TERMIDESK

Вариант лицензирования «TermideskTerminal»

РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-02 90 02

Версия 4.1.1. Выпуск от июня 2023

Настройка программного комплекса

ОГЛАВЛЕНИЕ

1 . ОБЩИЕ СВЕДЕНИЯ

1.1 . О документе

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

Во второй части руководства приведена настройка Termidesk, рассмотрены взаимодействие компонентов, разграничение функций по администрированию. Для того, чтобы получить информацию об установке программного комплекса, необходимо обратиться к первой части руководства администратора - СЛЕТ.10001-02 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), 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 пользователяTermidesk;
- функции оператора Termidesk.

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

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

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

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

Пользователь Termidesk использует компонент «Клиент» для получения доступа к виртуальному рабочему месту (BPM).
Оператор Termidesk задается администратором Termidesk. Оператору Termidesk доступен ограниченный администратором Termidesk список полномочий по доступу в графический интерфейс управления.

2.2 . Схема сетевого взаимодействия компонентов Termidesk

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

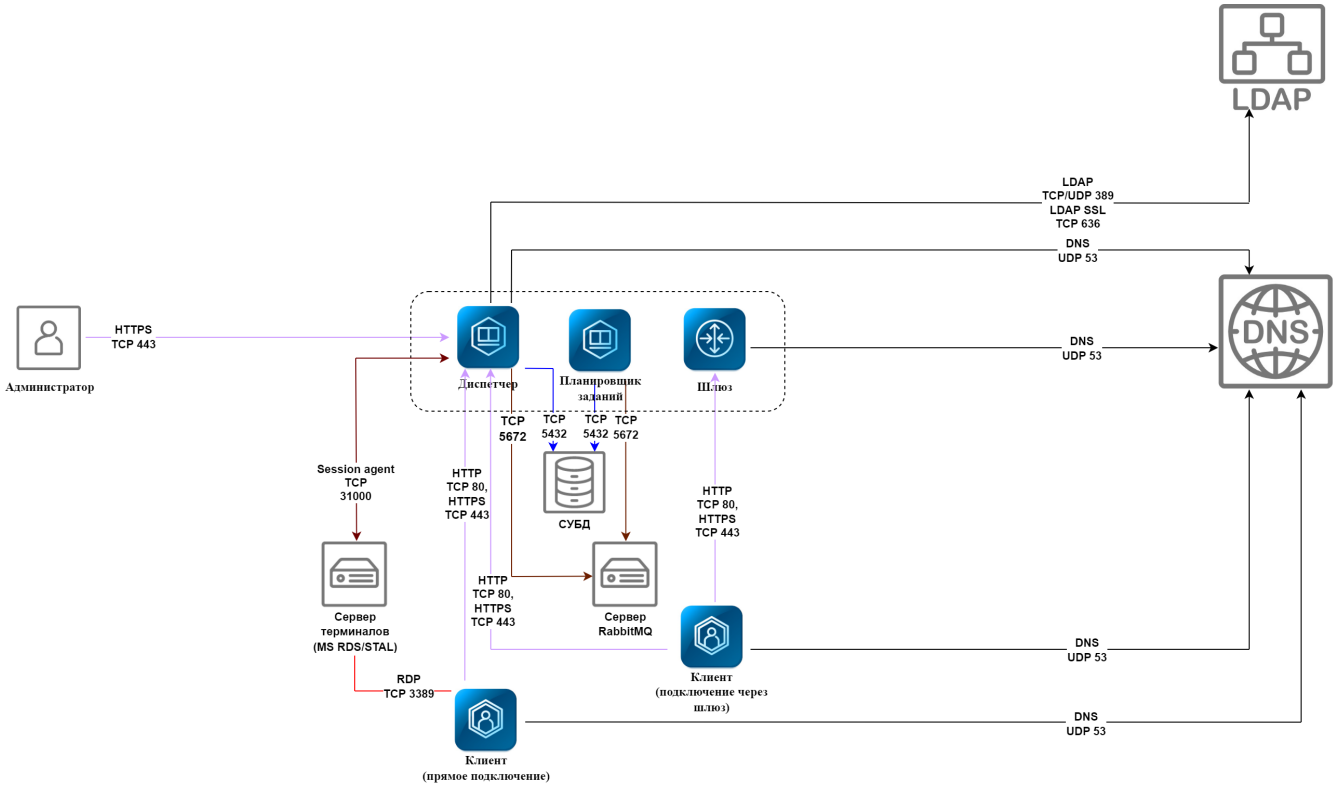

Рисунок 1 – Схема сетевого взаимодействия компонентов Termidesk

Общий перечень узлов и компонентов Termidesk представлен в таблице.

Таблица 1 – Перечень узлов и компонентов

Компонент	Наименование на схеме	Узел установки	Наименование пакета установки
«Универсальный диспетчер»	Диспетчер	Отдельный узел для установки	`termidesk-vdi`
«Менеджер рабочих мест»	Планировщик заданий	Отдельный узел для установки или установка совместно с диспетчером	`termidesk-vdi`
«Шлюз»	Шлюз	Отдельный узел для установки или установка совместно с диспетчером	`termidesk-vdi`
«Агент» (сессионный агент)	Session agent	Сервер терминалов (Microsoft Windows Server с ролью «Remote Desktop Services» (далее - MS RDS), Terminal Server Astra Linux (далее - STAL))	`termidesk-session-agent`
«Клиент»	Клиент	Рабочее место пользователя (пользовательская рабочая станция)	`termidesk-client`
«Сервер терминалов»	-	Сервер терминалов Astra Linux (STAL)	`stal`

