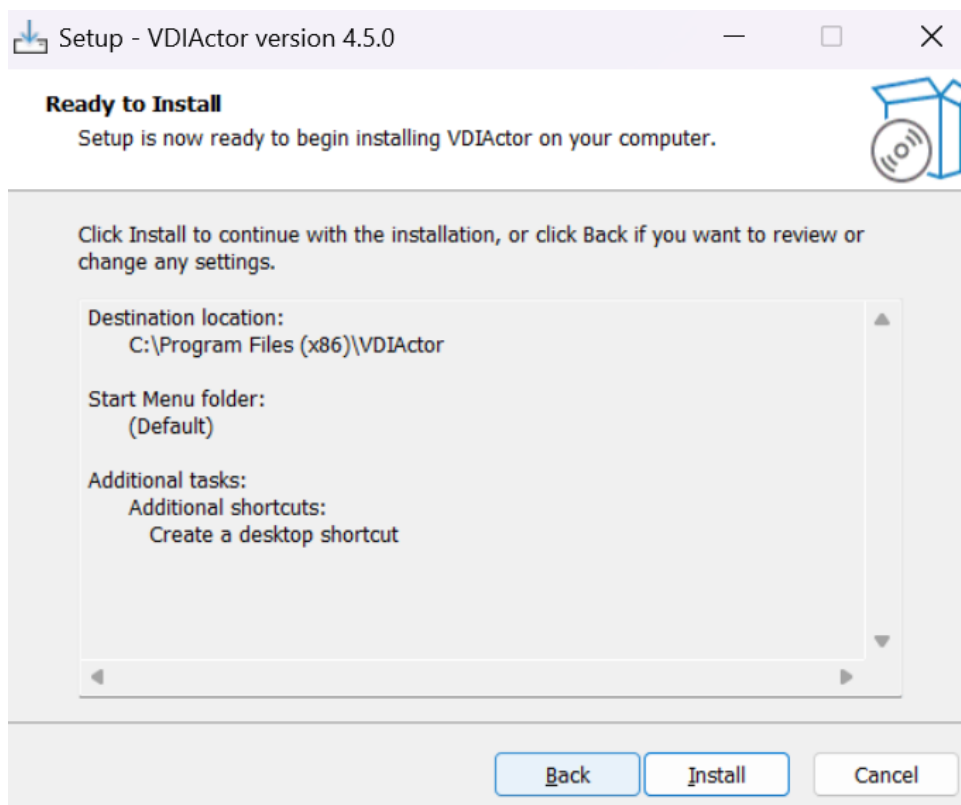


Рисунок 9

5. Установка завершена (Рисунок 10).

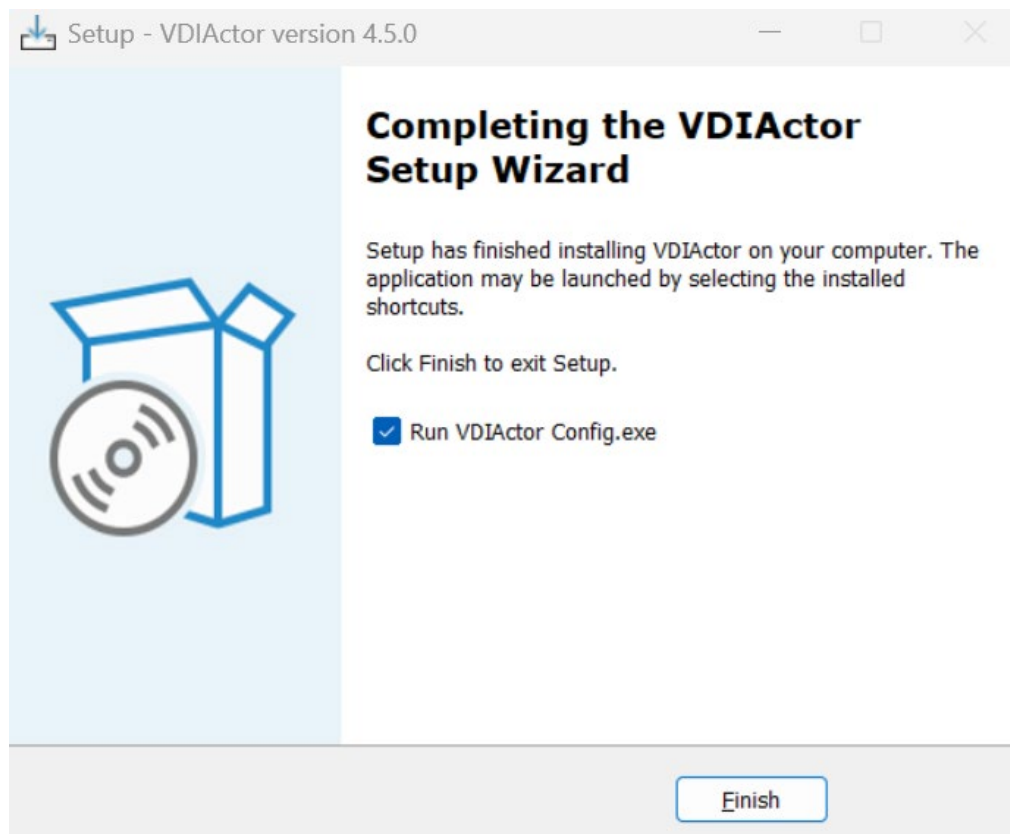


Рисунок 10

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.

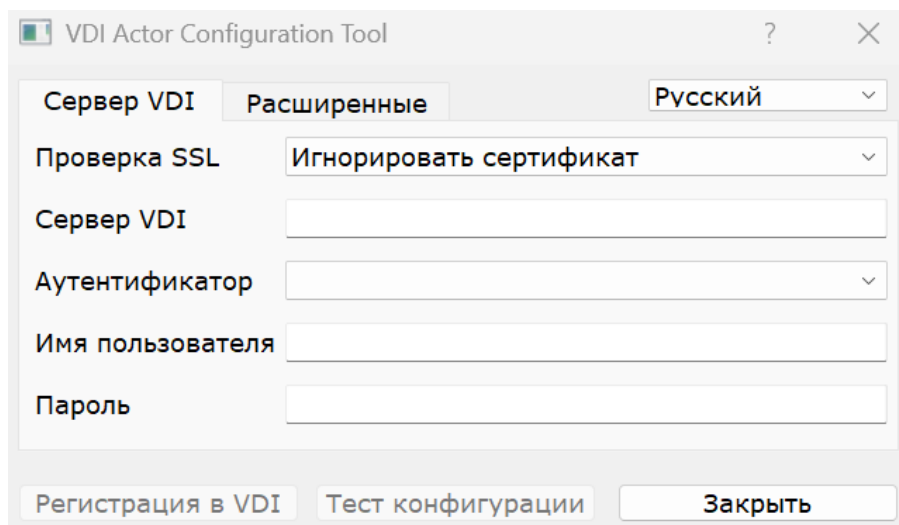


Рисунок 11

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

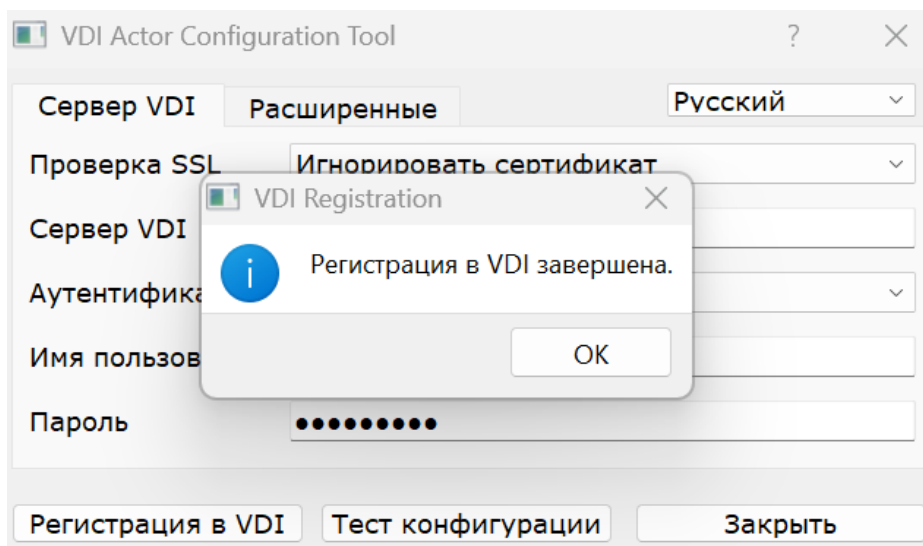


Рисунок 12

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

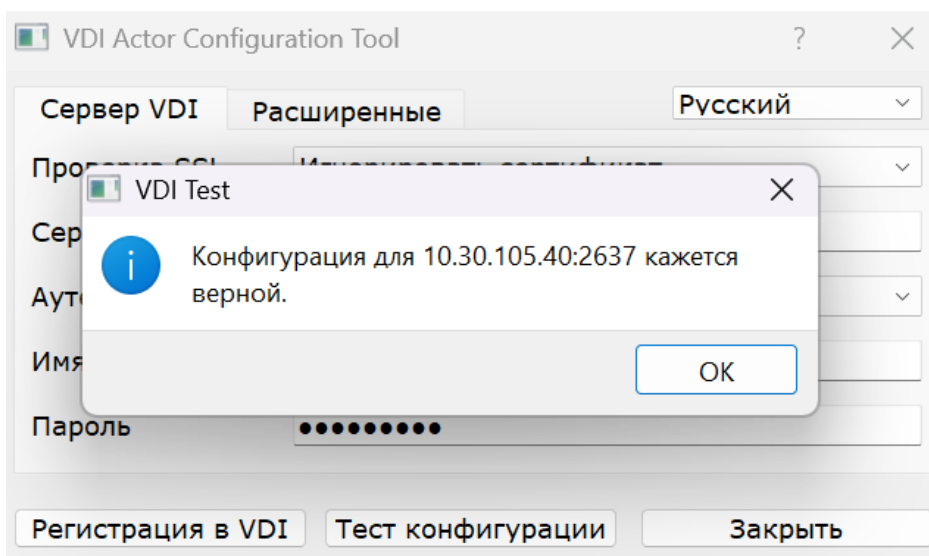


Рисунок 13

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, rsoip...), 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).

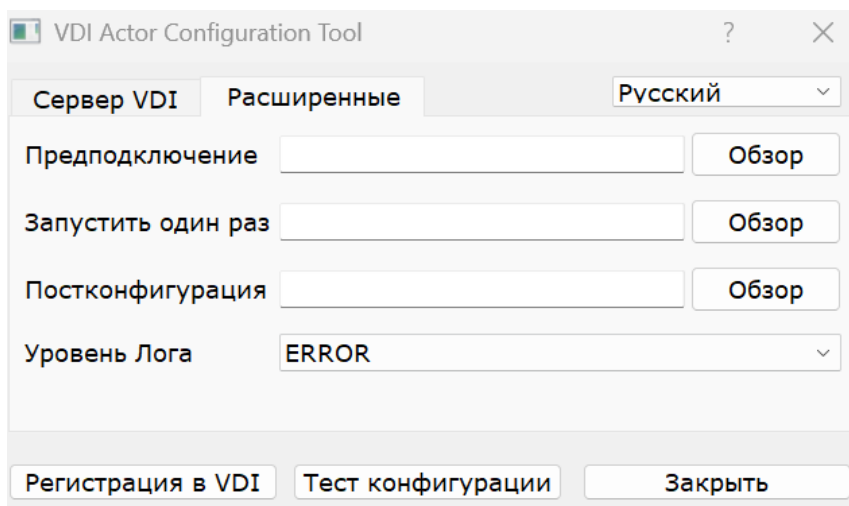


Рисунок 14

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 RCoIP и т.д.).

2.2.2 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.

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.

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

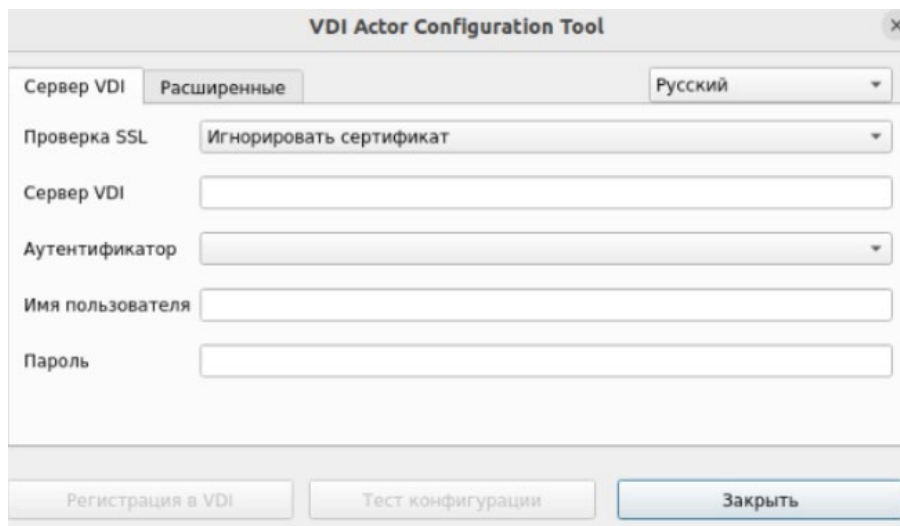


Рисунок 15

- 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).

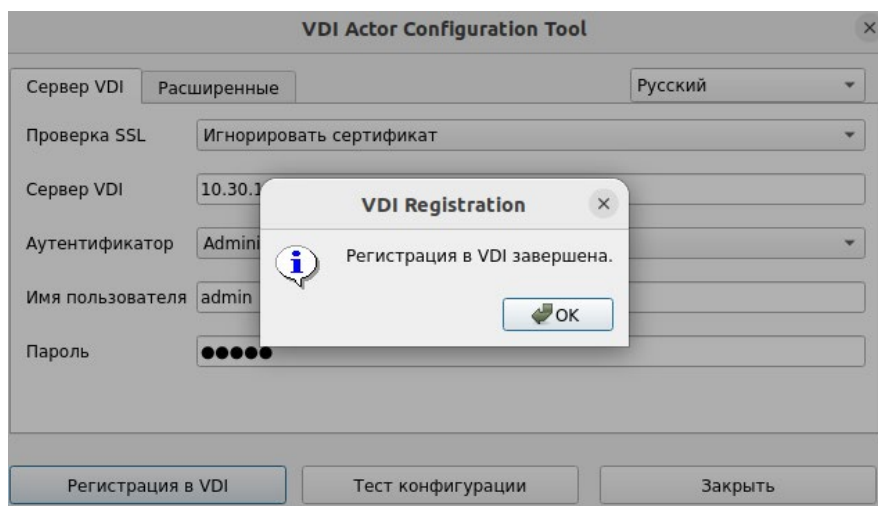


Рисунок 16

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

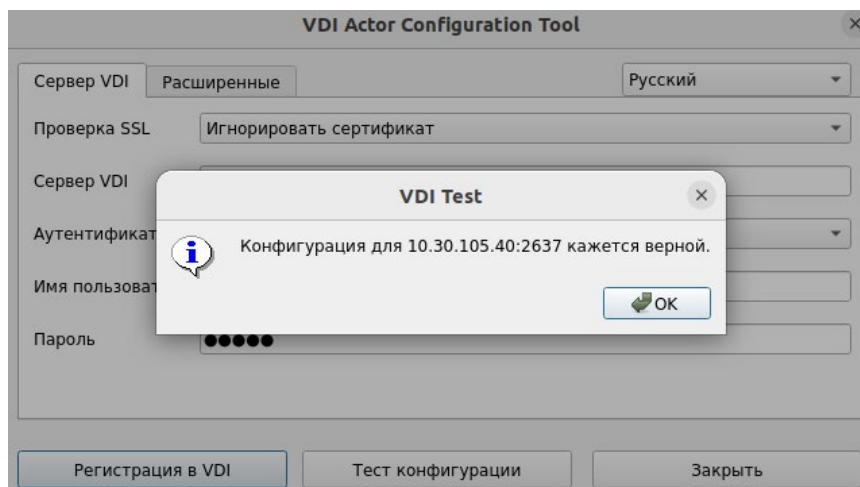


Рисунок 17

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, rsoip...), 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/`

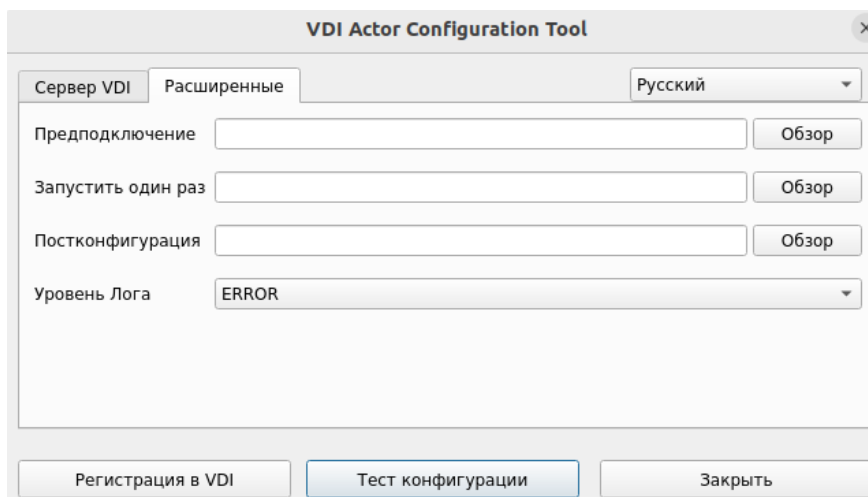


Рисунок 18

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.).

3 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 19) (например, <https://10.10.10.10:3030>).

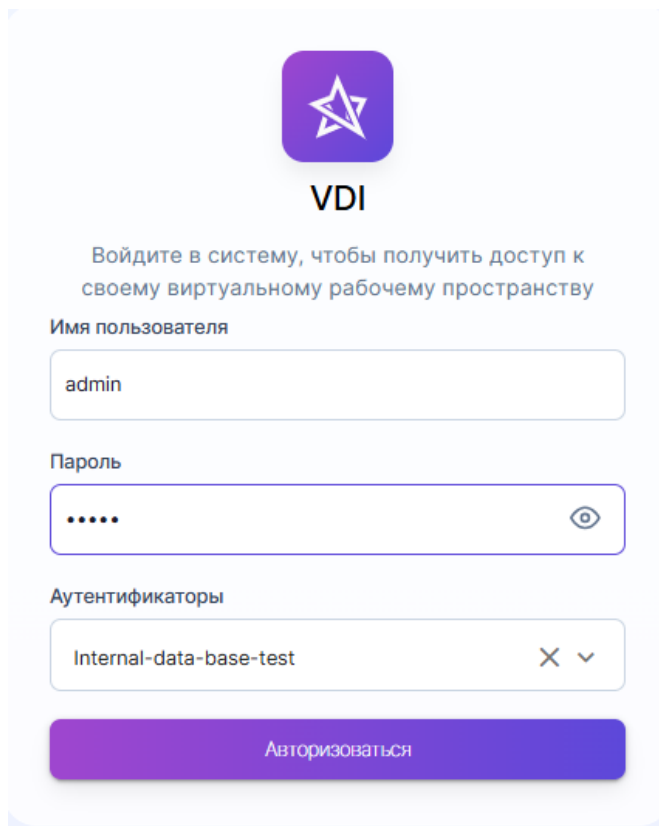


Рисунок 19

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 20).

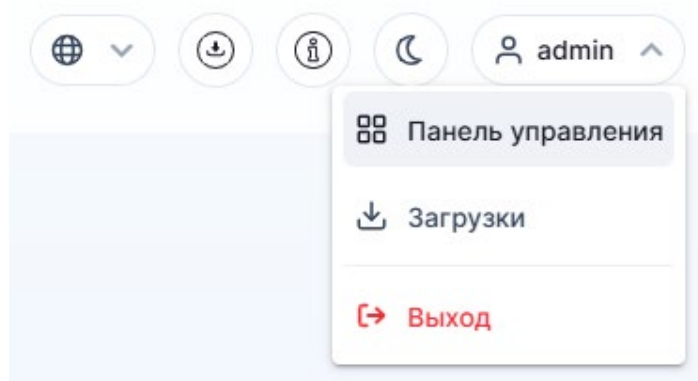


Рисунок 20

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 21) 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 3.2;
- *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 3.4.1).

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

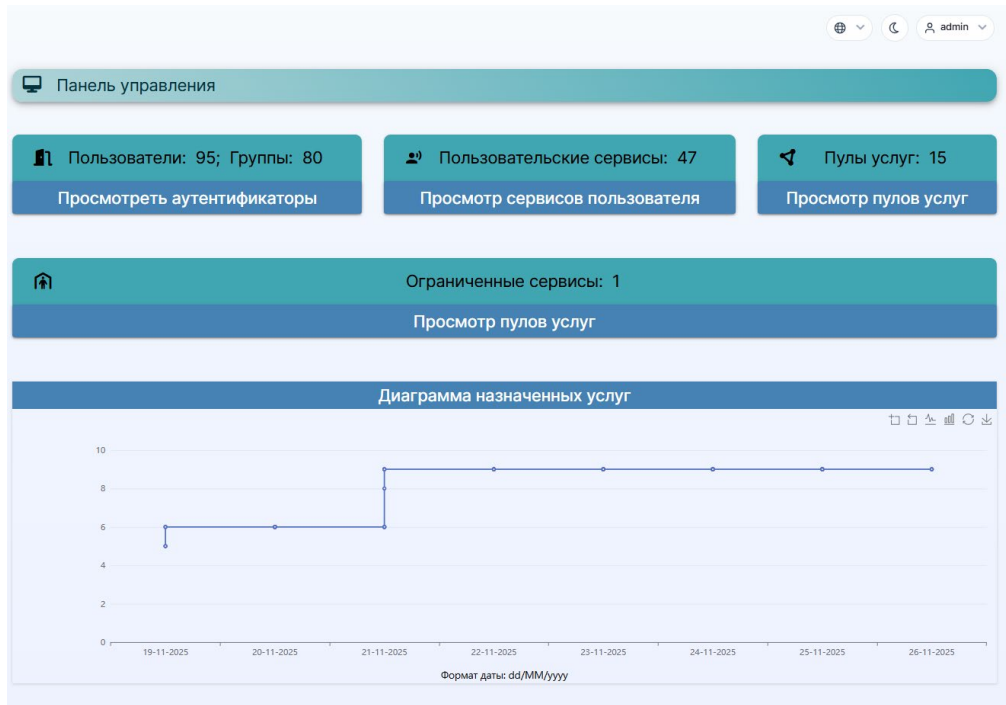


Рисунок 21

3.1 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 Звезда;
- Поставщик платформы RDS.

3.1.1 Регистрация поставщика статических IP-машин

Примечание: для использования поставщика статических IP-машин 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 22).
2. Откроется окно добавления поставщика.

The screenshot shows a web interface for adding a new provider. At the top, there are two tabs: 'Новый поставщик' (New provider) and 'Поставщик статически...' (Static IP provider...). Below the tabs are two sub-tabs: 'ОСНОВНОЙ' (Basic) and 'РАСШИРЕННЫЙ' (Advanced). The 'ОСНОВНОЙ' tab is active. It contains several input fields: 'Тэги' (Tags) with the value 'tags', 'Имя*' (Name*) which is required, 'Имя этого элемента' (Name of this element), 'Комментарии' (Comments), and 'Комментарии для этого элемента' (Comments for this element). At the bottom, there are three buttons: 'ТЕСТ' (Test), 'ОТМЕНИТЬ' (Cancel), and 'СОХРАНИТЬ' (Save).

Рисунок 22

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 23).

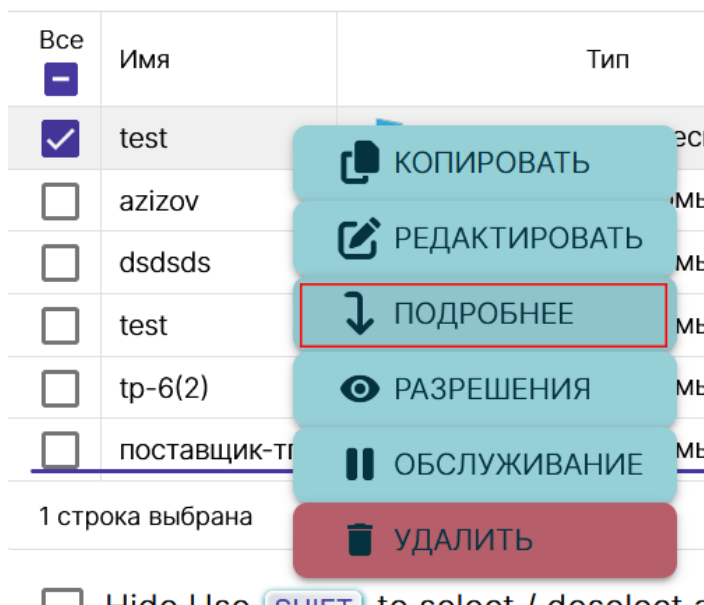


Рисунок 23

3.1.1.1 *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**.

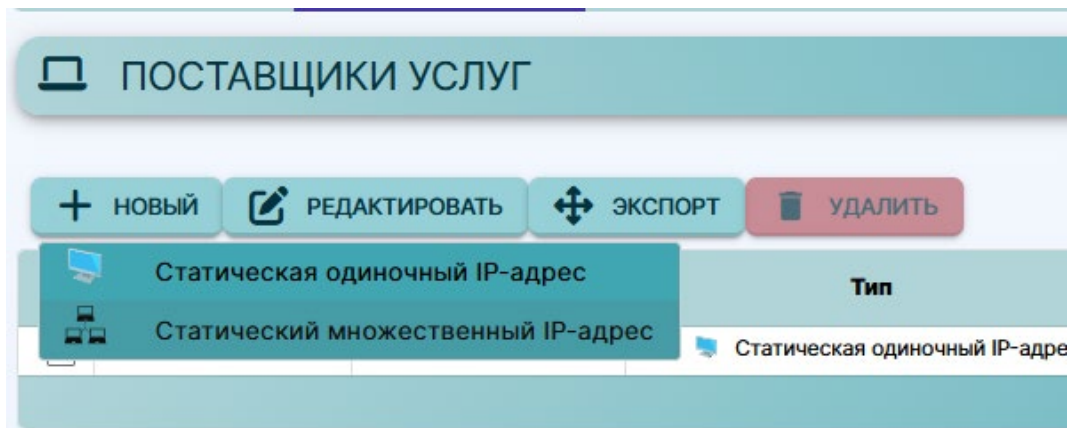


Рисунок 24

5. Откроется окно создания службы (Рисунок 25).

Новый сервис Статический множественный IP...

ОСНОВНОЙ РАСШИРЕННЫЙ

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Список серверов

Ключ услуги*

Ключ услуги, который будет использоваться для связи с сервисом. Оставьте пустым для постоянного назначения.

Рисунок 25

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 26).

Рисунок 26

- **Ключ услуги** (Рисунок 27). 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.

Новый сервис  Статический множественный IP...

[ОСНОВНОЙ](#) [РАСШИРЕННЫЙ](#)

Тэги
tags

Имя*
VDI_Static

Имя этого элемента

Комментарии
static

Комментарии для этого элемента

[Список серверов](#)
10.10.102.43

Ключ услуги*
1234567890

Ключ услуги, который будет использоваться для связи с сервисом. Оставьте пустым для постоянного назначения.

ТЕСТ [ОТМЕНИТЬ](#) [СОХРАНИТЬ](#)

Рисунок 27

6. Вкладка **Расширенные настройки** (Рисунок 28):

- **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.

Новый сервис

Статический множественный IP...

ОСНОВНОЙ

РАСШИРЕННЫЙ

Время ожидания*

0

Если хост не выполнит проверку, пропустить ее на это время (в минутах).

Проверить порт*

0

Если не ноль, будут обслуживаться только хосты, отвечающие на соединение через этот порт.

Максимальное количество сеансов для машины*

0

Максимальная продолжительность сеанса, после которой VDI посчитает, что машина заблокирована, и разблокирует ее (часов). 0 означает «никогда»

Блокировать машину с помощью внешнего доступа

☐ Нет

ТЕСТ

ОТМЕНИТЬ

СОХРАНИТЬ

Рисунок 28

7. Нажать кнопку **Сохранить**.
8. Созданный сервис будет доступен в списке.

3.1.1.2 *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.

