TERMIDESK

Вариант лицензирования «TermideskTerminal»

# РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-02 90 02

Версия 5.1. Выпуск от ноября 2024

## Настройка программного комплекса

# ОГЛАВЛЕНИЕ

# 1 . ОБЩИЕ СВЕДЕНИЯ

## 1.1 . О документе

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

Во второй части руководства приведена настройка Termidesk, рассмотрены взаимодействие компонентов, разграничение функций по администрированию. Для того чтобы получить информацию об установке программного комплекса, необходимо обратиться к первой части руководства администратора - СЛЕТ.10001-02 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), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

# 2 . ПОЛЬЗОВАТЕЛИ И КОМПОНЕНТЫ TERMIDESK

## 2.1 . Разграничение функций

Предусмотрено следующее разграничение функций по управлению Termidesk:

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

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

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

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

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

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

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

## 2.2 . Схема взаимодействия компонентов и приложений

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

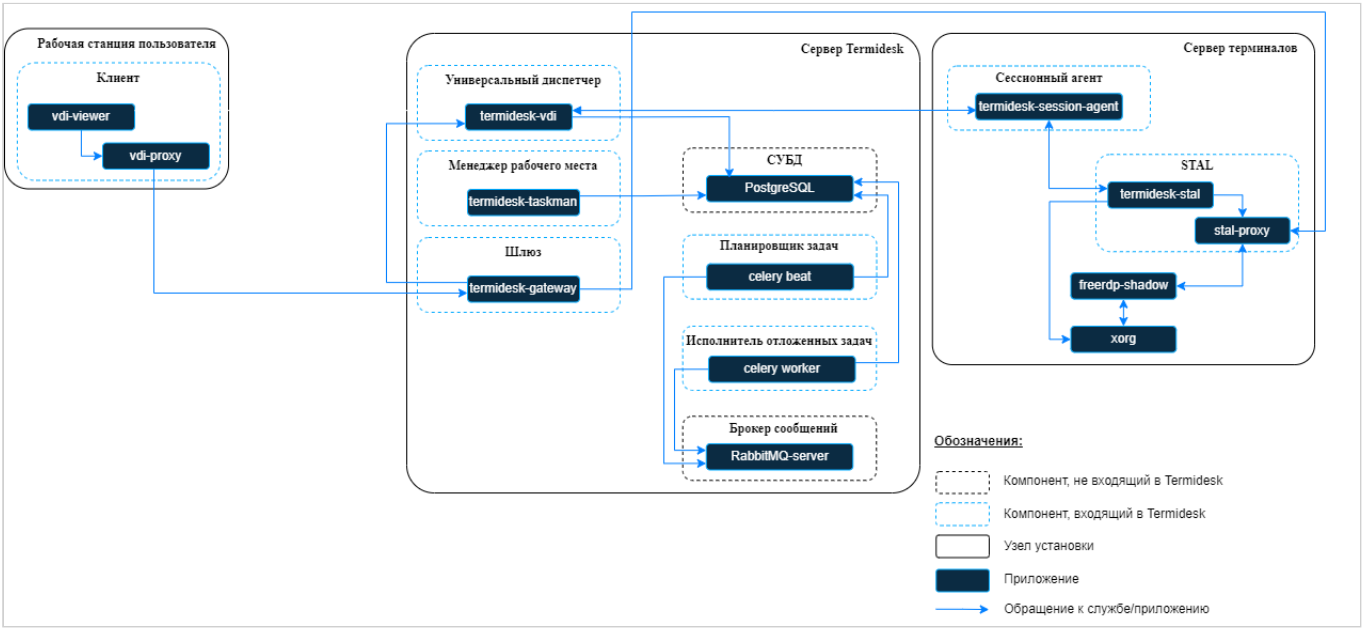


Рисунок 1 – Схема взаимодействия компонентов и процессов

## 2.3 . Схема сетевого взаимодействия компонентов Termidesk

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

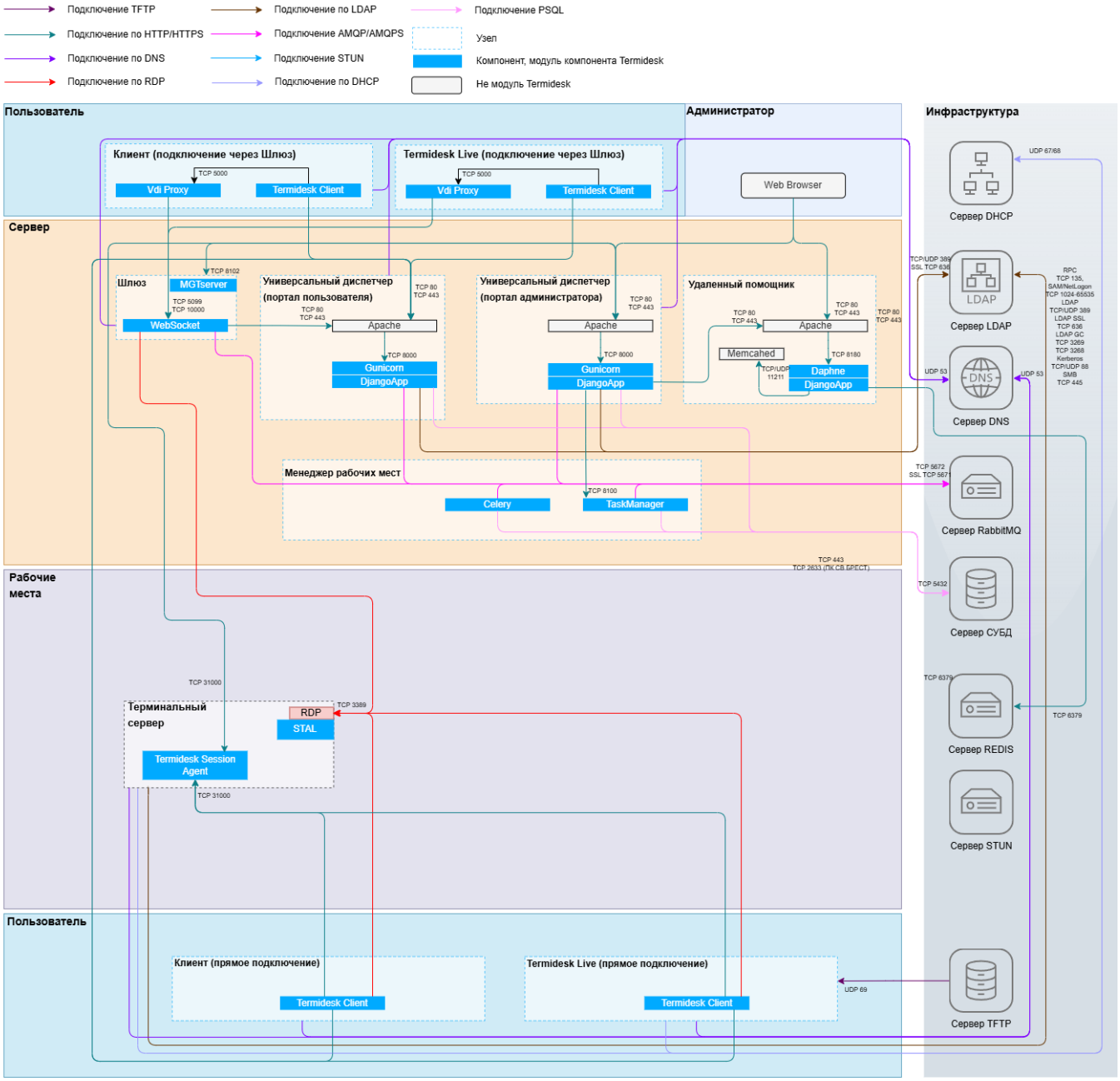


Рисунок 2 – Схема сетевого взаимодействия компонентов Termidesk

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

Таблица 1 – Перечень узлов и компонентов

| Компонент | Наименование на схеме | Узел установки | Наименование пакета установки |
|---|---|---|---|
| «Универсальный диспетчер» | Универсальный диспетчер | Отдельный узел для установки | `termidesk-vdi` |
| «Менеджер рабочих мест» | Менеджер BPM | Отдельный узел для установки или установка совместно с диспетчером | `termidesk-vdi` |
| «Шлюз» | Шлюз | Отдельный узел для установки или установка совместно с диспетчером | `termidesk-vdi` |

| Компонент | Наименование на схеме | Узел установки | Наименование пакета установки |
|---|---|---|---|
| «Сессионный агент» | Сессионный агент | Сервер терминалов (Microsoft Windows Server с ролью «Remote Desktop Services» (далее - MS RDS), Terminal Server Astra Linux (далее - STAL)) | `termidesk-session-agent` |
| «Клиент» | Клиент | Рабочее место пользователя (пользовательская рабочая станция) | `termidesk-client` |
| «Сервер терминалов Astra Linux» | - | Сервер терминалов Astra Linux (STAL), возможна установка на том же узле, где установлен диспетчер | `stal` |

## 2.4 . Последовательность сетевых запросов компонентов Termidesk

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

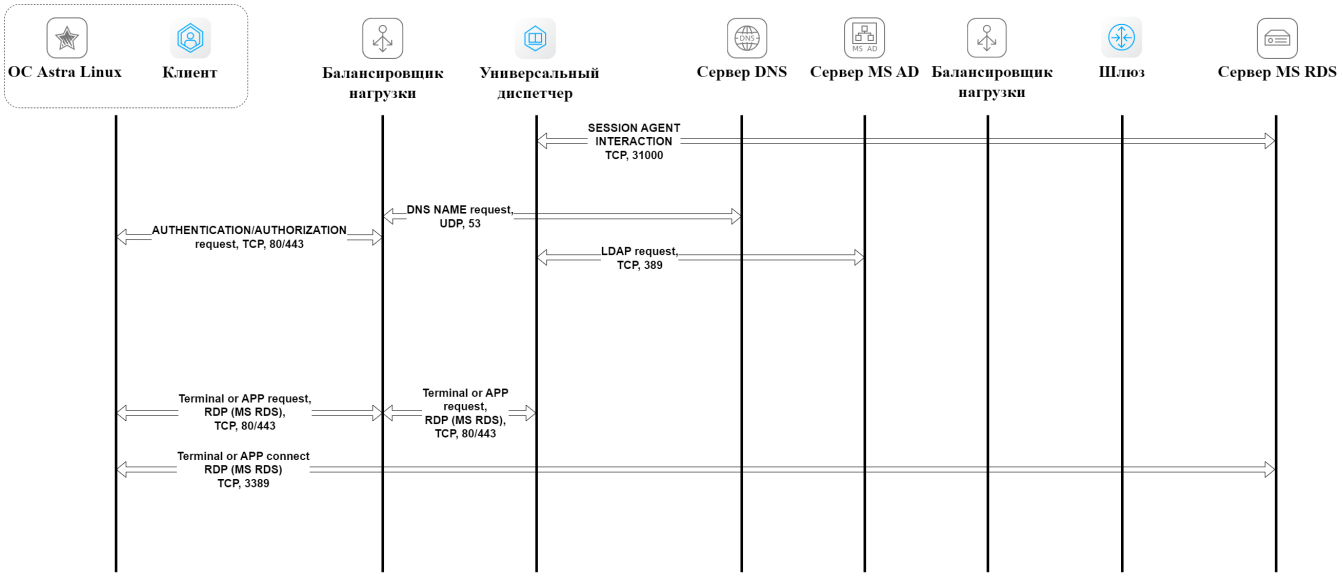


Рисунок 3 – Общая последовательность сетевых запросов

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

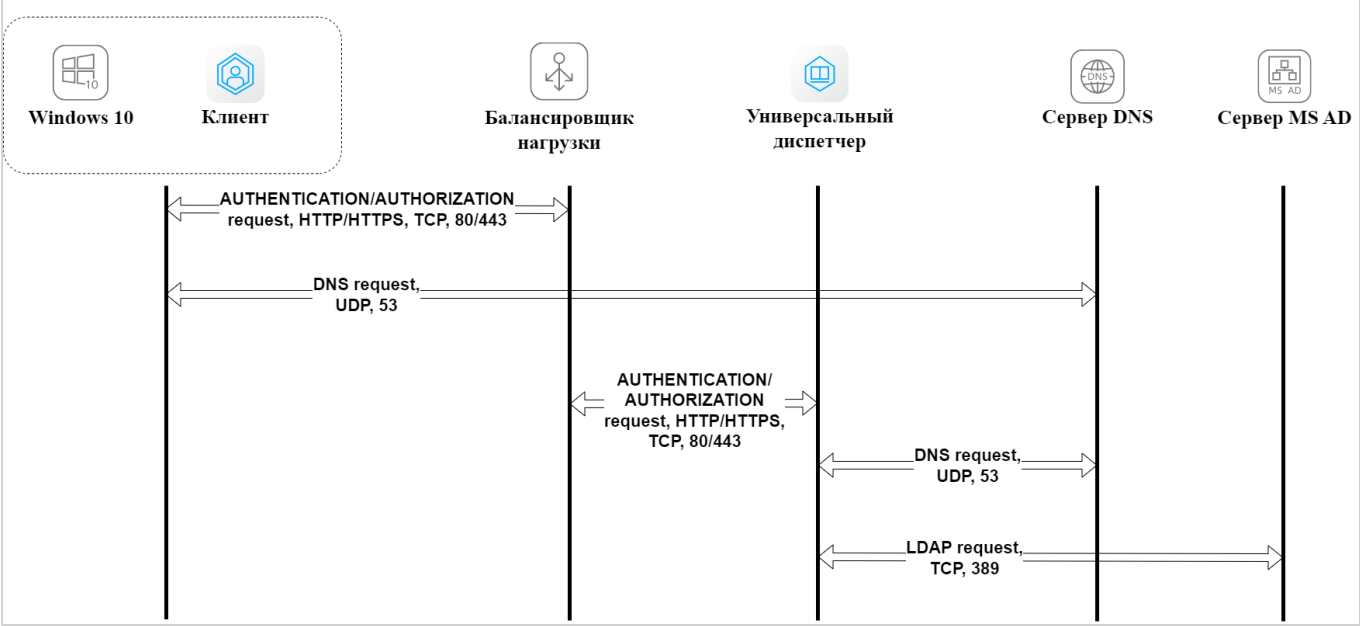


Рисунок 4 – Последовательность сетевых запросов при аутентификации и авторизации

## 2.5 . Перечень сетевых портов компонентов Termidesk

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

Таблица 2 – Перечень сетевых портов, используемых компонентами Termidesk

| Служба | Протокол | Порт |
|---|---|---|
| **«Универсальный диспетчер»** | | |
| HTTP | TCP | 80 |
| LDAP | TCP/UDP | 389 |
| HTTPS | TCP | 443 |
| LDAP SSL | TCP | 636 |
| AMQP (RabbitMQ) | TCP | 5672 |
| AMQPS (RabbitMQ) | TCP | 5671 |
| POSTGRESQL | TCP | 5432 |
| VDI (`termidesk-vdi`) | TCP | 8000 |
| SESSION AGENT (`TermideskSessionAgent`) | TCP | 31000 |
| RPC INTERACTION | TCP | 43900-44000 |
| DNS | UDP | 53 |
| **«Менеджер рабочих мест»** | | |
| POSTGRESQL | TCP | 5432 |
| AMQP (RabbitMQ) | TCP | 5672 |
| AMQPS (RabbitMQ) | TCP | 5671 |

| Служба | Протокол | Порт |
|---|---|---|
| HEALTH_CHECK | TCP | 8100 |
| **«Шлюз»** | | |
| HTTP | TCP | 80 |
| HTTPS | TCP | 443 |
| RDP | TCP | 3389 |
| WSPROXY_HEALTHCHECK | TCP | 8101 |
| WSPROXY (`termidesk-wsproxy`) | TCP | 5099 |
| SPICE | TCP | 5900-6166 |
| DNS | UDP | 53 |
| **Программное обеспечение termidesk-viewer (устанавливается с компонентом «Клиент»)** | | |
| HTTP | TCP | 80 |
| HTTPS | TCP | 443 |
| VNC | TCP | 5900-59XX* |
| SPICE | TCP | 5900-59XX* |
| RDP | TCP | 3389 |
| **«Сессионный агент»** | | |
| SESSION AGENT HTTP/HTTPS (`TermideskSessionAgent`) | TCP | 31000 |
| **«Клиент»** | | |
| HTTP | TCP | 80 |
| HTTPS | TCP | 443 |
| RDP | TCP | 3389 |
| CLIENT (`termidesk-client`) | TCP | 49152-65535** |
| **«Виртуальный модуль Termidesk»** | | |
| ETCD | TCP/UDP | 2379, 2380 |
| **«Сервер терминалов Astra Linux» (STAL)** | | |
| RDP | TCP | 3389 |
| **«Удаленный помощник»** | | |
| HTTP | TCP | 80 |
| HTTPS | TCP | 443 |
| STUN | TCP | 19302 |
| WebRTC | TCP/UDP | 1024-65535 |

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

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

В таблице приняты обозначения:

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

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

Таблица 3 – Перечень правил межсетевого экрана

| Узел-источник | Узел-приемник | Протокол | Порт приемника | Описание |
|---|---|---|---|---|
| «Универсальный диспетчер» | localhost | TCP | 8000 | Работа веб-сервера «Универсального диспетчера» для обслуживания входящих подключений. Порт открывается на localhost |
| | Контроллеры доменов аутентификации | TCP/UDP | 389 | LDAP |
| | | TCP | 3268 | LDAP |
| | | TCP | 636, 3269 | LDAPS |
| | Сервер DNS | UDP | 53 | DNS |
| | «Сессионный агент» | TCP | 31000 | Для обслуживания подключений к серверам терминалов, на которых установлен «Сессионный агент» |
| | СУБД | TCP | 5432 | Для обслуживания запросов к СУБД |
| | Сервер RabbitMQ | TCP | 5672, 5671 (TLS) | Для обслуживания запросов к RabbitMQ |

| Узел-источник | Узел-приемник | Протокол | Порт приемника | Описание |
|---|---|---|---|---|
| | «Шлюз» | TCP | 8102 | Для обслуживания запросов проверок состояния (health check) «Шлюза» |
| | «Менеджер рабочих мест» | TCP | 8100 | Для обслуживания запросов проверок состояния (health check) «Менеджера рабочих мест» |
| Рабочее место администратора | «Универсальный диспетчер» | TCP | 443 | Защищенное подключение к порталу Termidesk |
| | «Удаленный помощник» (серверная часть) | TCP | 80, 443 | Защищенное подключение к серверной части «Удаленного помощника» |
| «Менеджер рабочих мест» | localhost | TCP | 8100 | Для обслуживания запросов проверок состояния (health check) «Менеджера рабочих мест». Порт открывается на localhost |
| | СУБД | TCP | 5432 | Для обслуживания запросов к СУБД |
| | Сервер RabbitMQ | TCP | 5672, 5671 (TLS) | Для обслуживания запросов к RabbitMQ |
| «Шлюз» | localhost | TCP | 5099 | Для обслуживания входящих подключений к «Шлюзу». Порт открывается на localhost, при распределенной установке - на IP-адресе «0.0.0.0» |

| Узел-источник | Узел-приемник | Протокол | Порт приемника | Описание |
|---|---|---|---|---|
| | localhost | TCP | 8102 | Для обслуживания запросов проверок состояния (health check) «Шлюза». Порт открывается на localhost |
| | Сервер DNS | UDP | 53 | DNS |
| «Клиент» | Сервер DNS | UDP | 53 | DNS |
| | «Универсальный диспетчер» | TCP | 80, 443 | Для обслуживания подключений к «Универсальному диспетчеру» |
| | Сервер терминалов | TCP | 3389 | Для обслуживания подключений RDP к серверу терминалов |
| | | TCP | 43900-44000 | Для корректной работы технологии единого входа (SSO) при прямом подключении к РМ (не через «Шлюз») |
| «Сервер терминалов Astra Linux» | Сервер DNS | UDP | 53 | DNS |
| | Контроллеры доменов аутентификации | TCP/UDP | 389 | LDAP |
| | | TCP | 3268 | LDAP |
| | | TCP | 636, 3269 | LDAPS |
| «Виртуальный модуль Termidesk» | «Виртуальный модуль Termidesk» | TCP/UDP | 2379, 2380 | Подключение ETCD для хранения и синхронизации конфигураций между узлами «Виртуального модуля Termidesk» |
| «Удаленный помощник» (клиентская часть) | «Удаленный помощник» (серверная часть) | TCP/UDP | 80, 443 | Для обслуживания подключений к серверной части «Удаленного помощника» |

| Узел-источник | Узел-приемник | Протокол | Порт приемника | Описание |
|---|---|---|---|---|
| | Сервер STUN | TCP | 19302 | Для обслуживания подключений к серверу STUN (stun:// stun.l.google.com: 19302) |
| «Удаленный помощник» (серверная часть) | «Удаленный помощник» (клиентская часть) | TCP | 1024-65535 | Для обслуживания подключений к клиентской части «Удаленного помощника» |

# 3 . НАЧАЛО РАБОТЫ

## 3.1 . Последовательность ввода в действие Termidesk Terminal

Общая последовательность шагов для ввода в действие Termidesk Terminal состоит в следующем:

- подготовка сетевой инфраструктуры в соответствии с требованиями раздела **Требования к среде функционирования** документа СЛЕТ.10001-02 90 01 «Руководство администратора. Установка программного комплекса»;
- установка Termidesk в зависимости от выбранной конфигурации: комплексная или распределенная (см. разделы и подразделы **Подготовка среды функционирования**, **Неавтоматизированная установка Termidesk**, **Распределенная установка программного комплекса** документа СЛЕТ.10001-02 90 01 «Руководство администратора. Установка программного комплекса»). Ввод в домен (при необходимости, согласно схеме сетевой инфраструктуры предприятия);
- при использовании терминального сервера на базе ОС Astra Linux Special Edition - установка компонента STAL (см. подраздел **Установка STAL** документа СЛЕТ.10001-02 90 06 «Руководство администратора. Настройка компонента «Сервер терминалов»). Рекомендуется использовать отдельный узел (физический или виртуальный) и не совмещать установку с сервером Termidesk;
- установка компонента «Сессионный агент» на терминальный сервер (см. подраздел **Установка сессионного Агента** документа СЛЕТ.10001-02 90 04 «Руководство администратора. Настройка компонента «Агент»);
- переход в графический интерфейс Termidesk и добавление поставщика ресурсов в Termidesk (см. раздел **Добавление терминального сервера (MS RDS и STAL) в качестве поставщика ресурсов**);
- добавление необходимого домена аутентификации (при необходимости, если в инфраструктуре используются серверы каталогов) (см. раздел **Аутентификация пользователей**);
- создание шаблона РМ для поставщика «Сервер терминалов» в Termidesk (см. подраздел **Шаблоны РМ для терминальных серверов**);
- добавление протоколов доставки, которые будут использоваться для подключения к РМ (см. раздел **Протоколы доставки**);
- создание и настройка фонда РМ в Termidesk (см. раздел **Фонд рабочих мест**);
- назначение групп в созданном ранее фонде (см. подраздел **Назначение групп доступа фонду РМ**);

- назначение протоколов доставки в созданном ранее фонде (см. подраздел **Назначение протоколов фонду PM**).

# 4 . ПОСТАВЩИКИ РЕСУРСОВ

## 4.1 . Общие сведения о поставщиках ресурсов

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

Поддержка некоторых поставщиков ресурсов может добавляться в режиме экспериментальных функций.

В Termidesk поддерживаются следующие поставщики ресурсов:

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

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

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

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

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

Для сохранения параметров конфигурации необходимо использовать экранную кнопку **[Сохранить]**.

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

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

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

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

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

⚠ Для взаимодействия с терминальным сервером (MS RDS или STAL) необходимо установить компонент «Сессионный агент» в соответствии с подразделом **Установка сессионного Агента** документа СЛЕТ.10001-02 90 04 «Руководство администратора. Настройка компонента «Агент».
Работа с MS RDS поддерживается только при условии развернутой полнофункциональной инфраструктуры MS RDS, при этом роль «Remote Desktop Gateway» должна быть развернута, но не должна использоваться. Если такой инфраструктуры нет, то рекомендуется воспользоваться решением, основанным на поставщике ресурсов «метапоставщик».
Терминальный сервер для ОС Astra Linux реализуется компонентом «Сервер терминалов Asta Linux» (STAL) Termidesk, который может быть установлен на узел совместно с Termidesk, в соответствии с подразделом **Установка STAL** документа СЛЕТ.10001-02 90 07 «Руководство администратора. Настройка компонента «Сервер терминалов».

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

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

Таблица 4 – Данные для добавления сервера терминалов

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

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

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

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

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

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

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

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

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

### 4.3 . Режим техобслуживания поставщика ресурсов

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

Для перевода поставщика ресурсов в режим техобслуживания следует перейти «Компоненты - Поставщики ресурсов» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить» (см. Рисунок 5). Затем подтвердить включение режима (см. Рисунок 6).

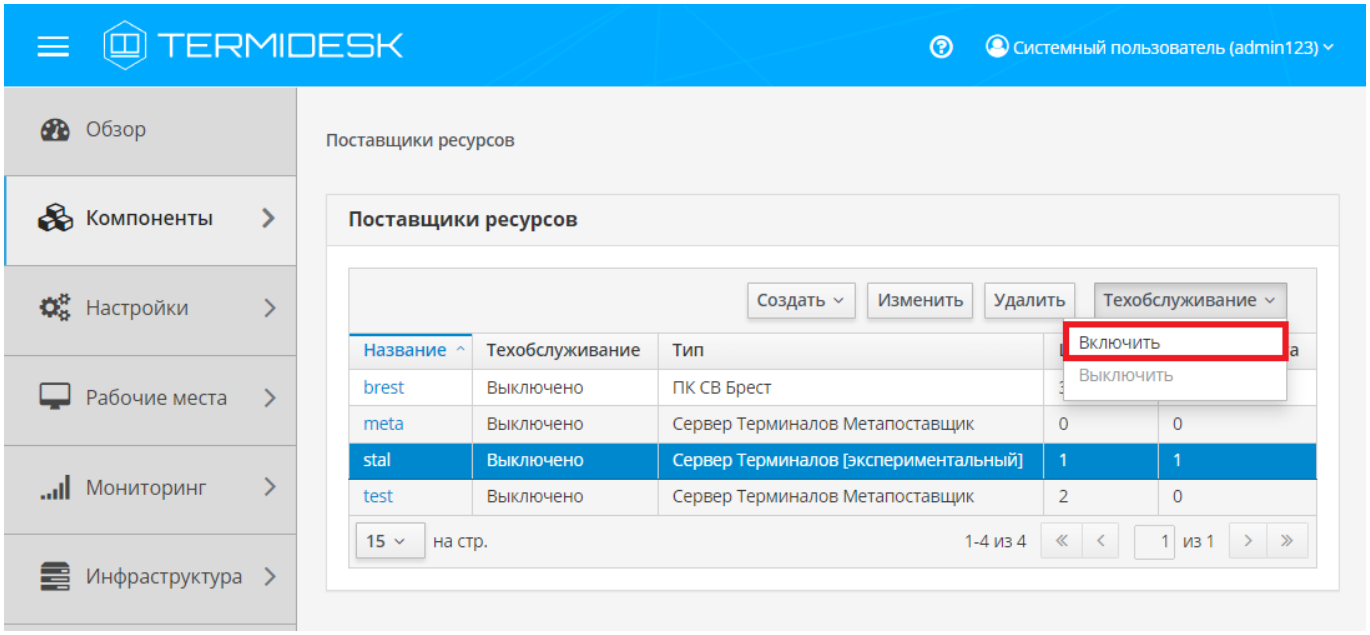


Рисунок 5 – Включение режима техобслуживания поставщика ресурсов

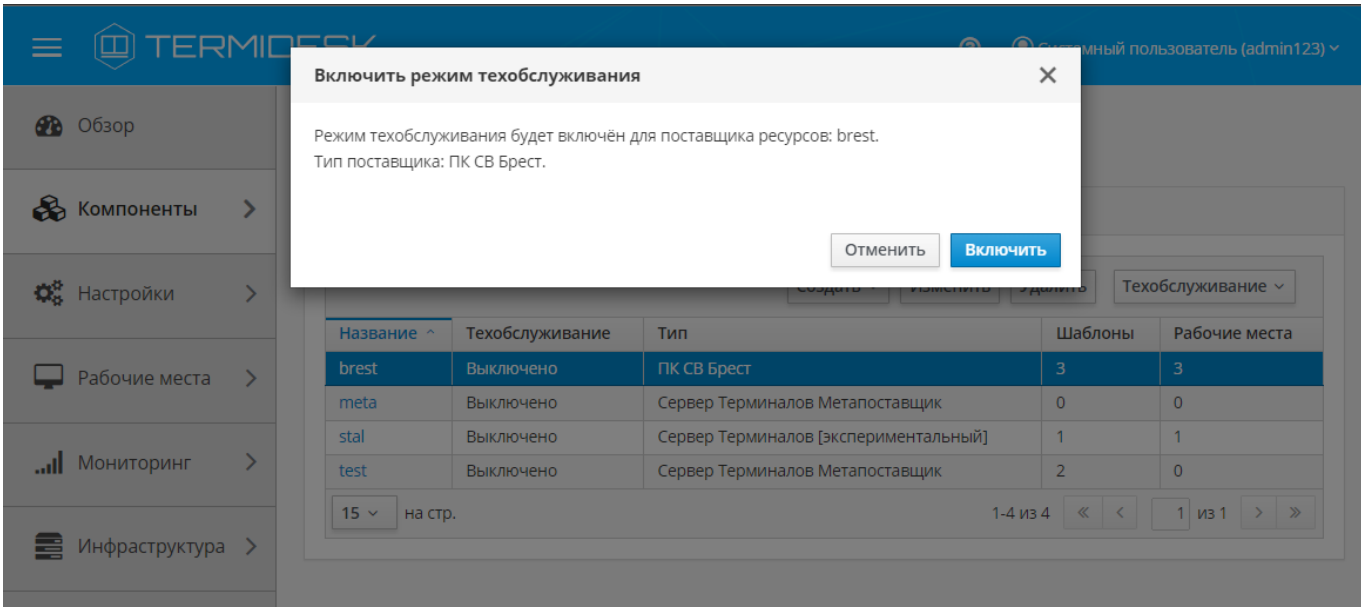


Рисунок 6 – Подтверждение включения режима техобслуживания

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

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

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

# 5 . АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

## 5.1 . Общие сведения о доменах аутентификации

Домен аутентификации - источник сведений о субъектах и их полномочиях.

В Termidesk поддерживаются следующие домены аутентификации:

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

Поддержка некоторых доменов аутентификации может добавляться в режиме экспериментальных функций.

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

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

Созданный домен аутентификации можно отредактировать. Для этого в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем пометить необходимый домен аутентификации и нажать экранную кнопку [Изменить] (см. Рисунок 7).

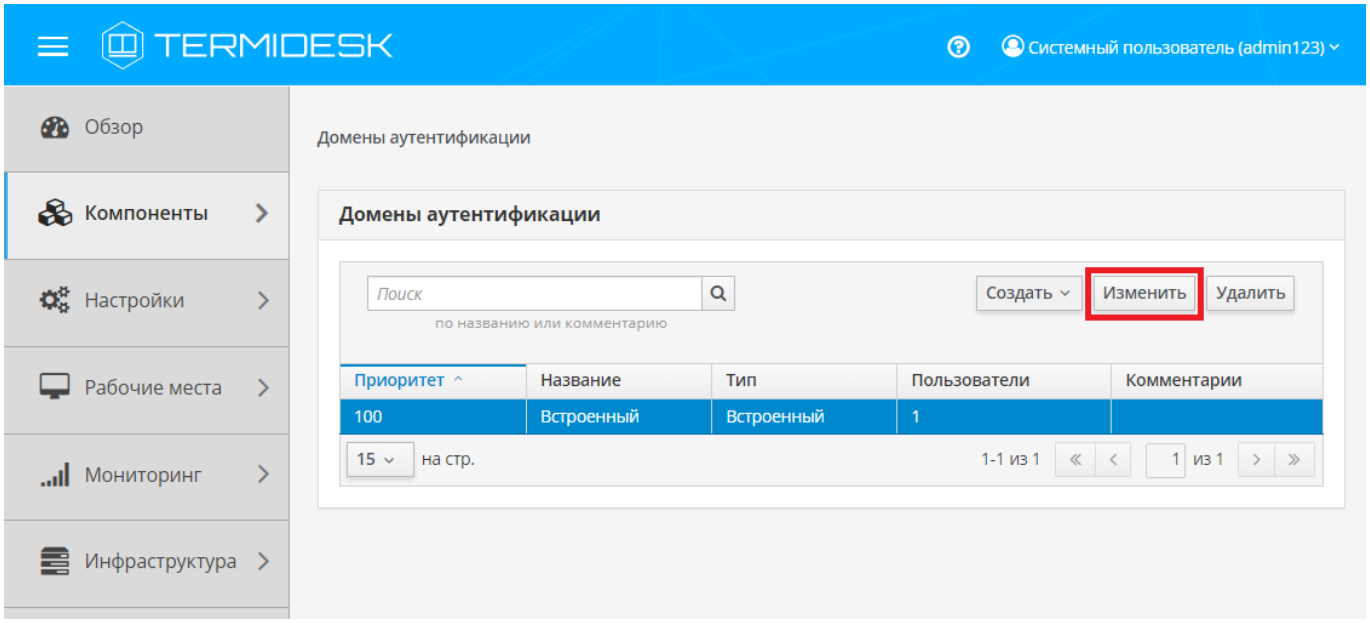


Рисунок 7 – Окно выбора домена аутентификации для редактирования

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

### 5.2.1 . Получение и добавление файла keytab

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

Действия на контроллере домена (например, FreeIPA):

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

```
sudo kinit admin
```

- выполнить команду для добавления узла:

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

где:

`--force` - флаг для принудительного создания;

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

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

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

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

- выполнить команду добавления службы для нового сервисного аккаунта:

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

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

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

где:

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

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

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

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

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

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

где:

`localuser` - имя пользователя целевого узла;

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

После передачи файла на узле Termidesk необходимо выполнить следующее:

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

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

- сделать владельцем этого файла пользователя `termidesk`:

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

- перезапустить службу `termidesk-vdi`:

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

### 5.2.2 . Перечень параметров для добавления аутентификации через FreeIPA

Для добавления аутентификации через FreeIPA администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «FreeIPA».Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 5).

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

Таблица 5 – 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.<br>Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание) |
| «Сервисный аккаунт» | Название сервисного аккаунта, созданного при добавлении поставщика ресурсов |
| «Домен» | Идентификатор области Kerberos для аутентификации |
| «Keytab» | Путь к файлу с ключами для сервисного аккаунта (пример формирования файла приведен в подразделе **Получение и добавление файла keytab**). Каждая генерация `keytab` должна производиться в новый файл. При необходимости повторного использования имени файла существующий файл **обязательно** должен быть удален перед генерацией.<br>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 |

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

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

После включения параметра при переходе «Компоненты - Домены аутентификации» и нажатия экранной кнопки **[Создать]** появятся новые домены аутентификации:

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

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

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

### 5.3 . Добавление аутентификации через ALD Pro

Для добавления аутентификации через ALD Pro администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «ALD Pro». Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 6).

Таблица 6 – Данные для добавления аутентификации через ALD PRO

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование домена аутентификации |
| «Комментарий» | Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях |
| «Приоритет» | Преимущество использования домена аутентификации при проверке субъекта и его полномочий |
| «Метка» | Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk.<br>Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание) |
| «Сервисный аккаунт» | Название сервисного аккаунта, созданного при добавлении поставщика ресурсов |
| «Домен» | Идентификатор области Kerberos для аутентификации |
| «Keytab» | Путь к файлу с ключами для сервисного аккаунта (пример формирования файла приведен в подразделе **Получение и добавление файла keytab**). Каждая генерация `keytab` должна производиться в новый файл. При необходимости повторного использования имени файла существующий файл **обязательно** должен быть удален перед генерацией.<br>Неважно, для какого узла создан `keytab`, необходимо само его наличие |

| Параметр | Описание |
|---|---|
| «Сервер ALD Pro» | IP-адрес или FQDN ресурса, являющегося источником сведений о субъектах и их полномочиях.<br>Можно указать до пяти ресурсов, разделенных символом «;». Ресурсы будут использоваться в указанном порядке: обращение к следующему будет выполняться при недоступности предыдущего |
| «Проверка SSL» | Проверка использования SSL |

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

### 5.4 . Добавление аутентификации через ALD

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

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

Таблица 7 – 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.<br>Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание) |
| «Сервисный аккаунт» | Название сервисного аккаунта, созданного при добавлении поставщика ресурсов |
| «Домен» | Идентификатор области Kerberos для аутентификации |
| «Keytab» | Путь к файлу с ключами для сервисного аккаунта (пример формирования файла приведен в подразделе **Получение и добавление файла keytab**). Каждая генерация `keytab` должна производиться в новый файл. При необходимости повторного использования имени файла существующий файл **обязательно** должен быть удален перед генерацией.<br>Неважно, для какого узла создан `keytab`, необходимо само его наличие |
| «Сервер LDAP (ALD)» | Доменное имя ресурса, являющегося источником сведений о субъектах и их полномочиях |

| Параметр | Описание |
|---|---|
| «Таймаут подключения» | Время ожидания (в секундах) ответа ресурса, являющегося источником сведений о субъектах и их полномочиях |
| «Base DN» | Корень поиска в домене аутентификации |

### 5.5 . Добавление аутентификации через SAML

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

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

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

Таблица 8 – 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.<br>Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание) |
| «ID клиента» | Уникальный идентификатор клиента на сервисе аутентификации SAML |
| «URL метаданных» | URL для подключения к сервису аутентификации SAML |
| «Проверка SSL» | Строгая проверка SSL-сертификатов |
| «Тип биндинга» | Способ отправки ответа сервисом SAML на запрос аутентификации. Поддерживаются следующие типы: HTTP-Redirect, HTTP-POST |
| «Response Binding Type» | Выбор типа биндинга для обратного перенаправления в SAML-запросе. Поддерживаются следующие типы: HTTP-Redirect, HTTP-POST |
| «Приватный ключ» | Набор символов приватного ключа для подписи SAML-запросов |
| «Формат Name ID» | Формат сопоставления идентификаторов имен SAML у поставщиков удостоверений и поставщиков услуг |
| «Group Attr Name» | Тип атрибута пользователя (обычно в этом поле указывается значение «Group») |

| Параметр | Описание |
|---|---|
| «Таймаут» | Время ожидания ответа от SAML, в секундах |

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

## 5.6 . Добавление аутентификации OIDC

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

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

Для добавления аутентификации OIDC следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «OIDC аутентификация».

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 9). Для сохранения параметров конфигурации использовать экранную кнопку **[Сохранить]**.

Таблица 9 – Данные для добавления аутентификации через OIDC

| 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.<br>Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание) |
| «Client ID» | Уникальный идентификатор приложения, полученный от службы идентификации IdP.<br>Пример: «openid-test-cl» |
| «Client secret» | Ключ приложения, полученный от службы идентификации IdP |
| «Authorization endpoint» | URL-адрес авторизации службы идентификации IdP.<br>Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/auth» |
| «Token endpoint» | URL-адрес получения токена службы идентификации IdP.<br>Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/token» |

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

## 5.7 . Добавление IP-аутентификации

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

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

Таблица 10 – 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 |

| Параметр | Описание |
|---|---|
| «Метка» | Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk.<br>Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание) |
| «Разрешить проксирование» | Разрешить субъектам доставку PM, находящихся за прокси-сервером |

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

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

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

Таблица 11 – Данные для добавления аутентификации через MS AD (LDAP)

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование домена аутентификации |
| «Комментарий» | Информационное сообщение, используемое для описания назначения домена аутентификации |
| «Приоритет» | Преимущество использования домена аутентификации при проверке субъекта и его полномочий |
| «Метка» | Информационное поле, используемое для идентификации объекта во внутренней структуре данных.<br>Параметр используется для поиска аналогичного домена «Универсального диспетчера», поэтому должен быть одинаковым как на портале «Агрегатор» (при его использовании), так и на «Универсальном диспетчере».<br>Поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание) |
| «Сервер LDAP» | IP-адрес или доменное имя сервера службы каталогов, являющегося источником сведений о субъектах и их полномочиях |
| «Порт» | TCP-порт, на котором запущена служба каталогов.<br>Возможные стандартные значения:<br>▪ «389» (по умолчанию). Используется, если доступ к службе каталогов реализован осуществляется по протоколу LDAP;<br>▪ «636». Используется, если доступ к службе каталогов реализован осуществляется по протоколу LDAPS;<br>▪ «3268». Альтернативный порт. Используется, если доступ к службе каталогов реализован осуществляется по протоколу LDAP;<br>▪ «3269». Альтернативный порт. Используется, если доступ к службе каталогов реализован осуществляется по протоколу LDAPS.<br>Для ускорения поиска пользователей в службе каталогов рекомендуется указывать альтернативный порт |
| «Использовать SSL» | Использовать защищенное соединение при взаимодействии со службой каталогов |
| «Учетная запись» | Учетная запись в формате Distinguished Name (DN) в домене MS AD (LDAP), используемая для подключения к службе каталогов.<br>Пример: «CN=admin,OU=user,DC=test,DC=desk» |

| Параметр | Описание |
|---|---|
| «Пароль учетной записи» | Набор символов, подтверждающий полномочия объекта для подключения к службе каталогов |
| «Таймаут» | Время ожидания (в секундах) ответа от службы каталогов.<br>Значение по умолчанию: «10» |
| «Base DN» | Корень поиска в службе каталогов в формате DN. Параметру следует задавать значение, соответствующее записи верхнего уровня в иерархии службы каталогов (без указания OU).<br>Вводимое значение не должно содержать пробелов:<br>▪ в начале и конце строки;<br>▪ рядом с разделителями (запятыми);<br>▪ в элементах пути (например, «DC=company name,DC=de»).<br>Пример: «DC=test,DC=desk» |
| «Имя класса пользователя» | Атрибут класса пользователя в службе каталогов.<br>Для корректного заполнения данного поля необходимо указать значение «person» |
| «Атрибут идентификатора пользователя» | Атрибут уникального имени или идентификатора пользователя в службе каталогов.<br>Для корректного заполнения данного поля необходимо указать:<br>▪ значение «name», если активирован параметр «Использовать PKINIT»;<br>⚠ Атрибут идентификатора пользователя задается с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Например, значение «name» для механизма аутентификации Kerberos PKINIT указывается в том случае, если сертификат для подключения выдан на имя пользователя.<br>▪ значение «SamAccountName» в остальных случаях |
| «Список атрибутов пользователя» | Список атрибутов, содержащий уникальные данные пользователя, разделенные запятыми.<br>Для корректного заполнения данного поля необходимо указать значение «name» |
| «Имя атрибута группы» | Атрибут принадлежности к группе в службе каталогов.<br>Для корректного заполнения данного поля необходимо указать значение «group» |
| «Атрибут имени группы» | Атрибут идентификатора группы, к которой относится субъект в службе каталогов.<br>Для корректного заполнения данного поля необходимо указать:<br>▪ значение «distinguishedname», если включены параметры «Использовать рекурсивный поиск групп» или «Использовать обратный порядок проверки членства пользователей»;<br>▪ значение «name», если активирован параметр «Использовать PKINIT»;<br>⚠ Атрибут имени группы задается с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Например, значение «name» для механизма аутентификации Kerberos PKINIT указывается в том случае, если сертификат для подключения выдан на имя пользователя.<br>▪ значение «cn» в остальных случаях.<br>Если используется значение «distinguishedname», то при добавлении группы в домен аутентификации по пути «Компоненты - Домены аутентификации - Наименование домена - Группы» нужно указывать длинные имена групп, например: «CN=RootGroup,CN=Users,DC=test,DC=desk». Если используется значение «cn», то нужно указывать короткие имена групп.<br>Если параметр «Атрибут имени группы» был изменен, то необходимо заново добавить группы, используя соответствующие имена групп: для «cn» - короткие имена, для «distinguishedname» - длинные имена |

| Параметр | Описание |
|---|---|
| «Атрибут членства в группе» | Идентификатор группы для назначения полномочий субъекту.<br>Для корректного заполнения данного поля необходимо указать значение «member» |
| «Атрибут групп для LDAP-запросов» | Атрибут, определяющий группы пользователя при запросах к службе каталогов.<br>Возможные значения: «objectClass», «objectCategory» |
| «Использовать рекурсивный поиск групп» | При запросе групп пользователя будут учтены его родительские группы, в которых он состоит неявно.<br>Если дополнительно включен параметр «Использовать обратный порядок проверки членства пользователей», то параметр «Использовать рекурсивный поиск групп» можно не включать.<br>Возможные значения:<br>▪ «Да» - использовать рекурсивный поиск;<br>▪ «Нет» (по умолчанию) - не использовать рекурсивный поиск |
| «Использовать обратный порядок проверки членства пользователей» | Проверка соответствия членства пользователя в группах службы каталогов членству в группах домена аутентификации. Для работы функционала необходимо, чтобы был задан параметр «Атрибут имени группы».<br>Этот параметр нужно включить при большом количестве групп непосредственно на службе каталогов MS AD. В этом случае сначала будет проверяться вхождение пользователя в группы домена аутентификации (в том числе рекурсивно), затем будет происходить проверка найденных групп в службе каталогов MS AD.<br>При выключении этого параметра применяется настройка выбора «Атрибут групп для LDAP-запросов»: «objectClass» или «objectCategory».<br>При включении этого параметра всегда применяется настройка выбора «Атрибут групп для LDAP-запросов»: «objectClass».<br>Возможные значения:<br>▪ «Да» - использовать обратный порядок;<br>▪ «Нет» (по умолчанию) - не использовать обратный порядок |
| «Использовать PKINIT» | Использовать механизм аутентификации Kerberos PKINIT при аутентификации пользователя. PKINIT - механизм, позволяющий использовать сертификаты X.509 в качестве метода аутентификации.<br>Предполагается, что механизм аутентификации Kerberos PKINIT настроен в инфраструктуре организации и пользователю выданы соответствующие сертификаты и ключи для подключения (персональный сертификат, закрытый ключ к нему и корневой сертификат ЦС, на котором выпущен персональный сертификат).<br>При активации механизма аутентификации Kerberos PKINIT нужно указать актуальный порт в параметре «Порт PKINIT», а также указать нужные значения параметров «Атрибут имени группы» и «Атрибут идентификатора пользователя».<br>Возможные значения:<br>▪ «Да» - использовать механизм;<br>▪ «Нет» (по умолчанию) - не использовать механизм |
| «Порт PKINIT» | TCP/UDP порт, на котором запущена служба Kerberos.<br>Значение по умолчанию: «88» |

### 5.9 . Добавление домена аутентификации RADIUS

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

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

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 12).

Таблица 12 – Данные для добавления аутентификации Radius

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование домена аутентификации |
| «Комментарий» | Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях |
| «Приоритет» | Преимущество использования домена аутентификации при проверке субъекта и его полномочий |
| «Метка» | Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk.<br>Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание) |
| «Radius сервер» | IP-адрес или доменное имя ресурса, являющегося источником сведений о субъектах и их полномочиях (сервер RADIUS) |
| «Аутентификационный порт» | Порт для обработки запросов на аутентификацию |
| «Секрет» | Набор символов (пароль), подтверждающий подключение к серверу RADIUS |
| «Таймаут» | Максимальное время ожидания (в секундах) для установки соединения |

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

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

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

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

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

⚠ Пример настройки приведен для сервера freeRADIUS.

