



РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-01 90 01

Версия 4.3.2. Выпуск от января 2024

Установка программного комплекса

ОГЛАВЛЕНИЕ

1 .	ОБЩИЕ СВЕДЕНИЯ.....	5
1.1 .	О документе.....	5
1.2 .	Назначение.....	5
1.3 .	Область применения.....	5
1.4 .	Основные характеристики.....	5
1.5 .	Требования к уровню подготовки персонала.....	8
1.6 .	Типографские соглашения.....	8
2 .	ТРЕБОВАНИЯ К СРЕДЕ ФУНКЦИОНИРОВАНИЯ.....	10
2.1 .	Требования к аппаратному обеспечению.....	10
2.2 .	Требования к программному обеспечению.....	10
2.3 .	Требования к синхронизации времени.....	10
2.4 .	Требования к DNS и DHCP.....	10
2.5 .	Требования к серверам каталогов.....	10
2.6 .	Требования к серверам терминалов.....	11
2.7 .	Требования к платформе виртуализации.....	11
3 .	ИСПОЛЬЗОВАНИЕ КОНТЕКСТУАЛИЗАЦИИ ПК СВ БРЕСТ.....	14
3.1 .	Контекстуализация в ПК СВ Брест.....	14
4 .	ПОДГОТОВКА СРЕДЫ ФУНКЦИОНИРОВАНИЯ.....	15
4.1 .	Установка СУБД Postgres-11.....	15
4.2 .	Настройка СУБД Postgres-11.....	16
4.3 .	Установка брокера сообщений RabbitMQ-server.....	17
4.4 .	Настройка брокера сообщений RabbitMQ-server.....	17
5 .	УСТАНОВКА ПРОГРАММНОГО КОМПЛЕКСА.....	22
5.1 .	Получение пакетов установки в ОС Astra Linux Special Edition.....	22
5.2 .	Установка и настройка отделяемых компонентов на одном узле.....	24
5.2.1 .	Автоматизированная установка.....	24

5.2.1.1 . Автоматизированная установка через исполняемый файл	24
5.2.1.2 . Автоматизированная установка через файл ответов	24
5.2.2 . Неавтоматизированная установка Termidesk.....	27
5.3 . Распределенная установка программного комплекса.....	37
5.3.1 . Основные принципы распределенной установки.....	37
5.3.2 . Установка и настройка СУБД Postgres-11.....	40
5.3.3 . Установка первого узла с универсальным диспетчером Termidesk	40
5.3.4 . Установка узлов - шлюзов подключений.....	41
5.3.5 . Установка узлов - менеджеров ВРМ	41
5.3.6 . Установка балансировщиков.....	41
5.3.7 . Действия после распределенной установки	42
5.4 . Отказоустойчивая установка Termidesk.....	42
5.4.1 . Основные принципы отказоустойчивой установки.....	42
5.4.2 . Установка и настройка СУБД Postgres-11.....	40
5.4.3 . Установка основного узла Termidesk	45
5.4.4 . Перенос каталога с конфигурационными файлами и ключами	46
5.4.5 . Установка резервных узлов Termidesk	46
5.4.6 . Проверка работоспособности узлов Termidesk	46
5.4.7 . Настройка узлов в режиме высокой доступности	47
5.5 . Установка программного комплекса в режиме замкнутой программной среды.....	51
5.6 . Проверка работоспособности после установки.....	52
6 . ОБНОВЛЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА.....	54
6.1 . Комплексное обновление Termidesk.....	54
6.2 . Обновление для распределенной конфигурации установки.....	56
6.2.1 . Общая концепция обновления	56
6.2.2 . Шаг 1: установка и настройка RabbitMQ-server	58
6.2.3 . Шаг 2: резервное копирование RSA-ключей	58
6.2.4 . Шаг 3: редактирование конфигурации балансировщика нагрузки	59

6.2.5 .	Шаг 4: редактирование конфигурации остальных балансировщиков нагрузки.....	59
6.2.6 .	Шаг 5: обновление диспетчера	60
6.2.7 .	Шаг 6: восстановление RSA ключей из резервной копии.....	60
6.2.8 .	Шаг 7: обновление следующего по списку диспетчера	60
6.2.9 .	Шаг 8: восстановление конфигурации балансировщика нагрузки	61
6.2.10 .	Шаги 9-14: обновление шлюзов	61
6.2.11 .	Шаг 15: останов служб на менеджере BPM	62
6.2.12 .	Шаг 16: обновление менеджеров BPM	62
6.2.13 .	Шаг 17: восстановление RSA ключей на менеджере BPM	62
6.2.14 .	Шаг 18: восстановление службы keepalived.....	63
6.2.15 .	Шаги 19-22: обновление основного менеджера BPM	63
7 .	УДАЛЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА	64
8 .	ЛИЦЕНЗИРОВАНИЕ	66
8.1 .	Получение лицензионного ключа.....	66
8.2 .	Ввод лицензии	68
8.3 .	Проверка сведений о лицензии.....	68
9 .	ПЕРЕЧЕНЬ ТЕРМИНОВ	69
10 .	ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	71

1 . ОБЩИЕ СВЕДЕНИЯ

1.1 . О документе

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

В первой части руководства приведено назначение и установка Termidesk. Для того, чтобы получить информацию о настройке Termidesk, необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

1.2 . Назначение

Termidesk предназначен для доставки виртуальных рабочих мест (ВРМ) и приложений, организации терминального доступа пользователей к ресурсам посредством различных протоколов удаленного доступа.

1.3 . Область применения

Termidesk может применяться для создания или модернизации инфокоммуникационной инфраструктуры масштаба предприятия, а также поставщиками услуг, реализующих облачную услугу ВРМ.

Termidesk ориентирован на образовательные и иные организации, в которых предусмотрено использование одного ВРМ множеством лиц, с возможностями очистки ВРМ по завершению сеанса работы.

Termidesk подходит для применения в сети предприятий с разветвленной филиальной сетью.

Termidesk позволяет реализовать политики повышенных требований к безопасности данных, препятствующих несанкционированному распространению информации. Помимо этого, Termidesk обеспечивает работу с виртуализированными графическими адаптерами (vGPU) и адаптацией к низкоскоростным каналам связи.

1.4 . Основные характеристики

Termidesk состоит из ряда компонентов, которые могут быть либо отделяемыми (подразумевает выбор роли при установке из общего пакета), либо самостоятельными (компонент устанавливается из отдельного пакета, но используется в составе общего комплекса). Такое разделение обеспечивает гибкое масштабирование системы для различных сценариев применения.

В состав Termidesk входят следующие компоненты:

- «Универсальный диспетчер» - компонент, отвечающий за идентификацию пользователей, назначение и контроля доставки им ВРМ;
- «Шлюз» - компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP;
- «Менеджер рабочих мест» - компонент, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом ВРМ, включая создание, настройку, запуск, отключение и удаление;
- «Агент» - компонент, отвечающий за контролируруемую доставку ВРМ, взаимодействие с универсальным диспетчером и менеджером ВРМ;
- «Клиент» - компонент, отвечающий за доставку ВРМ на пользовательскую рабочую станцию с возможностью перенаправления периферии, каталогов, и оптимизацию их использования в протоколе доставки;
- «Оркестратор» - компонент, отвечающий за автоматизацию развертывания Termidesk в облачных структурах;
- «Сервер терминалов» - компонент, отвечающий за организацию терминального доступа в ОС Astra Linux Special Edition;
- «Удаленный помощник» - компонент, предоставляющий администратору или специалисту технической поддержки экран узла пользователя через сеанс удаленного подключения и обеспечивающий передачу голосовой информации для взаимодействия с пользователем;
- «Виртуальный модуль Termidesk» - компонент, представляющий собой образ виртуальной машины (ВМ) (или диска ВМ) с предварительно установленной и настроенной операционной системой (ОС) и набором программного обеспечения, необходимого для эксплуатации Termidesk. Компонент позволяет быстро развернуть и использовать компоненты «Универсальный диспетчер», «Шлюз», «Менеджер рабочих мест»;
- «Termidesk Live» - компонент, представляющий собой загрузочный образ ОС с предустановленным компонентом «Клиент».

