TERMIDESK

РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-01 90 02

Версия 4.3.1. Выпуск от декабря 2023

Настройка программного комплекса

ОГЛАВЛЕНИЕ

1 . ОБЩИЕ СВЕДЕНИЯ

1.1 . О документе

Настоящий документ является второй частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk» (далее - Termidesk). Документ предназначен для администраторов системы и сети.

Во второй части руководства приведена настройка Termidesk, рассмотрены взаимодействие компонентов, разграничение функций по администрированию. Для того, чтобы получить информацию об установке программного комплекса, необходимо обратиться к первой части руководства администратора - СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

1.2 . Типографские соглашения

В настоящем документе приняты следующие типографские соглашения:

- моноширинный шрифт – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

2 . ПОЛЬЗОВАТЕЛИ И КОМПОНЕНТЫ TERMIDESK

2.1 . Разграничение функций

Предусмотрено следующее разграничение функций по управлению Termidesk:

- функции администратора Termidesk;
- функции пользователя Termidesk;
- функции оператора Termidesk.

Администратору Termidesk доступны настройка и управление программным комплексом после успешного прохождения процедуры идентификации и аутентификации. По умолчанию с администратором ассоциируется локальный пользователь операционной системы (ОС) с полномочиями администратора на узле с установленным Termidesk.

> ⓘ Termidesk интегрирован со встроенным комплексом средств защиты информации ОС Astra Linux Special Edition. Идентификация и аутентификация, а также защита аутентификационной информации осуществляется средствами ОС.

Также поддерживаются следующие централизованные сетевые хранилища данных о субъектах и их полномочиях:

- FreeIPA;
- SAML;
- IP-аутентификация;
- Microsoft Active Directory (MS AD) или LDAP;
- RADIUS.

Пользователь Termidesk использует компонент «Клиент» для получения доступа к виртуальному рабочему месту (BPM).

Оператор Termidesk задается администратором Termidesk. Оператору Termidesk доступен ограниченный администратором Termidesk список полномочий по доступу в графический интерфейс управления.

2.2 . Схема взаимодействия компонентов и приложений

Схема взаимодействия компонентов Termidesk и приложений представлена на рисунке (см. Рисунок 1).

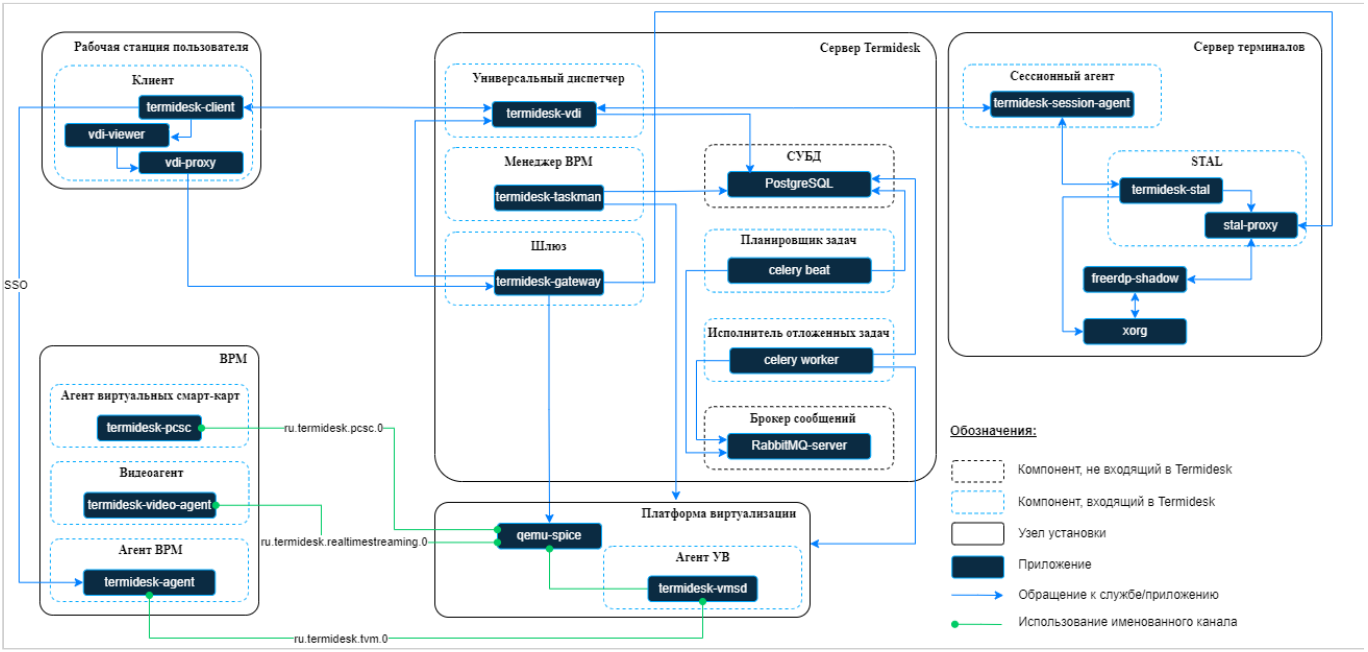

Рисунок 1 – Схема взаимодействия компонентов и процессов

2.3 . Схема сетевого взаимодействия компонентов Termidesk

Схема взаимодействия между сетевыми портами и компонентами Termidesk представлена на рисунке (см. Рисунок 2).

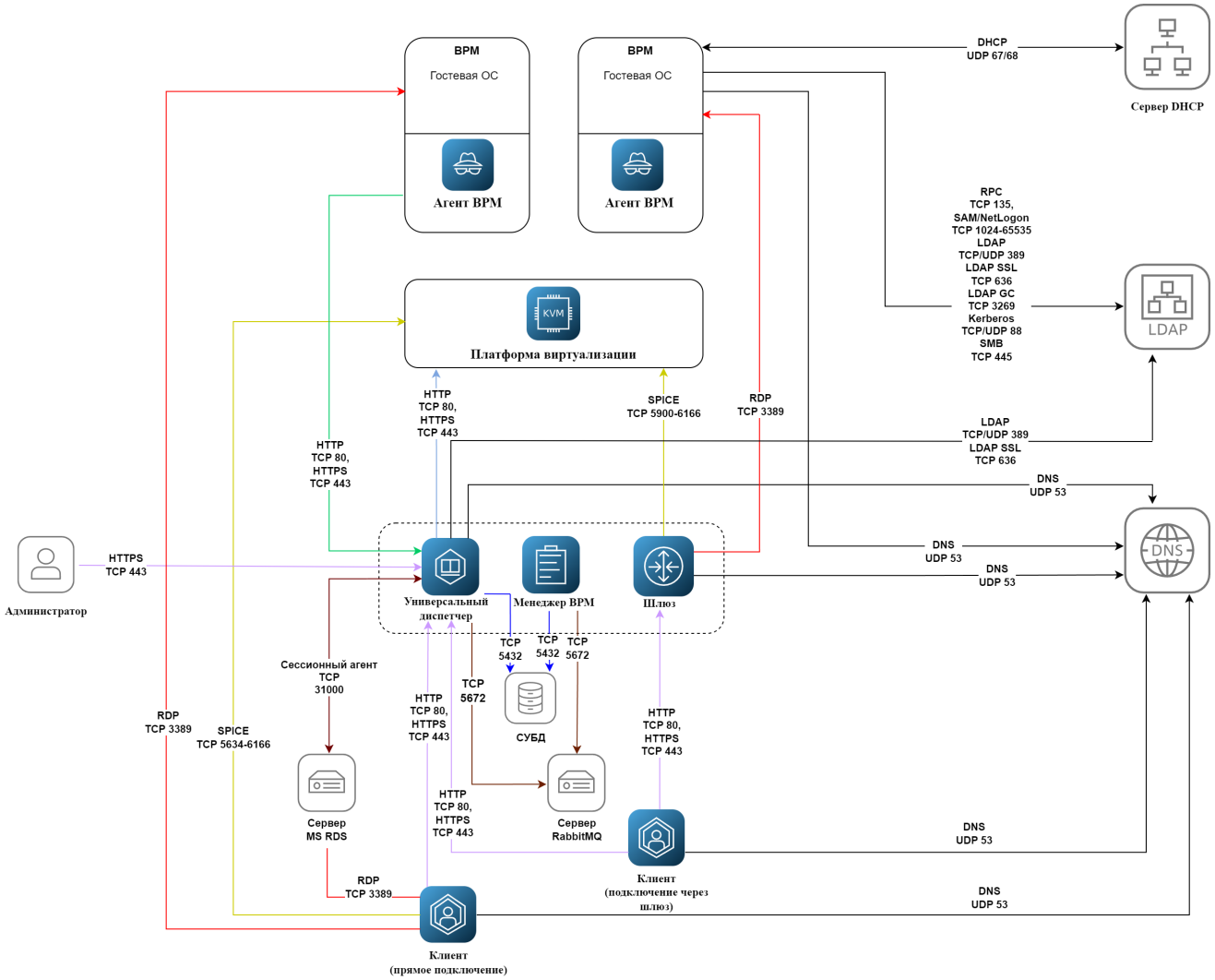

Рисунок 2 – Схема сетевого взаимодействия компонентов Termidesk

Общий перечень узлов и компонентов Termidesk представлен в таблице (см. Таблица 1).

Таблица 1 – Перечень узлов и компонентов

Компонент	Наименование на схеме	Узел установки	Наименование пакета установки
«Универсальный диспетчер»	Универсальный диспетчер	Отдельный узел для установки	`termidesk-vdi`
«Менеджер рабочих мест»	Менеджер ВРМ	Отдельный узел для установки или установка совместно с диспетчером	`termidesk-vdi`
«Шлюз»	Шлюз	Отдельный узел для установки или установка совместно с диспетчером	`termidesk-vdi`
«Агент» (агент ВРМ)	Агент ВРМ	Виртуальная машина (ВМ), установка на этапе подготовки образа	`python3-termidesk-agent` / `termidesk-agent`

Компонент	Наименование на схеме	Узел установки	Наименование пакета установки
«Агент» (агент узла виртуализации)	Агент УВ	Узел виртуализации (платформа виртуализации)	`python3-termidesk-vmsd`
«Агент» (сессионный агент)	Сессионный агент	Сервер терминалов (Microsoft Windows Server с ролью «Remote Desktop Services» (далее - MS RDS), Terminal Server Astra Linux (далее - STAL))	`termidesk-session-agent`
«Агент» (видеоагент)	Видеоагент	ВМ, установка на этапе подготовки образа	`termidesk-video-agent`
«Агент» (агент виртуальных смарт-карт)	Агент виртуальных смарт-карт	ВМ, установка на этапе подготовки образа	`termidesk-pcsc-vscard`
«Клиент»	Клиент	Рабочее место пользователя (пользовательская рабочая станция)	`termidesk-client`
«Оркестратор»	-	Отдельный узел для установки, применяется в облачной конфигурации	`termidesk-orchestrator`
«Сервер терминалов»	STAL	Сервер терминалов Astra Linux (STAL), возможна установка на том же узле, где установлен диспетчер	`stal`

2.4 . Последовательность сетевых запросов компонентов Termidesk

Последовательность сетевых запросов с указанием перечня портов для компонентов Termidesk и элементов инфраструктуры представлена на рисунке (см. Рисунок 3).

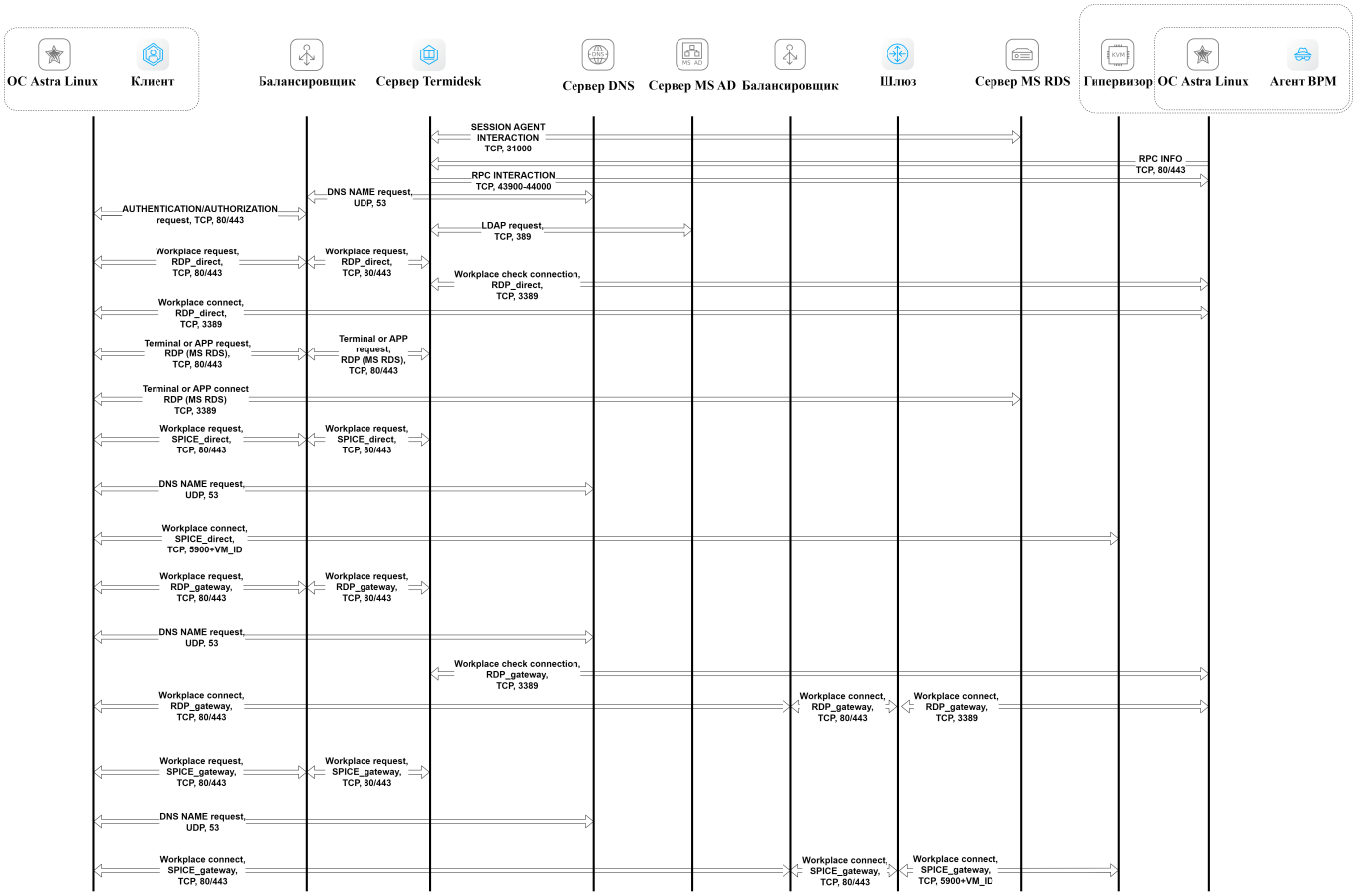

Рисунок 3 – Общая последовательность сетевых запросов

Последовательность сетевых запросов с указанием перечня портов при аутентификации и авторизации пользователя через компонент «Клиент» представлена на рисунке (см. Рисунок 4).

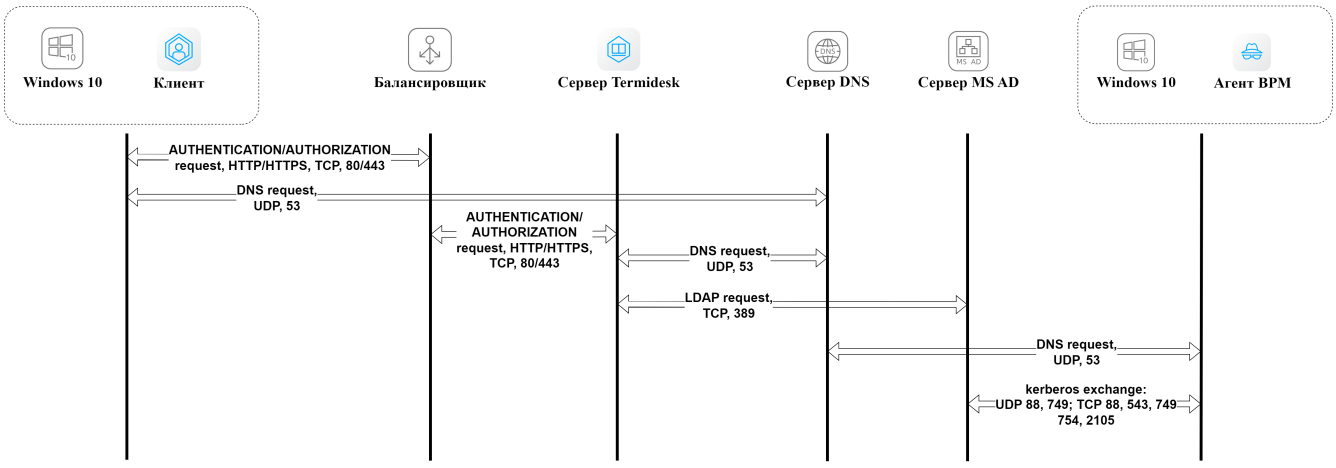

Рисунок 4 – Последовательность сетевых запросов при аутентификации и авторизации

2.5 . Перечень сетевых портов компонентов Termidesk

Перечень сетевых портов, используемых компонентами Termidesk, приведен в таблице (см. Таблица 2).

Таблица 2 – Перечень сетевых портов, используемых компонентами Termidesk

Служба	Протокол	Порт
«Универсальный диспетчер»		
HTTP	TCP	80
LDAP	TCP/UDP	389
HTTPS	TCP	443
LDAP SSL	TCP	636
AMQP (RabbitMQ)	TCP	5672
POSTGRESQL	TCP	5432
VDI (`termidesk-vdi`)	TCP	8000
SESSION AGENT (`TermideskSessionAgent`)	TCP	31000
RPC INTERACTION	TCP	43900-44000
DNS	UDP	53
«Менеджер рабочих мест»		
POSTGRESQL	TCP	5432
AMQP (RabbitMQ)	TCP	5672
HEALTH_CHECK	TCP	8100
«Шлюз»		
HTTP	TCP	80
HTTPS	TCP	443
RDP	TCP	3389
WSPROXY_HEALTHCHECK	TCP	8101
WSPROXY (`termidesk-wsproxy`)	TCP	5099
SPICE	TCP	5900-6166
DNS	UDP	53
«Агент» (агент BPM)		
HTTP	TCP	80
Kerberos	TCP/UDP	88

Служба	Протокол	Порт
RPC	TCP	135
LDAP	TCP/UDP	389
HTTPS	TCP	443
SMB	TCP	445
LDAP SSL	TCP	636
LDAP GC	TCP	3269
RDP	TCP	3389
SAM/NetLogon	TCP	1024-65535
AGENT (`termidesk-agent`)	TCP	39188
RPC INTERACTION	TCP	43900-44000
DNS	UDP	53
DHCP	UDP	67/68
«Агент» (агент узла виртуализации)		
VMSD (`termidesk-vmsd`)	TCP	17082
Программное обеспечение termidesk-viewer (устанавливается с компонентом «Клиент»)		
HTTP	TCP	80
HTTPS	TCP	443
VNC	TCP	5900-59XX
SPICE	TCP	5900-59XX
«Агент» (сессионный агент)		
SESSION AGENT HTTP/HTTPS (`TermideskSessionAgent`)	TCP	31000
«Клиент»		
HTTP	TCP	80
HTTPS	TCP	443
RDP	TCP	3389
CLIENT (`termidesk-client`)	TCP	1024-49151
SPICE	TCP	5900, 5634-6166
«Виртуальный модуль Termidesk»		
ETCD	TCP/UDP	2379, 2380
«Оркестратор»		
HTTP	TCP	80

Служба	Протокол	Порт
HTTPS	TCP	443
«Сервер терминалов» (STAL)		
RDP	TCP	3389

3 . НАЧАЛО РАБОТЫ

3.1 . Последовательность ввода в действие Termidesk VDI

Общая последовательность шагов для ввода Termidesk в действие выглядит следующим образом:

- подготовка сетевой инфраструктуры в соответствии с требованиями раздела **Требования к среде функционирования** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса»;
- подготовка узла виртуализации в соответствии с требованиями подраздела **Требования к платформе виртуализации** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса»;
- установка Termidesk в зависимости от выбранной конфигурации: комплексная или распределенная (см. разделы и подразделы **Подготовка среды функционирования**, **Установка и настройка отделяемых компонентов на одном узле**, **Распределенная установка программного комплекса** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса»). Ввод в домен (при необходимости, согласно схеме сетевой инфраструктуры предприятия);
- установка компонента «Агент» на узел виртуализации (см. подраздел **Установка Агента УВ** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»);
- подготовка базового шаблона ВМ на узле виртуализации (пример для ПК СВ Брест приведен в подразделе **Подготовка базового шаблона ВМ на примере ПК СВ Брест**);
- подготовка базового ВРМ на основе созданного шаблона:
  - настройка гостевой ОС ВМ (см. подраздел **Подготовка базового ВРМ**);
  - установка компонента «Агент ВРМ» (см. раздел **Установка и удаление компонента** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»);
  - настройка компонента «Агент ВРМ» (см. раздел **Настройка Агента ВРМ** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»);

ⓘ Базовое ВРМ - прототип будущих ВРМ.
В базовое ВРМ также могут быть установлены компоненты «Видеоагент», «Агент виртуальных смарт-карт» для активации возможности перенаправления видеокамеры и смарт-карты из пользовательской рабочей станции в ВРМ, однако это потребует активации каналов на узле виртуализации (см. подраздел **Требования к платформе виртуализации** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса»).

- переход в графический интерфейс Termidesk и добавление необходимого поставщика ресурсов в Termidesk (см. раздел **Поставщики ресурсов**);
- добавление необходимого домена аутентификации (при необходимости, если в инфраструктуре используются серверы каталогов) (см. раздел **Аутентификация пользователей**);
- создание шаблона ВРМ в Termidesk в добавленном поставщике ресурсов (см. раздел **Виртуальные рабочие места**);
- добавление настроек гостевых ОС для созданного шаблона ВРМ (см. раздел **Управление параметрами гостевых ОС**);
- создание и настройка фонда ВРМ в Termidesk (см. раздел **Фонд рабочих мест**);
- добавление протоколов доставки, которые будут использоваться для подключения к ВРМ (см. раздел **Протоколы доставки**);
- назначение групп в созданном ранее фонде (см. подраздел **Назначение групп доступа фонду ВРМ**);
- назначение протоколов доставки в созданном ранее фонде (см. подраздел **Назначение протоколов фонду ВРМ**);
- выполнение публикации настроенного фонда ВРМ в Termidesk (см. подраздел **Публикация фонда ВРМ**).

3.2 . Последовательность настройки при использовании терминального сервера

Общая последовательность шагов при необходимости использования терминальных серверов выглядит следующим образом:

- при использовании сервера терминалов на базе ОС Astra Linux Special Edition - установка компонента STAL (см. подраздел **Установка STAL** документа СЛЕТ.10001-01 90 07 «Руководство администратора. Настройка компонента «Сервер терминалов»). Рекомендуется использовать отдельный узел (физический или виртуальный) для сервера терминалов и не совмещать его установку с сервером Termidesk;
- установка компонента «сессионный Агент» на сервер терминалов (см. подраздел **Установка сессионного Агента** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»);
- переход в графический интерфейс Termidesk и добавление поставщика ресурсов «Сервер терминалов» в Termidesk (см. раздел **Добавление сервера терминалов (MS RDS и STAL) в качестве поставщика ресурсов**);
- добавление необходимого домена аутентификации (при необходимости, если в инфраструктуре используются серверы каталогов) (см. раздел **Аутентификация пользователей**);

- создание шаблона BPM для поставщика «Сервер терминалов» в Termidesk (см. подраздел **Шаблоны BPM для серверов терминалов**);
- добавление протоколов доставки, которые будут использоваться для подключения к BPM (см. раздел **Протоколы доставки**);
- создание и настройка фонда BPM в Termidesk (см. раздел **Фонд рабочих мест**)
- назначение групп в созданном ранее фонде (см. подраздел **Назначение групп доступа фонду BPM**);
- назначение протоколов доставки в созданном ранее фонде (см. подраздел **Назначение протоколов фонду BPM**).

3.3 . Подготовка базового шаблона ВМ на примере ПК СВ Брест

При создании базового шаблона ВМ в программном комплексе «Средства виртуализации «Брест» (далее - ПК СВ Брест) необходимо учесть следующее:

- при создании образа диска в панели управления ПК СВ Брест следует перейти «Хранилище - Образ - Постоянный», затем в поле «Постоянный» выбрать значение «Да». Во время установки и настройки ОС тип образа должен быть подключен как постоянный. После установки и завершения настройки ОС в поле «Постоянный» выбрать значение «Нет» (см. Рисунок 5);

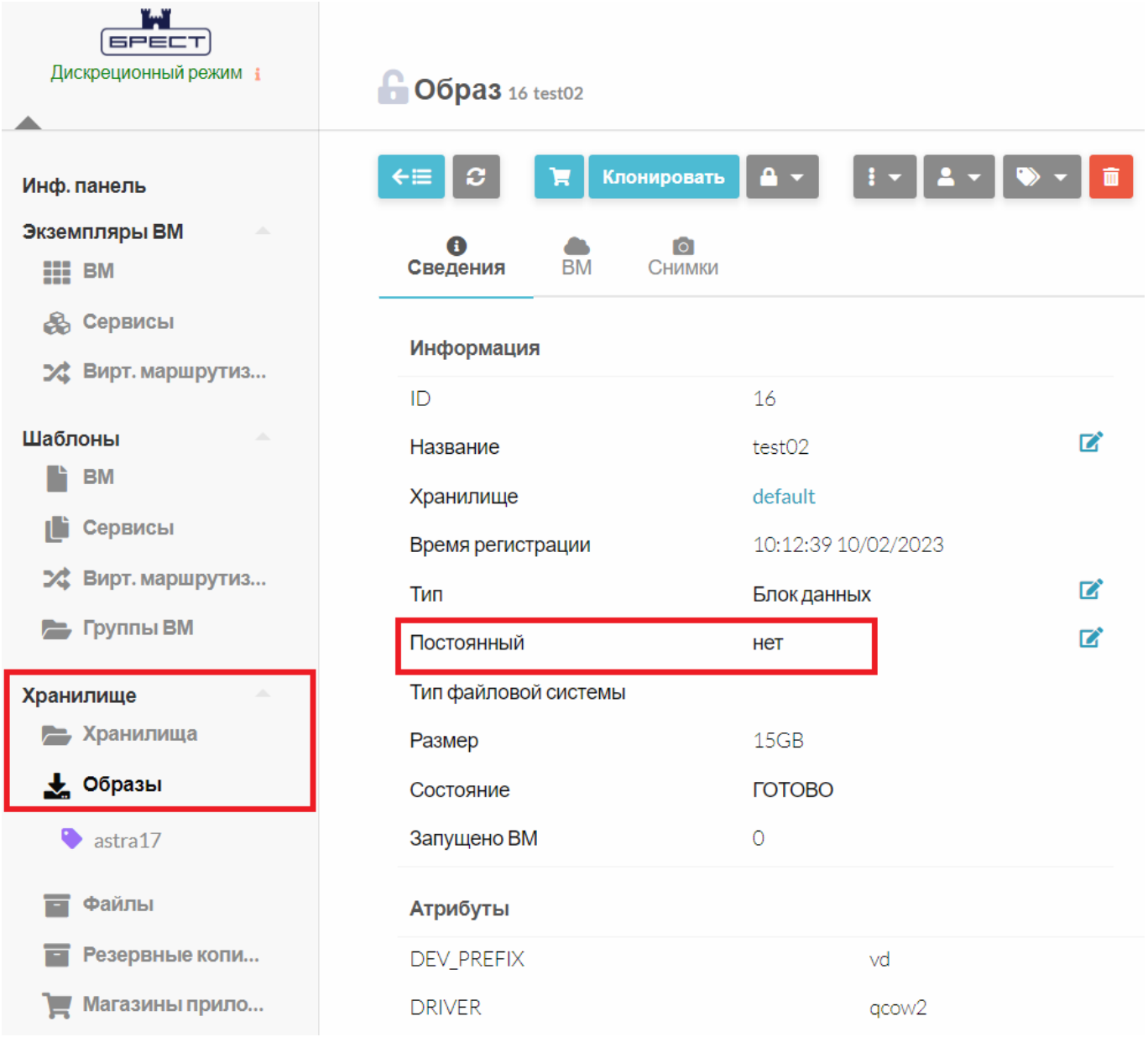

Рисунок 5 – Окно выбора типа подключаемого образа в ПК СВ Брест

⚠ Если ВМ в качестве гостевой ОС будет использовать ОС Windows, то при установке на диск на шине Virtio до включения ВМ необходимо подключить `iso`-образ диска с драйверами `Virtio-win`.

- при создании образа диска в панели управления ПК СВ Брест следует перейти «Хранилище - Образ - Расширенные настройки», затем в поле «Шина» выбрать значение «Virtio», а в поле «Формат» выбрать значение «qcow2» (см. Рисунок 6);

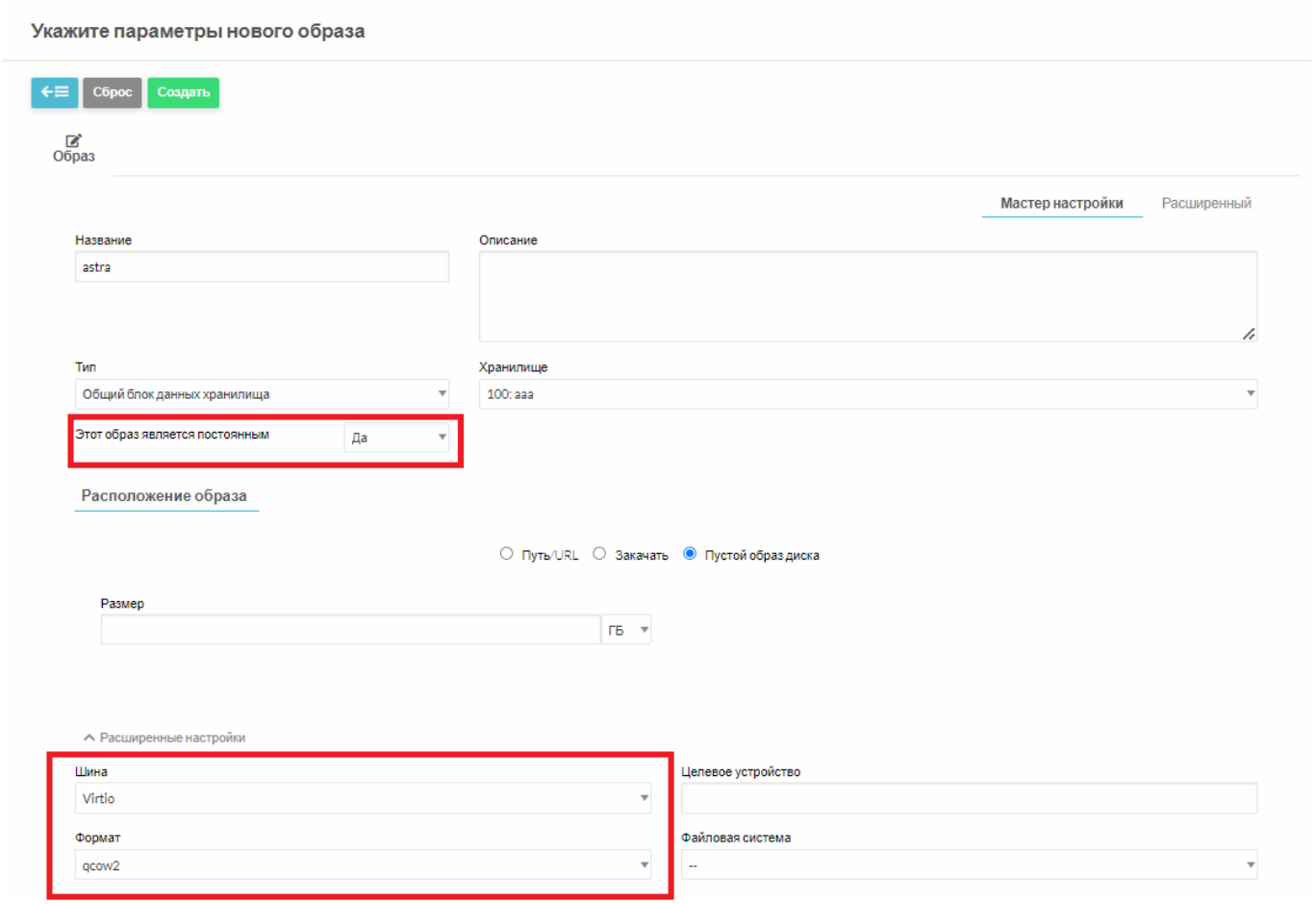

Рисунок 6 – Окно назначения параметров образа диска в ПК СВ Брест

⚠ Значение в поле «Формат» зависит от типа подключенного к ПК СВ Брест хранилища.

- в настройках шаблона ВМ следует перейти «Хранилище - Расширенные настройки», в поле «Шина» выбрать значение «Virtio» (см. Рисунок 7);

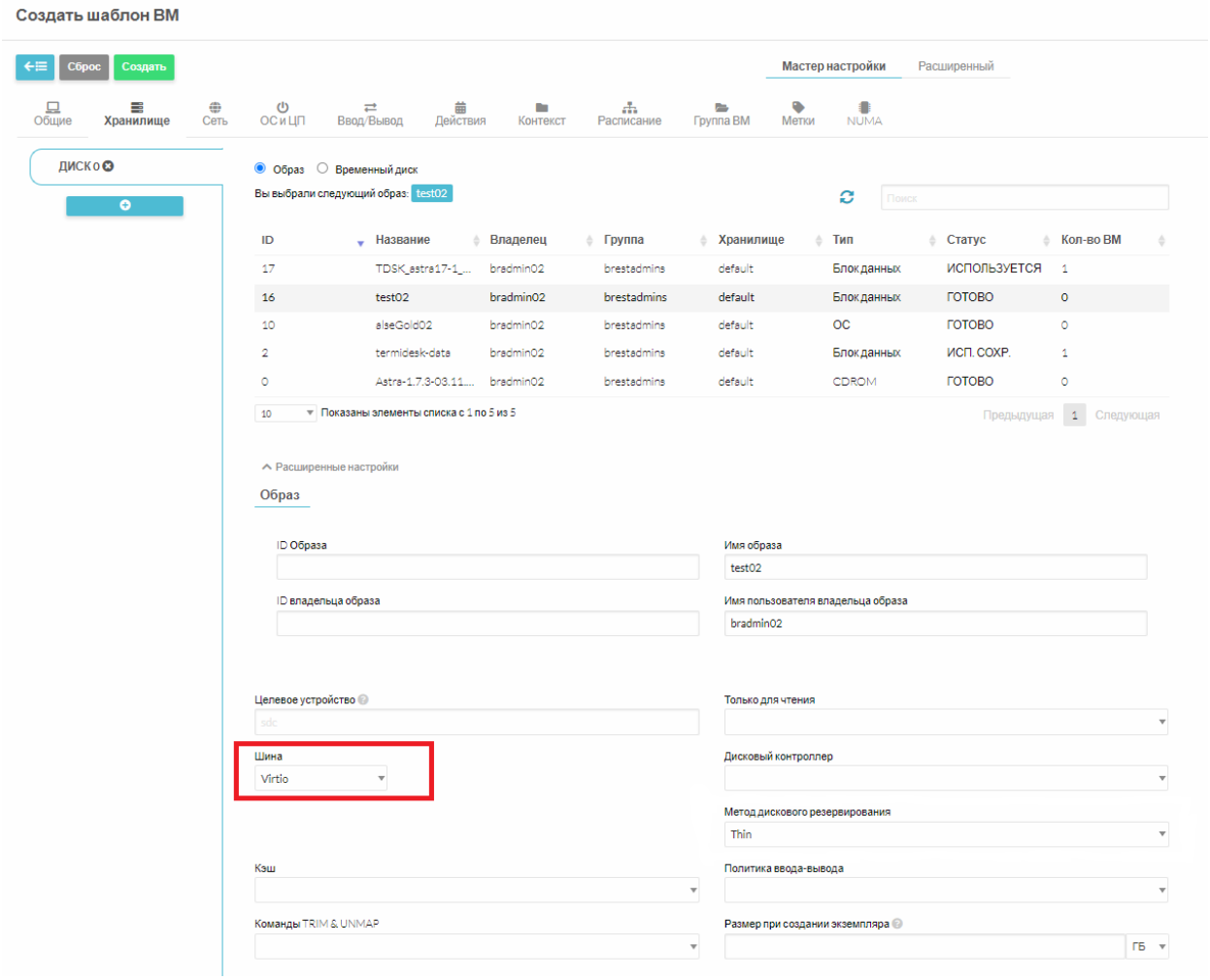

Рисунок 7 – Окно назначения расширенных параметров диска шаблона ВМ

- в настройках шаблона ВМ следует перейти в «Ввод/Вывод», затем в поле «Средства графического доступа» выбрать значение «SPICE», а в поле «Видеокарта» выбрать значение «QXL» (см. Рисунок 8);

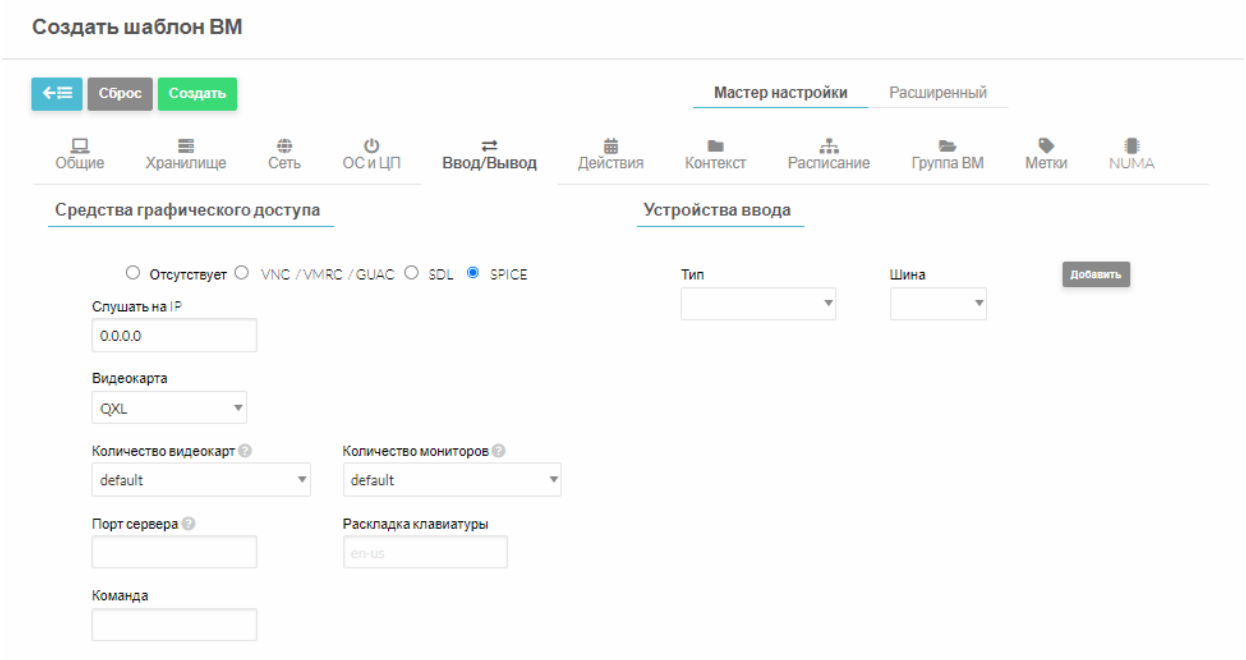

Рисунок 8 – Окно назначения средств графического доступа шаблона ВМ

- в случае многомониторной конфигурации необходимо в выпадающем списке «Количество мониторов» выбрать соответствующее значение для гостевой ОС Astra Linux, а в выпадающем списке «Количество видеокарт» выбрать соответствующее значение для гостевой ОС Windows;
- в настройках шаблона ВМ перейти во вкладку «ОС и ЦП», в поле «Архитектура CPU» следует оставить значение по умолчанию (не менять);
- в случае, если необходим автоматический запуск ВМ, то после создания шаблона ВМ в панели управления ПК СВ Брест следует перейти в созданный шаблон и задать для параметра «Служебная ВМ» значение «Да» (см. Рисунок 9). При добавлении поставщика ресурсов ПК СВ Брест должен быть активирован параметр «Запуск от имени служебного пользователя (см. подраздел **Добавление поставщика ресурсов ПК СВ Брест**).