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

```
ldap {
...
  update {
```

```
    ...
    reply:memberOf                  += 'memberOf'
  }
...
}
```

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

```
ATTRIBUTE       memberOf                3001    string
```

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

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

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

```
wait = yes
```

### 5.10 . Добавление аутентификации через внутреннюю БД

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

### 5.11 . Действия над группами в домене аутентификации

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

Доступны следующие действия над группами домена аутентификации:

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

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

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

- «Группа» (см. Рисунок 8) - стандартная группа, созданная в службе каталогов и будет добавлена в Termidesk;
- «Метагруппа» (см. Рисунок 9) - группа, объединяющая несколько стандартных групп в Termidesk.

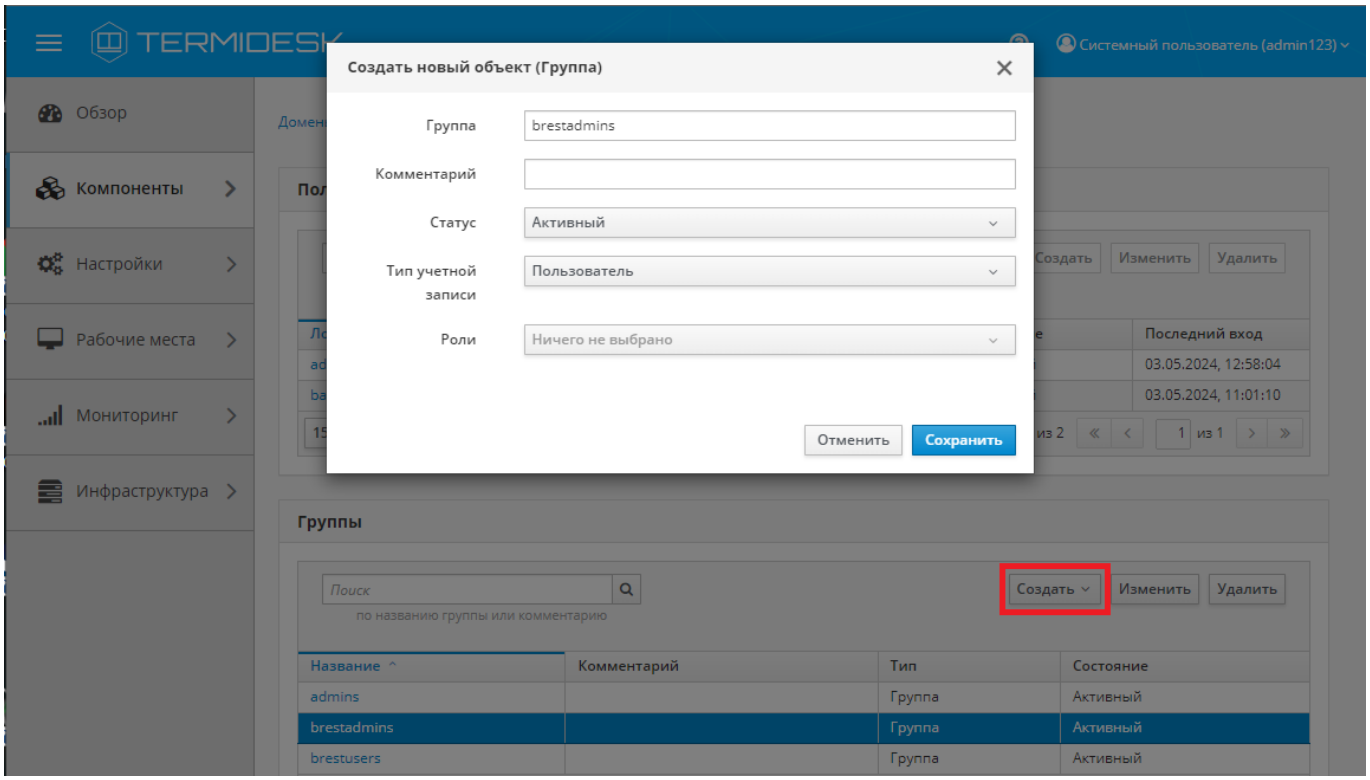


Рисунок 8 – Окно добавления группы домена аутентификации

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

Таблица 13 – Данные для добавления группы домена аутентификации

| Параметр | Описание |
|---|---|
| «Группа» | Наименование группы, полученное от домена аутентификации. Для выбора группы из списка доступных необходимо начать ввод ее наименования |
| «Комментарий» | Информационное сообщение, используемое для описания группы |

| Параметр | Описание |
|---|---|
| «Статус» | Характеристика состояния субъектов группы при доступе к фонду BPM.<br>Доступные значения:<br>▪ «Активный» - субъекты группы могут аутентифицироваться в Termidesk;<br>▪ «Неактивный» - субъекты группы не могут аутентифицироваться в Termidesk;<br>▪ «Временно заблокирован» - субъекты группы не могут аутентифицироваться в Termidesk. Статус присваивается также по истечении попыток аутентификации, определенных в параметрах «Максимум попыток входа Администраторов», «Максимум попыток входа Персонала», «Максимум попыток входа Пользователей» на странице «Настройки - Системные параметры - Безопасность» (см. подраздел **Параметры безопасности Termidesk**) |
| «Тип учетной записи» | Служебные функции субъектов группы при доступе к Termidesk.<br>Доступные значения параметра:<br>▪ «Пользователь» - субъекты группы не будут иметь доступ к порталу администратора. При выборе этого значения параметр «Роли» будет пустым;<br>▪ «Персонал» - субъекты группы будут иметь доступ к странице «Обзор» и будут обладать набором разрешений, определенных служебными функциями. При выборе этого значения в параметре «Роль» можно выбрать одно или несколько значений классов администратора, созданных на странице «Настройки - Управление ролями» (см. подраздел **Назначение служебных функций администраторам**);<br>▪ «Администратор» - субъекты группы будут иметь полный доступ к порталу администратора. При выборе этого значения параметр «Роли» будет пустым |
| «Роли» | Назначение служебных функций пользователям группы.<br>Доступность выбора значений зависит от параметра «Тип учетной записи» и того, созданы ли роли на странице «Настройки - Управление ролями» |

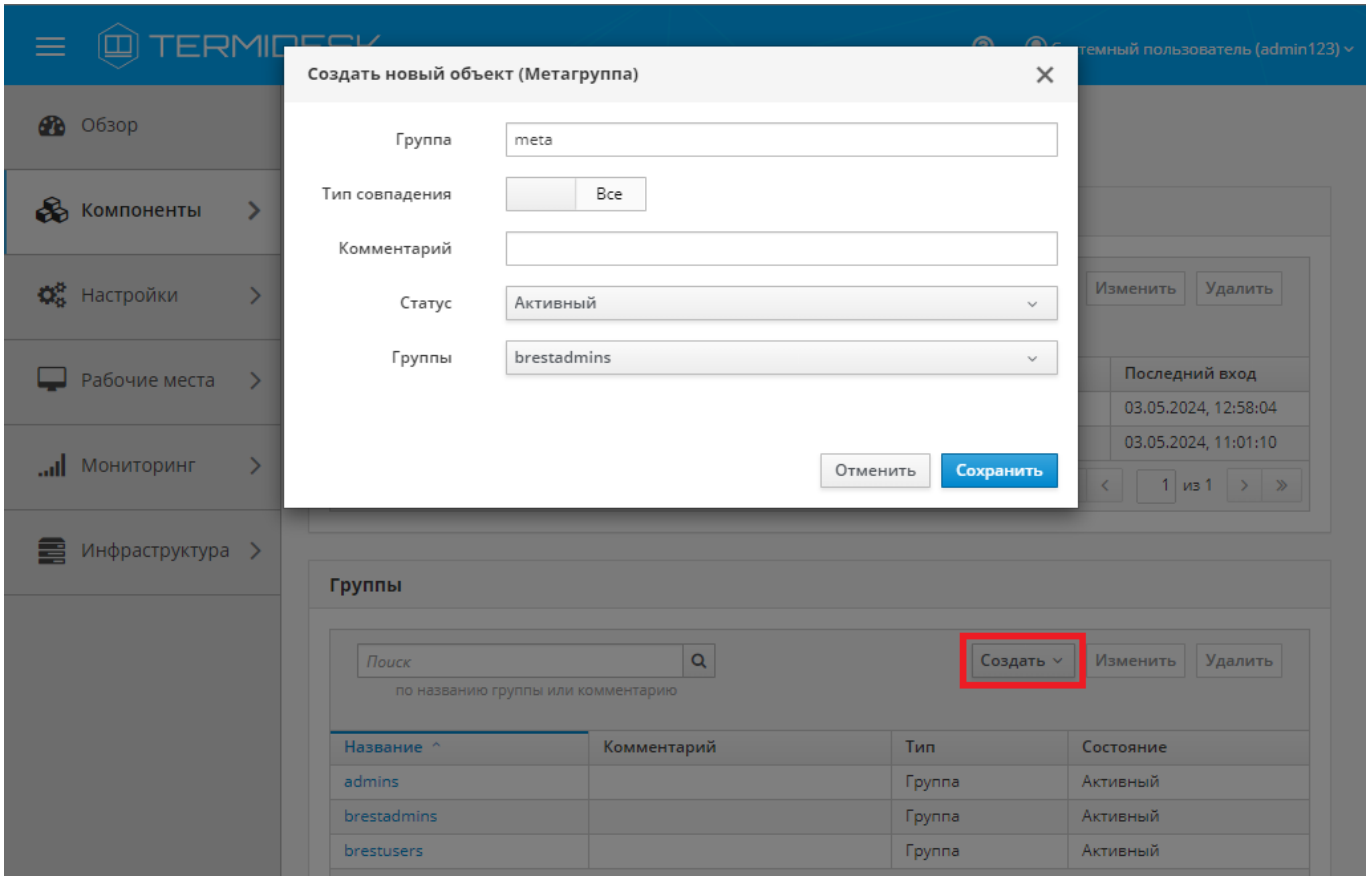


Рисунок 9 – Окно добавления метагруппы домена аутентификации

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

Таблица 14 – Данные для добавления метагруппы домена аутентификации

| Параметр | Описание |
|---|---|
| «Группа» | Наименование группы |
| «Тип совпадения» | Выбор способа определения принадлежности группы к метагруппе.<br>Доступные значения:<br>▪ «Любой» - любая из групп, перечисленных в параметре «Группы»;<br>▪ «Все» (значение по умолчанию) - все группы, перечисленные в параметре «Группы» |
| «Комментарий» | Информационное сообщение, используемое для описания метагруппы |
| «Статус» | Характеристика состояния субъектов метагруппы при доступе к фонду BPM.<br>Доступные значения:<br>▪ «Активный» - субъекты метагруппы могут аутентифицироваться в Termidesk;<br>▪ «Неактивный» - субъекты метагруппы не могут аутентифицироваться в Termidesk |
| «Группы» | Наименования групп, к которым должна примениться метагруппа |

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

открывшемся окне в таблице «Группы» выделить строку с именем пользователя и нажать экранную кнопку **[Изменить]**. В режиме редактирования невозможно изменить идентификатор группы домена аутентификации, поскольку он получен автоматически от службы каталогов.
Для удаления группы используется экранная кнопка **[Удалить]**.

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

### 5.12 . Действия над пользователями в домене аутентификации

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

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

Администратору доступны следующие действия над пользователями внутри домена аутентификации:

- редактирование;
- удаление;
- просмотр сведений.

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

Для отображения списка пользователей следует перейти «Компоненты - Домены аутентификации». Основные параметры списка приведены в таблице (см. Таблица 15).

Таблица 15 – Параметры списка пользователей

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

Для редактирования информации о пользователе следует в столбце «Название» нажать на наименование домена аутентификации и в открывшемся окне в таблице «Пользователи» выделить строку с именем пользователя, нажать экранную кнопку [Изменить] (см. Рисунок 10).

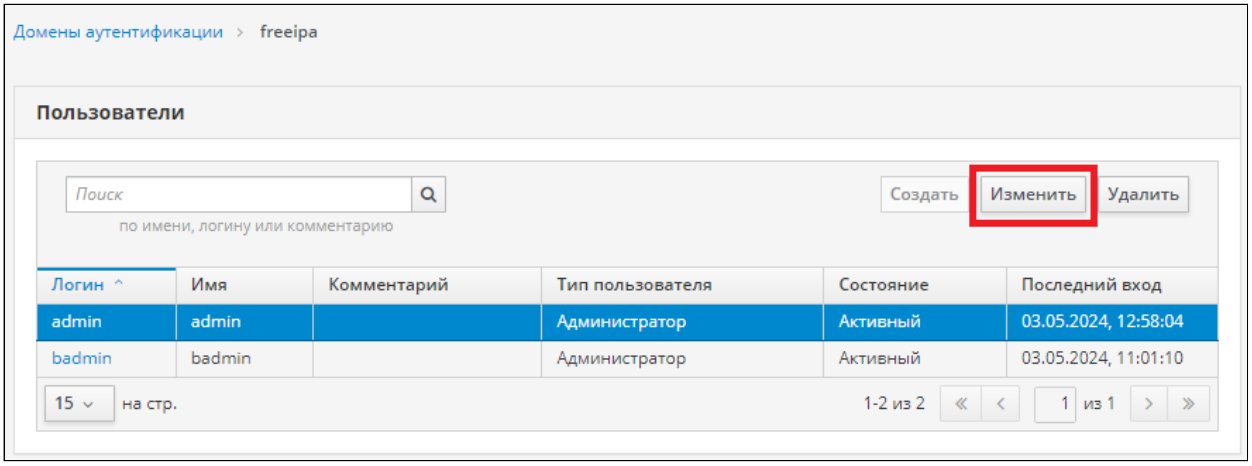


Рисунок 10 – Редактирование пользователя домена аутентификации

Для редактирования пользователя администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 16).

Таблица 16 – Данные для редактирования пользователя домена аутентификации

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

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

Для удаления пользователя из домена аутентификации следует перейти в «Компоненты - Домены аутентификации», в столбце «Название» сводной таблицы нажать на наименование домена

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

### 5.13 . Управление аутентификацией на основе адресов сети

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

Для добавления диапазона сети администратору Termidesk следует перейти «Компоненты - Сети», нажать экранную кнопку **[Создать]**, затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 17).

Таблица 17 – Данные для добавления аутентификации на основе адресов сети

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

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

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

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

# 6 . РАБОЧИЕ МЕСТА

## 6.1 . Общие сведения о РМ

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

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

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

- шаблон на основе связанного клона (только для варианта лицензирования Termidesk VDI) - предполагает создание ВРМ из базового образа на платформе виртуализации в режиме инкрементного копирования;
- шаблон на основе полного клона (только для варианта лицензирования Termidesk VDI) - предполагает создание ВРМ из базового образа на платформе виртуализации в режиме полного копирования;
- связанный клон на базе снапшота (только для варианта лицензирования Termidesk VDI) - предполагает создание ВРМ на основе снимка виртуального жесткого диска базовой ВМ. В этом случае на платформе виртуализации должна быть развернута непосредственно ВМ;
- шаблоны серверов терминалов - предполагают создание РМ на основе терминального доступа или доступа к опубликованным на терминальном сервере приложениям;
- шаблон на основе автономных машин (только для варианта лицензирования Termidesk VDI) - предполагает создание ВРМ на основе шаблона «Автономные машины», созданного для автономной машины.

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

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

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

## 6.2 . Отображение списка РМ из всех фондов

### 6.2.1 . Отображение списка РМ

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

Для получения списка необходимо перейти «Рабочие места - Индивидуальные рабочие места» (см. Рисунок 11) или перейти по ссылке «Рабочие места» из функции «Обзор» (см. Рисунок 12). По умолчанию записи в представленном списке (см. Рисунок 13) будут упорядочены согласно столбцу «Дата создания» по убыванию.

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

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

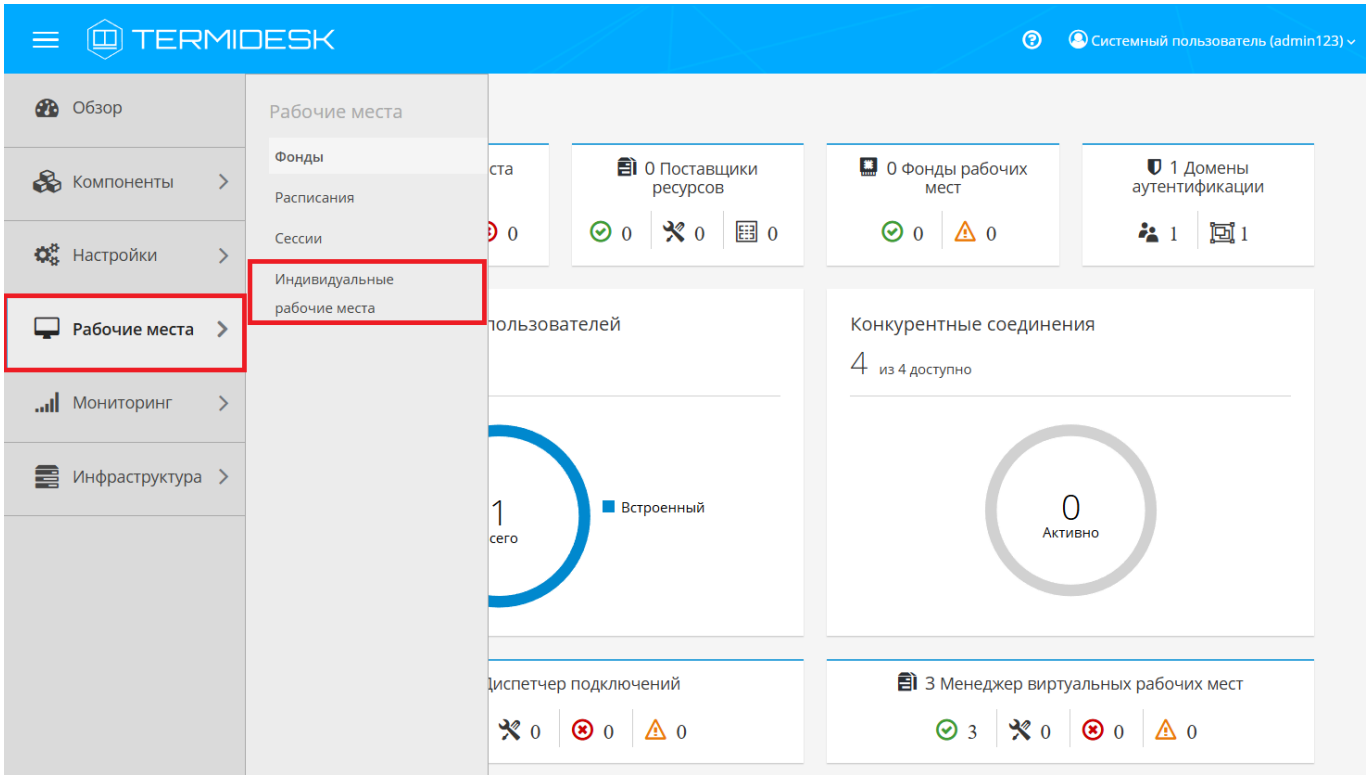


Рисунок 11 – Переход к списку РМ через «Рабочие места - Индивидуальные рабочие места»

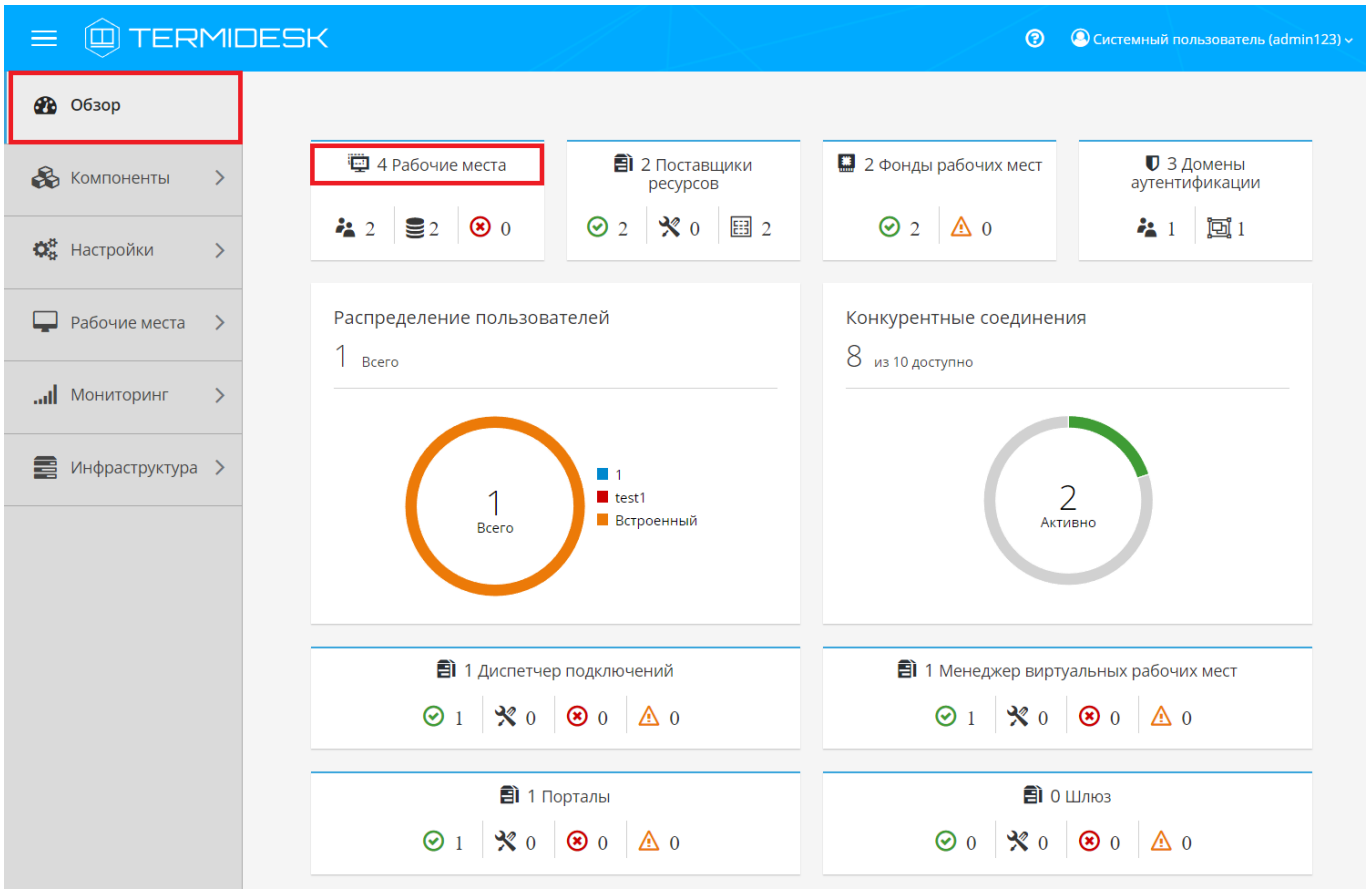


Рисунок 12 – Переход к списку РМ через функцию «Обзор»

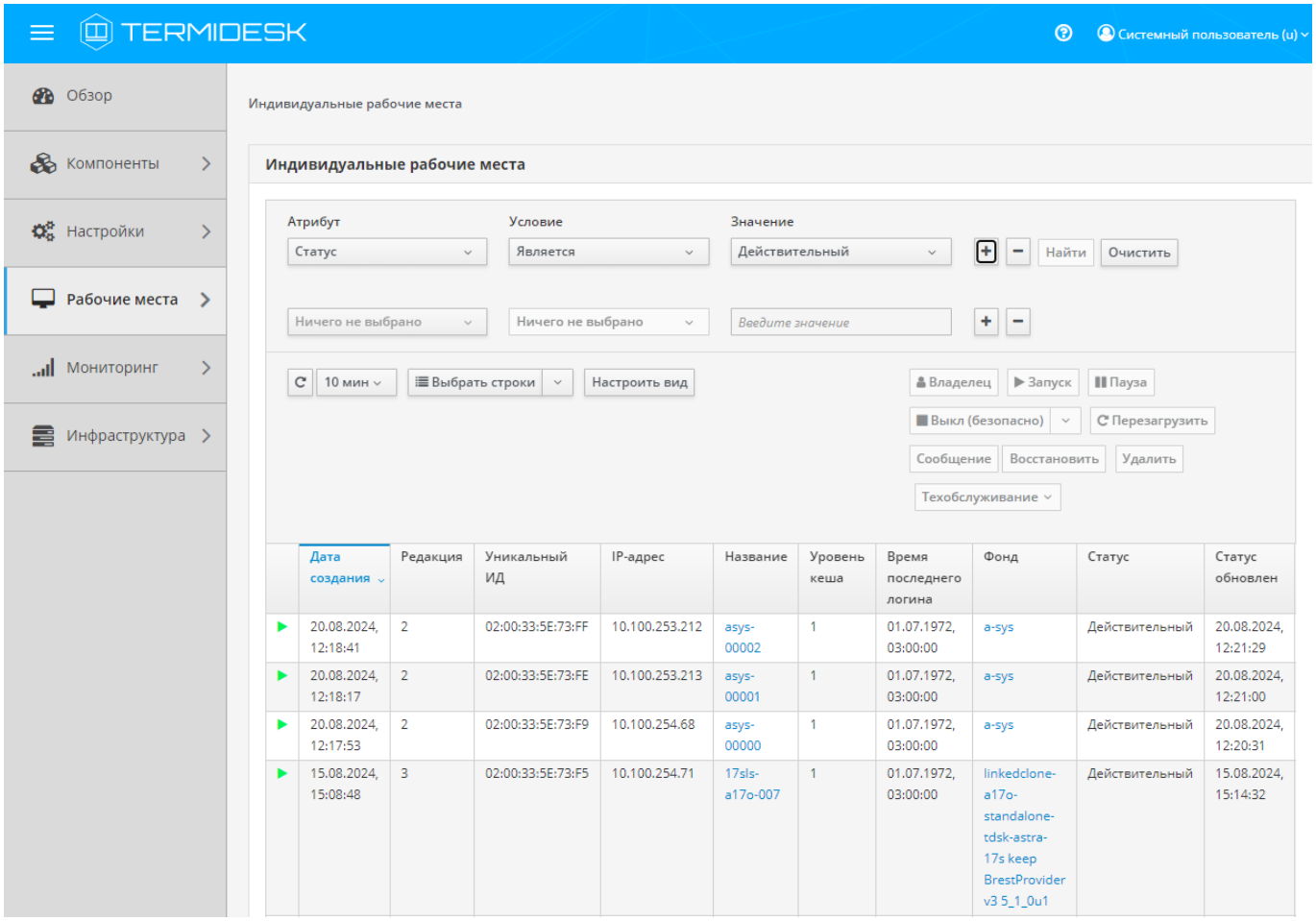


Рисунок 13 – Пример отображения списка РМ

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

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

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

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

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

Для обновления значений таблицы используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список (см. Рисунок 14) со значениями интервала в минутах, расположенный рядом с указанным элементом.

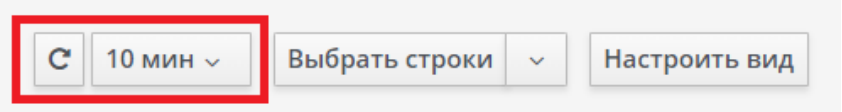


Рисунок 14 – Обновление значений таблицы

Внешний вид таблицы списка РМ можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться экранной кнопкой **[Настроить вид]** и отметить наименования столбцов (см. Рисунок 15), которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для применения изменений нажать экранную кнопку **[Сохранить]**. При попытке убрать выбор со всех пунктов экранная кнопка **[Сохранить]** будет заблокирована. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить вид]**;

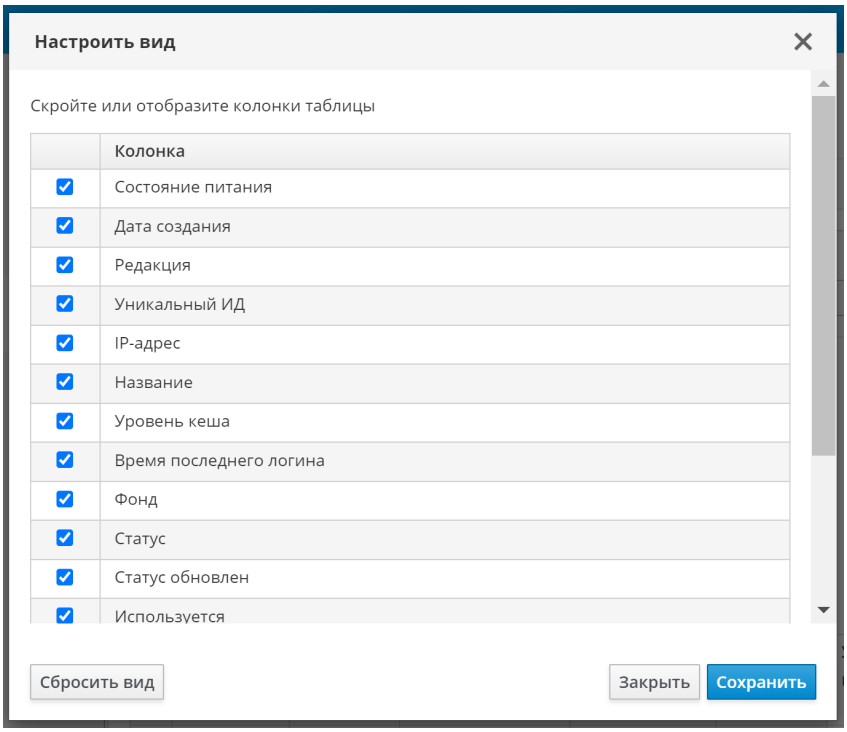


Рисунок 15 – Выбор столбцов для отображения

- порядок следования столбцов. Для изменения порядка следования нужно захватить левой кнопкой мыши заголовок столбца, и, не отпуская ее, перенести его в нужное расположение (см. Рисунок 16). Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок колонок]**, которая становится доступна только после изменения порядка следования столбцов и будет скрыта после сброса;

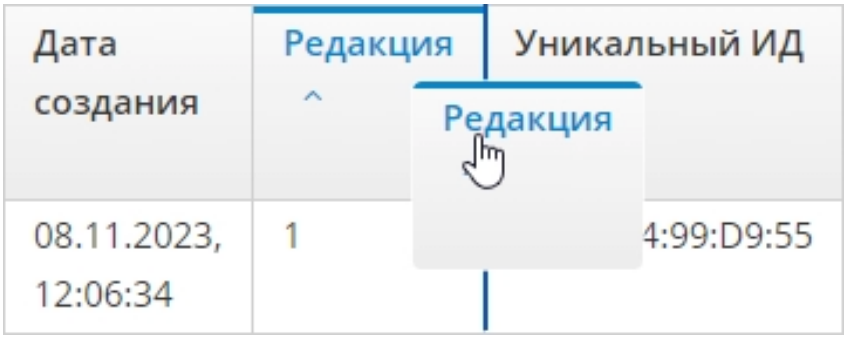


Рисунок 16 – Изменение порядка следования столбцов

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца (см. Рисунок 17).

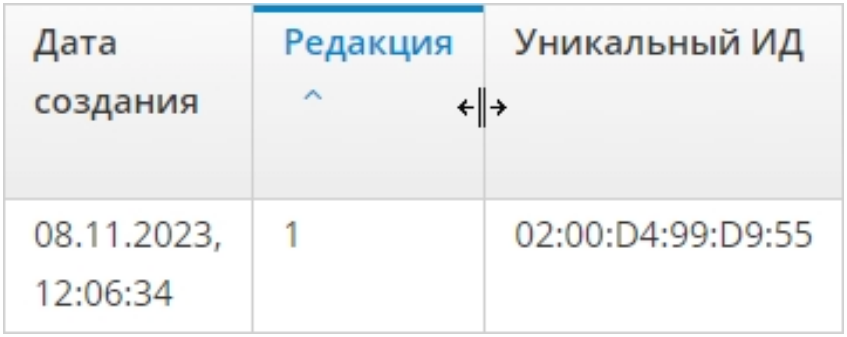


Рисунок 17 – Изменение ширины столбцов

Для сброса ранее выполненных изменений внешнего вида таблицы необходимо нажать экранную кнопку **[Сбросить порядок колонок]**.

Основные параметры списка РМ приведены в таблице (см. Таблица 18).

Таблица 18 – Основные параметры списка BPM

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

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

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

### 6.2.2 . Фильтрация списка РМ

Для списка РМ доступен механизм фильтрации (см. Рисунок 13). Фильтрация осуществляется путем задания значений для параметров «Атрибут», «Условие» и «Значение».

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

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

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

Подробное описание механизма фильтрации списка РМ приведено в таблице (см. Таблица 19).

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

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

Таблица 19 – Параметры фильтрации

| Атрибут | Условия | Значение |
|---|---|---|
| «Дата создания» | Формирование списка РМ по времени создания:<br>▪ «В пределах» - в указанном временном промежутке;<br>▪ «Не в пределах» - исключая указанный временной промежуток | ▪ «Минута»;<br>▪ «5 минут»;<br>▪ «30 минут»;<br>▪ «1 час»;<br>▪ «12 часов»;<br>▪ «24 часа»;<br>▪ «Сегодня»;<br>▪ «Эта неделя»;<br>▪ «Этот месяц» |

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

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

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

## 6.3 . Шаблоны РМ для терминальных серверов

### 6.3.1 . Шаблон для доступа к терминальному серверу MS RDS

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

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «RDS Terminal Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 20).

Таблица 20 – Данные для добавления шаблона для доступа к терминальному серверу MS RDS

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

### 6.3.2 . Шаблон для доступа к опубликованным приложениям MS RDS

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

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «RDS Remote App Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 21).

Таблица 21 – Данные для добавления шаблона для доступа к приложениям MS RDS

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование шаблона |

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

### 6.3.3 . Шаблон для доступа к терминальному серверу STAL

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

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «STAL Terminal Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 22).

Таблица 22 – Данные для добавления шаблона для доступа к терминальному серверу STAL

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

### 6.3.4 . Шаблон для доступа к опубликованным приложениям STAL

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

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «STAL Remote App Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 23).

Таблица 23 – Данные для добавления шаблона для доступа к приложениям STAL

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

## 6.4 . Настройка технологии единого входа

### 6.4.1 . Активация технологии единого входа на терминальном сервере MS RDS

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

- на контроллере домена MS AD создать групповую политику с названием SSO;
- в созданную групповую политику внести следующие изменения:

- в редакторе групповой политики перейти «Конфигурация компьютера - Административные шаблоны - Система - Передача учетных данных», выбрать параметр «Разрешить передачу учетных данных, установленных по умолчанию» и присвоить ему значение «Включено». Затем нажать экранную кнопку **[Добавить серверы в список]** и задать значение «TERMSRV/disp.termidesk.local» (см. Рисунок 18), где `disp.termidesk.local` - имя узла с «Универсальным диспетчером» Termidesk. Далее нажать экранные кнопки **[OK]** и **[Применить]**;

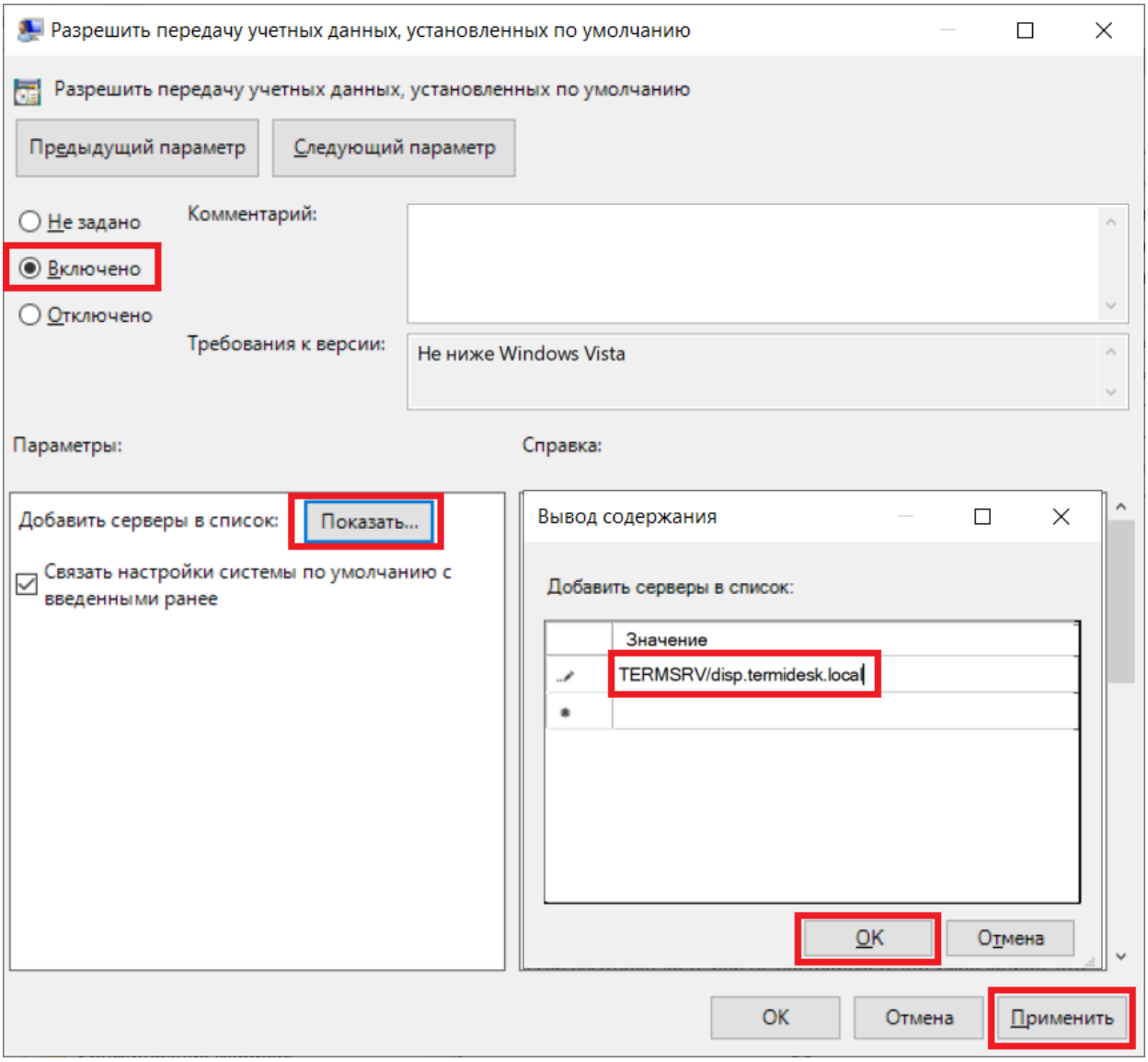


Рисунок 18 – Редактирование параметра «Разрешить передачу учетных данных, установленных по умолчанию» групповых политик

- в этом же списке выбрать параметр «Разрешить передачу новых учетных данных с проверкой подлинности сервера «только NTLM» и присвоить ему значение «Включено». Затем нажать экранную кнопку **[Добавить серверы в список]** и задать

значение «TERMSRV/disp.termidesk.local» (см. Рисунок 18). Далее нажать экранные кнопки **[OK]** и **[Применить]**;

- в редакторе групповой политики перейти «Конфигурация компьютера - Административные шаблоны - Компоненты Windows - Службы удаленных рабочих столов - Клиент подключения к удаленному рабочему столу», выбрать параметр «Запрашивать учетные данные на клиентском компьютере» и присвоить ему значение «Отключено».

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

# 7 . УПРАВЛЕНИЕ ПАРМЕТРАМИ ГОСТЕВЫХ ОС

⚠ Раздел приведен в качестве справки. При настройке Termidesk в варианте лицензирования Termidesk Terminal параметры гостевых ОС не используются.

## 7.1 . Общие сведения о параметрах гостевых ОС

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

Веб-интерфейс Termidesk с установленной ролью «Портал администратора» обеспечивает следующие операции управления параметрами гостевых ОС:

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

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

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

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

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

## 7.2 . Параметры гостевой ОС Microsoft Windows

### 7.2.1 . Конфигурация без домена

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

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 24).

Таблица 24 – Данные для гостевой ОС Microsoft Windows без ввода в домен

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

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

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

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 25).

Таблица 25 – Данные для гостевой ОС Microsoft Windows при вводе в домен MS AD

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

### 7.2.3 . Конфигурация ОС Windows при использовании автономной машины

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

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

Таблица 26 – Данные для ОС Windows при использовании автономной машины

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

## 7.3 . Параметры гостевой ОС Linux

### 7.3.1 . Конфигурация без домена

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

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 27).

Таблица 27 – Данные для гостевой ОС Linux без ввода в домен

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование параметров гостевой ОС |

| Параметр | Описание |
|---|---|
| «Комментарий» | Информационное сообщение, используемое для описания назначения параметров гостевой ОС |

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

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

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 28).

Таблица 28 – 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 РМ в домен |
| «Пароль» | Набор символов, подтверждающий назначение полномочий |
| «OU» | Идентификатор организационной единицы, в которую будут добавлены РМ (опционально).<br>Следует учесть, что при вводе гостевой ОС в домен MS AD:<br>▪ если учетная запись РМ находится не в стандартном каталоге «Computers», то параметр «OU» должен принимать значения вида: «OU=Computers,DC=domain,DC=local», т.е. не должен использоваться Common Name (CN);<br>▪ если учетная запись РМ находится в стандартном каталоге «Computers», то параметр «OU» должен принимать значения вида: «CN=Computers,DC=domain,DC=local», т.е. должен использоваться Common Name (CN) |

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

### 7.3.3 . Конфигурация при вводе в домен FreeIPA

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

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 29).

Таблица 29 – 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 РМ в домен |
| «Пароль» | Набор символов, подтверждающий назначение полномочий |

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

### 7.3.4 . Конфигурация при вводе в домен ALD Pro

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

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 30).

Таблица 30 – Данные для гостевой ОС Linux при вводе в домен ALD Pro

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование параметров гостевой ОС |
| «Комментарий» | Информационное сообщение, используемое для описания назначения параметров гостевой ОС |
| «Домен аутентификации» | Идентификатор домена ALD Pro |
| «Аккаунт» | Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен |
| «Пароль» | Набор символов, подтверждающий назначение полномочий |

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

### 7.3.5 . Конфигурация при вводе в домен ALD

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

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 31).

Таблица 31 – Данные для гостевой ОС Linux при вводе в домен ALD

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование параметров гостевой ОС |

| Параметр | Описание |
|---|---|
| «Комментарий» | Информационное сообщение, используемое для описания назначения параметров гостевой ОС |
| «Домен аутентификации» | Идентификатор домена ALD |
| «Аккаунт» | Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен |
| «Пароль» | Набор символов, подтверждающий назначение полномочий |

### 7.3.6 . Конфигурация ОС Linux при использовании автономной машины

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

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 32).

Таблица 32 – Данные для ОС Linux при использовании автономной машины

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

## 7.4 . Действие при выходе пользователя из ОС

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

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

## 7.5 . Изменение изображения гостевых ОС

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

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

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

Требования к изображению:

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

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

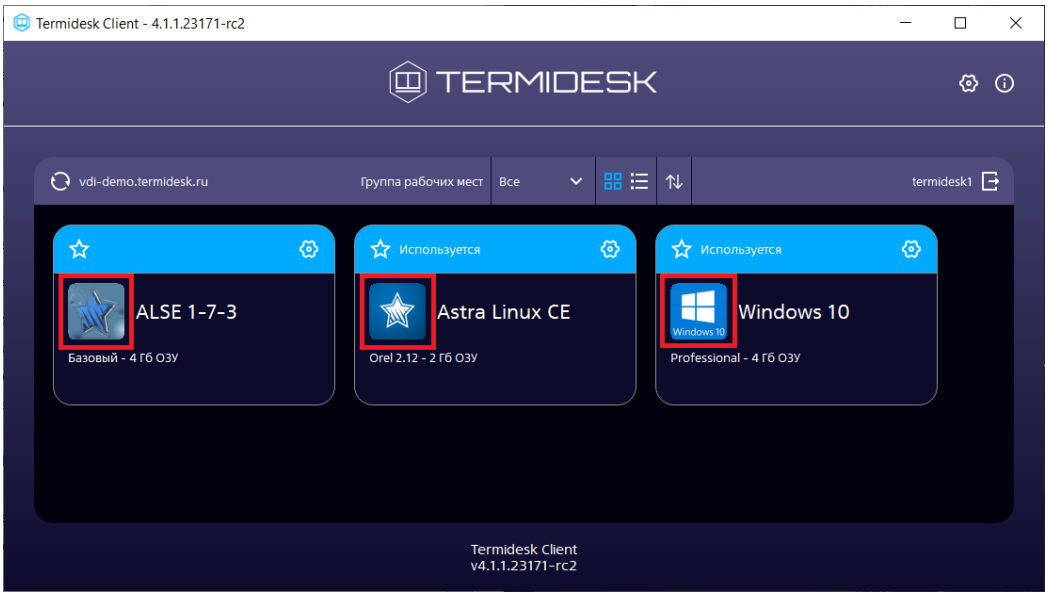


Рисунок 19 – Отображение назначенных изображений в сеансе пользователя

# 8 . ФОНД РАБОЧИХ МЕСТ

## 8.1 . Общие сведения о фонде РМ

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

Для отображения списка фондов РМ следует перейти «Рабочие места - Фонды». Основные параметры списка приведены в таблице (см. Таблица 33).

Таблица 33 – Параметры списка фондов

| Параметр | Описание |
|---|---|
| «Фонд рабочих мест» | Наименование фонда РМ |
| «Статус» | Состояние готовности фонда РМ |
| «Места» | Общее количество РМ в фонде |
| «Готовятся» | Количество подготавливаемых РМ |
| «Выбор протокола» | Флаг возможности выбора пользователем протокола доставки при работе с фондом РМ.<br>Значение определяется политикой фонда РМ «Выбор пользователем протокола доставки» |
| «Группа рабочих мест» | Принадлежность фонда группе РМ |
| «Шаблон» | Шаблон РМ, примененный в фонде |
| «Комментарий» | Информационное сообщение, используемое для описания назначения фонда РМ |

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

Созданные фонды можно:

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

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

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

На открывшейся странице будут представлены следующие разделы:

- «Рабочие места» – список ВМ и информация о подготовленных РМ, используемых субъектами;

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

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

## 8.2 . Добавление фонда РМ

### 8.2.1 . Добавление фонда РМ

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

Откроется мастер публикации фонда (см. Рисунок 20). Необходимо заполнить параметры, указанные в таблице, (см. Таблица 34) и нажать экранную кнопку **[Далее]**. При нажатии экранной кнопки **[Отменить]**, или клавиши **<Esc>**, или иконки «Крестик», на любом из этапов работы произойдет закрытие мастера без сохранения настроек.