Компоненты «Универсальный диспетчер», «Шлюз», «Менеджер рабочих мест» являются отделяемыми и могут устанавливаться как в комплексном варианте, так и в распределенной конфигурации.

Параметры конфигурирования отделяемых компонентов приведены в следующих документах:

- СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»;
- СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз».

Компоненты «Агент», «Клиент», «Оркестратор», «Сервер терминалов», «Удаленный помощник», «Virtual Appliance», «Termidesk Live» являются самостоятельными, но работающими в составе программного комплекса.

К компоненту «Агент» относятся следующие подкомпоненты, каждый из которых устанавливается отдельно:

- агент ВРМ (устанавливается в гостевую ОС ВМ);
- агент узла виртуализации (устанавливается на узел виртуализации);
- сессионный агент (устанавливается на узел сервера терминалов);
- видеоагент (устанавливается в гостевую ОС ВМ);
- агент виртуальных смарт-карт (устанавливается в гостевую ОС ВМ).

Параметры установки и конфигурирования компонента «Агент» приведены в документе СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент».

Параметры установки и конфигурирования компонента «Клиент» приведены в документе СЛЕТ.10001-01 92 01 «Руководство пользователя. Настройка и эксплуатация компонента «Клиент».

Параметры установки и конфигурирования компонента «Оркестратор» приведены в документе СЛЕТ.10001-01 90 06 «Руководство администратора. Настройка компонента «Оркестратор».

Параметры установки и конфигурирования компонента «Сервер терминалов» приведены в документе СЛЕТ.10001-01 90 07 «Руководство администратора. Настройка компонента «Сервер терминалов».

Использование компонента «Удаленный помощник» приведено в документе СЛЕТ.10001-01 91 02 «Инструкция по использованию. Компонент «Удаленный помощник».

Использование компонента «Virtual Appliance» приведено в документе СЛЕТ.10001-01 91 03 «Инструкция по использованию. Компонент «Virtual Appliance».

Использование компонента «Termidesk Live» приведено в документе СЛЕТ.10001-01 91 04 «Инструкция по использованию. Компонент «Termidesk Live».

Termidesk обеспечивает доставку ВРМ на пользовательскую рабочую станцию посредством следующих протоколов:

- SPICE;
- RDP;
- VNC;
- Loudplay.

Для протоколов доставки Termidesk реализует режим прямого и туннельного соединения. Прямое соединение позволяет подключиться к протоколу, запущенному внутри гостевой ОС или на гипервизоре. Туннельное соединение применяется при подключении ВРМ из недоверенных сетей. Комбинация протоколов доставки и способы подключения predeterminedены в Termidesk.

Termidesk поддерживает работу с платформами виртуализации:

- программный комплекс «Средства виртуализации «Брест» (далее – ПК СВ Брест);
- VMmanager;

- zVirt;
- oVirt;
- «РЕД Виртуализация»;
- Openstack (версия Xen);
- VMware vSphere.

Termidesk поддерживает работу с серверами терминалов и публикации приложений:

- Microsoft Windows Server с ролью «Remote Desktop Session Host» из состава «Remote Desktop Services» (далее - MS RDS, MS RDSH);
- Terminal Server Astra Linux (далее - STAL). Реализуется компонентом «Сервер терминалов».

1.5 . Требования к уровню подготовки персонала

Для штатной эксплуатации Termidesk требуется следующий персонал:

- системный администратор;
- специалист по техническому обслуживанию.

Системный администратор должен иметь опыт работы с платформами виртуализации и администрирования серверов с ОС Astra Linux Special Edition 1.7.

Основными обязанностями системного администратора являются:

- установка, настройка и мониторинг работоспособности Termidesk;
- регламентные работы;
- восстановление работоспособности Termidesk после устранения неисправностей комплекса технических средств.

Специалист по техническому обслуживанию должен иметь опыт работы с ОС Astra Linux Special Edition 1.7, знать и понимать принципы работы сетей передачи данных, а также владеть базовыми знаниями по обслуживанию комплекса технических средств.

Основными обязанностями специалиста по техническому обслуживанию являются:

- настройка, модернизация и проверка состояния комплекса технических средств;
- диагностика типовых неисправностей комплекса технических средств;
- настройка сетевых подключений.

1.6 . 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 . ТРЕБОВАНИЯ К СРЕДЕ ФУНКЦИОНИРОВАНИЯ

2.1 . Требования к аппаратному обеспечению

Для установки Termidesk минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры Intel x86 с разрядностью 64 бит;
- оперативная память, не менее 4 ГБ;
- свободное дисковое пространство, не менее 1 ГБ;
- сетевое соединение, не менее 100 Мбит/с.

2.2 . Требования к программному обеспечению

В среде функционирования Termidesk должны быть предварительно установлены:

- ОС Astra Linux Special Edition версии 1.7 (и выше);
- СУБД Postgres-11 из состава репозитория ОС Astra Linux Special Edition версии 1.7;
- программный брокер сообщений RabbitMQ-server версии 3.7.8 (и выше) из состава репозитория ОС Astra Linux Special Edition версии 1.7.

ОС Astra Linux Special Edition версии 1.7 должна быть установлена из iso-образа, доступного в личном кабинете на портале Astra Linux: <https://lk-new.astralinux.ru/>. Работа Termidesk на преднастроенных образах ОС не гарантируется.

2.3 . Требования к синхронизации времени

В сетевой инфраструктуре должен быть настроен NTP-сервер, обеспечивающий синхронизацию времени для «Универсального диспетчера», «Шлюза», «Менеджера рабочих мест».

2.4 . Требования к DNS и DHCP

В сетевой инфраструктуре должны быть развернуты и исправно функционировать службы доменных имен (DNS) и автоматического назначения сетевых параметров (DHCP) в необходимых сегментах сети.

Службы DNS и DHCP могут быть реализованы как отдельно, так и средствами платформы виртуализации (например, контекстуализацией ПК СВ Брест).

2.5 . Требования к серверам каталогов

Серверы каталогов должны удовлетворять следующим требованиям:

- сервер каталогов должен размещаться в том же сегменте локальной сети, где будут развернуты ВРМ. Если выполнение требования невозможно и сервер каталогов находится в другом сегменте, то необходимо обеспечить маршрутизацию между этими сегментами;
- при использовании в качестве сервера каталогов Microsoft Active Directory (MS AD) необходимо создать сервисную учетную запись для взаимодействия Termidesk с контроллером домена (КД). Допускается использование учетной записи администратора домена;
- при использовании MS AD рекомендуется создавать отдельные организационные подразделения (OU) для пользователей ВРМ и для учетных записей типа «Компьютер» для самих ВРМ. Права на OU для компьютеров должны быть либо у созданной сервисной учетной записи, либо у отдельной созданной учетной записи, допускается также использовать учетную запись администратора домена;
- при использовании серверов каталогов FreeIPA и ALDPro в качестве сервисной учетной записи для взаимодействия Termidesk с КД по умолчанию используется учетная запись администратора домена, либо отдельная учетная запись с аналогичными полномочиями.

 Механизм подключения к LDAP-серверу `simple bind` передает данные для подключения в открытом виде.

2.6 . Требования к серверам терминалов

При использовании сервера терминалов Microsoft необходимо наличие внутри домена MS AD серверов с соответствующими ролями (MS RDSH - роль сервера терминалов, MS RDS - роль сервера публикации приложений).

2.7 . Требования к платформе виртуализации

Узлы виртуализации должны удовлетворять следующим требованиям:

- должна быть поддержка виртуального чипсета (`ich9-intel-hda`);
- пул в настройках DHCP или параметрах контекстуализации должен поддерживать достаточное количество IP-адресов;
- виртуальный коммутатор платформы должен поддерживать достаточное количество MAC-адресов;
- в платформе виртуализации должны быть реализованы именованные каналы, необходимые для работы Termidesk:
 - для перенаправления каталогов - `org.spice-space.webdav.0(/dev/virtio-ports/org.spice-space.webdav.0)`;
 - для взаимодействия с libvirt (необходим компоненту «Агент узла виртуализации») - `ru.termidesk.tvm.0 (/dev/virtio-ports/ru.termidesk.tvm.0)`;

- для включения перенаправления видеокамеры - `ru.termidesk.RealtimeStreaming.0 (/dev/virtio-ports/ru.termidesk.RealtimeStreaming.0)`;
- канал для включения перенаправления смарт-карт - `ru.termidesk.PCSC.0 (/dev/virtio-ports/ru.termidesk.PCSC.0)`;
- канал для включения перенаправления принтера - `ru.termidesk.Printer.0 (/dev/virtio-ports/ru.termidesk.Printer.0)`.