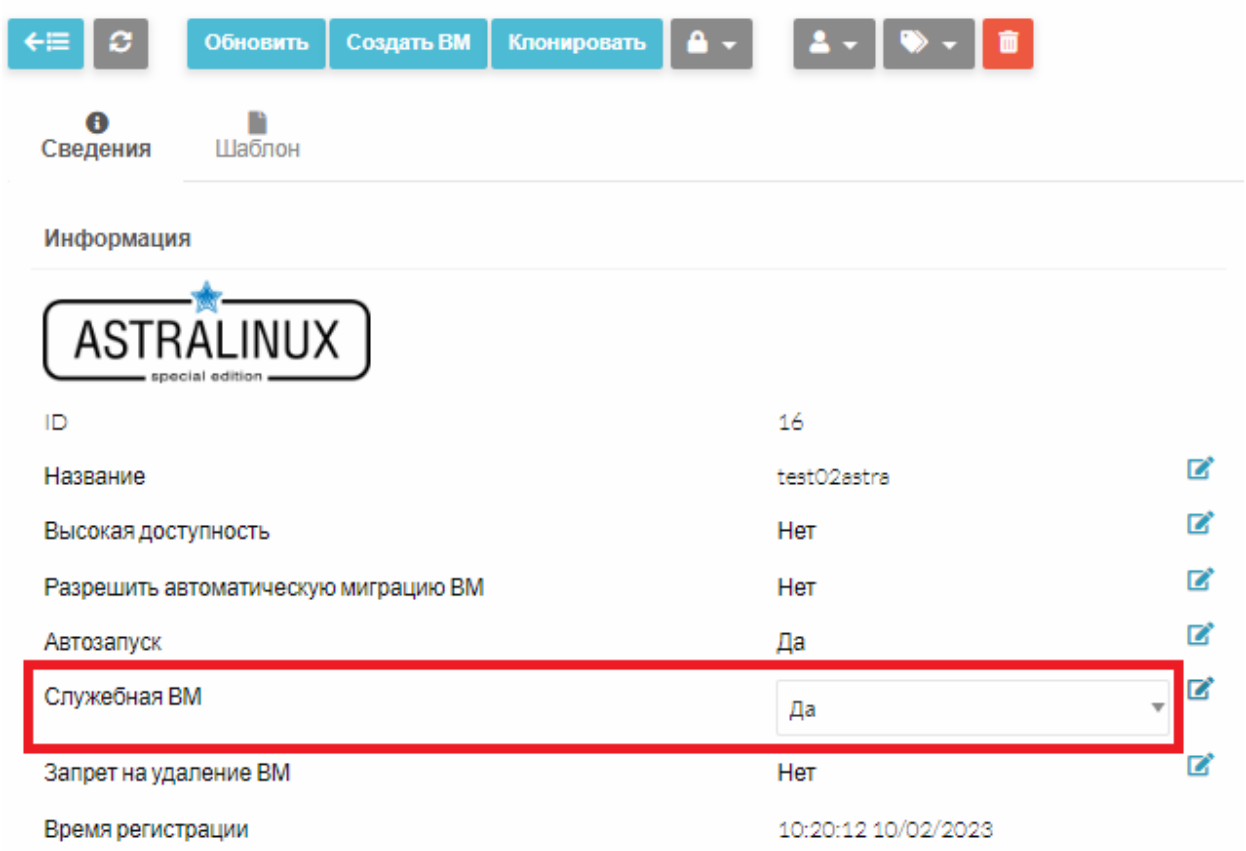

Рисунок 9 – Расположение параметра «Служебная ВМ»

3.4 . Подготовка базового ВРМ

3.4.1 . Обязательные настройки

Для подготовки необходимо:

- в созданной ранее ВМ выполнить настройку гостевой ОС;
- выполнить установку и настройку компонента «Агент» (агента ВРМ, видеоагента, агента виртуальных смарт-карт) Termidesk (см. раздел **Установка и удаление компонента** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»).

⚠ Базовое ВРМ в домен вводить не нужно: процесс ввода контролируется параметрами гостевых ОС (см. подраздел **Управление параметрами гостевых ОС в Termidesk**), которые указываются при создании фонда ВРМ (см. подраздел **Добавление фонда ВРМ**).

Настройка гостевой ОС Windows сводится к выполнению следующих действий:

- отключить режим гибернации;
- отключить выключение дисплея и жесткого диска в дополнительных параметрах схемы электропитания;

⚠ Установку приложений `qemu-guest-agent for Windows`, `spice-guest-tools`, `spice-webdavd` нужно пропустить, если BPM реализовано на базе поставщика ресурсов VMware vSphere, поскольку подключиться к такому BPM можно только по протоколу RDP.

- установить приложения `qemu-guest-agent for Windows` (доступ: https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-qemu-ga/qemu-ga-win-106.0.1-1.el9/) и `spice-guest-tools` (доступ: https://www.spice-space.org/download/windows/spice-guest-tools/);
- установить пакет `spice-webdavd` для Windows (доступ: https://www.spice-space.org/download/windows/spice-webdavd/) для включения возможности перенаправления каталога из пользовательской рабочей станции в BPM. Перенаправление каталогов из пользовательской рабочей станции в BPM с установкой пакета `spice-webdavd` работает только для протокола SPICE;
- включить возможность удаленного подключения по протоколу RDP. Для включения доступа по протоколу RDP в меню «Пуск» нужно выбрать путь «Параметры - Система - Удаленный рабочий стол» и нажать экранную кнопку **[Включить удаленный рабочий стол]**. Также снять галочку в экранном поле «Разрешить подключения только с компьютеров, на которых работает удаленный рабочий стол с проверкой подлинности на уровне сети» (рекомендуется выполнить для ОС Windows 7, а также при подключении по протоколу RDP с пользовательской рабочей станции на основе ОС Linux);
- для возможности перенаправления принтеров из пользовательской рабочей станции с ОС Windows необходимо установить драйвер Microsoft Software Printer Driver. Для установки перейти «Принтеры и сканеры - Свойства сервера печати - Драйверы», нажать экранную кнопку **[Добавить]**, после выбора типа архитектуры нужно указать изготовителя «Microsoft» и выбрать «Microsoft Software Printer Driver»;
- для возможности перенаправления принтеров из пользовательской рабочей станции с ОС Linux необходимо установить драйвер MS Publisher Imagesetter. Для установки перейти «Принтеры и сканеры - Свойства сервера печати - Драйверы», нажать экранную кнопку **[Добавить]**, после выбора типа архитектуры нужно указать изготовителя «Generic» и выбрать «MS Publisher Imagesetter».

Настройка гостевой ОС Astra Linux сводится к выполнению следующих действий:

- установить пакеты `qemu-guest-agent`, `spice-vdagent`, `xserver-xorg-video-qxl`:

```
:~$ sudo apt install -y qemu-guest-agent spice-vdagent xserver-xorg-video-qxl
```

где:

`-y` - ключ для пропуска подтверждения установки;

- установить пакет `xrdp` для корректной работы подключения по протоколу RDP к BPM:

```
:~$ sudo apt install -y xrdp
```

- установить пакет `libcanberra-pulse` для корректной работы аудио:

```
:~$ sudo apt install -y libcanberra-pulse
```

- установить пакеты `spice-webdavd` и `davfs2` для включения возможности перенаправления каталога из пользовательской рабочей станции в BPM по протоколу SPICE:

```
:~$ sudo apt install -y spice-webdavd  davfs2
```

- создать каталог для монтирования `/media/davfs` и выполнить монтирование файловой системы для возможности перенаправления каталога из пользовательской рабочей станции в BPM:

```
:~$ sudo mkdir /media/davfs
:~$ sudo mount -t davfs http://localhost:9843 /media/davfs
```

- привести файл `/etc/acpi/events/powerbtn-acpi-support` к виду:

```
1 event=button/power
2 action=/sbin/poweroff
```

- установить пакет `astra-ad-sssd-client` для возможности ввода BPM с ОС Astra Linux в домен MS AD:

```
:~$ sudo apt install -y astra-ad-sssd-client
```

- установить пакет `astra-freeipa-client` для возможности ввода BPM с ОС Astra Linux в домен FreeIPA:

```
:~$ sudo apt install -y astra-freeipa-client
```

⚠ При необходимости работы с vGPU по протоколу доставки Loudplay в гостевой ОС дополнительно должны быть установлены серверные драйверы NVIDIA и сервер Loudplay.

Для гостевой ОС Astra Linux необходимо также изменить способ назначения сетевых настроек:

- отключить (`systemctl --now mask`) и удалить (`apt remove`) встроенную программу для управления сетевыми соединениями `NetworkManager`:

```
:~$ sudo systemctl --now mask NetworkManager && sudo apt remove network-manager
```

- выполнить настройку сетевых интерфейсов при помощи конфигурационных файлов `/etc/network/interfaces.d/<имя интерфейса>.conf`. Необходимо создать конфигурационные файлы и описать их, воспользовавшись справочным центром Astra Linux: `https://wiki.astralinux.ru/pages/viewpage.action?pageId=3277370`;
- отредактировать файл `/etc/network/interfaces`, добавив в нее следующую строку, если ее нет:

```
source /etc/network/interfaces.d/*
```

- после изменения настроек выполнить перезапуск службы сети:

```
:~$ sudo systemctl restart networking
```

Для гостевой ОС Linux, отличной от Astra Linux, при необходимости ввода ВРМ в домен FreeIPA нужно внести изменения в файл `/usr/lib/python3.6/site-packages/ipalib/constants.py`:

```
1  :~$ sudo sed -i "s/^NAME_REGEX.*$/NAME_REGEX = r'[a-z][_a-z0-9\\\-]*[a-z0-9]$|[a-z]$'/g" $(sudo find / -name constants.py -type f | grep -FzZ 'ipalib/constants.py')
```

Команда осуществляет поиск файла `constants.py` в корневой директории и учитывает, что найденный путь к файлу должен содержать каталог «ipalib». В найденный файл вносится изменение переменной `NAME_REGEX`.

⚠ Путь к файлу зависит от используемой ОС Linux и версии Python и может отличаться от указанного. Для определения пути к файлу можно воспользоваться утилитой `find`:

```
:~$ sudo find / -name constants.py -type f
```

При стандартной настройке сетевой инфраструктуры предполагается, что IP-адрес DNS-сервера определяется DHCP-сервером. Однако если это не так, необходимо скорректировать файл `/etc/resolv.conf` в гостевой ОС Astra Linux:

- указать имя домена и IP-адрес DNS-сервера:

```
:~$ echo -e 'domain <имя_домена>\nsearch <имя_домена>\nnameserver <IP-адрес_DNS-сервера>' | sudo tee /etc/resolv.conf
```

- защитить файл `/etc/resolv.conf` от перезаписи:

```
:~$ sudo chattr +i /etc/resolv.conf
```

Вернуть возможность перезаписи файла `/etc/resolv.conf` можно командой:

```
:~$ sudo chattr -i /etc/resolv.conf
```

3.4.2 . Автоматическое масштабирование экрана в ОС Astra Linux

В некоторых случаях при переходе в полноэкранный режим в пользовательской рабочей станции гостевая ОС Astra Linux не производит автоматическое масштабирование экрана.

> ⚠ Условием масштабирования является запущенный процесс `spice-vdagent` в сессии пользователя.

Для настройки автоматического масштабирования экрана необходимо:

- отредактировать файл `/etc/udev/rules.d/50-spice-vdagent.rules`, создав правило для udev:

```
ACTION=="change", KERNEL=="card0", SUBSYSTEM=="drm", RUN=="/usr/local/bin/x-resize"
```

- перезапустить сервис udev командой:

```
:~$ sudo systemctl restart udev
```

- создать один из вариантов исполняемого файла `/usr/local/bin/x-resize`:
  - вариант 1 - простое масштабирование:

```
#!/bin/sh
PATH=/usr/bin
desktopuser=$(/bin/ps -o user:80= -C spice-vdagent | grep -v fly-dm) || exit 0
export DISPLAY=:0
export XAUTHORITY=$(eval echo "~$desktopuser")/.Xauthority
xrandr --output $(xrandr | awk '/ connected/{print $1; exit; }') --auto
```

  - вариант 2 - масштабирование конкретного монитора. В данном примере исполняемого файла второй монитор располагается слева от основного:

```
#!/bin/sh
PATH=/usr/bin
# Имя пользователя получается через вывод списка пользователей (заголовки отключены), от имени которых запущен spice-vdagent | из списка вырезается имя fly-dm (сессия отображения ввода логина-пароля)
desktopuserlist=$(/bin/ps -o user:80= -C spice-vdagent | grep -v fly-dm) || exit 0
# Проверенное решение, но работает только для имён пользователей без дефисов, пробелов и т.д.
#desktopuserlist=$(/bin/ps -ef  | /bin/grep -oP  '^\w+ (?=.*vdagent( |$))') || exit 0
for desktopuser in $desktopuserlist; do
  export DISPLAY=:0
  export XAUTHORITY=$(eval echo "~$desktopuser")/.Xauthority

#Get active monitors
```

```
  ACTMONS=$(xrandr --listactivemonitors | awk '/[[:alnum:]]+ +/ {print $4}' | sort)
#Get primary monitor
  PRIMARYMON=$(xrandr --listactivemonitors | awk '/*/ {print $4}')

#Get current and preferred display resolutions
  for MON in $ACTMONS
  do
    #Get preferred display resolution
    PREFRES=$(xrandr | awk -v monpref="$MON connected" '/connected/ {p = 0} $0 ~ monpref {p = 1} p' | awk '/+/ {print $1;}' | sed -n '2~2p')
    #Get current display resolution
    CURNRES=$(xrandr | awk -v moncurn="$MON connected" '/connected/ {p = 0} $0 ~ moncurn {p = 1} p' | awk '/*/ {print $1;}')
    if [[ $CURNRES != $PREFRES ]];
    then
        if [[ $MON == $PRIMARYMON ]];
        then
                xrandr --output $MON --auto
                logger -p local0.notice -t ${0##*/}[$$] "$MON primary display change resolution to preferred $PREFRES"
        else
                xrandr --output $MON --left-of $PRIMARYMON --auto
                logger -p local0.notice -t ${0##*/}[$$] "$MON display change resolution to preferred $PREFRES and left of $PRIMARYMON"
        fi
    else
        logger -p local0.notice -t ${0##*/}[$$] "$MON display is already using preferred resolution $PREFRES"

    fi
  done
done
```

- сделать файл исполняемым при помощи команды:

```
:~$ sudo chmod +x /usr/local/bin/x-resize
```

Для масштабирования экрана приветствия необходимо выполнить:

- заблокировать автостарт `kscreen`, переименовав расширение или удалив данные файлы из указанных директорий: `/usr/share/fly-dm/autostart/greeter/kscreend_autostart.desktop`, `/usr/share/fly-dm/preload/greeter/kscreend_preload.desktop`;
- сделать символьную ссылку на ярлык для автозапуска `spice-vdagent` для экрана приветствия:

```
:~$ sudo ln -s /etc/xdg/autostart/spice-vdagent.desktop /usr/share/fly-dm/autostart/greeter/spice-vdagent.desktop
```

- перезапустить процесс `fly-dm` командой:

```
:~$ sudo systemctl restart fly-dm
```

⚠ Если файл `/usr/bin/fly-monitor-hotplug.sh` не является исполняемым или удален, то на экране приветствия масштабирование не выполняется.

4 . ПОСТАВЩИКИ РЕСУРСОВ

4.1 . Общие сведения о поставщиках ресурсов

Поставщик ресурсов - это ОС, платформа виртуализации или терминальный сервер, предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения ВРМ.

Поддержка некоторых поставщиков ресурсов может добавляться в режиме экспериментальных функций или при помощи плагинов расширений.
В Termidesk поддерживаются следующие поставщики ресурсов:

- ПК СВ Брест;
- VMmanager;
- zVirt;
- oVirt;
- «РЕД Виртуализация»;
- Openstack;
- VMware vSphere;
- MS RDSH;
- STAL.

Графический интерфейс управления Termidesk обеспечивает следующие операции управления поставщиками ресурсов:

- добавление;
- редактирование;
- удаление;
- техобслуживание;
- просмотр сведений;
- организация шаблона ВРМ.

Для добавления в Termidesk поставщика ресурсов в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка необходимого поставщика.
Каждый поставщик ресурсов описывается перечнем параметров, требуемых Termidesk для получения идентификаторов субъектов и информации о полномочиях. Проверить корректность указанных параметров можно при помощи экранной кнопки **[Тест]**, расположенной в том же окне. Для сохранения параметров конфигурации необходимо использовать экранную кнопку **[Сохранить]**.

Для редактирования информации о созданном поставщике ресурсов следует перейти «Компоненты - Поставщики ресурсов», затем выбрать необходимого поставщика и нажать на экранную кнопку **[Редактировать]**.

Для удаления созданного поставщика ресурсов следует перейти «Компоненты - Поставщики ресурсов», затем выбрать необходимого поставщика и нажать на экранную кнопку **[Удалить]**.

⚠ Поставщик ресурсов может быть удален только в том случае, если на нем не производится размещение фондов BPM.

4.2 . Добавление поставщика ресурсов ПК СВ Брест

4.2.1 . Получение и добавление файла keytab

`Keytab`-файлы используются для аутентификации в системах, использующих `Kerberos`. Для получения `keytab`-файла на контроллере домена и добавления его на сервер, где установлен Termidesk, необходимо выполнить ряд действий.

Действия на контроллере домена (например, FreeIPA):

- получить доступ к контроллеру домена в режиме интерфейса командной строки;
- получить `kerberos-ticket` для пользователя с полномочиями администратора домена при помощи команды:

```
:~$ sudo kinit admin
```

- выполнить команду для добавления узла:

```
:~$ sudo ipa host-add --force --ip-address=192.0.2.30 disp.termidesk.local
```

где:

`--force` - флаг для принудительного создания;

`--ip-address` - задание IP-адреса целевого узла;

`192.0.2.30` - IP-адрес сервера, где установлен Termidesk,

`disp.termidesk.local` - мнимый FQDN узла в текущем домене (в примере `termidesk.local`);

⚠ Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре предприятия.
Мнимый FQDN означает, что он не обязательно должен быть привязан к действительно существующему узлу.

- выполнить команду добавления службы для нового сервисного аккаунта:

```
:~$ sudo ipa service-add HTTP/disp.termidesk.local
```

- создать файл `termidesk.keytab` для сервисного аккаунта:

```
:~$ sudo ipa-getkeytab -s freeipa.termidesk.local -p HTTP/disp.termidesk.local -k /home/
user/termidesk.keytab
```

где:

`-s freeipa.termidesk.local` - задание FQDN сервера-контроллера домена FreeIPA;

`-p HTTP/disp.termidesk.local` - указание ранее созданного субъекта-службы;

`-k /home/user/termidesk.keytab` - сохранение в файл `termidesk.keytab`;

⚠ Неважно, для какого узла создан `keytab`, необходимо само его наличие.

- передать полученный файл `termidesk.keytab` на узел Termidesk, например, воспользовавшись командой:

```
:~$ sudo scp termidesk.keytab localuseruser@192.0.2.30:termidesk.keytab
```

где:

`localuser` - имя пользователя целевого узла;

`192.0.2.30` - IP-адрес сервера, где установлен Termidesk.

После передачи файла на узле Termidesk необходимо выполнить следующее:

- переместить файл `termidesk.keytab` в каталог `/etc/opt/termidesk-vdi`:

```
:~$ sudo mv /home/user/termidesk.keytab /etc/opt/termidesk-vdi/
```

- сделать владельцем этого файла пользователя `termidesk`:

```
:~$ sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/termidesk.keytab
```

- перезапустить службу `termidesk-vdi`:

```
:~$ sudo systemctl restart termidesk-vdi
```

4.2.2 . Перечень параметров для добавления

Для добавления в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка «ПК СВ Брест».

При добавлении в Termidesk поставщика ресурсов ПК СВ Брест администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 3).

Таблица 3 – Данные для добавления поставщика ресурсов ПК СВ Брест

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Версия ПК СВ Брест»	Выбор версии установленной платформы виртуализации
«Адрес сервера»	IP-адрес или доменное имя фронтальной машины платформы виртуализации
«Домен»	Идентификатор области `Kerberos` для аутентификации
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (полученный ранее `termidesk.keytab`, `/etc/opt/termidesk-vdi/termidesk.keytab`)
«Порт»	Номер порта для подключения к API платформы виртуализации. По умолчанию используется порт 2633, если на платформе виртуализации не было указано иное
«Использовать SSL»	Включение использования протокола SSL
«Проверка SSL»	Включение строгой проверки SSL
«Запуск ВМ от имени служебного пользователя»	Переключатель для запуска ВМ на платформе виртуализации от имени служебного пользователя. Если данный параметр активирован, то параметры «Делегация запуска ВМ», «Логин делегата», «Пароль делегата» настраивать не нужно
«Логин»	Субъект, имеющий полномочия для управления платформой виртуализации
«Пароль»	Пароль субъекта с полномочиями для управления платформой виртуализации
«Токен»	Электронный ключ субъекта с полномочиями для управления платформой виртуализации, который нужно скопировать из интерфейса управления платформой виртуализации. Для этого следует зайти в интерфейс управления платформой виртуализации с помощью логина и пароля указанного пользователя, в главном меню развернуть раздел «System» и выбрать строку «Users». В появившемся окне выбрать указанного пользователя, перейти на вкладку «Auth» и нажать экранную кнопку **[Manage login tokens]**, в появившейся форме скопировать значение из поля «Token»
«Делегация запуска ВМ»	Включение делегирования прав на запуск ВМ на платформе виртуализации другому пользователю
«Логин делегата»	Субъект, которому делегируется право на запуск ВМ на платформе виртуализации

Параметр	Описание
«Пароль делегата»	Пароль субъекта, которому делегируется право на запуск ВМ на платформе виртуализации
«Подготавливать ВМ одновременно»	Количество одновременно создаваемых ВМ на платформе виртуализации
«Удалять ВМ одновременно»	Количество одновременно удаляемых ВМ с платформы виртуализации
«Время ожидания»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации

⚠ Необходимо задать перечисленные параметры таким образом, чтобы использовался либо запуск ВМ от имени служебного пользователя (назначается параметр «Запуск ВМ от имени служебного пользователя»), либо запуск от имени пользователя-делегата (назначаются параметры «Делегация запуска ВМ», «Логин делегата», «Пароль делегата»). Использовать одновременно оба типа запуска запрещено.

Для управления платформой ПК СВ Брест субъект должен иметь привилегии, указанные в таблице (см. Таблица 4).

Таблица 4 – Перечень привилегий для роли в ПК СВ Брест

Путь к привилегии	Требуемые настройки
«Система - Группы»	Создать группу `termidesk`, установив настройки: ▪ на вкладке «Представление»: • отключить предоставление всех привилегий; ▪ на вкладке «Права» предоставить привилегии: • ВМ; • образы; • шаблоны
«Система - Пользователи»	Создать пользователя `termidesk-tech` и добавить в группу `termidesk`
«Хранилища - Образы»	В разделе «Владелец» назначить: ▪ «Владелец» - `termidesk-tech`; ▪ «Группа» - `termidesk`
«Шаблоны - ВМ»	Отредактировать шаблон ВМ: ▪ перейти: «Хранилище - Расширенные настройки - Образ»; ▪ в строке «Имя пользователя владельца образа» указать нужного пользователя; ▪ обновить шаблон ВМ

4.3 . Добавление платформы oVirt/zVirt/RHEV

Для добавления в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка «Платформа oVirt/RHEV».

Для добавления в Termidesk платформы oVirt/RHEV администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 5).

Таблица 5 – Данные для добавления платформы oVirt/RHEV

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Версия oVirt»	Выбор используемой версии oVirt
«Адрес oVirt»	IP-адрес или доменное имя платформы виртуализации oVirt
«Логин»	Субъект, имеющий полномочия для управления платформой виртуализации oVirt. Указывается в формате `login@internal`
«Пароль»	Набор символов, подтверждающий назначение полномочий
«Создавать ВМ одновременно»	Количество одновременно создаваемых ВМ на платформе виртуализации oVirt
«Удалять ВМ одновременно»	Количество одновременно удаляемых ВМ с платформы виртуализации oVirt
«Время ожидания»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации oVirt

Для платформы oVirt субъект должен иметь привилегии, указанные в таблице (см. Таблица 6).

ⓘ В общем случае назначение ролей выглядит следующим образом: на сервере oVirt создается пользователь (например, `termidesk`), создается роль (в рамках oVirt употребляется термин «роль») (`termidesk`). Пользователю `termidesk` выдается роль `termidesk`.

ⓘ Создать роль `termidesk` быстрее и проще через копирование существующей:`PowerUserRole` (необходимо перейти в графическом интерфейсе oVirt в «Administration - Configure - Roles, выбрать роль `PowerUserRole` и нажать **[Copy]**, изменить наименования на `termidesk`). Созданную роль затем изменить, добавив отсутствующие привилегии в соответствии с таблицей.

⚠ Роль `termidesk` с указанными привилегиями подходит только для управления ВМ, она не имеет прав доступа на администрирование oVirt.

Таблица 6 – Перечень привилегий для роли в oVirt

Тип привилегий	Наименование привилегий
«System»: «Configure System»	«Login Permissions»
«Network»: «Configure vNIC Profile»	«Assign vNIC Profile to VM»
«Template»: «Provisioning Operations»	«Create» «Delete»
«VM»: «Basic Operations»	«Reboot VM» «Reset VM» «Stop VM» «Shutdown VM» «Hibernate VM» «Run VM» «Change CD»
«VM»: «Provisioning Operations»	«Create» «Create Instance» «Delete»
«Disk»: «Provisioning Operations»	«Create» «Delete» «Attach» «Access Image Storage Domains»
«Disk»: «Disk Profile»	«Attach Disk Profile»

4.4 . Добавление платформы zVirt

Для добавления в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка «Платформа zVirt».

⚠ Для корректной интеграции Termidesk с платформой zVirt нужно:

- на хост zVirt Node установить дополнительный пакет `termidesk_zVirt_hook-<версия>-zvirt.noarch.rpm`:

```
:~$ rpm -i termidesk_zVirt_hook-<версия>-zvirt.noarch.rpm
```

- перезапустить сервис `ovirt-engine`:

```
:~$ service ovirt-engine restart
```

- убедиться, что каналы `ru.termidesk.PCSC.0`, `ru.termidesk.Printer.0`, `ru.termidesk.RealtimeStreaming.0`, `ru.termidesk.tvm.0` отображены в выводе команды:

```
:~$ ls /dev/virtio-ports
```

Для добавления в Termidesk платформы zVirt администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 7).

Таблица 7 – Данные для добавления платформы zVirt

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Версия zVirt»	Выбор используемой версии zVirt
«Адрес zVirt»	IP-адрес или доменное имя платформы виртуализации zVirt
«Логин»	Субъект, имеющий полномочия для управления платформой виртуализации zVirt. Указывается в формате `login@internal`
«Пароль»	Набор символов, подтверждающий назначение полномочий
«Подготавливать ВМ одновременно»	Количество одновременно создаваемых ВМ на платформе виртуализации zVirt
«Удалять ВМ одновременно»	Количество одновременно удаляемых ВМ с платформы виртуализации zVirt
«Время ожидания»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации zVirt

4.5 . Добавление платформы «РЕД Виртуализация»

Для добавления в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка «Платформа RED Virtualization».

⚠ Для корректной интеграции Termidesk с платформой «РЕД Виртуализация» нужно:

- установить на всех хостах пакет `vdsm-hook-qemucmdline`:

```
:~$ sudo dnf install vdsm-hook-qemucmdline
```

Для варианта `HostedEngine`:

- выполнить:

```
:~$ sudo engine-config -s "UserDefinedVMProperties=qemu_cmdline=^.*$"
```

- на запрос выбора версии выбрать 4.6 или более позднюю;
- выполнить перезапуск службы:

```
:~$ sudo service ovirt-engine restart
```

Для добавления в Termidesk платформы «РЕД Виртуализация» администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 8).

Таблица 8 – Данные для добавления платформы РЕД

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Версия REDVirt»	Выбор используемой версии REDVirt
«Адрес REDVirt»	IP-адрес или доменное имя платформы виртуализации REDVirt
«Логин»	Субъект, имеющий полномочия для управления платформой виртуализации REDVirt. Указывается в формате `login@internal`
«Пароль»	Набор символов, подтверждающий назначение полномочий
«Подготавливать ВМ одновременно»	Количество одновременно создаваемых ВМ на платформе виртуализации REDVirt
«Удалять ВМ одновременно»	Количество одновременно удаляемых ВМ с платформы виртуализации REDVirt
«Время ожидания»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации REDVirt

4.6 . Добавление поставщика VMmanager

Для добавления в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка «Платформа VMmanager».

Для добавления в Termidesk поставщика VMmanager администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 9).

Таблица 9 – Данные для добавления поставщика ресурсов VMmanager

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Хост»	IP-адрес или полное доменное имя сервера VMmanager
«Логин (эл. почта)»	Субъект, имеющий полномочия для управления платформой виртуализации VMmanager
«Пароль»	Набор символов, подтверждающий назначение полномочий субъекта
«Использовать SSL»	Включение использования протокола SSL
«Проверять SSL»	Включение строгой проверки SSL
«Подготавливать ВМ одновременно»	Количество одновременно создаваемых ВМ на платформе виртуализации VMmanager
«Удалять ВМ одновременно»	Количество одновременно удаляемых ВМ с платформы виртуализации VMmanager
«Таймаут (сек)»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации VMmanager

4.7 . Добавление поставщика ресурсов VMware vSphere

Для добавления в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка «Платформа VMware».

> ⚠ При взаимодействии Termidesk с платформой VMware необходимо наличие ВМ управления (vCenter). Начиная с версии Termidesk 4.1 поддерживается работа как с кластерами данных в качестве системы хранения, так и с обычными хранилищами (Datastore).

Для добавления в Termidesk поставщика VMware vSphere администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 10).

Таблица 10 – Данные для добавления поставщика ресурсов VMware vSphere

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Версия платформы»	Выбор используемой версии платформы виртуализации
«Адрес сервера»	IP-адрес или доменное имя ВМ управления платформой виртуализации VMware (vCenter)

Параметр	Описание
«Порт»	Номер порта для подключения к API
«Использовать SSL»	Форсировать использование протокола SSL
«Логин»	Субъект, имеющий полномочия для управления платформой виртуализации VMware
«Пароль»	Набор символов, подтверждающий назначение полномочий субъекта
«Подготавливать ВМ одновременно»	Количество одновременно создаваемых ВМ на платформе виртуализации VMware
«Удалять ВМ одновременно»	Количество одновременно удаляемых ВМ с платформы виртуализации VMware

Субъект должен иметь привилегии, указанные в таблице (see page 0).

ⓘ В общем случае назначение ролей выглядит следующим образом: на сервере vCenter создается пользователь (например, `termidesk`), создается группа (`Termidesk Group`) и класс (в рамках vCenter употребляется термин «роль») (`Termidesk`). Созданной группе `Termidesk Group` выдается роль `Termidesk`.

ⓘ Роль `Termidesk` состоит из сочетания встроенной группы Virtual machine power user (sample) и VMware virtualization environments(Citrix).

Таблица 11 – Перечень привилегий для роли в VMware vCenter

Тип привилегий	Наименование привилегий
«Datastore»	«Allocate space» «Browse datastore» «Low level file operations»
«Global»	«Cancel task»
«Network»	«Assign network»
«Resource»	«Assign virtual machine to resource pool»
«Scheduled task»	«Create tasks» «Modify task» «Remove task» «Run task»

Тип привилегий	Наименование привилегий
«Virtual machine»: «Change Configuration»	«Acquire disk lease» «Add existing disk» «Add new disk» «Add or remove device» «Advanced configuration» «Change CPU count» «Change Memory» «Change Settings» «Change resource» «Modify device settings» «Remove disk» «Rename» «Reset guest information» «Upgrade virtual machine compatibility»
«Virtual machine»: «Edit Inventory»	«Create from existing» «Create new» «Remove»
«Virtual machine»: «Interaction»	«Answer question» «Configure CD media» «Configure floppy media» «Connect devices» «Console interaction» «Pause or Unpause» «Power off» «Power on» «Reset» «Suspend»
«Virtual machine»: «Provisioning»	«Clone virtual machine» «Create template from virtual machine» «Deploy template»
«Virtual machine»: «Snapshot management»	«Create snapshot» «Remove snapshot» «Rename snapshot» «Revert to snapshot»

4.8 . Добавление поставщика vAir

Для возможности добавления поставщика ресурсов vAir необходимо включить экспериментальный параметр `experimental.vair.provider.enabled` в соответствии с подразделом **Управление экспериментальными параметрами Termidesk**.

После включения экспериментального параметра в графическом интерфейсе управления перейти в «Компоненты - Поставщики ресурсов», а затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка «Поставщик vAir».

Для добавления поставщика ресурсов vAir администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 12).

Таблица 12 – Данные для добавления поставщика ресурсов vAir

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Версия API платформы»	Выбор используемой версии
«Адрес сервера»	IP-адрес или доменное имя платформы виртуализации
«Порт»	Порт для подключения к API
«Использовать SSL»	Включение использования протокола SSL
«Логин»	Субъект, имеющий полномочия для управления платформой виртуализации
«Пароль»	Набор символов, подтверждающий назначение полномочий
«Подготавливать ВМ одновременно»	Количество одновременно создаваемых ВМ на платформе виртуализации
«Удалять ВМ одновременно»	Количество одновременно удаляемых ВМ с платформы виртуализации

4.9 . Добавление сервера терминалов (MS RDS и STAL) в качестве поставщика ресурсов

Для добавления в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», затем нажать экранную кнопку **[Новый]** и выбрать из выпадающего списка «Сервер терминалов».

⚠ Для взаимодействия с сервером терминалов (MS RDS или STAL) необходимо установить сессионный агент в соответствии с подразделом **Установка сессионного Агента** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент».
Работа с сервером терминалов MS RDS поддерживается только при условии развернутой полнофункциональной инфраструктуры MS RDS. Если такой инфраструктуры нет, то рекомендуется воспользоваться решением, основанным на поставщике ресурсов «метапровайдер».

⚠ STAL реализуется компонентом «Сервер терминалов», который может быть установлен на узел совместно с Termidesk, в соответствии с подразделом **Установка STAL** документа СЛЕТ.10001-01 90 07 «Руководство администратора. Настройка компонента «Сервер терминалов».

Для добавления в Termidesk сервера терминалов администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 13).

Таблица 13 – Данные для добавления сервера терминалов

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Адрес сессионного агента»	**FQDN** узла, на котором установлен сессионный агент Termidesk ⚠ Для инфраструктуры MS RDS в этом параметре обязательно нужно указывать не IP-адрес, а FQDN узла. Для STAL можно указать внешний IP-адрес узла. Если STAL установлен на одном узле с Termidesk, нужно также указывать внешний IP-адрес узла. Перед изменением FQDN или IP-адреса STAL необходимо завершить все активные сессии. После смены FQDN или IP-адреса STAL активные сессии, связанные с предыдущим FQDN или IP-адресом, становятся недоступными. Для восстановления доступа к STAL необходимо удалить предыдущие сессии и выполнить новое подключение.
«Порт сессионного агента»	Номер порта сессионного агента Termidesk. По умолчанию номер порта 31000
«Домен»	Наименование домена для подключения к серверу терминалов
«Логин»	Субъект, имеющий полномочия для управления сервером терминалов. Для подключения STAL в домене MS AD необходимо указывать логин локального администратора ОС узла, на котором установлен STAL. В ином случае тест соединения для поставщика может пройти успешно, но шаблон рабочего места при этом добавить не получится
«Пароль»	Набор символов, подтверждающий назначение полномочий
«Использовать HTTPS»	Выбор использования протокола HTTPS для запросов к сессионному агенту. По умолчанию выключено. При включении параметра на сервере терминалов должны быть добавлены валидные сертификаты и установлена опция `USE_HTTPS` в значение «True» в конфигурационном файле сессионного агента. В случае необходимости использовать протокол HTTP нужно отключить данный параметр и установить опцию `USE_HTTPS` в значение «False» в конфигурационном файле сессионного агента
«Валидация сертификата»	Выбор проверки подлинности сертификата при запросах к сессионному агенту. По умолчанию выключено

⚠ Если после попытки проверить введенные данные экранной кнопкой **[Тест]** появляются сообщения об ошибке, то при создании шаблона BPM будет блокироваться возможность его сохранения (создания).

⚠ Для корректного подключения через компонент «Клиент» к серверу терминалов необходимо задать параметр «Механизм обеспечения безопасности на уровне сети (RDP)» в политиках конкретного фонда BPM («Рабочие места - Фонды») в соответствии с выбранным сервером:

- «TLS» или «RDP» - для подключения к STAL;
- «NLA» - для подключения к MS RDS.

4.10 . Добавление сервера терминалов (метапровайдер) в качестве поставщика ресурсов

Для возможности добавления поставщика ресурсов «Сервер терминалов (метапровайдер)» необходимо включить экспериментальный параметр `experimental.metasessions.provider.enabled` в соответствии с подразделом **Управление экспериментальными параметрами Termidesk**.

Метапровайдер нужен для тиражирования приложений через мультиплицирование (размножение) ВМ на платформе виртуализации. Данный подход не требует полностью развернутой инфраструктуры терминальных серверов.

Алгоритм подготовки для добавления метапровайдера выглядит следующим образом:

- на платформе виртуализации создается ВМ с гостевой ОС Windows Server (2016 и выше) (для тиражирования приложений Windows) или ОС Astra Linux Special Edition 1.7 (Server) (для тиражирования приложений Astra Linux Special Edition);
- в гостевую ОС устанавливается и настраивается агент BPM и сессионный агент (см. документ СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»);
- для тиражирования приложений Windows в гостевую ОС Windows Server устанавливается роль сервера публикации приложений «Remote Desktop Session Host» из состава «Remote Desktop Services», затем выполняется активация роли при помощи сессионного агента (см. подраздел **Активация роли сервера терминалов в ОС Microsoft Windows Server** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»). Если ОС Windows Server не вводится в домен, то в ОС следует создать пользователя с правами доступа к удалённому рабочему столу;
- для тиражирования приложений Astra Linux Special Edition устанавливается STAL. Для установки STAL следует обратиться к документу СЛЕТ.10001-01 90 07 «Руководство администратора. Настройка компонента «Сервер терминалов»);
- необходимые приложения должны быть вручную опубликованы, для MS RDS используется утилита `RemoteApp Tool`. Для STAL основной список приложений, предлагаемый ОС Astra

Linux Specsial Edition, уже доступен к публикации. При необходимости опубликовать нестандартное приложение следует обратиться к документу СЛЕТ.10001-01 90 07 «Руководство администратора. Настройка компонента «Сервер терминалов»;

- на этом этапе подготовка завершена, ВМ выключается;

ⓘ В гостевой ОС должен быть настроен встроенный межсетевой экран для доступа по портам протокола RDP.

- в графическом интерфейсе управления Termidesk создается поставщик ресурсов с той платформой виртуализации, на которой создана ВМ сервера публикации приложений (см. раздел **Поставщики ресурсов**);
- в созданном поставщике ресурсов создается шаблон ВРМ (см. раздел **Виртуальные рабочие места**), в параметре «Базовая ВМ» выбирается подготовленная ВМ сервера публикации приложений;
- в графическом интерфейсе управления Termidesk создается сервисный фонд ВРМ для созданного шаблона ВРМ (см. подраздел **Добавление фонда ВРМ**). В сервисном фонде **не** указываются группы пользователей, пользователи, протоколы доставки. Сервисный фонд должен использовать кеш 1 уровня (кеш 2 уровня не используется) ;

⚠ Хотя бы одно ВРМ должно получить статус «Действительный» во вкладке «Рабочие места» созданного фонда, иначе все дальнейшие действия будут завершаться ошибкой «Не удалось найти подходящую для подключения машину».

- в графическом интерфейсе управления Termidesk после включения экспериментального параметра `experimental.metasessions.provider.enabled` перейти в «Компоненты - Поставщики ресурсов», а затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка «Сервер Терминалов Метапровайдер». Необходимо добавить поставщик ресурсов, заполнив данные, приведенные ниже;
- после добавления поставщика ресурсов «Сервер терминалов (метапровайдер)» станет доступным создание шаблона ВРМ для него (см. подраздел **Шаблоны ВРМ для метапровайдера**). Необходимо создать шаблон ВРМ;
- в графическом интерфейсе управления Termidesk добавить фонд ВРМ (см. подраздел **Добавление фонда ВРМ**) для публикуемого приложения, указав при добавлении созданный шаблон ВРМ для метапровайдера.

⚠ При необходимости публикации нескольких приложений, необходимо создавать шаблон ВРМ для метапровайдера и фонд ВРМ для каждого приложения.

⚠ Перед изменением FQDN или IP-адреса метапровайдера необходимо завершить все активные сессии. После смены FQDN или IP-адреса метапровайдера активные сессии, связанные с предыдущим FQDN или IP-адресом, становятся недоступными. Для восстановления доступа к метапровайдеру необходимо удалить предыдущие сессии и выполнить новое подключение.

Для добавления в Termidesk сервера терминалов администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 14).

Таблица 14 – Данные для добавления сервера терминалов (метапровайдер)

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Порт сессионного агента»	Номер порта сессионного агента Termidesk. По умолчанию номер порта 31000
«Домен»	Наименование домена для подключения к серверу терминалов
«Логин»	Субъект, имеющий полномочия для управления сервером терминалов
«Пароль»	Набор символов, подтверждающий назначение полномочий
«Фонд»	Выбор **сервисного фонда** для размещения
«Использовать HTTPS»	Выбор использования протокола HTTPS для запросов к сессионному агенту. По умолчанию выключено. При включении параметра на сервере терминалов должны быть добавлены валидные сертификаты и установлена опция `USE_HTTPS` в значение «True» конфигурационном файле сессионного агента. В случае необходимости использовать протокол HTTP нужно отключить данный параметр и установить опцию `USE_HTTPS` в значение «False» в конфигурационном файле сессионного агента
«Валидация сертификата»	Выбор проверки подлинности сертификата при запросах к сессионному агенту. По умолчанию выключено
«Модифицированный способ балансировки»	Выбор модифицированного способа балансировки пользователей. По умолчанию выключен (используется стандартная балансировка, описанная ниже). Модифицированный способ балансировки учитывает наличие активной или отключенной сессии у пользователя для его переподключения. Для экономии серверных ресурсов рекомендуется включить параметр

Подключения пользователей при доступе к опубликованным через метапровайдер приложениям по умолчанию балансируются: при запросе одного и того же приложения разные пользователи будут подключаться к разным серверам.