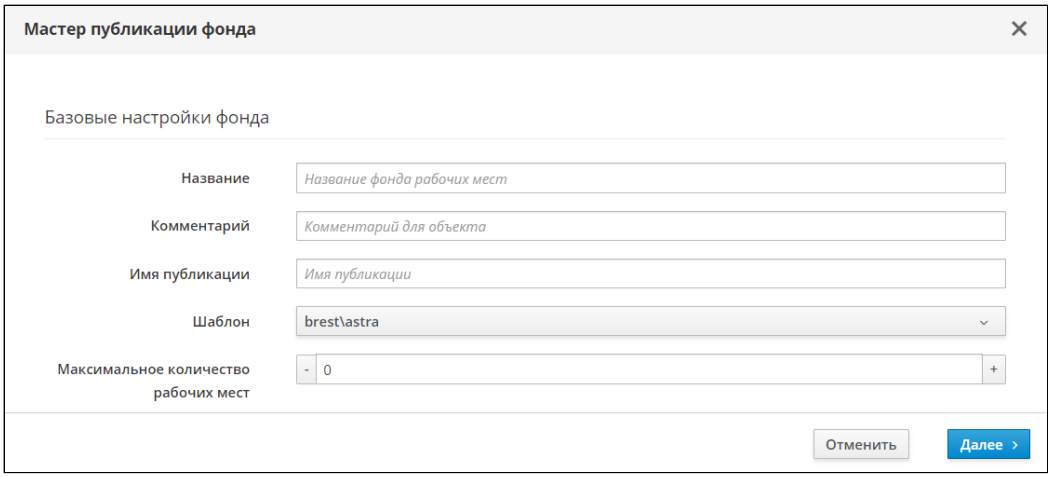


Рисунок 20 – Базовые настройки фонда в Мастере публикации

Таблица 34 – Базовые настройки фонда

| Параметр | Описание |
|---|---|
| «Название» | Ввести текстовое наименование фонда. Наименование может содержать только латинские буквы, цифры, пробел, дефис и нижнее подчеркивание.<br>Параметр обязателен для заполнения |
| «Комментарий» | Ввести информационное сообщение, используемое для описания назначения фонда |
| «Имя публикации» | Ввести текстовое наименование публикации. Параметр применяется для георасределенной установки и позволяет отображать однообразные фонды РМ в виде единого ярлыка в компоненте «Клиент». Для этого на каждой из установок компонента «Универсальный диспетчер» в базовых настройках фонда следует задавать идентичное значение параметра.<br>Параметр обязателен для заполнения |
| «Шаблон» | Выбрать из списка шаблон, который будет использоваться при создании |
| «Максимальное количество рабочих мест» | Задать максимальное количество РМ в фонде.<br>Максимальное число РМ не может быть меньше значения, указанного в параметре «Кеш рабочих мест 1-го уровня» на следующем шаге мастера |

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

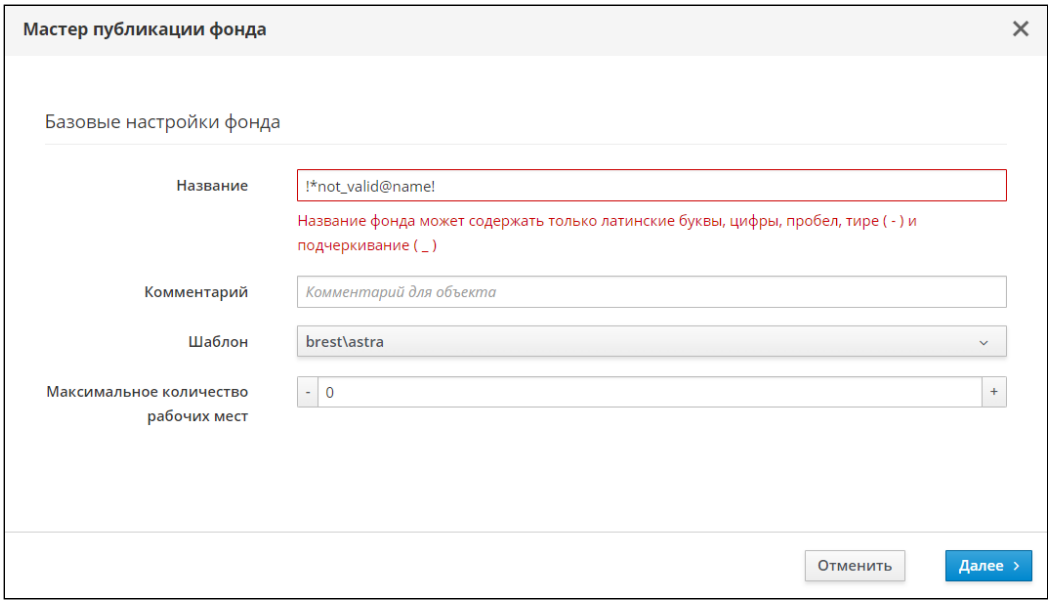


Рисунок 21 – Пример сообщения об ошибке

Далее будет выполнен переход на следующий шаг настройки (см. Рисунок 22) мастера публикации фонда, в котором нужно заполнить параметры, указанные в таблице (см. Таблица 35). Поскольку во время перехода выполняется отправка данных на сервер, возможна ситуация, что при возвращении

на предыдущий шаг появится сообщение об ошибке, если параметр «Протоколы доставки» не был заполнен. Отправка данных на сервер происходит всегда при переходе между шагами, кроме перехода назад с завершающего этапа.

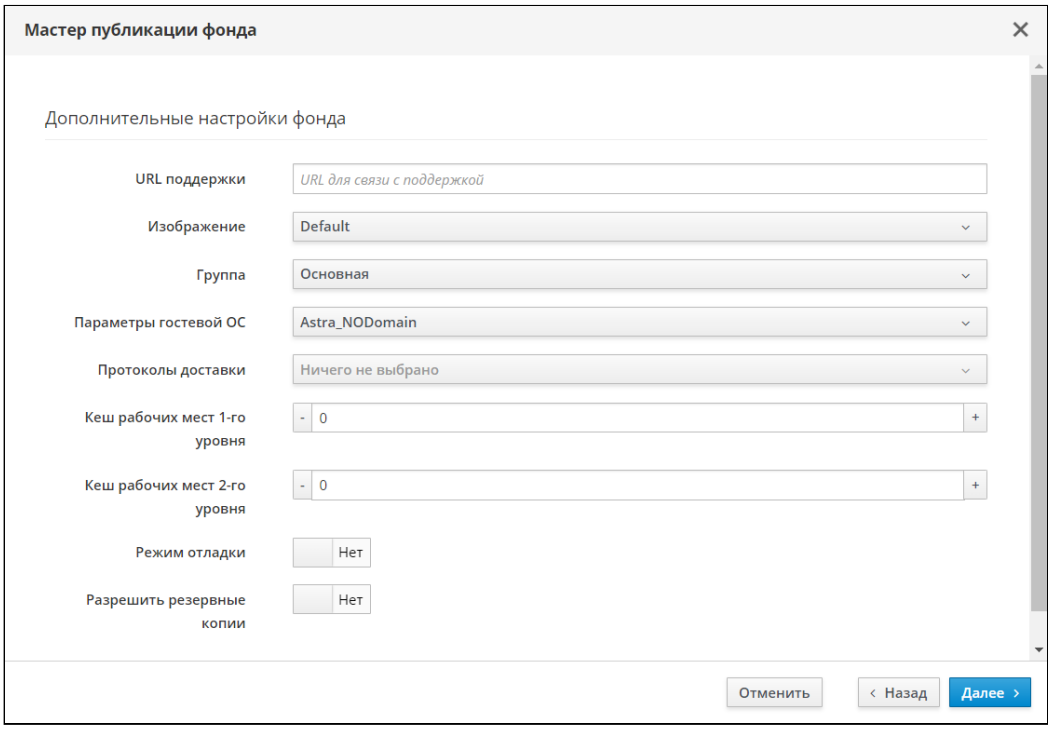


Рисунок 22 – Дополнительные настройки фонда Мастера публикации

Таблица 35 – Дополнительные настройки фонда

| Параметр | Описание |
|---|---|
| «URL поддержки» | Ввести URL для связи с технической поддержкой |
| «Изображение» | Выбрать графическое представление фонда |
| «Группа» | Выбрать группу рабочих мест, в которой будет отображаться созданный фонд |
| «Параметры гостевой ОС» | Выбрать параметры конфигурации гостевой ОС, которые будут использованы при создании РМ |
| «Протоколы доставки» | Выбрать один или несколько протоколов доставки, которые будут доступны для фонда |
| «Кеш рабочих мест 1-го уровня» | Задать количество созданных, настроенных и запущенных РМ в фонде<br>⚠ Параметр не задается, если создается фонд РМ для терминальных серверов. |

| Параметр | Описание |
|---|---|
| «Кеш рабочих мест 2-го уровня» | Задать количество созданных, настроенных и выключенных РМ.<br>Для использования кеша рабочих места 2-го уровня необходимо, чтобы в параметре «Кеш рабочих мест 1-го уровня» было задано хотя бы одно РМ<br>⚠ Параметр не задается, если создается фонд РМ для терминальных серверов. |
| «Режим отладки» | Активация более подробной детализации логов для фонда, по умолчанию режим отключен.<br>При включении режима Termidesk перестает удалять ВМ в фонде |
| «Разрешить резервные копии» | Активация режима резервного копирования ВМ фонда при использовании системы Rubackup.<br>По умолчанию режим отключен |

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

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

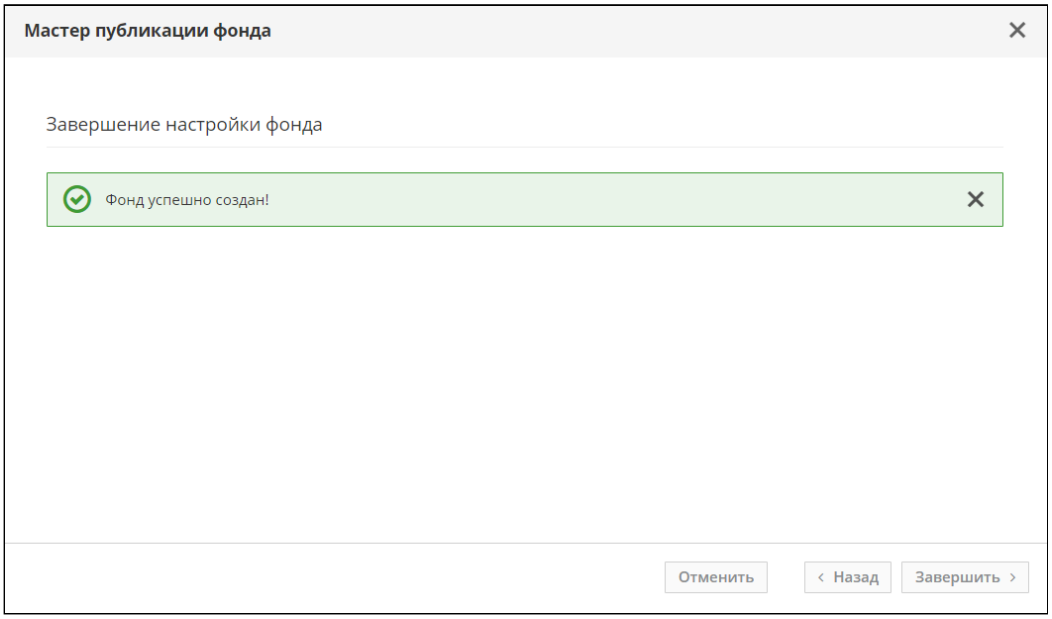


Рисунок 23 – Успешное завершение настройки публикации фонда

### 8.3 . Политики фонда РМ

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

- глобальные - применяются ко всем фондам РМ и устанавливают общие настройки доступа и использования ресурсов пользователями РМ. Для редактирования глобальных политик

следует перейти «Настройки - Глобальные политики», выбрать политику и нажать экранную кнопку **[Изменить]**;

- индивидуальные - переопределяют настройки глобальных политик и устанавливают индивидуальные настройки доступа и использования ресурсов пользователями конкретного фонда РМ. Для редактирования индивидуальных политик следует перейти «Рабочие места - Фонды», выбрать нужный фонд РМ, нажать экранную кнопку **[Политики]**, выбрать политику и нажать экранную кнопку **[Изменить]**.

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

Начиная с Termidesk версии 5.0 изменен способ работы и хранения политик фонда РМ. Во время обновления распределенной или отказоустойчивой конфигурации установки с Termidesk версии 4.X на версию 5.X изменение политик нужно проводить после обновления на новую версию всех узлов Termidesk.
Если на ВРМ есть сессия пользователя, то политика применится после перезагрузки ВМ. Для терминального сервера перезагрузка обязательна!

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

Список доступных политик представлен в таблице (см. Таблица 36).

Таблица 36 – Перечень доступных политик фонда ВРМ

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

| Название политики | Описание |
|---|---|
| «Буфер обмена в протоколах доставки "RDP" и "SPICE (vdi-viewer, эксперим.)"» | Управление использованием буфера обмена в протоколах RDP и SPICE.<br>Применимость:<br>▪ BPM (SPICE, RDP);<br>▪ автономные машины (RDP);<br>▪ терминальные сессии MS RDS;<br>▪ опубликованные приложения MS RDS;<br>▪ терминальные сессии STAL;<br>▪ опубликованные приложения STAL;<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS;<br>▪ терминальные сессии метапоставщика STAL;<br>▪ публикованные приложения метапоставщика STAL.<br>Возможные значения:<br>▪ «Выключить перенаправление буфера»;<br>▪ «Двустороннее перенаправление буфера» (по умолчанию);<br>▪ «Перенаправление буфера только от сервера клиенту»;<br>▪ «Перенаправление буфера только от клиента серверу» |
| «Выбор пользователем протокола доставки» | Определяет, может ли пользователь выбрать протокол доставки для подключения к РМ. Политика применяется только при подключении пользователя через веб-браузер.<br>Возможные значения:<br>▪ «Разрешено» (по умолчанию);<br>▪ «Запрещено» |
| «Действие при выходе пользователя из ОС» | Определяет действие после выхода пользователя из ОС.<br>Для сервисного фонда РМ поставщика ресурсов «метапоставщик» должно быть оставлено значение по умолчанию.<br>Применимость:<br>▪ BPM (RDP, SPICE, TERA);<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS.<br>Возможные значения:<br>▪ «Нет» (по умолчанию);<br>▪ «Удалять рабочее место»;<br>▪ «Не сохранять изменения» - ВМ будет возвращена к ранее созданному снимку. Значение политики применимо для фондов, основанных на шаблонах «Связанный клон oVirt/RHEV», «Связанный клон» или «Полный клон» VMware vSphere.<br>При применении последних двух значений в индивидуальных политиках фонда РМ может быть выведено уведомление «Данное значение политики не применимо к выбранному фонду», если у поставщика ресурсов фонда РМ нет возможности создавать снимки ВМ |

| Название политики | Описание |
|---|---|
| «Завершать сеанс при достижении лимита времени» | Политика определяет, будет ли сессия пользователя завершена по заданным в других политиках лимитам времени, а не отключена. Политика действует на ОС Microsoft Windows.<br>Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена.<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP);<br>▪ терминальные сессии метапоставщика MS RDS.<br>Возможные значения:<br>▪ «Не задано»;<br>▪ «Выключено» (по умолчанию);<br>▪ «Включено» |
| «Интервал мониторинга кеша перемещаемых профилей пользователей (RDP)» | Политика позволяет ограничить интервал мониторинга (в минутах) размера кеша перемещаемых профилей пользователей для протокола RDP. Политика действует на ОС Microsoft Windows.<br>Политика определяет, как часто проверяется размер всего кеша перемещаемых профилей пользователей, указанный в политике «Ограничить размер полного кеша перемещаемых профилей пользователей (RDP)».<br>При изменении политики требуется перезагрузка ВМ или терминальных серверов.<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP);<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS.<br>Возможные значения (в минутах): от 15 до 10080.<br>Значение по умолчанию: «900» |
| «Использование механизма RemoteFX (RDP)» | Политика активации механизма RemoteFX для протокола RDP. Если необходимо активировать возможность перенаправления USB-устройств из пользовательской рабочей станции в РМ, нужно установить политике значение «Включен».<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP).<br>Возможные значения:<br>▪ «Выключен» (по умолчанию);<br>▪ «Включен» |

| Название политики | Описание |
|---|---|
| «Использовать обязательные профили на сервере узла сеанса удаленных рабочих столов (RDP)» | Политика позволяет указать, используют ли службы удаленных рабочих столов обязательный профиль для всех пользователей, удаленно подключающихся к серверу узла сеанса удаленных рабочих столов. Политика действует на ОС Microsoft Windows.<br>При включении политики службы удаленных рабочих столов используют путь, указанный в политике «Указать путь для перемещаемого профиля пользователя служб удаленного рабочего стола (RDP)», в качестве корневого каталога для обязательного профиля пользователя. Все пользователи, удаленно подключающиеся к серверу узла сеансов удаленных рабочих столов, используют один и тот же профиль пользователя.<br>При отключении политики обязательные профили пользователей не будут использоваться пользователями, удаленно подключающимися к серверу узла сеанса удаленных рабочих столов.<br>При изменении политики требуется перезагрузка ВМ или терминальных серверов.<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP);<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS.<br>Возможные значения:<br>▪ «Выключено» (по умолчанию);<br>▪ «Включено» |
| «Лимит времени для активных сеансов служб удаленных рабочих столов (RDP, SPICE, и т.д.)» | Политика задает максимальное время, по истечении которого активный сеанс будет отключен.<br>Политика распространяется на компонент «Агент виртуального рабочего места».<br>Политика действует как для ОС Microsoft Windows, так и для ОС Astra Linux Special Edition:<br>▪ для протокола SPICE - для BPM с указанными ОС;<br>▪ для RDP - как для терминальных сессий и приложений метапоставщика, так и для BPM с указанными ОС.<br>ⓘ Для BPM с ОС Microsoft Windows политика применяется в момент авторизации пользователя в ОС.<br>В версиях Termidesk ниже 4.3 параметр задавался при настройке гостевых ОС («Компоненты - Параметры гостевых ОС»). При возврате к версиям Termidesk ниже 4.3 параметр будет выставлен в значение по умолчанию.<br>Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена MS AD.<br>Возможные значения:<br>▪ «Нет ограничений» (по умолчанию; сессии будут оставаться активными без ограничений по времени);<br>▪ «Не задано»;<br>▪ выбор: «1 мин», «5 мин», «10 мин», «15 мин», «30 мин», «1 час», «2 часа», «3 часа», «6 часов», «8 часов», «12 часов», «16 часов», «18 часов», «1 день», «2 дня», «3 дня», «4 дня», «5 дней» |

| Название политики | Описание |
|---|---|
| «Лимит времени для выхода из сеансов RemoteApp» | Политика позволяет указать, как долго сеанс пользователя при использовании RemoteApp (удаленное приложение) будет оставаться активным после закрытия всех программ RemoteApp.<br>Если в течение указанного времени пользователь не запускает другое приложение RemoteApp, то сеанс заврешается.<br>Политика распространяется на компонент «Агент виртуального рабочего места» и действует для подключений по протоколу RDP к терминальному серверу метапоставщика MS RDS.<br>Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена MS AD.<br>Если заданы другие политики с лимитами времени, то будет использоваться та, в которой задан более короткий период.<br>Возможные значения:<br>▪ «Никогда» (по умолчанию; при закрытии приложения сеанс будет отключен, но не завершен);<br>▪ «Сразу»;<br>▪ «Не задано»;<br>▪ выбор: «1 мин», «5 мин», «10 мин», «15 мин», «30 мин», «1 час», «2 часа», «3 часа», «6 часов», «8 часов», «12 часов», «16 часов», «18 часов», «1 день», «2 дня», «3 дня», «4 дня», «5 дней» |
| «Лимит времени для отключенной сессии» | Политика задает максимальный время, в течение которого сессия будет считаться отключенной, а не завершенной.<br>Политика распространяется на компонент «Агент виртуального рабочего места» и действует для подключений по протоколу RDP как для терминальных сессий метапоставщика MS RDS, так и для BPM.<br>Работает совместно с политикой «Завершать сеанс при достижении лимита времени».<br>Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена MS AD.<br>Возможные значения:<br>▪ «Нет ограничений» (по умолчанию; сессия останется незавершенной без ограничения по времени);<br>▪ «Не задано»;<br>▪ выбор: «1 мин», «5 мин», «10 мин», «15 мин», «30 мин», «1 час», «2 часа», «3 часа», «6 часов», «8 часов», «12 часов», «16 часов», «18 часов», «1 день», «2 дня», «3 дня», «4 дня», «5 дней» |
| «Масштабирование экрана для протокола RDP» | Политика управления масштабированием экрана для протокола RDP.<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP).<br>Возможные значения:<br>▪ «Выключено» (по умолчанию);<br>▪ «Включено» |

| Название политики | Описание |
|---|---|
| «Механизм обеспечения безопасности на уровне сети (RDP)» | Политика управления обеспечением безопасности на уровне сети для протокола RDP.<br>Для подключения к STAL необходимо использовать значение «TLS» или «RDP».<br>Для подключения к MS RDS необходимо использовать значение «NLA».<br>Если пользователь использует в качестве программы доставки ПО Termidesk Viewer, следует учесть ограничения:<br>▪ для подключения пользователя с ОС Windows к BPM ОС Astra Linux Special Edition необходимо использовать значения «Автосогласование» или «TLS»;<br>▪ для подключения пользователя с ОС Astra Linux Special Edition к BPM ОС Astra Linux Special Edition необходимо использовать значения «Автосогласование», или «RDP», или «TLS».<br>Политика может быть задана для конкретного фонда РМ на странице самого фонда РМ.<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP);<br>▪ терминальные сессии MS RDS;<br>▪ опубликованные приложения MS RDS;<br>▪ терминальные сессии STAL;<br>▪ опубликованные приложения STAL;<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS;<br>▪ терминальные сессии метапоставщика STAL;<br>▪ опубликованные приложения метапоставщика STAL.<br>Возможные значения:<br>▪ «Автосогласование» (по умолчанию);<br>▪ «RDP»;<br>▪ «TLS»;<br>▪ «NLA» |
| «Ограничить размер информации, передаваемой буфером обмена клиента (RDP, SPICE, TERA)» | Политика позволяет ограничить размер буфера обмена, доступный в обе стороны (от клиента к серверу и от сервера к клиенту). Значение указывается в килобайтах. Если размер передаваемых данных превышает заданный лимит, то будет передан только объем данных, соответствующий установленному лимиту.<br>Для совместимости с предыдущими версиями программы доставки ПО Termidesk Viewer используется значение по умолчанию.<br>Применимость:<br>▪ BPM (RDP, SPICE, TERA);<br>▪ автономные машины (RDP, TERA);<br>▪ терминальные сессии MS RDS;<br>▪ опубликованные приложения MS RDS;<br>▪ терминальные сессии STAL;<br>▪ опубликованные приложения STAL;<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS;<br>▪ терминальные сессии метапоставщика STAL;<br>▪ опубликованные приложения метапоставщика STAL.<br>Значение по умолчанию: «0» (без ограничений) |

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

| Название политики | Описание |
|---|---|
| «Передача файлов в протоколе доставки "SPICE (vdi-viewer, эксперим.)"» | Управление передачей файлов в протоколе SPICE и TERA.<br>Применимость: BPM (SPICE, TERA).<br>Возможные значения:<br>▪ «Разрешена» (по умолчанию);<br>▪ «Запрещена» |

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

| Название политики | Описание |
|---|---|
| | ▪ разрядность чисел ограничена 16 битами.<br>Пример задания правила для двух фильтров: разрешение аудиоустройств любых вендоров, продуктов и версий и запрет принтера с определенным идентификатором производителя:<br>«0x01,-1,-1,-1,1\|0x07,0xffff,-1,-1,0» |
| «Перенаправление видеокамеры в протоколе доставки "SPICE (vdi-viewer, эксперим.)", RDP» | Управление перенаправлением видеокамеры для протоколов RDP, SPICE и TERA.<br>Применимость:<br>▪ BPM (RDP, SPICE, TERA);<br>▪ автономные машины (RDP, TERA).<br>Возможные значения:<br>▪ «Разрешено» (по умолчанию);<br>▪ «Запрещено» |
| «Перенаправление смарт-карт в протоколе доставки "SPICE (vdi-viewer, эксперим.), RDP"» | Управление перенаправлением смарт-карт для протоколов RDP, SPICE, TERA.<br>Ранее в версии Termidesk 5.0 для протокола RDP существовала отдельная политика «Политика управления перенаправлением смарт-карт (RDP)», в версии Termidesk 5.1 она была заменена на общую для протоколов SPICE и RDP политику.<br>Применимость:<br>▪ BPM (RDP, SPICE, TERA);<br>▪ автономные машины (RDP, TERA);<br>▪ терминальные сессии MS RDS;<br>▪ опубликованные приложения MS RDS;<br>▪ терминальные сессии STAL;<br>▪ опубликованные приложения STAL;<br>▪ терминальные сессии метапоставщика STAL;<br>▪ опубликованные приложения метапоставщика STAL.<br>Возможные значения:<br>▪ «Разрешено» (по умолчанию);<br>▪ «Запрещено» |
| «Подключение с отличным именем пользователя» | Политика управления подключением пользователя к ВМ. Применяется в случае, если вводимый в ВМ логин отличен от логина назначенной машины в Termidesk.<br>Возможные значения:<br>▪ «Разрешено»;<br>▪ «Запрещено» (по умолчанию) |
| «Показывать обои рабочего стола» | Управление отображением обоев рабочего стола РМ для протокола RDP.<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP);<br>▪ терминальные сессии MS RDS;<br>▪ терминальные сессии метапоставщика MS RDS.<br>Возможные значения:<br>▪ «Разрешить» - обои будут отображены;<br>▪ «Запретить» (по умолчанию) - обои не будут отображаться |

| Название политики | Описание |
|---|---|
| «Политика простоя рабочего места» | Разрешенное время простоя рабочего места в секундах. Значение «-1» означает неограниченное время простоя. Политика распространяется на компонент «Агент виртуального рабочего места».<br>Применимость:<br>▪ BPM (RDP, SPICE);<br>▪ автономные машины (RDP).<br>Значение по умолчанию: «-1» |
| «Политика управления автоподключением устройств (RDP)» | Управление возможностью автоматически перенаправлять устройства для протокола RDP.<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP).<br>Возможные значения:<br>▪ «Не используется» (по умолчанию);<br>▪ «Разрешить автоподключение»;<br>▪ «Запретить автоподключение» |
| «Политика управления глубиной цвета (RDP)» | Управление максимально допустимым количеством цветов, отображаемых экраном РМ, для протокола RDP.<br>Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена.<br>Для подключения к STAL через стандартную утилиту Windows `mstsc` необходимо использовать значение «32 бит».<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP);<br>▪ терминальные сессии MS RDS;<br>▪ опубликованные приложения MS RDS;<br>▪ терминальные сессии STAL;<br>▪ опубликованные приложения STAL;<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS;<br>▪ терминальные сессии метапоставщика STAL;<br>▪ опубликованные приложения метапоставщика STAL.<br>Возможные значения:<br>▪ «15 бит»;<br>▪ «16 бит» (по умолчанию);<br>▪ «24 бит»;<br>▪ «32 бит»;<br>▪ «Не задано» |
| «Политика управления композицией рабочего стола (RDP)» | Управление отображением художественных эффектов рабочего стола.<br>Для корректного отображения художественных эффектов в параметре «Политика управления глубиной цвета (RDP)» требуется установить значение «32 бита».<br>Политика применяется только при подключении по протоколу RDP к гостевой ОС Microsoft Windows.<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP).<br>Возможные значения:<br>▪ «Разрешить композицию»;<br>▪ «Запретить композицию» (по умолчанию) |

| Название политики | Описание |
|---|---|
| «Политика управления многомониторным режимом (RDP/SPICE)» | Управление многомониторным режимом при подключении к РМ по протоколам RDP, SPICE, TERA.<br>Политика влияет на возможность пользователя использовать экран РМ на нескольких физических мониторах.<br>Применимость:<br>▪ BPM (RDP, SPICE, TERA);<br>▪ автономные машины (RDP, TERA);<br>▪ терминальные сессии STAL;<br>▪ терминальные сессии MS RDS;<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ терминальные сессии метапоставщика STAL.<br>⚠ При подключении к STAL через стандартную утилиту ОС Microsoft Windows (`mstsc.exe`) включать политику не рекомендуется.<br>При подключении к BPM с ОС Astra Linux Special Edition или к STAL через стандартную утилиту ОС Linux (`xfreerdp`) рекомендуется использовать мониторы с одинаковым разрешением экрана.<br>При подключении к STAL рекомендуется использовать конфигурацию, при которой основной монитор расположен слева от остальных.<br>Возможные значения:<br>▪ «Разрешить» - будет поддерживаться возможность вывода экрана РМ на нескольких дополнительных физических мониторах (если они подключены). При этом вариант использования экрана может быть различен в зависимости от дополнительных настроек программы доставки (см. подраздел **Выбор монитора** документа СЛЕТ.10001-02 92 01 «Руководство пользователя. Установка и эксплуатация компонента «Клиент»): дублирование, растяжение экрана и др.;<br>▪ «Запретить» (по умолчанию) - экран РМ будет выведен только на основном физическом мониторе, вариант использования которого может быть различен в зависимости от дополнительных настроек параметров в ОС |
| «Политика управления параметрами перенаправления принтеров» | Управление перенаправлением принтеров. Можно запретить перенаправление, разрешить перенаправлять все принтеры или только выбранные пользователем.<br>Применимость:<br>▪ BPM (RDP, SPICE, TERA);<br>▪ автономные машины (RDP, TERA);<br>▪ терминальные сессии MS RDS;<br>▪ опубликованные приложения MS RDS;<br>▪ терминальные сессии STAL;<br>▪ опубликованные приложения STAL;<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS;<br>▪ терминальные сессии метапоставщика STAL;<br>▪ опубликованные приложения метапоставщика STAL.<br>Возможные значения:<br>▪ «Не перенаправлять» (по умолчанию);<br>▪ «Перенаправлять все»;<br>▪ «Перенаправлять выбранные пользователем» |

| Название политики | Описание |
|---|---|
| «Политика управления перенаправлением дисков и папок» | Управление перенаправлением дисков и каталогов.<br>Применимость:<br>▪ BPM (RDP, SPICE, TERA);<br>▪ автономные машины (RDP, TERA);<br>▪ терминальные сессии MS RDS;<br>▪ опубликованные приложения MS RDS;<br>▪ терминальные сессии STAL;<br>▪ опубликованные приложения STAL;<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS;<br>▪ терминальные сессии метапоставщика STAL;<br>▪ опубликованные приложения метапоставщика STAL.<br>Возможные значения:<br>▪ «Разрешить перенаправление»;<br>▪ «Запретить перенаправление» (по умолчанию)<br>⚠ В Termidesk версии 5.1 перенаправление дисков и каталогов выполняется всегда. |
| «Политика управления перенаправлением звука (аудио и микрофон) (RDP)» | Управление перенаправлением звука в протоколе RDP.<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP);<br>▪ терминальные сессии MS RDS;<br>▪ опубликованные приложения MS RDS;<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS;<br>▪ терминальные сессии метапоставщика STAL;<br>▪ опубликованные приложения метапоставщика STAL.<br>Возможные значения:<br>▪ «Не используется» (по умолчанию);<br>▪ «Разрешить перенаправление»;<br>▪ «Запретить перенаправление» |
| «Политика управления перенаправлением последовательных портов (RDP)» | Управление перенаправлением последовательных портов для протокола RDP.<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP).<br>Возможные значения:<br>▪ «Разрешить перенаправление»;<br>▪ «Запретить перенаправление» (по умолчанию) |

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

| Название политики | Описание |
|---|---|
| «Политика управления типом сети (RDP)» | Управление типом сетевого подключения, используемого при подключении к РМ по протоколу RDP.<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP);<br>▪ терминальные сессии MS RDS;<br>▪ опубликованные приложения MS RDS;<br>▪ терминальные сессии STAL;<br>▪ опубликованные приложения STAL;<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS;<br>▪ терминальные сессии метапоставщика STAL;<br>▪ опубликованные приложения метапоставщика STAL.<br>Возможные значения:<br>▪ «Модем»;<br>▪ «Низкоскоростное широкополосное подключение»;<br>▪ «Широкополосное подключение»;<br>▪ «Высокоскоростное широкополосное подключение»;<br>▪ «Глобальная сеть»;<br>▪ «Локальная сеть»;<br>▪ «Авто» (по умолчанию) |
| «Политика управления уровнем сжатия (RDP)» | Управление уровнем сжатия данных, при взаимодействии с РМ по протоколу RDP.<br>Если политика имеет значение «Не задано», то она не будет применяться, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена.<br>Применимость:<br>▪ BPM (RDP);<br>▪ автономные машины (RDP);<br>▪ терминальные сессии MS RDS;<br>▪ опубликованные приложения MS RDS;<br>▪ терминальные сессии STAL;<br>▪ опубликованные приложения STAL;<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS;<br>▪ терминальные сессии метапоставщика STAL;<br>▪ опубликованные приложения метапоставщика STAL.<br>Возможные значения:<br>▪ «0»;<br>▪ «1» (по умолчанию);<br>▪ «2»;<br>▪ «Не задано» |
| «Полноэкранный режим (SPICE, TERA)» | Управление работой в полноэкранном режиме для протоколов SPICE и TERA.<br>Применимость: BPM (SPICE, TERA).<br>Возможные значения:<br>▪ «Включен» (по умолчанию);<br>▪ «Выключен» |
| «Разрешение видеокамеры в протоколе доставки "SPICE (vdi-viewer, эксперим.)", RDP» | Допустимые разрешения видеокамеры в протоколах RDP, SPICE, TERA.<br>Применимость:<br>▪ BPM (RDP, SPICE, TERA);<br>▪ автономные машины (RDP, TERA).<br>Значение по умолчанию: «320-2560x240-1440» |

| Название политики | Описание |
|---|---|
| «Разрешенные форматы передаваемые буфером обмена клиента (RDP, SPICE, TERA)» | Политика определяет разрешенный формат записей в буфере обмена. В зависимости от направления передачи перед отправкой или после получения данных из буфера обмена запрашивается их тип и сопоставляется с разрешенными значениями. В зависимости от типа передача данных разрешается или запрещается.<br>Для совместимости с предыдущими версиями ПО Termidesk Viewer используется значение по умолчанию.<br>Применимость:<br>▪ BPM (RDP, SPICE, TERA);<br>▪ автономные машины (RDP, TERA);<br>▪ терминальные сессии MS RDS;<br>▪ опубликованные приложения MS RDS;<br>▪ терминальные сессии STAL;<br>▪ опубликованные приложения STAL;<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS;<br>▪ терминальные сессии метапоставщика STAL;<br>▪ опубликованные приложения метапоставщика STAL.<br>Возможные значения:<br>▪ «Любой» (по умолчанию);<br>▪ «Текст без форматирования» |
| «Удаление рабочего места после» | Политика определяет событие, после которого будет произведено удаление РМ. Работает совместно с политикой «Действие при выходе пользователя из ОС».<br>Применимость:<br>▪ BPM (RDP, SPICE, TERA);<br>▪ терминальные сессии метапоставщика MS RDS;<br>▪ опубликованные приложения метапоставщика MS RDS.<br>Возможные значения:<br>▪ «После события выхода пользователя из ОС» (по умолчанию);<br>▪ «После события завершения синхронизации профиля» |

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

## 8.4 . Объединение фондов в группы РМ

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

Для добавления группы администратору Termidesk следует перейти «Настройки - Группы рабочих мест» и нажать экранную кнопку **[Создать]**, затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 37).

Таблица 37 – Данные для объединения фондов BPM в группы

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

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

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

### 8.5 . Назначение пользователей фонду PM

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

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

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

### 8.6 . Назначение групп доступа фонду PM

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

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

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

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

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

### 8.7 . Назначение протоколов фонду РМ

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

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

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

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

### 8.8 . Управление РМ

#### 8.8.1 . Управление терминальными сессиями в назначенном фонде РМ

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

Для просмотра основных сведений о сессиях пользователей в назначенном фонде РМ следует перейти «Рабочие места - Фонды», затем выбрать нужный фонд, перейти во вкладку «Рабочие места» (см. Рисунок 24).

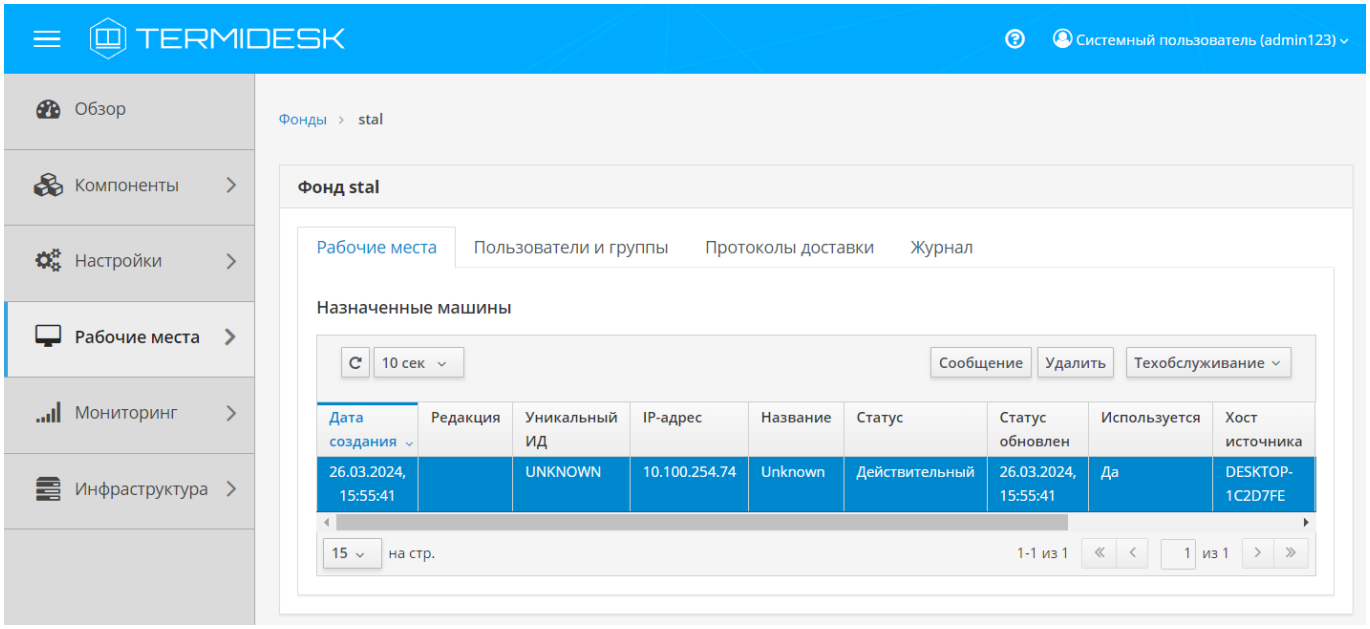


Рисунок 24 – Просмотр сведений о сессиях пользователей в назначенном фонде РМ

Для изменения состояния подключений предусмотрены элементы управления (см. Таблица 38).

Таблица 38 – Элементы управления состоянием терминального сервера

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

После нажатия экранной кнопки **[Удалить]** принудительный штатный выход пользователя из ОС РМ произойдет в течение 30 секунд.
Сессия пользователя также будет автоматически и принудительно завершена, если пользователь был удален или домен аутентификации, в который входит этот пользователь, был отключен или удален.
Экранная кнопка **[Сообщение]** не вызывает отправку сообщения в терминальную сессию.

Для терминальных сессий может возникнуть ситуация, при которой статус сессии отображен как «Действительный», но идентификатор ей не назначен. Такие сессии считаются неактивными и удаляются периодической задачей, которая срабатывает с интервалом 240 секунд.

Основные параметры сессий перечислены в столбце «Параметр» следующей таблицы (см. Таблица 39).

Таблица 39 – Основные параметры сессий в назначенном фонде ВРМ

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

| Параметр | Описание |
|---|---|
| «IP источника» | IP-адрес инициатора сессии |
| «Владелец» | Субъект, инициировавший выдачу сессии |
| «Версия агента» | Версия компонента «Агент», установленного на терминальном сервере |

### 8.8.2 . Назначение владельца РМ

В Termidesk предусмотрена возможность назначения владельца РМ для гарантированного закрепления за пользователем конкретной ВМ. В этом случае пользователь всегда будет получать одну и ту же ВМ при подключении к фонду РМ.

Назначение владельца возможно при соблюдении следующих условий:

- РМ находится в статусе «Подготовка» или «Действительный»;
- РМ находится в кеше 1-го уровня;
- для данного РМ отсутствует назначенный пользователь в столбце «Владелец» списка РМ.

Для назначения владельца следует перейти «Рабочие места - Фонды», затем выбрать нужный фонд, перейти во вкладку «Рабочие места». Выбрать нужное РМ, которое находится в таблице «Кеш», и нажать экранную кнопку [Владелец] (см. Рисунок 25). В открывшемся окне «Владелец» выбрать домен аутентификации и пользователя, которому будет назначено РМ. Выбранный пользователь автоматически добавится в фонд РМ и будет отображен во вкладке «Пользователи и группы».

⚠ Назначение владельца будет доступно только в том случае, если пользователь хотя бы один раз осуществил вход в «Портал пользователя» или подключился к «Универсальному диспетчеру» через компонент «Клиент» под своей учетной записью.

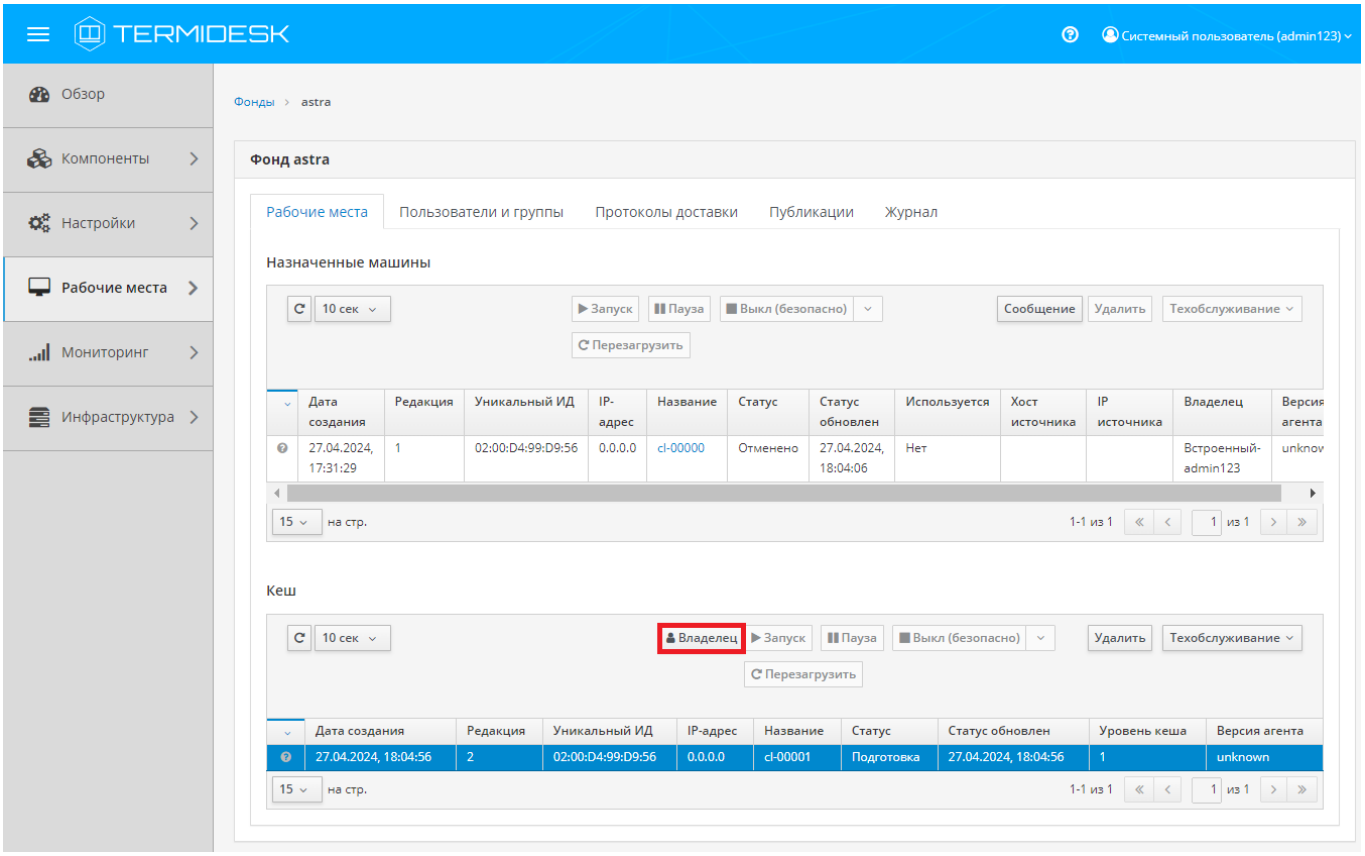


Рисунок 25 – Назначение владельца РМ на странице фонда РМ

Назначить владельца РМ можно также перейдя «Рабочие места - Индивидуальные рабочие места» (см. Рисунок 26).

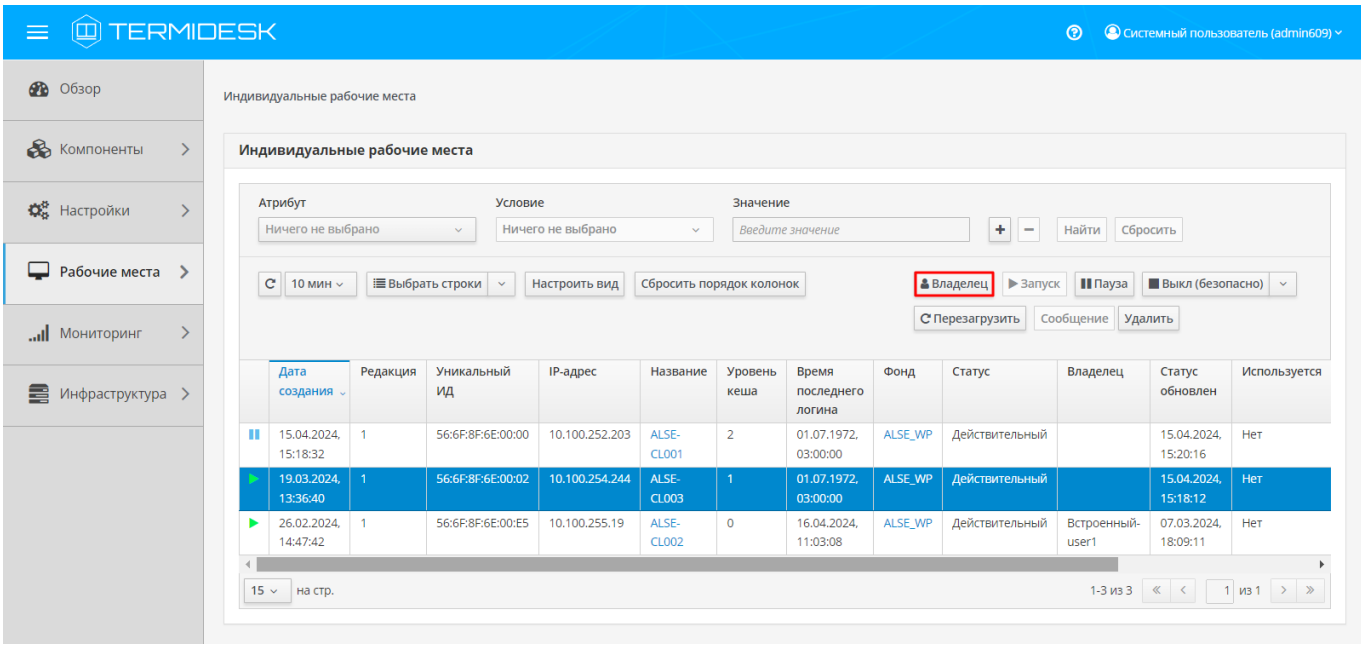


Рисунок 26 – Назначение владельца в списке индивидуальных РМ

## 8.9 . Управление сессиями подключенных к фонду РМ пользователей

### 8.9.1 . Управление активными сессиями пользователей

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

Доступны следующие возможности по управлению сессией:

- отключение сессии пользователя. Следует перейти «Рабочие места - Сессии», пометить сессию пользователя и нажать экранную кнопку **[Отключить]**. После нажатия экранной кнопки **[Отключить]** принудительный штатный выход пользователя из ОС ВРМ произойдет в течение 30 секунд. Также сессия пользователя будет автоматически и принудительно завершена, если он был удален или домен аутентификации, в который входит этот пользователь, был отключен или удален;
- сброс сессии пользователя. Следует перейти «Рабочие места - Сессии», пометить сессию пользователя и нажать экранную кнопку **[Сбросить]**;
- подключение к сессии пользователя. Следует перейти «Рабочие места - Сессии», пометить сессию пользователя и нажать экранную кнопку **[Помощник]**. Для работы подключения необходимо, чтобы:
  - в гостевой ОС был установлен компонент «Удаленный помощник» (клиентская часть);
  - в сетевой инфраструктуре организации существовал узел с установленным компонентом «Удаленный помощник» (серверная часть) и он был доступен для взаимодействия с «Универсальным диспетчером».