Для ПК СВ Брест включение именованных каналов определяется конфигурационным файлом / `etc/one/vmm_exec/vmm_exec_kvm.conf`, который находится на фронтальных машинах ПК СВ Брест.

Для включения каналов необходимо на узле системы виртуализации ПК СВ Брест предварительно сделать следующее:

- установить компонент «Агент узла виртуализации» (подробно о назначении и установке компонента см. документ СЛЕТ.10001-01.90.04 «Руководство администратора. Настройка компонента «Агент») командой:

```
~$ sudo apt install python3-termidesk-vmtd
```

- убедиться, что состояние службы компонента «Агент узла виртуализации» находится в состоянии «active (running)» командой:

```
~$ systemctl status termidesk-vmtd
```

Затем на фронтальной машине ПК СВ Брест выполнить активацию именованных каналов:

- открыть на редактирование файл `/etc/one/vmm_exec/vmm_exec_kvm.conf`;
- присвоить параметрам `WEBDAV_USE_DEFAULT`, `VIDEOCAM_OPTIMIZATION_USE_DEFAULT`, `PRINTER_OPTIMIZATION_USE_DEFAULT`, `USBTOKEN_OPTIMIZATION_USE_DEFAULT`, `SPIECE_DETECT_USE_DEFAULT` значение «yes». Пример фрагмента файла с нужными значениями:

```

1  #rbt: webdav use
2  WEBDAV_USE_DEFAULT="yes"
3  WEBDAV_OPTIONS=""
4      <channel type='spiceport'>
5          <source channel='org.spice-space.webdav.0' />
6          <target type='virtio' name='org.spice-space.webdav.0' />
7      </channel>"
8
9  #rbt: camera optimization
10 VIDEOCAM_OPTIMIZATION_USE_DEFAULT="yes"
11 VIDEOCAM_OPTIMIZATION_OPTIONS=""
12     <channel type='spiceport'>
13         <source channel='TDSK_STREAM' />
14         <target type='virtio' name='ru.termidesk.RealtimeStreaming.0' />

```

```

15     </channel>"
16
17     #rbt: printer optimization
18     PRINTER_OPTIMIZATION_USE_DEFAULT="yes"
19     PRINTER_OPTIMIZATION_OPTIONS=""
20     <channel type='spiceport'>
21         <source channel='TDSK_PRINTER' />
22         <target type='virtio' name='ru.termidesk.Printer.0' />
23     </channel>"
24
25     #rbt: USB token optimization
26     USBTOKEN_OPTIMIZATION_USE_DEFAULT="yes"
27     USBTOKEN_OPTIMIZATION_OPTIONS=""
28     <channel type='spiceport'>
29         <source channel='TDSK_PCSC' />
30         <target type='virtio' name='ru.termidesk.PCSC.0' />
31     </channel>"
32
33     #rbt: SPICE detect
34     SPICE_DETECT_USE_DEFAULT="yes"
35     SPICE_DETECT_OPTIONS=""
36     <channel type='unix'>
37         <source mode='connect' path='/var/run/tvmd.sock' >
38             <reconnect enabled='yes' timeout='1' />
39         </source>
40         <target type='virtio' name='ru.termidesk.tvmd.0' />
41     </channel>"
    
```

⚠ Присвоение параметру `SPICE_DETECT_USE_DEFAULT` значения «yes» должно происходить только после установки на узлы системы виртуализации компонента «Агент узла виртуализации» и успешного запуска его службы.

- сохранить изменения в файле `/etc/one/vmm_exec/vmm_exec_kvm.conf`;
- перезапустить службу `opennebula`:

```
:~$ sudo systemctl restart opennebula
```

3. ИСПОЛЬЗОВАНИЕ КОНТЕКСТУАЛИЗАЦИИ ПК СВ БРЕСТ

3.1 . Контекстуализация в ПК СВ Брест

В ПК СВ Брест применяется метод контекстуализации для отправки информации на ВМ во время загрузки. Основная задача метода — передача настроек сети и учетных данных на ВМ для ее настройки. Дополнительная задача – передача индивидуальных сценариев для загрузки ВМ.

i Использование метода контекстуализации ПК СВ Брест не является обязательным, однако значительно упрощает и автоматизирует процесс подготовки узлов с компонентами Termidesk.

Для включения контекстуализации в гостевой ОС Astra Linux нужно в базовый образ установить пакет `one-context`:

```
~$ sudo apt install one-context
```

Если после выполнения команды появляются сообщения об ошибке «Невозможно найти пакет `one-context`», «Пакеты имеют неудовлетворенные зависимости» 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 `one-context`.

Для включения контекстуализации в гостевой ОС Windows нужно включить службу, обрабатывающую скрипты контекстуализации. Для этого следует установить пакет `one-context-6.2.0` или более новый.

Параметры непосредственно контекста задаются в шаблоне ВМ, для этого в панели управления ПК СВ Брест надо открыть шаблон ВМ и перейти во вкладку «Контекст».

4. ПОДГОТОВКА СРЕДЫ ФУНКЦИОНИРОВАНИЯ

- ❗ Если Termidesk планируется устанавливать автоматизированно согласно подразделу **Автоматизированная установка**, то подготовку среды функционирования выполнять не нужно.

4.1 . Установка СУБД Postgres-11

Для установки СУБД Postgres-11 необходимо:

- отредактировать файл `/etc/apt/sources.list`, оставив в качестве источников получения пакетов сетевые репозитории. Для этого закомментировать строку, начинающуюся с `deb cdrom`. Должен получиться следующий список:

```

1 # Astra Linux repository description https://wiki.astralinux.ru/x/0oLiC
2
3 #deb cdrom:[OS Astra Linux 1.7.3 1.7_x86-64 DVD ]/ 1.7_x86-64 contrib main non-
  free
4 deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/
  1.7_x86-64 main contrib non-free
5 deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update/
  1.7_x86-64 main contrib non-free
6
7 deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/
  1.7_x86-64 main contrib non-free
8 deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/
  1.7_x86-64 main contrib non-free
    
```

- ❗ Если в файле `/etc/apt/sources.list` присутствует репозиторий `astra-ce`:
`# Расширенный репозиторий (компонент astra-ce)`
`deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 astra-ce`
 необходимо закомментировать его, чтобы избежать установки несовместимых версий пакетов.

- перейти в интерфейс командной строки через программу «Терминал Fly», выполнить команду обновления списков пакетов:

```
:~$ sudo apt update
```

- выполнить команду установки СУБД Postgres-11:

```
:~$ sudo apt install -y postgresql-11
```

где:

`-y` - ключ для пропуска подтверждения установки.

4.2 . Настройка СУБД Postgres-11

Перед установкой Termidesk нужно выполнить настройку базы данных (БД).

Для настройки БД следует перейти в интерфейс командной строки и выполнить следующее:

- переключиться последовательно на пользователя root, затем на postgres:

```
1  :~$ sudo -s
2  :/home/astra# su postgres
```

- запустить терминальный клиент СУБД Postgres-11:

```
:/home/astra$ psql
```

⚠ Если после выполнения команды отображается ошибка «could not change directory to "/home/": Отказано в доступе» и не появляется приглашение командной строки postgres=#, необходимо вместо «su postgres» использовать конструкцию «su - postgres». Если приглашение postgres=# появилось, то сообщение об ошибке можно проинигорировать.