Пример: пользователь «1» запрашивает приложение «notepad.exe», при этом подключается к серверу «1». Пользователь «2» тоже запрашивает приложение «notepad.exe», но при этом автоматически подключается уже к серверу «2».

Максимальное количество подключений к ноде метапровайдера можно задать командой `termidesk-vdi-manage`, предварительно переключившись на пользователя `termidesk`:

```
:~$ sudo -u termidesk bash
:~$ /opt/termidesk/sbin/termidesk-vdi-manage tsdk_config set --section
Experimental --key experimental.plugins.metasessionsprov.maxConnectionCount --
value <значение>
```

4.11 . Добавление поставщика ресурсов «Физическая рабочая станция»

Для возможности добавления физической рабочей станции как поставщика ресурсов необходимо включить экспериментальный параметр `experimental.provider.physmachine.enabled` в соответствии с подразделом **Управление экспериментальными параметрами Termidesk**.

Физическая рабочая станция должна быть доступна для подключения по протоколу RDP.

После включения экспериментального параметра в графическом интерфейсе управления перейти в «Компоненты - Поставщики ресурсов», а затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка «Static IP Machines».

Для добавления поставщика ресурсов администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 15).

Таблица 15 – Данные для добавления физической рабочей станции как поставщика ресурсов

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов

4.12 . Добавление поставщика Openstack

Для возможности добавления поставщика ресурсов Opencstack необходимо включить экспериментальный параметр `experimental.openstack.provider.enabled` в соответствии с подразделом **Управление экспериментальными параметрами Termidesk**.

Затем в графическом интерфейсе управления перейти в «Компоненты - Поставщики ресурсов», а затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка «OpenStack Platform».

Для добавления поставщика ресурсов Openstack администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 16).

Таблица 16 – Данные для добавления поставщика ресурсов Openstack

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Имя хоста»	IP-адрес или FQDN сервиса аутентификации
«Порт»	Порт для подключения к Openstack, по умолчанию 5000
«Путь»	Опциональная составляющая URI
«Использовать SSL»	Включение использования протокола SSL
«Проверять SSL»	Включение строгой проверки SSL
«Интерфейс доступа»	Идентификатор интерфейса доступа Openstack
«Домен»	Идентификатор домена Openstack
«Пользователь»	Субъект, имеющий полномочия для управления в Openstack
«Пароль»	Набор символов, подтверждающий назначение полномочий
«Количество одновременно создаваемых ВМ»	Количество одновременно создаваемых ВМ на платформе
«Количество одновременно удаляемых ВМ»	Количество одновременно удаляемых ВМ с платформы
«Таймаут»	Максимальное время ожидания (в секундах) отклика от Openstack

4.13 . Режим техобслуживания поставщика ресурсов

Режим техобслуживания предназначен для плановых регламентных или аварийных режимах работы поставщика ресурсов. В режиме техобслуживания Termidesk не использует поставщика ресурсов для размещения фондов ВРМ.

Для перевода поставщика ресурсов в режим техобслуживания следует перейти «Компоненты - Поставщики ресурсов» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить» (см. Рисунок 10). Затем подтвердить включение режима (см. Рисунок 11).

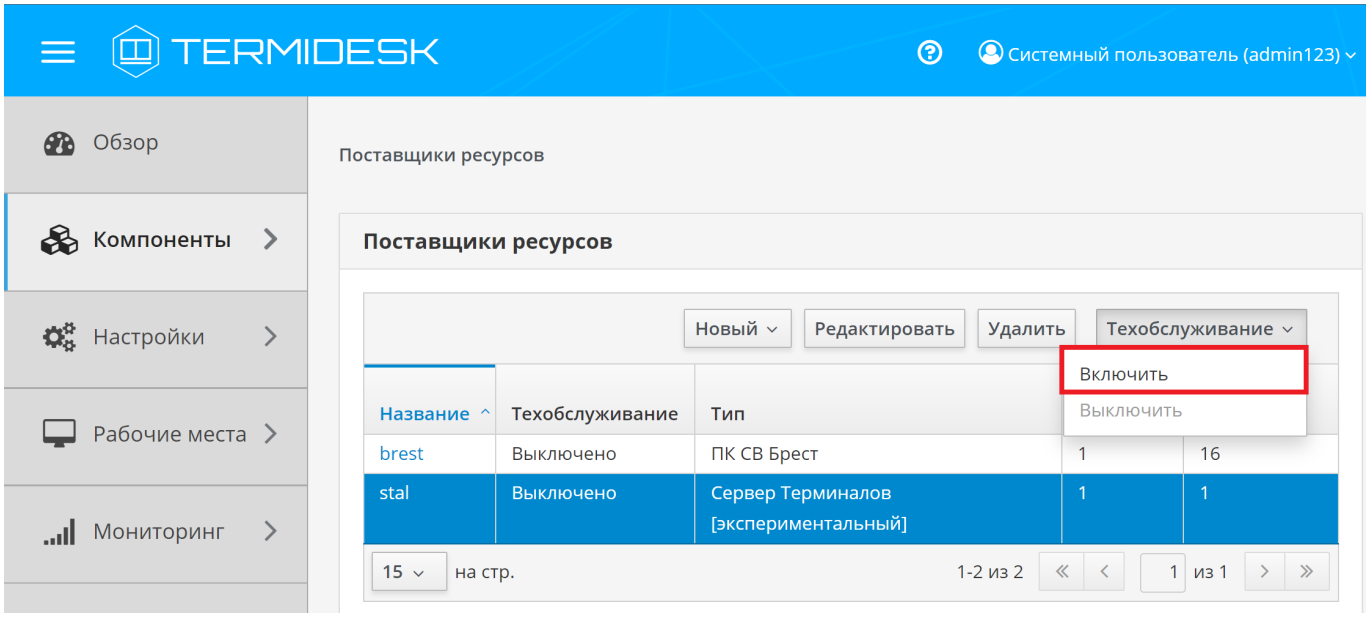

Рисунок 10 – Включение режима техобслуживания поставщика ресурсов

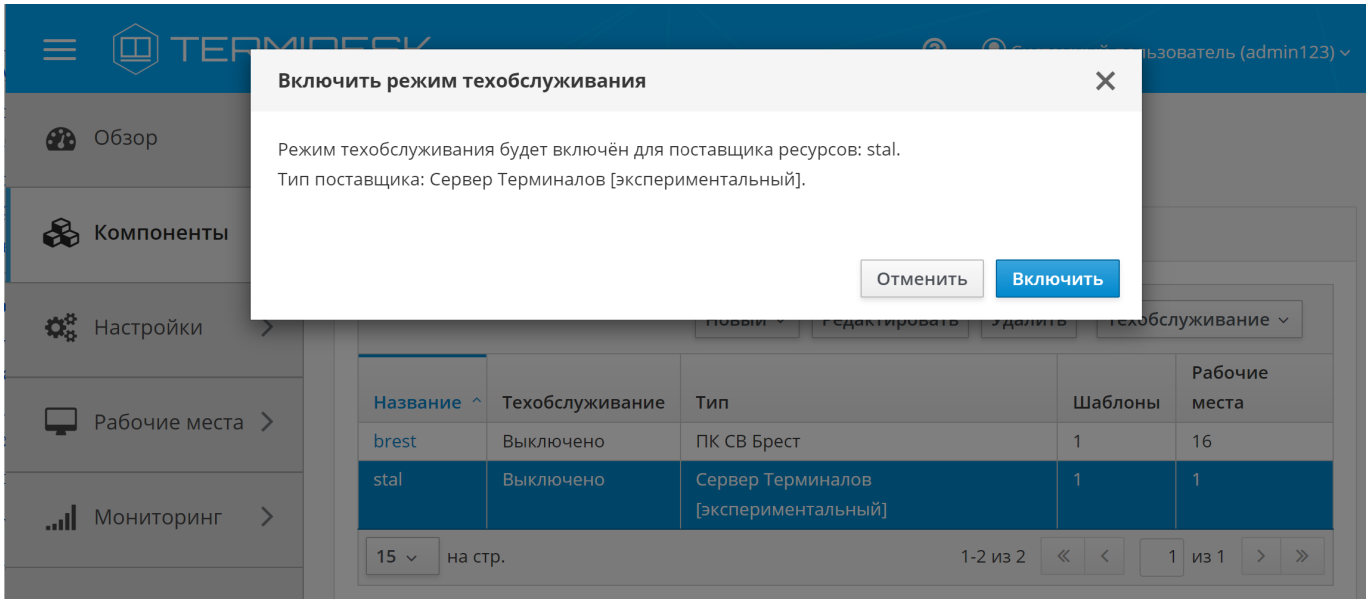

Рисунок 11 – Подтверждение включения режима техобслуживания

Состояние режима техобслуживания будет отображено в столбце «Техобслуживание» списка поставщиков ресурсов.

Для отключения режима техобслуживания нужно выбрать поставщика ресурсов, нажать экранную кнопку **[Техобслуживание]**, а затем выбрать из выпадающего списка значение «Выключить».

По завершении техобслуживания поставщик ресурсов может быть снова использован Termidesk для размещения фондов ВРМ.

5 . АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

5.1 . Общие сведения о доменах аутентификации

Домен аутентификации - источник сведений о субъектах и их полномочиях.

В Termidesk поддерживаются следующие домены аутентификации:

- FreeIPA;
- SAML;
- IP-аутентификация;
- MS AD или LDAP;
- RADIUS.

Поддержка некоторых доменов аутентификации может добавляться в режиме экспериментальных функций.

Для добавления в Termidesk домена аутентификации в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Новый]** и выбрать из выпадающего списка нужный домен аутентификации.
Каждый домен аутентификации описывается перечнем параметров, требуемых для получения идентификаторов субъектов и информации о полномочиях. Проверить корректность указанных параметров можно при помощи экранной кнопки **[Тест]**, расположенной в том же окне. Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Сохранить]**.

> ⚠ Следует предусмотреть, что в целях безопасности учетная запись для биндинга (подключения) к домену не должна иметь прав на удаление или изменение объекта типа «пользователь».

Созданный домен аутентификации можно отредактировать. Для этого в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем пометить необходимый домен аутентификации и нажать экранную кнопку [Редактировать] (см. Рисунок 12).

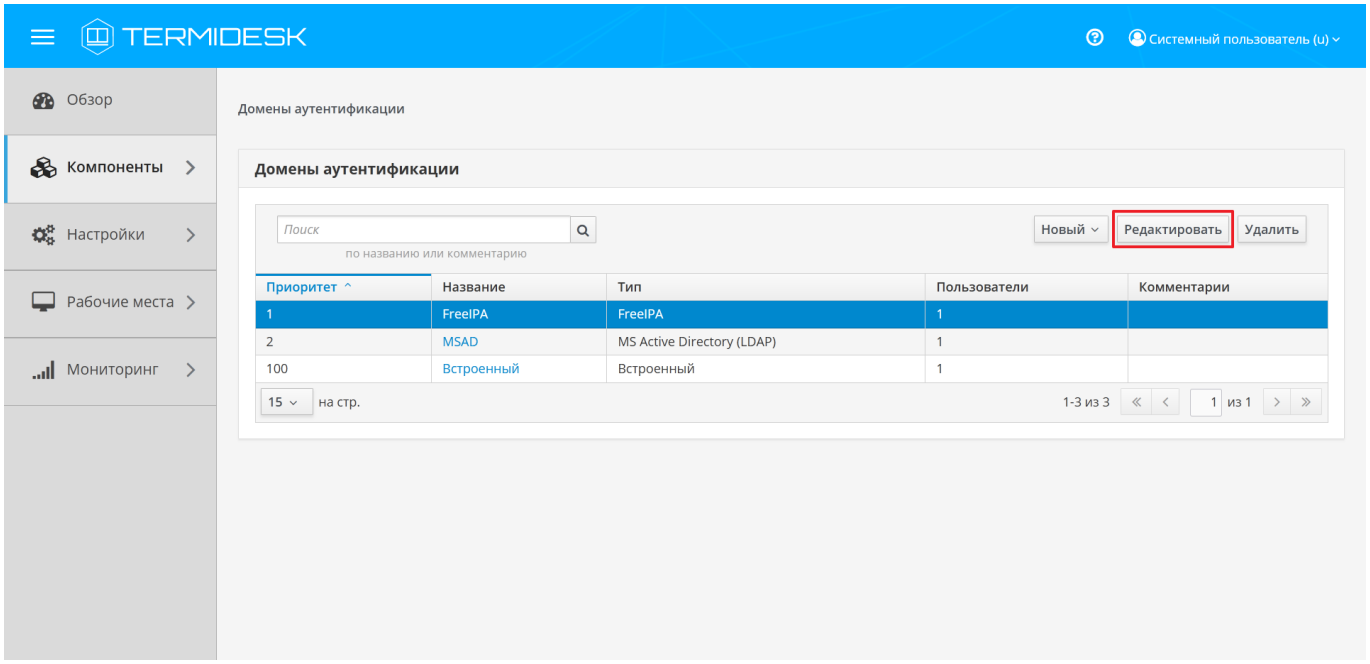

Рисунок 12 – Окно выбора домена аутентификации для редактирования

Созданный домен аутентификации можно при необходимости удалить. Для этого в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем пометить нужный домен аутентификации и нажать экранную кнопку **[Удалить]**.

5.2 . Добавление аутентификации через FreeIPA

Для добавления в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Новый]** и выбрать из выпадающего списка «FreeIPA».

Для добавления в Termidesk аутентификации через FreeIPA администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 17).

Таблица 17 – Данные для добавления аутентификации через FreeIPA

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Сервисный аккаунт»	Название сервисного аккаунта, созданного при добавлении поставщика ресурсов

Параметр	Описание
«Домен»	Идентификатор области Kerberos для аутентификации
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (пример формирования файла приведен в подразделе **Получение и добавление файла keytab**). Каждая генерация `keytab` должна производиться в новый файл. При необходимости повторного использования имени файла существующий файл **обязательно** должен быть удален перед генерацией. Неважно, для какого узла создан `keytab`, необходимо само его наличие
«Сервер FreeIPA»	FQDN ресурса, являющегося источником сведений о субъектах и их полномочиях
«Проверка SSL»	Проверка использования SSL
«Группа администраторов»	Название группы, членам которой предоставляются функции администрирования Termidesk

При добавлении второго домена аутентификации FreeIPA (или доменов, основанных на FreeIPA, например, программного комплекса «ALD PRO») необходимо создать новый файл `keytab` и задать ему имя, отличное от уже существующего.
Добавление второго домена аутентификации не отличается от добавления первого.

При необходимости ввода в домен FreeIPA, развернутый на ОС Astra Linux Special Edition, BPM с другой гостевой ОС Linux, необходимо внести изменения в файл `/usr/lib/python3.6/site-packages/ipalib/constants.py` (см. подраздел **Подготовка базового BPM**).

Для возможности подключения двухфакторной аутентификации нужно включить экспериментальный параметр `experimental.2fa.enabled` (см. подраздел **Управление экспериментальными параметрами Termidesk**).

После включения параметра при переходе «Компоненты - Домены аутентификации» и нажатия экранной кнопки **[Новый]** появятся новые домены аутентификации «FreeIPA, эксперим.» и «FreeIPA, нативн., эксперим.».

Termidesk не реализует непосредственно механизм аутентификации. На контроллере домена FreeIPA должна быть подключена двухфакторная аутентификация, только после этого ее необходимо добавить в Termidesk, как приведено выше.

5.3 . Добавление аутентификации через ALD

Добавление программного комплекса «ALD PRO» в качестве домена аутентификации производится через добавление FreeIPA.

Для добавления в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Новый]** и выбрать из выпадающего списка «Astra Linux Directory».

Для добавления в Termidesk аутентификации через Astra Linux Directory (далее - ALD) администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (see page 0).

Таблица 18 – Данные для добавления аутентификации через ALD

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Сервисный аккаунт»	Название сервисного аккаунта, созданного при добавлении поставщика ресурсов
«Домен»	Идентификатор области Kerberos для аутентификации
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (пример формирования файла приведен в подразделе **Получение и добавление файла keytab**). Каждая генерация `keytab` должна производиться в новый файл. При необходимости повторного использования имени файла существующий файл **обязательно** должен быть удален перед генерацией. Неважно, для какого узла создан `keytab`, необходимо само его наличие
«Группа администраторов»	Название группы, членам которой предоставляются права администрирования Termidesk
«Сервер LDAP (ALD)»	Доменное имя ресурса, являющегося источником сведений о субъектах и их полномочиях
«Таймаут подключения»	Время ожидания (в секундах) ответа ресурса, являющегося источником сведений о субъектах и их полномочиях
«Base DN»	Корень поиска в домене аутентификации

5.4 . Добавление аутентификации через SAML

Провайдер SAML - это единая точка входа пользователей в распределенной системе, позволяющей аутентифицироваться в разных и несвязных между собой частях системы посредством веб-браузера. Независимо от того, какой используется тип биндинга (binding), всегда происходит перенаправление на страницу аутентификации «Провайдер SAML».

Для добавления в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Новый]** и выбрать из выпадающего списка «SAML».

Для добавления в Termidesk аутентификации через SAML администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 19).

Таблица 19 – Данные для добавления аутентификации через SAML

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Приоритет использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«ID клиента»	Уникальный идентификатор клиента на сервисе аутентификации SAML
«URL метаданных»	URL для подключения к сервису аутентификации SAML
«Проверка SSL»	Строгая проверка SSL-сертификатов
«Тип биндинга»	Способ отправки ответа сервисом SAML на запрос аутентификации. Поддерживаются следующие типы: `HTTP-Redirect`, `HTTP-POST`
«Response Binding Type»	Выбор типа биндинга для обратного перенаправления в SAML-запросе. Поддерживаются следующие типы: `HTTP-Redirect`, `HTTP-POST`
«Приватный ключ»	Набор символов приватного ключа для подписи SAML-запросов
«Формат Name ID»	Формат сопоставления идентификаторов имен SAML у поставщиков удостоверений и поставщиков услуг
«Group Attr Name»	Тип атрибута пользователя (обычно в этом поле указывается значение `Group`)
«Таймаут»	Время ожидания ответа от SAML, в секундах

Для работы с сертификатами при получении метаданных от домена аутентификации SAML необходимо установить корневой сертификат центра сертификации и настроить Termidesk на работу с сертификатами (см. подраздел **Установка корневого сертификата центра сертификации**).

5.5 . Добавление IP-аутентификации

Для добавления в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Новый]** и выбрать из выпадающего списка «IP аутентификация».

Домен «IP аутентификация» позволяет определять назначение прав на основе сетевых адресов. Для добавления в Termidesk IP-аутентификации администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 20).

Таблица 20 – Данные для добавления IP-аутентификации

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения домена аутентификации
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Разрешить проксирование»	Разрешить субъектам доставку BPM, находящихся за прокси-сервером

5.6 . Добавление аутентификации через MS AD (LDAP)

Для добавления в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», а затем нажать экранную кнопку **[Новый]** и выбрать из выпадающего списка «MS Active Directory (LDAP)».

Для добавления в Termidesk аутентификации через LDAP администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 21).

Таблица 21 – Данные для добавления аутентификации через MS AD (LDAP)

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения домена аутентификации
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Сервер LDAP»	IP-адрес или доменное имя сервера, являющегося источником сведений о субъектах и их полномочиях

Параметр	Описание
«Порт»	TCP-порт, на котором запущена служба домена аутентификации
«Использовать SSL»	Использовать защищенное соединение при взаимодействии с доменом аутентификации
«Учетная запись»	Учетная запись в формате Distinguished Name (DN) в домене MS AD (LDAP), используемая для подключения к LDAP. Пример: `CN=admin,OU=user,DC=test,DC=desk`
«Пароль учетной записи»	Набор символов, подтверждающий полномочия объекта для подключения к серверу LDAP
«Таймаут»	Время ожидания (в секундах) ответа ресурса, являющегося источником сведений о субъектах и их полномочиях
«Корень поиска»	Корень поиска в домене аутентификации в формате DN. Пример: `DC=test,DC=desk`
«Имя класса пользователя»	Атрибут класса пользователя в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «Person»)
«Атрибут идентификатора пользователя»	Атрибут уникального имени или идентификатора пользователя в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «SamAccountName»)
«Список атрибутов пользователя»	Список атрибутов, содержащий уникальные данные пользователя, разделенные запятыми (для корректного заполнения данного поля необходимо указать значение «name»)
«Имя атрибута группы»	Атрибут принадлежности к группе в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «group»)
«Атрибут имени группы»	Идентификатор группы, к которой относится субъект в домене аутентификации. Если включены параметры «Использовать рекурсивный поиск групп» или «Использовать обратный порядок проверки членства пользователей», то необходимо указать значение «distinguishedname». Если указанные параметры отключены, то можно использовать значение «cn». При использовании значения «distinguishedname» при добавлении группы в домен аутентификации по пути «Компоненты - Домены аутентификации - Наименование домена - Группы» нужно задавать длинные имена групп, например: `CN=Корневая группа,CN=Users,DC=test,DC=desk`. При использовании значения «cn» нужно использовать короткие имена групп. Если параметр «Атрибут имени группы» был изменен, то необходимо заново добавить группы, используя соответствующие имена групп: для «cn» - короткие имена, для «distinguishedname» - длинные имена
«Атрибут членства в группе»	Идентификатор группы для назначения полномочий субъекту (для корректного заполнения данного поля необходимо указать значение «member»)
«Атрибут групп для LDAP-запросов»	Атрибут, определяющий группы пользователя при запросах к службе каталогов. Возможные значения: «objectClass», «objectCategory»
«Использовать рекурсивный поиск групп»	При запросе групп пользователя будут учтены его родительские группы, в которых он состоит неявно. Если дополнительно включен параметр «Использовать обратный порядок проверки членства пользователей», то параметр «Использовать рекурсивный поиск групп» можно не включать

Параметр	Описание
«Использовать обратный порядок проверки членства пользователей»	Проверка соответствия членства пользователя в группах домена аутентификации членству в группах Termidesk. Для работы функционала необходимо, чтобы был задан параметр «Атрибут имени группы». При большом количестве групп непосредственно в домене аутентификации MS AD (LDAP) нужно включить этот параметр. В этом случае сначала будет проверяться вхождение пользователя в группы в Termidesk (в том числе рекурсивно), затем будет происходить проверка найденных групп на сервере MS AD (LDAP). При выключении этого параметра применяется настройка выбора Атрибут групп для LDAP-запросов: «objectClass» или «objectCategory». При включении этого параметра всегда применяется настройка выбора Атрибут групп для LDAP-запросов: «objectClass».

5.7 . Добавление домена аутентификации RADIUS

Для добавления домена аутентификации RADIUS необходимо включить экспериментальный параметр `experimental.radiusauth.enabled` в соответствии с подразделом **Управление экспериментальными параметрами Termidesk**.

После включения экспериментального параметра в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Новый]** и выбрать из выпадающего списка «Radius».

Затем администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 22).

Таблица 22 – Данные для добавления аутентификации Radius

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Radius сервер»	IP-адрес или доменное имя ресурса, являющегося источником сведений о субъектах и их полномочиях (сервер RADIUS)
«Аутентификационный порт»	Порт для обработки запросов на аутентификацию
«Секрет»	Набор символов (пароль), подтверждающий подключение к серверу RADIUS
«Таймаут»	Максимальное время ожидания (в секундах) для установки соединения

Валидация заданных параметров экранной кнопкой **[Тест]** проверяет корректность заданного имени сервера (возможность получить IP-адрес, используя DNS), доступность сервера (корректный порт, работоспособность сервера RADIUS).

После добавления домена аутентификации RADIUS необходимо перейти в созданный объект и указать актуальный список групп, пользователи которых могут производить вход в Termidesk.

При дальнейшей эксплуатации сервер Termidesk, обрабатывая запрос на аутентификацию, получает актуальный список групп пользователя и сравнивает со своей конфигурацией. Если ни одного совпадения не обнаружено, то пользователю будет отказано в доступе.

⚠ Конфигурация сервера RADIUS должна учитывать передачу списка групп пользователя в атрибуте с ключом 25 (Class) в ответе со статусом авторизации.

Для корректного получения списка групп на Termidesk сервер RADIUS может быть настроен следующим образом:

⚠ Пример настройки приведен для сервера freeRADIUS.

- файл `/etc/freeradius/3.0/mods-enabled/ldap` должен содержать конструкцию вида:

```
ldap {
...
  update {
     ...
     reply:memberOf                  += 'memberOf'
  }
...
}
```

- в файл `/etc/freeradius/3.0/dictionary` необходимо добавить строку:

```
ATTRIBUTE       memberOf                3001    string
```

- в файле `/etc/freeradius/3.0/sites-enabled/default` необходимо найти секцию `post-auth` и добавить регулярное выражение, фильтрующее название группы из получаемых от сервера атрибутов:

```
foreach &reply:memberOf {
       if ("%{Foreach-Variable-0}" =~ /CN=([^,=]+)/) {
             update reply { Class += "%{1}" }
           }
```

- в файле `/etc/freeradius/3.0/mods-enabled/exec` указать для параметра `wait` значение `yes`:

```
wait = yes
```

5.8 . Добавление аутентификации через внутреннюю БД

Для добавления аутентификации пользователей через внутреннюю БД необходимо установить в Termidesk плагин расширения `termidesk_internaldbauth` в соответствии с подразделом **Установка плагинов расширений**.

После установки плагина расширения в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Новый]** и выбрать из выпадающего списка «Внутренняя БД, эксперим.».
Для добавления внутренней БД как домена аутентификации администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 23).

Таблица 23 – Данные для добавления аутентификации через внутреннюю БД

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Разные пользователи для хостов»	Для пользователя, выполняющего вход с разных хостов, будут созданы разные учетные записи
«Обратный просмотр DNS»	Для подключающихся хостов будет производиться обратный просмотр DNS для определения имени хоста по его IP-адресу
«Разрешить проксирование»	Запросы через прокси-сервер будут осуществляться от пересылаемого IP-источника

5.9 . Действия над пользователями в домене аутентификации

Пользователи – перечень объектов, имеющих в рамках домена аутентификации служебные функции на использование фондов BPM.

После входа пользователя в графический интерфейс управления Termidesk доступны следующие действия над пользователями внутри домена аутентификации:

- редактирование;

- удаление;
- просмотр сведений.

> Редактирование и удаление пользователя в домене аутентификации в графическом интерфейсе управления Termidesk не приводит к каким-либо изменениям объекта в службе каталогов.

Для редактирования информации о пользователе следует перейти «Компоненты - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации.

В открывшемся окне в таблице «Пользователи» выделить строку с именем пользователя и нажать экранную кнопку [Редактировать] (см. Рисунок 13).

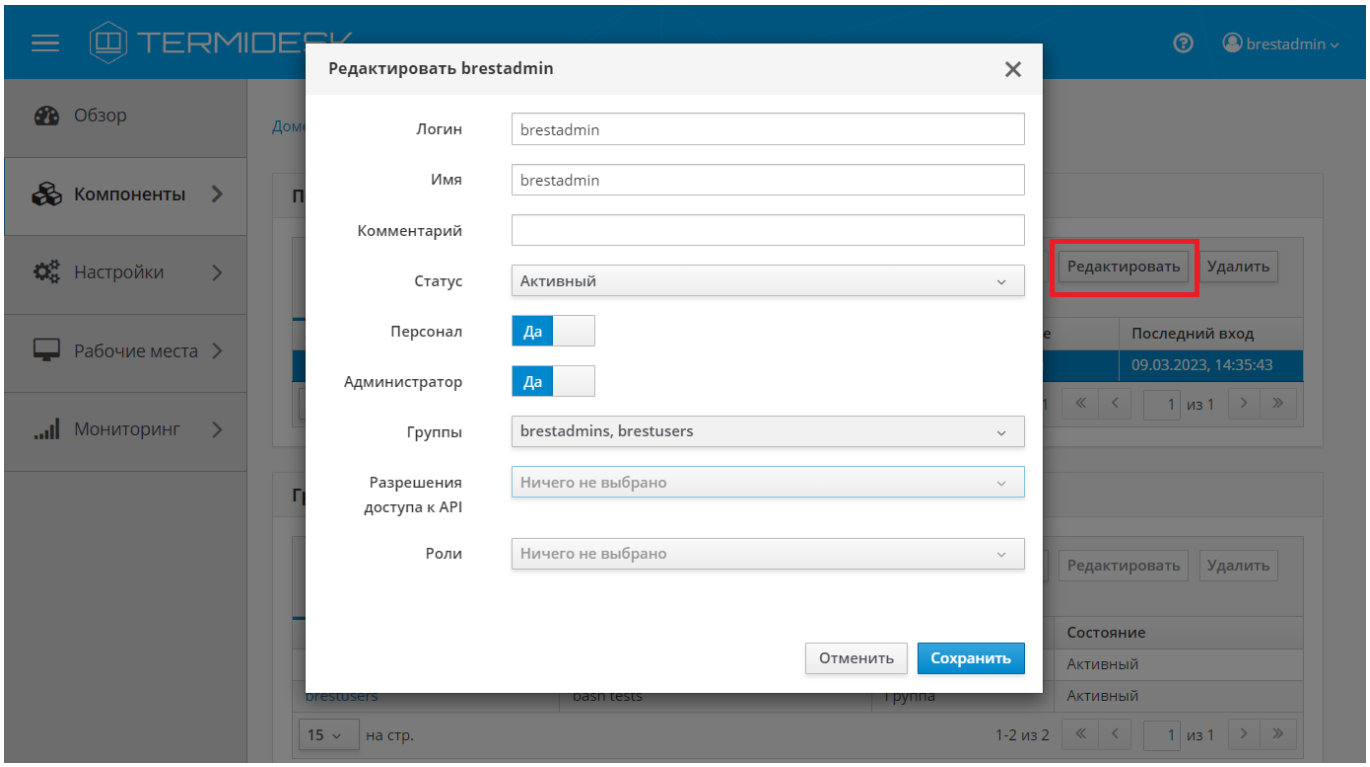

Рисунок 13 – Окно редактирования пользователя домена аутентификации

Для редактирования пользователя администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 24).

Таблица 24 – Данные для редактирования пользователя домена аутентификации

Параметр	Описание
«Логин»	Идентификатор субъекта в домене аутентификации
«Имя»	Отображаемое имя субъекта в Termidesk

Параметр	Описание
«Комментарий»	Информационное сообщение, используемое для описания назначения пользователя
«Статус»	Характеристика состояния субъекта при доступе к фонду BPM
«Персонал»	Служебные функции субъекта при доступе к Termidesk
«Администратор»	Служебные функции субъекта при доступе к графическому интерфейсу управления Termidesk
«Группы»	Наименование групп, используемых для определения разрешений по доступу к фондам BPM
«Разрешения доступа к API»	Полномочия для доступа к API-интеграции с системой резервного копирования
«Роли»	Назначение служебной функции указанному пользователю

Для удаления пользователя из домена аутентификации необходимо перейти в «Компоненты - Домены аутентификации», в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне в таблице «Пользователи» выделить строку с именем пользователя и нажать экранную кнопку **[Удалить]**.

5.10 . Управление аутентификацией на основе адресов сети

Аутентификация на основе адресов сети используется для предоставления доступа к BPM, базируясь на IP-адресе источника, с которого производится запрос к фонду BPM.

Для добавления диапазона сети администратору Termidesk в графическом интерфейсе управления следует перейти «Компоненты - Сети», нажать экранную кнопку **[Новый]**, затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 25).

Таблица 25 – Данные для добавления аутентификации на основе адресов сети

Параметр	Описание
«Название»	Текстовое наименование источника сведений о субъектах и их полномочиях
«Диапазон»	Диапазон сетевых адресов, которые будут использоваться для идентификации субъекта

Созданные таким образом диапазоны можно отредактировать, для этого нужно пометить желаемый диапазон адресов, а затем нажать экранную кнопку **[Редактировать]**.

Для удаления созданного диапазона необходимо пометить желаемый диапазон адресов, а затем нажать экранную кнопку **[Удалить]**.

⚠ Диапазон сетевых адресов может быть удален только в том случае, если он не используется фондом BPM.

6 . ВИРТУАЛЬНЫЕ РАБОЧИЕ МЕСТА

6.1 . Общие сведения о ВРМ

ВРМ - это гостевая ОС, установленная на ВМ, доступ к которой реализуется с помощью протокола удаленного доступа.

Termidesk выполняет подготовку ВРМ на основе заданных шаблонов ВРМ. Каждый поставщик ресурсов поддерживает свой набор типов шаблонов ВРМ.
Поддерживаемый в Termidesk список типов шаблонов ВРМ приведен ниже:

- шаблон на основе связанного клона - предполагает создание ВРМ из базового образа на платформе виртуализации в режиме инкрементного копирования;
- шаблон на основе полного клона - предполагает создание ВРМ из базового образа на платформе виртуализации в режиме полного копирования;
- связанный клон на базе снапшота - предполагает создание ВРМ на основе снимка виртуального жесткого диска базовой ВМ. В этом случае на платформе виртуализации должна быть развернута непосредственно ВМ;
- шаблоны серверов терминалов - предполагает создание ВРМ на основе терминального доступа или доступа к опубликованным на сервере терминалов приложениям.

Для добавления шаблона ВРМ в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.
Далее в открывшемся окне следует нажать на экранную кнопку **[Новый]**, а затем из выпадающего списка выбрать поддерживаемый в Termidesk способ формирования шаблона ВРМ.
Созданные шаблоны ВРМ можно редактировать, для этого необходимо выбрать шаблон, а затем нажать на экранную кнопку **[Редактировать]**.
Созданные шаблоны можно удалить, для этого необходимо выбрать шаблон, а затем нажать на экранную кнопку **[Удалить]**.

⚠ Шаблон может быть удалён только в том случае, если он не используется фондом ВРМ.

6.2 . Отображение списка ВРМ из всех фондов

Для более эффективного администрирования Termidesk предусмотрено отображение ВРМ из всех фондов, в том числе назначенные ВРМ, а также созданные и размещенные в кеше.
Для получения списка необходимо перейти «Рабочие места - Индивидуальные рабочие места» (см. Рисунок 14) или перейти по ссылке «Рабочие места» из функции «Обзор» (см. Рисунок 15). По

умолчанию записи в представленном списке (см. Рисунок 16) будут упорядочены согласно столбцу «Дата создания» по убыванию.

> ⚠ Отображение списка будет доступно администратору, если у него есть пользовательское разрешение «Просмотр фондов рабочих мест».

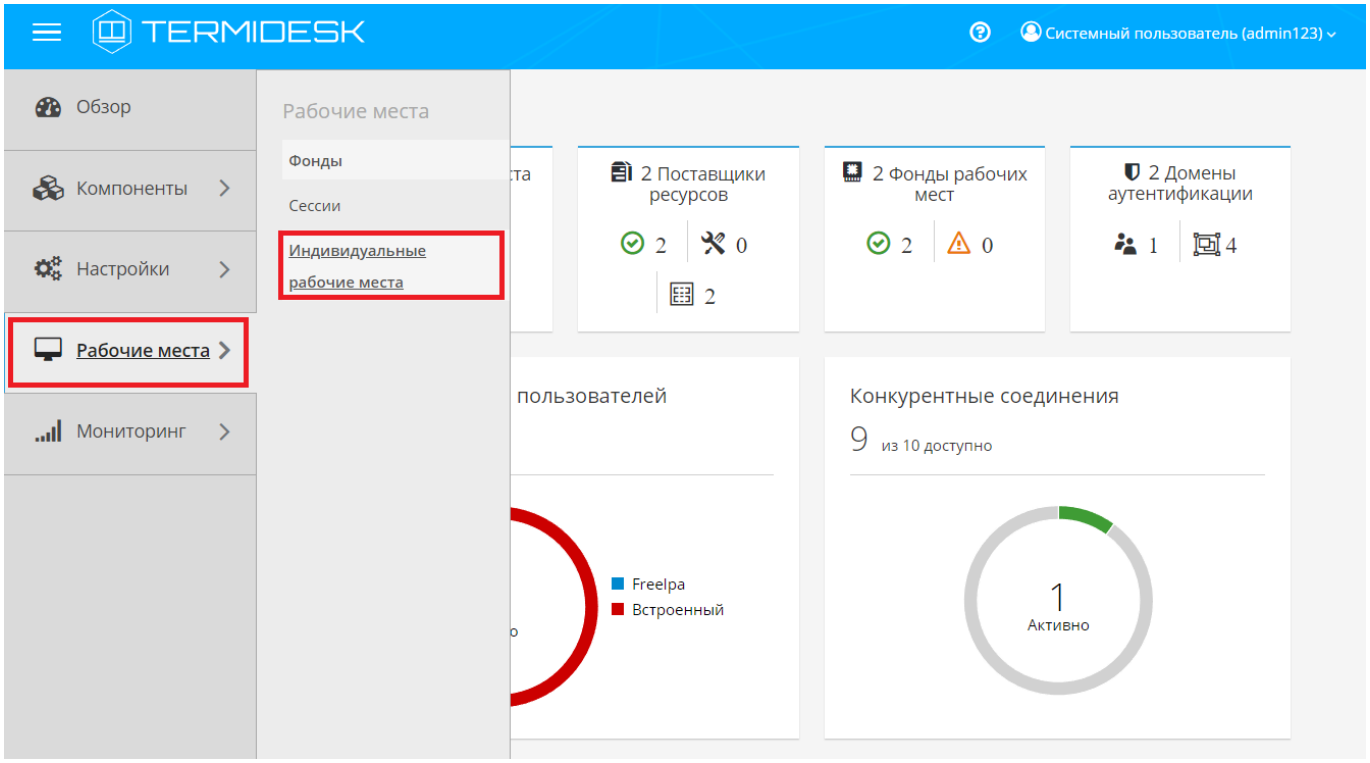

Рисунок 14 – Переход к списку BPM через «Рабочие места - Индивидуальные рабочие места»

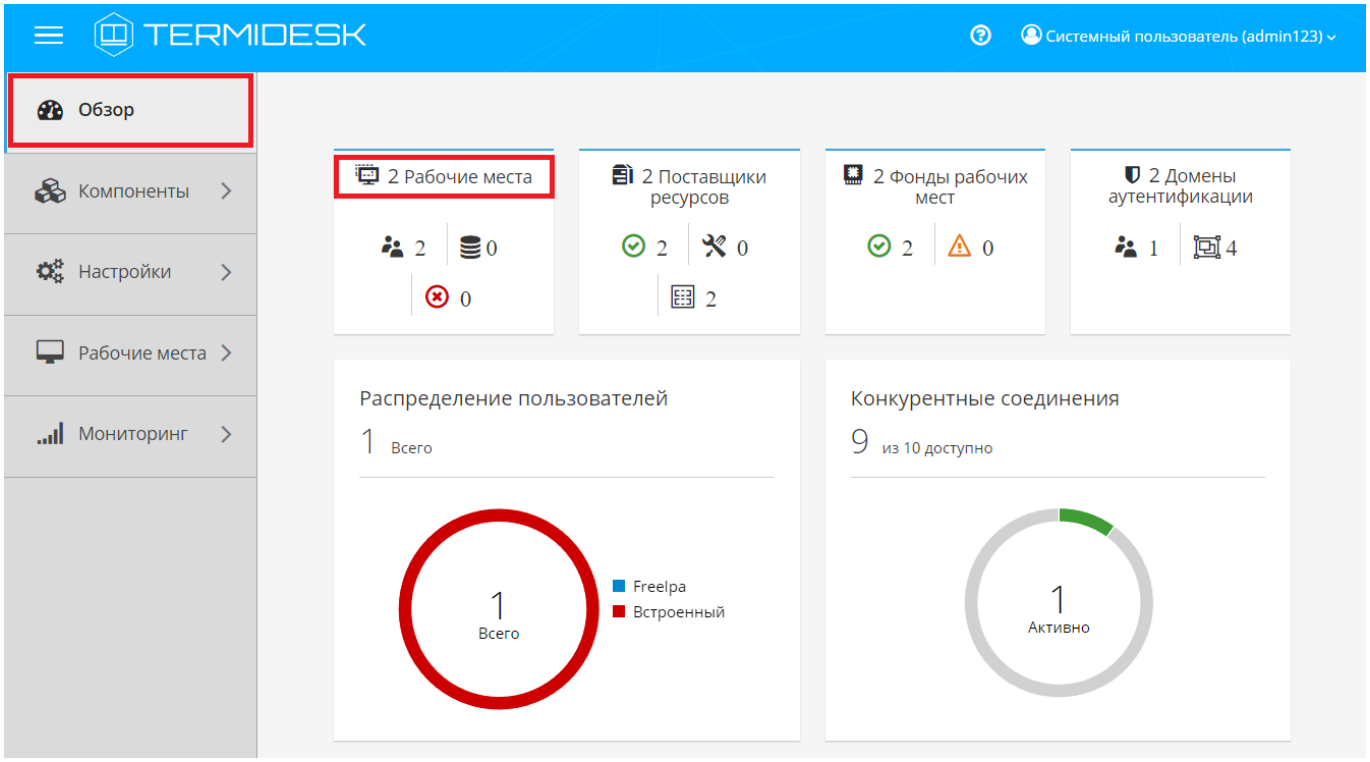

Рисунок 15 – Переход к списку ВРМ через функцию «Обзор»

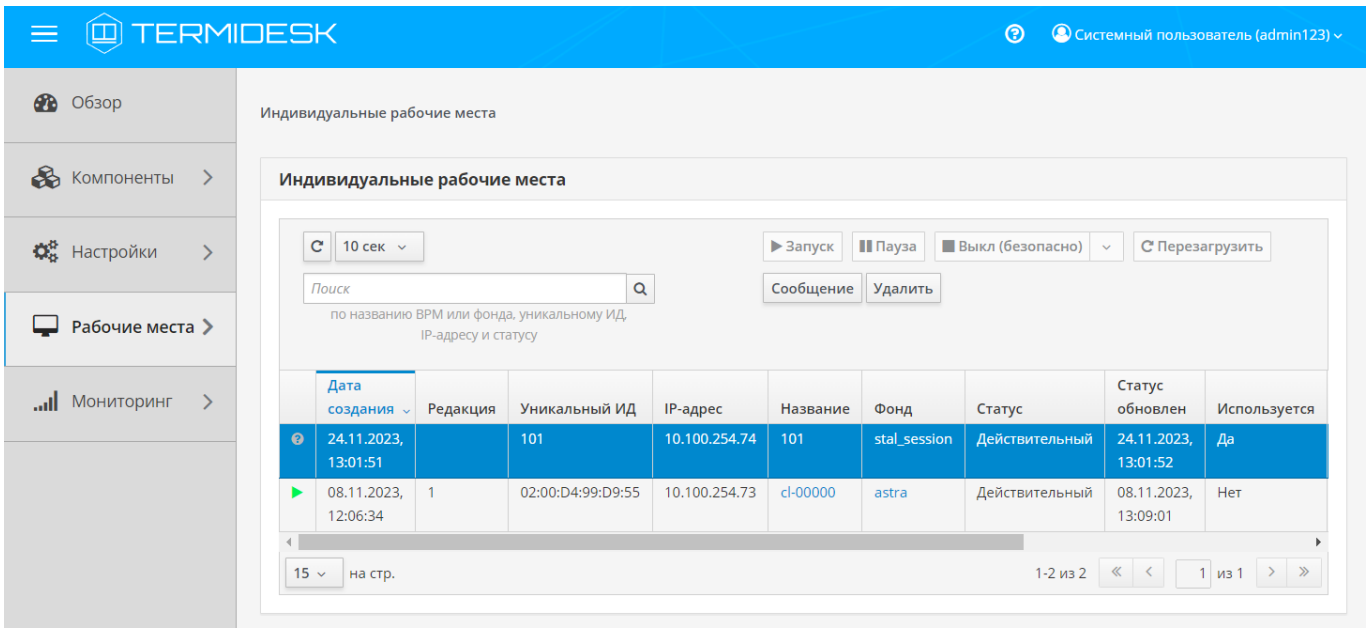

Рисунок 16 – Пример отображения списка ВРМ

Каждая запись списка будет сопровождаться индикацией (см. Таблица 26) состояния ВМ.