Функционал управления сессиями пользователя из страницы «Рабочие места - Сессии» недоступен для терминальных сессий. Возможности по управлению такими сессиями приведены в подразделе **Управление терминальными сессиями в назначенном фонде РМ**.

Не рекомендуется устанавливать компонент «Удаленный помощник» (серверная часть) на узел с установленным компонентом «Универсальный диспетчер», поскольку оба компонента вносят изменения в конфигурацию веб-сервера apache.

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

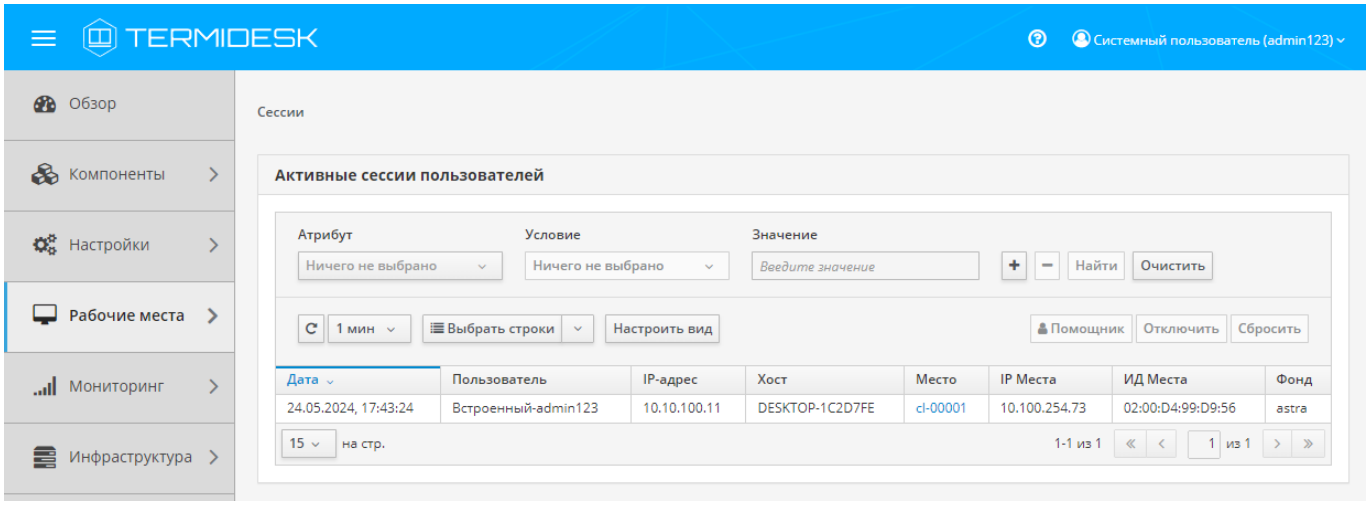


Рисунок 27 – Просмотр сведений об активных сессиях пользователей в фондах BPM

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

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

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

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

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

Для обновления значений таблицы используется графический элемент  . Для задания периода обновления или его отключения следует использовать выпадающий список (см. Рисунок 28) со значениями интервала в минутах, расположенный рядом с указанным элементом.

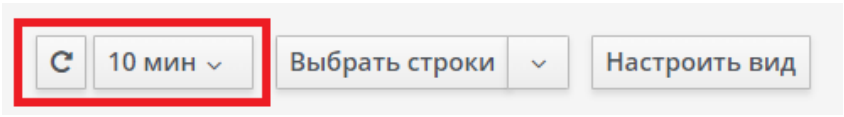


Рисунок 28 – Обновление значений таблицы

Внешний вид таблицы списка активных сессий можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться экранной кнопкой **[Настроить вид]** и отметить наименования столбцов (см. Рисунок 29), которые будут

отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для применения изменений нужно нажать экранную кнопку **[Сохранить]**. При попытке убрать выбор со всех пунктов экранная кнопка **[Сохранить]** будет заблокирована. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить вид]**;

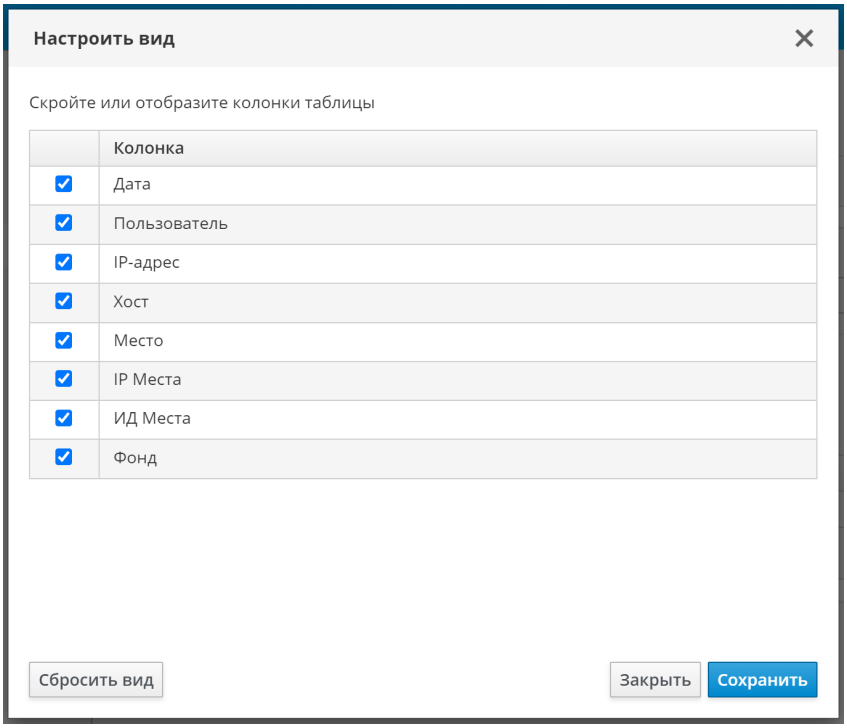


Рисунок 29 – Выбор столбцов для отображения

- порядок следования столбцов. Для изменения порядка следования нужно захватить левой кнопкой мыши заголовок столбца, и, не отпуская кнопку мыши, перенести его в нужное расположение (см. Рисунок 30). Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок колонок]**, которая становится доступна только после изменения порядка следования столбцов и будет скрыта после сброса;


Рисунок 30 – Изменение порядка следования столбцов

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца (см. Рисунок 31).

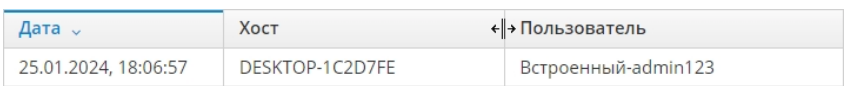


Рисунок 31 – Изменение ширины столбцов

Основные параметры сессий перечислены в столбце «Параметр» следующей таблицы (см. Таблица 40).

Таблица 40 – Основные параметры сессий пользователей

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

ⓘ Записи в списке поддерживают функцию множественного выбора и выполнения операций над несколькими объектами одновременно. Выполнить операцию над несколькими объектами можно только тогда, когда она допустима для всех выбранных объектов. Для выбора нескольких записей нужно зажать и удерживать клавиши **<CTRL>** или **< SHIFT>**.

### 8.9.2 . Фильтрация списка активных сессий

На странице со списком активных сессий доступен механизм фильтрации (см. Рисунок 27). Фильтрация осуществляется путем задания значений для параметров «Атрибут», «Условие» и «Значение».

Для добавления дополнительного фильтра следует нажать экранную кнопку **[+]**. Для удаления фильтра нужно использовать экранную кнопку **[-]** в соответствующей строке. Максимально допустимое число фильтров - 15.

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

Экранная кнопка **[Очистить]** сбрасывает все фильтры, возвращая значения к исходному состоянию: удаляются дополнительные строки фильтра (остается только одна строка), все значения сбрасываются, поля «Условие» и «Значение» блокируются.

Подробное описание механизма фильтрации списка сессий приведено в таблице (см. Таблица 41).

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

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

Таблица 41 – Параметры фильтрации списка РМ

| Атрибут | Условия | Значение |
|---|---|---|
| «Дата» | Формирование списка сессий:<br>▪ «В пределах» - в указанном временном промежутке;<br>▪ «Не в пределах» - исключая указанный временной промежуток | ▪ «Минута»;<br>▪ «5 минут»;<br>▪ «30 минут»;<br>▪ «1 час»;<br>▪ «12 часов»;<br>▪ «24 часа»;<br>▪ «Сегодня»;<br>▪ «Эта неделя»;<br>▪ «Этот месяц» |
| «Пользователь» | Формирование списка сессий:<br>▪ «Является» - по указанному имени пользователя;<br>▪ «Не является» - исключая указанное имя пользователя;<br>▪ «Начинается с» - по начальной части имени пользователя;<br>▪ «Оканчивается на» - по конечной части имени пользователя;<br>▪ «Содержит» - включая указанную часть имени пользователя | Ручной ввод |
| «IP-адрес» | Формирование списка сессий:<br>▪ «Является» - по указанному IP-адресу инициатора сессии;<br>▪ «Не является» - исключая указанный IP-адрес инициатора сессии;<br>▪ «Начинается с» - по начальной части IP-адреса инициатора сессии;<br>▪ «Оканчивается на» - по конечной части IP-адреса инициатора сессии;<br>▪ «Содержит» - включая указанную часть IP-адреса инициатора сессии | Ручной ввод |
| «Хост» | Формирование списка сессий:<br>▪ «Является» - по указанному наименованию инициатора сессии;<br>▪ «Не является» - исключая указанное наименование инициатора сессии;<br>▪ «Начинается с» - по начальной части наименования инициатора сессии;<br>▪ «Оканчивается на» - по конечной части наименования инициатора сессии;<br>▪ «Содержит» - включая указанную часть наименования инициатора сессии | Ручной ввод |
| «Место» | Формирование списка сессий:<br>▪ «Является» - по указанному наименованию РМ, выданного пользователю;<br>▪ «Не является» - исключая указанное наименование РМ, выданного пользователю;<br>▪ «Начинается с» - по начальной части наименования РМ, выданного пользователю;<br>▪ «Оканчивается на» - по конечной части наименования РМ, выданного пользователю;<br>▪ «Содержит» - включая указанную часть наименования РМ, выданного пользователю | Ручной ввод |

| Атрибут | Условия | Значение |
|---|---|---|
| «IP Места» | Формирование списка сессий:<br>▪ «Является» - по указанному IP-адресу РМ, выданного пользователю;<br>▪ «Не является» - исключая указанный IP-адрес РМ, выданного пользователю;<br>▪ «Начинается с» - по начальной части IP-адреса РМ, выданного пользователю;<br>▪ «Оканчивается на» - по конечной части IP-адреса РМ, выданного пользователю;<br>▪ «Содержит» - включая указанную часть IP-адреса РМ, выданного пользователю | Ручной ввод |
| «ИД Места» | Формирование списка сессий:<br>▪ «Является» - по указанному идентификатору РМ, выданного пользователю;<br>▪ «Не является» - исключая указанный идентификатор РМ, выданного пользователю;<br>▪ «Начинается с» - по начальной части идентификатора РМ, выданного пользователю;<br>▪ «Оканчивается на» - по конечной части идентификатора РМ, выданного пользователю;<br>▪ «Содержит» - включая указанную часть идентификатора РМ, выданного пользователю | Ручной ввод |
| «Фонд» | Формирование списка сессий:<br>▪ «Является» - по указанному наименованию фонда, в котором находится РМ;<br>▪ «Не является» - исключая указанное наименование фонда, в котором находится РМ;<br>▪ «Начинается с» - по начальной части наименования фонда, в котором находится РМ;<br>▪ «Оканчивается на» - по конечной части наименования фонда, в котором находится РМ;<br>▪ «Содержит» - включая указанную часть наименования фонда, в котором находится РМ | Ручной ввод |

## 8.10 . Настройка автоматического подключения к фонду РМ

### 8.10.1 . Автоматическое подключение к фонду РМ

Автоматическое подключение к фонду РМ позволяет компоненту «Клиент» выполнить поиск в сети компонента «Универсальный диспетчер» и реализовать автоматическое подключение к опубликованным фондам.

Для автоматического подключения к фонду РМ после настройки автоматического поиска сервера подключений на узле с установленным Termidesk следует перейти «Настройки - Системные параметры - Общие», активировать параметр «Автозапуск рабочего места» и нажать экранную кнопку **[Сохранить]**.

⚠ Для автоматического подключения к фонду РМ нужно настроить группы доступа к фондам так, чтобы пользователям из каждой группы был доступен только один фонд. Если пользователь является членом нескольких групп, и каждой из этих групп предоставлен

доступ к отдельному фонду РМ, то пользователь получает доступ к нескольким фондам одновременно. В таком случае, автоматическое подключение невыполнимо. При этом возможность ручного подключения сохраняется.

⚠ Для корректной работы автоматического подключения к фонду РМ необходимо выполнить настройку службы DNS.

### 8.10.2 . Настройка автоматического поиска в сети сервера Termidesk

Автоматический поиск сервера подключений позволяет компоненту «Клиент» выполнить поиск в сети компонента «Универсальный диспетчер».

Для этого на DNS-сервере должна быть внесена одна из записей:

- либо запись `daas` типа `TXT` с URL-адресом сервера Termidesk, например: `https://termidesk.domain.local`;
- либо запись `vdi` типа `TXT` с URL-адресом сервера Termidesk, например: `https://termidesk.domain.local`.

## 8.11 . Режим техобслуживания фонда РМ

### 8.11.1 . Режим техобслуживания фонда терминального сервера

Режим техобслуживания фонда - это запрет пользователям подключаться (создавать новую сессию) и/или переподключаться повторно в существующую сессию фонда терминального сервера. Этот режим предназначен для проведения плановых регламентных или аварийных работ, например, когда нужно применить обновления или исправления для терминального сервера и требуется временно прекратить новые подключения к фонду.

ⓘ Режим техобслуживания может применяться и к отдельному терминальному серверу в выбранном фонде (см. подраздел **Управление терминальными сессиями в назначенном фонде РМ**).

Для перевода фонда в режим техобслуживания следует перейти «Компоненты - Фонды» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить» (см. Рисунок 32). Затем подтвердить включение режима.

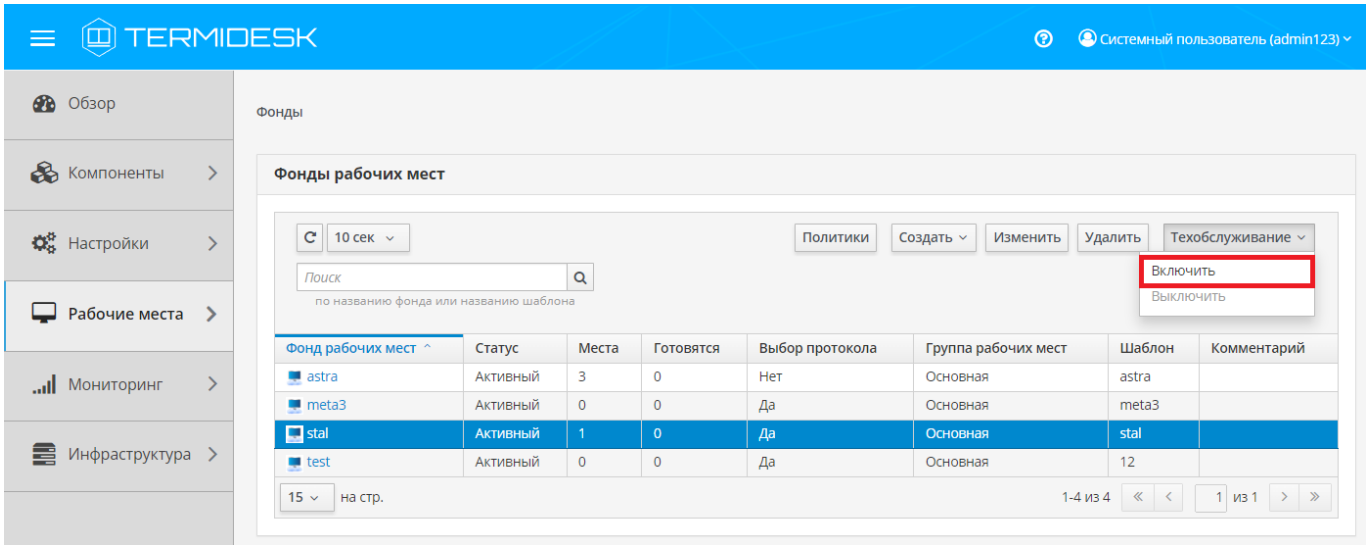


Рисунок 32 – Перевод фонда терминального сервера в режим техобслуживания

Состояние режима техобслуживания будет отображено в столбце «Статус» списка фондов.

Для отключения режима техобслуживания нужно выбрать фонд терминального сервера, нажать экранную кнопку **[Техобслуживание]**, а затем выбрать из выпадающего списка значение «Выключить». По завершении техобслуживания фонд может быть снова использован.

## 8.12 . Управление расписанием задач

Расписание позволяет составить график задач, которые должны быть выполнены для фондов РМ.

Для отображения списка задач следует перейти «Рабочие места - Расписания». Основные параметры списка приведены в таблице (см. Таблица 42). Сортировка списка выполняется по столбцу «Название».

Таблица 42 – Параметры списка расписаний

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование задачи |
| «Действие» | Действие, выполняемое в рамках расписания |
| «Фонды» | Список фондов, к которым будет применена задача |
| «Включено» | Отображение состояния задачи |
| «Комментарий» | Информационное сообщение, используемое для описания назначения задачи |
| «Дата активации» | Дата активации задачи |
| «Время начала» | Время начала очередного действия задачи |
| «Повтор» | Периодичность выполнения задачи |
| «Длительность» | Длительность (в минутах) выполнения задачи с момента, заданного в параметре «Время начала» |

Над созданными задачами можно выполнить следующие действия:

- отредактировать, для этого нажать экранную кнопку **[Изменить]**;

- удалить, для этого нажать экранную кнопку **[Удалить]**. При попытке удаления активной задачи будет отображено сообщение: «Вы уверены, что хотите удалить расписание, которое используется?». Удаление активной задачи производится без учета ее текущего выполнения;
- изменить состояние задачи, для этого нажать экранную кнопку **[Активация]** и выбрать соответствующий пункт:
  - **[Включить]** - активировать задачу;
  - **[Выключить]** - деактивировать задачу.

Для поиска задачи предусмотрено поле «Поиск». Предусмотрен поиск по параметрам «Название», «Фонды», «Комментарий».

Для добавления задачи в раскрывающемся списке экранной кнопки **[Создать]** следует выбрать тип действия, которое будет выполняться по расписанию:

- «Запуск» - включение ВМ, реализуется через гипервизор;
- «Перезагрузка» - перезагрузка ВМ, реализуется через гипервизор;
- «Перезагрузка (безопасная)» - перезагрузка ВМ, реализуется через гипервизор. В ВМ должен быть установлен пакет инструментов «Guest tools», который предоставляется производителем гипервизора;
- «Пауза» - приостанов ВМ, реализуется через гипервизор;
- «Останов (небезопасный)» - выключение ВМ, реализуется через гипервизор;
- «Выключение (безопасное)» - выключение ВМ, реализуется через гипервизор. В ВМ должен быть установлен пакет инструментов «Guest tools», который предоставляется производителем гипервизора;
- «Восстановление» (откат к снапшоту) - восстановление ВМ из базового снимка (снапшота), реализуется через гипервизор;
- «Техобслуживание» - отправка ВМ на техобслуживание.

Действия, реализуемые через гипервизор, могут быть успешно выполнены только на гипервизорах, поддерживающих указанные команды.
Действие «Восстановление» будет доступно оператору, если у него есть пользовательское разрешение «Восстановление рабочих мест».

Для корректной работы расписаний для узлов Termidesk должна быть настроена синхронизация времени (см. подраздел **Требования к синхронизации времени** документа СЛЕТ.10001-02 90 01 «Руководство администратора. Установка программного комплекса»).

Доступные для заполнения параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 43). Для сохранения конфигурации нужно использовать экранную кнопку **[Сохранить]**.

Таблица 43 – Параметры расписаний

| Параметр | Описание |
|---|---|
| «Включено» | Управление состоянием задачи.<br>Возможные значения:<br>▪ «Да» (по умолчанию) - задача активирована;<br>▪ «Нет» - задача деактивирована.<br>Если задача уже успела активироваться, то при ее выключении (значение «Нет» переключателя параметра) действие будет применено в этот раз, но не в следующий |
| «Название» | Текстовое наименование создаваемой задачи |
| «Комментарий» | Информационное сообщение, используемое для описания назначения задачи |
| «Фонды» | Выбор одного или нескольких фондов, к которым будет применена задача |
| «Дата активации расписания» | Дата активации задачи по расписанию |
| «Время начала» | Время начала очередного действия задачи по расписанию |
| «Длительность» | Длительность (в минутах) выполнения задачи с момента, заданного в параметре «Время начала».<br>Возможные значения:<br>▪ «1 мин.»;<br>▪ «5 мин.»;<br>▪ «15 мин.» (по умолчанию);<br>▪ «30 мин.»;<br>▪ «60 мин.»;<br>▪ «180 мин. (3 ч.)»;<br>▪ «360 мин. (6 ч.)» |
| «Повтор» | Выбор периодичности запуска задачи.<br>Возможные значения:<br>▪ «Дни недели»;<br>▪ «Дни месяца» |
| «Дни недели» | Выбор одного или нескольких дней недели, в которые будет запускаться задача. Доступен при выборе значения «Дни недели» в параметре «Повтор».<br>Возможные значения:<br>▪ «Понедельник»;<br>▪ «Вторник»;<br>▪ «Среда»;<br>▪ «Четверг»;<br>▪ «Пятница»;<br>▪ «Суббота»;<br>▪ «Воскресенье» |
| «Дни месяца» | Указание даты или дат (через запятую), в которые будет запускаться задача ежемесячно. Параметр доступен при выборе значения «Дни месяца» в параметре «Повтор».<br>Допускается использование специального значения «*» - все дни месяца.<br>Пример: «10,20,30» |

| Параметр | Описание |
|---|---|
| «Включение всех назначенных рабочих мест» | Управление состоянием назначенных РМ. Доступен при выборе действия «Запуск» в раскрывающемся списке экранной кнопки **[Создать]**.<br>Возможные значения:<br>▪ «Да» (по умолчанию) - ВМ назначенных РМ будут включены;<br>▪ «Нет» - ВМ назначенных РМ не будут включены |
| «Включение неназначенных рабочих мест» | Выбор того, как будут учитываться ВМ, которые были запущены до активации задачи и не были назначены пользователю. Доступен при выборе действия «Запуск» в раскрывающемся списке экранной кнопки **[Создать]**.<br>Возможные значения:<br>▪ «Процент от общего числа» (по умолчанию);<br>▪ «Абсолютное число» |
| «Выключение рабочих мест» | Выбор того, как будут учитываться ВМ, которые были запущены до активации задачи. Доступен при выборе действия «Останов (небезопасный)» в раскрывающемся списке экранной кнопки **[Создать]**.<br>Возможные значения:<br>▪ «Процент от общего числа»;<br>▪ «Абсолютное число» (по умолчанию) |
| «Процент от общего числа» | Процент запускаемых или выключаемых ВМ, рассчитывается от общего числа ВМ в фонде. Доступен при выборе действия «Запуск» или «Останов (небезопасный)» в раскрывающемся списке экранной кнопки **[Создать]**.<br>Параметр позволяет регулировать долю запускаемых или выключаемых ВМ в течение времени, заданного в параметре «Длительность».<br>Например, если общее число ВМ составляет 100, и для параметра «Процент от общего числа» установлено значение «30», а для параметра «Длительность» установлено значение «15 мин.», то в течение 15 минут 30 ВМ будут запускаться или выключаться по 2 машины каждую минуту.<br>ⓘ Соотношение параметров «Длительность», «Процент от общего числа» и «Абсолютное число» позволяет оптимизировать нагрузку на платформу виртуализации.<br>По умолчанию для действия «Запуск»: «20».<br>По умолчанию для действия «Останов (небезопасный)»: «1» |
| «Абсолютное число» | Число запускаемых или выключаемых ВМ. Доступен при выборе действия «Запуск» или «Останов (небезопасный)» в раскрывающемся списке экранной кнопки **[Создать]**.<br>Параметр позволяет регулировать количество запускаемых или выключаемых ВМ в течение времени, заданного в параметре «Длительность».<br>Например, если для параметра «Абсолютное число» установлено значение «30», а для параметра «Длительность» установлено значение «15 мин.», то в течение 15 минут будут запускаться или выключаться по 2 машины каждую минуту.<br>По умолчанию для действия «Запуск»: «20».<br>По умолчанию для действия «Останов (небезопасный)»: «1» |

# 9 . ПРОТОКОЛЫ ДОСТАВКИ

## 9.1 . Общие сведения о протоколах доставки

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

Для отображения списка добавленных протоколов доставки следует перейти «Компоненты - Протоколы доставки». Основные параметры списка приведены в таблице (см. Таблица 44). Для добавления протокола доставки следует нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка поддерживаемый протокол и способ доставки.

Добавленные протоколы можно:

- редактировать, для этого нужно пометить протокол и нажать на экранную кнопку **[Изменить]** (см. Рисунок 33);
- удалить, для этого нужно пометить протокол и нажать на экранную кнопку **[Удалить]**.

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

Таблица 44 – Параметры списка протоколов доставки

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

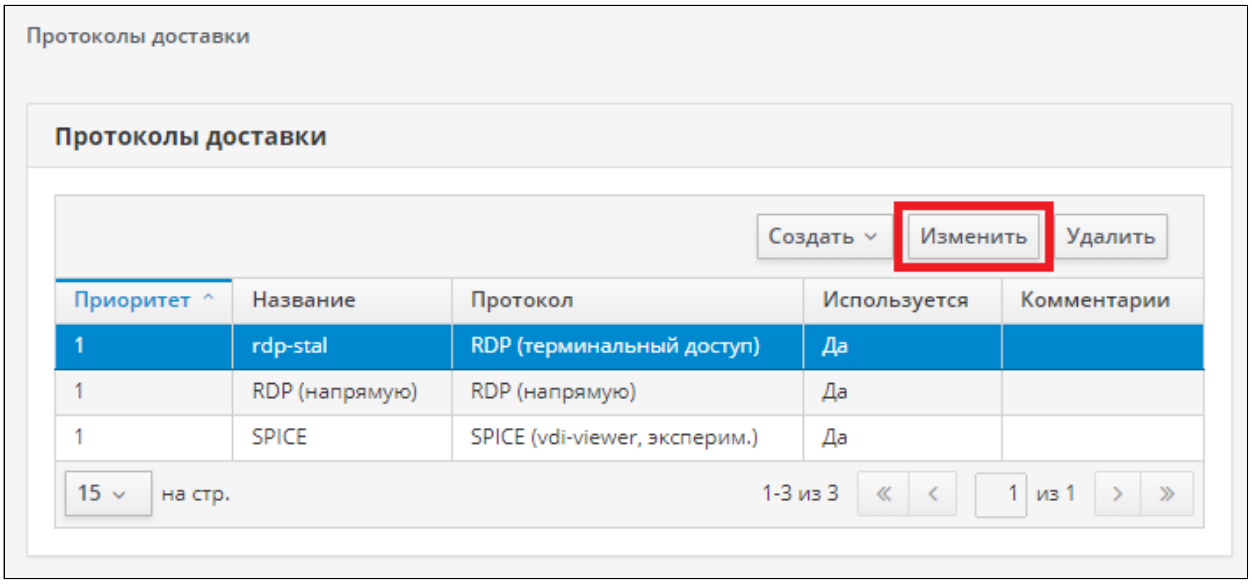


Рисунок 33 – Редактирование протокола доставки

Termidesk поддерживает следующие протоколы удаленного доступа:

- SPICE, поддерживается, в том числе, при доставке BPM через HTML5-клиент;
- TERA (экспериментально), поддерживается, в том числе, при доставке BPM через HTML5-клиент;
- VNC (только через HTML5-клиент);
- RDP;
- Loudplay.

Сравнительная таблица функциональных возможностей протоколов доставки приведена в справочном центре Termidesk: https://wiki.astralinux.ru/pages/viewpage.action?pageId=338007913.

## 9.2 . Подключения по протоколу RDP для доступа к ресурсам терминальных серверов

### 9.2.1 . Подключение по протоколу RDP для доступа к ресурсам терминального сервера

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

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 45).

Таблица 45 – Данные для добавления прямого подключения к серверам терминалов

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

| Параметр | Описание |
|---|---|
| «URL шлюза» | Адрес «Шлюза», обеспечивающего формирование и поддержание соединения, в формате `ws(s)://<IP-адрес>:<порт>`.<br>Протокол WS (WebSocket) используется, если «Шлюз» не настроен на защищенное соединение, протокол WSS используется, если выполняется защищенное подключение к «Шлюзу».<br>По умолчанию «Шлюз» использует порты:<br>▪ 5099 - для незащищенного подключения;<br>▪ 10000 - для защищенного подключения.<br>Администратор может задать нужное значение порта, если используется нестандартный порт в настройках «Шлюза» |
| «Время ожидания соединения» | Время ожидания (в секундах) отклика «Шлюза».<br>При прямом соединении (не через «Шлюз») можно оставить значение по умолчанию, т.к. параметр не будет оказывать влияния на подключение |
| «Порт» | Выбор порта для подключения. По умолчанию используется порт 3389 |
| «Разрешить смарт-карты» | Разрешить идентификацию субъектов на основе смарт-карт |
| «Разрешить принтеры» | Разрешить перенаправление устройств печати по протоколу RDP |
| «Разрешить диски» | Разрешить перенаправление устройств хранения по протоколу RDP |
| «Разрешить последовательные порты» | Разрешить перенаправление последовательных портов по протоколу RDP |
| «Показывать обои» | Отображать фоновое изображение, настроенное на рабочем столе |
| «Разрешить композицию рабочего стола» | Разрешить темы рабочего стола |
| «Сглаживание шрифтов» | Использовать технологию сглаживания шрифтов |
| «Поддержка CredSSP» | Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider |
| «Использовать ALSA» | Использовать программный микшер для передачи звука |
| «Параметры смарт-карты» | Указать конфигурацию идентификации по смарт-картам |
| «Все принтеры» | Выполнить перенаправление всех устройств печати по протоколу RDP. При выключенном параметре «Разрешить принтеры» данный параметр игнорируется |
| «RemoteFX» | Использовать технологию RemoteFX |
| «Все RemoteFX устройства» | Использовать все RemoteFX устройства |
| «Динамическое разрешение» | Разрешить передачу динамического разрешения для экрана рабочего стола<br>⚠ Параметр должен быть отключен при реализации доступа к STAL с рабочей станции пользователя на ОС Microsoft Windows 11 |

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

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

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

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

# 10 . СИСТЕМНЫЕ НАСТРОЙКИ

## 10.1 . Параметры конфигурирования компонентов «Универсальный диспетчер», «Менеджер рабочих мест»

Для настройки «Универсального диспетчера», «Менеджера рабочих мест» используется конфигурационный файл `/etc/opt/termidesk-vdi/termidesk.conf`.

> При установке пакета `termidesk-vdi` возможно активировать режим отладки инсталлятора переменную окружения `TDSK_PKG_DEBUG=1`.

Перечень параметров, задающихся через файл, приведен в таблице (см. Таблица 46). Указанные параметры можно поменять также через утилиту `termidesk-config` (см. подраздел **Утилита termidesk-config**).

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

Таблица 46 – Параметры конфигурирования «Универсального диспетчера»

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| `TDSK_AUTOFS_IMAGES_ID` | Не задано | Параметр может быть задан на узлах «Универсального диспетчера».<br>Используется для настройки шаблонов переносимых профилей. В качестве значения используются идентификаторы дисков.<br>Пример: `TDSK_AUTOFS_IMAGES_ID=xx[,yy[,zz[,...]]]` |
| `DBHOST` | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет IP-адрес или FQDN СУБД PostgreSQL.<br>Начальное значение задается на этапе подготовке среды функционирования и установки Termidesk |
| `DBPORT` | 5432 | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет порт соединения с сервером БД |
| `DBSSL` | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет протокол подключения к БД.<br>Возможные значения: `Disable`, `TLSv1.2`, `TLSv1.3`.<br>Начальное значение задается на этапе установки Termidesk |
| `DBNAME` | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет имя БД.<br>Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| DBUSER | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет имя пользователя, имеющего доступ к БД.<br>Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk |
| DBPASS | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет пароль пользователя, имеющего доступ к БД.<br>Начальное значение задается на этапе подготовки среды функционирования во время установки Termidesk и хранится в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` в преобразованном виде.<br>⚠ В стандартных установках значения менять не следует.<br>Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой `scramble`:<br>▪ для получения значения по стандартному алгоритму: `/opt/termidesk/bin/scramble --value <пароль> --type AES256`;<br>▪ для получения значения с увеличенным числом итераций преобразования: `/opt/termidesk/bin/scramble --value <пароль> --type AES256_V2`.<br>Утилита `scramble` использует в качестве вектора преобразования значение из файла `/etc/opt/termidesk-vdi/termidesk.cookie`. Значение генерируется автоматически на этапе установки Termidesk |
| DBCERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет путь к сертификату mTLS для защищенного подключения к БД.<br>⚠ mTLS - метод обеспечения защищенного соединения с БД через двустороннюю аутентификацию с использованием сертификатов.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;<br>▪ назначить владельцем файла пользователя `termidesk`:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.crt`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.crt`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**) |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| DBKEY | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет путь к ключу mTLS для защищенного подключения к БД.<br>Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению:<br>`openssl rsa -in <путь_к_файлу_ключа>.key -out <путь_сохранения_преобразованного_ключа>.key`<br>Для использования ключа также нужно:<br>▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;<br>▪ назначить владельцем файла пользователя `termidesk`:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.key`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.key`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен |
| DBCHAIN | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет путь к промежуточному сертификату mTLS для защищенного подключения к БД.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;<br>▪ назначить владельцем файла пользователя `termidesk`:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.pem`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.pem`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен |
| DJANGO_SECRET_KEY | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Используется для проверки данных, пересылаемых между компонентами Termidesk. Значение генерируется при установке Termidesk и должно быть одинаковым для всех узлов при распределенной установке |
| RABBITMQ_URL | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет URL-адрес подключения к серверам RabbitMQ. Можно подключить до трех (включительно) серверов.<br>Пароль подключения к серверу RabbitMQ, указанный в `RABBITMQ_URL`, хранится в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` в преобразованном виде.<br>Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой `scramble`:<br>▪ для получения значения по стандартному алгоритму: `/opt/termidesk/bin/scramble --value <пароль> --type AES256`;<br>▪ для получения значения с увеличенным числом итераций преобразования: `/opt/termidesk/bin/scramble --value <пароль> --type AES256_V2`.<br>Для использования преобразованного значения следует указать его в `RABBITMQ_URL` и выполнить перезапуск служб.<br>Начальное значение `RABBITMQ_URL` задается на этапе установки |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| RABBITMQ_SSL | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет протокол подключения к RabbitMQ.<br>Возможные значения: Disable, TLSv1.2.<br>Начальное значение задается на этапе установки |
| NODE_ROLES | Не задано | Параметр обязателен и задается на этапе установки.<br>Определяет тип роли, с которой будет установлен Termidesk. Возможные значения:<br>▪ ADMIN - роль «Портал администратора»;<br>▪ USER - роль «Портал пользователя»;<br>▪ TASKMAN - роль «Менеджер рабочих мест»;<br>▪ CELERYMAN - роль «Менеджер рабочих мест (очереди)»;<br>▪ AGGR_ADM - роль «Агрегатор администратора»;<br>▪ AGGR_USR - роль «Агрегатор пользователя».<br>Установка ролей «Агрегатор администратора» и/или «Агрегатор пользователя» должна производиться на узле, отличном от «Портала администратора» и/или «Портала пользователя», «Менеджера рабочих мест».<br>При переустановке значение параметра в конфигурационном файле будет перезаписано |
| LOG_LEVEL | INFO | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет уровень журналирования сообщений.<br>Возможные значения: DEBUG, INFO, WARNING, ERROR, CRITICAL |
| LOG_ADDRESS | /dev/log | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет адрес отправки записей в системный журнал. Обычно это /dev/log для Linux-систем. Возможно указать IP-адрес и порт |
| LOG_FACILITY | local3 | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет категорию сообщений syslog.<br>Категория должна совпадать с настройками в конфигурационном файле /etc/syslog-ng/conffirst.d/termidesk.conf |
| HEALTH_CHECK_ACCESS_KEY | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет токен доступа к API проверки состояния сервера. Начальное значение генерируется на этапе установки.<br>При задании значения параметра следует руководствоваться правилом, что:<br>▪ размер должен составлять от 0 до 64 символа;<br>▪ должны использоваться символы в шестнадцатеричной системе (0-9, a-f).<br>Значение также может быть сгенерировано через openssl:<br>openssl rand -hex 32 |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| METRICS_ACCESS_KEY | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет токен доступа к API получения метрик сервера. Начальное значение генерируется на этапе установки.<br>При задании значения параметра следует руководствоваться правилом, что:<br>▪ размер должен составлять от 0 до 64 символа;<br>▪ должны использоваться символы в шестнадцатеричной системе (0-9, a-f).<br>Значение также может быть сгенерировано через openssl:<br>`openssl rand -hex 32` |
| HEALTH_CHECK_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет путь к сертификату SSL/TLS для защищенного подключения к API проверки состояния сервера.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.pem`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.pem`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| HEALTH_CHECK_KEY | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет путь к ключу SSL/TLS для защищенного подключения к API проверки состояния сервера.<br>Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению:<br>`openssl rsa -in <путь_к_файлу_ключа>.key -out <путь_сохранения_преобразованного_ключа>.key`<br>Для использования ключа также нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.key`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.key`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| TASKMAN_HEALTH_CHECK_PORT | 8100 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест».<br>Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест».<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| TASKMAN_HEALTH_CHECK_IP | 0.0.0.0 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест».<br>Определяет IP-адрес, с которым служба termidesk-taskman регистрируется в подсистеме проверки состояния на странице «Инфраструктура» Termidesk. Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла.<br>Изначально параметр закомментирован (используется значение по умолчанию) |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| CELERY_BEAT_HEALTH_CHECK_PORT | 8103 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест (очереди)».<br>Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест (очереди)».<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| CELERY_BEAT_HEALTH_CHECK_IP | 0.0.0.0 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест (очереди)».<br>Определяет IP-адрес, с которым служба termidesk-celery-beat регистрируется в подсистеме проверки состояния на странице «Инфраструктура» Termidesk. Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла.<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| CELERY_WORKER_HEALTH_CHECK_PORT | 8104 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест (очереди)».<br>Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест (очереди)».<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| CELERY_WORKER_HEALTH_CHECK_IP | 0.0.0.0 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест (очереди)».<br>Определяет IP-адрес, с которым служба termidesk-celery-worker регистрируется в подсистеме проверки состояния на странице «Инфраструктура». Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла.<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| REQUESTS_CA_BUNDLE | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет путь к файлу с доверенным корневым сертификатом, задается для настройки работы с сертификатами собственных ЦС.<br>По умолчанию параметр не используется (закомментирован) |
| EULA_ACCEPTED | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет принятие лицензионного соглашения при установке. В случае автоматизированной установки наличие параметра обязательно |
| AGGREGATOR_JWT_SSL_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», использующихся в фермах, подключаемых к «Агрегатору». Обязателен для заполнения в случае, если в инфраструктуре также используется «Агрегатор».<br>Определяет путь к сертификату для получения значения JWT-токена «Агрегатора» |
| AGGREGATOR_JWT_SSL_CERT_SECOND | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», использующихся в фермах, подключаемых к «Агрегатору». Обязателен для заполнения в случае, если в инфраструктуре также используется «Агрегатор».<br>Определяет путь к резервному сертификату для получения значения JWT-токена «Агрегатора».<br>Если сертификат, заданный в AGGREGATOR_JWT_SSL_CERT, станет невалидным, то будет использоваться сертификат, указанный в AGGREGATOR_JWT_SSL_CERT_SECOND |
| AGGREGATOR_JWT_SSL_KEY | Не задано | Параметр обязателен и задается на узлах с установленным «Агрегатором» (портал «Агрегатор пользователя»).<br>Определяет путь к ключу для подписи JWT-токена «Агрегатора» |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| AGGREGATOR_ACCESS_TOKEN_TITLE | Termidesk JWT Title | Параметр обязателен и должен быть одинаковым на всех узлах, работающих совместно: на «Агрегаторе» (портал «Агрегатор пользователя»), на «Универсальных диспетчерах», подключаемых к «Агрегатору».<br>Задает заголовок JWT-токена, предназначенный для настройки взаимодействия между «Агрегатором» и «Универсальным диспетчером» |
| AGGREGATOR_ACCESS_TOKEN_TTL_SECONDS | 600 | Параметр обязателен и задается на узлах с установленным «Агрегатором».<br>Определяет времени жизни (в секундах) JWT-токена, подписанного «Агрегатором» |
| AGGREGATOR_IMAGE_CACHE_LIFETIME_HOURS | 672 | Параметр обязателен и задается на узлах с установленным «Агрегатором».<br>Определяет время жизни (в часах) кеша иконок фондов РМ. По истечении этого времени иконка обновляется |
| SECRETS_STORAGE_METHOD | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет способ хранения паролей подключения к СУБД и RabbitMQ:<br>▪ config - пароли будут храниться в преобразованном виде в файле /etc/opt/termidesk-vdi/termidesk.conf;<br>▪ openbao - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено).<br>⚠ Хранилище паролей OpenBao должно быть реализовано в отказоустойчивом варианте, иначе Termidesk не будет работать в период простоя узлов OpenBao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_URL | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет IP-адреса или FQDN узла и порта с установленным хранилищем OpenBao.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Формат: http://<IP-адрес или FQDN>:8200. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_TOKEN | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет токен (Initial Root Token), сформированный при инициализации хранилища OpenBao.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки и хранится в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf в преобразованном виде.<br>Для преобразования значения параметра, заданного вручную, следует воспользоваться утилитой scramble:<br>▪ для получения значения по стандартному алгоритму: /opt/termidesk/bin/scramble --value <пароль> --type AES256;<br>▪ для получения значения с увеличенным числом итераций преобразования: /opt/termidesk/bin/scramble --value <пароль> --type AES256_V2. |
| SECRETS_OPENBAO_DB_PATH | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет путь, настроенный на OpenBao для хранения пароля СУБД.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| SECRETS_OPENBAO_DB_ROLE_NAME | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет роль, настроенную на OpenBao и имеющую доступ к паролю СУБД.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_RABBITMQ_PATH | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора»».<br>Определяет путь, настроенный на OpenBao для хранения пароля RabbitMQ.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_RABBITMQ_ROLE_NAME | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет роль, настроенную на OpenBao и имеющую доступ к паролю RabbitMQ.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_CLIENT_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет путь к сертификату SSL/TLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.crt`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.crt`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**).<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| SECRETS_OPENBAO_CLIENT_KEY | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет путь к ключу SSL/TLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы.<br>Ключ может иметь парольную защиту. Для использования ключа в Termidesk нужно преобразовать его к начальному значению:<br>`openssl rsa -in <путь_к_файлу_ключа>.key -out <путь_сохранения_преобразованного_ключа>.key`<br>Для использования ключа также нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.key`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.key`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Изначально параметр закомментирован (используется значение по умолчанию) |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| SECRETS_OPENBAO_SERVER_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет путь к промежуточному сертификату ЦС SSL/TLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.pem<br>▪ изменить права на файл:<br>sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.pem<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| SECRETS_OPENBAO_TERMIDESK_PATH | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет путь, настроенный на OpenBao для хранения паролей Termidesk.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_TERMIDESK_ROLE_NAME | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет роль, настроенную на OpenBao и имеющую доступ к паролям Termidesk.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_KV_VERSION | 1 | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Используется для указания версии API OpenBao.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Возможные значения:<br>▪ 1 (по умолчанию);<br>▪ 2.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_CACHE_LIFETIME | 5 | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти. Позволяет сохранить полученный от OpenBao пароль на некоторое время в кеше для сокращения количества обращений к OpenBao.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |
| FLUENTD_CACHE | 15 | Параметр может быть задан на узлах «Универсального диспетчера».<br>Определяет время (в секундах) кеширования параметров подключения к узлу «Ретранслятора».<br>По умолчанию после установки время кеширования составляет 15 секунд.<br>В случае, если нужно изменить значение, следует раскомментировать параметр и задать ему новое значение |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| FLUENTD_TABLE | logs | Параметр может быть задан на узлах «Универсального диспетчера».<br>Определяет таблицу хранения событий фермы Termidesk.<br>По умолчанию после установки «Универсальный диспетчер» обращается к таблице «logs» БД «Ретранслятора».<br>В случае, если в БД «Ретранслятора» для хранения событий используется другая таблица, следует раскомментировать параметр и указать новое имя таблицы |
| WSPROXY_TICKET_TIMEOUT | 20 | При штатном функционировании Terrmidesk менять параметр не рекомендуется.<br>Параметр может быть задан на узлах «Универсального диспетчера».<br>Определяет время ожидания отклика «Шлюза» и применяется для решения нештатных ситуаций, например: если параметр «Время ожидания соединения» по каким-либо причинам не используется в протоколе доставки, или если запрос к «Шлюзу» выполняется долго и подключение пользователя не устанавливается.<br>По умолчанию после установки время ожидания составляет 20 секунд.<br>В случае, если нужно изменить значение, следует раскомментировать параметр и задать ему новое значение |

Пример файла конфигурации сервера OpenBao, который активирует строгую проверку клиентского SSL-сертификата:

```
listener "tcp" {
tls_min_version = "tls12"
tls_disable = "false"
address = "0.0.0.0:8200"
tls_cert_file = "/etc/bao/openbao.stand8.local.crt"
tls_key_file = "/etc/bao/openbao.stand8.local.key"
# Если включён, то будет проверять сертификат клиента на корректность
tls_require_and_verify_client_cert = "true"
# Если выключён, то будет требовать наличие сертификата клиента
tls_disable_client_certs = "false"
}
```

### 10.2 . Общие системные параметры Termidesk

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

Для конфигурации общих системных параметров следует перейти «Настройки - Системные параметры - Общие».

Доступные для редактирования параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 46).

Изменение системных параметров вступают в силу только после перезагрузки Termidesk.