2.3 . Последовательность сетевых запросов компонентов Termidesk

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

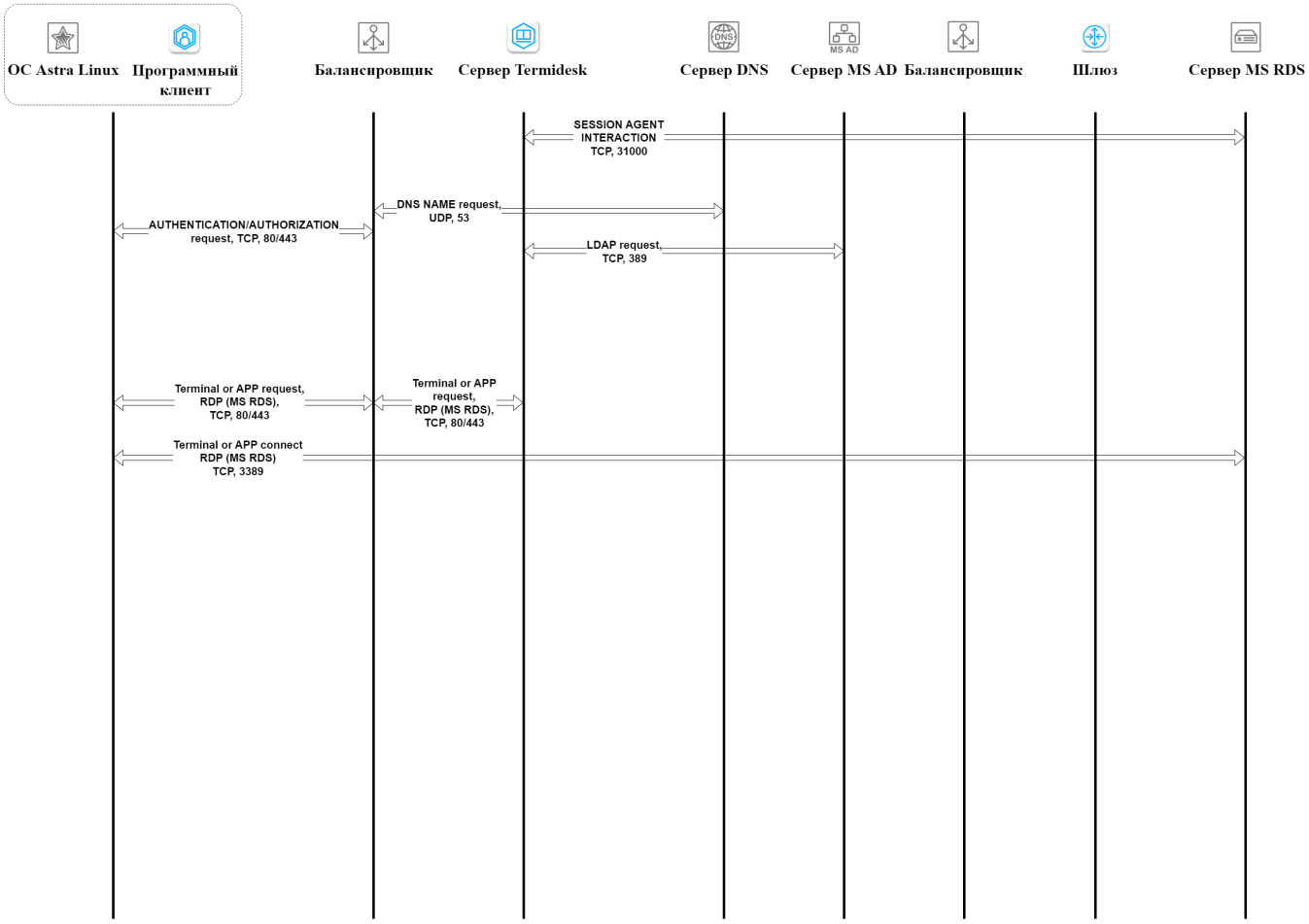

Рисунок 2 – Общая последовательность сетевых запросов

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

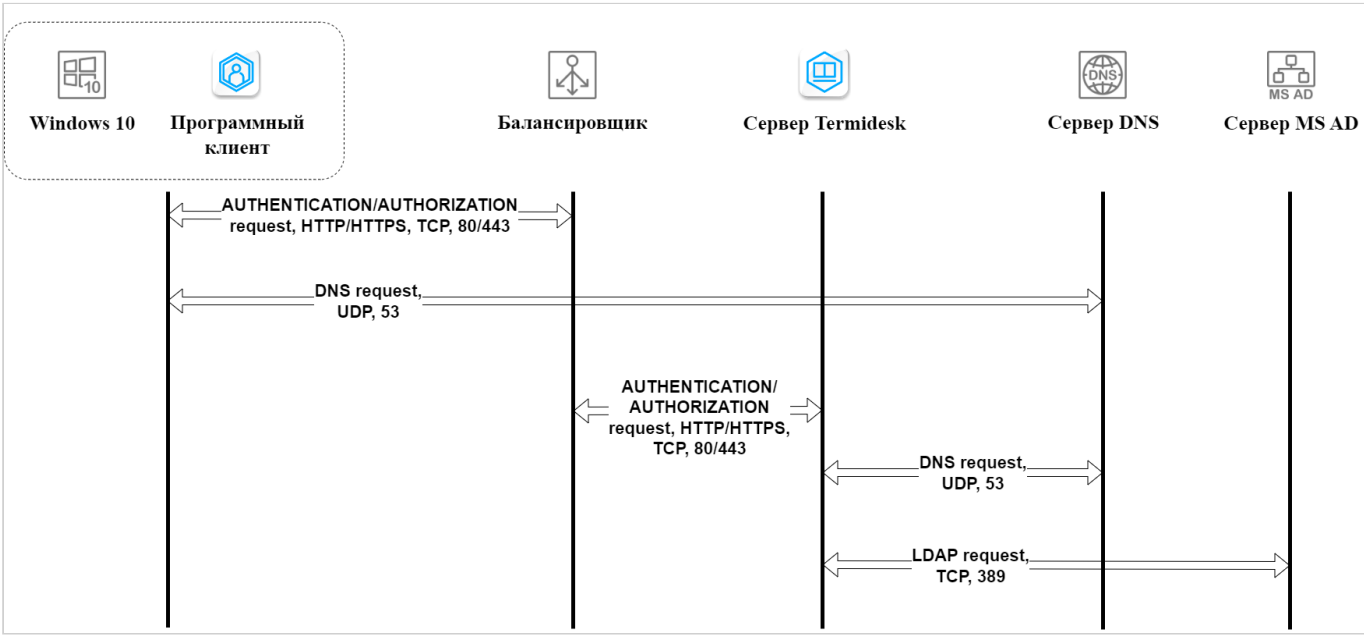

Рисунок 3 – Последовательность сетевых запросов при аутентификации и авторизации

2.4 . Перечень сетевых портов компонентов Termidesk

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

Таблица 2 – Перечень сетевых портов, используемых компонентами Termidesk

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

HTTP	TCP	80
HTTPS	TCP	443
RDP	TCP	3389
WSPROXY (`termidesk-wsproxy`)	TCP	5099
DNS	UDP	53
«Агент» (сессионный агент)		
SESSION AGENT (`TermideskSessionAgent`)	TCP	31000
«Клиент»		
HTTP	TCP	80
HTTPS	TCP	443
RDP	TCP	3389
CLIENT (`termidesk-client`)	TCP	1024-49151

3 . НАЧАЛО РАБОТЫ

3.1 . Последовательность ввода в действие

Общая последовательность шагов для ввода Termidesk в варианте лицензирования Termidesk Terminal в действие 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, Установка и настройка отделяемых компонентов на одном узле, 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);
- установка компонента «Агент» на сервер терминалов (см. подраздел **Установка сессионного Агента** документа СЛЕТ.10001-02 90 04 «Руководство администратора. Настройка компонента «Агент»);
- запуск панели управления Termidesk и добавление поставщика ресурсов «Сервер терминалов» в Termidesk;
- добавление домена аутентификации;
- создание шаблона BPM для поставщика «Сервер терминалов» в Termidesk;
- добавление пользователей, групп, протоколов доставки в Termidesk;
- создание и настройка фонда BPM в Termidesk.

4 . ПОСТАВЩИКИ РЕСУРСОВ

4.1 . Общие сведения о поставщиках ресурсов

Поставщик ресурсов в Termidesk варианта лицензирования «Termidesk Terminal» - это терминальный сервер, предоставляющий вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения ВРМ.

Графический интерфейс управления Termidesk обеспечивает следующие операции управления поставщиками ресурсов:

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

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

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

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

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

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

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

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

⚠ Для взаимодействия с сервером терминалов (MS RDS или STAL) необходимо установить специализированный агент в соответствии с подразделом **Установка сессионного Агента** документа СЛЕТ.10001-02 90 04 «Руководство администратора. Настройка компонента «Агент».

⚠ STAL реализуется компонентом «Сервер терминалов», который нужно установить на узел в соответствии с подразделом **Установка STAL** документа СЛЕТ.10001-02 90 06 «Руководство администратора. Настройка компонента «Сервер терминалов».

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

Таблица 3 – Данные для добавления сервера терминалов

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

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

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

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

4.3 . Режим техобслуживания поставщика ресурсов

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

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

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

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

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

5 . АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

5.1 . Общие сведения о доменах аутентификации

Домен аутентификации - источник сведений о субъектах и их полномочиях.

В Termidesk поддерживаются следующие домены аутентификации:

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

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

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

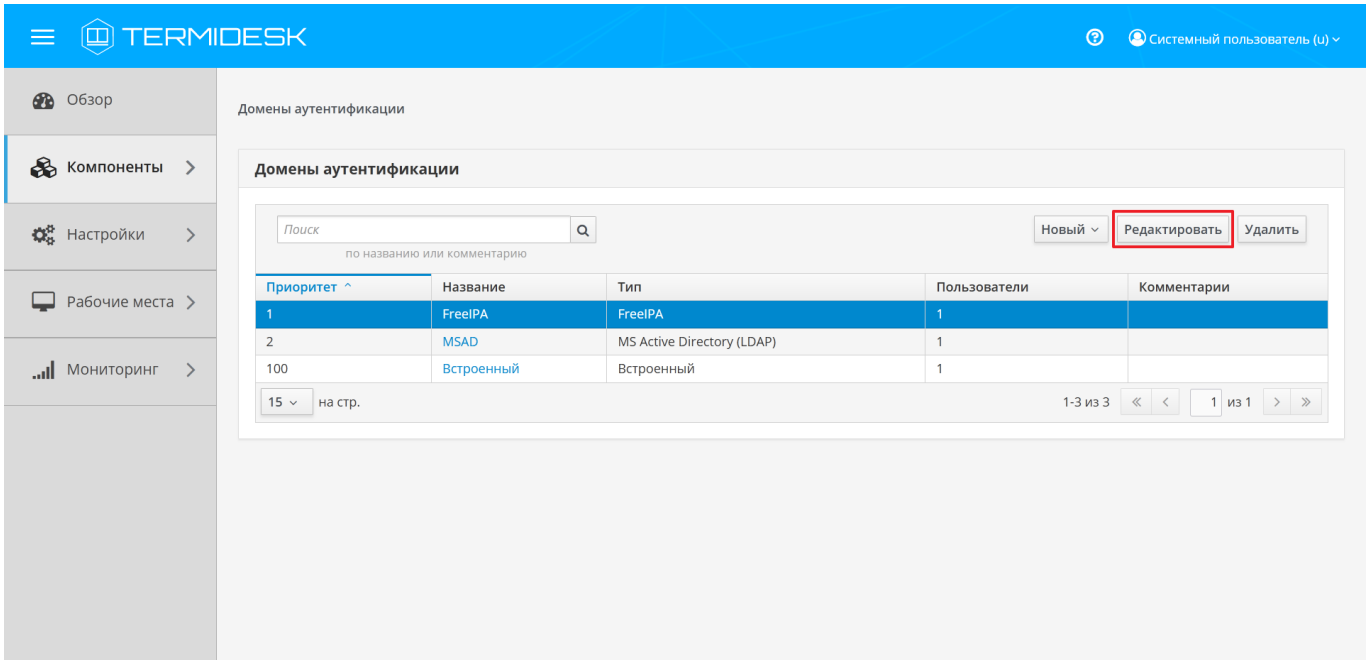

Рисунок 4 – Окно выбора домена аутентификации для редактирования

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 `Kerberos`. Для получения `keytab`-файла на контроллере домена и добавления его на сервер, где установлен Termidesk, необходимо выполнить ряд действий.