Таблица 26 – Индикация состояния ВМ

Индикация	Описание
	Состояние неизвестно. Статус появляется, когда состояние ВМ не подходит под приведенные ниже. Такое состояние также может свидетельствовать, что в фонде, которому принадлежит BPM, не поддерживается управление питанием ВМ. Экранные кнопки **[Запуск]**, **[Пауза]**, **[Выкл (безопасно)]**, **[Перезагрузить]** будут недоступны для использования
	ВМ включена
	ВМ находится в спящем режиме
	ВМ выключена

Основные параметры списка BPM приведены в таблице (см. Таблица 27).

Таблица 27 – Основные параметры списка BPM

Параметр	Описание
«Дата создания»	Временная метка выполнения публикации BPM
«Редакция»	Порядковый номер версии публикации
«Уникальный ИД»	Уникальный идентификатор BPM: MAC-адрес или номер сессии
«IP-адрес»	IP-адрес, назначенный BPM
«Название»	Наименование BPM и ссылка на его журнал
«Фонд»	Наименование фонда BPM и ссылка на него
«Статус»	Флаг использования публикации BPM из фонда BPM
«Статус обновлен»	Временная метка обновления статуса
«Используется»	Флаг назначения BPM. Значение «Нет» свидетельствует о том, что BPM находится в кеше
«Хост источника»	Наименование инициатора выдачи BPM
«IP источника»	IP-адрес инициатора выдачи BPM
«Владелец»	Субъект, инициировавший выдачу BPM
«Версия агента»	Версия компонента «Агент», установленного в гостевой ОС BPM

На странице со списком BPM можно выполнить поиск по:

- наименованию BPM;
- наименованию фонда BPM;
- уникальному идентификатору BPM;
- IP-адресу BPM;

- статусу. Поиск по статусу возможен при **полном** указании наименования статуса в строке поиска, например: «Действительный».

> В строке поиска можно задать множественные параметры, они будут объединены логическим «И»: то есть, результат поиска будет отражать те ВРМ, которые удовлетворяют всем заданным параметрам. В качестве разделителя значений могут быть использованы символы: «,» (запятая), «, » (запятая с пробелом), пробел.

Для отправки сообщения во все назначенные пользователям ВРМ фонда, к которому принадлежит выбранная в списке ВРМ, нужно нажать экранную кнопку **[Сообщение]**. Отправка сообщения возможна, если параметр «Статус» имеет значение «Действительный» или «Подготовка». ВМ при этом необязательно должна находиться в состоянии «Включена» (например, ВМ может быть в состоянии «Приостановлена»).

6.3 . Шаблоны ВРМ для ПК СВ Брест

6.3.1 . Шаблон на основе связанного и полного клона для ПК СВ Брест

Для добавления шаблона администратору Termidesk в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов ПК СВ Брест.

> Если в более ранних версиях Termidesk использовался шаблон «Связанный клон ВМ ПК СВ «БРЕСТ» (non-qcow2)», то при обновлении на новую версию все фонды ВРМ на основе этого шаблона **будут удалены** без дополнительных предупреждений и подтверждений. Перед обновлением на новую версию Termidesk необходимо перевести пользователей на новые фонды ВРМ с шаблоном «Полный клон ВМ ПК СВ «БРЕСТ».

Далее в открывшемся окне нужно нажать на экранную кнопку **[Новый]**, из выпадающего списка выбрать один из шаблонов «Полный клон ВМ ПК СВ «БРЕСТ» или «Связанный клон ВМ ПК СВ «БРЕСТ», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 28).

Таблица 28 – Данные для добавления шаблонов на основе клонов для ПК СВ Брест

Параметр	Описание
«Название»	Текстовое наименование шаблона ВРМ
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона ВРМ
«Хранилище»	Идентификатор ресурсов хранения, представленных в платформе виртуализации, используемых для размещения файлов ВМ, входящих в фонд ВРМ

Параметр	Описание
«Базовый шаблон»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут создаваться ВРМ. Базовый образ составляет базовый шаблон ВМ, подготовленный в платформе виртуализации совместно с выполненными в гостевой ОС настройками (см. подразделы **Подготовка базового шаблона ВМ на примере ПК СВ Брест** и **Подготовка базового ВРМ**)
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера текстового наименования, используемая в идентификаторе каждого ВРМ

6.3.2 . Шаблон на базе снапшота для ПК СВ Брест

Для добавления шаблона администратору Termidesk в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов ПК СВ Брест.

Далее в открывшемся окне нужно нажать на экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «Связанный клон базовой ВМ ПК СВ «БРЕСТ» на базе снапшота», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 29).

Таблица 29 – Данные для добавления шаблона на базе снапшота для ПК СВ Брест

Параметр	Описание
«Название»	Текстовое наименование шаблона ВРМ
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона ВРМ
«Хранилище»	Идентификатор ресурсов хранения, представленных в платформе виртуализации, используемых для размещения файлов ВМ, входящих в фонд ВРМ
«Базовая ВМ»	ВМ, на базе которой будут создаваться фонды ВРМ
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера текстового наименования, используемая в идентификаторе каждого ВРМ

6.4 . Шаблоны BPM для платформ oVirt/RHEV, zVirt, «РЕД Виртуализация»

6.4.1 . Шаблон на основе связанного клона для oVirt/RHEV

Для добавления шаблона администратору Termidesk в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне нужно нажать на экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «Связанный клон oVirt/RHEV», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 30).

Таблица 30 – Данные для добавления шаблона на основе связанного клона для oVirt/RHEV

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM
«Кластер»	Идентификатор кластера на платформе oVirt/RHEV, используемый для размещения фондов BPM
«Хранилище»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд BPM
«Место»	Минимально необходимое дисковое пространство на объекте «Хранилище» для размещения файлов ВМ, входящих в фонд BPM
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды BPM
«Память»	Объем оперативной памяти, выделяемый BPM
«Гарантированная память»	Минимальный объем оперативной памяти, резервируемый для BPM
«USB»	Политика разрешения доступа к USB-портам
«Дисплей»	Используемый протокол удаленного доступа к BPM
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого BPM. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера текстового наименования, используемого в идентификаторе каждого BPM

ⓘ ВМ, из которой планируется создать шаблон BPM, может отображаться с некоторой задержкой, если она была только что создана на платформе. В таком случае следует немного подождать, пока она отобразится в параметре «Базовая ВМ».

6.4.2 . Шаблон на основе статичной ВМ для oVirt/RHEV

Для добавления шаблона администратору Termidesk в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне нужно нажать на экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «Статичная ВМ oVirt/RHEV», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 31).

Таблица 31 – Данные для добавления шаблона на основе статичной ВМ для oVirt/RHEV

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM
«ВМ»	Наименование ВМ на платформе виртуализации

ⓘ ВМ, из которой планируется создать шаблон BPM, может отображаться с некоторой задержкой, если она была только что создана на платформе. В таком случае следует немного подождать, пока она отобразится в параметре «ВМ».

6.5 . Шаблоны BPM для VMmanager

6.5.1 . Шаблон BPM на основе образа ВМ

Для добавления шаблона BPM на основе образа ВМ администратору Termidesk необходимо в графическом интерфейсе управления перейти в «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов VMmanager.

Далее в открывшемся окне следует нажать на экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «ВМ из образа», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 32).

ⓘ Для добавления шаблона BPM на основе связанного клона для VMmanager необходимо создать шаблон «ВМ из образа», в котором включить переключатель «Создать как связанный клон».

Таблица 32 – Данные для добавления шаблона на основе образа ВМ

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM

Параметр	Описание
«Кластер»	Идентификатор кластера на платформе VMmanager, используемый для размещения фондов ВРМ
«Образ ВМ»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды ВРМ
«Количество ЦПУ»	Количество процессоров, выделяемых ВМ
«Объем памяти, Мб»	Объем оперативной памяти, выделяемый ВМ
«Объем диска, Мб»	Размер диска, выделяемый ВМ
«Пул ip-адресов»	Идентификатор пула IP-адресов, используемый для ВМ
«Пользовательский скрипт»	Выбор выполняемого пользовательского скрипта
«Пароль root»	Пароль пользователя root
«Доменное имя»	Имя домена для ВМ (опционально)
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера текстового наименования, используемого в идентификаторе каждого ВРМ
«Создать как связанный клон»	Переключатель для управления созданием ВМ в режиме связанного клона

6.5.2 . Шаблон ВРМ на основе статичной ВМ

Для добавления шаблона ВРМ на основе статичной ВМ администратору Termidesk необходимо в графическом интерфейсе управления перейти в «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов VMmanager.

Далее в открывшемся окне следует нажать на экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «Статичная ВМ VMmanager», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 33).

Таблица 33 – Данные для добавления шаблона на основе статичной ВМ

Параметр	Описание
«Название»	Текстовое наименование шаблона ВРМ
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона ВРМ
«Виртуальная машина»	Наименование ВМ на платформе виртуализации

6.6 . Шаблоны BPM для платформ VMware vSphere

Для добавления шаблона администратору Termidesk в графическом интерфейсе управления следует перейти «Компоненты - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов VMware vSphere.

Далее в открывшемся окне нужно нажать на экранную кнопку **[Новый]**, из выпадающего списка выбрать один из доступных шаблонов «Полный клон» или «Связанный клон», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 34).

Таблица 34 – Данные для добавления шаблона для VMware vSphere

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM
«Датацентр»	Идентификатор виртуального центра обработки данных, используемый для размещения ВМ
«Кластер данных»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд BPM
«Кластер ресурсов»	Идентификатор кластера ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд BPM
«Пул ресурсов»	Идентификатор пула ресурсов, используемый для размещения ВМ
«Размещение ВМ»	Идентификатор каталога размещения создаваемых ВМ
«Место (Гб)»	Минимальный размер свободного пространства для размещения ВМ
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды BPM
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого BPM. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера текстового наименования, используемого в идентификаторе каждого BPM

6.7 . Шаблоны BPM для серверов терминалов

6.7.1 . Шаблон BPM для доступа к серверу терминалов MS RDS

Для добавления шаблона администратору Termidesk необходимо в графическом интерфейсе управления перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов сервера терминалов.

Далее в открывшемся окне следует нажать экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «RDS Terminal Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 35).

Таблица 35 – Данные для добавления шаблона для доступа к терминалу MS RDS

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM
«Терминал»	Наименование существующего терминала MS RDS

6.7.2 . Шаблон BPM для доступа к опубликованным приложениям MS RDS

Для добавления шаблона администратору Termidesk необходимо в графическом интерфейсе управления перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов сервера терминалов.

Далее в открывшемся окне следует нажать экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «RDS Remote App Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 36).

Таблица 36 – Данные для добавления шаблона для доступа к приложениям MS RDS

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM
«RDS коллекция»	Название существующей в инфраструктуре MS RDS коллекции опубликованных приложений
«Удалённое приложение»	Наименование опубликованного в коллекции приложения

6.7.3 . Шаблон BPM для доступа к серверу терминалов STAL

Для добавления шаблона администратору Termidesk необходимо в графическом интерфейсе управления перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов сервера терминалов.

Далее в открывшемся окне следует нажать экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «STAL Terminal Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 37).

Таблица 37 – Данные для добавления шаблона для доступа к терминалу STAL

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM

6.7.4 . Шаблон BPM для доступа к опубликованным приложениям STAL

Для добавления шаблона администратору Termidesk необходимо в графическом интерфейсе управления перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов сервера терминалов.

Далее в открывшемся окне следует нажать экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «STAL Remote App Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 38).

Таблица 38 – Данные для добавления шаблона для доступа к приложениям STAL

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM
«Удалённое приложение»	Наименование опубликованного в коллекции приложения

6.8 . Шаблоны BPM для метапровайдера

6.8.1 . Шаблон для публикации приложений

Для добавления шаблона администратору Termidesk необходимо в графическом интерфейсе управления перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов «Сервер терминалов (метапровайдер)».

Далее в открывшемся окне следует нажать экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «Meta Remote App Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 39).

Таблица 39 – Данные для добавления шаблона публикации приложений для метапровайдера

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM
«Удаленное приложение»	Наименование опубликованного приложения

6.8.2 . Шаблон для терминальных сессий

Для добавления шаблона администратору Termidesk необходимо в графическом интерфейсе управления перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов «Сервер терминалов (метапровайдер)».

Далее в открывшемся окне следует нажать экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «Meta Terminal Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 40).

Таблица 40 – Данные для добавления шаблона терминальных сессий для метапровайдера

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM

6.9 . Шаблоны BPM для физической рабочей станции

6.9.1 . Шаблон BPM на основе одного статического IP-адреса

Для добавления шаблона BPM на основе одного статического IP-адреса администратору Termidesk необходимо в графическом интерфейсе управления перейти в «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов «Static IP Machines».

Далее в открывшемся окне следует нажать на экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «Static Single IP», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 41).

Таблица 41 – Данные для добавления шаблона BPM на основе одного IP-адреса

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM
«Machine IP»	IP-адрес ВМ

6.9.2 . Шаблон BPM на основе множественных IP-адресов

Для добавления шаблона BPM на основе множественных IP-адресов администратору Termidesk необходимо в графическом интерфейсе управления перейти в «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов «Static IP Machines».

⚠ Данный шаблон использовать не рекомендуется.

Далее в открывшемся окне следует нажать на экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «Static Multiple IP», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 42).

Таблица 42 – Данные для добавления шаблона BPM на основе множественных IP-адресов

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM

6.10 . Шаблоны BPM для Openstack

6.10.1 . Шаблон BPM на основе образа ВМ

Для добавления шаблона BPM на основе образа ВМ администратору Termidesk необходимо в графическом интерфейсе управления перейти в «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов Openstack.

Далее в открывшемся окне следует нажать на экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «ВМ из образа», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 43).

Таблица 43 – Данные для добавления шаблона на основе образа ВМ для Openstack

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM
«Регион»	Идентификатор кластера на платформе VMmanager, используемый для размещения фондов BPM
«Проект»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды BPM
«Зона доступности»	Выбор зоны доступности ВМ
«Образ диска»	Выбор базового образа диска, ограничен зоной доступности
«Сеть»	Выбор сети, в которой будет расположена ВМ
«Тип диска»	Тип диска ВМ
«Размер диска»	Размер диска ВМ, в Гб
«Конфигурация ВМ»	Выбор конфигурации ВМ, созданной в Openstack
«Группа безопасности»	Выбор группы безопасности, созданной в Openstack

Параметр	Описание
«Префикс имени ВМ»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака «-» (дефис)
«Длина счетчика имен»	Длина порядкового номера текстового наименования, используемого в идентификаторе каждого ВРМ
«Состояние ВМ в кеше 2 уровня»	Выбор состояния ВМ по умолчанию в кеше второго уровня
«Метадата»	Информация о метаданных
«Cloud-init скрипт»	Скрипт cloud-init, выполняемый при создании ВМ

6.10.2 . Шаблон ВРМ на основе статичной ВМ

Для добавления шаблона ВРМ на основе статичной ВМ администратору Termidesk необходимо в графическом интерфейсе управления перейти в «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов Openstack.

Далее в открывшемся окне следует нажать на экранную кнопку **[Новый]**, из выпадающего списка выбрать шаблон «Статичная ВМ», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 44).

Таблица 44 – Данные для добавления шаблона на основе статичной ВМ для Openstack

Параметр	Описание
«Название»	Текстовое наименование шаблона ВРМ
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона ВРМ
«Регион»	Выбор региона, в котором находится ВМ
«Проект»	Выбор проекта, в котором находится ВМ
«Виртуальная машина»	Выбор уникального идентификатора ВМ на платформе виртуализации

6.11 . Настройка переносимых профилей

6.11.1 . Общие сведения

Переносимые профили - это средство для сохранения настроек и документов пользователя между сеансами работы в ВРМ.

Назначение переносимых (второе название - отделяемых) профилей заключается в том, что для каждого пользователя автоматически и по мере необходимости создается образ диска, который подключается к ВРМ.

Действия по настройке переносимых профилей сводятся к следующей последовательности шагов:

1) создание базового образа диска для профилей в ПК СВ Брест;

2) задание созданному образу атрибута `TDSK_SHARED_TYPE` со значением `PRIVATE`;

3) настройка модуля `PAM (pam_tdsk)` в базовом ВРМ;

4) включение механизма переносимых профилей в Termidesk;

5) включение в настройках глобальных политик Termidesk политики «Отделяемый пользовательский профиль».

6.11.2 . Создание базового образа диска в ПК СВ Брест

Для создания переносимого профиля (диска) на платформе ПК СВ Брест необходимо:

- создать постоянный диск требуемого размера и подключить его к ВМ с установленной ОС Astra Linux. При создании выбрать шину SCSI (`DEV_PREFIX=sd`) или Virtio (`DEV_PREFIX=vd`) (см. подраздел **Подготовка базового шаблона ВМ на примере ПК СВ Брест**);

> ⚠ При создании образа на шине Virtio может возникнуть сообщение об ошибке «Error attaching new VM Disk: Could not attach /var/lib/one/datastores/0/248/disk.2 (vdb) to one-248» при подключении диска в ПК СВ Брест версии 2.9.
> В случае возникновения такой ошибки нужно изменить атрибут `DEV_PREFIX` в свойствах образа диска.

- создать текстовый файл `/tmp/sfdisk.gpt` и привести его к виду:

```
label:gpt
type=773f91ef-66d4-49b5-bd83-d683bf40ad16
```

> ⚠ Важно: тип раздела должен быть 773f91ef-66d4-49b5-bd83-d683bf40ad16.

- внести изменения в таблицу разделов на диске в соответствии с файлом `/tmp/sfdisk.gpt` при помощи утилиты `sfdisk` :

```
:$ sfdisk /dev/sdb < /tmp/sfdisk.gpt
```

> ⓘ В примерах используется обозначение диска `/dev/sdb`. Чтобы узнать, какое обозначение присвоилось диску, необходимо воспользоваться утилитой `lsblk`.

- преобразовать новый раздел диска в формат `ext4`:

```
:$ mkfs.ext4 /dev/sdb1
```

- проверить успешность создания диска:

```
:$ lsblk -JO /dev/sdb1
```

где:

`-JO` - ключ для вывода всех столбцов в формате JSON.

6.11.3 . Задание атрибутов созданному диску

Для задания атрибутов созданному ранее диску необходимо:

- выключить ВМ и отключить диск от нее;
- в свойствах диска добавить атрибут `TDSK_SHARED_TYPE` со значением `PRIVATE`. Запомнить идентификатор (ID) диска (см. Рисунок 17).

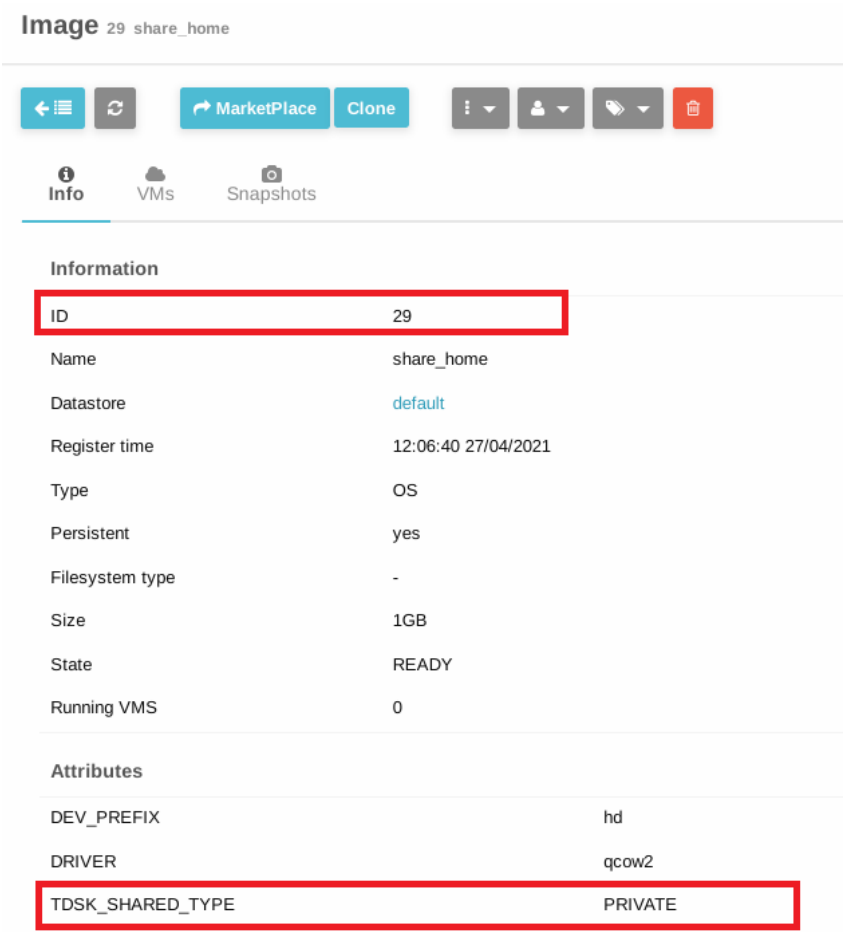

Рисунок 17 – Окно просмотра ID диска в ПК СВ Брест

6.11.4 . Настройка модуля PAM в базовом ВРМ

Для настройки модуля PAM в гостевой ОС базового ВРМ необходимо выполнить следующее:

- выполнить подготовку базового ВРМ (см. подраздел **Подготовка базового ВРМ**);
- создать файл `/usr/share/pam-configs/pam_tdsk` со следующим содержимым:

```
Name: Termidesk session
Default: yes
Priority: -1
Session-Interactive-Only: yes
Session-Type: Additional
Session:
```

```
7 required pam_exec.so /usr/bin/pam_tdsk --autofs --skel=/etc/skel --ch
mod=700 --uid-ext-range 65536-2000000000
```

⚠ Параметр `--uid-ext-range` должен иметь минимальное значение 65536, максимальное значение 4000000000.
Максимальная граница диапазона зависит от используемого домена в сети, от настроек отображения идентификаторов пользователей домена в идентификаторы пользователей BPM.

⚠ Приоритет `Priority: -1` задан для того, чтобы домашний каталог (файл `/usr/share/pam-configs/mkhomedir`, `Priority: 0`) был создан прежде, чем будет выполнено подключение диска.

- выполнить обновление профилей PAM:

```
:$ sudo pam-auth-update
```

- убедиться, что в файле `/etc/pam.d/common-session` появилась строка с модулем `pam_tdsk`:

```
1 session required pam_exec.so /usr/bin/pam_tdsk --autofs --skel=/etc/
skel --chmod=700 --uid-ext-range 65536-2000000000
```

6.11.5 . Активация механизма переносимых профилей в Termidesk

Для активации механизма переносимых профилей необходимо выполнить следующее:

- задать в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` в параметре `TDSK_AUTOFS_IMAGES_ID` список ID дисков, например:

```
1 # Список идентификаторов образов дисков для хранения отделяемых пользовательских профилей.
Может быть задано несколько значений, через запятую.
2 TDSK_AUTOFS_IMAGES_ID=29
```

⚠ При наличии нескольких дисков необходимо перечислить их через запятую.

- перезапустить службу `termidesk-vdi`:

```
:$ systemctl restart termidesk-vdi
```

- убедиться, что необходимая переменная установлена:

```
:$ ps eanxww | grep TDSK_AUTOFS
```

Вывод команды должен включать установленную переменную, например `TDSK_AUTOFS_IMAGES_ID=29`.

6.11.6 . Активация политики в интерфейсе Termidesk

Для включения в настройках глобальных политик Termidesk политики «Отделяемый пользовательский профиль» в графическом интерфейсе управления Termidesk следует перейти «Настройки - Глобальные политики», затем параметру «Отделяемый пользовательский профиль» присвоить значение «Включен».

6.12 . Перенаправление видеокамеры

Перенаправление видеокамеры позволяет передать по сети сжатое алгоритмом кодирования видео от устройств видеозахвата, подключенных к USB-шине персонального компьютера, на удаленное устройство, такое как BPM или терминальный сервер.

Виртуальная видеокамера определяется как видеоустройство веб-браузерами, программами видеоконференцсвязи, диагностическими утилитами и иными программами, работающими с устройствами захвата видео.

Для реализации функционала перенаправления видеокамеры пользователю необходимо использовать специализированный клиент подключений (`termidesk-viewer`), который является дополнением к компоненту «Клиент».

> ⚠ Возможность перенаправления видеокамеры доступна по протоколу SPICE (vdi-viewer, эксперим.). Для активации этой возможности следует в графическом интерфейсе управления Termidesk перейти «Настройки – Глобальные политики», затем в поле «Перенаправление видеокамеры в протоколе доставки "SPICE (vdi-viewer, эксперим.)» выбрать значение «Разрешено».

В базовое BPM, наряду со стандартными настройками (см. подраздел **Подготовка базового рабочего места**), должен быть установлен видеоагент `termidesk-video-agent` (см. подраздел **Установка в среде ОС Astra Linux Special Edition 1.7** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»).

6.13 . Перенаправление смарт-карты

Перенаправление смарт-карты позволяет передать подключенную к USB-шине персонального компьютера смарт-карту на удаленное устройство, такое как BPM или терминальный сервер.

Виртуальная смарт-карта определяется диагностическими утилитами и иными программами, работающими с устройствами подобного типа.

Для реализации функционала перенаправления смарт-карт пользователю необходимо использовать специализированный клиент подключений (`termidesk-viewer`), который является дополнением к компоненту «Клиент».

⚠ Возможность перенаправления смарт-карты доступна по протоколу SPICE (vdi-viewer, эксперим.). Для активации этой ворзможности следует в графическом интерфейсе управления Termidesk перейти «Настройки – Глобальные политики», затем в поле «Перенаправление смарт-карт в протоколе доставки "SPICE (vdi-viewer, эксперим.)» выбрать значение «Разрешено».

В базовое ВРМ, наряду со стандартными настройками (см. подраздел **Подготовка базового рабочего места**), должен быть установлен агент виртуальных смарт-карт `termidesk-video-agent` (см. подраздел **Установка в среде ОС Astra Linux Special Edition 1.7** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»).

6.14 . Настройка технологии единого входа

6.14.1 . Настройка технологии единого входа в гостевой ОС ВМ

6.14.1.1 . Общие сведения

Настройка технологии единого входа (SSO) позволяет автоматически авторизовываться в гостевую ОС ВМ при подключении пользователя по протоколу `SPICE`.

⚠ Начиная с Termidesk версии 4.3 достаточно только включить механизм автоматической авторизации в гостевую ОС.

6.14.1.2 . Включение механизма автоматической авторизации

Механизм автоматической авторизации в ОС Linux может быть включен двумя способами:

1) через задание переменной `DM_LOGIN_AUTOMATION` со значением «1» в файле `/lib/systemd/system/fly-dm.service`. Пример файла:

```
[Unit]
Description=The FLY login manager

#replaces getty
#Conflicts=getty@tty1.service
#After=getty@tty1.service

#replaces plymouth-quit  since it quits plymouth on its own
#Conflicts=plymouth-quit.service
#After=plymouth-quit.service

After=rc-local.service plymouth-start.service dbus.service systemd-user-sessions.service libflygetexe-bin.service

#resposible for plymouth stopping, so if fails then make sure plymouth still stop
OnFailure=plymouth-quit.service

[Service]
```

```
ExecStartPre=/bin/bash -c /usr/bin/fly-dm-prepare.sh
ExecStart=/usr/bin/fly-dm vt7

IgnoreSIGPIPE=no

EnvironmentFile=-/etc/default/locale
Environment="DM_LOGIN_AUTOMATION=1"

[Install]
Alias=display-manager.service
```

2) дополнительно к первому способу задать переменную `DM_LOGIN_AUTOMATION` со значением «1» в файле `/etc/default/locale`. Пример файла:

```
# File generated by update-locale
LANG="ru_RU.UTF-8"
DM_LOGIN_AUTOMATION=1
```

⚠ Данный способ (второй) является предпочтительным.

После включения автоматической авторизации одним из перечисленных выше способов необходимо выполнить перезапуск конфигурации загруженных модулей:

```
:$ sudo systemctl daemon-reload
```

Затем выполнить перезапуск службы:

```
:$ sudo systemctl restart fly-dm
```

Для работы механизма SSO в ОС Windows необходимо установить пакет переносимых библиотек из состава Visual Studio C++ в гостевую ОС: https://aka.ms/vs/17/release/vc_redist.x64.exe.

6.14.2 . Активация технологии единого входа на сервере терминалов MS RDS

Для включения SSO на MS RDS необходимо выполнить следующую последовательность шагов:

- на контроллере домена MS AD создать групповую политику с названием SSO;
- в созданную групповую политику внести следующие изменения:
  - в редакторе групповой политики перейти «Конфигурация компьютера - Административные шаблоны - Система - Передача учетных данных», выбрать параметр «Разрешить передачу учетных данных, установленных по умолчанию» и присвоить ему значение «Включено». Затем нажать экранную кнопку **[Добавить серверы в список]** и задать значение «TERMSRV/disp.termidesk.local» (см. Рисунок 18), где `disp.termidesk.local` - имя сервера Termidesk. Далее нажать экранные кнопки **[OK]** и **[Применить]**;

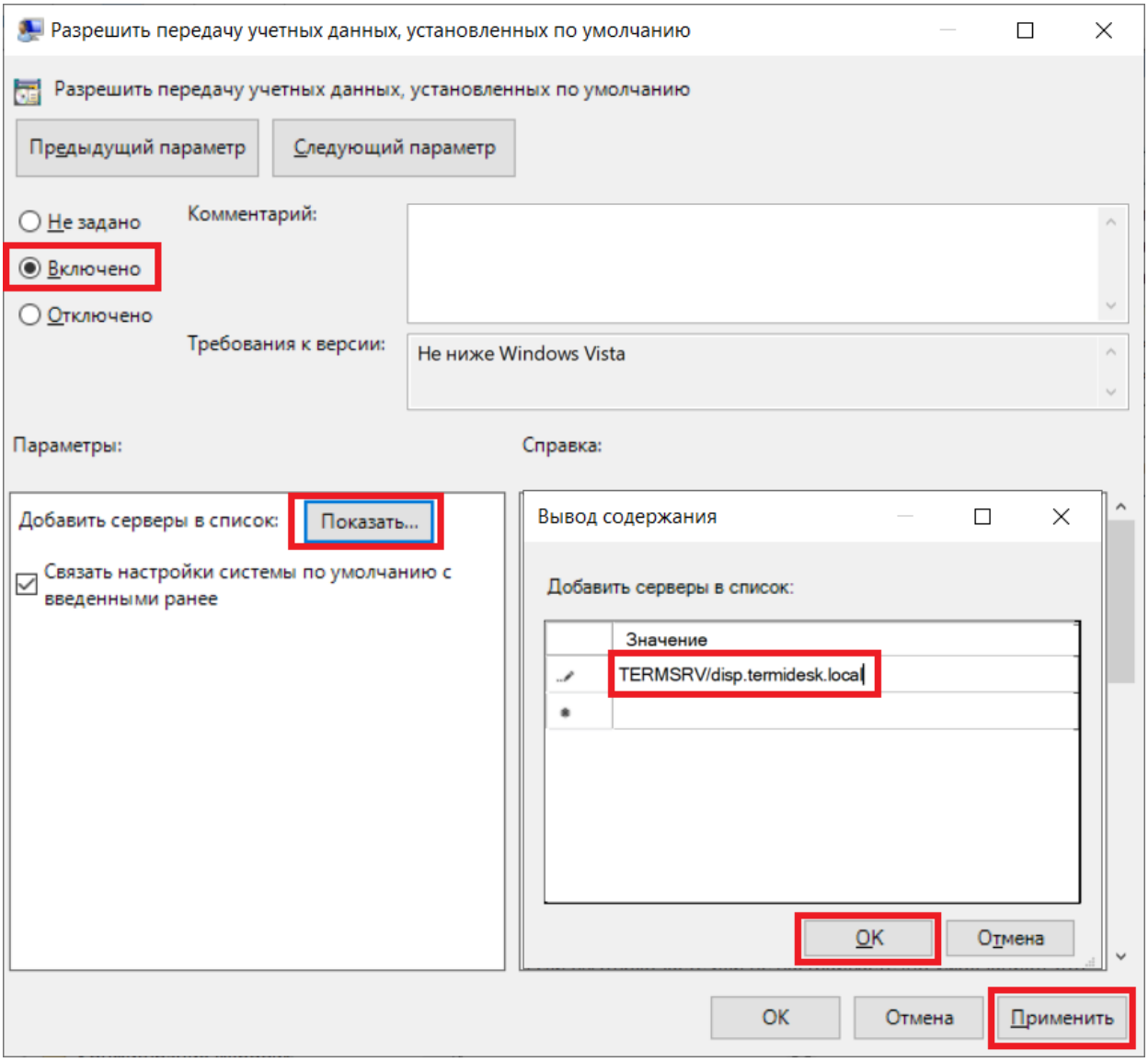

Рисунок 18 – Редактирование параметра «Разрешить передачу учетных данных, установленных по умолчанию» групповых политик

- в этом же списке выбрать параметр «Разрешить передачу новых учетных данных с проверкой подлинности сервера «только NTLM» и присвоить ему значение «Включено». Затем нажать экранную кнопку **[Добавить серверы в список]** и задать значение «TERMSRV/disp.termidesk.local» (см. Рисунок 18), где `disp.termidesk.local` - имя сервера Termidesk. Далее нажать экранные кнопки **[OK]** и **[Применить]**;
- в редакторе групповой политики перейти «Конфигурация компьютера - Административные шаблоны - Компоненты Windows - Службы удаленных рабочих столов - Клиент подключения к удаленному рабочему столу», выбрать параметр «Запрашивать учетные данные на клиентском компьютере» и присвоить ему значение «Отключено».

По умолчанию время гарантированного автоматического применения изменений соответствует интервалу 90 – 120 минут после обновления файлов групповых политик на контроллере домена. Если необходимо форсировать применение политики, то на контроллере домена, MS RDS и рабочих станциях пользователей необходимо выполнить команду `gpupdate /force`.

6.15 . Настройка аутентификации пользователей BPM через файл

6.15.1 . Общие сведения

Действия по настройке аутентификации пользователей BPM через файл сводятся к следующей последовательности шагов, выполняемых в гостевой ОС:

- задание файла для хранения паролей в модуле PAM;
- включение механизма автоматической авторизации в гостевую ОС.

> Termidesk интегрирован со встроенным комплексом средств защиты информации ОС Astra Linux Special Edition. Идентификация и аутентификация, а также защита аутентификационной информации осуществляется средствами ОС.

6.15.2 . Настройка модуля PAM

Для задания файла хранения паролей в модуле PAM необходимо отредактировать файл `/etc/pam.d/fly-dm`, добавив следующую строку перед секцией `@include common-auth`:

```
auth sufficient pam_exec.so expose_authtok quiet /usr/bin/pam_tdsk --htpasswd /etc/htpasswd
```

где `/etc/htpasswd` - путь к файлу с парами «логин:пароль» пользователей, имеющих право на автоматический вход в сессию.

Пример файла `/etc/pam.d/fly-dm`:

```
#%PAM-1.0
auth required pam_parsec_mac.so

auth    requisite       pam_nologin.so

auth    required        pam_env.so readenv=1
auth    required        pam_env.so readenv=1 envfile=/etc/default/locale
auth sufficient pam_exec.so expose_authtok quiet /usr/bin/pam_tdsk --htpasswd /etc/htpasswd

@include common-auth
-auth   optional        pam_gnome_keyring.so
-auth   optional        pam_kwallet5.so

session required pam_parsec_mac.so unshare_root_only
session required        pam_limits.so
```

```
session  required       pam_loginuid.so

@include common-account
account required pam_parsec_mac.so labelselect=appset
@include common-session
session required pam_parsec_cap.so
session required pam_parsec_aud.so
session required pam_parsec_mac.so
-session optional       pam_gnome_keyring.so auto_start
-session optional       pam_kwallet5.so auto_start
@include common-password
```

6.15.3 . Включение механизма автоматической авторизации

Механизм автоматической авторизации включается аналогично пункту **Включение механизма автоматической авторизации** подраздела **Настройка технологии единого входа в гостевой ОС ВМ**.

7 . УПРАВЛЕНИЕ ПАРАМЕТРАМИ ГОСТЕВЫХ ОС

7.1 . Общие сведения

Параметры гостевых ОС позволяют произвести автоматическую и идентичную настройку одной или нескольких гостевых ОС для использования в фонде ВРМ.

Графический интерфейс управления Termidesk обеспечивает следующие операции управления параметрами гостевых ОС:

- добавление;
- редактирование;
- удаление;
- просмотр сведений.

Для добавления параметров конфигурации гостевой ОС следует перейти «Компоненты - Параметры гостевых ОС», затем нажать экранную кнопку **[Новый]** и выбрать из выпадающего списка тип ОС.

Созданные конфигурации можно редактировать, для этого нужно пометить необходимые параметры ОС, а затем нажать экранную кнопку **[Редактировать]**.
Созданные конфигурации можно удалить, для этого нужно пометить необходимые параметры ОС, а затем нажать экранную кнопку **[Удалить]**.

⚠ Параметры конфигурации гостевой ОС могут быть удалены только в том случае, если они не используются фондом ВРМ.

7.2 . Параметры гостевой ОС Windows

7.2.1 . Конфигурация без домена

Для добавления в Termidesk параметров гостевой ОС Microsoft Windows 7 или Microsoft Windows 10 без ввода в домен администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 45).

Таблица 45 – Данные для гостевой ОС Windows без ввода в домен

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС

7.2.2 . Конфигурация при вводе в домен MS AD

Для добавления в Termidesk параметров гостевой ОС Microsoft Windows 7 или Microsoft Windows 10 с последующим вводом в домен администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 46).

Таблица 46 – Данные для гостевой ОС Windows при вводе в домен MS AD

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен»	Доменное имя службы каталогов MS AD
«Аккаунт»	Идентификатор субъекта, имеющий полномочия по добавлению BPM к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий
«OU»	Идентификатор организационной единицы, в которую будет добавлены BPM

7.3 . Параметры гостевой ОС Linux

7.3.1 . Конфигурация без домена

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux без ввода в домен администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 47).

Таблица 47 – Данные для гостевой ОС Linux без ввода в домен

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС

7.3.2 . Конфигурация при вводе в домен MS AD

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux при вводе в домен MS AD администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 48).

Таблица 48 – Данные для гостевой ОС Linux при вводе в домен MS AD

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС

Параметр	Описание
«Домен»	Идентификатор домена MS AD
«Аккаунт»	Идентификатор субъекта, имеющий полномочия по добавлению BPM к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий
«OU»	Идентификатор организационной единицы, в которую будет добавлены BPM (опционально)

⚠ Для ввода BPM с ОС Astra Linux в домен MS AD необходимо в базовое BPM установить пакет `astra-ad-sssd-client`.

7.3.3 . Конфигурация при вводе в домен FreeIPA

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux при вводе в домен FreeIPA администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 49).

Таблица 49 – Данные для гостевой ОС Linux при вводе в домен FreeIPA

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен аутентификации»	Идентификатор домена FreeIPA
«Аккаунт»	Идентификатор субъекта, имеющий полномочия по добавлению BPM к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий

⚠ Для ввода BPM с ОС Astra Linux в домен FreeIPA необходимо в базовое BPM установить пакет `astra-freeipa-client`.