- используя интерактивный интерфейс терминального клиента СУБД, создать БД termidesk (символ «;» в конце строки при работе с интерактивным интерфейсом обязателен):

```
postgres=# CREATE DATABASE termidesk LC_COLLATE 'ru_RU.utf8' LC_CTYPE 'ru_RU.utf8'
TEMPLATE template0;
```

где:

LC_COLLATE - порядок сортировки для использования в БД, влияет на порядок сортировки, применяемый к строкам. Значение «ru_RU.utf8» указывает на использование русской локализации;

LC_CTYPE - классификация символов для использования в БД, влияет на категоризацию символов;

TEMPLATE - имя шаблона, из которого создается БД. Шаблон «template0» используется для системной БД самой СУБД Postgres-11.

- создать пользователя termidesk с паролем ksedimret для дальнейшего подключения к БД:

```
postgres=# CREATE USER termidesk WITH PASSWORD 'ksedimret';
```

⚠ В приведенной команде имя пользователя и пароль используются в качестве примера. Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты.

- назначить права по использованию БД termidesk созданному пользователю termidesk:

```
postgres=# GRANT ALL PRIVILEGES ON DATABASE termidesk TO termidesk;
```

- выйти из интерактивного интерфейса терминального клиента СУБД:

```
postgres=# \q
```

- выйти из сеансов пользователей postgres и root:

```
1  :/home/astra$ exit
2  :/home/astra# exit
```

- отредактировать файл /etc/parsec/mswitch.conf, установив параметр zero_if_notfound в значение yes, точно соблюдая отступы и пробелы:

```
1  # Return zero data instead of ENOENT/ENODATA in the absence of record
2  zero_if_notfound: yes
```

⚠ В случае последующего обновления СУБД Postgres может понадобится пересоздание БД. В этом случае следует предусмотреть экспорт БД перед обновлением СУБД Postgres.

4.3 . Установка брокера сообщений RabbitMQ-server

⚠ Если узел с уже установленным RabbitMQ-server будет переименован, то брокер сообщений перестанет принимать подключения. Для исправления ситуации необходимо удалить RabbitMQ-server, затем выполнить его переустановку.

Для установки RabbitMQ-server нужно перейти в интерфейс командной строки через программу «Терминал Fly» и выполнить команду:

```
:~$ sudo apt install -y rabbitmq-server
```

где:

-y - ключ для пропуска подтверждения установки.

4.4 . Настройка брокера сообщений RabbitMQ-server

Для настройки RabbitMQ-server следует:

- перейти в интерфейс командной строки через программу «Терминал Fly» и убедиться в наличии каталога /etc/rabbitmq:

```
:~$ ls /etc/
```

- если каталог отсутствует, необходимо создать его:

```

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

где:

- p - ключ для автоматического создания директорий, указанных внутри пути;
- перейти в каталог /etc/rabbitmq:

```

:~$ cd /etc/rabbitmq
    
```

- создать пустые файлы rabbitmq.conf (основной файл конфигурации RabbitMQ-server) и definitions.json (файл определения данных для подключения):

```

1  :~$ sudo touch rabbitmq.conf
2  :~$ sudo touch definitions.json
    
```

- поменять владельца (rabbitmq) и идентификатор группы (rabbitmq) для созданных файлов:

```

:~$ sudo chown rabbitmq:rabbitmq definitions.json rabbitmq.conf
    
```

- отредактировать файл rabbitmq.conf, приведя его к виду:

```

1  # ===== Management section
   # =====
2  ## Preload schema definitions from the following JSON file.
3  ## Related doc guide: https://rabbitmq.com/management.html#load-definitions.
4  ##
5  # management.load_definitions = /path/to/exported/definitions.json
6  management.load_definitions = /etc/rabbitmq/definitions.json
    
```

⚠ Если необходимо, чтобы RabbitMQ работал через TLS-соединение, то файл rabbitmq.conf нужно привести к виду:

```

1  # ===== Management section
   # =====
2  ## Preload schema definitions from the following JSON file.
3  ## Related doc guide: https://rabbitmq.com/management.html#load-
   definitions.
4  ##
5  # management.load_definitions = /path/to/exported/definitions.json
6  management.load_definitions = /etc/rabbitmq/definitions.json
7  listeners.tcp.default = 5672
8
9  # TLS Port
10 listeners.ssl.default = 5671
11
12 ssl_options.cacertfile = /var/ssl/root-ca.crt
13 ssl_options.certfile   = /var/ssl/cert.crt
14 ssl_options.keyfile    = /var/ssl/private/private-key.key
15
    
```

```

16 # Should peer verification be enabled?
17 ssl_options.verify      = verify_peer
18
19 # When set to true, TLS connection will be rejected if client fails to
    provide a certificate
20 ssl_options.fail_if_no_peer_cert = false
21
22 ssl_options.versions.default = tlsv1.2
    
```

Предполагается, что файлы корневого сертификата (/var/ssl/root-ca.crt), сертификата узла (/var/ssl/cert.crt) и закрытого ключа (/var/ssl/private/private-key.key) к нему уже существуют и доступны по указанному пути.

- отредактировать файл definitions.json, задав пользователей termidesk и admin, приведя его к виду:

⚠ В файле /etc/rabbitmq/definitions.json пароли указываются в виде преобразованного значения, которое можно получить через исполняемый файл rabbitmq_password2hash.sh. Подробно о том, как преобразовать пароль, приведено далее.

```

1  {
2    "rabbit_version": "3.7.8",
3    "users": [
4      {
5        "name": "termidesk",
6        "password_hash": "pnXiDJtUdk7Zcel9i0qx44PeDgRa+X1+eIq+7wf/PTONLb1h",
7        "hashing_algorithm": "rabbit_password_hashing_sha256",
8        "tags": ""
9      },
10     {
11       "name": "admin",
12       "password_hash": "FXQ9WFNSrsGwRki9BT2dCITnsDwYu2lsy7BEN7+UncsPzCDZ",
13       "hashing_algorithm": "rabbit_password_hashing_sha256",
14       "tags": "administrator"
15     }
16   ],
17   "vhosts": [
18     {
19       "name": "/"
20     },
21     {
22       "name": "termidesk"
23     }
24   ],
25   "permissions": [
26     {
27       "user": "termidesk",
28       "vhost": "termidesk",
29       "configure": ".*",
30       "write": ".*",
31       "read": ".*"
    
```

```

32     },
33     {
34         "user": "admin",
35         "vhost": "termidesk",
36         "configure": ".*",
37         "write": ".*",
38         "read": ".*"
39     }
40 ],
41 "topic_permissions": [
42     {
43         "user": "termidesk",
44         "vhost": "termidesk",
45         "exchange": "",
46         "write": ".*",
47         "read": ".*"
48     }
49 ],
50 "parameters": [],
51 "global_parameters": [
52     {
53         "name": "cluster_name",
54         "value": "rabbit@rabbitmq"
55     }
56 ],
57 "policies": [],
58 "queues": [],
59 "exchanges": [],
60 "bindings": []
61 }
    
```

⚠ В примере используются следующие пары логин-пароль: admin:admin, termidesk:ksedimret. Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты.

- выполнить команду инициализации RabbitMQ-server:

```
:~$ sudo rabbitmq-plugins enable rabbitmq_management
```

- перезапустить RabbitMQ-server:

```
:~$ sudo systemctl restart rabbitmq-server
```

Чтобы получить преобразованное значение пароля нужно воспользоваться исполняемым файлом rabbitmq_password2hash.sh, расположенным в подключенном репозитории Termidesk (см. **Получение пакетов установки в ОС Astra Linux Special Edition**) по пути /var/repos/Addons/Scripts/:

- перейти в каталог `/var/repos/Addons/Scripts/`:

```
:~$ cd /var/repos/Addons/Scripts/
```

- задать файлу `rabbitmq_password2hash.sh` флаг для запуска:

```
:~$ sudo chmod +x rabbitmq_password2hash.sh
```

где:

`+x` - ключ установки разрешения на запуск файла для всех пользователей;

- выполнить исполняемый файл:

```
:~$ sudo ./rabbitmq_password2hash.sh
```

При выполнении исполняемого файла будет предложено ввести пароль и повторить его. Преобразованное значение введенного пароля будет отображено в интерфейсе командной строки. Необходимо внести полученное значение при формировании файла `/etc/rabbitmq/definitions.json` (секция `password_hash`).

Если конфигурационный файл `/etc/rabbitmq/definitions.json` уже существует, но требуется изменить значение преобразованного пароля в нем, нужно:

- выполнить преобразование и добавление пароля в файл `/etc/rabbitmq/definitions.json`:

```
:~$ sudo ./rabbitmq_password2hash.sh -w -u <user> -p <пароль>
```

где:

`-w` - ключ для сохранения изменений в файл `/etc/rabbitmq/definitions.json`;

`-u` - пользователь rabbitMQ. В стандартной установке можно указывать `admin`;

`-p` - пароль;

- перезапустить RabbitMQ-server:

```
:~$ sudo systemctl restart rabbitmq-server
```

5. УСТАНОВКА ПРОГРАММНОГО КОМПЛЕКСА

5.1. Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета программного обеспечения (ПО) в deb-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате iso-образа.

Получить iso-образ можно двумя способами:

- заполнив запрос через сайт Termidesk: <https://termidesk.ru/support/#request-support>;
- через личный кабинет: <https://lk-new.astralinux.ru/>.

Для подключения локального репозитория Termidesk на узле, где предполагается установка, нужно выполнить следующее:

- скопировать в домашний каталог пользователя образ диска `termidesk-⟨версия⟩.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
~$ sudo mount -o loop termidesk-⟨версия⟩.iso /mnt
```

где:

- o loop - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-⟨версия⟩.iso`, устройство затем монтируется в указанный каталог `/mnt`;
- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
~$ sudo cp -Rp /mnt/repos /var
```

где:

- Rp - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;
- отключить подключенный ранее образ диска от узла:

```
~$ sudo umount /mnt
```

- установить пакет `lsb-release`:

```
~$ sudo apt install -y lsb-release
```

где:

- y - ключ для пропуска подтверждения установки;

- добавить локальный репозиторий Termidesk (/var/repos/astra) в файл /etc/apt/sources.list.d/termidesk_local.list через командный интерпретатор sh:

```
1 :~$ sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs) non-free" > /etc/apt/sources.list.d/termidesk_local.list'
```

где:

-c - ключ для чтения команд из вводимой строки (стандартный ввод);

echo - команда вывода текста, совместно с символом «>» используется для перенаправления строки deb file:/var/repos/astra \$(lsb_release -cs) non-free в файл /etc/apt/sources.list.d/termidesk_local.list;

deb file:/var/repos/astra \$(lsb_release -cs) non-free - добавляемый репозиторий, вложенная команда \$(lsb_release -cs) подставляет версию - 1.7_x86-64;

- выполнить поиск ключа репозитория Termidesk GPG-KEY-PUBLIC и добавить его в ОС:

```
:~$ cat /var/repos/astra/GPG-KEY-PUBLIC | sudo apt-key add -
```

- убедиться, что ключ с uid «release@uveon.ru» был успешно добавлен:

```
:~$ apt-key list
```

⚠ В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ GPG-KEY-PUBLIC существует:

```
:~$ cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, необходимо проверить правильность выполнения шагов по добавлению репозитория Termidesk в файл /etc/apt/sources.list.d/termidesk_local.list.

При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

- обновить данные пакетного менеджера:

```
:~$ sudo apt update
```

Данную команду (sudo apt update) необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

5.2 . Установка и настройка отделяемых компонентов на одном узле

5.2.1 . Автоматизированная установка

5.2.1.1 . Автоматизированная установка через исполняемый файл

Для автоматизированной установки Termidesk без использования псевдографического интерфейса можно воспользоваться исполняемым файлом `termidesk-standalone.sh`, расположенным в подключенном репозитории Termidesk: `/var/repos/Addons/Scripts/`.

В этом случае **все действия** по подготовке среды функционирования и установки Termidesk будут выполнены исполняемым файлом.

⚠ Использование исполняемого файла для установки Termidesk допускается только в ознакомительных целях!

Для вызова процесса установки через исполняемый файл нужно:

- перейти в каталог `/var/repos/Addons/Scripts/`:

```
~$ cd /var/repos/Addons/Scripts/
```

- разархивировать файл `Termidesk.zip`:

```
~$ sudo unzip -j Termidesk.zip
```

где:

`-j` - ключ для разархивации всех файлов внутри `Termidesk.zip` в текущую директорию;

- задать файлу флаг для запуска:

```
~$ sudo chmod +x termidesk-standalone.sh
```

где:

`+x` - ключ установки разрешения на запуск файла для всех пользователей;

- запустить исполняемый файл:

```
~$ sudo ./termidesk-standalone.sh
```

5.2.1.2 . Автоматизированная установка через файл ответов

В ОС Astra Linux Special Edition есть возможность подготовить файл ответов, в котором можно указать определения и значения параметров для использования во время установки пакетов.

Для автоматизированной установки Termidesk через файл ответов необходимо:

- подготовить и сохранить файл ответов, пример файла приведен ниже;
- установить утилиту `debconf`, если она не установлена в ОС:

```
~$ sudo apt install debconf
```

- выполнить добавление файла ответов в утилиту debconf:

```
~$ sudo debconf-set-selections /home/user/notification_file
```

где:

/home/user/notification_file - путь к сохраненному файлу ответов.

Пример файла ответов:

```

1  # Вы принимаете условия пользовательской лицензии?
2  termidesk-vdi  termidesk-vdi/yesno-eula          boolean true
3
4  # true - интерактивный режим. false - пакетный (тихий) режим:
5  termidesk-vdi  termidesk-vdi/interactive        boolean false
6
7  # ПАРАМЕТРЫ ПОДКЛЮЧЕНИЯ К СУБД
8  # Адрес сервера СУБД Termidesk:
9  termidesk-vdi  termidesk-vdi/dbhost            string 127.0.0.1
10 # Добавлено в версии 4.1.1. Порт сервера (балансировщика) СУБД Termidesk:
11 termidesk-vdi  termidesk-vdi/dbport           string 5432
12 # Имя базы данных Termidesk:
13 termidesk-vdi  termidesk-vdi/dbname           string termidesk
14 # Пользователь базы данных Termidesk:
15 termidesk-vdi  termidesk-vdi/dbuser          string termidesk
16 # Пароль базы данных Termidesk:
17 termidesk-vdi  termidesk-vdi/dbpass          string ksedimret
18 # Добавлено в версии 4.3. Использование защищённого подключения к СУБД.
19 # Возможные варианты значений: Disable, TLSv1.2, TLSv1.3
20 # Значение по умолчанию: Disable
21 termidesk-vdi  termidesk-vdi/dbssl           select Disable
22
23 # ПАРАМЕТРЫ ПОДКЛЮЧЕНИЯ К СЕРВЕРАМ RABBITMQ
24 # RabbitMQ URL #1
25 termidesk-vdi  termidesk-vdi/rabbitmq_url1     password amqp://termidesk:ksedim
ret@127.0.0.1:5672/termidesk
26 # RabbitMQ URL #3
27 termidesk-vdi  termidesk-vdi/rabbitmq_url3     password
28 # RabbitMQ URL #2
29 termidesk-vdi  termidesk-vdi/rabbitmq_url2     password
30 # Добавлено в версии 4.3.1. Использование защищённого подключения к серверам RabbitMQ
31 # Возможные варианты значений: Disable, TLSv1.2
32 # Значение по умолчанию: Disable
33 termidesk-vdi  termidesk-vdi/rabbitmq_ssl      select Disable
34
35 # Добавлено в версии 4.1. Выбор устанавливаемых на узле ролей.
36 # Список, разделитель - запятые. Фактически, это выбор служб, которые будут
37 # автоматически запускаться. Доступные роли: Broker, Gateway, Task manager
38 # Если не требуется автоматический запуск служб (например, при использовании
39 # VRRP), то в качестве роли можно указать несуществующее название роли,
40 # например - Empty.