Таблица 47 – Общие системные параметры Termidesk

| Параметр | Описание |
|---|---|
| «Генератор имен» | Варианты использования имен при развертывании ВРМ.<br>Значение по умолчанию: «С переиспользованием имен» |
| «Тема оформления» | Выбор темы оформления графического интерфейса пользователя и управления |
| «Действие с учетной записью рабочего места» | Выбор действия, которое будет произведено над учетной записью в службе каталогов при удалении ВРМ из фонда.<br>ⓘ DNS-сервер, указанный в настройках узла «Универсального диспетчера», должен иметь возможность разрешать имена узлов в зонах службы каталогов (MS AD, FreeIPA, ALD Pro).<br>Для корректного сброса пароля учетной записи при удалении РМ из фонда на узле «Универсального диспетчера» требуется наличие сертификата, выпущенного центром сертификации для работы по протоколу LDAPS. Также на узле службы каталогов MS AD должны быть созданы соответствующие SRV-записи.<br>Возможные значения:<br>▪ «Удалить при удалении фонда» (по умолчанию) - при удалении РМ из фонда учетная запись будет удалена из службы каталогов. Применимость: MS AD, FreeIPA, ALD Pro;<br>▪ «Сбросить пароль при удалении фонда» - при удалении РМ из фонда у учетной записи будет сброшен пароль. Применимость: MS AD;<br>▪ «Выключить при удалении фонда» - при удалении РМ из фонда учетная запись будет отключена. Применимость: MS AD;<br>▪ «Хранить при удалении фонда» - при удалении РМ из фонда учетная запись будет сохранена в службе каталогов. Применимость: MS AD, FreeIPA, ALD Pro.<br>Следует учесть, что при вводе гостевой ОС в MS AD:<br>▪ если учетная запись РМ находится не в стандартном каталоге «Computers», то параметр «OU» должен принимать значения вида: «OU=Computers,DC=domain,DC=local», т.е. не должен использоваться Common Name (CN);<br>▪ если учетная запись РМ находится в стандартном каталоге «Computers», то параметр «OU» должен принимать значения вида: «CN=Computers,DC=domain,DC=local», т.е. должен использоваться Common Name (CN) |
| «Автозапуск рабочего места» | Параметр автоматического подключения к фонду РМ через компонент «Клиент» (см. подраздел **Настройка автоматического подключения к фонду РМ**).<br>Значение по умолчанию: «Нет» |

| Параметр | Описание |
|---|---|
| «Подключаться к ВРМ по» | Параметр определяет, какое значение в параметрах подключения к ВРМ «Универсальный диспетчер» должен передать компоненту «Клиент».<br>Возможные значения:<br>▪ «Сетевому адресу (IP)» - в параметрах подключения будет передаваться IP-адрес ВРМ;<br>▪ «Полному доменному имени (FQDN)» - в параметрах подключения будет передаваться FQDN ВРМ.<br>Действие параметра не распространяется на протокол подключения к терминальному серверу - при таком подключении всегда передается IP-адрес.<br>При использовании метапоставщика значение параметра будет учитываться:<br>▪ при использовании значения «Полному доменному имени (FQDN)» метапоставщик будет передавать FQDN ВМ из сервисного фонда;<br>▪ при использовании значения «Сетевому адресу (IP)», метапоставщик будет передавать IP-адрес ВМ из сервисного фонда |
| «Интервал проверок кэша рабочих мест» | Периодичность (в секундах) опроса ВМ в фонде для определения статуса их готовности.<br>Значение по умолчанию: «19» |
| «Интервал проверок неиспользуемых рабочих мест» | Периодичность (в секундах) проверки наличия неактивных ВРМ для последующего их удаления.<br>Для удаления неиспользуемых ВРМ требуется задать значение «Удалять рабочее место» для политики «Действие при выходе пользователя из ОС».<br>Значение по умолчанию: «631» |
| «Интервал очистки информационных объектов» | Периодичность (в секундах) поиска информации о фондах в статусе «Удален», «Отменен», «Ошибка» для ее дальнейшей очистки. Очистка производится после истечения времени, заданного в параметре «Время хранения информационных объектов».<br>Значение по умолчанию: «3607» |
| «Количество потоков фоновых задач» | Количество одновременных задач, выполняемых «Менеджером рабочих мест» в фоновом процессе. Параметр учитывается при оценке количества подключений к СУБД (см. подразделы **Настройка СУБД PostgreSQL** и **Настройка СУБД Tantor** документа СЛЕТ.10001-02 90 02 «Руководство администратора. Настройка программного комплекса»).<br>Суммарное количество потоков, заданных в «Количество потоков фоновых задач» и «Количество потоков «Менеджера рабочих мест», не должно превышать 50. При отклонении от указанного ограничения будет отображена ошибка при попытке сохранить изменения.<br>Значение по умолчанию: «4» |
| «Не учитывать максимальные ограничения» | Не учитывать ограничения, заданные в полях «Подготавливать ВМ одновременно» и «Удалять ВМ одновременно» поставщика ресурсов при формировании фондов. Если параметр активен, в фонде одновременно может создаваться и удаляться до 1000 ВМ.<br>Значение по умолчанию: «Нет» |
| «Время хранения информационных объектов» | Время хранения (в секундах) информации о фондах в статусе «Удален», «Отменен», «Ошибка».<br>Значение по умолчанию: «14401» |

| Параметр | Описание |
|---|---|
| «Время блокировки входа» | Время (в секундах) после истечения которого будет возможен повторный вход субъекта «Администратор», «Персонал» или «Пользователь» в случае превышения субъектом лимита неудачных попыток входа.<br>По истечении этого времени пользователь продолжит визуально быть заблокированным (статус «Временно заблокирован») в списке пользователей в домене аутентификации. Статус сменится на «Активный» только после авторизации пользователя с правильным паролем или после смены статуса администратором.<br>Значение по умолчанию: «300» |
| «URL входа» | URL-адрес начальной страницы графического интерфейса управления<br>⚠ Значение параметра менять не следует.<br>Значение по умолчанию: «/login» |
| «Адрес сервера удаленного помощника» | URL-адрес узла с установленной серверной частью «Удаленного помощника».<br>Пример: «https://192.168.0.2».<br>По умолчанию значение не задано |
| «Максимальное время инициализации рабочего места» | Максимальное время (в секундах) ожидания готовности ВРМ, после истечения которого ВМ будет удалена как зависшая.<br>Значение по умолчанию: «3601» |
| «Максимум записей в журнале для объектов» | Максимальное количество системных событий, добавляемых в журнал объекта.<br>Значение по умолчанию: «100» |
| «Интервал проверки для удаления объектов» | Периодичность проверки (в секундах) ВРМ, помеченных для удаления.<br>Значение по умолчанию: «31» |
| «Количество ошибок для ограничения фонда» | Пороговое значение количества ошибок, после которого фонд будет переведен в статус «Ограниченный».<br>Значение по умолчанию: «3» |
| «Интервал отслеживания ошибок в фонде» | Периодичность отслеживания появления ошибок (в секундах), связанных с функционированием фонда.<br>Значение по умолчанию: «600» |
| «Количество потоков «Менеджера рабочих мест» | Пороговое значение потоков задач, выполняемых «Менеджером рабочих мест», при обеспечении жизненного цикла фонда РМ. Параметр учитывается при оценке количества подключений к СУБД (см. подразделы **Настройка СУБД PostgreSQL** и **Настройка СУБД Tantor** документа СЛЕТ.10001-02 90 02 «Руководство администратора. Настройка программного комплекса»).<br>Суммарное количество потоков, заданных в «Количество потоков фоновых задач» и «Количество потоков «Менеджера рабочих мест», не должно превышать 50. При отклонении от указанного ограничения будет отображена ошибка при попытке сохранить изменения.<br>Значение по умолчанию: «3» |

| Параметр | Описание |
|---|---|
| «Срок действия устаревшей публикации» | Время (в часах), по истечении которого ВМ будет удалена, если публикация фонда объявлена устаревшей.<br>При обновлении параметра его значение применяется к новым публикациям. Для публикаций, созданных до изменения параметра, будет действовать предыдущее значение параметра.<br>Если значение параметра будет равным «-1», то при перепубликации фонда РМ произойдет следующее:<br>▪ предыдущая публикация будет переведена в статус «Публикация частично удалена» (см. подраздел **Публикация фонда РМ**), если есть назначенная и используемая ВМ;<br>▪ используемая ВМ автоматически не удалится, но при этом будет создана новая публикация.<br>Если значение параметра будет равным «0», то при перепубликации фонда назначенная ВМ будет немедленно заменена на новую публикацию.<br>Если значение параметра будет равным «1», то при перепубликации фонда назначенная ВМ будет доступна 1 час, после чего удалится.<br>Значение по умолчанию: «24» |
| «Срок хранения статистики» | Время (в днях) хранения файлов журналов, по истечению которого журналы будут перезаписаны.<br>Значение по умолчанию: «365» |
| «Количество удаляемых рабочих мест за один проход» | Максимальное количество ВРМ, помеченных к удалению, которые будут проверены и удалены при каждой итерации запуска фоновой задачи очистки.<br>Значение по умолчанию: «3» |

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

### 10.3 . Параметры безопасности Termidesk

Для конфигурации системных параметров безопасности следует перейти «Настройки - Системные параметры - Безопасность».

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

Таблица 48 – Параметры безопасности Termidesk

| Параметр | Описание |
|---|---|
| «Мастер-ключ» | Идентификатор регистрации субъектов в Termidesk при доступе к фонду |
| «Доверенные хосты» | Идентификатор узлов, имеющих право подключаться к Termidesk |
| «Длительность сессии администратора» | Временной интервал сессии (в секундах), инициированной на «Портале администратора» |
| «Доступ к веб-части системным пользователем» | Возможность администратора подключаться к «Порталу администратора» |

| Параметр | Описание |
|---|---|
| «Использовать анонсируемый IP клиента» | Использовать IP-адрес клиента, передаваемый в процессе входа в Termidesk.<br>Параметр необходимо включить, если узел «Универсального диспетчера» используется в ферме Termidesk, подключаемой к порталу «Агрегатор». В противном случае при подключении пользователей к ресурсам ферм Termidesk в журнале «Универсального диспетчера» будет отображен IP-адрес портала «Агрегатор», а не IP-адреса подключившихся пользователей |
| «GID системной группы администратора» | Идентификатор группы, в которую входит учетная запись администратора |
| «Длительность сессии пользователя» | Временной интервал (в секундах) сессии пользователя.<br>Параметр влияет на длительность сессии пользователя в «Портале пользователя». Начиная с Termidesk версии 5.0 параметр также определяет общее время подключения пользователя к «Универсальному диспетчеру» Termidesk.<br>Вне зависимости от того, активен пользователь или нет, каждую секунду происходит уменьшение значения параметра на 1, при достижении значения 0 подключение пользователя завершится, при этом в системном трее на пользовательской рабочей станции отобразится уведомление от приложения «Клиент»: «Ваш сеанс завершился».<br>В журнале «Клиента» отражаются события как получения параметра («userSessionLength»), так и завершения сессии по таймауту |
| «Максимум попыток входа Администраторов» | Пороговое положительное значение числа неудачных попыток входа администратора. Параметр может быть изменен только администратором (см. **Назначение служебных функций администраторам**).<br>Значение «0» эквивалентно «без ограничений» |
| «Максимум попыток входа Персонала» | Пороговое положительное значение числа неудачных попыток входа субъектов, не относящихся к администратору.<br>Значение «0» эквивалентно «без ограничений» |
| «Максимум попыток входа Пользователей» | Пороговое положительное значение числа неудачных попыток входа пользователей.<br>Значение «0» эквивалентно «без ограничений» |

## 10.4 . Утилиты интерфейса командной строки для настройки Termidesk

### 10.4.1 . Утилита termidesk-config

Утилита `termidesk-config` используется для переопределения настроек, заданных на этапе установки и вносит изменения в конфигурационный файл `/etc/opt/termidesk-vdi/termidesk.conf` (см. подраздел **Параметры конфигурирования компонентов «Универсальный диспетчер», «Менеджер рабочих мест»**).

Для вызова утилиты следует:

- в интерфейсе командной строки перейти в каталог `/opt/termidesk/sbin/`:

```
cd /opt/termidesk/sbin/
```

- выполнить запуск:

```
sudo ./termidesk-config
```

- откроется интерфейс утилиты (см. Рисунок 34).

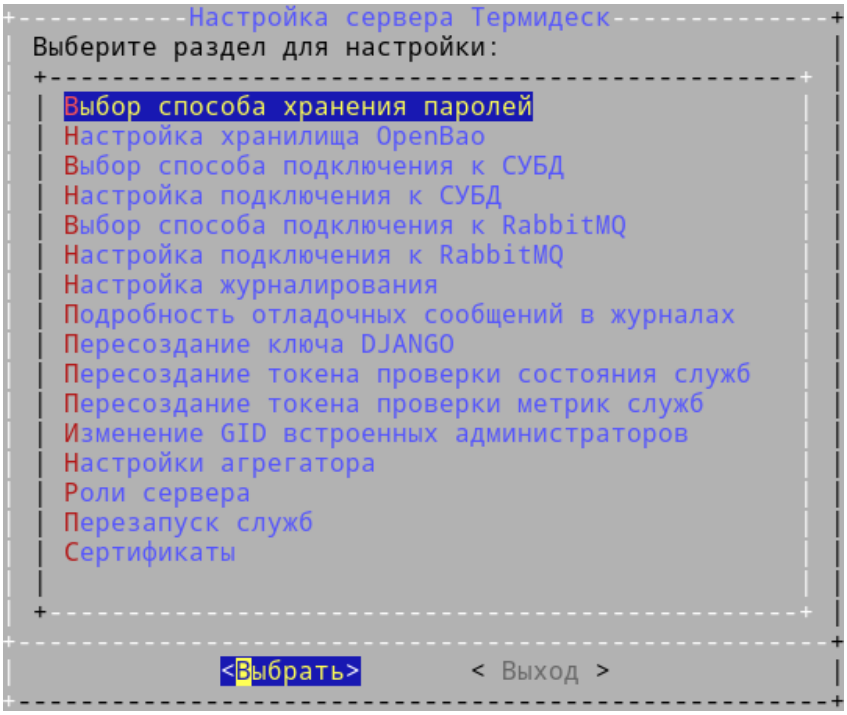


Рисунок 34 – Интерфейс утилиты termidesk-config

Доступны следующие функции утилиты:

- «Выбор способа хранения паролей»: позволяет настроить способ хранения паролей подключения к СУБД и RabbitMQ (параметр `SECRETS_STORAGE_METHOD`):
  - «config» - пароли будут храниться в преобразованном виде в файле `/etc/opt/termidesk-vdi/termidesk.conf`;
  - «openbao» - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено).

  В случае выбора «openbao» необходимо выполнить настройку подключения к хранилищу через функцию «Настройка хранилища OpenBao»;
- «Настройка хранилища OpenBao»: позволяет настроить параметры подключения к хранилищу и задать параметры, настроенные непосредственно на хранилище:
  - «URL хранилища» - IP-адрес или FQDN узла и порт с установленным хранилищем OpenBao (параметр `SECRETS_OPENBAO_URL`). Формат: `http://<IP-адрес>:8200` или `http://<FQDN>:8200`. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом;
  - «Версия API OpenBao» - установленная версия API на OpenBao (параметр `SECRETS_OPENBAO_KV_VERSION`). Может принимать значения: «1» или «2»;

- «Токен доступа к хранилищу» - токен (Initial Root Token), который был сформирован при инициализации хранилища (параметр SECRETS_OPENBAO_TOKEN);
- «Путь к паролю СУБД» - путь, настроенный на OpenBao для хранения пароля СУБД (параметр SECRETS_OPENBAO_DB_PATH);
- «Роль доступа к паролю СУБД» - роль, настроенная на OpenBao, которая имеет доступ к паролю СУБД (параметр SECRETS_OPENBAO_DB_ROLE_NAME);
- «Путь к паролям RabbitMQ» - путь, настроенный на OpenBao для хранения пароля RabbitMQ (параметр SECRETS_OPENBAO_RABBITMQ_PATH);
- «Роль доступа к паролям RabbitMQ» - роль, настроенная на OpenBao, которая имеет доступ к паролю RabbitMQ (параметр SECRETS_OPENBAO_RABBITMQ_ROLE_NAME);
- «Путь к паролям Termidesk» - путь, настроенный на OpenBao для хранения пароля Termidesk (параметр SECRETS_OPENBAO_TERMIDESK_PATH);
- «Роль доступа к паролям Termidesk» - роль, настроенная на OpenBao, которая имеет доступ к паролю Termidesk (параметр SECRETS_OPENBAO_TERMIDESK_ROLE_NAME);
- «Время кеширования паролей, сек» - время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти (параметр SECRETS_OPENBAO_CACHE_LIFETIME);

- «Выбор способа подключения к СУБД»: позволяет выбрать протокол при подключении к СУБД (параметр DBSSL);
- «Настройка подключения к СУБД»: позволяет настроить параметры подключения к СУБД:
  - «Адрес СУБД» - IP-адрес или FQDN СУБД PostgreSQL (параметр DBHOST);
  - «Порт СУБД» - порт, который используется для соединения с сервером БД (параметр DBPORT);
  - «Имя базы данных» - имя БД (параметр DBNAME);
  - «Имя пользователя» - имя пользователя для подключения к БД (параметр DBUSER);
  - «Пароль» - пароль пользователя в открытом виде (параметр DBPASS);
- «Выбор способа подключения к RabbitMQ»: позволяет выбрать протокол при подключении к RabbitMQ (параметр RABBITMQ_SSL);
- «Настройка подключения к RabbitMQ»: позволяет настроить параметры подключения к RabbitMQ (параметр RABBITMQ_URL). При запросе пароль задается в открытом виде;
- «Настройка журналирования»: позволяет настроить параметры журналирования, такие как «Адрес логгера» (параметр LOG_ADDRESS), «Поток (facility) журнала» (параметр LOG_FACILITY);
- «Подробность отладочных сообщений в журналах»: позволяет выбрать уровень подробности отладочных сообщений (параметр LOG_LEVEL);
- «Пересоздание ключа DJANGO»: позволяет переопределить значение ключа DJANGO (параметр DJANGO_SECRET_KEY), создаваемого на этапе установки. Переопределение ключа может понадобиться при его компрометации;

- «Пересоздание я токена проверки состояния служб»: позволяет переопределить значение токена проверки состояния служб (параметр `HEALTH_CHECK_ACCESS_KEY`). Переопределение токена может понадобиться при его компрометации;
- «Пересоздание токена проверки метрик служб»: позволяет переопределить значение токена проверки метрики служб (параметр `METRICS_ACCESS_KEY`). Переопределение токена может понадобиться при его компрометации;
- «Изменение GID встроенных администраторов»: позволяет назначить идентификатор группы, использующегося для встроенного домена. Изменение идентификатора может понадобиться, если встроенная в ОС группа администраторов отличается от `astra-admin (1001)` или если нужно предоставить права администрирования Termidesk группе непривилегированных пользователей;
- «Настройки Агрегатора»: позволяет переопределить настройки портала «Агрегатор»:
  - «Время жизни токена Агрегатора, секунд» - время жизни JWT-токена (параметр `AGGREGATOR_ACCESS_TOKEN_TTL_SECONDS`, доступная для изменения только на узле с установленным порталом «Агрегатор»);
  - «Заголовок JWT-токена Агрегатора» - заголовок JWT-токена, предназначенный для настройки взаимодействия между порталом «Агрегатор» и «Универсальным диспетчером». Параметр должен быть одинаковым на всех узлах, работающих совместно: на порталах «Агрегатора», на «Универсальных диспетчерах» (параметр `AGGREGATOR_ACCESS_TOKEN_TITLE`);
  - «Время кеширования иконок фондов, часов» - время жизни кеша иконок фондов (параметр `AGGREGATOR_IMAGE_CACHE_LIFETIME_HOURS`);
- «Роли сервера»: позволяет изменить роли, которые запускаются на узле. Доступные роли: «Портал администратора», «Портал пользователя», «Менеджер рабочих мест», «Менеджер рабочих мест (очереди)», «Агрегатор администратора», «Агрегатор пользователя»;
- «Перезапуск служб» - позволяет выполнить перезапуск служб Termidesk;
- «Сертификаты» - позволяет выполнить настройку сертификатов и ключей:

> ⚠ Пункт «Серт. для расшифровки JWT-токена» настраивается только на узле с установленным «Универсальным диспетчером» («Портал администратора» и (или) «Портал пользователя») фермы Termidesk.
> Пункт «Прив. ключ для подписи JWT-токена» настраивается только на узле портала «Агрегатор» («Агрегатор администратора» и (или) «Агрегатор пользователя»).
> Оставшиеся пункты могут быть настроены на обоих узлах индивидуально.

  - «Сертификат Health Check» - путь к сертификату для защищенного подключения к API проверки состояния (параметр `HEALTH_CHECK_CERT`);

- «Секр. ключ Health Check» - путь к ключу для защищенного подключения к API проверки состояния (параметр `HEALTH_CHECK_KEY`);
- «Сертификат Postgres mTLS» - путь к сертификату для защищенного подключения к СУБД (параметр `DBCERT`);
- «Секр. ключ Postgres mTLS» - путь к ключу для защищенного подключения к СУБД (параметр `DBKEY`);
- «Серт. промеж. ЦС Postgres mTLS» - путь к корневому и промежуточным сертификатам mTLS для защищенного подключения к СУБД (параметр `DBCHAIN`);
- «Сертификат OpenBao mTLS» - путь к сертификату для защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_CLIENT_CERT`);
- «Секр. ключ OpenBao mTLS» - путь к ключу для защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_CLIENT_KEY`);
- «Серт. промеж. ЦС OpenBao mTLS» - путь к корневому и промежуточным сертификатам mTLS для защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_SERVER_CERT`);
- «Осн. серт. для расшифровки JWT-токена» - путь к сертификату для получения значения JWT-токена портала «Агрегатор» (параметр `AGGREGATOR_JWT_SSL_CERT`);
- «Рез. серт. для расшифровки JWT-токена» - путь к резервному сертификату для получения значения JWT-токена портала «Агрегатор» (параметр `AGGREGATOR_JWT_SSL_CERT_SECOND`);
- «Секр. ключ для подписи JWT-токена» - путь к ключу для подписи JWT-токена портала «Агрегатор» (параметр `AGGREGATOR_JWT_SSL_KEY`).

Установка ролей «Агрегатор администратора» и (или) «Агрегатор пользователя» должна производиться на узле, отличном от «Портала администратора» и (или) «Портала пользователя», «Менеджера рабочих мест».
Смена ролей через функцию «Роли сервера» в этом случае не предусмотрена: нельзя ранее установленные «Портал администратора» и (или) «Портал пользователя» перенастроить на использование ролей «Агрегатор администратора» и (или) «Агрегатор пользователя».
Роль «Менеджер рабочих мест» не должна устанавливаться с «Агрегатором администратора» и (или) «Агрегатором пользователя».
Роль «Менеджер рабочих мест» (очереди) устанавливается с «Агрегатором администратора» и (или) «Агрегатором пользователя».

- «Перезапуск служб»: позволяет выполнить перезапуск служб Termidesk.

После выполнения изменений в любом из разделов рекомендуется воспользоваться пунктом «Перезапуск служб» для применения изменений.

### 10.4.2 . Утилита termidesk-vdi-manage

Утилита `termidesk-vdi-manage` используется для настройки «Универсального диспетчера» из интерфейса командной строки.

Для вызова утилиты следует:

- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- вывести список команд утилиты:

```
/opt/termidesk/sbin/termidesk-vdi-manage help
```

Каждая подкоманда в приведенных ниже командах поддерживает вывод справки через ключ `-h`.
Для управления параметрами поставщиков ресурсов, доменов аутентификации, протоколов доставки и других компонентов, настраиваемых через «Портал администратора» Termidesk, следует обратиться к командам секции `[termidesk]`.

Большая часть команд из вывода `/opt/termidesk/sbin/termidesk-vdi-manage help` предназначена для работы с БД и фреймворком Django и не приведена здесь.

Команды секции `[termidesk]` приведены в таблице (см. Таблица 49).

Таблица 49 – Команды секции [termidesk]

| Параметр | Описание |
|---|---|
| `drop_tables` | Удаляет таблицы из БД. Для просмотра списка ключей следует воспользоваться аргументом `-h`:<br>`/opt/termidesk/sbin/termidesk-vdi-manage drop_tables -h`<br>Поддерживаются аргументы:<br>▪ `--noinput`, `--no-input` - сообщает Django НЕ запрашивать у пользователя ввод;<br>▪ `-R <МАРШРУТИЗАТОР>`, `--router <МАРШРУТИЗАТОР>` - использование указанного маршрутизатора БД вместо определенного в настройках `settings.py`;<br>▪ `-S <СХЕМА>`, `--schema <СХЕМА>` - удаление указанной схемы вместо `public`;<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы |

| Параметр | Описание |
|---|---|
| `tdsk_auth` | Создает домен аутентификации. Для просмотра списка ключей следует воспользоваться аргументом `-h`:<br>`/opt/termidesk/sbin/termidesk-vdi-manage tdsk_auth -h`<br>Поддерживаются аргументы:<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы.<br>Поддерживаются подкоманды:<br>▪ `create` - создание домена аутентификации;<br>▪ `list` - вывод списка доменов аутентификации;<br>▪ `remove` - удаление домена аутентификации;<br>▪ `login` - аутентификация в указанный домен;<br>▪ `logout` - завершение сессии.<br>Подкоманда `create` принимает аргументы:<br>▪ `--type` - задание типа домена аутентификации. Доступны: `ALDAuthenticatorPlugin` («Astra Linux Directory»), `IPAuth` («IP аутентификация»), `KerberosAuthenticatorPlugin` («FreeIPA»), `SAMLAuthenticator` («SAML»), `SimpleLdapAuthenticator` («MS Active Directory (LDAP)»);<br>▪ `--params` - задание параметров домена аутентификации. Формат: `имя1=значение1 имя2=значение2` и т.д. Доступные параметры для указанного типа домена аутентификации можно получить через команду `--list` , например: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_auth create --type KerberosAuthenticatorPlugin --name test --small_name test--list --test`;<br>▪ `--list` - вывод параметров домена аутентификации;<br>▪ `--test` - проверка параметров без создания домена аутентификации;<br>▪ `--quiet` - вывод только сообщений об ошибках;<br>▪ `--name <ИМЯ>` - имя домена аутентификации;<br>▪ `--small_name <короткое имя>` - короткое имя домена аутентификации. Допустимые символы: a-z, A-Z, 0-9. Максимальная длина 32 символа;<br>▪ `--priority <приоритет>` - числовое значение приоритета домена аутентификации, по умолчанию «1»;<br>▪ `--comments <комментарий>` - комментарий к создаваемому домену.<br>Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате JSON.<br>Подкоманда `remove` принимает аргументы:<br>▪ `--output json` - вывод параметров в формате JSON;<br>▪ `--silent` - «тихое» удаление для выполнения команды из исполняемого файла;<br>▪ `--uuid <идентификатор>` - идентификатор объекта для удаления.<br>Подкоманда `login` принимает аргументы:<br>▪ `--uuid <идентификатор>` - идентификатор объекта для аутентификации;<br>▪ `--small_name <короткое имя>` - короткое имя домена аутентификации; |

| Параметр | Описание |
|---|---|
| | ▪ `--output json` - вывод параметров в формате JSON.<br>Подкоманда `logout` принимает аргументы:<br>▪ `--token <токен>` - токен сессии пользователя;<br>▪ `--output json` - вывод параметров в формате JSON |
| `tdsk_clearsessions` | Порционная очистка сессий.<br>Поддерживаются аргументы:<br>▪ `-chunk <количество>` - количество сессий для удаления, по умолчанию 1000;<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы |
| `tdsk_config` | Работа с системными настройками.<br>Поддерживаются аргументы:<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы.<br>Поддерживаются подкоманды:<br>▪ `list` - вывод конфигурационных параметров и их значений;<br>▪ `set` - установка значения конфигурационному параметру.<br>Подкоманда `set` принимает аргументы:<br>▪ `--section` - секция параметра из доступных: `Security`, `IPAUTH`, `Global`, `Monitoring`, `Experimental`, `Notifications`, `Audit`, `Metrics`;<br>▪ `--key <ключ>` - ключ параметра;<br>▪ `--value <значение>` - значение параметра.<br>Пример команды для смены значения параметра `metrics.cacheSize` («Размер кеша») секции `Metrics` на «9»:<br>`:~$ /opt/termidesk/sbin/termidesk-vdi-manage set --section Metrics --key metrics.cacheSize --value 9` |

| Параметр | Описание |
|---|---|
| `tdsk_exp_2fa_add_statictoken` | Добавление токена пользователю.<br>Поддерживаются аргументы:<br>▪ `username` - имя пользователя, с которым будет ассоциирован токен;<br>▪ `-t <токен>`, `--token <токен>` - токен, который нужно добавить. Если этот параметр пропущен, он будет сгенерирован случайным образом;<br>▪ `--auth_uuid <идентификатор>` - идентификатор домена аутентификации;<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы |
| `tdsk_exp_2fa_clear_totpdevice` | Удаление TOTP-устройства пользователя.<br>Поддерживаются аргументы:<br>▪ `username` - имя пользователя, которому нужно удалить TOTP-устройство;<br>▪ `--auth_uuid <идентификатор>` - идентификатор домена аутентификации;<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы |

| Параметр | Описание |
|---|---|
| `tdsk_graph_models` | Создание файла GraphViz с описанием моделей БД для указанных имен приложений.<br>Можно передать несколько имен приложений, и все они будут объединены в одну модель.<br>Пример использования команды приведен в подразделе **Генерация отчета по моделям данных и структурам БД Termidesk**.<br>Поддерживаются аргументы:<br>▪ `app_label` - наименование приложения;<br>▪ `--pygraphviz` - использование PyGraphViz для создания изображения;<br>▪ `--pydot` - использование PyDot(Plus) для создания изображения;<br>▪ `--disable-fields`, `-d` - не показывать поля;<br>▪ `--group-models`, `-g` - сгруппировать модели в соответствии с их применением;<br>▪ `--all-applications`, `-a` - включить все приложения для вывода модели;<br>▪ `--output <путь к файлу>`, `-o <путь к файлу>` - запись вывода в файл;<br>▪ `--layout <макет>`, `-l <макет>` - использование макета GraphViz для визуализации. Поддерживаются: `circo`, `dot`, `fdpneato`, `nop`, `nop1`, `nop2`, `twopi`;<br>▪ `--verbose-names`, `-n` - использование подробных имен для моделей и полей;<br>▪ `--language <локализация>`, `-L <локализация>` - указания языка, который будет использоваться для подробных имен;<br>▪ `--exclude-columns <столбцы>`, `-x <столбцы>` - исключение определенных столбцов;<br>▪ `--exclude-models <модели>`, `-X <модели>` - исключение определенных моделей;<br>▪ `--include-models <модели>`, `-I <модели>` - ограничение только указанными моделями;<br>▪ `--inheritance`, `-e` - включение наследования (используется по умолчанию);<br>▪ `--no-inheritance`, `-E` - выключение наследования;<br>▪ `--hide-relations-from-fields`, `-R` -<br>▪ `--disable-sort-fields`, `-S` -<br>▪ `--json` - вывод в формат JSON;<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы |

| Параметр | Описание |
|---|---|
| `tdsk_group` | Создание группы РМ.<br>Поддерживаются аргументы:<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы.<br>Поддерживаются подкоманда `create` (создание группы рабочих мест) со следующими аргументами:<br>▪ `--quiet` - вывод только сообщений об ошибках;<br>▪ `--name <имя>` - имя создаваемой группы;<br>▪ `--comments <комментарий>` - комментарий к создаваемой группе;<br>▪ `--priority <приоритет>` - числовое значение приоритета группы |
| `tdsk_license` | Управление лицензией Termidesk.<br>Поддерживаются аргументы:<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы.<br>Поддерживаются подкоманды:<br>▪ `install` - установить лицензию из файла, поддерживается относительный или абсолютный путь к файлу. Пример команды для установки лицензии: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_license install <путь к файлу лицензии>`;<br>▪ `show` - вывести информацию об установленной лицензии. Для вывода в формате JSON следует использовать аргумент `--output`: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_license show --output json` |

| Параметр | Описание |
|---|---|
| `tdsk_net` | Создание сети.<br>Поддерживаются аргументы:<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы.<br>Поддерживается подкоманда `create` (создание сети) со следующими аргументами:<br>▪ `--quiet` - вывод только сообщений об ошибках;<br>▪ `--name <имя>` - имя создаваемой сети;<br>▪ `--netRange <диапазон>` - диапазон IP-адресов. Допустимы различные форматы, например: A.B.C.*, A.B.C.D/N, A.B.C.D - E.F.G.D |
| `tdsk_openbao_migrate` | Миграция способа хранения паролей и переход с конфигурационного файла на использование хранилища OpenBao.<br>Поддерживаются аргументы:<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы |
| `tdsk_openbao_reverse_migrate` | Миграция способа хранения паролей и переход с хранилища OpenBao на конфигурационный файл.<br>Поддерживаются аргументы:<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы |

| Параметр | Описание |
|---|---|
| `tdsk_osm` | Создание параметров гостевой ОС.<br>Поддерживаются аргументы:<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы.<br>Поддерживается подкоманда `create` (создание параметров гостевой ОС) со следующими аргументами:<br>▪ `--params` - задание параметров гостевой ОС. Формат: `имя1=значение1 имя2=значение2` и т.д.;<br>▪ `--list` - вывод параметров гостевой ОС;<br>▪ `--test` - проверка параметров без создания объекта;<br>▪ `--quiet` - вывод только сообщений об ошибках;<br>▪ `--name <ИМЯ>` - наименование параметров гостевой ОС;<br>▪ `--comments <комментарий>` - комментарий к создаваемым параметрам |
| `tdsk_pool` | Управление фондами РМ.<br>Поддерживаются аргументы:<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы.<br>Поддерживаются подкоманды:<br>▪ `create` - создание фонда РМ;<br>▪ `list` - вывод списка фондов РМ.<br>Подкоманда `create` принимает аргументы:<br>▪ `--quiet` - вывод только сообщений об ошибках;<br>▪ `--name <ИМЯ>` - имя фонда РМ;<br>▪ `--comments <комментарий>` - комментарий к создаваемому фонду РМ;<br>▪ `--service_id <идентификатор>` - указание идентификатора шаблона РМ;<br>▪ `--osmanager_id <идентификатор>` - указание идентификатора параметров гостевой ОС РМ;<br>▪ `--image_id <идентификатор>` - указание идентификатора изображения гостевой ОС;<br>▪ `--servicesPoolGroup_id <идентификатор>` - указание идентификатора группы РМ;<br>▪ `--cache_l1_srvs <значение>` - количество РМ в кеше 1-го уровня;<br>▪ `--cache_l2_srvs <значение>` - количество РМ в кеше 2-го уровня;<br>▪ `--max_srvs <значение>` - максимальное количество РМ.<br>Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате JSON |

| Параметр | Описание |
|---|---|
| `tdsk_prov` | Управление поставщиками ресурсов.<br>Поддерживаются аргументы:<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы.<br>Поддерживаются подкоманды:<br>▪ `create` - создание поставщика ресурсов;<br>▪ `list` - вывод списка поставщиков ресурсов.<br>Подкоманда `create` принимает аргументы:<br>▪ `--type` - задание типа поставщика ресурсов. Доступны: `RedVirtPlatform` («Платформа RED Virtualization»), `SessionsPlatform` («Сервер Терминалов [экспериментальный]»), `VMmanagerPlatform` («Платформа VMmanager»), `oVirtPlatform` («Платформа oVirt/RHEV»), `pksvbrestPlatform` («ПК СВ Брест»), `vmwarePlatform` («Платформа VMware»), `zVirtPlatform` («Платформа zVirt»), `PhysicalMachinesServiceProvider` («Автономная машина»);<br>▪ `--params` - задание параметров поставщика ресурсов. Формат: `имя1=значение1 имя2=значение2` и т.д. Доступные параметры для указанного типа поставщика ресурсов можно получить через команду `--list` , например: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_prov create --type RedVirtPlatform --name test --list --test` ;<br>▪ `--list` - вывод параметров поставщика ресурсов;<br>▪ `--test` - проверка параметров без создания поставщика ресурсов;<br>▪ `--quiet` - вывод только сообщений об ошибках;<br>▪ `--name <имя>` - наименование поставщика ресурсов;<br>▪ `--comments <комментарий>` - комментарий к создаваемому поставщику ресурсов.<br>Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате JSON |
| `tdsk_refresh_ssa` | Регистрация «Сессионного агента» в БД Termidesk.<br>Поддерживаются аргументы:<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы |

| Параметр | Описание |
|---|---|
| `tdsk_trans` | Управление протоколами доставки.<br>Поддерживаются аргументы:<br>▪ `--version` - вывод версии программы;<br>▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;<br>▪ `--settings <настройки>` - путь к модулю настроек Python;<br>▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;<br>▪ `--traceback` - вызов исключений;<br>▪ `--no-color` - вывод команды без подсвечивания;<br>▪ `--force-color` - вывод команды с принудительным подсвечиванием;<br>▪ `--skip-checks` - пропуск проверки системы.<br>Поддерживаются подкоманды:<br>▪ `create` - добавление протокола доставки;<br>▪ `list` - вывод списка протоколов доставки;<br>▪ `remove` - удалить протокол доставки;<br>▪ `convert` - конвертировать протокол доставки (`RDSTransport`, `RDSWSTRDPTransport`, `STALTransport`, `STALWSTRDPTransport`) в новый протокол `TerminalTransport`.<br>Подкоманда `create` принимает аргументы:<br>▪ `--type` - задание типа протокола. Доступны: `HTML5Transport` («HTML5»), `HTML5VNCTransport` («VNC (HTML5, через локальный прокси)»), `LoudplayDirectTransport` («Loudplay (напрямую, эксперим.)»), `LoudplayTunneledTransport` («Loudplay (через вебсокет шлюз, эксперим.)»), `RDPTransport` («RDP (напрямую)»), `RDSTransport` («Доступ к MS RDS по RDP (напрямую) [экспериментальный]»), `RDSWSTRDPTransport` («Доступ к MS RDS по RDP (через шлюз) [экспериментальный]»), `STALTransport` («Доступ к STAL по RDP (напрямую) [экспериментальный]»), `STALWSTRDPTransport` («Доступ к STAL по RDP (через шлюз) [экспериментальный]»), `TDSKSPICETransport` («SPICE (vdi-viewer, эксперим.)»), `WSTRDPTransport` («RDP (через вебсокет шлюз)»), `TERATransport` («TERA [экспериментальный]»), `TerminalTransport` («RDP (терминальный доступ)»);<br>▪ `--params` - задание параметров протокола доставки. Формат: `имя1=значение1 имя2=значение2` и т.д. Доступные параметры для указанного типа протокола доставки можно получить через команду `--list`, например: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_trans create --type RDPTransport --name test --list`;<br>▪ `--list` - вывод параметров протокола доставки;<br>▪ `--test` - проверка параметров без создания протокола доставки;<br>▪ `--quiet` - вывод только сообщений об ошибках;<br>▪ `--name <имя>` - наименование протокола доставки;<br>▪ `--comments <комментарий>` - комментарий к создаваемому протоколу доставки;<br>▪ `--priority <приоритет>` - числовое значение приоритета протокола доставки;<br>▪ `--allowed_oss <перечень ОС>` - перечень разрешенных ОС из списка: `Android`, `CrOS`, `FreeBSD`, `iPad`, `iPhone`, `Linux`, `Mac`, `Windows`, `Windows Phone`. Формат: `имя1,имя2,имя3`;<br>▪ `--nets_positive <yes/no>` - указание, что протокол должен быть доступен только из сетей, указанных в параметре `--networks`. Может принимать значения не только `yes` или `no`, подходит в целом любое непустое значение; |

| Параметр | Описание |
|---|---|
| | ▪ `--networks <наименования сетей>` - перечень сетей, доступ из которых разрешен для создаваемого протокола доставки. Формат: `имя1,имя2,имя3`.<br>Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате JSON.<br>Подкоманда `create` принимает аргументы:<br>▪ `--output json` - вывод списка в формате JSON;<br>▪ `--silent` - выполнение в «тихом» режиме;<br>▪ `--uuid <идентификатор>` - идентификатор объекта для удаления.<br>Подкоманда `convert` принимает аргументы:<br>▪ `--uuid <идентификатор>` - идентификатор протокола доставки, который необходимо конвертировать (`RDSTransport`, `RDSWSTRDPTransport`, `STALTransport`, `STALWSTRDPTransport`);<br>▪ `--all` - ковернтировать все протоколы доставки MS RDS и STAL |
| `tdsk_version` | Получение версии Termidesk |

## 10.5 . Назначение служебных функций администраторам

В Termidesk для администраторов реализовано разделение доступных служебных функций.

Для назначения доступных служебных функций следует перейти «Настройки - Управление ролями» и нажать экранную кнопку [Создать] (см. Рисунок 35).

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

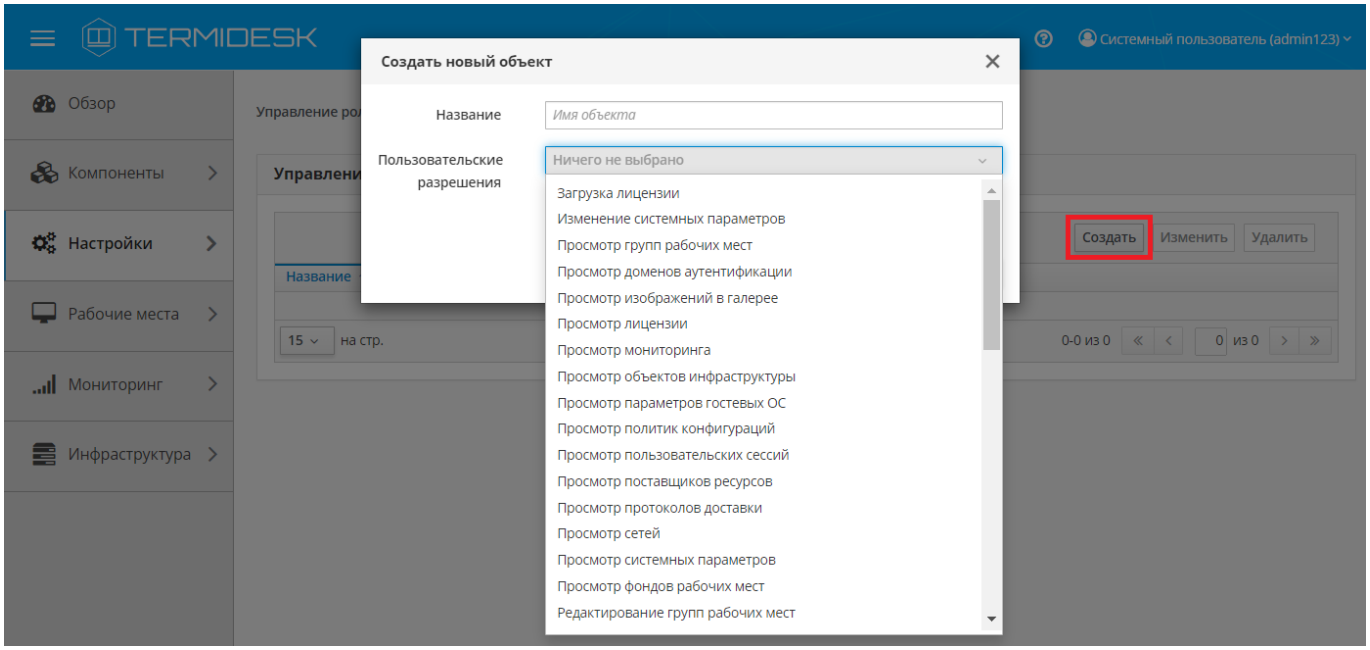


Рисунок 35 – Окно назначения пользовательских разрешений

Список разрешений для назначения служебных функций администраторам перечислен в столбце «Разрешение» следующей таблицы (см. Таблица 50).

⚠ Перед назначением разрешения на редактирование, создание, удаление или управление необходимо предоставить соответствующее разрешение на просмотр страницы.