Действия на контроллере домена (например, FreeIPA):

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

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

- выполнить команду для добавления узла:

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

где:

`--force` - флаг для принудительного создания;

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

`IP_disp1.termidesk.local` - IP-адрес сервера, где установлен Termidesk,
`disp.termidesk.local` - мнимый FQDN узла в текущем домене (в примере `termidesk.local`);

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

- выполнить команду добавления службы для нового сервисного аккаунта:

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

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

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

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

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

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

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

где:
`localuser` - имя пользователя целевого узла;
`IP_disp.termidesk.local` - IP-адрес целевого узла.

После передачи файла на узле Termidesk необходимо выполнить следующее:

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

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

- сделать владельцем этого файла пользователя `termidesk`:

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

- перезапустить службу `termidesk-vdi`:

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

5.2.2 . Перечень параметров для добавления аутентификации через FreeIPA

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

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

Таблица 4 – Данные для добавления аутентификации через FreeIPA

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Сервисный аккаунт»	Название сервисного аккаунта, созданного при добавлении поставщика ресурсов
«Домен»	Идентификатор области Kerberos для аутентификации
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (файл `keytab`)
«Сервер FreeIPA»	FQDN ресурса, являющегося источником сведений о субъектах и их полномочиях
«Проверка SSL»	Проверка использования SSL
«Группа администраторов»	Название группы, членам которой предоставляются права администрирования Termidesk

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

5.3 . Добавление аутентификации через ALD

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

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

Таблица 5 – Данные для добавления аутентификации через ALD

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

5.4 . Добавление аутентификации через SAML

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

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

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

Таблица 6 – Данные для добавления аутентификации через SAML

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

5.5 . Добавление IP-аутентификации

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

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

Таблица 7 – Данные для добавления IP-аутентификации

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации

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

5.6 . Добавление аутентификации через MS AD (LDAP)

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

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

Таблица 8 – Данные для добавления аутентификации через MS AD (LDAP)

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения домена аутентификации
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Адрес LDAP»	IP-адрес или доменное имя ресурса, являющегося источником сведений о субъектах и их полномочиях
«Порт»	TCP-порт, на котором запущена служба домена аутентификации
«Использовать SSL»	Использовать защищенное соединение при взаимодействии с доменом аутентификации
«Bind DN»	Объект в MS AD (LDAP), имеющий полномочия для доступа к конкретной записи
«Bind DN password»	Набор символов, подтверждающий полномочия объекта по доступу к конкретной записи

Параметр	Описание
«Timeout»	Время ожидания (в секундах) ответа ресурса, являющегося источником сведений о субъектах и их полномочиях
«Base DN»	Корень поиска в домене аутентификации
«User class name»	Атрибут класса пользователя в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «Person»)
«User attr id»	Идентификатор пользователя в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «SamAccountName»)
«User attrs name»	Идентификатор имени пользователя в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «name»)
«Group class name»	Атрибут принадлежности к группе в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «group»)
«Group attr name»	Идентификатор группы, к которой относится субъект в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «cn»)
«Group attr membership»	Идентификатор группы для назначения полномочий субъекту (для корректного заполнения данного поля необходимо указать значение «member»)

5.7 . Добавление аутентификации через внутреннюю БД

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

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

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

Таблица 9 – Данные для добавления аутентификации через внутреннюю БД

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях

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

5.8 . Действия над пользователями в домене аутентификации

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

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

- редактирование;
- удаление;
- просмотр сведений.

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

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

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

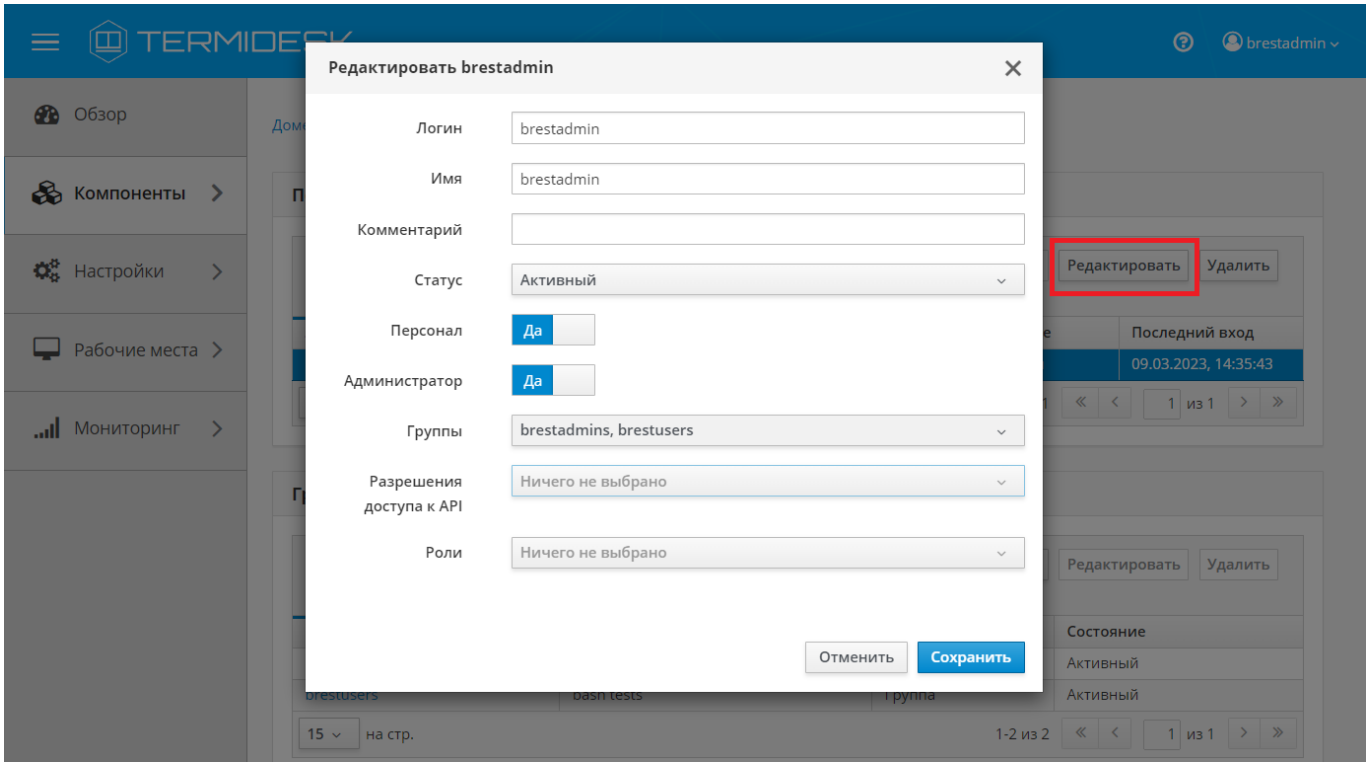

Рисунок 5 – Окно редактирования пользователя домена аутентификации

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

Таблица 10 – Данные для редактирования пользователя домена аутентификации

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

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

5.9 . Управление аутентификацией на основе адресов сети

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

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

Таблица 11 – Данные для добавления аутентификации на основе адресов сети

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

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

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

6 . ВИРТУАЛЬНЫЕ РАБОЧИЕ МЕСТА

6.1 . Общие сведения о BPM

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

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

Шаблоны серверов терминалов предполагают создание BPM на основе терминального доступа или доступа к опубликованным на сервере терминалов приложениям.