```

```

41 termidesk-vdi termidesk-vdi/roles string Broker, Gateway, Task manager
42
43 # Добавлено в версии 4.2.
44 # Тип веб-интерфейса. Имеет смысл при запуске демона termidesk-vdi (Выбор роли Broker
при установке пакета).
45 # admin - доступен только функционал администрирования,
46 # user - доступен только пользовательский функционал,
47 # universal - доступен как пользовательский, так и административный функционал.
48 # По умолчанию, используется режим universal
49 termidesk-vdi termidesk-vdi/webportaltype select universal
50
51 # НЕ ТРЕБУЮЩИЕСЯ ПЕРЕМЕННЫЕ, сугубо для справки
52 # Временные переменные для промежуточного хранения параметров подключения
53 # к серверу RabbitMQ, из которых создаются строки termidesk-vdi/rabbitmq_url1,
54 # termidesk-vdi/rabbitmq_url2, termidesk-vdi/rabbitmq_url3
55 # Choices: 1 amqp://termidesk:termidesk@127.0.0.1:5672/termidesk, 2 Empty, 3
Empty, Save
56 termidesk-vdi termidesk-vdi/rabbitmq_select select Save
57
58 # Termidesk RabbitMQ host
59 termidesk-vdi termidesk-vdi/rabbitmq_host string 127.0.0.1
60 # Termidesk RabbitMQ port
61 termidesk-vdi termidesk-vdi/rabbitmq_port string 5672
62 # Termidesk RabbitMQ user
63 termidesk-vdi termidesk-vdi/rabbitmq_user string termidesk
64 # Termidesk RabbitMQ pass
65 termidesk-vdi termidesk-vdi/rabbitmq_pass string termidesk
66 # Termidesk RabbitMQ Virtual Host
67 termidesk-vdi termidesk-vdi/rabbitmq_vhost string termidesk
68
69 # Временная переменная для промежуточного хранения выбора да/нет
70 termidesk-vdi termidesk-vdi/yesno boolean false
71 # Временная переменная для отображения сообщения на экране
72 termidesk-vdi termidesk-vdi/message note
73 # Временная переменная для отображения пользовательской лицензии
74 termidesk-vdi termidesk-vdi/text-eula note
    
```

❗ Выражение `termidesk-vdi termidesk-vdi/rabbitmq_url1 password amqp://termidesk:ksedimret@127.0.0.1:5672/termidesk` в блоке `# RabbitMQ URL #1` должно быть записано в одну строку!

⚠ Между типом параметра (`string`, `password`, `boolean` и т.д.) и значением параметра должен быть только один символ пробела.

ℹ В дальнейшем необходимые параметры для подготовки файла ответов могут быть получены командой:

```

:~$ sudo debconf-get-selections | grep -i termidesk
    
```

Команда выполняется в ОС, в которой установлен Termidesk.

5.2.2 . Неавтоматизированная установка Termidesk

Для установки Termidesk с использованием псевдографического интерфейса нужно выполнить следующее:

- подключить репозиторий Termidesk;
- установить Termidesk:

⚠ Начиная с версии 4.3 в зависимости пакета установки `termidesk-vdi` добавлена служба ведения журналов `syslog-ng`. Работа с другими службами ведения журналов не гарантируется.

Перед обновлением ОС или службы `syslog-ng` рекомендуется создать резервную копию файла `syslog-ng.conf`. В случае обновления ОС или службы `syslog-ng` без предварительного создания резервной копии файла, может потребоваться переустановка Termidesk для восстановления его корректной работы.

Начиная с версии 4.3.2 в зависимости установки также добавлен пакет `libpython3.7`, который предоставит возможность установить Termidesk в ОС с минимальной конфигурацией (без графического интерфейса ОС).

```
~$ sudo apt -y install termidesk-vdi
```

где:

`-y` - ключ для пропуска подтверждения установки.

В процессе установки нужно выполнить следующее:

i Для переключения между экранными кнопками **[Ок]** и **[Отмена]** в псевдографическом интерфейсе используется клавиша **<Tab>**.

- ознакомиться с лицензионным соглашением и нажать экранную кнопку **[Ок]** (см. Рисунок 1);

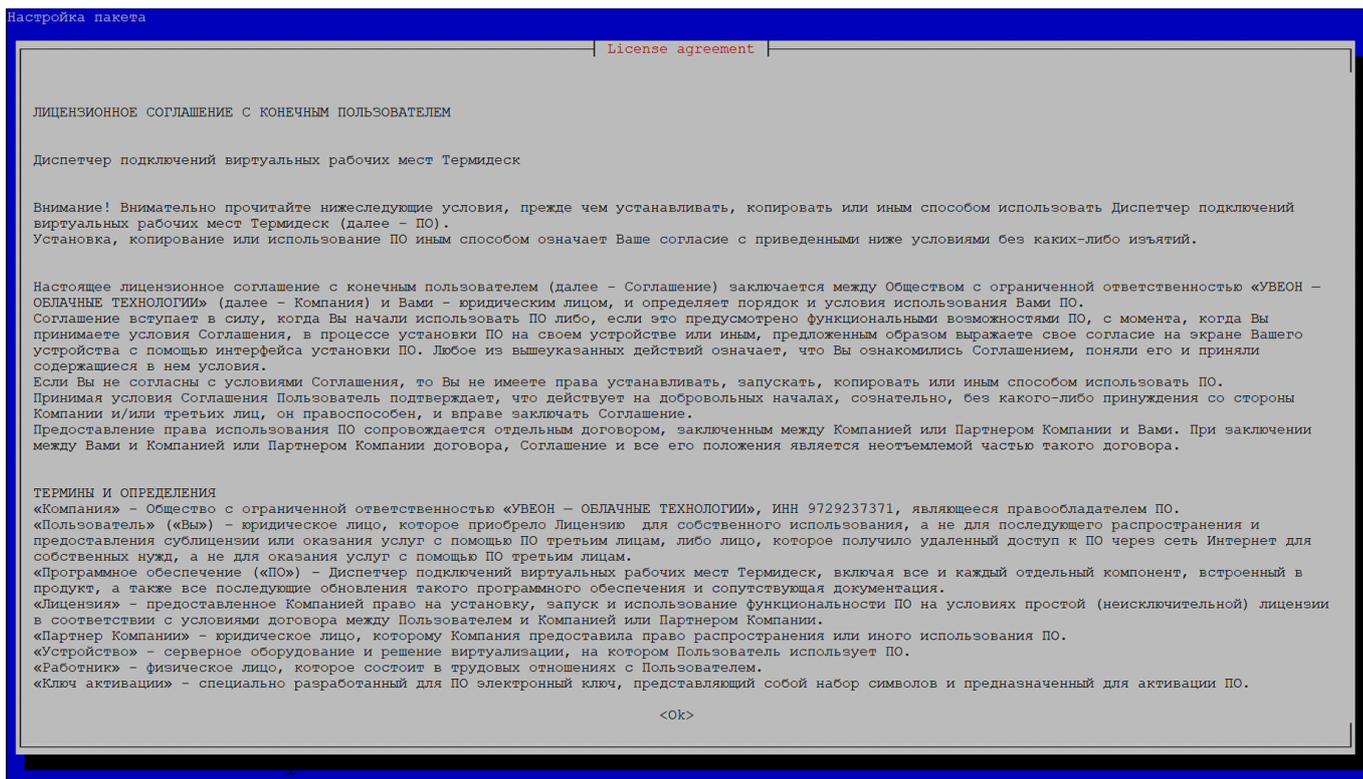


Рисунок 1 – Лицензионное соглашение

- для принятия условий лицензионного соглашения и продолжения установки следует нажать экранную кнопку **[Да]**. В случае отказа от условий соглашения следует нажать экранную кнопку **[Нет]**. При этом установка прервется (см. Рисунок 2);

