TERMIDESK

Руководство администратора

СЛЕТ.10001-01 90 02

Версия 6.0. Выпуск от июня 2025

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

Приняты следующие типографские соглашения:

- моноширинный шрифт – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, 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;
- ALD Pro;
- SAML;
- IP-аутентификация;
- Microsoft Active Directory (MS AD) или LDAP;
- RADIUS.

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

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).

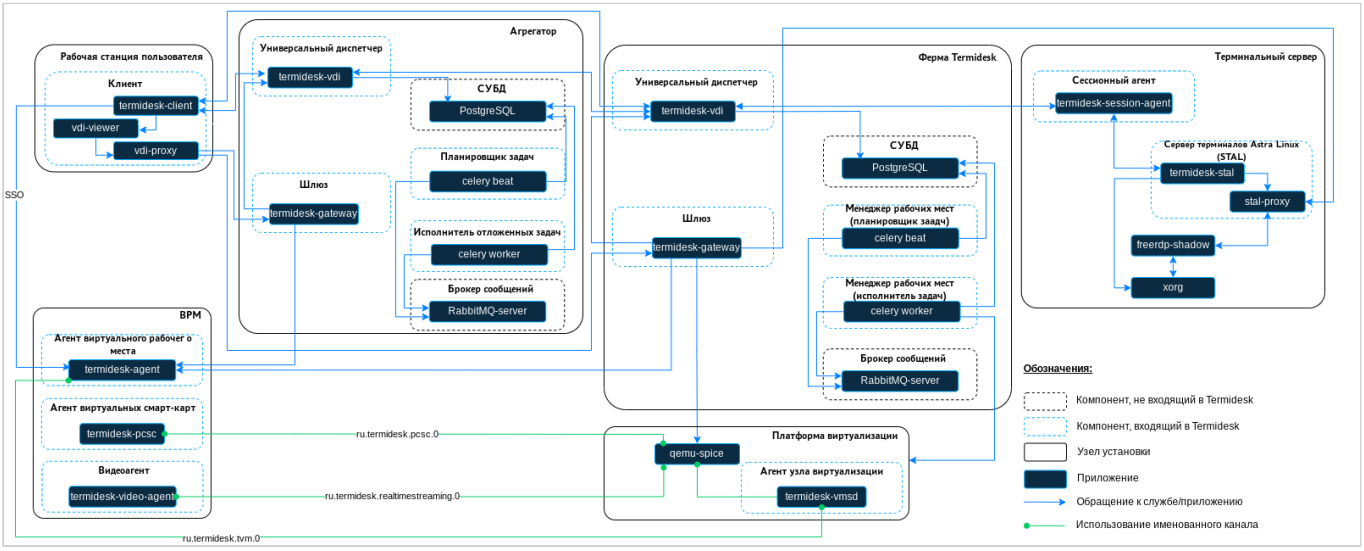

Рисунок 1 – Схема взаимодействия компонентов и приложений

2.3 . Схема сетевого взаимодействия компонентов Termidesk

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

> ⓘ Сервер REDIS, с которым взаимодействует компонент «Удаленный помощник» (серверная часть), в текущей версии обращается на `localhost`.

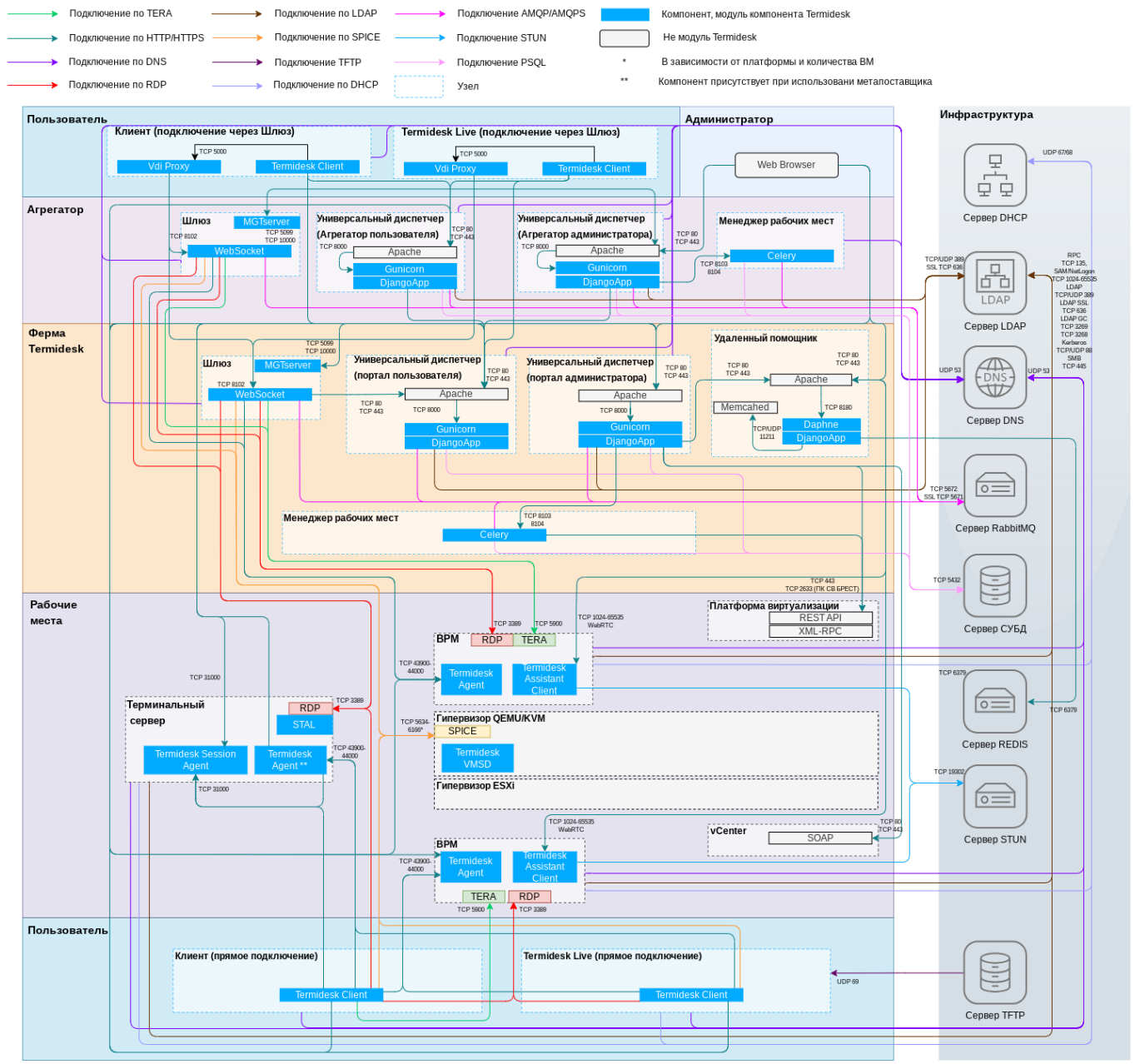

Рисунок 2 – Схема сетевого взаимодействия компонентов Termidesk

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

Таблица 1 – Перечень узлов и компонентов

Компонент	Узел установки	Наименование пакета установки
«Универсальный диспетчер»	Отдельный узел для установки	`termidesk-vdi`
«Менеджер рабочих мест»	Отдельный узел для установки или установка совместно с «Универсальным диспетчером» в составе фермы Termidesk	`termidesk-vdi`
«Шлюз»	Отдельный узел для установки или установка совместно с «Универсальным диспетчером»	`termidesk-gateway`

Компонент	Узел установки	Наименование пакета установки
«Агент виртуального рабочего места»	Виртуальная машина (ВМ), установка на этапе подготовки образа для ВРМ	`termidesk-agent`
«Агент узла виртуализации»	Узел виртуализации (гипервизор) ПК СВ Брест	`termidesk-vmsd`
«Сессионный агент»	Установка на узле сервера терминалов: ▪ ОС Microsoft Windows Server с ролью «Remote Desktop Services» (далее - MS RDS); ▪ ОС Astra Linux Special Edition с установленным компонентом «Сервер терминалов Astra LInux» (далее - STAL)	`termidesk-session-agent`
«Видеоагент»	ВМ, установка на этапе подготовки образа для ВРМ	`termidesk-video-agent`
«Агент виртуальных смарт-карт»	ВМ, установка на этапе подготовки образа для ВРМ	`termidesk-pcsc-vscard`
«Клиент»	Рабочее место пользователя (пользовательская рабочая станция)	`termidesk-client`
«Оркестратор»	Отдельный узел для установки, применяется в облачной конфигурации	`termidesk-orchestrator`
«Сервер терминалов Astra Linux»	Отдельный узел для установки, возможна установка на том же узле, где установлен «Универсальный диспетчер»	`stal`
«Удаленный помощник» (серверная часть)	Отдельный узел для установки	`termidesk-assistant-server`
«Удаленный помощник» (клиентская часть)	Рабочее место пользователя (пользовательская рабочая станция) или ВМ (установка на этапе подготовки образа для ВРМ)	`termidesk-assistant-client`
«Termidesk Live»	Отдельный узел, тонкий клиент	`thinstation` (образ)
«Виртуальный модуль Termidesk»	Отдельная ВМ. Компонент позволяет быстро развернуть и использовать «Универсальный диспетчер», «Менеджер рабочих мест», «Шлюз»	`termidesk-virtual-appliance` (образ)

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).

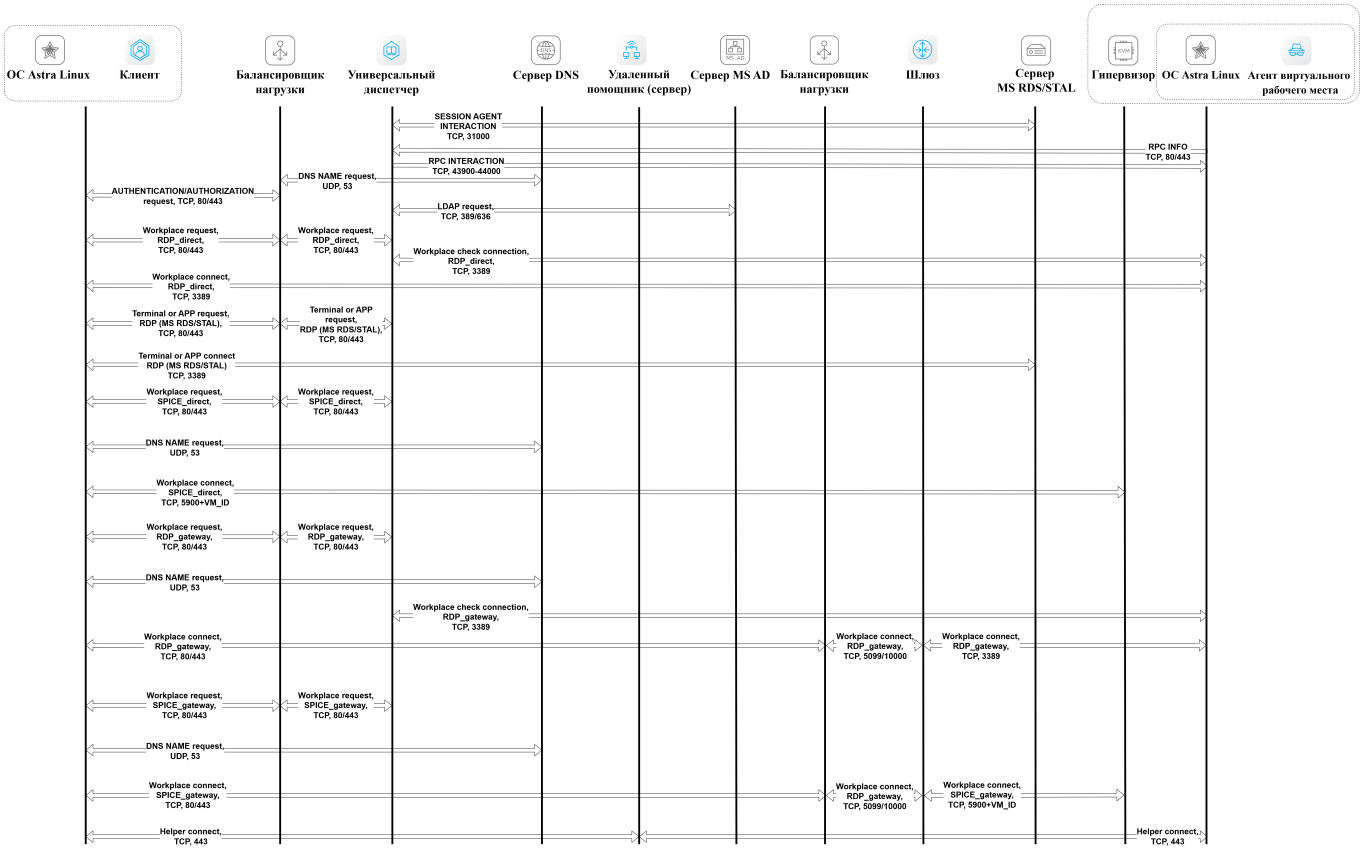

Рисунок 3 – Последовательность сетевых запросов

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

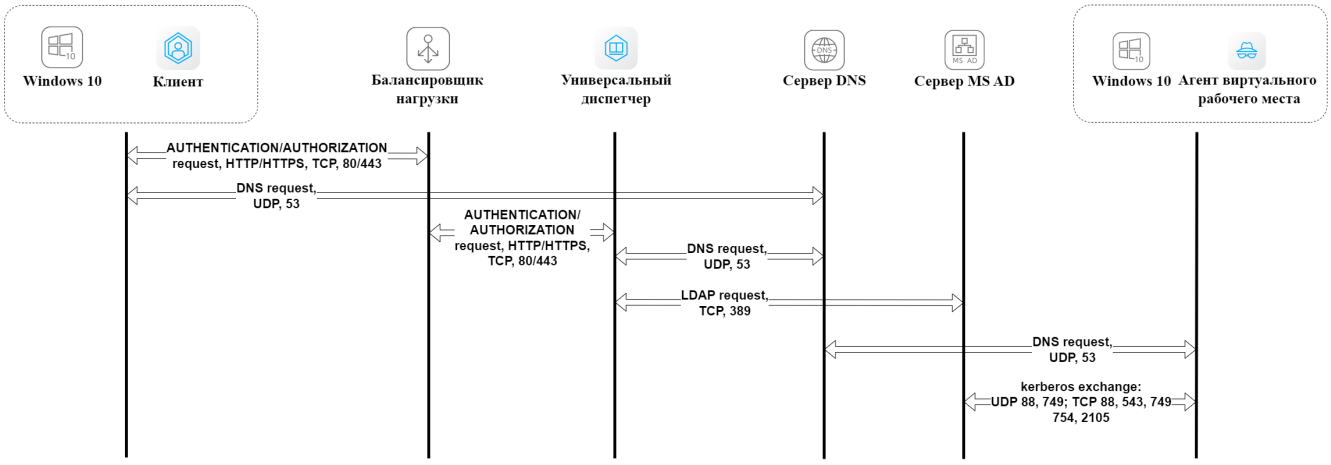

Рисунок 4 – Последовательность сетевых запросов при аутентификации и авторизации

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
AMQPS (RabbitMQ)	TCP	5671
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
AMQPS (RabbitMQ)	TCP	5671
HEALTH_CHECK	TCP	8100
«Шлюз»		
HTTP	TCP	80
HTTPS	TCP	443
RDP	TCP	3389
HEALTHCHECK	TCP	8101
GATEWAY (`termidesk-gateway`)	TCP	5099
SPICE	TCP	5634-6166*
DNS	UDP	53
«Агент виртуального рабочего места»		
HTTP	TCP	80
Kerberos	TCP/UDP	88
RPC	TCP	135
LDAP	TCP/UDP	389
HTTPS	TCP	443
SMB	TCP	445

Служба	Протокол	Порт
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 узла виртуализации»		
VMSD (`termidesk-vmsd`)	TCP	17082
Программное обеспечение termidesk-viewer (устанавливается с компонентом «Клиент»)		
HTTP	TCP	80
HTTPS	TCP	443
SPICE	TCP	5634-6166*
RDP	TCP	3389
«Сессионный агент»		
SESSION AGENT HTTP/HTTPS (`TermideskSessionAgent`)	TCP	31000
«Клиент»		
HTTP	TCP	80
HTTPS	TCP	443
RDP	TCP	3389
CLIENT (`termidesk-client`)	TCP	49152-65535**
«Виртуальный модуль Termidesk»		
ETCD	TCP/UDP	2379, 2380
«Оркестратор»		
HTTP	TCP	80
HTTPS	TCP	443
«Сервер терминалов Astra Linux» (STAL)		
RDP	TCP	3389
«Удаленный помощник»		
HTTP	TCP	80
HTTPS	TCP	443
STUN	TCP	19302

Служба	Протокол	Порт
WebRTC	TCP/UDP	1024-65535
Memcached	TCP	6379
REDIS	TCP/UDP	11211

Примечание:

* Фактический верхний предел диапазона портов определяется платформой виртуализации и зависит от количества ВМ на ее узле.

** Сетевой порт, открываемый узлом-источником для установления соединения, назначается динамически из диапазона 49152–65535, который определен настройками стека TCP/IP в ОС. В стеке TCP/IP ОС эти значения могут быть изменены.

> ⚠ При необходимости ограничить использование всех сетевых портов в ОС только теми, которые нужны компонентам, следует обратиться ко встроенным средствам ОС (например, «Брандмауэр» для ОС Microsoft Windows или `ufw` для ОС Linux).

Для управления сетевыми портами в ОС Microsoft Windows нужно:

- проверить список открытых портов и управляющих ими служб через интерфейс командной строки:

```
C:\Windows\system32> netstat -ab
```

- для разрешения или запрета сетевого порта перейти «Пуск» - «Параметры» - «Обновление и безопасность» - «Безопасность Windows» - «Брандмауэр и защита сети» - «Дополнительные параметры». Затем перейти во вкладку «Правила для входящих подключений», нажать экранную кнопку **[Создать правило]** и выбрать тип правила «Порт» (см. Рисунок 5). Далее выбрать нужный протокол (TCP или UDP), определить нужный порт (или несколько портов) в параметре «Определенные локальные порты» и на шаге «Действие» задать правило разрешения или запрета подключения.

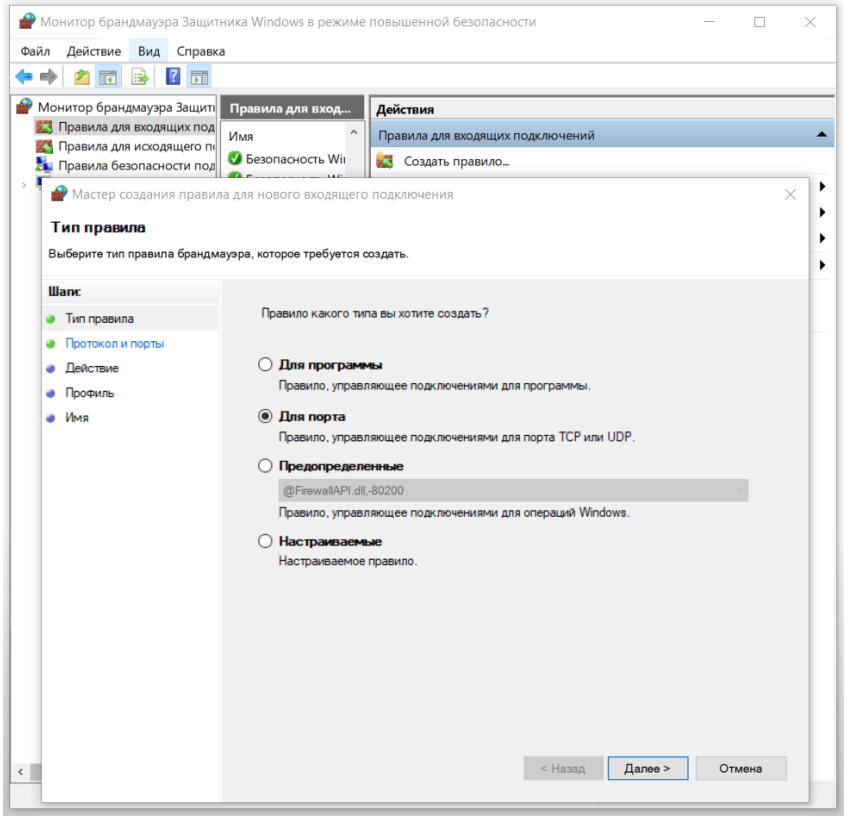

Рисунок 5 – Создание правила для типа «Порт»

Для управления сетевыми портами в ОС Linux нужно:

- проверить список открытых портов через интерфейс командной строки:

```
:~$ sudo ss -tulpn
```

- убедиться, что брандмауэр активен (должен отобразиться статус «Status: active»):

```
:~$ sudo ufw status verbose
```

- если брандмауэр неактивен, включить его:

```
:~$ sudo ufw enable
```

- для разрешения определенного сетевого порта выполнить:

```
:~$ sudo ufw allow <номер порта>
```

- для разрешения определенного диапазона сетевых портов выполнить:

```
:~$ sudo ufw allow <начальный номер порта:конечный номер порта/протокол>
```

Пример команды для разрешения портов 6000-6007 для протокола TCP:

```
:~$ sudo ufw allow 6000:6007/tcp
```

- для запрета сетевых портов подходит синтаксис, приведенный выше, но вместо команды `allow` используется `deny`.

2.6 . Перечень разрешающих правил межсетевого экрана, необходимых для работы компонентов Termidesk

На межсетевом экране, использующемся в организации, нужно задать следующие разрешающие правила (см. Таблица 3) для работы компонентов Termidesk.

В таблице приняты обозначения:

- «Узел-источник» - узел, являющийся инициатором сетевого соединения;
- «Узел-приемник» - узел, являющийся принимающей стороной сетевого соединения;
- «Протокол» - протокол транспортного уровня или уровня приложения, используемый в рамках соединения;
- «Порт приемника» - сетевой порт, прослушиваемый принимающей стороной.

Сетевой порт, открываемый узлом-источником для установления соединения, назначается динамически из диапазона 49152–65535, который определен настройками стека TCP/IP в ОС. В стеке TCP/IP ОС эти значения могут быть изменены.

Таблица 3 – Перечень правил межсетевого экрана

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
«Универсальный диспетчер»	localhost	TCP	8000	Работа веб-сервера «Универсального диспетчера» для обслуживания входящих подключений. Порт открывается на localhost
	Контроллеры доменов аутентификации	TCP/UDP	389	LDAP
		TCP	3268	LDAP
		TCP	636, 3269	LDAPS
	Сервер DNS	UDP	53	DNS
	Платформа виртуализации	TCP	80, 443	Для обслуживания запросов к платформе виртуализации
	ПК СВ Брест	TCP/UDP	2633	Для взаимодействия с ПК СВ Брест

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
	«Сессионный агент»	TCP	31000	Для обслуживания подключений к терминальным серверам, на которых установлен «Сессионный агент»
	СУБД	TCP	5432	Для обслуживания запросов к СУБД
	Сервер RabbitMQ	TCP	5672, 5671 (TLS)	Для обслуживания запросов к RabbitMQ
	«Агент виртуального рабочего места»	TCP	43900-44000	Обслуживание удаленных вызовов процедур (RPC)
	«Шлюз»	TCP	8102	Для обслуживания запросов проверок состояния (health check) «Шлюза»
	«Менеджер рабочих мест»	TCP	8103, 8104	Для обслуживания запросов проверок состояния (health check) «Менеджера рабочих мест» (`termidesk-celery-beat` и `termidesk-celery-worker`)
Рабочее место администратора	«Универсальный диспетчер»	TCP	443	Защищенное подключение к порталу Termidesk
	«Удаленный помощник» (серверная часть)	TCP	80, 443	Защищенное подключение к серверной части «Удаленного помощника»

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
«Менеджер рабочих мест»	localhost	TCP	8103, 8104	Для обслуживания запросов проверок состояния (health check) «Менеджера рабочих мест». Порт открывается на localhost
	СУБД	TCP	5432	Для обслуживания запросов к СУБД
	Сервер RabbitMQ	TCP	5672, 5671 (TLS)	Для обслуживания запросов к RabbitMQ
	ПК СВ Брест	TCP/UDP	2633	Для взаимодействия с ПК СВ Брест
«Шлюз»	localhost	TCP	5099 10000	Для обслуживания входящих подключений к «Шлюзу». Порт открывается на localhost, при распределенной установке - на IP-адресе 0.0.0.0
	localhost	TCP	8102	Для обслуживания запросов проверок состояния (health check) «Шлюза». Порт открывается на localhost
	Гипервизор	TCP	5634-6166	Для обслуживания подключений SPICE к ВМ. Фактический верхний предел диапазона портов определяется платформой виртуализации и зависит от количества ВМ на ее узле
	Сервер DNS	UDP	53	DNS

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
	«Агент виртуального рабочего места»	TCP	3389	Для обслуживания подключений по протоколу RDP к ВМ (при подключении пользователя через «Шлюз»)
		TCP	43900-44000	Для корректной работы технологии единого входа (SSO) при подключении через «Шлюз»
		TCP	5900	Для обслуживания подключений по протоколу TERA к ВМ (при подключении пользователя через «Шлюз»)
	«Универсальный диспетчер»	TCP	80, 443	Защищенное подключение к порталу Termidesk
	Терминальный сервер	TCP	31000	Для обслуживания подключений к терминальным серверам, на которых установлен «Сессионный агент»
«Клиент»	Сервер DNS	UDP	53	DNS
	«Универсальный диспетчер»	TCP	80, 443	Для обслуживания подключений к «Универсальному диспетчеру»

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
	Платформа виртуализации	TCP	5634-6166	Для обслуживания подключений SPICE к ВМ при подключении к ВРМ. Фактический верхний предел диапазона портов определяется платформой виртуализации и зависит от количества ВМ на ее узле
	ВМ или терминальный сервер	TCP	3389	Для обслуживания подключений RDP к ВМ или терминальному серверу
		TCP	43900-44000	Для корректной работы технологии единого входа (SSO) при прямом подключении к ВРМ (не через «Шлюз»)
		TCP	31000	Для обслуживания подключений к терминальным серверам, на которых установлен «Сессионный агент»
Клиент Loudplay (устанавливается на узел с «Клиентом» Termidesk)	Сервер Loudplay	UDP	6970, 6971	Для обмена видеопотоком между клиентом Loudplay и Сервером Loudplay
		UDP	6972, 6973	Для обмена аудиопотоком между клиентом Loudplay и Сервером Loudplay

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
		UDP	6974, 6975	Для обмена между клиентом Loudplay и Сервером Loudplay при использовании двух виртуальных мониторов и двух vGPU
		TCP	8554	Для обслуживания подключений к RTSP-серверу
		UDP	8555	Для обмена сообщениями, связанными с клавиатурой и мышью, между клиентом Loudplay и Сервером Loudplay
		TCP	8556	Для обмена RPC-сообщениями между клиентом Loudplay и Сервером Loudplay
		TCP	8557	Для обмена между клиентом Loudplay и Сервером Loudplay
«Агент виртуального рабочего места»	`localhost`	TCP	39188	Для обслуживания входящих подключений к «Агенту виртуальных рабочих мест». Порт открывается на localhost
	«Универсальный диспетчер»	TCP	80, 443	Для подключения к «Универсальному диспетчеру» и передачи информации о готовности ВМ
	Контроллеры доменов аутентификации	TCP	389	LDAP
		TCP	3268	LDAP
		TCP	636, 3269	LDAPS
		TCP	135	RPC

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
		TCP	1024-65535	SAM/NetLogon
		TCP/UDP	88	Kerberos
		TCP	445	SMB
	Сервер DHCP	TCP	67, 68	DHCP
	Сервер DNS	UDP	53	DNS
Сервер Loudplay (устанавливается на узел с «Агентом виртуального рабочего места» Termidesk)	Сервер лицензирования Loudplay	TCP	5555	Для обслуживания API-запросов о лицензиях и их статусе
		TCP	5556	Для обслуживания запросов к модулю лицензирования
«Агент узла виртуализации»	localhost	TCP	17082	Для обслуживания входящих подключений к «Агенту узла виртуализации». Порт открывается на localhost
«Сервер терминалов Astra Linux»	Сервер DNS	UDP	53	DNS
	Контроллеры доменов аутентификации	TCP/UDP	389	LDAP
		TCP	3268	LDAP
		TCP	636, 3269	LDAPS
	Сервер DHCP	TCP	67, 68	DHCP
«Оркестратор»	«Универсальный диспетчер»	TCP	80, 443	Для обслуживания подключений к «Универсальному диспетчеру»
	Служба облачной идентификации (cloud identity service)	TCP	Не определен	Для подключения к службе облачной идентификации с целью валидации токена. Порт определяется архитектурой конкретной облачной платформы

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
Агент облака (cloud agent)	«Оркестратор»	TCP	80, 443	Для обслуживания подключений между агентом облака (не является компонентом Termidesk) и «Оркестратором»
«Виртуальный модуль Termidesk»	«Виртуальный модуль Termidesk»	TCP/UDP	2379, 2380	Подключение ETCD для хранения и синхронизации конфигураций между узлами «Виртуального модуля Termidesk»
«Удаленный помощник» (клиентская часть)	«Удаленный помощник» (серверная часть)	TCP/UDP	80, 443	Для обслуживания подключений к серверной части «Удаленного помощника»
	Сервер STUN	TCP	19302	Для обслуживания подключений к серверу STUN (stun:// stun.l.google.com: 19302)
«Удаленный помощник» (серверная часть)	«Удаленный помощник» (клиентская часть)	TCP	1024-65535	Для обслуживания подключений к клиентской части «Удаленного помощника» WebRTC
	localhost	TCP	6379	Для обслуживания подключений к серверу REDIS. В текущей версии порт открывается на `localhost`
		TCP/UPD	11211	Для обслуживания подключений к серверу Memcached. Порт открывается на localhost

2.7 . Перечень сертификатов и ключей для компонентов Termidesk

Компоненты Termidesk и компоненты среды функционирования (например, брокер сообщений RabbitMQ или СУБД) могут использовать защищенное соединение для взаимодействия между собой.

Перечень сертификатов и ключей, используемых различными компонентами, приведен на схеме (см. Рисунок 6).

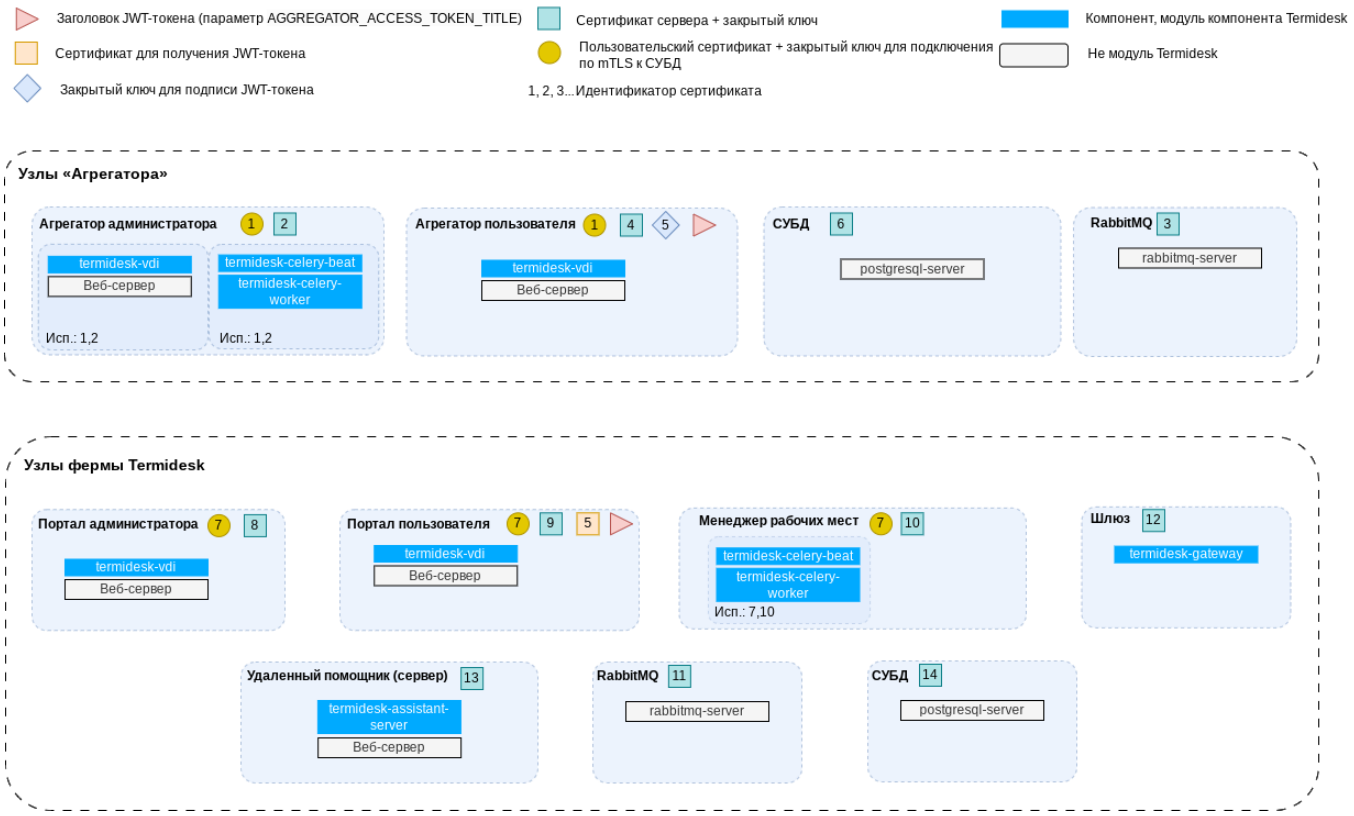

Рисунок 6 – Распределение сертификатов и ключей по компонентам

3 . НАЧАЛО РАБОТЫ

3.1 . Последовательность ввода в действие Termidesk VDI

Общая последовательность шагов для ввода Termidesk VDI 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**, **Комплексная установка Termidesk**, **Распределенная установка программного комплекса** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса»). Ввод в домен (при необходимости, согласно схеме сетевой инфраструктуры организации);
- установка компонента «Агент узла виртуализации» на узел виртуализации, если используется поставщик ресурсов ПК СВ Брест (см. подраздел **Требования к платформе виртуализации** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса»);
- 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 (см. подраздел **Подготовка базового ВРМ**);

> 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.

- добавление необходимого домена аутентификации (при необходимости, если в инфраструктуре используются серверы каталогов) (см. раздел **Аутентификация пользователей**);
- переход в графический интерфейс Termidesk и добавление необходимого поставщика ресурсов в Termidesk (см. раздел **Поставщики ресурсов**);

- создание шаблона РМ в Termidesk в добавленном поставщике ресурсов (см. раздел **Рабочие места**);
- добавление настроек гостевых ОС для созданного шаблона ВРМ (см. раздел **Управление параметрами гостевых ОС**);
- добавление протоколов доставки, которые будут использоваться для подключения к ВРМ (см. раздел **Протоколы доставки**);
- добавление сетей, которые будут использоваться для настройки доступа пользователей (см. раздел **Сети**);
- создание и настройка фонда РМ в Termidesk (см. раздел **Фонд рабочих мест**);
- назначение групп в созданном ранее фонде (см. подраздел **Назначение групп доступа фонду РМ**);
- назначение протоколов доставки в созданном ранее фонде (см. подраздел **Назначение протоколов фонду РМ**);
- назначение сетей в созданном ранее фонде (см. подраздел **Назначение сетей фонду РМ**);
- выполнение публикации настроенного фонда РМ в Termidesk (см. подраздел **Публикация фонда РМ**).

3.2 . Последовательность настройки при использовании терминального сервера

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

- при использовании терминального сервера 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 терминальный сервер (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. подраздел **Добавление терминального сервера (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 РМ для поставщика «Сервер терминалов» в Termidesk (см. подраздел **Шаблоны РМ для терминальны серверов**);

- добавление протоколов доставки, которые будут использоваться для подключения к РМ (см. раздел **Протоколы доставки**);
- добавление сетей, которые будут использоваться для настройки доступа пользователей (см. раздел **Сети**);
- создание и настройка фонда РМ в Termidesk (см. раздел **Фонд рабочих мест**);
- назначение групп в созданном ранее фонде (см. подраздел **Назначение групп доступа фонду РМ**);
- назначение протоколов доставки в созданном ранее фонде (см. подраздел **Назначение протоколов фонду РМ**);
- назначение сетей в созданном ранее фонде (см. подраздел **Назначение сетей фонду РМ**).

3.3 . Последовательность настройки при использовании автономных машин

Общая последовательность шагов при необходимости использования автономных машин выглядит следующим образом:

- установка компонента «Агент виртуального рабочего места» в ОС автономной машины (см. подраздел **Установка Агента ВРМ** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»);

> ⚠ Если автономная машина будет терминальным сервером, то требуется также установить компонент «Сессионный агент».

- переход в графический интерфейс Termidesk и добавление поставщика ресурсов «Автономные машины» в Termidesk (см. подраздел **Добавление автономной машины как поставщика ресурсов**);
- добавление необходимого домена аутентификации (при необходимости, если в инфраструктуре используются серверы каталогов) (см. раздел **Аутентификация пользователей**);
- создание шаблона РМ для поставщика «Автономные машины» в Termidesk (см. подраздел **Шаблон РМ для автономной машины**);
- добавление протоколов доставки, которые будут использоваться для подключения к РМ (см. раздел **Протоколы доставки**);
- добавление сетей, которые будут использоваться для настройки доступа пользователей (см. раздел **Сети**);
- создание и настройка фонда РМ в Termidesk (см. раздел **Фонд рабочих мест**);
- назначение групп в созданном ранее фонде (см. подраздел **Назначение групп доступа фонду РМ**);

- назначение протоколов доставки в созданном ранее фонде (см. подраздел **Назначение протоколов фонду РМ**);
- назначение сетей в созданном ранее фонде (см. подраздел **Назначение сетей фонду РМ**);
- выполнение публикации настроенного фонда РМ в Termidesk (см. подраздел **Публикация фонда РМ**).

3.4 . 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:

- для стабильной работы ВМ рекомендуется назначать ресурсы в соответствии с минимальными системными требованиями, установленными производителем ОС;
- 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 7);

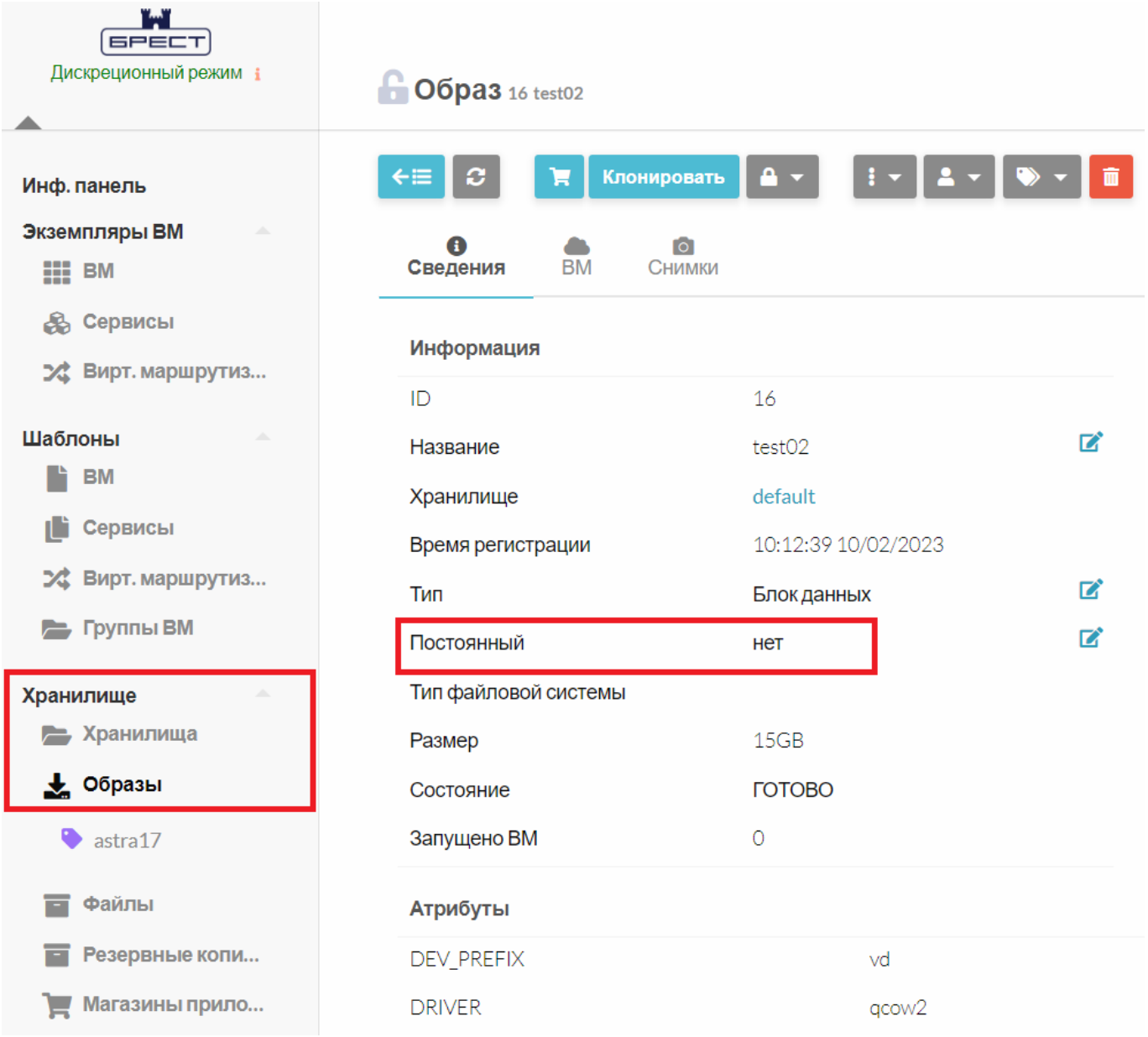

Рисунок 7 – Окно выбора типа подключаемого образа в ПК СВ Брест

⚠ Если ВМ в качестве гостевой ОС будет использовать ОС Microsoft 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 8);

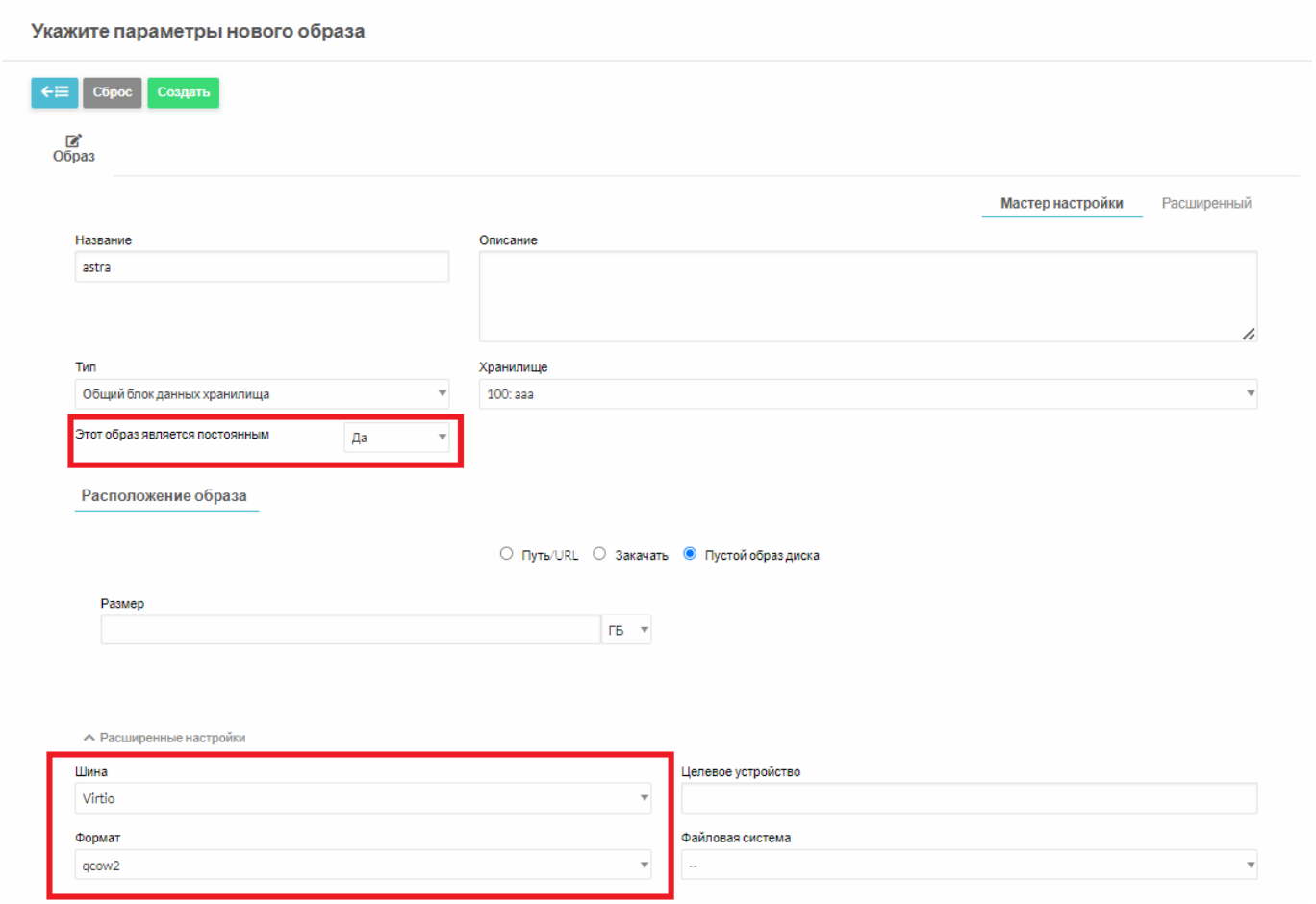

Рисунок 8 – Окно назначения параметров образа диска в ПК СВ Брест

⚠ 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 9);
  - в поле «ID Образа» указать идентификатор (ID) подключенного к шаблону ВМ образа диска;
  - поля «Имя образа» и «Имя пользователя владельца образа» очистить от любых значений;

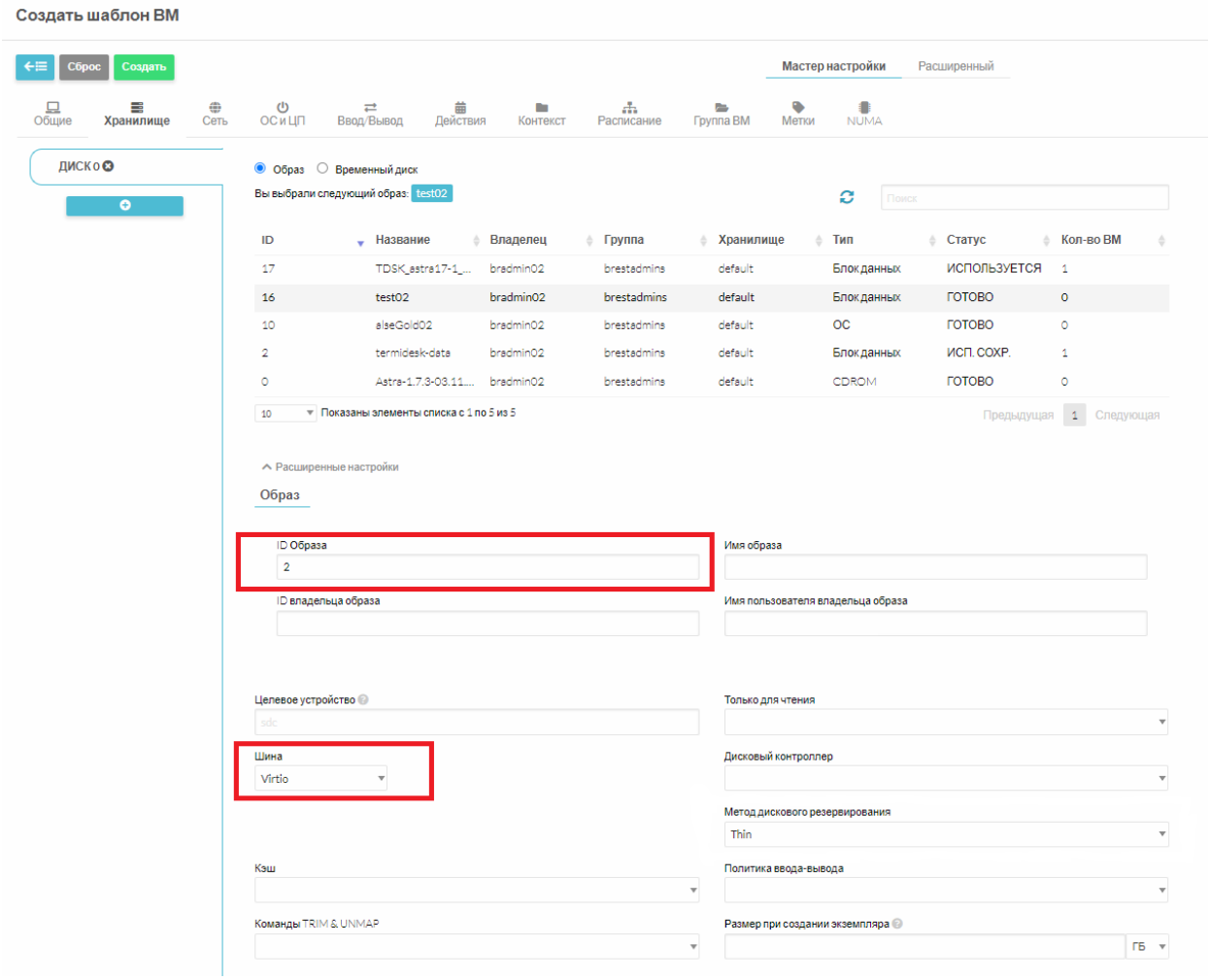

Рисунок 9 – Окно назначения расширенных параметров диска шаблона ВМ

- перейти в «Ввод/Вывод», затем в поле «Средства графического доступа» выбрать значение «SPICE», а в поле «Видеокарта» выбрать значение «QXL» (см. Рисунок 10);

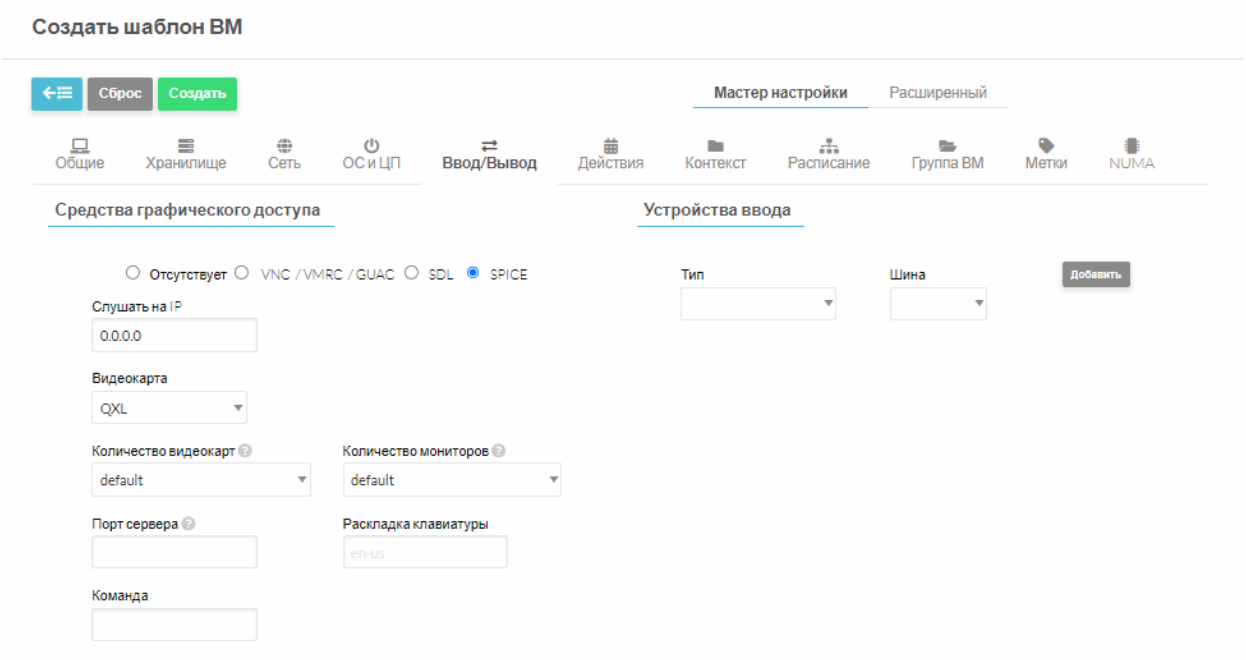

Рисунок 10 – Окно назначения средств графического доступа шаблона ВМ

- 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 Microsoft Windows;
- 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 11). 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 11 – Расположение параметра «Служебная ВМ»

3.5 . Подготовка базового шаблона ВМ на примере VMmanager

При создании базового шаблона ВМ в платформе управления виртуализации VMmanager необходимо учесть следующее:

⚠ Данная инструкция по подготовке базового шаблона актуальна для случая, если сервер VMmanager установлен на ОС Astra Linux 1.7.4.

- при добавлении конфигурации ВМ необходимо установить технологию вирутализации KVM, активировать чек-боксы (см. Рисунок 12) «Разрешить подключения по протоколу SPICE» и «Интеграция с TERMIDESK»;
- для стабильной работы ВМ рекомендуется назначать ресурсы в соответствии с минимальными системными требованиями, установленными производителем ОС;

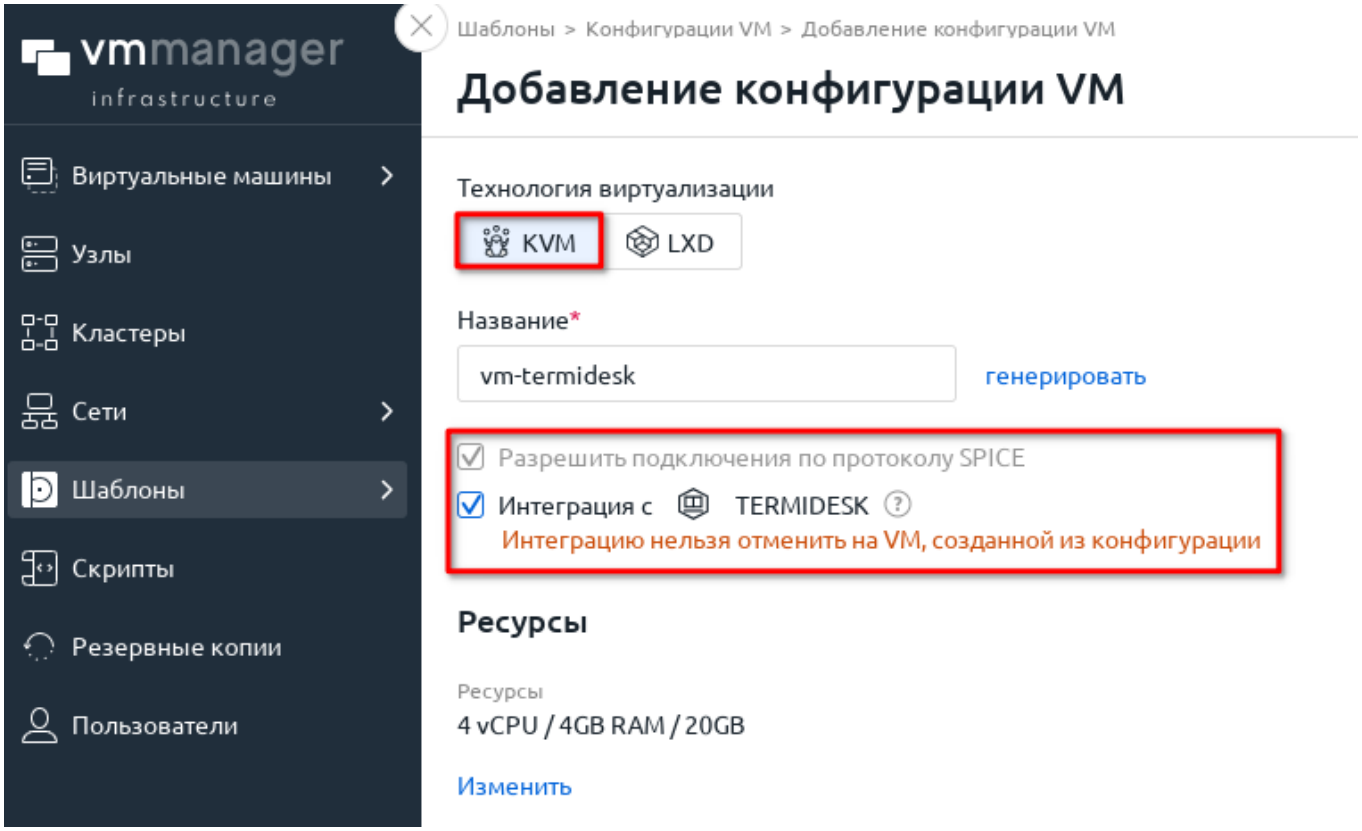

Рисунок 12 – Окно добавления конфигурации в VMmanager

- при создании ВМ необходимо:
  - выбрать ОС;

⚠ В случае выбора ОС Windows 10 необходимо использовать ОС Windows 10 RUS GPT для корректной работы автоматической выдачи IP-адресов.

  - выбрать созданную конфигурацию (см. Рисунок 13) для работы с Termidesk;

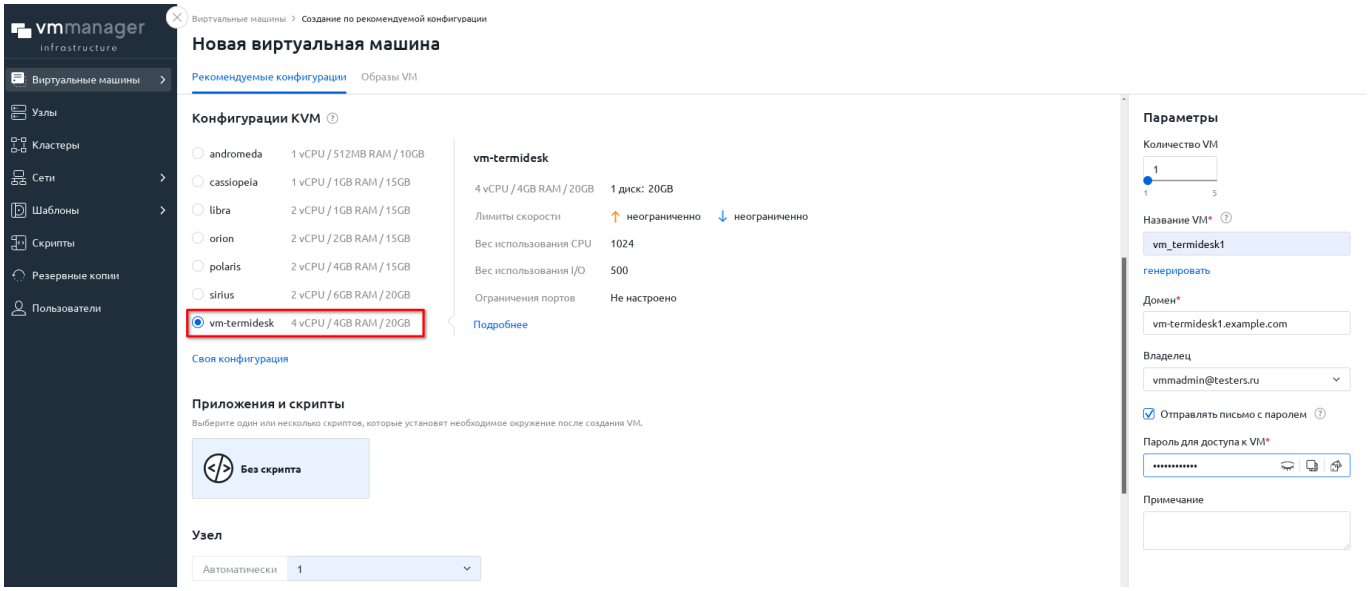

Рисунок 13 – Окно создания новой ВМ в VMmanager

- в блоке настроек «Приложение и скрипты» установить «без скрипта»;
- настроить узел, сеть;
- назначить название ВМ и пароль.

3.6 . Подготовка базового ВРМ

3.6.1 . Обязательные настройки базового ВРМ

3.6.1.1 . Обязательные настройки

Для подготовки необходимо:

- в созданной ранее ВМ выполнить настройку гостевой ОС;
- выполнить установку и настройку компонента «Агент виртуального рабочего места» (см. раздел **Установка и удаление компонента** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»);
- для активации функционала перенаправления видеокамеры и смарт-карт выполнить установку и настройку компонентов «Видеоагент» и «Агент виртуальных смарт-карт» (см. раздел **Установка и удаление компонента** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»);
- для активации возможности подключения к сессии пользователя через компонент «Удаленный помощник» (см. подраздел **Управление активными сессиями пользователей**) выполнить установку клиентской части «Удаленного помощника» (см. раздел **Установка и**

удаление компонента документа СЛЕТ.10001-01 91 02 «Инструкция по использованию. Компонент «Удаленный помощник»).

⚠ 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 РМ (см. подраздел **Добавление фонда РМ**).

3.6.1.2 . Настройка гостевой ОС Microsoft Windows

Настройка гостевой ОС Microsoft 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 ВРМ реализовано на базе поставщика ресурсов VMware vSphere, поскольку подключиться к такому ВРМ можно только по протоколам RDP или TERA.

- 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 ОС Microsoft Windows (доступ: https://www.spice-space.org/download/windows/spice-webdavd/) для включения возможности перенаправления каталога из пользовательской рабочей станции в ВРМ. Перенаправление каталогов из пользовательской рабочей станции в ВРМ 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 Microsoft Windows 7, а также при подключении по протоколу RDP с пользовательской рабочей станции на основе ОС Linux);
- для возможности подключения к ВРМ по протоколу TERA установить соответствующие пакеты, как это приведено в документе СЛЕТ.10001-01 90 09 «Руководство администратора. Настройка компонента TERA»;
- для возможности перенаправления принтеров из пользовательской рабочей станции с ОС Microsoft 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»;
- в настройках восстановления (см. Рисунок 14) служб `spice-agent` (`Spice Agent`), `vdservice` (`SPICE VDAgent`) и `TermideskService` (`Termidesk Agent Daemon`) назначить значение «Перезапуск служб» для действий при сбое. Для этого перейти «Диспетчер задач» - «Службы» - «Открыть службы», правой кнопкой мыши нажать на нужное наименование и перейти «Свойства» - «Восстановление».

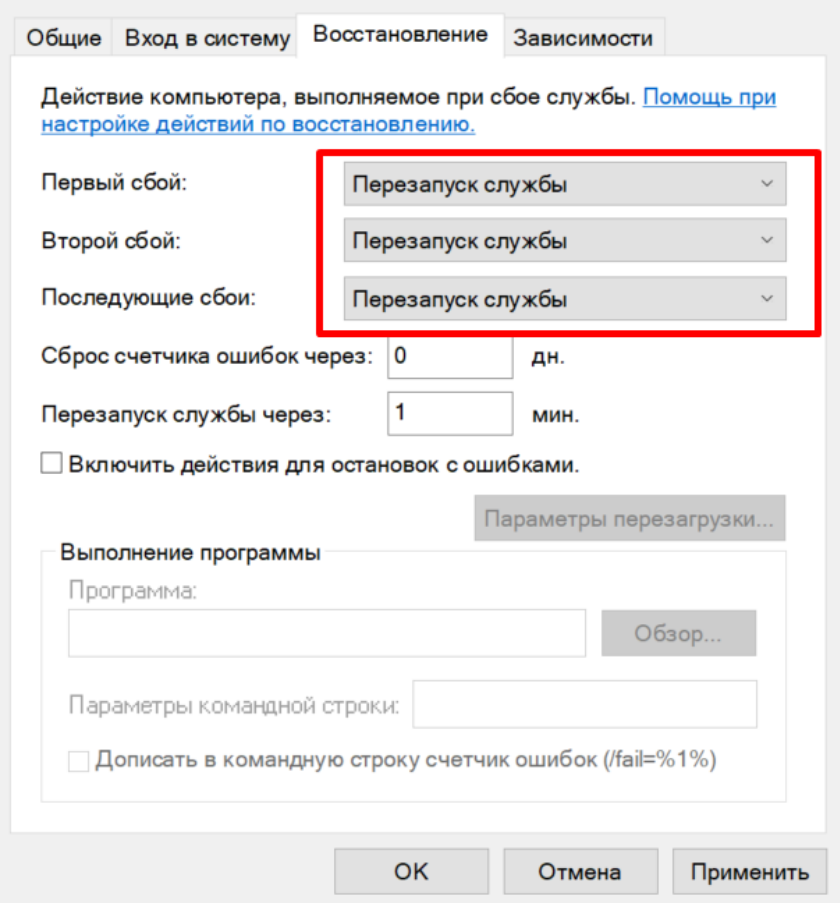

Рисунок 14 – Дополнительные свойства служб для ОС Microsoft Windows

3.6.1.3 . Настройка гостевой ОС Astra Linux

Настройка гостевой ОС Astra Linux сводится к выполнению следующих действий:

- для возможности подключения к ВМ по протоколу SPICE 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;

- для включения возможности перенаправления каталога в ВРМ по протоколу SPICE установить пакеты `spice-webdavd` и `davfs2`:

```
sudo apt install -y spice-webdavd davfs2
```

⚠ Для предоставления пользователям возможности перенаправления каталога в ВРМ необходимо также выполнить настройки, указанные в подразделе **Настройка перенаправления каталога из пользовательской рабочей станции в ВРМ**.

- для возможности подключения к ВРМ по протоколу RDP установить пакет `xrdp` и выполнить команды:

```
1 sudo apt install -y xrdp
2 sudo adduser xrdp ssl-cert
3 sudo systemctl restart xrdp
```

- для работы звука при подключении к ВРМ по протоколу RDP установить пакет `pulseaudio-module-xrdp`:

```
sudo apt install pulseaudio-module-xrdp
```

- для возможности подключения к ВРМ по протоколу TERA установить соответствующие пакеты, как это приведено в документе СЛЕТ.10001-01 90 09 «Руководство администратора. Настройка компонента TERA»;
- привести файл `/etc/acpi/events/powerbtn-acpi-support` к виду:

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

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

```
sudo apt install -y astra-ad-sssd-client
```

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

```
sudo apt install -y astra-freeipa-client
```

- для возможности ввода BPM с ОС Astra Linux в домен ALD Pro нужно:
  - подключить необходимый репозиторий согласно документации на программный комплекс ALD Pro;
  - установить пакеты `astra-freeipa-client` и `aldpro-client`:

```
sudo apt install -y astra-freeipa-client aldpro-client
```

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

- если планируется использование BPM доменными пользователями, то убедиться, что в конфигурационном файле `/etc/sssd/sssd.conf` параметру `use_fully_qualified_names` присвоено значение `False`. Если это не так, то изменить значение и перезапустить службу `sssd`:

```
sudo systemctl restart sssd
```

Для гостевой ОС Astra Linux 1.7 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;

⚠ Настройка должна быть выполнена для имен сетевых интерфейсов, а не их псевдонимов.

- отредактировать файл `/etc/network/interfaces`, добавив в него следующую строку, если ее нет:

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

- после изменения настроек выполнить перезапуск службы сети:

```
sudo systemctl restart networking
```

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
```

- для защиты файла `/etc/resolv.conf` от перезаписи нужно создать файл `/etc/dhcp/dhclient-enter-hooks.d/nodnsupdate`:

```
sudo touch /etc/dhcp/dhclient-enter-hooks.d/nodnsupdate
```

- отредактировать его содержимое, приведя к виду:

```
1  #!/bin/bash
2  make_resolv_conf() {
3          :
4  }
```

- сохранить файл и закрыть.

Вернуть возможность перезаписи файла `/etc/resolv.conf` можно, удалив ранее созданный файл `/etc/dhcp/dhclient-enter-hooks.d/nodnsupdate` и выполнив перезапуск сетевой службы:

```
sudo systemctl restart networking
```

3.6.1.4 . Настройка гостевой ОС РЕД

Настройка гостевой ОС РЕД сводится к выполнению следующих действий:

- для корректного отображения в Termidesk статуса ВМ нужно задать полное доменное имя гостевой ОС РЕД:

```
hostnamectl set-hostname workplace.termdiesk.local
```

где:

`workplace.termidesk.local` - полное доменное имя гостевой ОС;

- для возможности подключения к ВМ по протоколу SPICE установить пакеты `qemu-guest-agent`, `spice-vdagent`, `xorg-x11-drv-qxl`:

```
sudo dnf install -y qemu-guest-agent spice-vdagent xorg-x11-drv-qxl
```

где:

`-y` - ключ для пропуска подтверждения установки;

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

```
sudo dnf install -y spice-webdavd davfs2
```

⚠ Для предоставления пользователям возможности перенаправления каталога в BPM необходимо также выполнить настройки, указанные в подразделе **Настройка перенаправления каталога из пользовательской рабочей станции в BPM**.

- для возможности подключения к BPM по протоколу RDP нужно выполнить настройки согласно подразделу «Установка и настройка xrdp-сервера в РЕД ОС» официальной документации РЕД СОФТ:
  - для РЕД ОС версии 7.3 (доступ по ссылке: https://redos.red-soft.ru/base/redos-7_3/7_3-remote-access/7_3-sett-xrdp/7_3-xrdp/);
  - для РЕД ОС версии 8 (доступ по ссылке: https://redos.red-soft.ru/base/redos-8_0/8_0-remote-access/8_0-sett-xrdp/8_0-xrdp/);
- привести файл `/etc/acpi/events/powerbtn-acpi-support` к виду:

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

- для ввода BPM с ОС РЕД в домен FreeIPA нужно:
  - установить пакет `ipa-client`:

```
sudo dnf install -y ipa-client
```

  - для FreeIPA из состава ОС Astra Linux Special Edition внести изменения в файл `/usr/lib/python3/site-packages/ipalib/constants.py`:

```
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
```

В зависимости от дистрибутива ОС Linux команды могут отличаться от приведенных.

Для гостевой ОС РЕД необходимо также изменить способ назначения сетевых настроек.

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`:

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

```
echo -e 'domain <имя_домена>\nsearch <имя_домена>\nameserver <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 выполнив команду:

```
sudo chattr -i /etc/resolv.conf
```

3.6.1.5 . Настройка других гостевых ОС Linux

Настройка других гостевых ОС Linux сводится к выполнению следующих действий:

- для возможности подключения к ВРМ по протоколу SPICE установить пакеты `qemu-guest-agent`, `spice-vdagent`, `xserver-xorg-video-qxl`:

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

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

```
sudo apt install -y spice-webdavd davfs2
```

⚠ Для предоставления пользователям возможности перенаправления каталога в ВРМ необходимо также выполнить настройки, указанные в подразделе **Настройка перенаправления каталога из пользовательской рабочей станции в ВРМ**.

- для возможности подключения к ВРМ по протоколу RDP установить пакет `xrdp` и выполнить команды:

```
1 sudo apt install -y xrdp
2 sudo adduser xrdp ssl-cert
3 sudo systemctl restart xrdp
```

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

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

- при необходимости ввода BPM в домен FreeIPA:
  - для ОС CentOS установить пакеты `realm`, `ipa-client`;
  - для FreeIPA из состава ОС Astra Linux Special Edition внести изменения в файл `/usr/lib/python3/site-packages/ipalib/constants.py`:

```
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
> ```
>
> В зависимости от дистрибутива ОС Linux команды могут отличаться от приведенных.

  - настроить создание домашнего каталога для новых пользователей. Для этого выполнить:

```
sudo pam-auth-update
```

  - в псевдографическом интерфейсе активировать пункт «Create home directory on login» и нажать экранную кнопку [Ok] (см. Рисунок 15). Это добавит модуль `pam_mkhomedir.so` в файл `/etc/pam.d/common-session`.

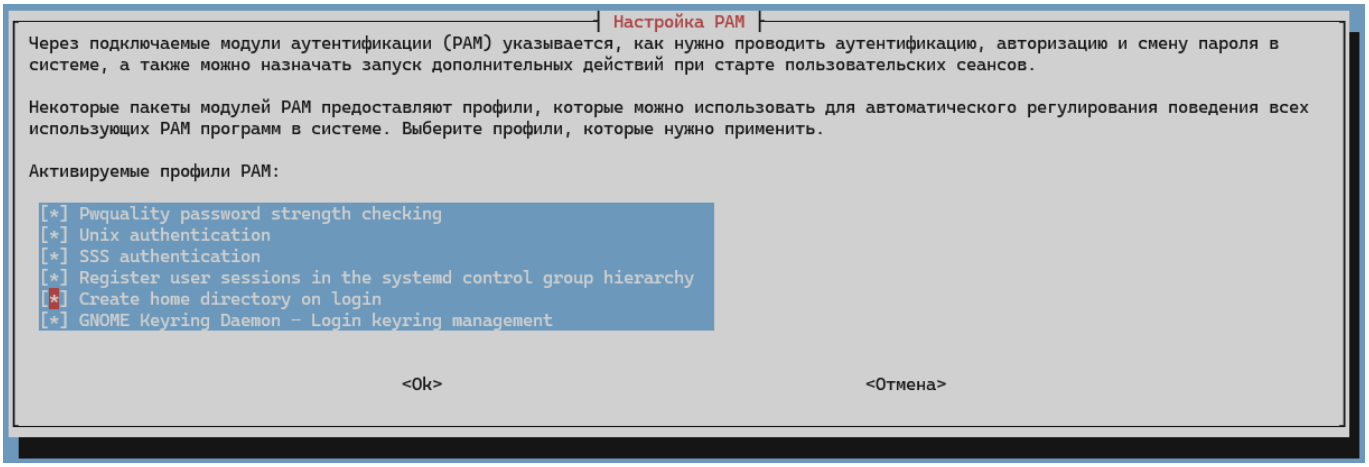

Рисунок 15 – Настройка PAM

3.6.2 . Настройка перенаправления каталога из пользовательской рабочей станции в BPM

Перенаправление каталога из пользовательской рабочей станции в BPM работает для протоколов SPICE, TERA и RDP. При этом:

- для протоколов RDP и TERA дополнительная настройка не выполняется;
- для протокола SPICE выполняется дополнительная настройка гостевой ОС BPM, как приведено ниже.

Для протокола TERA необходимо убедиться, что в гостевой ОС служба `tera-webdav-service` запущена:

```
sudo systemctl status tera-webdav-service
```

Для гостевой ОС Astra Linux Special Edition:

- должны быть установлены пакеты `spice-webdavd`, `davfs2`, `autofs`:

```
sudo apt install -y spice-webdavd davfs2 autofs
```

- далее создать каталог для монтирования:

```
sudo mkdir /media/davfs
```

- создать файл `/etc/auto.master.d/spice-webdav.autofs` следующего содержания:

```
/-  /etc/auto.master.d/auto.localwebdav.mount
```

где:

`/-` - опция, указывающая утилите `autofs` выполнять монтирование по существующему пути вместо автоматического создания подкаталогов в корневой точке монтирования;

- создать файл `/etc/auto.master.d/auto.localwebdav.mount` следующего содержания:

```
/media/davfs -fstype=davfs,rw,dir_mode=0777,file_mode=666 :http\://localhost\:9843
```

где:

`/media/davfs` - каталог, в который будет происходить монтирование;

`-fstype=davfs,rw` - тип смонтированной файловой системы с правами на чтение и запись в нее (`rw`);

`dir_mode=0777,file_mode=666` - права, с которыми будут доступны файлы и каталоги. Рекомендуется не менять указанные значения для исключения случаев монтирования файловой системы от пользователя `root` и недоступности файлов при подключении через программу доставки РМ (ПО Termidesk Viewer);

- отредактировать файл `/etc/davfs2/secrets`, добавив строку:

```
"http://localhost:9843/" "" ""
```

где:

`http://localhost:9843/` - место размещения файловой системы, по которому определяется устройство хранения для монтирования;

`"" ""` - логин и пароль пользователя, по умолчанию пусты для утилиты `spice-webdav`;

- перезапустить службу автоматического монтирования:

```
sudo systemctl restart autofs
```

Для гостевой ОС РЕД:

- установка пакетов `spice-webdavd`, `davfs2`, `autofs` выполняется через пакетный менеджер `dnf`:

```
sudo dnf install -y spice-webdavd davfs2 autofs
```

- остальные настройки перенаправления каталога по протоколу SPICE выполняются аналогично настройкам, приведенным для ОС Astra Linux Special Edition.

Для гостевой ОС Microsoft Windows должен быть установлен пакет `spice-webdavd` (доступ: https://www.spice-space.org/download/windows/spice-webdavd/spice-webdavd-x64-latest.msi).
После установки пакета в гостевой ОС Microsoft Windows произойдет следующее:

- будет добавлен сетевой диск;
- перенаправляемый каталог будет монтироваться в добавленный сетевой диск.

3.6.3 . 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. При этом:

- для протокола SPICE: условием масштабирования является запущенный процесс `spice-vdagent` в сессии пользователя. Дополнительно нужно выполнить настройку, описанную ниже, в том числе для экрана приветствия;
- для протокола TERA: условием автоматического масштабирования является запущенный процесс `tera-vdagent` в сессии пользователя. Дополнительные настройки могут выполняться при установке TERA (см. документ СЛЕТ.10001-01 90 09 «Руководство администратора. Настройка компонента TERA»).

Для настройки автоматического масштабирования экрана для протокола SPICE нужно:

- 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`:

> В примерах исполняемого файла указана переменная окружения `DISPLAY=:0`, актуальная только без активированного механизма единого входа (SSO).
> Для того чтобы задать для нее правильное значение при активированном механизме SSO, нужно проверить, какой дисплей используется:
>
> ```
> printenv | grep DISPLAY
> ```
>
> И далее использовать полученное значение вместо `DISPLAY=:0`.

- 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:

```
sudo chmod +x /usr/local/bin/x-resize
```

Для масштабирования экрана приветствия для протокола SPICE 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.

3.6.4 . Настройка вызова виртуальной клавиатуры в ОС Astra Linux

Настройка позволяет отображать виртуальную клавиатуру в гостевой ОС Astra Linux. Это нужно для случаев, когда ОС не реагирует на передачу данных с физической клавиатуры пользовательской рабочей станции.

Для настройки отображения виртуальной клавиатуры нужно:

- в графическом интерфейсе ОС Astra Linux перейти «Звезда - Панель управления - Рабочий стол» и выбрать ярлык «Горячие клавиши Fly» (см. Рисунок 16);

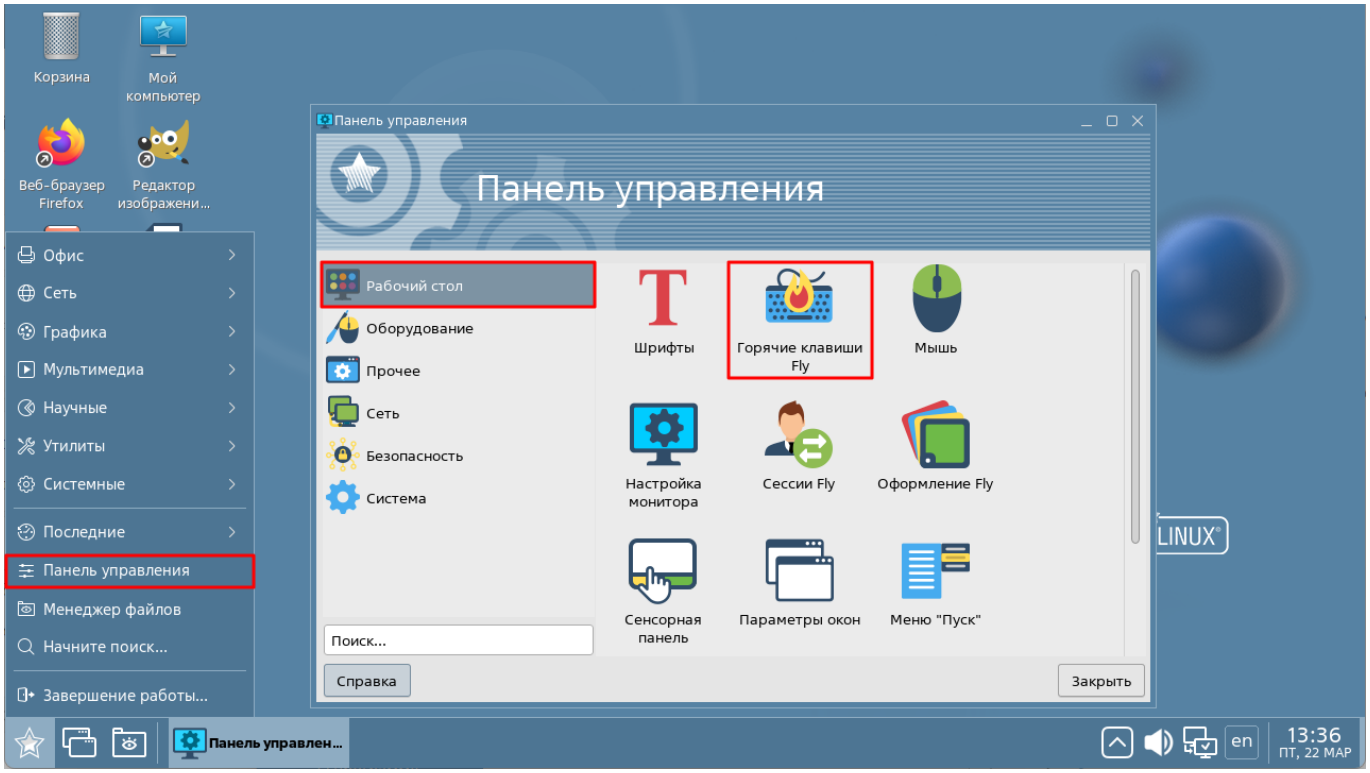

Рисунок 16 – Расположение ярлыка «Горячие клавиши Fly»

- в окне «Редактор горячих клавиш Fly» выбрать список «Клавиши для приложений» и нажать экранную кнопку [+] (см. Рисунок 17);

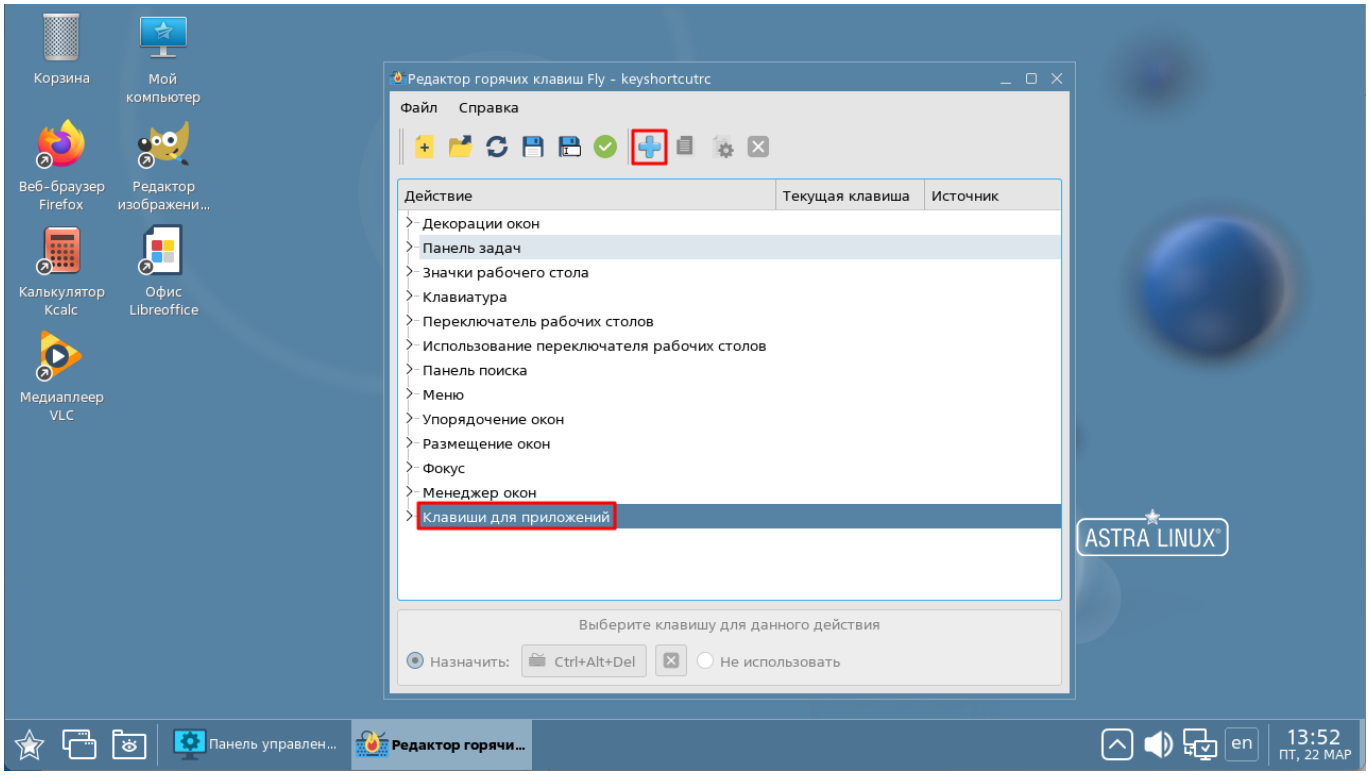

Рисунок 17 – Добавление команды вызова виртуальной клавиатуры

- в окне «Выбор команды» ввести команду вызова виртуальной клавиатуры `fly-vkbd` и нажать экранную кнопку [Да] (см. Рисунок 18);

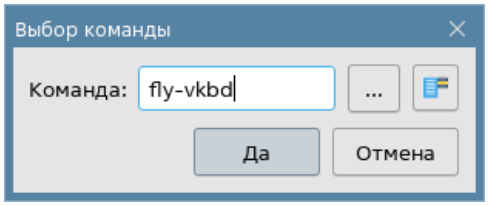

Рисунок 18 – Ввод команды вызова виртуальной клавиатуры

- выделить созданное действие, в области «Выберите клавишу для данного действия» выбрать параметр «Назначить», нажать сочетание клавиш **<Win>** + **<Ctrl>** + **<O>** и нажать экранную кнопку [Применить] (см. Рисунок 19).

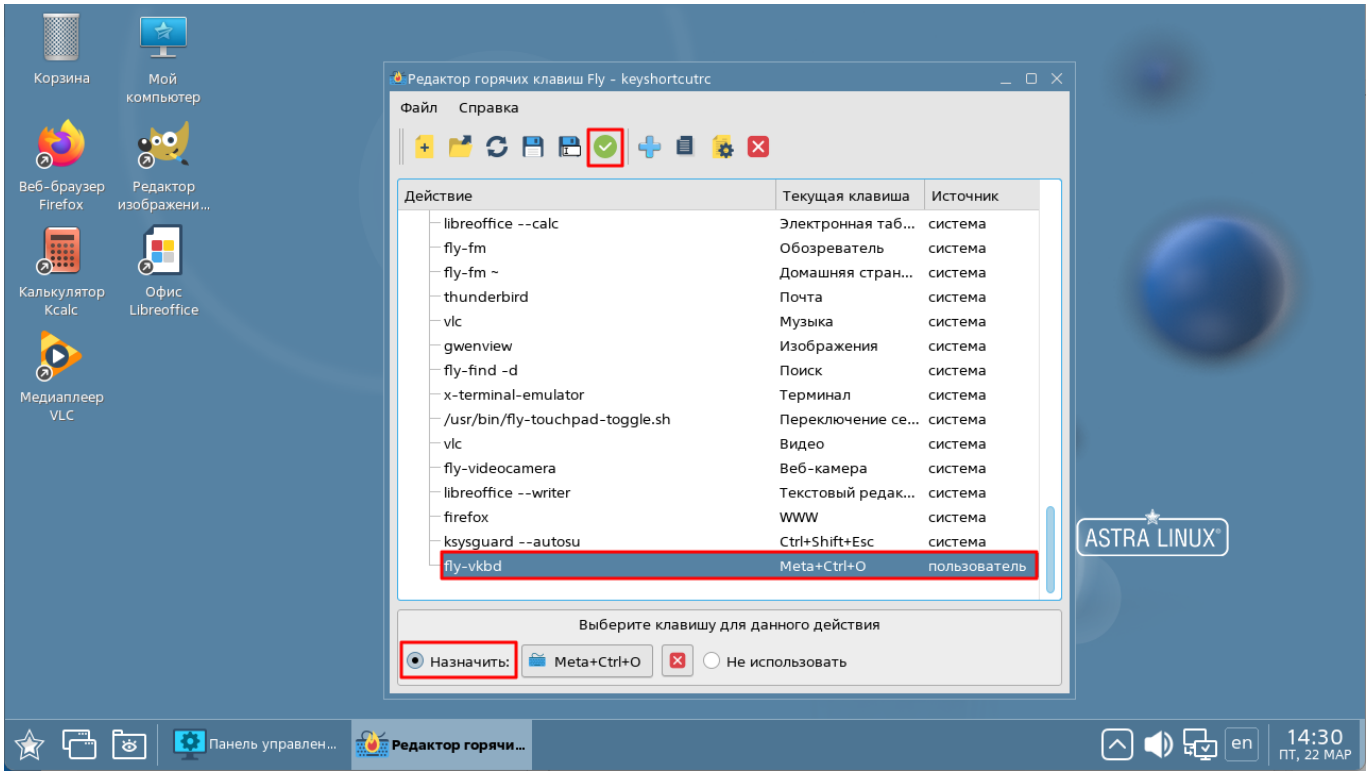

Рисунок 19 – Назначение сочетания клавиш вызова виртуальной клавиатуры

3.6.5 . Настройки для перенаправления принтеров

Для перенаправления принтера должны быть выполнены условия:

- в ОС пользовательской рабочей станции должен быть добавлен нужный принтер. Поддерживается перенаправление программных принтеров (например, программный виртуальный принтер PDF/XPS);
- в гостевой ОС ВРМ должен быть добавлен нужный принтер через существующую в гостевой ОС оснастку (например, «Менеджер печати Fly» для ОС Astra Linux Special Edition). Для выбранного принтера должен быть установлен драйвер «generic raw» или тот же драйвер, который используется в ОС пользовательской рабочей станции.

Добавление принтера может быть выполнено альтернативным способом (не через оснастку гостевой ОС) для гостевой ОС Linux, для этого:

- открыть в браузере URL-адрес: http://127.0.0.1:631/;
- перейти во вкладку «Администрирование». Выбрать пункт «Добавить принтер» и авторизоваться, использовав логин и пароль для входа в гостевую ОС;
- доступные принтеры будут отображены в списке «Найденные сетевые принтеры» (см. Рисунок 20). Выбрать принтер для добавления;

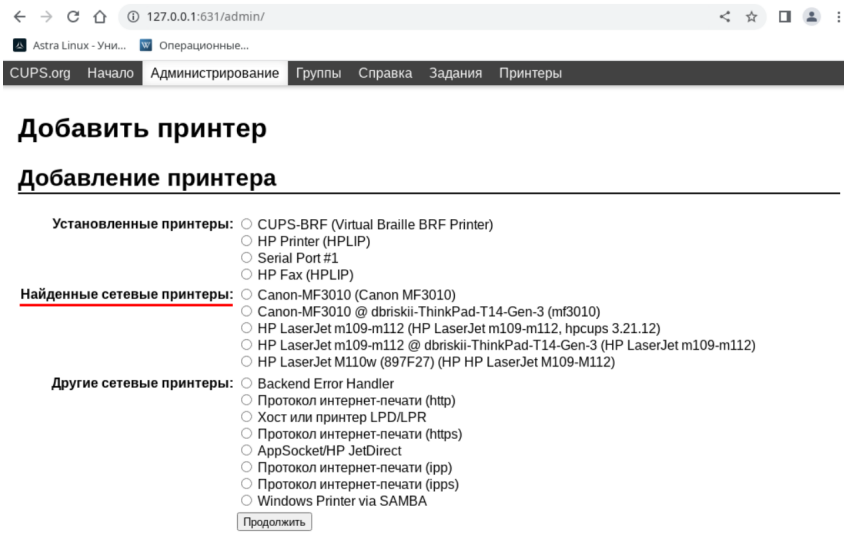

Рисунок 20 – Список найденных сетевых принтеров

- убедиться, что в строке «Подключение» (см. Рисунок 21) адрес начинается с «tdsk-prt»;

⚠ Настройка «tdsk-prt» актуальна при подключении по протоколу SPICE.

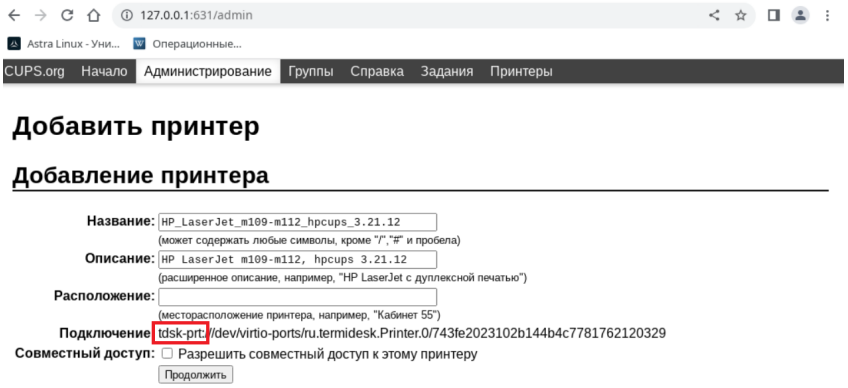

Рисунок 21 – Проверка URL

- выбрать модель принтера из списка (см. Рисунок 22) или использовать файл драйвера принтера PPD;

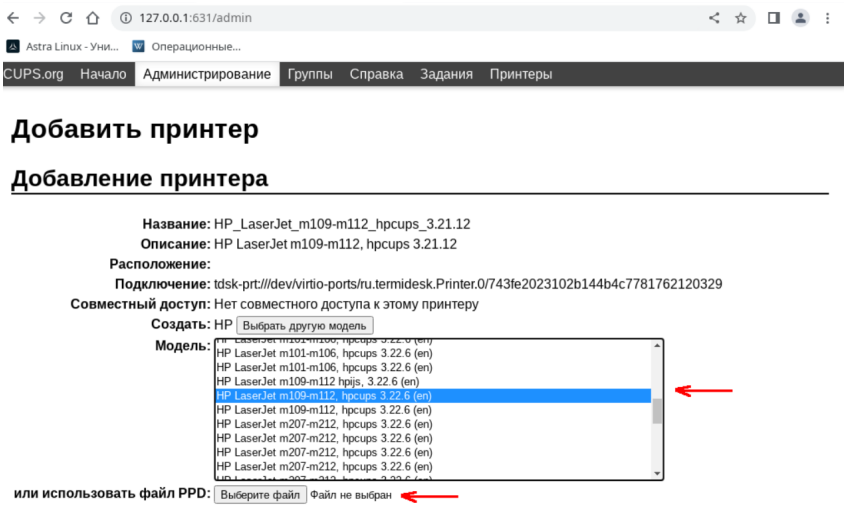

Рисунок 22 – Выбор модели принтера

- завершить добавление принтера.

Если список «Найденные сетевые принтеры» пуст:

> ⚠ Настройка актуальна при подключении по протоколу SPICE.

- выбрать значение «Termidesk Virtual Printer» в списке «Другие сетевые принтеры» (см. Рисунок 23);

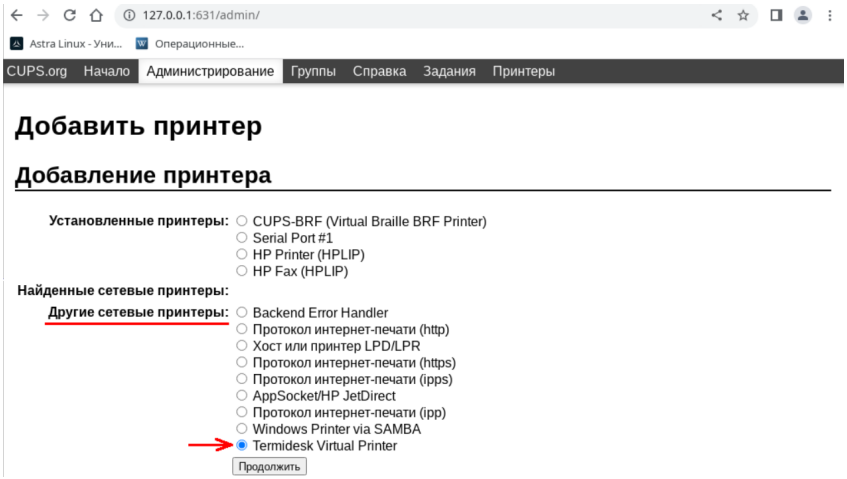

Рисунок 23 – Выбор другого сетевого принтера

- перейти к интерфейсу командной строки (открыть программу «Терминал Fly») и выполнить:

```
cd /usr/lib/cups/backend
sudo ./tdsk-prt
```

- выбрать адрес нужного принтера и скопировать его в поле «Подключение» в браузере;

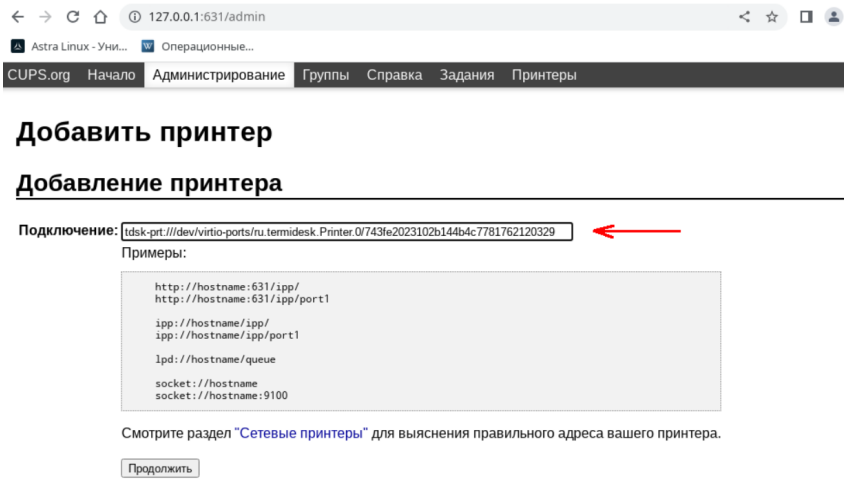

Рисунок 24 – Добавление адреса принтера

- завершить добавление принтера аналогично описанию выше, когда список «Найденные сетевые принтеры» содержал записи.

Добавленный принтер должен отобразиться в менеджере печати (например, «Менеджер печати Fly») гостевой ОС.

При перенаправлении принтера из пользовательской рабочей станции на ОС Microsoft Windows в BPM на ОС Microsoft Windows доступны следующие конфигурации драйверов:

⚠ Настройка актуальна при подключении по протоколу RDP.

- использование нативных драйверов: установка нативных драйверов на пользовательской рабочей станции и BPM позволяет использовать весь функционал принтера, включая двустороннюю печать. Для корректного перенаправления принтера версии драйверов должны совпадать;
- использование универсального драйвера Microsoft Software Printer Driver: универсальный драйвер позволяет избежать установки драйверов для каждого принтера. При этом драйвер поддерживает только одностороннюю печать.

Для использования универсального драйвера на пользовательской рабочей станции с установленным ПО Termidesk Viewer нужно создать переменную окружения `TDSK_RDP_PRT_UNIVERSAL`. Для перенаправления принтера с использованием нативного драйвера переменную нужно удалить.

3.6.6 . Технология единого входа

3.6.6.1 . Настройка технологии единого входа в гостевой ОС ВМ для протокола SPICE

Технология единого входа (автоматической авторизации) пользователя в гостевую ОС для протокола SPICE работает для:

- ОС Astra Linux Special Edition. При этом начиная с Termidesk версии 4.3 достаточно только включить механизм автоматической авторизации в гостевую ОС, как написано ниже;
- ОС Microsoft Windows. При этом необходимо установить пакет переносимых библиотек из состава Visual Studio C++ в гостевую ОС: https://aka.ms/vs/17/release/vc_redist.x64.exe.

Технология управляется политикой фонда РМ «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)» (см. **Политики фонда РМ**).

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

> Активация автоматической авторизации в ОС Linux влияет на настройку автоматического масштабирования экрана. Поэтому после активации этого механизма нужно проверить значение переменной окружения `DISPLAY` и скорректировать файл `/usr/local/bin/x-resize`, указав правильное значение для нее (см. подраздел **Автоматическое масштабирование экрана в ОС Astra Linux**).

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
```

3.6.6.2 . Настройка технологии единого входа в гостевой ОС ВМ для протокола TERA

Технология единого входа (автоматической авторизации) пользователя в гостевую ОС для протокола TERA работает для ОС Astra Linux Special Edition. При этом достаточно только включить механизм автоматической авторизации в гостевую ОС аналогично подразделу **Настройка технологии единого входа в гостевой ОС ВМ для протокола SPICE**.

Технология управляется политикой фонда РМ «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)» (см. **Политики фонда РМ**).

3.6.6.3 . Настройка технологии единого входа в гостевой ОС ВМ для протокола RDP

Технология единого входа (автоматической авторизации) пользователя в гостевую ОС для протокола RDP поддерживается средствами самого протокола.

Технология управляется политикой фонда РМ «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)» (см. **Политики фонда РМ**).

3.6.6.4 . Активация технологии единого входа на терминальном сервере 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 25), где `disp.termidesk.local` - имя узла с «Универсальным диспетчером» Termidesk. Далее нажать экранные кнопки **[OK]** и **[Применить]**;

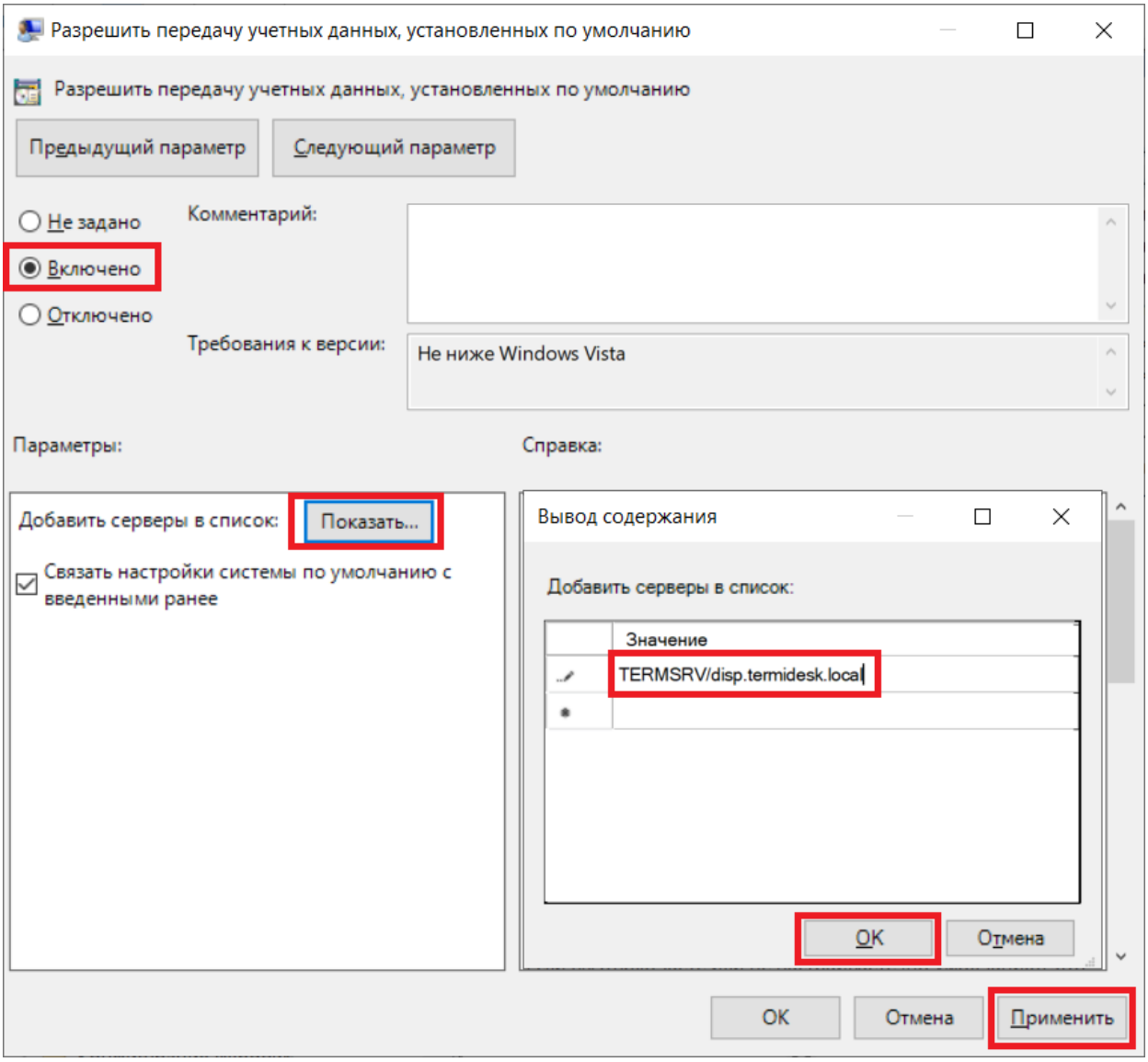

Рисунок 25 – Редактирование параметра «Разрешить передачу учетных данных, установленных по умолчанию» групповых политик

- 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 25). 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`.

3.6.7 . Настройка аутентификации пользователей BPM через файл

3.6.8 . 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. Механизм автоматической авторизации включается аналогично подразделу **Настройка технологии единого входа в гостевой ОС BM для протокола SPICE**.

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

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
```

3.6.9 . 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 - ПО Termidesk Viewer.

> ⚠ Возможность перенаправления видеокамеры определяется политикой «Перенаправление веб-камеры (RDP, SPICE, TERA)» (см. подраздел **Политики фонда РМ**).

В гостевую ОС РМ должен быть установлен компонент «Видеоагент».

3.6.10 . 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 - ПО Termidesk Viewer.

> ⚠ Возможность перенаправления смарт-карт определяется политикой «Перенаправление смарт-карт (RDP, SPICE, TERA)» (см. подраздел **Политики фонда РМ**).

В гостевую ОС РМ должен быть установлен компонент «Агент виртуальных смарт-карт».

3.6.11 . Аутентификация пользователей через носитель TouchMemory

Компонент «Клиент» Termidesk поддерживает аутентификацию пользователя через носитель TouchMemory, а именно - через программный продукт «Сетевой модуль ТМ-аутентификации WinNET» производства ООО «Фирма ИнфоКрипт».

Поддерживаемые ОС:

- для пользовательской рабочей станции: ОС Microsoft Windows, Debian (только с графическим окружением GNOME);
- для BPM: ОС Microsoft Windows.

Для реализации функционала администратору необходимо установить в гостевую ОС BPM:

- ПО WinNET 3.1, при установке выбрать значение «Сервер с MsTS»;
- ПО Vitamin (сервер).

3.6.12 . Перемещаемые профили

3.6.12.1 . Общие сведения по перемещаемым профилям

Перемещаемый профиль - это средство для сохранения настроек и документов пользователя между сеансами работы в РМ. Он представляет собой образ диска или каталога с пользовательскими данными и настройками РМ.

В зависимости от ОС РМ реализация перемещаемых профилей может различаться:

- ПК СВ Брест (ОС Astra Linux Special Edition): может применяться альтернативный способ, подразумевающий настройку атрибутов диска и модуля `PAM` (см. подраздел **Настройка перемещаемых профилей для ПК СВ Брест**);
- ОС Microsoft Windows: перемещаемые профили размещаются во вложенных каталогах общего сетевого ресурса (см. подраздел **Настройка перемещаемых профилей для ОС Microsoft Windows**).

3.6.12.2 . Настройка перемещаемых профилей для ПК СВ Брест

3.6.12.2.1 . Общие действия по настройке

> Функционал будет работать только для ОС Astra Linux Special Edition («Орел»).

Действия по настройке перемещаемых профилей сводятся к следующей последовательности:

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 BPM;
4) активация механизма перемещаемых профилей в Termidesk;
5) активация политики «Отделяемый пользовательский профиль».

3.6.12.2.2 . Создание базового образа диска в ПК СВ Брест

Для создания перемещаемого профиля (диска) на платформе ПК СВ Брест нужно:

- 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 появиться 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`:

```
sudo sfdisk /dev/sdb < /tmp/sfdisk.gpt
```

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

- преобразовать новый раздел диска в формат `ext4`:

```
sudo mkfs.ext4 /dev/sdb1
```

- проверить успешность создания диска:

```
sudo lsblk -JO /dev/sdb1
```

где:

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

3.6.12.2.3 . Задание атрибутов созданному диску

Для задания атрибутов созданному ранее диску нужно:

- выключить ВМ и отключить диск от нее;

- в свойствах диска добавить атрибут `TDSK_SHARED_TYPE` со значением `PRIVATE`. Запомнить идентификатор (ID) диска (см. Рисунок 26).

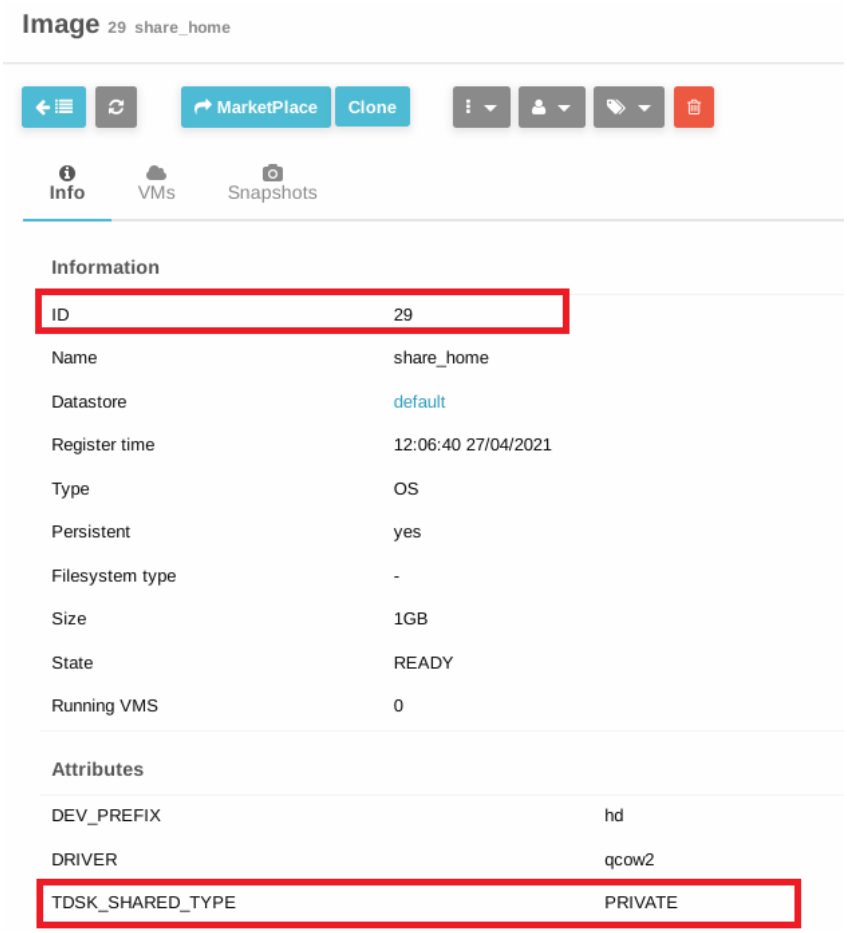

Рисунок 26 – Окно просмотра ID диска в ПК СВ Брест

3.6.12.2.4 . Настройка модуля PAM в базовом ВРМ

Для настройки модуля PAM в гостевой ОС базового ВРМ нужно:

- 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:
required        pam_exec.so     /usr/bin/pam_tdsk --autofs --skel=/etc/skel --chmod=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
```

3.6.12.2.5 . Активация механизма перемещаемых профилей в Termidesk

Для активации механизма перемещаемых профилей нужно:

- 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 профилей. Может быть задано
  несколько значений, через запятую.
2 TDSK_AUTOFS_IMAGES_ID=29
```

⚠ При наличии нескольких дисков требуется перечислить их через запятую.

- перезапустить службу `termidesk-vdi`:

```
sudo 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`.

3.6.12.2.6 . Активация политики в интерфейсе Termidesk

Для активации политики «Отделяемый пользовательский профиль» в «Портал администратора» Termidesk следует перейти «Настройки - Глобальные политики», затем параметру «Отделяемый пользовательский профиль» присвоить значение «Включен».

3.6.12.3 . Настройка перемещаемых профилей для ОС Microsoft Windows

Действия по настройке перемещаемых профилей сводятся к следующей последовательности:

1) подготовка сетевого хранилища, в котором профили пользователей будут храниться централизованно, позволяя пользователю получать доступ к одному и тому же профилю на всех серверах узла сеансов удаленных рабочих столов, настроенных на использование общего сетевого ресурса для профилей пользователей;

2) включение в настройках фонда РМ политик «Использование обязательных профилей на сервере узла сеанса удаленных рабочих столов (RDP)» и «Путь для перемещаемого профиля пользователя служб удаленного рабочего стола (RDP)» (см. подраздел **Политики фонда РМ**);

3) публикация фонда РМ.

Профили пользователей будут содержаться во вложенных каталогах на указанном в политике «Путь для перемещаемого профиля пользователя служб удаленного рабочего стола (RDP)» сетевом ресурсе. Каталоги будут созданы автоматически после подключения пользователей и названы по имени учетной записи каждого пользователя `%USERNAME%`.

3.6.13 . Настройка модуля `PAM` без монтирования перемещаемых профилей

Настройка модуля `PAM` (`pam_tdsk`) необходима для изменения конфигурации системы аутентификации, что требуется, например, при включении политики фонда РМ «Подключение с отличающимся именем пользователя».

Для настройки модуля PAM в гостевой ОС базового ВРМ нужно:

- выполнить подготовку базового ВРМ (см. подраздел **Подготовка базового ВРМ**);
- создать файл `/usr/share/pam-configs/pam_tdsk` со следующим содержимым:
  - если требуется аутентификация через файл паролей `/etc/htpasswd`:

```
Name: Termidesk PAM
Default: yes
Priority: 901
Auth-Type: Primary
Auth:
sufficient pam_exec.so expose_authtok quiet /usr/bin/pam_tdsk --htpasswd /etc/
htpasswd
```

  - в остальных случаях:

```
Name: Termidesk PAM
```

```
Default: yes
Priority: 901
Session-Type: Additional
Session:
required pam_exec.so quiet /usr/bin/pam_tdsk
```

- выполнить обновление профилей PAM:

```
sudo pam-auth-update
```

- убедиться, что в соответствующих файлах появилась строка с модулем `pam_tdsk`:
  - если использовался файл паролей `/etc/htpasswd`, то строка появится в `/etc/pam.d/common-auth`:

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

  - в остальных случаях строка появится в файле `/etc/pam.d/common-session`:

```
session    required pam_exec.so quiet /usr/bin/pam_tdsk
```

3.6.14 . Ограничение числа интерактивных сессий на РМ

Termidesk поддерживает ограничение числа сессий пользователя, подключенного к РМ:

- для терминальных сессий метапоставщика ограничение задается на этапе создания или редактирования сервисного фонда (см. подраздел **Добавление фонда РМ**);
- для ВРМ и автономных машин сессии ограничиваются одной. При этом для ОС Linux должна быть выполнена настройка модуля PAM (см. подраздел **Настройка модуля PAM без монтирования перемещаемых профилей**). Ограничение применяется после прохождения аутентификации пользователя на РМ, последовательность выглядит так:
  - пользователь аутентифицируется на сервере Termidesk;
  - пользователь аутентифицируется в гостевой ОС РМ;
  - модуль PAM выполняет аутентификацию и авторизацию по модулям, включая модуль «Агента виртуального рабочего места» - `pam_tdsk`;
  - модуль `pam_tdsk` получает значения, ограничивающие число сессий, у «Агента виртуального рабочего места»;
  - модуль `pam_tdsk` получает фактическое количество активных сессий в ОС;
  - в зависимости от полученных и фактических значений подключение пользователя будет разрешено или запрещено.

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 РМ.

Поддержка некоторых поставщиков ресурсов может добавляться в режиме экспериментальных функций.

В Termidesk поддерживаются следующие поставщики ресурсов:

- ПК СВ Брест (только для варианта лицензирования Termidesk VDI);
- платформа VMmanager (только для варианта лицензирования Termidesk VDI);
- платформа zVirt (только для варианта лицензирования Termidesk VDI);
- платформа oVirt (только для варианта лицензирования Termidesk VDI);
- платформа РЕД Виртуализация (только для варианта лицензирования Termidesk VDI);
- Openstack (только для варианта лицензирования Termidesk VDI);
- платформа VMware vSphere (только для варианта лицензирования Termidesk VDI);
- автономная машина (только для варианта лицензирования Termidesk VDI);
- терминальный сервер (MS RDSH или STAL), подключаемый через функционал метапоставщика (только для варианта лицензирования Termidesk VDI);
- терминальные серверы MS RDSH и STAL.

Веб-интерфейс Termidesk с установленной ролью «Портал администратора» обеспечивает следующие операции управления поставщиками ресурсов:

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

Для добавления в Termidesk поставщика ресурсов администратору Termidesk следует перейти «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка нужный вариант.

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 **[Изменить]**.

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 РМ.

4.2 . Добавление поставщика ресурсов ПК СВ Брест

4.2.1 . Получение и добавление файла keytab

`Keytab`-файлы используются для аутентификации в системах, использующих механизм 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 организации.

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 localuser@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 следует перейти «Компоненты - Поставщики ресурсов», нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка «ПК СВ Брест».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 4).

Таблица 4 – 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. Если ПК СВ Брест используется в сервисном режиме, то параметр можно не заполнять
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (полученный ранее `termidesk.keytab`). Если ПК СВ Брест используется в сервисном режиме, то параметр можно не заполнять. Пример: ▪ в случае стандартного хранения файла: «/etc/opt/termidesk-vdi/termidesk.keytab»; ▪ в случае хранения файла в хранилище hvac: «hvac-kv://secret#termidesk-admin/keytabs/termidesk». Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Если используется хранилище, то сгенерированный на контроллере домена `keytab`-файл должен быть преобразован к формату BASE64.
«Порт»	Номер порта для подключения к API платформы виртуализации. Значение по умолчанию: «2633», если на платформе не было указано иное
«Использовать SSL»	Управление использованием протокола SSL. Значение по умолчанию: «Нет»
«Проверка SSL»	Управление режимом строгой проверки SSL. Значение по умолчанию: «Да»
«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. При активации параметра проверка аутентификации `kerberos` (`termidesk.keytab`) не производится, проверяется только доступность поставщика ресурсов и его версия. Значение по умолчанию: «Да»
«Логин»	Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления платформой виртуализации

Параметр	Описание
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Пароль субъекта с полномочиями для управления платформой виртуализации
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/brest/»
«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. Значение по умолчанию: «Нет»
«Логин делегата»	Субъект, которому делегируется право на запуск ВМ на платформе виртуализации
«Пароль делегата»	Пароль субъекта, которому делегируется право на запуск ВМ на платформе виртуализации
«Подготавливать ВМ одновременно»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью «Интервал проверок кэша рабочих мест» (см. подраздел **Общие системные параметры Termidesk**). Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10», в параметре «Интервал проверок кэша рабочих мест» задано «19». Тогда за одну проверку (каждые 19 секунд) будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»
«Удалять ВМ одновременно»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»
«Время ожидания соединения»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации. Значение по умолчанию: «10»

⚠ 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 5).

Таблица 5 – 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/RHEV

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

⚠ Платформа oVirt версии 4.0 и выше поддерживает интеграцию с Termidesk без установки дополнительных пакетов.
Для корректной интеграции Termidesk с платформой oVirt версии ниже 4.0 нужно:

- на хост oVirt 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
```

- на управляющей ВМ платформы oVirt 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
```

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 6).

Таблица 6 – 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
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/ovirt/»
«Логин»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления платформой виртуализации. Указывается в формате: login@internal
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Подготавливать ВМ одновременно»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью «Интервал проверок кэша рабочих мест» (см. подраздел **Общие системные параметры Termidesk**). Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10», в параметре «Интервал проверок кэша рабочих мест» задано «19». Тогда за одну проверку (каждые 19 секунд) будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»

Параметр	Описание
«Удалять ВМ одновременно»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»
«Интервал опроса поставщика»	Периодичность (в минутах) выполнения опроса платформы. После завершения предыдущего опроса следующий запустится через время, указанное в этом параметре. При превышении указанного интервала администратору будет отображено уведомление, если настроен системный параметр отправки уведомления (см. подраздел **Общие системные настройки в интерфейсе Termidesk**). Возможные значения: от 1 до 1140. Значение по умолчанию: «5»
«Нижний предел свободного места на хранилище»	Минимальный объем (в Гб) хранилища, который должен быть доступен для последующего создания и размещения максимального числа ВРМ. Возможные значения: от 1 до 65000. Значение по умолчанию: «1000»
«Время ожидания соединения»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации. Значение по умолчанию: «10»

Для платформы oVirt субъект должен иметь привилегии, указанные в таблице (см. Таблица 7).

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 7 – 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»

Тип привилегий	Наименование привилегий
«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 следует перейти «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка «Платформа zVirt».

⚠ Для корректной интеграции Termidesk с платформой zVirt нужно:

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

```
sudo dnf install vdsm-hook-qemucmdline
```

- если пакет не найден, нужно выполнить активацию:

```
sudo dnf config-manager --enable "zvirt*"
```

и повторить установку.

Затем на управляющей машине («HostedEngine»):

- выполнить:

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

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

```
sudo service ovirt-engine restart
```

Далее подготовить образ ВМ, затем выполнить для него:

- перейти в меню редактирования свойств образа нажав экранную кнопку **[Edit]**. В разделе «Console» активировать пункты «USB Enabled» и «Smartcard Enabled»;
- перейти в раздел «Custom Properties». В правом меню нажать на выпадающий список «Please select a key...». Выбрать «qemu_cmdline» и в соседнем поле ввести (обязательно с сохранением квадратных скобок):
  - для zVirt 4.3:

```
["-device", "ich9-intel-hda,bus=pcie.0,addr=0x5",
 "-device", "hda-duplex",
 "-device", "nec-usb-xhci,id=xhci,bus=pcie.0,addr=0x7",
 "-device", "usb-host,hostbus=2,hostport=3,id=usb23",
 "-spice", "jpeg-wan-compression=always",
 "-device", "virtio-serial,bus=pcie.0,addr=0x8",
 "-chardev", "spiceport,id=WebDavPort,name=org.spice-space.webdav.0",
 "-device", "virtserialport,chardev=WebDavPort,name=org.spice-space.webdav.0",
 "-chardev",                                              "socket,path=/tmp/termidesk/
tvmd.sock,server=off,reconnect=1,mux=on,id=ru_termidesk_tvm",
 "-device", "virtserialport,chardev=ru_termidesk_tvm,name=ru.termidesk.tvm.0",
 "-chardev", "spiceport,id=RealtimeStreamingPort,name=TDSK_STREAM",
 "-device",
"virtserialport,chardev=RealtimeStreamingPort,name=ru.termidesk.RealtimeStreaming.0
",
 "-chardev", "spiceport,id=PrinterPort,name=TDSK_PRINTER",
 "-device", "virtserialport,chardev=PrinterPort,name=ru.termidesk.Printer.0",
 "-chardev", "spiceport,id=SmardCardPort,name=TDSK_PCSC",
 "-device", "virtserialport,chardev=SmardCardPort,name=ru.termidesk.PCSC.0"]
```

  - для zVirt ниже 4.3:

```
["-device", "ich9-intel-hda",
 "-device", "hda-duplex",
 "-device", "nec-usb-xhci,id=xhci",
 "-device", "usb-host,hostbus=2,hostport=3,id=usb23",
 "-spice", "jpeg-wan-compression=always",
 "-device", "virtio-serial",
 "-chardev", "spiceport,id=WebDavPort,name=org.spice-space.webdav.0",
 "-chardev",                                              "socket,path=/tmp/termidesk/
tvmd.sock,server=off,reconnect=1,mux=on,id=ru_termidesk_tvm",
 "-device", "virtserialport,chardev=ru_termidesk_tvm,name=ru.termidesk.tvm.0",
 "-chardev", "spiceport,id=RealtimeStreamingPort,name=TDSK_STREAM",
 "-device",
"virtserialport,chardev=RealtimeStreamingPort,name=ru.termidesk.RealtimeStreaming.0
",
 "-chardev", "spiceport,id=PrinterPort,name=TDSK_PRINTER",
 "-device", "virtserialport,chardev=PrinterPort,name=ru.termidesk.Printer.0",
 "-chardev", "spiceport,id=SmardCardPort,name=TDSK_PCSC",
 "-device", "virtserialport,chardev=SmardCardPort,name=ru.termidesk.PCSC.0"]
```

- нажать экранную кнопку **[Ok]** и сохранить изменения.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 8).

Таблица 8 – 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
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/zvirt/»
«Логин»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления платформой виртуализации. Указывается в формате: ▪ для zVirt 4.3: admin@zvirt@internalsso; ▪ для zVirtv ниже 4.3: login@internal
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Подготавливать ВМ одновременно»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью «Интервал проверок кэша рабочих мест» (см. подраздел **Общие системные параметры Termidesk**). Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10», в параметре «Интервал проверок кэша рабочих мест» задано «19». Тогда за одну проверку (каждые 19 секунд) будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»
«Удалять ВМ одновременно»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»
«Время ожидания соединения»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации. В случае возникновения проблем с созданием ВМ нужно увеличить время ожидания отклика. Значение по умолчанию: «10»

4.5 . Добавление платформы «РЕД Виртуализация»

Для добавления следует перейти «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** 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
```

Затем на управляющей ВМ («HostedEngine»):

- выполнить:

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

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

```
sudo service ovirt-engine restart
```

Далее подготовить образ ВМ, затем выполнить для него:

- перейти в меню редактирования свойств образа нажав экранную кнопку **[Edit]**. В разделе «Console» активировать пункты «USB Enabled» и «Smartcard Enabled»;
- перейти в раздел «Custom Properties». В правом меню нажать на выпадающий список «Please select a key...». Выбрать «qemu_cmdline» и в соседнем поле ввести (обязательно с сохранением квадратных скобок):

```
["-device", "ich9-intel-hda",
 "-device", "hda-duplex",
 "-device", "nec-usb-xhci,id=xhci",
 "-device", "usb-host,hostbus=2,hostport=3,id=usb23",
 "-spice", "jpeg-wan-compression=always",
 "-device", "virtio-serial",
 "-chardev", "spiceport,id=WebDavPort,name=org.spice-space.webdav.0",
 "-chardev",                                              "socket,path=/tmp/termidesk/
tvmd.sock,server=off,reconnect=1,mux=on,id=ru_termidesk_tvm",
 "-device", "virtserialport,chardev=ru_termidesk_tvm,name=ru.termidesk.tvm.0",
 "-chardev", "spiceport,id=RealtimeStreamingPort,name=TDSK_STREAM",
 "-device",
"virtserialport,chardev=RealtimeStreamingPort,name=ru.termidesk.RealtimeStreaming.0
",
 "-chardev", "spiceport,id=PrinterPort,name=TDSK_PRINTER",
 "-device", "virtserialport,chardev=PrinterPort,name=ru.termidesk.Printer.0",
 "-chardev", "spiceport,id=SmardCardPort,name=TDSK_PCSC",
 "-device", "virtserialport,chardev=SmardCardPort,name=ru.termidesk.PCSC.0"]
```

- нажать экранную кнопку **[Ok]** и сохранить изменения.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 9).

Таблица 9 – 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
«Логин»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления платформой виртуализации. Указывается в формате: login@internal
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/red/ (see page 13)»
«Подготавливать ВМ одновременно»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью «Интервал проверок кэша рабочих мест» (см. подраздел **Общие системные параметры Termidesk**). Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10», в параметре «Интервал проверок кэша рабочих мест» задано «19». Тогда за одну проверку (каждые 19 секунд) будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»
«Удалять ВМ одновременно»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»
«Время ожидания соединения»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации. Значение по умолчанию: «10»

4.6 . Добавление поставщика VMmanager

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

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 10).

Таблица 10 – 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
«Порт»	Номер порта для подключения к VMmanager. Значение по умолчанию: «5000», если на платформе не настроен другой
«Логин (эл. почта)»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления платформой виртуализации VMmanager
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий субъекта
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/vmm/»
«Использовать SSL»	Включение использования протокола SSL. Значение по умолчанию: «Нет»
«Проверять SSL»	Включение строгой проверки SSL. Значение по умолчанию: «Нет»
«Подготавливать ВМ одновременно»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью «Интервал проверок кэша рабочих мест» (см. подраздел **Общие системные параметры Termidesk**). Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10», в параметре «Интервал проверок кэша рабочих мест» задано «19». Тогда за одну проверку (каждые 19 секунд) будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»
«Удалять ВМ одновременно»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»

Параметр	Описание
«Интервал опроса поставщика»	Периодичность (в минутах) выполнения опроса платформы. После завершения предыдущего опроса следующий запустится через время, указанное в этом параметре. При превышении указанного интервала администратору будет отображено уведомление, если настроен системный параметр отправки уведомления (см. подраздел **Общие системные настройки в интерфейсе Termidesk**). Возможные значения: от 1 до 1140. Значение по умолчанию: «5»
«Нижний предел свободного места на хранилище»	Минимальный объем (в Гб) хранилища, который должен быть доступен для последующего создания и размещения максимального числа ВРМ. Возможные значения: от 1 до 65000. Значение по умолчанию: «1000»
«Таймаут»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации. Значение по умолчанию: «10»

4.7 . Добавление платформы VMware vSphere

Для добавления следует перейти «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** 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).

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 11).

Таблица 11 – 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)
«Порт»	Номер порта для подключения к API платформы. Значение по умолчанию: «443»
«Использовать SSL»	Форсировать использование протокола SSL. Значение по умолчанию: «Да»
«Логин»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления платформой виртуализации VMware

Параметр	Описание
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий субъекта
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/vmware/»
«Выбрать ресурсы платформы»	Активировать использование ресурсов платформы для размещения ВМ. После активации в параметрах «Кластер ресурсов», «Кластеры данных», «Сети» станет доступен выбор ресурсов, полученных от платформы виртуализации. Значение по умолчанию: «Нет» ⚠ Перед активацией параметра нужно заполнить поля «Название», «Адрес сервера», «Порт» (при необходимости), «Логин», «Пароль» и нажать экранную кнопку **[Тест]**. Необходимо обязательно задать этот параметр!
«Кластер ресурсов»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд ВРМ. Доступные значения получены от платформы виртуализации ⚠ Необходимо обязательно задать этот параметр!
«Кластеры данных»	Идентификатор кластера ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд ВРМ. Доступные значения получены от платформы виртуализации ⚠ Необходимо обязательно задать этот параметр!
«Сети»	Выбор одной или нескольких сетей, созданных на платформе виртуализации VMware, адреса из которых могут быть назначены ВМ из фонда ВРМ ⚠ Необходимо обязательно задать этот параметр!
«Подготавливать ВМ одновременно»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью «Интервал проверок кэша рабочих мест» (см. подраздел **Общие системные параметры Termidesk**). Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10», в параметре «Интервал проверок кэша рабочих мест» задано «19». Тогда за одну проверку (каждые 19 секунд) будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»

Параметр	Описание
«Удалять ВМ одновременно»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»
«Интервал опроса поставщика»	Периодичность (в минутах) выполнения опроса платформы. После завершения предыдущего опроса следующий запустится через время, указанное в этом параметре. При превышении указанного интервала администратору будет отображено уведомление, если настроен системный параметр отправки уведомления (см. подраздел **Общие системные настройки в интерфейсе Termidesk**). Возможные значения: от 1 до 1140. Значение по умолчанию: «5»
«Нижний предел свободного места на хранилище»	Минимальный объем (в Гб) хранилища, который должен быть доступен для последующего создания и размещения максимального числа ВРМ. Возможные значения: от 1 до 65000. Значение по умолчанию: «1000»

Субъект должен иметь привилегии, указанные в таблице (см. Таблица 12).

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 12 – 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» «Mark as template» «Mark as virtual machine»
«Virtual machine»: «Snapshot management»	«Create snapshot» «Remove snapshot» «Rename snapshot» «Revert to snapshot»

4.8 . Добавление терминального сервера (MS RDS и STAL) в качестве поставщика ресурсов

Для добавления следует перейти «Компоненты - Поставщики ресурсов», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Сервер терминалов [экспериментальный]».

⚠ Для взаимодействия с терминальным сервером (MS RDS или STAL) необходимо установить компонент «Сессионный агент» в соответствии с подразделом **Установка сессионного Агента** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент».

Работа с MS RDS поддерживается только при условии развернутой полнофункциональной инфраструктуры MS RDS, при этом роль «Remote Desktop Gateway» должна быть развернута, но не должна использоваться. Если такой инфраструктуры нет, то рекомендуется воспользоваться решением, основанным на поставщике ресурсов «метапоставщик».

Терминальный сервер для ОС Astra Linux реализуется компонентом «Сервер терминалов Asta Linux» (STAL) Termidesk, 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».

Следует использовать отдельные установки терминальных серверов: на одном сервере MS RDS или STAL - публикация только приложений, на другом MS RDS или STAL - только терминальных сессий.

Далее 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»	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. **FQDN** узла, на котором установлен «Сессионный агент» Termidesk
«Порт сессионного агента»	Номер порта «Сессионного агента» Termidesk. Значение по умолчанию: «31000»
«Домен»	Наименование домена для подключения к терминальному серверу
«Логин»	Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления терминальным сервером. 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 РМ при этом добавить не получится

Параметр	Описание
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/terminal/»
«Таймаут сессионного агента»	Время ожидания (в секундах) отклика от «Сессионного агента». Указанное значение также определяет время ожидания обработки запросов при подключении пользователя к STAL и отправляется на компонент «Клиент». Значение по умолчанию: «10»
«Использовать HTTPS»	Выбор использования протокола HTTPS для запросов к «Сессионному агенту». 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». Если используется протокол HTTP , то необходимо настроить «Универсальный диспетчер» на использование протокола HTTP, скорректировав файл `/etc/apache2/sites-available/termidesk.conf` (см. подраздел **Перенаправление на HTTPS**) Значение по умолчанию: «Нет»
«Валидация сертификата»	Выбор проверки подлинности сертификата при запросах к «Сессионному агенту». Значение по умолчанию: «Нет»

⚠ В инфраструктуре должна быть сетевая связанность между компонентами «Универсальный диспетчер» и «Сессионный агент» по IP-адресу. Если на узле «Универсального диспетчера» используется VPN с туннелированием, функционал оповещения и регистрации, приведенный ниже, между этими компонентами работать не будет.

После добавления сервера терминалов в Termidesk будет зарегистрирован MAC-адрес узла, на котором установлен «Сессионный агент». В то же время непосредственно «Сессионный агент» сохранит IP-адрес «Универсального диспетчера», который отправил ему запрос. Поскольку MAC-адрес нужен для регистрации событий, то в случае его изменения «Универсальный диспетчер» перестанет принимать события от этого «Сессионного агента», однако подключение при этом будет работать.

Для исправления ситуации, когда MAC-адрес был изменен и от «Сессионного агента» перестали регистрироваться события, нужно:

- либо открыть поставщик ресурсов и нажать экранные кнопки **[Тест]** и **[Сохранить]** для перерегистрации «Сессионного агента»;
- либо создать новый поставщик ресурсов с указанием нужного «Сессионного агента»;
- либо выполнить на узле с «Универсальным диспетчером» команды:

```
sudo -u termidesk bash
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_refresh_ssa
```

Указанные команды выполняются также для регистрации «Сессионного агента» в случае, если компонент «Универсальный диспетчер» был обновлен раньше него.

Если после попытки проверить введенные данные экранной кнопкой **[Тест]** появляются сообщения об ошибке, то при создании шаблона РМ будет блокироваться возможность его сохранения (создания).
Для корректного подключения через компонент «Клиент» к серверу терминалов необходимо задать параметр «Аутентификация 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.

4.9 . Добавление терминального сервера (метапоставщика) в качестве поставщика ресурсов

4.9.1 . Предварительная настройка для добавления терминального сервера метапоставщика

Алгоритм подготовки для добавления терминального сервера метапоставщика выглядит следующим образом:

- на платформе виртуализации создается ВМ терминального сервера («золотой образ») с гостевой ОС Microsoft Windows Server (2016 и выше) (для тиражирования ОС Microsoft Windows) или ОС Astra Linux Special Edition (Server) (для тиражирования ОС Astra Linux Special Edition);
- в гостевую ОС устанавливается и настраивается компонент «Агент виртуального рабочего места» и компонент «Сессионный агент» (см. документ СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»);
- для тиражирования приложений и терминальных сессий в гостевую ОС Microsoft Windows Server устанавливается роль сервера публикации приложений «Remote Desktop Session Host» из состава «Remote Desktop Services», выполняется активация роли через «Сессионноый агент» (см. подраздел **Активация роли терминального сервера в ОС Microsoft Windows Server** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента

«Агент»). Если ОС Microsoft Windows Server не вводится в домен, то в ОС следует создать пользователя с правами доступа к удаленному рабочему столу;

- для тиражирования приложений и терминальных сессий в гостевую ОС 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.

Не допускается вмешательство (переустановка «Сессионного агента», удаление БД «Сессионного агента» и др.) в уже функционирующую ноду терминального сервера.
Обновление или переустановка «Сессионного агента» выполняется только на ВМ терминального сервера, которая является «золотым образом» для нод терминального сервера метапоставщика.

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

Далее нужно добавить соответствующие объекты в в веб-интерфейсе Termidesk:

- создать поставщик ресурсов с той платформой виртуализации, на которой создана подготовленная ВМ терминального сервера (см. раздел **Поставщики ресурсов**);
- в поставщике ресурсов создать нужный шаблон РМ для выбранной платформы виртуализации (см. раздел **Рабочие места**). В параметре «Базовая ВМ» выбранного шаблона указать подготовленную ВМ терминального сервера;
- создать сервисный фонд РМ для шаблона РМ (см. подраздел **Добавление фонда РМ**). В сервисном фонде **не** указываются группы пользователей, пользователи, протоколы доставки (их можно удалить после создания фонда). Сервисный фонд должен использовать кеш 1-го уровня (кеш 2-го уровня не используется);

Для сервисного фонда РМ обязательно нужно проверить используемое значение политики «Действие при выходе пользователя из ОС» (см. подраздел **Политики фонда РМ**).
Хотя бы одно РМ должно получить статус «Действительный» во вкладке «Рабочие места» созданного фонда, иначе все дальнейшие действия будут завершаться ошибкой «Не удалось найти подходящую для подключения машину».
При понижении количества ВМ в кеше 1-го уровня сервисного фонда те ВМ, на которых есть активные сессии метапоставщика, не будут удалены.

- добавить поставщик «Сервер Терминалов Метапоставщик» (см. подраздел **Перечень параметров для добавления терминального сервера метапоставщика**);
- создать шаблон РМ для этого поставщика, выбрав тип в зависимости от того, что нужно опубликовать - терминальную сессию или приложение (см. подразделы **Шаблон для публикации приложений** или **Шаблон для терминальных сессий**);
- добавить фонд РМ для метапоставщика (см. подраздел **Добавление фонда публикации служб «метапоставщика»**).

4.9.2 . Перечень параметров для добавления терминального сервера метапоставщика

ⓘ Ранее поставщик ресурсов «Сервер терминалов (метапоставщик)» активировался через экспериментальный параметр `experimental.metasessions.provider.enabled`, однако, начиная с версии Termidesk 6.0 активация данного параметра не требуется.

Для добавления поставщика ресурсов следует перейти «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка «Сервер терминалов Метапоставщик».

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 14).

ⓘ Сразу после создания поставщика ресурсов «Сервер терминалов (метапоставщик)» будет создан шаблон рабочего места с наименованием «Meta Terminal Service».

Таблица 14 – Данные для добавления терминального сервера (метапоставщика)

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Порт сессионного агента»	Номер порта «Сессионного агента» Termidesk. Значение по умолчанию: «31000»
«Домен»	Наименование домена для подключения к серверу терминалов
«Логин»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления сервером терминалов
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий

Параметр	Описание
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/meta/»
«Фонд»	Выбор **сервисного фонда** для размещения. ⓘ В качестве сервисного фонда может быть выбран фонд автономных машин. В списке отображаются только те сервисные фонды, которые не используются другим метапоставщиком
«Таймаут сессионного агента»	Время ожидания (в секундах) отклика от «Сессионного агента». Указанное значение также определяет время ожидания обработки запросов при подключении пользователя к STAL и отправляется на компонент «Клиент». Значение по умолчанию: «10»
«Использовать HTTPS»	Выбор использования протокола HTTPS для запросов к «Сессионному агенту». 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 использования протокола HTTP нужно отключить данный параметр и установить опцию `USE_HTTPS` в значение «False» в конфигурационном файле «Сессионного агента». Если используется протокол HTTP, то необходимо настроить «Универсальный диспетчер» на использование протокола HTTP, скорректировав файл `/etc/apache2/sites-available/termidesk.conf` (см. подраздел **Перенаправление на HTTPS**). По умолчанию параметр выключен
«Проверка сертификата»	Выбор проверки подлинности сертификата при запросах к «Сессионному агенту». По умолчанию параметр выключен
«Соиспользование сессий»	Выбор метода балансировки, основанного на совместном использовании сессии приложениями. Если параметр выключен, то подключение пользователя будет происходить на любую ноду (первую во внутреннем списке). При включении параметра будет производиться поиск и учет активной сессии пользователя. Если такая сессия найдена, приложение будет запущено на той же ноде. По умолчанию параметр включен

Параметр	Описание
«Балансировка по метрикам»	Выбор метода балансировки, основанного на полученных метриках, регулярно присылаемых от «Сессионного агента», установленного на метапоставщике (MS RDS или STAL). Описание механизма балансировки приведено в подразделе **Балансировка подключений на основе загрузки терминальных серверов метапоставщика**. Возможные значения: ▪ «Да» - для балансировки будет рассчитываться нагрузка ноды метапоставщика. Пользователю будет выдана для подключения та нода, которая имеет в момент запроса наименьшее значение нагрузки; ▪ «Нет» - метод балансировки по метрикам использоваться не будет. В этом случае параметр «Предпочитать соиспользование сессий вместо балансировки» не проверяется Поведение при балансировке также зависит от значений других параметров: ▪ если активированы «Балансировка по метрикам», «Соиспользование сессий», «Предпочитать соиспользование сессий вместо балансировки», то новая сессия пользователя будет направлена на ту же ноду метапоставщика, на которой у пользователя есть хотя бы одна сессия. Значение нагрузки ноды будет проигнорировано; ▪ если активированы только «Балансировка по метрикам» и «Соиспользование сессий», то будет проверено значение нагрузки ноды. Если нагрузка = 10000, то новая сессия будет направлена на наименее загруженную ноду. Значение нагрузки ноды рассчитывается на основании значения индекса нагрузки, вычисляемого из имеющихся показателей метрик. В случае, если несколько нод имеют одинаковое наименьшее значение нагрузки, то подключение может быть выполнено на любую ноду. ⚠ Механизм оповещения и связанный с ним механизм балансировки по метрикам передает IP-адрес «Универсального диспетчера» на «Сессионный агент», поэтому в инфраструктуре должна быть сетевая связанность между этими компонентами по IP-адресу. Если на узле «Универсального диспетчера» используется VPN с туннелированием, функционал балансировки по метрикам работать не будет. Оценка нагрузки при выборе этого метода балансировки происходит на основании параметров (метрик балансировки), заданных ниже. Периодичность отправки метрик определяется настройками, заданными на странице «Настройки - Системные параметры - Метрики» (см. подраздел **Настройка отправки метрик для «Сессионного агента»**)
«Применить "Утилизпация ЦП"»	ⓘ Использование возможно при активации параметра «Балансировка по метрикам». Управление использованием метрики при расчете нагрузки. Значение по умолчанию: «Да» (метрика используется)

Параметр	Описание
«Утилизация ЦП»	Использование возможно при активации параметра «Балансировка по метрикам». Для формирования кеша метрик, на основании которых будет происходить балансировка, нужно активировать настройку «Применить "Использование ЦП"». Параметр задает предел загруженности процессора ноды метапоставщика в процентах. Изменение применяется на компоненте «Сессионный агент» сразу. Диапазон значений: от 1 до 100. Значение по умолчанию: «100»
«Применить "Использование ОЗУ"»	Использование возможно при активации параметра «Балансировка по метрикам». Управление использованием метрики при расчете нагрузки. Значение по умолчанию: «Да» (метрика используется)
«Использование ОЗУ»	Использование возможно при активации параметра «Балансировка по метрикам». Для формирования кеша метрик, на основании которых будет происходить балансировка, нужно активировать настройку «Применить "Использование ОЗУ"». Параметр задает предел загруженности оперативной памяти ноды терминального сервера в процентах. Изменение применяется на компоненте «Сессионный агент» сразу. Диапазон значений: от 1 до 100. Значение по умолчанию: «100»
«Применить "Сессий всего"»	Использование возможно при активации параметра «Балансировка по метрикам». Управление использованием параметром «Сессий всего» при расчете нагрузки. Если параметр выключен, то: ▪ предел числа подключений пользователей будет определяться параметром `MAX_SESSIONS` конфигурационного файла компонента «Сессионный агент». Компонент «Сессионный агент» отправляет значение параметра вместе с метриками узла; ▪ если число подключений пользователей достигло предела, заданного в параметре `MAX_SESSIONS`, то терминальный сервер считается полностью нагруженным и не может принимать новые подключения. Значение по умолчанию: «Да» (параметр используется)

Параметр	Описание
«Сессий всего»	Использование возможно при активации параметра «Балансировка по метрикам». Параметр задает предел числа подключений пользователей к ноде метапоставщика. При достижении заданного лимита новые подключения будут происходить к другой доступной ноде. Текущие пользователи, уже имеющие открытую сессию на ноде, будут подключены к ней же, если в настройках метапоставщика активирован параметр «Соиспользование сессий». Изменение применяется на компоненте «Сессионный агент» сразу. Диапазон значений: от 1 до 181. Значение по умолчанию: «181»
«Влияние входов в систему на нагрузку»	Использование возможно при активации параметра «Балансировка по метрикам». Параметр определяет, как сильно влияет процесс входа пользователя в ОС ноды на производительность ноды метапоставщика. Используется для предотвращения перегрузки ноды в момент балансировки. Чем менее производительна нода, тем сильнее на нее влияет число подключившихся пользователей и тем выше будет нагрузка на нее. Для снижения нагрузки следует назначить более высокую степень влияния на производительность. Изменение применяется на компоненте «Сессионный агент» сразу. Возможные значения: ▪ «Экстремальное (Extreme)»; ▪ «Высокое (High)»; ▪ «Выше среднего (Medium-High)»; ▪ «Среднее (Medium)» (по умолчанию); ▪ «Ниже среднего (Medium-Low)»; ▪ «Не использовать» - при выборе этого значения параметр не будет учитываться при балансировке
«Предпочитать соиспользование сессий вместо балансировки»	Использование возможно при активации параметра «Балансировка по метрикам». Параметр переопределяет механизм балансировки при полной загрузке ноды метапоставщика: будет использоваться механизм соиспользования сессий, а не балансировка по метрикам узла

Максимальное число подключений к ноде (одной) метапоставщика, если не используется «Балансировка по метрикам», можно задать командой `termidesk-vdi-manage`, предварительно переключившись на пользователя `termidesk`:

```
sudo -u termidesk bash
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_config set --key experimental.metasessionsprov.maxConnectionCount --value <значение>
```

В случае, если используется «Балансировка по метрикам» максимальное число подключений задается параметром «Сессий всего».

После добавления метапоставщика в Termidesk будет зарегистрирован MAC-адрес узла, на котором установлен «Сессионный агент». В то же время непосредственно «Сессионный агент» сохранит IP-адрес «Универсального диспетчера», отправившего ему запрос. Поскольку MAC-адрес нужен для регистрации событий, то в случае его изменения «Универсальный диспетчер» перестанет принимать события от этого «Сессионного агента», однако подключение при этом будет работать.

Для исправления ситуации, когда MAC-адрес был изменен и от «Сессионного агента» перестали регистрироваться события, нужно:

- либо открыть поставщик ресурсов и нажать экранные кнопки **[Тест]** и **[Сохранить]** для перерегистрации «Сессионного агента»;
- либо создать новый поставщик ресурсов с указанием нужного «Сессионного агента»;
- либо выполнить на узле с «Универсальным диспетчером» команды:

```
sudo -u termidesk bash
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_refresh_ssa
```

Указанные команды выполняются также для регистрации «Сессионного агента» в случае, если компонент «Универсальный диспетчер» был обновлен раньше него.

4.9.3 . Балансировка подключений на основе загрузки терминальных серверов метапоставщика

Для эффективного распределения ресурсов терминальных серверов метапоставщика реализована поддержка балансировки подключений на основе метрик, которые отправляет «Сессионный агент».

Балансировка подключений будет работать только при выборе протокола доставки «RDP (терминальный доступ)». Более ранние протоколы доставки не поддерживаются.

Процесс балансировки выглядит следующим образом:

- «Сессионный агент», установленный на ноды метапоставщика, собирает метрики узла и хранит их в своей БД;
- «Универсальному диспетчеру» передаются средние значения метрик ноды, подсчет которых задается через параметр «Размер кеша» (см. подраздел **Настройка отправки метрик для «Сессионного агента»**);
- на основе полученных метрик «Универсальный диспетчер» рассчитывает нагрузку на каждую ноду метапоставщика. Расчет нагрузки хранится в таблице БД «Универсального диспетчера»;
- при запросе пользователя на подключение метапоставщик:
  - проверяет, установлен ли в его свойствах параметр «Соиспользование сессий» (см. подраздел **Перечень параметров для добавления терминального сервера**

метапоставщика). Если параметр активирован и у пользователя уже есть активная сессия, то метапоставщик вернет адрес подключения той ноды, на которую терминирована сессия;

- проверяет, активирован ли параметр «Балансировка по метрикам». Если параметр активирован, то метапоставщик получит список всех нод и выполнит балансировку подключения, вернув пользователю ноду, имеющую минимальную нагрузку или любую, если несколько нод имеют одинаково наименьшее значение нагрузки. При этом во время балансировки будут проверены условия как получения метрик, так и их актуальности.

⚠ Если активированы оба параметра «Балансировка по метрикам» и «Соиспользование сессий», то проверяется параметр «Предпочитать соиспользование сессий вместо балансировки». В зависимости от его значения новая сессия либо будет направлена на ту же ноду, либо на наименее нагруженную.

ⓘ Если метрики с какой-либо из нод не получены или стали неактуальны, такая нода будет переведена в режим техобслуживания, а соответствующее событие об этом будет отражено в журнале «Универсального диспетчера» `/var/log/termidesk/termidesk.log`.
Следующие события, связанные с механизмом балансировки, регистрируются в журнале фонда метапоставщика:

- достижение максимальной нагрузки ноды: «Значение индекса нагрузки достигло предела в 10000 slv. Узел <IP-адрес> не будет принимать новых пользователей до тех пор, пока нагрузка не снизится»;
- выбор наименее загруженной ноды (событие регистрируется для уровня DEBUG): «Пользователь будет перенаправлен на этот узел: <IP-адрес>, т.к. он наименее загружен»;
- вход пользователя на ноду: «Пользователь <Имя пользователя> успешно вошел в систему». Ограничение: в журнале РМ отражаются события входа всех пользователей, добавленных в фонд метапоставщика и подключившихся к одной ноде. Например, если в фонд добавлена группа с пользователями «user1» и «user2», тогда, несмотря на то, что пользователи получат разные РМ при подключении к одной ноде (назначенной ВМ), событие подключения «user2», присоединившегося позже, также зарегистрируется в журнале РМ «user1».

Из очереди балансировки исключаются поставщики ресурсов и фонды, находящиеся в режиме техобслуживания.

4.10 . Добавление автономной машины как поставщика ресурсов

Автономная машина - это машина (физическая или виртуальная), которая является постоянной (статической) и не пересоздается для пользователей. То есть пользователи всегда подключаются к одной и той же машине.

Для подключения к автономной машине могут использоваться протоколы:

- RDP;
- TERA;
- Loudplay.

> Для работы подключения в BPM должны быть установлены соответствующие пакеты поддержки (см. подраздел **Подготовка базового BPM**).
> Ранее поставщик активировался через экспериментальный параметр `experimental.provider.physmachine.enabled`, однако, начиная с версии Termidesk 5.1 активация данного параметра не требуется.

> В ОС автономной машины должен быть установлен компонент «Агент виртуального рабочего места» для регистрации РМ в Termidesk.

Для добавления поставщика ресурсов следует перейти в «Компоненты - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка «Автономные машины».

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 15).

Таблица 15 – Данные для добавления автономной машины как поставщика ресурсов

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

4.11 . 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 следует перейти в «Компоненты - Поставщики ресурсов» и нажать на экранную кнопку **[Создать]**, выбрать из выпадающего списка «OpenStack Platform».

Далее 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. Значение по умолчанию: «5000»
«Путь»	Опциональная составляющая URI
«Использовать SSL»	Управление использованием протокола SSL. Значение по умолчанию: «Нет»
«Проверять SSL»	Управление режимом строгой проверки SSL. Значение по умолчанию: «Нет»
«Интерфейс доступа»	Идентификатор интерфейса доступа Openstack. Значение по умолчанию: «public»
«Домен»	Идентификатор домена Openstack
«Пользователь»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления в Openstack
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/openstack/»
«Количество одновременно создаваемых ВМ»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью «Интервал проверок кэша рабочих мест» (см. подраздел **Общие системные параметры Termidesk**). Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10», в параметре «Интервал проверок кэша рабочих мест» задано «19». Тогда за одну проверку (каждые 19 секунд) будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»
«Количество одновременно удаляемых ВМ»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»

Параметр	Описание
«Таймаут»	Максимальное время ожидания (в секундах) отклика от Openstack. Значение по умолчанию: «15»

4.12 . Режим техобслуживания поставщика ресурсов

Режим техобслуживания предназначен для проведения плановых регламентных или аварийных работ поставщика ресурсов. В режиме техобслуживания Termidesk не использует поставщика ресурсов для размещения фондов РМ.

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 27). Затем подтвердить включение режима (см. Рисунок 28).

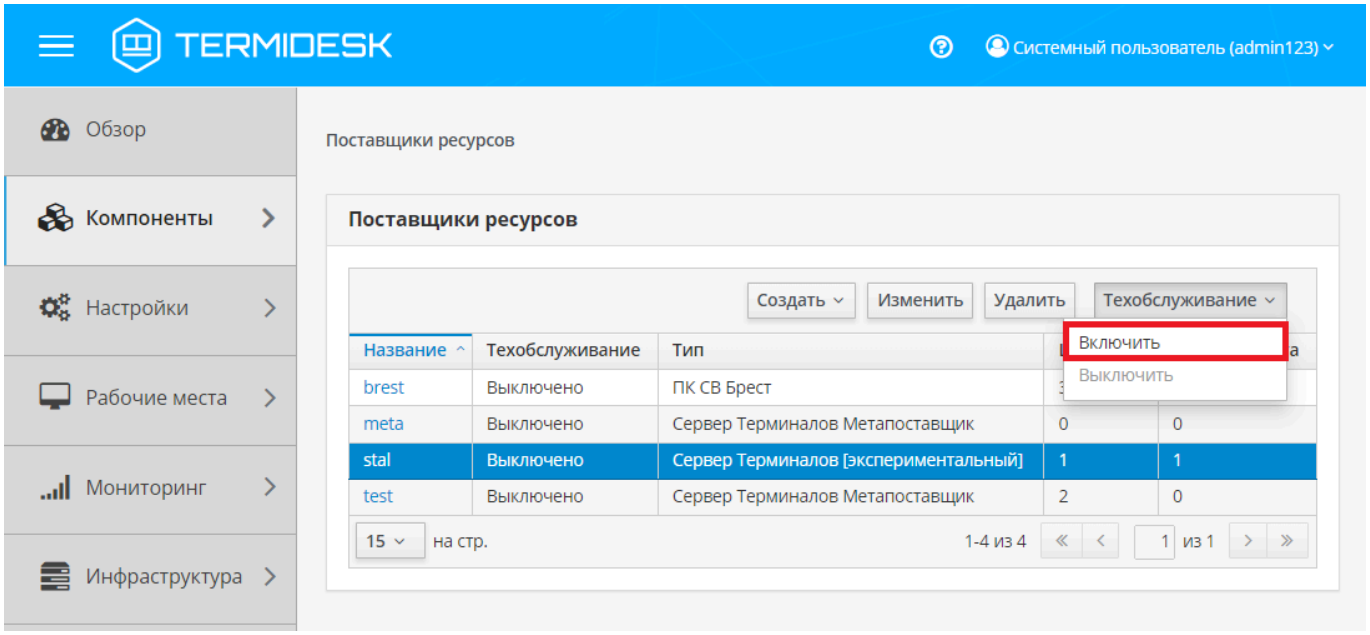

Рисунок 27 – Включение режима техобслуживания поставщика ресурсов

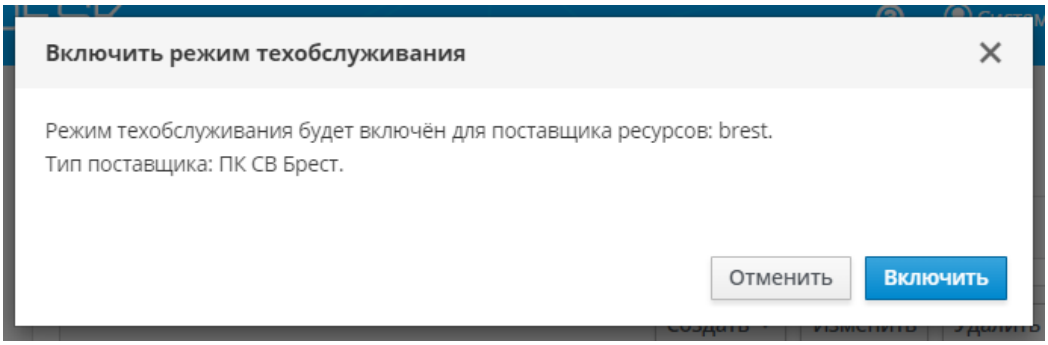

Рисунок 28 – Подтверждение включения режима техобслуживания

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 для размещения фондов РМ.

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;
- ALD Pro;
- SAML;
- IP-аутентификация;
- MS AD или LDAP;
- RADIUS;
- OIDC.

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 **[Создать]** 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 [Изменить] (см. Рисунок 29).

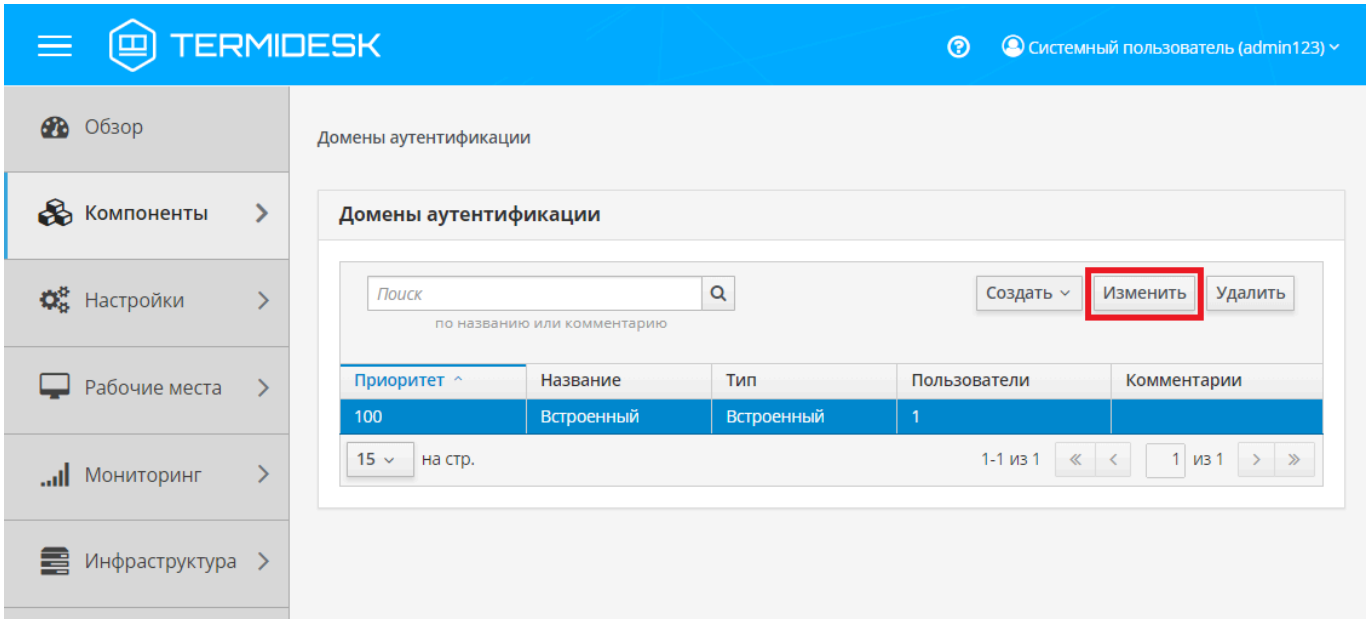

Рисунок 29 – Окно выбора домена аутентификации для редактирования

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

⚠ 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 добавления аутентификации через FreeIPA администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «FreeIPA». Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 17).

ⓘ Termidesk поддерживает авторизацию пользователей, находящихся во вложенных доменных группах FreeIPA.

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

Параметр	Описание
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk. Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: ▪ «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; ▪ «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; ▪ «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; ▪ «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала
«Сервисный аккаунт»	Название сервисного аккаунта, созданного в службе каталогов FreeIPA
«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. Пример: ▪ в случае стандартного хранения файла: «/etc/opt/termidesk-vdi/termidesk.keytab»; ▪ в случае хранения файла в хранилище hvac: «hvac-kv://secret#termidesk-admin/keytabs/termidesk (see page 13)». Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Если используется хранилище, то сгенерированный на контроллере домена `keytab`-файл должен быть преобразован к формату BASE64.
«Сервер FreeIPA»	FQDN ресурса, являющегося источником сведений о субъектах и их полномочиях
«Проверка SSL»	Проверка использования SSL

При добавлении второго домена аутентификации необходимо создать новый файл `keytab` и задать ему имя, отличное от уже существующего.
Добавление второго домена аутентификации не отличается от добавления первого.

Для возможности подключения двухфакторной аутентификации (2FA) 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 **[Создать]** появятся новые домены аутентификации:

- «FreeIPA (2FA, эксперим.)» - позволяет всем пользователям проходить двухфакторную аутентификацию;
- «FreeIPA (2FA, нативн., эксперим.)» - пользователям требуется вручную отправлять QR-код для настройки двухфакторной аутентификации.

Двухфакторная аутентификация доступна только при входе в Termidesk через веб-интерфейс. Для ее прохождения необходимо установить приложение `FreeOTP Authenticator` на мобильные устройства пользователей.

> 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 Pro

Для добавления аутентификации через ALD Pro администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «ALD Pro». Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 18).

Таблица 18 – Данные для добавления аутентификации через ALD PRO

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. Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)

Параметр	Описание
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: ▪ «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; ▪ «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; ▪ «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; ▪ «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала
«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. Пример: ▪ в случае стандартного хранения файла: «/etc/opt/termidesk-vdi/termidesk.keytab»; ▪ в случае хранения файла в хранилище hvac: «hvac-kv://secret#termidesk-admin/keytabs/termidesk». Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Если используется хранилище, то сгенерированный на контроллере домена `keytab`-файл должен быть преобразован к формату BASE64.
«Сервер ALD Pro»	IP-адрес или FQDN ресурса, являющегося источником сведений о субъектах и их полномочиях. Можно указать до пяти ресурсов, разделенных символом «;». Ресурсы будут использоваться в указанном порядке: обращение к следующему будет выполняться при недоступности предыдущего
«Проверка SSL»	Проверка использования SSL

При добавлении второго домена аутентификации необходимо создать новый файл `keytab` и задать ему имя, отличное от уже существующего. Добавление второго домена аутентификации не отличается от добавления первого.
Termidesk поддерживает авторизацию пользователей, находящихся во вложенных доменных группах ALD Pro.

5.4 . Добавление аутентификации через ALD

⚠ Домен аутентификации Astra Linux Directory (ALD) будет удален в Termidesk версии 6.1.

Для добавления аутентификации через ALD администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Astra Linux Directory».

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (see page 0).

Таблица 19 – 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. Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: ▪ «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; ▪ «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; ▪ «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; ▪ «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала
«Сервисный аккаунт»	Название сервисного аккаунта, созданного при добавлении поставщика ресурсов
«Домен»	Идентификатор области Kerberos для аутентификации

Параметр	Описание
«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. Пример: ▪ в случае стандартного хранения файла: «/etc/opt/termidesk-vdi/termidesk.keytab»; ▪ в случае хранения файла в хранилище hvac: «hvac-kv://secret#termidesk-admin/keytabs/termidesk». Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Если используется хранилище, то сгенерированный на контроллере домена `keytab`-файл должен быть преобразован к формату BASE64.
«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

5.5 . 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 аутентификации через SAML администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «SAML».

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 20).

Таблица 20 – 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

Параметр	Описание
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk. Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: ▪ «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; ▪ «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; ▪ «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; ▪ «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала
«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
«Тип Биндинга в ответе»	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**).

5.6 . Добавление аутентификации OIDC

OIDC - это механизм, позволяющий приложению связаться со службой идентификации IdP, получить данные о пользователе и вернуть их обратно в приложение. Таким образом OIDC обеспечивает аутентификацию администраторов и пользователей без необходимости ввода логина и пароля.

Служба идентификации IdP (например, keycloak) должна быть предварительно настроена в инфраструктуре организации для возможности использования OIDC как домена аутентификации.
Поддерживаются следующие типы аутентификации:

- по идентификатору и секрету. В этом случае используются параметры «Client ID» и «Client Secret», заданные в службе идентификации IdP;
- по подписанному JWT-токену. В этом случае используются параметры «Client ID» и «Signed Jwt», заданные в службе идентификации IdP. Закрытый ключ, использующийся для подписи JWT-токена, должен быть загружен на узлы «Универсального диспетчера» («Портал администратора», «Портал пользователя»).

Для добавления домена аутентификации OIDC следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Аутентификация через OIDC».
Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 21).
Для сохранения параметров конфигурации использовать экранную кнопку **[Сохранить]**.

Таблица 21 – Данные для добавления аутентификации через OIDC

Параметр	Описание
«Название»	Параметр обязателен для заполнения. 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»	Параметр обязателен для заполнения. Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk. Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)

Параметр	Описание
«Субъекты»	Параметр обязателен для заполнения. Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: ▪ «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; ▪ «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; ▪ «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; ▪ «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала
«Client ID»	Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Уникальный идентификатор приложения, полученный от службы идентификации IdP. Пример: «openid-test-cl»
«Client secret»	Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Ключ приложения, полученный от службы идентификации IdP. Параметр должен быть пустым, если задан параметр «Приватный Ключ»
«Приватный Ключ»	Путь к закрытому ключу, использующемуся для подписи JWT-токена. Закрытый ключ, используемый в службе идентификации IdP, должен быть добавлен на сервер Termidesk. Для этого: ▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`; ▪ назначить владельцем файла пользователя `termidesk`: `sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.key` Пример: «/etc/opt/termidesk-vdi/client.key»
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Требуется использовать статические данные (префикс `hvac-kv`). Пример: «hvac-kv://secret#termidesk-admin/oidc/»

Параметр	Описание
«Authorization endpoint»	Параметр обязателен для заполнения. URL-адрес авторизации службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/auth»
«Logout endpoint»	Параметр обязателен для заполнения. URL-адрес получения информации о завершении сессии пользователя от службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/logout»
«Token endpoint»	Параметр обязателен для заполнения. URL-адрес получения токена службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/token»
«Userinfo endpoint»	Параметр обязателен для заполнения. URL-адрес получения информации о пользователе от службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/userinfo»
«JWKS URI»	URL-адрес получения сертификатов службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/certs»
«Scope»	Набор областей действия, поддерживаемый в службе идентификации IdP. Области действия определяются спецификацией протокола OAuth 2.0. Неполный список возможных значений (указываются через пробел): ▪ «openid» (обязательное значение для OIDC) - запуск аутентификации с использованием OIDC; ▪ «profile» - доступ к профилю пользователя; ▪ «email» - доступ к адресу электронной почты пользователя; ▪ «offline_access» - обновление токена доступа без необходимости повторной аутентификации; ▪ «groups» - доступ к списку ролей пользователя. Значение по умолчанию: «openid email profile groups». Если нужно указать другой набор значений, следует убедиться, что он поддерживается используемой службой идентификации IdP
«Атрибут имени пользователя»	Имя атрибута, в котором хранится имя пользователя (логин) в службе идентификации IdP. Значение по умолчанию: «email»
«Проверка SSL»	Проверка использования SSL

5.7 . Добавление IP-аутентификации

Домен «IP аутентификация» позволяет определять назначение прав на основе сетевых адресов. Для добавления IP-аутентификации администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «IP аутентификация».

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

Таблица 22 – 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. Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: ▪ «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; ▪ «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; ▪ «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; ▪ «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала
«Разрешить проксирование»	Разрешить субъектам доставку PM, находящихся за прокси-сервером

5.8 . Добавление аутентификации через MS AD (LDAP)

5.8.1 . Перечень параметров для добавления домена аутентификации MS AD (LDAP)

Для добавления аутентификации MS AD (LDAP) администратору Termidesk следует перейти «Компоненты - Домены аутентификации», а затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «MS Active Directory (LDAP)».

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 23).

Таблица 23 – 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. Параметр используется для поиска аналогичного домена «Универсального диспетчера», поэтому должен быть одинаковым как на портале «Агрегатор» (при его использовании), так и на «Универсальном диспетчере». Поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: ▪ «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; ▪ «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; ▪ «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; ▪ «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала
«Сервер LDAP»	IP-адрес или доменное имя сервера службы каталогов, являющегося источником сведений о субъектах и их полномочиях
«Порт»	TCP-порт, на котором запущена служба каталогов. Возможные стандартные значения: ▪ «389» (по умолчанию). Используется, если доступ к службе каталогов осуществляется по протоколу LDAP; ▪ «636». Используется, если доступ к службе каталогов осуществляется по протоколу LDAPS; ▪ «3268». Альтернативный порт. Используется, если доступ к службе каталогов осуществляется по протоколу LDAP; ▪ «3269». Альтернативный порт. Используется, если доступ к службе каталогов осуществляется по протоколу LDAPS. Для ускорения поиска пользователей в службе каталогов рекомендуется указывать альтернативный порт
«Использовать SSL»	Использовать защищенное соединение при взаимодействии со службой каталогов

Параметр	Описание
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/msad/»
«Учетная запись»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Учетная запись в формате Distinguished Name (DN) в домене MS AD (LDAP), используемая для подключения к службе каталогов. Пример: «CN=admin,OU=user,DC=test,DC=desk»
«Пароль учетной записи»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий полномочия объекта для подключения к службе каталогов
«Таймаут»	Время ожидания (в секундах) ответа от службы каталогов. Значение по умолчанию: «10»
«Base DN»	Корень поиска в службе каталогов в формате DN. Параметру следует задавать значение, соответствующее записи верхнего уровня в иерархии службы каталогов (без указания OU). Вводимое значение не должно содержать пробелов: ▪ в начале и конце строки; ▪ рядом с разделителями (запятыми); ▪ в элементах пути (например, «DC=company name,DC=de»). Пример: «DC=test,DC=desk»
«Имя класса пользователя»	Атрибут класса пользователя в службе каталогов. Для корректного заполнения данного поля необходимо указать значение «person»
«Атрибут идентификатора пользователя»	Атрибут уникального имени или идентификатора пользователя в службе каталогов. Для корректного заполнения данного поля необходимо указать: ▪ значение «name», если активирован параметр «Использовать PKINIT»; ⚠ Атрибут идентификатора пользователя задается с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Например, значение «name» для механизма аутентификации Kerberos PKINIT указывается в том случае, если сертификат для подключения выдан на имя пользователя. ▪ значение «userPrincipalName», если в параметре «Формат имени пользователя для аутентификации» используется «userPrincipalName»; ▪ значение «SamAccountName» в остальных случаях
«Список атрибутов пользователя»	Список атрибутов, содержащий уникальные данные пользователя, разделенные запятыми. Для корректного заполнения данного поля необходимо указать значение: ▪ «userPrincipalName», если в параметре «Формат имени пользователя для аутентификации» используется «userPrincipalName»; ▪ «name», если в параметре «Формат имени пользователя для аутентификации» используется «sAMAccountName»

Параметр	Описание
«Формат имени пользователя для аутентификации»	Формат имени пользователя, заданный в службе каталогов. ⚠ Если на пользовательской рабочей станции установлен компонент «Клиент» версии, младше 6.0, то он будет поддерживать только формат «sAMAccountName». Возможные значения: ▪ «sAMAccountName» (по умолчанию) - имя пользователя без доменной части; ▪ «userPrincipalName» - имя пользователя с доменной частью
«Имя атрибута группы»	Атрибут принадлежности к группе в службе каталогов. Для корректного заполнения данного поля необходимо указать значение «group»
«Атрибут имени группы»	Атрибут идентификатора группы, к которой относится субъект в службе каталогов. Для корректного заполнения данного поля необходимо указать: ▪ значение «distinguishedname», если включены параметры «Использовать рекурсивный поиск групп» или «Использовать обратный порядок проверки членства пользователей»; ▪ значение «name», если активирован параметр «Использовать PKINIT»; ⚠ Атрибут имени группы задается с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Например, значение «name» для механизма аутентификации Kerberos PKINIT указывается в том случае, если сертификат для подключения выдан на имя пользователя. ▪ значение «cn» в остальных случаях. Если используется значение «distinguishedname», то при добавлении группы в домен аутентификации по пути «Компоненты - Домены аутентификации - Наименование домена - Группы» нужно указывать длинные имена групп, например: «CN=RootGroup,CN=Users,DC=test,DC=desk». Если используется значение «cn», то нужно указывать 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. Возможные значения: ▪ «Да» - использовать рекурсивный поиск; ▪ «Нет» (по умолчанию) - не использовать рекурсивный поиск

Параметр	Описание
«Использовать обратный порядок проверки членства пользователей»	Проверка соответствия членства пользователя в группах службы каталогов членству в группах домена аутентификации. Для работы функционала необходимо, чтобы был задан параметр «Атрибут имени группы». Этот параметр нужно включить при большом количестве групп непосредственно на службе каталогов MS AD. В этом случае сначала будет проверяться вхождение пользователя в группы домена аутентификации (в том числе рекурсивно), затем будет происходить проверка найденных групп в службе каталогов MS AD. 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». Возможные значения: ▪ «Да» - использовать обратный порядок; ▪ «Нет» (по умолчанию) - не использовать обратный порядок
«Использовать PKINIT»	Использовать механизм аутентификации Kerberos PKINIT при аутентификации пользователя. PKINIT - механизм, позволяющий использовать сертификаты X.509 в качестве метода аутентификации. Предполагается, что механизм аутентификации Kerberos PKINIT настроен в инфраструктуре организации и пользователю выданы соответствующие сертификаты и ключи для подключения (персональный сертификат, закрытый ключ к нему и корневой сертификат ЦС, на котором выпущен персональный сертификат). При активации механизма аутентификации Kerberos PKINIT нужно указать актуальный порт в параметре «Порт PKINIT», а также указать нужные значения параметров «Атрибут имени группы» и «Атрибут идентификатора пользователя». Возможные значения: ▪ «Да» - использовать механизм; ▪ «Нет» (по умолчанию) - не использовать механизм
«Порт PKINIT»	TCP/UDP порт, на котором запущена служба Kerberos. Значение по умолчанию: «88»
«Использовать Kerberos»	Использовать механизм аутентификации по билету Kerberos. Предполагается, что механизм аутентификации по билету Kerberos настроен в инфраструктуре организации (см. подразделы **Получение и добавление файла keytab для Kerberos-аутентификации** и **Настройка пользовательской рабочей станции для Kerberos-аутентификации**). ⚠ Для работы аутентификации по билету Kerberos на терминальных серверах MS RDS, необходимо выполнить дополнительную настройку «Сессионного агента», задав значения параметрам `MASTER_KEY` и `URL_BALANCER` в его конфигурационном файле. Если используется аутентификация Kerberos, то нужно заполнить параметр «Путь до Keytab». Возможные значения: ▪ «Да» - использовать механизм; ▪ «Нет» (по умолчанию) - не использовать механизм
«Путь до Keytab»	Путь к файлу с ключами для сервисного аккаунта. В зависимости от места хранения файла следует указать путь в формате: ▪ в случае стандартного хранения файла: «/etc/opt/termidesk-vdi/termidesk.keytab»; ▪ в случае хранения файла в хранилище hvac: «hvac-kv://secret#termidesk-admin/keytabs/kerberos». Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. ⚠ Если используется хранилище, то сгенерированный на контроллере домена `keytab`-файл должен быть преобразован к формату BASE64.

5.8.2 . Получение и добавление файла keytab для Kerberos-аутентификации

Для получения `keytab`-файла на контроллере домена MS AD нужно:

- заранее создать учетную запись (сервисный аккаунт), от имени которой будет работать служба. Для создания учетной записи нужно на контроллере домена перейти в стандартную утилиту «Active Directory - пользователи и компьютеры»;
- в свойствах учетной записи во вкладке «Account» активировать параметр «This account supports Kerberos AES 256 bit encryption» (см. Рисунок 30);

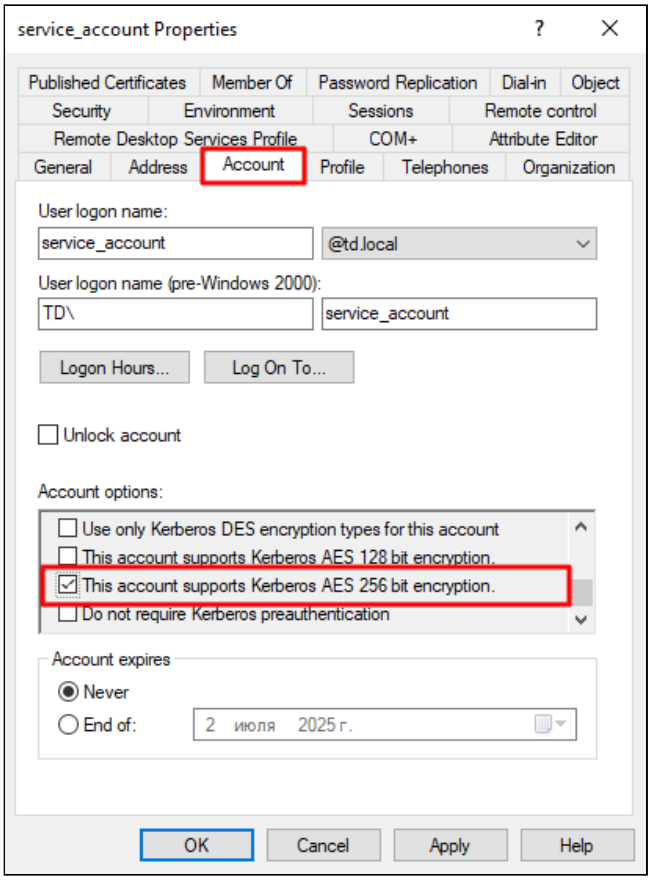

Рисунок 30 – Активация параметра «This account supports Kerberos AES 256 bit encryption»

- открыть интерфейс командной строки PowerShell и выполнить команду добавления службы для сервисного аккаунта:

```
setspn -A HTTP/disp.termidesk.local service_account
```

где:

`service_account` - наименование сервисного аккаунта;

- для просмотра списка служб сервисного аккаунта можно воспользоваться командой:

```
setspn -L service_account
```

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

```
ktpass -princ HTTP/disp.termidesk.local@TERMIDESK.LOCAL -mapuser
service_account@TERMIDESK.LOCAL -pass <пароль_сервисного_аккаунта> -ptype
KRB5_NT_PRINCIPAL -out termidesk-msad.keytab -crypto AES256-SHA1
```

где:

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

`service_account@TERMIDESK.LOCAL` - наименование сервисного аккаунта;

`-out termidesk-msad.keytab` - сохранение в файл `termidesk-msad.keytab`;

`-crypto AES256-SHA1` - алгоритм для преобразования `keytab`-файла.

⚠ Алгоритм преобразования `keytab`-файла следует выбирать согласно установленным политикам безопасности MS AD.

Полученный файл `termidesk-msad.keytab` следует передать на соответствующий узел для хранения. Файл может быть сохранен в файловой системе узла Termidesk или в хранилище OpenBao.

Для передачи файла на целевой узел нужно выполнить команду:

```
scp C:\Windows\System32\termidesk-msad.keytab localuser@192.0.2.30:termidesk-msad.keytab
```

где:

`C:\Windows\System32\termidesk-msad.keytab` - путь к `keytab`-файлу;

`localuser` - имя пользователя целевого узла;

`192.0.2.30` - IP-адрес целевого узла.

После передачи файла необходимо выполнить ряд действий в зависимости от выбранного хранилища.

При хранении файла в файловой системе узла Termidesk:

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

```
sudo mv /home/user/termidesk-msad.keytab /etc/opt/termidesk-vdi/
```

- сделать владельцем этого файла пользователя `termidesk`:

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

- перезапустить службу `termidesk-vdi`:

```
sudo systemctl restart termidesk-vdi
```

При хранении файла в хранилище OpenBao:

- запустить интерпретатор Python:

```
sudo python3
```

- перевести файл в формат base64:

```
1  import base64 with open('/home/user/termidesk-msad.keytab', 'rb') as file:
   keytab_bytes = file.read() keytab_base64 =
   base64.b64encode(keytab_bytes).decode('utf-8') keytab_base64
```

где:

`/home/user/termidesk-msad.keytab` - путь к `keytab`-файлу;

- сохранить результат выполнения команды в хранилище OpenBao:

```
bao kv put secret/termidesk/ldap keytab='BQIAAABGAAIAC1VTVVA0MDcuTEFOAARIVFRQABJ0ZXJtaWRlc
2subXlkb21h aW4AAAABAAAAAAUAFwAQhKQHwhUvWGEJk92QgI/tNA=='
```

где:

`termidesk` - значение переменной `SECRETS_OPENBAO_TERMIDESK_PATH`, заданной в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf`;

`ldap` - путь к хранилищу OpenBao, где следует сохранить результат выполнения команды.

5.8.3 . Настройка пользовательской рабочей станции для Kerberos-аутентификации

Для корректной аутентификации пользовательская рабочая станция должна быть введена в соответствующий домен аутентификации Kerberos, используемый в ферме Termidesk и указанный в «Портале администратора».

По умолчанию билет Kerberos выдается автоматически при аутентификации пользователя в системе. Однако, если билет не был выдан автоматически, нужно:

- просмотреть список билетов:

```
klist
```

- получить билет Kerberos:

```
kinit -f termidesk@TERMIDESK.LOCAL
```

где:

`termidesk@TERMIDESK.LOCAL` - учетная запись, для которой запрашивается билет.

Kerberos-аутентификация через веб-браузер требует настройки параметров безопасности в зависимости от используемой ОС и типа браузера.

На пользовательской рабочей станции с ОС Microsoft Windows:

- при использовании веб-браузера, основанного на Chromium нужно настроить параметры безопасности браузера для зоны, в которой находится сервер Termidesk. Для этого:
  - перейти «Панель управления - Свойства браузера - Безопасность»;

- в разделе «Выберите зону для параметры ее параметров безопасности» выбрать зону «Местная интрасеть», нажать экранную кнопку **[Сайты]**;
- в окне «Местная интрасеть» нажать экранную кнопку **[Дополнительно]**;
- в поле «Добавить в зону следующий узел» ввести FQDN сервера Termidesk, нажать экранную кнопку [Добавить] (см. Рисунок 31);

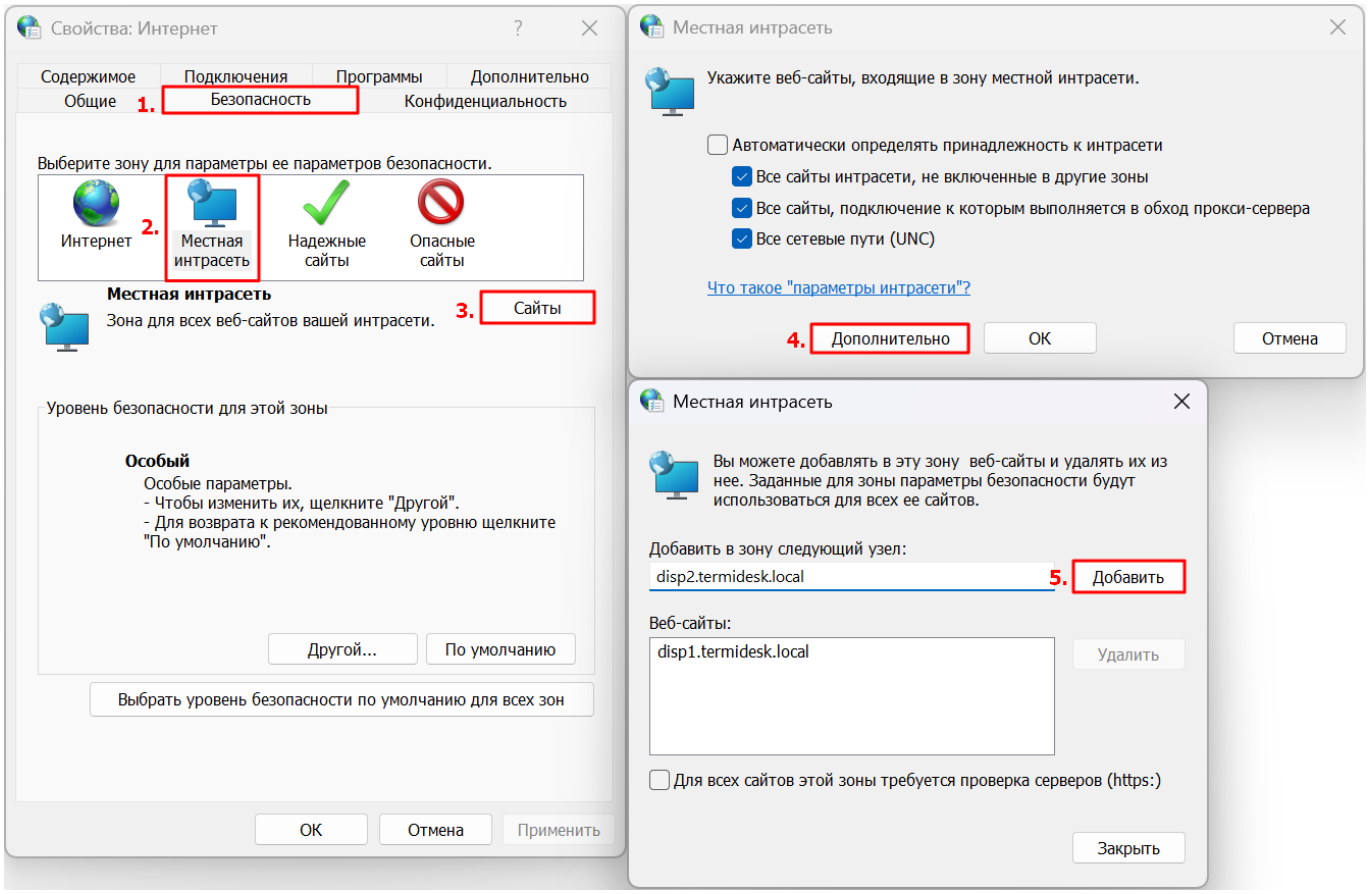

Рисунок 31 – Добавление FQDN компонента «Универсальный диспетчер» в зону «Местная интрасеть»

- при использовании в ОС Microsoft Windows веб-браузера Mozilla Firefox нужно:
  - в адресной строке ввести `about:config`;
  - присвоить соответствующие значения параметрам, перечисленным в таблице (см. Таблица 24).

Таблица 24 – Данные для настройки Kerberos-аутентификации через веб-браузер Mozilla Firefox в ОС Microsoft Windows

Параметр	Значение
`network.negotiate-auth.allow-proxies`	`True`
`network.negotiate-auth.delegation-uris`	`.termidesk.local`
`network.negotiate-auth.trusted-uris`	`.termidesk.local`

На пользовательской рабочей станции с ОС Astra Linux Special Edition:

- для настройки веб-браузера Chromium нужно:
  - в файл `/etc/chromium/policies/managed/policies.json` добавить строки:

```
{
    "AuthServerAllowlist": "*.termidesk.local" ,
    "AuthNegotiateDelegateAllowlist": "*.termidesk.local"
}
```

где:

`*.termidesk.local` - имя домена, для которого применяется Kerberos-аутентификация;

- для настройки веб-браузера Яндекс.Браузер нужно:
  - создать каталог `/etc/opt/yandex/browser/policies/managed`:

```
mkdir -p /etc/opt/yandex/browser/policies/managed
```

  - создать файл `/etc/opt/yandex/browser/policies/managed/policies.json` следующего содержания:

```
{
    "AuthServerAllowlist": "*.termidesk.local",
    "AuthNegotiateDelegateAllowlist": "*.termidesk.local"
}
```

- для настройки веб-браузера Mozilla Firefox нужно:
  - в адресной строке ввести `about:config`;
  - присвоить соответствующие значения параметрам, перечисленным в таблице (см. Таблица 25).

Таблица 25 – Данные для настройки Kerberos-аутентификации через веб-браузер Mozilla Firefox в ОС Astra Linux Special Edition

Параметр	Значение
`network.negotiate-auth.allow-proxies`	`True`
`network.negotiate-auth.delegation-uris`	`.termidesk.local`
`network.negotiate-auth.trusted-uris`	`.termidesk.local`

5.9 . 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 администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Radius».

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 26).

Таблица 26 – 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. Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: ▪ «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; ▪ «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; ▪ «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; ▪ «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала
«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
```

5.10 . Добавление аутентификации через внутреннюю БД

⚠ Начиная с Termidesk версии 5.1 использование функционала, подключаемого через плагин расширения, исключено.

5.11 . Действия над группами в домене аутентификации

Группы – перечень объектов домена аутентификации, определяющих разрешения пользователей на доступ к фондам BPM. Перечень групп, доступных для добавления в Termidesk, запрашивается у домена аутентификации.

Доступны следующие действия над группами домена аутентификации:

- создание - добавление существующей в службе каталогов группы в Termidesk;
- редактирование;
- удаление;
- просмотр сведений таблицы «Группы».

> ⓘ Редактирование и удаление групп в домене аутентификации в «Портале администратора» Termidesk не приводит к каким-либо изменениям объекта в службе каталогов.

Для добавления группы следует перейти «Компоненты - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне в таблице «Группы» нажать экранную кнопку **[Создать]**. Для добавления будут доступны два типа групп:

- «Группа» (см. Рисунок 32) - стандартная группа, созданная в службе каталогов и которая будет добавлена в Termidesk;
- «Метагруппа» (см. Рисунок 33) - группа, объединяющая несколько стандартных групп в Termidesk.

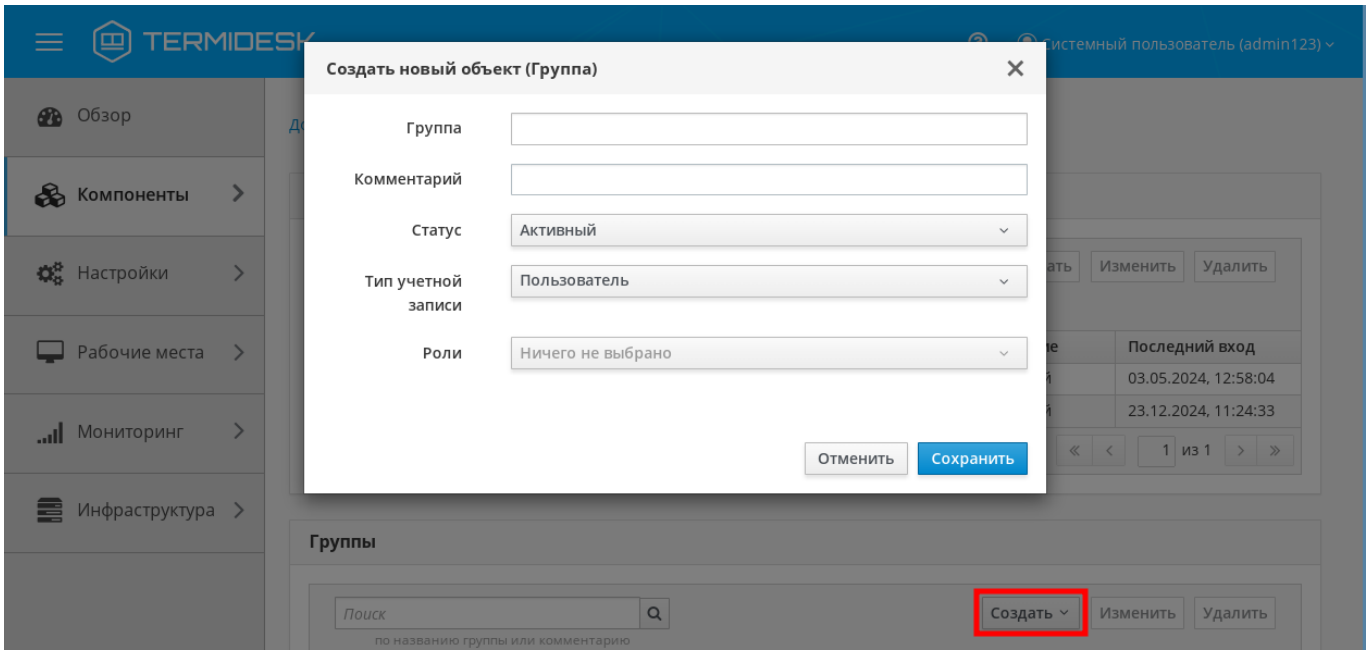

Рисунок 32 – Окно добавления группы домена аутентификации

Для добавления группы администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 27).

Таблица 27 – Данные для добавления группы домена аутентификации

Параметр	Описание
«Группа»	Наименование группы, полученное от домена аутентификации. Для выбора группы из списка доступных необходимо начать ввод ее наименования
«Диапазон IP»	Параметр доступен только для домена аутентификации с типом «IP аутентификация». IP-адрес или IP-адреса группы. Может быть указан IP-адрес, диапазон IP-адресов, перечень IP-адресов. Пример: ▪ «192.0.2.2»; ▪ «192.0.2.0/24»; ▪ «192.0.2.1/24, 192.0.2.5/24, 192.0.2.10/24»; ▪ «192.0.2.2-192.0.2.253»
«Комментарий»	Информационное сообщение, используемое для описания группы
«Статус»	Характеристика состояния субъектов группы при доступе к фонду BPM. Доступные значения: ▪ «Активный» - субъекты группы могут аутентифицироваться в Termidesk; ▪ «Неактивный» - субъекты группы не могут аутентифицироваться в Termidesk; ▪ «Временно заблокирован» - субъекты группы не могут аутентифицироваться в Termidesk. Статус присваивается также по истечении попыток аутентификации, определенных в параметрах «Максимум попыток входа Администраторов», «Максимум попыток входа Персонала», «Максимум попыток входа Пользователей» на странице «Настройки - Системные параметры - Безопасность» (см. подраздел **Параметры безопасности Termidesk**)
«Тип учетной записи»	Служебные функции субъектов группы при доступе к Termidesk. Доступные значения параметра: ▪ «Пользователь» - субъекты группы не будут иметь доступ к порталу администратора. При выборе этого значения параметр «Роли» будет пустым; ▪ «Персонал» - субъекты группы будут иметь доступ к странице «Обзор» и будут обладать набором разрешений, определенных служебными функциями. При выборе этого значения в параметре «Роль» можно выбрать одно или несколько значений классов администратора, созданных на странице «Настройки - Управление ролями» (см. подраздел **Назначение служебных функций администраторам**); ▪ «Администратор» - субъекты группы будут иметь полный доступ к порталу администратора. При выборе этого значения параметр «Роли» будет пустым
«Роли»	Назначение служебных функций пользователям группы. Доступность выбора значений зависит от параметра «Тип учетной записи» и того, созданы ли роли на странице «Настройки - Управление ролями»

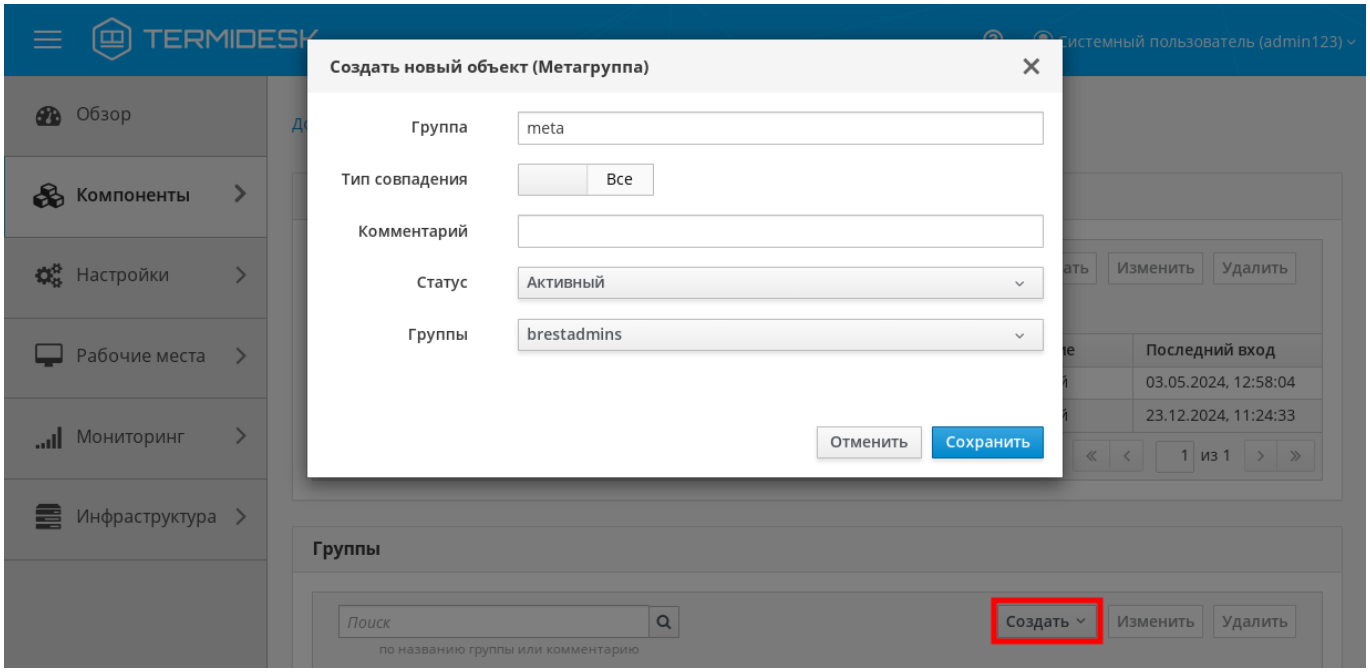

Рисунок 33 – Окно добавления метагруппы домена аутентификации

Для добавления метагруппы администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 28).

Таблица 28 – Данные для добавления метагруппы домена аутентификации

Параметр	Описание
«Группа»	Наименование группы
«Диапазон IP»	Параметр доступен только для домена аутентификации с типом «IP аутентификация». IP-адрес или IP-адреса группы. Может быть указан IP-адрес, диапазон IP-адресов, перечень IP-адресов. Пример: ▪ «192.0.2.2»; ▪ «192.0.2.0/24»; ▪ «192.0.2.1/24, 192.0.2.5/24, 192.0.2.10/24»; ▪ «192.0.2.2-192.0.2.253»
«Тип совпадения»	Выбор способа определения принадлежности группы к метагруппе. Доступные значения: ▪ «Любой» - любая из групп, перечисленных в параметре «Группы»; ▪ «Все» (значение по умолчанию) - все группы, перечисленные в параметре «Группы»
«Комментарий»	Информационное сообщение, используемое для описания метагруппы
«Статус»	Характеристика состояния субъектов метагруппы при доступе к фонду BPM. Доступные значения: ▪ «Активный» - субъекты метагруппы могут аутентифицироваться в Termidesk; ▪ «Неактивный» - субъекты метагруппы не могут аутентифицироваться в Termidesk

Параметр	Описание
«Группы»	Наименования групп, к которым должна примениться метагруппа

Для редактирования группы следует перейти «Компоненты - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне в таблице «Группы» выделить строку с именем пользователя и нажать экранную кнопку **[Изменить]**. В режиме редактирования невозможно изменить идентификатор группы домена аутентификации, поскольку он получен автоматически от службы каталогов.

Для удаления группы используется экранная кнопка **[Удалить]**.

⚠ Группа может быть удалена только в том случае, если в ней нет пользователей. Для удаления группы следует предварительно удалить из нее всех пользователей.

5.12 . Действия над пользователями в домене аутентификации

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

ⓘ Создание учетной записи пользователя в Termidesk выполняется после его первой авторизации на портале Termidesk.

Администратору доступны следующие действия над пользователями внутри домена аутентификации:

- редактирование;
- удаление;
- просмотр сведений.

ⓘ В компоненте «Универсальный диспетчер» предусмотрена возможность автоматической регистрации пользователей, запросивших опубликованные ресурсы через портал «Агрегатора». Для этого нужно, чтобы идентичные группы были добавлены как в доменах аутентификации портала «Агрегатор администратора», так и в доменах аутентификации «Портала администратора» Termidesk. Если пользователь состоит в указанных группах, то после входа на портал «Агрегатора» и запроса ресурсов его учетная запись будет автоматически зарегистрирована для компонента «Универсальный диспетчер», использующегося в ферме Termidesk.
Редактирование и удаление пользователя в домене аутентификации в указанных порталах Termidesk не приводит к каким-либо изменениям объекта в службе каталогов.
Termidesk хранит информацию о назначении прав пользователя в БД, поэтому в случае, если пользователь должен быть исключен из группы администрирования Termidesk, то необходимо удалить пользователя из группы непосредственно в доменной службе каталогов и на стороне Termidesk одновременно.

Для отображения списка пользователей следует перейти «Компоненты - Домены аутентификации». Основные параметры списка приведены в таблице (см. Таблица 29).

Таблица 29 – Параметры списка пользователей

Параметр	Описание
«Логин»	Идентификатор пользователя в домене аутентификации
«Имя»	Отображаемое имя пользователя в Termidesk
«Комментарий»	Информационное сообщение, используемое для описания назначения пользователя
«Тип пользователя»	Тип служебных функций, назначенный пользователю
«Состояние»	Характеристика состояния субъекта при доступе к фонду РМ
«Последний вход»	Временная метка, отражающая момент последней авторизации

Для редактирования информации о пользователе следует в столбце «Название» нажать на наименование домена аутентификации и в открывшемся окне в таблице «Пользователи» выделить строку с именем пользователя, нажать экранную кнопку [Изменить] (см. Рисунок 34).

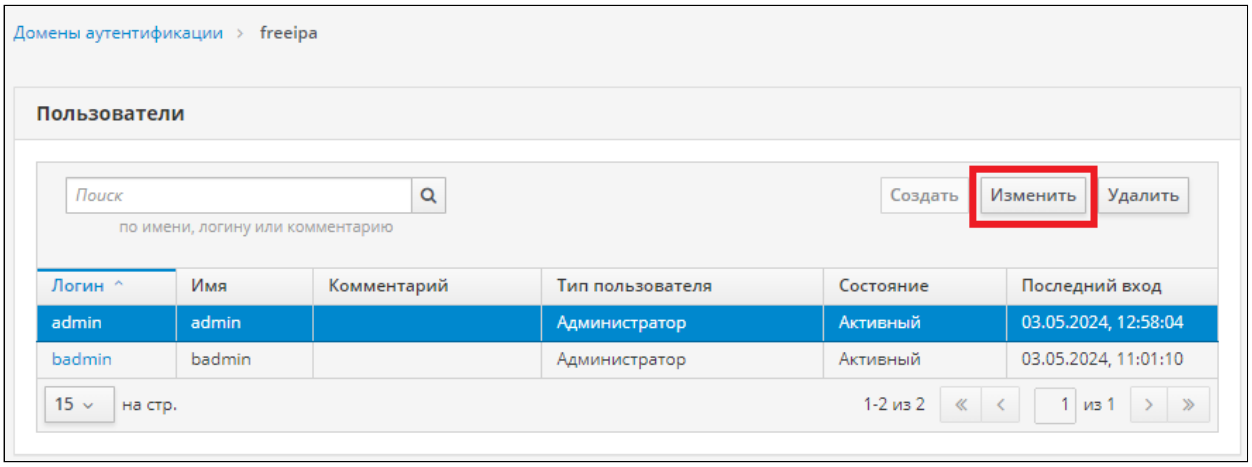

Рисунок 34 – Редактирование пользователя домена аутентификации

Для редактирования пользователя администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 30).

Таблица 30 – Данные для редактирования пользователя домена аутентификации

Параметр	Описание
«Логин»	Идентификатор субъекта в службе каталогов
«Имя»	Отображаемое имя субъекта в Termidesk
«Комментарий»	Информационное сообщение, используемое для описания назначения пользователя

Параметр	Описание
«Статус»	Характеристика состояния субъекта при доступе к фонду РМ. Доступные значения: ▪ «Активный» - субъект может аутентифицироваться в Termidesk; ▪ «Неактивный» - субъект не может аутентифицироваться в Termidesk; ▪ «Временно заблокирован» - субъект не может аутентифицироваться в Termidesk. Статус присваивается также по истечении попыток аутентификации, определенных в параметрах «Максимум попыток входа Администраторов», «Максимум попыток входа Персонала», «Максимум попыток входа Пользователей» на странице «Настройки - Системные параметры - Безопасность» (см. подраздел **Параметры безопасности Termidesk**). Время блокировки определяется параметром «Время блокировки входа» на странице «Настройки - Системные параметры - Общие» (см. подраздел **Общие системные параметры Termidesk**)
«Тип учетной записи»	Служебные функции субъекта при доступе к Termidesk. Значение наследуется от группы, в которую входит пользователь. При этом по умолчанию тип учетной записи устанавливается в значение с более высоким уровнем прав. Пример: если пользователь одновременно состоит в группе с типом учетной записи «Администратор» и группе с типом «Пользователь», то по умолчанию для пользователя будет установлен тип учетной записи «Администратор». Доступные значения параметра: ▪ «Пользователь» - субъект не будет иметь доступ к «Порталу администратора». При выборе этого значения параметр «Роли» будет пустым; ▪ «Персонал» - субъект будет иметь доступ к странице «Обзор» и будет обладать набором разрешений, определенных служебными функциями. При выборе этого значения в параметре «Роль» можно выбрать одно или несколько значений классов администратора, созданных на странице «Настройки - Управление ролями» (см. подраздел **Назначение служебных функций администраторам**); ▪ «Администратор» - субъект будет иметь полный доступ к «Порталу администратора». При выборе этого значения параметр «Роли» будет пустым ⚠ Если пользователь состоит в группе администраторов Termidesk, то ему автоматически будет присвоен тип учетной записи «Администратор» после первой авторизации на портале Termidesk. Для того чтобы пользователь не обладал административными правами, нужно изменить для него параметр «Тип учетной записи» и удалить его из группы администраторов (либо изменить тип группы) Termidesk (см. подраздел **Действия над группами в домене аутентификации**).
«Группы»	Наименования групп, используемых для определения разрешений по доступу к фондам РМ. Список групп пользователя будет получен автоматически от службы каталогов
«Роли»	Назначение служебной функции указанному пользователю. Доступность выбора значений зависит от параметра «Тип учетной записи» и того, созданы ли роли на странице «Настройки - Управление ролями». Назначение параметра «Роли» будет доступно, если «Тип учетной записи» соответствует «Персонал»

Для удаления пользователя из домена аутентификации следует 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]**.

5.13 . Управление аутентификацией на основе адресов сети

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

Для добавления диапазона сети администратору Termidesk следует перейти «Компоненты - Сети», нажать экранную кнопку **[Создать]**, затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 31).

Таблица 31 – 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 **[Изменить]**.

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 РМ.

6 . РАБОЧИЕ МЕСТА

6.1 . Общие сведения о РМ

РМ в общем случае представляет собой гостевую ОС или ОС, установленную на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа.
Сокращение ВРМ относится к технологии VDI, поэтому в рамках документации принято, что ВРМ - это развернутая на ВМ гостевая ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО, доступ к которой реализуется с помощью протокола удаленного доступа. Сокращение будет использоваться там, где описание относится непосредственно к ВРМ.

> ⓘ ВРМ - это частный случай РМ. Терминальный доступ или доступ к опубликованным на сервере терминалов приложениям - это также частный случай РМ.
> Termidesk выполняет подготовку РМ на основе заданных шаблонов. В случае с подготовкой ВРМ Termidesk создает шаблон с префиксом «TDSK», а не из исходных шаблонов базового ВРМ, настроенных администратором на поставщике ресурсов.

Каждый поставщик ресурсов поддерживает свой набор типов шаблонов РМ. Поддерживаемый в Termidesk список типов шаблонов приведен ниже:

- шаблон на основе связанного клона (только для варианта лицензирования Termidesk VDI) - предполагает создание ВРМ из базового образа на платформе виртуализации в режиме инкрементного копирования;
- шаблон на основе полного клона (только для варианта лицензирования Termidesk VDI) - предполагает создание ВРМ из базового образа на платформе виртуализации в режиме полного копирования;
- связанный клон на базе снапшота (только для варианта лицензирования Termidesk VDI) - 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 - предполагают создание РМ на основе терминального доступа или доступа к опубликованным на терминальном сервере приложениям;
- шаблон на основе автономных машин (только для варианта лицензирования Termidesk VDI) - предполагает создание ВРМ на основе шаблона «Автономные машины», созданного для автономной машины.

Для добавления шаблона в веб-интерфейсе Termidesk следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов. Далее в открывшемся окне следует нажать на экранную кнопку **[Создать]**, а затем из выпадающего списка выбрать поддерживаемый в Termidesk способ формирования шаблона РМ.

Созданные шаблоны можно:

- редактировать, для этого необходимо выбрать шаблон, а затем нажать на экранную кнопку **[Изменить]**;
- 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 РМ.

6.2 . Отображение списка РМ из всех фондов

6.2.1 . Отображение списка РМ

Для более эффективного администрирования Termidesk предусмотрено отображение РМ из всех фондов, в том числе назначенных РМ, а также созданных и размещенных в кеше.

Для получения списка необходимо перейти «Рабочие места - Индивидуальные рабочие места» (см. Рисунок 35) или перейти по ссылке «Рабочие места» из функции «Обзор» (см. Рисунок 36). По умолчанию записи в представленном списке (см. Рисунок 37) будут упорядочены согласно столбцу «Дата создания» по убыванию.

ⓘ Подробная информация об управлении состоянием ВМ и ее индикации содержится в подразделе **Управление ВМ в назначенном фонде РМ**, информация по назначению владельца РМ приведена в подразделе **Назначение владельца РМ**.
Терминальные сессии также могут быть удалены экранной кнопкой **[Удалить]**.

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

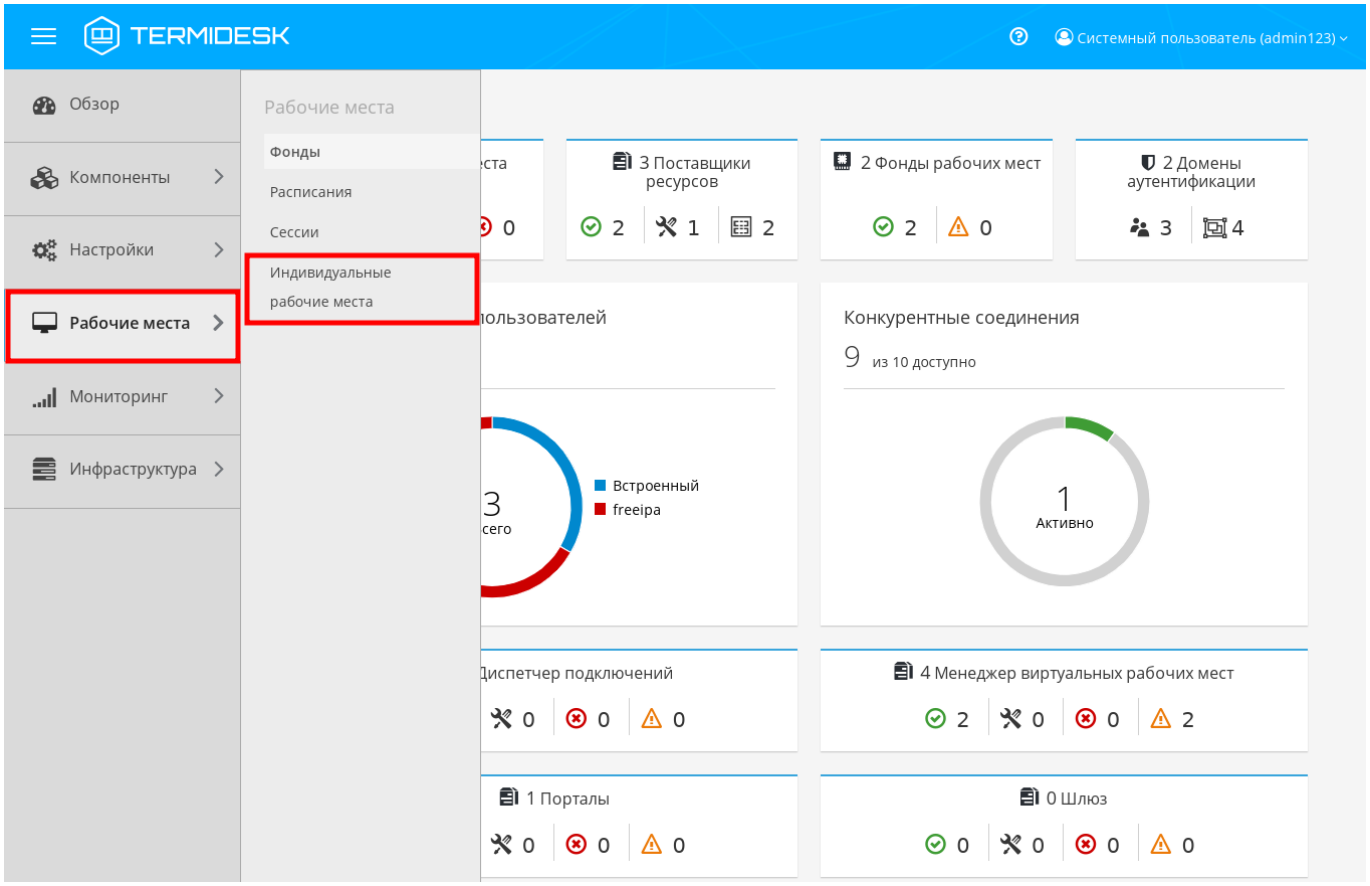

Рисунок 35 – Переход к списку РМ через «Рабочие места - Индивидуальные рабочие места»

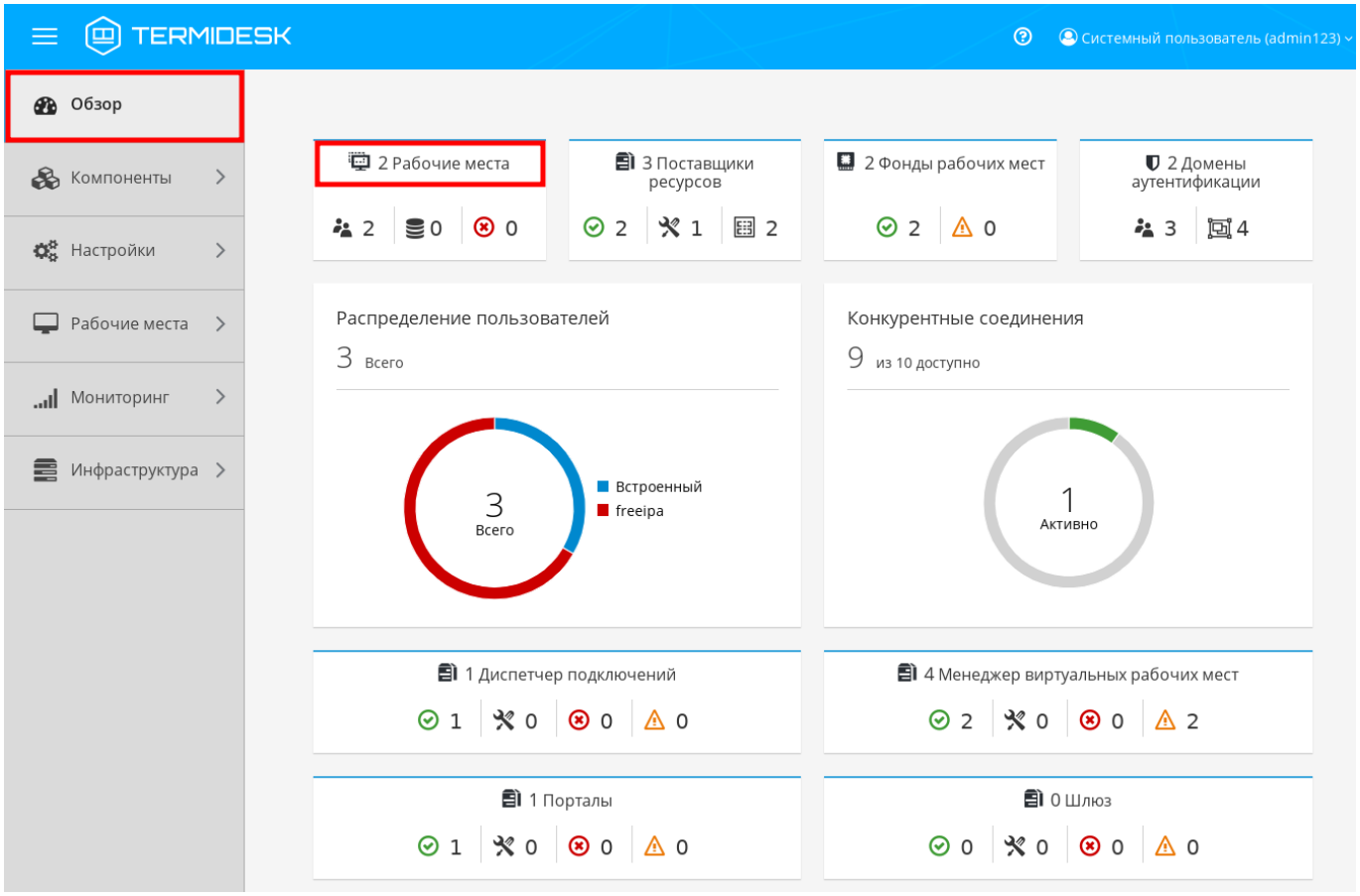

Рисунок 36 – Переход к списку РМ через функцию «Обзор»

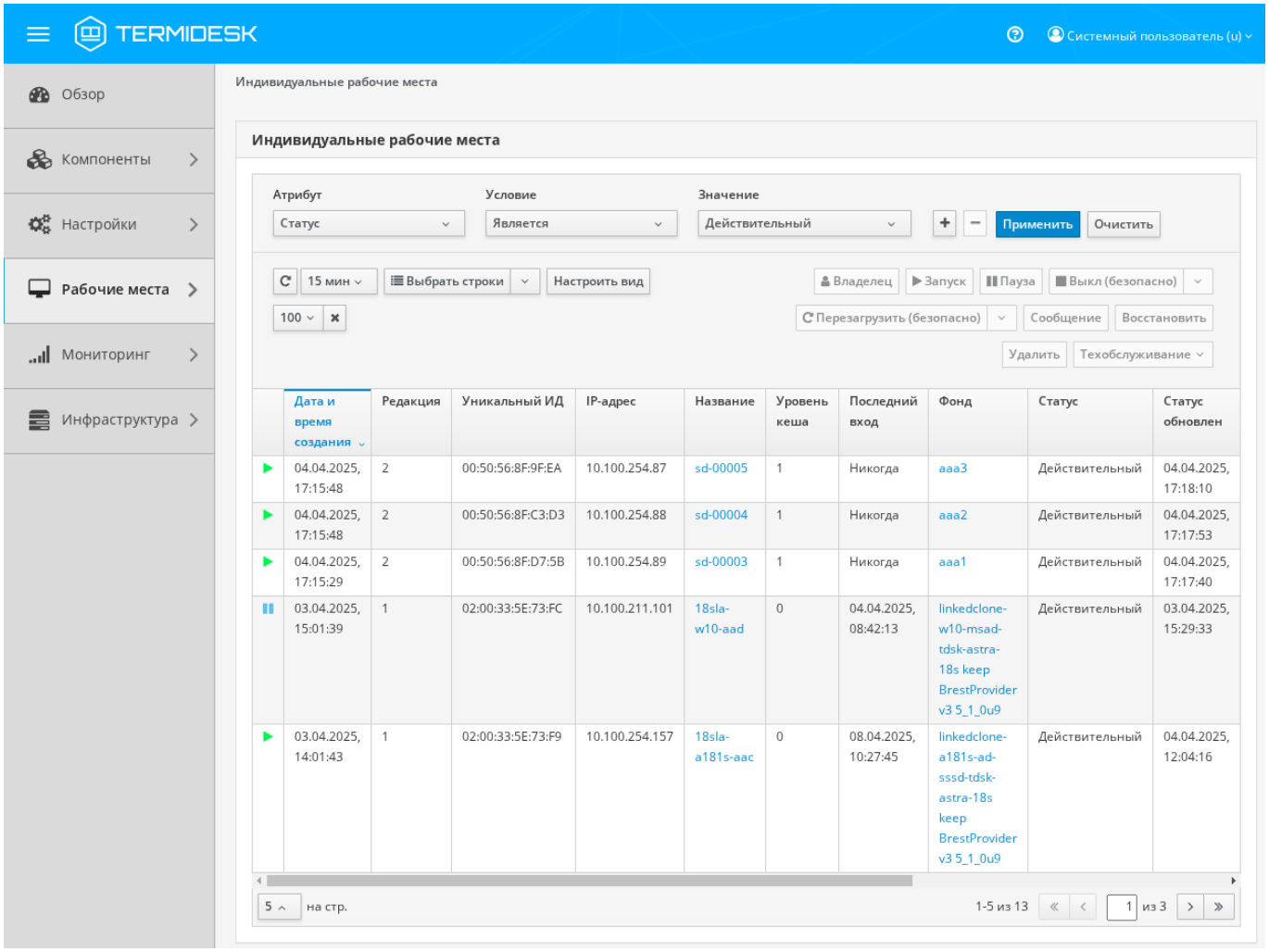

Рисунок 37 – Пример отображения списка РМ

Основные параметры списка РМ приведены в таблице (см. Таблица 32).

Таблица 32 – Основные параметры списка ВРМ

Параметр	Описание
«Дата и время создания»	Временная метка выполнения публикации РМ
«Редакция»	Порядковый номер версии публикации
«Уникальный ИД»	Уникальный идентификатор РМ: MAC-адрес или номер сессии
«IP-адрес»	IP-адрес, назначенный РМ
«Название»	Наименование РМ и ссылка на его журнал
«Уровень кеша»	Уровень кеша, на котором находится РМ
«Последний вход»	Временная метка последней успешной аутентификации пользователя
«Фонд»	Наименование фонда РМ и ссылка на него
«Статус»	Флаг использования публикации РМ из фонда РМ
«Статус обновлен»	Временная метка обновления статуса

Параметр	Описание
«Используется»	Флаг назначения РМ. Значение «Нет» свидетельствует о том, что РМ находится в кеше
«Хост источника»	Наименование инициатора выдачи РМ
«IP источника»	IP-адрес инициатора выдачи РМ
«Владелец»	Субъект, запросивший выдачу РМ
«Версия агента»	Версия компонента «Агент», установленного в гостевой ОС РМ

Для отправки сообщения во все назначенные пользователям РМ фонда, к которому принадлежит выбранная в списке РМ, 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»).

Для задания лимита записей, загружаемых из БД и отображаемых в веб-интерфейсе, нужно:

- нажать на экранную кнопку **[Выберите лимит]**. По умолчанию загружаются 100 записей, значение «100» отображается как значение экранной кнопки;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке;
- или ввести свое значение в доступном поле и подтвердить выбор, используя графический элемент  или клавишу **<ENTER>**. Возможные значения: от 1 до 1 000 000. Указанное значение сохранится в списке до перезагрузки страницы.

Для сброса заданного лимита нужно воспользоваться графическим элементом  .

> При включенной фильтрации записей по атрибутам сначала выполняется поиск записей в БД, удовлетворяющих условиям фильтра, и только затем применяется ограничение выбранного лимита.
> Пример: пусть в таблице БД существует 101 запись, а в веб-интерфейсе задана фильтрация по атрибутам и лимит в 100 записей. Если параметрам фильтрации удовлетворяют порядковые записи 5, 10, 101, то 101-ая запись не отобразится.

Также поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент 

под таблицей. По умолчанию отображаются 15 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента.

> Записи в таблице поддерживают функцию множественного выбора и выполнения операций над несколькими объектами одновременно. Выполнить операцию над несколькими объектами можно только тогда, когда она допустима для всех выбранных объектов.

Для выбора нескольких записей нужно зажать и удерживать клавиши **<CTRL>** или **<SHIFT>**. Для сброса множественного выбора записей нужно активировать функцию «Сбросить» экранной кнопки **[Выбрать строки]** или нажать на произвольную строку таблицы.

Существуют варианты выбора записей таблицы, доступные через выпадающий список экранной кнопки **[Выбрать строки]**, а именно:

- выделить все строки таблицы, активировав «Выбрать все»;
- выделить все строки на текущей странице таблицы, активировав «Выбрать все на стр.»;
- сбросить выделение строк, активировав «Сбросить».

⚠ В случае изменения ширины столбцов или их порядка произойдет сброс ранее выполненного выделения.

Для обновления значений таблицы используется графический элемент  . Для задания периода обновления или его отключения следует использовать выпадающий список (см. Рисунок 38) со значениями интервала в минутах, расположенный рядом с указанным элементом.

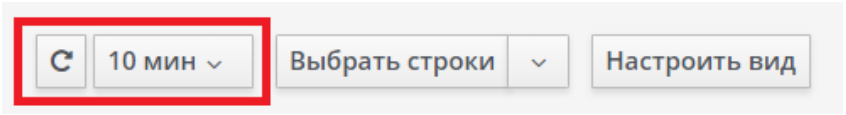

Рисунок 38 – Обновление значений таблицы

Внешний вид таблицы списка РМ можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться экранной кнопкой **[Настроить вид]** и отметить наименования столбцов (см. Рисунок 39), которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для применения изменений нажать экранную кнопку **[Сохранить]**. При попытке убрать выбор со всех пунктов экранная кнопка **[Сохранить]** будет заблокирована. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить вид]**;

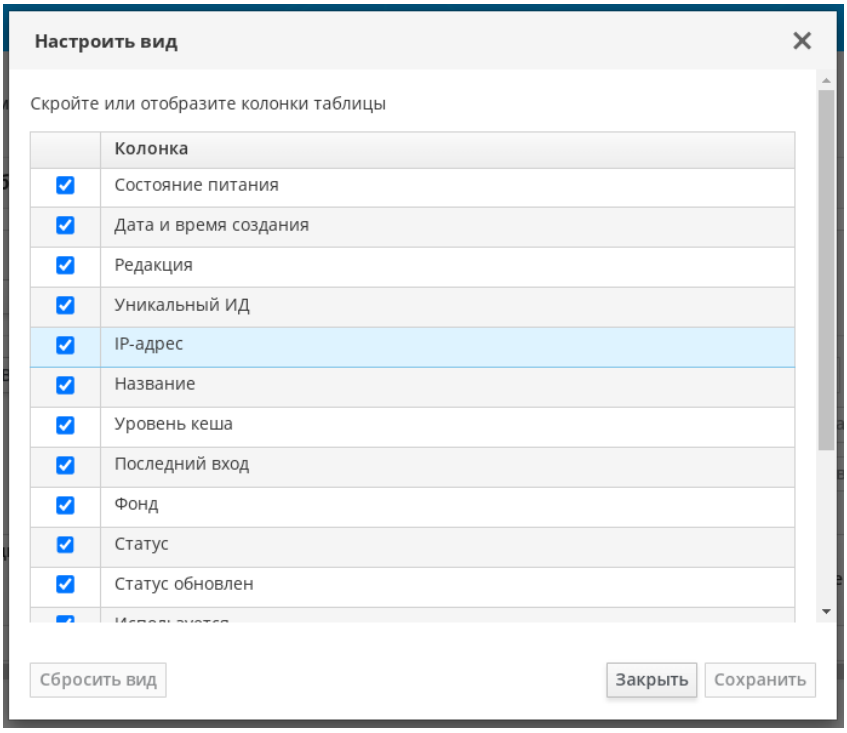

Рисунок 39 – Выбор столбцов для отображения

- порядок следования столбцов. Для изменения порядка следования нужно захватить левой кнопкой мыши заголовок столбца, и, не отпуская ее, перенести его в нужное расположение (см. Рисунок 40). Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок колонок]**, которая становится доступна только после изменения порядка следования столбцов и будет скрыта после сброса;

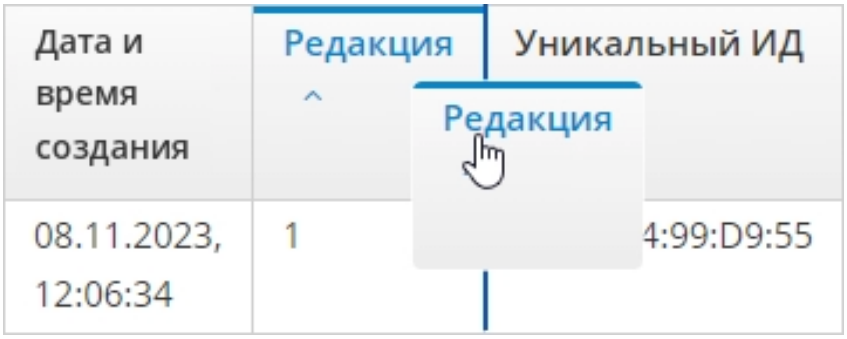

Рисунок 40 – Изменение порядка следования столбцов

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца (см. Рисунок 41).

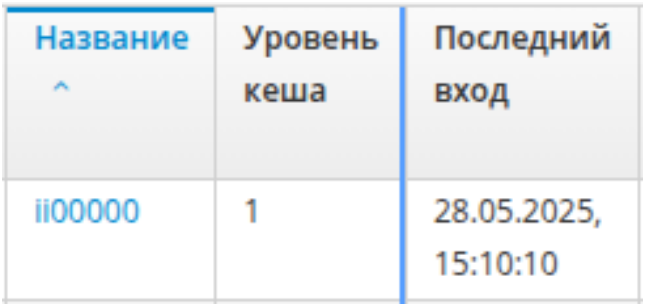

Рисунок 41 – Изменение ширины столбцов

6.2.2 . Фильтрация списка РМ

Для списка РМ доступен механизм фильтрации (см. Рисунок 37). Фильтрация осуществляется путем задания значений для параметров «Атрибут», «Условие» и «Значение».

Для добавления дополнительного фильтра следует нажать экранную кнопку **[+]**. Для удаления фильтра нужно использовать экранную кнопку **[-]** в соответствующей строке.

Чтобы применить установленные параметры фильтрации, следует нажать экранную кнопку **[Применить]**.

Экранная кнопка **[Очистить]** возвращает параметры фильтра к исходному состоянию: удаляются дополнительные строки фильтра, все значения сбрасываются, поля «Условие» и «Значение» блокируются.

Подробное описание механизма фильтрации списка РМ приведено в таблице (см. Таблица 33).

ⓘ При ручном вводе данных в поле фильтра «Значение» допускается полный или частичный ввод только одного параметра фильтрации.

⚠ При применении нескольких одинаковых фильтров к списку фильтрация выполняется с учетом только последнего заданного фильтра.

Таблица 33 – Параметры фильтрации

Атрибут	Условия	Значение
«Дата создания»	Формирование списка РМ по времени создания: ▪ «В пределах» - в указанном временном промежутке; ▪ «Не в пределах» - исключая указанный временной промежуток	▪ «Минута»; ▪ «5 минут»; ▪ «30 минут»; ▪ «1 час»; ▪ «12 часов»; ▪ «24 часа»; ▪ «Сегодня»; ▪ «Эта неделя»; ▪ «Этот месяц»
«Редакция»	Формирование списка РМ: ▪ «Является» - включая указанную редакцию; ▪ «Не является» - исключая указанную редакцию	Ручной ввод

Атрибут	Условия	Значение
«Уникальный ИД»	Формирование списка РМ: ▪ «Является» - по указанному идентификатору; ▪ «Не является» - исключая указанный идентификатор; ▪ «Начинается с» - по начальной части идентификатора; ▪ «Оканчивается на» - по конечной части идентификатора; ▪ «Содержит» - включая указанную часть идентификатора	Ручной ввод
«IP-адрес»	Формирование списка РМ: ▪ «Является» - по указанному IP-адресу инициатора выдачи РМ; ▪ «Не является» - исключая указанный IP-адрес инициатора выдачи РМ; ▪ «Начинается с» - по начальной части IP-адреса инициатора выдачи РМ; ▪ «Оканчивается на» - по конечной части IP-адреса инициатора выдачи РМ; ▪ «Содержит» - включая указанную часть IP-адреса инициатора выдачи РМ	Ручной ввод
«Название»	Формирование списка РМ: ▪ «Является» - по указанному наименованию РМ; ▪ «Не является» - исключая указанное наименование РМ; ▪ «Начинается с» - по начальной части наименования РМ; ▪ «Оканчивается на» - по конечной части наименования РМ; ▪ «Содержит» - включая указанную часть наименования РМ	Ручной ввод
«Фонд»	Формирование списка РМ: ▪ «Является» - по указанному наименованию фонда РМ; ▪ «Не является» - исключая указанное наименование фонда РМ; ▪ «Начинается с» - по начальной части наименования фонда РМ; ▪ «Оканчивается на» - по конечной части наименования фонда РМ; ▪ «Содержит» - включая указанную часть наименования фонда РМ	Ручной ввод
«Статус»	Формирование списка РМ: ▪ «Является» - по указанному статусу РМ; ▪ «Не является» - исключая указанный статус РМ	▪ «Подготовка»; ▪ «Действительный»; ▪ «Удаление»; ▪ «Удаляется»; ▪ «Удален»; ▪ «Ошибка»; ▪ «Отменяется»; ▪ «Отменено»

Атрибут	Условия	Значение
«Статус обновлен»	Формирование списка РМ по времени обновления статуса: ▪ «В пределах» - в указанном временном промежутке; ▪ «Не в пределах» - исключая указанный временной промежуток	▪ «Минута»; ▪ «5 минут»; ▪ «30 минут»; ▪ «1 час»; ▪ «12 часов»; ▪ «24 часа»; ▪ «Сегодня»; ▪ «Эта неделя»; ▪ «Этот месяц»
«Используется»	Формирование списка РМ: ▪ «Является» - по используемым РМ; ▪ «Не является» - исключая используемые РМ	▪ «Да»; ▪ «Нет»
«Хост источника»	Формирование списка РМ: ▪ «Является» - по указанному наименованию инициатора выдачи РМ; ▪ «Не является» - исключая указанное наименование инициатора выдачи РМ; ▪ «Начинается с» - по начальной части наименования инициатора выдачи РМ; ▪ «Оканчивается на» - по конечной части наименования инициатора выдачи РМ; ▪ «Содержит» - включая указанную часть наименования инициатора выдачи РМ	Ручной ввод
«IP источника»	Формирование списка РМ: ▪ «Является» - по указанному IP-адресу инициатора выдачи РМ; ▪ «Не является» - исключая указанный IP-адрес инициатора выдачи РМ; ▪ «Начинается с» - по начальной части IP-адреса инициатора выдачи РМ; ▪ «Оканчивается на» - по конечной части IP-адреса инициатора выдачи РМ; ▪ «Содержит» - включая указанную часть IP-адреса инициатора выдачи РМ	Ручной ввод
«Владелец»	Формирование списка РМ: ▪ «Является» - по указанному субъекту, инициировавшего выдачу РМ; ▪ «Не является» - исключая указанный субъект, инициировавшего выдачу РМ; ▪ «Начинается с» - по начальной части субъекта, инициировавшего выдачу РМ; ▪ «Оканчивается на» - по конечной части субъекта, инициировавшего выдачу РМ; ▪ «Содержит» - включая указанную часть субъекта, инициировавшего выдачу РМ	Ручной ввод
«Версия агента»	Формирование списка РМ: ▪ «Является» - по указанной версии Агента; ▪ «Не является» - исключая указанную версию Агента; ▪ «Начинается с» - по начальной части версии Агента; ▪ «Оканчивается на» - по конечной части версии Агента; ▪ «Содержит» - включая указанную часть версии Агента	Ручной ввод

Атрибут	Условия	Значение
«Состояние»	Формирование списка РМ: ▪ «Является» - по указанному состоянию ВМ; ▪ «Не является» - исключая указанное состояние ВМ	▪ «Выключена»; ▪ «Включена»; ▪ «Спящий режим»; ▪ «Неизвестно»
«Уровень кеша»	Формирование списка РМ: ▪ «Является» - по указанному уровню кеша; ▪ «Не является» - исключая указанный уровень кеша	▪ «0»; ▪ «1»; ▪ «2»
«Время последнего логина»	Формирование списка по времени последнего запуска РМ: ▪ «В пределах» - в указанном временном промежутке; ▪ «Не в пределах» - исключая указанный временной промежуток	▪ «Минута»; ▪ «5 минут»; ▪ «30 минут»; ▪ «1 час»; ▪ «12 часов»; ▪ «24 часа»; ▪ «Сегодня»; ▪ «Эта неделя»; ▪ «Этот месяц»

6.3 . Статусы РМ

Статусы позволяют отслеживать состояние РМ на разных этапах его жизненного цикла.

Возможные статусы, в которые может переходить РМ, приведены в таблице (см. Таблица 33).

Таблица 34 – Статусы РМ

Статус	Описание
«Подготовка»	Указывает на этап создания РМ. Статус назначается автоматически при запуске процесса создания РМ. Если РМ находится в этом статусе, то оно не готово к использованию и пользователь не может подключиться к нему. Если РМ успешно создано, то произойдет переход в статус «Действительный». Если во время создания РМ произошла ошибка, то произойдет переход в статус «Ошибка». Если РМ было удалено до окончания создания, то произойдет переход в статус «Отменено»
«Действительный»	Указывает на успешное завершение этапа подготовки РМ. Если РМ находится в этом статусе, то оно готово к использованию и пользователь может подключиться к нему. РМ переходит в «Действительный» из статуса «Подготовка» автоматически после успешного завершения создания РМ. Если инициирован процесс удаления РМ, то произойдет переход в статус «Удаление»
«Удаление»	Указывает на ожидание удаления РМ. Статус назначается автоматически при инициировании процесса удаления РМ. Если РМ находится в этом статусе, то пользователь не может подключиться к нему. Если начато фактическое удаление РМ (процесс перешел в фазу исполнения), то произойдет переход в статус «Удаляется»

Статус	Описание
«Удаляется»	Указывает на процесс удаления РМ. Статус назначается автоматически при переходе процесса удаления РМ к исполнению. Если РМ находится в этом статусе, то пользователь не может подключиться к нему. Если удаление РМ успешно выполнено, то произойдет переход в статус «Удален». Если во время удаления РМ произошла ошибка, то произойдет переход в статус «Ошибка»
«Удален»	Указывает на успешное удаление РМ. Статус назначается автоматически после успешного завершения процесса удаления РМ. Если РМ находится в этом статусе, то пользователь не может подключиться к нему. Переход между статусами не предусмотрен
«Ошибка»	Указывает на неуспешное завершение одного из этапов: создания, удаления или отмены РМ. Статус назначается автоматически. Если РМ находится в этом статусе, то пользователь не может подключиться к нему. Переход между статусами не предусмотрен
«Отменяется»	Указывает на процесс отмены создания РМ. Статус назначается автоматически при удалении РМ, находящегося в статусе «Подготовка». Если РМ находится в этом статусе, то пользователь не может подключиться к нему. Если процесс отмены (удаления РМ) успешно завершился, то произойдет переход в статус «Отменено»
«Отменено»	Указывает на успешную отмену создания РМ. Статус назначается автоматически после успешного завершения процесса отмены создания РМ. Если РМ находится в этом статусе, то пользователь не может подключиться к нему. Переход между статусами не предусмотрен
«Техобслуживание»	Указывает на нахождение РМ в режиме техобслуживания. Режим техобслуживания активируется вручную (см. подразделы **Режим техобслуживания фонда для ВРМ** и **Режим техобслуживания фонда терминального сервера**). Статус назначается автоматически после активации режима. Если РМ выведено из режима техобслуживания, то произойдет переход в статус «Действительный»

6.4 . Шаблоны ВРМ для ПК СВ Брест

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

Для добавления шаблона 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 **[Создать]**, 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 35).

Таблица 35 – Данные для добавления шаблонов на основе клонов для ПК СВ Брест

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Хранилище»	Идентификатор ресурсов хранения, представленных в платформе виртуализации, используемых для размещения файлов ВМ, входящих в фонд РМ
«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 (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемая в идентификаторе каждого ВРМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: ▪ «0-9» - числовой формат порядкового номера; ▪ «a-z» - символьный формат порядкового номера

6.4.2 . Шаблон на базе снапшота для ПК СВ Брест

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

Далее в открывшемся окне нажать на экранную кнопку **[Создать]**, 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 36).

Таблица 36 – Данные для добавления шаблона на базе снапшота для ПК СВ Брест

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Хранилище»	Идентификатор ресурсов хранения, представленных в платформе виртуализации, используемых для размещения файлов ВМ, входящих в фонд РМ
«Базовая ВМ»	ВМ, на базе которой будут создаваться фонды РМ
«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 (только строчных), цифр и знака «-» (дефис)

Параметр	Описание
«Длина суффикса»	Длина порядкового номера наименования, используемая в идентификаторе каждого ВРМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: ▪ «0-9» - числовой формат порядкового номера; ▪ «a-z» - символьный формат порядкового номера

6.5 . Шаблоны ВРМ для платформы oVirt/RHEV

6.5.1 . Шаблон на основе связанного клона для oVirt/RHEV

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

Далее в открывшемся окне нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Связанный клон oVirt/RHEV», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 37).

Таблица 37 – Данные для добавления шаблона на основе связанного клона для oVirt/RHEV

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Кластер»	Идентификатор кластера на платформе oVirt/RHEV, используемый для размещения фондов РМ
«Хранилище»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд РМ
«Место»	Минимально необходимое дисковое пространство на объекте «Хранилище» для размещения файлов ВМ, входящих в фонд РМ
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды РМ
«Память»	Объем оперативной памяти, выделяемый ВРМ
«Гарантированная память»	Минимальный объем оперативной памяти, резервируемый для ВРМ
«USB»	Политика разрешения доступа к USB-портам
«Дисплей»	Используемый протокол удаленного доступа к 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 (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого ВРМ

Параметр	Описание
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: ▪ «0-9» - числовой формат порядкового номера; ▪ «a-z» - символьный формат порядкового номера

ВМ, из которой планируется создать шаблон, может отображаться с некоторой задержкой, следует немного подождать ее появления в параметре «Базовая ВМ».

6.5.2 . Шаблон на основе статичной ВМ для oVirt/RHEV

Начиная с Termidesk версии 5.1 этот шаблон исключен. Для добавления статичных ВМ следует воспользоваться поставщиком ресурсов и шаблоном для автономных машин. Начиная с Termidesk версии 6.0 работоспособность Termidesk при наличии шаблонов статичных ВМ (не автономных машин) из прошлых инсталляций не гарантируется.

6.6 . Шаблоны ВРМ для платформы zVirt

6.6.1 . Шаблон на основе связанного клона для zVirt

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

Далее в открывшемся окне нужно на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Связанный клон zVirt», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 38).

Таблица 38 – Данные для добавления шаблона на основе связанного клона для zVirt

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Кластер»	Идентификатор кластера на платформе zVirt, используемый для размещения фондов РМ
«Хранилище»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд РМ
«Место»	Минимально необходимое дисковое пространство на объекте «Хранилище» для размещения файлов ВМ, входящих в фонд РМ
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды РМ
«Память»	Объем оперативной памяти, выделяемый ВРМ
«Гарантированная память»	Минимальный объем оперативной памяти, резервируемый для ВРМ
«USB»	Политика разрешения доступа к USB-портам

Параметр	Описание
«Дисплей»	Используемый протокол удаленного доступа к 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 (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого ВРМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: ▪ «0-9» - числовой формат порядкового номера; ▪ «a-z» - символьный формат порядкового номера

6.6.2 . Шаблон на основе статичной ВМ для zVirt

⚠ Начиная с Termidesk версии 5.1 этот шаблон исключен. Для добавления статичных ВМ следует воспользоваться поставщиком ресурсов и шаблоном для автономных машин. Начиная с Termidesk версии 6.0 работоспособность Termidesk при наличии шаблонов статичных ВМ (не автономных машин) из прошлых инсталляций не гарантируется.

6.7 . Шаблоны ВРМ для платформы «РЕД Виртуализация»

6.7.1 . Шаблон на основе связанного клона для платформы «РЕД Виртуализация»

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

Далее в открывшемся окне нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Связанный клон REDVirt», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 39).

Таблица 39 – Данные для добавления шаблона на основе связанного клона для платформы «РЕД Виртуализация»

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Кластер»	Идентификатор кластера на платформе «РЕД Виртуализация», используемый для размещения фондов ВМ
«Хранилище»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд ВМ
«Место»	Минимально необходимое дисковое пространство на объекте «Хранилище» для размещения файлов ВМ, входящих в фонд ВМ
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды ВМ
«Память»	Объем оперативной памяти, выделяемый ВРМ
«Гарантированная память»	Минимальный объем оперативной памяти, резервируемый для ВРМ

Параметр	Описание
«USB»	Политика разрешения доступа к USB-портам
«Дисплей»	Используемый протокол удаленного доступа к 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 (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого ВРМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: ▪ «0-9» - числовой формат порядкового номера; ▪ «a-z» - символьный формат порядкового номера

6.7.2 . Шаблон на основе статичной ВМ для платформы «РЕД Виртуализация»

⚠ Начиная с Termidesk версии 5.1 этот шаблон исключен. Для добавления статичных ВМ следует воспользоваться поставщиком ресурсов и шаблоном для автономных машин. Начиная с Termidesk версии 6.0 работоспособность Termidesk при наличии шаблонов статичных ВМ (не автономных машин) из прошлых инсталляций не гарантируется.

6.8 . Шаблоны ВРМ для VMmanager

6.8.1 . Шаблон на основе образа ВМ для VMmanager

Для добавления шаблона следует перейти в «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

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

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

Таблица 40 – Данные для добавления шаблона на основе образа ВМ

Параметр	Описание
«Название»	⚠ Параметр обязателен для заполнения! Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона

Параметр	Описание
«Кластер»	⚠ Параметр обязателен для заполнения! Идентификатор кластера на платформе VMmanager, используемый для размещения фондов РМ
«Узел»	Идентификатор узла кластера на платформе VMmanager, используемый для размещения фондов РМ. Значение по умолчанию: «Автоматически» (размещением управляет платформа VMmanager)
«Образ ВМ»	⚠ Параметр обязателен для заполнения! Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды РМ
«Количество ЦПУ»	Количество процессоров ВМ. Значение по умолчанию: «1»
«Объем памяти, Мб»	Объем оперативной памяти ВМ. Значение по умолчанию: «512»
«Объем диска, Мб»	Размер диска, выделяемый ВМ. Значение по умолчанию: «512»
«Использовать VxLAN»	Управление использованием виртуальной сети VxLAN. Следует включить параметр, если базовая ВМ создана с использованием виртуальной сети VxLAN. При использовании физической сети следует оставить значение по умолчанию. Значение по умолчанию: «Нет»
«Виртуальная сеть»	ⓘ Использование параметра возможно, если включен «Использовать VxLAN». Выбор виртуальной сети, созданной в кластере платформы VMmanager, к которой будет подключена ВМ
«Локальная сеть»	ⓘ Использование параметра возможно, если включен «Использовать VxLAN». Выбор локальной сети, к которой будет подключена ВМ. Параметр используется, если на платформе VMmanager создана дополнительная локальная сеть для виртуальной сети
«Подключить к бриджу»	ⓘ Использование параметра возможно, если выключен «Использовать VxLAN». Выбор сетевого моста (бриджа) узла кластера платформы VMmanager, к которому будет подключен сетевой интерфейс ВМ
«Использовать DHCP»	ⓘ Использование параметра возможно, если выключен «Использовать VxLAN». Управление использованием автоматического назначения IP-адресов по протоколу DHCP. Значение по умолчанию: «Нет»

Параметр	Описание
«Пул IP-адресов»	Использование параметра возможно, если выключен «Использовать DHCP». Идентификатор пула IP-адресов, настроенный на платформе VMmanager, из которого будут назначаться IP-адреса ВМ
«Количество IP-адресов»	Использование параметра возможно, если выключен «Использовать DHCP». Количество IP-адресов, которое может быть выделено ВМ. Ограничение возможного количества определяется платформой VMmanager. Значение по умолчанию: «1»
«Пользовательский скрипт»	Параметр обязателен для заполнения! Выбор выполняемого пользовательского скрипта. Если пользовательский скрипт не используется, следует выбрать «Без скрипта»
«Пароль root»	Параметр обязателен для заполнения! Пароль пользователя root
«Доменное имя»	Имя домена для ВМ (опционально)
«Базовое имя»	Параметр обязателен для заполнения! 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 (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого ВРМ Значение по умолчанию: «5»
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: ▪ «0-9» (по умолчанию) - числовой формат порядкового номера; ▪ «a-z» - символьный формат порядкового номера
«Создать как связанный клон»	Управление созданием ВМ в режиме связанного клона. Значение по умолчанию: «Нет»

6.8.2 . Шаблон на основе статичной ВМ для VMmanager

Начиная с Termidesk версии 5.1 этот шаблон исключен. Для добавления статичных ВМ следует воспользоваться поставщиком ресурсов и шаблоном для автономных машин. Начиная с Termidesk версии 6.0 работоспособность Termidesk при наличии шаблонов статичных ВМ (не автономных машин) из прошлых инсталляций не гарантируется.

6.9 . Шаблоны ВРМ для VMware vSphere

6.9.1 . Шаблоны на основе связанного или полного клона для платформ VMware vSphere

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

Далее в открывшемся окне нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать один из доступных шаблонов «Полный клон» или «Связанный клон», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 41).