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

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

Созданные шаблоны BPM можно редактировать, для этого надо выбрать шаблон, а затем нажать экранную кнопку **[Редактировать]**.

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

Шаблон может быть удален только в том случае, если он не используется фондом BPM.

6.2 . Шаблоны BPM для серверов терминалов

6.2.1 . Шаблон BPM для доступа к серверу терминалов MS RDS

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

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

Таблица 12 – Данные для добавления шаблона для доступа к терминалу MS RDS

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

6.2.2 . Шаблон BPM для доступа к опубликованным приложениям MS RDS

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

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

Таблица 13 – Данные для добавления шаблона для доступа к приложениям MS RDS

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

6.2.3 . Шаблон BPM для доступа к серверу терминалов STAL

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

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

Таблица 14 – Данные для добавления шаблона для доступа к терминалу STAL

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

6.2.4 . Шаблон BPM для доступа к опубликованным приложениям STAL

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

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

Таблица 15 – Данные для добавления шаблона для доступа к приложениям STAL

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

6.3 . Активация технологии единого входа на сервере терминалов MS RDS

Для включения SSO на MS RDS нужно выполнить следующее:

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

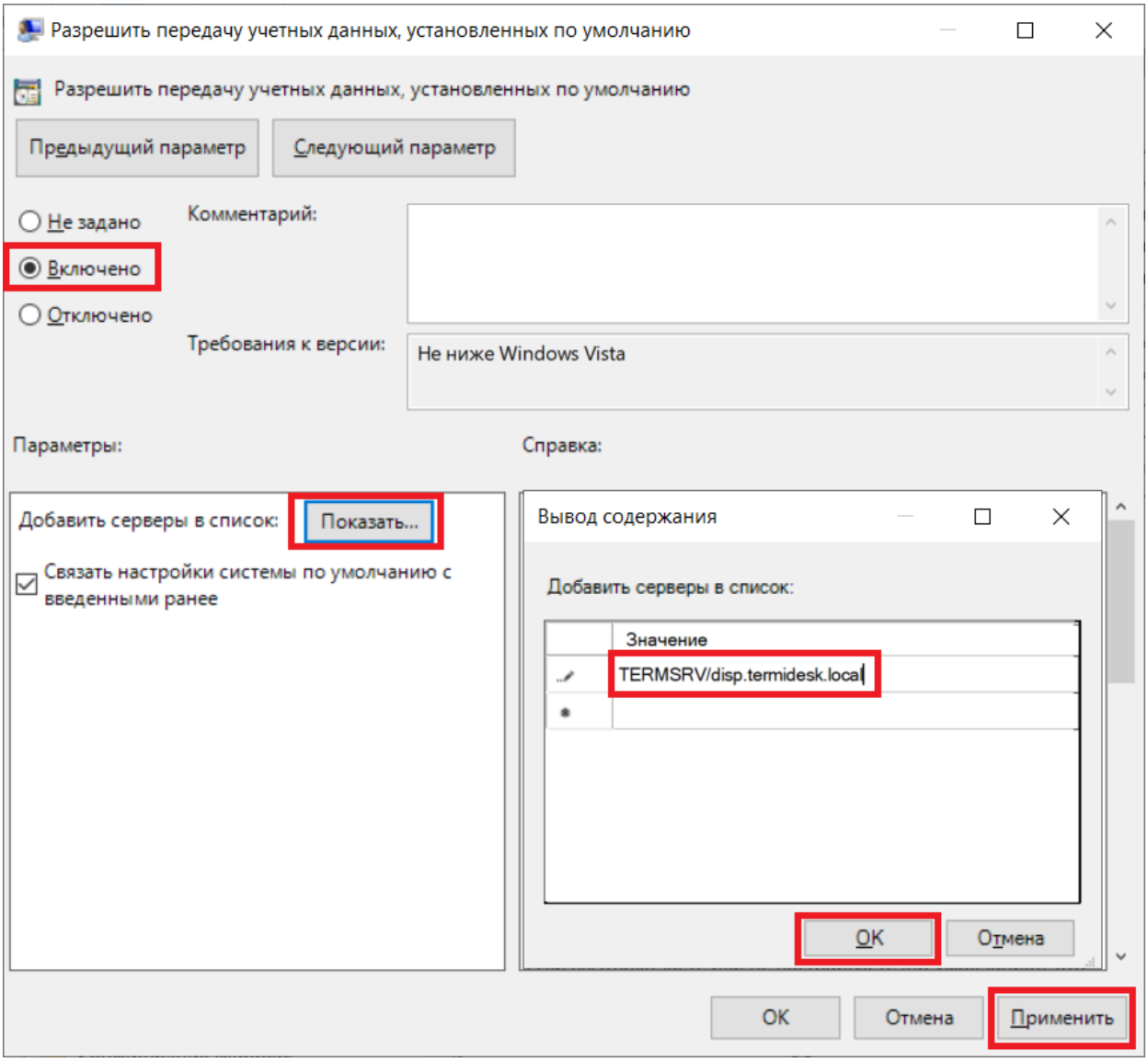

Рисунок 6 – Редактирование параметра «Разрешить передачу учетных данных, установленных по умолчанию» групповых политик

- в этом же списке выбрать параметр «Разрешить передачу новых учетных данных с проверкой подлинности сервера «только NTLM» и присвоить ему значение «Включено». Затем нажать экранную кнопку **[Добавить серверы в список]** и задать значение «TERMSRV/disp.termidesk.local», где `disp.termidesk.local` - имя сервера Termidesk. Далее нажать экранные кнопки **[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 нужно форсировать применение политики, то на контроллере домена, MS RDS и рабочих станциях пользователей надо 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 . Управление параметрами гостевых ОС в Termidesk

7.1.1 . Общие сведения

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

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

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

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

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

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

7.1.2 . Параметры гостевой ОС Windows

7.1.2.1 . Конфигурация без домена

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

Таблица 16 – Данные для гостевой ОС Windows без ввода в домен

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС

Параметр	Описание
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Длительность сессии пользователя»	Время (в секундах), которое ожидает Termidesk, прежде чем будет запущена процедура принудительного выхода пользователя из ОС

7.1.2.2 . Конфигурация при вводе в домен MS AD

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

Таблица 17 – Данные для гостевой ОС Windows при вводе в домен MS AD

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

7.1.3 . Параметры гостевой ОС Linux

7.1.3.1 . Конфигурация без домена

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

Таблица 18 – Данные для гостевой ОС Linux без ввода в домен

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

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

7.1.3.2 . Конфигурация при вводе в домен MS AD

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

Таблица 19 – Данные для гостевой ОС Linux при вводе в домен MS AD

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

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

7.1.3.3 . Конфигурация при вводе в домен FreeIPA

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

Таблица 20 – 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 ВРМ к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий
«Длительность сессии пользователя»	Время (в секундах), которое ожидает Termidesk, прежде чем будет запущена процедура принудительного выхода пользователя из ОС

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

7.1.3.4 . Конфигурация при вводе в домен ALD

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

Таблица 21 – Данные для гостевой ОС Linux при вводе в домен ALD

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен аутентификации»	Идентификатор домена ALD
«Аккаунт»	Идентификатор субъекта, имеющий полномочия по добавлению ВРМ к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий
«Длительность сессии пользователя»	Время (в секундах), которое ожидает Termidesk, прежде чем будет запущена процедура принудительного выхода пользователя из ОС