7.3.4 . Конфигурация при вводе в домен ALD

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux при вводе в домен ALD администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 50).

Таблица 50 – Данные для гостевой ОС Linux при вводе в домен ALD

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС

Параметр	Описание
«Домен аутентификации»	Идентификатор домена ALD
«Аккаунт»	Идентификатор субъекта, имеющий полномочия по добавлению BPM к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий

7.4 . Действие при выходе пользователя из ОС

Termidesk поддерживает назначение действий с BPM при выходе пользователя из сессии.

Для назначения действия в графическом интерфейсе управления следует перейти «Настройки - Глобальные политики - Действие при выходе пользователя из ОС», затем нажать экранную кнопку **[Редактировать]** и выбрать один из следующих вариантов:

- «Удалять рабочее место» - удалить BPM после выхода пользователя;
- «Нет» - не производить действий с BPM (сохранять состояние).

Совместно с политикой «Действие при выходе пользователя из ОС» применяется политика «Удаление рабочего места после», которая может принимать следующие значения:

- «После события выхода пользователя из ОС»;
- «После события завершения синхронизации профиля».

⚠ Обработка значения «После события завершения синхронизации профиля» не поддерживается в агенте BPM версии 4.1. Функционал приведен для справки.

7.5 . Изменение изображения гостевых ОС

Графические изображения в Termidesk применяются для визуальной идентификации используемых гостевых ОС в фондах BPM.

Для добавления графического изображения следует перейти «Настройки - Галерея» и нажать экранную кнопку **[Новый].**

В окне добавления изображения нужно заполнить наименование добавляемого объекта, а также добавить само изображение, нажав экранную кнопку **[Выберите изображение].**

Требования к изображению:

- размер: от 16x16 до 256x256 пикселей;
- соотношение сторон: 1:1;
- поддерживаемые форматы: `.ico`, `.jpeg`, `.jpg`, `.png`.

После добавления изображений гостевых ОС в Termidesk пользователь, подключившись к серверу через компонент «Клиент», увидит их в своем интерфейсе (см. Рисунок 19).

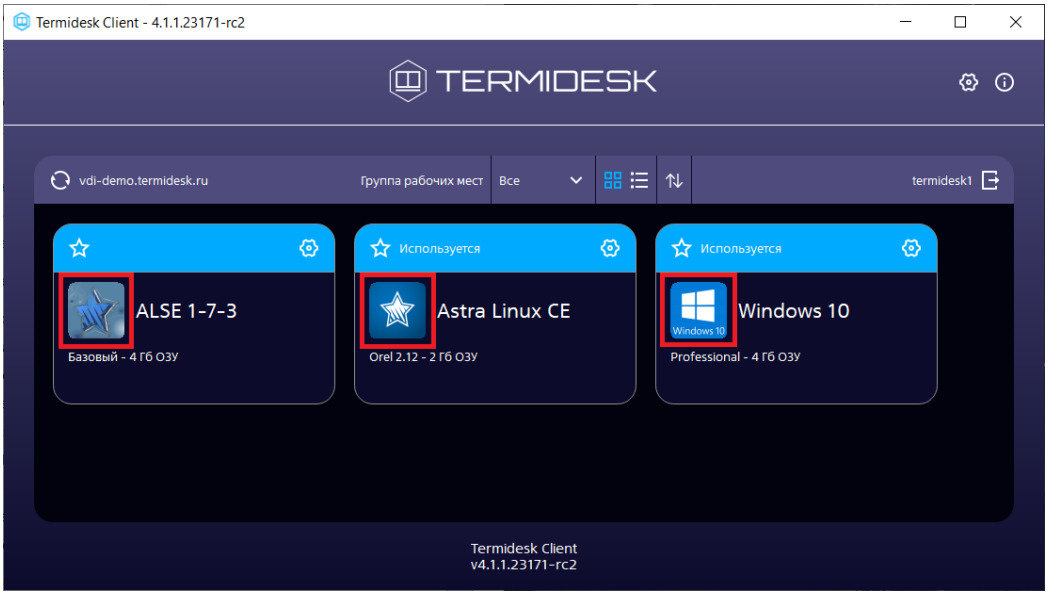

Рисунок 19 – Отображение назначенных изображений в сеансе пользователя

8 . ФОНД РАБОЧИХ МЕСТ

8.1 . Общие сведения о фонде BPM

Фонд BPM – это совокупность подготовленных BPM для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей.

Для добавления нового фонда BPM в графическом интерфейсе управления следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Новый]**.
Созданные фонды можно редактировать, для этого нужно пометить название фонда, а затем нажать экранную кнопку **[Редактировать]**.
Созданные фонды можно удалить, для этого нужно пометить название фонда, а затем нажать экранную кнопку **[Удалить]**.
Экранная кнопка **[Политики]**, доступная при выборе названия фонда, открывает параметры выбранного фонда. Совокупность параметров аналогична представленной в «Настройки - Глобальные политики».

После добавления фонда BPM можно перейти к его детальному просмотру. Для этого в сводной таблице окна «Фонды» в столбце «Название» следует нажать на наименование фонда BPM.
На открывшейся странице будут представлены следующие разделы:

- «Рабочие места» – список ВМ и информация о подготовленных BPM, используемых субъектами;
- «Пользователи и группы» – имена пользователей и наименование групп, используемые для определения разрешений по доступу к фондам BPM;
- «Протоколы доставки» – доступные протоколы удаленного доступа, используемые при доставке BPM;
- «Публикации» – актуальная информация о созданном фонде BPM. Раздел будет отсутствовать, если фонд используется для публикации приложений или для доступа к терминальным сессиям;
- «Журнал» – системные сообщения, связанные с жизненным циклом фонда BPM.

Настройка отдельных глобальных параметров по управлению фондами BPM (например, «Максимальное количество рабочих мест, удаляемых единовременно из фонда рабочих мест») доступна в общих системных параметрах Termidesk (см. подраздел **Общие системные параметры Termidesk**).

8.2 . Добавление фонда BPM

Для добавления в графическом интерфейсе управления следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Новый]**, выбрать тип мастера публикации «Виртуальные машины».

Откроется мастер публикации фонда (см. Рисунок 20). Необходимо заполнить параметры, указанные в таблице, (см. Таблица 51) и нажать экранную кнопку **[Далее]**. При нажатии экранной кнопки **[Отменить]**, или клавиши **<Esc>**, или иконки «Крестик», на любом из этапов работы произойдет закрытие мастера без сохранения настроек.

Рисунок 20 – Базовые настройки фонда в Мастере публикации

Таблица 51 – Базовые настройки фонда

Параметр	Описание
«Название»	Ввести текстовое наименование фонда BPM. Наименование может содержать только латинские буквы, цифры, пробел, дефис и нижнее подчеркивание. Параметр обязателен для заполнения
«Комментарий»	Ввести информационное сообщение, используемое для описания назначения фонда BPM
«Шаблон»	Выбрать из списка шаблон, который будет использоваться при создании BPM
«Максимальное количество рабочих мест»	Задать максимальное количество BPM в фонде. Максимальное число BPM не может быть меньше значения, указанного в параметре «Кеш рабочих мест 1-го уровня» на следующем шаге мастера

Если обязательное поле не было заполнено или есть ошибка при заполнении, оно будет подсвечено красным цветом и будет выведено сообщение об ошибке (см. Рисунок 21) после нажатия экранной кнопки **[Далее]**. Индикация цветом и сообщение не исчезнут после заполнения поля.

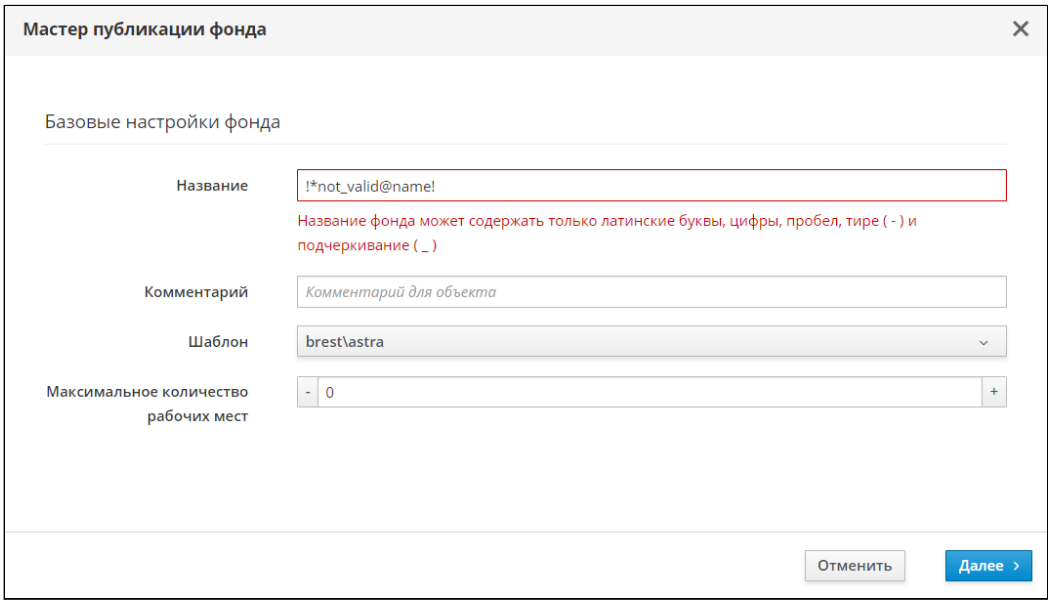

Рисунок 21 – Пример сообщения об ошибке

Далее будет выполнен переход на следующий шаг настройки (см. Рисунок 22) мастера публикации фонда, в котором нужно заполнить параметры, указанные в таблице (см. Таблица 52). Поскольку во время перехода выполняется отправка данных на сервер, возможна ситуация, что при возвращении на предыдущий шаг появится сообщение об ошибке, если параметр «Протоколы доставки» не был заполнен. Отправка данных на сервер происходит всегда при переходе между шагами, кроме перехода назад с завершающего этапа.

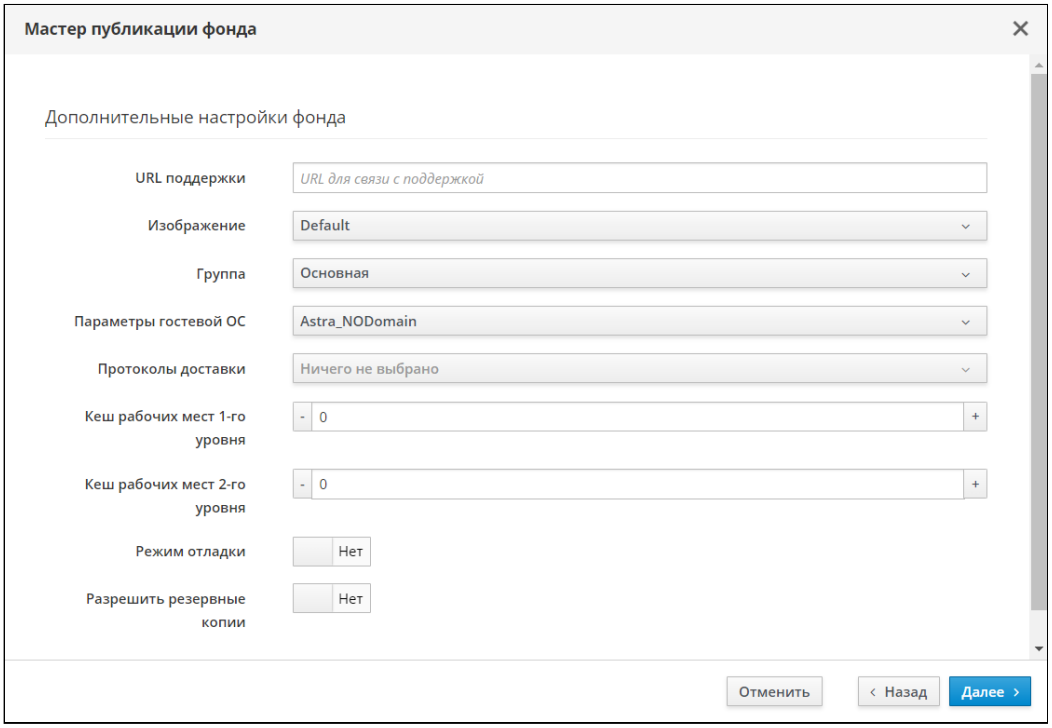

Рисунок 22 – Дополнительные настройки фонда Мастера публикации

Таблица 52 – Дополнительные настройки фонда

Параметр	Описание
«URL поддержки»	Ввести URL для связи с технической поддержкой
«Изображение»	Выбрать графическое представление фонда BPM
«Группа»	Выбрать группу в которую будут входить субъекты для доступа к фонду BPM
«Параметры гостевой ОС»	Выбрать параметры конфигурации гостевой ОС, которые будут использованы при создании BPM
«Протоколы доставки»	Выбрать один или несколько протоколов доставки, которые будут доступны для фонда BPM
«Кеш рабочих мест 1-го уровня»	Задать количество созданных, настроенных и запущенных BPM в фонде
«Кеш рабочих мест 2-го уровня»	Задать количество созданных, настроенных и выключенных BPM. Для использования кеша рабочих места 2-го уровня необходимо, чтобы в параметре «Кеш рабочих мест 1-го уровня» было задано хотя бы одно BPM
«Режим отладки»	Включение режима отладки, по умолчанию отключен
«Разрешить резервные копии»	Включение режима резервного копирования BPM фонда, по умолчанию отключен

После заполнения параметров нужно нажать экранную кнопку **[Далее]**.

В следующем окне завершить настройку фонда, нажав экранную кнопку **[Завершить]**. Далее будет отображено временное окно с заблокированными экранными кнопками. При успешном создании фонда в этом же окне должно появиться сообщение (см. Рисунок 23) «Фонд успешно создан!», окно будет автоматически закрыто по истечении 3 секунд.

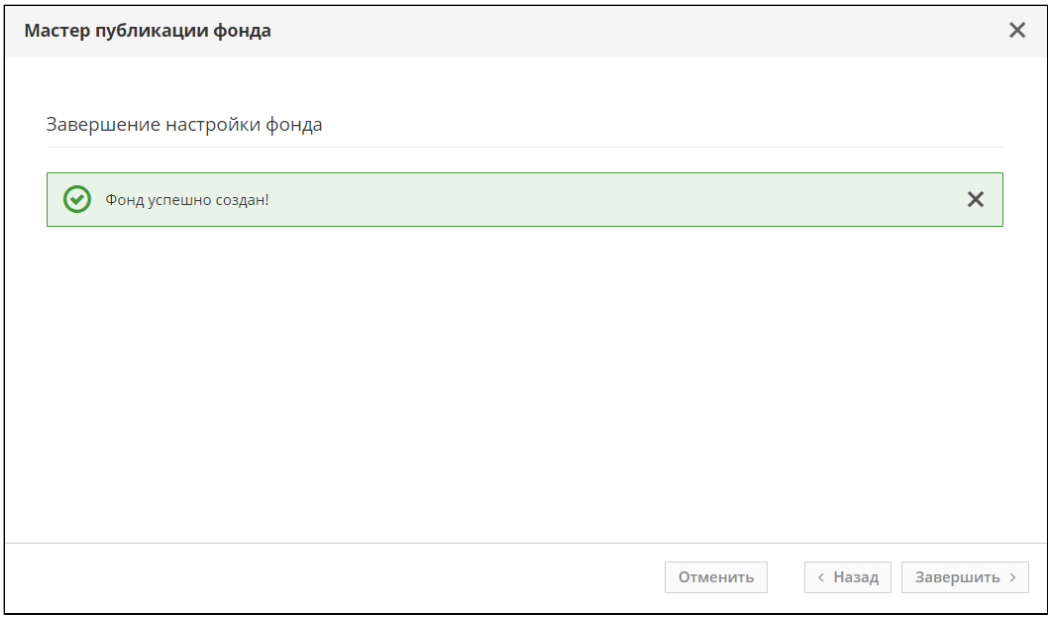

Рисунок 23 – Успешное завершение настройки публикации фонда

8.3 . Глобальные политики фонда BPM

Глобальные политики задают параметры для работы пользователей с BPM, перекрывающие индивидуальные настройки фондов BPM.

Для редактирования глобальных политик в графическом интерфейсе управления следует перейти «Настройки - Глобальные политики», выбрать необходимый параметр и нажать экранную кнопку **[Редактировать]**.

Настройки выбранного параметра можно сбросить до значений по умолчанию при помощи экранной кнопки **[Сбросить]**.

Для редактирования глобальных политик администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 53).

Таблица 53 – Доступные параметры глобальных политик фонда BPM

Параметр	Описание
«Буфер обмена в протоколах доставки "RDP" и "SPICE (vdi-viewer, эксперим.)"»	Разрешение на использование буфера обмена в протоколах доставки. Использование буфера обмена можно выключить, включить только от сервера к клиенту, включить только от клиента к серверу, разрешить двунаправленный обмен. Значение по умолчанию: «Двустороннее перенаправление буфера»
«Выбор пользователем протокола доставки»	Определяет возможность выбрать протокол доставки пользователем для подключения к BPM. Значение по умолчанию: «Разрешен»
«Действие при выходе пользователя из ОС»	Определяет действие после выхода пользователя из ОС. Значение по умолчанию: «Нет»
«Подключение с отличным именем пользователя»	Разрешение подключения пользователя к ВМ, если вводимый в ВМ логин отличен от логина назначенной машины в Termidesk. Значение по умолчанию: «Запрещено»
«Завершать сеанс при достижении лимита времени»	Управление сеансами пользователей при достижении заданного лимита времени: по истечении лимита времени RDP-сессия будет завершена, а не отключена. Значение по умолчанию: «Выключено»
«Лимит времени для отключенной сессии»	Установка лимита времени для отключенной RDP-сессии. Работает совместно с политикой «Завершать сеанс при достижении лимита времени». Значение по умолчанию: «Нет ограничений»

Параметр	Описание
«Лимит времени для выхода из сеансов RemoteApp»	Управление лимитом времени для выхода из сеансов RemoteApp. Позволяет указать, как долго сеанс пользователя при использовании RemoteApp (удаленное приложение) будет оставаться в отключенном состоянии после закрытия всех программ RemoteApp. Значение по умолчанию: «Никогда»
«Лимит времени для активных сеансов служб удаленных рабочих столов»	Управление лимитом времени для активных сеансов служб удаленных рабочих столов. Указывается время, по истечении которого сеанс переходит в отключенное состояние (завершается). Политика применяется в момент авторизации пользователя в BPM. В версиях Termidesk ниже 4.3 параметр задавался при настройке гостевых ОС («Компоненты - Параметры гостевых ОС»). При возврате к версиям Termidesk ниже 4.3 параметр будет выставлен в значение по умолчанию. Значение по умолчанию: «Нет ограничений»
«Использование механизма RemoteFX (RDP)»	Политика активации механизма RemoteFX для протокола RDP. Значение по умолчанию: «Выключен»
«Масштабирование экрана для протокола RDP»	Политика управления масштабированием экрана для протокола RDP. Значение по умолчанию: «Выключено»
«Механизм обеспечения безопасности на уровне сети (RDP)»	Политика управления обеспечением безопасности на уровне сети для протокола RDP. Для подключения к STAL необходимо использовать политику «TLS» или «RDP». Для подключения к MS RDS необходимо использовать политику «NLA». Политика может быть задана для конкретного фонда BPM на странице самого фонда BPM. Значение по умолчанию: «Автосогласование»
«Отделяемый пользовательский профиль»	Использование отделяемого пользовательского профиля в BPM. Политика применяется при старте BPM. Значение по умолчанию: «Выключен»
«Передача файлов в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Разрешение на передачу файлов в протоколах доставки. Политика пока применяется только для протокола SPICE (vdi-viewer, эксперим.). Значение по умолчанию: «Разрешена»
«Перенаправление видеокамеры в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Разрешение на перенаправление видеокамеры в протоколах доставки. Политика пока применяется только для протокола SPICE (vdi-viewer, эксперим.). Значение по умолчанию: «Разрешено»

Параметр	Описание
«Перенаправление смарт-карт в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Разрешение на перенаправление смарт-карт в протоколах доставки. Политика применяется только для протокола `SPICE (vdi-viewer, эксперим.)`. Значение по умолчанию: «Разрешено»
«Политика простоя рабочего места»	Разрешенное время простоя ВРМ в секундах. Значение «-1» означает неограниченное время простоя. Значение по умолчанию: «-1»
«Политика управления параметрами перенаправления принтеров»	Управление перенаправлением принтеров в протоколах доставки. Можно запретить перенаправление, разрешить перенаправлять все принтеры или только выбранные пользователем. Значение по умолчанию: «Не перенаправлять»
«Полноэкранный режим (для SPICE)»	Политика ограничения работы в полноэкранном режиме. Значение по умолчанию: «Включен»
«Разрешение видеокамеры в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Допустимые разрешения видеокамеры в протоколах доставки. Политика применяется только для протокола `SPICE (vdi-viewer, эксперим.)`. Значение по умолчанию: «320-2560x240-1440»

8.4 . Объединение фондов в группы ВРМ

Группы ВРМ отображаются как самостоятельные разделы в интерфейсе пользователя. Группы ВРМ являются логическим признаком, по которому можно объединять отображение фондов ВРМ для пользователей.

Для добавления группы администратору Termidesk в графическом интерфейсе управления следует перейти «Настройки - Группы рабочих мест» и нажать экранную кнопку **[Новый]**, затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 54).

Таблица 54 – Данные для объединения фондов ВРМ в группы

Параметр	Описание
«Название»	Текстовое наименование группы ВРМ
«Комментарий»	Информационное сообщение, используемое для описания назначения группы ВРМ
«Приоритет»	Преимущество использования группы ВРМ в графическом интерфейсе пользователя

Для редактирования группы рабочих мест в Termidesk нужно пометить необходимую группу и нажать экранную кнопку **[Редактировать]**.

Для удаления группы рабочих мест в Termidesk нужно пометить необходимую группу и нажать экранную кнопку **[Удалить]**.

8.5 . Публикация фонда BPM

Публикация фонда BPM позволяет создать BPM внутри фонда в соответствии с заданным в настройках количеством или обновить уже имеющиеся внутри фонда BPM и подготовить их для дальнейшего использования.

Для публикации фонда BPM в графическом интерфейсе управления следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» выбрать наименование фонда BPM.
На открывшейся странице в разделе «Публикации» нажать экранную кнопку **[Новая]**. В окне подтверждения публикации после ввода опционального текстового комментария нужно нажать экранную кнопку **[Опубликовать]** для запуска задачи обновления фонда BPM.
Нажатие экранной кнопки **[Отменить]** не вызывает обновления фонда BPM.
Прогресс выполнения публикации будет отображен в этом же разделе. Индикатор прогресса относится только к созданию BM в кеше (BM, поддерживаемых в определенном состоянии) и не отображает факт получения пользователем BPM.
Существуют несколько состояний публикации, которые могут быть отражены в столбце «Прогресс»:

- «Идет создание BM», индикация серым цветом (см. Рисунок 24) - начало процесса публикации;
- «Идет создание BM», индикация синим цветом (см. Рисунок 24) - непосредственно процесс выполнения публикации, при котором выполняется обращение к поставщику ресурсов и создание BM;

Частота обновления прогресса зависит от значения интервала обновления для таблицы «Публикации». Отображаемый цвет и текст зависят от состояния публикации.

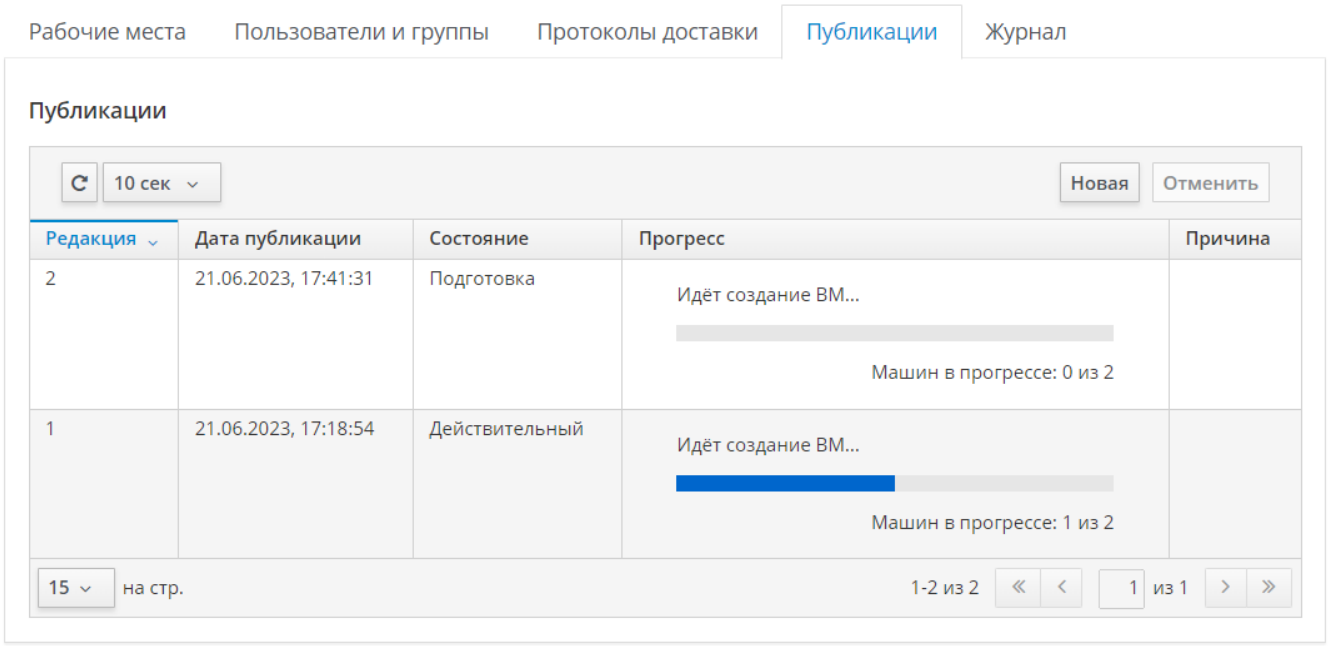

Рисунок 24 – Индикация прогресса выполнения публикации со статусом «Идет создание ВМ»

- «Публикация успешно завершена», индикация зеленым цветом (см. Рисунок 25) - публикация ВМ в кеше завершена. При выдаче ВРМ из кеша прогресс вновь вернется на начало процесса публикации;

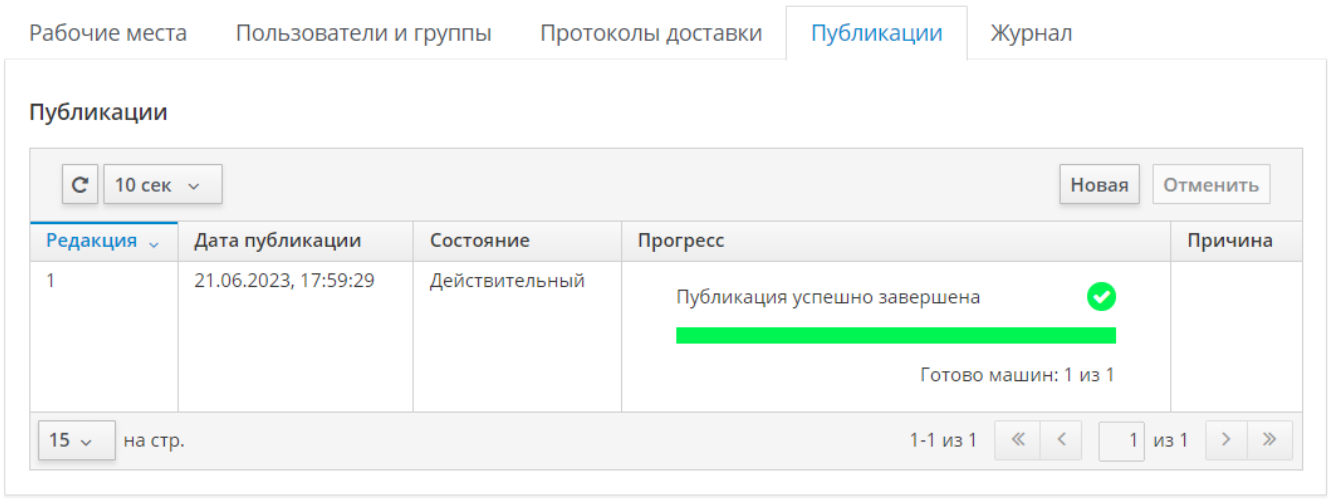

Рисунок 25 – Индикация прогресса выполнения публикации со статусом «Публикация успешно завершена»

- «Во время публикации возникла ошибка», индикация серым цветом с пиктограммой красного цвета (см. Рисунок 26) - процесс публикации завершился с ошибкой, текст ошибки отобразится в столбце «Причина»;

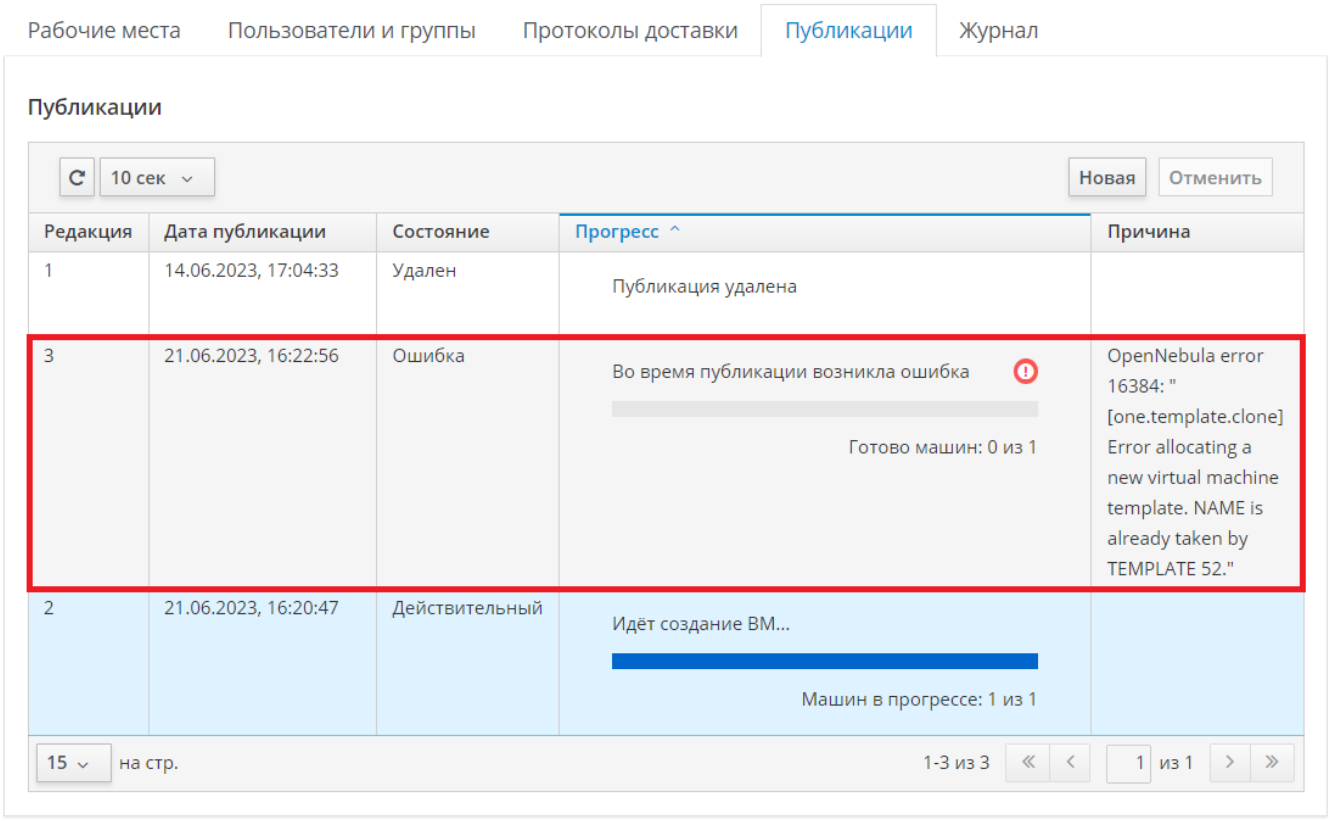

Рисунок 26 – Индикация возникновения ошибки при публикации

- «Публикация удалена», без индикации - информирование о завершении удаления публикации. Получить данное состояние можно при инициировании новой публикации (в таком случае старая публикация удаляется);
- «Нет машин в кеше 1-го и 2-го уровней», без индикации - информирование об отсутствии ВМ, поддерживаемых в кеше 1-го и 2-го уровней. Это означает, что в настройках фонда параметры «Кеш рабочих мест 1-го уровня» и «Кеш рабочих мест 2-го уровня» не заданы (для них выбрано значение «0»).

Для отмены существующей публикации фонда BPM следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» выбрать наименование фонда BPM.

⚠ Отмена публикации возможна, если публикация не находится в статусе «Действительный».

На открывшейся странице в разделе «Публикации» нужно нажать экранную кнопку **[Отменить]**. Отмена публикации удаляет BPM из фонда, а также параметры конфигурации фонда BPM из Termidesk.

8.6 . Назначение пользователей доступа

Фонду BPM можно назначать пользователей, которым этот фонд будет доступен.

Для добавления нового пользователя к фонду BPM в графическом интерфейсе управления следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда BPM. На открывшейся странице в разделе «Пользователи и группы» нажать на экранную кнопку **[Новый]** в области «Пользователи».

⚠ Добавление пользователя домена будет доступно только в том случае, если пользователь хотя бы один раз осуществил вход в интерфейс пользователя Termidesk под своей учетной записью.

8.7 . Назначение групп доступа фонду BPM

Фонду BPM можно назначать группы пользователей домена аутентификации, которым этот фонд будет доступен.

Для добавления новой группы к фонду BPM в графическом интерфейсе управления следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда BPM.

На открывшейся странице в разделе «Пользователи и группы» нужно нажать экранную кнопку **[Новый]** в области «Группы». В окне добавления объекта из выпадающего списка выбрать необходимый домен аутентификации, а затем требуемую для него группу.
Для удаления группы из фонда используется экранная кнопка **[Удалить]**.

⚠ Добавление группы пользователей домена будет возможно только в том случае, если указанная группа существует в службе каталога и добавлена в домен аутентификации в интерфейсе Termidesk.

8.8 . Назначение протоколов фонду BPM

Фонду BPM можно назначать доступные для него протоколы доставки как на этапе настройки при помощи «Мастера публикации фонда», так и после.

Для добавления нового протокола доставки фонду BPM в графическом интерфейсе управления следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда BPM.

На открывшейся странице в разделе «Протоколы доставки» нужно нажать экранную кнопку **[Новый]**. В окне добавления объекта из выпадающего списка выбрать необходимый протокол доставки.

⚠ Добавление протокола доставки в фонд BPM будет доступно только в том случае, если настроен хотя бы один протокол доставки в «Компоненты - Протоколы доставки».

8.9 . Управление сессиями подключенных к фонду BPM пользователей

В графическом интерфейсе управления Termidesk реализована возможность просмотра информации и управления текущими активными сессиями пользователей в фондах BPM.

Для просмотра основных сведений об активных сессиях пользователей в фондах BPM следует перейти «Рабочие места - Сессии», после чего откроется сводная таблица (см. Рисунок 27).

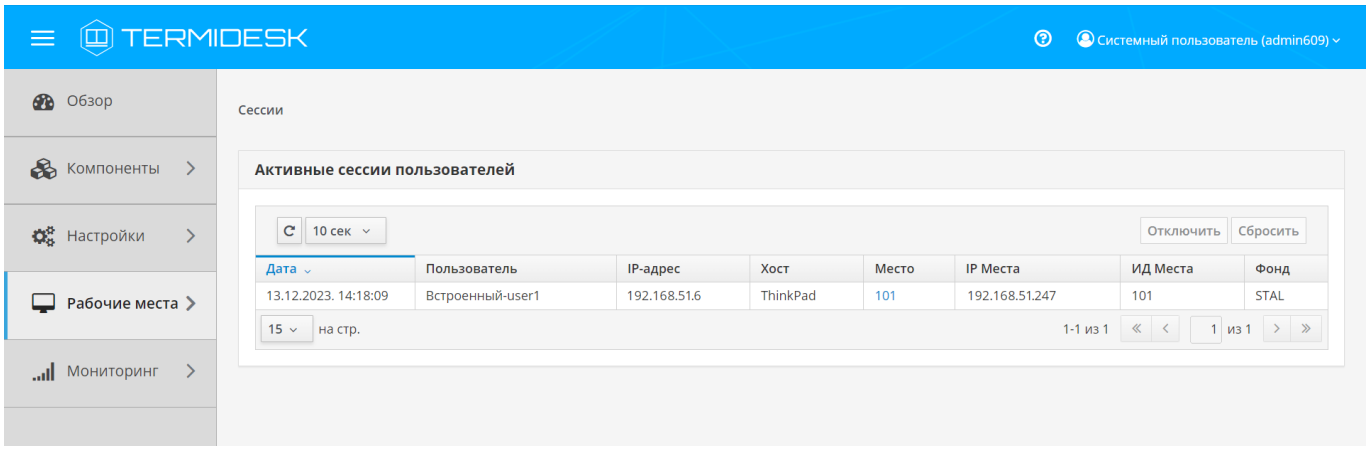

Рисунок 27 – Просмотр сведений об активных сессиях пользователей фонда BPM

Основные параметры сессий перечислены в столбце «Параметр» следующей таблицы (см. Таблица 55).

Таблица 55 – Основные параметры сессий пользователей

Параметр	Описание
«Дата»	Дата и время входа пользователя на BPM
«Пользователь»	Имя пользователя, которому было выдано BPM
«IP-адрес»	IP-адрес инициатора сессии
«Хост»	Наименование инициатора сессии
«Место»	Наименование BPM, выданного пользователю
«IP Места»	Наименование BPM, выданного пользователю
«ИД Места»	Наименование BPM, выданного пользователю
«Фонд»	Название фонда, в составе которого находится выданное BPM

Для принудительного отключения сессии пользователя следует перейти «Рабочие места - Сессии». В таблице с актуальной информацией об текущих активных сессиях пользователей ВРМ необходимо пометить сессию пользователя для отключения и нажать экранную кнопку **[Отключить]**.

> ⚠ После нажатия экранной кнопки **[Отключить]** принудительный штатный выход пользователя из ОС ВРМ произойдет в течение 30 секунд.

> ⚠ Сессия пользователя будет автоматически и принудительно завершена, если он был удален или домен аутентификации, в который входит этот пользователь, был отключен или удален.

8.10 . Управление назначенными ВМ

8.10.1 . Управление состоянием

Termidesk поддерживает управление состоянием назначенных ВМ для ВРМ, созданных для следующих поставщиков ресурсов:

- ПК СВ Брест;
- zVirt;
- oVirt;
- VMware vSphere.

Для изменения состояния ВМ необходимо перейти «Рабочие места - Фонды», затем выбрать нужный фонд, перейти во вкладку «Рабочие места» и выбрать назначенную ВМ (см. Рисунок 28).

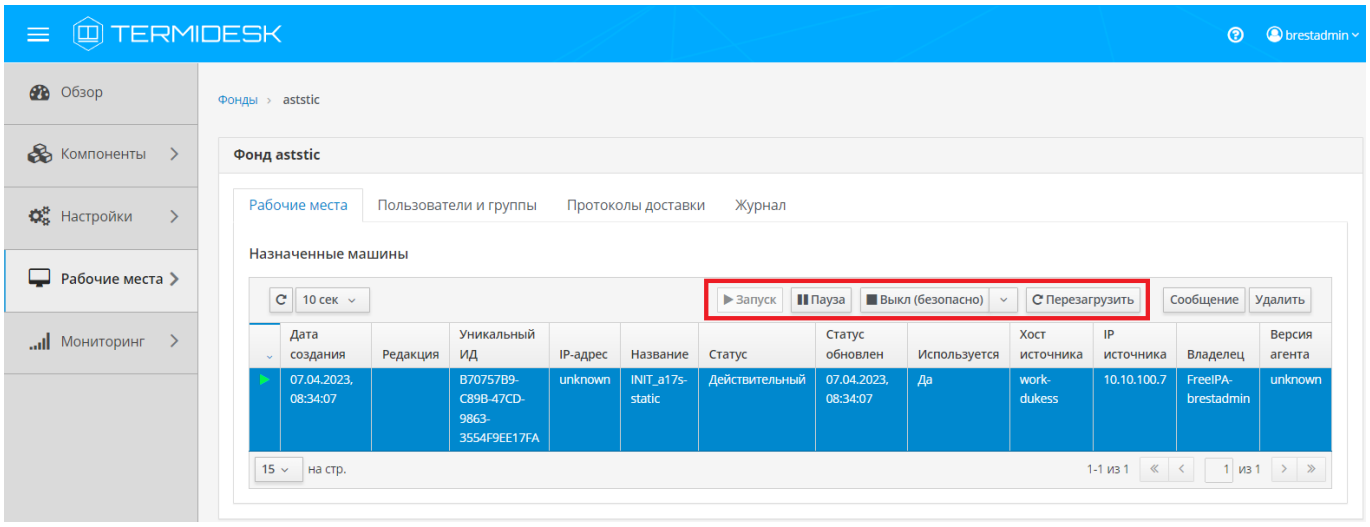

Рисунок 28 – Расположение экранных кнопок для управления состоянием назначенных ВМ

8.10.2 . Отправка сообщения в ВМ

В разделе «Рабочие места» есть возможность отправить сообщение пользователю ВРМ, нажав экранную кнопку **[Сообщение]**.