Таблица 41 – Данные для добавления шаблона для VMware vSphere

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Датацентр»	Идентификатор виртуального центра обработки данных, используемый для размещения ВМ
«Кластер ресурсов»	⚠ Параметр обязателен для заполнения! Идентификатор кластера ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд
«Кластер данных»	⚠ Параметр обязателен для заполнения! Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд
«Пул ресурсов»	⚠ Параметр обязателен для заполнения! 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
«Сети»	Выбор одной или нескольких сетей, которые будут использоваться для назначения создаваемым ВМ. Список доступных сетей определяется значениями параметра «Сети», заданного в параметрах поставщика ресурсов («Компоненты - Поставщики ресурсов»). При создании новой ВМ Termidesk проверяет доступность указанных сетей (по порядку следования) и наличие в них свободного IP-адреса

Параметр	Описание
«Максимальное количество BPM, подключаемых к каждой выбранной сети поставщика ресурсов»	Выбор максимального количества BPM для подключения к каждой сети, заданной в параметре «Сети». ⚠ При добавлении фонда PM для поставщика ресурсов VMware vSphere суммарное количество создаваемых BPM в кеше 1-го уровня не должно превышать установленное значение данного параметра. При достижении предельного количества подключаемых к сети BPM вновь создаваемые при публикации BPM будут отображаться с ошибкой «No available network found». Предельное количество подключаемых к сети BPM - это количество сетей, выбранных в параметре «Сети», умноженное на значение параметра «Максимальное количество BPM, подключаемых к каждой выбранной сети поставщика ресурсов»
«Режим диска»	Выбор режима работы диска BPM. Возможные значения: ▪ «Зависимый» - при таком режиме все изменения при работе пользователя с BPM записываются на основной диск. Механизм восстановления BPM (см. подраздел **Управление ВМ в назначенном фонде PM**) для этого режима основывается на восстановлении снимка ВМ (снапшота); ▪ «Независимый-Непостоянный» - при таком режиме на момент запуска ВМ (получения BPM пользователем) создается временный диск, являющийся копией основного. Все изменения при работе пользователя с BPM записываются на временный диск. При небезопасной перезагрузке или небезопасном выключении временный диск удаляется. Механизм восстановления BPM для этого режима происходит через небезопасное выключение ВМ
«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 (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемая в идентификаторе каждого BPM
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого BPM: ▪ «0-9» - числовой формат порядкового номера; ▪ «a-z» - символьный формат порядкового номера
«Использовать статический MAC-адрес при создании»	Управление режимом назначения статического MAC-адреса для ВМ. Значение по умолчанию: «Нет»

Параметр	Описание
«Префикс диапазона MAC-адресов»	⚠ Использование возможно при: ▪ активации параметра «Использовать статический MAC-адрес при создании»; ▪ указании сети в параметре «Сети». В разных шаблонах РМ необходимо указывать разные префиксы MAC-адресов для исключения их дублирования. Задание префикса диапазона частных MAC-адресов, который будет использоваться для создания MAC-адреса ВМ. Если у ВМ будет несколько сетевых интерфейсов, то настройка префикса будет действовать только для первого интерфейса (eth0). Если используется переиспользование имен для ВМ (см. подраздел **Общие системные параметры Termidesk**), то для ВМ с переиспользованным именем будет назначен ранее записанный в БД MAC-адрес. Значение префикса должно удовлетворять условиям: ▪ допускается задание от 3 до 5 октетов; ▪ запрещено использовать значение «00:05:56». Значение по умолчанию: «00:00:6C»

6.9.2 . Создание снимка ВМ для VMware vSphere

Для создания снимка ВМ (снапшота) следует перейти «Компоненты - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Перед созданием снимка ВМ, состояние которой нужно зафиксировать, должна быть выключена!

Далее в открывшемся окне нужно нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Снапшоты», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 42).

Таблица 42 – Данные для добавления снимка ВМ для VMware vSphere

Параметр	Описание
«Название»	Текстовое наименование создаваемого снимка ВМ
«Шаблон»	Выбор шаблона для поставщика VMware vSphere, для которого будет сделан снимок ВМ. Шаблон для поставщика VMware vSphere должен существовать к моменту создания снимка ВМ
«Комментарий»	Информационное сообщение, используемое для описания назначения создаваемого снимка ВМ

6.10 . Шаблоны РМ для терминальных серверов

6.10.1 . Шаблон для доступа к терминальному серверу MS RDS

Для добавления шаблона следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

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

Таблица 43 – Данные для добавления шаблона для доступа к терминальному серверу MS RDS

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

6.10.2 . Шаблон для доступа к опубликованным приложениям MS RDS

Для добавления шаблона следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «RDS Remote App Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 44).

Таблица 44 – Данные для добавления шаблона для доступа к приложениям MS RDS

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

6.10.3 . Шаблон для доступа к терминальному серверу STAL

Для добавления шаблона следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «STAL Terminal Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 45).

Таблица 45 – Данные для добавления шаблона для доступа к терминальному серверу STAL

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

6.10.4 . Шаблон для доступа к опубликованным приложениям STAL

Для добавления шаблона следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «STAL Remote App Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 46).

Таблица 46 – Данные для добавления шаблона для доступа к приложениям STAL

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

6.11 . Шаблоны PM для метапровайдера

6.11.1 . Шаблон для публикации приложений

Для добавления шаблона следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов «Сервер терминалов Метапоставщик».

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Meta Remote App Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 47).

Таблица 47 – Данные для добавления шаблона публикации приложений для метапоставщика

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

6.11.2 . Шаблон для терминальных сессий

Для добавления шаблона следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов «Сервер терминалов Метапоставщик».

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Meta Terminal Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 48).

Таблица 48 – Данные для добавления шаблона терминальных сессий для метапоставщик

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

6.12 . Шаблон РМ для автономной машины

Для добавления шаблона следует перейти в «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

⚠ В ОС автономной машины должен быть установлен компонент «Агент виртуального рабочего места» для регистрации РМ в Termidesk.

Далее в открывшемся окне следует нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Автономные машины», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 49).

Таблица 49 – Данные для добавления шаблона для автономной машины

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«IP машин»	IP-адрес или IP-адреса добавляемого хоста. Может быть указан один IP-адрес, диапазон IP-адресов, перечень IP-адресов. Пример: ▪ «192.0.2.1»; ▪ «192.0.2.1, 192.0.2.1, 192.0.2.7»; ▪ «192.0.2.1, 192.0.2.2-192.0.2.7, 192.0.2.10»; ▪ «192.0.2.2-192.0.2.253»

6.13 . Шаблоны ВРМ для Openstack

6.13.1 . Шаблон на основе образа ВМ для Openstack

Для добавления шаблона следует перейти в «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «ВМ из образа», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 50).

Таблица 50 – Данные для добавления шаблона на основе образа ВМ для Openstack

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

Параметр	Описание
«Регион»	Идентификатор региона на платформе Openstack, используемый для размещения фондов РМ
«Проект»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды РМ
«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
«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 наименования, используемого в идентификаторе каждого ВРМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: ▪ «0-9» - числовой формат порядкового номера; ▪ «a-z» - символьный формат порядкового номера
«Состояние ВМ в кеше 2 уровня»	Выбор состояния ВМ по умолчанию в кеше 2-го уровня
«Метадата»	Информация о метаданных
«Cloud-init скрипт»	Скрипт cloud-init, выполняемый при создании ВМ

6.13.2 . Шаблон на основе статичной ВМ для Openstack

⚠ Начиная с Termidesk версии 5.1 этот шаблон исключен. Для добавления статичных ВМ следует воспользоваться поставщиком ресурсов и шаблоном для автономных машин. Начиная с Termidesk версии 6.0 работоспособность Termidesk при наличии шаблонов статичных ВМ (не автономных машин) из прошлых инсталляций не гарантируется.

7 . УПРАВЛЕНИЕ ПАРАМЕТРАМИ ГОСТЕВЫХ ОС

7.1 . Общие сведения о параметрах гостевых ОС

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

Веб-интерфейс Termidesk с установленной ролью «Портал администратора» 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 **[Создать]** и выбрать из выпадающего списка тип ОС.

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

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 РМ.

7.2 . Параметры гостевой ОС Microsoft Windows

7.2.1 . Конфигурация ОС Windows без домена

Для добавления в Termidesk параметров гостевой ОС Microsoft Windows без ввода в домен следует перейти «Компоненты - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «ОС Windows».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 51).

Таблица 51 – Данные для гостевой ОС Microsoft 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 ОС Windows при вводе в домен MS AD

Для добавления в Termidesk параметров гостевой ОС Microsoft Windows с вводом в домен следует перейти «Компоненты - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «ОС Windows (в домене MS Active Directory)».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 52).

Таблица 52 – Данные для гостевой ОС Microsoft 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 (DNS) службы каталогов MS AD
«Аккаунт»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/msad/»
«OU»	Идентификатор организационной единицы, в которую будут добавлены РМ. Следует учесть, что при вводе гостевой ОС в домен MS AD рекомендуется создавать обособленные подразделения домена, и не создавать учетные записи в подразделении «Computers». ⚠ Если учетные записи используют подразделение «Computers», то ввод РМ в домен не гарантируется! Строка не должна быть пустой, если используется функционал удаления учетной записи при удалении фонда РМ. Если строка будет пустой, то учетная запись не будет удалена. Параметр «OU» должен принимать значения вида: «OU=Computers,DC=domain,DC=local», т.е. не должен использоваться Common Name (CN)

7.2.3 . Конфигурация ОС Windows при использовании автономной машины

Для добавления в Termidesk параметров ОС автономной машины следует перейти «Компоненты - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Автономные машины Windows».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 53).

Таблица 53 – Данные для ОС Windows при использовании автономной машины

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

7.3 . Параметры гостевой ОС Linux

7.3.1 . Конфигурация ОС Linux без домена

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux без ввода в домен следует перейти «Компоненты - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «ОС Linux»

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 54).

Таблица 54 – 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 ОС Linux при вводе в домен MS AD

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux при вводе в домен MS AD следует перейти «Компоненты - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «ОС Linux (в домене MS Active Directory)».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 55).

Таблица 55 – 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
«Домен»	Доменное имя (DNS) службы каталогов MS AD

Параметр	Описание
«Аккаунт»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/msad/»
«OU»	Идентификатор организационной единицы, в которую будут добавлены РМ. Следует учесть, что при вводе гостевой ОС в домен MS AD рекомендуется создавать обособленные подразделения домена, и не создавать учетные записи в подразделении «Computers». ⚠ Если учетные записи используют подразделение «Computers», то ввод РМ в домен не гарантируется! Строка не должна быть пустой, если используется функционал удаления учетной записи при удалении фонда РМ. Если строка будет пустой, то учетная запись не будет удалена. Параметр «OU» должен принимать значения вида: «OU=Computers,DC=domain,DC=local», т.е. не должен использоваться Common Name (CN)

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

7.3.3 . Конфигурация ОС Linux при вводе в домен FreeIPA

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux с вводом в домен FreeIPA следует перейти «Компоненты - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «ОС Linux (в домене FreeIPA)».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 56).

Таблица 56 – 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

Параметр	Описание
«Домен аутентификации»	Идентификатор домена FreeIPA
«Аккаунт»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/freeipa/»

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

7.3.4 . Конфигурация ОС Linux при вводе в домен ALD Pro

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux с вводом в домен ALD Pro следует перейти «Компоненты - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «ОС Linux (в домене ALD Pro)».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 57).

Таблица 57 – Данные для гостевой ОС Linux при вводе в домен ALD Pro

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен аутентификации»	Идентификатор домена ALD Pro
«Аккаунт»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий

Параметр	Описание
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/aldpro/»

⚠ Для ввода РМ с ОС Astra Linux в домен ALD Pro необходимо в гостевую ОС установить пакеты `astra-freeipa-client` и `aldpro-client`.
Для корректного ввода РМ в домен нужно обеспечить корректное разрешение имен узлов в домене ALD Pro.

7.3.5 . Конфигурация ОС Linux при вводе в домен ALD

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux с вводом в домен ALD следует перейти «Компоненты - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «ОС Linux (в домене ALD)».
Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 58).

Таблица 58 – 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
«Домен аутентификации»	Идентификатор домена ALD
«Аккаунт»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен
«Пароль»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	⚠ Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/ald/»

7.3.6 . Конфигурация ОС Linux при использовании автономной машины

Для добавления в Termidesk параметров ОС автономной машины следует перейти «Компоненты - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Автономные машины Linux».

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

Таблица 59 – Данные для ОС Linux при использовании автономной машины

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

7.4 . Действие при выходе пользователя из ОС

Termidesk поддерживает назначение действий с РМ при выходе пользователя из сессии в политике «Действие при выходе пользователя из ОС» (см. подраздел **Политики фонда РМ**).

Совместно с политикой «Действие при выходе пользователя из ОС» применяется политика «Удаление рабочего места».

7.5 . Изменение изображения гостевых ОС

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

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

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 «Универсальному диспетчеру» Termidesk через компонент «Клиент», увидит их в своем интерфейсе (см. Рисунок 42).

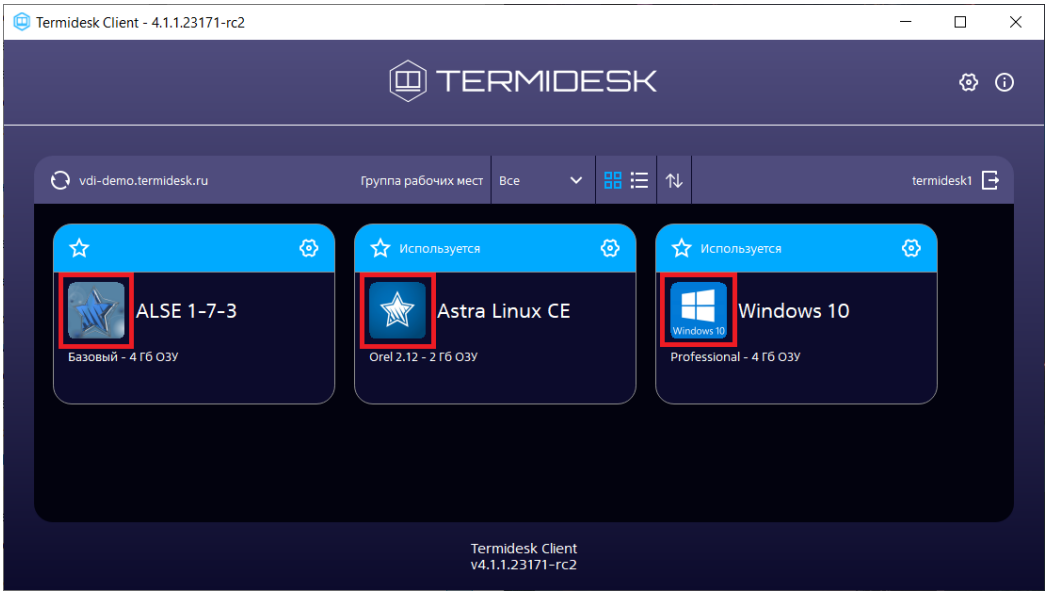

Рисунок 42 – Отображение назначенных изображений в сеансе пользователя

8 . СЕТИ

8.1 . Общие сведения о сетях в Termidesk

Сети - это IP-адреса или диапазоны IP-адресов пользователей, подключающихся к Termidesk. Сети используются для реализации «белого» или «черного» списка доступа на уровне:

- протокола доставки;
- фонда РМ.

Для отображения списка сетей следует перейти «Компоненты - Сети». Основные параметры списка приведены в таблице (см. Таблица 60).

Таблица 60 – Параметры списка сетей

Параметр	Описание
«Название»	Наименование сети
«Диапазон»	IP-адреса или диапазоны IP-адресов, назначенных для сети
«Используется в фондах»	Характеристика использования сети в каком-либо фонде
«Используется в протоколах доставки»	Характеристика использования сети в каком-либо протоколе доставки

Для добавления сети следует перейти «Компоненты - Сети» и нажать экранную кнопку **[Создать]**.

Созданные сети можно:

- редактировать, для этого нужно пометить название сети, а затем нажать экранную кнопку **[Изменить]**;
- удалить, для этого нужно пометить название сети, а затем нажать экранную кнопку **[Удалить]**.

8.2 . Добавление сети

Для добавления сети следует перейти «Компоненты - Сети», нажать экранную кнопку **[Создать]** и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 61).

Таблица 61 – Данные для добавления сети

Параметр	Описание
«Название»	Наименование сети
«Диапазон»	IP-адрес или диапазоны IP-адресов, назначаемые для сети. Может быть указан один IP-адрес или диапазон IP-адресов. Пример: ▪ «192.0.2.1»; ▪ «192.0.2.5/24»; ▪ «192.0.2.2-192.0.2.253»

9 . ПРОТОКОЛЫ ДОСТАВКИ

9.1 . Общие сведения о протоколах доставки

Протокол доставки – это поддерживаемый в Termidesk протокол удаленного доступа к РМ. Протоколы доставки обеспечивают подключение к BPM, а также к терминальным сессиям и приложениям, и могут выполнять доставку РМ как напрямую, так и через компонент «Шлюз».

Для отображения списка добавленных протоколов доставки следует перейти «Компоненты - Протоколы доставки». Основные параметры списка приведены в таблице (см. Таблица 62). Для добавления протокола доставки следует нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка поддерживаемый протокол и способ доставки.

Добавленные протоколы можно:

- редактировать, для этого нужно пометить протокол и нажать на экранную кнопку **[Изменить]** (см. Рисунок 43);
- удалить, для этого нужно пометить протокол и нажать на экранную кнопку **[Удалить]**.

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

Таблица 62 – Параметры списка протоколов доставки

Параметр	Описание
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя
«Название»	Текстовое наименование протокола доставки в Termidesk
«Протокол»	Тип протокола доставки
«Используется»	Характеристика использования протокола доставки в каком-либо фонде
«Комментарии»	Информационное сообщение, используемое для описания назначения протокола доставки

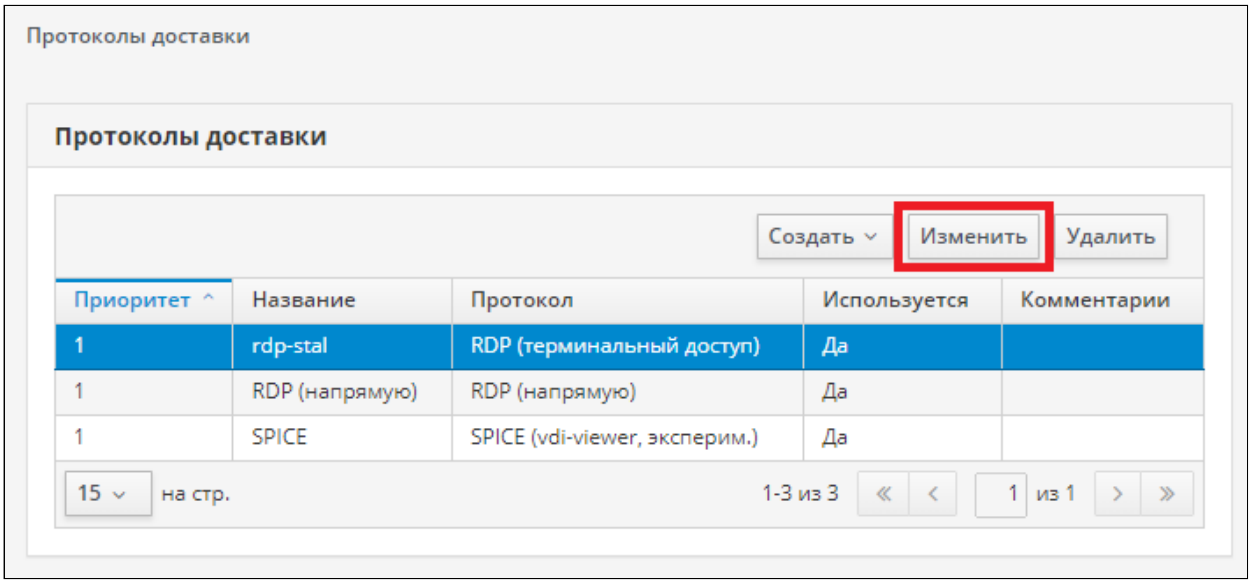

Рисунок 43 – Редактирование протокола доставки

Termidesk поддерживает следующие протоколы удаленного доступа:

- SPICE, поддерживается, в том числе, при доставке BPM через HTML5-клиент (только для варианта лицензирования Termidesk VDI);
- TERA (экспериментально), поддерживается, в том числе, при доставке BPM через HTML5-клиент (только для варианта лицензирования Termidesk VDI);
- VNC (только через HTML5-клиент, только для варианта лицензирования Termidesk VDI);
- RDP. Для варианта лицензирования Termidesk Terminal доступны только протоколы доступа к ресурсам терминального сервера;
- Loudplay (только для варианта лицензирования Termidesk VDI).

Сравнительная таблица функциональных возможностей протоколов доставки приведена в справочном центре Termidesk: https://wiki.astralinux.ru/pages/viewpage.action?pageId=359057145.

9.2 . Протокол доставки RDP

9.2.1 . Прямое подключение по протоколу RDP

Для добавления прямого подключения по протоколу RDP следует перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «RDP (напрямую)» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 63).

Таблица 63 – Данные для добавления прямого подключения по протоколу RDP

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

Параметр	Описание
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя
«Пустые учетные данные»	Использование технологии единого входа. Возможные значения: ▪ «Да» - не использовать учетные данные в полях «Логин» и «Пароль» при подключении по протоколу RDP; ▪ «Нет» - использовать учетные данные в полях «Логин» и «Пароль» при подключении по протоколу RDP
«Логин»	Субъект, имеющий полномочия для подключения по протоколу RDP к BPM
«Пароль»	Набор символов, подтверждающий полномочия
«Без домена»	Использование идентификатора домена MS AD при проверке полномочий субъекта. Возможные значения: ▪ «Да» - не использовать идентификатор домена MS AD в поле «Домен» при подключении; ▪ «Нет» - использовать идентификатор домена MS AD в поле «Домен» при подключении
«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»	Разрешить отображение фонового изображения, настроенного на рабочем столе
«Разрешить композицию рабочего стола»	Разрешить отображение 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
«Доступ из сетей»	Ограничение доступа для указанного диапазона сетей. Возможные значения: ▪ «Да» - протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа); ▪ «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 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» следует перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «RDP (через вебсокет шлюз)» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 64).

Таблица 64 – 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»	Приоритет отображения в списке протоколов доставки для пользователя
«URL шлюза»	Адрес «Шлюза», обеспечивающего формирование и поддержание соединения, в формате `ws(s)://<IP-адрес>:<порт>`. Протокол WS (WebSocket) используется, если «Шлюз» не настроен на защищенное соединение, протокол WSS используется, если выполняется защищенное подключение к «Шлюзу». По умолчанию «Шлюз» использует порты: ▪ 5099 - для незащищенного подключения; ▪ 10000 - для защищенного подключения. Администратор может задать нужное значение порта, если используется нестандартный порт в настройках «Шлюза»
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза
«Пустые учетные данные»	Использование технологии единого входа. Возможные значения: ▪ «Да» - не использовать учетные данные в полях «Логин» и «Пароль» при подключении по протоколу RDP; ▪ «Нет» - использовать учетные данные в полях «Логин» и «Пароль» при подключении по протоколу RDP
«Логин»	Субъект, имеющий полномочия для подключения по протоколу RDP к BPM
«Пароль»	Набор символов, подтверждающий полномочия

Параметр	Описание
«Без домена»	Использование идентификатора домена MS AD при проверке полномочий субъекта. Возможные значения: ▪ «Да» - не использовать идентификатор домена MS AD в поле «Домен» при подключении; ▪ «Нет» - использовать идентификатор домена MS AD в поле «Домен» при подключении
«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
«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
«Доступ из сетей»	Ограничение доступа для указанного диапазона сетей. Возможные значения: ▪ «Да» - протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа); ▪ «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 . Подключение по протоколу RDP для доступа к ресурсам терминального сервера

Для добавления подключения для доступа к MS RDS или STAL следует перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Создать]** и выбрать «RDP (терминальный доступ)».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 65).

Таблица 65 – 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»	Приоритет отображения в списке протоколов доставки для пользователя
«URL шлюза»	Адрес «Шлюза», обеспечивающего формирование и поддержание соединения, в формате `ws(s)://<IP-адрес>:<порт>`. Работа через компонент «Шлюз» с инфраструктурой терминального сервера MS RDS, развернутого не через метапоставщик, не обеспечивается. Протокол WS (WebSocket) используется, если «Шлюз» не настроен на защищенное соединение, протокол WSS используется, если выполняется защищенное подключение к «Шлюзу». По умолчанию «Шлюз» использует порты: ▪ 5099 - для незащищенного подключения; ▪ 10000 - для защищенного подключения. Администратор может задать нужное значение порта, если используется нестандартный порт в настройках «Шлюза»
«Время ожидания соединения»	Время ожидания (в секундах) отклика «Шлюза». При прямом соединении (не через «Шлюз») можно оставить значение по умолчанию, т.к. параметр не будет оказывать влияния на подключение
«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
«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	Описание
«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 Microsoft 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 РМ. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к РМ

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

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

Начиная с Termidesk версии 5.0 подключение к ресурсам терминального сервера через «Шлюз» настраивается при выборе протокола «RDP (терминальный доступ)».

9.3 . Протокол доставки SPICE

9.3.1 . Подключение по протоколу SPICE через vdi-viewer

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

Для подключения по протоколу SPICE нужно:

- на узлах платформы виртуализации включить оптимизацию для протокола SPICE;
- на пользовательскую рабочую станцию установить ПО Termidesk Viewer согласно документу СЛЕТ.10001-01 92 01 «Руководство администратора. Настройка и эксплуатация компонента «Клиент»).

Для добавления подключения по протоколу SPICE следует перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «SPICE (vdi-viewer, эксперим.)» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 66).

Таблица 66 – 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
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя
«URL шлюза»	Адрес «Шлюза», обеспечивающего формирование и поддержание соединения, в формате `ws(s)://<IP-адрес>:<порт>`. Протокол WS (WebSocket) используется, если «Шлюз» не настроен на защищенное соединение, протокол WSS используется, если выполняется защищенное подключение к «Шлюзу». По умолчанию «Шлюз» использует порты: ▪ 5099 - для незащищенного подключения; ▪ 10000 - для защищенного подключения. Администратор может задать нужное значение порта, если используется нестандартный порт в настройках «Шлюза»
«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 5.1 использование функционала, подключаемого через плагин расширения, исключено. Для настройки подключения по протоколу SPICE через HTML5 (локальный прокси) следует обратиться к подразделу **Протокол доставки HTML5**.

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

Протокол VNC через HTML5 не поддерживается компонентом «Клиент» и приведен для справки.

Для добавления подключения по протоколу VNC через HTML5 (локальный прокси) следует перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «VNC (HTML5, через локальный прокси)» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 67).

Таблица 67 – 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»	Приоритет отображения в списке протоколов доставки для пользователя
«URL шлюза»	Адрес «Шлюза», обеспечивающего формирование и поддержание соединения, в формате `ws(s)://<IP-адрес>:<порт>`. Протокол WS (WebSocket) используется, если «Шлюз» не настроен на защищенное соединение, протокол WSS используется, если выполняется защищенное подключение к «Шлюзу». По умолчанию «Шлюз» использует порты: ▪ 5099 - для незащищенного подключения; ▪ 10000 - для защищенного подключения. Администратор может задать нужное значение порта, если используется нестандартный порт в настройках «Шлюза»
«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 TERA

9.5.1 . Подключение по протоколу TERA

Протокол TERA обеспечивает прямое подключение к гостевой ОС РМ независимо от используемой платформы виртуализации. TERA поддерживает безопасную аутентификацию пользователя по логину и паролю, передаваемого в преобразованном виде. Для безопасной аутентификации по умолчанию используются самоподписанные сертификаты.

Для подключения по протоколу TERA в гостевой ОС Astra Linux Special Edition базового РМ нужно:

- после выполнения обязательных настроек (см. подраздел **Обязательные настройки**) установить соответствующие пакеты, как это приведено в документе СЛЕТ.10001-01 90 09 «Руководство администратора. Настройка компонента TERA»;
- на пользовательскую рабочую станцию установить ПО Termidesk Viewer согласно документу СЛЕТ.10001-01 92 01 «Руководство администратора. Настройка и эксплуатация компонента «Клиент»).

Для использования протокола TERA в качестве протокола доставки необходимо включить экспериментальный параметр `experimental.tera.transports.enabled` в соответствии с подразделом **Управление экспериментальными параметрами Termidesk**.

Для добавления подключения по протоколу TERA следует перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «TERA [экспериментальный]» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 68).

Таблица 68 – Данные для добавления подключения по TERA

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя

Параметр	Описание
«URL шлюза»	⚠ Работа протокола TERA через «Шлюз» не гарантируется при включенной безопасной аутентификации пользователя в настройках TERA. Для работы соединения по протоколу TERA через «Шлюз» нужно дополнительно выполнить: ▪ в параметре «Порт» указать значение порта TERA для TLS, заданного в конфигурационном файле TERA: • для TERA на физической машине - значение из параметра `listen` (по умолчанию `5900`); • для TERA на ВМ - значение из параметра `SpiceTlsPort` (следует убедиться, что параметр задан и используется); ▪ убедиться, что TERA настроена на использование TLS в соответствующих параметрах конфигурационного файла TERA; ▪ в параметре «TLS порт» оставить значение по умолчанию «-1». Адрес «Шлюза», обеспечивающего формирование и поддержание соединения, в формате `ws(s)://<IP-адрес>:<порт>`. Протокол WS (WebSocket) используется, если «Шлюз» не настроен на защищенное соединение, протокол WSS используется, если выполняется защищенное подключение к «Шлюзу». По умолчанию «Шлюз» использует порты: ▪ 5099 - для незащищенного подключения; ▪ 10000 - для защищенного подключения. Администратор может задать нужное значение порта, если используется нестандартный порт в настройках «Шлюза».
«Время ожидания соединения»	Время ожидания (в секундах) отклика «Шлюза»
«Порт»	Порт подключения к TERA. Значение по умолчанию: «5900»
«TLS порт»	TLS-порт для подключения к TERA. Для работы TLS-подключения следует: ▪ убедиться, что в конфигурационном файле TERA параметр `SpiceTlsPort` не закомментирован; ▪ изменить значение по умолчанию на используемое в конфигурационном файле TERA. Значение по умолчанию: «-1» - не использовать TLS
«Пароль»	Набор символов, подтверждающий подключение. Если пароль не задан, он не используется для подключения. В текущей версии параметр не оказывает влияния на подключение
«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 РМ. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении к РМ

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

9.5.2 . Настройка параметров протокола TERA

Для настройки параметров TERA следует обратиться к документу СЛЕТ.10001-01 90 09 «Руководство администратора. Настройка компонента TERA»

9.6 . Протокол доставки Loudplay

9.6.1 . Прямое подключение по протоколу Loudplay

Для возможности добавления протокола доставки Loudplay нужно включить экспериментальный параметр `experimental.loudplay.transports.enabled`.

Процесс активации протокола доставки и параметры, доступные для его настройки, приведены в подразделе **Управление экспериментальными параметрами Termidesk**.

> Для подключения к РМ по протоколу доставки Loudplay нужно:
> - на пользовательскую рабочую станцию нужно дополнительно установить ПО LoudPlay-client, которое не входит в состав Termidesk;
> - в ОС РМ нужно дополнительно установить серверные драйверы NVIDIA и сервер Loudplay.

После включения экспериментального параметра перейти в «Компоненты - Протоколы доставки», а затем нажать на экранную кнопку **[Создать]** 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 69).

Таблица 69 – 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»	Приоритет отображения в списке протоколов доставки для пользователя
«Протокол передачи видео»	Выбор протокола для передачи видеопотока. Значение по умолчанию: «TCP»
«Технология захвата»	Выбор технологии захвата изображения. Значение по умолчанию: «FFmpeg DDA»
«Уровень логирования клиента LP»	Выбор категории сообщений, которые будут записываться в журнал клиента Loudplay. Значение по умолчанию: «DEBUG»

Параметр	Описание
«Уровень логирования модуля проброса USB»	Выбор категории сообщений, которые будут записываться в журнал клиента Loudplay при перенаправлении USB-устройств. Значение по умолчанию: «INFO»
«Максимальная частота кадров видео»	Параметр позволяет задать максимально возможную частоту смены кадров (в секунду) видеопотока. Диапазон значений: от 1 до 120. Значение по умолчанию: «30»
«Скорость видеопотока (Kbit/s)»	Параметр позволяет задать максимально возможную скорость видеопотока (Kbit/s). Диапазон значений: от 50 до 100000. Значение по умолчанию: «5000»
«Автоматическое изменение скорости видеопотока»	Управление автоматическим изменением скорости видеопотока. Возможные значения: ▪ «Да» - разрешить автоматическое изменение скорости видеопотока; ▪ «Нет» - запретить автоматическое изменение скорости видеопотока
«Аппаратное ускорение»	Использование вычислительных ресурсов графического процессора (GPU) для обработки видеопотока. Возможные значения: ▪ «Да» - разрешить использование вычислительных ресурсов GPU; ▪ «Нет» - запретить использование вычислительных ресурсов GPU
«Выбор монитора на сервере»	Выбор приоритетного монитора для подключения в многомониторной конфигурации сервера. Возможные значения: ▪ «0» - вывод изображения на первый монитор; ▪ «1» - вывод изображения на второй монитор. Значение по умолчанию: «0»
«Выбор монитора пользовательского ПК»	Выбор приоритетного монитора на пользовательской рабочей станции для отображения клиента Loudplay. Возможные значения: ▪ «0» - вывод изображения на первый монитор; ▪ «1» - вывод изображения на второй монитор. Значение по умолчанию: «0»
«Протокол передачи сигналов клавиатуры и мыши»	Выбор протокола для передачи сигналов клавиатуры и мыши. Значение по умолчанию: «UDP»
«Помехоустойчивое кодирование»	Использование режима помехоустойчивого кодирования. При использовании значения «UDP» в параметре «Протокол передачи видео» режим помехоустойчивого кодирования обеспечивает непрерывную передачу видеоизображения на каналах с потерями до 30%. Возможные значения: ▪ «Да» - разрешить использование помехоустойчивого кодирования; ▪ «Нет» - запретить использование помехоустойчивого кодирования

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 РМ. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу Loudplay к РМ

9.6.2 . Подключение через компонент «Шлюз» по протоколу Loudplay

Работа с протоколом Loudplay поддерживается только при прямом подключении, для добавления протокола нужно обратиться к подразделу **Прямое подключение по протоколу Loudplay**.

9.7 . Протокол доставки HTML5

9.7.1 . Протокол доставки HTML5 SPICE

Протокол доставки HTML5 SPICE позволяет получить пользователю РМ по протоколу SPICE и работать с ним из веб-браузера, не устанавливая компонент «Клиент» на пользовательскую рабочую станцию. Подключение по протоколу SPICE происходит к гипервизору платформы виртуализации.

⚠ Для корректной работы протокола доставки HTML5 SPICE рекомендуется использовать компонент «Шлюз» версии 0.7.0 и выше.

ⓘ Использование протокола доставки HTML5 SPICE является экспериментальным.

Для активации протокола доставки нужно включить экспериментальный параметр `experimental.html5.transports.enabled` в соответствии с подразделом **Управление экспериментальными параметрами Termidesk**.

Для добавления протокола доставки следует перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «HTML5» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 70).

Таблица 70 – Данные для добавления протокола HTML5

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя

Параметр	Описание
«Способ подключения»	Выбор протокола, который будет использоваться для подключения. Возможные варианты: ▪ «SPICE (hypervisor)» - подключение по протоколу SPICE происходит к гипервизору платформы виртуализации; ▪ «TERA (host)» - подключение по протоколу TERA происходит непосредственно к ВМ, обращением на IP-адрес или по имени узла (hostname). ⓘ Для работы подключения в гостевую ОС должны быть установлены соответствующие пакеты поддержки (см. подраздел **Подготовка базового ВРМ**).
«URL шлюза»	Адрес «Шлюза», обеспечивающего формирование и поддержание соединения, в формате `ws(s)://<IP-адрес>:<порт>`. Протокол WS (WebSocket) используется, если «Шлюз» не настроен на защищенное соединение, протокол WSS используется, если выполняется защищенное подключение к «Шлюзу». По умолчанию «Шлюз» использует порты: ▪ 5099 - для незащищенного подключения; ▪ 10000 - для защищенного подключения. Администратор может задать нужное значение порта, если используется нестандартный порт в настройках «Шлюза». ⚠ Для работы протокола доставки HTML5 SPICE по защищенному соединению со «Шлюзом» необходимо убедиться, что: ▪ «Шлюз» настроен соответствующим образом (см. подраздел **Настройка защищенного подключения к Шлюзу** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз»); ▪ на узле «Шлюза» установлены валидные сертификаты (непосредственно сертификат SSL и корневой сертификат к нему). Параметр обязателен для заполнения
«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 РМ. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении к РМ

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

9.7.2 . Протокол доставки HTML5 TERA

Протокол доставки HTML5 TERA позволяет получить пользователю РМ по протоколу TERA и работать с ним из веб-браузера, не устанавливая компонент «Клиент» на пользовательскую рабочую станцию. Подключение по протоколу TERA происходит непосредственно к ВМ, обращением на IP-адрес или по имени узла (hostname).

Использование протокола доставки HTML5 TERA является экспериментальным.

Для корректной работы протокола доставки HTML5 TERA рекомендуется использовать компонент «Шлюз» версии 0.7.0 и выше.

Для активации протокола доставки нужно включить экспериментальный параметр `experimental.html5.transports.enabled` в соответствии с подразделом **Управление экспериментальными параметрами Termidesk**.

Для добавления протокола доставки следует перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «HTML TERA» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 71).

Таблица 71 – Данные для добавления протокола HTML5 TERA

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя
«URL шлюза»	Адрес «Шлюза», обеспечивающего формирование и поддержание соединения, в формате `ws(s)://<IP-адрес>:<порт>`. Протокол WS (WebSocket) используется, если «Шлюз» не настроен на защищенное соединение, протокол WSS используется, если выполняется защищенное подключение к «Шлюзу». По умолчанию «Шлюз» использует порты: ▪ 5099 - для незащищенного подключения; ▪ 10000 - для защищенного подключения. Администратор может задать нужное значение порта, если используется нестандартный порт в настройках «Шлюза». Для работы протокола доставки HTML5 TERA по защищенному соединению со «Шлюзом» необходимо убедиться, что: ▪ «Шлюз» настроен соответствующим образом (см. подраздел **Настройка защищенного подключения к Шлюзу** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз»); ▪ на узле «Шлюза» установлены валидные сертификаты (непосредственно сертификат SSL и корневой сертификат к нему). Параметр обязателен для заполнения

Параметр	Описание
«Время ожидания соединения»	Время ожидания (в секундах) отклика «Шлюза»
«Порт»	Порт подключения к TERA, заданный в настройках протокола (см. подраздел **Настройка параметров протокола TERA**)
«Использовать TLS»	Управление режимом использования протокола TLS. Следует включить параметр, если используется защищенное подключение по протоколу TERA и параметры протокола настроены для него (см. подраздел **Настройка параметров протокола TERA**)
«Пароль»	Пароль доступа к подключению, заданный в настройках протокола (см. подраздел **Настройка параметров протокола TERA**)
«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 РМ. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении к РМ

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

10 . ФОНД РАБОЧИХ МЕСТ

10.1 . Общие сведения о фонде РМ

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

Для отображения списка фондов РМ следует перейти «Рабочие места - Фонды». Основные параметры списка приведены в таблице (см. Таблица 72).

Таблица 72 – Параметры списка фондов

Параметр	Описание
«Фонд рабочих мест»	Наименование фонда РМ
«Статус»	Состояние готовности фонда РМ Если фонд РМ находится в зависшем состоянии в статусах «Удален», «Отменен», «Ошибка», «Подготовка», «Создание» более 48 часов, то ВМ, вызвавшая это состояние, будет удалена периодической задачей, выполняемой раз в 24 часа. Фонд РМ также будет удален.
«Места»	Общее количество РМ в фонде
«Готовятся»	Количество подготавливаемых РМ
«Выбор протокола»	Флаг возможности выбора пользователем протокола доставки при работе с фондом РМ. Значение определяется политикой фонда РМ «Выбор пользователем протокола доставки»
«Группа рабочих мест»	Принадлежность фонда группе РМ
«Шаблон»	Шаблон РМ, примененный в фонде
«Комментарий»	Информационное сообщение, используемое для описания назначения фонда РМ

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент 

под таблицей. По умолчанию отображаются 15 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента.

Для добавления нового фонда РМ следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Создать]**.

Созданные фонды можно:

- редактировать, для этого нужно пометить название фонда, а затем нажать экранную кнопку **[Изменить]**;
- 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 РМ можно перейти к его детальному просмотру. Для этого в сводной таблице окна «Фонды» в столбце «Название» следует нажать на наименование фонда РМ.
На открывшейся странице будут представлены следующие разделы:

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

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

10.2 . Добавление фонда РМ

10.2.1 . Добавление фонда РМ

Для добавления фонда РМ следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Создать]**, выбрать тип мастера публикации «Виртуальные машины».

Откроется мастер публикации фонда (см. Рисунок 44). Необходимо заполнить параметры, указанные в таблице, (см. Таблица 73) 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.

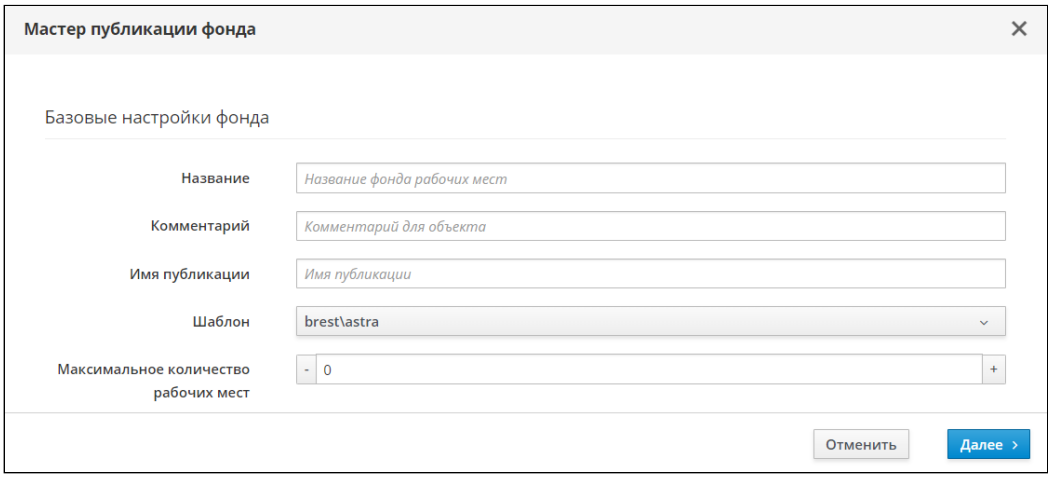

Рисунок 44 – Базовые настройки фонда в Мастере публикации

Таблица 73 – Базовые настройки фонда

Параметр	Описание
«Название»	Ввести текстовое наименование фонда. Наименование может содержать только буквы латинского алфавита, цифры, знаки «-» (дефис), пробел и «_» (нижнее подчеркивание) Параметр обязателен для заполнения
«Комментарий»	Ввести информационное сообщение, используемое для описания назначения фонда
«Имя публикации»	Ввести текстовое наименование публикации. Параметр применяется для георазпределенной установки и позволяет отображать однообразные фонды РМ в виде единого ярлыка в компоненте «Клиент». Для этого на каждой из установок компонента «Универсальный диспетчер» в базовых настройках фонда следует задавать идентичное значение параметра. Параметр обязателен для заполнения
«Шаблон»	Выбрать из списка шаблон, который будет использоваться при создании
«Максимальное количество рабочих мест»	Задать максимальное количество РМ в фонде ⚠ При задании максимального количества стоит учитывать, что оно 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 45) после нажатия экранной кнопки **[Далее]**. Индикация цветом и сообщение не исчезнут после корректного заполнения поля.

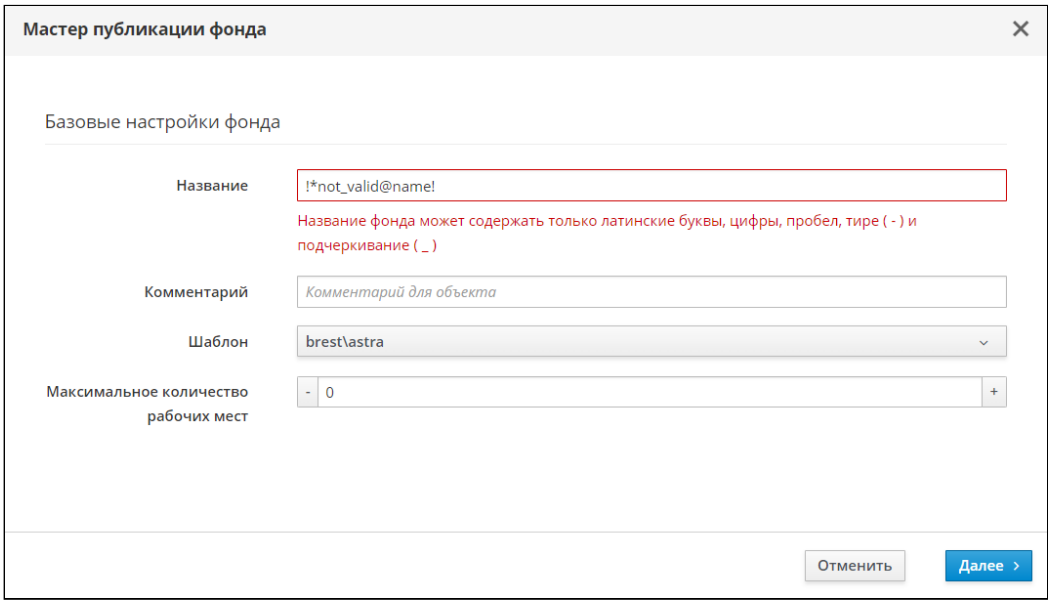

Рисунок 45 – Пример сообщения об ошибке

Далее будет выполнен переход на следующий шаг настройки (см. Рисунок 46) мастера публикации фонда, в котором нужно заполнить параметры, указанные в таблице (см. Таблица 74). 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.

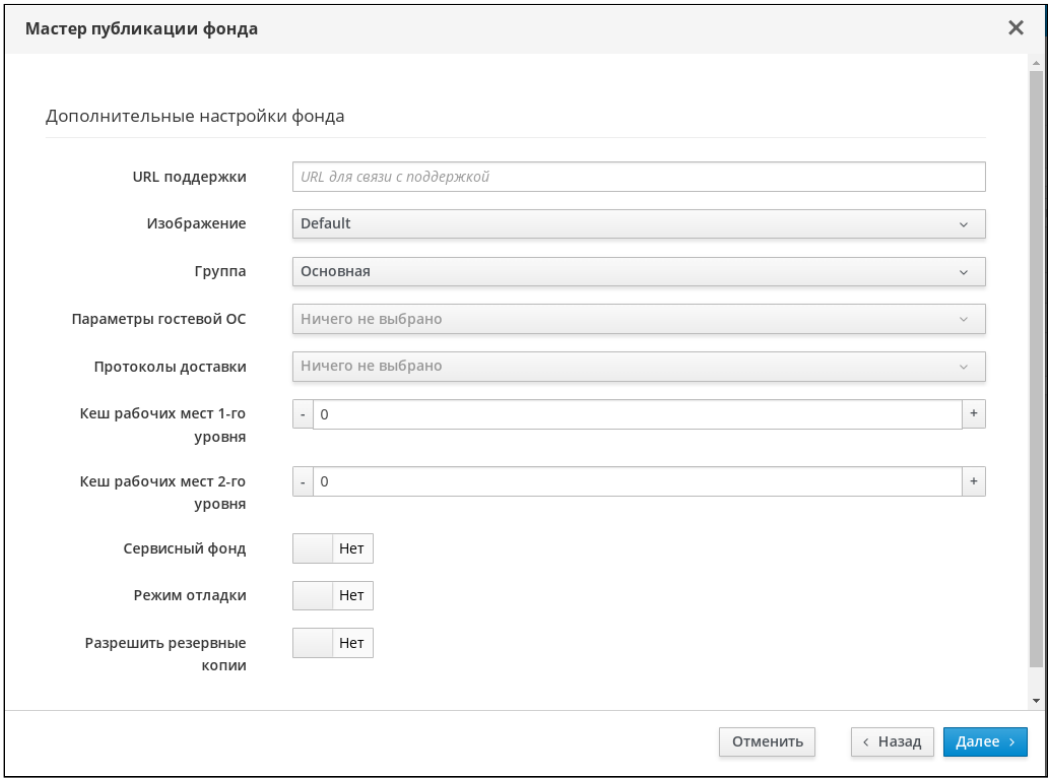

Рисунок 46 – Дополнительные настройки фонда Мастера публикации

Таблица 74 – Дополнительные настройки фонда

Параметр	Описание
«URL поддержки»	Ввести URL для связи с технической поддержкой. Адрес должен соответствовать стандарту кодирования URI. В случае задания некорректного URL, графический элемент для обращения в техническую поддержку в компоненте «Клиент» будет недоступен. Примеры схем для задания URL: ▪ `http(s)://termidesk.local/support`; ▪ `ws(s)://chat.termidesk.local`; ▪ `file:///home/support/help.html`; ▪ `mailto:support@termidesk.local`
«Изображение»	Выбрать графическое представление фонда
«Группа»	Выбрать группу рабочих мест, в которой будет отображаться созданный фонд
«Параметры гостевой ОС»	Выбрать параметры конфигурации гостевой ОС, которые будут использованы при создании РМ
«Протоколы доставки»	Выбрать один или несколько протоколов доставки, которые будут доступны для фонда
«Кеш рабочих мест 1-го уровня»	Задать количество созданных, настроенных и запущенных РМ в фонде ⚠ Параметр не задается, если создается фонд РМ для терминальных серверов.
«Кеш рабочих мест 2-го уровня»	Задать количество созданных, настроенных и выключенных РМ. Для использования кеша рабочих места 2-го уровня необходимо, чтобы в параметре «Кеш рабочих мест 1-го уровня» было задано хотя бы одно РМ ⚠ Параметр не задается, если создается фонд РМ для терминальных серверов.
«Сервисный фонд»	Активация использования фонда как **сервисного** для «метапоставщика»
«Режим отладки»	Активация более подробной детализации логов для фонда, по умолчанию режим отключен. При включении режима Termidesk перестает удалять ВМ в фонде
«Разрешить резервные копии»	Активация режима резервного копирования ВМ фонда при использовании системы Rubackup. По умолчанию режим отключен
«Доступ из связанных сетей»	⚠ Параметр недоступен, если создается сервисный фонд. Управление доступом пользователей из связанных сетей. Сети указываются в настройках фонда РМ после его создания. Возможные значения: ▪ «Разрешить» - все пользователи из указанных сетей смогут подключаться к фонду РМ; ▪ «Запретить» (по умолчанию) - всем пользователям из указанных сетей будет запрещено подключение к фонду РМ

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

Если был активирован параметр «Сервисный фонд», то мастер публикации отобразит шаг «Настройки ограничений по количеству интерактивных сессий» (см. Рисунок 47), в котором нужно заполнить параметры, указанные в таблице (см. Таблица 75).

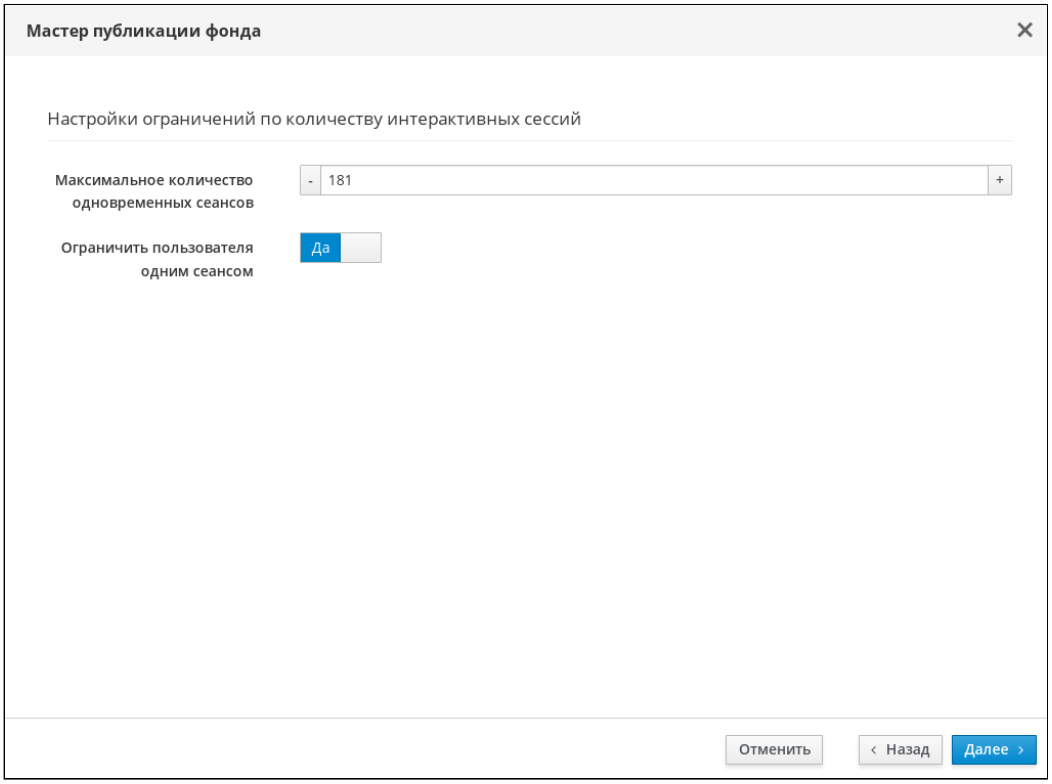

Рисунок 47 – Настройки ограничений для сервисного фонда

Таблица 75 – Настройки ограничений по количеству интерактивных сессий

Параметр	Описание
«Максимальное количество одновременных сеансов»	Задать количество одновременных сеансов на терминальном сервере. Параметр используется для ограничения количества одновременных сеансов на сервере. Максимальное количество сеансов ограничивается в соответствии с использующимся на терминальном сервере решением: ▪ STAL - 181 одновременных сеансов; ▪ MS RDSH - 250 одновременных сеансов. Ограничение количества сеансов повышает производительность, поскольку меньшее количество сеансов требует системных ресурсов. Значение по умолчанию: «181»

Параметр	Описание
«Ограничить пользователя одним сеансом»	Активация ограничения пользователей одним сеансом терминального сервера. При активации параметра пользователи, подключающиеся к ОС терминального сервера, будут ограничены одним сеансом (активным или отключенным) на этом сервере. Если пользователь покидает сеанс в отключенном состоянии, он автоматически подключается к этому сеансу при следующем входе в систему. При деактивации параметра пользователям будет разрешено устанавливать неограниченное количество одновременных сеансов на сервере. Значение по умолчанию: «Да»

После заполнения параметров 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 48) «Фонд успешно создан!», окно будет автоматически закрыто по истечении 3 секунд.

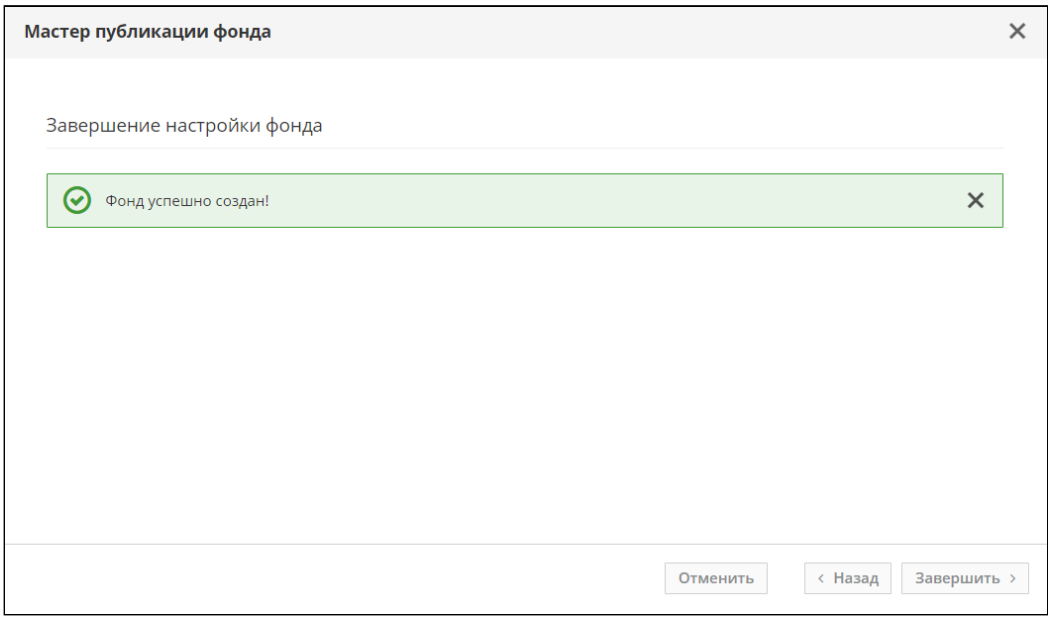

Рисунок 48 – Успешное завершение настройки публикации фонда

10.2.2 . Добавление фонда публикации служб «метапоставщика»

Для добавления фонда следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Создать]**, выбрать тип мастера публикации «Публикация служб Метапоставщика».

> Сервисный фонд для метапоставщика должен быть предварительно создан (см. подраздел **Предварительная настройка для добавления терминального сервера метапоставщика**).
> Хотя бы одно BPM из сервисного фонда должно получить статус «Действительный» во вкладке «Рабочие места».

Откроется мастер публикации фонда. Необходимо выбрать тип публикации (см. Рисунок 49):

- «Удаленный рабочий стол» - для публикации терминальной сессии;
- «Удаленное приложение» - для публикации приложения.

Затем нажать экранную кнопку **[Далее]**. Экранная кнопка **[Отменить]**, клавиша **<Esc>**, иконка «Крестик» на любом из этапов работы закрывает мастер без сохранения настроек.

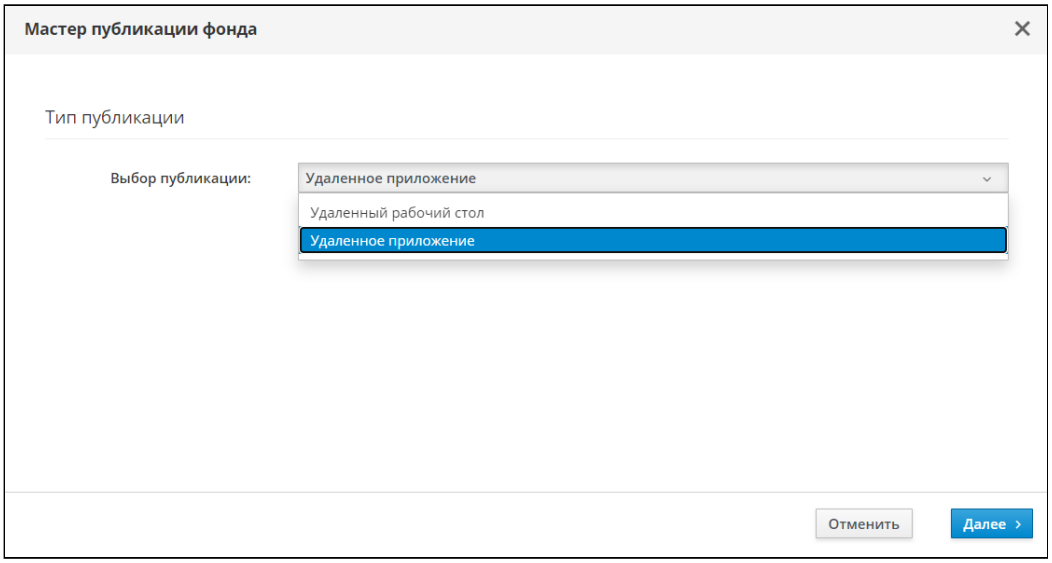

Рисунок 49 – Выбор типа публикации

Далее нужно выбрать (см. Рисунок 50) поставщик ресурсов с типом «Сервер Терминалов Метапоставщик» для публикации. Если он не был создан ранее, выбрать «Новый поставщик ресурсов» и заполнить параметры для его создания.

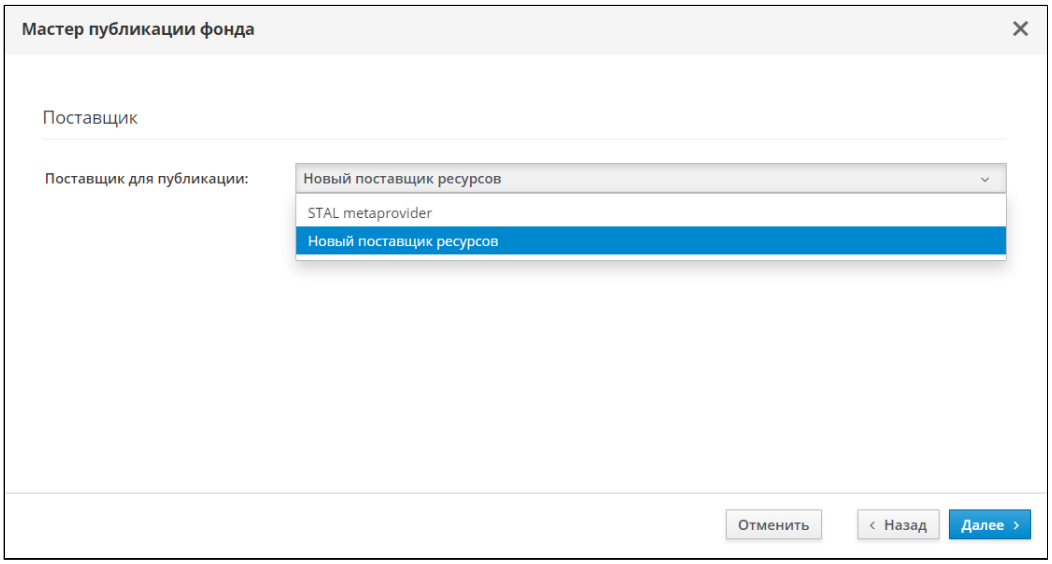

Рисунок 50 – Выбор метапоставщика для публикации

На следующем шаге (см. Рисунок 51) задать наименование приложения и выбрать приложение для публикации (если ранее был выбран тип публикации «Удаленное приложение»), или задать наименование терминальной сессии (если ранее был выбран тип публикации «Удаленный рабочий стол»).

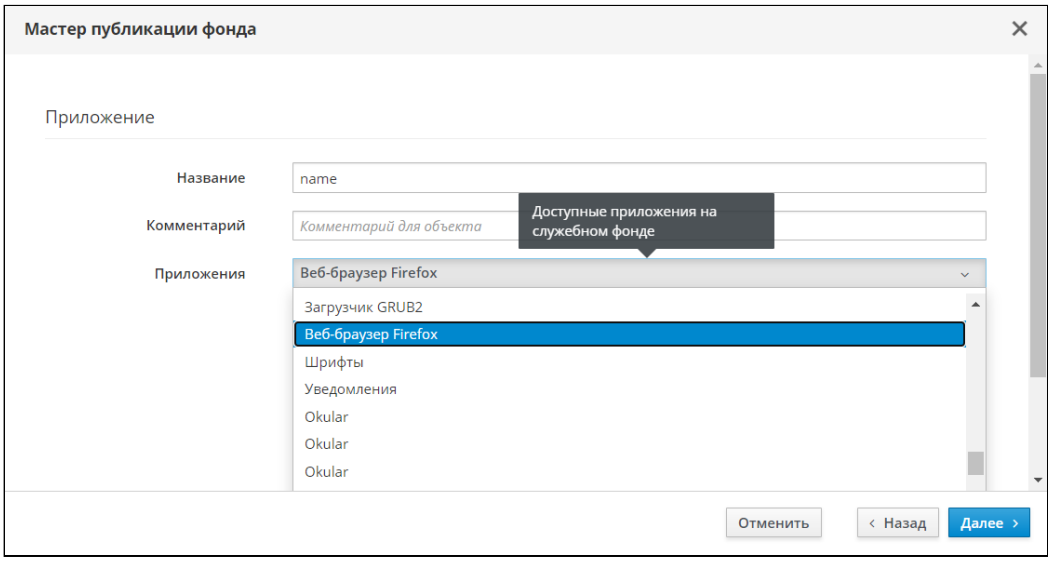

Рисунок 51 – Ввод наименования сессии или приложения

Далее будет выполнен переход на следующий шаг настройки мастера публикации фонда, в котором нужно заполнить параметры, указанные в таблице (см. Таблица 76).

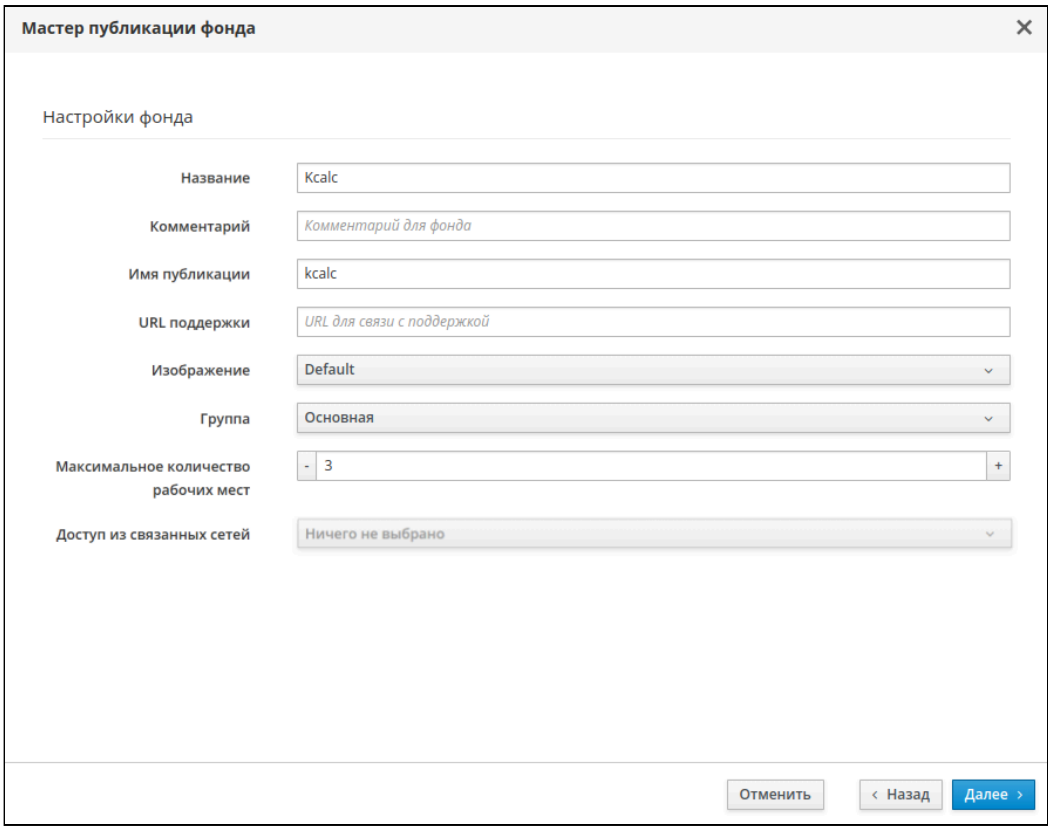

Рисунок 52 – Настройка фонда публикации служб метапоставщика

Таблица 76 – Настройки фонда публикации служб метапоставщика

Параметр	Описание
«Название»	Ввести текстовое наименование фонда

Параметр	Описание
«Комментарий»	Ввести информационное сообщение, используемое для описания назначения фонда
«Имя публикации»	Ввести текстовое наименование публикации. Параметр применяется для георасределенной установки и позволяет отображать однообразные фонды BPM в виде единого ярлыка в компоненте «Клиент». Для этого на каждой из установок компонента «Универсальный диспетчер» в базовых настройках фонда следует задавать идентичное значение параметра. Параметр обязателен для заполнения
«URL поддержки»	Ввести URL для связи с технической поддержкой. Адрес должен соответствовать стандарту кодирования URI. В случае задания некорректного URL, графический элемент для обращения в техническую поддержку в компоненте «Клиент» будет недоступен. Примеры схем для задания URL: ▪ `http(s)://termidesk.local/support`; ▪ `ws(s)://chat.termidesk.local`; ▪ `file:///home/support/help.html`; ▪ `mailto:support@termidesk.local`
«Изображение»	Выбрать графическое представление фонда
«Группа»	Выбрать группу РМ, в которой будет отображаться созданный фонд
«Максимальное количество рабочих мест»	Максимальное количество РМ в фонде. При достижении указанного предела BPM новые пользователи не смогут подключиться к фонду
«Доступ из связанных сетей»	Управление доступом пользователей из связанных сетей. Сети указываются в настройках фонда РМ после его создания. Возможные значения: ▪ «Разрешить» - все пользователи из указанных сетей смогут подключаться к фонду РМ; ▪ «Запретить» - всем пользователям из указанных сетей будет запрещено подключение к фонду РМ

На следующем шаге (см. Рисунок 53) задать домен аутентификации и группу пользователей, входящую в этот домен, которым будет доступен фонд. Для выбора будут доступны те домены аутентификации, для которых в параметре «Субъекты» задано значение «Пользователи» или «Все».

Шаг опционален: параметры можно добавить после завершения работы мастера публикации, в созданном фонде на странице «Рабочие места - Фонды».

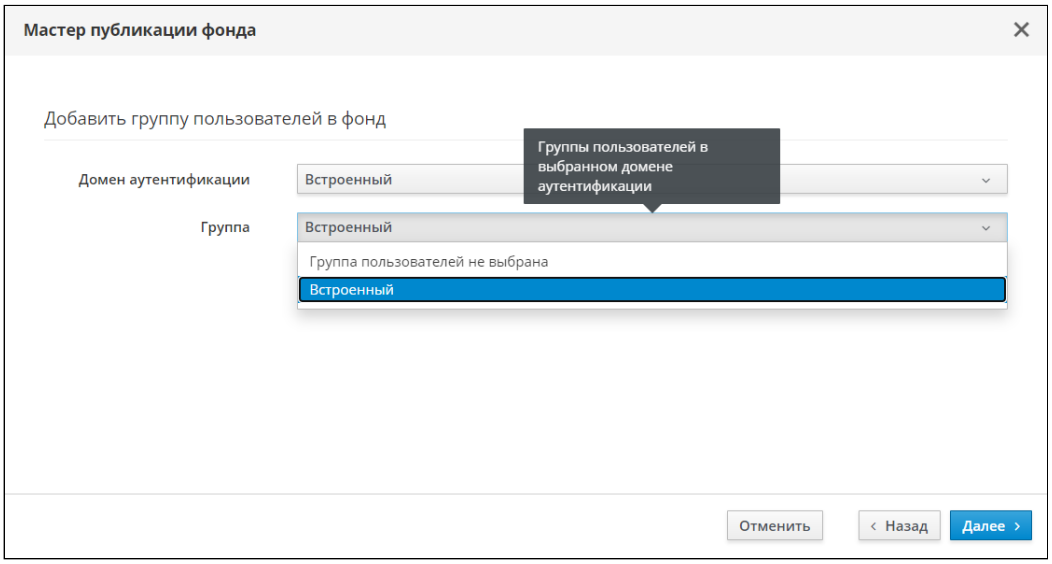

Рисунок 53 – Выбор домена аутентификации и группы пользователей

Затем выбрать (см. Рисунок 54) пользователя домена аутентификации. Шаг опционален: параметры можно добавить после завершения работы мастера публикации, в созданном фонде на странице «Рабочие места - Фонды».

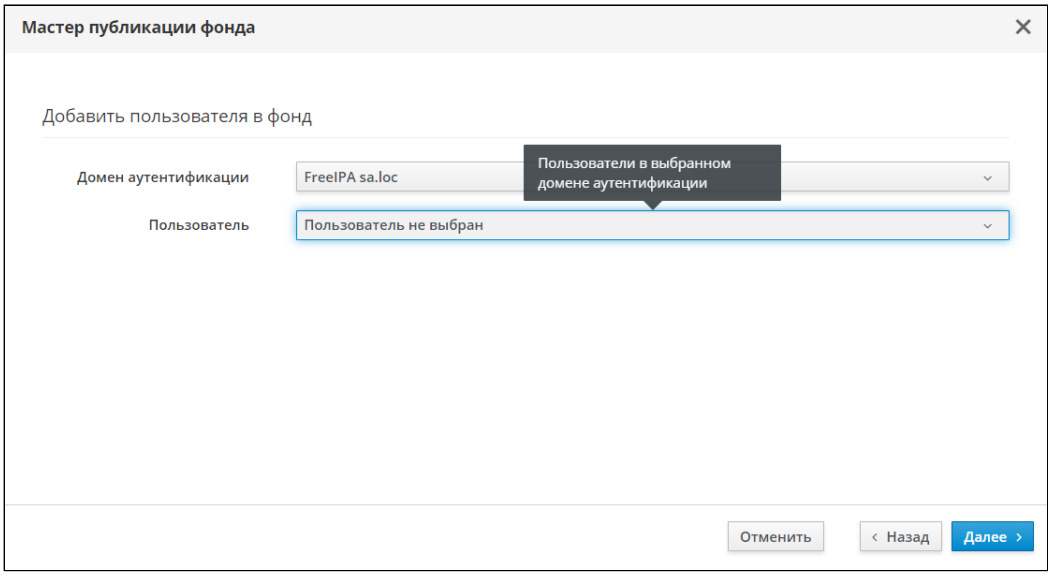

Рисунок 54 – Выбор пользователей

Далее выбрать (см. Рисунок 55) протокол доставки, который будет доступен для фонда. Если он не был создан ранее, выбрать «RDP (терминальный доступ)» и заполнить параметры для его создания (см. данные для добавления в подразделе **Подключение по протоколу RDP для доступа к ресурсам сервера терминалов**). Протокол доставки можно добавить и (или) изменить после завершения работы мастера публикации в созданном фонде на странице «Рабочие места - Фонды».

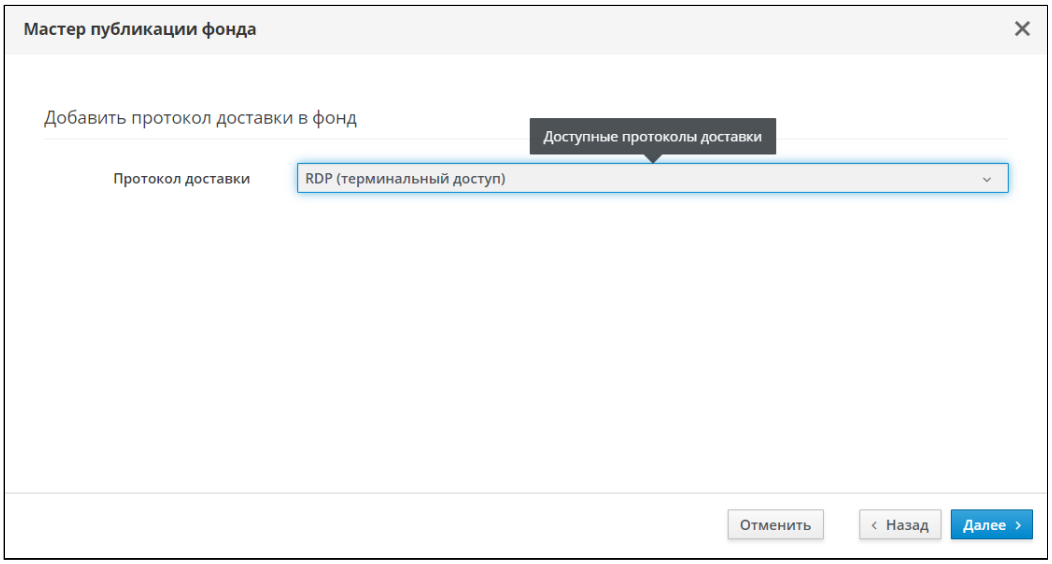

Рисунок 55 – Выбор протокола доставки

В следующем окне ознакомиться (см. Рисунок 56) с параметрами будущего фонда и завершить настройку, нажав экранную кнопку **[Завершить]**. Далее будет отображено временное окно с заблокированными экранными кнопками. При успешном создании фонда в этом же окне должно появиться сообщение «Фонд успешно создан!», окно будет автоматически закрыто по истечении 3 секунд.

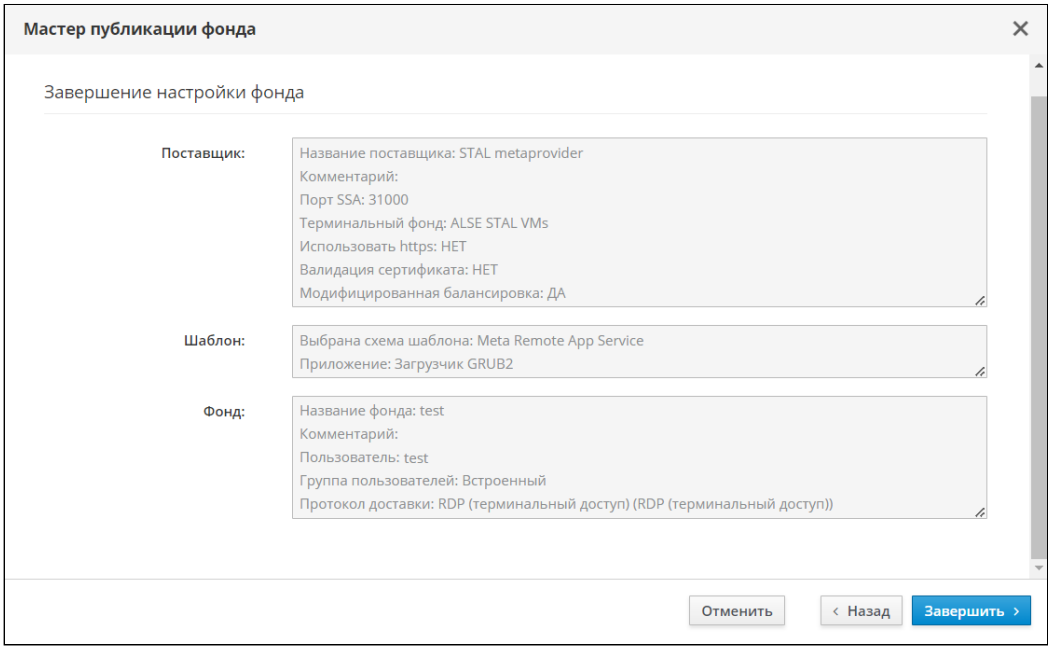

Рисунок 56 – Завершение настройки фонда

После успешного завершения работы мастера публикации информация о создании фонда, добавленных пользователях и их группах, протоколах доставки будет отображена в журнале фонда. Для просмотра журнала нужно перейти на страницу «Рабочие места - Фонды», выбрать наименование фонда и перейти во вкладку «Журнал».

10.2.3 . Добавление фонда автономных машин

Для добавления фонда автономных машин следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Создать]**, выбрать тип мастера публикации «Автономные машины».

Фонд автономных машин используется для публикации фонда, основанного на шаблонах автономных машин (см. подраздел **Шаблон РМ для автономной машины**).

Откроется мастер публикации фонда (см. Рисунок 57). Необходимо заполнить параметры, указанные в таблице, (см. Таблица 77) 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.

> ⚠ При создании фонда автономных машин нужно следовать правилу «Один шаблон - один фонд». Создание фондов с одинаковыми шаблонами не допускается.

Рисунок 57 – Базовые настройки фонда в Мастере публикации

Таблица 77 – Базовые настройки фонда

Параметр	Описание
«Название»	Ввести текстовое наименование фонда. Параметр обязателен для заполнения
«Комментарий»	Ввести информационное сообщение, используемое для описания назначения фонда
«Имя публикации»	Ввести текстовое наименование публикации. Параметр применяется для георасределенной установки и позволяет отображать однообразные фонды в виде единого ярлыка в компоненте «Клиент». Для этого на каждой из установок компонента «Универсальный диспетчер» в базовых настройках фонда следует задавать идентичное значение параметра. Параметр обязателен для заполнения
«Шаблон»	Выбрать из списка шаблон автономных машин, который будет использоваться при создании фонда. Выбор шаблонов, не относящихся к автономным машинам, не допускается. Параметр обязателен для заполнения

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

Далее будет выполнен переход на следующий шаг настройки (см. Рисунок 58) мастера публикации фонда, в котором нужно заполнить параметры, указанные в таблице (см. Таблица 78).

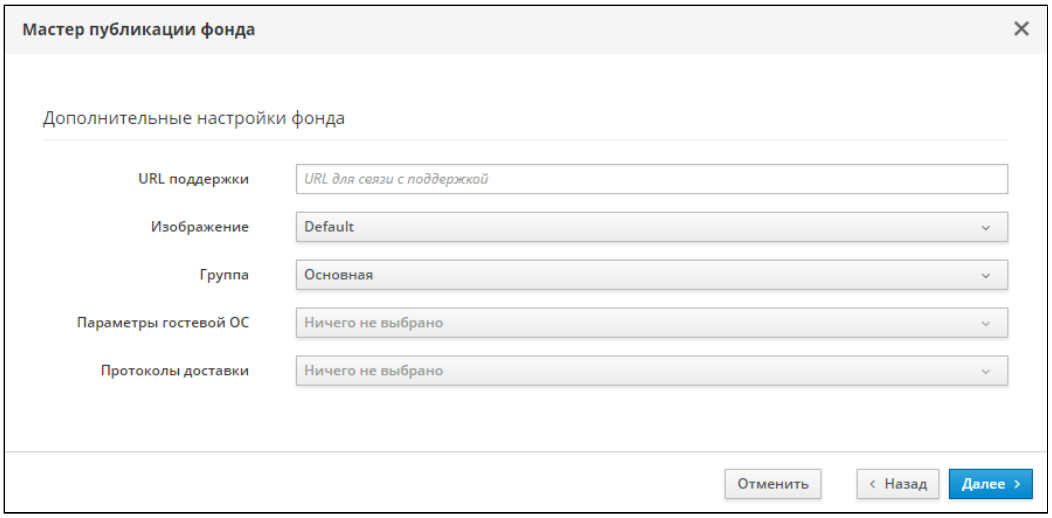

Рисунок 58 – Дополнительные настройки фонда Мастера публикации

Таблица 78 – Дополнительные настройки фонда

Параметр	Описание
«URL поддержки»	Ввести URL для связи с технической поддержкой. Адрес должен соответствовать стандарту кодирования URI. В случае задания некорректного URL, графический элемент для обращения в техническую поддержку в компоненте «Клиент» будет недоступен. Примеры схем для задания URL: ▪ `http(s)://termidesk.local/support`; ▪ `ws(s)://chat.termidesk.local`; ▪ `file:///home/support/help.html`; ▪ `mailto:support@termidesk.local`
«Изображение»	Выбрать графическое представление фонда
«Группа»	Выбрать группу РМ, в которой будет отображаться созданный фонд
«Параметры гостевой ОС»	Выбрать параметры конфигурации гостевой ОС автономных машин, которые будут использованы при создании фонда. Выбор параметров гостевой ОС, не относящихся к автономным машинам, не допускается
«Протоколы доставки»	Выбрать один или несколько протоколов доставки, которые будут доступны для фонда
«Сервисный фонд»	Активация использования фонда как **сервисного** для «метапоставщика»

Параметр	Описание
«Доступ из связанных сетей»	Управление доступом пользователей из связанных сетей. Сети указываются в настройках фонда РМ после его создания. Возможные значения: ▪ «Разрешить» - все пользователи из указанных сетей смогут подключаться к фонду РМ; ▪ «Запретить» - всем пользователям из указанных сетей будет запрещено подключение к фонду РМ

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

В следующем окне завершить настройку фонда, нажав экранную кнопку **[Завершить]**. При успешном создании фонда в этом же окне должно появиться сообщение (см. Рисунок 48) «Фонд успешно создан!», окно будет автоматически закрыто по истечении 3 секунд.