Таблица 50 – Список доступных для выбора разрешений

| Разрешение | Описание |
|---|---|
| «Загрузка лицензии» | Разрешение позволяет загружать лицензии на странице «Настройки - Лицензия» на вкладке «Загрузка» |
| «Изменение системных параметров» | Разрешение позволяет управлять системными параметрами на странице «Настройки - Системные параметры» |
| «Просмотр групп рабочих мест» | Предоставляет доступ на чтение страницы «Настройки - Группы рабочих мест» для просмотра списка созданных групп РМ |
| «Просмотр доменов аутентификации» | Предоставляет доступ на чтение страницы «Компоненты - Домены аутентификации». Разрешение позволяет выполнять просмотр:<br>▪ пользователей домена, назначенных им групп, РМ, ВМ и журнал;<br>▪ списка групп домена и пользователей, входящих в каждую группу;<br>▪ журнала |
| «Просмотр изображений в галерее» | Предоставляет доступ на чтение страницы «Настройки - Галерея» для просмотра списка загруженных изображений |
| «Просмотр лицензии» | Предоставляет доступ на чтение страницы «Настройки - Лицензия» для просмотра информации о лицензии и системе |
| «Просмотр мониторинга» | Предоставляет доступ на чтение страницы «Мониторинг». Разрешение позволяет выполнять просмотр:<br>▪ раздела «Журналы», экспорт записей в формате `.CSV`;<br>▪ раздела «Аудит», экспорт записей в формате `.CSV`;<br>▪ раздела «Отчёты», создание, редактирование, удаление отчетов, экспорт записей в формате `.CSV` |
| «Просмотр объектов инфраструктуры» | Предоставляет доступ на чтение страниц раздела «Инфраструктура» для просмотра информации о статусе компонентов Termidesk |
| «Просмотр параметров гостевых ОС» | Предоставляет доступ на чтение страницы «Компоненты - Параметры гостевых ОС» для просмотра списка созданных параметров гостевых ОС |
| «Просмотр политик конфигураций» | Предоставляет доступ на чтение страницы «Настройки - Глобальные политики» для просмотра значений параметров политик |
| «Просмотр пользовательских сессий» | Предоставляет доступ на чтение страницы «Рабочие места - Сессии» для просмотра списка активных сессий пользователей |
| «Просмотр поставщиков ресурсов» | Предоставляет доступ на чтение страницы «Компоненты - Поставщики ресурсов». Разрешение позволяет выполнять просмотр:<br>▪ списка созданных поставщиков ресурсов;<br>▪ списка созданных шаблонов РМ |

| Разрешение | Описание |
|---|---|
| «Просмотр протоколов доставки» | Предоставляет доступ на чтение страницы «Компоненты - Протоколы доставки» для просмотра списка созданных протоколов доставки |
| «Просмотр сетей» | Предоставляет доступ на чтение страницы «Компоненты - Сети» для просмотра списка созданных сетей |
| «Просмотр системных параметров» | Предоставляет доступ на чтение страницы «Настройки - Системные параметры» для просмотра заданных системных параметров |
| «Просмотр фондов рабочих мест» | Предоставляет доступ на чтение страницы «Рабочие места - Фонды». Разрешение позволяет выполнять:<br>▪ просмотр раздела «Фонды» и выполнять действия в разделе:<br>• просматривать список опубликованных фондов РМ;<br>• просматривать вкладки «Рабочие места», «Пользователи и группы», «Протоколы доставки», «Журнал» при выборе опубликованного фонда РМ;<br>▪ просмотр раздела «Индивидуальные рабочие места» для просмотра информации о назначенных ВМ |
| «Редактирование групп рабочих мест» | Разрешение позволяет редактировать параметры созданных групп РМ |
| «Редактирование доменов аутентификации» | Разрешение позволяет редактировать параметры созданных доменов аутентификации |
| «Редактирование изображений в галерее» | Разрешение позволяет редактировать параметры загруженных изображений в галерее |
| «Редактирование параметров гостевых ОС» | Разрешение позволяет редактировать созданные параметры гостевых ОС |
| «Редактирование политик конфигураций» | Разрешение позволяет выполнять:<br>▪ редактирование политик;<br>▪ сброс значения политики |
| «Редактирование поставщика ресурсов» | Разрешение позволяет редактировать параметры созданных поставщиков ресурсов |
| «Редактирование протоколов доставки» | Разрешение позволяет редактировать параметры созданных протоколов доставки |
| «Редактирование сетей» | Разрешение позволяет редактировать параметры созданных сетей |
| «Редактирование фондов рабочих мест» | Разрешение позволяет редактировать параметры:<br>▪ созданных фондов РМ;<br>▪ индивидуальных РМ |
| «Создание групп рабочих мест» | Разрешение позволяет создавать группы РМ |
| «Создание доменов аутентификации» | Разрешение позволяет добавлять домены аутентификации |
| «Создание изображений в галерее» | Разрешение позволяет загружать изображения в галерею |
| «Создание параметров гостевых ОС» | Разрешение позволяет создавать параметры гостевых ОС |
| «Создание поставщика ресурсов» | Разрешение позволяет добавлять поставщиков ресурсов |
| «Создание протоколов доставки» | Разрешение позволяет добавлять протоколы доставки |

| Разрешение | Описание |
|---|---|
| «Создание сетей» | Разрешение позволяет добавлять сети |
| «Создание фондов рабочих мест» | Разрешение позволяет создавать фонды РМ |
| «Удаление групп рабочих мест» | Разрешение позволяет удалять группы РМ |
| «Удаление доменов аутентификации» | Разрешение позволяет удалять домены аутентификации |
| «Удаление изображений из галереи» | Разрешение позволяет удалять изображения из галереи |
| «Удаление объектов инфраструктуры» | Разрешение позволяет удалять компоненты Termidesk из таблиц раздела «Инфраструктура» |
| «Удаление параметров гостевых ОС» | Разрешение позволяет удалять параметры гостевых ОС |
| «Удаление поставщика ресурсов» | Разрешение позволяет удалять поставщиков ресурсов |
| «Удаление протоколов доставки» | Разрешение позволяет удалять протоколы доставки |
| «Удаление сетей» | Разрешение позволяет удалять сети |
| «Удаление фондов рабочих мест» | Разрешение позволяет удалять фонды РМ |
| «Управление группами домена аутентификации» | Разрешение позволяет выполнять действия:<br>▪ добавление группы домена аутентификации;<br>▪ редактирование группы домена аутентификации;<br>▪ удаление группы домена аутентификации |
| «Управление пользовательскими сессиями» | Разрешение позволяет выполнять действия с активными сессиями пользователей:<br>▪ отключение сессии;<br>▪ сброс сессии |
| «Управление пользователями домена аутентификации» | Разрешение позволяет выполнять действия:<br>▪ добавление пользователя домена аутентификации;<br>▪ редактирование пользователя домена аутентификации;<br>▪ удаление пользователя домена аутентификации |
| «Управление ролями» | Разрешение позволяет выполнять:<br>▪ просмотр раздела «Управление ролями» и выполнять действия в разделе:<br>• создавать роли;<br>• редактировать роли;<br>• удалять роли;<br>▪ просмотр раздела «Управление ACL» и выполнять действия в разделе:<br>• создавать разрешения для объектов;<br>• редактировать разрешения для объектов;<br>• удалять разрешения для объектов |
| «Управление шаблонами рабочих мест» | Разрешение позволяет выполнять действия:<br>▪ создание шаблона РМ;<br>▪ редактирование шаблона РМ;<br>▪ удаление шаблона РМ |

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

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

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

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

На открывшейся странице в таблице «Пользователи» нужно выбрать пользователя и нажать экранную кнопку **[Изменить]**. В открывшейся форме редактирования пользователя в поле «Роли» выбрать класс (см. Рисунок 36).

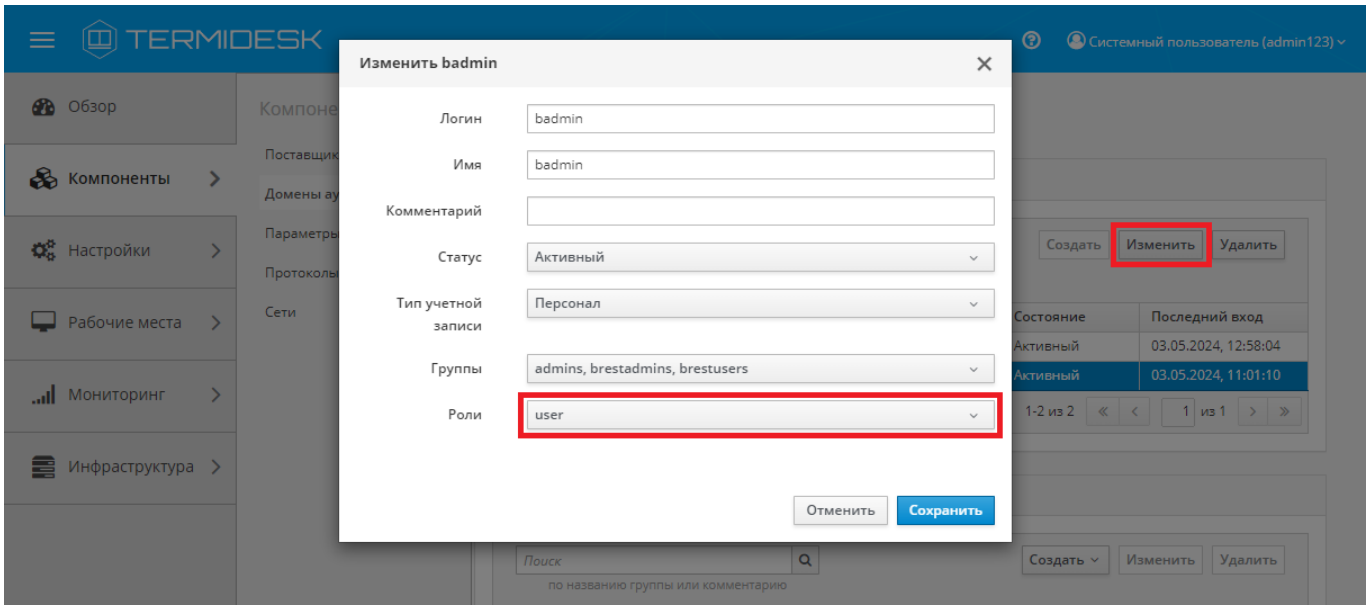


Рисунок 36 – Окно назначения пользовательских ролей

⚠ 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 PM. Для добавления нового разрешения объекту следует перейти «Настройки - Управление ACL», нажать экранную кнопку **[Создать]** и выбрать объект «Фонд рабочих мест».

В режиме добавления нового разрешения для объекта администратору Termidesk необходимо заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 51).

Таблица 51 – Доступные параметры при добавлении пользовательских разрешений для фондов PM

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

| Параметр | Описание |
|---|---|
| «Пользовательское разрешение» | Выбор пользовательских разрешений, касающихся фондов РМ.<br>Список всех доступных разрешений, можно выбрать несколько:<br>▪ «Восстановление рабочих мест»;<br>▪ «Просмотр фондов рабочих мест»;<br>▪ «Редактирование фондов рабочих мест»;<br>▪ «Удаление фондов рабочих мест»;<br>▪ «Управление кешем фондов рабочих мест»;<br>▪ «Управление питанием фондов рабочих мест». Если в версии Termidesk ниже 5.1 было задано разрешение «Управление кешем фондов рабочих мест», во время обновления для него создастся разрешение «Управление питанием фондов рабочих мест»;<br>▪ «Управление пользовательскими группами фондов рабочих мест»;<br>▪ «Управление пользователями фондов рабочих мест»;<br>▪ «Управление протоколами доставки фондов рабочих мест»;<br>▪ «Управление публикациями фондов рабочих мест» |
| «Объект» | Ранее созданный фонд РМ |

⚠ При изменении ранее созданного разрешения параметр «Объект» менять не рекомендуется. Если нужно изменить непосредственно объект, то следует создать новое разрешение.

### 10.6 . Перенаправление на HTTPS

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

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

```
sudo systemctl restart apache2
```

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

Пример исходного конфигурационного файла:

```
1  #<VirtualHost *:80>
2  #    ServerName #HOSTNAME#
3  #    DocumentRoot /opt/termidesk/share/termidesk-vdi/src
4  #
5  #    Alias /media/ /opt/termidesk/share/termidesk-vdi/src/media/
6  #    Alias /static/ /opt/termidesk/share/termidesk-vdi/src/static/
7  #
8  #    <Directory /opt/termidesk/share/termidesk-vdi/src/static>
9  #        Order deny,allow
10 #        Allow from all
```

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

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

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

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

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

```
    </Directory>

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

    RewriteEngine on
    ProxyTimeout 70
    ProxyPreserveHost On
    ProxyRequests Off

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

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

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

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

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

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

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

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

Пример конфигурационного файла для работы по незащищенному протоколу HTTP:

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

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

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

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

    RewriteEngine on
    ProxyTimeout 70
    ProxyPreserveHost On
    ProxyRequests Off

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

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

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

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

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

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

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

```

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

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

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

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

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

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

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

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

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

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

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

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

```
111 #</IfModule>
```

### 10.7 . Замена SSL-сертификата веб-сервера

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

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

Для замены SSL-сертификатов необходимо:

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

```
sudo cp <путь_к_сертификату> /etc/ssl/certs/
```

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

```
sudo cp <путь_к_ключу> /etc/ssl/certs/
```

> Если сертификат и ключ находятся в PKCS12-контейнере (файл формата `.pfx`), необходимо сначала сконвертировать их в нужный формат:
>
> ```
> 1 openssl pkcs12 -in <путь_к_pfx-контейнеру> -out <путь_к_создаваемому_файлу.pem> -nodes
> 2 openssl pkcs12 -in <путь_к_pfx-контейнеру> -nocerts -nodes -out <путь_к_создаваемому_файлу.key>
> ```

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

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

- перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

### 10.8 . Установка корневого сертификата центра сертификации

Установка корневого сертификата центра сертификации (ЦС) может быть необходима при настройке доступа между компонентами по протоколу SSL. Предполагается, что инфраструктура открытых ключей (PKI) уже развернута в организации и ЦС установлен.
Для установки корневого сертификата ЦС (например, `CA.crt`) на «Универсальный диспетчер» Termidesk, нужно:

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

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

- выполнить добавление корневого сертификата ЦС:

```
sudo dpkg-reconfigure ca-certificates
```

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

Для настройки Termidesk на работу с сертификатами нужно:

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

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

- выполнить перезапуск службы `termidesk-vdi`:

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

### 10.9 . Работа веб-интерфейса Termidesk с протоколом TLS

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

- выполнить резервное копирование текущего файла конфигурации:

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

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

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

- выполнить обновление файлов конфигурации:

```
sudo systemctl reload apache2
```

### 10.10 . Настройка защищенного подключения к компоненту «Универсальный диспетчер»

Для настройки защищенного подключения к компоненту «Универсальный диспетчер» нужно:

- скопировать закрытый ключ формата `.key` и сертификат формата `.pem` в каталог `/etc/opt/termidesk-vdi`:

```
sudo cp /etc/ssl/private/ssl-cert-snakeoil.key /etc/opt/termidesk-vdi/
sudo cp /etc/ssl/certs/ssl-cert-snakeoil.pem /etc/opt/termidesk-vdi/
```

- назначить права по использованию ключа и сертификата пользователю `termidesk`:

```
sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/ssl-cert-snakeoil.*
```

- предоставить права на чтение файла `ssl-cert-snakeoil.key`:

```
:~$ sudo chmod 644 /etc/opt/termidesk-vdi/ssl-cert-snakeoil.key
```

- отредактировать файл `/lib/systemd/system/termidesk-vdi.service`, добавив аргументы `--certfile` и `--keyfile` с указанием пути к файлам ключа и сертификата:

```
--keyfile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.key
--certfile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.pem
```

- пример содержимого файла `termidesk-vdi.service`:

```
[Unit]
Description=Termidesk-VDI daemon
After=network.target

[Service]
PIDFile=/run/termidesk-vdi/pid
Restart=on-failure
RestartSec=5

User=termidesk
Group=termidesk
WorkingDirectory=/opt/termidesk/share/termidesk-vdi/src

```

```
Environment=VIRTUAL_ENV=/opt/termidesk/share/termidesk-vdi/venv
Environment=PATH=/opt/termidesk/share/termideskvdi/venv/bin:/usr/sbin:/usr/bin:/sbin:/bin
EnvironmentFile=/etc/opt/termidesk-vdi/termidesk.conf

ExecStart=/bin/bash -c '/opt/termidesk/share/termidesk-vdi/venv/bin/gunicorn server.wsgi:application --timeout 60 --workers $(expr $(nproc --all) \* 3) --keyfile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.key --certfile /etc/opt/termidesk-vdi/ssl-certsnakeoil.pem --bind 127.0.0.1:8000'

ExecReload=/bin/kill -s HUP $MAINPID
ExecStop=/bin/kill -s TERM $MAINPID
PrivateTmp=true

[Install]
WantedBy=multi-user.target
```

- перезапустить сервис `termidesk-vdi.service`:

```
sudo systemctl daemon-reload && systemctl restart termidesk-vdi.service
```

- отредактировать файл `/etc/apache2/sites-available/termidesk.conf`:
  - добавить в файл следующие строки:

```
SSLProxyEngine on
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
```

где:

`SSLProxyEngine` - использование защищенного подключения по протоколу SSL/TLS, `on` - включить использование;

`SSLProxyVerify` - параметр контроля проверки сертификата. Доступны следующие значения: `none` - отключение проверки сертификата, `optional` - необязательная проверка сертификата, `require` - обязательная проверка сертификата, `optional_no_ca` - проверка сертификата без обязательной проверки цепочки сертификатов;

`SSLProxyCheckPeerCN` - проверка общего имени (Common Name, CN) сервера в сертификате, `off` - выключить проверку;

`SLProxyCheckPeerName` - проверка имени узла сервера в сертификате, `off` - выключить проверку;

`SSLProxyCheckPeerExpire` - проверка срока действия сертификата, `off` - выключить проверку.

  - изменить значения в параметрах `ProxyPass` и `ProxyPassReverse` с `http` на `https`:

```
ProxyPass / https://127.0.0.1:8000/
```

```
ProxyPassReverse / https://127.0.0.1:8000/
```

- изменить значения параметров `SSLCertificateFile` и `SSLCertificateKeyFile`, указав путь до сертификатов:

```
SSLCertificateFile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.pem
SSLCertificateKeyFile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.key
```

- пример файла `termidesk.conf`:

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

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

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

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

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

    RewriteEngine on
    ProxyTimeout 70
    ProxyPreserveHost On
    ProxyRequests Off

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

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

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

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

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

    SSLEngine on
    SSLProxyEngine on
    SSLProxyVerify none
    SSLProxyCheckPeerCN off
    SSLProxyCheckPeerName off
    SSLProxyCheckPeerExpire off
    SSLCertificateFile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/opt/termidesk-vdi/ssl-cert-snakeoil.key

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

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

- перезапустить веб-сервер:

```
sudo systemctl daemon-reload && systemctl restart apache2.service
```

- проверить доступность веб-интерфейса.

### 10.11 . Управление авторизацией пользователя в компоненте «Клиент»

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

Для изменения параметров авторизации следует перейти «Настройки - Системные параметры - Аутентификация» и настроить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 52).

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

Таблица 52 – Доступные параметры при настройке сохранения паролей в компоненте «Клиент»

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

## 10.12 . Настройка отправки метрик для «Сессионного агента»

Метрики узла «Сессионного агента» используются в механизмах балансировки терминальных серверов (метапоставщик) (см. подразделы **Перечень параметров для добавления терминального сервера метапоставщика** и **Балансировка подключений на основе загрузки терминальных серверов метапоставщика**), а также могут направляться в подключаемые внешние системы мониторинга.

Для настройки отправки метрик узла «Сессионного агента» следует перейти «Настройки - Системные параметры - Метрики». Доступные параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 53).

> ⓘ Конфигурацию параметров можно изменить также через утилиту `termidesk-vdi-manage`: функцию `tdsk_config` и секцию `Metrics` (см. подраздел **Утилита termidesk-vdi-manage**).

Таблица 53 – Параметры отправки метрик узла «Сессионного агента»

| Параметр | Описание |
|---|---|
| «Пороговое значение» | Величина изменения метрики, при которой необходимо принудительно оповестить «Универсальный диспетчер».<br>Диапазон значений: «1-500».<br>Значение по умолчанию: «500» |
| «Периодичность проверки» | Периодичность (в секундах), с которой «Сессионный агент» опрашивает ОС и собирает метрики узла.<br>⚠ Изменение параметра вступит в силу только после перезагрузки Termidesk или перезапуска службы `termidesk-vdi`.<br>Следует дождаться отправки обновленного значения на «Сессионный агент» (ориентировочно спустя период, заданный в параметре «Периодичность отправки среднего значения»).<br>Когда «Сессионный агент» получит обновленное значение, нужно перезапустить его службу после появления следующего сообщения в журнале «Сессионного агента»: «Получены новые настройки. Для применения изменений потребуется перезагрузка приложения».<br>Диапазон значений: «1-60».<br>Значение по умолчанию: «5» |

| Параметр | Описание |
|---|---|
| «Периодичность отправки среднего значения» | Периодичность (в секундах), с которой «Сессионный агент» отправляет средние значения метрик «Универсальному диспетчеру».<br>⚠ Изменение параметра вступит в силу только после перезагрузки Termidesk или перезапуска службы `termidesk-vdi`.<br>Следует дождаться отправки обновленного значения на «Сессионный агент» (ориентировочно спустя период, заданный в параметре «Периодичность отправки среднего значения»).<br>Когда «Сессионный агент» получит обновленное значение, нужно перезапустить его службу после появления следующего сообщения в журнале «Сессионного агента»: «Получены новые настройки. Для применения изменений потребуется перезагрузка приложения».<br>Диапазон значений: 1-60.<br>Значение по умолчанию: «30» |
| «Размер кеша» | Размер кеша (записей) на «Сессионном агенте» для хранения метрик. На основании этого параметра происходит подсчет средних значений для отправки.<br>⚠ Изменение параметра вступит в силу только после перезагрузки Termidesk или перезапуска службы `termidesk-vdi`.<br>Следует дождаться отправки обновленного значения на «Сессионный агент» (ориентировочно спустя период, заданный в параметре «Периодичность отправки среднего значения»).<br>Когда «Сессионный агент» получит обновленное значение, нужно перезапустить его службу после появления следующего сообщения в журнале «Сессионного агента»: «Получены новые настройки. Для применения изменений потребуется перезагрузка приложения».<br>Диапазон значений: «2-10».<br>Значение по умолчанию: «10» |

### 10.13 . Управление переподключением пользователя к сеансам для компонента «Клиент»

В Termidesk предусмотрена возможность управлять переподключением пользователя к сеансам через портал «Универсального диспетчера». Настройки применяются к компоненту «Клиент».

Для изменения параметров переподключения следует перейти «Настройки - Системные параметры - Клиент» и настроить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 54). Для сохранения параметров после изменения нажать экранную кнопку **[Сохранить]**.

Таблица 54 – Доступные параметры при настройке переподключения к сеансам

| Параметр | Описание |
|---|---|
| «Активировать управление перемещением сеансов» | Форсировать управление режимом повторного подключения пользователя. При активации параметра пользователь не сможет самостоятельно изменить настройку повторного подключения в интерфейсе «Клиента».<br>Возможные значения:<br>▪ «Да» - переподключение пользователя будет форсировано со стороны «Универсального диспетчера»;<br>▪ «Нет» (по умолчанию) - переподключение пользователя будет управляться в интерфейсе «Клиента» |
| «Использовать перемещение сеансов» | Использование возможно при активации параметра «Активировать управление перемещением сеансов».<br>Управление повторным подключением пользователя к отключенным и активным сеансам для компонента «Клиент». Функционал позволяет восстанавливать подключение после разрыва соединения или смены устройства (пользовательской рабочей станции). Таким образом пользователь сможет получить тот же сеанс, с которым работал ранее, не теряя прогресс работы.<br>Возможные значения:<br>▪ «Не назначено» (по умолчанию) - выбор режима будет задан пользователем в интерфейсе «Клиента»;<br>▪ «Запрещено» - повторное переподключение не используется;<br>▪ «Повторно подключаться к активным и отключенным сеансам» (по умолчанию). В этом случае при переподключении на РМ сначала будет произведена процедура отключения активного сеанса пользователя, после которой он будет повторно подключен к отключенному сеансу;<br>▪ «Повторно подключаться только к отключенным сеансам». В этом случае переподключение пользователя будет происходить только к отключенным сеансам |
| «Повторно подключаться к сеансам при аутентификации» | Использование возможно при активации параметра «Активировать управление перемещением сеансов».<br>Параметр определяет режим повторного подключения при активации параметра «Разрешить повторное подключение».<br>Возможные значения:<br>▪ «Да» - переподключение будет происходить при аутентификации пользователя через «Клиент»;<br>▪ «Нет» (по умолчанию) - переподключение не будет происходить при аутентификации пользователя |
| «Повторно подключаться к сеансам при обновлении списка приложений» | Использование возможно при активации параметра «Активировать управление перемещением сеансов».<br>Параметр определяет режим повторного подключения при активации параметра «Разрешить повторное подключение».<br>Возможные значения:<br>▪ «Да» - переподключение будет происходить при обновлении списка приложений;<br>▪ «Нет» (по умолчанию) - переподключение не будет происходить при обновлении списка приложений |

ⓘ Отключенный сеанс - это сеанс работающего РМ без активного подключения со стороны программы доставки (например, ПО Termidesk Viewer). Активный сеанс, соответственно, предполагает активное подключение со стороны программы доставки.

### 10.14 . Изменение способа хранения паролей на OpenBao

При стандартной настройке Termidesk пароли хранятся в преобразованном виде в файле `/etc/opt/termidesk-vdi/termidesk.conf`. В Termidesk версии 5.1 добавлен новый способ хранения паролей с использованием настроенного хранилища OpenBao.

Для изменения способа хранения паролей и перехода на использование хранилища OpenBao нужно:

- задать в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` параметру `SECRET_STORAGE_METHOD` значение `openbao`;
- задать остальные параметры конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf`, относящиеся к OpenBao (см. подраздел **Параметры конфигурирования компонентов «Универсальный диспетчер», «Менеджер рабочих мест»**);
- в интерфейсе командной строки переключиться на пользователя `termidesk`:

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

- выполнить команду миграции:

```
:~$ /opt/termidesk/sbin/termidesk-vdi-manage tdsk_openbao_migrate
```

При появлении ошибок после выполнения команды миграции нужно:

- изменить значение параметра `SECRET_STORAGE_METHOD` на `config`;
- повторить ввод паролей для параметров, указанных в ошибке;
- снова изменить значение `SECRET_STORAGE_METHOD` на `openbao`;
- выполнить команду миграции:

```
:~$ /opt/termidesk/sbin/termidesk-vdi-manage tdsk_openbao_migrate
```

Для возврата к способу хранения паролей из конфигурационного файла нужно:

- убедиться, что в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` параметру `SECRET_STORAGE_METHOD` задано значение `openbao`;
- в интерфейсе командной строки переключиться на пользователя `termidesk`:

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

- выполнить команду миграции:

```
:~$ /opt/termidesk/sbin/termidesk-vdi-manage tdsk_openbao_reverse_migrate
```

- задать в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` параметру `SECRET_STORAGE_METHOD` значение `config`.

# 11 . РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

## 11.1 . Общие сведения

Поскольку каждая установка компонентов Termidesk может отличаться от других, подробные шаги по резервному копированию и восстановлению и используемые инструменты будут приведены только для некоторых компонентов. Резервное копирование и восстановление может выполняться как средствами и службами ОС, так и специализированными системами. Порядок выполнения и периодичность резервного копирования определяются эксплуатирующей организацией.

Резервному копированию подлежат:

- БД Termidesk;
- конфигурационные файлы компонента «Универсальный диспетчер» и административного и/или пользовательского порталов;
- конфигурационные файлы компонента «Шлюз»;
- конфигурационные файлы компонента «Менеджер рабочих мест»;
- конфигурационные файлы компонента «Сервер терминалов Astra Linux»;
- конфигурационные файлы компонента «Сессионный агент»;
- конфигурационные файлы балансировщика нагрузки;
- конфигурационные файлы, использующиеся для режима высокой доступности.

В качестве альтернативного варианта могут резервироваться целиком узлы компонентов, если они установлены на ВМ. Такой подход применяется, например, для резервирования компонента «Виртуальный модуль Termidesk».

Как правило, файлы компонентов «Удаленный помощник», «Клиент» не подлежат резервному копированию, т.к. повторная установка в большинстве случаев будет быстрее.

## 11.2 . Действия с БД Termidesk

### 11.2.1 . Резервное копирование БД

Резервное копирование БД, созданной СУБД PostgreSQL можно выполнить утилитой `pg_dump`:

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

где:

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

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

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

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

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

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

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

### 11.2.2 . Восстановление БД из резервной копии

Восстановление БД из резервной копии выполняется командой:

```
pg_restore -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W --format=t <файл_копии_БД.tar>
```

где:

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

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

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

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

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

`--format=t <файл_копии_БД.tar>` - ключ для восстановления БД из резервной копии в формате `tar`.

## 11.3 . Действия с брокером сообщений RabbitMQ

### 11.3.1 . Резервное копирование данных брокера сообщений RabbitMQ

Для брокера сообщений RabbitMQ следует:

- остановить службу `rabbitmq-server`:

```
sudo systemctl stop rabbitmq-server
```

- выполнить резервное копирование каталога `/etc/rabbitmq/` вместе с его содержимым;
- выполнить резервное копирование каталога данных `/var/lib/rabbitmq/mnesia/`;
- запустить службу `rabbitmq-server`:

```
sudo systemctl start rabbitmq-server
```

### 11.3.2 . Восстановление брокера сообщений RabbitMQ из резервной копии

> ⓘ Современные версии RabbitMQ (3.8.0+) поддерживают восстановление из резервной копии тогда, когда они восстанавливаются на узел RabbitMQ с точно таким же именем узла, с которого была создана резервная копия данных.

Для восстановления конфигурации RabbitMQ следует:

- остановить службу `rabbitmq-server`:

```
sudo systemctl stop rabbitmq-server
```

- восстановить резервные копии каталогов `/etc/rabbitmq/` и `/var/lib/rabbitmq/mnesia/`;
- запустить службу `rabbitmq-server`:

```
sudo systemctl start rabbitmq-server
```

## 11.4 . Действия с компонентом «Универсальный диспетчер»

### 11.4.1 . Резервное копирование данных «Универсального диспетчера»

Для компонента «Универсальный диспетчер» следует выполнить резервное копирование:

- каталога `/etc/opt/termidesk-vdi/` вместе с его содержимым;
- конфигурационного файла `/etc/apache2/sites-available/termidesk.conf`;
- ключей `/etc/ssl/certs/ssl-cert-snakeoil.pem` и `/etc/ssl/private/ssl-cert-snakeoil.key`, использующихся для защищенного подключения.

### 11.4.2 . Восстановление «Универсального диспетчера» из резервной копии

Для восстановления конфигурации «Универсального диспетчера» следует:

- восстановить резервную копию каталога `/etc/opt/termidesk-vdi/`;
- восстановить резервные копии конфигурационного файла `/etc/apache2/sites-available/termidesk.conf` и ключей `/etc/ssl/certs/ssl-cert-snakeoil.pem`, `/etc/ssl/private/ssl-cert-snakeoil.key`;
- перезапустить службу `termidesk-vdi`:

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

- перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

## 11.5 . Действия с компонентом «Шлюз»

### 11.5.1 . Резервное копирование данных «Шлюза»

Для компонента «Шлюз» следует выполнить резервное копирование:

- конфигурационного файла `/etc/termidesk/gateway.yaml`;
- ключей, использующихся для защищенного соединения, указанных в файле `/etc/termidesk/gateway.yaml`.

#### 11.5.2 . Восстановление «Шлюза» из резервной копии

Для восстановления конфигурации «Шлюза» следует:

- восстановить резервную копию файла `/etc/termidesk/gateway.yaml` и ключей указанных в этом файле;
- перезапустить службу `termidesk-gateway`:

```
sudo systemctl restart termidesk-gateway
```

### 11.6 . Действия с компонентом «Менеджер рабочих мест»

#### 11.6.1 . Резервное копирование данных «Менеджера рабочих мест»

Для компонента «Менеджер рабочих мест» следует выполнить резервное копирование каталога `/etc/opt/termidesk-vdi/` вместе с его содержимым.

#### 11.6.2 . Восстановление «Менеджера рабочих мест» из резервной копии

Для восстановления конфигурации «Менеджера рабочих мест» следует:

- восстановить резервную копию каталога `/etc/opt/termidesk-vdi/`;
- перезапустить службы:

```
sudo systemctl restart termidesk-taskman termidesk-celery-beat termidesk-celery-worker
```

⚠ Если компонент «Менеджер рабочих мест» был установлен в распределенном варианте установки Termidesk, необходимо учесть, что одновременно служба `termidesk-taskman` должна быть запущена только на одном из узлов, работающих в режиме балансировки.

### 11.7 . Действия с компонентом «Сервер терминалов Astra Linux»

#### 11.7.1 . Резервное копирование данных «Сервера терминалов Astra Linux»

Для компонента «Сервер терминалов Astra Linux» следует выполнить резервное копирование каталога `/etc/stal/` и компонента «Сессионный агент» (см. подраздел **Резервное копирование данных «Сессионного агента»**).

#### 11.7.2 . Восстановление «Сервера терминалов Astra Linux» из резервной копии

Для восстановления конфигурации «Сервера терминалов Astra Linux» следует:

- восстановить резервную копию каталога `/etc/stal/`;
- восстановить компонент «Сессионный агент» (см. подраздел **Восстановление «Сессионного агента» из резервной копии**);
- перезапустить службы:

```
sudo systemctl restart termidesk-stal stal-proxy stal-rdpepc
```

### 11.8 . Действия с компонентом «Сессионный агент»

#### 11.8.1 . Резервное копирование данных «Сессионного агента»

Для компонента «Сессионный агент» следует выполнить резервное копирование:

- каталога `/etc/opt/termidesk-ssa/` (для ОС Astra Linux Special Edition (Server));
- каталога `%ProgramData%\UVEON\Termidesk Session Agent\` (для ОС Microsoft Windows Server).

#### 11.8.2 . Восстановление «Сессионного агента» из резервной копии

Для восстановления конфигурации «Сессионного агента» следует:

- восстановить резервную копию каталога `/etc/opt/termidesk-ssa/` (для ОС Astra Linux Special Edition (Server)) или `%ProgramData%\UVEON\Termidesk Session Agent\` (для ОС Microsoft Windows Server);
- перезапустить службу `TermideskSessionAgentService` через оснастку «Службы» в ОС Microsoft Windows Server или командой в ОС Astra Linux Special Edition (Server):

```
sudo systemctl restart termidesk-session-agent
```

### 11.9 . Действия с балансировщиком нагрузки

#### 11.9.1 . Резервное копирование данных балансировщика нагрузки

> ⓘ Пример приведен для балансировщика nginx, поскольку его настройка описана в качестве примера в подразделе **Настройка балансировщика для работы с самоподписанными сертификатами**.

Для балансировщика нагрузки `nginx` следует выполнить резервное копирование:

- каталога `/etc/nginx/snippets`;
- каталога с ключами и сертификатами `/etc/ssl/`;
- каталога `/etc/nginx/sites-available/`;
- каталога `/etc/nginx/conf.d/`.

#### 11.9.2 . Восстановление балансировщика нагрузки из резервной копии

Для восстановления конфигурации балансировщика нагрузки `nginx` следует:

- восстановить резервные копии каталогов `/etc/nginx/snippets`, `/etc/ssl/`, `/etc/nginx/sites-available/`, `/etc/nginx/conf.d/`;
- перезапустить веб-сервер:

```
sudo systemctl restart nginx
```

## 11.10 . Действия для режима высокой доступности

### 11.10.1 . Резервное копирование конфигурации режима высокой доступности

Для режима высокой доступности, настраиваемого для отказоустойчивой или распределенной установки Termidesk, следует выполнить резервное копирование каталога `/etc/keepalived/`.

### 11.10.2 . Восстановление конфигурации режима высокой доступности из резервной копии

Для восстановления конфигурации режима высокой доступности следует:

- восстановить из резервной копии каталог `/etc/keepalived/`;
- перезапустить сервис `keeaplived`:

```
sudo systemctl restart keepalived
```

# 12 . ГЕНЕРАЦИЯ ОТЧЕТА ПО МОДЕЛЯМ ДАННЫХ И СТРУКТУРАМ БД TERMIDESK

## 12.1 . Генерация отчета по моделям данных и структурам БД Termidesk

В Termidesk реализована возможность генерации отчета по моделям данных и структурам БД с описанием полей таблиц, их значений и межтабличных связей.

Для генерации отчета следует перейти в интерфейс командной строки и выполнить следующее:

- если требуется сгенерировать отчет по модели данных и структуре БД приложения:

```
sudo /opt/termidesk/sbin/termidesk-vdi-manage tdsk_graph_models termidesk >
<имя_файла_для_сохранения.html>
```

где:

`termidesk` - название приложения;

`<имя_файла_для_сохранения.html>` - имя и формат файла (`html`) для сохранения отчета.

> ⚠ Для генерации отчета по модели данных и структуре БД нескольких приложений их названия указываются через пробел.

- если требуется сгенерировать отчет по всей модели данных и структуре БД Termidesk:

```
sudo /opt/termidesk/sbin/termidesk-vdi-manage tdsk_graph_models -a -g >
<имя_файла_для_сохранения.html>
```

где:

`-a` - ключ для генерации отчета, описывающего все доступные модели данных и структуры БД;

`-g` - ключ группировки таблиц в соответствии с их приложениями;

`<имя_файла_для_сохранения.html>` - имя и формат файла (`html`) для сохранения отчета.

Структура файла отчета приведена в таблице (см. Таблица 55).

Таблица 55 – Структура файла отчёта

| Параметр | Описание |
|---|---|
| `App` | Название приложения, для которого представлена структура модели данных |
| `Model` | Идентификатор модели с представлением структуры данных |
| `Abstract Model` | Идентификатор модели, для которой представлена структура данных |
| `<Информационная строка>` | Строка содержит модель отчета с перечислением полей, либо дополнительную информацию о модели данных |
| `NAME` | Столбец содержит имена параметров |

| Параметр | Описание |
|---|---|
| VALUE | Столбец содержит тип данных параметров |
| HELP TEXT | Столбец содержит описание параметров |

# 13 . МОНИТОРИНГ И УВЕДОМЛЕНИЯ

## 13.1 . Системные параметры мониторинга

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

Для конфигурации системных параметров мониторинга следует перейти «Настройки - Системные параметры - Мониторинг».

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 56).

Таблица 56 – 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.<br>Доступные значения: «UDP», «TCP», «TLS». При использовании протокола «TLS» необходимо установить на узел с «Универсальным диспетчером» Termidesk корневой сертификат ЦС, использующийся в syslog-сервере, согласно подразделу **Установка корневого сертификата центра сертификации**.<br>Значение по умолчанию: «UDP» |
| «Категория сообщения» | Выбор категории сообщений, которые будут записываться в журнал мониторинга |
| «Уровень логирования» | Выбор уровня логирования событий (`INFO`, `WARNING`, `ERROR`, `CRITICAL`, `DEBUG`) |

## 13.2 . Настройка отправки уведомлений о системных событиях

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

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 57).

> Уведомление о достижении максимальной нагрузки терминального сервера («Терминальный сервер (Максимальная нагрузка)») отправляется всегда, если включена возможность отправки почтовых уведомлений.

Таблица 57 – Параметры отправки уведомлений о событиях

| Параметр | Описание |
|---|---|
| «Вкл/выкл почтовых уведомлений» | Включение или отключение возможности отправки уведомлений о системных событиях по электронной почте |
| «Хост» | IP-адрес или имя узла сервера исходящей электронной почты.<br>Пример: «smtp.mail.ru» |

| Параметр | Описание |
|---|---|
| «Порт» | Номер порта, на котором ведется прослушивание службой сервера электронной почты.<br>При указании номера порта стоит руководствоваться правилами:<br>▪ если используется порт 25, то параметры «Поддержка TLS» и «Поддержка SSL» активировать не нужно;<br>▪ если используется порт 465, то нужно активировать параметр «Поддержка SSL»;<br>▪ если используется порт 587, то нужно активировать параметр «Поддержка TLS»;<br>▪ если используется порт 2525, то нужно активировать параметр «Поддержка TLS» |
| «Email отправителя» | Почтовый адрес отправителя сообщений на сервере электронной почты.<br>Формат: user@domain.<br>Пример: «user.mail.ru» |
| «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.<br>Возможные значения: от 1 до 180.<br>Значение по умолчанию: «30» |
| «Email получателей (через запятую)» | Перечень адресов электронной почты получателей уведомлений.<br>Формат: user@domain.<br>Пример: «user.mail.ru» |
| «Префикс для темы письма» | Текстовое поле, содержащее информацию для подстановки в тему электронного письма |
| «Уведомление о смене режима техобслуживания в поставщике ресурсов» | Включение возможности отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания в поставщике ресурсов» |
| «Уведомление о смене режима техобслуживания в фонде рабочих мест» | Включение возможности отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания в фонде рабочих мест» |
| «Уведомление о смене режима техобслуживания для рабочих мест» | Включение возможности отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания для рабочих мест» |
| «Уведомление о возникновении ошибок с рабочими местами» | Включение возможности отправки уведомления по электронной почте о системном событии «Возникновение ошибок внутри фонда рабочих мест» |
| «Уведомление о превышении лицензированного количества подключений» | Включение возможности отправки уведомления по электронной почте о системном событии «Запрос подключения сверх лимита, установленного лицензией» |
| «Уведомление о превышении лицензированного количества пользователей» | Включение возможности отправки уведомления по электронной почте о системном событии «Запрос входа пользователя сверх лимита, установленного лицензией» |

### 13.3 . Шаблон для мониторинга Zabbix

Termidesk поддерживает мониторинг состояния компонентов через ПО Zabbix.

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

В шаблоне находятся метрики для мониторинга компонентов Termidesk: «Универсального диспетчера», «Шлюза», «Менеджера рабочих мест».

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

### 13.4 . Отчеты

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

Можно сформировать следующие отчеты:

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

Для формирования отчета по последнему пользовательскому входу в систему нажать экранную кнопку **[Создать]**, выбрать тип отчета «Отчет по последнему пользовательскому входу в систему» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 58).

Таблица 58 – Параметры для формирования отчета по последнему пользовательскому входу в Termidesk

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

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

Для формирования отчета по пользовательским сеансам нажать экранную кнопку **[Создать]**, выбрать тип отчета «Отчет по пользовательским сеансам» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 59).

Таблица 59 – Параметры для формирования отчета по пользовательским сеансам

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование отчета |

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

Для формирования отчета по пользовательским подключениям нажать экранную кнопку **[Создать]**, выбрать тип отчета «Отчет по пользовательским подключениям» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 60).

Таблица 60 – Параметры для формирования отчета по пользовательским подключениям

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

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

При помощи экранной кнопки **[CSV]** можно выгрузить в csv-файл весь представленный отчет (см. Рисунок 37).

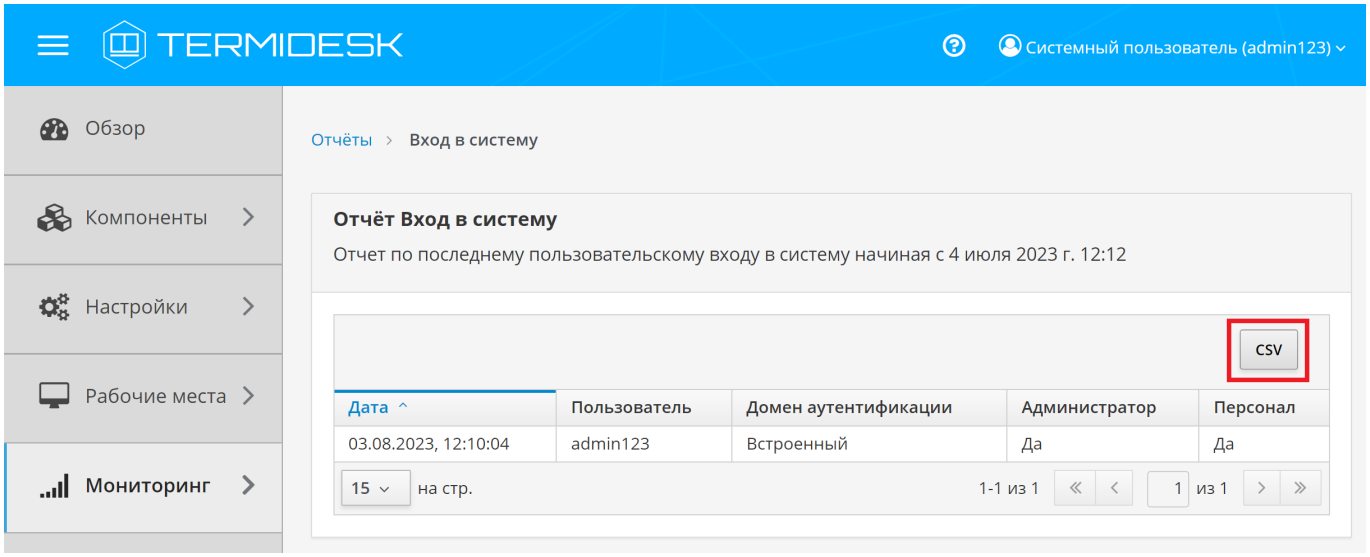


Рисунок 37 – Окно сформированного отчета по последнему пользовательскому входу

### 13.5 . Получение метрик узлов компонентов

В Termidesk реализован механизм API-запросов для получения метрик узлов, на которых установлены компоненты Termidesk, что позволяет использовать полученные метрики во внешних системах мониторинга.

Подробная информация по формату API-запросов приведена в документе СЛЕТ.10001-02 91 01 «Инструкция по использованию. REST API».

# 14 . СИСТЕМА АУДИТА

## 14.1 . Системные параметры аудита

Для конфигурации системных параметров аудита следует перейти «Настройки - Системные параметры - Аудит».

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 60).

Таблица 61 – 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.<br>Доступные значения: «UDP», «TCP», «TLS». При использовании протокола «TLS» необходимо установить на «Универсальный диспетчер» Termidesk корневой сертификат ЦС, использующийся в syslog-сервере, согласно подразделу **Установка корневого сертификата центра сертификации**.<br>Значение по умолчанию: «UDP» |
| «Порт» | Порт, на котором находится служба syslog-сервера |
| «Категория сообщения» | Выбор категории сообщений, которые будут записываться в журнал аудита |

События аудита, регистрируемые Termidesk, приведены в подразделе **Типы и шаблоны регистрируемых событий аудита**.

## 14.2 . Журналы

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

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

- `auth.log` - записываются события об авторизации субъектов в Ternidesk;
- `celery-beat.log` - записываются события периодической проверки состояния обработчика заданий через RabbitMQ. Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;
- `celery-worker.log` - записываются события обработчика заданий через RabbitMQ. Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;
- `other.log` - записываются события платформ ПК СВ Брест и VMware, а также события, не относящиеся к другим модулям;
- `services.log` - записываются события работы ВМ на платформе oVirt;
- `database.log` - записываются отладочные события БД;
- `termidesk.log` - записываются события работы «Универсального диспетчера» Termidesk;
- `use.log` - записываются события подключения пользователей РМ;
- `workers.log` - записываются события обработчика фоновых задач;
- `aggregator.log` - записываются события работы портала «Агрегатор».

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

### 14.3 . Настройка журналирования

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

Для изменения уровня журналирования нужно:

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

```
1  sudo systemctl restart termidesk-vdi.service termidesk-taskman.service
   termidesk-celery-beat.service termidesk-celery-worker.service
```

### 14.4 . Просмотр системных журналов

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

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

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

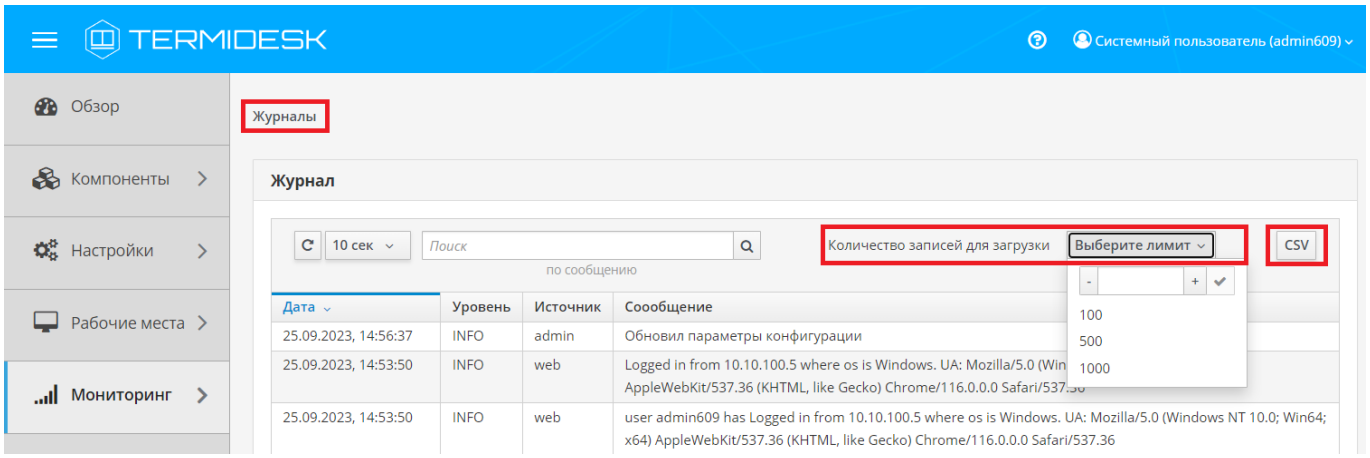


Рисунок 38 – Отображение общего журнала в графическом интерфейсе управления Termidesk

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

При помощи экранной кнопки [CSV] (см. Рисунок 39) можно выгрузить в csv-файл весь представленный журнал событий, либо строки событий.