Поставщики услуг

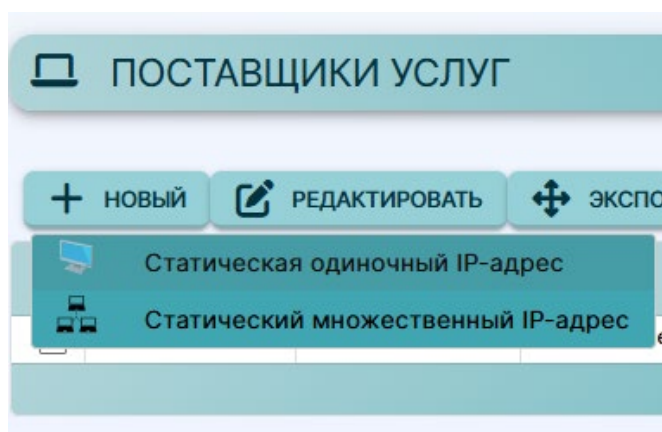
+ НОВЫЙ
 РЕДАКТИРОВАТЬ
 РАЗРЕШЕНИЯ
 ОБСЛУЖИВАНИЕ ВЫБОР

Поиск

Все	Имя	Тип	Комментарии	Статус
☐		Поставщик платформы Иридиум		Обслуживание
☐		Поставщик статических IP-машин		Активный
☐	1-QA-SPHERE	Поставщик платформы Иридиум		Обслуживание
☐	1-QA-STATIC	Поставщик статических IP-машин		Обслуживание
☐	1111	Поставщик платформы Иридиум	test1	Обслуживание
☐	1aaaaaaaaaaaaa1	Поставщик платформы Иридиум		Активный
☐	21-IRIDI	Поставщик платформы Иридиум		Обслуживание
☐	ForStaffchicl	Поставщик платформы Иридиум		Обслуживание
☐	IRIDIUM	Поставщик платформы Иридиум		Обслуживание
☐	STATIC	Поставщик статических IP-машин		Обслуживание

Рисунок 29

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 30).

Новый сервис

Статическая одиночный IP...

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Spice порт*
5900

Spice порт

IP-адрес машины*

IP-адрес машины

ТЕСТ

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 30

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**.

3.1.2 Поставщик ПК «Звезда»

Для добавления поставщика «Звезда»:

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

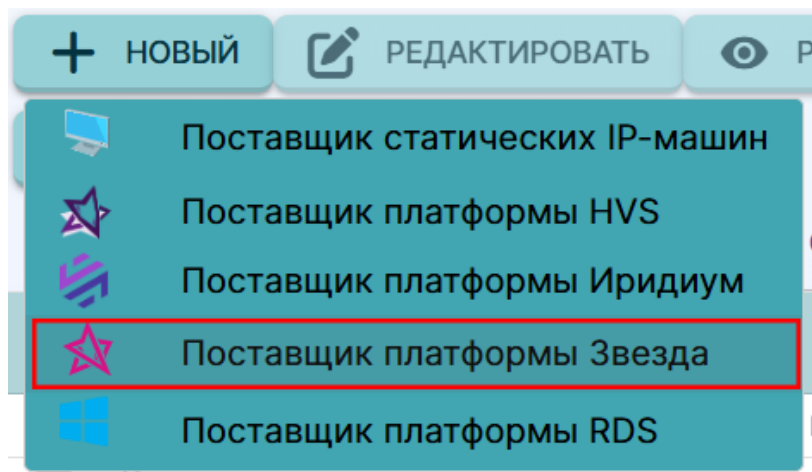


Рисунок 31

3. Откроется окно добавления поставщика.
4. Заполнить следующие поля:
 - **Имя;**
 - **Хост;**
 - **Порт;**
 - **Имя пользователя (с действительными привилегиями);**
 - **Пароль от учетной записи пользователя.**

Новый поста...



Поставщик плат...

Тэги

tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Хост*

Звезда Хост

Порт*

3651

Звезда порт (по умолчанию 3651 для не-SSL-подключения)

Имя пользователя*

Пользователь с действительными привилегиями в Звезде

Пароль*

Пароль пользователя Звезды

ТЕСТ

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 32

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

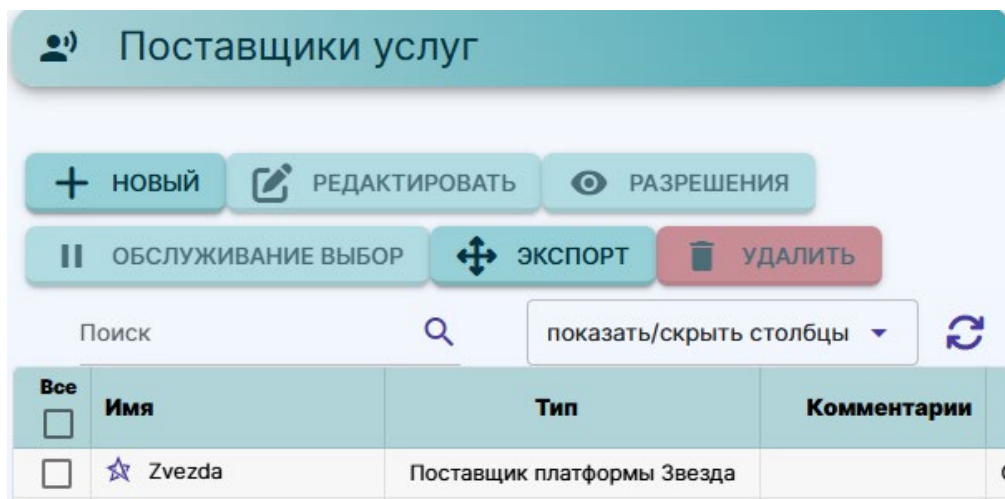


Рисунок 33

3.1.2.1 *Изменение параметров поставщика «Звезда»*

Для изменения настроек поставщика:

1. Выбрать созданный ранее поставщик.
2. Нажать кнопку **Редактировать**.

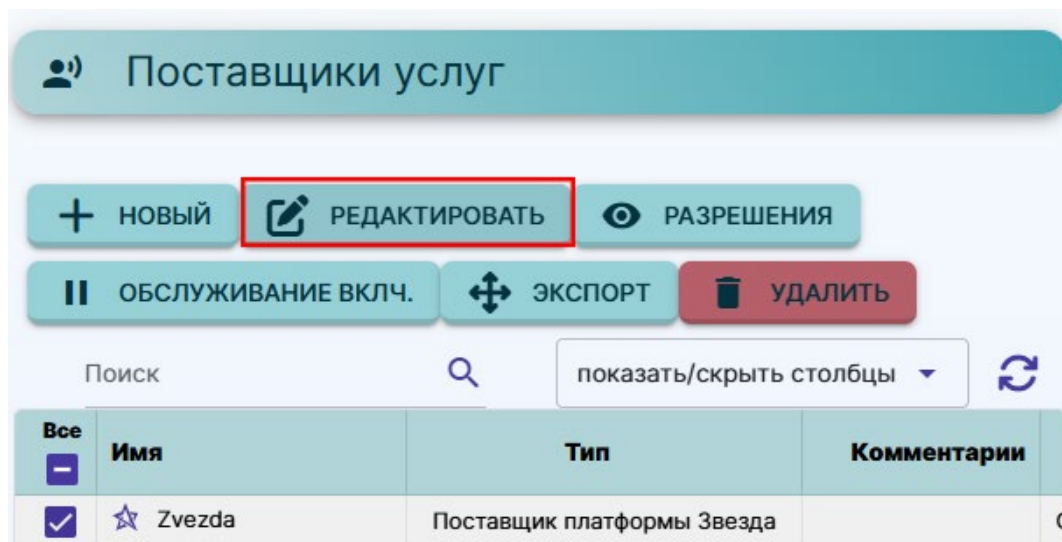


Рисунок 34

3. Откроется окно редактирования поставщика.

Новый поста... ☆ Поставщик плат...

Тэги

tags

Имя*

zvezda

Имя этого элемента

Комментарии

Комментарии для этого элемента

Хост*

10.10.105.42

Звезда Хост

Порт*

3651

Звезда порт (по умолчанию 3651 для не-SSL-подключения)

Имя пользователя*

admin

Пользователь с действительными привилегиями в Звезде

Пароль*

.....|

Пароль пользователя Звезды

ТЕСТ

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 35

4. Нажать кнопку **Сохранить**.

3.1.2.2 Создание службы на основе поставщика Звезда

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

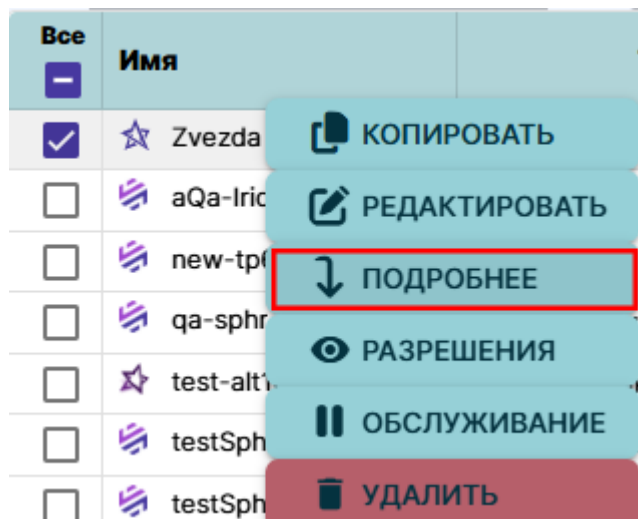


Рисунок 36

3. Нажать кнопку **Новый** -> Действующий образы Звезды.

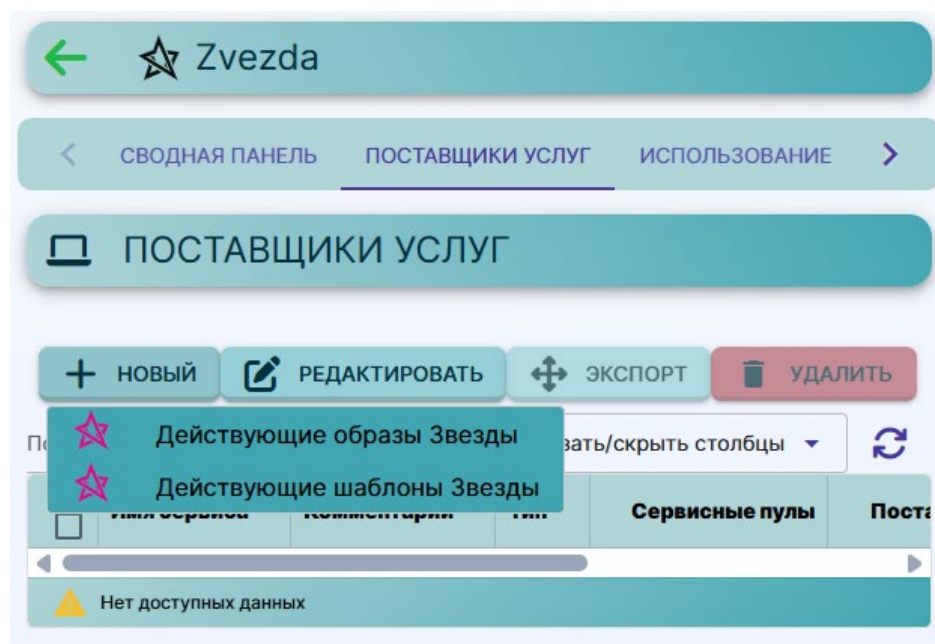


Рисунок 37

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

Новый сервис  Действующие о...

ОСНОВНОЙ

МАШИНА

Тэги

tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Хранилище*

Datastore

Рисунок 38

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

Новый сервис**Действующие о...**

ОСНОВНОЙ

МАШИНА

Базовый шаблон*

Alt10-for-test_5



Базовое имя*

Базовое имя для клонов этой машины

Длина имени*

5

Размер числовой части названий этих машин

Связанный клон



Нет

Рисунок 39

6. Нажать кнопку **Сохранить**.

3.1.3 Поставщик «Иридиум»

Для добавления поставщика «Иридиум»:

8. В разделе **Поставщики услуг** нажать кнопку **Новый**.
9. В списке выбрать **Поставщик платформы Иридиум**.

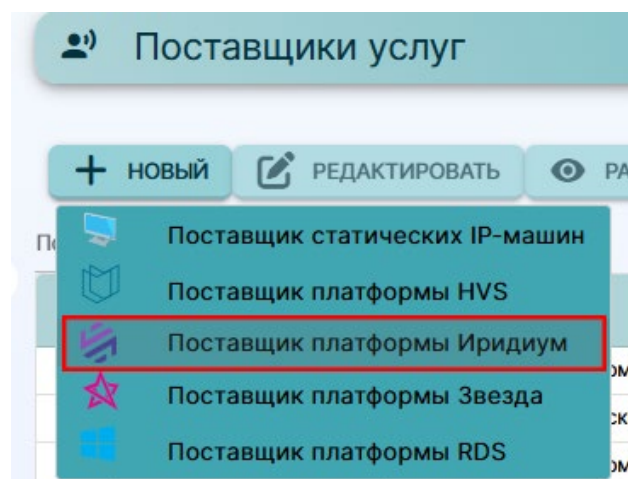


Рисунок 40

10. Откроется окно добавления поставщика.

11. Заполнить следующие поля:

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

Рисунок 41

12. Нажать кнопку **Тест** для тестирования подключения к поставщику.

13. Нажать кнопку **Сохранить**.

14. 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 IridiumSphere 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 42

3.1.3.1 Изменение параметров поставщика Иридиум

Для изменения настроек поставщика:

7. Выбрать созданный ранее поставщик.
8. Нажать кнопку **Редактировать**.

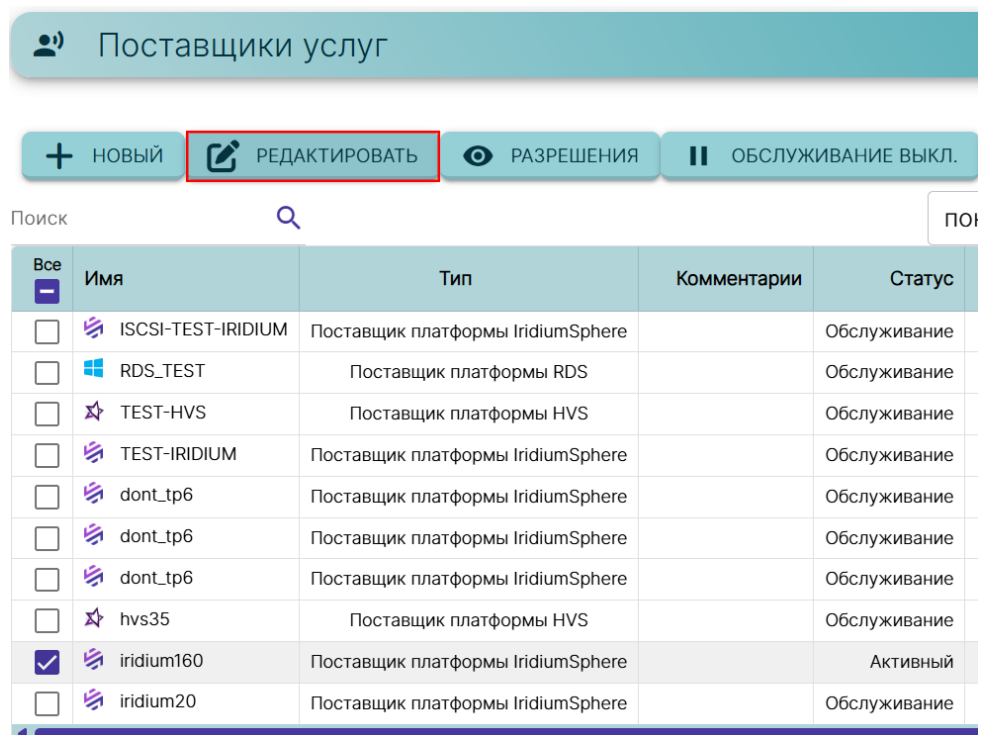


Рисунок 43

9. Откроется окно редактирования поставщика.

Изменить постав...

 Поставщик платформы...

iridium160

Имя этого элемента

Комментарии

Комментарии для этого элемента

Хост*

10.10.102.160

Sphere Хост

Порт*

3651

Порт Sphere (по умолчанию 2633 для не-SSL-подключения)

Имя пользователя*

admin

Пользователь с действительными привилегиями в Sphere

Пароль*

.....

Пароль пользователя Sphere

ТЕСТ

ОТМЕНИТЬ

СОХРАНИТЬ

Рисунок 44

10. Нажать кнопку **Сохранить**.

3.1.3.2 *Создание службы на основе поставщика Иридиум*

5. Дважды нажать на созданный ранее поставщик.

6. Выбрать кнопку **Подробнее**.

Все	Имя	Тип	Кс
☐	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 IridiumSphere	
☐	dont_tp6	Поставщик платформы IridiumSphere	
☐	dont_tp6	Поставщик платформы IridiumSphere	
☐	hvs35	Поставщик платформы HVS	
☒	iridium100	Поставщик платформы IridiumSphere	
☐	iridium100	Поставщик платформы IridiumSphere	

1 строка в

ПОДРОБНЕЕ

РАЗРЕШЕНИЯ IFT для выбора/отмены выбора

ОБСЛУЖИВАНИЕ

Рисунок 45

7. Нажать кнопку **Новый**. Выбрать, на основе шаблона или образа будет создана услуга.

← 21-IRIDI

СВОДНАЯ ПАНЕЛЬ ПОСТАВЩИКИ УСЛУГ ИСПОЛЬЗОВАНИЕ ЖУРНАЛЫ

ПОСТАВЩИКИ УСЛУГ

+ НОВЫЙ РЕДАКТИРОВАТЬ ЭКСПОРТ УДАЛИТЬ

Действующие образы Иридиум

Действующие шаблоны Иридиум

Имя	Тип
Aziziov-temp-astra	Действующие шаблоны Иридиум
new-temp-link	Действующие шаблоны Иридиум
qa-notlink-temp-astra1.8	Действующие шаблоны Иридиум
qa-vm-link-astra	Действующие образы Иридиум
qa-vm-notlink-astra	Действующие образы Иридиум
temp-linked-win10	Действующие шаблоны Иридиум

Рисунок 46

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

Новый сервис



Действующие образы I...

ОСНОВНОЙ

МАШИНА

Тэги

tags

Имя*

pool1

Имя этого элемента

Комментарии

Комментарии для этого элемента

Хранилище*

Datastore

Datastore

ТЕСТ

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 47

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

Новый сервис



Действующие образы I...

ОСНОВНОЙ

МАШИНА

Базовый шаблон*

alpine



Базовое имя*

alpine|

Базовое имя для клонов этой машины

Длина имени*

5

Размер числовой части названий этих машин

ТЕСТ

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 48

12. Нажать кнопку **Сохранить**.

3.1.4 Поставщик платформы RDS

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

Для обеспечения доступа требуется сопоставление учетных записей пользователей.

Для добавления поставщика платформы RDS необходимо выполнить следующие действия:

1. Перейти в раздел **Поставщики услуг**.
2. Нажать **Новый** и выбрать **Поставщик платформы RDS** (Рисунок 49):

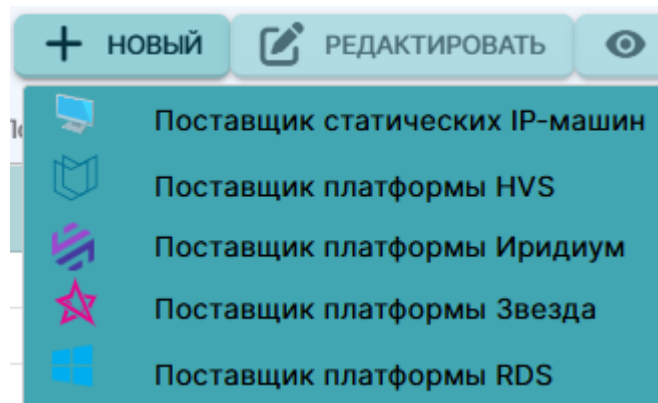


Рисунок 49

3. Заполнить следующие поля (Рисунок 50):

Новый постав...  Поставщик плат...

< ОСНОВНОЙ СОПОСТАВЛЕНИЕ ПОЛЬЗОВАТЕЛ >

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Список серверов

Проверка сервера

☐ Нет

ТЕСТ ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 50

- **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 51

- **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 та же служба RDS может иметь несколько IP-адресов, соединяющих различные существующие серверы RDS, что обеспечивает высокую доступность приложений. Кроме того, при указании нескольких IP-адресов необходимо отметить флажок «Сервер проверяется».

4. Вкладка **Сопоставление пользователей** (Рисунок 53) 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:

Новый постав...  Поставщик плат...

< ПОСТАВЛЕНИЕ ПОЛЬЗОВАТЕЛЕЙ УПРАВЛЕНИЕ >

Сопоставление пользователей

☒ Да

Пользователи

user

Пароль*

Пароль по умолчанию для пользователей в списке сопоставления.
(Не используется, если сопоставление пользователей отключено)

ТЕСТ

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 52

- Необходимо нажать на поле **Пользователи**, ввести имя пользователя (Рисунок 53);
- нажать кнопку **Добавить**;
- Нажать кнопку **Сохранить**.
- Поле **Пароль**. Пароль по умолчанию для пользователей в списке сопоставления. Все пользователи сопоставления должны иметь одинаковый пароль.

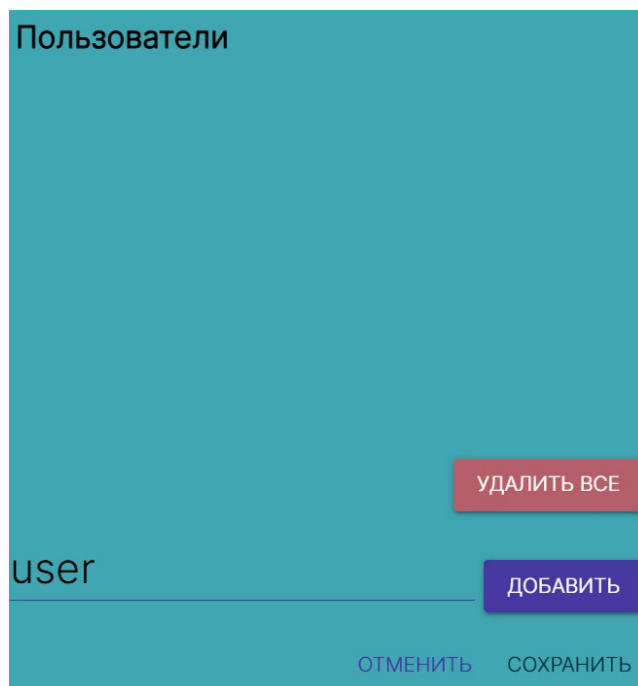


Рисунок 53

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 54). Эти пользователи будут автоматически созданы VDI.

Новый поставщик Поставщик платформы RDS

ОСНОВНОЙ СОПОСТАВЛЕНИЕ ПОЛЬЗОВАТЕЛЕЙ УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ AD

Автоматическое создание пользователя в AD

☐ Нет

Сервер AD

IP или ХОСТ сервера AD. Должна быть включена поддержка LDAPS

Порт*

636

Порт AD LDAPS (по умолчанию 636)

OU сервера AD для созданных пользователей

Ветвь сервера AD, где пользователи будут созданы VDI

Имя пользователя

Имя пользователя с правами на создание/удаление учетных записей. Используйте: USER@DOMAIN.XXX

Пароль

Пароль пользователя с привилегиями

Префикс для созданных пользователей

VDI_

Если не пусто, VDI попытается добавить управляемых пользователей в эту группу

ТЕСТ ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 54

- 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.

OU сервера AD для созданных пользователей

Ветвь сервера AD, где пользователи будут созданы VDI

Имя пользователя

Имя пользователя с правами на создание/удаление учетных записей. Используйте: USER@DOMAIN.XXX

Пароль

Пароль пользователя с привилегиями

Префикс для созданных пользователей VDI_

Если не пусто, VDI попытается добавить управляемых пользователей в эту группу

AD Домен

Домен для вновь созданных пользователей (например, example.com, example.local). Если пусто, будет выведено из имени пользователя

Группа AD*

Если не пусто, VDI попытается добавить управляемых пользователей в эту группу

ТЕСТ

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 55

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

15. С помощью кнопки **Тест** производится успешность подключения.

16. Для сохранения конфигурации нажать кнопку **Сохранить**.

3.1.4.1 *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.

3.1.4.2 *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 56).

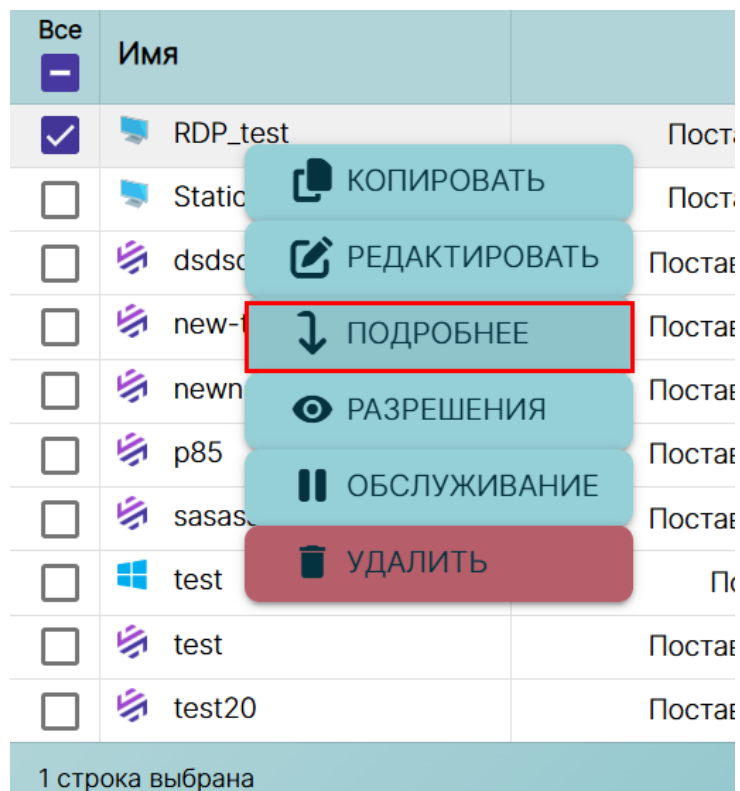


Рисунок 56

2. Нажать кнопку **Новый**.
3. Откроется окно выбора типа службы: на основе статической одиночной IP-адресации или на основе множественной IP-адресации (Рисунок 57).

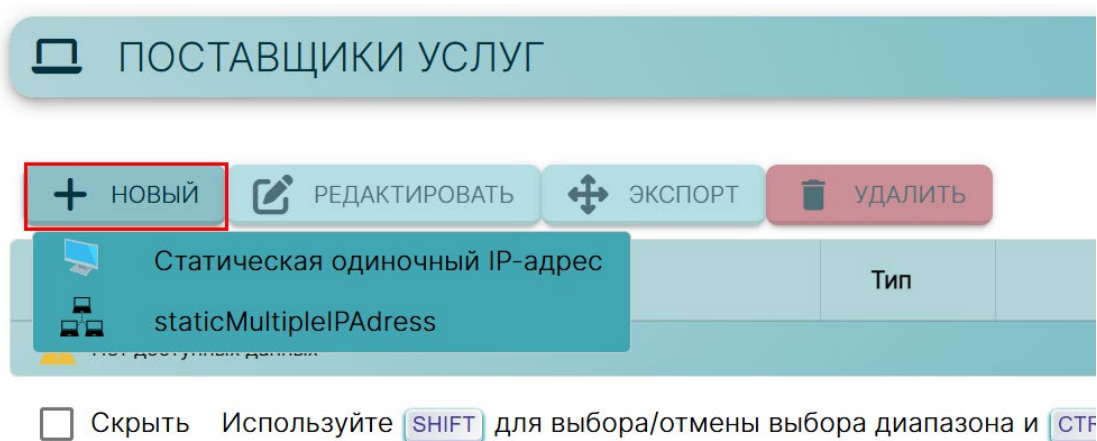


Рисунок 57

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 58):

- 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 58

- Дополнительно (Рисунок 59):

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

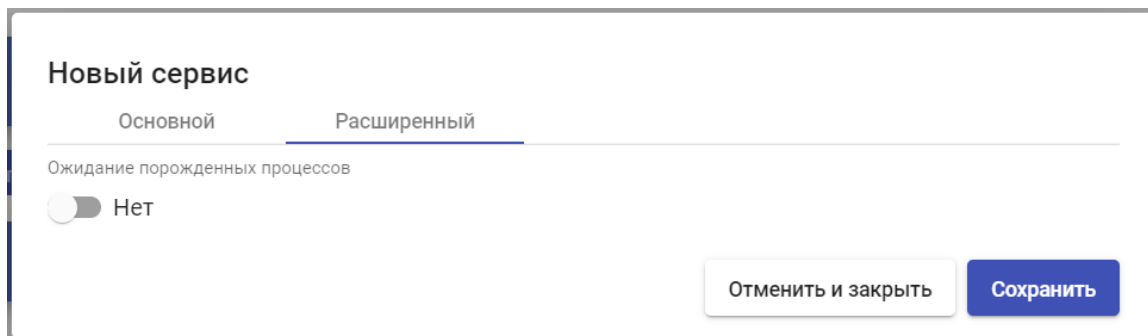


Рисунок 59

3.2 Настройки аутентификации

3.2.1 Аутентификатор Active Directory

Этот внешний аутентификатор обеспечивает доступ к виртуальным рабочим столам и приложениям для пользователей и групп пользователей, принадлежащих Active Directory (Рисунок 60).