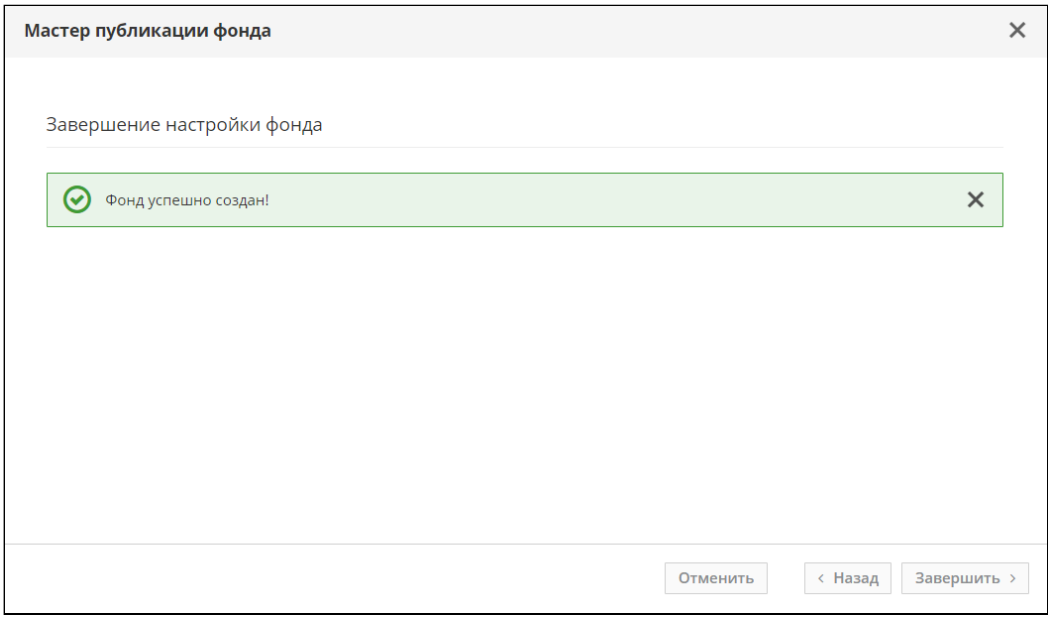

Рисунок 59 – Успешное завершение настройки публикации фонда

10.3 . Политики фонда РМ

Для управления доступом и ресурсами в фондах РМ используются следующие виды политик:

- глобальные - применяются ко всем фондам РМ и устанавливают общие настройки доступа и использования ресурсов пользователями РМ. Для редактирования глобальных политик следует перейти «Настройки - Глобальные политики», выбрать политику и нажать экранную кнопку **[Изменить]**;
- индивидуальные - переопределяют настройки глобальных политик и устанавливают индивидуальные настройки доступа и использования ресурсов пользователями конкретного фонда РМ. Для редактирования индивидуальных политик следует перейти «Рабочие места - Фонды», выбрать нужный фонд РМ, нажать экранную кнопку **[Политики]**, выбрать политику и нажать экранную кнопку **[Изменить]**.

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

Во время обновления распределенной или отказоустойчивой конфигурации установки изменение политик нужно проводить после обновления на новую версию всех узлов Termidesk.
Если на ВРМ есть сессия пользователя, то политика применится после перезагрузки ВМ. Для терминального сервера перезагрузка обязательна!

Администратор должен включить соответствующие политики фонда РМ для перенаправления ресурсов, если при подключении к РМ пользователь использует ПО Termidesk Viewer. При подключении пользователя по протоколу RDP из компонента «Клиент» могут использоваться стандартные утилиты ОС, в этом случае возможность перенаправления регулируется на уровне протокола доставки.
Политики, применимые к протоколу RDP, запрашиваются компонентом «Агент виртуального рабочего места» перед подключением пользователя к ВРМ по указанному протоколу и обновляются в реестре ОС в случае, если это гостевая ОС Microsoft Windows.

Список доступных политик представлен в таблице (см. Таблица 79).

Таблица 79 – Перечень доступных политик фонда РМ

Название политики	Описание
«Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)»	Политика определяет, должен ли пользователь вводить логин и пароль на РМ при запуске рабочих столов. Применимость: ▪ ВРМ (SPICE, RDP, TERA); ▪ автономные машины (RDP). В ОС РМ при этом должна быть выполнена настройка технологии единого входа. Возможные значения: ▪ «Выключен» (по умолчанию) - учетные данные будут запрашиваться; ▪ «Включен» - запрос учетных данных не происходит

Название политики	Описание
«Буфер обмена (RDP, SPICE, TERA)»	Управление использованием буфера обмена в протоколах RDP и SPICE. Применимость: ▪ BPM (SPICE, RDP); ▪ автономные машины (RDP); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ публикованные приложения метапоставщика STAL. Возможные значения: ▪ «Выключить перенаправление буфера»; ▪ «Двустороннее перенаправление буфера» (по умолчанию); ▪ «Перенаправление буфера только от сервера клиенту»; ▪ «Перенаправление буфера только от клиента серверу»
«Выбор пользователем протокола доставки»	Определяет, может ли пользователь выбрать протокол доставки для подключения к РМ. Политика применяется как при подключении пользователя через веб-браузер, так и при подключении из компонента «Клиент». Возможные значения: ▪ «Разрешен» (по умолчанию) - пользователь может выбирать протокол доставки при подключении к ресурсу; ▪ «Запрещен» - пользователю будет доступен только один протокол доставки: либо высокоприоритетный, либо, если приоритет одинаков, первый по алфавиту

Название политики	Описание
«Действие при выходе пользователя из ОС»	Определяет действие после выхода пользователя из ОС. Применимость: ВРМ (RDP, SPICE, TERA). Политика неприменима для метапоставщика и будет проигнорирована для сервисного фонда. Возможные значения: ▪ «Не задано» (по умолчанию); ▪ «Удалять рабочее место» - ВМ будет удалена. Периодичность проверки наличия назначенных, но неиспользуемых РМ для последующего их удаления, составляет 631 секунду; ▪ «Не сохранять изменения» - ВМ будет возвращена к ранее созданному снимку. Значение политики применимо для фондов, основанных на шаблонах «Связанный клон oVirt/RHEV», «Связанный клон» или «Полный клон» VMware vSphere; ▪ «Не сохранять изменения и назначение ВРМ» - ВМ будет перезагружена с возвратом к ранее созданному снимку (если он поддерживается для диска ВМ), назначение пользователя на ВРМ будет удалено. Значение политики применимо для фондов, основанных на шаблонах «Связанный клон» или «Полный клон» VMware vSphere. При применении значений в индивидуальных политиках фонда РМ может быть выведено уведомление «Данное значение политики не применимо к выбранному фонду», если у поставщика ресурсов фонда РМ нет возможности создавать снимки ВМ
«Действие с ВРМ в кеше 2-го уровня»	Определяет состояние ВРМ в кеше второго уровня. Политика распространяется на платформы виртуализации, которые поддерживают приостановку ВМ: ▪ ПК СВ Брест; ▪ oVirt; ▪ zVirt; ▪ «РЕД Виртуализация»; ▪ VMware vSphere. Возможные значения: ▪ «Выключить машину после публикации» - ВРМ будут выключены после завершения их подготовки (после перехода в статус «Действительный»); ▪ «Приостановить машину после публикации» (по умолчанию) - ВРМ будут приостановлены после завершения их подготовки (после перехода в статус «Действительный»). Изменение значения учитывается для новых ВРМ, создаваемых в кеше второго уровня. ВРМ, уже находящиеся в кеше второго уровня, не будут принудительно переводиться в другое состояние

Название политики	Описание
«Завершение сеанса при достижении лимита времени (RDP)»	Политика определяет, будет ли сессия пользователя сразу завершена (logoff) по истечении заданных лимитов времени, а не отключена (disconnect). Применимость: ▪ BPM (RDP, SPICE, TERA); ▪ автономные машины (RDP, TERA); ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена. Возможные значения: ▪ «Не задано»; ▪ «Выключено» (по умолчанию); ▪ «Включено»
«Интервал мониторинга кеша перемещаемых профилей пользователей (RDP)»	Политика позволяет ограничить интервал мониторинга (в минутах) размера кеша перемещаемых профилей пользователей для протокола RDP. Политика действует на ОС Microsoft Windows. Политика определяет, как часто проверяется размер всего кеша перемещаемых профилей пользователей, указанный в политике «Ограничить размер полного кеша перемещаемых профилей пользователей (RDP)». При изменении политики требуется перезагрузка ВМ или терминальных серверов. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP); ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS. Возможные значения (в минутах): от 15 до 10080. Значение по умолчанию: «900»
«Использование веб-камеры в сеансе Удалённого Помощника»	Политика позволяет разрешить или запретить использование видеокамеры. Политика действует для всех сессий «Удаленного помощника». Возможные значения: ▪ «Разрешено»; ▪ «Запрещено» (по умолчанию)
«Использование аудиосвязи в сеансе Удалённого Помощника»	Политика позволяет разрешить или запретить использование микрофона (голосового чата) и звука. Политика действует для всех сессий «Удаленного помощника». Возможные значения: ▪ «Разрешено»; ▪ «Запрещено» (по умолчанию)

Название политики	Описание
«Перенаправление USB-устройств посредством RemoteFX (RDP)»	Политика активации механизма RemoteFX для протокола RDP. Если необходимо активировать возможность перенаправления USB-устройств из пользовательской рабочей станции в РМ, нужно установить политике значение «Включен». Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP). Возможные значения: ▪ «Запрещено» (по умолчанию); ▪ «Разрешено»
«Использование обязательных профилей на сервере узла сеанса удаленных рабочих столов (RDP)»	Политика позволяет указать, используют ли службы удаленных рабочих столов обязательный профиль для всех пользователей, удаленно подключающихся к серверу узла сеанса удаленных рабочих столов. Политика действует на ОС Microsoft Windows. При включении политики службы удаленных рабочих столов используют путь, указанный в политике «Путь для перемещаемого профиля пользователя служб удаленного рабочего стола (RDP)», в качестве корневого каталога для обязательного профиля пользователя. Все пользователи, удаленно подключающиеся к серверу узла сеансов удаленных рабочих столов, используют один и тот же профиль пользователя. При отключении политики обязательные профили пользователей не будут использоваться пользователями, удаленно подключающимися к серверу узла сеанса удаленных рабочих столов. При изменении политики требуется перезагрузка ВМ или терминальных серверов. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP); ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS. Возможные значения: ▪ «Запрещено» (по умолчанию); ▪ «Разрешено»

Название политики	Описание
«Лимит времени для активных сеансов (RDP, SPICE, TERA)»	Политика задает максимальное время для активного сеанса, по истечении которого он будет отключен (disconnect). Для BPM с ОС Microsoft Windows действие политики (завершение сеанса вместо его отключения) может быть изменено через: ▪ «Завершение сеанса при достижении лимита времени (RDP)»; ▪ «Лимит времени для отключенных сеансов (RDP)». ⚠ Для BPM с ОС Linux данная политика будет всегда завершать сеанс, а не отключать его. Политика распространяется на компонент «Агент виртуального рабочего места». Применимость: ▪ BPM (RDP, SPICE, TERA); ▪ автономные машины (RDP, TERA); ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. ⓘ Для BPM с ОС Microsoft Windows политика применяется в момент авторизации пользователя в ОС. Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена MS AD. Возможные значения: ▪ «Нет ограничений» (по умолчанию; сессии будут оставаться активными без ограничений по времени); ▪ «Не задано»; ▪ выбор: «1 мин», «5 мин», «10 мин», «15 мин», «30 мин», «1 час», «2 часа», «3 часа», «6 часов», «8 часов», «12 часов», «16 часов», «18 часов», «1 день», «2 дня», «3 дня», «4 дня», «5 дней»

Название политики	Описание
«Лимит времени для выхода из сеансов RemoteApp (RDP)»	Политика позволяет указать, как долго сеанс пользователя при использовании RemoteApp (удаленного приложения) будет оставаться активным после закрытия всех программ RemoteApp. Если в течение указанного времени пользователь не запустит другое приложение RemoteApp, то сеанс завершится. Политика распространяется на компонент «Агент виртуального рабочего места» и действует для подключений по протоколу RDP к терминальному серверу метапоставщика MS RDS. Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена MS AD. Если заданы другие политики с лимитами времени, то будет использоваться та, в которой задан более короткий период. Возможные значения: ▪ «Никогда» (по умолчанию; при закрытии приложения сеанс будет отключен, но не завершен); ▪ «Сразу»; ▪ «Не задано»; ▪ выбор: «1 мин», «5 мин», «10 мин», «15 мин», «30 мин», «1 час», «2 часа», «3 часа», «6 часов», «8 часов», «12 часов», «16 часов», «18 часов», «1 день», «2 дня», «3 дня», «4 дня», «5 дней»
«Лимит времени для отключенных сеансов (RDP)»	Политика задает максимальное время, по истечении которого отключенная (disconnect) сессия будет завершена (logoff). Политика распространяется на компонент «Агент виртуального рабочего места». Работает совместно с политикой «Завершение сеанса при достижении лимита времени (RDP)». Применимость: ▪ BPM (RDP, TERA); ▪ автономные машины (RDP, TERA); ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена MS AD. Возможные значения: ▪ «Нет ограничений» (по умолчанию; сессия останется незавершенной без ограничения по времени); ▪ «Не задано»; ▪ выбор: «1 мин», «5 мин», «10 мин», «15 мин», «30 мин», «1 час», «2 часа», «3 часа», «6 часов», «8 часов», «12 часов», «16 часов», «18 часов», «1 день», «2 дня», «3 дня», «4 дня», «5 дней»

Название политики	Описание
«Максимальное количество устаревших шаблонов связанных клонов»	Политика определяет количество служебных шаблонов, хранящихся для каждого из фондов РМ. Служебный шаблон - это шаблон, используемый для создания РМ и размещаемый на платформе виртуализации. Если достигнуто заданное максимальное количество, то: ▪ возможность новой публикации фонда РМ будет заблокирована; ▪ для новой публикации нужно удалить некоторые существующие РМ или задать новое значение политике. ⚠ Если будут удалены все РМ, принадлежащие служебному шаблону, то удалится и сам шаблон. При значении «-1» максимальное количество служебных шаблонов не ограничивается. Возможные значения: от -1 до 100. Значение по умолчанию: «10»
«Масштабирование экрана (RDP)»	Политика управления масштабированием экрана для протокола RDP. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP). Возможные значения: ▪ «Выключено» (по умолчанию); ▪ «Включено»

Название политики	Описание
«Аутентификация на уровне сети (RDP)»	Политика позволяет выбрать уровень безопасности для протокола RDP. Выбранный уровень безопасности влияет на способ запроса учетных данных пользователя. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «Автосогласование» (по умолчанию). Используется для автоматического согласования уровня безопасности. Этот параметр может не передаваться для некоторых программ доставки, поэтому следует учесть ограничения, приведенные ниже; ▪ «RDP». Этот уровень безопасности не требует предварительной аутентификации пользователя до начала подключения по протоколу RDP; ▪ «TLS». Используется для защиты подключения пользователя. Этот уровень безопасности преобразует передаваемые учетные данные пользователя в RDP-сессии для их сокрытия от злоумышленника, но при этом не требует предварительной аутентификации до начала подключения по протоколу RDP; ▪ «NLA». Применяется только для ОС Microsoft Windows. Этот уровень безопасности предполагает, что пользователь должен быть аутентифицирован до начала подключения по протоколу RDP. Для NLA требуются, чтобы были переданы полные учетные данные пользователя для подключения. Ограничения для фондов: ▪ для работы подключения к фондам терминальных серверов должны использоваться: • для STAL значения «TLS» или «RDP»; • для MS RDS значение «NLA»; ▪ для фондов BPM, если пользователь использует программу доставки ПО Termidesk Viewer: • для подключения с ОС Microsoft Windows к BPM ОС Astra Linux Special Edition необходимо использовать значения «Автосогласование» или «TLS»; • для подключения с ОС Astra Linux Special Edition к BPM ОС Astra Linux Special Edition необходимо использовать значения «Автосогласование», или «RDP», или «TLS»

Название политики	Описание
«Ограничение полосы пропускания видеоканала (TERA)»	Политика позволяет ограничить полосу пропускания видеоканала при передаче экрана BPM по протоколу TERA. Значение указывается в килобитах в секунду. Применимость: ▪ BPM (TERA); ▪ автономные машины (TERA). Значение по умолчанию: «0» (без ограничений)
«Ограничение полосы пропускания копирования файлов (TERA)»	Политика позволяет ограничить полосу пропускания при копировании файлов по протоколу TERA. Значение указывается в килобитах в секунду. Применимость: ▪ BPM (TERA); ▪ автономные машины (TERA). Значение по умолчанию: «0» (без ограничений)
«Ограничение размера буфера обмена (RDP, SPICE, TERA)»	Политика позволяет ограничить размер буфера обмена, доступный в обе стороны (от клиента к серверу и от сервера к клиенту). Значение указывается в килобайтах. Если размер передаваемых данных превышает заданный лимит, то будет передан только объем данных, соответствующий установленному лимиту. Для совместимости с предыдущими версиями программы доставки ПО Termidesk Viewer используется значение по умолчанию. Применимость: ▪ BPM (RDP, SPICE, TERA); ▪ автономные машины (RDP, TERA); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Значение по умолчанию: «0» (без ограничений)

Название политики	Описание
«Ограничение размера кеша перемещаемых профилей пользователей (RDP)»	Политика позволяет ограничить размер всего кеша перемещаемых профилей пользователей на локальном диске. Политика действует на ОС Microsoft Windows. Для политики необходимо указать максимальный размер (в гигабайтах) для всего кеша перемещаемых профилей пользователей. Когда размер всего кеша перемещаемых профилей пользователей превысит указанную величину, самые давние по времени использования перемещаемые пользователей будут удаляться до тех пор, пока размер всего кеша перемещаемых профилей пользователей не станет меньше этого максимального размера. При изменении политики требуется перезагрузка ВМ или терминальных серверов. Зависит от политики «Интервал мониторинга кеша перемещаемых профилей пользователей (RDP)». Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP); ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS. Возможные значения (в гигабайтах): от 5 до 10000. Значение по умолчанию: «600»
«Ограничение разрешенных форматов буфера обмена (RDP, SPICE, TERA)»	Политика позволяет ограничить разрешенные форматы записи в буфер обмена «Клиента», сами форматы задаются в политике «Разрешенные форматы буфера обмена (RDP, SPICE, TERA)». Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена. Для совместимости с предыдущими версиями программы доставки ПО Termidesk Viewer используется значение по умолчанию. Применимость: ▪ BPM (RDP, SPICE); ▪ автономные машины (RDP); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «Не задано» (по умолчанию); ▪ «Выключено»; ▪ «Включено»
«Отделяемый пользовательский профиль»	Использование отделяемого пользовательского профиля в BPM. Политика применяется при старте BPM. Применимость: BPM (RDP, SPICE, TERA). Возможные значения: ▪ «Выключен» (по умолчанию); ▪ «Включен»

Название политики	Описание
«Передача файлов (SPICE, TERA)»	Управление передачей файлов в протоколе SPICE и TERA. Применимость: BPM (SPICE, TERA). Возможные значения: ▪ «Разрешена» (по умолчанию); ▪ «Запрещена»

Название политики	Описание
«Правила фильтрации перенаправления USB-устройств по PID/VID (RDP, SPICE)»	Управление параметрами перенаправления USB-устройств с возможностью их фильтрации по параметрам: «Vendor ID» (VID), «Product ID» (PID), класс устройства, его версия. Применимость: ▪ BPM (RDP, SPICE); ▪ автономные машины (RDP); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS. Возможные значения: ▪ «0» (по умолчанию) - запрещено перенаправление всех устройств; ▪ «1» - разрешено перенаправление всех устройств; ▪ «A,B,C,D,E|.....|R,S,T,U,V» - перенаправление устройств в соответствии с фильтром. Каждые пять параметров, разделенных символом «|», составляют один фильтр. Число таких фильтров может быть произвольным. Правила составления фильтра USB-устройств: ▪ параметры разделяются запятыми (без пробелов); ▪ первый параметр (A) - класс USB-устройства. Может указываться как в шестнадцатеричном, так и в десятичном формате. Например: • «0x01» (шестнад.), «01» (десятич.) - аудиоустройства; • «0x02» (шестнад.), «02» (десятич.) - устройства связи, коммуникации. Например: модем; • «0x03» (шестнад.), «03» (десятич.) - устройства взаимодействия. Например: клавиатура, мышь; • «0x06» (шестнад.), «06» (десятич.) - устройства получения статичных изображений. Например: сканер; • «0x07» (шестнад.), «07» (десятич.) - принтеры; • «0x08» (шестнад.), «08» (десятич.) - запоминающие устройства. Например: внешний жесткий диск, флеш-накопитель; • «0x09» (шестнад.), «09» (десятич.) - концентраторы; • «0x0b» (шестнад.), «11» (десятич.) - смарт-карты; • «0x0E» (шестнад.), «15» (десятич.) - видеоустройства; ▪ второй параметр (B) - идентификатор производителя, VID. Может указываться как в шестнадцатеричном, так и в десятичном формате; ▪ третий параметр (C) - идентификатор продукта, PID. Может указываться как в шестнадцатеричном, так и в десятичном формате; ▪ четвертый параметр (D) - версия продукта. Может указываться как в шестнадцатеричном, так и в десятичном формате; ▪ пятый параметр (E) - разрешить («1») или запретить («0») перенаправление USB-устройства. Для всех параметров, кроме последнего: ▪ поддерживается использование «-1» - разрешено любое значение для параметра;

Название политики	Описание
	▪ разрядность чисел ограничена 16 битами. Пример задания правила для двух фильтров: разрешение аудиоустройств любых вендоров, продуктов и версий и запрет принтера с определенным идентификатором производителя: «0x01,-1,-1,-1,1|0x07,0xffff,-1,-1,0»
«Перенаправление веб-камеры (RDP, SPICE, TERA)»	Управление перенаправлением видеокамеры для протоколов RDP, SPICE и TERA. Применимость: ▪ BPM (RDP, SPICE, TERA); ▪ автономные машины (RDP, TERA). Возможные значения: ▪ «Разрешено» (по умолчанию); ▪ «Запрещено»
«Перенаправление смарт-карт (RDP, SPICE, TERA)»	Управление перенаправлением смарт-карт для протоколов RDP, SPICE, TERA. Ранее в версии Termidesk 5.0 для протокола RDP существовала отдельная политика «Политика управления перенаправлением смарт-карт (RDP)», в версии Termidesk 5.1 она была заменена на общую для протоколов SPICE и RDP политику. Применимость: ▪ BPM (RDP, SPICE, TERA); ▪ автономные машины (RDP, TERA); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «Разрешено» (по умолчанию); ▪ «Запрещено»
«Подключение с отличающимся именем пользователя»	⚠ Для работы политики необходимо, чтобы в гостевой ОС BPM была настроен модуль PAM (см. подраздел **Настройка модуля PAM без монтирования перемещаемых профилей**). Политика управления подключением пользователя к ВМ. Применяется в случае, если вводимый в ВМ логин отличен от логина, введенного пользователем при аутентификации в Termidesk. Применимость: ▪ BPM (SPICE, TERA); ▪ автономные машины (TERA). Возможные значения: ▪ «Разрешено»; ▪ «Запрещено» (по умолчанию)

Название политики	Описание
«Показ обоев рабочего стола (RDP)»	Управление отображением обоев рабочего стола РМ для протокола RDP. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP); ▪ терминальные сессии MS RDS; ▪ терминальные сессии метапоставщика MS RDS. Возможные значения: ▪ «Разрешен» - обои будут отображены; ▪ «Запрещен» (по умолчанию) - обои не будут отображаться
«Время простоя рабочего места (RDP, SPICE, TERA)»	Разрешенное время простоя РМ (отсутствуют действия пользователя с мышью и клавиатурой) в секундах. По достижении указанного времени сеанс будет отключен (disconnect). Политика распространяется на компонент «Агент виртуального рабочего места». Применимость: ▪ BPM (RDP, TERA); ▪ автономные машины (RDP, TERA). Значение «-1» означает неограниченное время простоя. Значение по умолчанию: «-1»
«Автоматическое подключение USB-устройств (RDP)»	Управление возможностью автоматически перенаправлять устройства для протокола RDP. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP). Возможные значения: ▪ «Не используется» (по умолчанию); ▪ «Разрешить автоподключение»; ▪ «Запретить автоподключение»

Название политики	Описание
«Глубина цвета (RDP)»	Управление максимально допустимым количеством цветов, отображаемых экраном РМ, для протокола RDP. Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена. Для подключения к STAL через стандартную утилиту Windows `mstsc` необходимо использовать значение «32 бит». Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «15 бит»; ▪ «16 бит» (по умолчанию); ▪ «24 бит»; ▪ «32 бит»; ▪ «Не задано»
«Композиция рабочего стола (RDP)»	Управление отображением художественных эффектов рабочего стола. Для корректного отображения художественных эффектов в параметре «Глубина цвета (RDP)» требуется установить значение «32 бита». Политика применяется только при подключении по протоколу RDP к гостевой ОС Microsoft Windows. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP). Возможные значения: ▪ «Разрешена»; ▪ «Запрещена» (по умолчанию)

Название политики	Описание
«Многомониторный режим (RDP, SPICE, TERA)»	Управление многомониторным режимом при подключении к РМ по протоколам RDP, SPICE, TERA. Политика влияет на возможность пользователя использовать экран РМ на нескольких физических мониторах. Применимость: ▪ BPM (RDP, SPICE, TERA); ▪ автономные машины (RDP, TERA); ▪ терминальные сессии STAL; ▪ терминальные сессии MS RDS; ▪ терминальные сессии метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL. ⚠ При подключении к STAL через стандартную утилиту ОС Microsoft Windows (`mstsc.exe`) включать политику не рекомендуется. При подключении к BPM с ОС Astra Linux Special Edition или к STAL через стандартную утилиту ОС Linux (`xfreerdp`) рекомендуется использовать мониторы с одинаковым разрешением экрана. При подключении к STAL рекомендуется использовать конфигурацию, при которой основной монитор расположен слева от остальных. Возможные значения: ▪ «Разрешен» - будет поддерживаться возможность вывода экрана РМ на нескольких дополнительных физических мониторах (если они подключены). При этом вариант использования экрана может быть различен в зависимости от дополнительных настроек программы доставки (см. подраздел **Выбор монитора** документа СЛЕТ.10001-01 92 01 «Руководство пользователя. Установка и эксплуатация компонента «Клиент»): дублирование, растяжение экрана и др.; ▪ «Запрещен» (по умолчанию) - экран РМ будет выведен только на основном физическом мониторе, вариант использования которого может быть различен в зависимости от дополнительных настроек параметров в ОС

Название политики	Описание
«Перенаправление принтеров (RDP, SPICE, TERA)»	Управление перенаправлением принтеров. Можно запретить перенаправление, разрешить перенаправлять все принтеры или только выбранные пользователем. Применимость: ▪ BPM (RDP, SPICE, TERA); ▪ автономные машины (RDP, TERA); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «Не перенаправлять» (по умолчанию); ▪ «Перенаправлять все»; ▪ «Перенаправлять выбранные пользователем»
«Перенаправление дисков и папок (RDP, SPICE, TERA)»	Управление перенаправлением дисков и каталогов. Применимость: ▪ BPM (RDP, SPICE, TERA); ▪ автономные машины (RDP, TERA); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «Разрешено»; ▪ «Запрещено» (по умолчанию) ⚠ В Termidesk версии 5.1 перенаправление дисков и каталогов выполняется всегда.

Название политики	Описание
«Перенаправление домашнего каталога пользователя»	Управление перенаправлением домашнего каталога пользователя в РМ. ⚠ Политика зависит от значения, заданного в политике «Перенаправление дисков и папок (RDP, SPICE, TERA)»: ▪ если задано «Разрешено», то будет учтено значение политики «Перенаправление домашнего каталога пользователя»; ▪ если задано «Запрещено», то перенаправление будет запрещено при любом значении политики «Перенаправление домашнего каталога пользователя». Применимость: ▪ BPM (RDP, SPICE, TERA); ▪ автономные машины (RDP, TERA); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «Разрешено» - при подключении пользователя к РМ его домашний каталог из пользовательской рабочей станции будет перенаправлен в РМ с правами на чтение и запись; ▪ «Запрещено» (по умолчанию)
«Перенаправление воспроизведения и записи звука (RDP)»	Управление перенаправлением звука в протоколе RDP. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «Не используется» (по умолчанию); ▪ «Разрешено»; ▪ «Запрещено»
«Перенаправление последовательных портов (RDP)»	Управление перенаправлением последовательных портов для протокола RDP. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP). Возможные значения: ▪ «Разрешено»; ▪ «Запрещено» (по умолчанию)

Название политики	Описание
«Сглаживание шрифтов (RDP)»	Управление сглаживанием шрифтов, отображаемых экраном РМ, для протокола RDP. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «Разрешено» (по умолчанию); ▪ «Запрещено»
«Сжатие данных (RDP)»	Управление использованием сжатия данных при взаимодействии с РМ по протоколу RDP. Если политика имеет значение «Не задано», то она не будет применяться на РМ, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «Включено» (по умолчанию); ▪ «Выключено»; ▪ «Не задано»

Название политики	Описание
«Тип сети (RDP)»	Управление типом сетевого подключения, используемого при подключении к РМ по протоколу RDP. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «Модем»; ▪ «Низкоскоростное широкополосное подключение»; ▪ «Широкополосное подключение»; ▪ «Высокоскоростное широкополосное подключение»; ▪ «Глобальная сеть»; ▪ «Локальная сеть»; ▪ «Авто» (по умолчанию)
«Уровень сжатия (RDP)»	Управление уровнем сжатия данных, при взаимодействии с РМ по протоколу RDP. Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «0»; ▪ «1» (по умолчанию); ▪ «2»; ▪ «Не задано»
«Полноэкранный режим (SPICE, TERA)»	Управление работой в полноэкранном режиме для протоколов SPICE и TERA. Применимость: BPM (SPICE, TERA). Возможные значения: ▪ «Включен» (по умолчанию); ▪ «Выключен»

Название политики	Описание
«Разрешение веб-камеры (RDP, SPICE, TERA)»	Допустимые разрешения видеокамеры в протоколах RDP, SPICE, TERA. Применимость: ▪ BPM (RDP, SPICE, TERA); ▪ автономные машины (RDP, TERA). Значение по умолчанию: «320-2560x240-1440»
«Разрешенные форматы буфера обмена (RDP, SPICE, TERA)»	Политика определяет разрешенный формат записей в буфере обмена. В зависимости от направления передачи перед отправкой или после получения данных из буфера обмена запрашивается их тип и сопоставляется с разрешенными значениями. В зависимости от типа данных передача данных разрешается или запрещается. Для совместимости с предыдущими версиями ПО Termidesk Viewer используется значение по умолчанию. Применимость: ▪ BPM (RDP, SPICE, TERA); ▪ автономные машины (RDP, TERA); ▪ терминальные сессии MS RDS; ▪ опубликованные приложения MS RDS; ▪ терминальные сессии STAL; ▪ опубликованные приложения STAL; ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS; ▪ терминальные сессии метапоставщика STAL; ▪ опубликованные приложения метапоставщика STAL. Возможные значения: ▪ «Любой» (по умолчанию); ▪ «Текст без форматирования»
«Согласие пользователя для подключения администратора в Удалённом Помощнике»	Политика определяет необходимость согласия пользователя для подключения администратора к его сеансу через «Удаленный помощник». Возможные значения: ▪ «Требуется» (по умолчанию) - запрос на подключение администратора отобразится пользователю в диалоговом окне клиентской части «Удаленного помощника». Администратор подключится к сеансу только после согласия пользователя. Имя подключившегося администратора отобразится у пользователя; ▪ «Не требуется» - запрос на подключение администратора не будет отображен пользователю, т.к. подтверждение запроса не требуется. Уведомление о подключении администратора отобразится пользователю в клиентской части «Удаленного помощника». Имя подключившегося администратора отобразится у пользователя

Название политики	Описание
«Удаление рабочего места»	Политика определяет событие, после которого будет произведено удаление РМ. Работает совместно с политикой «Действие при выходе пользователя из ОС». Применимость: ▪ BPM (RDP, SPICE, TERA); ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS. Возможные значения: ▪ «После события выхода пользователя из ОС» (по умолчанию); ▪ «После события завершения синхронизации профиля»
«Удаление устаревшей публикации»	Политика определяет действие, применимое к устаревшей публикации. Использование политики меняет поведение параметра «Срок действия устаревшей публикации» (см. подраздел **Общие системные параметры Termidesk**) на уровне фонда РМ. Возможные значения: ▪ «Удалять по истечении срока действия» (по умолчанию) - устаревшие публикации будут удалены по истечении срока, заданного в параметре «Срок действия устаревшей публикации»; ▪ «Удалять немедленно» - при перепубликации фонда назначенная ВМ будет немедленно заменена на новую публикацию; ▪ «Не удалять назначенные машины» - назначенные РМ не будут удалены при перепубликации (такие РМ будут требовать ручного удаления). Неназначенные РМ удаляются и публикуются заново. При этом значении: • текущая публикация будет находиться в состоянии частичного удаления, пока существует хотя бы одно назначенное РМ; • после удаления последнего назначенного РМ публикация будет переведена в статус «Публикация удалена». Новая публикация будет переведена в статус «Публикация успешно завершена», если она завершена успешно

Название политики	Описание
«Путь для перемещаемого профиля пользователя служб удаленного рабочего стола (RDP)»	По умолчанию службы удаленных рабочих столов хранят все профили пользователей локально на сервере узла сеанса удаленных рабочих столов. Политика действует на ОС Microsoft Windows. Политика используется для указания общего сетевого ресурса, в котором профили пользователей могут храниться централизованно, позволяя пользователю получать доступ к одному и тому же профилю для сеансов на всех серверах узла сеансов удаленных рабочих столов, настроенных на использование общего сетевого ресурса для профилей пользователей. При задании значения для политики, службы удаленных рабочих столов будут использовать указанный путь в качестве корневого каталога для всех профилей пользователей. Непосредственно профили будут содержаться во вложенных каталогах, названных по имени учетной записи каждого пользователя `%USERNAME%`, которые появятся на сетевом ресурсе автоматически после подключения пользователя. При изменении политики требуется перезагрузка ВМ или терминальных серверов. Зависит от политики «Использование обязательных профилей на сервере узла сеанса удаленных рабочих столов (RDP)». Формат указания сетевого ресурса (пример): `\\имя_компьютера\имя_общего_ресурса\`. Применимость: ▪ BPM (RDP); ▪ автономные машины (RDP); ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS. Значение по умолчанию: «Не задан»
«Домашний каталог пользователя служб удаленного рабочего стола (RDP)»	Политика указывает, будут ли службы удаленных рабочих столов использовать указанный сетевой ресурс или путь к локальному каталогу в качестве корневого каталога домашнего каталога пользователя для сеанса служб удаленных рабочих столов. Политика действует на ОС Microsoft Windows. Формат указания сетевого ресурса (пример): `\\имя_компьютера\имя_общего_ресурса\`. При изменении политики требуется перезагрузка терминальных серверов. Применимость: ▪ терминальные сессии метапоставщика MS RDS; ▪ опубликованные приложения метапоставщика MS RDS. Значение по умолчанию: «Не задан»

10.4 . Объединение фондов в группы РМ

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

Для добавления группы администратору Termidesk следует перейти «Настройки - Группы рабочих мест» и нажать экранную кнопку **[Создать]**, затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 80).

Таблица 80 – Данные для объединения фондов BPM в группы

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

Для редактирования группы PM в Termidesk нужно пометить необходимую группу и нажать экранную кнопку **[Изменить]**.

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

10.5 . Публикация фонда PM

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

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

На открывшейся странице в разделе «Публикации» нажать экранную кнопку **[Создать]**. В окне подтверждения публикации нажать экранную кнопку **[Опубликовать]** для запуска задачи обновления фонда PM.

При этом:

- для фондов, созданных на основе поставщиков ресурсов VMware vSphere, oVirt, при публикации также доступен выбор снимка ВМ (снапшота), который будет использован для формирования PM;
- для поставщика ресурсов VMware vSphere все наименования снапшотов будут содержать дату и время их создания. Активный снапшот будет помечен как «Active VM»;
- при публикации фонда PM будет доступен выбор действия, применимого к учетной записи PM. Описание действий приведено в параметре «Действие с учетной записью рабочего места» подраздела **Общие системные параметры Termidesk**.

ⓘ Публикация фонда PM применима также к фонду автономных машин (см. подраздел **Добавление фонда автономных машин**). При перепубликации фонда автономных машин назначенные машины не будут удалены.

Нажатие экранной кнопки **[Отменить]** не вызывает обновления фонда РМ.

Прогресс выполнения публикации будет отображен в этом же разделе. Индикатор прогресса относится только к созданию ВМ в кеше (ВМ, поддерживаемых в определенном состоянии) и не отображает факт получения пользователем РМ.

Существуют несколько состояний публикации, отражаемых в столбце «Прогресс»:

- «Идет создание ВМ», индикация серым цветом (см. Рисунок 60) - начало процесса публикации;
- «Идет создание ВМ», индикация синим цветом (см. Рисунок 60) - непосредственно процесс выполнения публикации, при котором выполняется обращение к поставщику ресурсов и создание ВМ;

> Частота обновления прогресса зависит от значения интервала обновления для таблицы «Публикации». Отображаемый цвет и текст зависят от состояния публикации.
> Максимальное время ожидания готовности РМ определяется системным параметром «Максимальное время инициализации рабочего места» (см. подраздел **Общие системные параметры Termidesk**).

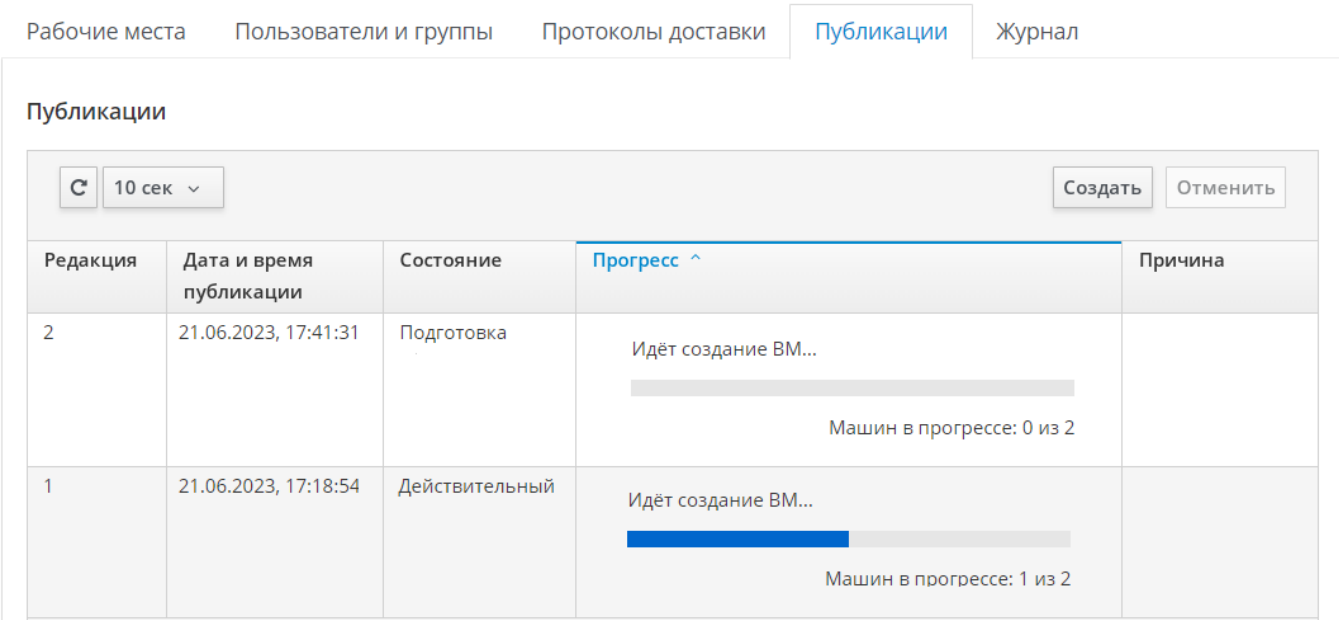

Рисунок 60 – Индикация прогресса выполнения публикации со статусом «Идет создание ВМ»

- «Публикация успешно завершена», индикация зеленым цветом (см. Рисунок 61) - публикация ВМ в кеше завершена. При выдаче РМ из кеша прогресс вновь вернется на начало процесса публикации;

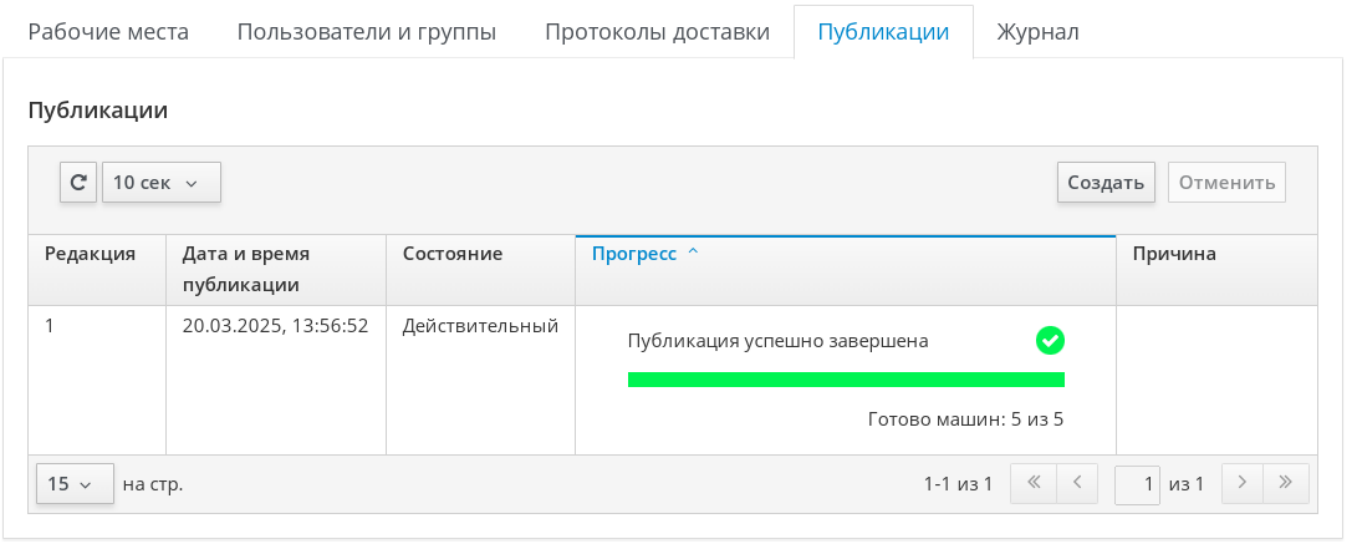

Рисунок 61 – Индикация прогресса выполнения публикации со статусом «Публикация успешно завершена»

- «Во время публикации возникла ошибка», индикация серым цветом с пиктограммой красного цвета (см. Рисунок 62) - процесс публикации завершился с ошибкой, текст ошибки отобразится в столбце «Причина»;

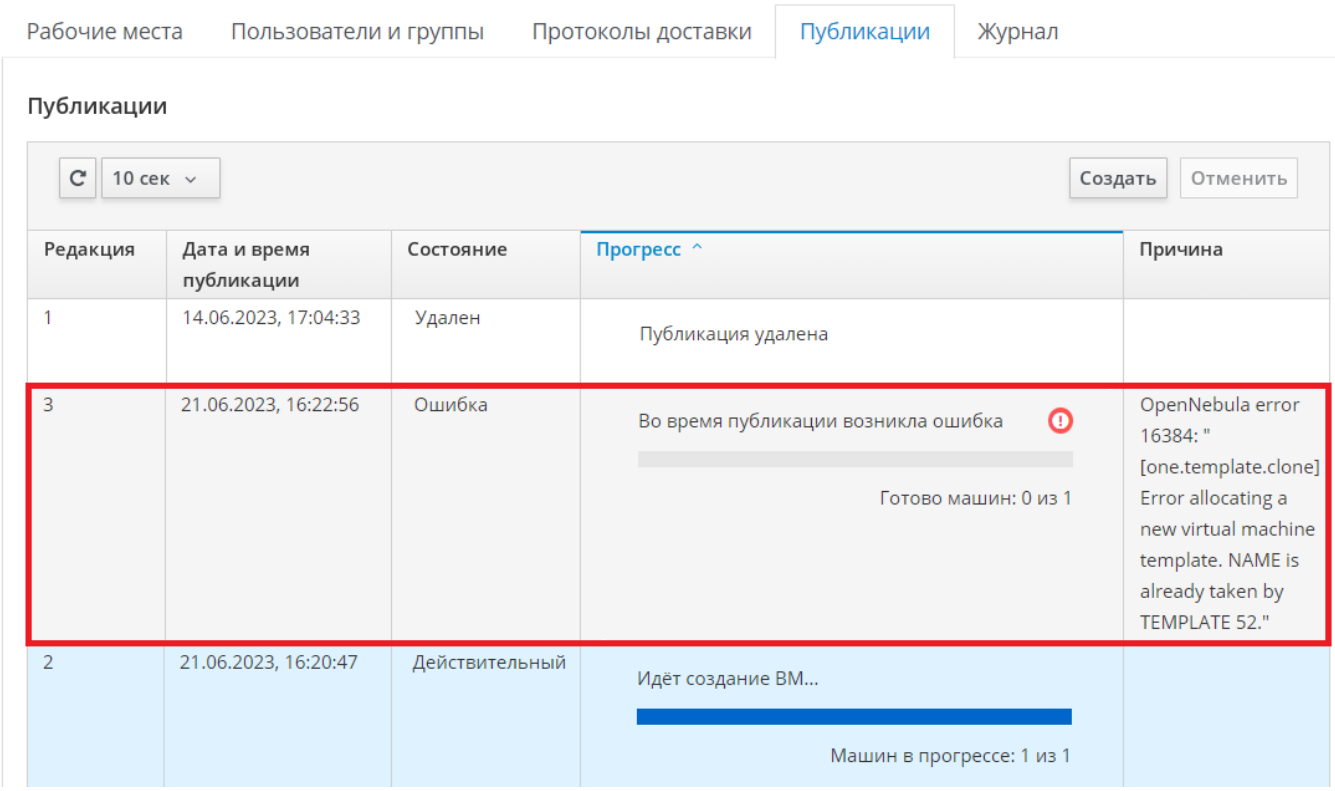

Рисунок 62 – Индикация возникновения ошибки при публикации

- «Публикация удалена», без индикации - информирование о завершении удаления публикации. Получить данное состояние можно при инициировании новой публикации (в таком случае старая публикация удаляется);
- «Публикация частично удалена», без индикации - информирование о частичном удалении предыдущей публикации. В это состояние публикация переходит, если в фонде есть назначенная и используемая ВМ, и параметру «Срок действия устаревшей публикации» (см. подраздел **Общие системные параметры Termidesk**) задано значение «-1»;
- «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»).

⚠ Состояние «Нет машин в кеше 1-го и 2-го уровней» не отображается для фонда автономных машин.

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

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

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

10.6 . Назначение пользователей фонду РМ

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

Для добавления нового пользователя к фонду РМ следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда. На открывшейся странице в разделе «Пользователи и группы» нажать на экранную кнопку **[Создать]** в области «Пользователи».
Для выбора будут доступны те домены аутентификации, для которых в параметре «Субъекты» задано значение «Пользователи» или «Все».

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

10.7 . Назначение групп доступа фонду РМ

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

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

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

Для выбора будут доступны те домены аутентификации, для которых в параметре «Субъекты» задано значение «Пользователи» или «Все».

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 Termidesk.

10.8 . Назначение сетей фонду РМ

Фонду РМ нужно назначить одну или несколько сетей, каждая из которых задает IP-адреса или диапазоны IP-адресов пользователей.

⚠ Отображение списка будет доступно администратору, если у него есть пользовательское разрешение «Управление списками сетей фондов рабочих мест».
Назначение сетей недоступно для **сервисного** фонда «метапоставщика».

Для добавления сетей фонду РМ следует:

- перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда РМ;
- на открывшейся странице в разделе «Сети» нажать экранную кнопку **[Создать]**;
- в окне добавления объекта из выпадающего списка выбрать необходимую сеть и нажать экранную кнопку **[Сохранить]**. Для выбора будут доступны сети, предварительно заданные на странице «Компоненты - Сети».

При этом:

- если в свойствах фонда параметру «Доступ из связанных сетей» задано значение «Разрешить», то подключение к фонду будет разрешено только для перечисленных на вкладке «Сети» диапазонов сетей (реализация «белого» списка доступа);

- если в свойствах фонда параметру «Доступ из связанных сетей» задано значение «Запретить», то подключение к фонду будет запрещено для перечисленных на вкладке «Сети» диапазонов сетей (реализация «черного» списка доступа);
- если ни одна сеть не будет задана, то подключение к фонду будет разрешено для всех сетей.

Для сокрытия недоступных пользователю фондов используется параметр «Скрывать недоступные ресурсы» (см. подраздел **Управление настройками компонента «Клиент»**).

Для удаления сети из фонда используется экранная кнопка **[Удалить]**.

⚠ Для фондов, созданных в Termidesk до версии 6.0, по умолчанию действует значение «Запретить» для параметра «Доступ из связанных сетей». Для изменения параметра нужно выбрать фонд на странице «Рабочие места - Фонды» и нажать экранную кнопку **[Изменить]**.

Если списки доступа заданы как на уровне фонда, так и на уровне протоколов доставки, то:

- в первую очередь проверка доступности будет происходить на уровне фонда, во вторую очередь проверяется ограничение сетей в протоколах доставки;
- будет применено наиболее строгое ограничение:
  - если в фонде РМ задан «белый» список с определенным IP-адресом, и на уровне протокола доставки задан «черный» список доступа, то фонд не будет доступен;
  - если в фонде РМ задан «белый» список, но в списке нет нужного IP-адреса, и на уровне протокола доставки задан «белый» список доступа, то фонд не будет доступен;
  - если в фонде РМ задан «белый» список, в котором есть нужный IP-адрес, и на уровне протокола доставки задан «белый» список доступа, то фонд будет доступен.

10.9 . Назначение протоколов фонду РМ

Фонду РМ 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 РМ следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда.

На открывшейся странице в разделе «Протоколы доставки» нужно нажать экранную кнопку **[Создать]**. 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».

10.10 . Управление РМ

10.10.1 . Управление терминальными сессиями в назначенном фонде РМ

В графическом интерфейсе управления Termidesk предусмотрена возможность просмотра информации и управления терминальными сессиями пользователей в назначенном фонде РМ.

Для просмотра основных сведений о сессиях пользователей в назначенном фонде РМ следует перейти «Рабочие места - Фонды», затем выбрать нужный фонд, перейти во вкладку «Рабочие места» (см. Рисунок 63).

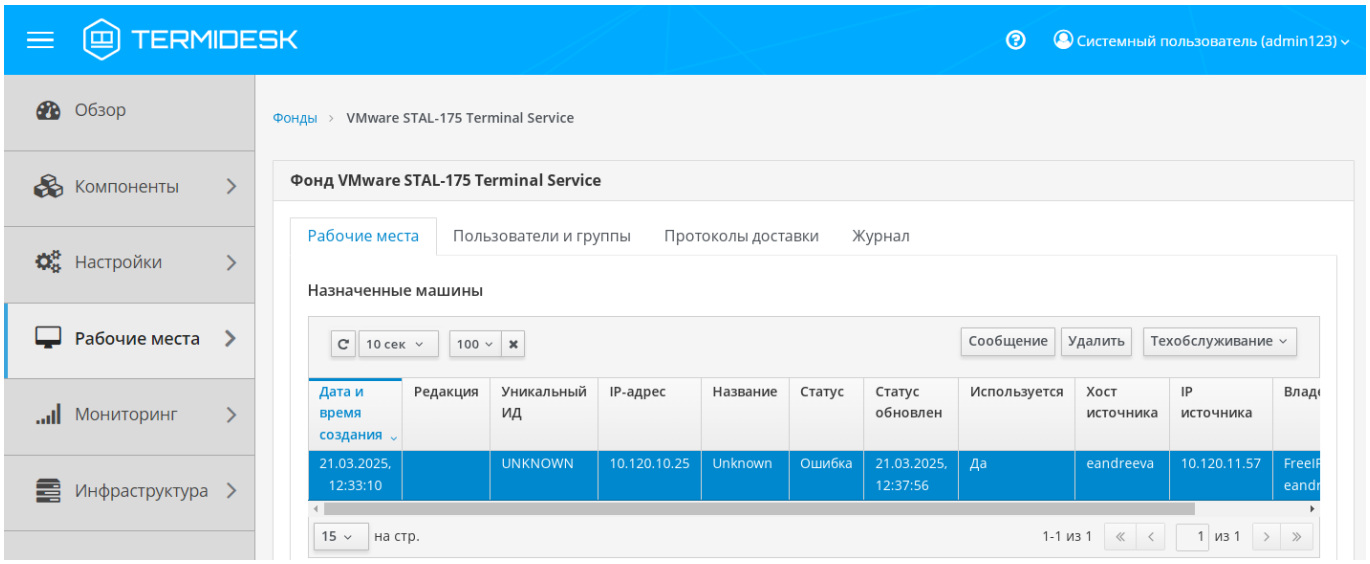

Рисунок 63 – Просмотр сведений о сессиях пользователей в назначенном фонде РМ

Основные параметры сессий перечислены в столбце «Параметр» следующей таблицы (см. Таблица 81).

Таблица 81 – Основные параметры сессий в назначенном фонде ВРМ

Параметр	Описание
«Дата и время создания»	Временная метка создания сессии
«Редакция»	Порядковый номер версии сессии
«Уникальный ИД»	Уникальный идентификатор сессии
«IP-адрес»	IP-адрес терминального сервера, к которому установлено подключение сессии
«Название»	Номер сессии, выданной пользователю и ссылка на ее журнал
«Статус»	Флаг использования сессии
«Статус обновлен»	Временная метка обновления статуса
«Используется»	Флаг назначения сессии
«Хост источника»	Наименование инициатора сессии
«IP источника»	IP-адрес инициатора сессии

Параметр	Описание
«Владелец»	Субъект, инициировавший выдачу сессии
«Версия агента»	Версия компонента «Агент», установленного на терминальном сервере

Для задания лимита записей, загружаемых из БД и отображаемых в веб-интерфейсе, нужно:

- нажать на экранную кнопку **[Выберите лимит]**. По умолчанию загружаются 100 записей, значение «100» отображается как значение экранной кнопки;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке;
- или ввести свое значение в доступном поле и подтвердить выбор, используя графический элемент  или клавишу **<ENTER>**. Возможные значения: от 1 до 1 000 000. Указанное значение сохранится в списке до перезагрузки страницы.

Для сброса заданного лимита нужно воспользоваться графическим элементом  .
Также поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент  под таблицей. По умолчанию отображаются 15 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента.

Для изменения состояния подключений предусмотрены элементы управления (см. Таблица 82).

Таблица 82 – Элементы управления состоянием терминального сервера

Элемент управления	Описание
«Техобслуживание»	Перевод ВМ терминального сервера в режим техобслуживания (значение «Включить» в выпадающем списке) или вывод из него (значение «Выключить»). Режим техобслуживания - это запрет пользователям подключаться (создавать новую сессию) и/или переподключаться повторно в сессию на терминальном сервере. Если узел находится в режиме техобслуживания, то: ▪ пользователи могут подключаться к существующим сеансам, но не могут запускать новые сеансы; ▪ в существующем активном сеансе, который был создан до включения режима техобслуживания, пользователь может запускать новые приложения на этом терминальном сервере
«Удалить»	Отключение выбранной сессии для терминальных подключений. Отображение статуса «Удален» в столбце «Статус» свидетельствует об успешном удалении сессии. Терминальные сессии также могут быть удалены на странице «Рабочие места - Индивидуальные рабочие места»

⚠ После нажатия экранной кнопки **[Удалить]** принудительный штатный выход пользователя из ОС РМ произойдет в течение 30 секунд.
Сессия пользователя также будет автоматически и принудительно завершена, если пользователь был удален или домен аутентификации, в который входит этот пользователь, был отключен или удален.

Экранная кнопка **[Сообщение]** не вызывает отправку сообщения в терминальную сессию.

Частота обновления статусов терминальных сессий (в том числе сессий метапоставщика) для небольшого количества машин составляет 2 секунды.
Для терминальных сессий может возникнуть ситуация, при которой статус сессии отображен как «Действительный», но идентификатор ей не назначен. Такие сессии считаются неактивными и удаляются периодической задачей, которая срабатывает с интервалом 240 секунд.

10.10.2 . Управление состоянием ВМ в назначенном фонде РМ

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

- ПК СВ Брест (обязательна установка компонента «Агент узла виртуализации»);
- zVirt;
- РЕД Виртуализация;
- OpenStack;
- oVirt;
- VMware vSphere.

Для просмотра списка и управления состоянием ВМ в фонде РМ необходимо перейти «Рабочие места - Фонды», затем выбрать нужный фонд во вкладке «Рабочие места» (см. Рисунок 64).

Отображение списка будет доступно оператору, если у него есть пользовательское разрешение «Просмотр фондов рабочих мест».
Управление состоянием ВМ будет доступно оператору, если у него есть пользовательское разрешение «Управление питанием фондов рабочих мест».

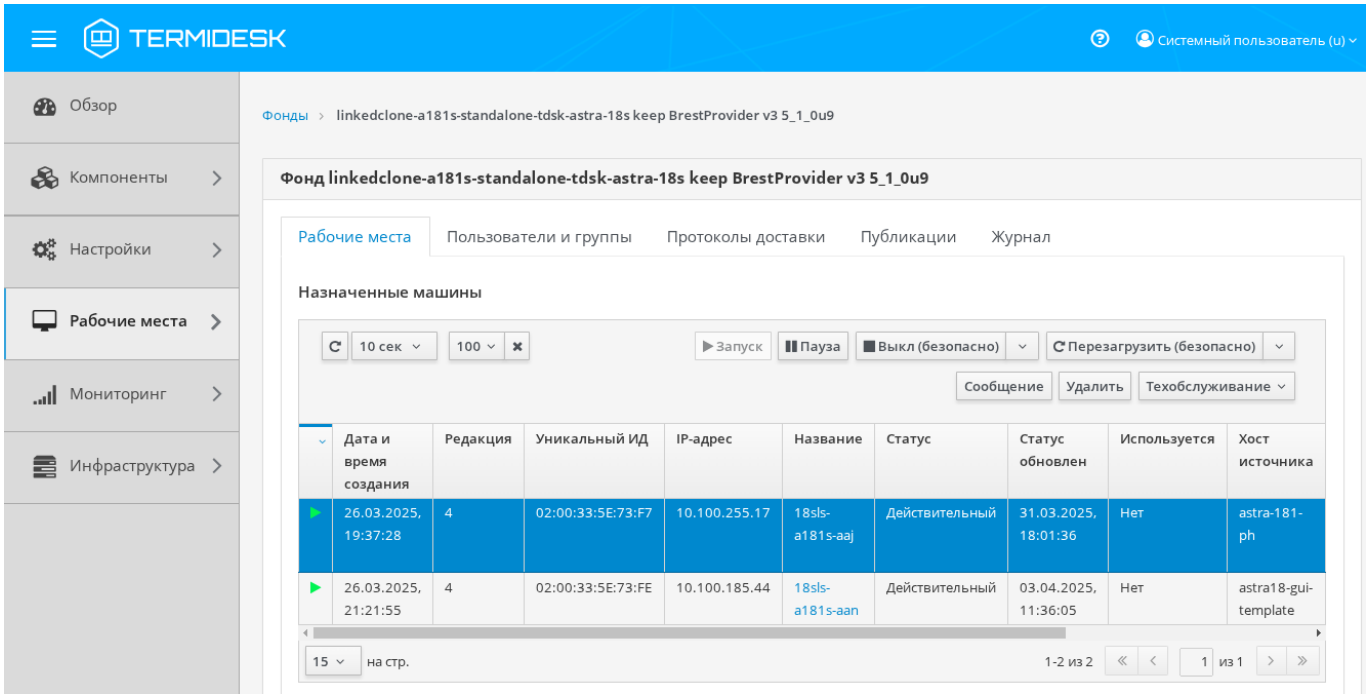

Рисунок 64 – Страница управления состоянием назначенных ВМ

Основные параметры списка ВМ в назначенном фонде РМ перечислены в столбце «Параметр» следующей таблицы (см. Таблица 83).

Таблица 83 – Основные параметры списка ВМ в назначенном фонде РМ

Параметр	Описание
«Дата и время создания»	Временная метка выполнения публикации РМ
«Редакция»	Порядковый номер версии публикации
«Уникальный ИД»	Уникальный идентификатор РМ: MAC-адрес или номер сессии
«IP-адрес»	IP-адрес, назначенный РМ
«Название»	Наименование РМ и ссылка на его журнал
«Статус»	Флаг использования публикации РМ из фонда РМ
«Статус обновлен»	Временная метка обновления статуса

Параметр	Описание
«Используется»	Флаг назначения РМ. Значение «Нет» свидетельствует о том, что РМ находится в кеше. ⚠ Значение «Нет» также может свидетельствовать, что сессия пользователя была завершена некорректно: например, пользователь закрыл окно программы доставки РМ без завершения сессии, затем подключился через сеанс удаленного подключения (например, по протоколу SSH) и закрыл подключение. Такой сценарий не является штатным для Termidesk, поэтому отображение корректного значения параметра в таком случае не гарантируется. Корректное завершение сессии выполняется через встроенные в ОС средства, например, через «Пуск» - «Завершение работы» - «Выход из сессии»
«Хост источника»	Наименование инициатора выдачи РМ
«IP источника»	IP-адрес инициатора выдачи РМ
«Владелец»	Субъект, инициировавший выдачу РМ
«Версия агента»	Версия компонента «Агент», установленного в гостевой ОС РМ

Для задания лимита записей, загружаемых из БД и отображаемых в веб-интерфейсе, нужно:

- нажать на экранную кнопку **[Выберите лимит]**. По умолчанию загружаются 100 записей, значение «100» отображается как значение экранной кнопки;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке;
- или ввести свое значение в доступном поле и подтвердить выбор, используя графический элемент  или клавишу **<ENTER>**. Возможные значения: от 1 до 1 000 000. Указанное значение сохранится в списке до перезагрузки страницы.

Для сброса заданного лимита нужно воспользоваться графическим элементом  .

Также поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент 

под таблицей. По умолчанию отображаются 15 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента.

Каждая запись списка сопровождается индикацией состояния ВМ.

Таблица 84 – 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 РМ, не поддерживается управление состоянием ВМ. Экранные кнопки **[Запуск]**, **[Пауза]**, **[Выкл (безопасно)]**, **[Перезагрузить (безопасно)]** будут недоступны для использования
	ВМ включена
	ВМ находится в спящем режиме
	ВМ выключена

Для изменения состояния ВМ предусмотрены элементы управления (см. Таблица 85). Управление состоянием ВМ будет доступно даже при переводе ВМ, фонда РМ или поставщика ресурсов в режим техобслуживания.

Таблица 85 – Элементы управления состоянием ВМ

Элемент управления	Описание
«Запуск»	Инициирует процесс старта ВМ
«Пауза»	Приостанавливает работу ВМ, с сохранением текущего состояния
«Выкл (безопасно)»	Инициирует процесс безопасного отключения ВМ, с завершением активных процессов и сохранением данных. Для безопасного отключения ВМ, размещенной на VMware, нужно дополнительно установить утилиты (VMware Tools) в гостевую ОС. Для принудительного выключения ВМ в раскрывающемся списке элемента управления следует нажать экранную кнопку **[Выключить]** ⚠ Принудительное выключение ВМ может привести к потере несохраненных данных или повреждению гостевой ОС.
«Перезагрузить (безопасно)»	Инициирует процесс безопасной перезагрузки ВМ, применяя изменения в конфигурации или гостевой ОС. Для безопасной перезагрузки ВМ, размещенной на VMware, нужно дополнительно установить утилиты (VMware Tools) в гостевую ОС. Для принудительной перезагрузки ВМ в раскрывающемся списке элемента управления следует нажать экранную кнопку **[Перезагрузить]** ⚠ Принудительная перезагрузка ВМ завершает активные сессии гостевой ОС и может привести к потере несохраненных данных. Для ВРМ, размещенного на поставщике ресурсов VMware vSphere и использующего диск с режимом «Независимый-Непостоянный», сброс состояния ВМ не происходит, если перезагрузка инициирована из гостевой ОС или через экранную кнопку **[Перезагрузить (безопасно)]**.
«Сообщение»	Отправка сообщения пользователям РМ. 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»)

Элемент управления	Описание
«Восстановить»	Элемент доступен только для поставщиков ресурсов zVirt, oVirt, VMware vSphere. Производит возврат ВМ к снимку (снапшоту), созданному на завершающей стадии подготовки РМ, то есть к состоянию до момента затребования РМ пользователем. ℹ Восстановление может быть применимо и для неназначенных ВМ. Функционал восстановления ВМ будет доступен оператору, если у него есть пользовательское разрешение «Восстановление рабочих мест». Восстановление может быть применено, если есть снимок, к которому ВМ может быть возвращена. ⚠ Для поставщика ресурсов VMware vSphere: ▪ восстановление ВМ осуществляется через процедуру «выключить», а не «приостановить» («suspend»); ▪ если диск ВМ создан в режиме «Зависимый», то механизм восстановления вернет состояние ВМ к снимку; ▪ если диск ВМ создан в режиме «Независимый-Непостоянный», то механизм восстановления вернет состояние ВМ, актуальное до внесенных пользователем изменений (все изменения будут потеряны). Механизм восстановления для этого режима диска происходит через небезопасное выключение ВМ. Для массового восстановления ВМ следует выбрать несколько строк с ВМ, удовлетворяющих перечисленным условиям, и воспользоваться указанным элементом управления. При повторной публикации фонда РМ возврат к снимку для ранних публикаций будет невозможен
«Техобслуживание»	Перевод ВМ в режим техобслуживания (значение «Включить» в выпадающем списке) или вывод из него (значение «Выключить»). Режим техобслуживания ВМ - это запрет пользователям подключаться и/или переподключаться к ВМ. Текущие подключения остаются до тех пор, пока пользователи не отключатся или не выйдут из ОС самостоятельно или при управляющем воздействии (активации политики фонда РМ или действии администратора). ВМ, находящаяся в режиме техобслуживания: ▪ не назначается пользователю; ▪ не удаляется, если зависла; ▪ не может быть переведена в другое состояние из интерфейса портала Termidesk; ▪ не обновляет информацию о своем состоянии; ▪ не переходит из кеша второго уровня в первый; ▪ может быть удалена, однако ее удаление произойдет после вывода ВМ из режима техобслуживания
«Удалить»	Инициирует процесс полного удаления ВМ, включая все связанные с ней данные и конфигурации. При удалении ВМ из фонда отобразится окно «Удалить объект». В раскрывающемся списке окна нужно выбрать действие, которое будет произведено над учетной записью РМ в службе каталогов: ℹ Список будет отображен, если действие над учетной записью применимо к РМ. ▪ «Удалить» (по умолчанию) - при удалении РМ из фонда учетная запись будет удалена из службы каталогов. Применимость: MS AD, FreeIPA, ALD Pro; ▪ «Сбросить пароль» - при удалении РМ из фонда у учетной записи будет сброшен пароль. Применимость: MS AD; ▪ «Выключить» - при удалении РМ из фонда учетная запись будет отключена. Применимость: MS AD; ▪ «Хранить» - при удалении РМ из фонда учетная запись будет сохранена в службе каталогов. Применимость: MS AD, FreeIPA, ALD Pro

10.10.3 . Управление состоянием автономных машин в назначенном фонде

В графическом интерфейсе управления Termidesk предусмотрена возможность просмотра информации и управления автономными машинами в назначенном фонде.

Для просмотра списка и управления состоянием автономных машин в фонде необходимо перейти «Рабочие места - Фонды», затем выбрать фонд, перейти во вкладку «Рабочие места».

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

Основные параметры списка машин в назначенном фонде перечислены в столбце «Параметр» следующей таблицы (см. Таблица 86).

Таблица 86 – Основные параметры списка физических машин

Параметр	Описание
«Дата и время создания»	Временная метка выполнения публикации
«Редакция»	Порядковый номер версии публикации
«Уникальный ИД»	Уникальный идентификатор РМ: MAC-адрес автономной машины. В случае, если установленный на автономной машине «Агент виртуальных рабочих мест» запускается на VPN-соединении или сетевом адаптере без MAC-адреса, то он не сможет зарегистрироваться на «Универсальном диспетчере»
«IP-адрес»	IP-адрес автономной машины
«Название»	Наименование РМ и ссылка на журнал
«Статус»	Флаг использования публикации из фонда
«Статус обновлен»	Временная метка обновления статуса
«Используется»	Флаг назначения РМ. Значение «Нет» свидетельствует о том, что РМ находится в кеше
«Хост источника»	Наименование инициатора выдачи РМ
«IP источника»	IP-адрес инициатора выдачи РМ
«Владелец»	Субъект, инициировавший выдачу РМ
«Версия агента»	Версия компонента «Агент виртуального рабочего места», установленного в ОС автономной машины

Для задания лимита записей, загружаемых из БД и отображаемых в веб-интерфейсе, нужно:

- нажать на экранную кнопку **[Выберите лимит]**. По умолчанию загружаются 100 записей, значение «100» отображается как значение экранной кнопки;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке;
- или ввести свое значение в доступном поле и подтвердить выбор, используя графический элемент  или клавишу **<ENTER>**. Возможные значения: от 1 до 1 000 000. Указанное значение сохранится в списке до перезагрузки страницы.

Для сброса заданного лимита нужно воспользоваться графическим элементом  .
Также поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент  под таблицей. По умолчанию отображаются 15 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента.

Для изменения состояния автономной машины предусмотрены элементы управления (см. Таблица 87).

Таблица 87 – Элементы управления автономными машинами

Элемент управления	Описание
«Выкл (безопасно)»	Инициирует процесс безопасного отключения с завершением активных процессов и сохранением данных. Для безопасного отключения автономной машины, размещенной на VMware, нужно дополнительно установить утилиты (VMware Tools) в гостевую ОС. Экранная кнопка выпадающего списка **[Выключить]** не поддерживается
«Перезагрузить (безопасно)»	Инициирует процесс безопасной перезагрузки, применяя изменения в конфигурации или гостевой ОС
«Сообщение»	Отправка сообщения пользователям РМ. Отправка сообщения возможна, если параметр «Статус» имеет значение «Действительный» или «Подготовка»
«Техобслуживание»	Перевод автономной машины в режим техобслуживания (значение «Включить» в выпадающем списке) или вывод из него (значение «Выключить»). Режим техобслуживания - это запрет пользователям подключаться и (или) переподключаться к РМ. Текущие подключения остаются до тех пор, пока пользователи не отключатся или не выйдут из ОС самостоятельно или при управляющем воздействии (активации политики фонда или действии администратора). РМ, находящаяся в режиме техобслуживания: ▪ не назначается пользователю; ▪ не удаляется, если машина зависла; ▪ не может быть переведено в другое состояние из интерфейса портала Termidesk; ▪ не обновляет информацию о своем состоянии; ▪ не переходит из кеша второго уровня в первый; ▪ может быть удалено, однако его удаление произойдет после вывода из режима техобслуживания
«Удалить»	Инициирует процесс полного удаления РМ, включая все связанные с ним данные и конфигурации. Действие над учетной записью РМ в службе каталогов не поддерживается

10.10.4 . Назначение владельца РМ

В Termidesk предусмотрена возможность назначения владельца РМ для гарантированного закрепления за пользователем конкретной ВМ. В этом случае пользователь всегда будет получать одну и ту же ВМ при подключении к фонду РМ.

Назначение владельца возможно при соблюдении следующих условий:

- РМ находится в статусе «Подготовка» или «Действительный»;
- РМ находится в кеше 1-го уровня;

- для данного РМ отсутствует назначенный пользователь в столбце «Владелец» списка РМ.

Назначить владельца РМ можно:

- со страницы фонда. Для этого следует перейти «Рабочие места - Фонды», затем выбрать нужный фонд, перейти во вкладку «Рабочие места». Выбрать нужное РМ, которое находится в таблице «Кеш», и нажать экранную кнопку [Владелец] (см. Рисунок 65). В открывшемся окне «Владелец» выбрать домен аутентификации и пользователя, которому будет назначено РМ. Выбранный пользователь автоматически добавится в фонд РМ и будет отображен во вкладке «Пользователи и группы»;
- со страницы «Рабочие места - Индивидуальные рабочие места».

⚠ Назначение владельца будет доступно только в том случае, если пользователь хотя бы один раз осуществил вход в «Портал пользователя» или подключился к «Универсальному диспетчеру» через компонент «Клиент» под своей учетной записью.

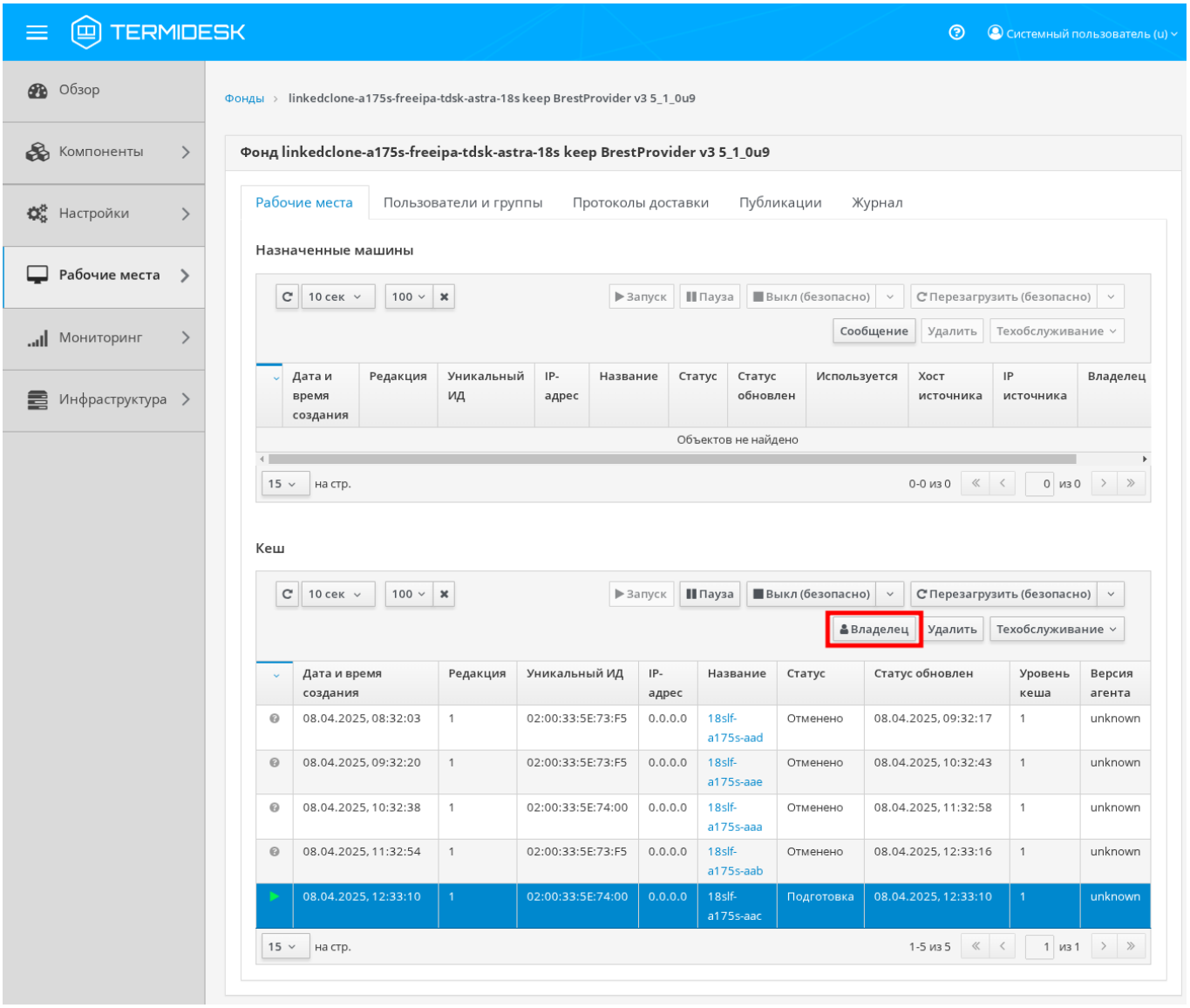

Рисунок 65 – Назначение владельца РМ на странице фонда РМ

10.11 . Управление сессиями подключенных к фонду РМ пользователей

10.11.1 . Управление активными сессиями пользователей

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

Доступны следующие возможности по управлению сессией:

- завершение сессии пользователя. Следует перейти «Рабочие места - Сессии», пометить сессию пользователя и нажать экранную кнопку **[Завершить]**. После нажатия экранной кнопки **[Завершить]** принудительный штатный выход пользователя из ОС ВРМ произойдет в течение 30 секунд. Также сессия пользователя будет автоматически и принудительно

завершена, если он был удален или домен аутентификации, в который входит этот пользователь, был отключен или удален;

- отключение сессии пользователя. Следует перейти «Рабочие места - Сессии», пометить сессию пользователя и нажать экранную кнопку **[Отключить]**. Сессия пользователя прервется, но если он снова подключится, то состояние сессии до отключения восстановится;
- подключение к сессии пользователя. Следует перейти «Рабочие места - Сессии», пометить сессию пользователя и нажать экранную кнопку **[Помощник]**. При этом пользователю не нужно вводить данные для подключения в компоненте «Удаленный помощник» (клиентская часть) - они будут заполнены автоматически. Для работы подключения необходимо, чтобы:
  - в гостевой ОС был установлен компонент «Удаленный помощник» (клиентская часть);
  - в сетевой инфраструктуре организации существовал узел с установленным компонентом «Удаленный помощник» (серверная часть) и он был доступен для взаимодействия с «Универсальным диспетчером»;
  - в системных параметрах был установлен параметр «Адрес сервера удаленного помощника» (см. подраздел **Общие системные параметры Termidesk**).

Функционал управления сессиями (завершение, отключение) пользователя из страницы «Рабочие места - Сессии» доступен для терминальных сессий.
Сброс сессии для BPM будет работать для поставщика ПК СВ Брест, если выполнена дополнительная настройка «Агента узла виртуализации» (см. подраздел **Использование альтернативного механизма сброса сессий** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»).
Отключение сессии пользователя, подключенного по протоколу TERA, работает для гостевой ОС Astra Linux Special Edition, и применяется как для физической машины, так и для ВМ.

Не рекомендуется устанавливать компонент «Удаленный помощник» (серверная часть) на узел с установленным компонентом «Универсальный диспетчер», поскольку оба компонента вносят изменения в конфигурацию веб-сервера Apache.

Для просмотра основных сведений об активных сессиях пользователей в фондах РМ следует перейти «Рабочие места - Сессии», после чего откроется сводная таблица (см. Рисунок 66).

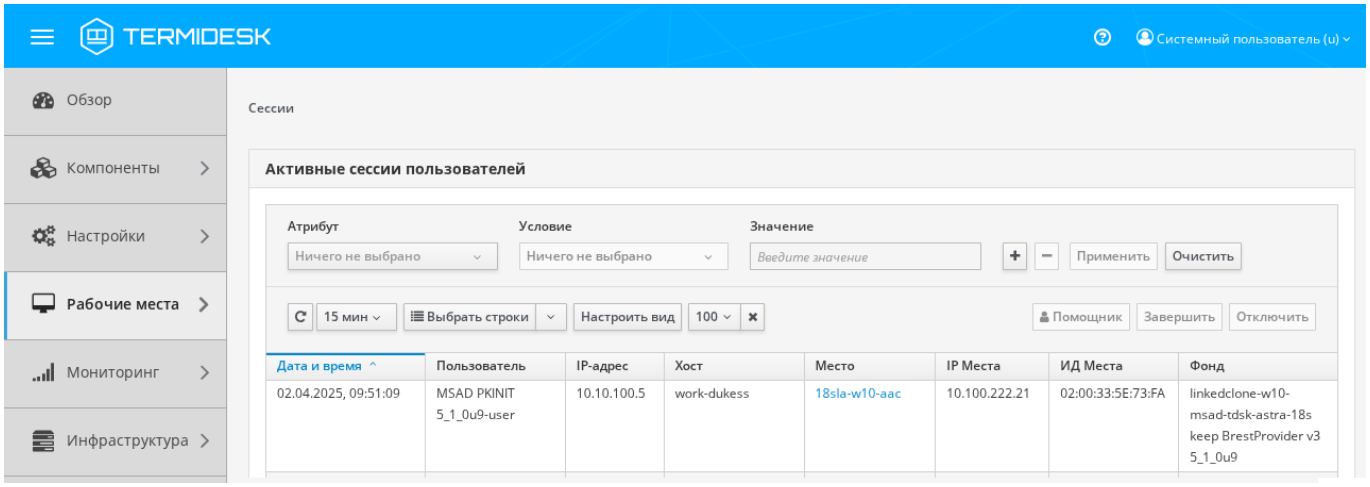

Рисунок 66 – Просмотр сведений об активных сессиях пользователей в фондах BPM

Основные параметры сессий перечислены в столбце «Параметр» следующей таблицы (см. Таблица 88).

Таблица 88 – Основные параметры сессий пользователей

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

Для задания лимита записей, загружаемых из БД и отображаемых в веб-интерфейсе, нужно:

- нажать на экранную кнопку **[Выберите лимит]**. По умолчанию загружаются 100 записей, значение «100» отображается как значение экранной кнопки;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке;
- или ввести свое значение в доступном поле и подтвердить выбор, используя графический элемент  или клавишу **<ENTER>**. Возможные значения: от 1 до 1 000 000. Указанное значение сохранится в списке до перезагрузки страницы.

Для сброса заданного лимита нужно воспользоваться графическим элементом  .

⚠ При включенной фильтрации записей по атрибутам сначала выполняется поиск записей в БД, удовлетворяющих условиям фильтра, и только затем применяется ограничение выбранного лимита.

Пример: пусть в таблице БД существует 101 запись, а в веб-интерфейсе задана фильтрация по атрибутам и лимит в 100 записей. Если параметрам фильтрации удовлетворяют порядковые записи 5, 10, 101, то 101-ая запись не отобразится.

Также поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент 15 под таблицей. По умолчанию отображаются 15 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента.

Записи в таблице поддерживают функцию множественного выбора и выполнения операций над несколькими объектами одновременно. Выполнить операцию над несколькими объектами можно только тогда, когда она допустима для всех выбранных объектов.
Для выбора нескольких записей нужно зажать и удерживать клавиши **<CTRL>** или **<SHIFT>**. Для сброса множественного выбора записей нужно активировать функцию «Сбросить» экранной кнопки **[Выбрать строки]** или нажать на произвольную строку таблицы.

Существуют варианты выбора записей таблицы, доступные через выпадающий список экранной кнопки **[Выбрать строки]**, а именно:

- выделить все строки таблицы, активировав «Выбрать все»;
- выделить все строки на текущей странице таблицы, активировав «Выбрать все на стр.»;
- сбросить выделение строк, активировав «Сбросить».