7.1.4 . Действие при выходе пользователя из ОС

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

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

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

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

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

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

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

7.1.5 . Изменение изображения гостевых ОС

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

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

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

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

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

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

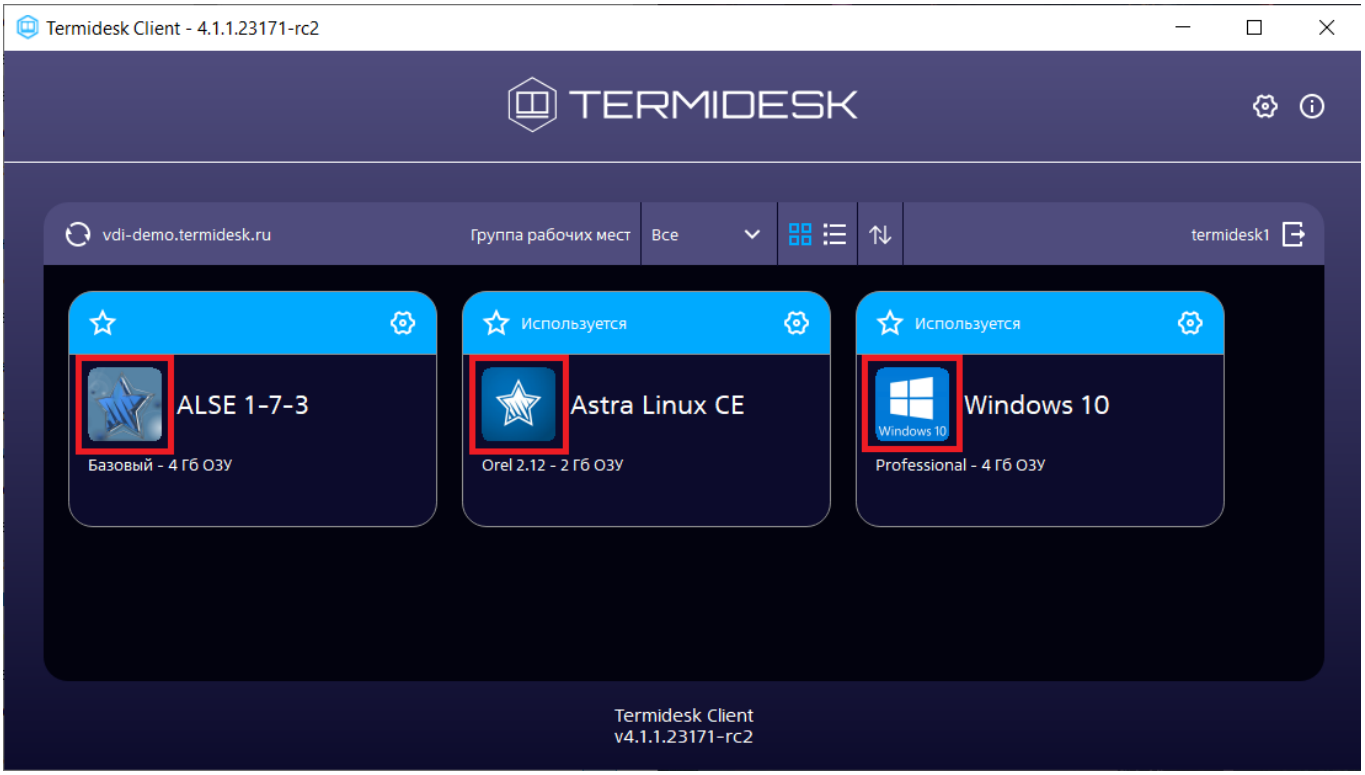

Рисунок 7 – Отображение назначенных изображений в сеансе пользователя

8 . ФОНД РАБОЧИХ МЕСТ

8.1 . Общие сведения о фонде BPM

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

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

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

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

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

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

На открывшейся странице будут представлены следующие разделы:

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

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

8.2 . Добавление фонда BPM

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

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

Таблица 22 – Данные для добавления фонда BPM

Параметр	Описание
«Название»	Текстовое наименование фонда BPM

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

8.3 . Глобальные политики фонда BPM

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

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

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

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

Таблица 23 – Доступные параметры глобальных политик фонда BPM

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

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

8.4 . Объединение фондов в группы ВРМ

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

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

Таблица 24 – Данные для объединения фондов ВРМ в группы

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

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

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

8.5 . Назначение пользователей доступа

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

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

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

8.6 . Назначение групп доступа фонду BPM

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

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

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

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

8.7 . Назначение протоколов фонду BPM

Фонду BPM можно назначать доступные для него протоколы доставки.

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

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

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

8.8 . Управление сессиями подключенных к фонду BPM пользователей

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

Для просмотра основных сведений об активных сессиях пользователей в фондах BPM следует перейти «Рабочие места - Сессии», после чего откроется сводная таблица.
Для принудительного отключения сессии пользователя следует перейти «Рабочие места - Сессии». В таблице с актуальной информацией об текущих активных сессиях пользователей BPM необходимо пометить сессию пользователя для отключения и нажать экранную кнопку **[Отключить]**.

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

8.9 . Отправка сообщения в BPM

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

9 . ПРОТОКОЛЫ ДОСТАВКИ

9.1 . Общие сведения о протоколах доставки

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

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

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

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

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

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

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

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

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

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

Таблица 25 – Данные для добавления прямого подключения к серверам терминалов

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде BPM
«Без домена»	Не использовать идентификатор домена при проверке полномочий субъекта
«Домен»	Идентификатор домена при проверке полномочий субъекта. Должно использоваться короткое имя домена

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

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

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

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

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

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

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

Таблица 26 – Данные для добавления подключения к серверам терминалов через «Шлюз»

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде BPM
«URL шлюза»	Адрес сервера в формате `ws(s)://ip-address_or_FQDN/websockify`, обеспечивающего формирование и поддержание соединения. Директива `ws` относится к использованию порта 80, директива `wss` означает использование 443 порта. Параметр `ip-address_or_FQDN` - доступный IP-адрес шлюза. Значение этого параметра не относится к значению `WSPROXY_BIND_ADDRESS` из конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf`
«Время ожидания соединения»	Время ожидания (в секундах) отклика шлюза
«Без домена»	Не использовать идентификатор домена при проверке полномочий субъекта
«Домен»	Идентификатор домена при проверке полномочий субъекта. Должно использоваться короткое имя домена
«Порт»	Выбор порта для подключения. По умолчанию используется порт 3389

Параметр	Описание
«Разрешить смарт-карты»	Разрешить идентификацию субъектов на основе смарт-карт
«Разрешить принтеры»	Разрешить перенаправление устройств печати по протоколу RDP
«Все принтеры»	Выполнить перенаправление всех устройств печати по протоколу RDP. При выключенном параметре «Разрешить принтеры» данный параметр игнорируется
«Разрешить диски»	Разрешить перенаправление устройств хранения по протоколу RDP
«Разрешить последовательные порты»	Разрешить перенаправление последовательных портов по протоколу RDP
«RemoteFX»	Использовать технологию RemoteFX
«Показывать обои»	Отображать фоновое изображение, настроенное на рабочем столе
«Все RemoteFX устройства»	Использовать все RemoteFX устройства
«Несколько мониторов»	Разрешить использовать несколько мониторов
«Разрешить композицию рабочего стола»	Разрешить темы рабочего стола
«Сглаживание шрифтов»	Использовать технологию сглаживания шрифтов
«Поддержка CredSSP»	Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider
«Мультимедиа синхронизация»	Использовать синхронизацию с `xfreerdp`
«Использовать ALSA»	Использовать программный микшер для передачи звука
«Параметры смарт-карты»	Указать конфигурацию идентификации по смарт-картам
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к BPM. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к BPM

10 . СИСТЕМНЫЕ НАСТРОЙКИ

10.1 . Общие системные параметры Termidesk

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

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

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

Таблица 27 – Общие системные параметры Termidesk

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

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

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

10.2 . Параметры безопасности Termidesk

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

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

Таблица 28 – Параметры безопасности Termidesk

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

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

10.3 . Назначение служебных функций администраторам

В Termidesk реализовано разделение доступных служебных функций для администраторов.