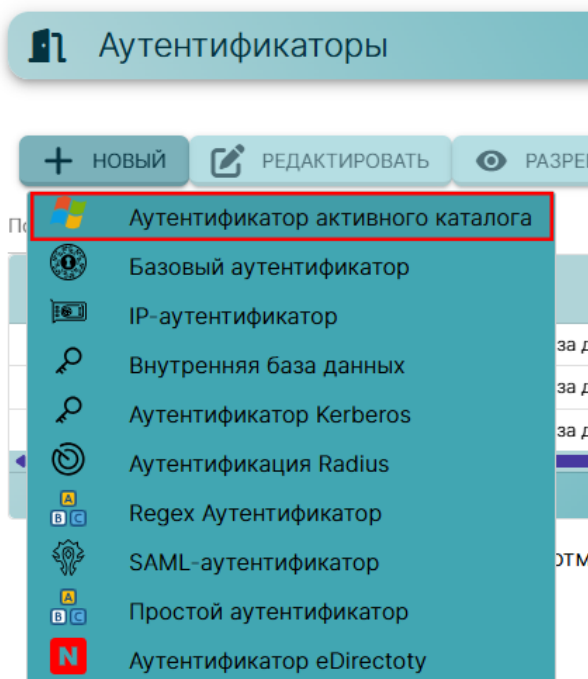


Рисунок 60

Для настройки аутентификатора Active Directory необходимо:

1. Перейти в раздел **Аутентификаторы**.

2. Нажать кнопку **Новый**.
3. Откроется окно добавления аутентификатора, **Основная вкладка** (Рисунок 61) 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.

Новый поставщик  Аутентификатор акт...

< **ОСНОВНОЙ** УЧЕТНЫЕ ДАННЫЕ РАСШИРЕННЫЙ >

Тэги
tags

Имя*
Имя этого элемента

Комментарии
Комментарии для этого элемента

Приоритет*
1
Выбирает приоритет этого элемента (меньшее число означает более высокая приоритет)

Метка*
Метка транспорта Metapool (используется только в группировке транспортов Metapool)

Хост*
Хост

Использовать SSL
☐ Нет

Совместимость
WindowsNT

Тайм-аут*
10
Время ожидания соединения в секундах

ТЕСТ [ОТМЕНИТЬ](#) [СОХРАНИТЬ](#)

Рисунок 61

4. Вкладка **Учетные данные** (Рисунок 62). Заполнить поля **Имя пользователя** и **Пароль**.

Новый поставщик  Аутентификатор акт...

< ОСНОВНОЙ **УЧЕТНЫЕ ДАННЫЕ** РАСШИРЕННЫЙ >

Имя пользователя*
Имя пользователя с правами чтения на выбранной базе. Для этого используйте форму USER@DOMAIN.XXX

Пароль*
Пароль пользователя ldap

Рисунок 62

5. Вкладка **Расширенный** (Рисунок 63). Поле **Переопределить базу** позволяет вручную указать «базу поиска» (Search Base) для LDAP-запросов к домену Active Directory.

- значение 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**.

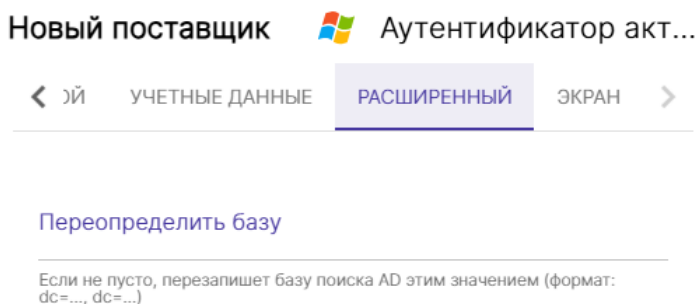


Рисунок 63

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.

3.2.2 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 64).

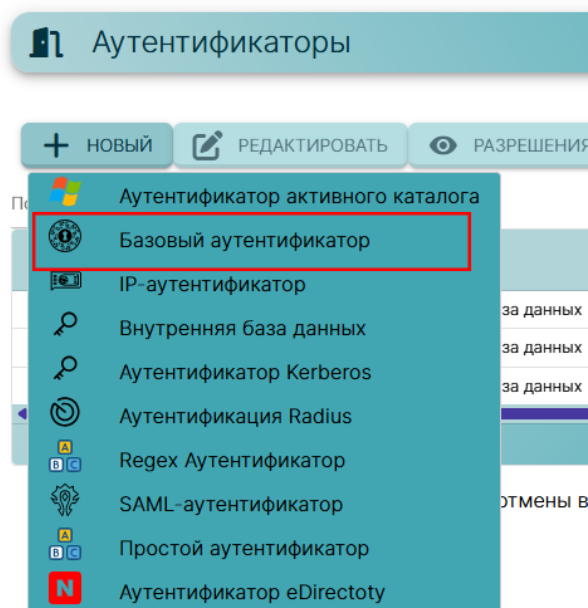


Рисунок 64

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 65):

Новый поставщик



Базовый аутентификатор

ОСНОВНОЙ

СЕРВЕР

РАСШИРЕННЫЙ

АТРИБУТЫ

ЭКРАН

Тэги

tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Приоритет*

1

Выбирает приоритет этого элемента (меньшее число означает более высокая приоритет)

Метка*

Метка транспорта Metapool (используется только в группировке транспортных Metapool)

ТЕСТ

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 65

- **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 пытаться использовать этого поставщика аутентификации;
- **Метка**. Поле необходимо для группировки в механизме Metapool.

3. Вкладка **Сервер** (Рисунок 66):

ОСНОВНОЙ	СЕРВЕР	РАСШИРЕННЫЙ	АТРИБУТЫ	ЭКРАН
Идентификатор клиента				
Получено из приложения, созданного в Azure для UDS Enterprise				
Секрет клиента				
Получено из приложения, созданного в Azure для UDS Enterprise - Ключи				
Область				
Область действия OAuth2.				
Общие группы				
Пользователь будет назначен в эту группу после аутентификации. Список групп, разделенных запятыми				
Конечная точка авторизации				
Конечная точка авторизации для OAuth2.				

Рисунок 66

- **Идентификатор клиента.** Уникальный идентификатор приложения;
 - **Секрет клиента.** Секретный ключ 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 67). Вкладка настраивает аутентификацию по протоколу OAuth 2.0.

ОСНОВНОЙ	СЕРВЕР	РАСШИРЕННЫЙ	АТРИБУТЫ	ЭКРАН
----------	--------	--------------------	----------	-------

Конечная точка перенаправления

Конечная точка перенаправления для OAuth2. (Заполняется UDS)

Тип ответа*

Тип ответа для OAuth2.

Конечная точка токена

Конечная точка токена для OAuth2. Требуется только для типа ответа 'code'.

Конечная точка информации о пользователе

Конечная точка информации о пользователе для OAuth2. Требуется только для типа ответа 'code'.

Открытый ключ

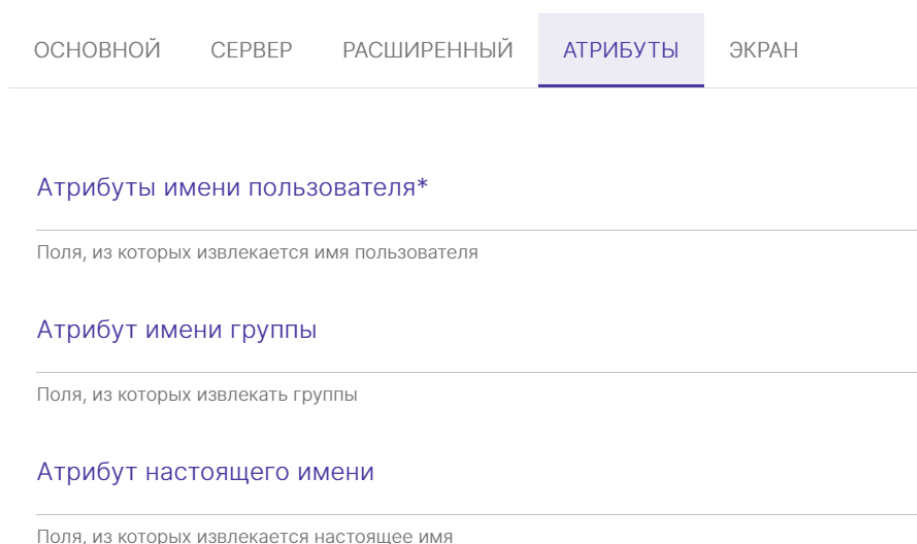
Предоставлено провайдером OAuth2

Рисунок 67

- **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 68) 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.



ОСНОВНОЙ	СЕРВЕР	РАСШИРЕННЫЙ	АТРИБУТЫ	ЭКРАН
----------	--------	-------------	-----------------	-------

Атрибуты имени пользователя*

Поля, из которых извлекается имя пользователя

Атрибут имени группы

Поля, из которых извлекать группы

Атрибут настоящего имени

Поля, из которых извлекается настоящее имя

Рисунок 68

6. Вкладка **Экран** (Рисунок 69). Настраивает видимость аутентификатора для пользователя.

Новый поставщик



Базовый аутентификатор

ОСНОВНОЙ

СЕРВЕР

РАСШИРЕННЫЙ

АТРИБУТЫ

ЭКРАН

Видимый



Да

Рисунок 69

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

3.2.3 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 70).

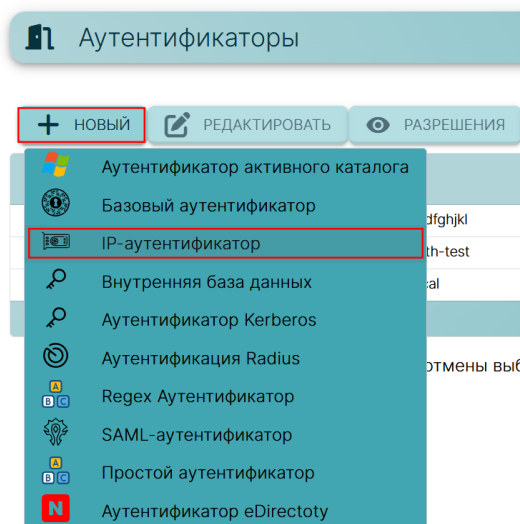


Рисунок 70

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.

Новый аутентификатор 📺 IP-аутентификатор

ОСНОВНОЙ **РАСШИРЕННЫЙ** ЭКРАН

Принять прокси ☐ Нет

Видно только из этих сетей

Этот аутентификатор будет виден только из этих сетей. Оставьте пустым, чтобы разрешить все сети

Рисунок 71

6. Вкладка **Экран** (Рисунок 72) управляет видимостью аутентификатора при выборе способа аутентификации в систему.

Новый поставщик 📺 IP-аутентификатор

ОСНОВНОЙ РАСШИРЕННЫЙ **ЭКРАН**

Видимый1 ☒ Да

Рисунок 72

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

3.2.4 Внутренняя база данных

Аутентификатор **Внутренняя 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 73).

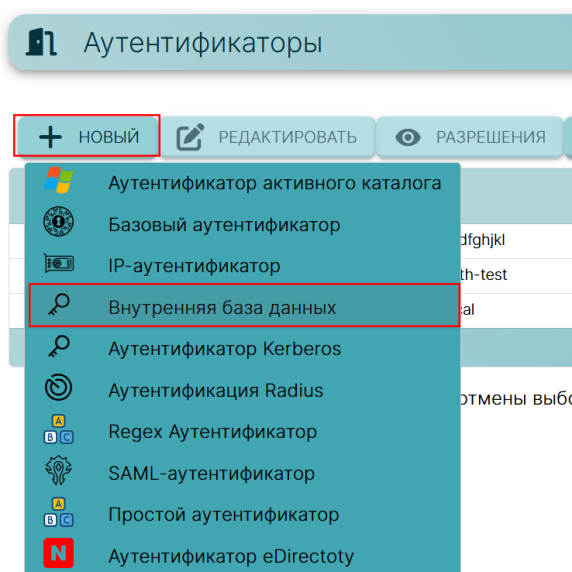


Рисунок 73

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.

3.2.5 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.

Для создания:

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

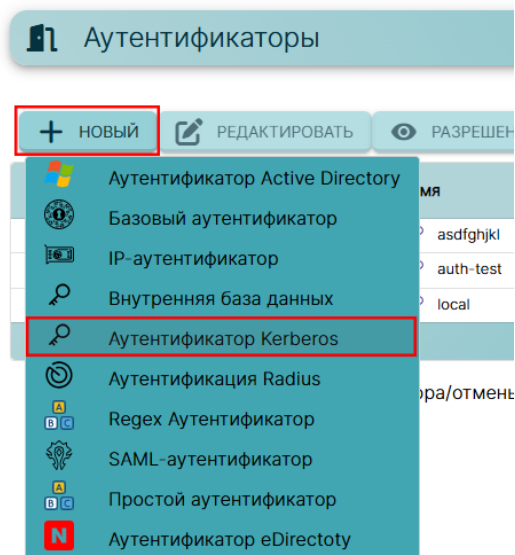


Рисунок 74

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;

3.2.6 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**.

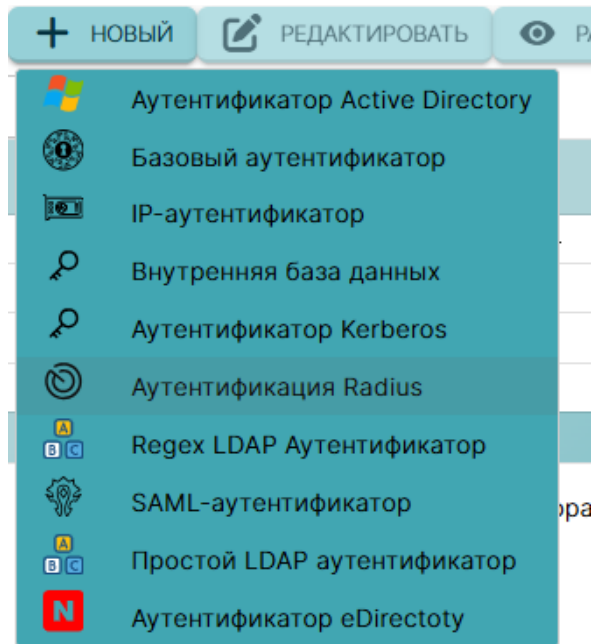


Рисунок 75

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).

Новый аутентификатор

 Аутентификация Radius

ОСНОВНОЙ

РАСШИРЕННЫЙ

МФА

ЭКРАН

Тэги

tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Приоритет*

1

Выбирает приоритет этого элемента (меньшее число означает более высокий приоритет)

Метка*

Метка транспорта Metapool (используется только в группировке транспортов Metapool)

Хост*

IP-адрес или имя хоста сервера Radius

Порт*

Порт аутентификации Radius (обычно 1812)

Секрет*

Секрет клиента Radius

ТЕСТ

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 76

5. На вкладке **Расширенный** (Рисунок 77):

- **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).

Новый аутентификатор 🔒 Аутентификация Radius

ОСНОВНОЙ РАСШИРЕННЫЙ МФА ЭКРАН

Идентификатор NAS*

Идентификатор NAS для Radius-сервера

Префикс приложения для атрибута класса

Префикс приложения для фильтрации групп по атрибуту 'Класс'

Глобальная группа

Если установлено, это значение будет добавлено как группа для всех пользователей радиуса

Рисунок 77

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 78):

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

Новый аутентификатор 🔒 Аутентификация Radius

ОСНОВНОЙ РАСШИРЕННЫЙ МФА ЭКРАН

Атрибут MFA

Атрибут, из которого можно извлечь код MFA

mFAProvider

Нет

Рисунок 78

7. На вкладке **«Экран»** (Рисунок 79):

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

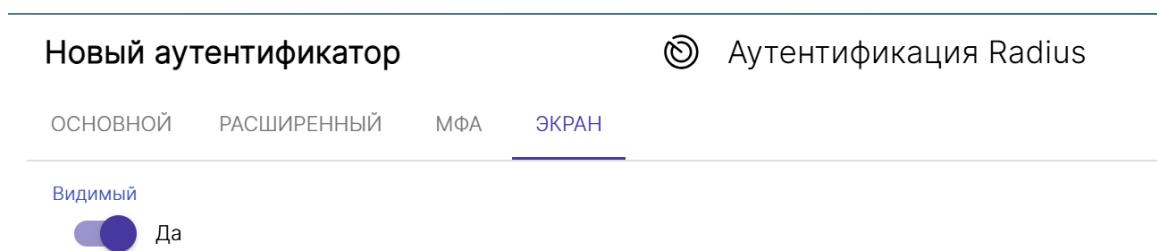


Рисунок 79

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

3.2.7 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**.

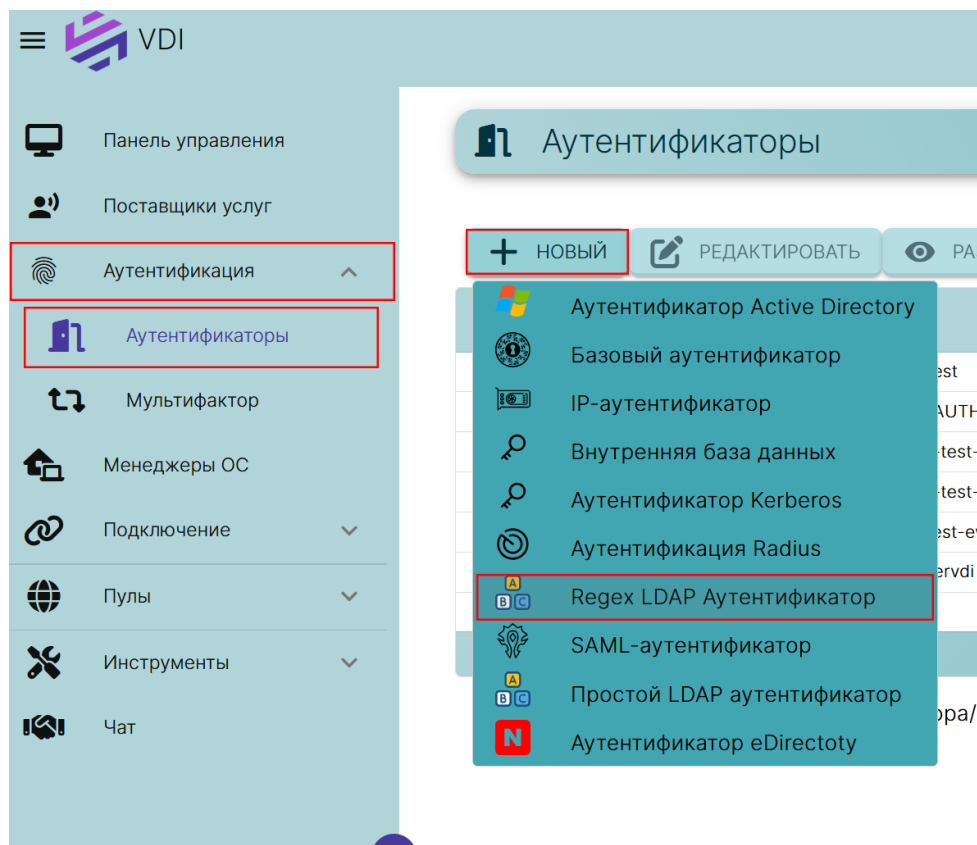


Рисунок 80

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.

Новый аутентиф...  Regex LDAP Аутент...

< **ОСНОВНОЙ** УЧЕТНЫЕ ДАННЫЕ РАСШИРЕННЫЙ LI >

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Приоритет*
1

Выбирает приоритет этого элемента (меньшее число означает более высокий приоритет)

Метка*

Метка транспорта Metapool (используется только в группировке транспортов Metapool)

Хост*

IP-адрес или имя хоста сервера Radius

Порт*
389

Порт аутентификации Radius (обычно 1812)

Использовать SSL

☐ Нет

Рисунок 81

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.

Новый аутентиф...  Regex LDAP Аутент...

< ОСНОВНОЙ **УЧЕТНЫЕ ДАННЫЕ** РАСШИРЕННЫЙ LI >

Имя пользователя*

Имя пользователя с правами чтения на выбранной базе. Для этого используйте форму USER@DOMAIN.XXX

Пароль*

Пароль пользователя ldap

Рисунок 82

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).

The screenshot shows a web interface for configuring LDAP authentication. At the top, there's a title bar with 'Новый аутентиф...' and 'Regex LDAP Аутент...'. Below it are four tabs: 'ОСНОВНОЙ', 'УЧЕТНЫЕ ДАННЫЕ', 'РАСШИРЕННЫЙ' (which is active and highlighted with a blue underline), and 'LI'. The 'РАСШИРЕННЫЙ' tab contains several settings:

- Тайм-аут***: A text input field containing the value '10'. Below it is a small text label: 'Время ожидания подключения к OpenGnsys в секундах'.
- Проверить сертификат**: A toggle switch that is currently turned off, with the label 'Нет' next to it.
- Сертификат**: A text input field. Below it is a small text label: 'Сертификат, используемый для проверки SSL'.
- Альтернативный класс**: A text input field. Below it is a small text label: 'Класс для объектов LDAP, которые также будут проверяться на предмет извлечения групп (обычно пустой)'.

Рисунок 83

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.

Новый аутентиф...  Regex LDAP Аутент...

< НЫЕ ДАННЫЕ РАСШИРЕННЫЙ **LDAPINFO** МФА : >

База*

Общая база поиска (используется для 'пользователей' и 'групп')

Класс пользователя*

Класс для пользователей LDAP (обычно учетная запись)

Атрибут идентификатора пользователя*

Атрибут, содержащий идентификатор пользователя

Атрибуты имени пользователя*

Поля, из которых извлекается имя пользователя

Атрибут имени группы*

Поля, из которых извлекать группы

Рисунок 84

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.

Новый аутентиф...  Regex LDAP Аутент...

< НЫЕ ДАННЫЕ РАСШИРЕННЫЙ LDAPINFO **МФА** : >

Атрибут MFA

Атрибут, из которого можно извлечь код MFA

mFAProvider

Нет

Рисунок 85

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

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

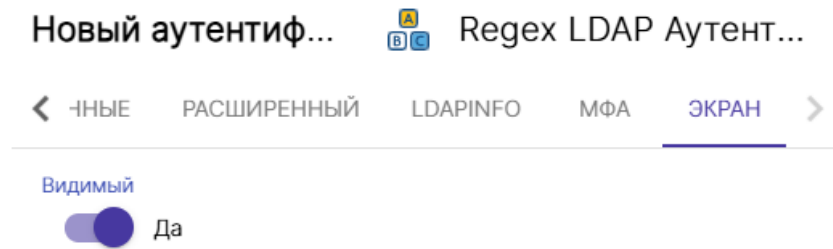


Рисунок 86

9. Нажать кнопку **Сохранить**.

10. Аутентификатор станет доступен в общем списке аутентификаторов.

3.2.8 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**.

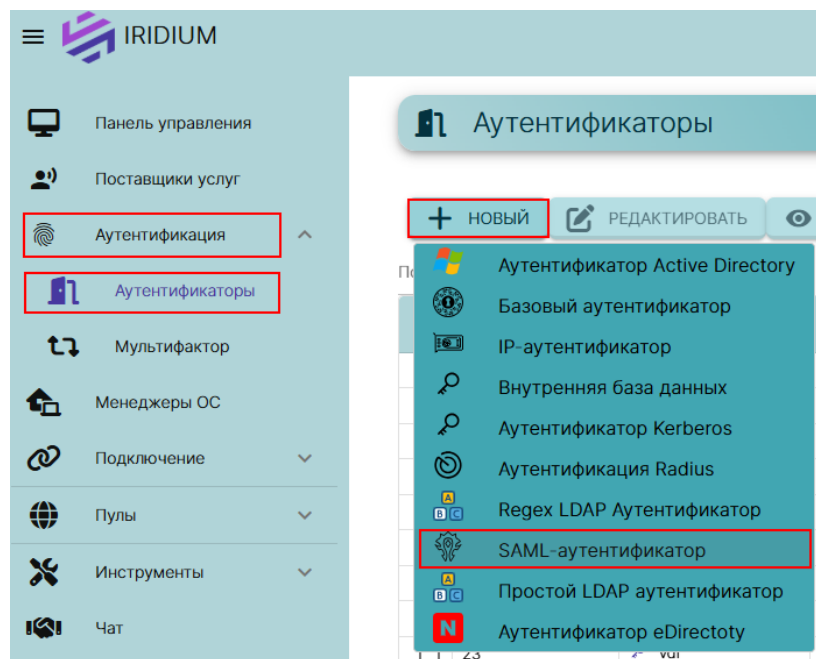


Рисунок 87

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.

Новый аутентиф...  SAML-аутентификат...

< ОСНОВНОЙ СЕРТИФИКАТ МЕТАДАННЫЕ АТРИБУТ >

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Приоритет*

1

Выбирает приоритет этого элемента (меньшее число означает более высокий приоритет)

Метка*

Метка транспорта Metapool (используется только в группировке транспортов Metapool)

Рисунок 88

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.

Новый аутентиф...  SAML-аутентификат...

< ОСНОВНОЙ СЕРТИФИКАТ МЕТАДАННЫЕ АТРИБУТ >

Закрытый ключ*

Закрытый ключ, используемый для подписи и шифрования, генерируется в восьми цветах (64) с помощью открытого летальности

Сертификат*

Сертификат сервера, используемый в SAML, созданный в Bash1 64 на основе открытого летальности

Рисунок 89

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).

The screenshot shows a web interface with a top navigation bar containing 'Новый аутентиф...' and 'SAML-аутентификат...'. Below this is a tabbed interface with four tabs: 'ОСНОВНОЙ', 'СЕРТИФИКАТ', 'МЕТАДАННЫЕ' (which is active and highlighted with a purple underline), and 'АТТРИБУТ'. The 'МЕТАДАННЫЕ' tab contains the following fields:

- Метаданные IDP***: A text input field with the placeholder 'IDPMetaDataTooltip'.
- Идентификатор сущности**: A text input field with the placeholder 'Вы можете ввести здесь URL или метаданные IDP или сами метаданные (xml)'.
- Срок действия MetaData**: A numeric input field with the value '0' and a spinner control. Below it is a tooltip: 'Срок действия метаданных в днях. 0 означает значение по умолчанию (десять лет)'.
- Длительность кэширования MetaData**: A numeric input field with the value '0'. Below it is a tooltip: 'Длительность кэша метаданных в днях. 0 означает значение по умолчанию (десять лет)'.

Рисунок 90

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.

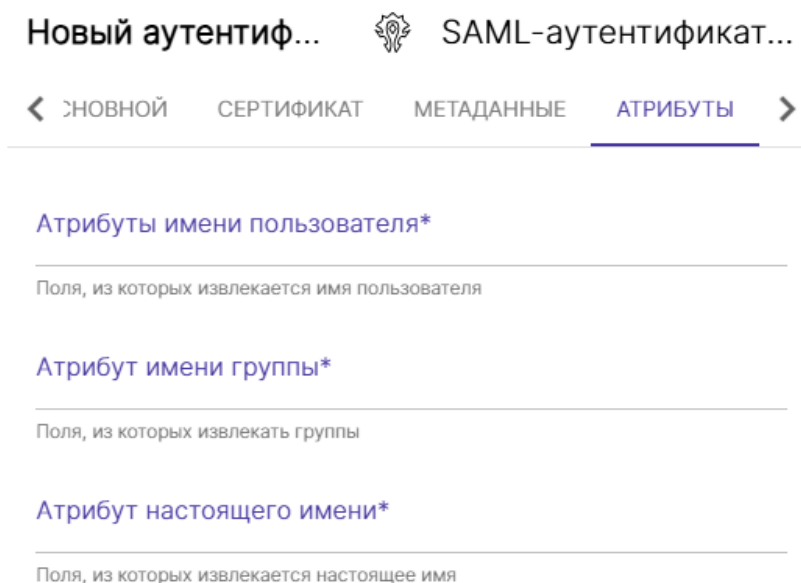


Рисунок 91

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.

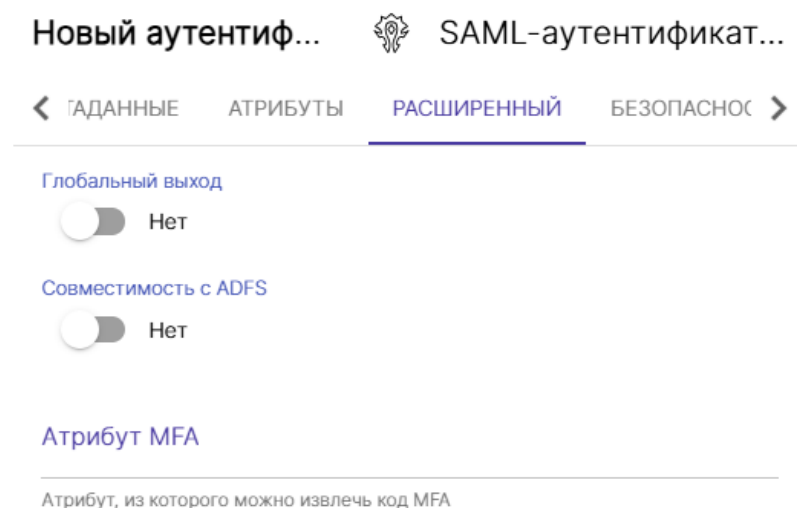


Рисунок 92

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.