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

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

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

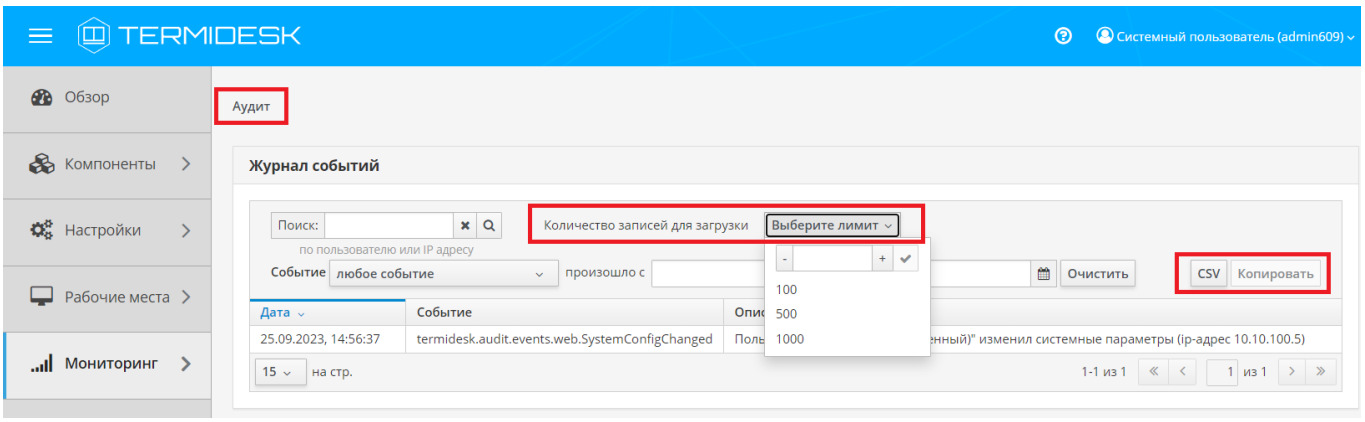


Рисунок 39 – Отображение журнала аудита в графическом интерфейсе управления Termidesk

### 14.5 . Просмотр централизованных журналов фермы

Для просмотра централизованных журналов событий, связанного с функционированием фермы Termidesk, следует перейти «Мониторинг - Журналы фермы», где визуализируются события из «Хранилища журналов».

> Ферма Termidesk - логическое объединение узлов Termidesk, взаимодействующих с одной БД.

Для отображения событий нужно убедиться, что:

- добавлен и настроен «Ретранслятор» согласно подразделам **Добавление «Ретранслятора»** и **Настройка узла «Ретранслятора»**;
- добавлено «Хранилище журналов» согласно подразделу **Управление «Хранилищами журналов»**.

По умолчанию записи событий представлены в табличном виде и упорядочены согласно столбцу «Время». Основные параметры списка приведены в таблице (см. Таблица 62).

Таблица 62 – Основные параметры списка событий централизованного журнала

| Параметр | Описание |
|---|---|
| «Время» | Время регистрации события |
| «Источник» | Системный UUID узла, который зарегистрировал событие |
| «Тип» | Тип портала, который зарегистрировал событие.<br>Может быть: «admin» («Портал администратора»), «user» («Портал пользователя»), «universal» («Портал универсальный») |
| «Уровень» | Категория сообщения.<br>Возможные значения:«INFO», «DEBUG», «ERROR» |
| «Модуль» | Служба Termidesk, которая зарегистрировала событие |
| «Сообщение» | Подробное описание события |

### 14.6 . Описание шаблонов событий аудита

#### 14.6.1 . Типы данных регистрируемой информации событий аудита

При фиксации событий аудита используется ряд типов данных (см. Таблица 63) регистрируемой информации, состав которых может отличаться для разных событий.

Таблица 63 – Типы данных регистрируемой информации

| Тип данных | Описание |
|---|---|
| Дата/время | Дата и время указываются в формате: `DD.MM.YYYY, hh:mm:ss`, где:<br>`DD.MM.YYYY` обозначает «день» - «месяц» - «год»;<br>`hh:mm:ss` обозначает элементы времени «час» - «минута» - «секунда»;<br>«.» и «:» используются как разделители в обозначениях даты и времени дня соответственно |

| Тип данных | Описание |
|---|---|
| Имя/логин | Идентификационные данные субъекта, совершающего доступ к объекту |
| Наименование параметра/секции/политики | Указывает объект, над которым производится действие |
| Значение | Указывается значение, которое принимал или принял объект после выполнения над ним операции |
| Тип объекта/сущности | Указывает тип объекта, над которым производится действие |
| Действие | Название операции, которую совершил субъект над объектом |
| Уровень важности | Показатель критичности события |
| Идентификатор | Указывают уникальную (для соответствующего объекта) последовательность чисел для его однозначной идентификации |
| IP-адрес | 32-битовое число. Формой записи IP-адреса является запись в виде четырех десятичных чисел значением от 0 до 255, разделенных точками (например, 192.0.2.1) |

### 14.6.2 . Типы и шаблоны регистрируемых событий аудита

Список регистрируемых событий и шаблоны к ним приведены в таблице (см. Таблица 64).

Таблица 64 – Список типов и шаблонов регистрируемых событий аудита

| Наименование события | Состав регистрируемой информации | Шаблон регистрации события |
|---|---|---|
| **События, связанные с командной строкой** | | |
| Изменение системных параметров «Универсального диспетчера» через командную строку<br>`cli.SystemConfigChanged` | Регистрируется:<br>▪ логин пользователя (`username`);<br>▪ название секции (`section_name`);<br>▪ название изменяемого параметра; (`parameter_key`);<br>▪ новое значение параметра (`parameter_value`) | «Пользователь `"[username]"` изменил системный параметр `[section_name].[parameter_key]=[parameter_value]`» |
| CRU- операции с объектами через командную строку<br>`cli.EntityAction` | Регистрируется:<br>▪ имя системного пользователя, запустившего команду (`username`);<br>▪ тип сущности (`entity`);<br>▪ уникальный идентификатор (`uuid`);<br>▪ тип объекта (`subtype`);<br>▪ название объекта (`name`);<br>▪ действие над объектом (`action`) | «Пользователь `"[username]"` выполнил операцию `[action]` для объекта `[entity] ([uuid]) [subtype] "[name]"`» |
| Вход пользователя в систему через командную строку<br>`cli.UserLogin` | Регистрируется:<br>▪ наименование домена аутентификации (`authenticator`);<br>▪ логин пользователя (`username`);<br>▪ тип портала (`portal`);<br>▪ идентификатор портала (`portal_uuid`) | «Пользователь `"[username] ([authenticator])"` вошел в систему через `[portal] ([portal_uuid])`» |
| Выход пользователя из системы через командную строку<br>`cli.UserLogout` | Регистрируется:<br>▪ наименование домена аутентификации (`authenticator`);<br>▪ логин пользователя (`username`);<br>▪ тип портала (`portal`);<br>▪ идентификатор портала (`portal_uuid`) | «Пользователь `"[username] ([authenticator])"` вышел из системы через `[portal] ([portal_uuid])`» |
| **События, связанные с политиками** | | |

| | | |
|---|---|---|
| Изменение глобальных политик<br>`policies.GlobalPolicyChanged` | Регистрируется:<br>▪ имя пользователя (`username`);<br>▪ название домена аутентификации пользователя (`authenticator_name`);<br>▪ название политики (`policy_name`);<br>▪ новое значение в дружественном к пользователю описании (`value`);<br>▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`);<br>▪ новое значение в оригинальном формате (`value_raw`) | «Пользователь `"[username] ([authenticator_name])"` изменил значение глобальной политики `"[policy_name]"` на `"[value]"`» |
| Изменение политик РМ<br>`policies.DeployedServicePolicyChanged` | Регистрируется:<br>▪ имя пользователя (`username`);<br>▪ название домена аутентификации пользователя (`authenticator_name`);<br>▪ название политики (`policy_name`);<br>▪ название фонда РМ (`deployed_service_name`);<br>▪ новое значение в дружественном к пользователю описании (`value`);<br>▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`);<br>▪ идентификатор фонда РМ (`deployed_service_uuid`);<br>▪ новое значение в оригинальном формате (`value_raw`) | «Пользователь `"[username] ([authenticator_name])"` изменил значение политики `"[policy_name]"` для фонда `"[deployed_service_name]"`на `"[value]"`» |
| Сброс политики РМ<br>`policies.DeployedServicePolicyDeleted` | Регистрируется:<br>▪ имя пользователя (`username`);<br>▪ название домена аутентификации пользователя (`authenticator_name`);<br>▪ название политики (`policy_name`);<br>▪ название фонда РМ (`deployed_service_name`);<br>▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`);<br>▪ идентификатор фонда РМ (`deployed_service_uuid`) | «Пользователь `"[username] ([authenticator_name])"` сбросил значение политики `"[policy_name]"` для фонда `"[deployed_service_name]"`» |
| Сброс глобальных политик<br>`policies.GlobalPolicyDeleted` | Регистрируется:<br>▪ имя пользователя (`username`);<br>▪ название домена аутентификации пользователя (`authenticator_name`);<br>▪ название политики (`policy_name`);<br>▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`) | «Пользователь `"[username] ([authenticator_name])"` сбросил значение глобальной политики `"[policy_name]"`» |
| **События, связанные с пользователем** | | |
| Подключение пользователя к РМ<br>`workplace.UserConnected` | Регистрируется:<br>▪ название домена аутентификации пользователя (`authenticator`);<br>▪ логин пользователя (`username`);<br>▪ имя фонда РМ (`workplace`);<br>▪ имя выданной ВМ (`vm_name`);<br>▪ IP-адрес выданной ВМ (`vm_ip`);<br>▪ протокол доставки (`transport`) | «К рабочему месту `[vm_name]([vm_ip])` фонда `[workplace]` пользователя `"[username] ([authenticator])"` произведено подключение с помощью протокола `[transport]`» |

| | | |
|---|---|---|
| Отключение пользователя от РМ<br>workplace.UserDisconnected | Регистрируется:<br>▪ название домена аутентификации пользователя (authenticator);<br>▪ логин пользователя (username);<br>▪ имя фонда РМ (workplace);<br>▪ имя выданной ВМ (vm_name);<br>▪ IP-адрес выданной ВМ (vm_ip);<br>▪ протокол доставки (transport) | «Подключение к рабочему месту [vm_name]([vm_ip]) фонда [workplace] пользователя "[username] ([authenticator])" по протоколу [transport] разорвано» |
| Вход пользователя в ОС РМ<br>workplace.UserLogin | Регистрируется:<br>▪ название домена аутентификации пользователя (authenticator);<br>▪ Логин пользователя (username);<br>▪ имя пользователя совершающего вход в гостевую ОС ВМ (guest_os_username);<br>▪ IP-адрес, с которого был сделан запрос (ip);<br>▪ имя фонда РМ (workplace);<br>▪ имя выданной ВМ (vm_name);<br>▪ IP-адрес выданной ВМ (vm_ip) | «Пользователь "[username] ([authenticator])" вошел в гостевую ОС ВМ [vm_name] ([vm_ip]) фонда [workplace] как пользователь [guest_os_username] с ip-адреса [ip]» |
| Выход пользователя из ОС ВМ<br>workplace.UserLogout | Регистрируется:<br>▪ название домена аутентификации пользователя (authenticator);<br>▪ логин пользователя (username);<br>▪ имя пользователя совершающего вход в гостевую ОС ВМ (guest_os_username);<br>▪ IP-адрес, с которого был сделан запрос (ip);<br>▪ имя фонда РМ (workplace);<br>▪ имя выданной ВМ (vm_name);<br>▪ IP-адрес выданной ВМ (vm_ip) | «Пользователь "[username] ([authenticator])" вышел из гостевой ОС ВМ [vm_name] ([vm_ip]) фонда [workplace] как пользователь [guest_os_username] с ip-адреса [ip]» |
| Блокировка РМ<br>workplace.UserLock | Регистрируется:<br>▪ название домена аутентификации пользователя (authenticator);<br>▪ логин пользователя (username);<br>▪ имя пользователя совершающего выход из гостевой ОС ВМ (guest_os_username);<br>▪ IP-адрес, с которого был сделан запрос (ip);<br>▪ имя фонда РМ (workplace);<br>▪ имя выданной ВМ (vm_name);<br>▪ IP-адрес выданной ВМ (vm_ip) | «Пользователь "[username] ([authenticator])" заблокировал гостевую ОС ВМ [vm_name] ([vm_ip]) фонда [workplace] как пользователь [guest_os_username]» |
| Разблокировка РМ<br>workplace.UserUnlock | Регистрируется:<br>▪ название домена аутентификации пользователя (authenticator);<br>▪ логин пользователя (username);<br>▪ имя пользователя совершающего выход из гостевой ОС ВМ (guest_os_username);<br>▪ IP-адрес, с которого был сделан запрос (ip);<br>▪ имя фонда РМ (workplace);<br>▪ имя выданной ВМ (vm_name);<br>▪ IP-адрес выданной ВМ (vm_ip) | «Пользователь "[username] ([authenticator])" разблокировал гостевую ОС ВМ [vm_name] ([vm_ip]) фонда [workplace] как пользователь [guest_os_username]» |

| | | |
|---|---|---|
| Пользователь неактивен<br>`workplace.UserIdle` | Регистрируется:<br>▪ название домена аутентификации пользователя (`authenticator`);<br>▪ логин пользователя (`username`);<br>▪ имя пользователя совершающего выход из гостевой ОС ВМ (`guest_os_username`);<br>▪ IP-адрес, с которого был сделан запрос (`ip`);<br>▪ имя фонда РМ (`workplace`);<br>▪ имя выданной ВМ (`vm_name`);<br>▪ IP-адрес выданной ВМ (`vm_ip`) | «Пользователь `"[username] ([authenticator])"` неактивен в гостевой ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]`» |
| Пользователь активен<br>`workplace.UserActive` | Регистрируется:<br>▪ название домена аутентификации пользователя (`authenticator`);<br>▪ логин пользователя (`username`);<br>▪ имя пользователя совершающего выход из гостевой ОС ВМ (`guest_os_username`);<br>▪ IP-адрес, с которого был сделан запрос (`ip`);<br>▪ имя фонда РМ (`workplace`);<br>▪ имя выданной ВМ (`vm_name`);<br>▪ IP-адрес выданной ВМ (`vm_ip`) | «Пользователь `"[username] ([authenticator])"` вновь активен в гостевой ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]`» |
| Подключение пользователя к РМ и начало работы<br>`user.WorkplaceConnectionRequest` | Регистрируется:<br>▪ название домена аутентификации пользователя (`authenticator`);<br>▪ логин пользователя (`username`);<br>▪ IP-адрес, с которого был сделан запрос (`ip`);<br>▪ название фонда РМ (`workplace`);<br>▪ имя выданной ВМ (`vm_name`);<br>▪ название протокола доставки (`transport`) | «Пользователь `"[username] ([authenticator])"` подключился к ВМ `[vm_name]` фонда `[workplace]` по протоколу `[transport]` с ip-адреса `[ip]`» |
| Отправка сообщения в РМ<br>`user.WorkplaceMessageSent` | Регистрируется:<br>▪ название домена аутентификации пользователя (`authenticator`);<br>▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`);<br>▪ имя пользователя (`username`);<br>▪ название фонда РМ (`deployed_service_name`);<br>▪ идентификатор фонда РМ (`deployed_service_uuid`);<br>▪ название РМ (`user_service_name`);<br>▪ идентификатор РМ (`user_service_uuid`);<br>▪ тип сообщения (`msg_level`);<br>▪ текст сообщения (`msg_text`) | «Пользователь `[username] ([authenticator])` отправил сообщение `"[msg_text]"` уровня `[msg_level]` на рабочее место `[user_service_name]` фонда `[deployed_service_name]`» |
| Назначение пользователя на РМ<br>`workplace.UserAssigned` | Регистрируется:<br>▪ логин пользователя (`username`);<br>▪ назначенный пользователь (`assigned_to`);<br>▪ кем назначен пользователь (`assigned_by`);<br>▪ время назначения (`assignment_time`) | «Пользователь `"[username]"` назначен на рабочее место `"[assigned_to]"` пользователем `"[assigned_by]"`» |
| **События, связанные с веб-интерфейсом** | | |

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

| | | |
|---|---|---|
| Попытка повышения прав<br>`web.AdminAssigned` | Регистрируется:<br>▪ логин пользователя (`user`);<br>▪ пользователь, которому назначаются права (`user1`);<br>▪ название домена аутентификации пользователя (`authenticator`)<br>:param username: Логин пользователя - args[0]<br>:param assigned_to: Пользователь, которому назначаются права - args[1]<br>:param auth_domain: Домен аутентификации - args[2] | «Пользователь "`[user]`" попытался установить тип учетной записи "Администратор" для пользователя "`[user1]`" в домене аутентификации "`[authenticator]`"» |
| **События, связанные с разными API** | | |
| Вход пользователя в систему через API<br>`api.UserLogin` | Регистрируется:<br>▪ название домена аутентификации пользователя (`authenticator`);<br>▪ логин пользователя (`username`);<br>▪ IP-адрес, с которого был сделан запрос (`ip`);<br>▪ тип портала (`portal`);<br>▪ идентификатор портала (`portal_uuid`) | «Пользователь "`[username]` (`[authenticator]`)" вошел в систему с ip-адреса `[ip]`через `[portal]` (`[portal_uuid]`)» |
| Выход пользователя из системы через API<br>`api.UserLogout` | ▪ название домена аутентификации пользователя (`authenticator`);<br>▪ логин пользователя (`username`);<br>▪ IP-адрес, с которого был сделан запрос (`ip`);<br>▪ тип портала (`portal`);<br>▪ идентификатор портала (`portal_uuid`) | «Пользователь "`[username]` (`[authenticator]`)" вышел из системы с ip-адреса `[ip]` через `[portal]` (`[portal_uuid]`)» |

### 14.6.3 . Форматы регистрируемых событий аудита и их примеры

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

Пример регистрации события аудита «Изменение системных параметров «Универсального диспетчера»:

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

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

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

Пример регистрации события аудита «Пользователь неактивен»:

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

### 14.7 . Отслеживание жизненного цикла сессий и ресурсов пользователей

Начиная с Termidesk версии 5.0 поддерживается возможность отследить действия пользователя (или администратора) по идентификаторам, которыми маркируются все события, относящихся к работе с Termidesk с момента аутентификации и до завершения работы:

- глобальный уникальный сессионный идентификатор (Global Unique Session ID, GUSID, ГУСИ) - позволяет однозначно сопоставить субъект (пользователя или администратора) и производимые им действия. Присваивается в момент аутентификации в Termidesk;
- уникальный идентификатор запуска ресурса (Unique Resource Start ID, URSI) - позволяет однозначно сопоставить пользователя и конкретный ресурс, который он получает - РМ и/или приложение. Присваивается в момент запуска пользователем ресурса.

Последовательность присвоения и отправки идентификаторов представлена на рисунке.

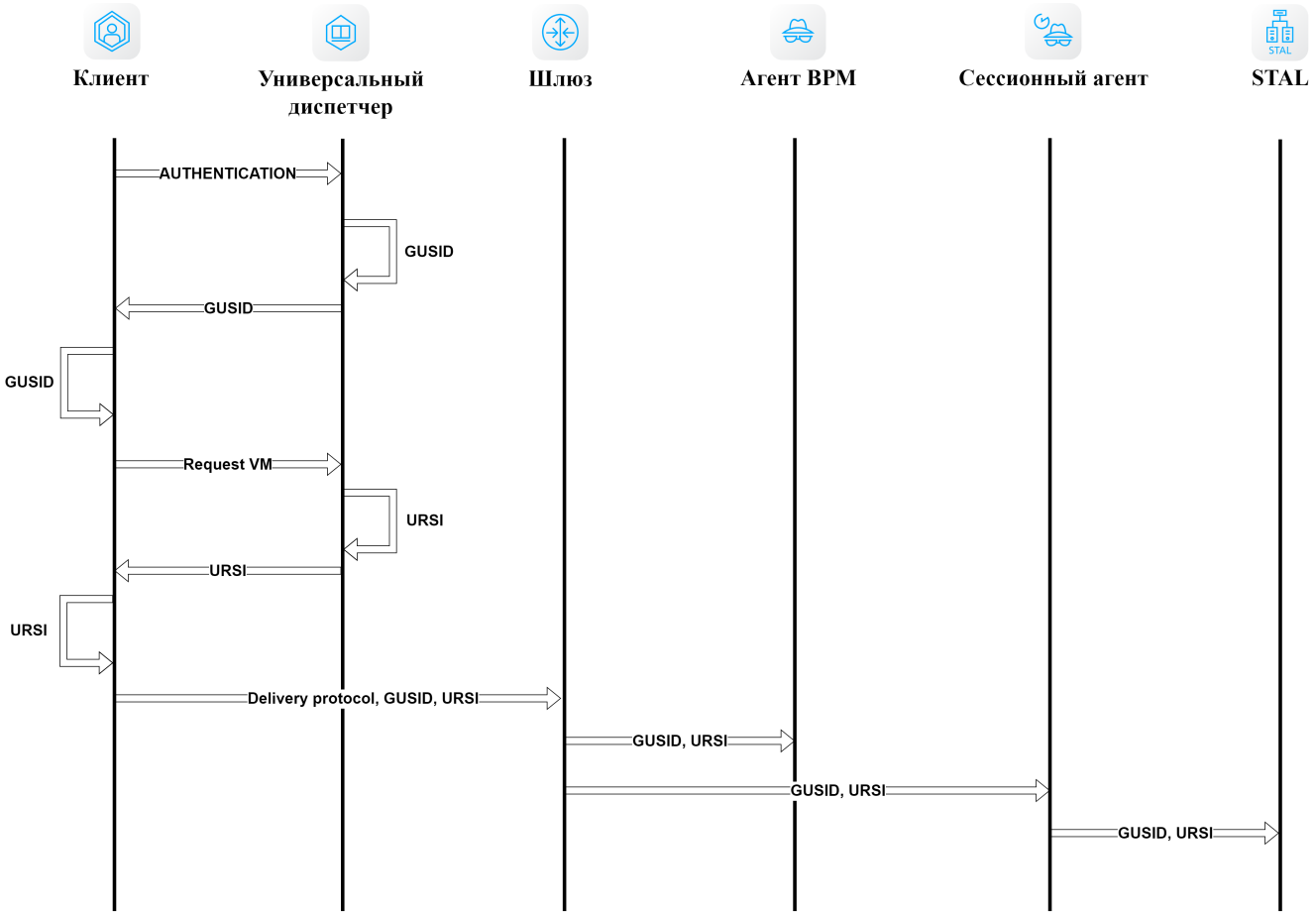


Рисунок 40 – Последовательность присвоения и отправки GUSID и URSI

Аннулирование GUSID происходит при:

- завершении сессии по истечении времени, заданного параметром «Длительность сессии пользователя» или «Длительность сессии администратора» (см. подраздел **Параметры безопасности Termidesk**);

- отключении от «Универсального диспетчера»;
- закрытии компонента «Клиент» пользователем;
- запуске нового экземпляра компонента «Клиент» на той же пользовательской рабочей станции;
- невозможности восстановления подключения после обрыва связи - GUSID и URSI будут считаться недействительными и при следующем подключении к «Универсальному диспетчеру» будут назначены новые идентификаторы.

Аннулирование URSI происходит при:

- закрытии пользователем окна опубликованного приложения или выходе из сеанса PM (`logoff`);
- отключении от сеанса PM (`disconnect`);
- закрытии компонента «Клиент» и окна программы доставки PM (`termidesk-viewer`);
- невозможности восстановления подключения после обрыва связи - GUSID и URSI будут считаться недействительными и при следующем подключении пользователя к «Универсальному диспетчеру» будут назначены новые идентификаторы

GUSID и URSI регистрируются в журналах:

- компонента «Сессионный агент»;
- компонента «Агент виртуального рабочего места».

События, связанные с GUSID и URSI, хранятся в БД. Они доступны для просмотра в журнале на портале Termidesk (см. подраздел **Просмотр журналов**). Пример сообщения от источника «agent»: «preConnect. User: u, Protocol: spice, GUSID: 93418bcd-5c95-5f46-ae1b-980a8519ae8f, URSI: 73fe89e3-5fe4-5b02-81a8-06b8e3bac2d1».

# 15 . УПРАВЛЕНИЕ ИНФРАСТРУКТУРОЙ TERMIDESK

## 15.1 . Общие сведения об инфраструктуре Termidesk

Раздел «Инфраструктура» предназначен для использования в качестве единого центра управления при распределенной установке Termidesk. Он позволяет централизованно управлять компонентами и просматривать их статус на сервере.

Просмотр компонентов и их состояния также доступен в разделе «Обзор» (см. Рисунок 41), наименования элементов в котором служат активной ссылкой на соответствующий подраздел веб-интерфейса.

Состояние компонента визуализируется пиктограммой:

-  - количество узлов, находящихся в статусе «ok», которое вернул запрос `healthcheck`;
-  - количество узлов, находящихся в статусе «maintance» (техобслуживание), которое вернул запрос `healthcheck`;
-  - количество узлов, находящихся в статусе «error» (ошибка), которое вернул запрос `healthcheck`;
-  - количество узлов, находящихся в статусе «unknown» (неизвестно). Статус появляется, если после регистрации компонента еще не было ни одной попытки запроса состояния `healthcheck`.

По умолчанию запрос состояния компонентов производится с интервалом 60 секунд.

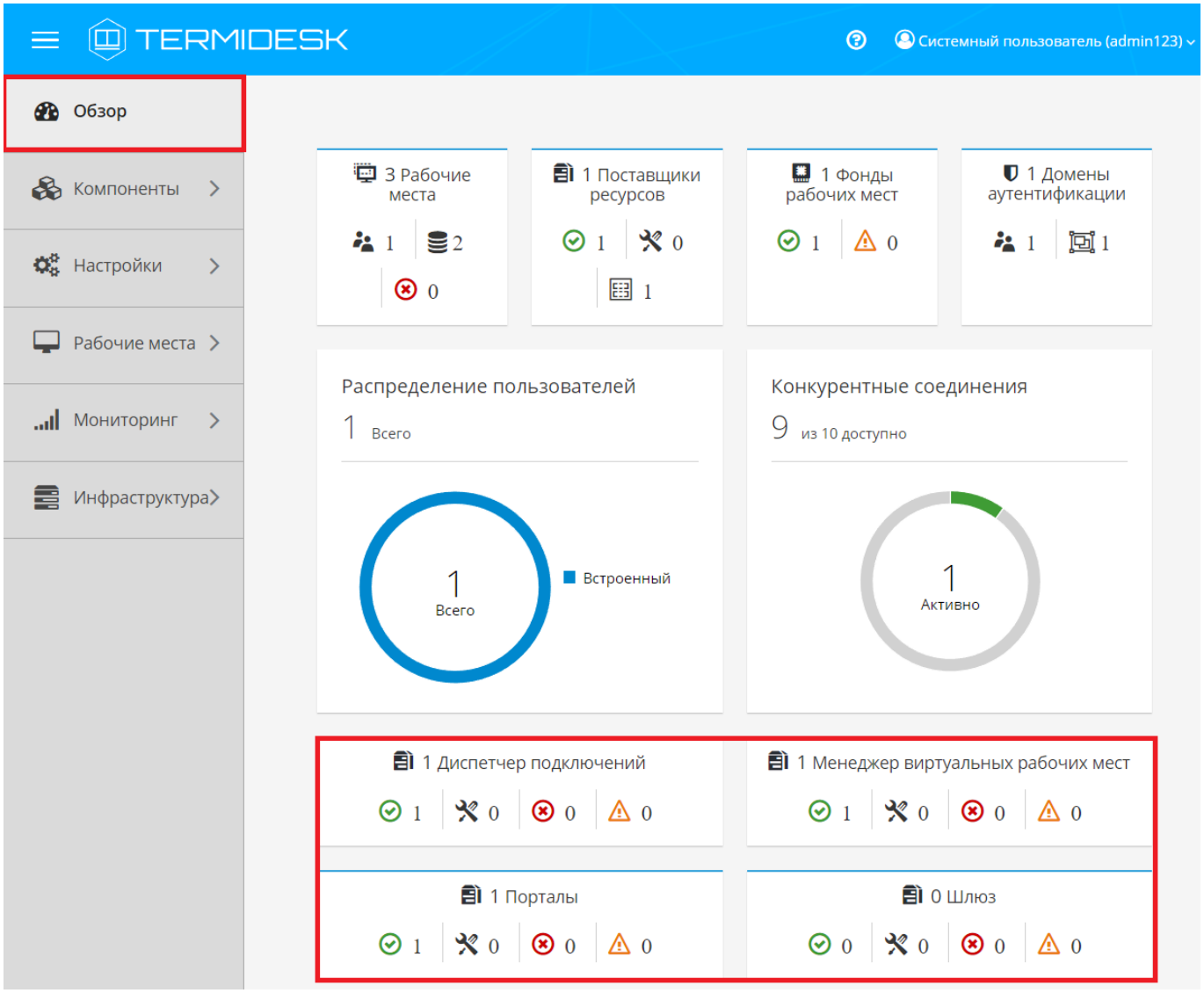


Рисунок 41 – Отображение компонентов в разделе «Обзор»

Регистрация компонента Termidesk в системе происходит через подключение к серверу RabbitMQ, передающему информацию об узле компоненту «Менеджер рабочих мест» (`termidesk-taskman`) для обработки и добавления в таблицу раздела «Инфраструктура». Регистрация компонентов происходит при их запуске.

### 15.2 . Управление списком узлов компонента «Универсальный диспетчер»

Для получения списка зарегистрированных узлов компонента «Универсальный диспетчер» нужно перейти «Инфраструктура - Диспетчеры подключений».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя». Для удаления узла компонента из таблицы следует выбрать нужный объект и нажать экранную кнопку **[Удалить]**.

Удаление объекта из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова.

Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».
Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

Основные регистрируемые параметры узлов приведены в таблице (см. Таблица 65).

Таблица 65 – Основные параметры списка узлов компонента «Универсальный диспетчер»

| Параметр | Описание |
|---|---|
| «Имя» | Наименование объекта |
| «Статус» | Текущее состояние, может принимать значения:<br>▪ «ok» - объект нормально функционирует;<br>▪ «failed» - объект функционирует с ошибками;<br>▪ «unknown» - состояние неизвестно или не поддерживается |
| «Полное доменное имя» | Полное доменное имя узла объекта |
| «IP адрес(а)» | Список IP-адресов на узле объекта |
| «Изменено кем» | Наименование субъекта, который внес последние изменения |
| «Дата изменения» | Дата внесения последних изменений |
| «Создано кем» | Наименование субъекта, который создал объект |
| «Дата создания» | Дата создания записи в таблице об объекте |
| «UID ноды» | Системный UUID узла объекта |
| «Уникальный номер» | Уникальный идентификатор объекта |

### 15.3 . Управление списком узлов компонента «Менеджер рабочих мест»

Для получения списка зарегистрированных узлов компонента «Менеджер рабочих мест» нужно перейти «Инфраструктура - Менеджеры BPM».
По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя».
Для удаления узла компонента из таблицы следует выбрать нужный объект и нажать экранную кнопку **[Удалить]**.

Удаление объекта из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова.

Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».

Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

Основные регистрируемые параметры узлов приведены в таблице (см. Таблица 66).

Таблица 66 – Основные параметры списка узлов компонента «Менеджер рабочих мест»

| Параметр | Описание |
|---|---|
| «Имя» | Наименование объекта |
| «Статус» | Текущее состояние, может принимать значения:<br>▪ «ok» - объект нормально функционирует;<br>▪ «failed» - объект функционирует с ошибками;<br>▪ «unknown» - состояние неизвестно или не поддерживается |
| «Полное доменное имя» | Полное доменное имя узла объекта |
| «IP адрес(а)» | Список IP-адресов на узле объекта |
| «Изменено кем» | Наименование субъекта, который внес последние изменения |
| «Дата изменения» | Дата внесения последних изменений |
| «Создано кем» | Наименование субъекта, который создал объект |
| «Дата создания» | Дата создания записи в таблице об объекте |
| «UID ноды» | Системный UUID узла объекта |
| «Уникальный номер» | Уникальный идентификатор объекта |

### 15.4 . Управление списком узлов с ролями «Порталов»

Для получения списка зарегистрированных узлов с ролями «Порталов» нужно перейти «Инфраструктура - Порталы».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя».

Для удаления узла компонента из таблицы следует выбрать нужный объект и нажать экранную кнопку **[Удалить]**.

Удаление объекта из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова.

Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».
Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

Основные регистрируемые параметры узлов приведены в таблице (см. Таблица 67).

Таблица 67 – Основные параметры списка узлов с ролями «Порталов»

| Параметр | Описание |
|---|---|
| «Имя» | Наименование объекта |
| «Роль» | Тип портала, с которым установлен компонент «Универсальный диспетчер».<br>Может быть: «admin» («Портал администратора»), «user» («Портал пользователя»), «universal» («Портал универсальный») |
| «Статус» | Текущее состояние, может принимать значения:<br>▪ «ok» - объект нормально функционирует;<br>▪ «failed» - объект функционирует с ошибками;<br>▪ «unknown» - состояние неизвестно или не поддерживается |
| «Полное доменное имя» | Полное доменное имя узла объекта |
| «IP адрес(а)» | Список IP-адресов на узле объекта |
| «Изменено кем» | Наименование субъекта, который внес последние изменения |
| «Дата изменения» | Дата внесения последних изменений |
| «Создано кем» | Наименование субъекта, который создал объект |
| «Дата создания» | Дата создания записи в таблице об объекте |
| «UID ноды» | Системный UUID узла объекта |
| «Уникальный номер» | Уникальный идентификатор объекта |

### 15.5 . Управление списком узлов компонента «Шлюз»

Для получения списка зарегистрированных узлов компонента «Шлюз» нужно перейти «Инфраструктура - Шлюзы».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя». Для удаления узла компонента из таблицы следует выбрать нужный объект и нажать экранную кнопку **[Удалить]**.

Удаление объекта из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова.

Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».
Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

Основные регистрируемые параметры узлов приведены в таблице (см. Таблица 68).

Таблица 68 – Основные параметры списка узлов компонента «Шлюз»

| Параметр | Описание |
|---|---|
| «Имя» | Наименование объекта |

| Параметр | Описание |
|---|---|
| «Статус» | Текущее состояние, может принимать значения:<br>▪ «ok» - объект нормально функционирует;<br>▪ «failed» - объект функционирует с ошибками;<br>▪ «unknown» - состояние неизвестно или не поддерживается |
| «Полное доменное имя» | Полное доменное имя узла объекта |
| «IP адрес(а)» | Список IP-адресов на узле объекта |
| «Изменено кем» | Наименование субъекта, который внес последние изменения |
| «Дата изменения» | Дата внесения последних изменений |
| «Создано кем» | Наименование субъекта, который создал объект |
| «Дата создания» | Дата создания записи в таблице об объекте |
| «UID ноды» | Системный UUID узла объекта |
| «Уникальный номер» | Уникальный идентификатор объекта |

## 15.6 . Управление «Ретрансляторами»

### 15.6.1 . Добавление «Ретранслятора»

«Ретранслятор» - узел с установленным ПО Fluentd, предназначенный для сбора и фильтрации записей журналов, поступающих от компонентов Termidesk, и их перенаправления в централизованное хранилище журналов или БД.

Для отображения списка «Ретрансляторов» следует перейти «Инфраструктура - Ретрансляторы». По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 69).

Таблица 69 – Основные параметры списка «Ретрансляторов»

| Параметр | Описание |
|---|---|
| «Имя» | Наименование объекта |
| «Статус» | Текущее состояние объекта, может принимать значения:<br>▪ «ok» - объект нормально функционирует;<br>▪ «failed» - объект функционирует с ошибками;<br>▪ «unknown» - состояние неизвестно или не поддерживается |
| «Используется» | Флаг использования объекта.<br>Возможные значения:<br>▪ «Да» - «Ретранслятор» используется для сбора журналов;<br>▪ «Нет» - «Ретранслятор» не используется для сбора журналов |
| «Полное доменное имя» | Полное доменное имя узла, на котором функционирует «Ретранслятор» |
| «IP-адрес(а)» | Список IP-адресов на узле, на котором функционирует «Ретранслятор» |
| «Изменено кем» | Наименование субъекта, который внес последние изменения |
| «Дата изменения» | Дата внесения последних изменений |

| Параметр | Описание |
|---|---|
| «Создано кем» | Наименование субъекта, который создал объект |
| «Дата создания» | Дата создания записи в таблице об объекте |
| «UUID ноды» | Системный UUID узла, на котором функционирует «Ретранслятор»<br>Параметр имеет постоянное значение: «00000000-0000-0000-0000-000000000000» |
| «Уникальный номер» | Уникальный идентификатор объекта |

Для добавления «Ретранслятора» нужно перейти «Инфраструктура - Ретрансляторы» и нажать экранную кнопку **[Создать]**. Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 70).

В Termidesk версии 5.1 рекомендуется добавлять только один узел «Ретранслятора». В отличие от компонентов Termidesk, которые регистрируются в разделе «Инфраструктура» автоматически, «Ретранслятор» добавляется вручную.

Таблица 70 – Данные для добавления узла «Ретранслятора»

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование «Ретранслятора» |
| «IP адрес» | IP-адрес «Ретранслятора» |
| «Порт» | Порт, который будет использоваться при подключении к «Ретранслятору».<br>Значение по умолчанию: «24224» |
| «Альтернативный порт» | Дополнительный порт, который будет использоваться при подключении к «Ретранслятору».<br>Значение по умолчанию: «9880» |
| «Включено» | Управление использованием «Ретранслятора».<br>Возможные значения:<br>▪ «Да» - использовать «Ретранслятор» для сбора журналов;<br>▪ «Нет» - не использовать «Ретранслятор» для сбора журналов.<br>Параметр предназначен для прекращения взаимодействия компонентов Termidesk с узлом «Ретранслятора», который по каким-либо причинам выведен из стандартного рабочего состояния |

Над созданными «Ретрансляторами» можно выполнять следующие действия:

- редактировать, для этого следует выбрать нужный объект в таблице, а затем нажать экранную кнопку **[Изменить]**;
- удалить, для этого следует выбрать нужный объект в таблице, а затем нажать экранную кнопку **[Удалить];**
- управлять состоянием, для этого следует выбрать нужный объект в таблице, нажать экранную кнопку **[Использование]** и в раскрывающемся списке выбрать состояние «Ретранслятора»:

- «Использовать»;
- «Не использовать».

⚠ Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».
Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

### 15.6.2 . Настройка узла «Ретранслятора»

Для централизованного сбора событий в «Хранилище журналов» необходимо настроить отдельный узел с установленным ПО Fluentd и СУБД PostgreSQL, выступающей в качестве «Хранилища журналов» (в общем случае данные компоненты могут устанавливаться на отдельный узел, но в рамках настоящей процедуры этот вариант не рассматривается). Для этого на узле «Ретранслятора» нужно создать и настроить БД «Хранилища журналов»:

- переключиться на пользователя `postgres`:

```
sudo su postgres
```

- запустить терминальный клиент СУБД PostgreSQL:

```
psql
```

ⓘ Если после выполнения команды отображается ошибка «could not change directory to "/home/": Отказано в доступе» и не появляется приглашение командной строки `postgres=#`, необходимо вместо «`su postgres`» использовать конструкцию «`su - postgres`». Если приглашение `postgres=#` появилось, то сообщение об ошибке можно проингорировать.

- используя интерактивный интерфейс терминального клиента СУБД, создать БД `fluentd_logs_db` (символ ; в конце строки при работе с интерактивным интерфейсом обязателен):

```
postgres=# CREATE DATABASE fluentd_logs_db;
```

- создать пользователя `fluentd` с паролем `tufotukur` для дальнейшего подключения к БД:

```
postgres=# CREATE USER fluentd WITH PASSWORD 'tufotukur';
```

⚠ В приведенной команде имя пользователя и пароль используются в качестве примера. Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты. Для задания пароля разрешено использовать только латинские буквы A-Z, a-z, цифры 0-9 и символы $!@%^&#_-=+~`;:.,?()*{}[]\/.

- назначить права по использованию БД `fluentd_logs_db` созданному пользователю `fluentd`:

```
postgres=# GRANT ALL PRIVILEGES ON DATABASE fluentd_logs_db TO fluentd;
```

- подключиться к БД `fluentd_logs_db`:

```
postgres=# \c fluentd_logs_db
```

- создать таблицу `logs`:

⚠ При использовании СУБД PostgreSQL версии выше 11 могут понадобиться права на создание объектов для схемы `public`. Для предоставления прав на создание объектов схемы нужно выполнить команду:

```
postgres=# GRANT CREATE ON SCHEMA public TO fluentd;
```

```
postgres=# CREATE TABLE logs (
    id SERIAL PRIMARY KEY,
    time timestamp with time zone NOT NULL,
    source VARCHAR(255) NOT NULL,
    "sourceType" VARCHAR(255) NOT NULL,
    loglevel VARCHAR(255) NOT NULL,
    module VARCHAR(255) NOT NULL,
    message TEXT NOT NULL
);
```

- выйти из интерактивного интерфейса терминального клиента СУБД:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

После создания БД нужно создать и настроить «Ретранслятор»:

- установить ПО Fluentd на узел «Ретранслятора» согласно документации https://docs.fluentd.org/;

- установить плагины fluent-plugin-sql и pg, доступ по ссылкеhttps://github.com/fluent/fluent-plugin-sql;
- отредактировать файл `/etc/fluent/fluentd.conf`:

> ⚠ Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре организации.

```
<source>
  @type forward
  port 24224
  bind 0.0.0.0
</source>

<system>
  log_level debug
</system>

<match termidesk.*>
  @type sql
  host 192.0.2.33
  port 5433
  database fluentd_logs_db
  adapter postgresql
  username fluentd
  password tufotukur

  <table>
    logs
    column_mapping
"time:time,source:source,sourceType:sourceType,loglevel:loglevel,module:module,message:message"
  </table>
</match>
```

Перечень параметров, задающихся через файл, приведен в таблице (см. Таблица 71).

Таблица 71 – Параметры конфигурирования файла fluentd.conf

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| Секция `source` | | |
| `@type` | `forward` | Параметр менять не рекомендуется |
| `port` | `24224` | Порт прослушивания входящих событий |
| `bind` | `0.0.0.0` | IP-адрес прослушивания входящих событий |
| Секция `system` | | |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| log_level | debug | Категория служебных сообщений для журналирования событий ПО Fluentd.<br>Возможные значения:<br>▪ debug;<br>▪ info;<br>▪ warn;<br>▪ error |
| Секция match | | |
| @type | sql | Параметр менять не рекомендуется |
| host | 192.0.2.33 | IP-адрес или полное доменное имя БД для сохранения событий |
| port | 5433 | Порт подключения к БД для сохранения событий |
| database | fluentd_logs_db | Наименование БД для сохранения событий |
| adapter | postgresql | Параметр изменять не рекомендуется |
| username | fluend | Имя пользователя БД для подключения к ней |
| password | tufotukur | Пароль для подключения к БД |
| Секция table | | |
| logs | не задано | Наименование таблицы БД для сохранения событий |
| column_mapping | "time:time, source:source, sourceType:sourceType, loglevel:loglevel, module:module, message:message" | Параметр распределяет значения событий, полученных от фермы Termidesk в поля таблицы «logs» |

## 15.7 . Управление «Хранилищами журналов»

«Хранилище журналов» отображает список подключенных БД, в которые сохраняет события подключенный «Ретранслятор».

> ⓘ В Termidesk версии 5.1 функционал «Хранилища журналов» является экспериментальным. Поскольку предполагается использование одного узла «Ретранслятора» с одной БД, то компоненты Termidesk будут отправлять события на первый полностью работающий «Ретранслятор» и его БД.
> Записанные «Ретранслятором» события в БД доступны для просмотра в разделе «Мониторинг - Журналы фермы» (см. подраздел **Просмотр централизованных журналов фермы**).
> В отличие от компонентов Termidesk, регистрирующихся в разделе «Инфраструктура» автоматически, «Хранилище журналов» добавляется вручную.

Для отображения списка «Хранилищ журналов» нужно перейти «Инфраструктура - Хранилища журналов». По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Название».

Основные параметры списка приведены в таблице (см. Таблица 72).

Таблица 72 – Основные параметры списка «Хранилищ журналов»

| Параметр | Описание |
|---|---|
| «Название» | Наименование «Хранилища журналов» |
| «Используется» | Флаг использования «Хранилища журналов».<br>Возможные значения:<br>▪ «Да» - объект используется для сбора журналов;<br>▪ «Нет» - объект не используется для сбора журналов |

Для добавления «Хранилища журналов» следует перейти «Инфраструктура - Хранилища журналов» и нажать экранную кнопку **[Создать]**. Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 73).

Таблица 73 – Данные для добавления «Хранилища журналов»

| Параметр | Описание |
|---|---|
| «Имя журнала» | Текстовое наименование «Хранилища журналов» |
| «Имя БД» | Наименование БД, в которой расположено «Хранилище журналов» |
| «УЗ БД» | Имя пользователя для подключения к БД «Хранилища журналов».<br>Для обеспечения безопасного доступа к «Хранилищу журналов» рекомендуется создать учетные записи БД с нижеперечисленными ролями:<br>▪ «Администратора» - учетная запись должна обладать правами на создание учетных записей «Ретранслятора» и «Читателя», задание паролей, создание БД для хранения событий;<br>▪ «Ретранслятора» - учетная запись должна обладать правами на перенаправление событий из журналов компонентов Termidesk в БД «Хранилища журналов» и управление сроком хранения данных в БД;<br>▪ «Читателя» - учетная запись должна обладать правами на чтение данных из БД.<br>В текущей версии Termidesk для подключения к БД «Хранилища журналов» используется только учетная запись «Администратора» |
| «Пароль БД» | Пароль для подключения к БД «Хранилища журналов» |
| «IP-адрес БД» | IP-адрес узла с установленной БД «Хранилища журналов» |
| «Порт» | Порт для подключения к БД «Хранилища журналов».<br>Значение по умолчанию: «5432» |
| «Включено» | Управление использованием «Хранилища журналов».<br>Возможные значения:<br>▪ «Да» - использовать «Хранилище журналов» для сбора журналов;<br>▪ «Нет» - не использовать «Хранилище журналов» для сбора журналов.<br>Параметр предназначен для прекращения взаимодействия компонентов Termidesk с узлом «Хранилища журналов», который по каким-либо причинам выведен из стандартного рабочего состояния |
| «Максимальный размер (гб)» | Максимальный размер (в гигабайтах) «Хранилища журналов» |
| «Время хранения» | Время хранения (в днях) событий в «Хранилище журналов» |

Над созданными «Хранилищами журналов» можно выполнять следующие действия:

- редактировать, для этого следует выбрать нужный объект в таблице, а затем нажать экранную кнопку **[Изменить]**;
- удалить, для этого следует выбрать нужный объект в таблице, а затем нажать экранную кнопку **[Удалить];**
- управлять состоянием, для этого следует выбрать нужный объект в таблице, нажать экранную кнопку **[Использование]** и в раскрывающемся списке выбрать состояние «Хранилища журналов»:
  - «Использовать»;
  - «Не использовать».

⚠ Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».
Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

# 16 . РЕЖИМ ВЫСОКОЙ ДОСТУПНОСТИ И РАБОТА С СЕРТИФИКАТАМИ

## 16.1 . Настройка «Менеджера рабочего места» в режиме высокой доступности

Настройка выполняется после установки программного комплекса в распределенной конфигурации.