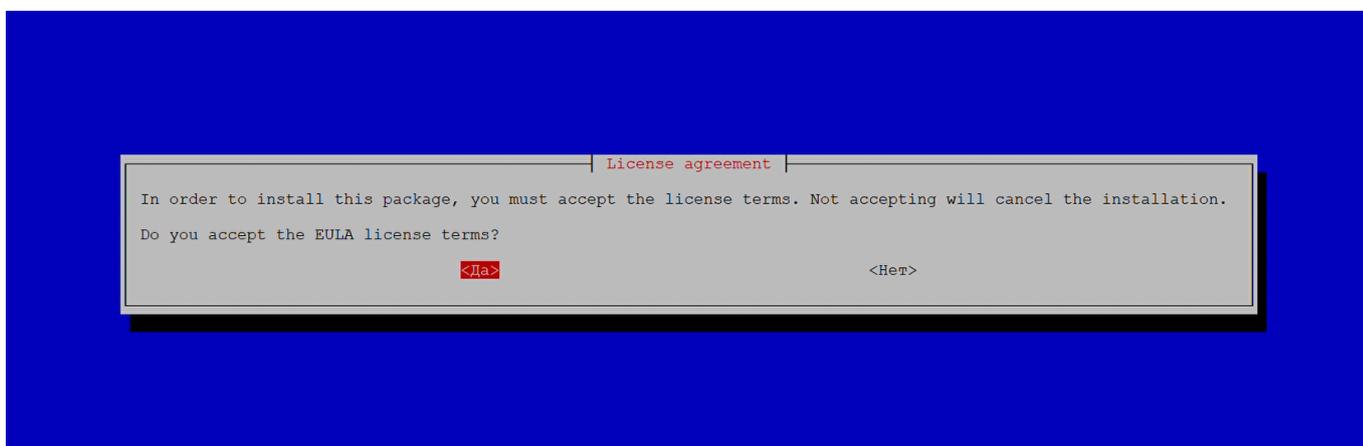


Рисунок 2 – Принятие условий лицензионного соглашения

После принятия условий лицензионного соглашения необходимо заполнить экранные поля информацией о подключении к БД Termidesk:

- «Termidesk DB server address»: адрес узла с установленной БД (в случае локальной установки – 127.0.0.1 (см. Рисунок 3));

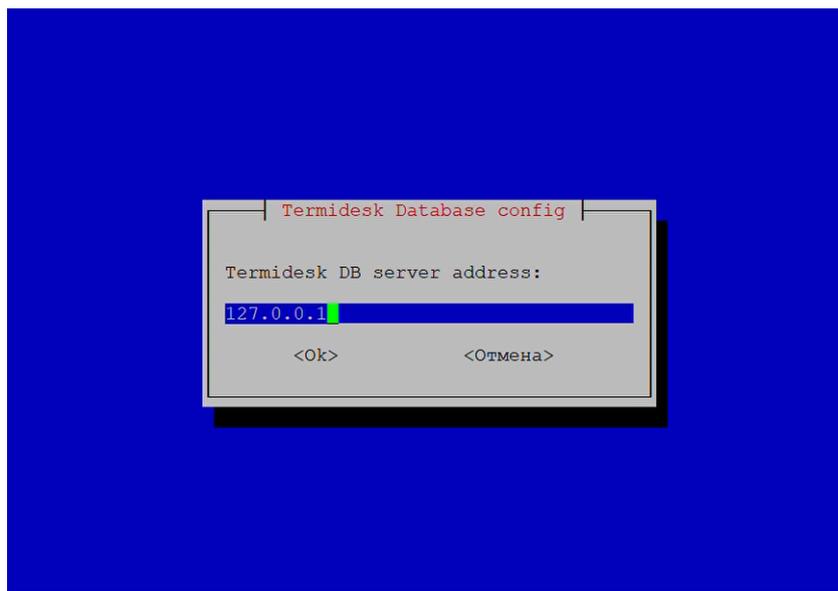


Рисунок 3 – Ввод адреса узла с установленной БД

- «Termidesk DB server port»: номер порта, который используется для соединения с сервером БД (указан стандартный порт — 5432 (см. Рисунок 4));

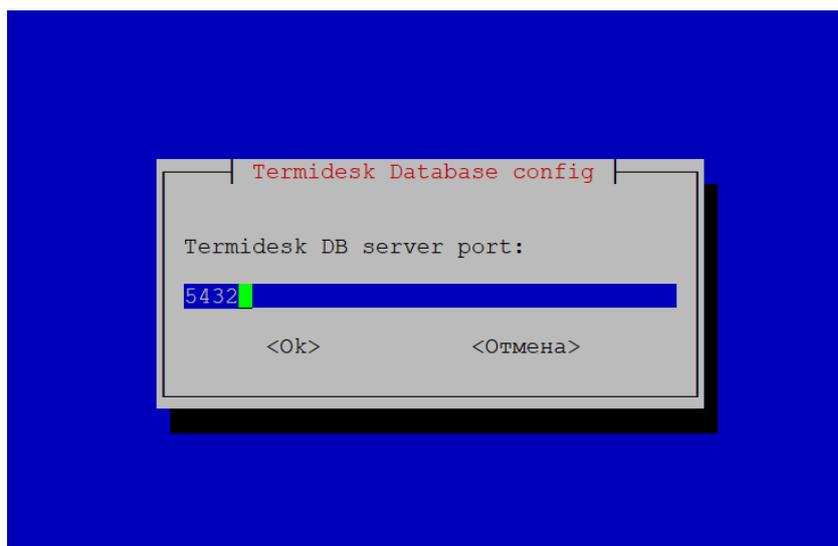


Рисунок 4 – Ввод номера порта БД

- «Minimum TLS version for connecting to DB»: выбрать протокол, который будет использоваться при подключении к БД (см. Рисунок 5). При выборе значения «Disable» защищенное соединение при подключении к БД использоваться не будет;



Рисунок 5 – Выбор протокола для подключения к БД

- «Termidesk DB name»: termidesk (данный параметр задавался при создании БД (см. Рисунок 6));

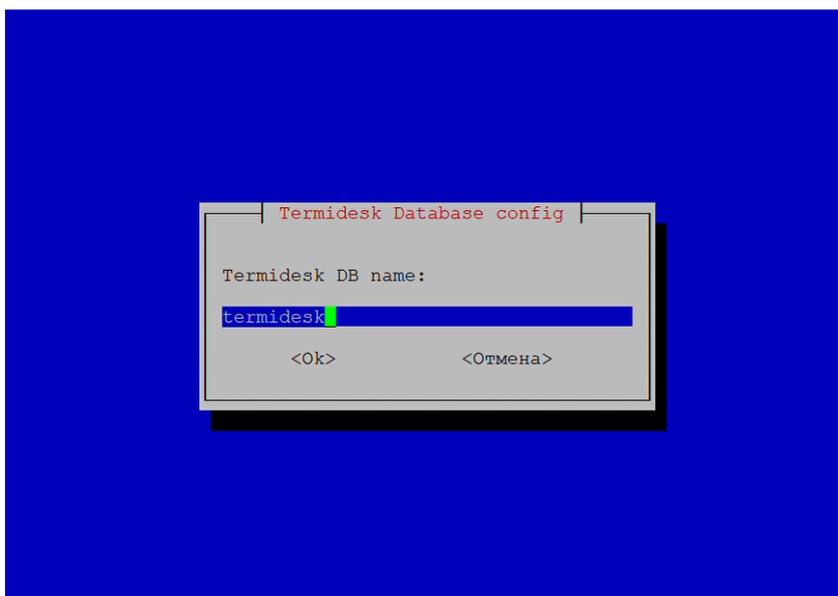


Рисунок 6 – Ввод названия БД

- «Termidesk DB user»: termidesk (данный параметр задавался при создании БД (см. Рисунок 7));

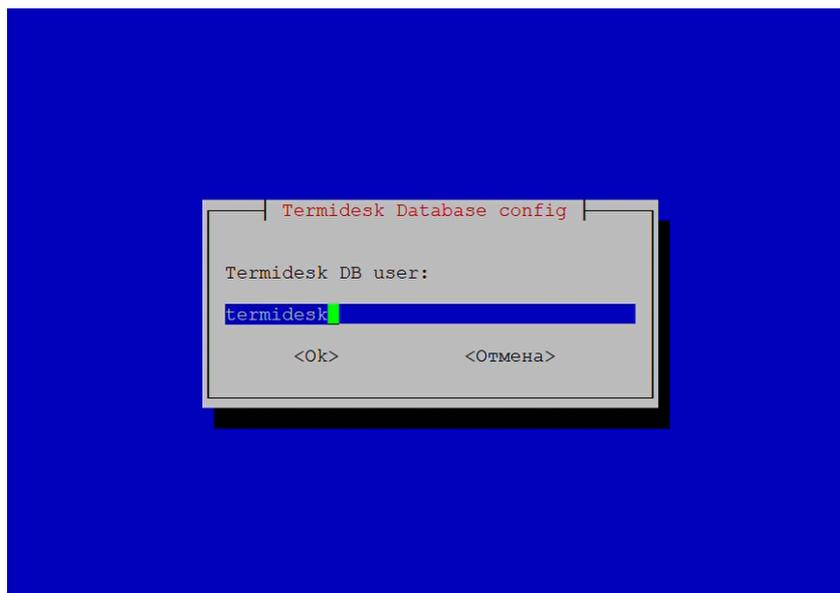


Рисунок 7 – Ввод имени пользователя БД

- «Termidesk DB password»: ввести пароль ksedimret (данный параметр задавался при создании БД (см. Рисунок 8)).