Новый аутентиф... SAML-аутентификат...

← БЕЗОПАСНОСТЬ **ОРГАНИЗАЦИЯ** ЭКРАН МФА →

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 93

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

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

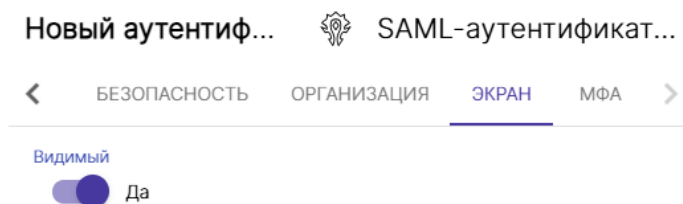


Рисунок 94

12. На вкладке **МФА** заполнить поля:

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

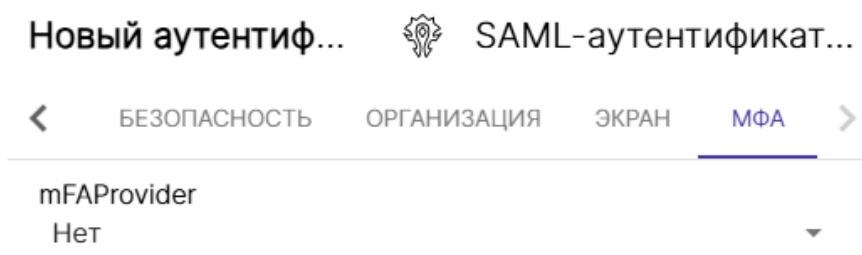


Рисунок 95

13. Нажать кнопку **Сохранить**.

14. Аутентификатор станет доступен в общем списке аутентификаторов.

3.2.9 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**.

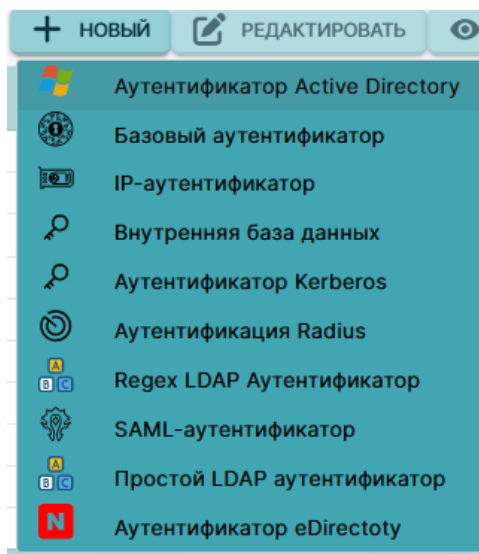


Рисунок 96

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.

Новый аутентиф...  Простой LDAP ауте...

< **ОСНОВНОЙ** УЧЕТНЫЕ ДАННЫЕ РАСШИРЕННЫЙ >

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Приоритет*

1

Выбирает приоритет этого элемента (меньшее число означает более высокий приоритет)

Метка*

Метка транспорта Metapool (используется только в группировке транспортов Metapool)

Хост*

IP-адрес или имя хоста сервера Ldap

Порт*

389

Порт LDAP (обычно 389 для не-SSL и 636 для SSL)

Использовать SSL

☐ Нет

Рисунок 97

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.

Новый аутентиф...  Простой LDAP ауте...

< ОСНОВНОЙ **УЧЕТНЫЕ ДАННЫЕ** РАСШИРЕННЫЙ >

Имя пользователя*

Имя пользователя с правами чтения на выбранной базе. Для этого используйте форму USER@DOMAIN.XXX

Пароль*

Пароль пользователя ldap

Рисунок 98

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.

Новый аутентиф...  Простой LDAP ауте...

< ОСНОВНОЙ УЧЕТНЫЕ ДАННЫЕ **РАСШИРЕННЫЙ** >

Тайм-аут*

10

Время ожидания соединения в секундах

Проверить сертификат

☐ Нет

Сертификат

Сертификат, используемый для проверки SSL

Рисунок 99

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.

Новый аутентиф...  Простой LDAP ауте...

← ЧИТЫЕ РАСШИРЕННЫЙ **МФА** LDAPINFO ЭКРАН →

Атрибут MFA

Атрибут, из которого можно извлечь код MFA

mFAProvider

Нет ▼

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`).

Новый аутентиф...  Простой LDAP ауте...

< ЧИНЫЕ РАСШИРЕННЫЙ МФА **LDAPINFO** ЭКРАН >

База*

Общая база поиска (используется для 'пользователей' и 'групп')

Класс пользователя*

Класс для пользователей LDAP (обычно учетная запись)

Атрибут идентификатора пользователя*

Атрибут, содержащий идентификатор пользователя

Атрибуты имени пользователя*

Поля, из которых извлекается имя пользователя

Групповой класс*

Класс для групп LDAP (обычно posixGroup)

Атрибут идентификатора группы*

Атрибут, содержащий идентификатор группы

Атрибут членства в группе*

Атрибут группы, содержащий пользователей, входящих в нее

Рисунок 100

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

Новый аутентиф...  Простой LDAP ауте...

< ЧИНЫЕ РАСШИРЕННЫЙ МФА LDAPINFO **ЭКРАН** >

Видимый

☒ Да

Рисунок 101

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

3.2.10 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**.

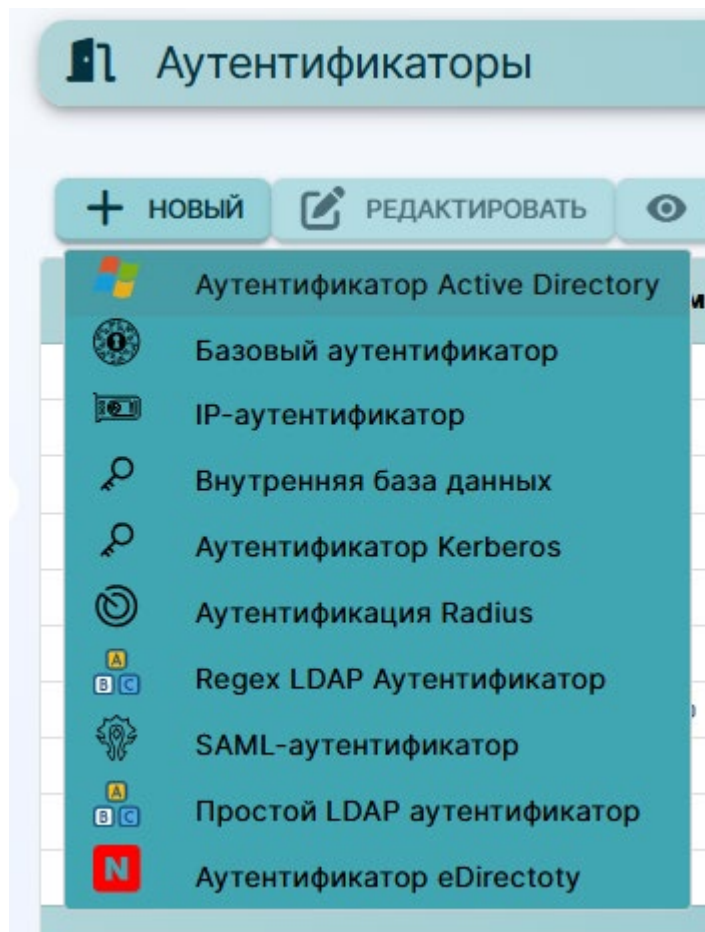


Рисунок 102

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.

Новый аутентиф...  Аутентификатор eDi...

ОСНОВНОЙ УЧЕТНЫЕ ДАННЫЕ ЭКРАН

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Приоритет*

1

Выбирает приоритет этого элемента (меньшее число означает более высокий приоритет)

Метка*

Метка транспорта Metapool (используется только в группировке транспортов Metapool)

Хост*

IP-адрес или имя хоста сервера Ldap

Порт*

389

Порт LDAP (обычно 389 для не-SSL и 636 для SSL)

Использовать SSL

☐ Нет

Тайм-аут*

10

Время ожидания соединения в секундах

Рисунок 103

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

- **Имя пользователя:** Учетная запись пользователя с правами чтения в eDirectory.

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

Новый аутентификатор... **N** Аутентификатор eDi...

ОСНОВНОЙ УЧЕТНЫЕ ДАННЫЕ ЭКРАН

Имя пользователя*

Имя пользователя с правами чтения в eDirectory

Пароль*

Пароль пользователя ldap

Рисунок 104

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

Новый аутентификатор... **N** Аутентификатор eDi...

ОСНОВНОЙ УЧЕТНЫЕ ДАННЫЕ ЭКРАН

Видимый

☒ Да

Рисунок 105

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

3.2.11 Настройка многофакторной аутентификации

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

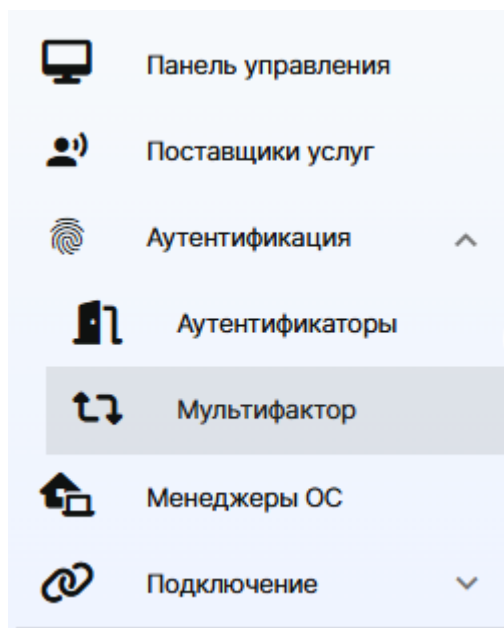


Рисунок 106

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.

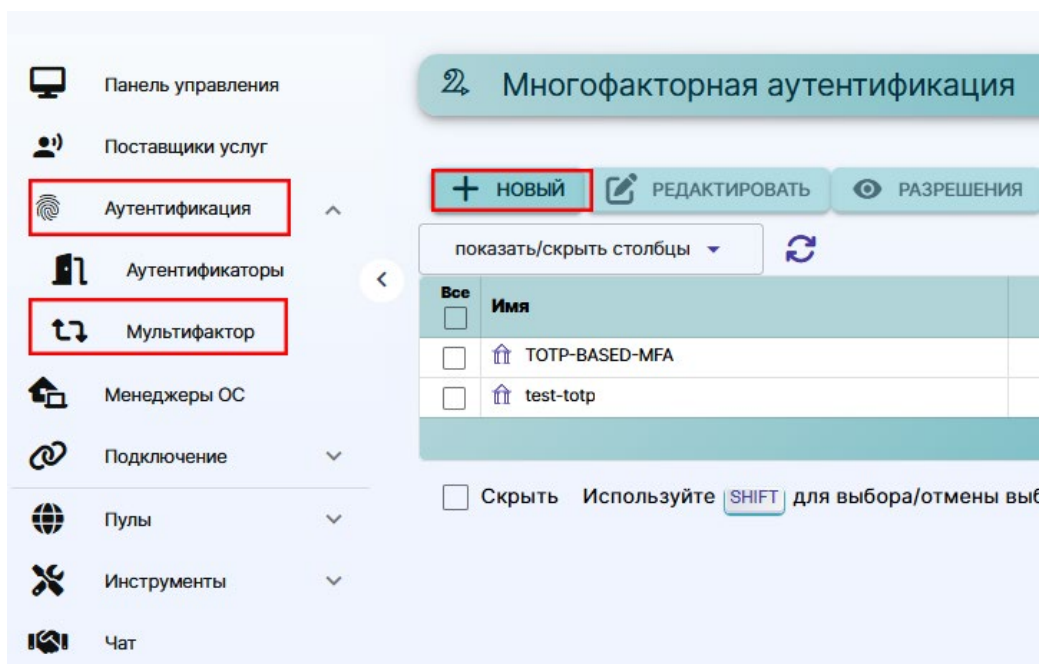


Рисунок 107

Многофакторная конфигурация не является необходимым компонентом для создания Пула услуг.

3.2.11.1 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**.

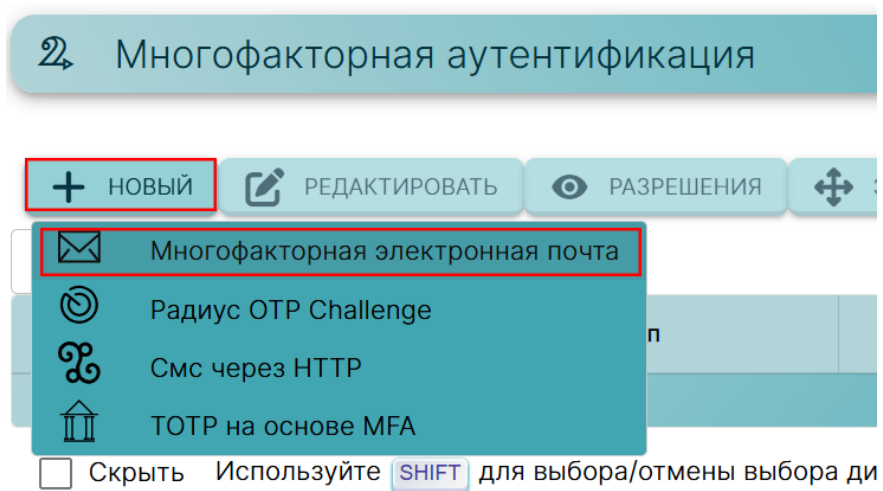


Рисунок 108

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.

Новый аутентифик...  Многофакторная элект...

ОСНОВНОЙ

SMTP СЕРВЕР

КОНФИГУРАЦИЯ

Тэги

tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Кэширование устройства

0

Время в часах для кэширования устройства, чтобы MFA больше не требовалась. На основе пользователя.

Действительность кода MFA

5

Время в минутах, в течение которого можно использовать код MFA.

[ОТМЕНИТЬ](#) [СОХРАНИТЬ](#)

Рисунок 109

3. На вкладке **SMTP-сервер** (Рисунок 110) 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.

Новый аутентификатор... ☒ Многофакторная элект...

ОСНОВНОЙ SMTP СЕРВЕР КОНФИГУРАЦИЯ

SMTP Хост*

Имя хоста или IP-адрес SMTP-сервера. Если вы используете нестандартный порт, добавьте его после двоеточия, например: smtp.gmail.com:587

Безопасность

TLS

Имя пользователя

Пользователь с доступом к SMTP-серверу

Пароль

Пароль пользователя с доступом к SMTP-серверу

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 110

4. На вкладке «Конфигурация» (Рисунок 111):

- **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.
- **ОТР Сети.** Выпадающий список для выбора сетей одноразовых паролей (ОТР), 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.

Новый аутентификат... ☒ Многофакторная электро...

ОСНОВНОЙ SMTP СЕРВЕР **КОНФИГУРАЦИЯ**

Тема*

Тема письма

Из электронной почты*

Адрес электронной почты, который будет использоваться в качестве отправителя

enable HTML

☐ Нет

Пользователь без политики MFA*

allowUserLogin

ОТР Сети

Текст письма*

Текст письма. Если пусто, будет использован текст по умолчанию. Разрешенные переменные: , , .

Почта HTML

HTML письма. Если пусто, будет использован HTML по умолчанию Разрешенные переменные: , , .

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 111

5. Нажать кнопку **Сохранить**.

3.2.11.2 *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**.

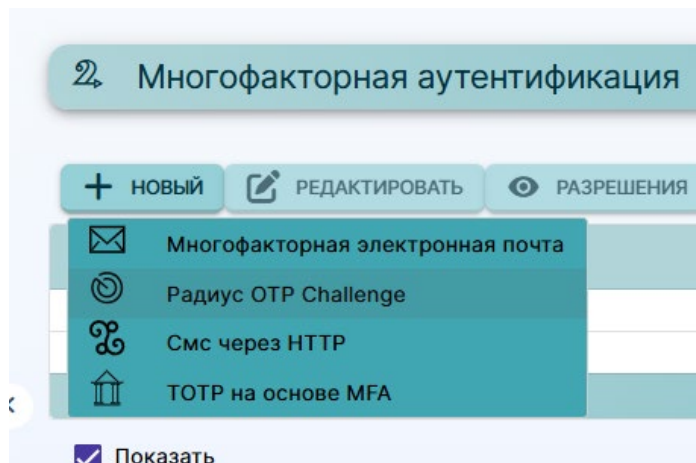


Рисунок 112

3. На вкладке **Основной** заполнить поля (Рисунок 113):

- **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.

Новый аутентиф...  Радиус OTP Challen...

ОСНОВНОЙ КОНФИГУРАЦИЯ

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Хост*

IP-адрес или имя хоста сервера Radius

Порт*

Порт аутентификации Radius (обычно 1812)

Секрет*

Секрет клиента Radius

Все пользователи должны отправить OTP

☐ Нет

Идентификатор NAS*

Идентификатор NAS для Radius-сервера

Кэширование устройства

0

Время в часах для кэширования устройства, чтобы MFA больше не требовалась. На основе пользователя.

Действительность кода MFA

5

Время в минутах, в течение которого можно использовать код MFA.

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 113

4. На вкладке **Конфигурация** заполнить поля (Рисунок 114):

- **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.

Новый аутентиф...
⦿ Радиус OTP Challen...

ОСНОВНОЙ	КОНФИГУРАЦИЯ
Radius OTP Действие при ошибке связи*	Разрешить вход пользователю ▼
Radius OTP Сети	▼
Пользователь без политики MFA*	allowLoginWithoutMFA ▼

Рисунок 114

5. Нажать кнопку **Сохранить**.

3.2.11.3 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**.

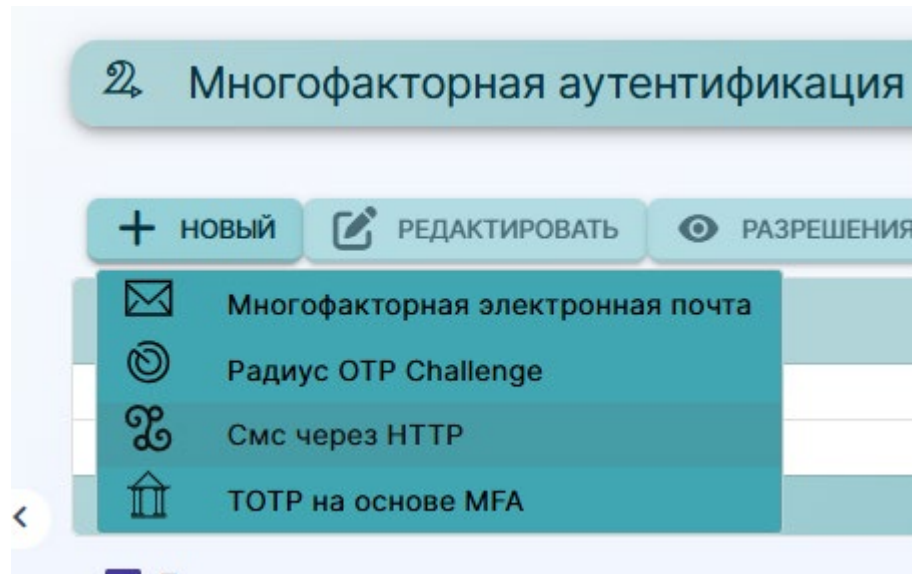


Рисунок 115

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.

Новый аутентиф...  Смс через HTTP

< **ОСНОВНОЙ** HTTP-СЕРВЕР HTTP АУТЕНТИФИКАЦИЯ >

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Кэширование устройства
0

Время в часах для кэширования устройства, чтобы MFA больше не требовалась.
На основе пользователя.

Действительность кода MFA
5

Время в минутах, в течение которого можно использовать код MFA.

Рисунок 116

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`).

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.

Новый аутентиф...  Смс через HTTP

< HTTP АУТЕНТИФИКАЦИЯ HTTP ОТВЕТ КОНФИГУРАЦИ >

Метод аутентификации SMS*

Нет

Пользователь или токен аутентификации SMS

Пользователь или токен для аутентификации по SMS

Пароль аутентификации SMS

Пароль для аутентификации по SMS

Рисунок 117

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.

Новый аутентиф...  Смс через HTTP

< HTTP АУТЕНТИФИКАЦИЯ HTTP ОТВЕТ КОНФИГУРАЦИ >

Регулярное выражение для ответа SMS OK

Регулярное выражение для ответа SMS OK. Если пусто, ответ считается OK, если код статуса равен 200.

Рисунок 118

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.

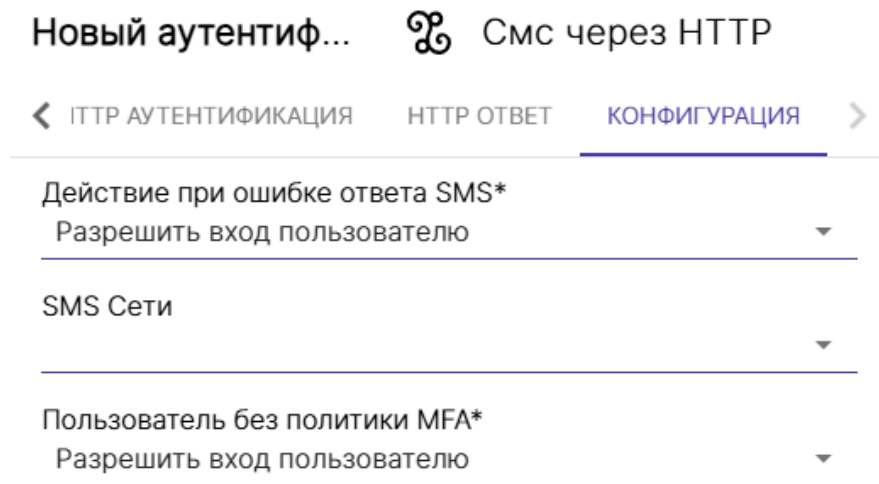


Рисунок 119

3.2.11.4 МФА на основе ТОТР

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 ТОТР, 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.

Перед созданием МФА необходимо убедиться, что в настройках системы включена опция **Включить МФА для клиентов:**

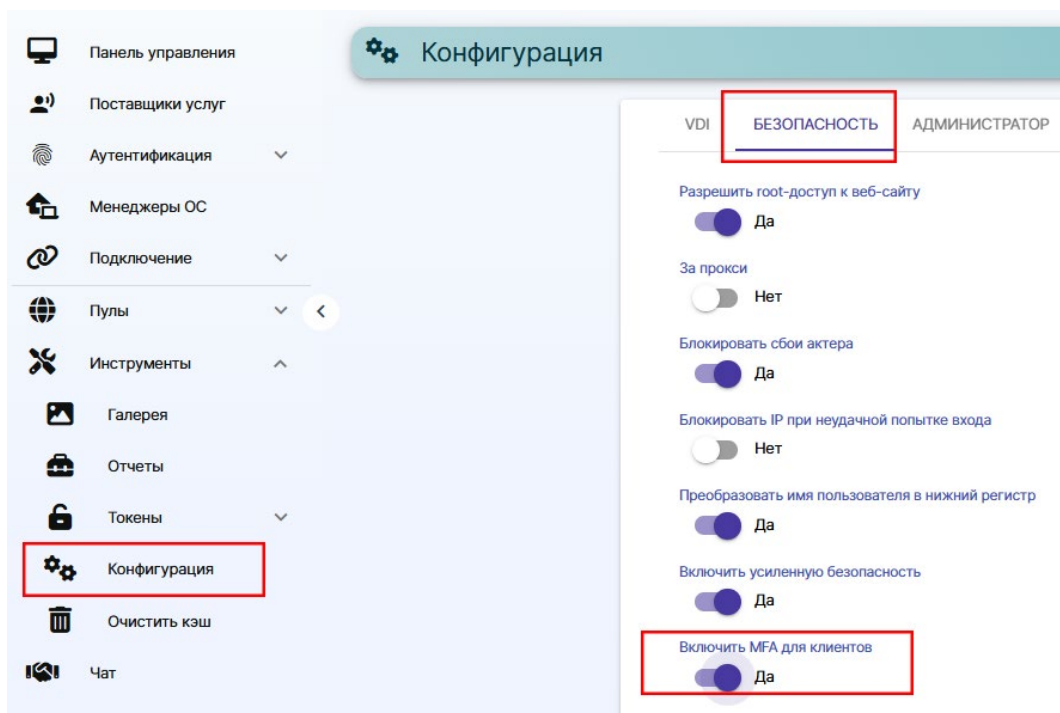


Рисунок 120

Для создания провайдера:

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

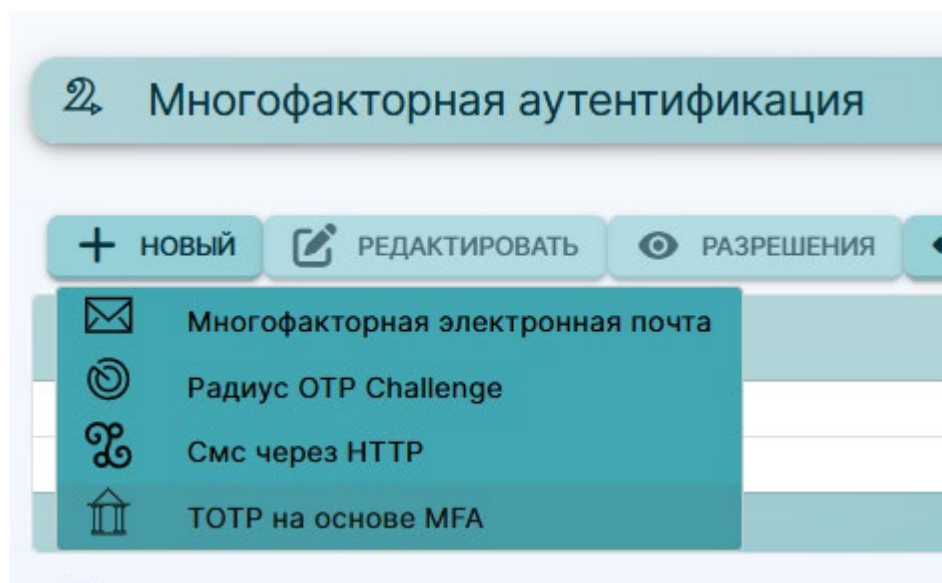


Рисунок 121

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.

Новый аутентиф...

 TOTP на основе MFA

ОСНОВНОЙ

КОНФИГУРАЦИЯ

Тэги

tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Эмитент*

Эмитент для OTP. После создания его нельзя изменить

Кэширование устройства

0

Время в часах для кэширования устройства, чтобы MFA больше не требовалась. На основе пользователя.

Действительность кода MFA

5

Время в минутах, в течение которого можно использовать код MFA.

Рисунок 122

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.

Новый аутентиф...  TOTP на основе MFA

ОСНОВНОЙ КОНФИГУРАЦИЯ

Действительное окно*
1

Количество допустимых кодов до и после текущего

Сети TOTP

Рисунок 123

5. Нажать кнопку **Сохранить**.
6. Перейти в раздел **Аутентификаторы**.
7. Выбрать необходимый аутентификатор, к которому нужно добавить МФА.
8. Нажать кнопку **Редактировать**.
9. В открывшемся окне перейти в раздел **МФА**.
10. Выбрать провайдера МФА.

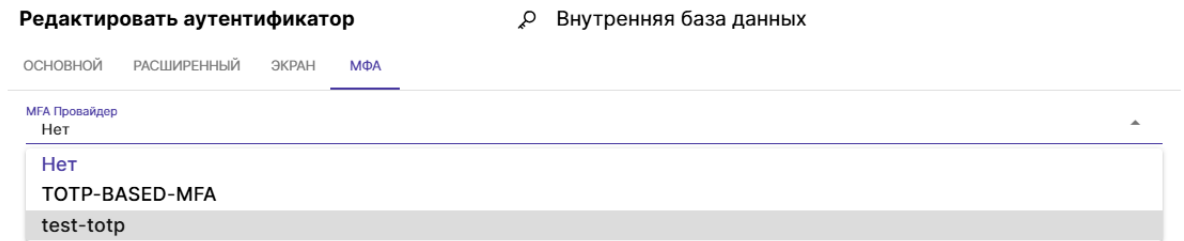


Рисунок 124

3.2.12 Создание групп пользователей

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

(Рисунок 125).

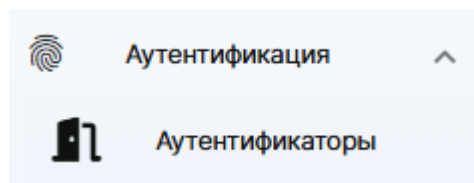


Рисунок 125

2. Выбрать созданный ранее аутентификатор.

