



РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-01 90 02

Версия 4.1.1. Выпуск от июня 2023

Настройка программного комплекса

## ОГЛАВЛЕНИЕ

1 .	ОБЩИЕ СВЕДЕНИЯ.....	8
1.1 .	О документе.....	8
1.2 .	Типографские соглашения .....	8
2 .	ПОЛЬЗОВАТЕЛИ И КОМПОНЕНТЫ TERMIDESK .....	9
2.1 .	Разграничение функций .....	9
2.2 .	Схема сетевого взаимодействия компонентов Termidesk.....	9
2.3 .	Последовательность сетевых запросов компонентов Termidesk.....	11
2.4 .	Перечень сетевых портов компонентов Termidesk .....	12
3 .	НАЧАЛО РАБОТЫ.....	15
3.1 .	Последовательность ввода в действие .....	15
3.2 .	Подготовка базового шаблона ВМ на примере ПК СВ Брест .....	16
3.3 .	Подготовка базового ВРМ.....	20
3.3.1 .	Обязательные настройки .....	20
3.3.2 .	Автоматическое масштабирование экрана в ОС Astra Linux.....	22
4 .	ПОСТАВЩИКИ РЕСУРСОВ .....	25
4.1 .	Общие сведения о поставщиках ресурсов.....	25
4.2 .	Добавление поставщика ресурсов ПК СВ Брест .....	26
4.2.1 .	Получение и добавление файла keytab .....	26
4.2.2 .	Перечень параметров для добавления .....	27
4.3 .	Добавление платформы oVirt/zVirt/RHEV.....	29
4.4 .	Добавление поставщика VMmanager.....	30
4.5 .	Добавление поставщика ресурсов VMware vSphere .....	31
4.6 .	Добавление поставщика vAir.....	33
4.7 .	Добавление сервера терминалов (MS RDS и STAL) в качестве поставщика ресурсов .....	34
4.8 .	Добавление сервера терминалов (метапровайдер) в качестве поставщика ресурсов .....	35
4.9 .	Добавление поставщика ресурсов «Физическая рабочая станция».....	37

4.10 .	Добавление поставщика Openstack .....	37
4.11 .	Режим техобслуживания поставщика ресурсов .....	38
5 .	<b>АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ</b> .....	40
5.1 .	Общие сведения о доменах аутентификации .....	40
5.2 .	Добавление аутентификации через FreeIPA .....	41
5.3 .	Добавление аутентификации через ALD .....	43
5.4 .	Добавление аутентификации через SAML .....	44
5.5 .	Добавление IP-аутентификации.....	45
5.6 .	Добавление аутентификации через MS AD (LDAP).....	45
5.7 .	Добавление аутентификации через внутреннюю БД .....	46
5.8 .	Действия над пользователями в домене аутентификации.....	47
5.9 .	Управление аутентификацией на основе адресов сети .....	49
6 .	<b>ВИРТУАЛЬНЫЕ РАБОЧИЕ МЕСТА</b> .....	50
6.1 .	Общие сведения о ВРМ.....	50
6.2 .	Шаблоны ВРМ для ПК СВ Брест .....	50
6.2.1 .	Шаблон на основе связанного и полного клона для ПК СВ Брест .....	50
6.2.2 .	Шаблон на базе снапшота для ПК СВ Брест.....	51
6.3 .	Шаблоны ВРМ для платформ oVirt/RHEV .....	52
6.3.1 .	Шаблон на основе связанного клона для oVirt/RHEV.....	52
6.3.2 .	Шаблон на основе статичной VM для oVirt/RHEV .....	53
6.4 .	Шаблоны ВРМ для платформ VMware vSphere.....	53
6.5 .	Шаблоны ВРМ для серверов терминалов.....	54
6.5.1 .	Шаблон ВРМ для доступа к серверу терминалов MS RDS .....	54
6.5.2 .	Шаблон ВРМ для доступа к опубликованным приложениям MS RDS.....	55
6.5.3 .	Шаблон ВРМ для доступа к серверу терминалов STAL .....	55
6.5.4 .	Шаблон ВРМ для доступа к опубликованным приложениям STAL.....	56
6.6 .	Шаблон ВРМ для метапровайдера .....	56
6.7 .	Шаблоны ВРМ для физической рабочей станции .....	57

6.7.1 .	Шаблон ВРМ на основе одного статического IP-адреса.....	57
6.8 .	Шаблон ВРМ на основе множественных IP-адресов .....	57
6.9 .	Настройка переносимых профилей.....	58
6.9.1 .	Общие сведения .....	58
6.9.2 .	Создание базового образа диска в ПК СВ Брест .....	58
6.9.3 .	Задание атрибутов созданному диску .....	59
6.9.4 .	Настройка модуля РАМ в базовом ВРМ .....	60
6.9.5 .	Активация механизма переносимых профилей в Termidesk.....	61
6.9.6 .	Активация политики в интерфейсе Termidesk .....	62
6.10 .	Перенаправление видеокамеры .....	62
6.11 .	Перенаправление смарт-карты.....	62
6.12 .	Настройка технологии единого входа в гостевой ОС ВМ .....	63
6.12.1 .	Общие сведения .....	58
6.12.2 .	Активация модуля РАМ.....	63
6.12.3 .	Включение механизма автоматической авторизации .....	64
6.12.4 .	Активация технологии единого входа на сервере терминалов MS RDS .....	65
6.13 .	Настройка аутентификации пользователей ВРМ через файл .....	67
6.13.1 .	Общие сведения .....	58
6.13.2 .	Настройка модуля РАМ .....	67
6.13.3 .	Включение механизма автоматической авторизации .....	64
7 .	<b>УПРАВЛЕНИЕ ПАРАМЕТРАМИ ГОСТЕВЫХ ОС .....</b>	<b>69</b>
7.1 .	Управление параметрами гостевых ОС в Termidesk .....	69
7.1.1 .	Общие сведения .....	58
7.1.2 .	Параметры гостевой ОС Windows.....	69
7.1.2.1 .	Конфигурация без домена .....	69
7.1.2.2 .	Конфигурация при вводе в домен MS AD .....	70
7.1.3 .	Параметры гостевой ОС Linux .....	70
7.1.3.1 .	Конфигурация без домена .....	70

7.1.3.2 . Конфигурация при вводе в домен MS AD .....	71
7.1.3.3 . Конфигурация при вводе в домен FreeIPA .....	71
7.1.3.4 . Конфигурация при вводе в домен ALD.....	72
7.1.4 . Действие при выходе пользователя из ОС .....	72
7.1.5 . Изменение изображения гостевых ОС.....	73
<b>8 . ФОНД РАБОЧИХ МЕСТ.....</b>	<b>75</b>
8.1 . Общие сведения о фонде ВРМ .....	75
8.2 . Добавление фонда ВРМ .....	75
8.3 . Глобальные политики фонда ВРМ .....	76
8.4 . Объединение фондов в группы ВРМ .....	78
8.5 . Публикация фонда ВРМ .....	79
8.6 . Назначение пользователей доступа.....	82
8.7 . Назначение групп доступа фонду ВРМ .....	82
8.8 . Назначение протоколов фонду ВРМ .....	82
8.9 . Управление сессиями подключенных к фонду ВРМ пользователей .....	83
8.10 . Управление назначенными ВМ.....	83
8.10.1 . Управление состоянием.....	83
8.10.2 . Отправка сообщения в ВМ.....	84
<b>9 . ПРОТОКОЛЫ ДОСТАВКИ .....</b>	<b>85</b>
9.1 . Общие сведения о протоколах доставки.....	85
9.2 . Протокол доставки RDP .....	87
9.2.1 . Прямое подключение по протоколу RDP .....	87
9.2.2 . Подключение через компонент «Шлюз» по протоколу RDP.....	88
9.2.3 . Прямое подключение по протоколу RDP для доступа к ресурсам серверов терминалов ...	90
9.2.4 . Подключение по протоколу RDP для доступа к ресурсам сервера терминалов через компонент «Шлюз».....	92
9.3 . Протокол доставки SPICE .....	94
9.3.1 . Прямое подключение по протоколу SPICE .....	94

9.3.2 .	Подключение через компонент «Шлюз» по протоколу SPICE.....	95
9.3.3 .	Подключение по протоколу SPICE через HTML5 (локальный прокси).....	96
9.3.4 .	Подключение по протоколу SPICE через vdi-viewer .....	97
9.4 .	Протокол доставки VNC .....	98
9.4.1 .	Подключение по протоколу VNC через HTML5 (локальный прокси).....	98
9.5 .	Протокол доставки Loudplay.....	99
9.5.1 .	Прямое подключение по протоколу Loudplay .....	99
9.5.2 .	Подключение через компонент «Шлюз» по протоколу Loudplay .....	101
10 .	<b>СИСТЕМНЫЕ НАСТРОЙКИ</b> .....	103
10.1 .	Общие системные параметры Termidesk .....	103
10.2 .	Параметры безопасности Termidesk.....	104
10.3 .	Назначение служебных функций администраторам.....	105
11 .	<b>МОНИТОРИНГ И УВЕДОМЛЕНИЯ</b> .....	109
11.1 .	Системные параметры мониторинга.....	109
11.2 .	Настройка отправки уведомлений о системных событиях.....	109
11.3 .	Уведомление об ошибках аутентификации в графическом интерфейсе управления .....	110
11.4 .	Шаблон для мониторинга Zabbix .....	110
11.5 .	Отчеты.....	111
12 .	<b>СИСТЕМА АУДИТА</b> .....	113
12.1 .	Системные параметры аудита.....	113
12.2 .	Журналы .....	113
12.3 .	Настройка журналирования.....	114
12.4 .	Просмотр журналов.....	114
13 .	<b>РЕЖИМ ВЫСОКОЙ ДОСТУПНОСТИ И РАБОТА С СЕРТИФИКАТАМИ</b> .....	117
13.1 .	Настройка менеджера BPM в режиме высокой доступности.....	117
13.2 .	Настройка балансировщика для работы с самоподписанными сертификатами.....	120
13.2.1 .	Создание самоподписанного SSL-сертификата .....	120
13.2.2 .	Настройка nginx для поддержки SSL .....	122

13.2.3 .	Конфигурирование веб-сервера.....	123
14 .	ЭКСПЕРИМЕНТАЛЬНЫЕ ФУНКЦИИ .....	125
14.1 .	Перечень переменных окружения универсального диспетчера.....	125
14.2 .	Управление экспериментальными параметрами Termidesk.....	125
14.3 .	Установка плагинов расширений .....	127
14.4 .	Удаление плагинов расширений.....	128
14.5 .	Откат к предыдущей версии плагина.....	128
15 .	ТИПОВЫЕ НЕИСПРАВНОСТИ .....	130
15.1 .	Нештатные ситуации и способы их устранения .....	130
16 .	ПЕРЕЧЕНЬ ТЕРМИНОВ .....	132
17 .	ПЕРЕЧЕНЬ СОКРАЩЕНИЙ .....	134

## 1 . ОБЩИЕ СВЕДЕНИЯ

### 1.1 . О документе

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

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

### 1.2 . Типографские соглашения

В настоящем документе приняты следующие типографские соглашения:

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



## 2 . ПОЛЬЗОВАТЕЛИ И КОМПОНЕНТЫ TERMIDESK

### 2.1 . Разграничение функций

Предусмотрено следующее разграничение функций по управлению Termidesk:

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

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

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

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

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

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

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

### 2.2 . Схема сетевого взаимодействия компонентов Termidesk

Схема взаимодействия между сетевыми портами и компонентами Termidesk представлена на рисунке.

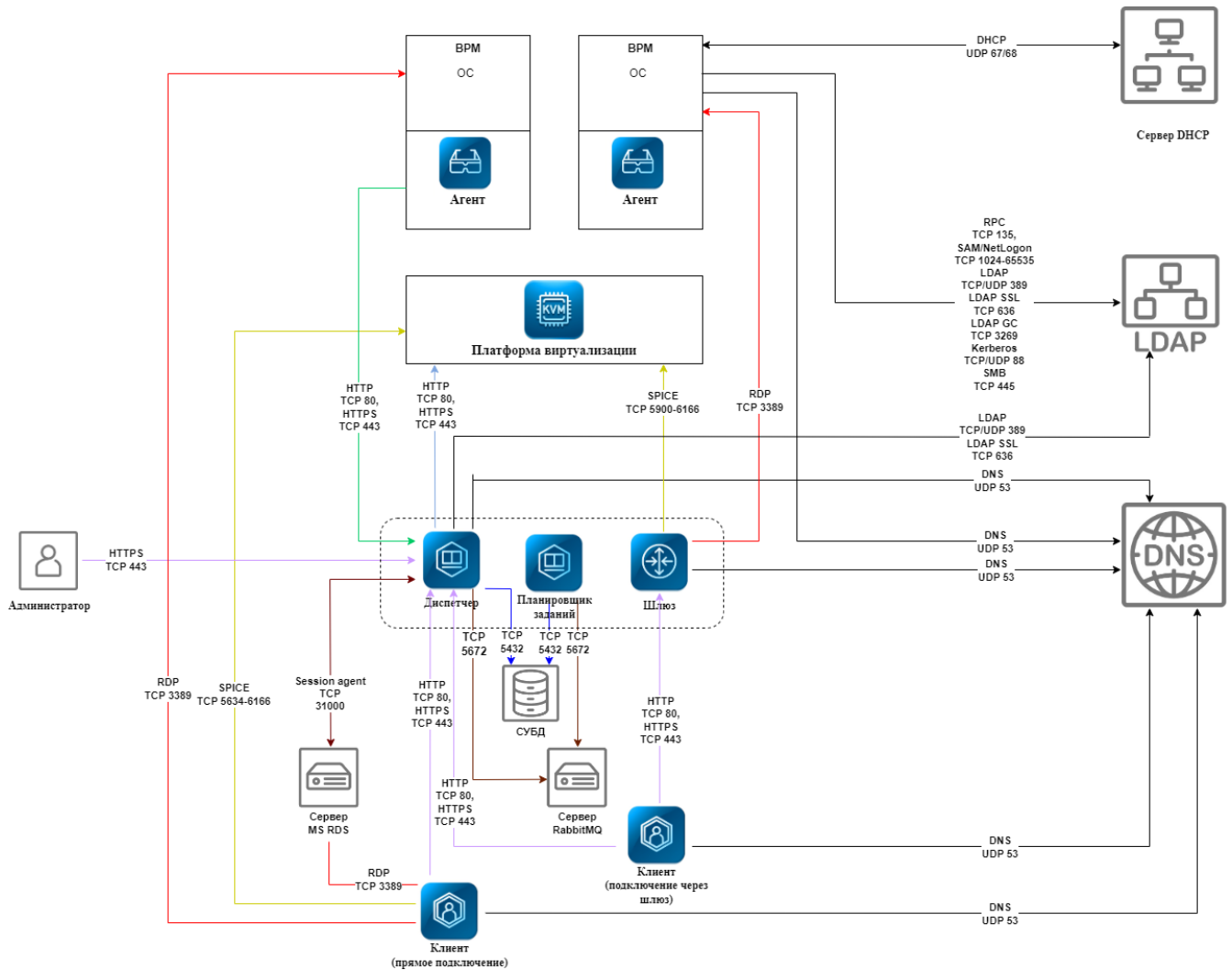


Рисунок 1 – Схема сетевого взаимодействия компонентов Termidesk

Общий перечень узлов и компонентов Termidesk представлен в таблице.

Таблица 1 – Перечень узлов и компонентов

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

Компонент	Наименование на схеме	Узел установки	Наименование пакета установки
«Агент» (агент узла виртуализации)	-	Узел виртуализации (платформа виртуализации)	python3-termidesk-vm <sup>s</sup> d
«Агент» (сессионный агент)	Session agent	Сервер терминалов (Microsoft Windows Server с ролью «Remote Desktop Services» (далее - MS RDS), Terminal Server Astra Linux (далее - STAL))	termidesk-session-agent
«Агент» (видеоагент)	-	ВМ, установка на этапе подготовки образа	termidesk-video-agent
«Агент» (агент виртуальных смарт-карт)	-	ВМ, установка на этапе подготовки образа	termidesk-pcsc-vscard
«Клиент»	Клиент	Рабочее место пользователя (пользовательская рабочая станция)	termidesk-client
«Оркестратор»	-	Отдельный узел для установки, применяется в облачной конфигурации	termidesk-orchestrator
«Сервер терминалов»	-	Сервер терминалов Astra Linux (STAL)	stal

### 2.3 . Последовательность сетевых запросов компонентов Termidesk

Последовательность сетевых запросов с указанием перечня портов для компонентов Termidesk и элементов инфраструктуры представлена на рисунке.