Последовательность настройки узлов с компонентом «Менеджер рабочих мест» 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):

```
1 sudo touch /etc/keepalived/keepalived.conf
2 sudo touch /etc/keepalived/notify.sh
```

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

⚠ Значения параметров в файле `keepalived.conf` приведены в качестве примера. Значения должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре организации.

```
1 global_defs {
2
```

```
    router_id NAME_OF_ROUTER_ID # НУЖНО УКАЗАТЬ: имя зоны маршрутизации VRRP
    script_user user # НУЖНО УКАЗАТЬ: вместо user -> 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
    # НУЖНО УКАЗАТЬ: 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).
    # НУЖНО УКАЗАТЬ: вместо 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.
    # НУЖНО УКАЗАТЬ: вместо 128 -> приоритет  экземпляра vrrp_instance
    priority 128

    preempt_delay 5 # Seconds

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

    # НУЖНО УКАЗАТЬ: вместо IP_ADDRESS_OF_THIS_HOST -> IPv4-адрес интерфейса, смотрящего в Интернет
    unicast_src_ip IP_ADDRESS_OF_THIS_HOST

    authentication {
        auth_type PASS
```

```
        # НУЖНО УКАЗАТЬ: ksedimret -> заменить на безопасный пароль
        auth_pass ksedimret
    }

    virtual_ipaddress {
        # НУЖНО УКАЗАТЬ: вместо VIRTUAL_IP_ADDREESS/MASK -> виртуальный IPv4-адрес и сетевой префикс с интерфейса, смотрящего в Интернет
        # НУЖНО УКАЗАТЬ: вместо eth0 -> интерфейс, смотрящий в Интернет
        # НУЖНО УКАЗАТЬ: вместо eth0:<значение> -> интерфейс, смотрящий в Интернет:4-й октет виртуального IPv4-адреса
        VIRTUAL_IP_ADDREESS/MASK dev eth0 label eth0:<значение>
    }

    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 узлов `master` и `slave`);

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

`VIRTUAL_IP_ADDRESS/MASK` - виртуальный статический IP-адрес и маска (общие для узлов `master` и `slave`);

`eth0:<значение>` - значение четвертого октета виртуального IPv4-адреса. Например, если используется виртуальный статический IP-адрес 192.0.2.30, то данный параметр примет значение `eth0:30`;

⚠ В рамках одной распределенной установки значение `NAME_OF_ROUTER_ID` параметра `router_id` должно быть идентичным. Если в сети или в одном VLAN присутствуют несколько распределенных установок Termidesk, то значение `NAME_OF_ROUTER_ID` параметра `router_id` должно быть уникальным для каждого экземпляра установки.

- 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 `keeaplived`

```
sudo systemctl enable keepalived
sudo systemctl start keepalived
```

### 16.2 . Настройка балансировщика для работы с самоподписанными сертификатами

#### 16.2.1 . Создание самоподписанного SSL-сертификата

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

- получить доступ к интерфейсу командной строки;

- выполнить генерацию SSL-сертификата (`/etc/ssl/certs/nginx-selfsigned.crt`) и ключа к нему (`/etc/ssl/private/nginx-selfsigned.key`):

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

Используемые ключи команды:

- `openssl` - базовый инструмент командной строки для создания и управления сертификатами, ключами и другими файлами OpenSSL;
- `req` - эта опция указывает, что на данном этапе нужно использовать запрос на подпись сертификата X.509 (CSR). X.509 – это стандарт инфраструктуры открытого ключа, которого придерживаются SSL и TLS при управлении ключами и сертификатами. Данная команда позволяет создать новый сертификат X.509;
- `new` - эта опция указывает, что будет создаваться новый запрос;
- `x509` - эта опция вносит поправку в предыдущую команду, сообщая утилите о том, что вместо запроса на подписание сертификата необходимо создать самоподписанный сертификат;
- `nodes` - ключ для пропуска опции защиты сертификата парольной фразой. Нужно, чтобы при запуске балансировщик нагрузки (nginx) имел возможность читать файл без вмешательства пользователя. Установив пароль, придется вводить его после каждой перезагрузки;
- `days 365` - эта опция устанавливает срок действия сертификата (в данном случае сертификат действителен в течение года);
- `newkey rsa:2048` - эта опция позволяет одновременно создать новый сертификат и новый ключ. Поскольку ключ, необходимый для подписания сертификата, не был создан ранее, нужно создать его вместе с сертификатом. Данная опция создаст RSA-ключ размером 2048 бит;
- `keyout` - эта опция сообщает OpenSSL, куда поместить сгенерированный файл ключа;
- `out` - эта опция сообщает OpenSSL, куда поместить созданный сертификат.

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

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

- `Email Address` [].

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

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

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

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

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

### 16.2.2 . Настройка nginx для поддержки SSL

Для настройки nginx нужно:

- создать новый пустой сниппет nginx в каталоге `/etc/nginx/snippets` для указания размещения сертификата и ключа:

```
sudo touch /etc/nginx/snippets/self-signed.conf
```

- отредактировать созданный файл, приведя его к виду:

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

- создать еще один пустой сниппет, предназначенный для настроек SSL (это позволит серверу nginx использовать надежный механизм преобразования и включит некоторые дополнительные функции безопасности):

```
sudo touch /etc/nginx/snippets/ssl-params.conf
```

- отредактировать созданный файл `ssl-params.conf`, приведя его к виду:

```
1 ssl_protocols TLSv1.3;
2 ssl_prefer_server_ciphers on;
3 ssl_dhparam /etc/nginx/dhparam.pem;
4 ssl_ciphers ECDHE-RSA-AES256-GCM-SHA512:DHE-RSA-AES256-GCM-SHA512:ECDHE-RSA-
  AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384;
5 ssl_ecdh_curve secp384r1; # Requires nginx >= 1.1.0
6 ssl_session_timeout  10m;
7 ssl_session_cache shared:SSL:10m;
```

```
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.

### 16.2.3 . Конфигурирование веб-сервера

Для конфигурирования веб-сервера нужно:

- создать пустой конфигурационный файл:

```
sudo touch /etc/nginx/sites-available/sampledomain.ru.conf
```

- отредактировать созданный файл, приведя его к виду:

⚠ Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре организации.

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

     server 192.0.2.41:5099;
     server 192.0.2.42:5099;
     server 192.0.2.43:5099;
     server 192.0.2.44:5099;

}

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

     server 192.0.2.30:443;
     server 192.0.2.31:443;
     server 192.0.2.32:443;
```

```
 }

server {
 listen 0.0.0.0:80;
 listen 0.0.0.0:443 ssl;

  include snippets/self-signed.conf;
  include snippets/ssl-params.conf;

 location /websockify {
         # limit_req zone=fast nodelay;
        proxy_http_version 1.1;
        proxy_pass http://daas-upstream-ws/;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";

        # Connection timeout
        proxy_connect_timeout 1000;
        proxy_send_timeout 1000;
        proxy_read_timeout 1000;
        send_timeout 1000;

        # Disable cache
        proxy_buffering off;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 }

 location / {
        proxy_pass https://daas-upstream-nodes/;

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

 }

}
```

⚠ IP-адреса, перечисленные в директиве `daas-upstream-ws`, являются адресами «Шлюзов» Termidesk, а IP-адреса, перечисленные в директиве `daas-upstream-nodes`, являются адресами «Универсальных диспетчеров» Termidesk.

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

```
sudo ln -s /etc/nginx/sites-available/sampledomain.ru.conf /etc/nginx/sites-enabled/
```

- проверить корректность настроек:

```
sudo nginx -t
```

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

⚠ Веб-сервер возвращает предупреждение в случае использования самоподписанного сертификата, однако это не влияет на работу.

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

```
sudo systemctl restart nginx
```

# 17 . ЭКСПЕРИМЕНТАЛЬНЫЕ ФУНКЦИИ

## 17.1 . Параметры конфигурирования компонентов «Универсальный диспетчер», «Менеджер рабочих мест»

Для настройки «Универсального диспетчера», «Менеджера рабочих мест» используется конфигурационный файл `/etc/opt/termidesk-vdi/termidesk.conf`.

При установке пакета `termidesk-vdi` возможно активировать режим отладки инсталлятора переменную окружения `TDSK_PKG_DEBUG=1`.

Перечень параметров, задающихся через файл, приведен в таблице (см. Таблица 46). Указанные параметры можно поменять также через утилиту `termidesk-config` (см. подраздел **Утилита termidesk-config**).

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

Таблица 74 – Параметры конфигурирования «Универсального диспетчера»

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| `TDSK_AUTOFS_IMAGES_ID` | `Не задано` | Параметр может быть задан на узлах «Универсального диспетчера».<br>Используется для настройки шаблонов переносимых профилей. В качестве значения используются идентификаторы дисков.<br>Пример: `TDSK_AUTOFS_IMAGES_ID=xx[,yy[,zz[,...]]]` |
| `DBHOST` | `Не задано` | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет IP-адрес или FQDN СУБД PostgreSQL.<br>Начальное значение задается на этапе подготовке среды функционирования и установки Termidesk |
| `DBPORT` | `5432` | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет порт соединения с сервером БД |
| `DBSSL` | `Не задано` | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет протокол подключения к БД.<br>Возможные значения: `Disable`, `TLSv1.2`, `TLSv1.3`.<br>Начальное значение задается на этапе установки Termidesk |
| `DBNAME` | `Не задано` | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет имя БД.<br>Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| DBUSER | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет имя пользователя, имеющего доступ к БД.<br>Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk |
| DBPASS | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет пароль пользователя, имеющего доступ к БД.<br>Начальное значение задается на этапе подготовки среды функционирования во время установки Termidesk и хранится в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` в преобразованном виде.<br>⚠ В стандартных установках значения менять не следует.<br>Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой `scramble`:<br>▪ для получения значения по стандартному алгоритму: `/opt/termidesk/bin/scramble --value <пароль> --type AES256`;<br>▪ для получения значения с увеличенным числом итераций преобразования: `/opt/termidesk/bin/scramble --value <пароль> --type AES256_V2`.<br>Утилита `scramble` использует в качестве вектора преобразования значение из файла `/etc/opt/termidesk-vdi/termidesk.cookie`. Значение генерируется автоматически на этапе установки Termidesk |
| DBCERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет путь к сертификату mTLS для защищенного подключения к БД.<br>⚠ mTLS - метод обеспечения защищенного соединения с БД через двустороннюю аутентификацию с использованием сертификатов.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;<br>▪ назначить владельцем файла пользователя `termidesk`:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.crt`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.crt`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**) |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| DBKEY | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет путь к ключу mTLS для защищенного подключения к БД.<br>Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению:<br>`openssl rsa -in <путь_к_файлу_ключа>.key -out <путь_сохранения_преобразованного_ключа>.key`<br>Для использования ключа также нужно:<br>▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;<br>▪ назначить владельцем файла пользователя `termidesk`:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.key`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.key`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен |
| DBCHAIN | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет путь к промежуточному сертификату mTLS для защищенного подключения к БД.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;<br>▪ назначить владельцем файла пользователя `termidesk`:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.pem`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.pem`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен |
| DJANGO_SECRET_KEY | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Используется для проверки данных, пересылаемых между компонентами Termidesk. Значение генерируется при установке Termidesk и должно быть одинаковым для всех узлов при распределенной установке |
| RABBITMQ_URL | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет URL-адрес подключения к серверам RabbitMQ. Можно подключить до трех (включительно) серверов.<br>Пароль подключения к серверу RabbitMQ, указанный в `RABBITMQ_URL`, хранится в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` в преобразованном виде.<br>Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой `scramble`:<br>▪ для получения значения по стандартному алгоритму: `/opt/termidesk/bin/scramble --value <пароль> --type AES256`;<br>▪ для получения значения с увеличенным числом итераций преобразования: `/opt/termidesk/bin/scramble --value <пароль> --type AES256_V2`.<br>Для использования преобразованного значения следует указать его в `RABBITMQ_URL` и выполнить перезапуск служб.<br>Начальное значение `RABBITMQ_URL` задается на этапе установки |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| RABBITMQ_SSL | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет протокол подключения к RabbitMQ.<br>Возможные значения: `Disable`, `TLSv1.2`.<br>Начальное значение задается на этапе установки |
| NODE_ROLES | Не задано | Параметр обязателен и задается на этапе установки.<br>Определяет тип роли, с которой будет установлен Termidesk. Возможные значения:<br>▪ `ADMIN` - роль «Портал администратора»;<br>▪ `USER` - роль «Портал пользователя»;<br>▪ `TASKMAN` - роль «Менеджер рабочих мест»;<br>▪ `CELERYMAN` - роль «Менеджер рабочих мест (очереди)»;<br>▪ `AGGR_ADM` - роль «Агрегатор администратора»;<br>▪ `AGGR_USR` - роль «Агрегатор пользователя».<br>ⓘ Установка ролей «Агрегатор администратора» и/или «Агрегатор пользователя» должна производиться на узле, отличном от «Портала администратора» и/или «Портала пользователя», «Менеджера рабочих мест».<br>При переустановке значение параметра в конфигурационном файле будет перезаписано |
| LOG_LEVEL | INFO | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет уровень журналирования сообщений.<br>Возможные значения: `DEBUG`, `INFO`, `WARNING`, `ERROR`, `CRITICAL` |
| LOG_ADDRESS | /dev/log | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет адрес отправки записей в системный журнал. Обычно это `/dev/log` для Linux-систем. Возможно указать IP-адрес и порт |
| LOG_FACILITY | local3 | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет категорию сообщений syslog.<br>Категория должна совпадать с настройками в конфигурационном файле `/etc/syslog-ng/conffirst.d/termidesk.conf` |
| HEALTH_CHECK_ACCESS_KEY | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет токен доступа к API проверки состояния сервера. Начальное значение генерируется на этапе установки.<br>При задании значения параметра следует руководствоваться правилом, что:<br>▪ размер должен составлять от 0 до 64 символа;<br>▪ должны использоваться символы в шестнадцатеричной системе (0-9, a-f).<br>Значение также может быть сгенерировано через `openssl`:<br>`openssl rand -hex 32` |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| METRICS_ACCESS_KEY | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет токен доступа к API получения метрик сервера. Начальное значение генерируется на этапе установки.<br>При задании значения параметра следует руководствоваться правилом, что:<br>▪ размер должен составлять от 0 до 64 символа;<br>▪ должны использоваться символы в шестнадцатеричной системе (0-9, a-f).<br>Значение также может быть сгенерировано через openssl:<br>`openssl rand -hex 32` |
| HEALTH_CHECK_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет путь к сертификату SSL/TLS для защищенного подключения к API проверки состояния сервера.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.pem`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.pem`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| HEALTH_CHECK_KEY | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет путь к ключу SSL/TLS для защищенного подключения к API проверки состояния сервера.<br>Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению:<br>`openssl rsa -in <путь_к_файлу_ключа>.key -out <путь_сохранения_преобразованного_ключа>.key`<br>Для использования ключа также нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.key`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.key`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| TASKMAN_HEALTH_CHECK_PORT | 8100 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест».<br>Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест».<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| TASKMAN_HEALTH_CHECK_IP | 0.0.0.0 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест».<br>Определяет IP-адрес, с которым служба termidesk-taskman регистрируется в подсистеме проверки состояния на странице «Инфраструктура» Termidesk. Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла.<br>Изначально параметр закомментирован (используется значение по умолчанию) |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| CELERY_BEAT_HEALTH_CHECK_PORT | 8103 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест (очереди)».<br>Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест (очереди)».<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| CELERY_BEAT_HEALTH_CHECK_IP | 0.0.0.0 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест (очереди)».<br>Определяет IP-адрес, с которым служба termidesk-celery-beat регистрируется в подсистеме проверки состояния на странице «Инфраструктура» Termidesk. Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла.<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| CELERY_WORKER_HEALTH_CHECK_PORT | 8104 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест (очереди)».<br>Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест (очереди)».<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| CELERY_WORKER_HEALTH_CHECK_IP | 0.0.0.0 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест (очереди)».<br>Определяет IP-адрес, с которым служба termidesk-celery-worker регистрируется в подсистеме проверки состояния на странице «Инфраструктура». Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла.<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| REQUESTS_CA_BUNDLE | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет путь к файлу с доверенным корневым сертификатом, задается для настройки работы с сертификатами собственных ЦС.<br>По умолчанию параметр не используется (закомментирован) |
| EULA_ACCEPTED | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет принятие лицензионного соглашения при установке. В случае автоматизированной установки наличие параметра обязательно |
| AGGREGATOR_JWT_SSL_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», использующихся в фермах, подключаемых к «Агрегатору». Обязателен для заполнения в случае, если в инфраструктуре также используется «Агрегатор».<br>Определяет путь к сертификату для получения значения JWT-токена «Агрегатора» |
| AGGREGATOR_JWT_SSL_CERT_SECOND | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», использующихся в фермах, подключаемых к «Агрегатору». Обязателен для заполнения в случае, если в инфраструктуре также используется «Агрегатор».<br>Определяет путь к резервному сертификату для получения значения JWT-токена «Агрегатора».<br>Если сертификат, заданный в AGGREGATOR_JWT_SSL_CERT, станет невалидным, то будет использоваться сертификат, указанный в AGGREGATOR_JWT_SSL_CERT_SECOND |
| AGGREGATOR_JWT_SSL_KEY | Не задано | Параметр обязателен и задается на узлах с установленным «Агрегатором» (портал «Агрегатор пользователя»).<br>Определяет путь к ключу для подписи JWT-токена «Агрегатора» |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| AGGREGATOR_ACCESS_TOKEN_TITLE | Termidesk JWT Title | Параметр обязателен и должен быть одинаковым на всех узлах, работающих совместно: на «Агрегаторе» (портал «Агрегатор пользователя»), на «Универсальных диспетчерах», подключаемых к «Агрегатору».<br>Задает заголовок JWT-токена, предназначенный для настройки взаимодействия между «Агрегатором» и «Универсальным диспетчером» |
| AGGREGATOR_ACCESS_TOKEN_TTL_SECONDS | 600 | Параметр обязателен и задается на узлах с установленным «Агрегатором».<br>Определяет времени жизни (в секундах) JWT-токена, подписанного «Агрегатором» |
| AGGREGATOR_IMAGE_CACHE_LIFETIME_HOURS | 672 | Параметр обязателен и задается на узлах с установленным «Агрегатором».<br>Определяет время жизни (в часах) кеша иконок фондов РМ. По истечении этого времени иконка обновляется |
| SECRETS_STORAGE_METHOD | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».<br>Определяет способ хранения паролей подключения к СУБД и RabbitMQ:<br>▪ config - пароли будут храниться в преобразованном виде в файле /etc/opt/termidesk-vdi/termidesk.conf;<br>▪ openbao - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено).<br>⚠ Хранилище паролей OpenBao должно быть реализовано в отказоустойчивом варианте, иначе Termidesk не будет работать в период простоя узлов OpenBao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_URL | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет IP-адреса или FQDN узла и порта с установленным хранилищем OpenBao.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Формат: http://<IP-адрес или FQDN>:8200. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_TOKEN | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет токен (Initial Root Token), сформированный при инициализации хранилища OpenBao.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки и хранится в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf в преобразованном виде.<br>Для преобразования значения параметра, заданного вручную, следует воспользоваться утилитой scramble:<br>▪ для получения значения по стандартному алгоритму: /opt/termidesk/bin/scramble --value <пароль> --type AES256;<br>▪ для получения значения с увеличенным числом итераций преобразования: /opt/termidesk/bin/scramble --value <пароль> --type AES256_V2. |
| SECRETS_OPENBAO_DB_PATH | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет путь, настроенный на OpenBao для хранения пароля СУБД.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| SECRETS_OPENBAO_DB_ROLE_NAME | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет роль, настроенную на OpenBao и имеющую доступ к паролю СУБД.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_RABBITMQ_PATH | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора»».<br>Определяет путь, настроенный на OpenBao для хранения пароля RabbitMQ.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_RABBITMQ_ROLE_NAME | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет роль, настроенную на OpenBao и имеющую доступ к паролю RabbitMQ.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_CLIENT_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет путь к сертификату SSL/TLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.crt<br>▪ изменить права на файл:<br>sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.crt<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**).<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| SECRETS_OPENBAO_CLIENT_KEY | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет путь к ключу SSL/TLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы.<br>Ключ может иметь парольную защиту. Для использования ключа в Termidesk нужно преобразовать его к начальному значению:<br>openssl rsa -in <путь_к_файлу_ключа>.key -out <путь_сохранения_преобразованного_ключа>.key<br>Для использования ключа также нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.key<br>▪ изменить права на файл:<br>sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.key<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Изначально параметр закомментирован (используется значение по умолчанию) |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| SECRETS_OPENBAO_SERVER_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет путь к промежуточному сертификату ЦС SSL/TLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.pem<br>▪ изменить права на файл:<br>sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.pem<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| SECRETS_OPENBAO_TERMIDESK_PATH | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет путь, настроенный на OpenBao для хранения паролей Termidesk.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_TERMIDESK_ROLE_NAME | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет роль, настроенную на OpenBao и имеющую доступ к паролям Termidesk.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_KV_VERSION | 1 | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Используется для указания версии API OpenBao.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Возможные значения:<br>▪ 1 (по умолчанию);<br>▪ 2.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_CACHE_LIFETIME | 5 | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора».<br>Определяет время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти. Позволяет сохранить полученный от OpenBao пароль на некоторое время в кеше для сокращения количества обращений к OpenBao.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao.<br>Начальное значение задается на этапе установки |
| FLUENTD_CACHE | 15 | Параметр может быть задан на узлах «Универсального диспетчера».<br>Определяет время (в секундах) кеширования параметров подключения к узлу «Ретранслятора».<br>По умолчанию после установки время кеширования составляет 15 секунд.<br>В случае, если нужно изменить значение, следует раскомментировать параметр и задать ему новое значение |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| FLUENTD_TABLE | logs | Параметр может быть задан на узлах «Универсального диспетчера».<br>Определяет таблицу хранения событий фермы Termidesk.<br>По умолчанию после установки «Универсальный диспетчер» обращается к таблице «logs» БД «Ретранслятора».<br>В случае, если в БД «Ретранслятора» для хранения событий используется другая таблица, следует раскомментировать параметр и указать новое имя таблицы |
| WSPROXY_TICKET_TIMEOUT | 20 | При штатном функционировании Terrmidesk менять параметр не рекомендуется.<br>Параметр может быть задан на узлах «Универсального диспетчера».<br>Определяет время ожидания отклика «Шлюза» и применяется для решения нештатных ситуаций, например: если параметр «Время ожидания соединения» по каким-либо причинам не используется в протоколе доставки, или если запрос к «Шлюзу» выполняется долго и подключение пользователя не устанавливается.<br>По умолчанию после установки время ожидания составляет 20 секунд.<br>В случае, если нужно изменить значение, следует раскомментировать параметр и задать ему новое значение |

Пример файла конфигурации сервера OpenBao, который активирует строгую проверку клиентского SSL-сертификата:

```
listener "tcp" {
tls_min_version = "tls12"
tls_disable = "false"
address = "0.0.0.0:8200"
tls_cert_file = "/etc/bao/openbao.stand8.local.crt"
tls_key_file = "/etc/bao/openbao.stand8.local.key"
# Если включён, то будет проверять сертификат клиента на корректность
tls_require_and_verify_client_cert = "true"
# Если выключён, то будет требовать наличие сертификата клиента
tls_disable_client_certs = "false"
}
```

### 17.2 . Управление экспериментальными параметрами Termidesk

Включение и отключение экспериментальных параметров сервера Termidesk производится из командной строки.

Перечень экспериментальных параметров приведен в таблице (см. Таблица 75).

Таблица 75 – Экспериментальные параметры Termidesk

| Параметр | Описание | Значение по умолчанию |
|---|---|---|
| experimental.2fa.enabled | Параметр поддержки двухфакторной аутентификации | 0 |
| experimental.deviceauth.enabled | Параметр поддержки авторизации устройств доступа | 0 |

| Параметр | Описание | Значение по умолчанию |
|---|---|---|
| experimental.radiusauth.enabled | Параметр поддержки домена аутентификации RADIUS | 0 |

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

- переключиться на пользователя termidesk :

```
sudo -u termidesk bash
```

- активировать параметр:

```
/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.

### 17.3 . Установка плагинов расширений

Начиная с Termidesk версии 5.1 использование функционала, подключаемого через плагин расширения, исключено. Описание приведено для справки.

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

Для установки плагинов нужно:

- переключиться на пользователя Termidesk:

```
sudo -u termidesk bash
```

- перейти в каталог Termidesk:

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

- активировать виртуальное окружение Termidesk:

```
source venv/bin/activate
```

- установить необходимый плагин:

```
pip install --upgrade --no-index --find-links /var/repos/Addons/Plugins/v5.0/
termidesk_internaldbauth
```

где:

`/var/repos/Addons/Plugins/v5.0/` - каталог с `whl`-файлами;

`termidesk_internaldbauth` - имя плагина (без версии, платформы и расширения файла);

- выйти из окружения пользователя `Termidesk`:

```
exit
```

- обновить структуру БД и статических файлов командами:

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

- перезапустить службу Termidesk:

```
sudo systemctl restart termidesk-vdi.service
```

### 17.4 . Удаление плагинов расширений

Перед удалением плагина необходимо удалить фонды РМ, шаблоны ВМ и поставщика ресурсов, соответствующих данному плагину.
Удаление фонда РМ может занять продолжительное время.

Начиная с Termidesk версии 5.1 использование функционала, подключаемого через плагин расширения, исключено. Описание приведено для справки.

Для удаления плагина расширений нужно:

- переключиться на пользователя `Termidesk`:

```
sudo -u termidesk bash
```

- перейти в каталог `Termidesk`:

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

- активировать виртуальное окружение `Termidesk`:

```
source venv/bin/activate
```

- удалить необходимый плагин:

```
pip uninstall -y termidesk_internaldbauth
```

где:

`termidesk_internaldbauth` - имя плагина (без версии, платформы и расширения файла);

- выйти из окружения пользователя `Termidesk`:

```
exit
```

- перезапустить службу Termidesk:

```
sudo systemctl restart termidesk-vdi.service
```

### 17.5 . 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:

> Начиная с Termidesk версии 5.1 использование функционала, подключаемого через плагин расширения, исключено. Описание приведено для справки.

```
1 pip install --no-index --find-links /var/repos/Addons/Plugins/v5.0/
termidesk_internaldbauth==4.0.1
```

где:

`/var/repos/Addons/Plugins/v5.0/` - каталог с `whl`-файлами, `whl`-файл с версией плагина должен существовать в данном каталоге;

`termidesk_internaldbauth` - имя плагина с указанием версии.

# 18 . РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ ОТСЛЕЖИВАНИЯ СОСТОЯНИЯ КОМПОНЕНТОВ TERMIDESK

## 18.1 . Общие сведения по проверке состояния компонентов

Для отслеживания состояния компонентов Termidesk и обращения к ним для выполнения проверок состояния (health check) используется API-запрос `/api/health`.

Начальная спецификация схемы HealthCheck API в формате OpenAPI соответствует описанию:

```
openapi: 3.0.3
info:
  title: Termidesk health check api schema
  version: 0.1
paths:
  /api/health:
    get:
      responses:
        '200':
          description: Successful Response
          content:
            application/json:
              schema:
                type: object
                properties:
                  status:
                    type: string
                    enum: [pass, warn, fail]
                    example: fail
                    description: "Состояние компонента"
                  version:
                    type: string
                    example: 3.3
                    description: "Версия компонента"
                  description:
                    type: string
                    example: termidesk-taskman
                    description: "Описание компонента"
                  output:
                    type: string
                    example: "django.db.utils.OperationalError: FATAL:  password authentication failed for user 'termidesk'"
                    description: "Описание ошибки (если есть)"
                required:
                  - status
        '401':
          description: Authorization information is missing or invalid
```

Базовый URL для API: `/api/health`.

Тип контента: `application/json`.

Для каждого компонента Termidesk механизм проверки состояния доступен на порте, заданном в конфигурационном файле:

> ⚠ Для компонента «Универсальный диспетчер» порт определен настройками веб-сервера (по умолчанию используется 443).

- для компонента «Менеджер рабочих мест» - в файле `/etc/opt/termidesk-vdi/termidesk.conf`, в параметрах `TASKMAN_HEALTH_CHECK_PORT` (по умолчанию используется 8100), `CELERY_BEAT_HEALTH_CHECK_PORT` (по умолчанию используется 8103), `CELERY_WORKER_HEALTH_CHECK_PORT` (по умолчанию используется 8104);
- для компонента «Шлюз» - в файле `/etc/termidesk/gateway.yaml`, в параметре `${mgtServerPort:8102}` (по умолчанию используется 8102).

Для исключения злоупотреблением частыми вызовами API, способными создать нагрузку на систему, доступ к API-запросу контролируется отдельным токеном. Значение токена задается конфигурационным файлом:

- для компонентов «Универсальный диспетчер», «Менеджер рабочих мест» - в файле `/etc/opt/termidesk-vdi/termidesk.conf`, в параметре `HEALTH_CHECK_ACCESS_KEY`;
- для компонента «Шлюз» - в файле `/etc/termidesk/gateway.yaml`, в параметре `token: ${healthCheckAccessKey}`.

Пример `HEALTH_CHECK_ACCESS_KEY`:

```
HEALTH_CHECK_ACCESS_KEY = "9944b09199c62bcf9418ad846dd0e4bbdfc6ee4b"
```

Пример `token: ${healthCheckAccessKey}`:

```
${healthCheckAccessKey:9944b09199c62bcf9418ad846dd0e4bbdfc6ee4b}
```

### 18.2 . Состояние компонента «Универсальный диспетчер»

При распределенной установке Termidesk экземпляры компонента «Универсальный диспетчер» могут быть установлены на нескольких узлах. Доступ к узлам организуется через балансировщик нагрузки, но для механизма проверок состояния нужно обращаться к каждому узлу напрямую.
Компонент изначально задействован для работы по протоколу HTTP, поэтому механизм проверки состояния реализуется отдельными вызовами REST API.
Пример команды проверки состояния компонента через утилиту `curl`:

```
1  curl --insecure -v -s -X 'GET' "https://${HOSTNAME}:443/api/health/check" -H
   'accept: application/json' -H "Authorization: Token ${HEALTH_CHECK_ACCESS_KEY}"
```

⚠ Ключ `--insecure` используется для отключения проверки валидности сертификатов. Выполнение запроса без использования проверки SSL допустимо только на тестовых стендах. В производственной среде необходимо установить валидные сертификаты.

### 18.3 . Состояние компонента «Шлюз»

При распределенной установке Termidesk экземпляры компонента «Шлюз» могут быть установлены на нескольких узлах. Доступ к узлам организуется через балансировщик нагрузки, но для механизма проверок состояния нужно обращаться к каждому узлу напрямую.

Для исключения злоупотреблением частыми вызовами API, способными создать нагрузку на систему, доступ к API-запросу компонента «Шлюз» `termidesk-gateway` контролируется отдельным токеном. Значение токена задается при запуске службы «Шлюза» в параметре `token: ${healthCheckAccessKey}`.

Пример команды проверки состояния компонента через утилиту `curl` для компонента «Шлюз» `termidesk-gateway` (предполагается, что «Шлюз» настроен для работы по защищенному соединению):

```
curl --insecure -v -s -X 'GET' "https://${HOSTNAME}:8102/api/health" -H 'accept: application/json' -H "Authorization: Token ${healthCheckAccessKey}"
```

### 18.4 . Состояние компонента «Менеджер рабочих мест»

При распределенной установке Termidesk экземпляры компонента «Менеджер рабочих мест» могут быть установлены на нескольких узлах, но активен должен быть только один из них. Все остальные компоненты являются резервными и, по умолчанию, находятся в состоянии «Passive».

Для использования механизма проверки состояния компонента необходимо в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` раскомментировать строки параметров:

- для непосредственно компонента «Менеджер рабочих мест», а именно службы `termidesk-taskman`: `TASKMAN_HEALTH_CHECK_IP`, `TASKMAN_HEALTH_CHECK_PORT`, `HEALTH_CHECK_CERT`, `HEALTH_CHECK_KEY`. Для параметров `HEALTH_CHECK_CERT`, `HEALTH_CHECK_KEY` нужно указать путь к сертификату и ключу, используемых для защищенного подключения, и выполнить перезапуск служб Termidesk;
- для непосредственно компонента «Менеджер рабочих мест (очереди)», а именно службы `termidesk-celery-beat`: `CELERY_BEAT_CHECK_IP`, `CELERY_BEAT_HEALTH_CHECK_PORT`, `HEALTH_CHECK_CERT`, `HEALTH_CHECK_KEY`. Для параметров `HEALTH_CHECK_CERT`, `HEALTH_CHECK_KEY` нужно указать путь к сертификату и ключу, используемых для защищенного подключения, и выполнить перезапуск служб Termidesk;

- для непосредственно компонента «Менеджер рабочих мест (очереди)», а именно службы `termidesk-celery-worker`: `CELERY_WORKER_CHECK_IP`, `CELERY_WORKER_HEALTH_CHECK_PORT`, `HEALTH_CHECK_CERT`, `HEALTH_CHECK_KEY`. Для параметров `HEALTH_CHECK_CERT`, `HEALTH_CHECK_KEY` нужно указать путь к сертификату и ключу, используемых для защищенного подключения, и выполнить перезапуск служб Termidesk.

Пример задания значений:

```
TASKMAN_HEALTH_CHECK_PORT=8100
TASKMAN_HEALTH_CHECK_IP='0.0.0.0'
CELERY_BEAT_HEALTH_CHECK_PORT=8103
CELERY_BEAT_HEALTH_CHECK_IP='0.0.0.0'
CELERY_WORKER_HEALTH_CHECK_PORT=8104
CELERY_WORKER_HEALTH_CHECK_IP='0.0.0.0'
HEALTH_CHECK_CERT=/etc/opt/termidesk-vdi/healthcheck.pem
HEALTH_CHECK_KEY=/etc/opt/termidesk-vdi/healthcheck-decrypted.key
```

Пример команды проверки состояния компонента «Менеджер рабочих мест», а именно службы `termidesk-taskman`, через утилиту `curl` (предполагается, что «Менеджер рабочих мест» настроен для работы по защищенному соединению):

```
curl --insecure -v -s -X 'GET' "${HOSTNAME}:8100/api/health/check" -H 'accept: application/json' -H "Authorization: Token ${HEALTH_CHECK_ACCESS_KEY}"
```

# 19 . НЕШТАТНЫЕ СИТУАЦИИ

## 19.1 . Нештатные ситуации и способы их устранения

Возможные неисправности при работе с Termidesk и способы их устранения приведены в таблице (см. Таблица 76).

Таблица 76 – Перечень возможных нештатных ситуаций

| Индикация | Описание | Возможное решение |
|---|---|---|
| Ошибка:<br>«СБОЙ: оставшиеся слоты подключений зарезервированы для подключений суперпользователя (не для репликации)» | Ошибка возникает при попытке авторизации на сервере Termidesk | Изменить максимальное количество подключений в настройках БД: изменить значение `max_connections` в конфигурационном файле `/etc/postgresql/11/main/postgresql.conf` в бОльшую сторону |
| Ошибка:<br>«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» |
| Ошибка:<br>«kinit: Client 'HTTP/termidesk.local@LOCAL' not found in Kerberos database while getting initial credentials» | Ошибка возникает при добавлении или редактировании домена аутентификации FreeIPA | Необходимо создать указанную учетную запись на КД FreeIPA |
| Ошибка при установке пакета:<br>«Невозможно найти пакет» или «Неудовлетворенные зависимости» | Ошибка возникает при попытке установить пакет в ОС | Необходимо убедиться, что в файле `/etc/apt/sources.list` заданы и не закомментированы источники получения пакетов (репозитории), затем обновить списки пакетов:<br>`udo apt update`<br>После этого нужно вновь выполнить команду установки пакета.<br>Для решения проблемы с неудовлетворенными зависимостями, помимо подключения репозиториев в файле `/etc/apt/sources.list`, можно воспользоваться командой:<br>`sudo apt -f install`<br>Ключ `-f` используется для попытки исправить нарушенные зависимости пакетов. |

| Индикация | Описание | Возможное решение |
|---|---|---|
| Ошибка при установке пакета:<br>«Невозможно найти пакет» или «Неудовлетворенные зависимости» | Ошибка возникает при попытке установить пакет в ОС | Необходимо убедиться, что в файле `/etc/apt/sources.list` заданы и не закомментированы источники получения пакетов (репозитории), затем обновить списки пакетов:<br>`sudo apt update`<br>После этого нужно вновь выполнить команду установки пакета.<br>Для решения проблемы с неудовлетворенными зависимостями, помимо подключения репозиториев в файле `/etc/apt/sources.list`, можно воспользоваться командой:<br>`sudo apt -f install`<br>Ключ `-f` используется для попытки исправить нарушенные зависимости пакетов |

# 20 . ПЕРЕЧЕНЬ ТЕРМИНОВ

| Термин | Определение |
|---|---|
| Агрегатор администратора | Веб-интерфейс управления порталом «Агрегатор» |
| Агрегатор пользователя | Веб-интерфейс пользователя для получения ресурсов, предоставляемых порталом «Агрегатор» |
| Компонент «Агент» | Собирательное название для следующих компонентов Termidesk:<br>▪ «Агент виртуального рабочего места»;<br>▪ «Агент узла виртуализации»;<br>▪ «Сессионный агент»;<br>▪ «Видеоагент»;<br>▪ «Агент виртуальных смарт-карт».<br>Самостоятельный компонент, отвечающий за контролируемую доставку РМ, взаимодействие с «Универсальным диспетчером» и «Менеджером рабочих мест» |
| Компонент «Агент виртуальных смарт-карт» | Компонент Termidesk. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление подключенных к пользовательской рабочей станции смарт-карт в ВРМ |
| Компонент «Агент виртуального рабочего места» | Компонент Termidesk. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет взаимодействие с «Универсальным диспетчером», конфигурирует ВРМ, фиксирует действия пользователя, реализует передачу управляющих сообщений |
| Компонент «Агент узла виртуализации» | Компонент Termidesk. Устанавливается на узел виртуализации, взаимодействует с гипервизором через модуль `libvirt` |
| Базовое ВРМ | Также: золотой образ, базовый образ.<br>Подразумевает собой образ диска ВМ с предустановленным прикладным ПО и установленным «Агентом виртуального рабочего места». Этот образ далее будет использоваться для создания ВРМ для пользователей |
| Балансировщик нагрузки | Самостоятельный компонент, отвечающий за распределение нагрузки на множество «Универсальных диспетчеров» и «Шлюзов» |
| Компонент «Видеоагент» | Компонент Termidesk. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление видеокамеры с пользовательской рабочей станции в ВРМ |
| Виртуальное рабочее место (ВРМ) | Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО. Подключение к ВРМ происходит через протоколы удаленного доступа |
| Рабочее место (РМ) | Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа.<br>Под РМ подразумеваются как ВРМ, так и терминальный доступ или доступ к опубликованным на терминальном сервере приложениям |
| Гостевая ОС | ОС, функционирующая на ВМ |
| Группы РМ | Функциональное объединение множества фондов РМ по определенному признаку |
| Домен аутентификации | Способ проверки субъектов и их полномочий |
| Компонент «Менеджер рабочих мест» | Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом РМ, включая создание, настройку, запуск, отключение и удаление.<br>Является обработчиком фоновых задач.<br>Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-taskman.service` |

| Термин | Определение |
|---|---|
| Компонент «Оркестратор» | Компонент Termidesk. Самостоятельный компонент, отвечающий за согласованную работу всех компонентов программного комплекса при децентрализованном развертывании, для нужд отказоустойчивости и комплексирования с облачными службами |
| Поставщик ресурсов | ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ |
| Протокол доставки | Поддерживаемый в Termidesk протокол удаленного доступа к РМ |
| Связанный клон | Способ организации ВРМ на основе единого образа, с возможностью экономии дискового пространства, за счет технологии «копирование при записи», и ускорения операций возврата к базовому состоянию, установки дополнительного ПО и обновлений |
| Компонент «Сессионный агент» | Компонент Termidesk. Устанавливается на терминальный сервер (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям |
| Компонент «Универсальный диспетчер» | Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ.<br>Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service` |
| Фонд РМ | Совокупность подготовленных рабочих мест для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей |
| Шаблон РМ | Параметры конфигурации РМ для использования в фонде РМ |
| Компонент «Шлюз» | Компонент Termidesk. Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP.<br>Устанавливается из пакета `termidesk-gateway`. Наименование службы после установки: `termidesk-gateway.service` |
| Компонент «Сервер терминалов Astra Linux» | Компонент Termidesk. Также: STAL.<br>Обеспечивает подключение пользовательских рабочих станций к РМ с ОС Astra Linux Special Edition через сеанс удаленного терминала |
| Портал «Агрегатор» | Роль компонента «Универсальный диспетчер», доступная при установке Termidesk. Является единой точкой входа для получения ресурсов пользователями, предоставляет им объединенный список приложений и ВРМ с ферм Termidesk |
| Портал администратора | Предоставляет веб-интерфейс для управления Termidesk и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API |
| Портал пользователя | Предоставляет пользовательский веб-интерфейс Termidesk (без доступа к функциям управления) и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API |
| Портал универсальный | Предоставляет функции обоих вариантов - и «Портала администратора», и «Портала пользователя». При этом активируется доступ ко всем модулям документации по командам REST API, предоставляемым интерфейсом `swagger` |
| Ключ | Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом |
| Сертификат | Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу |
| Ферма | Логическое объединение узлов, взаимодействующих с одной БД |

# 21 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

| Сокращение | Пояснение |
|---|---|
| БД | База данных |
| ВМ | Виртуальная машина |
| ВРМ | Виртуальное рабочее место |
| ГУСИ | Глобальный уникальный сессионный идентификатор |
| ЗПС | Замкнутая программная среда |
| КД | Контроллер домена |
| ОЗУ | Оперативное запоминающее устройство |
| ОС | Операционная система |
| ПК СВ Брест | Программный комплекс «Средства виртуализации «Брест» |
| ПО | Программное обеспечение |
| РМ | Рабочее место |
| СУБД | Система управления базами данных |
| ЦП | Центральный процессор |
| ЦС | Центр сертификации |
| ЭЦП | Электронная цифровая подпись |
| ACL | Access Control List (список контроля доступа) |
| ALD | Astra Linux Directory (единое пространство пользователей) |
| AMQP | Advanced Message Queueing Protocol (открытый протокол для передачи сообщений между компонентами системы) |
| AMQPS | Расширение протокола AMQP с использованием TLS для шифрования |
| API | Application Programming Interface (интерфейс прикладного программирования) |
| CRUD | Create Read Update Delete (акроним основных операций с информацией в БД) |
| CSR | Certificate Signing Request (зашифрованный запрос на выпуск сертификата) |
| DHCP | Dynamic Host Configuration Protocol (протокол назначения сетевого адреса) |
| DN | Domain Name (доменное имя) |
| DNS | Domain Name System (система доменных имен) |
| FQDN | Fully Qualified Domain Name (полностью определенное имя домена) |
| FreeIPA | Free Identity, Policy and Audit (открытое решение по безопасности Linux-систем) |
| GC | Global Catalog (глобальный каталог) |
| GID | Group Identification Data (идентификатор группы) |

| Сокращение | Пояснение |
|---|---|
| GPU | Graphics Processing Unit (графический процессор) |
| GUSID | Global Unique Session ID (глобальный уникальный сессионный идентификатор) |
| HTML | Hypertext Markup Language (язык гипертекстовой разметки) |
| HTTPS | Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования) |
| ID | Identification Data (идентификатор) |
| IdP | Identity Provider (сервис, управляющий идентификационной информацией) |
| IP | Internet Protocol (межсетевой протокол) |
| JSON | JavaScript Object Notation (стандартный текстовый формат для структурированных данных) |
| JWKS | JSON Web Key Set (набор открытых ключей для проверки веб-токена) |
| JWT | JSON Web Token (открытый стандартдля создания токенов доступа) |
| LDAP | Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов) |
| LDAPS | Lightweight Directory Access Protocol over SSL/TSL (расширение протокола LDAP) |
| MAC | Media Access Control (уникальный идентификатор сетевого устройства) |
| MS AD | Microsoft Active Directory (службы каталогов Microsoft) |
| mTLS | Multiplexed Transport Layer Security (протокол, основанный на TLS с усиленной безопасностью) |
| OIDC | OpenID Connect (протокол аутентификации, построенный поверх стандарта OAuth 2.0) |
| OU | Organizational Unit (организационная единица) |
| PAM | Pluggable Authentication Module (подключаемый модуль аутентификации) |
| PID | Product ID (идентификатор продукта) |
| PKCS | Public Key Cryptography Standards (стандарты криптографии с открытым ключом) |
| PKINIT | Public Key Cryptography for Initial Authentication (механизм Kerberos, позволяющий использовать сертификаты X.509) |
| RADIUS | Remote Authentication Dial-In User Service (протокол, предоставляющий функции аутентификации, авторизации и учета) |
| RDP | Remote Desktop Protocol (протокол удаленного рабочего стола) |
| RDS | Remote Desktop Services (службы удаленного рабочего стола Microsoft) |
| RDSH | Remote Desktop Session Host (хост сеансов удаленных рабочих столов) |
| REDIS | REmote DIctionary Service (резидентная СУБД) |
| REST | Representational State Transfer (программная архитектура, определяющая условия работы API) |

| Сокращение | Пояснение |
|---|---|
| RFC | Request for Comments (рабочее предложение Интернет) |
| RPC | Remote Procedure Call (удаленный вызов процедур) |
| RSA | Rivest, Shamir and Adleman (криптографический алгоритм с открытым ключом) |
| RTSP | Real-Time Streaming Protocol (протокол для управления потоковой передачей данных) |
| PKI | Public Key Infrastructure (инфраструктура открытых ключей) |
| SAM | Security Account Manager (диспетчер учетных записей безопасности) |
| SAML | Security Assertion Markup Language (открытый стандарт обмена данными аутентификации) |
| SASL | Simple Authentication and Security Layer (фреймворк для аутентификации и обеспечения безопасности) |
| SCSI | Small Computer System Interface (набор стандартов для физического подключения и передачи данных между компьютерами и периферийными устройствами) |
| SMB | Server Message Block (протокол для удалённого доступа к сетевым ресурсам) |
| SPICE | Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды) |
| SRV | Service Record DNS (служебная запись в DNS) |
| SSL | Secure Sockets Layer (криптографический протокол) |
| SSO | Single Sign-On (технология единого входа) |
| STAL | Terminal Server Astra Linux (сервер терминалов Astra Linux) |
| STUN | Session Traversal Utilities for NAT (сетевой протокол, позволяющий определить внешний IP-адрес и другие параметры |
| TCP | Transmission Control Protocol (протокол управления передачей) |
| TERA | Termidesk Remote Access protocol (протокол удаленного доступа собственной разработки) |
| TLS | Transport Layer Security (протокол защиты транспортного уровня) |
| TOTP | Time-based One Time Password (метод авторизации пользователя) |
| UDP | User Datagram Protocol (протокол пользовательских датаграмм) |
| URI | Uniform Resource Identifier (унифицированный идентификатор ресурса) |
| URL | Uniform Resource Locator (унифицированный указатель ресурса) |
| URSI | Unique Resource Start ID (уникальный идентификатор запуска ресурса) |
| USB | Universal Serial Bus (последовательный интерфейс для подключения периферийных устройств) |
| UUID | Universally Unique Identifier (уникальный идентификатор) |
| vGPU | Virtual Graphics Processing Unit (виртуальный графический процессор) |
| VDI | Virtual Desktop Infarsticture (инфраструктура виртуальных рабочих столов) |

| Сокращение | Пояснение |
|---|---|
| VLAN | Virtual Local Area Network (виртуальная локальная сеть) |
| VNC | Virtual Network Computing (система удаленного доступа к рабочему столу компьютера) |
| VPN | Virtual Private Network (технология для зашифрованного безопасного соединения) |
| VRRP | Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности) |
| WebRTC | Web Real-Time Communications (открытый проект для организации передачи потоковых данных) |
| WS | WebSocket (двунаправленный протокол, позволяющий клиенту установить связь с сервером) |
| WSS | WebSocketSecure (двунаправленный протокол, позволяющий клиенту установить защищенную связь с сервером) |
| X.509 | Стандарт для инфраструктуры открытого ключа |

UVEON
Unified Virtualization
Experience, Opportunities, Now



119571, г. Москва, Ленинский проспект,
д. 119А, помещ. 9Н
https://termidesk.ru/
Телефон: +7 (495) 975-1-975

Общий e-mail: info@uveon.ru
Отдел продаж: sales@uveon.ru
Техническая поддержка: support@uveon.ru