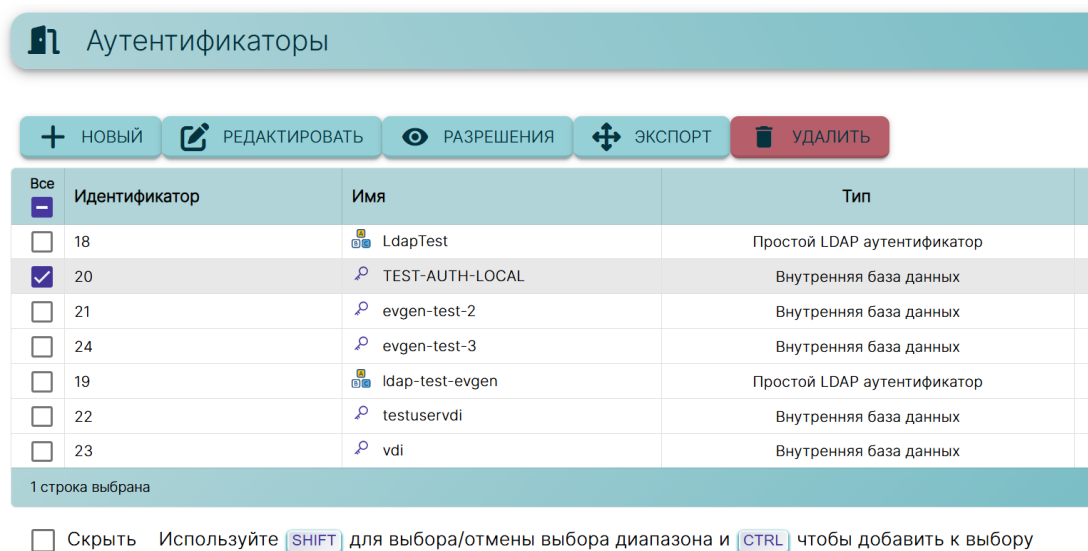


Рисунок 126

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

☒	13	КОПИРОВАТЬ	db-local
☐	12	РЕДАКТИРОВАТЬ	evgen-test
☐	7	ПОДРОБНЕЕ	ldap
☐	5	РАЗРЕШЕНИЯ	local
☐	8	УДАЛИТЬ	local-DB
☐	9		maax

Рисунок 127

4. Перейти в раздел **Группы**.

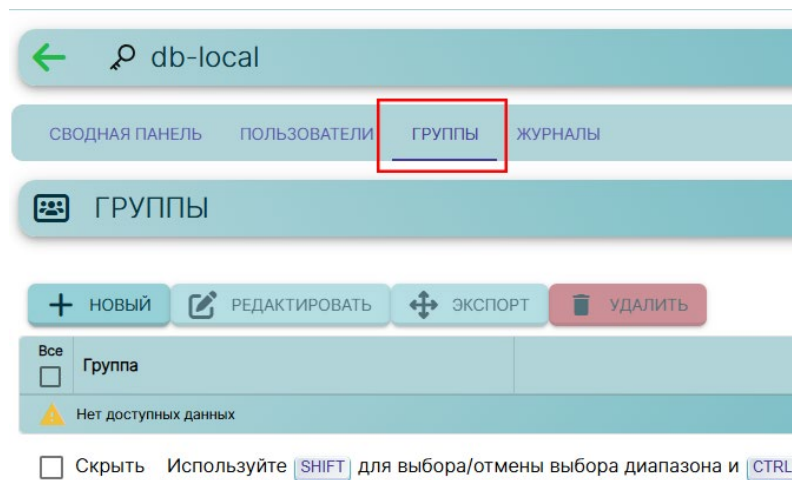


Рисунок 128

5. Нажать кнопку **Новый** -> **Группа**.

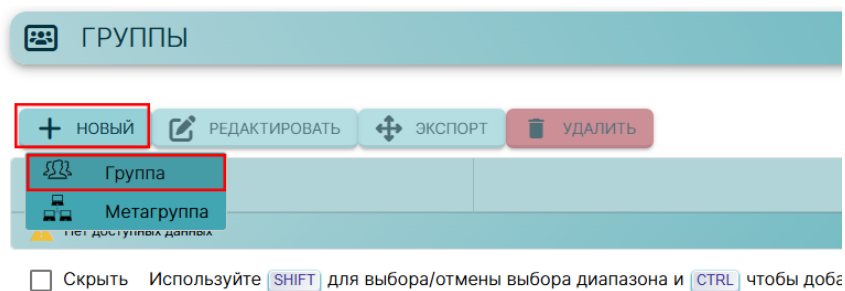


Рисунок 129

6. Откроется окно создания группы.

7. Ввести имя группы, состояние – включено, назначить пулы (опционально).

[Добавить новую группу](#) Группа

Группа
gr1

Добавить новую группу

Комментарии

Комментарии для этого элемента

Состояние
Включено

Пулы
win10_hvs35

[ОТМЕНИТЬ](#) [СОХРАНИТЬ](#)

Рисунок 130

8. Нажать кнопку **Сохранить**.

СОХРАНИТЬ

3.2.13 Создание пользователя с ролью «Сотрудник»

1. Перейти в раздел **Пользователи**.

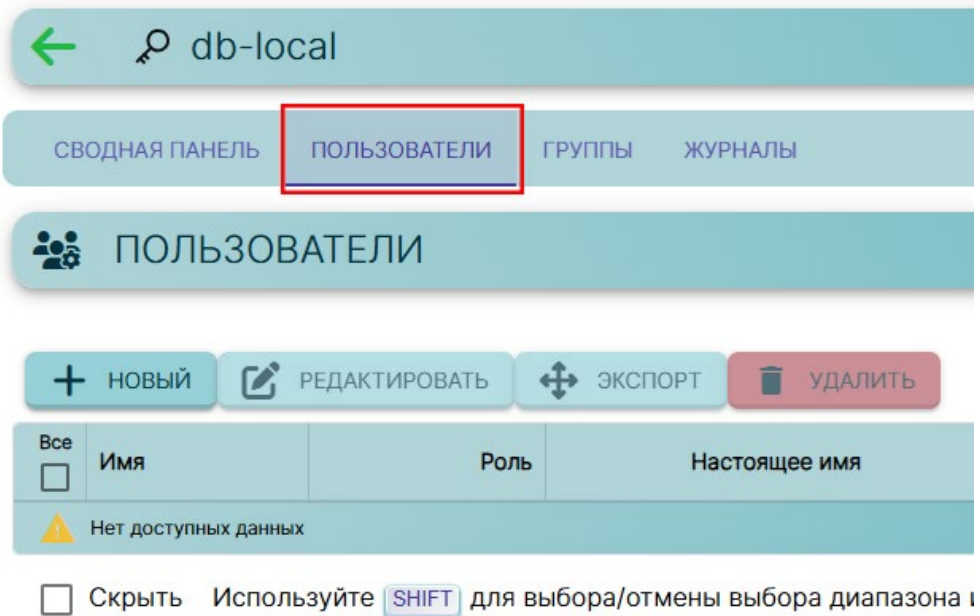


Рисунок 131

2. Нажать кнопку **Новый**.
3. Откроется окно создания нового пользователя. Необходимо заполнить поля:
 - Имя пользователя;
 - Пароль;
 - Выбрать роль для пользователя **Сотрудник**.

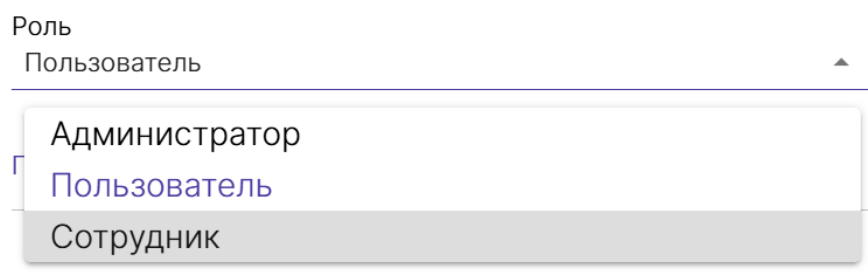


Рисунок 132

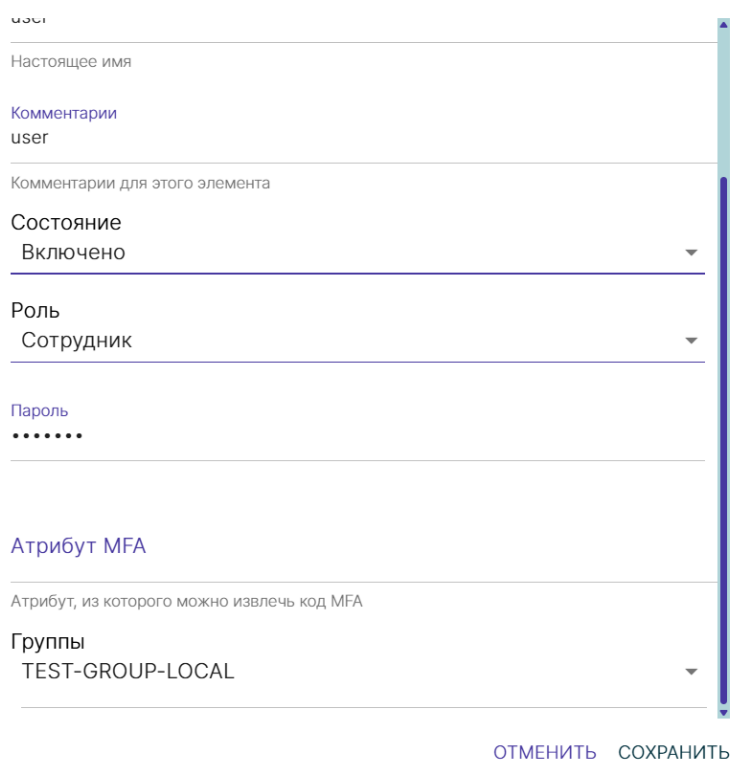
- Выбрать ранее созданную группу;



Рисунок 133

- При необходимости указать атрибут MFA.

Новый пользовате...



Имя
Настоящее имя
user

Комментарии
Комментарии для этого элемента

Состояние
Включено

Роль
Сотрудник

Пароль
.....

Атрибут MFA
Атрибут, из которого можно извлечь код MFA

Группы
TEST-GROUP-LOCAL

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 134

4. Нажать кнопку **Сохранить**.

3.2.14 Создание пользователя с ролью «Администратор»

1. Перейти в раздел **Пользователи**.

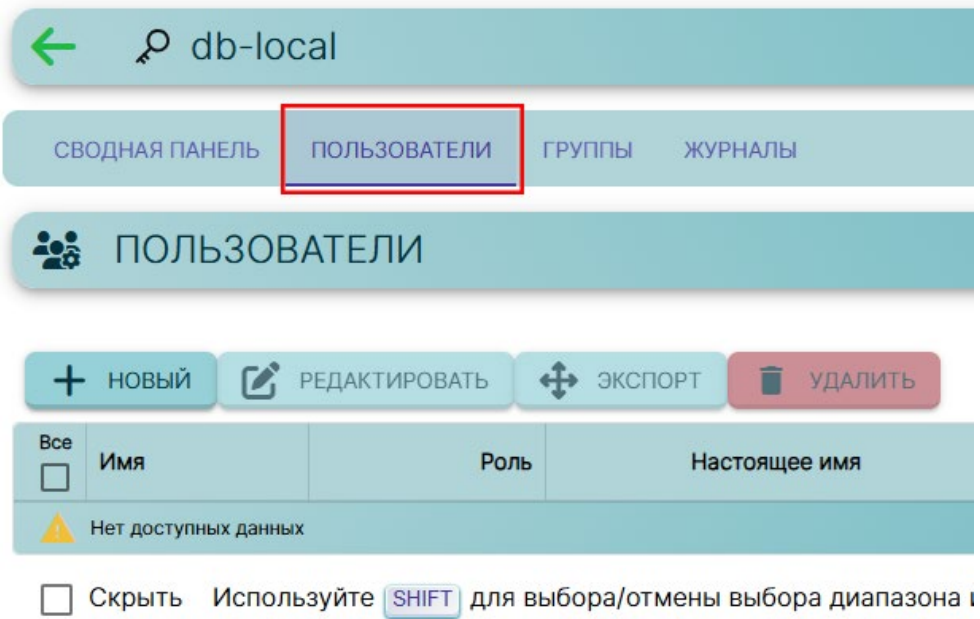


Рисунок 135

2. Нажать кнопку **Новый**.
3. Откроется окно создания нового пользователя. Необходимо заполнить поля:
 - Имя пользователя;
 - Пароль;
 - Выбрать роль для пользователя **Администратор**;



Рисунок 136

- Выбрать ранее созданную группу;



Рисунок 137

- При необходимости указать атрибут MFA.

Новый пользователь

Имя пользователя
username

Имя пользователя

Настоящее имя

Настоящее имя

Комментарии

Комментарии для этого элемента

Состояние

Включено



Роль

Администратор



Пароль*

••••••••

Атрибут MFA

Атрибут, из которого можно извлечь код MFA

Группы

gr1



[ОТМЕНИТЬ](#) [СОХРАНИТЬ](#)

Рисунок 138

4. Нажать кнопку **Сохранить**.

3.2.15 Создание пользователя с ролью «Пользователь»

1. Перейти в раздел **Пользователи**.

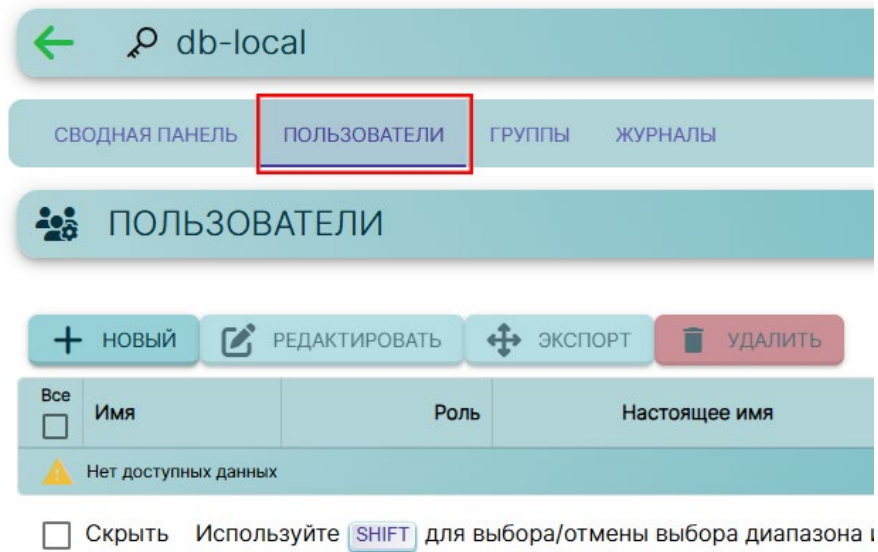


Рисунок 139

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 140

- Выбрать ранее созданную группу;



Рисунок 141

- При необходимости указать атрибут MFA.

Новый пользовате...

user

Настоящее имя

Комментарии
user

Комментарии для этого элемента

Состояние
Включено ▼

Роль
Пользователь ▼

Пароль
.....

Атрибут MFA

Атрибут, из которого можно извлечь код MFA

Группы
TEST-GROUP-LOCAL ▼

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 142

4. Нажать кнопку **Сохранить**.

3.3 Настройка Менеджеров ОС

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

3.3.1 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 143):

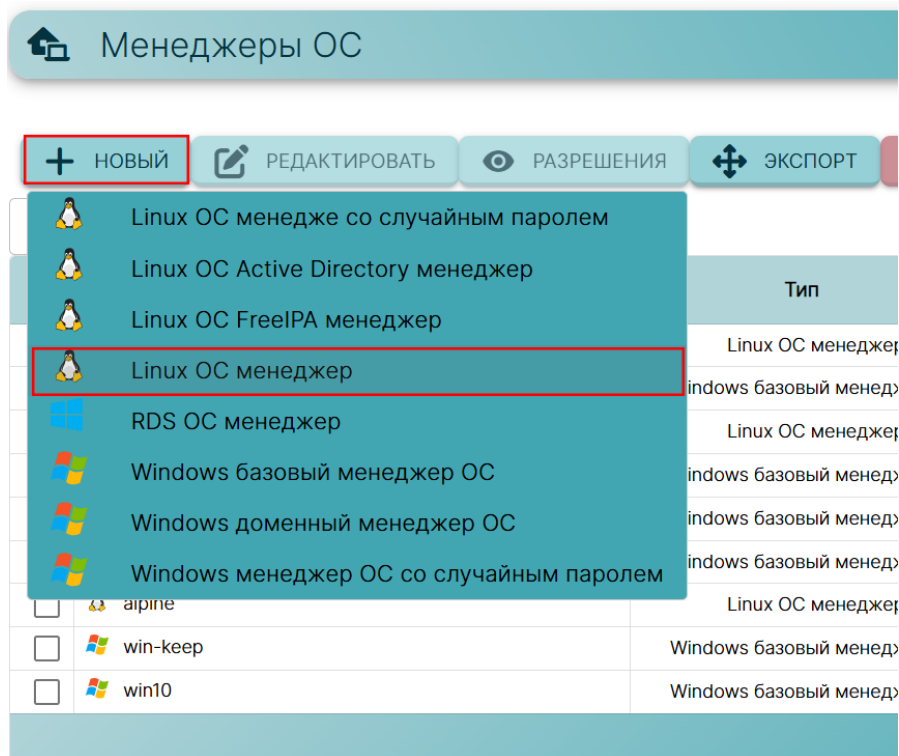


Рисунок 143

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.

3.3.2 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**.

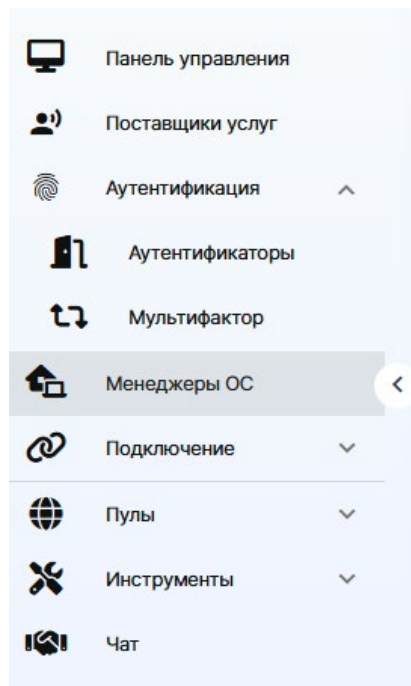
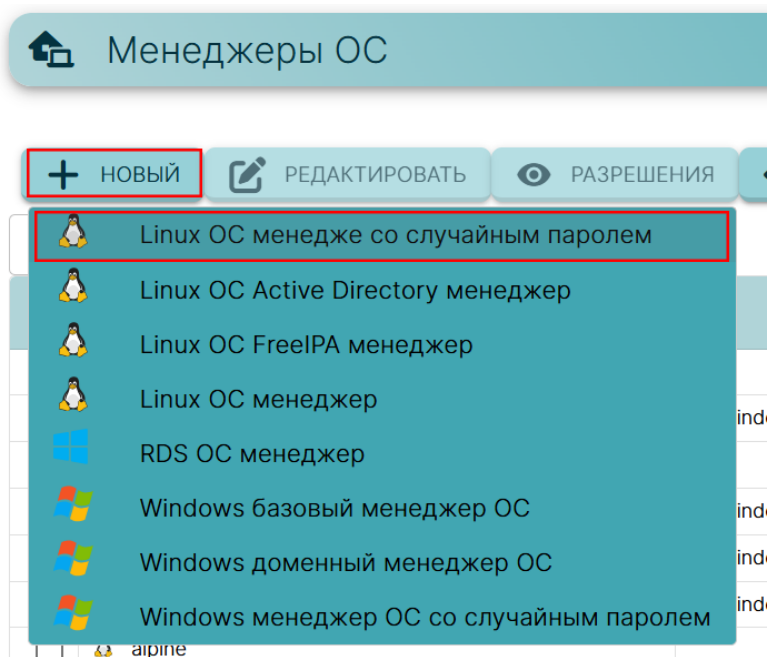


Рисунок 144

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



3. Заполнить поля:

Новый менеджер ...  Linux ОС менедже со с...

ОСНОВНОЙ РАСШИРЕННЫЙ

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Аккаунт

Учетная запись с правами на добавление машин в домен

Действие при выходе из системы
Держать сервис привязанным

Максимальное время простоя*
-1

Максимальное время простоя (в секундах) перед автоматическим закрытием сеанса (<= 0 - означает отсутствие ограничений)

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 145

- **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.

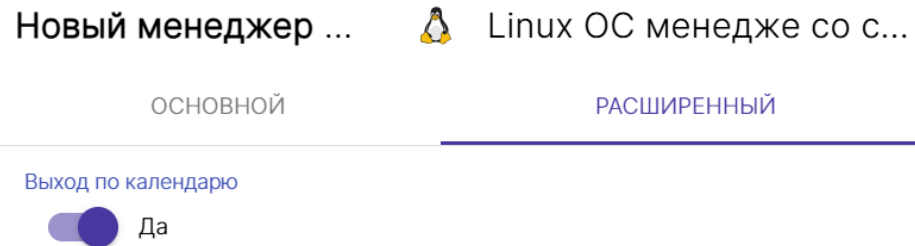


Рисунок 146

3.3.3 RDS

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

Для создания **RDS ОС менеджер** выполнить:

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

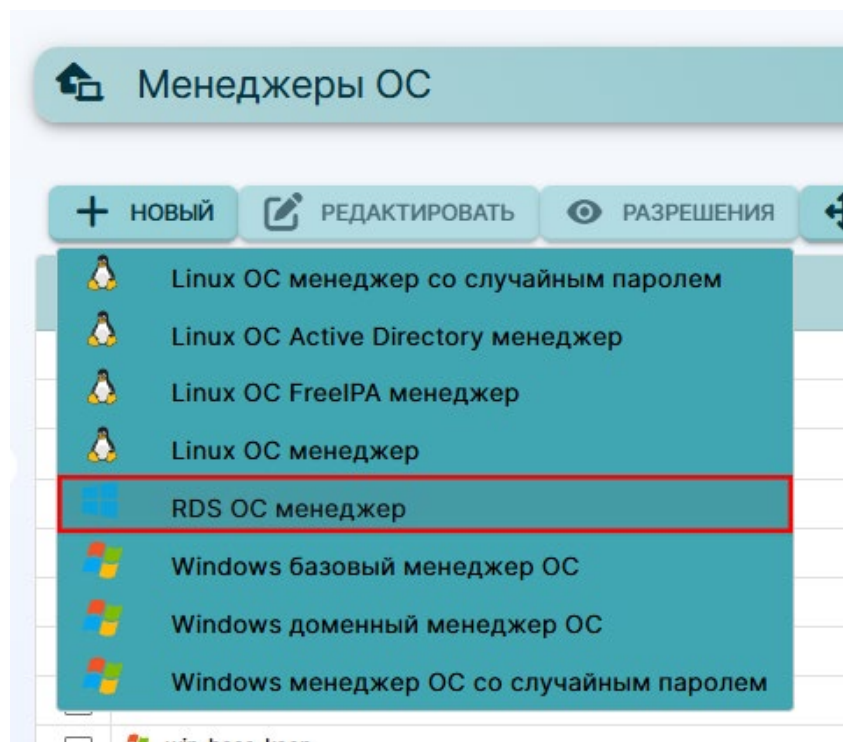


Рисунок 147

3. Заполнить поля:

– **Имя;**

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

Новый менедже...  RDS ОС менеджер

Теги
tags

Имя*
Имя этого элемента

Комментарии
Комментарии для этого элемента

Максимальное время сессии *
24

Максимальная продолжительность сеанса в часах (0 означает отсутствие ограничений). По истечении этого периода сеанс будет завершен

Рисунок 148

4. Нажать кнопку **Сохранить**.

3.3.4 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**.

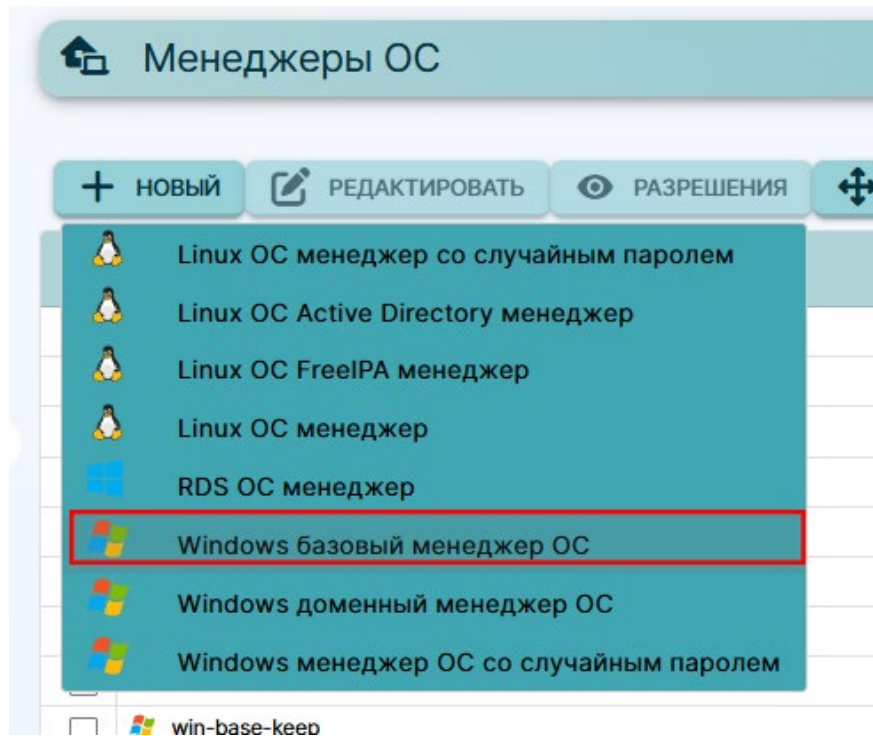


Рисунок 149

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;

Новый менедже... Windows базовый м...

ОСНОВНОЙ РАСШИРЕННЫЙ

Тэги
tags

Имя*
Имя этого элемента

Комментарии
Комментарии для этого элемента

Действие при выходе из системы
Держать сервис привязанным

Максимальное время простоя*
-1

Максимальное время простоя (в секундах) перед автоматическим закрытием сеанса (<= 0 - означает отсутствие ограничений)

Рисунок 150

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

Новый менедже... Windows базовый м...

ОСНОВНОЙ РАСШИРЕННЫЙ

Выход по календарю
☒ Да

Рисунок 151

Нажать кнопку **Сохранить**.

3.3.5 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**.

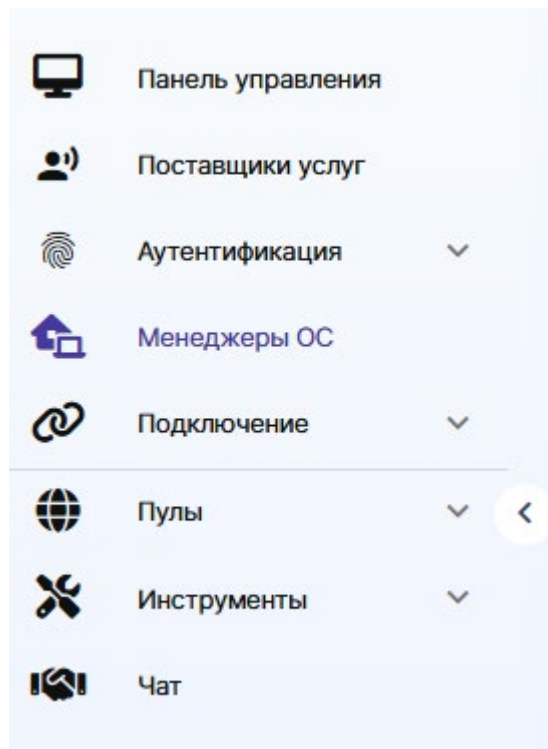


Рисунок 152

2. Нажать кнопку **Новый**.

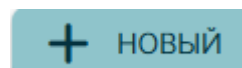


Рисунок 153

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

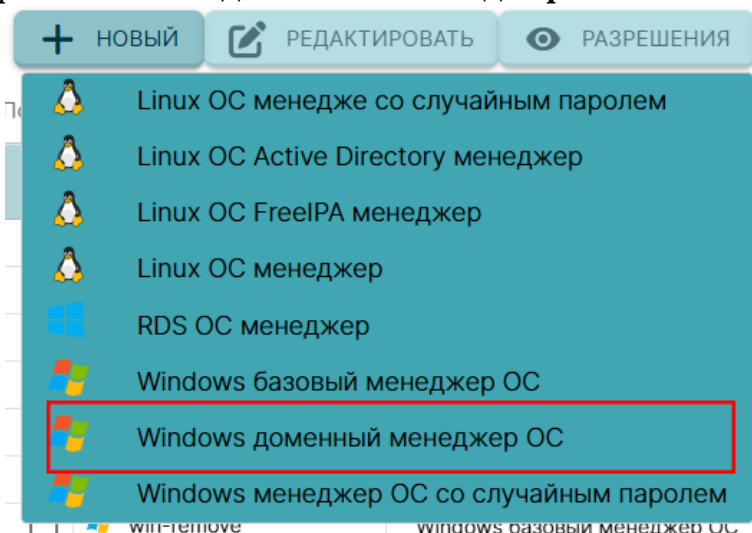


Рисунок 154

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;

Новый менедже... Windows доменный ...