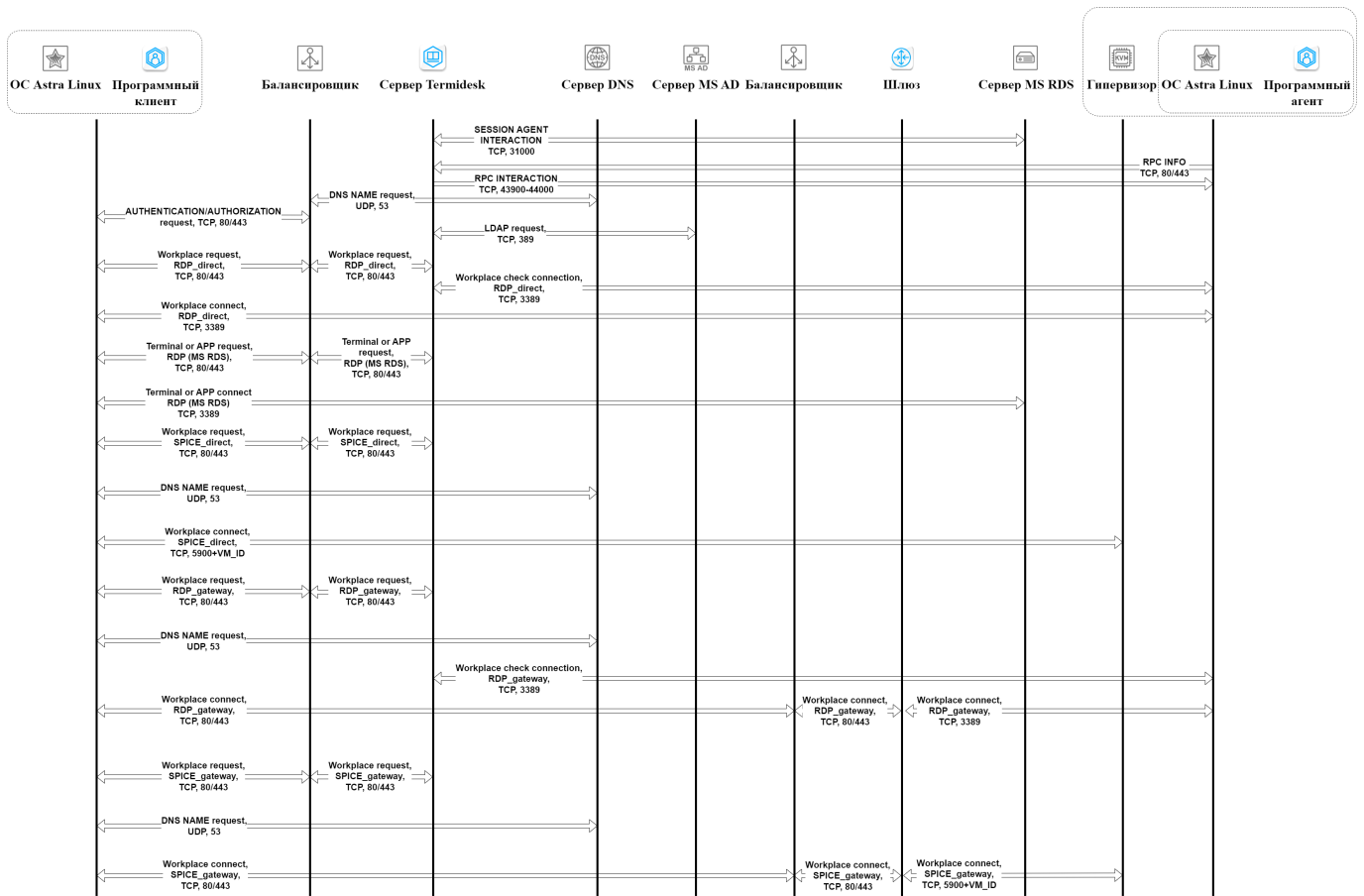


Рисунок 2 – Общая последовательность сетевых запросов

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

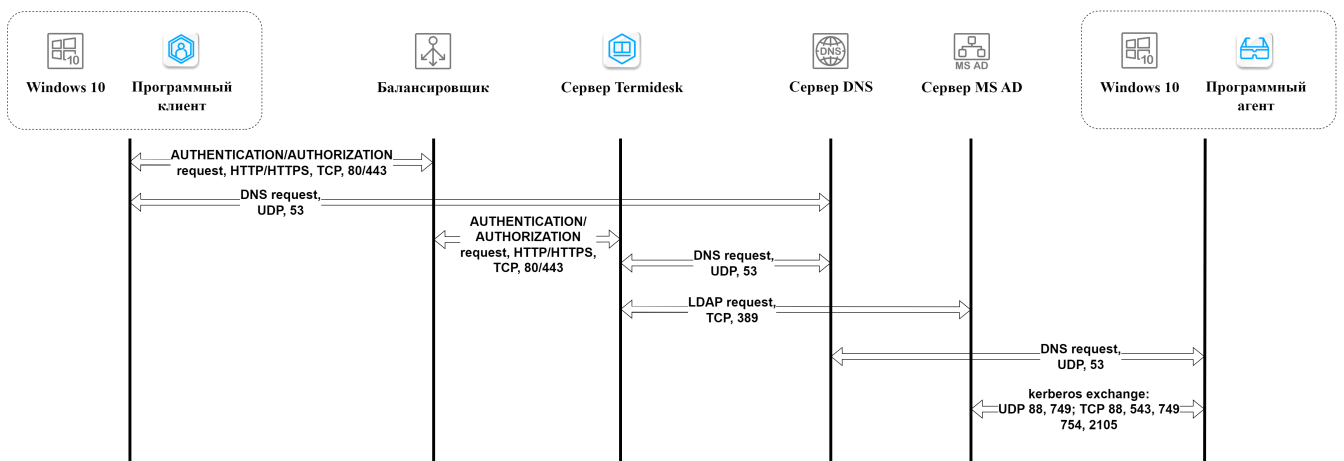


Рисунок 3 – Последовательность сетевых запросов при аутентификации и авторизации

## 2.4 . Перечень сетевых портов компонентов Termidesk

Перечень сетевых портов, используемых компонентами Termidesk, приведен в таблице.

Таблица 2 – Перечень сетевых портов, используемых компонентами Termidesk

Служба	Протокол	Порт
<b>«Универсальный диспетчер»</b>		
HTTP	TCP	80
LDAP	TCP/UDP	389
HTTPS	TCP	443
LDAP SSL	TCP	636
AMQP (RabbitMQ)	TCP	5672
POSTGRESQL	TCP	5432
VDI (termidesk-vdi)	TCP	8000
SESSION AGENT (TermideskSessionAgent)	TCP	31000
RPC INTERACTION	TCP	43900-44000
DNS	UDP	53
<b>«Менеджер рабочих мест»</b>		
POSTGRESQL	TCP	5432
AMQP (RabbitMQ)	TCP	5672
<b>«Шлюз»</b>		
HTTP	TCP	80
HTTPS	TCP	443
RDP	TCP	3389
WSPROXY (termidesk-wsproxy)	TCP	5099
SPICE	TCP	5900-6166
DNS	UDP	53
<b>«Агент» (агент BPM)</b>		
HTTP	TCP	80
Kerberos	TCP/UDP	88
RPC	TCP	135
LDAP	TCP/UDP	389
HTTPS	TCP	443

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

### 3. НАЧАЛО РАБОТЫ

#### 3.1 . Последовательность ввода в действие

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

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

 Базовое ВРМ - прототип будущих ВРМ.

- запуск панели управления Termidesk и добавление поставщика ресурсов в Termidesk;
- добавление домена аутентификации (при необходимости, если в инфраструктуре используются серверы каталогов);
- создание шаблона ВРМ в Termidesk;
- создание и настройка фонда ВРМ в Termidesk;
- добавление пользователей, групп, протоколов доставки в Termidesk;

- выполнение публикации настроенного фонда ВРМ в Termidesk.

### 3.2 . Подготовка базового шаблона ВМ на примере ПК СВ Брест

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

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

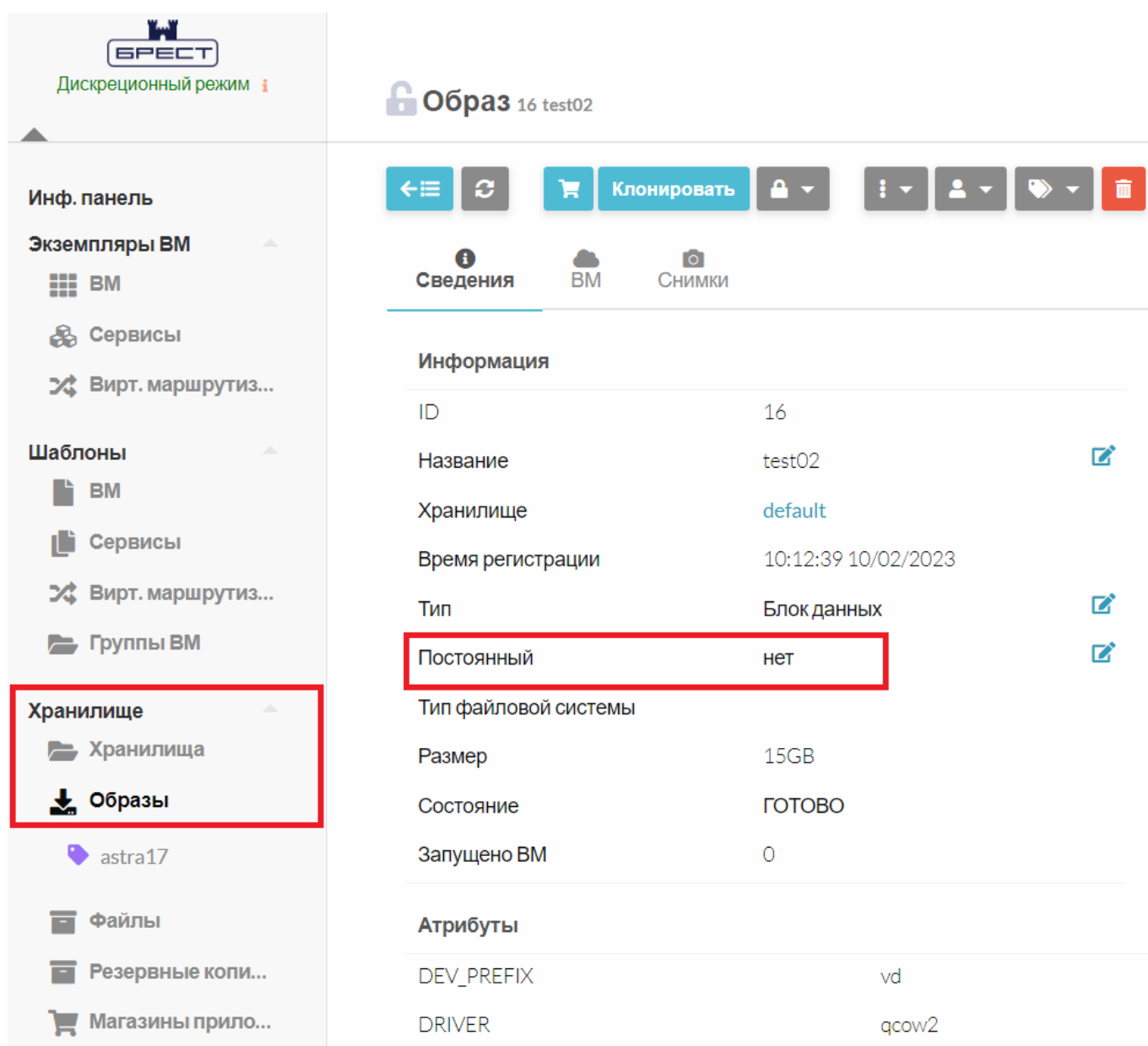


Рисунок 4 – Окно выбора типа подключаемого образа в ПК СВ Брест



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

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

Укажите параметры нового образа

← Сброс Создать

Образ

Мастер настройки Расширенный

Название: astra

Описание:

Тип: Общий блок данных хранилища

Хранилище: 100:aaa

Этот образ является постоянным: Да

Расположение образа

Путь/URL  Закачать  Пустой образ диска

Размер: ГБ

Расширенные настройки

Шина: Virtio

Целевое устройство:

Формат: qcow2

Файловая система: --

Рисунок 5 – 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», затем в поле «Метод дискового резервирования» выбрать значение «Thin»;

Создать шаблон VM

← Сброс Создать

Мастер настройки Расширенный

Общие Хранилище Сеть ОС и ЦП Ввод/Вывод Действия Контекст Расписание Группа VM Метки NUMA

ДИСК 0

Образ  Временный диск

Вы выбрали следующий образ: test02

ID	Название	Владелец	Группа	Хранилище	Тип	Статус	Кол-во VM
17	TDSK_astra17-1_...	bradmin02	brestdadmins	default	Блок данных	ИСПОЛЬЗУЕТСЯ	1
16	test02	bradmin02	brestdadmins	default	Блок данных	ГОТОВО	0
10	alseGold02	bradmin02	brestdadmins	default	ОС	ГОТОВО	0
2	termidesk-data	bradmin02	brestdadmins	default	Блок данных	ИСП. СОХР.	1
0	Astra-1.7.8-03.11...	bradmin02	brestdadmins	default	CDROM	ГОТОВО	0

10 Показаны элементы списка с 1 по 5 из 5

Расширенные настройки

Образ

ID Образа:

Имя образа:

ID владельца образа:

Имя пользователя владельца образа:

Целевое устройство:

Только для чтения:

Шина:

Дисковый контроллер:

Метод дискового резервирования:

Кэш:

Политика ввода-вывода:

Команды TRIM & UNMAP:

Размер при создании экземпляра:  ГБ

Рисунок 6 – Окно назначения расширенных параметров диска шаблона VM

- в настройках шаблона VM следует перейти в «Ввод/Вывод», затем в поле «Средства графического доступа» выбрать значение «SPICE», а в поле «Видеокарта» выбрать значение «QXL»;

### Создать шаблон VM

←
Сброс
Создать

Мастер настройки
Расширенный

---

**Средства графического доступа**

Отсутствует
  VNC /VMRC /GUAC
  SDL
  SPICE

Слушать на IP

Видеокарта

Количество видеокарт 
 Количество мониторов

Порт сервера 
 Раскладка клавиатуры

Команда

**Устройства ввода**

Тип 
 Шина 
Добавить

Рисунок 7 – Окно назначения средств графического доступа шаблона VM

- в случае многомониторной конфигурации необходимо в выпадающем списке «Количество мониторов» выбрать соответствующее значение для гостевой ОС Astra Linux, а в выпадающем списке «Количество видеокарт» выбрать соответствующее значение для гостевой ОС Windows;
- в настройках шаблона VM перейти во вкладку «ОС и ЦП», в поле «Архитектура CPU» следует оставить значение по умолчанию (не менять);
- в случае, если необходим автоматический запуск VM, то после создания шаблона VM в панели управления ПК СВ Брест следует перейти в созданный шаблон и задать для параметра «Служебная VM» значение «Да». 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 8 – Расположение параметра «Служебная VM»

### 3.3 . Подготовка базового ВРМ

#### 3.3.1 . Обязательные настройки

Для подготовки необходимо:

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

Настройка гостевой ОС сводится к выполнению следующих требований:

- для гостевой ОС Windows: должен быть отключен режим гибернации;
- для гостевой ОС Windows: отключить выключение дисплея и жесткого диска в дополнительных параметрах схемы электропитания;
- для гостевой ОС Windows: установить приложения qemu-guest-agent for Windows и spice-guest-tools;

- для гостевой ОС Windows: включить возможность удаленного подключения по протоколу RDP. Для включения доступа по протоколу RDP в меню «Пуск» нужно выбрать путь «Параметры - Система - Удаленный рабочий стол» и нажать экранную кнопку **[Включить удаленный рабочий стол]**. Также снять галочку в экранном поле «Разрешить подключения только с компьютеров, на которых работает удаленный рабочий стол с проверкой подлинности на уровне сети» (рекомендуется выполнить для ОС Windows 7, а также при подключении по протоколу RDP с пользовательской рабочей станции на основе ОС Linux);
- для гостевой ОС Astra Linux: установить пакеты `qemu-guest-agent,spice-vdagent,xserver-xorg-video-qxl`. Установить эти пакеты можно командой:

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

где:

-y - ключ для пропуска подтверждения установки.

- для гостевой ОС Astra Linux: установить пакет `xrdp` для корректной работы подключения по протоколу RDP к ВРМ. Установить этот пакет можно командой:

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

- для гостевой ОС Astra Linux: для штатного выключения ВРМ файл `/etc/acpi/events/powerbtn-acpi-support` должен быть приведен к виду:

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

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

**⚠** Для ввода ВРМ с ОС Astra Linux в домен MS AD необходимо в базовое ВРМ установить пакет `astra-ad-sssd-client`.  
 Для ввода ВРМ с ОС Astra Linux в домен FreeIPA необходимо в базовое ВРМ установить пакет `astra-freeipa-client`.  
 Базовое ВРМ в домен при этом вводить не нужно: процесс ввода контролируется параметрами гостевых ОС (см. подраздел **Управление параметрами гостевых ОС в Termidesk**), которые указываются при создании фонда ВРМ (см. подраздел **Добавление фонда ВРМ**).

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

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

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

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

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

- после изменения настроек выполнить перезапуск службы сети:

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

Для гостевой ОС Linux, отличной от Astra Linux, при необходимости ввода BPM в домен FreeIPA нужно внести изменения в файл `/usr/lib/python3.6/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 -Fz '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
```

### 3.3.2 . Автоматическое масштабирование экрана в ОС Astra Linux

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

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

Для настройки автоматического масштабирования экрана необходимо:

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

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

- перезапустить сервис udev командой:

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

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

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

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

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

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

#Get current and preferred display resolutions
    for MON in $ACTMONS
    do
        #Get preferred display resolution
        PREFRES=$(xrandr | awk -v monpref="$MON connected" '/connected/ {p = 0} $0 ~ monpref
        {p = 1} p' | awk '/+/ {print $1;}' | sed -n '2~2p')
        #Get current display resolution
        CURNRES=$(xrandr | awk -v moncurn="$MON connected" '/connected/ {p = 0} $0 ~ moncurn
        {p = 1} p' | awk '/*/ {print $1;}' )
        if [[ $CURNRES != $PREFRES ]];
        then
            if [[ $MON == $PRIMARYMON ]];
            then
                xrandr --output $MON --auto
```

```

        logger -p local0.notice -t ${0##*/}[$$] "$MON primary display change
resolution to preferred $PREFRES"
    else
        xrandr --output $MON --left-of $PRIMARYMON --auto
        logger -p local0.notice -t ${0##*/}[$$] "$MON display change resolution to
preferred $PREFRES and left of $PRIMARYMON"
    fi
else
    logger -p local0.notice -t ${0##*/}[$$] "$MON display is already using preferred
resolution $PREFRES"

fi
done
done

```

- сделать файл исполняемым при помощи команды:

```

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

```

Для масштабирования экрана приветствия необходимо выполнить:

- заблокировать автостарт kscreen, переименовав расширение или удалив данные файлы из указанных директорий:
 

	/usr/share/fly-dm/autostart/greeter/
kscreend_autostart.desktop,	/usr/share/fly-dm/preload/greeter/
kscreend_preload.desktop;	
- сделать символическую ссылку на ярлык для автозапуска spice-vdagent для экрана приветствия:

```

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

```

- перезапустить процесс fly-dm командой:

```

:~$ sudo systemctl restart fly-dm

```

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



## 4. ПОСТАВЩИКИ РЕСУРСОВ

### 4.1 . Общие сведения о поставщиках ресурсов

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

Поддержка некоторых поставщиков ресурсов может добавляться в режиме экспериментальных функций или при помощи плагинов расширений.

В Termidesk поддерживаются следующие поставщики ресурсов:

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

Графический интерфейс управления Termidesk обеспечивает следующие операции управления поставщиками ресурсов:

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

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

Каждый поставщик ресурсов описывается перечнем параметров, требуемых Termidesk для получения идентификаторов субъектов и информации о полномочиях. Проверить корректность указанных параметров можно при помощи экранной кнопки **[Тест]**, расположенной в том же окне. Для сохранения параметров конфигурации необходимо использовать экранную кнопку **[Сохранить]**.