В случае изменения ширины столбцов или их порядка произойдет сброс ранее выполненного множественного выбора записей.

Для обновления значений таблицы используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список (см. Рисунок 67) со значениями интервала в минутах, расположенный рядом с указанным элементом.

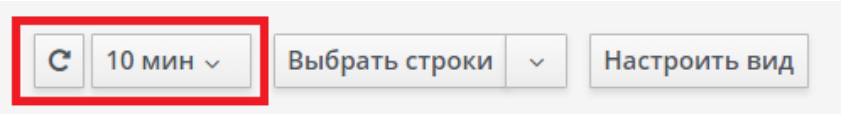

Рисунок 67 – Обновление значений таблицы

Внешний вид таблицы списка активных сессий можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться экранной кнопкой **[Настроить вид]** и отметить наименования столбцов (см. Рисунок 68), которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для применения изменений нужно нажать экранную кнопку **[Сохранить]**. При

попытке убрать выбор со всех пунктов экранная кнопка **[Сохранить]** будет заблокирована. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить вид]**;

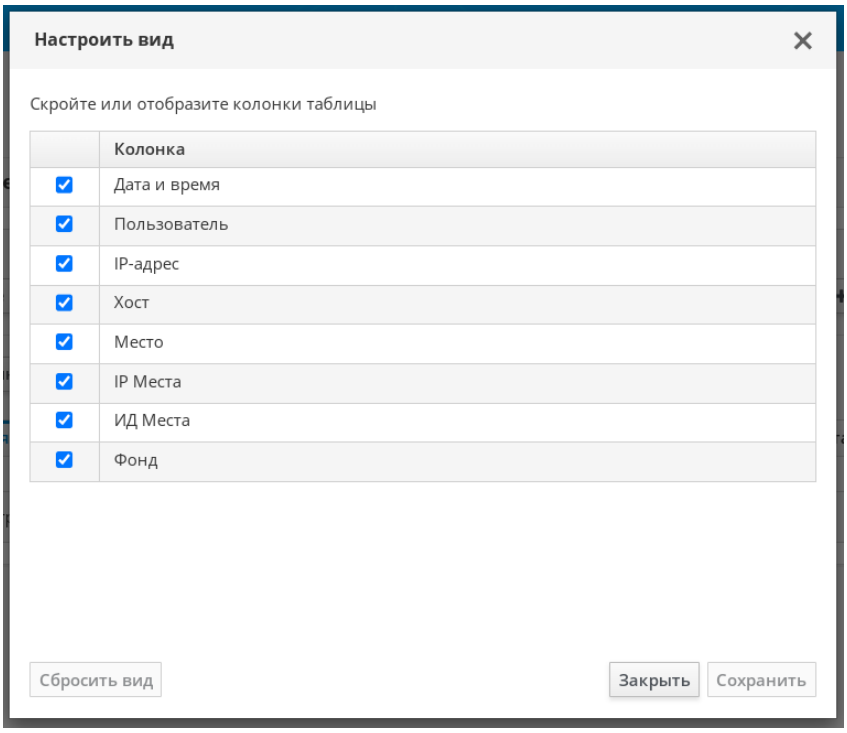

Рисунок 68 – Выбор столбцов для отображения

- порядок следования столбцов. Для изменения порядка следования нужно захватить левой кнопкой мыши заголовок столбца, и, не отпуская кнопку мыши, перенести его в нужное расположение (см. Рисунок 69). Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок колонок]**, которая становится доступна только после изменения порядка следования столбцов и будет скрыта после сброса;

Рисунок 69 – Изменение порядка следования столбцов

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.

10.11.2 . Фильтрация списка активных сессий

На странице со списком активных сессий доступен механизм фильтрации (см. Рисунок 66). Фильтрация осуществляется путем задания значений для параметров «Атрибут», «Условие» и «Значение».

Для добавления дополнительного фильтра следует нажать экранную кнопку **[+]**. Для удаления фильтра нужно использовать экранную кнопку **[-]** в соответствующей строке. Максимально допустимое число фильтров - 15.

Чтобы применить установленные параметры фильтрации, следует нажать экранную кнопку **[Применить]**.

Экранная кнопка **[Очистить]** сбрасывает все фильтры, возвращая значения к исходному состоянию: удаляются дополнительные строки фильтра (остается только одна строка), все значения сбрасываются, поля «Условие» и «Значение» блокируются.

Подробное описание механизма фильтрации списка сессий приведено в таблице (см. Таблица 89).

При ручном вводе данных в поле фильтра «Значение» допускается полный или частичный ввод только одного параметра фильтрации.

При применении нескольких одинаковых фильтров к списку, фильтрация выполняется с учетом только последнего заданного фильтра.

Таблица 89 – Параметры фильтрации списка РМ

Атрибут	Условия	Значение
«Дата»	Формирование списка сессий: ▪ «В пределах» - в указанном временном промежутке; ▪ «Не в пределах» - исключая указанный временной промежуток	▪ «Минута»; ▪ «5 минут»; ▪ «30 минут»; ▪ «1 час»; ▪ «12 часов»; ▪ «24 часа»; ▪ «Сегодня»; ▪ «Эта неделя»; ▪ «Этот месяц»
«Пользователь»	Формирование списка сессий: ▪ «Является» - по указанному имени пользователя; ▪ «Не является» - исключая указанное имя пользователя; ▪ «Начинается с» - по начальной части имени пользователя; ▪ «Оканчивается на» - по конечной части имени пользователя; ▪ «Содержит» - включая указанную часть имени пользователя	Ручной ввод
«IP-адрес»	Формирование списка сессий: ▪ «Является» - по указанному IP-адресу инициатора сессии; ▪ «Не является» - исключая указанный IP-адрес инициатора сессии; ▪ «Начинается с» - по начальной части IP-адреса инициатора сессии; ▪ «Оканчивается на» - по конечной части IP-адреса инициатора сессии; ▪ «Содержит» - включая указанную часть IP-адреса инициатора сессии	Ручной ввод

Атрибут	Условия	Значение
«Хост»	Формирование списка сессий: ▪ «Является» - по указанному наименованию инициатора сессии; ▪ «Не является» - исключая указанное наименование инициатора сессии; ▪ «Начинается с» - по начальной части наименования инициатора сессии; ▪ «Оканчивается на» - по конечной части наименования инициатора сессии; ▪ «Содержит» - включая указанную часть наименования инициатора сессии	Ручной ввод
«Место»	Формирование списка сессий: ▪ «Является» - по указанному наименованию РМ, выданного пользователю; ▪ «Не является» - исключая указанное наименование РМ, выданного пользователю; ▪ «Начинается с» - по начальной части наименования РМ, выданного пользователю; ▪ «Оканчивается на» - по конечной части наименования РМ, выданного пользователю; ▪ «Содержит» - включая указанную часть наименования РМ, выданного пользователю	Ручной ввод
«IP Места»	Формирование списка сессий: ▪ «Является» - по указанному IP-адресу РМ, выданного пользователю; ▪ «Не является» - исключая указанный IP-адрес РМ, выданного пользователю; ▪ «Начинается с» - по начальной части IP-адреса РМ, выданного пользователю; ▪ «Оканчивается на» - по конечной части IP-адреса РМ, выданного пользователю; ▪ «Содержит» - включая указанную часть IP-адреса РМ, выданного пользователю	Ручной ввод
«ИД Места»	Формирование списка сессий: ▪ «Является» - по указанному идентификатору РМ, выданного пользователю; ▪ «Не является» - исключая указанный идентификатор РМ, выданного пользователю; ▪ «Начинается с» - по начальной части идентификатора РМ, выданного пользователю; ▪ «Оканчивается на» - по конечной части идентификатора РМ, выданного пользователю; ▪ «Содержит» - включая указанную часть идентификатора РМ, выданного пользователю	Ручной ввод
«Фонд»	Формирование списка сессий: ▪ «Является» - по указанному наименованию фонда, в котором находится РМ; ▪ «Не является» - исключая указанное наименование фонда, в котором находится РМ; ▪ «Начинается с» - по начальной части наименования фонда, в котором находится РМ; ▪ «Оканчивается на» - по конечной части наименования фонда, в котором находится РМ; ▪ «Содержит» - включая указанную часть наименования фонда, в котором находится РМ	Ручной ввод

10.12 . Настройка автоматического подключения к фонду РМ

10.12.1 . Автоматическое подключение к фонду РМ

Автоматическое подключение к фонду РМ позволяет компоненту «Клиент» выполнить поиск в сети компонента «Универсальный диспетчер» и реализовать автоматическое подключение к опубликованным фондам.

Для автоматического подключения к фонду РМ после настройки автоматического поиска сервера подключений на узле с установленным Termidesk следует перейти «Настройки - Системные параметры - Общие», активировать параметр «Автозапуск рабочего места» и нажать экранную кнопку **[Сохранить]**.

⚠ Для автоматического подключения к фонду РМ нужно настроить группы доступа к фондам так, чтобы пользователям из каждой группы был доступен только один фонд. Если пользователь является членом нескольких групп, и каждой из этих групп предоставлен доступ к отдельному фонду РМ, то пользователь получает доступ к нескольким фондам одновременно. В таком случае, автоматическое подключение невыполнимо. При этом возможность ручного подключения сохраняется.

⚠ Для корректной работы автоматического подключения к фонду РМ необходимо выполнить настройку службы DNS.

10.12.2 . Настройка автоматического поиска в сети сервера Termidesk

Автоматический поиск сервера подключений позволяет компоненту «Клиент» выполнить поиск в сети компонента «Универсальный диспетчер».

Для этого на DNS-сервере должна быть внесена одна из записей:

- либо запись `daas` типа `TXT` с URL-адресом сервера Termidesk, например: `https://termidesk.domain.local`;
- либо запись `vdi` типа `TXT` с URL-адресом сервера Termidesk, например: `https://termidesk.domain.local`.

10.13 . Режим техобслуживания фонда РМ

10.13.1 . Режим техобслуживания фонда для BPM

Режим техобслуживания фонда для BPM - это запрет пользователям подключаться (создавать новую сессию) и/или переподключаться повторно в существующую сессию фонда РМ. Этот режим предназначен для проведения плановых регламентных или аварийных работ, например, когда нужно применить обновления или исправления для гостевых ОС или ВМ и требуется временно прекратить новые подключения к фонду.

> Режим техобслуживания может применяться и к отдельным ВМ в выбранном фонде (см. подраздел **Управление состоянием ВМ в назначенном фонде РМ**).

Для перевода фонда в режим техобслуживания следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить» (см. Рисунок 70). Затем подтвердить включение режима.

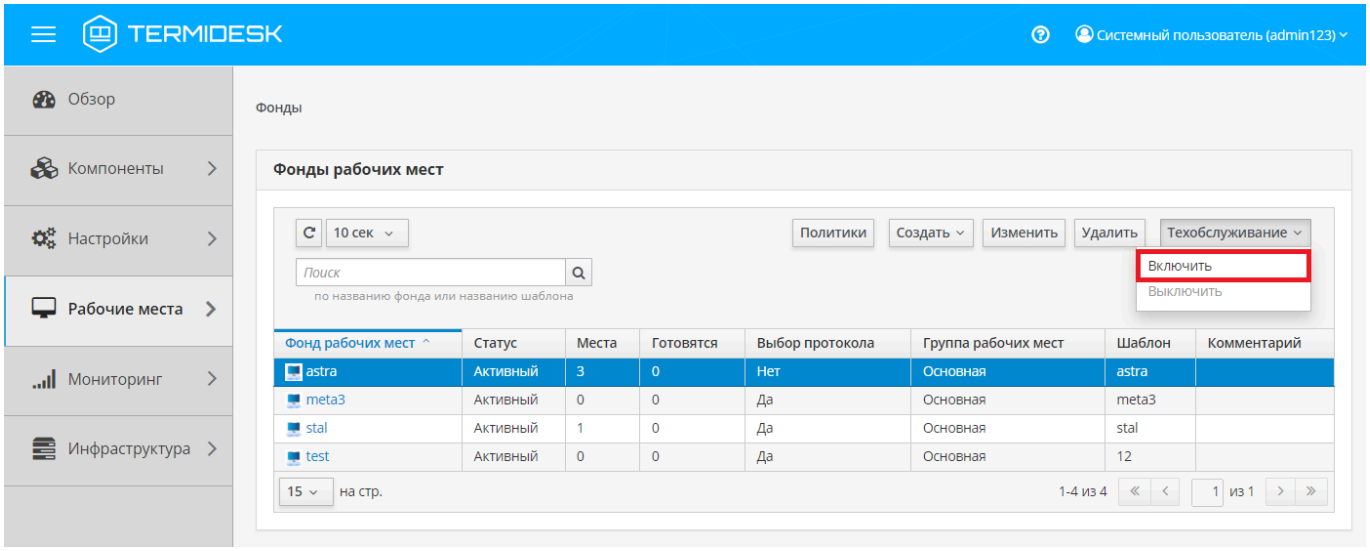

Рисунок 70 – Перевод фонда ВРМ в режим техобслуживания

Состояние режима техобслуживания будет отображено в столбце «Статус» списка фондов.

Для отключения режима техобслуживания нужно выбрать фонд, нажать экранную кнопку **[Техобслуживание]**, а затем выбрать из выпадающего списка значение «Выключить». По завершении техобслуживания фонд может быть снова использован для размещения РМ.

10.13.2 . Режим техобслуживания фонда терминального сервера

Режим техобслуживания фонда - это запрет пользователям подключаться (создавать новую сессию) и/или переподключаться повторно в существующую сессию фонда терминального сервера. Этот режим предназначен для проведения плановых регламентных или аварийных работ, например, когда нужно применить обновления или исправления для терминального сервера и требуется временно прекратить новые подключения к фонду.

> Режим техобслуживания может применяться и к отдельному терминальному серверу в выбранном фонде (см. подраздел **Управление терминальными сессиями в назначенном фонде РМ**).

Для перевода фонда в режим техобслуживания следует перейти «Компоненты - Фонды» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить» (см. Рисунок 71). Затем подтвердить включение режима.

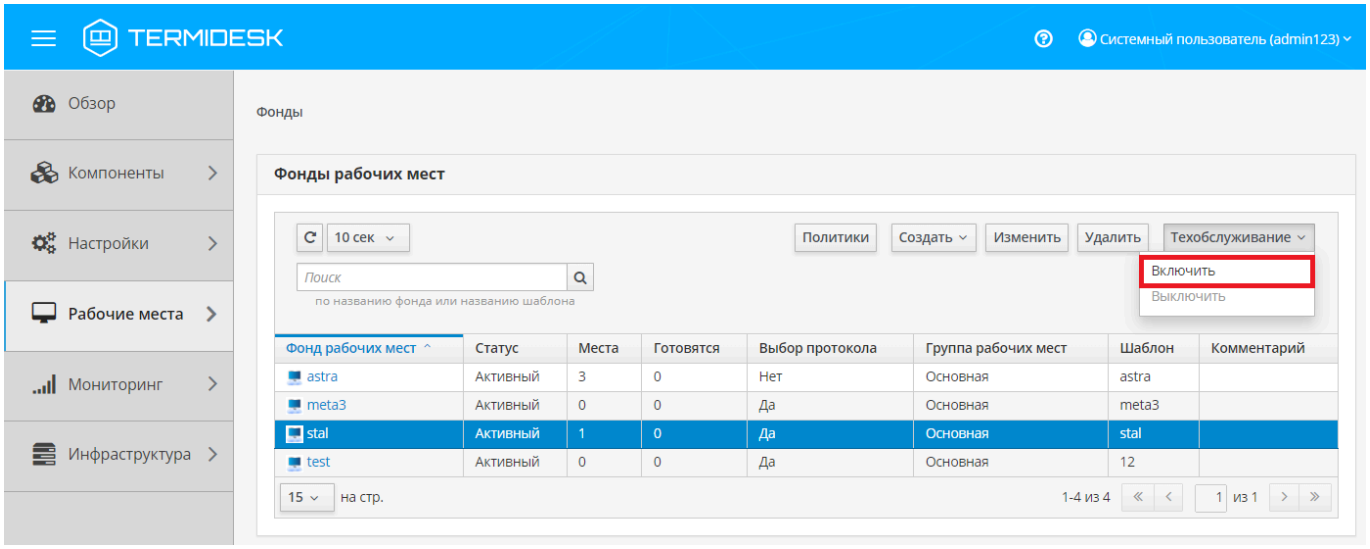

Рисунок 71 – Перевод фонда терминального сервера в режим техобслуживания

Состояние режима техобслуживания будет отображено в столбце «Статус» списка фондов.

Для отключения режима техобслуживания нужно выбрать фонд терминального сервера, нажать экранную кнопку **[Техобслуживание]**, а затем выбрать из выпадающего списка значение «Выключить». По завершении техобслуживания фонд может быть снова использован.

10.14 . Управление расписанием задач

Расписание позволяет составить график задач, которые должны быть выполнены для фондов РМ.

Для отображения списка задач следует перейти «Рабочие места - Расписания». Основные параметры списка приведены в таблице (см. Таблица 90). Сортировка списка выполняется по столбцу «Название».

Таблица 90 – Параметры списка расписаний

Параметр	Описание
«Название»	Текстовое наименование задачи
«Действие»	Действие, выполняемое в рамках расписания
«Фонды»	Список фондов, к которым будет применена задача
«Включено»	Отображение состояния задачи
«Комментарий»	Информационное сообщение, используемое для описания назначения задачи
«Дата активации»	Дата активации задачи
«Время начала»	Время начала очередного действия задачи
«Повтор»	Периодичность выполнения задачи
«Длительность»	Длительность (в минутах) выполнения задачи с момента, заданного в параметре «Время начала»

Над созданными задачами можно выполнить следующие действия:

- отредактировать, для этого нажать экранную кнопку **[Изменить]**;

- удалить, для этого нажать экранную кнопку **[Удалить]**. При попытке удаления активной задачи будет отображено сообщение: «Вы уверены, что хотите удалить расписание, которое используется?». Удаление активной задачи производится без учета ее текущего выполнения;
- изменить состояние задачи, для этого нажать экранную кнопку **[Активация]** и выбрать соответствующий пункт:
  - **[Включить]** - активировать задачу;
  - **[Выключить]** - деактивировать задачу.

Для поиска задачи предусмотрено поле «Поиск». Предусмотрен поиск по параметрам «Название», «Фонды», «Комментарий».

Для добавления задачи в раскрывающемся списке экранной кнопки **[Создать]** следует выбрать тип действия, которое будет выполняться по расписанию:

- «Запуск» - включение ВМ, реализуется через гипервизор;
- «Перезагрузка» - перезагрузка ВМ, реализуется через гипервизор;
- «Перезагрузка (безопасная)» - перезагрузка ВМ, реализуется через гипервизор. В ВМ должен быть установлен пакет инструментов «Guest tools», который предоставляется производителем гипервизора;
- «Пауза» - приостанов ВМ, реализуется через гипервизор;
- «Останов (небезопасный)» - выключение ВМ, реализуется через гипервизор;
- «Выключение (безопасное)» - выключение ВМ, реализуется через гипервизор. В ВМ должен быть установлен пакет инструментов «Guest tools», который предоставляется производителем гипервизора;
- «Восстановление» (откат к снапшоту) - восстановление ВМ из базового снимка (снапшота), реализуется через гипервизор;
- «Техобслуживание» - отправка ВМ на техобслуживание.

Действия, реализуемые через гипервизор, могут быть успешно выполнены только на гипервизорах, поддерживающих указанные команды.
Действие «Восстановление» будет доступно оператору, если у него есть пользовательское разрешение «Восстановление рабочих мест».

Для корректной работы расписаний для узлов Termidesk должна быть настроена синхронизация времени (см. подраздел **Требования к синхронизации времени** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса»).

Доступные для заполнения параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 91). Для сохранения конфигурации нужно использовать экранную кнопку **[Сохранить]**.

Таблица 91 – Параметры расписаний

Параметр	Описание
«Включено»	Управление состоянием задачи. Возможные значения: ▪ «Да» (по умолчанию) - задача активирована; ▪ «Нет» - задача деактивирована. Если задача уже успела активироваться, то при ее выключении (значение «Нет» переключателя параметра) действие будет применено в этот раз, но не в следующий
«Название»	Текстовое наименование создаваемой задачи
«Комментарий»	Информационное сообщение, используемое для описания назначения задачи
«Фонды»	Выбор одного или нескольких фондов, к которым будет применена задача
«Дата активации расписания»	Дата активации задачи по расписанию. Задача расписания активируется в 00:00 указанного дня
«Время начала»	Время начала очередного действия задачи по расписанию
«Длительность»	Длительность (в минутах) выполнения задачи с момента, заданного в параметре «Время начала». Возможные значения: ▪ «1 мин.»; ▪ «5 мин.»; ▪ «15 мин.» (по умолчанию); ▪ «30 мин.»; ▪ «60 мин.»; ▪ «180 мин. (3 ч.)»; ▪ «360 мин. (6 ч.)»
«Повтор»	Выбор периодичности запуска задачи. Возможные значения: ▪ «Дни недели»; ▪ «Дни месяца»
«Дни недели»	Выбор одного или нескольких дней недели, в которые будет запускаться задача. Доступен при выборе значения «Дни недели» в параметре «Повтор». Возможные значения: ▪ «Понедельник»; ▪ «Вторник»; ▪ «Среда»; ▪ «Четверг»; ▪ «Пятница»; ▪ «Суббота»; ▪ «Воскресенье»
«Дни месяца»	Указание даты или дат (через запятую), в которые будет запускаться задача ежемесячно. Параметр доступен при выборе значения «Дни месяца» в параметре «Повтор». Допускается использование специального значения «*» - все дни месяца. Пример: «10,20,30»

Параметр	Описание
«Включение всех назначенных рабочих мест»	Управление состоянием назначенных РМ. Доступен при выборе действия «Запуск» в раскрывающемся списке экранной кнопки **[Создать]**. Возможные значения: ▪ «Да» (по умолчанию) - ВМ назначенных РМ будут включены; ▪ «Нет» - ВМ назначенных РМ не будут включены
«Включение неназначенных рабочих мест»	Выбор того, как будут учитываться ВМ, которые были запущены до активации задачи и не были назначены пользователю. Доступен при выборе действия «Запуск» в раскрывающемся списке экранной кнопки **[Создать]**. Возможные значения: ▪ «Процент от общего числа» (по умолчанию); ▪ «Абсолютное число»
«Выключение рабочих мест»	Выбор того, как будут учитываться ВМ, которые были запущены до активации задачи. Доступен при выборе действия «Останов (небезопасный)» в раскрывающемся списке экранной кнопки **[Создать]**. Возможные значения: ▪ «Процент от общего числа»; ▪ «Абсолютное число» (по умолчанию)
«Процент от общего числа»	Процент запускаемых или выключаемых ВМ, рассчитывается от общего числа ВМ в фонде. Доступен при выборе действия «Запуск» или «Останов (небезопасный)» в раскрывающемся списке экранной кнопки **[Создать]**. Параметр позволяет регулировать долю запускаемых или выключаемых ВМ в течение времени, заданного в параметре «Длительность». Например, если общее число ВМ составляет 100, и для параметра «Процент от общего числа» установлено значение «30», а для параметра «Длительность» установлено значение «15 мин.», то в течение 15 минут 30 ВМ будут запускаться или выключаться по 2 машины каждую минуту. Соотношение параметров «Длительность», «Процент от общего числа» и «Абсолютное число» позволяет оптимизировать нагрузку на платформу виртуализации. По умолчанию для действия «Запуск»: «20». По умолчанию для действия «Останов (небезопасный)»: «1»
«Абсолютное число»	Число запускаемых или выключаемых ВМ. Доступен при выборе действия «Запуск» или «Останов (небезопасный)» в раскрывающемся списке экранной кнопки **[Создать]**. Параметр позволяет регулировать количество запускаемых или выключаемых ВМ в течение времени, заданного в параметре «Длительность». Например, если для параметра «Абсолютное число» установлено значение «30», а для параметра «Длительность» установлено значение «15 мин.», то в течение 15 минут будут запускаться или выключаться по 2 машины каждую минуту. По умолчанию для действия «Запуск»: «20». По умолчанию для действия «Останов (небезопасный)»: «1»

11 . СИСТЕМНЫЕ НАСТРОЙКИ

11.1 . Параметры конфигурирования компонентов «Универсальный диспетчер», «Менеджер рабочих мест»

Для настройки «Универсального диспетчера», «Менеджера рабочих мест» используется конфигурационный файл `/etc/opt/termidesk-vdi/termidesk.conf`.

> При установке пакета `termidesk-vdi` возможно активировать режим отладки инсталлятора через переменную окружения `TDSK_PKG_DEBUG=1`.

Перечень параметров, задающихся через файл, приведен в таблице (см. Таблица 92). Указанные параметры можно поменять также через утилиту `termidesk-config` (см. подраздел **Утилита termidesk-config**).

Перечень параметров, используемых в других компонентах программного комплекса, приведен в соответствующих им документах.

Таблица 92 – Параметры конфигурирования

Параметр	Значение по умолчанию	Описание
Настройки параметров перемещаемых профилей		
`TDSK_AUTOFS_IMAGES_ID`	Не задано	Параметр может быть задан на узлах «Универсального диспетчера». Используется для настройки шаблонов перемещаемых профилей. В качестве значения используются идентификаторы дисков. Пример: `TDSK_AUTOFS_IMAGES_ID=xx[,yy[,zz[,...]]]`
Настройки подключения к СУБД		
`DB_CLUSTER_MODE`	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет тип установки СУБД, к которой осуществляется подключение. Возможные значения: ▪ `single` - подключение производится к отдельному серверу СУБД; ▪ `cluster` - подключение производится к кластеру СУБД
`DBHOST`	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет IP-адрес или FQDN СУБД PostgreSQL. Начальное значение задается на этапе подготовке среды функционирования и установки Termidesk
`DBHOST2`	Не задано	Параметр необязательный, может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет IP-адрес или FQDN дополнительного узла СУБД PostgreSQL, если используется подключение к кластеру СУБД (см. параметр `DB_CLUSTER_MODE`). Начальное значение задается на этапе установки Termidesk

Параметр	Значение по умолчанию	Описание
DBHOST3	Не задано	Параметр необязательный, может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет IP-адрес или FQDN дополнительного узла СУБД PostgreSQL, если используется подключение к кластеру СУБД (см. параметр DB_CLUSTER_MODE). Начальное значение задается на этапе установки Termidesk
DBPORT	5432	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет порт соединения с сервером БД
DBSSL	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет протокол подключения к БД. Возможные значения: ▪ Disable; ▪ TLSv1.2; ▪ TLSv1.3. Начальное значение задается на этапе установки Termidesk
DBNAME	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет имя БД. Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk
DBUSER	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет имя пользователя, имеющего доступ к БД. Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk

Параметр	Значение по умолчанию	Описание
DBPASS	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет 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. Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой `scramble`: ▪ для получения значения по стандартному алгоритму: `/opt/termidesk/bin/scramble --value <пароль> --type AES256`; ▪ для получения значения с увеличенным числом итераций преобразования: `/opt/termidesk/bin/scramble --value <пароль> --type AES256_V2`. ⚠ Если значение пароля указывается в формате ключа (значение предваряется символом «-»), то следует изменить его передачу в параметр `--value`: `/opt/termidesk/bin/scramble --value=<-пароль> --type AES256` Утилита `scramble` использует в качестве вектора преобразования значение из файла `/etc/opt/termidesk-vdi/termidesk.cookie`. Значение генерируется автоматически на этапе установки Termidesk

DBCERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».
		Определяет путь к клиентскому сертификату mTLS для защищенного подключения к БД.
		⚠ mTLS - метод обеспечения защищенного соединения с БД через двустороннюю аутентификацию с использованием сертификатов.
		Для использования сертификата нужно:
		▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;
		▪ назначить владельцем файла пользователя `termidesk`:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**).
		Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:
		`DBCERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'`

Параметр	Значение по умолчанию	Описание

DBKEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».
		Определяет путь к ключу mTLS для защищенного подключения к БД.
		Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению:
		`openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key>`
		Для использования ключа также нужно:
		▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;
		▪ назначить владельцем файла пользователя `termidesk`:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.
		Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:
		`DBKEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'`

DBCHAIN	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».
		Определяет путь к промежуточному сертификату mTLS для защищенного подключения к БД.
		Для использования сертификата нужно:
		▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;
		▪ назначить владельцем файла пользователя `termidesk`:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.
		Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:
		`DBCHAIN='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/ca'`

Настройка проверки данных при взаимодействии компонентов Termidesk		
DJANGO_SECRET_KEY	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Используется для проверки данных, пересылаемых между компонентами Termidesk. Значение генерируется при установке Termidesk и должно быть одинаковым для всех узлов при распределенной установке
Настройка подключения к RabbitMQ		

Параметр	Значение по умолчанию	Описание
RABBITMQ_URL	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет URL-адрес подключения к серверам RabbitMQ. Можно подключить до трех (включительно) серверов. Пароль подключения к серверу RabbitMQ, указанный в RABBITMQ_URL, хранится в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf в преобразованном виде. Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой scramble: ▪ для получения значения по стандартному алгоритму: /opt/termidesk/bin/scramble --value <пароль> --type AES256 ▪ для получения значения с увеличенным числом итераций преобразования: /opt/termidesk/bin/scramble --value <пароль> --type AES256_V2 ⚠ Если значение пароля указывается в формате ключа (значение предваряется символом «-»), то следует изменить его передачу в параметр --value: /opt/termidesk/bin/scramble --value=<-пароль> --type AES256 Для использования преобразованного значения следует указать его в RABBITMQ_URL и выполнить перезапуск служб. Начальное значение RABBITMQ_URL задается на этапе установки
RABBITMQ_SSL	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет протокол подключения к RabbitMQ. Возможные значения: Disable, TLSv1.2. Начальное значение задается на этапе установки
Настройки защищенного подключения к RabbitMQ		
CELERY_BROKER_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому сертификату mTLS для защищенного подключения к RabbitMQ. Для использования сертификата нужно: ▪ скопировать его в каталог /etc/opt/termidesk-vdi/; ▪ назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt ▪ изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt ▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища: CELERY_BROKER_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'

Параметр	Значение по умолчанию	Описание

CELERY_BROKER_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».
		Определяет путь к закрытому ключу mTLS для защищенного подключения к RabbitMQ.
		Ключ может иметь парольную защиту. Для использования в Termidesk нужно преобразовать его к начальному значению:
		`openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key>`
		Для использования ключа также нужно:
		▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;
		▪ назначить владельцем файла пользователя `termidesk`:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.
		Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:
		`CELERY_BROKER_KEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'`

CELERY_BROKER_CA	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».
		Определяет путь к корневому сертификату ЦС mTLS для защищенного подключения к RabbitMQ.
		Для использования сертификата нужно:
		▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;
		▪ назначить владельцем файла пользователя `termidesk`:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**).
		Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:
		`CELERY_BROKER_CA='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/ca'`

Настройки установленных ролей Termidesk		
NODE_ROLES	Не задано	Параметр обязателен и задается на этапе установки. Определяет тип роли, с которой будет установлен Termidesk. Возможные значения: ▪ `ADMIN` - роль «Портал администратора»; ▪ `USER` - роль «Портал пользователя»; ▪ `CELERYMAN` - роль «Менеджер рабочих мест»; ▪ `AGGR_ADM` - роль «Агрегатор администратора»; ▪ `AGGR_USR` - роль «Агрегатор пользователя». ⓘ Установка ролей «Агрегатор администратора» и/или «Агрегатор пользователя» должна производиться на узле, отличном от «Портала администратора» и/или «Портала пользователя». Таким образом одновременно на одном узле могут быть заданы роли: ▪ либо `ADMIN` и (или) `USER`; ▪ либо `AGGR_ADM` и (или) `AGGR_USR`. При переустановке значение параметра в конфигурационном файле будет перезаписано

Параметр	Значение по умолчанию	Описание
Настройки журналирования		
LOG_LEVEL	INFO	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет уровень журналирования сообщений. Возможные значения: DEBUG, INFO, WARNING, ERROR, CRITICAL
LOG_ADDRESS	/dev/log	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет адрес отправки записей в системный журнал. Обычно это /dev/log для Linux-систем. Возможно указать IP-адрес и порт
LOG_FACILITY	local3	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет категорию сообщений syslog. Категория должна совпадать с настройками в конфигурационном файле /etc/syslog-ng/conffirst.d/termidesk.conf
Настройки токена доступа к API для проверок состояния служб Termidesk		
HEALTH_CHECK_ACCESS_KEY	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет токен доступа к API проверки состояния сервера. Начальное значение генерируется на этапе установки. 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). Значение также может быть сгенерировано через openssl: `openssl rand -hex 32`
Настройки токена доступа к API получения метрик узла		
METRICS_ACCESS_KEY	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет токен доступа к API получения метрик узла. Начальное значение генерируется на этапе установки. 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). Значение также может быть сгенерировано через openssl: `openssl rand -hex 32`
Настройки защищенного подключения для проверок состояния служб «Менеджера рабочих мест»		

Параметр	Значение по умолчанию	Описание

HEALTH_CHECK_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора» (в зависимости от варианта установки).
		Определяет путь к сертификату SSL/TLS для защищенного подключения к API проверки состояния служб «Менеджера рабочих мест».
		Для использования сертификата нужно:
		▪ скопировать его в каталог /etc/opt/termidesk-vdi/;
		▪ назначить владельцем файла пользователя termidesk:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.
		Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:
		`HEALTH_CHECK_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'`

HEALTH_CHECK_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора» (в зависимости от варианта установки).
		Определяет путь к ключу SSL/TLS для защищенного подключения к API проверки состояния служб «Менеджера рабочих мест».
		Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению:
		`openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key>`
		Для использования ключа также нужно:
		▪ скопировать его в каталог /etc/opt/termidesk-vdi/;
		▪ назначить владельцем файла пользователя termidesk:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.
		Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:
		`HEALTH_CHECK_KEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'`

Настройки компонента «Менеджер рабочих мест» (службы termidesk-celery-beat)		
CELERY_BEAT_HEALTH_CHECK_PORT	8103	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест». Изначально параметр закомментирован (используется значение по умолчанию)
CELERY_BEAT_HEALTH_CHECK_IP	0.0.0.0	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет IP-адрес, с которым служба termidesk-celery-beat регистрируется в подсистеме проверки состояния на странице «Инфраструктура» Termidesk. Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла. Изначально параметр закомментирован (используется значение по умолчанию)
Настройки компонента «Менеджер рабочих мест» (службы termidesk-celery-worker)		

Параметр	Значение по умолчанию	Описание
CELERY_WORKER_HEALTH_CHECK_PORT	8104	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест». Изначально параметр закомментирован (используется значение по умолчанию)
CELERY_WORKER_HEALTH_CHECK_IP	0.0.0.0	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет IP-адрес, с которым служба `termidesk-celery-worker` регистрируется в подсистеме проверки состояния на странице «Инфраструктура». Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла. Изначально параметр закомментирован (используется значение по умолчанию)
Настройки подключения к серверу «Удаленного помощника»		

REMOTE_ASSISTANT_SERVER_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора».
		Определяет путь к серверному сертификату SSL/TLS для проверки подключения к «Удаленному помощнику».
		Для использования сертификата нужно:
		▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;
		▪ назначить владельцем файла пользователя `termidesk`:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.
		Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:
		`REMOTE_ASSISTANT_SERVER_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'`

Настройки доверенных корневых сертификатов		
REQUESTS_CA_BUNDLE	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к файлу с доверенным корневым сертификатом, задается для настройки работы с сертификатами собственных ЦС. По умолчанию параметр не используется (закомментирован)
Настройки принятия лицензионного соглашения		
EULA_ACCEPTED	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет принятие лицензионного соглашения при установке. В случае автоматизированной установки наличие параметра обязательно
Настройки взаимодействия между узлами «Агрегатора» и «Универсального диспетчера»		
AGGREGATOR_JWT_SSL_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», использующихся в фермах, подключаемых к «Агрегатору». Обязателен для заполнения в случае, если в инфраструктуре также используется «Агрегатор». Определяет путь к сертификату для получения значения JWT-токена «Агрегатора»

Параметр	Значение по умолчанию	Описание
AGGREGATOR_JWT_SSL_CERT_SECOND	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», использующихся в фермах, подключаемых к «Агрегатору». Обязателен для заполнения в случае, если в инфраструктуре также используется «Агрегатор». Определяет путь к резервному сертификату для получения значения JWT-токена «Агрегатора». Если сертификат, заданный в AGGREGATOR_JWT_SSL_CERT, станет невалидным, то будет использоваться сертификат, указанный в AGGREGATOR_JWT_SSL_CERT_SECOND
AGGREGATOR_JWT_SSL_KEY	Не задано	Параметр обязателен и задается на узлах с установленным «Агрегатором» (портал «Агрегатор пользователя»). Определяет путь к ключу для подписи JWT-токена «Агрегатора»
AGGREGATOR_ACCESS_TOKEN_TITLE	Termidesk JWT Title	Параметр обязателен и должен быть одинаковым на всех узлах, работающих совместно: на «Агрегаторе» (портал «Агрегатор пользователя»), на «Универсальных диспетчерах», подключаемых к «Агрегатору». Задает заголовок JWT-токена, предназначенный для настройки взаимодействия между «Агрегатором» и «Универсальным диспетчером»
AGGREGATOR_ACCESS_TOKEN_TTL_SECONDS	600	Параметр обязателен и задается на узлах с установленным «Агрегатором». Определяет времени жизни (в секундах) JWT-токена, подписанного «Агрегатором»
AGGREGATOR_IMAGE_CACHE_LIFETIME_HOURS	672	Параметр обязателен и задается на узлах с установленным «Агрегатором». Определяет время жизни (в часах) кеша иконок фондов РМ. По истечении этого времени иконка обновляется
Настройки подключения к хранилищу паролей OpenBao		
SECRETS_STORAGE_METHOD	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет способ хранения паролей подключения к СУБД и RabbitMQ: ▪ config - пароли будут храниться в преобразованном виде в файле /etc/opt/termidesk-vdi/termidesk.conf; ▪ hvac - для хранения паролей будет использоваться хранилище паролей OpenBao или Hashicorp Vault (хранилище должно быть заранее создано и настроено). Подробная информация по этому способу хранения паролей приведена в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»; ▪ openbao - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено). При этом пароли располагаются внутри хранилища, имена контейнеров хранения генерируются автоматически. ⚠ Хранилище паролей OpenBao должно быть реализовано в отказоустойчивом варианте, иначе Termidesk не будет работать в период простоя узлов OpenBao. Начальное значение задается на этапе установки

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_URL	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет IP-адреса или FQDN узла и порта с установленным хранилищем OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Формат: http://<IP-адрес или FQDN>:8200. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом. Начальное значение задается на этапе установки
SECRETS_OPENBAO_TOKEN	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет токен (Initial Root Token), сформированный при инициализации хранилища OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки и хранится в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf в преобразованном виде. Для преобразования значения параметра, заданного вручную, следует воспользоваться утилитой scramble: ▪ для получения значения по стандартному алгоритму: /opt/termidesk/bin/scramble --value <пароль> --type AES256 ▪ для получения значения с увеличенным числом итераций преобразования: /opt/termidesk/bin/scramble --value <пароль> --type AES256_V2 ⚠ Если значение пароля указывается в формате ключа (значение предваряется символом «-»), то следует изменить его передачу в параметр--value: /opt/termidesk/bin/scramble --value=<-пароль> --type AES256
SECRETS_OPENBAO_DB_PATH	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь, настроенный на OpenBao для хранения пароля СУБД. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки
SECRETS_OPENBAO_DB_ROLE_NAME	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет роль, настроенную на OpenBao и имеющую доступ к паролю СУБД. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки
SECRETS_OPENBAO_RABBITMQ_PATH	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора»». Определяет путь, настроенный на OpenBao для хранения пароля RabbitMQ. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки
SECRETS_OPENBAO_RABBITMQ_ROLE_NAME	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет роль, настроенную на OpenBao и имеющую доступ к паролю RabbitMQ. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки

Параметр	Значение по умолчанию	Описание

SECRETS_OPENBAO_CLIENT_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».
		Определяет путь к сертификату mTLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы.
		Для использования сертификата нужно:
		▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;
		▪ назначить владельцем файла пользователя `termidesk`:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.
		Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:
		`SECRETS_OPENBAO_CLIENT_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'`

SECRETS_OPENBAO_CLIENT_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».
		Определяет путь к ключу mTLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы.
		Ключ может иметь парольную защиту. Для использования ключа в Termidesk нужно преобразовать его к начальному значению:
		`openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key>`
		Для использования ключа также нужно:
		▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;
		▪ назначить владельцем файла пользователя `termidesk`:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.
		Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:
		`SECRETS_OPENBAO_CLIENT_KEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'`

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_SERVER_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к промежуточному сертификату ЦС mTLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы. Для использования сертификата нужно: ▪ скопировать его в каталог /etc/opt/termidesk-vdi/; ▪ назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem ▪ изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem ▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища: SECRETS_OPENBAO_SERVER_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'
SECRETS_OPENBAO_TERMIDESK_PATH	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь, настроенный на OpenBao для хранения паролей Termidesk. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки
SECRETS_OPENBAO_TERMIDESK_ROLE_NAME	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет роль, настроенную на OpenBao и имеющую доступ к паролям Termidesk. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки
SECRETS_OPENBAO_KV_VERSION	1	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Используется для указания версии API OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Возможные значения: ▪ 1 (по умолчанию); ▪ 2. Начальное значение задается на этапе установки
SECRETS_OPENBAO_CACHE_LIFETIME	5	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти. Позволяет сохранить полученный от OpenBao пароль на некоторое время в кеше для сокращения количества обращений к OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки
Настройки взаимодействия с узлом «Ретранслятора»		
FLUENTD_CACHE	15	Параметр может быть задан на узлах «Универсального диспетчера». Определяет время (в секундах) кеширования параметров подключения к узлу «Ретранслятора». По умолчанию после установки время кеширования составляет 15 секунд. В случае, если нужно изменить значение, следует раскомментировать параметр и задать ему новое значение

Параметр	Значение по умолчанию	Описание
FLUENTD_TABLE	logs	Параметр может быть задан на узлах «Универсального диспетчера». Определяет таблицу хранения событий фермы Termidesk. По умолчанию после установки «Универсальный диспетчер» обращается к таблице «logs» БД «Ретранслятора». В случае, если в БД «Ретранслятора» для хранения событий используется другая таблица, следует раскомментировать параметр и указать новое имя таблицы
Настройки «Шлюза»		
WSPROXY_PUB_KEY_FILE	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Задает путь к открытому ключу id_rsa.pub. Используется для подписи токенов при взаимной аутентификации «Шлюза» и «Универсального диспетчера», «Агрегатора». По умолчанию создается при первой установке и хранится в подкаталоге wsproxy. Явно задавать путь следует только при использовани внешнего хранилища (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример: WSPROXY_PUB_KEY_FILE='hvac-kv://secret#termidesk-admin/wsproxy/pub'
WSPROXY_PRIV_KEY_FILE	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Задает путь к закрытому ключу id_rsa. Используется для подписи токенов при взаимной аутентификации «Шлюза» и «Универсального диспетчера», «Агрегатора». По умолчанию создается при первой установке и хранится в подкаталоге wsproxy. Явно задавать путь следует только при использовани внешнего хранилища (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример: WSPROXY_PRIV_KEY_FILE='hvac-kv://secret#termidesk-admin/wsproxy/priv'

Пример файла конфигурации сервера OpenBao, который активирует строгую проверку клиентского SSL-сертификата:

```
listener "tcp" {
tls_min_version = "tls12"
tls_disable = "false"
address = "0.0.0.0:8200"
tls_cert_file = "/etc/bao/openbao.stand8.local.crt"
tls_key_file = "/etc/bao/openbao.stand8.local.key"
# Если включён, то будет проверять сертификат клиента на корректность
tls_require_and_verify_client_cert = "true"
# Если выключён, то будет требовать наличие сертификата клиента
tls_disable_client_certs = "false"
}
```

11.2 . Общие системные параметры Termidesk

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

Для конфигурации общих системных параметров следует перейти «Настройки - Системные параметры», выбрать раздел «Общие».

Доступные для редактирования параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 92).

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

Таблица 93 – Общие системные параметры Termidesk

Параметр	Описание
«Генератор имен»	Варианты использования имен при развертывании ВРМ. Значение по умолчанию: «С переиспользованием имен»
«Действие с учетной записью рабочего места»	Выбор действия, которое будет произведено над учетной записью в службе каталогов при удалении ВРМ из фонда. ⓘ DNS-сервер, указанный в настройках узла «Универсального диспетчера», должен иметь возможность разрешать имена узлов в зонах службы каталогов (MS AD, FreeIPA, ALD Pro). Для корректного сброса пароля учетной записи при удалении РМ из фонда на узле «Универсального диспетчера» требуется наличие сертификата, выпущенного центром сертификации для работы по протоколу LDAPS. Также на узле службы каталогов MS AD должны быть созданы соответствующие SRV-записи. Возможные значения: ▪ «Удалить при удалении фонда» (по умолчанию) - при удалении РМ из фонда учетная запись будет удалена из службы каталогов. Применимость: MS AD, FreeIPA, ALD Pro; ▪ «Сбросить пароль при удалении фонда» - при удалении РМ из фонда у учетной записи будет сброшен пароль. Применимость: MS AD; ▪ «Выключить при удалении фонда» - при удалении РМ из фонда учетная запись будет отключена. Применимость: MS AD; ▪ «Хранить при удалении фонда» - при удалении РМ из фонда учетная запись будет сохранена в службе каталогов. Применимость: MS AD, FreeIPA, ALD Pro. Следует учесть, что при вводе гостевой ОС в MS AD: ▪ если учетная запись РМ находится не в стандартном каталоге «Computers», то параметр «OU» должен принимать значения вида: «OU=Computers,DC=domain,DC=local», т.е. не должен использоваться Common Name (CN); ▪ если учетная запись РМ находится в стандартном каталоге «Computers», то параметр «OU» должен принимать значения вида: «CN=Computers,DC=domain,DC=local», т.е. должен использоваться Common Name (CN)
«Автозапуск рабочего места»	Параметр автоматического подключения к фонду РМ через компонент «Клиент» (см. подраздел **Настройка автоматического подключения к фонду РМ**). Значение по умолчанию: «Нет»

Параметр	Описание
«Подключаться к BPM по»	Параметр определяет, какое значение в параметрах подключения к BPM «Универсальный диспетчер» должен передать компоненту «Клиент». Возможные значения: ▪ «Сетевому адресу (IP)» - в параметрах подключения будет передаваться IP-адрес BPM; ▪ «Полному доменному имени (FQDN)» - в параметрах подключения будет передаваться FQDN BPM. Действие параметра не распространяется на протокол подключения к терминальному серверу - при таком подключении всегда передается IP-адрес. При использовании метапоставщика значение параметра будет учитываться: ▪ при использовании значения «Полному доменному имени (FQDN)» метапоставщик будет передавать FQDN ВМ из сервисного фонда; ▪ при использовании значения «Сетевому адресу (IP)», метапоставщик будет передавать IP-адрес ВМ из сервисного фонда
«Интервал проверок кэша рабочих мест»	Периодичность (в секундах) опроса ВМ в фонде для определения статуса их готовности. Значение по умолчанию: «19»
«Не учитывать максимальные ограничения»	Не учитывать ограничения, заданные в полях «Подготавливать ВМ одновременно» и «Удалять ВМ одновременно» поставщика ресурсов при формировании фондов. Если параметр активен, в фонде одновременно может создаваться и удаляться до 1000 ВМ. Значение по умолчанию: «Нет»
«Время хранения информационных объектов»	Время хранения (в секундах) информации о фондах в статусе «Удален», «Отменен», «Ошибка». Значение по умолчанию: «14401» Очистка фондов РМ, находящихся в статусах «Удалены», «Отменены», «Ошибка» происходит через время, указано в параметре «Время хранения информационных объектов». Периодичность удаления таких фондов составляет 30 секунд. Периодичность очистки фондов, находящихся в процессе удаления (ожидающих удаления и удаляемых), составляет 31 секунду
«Время блокировки входа»	Время (в секундах) после истечения которого будет возможен повторный вход субъекта «Администратор», «Персонал» или «Пользователь» в случае превышения субъектом лимита неудачных попыток входа. По истечении этого времени пользователь продолжит визуально быть заблокированным (статус «Временно заблокирован») в списке пользователей в домене аутентификации. Статус сменится на «Активный» только после авторизации пользователя с правильным паролем или после смены статуса администратором. Значение по умолчанию: «300»
«URL входа»	URL-адрес начальной страницы графического интерфейса управления ⚠ Значение параметра менять не следует. Значение по умолчанию: «/login»

Параметр	Описание
«Адрес сервера удаленного помощника»	URL-адрес узла с установленной серверной частью «Удаленного помощника». Пример: «https://192.168.0.2». По умолчанию значение не задано
«Максимальное время инициализации рабочего места»	Максимальное время (в секундах) ожидания готовности ВРМ, после истечения которого оно будет считаться зависшим. Если ВМ находятся в состоянии «Подготовка» или не назначена пользователю по истечении времени «Максимальное время инициализации рабочего места», то она будет очищена фоновой задачей, выполняемой каждые 60 секунд. Значение по умолчанию: «3601»
«Максимум записей в журнале для объектов»	Максимальное количество системных событий, добавляемых в журнал объекта. Значение по умолчанию: «100»
«Количество ошибок для ограничения фонда»	Пороговое значение количества ошибок, после которого фонд будет переведен в статус «Ограниченный». Значение по умолчанию: «3»
«Интервал отслеживания ошибок в фонде»	Периодичность отслеживания появления ошибок (в секундах), связанных с функционированием фонда. Значение по умолчанию: «600»
«Срок действия устаревшей публикации»	Время (в часах), по истечении которого ВМ будет удалена, если публикация фонда объявлена устаревшей. ⚠ Поведение параметра переопределяется на уровне фонда РМ политикой «Удаление устаревшей публикации» (см. подраздел **Политики фонда РМ**): совместимость обеспечивается только при ее значении «Удалять по истечении срока действия», что соответствует значению «-1» этого параметра. При обновлении параметра его значение применяется к новым публикациям. Для публикаций, созданных до изменения параметра, будет действовать предыдущее значение параметра. Если значение параметра будет равным «-1», то при перепубликации фонда РМ произойдет следующее: ▪ предыдущая публикация будет переведена в статус «Публикация частично удалена» (см. подраздел **Публикация фонда РМ**), если есть назначенная и используемая ВМ; ▪ используемая ВМ автоматически не удалится, но при этом будет создана новая публикация. Если значение параметра будет равным «0», то при перепубликации фонда назначенная ВМ будет немедленно заменена на новую публикацию. Если значение параметра будет равным «1», то при перепубликации фонда назначенная ВМ будет доступна 1 час, после чего удалится. Значение по умолчанию: «24»
«Срок хранения статистики»	Время (в сутках) хранения файлов журналов, по истечению которого журналы будут перезаписаны. Значение по умолчанию: «365»

Параметр	Описание
«Количество удаляемых рабочих мест за один проход»	Максимальное количество ВРМ, помеченных к удалению, которые будут проверены и удалены при каждой итерации запуска фоновой задачи очистки. Значение по умолчанию: «3»
«Отправлять уведомление при превышении лимита интервала опроса поставщика»	Управление возможностью отправки уведомлений администратору, если превышен интервал опроса, заданный в настройках поставщика ресурсов. Параметр также влияет на отправку почтовых уведомлений. Возможные значения: ▪ «Да» - администратору будет отправлено почтовое уведомление и уведомление в веб-интерфейсе, если заданный интервал опроса превышен; ▪ «Нет» (по умолчанию) - администратору не будут отправлены уведомления при превышении интервала опроса

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

11.3 . Параметры безопасности Termidesk

Для конфигурации системных параметров безопасности следует перейти «Настройки - Системные параметры», выбрать раздел «Безопасность».

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

Таблица 94 – Параметры безопасности Termidesk

Параметр	Описание
«Мастер-ключ»	Идентификатор для регистрации РМ в Termidesk. Значение идентификатора должно удовлетворять условиям: ▪ длина должна составлять от 1 до 32 символов; ▪ должны использоваться символы в шестнадцатеричной системе (0-9, a-f)
«Доверенные хосты»	Идентификатор узлов, имеющих право подключаться к Termidesk
«Длительность сессии администратора»	Временной интервал сессии (в секундах), инициированной на «Портале администратора»
«Доступ к веб-части системным пользователем»	Возможность администратора подключаться к «Порталу администратора»
«Использовать анонсируемый IP клиента»	Использовать IP-адрес «Клиента», передаваемый в процессе входа в Termidesk. Параметр необходимо включить, если узел «Универсального диспетчера» используется в ферме Termidesk, подключаемой к порталу «Агрегатор». В противном случае при подключении пользователей к ресурсам ферм Termidesk в журнале «Универсального диспетчера» будет отображен IP-адрес портала «Агрегатор», а не IP-адреса подключившихся пользователей
«GID системной группы администратора»	Идентификатор группы, в которую входит учетная запись администратора

Параметр	Описание
«Длительность сессии пользователя»	Временной интервал (в секундах) сессии пользователя. Параметр влияет на длительность сессии пользователя в «Портале пользователя». Начиная с Termidesk версии 5.0 параметр также определяет общее время подключения пользователя к «Универсальному диспетчеру» Termidesk. Вне зависимости от того, активен пользователь или нет, каждую секунду происходит уменьшение значения параметра на 1, при достижении значения 0 подключение пользователя завершится, при этом в системном трее на пользовательской рабочей станции отобразится уведомление от приложения «Клиент»: «Ваш сеанс завершился». В журнале «Клиента» отражаются события как получения параметра («userSessionLength»), так и завершения сессии по таймауту
«Максимум попыток входа Администраторов»	Пороговое положительное значение числа неудачных попыток входа администратора. Параметр может быть изменен только администратором (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 администратору. Значение «0» эквивалентно «без ограничений»
«Максимум попыток входа Пользователей»	Пороговое положительное значение числа неудачных попыток входа пользователей. Значение «0» эквивалентно «без ограничений»

11.4 . Утилиты интерфейса командной строки для настройки Termidesk

11.4.1 . Утилита termidesk-config

Утилита `termidesk-config` используется для переопределения настроек, заданных на этапе установки, и вносит изменения в конфигурационный файл `/etc/opt/termidesk-vdi/termidesk.conf` (см. подраздел **Параметры конфигурирования компонентов «Универсальный диспетчер», «Менеджер рабочих мест»**).

Для вызова утилиты следует:

- в интерфейсе командной строки перейти в каталог `/opt/termidesk/sbin/`:

```
cd /opt/termidesk/sbin/
```

- выполнить запуск:

```
sudo ./termidesk-config
```

- откроется интерфейс утилиты (см. Рисунок 72).

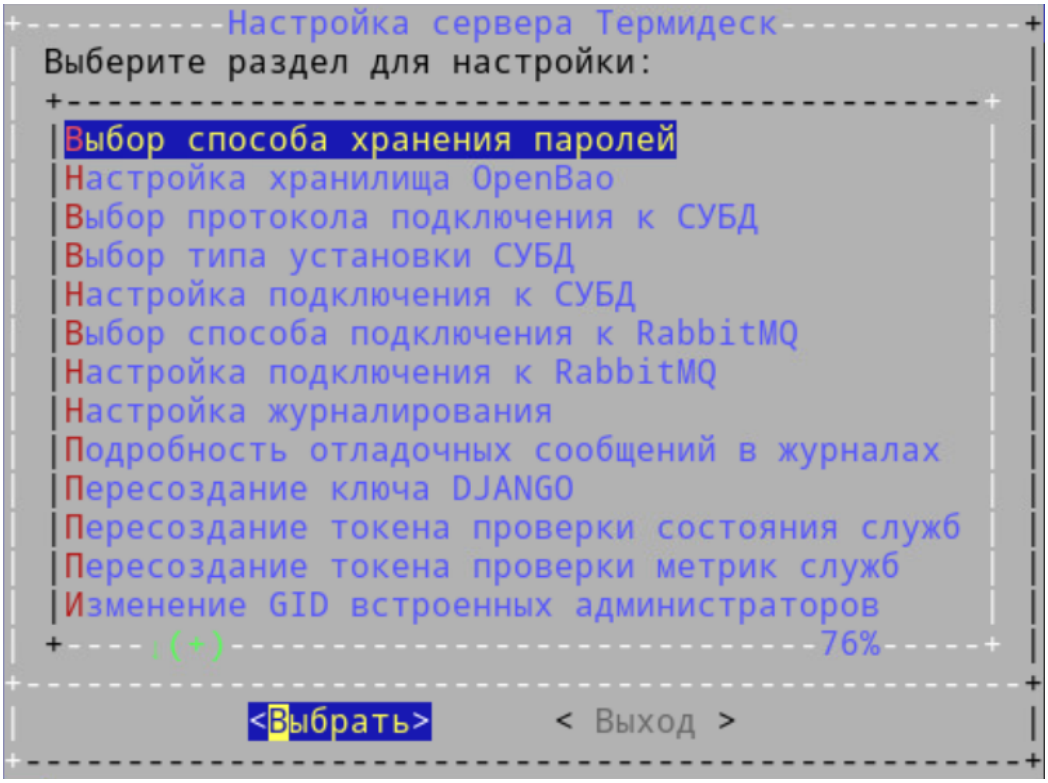

Рисунок 72 – Интерфейс утилиты termidesk-config

Доступны следующие функции утилиты:

- «Выбор способа хранения паролей»: позволяет настроить способ хранения паролей подключения к СУБД и RabbitMQ (параметр `SECRETS_STORAGE_METHOD`):
  - «config» - пароли будут храниться в преобразованном виде в файле `/etc/opt/termidesk-vdi/termidesk.conf`;
  - «hvac» (рекомендуемый способ для безопасного хранения) - для хранения паролей будет использоваться хранилище паролей OpenBao или Hashicorp Vault (хранилище должно быть заранее создано и настроено);
  - «openbao» - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено).

  В случае выбора «openbao» необходимо выполнить настройку подключения к хранилищу через функцию «Настройка хранилища OpenBao»;
- «Настройка хранилища OpenBao»: позволяет настроить параметры подключения к хранилищу и задать параметры, настроенные непосредственно на хранилище:
  - «URL хранилища» - IP-адрес или FQDN узла и порт с установленным хранилищем OpenBao (параметр `SECRETS_OPENBAO_URL`). Формат: `http://<IP-адрес>:8200` или `http://<FQDN>:8200`. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом;

- «Версия API OpenBao» - установленная версия API на OpenBao (параметр SECRETS_OPENBAO_KV_VERSION). Может принимать значения: «1» или «2»;
- «Токен доступа к хранилищу» - токен (Initial Root Token), который был сформирован при инициализации хранилища (параметр SECRETS_OPENBAO_TOKEN);
- «Путь к паролю СУБД» - путь, настроенный на OpenBao для хранения пароля СУБД (параметр SECRETS_OPENBAO_DB_PATH);
- «Роль доступа к паролю СУБД» - роль, настроенная на OpenBao, которая имеет доступ к паролю СУБД (параметр SECRETS_OPENBAO_DB_ROLE_NAME);
- «Путь к паролям RabbitMQ» - путь, настроенный на OpenBao для хранения пароля RabbitMQ (параметр SECRETS_OPENBAO_RABBITMQ_PATH);
- «Роль доступа к паролям RabbitMQ» - роль, настроенная на OpenBao, которая имеет доступ к паролю RabbitMQ (параметр SECRETS_OPENBAO_RABBITMQ_ROLE_NAME);
- «Путь к паролям Termidesk» - путь, настроенный на OpenBao для хранения пароля Termidesk (параметр SECRETS_OPENBAO_TERMIDESK_PATH);
- «Роль доступа к паролям Termidesk» - роль, настроенная на OpenBao, которая имеет доступ к паролю Termidesk (параметр SECRETS_OPENBAO_TERMIDESK_ROLE_NAME);
- «Время кеширования паролей, сек» - время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти (параметр SECRETS_OPENBAO_CACHE_LIFETIME);

- «Выбор протокола подключения к СУБД»: позволяет выбрать протокол при подключении к СУБД (параметр DBSSL);
- «Выбор типа установки СУБД»: позволяет выбрать тип СУБД, к которой будет подключаться Termidesk (параметр DB_CLUSTER_MODE);
- «Настройка подключения к СУБД»: позволяет настроить параметры подключения к СУБД:
  - «Адрес СУБД» - IP-адрес или FQDN СУБД PostgreSQL (параметр DBHOST);
  - «Адрес СУБД (узел 2)»: IP-адрес или FQDN дополнительного узла СУБД (параметр DBHOST2);
  - «Адрес СУБД (узел 3)»: IP-адрес или FQDN дополнительного узла СУБД (параметр DBHOST3);
  - «Порт СУБД» - порт, который используется для соединения с сервером БД (параметр DBPORT);
  - «Имя базы данных» - имя БД (параметр DBNAME);
  - «Имя пользователя» - имя пользователя для подключения к БД (параметр DBUSER);
  - «Пароль» - пароль пользователя в открытом виде (параметр DBPASS);
- «Выбор способа подключения к RabbitMQ»: позволяет выбрать протокол при подключении к RabbitMQ (параметр RABBITMQ_SSL);

- «Настройка подключения к RabbitMQ»: позволяет настроить параметры подключения к RabbitMQ (параметр `RABBITMQ_URL`). При запросе пароль задается в открытом виде;
- «Настройка журналирования»: позволяет настроить параметры журналирования, такие как «Адрес логгера» (параметр `LOG_ADDRESS`), «Поток (facility) журнала» (параметр `LOG_FACILITY`);
- «Подробность отладочных сообщений в журналах»: позволяет выбрать уровень подробности отладочных сообщений (параметр `LOG_LEVEL`);
- «Пересоздание ключа DJANGO»: позволяет переопределить значение ключа DJANGO (параметр `DJANGO_SECRET_KEY`), создаваемого на этапе установки. Переопределение ключа может понадобиться при его компрометации;
- «Пересоздание я токена проверки состояния служб»: позволяет переопределить значение токена проверки состояния служб (параметр `HEALTH_CHECK_ACCESS_KEY`). Переопределение токена может понадобиться при его компрометации;
- «Пересоздание токена проверки метрик служб»: позволяет переопределить значение токена проверки метрики служб (параметр `METRICS_ACCESS_KEY`). Переопределение токена может понадобиться при его компрометации;
- «Изменение GID встроенных администраторов»: позволяет назначить идентификатор группы, использующегося для встроенного домена. Изменение идентификатора может понадобиться, если встроенная в ОС группа администраторов отличается от `astra-admin (1001)` или если нужно предоставить права администрирования Termidesk группе непривилегированных пользователей;
- «Настройки Агрегатора»: позволяет переопределить настройки портала «Агрегатор»:
  - «Время жизни токена Агрегатора, секунд» - время жизни JWT-токена (параметр `AGGREGATOR_ACCESS_TOKEN_TTL_SECONDS`, доступная для изменения только на узле с установленным порталом «Агрегатор»);
  - «Заголовок JWT-токена Агрегатора» - заголовок JWT-токена, предназначенный для настройки взаимодействия между порталом «Агрегатор» и «Универсальным диспетчером». Параметр должен быть одинаковым на всех узлах, работающих совместно: на порталах «Агрегатора», на «Универсальных диспетчерах» (параметр `AGGREGATOR_ACCESS_TOKEN_TITLE`);
  - «Время кеширования иконок фондов, часов» - время жизни кеша иконок фондов (параметр `AGGREGATOR_IMAGE_CACHE_LIFETIME_HOURS`);
- «Роли сервера»: позволяет изменить роли, которые запускаются на узле. Доступные роли: «Портал администратора», «Портал пользователя», «Менеджер рабочих мест», «Агрегатор администратора», «Агрегатор пользователя»;

Установка ролей «Агрегатор администратора» и (или) «Агрегатор пользователя» должна производиться на узле, отличном от «Портала администратора» и (или) «Портала пользователя», «Менеджера рабочих мест».
Смена ролей через функцию «Роли сервера» в этом случае не предусмотрена: нельзя ранее установленные «Портал администратора» и (или) «Портал пользователя» перенастроить на использование ролей «Агрегатор администратора» и (или) «Агрегатор пользователя».

- «Перезапуск служб» - позволяет выполнить перезапуск служб Termidesk;
- «Сертификаты» - позволяет выполнить настройку сертификатов и ключей:

Пункт «Серт. для расшифровки JWT-токена» настраивается только на узле с установленным «Универсальным диспетчером» («Портал администратора» и (или) «Портал пользователя») фермы Termidesk.
Пункт «Прив. ключ для подписи JWT-токена» настраивается только на узле портала «Агрегатор» («Агрегатор администратора» и (или) «Агрегатор пользователя»).
Оставшиеся пункты могут быть настроены на обоих узлах индивидуально.

- «Сертификат Health Check» - путь к сертификату для защищенного подключения к API проверки состояния (параметр `HEALTH_CHECK_CERT`);
- «Секр. ключ Health Check» - путь к ключу для защищенного подключения к API проверки состояния (параметр `HEALTH_CHECK_KEY`);
- «Сертификат Postgres mTLS» - путь к сертификату для защищенного подключения к СУБД (параметр `DBCERT`);
- «Секр. ключ Postgres mTLS» - путь к ключу для защищенного подключения к СУБД (параметр `DBKEY`);
- «Серт. промеж. ЦС Postgres mTLS» - путь к корневому и промежуточным сертификатам mTLS для защищенного подключения к СУБД (параметр `DBCHAIN`);
- «Сертификат OpenBao mTLS» - путь к сертификату для защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_CLIENT_CERT`);
- «Секр. ключ OpenBao mTLS» - путь к ключу для защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_CLIENT_KEY`);
- «Серт. промеж. ЦС OpenBao mTLS» - путь к корневому и промежуточным сертификатам mTLS для защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_SERVER_CERT`);
- «Осн. серт. для расшифровки JWT-токена» - путь к сертификату для получения значения JWT-токена портала «Агрегатор» (параметр `AGGREGATOR_JWT_SSL_CERT`);
- «Рез. серт. для расшифровки JWT-токена» - путь к резервному сертификату для получения значения JWT-токена портала «Агрегатор» (параметр `AGGREGATOR_JWT_SSL_CERT_SECOND`);

- «Секр. ключ для подписи JWT-токена» - путь к ключу для подписи JWT-токена портала «Агрегатор» (параметр `AGGREGATOR_JWT_SSL_KEY`);
- «Сертификат для подключения к серверу RA» - путь к серверному сертификату SSL/TLS для проверки подключения к «Удаленному помощнику» (`REMOTE_ASSISTANT_SERVER_CERT`);
- «Сертификат RabbitMQ mTLS» - путь к клиентскому сертификату SSL/TLS для защищенного подключения к RabbitMQ (`CELERY_BROKER_CERT`);
- «Секр.ключ RabbitMQ mTLS» - путь к клиентскому ключу SSL/TLS для защищенного подключения к RabbitMQ (`CELERY_BROKER_KEY`);
- «Серт. ЦС RabbitMQ mTLS» - путь к корневому сертификату ЦС SSL/TLS для защищенного подключения к RabbitMQ (`CELERY_BROKER_CA`);
- «Публичный ключ ws-proxy»: путь к открытому ключу `id_rsa.pub`. Явно задавать путь следует только при использовани внешнего хранилища (`WSPROXY_PUB_KEY_FILE`);
- «Секретный ключ ws-proxy»: путь к озакрытому ключу `id_rsa`. Явно задавать путь следует только при использовани внешнего хранилища (`WSPROXY_PRIV_KEY_FILE`);

- «Перезапуск служб»: позволяет выполнить перезапуск служб Termidesk.

> После выполнения изменений в любом из разделов рекомендуется воспользоваться пунктом «Перезапуск служб» для применения изменений.

11.4.2 . Утилита termidesk-vdi-manage

Утилита `termidesk-vdi-manage` используется для настройки «Универсального диспетчера» из интерфейса командной строки.

Для вызова утилиты следует:

- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- вывести список команд утилиты:

```
/opt/termidesk/sbin/termidesk-vdi-manage help
```

> Каждая подкоманда в приведенных ниже командах поддерживает вывод справки через ключ `-h`.
> Для управления параметрами поставщиков ресурсов, доменов аутентификации, протоколов доставки и других компонентов, настраиваемых через «Портал администратора» Termidesk, следует обратиться к командам секции `[termidesk]`.

Большая часть команд из вывода `/opt/termidesk/sbin/termidesk-vdi-manage help` предназначена для работы с БД и фреймворком Django и не приведена здесь.

Команды секции `[termidesk]` приведены в таблице (см. Таблица 95).

Таблица 95 – Команды секции [termidesk]

Параметр	Описание
`drop_tables`	Удаляет таблицы из БД. Для просмотра списка ключей следует воспользоваться аргументом `-h`: `/opt/termidesk/sbin/termidesk-vdi-manage drop_tables -h` Поддерживаются аргументы: ▪ `--noinput`, `--no-input` - сообщает Django НЕ запрашивать у пользователя ввод; ▪ `-R <МАРШРУТИЗАТОР>`, `--router <МАРШРУТИЗАТОР>` - использование указанного маршрутизатора БД вместо определенного в настройках `settings.py`; ▪ `-S <СХЕМА>`, `--schema <СХЕМА>` - удаление указанной схемы вместо `public`; ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы

Параметр	Описание

`tdsk_auth`	Управление доменами аутентификации. Для просмотра списка ключей следует воспользоваться аргументом `-h`:
	`/opt/termidesk/sbin/termidesk-vdi-manage tdsk_auth -h`
	Поддерживаются аргументы:
	▪ `--version` - вывод версии программы;
	▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;
	▪ `--settings <настройки>` - путь к модулю настроек Python;
	▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;
	▪ `--traceback` - вызов исключений;
	▪ `--no-color` - вывод команды без подсвечивания;
	▪ `--force-color` - вывод команды с принудительным подсвечиванием;
	▪ `--skip-checks` - пропуск проверки системы.
	Поддерживаются подкоманды:
	▪ `create` - создание домена аутентификации;
	▪ `list` - вывод списка доменов аутентификации;
	▪ `remove` - удаление домена аутентификации;
	▪ `login` - аутентификация в указанный домен;
	▪ `logout` - завершение сессии.
	Подкоманда `create` принимает аргументы:
	▪ `--type` - задание типа домена аутентификации. Доступны: `ALDAuthenticatorPlugin` («Astra Linux Directory»), `IPAuth` («IP аутентификация»), `KerberosAuthenticatorPlugin` («FreeIPA»), `SAMLAuthenticator` («SAML»), `SimpleLdapAuthenticator` («MS Active Directory (LDAP)»);
	▪ `--params` - задание параметров домена аутентификации. Формат: `имя1=значение1 имя2=значение2` и т.д. Доступные параметры для указанного типа домена аутентификации можно получить через команду `--list` , например:
	`/opt/termidesk/sbin/termidesk-vdi-manage tdsk_auth create --type IPAuth --name test --small_name test`
	▪ `--list` - вывод параметров домена аутентификации;
	▪ `--test` - проверка параметров без создания домена аутентификации;
	▪ `--quiet` - вывод только сообщений об ошибках;
	▪ `--name <ИМЯ>` - имя домена аутентификации;
	▪ `--small_name <короткое имя>` - короткое имя домена аутентификации. Допустимые символы: a-z, A-Z, 0-9. Максимальная длина 32 символа;
	▪ `--priority <приоритет>` - числовое значение приоритета домена аутентификации, по умолчанию «1»;
	▪ `--comments <комментарий>` - комментарий к создаваемому домену.
	Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате JSON.
	Подкоманда `remove` принимает аргументы:
	▪ `--output json` - вывод параметров в формате JSON;
	▪ `--silent` - «тихое» удаление для выполнения команды из исполняемого файла;

Параметр	Описание
	▪ `--uuid <идентификатор>` - идентификатор объекта для удаления. Подкоманда `login` принимает аргументы: ▪ `--uuid <идентификатор>` - идентификатор объекта для аутентификации; ▪ `--small_name <короткое имя>` - короткое имя домена аутентификации; ▪ `--output json` - вывод параметров в формате JSON. Подкоманда `logout` принимает аргументы: ▪ `--token <токен>` - токен сессии пользователя; ▪ `--output json` - вывод параметров в формате JSON
`tdsk_clearsessions`	Порционная очистка сессий. Поддерживаются аргументы: ▪ `-chunk <количество>` - количество сессий для удаления, по умолчанию 1000; ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы
`tdsk_config`	Управление системными настройками. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживаются подкоманды: ▪ `list` - вывод конфигурационных параметров и их значений; ▪ `set` - установка значения конфигурационному параметру. Подкоманда `set` принимает аргументы: ▪ `--key <ключ>` - ключ параметра; ▪ `--value <значение>` - значение параметра. Пример команды для смены значения параметра `metrics.cacheSize` («Размер кеша») секции `Metrics` на «9»: `/opt/termidesk/sbin/termidesk-vdi-manage set --key metrics.cacheSize --value 9`

Параметр	Описание
`tdsk_exp_2fa_add_statictoken`	Добавление токена пользователю. Поддерживаются аргументы: ▪ `username` - имя пользователя, с которым будет ассоциирован токен; ▪ `-t <токен>`, `--token <токен>` - токен, который нужно добавить. Если этот параметр пропущен, он будет сгенерирован случайным образом; ▪ `--auth_uuid <идентификатор>` - идентификатор домена аутентификации; ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы
`tdsk_exp_2fa_clear_totpdevice`	Удаление TOTP-устройства пользователя. Поддерживаются аргументы: ▪ `username` - имя пользователя, которому нужно удалить TOTP-устройство; ▪ `--auth_uuid <идентификатор>` - идентификатор домена аутентификации; ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы

Параметр	Описание
`tdsk_graph_models`	Создание файла GraphViz с описанием моделей БД для указанных имен приложений. Можно передать несколько имен приложений, и все они будут объединены в одну модель. Пример использования команды приведен в подразделе **Генерация отчета по моделям данных и структурам БД Termidesk**. Поддерживаются аргументы: ▪ `app_label` - наименование приложения; ▪ `--pygraphviz` - использование PyGraphViz для создания изображения; ▪ `--pydot` - использование PyDot(Plus) для создания изображения; ▪ `--disable-fields`, `-d` - не показывать поля; ▪ `--group-models`, `-g` - сгруппировать модели в соответствии с их применением; ▪ `--all-applications`, `-a` - включить все приложения для вывода модели; ▪ `--output <путь к файлу>`, `-o <путь к файлу>` - запись вывода в файл; ▪ `--layout <макет>`, `-l <макет>` - использование макета GraphViz для визуализации. Поддерживаются: `circo`, `dot`, `fdpneato`, `nop`, `nop1`, `nop2`, `twopi`; ▪ `--verbose-names`, `-n` - использование подробных имен для моделей и полей; ▪ `--language <локализация>`, `-L <локализация>` - указания языка, который будет использоваться для подробных имен; ▪ `--exclude-columns <столбцы>`, `-x <столбцы>` - исключение определенных столбцов; ▪ `--exclude-models <модели>`, `-X <модели>` - исключение определенных моделей; ▪ `--include-models <модели>`, `-I <модели>` - ограничение только указанными моделями; ▪ `--inheritance`, `-e` - включение наследования (используется по умолчанию); ▪ `--no-inheritance`, `-E` - выключение наследования; ▪ `--hide-relations-from-fields`, `-R` - ▪ `--disable-sort-fields`, `-S` - ▪ `--json` - вывод в формат JSON; ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы

Параметр	Описание
`tdsk_group`	Создание группы РМ. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживается подкоманда `create` (создание группы рабочих мест) со следующими аргументами: ▪ `--quiet` - вывод только сообщений об ошибках; ▪ `--name <имя>` - имя создаваемой группы; ▪ `--comments <комментарий>` - комментарий к создаваемой группе; ▪ `--priority <приоритет>` - числовое значение приоритета группы

`tdsk_license`	Управление лицензией Termidesk.
	Поддерживаются аргументы:
	▪ `--version` - вывод версии программы;
	▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;
	▪ `--settings <настройки>` - путь к модулю настроек Python;
	▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;
	▪ `--traceback` - вызов исключений;
	▪ `--no-color` - вывод команды без подсвечивания;
	▪ `--force-color` - вывод команды с принудительным подсвечиванием;
	▪ `--skip-checks` - пропуск проверки системы.
	Поддерживаются подкоманды:
	▪ `install` - установить лицензию из файла, поддерживается относительный или абсолютный путь к файлу. Пример команды для установки лицензии:
	`/opt/termidesk/sbin/termidesk-vdi-manage tdsk_license install <путь к файлу лицензии>`
	▪ `show` - вывести информацию об установленной лицензии. Для вывода в формате JSON следует использовать аргумент `--output`:
	`/opt/termidesk/sbin/termidesk-vdi-manage tdsk_license show --output json`
	▪ `remove` - удалить лицензию из БД. Перед выполнением команды необходимо авторизоваться:
	`/opt/termidesk/sbin/termidesk-vdi-manage tdsk_auth login`
	`/opt/termidesk/sbin/termidesk-vdi-manage tdsk_license remove`

Параметр	Описание
`tdsk_net`	Создание сети. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживается подкоманда `create` (создание сети) со следующими аргументами: ▪ `--quiet` - вывод только сообщений об ошибках; ▪ `--name <имя>` - имя создаваемой сети; ▪ `--netRange <диапазон>` - диапазон IP-адресов. Допустимы различные форматы, например: A.B.C.*, A.B.C.D/N, A.B.C.D - E.F.G.D
`tdsk_openbao_migrate`	Миграция способа хранения паролей и переход с конфигурационного файла на использование хранилища OpenBao. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы
`tdsk_openbao_reverse_migrate`	Миграция способа хранения паролей и переход с хранилища OpenBao на конфигурационный файл. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы

Параметр	Описание
`tdsk_osm`	Создание параметров гостевой ОС. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживается подкоманда `create` (создание параметров гостевой ОС) со следующими аргументами: ▪ `--params` - задание параметров гостевой ОС. Формат: `имя1=значение1 имя2=значение2` и т.д.; ▪ `--list` - вывод параметров гостевой ОС; ▪ `--test` - проверка параметров без создания объекта; ▪ `--quiet` - вывод только сообщений об ошибках; ▪ `--name <ИМЯ>` - наименование параметров гостевой ОС; ▪ `--comments <комментарий>` - комментарий к создаваемым параметрам
`tdsk_pool`	Управление фондами РМ. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживаются подкоманды: ▪ `create` - создание фонда РМ; ▪ `list` - вывод списка фондов РМ. Подкоманда `create` принимает аргументы: ▪ `--quiet` - вывод только сообщений об ошибках; ▪ `--name <имя>` - имя фонда РМ; ▪ `--comments <комментарий>` - комментарий к создаваемому фонду РМ; ▪ `--service_id <идентификатор>` - указание идентификатора шаблона РМ; ▪ `--osmanager_id <идентификатор>` - указание идентификатора параметров гостевой ОС РМ; ▪ `--image_id <идентификатор>` - указание идентификатора изображения гостевой ОС; ▪ `--servicesPoolGroup_id <идентификатор>` - указание идентификатора группы РМ; ▪ `--cache_l1_srvs <значение>` - количество РМ в кеше 1-го уровня; ▪ `--cache_l2_srvs <значение>` - количество РМ в кеше 2-го уровня; ▪ `--max_srvs <значение>` - максимальное количество РМ. Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате JSON

Параметр	Описание
`tdsk_prov`	Управление поставщиками ресурсов. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживаются подкоманды: ▪ `create` - создание поставщика ресурсов; ▪ `list` - вывод списка поставщиков ресурсов; ▪ `id {id}` - действия с поставщиком ресурсов с идентификатором `id`. Подкоманда `create` принимает аргументы: ▪ `--type` - задание типа поставщика ресурсов. Доступны: `RedVirtPlatform` («Платформа RED Virtualization»), `SessionsPlatform` («Сервер Терминалов [экспериментальный]»), `VMmanagerPlatform` («Платформа VMmanager»), `oVirtPlatform` («Платформа oVirt/RHEV»), `pksvbrestPlatform` («ПК СВ Брест»), `vmwarePlatform` («Платформа VMware»), `zVirtPlatform` («Платформа zVirt»), `PhysicalMachinesServiceProvider` («Автономная машина»); ▪ `--params` - задание параметров поставщика ресурсов. Формат: `имя1=значение1 имя2=значение2` и т.д. Доступные параметры для указанного типа поставщика ресурсов можно получить через команду `--list` , например: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_prov create --type RedVirtPlatform --list --name test` ▪ `--list` - вывод параметров поставщика ресурсов; ▪ `--test` - проверка параметров без создания поставщика ресурсов; ▪ `--quiet` - вывод только сообщений об ошибках; ▪ `--name <имя>` - наименование поставщика ресурсов; ▪ `--comments <комментарий>` - комментарий к создаваемому поставщику ресурсов. Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате JSON. Подкоманда `id {id}` принимает: ▪ `tpl create` - создание шаблона РМ в поставщике ресурсов; ▪ `tpl list` - вывод списка шаблонов РМ поставщика ресурсов; ▪ `tpl remove` - удаление шаблона РМ в поставщике ресурсов

Параметр	Описание
`tdsk_refresh_ssa`	Регистрация «Сессионного агента» в БД Termidesk. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы

Параметр	Описание
tdsk_trans	Управление протоколами доставки. Поддерживаются аргументы: ▪ --version - вывод версии программы; ▪ -v {0,1,2,3}, --verbosity {0,1,2,3} - уровень детализации сообщений; ▪ --settings <настройки> - путь к модулю настроек Python; ▪ --pythonpath <каталог Python> - каталог, который нужно добавить в путь Python, например /home/djangoprojects/myproject; ▪ --traceback - вызов исключений; ▪ --no-color - вывод команды без подсвечивания; ▪ --force-color - вывод команды с принудительным подсвечиванием; ▪ --skip-checks - пропуск проверки системы. Поддерживаются подкоманды: ▪ create - добавление протокола доставки; ▪ list - вывод списка протоколов доставки; ▪ remove - удалить протокол доставки; ▪ convert - конвертировать протокол доставки (RDSTransport, RDSWSTRDPTransport, STALTransport, STALWSTRDPTransport) в новый протокол TerminalTransport. Подкоманда create принимает аргументы: ▪ --type - задание типа протокола. Доступны: HTML5Transport («HTML5»), HTML5VNCTransport («VNC (HTML5, через локальный прокси)»), LoudplayDirectTransport («Loudplay (напрямую, эксперим.)»), LoudplayTunneledTransport («Loudplay (через вебсокет шлюз, эксперим.)»), RDPTransport («RDP (напрямую)»), RDSTransport («Доступ к MS RDS по RDP (напрямую) [экспериментальный]»), RDSWSTRDPTransport («Доступ к MS RDS по RDP (через шлюз) [экспериментальный]»), STALTransport («Доступ к STAL по RDP (напрямую) [экспериментальный]»), STALWSTRDPTransport («Доступ к STAL по RDP (через шлюз) [экспериментальный]»), TDSKSPICETransport («SPICE (vdi-viewer, эксперим.)»), WSTRDPTransport («RDP (через вебсокет шлюз)»), TERATransport («TERA [экспериментальный]»), TerminalTransport («RDP (терминальный доступ)»); ▪ --params - задание параметров протокола доставки. Формат: имя1=значение1 имя2=значение2 и т.д. Доступные параметры для указанного типа протокола доставки можно получить через команду --list, например: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_trans create --type RDPTransport --list --name test` ▪ --list - вывод параметров протокола доставки; ▪ --test - проверка параметров без создания протокола доставки; ▪ --quiet - вывод только сообщений об ошибках; ▪ --name <имя> - наименование протокола доставки; ▪ --comments <комментарий> - комментарий к создаваемому протоколу доставки; ▪ --priority <приоритет> - числовое значение приоритета протокола доставки; ▪ --allowed_oss <перечень ОС> - перечень разрешенных ОС из списка: Android, CrOS, FreeBSD, iPad, iPhone, Linux, Mac, Windows, Windows Phone. Формат: имя1,имя2,имя3; ▪ --nets_positive <yes/no> - указание, что протокол должен быть доступен только из сетей, указанных в параметре --networks. Может принимать значения не только yes или no, подходит в целом любое непустое значение;

Параметр	Описание
	▪ `--networks <наименования сетей>` - перечень сетей, доступ из которых разрешен для создаваемого протокола доставки. Формат: `имя1,имя2,имя3`. Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате JSON. Подкоманда `create` принимает аргументы: ▪ `--output json` - вывод списка в формате JSON; ▪ `--silent` - выполнение в «тихом» режиме; ▪ `--uuid <идентификатор>` - идентификатор объекта для удаления. Подкоманда `convert` принимает аргументы: ▪ `--uuid <идентификатор>` - идентификатор протокола доставки, который необходимо конвертировать (`RDSTransport`, `RDSWSTRDPTransport`, `STALTransport`, `STALWSTRDPTransport`); ▪ `--all` - ковернтировать все протоколы доставки MS RDS и STAL
`tdsk_version`	Получение версии Termidesk

11.5 . Назначение служебных функций администраторам

В Termidesk для администраторов реализовано разделение доступных служебных функций.