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

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

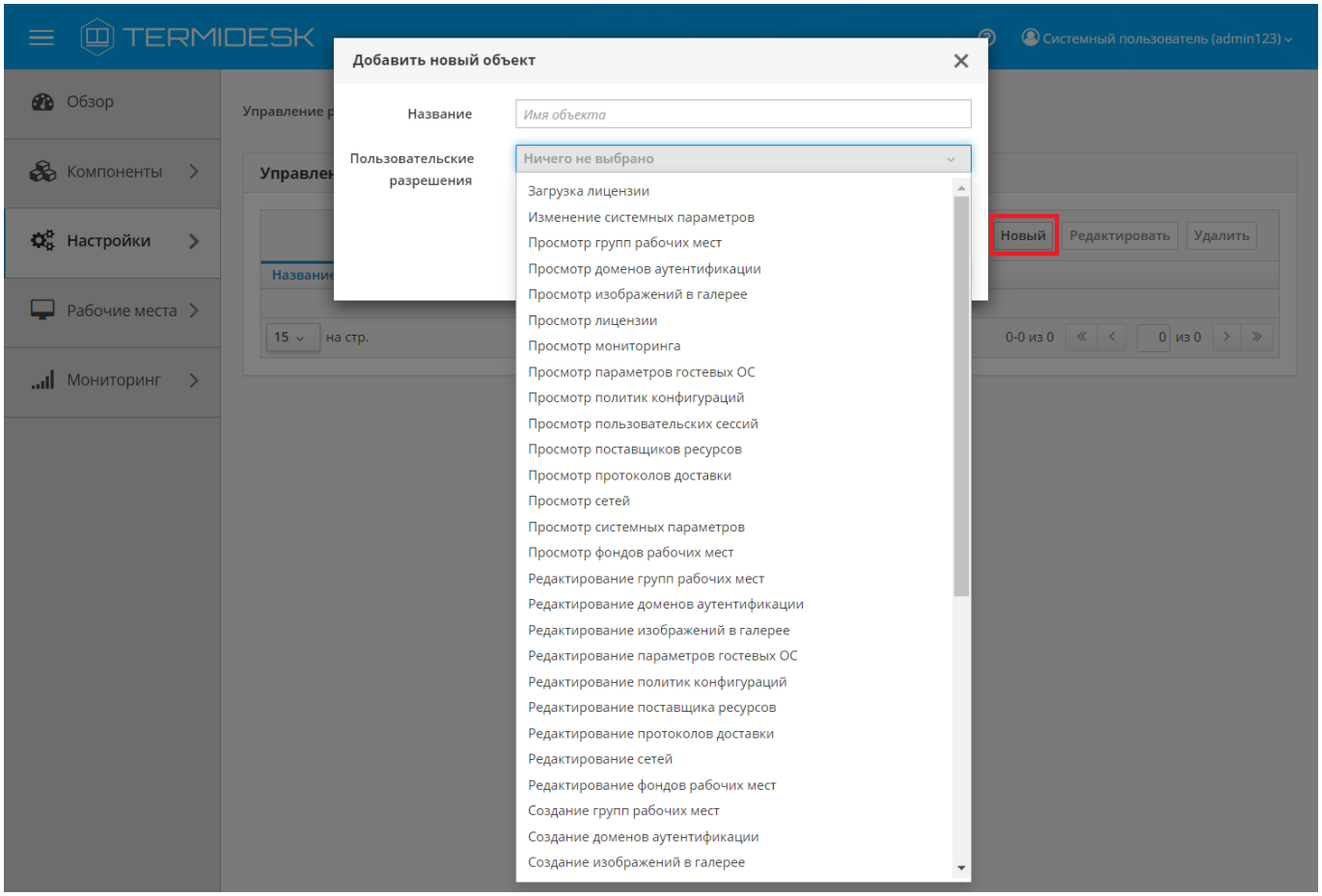

Рисунок 8 – Окно назначения пользовательских разрешений

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

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

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

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

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

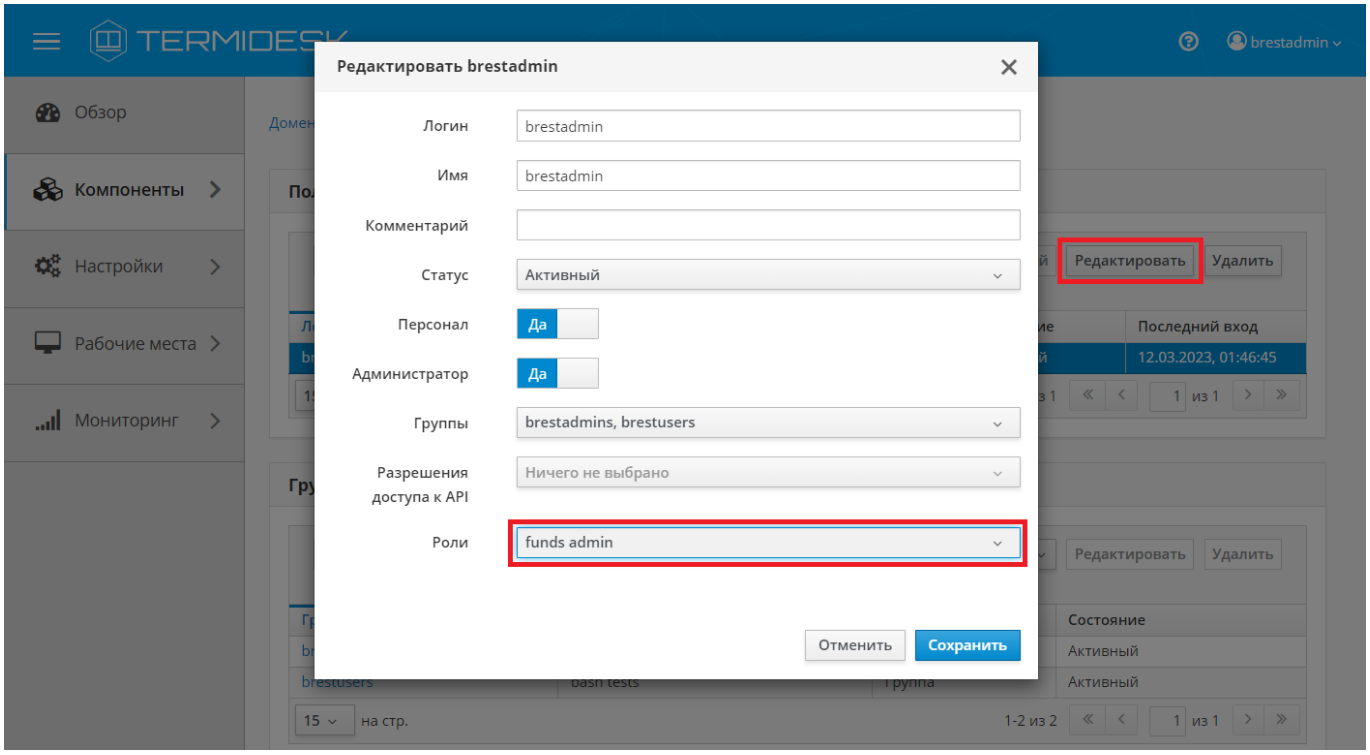

Рисунок 9 – Окно назначения пользовательских ролей

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

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

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

Таблица 29 – Доступные параметры при добавлении пользовательских разрешений для фондов BPM

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

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

11 . МОНИТОРИНГ И УВЕДОМЛЕНИЯ

11.1 . Системные параметры мониторинга

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

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

Таблица 30 – Параметры мониторинга Termidesk

Параметр	Описание
«Логирование Syslog»	Перенаправление потока событий мониторинга на отдельный syslog-сервер
«Хост 1» — «Хост 3»	IP-адреса или имена узлов, на которых развернута служба syslog-сервера
«Протокол»	Выбор протокола работы для службы syslog-сервера
«Категория сообщения»	Выбор категории сообщений, которые будут записываться в журнал мониторинга
«Уровень логирования»	Выбор уровня логирования событий (`INFO`, `WARNING`, `ERROR`, `CRITICAL`, `DEBUG`)

11.2 . Настройка отправки уведомлений о системных событиях

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

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

Таблица 31 – Параметры отправки уведомлений о событиях

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

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

11.3 . Уведомление об ошибках аутентификации в графическом интерфейсе управления

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

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

11.4 . Шаблон для мониторинга Zabbix

Termidesk поддерживает мониторинг состояния компонентов через `Zabbix`.

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

В шаблоне находятся метрики для мониторинга компонентов сервера Termidesk: универсального диспетчера, шлюза, менеджера BPM.
Реализованы как простые проверки (подключение к портам), так и опрос состояния служб `health checking`.

11.5 . Отчеты

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

Можно сформировать следующие отчеты:

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

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

Таблица 32 – Параметры для формирования отчета по последнему пользовательскому входу в Termidesk

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

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

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

Таблица 33 – 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 надо нажать экранную кнопку **[Новый]**, выбрать тип отчета «Отчет по пользовательским подключениям» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы.

Таблица 34 – 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.

12 . СИСТЕМА АУДИТА

12.1 . Системные параметры аудита

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

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

Таблица 35 – Системные параметры аудита

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

12.2 . Журналы

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

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

- `auth.log` - записываются события об авторизации субъектов в Ternidesk;

- `celery-beat.log` - записываются события периодической проверки состояния обработчика заданий через RabbitMQ;
- `celery-worker.log` - записываются события обработчика заданий через RabbitMQ;
- `other.log` - записываются события, не относящиеся к другим модулям;
- `sql.log` - записываются отладочные события БД;
- `termidesk.log` - записываются события работы сервера Termidesk;
- `use.log` - записываются события пользователей BPM;
- `workers.log` - записываются события обработчика фоновых задач;
- `wsproxy.log` - записываются события компонента «Шлюз»;
- `stal_proxy.log` - записываются события службы `proxy` компонента «Сервер терминалов»;
- `stal_service.log` - записываются события службы `stal` компонента «Сервер терминалов».