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

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

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

## 4.2 . Добавление поставщика ресурсов ПК СВ Брест

### 4.2.1 . Получение и добавление файла keytab

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

Действия на контроллере домена (например, FreeIPA):

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

```
~$ sudo kinit admin
```

- выполнить команду для добавления узла:

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

где:

`--force` - флаг для принудительного создания;

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

`IP_disp1.termidesk.local` - IP-адрес сервера, где установлен Termidesk,

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

**⚠** Мнимый FQDN означает, что он не обязательно должен быть привязан к действительно существующему узлу.

- выполнить команду добавления службы для нового сервисного аккаунта:

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

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

```

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

где:

- s freeipa.termidesk.local - задание FQDN сервера-контроллера домена FreeIPA;
- p HTTP/disp.termidesk.local - указание ранее созданного субъекта-службы;
- k /home/user/termidesk.keytab - сохранение в файл termidesk.keytab;

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

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

```

:~$ sudo scp termidesk.keytab localuseruser@IP_disp.termidesk.local:termidesk.keytab
    
```

где:

- localuser - имя пользователя целевого узла;
- IP\_disp.termidesk.local - IP-адрес целевого узла.

После передачи файла на узле Termidesk необходимо выполнить следующее:

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

```

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

- сделать владельцем этого файла пользователя termidesk:

```

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

- перезапустить службу termidesk-vdi:

```

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

#### 4.2.2 . Перечень параметров для добавления

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

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

Таблица 3 – Данные для добавления поставщика ресурсов ПК СВ Брест

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов

Параметр	Описание
«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
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (полученный ранее <code>termidesk.keytab</code> , <code>/etc/opt/termidesk-vdi/termidesk.keytab</code> )
«Домен»	Идентификатор области Kerberos для аутентификации
«Порт»	Номер порта для подключения к API платформы виртуализации. По умолчанию используется порт 2633, если на платформе виртуализации не было указано иное
«Использовать SSL»	Включение использования протокола SSL
«Проверка SSL»	Включение строгой проверки SSL
«Запуск VM от имени служебного пользователя»	Переключатель для запуска VM на платформе виртуализации от имени служебного пользователя. Если данный параметр активирован, то параметры «Делегация запуска VM», «Логин делегата», «Пароль делегата» настраивать не нужно
«Логин»	Субъект, имеющий полномочия для управления платформой виртуализации
«Пароль»	Пароль субъекта с полномочиями для управления платформой виртуализации
«Токен»	Электронный ключ субъекта с полномочиями для управления платформой виртуализации, который нужно скопировать из интерфейса управления платформой виртуализации. Для этого следует зайти в интерфейс управления платформой виртуализации с помощью логина и пароля указанного пользователя, в главном меню развернуть раздел «System» и выбрать строку «Users». В появившемся окне выбрать указанного пользователя, перейти на вкладку «Auth» и нажать экранную кнопку <b>[Manage login tokens]</b> , в появившейся форме скопировать значение из поля «Token»
«Делегация запуска VM»	Включение делегирования прав на запуск VM на платформе виртуализации другому пользователю
«Логин делегата»	Субъект, которому делегируется право на запуск VM на платформе виртуализации
«Пароль делегата»	Пароль субъекта, которому делегируется право на запуск VM на платформе виртуализации

Параметр	Описание
«Создавать VM одновременно»	Количество одновременно создаваемых VM на платформе виртуализации
«Время ожидания»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации
«Удалять VM одновременно»	Количество одновременно удаляемых VM с платформы виртуализации

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

### 4.3 . Добавление платформы oVirt/zVirt/RHEV

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

Для добавления в Termidesk платформы oVirt/zVirt/RHEV администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 4 – Данные для добавления платформы oVirt/RHEV

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Версия oVirt»	Выбор используемой версии oVirt
«Адрес oVirt»	IP-адрес или доменное имя платформы виртуализации oVirt
«Логин»	Субъект, имеющий полномочия для управления платформой виртуализации oVirt. Указывается в формате login@internal
«Пароль»	Набор символов, подтверждающий назначение полномочий
«Создавать VM одновременно»	Количество одновременно создаваемых VM на платформе виртуализации oVirt

Параметр	Описание
«Удалять VM одновременно»	Количество одновременно удаляемых VM с платформы виртуализации oVirt
«Время ожидания»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации oVirt

#### 4.4 . Добавление поставщика VMmanager

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

Для добавления в Termidesk поставщика VMmanager администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 5 – Данные для добавления поставщика ресурсов VMmanager

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

#### 4.5 . Добавление поставщика ресурсов VMware vSphere

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

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

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

Таблица 6 – 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
«Использовать SSL»	Форсировать использование протокола SSL
«Логин»	Субъект, имеющий полномочия для управления платформой виртуализации VMware
«Пароль»	Набор символов, подтверждающий назначение полномочий субъекта
«Подготавливать ВМ одновременно»	Количество одновременно создаваемых ВМ на платформе виртуализации VMware
«Удалять ВМ одновременно»	Количество одновременно удаляемых ВМ с платформы виртуализации VMware

Субъект должен иметь привилегии, указанные в таблице.

**ⓘ** 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.

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

Таблица 7 – 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»
«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»



Тип привилегий	Наименование привилегий
«Virtual machine»: «Provisioning»	«Clone virtual machine» «Create template from virtual machine» «Deploy template»
«Virtual machine»: «Snapshot management»	«Create snapshot» «Remove snapshot» «Rename snapshot» «Revert to snapshot»

#### 4.6 . Добавление поставщика vAir

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

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

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

Таблица 8 – Данные для добавления поставщика ресурсов vAir

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

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

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

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

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

Для добавления в Termidesk сервера терминалов администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 9 – Данные для добавления сервера терминалов

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Адрес сессионного агента»	FQDN узла, на котором установлен сессионный агент Termidesk
«Порт сессионного агента»	Номер порта сессионного агента Termidesk. По умолчанию номер порта 31000
«Домен»	Наименование домена для подключения к серверу терминалов
«Логин»	Субъект, имеющий полномочия для управления сервером терминалов
«Пароль»	Набор символов, подтверждающий назначение полномочий

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

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

#### 4.8 . Добавление сервера терминалов (метапровайдер) в качестве поставщика ресурсов

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

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

Алгоритм подготовки для добавления метапровайдера выглядит следующим образом:

- на платформе виртуализации создается VM с гостевой ОС Windows Server (2016 и выше) или ОС Astra Linux Special Edition 1.7 (Server);
- в гостевую ОС устанавливается агент BPM и сессионный агент (см. документ СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»);
- в гостевую ОС устанавливается роль сервера публикации приложений MS RDS или STAL (см. документ СЛЕТ.10001-01 90 07 «Руководство администратора. Настройка компонента «Сервер терминалов»). Необходимые приложения должны быть вручную опубликованы (для MS RDS используется утилита RemoteApp Tool). На этом этапе подготовка завершена, VM выключается;

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

- в графическом интерфейсе управления Termidesk создается поставщик ресурсов с той платформой виртуализации, на которой создана VM сервера публикации приложений (см. раздел **Поставщики ресурсов**);
- в созданном поставщике ресурсов создается шаблон BPM (см. раздел **Виртуальные рабочие места**), в параметре «Базовая VM» выбирается подготовленная VM сервера публикации приложений;

- в графическом интерфейсе управления Termidesk создается сервисный фонд ВРМ для созданного шаблона ВРМ (см. подраздел **Добавление фонда ВРМ**). В сервисном фонде **не** указываются группы пользователей, пользователи, протоколы доставки. Сервисный фонд должен использовать кеш 1 уровня (кеш 2 уровня не используется);

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

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

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

Для добавления в Termidesk сервера терминалов администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 10 – Данные для добавления сервера терминалов (метапровайдер)

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Порт сессионного агента»	Номер порта сессионного агента Termidesk. По умолчанию номер порта 31000
«Фонд»	Выбор <b>сервисного фонда</b> для размещения
«Домен»	Наименование домена для подключения к серверу терминалов
«Логин»	Субъект, имеющий полномочия для управления сервером терминалов

Параметр	Описание
«Пароль»	Набор символов, подтверждающий назначение полномочий

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

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

#### 4.9 . Добавление поставщика ресурсов «Физическая рабочая станция»

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

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

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

Для добавления поставщика ресурсов администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 11 – Данные для добавления физической рабочей станции как поставщика ресурсов

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

#### 4.10 . Добавление поставщика Openstack

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

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

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

Таблица 12 – Данные для добавления поставщика ресурсов Openstack

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

#### 4.11 . Режим техобслуживания поставщика ресурсов

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

Для перевода поставщика ресурсов в режим техобслуживания следует перейти «Компоненты - Поставщики ресурсов» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить».

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

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

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

## 5 . АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

### 5.1 . Общие сведения о доменах аутентификации

Домен аутентификации - источник сведений о субъектах и их полномочиях.

В Termidesk поддерживаются следующие домены аутентификации:

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

Поддержка некоторых доменов аутентификации может добавляться в режиме экспериментальных функций (при помощи плагинов расширений).

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

Каждый домен аутентификации описывается перечнем параметров, требуемых для получения идентификаторов субъектов и информации о полномочиях. Проверить корректность указанных параметров можно при помощи экранной кнопки **[Тест]**, расположенной в том же окне. Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Сохранить]**.

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



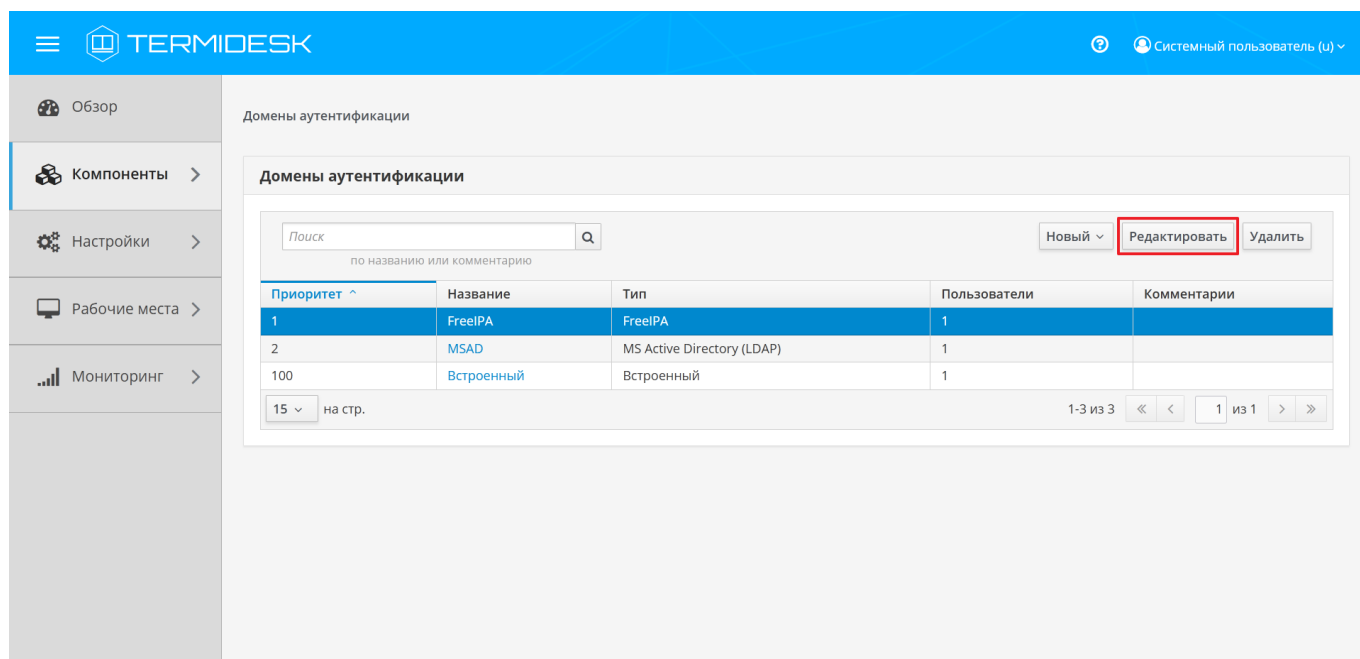


Рисунок 9 – Окно выбора домена аутентификации для редактирования

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

## 5.2 . Добавление аутентификации через FreeIPA

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

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

Таблица 13 – Данные для добавления аутентификации через FreeIPA

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

Параметр	Описание
«Сервисный аккаунт»	Название сервисного аккаунта, созданного при добавлении поставщика ресурсов ПК СВ Брест
«Домен»	Идентификатор области Kerberos для аутентификации
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (файл <code>termidesk.keytab</code> , полученный в соответствии с подразделом <b>Добавление поставщика ресурсов ПК СВ Брест</b> ). Неважно, для какого узла создан keytab, необходимо само его наличие
«Сервер FreeIPA»	FQDN ресурса, являющегося источником сведений о субъектах и их полномочиях
«Проверка SSL»	Проверка использования SSL
«Группа администраторов»	Название группы, членам которой предоставляются функции администрирования Termidesk

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

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

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

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

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

### 5.3 . Добавление аутентификации через ALD

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

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

Таблица 14 – Данные для добавления аутентификации через ALD

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Сервисный аккаунт»	Название сервисного аккаунта, созданного при добавлении поставщика ресурсов
«Домен»	Идентификатор области Kerberos для аутентификации
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (файл keytab, полученный в соответствии с подразделом <b>Добавление поставщика ресурсов ПК СВ Брест</b> ). Неважно, для какого узла создан keytab, необходимо само его наличие
«Группа администраторов»	Название группы, членам которой предоставляются права администрирования Termidesk
«Сервер LDAP (ALD)»	Доменное имя ресурса, являющегося источником сведений о субъектах и их полномочиях
«Таймаут подключения»	Время ожидания (в секундах) ответа ресурса, являющегося источником сведений о субъектах и их полномочиях
«Base DN»	Корень поиска в домене аутентификации

#### 5.4 . Добавление аутентификации через SAML

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

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

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

Таблица 15 – Данные для добавления аутентификации через SAML

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Приоритет использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«ID клиента»	Уникальный идентификатор клиента на сервисе аутентификации SAML
«URL метаданных»	URL для подключения к сервису аутентификации SAML
«Тип биндинга»	Способ отправки ответа сервисом SAML на запрос аутентификации. Поддерживаются следующие типы: HTTP-Redirect, HTTP-POST
«Приватный ключ»	Набор символов приватного ключа для подписания 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)

## 5.5 . Добавление IP-аутентификации

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

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

Таблица 16 – Данные для добавления IP-аутентификации

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

## 5.6 . Добавление аутентификации через MS AD (LDAP)

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

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

Таблица 17 – 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

Параметр	Описание
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Адрес LDAP»	IP-адрес или доменное имя ресурса, являющегося источником сведений о субъектах и их полномочиях
«Порт»	TCP-порт, на котором запущена служба домена аутентификации
«Использовать SSL»	Использовать защищенное соединение при взаимодействии с доменом аутентификации
«Bind DN»	Объект в MS AD (LDAP), имеющий полномочия для доступа к конкретной записи
«Bind DN password»	Набор символов, подтверждающий полномочия объекта по доступу к конкретной записи
«Timeout»	Время ожидания (в секундах) ответа ресурса, являющегося источником сведений о субъектах и их полномочиях
«Base DN»	Корень поиска в домене аутентификации
«User class name»	Атрибут класса пользователя в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «Person»)
«User attr id»	Идентификатор пользователя в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «SamAccountName»)
«User attrs name»	Идентификатор имени пользователя в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «name»)
«Group class name»	Атрибут принадлежности к группе в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «group»)
«Group attr name»	Идентификатор группы, к которой относится субъект в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «cn»)
«Group attr membership»	Идентификатор группы для назначения полномочий субъекту (для корректного заполнения данного поля необходимо указать значение «member»)

### 5.7 . Добавление аутентификации через внутреннюю БД

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

После установки плагина расширения в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Новый]** и выбрать из выпадающего списка «Внутренняя БД, эксперим.».

Для добавления внутренней БД как домена аутентификации администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 18 – Данные для добавления аутентификации через внутреннюю БД

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

### 5.8 . Действия над пользователями в домене аутентификации

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

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

- редактирование;
- удаление;
- просмотр сведений.

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

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

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

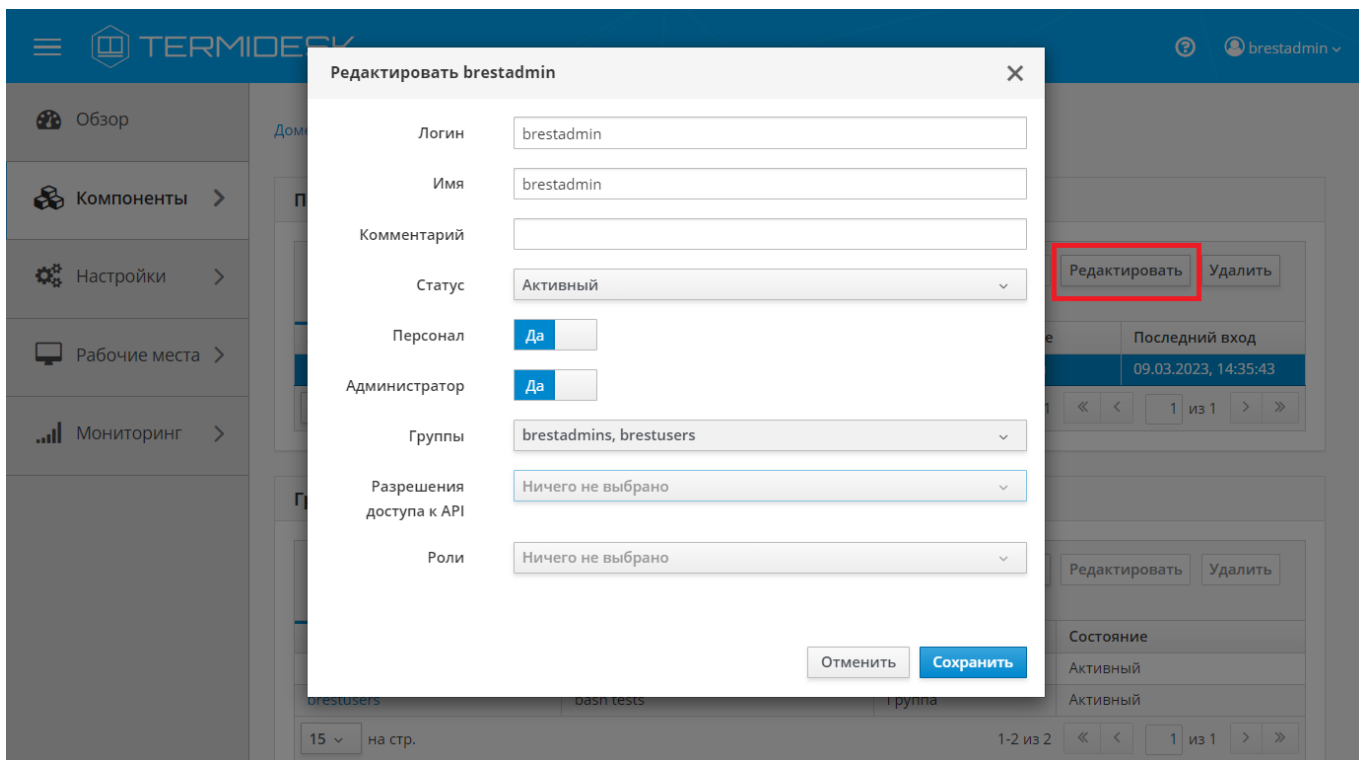


Рисунок 10 – Окно редактирования пользователя домена аутентификации

Для редактирования пользователя администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 19 – Данные для редактирования пользователя домена аутентификации

Параметр	Описание
«Логин»	Идентификатор субъекта в домене аутентификации
«Имя»	Отображаемое имя субъекта в Termidesk
«Комментарий»	Информационное сообщение, используемое для описания назначения пользователя
«Статус»	Характеристика состояния субъекта при доступе к фонду ВРМ
«Персонал»	Служебные функции субъекта при доступе к Termidesk
«Администратор»	Служебные функции субъекта при доступе к графическому интерфейсу управления Termidesk



Параметр	Описание
«Группы»	Наименование групп, используемых для определения разрешений по доступу к фондам ВРМ
«Разрешения доступа к API»	Полномочия для доступа к API-интеграции с системой резервного копирования
«Роли»	Назначение служебной функции указанному пользователю

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

### 5.9 . Управление аутентификацией на основе адресов сети

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


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

Таблица 20 – Данные для добавления аутентификации на основе адресов сети

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

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

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

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

## 6 . ВИРТУАЛЬНЫЕ РАБОЧИЕ МЕСТА

### 6.1 . Общие сведения о ВРМ

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

Termidesk выполняет подготовку ВРМ на основе заданных шаблонов ВРМ. Каждый поставщик ресурсов поддерживает свой набор типов шаблонов ВРМ.