9 . ПРОТОКОЛЫ ДОСТАВКИ

9.1 . Общие сведения о протоколах доставки

Протокол доставки – это поддерживаемый в Termidesk протокол удаленного доступа к BPM. Протоколы доставки обеспечивают передачу экрана BPM на пользовательскую рабочую станцию.

Доставка экрана BPM может быть выполнена как напрямую, так и через компонент «Шлюз».
Для добавления протокола доставки в графическом интерфейсе управления следует перейти «Компоненты - Протоколы доставки», затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка поддерживаемый протокол и способ доставки.
Добавленные протоколы можно редактировать, для этого нужно пометить протокол и после нажать на экранную кнопку **[Редактировать]**.
Добавленные ранее протоколы можно удалить, для этого нужно пометить протокол и после нажать на экранную кнопку **[Удалить]**.

⚠ Протокол доставки может быть удален только в том случае, если он не используется фондом BPM.

Termidesk поддерживает следующие протоколы доставки:

- SPICE;
- VNC;
- RDP;
- loudplay (экспериментально).

Возможности каждого протокола при доставке BPM пользователю приведены в таблице (см. Таблица 56).

Таблица 56 – Функциональные возможности протоколов доставки

Возможность	SPICE	RDP	VNC	Loudplay
Программа подключения	termidesk-viewer, remote-viewer, веб-браузер	Windows: mtsc.exe, wfreerdp.exe, termidesk-viewer Linux: xfreerdp, termidesk-viewer	Веб-браузер	Loudplay-client
Туннелирование протокола через компонент «Шлюз»	Да	Да	Да	Нет
Возможность прямого подключения к рабочему столу	Через платформу виртуализации (к гипервизору)	Да	Да	Да

Возможность	SPICE	RDP	VNC	Loudplay
Поддержка нескольких мониторов	Да	Да	Нет	Нет
Передача буфера обмена	Да	Да	Нет	Нет
Перенаправление USB	Да	Нет *	Нет	Нет
Перенаправление последовательных портов	Нет	Да	Нет	Нет
Перенаправление принтера	Да	Да	Нет	Нет
Virtual Printing / Оптимизация печати (уменьшение полосы)	Нет	Нет	Нет	Нет
Воспроизведение звука	Да	Да	Нет	Да
Перенаправление микрофона	Да	Да	Нет	Да
Перенаправление сканера	Да	Нет	Нет	Нет
Оптимизация сканирования (уменьшение полосы)	Нет	Нет	Нет	Нет
Перенаправление локальных дисков	Нет	Да	Нет	Нет
Поддержка веб-камеры	Да	Нет	Нет	Нет
Поддержка смарт-карт	Да	Да	Нет	Нет
Автоматическое изменение разрешения экрана	Да	Да **	Нет	Нет
Поддержка единого входа	Да	Да	Нет	Нет
Получение статистики использования соединения	Да	Нет	Нет	Да
Поддержка vGPU/ прямое перенаправление видеокарты	Нет	Нет	Нет	Да
Оптимизация канала связи от ВРМ к пользовательской рабочей станции	Да	Да	Нет	Да

Примечание:

* необходима поддержка технологии RemoteFX;

** зависит от используемой ОС.

9.2 . Протокол доставки RDP

9.2.1 . Прямое подключение по протоколу RDP

Для добавления прямого подключения по протоколу RDP администратору Termidesk в графическом интерфейсе управления следует перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Новый]**, выбрать «RDP (напрямую)» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 57).

Таблица 57 – Данные для добавления прямого подключения по протоколу RDP

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде BPM
«Пустые учетные данные»	Не использовать технологию единого входа
«Логин»	Субъект, имеющий полномочия для подключения по протоколу RDP к BPM
«Пароль»	Набор символов, подтверждающий полномочия
«Без домена»	Не использовать идентификатор домена MS AD при проверке полномочий субъекта
«Домен»	Идентификатор домена MS AD при проверке полномочий субъекта
«Порт»	Выбор порта для подключения. По умолчанию используется порт 3389
«Разрешить смарт-карты»	Разрешить идентификацию субъектов на основе смарт-карт
«Разрешить принтеры»	Разрешить перенаправление устройств печати по протоколу RDP
«Разрешить диски»	Разрешить перенаправление устройств хранения по протоколу RDP
«Разрешить последовательные порты»	Разрешить перенаправление последовательных портов по протоколу RDP
«Показывать обои»	Отображать фоновое изображение, настроенное на рабочем столе
«Несколько мониторов»	Разрешить использовать несколько мониторов
«Разрешить композицию рабочего стола»	Разрешить темы рабочего стола
«Сглаживание шрифтов»	Использовать технологию сглаживания шрифтов

Параметр	Описание
«Поддержка CredSSP»	Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider
«Использовать ALSA»	Использовать программный микшер для передачи звука
«Параметры принтера»	Указать конфигурацию перенаправляемого принтера
«Параметры смарт-карты»	Указать конфигурацию идентификации по смарт-картам
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к BPM. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к BPM

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

9.2.2 . Подключение через компонент «Шлюз» по протоколу RDP

Для добавления подключения по протоколу RDP через компонент «Шлюз» администратору Termidesk необходимо перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Новый]**, выбрать «RDP (через вебсокет шлюз)» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 58).

Таблица 58 – Данные для добавления подключения по протоколу RDP через «Шлюз»

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде BPM

Параметр	Описание
«URL шлюза»	Адрес сервера в формате `ws(s)://192.0.2.30/websockify`, обеспечивающего формирование и поддержание соединения. Директива `ws` относится к использованию порта 80, директива `wss` означает использование 443 порта. Параметр `192.0.2.30` - доступный IP-адрес шлюза. Пример IP-адреса приведен в соответствии с RFC 5737, он должен быть заменен на актуальный, используемый согласно схеме адресации, принятой в инфраструктуре предприятия. Значение этого параметра не относится к значению `WSPROXY_BIND_ADDRESS` из конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf`
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза
«Пустые учетные данные»	Не использовать технологию единого входа
«Логин»	Субъект, имеющий полномочия для подключения по протоколу RDP к BPM
«Пароль»	Набор символов, подтверждающий полномочия
«Без домена»	Не использовать идентификатор домена MS AD при проверке полномочий субъекта
«Домен»	Идентификатор домена MS AD при проверке полномочий субъекта
«Порт»	Выбор порта для подключения. По умолчанию используется порт 3389
«Разрешить смарт-карты»	Разрешить идентификацию субъектов на основе смарт-карт
«Разрешить принтеры»	Разрешить перенаправление устройств печати по протоколу RDP
«Разрешить диски»	Разрешить перенаправление устройств хранения по протоколу RDP
«Разрешить последовательные порты»	Разрешить перенаправление последовательных портов по протоколу RDP
«Показывать обои»	Отображать фоновое изображение, настроенное на рабочем столе
«Несколько мониторов»	Разрешить использовать несколько мониторов
«Разрешить композицию рабочего стола»	Разрешить темы рабочего стола
«Сглаживание шрифтов»	Использовать технологию сглаживания шрифтов
«Поддержка CredSSP»	Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider
«Использовать ALSA»	Использовать программный микшер для передачи звука
«Параметры принтера»	Указать конфигурацию перенаправляемого принтера
«Параметры смарт-карты»	Указать конфигурацию идентификации по смарт-картам

Параметр	Описание
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к BPM. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к BPM

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

9.2.3 . Прямое подключение по протоколу RDP для доступа к ресурсам сервера терминалов

Для добавления подключения для доступа к MS RDS администратору Termidesk необходимо перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Новый]**, выбрать «Доступ к MS RDS по RDP (напрямую) [экспериментальный]».

Для добавления подключения для доступа к STAL администратору Termidesk необходимо перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Новый]**, выбрать «Доступ к STAL по RDP (напрямую) [экспериментальный]».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 59).

Таблица 59 – Данные для добавления прямого подключения к серверам терминалов

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде BPM
«Без домена»	Не использовать идентификатор домена при проверке полномочий субъекта. Для подключений к опубликованным приложениям и терминальным сессиям STAL переключатель «Без домена» должен быть установлен в положение «Да»
«Домен»	Идентификатор домена при проверке полномочий субъекта. Должно использоваться короткое имя домена. Для подключений к опубликованным приложениям и терминальным сессиям STAL значение параметра необходимо оставить пустым

Параметр	Описание
«Порт»	Выбор порта для подключения. По умолчанию используется порт 3389
«Разрешить смарт-карты»	Разрешить идентификацию субъектов на основе смарт-карт
«Разрешить принтеры»	Разрешить перенаправление устройств печати по протоколу RDP
«Разрешить диски»	Разрешить перенаправление устройств хранения по протоколу RDP
«Разрешить последовательные порты»	Разрешить перенаправление последовательных портов по протоколу RDP
«Показывать обои»	Отображать фоновое изображение, настроенное на рабочем столе
«Несколько мониторов»	Разрешить использовать несколько мониторов
«Разрешить композицию рабочего стола»	Разрешить темы рабочего стола
«Сглаживание шрифтов»	Использовать технологию сглаживания шрифтов
«Поддержка CredSSP»	Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider Параметр отсутствует для протокола «Доступ к STAL по RDP (напрямую)»
«Использовать ALSA»	Использовать программный микшер для передачи звука
«Параметры смарт-карты»	Указать конфигурацию идентификации по смарт-картам
«Все принтеры»	Выполнить перенаправление всех устройств печати по протоколу RDP. При выключенном параметре «Разрешить принтеры» данный параметр игнорируется
«RemoteFX»	Использовать технологию RemoteFX
«Все RemoteFX устройства»	Использовать все RemoteFX устройства
«Динамическое разрешение»	Разрешить передачу динамического разрешения для экрана рабочего стола ⚠ Параметр должен быть отключен при реализации доступа к STAL с рабочей станции пользователя на ОС Windows 11.
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к BPM. Указанные диапазоны должны быть созданы в «Компоненты - Сети»

Параметр	Описание
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к BPM

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

9.2.4 . Подключение по протоколу RDP для доступа к ресурсам сервера терминалов через компонент «Шлюз»

Для добавления подключения для доступа к MS RDS через компонент «Шлюз» администратору Termidesk необходимо перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Новый]**, выбрать «Доступ к MS RDS по RDP (через шлюз) [экспериментальный]».

> В Termidesk версии 4.3 протокол «Доступ к MS RDS по RDP (через шлюз) [экспериментальный]» не поддерживается. Для доступа к MS RDS следует выбирать протокол «Доступ к MS RDS по RDP (напрямую) [экспериментальный]».

Для добавления подключения для доступа к STAL через компонент «Шлюз» администратору Termidesk необходимо перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Новый]**, выбрать «Доступ к STAL по RDP (через шлюз) [экспериментальный]».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 60).

Таблица 60 – Данные для добавления подключения к серверам терминалов через «Шлюз»

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде BPM
«URL шлюза»	Адрес сервера в формате `ws(s)://192.0.2.30/websockify`, обеспечивающего формирование и поддержание соединения. Директива `ws` относится к использованию порта 80, директива `wss` означает использование 443 порта. Параметр `192.0.2.30` - доступный IP-адрес шлюза. Пример IP-адреса приведен в соответствии с RFC 5737, он должен быть заменен на актуальный, используемый согласно схеме адресации, принятой в инфраструктуре предприятия. Значение этого параметра не относится к значению `WSPROXY_BIND_ADDRESS` из конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf`
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза

Параметр	Описание
«Без домена»	Не использовать идентификатор домена при проверке полномочий субъекта. Для подключений к опубликованным приложениям и терминальным сессиям STAL переключатель «Без домена» должен быть установлен в положение «Да»
«Домен»	Идентификатор домена при проверке полномочий субъекта. Должно использоваться короткое имя домена. Для подключений к опубликованным приложениям и терминальным сессиям STAL значение параметра необходимо оставить пустым
«Порт»	Выбор порта для подключения. По умолчанию используется порт 3389
«Разрешить смарт-карты»	Разрешить идентификацию субъектов на основе смарт-карт
«Разрешить принтеры»	Разрешить перенаправление устройств печати по протоколу RDP
«Разрешить диски»	Разрешить перенаправление устройств хранения по протоколу RDP
«Разрешить последовательные порты»	Разрешить перенаправление последовательных портов по протоколу RDP
«Показывать обои»	Отображать фоновое изображение, настроенное на рабочем столе
«Несколько мониторов»	Разрешить использовать несколько мониторов
«Разрешить композицию рабочего стола»	Разрешить темы рабочего стола
«Сглаживание шрифтов»	Использовать технологию сглаживания шрифтов
«Поддержка CredSSP»	Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider Параметр отсутствует для протокола «Доступ к STAL по RDP (через шлюз)»
«Использовать ALSA»	Использовать программный микшер для передачи звука
«Параметры смарт-карты»	Указать конфигурацию идентификации по смарт-картам
«Все принтеры»	Выполнить перенаправление всех устройств печати по протоколу RDP. При выключенном параметре «Разрешить принтеры» данный параметр игнорируется
«RemoteFX»	Использовать технологию RemoteFX
«Все RemoteFX устройства»	Использовать все RemoteFX устройства
«Динамическое разрешение»	Разрешить передачу динамического разрешения для экрана рабочего стола ⚠ Параметр должен быть отключен при реализации доступа к STAL с рабочей станции пользователя на ОС Windows 11.

Параметр	Описание
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к BPM. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к BPM
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к BPM. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к BPM

9.3 . Протокол доставки SPICE

9.3.1 . Подключение по протоколу SPICE через vdi-viewer

Для подключения рабочей станции пользователя по протоколу SPICE имена узлов платформы виртуализации должны корректно разрешаться в IP-адреса этих узлов.

Для подключения по протоколу SPICE через vdi-viewer на узлах платформы виртуализации должна быть включена оптимизация для протокола SPICE, в базовый образ необходимо также установить пакет `termidesk-video-agent` (см. подраздел **Установка в среде ОС Astra Linux Special Edition 1.7** СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»), а на пользовательскую рабочую станцию необходимо установить пакет `termidesk-viewer` согласно подразделам **ОС Astra Linux Special Edition** и **ОС Microsoft Windows** документа СЛЕТ.10001-01 92 01 «Руководство администратора. Настройка и эксплуатация компонента «Клиент»).

Для добавления подключения по протоколу SPICE через `vdi-viewer` администратору Termidesk в графическом интерфейсе управления следует перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Новый]**, выбрать «SPICE (vdi-viewer, эксперим.)» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 61).

Таблица 61 – Данные для добавления подключения по SPICE через vdi-viewer

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки

Параметр	Описание
«Приоритет»	Преимущество использования протокола доставки в фонде BPM
«URL шлюза»	Адрес сервера в формате `ws(s)://192.0.2.30/websockify`, обеспечивающего формирование и поддержание соединения. Директива `ws` относится к использованию порта 80, директива `wss` означает использование 443 порта. Параметр `192.0.2.30` - доступный IP-адрес шлюза. Пример IP-адреса приведен в соответствии с RFC 5737, он должен быть заменен на актуальный, используемый согласно схеме адресации, принятой в инфраструктуре предприятия. Значение этого параметра не относится к значению `WSPROXY_BIND_ADDRESS` из конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf`
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза
«Сертификат»	Информация о публичном ключе для доступа к платформе виртуализации (опционально)
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к BPM. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу SPICE к BPM

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

9.3.2 . Подключение по протоколу SPICE через HTML5 (локальный прокси)

Начиная с Termidesk версии 4.3 для добавления подключения по протоколу SPICE через HTML5 необходимо установить в Termidesk плагин расширения `termidesk-html5spicetrans` в соответствии с подразделом **Установка плагинов расширений**. Существующий протокол этого типа не удалится из БД, однако не будет отображен в веб-интерфейсе без установки плагина расширения.

> ⚠ Для добавления этого протокола в Termidesk версии 4.3 необходимо использовать плагин расширения `termidesk-html5spicetrans` из плагинов версии 4.3.1.

После установки плагина расширения в графическом интерфейсе управления следует перейти «Компоненты - Протоколы доставки», затем нажать экранную кнопку **[Новый]** и выбрать из

выпадающего списка «SPICE (HTML5, через локальный прокси)». Заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 62).

Таблица 62 – Данные для добавления подключения по SPICE через локальный прокси

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде BPM
«URL шлюза»	Адрес сервера в формате `ws(s)://192.0.2.30/websockify`, обеспечивающего формирование и поддержание соединения. Директива `ws` относится к использованию порта 80, директива `wss` означает использование 443 порта. Параметр `192.0.2.30` - доступный IP-адрес шлюза. Пример IP-адреса приведен в соответствии с RFC 5737, он должен быть заменен на актуальный, используемый согласно схеме адресации, принятой в инфраструктуре предприятия. Значение этого параметра не относится к значению `WSPROXY_BIND_ADDRESS` из конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf`
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к BPM. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу SPICE к BPM

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

9.4 . Протокол доставки VNC

9.4.1 . Подключение по протоколу VNC через HTML5 (локальный прокси)

Для добавления подключения по протоколу VNC через HTML5 (локальный прокси) администратору Termidesk в графическом интерфейсе управления следует перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Новый]**, выбрать «VNC (HTML5, через локальный прокси)» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 63).

Таблица 63 – Данные для добавления подключения по VNC через локальный прокси

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде BPM
«URL шлюза»	Адрес шлюза в формате `ws(s)://192.0.2.30/websockify`, обеспечивающего формирование и поддержание соединения. Директива `ws` относится к использованию порта 80, директива `wss` означает использование 443 порта. Параметр `192.0.2.30` - доступный IP-адрес шлюза. Пример IP-адреса приведен в соответствии с RFC 5737, он должен быть заменен на актуальный, используемый согласно схеме адресации, принятой в инфраструктуре предприятия. По умолчанию используется адрес локальной установки `127.0.0.1`
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к BPM. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу VNC к BPM

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

9.5 . Протокол доставки Loudplay

9.5.1 . Прямое подключение по протоколу Loudplay

Для возможности добавления протокола доставки Loudplay необходимо включить экспериментальный параметр `experimental.loudplay.transports.enabled` в соответствии с подразделом **Управление экспериментальными параметрами Termidesk**.

⚠ Фонд BPM, использующий протокол доставки Loudplay, должен использовать шаблон BPM поставщика ресурсов «Физическая рабочая станция».
В шаблоне BPM должен быть указан IP-адрес ВМ, на которой установлен сервер Loudplay.

После включения экспериментального параметра в графическом интерфейсе управления перейти в «Компоненты - Протоколы доставки», а затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка «Loudplay (напрямую, эксперим.)».

Для добавления протокола доставки администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 64).

Таблица 64 – Данные для добавления прямого подключения по протоколу Loudplay

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде BPM
«Протокол передачи»	Выбор протокола для передачи данных. По умолчанию используется UDP
«Порт rtsp-сервера»	Выбор порта RTSP-сервера. По умолчанию используется 8554
«Путь к API»	Наименование канала для подключения. По умолчанию используется `/desktop`
«Порт управления (клавиатура/мышь)»	Выбор порта управления клавиатурой и мышью. По умолчанию используется 8555
«Порт служебный (bbr_port)»	Выбор служебного порта RPC. По умолчанию используется 8556
«Порт видео потока»	Выбор порта видеопотока. По умолчанию используется 6970
«Порт аудио потока»	Выбор порта аудиопотока. По умолчанию используется 6972
«Технология захвата»	Выбор технологии захвата изображения. По умолчанию используется FFmpeg DDA
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к BPM. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу Loudplay к BPM

9.5.2 . Подключение через компонент «Шлюз» по протоколу Loudplay

Ограничения возможности добавления протокола Loudplay через компонент «Шлюз» соответствуют ограничениям, приведенным для прямого подключения по данному протоколу.

После включения экспериментального параметра в графическом интерфейсе управления перейти в «Компоненты - Протоколы доставки», а затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка «Loudplay (через вебсокет шлюз, эксперим.)».

Для добавления протокола доставки администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 65).

Таблица 65 – Данные для добавления подключения через «Шлюз» по протоколу Loudplay

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде BPM
«URL шлюза»	Адрес сервера в формате `ws(s)://192.0.2.30/websockify`, обеспечивающего формирование и поддержание соединения. Директива `ws` относится к использованию порта 80, директива `wss` означает использование 443 порта. Параметр `192.0.2.30` - доступный IP-адрес шлюза. Пример IP-адреса приведен в соответствии с RFC 5737, он должен быть заменен на актуальный, используемый согласно схеме адресации, принятой в инфраструктуре предприятия. Значение этого параметра не относится к значению `WSPROXY_BIND_ADDRESS` из конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf`
«Протокол передачи»	Выбор протокола для передачи данных. По умолчанию используется UDP
«Порт rtsp-сервера»	Выбор порта RTSP-сервера. По умолчанию используется 8554
«Путь к API»	Наименование канала для подключения. По умолчанию используется `/desktop`
«Порт управления (клавиатура/мышь)»	Выбор порта управления клавиатурой и мышью. По умолчанию используется 8555
«Порт служебный (bbr_port)»	Выбор служебного порта RPC. По умолчанию используется 8556
«Порт видео потока»	Выбор порта видеопотока. По умолчанию используется 6970
«Порт аудио потока»	Выбор порта аудиопотока. По умолчанию используется 6972
«Технология захвата»	Выбор технологии захвата изображения. По умолчанию используется FFmpeg DDA
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)

Параметр	Описание
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к BPM. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу Loudplay к BPM

10 . СИСТЕМНЫЕ НАСТРОЙКИ

10.1 . Общие системные параметры Termidesk

Системные параметры позволяют задать основные значения, необходимые для успешного функционирования Termidesk.

Для конфигурации общих системных параметров в графическом интерфейсе управления следует перейти «Настройки - Системные параметры - Общие».
Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 65).

⚠ Изменение системных параметров вступают в силу только после перезагрузки Termidesk.

Таблица 66 – Общие системные параметры Termidesk

Параметр	Описание
«Генератор имен»	Варианты использования имен для развертывания ВРМ
«Тема оформления»	Тема оформления графического интерфейса пользователя и управления
«Автозапуск рабочего места»	Параметр конфигурации автоматического запуска ВРМ после его создания
«Интервал проверок кэша рабочих мест»	Период (в секундах) опроса фонда ВРМ для определения готовности ВРМ
«Интервал проверок неиспользуемых рабочих мест»	Временной интервал (в секундах) проверки ВРМ для последующего их отключения
«Интервал очистки информационных объектов»	Временной интервал очистки информации о событиях, возникающих в процессе эксплуатации Termidesk
«Количество потоков фоновых задач»	Количество одновременных задач, выполняемых планировщиком в фоновом процессе
«Не учитывать максимальные ограничения»	Не учитывать максимальные ограничения при формировании фондов ВРМ
«Время хранения информационных объектов»	Временной период хранения информации о событиях, возникающих в процессе эксплуатации
«Время блокировки входа»	Время (в секундах) после истечения которого будет возможен повторный вход субъекта с ролью «Администратор» или «Пользователь» в случае, если субъектом с указанной ролью был исчерпан лимит неудачных попыток входа

Параметр	Описание
«URL входа»	URL-адрес начальной страницы графического интерфейса управления ⚠ Значение параметра менять не следует.
«Максимальное время инициализации рабочего места»	Максимальное время (в секундах) ожидания готовности BPM
«Максимум записей в журнале для объектов»	Максимальное количество системных событий, добавляемых в журнал
«Интервал проверки для удаления объектов»	Интервал проверки (в секундах) BPM, помеченных для удаления
«Количество ошибок для ограничения фонда»	Пороговое значение количества ошибок, возникающих в процессе эксплуатации фонда BPM
«Интервал отслеживания ошибок в фонде»	Временной интервал появления ошибок, связанных с функционированием фонда BPM
«Количество потоков планировщика задач»	Пороговое значение потоков задач, выполняемых планировщиком, при обеспечении жизненного цикла фонда BPM
«Срок действия устаревшей публикации»	Временной интервал, по истечению которого публикация фонда BPM считается устаревшей и помечается для удаления из Termidesk
«Срок хранения статистики»	Временной интервал хранения файлов журналов
«Количество удаляемых рабочих мест за один проход»	Максимальное количество BPM, удаляемых единовременно из фонда BPM

Экранная кнопка **[Сохранить]** сохраняет общие системные параметры.

10.2 . Параметры безопасности Termidesk

Для конфигурации системных параметров безопасности в графическом интерфейсе управления следует перейти «Настройки - Системные параметры - Безопасность».

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей Настройка параметров безопасности в Termidesk.

Таблица 67 – Параметры безопасности Termidesk

Параметр	Описание
«Мастер-ключ»	Идентификатор регистрации субъектов в Termidesk при доступе к фонду BPM
«Доверенные хосты»	Идентификатор узлов, имеющих право подключаться к Termidesk
«Длительность сессии администратора»	Временной интервал сессии, инициированной на графический интерфейс управления

Параметр	Описание
«Доступ к веб-части системным пользователем»	Возможность субъекта с ролью «Администратор» подключаться к графическому интерфейсу
«Использовать анонсируемый IP клиента»	Использовать IP-адрес клиента, передаваемый в процессе входа в Termidesk
«GID системной группы администратора»	Идентификатор группы, в которую входит учетная запись субъекта с ролью «Администратор»
«Длительность сессии пользователя»	Временной интервал сессии субъекта с ролью «Пользователь», инициированной на графическом интерфейсе пользователя
«Максимум попыток входа Администраторов»	Пороговое положительное значение числа неудачных попыток входа Администраторов. Параметр может быть изменен только субъектом с правами администратора (см. **Назначение служебных функций администраторам**). Значение «0» эквивалентно «без ограничений»
«Максимум попыток входа Персонала»	Пороговое положительное значение числа неудачных попыток входа субъектов, не относящихся к Администраторам. Значение «0» эквивалентно «без ограничений»
«Максимум попыток входа Пользователей»	Пороговое положительное значение числа неудачных попыток входа пользователей. Значение «0» эквивалентно «без ограничений»

10.3 . Назначение служебных функций администраторам

В Termidesk реализовано разделение доступных служебных функций для администраторов.

Для добавления выбора доступных служебных функций следует перейти «Настройки - Управление ролями» и нажать экранную кнопку [Новый] (см. Рисунок 29).

При добавлении функции необходимо ввести текстовое наименование создаваемого класса администратора, а также выбрать список назначаемых разрешений.

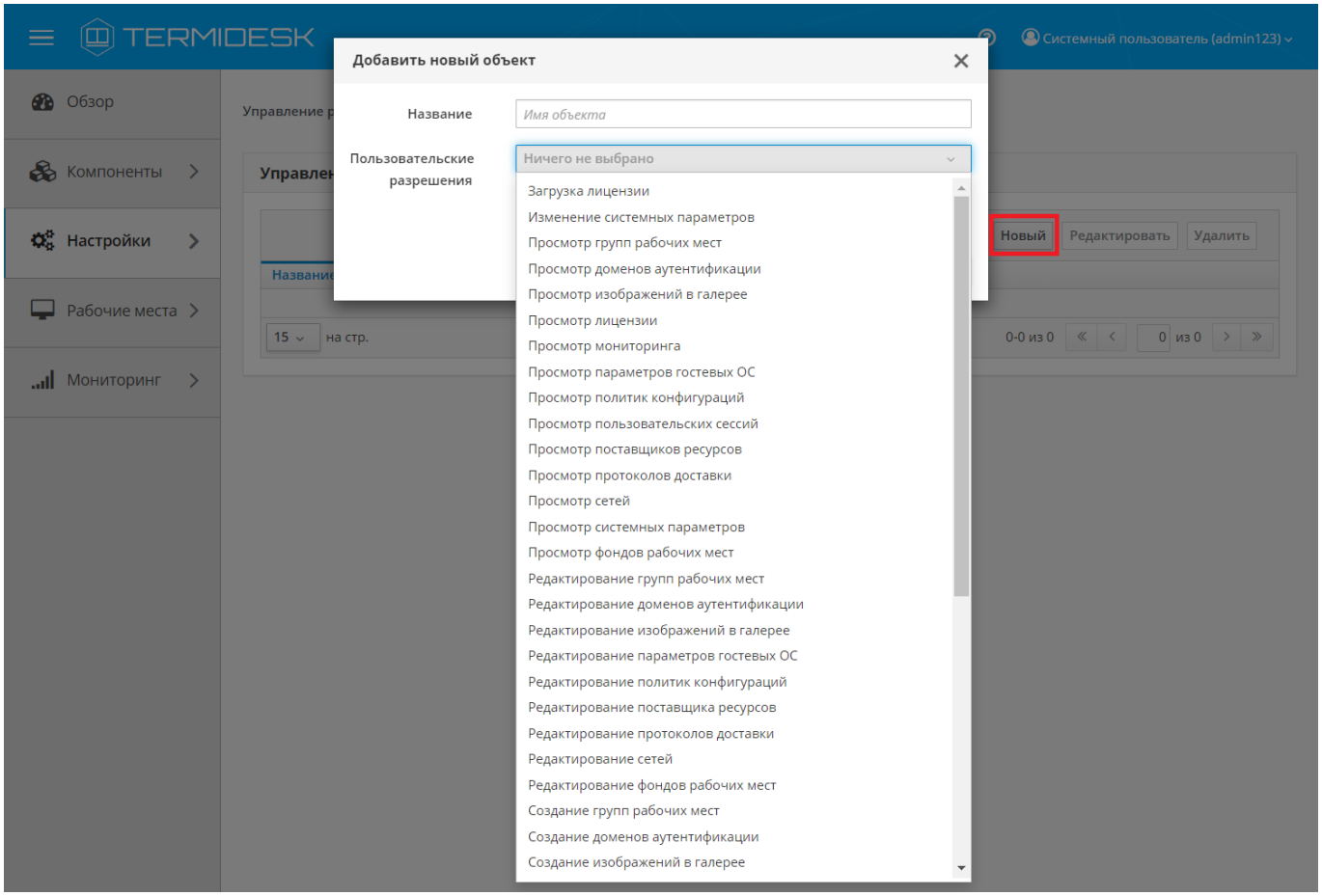

Рисунок 29 – Окно назначения пользовательских разрешений

Для редактирования класса администратора нужно выбрать его, а затем нажать экранную кнопку **[Редактировать]**.

Для удаления нужно выбрать созданный объект, а затем нажать экранную кнопку **[Удалить]**.

> ⚠ Класс администратора может быть удален только в том случае, если он не назначен пользователю.

Класс администратора может быть назначен определенному пользователю. Для назначения созданного класса следует перейти «Компоненты - Домены аутентификации» и затем в столбце «Название» сводной таблицы выбрать домен аутентификации, в который входит пользователь.

На открывшейся странице в таблице «Пользователи» нужно выбрать пользователя и нажать экранную кнопку **[Редактировать]**. В открывшейся форме редактирования пользователя в поле «Роли» выбрать класс (см. Рисунок 30).

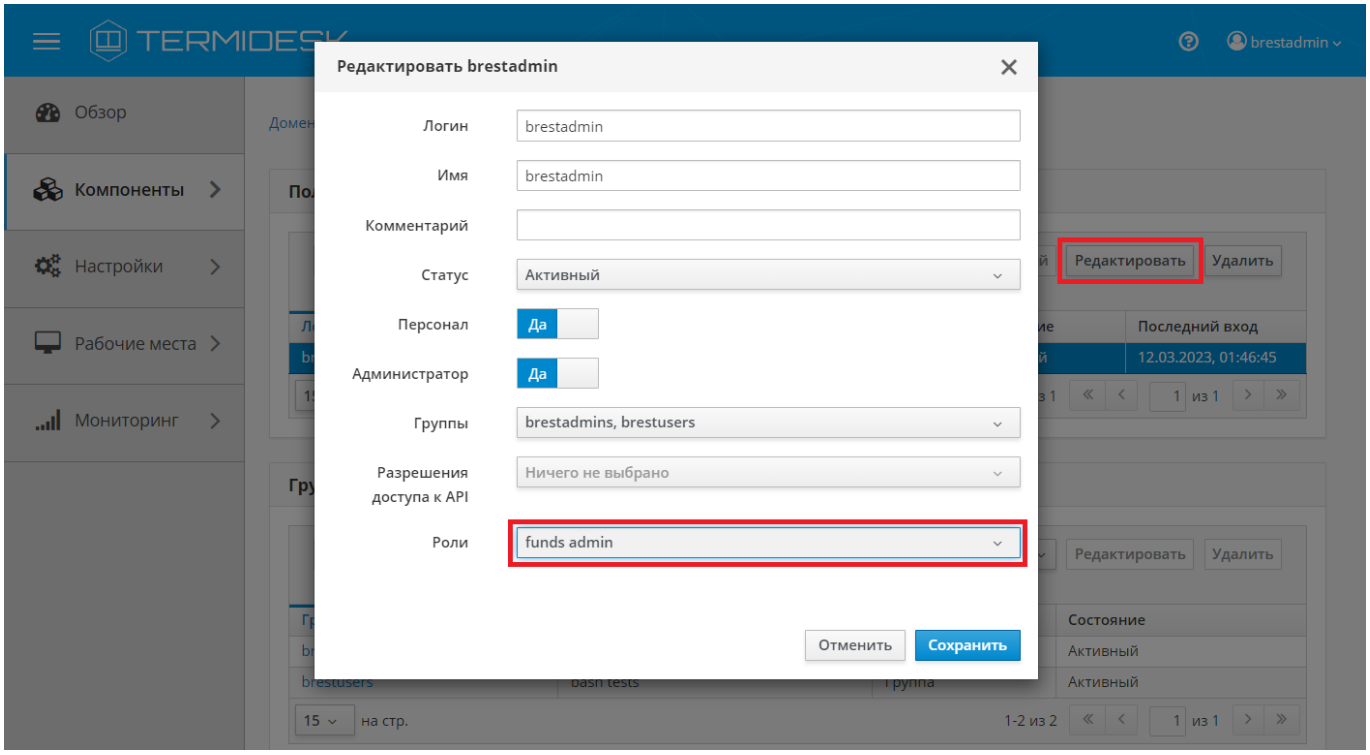

Рисунок 30 – Окно назначения пользовательских ролей

⚠ Параметр «Персонал» указывает, что пользователь является оператором Termidesk (класс администратора с ограниченными полномочиями в графическом интерфейсе Termidesk).

Созданным классам администраторов можно делегировать управление отдельными фондами BPM. Для добавления нового разрешения для объекта следует перейти «Настройки - Управление ACL», нажать экранную кнопку **[Новый]** и выбрать объект «Фонд рабочих мест».

В режиме добавления нового разрешения для объекта администратору Termidesk необходимо заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 68).

Таблица 68 – Доступные параметры при добавлении пользовательских разрешений для фондов BPM

Параметр	Описание
«Роль»	Наименование заранее созданного и назначенного пользователю класса администратора

Параметр	Описание
«Пользовательское разрешение»	Выбор пользовательских разрешений, касающихся фондов BPM. Список всех доступных разрешений: ▪ просмотр фондов BPM; ▪ редактирование фондов BPM; ▪ удаление фондов BPM; ▪ управление кешем фондов BPM; ▪ управление пользовательскими группами фондов BPM; ▪ управление пользователями фондов BPM; ▪ управление протоколами доставки фондов BPM; ▪ управление публикациями фондов BPM
«Объект»	Ранее созданный фонд BPM

10.4 . Перенаправление на HTTPS

Для того, чтобы веб-интерфейс Termidesk работал по безопасному протоколу HTTPS, используются настройки веб-сервера `apache` для перенаправления запроса с протокола HTTP на HTTPS.

Настройки перенаправления задаются в конфигурационном файле `/etc/apache2/sites-available/termidesk.conf`. После внесения любых изменений в этот файл необходимо перезапустить службу веб-сервера apache:

```
:~$ sudo systemctl restart apache2
```

⚠ Перенаправление на HTPS настроено по умолчанию после установки Termidesk. При необходимости использования незащищенного протокола HTTP администратор должен изменить файл `/etc/apache2/sites-available/termidesk.conf`, раскомментировав настройки VirtualHost и закомментировав настройки HTTPS.

Пример исходного конфигурационного файла:

```
#<VirtualHost *:80>
#    ServerName #HOSTNAME#
#    DocumentRoot /opt/termidesk/share/termidesk-vdi/src
#
#    Alias /media/ /opt/termidesk/share/termidesk-vdi/src/media/
#    Alias /static/ /opt/termidesk/share/termidesk-vdi/src/static/
#
#    <Directory /opt/termidesk/share/termidesk-vdi/src/static>
#        Order deny,allow
#        Allow from all
#        Require all granted
#    </Directory>
#
#    <Directory /opt/termidesk/share/termidesk-vdi/src/media>
#        Order deny,allow
```

```
#        Allow from all
#        Require all granted
#    </Directory>
#
#    RewriteEngine on
#    ProxyTimeout 70
#    ProxyPreserveHost On
#    ProxyRequests Off
#
#    ProxyPassMatch ^/media/ !
#    ProxyPassMatch ^/static/ !
#
#    ProxyPass /websockify  ws://127.0.0.1:5099/ timeout=10800
#    ProxyPassReverse /websockify ws://127.0.0.1:5099/ timeout=10800
#
#    ProxyPass / http://127.0.0.1:8000/
#    ProxyPassReverse / http://127.0.0.1:8000/
#
#    RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}
#
#    ErrorLog ${APACHE_LOG_DIR}/error.log
#    CustomLog ${APACHE_LOG_DIR}/access.log combined
#</VirtualHost>

# Сайт для принудительного перенаправления на протокол HTTPS.
<VirtualHost *:80>
        ServerName #HOSTNAME#
        ProxyPass /websockify  ws://127.0.0.1:5099/ timeout=10800
        ProxyPassReverse /websockify ws://127.0.0.1:5099/ timeout=10800
        RewriteEngine On
        RewriteCond "%{REQUEST_URI}" !^/websockify.*
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=308,L]
        RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<IfModule mod_ssl.c>
<VirtualHost _default_:443>
    ServerName #HOSTNAME#
    DocumentRoot /opt/termidesk/share/termidesk-vdi/src

    Alias /media/ /opt/termidesk/share/termidesk-vdi/src/media/
    Alias /static/ /opt/termidesk/share/termidesk-vdi/src/static/

    <Directory /opt/termidesk/share/termidesk-vdi/src/static>
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>

    <Directory /opt/termidesk/share/termidesk-vdi/src/media>
        Order deny,allow
        Allow from all
```

```
        Require all granted
    </Directory>

    RewriteEngine on
    ProxyTimeout 70
    ProxyPreserveHost On
    ProxyRequests Off

    ProxyPassMatch ^/media/ !
    ProxyPassMatch ^/static/ !

    ProxyPass /websockify  ws://127.0.0.1:5099/ timeout=10800
    ProxyPassReverse /websockify ws://127.0.0.1:5099/ timeout=10800

    ProxyPass / http://127.0.0.1:8000/
    ProxyPassReverse / http://127.0.0.1:8000/

    RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLEngine on
    SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

    # Для корректной работы Termidesk с MTLS необходимо настроить директивы ниже
    # в соответствии с условиями и требованиями окружения инсталляции
    # SSLCACertificateFile
    # SSLVerifyClient
    # SSLVerifyDepth

    # Проброс параметров клиентского сертификата в Termidesk
    # через набор собственных заголовков
    RequestHeader set X-TDSK-SSL_CLIENT_FORMAT 'apache'
    RequestHeader set X-TDSK-SSL_CLIENT_S_DN expr=%{SSL_CLIENT_S_DN}
    RequestHeader set X-TDSK-SSL_CLIENT_VALIDITY_START expr=%
{SSL_CLIENT_V_START}
    RequestHeader set X-TDSK-SSL_CLIENT_VALIDITY_END expr=%{SSL_CLIENT_V_END}
    RequestHeader set X-TDSK-SSL_CLIENT_VERIFY expr=%{SSL_CLIENT_VERIFY}
    RequestHeader set X-TDSK-SSL_CLIENT_CERT expr=%{SSL_CLIENT_CERT}
</VirtualHost>
</IfModule>
```

Пример конфигурационного файла для работы по незащищенному протоколу HTTP:

```
<VirtualHost *:80>
    ServerName #HOSTNAME#
    DocumentRoot /opt/termidesk/share/termidesk-vdi/src

    Alias /media/ /opt/termidesk/share/termidesk-vdi/src/media/
    Alias /static/ /opt/termidesk/share/termidesk-vdi/src/static/

    <Directory /opt/termidesk/share/termidesk-vdi/src/static>
```

```
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>

    <Directory /opt/termidesk/share/termidesk-vdi/src/media>
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>

    RewriteEngine on
    ProxyTimeout 70
    ProxyPreserveHost On
    ProxyRequests Off

    ProxyPassMatch ^/media/ !
    ProxyPassMatch ^/static/ !

    ProxyPass /websockify  ws://127.0.0.1:5099/ timeout=10800
    ProxyPassReverse /websockify ws://127.0.0.1:5099/ timeout=10800

    ProxyPass / http://127.0.0.1:8000/
    ProxyPassReverse / http://127.0.0.1:8000/

    RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

# Сайт для принудительного перенаправления на протокол  HTTPS.
# <VirtualHost *:80>
#        ServerName #HOSTNAME#
#        ProxyPass /websockify  ws://127.0.0.1:5099/ timeout=10800
#        ProxyPassReverse /websockify ws://127.0.0.1:5099/ timeout=10800
#        RewriteEngine On
#        RewriteCond "%{REQUEST_URI}" !^/websockify.*
#        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=308,L]
#        RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}
#    ErrorLog ${APACHE_LOG_DIR}/error.log
#    CustomLog ${APACHE_LOG_DIR}/access.log combined
#</VirtualHost>

# <IfModule mod_ssl.c>
# <VirtualHost _default_:443>
#    ServerName #HOSTNAME#
#    DocumentRoot /opt/termidesk/share/termidesk-vdi/src

#    Alias /media/ /opt/termidesk/share/termidesk-vdi/src/media/
#    Alias /static/ /opt/termidesk/share/termidesk-vdi/src/static/

#    <Directory /opt/termidesk/share/termidesk-vdi/src/static>
#        Order deny,allow
```

```
#        Allow from all
#        Require all granted
#    </Directory>

#    <Directory /opt/termidesk/share/termidesk-vdi/src/media>
#        Order deny,allow
#        Allow from all
#        Require all granted
#    </Directory>

#    RewriteEngine on
#    ProxyTimeout 70
#    ProxyPreserveHost On
#    ProxyRequests Off

#    ProxyPassMatch ^/media/ !
#    ProxyPassMatch ^/static/ !

#    ProxyPass /websockify  ws://127.0.0.1:5099/ timeout=10800
#    ProxyPassReverse /websockify ws://127.0.0.1:5099/ timeout=10800

#    ProxyPass / http://127.0.0.1:8000/
#    ProxyPassReverse / http://127.0.0.1:8000/

#    RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}

#    ErrorLog ${APACHE_LOG_DIR}/error.log
 #   CustomLog ${APACHE_LOG_DIR}/access.log combined

#    SSLEngine on
#    SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
#    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

    # Для корректной работы Termidesk с MTLS необходимо настроить директивы ниже
    # в соответствии с условиями и требованиями окружения инсталляции
    # SSLCACertificateFile
    # SSLVerifyClient
    # SSLVerifyDepth

    # Проброс параметров клиентского сертификата в Termidesk
    # через набор собственных заголовков
#    RequestHeader set X-TDSK-SSL_CLIENT_FORMAT 'apache'
#    RequestHeader set X-TDSK-SSL_CLIENT_S_DN expr=%{SSL_CLIENT_S_DN}
#    RequestHeader set X-TDSK-SSL_CLIENT_VALIDITY_START expr=%
{SSL_CLIENT_V_START}
#    RequestHeader set X-TDSK-SSL_CLIENT_VALIDITY_END expr=%{SSL_CLIENT_V_END}
#    RequestHeader set X-TDSK-SSL_CLIENT_VERIFY expr=%{SSL_CLIENT_VERIFY}
#   RequestHeader set X-TDSK-SSL_CLIENT_CERT expr=%{SSL_CLIENT_CERT}
# </VirtualHost>
#</IfModule>
```

10.5 . Замена SSL-сертификата веб-сервера

Для доступа к веб-интерфейсу Termidesk по протоколу HTTPS на этапе установки веб-сервера автоматически генерируется самоподписанный сертификат и закрытый ключ к нему. В некоторых случаях может понадобиться заменить эти сертификаты на другие.