12.3 . Настройка журналирования

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

Для изменения уровня журналирования необходимо:

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

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

12.4 . Просмотр журналов

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

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

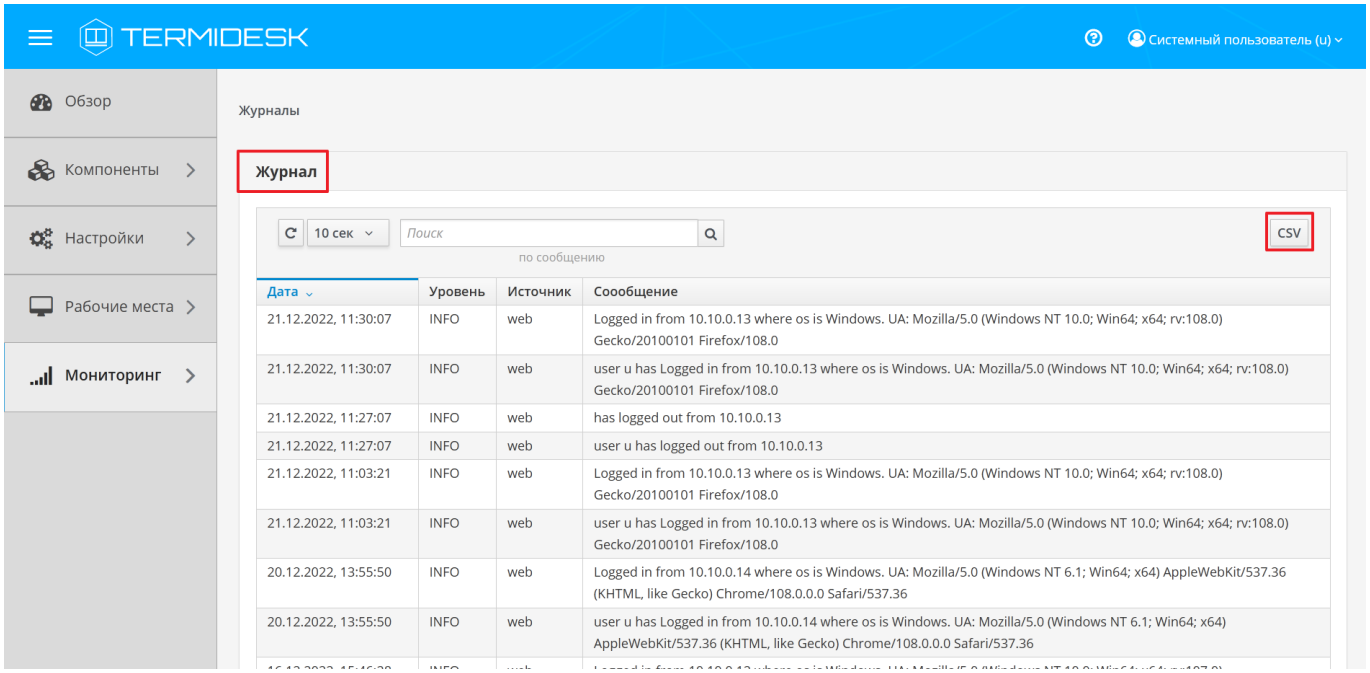

Рисунок 10 – Отображение общего журнала в графическом интерфейсе управления Termidesk

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

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

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

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

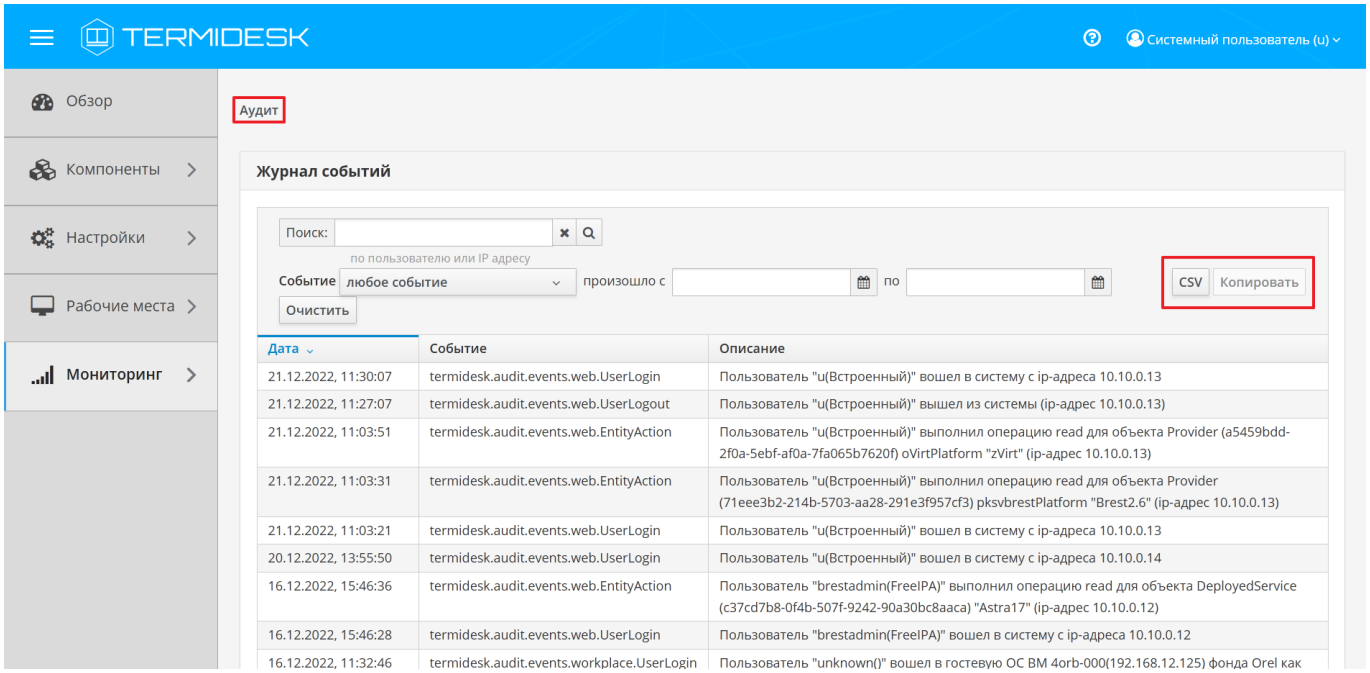

Рисунок 11 – Отображение журнала аудита в графическом интерфейсе управления Termidesk

13 . РЕЖИМ ВЫСОКОЙ ДОСТУПНОСТИ И РАБОТА С СЕРТИФИКАТАМИ

13.1 . Настройка менеджера BPM в режиме высокой доступности

Настройка выполняется после установки программного комплекса в распределенной конфигурации.

Последовательность настройки узлов с менеджером BPM следующая:

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

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

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

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

где:

`-y` - ключ для пропуска подтверждения установки;

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

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

где:

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

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

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

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

```
global_defs {

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

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

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

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

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

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

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

    preempt_delay 5 # Seconds

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

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

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

    virtual_ipaddress {
```

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

    track_script {
        check_httpd
    }
}
```

где:

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

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

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

VIRTUAL_IP_ADDRESS/MASK - виртуальный статический IP-адрес и маска (общие для узлов master и slave);

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

```
#!/bin/sh -e

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

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

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

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

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

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

13.2 . Настройка балансировщика для работы с самоподписанными сертификатами

13.2.1 . Создание самоподписанного SSL-сертификата

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

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

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

Используемые ключи команды:

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

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

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

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

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

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

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

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

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

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

13.2.2 . Настройка nginx для поддержки SSL

Для настройки nginx нужно:

- создать новый пустой 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:

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

- создать еще один пустой сниппет, предназначенный для настроек SSL (это позволит серверу nginx использовать надежный механизм преобразования и включит некоторые дополнительные функции безопасности):

```
:~$ sudo touch /etc/nginx/snippets/ssl-params.conf
```

- отредактировать созданный файл `ssl-params.conf`, приведя его к виду:

```
ssl_protocols TLSv1.2;
ssl_prefer_server_ciphers on;
ssl_dhparam /etc/nginx/dhparam.pem;
ssl_ciphers ECDHE-RSA-AES256-GCM-SHA512:DHE-RSA-AES256-GCM-SHA512:ECDHE-RSA-AES256-GCM-
SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384;
ssl_ecdh_curve secp384r1; # Requires nginx >= 1.1.0
ssl_session_timeout  10m;
ssl_session_cache shared:SSL:10m;
ssl_session_tickets off; # Requires nginx >= 1.5.9
ssl_stapling on; # Requires nginx >= 1.3.7
ssl_stapling_verify on; # Requires nginx => 1.3.7
resolver 77.88.8.8 77.88.8.1 valid=300s;
resolver_timeout 5s;
# Disable strict transport security for now. You can uncomment the following
# line if you understand the implications.
# add_header Strict-Transport-Security "max-age=63072000; includeSubDomains; preload";
add_header X-Frame-Options DENY;
add_header X-Content-Type-Options nosniff;
add_header X-XSS-Protection "1; mode=block";
```

⚠ Поскольку сертификат является самоподписанным, `SSL stapling` не будет использоваться. Сервер nginx выдаст предупреждение, отключит `stapling` для данного сертификата и продолжит работу.