Поддерживаемый в Termidesk список типов шаблонов ВРМ приведен ниже:

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

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

Далее в открывшемся окне следует нажать на экранную кнопку **[Новый]**, а затем из выпадающего списка выбрать поддерживаемый в Termidesk способ формирования шаблона ВРМ.

Созданные шаблоны ВРМ можно редактировать, для этого необходимо выбрать шаблон, а затем нажать на экранную кнопку **[Редактировать]**.

Созданные шаблоны можно удалить, для этого необходимо выбрать шаблон, а затем нажать на экранную кнопку **[Удалить]**.

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

### 6.2 . Шаблоны ВРМ для ПК СВ Брест

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

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

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

Таблица 21 – Данные для добавления шаблонов на основе клонов для ПК СВ Брест

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

### 6.2.2 . Шаблон на базе снимота для ПК СВ Брест

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

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

Таблица 22 – Данные для добавления шаблона на базе снимота для ПК СВ Брест

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

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

### 6.3 . Шаблоны ВРМ для платформ oVirt/RHEV

#### 6.3.1 . Шаблон на основе связанного клона для oVirt/RHEV

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

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

Таблица 23 – Данные для добавления шаблона на основе связанного клона для oVirt/RHEV

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

Параметр	Описание
«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 (как строчных, так и прописных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера текстового наименования, используемого в идентификаторе каждого ВРМ

### 6.3.2 . Шаблон на основе статичной ВМ для oVirt/RHEV

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

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

Таблица 24 – Данные для добавления шаблона на основе статичной ВМ для oVirt/RHEV

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

### 6.4 . Шаблоны ВРМ для платформ VMware vSphere

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

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

Таблица 25 – Данные для добавления шаблона для VMware vSphere

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

## 6.5 . Шаблоны ВРМ для серверов терминалов

### 6.5.1 . Шаблон ВРМ для доступа к серверу терминалов MS RDS

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

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

Таблица 26 – Данные для добавления шаблона для доступа к терминалу MS RDS

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

### 6.5.2 . Шаблон BPM для доступа к опубликованным приложениям MS RDS

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

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

Таблица 27 – Данные для добавления шаблона для доступа к приложениям MS RDS

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

### 6.5.3 . Шаблон BPM для доступа к серверу терминалов STAL

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

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

Таблица 28 – Данные для добавления шаблона для доступа к терминалу STAL

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM

Параметр	Описание
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона ВРМ

#### 6.5.4 . Шаблон ВРМ для доступа к опубликованным приложениям STAL

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

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

Таблица 29 – Данные для добавления шаблона для доступа к приложениям STAL

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

#### 6.6 . Шаблон ВРМ для метапровайдера

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

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

Таблица 30 – Данные для добавления шаблона для доступа к метапровайдеру

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



## 6.7 . Шаблоны ВРМ для физической рабочей станции

### 6.7.1 . Шаблон ВРМ на основе одного статического IP-адреса

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


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

Таблица 31 – Данные для добавления шаблона ВРМ на основе одного IP-адреса

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

### 6.8 . Шаблон ВРМ на основе множественных IP-адресов

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

 Данный шаблон использовать не рекомендуется.

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

Таблица 32 – Данные для добавления шаблона ВРМ на основе множественных IP-адресов

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

## 6.9 . Настройка переносимых профилей

### 6.9.1 . Общие сведения

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

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

Действия по настройке переносимых профилей сводятся к следующей последовательности шагов:

- 1) создание базового образа диска для профилей в ПК СВ Брест;
- 2) задание созданному образу атрибута TDSK\_SHARED\_TYPE со значением PRIVATE;
- 3) настройка модуля PAM (pam\_tdsk) в базовом ВРМ;
- 4) включение механизма переносимых профилей в Termidesk;
- 5) включение в настройках глобальных политик Termidesk политики «Отделяемый пользовательский профиль».

### 6.9.2 . Создание базового образа диска в ПК СВ Брест

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

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

**⚠** При создании образа на шине Virtio может возникнуть сообщение об ошибке «Error attaching new VM Disk: Could not attach /var/lib/one/datastores/0/248/disk.2 (vdb) to one-248» при подключении диска в ПК СВ Брест версии 2.9.

В случае возникновения такой ошибки нужно изменить атрибут DEV\_PREFIX в свойствах образа диска.

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

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

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

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

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

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

- преобразовать новый раздел диска в формат `ext4`:

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

- проверить успешность создания диска:

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

где:

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

### 6.9.3 . Задание атрибутов созданному диску

Для задания атрибутов созданному ранее диску необходимо:

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

Image 29 share\_home

← ☰
↻
↪ Marketplace
Clone
⋮ ▾
👤 ▾
🏷️ ▾
🗑️

📘 Info
☁️ VMs
📷 Snapshots

Information

ID	29
Name	share_home
Datastore	default
Register time	12:06:40 27/04/2021
Type	OS
Persistent	yes
Filesystem type	-
Size	1GB
State	READY
Running VMS	0

Attributes

DEV_PREFIX	hd
DRIVER	qcow2
TDSK_SHARED_TYPE	PRIVATE

Рисунок 11 – Окно просмотра ID диска в ПК СВ Брест

**6.9.4. Настройка модуля RAM в базовом ВРМ**

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

- выполнить подготовку базового ВРМ (см. подраздел **Подготовка базового ВРМ**);

- создать файл `/usr/share/pam-configs/pam_tdsk` со следующим содержимым:

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

**⚠** 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`:

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

### 6.9.5 . Активация механизма переносимых профилей в Termidesk

Для активации механизма переносимых профилей необходимо выполнить следующее:

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

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

**⚠** При наличии нескольких дисков необходимо перечислить их через запятую.

- перезапустить службу `termidesk-vdi`:

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

- убедиться, что необходимая переменная установлена:

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

Вывод команды должен включать установленную переменную, например TDSK\_AUTOFS\_IMAGES\_ID=29.

### 6.9.6 . Активация политики в интерфейсе Termidesk


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

### 6.10 . 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 ВРМ или терминальный сервер.

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

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

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

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

### 6.11 . Перенаправление смарт-карты

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

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

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

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

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

## 6.12 . Настройка технологии единого входа в гостевой ОС VM

### 6.12.1 . Общие сведения

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

**⚠** Данный функционал является экспериментальным, однако его активация через экспериментальные параметры Termidesk не требуется.

Действия по настройке SSO сводятся к следующей последовательности шагов:

- 1) активация модуля PAM (`pam_tdsd`) агента BPM;
- 2) включение механизма автоматической авторизации в гостевую ОС.

### 6.12.2 . Активация модуля PAM

Модуль PAM может быть активирован двумя способами:

- 1) через указание записи в цепочке авторизации PAM для графической подсистемы. Например, для гостевой ОС Astra Linux нужно 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_tdsd
```

Пример итогового файла:

```
##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

@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
    
```

2) через создание файла `/usr/share/pam-configs/termidesk-ss0` со следующим содержимым:

```

Name: Termidesk SS0
Default: yes
Priority: 301
Auth-Type: Primary
Auth:
sufficient pam_exec.so expose_authtok quiet /usr/bin/pam_tdsk
    
```

**⚠** Приоритет `Priority: 301` необходим для того, чтобы цепочка авторизации начиналась с модуля `/usr/bin/pam_tdsk`.

После активации модуля PAM одним из перечисленных выше способов необходимо выполнить обновление профилей PAM при помощи команды:

```

:$ sudo pam-auth-update
    
```

После выполнения команды в гостевой ОС AstraLinux обновится файл `/etc/pam.d/common-auth`.

### 6.12.3. Включение механизма автоматической авторизации

Механизм автоматической авторизации может быть включен двумя способами:

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



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

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

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

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

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

[Service]
ExecStartPre=/bin/bash -c /usr/bin/fly-dm-prepare.sh
ExecStart=/usr/bin/fly-dm vt7


IgnoreSIGPIPE=no

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

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

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

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

 Данный способ (второй) является предпочтительным.

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

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

Затем выполнить перезапуск службы:

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

#### 6.12.4. Активация технологии единого входа на сервере терминалов MS RDS

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

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

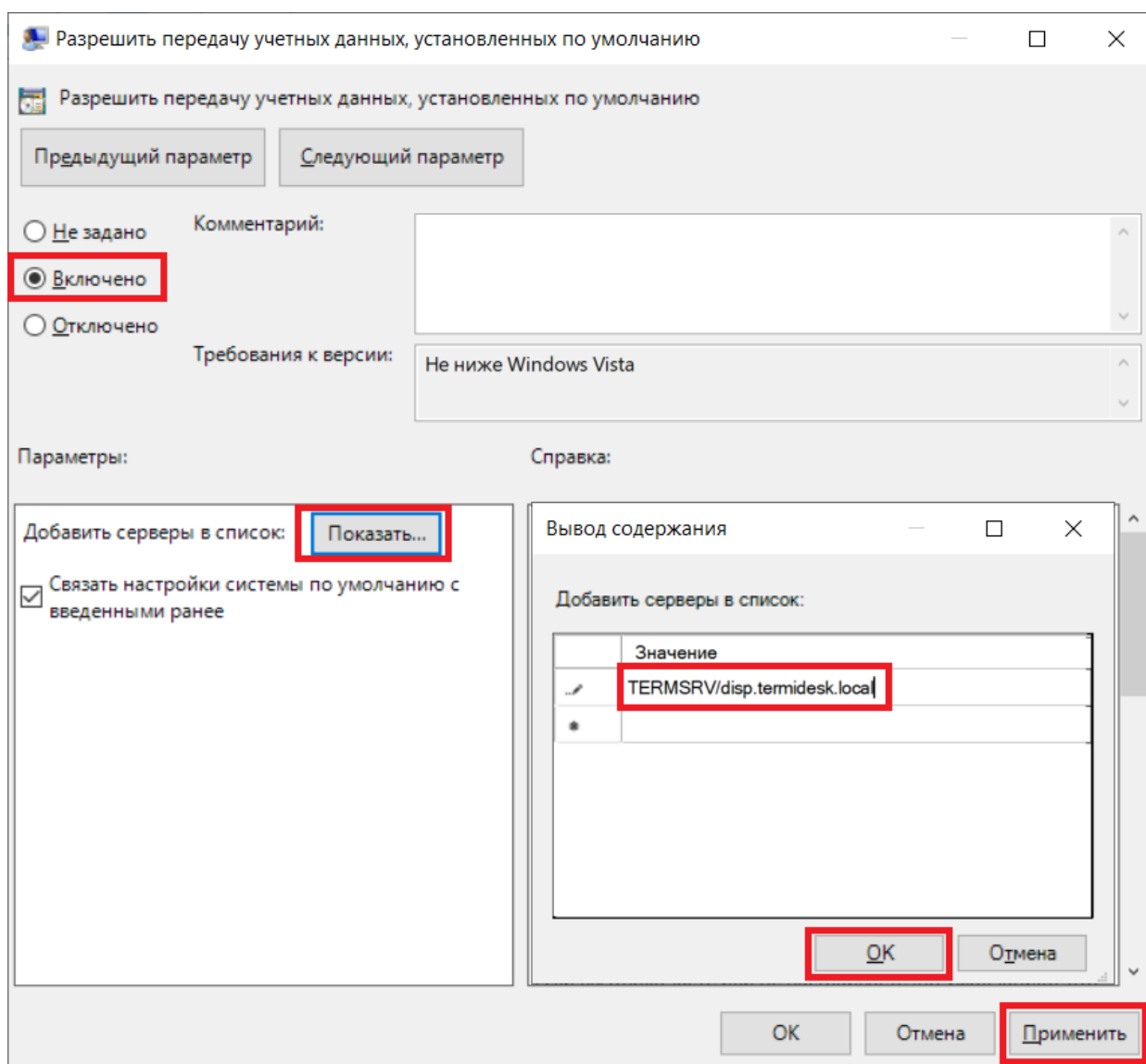


Рисунок 12 – Редактирование параметра «Разрешить передачу учетных данных, установленных по умолчанию» групповых политик

- 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», где `disp.termidesk.local` - имя сервера Termidesk. Далее нажать экранные кнопки **[ОК]** и **[Применить]**;
- в редакторе групповой политики перейти «Конфигурация компьютера - Административные шаблоны - Компоненты Windows - Службы удаленных рабочих столов - Клиент подключения к удаленному рабочему столу», выбрать параметр «Запрашивать учетные данные на клиентском компьютере» и присвоить ему значение «Отключено».

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

## 6.13 . Настройка аутентификации пользователей ВРМ через файл

### 6.13.1 . Общие сведения

Действия по настройке аутентификации пользователей ВРМ 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.

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

### 6.13.2 . Настройка модуля PAM

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

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

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

session required pam_parsec_mac.so unshare_root_only
session required pam_limits.so
session required pam_loginuid.so

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

### 6.13.3 . Включение механизма автоматической авторизации

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

## 7 . УПРАВЛЕНИЕ ПАРАМЕТРАМИ ГОСТЕВЫХ ОС

### 7.1 . Управление параметрами гостевых ОС в Termidesk

#### 7.1.1 . Общие сведения

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


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

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

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

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

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

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

### 7.1.2 . Параметры гостевой ОС Windows

#### 7.1.2.1 . Конфигурация без домена

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

Таблица 33 – Данные для гостевой ОС Windows без ввода в домен

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

Параметр	Описание
«Длительность сессии пользователя»	Время (в секундах), которое ожидает Termidesk, прежде чем будет запущена процедура принудительного выхода пользователя из ОС

### 7.1.2.2 . Конфигурация при вводе в домен MS AD

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

Таблица 34 – Данные для гостевой ОС Windows при вводе в домен MS AD

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен»	Доменное имя службы каталогов MS AD
«Аккаунт»	Идентификатор субъекта, имеющий полномочия по добавлению ВРМ к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий
«ОУ»	Идентификатор организационной единицы, в которую будет добавлены ВРМ
«Длительность сессии пользователя»	Время (в секундах), которое ожидает Termidesk, прежде чем будет запущена процедура принудительного выхода пользователя из ОС

### 7.1.3 . Параметры гостевой ОС Linux

#### 7.1.3.1 . Конфигурация без домена

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

Таблица 35 – 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


Параметр	Описание
«Длительность сессии пользователя»	Время (в секундах), которое ожидает Termidesk, прежде чем будет запущена процедура принудительного выхода пользователя из ОС

### 7.1.3.2 . Конфигурация при вводе в домен MS AD

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

Таблица 36 – 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»	Идентификатор домена MS AD
«Аккаунт»	Идентификатор субъекта, имеющий полномочия по добавлению ВРМ к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий
«ОУ»	Идентификатор организационной единицы, в которую будет добавлены ВРМ (опционально)
«Длительность сессии пользователя»	Время (в секундах), которое ожидает Termidesk, прежде чем будет запущена процедура принудительного выхода пользователя из ОС

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


### 7.1.3.3 . Конфигурация при вводе в домен FreeIPA

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

Таблица 37 – 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»	Идентификатор субъекта, имеющий полномочия по добавлению BPM к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий
«Длительность сессии пользователя»	Время (в секундах), которое ожидает Termidesk, прежде чем будет запущена процедура принудительного выхода пользователя из ОС

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

#### 7.1.3.4 . Конфигурация при вводе в домен ALD

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

Таблица 38 – 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»	Идентификатор субъекта, имеющий полномочия по добавлению BPM к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий
«Длительность сессии пользователя»	Время (в секундах), которое ожидает Termidesk, прежде чем будет запущена процедура принудительного выхода пользователя из ОС

#### 7.1.4 . Действие при выходе пользователя из ОС

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

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


- «Удалять рабочее место» - удалить BPM после выхода пользователя;



- «Нет» - не производить действий с ВРМ (сохранять состояние).

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

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

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

### 7.1.5 . Изменение изображения гостевых ОС

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

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

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

Для редактирования пометить добавленный объект, а затем нажать экранную кнопку **[Редактировать]**.

Для удаления пометить добавленный объект, а затем нажать экранную кнопку **[Удалить]**.

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

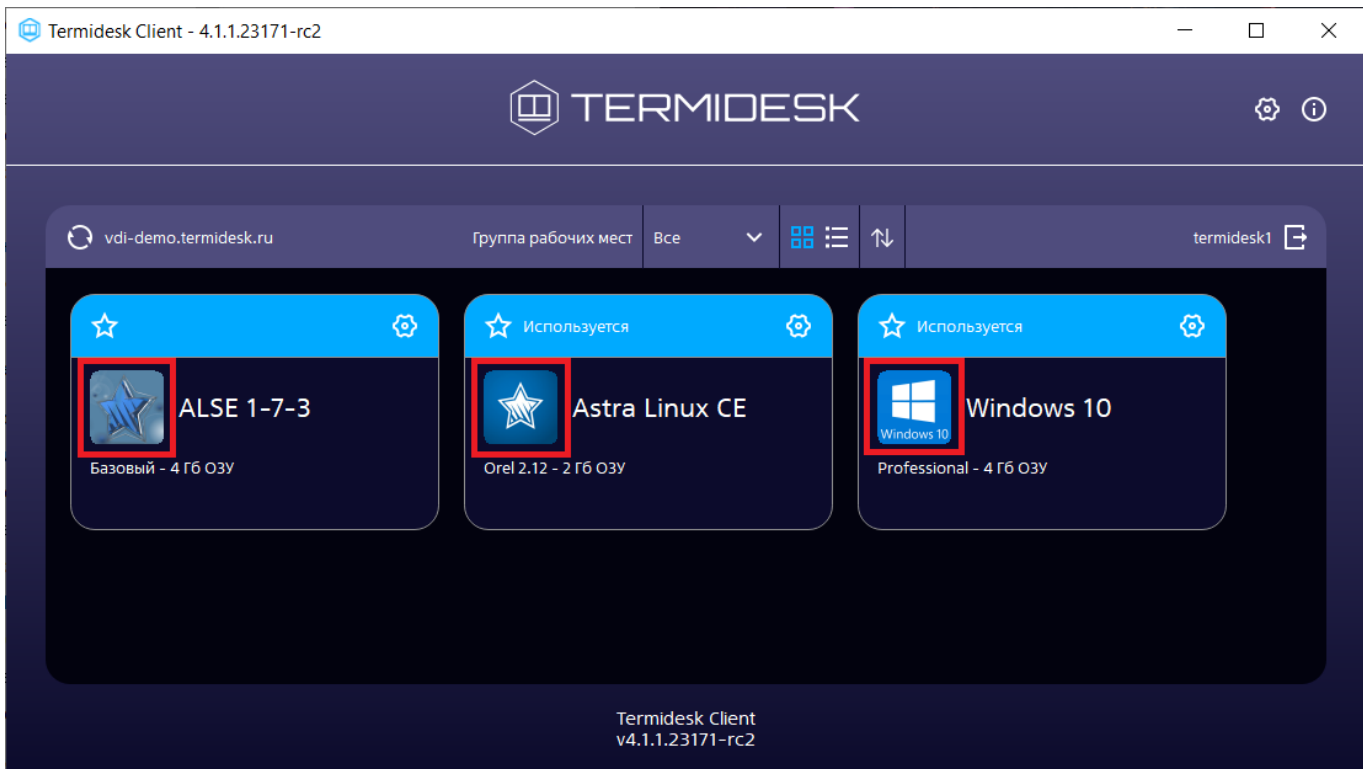


Рисунок 13 – Отображение назначенных изображений в сеансе пользователя

## 8. ФОНД РАБОЧИХ МЕСТ

### 8.1 . Общие сведения о фонде ВРМ

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

Для добавления нового фонда ВРМ в графическом интерфейсе управления следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Новый]**.

Созданные фонды можно редактировать, для этого нужно пометить название фонда, а затем нажать экранную кнопку **[Редактировать]**.

Созданные фонды можно удалить, для этого нужно пометить название фонда, а затем нажать экранную кнопку **[Удалить]**.

Экранная кнопка **[Политики]**, доступная при выборе названия фонда, открывает параметры выбранного фонда. Совокупность параметров аналогична представленной в «Настройки - Глобальные политики».

После добавления фонда ВРМ можно перейти к его детальному просмотру. Для этого в сводной таблице окна «Фонды» в столбце «Название» следует нажать на наименование фонда ВРМ.

На открывшейся странице будут представлены следующие разделы:

- «Рабочие места» – список ВМ и информация о подготовленных ВРМ, используемых субъектами;
- «Пользователи и группы» – имена пользователей и наименование групп, используемые для определения разрешений по доступу к фондам ВРМ;
- «Протоколы доставки» – доступные протоколы удаленного доступа, используемые при доставке ВРМ;
- «Публикации» – актуальная информация о созданном фонде ВРМ;
- «Журнал» – системные сообщения, связанные с жизненным циклом фонда ВРМ.

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

### 8.2 . Добавление фонда ВРМ

Для добавления в графическом интерфейсе управления следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Новый]**.

Для добавления в Termidesk фондов ВРМ администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 39 – Данные для добавления фонда ВРМ

Параметр	Описание
«Название»	Текстовое наименование фонда ВРМ
«Комментарий»	Информационное сообщение, используемое для описания назначения фонда ВРМ
«Шаблон»	Используемый шаблон при создании ВРМ
«Параметры гостевой ОС»	Параметры конфигурации гостевой ОС, используемые при создании ВРМ
«Изображение»	Графическое представление фонда ВРМ
«Группа»	Вхождение субъекта в группу безопасности для доступа к фонду ВРМ
«URL поддержки»	URL для связи с технической поддержкой
«Кеш рабочих мест 1-го уровня»	Количество созданных, настроенных и запущенных ВРМ в фонде
«Кеш рабочих мест 2-го уровня»	Количество созданных, настроенных и выключенных ВРМ
«Максимальное количество рабочих мест»	Максимальное количество ВРМ в фонде
«Режим отладки»	Включение режима отладки
«Разрешить резервные копии»	Включение режима резервного копирования ВРМ фонда

### 8.3 . Глобальные политики фонда ВРМ

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

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

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

Для редактирования глобальных политик администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 40 – Доступные параметры глобальных политик фонда ВРМ

Параметр	Описание
«Буфер обмена в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Разрешение на использование буфера обмена в протоколах доставки. Политика применяется только для протокола SPICE (vdi-viewer, эксперим.). Значение по умолчанию: «Включен»
«Выбор пользователем протокола доставки»	Определяет возможность выбрать протокол доставки пользователем для подключения к ВРМ. Значение по умолчанию: «Разрешен»
«Действие при выходе пользователя из ОС»	Определяет действие после выхода пользователя из ОС. Значение по умолчанию: «Нет»
«Использование механизма RemoteFX (RDP)»	Политика активации механизма RemoteFX для протокола RDP. Значение по умолчанию: «Выключен»
«Механизм обеспечения безопасности на уровне сети (RDP)»	Политика управления обеспечением безопасности на уровне сети для протокола RDP. Значение по умолчанию: «Автосогласование» Для подключения компонента «Клиент» с ОС Astra Linux Special Edition 1.7 к STAL необходимо использовать политику «TLS» или «RDP». Для подключения к MS RDS необходимо использовать политику «NLA». Политика может быть задана для конкретного фонда ВРМ на странице самого фонда ВРМ
«Отделяемый пользовательский профиль»	Использование отделяемого пользовательского профиля в ВРМ. Политика применяется при старте ВРМ. Значение по умолчанию: «Выключен»
«Передача файлов в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Разрешение на передачу файлов в протоколах доставки. Политика пока применяется только для протокола SPICE (vdi-viewer, эксперим.). Значение по умолчанию: «Разрешена»
«Перенаправление видеокamеры в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Разрешение на перенаправление видеокamеры в протоколах доставки. Политика пока применяется только для протокола SPICE (vdi-viewer, эксперим.). Значение по умолчанию: «Разрешено»

Параметр	Описание
«Перенаправление смарт-карт в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Разрешение на перенаправление смарт-карт в протоколах доставки. Политика применяется только для протокола SPICE (vdi-viewer, эксперим.). Значение по умолчанию: «Разрешено»
«Политика простоя рабочего места»	Разрешенное время простоя ВРМ в секундах. Значение -1 означает неограниченное время простоя. Значение по умолчанию: «-1»
«Полноэкранный режим (для SPICE)»	Политика ограничения работы в полноэкранном режиме. Значение по умолчанию: «Включен»
«Разрешение видеокamеры в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Допустимые разрешения видеокamеры в протоколах доставки. Политика применяется только для протокола SPICE (vdi-viewer, эксперим.). Значение по умолчанию: «320-2560x240-1440»
«Удаление рабочего места после»	Определяет, после какого события пометать ВРМ для удаления. Работает совместно с параметром «Действие при выходе пользователя из ОС». Значение по умолчанию (рекомендуется): «После события выхода пользователя из ОС»

#### 8.4 . Объединение фондов в группы ВРМ

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

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

Таблица 41 – Данные для объединения фондов ВРМ в группы

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

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

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

## 8.5 . Публикация фонда ВРМ

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

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

На открывшейся странице в разделе «Публикации» нажать экранную кнопку **[Новая]**. В окне подтверждения публикации после ввода опционального текстового комментария нужно нажать экранную кнопку **[Опубликовать]** для запуска задачи обновления фонда ВРМ.

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

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 ВРМ.

Существуют несколько состояний публикации, которые могут быть отражены в столбце «Прогресс»:

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

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

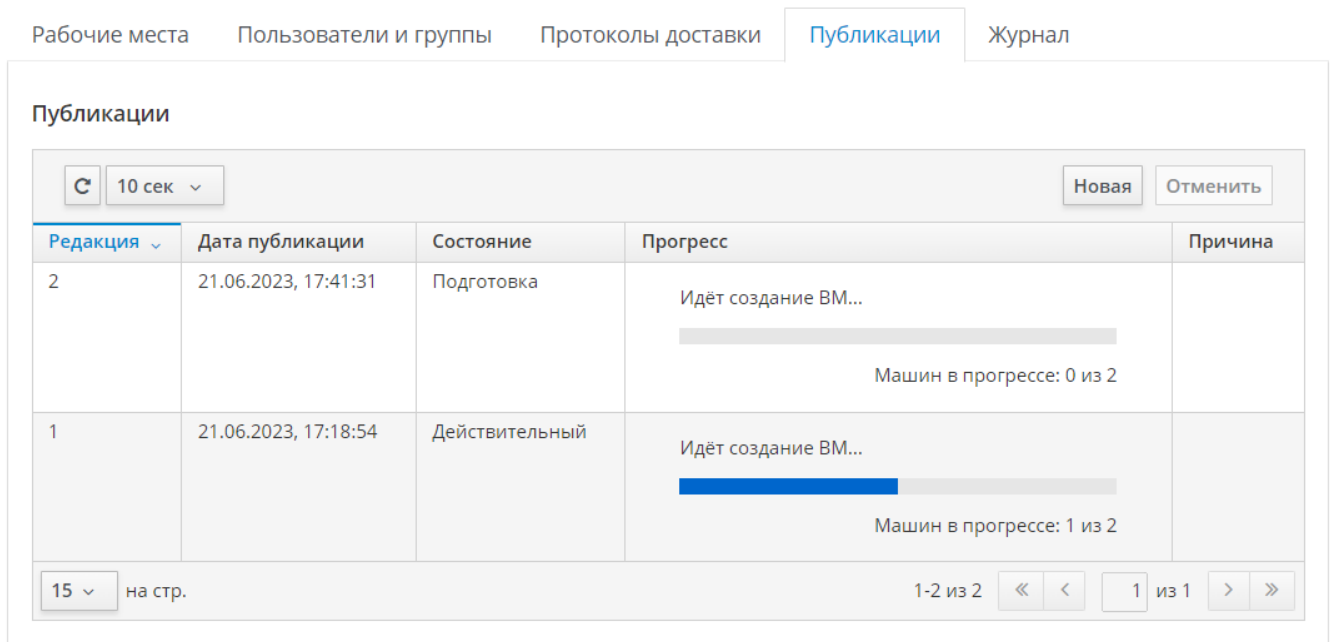


Рисунок 14 – Индикация прогресса выполнения публикации со статусом «Идёт создание VM»

- «Публикация успешно завершена», индикация зеленым цветом - публикация VM в кеше завершена. При выдаче ВРМ из кеша прогресс вновь вернется на начало процесса публикации;

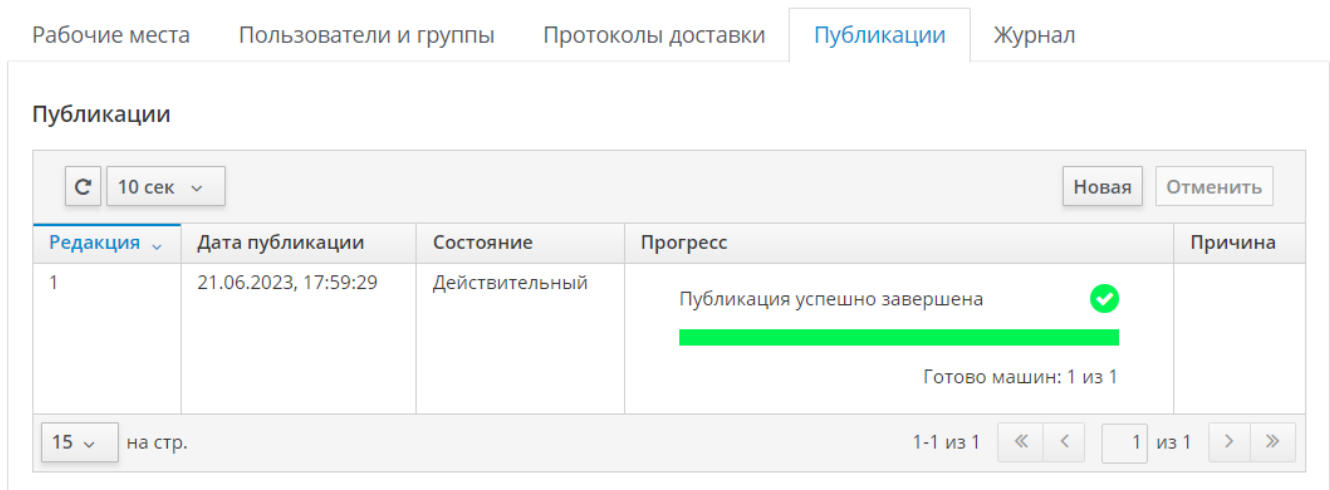


Рисунок 15 – Индикация прогресса выполнения публикации со статусом «Публикация успешно завершена»


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



Рабочие места    Пользователи и группы    Протоколы доставки    **Публикации**    Журнал

Публикации

   10 сек ▾       


Редакция	Дата публикации	Состояние	Прогресс ^	Причина
1	14.06.2023, 17:04:33	Удален	Публикация удалена	
3	21.06.2023, 16:22:56	Ошибка	Во время публикации возникла ошибка  Готово машин: 0 из 1	OpenNebula error 16384: "[one.template.clone] Error allocating a new virtual machine template. NAME is already taken by TEMPLATE 52."
2	21.06.2023, 16:20:47	Действительный	Идёт создание VM... Машин в прогрессе: 1 из 1	

15 ▾ на стр.    1-3 из 3    << < 1 из 1 > >>

Рисунок 16 – Индикация возникновения ошибки при публикации

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

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


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

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

## 8.6 . Назначение пользователей доступа

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

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

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


## 8.7 . Назначение групп доступа фонду ВРМ

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

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

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

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

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

## 8.8 . Назначение протоколов фонду ВРМ

Фонду ВРМ можно назначать доступные для него протоколы доставки.

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

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

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

## 8.9 . Управление сессиями подключенных к фонду ВРМ пользователей

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

Для просмотра основных сведений об активных сессиях пользователей в фондах ВРМ следует перейти «Рабочие места - Сессии», после чего откроется сводная таблица.

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

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

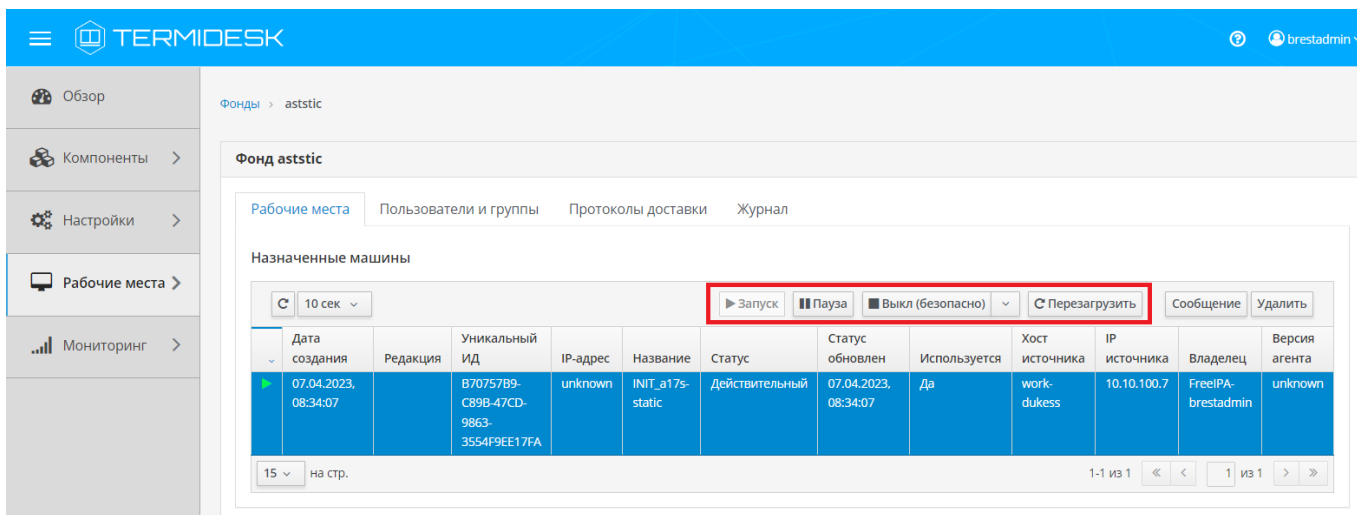
## 8.10 . Управление назначенными ВМ

### 8.10.1 . Управление состоянием

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

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

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



Фонды > aststic

Фонд aststic

Рабочие места | Пользователи и группы | Протоколы доставки | Журнал

Назначенные машины

10 сек

▶ Запуск | || Пауза | ■ Выкл (безопасно) | ⌂ Перезагрузить | Сообщение | Удалить

Дата создания	Редакция	Уникальный ID	IP-адрес	Название	Статус	Статус обновлен	Используется	Хост источника	IP источника	Владелец	Версия агента
07.04.2023, 08:34:07		B70757B9-C89B-47CD-9863-3554F9EE17FA	unknown	INIT_a17s-static	Действительный	07.04.2023, 08:34:07	Да	work-dukess	10.10.100.7	FreeIPA-brestadmin	unknown

15 на стр. 1-1 из 1

Рисунок 17 – Расположение экранных кнопок для управления состоянием назначенных VM

### 8.10.2 . Отправка сообщения в VM

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

## 9. ПРОТОКОЛЫ ДОСТАВКИ

### 9.1 . Общие сведения о протоколах доставки


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

Доставка экрана ВРМ может быть выполнена как напрямую, так и через компонент «Шлюз».

Для добавления протокола доставки в графическом интерфейсе управления следует перейти «Компоненты - Протоколы доставки», затем нажать на экранную кнопку **[Новый]** и выбрать из выпадающего списка поддерживаемый протокол и способ доставки.

Добавленные протоколы можно редактировать, для этого нужно пометить протокол и после нажать на экранную кнопку **[Редактировать]**.

Добавленные ранее протоколы можно удалить, для этого нужно пометить протокол и после нажать на экранную кнопку **[Удалить]**.

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

Termidesk поддерживает следующие протоколы доставки:

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

Возможности каждого протокола при доставке ВРМ пользователю приведены в таблице.

Таблица 42 – Функциональные возможности протоколов доставки

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

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

Возможность	SPICE	RDP	VNC	Loudplay
Оптимизация канала связи от ВРМ к пользовательской рабочей станции	Да	Да	Нет	Да

Примечание:

\* необходима поддержка технологии RemoteFX;

\*\* зависит от используемой ОС.

## 9.2 . Протокол доставки RDP

### 9.2.1 . Прямое подключение по протоколу RDP

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

Таблица 43 – Данные для добавления прямого подключения по протоколу RDP

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде ВРМ
«Пустые учетные данные»	Не использовать технологию единого входа
«Логин»	Субъект, имеющий полномочия для подключения по протоколу RDP к ВРМ
«Пароль»	Набор символов, подтверждающий полномочия
«Без домена»	Не использовать идентификатор домена MS AD при проверке полномочий субъекта
«Домен»	Идентификатор домена MS AD при проверке полномочий субъекта
«Порт»	Выбор порта для подключения. По умолчанию используется порт 3389
«Разрешить смарт-карты»	Разрешить идентификацию субъектов на основе смарт-карт
«Разрешить принтеры»	Разрешить перенаправление устройств печати по протоколу RDP

Параметр	Описание
«Разрешить диски»	Разрешить перенаправление устройств хранения по протоколу RDP
«Разрешить последовательные порты»	Разрешить перенаправление последовательных портов по протоколу RDP
«Показывать обои»	Отображать фоновое изображение, настроенное на рабочем столе
«Несколько мониторов»	Разрешить использовать несколько мониторов
«Разрешить композицию рабочего стола»	Разрешить темы рабочего стола
«Сглаживание шрифтов»	Использовать технологию сглаживания шрифтов
«Поддержка CredSSP»	Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider
«Использовать ALSA»	Использовать программный микшер для передачи звука
«Параметры принтера»	Указать конфигурацию перенаправляемого принтера
«Параметры смарт-карты»	Указать конфигурацию идентификации по смарт-картам
«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 ВРМ. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к ВРМ

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

### 9.2.2 . Подключение через компонент «Шлюз» по протоколу RDP

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



Таблица 44 – Данные для добавления подключения по протоколу RDP через «Шлюз»

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде ВРМ
«URL шлюза»	Адрес сервера в формате ws(s)://ip-address_or_FQDN/websockify, обеспечивающего формирование и поддержание соединения. Директива ws относится к использованию порта 80, директива wss означает использование 443 порта. Параметр ip-address_or_FQDN - доступный IP адрес шлюза. Значение этого параметра не относится к значению WSPROXY_BIND_ADDRESS из конфигурационного файла /etc/opt/termidesk-vdi/termidesk.conf