> Ключ - последовательность псевдослучайных чисел, сгенерированная особым образом. Сертификат - артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу.

Для замены SSL-сертификатов необходимо:

- получить новый сертификат и ключ к нему;
- поместить новый сертификат формата `.pem` в каталог `/etc/ssl/certs/`:

```
:~$ sudo cp <путь_к_сертификату> /etc/ssl/certs/
```

- поместить новый ключ формата `.key` в каталог `/etc/ssl/private/`:

```
:~$ sudo cp <путь_к_ключу> /etc/ssl/certs/
```

> Если сертификат и ключ находятся в PKCS12-контейнере (файл формата `.pfx`), необходимо сначала сконвертировать их в нужный формат:
>
> ```
> :~$ openssl pkcs12 -in <путь_к_pfx-контейнеру> -out <путь_к_создаваемому_файлу.pem> -nodes
> :~$ openssl pkcs12 -in <путь_к_pfx-контейнеру> -nocerts -nodes -out <путь_к_создаваемому_файлу.key>
> ```

- отредактировать файл `/etc/apache2/sites-available/termidesk.conf`, заменив путь к сертификату и ключу для параметров `SSLCertificateFile` и `SSLCertificateKeyFile` на новые:

```
SSLEngine on
SSLCertificateFile      /etc/ssl/certs/new_cert.pem
SSLCertificateKeyFile /etc/ssl/private/new_key.key
</VirtualHost>
```

- перезапустить веб-сервер:

```
:~$ sudo systemctl restart apache2
```

10.6 . Установка корневого сертификата центра сертификации

Установка корневого сертификата центра сертификации (ЦС) может быть необходима при настройке доступа между компонентами по протоколу SSL. Предполагается, что инфраструктура открытых ключей (PKI) уже развернута в организации, ЦС установлен.

Для того чтобы установить корневой сертификат ЦС (например, `CA.crt`) на сервер Termidesk, нужно:

- скопировать файл `CA.crt` на сервер Termidesk;
- затем скопировать `CA.crt` в каталог `/usr/share/ca-certificates`:

```
:~$ sudo cp <путь_к_сертификату> /usr/share/ca-certificates/
```

- выполнить команду добавления корневого сертификата ЦС:

```
:~$ sudo dpkg-reconfigure ca-certificates
```

- на запрос «Доверять новым сертификатам удостоверяющих центров» ответить «Да»;
- убедиться, что сертификат `CA.crt` отмечен для активации;
- нажать экранную кнопку **[Ok]** и дождаться окончания операции.

Для настройки Termidesk на работу с сертификатами нужно:

- добавить переменную окружения `REQUESTS_CA_BUNDLE` в файле `/etc/opt/termidesk-vdi/termidesk.conf`. В переменной окружения нужно указать путь к файлу с доверенным корневым сертификатом. Пример:

```
REQUESTS_CA_BUNDLE=/etc/ssl/certs/ca.crt
```

- выполнить перезапуск службы `termidesk-vdi`:

```
:~$ sudo systemctl restart termidesk-vdi
```

10.7 . Работа веб-интерфейса Termidesk с протоколом TLS

Веб-интерфейс Termidesk по умолчанию поддерживает работу на всех протоколах, кроме SSLv3. Для того чтобы включить поддержку только протоколов TLS1.2 и TLS 1.3 в веб-сервере `apache`, нужно скорректировать файл конфигурации `/etc/apache2/mods-available/ssl.conf`.

Для этого:

- выполнить резервное копирование текущего файла конфигурации:

```
:~$ sudo cp /etc/apache2/mods-available/ssl.conf /etc/apache2/mods-available/ssl.conf_bkp
```

- включить поддержку только протоколов TLS1.2 и TLS 1.3, внеся изменения в файл конфигурации `/etc/apache2/mods-available/ssl.conf`:

```
:~$ sudo sed -i 's/SSLProtocol all -SSLv3/SSLProtocol -all +TLSv1.2 +TLSv1.3/g' /etc/apache2/mods-available/ssl.conf
:~$ sudo sed -i 's/SSLCipherSuite HIGH:!aNULL/SSLCipherSuite HIGH:!aNULL:!MD5:!3DES/g' /etc/apache2/mods-available/ssl.conf
:~$ sudo sed -i 's/#SSLHonorCipherOrder on/SSLHonorCipherOrder on/g' /etc/apache2/mods-available/ssl.conf
```

- выполнить обновление файлов конфигурации веб-сервера apache:

```
:~$ sudo systemctl reload apache2
```

10.8 . Управление авторизацией пользователя в компоненте «Клиент»

В Termidesk предусмотрена возможность управления авторизацией пользователя в компоненте «Клиент».

Для изменения параметров авторизации следует перейти «Настройки - Системные параметры - Аутентификация», и настроить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 69).

Для сохранения параметров авторизации нужно нажать экранную кнопку **[Сохранить]**.

Таблица 69 – Доступные параметры при настройке сохранения паролей в компоненте «Клиент»

Параметр	Описание
«Разрешить сохранение имени пользователя в клиенте»	Управление параметром сохранения имени пользователя в компоненте «Клиент» при подключении к серверу. Значение по умолчанию: «Да»
«Разрешить сохранение пароля в клиенте»	Управление параметром сохранения пароля в компоненте «Клиент» при подключении к серверу. Значение по умолчанию: «Да»
«Доп. информация при ошибке входа»	Информационное сообщение, отображаемое при ошибке входа

11 . РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ БД

11.1 . Резервное копирование БД

Резервное копирование БД, созданной СУБД Postgres-11 можно выполнить утилитой `pg_dump`:

```
:$ pg_dump -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W
--format=t > <имя_файла_для_сохранения_БД.tar>
```

где:

`-d <наименование БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`-h <IP-адрес_хоста>` - IP-адрес узла, где расположена БД. Если БД устанавливалась локально, нужно указать `localhost`;

`-p <порт>` - порт для подключения к БД. При стандартных настройках используется `5432`;

`-U <пользователь>` - имя пользователя для подключения. При стандартных настройках используется имя `termidesk`;

`-W` - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать `ksedimret`;

`--format=t` - ключ для экспорта БД в формате `tar`;

`<имя_файла_для_сохранения_БД.tar>` - имя и формат файла (`tar`) для сохранения БД.

11.2 . Восстановление БД из резервной копии

Восстановление БД из резервной копии выполняется командой:

```
:$ pg_restore -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь>
-W -f <файл_копии_БД.tar>
```

где:

`-d <наименование БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`-h <IP-адрес_хоста>` - IP-адрес узла, где расположена БД. Если используется локальная БД, нужно указать `localhost`;

`-p <порт>` - порт для подключения к БД. При стандартных настройках используется `5432`;

`-U <пользователь>` - имя пользователя для подключения. При стандартных настройках используется имя `termidesk`;

`-W` - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать `ksedimret`;

`-f <файл_копии_БД.tar>` - путь к файлу резервной копии БД.

12 . МОНИТОРИНГ И УВЕДОМЛЕНИЯ

12.1 . Системные параметры мониторинга

Системные параметры мониторинга позволяют настроить вывод событий в syslog-сервер.

Для конфигурации системных параметров мониторинга в графическом интерфейсе управления следует перейти «Настройки - Системные параметры - Мониторинг».
Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 70).

Таблица 70 – Параметры мониторинга Termidesk

Параметр	Описание
«Логирование Syslog»	Перенаправление потока событий мониторинга на отдельный syslog-сервер
«Хост 1» — «Хост 3»	IP-адреса или имена узлов, на которых развернута служба syslog-сервера
«Протокол»	Выбор протокола работы для службы syslog-сервера. Доступные значения: «UDP», «TCP», «TLS». При использовании протокола «TLS» необходимо установить на сервер Termidesk корневой сертификат ЦС, использующийся в syslog-сервере, согласно подразделу **Установка корневого сертификата центра сертификации**. Значение по умолчанию: «UDP»
«Категория сообщения»	Выбор категории сообщений, которые будут записываться в журнал мониторинга
«Уровень логирования»	Выбор уровня логирования событий (`INFO`, `WARNING`, `ERROR`, `CRITICAL`, `DEBUG`)

12.2 . Настройка отправки уведомлений о системных событиях

Для настройки отправки уведомлений о системных событиях в графическом интерфейсе управления следует перейти «Настройки - Системные параметры - Уведомления».

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 71).

Таблица 71 – Параметры отправки уведомлений о событиях

Параметр	Описание
«Вкл/выкл почтовых уведомлений»	Включение или отключение возможности отправки уведомлений о системных событиях по электронной почте
«Хост»	IP-адрес или имя узла, на котором развернута служба сервера электронной почты

Параметр	Описание
«Порт»	Номер порта, на котором ведется прослушивание службой сервера электронной почты
«Email отправителя»	Почтовый адрес отправителя сообщений на сервере электронной почты. Формат: `mailto:user@mail.domain`
«Пользователь»	Идентификатор пользователя сервиса электронной почты
«Пароль»	Последовательность символов для подтверждения полномочий пользователя сервиса электронной почты
«Поддержка TLS»	Включение поддержки протокола TLS при взаимодействии с сервером электронной почты
«Поддержка SSL»	Включение поддержки протокола SSL при взаимодействии с сервером электронной почты
«Таймаут»	Время ожидания (в секундах) ответа от сервера электронной почты
«Email получателей (через запятую)»	Перечень адресов электронной почты получателей уведомлений. Формат: `mailto:user@mail.domain`
«Префикс для темы письма»	Текстовое поле, содержащее информацию для подстановки в тему электронного письма
«Уведомление о смене режима техобслуживания в поставщике ресурсов»	Включение возможности отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания в поставщике ресурсов»
«Уведомление о смене режима техобслуживания в фонде рабочих мест»	Включение возможности отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания в фонде рабочих мест»
«Уведомление о возникновении ошибок с рабочими местами»	Включение возможности отправки уведомления по электронной почте о системном событии «Возникновение ошибок внутри фонда рабочих мест»
«Уведомление о превышении лицензированного количества подключений»	Включение возможности отправки уведомления по электронной почте о системном событии «Запрос подключения сверх лимита, установленного лицензией»
«Уведомление о превышении лицензированного количества пользователей»	Включение возможности отправки уведомления по электронной почте о системном событии «Запрос входа пользователя сверх лимита, установленного лицензией»

12.3 . Шаблон для мониторинга Zabbix

Termidesk поддерживает мониторинг состояния компонентов через `Zabbix`.

Шаблон для мониторинга распространяется через `iso`-образ Termidesk.

В шаблоне находятся метрики для мониторинга компонентов сервера Termidesk: универсального диспетчера, шлюза, менеджера BPM.

Реализованы как простые проверки (подключение к портам), так и опрос состояния служб `health checking`.

12.4 . Отчеты

Для формирования отчетов о событиях в графическом интерфейсе управления следует перейти «Мониторинг - Отчеты».

Можно сформировать следующие отчеты:

- отчет по последнему пользовательскому входу в систему;
- отчет по пользовательским сеансам;
- отчет по пользовательским подключениям.

Для формирования отчета по последнему пользовательскому входу в систему надо нажать экранную кнопку **[Новый]**, выбрать тип отчета «Отчет по последнему пользовательскому входу в систему» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 72).

Таблица 72 – Параметры для формирования отчета по последнему пользовательскому входу в Termidesk

Параметр	Описание
«Название»	Текстовое наименование отчета
«Комментарий»	Информационное сообщение, используемое для описания отчета
«Дата и время начала»	Дата и время начала события, от которых будет сформирован отчет. Для выбора даты и времени надо нажать левой кнопкой мыши в поле ввода, затем выбрать нужное значение и нажать клавишу **<Enter>** для подтверждения выбора

⚠ Если сформированные отчеты не содержат никакой информации (пустые), необходимо проверить, что системный параметр аудита «Сохранение в БД» установлен в значение «Да» (см. подраздел **Системные параметры аудита**).

Для формирования отчета по пользовательским сеансам надо нажать экранную кнопку **[Новый]**, выбрать тип отчета «Отчет по пользовательским сеансам» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 73).

Таблица 73 – Параметры для формирования отчета по пользовательским сеансам

Параметр	Описание
«Название»	Текстовое наименование отчета
«Комментарий»	Информационное сообщение, используемое для описания отчета
«Дата и время начала сеанса»	Дата и время начала события. Для выбора даты и времени надо нажать левой кнопкой мыши в поле ввода, затем выбрать нужное значение и нажать клавишу **<Enter>** для подтверждения выбора

Параметр	Описание
«Дата и время завершения сеанса»	Дата и время завершения события. Для выбора даты и времени надо нажать левой кнопкой мыши в поле ввода, затем выбрать нужное значение и нажать клавишу **<Enter>** для подтверждения выбора
«Домен аутентификации»	Наименование домена аутентификации, по которому будет осуществлен поиск события
«Пользователь»	Логин пользователя, по которому будет осуществлен поиск события

Для формирования отчета по пользовательским подключениям надо нажать экранную кнопку **[Новый]**, выбрать тип отчета «Отчет по пользовательским подключениям» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 74).

Таблица 74 – Параметры для формирования отчета по пользовательским подключениям

Параметр	Описание
«Название»	Текстовое наименование отчета
«Комментарий»	Информационное сообщение, используемое для описания отчета
«Дата и время начала подключения»	Дата и время начала события. Для выбора даты и времени надо нажать левой кнопкой мыши в поле ввода, затем выбрать нужное значение и нажать клавишу **<Enter>** для подтверждения выбора
«Дата и время завершения подключения»	Дата и время завершения события. Для выбора даты и времени надо нажать левой кнопкой мыши в поле ввода, затем выбрать нужное значение и нажать клавишу **<Enter>** для подтверждения выбора

Для просмотра сформированного отчета следует перейти «Мониторинг – Отчеты» и выбрать название отчета.

При помощи экранной кнопки **[CSV]** можно выгрузить в `csv`-файл весь представленный отчет (см. Рисунок 31).

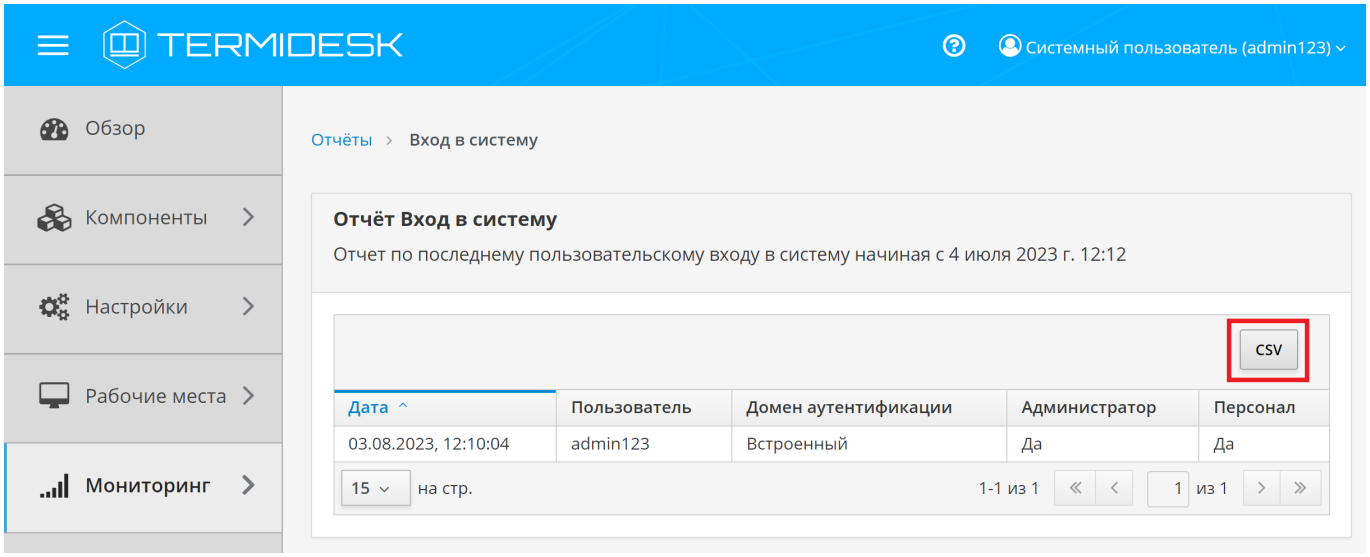

Рисунок 31 – Окно сформированного отчета по последнему пользовательскому входу

13 . СИСТЕМА АУДИТА

13.1 . Системные параметры аудита

Для конфигурации системных параметров аудита в графическом интерфейсе управления следует перейти «Настройки - Системные параметры - Аудит».

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 74).

Таблица 75 – Системные параметры аудита

Параметр	Описание
«Использовать "строгий" режим аудита»	Включение режима максимально полного сохранения информации о событиях аудита
«Сохранение в БД»	Выбор сохранения событий аудита в БД
«Время хранения записи в БД (дней)»	Время хранения (в днях) записи события аудита в БД
«Максимум удаляемых событий»	Максимальное количество удаляемых событий в журнале аудита
«Сохранение в файл»	Выбор сохранения событий аудита в отдельный файл журнала
«Файл хранения событий»	Указание полного пути к файлу хранения журнала событий аудита при выбранной опции «Сохранение в файл»
«Количество архивных файлов»	Максимальное количество архивных файлов журнала событий аудита, по достижении которого начинается перезапись
«Отправка в Syslog»	Направление логирования на отдельный syslog-сервер
«Хост»	IP-адрес или имя узла, на котором развёрнута служба syslog-сервера
«Протокол»	Выбор протокола работы для службы syslog-сервера. Доступные значения: «UDP», «TCP», «TLS». При использовании протокола «TLS» необходимо установить на сервер Termidesk корневой сертификат ЦС, использующийся в syslog-сервере, согласно подразделу **Установка корневого сертификата центра сертификации**. Значение по умолчанию: «UDP»
«Порт»	Порт, на котором находится служба syslog-сервера
«Категория сообщения»	Выбор категории сообщений, которые будут записываться в журнал аудита

События аудита, регистрируемые Termidesk:

- события, связанные с интерфейсом командной строки:
  - изменение системных параметров Диспетчера подключений через командную строку;
  - операции пользователей с объектами;

- события, связанные с политиками фонов BPM:
  - изменение глобальных политик;
  - изменение политик рабочего места;
  - сброс политики рабочего места;
  - сброс глобальных политик;
- события, связанные с пользователем:
  - подключение пользователя к BPM;
  - отключение пользователя от BPM;
  - вход пользователя в ОС BPM;
  - выход пользователя из ОС BPM;
  - блокировка гостевой ОС BPM;
  - разблокировка гостевой ОС BPM;
  - неактивность пользователя;
  - активность пользователя;
  - подключение пользователя к BPM и начало работы;
  - прекращение сессии пользователя по команде с сервера;
- события, связанные с веб-интерфейсом Termidesk:
  - вход пользователя в систему через веб-интерфейс;
  - выход пользователя из веб-интерфейса;
  - изменение системных параметров Termidesk;
  - операции пользователей с объектами через REST API;
  - загрузка файла лицензии через REST API;
  - прекращение сессии пользователя по команде с сервера;
  - сброс сессии пользователя по команде с сервера.

13.2 . Журналы

Журналы сервера Termidesk хранятся в каталоге `/var/log/termidesk`.

Установлены следующие журналы Termidesk, разделенные по типам событий, которые в них записываются:

- `auth.log` - записываются события об авторизации субъектов в Ternidesk;
- `celery-beat.log` - записываются события периодической проверки состояния обработчика заданий через RabbitMQ. Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;
- `celery-worker.log` - записываются события обработчика заданий через RabbitMQ. Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;

- other.log - записываются события платформ ПК СВ Брест и VMware, а также события, не относящиеся к другим модулям;
- services.log - записываются события работы ВМ на платформе oVirt;
- database.log - записываются отладочные события БД;
- termidesk.log - записываются события работы сервера Termidesk;
- use.log - записываются события подключения пользователей BPM;
- workers.log - записываются события обработчика фоновых задач;
- wsproxy.log - записываются события компонента «Шлюз», если он установлен на узле.

Настройки ротации журналов определены в конфигурационном файле /etc/logrotate.d/termidesk.local.

13.3 . Настройка журналирования

Уровень журналирования задается параметром LOG_LEVEL в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf.

Для изменения уровня журналирования необходимо:

- изменить параметр LOG_LEVEL;
- перезапустить службы Termidesk:

```
:~$ sudo systemctl restart termidesk-vdi.service termidesk-taskman.service termidesk-wsproxy.service termidesk-celery-beat.service termidesk-celery-worker.service
```

13.4 . Просмотр журналов

Для просмотра общего журнала событий, связанного с функционированием Termidesk и действиями субъектов доступа, следует перейти «Мониторинг – Журнал», где визуализируются системные события с указанием уровня важности (CRITICAL, ERROR, WARNING, INFO, DEBUG) и источника возникновения события.

При помощи экранной кнопки [CSV] можно выгрузить в csv-файл весь представленный журнал событий.

Количество событий, отображаемых в графическом интерфейсе или экспортируемых в csv-файл, можно менять при помощи выпадающего списка «Количество записей для загрузки». Таким образом можно задать 100, 500, 1000 записей или ввести свое значение в доступном поле.

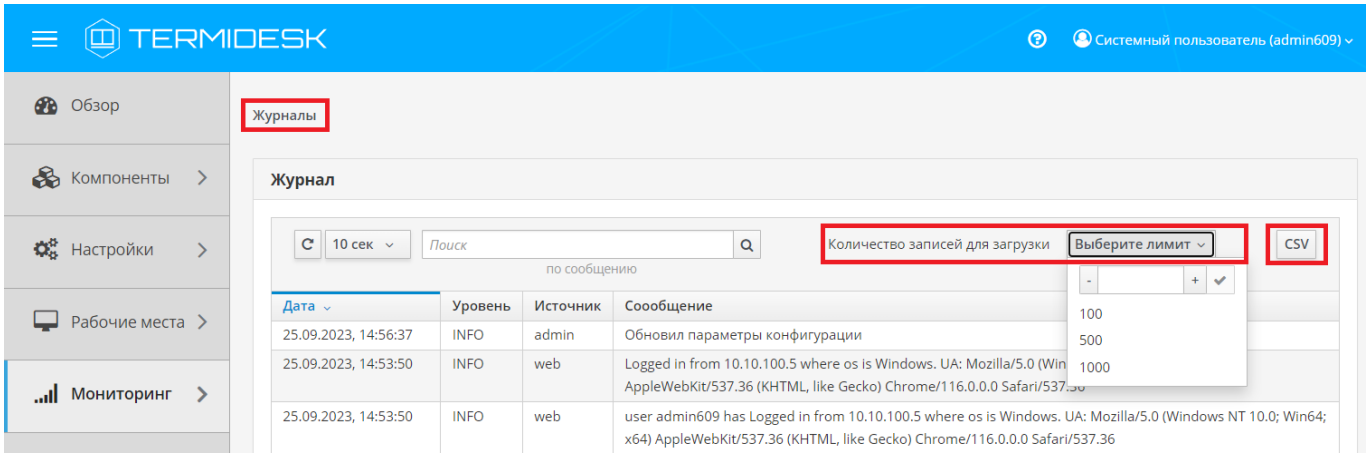

Рисунок 32 – Отображение общего журнала в графическом интерфейсе управления Termidesk

Для просмотра журнала событий, связанного с действиями субъектов доступа, следует перейти «Мониторинг – Аудит».

При помощи экранной кнопки [CSV] (см. Рисунок 33) можно выгрузить в csv-файл весь представленный журнал событий, либо строки событий.

Количество событий, отображаемых в графическом интерфейсе или экспортируемых в csv-файл, можно менять при помощи выпадающего списка «Количество записей для выгрузки». Таким образом можно задать 100, 500, 1000 записей или ввести свое значение в доступном поле.

При помощи экранной кнопки **[Копировать]** строки событий можно скопировать в буфер обмена.

> ⚠ Если события аудита не отображаются во вкладке «Мониторинг – Аудит», необходимо убедиться, что в «Настройки - Системные параметры - Аудит» параметр «Сохранение в БД» имеет значение «Да».

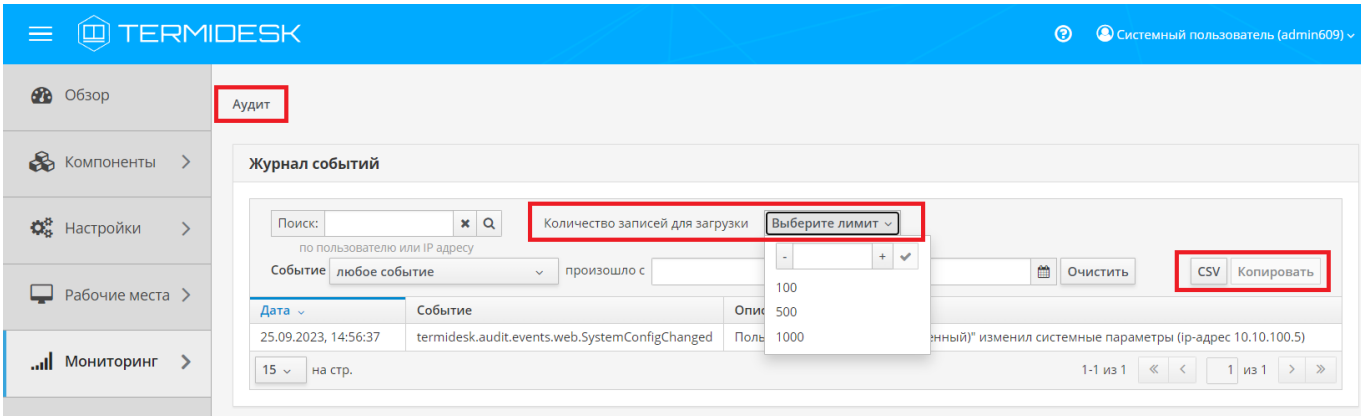

Рисунок 33 – Отображение журнала аудита в графическом интерфейсе управления Termidesk

13.5 . Описание шаблонов событий аудита

13.5.1 . Типы данных регистрируемой информации событий аудита

При фиксации событий аудита используется ряд типов данных (см. Таблица 76) регистрируемой информации, состав которых может отличаться для разных событий.

Таблица 76 – Типы данных регистрируемой информации

Тип данных	Описание
Дата/время	Дата и время указываются в формате: `DD.MM.YYYY`, `hh:mm:ss`, где: `DD.MM.YYYY` обозначает «день» - «месяц» - «год»; `hh:mm:ss` обозначает элементы времени «час» - «минута» - «секунда»; «.» и «:» используются как разделители в обозначениях даты и времени дня соответственно
Имя/логин	Идентификационные данные субъекта, совершающего доступ к объекту
Наименование параметра/секции/политики	Указывает объект, над которым производится действие
Значение	Указывается значение, которое принимал или принял объект после выполнения над ним операции
Тип объекта/сущности	Указывает тип объекта, над которым производится действие
Действие	Название операции, которую совершил субъект над объектом
Уровень важности	Показатель критичности события
Идентификатор	Указывают уникальную (для соответствующего объекта) последовательность чисел для его однозначной идентификации
IP-адрес	32-битовое число. Формой записи IP-адреса является запись в виде четырех десятичных чисел значением от 0 до 255, разделенных точками (например, 192.0.2.1)

13.5.2 . Типы и шаблоны регистрируемых событий аудита

Список регистрируемых событий и шаблоны к ним приведены в таблице (см. Таблица 77).

Таблица 77 – Список типов и шаблонов регистрируемых событий аудита

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
События, связанные с командной строкой		
Изменение системных параметров Диспетчера подключений через командную строку `cli.SystemConfigChanged`	Регистрируется: ▪ логин пользователя (`username`); ▪ название секции (`section_name`); ▪ название изменяемого параметра; (`parameter_key`); ▪ новое значение параметра (`parameter_value`)	«Пользователь "`[username]`" изменил системный параметр `[section_name].[parameter_key]=[parameter_value]`»

CRUD операции с объектами через CLI `cli.EntityAction`	Регистрируется: ▪ имя системного пользователя, запустившего команду (`username`); ▪ тип сущности (`entity`); ▪ уникальный идентификатор (`uuid`); ▪ тип объекта (`subtype`); ▪ название объекта (`name`); ▪ действие над объектом (`action`)	«Пользователь `"[username]"` выполнил операцию `[action]` для объекта `[entity] ([uuid]) [subtype] "[name]"`»
События, связанные с политиками		
Изменение глобальных политик `policies.GlobalPolicyChanged`	Регистрируется: ▪ имя пользователя (`username`); ▪ название домена аутентификации пользователя (`authenticator_name`); ▪ название политики (`policy_name`); ▪ новое значение в дружественном к пользователю описании (`value`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`); ▪ новое значение, в оригинальном формате (`value_raw`)	«Пользователь `"[username] ([authenticator_name])"` изменил значение глобальной политики `"[policy_name]"` на `"[value]"`»

Изменение политик BPM `policies.DeployedServicePolicyChanged`	Регистрируется: ▪ имя пользователя (`username`); ▪ название домена аутентификации пользователя (`authenticator_name`); ▪ название политики (`policy_name`); ▪ название фонда BPM (`deployed_service_name`); ▪ новое значение в дружественном к пользователю описании (`value`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`); ▪ идентификатор фонда BPM (`deployed_service_uuid`); ▪ новое значение, в оригинальном формате (`value_raw`)	«Пользователь "`[username] ([authenticator_name])`" изменил значение политики "`[policy_name]`" для фонда "`[deployed_service_name]`" на "`[value]`"»
Сброс политики BPM `policies.DeployedServicePolicyDeleted`	Регистрируется: ▪ имя пользователя (`username`); ▪ название домена аутентификации пользователя (`authenticator_name`); ▪ название политики (`policy_name`); ▪ название фонда BPM (`deployed_service_name`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`); ▪ идентификатор фонда BPM (`deployed_service_uuid`)	«Пользователь "`[username] ([authenticator_name])`" сбросил значение политики "`[policy_name]`" для фонда "`[deployed_service_name]`"»

Сброс глобальных политик `policies.GlobalPolicyDeleted`	Регистрируется: ▪ имя пользователя (`username`); ▪ название домена аутентификации пользователя (`authenticator_name`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`)	«Пользователь `"[username] ([authenticator_name])"` сбросил значение глобальной политики `"[policy_name]"`»
События, связанные с пользователем		
Подключение пользователя к BPM `workplace.UserConnected`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя фонда BPM (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`); ▪ Протокол доставки (`transport`)	«К рабочему месту `[vm_name]([vm_ip])` фонда `[workplace]` пользователя `"[username]([authenticator])"` произведено подключение с помощью протокола `[transport]`»
Отключение пользователя от BPM `workplace.UserDisconnected`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя фонда BPM (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`); ▪ Протокол доставки (`transport`)	«Подключение к рабочему месту `[vm_name]([vm_ip])` фонда `[workplace]` пользователя `"[username] ([authenticator])"` по протоколу `[transport]` разорвано»

Вход пользователя в ОС ВМ `workplace.UserLogin`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ Логин пользователя (`username`); ▪ Имя пользователя совершающего вход в гостевую ОС ВМ (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда ВРМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username] ([authenticator])`" вошел в гостевую ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]` с ip-адреса `[ip]`»
Выход пользователя из ОС ВМ `workplace.UserLogout`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя совершающего вход в гостевую ОС ВМ (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда ВРМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username] ([authenticator])`" вышел из гостевой ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]` с ip-адреса `[ip]`»
Блокировка ВРМ `workplace.UserLock`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя совершающего выход из гостевой ОС ВМ (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда ВРМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username] ([authenticator])`" заблокировал гостевую ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]`»

Разблокировка BPM `workplace.UserUnlock`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя совершающего выход из гостевой ОС ВМ (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда BPM (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username] ([authenticator])`" разблокировал гостевую ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]`»
Пользователь неактивен `workplace.UserIdle`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя совершающего выход из гостевой ОС ВМ (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда BPM (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username] ([authenticator])`" неактивен в гостевой ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]`»
Пользователь активен `workplace.UserActive`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя совершающего выход из гостевой ОС ВМ (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда BPM (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username] ([authenticator])`" вновь активен в гостевой ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]`»

Подключение пользователя к BPM и начало работы `user.WorkplaceConnectionRequest`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ название фонда BPM (`workplace`); ▪ имя выданной BM (`vm_name`); ▪ название протокола доставки (`transport`)	«Пользователь "`[username] ([authenticator])`" подключился к BM `[vm_name]` фонда `[workplace]` по протоколу `[transport]` с ip-адреса `[ip]`»
Прекращение сессии пользователя по команде с сервера `user.WorkplaceMessageSent`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`); ▪ имя пользователя (`username`); ▪ название фонда BPM (`deployed_service_name`); ▪ идентификатор фонда BPM (`deployed_service_uuid`); ▪ название BPM (`user_service_name`); ▪ идентификатор BPM (`user_service_uuid`); ▪ тип сообщения (`msg_level`); ▪ текст сообщения (`msg_text`)	«Пользователь `[username] ([authenticator])` отправил сообщение "`[msg_text]`" уровня `[msg_level]` на рабочее место `[user_service_name]` фонда `[deployed_service_name]`»
События, связанные с веб-интерфейсом		
Вход пользователя в систему через веб-интерфейс `web.UserLogin`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`)	«Пользователь "`[username] ([authenticator])`" вошел в систему с ip-адреса `[ip]`»

Выход пользователя из веб-интерфейса `web.UserLogout`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`)	«Пользователь "`[username]` (`[authenticator]`)" вышел из системы (ip-адрес `[ip]`)»
Изменение системных параметров Диспетчера подключений `web.SystemConfigChanged`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`)	«Пользователь "`[username]` (`[authenticator]`)" изменил системные параметры (ip-адрес `[ip]`)»
CRUD операции с объектами через REST API `web.EntityAction`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ тип сущности (`entity`); ▪ идентификатор (`uuid`); ▪ тип объекта (`subtype`); ▪ название объекта (`name`); ▪ действие над объектом (`action`)	«Пользователь "`[username]` (`[authenticator]`)" выполнил операцию `[action]` для объекта `[entity]` (`[uuid]`) `[subtype]` "`[name]`" (ip-адрес `[ip]`)»
Загрузка файла лицензии через REST API `web.LicenseUpdated`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя файла лицензии (`license_file_name`)	«Пользователь "`[username]` (`[authenticator]`)" загрузил новый файл лицензии `[license_file_name]` с ip-адреса `[ip]`»
Прекращение сессии пользователя по команде с сервера `web.LogoffUserservice`	Регистрируется: ▪ логин пользователя (`user`); ▪ данные гостевой ВМ, сессию которой прекратили (`userservice`)	«Пользователь "`[user]`" отправил запрос на прекращение сессии `[userservice]`»

Сброс сессии пользователя по команде с сервера `web.DisconnectUserservice`	Регистрируется: ▪ логин пользователя (`user`); ▪ данные гостевой ВМ, сессию которой прекратили (`userservice`)	«Пользователь "`[user]`" отправил запрос на сброс сессии `[userservice]`»

13.5.3 . Форматы регистрируемых событий аудита и их примеры

Каждая запись аудита регистрируются в формате: `[Дата][termidesk.audit.events.`Наименование события`]` `[Текст события согласно шаблону]`.

Пример регистрации события аудита «Изменение системных параметров Диспетчера подключений»:

Дата	Событие	Текст события
28.08.2023, 16:55:35	termidesk.audit.events.web.SystemConfigChanged	«Пользователь "admin123(Встроенный)" изменил системные параметры (ip-адрес 192.0.2.1)»

Пример регистрации события аудита «CRUD операции с объектами через REST API»:

Дата	Событие	Текст события
28.08.2023, 17:02:59	termidesk.audit.events.web.EntityAction	«Пользователь "u(Встроенный)" выполнил операцию read для объекта Provider (c1305fb0-e2ab-5fae-905b-b441c816f1f9) SessionsPlatform "RDS Provider (ip)" (ip-адрес 192.0.2.1)»

Пример регистрации события аудита «Пользователь неактивен»:

Дата	Событие	Текст события
28.08.2023, 17:04:00	termidesk.audit.events.workplace.UserIdle	«Пользователь "user1(FreeIPA)" неактивен в гостевой ОС ВМ a17olf-a17s-120(192.0.2.1) фонда a17olf-a17s-2 как пользователь u»

14 . РЕЖИМ ВЫСОКОЙ ДОСТУПНОСТИ И РАБОТА С СЕРТИФИКАТАМИ

14.1 . Настройка менеджера BPM в режиме высокой доступности

Настройка выполняется после установки программного комплекса в распределенной конфигурации.