ОСНОВНОЙ РАСШИРЕННЫЙ

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Домен*

Домен для присоединения к машинам (используйте имя FQDN, имя Netbios не поддерживается для большинства операций)

Аккаунт

Учетная запись с правами на добавление машин в домен

Пароль*

Пароль аккаунта

OU

Организационная единица для добавления машин в домен (проверьте перед использованием), например: ou = Мои машины, dc = mydomain, dc = local

Действие при выходе из системы

Держать сервис привязанным

Максимальное время простоя*

-1

Максимальное время простоя (в секундах) перед автоматическим закрытием сеанса (<= 0 - означает отсутствие ограничений)

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 155

– **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 156).

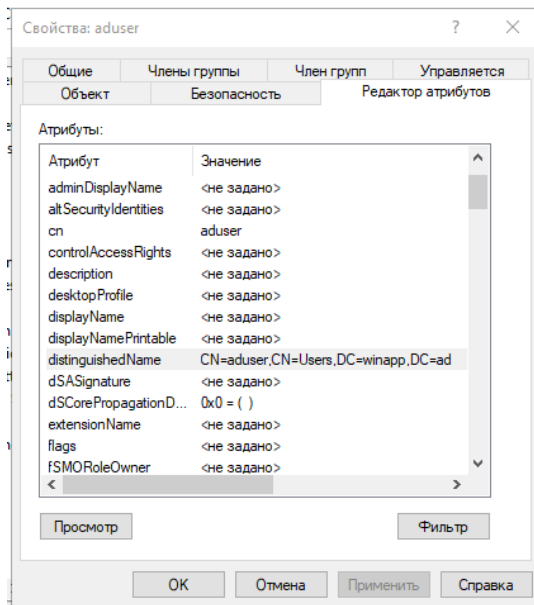


Рисунок 156

5. На вкладке **Расширенный** (Рисунок 157):

Новый менедже...  Windows доменный ...

ОСНОВНОЙ

РАСШИРЕННЫЙ

Группа машин

Группа, в которую добавляются машины при создании. Если пусто, группа не будет использоваться.

Убрать машину

☒ Да

Предпочитаемый сервер

В случае нескольких серверов AD, какой из них предпочтительнее

Использовать SSL

☒ Да

Выход по календарю

☒ Да

Рисунок 157

- **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**.

СОХРАНИТЬ

Рисунок 158

3.3.6 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**.

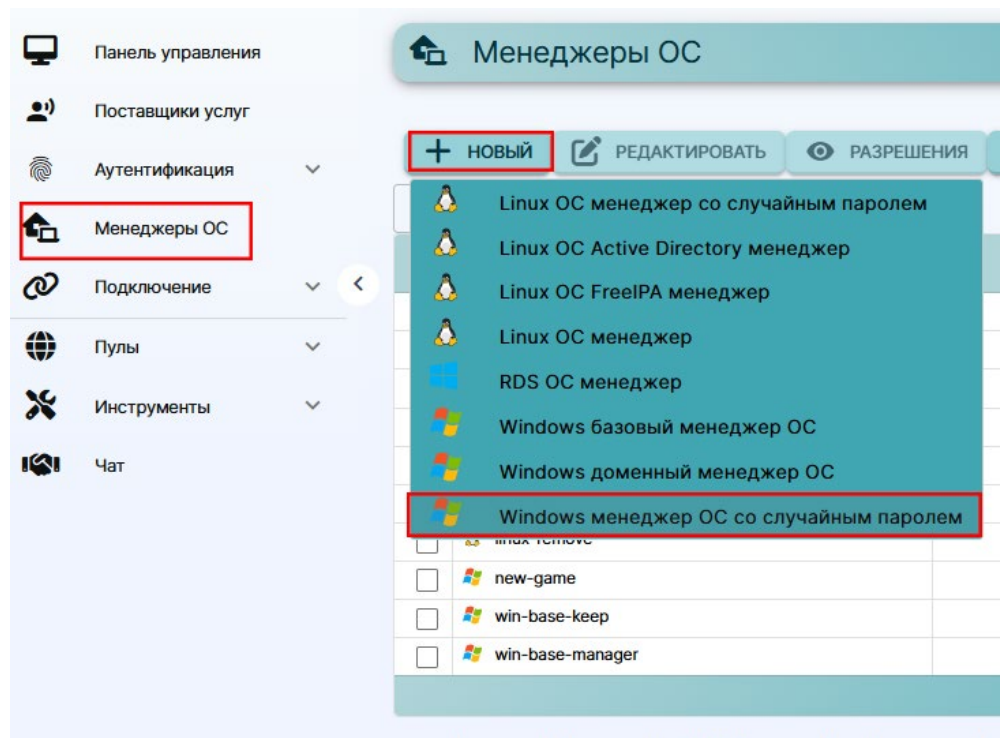


Рисунок 159

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;

Новый менедже...  Windows менеджер...

ОСНОВНОЙ РАСШИРЕННЫЙ

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Аккаунт

Учетная запись с правами на добавление машин в домен

Пароль*

Пароль аккаунта

Действие при выходе из системы
Держать сервис привязанным ▼

Максимальное время простоя*
-1

Максимальное время простоя (в секундах) перед автоматическим закрытием сеанса (< 0 - означает отсутствие ограничений)

Рисунок 160

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

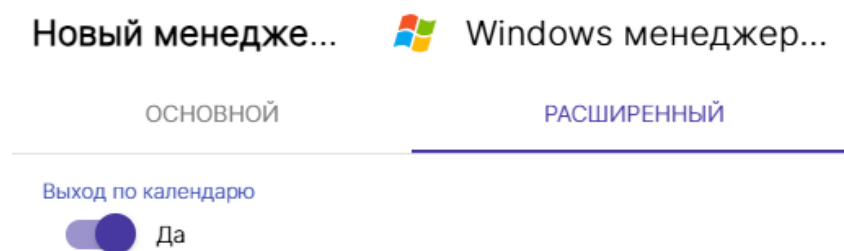


Рисунок 161

6. Нажать кнопку **Сохранить**.

3.4 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 транспортом 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.

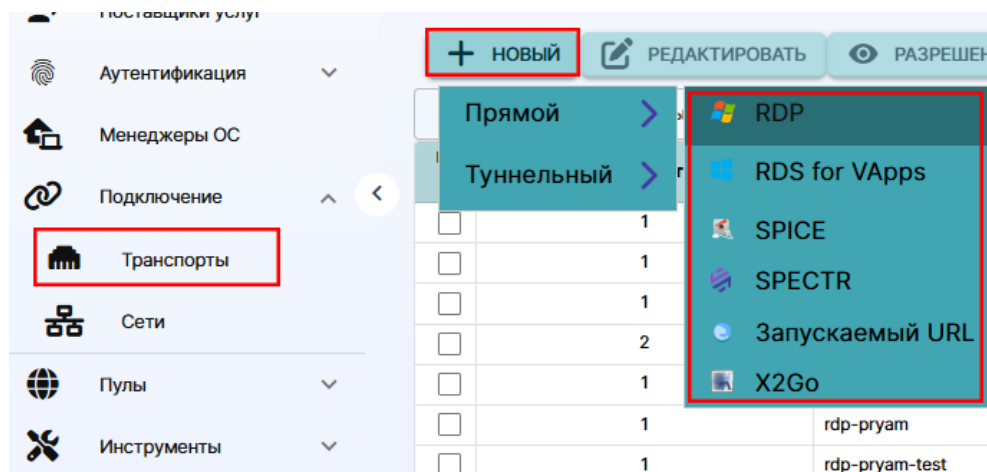


Рисунок 162

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.

3.4.1 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**.

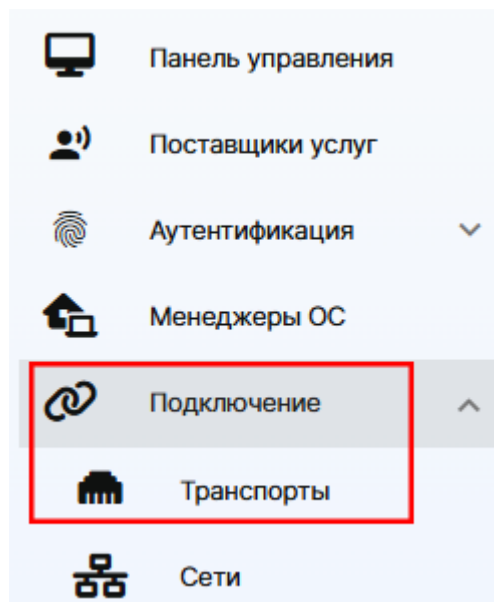


Рисунок 163

2. Нажать кнопку **Новый**.

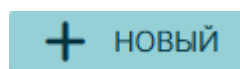


Рисунок 164

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

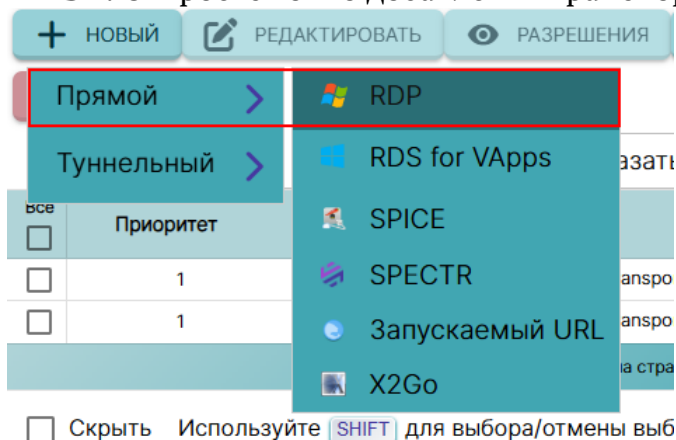


Рисунок 165

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.

< **ОСНОВНОЙ** РАСШИРЕННЫЙ УЧЕТНЫЕ ДАННЫЕ >

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Приоритет*
1

Выбирает приоритет этого элемента (меньшее число означает более высокая приоритет)

Сетевой доступ
☒ Да

Сети

Разрешенные устройства

Пулы услуг

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

- Имя пользователя;
- Пароль;
- Домен.

Новый транспорт  RDP

< ОСНОВНОЙ РАСШИРЕННЫЙ **УЧЕТНЫЕ ДАННЫЕ** ПАРАМЕТРЫ Э! >

Пропустить данные аккаунта
☐ Нет

Имя пользователя
user

Если не пусто, это имя пользователя всегда будет использоваться в качестве учетных данных

Пароль
•••••

Если не пусто, этот пароль всегда будет использоваться в качестве учетных данных

Без домена
☐ Нет

Домен
user/user

Если не пусто, этот домен всегда будет использоваться в качестве учетных данных (используется как 'ДОМЕН/пользователь')

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 166

6. На вкладке **Параметры** возможна настройка необязательных параметров.

Новый транспорт  RDP

← НОВОЙ РАСШИРЕННЫЙ УЧЕТНЫЕ ДАННЫЕ **ПАРАМЕТРЫ** ЭКРАН →

Разрешить смарт-карты

☐ Нет

Разрешить принтеры

☐ Нет

Политика локальных дисков

Не разрешать ничего

Принудительное подключение дисков

Используйте значения, разделенные запятыми, например 'C;D'. Если политика дисков запрещена, это будет проигнорировано

Разрешить серийные порты

☐ Нет

Разрешить буфер обмена

☒ Да

Включить звук

☒ Да

Включить веб-камеру

☐ Нет

Перенаправление USB

Разрешить все

Поддержка Credssp

☒ Да

Порт RDP*

3389

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 167

7. Нажать кнопку **Сохранить**.

8. Созданный транспорт будет отображен в списке.

 Транспорты

+ НОВЫЙ **РЕДАКТИРОВАТЬ** **РАЗРЕШЕНИЯ** **ЭКСПОРТ**

УДАЛИТЬ

Поиск  **показать/скрыть столбцы** 

Все ☐	Приоритет	Имя	Тип	Комментарии
☐	1	rdp	 RDPTransport	
☐	1	spice	 SPICETransport	
☐	1	test-spice	 SPICETransport	

строк на странице 10  строки с 1 по 3, всего 3

☐ Скрыть Используйте **SHIFT** для выбора/отмены выбора диапазона и **CTRL** чтобы добавить к выбору

Рисунок 168

3.4.1 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.

3.4.2 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**.

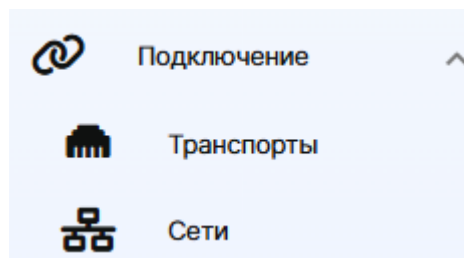


Рисунок 169

2. Нажать кнопку **Новый**.
3. Выбрать Прямой -> SPICE. Откроется окно добавления транспорта.

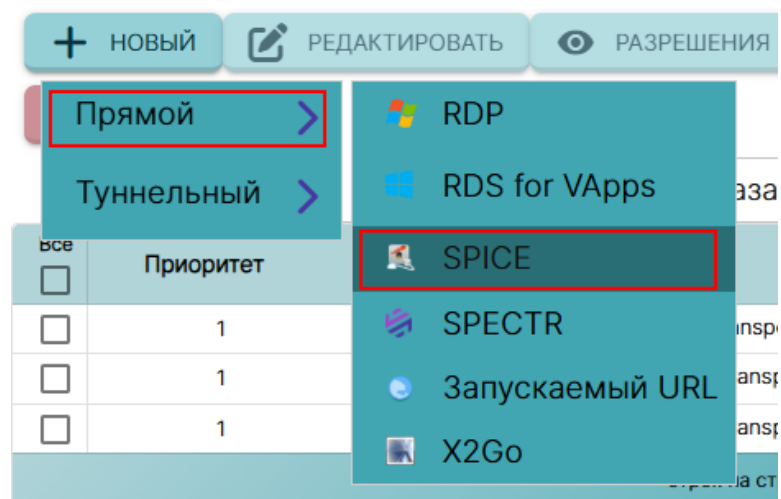


Рисунок 170

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

- **Имя.** Уникальное имя для SPICE-транспорта;
- **Приоритет.** Определяет порядок выбора транспорта, если их несколько. Меньшее число = высший приоритет;

Новый трансп...  SPICE

ОСНОВНОЙ

РАСШИРЕННЫЙ

Тэги

tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Приоритет*

1

Выбирает приоритет этого элемента (меньшее число означает более высокая приоритет)

Сертификат

Сертификат сервера (публичный) можно найти в вашем движке ovirt, вероятно, в /etc/pki/ovirt-engine/certs/ca.der (используйте содержимое этого файла).

Сетевой доступ

Да

Сети

Разрешенные устройства

Пулы услуг

Рисунок 171

5. Нажать кнопку **Сохранить**.

СОХРАНИТЬ

Рисунок 172

6. Транспорт появится в списке.

Транспорты

+

НОВЫЙ

✎

РЕДАКТИРОВАТЬ

👁

РАЗРЕШЕНИЯ

🔗

ЭКСПОРТ

🗑

УДАЛИТЬ

Поиск

показать/скрыть столбцы

↺

Все	Приоритет	Имя	Тип	Комментарии
☐	1	rdp	 RDPTTransport	
☐	1	spice	 SPICETransport	
☐	1	test-spice	 SPICETransport	

строк на странице 10 строки с 1 по 3, всего 3

Рисунок 173

3.4.3 Добавление протокола СПЕКТР

Для добавления протокола СПЕКТР:

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

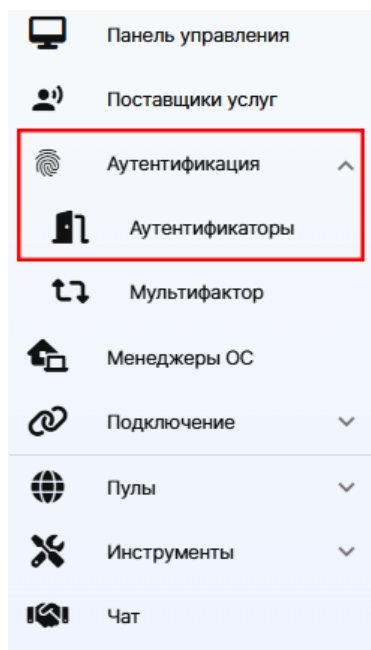


Рисунок 174

2. Нажать кнопку **Новый**.



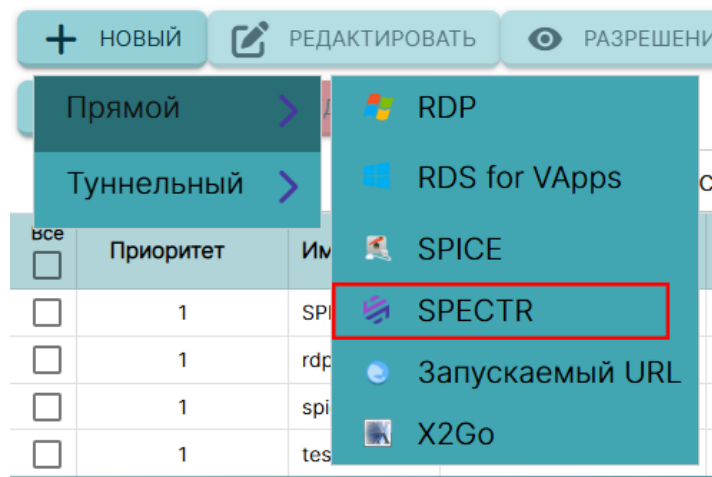
3. Выбрать **Прямой** -> **SPECTR**.

Рисунок 175

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

- **Имя;**
- **Приоритет;**
- **Сети** (опционально);
- **Разрешенные устройства** (опционально);
- **Пулы услуг** (опционально).

Новый трансп... SPECTR

ОСНОВНОЙ РАСШИРЕННЫЙ

Тэги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

Приоритет*

1

Выбирает приоритет этого элемента (меньшее число означает более высокая приоритет)

Сертификат

Сертификат сервера (публичный) можно найти в вашем движке ovirt, вероятно, в /etc/pki/ovirt-engine/certs/ca.der (используйте содержимое этого файла).

Сетевой доступ

☒ Да

Сети

Разрешенные устройства

Пулы услуг

Рисунок 176

5. Нажать кнопку **Сохранить**.

СОХРАНИТЬ

Рисунок 177

6. Транспорт появится в списке.

Все	Приоритет	Имя	Тип	Комментарии
☐	1	SPECTR	Spectr	
☐	1	rdp	RDPTTransport	
☐	1	spice	SPICETransport	
☐	1	test-spice	SPICETransport	

строк на странице 10 строки с 1 по 4, всего 4

Рисунок 178

3.4.4 X2Go (прямой)

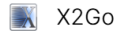
Транспорт **X2Go** (прямой) позволяет пользователям получать доступ к виртуальным рабочим столам Linux с помощью программного обеспечения **X2Go**.

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 179):

Новый транспорт

[ОСНОВНОЙ](#) [УЧЕТНЫЕ ДАННЫЕ](#) [ПАРАМЕТРЫ](#) [РАСШИРЕННЫЙ](#)[Тэги](#)
tags[Имя*](#)

Имя этого элемента

[Комментарии](#)

Комментарии для этого элемента

[Приоритет*](#)
1

Выбирает приоритет этого элемента (меньшее число означает более высокий приоритет)

[Сетевой доступ](#)☒ Да

Сети

Разрешенные устройства

Пулы услуг

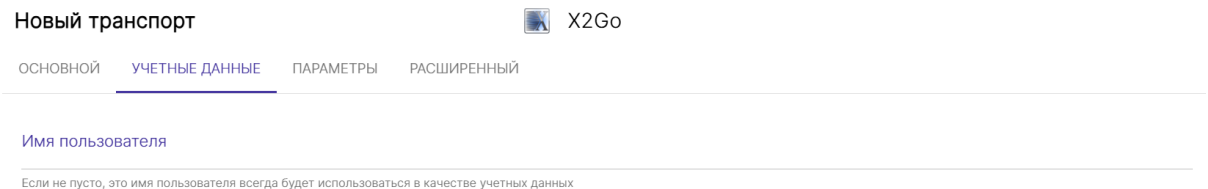
Рисунок 179

- **Имя:** Имя транспорта.
- **Приоритет:** приоритет, который будет иметь транспорт. Чем ниже этот приоритет, тем выше он будет отображаться в списке доступных транспортных средств для службы. Транспорт с наименьшим приоритетом будет использоваться по умолчанию при нажатии на изображение службы.
- **Сетевой доступ:** разрешает или запрещает доступ пользователя к службе в зависимости от сети, из которой осуществляется доступ, и сети, указанной в 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 180):

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



Новый транспорт X2Go

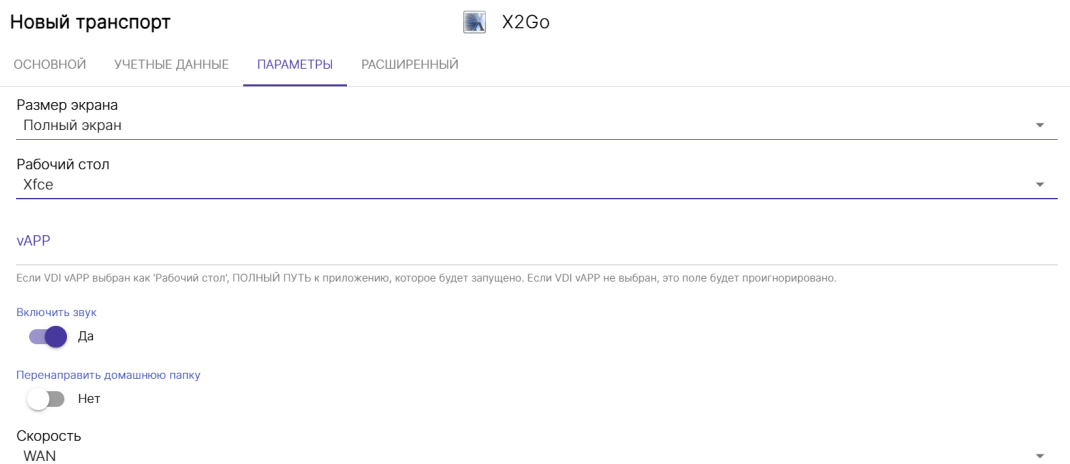
ОСНОВНОЙ **УЧЕТНЫЕ ДАННЫЕ** ПАРАМЕТРЫ РАСШИРЕННЫЙ

Имя пользователя

Если не пусто, это имя пользователя всегда будет использоваться в качестве учетных данных

Рисунок 180

4. В разделе **Параметры** (Рисунок 181):



Новый транспорт X2Go

ОСНОВНОЙ УЧЕТНЫЕ ДАННЫЕ **ПАРАМЕТРЫ** РАСШИРЕННЫЙ

Размер экрана
Полный экран

Рабочий стол
Xfce

vAPP

Если VDI vAPP выбран как 'Рабочий стол', ПОЛНЫЙ ПУТЬ к приложению, которое будет запущено. Если VDI vAPP не выбран, это поле будет проигнорировано.

Включить звук
☒ Да

Перенаправить домашнюю папку
☐ Нет

Скорость
WAN

Рисунок 181

- **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 182):

- **Звук:** Выбор типа звукового сервера.
- **Клавиатура:** Язык клавиатуры.

Новый транспорт X2Go

ОСНОВНОЙ УЧЕТНЫЕ ДАННЫЕ ПАРАМЕТРЫ **РАСШИРЕННЫЙ**

Звук
Pulse

Клавиатура

Раскладка клавиатуры (es, us, fr, ...). Пустое значение означает автоматическое определение.

Упаковать
16m-jpeg

Формат упаковки. Меняйте с осторожностью!

Качество*
6

Значение качества, используемое в некоторых форматах упаковки.

Метка

Метка транспорта Metapool (используется только в группировке транспортов Metapool)

Рисунок 182

6. Нажать кнопку **Сохранить**.

3.4.1 Установка ограничений на авторизацию с устройства доступа пользователя

Для установки запрета на авторизацию с устройства пользователя необходимо:

1. Выбрать созданный ранее транспорт.

 **Транспорты**

 **НОВЫЙ**
 **РЕДАКТИРОВАТЬ**
 **РАЗРЕШЕНИЯ**
 **ЭКСПОРТ**

 **УДАЛИТЬ**

Поиск  показать/скрыть столбцы  

Все 	Приоритет	Имя	Тип	Комментарии
☐	1	SPECTR	 Spectr	
☒	1	rdp	 RDPTTransport	
☐	1	spice	 SPICETransport	
☐	1	test-spice	 SPICETransport	

1 строка выбрана строк на странице 10  строки с 1 по 4, всего 4

Рисунок 183

- Нажать кнопку **Редактировать**.

 **НОВЫЙ**
 **РЕДАКТИРОВАТЬ**
 **РАЗРЕШЕНИЯ**
 **ЭКСПОРТ**

 **УДАЛИТЬ**

Поиск  показать/скрыть столбцы  

Все 	Приоритет	Имя	Тип	Комментарии
☐	1	SPECTR	 Spectr	
☒	1	rdp	 RDPTTransport	

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

Разрешенные устройства

- Android
- Linux
- Macintosh
- Windows

- Нажать кнопку **Сохранить**.

3.5 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.

3.5.1 Создание пула виртуальных машин Linux

1. Необходимо создать менеджер ОС Linux (см. 3.3).
2. Перейти в раздел **Пулы** -> **Пулы услуг**.

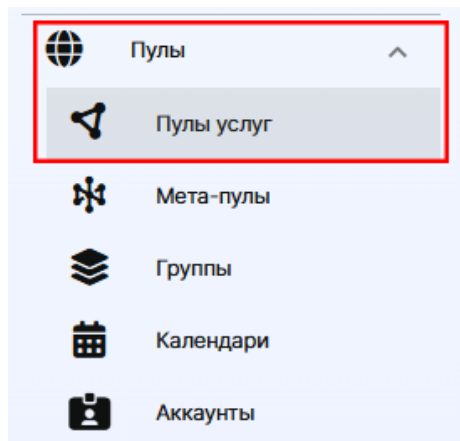


Рисунок 184

3. Нажать кнопку **Новый**.
4. Откроется окно создания пула. На вкладке Основной заполнить поля:
 - Имя;
 - Короткое имя;
 - Базовый сервис (поставщика услуг);

- Менеджер ОС. Выбрать созданный ранее менеджер ОС Linux.

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

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

Новый пул услуг

ОСНОВНОЙ	ЭКРАН	РАСШИРЕННЫЙ	ДОСТУПНОСТЬ
Начальные доступные услуги			
1			
Службы, изначально созданные для этого пула служб			
Сервисы, хранящиеся в кеше			
1			
Службы хранятся в кеше для улучшения назначения пользовательских служб			
Сервисы, хранящиеся в кеше L2			
0			
Службы хранятся в кеше L2 для улучшения назначения пользовательских служб			
Максимальное количество предоставляемых услуг			
1			
maxSrvsTooltip			

Рисунок 185

6. Нажать кнопку **Сохранить**.
7. Нажать на созданный пул правой кнопкой мыши, затем нажать **Подробнее**.

3.5.2 Создание пула виртуальных машин Windows

1. Необходимо создать менеджер ОС Linux (см. 3.3).
2. Перейти в раздел **Пулы** -> **Пулы услуг**.

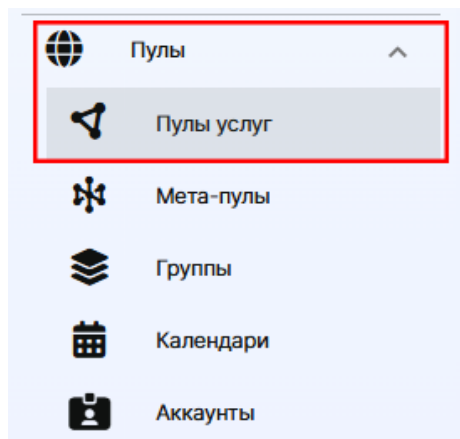


Рисунок 186

3. Нажать кнопку **Новый**.

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

- Имя;
- Короткое имя;
- Базовый сервис (поставщика услуг);
- Менеджер ОС. Выбрать созданный ранее менеджер ОС Windows.

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

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

Новый пул услуг

ОСНОВНОЙ	ЭКРАН	РАСШИРЕННЫЙ	ДОСТУПНОСТЬ
Начальные доступные услуги			
1			
Службы, изначально созданные для этого пула служб			
Сервисы, хранящиеся в кеше			
1			
Службы хранятся в кеше для улучшения назначения пользовательских служб			
Сервисы, хранящиеся в кеше L2			
0			
Службы хранятся в кеше L2 для улучшения назначения пользовательских служб			
Максимальное количество предоставляемых услуг			
1			
maxSrvsTooltip			

Рисунок 187

6. Нажать кнопку **Сохранить**.

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

3.5.3 Создание сессионного гостевого пула рабочих столов

8. Перед созданием гостевого пула необходимо убедиться, что был создан Менеджер ОС с политикой выхода – удаление (см п. 3.3).