Для назначения доступных служебных функций следует перейти «Настройки - Управление ролями» и нажать экранную кнопку [Создать] (см. Рисунок 73).

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

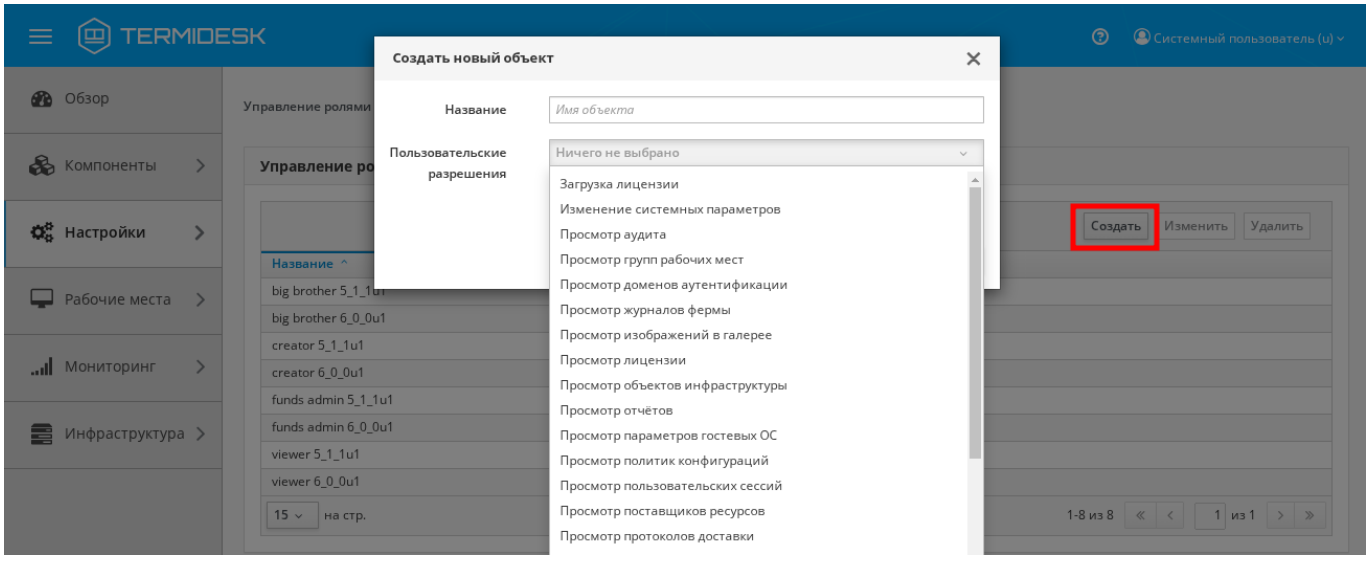

Рисунок 73 – Окно назначения пользовательских разрешений

Список разрешений для назначения служебных функций администраторам перечислен в столбце «Разрешение» следующей таблицы (см. Таблица 96).

> ⚠ Перед назначением разрешения на редактирование, создание, удаление или управление необходимо предоставить соответствующее разрешение на просмотр страницы.

Таблица 96 – Список доступных для выбора разрешений

Разрешение	Описание
«Загрузка лицензии»	Разрешение позволяет загружать лицензии на странице «Настройки - Лицензия» на вкладке «Загрузка»
«Изменение системных параметров»	Разрешение позволяет управлять системными параметрами на странице «Настройки - Системные параметры»
«Просмотр аудита»	Предоставляет доступ на чтение страницы «Мониторинг - Аудит»
«Просмотр групп рабочих мест»	Предоставляет доступ на чтение страницы «Настройки - Группы рабочих мест» для просмотра списка созданных групп РМ
«Просмотр доменов аутентификации»	Предоставляет доступ на чтение страницы «Компоненты - Домены аутентификации». Разрешение позволяет выполнять просмотр: ▪ пользователей домена, назначенных им групп, РМ, ВМ и журнал; ▪ списка групп домена и пользователей, входящих в каждую группу; ▪ журнала
«Просмотр журналов фермы»	Предоставляет доступ на чтение страницы «Мониторинг - Журналы фермы»
«Просмотр изображений в галерее»	Предоставляет доступ на чтение страницы «Настройки - Галерея» для просмотра списка загруженных изображений
«Просмотр лицензии»	Предоставляет доступ на чтение страницы «Настройки - Лицензия» для просмотра информации о лицензии и системе
«Просмотр объектов инфраструктуры»	Предоставляет доступ на чтение страниц раздела «Инфраструктура» для просмотра информации о статусе компонентов Termidesk
«Просмотр отчётов»	Предоставляет доступ на чтение страницы «Мониторинг - Отчёты»
«Просмотр параметров гостевых ОС»	Предоставляет доступ на чтение страницы «Компоненты - Параметры гостевых ОС» для просмотра списка созданных параметров гостевых ОС
«Просмотр политик конфигураций»	Предоставляет доступ на чтение страницы «Настройки - Глобальные политики» для просмотра значений параметров политик
«Просмотр пользовательских сессий»	Предоставляет доступ на чтение страницы «Рабочие места - Сессии» для просмотра списка активных сессий пользователей
«Просмотр поставщиков ресурсов»	Предоставляет доступ на чтение страницы «Компоненты - Поставщики ресурсов». Разрешение позволяет выполнять просмотр: ▪ списка созданных поставщиков ресурсов; ▪ списка созданных шаблонов РМ
«Просмотр протоколов доставки»	Предоставляет доступ на чтение страницы «Компоненты - Протоколы доставки» для просмотра списка созданных протоколов доставки

Разрешение	Описание
«Просмотр расписаний»	Предоставляет доступ на чтение страницы «Рабочие места - Расписания» для просмотра списка созданных расписаний
«Просмотр сертификатов»	Предоставляет доступ на чтение сертификатов со страниц объектов инфраструктуры
«Просмотр сетей»	Предоставляет доступ на чтение страницы «Компоненты - Сети» для просмотра списка созданных сетей
«Просмотр системных журналов»	Предоставляет доступ на чтение страницы «Мониторинг - Системные журналы»
«Просмотр системных параметров»	Предоставляет доступ на чтение страницы «Настройки - Системные параметры» для просмотра заданных системных параметров
«Просмотр фондов рабочих мест»	Предоставляет доступ на чтение страницы «Рабочие места - Фонды». Разрешение позволяет выполнять: ▪ просмотр раздела «Фонды» и выполнять действия в разделе: • просматривать список опубликованных фондов РМ; • просматривать вкладки «Рабочие места», «Пользователи и группы», «Протоколы доставки», «Журнал» при выборе опубликованного фонда РМ; ▪ просмотр раздела «Индивидуальные рабочие места» для просмотра информации о назначенных ВМ
«Редактирование групп рабочих мест»	Разрешение позволяет редактировать параметры групп РМ
«Редактирование доменов аутентификации»	Разрешение позволяет редактировать параметры доменов аутентификации
«Редактирование изображений в галерее»	Разрешение позволяет редактировать параметры загруженных изображений в галерее
«Редактирование объектов инфраструктуры»	Разрешение позволяет редактировать параметры объектов инфраструктуры
«Редактирование параметров гостевых ОС»	Разрешение позволяет редактировать параметры гостевых ОС
«Редактирование политик конфигураций»	Разрешение позволяет выполнять: ▪ редактирование политик; ▪ сброс значения политики
«Редактирование поставщика ресурсов»	Разрешение позволяет редактировать параметры поставщиков ресурсов
«Редактирование протоколов доставки»	Разрешение позволяет редактировать параметры протоколов доставки
«Редактирование расписаний»	Разрешение позволяет редактировать параметры расписаний
«Редактирование сертификатов»	Разрешение позволяет редактировать сертификаты на страницах объектов инфраструктуры
«Редактирование сетей»	Разрешение позволяет редактировать параметры сетей
«Редактирование фондов рабочих мест»	Разрешение позволяет редактировать параметры: ▪ созданных фондов РМ; ▪ индивидуальных РМ
«Создание групп рабочих мест»	Разрешение позволяет создавать группы РМ

Разрешение	Описание
«Создание доменов аутентификации»	Разрешение позволяет добавлять домены аутентификации
«Создание изображений в галерее»	Разрешение позволяет загружать изображения в галерею
«Создание объектов инфраструктуры»	Разрешение позволяет добавлять объекты инфраструктуры
«Создание параметров гостевых ОС»	Разрешение позволяет добавлять параметры гостевых ОС
«Создание поставщика ресурсов»	Разрешение позволяет добавлять поставщиков ресурсов
«Создание протоколов доставки»	Разрешение позволяет добавлять протоколы доставки
«Создание расписаний»	Разрешение позволяет добавлять расписания
«Создание сетей»	Разрешение позволяет добавлять сети
«Создание фондов рабочих мест»	Разрешение позволяет создавать фонды РМ
«Удаление групп рабочих мест»	Разрешение позволяет удалять группы РМ
«Удаление доменов аутентификации»	Разрешение позволяет удалять домены аутентификации
«Удаление изображений из галереи»	Разрешение позволяет удалять изображения из галереи
«Удаление объектов инфраструктуры»	Разрешение позволяет удалять компоненты Termidesk из таблиц раздела «Инфраструктура»
«Удаление параметров гостевых ОС»	Разрешение позволяет удалять параметры гостевых ОС
«Удаление поставщика ресурсов»	Разрешение позволяет удалять поставщиков ресурсов
«Удаление протоколов доставки»	Разрешение позволяет удалять протоколы доставки
«Удаление расписаний»	Разрешение позволяет удалять расписания
«Удаление сертификатов»	Разрешение позволяет удалять сертификаты
«Удаление сетей»	Разрешение позволяет удалять сети
«Удаление фондов рабочих мест»	Разрешение позволяет удалять фонды РМ
«Управление группами домена аутентификации»	Разрешение позволяет выполнять действия: ▪ добавление группы домена аутентификации; ▪ редактирование группы домена аутентификации; ▪ удаление группы домена аутентификации
«Управление пользовательскими сессиями»	Разрешение позволяет выполнять действия с активными сессиями пользователей: ▪ отключение сессии; ▪ завершение сессии
«Управление пользователями домена аутентификации»	Разрешение позволяет выполнять действия: ▪ добавление пользователя домена аутентификации; ▪ редактирование пользователя домена аутентификации; ▪ удаление пользователя домена аутентификации

Разрешение	Описание
«Управление ролями»	Разрешение позволяет выполнять: ▪ просмотр раздела «Управление ролями» и выполнять действия в разделе: • создавать роли; • редактировать роли; • удалять роли; ▪ просмотр раздела «Управление ACL» и выполнять действия в разделе: • создавать разрешения для объектов; • редактировать разрешения для объектов; • удалять разрешения для объектов
«Управление шаблонами рабочих мест»	Разрешение позволяет выполнять действия: ▪ создание шаблона РМ; ▪ редактирование шаблона РМ; ▪ удаление шаблона РМ

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

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 **[Изменить]**. В открывшейся форме редактирования пользователя в поле «Роли» выбрать класс (см. Рисунок 74).

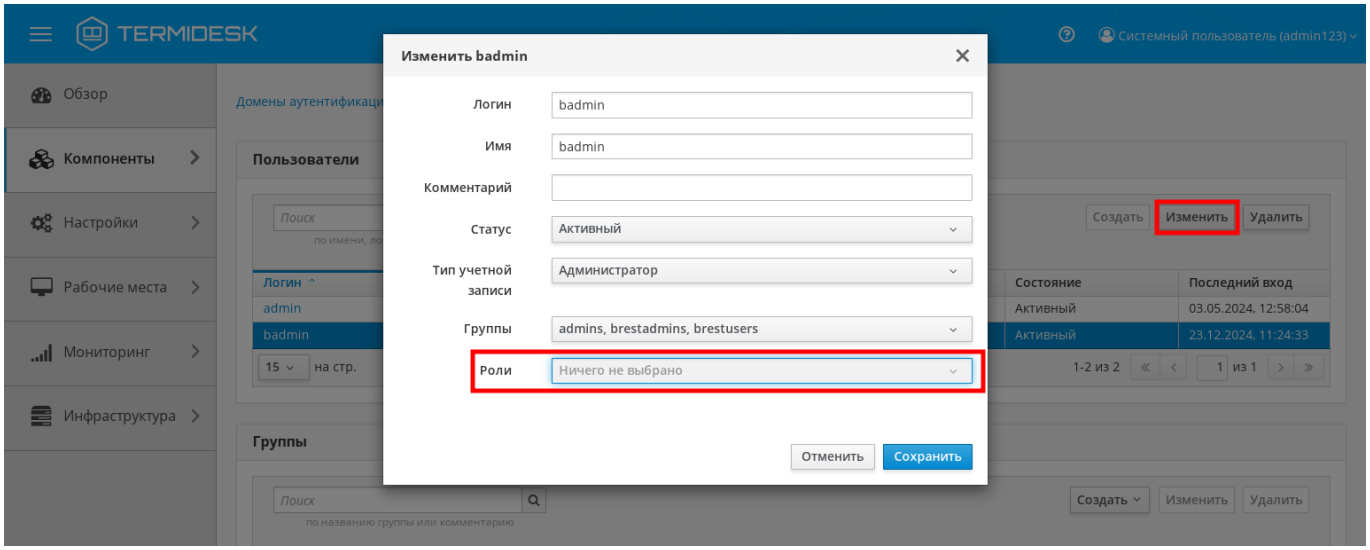

Рисунок 74 – Окно назначения пользовательских ролей

⚠ 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 РМ. Для добавления нового разрешения объекту следует перейти «Настройки - Управление ACL», нажать экранную кнопку **[Создать]** и выбрать «Фонд рабочих мест».

В режиме добавления нового разрешения для объекта администратору Termidesk необходимо заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 97).

Таблица 97 – Доступные параметры при добавлении пользовательских разрешений для фондов РМ

Параметр	Описание
«Роль»	Наименование заранее созданного и назначенного пользователю класса администратора
«Пользовательское разрешение»	Выбор пользовательских разрешений, касающихся фондов РМ. Список всех доступных разрешений, можно выбрать несколько: ▪ «Восстановление рабочих мест»; ▪ «Просмотр фондов рабочих мест»; ▪ «Редактирование фондов рабочих мест»; ▪ «Удаление фондов рабочих мест»; ▪ «Управление питанием фондов рабочих мест»; ▪ «Управление пользовательскими группами фондов рабочих мест»; ▪ «Управление пользователями фондов рабочих мест»; ▪ «Управление протоколами доставки фондов рабочих мест»; ▪ «Управление публикациями фондов рабочих мест»; ▪ «Управление рабочими местами в фонде»; ▪ «Управление списками сетей фондов рабочих мест»
«Объект»	Ранее созданный фонд РМ

⚠ При изменении ранее созданного разрешения параметр «Объект» менять не рекомендуется. Если нужно изменить непосредственно объект, то следует создать новое разрешение.

11.6 . Перенаправление на HTTPS

Для работы веб-интерфейса Termidesk по безопасному протоколу HTTPS, используются настройки веб-сервера `apache` для перенаправления запроса с протокола HTTP на HTTPS.

⚠ 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. Шаблон файла для протокола HTTP представлен ниже.

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

```
sudo systemctl restart apache2
```

Шаблон части конфигурационного файла для протокола HTTPS:

> Представлены только шаблоны конфигурационного файла! Изменение конфигурации не должно выполняться копированием представленного шаблона.

```
# Сайт для принудительного перенаправления на протокол HTTPS.
<VirtualHost *:80>
        ServerName #HOSTNAME#
        RewriteEngine On
        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 / 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
```

```
46
47      SSLEngine on
48      SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
49      SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
50
51      RequestHeader set X-TDSK-SSL_CLIENT_FORMAT 'apache'
52      RequestHeader set X-TDSK-SSL_CLIENT_S_DN expr=%{SSL_CLIENT_S_DN}
53      RequestHeader set X-TDSK-SSL_CLIENT_VALIDITY_START expr=%
    {SSL_CLIENT_V_START}
54      RequestHeader set X-TDSK-SSL_CLIENT_VALIDITY_END expr=%{SSL_CLIENT_V_END}
55      RequestHeader set X-TDSK-SSL_CLIENT_VERIFY expr=%{SSL_CLIENT_VERIFY}
56      RequestHeader set X-TDSK-SSL_CLIENT_CERT expr=%{SSL_CLIENT_CERT}
57  </VirtualHost>
58  </IfModule>
```

Шаблон части конфигурационного файла для работы по незащищенному протоколу HTTP (конфигурация HTTPS при этом должна быть закомментирована):

```
1   <VirtualHost *:80>
2       ServerName #HOSTNAME#
3       DocumentRoot /opt/termidesk/share/termidesk-vdi/src
4
5       Alias /media/ /opt/termidesk/share/termidesk-vdi/src/media/
6       Alias /static/ /opt/termidesk/share/termidesk-vdi/src/static/
7
8       <Directory /opt/termidesk/share/termidesk-vdi/src/static>
9           Order deny,allow
10          Allow from all
11          Require all granted
12      </Directory>
13
14      <Directory /opt/termidesk/share/termidesk-vdi/src/media>
15          Order deny,allow
16          Allow from all
17          Require all granted
18      </Directory>
19
20      RewriteEngine on
21      ProxyTimeout 70
22      ProxyPreserveHost On
23      ProxyRequests Off
24
25      ProxyPassMatch ^/media/ !
26      ProxyPassMatch ^/static/ !
27
28      ProxyPass / http://127.0.0.1:8000/
29      ProxyPassReverse / http://127.0.0.1:8000/
30
31      RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}
32
33      ErrorLog ${APACHE_LOG_DIR}/error.log
34      CustomLog ${APACHE_LOG_DIR}/access.log combined
35  </VirtualHost>
```

11.7 . Замена SSL-сертификата веб-сервера

Для доступа к веб-интерфейсу 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/private/
```

> Если сертификат и ключ находятся в PKCS12-контейнере (файл формата `.pfx`), необходимо сначала сконвертировать их в нужный формат:
>
> ```
> 1 openssl pkcs12 -in <путь_к_pfx-контейнеру> -out <путь_к_создаваемому_файлу.pem> -nodes
> 2 openssl pkcs12 -in <путь_к_pfx-контейнеру> -nocerts -nodes -out <путь_к_создаваемому_файлу.key>
> 3 openssl rsa -in <путь_к_созданному_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key>
> ```

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

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

- перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

11.8 . 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 и ЦС установлен.
Для установки корневого сертификата ЦС (например, `CA.crt`) на «Универсальный диспетчер» 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 добавление 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 параметр `REQUESTS_CA_BUNDLE` в файле `/etc/opt/termidesk-vdi/termidesk.conf`. В параметре 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
```

11.9 . 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:

```
sudo systemctl reload apache2
```

11.10 . Настройка защищенного подключения к компоненту «Универсальный диспетчер»

Для настройки защищенного подключения к компоненту «Универсальный диспетчер» нужно:

- скопировать закрытый ключ формата `.key` и сертификат формата `.pem` в каталог `/etc/opt/termidesk-vdi`:

```
sudo cp /etc/ssl/private/ssl-cert-snakeoil.key /etc/opt/termidesk-vdi/
sudo cp /etc/ssl/certs/ssl-cert-snakeoil.pem /etc/opt/termidesk-vdi/
```

- назначить права по использованию ключа и сертификата пользователю `termidesk`:

```
sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/ssl-cert-snakeoil.*
```

- предоставить права на чтение файла `ssl-cert-snakeoil.key`:

```
:~$ sudo chmod 644 /etc/opt/termidesk-vdi/ssl-cert-snakeoil.key
```

- отредактировать файл `/lib/systemd/system/termidesk-vdi.service`, добавив аргументы `--certfile` и `--keyfile` с указанием пути к файлам ключа и сертификата:

```
--keyfile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.key
--certfile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.pem
```

- пример содержимого файла `termidesk-vdi.service`:

```
[Unit]
Description=Termidesk-VDI daemon
After=network.target

[Service]
PIDFile=/run/termidesk-vdi/pid
Restart=on-failure
RestartSec=5

User=termidesk
Group=termidesk
WorkingDirectory=/opt/termidesk/share/termidesk-vdi/src

```

```
Environment=VIRTUAL_ENV=/opt/termidesk/share/termidesk-vdi/venv
Environment=PATH=/opt/termidesk/share/termideskvdi/venv/bin:/usr/sbin:/usr/bin:/sbin:/bin
EnvironmentFile=/etc/opt/termidesk-vdi/termidesk.conf

ExecStart=/bin/bash -c '/opt/termidesk/share/termidesk-vdi/venv/bin/gunicorn server.wsgi:application --timeout 60 --workers $(expr $(nproc --all) \* 3) --keyfile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.key --certfile /etc/opt/termidesk-vdi/ssl-certsnakeoil.pem --bind 127.0.0.1:8000'

ExecReload=/bin/kill -s HUP $MAINPID
ExecStop=/bin/kill -s TERM $MAINPID
PrivateTmp=true

[Install]
WantedBy=multi-user.target
```

- перезапустить сервис `termidesk-vdi.service`:

```
sudo systemctl daemon-reload && systemctl restart termidesk-vdi.service
```

- отредактировать файл `/etc/apache2/sites-available/termidesk.conf`:
  - добавить в файл следующие строки:

```
SSLProxyEngine on
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
```

где:

`SSLProxyEngine` - использование защищенного подключения по протоколу SSL/TLS, `on` - включить использование;

`SSLProxyVerify` - параметр контроля проверки сертификата. Доступны следующие значения: `none` - отключение проверки сертификата, `optional` - необязательная проверка сертификата, `require` - обязательная проверка сертификата, `optional_no_ca` - проверка сертификата без обязательной проверки цепочки сертификатов;

`SSLProxyCheckPeerCN` - проверка общего имени (Common Name, CN) сервера в сертификате, `off` - выключить проверку;

`SLProxyCheckPeerName` - проверка имени узла сервера в сертификате, `off` - выключить проверку;

`SSLProxyCheckPeerExpire` - проверка срока действия сертификата, `off` - выключить проверку.

  - изменить значения в параметрах `ProxyPass` и `ProxyPassReverse` с `http` на `https`:

```
ProxyPass / https://127.0.0.1:8000/
```

```
ProxyPassReverse / https://127.0.0.1:8000/
```

- изменить значения параметров `SSLCertificateFile` и `SSLCertificateKeyFile`, указав путь до сертификатов:

```
SSLCertificateFile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.pem
SSLCertificateKeyFile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.key
```

- пример файла `termidesk.conf`:

```
# 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
    SSLProxyEngine on
    SSLProxyVerify none
    SSLProxyCheckPeerCN off
    SSLProxyCheckPeerName off
    SSLProxyCheckPeerExpire off
    SSLCertificateFile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/opt/termidesk-vdi/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>
```

- перезапустить веб-сервер:

```
sudo systemctl daemon-reload && systemctl restart apache2.service
```

- проверить доступность веб-интерфейса.

11.11 . 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», выбрать раздел «Аутентификация» и настроить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 98).

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

Таблица 98 – 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 «Универсальному диспетчеру». Значение по умолчанию: «Да»
«Разрешить сохранение пароля в клиенте»	Управление параметром сохранения пароля в компоненте «Клиент» при подключении к «Универсальному диспетчеру». Значение по умолчанию: «Да»
«Доп. информация при ошибке входа»	Информационное сообщение, отображаемое при ошибке входа

11.12 . Настройка отправки метрик для «Сессионного агента»

Метрики узла «Сессионного агента» используются в механизмах балансировки терминальных серверов (метапоставщик) (см. подразделы **Перечень параметров для добавления терминального сервера метапоставщика** и **Балансировка подключений на основе загрузки терминальных серверов метапоставщика**), а также могут направляться в подключаемые внешние системы мониторинга.

Для настройки отправки метрик узла «Сессионного агента» следует перейти «Настройки - Системные параметры», выбрать раздел «Метрики». Доступные параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 99).

ⓘ Конфигурацию параметров можно изменить также через утилиту `termidesk-vdi-manage`: функцию `tdsk_config` и секцию `Metrics` (см. подраздел **Утилита termidesk-vdi-manage**).

Таблица 99 – Параметры отправки метрик узла «Сессионного агента»

Параметр	Описание
«Пороговое значение»	Предел индекса нагрузки, при достижении которого необходимо оповестить администратора. Для отправки уведомлений должны быть включены соответствующие параметры (см. подраздел **Настройка уведомлений о событиях**). Уведомление будет отправлено, если указанный предел индекса нагрузки достигнут однократно, но длится в течение времени, указанного в параметре «Периодичность отправки среднего значения». Диапазон значений: «1-10000». Значение по умолчанию: «5000»

Параметр	Описание
«Периодичность проверки»	Периодичность (в секундах), с которой «Сессионный агент» опрашивает ОС и собирает метрики узла. ⚠ Изменение параметра вступит в силу только после перезагрузки Termidesk или перезапуска службы `termidesk-vdi`. Следует дождаться отправки обновленного значения на «Сессионный агент» (ориентировочно спустя период, заданный в параметре «Периодичность отправки среднего значения»). Когда «Сессионный агент» получит обновленное значение, нужно перезапустить его службу после появления следующего сообщения в журнале «Сессионного агента»: «Получены новые настройки. Для применения изменений потребуется перезагрузка приложения». Диапазон значений: «1-60». Значение по умолчанию: «5»
«Периодичность отправки среднего значения»	Периодичность (в секундах), с которой «Сессионный агент» отправляет средние значения метрик «Универсальному диспетчеру». ⚠ Изменение параметра вступит в силу только после перезагрузки Termidesk или перезапуска службы `termidesk-vdi`. Следует дождаться отправки обновленного значения на «Сессионный агент» (ориентировочно спустя период, заданный в параметре «Периодичность отправки среднего значения»). Когда «Сессионный агент» получит обновленное значение, нужно перезапустить его службу после появления следующего сообщения в журнале «Сессионного агента»: «Получены новые настройки. Для применения изменений потребуется перезагрузка приложения». Диапазон значений: 1-60. Значение по умолчанию: «30»
«Размер кеша»	Размер кеша (записей) на «Сессионном агенте» для хранения метрик. На основании этого параметра происходит подсчет средних значений для отправки. ⚠ Изменение параметра вступит в силу только после перезагрузки Termidesk или перезапуска службы `termidesk-vdi`. Следует дождаться отправки обновленного значения на «Сессионный агент» (ориентировочно спустя период, заданный в параметре «Периодичность отправки среднего значения»). Когда «Сессионный агент» получит обновленное значение, нужно перезапустить его службу после появления следующего сообщения в журнале «Сессионного агента»: «Получены новые настройки. Для применения изменений потребуется перезагрузка приложения». Диапазон значений: «2-10». Значение по умолчанию: «10»

11.13 . Управление настройками компонента «Клиент»

В Termidesk предусмотрена возможность управлять некоторыми настройками компонента «Клиент»:

- переподключением пользователя к сеансам (функционал перемещения сеансов);
- обновлением списка ресурсов (РМ, опубликованных приложений) пользователя.

Для изменения настроек следует перейти «Настройки - Системные параметры», выбрать раздел «Клиент». Доступные для изменения параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 100). Для сохранения параметров после изменения нажать экранную кнопку **[Сохранить]**.

Таблица 100 – Доступные параметры при настройке переподключения к сеансам

Параметр	Описание
«Скрывать недоступные ресурсы»	Управление отображением недоступных ресурсов пользователю. Параметр действует как при подключении пользователя непосредственно через компонент «Клиент», так и при подключении через веб-браузер. Возможные значения: ▪ «Да» (по умолчанию) - недоступные ресурсы будут скрыты от пользователя; ▪ «Нет» - недоступные ресурсы будут отображены, но пользователь не сможет к ним подключиться
«Активировать управление перемещением сеансов»	Форсировать управление режимом повторного подключения пользователя. При активации параметра пользователь не сможет самостоятельно изменить настройку повторного подключения в интерфейсе «Клиента». Возможные значения: ▪ «Да» - переподключение пользователя будет форсировано со стороны «Универсального диспетчера»; ▪ «Нет» (по умолчанию) - переподключение пользователя будет управляться в интерфейсе «Клиента»
«Использовать перемещение сеансов»	ⓘ Использование возможно при активации параметра «Активировать управление перемещением сеансов». Управление повторным подключением пользователя к отключенным и активным сеансам. Функционал позволяет восстанавливать подключение после разрыва соединения или смены устройства (пользовательской рабочей станции). Таким образом пользователь сможет получить тот же сеанс, с которым работал ранее, не теряя прогресс работы. Возможные значения: ▪ «Не назначено» (по умолчанию) - выбор режима будет задан пользователем в интерфейсе «Клиента»; ▪ «Запрещено» - повторное переподключение не используется; ▪ «Повторно подключаться к активным и отключенным сеансам» (по умолчанию). В этом случае при переподключении сначала будет произведена процедура отключения активного сеанса пользователя, после которой он будет повторно подключен к отключенному сеансу; ▪ «Повторно подключаться только к отключенным сеансам». В этом случае переподключение пользователя будет происходить только к отключенным сеансам

Параметр	Описание
«Повторно подключаться к сеансам при аутентификации»	Использование возможно при активации параметра «Активировать управление перемещением сеансов». Параметр определяет режим повторного подключения к ресурсам при активации параметра «Разрешить повторное подключение». Возможные значения: ▪ «Да» - переподключение будет происходить при аутентификации пользователя через «Клиент»; ▪ «Нет» (по умолчанию) - переподключение не будет происходить при аутентификации пользователя
«Повторно подключаться к сеансам при обновлении списка приложений»	Использование возможно при активации параметра «Активировать управление перемещением сеансов». Параметр определяет режим повторного подключения к ресурсам при активации параметра «Активировать управление перемещением сеансов». Возможные значения: ▪ «Да» - переподключение будет происходить при обновлении списка ресурсов; ▪ «Нет» (по умолчанию) - переподключение не будет происходить при обновлении списка ресурсов
«Периодичность фонового обновления списка ресурсов»	Параметр определяет периодичность (в секундах), с которой будет происходить обновление списка ресурсов в интерфейсе «Клиента». Возможные значения: от 60 до 28800. Поддерживается задание специального значения «-1» - периодичность будет задана пользователем в интерфейсе «Клиента». Значение по умолчанию: «300»
«Обновлять список ресурсов при каждом запуске ресурса»	Управление режимом обновления списка ресурсов. Возможные значения: ▪ «Не задано» (по умолчанию) - выбор режима будет задан пользователем в интерфейсе «Клиента»; ▪ «Включено» - обновление списка ресурсов будет происходить при запуске какого-либо ресурса пользователем; ▪ «Выключено» - обновление списка ресурсов не будет происходить при запуске какого-либо ресурса пользователем

Отключенный сеанс - это сеанс работающего РМ без активного подключения со стороны программы доставки (например, ПО Termidesk Viewer). Активный сеанс, соответственно, предполагает активное подключение со стороны программы доставки.

11.14 . Изменение способа хранения паролей на OpenBao

При стандартной настройке Termidesk пароли хранятся в преобразованном виде в файле `/etc/opt/termidesk-vdi/termidesk.conf`. Начиная с Termidesk версии 5.1 добавлен новый способ хранения паролей с использованием настроенного хранилища OpenBao.

Для изменения способа хранения паролей и перехода на использование хранилища OpenBao нужно:

- задать в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` параметру `SECRET_STORAGE_METHOD` значение `openbao`;
- задать остальные параметры конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf`, относящиеся к OpenBao (см. подраздел **Параметры конфигурирования компонентов «Универсальный диспетчер», «Менеджер рабочих мест»**);
- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- выполнить команду миграции:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_openbao_migrate
```

При появлении ошибок после выполнения команды миграции нужно:

- изменить значение параметра `SECRET_STORAGE_METHOD` на `config`;
- повторить ввод паролей для параметров, указанных в ошибке;
- снова изменить значение `SECRET_STORAGE_METHOD` на `openbao`;
- выполнить команду миграции:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_openbao_migrate
```

Для возврата к способу хранения паролей из конфигурационного файла нужно:

- убедиться, что в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` параметру `SECRET_STORAGE_METHOD` задано значение `openbao`;
- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- выполнить команду миграции:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_openbao_reverse_migrate
```

- задать в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` параметру `SECRET_STORAGE_METHOD` значение `config`.

12 . РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

12.1 . Общие сведения

Поскольку каждая установка компонентов Termidesk может отличаться от других, подробные шаги по резервному копированию и восстановлению и используемые инструменты будут приведены только для некоторых компонентов. Резервное копирование и восстановление может выполняться как средствами и службами ОС, так и специализированными системами. Порядок выполнения и периодичность резервного копирования определяются эксплуатирующей организацией.

Резервному копированию подлежат:

- БД Termidesk;
- конфигурационные файлы компонента «Универсальный диспетчер» и административного и/или пользовательского порталов;
- конфигурационные файлы компонента «Шлюз»;
- конфигурационные файлы компонента «Менеджер рабочих мест»;
- конфигурационные файлы компонента «Сервер терминалов Astra Linux»;
- конфигурационные файлы компонента «Сессионный агент»;
- конфигурационные файлы балансировщика нагрузки;
- конфигурационные файлы, использующиеся для режима высокой доступности.

В качестве альтернативного варианта могут резервироваться целиком узлы компонентов, если они установлены на ВМ. Такой подход применяется, например, для резервирования компонента «Виртуальный модуль Termidesk».

Как правило, файлы компонентов «Удаленный помощник», «Клиент» не подлежат резервному копированию, т.к. повторная установка в большинстве случаев будет быстрее.

12.2 . Действия с БД Termidesk

12.2.1 . Резервное копирование БД

Резервное копирование БД, созданной СУБД PostgreSQL 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.

12.2.2 . 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 --format=t <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`;

`--format=t <файл_копии_БД.tar>` - ключ для восстановления БД из резервной копии в формате `tar`.

12.3 . Действия с брокером сообщений RabbitMQ

12.3.1 . Резервное копирование данных брокера сообщений RabbitMQ

Для брокера сообщений RabbitMQ следует:

- остановить службу `rabbitmq-server`:

```
sudo systemctl stop rabbitmq-server
```

- выполнить резервное копирование каталога `/etc/rabbitmq/` вместе с его содержимым;
- выполнить резервное копирование каталога данных `/var/lib/rabbitmq/mnesia/`;
- запустить службу `rabbitmq-server`:

```
sudo systemctl start rabbitmq-server
```

12.3.2 . Восстановление брокера сообщений RabbitMQ из резервной копии

> ⓘ Современные версии RabbitMQ (3.8.0+) поддерживают восстановление из резервной копии тогда, когда они восстанавливаются на узел RabbitMQ с точно таким же именем узла, с которого была создана резервная копия данных.

Для восстановления конфигурации RabbitMQ следует:

- остановить службу `rabbitmq-server`:

```
sudo systemctl stop rabbitmq-server
```

- восстановить резервные копии каталогов `/etc/rabbitmq/` и `/var/lib/rabbitmq/mnesia/`;
- запустить службу `rabbitmq-server`:

```
sudo systemctl start rabbitmq-server
```

12.4 . Действия с компонентом «Универсальный диспетчер»

12.4.1 . Резервное копирование данных «Универсального диспетчера»

Для компонента «Универсальный диспетчер» следует выполнить резервное копирование:

- каталога `/etc/opt/termidesk-vdi/` вместе с его содержимым;
- конфигурационного файла `/etc/apache2/sites-available/termidesk.conf`;
- ключей `/etc/ssl/certs/ssl-cert-snakeoil.pem` и `/etc/ssl/private/ssl-cert-snakeoil.key`, использующихся для защищенного подключения.

12.4.2 . Восстановление «Универсального диспетчера» из резервной копии

Для восстановления конфигурации «Универсального диспетчера» следует:

- восстановить резервную копию каталога `/etc/opt/termidesk-vdi/`;
- восстановить резервные копии конфигурационного файла `/etc/apache2/sites-available/termidesk.conf` и ключей `/etc/ssl/certs/ssl-cert-snakeoil.pem`, `/etc/ssl/private/ssl-cert-snakeoil.key`;
- перезапустить службу `termidesk-vdi`:

```
sudo systemctl restart termidesk-vdi
```

- перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

12.5 . Действия с компонентом «Шлюз»

12.5.1 . Резервное копирование данных «Шлюза»

Для компонента «Шлюз» следует выполнить резервное копирование:

- конфигурационного файла `/etc/termidesk/gateway.yaml`;
- ключей, использующихся для защищенного соединения, указанных в файле `/etc/termidesk/gateway.yaml`.

12.5.2 . Восстановление «Шлюза» из резервной копии

Для восстановления конфигурации «Шлюза» следует:

- восстановить резервную копию файла `/etc/termidesk/gateway.yaml` и ключей указанных в этом файле;
- перезапустить службу `termidesk-gateway`:

```
sudo systemctl restart termidesk-gateway
```

12.6 . Действия с компонентом «Менеджер рабочих мест»

12.6.1 . Резервное копирование данных «Менеджера рабочих мест»

Для компонента «Менеджер рабочих мест» следует выполнить резервное копирование каталога `/etc/opt/termidesk-vdi/` вместе с его содержимым.

12.6.2 . Восстановление «Менеджера рабочих мест» из резервной копии

Для восстановления конфигурации «Менеджера рабочих мест» следует:

- восстановить резервную копию каталога `/etc/opt/termidesk-vdi/`;
- перезапустить службы:

```
sudo systemctl restart termidesk-celery-beat termidesk-celery-worker
```

⚠ Служба `termidesk-taskman` исключена из Termidesk, начиная с версии 6.0.

12.7 . Действия с компонентом «Сервер терминалов Astra Linux»

12.7.1 . Резервное копирование данных «Сервера терминалов Astra Linux»

Для компонента «Сервер терминалов Astra Linux» следует выполнить резервное копирование каталога `/etc/stal/` и компонента «Сессионный агент» (см. подраздел **Резервное копирование данных «Сессионного агента»**).

12.7.2 . Восстановление «Сервера терминалов Astra Linux» из резервной копии

Для восстановления конфигурации «Сервера терминалов Astra Linux» следует:

- восстановить резервную копию каталога `/etc/stal/`;
- восстановить компонент «Сессионный агент» (см. подраздел **Восстановление «Сессионного агента» из резервной копии**);
- перезапустить службы:

```
sudo systemctl restart termidesk-stal stal-proxy stal-rdpepc
```

12.8 . Действия с компонентом «Сессионный агент»

12.8.1 . Резервное копирование данных «Сессионного агента»

Для компонента «Сессионный агент» следует выполнить резервное копирование:

- каталога `/etc/opt/termidesk-ssa/` (для ОС Astra Linux Special Edition (Server));
- каталога `%ProgramData%\UVEON\Termidesk Session Agent\` (для ОС Microsoft Windows Server).

12.8.2 . Восстановление «Сессионного агента» из резервной копии

Для восстановления конфигурации «Сессионного агента» следует:

- восстановить резервную копию каталога `/etc/opt/termidesk-ssa/` (для ОС Astra Linux Special Edition (Server)) или `%ProgramData%\UVEON\Termidesk Session Agent\` (для ОС Microsoft Windows Server);
- перезапустить службу `TermideskSessionAgentService` через оснастку «Службы» в ОС Microsoft Windows Server или командой в ОС Astra Linux Special Edition (Server):

```
sudo systemctl restart termidesk-session-agent
```

12.9 . Действия с балансировщиком нагрузки

12.9.1 . Резервное копирование данных балансировщика нагрузки

> ⓘ Пример приведен для балансировщика nginx, поскольку его настройка описана в качестве примера в подразделе **Настройка балансировщика для работы с самоподписанными сертификатами**.

Для балансировщика нагрузки `nginx` следует выполнить резервное копирование:

- каталога `/etc/nginx/snippets`;
- каталога с ключами и сертификатами `/etc/ssl/`;
- каталога `/etc/nginx/sites-available/`;
- каталога `/etc/nginx/conf.d/`.

12.9.2 . Восстановление балансировщика нагрузки из резервной копии

Для восстановления конфигурации балансировщика нагрузки `nginx` следует:

- восстановить резервные копии каталогов `/etc/nginx/snippets`, `/etc/ssl/`, `/etc/nginx/sites-available/`, `/etc/nginx/conf.d/`;
- перезапустить веб-сервер:

```
sudo systemctl restart nginx
```

12.10 . Действия для режима высокой доступности

12.10.1 . Резервное копирование конфигурации режима высокой доступности

Для режима высокой доступности, настраиваемого для отказоустойчивой или распределенной установки Termidesk, следует выполнить резервное копирование каталога `/etc/keepalived/`.

12.10.2 . Восстановление конфигурации режима высокой доступности из резервной копии

Для восстановления конфигурации режима высокой доступности следует:

- восстановить из резервной копии каталог `/etc/keepalived/`;
- перезапустить сервис `keeaplived`:

```
sudo systemctl restart keepalived
```

13 . ГЕНЕРАЦИЯ ОТЧЕТА ПО МОДЕЛЯМ ДАННЫХ И СТРУКТУРАМ БД TERMIDESK

13.1 . Генерация отчета по моделям данных и структурам БД Termidesk

В Termidesk реализована возможность генерации отчета по моделям данных и структурам БД с описанием полей таблиц, их значений и межтабличных связей.

Для генерации отчета следует перейти в интерфейс командной строки и выполнить следующее:

- если требуется сгенерировать отчет по модели данных и структуре БД приложения:

```
sudo /opt/termidesk/sbin/termidesk-vdi-manage tdsk_graph_models termidesk >
<имя_файла_для_сохранения.html>
```

где:

`termidesk` - название приложения;

`<имя_файла_для_сохранения.html>` - имя и формат файла (`html`) для сохранения отчета.

⚠ Для генерации отчета по модели данных и структуре БД нескольких приложений их названия указываются через пробел.

- если требуется сгенерировать отчет по всей модели данных и структуре БД Termidesk:

```
sudo /opt/termidesk/sbin/termidesk-vdi-manage tdsk_graph_models -a -g >
<имя_файла_для_сохранения.html>
```

где:

`-a` - ключ для генерации отчета, описывающего все доступные модели данных и структуры БД;

`-g` - ключ группировки таблиц в соответствии с их приложениями;

`<имя_файла_для_сохранения.html>` - имя и формат файла (`html`) для сохранения отчета.

Структура файла отчета приведена в таблице (см. Таблица 101).

Таблица 101 – Структура файла отчёта

Параметр	Описание
`App`	Название приложения, для которого представлена структура модели данных
`Model`	Идентификатор модели с представлением структуры данных
`Abstract Model`	Идентификатор модели, для которой представлена структура данных
`<Информационная строка>`	Строка содержит модель отчета с перечислением полей, либо дополнительную информацию о модели данных
`NAME`	Столбец содержит имена параметров

Параметр	Описание
VALUE	Столбец содержит тип данных параметров
HELP TEXT	Столбец содержит описание параметров

14 . МОНИТОРИНГ И УВЕДОМЛЕНИЯ

14.1 . Системные параметры мониторинга

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

Для конфигурации системных параметров мониторинга следует перейти «Настройки - Системные параметры», выбрать раздел «Мониторинг».
Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 102).

Таблица 102 – 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 узел с «Универсальным диспетчером» 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`)

14.2 . Настройка отправки уведомлений о системных событиях

Для настройки отправки уведомлений о системных событиях следует перейти «Настройки - Системные параметры», выбрать раздел «Уведомления».
Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 103).

Таблица 103 – 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 сервера исходящей электронной почты. Пример: «smtp.mail.ru»

Параметр	Описание
«Порт»	Номер порта, на котором ведется прослушивание службой сервера электронной почты. При указании номера порта стоит руководствоваться правилами: ▪ если используется порт 25, то параметры «Поддержка TLS» и «Поддержка SSL» активировать не нужно; ▪ если используется порт 465, то нужно активировать параметр «Поддержка SSL»; ▪ если используется порт 587, то нужно активировать параметр «Поддержка TLS»; ▪ если используется порт 2525, то нужно активировать параметр «Поддержка TLS»
«Email отправителя»	Почтовый адрес отправителя сообщений на сервере электронной почты. Формат: user@domain. Пример: «user.mail.ru»
«Пользователь»	Идентификатор пользователя сервиса электронной почты
«Пароль»	Последовательность символов для подтверждения полномочий пользователя сервиса электронной почты
«Поддержка TLS»	Управление режимом поддержки протокола TLS при взаимодействии с сервером электронной почты. Значение по умолчанию: «Нет»
«Поддержка SSL»	Управление режимом поддержки протокола SSL при взаимодействии с сервером электронной почты. Значение по умолчанию: «Нет»
«Таймаут»	Время ожидания (в секундах) ответа от сервера электронной почты. Возможные значения: от 1 до 180. Значение по умолчанию: «30»
«Email получателей (через запятую)»	Перечень адресов электронной почты получателей уведомлений. Формат: user@domain. Пример: «user.mail.ru»
«Префикс для темы письма»	Текстовое поле, содержащее информацию для подстановки в тему электронного письма
«Уведомление о смене режима техобслуживания в поставщике ресурсов»	Управление режимом отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания в поставщике ресурсов». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление о смене режима техобслуживания в фонде рабочих мест»	Управление режимом отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания в фонде рабочих мест». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление о смене режима техобслуживания для рабочих мест»	Управление режимом отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания для рабочих мест». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление о возникновении ошибок с рабочими местами»	Управление режимом отправки уведомления по электронной почте о системном событии «Возникновение ошибок внутри фонда рабочих мест». Значение по умолчанию: «Нет» (уведомления не отправляются)

Параметр	Описание
«Уведомление о превышении лицензированного количества подключений»	Управление режимом отправки уведомления по электронной почте о системном событии «Запрос подключения сверх лимита, установленного лицензией». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление о превышении лицензированного количества пользователей»	Управление режимом отправки уведомления по электронной почте о системном событии «Запрос входа пользователя сверх лимита, установленного лицензией». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление о превышении максимума индекса нагрузки»	Управление режимом отправки уведомления по электронной почте о системном событии «Превышение максимального индекса нагрузки». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление о превышении порога индекса нагрузки»	Управление режимом отправки уведомления по электронной почте о системном событии «Превышение порога индекса нагрузки». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление об истечении срока действия сертификата»	Управление режимом отправки уведомления по электронной почте о системном событии «Истечение срока действия сертификата». Указывается значение (в сутках), определяющее временной промежуток до окончания срока действия сертификата, по достижении которого администратору будет отправлено уведомление. Поддерживается указание специального значения «-1» - отправка уведомления отключена. Значение по умолчанию: «30»

Также возможна регистрация и отправка событий, управляемая параметром «Отправлять уведомление при превышении лимита интервала опроса поставщика» (см. подраздел **Общие системные параметры Termidesk**):

- о достижении предела свободного места на хранилище поставщика ресурсов;
- о недоступности хранилища поставщика ресурсов;
- о доступности хранилища поставщика ресурсов.

14.3 . Шаблон для мониторинга Zabbix

Termidesk поддерживает мониторинг состояния компонентов через ПО Zabbix.

Шаблон для мониторинга доступен по ссылке: https://gitflic.ru/project/uveon/termidesk-zabbix.

В шаблоне находятся метрики для мониторинга компонентов Termidesk: «Универсального диспетчера», «Шлюза», «Менеджера рабочих мест».

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

14.4 . 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 нажать экранную кнопку **[Создать]**, выбрать тип отчета «Отчет по последнему пользовательскому входу в систему» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 104).

Таблица 104 – 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 нажать экранную кнопку **[Создать]**, выбрать тип отчета «Отчет по пользовательским сеансам» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 105).

Таблица 105 – 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
«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 нажать экранную кнопку **[Создать]**, выбрать тип отчета «Отчет по пользовательским подключениям» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 106).

Таблица 106 – 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 75).

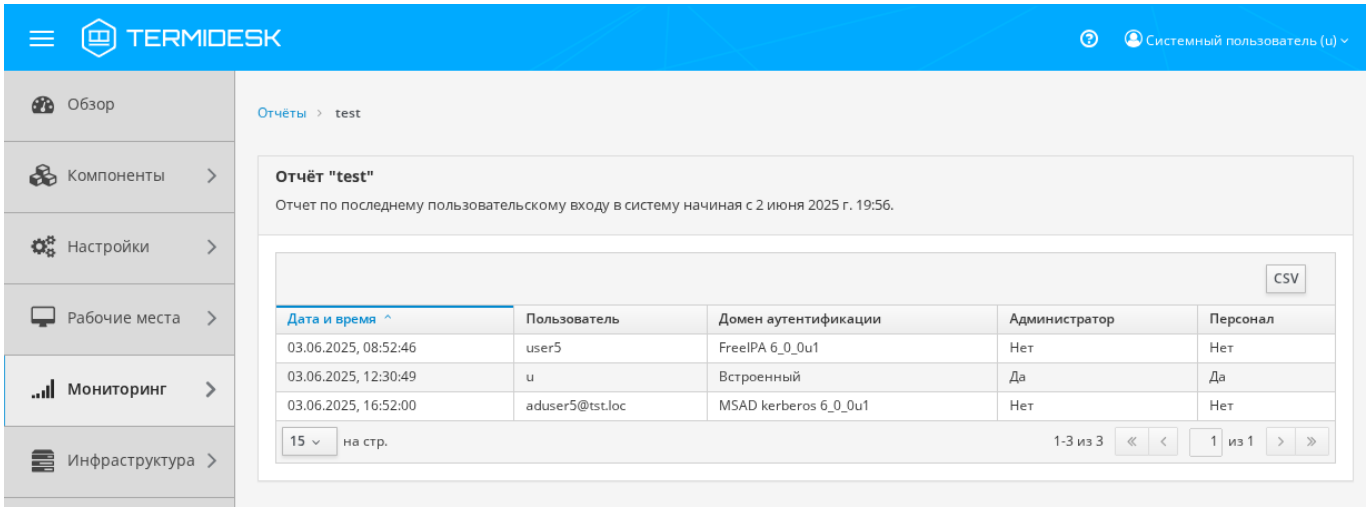

Рисунок 75 – Окно сформированного отчета по последнему пользовательскому входу

14.5 . Получение метрик узлов компонентов

В Termidesk реализован механизм API-запросов для получения метрик узлов, на которых установлены компоненты Termidesk, что позволяет использовать полученные метрики во внешних системах мониторинга и непосредственно в Termidesk. Например, метрики узла «Сессионного агента» используются в механизмах балансировки терминальных серверов метапоставщика (см. подразделы **Настройка отправки метрик для «Сессионного агента»** и **Балансировка подключений на основе загрузки терминальных серверов метапоставщика**).

Для получения метрик узлов компонентов используется библиотека `psutil`, документация которой доступна на сайте: https://psutil.readthedocs.io/en/latest/.

Формат API-запроса получения метрик, а также список возвращаемых метрик приведен в документе СЛЕТ.10001-01 91 01 «Инструкция по использованию. REST API» по каждому компоненту, поддерживающему эту функциональность, отдельно.

Поддерживается отправка метрик для следующих компонентов:

- «Универсальный диспетчер», см. подраздел **Доступные команды модуля «health»** документа СЛЕТ.10001-01 91 01 «Инструкция по использованию. REST API»;
- «Сессионный агент», см подраздел **Доступные команды модуля «health» компонента «Сессионный агент»** документа СЛЕТ.10001-01 91 01 «Инструкция по использованию. REST API»;
- «Агент виртуального рабочего места», см. подраздел **Доступные команды модуля «health» компонента «Агент виртуального рабочего места»** документа СЛЕТ.10001-01 91 01 «Инструкция по использованию. REST API»;
- «Шлюз», см. подраздел **Доступные команды модуля «health» компонента «Шлюз»** документа СЛЕТ.10001-01 91 01 «Инструкция по использованию. REST API».

15 . СИСТЕМА АУДИТА

15.1 . Системные параметры аудита

Для конфигурации системных параметров аудита следует перейти «Настройки - Системные параметры», выбрать раздел «Аудит».

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 106).

Таблица 107 – Системные параметры аудита

Параметр	Описание
«Использовать "строгий" режим аудита»	Управление использованием «строгого» режима аудита. Этот режим аудита запрещает внесение изменений в часть настроек при недоступности БД Termidesk (таблицы termidesk_audit_event_log). Значение по умолчанию: «Нет»
«Использовать формат CEF»	Управление использованием формата CEF для записи событий аудита. События аудита в этом формате: ▪ записываются в таблицу БД AuditEventV2, если параметр «Сохранение в БД» активирован; ▪ записываются в локальный файл журнала, если параметр «Сохранение в файл» активирован и задан путь к файлу в параметре «Файл хранения событий»; ▪ отправляются на отдельный syslog-сервер, если параметр «Отправка в Syslog» активирован и заданы параметры syslog-сервера. Значение по умолчанию: «Нет»
«Сохранение в БД»	Выбор сохранения событий аудита в БД
«Время хранения записи в БД»	Время хранения (в сутках) записи события аудита в БД. Удаление устаревших записей аудита выполняется периодической задачей каждые 24 часа. Значение по умолчанию: «7»
«Максимум удаляемых событий»	Максимальное количество удаляемых событий в журнале аудита Значение по умолчанию: «1000»
«Сохранение в файл»	Выбор сохранения событий аудита в отдельный файл журнала Значение по умолчанию: «Нет»
«Файл хранения событий»	Указание полного пути к файлу хранения журнала событий аудита при выбранной опции «Сохранение в файл» ⚠ Файл журнала должен располагаться в каталоге, к которому имеет доступ пользователь `termidesk`. Например, `/var/log/termidesk`.
«Количество архивных файлов»	Максимальное количество архивных файлов журнала событий аудита, по достижении которого начинается перезапись. Возможные значения: от 7 до 30. Значение по умолчанию: «7»

Параметр	Описание
«Отправка в Syslog»	Направление логирования на отдельный syslog-сервер. Значение по умолчанию: «Нет»
«Хост»	IP-адрес или имя узла, на котором развёрнута служба syslog-сервера. Значение по умолчанию: «localhost»
«Протокол»	Выбор протокола работы для службы syslog-сервера. Доступные значения: «UDP», «TCP», «TLS». При использовании протокола «TLS» необходимо установить на «Универсальный диспетчер» 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. Значение по умолчанию: «514»
«Категория сообщения»	Выбор категории сообщений, которые будут записываться в журнал аудита. Значение по умолчанию: «local7»

События аудита, регистрируемые Termidesk, приведены в подразделе **Типы и шаблоны регистрируемых событий аудита**.

15.2 . 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 «Универсального диспетчера» Termidesk;
- `use.log` - записываются события подключения пользователей РМ;
- `workers.log` - записываются события обработчика фоновых задач;
- `aggregator.log` - записываются события работы портала «Агрегатор».

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

15.3 . Настройка журналирования

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

Для изменения уровня журналирования нужно:

- изменить параметр `LOG_LEVEL`;
- перезапустить службы Termidesk:

```
1 sudo systemctl restart termidesk-vdi.service termidesk-celery-beat.service termidesk-celery-worker.service
```

15.4 . Просмотр журналов «Универсального диспетчера»

15.4.1 . Просмотр системного журнала

Для просмотра общего журнала событий, связанного с функционированием Termidesk, следует перейти «Мониторинг - Системные журналы», 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.

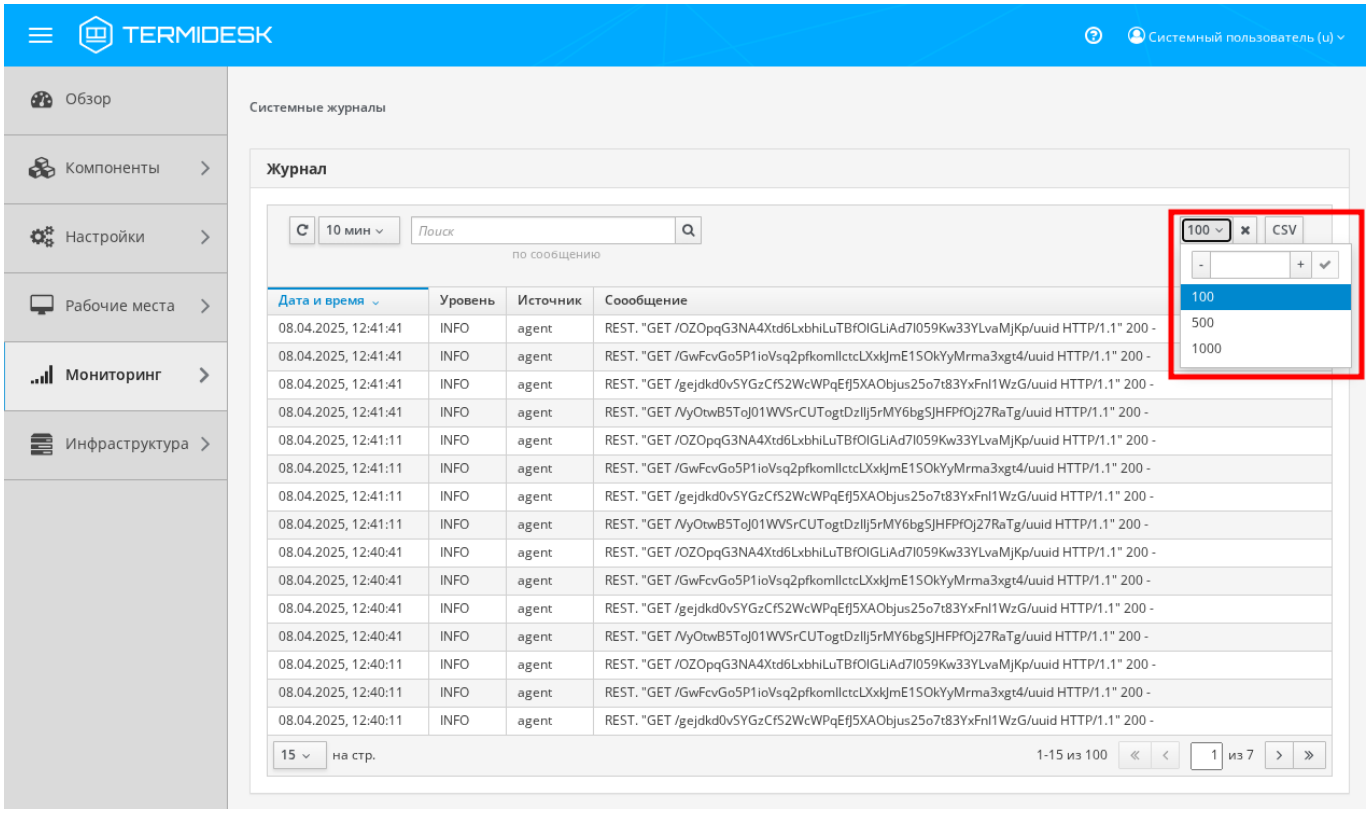

Рисунок 76 – Отображение общего журнала в графическом интерфейсе управления Termidesk

Для задания лимита записей, загружаемых из БД и отображаемых в веб-интерфейсе, нужно:

- нажать на экранную кнопку **[Выберите лимит]**. По умолчанию загружаются 100 записей, значение «100» отображается как значение экранной кнопки;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке;
- или ввести свое значение в доступном поле и подтвердить выбор, используя графический элемент  или клавишу **<ENTER>**. Возможные значения: от 1 до 100 000. Указанное значение сохранится в списке до перезагрузки страницы.

Для сброса заданного лимита нужно воспользоваться графическим элементом  .

> ⚠ Если задействовано поле ввода поискового запроса, сначала выполняется поиск записей в БД, удовлетворяющих условиям поиска, и только затем применяется ограничение выбранного лимита.
> Пример: пусть в таблице БД существует 101 запись, а в веб-интерфейсе задан поисковый запрос и лимит в 100 записей. Если параметрам поискового запроса удовлетворяют порядковые записи 5, 10, 101, то 101-ая запись не отобразится.

Для обновления значений таблицы используется графический элемент  . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом.

Также поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент  под таблицей. По умолчанию отображаются 15 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента.

15.4.2 . Просмотр журнала аудита

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

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

При помощи экранной кнопки [CSV] (см. Рисунок 77) можно выгрузить в csv-файл весь представленный журнал событий, либо строки событий.

Количество событий, отображаемых в графическом интерфейсе или экспортируемых в csv-файл, также можно менять при помощи экранной кнопки **[Выберите лимит]**, как это приведено в подразделе Просмотр системного журнала (see page 327).

> ⚠ Если задействовано поле ввода поискового запроса и задана фильтрация по событию и дате, сначала выполняется поиск записей в БД, удовлетворяющих условиям поиска и фильтрации, и только затем применяется ограничение выбранного лимита.
> Пример: пусть в таблице БД существует 101 запись, а в веб-интерфейсе задан поисковый запрос, фильтрация по типу события и дате, и лимит в 100 записей. Если параметрам поискового запроса удовлетворяют порядковые записи 5, 10, 101, то 101-ая запись не отобразится.

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

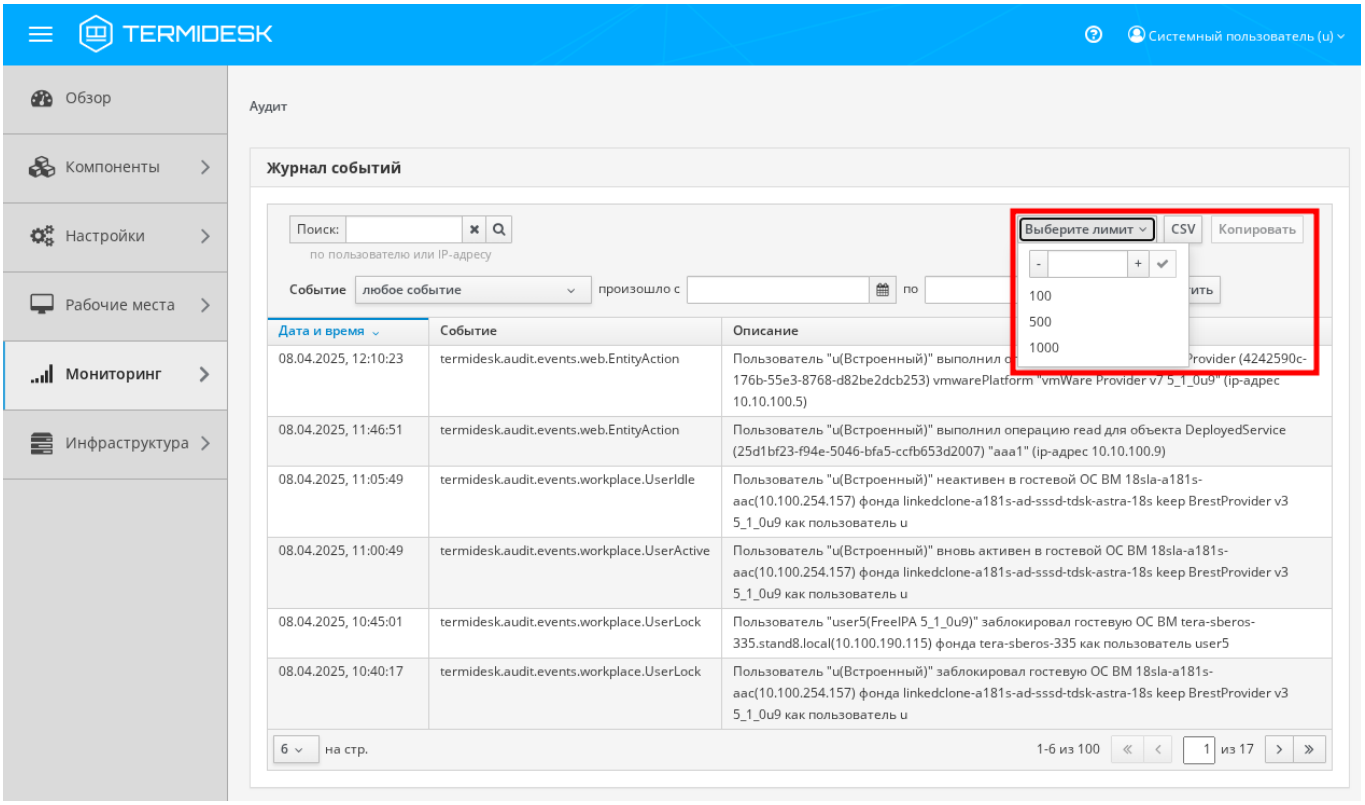

Рисунок 77 – Отображение журнала аудита в графическом интерфейсе управления Termidesk

15.5 . Просмотр централизованных журналов фермы

15.5.1 . Отображение централизованных журналов фермы

Для просмотра централизованных журналов событий, связанных с функционированием фермы Termidesk, следует перейти «Мониторинг - Журналы фермы», где визуализируются события из «Хранилища журналов».

> ⓘ Ферма Termidesk - логическое объединение узлов Termidesk, взаимодействующих с одной БД.

Для отображения событий нужно убедиться, что:

- добавлен и настроен «Ретранслятор» согласно подразделам **Добавление «Ретранслятора»** и **Настройка узла «Ретранслятора» с ПО Fluentd**;
- добавлено «Хранилище журналов» согласно подразделу **Управление «Хранилищами журналов»**.

> ⚠ Если ранее узел «Ретранслятора» настраивался для Termidesk версии младше 6.0, то его конфигурацию следует изменить (см. подраздел **Настройка узла «Ретранслятора» с ПО Fluentd**).

Представленный журнал событий можно выгрузить в csv-файл при помощи экранной кнопки [CSV].

По умолчанию записи событий представлены (см. Рисунок 77) в табличном виде и упорядочены согласно столбцу «Дата и время».

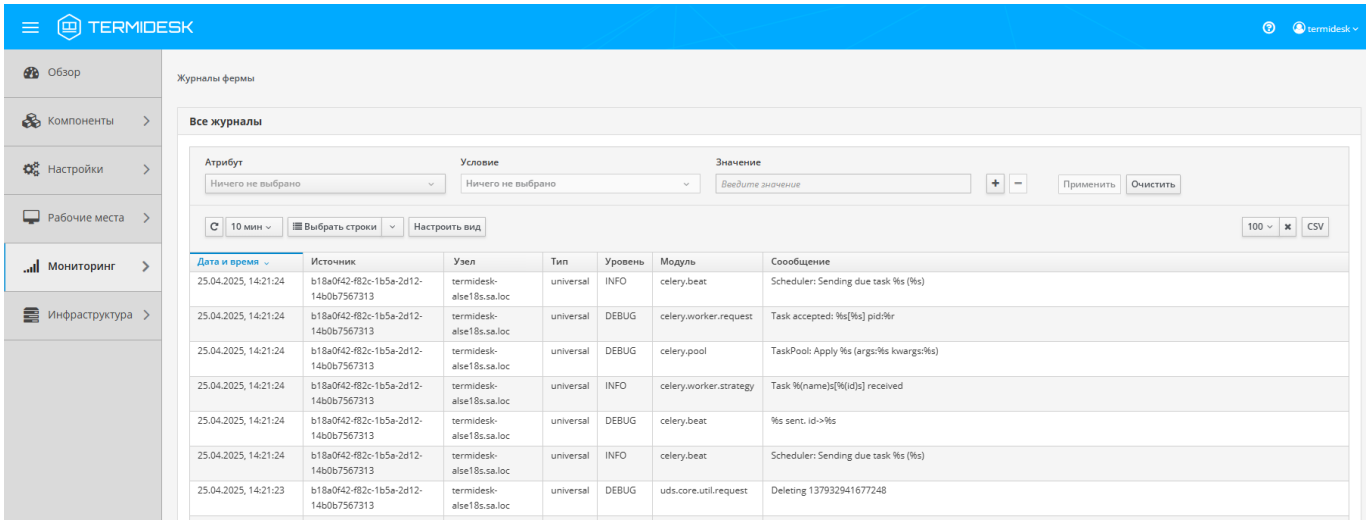

Рисунок 78 – Отображение централизованных журналов фермы

Основные параметры списка приведены в таблице (см. Таблица 108).

Таблица 108 – Основные параметры списка событий централизованного журнала

Параметр	Описание
«Дата и время»	Дата и время регистрации события
«Источник»	Системный UUID узла, который зарегистрировал событие
«Узел»	Имя узла
«Тип»	Тип портала, который зарегистрировал событие. Может быть: «admin» («Портал администратора»), «user» («Портал пользователя»), «universal» («Портал универсальный»)
«Уровень»	Категория сообщения. Возможные значения:«INFO», «DEBUG», «WARNING», «ERROR»
«Модуль»	Служба Termidesk, которая зарегистрировала событие
«Сообщение»	Подробное описание события

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться экранной кнопкой **[Настроить вид]** и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для применения изменений нажать экранную кнопку **[Сохранить]**. При попытке убрать выбор со всех пунктов экранная кнопка **[Сохранить]** будет заблокирована. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить вид]**;

- порядок следования столбцов. Для изменения порядка следования нужно захватить левой кнопкой мыши заголовок столбца, и, не отпуская ее, перенести его в нужное расположение. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок колонок]**, которая становится доступна только после изменения порядка следования столбцов и будет скрыта после сброса;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.

Для задания лимита записей, загружаемых из БД и отображаемых в веб-интерфейсе, нужно:

- нажать на экранную кнопку **[Выберите лимит]**. По умолчанию загружаются 100 записей, значение «100» отображается как значение экранной кнопки;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке;
- или ввести свое значение в доступном поле и подтвердить выбор, используя графический элемент  или клавишу **<ENTER>**. Возможные значения: от 1 до 1 000 000. Указанное значение сохранится в списке до перезагрузки страницы.

Для сброса заданного лимита нужно воспользоваться графическим элементом  .

> ⚠ При включенной фильтрации записей по атрибутам сначала выполняется поиск записей в БД, удовлетворяющих условиям фильтра, и только затем применяется ограничение выбранного лимита.
> Пример: пусть в таблице БД существует 101 запись, а в веб-интерфейсе задана фильтрация по атрибутам и лимит в 100 записей. Если параметрам фильтрации удовлетворяют порядковые записи 5, 10, 101, то 101-ая запись не отобразится.

Существуют варианты выбора записей таблицы, доступные через выпадающий список экранной кнопки **[Выбрать строки]**, а именно:

- выделить все строки таблицы, активировав «Выбрать все»;
- выделить все строки на текущей странице таблицы, активировав «Выбрать все на стр.»;
- сбросить выделение строк, активировав «Сбросить».

> ⚠ В случае изменения ширины столбцов или их порядка произойдет сброс ранее выполненного выделения.

Для обновления значений таблицы используется графический элемент  . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом.

Также поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент  под таблицей. По умолчанию отображаются 15 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента.

15.5.2 . Фильтрация списков событий журналов фермы

Для списка РМ доступен механизм фильтрации. Фильтрация осуществляется путем задания значений для параметров «Атрибут», «Условие» и «Значение».

Для добавления дополнительного фильтра следует нажать экранную кнопку **[+]**. Для удаления фильтра нужно использовать экранную кнопку **[-]** в соответствующей строке.

Чтобы применить установленные параметры фильтрации, следует нажать экранную кнопку **[Применить]**.

Экранная кнопка **[Очистить]** возвращает параметры фильтра к исходному состоянию: удаляются дополнительные строки фильтра, все значения сбрасываются, поля «Условие» и «Значение» блокируются.

Подробное описание механизма фильтрации списка РМ приведено в таблице (см. Таблица 109).

При ручном вводе данных в поле фильтра «Значение» допускается полный или частичный ввод только одного параметра фильтрации.

При применении нескольких одинаковых фильтров к списку фильтрация выполняется с учетом только последнего заданного фильтра.

Таблица 109 – Параметры фильтрации событий журналов фермы

Атрибут	Условия	Значение
«Дата и время»	Формирование списка событий по времени создания: ▪ «В пределах» - в указанном временном промежутке; ▪ «Не в пределах» - исключая указанный временной промежуток	▪ «Минута»; ▪ «5 минут»; ▪ «30 минут»; ▪ «1 час»; ▪ «12 часов»; ▪ «24 часа»; ▪ «Сегодня»; ▪ «Эта неделя»; ▪ «Этот месяц»
«Источник»	Формирование списка событий по источнику события: ▪ «Является» - по указанному наименованию источника; ▪ «Не является» - исключая указанное наименование источника; ▪ «Начинается с» - по начальной части наименования источника; ▪ «Оканчивается на» - по конечной части наименования источника; ▪ «Содержит» - включая указанную часть наименования источника	Ручной ввод

Атрибут	Условия	Значение
«Тип»	Формирование списка событий по типу события: ▪ «Является» - по указанному наименованию типа события; ▪ «Не является» - исключая указанное наименование типа события; ▪ «Начинается с» - по начальной части наименования типа события; ▪ «Оканчивается на» - по конечной части наименования типа события; ▪ «Содержит» - включая указанную часть наименования типа события	Ручной ввод
«Узел»	Формирование списка событий по имени узла: ▪ «Является» - по указанному наименованию; ▪ «Не является» - исключая указанное наименование; ▪ «Начинается с» - по начальной части наименования; ▪ «Оканчивается на» - по конечной части наименования; ▪ «Содержит» - включая указанную часть наименования	Ручной ввод
«Уровень»	Формирование списка событий по уровню: ▪ «Является» - по указанному уровню события; ▪ «Не является» - исключая указанный уровень события	▪ «INFO»; ▪ «DEBUG»; ▪ «WARNING»; ▪ «ERROR»
«Модуль»	Формирование списка событий по модулю: ▪ «Является» - по указанному наименованию модуля; ▪ «Не является» - исключая указанное наименование модуля; ▪ «Начинается с» - по начальной части наименования модуля; ▪ «Оканчивается на» - по конечной части наименования модуля; ▪ «Содержит» - включая указанную часть наименования модуля	Ручной ввод
«Сообщение»	Формирование списка событий по сообщению: ▪ «Является» - по указанному сообщению; ▪ «Не является» - исключая указанное сообщение; ▪ «Начинается с» - по начальной части сообщения; ▪ «Оканчивается на» - по конечной части сообщения; ▪ «Содержит» - включая указанную часть сообщения	Ручной ввод

15.6 . Описание шаблонов событий аудита

15.6.1 . Типы данных регистрируемой информации событий аудита

При фиксации событий аудита используется ряд типов данных (см. Таблица 110) регистрируемой информации, состав которых может отличаться для разных событий.

Таблица 110 – 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
Результат	Результат выполнения действия
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)

15.6.2 . Типы и шаблоны регистрируемых событий аудита

Список регистрируемых событий и шаблоны к ним приведены в таблице (см. Таблица 111).

Таблица 111 – Список типов и шаблонов регистрируемых событий аудита

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

Вход пользователя в систему через командную строку `cli.UserLogin`	Регистрируется: ▪ наименование домена аутентификации (`authenticator`); ▪ логин пользователя (`username`); ▪ тип портала (`portal`); ▪ идентификатор портала (`portal_uuid`)	«Пользователь `"[username] ([authenticator])"` вошел в систему через `[portal] ([portal_uuid])`»
Выход пользователя из системы через командную строку `cli.UserLogout`	Регистрируется: ▪ наименование домена аутентификации (`authenticator`); ▪ логин пользователя (`username`); ▪ тип портала (`portal`); ▪ идентификатор портала (`portal_uuid`)	«Пользователь `"[username] ([authenticator])"` вышел из системы через `[portal] ([portal_uuid])`»
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 РМ `policies.DeployedServicePolicyChanged`	Регистрируется: ▪ имя пользователя (`username`); ▪ название домена аутентификации пользователя (`authenticator_name`); ▪ название политики (`policy_name`); ▪ название фонда РМ (`deployed_service_name`); ▪ новое значение в дружественном к пользователю описании (`value`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`); ▪ идентификатор фонда РМ (`deployed_service_uuid`); ▪ новое значение в оригинальном формате (`value_raw`)	«Пользователь `"[username] ([authenticator_name])"` изменил значение политики `"[policy_name]"` для фонда `[deployed_service_name] "[value]"`на `"[value_raw]"`»
Сброс политики РМ `policies.DeployedServicePolicyDeleted`	Регистрируется: ▪ имя пользователя (`username`); ▪ название домена аутентификации пользователя (`authenticator_name`); ▪ название политики (`policy_name`); ▪ название фонда РМ (`deployed_service_name`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`); ▪ идентификатор фонда РМ (`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`); ▪ название политики (`policy_name`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`)	«Пользователь `"[username] ([authenticator_name])"` сбросил значение глобальной политики `"[policy_name]"`»
События, связанные с пользователем		
Подключение пользователя к РМ `workplace.UserConnected`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя фонда РМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`); ▪ протокол доставки (`transport`)	«Подключение к рабочему месту `[vm_name]([vm_ip])` пула служб `[workplace]` пользователя `"[username] ([authenticator])"` было выполнено с использованием протокола `[transport]`»
Отключение пользователя от РМ `workplace.UserDisconnected`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя фонда РМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`); ▪ протокол доставки (`transport`)	«Подключение к рабочему месту `[vm_name]([vm_ip])` пула служб `[workplace]` пользователя `"[username] ([authenticator])"` через протокол `[transport]` разорвано»
Вход пользователя в ОС РМ `workplace.UserLogin`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя гостевой ОС (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда РМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь `"[username] ([authenticator])"` вошел в ОС РМ `[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 гостевой ОС (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда РМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь `"[username] ([authenticator])"` вышел из гостевой ОС РМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]` с IP-адреса `[ip]`»

Блокировка РМ `workplace.UserLock`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя гостевой ОС (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда РМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username]` (`[authenticator]`)" заблокировал гостевую ОС РМ `[vm_name]` (`[vm_ip]`) фонда `[workplace]` как пользователь `[guest_os_username]` с IP-адреса `[ip]`»
Разблокировка РМ `workplace.UserUnlock`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя гостевой ОС (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда РМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username]` (`[authenticator]`)" разблокировал гостевую ОС РМ `[vm_name]` (`[vm_ip]`) фонда `[workplace]` как пользователь `[guest_os_username]` с IP-адреса `[ip]`»
Пользователь неактивен `workplace.UserIdle`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя гостевой ОС (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда РМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username]` (`[authenticator]`)" не активен в гостевой ОС РМ `[vm_name]` (`[vm_ip]`) фонда `[workplace]` как пользователь `[guest_os_username]` с IP-адреса `[ip]`»
Пользователь активен `workplace.UserActive`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя гостевой ОС (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда РМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username]` (`[authenticator]`)" снова активен в гостевой ОС РМ `[vm_name]` (`[vm_ip]`) фонда `[workplace]` как пользователь `[guest_os_username]` с IP-адреса `[ip]`»
Подключение пользователя к РМ и начало работы `user.WorkplaceConnectionRequest`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ название фонда РМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ название протокола доставки (`transport`)	«Пользователь "`[username]` (`[authenticator]`)" подключился к РМ`[vm_name]` фонда `[workplace]` по протоколу `[transport]` с IP- адреса `[ip]`»

Отправка сообщения в РМ `user.WorkplaceMessageSent`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ имя пользователя (`username`); ▪ название фонда РМ (`deployed_service_name`); ▪ название РМ (`user_service_name`); ▪ уровень сообщения (`msg_level`); ▪ текст сообщения (`msg_text`)	«Пользователь `[username]` (`[authenticator]`) отправил сообщение "`[msg_text]`" уровеня `[msg_level]` на РМ `[user_service_name]` фонда `[deployed_service_name]`»
Назначение пользователя на РМ `workplace.UserAssigned`	Регистрируется: ▪ логин пользователя (`username`); ▪ назначенный пользователь (`assigned_to`); ▪ кем назначен пользователь (`assigned_by`)	«Пользователю "`[username]`" назначено рабочее место "`[assigned_to]`" пользователем "`[assigned_by]`"»
Действие с учетными записями на сервере каталогов `tasks.AudiDeregistrationAction`	Регистрируется: ▪ имя учетной записи (`comp_name`); ▪ действие (`action_deregistration`)	«Выполнено действие "`[action_deregistration]`" с учётной записью компьютера `[comp_name]` на сервере каталогов»
События, связанные с веб-интерфейсом		
Неудачная попытка регистрации пользователя `web.UserLoginForbidden`	Регистрируется: ▪ API метод (`handler_path`); ▪ ошибка (`error`); ▪ IP-адрес, с которого был сделан запрос (`ip`)	«Выполнена неудачная попытка регистрации пользователя api - `[handler_path]` ошибка - `[error]` ip - `[ip]`»
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`); ▪ тип портала (`portal`); ▪ идентификатор портала (`portal_uuid`)	«Пользователь "`[username]` (`[authenticator]`)" вошел в систему с ip-адреса `[ip]`через `[portal]` (`[portal_uuid]`)»
Выход пользователя из веб-интерфейса `web.UserLogout`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ тип портала (`portal`); ▪ идентификатор портала (`portal_uuid`)	«Пользователь "`[username]` (`[authenticator]`)" вышел из системы (ip-адрес `[ip]`) через `[portal]` (`[portal_uuid]`)»
Изменение системных параметров «Универсального диспетчера» `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]`)»
Обновление лицензии `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]"` подал 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]"` подал запрос на сброс сессии `[userservice]`»
Попытка повышения прав `web.AdminAssigned`	Регистрируется: ▪ логин пользователя (`assigned_to`); ▪ пользователь, которому назначаются права (`user1`); ▪ название домена аутентификации пользователя (`authenticator`)	«Пользователь `"[user]"` попытался установить тип учетной записи "Администратор" для пользователя `"[assigned_to]"` в домене аутентификации `"[authenticator]"`»
Пользователь обновил данные сущности `web.EntityActionUpdate`	Регистрируется: ▪ логин пользователя (`user`); ▪ название домена аутентификации пользователя (`authenticator`); ▪ обновленные данные (`data`); ▪ объект (`entity`); ▪ идентификатор объекта (`uuid`); ▪ тип объекта (`subtype`); ▪ имя объекта (`name`); ▪ IP-адрес, с которого был сделан запрос (`ip`)	«Пользователь `"[username] ([authenticator])"` `[data]` для объекта `[entity] ([uuid]) [subtype] "[name]"` '(ip-адрес `[ip]`) »

Изменение правил балансировки web.LoadRules	Регистрируется: ▪ логин пользователя (user); ▪ название домена аутентификации пользователя (authenticator); ▪ правило (field); ▪ объект (entity); ▪ идентификатор объекта (uuid); ▪ тип объекта (subtype); ▪ имя объекта (name); ▪ IP-адрес, с которого был сделан запрос (ip); ▪ старое значение параметра (old_value); ▪ новое значение параметра (new_value)	«Пользователь "[username] ([authenticator])" изменил правило [field] для объекта '[entity] ([uuid]) [subtype] "[name]" (ip-адрес [ip]) . Старое значение: [old_value]. Новое значение: [new_value]»
Операция с публикациями фонда web.AuditPublication	Регистрируется: ▪ действие публикации (action_pub); ▪ фонд (pool)	«[action_pub] публикация фонда [pool]»
Операция с состоянием ВМ web.AuditMachineState	Регистрируется: ▪ имя ВМ (name_vm); ▪ новый статус ВМ (action_machine)	«Запрос на изменение статуса ВМ - [name_vm] статус - "[action_machine]"»
События, связанные с API		
Действия пользователя с API api.ApiViewAction	Регистрируется: ▪ название домена аутентификации пользователя (authenticator); ▪ логин пользователя (username); ▪ IP-адрес, с которого был сделан запрос (ip); ▪ запрос(action); ▪ URL-команда (request_path); ▪ код ответа (response_status)	«Пользователь "[username] ([authenticator])" выполнил запрос [action] для api [request_path] (статус код ответа - [response_status]) (ip-адрес [ip])»
Неудачная попытка создать сессию API api.ApiUserLoginForbidden	Регистрируется: ▪ метод (handler_path); ▪ ошибка (error); ▪ IP-адрес, с которого был сделан запрос (ip)	«Выполнена неудачная попытка регистрации пользователя api - [handler_path] ошибка - [error] ip - [ip]»
Вход пользователя в систему через API api.UserLogin	Регистрируется: ▪ название домена аутентификации пользователя (authenticator); ▪ логин пользователя (username); ▪ IP-адрес, с которого был сделан запрос (ip); ▪ тип портала (portal); ▪ идентификатор портала (portal_uuid) ; ▪ тип учетной записи пользователя (user_type)	«Пользователь "[username] ([authenticator])" с типом учетной записи [user_type] вошел в систему с IP-адресом [ip]через [portal] ([portal_uuid])»
Выход пользователя из системы через API api.UserLogout	Регистрируется: ▪ название домена аутентификации пользователя (authenticator); ▪ логин пользователя (username); ▪ IP-адрес, с которого был сделан запрос (ip); ▪ тип портала (portal); ▪ идентификатор портала (portal_uuid) ; ▪ тип учетной записи пользователя (user_type)	«Пользователь "[username] ([authenticator])" с типом учетной записи [user_type] и IP-адресом [ip] вышел из системы через [portal] ([portal_uuid])»

События, связанные с пользовательскими сессиями		
Старт сессии пользователя `session.SessionStarted`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ GUSID (`suid`)	«Сессии пользователя "`[username]` (`[authenticator]`)" назначен GUSID "`[suid]`"»
Окончание сессии пользователя `session.SessionEnded`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ GUSID (`suid`)	«Сессия пользователя "`[username]` (`[authenticator]`)" с GUSID "`[suid]`" завершена по запросу»
Сессия пользователя завершена по сроку действия `session.SessionExpired`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ GUSID (`suid`)	«Сессия пользователя "`[username]` (`[authenticator]`)" с GUSID "`[suid]`" завершена по сроку действия»
События, связанные с поставщиком ресурсов		
Изменение конфигурации на стороне поставщика ресурсов `provider.ChangeConfiguration`	Регистрируется: ▪ имя поставщика ресурсов (); ▪ параметр (`changed_field`)	«Была изменена конфигурация "`[provider]`". Был удален `[changed_field]`»
Создание ВМ на стороне поставщика ресурсов `provider.SuccessCreateVM`	Регистрируется: ▪ имя ВМ (`vm_name`)	«Успешно создалась виртуальная машина `[vm_name]`»
Удаление ВМ на стороне поставщика ресурсов `provider.SuccessRemoveVM`	Регистрируется: ▪ имя ВМ (`vm_name`)	«Успешно удалена виртуальная машина `[vm_name]`»

15.6.3 . Форматы регистрируемых событий аудита и их примеры

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

Пример регистрации события аудита «Пользователь обновил данные сущности»:

Дата	Событие	Текст события
06.06.2025, 12:35:24	termidesk.audit.events.workplace.EntityActionUpdate	«Пользователь "admin123(Встроенный)" обновил данные - "{'tunnelWait': {'старое_значение': 30, 'новое_значение': 29}}" для объекта Transport (ce5ecd63-041f-5d5e-99c9-9de93a7a663d) TERATransport "TERA" "(ip-адрес 10.10.100.11)" (уровень - высокий)»

Termidesk также поддерживает запись каждого события аудита в формате CEF (см. подраздел **Системные параметры аудита**):

`[Дата и время]|[Узел]|[CEF:версия]|[Uveon]|[Termidesk]|[Версия Termidesk]|[Идентификатор события]|[Наименование события]|[Уровень важности]|[Объекты события]`

Пример события «Пользователь обновил данные сущности» в формате CEF:

```
2025-06-06T12:35:24.367115 localhost CEF:0|Uveon|Termidesk|6.0-rc4|api/webui/
draft/transports/:PUT|Пользователь обновил данные сущности|6|suser=admin123
authenticator=Встроенный username=admin123 ip=10.10.100.11 entity=Transport
uuid=ce5ecd63-041f-5d5e-99c9-9de93a7a663d subtype=TERATransport name=TERA
action=update updatedata={'tunnelWait': {'старое_значение': 30, 'новое_значение':
 29}} level=высокий
```

Для отображения событий аудита в веб-портале происходит их конвертация в удобочитаемый формат, указанный в примерах выше.

15.7 . Отслеживание жизненного цикла сессий и ресурсов пользователей

Начиная с Termidesk версии 5.0 поддерживается возможность отследить действия пользователя (или администратора) по идентификаторам, которыми маркируются все события, относящихся к работе с Termidesk с момента аутентификации и до завершения работы:

- глобальный уникальный сессионный идентификатор (Global Unique Session ID, GUSID, также SUID) - позволяет однозначно сопоставить субъект (пользователя или администратора) и производимые им действия. Присваивается в момент аутентификации в Termidesk;
- уникальный идентификатор запуска ресурса (Unique Resource Start ID, URSI) - позволяет однозначно сопоставить пользователя и конкретный ресурс, который он получает - PM и/или приложение. Присваивается в момент запуска пользователем ресурса.

Последовательность присвоения и отправки идентификаторов представлена на рисунке.

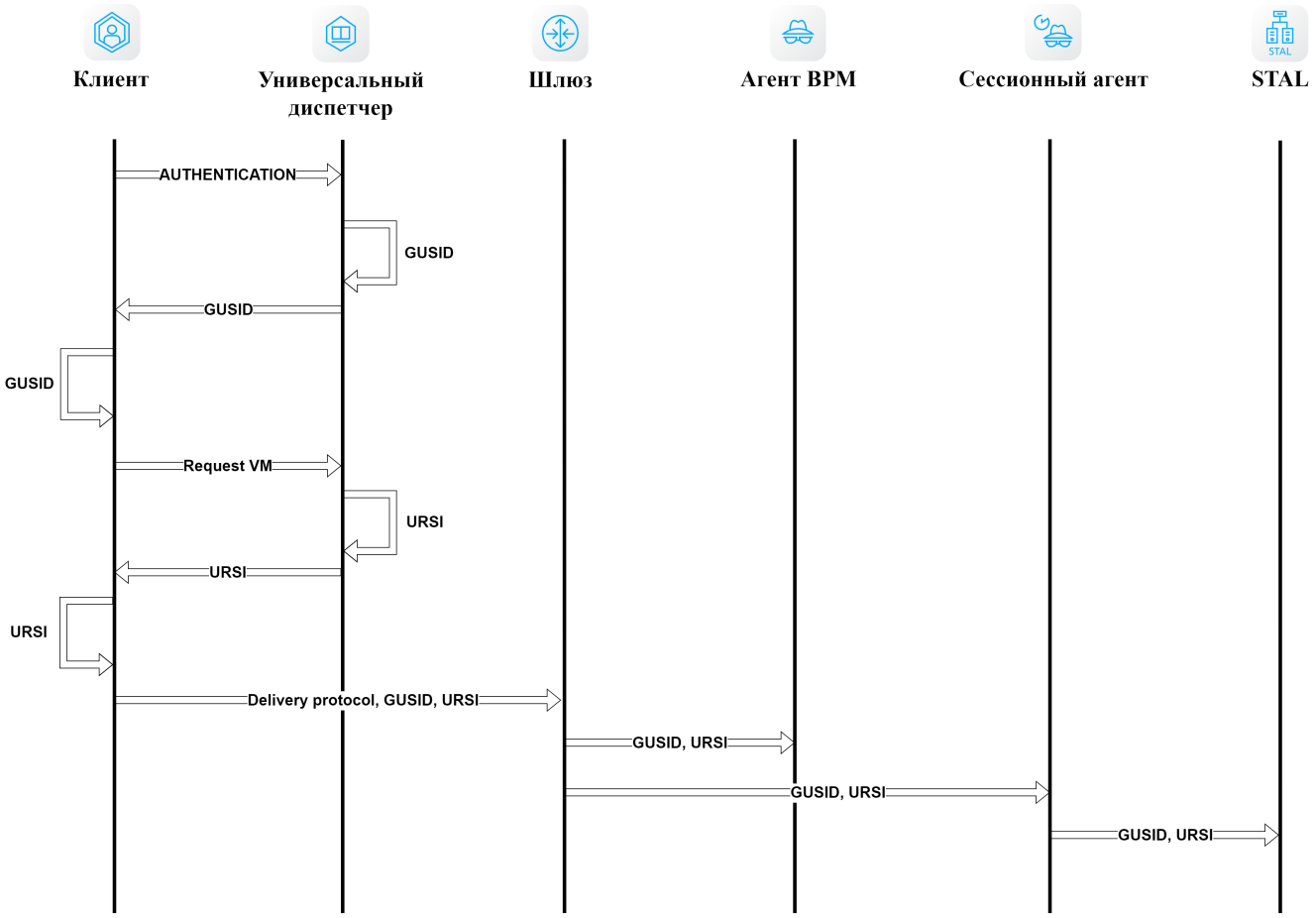

Рисунок 79 – Последовательность присвоения и отправки GUSID и URSI

Аннулирование GUSID происходит при:

- завершении сессии по истечении времени, заданного параметром «Длительность сессии пользователя» или «Длительность сессии администратора» (см. подраздел **Параметры безопасности Termidesk**);
- отключении от «Универсального диспетчера»;
- закрытии компонента «Клиент» пользователем;
- запуске нового экземпляра компонента «Клиент» на той же пользовательской рабочей станции;
- невозможности восстановления подключения после обрыва связи - GUSID и URSI будут считаться недействительными и при следующем подключении к «Универсальному диспетчеру» будут назначены новые идентификаторы.

Аннулирование URSI происходит при:

- закрытии пользователем окна опубликованного приложения или выходе из сеанса PM (`logoff`);
- отключении от сеанса PM (`disconnect`);
- закрытии компонента «Клиент» и окна программы доставки PM (`termidesk-viewer`);

- невозможности восстановления подключения после обрыва связи - GUSID и URSI будут считаться недействительными и при следующем подключении пользователя к «Универсальному диспетчеру» будут назначены новые идентификаторы

GUSID и URSI регистрируются в журналах:

- компонента «Сессионный агент»;
- компонента «Агент виртуального рабочего места».

События, связанные с GUSID и URSI, хранятся в БД. Они доступны для просмотра в журнале на портале Termidesk (см. подраздел **Просмотр журналов**). Пример сообщения от источника «agent»: «preConnect. User: u, Protocol: spice, GUSID: 93418bcd-5c95-5f46-ae1b-980a8519ae8f, URSI: 73fe89e3-5fe4-5b02-81a8-06b8e3bac2d1».

16 . УПРАВЛЕНИЕ ИНФРАСТРУКТУРОЙ TERMIDESK

16.1 . Общие сведения об инфраструктуре Termidesk

Раздел «Инфраструктура» предназначен для использования в качестве единого центра управления при распределенной установке Termidesk. Он позволяет централизованно управлять компонентами и просматривать их статус на сервере.

Просмотр компонентов и их состояния также доступен в разделе «Обзор» (см. Рисунок 80), наименования элементов в котором служат активной ссылкой на соответствующий подраздел веб-интерфейса.

Состояние компонента визуализируется пиктограммой:

-  - количество узлов, находящихся в статусе «ok», которое вернул запрос `healthcheck`;
-  - количество узлов, находящихся в статусе «maintance» (техобслуживание), которое вернул запрос `healthcheck`;
-  - количество узлов, находящихся в статусе «error» (ошибка), которое вернул запрос `healthcheck`;
-  - количество узлов, находящихся в статусе «unknown» (неизвестно). Статус появляется, если после регистрации компонента еще не было ни одной попытки запроса состояния `healthcheck`.

По умолчанию запрос состояния компонентов производится с интервалом 60 секунд.

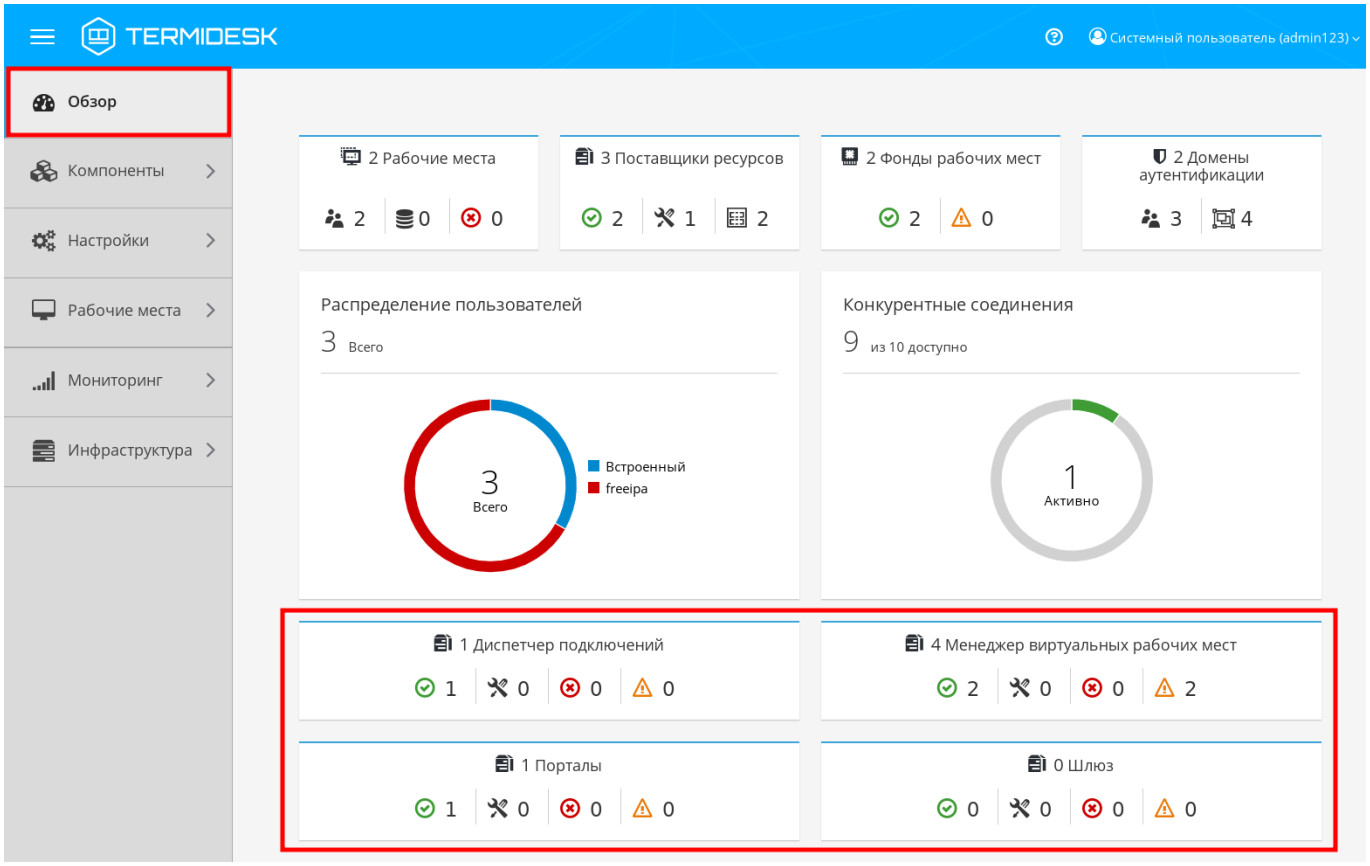

Рисунок 80 – Отображение компонентов в разделе «Обзор»

Регистрация компонента Termidesk в системе происходит через подключение к серверу RabbitMQ, передающему информацию об узле компоненту «Менеджер рабочих мест» для обработки и добавления в таблицу раздела «Инфраструктура». Регистрация компонентов происходит при их запуске (или при перезапуске их служб).

16.2 . Управление списком узлов компонента «Универсальный диспетчер»

Для получения списка зарегистрированных узлов компонента «Универсальный диспетчер» нужно перейти «Инфраструктура - Диспетчеры подключений».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя». Для удаления узла компонента из таблицы следует выбрать нужный объект и нажать экранную кнопку **[Удалить]**.

Удаление объекта из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова.

Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».
Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

Основные регистрируемые параметры узлов приведены в таблице (см. Таблица 112).

Таблица 112 – Основные параметры списка узлов компонента «Универсальный диспетчер»

Параметр	Описание
«Имя»	Наименование объекта
«Статус»	Текущее состояние, может принимать значения: ▪ «ok» - объект нормально функционирует; ▪ «failed» - объект функционирует с ошибками; ▪ «unknown» - состояние неизвестно или не поддерживается
«Полное доменное имя»	⚠ Необходимо обеспечить корректную передачу полного доменного имени (FQDN) узла в Termidesk. Для этого: ▪ убедиться, что на всех узлах инфраструктуры в файле `/etc/hosts` заданы FQDN; ▪ обеспечить разрешение имен узлов: • убедиться, что в сетевой инфраструктуре развернуты и исправно функционируют службы доменных имен (DNS); • убедиться, что задана корректная настройка файла `/etc/resolv.conf` на каждом узле. Полное доменное имя узла объекта
«IP адрес(а)»	Список IP-адресов на узле объекта
«Изменено кем»	Наименование субъекта, который внес последние изменения
«Сертификат»	Статус сертификата объекта. Может быть: ▪ «Истёк» - статус красного цвета, отображается при истечении срока действия сертификата; ▪ «Скоро истекает» - статус оранжевого цвета, отображается, если до окончания действия сертификата осталось менее 30 дней; ▪ «Переходное состояние» - статус серого цвета, отображается при любом переходном состоянии (например, если ожидается ответ от ЦС); ▪ «Ок» - статус зеленого цвета, отображается при отсутствии проблем с сертификатом. Для просмотра сертификата конкретного объекта используется экранная кнопка **[Сертификат]**. Сертификаты считываются из хранилища, используемого фермой Termidesk. Список сертификатов, отображаемый для объекта, приведен в таблице ниже ⚠ Просмотр сертификата будет доступен, если: ▪ узлы фермы Termidesk используют способ хранения конфигурации «hvac» (выбирается на этапе установки Termidesk); ▪ у оператора есть разрешение «Просмотр сертификатов». Узлы фермы Termidesk должны использовать единое хранилище конфигурации.
«Дата изменения»	Дата внесения последних изменений
«Создано кем»	Наименование субъекта, который создал объект
«Дата создания»	Дата создания записи в таблице об объекте

Параметр	Описание
«UUID ноды»	Системный UUID узла объекта
«Уникальный номер»	Уникальный идентификатор объекта

Для объекта «Универсальный диспетчер» доступен список сертификатов, приведенный в таблице (см. Таблица 113).

Таблица 113 – Список сертификатов «Универсального диспетчера»

Параметр	Описание
«Корневой сертификат БД»	Путь к корневому сертификату mTLS для защищенного подключения к БД
«Сертификат БД»	Путь к клиентскому сертификату mTLS для защищенного подключения к БД
«Закрытый ключ БД»	Путь к закрытому ключу mTLS для защищенного подключения к БД
«Сертификат сервера Удаленного помощника»	Путь к серверному сертификату SSL/TLS для проверки подключения к «Удаленному помощнику»
«Осн. серт. для расшифровки JWT-токена»	Путь к основному сертификату для получения значения JWT-токена «Агрегатора»
«Рез. серт. для расшифровки JWT-токена»	Путь к резервному сертификату для получения значения JWT-токена «Агрегатора»

16.3 . Управление списком узлов компонента «Менеджер рабочих мест»

Для получения списка зарегистрированных узлов компонента «Менеджер рабочих мест» нужно перейти «Инфраструктура - Менеджеры BPM».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя». Для удаления узла компонента из таблицы следует выбрать нужный объект и нажать экранную кнопку **[Удалить]**.

Удаление объекта из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова.

Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».
Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

Основные регистрируемые параметры узлов приведены в таблице (см. Таблица 114).

Таблица 114 – Основные параметры списка узлов компонента «Менеджер рабочих мест»

Параметр	Описание
«Имя»	Наименование объекта

Параметр	Описание
«Статус»	Текущее состояние, может принимать значения: ▪ «ok» - объект нормально функционирует; ▪ «failed» - объект функционирует с ошибками; ▪ «unknown» - состояние неизвестно или не поддерживается
«Полное доменное имя»	Необходимо обеспечить корректную передачу полного доменного имени (FQDN) узла в Termidesk. Для этого: ▪ убедиться, что на всех узлах инфраструктуры в файле `/etc/hosts` заданы FQDN; ▪ обеспечить разрешение имен узлов: • убедиться, что в сетевой инфраструктуре развернуты и исправно функционируют службы доменных имен (DNS); • убедиться, что задана корректная настройка файла `/etc/resolv.conf` на каждом узле. Полное доменное имя узла объекта
«IP адрес(а)»	Список IP-адресов на узле объекта
«Изменено кем»	Наименование субъекта, который внес последние изменения
«Сертификат»	Статус сертификата объекта. Может быть: ▪ «Истёк» - статус красного цвета, отображается при истечении срока действия сертификата; ▪ «Скоро истекает» - статус оранжевого цвета, отображается, если до окончания действия сертификата осталось менее 30 дней; ▪ «Переходное состояние» - статус серого цвета, отображается при любом переходном состоянии (например, если ожидается ответ от ЦС); ▪ «Ок» - статус зеленого цвета, отображается при отсутствии проблем с сертификатом. Для просмотра сертификата конкретного объекта используется экранная кнопка **[Сертификат]**. Сертификаты считываются из хранилища, используемого фермой Termidesk. Список сертификатов, отображаемый для объекта, приведен в таблице ниже Просмотр сертификата будет доступен, если: ▪ узлы фермы Termidesk используют способ хранения конфигурации «hvac» (выбирается на этапе установки Termidesk); ▪ у оператора есть разрешение «Просмотр сертификатов». Узлы фермы Termidesk должны использовать единое хранилище конфигурации.
«Дата изменения»	Дата внесения последних изменений
«Создано кем»	Наименование субъекта, который создал объект
«Дата создания»	Дата создания записи в таблице об объекте
«UUID ноды»	Системный UUID узла объекта
«Уникальный номер»	Уникальный идентификатор объекта

Для объекта «Менеджер рабочих мест» доступен список сертификатов, приведенный в таблице (см. Таблица 115).

Таблица 115 – Список сертификатов «Менеджера рабочих мест»

Параметр	Описание
«Сертификат Celery Health Check»	Путь к сертификату SSL/TLS для защищенного подключения к API проверки состояния служб «Менеджера рабочих мест»
«Закрытый ключ Celery Health Check»	Путь к закрытому ключу SSL/TLS для защищенного подключения к API проверки состояния служб «Менеджера рабочих мест»
«Закрытый ключ Celery Beat»	Путь к закрытому ключу mTLS для защищенного подключения к RabbitMQ
«Сертификат Celery Beat»	Путь к клиентскому сертификату mTLS для защищенного подключения к RabbitMQ
«Корневой сертификат Celery Beat»	Путь к корневому сертификату mTLS для защищенного подключения к RabbitMQ

16.4 . Управление списком узлов с ролями «Порталов»

Для получения списка зарегистрированных узлов с ролями «Порталов» нужно перейти «Инфраструктура - Порталы».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя». Для удаления узла компонента из таблицы следует выбрать нужный объект и нажать экранную кнопку **[Удалить]**.

Удаление объекта из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова.

Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».
Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

Основные регистрируемые параметры узлов приведены в таблице (см. Таблица 116).

Таблица 116 – Основные параметры списка узлов с ролями «Порталов»

Параметр	Описание
«Имя»	Наименование объекта
«Роль»	Тип портала, с которым установлен компонент «Универсальный диспетчер». Может быть: «admin» («Портал администратора»), «user» («Портал пользователя»), «universal» («Портал универсальный»)
«Статус»	Текущее состояние, может принимать значения: ▪ «ok» - объект нормально функционирует; ▪ «failed» - объект функционирует с ошибками; ▪ «unknown» - состояние неизвестно или не поддерживается

Параметр	Описание
«Полное доменное имя»	⚠ Необходимо обеспечить корректную передачу полного доменного имени (FQDN) узла в Termidesk. Для этого: ▪ убедиться, что на всех узлах инфраструктуры в файле `/etc/hosts` заданы FQDN; ▪ обеспечить разрешение имен узлов: • убедиться, что в сетевой инфраструктуре развернуты и исправно функционируют службы доменных имен (DNS); • убедиться, что задана корректная настройка файла `/etc/resolv.conf` на каждом узле. Полное доменное имя узла объекта
«IP адрес(а)»	Список IP-адресов на узле объекта
«Изменено кем»	Наименование субъекта, который внес последние изменения
«Дата изменения»	Дата внесения последних изменений
«Создано кем»	Наименование субъекта, который создал объект
«Дата создания»	Дата создания записи в таблице об объекте
«UID ноды»	Системный UUID узла объекта
«Уникальный номер»	Уникальный идентификатор объекта

16.5 . Управление списком узлов компонента «Шлюз»

Для получения списка зарегистрированных узлов компонента «Шлюз» нужно перейти «Инфраструктура - Шлюзы».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя». Для удаления узла компонента из таблицы следует выбрать нужный объект и нажать экранную кнопку **[Удалить]**.

Удаление объекта из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова.

⚠ Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».
Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

Основные регистрируемые параметры узлов приведены в таблице (см. Таблица 117).

Таблица 117 – Основные параметры списка узлов компонента «Шлюз»

Параметр	Описание
«Имя»	Наименование объекта

Параметр	Описание
«Статус»	Текущее состояние, может принимать значения: ▪ «ok» - объект нормально функционирует; ▪ «failed» - объект функционирует с ошибками; ▪ «unknown» - состояние неизвестно или не поддерживается
«Полное доменное имя»	Необходимо обеспечить корректную передачу полного доменного имени (FQDN) узла в Termidesk. Для этого: ▪ убедиться, что на всех узлах инфраструктуры в файле `/etc/hosts` заданы FQDN; ▪ обеспечить разрешение имен узлов: • убедиться, что в сетевой инфраструктуре развернуты и исправно функционируют службы доменных имен (DNS); • убедиться, что задана корректная настройка файла `/etc/resolv.conf` на каждом узле. Полное доменное имя узла объекта
«IP адрес(а)»	Список IP-адресов на узле объекта
«Изменено кем»	Наименование субъекта, который внес последние изменения
«Сертификат»	Статус сертификата объекта. Может быть: ▪ «Истёк» - статус красного цвета, отображается при истечении срока действия сертификата; ▪ «Скоро истекает» - статус оранжевого цвета, отображается, если до окончания действия сертификата осталось менее 30 дней; ▪ «Переходное состояние» - статус серого цвета, отображается при любом переходном состоянии (например, если ожидается ответ от ЦС); ▪ «Ок» - статус зеленого цвета, отображается при отсутствии проблем с сертификатом. Для просмотра сертификата конкретного объекта используется экранная кнопка **[Сертификат]**. Сертификаты считываются из хранилища, используемого фермой Termidesk. Список сертификатов, отображаемый для объекта, приведен в таблице ниже Просмотр сертификата будет доступен, если: ▪ узлы фермы Termidesk используют способ хранения конфигурации «hvac» (выбирается на этапе установки Termidesk); ▪ у оператора есть разрешение «Просмотр сертификатов». Узлы фермы Termidesk должны использовать единое хранилище конфигурации.
«Дата изменения»	Дата внесения последних изменений
«Создано кем»	Наименование субъекта, который создал объект
«Дата создания»	Дата создания записи в таблице об объекте
«UUID ноды»	Системный UUID узла объекта
«Уникальный номер»	Уникальный идентификатор объекта

Для объекта «Шлюз» доступен список сертификатов, приведенный в таблице (см. Таблица 118).

Таблица 118 – Список сертификатов «Шлюза»

Параметр	Описание
«Сертификат шлюза»	Путь к сертификату «Шлюза»
«Закрытый ключ шлюза»	Путь к закрытому ключу «Шлюза»

16.6 . Управление «Ретрансляторами»

16.6.1 . Добавление «Ретранслятора»

«Ретранслятор» - узел с установленным ПО Fluentd, предназначенный для сбора и фильтрации записей журналов, поступающих от компонентов Termidesk, и их перенаправления в централизованное хранилище журналов или БД.

Для отображения списка «Ретрансляторов» следует перейти «Инфраструктура - Ретрансляторы». По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 119).

Таблица 119 – Основные параметры списка «Ретрансляторов»

Параметр	Описание
«Имя»	Наименование объекта
«Статус»	Текущее состояние объекта, может принимать значения: ▪ «ok» - объект нормально функционирует; ▪ «failed» - объект функционирует с ошибками; ▪ «unknown» - состояние неизвестно или не поддерживается
«Используется»	Флаг использования объекта. Возможные значения: ▪ «Да» - «Ретранслятор» используется для сбора журналов; ▪ «Нет» - «Ретранслятор» не используется для сбора журналов
«Полное доменное имя»	⚠ Необходимо обеспечить корректную передачу полного доменного имени (FQDN) узла в Termidesk. Для этого: ▪ убедиться, что на всех узлах инфраструктуры в файле `/etc/hosts` заданы FQDN; ▪ обеспечить разрешение имен узлов: • убедиться, что в сетевой инфраструктуре развернуты и исправно функционируют службы доменных имен (DNS); • убедиться, что задана корректная настройка файла `/etc/resolv.conf` на каждом узле. Полное доменное имя узла, на котором функционирует «Ретранслятор»
«IP-адрес(а)»	Список IP-адресов на узле, на котором функционирует «Ретранслятор»
«Изменено кем»	Наименование субъекта, который внес последние изменения
«Дата изменения»	Дата внесения последних изменений
«Создано кем»	Наименование субъекта, который создал объект
«Дата создания»	Дата создания записи в таблице об объекте

Параметр	Описание
«UUID ноды»	Системный UUID узла, на котором функционирует «Ретранслятор» Параметр имеет постоянное значение: «00000000-0000-0000-0000-000000000000»
«Уникальный номер»	Уникальный идентификатор объекта

Для добавления «Ретранслятора» нужно перейти «Инфраструктура - Ретрансляторы» и нажать экранную кнопку **[Создать]**. Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 120).

Рекомендуется добавлять только один узел «Ретранслятора».
В отличие от компонентов Termidesk, которые регистрируются в разделе «Инфраструктура» автоматически, «Ретранслятор» добавляется вручную.

Таблица 120 – Данные для добавления узла «Ретранслятора»

Параметр	Описание
«Название»	Текстовое наименование «Ретранслятора»
«IP адрес»	IP-адрес «Ретранслятора»
«Порт»	Порт, который будет использоваться при подключении к «Ретранслятору». Значение по умолчанию: «24224»
«Альтернативный порт»	Дополнительный порт, который будет использоваться при подключении к «Ретранслятору». Значение по умолчанию: «9880»
«Включено»	Управление использованием «Ретранслятора». Возможные значения: ▪ «Да» - использовать «Ретранслятор» для сбора журналов; ▪ «Нет» - не использовать «Ретранслятор» для сбора журналов. Параметр предназначен для прекращения взаимодействия компонентов Termidesk с узлом «Ретранслятора», который по каким-либо причинам выведен из стандартного рабочего состояния

Над созданными «Ретрансляторами» можно выполнять следующие действия:

- редактировать, для этого следует выбрать нужный объект в таблице, а затем нажать экранную кнопку **[Изменить]**;
- удалить, для этого следует выбрать нужный объект в таблице, а затем нажать экранную кнопку **[Удалить]**;
- управлять состоянием, для этого следует выбрать нужный объект в таблице, нажать экранную кнопку **[Использование]** и в раскрывающемся списке выбрать состояние «Ретранслятора»:
  - «Использовать»;
  - «Не использовать».

⚠ Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».
Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

16.6.2 . Настройка узла «Ретранслятора» с ПО Fluentd

Для централизованного сбора событий в «Хранилище журналов» необходимо настроить отдельный узел с установленным ПО Fluentd и СУБД PostgreSQL, выступающей в качестве «Хранилища журналов» (в общем случае данные компоненты могут устанавливаться на отдельный узел, но в рамках настоящей процедуры этот вариант не рассматривается). Для этого на узле «Ретранслятора» нужно создать и настроить БД «Хранилища журналов»:

- переключиться на пользователя `postgres`:

```
sudo su postgres
```

- запустить терминальный клиент СУБД PostgreSQL:

```
psql
```

ⓘ Если после выполнения команды отображается ошибка «could not change directory to "/home/": Отказано в доступе» и не появляется приглашение командной строки `postgres=#`, необходимо вместо «`su postgres`» использовать конструкцию «`su - postgres`». Если приглашение `postgres=#` появилось, то сообщение об ошибке можно проигнорировать.

- используя интерактивный интерфейс терминального клиента СУБД, создать БД `fluentd_logs_db` (символ ; в конце строки при работе с интерактивным интерфейсом обязателен):

```
postgres=# CREATE DATABASE fluentd_logs_db;
```

- создать пользователя `fluentd` с паролем `tufotukur` для дальнейшего подключения к БД:

```
postgres=# CREATE USER fluentd WITH PASSWORD 'tufotukur';
```

⚠ В приведенной команде имя пользователя и пароль используются в качестве примера. Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты. Для задания пароля разрешено использовать только латинские буквы A-Z, a-z, цифры 0-9 и символы $!@%^&#_-=+~`;:.,?()*{}[]\/.

- назначить права по использованию БД `fluentd_logs_db` созданному пользователю `fluentd`:

```
postgres=# GRANT ALL PRIVILEGES ON DATABASE fluentd_logs_db TO fluentd;
```

- подключиться к БД `fluentd_logs_db`:

```
postgres=# \c fluentd_logs_db
```

- создать таблицу `logs`:

При использовании СУБД PostgreSQL версии выше 11 могут понадобиться дополнительные права для схемы `public`. Для предоставления прав нужно выполнить:

```
postgres=# GRANT CREATE ON SCHEMA public TO fluentd;
postgres=# GRANT USAGE, SELECT ON ALL SEQUENCES IN SCHEMA public TO fluentd;
```

Если таблица была ранее создана для Termidesk версии младше 6.0, то ее следует изменить:

```
postgres=# ALTER TABLE "logs" ADD COLUMN "fqdn" varchar(255) NULL;
postgres=# COMMIT;
```

```
fluentd_logs_db=# CREATE TABLE logs (
    id SERIAL PRIMARY KEY,
    time timestamp with time zone NOT NULL,
    source VARCHAR(255) NOT NULL,
    fqdn VARCHAR(255),
    sourceType VARCHAR(255) NOT NULL,
    loglevel VARCHAR(255) NOT NULL,
    module VARCHAR(255) NOT NULL,
    message TEXT NOT NULL
);
```

- назначить права по использованию таблицы пользователю `fluentd`:

```
fluentd_logs_db=# GRANT ALL PRIVILEGES ON TABLE logs TO fluentd;
```

- выйти из интерактивного интерфейса терминального клиента СУБД:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

После создания БД нужно создать и настроить «Ретранслятор»:

- установить ПО Fluentd на узел «Ретранслятора» согласно документации https://docs.fluentd.org/;

- установить плагины fluent-plugin-sql и pg, доступ по ссылке https://github.com/fluent/fluent-plugin-sql ;
- отредактировать файл `/etc/fluent/fluentd.conf`:

⚠ 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 организации.
Если файл `/etc/fluent/fluentd.conf` был ранее создан для Termidesk версии младше 6.0, то его следует изменить в части `column_mapping`:

```
column_mapping "time:time,source:source,fqdn:fqdn,sourceType:sourceType,loglevel:loglevel,module:module,message:message"
```

```
<source>
  @type forward
  port 24224
  bind 0.0.0.0
</source>

<system>
  log_level debug
</system>

<match termidesk.*>
  @type sql
  host 192.0.2.33
  port 5433
  database fluentd_logs_db
  adapter postgresql
  username fluentd
  password tufotukur

  <table>
    table logs
    column_mapping "time:time,source:source,fqdn:fqdn,sourceType:sourceType,loglevel:loglevel,module:module,message:message"
  </table>
</match>
```

Перечень параметров, задающихся через файл, приведен в таблице (см. Таблица 121).

Таблица 121 – Параметры конфигурирования файла fluentd.conf

Параметр	Значение по умолчанию	Описание
Секция source		
@type	forward	Параметр менять не рекомендуется

Параметр	Значение по умолчанию	Описание
port	24224	Порт прослушивания входящих событий
bind	0.0.0.0	IP-адрес прослушивания входящих событий
Секция system		
log_level	debug	Категория служебных сообщений для журналирования событий ПО Fluentd. Возможные значения: ▪ debug; ▪ info; ▪ warn; ▪ error
Секция match		
@type	sql	Параметр менять не рекомендуется
host	192.0.2.33	IP-адрес или полное доменное имя БД для сохранения событий
port	5433	Порт подключения к БД для сохранения событий
database	fluentd_logs_db	Наименование БД для сохранения событий
adapter	postgresql	Параметр изменять не рекомендуется
username	fluentd	Имя пользователя БД для подключения к ней
password	tufotukur	Пароль для подключения к БД
Секция table		
logs	не задано	Наименование таблицы БД для сохранения событий
column_mapping	"time:time,source:source,fqdn:fqdn,sourceType:sourceType,loglevel:loglevel,module:module,message:message"	Параметр распределяет значения событий, полученных от фермы Termidesk в поля таблицы «logs»

16.6.3 . Настройка узла «Ретранслятора» с ПО Fluent Bit

Для централизованного сбора событий в «Хранилище журналов» Вместо ПО Fluentd (см. подраздел **Настройка узла «Ретранслятора» с ПО Fluentd**) может использоваться ПО Fluent Bit.

ПО Fluent Bit может быть установлено на узел:

- ОС Linux. Описание установки приведено ниже. После установки нужно выполнить настройку ПО;
- ОС Microsoft Windows. Рекомендуется загрузить последнюю стабильную версию с официального сайта Fluent Bit: https://fluentbit.io/. После установки нужно выполнить настройку ПО.

Для установки ПО Fluent Bit в Linux нужно:

- в файл `/etc/apt/sources.list` добавить репозиторий ПО, например:

```
deb https://packages.fluentbit.io/ubuntu/focal focal main
```

- выполнить обновление списка пакетов:

```
sudo apt update
```

- установить ключ репозитория:

```
sudo wget -qO - https://packages.fluentbit.io/fluentbit.key | sudo apt-key add -
```

- установить пакеты `fluent-bit` и `td-agent-bit`:

```
sudo apt install fluent-bit td-agent-bit
```

- перейти к настройке ПО Fluent Bit.

Для настройки Fluent Bit в Linux нужно:

- добавить поля `[INPUT]` и `[OUTPUT]` в конфигурационный файл `/etc/fluent-bit/fluent-bit.conf`. Пример:

> ⚠ Секция `[INPUT]` определяет настройки для получения входящих событий, `[OUTPUT]` определяет настройки для сохранения полученных событий.
> 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 организации.

```
[INPUT]
    Name              forward
    Listen            0.0.0.0
    Port              24224
    Buffer_Chunk_Size 1M
    Buffer_Max_Size   6M

[OUTPUT]
    Name                pgsql
    Match               *
    Host                192.0.2.3
    Port                5432
    User                UserName
    Password            UserPassword
    Database            fluentbit
    Table               fluentbit_table
    Time_Key            timestamp
    Time_Format         %Y-%m-%d %H:%M:%S
    min_pool_size       1
    max_pool_size       20
```

- перезапустить службу `fluent-bit` для применения настроек:

```
sudo systemctl restart fluent-bit
```

- убедиться, что служба запустилась корректно, выполнив команду:

```
sudo systemctl status fluent-bit
```

Перечень параметров, задающихся через файл `/etc/fluent-bit/fluent-bit.conf`, приведен в таблице (см. Таблица 122).

Таблица 122 – Параметры файла /etc/fluent-bit/fluent-bit.conf

Параметр	Описание
Секция `[INPUT]`	
`Name`	Тип входного плагина. Значение `forward` используется для получения событий от других узлов Fluent Bit
`Listen`	IP-адрес прослушивания входящих событий. Значение `0.0.0.0` позволяет принимать соединения на всех интерфейсах
`Port`	Порт прослушивания входящих событий
`Buffer_Chunk_Size`	Размер буфера для хранения временных меток (chunk). Значение `1M` зарезервировало 1 МБ для хранения данных
`Buffer_Max_Size`	Максимальный размер буфера в случае очереди данных
Секция `[OUTPUT]`	
`Name`	Определение типа выходного плагина. Значение `pgsql` указывает на отправку данных в СУБД PostgreSQL
`Match`	Указывает на записи, обрабатываемые выходным плагином. Значение `*` соответствует всем записям
`Host`	Адрес сервера СУБД PostgreSQL
`Port`	Порт, на котором работает СУБД PostgreSQL
`User`	Имя пользователя для подключения к БД
`Password`	Пароль для пользователя БД
`Database`	Имя БД, в которую будут отправлены события
`Table`	Название таблицы БД, в которую будут записываться события
`Time_Key`	Ключ, под которым будет храниться временная метка. Необязательный параметр
`Time_Format`	Формат временной метки. Необязательный параметр
`min_pool_size`	Минимальный размер пула соединений
`max_pool_size`	Максимальный размер пула соединений

Для настройки Fluent Bit в Microsoft Windows нужно:

⚠ ПО Fluent Bit для ОС Microsoft Windows не поддерживает плагин для работы с СУБД PostgreSQL, настройка выгрузки событий будет производиться в файл.

- отредактировать файл конфигурации `C:\Program Files\fluent-bit\conf\fluent-bit.conf`. Пример:

```
[INPUT]
    Name              forward
    Listen            0.0.0.0
    Port              24224
    Buffer_Chunk_Size 1M
    Buffer_Max_Size   6M

[OUTPUT]
    Name file
    Match *
    File termidesk.log
    Path C:\logFolder\
```

- сохранить изменения и перезапустить службу Fluent Bit, для этого:
  - открыть меню «Пуск» и ввести «services.msc» для доступа к списку служб Windows;
  - найти службу `fluent-bit`, открыть контекстное меню правой кнопкой мыши и нажать экранную кнопку **[Перезапустить]**.

Перечень параметров, задающихся через файл `C:\Program Files\fluent-bit\conf\fluent-bit.conf`, приведен в таблице (см. Таблица 123).

Таблица 123 – Параметры файла C:\Program Files\fluent-bit\conf\fluent-bit.conf

Параметр	Описание
Секция `[INPUT]`	
`Name`	Тип входного плагина. Значение `forward` используется для получения событий от других узлов Fluent Bit
`Listen`	IP-адрес прослушивания входящих событий. Значение `0.0.0.0` позволяет принимать соединения на всех интерфейсах
`Port`	Порт прослушивания входящих событий
`Buffer_Chunk_Size`	Размер буфера для хранения временных меток (chunk). Значение `1M` зарезервировало 1 МБ для хранения данных
`Buffer_Max_Size`	Максимальный размер буфера в случае очереди данных
Секция `[OUTPUT]`	
`Name`	Определение типа выходного плагина. Значение `pgsql` указывает на отправку данных в СУБД PostgreSQL
`Match`	Указывает на записи, обрабатываемые выходным плагином. Значение `*` соответствует всем записям
`File`	Имя файла, в который будут записываться события

Параметр	Описание
Path	Путь к файлу

16.7 . Управление «Хранилищами журналов»

«Хранилище журналов» отображает список подключенных БД, в которые сохраняет события подключенный «Ретранслятор».

> Функционал «Хранилища журналов» является экспериментальным. Поскольку предполагается использование одного узла «Ретранслятора» с одной БД, то компоненты Termidesk будут отправлять события на первый полностью работающий «Ретранслятор» и его БД.
> Записанные «Ретранслятором» события в БД доступны для просмотра в разделе «Мониторинг - Журналы фермы» (см. подраздел **Просмотр централизованных журналов фермы**).
> В отличие от компонентов Termidesk, регистрирующихся в разделе «Инфраструктура» автоматически, «Хранилище журналов» добавляется вручную.

Для отображения списка «Хранилищ журналов» нужно перейти «Инфраструктура - Хранилища журналов». По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Название».

Основные параметры списка приведены в таблице (см. Таблица 124).

Таблица 124 – Основные параметры списка «Хранилищ журналов»

Параметр	Описание
«Название»	Наименование «Хранилища журналов»
«Используется»	Флаг использования «Хранилища журналов». Возможные значения: ▪ «Да» - объект используется для сбора журналов; ▪ «Нет» - объект не используется для сбора журналов

Для добавления «Хранилища журналов» следует перейти «Инфраструктура - Хранилища журналов» и нажать экранную кнопку **[Создать]**. Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 125).

Таблица 125 – Данные для добавления «Хранилища журналов»

Параметр	Описание
«Имя журнала»	Текстовое наименование «Хранилища журналов»
«Имя БД»	Наименование БД, в которой расположено «Хранилище журналов»

Параметр	Описание
«УЗ БД»	Имя пользователя для подключения к БД «Хранилища журналов». Для обеспечения безопасного доступа к «Хранилищу журналов» рекомендуется создать учетные записи БД с нижеперечисленными ролями: ▪ «Администратора» - учетная запись должна обладать правами на создание учетных записей «Ретранслятора» и «Читателя», задание паролей, создание БД для хранения событий; ▪ «Ретранслятора» - учетная запись должна обладать правами на перенаправление событий из журналов компонентов Termidesk в БД «Хранилища журналов» и управление сроком хранения данных в БД; ▪ «Читателя» - учетная запись должна обладать правами на чтение данных из БД. В текущей версии Termidesk для подключения к БД «Хранилища журналов» используется только учетная запись «Администратора»
«Пароль БД»	Пароль для подключения к БД «Хранилища журналов»
«IP-адрес БД»	IP-адрес узла с установленной БД «Хранилища журналов»
«Порт»	Порт для подключения к БД «Хранилища журналов». Значение по умолчанию: «5432»
«Включено»	Управление использованием «Хранилища журналов». Возможные значения: ▪ «Да» - использовать «Хранилище журналов» для сбора журналов; ▪ «Нет» - не использовать «Хранилище журналов» для сбора журналов. Параметр предназначен для прекращения взаимодействия компонентов Termidesk с узлом «Хранилища журналов», который по каким-либо причинам выведен из стандартного рабочего состояния
«Максимальный размер»	Максимальный размер (в гигабайтах) «Хранилища журналов»
«Время хранения»	Время хранения (в сутках) событий в «Хранилище журналов»

Над созданными «Хранилищами журналов» можно выполнять следующие действия:

- редактировать, для этого следует выбрать нужный объект в таблице, а затем нажать экранную кнопку **[Изменить]**;
- удалить, для этого следует выбрать нужный объект в таблице, а затем нажать экранную кнопку **[Удалить];**
- управлять состоянием, для этого следует выбрать нужный объект в таблице, нажать экранную кнопку **[Использование]** и в раскрывающемся списке выбрать состояние «Хранилища журналов»:
  - «Использовать»;
  - «Не использовать».

⚠ Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».
Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

17 . РЕЖИМ ВЫСОКОЙ ДОСТУПНОСТИ И РАБОТА С СЕРТИФИКАТАМИ

17.1 . Настройка «Менеджера рабочего места» в режиме высокой доступности

⚠ Начиная с Termidesk версии 6.0 дополнительные настройки «Менеджера рабочих мест» не требуются.

17.2 . Настройка балансировщика для работы с самоподписанными сертификатами

17.2.1 . Создание самоподписанного SSL-сертификата

Для создания самоподписанного SSL-сертификата и ключа к нему нужно:

- 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`):

```
1  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 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
```

17.2.2 . 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:

```
ssl_protocols TLSv1.3;
ssl_prefer_server_ciphers on;
ssl_dhparam /etc/nginx/dhparam.pem;
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;
ssl_ecdh_curve secp384r1; # Requires nginx >= 1.1.0
ssl_session_timeout  10m;
ssl_session_cache shared:SSL:10m;
ssl_session_tickets off; # Requires nginx >= 1.5.9
ssl_stapling on; # Requires nginx >= 1.3.7
ssl_stapling_verify on; # Requires nginx => 1.3.7
resolver 77.88.8.8 77.88.8.1 valid=300s;
resolver_timeout 5s;
# Disable strict transport security for now. You can uncomment the following
# line if you understand the implications.
# add_header Strict-Transport-Security "max-age=63072000; includeSubDomains; preload";
add_header X-Frame-Options DENY;
add_header X-Content-Type-Options nosniff;
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.

17.2.3 . 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 организации.

Для корректного отображения IP-адресов источника подключения следует в «Портале администратора» задать параметру «Использовать анонсируемый IP клиента» значение «Да» (см. подраздел **Параметры безопасности Termidesk**).

```
upstream daas-upstream-ws {
 least_conn;
    # PROXY TERMIDESK

     server 192.0.2.41:5099;
     server 192.0.2.42:5099;
     server 192.0.2.43:5099;
     server 192.0.2.44:5099;

}

upstream daas-upstream-nodes {
 least_conn;
     # DISPATCHER TERMIDESK

     server 192.0.2.30:443;
     server 192.0.2.31:443;
     server 192.0.2.32:443;

 }

server {
 listen 0.0.0.0:80;
 listen 0.0.0.0:443 ssl;

  include snippets/self-signed.conf;
  include snippets/ssl-params.conf;

 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/;
```

```
50
51          proxy_set_header Host $host;
52          proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
53
54   }
55
56  }
```

⚠ IP-адреса, перечисленные в директиве `daas-upstream-ws`, являются адресами «Шлюзов» 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
```

```
1  nginx: [warn] "ssl_stapling" ignored, issuer certificate not found
2  nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
3  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
```

18 . ЭКСПЕРИМЕНТАЛЬНЫЕ ФУНКЦИИ

18.1 . Управление экспериментальными параметрами Termidesk

Включение и отключение экспериментальных параметров Termidesk производится из командной строки.

Для активации экспериментального параметра нужно:

- перейти в интерфейс командной строки;
- переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- присвоить значение «True» ключу `--value`:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_config set --key experimental.2fa.enabled --
value True
```

где:

`experimental.2fa.enabled` - наименование параметра.

Перечень экспериментальных параметров приведен в таблице (см. Таблица 126).

Таблица 126 – Экспериментальные параметры Termidesk

Параметр	Описание	Значение по умолчанию
`experimental.2fa.enabled`	Параметр поддержки двухфакторной аутентификации	`False`
`experimental.converted.transports.backup.path`	Параметр устанавливает путь сохранения файла формата `.json` с параметрами ранее существовавших протоколов доставки. Параметр менять не рекомендуется	`/opt/termidesk.backups`
`experimental.deviceauth.enabled`	Параметр поддержки авторизации устройств доступа	`False`
`experimental.openstack.provider.enabled`	Параметр поддержки поставщика ресурсов Openstack	`False`
`experimental.provider.physmachine.enabled`	Параметр поддержки поставщика ресурсов для физических машин	`False`
`experimental.radiusauth.enabled`	Параметр поддержки домена аутентификации RADIUS	`False`
`experimental.html5.transports.enabled`	Параметр поддержки протокола HTML5	`False`
`experimental.html5.singleTab.enabled`	Параметр поддержки режима открытия HTML5-клиента в той же вкладке веб-браузера, из которой происходит его запуск	`False`

Параметр	Описание	Значение по умолчанию
`experimental.t1cloud.provider.enabled`	Параметр поддержки поставщика ресурсов «Платформа T1cloud»	`False`
`experimental.tera.transports.enabled`	Параметр поддержки протокола TERA	`False`
`experimental.metasessionsprov.maxConnectionCount`	Параметр позволяет задать максимальное количество подключений к ноде метапоставщика	`181`
`experimental.loudplay.transports.enabled`	Параметр поддержки протокола доставки Loudplay	`False`
`experimental.loudplay.serverPort`	Параметр позволяет задать порт для подключения по протоколу Loudplay. Диапазон значений: от 0 до 65535	`8554`
`experimental.loudplay.logPath`	Параметр позволяет задать путь к файлу журнала клиента Loudplay	`logs/lp_client.log`
`experimental.loudplay.bbrBitrateInitial`	Параметр позволяет задать начальную скорость видеопотока (Кб/с). Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Автоматическое изменение скорости видеопотока». Диапазон значений: от 100 до 5000	`1000`
`experimental.loudplay.bbrBitrateMin`	Параметр позволяет задать минимально возможную скорость видеопотока (Кб/с). Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Автоматическое изменение скорости видеопотока». Диапазон значений: от 50 до 3000	`50`
`experimental.loudplay.bbrBitrateMax`	Параметр позволяет задать максимально возможную скорость видеопотока (Кб/с). Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Автоматическое изменение скорости видеопотока». Диапазон значений: от 5000 до 100000	`12000`
`experimental.loudplay.bbrCycleDelay`	Параметр позволяет задать время (мс) между циклами расчета нового битрейта. Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Автоматическое изменение скорости видеопотока». Диапазон значений: от 100 до 10000	`8000`
`experimental.loudplay.bbrPingDelay`	Параметр позволяет задать время (мс) между циклами измерения состояния канала. Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Автоматическое изменение скорости видеопотока». Диапазон значений: от 10 до 1000	`50`
`experimental.loudplay.bbrGainIncrease`	Параметр позволяет регулировать скорость передачи данных в зависимости от пропускной способности сети. Диапазон значений: от 1.1 до 5	`2`

Параметр	Описание	Значение по умолчанию
`experimental.loudplay.bbrGainProbe`	Параметр позволяет регулировать частоту увеличения пропускной способности сети в зависимости от нагрузки. Диапазон значений: от 1.1 до 1.3	`1.15`
`experimental.loudplay.bbrGainStandby`	Параметр позволяет регулировать уровень увеличения пропускной способности сети в режиме ожидания. Диапазон значений: от 0.1 до 0.9	`0.75`
`experimental.loudplay.bbrGainDrain`	Параметр позволяет регулировать уровень уменьшения пропускной способности сети в зависимости от нагрузки. Диапазон значений: от 0.1 до 0.9	`0.5`
`experimental.loudplay.bbrPort`	Параметр позволяет задать порт для управления сетевыми соединениями. Диапазон значений: от 0 до 65535	`8556`
`experimental.loudplay.controlEnable`	Параметр позволяет управлять включением или отключением передачи сигналов клавиатуры и мыши. Возможные значения: ▪ «False» - запретить передачу сигналов клавиатуры и мыши; ▪ «True» - разрешить передачу сигналов клавиатуры и мыши	`True`
`experimental.loudplay.controlPort`	Параметр позволяет задать порт для передачи сигналов клавиатуры и мыши. Диапазон значений: от 0 до 65535	`8555`
`experimental.loudplay.rtpVideoPort`	Параметр позволяет задать порт для для передачи видео. Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно задать значение «UDP» параметру «Протокол передачи видео». Диапазон значений: от 0 до 65535	`6970`
`experimental.loudplay.rtpAudioPort`	Параметр позволяет задать порт для для передачи аудио. Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно задать значение «UDP» параметру «Протокол передачи видео». Диапазон значений: от 0 до 65535	`6972`
`experimental.loudplay.audioBitrate`	Параметр позволяет задать качество и объем передаваемых аудиоданных (kbit/s)	`128000`
`experimental.loudplay.peripheryPort`	Параметр позволяет порт для перенаправления USB-устройств. Диапазон значений: от 0 до 65535	`8558`
`experimental.loudplay.x1`	Параметр позволяет запустить таймер с отсчетом времени бездействия (в секундах), по истечении которого активируется действие или событие. Доступны следующие параметры запуска таймера: ▪ `experimental.loudplay.x1` - запуск первого таймера; ▪ `experimental.loudplay.x2` - запуск второго таймера	`0`
`experimental.loudplay.fecRedundancy`	Параметр позволяет задать избыточность данных (в процентах) для обеспечения устойчивости к потерям в сети. Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Помехоустойчивое кодирование». Диапазон значений: от 0 до 100	`20`

Параметр	Описание	Значение по умолчанию
`experimental.loudplay.rtpRetransmission`	Параметр позволяет управлять непрерывной передачей видеоизображения на каналах с потерями до 3%. Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Помехоустойчивое кодирование». Отключение параметра `rtpRetransmission`, в сочетании с «Помехоустойчивым кодированием», рекомендуется в исключительных случаях, когда важна минимальная задержка отклика на стабильных каналах связи без потерь. Возможные значения: ▪ «False» - запретить непрерывную передачу видеоизображения; ▪ «True» - разрешить непрерывную передачу видеоизображения	`True`
`experimental.loudplay.controlForceAbsoluteCursor`	Параметр позволяет управлять определением абсолютных или относительных координат мыши. Отключение параметра рекомендуется в случаях, когда курсор мыши плохо позиционируется в приложениях. Возможные значения: ▪ «False» - запретить определение абсолютных координат мыши; ▪ «True» - разрешить определение абсолютных координат мыши	`True`
`experimental.loudplay.showBadConnect`	Параметр активации отображения уведомлений при возникновении проблем с сетью. Возможные значения: ▪ «False» - запретить отображение уведомлений; ▪ «True» - разрешить отображение уведомлений	`False`
`experimental.loudplay.showResNotif`	Параметр активации отображения уведомлений при различии разрешений между экраном пользовательской рабочей станции и экраном РМ. Возможные значения: ▪ «False» - запретить отображение уведомлений; ▪ «True» - разрешить отображение уведомлений	`False`

18.2 . Установка плагинов расширений

Начиная с Termidesk версии 5.1 использование функционала, подключаемого через плагин расширения, исключено. Описание приведено для справки.

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:

- 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:

```
1  pip install --upgrade --no-index --find-links /var/repos/Addons/Plugins/v5.0/
   termidesk_internaldbauth
```

где:

`/var/repos/Addons/Plugins/v5.0/` - 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:

```
1  sudo /opt/termidesk/sbin/termidesk-vdi-manage migrate
2  sudo /opt/termidesk/sbin/termidesk-vdi-manage collectstatic --no-input
```

- перезапустить службу Termidesk:

```
sudo systemctl restart termidesk-vdi.service
```

18.3 . Удаление плагинов расширений

Перед удалением плагина необходимо удалить фонды РМ, шаблоны ВМ и поставщика ресурсов, соответствующих данному плагину.
Удаление фонда РМ может занять продолжительное время.

Начиная с Termidesk версии 5.1 использование функционала, подключаемого через плагин расширения, исключено. Описание приведено для справки.

Для удаления плагина расширений нужно:

- 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 службу Termidesk:

```
sudo systemctl restart termidesk-vdi.service
```

18.4 . 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:

> Начиная с Termidesk версии 5.1 использование функционала, подключаемого через плагин расширения, исключено. Описание приведено для справки.

```
1 pip install --no-index --find-links /var/repos/Addons/Plugins/v5.0/
termidesk_internaldbauth==4.0.1
```

где:

`/var/repos/Addons/Plugins/v5.0/` - каталог с `whl`-файлами, `whl`-файл с версией плагина должен существовать в данном каталоге;

`termidesk_internaldbauth` - имя плагина с указанием версии.

19 . РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ ОТСЛЕЖИВАНИЯ СОСТОЯНИЯ КОМПОНЕНТОВ TERMIDESK

19.1 . Общие сведения по проверке состояния компонентов

Для отслеживания состояния компонентов Termidesk и обращения к ним для выполнения проверок состояния (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-celery
                    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 доступен на порте, заданном в конфигурационном файле:

> ⚠ Для компонента «Универсальный диспетчер» порт определен настройками веб-сервера (по умолчанию используется 443).

- для компонента «Менеджер рабочих мест» - в файле `/etc/opt/termidesk-vdi/termidesk.conf`, в параметрах `CELERY_BEAT_HEALTH_CHECK_PORT` (по умолчанию используется 8103), `CELERY_WORKER_HEALTH_CHECK_PORT` (по умолчанию используется 8104);
- для компонента «Шлюз» - в файле `/etc/termidesk/gateway.yaml`, в параметре `${mgtServerPort:8102}` (по умолчанию используется 8102).

Для исключения злоупотреблением частыми вызовами API, способными создать нагрузку на систему, доступ к API-запросу контролируется отдельным токеном. Значение токена задается конфигурационным файлом:

- для компонентов «Универсальный диспетчер», «Менеджер рабочих мест» - в файле `/etc/opt/termidesk-vdi/termidesk.conf`, в параметре `HEALTH_CHECK_ACCESS_KEY`;
- для компонента «Шлюз» - в файле `/etc/termidesk/gateway.yaml`, в параметре `token: ${healthCheckAccessKey}`.

Пример `HEALTH_CHECK_ACCESS_KEY`:

```
HEALTH_CHECK_ACCESS_KEY = "9944b09199c62bcf9418ad846dd0e4bbdfc6ee4b"
```

Пример `token: ${healthCheckAccessKey}`:

```
${healthCheckAccessKey:9944b09199c62bcf9418ad846dd0e4bbdfc6ee4b}
```

19.2 . Состояние компонента «Универсальный диспетчер»

При распределенной установке Termidesk экземпляры компонента «Универсальный диспетчер» могут быть установлены на нескольких узлах. Доступ к узлам организуется через балансировщик нагрузки, 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`:

```
1  curl --insecure -v -s -X 'GET' "https://${HOSTNAME}:443/api/health/check" -H
   'accept: application/json' -H "Authorization: Token ${HEALTH_CHECK_ACCESS_KEY}"
```

⚠ Ключ `--insecure` используется для отключения проверки валидности сертификатов. Выполнение запроса без использования проверки SSL допустимо только на тестовых стендах. В производственной среде необходимо установить валидные сертификаты.

19.3 . Состояние компонента «Шлюз»

При распределенной установке Termidesk экземпляры компонента «Шлюз» могут быть установлены на нескольких узлах. Доступ к узлам организуется через балансировщик нагрузки, но для механизма проверок состояния нужно обращаться к каждому узлу напрямую.

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 `token: ${healthCheckAccessKey}`.

Пример команды проверки состояния компонента через утилиту `curl` для компонента «Шлюз» `termidesk-gateway` (предполагается, что «Шлюз» настроен для работы по защищенному соединению):

```
1  curl --insecure -v -s -X 'GET' "https://${HOSTNAME}:8102/api/health" -H 'accept:
   application/json' -H "Authorization: Token ${healthCheckAccessKey}"
```

19.4 . Состояние компонента «Менеджер рабочих мест»

При распределенной установке Termidesk экземпляры компонента «Менеджер рабочих мест» могут быть установлены на нескольких узлах.

Для использования механизма проверки состояния компонента необходимо в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` раскомментировать строки параметров:

- для непосредственно компонента «Менеджер рабочих мест», а именно службы `termidesk-celery-beat`: `CELERY_BEAT_CHECK_IP`, `CELERY_BEAT_HEALTH_CHECK_PORT`, `HEALTH_CHECK_CERT`, `HEALTH_CHECK_KEY`. Для параметров `HEALTH_CHECK_CERT`, `HEALTH_CHECK_KEY` нужно указать путь к сертификату и ключу, используемых для защищенного подключения, и выполнить перезапуск служб Termidesk;
- для непосредственно компонента «Менеджер рабочих мест», а именно службы `termidesk-celery-worker`: `CELERY_WORKER_CHECK_IP`, `CELERY_WORKER_HEALTH_CHECK_PORT`, `HEALTH_CHECK_CERT`, `HEALTH_CHECK_KEY`. Для параметров `HEALTH_CHECK_CERT`, `HEALTH_CHECK_KEY` нужно указать путь к сертификату и ключу, используемых для защищенного подключения, и выполнить перезапуск служб Termidesk.

Пример задания значений:

```
1  CELERY_BEAT_HEALTH_CHECK_PORT=8103
```

```
CELERY_BEAT_HEALTH_CHECK_IP='0.0.0.0'
CELERY_WORKER_HEALTH_CHECK_PORT=8104
CELERY_WORKER_HEALTH_CHECK_IP='0.0.0.0'
HEALTH_CHECK_CERT=/etc/opt/termidesk-vdi/healthcheck.pem
HEALTH_CHECK_KEY=/etc/opt/termidesk-vdi/healthcheck-decrypted.key
```

Пример команды проверки состояния компонента «Менеджер рабочих мест» через утилиту `curl` (предполагается, что «Менеджер рабочих мест» настроен для работы по защищенному соединению):

```
curl --insecure -v -s -X 'GET' "${HOSTNAME}:8103/api/health/check" -H 'accept:
application/json' -H "Authorization: Token ${HEALTH_CHECK_ACCESS_KEY}"
```

20 . ХРАНЕНИЕ ЧУВСТВИТЕЛЬНОЙ ИНФОРМАЦИИ

20.1 . Хранение чувствительной информации с выбранным способом хранения «hvac»

Способ хранения паролей выбирается на этапе установки Termidesk. Способ хранения паролей «hvac» подразумевает, что будет использоваться хранилище OpenBao или Hashicorp Vault. Хранилище при этом должно быть заранее создано и настроено. При использовании Hashicorp Vault со схемой AD (Active Directory) поддерживается автоматическое обновление паролей.

При этом способе чувствительная информация (имена учетных записей, пароли, открытые и закрытые ключи, keytab-файлы, токены) хранится в контейнерах, пути к которым задаются вручную.

В контейнерах может содержаться как динамически обновляемая чувствительная информация, так и статическая. Поэтому в Termidesk для определения типа информации используются префиксы при задании пути к контейнеру хранения:

- `hvac-ad://` - префикс используется для динамически обновляемой чувствительной информации. Может быть задан только для хранилища Hashicorp Vault;
- `hvac-kv://` - префикс используется для статической чувствительной информации. Может быть задан как для хранилища OpenBao, так и для Hashicorp Vault.

Для корректной работы Termidesk со статической чувствительной информацией в хранилище должна быть повторена структура данных Active Directory. Контейнер, содержащий чувствительную информацию, должен содержать параметры:

- `current_password` - пароль учетной записи;
- `username` - имя учетной записи.

Пример:

```
{
    'current_password': '?@09AZ3PlvTzMKhsvZ91YFyVjVRHceYQ34eizKcKhVNHPjQJ46kvGGdsBPSkRcE9',
    'username': 'adfs-s'
},
```

Помимо указания префикса должна использоваться точка монтирования (mount point), заданная администратором в хранилище.

Таким образом общий формат указания пути к контейнеру хранения чувствительной информации в Termidesk выглядит следующим образом:

Символ «/» определяет, что должно быть возвращено все содержимое контейнера.
Если нужно вернуть значение конкретной переменной (key) контейнера, символ «/» не используется.

- если нужно вернуть всю информацию из контейнера:

```
<префикс> <точка_монтирования#> <путь_к_контейнеру>/
```

- если нужно вернуть только значение конкретного параметра:

```
<префикс> <точка_монтирования#> <путь_к_параметру_в_хранилище>
```

Допустим, в хранилище создан контейнер со статической информацией `termidesk` и точкой монтирования `secret`:

```
vault kv get secret/termidesk
```

Контейнер содержит следующие параметры:

```
1  ========== Data ==========
2  Key                 Value
3  ---                 -----
4  current_password    my_password
5  username            Администратор
```

В этом случае в Termidesk следует указывать:

- для возврата всех параметров: `hvac-kv://secret#termidesk/` (будет возвращено: `{'current_password': 'my_password', 'username': 'Администратор'}`);
- для возврата значения параметра `username`: `hvac-kv://secret#termidesk/username` (будет возвращено: `'Администратор'`).

Дополнительные примеры приведены в таблице (see page 0).

Таблица 127 – Примеры указания путей к чувствительной информации в Termidesk

Команда в хранилище	Указание пути в Termidesk
Команда записи роли в хранилище: `vault write ad/roles/vvddaa service_account_name="vvddaa@domain.local"`	`hvac-ad://ad#vvddaa/` где: `hvac-ad://` - префикс; `ad#` - точка монтирования; `vvddaa/` - путь к роли
Команда записи сертификата в хранилище: `vault kv put secret/termidesk-admin/ssl-cert-snakeoil pem=@astra.local.pem` ⚠ Команды вида `vault kv put` перезаписывают контейнер сразу целиком, поэтому если задание сертификата и ключа будет разделено на разные команды, то в контейнере окажется только то, что добавлялось последним.	`hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem` где: `hvac-kv://` - префикс; `secret#` - точка монтирования; `termidesk-admin/ssl-cert-snakeoil/` - путь к контейнеру; `pem` - сертификат

Команда в хранилище	Указание пути в Termidesk

Сгенерированный на контроллере домена `keytab`-файл должен быть преобразован к формату BASE64 для использования в хранилище:
`base64 termidesk.keytab > termidesk.keytab.b64`
Команда записи `keytab`-файла в хранилище:
`vault kv put secret/termidesk-admin/keytabs termidesk=@kerberos.keytab.b64`
Пример команды для преобразования файла и одновременной записи в хранилище:
`vault kv put secret/termidesk-admin/keytabs termidesk="$(base64 -w 0 termidesk.keytab)"`
	`hvac-kv://secret#termidesk-admin/keytabs/termidesk`
	где:
	`hvac-kv://` - префикс;
	`secret#` - точка монтирования;
	`termidesk-admin/keytabs/` - путь к контейнеру;
	`termidesk` - `keytab`-файл

21 . НЕШТАТНЫЕ СИТУАЦИИ

21.1 . Нештатные ситуации и способы их устранения

Возможные неисправности при работе с Termidesk и способы их устранения приведены в таблице (см. Таблица 128).

Таблица 128 – 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 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 «Портале администратора» Termidesk	Необходимо указать правильный 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 РМ 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`

Ошибка: «Для фонда значение политики "Действие при выходе пользователя из ОС" не может быть "Удалять рабочее место"»	Ошибка возникает при создании фонда PM метапоставщика через мастер публикации фонда	Необходимо перейти в настройки политик указанного в ошибке сервисного фонда PM и для политики «Действие при выходе пользователя из ОС» выбрать значение «Не задано». Затем вновь перейти к созданию фонда PM метапоставщика
В записях журнала «Универсального диспетчера» отражен IP-адрес портала «Агрегатор», а не IP-адрес пользователя	При подключении пользователя к ресурсу фермы Termidesk через портал «Агрегатор» в журнале узла «Универсального диспетчера» фиксируется запись с указанием IP-адреса портала «Агрегатор», а не IP-адресом пользователя	Необходимо перейти «Настройки - Системные параметры - Безопасность» и включить параметр «Использовать анонсируемый IP клиента»

Индикация	Описание	Возможное решение
РМ не вводится в домен MS AD	Учтена запись РМ не создается в домене MS AD, несмотря на то, что используется параметры гостевых ОС с вводом в домен	Необходимо убедиться, что параметр OU в параметрах гостевых ОС задан правильно (см. подразделы **Конфигурация ОС Linux при вводе в домен MS AD** и **Конфигурация ОС Windows при вводе в домен MS AD**)
Учетная запись РМ не удаляется из домена MS AD	Учетная запись РМ не удаляется из домена MS AD, несмотря на то, что используется функционал удаления учетной записи при удалении фонда РМ	Необходимо убедиться, что параметр OU в параметрах гостевых ОС задан правильно (см. подразделы **Конфигурация ОС Linux при вводе в домен MS AD** и **Конфигурация ОС Windows при вводе в домен MS AD**)
Ошибка: «Информация о доступном месте хранилища не предоставлена поставщиком ресурсов»	Ошибка возникает при публикации связанных клонов через поставщика ресурсов oVirt (или zVirt, «РЕД Виртуализация»), если информация о свободном месте хранилища не приходит на сервер Termidesk	Необходимо убедиться, что на используемой платформе виртуализации хранилище доступно
Ошибка: «Данный шаблон не поддерживается выбранным терминальным сервером» или «The template is not supported by the terminal server»	Ошибка возникает при создании шаблона РМ для терминального сервера	Необходимо убедиться, что выбран верный шаблон РМ терминального сервера: ▪ если используется терминальный сервер STAL, то нужно выбрать шаблон «STAL Terminal Service» или «STAL Remote App Service»; ▪ если используется терминальный сервер MS RDS, то нужно выбрать шаблон «RDS Terminal Service» или «RDS Remote App Service»
Ошибка: «Достигнуто максимальное количество устаревших шаблонов публикаций» в разделе «Публикации» фонда РМ	При попытке опубликовать фонд РМ отображается подсказка «Достигнуто максимальное количество устаревших шаблонов публикаций»	Достигнуто заданное в политике «Максимальное количество устаревших шаблонов связанных клонов» количество шаблонов для фонда РМ. Необходимо удалить некоторые существующие РМ или задать новое значение политике

Индикация	Описание	Возможное решение

Ошибка:
«Incorrect MTLS based "Device auth" feature setup»
	Ошибка возникает после установки Termidesk и попытке перейти к веб-порталу Termidesk	Необходимо удалить использование экспериментального параметра `experimental.deviceauth.enabled`, если веб-сервер не настроен на использование mTLS:
		▪ перейти в интерфейс командной строки;
		▪ переключиться на пользователя `termidesk`:
		`sudo -u termidesk bash`
		▪ отключить использование параметра `experimental.deviceauth.enabled`:
		`/opt/termidesk/sbin/termidesk-vdi-manage tdsk_config set --key experimental.deviceauth.enable --value False`

Для поставщика ресурсов zVirt не тиражируются ВМ	Тиражирование ВМ аварийно завершается на финальной стадии подготовки (в момент создания снимка ВМ)	Необходимо увеличить время ожидания в настройках поставщика ресурсов (см. подраздел **Добавление платформы zVirt**)

22 . ПЕРЕЧЕНЬ ТЕРМИНОВ

Термин	Определение
Агрегатор администратора	Веб-интерфейс управления порталом «Агрегатор»
Агрегатор пользователя	Веб-интерфейс пользователя для получения ресурсов, предоставляемых порталом «Агрегатор»
Компонент «Агент»	Собирательное название для следующих компонентов Termidesk: ▪ «Агент виртуального рабочего места»; ▪ «Агент узла виртуализации»; ▪ «Сессионный агент»; ▪ «Видеоагент»; ▪ «Агент виртуальных смарт-карт». Самостоятельный компонент, отвечающий за контролируемую доставку РМ, взаимодействие с «Универсальным диспетчером» и «Менеджером рабочих мест»
Компонент «Агент виртуальных смарт-карт»	Компонент Termidesk. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление подключенных к пользовательской рабочей станции смарт-карт в ВРМ
Компонент «Агент виртуального рабочего места»	Компонент Termidesk. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет взаимодействие с «Универсальным диспетчером», конфигурирует ВРМ, фиксирует действия пользователя, реализует передачу управляющих сообщений
Компонент «Агент узла виртуализации»	Компонент Termidesk. Устанавливается на узел виртуализации, взаимодействует с гипервизором через модуль `libvirt`
Базовое виртуальное рабочее место	Также: золотой образ, базовый образ. Подразумевает собой образ диска ВМ с предустановленным прикладным ПО и установленным «Агентом виртуального рабочего места». Этот образ далее будет использоваться для создания ВРМ для пользователей
Балансировщик нагрузки	Самостоятельный компонент, отвечающий за распределение нагрузки на множество «Универсальных диспетчеров» и «Шлюзов»
Компонент «Видеоагент»	Компонент Termidesk. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление видеокамеры с пользовательской рабочей станции в ВРМ
Виртуальное рабочее место	Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО. Подключение к ВРМ происходит через протоколы удаленного доступа
Рабочее место	Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под РМ подразумеваются как ВРМ, так и терминальный доступ или доступ к опубликованным на терминальном сервере приложениям
Гостевая ОС	ОС, функционирующая на ВМ
Группы рабочих мест	Функциональное объединение множества фондов РМ по определенному признаку
Домен аутентификации	Способ проверки субъектов и их полномочий
Компонент «Менеджер рабочих мест»	Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом РМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета `termidesk-vdi`. Наименование служб после установки: `termidesk-celery-beat.service` и `termidesk-celery-worker.service`

Термин	Определение
Компонент «Оркестратор»	Компонент Termidesk. 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 РМ
Протокол доставки	Поддерживаемый в Termidesk протокол удаленного доступа к РМ
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
Компонент «Сессионный агент»	Компонент Termidesk. Устанавливается на терминальный сервер (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям
Компонент «Универсальный диспетчер»	Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service`
Фонд рабочих мест	Совокупность подготовленных рабочих мест для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей
Шаблон рабочего места	Параметры конфигурации РМ для использования в фонде РМ
Компонент «Шлюз»	Компонент Termidesk. Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP. Устанавливается из пакета `termidesk-gateway`. Наименование службы после установки: `termidesk-gateway.service`
Компонент «Сервер терминалов Astra Linux»	Компонент Termidesk. Также: STAL. Обеспечивает подключение пользовательских рабочих станций к РМ с ОС Astra Linux Special Edition через сеанс удаленного терминала
Портал «Агрегатор»	Роль компонента «Универсальный диспетчер», доступная при установке Termidesk. Является единой точкой входа для получения ресурсов пользователями, предоставляет им объединенный список приложений и ВРМ с ферм Termidesk
Портал администратора	Предоставляет веб-интерфейс для управления Termidesk и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API
Портал пользователя	Предоставляет пользовательский веб-интерфейс Termidesk (без доступа к функциям управления) и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API
Портал универсальный	Предоставляет функции обоих вариантов - и «Портала администратора», и «Портала пользователя». При этом активируется доступ ко всем модулям документации по командам REST API, предоставляемым интерфейсом `swagger`
Ключ	Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом
Сертификат	Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу
Ферма	Логическое объединение узлов, взаимодействующих с одной БД

23 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
БД	База данных
ВМ	Виртуальная машина
ВРМ	Виртуальное рабочее место
ЗПС	Замкнутая программная среда
КД	Контроллер домена
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПК СВ Брест	Программный комплекс «Средства виртуализации «Брест»
ПО	Программное обеспечение
РМ	Рабочее место
СУБД	Система управления базами данных
ЦП	Центральный процессор
ЦС	Центр сертификации
ЭЦП	Электронная цифровая подпись
ACL	Access Control List (список контроля доступа)
ALD	Astra Linux Directory (единое пространство пользователей)
AMQP	Advanced Message Queueing Protocol (открытый протокол для передачи сообщений между компонентами системы)
AMQPS	Расширение протокола AMQP с использованием TLS для шифрования
API	Application Programming Interface (интерфейс прикладного программирования)
CRUD	Create Read Update Delete (акроним основных операций с информацией в БД)
CSR	Certificate Signing Request (зашифрованный запрос на выпуск сертификата)
DHCP	Dynamic Host Configuration Protocol (протокол назначения сетевого адреса)
DN	Domain Name (доменное имя)
DNS	Domain Name System (система доменных имен)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
FreeIPA	Free Identity, Policy and Audit (открытое решение по безопасности Linux-систем)
GC	Global Catalog (глобальный каталог)
GID	Group Identification Data (идентификатор группы)
GPU	Graphics Processing Unit (графический процессор)

Сокращение	Пояснение
GUSID	Global Unique Session ID (глобальный уникальный сессионный идентификатор)
HTML	Hypertext Markup Language (язык гипертекстовой разметки)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
ID	Identification Data (идентификатор)
IdP	Identity Provider (сервис, управляющий идентификационной информацией)
IP	Internet Protocol (межсетевой протокол)
JSON	JavaScript Object Notation (стандартный текстовый формат для структурированных данных)
JWKS	JSON Web Key Set (набор открытых ключей для проверки веб-токена)
JWT	JSON Web Token (открытый стандартдля создания токенов доступа)
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов)
LDAPS	Lightweight Directory Access Protocol over SSL/TSL (расширение протокола LDAP)
MAC	Media Access Control (уникальный идентификатор сетевого устройства)
MS AD	Microsoft Active Directory (службы каталогов Microsoft)
mTLS	Multiplexed Transport Layer Security (протокол, основанный на TLS с усиленной безопасностью)
OIDC	OpenID Connect (протокол аутентификации, построенный поверх стандарта OAuth 2.0)
OU	Organizational Unit (организационная единица)
PAM	Pluggable Authentication Module (подключаемый модуль аутентификации)
PID	Product ID (идентификатор продукта)
PKCS	Public Key Cryptography Standards (стандарты криптографии с открытым ключом)
PKINIT	Public Key Cryptography for Initial Authentication (механизм Kerberos, позволяющий использовать сертификаты X.509)
RADIUS	Remote Authentication Dial-In User Service (протокол, предоставляющий функции аутентификации, авторизации и учета)
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)
REDIS	REmote DIctionary Service (резидентная СУБД)
REST	Representational State Transfer (программная архитектура, определяющая условия работы API)
RFC	Request for Comments (рабочее предложение Интернет)

Сокращение	Пояснение
RPC	Remote Procedure Call (удаленный вызов процедур)
RSA	Rivest, Shamir and Adleman (криптографический алгоритм с открытым ключом)
RTSP	Real-Time Streaming Protocol (протокол для управления потоковой передачей данных)
PKI	Public Key Infrastructure (инфраструктура открытых ключей)
SAM	Security Account Manager (диспетчер учетных записей безопасности)
SAML	Security Assertion Markup Language (открытый стандарт обмена данными аутентификации)
SASL	Simple Authentication and Security Layer (фреймворк для аутентификации и обеспечения безопасности)
SCSI	Small Computer System Interface (набор стандартов для физического подключения и передачи данных между компьютерами и периферийными устройствами)
SMB	Server Message Block (протокол для удалённого доступа к сетевым ресурсам)
SPICE	Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)
SRV	Service Record DNS (служебная запись в DNS)
SSL	Secure Sockets Layer (криптографический протокол)
SSO	Single Sign-On (технология единого входа)
STAL	Terminal Server Astra Linux (сервер терминалов Astra Linux)
STUN	Session Traversal Utilities for NAT (сетевой протокол, позволяющий определить внешний IP-адрес и другие параметры
SUID	Unique Session ID (уникальный сессионный идентификатор, то же самое, что GUSID)
TCP	Transmission Control Protocol (протокол управления передачей)
TERA	Termidesk Remote Access protocol (протокол удаленного доступа собственной разработки)
TLS	Transport Layer Security (протокол защиты транспортного уровня)
TOTP	Time-based One Time Password (метод авторизации пользователя)
UDP	User Datagram Protocol (протокол пользовательских датаграмм)
URI	Uniform Resource Identifier (унифицированный идентификатор ресурса)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
URSI	Unique Resource Start ID (уникальный идентификатор запуска ресурса)
USB	Universal Serial Bus (последовательный интерфейс для подключения периферийных устройств)
UUID	Universally Unique Identifier (уникальный идентификатор)
vGPU	Virtual Graphics Processing Unit (виртуальный графический процессор)

Сокращение	Пояснение
VDI	Virtual Desktop Infarsticture (инфраструктура виртуальных рабочих столов)
VLAN	Virtual Local Area Network (виртуальная локальная сеть)
VNC	Virtual Network Computing (система удаленного доступа к рабочему столу компьютера)
VPN	Virtual Private Network (технология для зашифрованного безопасного соединения)
VRRP	Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности)
WebRTC	Web Real-Time Communications (открытый проект для организации передачи потоковых данных)
WS	WebSocket (двунаправленный протокол, позволяющий клиенту установить связь с сервером)
WSS	WebSocketSecure (двунаправленный протокол, позволяющий клиенту установить защищенную связь с сервером)
X.509	Стандарт для инфраструктуры открытого ключа

UVEON
Unified Virtualization
Experience, Opportunities, Now

119571, г. Москва, Ленинский проспект,
д. 119А, помещ. 9Н
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