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза
«Пустые учетные данные»	Не использовать технологию единого входа
«Логин»	Субъект, имеющий полномочия для подключения по протоколу RDP к ВРМ
«Пароль»	Набор символов, подтверждающий полномочия
«Без домена»	Не использовать идентификатор домена MS AD при проверке полномочий субъекта
«Домен»	Идентификатор домена MS AD при проверке полномочий субъекта
«Порт»	Выбор порта для подключения. По умолчанию используется порт 3389
«Разрешить смарт-карты»	Разрешить идентификацию субъектов на основе смарт-карт
«Разрешить принтеры»	Разрешить перенаправление устройств печати по протоколу RDP
«Разрешить диски»	Разрешить перенаправление устройств хранения по протоколу RDP
«Разрешить последовательные порты»	Разрешить перенаправление последовательных портов по протоколу RDP
«Показывать обои»	Отображать фоновое изображение, настроенное на рабочем столе

Параметр	Описание
«Несколько мониторов»	Разрешить использовать несколько мониторов
«Разрешить композицию рабочего стола»	Разрешить темы рабочего стола
«Сглаживание шрифтов»	Использовать технологию сглаживания шрифтов
«Поддержка CredSSP»	Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider
«Использовать ALSA»	Использовать программный микшер для передачи звука
«Параметры принтера»	Указать конфигурацию перенаправляемого принтера
«Параметры смарт-карты»	Указать конфигурацию идентификации по смарт-картам
«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 ВРМ. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к ВРМ

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

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

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

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

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 45 – Данные для добавления прямого подключения к серверам терминалов

Параметр	Описание
«Название»	Текстовое наименование протокола доставки

<b>Параметр</b>	<b>Описание</b>
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде ВРМ
«Без домена»	Не использовать идентификатор домена при проверке полномочий субъекта
«Домен»	Идентификатор домена при проверке полномочий субъекта. Должно использоваться короткое имя домена
«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
«Все принтеры»	Выполнить перенаправление всех устройств печати по протоколу RDP. При выключенном параметре «Разрешить принтеры» данный параметр игнорируется
«Разрешить диски»	Разрешить перенаправление устройств хранения по протоколу RDP
«Разрешить последовательные порты»	Разрешить перенаправление последовательных портов по протоколу RDP
«RemoteFX»	Использовать технологию RemoteFX
«Показывать обои»	Отображать фоновое изображение, настроенное на рабочем столе
«Все RemoteFX устройства»	Использовать все RemoteFX устройства
«Несколько мониторов»	Разрешить использовать несколько мониторов
«Разрешить композицию рабочего стола»	Разрешить темы рабочего стола
«Сглаживание шрифтов»	Использовать технологию сглаживания шрифтов
«Поддержка CredSSP»	Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider
«Мультимедиа синхронизация»	Использовать синхронизацию с xfreerdp
«Использовать ALSA»	Использовать программный микшер для передачи звука
«Параметры смарт-карты»	Указать конфигурацию идентификации по смарт-картам

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

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

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

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

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

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 46 – Данные для добавления подключения к серверам терминалов через «Шлюз»

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

Параметр	Описание
«URL шлюза»	Адрес сервера в формате ws(s)://ip-address_or_FQDN/websockify, обеспечивающего формирование и поддержание соединения. Директива ws относится к использованию порта 80, директива wss означает использование 443 порта. Параметр ip-address_or_FQDN - доступный IP адрес шлюза. Значение этого параметра не относится к значению WSPROXY_BIND_ADDRESS из конфигурационного файла /etc/opt/termidesk-vdi/termidesk.conf
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза
«Без домена»	Не использовать идентификатор домена при проверке полномочий субъекта
«Домен»	Идентификатор домена при проверке полномочий субъекта. Должно использоваться короткое имя домена
«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
«Все принтеры»	Выполнить перенаправление всех устройств печати по протоколу RDP. При выключенном параметре «Разрешить принтеры» данный параметр игнорируется
«Разрешить диски»	Разрешить перенаправление устройств хранения по протоколу RDP
«Разрешить последовательные порты»	Разрешить перенаправление последовательных портов по протоколу RDP
«RemoteFX»	Использовать технологию RemoteFX
«Показывать обои»	Отображать фоновое изображение, настроенное на рабочем столе
«Все RemoteFX устройства»	Использовать все RemoteFX устройства
«Несколько мониторов»	Разрешить использовать несколько мониторов
«Разрешить композицию рабочего стола»	Разрешить темы рабочего стола
«Сглаживание шрифтов»	Использовать технологию сглаживания шрифтов

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

### 9.3 . Протокол доставки SPICE

#### 9.3.1 . Прямое подключение по протоколу SPICE

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

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

Таблица 47 – Данные для добавления прямого подключения по SPICE

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде ВРМ
«Сертификат»	Информация о публичном ключе для доступа к платформе виртуализации oVirt/RHEV

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

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

### 9.3.2 . Подключение через компонент «Шлюз» по протоколу SPICE

Для добавления подключения по протоколу SPICE через вебсокет-шлюз администратору Termidesk следует перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку [Новый], выбрать «SPICE (через вебсокет-шлюз)» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 48 – Данные для добавления подключения по SPICE через «Шлюз»

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде ВРМ
«URL шлюза»	Адрес сервера в формате ws(s)://ip-address_or_FQDN/websockify, обеспечивающего формирование и поддержание соединения. Директива ws относится к использованию порта 80, директива wss означает использование 443 порта. Параметр ip-address_or_FQDN - доступный IP-адрес шлюза, не 127.0.0.1. Значение этого параметра не относится к значению WSPROXY_BIND_ADDRESS из конфигурационного файла /etc/opt/termidesk-vdi/termidesk.conf
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза
«Сертификат»	Информация о публичном ключе для доступа к платформе виртуализации oVirt/RHEV

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

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

### 9.3.3 . Подключение по протоколу SPICE через HTML5 (локальный прокси)

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

Таблица 49 – Данные для добавления подключения по SPICE через локальный прокси

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде ВРМ
«URL шлюза»	Адрес сервера в формате ws(s)://ip-address_or_FQDN/websockify, обеспечивающего формирование и поддержание соединения. Директива ws относится к использованию порта 80, директива wss означает использование 443 порта. Параметр ip-address_or_FQDN - доступный IP-адрес шлюза, не 127.0.0.1. Значение этого параметра не относится к значению WSPROXY_BIND_ADDRESS из конфигурационного файла /etc/opt/termidesk-vdi/termidesk.conf
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза



Параметр	Описание
«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 ВРМ. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешённые устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу SPICE к ВРМ

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

#### 9.3.4 . Подключение по протоколу SPICE через vdi-viewer

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

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

Таблица 50 – 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»	Преимущество использования протокола доставки в фонде ВРМ

Параметр	Описание
«URL шлюза»	Адрес сервера в формате ws(s)://ip-address_or_FQDN/websockify, обеспечивающего формирование и поддержание соединения. Директива ws относится к использованию порта 80, директива wss означает использование 443 порта. Параметр ip-address_or_FQDN - доступный IP-адрес шлюза, не 127.0.0.1. Значение этого параметра не относится к значению WSPROXY_BIND_ADDRESS из конфигурационного файла /etc/opt/termidesk-vdi/termidesk.conf
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза
«Сертификат»	Информация о публичном ключе для доступа к платформе виртуализации (опционально)
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к ВРМ. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешённые устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу SPICE к ВРМ

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

## 9.4 . Протокол доставки VNC

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

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

Таблица 51 – Данные для добавления подключения по VNC через локальный прокси

Параметр	Описание
«Название»	Текстовое наименование протокола доставки

Параметр	Описание
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде ВРМ
«URL шлюза»	Адрес сервера в формате <code>ws(s)://ip-address_or_FQDN/websockify</code> , обеспечивающего формирование и поддержание соединения. Директива <code>ws</code> относится к использованию порта 80, директива <code>wss</code> означает использование 443 порта. Параметр <code>ip-address_or_FQDN</code> - доступный IP-адрес шлюза. Значение по умолчанию использует 127.0.0.1
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к ВРМ. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешённые устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу VNC к ВРМ

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

## 9.5 . Протокол доставки Loudplay

### 9.5.1 . Прямое подключение по протоколу Loudplay

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

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

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

Для добавления протокола доставки администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 52 – Данные для добавления прямого подключения по протоколу Loudplay

<b>Параметр</b>	<b>Описание</b>
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде ВРМ
«Порт rtsp-сервера»	Выбор порта RTSP-сервера. По умолчанию используется 8554
«Путь к API»	Наименование канала для подключения. По умолчанию используется /desktop
«Порт управления (клавиатура/мышь)»	Выбор порта управления клавиатурой и мышью. По умолчанию используется 8555
«Порт служебный (bbr_port)»	Выбор служебного порта RPC. По умолчанию используется 8556
«Порт видео потока»	Выбор порта видеопотока. По умолчанию используется 6970
«Порт аудио потока»	Выбор порта аудиопотока. По умолчанию используется 6972
«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 ВРМ. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу Loudplay к ВРМ

### 9.5.2 . Подключение через компонент «Шлюз» по протоколу Loudplay

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

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

Для добавления протокола доставки администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 53 – Данные для добавления подключения через «Шлюз» по протоколу Loudplay

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде ВРМ
«URL шлюза»	Адрес сервера в формате ws(s)://ip-address_or_FQDN/websockify, обеспечивающего формирование и поддержание соединения. Директива ws относится к использованию порта 80, директива wss означает использование 443 порта. Параметр ip-address_or_FQDN - доступный IP-адрес шлюза, не 127.0.0.1. Значение этого параметра не относится к значению WSPROXY_BIND_ADDRESS из конфигурационного файла /etc/opt/termidesk-vdi/termidesk.conf
«Протокол передачи»	Используемый протокол передачи. Возможное значение: UDP
«Порт rtsp-сервера»	Выбор порта RTSP-сервера. По умолчанию используется 8554
«Путь к API»	Наименование канала для подключения. По умолчанию используется /desktop
«Порт управления (клавиатура/мышь)»	Выбор порта управления клавиатурой и мышью. По умолчанию используется 8555
«Порт служебный (bbr_port)»	Выбор служебного порта RPC. По умолчанию используется 8556
«Порт видео потока»	Выбор порта видеопотока. По умолчанию используется 6970

Параметр	Описание
«Порт аудио потока»	Выбор порта аудиопотока. По умолчанию используется 6972
«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 ВРМ. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу Loudplay к ВРМ

## 10 . СИСТЕМНЫЕ НАСТРОЙКИ

### 10.1 . Общие системные параметры Termidesk

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

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

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы.


 Изменение системных параметров вступают в силу только после перезагрузки Termidesk.

Таблица 54 – Общие системные параметры Termidesk

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

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

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

## 10.2 . Параметры безопасности Termidesk

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

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы.

Таблица 55 – Параметры безопасности Termidesk

Параметр	Описание
«Эксклюзивный выход»	Запрет множественного входа в Termidesk для субъектов с различными полномочиями



Параметр	Описание
«Мастер-ключ»	Идентификатор регистрации субъектов в Termidesk при доступе к фонду ВРМ
«Доверенные хосты»	Идентификатор узлов, имеющих право подключаться к Termidesk
«Длительность сессии администратора»	Временной интервал сессии, инициированной на графический интерфейс управления
«Доступ к веб-части системным пользователем»	Возможность субъекта с ролью «Администратор» подключаться к графическому интерфейсу
«Использовать анонсируемый IP клиента»	Использовать IP-адрес клиента, передаваемый в процессе входа в Termidesk
«GID системной группы администратора»	Идентификатор группы, в которую входит учетная запись субъекта с ролью «Администратор»
«Длительность сессии пользователя»	Временной интервал сессии субъекта с ролью «Пользователь», инициированной на графическом интерфейсе пользователя

### 10.3 . Назначение служебных функций администраторам

В Termidesk реализовано разделение доступных служебных функций для администраторов.

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

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

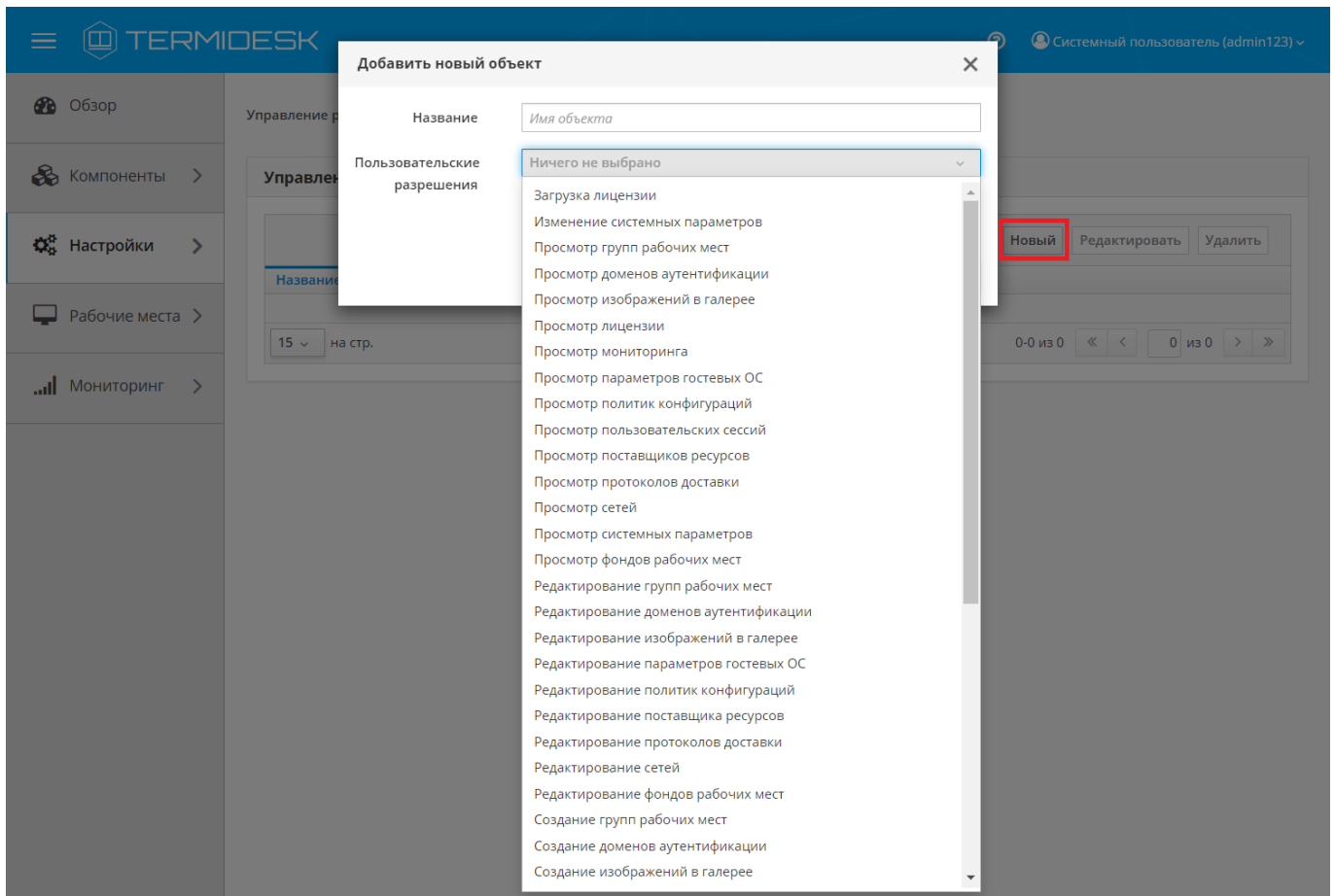


Рисунок 18 – Окно назначения пользовательских разрешений

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

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

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

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

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

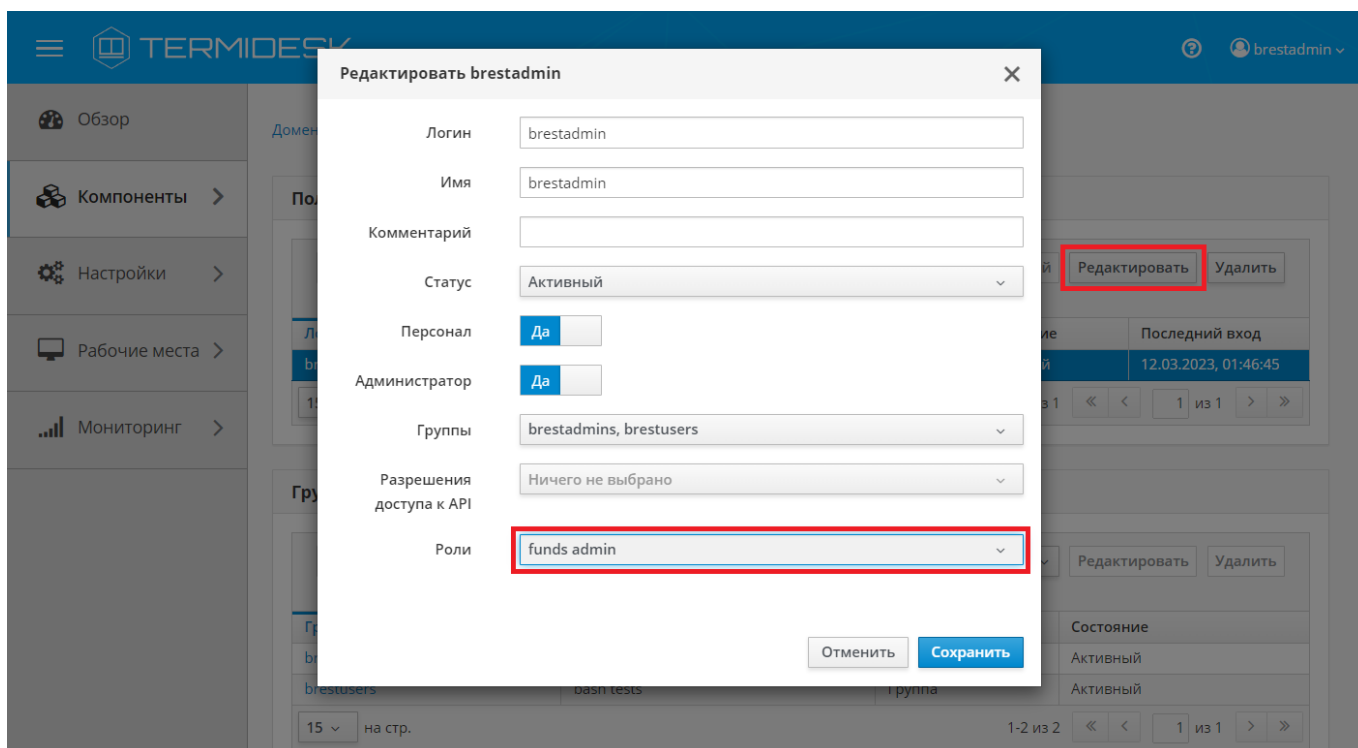


Рисунок 19 – Окно назначения пользовательских ролей

**⚠** 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 ВРМ. Для добавления нового разрешения для объекта следует перейти «Настройки - Управление ACL», нажать экранную кнопку **[Новый]** и выбрать объект «Фонд рабочих мест».

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

Таблица 56 – Доступные параметры при добавлении пользовательских разрешений для фондов ВРМ

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

Параметр	Описание
«Пользовательское разрешение»	Выбор пользовательских разрешений, касающихся фондов ВРМ. Список всех доступных разрешений: <ul style="list-style-type: none"> <li>▪ просмотр фондов ВРМ;</li> <li>▪ редактирование фондов ВРМ;</li> <li>▪ удаление фондов ВРМ;</li> <li>▪ управление кэшем фондов ВРМ;</li> <li>▪ управление пользовательскими группами фондов ВРМ;</li> <li>▪ управление пользователями фондов ВРМ;</li> <li>▪ управление протоколами доставки фондов ВРМ;</li> <li>▪ управление публикациями фондов ВРМ</li> </ul>
«Объект»	Ранее созданный фонд ВРМ

## 11 . МОНИТОРИНГ И УВЕДОМЛЕНИЯ

### 11.1 . Системные параметры мониторинга

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

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

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы.

Таблица 57 – 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
«Категория сообщения»	Выбор категории сообщений, которые будут записываться в журнал мониторинга
«Уровень логирования»	Выбор уровня логирования событий (INFO, WARNING, ERROR, CRITICAL, DEBUG)

### 11.2 . Настройка отправки уведомлений о системных событиях

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

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы.

Таблица 58 – Параметры отправки уведомлений о событиях

Параметр	Описание
«Вкл/выкл почтовых уведомлений»	Включение или отключение возможности отправки уведомлений о системных событиях по электронной почте
«Хост»	IP-адрес или имя узла, на котором развернута служба сервера электронной почты
«Порт»	Номер порта, на котором ведется прослушивание службой сервера электронной почты
«Email отправителя»	Почтовый адрес отправителя сообщений на сервере электронной почты. Формат: mailto:user@mail.domain

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

### 11.3 . Уведомление об ошибках аутентификации в графическом интерфейсе управления

Для конфигурации системных параметров аутентификации следует перейти «Настройки - Системные параметры - Аутентификация».

В открывшейся странице можно задать дополнительное текстовое сообщение, которое будет выдаваться в случае неуспешной аутентификации посредством графического интерфейса управления Termidesk.

### 11.4 . Шаблон для мониторинга Zabbix

Termidesk поддерживает мониторинг состояния компонентов через Zabbix.

Шаблон для мониторинга распространяется через iso-образ Termidesk.

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

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

### 11.5 . Отчеты

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

Можно сформировать следующие отчеты:

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

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

Таблица 59 – 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 <b>&lt;Enter&gt;</b> для подтверждения выбора

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

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

Таблица 60 – 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 <b>&lt;Enter&gt;</b> 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 <b>&lt;Enter&gt;</b> для подтверждения выбора
«Домен аутентификации»	Наименование домена аутентификации, по которому будет осуществлен поиск события
«Пользователь»	Логин пользователя, по которому будет осуществлен поиск события

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

Таблица 61 – 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 <b>&lt;Enter&gt;</b> 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 <b>&lt;Enter&gt;</b> 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.



## 12 . СИСТЕМА АУДИТА

### 12.1 . Системные параметры аудита

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

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы.

Таблица 62 – Системные параметры аудита

Параметр	Описание
«Использовать "строгий" режим аудита»	Включение режима максимально полного сохранения информации о событиях аудита
«Сохранение в БД»	Выбор сохранения событий аудита в БД
«Время хранения записи в БД (дней)»	Время хранения (в днях) записи события аудита в БД
«Максимум удаляемых событий»	Максимальное количество удаляемых событий в журнале аудита
«Сохранение в файл»	Выбор сохранения событий аудита в отдельный файл журнала
«Файл хранения событий»	Указание полного пути к файлу хранения журнала событий аудита при выбранной опции «Сохранение в файл»
«Количество архивных файлов»	Максимальное количество архивных файлов журнала событий аудита, по достижении которого начинается перезапись
«Отправка в Syslog»	Направление логирования на отдельный syslog-сервер
«Хост»	IP-адрес или имя узла, на котором развёрнута служба syslog-сервера
«Протокол»	Выбор протокола работы для службы syslog-сервера
«Порт»	Порт, на котором находится служба syslog-сервера
«Категория сообщения»	Выбор категории сообщений, которые будут записываться в журнал аудита

### 12.2 . 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 Termidesk;
- `celery-beat.log` - записываются события периодической проверки состояния обработчика заданий через RabbitMQ;
- `celery-worker.log` - записываются события обработчика заданий через RabbitMQ;
- `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;
- `sql.log` - записываются отладочные события БД;
- `termidesk.log` - записываются события работы сервера Termidesk;
- `use.log` - записываются события пользователей ВРМ;
- `workers.log` - записываются события обработчика фоновых задач;
- `wsproxy.log` - записываются события компонента «Шлюз»;
- `orchestrator.log` - записываются события компонента «Оркестратор»;
- `stal_proxy.log` - записываются события службы proxy компонента «Сервер терминалов»;
- `stal_service.log` - записываются события службы stal компонента «Сервер терминалов».

### 12.3 . Настройка журналирования

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

Для изменения уровня журналирования необходимо:

- изменить параметр `LOG_LEVEL`;
- перезапустить службы Termidesk:

```

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

### 12.4 . Просмотр журналов

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

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

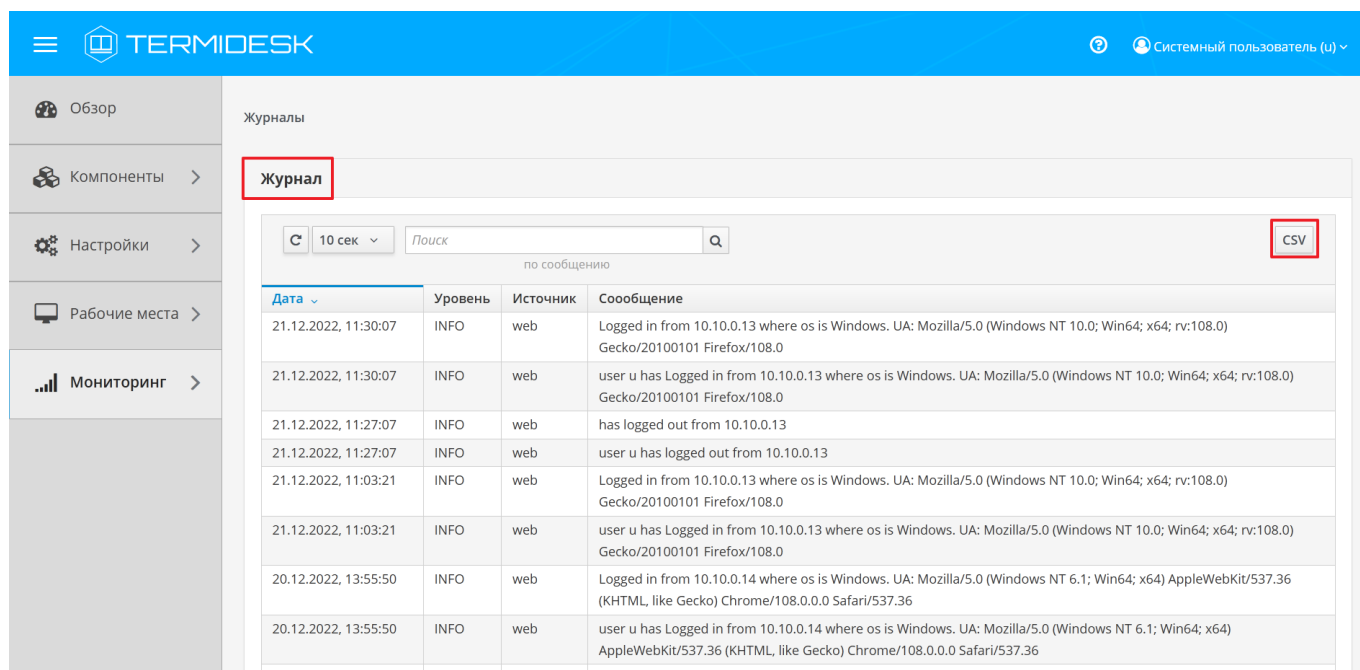


Рисунок 20 – Отображение общего журнала в графическом интерфейсе управления Termidesk

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

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

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

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

**Аудит**

### Журнал событий

Поиск:

по пользователю или IP адресу

Событие:  произошло с  по

Дата	Событие	Описание
21.12.2022, 11:30:07	termidesk.audit.events.web.UserLogin	Пользователь "ц(Встроенный)" вошел в систему с ip-адреса 10.10.0.13
21.12.2022, 11:27:07	termidesk.audit.events.web.UserLogout	Пользователь "ц(Встроенный)" вышел из системы (ip-адрес 10.10.0.13)
21.12.2022, 11:03:51	termidesk.audit.events.web.EntityAction	Пользователь "ц(Встроенный)" выполнил операцию read для объекта Provider (a5459bdd-2f0a-5ebf-af0a-7fa065b7620f) oVirtPlatform "zVirt" (ip-адрес 10.10.0.13)
21.12.2022, 11:03:31	termidesk.audit.events.web.EntityAction	Пользователь "ц(Встроенный)" выполнил операцию read для объекта Provider (71eee3b2-214b-5703-aa28-291e3f957cf3) pksvbrestPlatform "Brest2.6" (ip-адрес 10.10.0.13)
21.12.2022, 11:03:21	termidesk.audit.events.web.UserLogin	Пользователь "ц(Встроенный)" вошел в систему с ip-адреса 10.10.0.13
20.12.2022, 13:55:50	termidesk.audit.events.web.UserLogin	Пользователь "ц(Встроенный)" вошел в систему с ip-адреса 10.10.0.14
16.12.2022, 15:46:36	termidesk.audit.events.web.EntityAction	Пользователь "brestadmin(FreeIPA)" выполнил операцию read для объекта DeployedService (c37cd7b8-0f4b-507f-9242-90a30bc8aaca) "Astra17" (ip-адрес 10.10.0.12)
16.12.2022, 15:46:28	termidesk.audit.events.web.UserLogin	Пользователь "brestadmin(FreeIPA)" вошел в систему с ip-адреса 10.10.0.12
16.12.2022, 11:32:46	termidesk.audit.events.workplace.UserLogin	Пользователь "unknown()" вошел в гостевую ОС VM 4orb-000(192.168.12.125) фонда Orel как

Рисунок 21 – Отображение журнала аудита в графическом интерфейсе управления Termidesk

## 13. РЕЖИМ ВЫСОКОЙ ДОСТУПНОСТИ И РАБОТА С СЕРТИФИКАТАМИ

### 13.1. Настройка менеджера ВРМ в режиме высокой доступности

Настройка выполняется после установки программного комплекса в распределенной конфигурации.

Последовательность настройки узлов с менеджером ВРМ следующая:

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

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

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

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

где:

`-y` - ключ для пропуска подтверждения установки;

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

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

где:

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

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

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

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

```
global_defs {
    router_id NAME_OF_ROUTER_ID # CHANGE_ON: hostname хоста
    script_user user # CHANGE_ON: пользователь, от имени которого запускается keepalived
    enable_script_security
}
```

```

vrrp_script check_httpd {
    script "/usr/bin/pgrep apache" # path of the script to execute
    interval 1 # seconds between script invocations, default 1 second
    timeout 3 # seconds after which script is considered to have failed
    #weight <INTEGER:-254..254> # adjust priority by this weight, default 0
    rise 1 # required number of successes for OK transition
    fall 2 # required number of successes for KO transition
    #user USERNAME [GROUPNAME] # user/group names to run script under
    init_fail # assume script initially is in failed state
}

# Для каждого виртуального IPv4-адреса создается свой экземпляр vrrp_instance
vrrp_instance termidesk-taskman {
    notify /etc/keepalived/notify.sh

    # Initial state, MASTER|BACKUP
    # As soon as the other machine(s) come up,
    # an election will be held and the machine
    # with the highest priority will become MASTER.
    # So the entry here doesn't matter a whole lot.
    state BACKUP

    # interface for inside_network, bound by vrrp
    # CHANGE_ON: eth0 -> интерфейс, смотрящий в Интернет
    interface eth0

    # arbitrary unique number from 0 to 255
    # used to differentiate multiple instances of vrrpd
    # running on the same NIC (and hence same socket).
    # CHANGE_ON: 106 -> номер экземпляра vrrp_instance
    virtual_router_id 106

    # for electing MASTER, highest priority wins.
    # to be MASTER, make this 50 more than on other machines.
    # CHANGE_ON: заменить на приоритет экземпляра vrrp_instance
    priority 128

    preempt_delay 5 # Seconds

    # VRRP Advert interval in seconds (e.g. 0.92) (use default)
    advert_int 1

    # CHANGE_ON: 192.0.2.2 -> IPv4-адрес интерфейса, смотрящего в Интернет
    unicast_src_ip IP_ADDRESS_OF_THIS_HOST

    authentication {
        auth_type PASS
        # CHANGE_ON: ksedimret -> заменить на безопасный пароль
        auth_pass ksedimret
    }

    virtual_ipaddress {

```

```

        # CHANGE_ON: 192.168.16.106/24 -> виртуальный IPv4-адрес и сетевой префикс с
интерфейса, смотрящего в Интернет
        # CHANGE_ON: eth0 -> интерфейс, смотрящий в Интернет
        # CHANGE_ON: eth0:106 -> интерфейс, смотрящий в Интернет:4-й октет виртуального
IPv4-адреса
        VIRTUAL_IP_ADDREESS/MASK dev eth0 label eth0:106
    }

    track_script {
        check_httpd
    }
}

```

где:

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

NAME\_OF\_ROUTER\_ID - имя зоны маршрутизации VRRP (общее для обоих узлов);

IP\_ADDREESS\_OF\_THIS\_HOST - текущий статический IP-адрес узла, на котором запускается служба keepalived;

VIRTUAL\_IP\_ADDRESS/MASK - виртуальный статический IP-адрес и маска (общие для узлов master и slave );

- по очереди на каждом из узлов master и slave отредактировать созданный файл /etc/keepalived/notify.sh, приведя его к следующему виду:

```

#!/bin/sh -e

SELF_BIN=$(realpath ${0})
SELF_DIR=$(dirname ${SELF_BIN})
TYPE=${1}
NAME=${2}
STATE=${3}
PRIORITY=${4}
TASKMAN_SYSTEMCTL_NAME="termidesk-taskman"
TASKMAN_SYSTEMCTL_DESCRIPTION="Termidesk-VDI Taskman daemon"
TASKMAN_SYSTEMCTL_PIDFILE="/run/termidesk-taskman/pid"
msg2log () {
    logger -i "Termidesk: ${1}"
}
taskman_stop () {
    msg2log "Stopping ${TASKMAN_SYSTEMCTL_NAME} service"
    systemctl is-active -q ${TASKMAN_SYSTEMCTL_NAME} && systemctl stop -q $
{TASKMAN_SYSTEMCTL_NAME}
}
taskman_start () {
    msg2log "Starting ${TASKMAN_SYSTEMCTL_NAME} service"
    systemctl is-active -q ${TASKMAN_SYSTEMCTL_NAME} || systemctl start -q $
{TASKMAN_SYSTEMCTL_NAME}
}

```

```
# VRRP event type: INSTANCE, name: lsb_40, state: BACKUP, priority: 64
msg2log "VRRP event type: ${TYPE}, name: ${NAME}, state: ${STATE}, priority: ${PRIORITY}"
case ${STATE} in
    BACKUP)
        [ "${NAME}" = "${TASKMAN_SYSTEMCTL_NAME}" ] && taskman_stop
        ;;
    FAULT)
        [ "${NAME}" = "${TASKMAN_SYSTEMCTL_NAME}" ] && taskman_stop
        ;;
    MASTER)
        [ "${NAME}" = "${TASKMAN_SYSTEMCTL_NAME}" ] && taskman_start
        ;;
    *)
        msg2log "Error: unknown state ${STATE}"
        exit 1
        ;;
esac
exit 0
```

- на узлах master и slave сделать файл notify.sh исполняемым:

```
:~$ sudo chmod +x /etc/keepalived/notify.sh
```

- на узлах master и slave добавить в автоматическую загрузку и запустить сервис keepalived:

```
:~$ sudo systemctl enable keepalived
:~$ sudo systemctl start keepalived
```

## 13.2 . Настройка балансировщика для работы с самоподписанными сертификатами

### 13.2.1 . Создание самоподписанного SSL-сертификата

Для создания самоподписанного SSL-сертификата и ключа к нему нужно:

- открыть программу «Terminal Fly» и получить доступ к интерфейсу командной строки;
- выполнить генерацию SSL-сертификата (/etc/ssl/certs/nginx-selfsigned.crt) и ключа к нему (/etc/ssl/private/nginx-selfsigned.key):

```
:~$ sudo openssl req -new -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt
```

Используемые ключи команды:

- openssl - базовый инструмент командной строки для создания и управления сертификатами, ключами и другими файлами OpenSSL;
- req - эта опция указывает, что на данном этапе нужно использовать запрос на подпись сертификата X.509 (CSR). X.509 – это стандарт инфраструктуры открытого ключа, которого



придерживаются SSL и TLS при управлении ключами и сертификатами. Данная команда позволяет создать новый сертификат X.509;

- `new` - эта опция указывает, что будет создаваться новый запрос;
- `x509` - эта опция вносит поправку в предыдущую команду, сообщая утилите о том, что вместо запроса на подписание сертификата необходимо создать самоподписанный сертификат;
- `nodes` - ключ для пропуска опции защиты сертификата парольной фразой. Нужно, чтобы при запуске балансировщик нагрузки (nginx) имел возможность читать файл без вмешательства пользователя. Установив пароль, придется вводить его после каждой перезагрузки;
- `days 365` - эта опция устанавливает срок действия сертификата (в данном случае сертификат действителен в течение года);
- `newkey rsa:2048` - эта опция позволяет одновременно создать новый сертификат и новый ключ. Поскольку ключ, необходимый для подписания сертификата, не был создан ранее, нужно создать его вместе с сертификатом. Данная опция создаст RSA-ключ размером 2048 бит;
- `keyout` - эта опция сообщает OpenSSL, куда поместить сгенерированный файл ключа;
- `out` - эта опция сообщает OpenSSL, куда поместить созданный сертификат.