9. Перейти в раздел **Пулы** -> **Пулы услуг**.

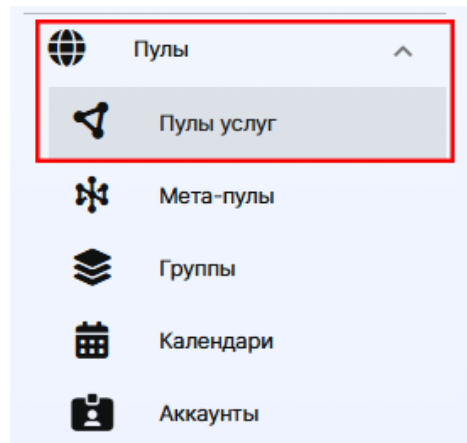


Рисунок 188

10. Нажать кнопку **Новый**.

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

- Имя;
- Короткое имя;
- Базовый сервис (поставщика услуг);
- Менеджер ОС.

Новый пул услуг

ОСНОВНОЙ ЭКРАН РАСШИРЕННЫЙ ДОСТУПНОСТЬ

Тэги
tags

Имя*
test_pool

Имя этого элемента

Короткое имя
Короткое имя для визуализации сервисов пользователя

Комментарии

Базовый сервис
TEST-IRIDIUM\TEST-IRIDIUM-SERVICE-WIN10-B1-L11

Менеджер ОС
TEST-MANAGER-WIN10-DELETE

Опубликовать при создании
☐ Нет

Рисунок 189

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

- Начальные доступные услуги: 1;
- Сервисы, хранящиеся в кеше: 1;
- Сервисы, хранящиеся в кеше L2: 0;

- Максимальное количество предоставляемые услуг:

Новый пул услуг

ОСНОВНОЙ	ЭКРАН	РАСШИРЕННЫЙ	ДОСТУПНОСТЬ
Начальные доступные услуги			
1			
Службы, изначально созданные для этого пула служб			
Сервисы, хранящиеся в кеше			
1			
Службы хранятся в кеше для улучшения назначения пользовательских служб			
Сервисы, хранящиеся в кеше L2			
0			
Службы хранятся в кеше L2 для улучшения назначения пользовательских служб			
Максимальное количество предоставляемых услуг			
1			
maxSrvsTooltip			

Рисунок 190

13. Нажать кнопку **Сохранить**.

14. После сохранения пул будет отображен в списке.

Пулы услуг

+ НОВЫЙ РЕДАКТИРОВАТЬ РАЗРЕ

УДАЛИТЬ

Поиск

Все	Имя	Статус	По
☐	wqwqwqwqw	На техническом обслуживании	
☐	win10i_160	На техническом обслуживании	
☐	win10	Активный	
☐	alpine	Активный	

стр

Рисунок 191

3.5.1 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. 3.1.1.2);
- Как минимум 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**.

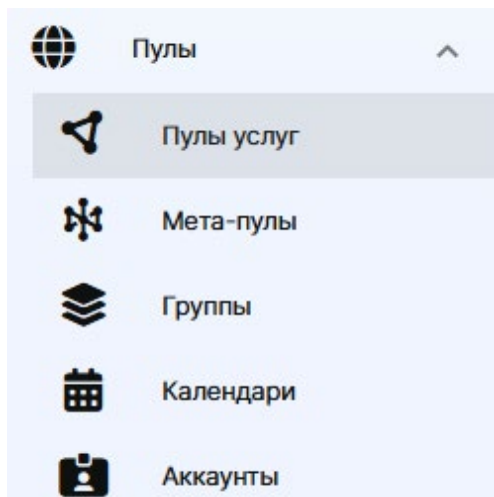


Рисунок 192

3. Нажать кнопку **Новый**.

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

- Имя;
- Базовый сервис (поставщика услуг);
- Менеджер ОС.

Новый пул усл...

< ОСНОВНОЙ ЭКРАН РАСШИРЕННЫЙ ДОСТ >

Теги
tags

Имя*

Имя этого элемента

Короткое имя

Короткое имя для визуализации сервисов пользователя

Комментарии

Базовый сервис

Менеджер ОС

Опубликовать при создании

☒ Да

Рисунок 193

5. Нажать кнопку **Сохранить**.

СОХРАНИТЬ

Рисунок 194

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

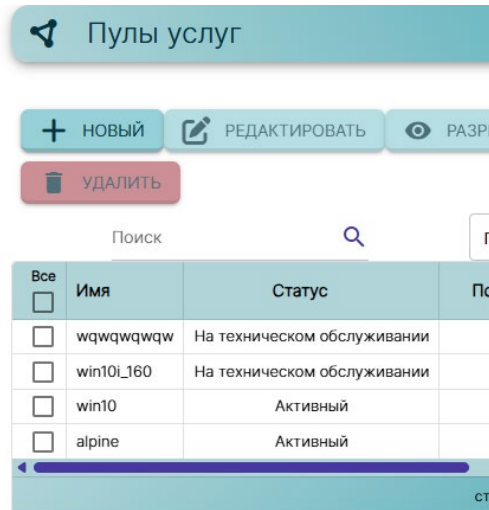


Рисунок 195

3.5.2 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.

3.5.3 Календари

Для создания календаря:

1. Перейти в раздел **Пулы – Календари**.
2. Нажать кнопку **Новый**. (Рисунок 196).

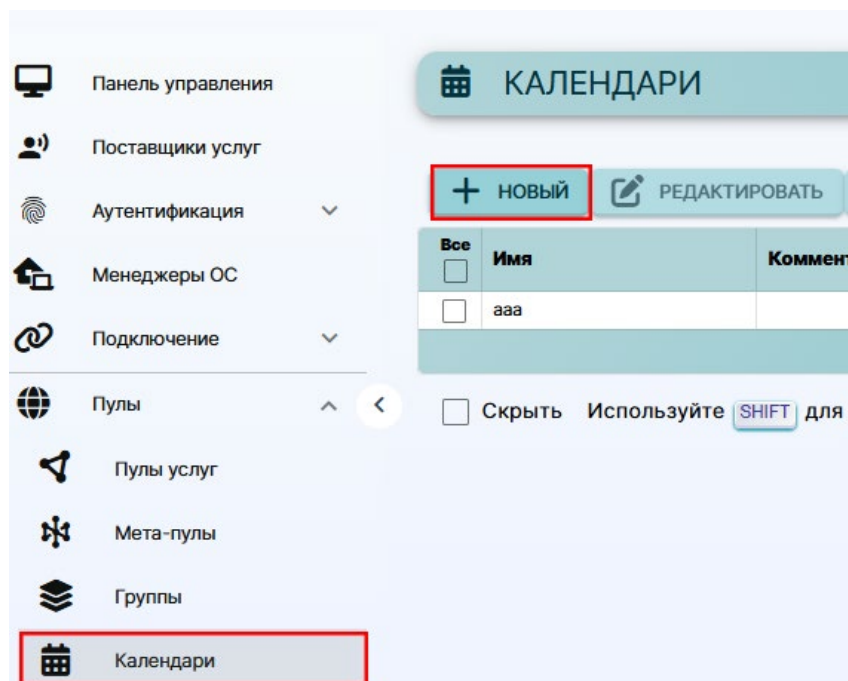


Рисунок 196

3. В открывшемся окне указать описательное имя для идентификации календаря (Рисунок 197).

Новый календарь

Теги
tags

Имя*

Имя этого элемента

Комментарии

Комментарии для этого элемента

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 197

4. Нажать кнопку **Сохранить**. Календарь будет отображен в списке. (Рисунок 198).

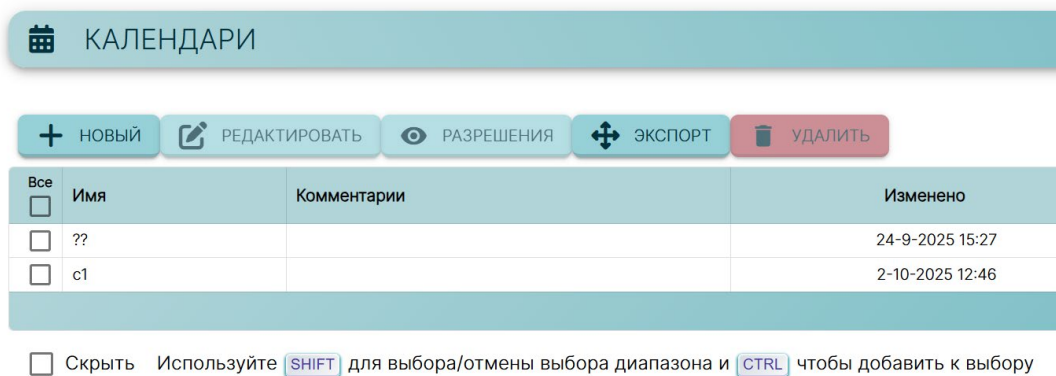


Рисунок 198

3.5.3.1 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**.

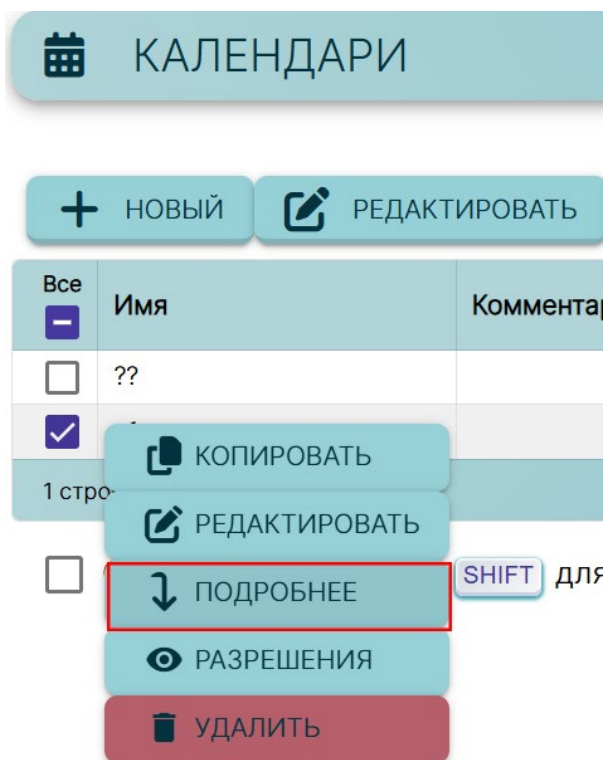


Рисунок 199

2. Нажать **Новый** (Рисунок 200).

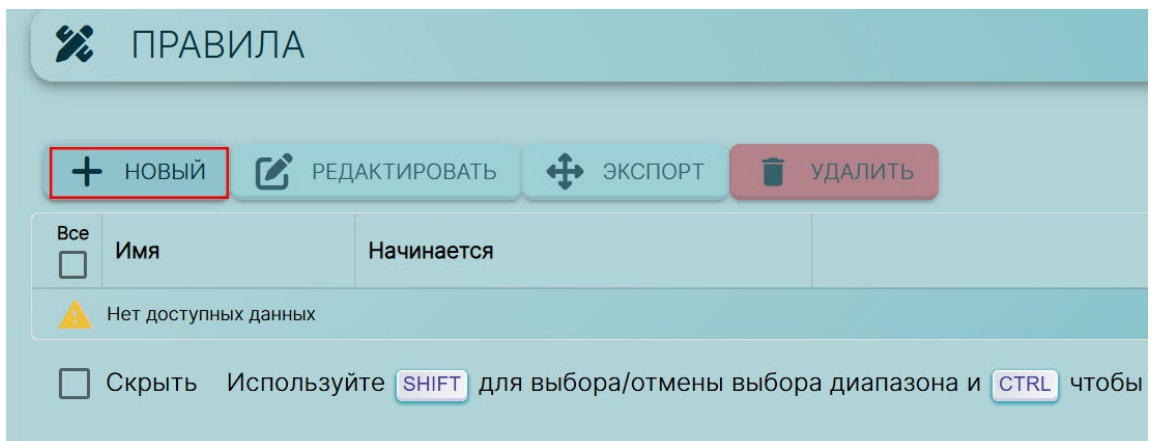


Рисунок 200

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.

Новое правило

Имя*

Комментарии

Событие

Время начала
13:00

Продолжительность
0

Единицы длительности
Минуты

Повторение

Дата начала
2.10.2025

Повторять до даты

Частота
Ежедневно

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 201

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

3.5.3.2 *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.

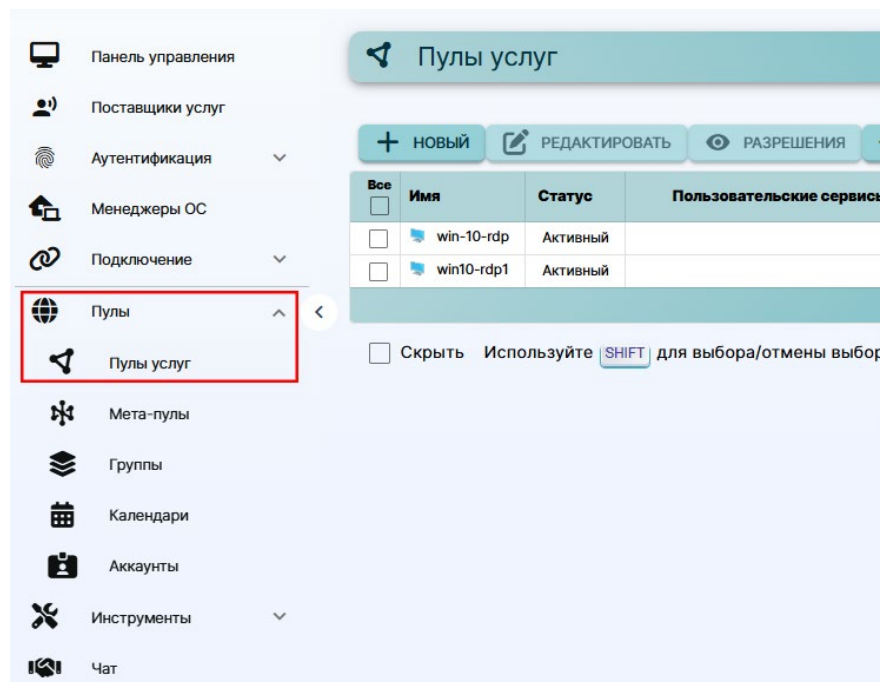


Рисунок 202

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

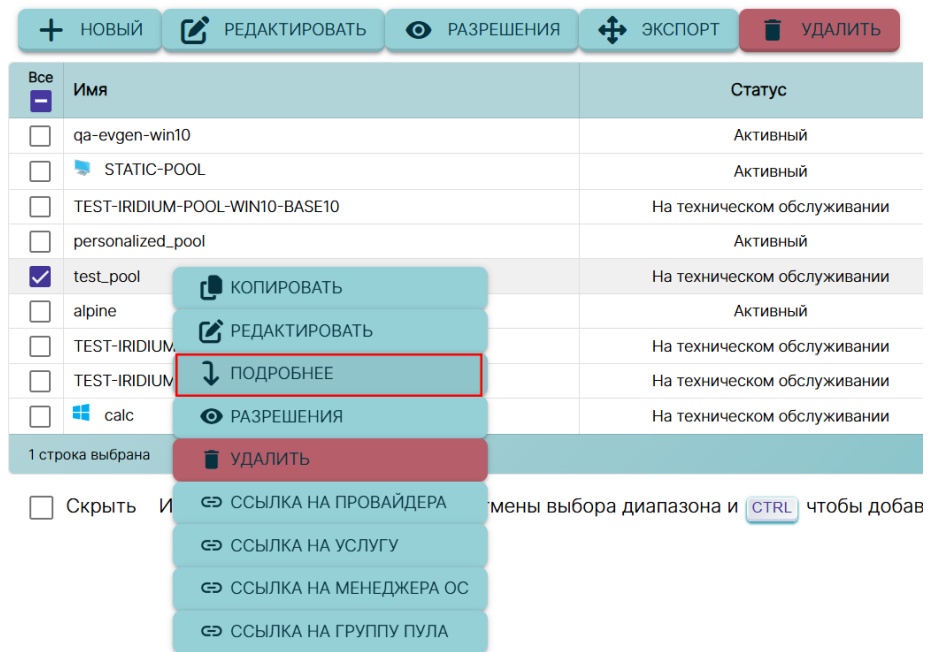


Рисунок 203

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

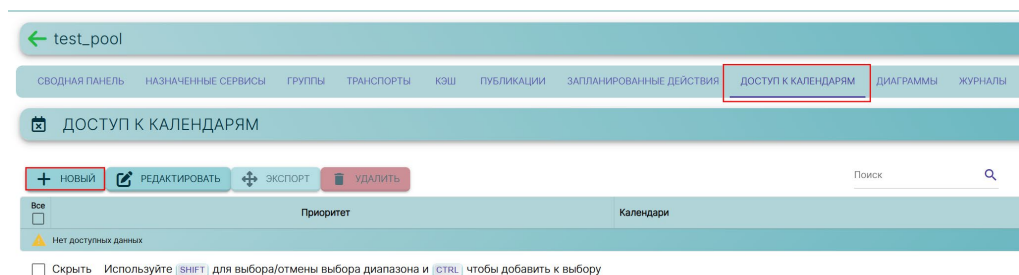


Рисунок 204

5. Указать приоритет доступа, выбрать существующий календарь и отметить действие, которое будет применяться при доступе к сервису (Рисунок 205).

Новое действие

Приоритет
0

Календари
с1

Доступ

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 205

6. Нажать кнопку **Сохранить**. Календарь будет отображен в списке. (Рисунок 206).



Рисунок 206

3.5.3.3 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**.

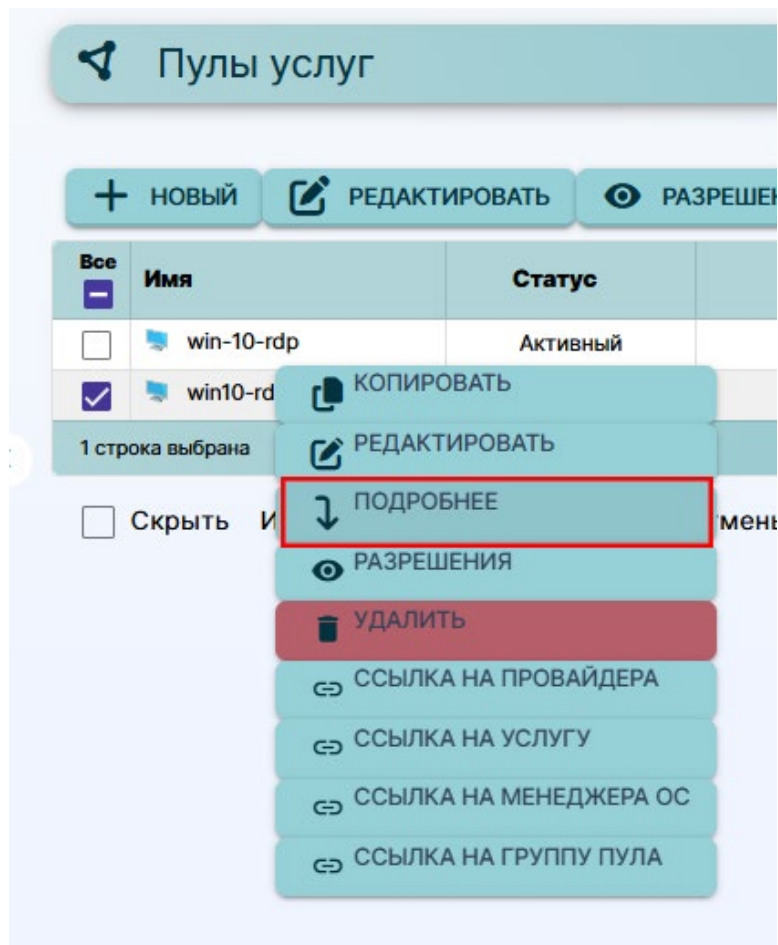


Рисунок 207

3. Перейти на вкладку **Запланированные действия** и нажать **Новый** (Рисунок 208).

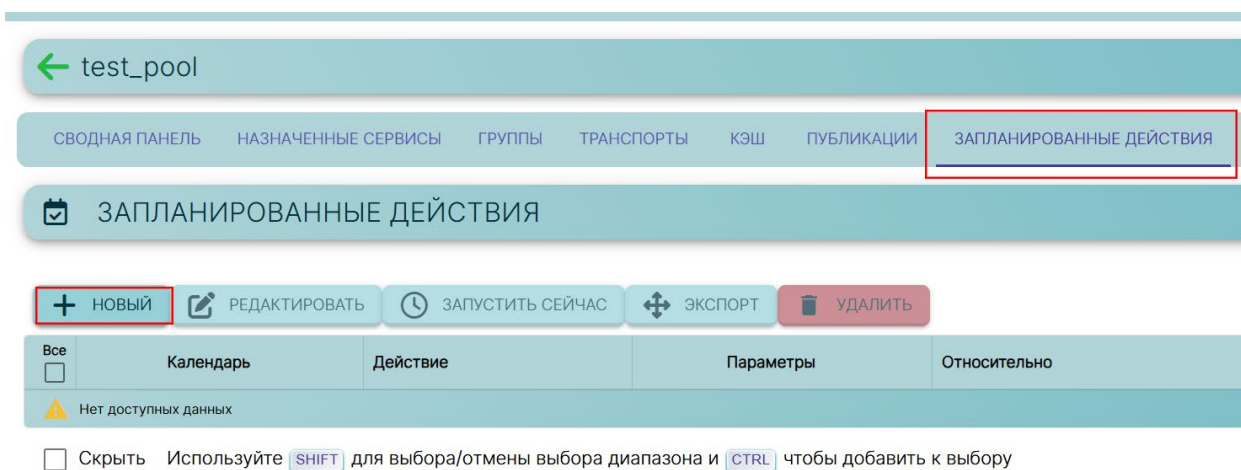


Рисунок 208

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**: удалить 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 служб в пуле служб.
8. После сохранения будет запланированная задача, которая выполняет определенное действие в пуле услуг.

3.5.4 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 209). 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.

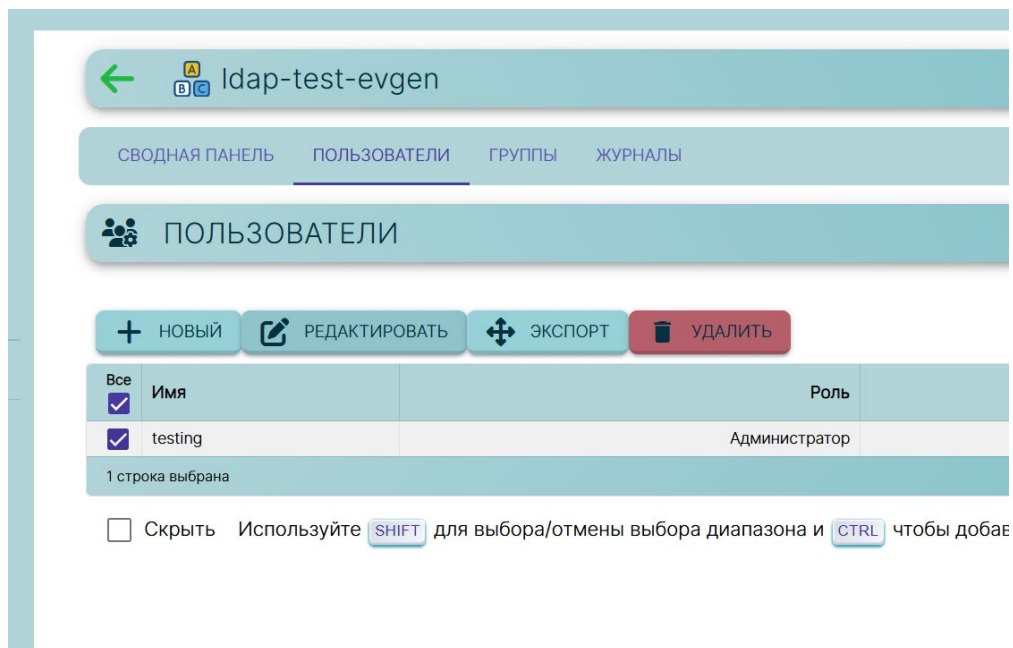


Рисунок 209

3. Далее необходимо перейти в элемент администрирования (Поставщики услуг, пулы услуг). Например, в **Поставщик услуг** (Рисунок 210).

Поставщики услуг		
+ НОВЫЙ РЕДАКТИРОВАТЬ РАЗРЕШЕНИЯ ОБСЛУЖИВАНИЕ ВКЛЧ. ЭКСПОРТ УДАЛИТЬ		
Все	Имя	Тип
☒	ISCSI-TEST-IRIDIUM	Поставщик платформы IridiumSphere
☐	RDS_TEST	Поставщик платформы RDS
☐	TEST-HVS	Поставщик платформы HVS
☐	TEST-IRIDIUM	Поставщик платформы IridiumSphere
☐	TEST-STAT-IP	Поставщик статических IP-машин
☐	dont_tp6	Поставщик платформы IridiumSphere
☐	dont_tp6	Поставщик платформы IridiumSphere
☐	dont_tp6	Поставщик платформы IridiumSphere
☐	hvs35	Поставщик платформы HVS
☐	iridium160	Поставщик платформы IridiumSphere
1 строка выбрана		

Рисунок 210

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 211).

Разрешения | для ISCSI-TEST-I... ×

Пользователи

Группы

Новое разрешение...

Новое разрешение ...

ХОРОШО

Рисунок 211

5. Нужно указать, будет ли этот пользователь или группа иметь доступ для чтения к элементу («Только чтение») или полный доступ («Полный доступ») (Рисунок 212).

Новое разрешение	дляISCSI-TEST-IRIDIUM
Аутентификатор	▼
Имя пользователя	▼
Разрешения	▼
Только для чтения	▼

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 212

6. После применения пользователи, у которых включена опция «Сотрудник», смогут получить доступ к этому элементу администрирования с назначенными разрешениями (Рисунок 213).

Новое разрешение	дляISCSI-TEST-IRIDIUM
Аутентификатор	TEST-AUTH-LOCAL ▼
Имя пользователя	testadmin ▼
Разрешения	Полный доступ ▼

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 213

7. Нажать кнопку **Сохранить**.

4 ПАРАМЕТРЫ КОНФИГУРАЦИИ VDI

4.1 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 214):

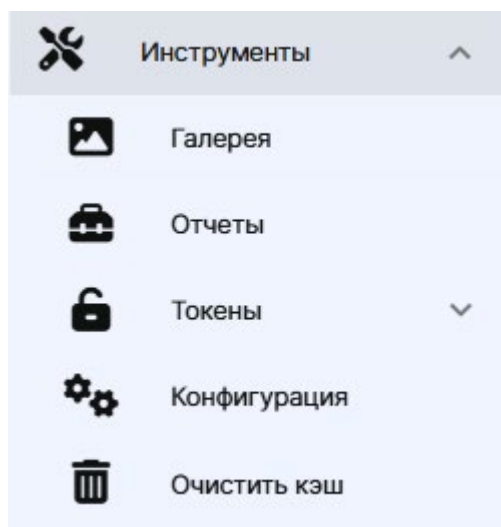


Рисунок 214

4.1.1 Вкладка «VDI»

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

The screenshot shows a configuration window for a VDI. At the top, there are tabs: 'VDI' (selected), 'БЕЗОПАСНОСТЬ', 'АДМИНИСТРАТОР', 'ПОЛЬЗОВАТЕЛЬСКИЙ', and 'NX'. The main content area lists several parameters:

- VDI ID:** 004ca901-5714-5e3c-a520-59a90cd5c5fd
- Служба автозапуска:** A toggle switch is turned off, with the label 'Нет'.
- Задержка проверки кэша:** 19
- Текст отказа в доступе к календарю:** (empty text field)
- Проверить неиспользованную задержку:** 300
- Проверить неиспользованное время:** 631
- Проверка очистки:** 3607
- Потоки отложенных задач:** 4
- Запретить глобальный вход:** A toggle switch is turned off, with the label 'Нет'.

At the bottom right, there are two buttons: 'ВЫХОД' and 'СОХРАНИТЬ'.

Рисунок 215

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 кэша 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 — отключает проверки на максимальное количество одновременно создаваемых (maxPreparingServices) и удаляемых (maxRemovingServices) виртуальных машин. Это "режим администратора", который нужен для массовых операций (например, быстро развернуть 100 рабочих столов), когда нужно проигнорировать стандартные защитные механизмы, чтобы ускорить процесс.