13.2.3 . Конфигурирование веб-сервера

Для конфигурирования веб-сервера нужно:

- создать пустой конфигурационный файл:

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

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

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

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

}

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

     server 192.168.0.30;
     server 192.168.0.31;
     server 192.168.0.32;

 }

server {
 listen 0.0.0.0:80;
 listen 0.0.0.0:443 ssl;

  include snippets/self-signed.conf;
  include snippets/ssl-params.conf;

 location /websockify {
         # limit_req zone=fast nodelay;
        proxy_http_version 1.1;
        proxy_pass http://daas-upstream-ws/;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";

        # Connection timeout
        proxy_connect_timeout 1000;
        proxy_send_timeout 1000;
        proxy_read_timeout 1000;
        send_timeout 1000;
```

```
        # Disable cache
        proxy_buffering off;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 }

 location / {
        proxy_pass http://daas-upstream-nodes/;

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

 }

}
```

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

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

```
:~$ sudo ln -s /etc/nginx/sites-available/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 соединения будут шифроваться правильно.

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

```
:~$ sudo systemctl restart nginx
```

14 . ЭКСПЕРИМЕНТАЛЬНЫЕ ФУНКЦИИ

14.1 . Перечень переменных окружения универсального диспетчера

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

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

Таблица 36 – Переменные окружения Termidesk

Переменная окружения	Значение по умолчанию	Описание
Установочный пакет termidesk-vdi		
TDSK_PKG_DEBUG	Не задано	Включение режима отладки при установке пакета. Пример: TDSK_PKG_DEBUG=1

14.2 . Управление экспериментальными параметрами Termidesk

Включение и отключение экспериментальных параметров сервера Termidesk производится из командной строки.

Перечень экспериментальных параметров приведен в таблице.

Таблица 37 – 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

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.

14.3 . Установка плагинов расширений

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

Для установки плагинов нужно на сервере Termidesk выполнить следующее:

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

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

- перейти в каталог `Termidesk`:

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

- активировать виртуальное окружение `Termidesk`:

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

- установить необходимый плагин:

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

где:

`/tmp/termidesk_internaldbauth` - каталог с `whl`-файлами;

`termidesk_internaldbauth` - имя плагина (без версии, платформы и расширения файла);

- выйти из окружения пользователя `Termidesk`:

```
:~$ exit
```

- обновить структуру БД и статических файлов командами:

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

- перезапустить службы Termidesk:

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

14.4 . Удаление плагинов расширений

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

Для удаления плагина расширений нужно на сервере Termidesk выполнить следующее:

- переключиться на пользователя `Termidesk`:

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

- перейти в каталог `Termidesk`:

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

- активировать виртуальное окружение `Termidesk`:

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

- удалить необходимый плагин:

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

где:

`termidesk_internaldbauth` - имя плагина (без версии, платформы и расширения файла);

- выйти из окружения пользователя `Termidesk`:

```
:~$ exit
```

- перезапустить службы Termidesk:

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

14.5 . Откат к предыдущей версии плагина

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

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

где:

`/tmp/termidesk_internaldbauth` - каталог с `whl`-файлами, `whl`-файл с версией плагина должен существовать в данном каталоге;
`termidesk_internaldbauth` - имя плагина с указанием версии.

15 . ТИПОВЫЕ НЕИСПРАВНОСТИ

15.1 . Нештатные ситуации и способы их устранения

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

Таблица 38 – Перечень возможных нештатных ситуаций

Индикация	Описание	Возможное решение
Ошибка: «СБОЙ: оставшиеся слоты подключений зарезервированы для подключений суперпользователя (не для репликации)»	Ошибка возникает при попытке авторизации на сервере Termidesk	Изменить максимальное количество подключений в настройках БД: изменить значение `max_connections` в конфигурационном файле `/etc/postgresql/11/main/postgresql.conf` в бОльшую сторону
Ошибка: «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: «kinit: Client 'HTTP/termidesk.local@LOCAL' not found in Kerberos database while getting initial credentials»	Ошибка возникает при добавлении или редактировании домена аутентификации FreeIPA	Необходимо создать указанную учетную запись на КД FreeIPA

Индикация	Описание	Возможное решение

Ошибка при установке пакета: «Невозможно найти пакет» или «Неудовлетворенные зависимости»	Ошибка возникает при попытке установить пакет в ОС	Необходимо убедиться, что в файле `/etc/apt/sources.list` заданы и не закомментированы источники получения пакетов (репозитории), затем обновить списки пакетов:
		`:~$ sudo apt update`
		После этого нужно вновь выполнить команду установки пакета.
		Для решения проблемы с неудовлетворенными зависимостями, помимо подключения репозиториев в файле `/etc/apt/sources.list`, можно воспользоваться командой:
		`:~$ sudo apt -f install`
		Ключ `-f` используется для попытки исправить нарушенные зависимости пакетов.

Ошибка при установке пакета: «Невозможно найти пакет» или «Неудовлетворенные зависимости»	Ошибка возникает при попытке установить пакет в ОС	Необходимо убедиться, что в файле `/etc/apt/sources.list` заданы и не закомментированы источники получения пакетов (репозитории), затем обновить списки пакетов:
		`:~$ sudo apt update`
		После этого нужно вновь выполнить команду установки пакета.
		Для решения проблемы с неудовлетворенными зависимостями, помимо подключения репозиториев в файле `/etc/apt/sources.list`, можно воспользоваться командой:
		`:~$ sudo apt -f install`
		Ключ `-f` используется для попытки исправить нарушенные зависимости пакетов

16 . ПЕРЕЧЕНЬ ТЕРМИНОВ

Термин	Определение
Балансировщик нагрузки	Самостоятельный компонент, отвечающий за распределение нагрузки на множество универсальных диспетчеров и шлюзов
ВРМ	Виртуальное рабочее место: гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа
Группы рабочих мест	Также: «группы ВРМ». Функциональное объединение множества фондов ВРМ по определенному признаку
Домен аутентификации	Способ проверки субъектов и их полномочий
Менеджер рабочих мест	Также: «планировщик заданий», «менеджер ВРМ». Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом ВРМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-taskman.service`
Поставщик ресурсов	В варианте лицензирования «Termidesk Terminal»: терминальный сервер (MS RDS/STAL), предоставляющий вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов ВРМ
Протокол доставки	Поддерживаемый в Termidesk протокол удаленного доступа к ВРМ
Сессионный агент	Устанавливается на сервер терминалов (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям. Устанавливается из пакета `termidesk-session-agent`
Универсальный диспетчер	Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им ВРМ и контроля доставки ВРМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service`
Фонд рабочих мест	Также: «фонд ВРМ». Совокупность подготовленных ВРМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей
Шаблон рабочего места	Также: «шаблон ВРМ». Параметры конфигурации базового ВРМ для использования в фонде ВРМ

Термин	Определение
Шлюз	Отделяемый компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-wsproxy.service`
STAL	Сервер терминалов Astra Linux. Реализован компонентом «Сервер терминалов» Termidesk. Устанавливается из пакета `stal`

17 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

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

Сокращение	Пояснение
SAML	Security Assertion Markup Language (открытый стандарт обмена данными аутентификации)
SSL	Secure Sockets Layer (криптографический протокол)
SSO	Single Sign-On (технология единого входа)
STAL	Terminal Server Astra Linux (сервер терминалов ОС Astra Linux Special Edition (Server))
TCP	Transmission Control Protocol (протокол управления передачей)
Termidesk	Программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk»
TLS	Transport Layer Security (протокол защиты транспортного уровня)
UDP	User Datagram Protocol (протокол пользовательских датаграмм)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
VRRP	Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности)

Адрес: 119415, г. Москва, проспект Вернадского, дом 41, строение 1, офис 645а
Сайт: www.termidesk.ru
Телефон: +7 (495) 975-1-975

Общий e-mail: info@uveon.ru
Отдел продаж: sales@uveon.ru
Техническая поддержка: support@uveon.ru