После исполнения команды надо последовательно ввести ряд параметров, запросы на которые отобразятся в командной строке:

- `Country Name (2 letter code) [AU];`
- `State or Province Name (full name) [Some-State];`
- `Locality Name (eg, city) [];`
- `Organization Name (eg, company) [Internet Widgits Pty Ltd];`
- `Organizational Unit Name (eg, section) [];`
- `Common Name (e.g. server FQDN or YOUR name) [];`
- `Email Address [].`

Наиболее важным параметром является `Common Name` (необходимо ввести FQDN-имя балансировщика). Как правило, в эту строку вносят доменное имя, с которым нужно связать сервер. В случае если доменного имени нет, нужно внести в эту строку IP-адрес сервера.

Файлы ключа и сертификата будут размещены в каталоге, указанном при вызове команды `openssl` в параметрах `keyout` и `out`.

При использовании OpenSSL необходимо также создать ключи Диффи-Хеллмана, для этого:

- открыть программу «Terminal Fly» и получить доступ к интерфейсу командной строки;
- сгенерировать ключи Диффи-Хеллмана длиной 4096 бит и сохранить их в файл `/etc/nginx/dhparam.pem`:

```
~$ sudo openssl dhparam -out /etc/nginx/dhparam.pem 4096
```

### 13.2.2 . Настройка nginx для поддержки SSL

Для настройки nginx нужно:

- создать новый пустой снippet 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:

```
ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;
```

- создать еще один пустой снippet, 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 TLSv1.2;
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.

### 13.2.3 . Конфигурирование веб-сервера

Для конфигурирования веб-сервера нужно:

- создать пустой конфигурационный файл:

```
~$ sudo touch /etc/nginx/sites-available/sampldomain.ru.conf
```

- отредактировать созданный файл, приведя его к виду (указанные IP-адреса необходимо заменить):

```
upstream daas-upstream-ws {
    least_conn;
    # PROXY TERMIDESK

    server 192.168.0.41:5099;
    server 192.168.0.42:5099;
    server 192.168.0.43:5099;
    server 192.168.0.44:5099;
}

upstream daas-upstream-nodes {
    least_conn;
    # DISPATCHER TERMIDESK

    server 192.168.0.30;
    server 192.168.0.31;
    server 192.168.0.32;
}

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 http://daas-upstream-nodes/;

        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}

```

**⚠** IP-адреса, перечисленные в директиве `daas-upstream-ws`, являются адресами шлюзов подключений Termidesk, а IP-адреса, перечисленные в директиве `daas-upstream-nodes`, являются адресами универсальных диспетчеров Termidesk.

- создать символическую ссылку на данный виртуальный хост из директории `/etc/nginx/sites-available` в директорию `/etc/nginx/sites-enabled`, чтобы nginx его обслуживал:

```

:~$ sudo ln -s /etc/nginx/sites-available/sampldomain.ru.conf /etc/nginx/sites-enabled/

```

- проверить корректность настроек:

```

:~$ sudo nginx -t

```

```

nginx: [warn] "ssl_stapling" ignored, issuer certificate not found
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful

```

**⚠** Веб-сервер возвращает предупреждение в случае использования самоподписанного сертификата, однако соединения будут шифроваться правильно.

- если в синтаксисе обнаружены ошибки, необходимо исправить их, затем перезапустить веб-сервер:

```

:~$ sudo systemctl restart nginx

```

## 14. ЭКСПЕРИМЕНТАЛЬНЫЕ ФУНКЦИИ

### 14.1. Перечень переменных окружения универсального диспетчера

В Termidesk используются переменные окружения для указания параметров настройки компонентов программного комплекса.

Перечень переменных, используемых при установке и универсальным диспетчером, приведены в таблице.

Перечень переменных, используемых в других компонентах программного комплекса, приведен в соответствующих им документах.

Таблица 63 – Переменные окружения Termidesk

Переменная окружения	Значение по умолчанию	Описание
<b>Универсальный диспетчер</b>		
TDSK_AUTOFS_IMAGES_ID	Не задано	Используется для настройки шаблонов переносимых профилей. В качестве значения используются идентификаторы дисков. Пример: TDSK_AUTOFS_IMAGES_ID=xx[,yy[,zz[,...]]]
<b>Установочный пакет termidesk-vdi</b>		
TDSK_PKG_DEBUG	Не задано	Включение режима отладки при установке пакета. Пример: TDSK_PKG_DEBUG=1

### 14.2. Управление экспериментальными параметрами Termidesk

Включение и отключение экспериментальных параметров сервера Termidesk производится из командной строки. Командная строка должна запускаться от имени пользователя termidesk.

Для вывода доступных экспериментальных параметров нужно выполнить следующее:

- перейти в интерфейс командной строки;
- переключиться на пользователя termidesk:

```
::~$ sudo -u termidesk bash
```

- вывести список экспериментальных параметров:

```
::~$ /opt/termidesk/sbin/termidesk-vdi-manage tdsk_config list | grep Experimental
```

Будет выведен список экспериментальных параметров Termidesk в формате Секция-Ключ-Значение.

**⚠** При вызове `/opt/termidesk/sbin/termidesk-vdi-manage` могут появляться уведомления «WARNINGS», не влияющие на выполнение команд.

Перечень экспериментальных параметров приведен в таблице.

Таблица 64 – Экспериментальные параметры Termidesk

Параметр	Описание	Значение по умолчанию
<code>experimental.2fa.enabled</code>	Параметр поддержки двухфакторной аутентификации	0
<code>experimental.deviceauth.enabled</code>	Параметр поддержки авторизации устройств доступа	0
<code>experimental.loudplay.transports.enabled</code>	Параметр поддержки протоколов доставки Loudplay	0
<code>experimental.metasessions.provider.enabled</code>	Параметр поддержки сервера терминалов (метапровайдер)	0
<code>experimental.openstack.provider.enabled</code>	Параметр поддержки поставщика ресурсов Openstack	0
<code>experimental.provider.physmachine.enabled</code>	Параметр поддержки поставщика ресурсов для физических машин	0
<code>experimental.vair.provider.enabled</code>	Параметр поддержки поставщика ресурсов vAir	0

Для активации экспериментального параметра необходимо присвоить ему значение 1, выполнив команду:

```

:~$ /opt/termidesk/sbin/termidesk-vdi-manage tdsk_config set --section Experimental --key experimental.2fa.enabled --value 1
    
```

где:

`experimental.2fa.enabled` - наименование параметра;

1 - значение параметра для его активации;

0 - значение параметра для его деактивации.

### 14.3 . Установка плагинов расширений

Экспериментальный функционал, не вошедший в основной релиз Termidesk, можно добавить в программный комплекс через установку плагинов расширений (каталог addons в комплектации поставки Termidesk).

Для установки плагинов нужно на сервере Termidesk выполнить следующее:

- распаковать содержимое zip-архива в целевой каталог (например, /tmp);
- переключиться на пользователя Termidesk:

```
~$ sudo -u termidesk bash
```

- перейти в каталог Termidesk:

```
~$ cd /opt/termidesk/share/termidesk-vdi/
```

- активировать виртуальное окружение Termidesk:

```
~$ source venv/bin/activate
```

- установить необходимый плагин:

```
~$ pip install --upgrade --no-index --find-links /tmp/termidesk_internaldbauth
termidesk_internaldbauth
```

где:

/tmp/termidesk\_internaldbauth - каталог с whl-файлами;

termidesk\_internaldbauth - имя плагина (без версии, платформы и расширения файла);

- выйти из окружения пользователя Termidesk:

```
~$ exit
```

- обновить структуру БД и статических файлов командами:

```
~$ sudo /opt/termidesk/sbin/termidesk-vdi-manage migrate
~$ sudo /opt/termidesk/sbin/termidesk-vdi-manage collectstatic --no-input
```

- перезапустить службы Termidesk:

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

#### 14.4 . Удаление плагинов расширений

- ⚠** Перед удалением плагина необходимо удалить фонды ВРМ, шаблоны ВМ и поставщика ресурсов, соответствующих данному плагину в графическом интерфейсе управления Termidesk.  
Удаление фонда ВРМ может занять продолжительное время.

Для удаления плагина расширений нужно на сервере Termidesk выполнить следующее:

- переключиться на пользователя Termidesk:

```
~$ sudo -u termidesk bash
```

- перейти в каталог Termidesk:

```
~$ cd /opt/termidesk/share/termidesk-vdi/
```

- активировать виртуальное окружение Termidesk:

```
~$ source venv/bin/activate
```

- удалить необходимый плагин:

```
~$ pip uninstall -y termidesk_internaldbauth
```

где:

termidesk\_internaldbauth - имя плагина (без версии, платформы и расширения файла);

- выйти из окружения пользователя Termidesk:

```
~$ exit
```

- перезапустить службы Termidesk:

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

#### 14.5 . Откат к предыдущей версии плагина

Откат к предыдущей версии файла выполняется в той же последовательности, что и установка, однако вместо команды установки плагина используется следующая:

```
~$ pip install --no-index --find-links /tmp/termidesk_internaldbauth termidesk_internaldbauth==4.0.1
```

где:



/tmp/termidesk\_internaldbauth - каталог с whl-файлами, whl-файл с версией плагина должен существовать в данном каталоге;

termidesk\_internaldbauth - имя плагина с указанием версии.

## 15 . ТИПОВЫЕ НЕИСПРАВНОСТИ

### 15.1 . Нештатные ситуации и способы их устранения

Возможные неисправности при работе с Termidesk и способы их устранения приведены в таблице.

Таблица 65 – Перечень возможных нестандартных ситуаций

Индикация	Описание	Возможное решение
Ошибка: «СБОЙ: оставшиеся слоты подключений зарезервированы для подключений суперпользователя (не для репликации)»	Ошибка возникает при попытке авторизации на сервере Termidesk	Изменить максимальное количество подключений в настройках БД: изменить значение <code>max_connections</code> в конфигурационном файле <code>/etc/postgresql/11/main/postgresql.conf</code> в БОльшую сторону
Ошибка: «OpenNebula Error 256 User couldn't authenticated, aborting call»	Ошибка возникает при попытке добавления поставщика ресурсов ПК СВ Брест в графическом интерфейсе управления Termidesk	Необходимо указать верный путь к файлу <code>keytab</code> и внести значения параметра «Токен» непосредственно в интерфейсе ПК СВ Брест (см. подраздел <b>Добавление поставщика ресурсов ПК СВ Брест</b> )
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 BPM 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

Индикация	Описание	Возможное решение
Ошибка: «'list' object has no attribute 'get'»	Ошибка возникает при разворачивании ВМ из шаблона, в котором указано больше одного диска	В шаблоне при первоначальном разворачивании ВМ должен быть указан только один диск
Ошибки при установке пакета «Невозможно найти пакет» или «Неудовлетворенные зависимости»	Ошибка возникает при попытке установить пакет в ОС	Необходимо убедиться, что в файле <code>/etc/apt/sources.list</code> заданы и не закомментированы источники получения пакетов (репозитории), затем обновить списки пакетов: <pre data-bbox="1085 672 1508 739">:~\$ sudo apt update</pre> После этого нужно вновь выполнить команду установки пакета. Для решения проблемы с неудовлетворенными зависимостями, помимо подключения репозитория в файле <code>/etc/apt/sources.list</code> , можно воспользоваться командой: <pre data-bbox="1085 1086 1508 1153">:~\$ sudo apt -f install</pre> Ключ <code>-f</code> используется для попытки исправить нарушенные зависимости пакетов

## 16 . ПЕРЕЧЕНЬ ТЕРМИНОВ

Термин	Определение
Агент	Собирательное название для следующих компонентов: <ul style="list-style-type: none"> <li>▪ агент ВРМ (python3-termidesk-agent);</li> <li>▪ агент УВ (termidesk-vmsd);</li> <li>▪ сессионный агент (termidesk-session-agent);</li> <li>▪ видеоагент (termidesk-video-agent);</li> <li>▪ агент виртуальных смарт-карт (termidesk-pcsc-vscard).</li> </ul> Самостоятельный компонент, отвечающий за контролируемую доставку ВРМ, взаимодействие с универсальным диспетчером и менеджером ВРМ
Агент виртуальных смарт-карт	Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление подключенных к пользовательской рабочей станции смарт-карт в ВРМ
Агент ВРМ	Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет взаимодействие с диспетчером Termidesk, конфигурирует ВРМ, фиксирует действия пользователя, реализует передачу управляющих сообщений
Агент УВ	Агент узла виртуализации. Устанавливается на узел виртуализации, взаимодействует с гипервизором через модуль libvirt
Базовое ВРМ	Также: «золотой образ», «базовое рабочее место», «базовый образ», «gold». Подразумевает собой образ диска виртуальной машины с предустановленным ПО, который далее будет использоваться для создания ВРМ для пользователей
Балансировщик нагрузки	Самостоятельный компонент, отвечающий за распределение нагрузки на множество универсальных диспетчеров и шлюзов
Видеоагент	Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление видеокамеры с пользовательской рабочей станции в ВРМ
ВРМ	Виртуальное рабочее место: гостевая ОС, установленная на отдельно взятой ВМ, доступ к которой реализуется с помощью протокола удаленного доступа
Гостевая ОС	ОС, функционирующая на ВМ
Группы рабочих мест	Также: «группы ВРМ». Функциональное объединение множества фондов ВРМ по определенному признаку
Домен аутентификации	Способ проверки субъектов и их полномочий
Менеджер рабочих мест	Также: «планировщик заданий», «менеджер ВРМ». Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом ВРМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета termidesk-vdi. Наименование службы после установки: termidesk-taskman.service

Термин	Определение
Оркестратор	Самостоятельный компонент, отвечающий за согласованную работу всех компонентов программного комплекса при децентрализованном развертывании, для нужд отказоустойчивости и комплексирования с облачными службами. Устанавливается из пакета <code>termidesk-orchestrator</code>
Поставщик ресурсов	ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов ВРМ
Протокол доставки	Поддерживаемый в Termidesk протокол удаленного доступа к ВРМ
Связанный клон	Способ организации ВРМ на основе единого образа, с возможностью экономии дискового пространства, за счет технологии «копирование при записи», и ускорения операций возврата к базовому состоянию, установки дополнительного ПО и обновлений
Сессионный агент	Устанавливается на сервер терминалов (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям
Универсальный диспетчер	Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им ВРМ и контроля доставки ВРМ. Устанавливается из пакета <code>termidesk-vdi</code> . Наименование службы после установки: <code>termidesk-vdi.service</code>
Фонд рабочих мест	Также: «фонд ВРМ». Совокупность подготовленных ВРМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей
Шаблон рабочего места	Также: «шаблон ВРМ». Параметры конфигурации базового ВРМ для использования в фонде ВРМ
Шлюз	Отделяемый компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP. Устанавливается из пакета <code>termidesk-vdi</code> . Наименование службы после установки: <code>termidesk-wsproxy.service</code>
STAL	Сервер терминалов Astra Linux. Реализован компонентом «Сервер терминалов» Termidesk. Устанавливается из пакета <code>stal</code>

## 17 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
БД	База данных
ВМ	Виртуальная машина
ВРМ	Виртуальное рабочее место
ЗПС	Замкнутая программная среда
ОС	Операционная система
ПК СВ Брест	Программный комплекс «Средства виртуализации «Брест»
ПО	Программное обеспечение
СУБД	Система управления базами данных
ЭЦП	Электронная цифровая подпись
ALD	Astra Linux Directory (единое пространство пользователей)
API	Application Programming Interface (интерфейс прикладного программирования)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
FreeIPA	Free Identity, Policy and Audit (открытое решение по безопасности Linux-систем)
GID	Group Identification Data (идентификатор группы)
HTML	Hypertext Markup Language (язык гипертекстовой разметки)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
ID	Identification Data (идентификатор)
IP	Internet Protocol (межсетевой протокол)
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов)
MS AD	Microsoft Active Directory (службы каталогов Microsoft)
OU	Organizational Unit (организационная единица)
PAM	Pluggable Authentication Module (подключаемый модуль аутентификации)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)

Сокращение	Пояснение
RDS	Remote Desktop Services (службы удаленного рабочего стола Microsoft)
RDSH	Remote Desktop Session Host (хост сеансов удаленных рабочих столов)
SAML	Security Assertion Markup Language (открытый стандарт обмена данными аутентификации)
SCSI	Small Computer System Interface (набор стандартов для физического подключения и передачи данных между компьютерами и периферийными устройствами)
SPICE	Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)
SSL	Secure Sockets Layer (криптографический протокол)
SSO	Single Sign-On (технология единого входа)
STAL	Terminal Server Astra Linux (сервер терминалов ОС Astra Linux Special Edition (Server))
TCP	Transmission Control Protocol (протокол управления передачей)
Termidesk	Программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk»
TLS	Transport Layer Security (протокол защиты транспортного уровня)
UDP	User Datagram Protocol (протокол пользовательских датаграмм)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
USB	Universal Serial Bus (последовательный интерфейс для подключения периферийных устройств)
UUID	Unique User Identifier (уникальный идентификатор пользователя)
vGPU	Virtual Graphics Processing Unit (виртуальный графический процессор)
VDI	Virtual Desktop Infrastructure (инфраструктура виртуальных рабочих столов)
VNC	Virtual Network Computing (система удаленного доступа к рабочему столу компьютера)
VRRP	Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности)



© ООО «УВЕОН - ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

Адрес: 119415, г. Москва, проспект Вернадского, дом 41, строение 1, офис 645а

Сайт: [www.termidesk.ru](http://www.termidesk.ru)

Телефон: +7 (495) 975-1-975

Общий e-mail: [info@uveon.ru](mailto:info@uveon.ru)

Отдел продаж: [sales@uveon.ru](mailto:sales@uveon.ru)

Техническая поддержка: [support@uveon.ru](mailto:support@uveon.ru)