VDI	БЕЗОПАСНОСТЬ	АДМИНИСТРАТОР	ПОЛЬЗОВАТЕЛЬСКИЙ	NX
VDI ID 3ab053c5-1ff1-5e13-8f1a-ed667aeeb3d7				
Служба автозапуска ☐ Нет				
Задержка проверки кэша 19				
Текст отказа в доступе к календарю				
Проверить неиспользованную задержку 300				
Проверить неиспользованное время 631				
Проверка очистки 3607				
Потоки отложенных задач 4				
Запретить глобальный вход ☐ Нет				
Экспериментальные функции ☐ Нет				
Игнорировать ограничения ☒ Да				

Рисунок 216

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 инициализации VDI-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 217

17. **Новое максимальное ограничение.** Этот флаг не устанавливает новый лимит, а изменяет логику подсчета максимального количества сервисов (виртуальных машин) у пользователя. Он переключает систему между двумя методами расчета. Когда флаг выключен (старый метод): Система считает все назначенные пользователю сервисы, включая те, что могут быть в процессе удаления или в состоянии ошибки. Когда флаг включен (новый метод): Система использует более "умный" подсчет, который, как видно из логики в `user_service.py`, игнорирует сервисы в переходных состояниях (например, удаляемые). По умолчанию выключено.
18. **Уведомить о новой публикации.** Флаг, определяющий, будут ли пользователи уведомлены 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 Hhttps..** 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.
23. **Ограничить количество.** По умолчанию: 600.

Эти два параметра работают вместе как единый защитный механизм для изоляции нестабильных сервисов. Они создают правило:

Если сервис (виртуальная машина) выдает `restrainCount` ошибок за последние `restrainTime` секунд, то он временно блокируется.

- `restrainCount`: Порог срабатывания. Сколько раз сервис должен "упасть", чтобы система отреагировала.
- `restrainTime`: Временное окно. За какой период времени система считает эти ошибки.

Зачем используется: Это автоматический "предохранитель". Если сервис превышает этот лимит ошибок, его состояние меняется на "ограниченное" (`restrained`). Это предотвращает "шторм ошибок", когда система бесконечно пытается перезапустить сбойный сервис, и защищает общую стабильность платформы.

- Для `restrainCount`: Порог ошибок
- Для `restrainTime`: Период проверки (в секундах)

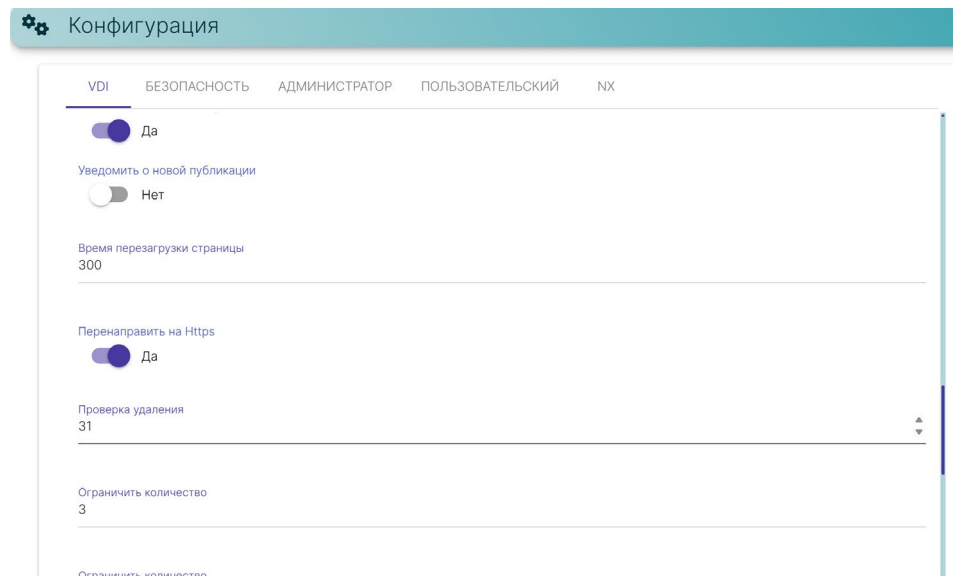


Рисунок 218

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.

VDI

БЕЗОПАСНОСТЬ

АДМИНИСТРАТОР

ПОЛЬЗОВАТЕЛЬСКИЙ

NX

Ограничить количество

600

Потоки планировщика

3

Время истечения сеанса

24

Частота накопления статистики

14400

Максимальное время накопления статистики

7

Длительность статистики

365

Номер очистки службы пользователя

8

ВЫХОД

СОХРАНИТЬ

Рисунок 219

4.1.2 Вкладка «Безопасность»

VDI

БЕЗОПАСНОСТЬ

АДМИНИСТРАТОР

ПОЛЬЗОВАТЕЛЬСКИЙ

NX

Разрешить root-доступ к веб-сайту

Да

За прокси

Нет

Блокировать сброс актера

Да

Блокировать IP при неудачной попытке входа

Нет

Преобразовать имя пользователя в нижний регистр

Да

Включить усиленную безопасность

Да

Включить MFA для клиентов

Нет

Применить режим нулевого доверия

Нет

Эксплоатированный выход

Нет

Удаленное IP-адреса клиента Налог

Нет

Время блокировки входа

20

Мастер-ключ

aba8946cf20f5d10bd2a742c76d3587b

Максимальная продолжительность журналов аудита

365

ВЫХОД

СОХРАНИТЬ

Рисунок 220

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 сбой 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.**

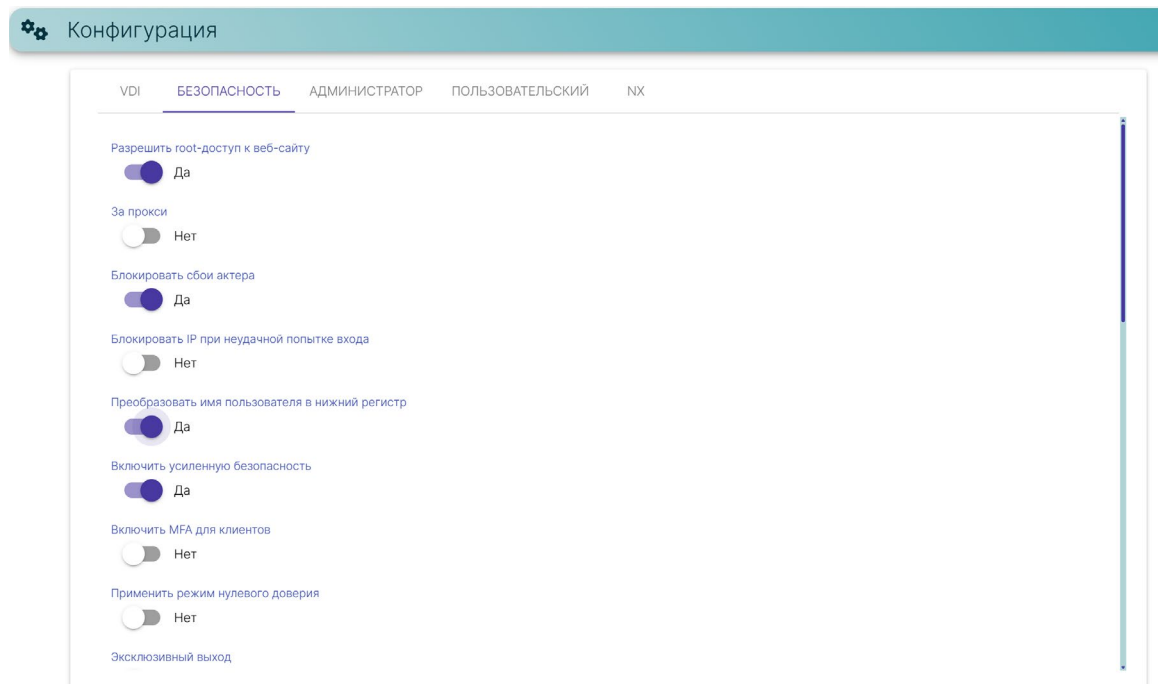


Рисунок 221

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

10. **Доверять IP-адресу от клиента.** Этот флаг определяет, какому источнику информации об IP-адресе клиента будет доверять сервер.

Зачем используется: у сервера есть два способа узнать IP клиента:

1. Из сетевого подключения (надежный способ, используется по умолчанию).
2. От самого клиента (клиентское приложение может само сообщить свой IP).

Этот флаг переключает эту логику:

- Когда флаг выключен (по умолчанию): Сервер доверяет только себе и использует IP-адрес из сетевого подключения.
- Когда флаг включен: Сервер доверяет клиенту и использует тот IP-адрес, который клиент ему сообщил.

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.**

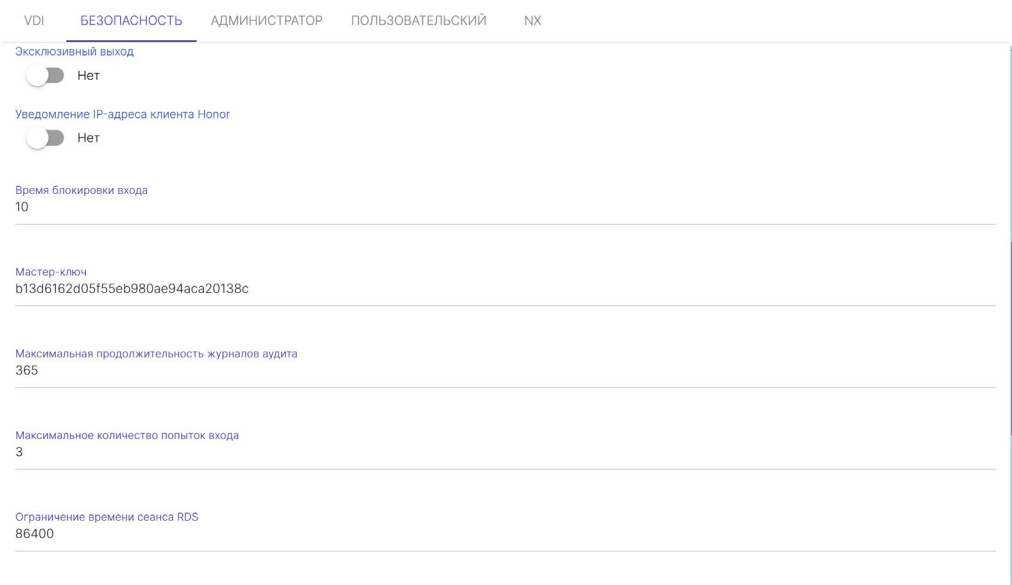
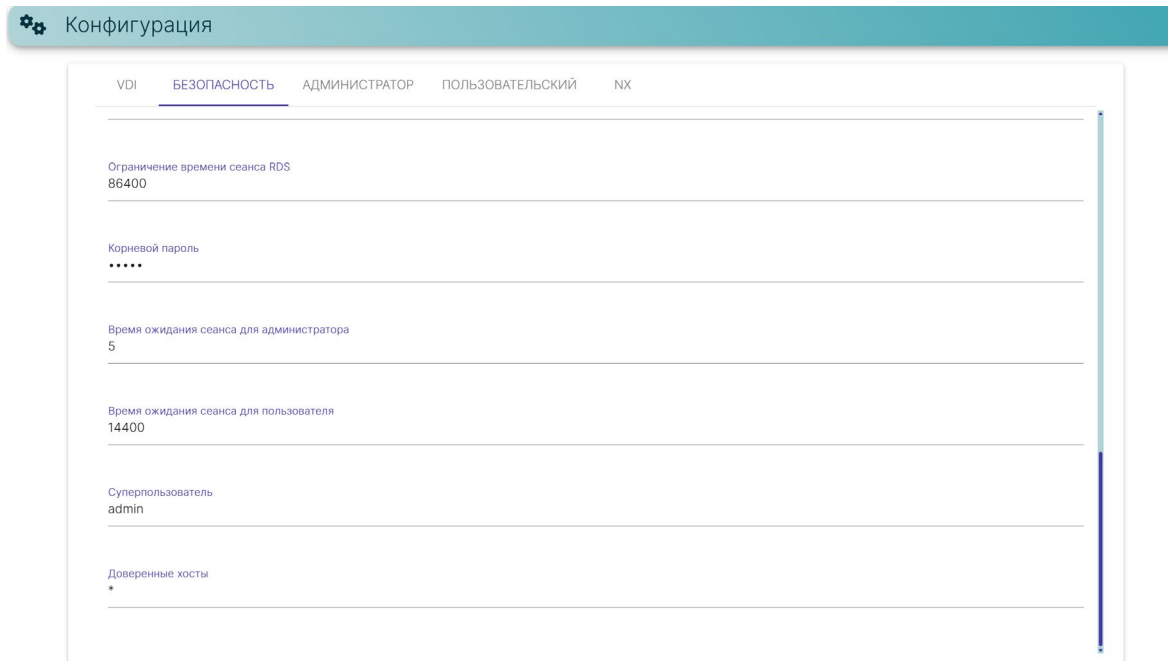


Рисунок 222

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.



Конфигурация

VDI БЕЗОПАСНОСТЬ АДМИНИСТРАТОР ПОЛЬЗОВАТЕЛЬСКИЙ NX

Ограничение времени сеанса RDS
86400

Корневой пароль

Время ожидания сеанса для администратора
5

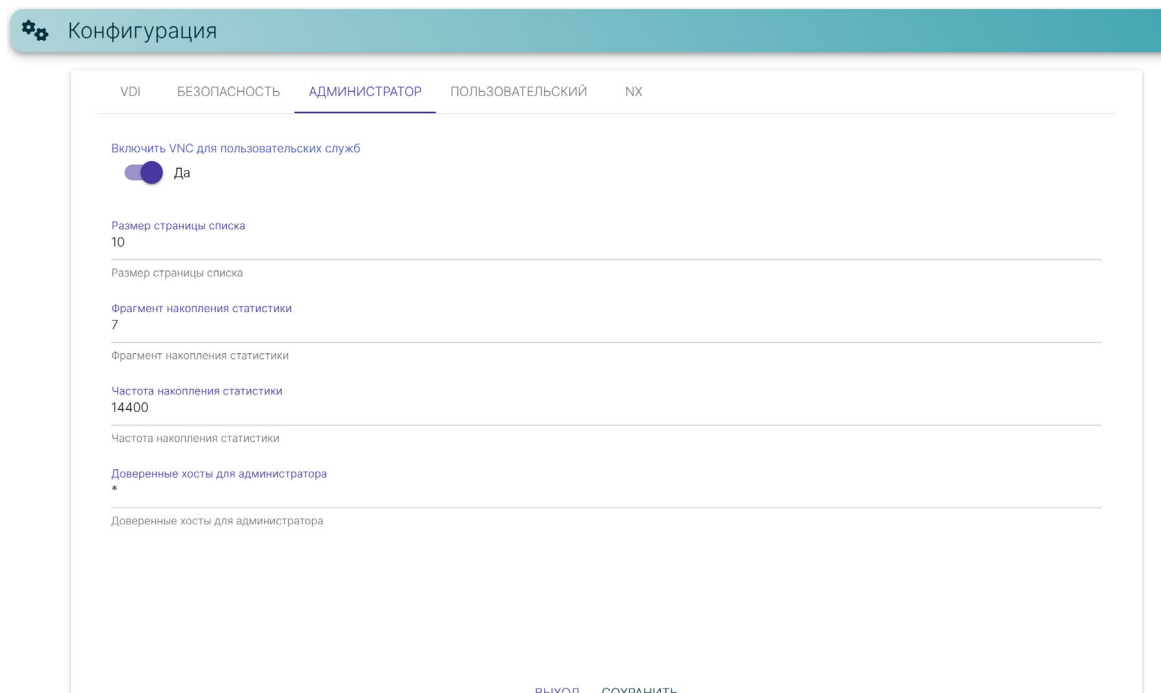
Время ожидания сеанса для пользователя
14400

Суперпользователь
admin

Доверенные хосты
*

Рисунок 223

4.1.3 Вкладка «Администратор»



Конфигурация

VDI БЕЗОПАСНОСТЬ АДМИНИСТРАТОР ПОЛЬЗОВАТЕЛЬСКИЙ NX

Включить VNC для пользовательских служб
☒ Да

Размер страницы списка
10

Размер страницы списка

Фрагмент накопления статистики
7

Фрагмент накопления статистики

Частота накопления статистики
14400

Частота накопления статистики

Доверенные хосты для администратора
*

Доверенные хосты для администратора

ВЫХОД СОХРАНИТЬ

Рисунок 224

- **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.** Задаёт 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.

4.1.4 Вкладка «Пользовательский»

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

Конфигурация

VDI БЕЗОПАСНОСТЬ АДМИНИСТРАТОР **ПОЛЬЗОВАТЕЛЬСКИЙ** НК

Название логотипа
VDI

Название логотипа

Минимальное количество услуг для отображения фильтра
8

Минимальное количество услуг для отображения фильтра

Показать фильтр сверху
☒ Да

Информация об авторских правах на сайте
IRIDIUM-SOFT

Информация об авторских правах на сайте

Ссылка на авторские права сайта
<https://iridium-soft.com/>

Ссылка на авторские права сайта

Информация о сайте

Имя сайта
VDI

Имя сайта

ВЫХОД СОХРАНИТЬ

Рисунок 225

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.

4.1 NX

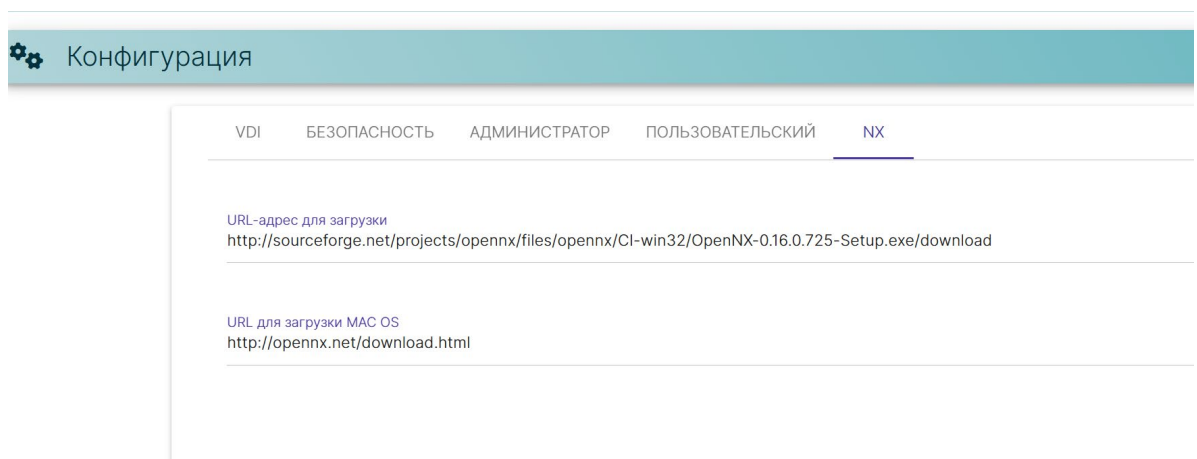


Рисунок 226

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

DownloadUrl: веб-адрес для загрузки программного обеспечения NX.

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

4.2 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 227):

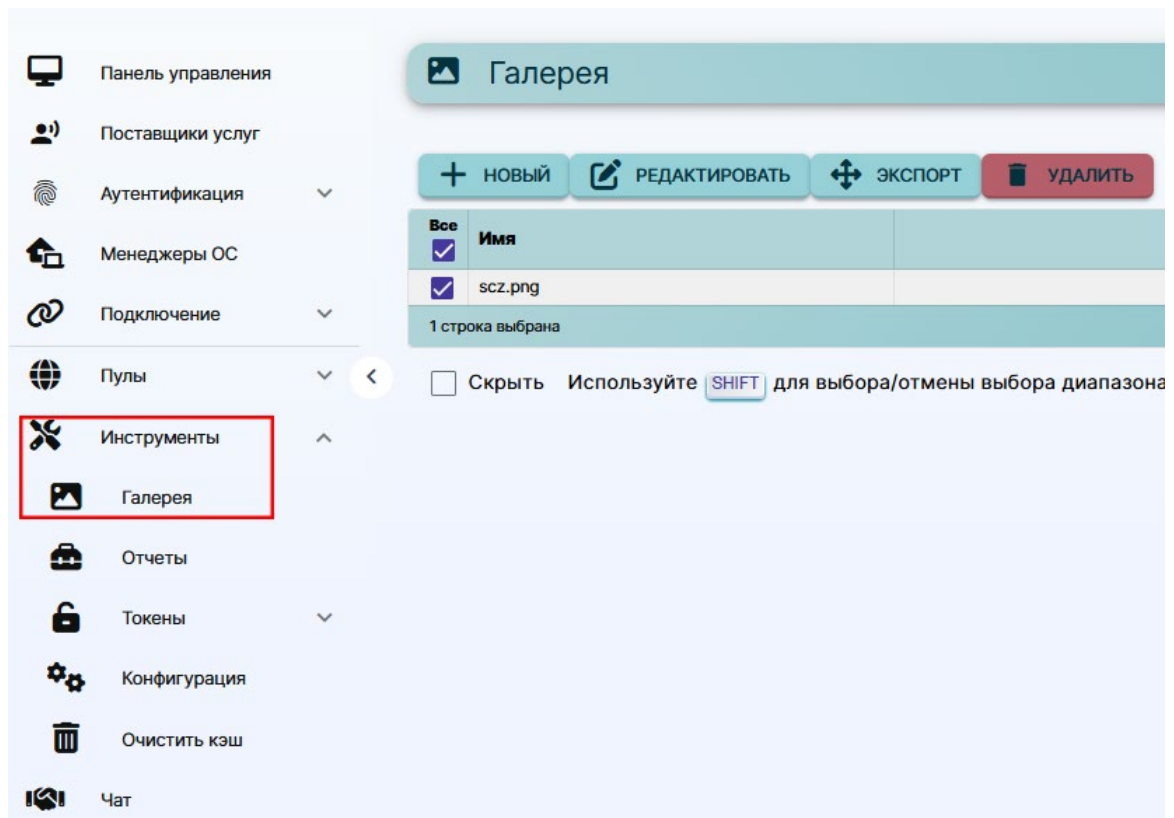


Рисунок 227

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

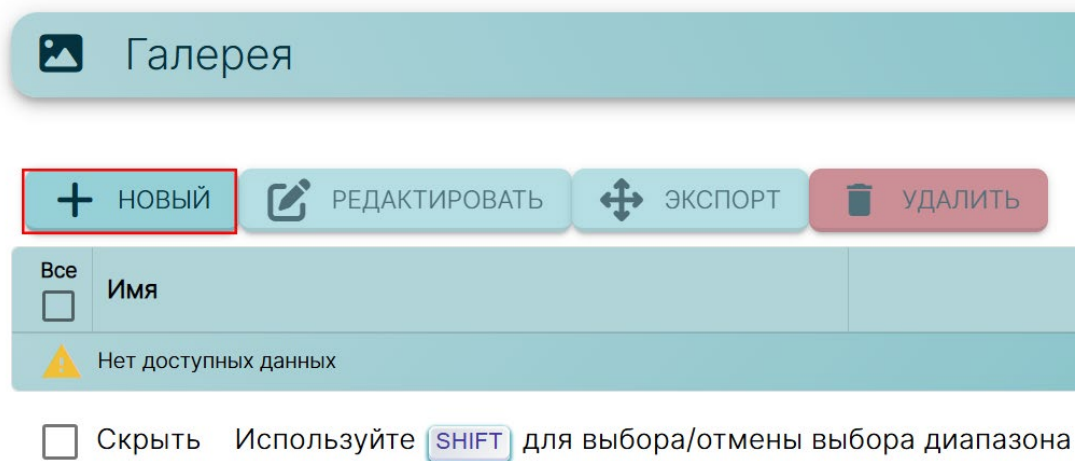


Рисунок 228

3. В открывшемся окне необходимо указать имя и с помощью кнопки **Выбрать изображение** найти образ, который нужно загрузить (Рисунок 229).

Новое изображение для

Имя*

Изображение.
Нажмите, чтобы выбрать



При загрузке размер изображения будет изменен до 128x128

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 229

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

4.1 Отчеты

VDI позволяет автоматически генерировать отчеты по различным элементам платформы.

Чтобы получить доступ к отчетам:

- Войти в раздел **Инструменты** и выбрать **Отчеты** (Рисунок 230).

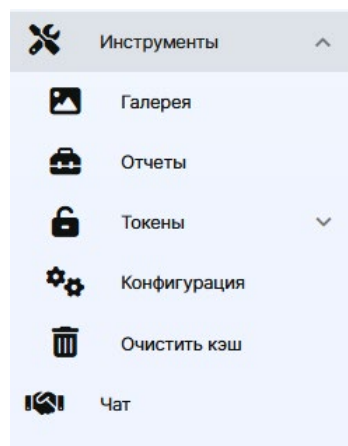


Рисунок 230

- В VDI можно генерировать различные отчеты
 - Список пользователей.** Выбрать отчет из списка, нажать **Сгенерировать отчет**.

 СГЕНЕРИРОВАТЬ ОТЧЕТ

Все 	Группа	Имя
☐	Статистика	Статистика по аутентификатору
☐	Списки	Список пользователей
☒	Списки	Список пользователей
☐	Списки	Список журналов аудита
☐	Статистика	Доступ пользователей по дате
☐	Статистика	Доступ пользователей по дате
☐	Статистика	Производительность пулов по дате
☐	Статистика	Производительность пулов по дате
☐	Статистика	Использование пулов в день
☐	Статистика	Использование пулов в день

1 строка выбрана

Рисунок 231

В открывшемся окне, в выпадающем списке выбрать аутентификатор, нажать кнопку **Сохранить**. (Рисунок 232).

Новый отчет

Аутентификатор*

-1

LdapTest
 TEST-AUTH-LOCAL
 evgen-test-2
 ldap-test-evgen
 testuservdi
 vdi

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 232

После создания будет список всех пользователей, принадлежащих этому аутентификатору.

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

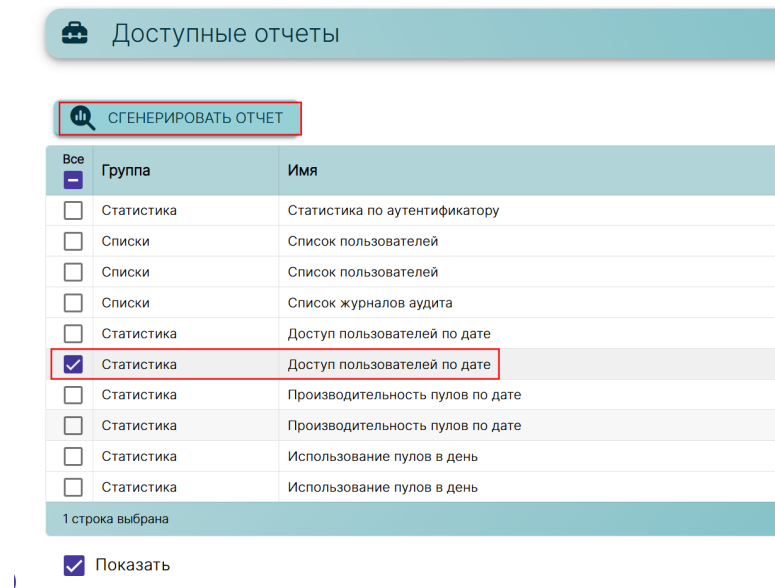


Рисунок 233

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

Рисунок 234Рисунок 234

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

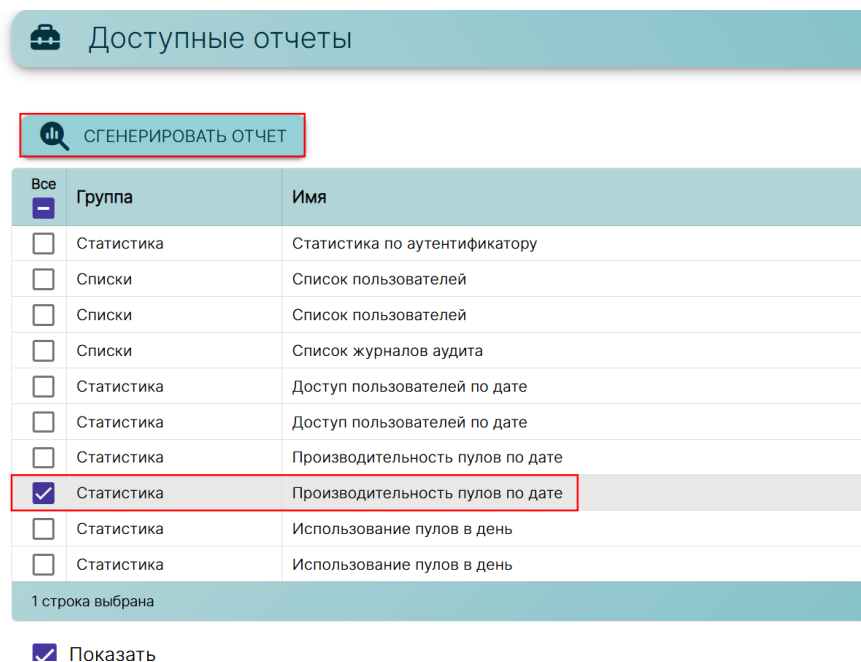


Рисунок 235

Указать пул, по которому нужно сформировать отчет, диапазон дат и количество интервалов (Рисунок 236), нажать кнопку **Сохранить**.

Новый отчет

Пулы*	▼
Дата начала ДД.ММ.ГГГГ	📅
Дата начала отчета	
Дата окончания ДД.ММ.ГГГГ	📅
Дата окончания отчета	
Количество интервалов 8	
Количество интервалов	

[ОТМЕНИТЬ](#) [СОХРАНИТЬ](#)

Рисунок 236

[illegible]