Последовательность настройки узлов с менеджером BPM следующая:

- на узле, выбранном в качестве `master`, помимо уже запущенных служб, запустить только службу `termidesk-taskman`, не добавляя ее в раздел автоматической загрузки:

```
:~$ sudo systemctl start termidesk-taskman
```

- на узлах `master` и `slave` установить пакеты программ для организации высокой доступности:

```
:~$ sudo apt install -y keepalived ipset
```

где:

`-y` - ключ для пропуска подтверждения установки;

- на узлах `master` и `slave` создать каталог `/etc/keepalived/` (если каталог ранее не был создан):

```
:~$ sudo mkdir -p /etc/keepalived
```

где:

`-p` - ключ для создания подкаталогов в указанном пути, если их не существует;

- на узлах `master` и `slave` в каталоге `/etc/keepalived/` создать пустые файлы `keepalived.conf` (файл настроек режима высокой доступности) и `notify.sh` (управление переключениями режимов высокой доступности):

```
:~$ sudo touch /etc/keepalived/keepalived.conf
:~$ sudo touch /etc/keepalived/notify.sh
```

- отредактировать созданный файл `/etc/keepalived/keepalived.conf`, приведя его к следующему виду (по очереди на каждом из узлов):

```
global_defs {

    router_id NAME_OF_ROUTER_ID # НУЖНО УКАЗАТЬ: hostname хоста
    script_user user # НУЖНО УКАЗАТЬ: вместо user -> пользователь, от имени которого запускается keepalived
    enable_script_security
}
```

```
7
8   vrrp_script check_httpd {
9       script "/usr/bin/pgrep apache" # path of the script to execute
10      interval 1  # seconds between script invocations, default 1 second
11      timeout 3   # seconds after which script is considered to have failed
12      #weight <INTEGER:-254..254>  # adjust priority by this weight, default
    0
13      rise 1              # required number of successes for OK transition
14      fall 2              # required number of successes for KO transition
15      #user USERNAME [GROUPNAME]   # user/group names to run script under
16      init_fail                   # assume script initially is in failed
    state
17  }
18
19  # Для каждого виртуального IPv4-адреса создается свой экземпляр vrrp_instance
20  vrrp_instance termidesk-taskman {
21      notify /etc/keepalived/notify.sh
22
23      # Initial state, MASTER|BACKUP
24      # As soon as the other machine(s) come up,
25      # an election will be held and the machine
26      # with the highest priority will become MASTER.
27      # So the entry here doesn't matter a whole lot.
28      state BACKUP
29
30      # interface for inside_network, bound by vrrp
31      # НУЖНО УКАЗАТЬ: eth0 -> интерфейс, смотрящий в Интернет
32      interface eth0
33
34      # arbitrary unique number from 0 to 255
35      # used to differentiate multiple instances of vrrpd
36      # running on the same NIC (and hence same socket).
37      # НУЖНО УКАЗАТЬ: вместо 106 -> номер экземпляра vrrp_instance
38      virtual_router_id 106
39
40      # for electing MASTER, highest priority wins.
41      # to be MASTER, make this 50 more than on other machines.
42      # НУЖНО УКАЗАТЬ: вместо 128 -> приоритет экземпляра vrrp_instance
43      priority 128
44
45      preempt_delay 5 # Seconds
46
47      # VRRP Advert interval in seconds (e.g. 0.92) (use default)
48      advert_int 1
49
50      #  НУЖНО УКАЗАТЬ:  вместо  IP_ADDRESS_OF_THIS_HOST  ->  IPv4-адрес
    интерфейса, смотрящего в Интернет
51      unicast_src_ip IP_ADDRESS_OF_THIS_HOST
52
53      authentication {
54          auth_type PASS
55          # НУЖНО УКАЗАТЬ: ksedimret -> заменить на безопасный пароль
56          auth_pass ksedimret
57      }
```

```
58
59      virtual_ipaddress {
60          # НУЖНО УКАЗАТЬ: вместо VIRTUAL_IP_ADDREESS/MASK -> виртуальный
 IPv4-адрес и сетевой префикс с интерфейса, смотрящего в Интернет
61          # НУЖНО УКАЗАТЬ: вместо eth0 -> интерфейс, смотрящий в Интернет
62          # НУЖНО УКАЗАТЬ: вместо eth0:<значение> -> интерфейс, смотрящий в
Интернет:4-й октет виртуального IPv4-адреса
63          VIRTUAL_IP_ADDREESS/MASK dev eth0 label eth0:<значение>
64      }
65
66      track_script {
67          check_httpd
68      }
69  }
```

где:

script_user - значение этого параметра соответствует наименованию пользователя, от имени которого запускается служба keepalived (обычно - root);

NAME_OF_ROUTER_ID - имя зоны маршрутизации VRRP (общее для обоих узлов);

IP_ADDREESS_OF_THIS_HOST - текущий статический IP-адрес узла, на котором запускается служба keepalived;

VIRTUAL_IP_ADDRESS/MASK - виртуальный статический IP-адрес и маска (общие для узлов master и slave);

eth0:<значение> - значение четвертого октета виртуального IPv4-адреса. Например, если используется виртуальный статический IP-адрес 192.0.2.30, то данный параметр примет значение eth0:30;

- по очереди на каждом из узлов master и slave отредактировать созданный файл /etc/keepalived/notify.sh, приведя его к следующему виду:

```
1   #!/bin/sh -e
2
3   SELF_BIN=$(realpath ${0})
4   SELF_DIR=$(dirname ${SELF_BIN})
5   TYPE=${1}
6   NAME=${2}
7   STATE=${3}
8   PRIORITY=${4}
9   TASKMAN_SYSTEMCTL_NAME="termidesk-taskman"
10  TASKMAN_SYSTEMCTL_DESCRIPTION="Termidesk-VDI Taskman daemon"
11  TASKMAN_SYSTEMCTL_PIDFILE="/run/termidesk-taskman/pid"
12  msg2log () {
13      logger -i "Termidesk: ${1}"
14  }
15  taskman_stop () {
16      msg2log "Stopping ${TASKMAN_SYSTEMCTL_NAME} service"
17      systemctl is-active -q ${TASKMAN_SYSTEMCTL_NAME} && systemctl stop -q
${TASKMAN_SYSTEMCTL_NAME}
```

```
}
taskman_start () {
    msg2log "Starting ${TASKMAN_SYSTEMCTL_NAME} service"
    systemctl is-active -q ${TASKMAN_SYSTEMCTL_NAME} || systemctl start -q
${TASKMAN_SYSTEMCTL_NAME}
}
# VRRP event type: INSTANCE, name: lsb_40, state: BACKUP, priority: 64
msg2log "VRRP event type: ${TYPE}, name: ${NAME}, state: ${STATE},
priority: ${PRIORITY}"
case ${STATE} in
    BACKUP)
        [ "${NAME}" = "${TASKMAN_SYSTEMCTL_NAME}" ] && taskman_stop
    ;;
    FAULT)
        [ "${NAME}" = "${TASKMAN_SYSTEMCTL_NAME}" ] && taskman_stop
    ;;
    MASTER)
        [ "${NAME}" = "${TASKMAN_SYSTEMCTL_NAME}" ] && taskman_start
    ;;
    *)
        msg2log "Error: unknown state ${STATE}"
        exit 1
    ;;
esac
exit 0
```

- на узлах `master` и `slave` сделать файл `notify.sh` исполняемым:

```
:~$ sudo chmod +x /etc/keepalived/notify.sh
```

- на узлах `master` и `slave` добавить в автоматическую загрузку и запустить сервис `keeaplived`:

```
:~$ sudo systemctl enable keepalived
:~$ sudo systemctl start keepalived
```

14.2 . Настройка балансировщика для работы с самоподписанными сертификатами

14.2.1 . Создание самоподписанного SSL-сертификата

Для создания самоподписанного SSL-сертификата и ключа к нему нужно:

- открыть программу «Terminal Fly» и получить доступ к интерфейсу командной строки;
- выполнить генерацию SSL-сертификата (`/etc/ssl/certs/nginx-selfsigned.crt`) и ключа к нему (`/etc/ssl/private/nginx-selfsigned.key`):

```
:~$ sudo openssl req -new -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/
ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt
```

Используемые ключи команды:

- `openssl` - базовый инструмент командной строки для создания и управления сертификатами, ключами и другими файлами OpenSSL;
- `req` - эта опция указывает, что на данном этапе нужно использовать запрос на подпись сертификата X.509 (CSR). X.509 – это стандарт инфраструктуры открытого ключа, которого придерживаются SSL и TLS при управлении ключами и сертификатами. Данная команда позволяет создать новый сертификат X.509;
- `new` - эта опция указывает, что будет создаваться новый запрос;
- `x509` - эта опция вносит поправку в предыдущую команду, сообщая утилите о том, что вместо запроса на подписание сертификата необходимо создать самоподписанный сертификат;
- `nodes` - ключ для пропуска опции защиты сертификата парольной фразой. Нужно, чтобы при запуске балансировщик нагрузки (nginx) имел возможность читать файл без вмешательства пользователя. Установив пароль, придется вводить его после каждой перезагрузки;
- `days 365` - эта опция устанавливает срок действия сертификата (в данном случае сертификат действителен в течение года);
- `newkey rsa:2048` - эта опция позволяет одновременно создать новый сертификат и новый ключ. Поскольку ключ, необходимый для подписания сертификата, не был создан ранее, нужно создать его вместе с сертификатом. Данная опция создаст RSA-ключ размером 2048 бит;
- `keyout` - эта опция сообщает OpenSSL, куда поместить сгенерированный файл ключа;
- `out` - эта опция сообщает OpenSSL, куда поместить созданный сертификат.

После исполнения команды надо последовательно ввести ряд параметров, запросы на которые отобразятся в командной строке:

- `Country Name` (2 letter code) [AU];
- `State or Province Name` (full name) [Some-State];
- `Locality Name` (eg, city) [];
- `Organization Name` (eg, company) [Internet Widgits Pty Ltd];
- `Organizational Unit Name` (eg, section) [];
- `Common Name` (e.g. server FQDN or YOUR name) [];
- `Email Address` [].

Наиболее важным параметром является `Common Name` (необходимо ввести FQDN-имя балансировщика). Как правило, в эту строку вносят доменное имя, с которым нужно связать сервер. В случае если доменного имени нет, нужно внести в эту строку IP-адрес сервера.

Файлы ключа и сертификата будут размещены в каталоге, указанном при вызове команды `openssl` в параметрах `keyout` и `out`.

При использовании OpenSSL необходимо также создать ключи Диффи-Хеллмана, для этого:

- открыть программу «Terminal Fly» и получить доступ к интерфейсу командной строки;
- сгенерировать ключи Диффи-Хеллмана длиной 4096 бит и сохранить их в файл `/etc/nginx/dhparam.pem`:

```
:~$ sudo openssl dhparam -out /etc/nginx/dhparam.pem 4096
```

14.2.2 . Настройка nginx для поддержки SSL

Для настройки nginx нужно:

- создать новый пустой сниппет nginx в каталоге `/etc/nginx/snippets` для указания размещения сертификата и ключа:

```
:~$ sudo touch /etc/nginx/snippets/self-signed.conf
```

- отредактировать созданный файл, приведя его к виду:

```
1 ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
2 ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;
```

- создать еще один пустой сниппет, предназначенный для настроек SSL (это позволит серверу nginx использовать надежный механизм преобразования и включит некоторые дополнительные функции безопасности):

```
:~$ sudo touch /etc/nginx/snippets/ssl-params.conf
```

- отредактировать созданный файл `ssl-params.conf`, приведя его к виду:

```
1  ssl_protocols TLSv1.2;
2  ssl_prefer_server_ciphers on;
3  ssl_dhparam /etc/nginx/dhparam.pem;
4  ssl_ciphers ECDHE-RSA-AES256-GCM-SHA512:DHE-RSA-AES256-GCM-SHA512:ECDHE-RSA-
   AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384;
5  ssl_ecdh_curve secp384r1; # Requires nginx >= 1.1.0
6  ssl_session_timeout  10m;
7  ssl_session_cache shared:SSL:10m;
8  ssl_session_tickets off; # Requires nginx >= 1.5.9
9  ssl_stapling on; # Requires nginx >= 1.3.7
10 ssl_stapling_verify on; # Requires nginx => 1.3.7
11 resolver 77.88.8.8 77.88.8.1 valid=300s;
12 resolver_timeout 5s;
13 # Disable strict transport security for now. You can uncomment the following
14 # line if you understand the implications.
15 # add_header Strict-Transport-Security "max-age=63072000; includeSubDomains;
   preload";
16 add_header X-Frame-Options DENY;
17 add_header X-Content-Type-Options nosniff;
```

```
18  add_header X-XSS-Protection "1; mode=block";
```

⚠ Поскольку сертификат является самоподписанным, `SSL stapling` не будет использоваться. Сервер nginx выдаст предупреждение, отключит `stapling` для данного сертификата и продолжит работу.

14.2.3 . Конфигурирование веб-сервера

Для конфигурирования веб-сервера нужно:

- создать пустой конфигурационный файл:

```
:~$ sudo touch /etc/nginx/sites-available/sampledomain.ru.conf
```

- отредактировать созданный файл, приведя его к виду:

⚠ Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре предприятия.

```
1   upstream daas-upstream-ws {
2    least_conn;
3       # PROXY TERMIDESK
4
5        server 192.0.2.41:5099;
6        server 192.0.2.42:5099;
7        server 192.0.2.43:5099;
8        server 192.0.2.44:5099;
9
10  }
11
12  upstream daas-upstream-nodes {
13   least_conn;
14       # DISPATCHER TERMIDESK
15
16       server 192.0.2.30:443;
17       server 192.0.2.31:443;
18       server 192.0.2.32:443;
19
20   }
21
22  server {
23   listen 0.0.0.0:80;
24   listen 0.0.0.0:443 ssl;
25
26    include snippets/self-signed.conf;
27    include snippets/ssl-params.conf;
28
29   location /websockify {
```

```
         # limit_req zone=fast nodelay;
        proxy_http_version 1.1;
        proxy_pass http://daas-upstream-ws/;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";

        # Connection timeout
        proxy_connect_timeout 1000;
        proxy_send_timeout 1000;
        proxy_read_timeout 1000;
        send_timeout 1000;

        # Disable cache
        proxy_buffering off;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 }

 location / {
        proxy_pass https://daas-upstream-nodes/;

        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-Proto $scheme;

 }

}
```

⚠ IP-адреса, перечисленные в директиве `daas-upstream-ws`, являются адресами шлюзов подключений Termidesk, а IP-адреса, перечисленные в директиве `daas-upstream-nodes`, являются адресами универсальных диспетчеров Termidesk.

- создать символическую ссылку на данный виртуальный хост из директории `/etc/nginx/sites-available` в директорию `/etc/nginx/sites-enabled`, чтобы nginx его обслуживал:

```
:~$ sudo ln -s /etc/nginx/sites-available/sampledomain.ru.conf /etc/nginx/sites-enabled/
```

- проверить корректность настроек:

```
:~$ sudo nginx -t
```

```
nginx: [warn] "ssl_stapling" ignored, issuer certificate not found
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

⚠ Веб-сервер возвращает предупреждение в случае использования самоподписанного сертификата, однако это не влияет на работу.

- если в синтаксисе обнаружены ошибки, необходимо исправить их, затем перезапустить веб-сервер:

```
:~$ sudo systemctl restart nginx
```

15 . ЭКСПЕРИМЕНТАЛЬНЫЕ ФУНКЦИИ

15.1 . Перечень переменных окружения универсального диспетчера

В Termidesk используются переменные для указания параметров настройки компонентов программного комплекса.

Перечень переменных и параметров, используемых при установке и универсальным диспетчером, приведены в таблице (см. Таблица 78).

Перечень переменных, используемых в других компонентах программного комплекса, приведен в соответствующих им документах.

Таблица 78 – Переменные окружения Termidesk

Переменная окружения	Значение по умолчанию	Описание
Универсальный диспетчер		
`TDSK_AUTOFS_IMAGES_ID`	Не задано	Используется для настройки шаблонов переносимых профилей. В качестве значения используются идентификаторы дисков. Пример: `TDSK_AUTOFS_IMAGES_ID=xx[,yy[,zz[,...]]]`. Значение переменной задается в файле `/etc/opt/termidesk-vdi/termidesk.conf`
`DBHOST`	Не задано	IP-адрес или FQDN СУБД PostgreSQL. Начальное значение задается на этапе подготовке среды функционирования и установки Termidesk. Изменить значение переменной можно через файл `/etc/opt/termidesk-vdi/termidesk.conf`
`DBPORT`	`5432`	Порт, который используется для соединения с сервером БД. Изменить значение переменной можно через файл `/etc/opt/termidesk-vdi/termidesk.conf`
`DBSSL`	Не задано	Протокол, использующийся при подключении к БД. Возможные значения: `Disable`, `TLSv1.2`, `TLSv1.3`. Начальное значение задается на этапе установки Termidesk. Изменить значение можно через файл `/etc/opt/termidesk-vdi/termidesk.conf`
`DBNAME`	Не задано	Имя БД. Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk. Изменить значение переменной можно через файл `/etc/opt/termidesk-vdi/termidesk.conf`

DBUSER	Не задано	Имя пользователя, имеющего доступ к БД. Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk. Изменить значение переменной можно через файл /etc/opt/termidesk-vdi/termidesk.conf
DBPASS	Не задано	Пароль пользователя, имеющего доступ к БД. Начальное значение задается на этапе подготовки среды функционирования во время установки Termidesk и хранится в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf в преобразованном виде. ⚠ В стандартных установках значения менять не следует. Изменить значение переменной можно через файл /etc/opt/termidesk-vdi/termidesk.conf . Для получения преобразованного значения пароля следует воспользоваться утилитой scramble : `:~$ sudo /opt/termidesk/bin/scramble -v <пароль>` Утилита scramble использует в качестве вектора преобразования значение из файла /etc/opt/termidesk-vdi/termidesk.cookie. Значение генерируется автоматически на этапе установки Termidesk
DJANGO_SECRET_KEY	Не задано	Параметр, используемый для проверки данных, пересылаемых между компонентами Termidesk. Значение генерируется при установке Termidesk и должно быть одинаковым для всех узлов при распределённой установке. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf
WSPROXY_PORT	5099	Порт, который будет прослушивать служба компонента «Шлюз». Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf
WSPROXY_BIND_ADDRESS	127.0.0.1	IP-адрес, который будет прослушивать служба компонента «Шлюз» в случае комплексной установки. В распределенной установке данный параметр должен быть установлен в значение 0.0.0.0. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf

RABBITMQ_URL	Не задано	Параметры для подключения к серверам RabbitMQ. Можно подключить до трех (включительно) серверов. Начальное значение задается на этапе установки Termidesk. Значение этого параметра записывается в файл /etc/opt/termidesk-vdi/termidtermidesk-vdi/termidesk.conf. Пароль, указанный для подключения к серверу RabbitMQ хранится в преобразованном виде. Этот функционал реализован, начиная с версии Termidesk 4.3.1, и применяется только для новых установок. При обновлении с более старой версии сохраняется значение этой переменной. При необходимости изменить пароль подключения следует получить преобразованное значение утилитой scramble и выполнить перезапуск служб Termidesk
RABBITMQ_SSL	Не задано	Протокол, использующийся при подключении к RabbitMQ. Возможные значения: Disable, TLSv1.2. Начальное значение задается на этапе установки Termidesk. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf
WEB_PORTAL_TYPE	Не задано	Параметр, задающий тип веб-интерфейса Termidesk. Возможные значения: admin, user, universal. Начальное значение задается на этапе установки Termidesk. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. Настройки будут применены после перезапуска службы termidesk-vdi: `:~$ sudo systemctl restart termidesk-vdi` При переустановке Termidesk значение параметра в конфигурационном файле будет перезаписано
LOG_LEVEL	INFO	Уровень журналирования сообщений. Возможные значения: DEBUG, INFO, WARNING, ERROR, CRITICAL. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf
LOG_ADDRESS	/dev/log	Адрес для отправки записей в системный журнал. Обычно это /dev/log для Linux-систем. Возможно указать IP-адрес и порт. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf
LOG_FACILITY	local3	Параметр, определяющий категорию сообщений syslog. Категория должна совпадать с настройками в конфигурационном файле /etc/syslog-ng/conffirst.d/termidesk.conf

HEALTH_CHECK_ACCESS_KEY	Не задано	Параметр для доступа к проверке состояния API сервера. Начальное значение генерируется на этапе установки Termidesk. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. При задании значения параметра следует руководствоваться правилом, что: ▪ размер должен составлять от 0 до 64 символа; ▪ должны использоваться символы в шестнадцатеричной системе (0-9, a-f)
WSPROXY_HEALTH_CHECK_PORT	8101	Порт, на котором работает веб-сервер для обслуживания запросов проверки состояния API компонента «Шлюз». Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. По умолчанию переменная не используется (закомментирована)
WSPROXY_HEALTH_CHECK_CERT	/etc/opt/termidesk-vdi/wsproxy-healthcheck.pem	Путь к сертификату SSL/TLS для защищенного подключения к проверке состояния API компонента «Шлюз». Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. По умолчанию переменная не используется (закомментирована)
WSPROXY_HEALTH_CHECK_KEY	/etc/opt/termidesk-vdi/wsproxy-healthcheck.key	Путь к ключу SSL/TLS для защищенного подключения к проверке состояния API компонента «Шлюз». Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. По умолчанию переменная не используется (закомментирована)
TASKMAN_HEALTH_CHECK_PORT	8100	Порт, на котором работает веб-сервер для обслуживания запросов проверки состояния API компонента «Менеджер рабочих мест». Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. По умолчанию переменная не используется (закомментирована)
TASKMAN_HEALTH_CHECK_CERT	/etc/opt/termidesk-vdi/taskman-healthcheck.pem	Путь к сертификату SSL/TLS для защищенного подключения к проверке состояния API компонента «Менеджер рабочих мест». Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. По умолчанию переменная не используется (закомментирована)
TASKMAN_HEALTH_CHECK_KEY	/etc/opt/termidesk-vdi/taskman-healthcheck.key	Путь к ключу SSL/TLS для защищенного подключения к проверке состояния API компонента «Менеджер рабочих мест». Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. По умолчанию переменная не используется (закомментирована)
REQUESTS_CA_BUNDLE	Не задано	Путь к файлу с доверенным корневым сертификатом. Переменная используется для настройки работы с сертификатами собственных ЦС. Добавить переменную можно через файл /etc/opt/termidesk-vdi/termidesk.conf. По умолчанию переменная не используется (закомментирована)

Установочный пакет termidesk-vdi		
TDSK_PKG_DEBUG	Не задано	Включение режима отладки при установке пакета. Пример: TDSK_PKG_DEBUG=1

15.2 . Управление экспериментальными параметрами Termidesk

Включение и отключение экспериментальных параметров сервера Termidesk производится из командной строки. Командная строка должна запускаться от имени пользователя `termidesk`.

Для вывода доступных экспериментальных параметров нужно выполнить следующее:

- перейти в интерфейс командной строки;
- переключиться на пользователя `termidesk`:

```
:~$ sudo -u termidesk bash
```

- вывести список экспериментальных параметров:

```
:~$ /opt/termidesk/sbin/termidesk-vdi-manage tdsk_config list | grep Experimental
```

Будет выведен список экспериментальных параметров Termidesk в формате Секция-Ключ-Значение.

⚠ При вызове `/opt/termidesk/sbin/termidesk-vdi-manage` могут появляться уведомления «WARNINGS», не влияющие на выполнение команд.

Перечень экспериментальных параметров приведен в таблице (см. Таблица 79).

Таблица 79 – Экспериментальные параметры Termidesk

Параметр	Описание	Значение по умолчанию
experimental.2fa.enabled	Параметр поддержки двухфакторной аутентификации	0
experimental.deviceauth.enabled	Параметр поддержки авторизации устройств доступа	0
experimental.loudplay.transports.enabled	Параметр поддержки протоколов доставки Loudplay	0
experimental.metasessions.provider.enabled	Параметр поддержки сервера терминалов (метапровайдер)	0
experimental.openstack.provider.enabled	Параметр поддержки поставщика ресурсов Openstack	0
experimental.provider.physmachine.enabled	Параметр поддержки поставщика ресурсов для физических машин	0

Параметр	Описание	Значение по умолчанию
experimental.radiusauth.enabled	Параметр поддержки домена аутентификации RADIUS	0
experimental.vair.provider.enabled	Параметр поддержки поставщика ресурсов vAir	0

Для активации экспериментального параметра необходимо присвоить ему значение 1, выполнив команду:

```
:~$ /opt/termidesk/sbin/termidesk-vdi-manage tdsk_config set --section
Experimental --key experimental.2fa.enabled --value 1
```

где:

experimental.2fa.enabled - наименование параметра;

1 - значение параметра для его активации;

0 - значение параметра для его деактивации.

15.3 . Установка плагинов расширений

Экспериментальный функционал, не вошедший в основной релиз Termidesk, можно добавить в программный комплекс через установку плагинов расширений (каталог addons в комплектации поставки Termidesk).

Для установки плагинов нужно на сервере Termidesk выполнить следующее:

- распаковать содержимое zip-архива в целевой каталог (например, /tmp);
- переключиться на пользователя Termidesk:

```
:~$ sudo -u termidesk bash
```

- перейти в каталог Termidesk:

```
:~$ cd /opt/termidesk/share/termidesk-vdi/
```

- активировать виртуальное окружение Termidesk:

```
:~$ source venv/bin/activate
```

- установить необходимый плагин:

```
:~$ pip install --upgrade --no-index --find-links /tmp/termidesk_internaldbauth
 termidesk_internaldbauth
```

где:

/tmp/termidesk_internaldbauth - каталог с whl-файлами;

`termidesk_internaldbauth` - имя плагина (без версии, платформы и расширения файла);

- выйти из окружения пользователя `Termidesk`:

```
:~$ exit
```

- обновить структуру БД и статических файлов командами:

```
:~$ sudo /opt/termidesk/sbin/termidesk-vdi-manage migrate
:~$ sudo /opt/termidesk/sbin/termidesk-vdi-manage collectstatic --no-input
```

- перезапустить службы Termidesk:

```
:~$ sudo systemctl restart termidesk-vdi.service termidesk-taskman.service
termidesk-wsproxy.service termidesk-celery-beat.service termidesk-celery-
worker.service
```

15.4 . Удаление плагинов расширений

Перед удалением плагина необходимо удалить фонды BPM, шаблоны ВМ и поставщика ресурсов, соответствующих данному плагину в графическом интерфейсе управления Termidesk.
Удаление фонда BPM может занять продолжительное время.

Для удаления плагина расширений нужно на сервере Termidesk выполнить следующее:

- переключиться на пользователя `Termidesk`:

```
:~$ sudo -u termidesk bash
```

- перейти в каталог `Termidesk`:

```
:~$ cd /opt/termidesk/share/termidesk-vdi/
```

- активировать виртуальное окружение `Termidesk`:

```
:~$ source venv/bin/activate
```

- удалить необходимый плагин:

```
:~$ pip uninstall -y termidesk_internaldbauth
```

где:

`termidesk_internaldbauth` - имя плагина (без версии, платформы и расширения файла);

- выйти из окружения пользователя `Termidesk`:

```
:~$ exit
```

- перезапустить службы Termidesk:

```
1  :~$ sudo systemctl restart termidesk-vdi.service termidesk-taskman.service
   termidesk-wsproxy.service termidesk-celery-beat.service termidesk-celery-
   worker.service
```

15.5 . Откат к предыдущей версии плагина

Откат к предыдущей версии файла выполняется в той же последовательности, что и установка, однако вместо команды установки плагина используется следующая:

```
1  :~$ pip install --no-index --find-links /tmp/termidesk_internaldbauth
    termidesk_internaldbauth==4.0.1
```

где:

`/tmp/termidesk_internaldbauth` - каталог с `whl`-файлами, `whl`-файл с версией плагина должен существовать в данном каталоге;

`termidesk_internaldbauth` - имя плагина с указанием версии.

16 . РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ ОТСЛЕЖИВАНИЯ СОСТОЯНИЯ КОМПОНЕНТОВ TERMIDESK

16.1 . Общие сведения по проверке состояния компонентов

Для отслеживания состояния компонентов Termidesk и обращения к ним для выполнения проверок состояния здоровья (health check) используется API-запрос `/api/health`.

Начальная спецификация схемы HealthCheck API в формате OpenAPI соответствует описанию:

```
openapi: 3.0.3
info:
  title: Termidesk health check api schema
  version: 0.1
paths:
  /api/health:
    get:
      responses:
        '200':
          description: Successful Response
          content:
            application/json:
              schema:
                type: object
                properties:
                  status:
                    type: string
                    enum: [pass, warn, fail]
                    example: fail
                    description: "Состояние компонента"
                  version:
                    type: string
                    example: 3.3
                    description: "Версия компонента"
                  description:
                    type: string
                    example: termidesk-taskman
                    description: "Описание компонента"
                  output:
                    type: string
                    example: "django.db.utils.OperationalError: FATAL:  password authentication failed for user 'termidesk'"
                    description: "Описание ошибки (если есть)"
                required:
                  - status
        '401':
          description: Authorization information is missing or invalid
```

Базовый URL для API: `/api/health`.

Тип контента: `application/json`.

Для каждого компонента Termidesk механизм проверки состояния должен быть доступен на порте, заданном в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf`. Порт можно переопределить в этом же файле.

Для исключения злоупотреблением частыми вызовами API, способными создать нагрузку на систему, доступ к API-запросу контролируется отдельным токеном. Значение токена задается конфигурационным файлом `/etc/opt/termidesk-vdi/termidesk.conf` в переменной `HEALTH_CHECK_ACCESS_KEY`.

Пример:

```
HEALTH_CHECK_ACCESS_KEY = "9944b09199c62bcf9418ad846dd0e4bbdfc6ee4b"
```

16.2 . Состояние компонента «Универсальный диспетчер»

При распределенной установке Termidesk экземпляры компонента «Универсальный диспетчер» могут быть установлены на нескольких узлах. Доступ к узлам организуется через балансировщик трафика, но для механизма проверок состояния нужно обращаться к каждому узлу напрямую.

Компонент изначально задействован для работы по протоколу HTTP, поэтому механизм проверки состояния реализуется отдельными вызовами REST API.

Пример команды проверки состояния компонента через утилиту `curl`:

```
:~$ curl -v -s -X 'GET' "${HOSTNAME}:${HEALTH_PORT}/api/health" -H 'accept: application/json' -H "Authorization: Token ${HEALTH_CHECK_ACCESS_KEY}" --fail -w "\n%{http_code}"
```

16.3 . Состояние компонента «Шлюз»

При распределенной установке Termidesk экземпляры компонента «Шлюз» могут быть установлены на нескольких узлах. Доступ к узлам организуется через балансировщик трафика, но для механизма проверок состояния нужно обращаться к каждому узлу напрямую.

Пример команды проверки состояния компонента через утилиту `curl`:

```
:~$ curl -I -X 'GET' -H "Accept: text/plain" http://<IP-адрес_шлюза>:5099/info
```

Пример ответа для работоспособного компонента:

```
HTTP/1.1 200 OK
Date: Tue, 28 Nov 2023 07:37:51 GMT
uWebSockets: 20
Content-Length: 314
```

Код 200 в ответе на API-запрос свидетельствует о работоспособности компонента «Шлюз». Отсутствие ответа говорит о том, что компонент не работает. Данное правило необходимо добавить на балансировщике трафика.

Для исключения злоупотреблением частыми вызовами API, способными создать нагрузку на систему, доступ к API-запросу компонента «Шлюз» `termidesk-gateway` контролируется отдельным токеном. Значение токена задается при запуске службы «Шлюза» в параметре `--healthCheckAccessKey`.

Для использования механизма проверки состояния компонента необходимо выполнить запуск Шлюза `termidesk-gateway` с указанием путей расположения сертификата и ключа (`--sslKey` и `--sslCert`), используемых для защищенного подключения.

Пример команды запуска службы `termidesk-gateway`:

```
:~$ termidesk-gateway --wssServerIP=0.0.0.0 --wssServerPort=8443 --sslKey=<путь_к_ключу> --sslCert=<путь_к_сертифкату> --urlCheckToken=http://<FQDN_Узла>/api/wsproxy/v1/verify --wsIdleTimeout=30 --mgtServerIP=0.0.0.0 --mgtServerPort=8102 --healthCheckAccessKey=<HEALTH_CHECK_ACCESS_KEY> --debug
```

Пример команды проверки состояния компонента через утилиту `curl` для компонента «Шлюз» `termidesk-gateway`:

```
:~$ curl -v -s -X 'GET' "${HOSTNAME}:8102/api/health" -H 'accept: application/json' -H "Authorization: Token ${HEALTH_CHECK_ACCESS_KEY}" --fail -w "\n%{http_code}"
```

16.4 . Состояние компонента «Менеджер рабочих мест»

При распределенной установке Termidesk экземпляры компонента «Менеджер рабочих мест» могут быть установлены на нескольких узлах, но активен должен быть только один из них. Все остальные компоненты являются резервными и, по умолчанию, находятся в состоянии «Passive».

Для использования механизма проверки состояния компонента необходимо в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` раскомментировать строки параметров `TASKMAN_HEALTH_CHECK_PORT`, `TASKMAN_HEALTH_CHECK_CERT`, `TASKMAN_HEALTH_CHECK_KEY`. Для параметров `TASKMAN_HEALTH_CHECK_CERT`, `TASKMAN_HEALTH_CHECK_KEY` нужно указать путь к сертификату и ключу, используемых для защищенного подключения, и выполнить перезапуск служб Termidesk.

Пример задания значений:

```
TASKMAN_HEALTH_CHECK_PORT=8100
TASKMAN_HEALTH_CHECK_CERT=/etc/opt/termidesk-vdi/taskman-healthcheck.pem
TASKMAN_HEALTH_CHECK_KEY=/etc/opt/termidesk-vdi/taskman-healthcheck-decrypted.key
```

Пример команды проверки состояния компонента через утилиту `curl`:

```
:~$ curl -v -s -X 'GET' "${HOSTNAME}:8100/api/health" -H 'accept: application/
json' -H "Authorization: Token ${HEALTH_CHECK_ACCESS_KEY}" --fail -w "\n%
{http_code}"
```

17 . НЕШТАТНЫЕ СИТУАЦИИ

17.1 . Нештатные ситуации и способы их устранения

Возможные неисправности при работе с Termidesk и способы их устранения приведены в таблице (см. Таблица 80).

Таблица 80 – Перечень возможных нештатных ситуаций

Индикация	Описание	Возможное решение
Ошибка: «СБОЙ: оставшиеся слоты подключений зарезервированы для подключений суперпользователя (не для репликации)»	Ошибка возникает при попытке авторизации на сервере Termidesk	Изменить максимальное количество подключений в настройках БД: изменить значение `max_connections` в конфигурационном файле `/etc/postgresql/11/main/postgresql.conf` в бОльшую сторону
Ошибка: «OpenNebula Error 256 User coulnd't authenticated, abording call»	Ошибка возникает при попытке добавления поставщика ресурсов ПК СВ Брест в графическом интерфейсе управления Termidesk	Необходимо указать верный путь к файлу `keytab` и внести значения параметра «Токен» непосредственно в интерфейсе ПК СВ Брест (см. подраздел **Добавление поставщика ресурсов ПК СВ Брест**)
Ошибка: «OpenNebula error 256 User could't be authericated»	Ошибка возникает при попытке добавления поставщика ресурсов ПК СВ Брест	Необходимо создать новое значение параметра Токен для пользователя непосредственно в интерфейсе ПК СВ Брест
Ошибка: «SSL: WRONG_VERSION_NUMBER] wrong version number (_ssl.c:1056)»	Ошибка возникает, если сервер поставщика ресурсов не поддерживает SSL	Необходимо отредактировать поставщика ресурсов, выставив параметру «Использовать SSL» значение «Нет»
Нельзя заполнить поле Кластер данных, невозможно сохранить шаблон	Ошибка возникает при попытке создания шаблона ВРМ для поставщика ресурсов VMware поле «Кластер данных» неактивно, невозможно сохранить шаблон	На платформе виртуализации VMware необходимо объявить кластер хранилища данных (Datastore Cluster)
Ошибка: «kinit: Client 'HTTP/termidesk.local@LOCAL' not found in Kerberos database while getting initial credentials»	Ошибка возникает при добавлении или редактировании домена аутентификации FreeIPA	Необходимо создать указанную учетную запись на КД FreeIPA
Ошибка: «'list' object has no attribute 'get'»	Ошибка возникает при разворачивании ВМ из шаблона, в котором указанно больше одного диска	В шаблоне при первоначальном разворачивании ВМ должен быть указан только один диск

Индикация	Описание	Возможное решение

Ошибки при установке пакета «Невозможно найти пакет» или «Неудовлетворенные зависимости»	Ошибка возникает при попытке установить пакет в ОС	Необходимо убедиться, что в файле `/etc/apt/sources.list` заданы и не закомментированы источники получения пакетов (репозитории), затем обновить списки пакетов:
		`:~$ sudo apt update`
		После этого нужно вновь выполнить команду установки пакета.
		Для решения проблемы с неудовлетворенными зависимостями, помимо подключения репозиториев в файле `/etc/apt/sources.list`, можно воспользоваться командой:
		`:~$ sudo apt -f install`
		Ключ `-f` используется для попытки исправить нарушенные зависимости пакетов

Ошибка:
«Проверка не пройдена. ValueError: Метаданные не получены. Проверьте URL Метаданных и доступность сервера»
	При активации параметра «Проверка SSL» для домена аутентификации SAML тест соединения завершается с ошибкой	Необходимо настроить работу с сертификатами при получении метаданных от домена аутентификации SAML. Для этого:
		▪ добавить переменную окружения `REQUESTS_CA_BUNDLE` в файле `/etc/opt/termidesk-vdi/termidesk.conf`. В переменной окружения нужно указать путь к файлу с доверенным корневым сертификатом. Пример:
		`REQUESTS_CA_BUNDLE=/etc/ssl/certs/ca.crt`
		▪ выполнить перезапуск службы `termidesk-vdi`:
		`:~$ sudo systemctl restart termidesk-vdi`

18 . ПЕРЕЧЕНЬ ТЕРМИНОВ

Термин	Определение
Агент	Собирательное название для следующих компонентов: ▪ агент ВРМ; ▪ агент УВ; ▪ сессионный агент; ▪ видеоагент; ▪ агент виртуальных смарт-карт. Самостоятельный компонент, отвечающий за контролируемую доставку ВРМ, взаимодействие с универсальным диспетчером и менеджером ВРМ
Агент виртуальных смарт-карт (`termidesk-pcsc-vscard`)	Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление подключенных к пользовательской рабочей станции смарт-карт в ВРМ
Агент ВРМ (`python3-termidesk-agent`)	Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет взаимодействие с диспетчером Termidesk, конфигурирует ВРМ, фиксирует действия пользователя, реализует передачу управляющих сообщений
Агент УВ (`termidesk-vmsd`)	Агент узла виртуализации. Устанавливается на узел виртуализации, взаимодействует с гипервизором через модуль `libvirt`
Базовое ВРМ	Также: «золотой образ», «базовое рабочее место», «базовый образ», «gold». Подразумевает собой образ диска виртуальной машины с предустановленным прикладным ПО и установленным агентом ВРМ. Этот образ далее будет использоваться для создания ВРМ для пользователей
Балансировщик нагрузки	Самостоятельный компонент, отвечающий за распределение нагрузки на множество универсальных диспетчеров и шлюзов
Видеоагент (`termidesk-video-agent`)	Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление видеокамеры с пользовательской рабочей станции в ВРМ
ВРМ	Виртуальное рабочее место: развернутая на ВМ ОС с установленным агентом ВРМ и необходимым прикладным ПО. Подключение к ВРМ происходит при помощи протоколов удаленного доступа, чаще всего называемыми протоколами доставки
Гостевая ОС	ОС, функционирующая на ВМ
Группы рабочих мест	Также: «группы ВРМ». Функциональное объединение множества фондов ВРМ по определенному признаку
Домен аутентификации	Способ проверки субъектов и их полномочий
Менеджер рабочих мест (`termidesk-vdi`)	Также: «планировщик заданий», «менеджер ВРМ». Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом ВРМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-taskman.service`

Термин	Определение
Оркестратор (`termidesk-orchestrator`)	Самостоятельный компонент, отвечающий за согласованную работу всех компонентов программного комплекса при децентрализованном развертывании, для нужд отказоустойчивости и комплексирования с облачными службами
Поставщик ресурсов	ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов ВРМ
Протокол доставки	Поддерживаемый в Termidesk протокол удаленного доступа к ВРМ
Связанный клон	Способ организации ВРМ на основе единого образа, с возможностью экономии дискового пространства, за счет технологии «копирование при записи», и ускорения операций возврата к базовому состоянию, установки дополнительного ПО и обновлений
Сессионный агент (`termidesk-session-agent`)	Устанавливается на сервер терминалов (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям
Универсальный диспетчер (`termidesk-vdi`)	Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им ВРМ и контроля доставки ВРМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service`
Фонд рабочих мест	Также: «фонд ВРМ». Совокупность подготовленных ВРМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей
Шаблон рабочего места	Также: «шаблон ВРМ». Параметры конфигурации базового ВРМ для использования в фонде ВРМ
Шлюз (`termidesk-vdi` / `termidesk-gateway`)	Отделяемый компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP. В более старой реализации устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-wsproxy.service`. В новой реализации устанавливается из пакета `termidesk-gateway`, поддержка старой реализации также осталась. Наименование службы после установки в новой реализации: `termidesk-gateway.service`.
STAL (`stal`)	Сервер терминалов Astra Linux. Реализован компонентом «Сервер терминалов» Termidesk

19 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
БД	База данных
ВМ	Виртуальная машина
ВРМ	Виртуальное рабочее место
ЗПС	Замкнутая программная среда
ОС	Операционная система
ПК СВ Брест	Программный комплекс «Средства виртуализации «Брест»
ПО	Программное обеспечение
СУБД	Система управления базами данных
ЦС	Центр сертификации
ЭЦП	Электронная цифровая подпись
ALD	Astra Linux Directory (единое пространство пользователей)
API	Application Programming Interface (интерфейс прикладного программирования)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
FreeIPA	Free Identity, Policy and Audit (открытое решение по безопасности Linux-систем)
GID	Group Identification Data (идентификатор группы)
HTML	Hypertext Markup Language (язык гипертекстовой разметки)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
ID	Identification Data (идентификатор)
IP	Internet Protocol (межсетевой протокол)
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов)
MS AD	Microsoft Active Directory (службы каталогов Microsoft)
OU	Organizational Unit (организационная единица)
PAM	Pluggable Authentication Module (подключаемый модуль аутентификации)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)
RDS	Remote Desktop Services (службы удаленного рабочего стола Microsoft)
RDSH	Remote Desktop Session Host (хост сеансов удаленных рабочих столов)
PKI	Public Key Infrastructure (инфраструктура открытых ключей)

Сокращение	Пояснение
SAML	Security Assertion Markup Language (открытый стандарт обмена данными аутентификации)
SCSI	Small Computer System Interface (набор стандартов для физического подключения и передачи данных между компьютерами и периферийными устройствами)
SPICE	Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)
SSL	Secure Sockets Layer (криптографический протокол)
SSO	Single Sign-On (технология единого входа)
STAL	Terminal Server Astra Linux (сервер терминалов ОС Astra Linux Special Edition (Server))
TCP	Transmission Control Protocol (протокол управления передачей)
Termidesk	Программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk»
TLS	Transport Layer Security (протокол защиты транспортного уровня)
UDP	User Datagram Protocol (протокол пользовательских датаграмм)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
USB	Universal Serial Bus (последовательный интерфейс для подключения периферийных устройств)
UUID	Unique User Identifier (уникальный идентификатор пользователя)
vGPU	Virtual Graphics Processing Unit (виртуальный графический процессор)
VDI	Virtual Desktop Infarsticture (инфраструктура виртуальных рабочих столов)
VNC	Virtual Network Computing (система удаленного доступа к рабочему столу компьютера)
VRRP	Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности)

Адрес: 119571, г. Москва, Ленинский проспект, д. 119А, помещ. 9Н
Сайт: https://termidesk.ru
Телефон: +7 (495) 975-1-975

Общий e-mail: info@uveon.ru
Отдел продаж: sales@uveon.ru
Техническая поддержка: support@uveon.ru