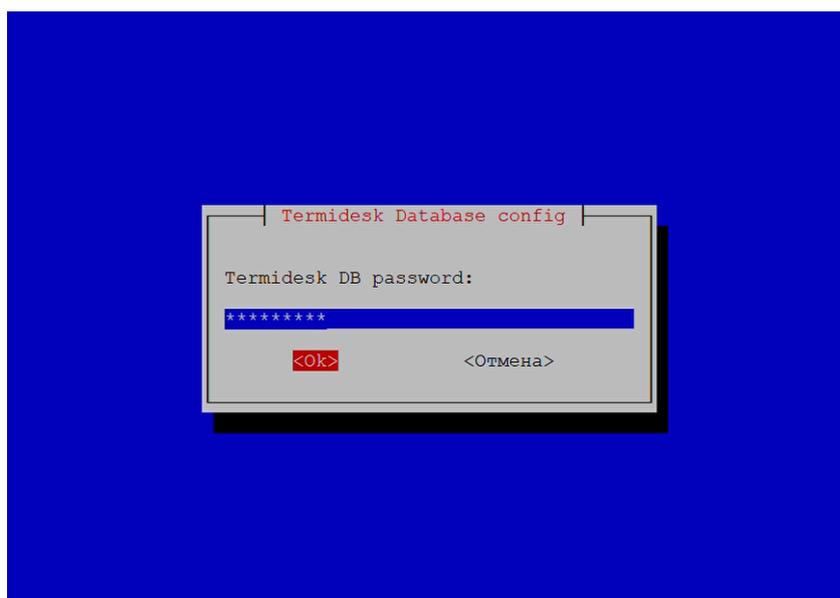


Рисунок 8 – Ввод пароля пользователя для доступа к БД

⚠ Значения могут быть оставлены по умолчанию, если БД была предварительно настроена (см. подраздел **Установка СУБД Postgres-11** и **Настройка СУБД Postgres-11**), однако пароль к БД нужно ввести вручную.

После окончания процесса настройки БД, необходимо настроить подключение к RabbitMQ-server. Для этого нужно выполнить следующее:

- в экранной форме «TLS connections to RabbitMQ servers» выбрать протокол, который будет использоваться при подключении к RabbitMQ-server (см. Рисунок 9). При выборе значения «Disable» защищенное соединение при подключении к RabbitMQ-server использоваться не будет;



Рисунок 9 – Выбор протокола для подключения к RabbitMQ-server

- в окне «RabbitMQ URL» нажать экранную кнопку [Ok] (см. Рисунок 10).

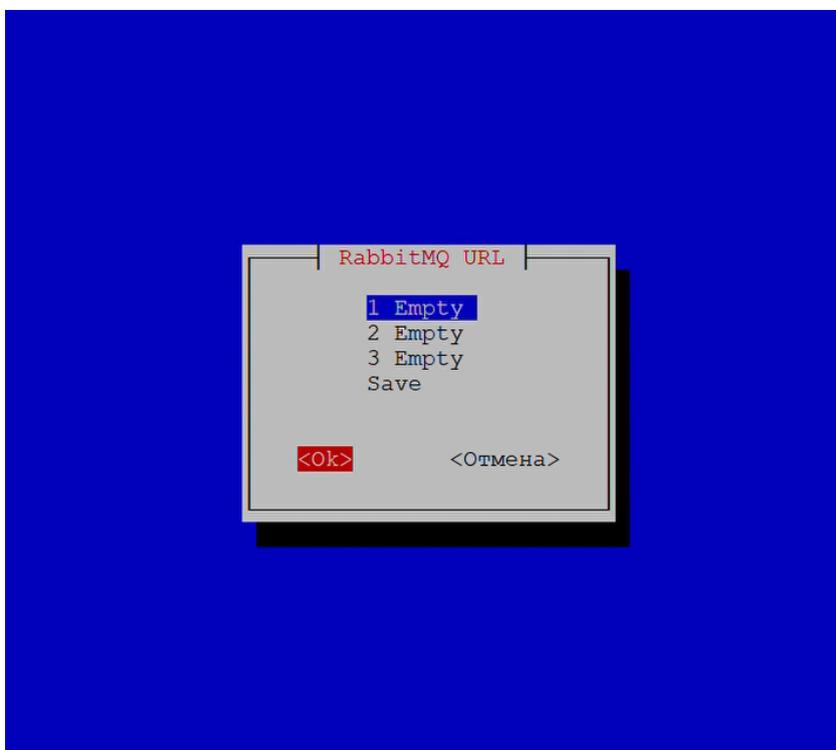


Рисунок 10 – Экранная форма «RabbitMQ URL»

Заполнить экранные поля информацией о подключении к RabbitMQ-server:

- «Termidesk RabbitMQ user»: termidesk (данный параметр задавался при настройке RabbitMQ-server (см. Рисунок 11));

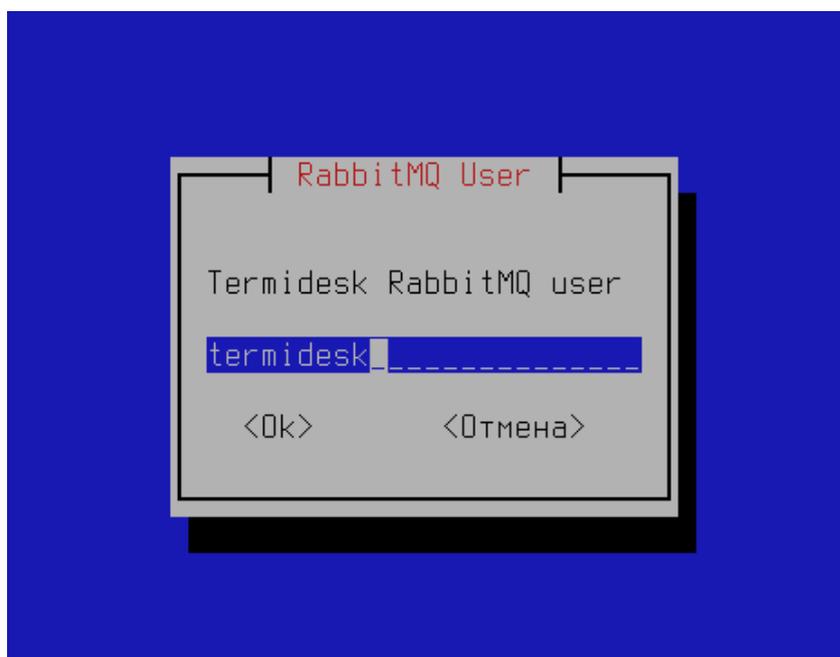


Рисунок 11 – Ввод имени пользователя RabbitMQ

- «Termidesk RabbitMQ pass»: ввести пароль к RabbitMQ ksedimret (данный параметр задавался при настройке RabbitMQ-server (см. Рисунок 12));



Рисунок 12 – Ввод пароля пользователя RabbitMQ

- «Termidesk RabbitMQ host»: адрес узла с установленным RabbitMQ-server (в случае локальной установки — 127.0.0.1 (см. Рисунок 13));



Рисунок 13 – Ввод адреса узла с установленным RabbitMQ-server

- «Termidesk RabbitMQ port»: номер порта, который используется для установления соединения с RabbitMQ (указан стандартный порт — 5672 (см. Рисунок 14));



Рисунок 14 – Ввод номера порта RabbitMQ

- «Termidesk RabbitMQ Virtual Host»: termidesk (см. Рисунок 15).

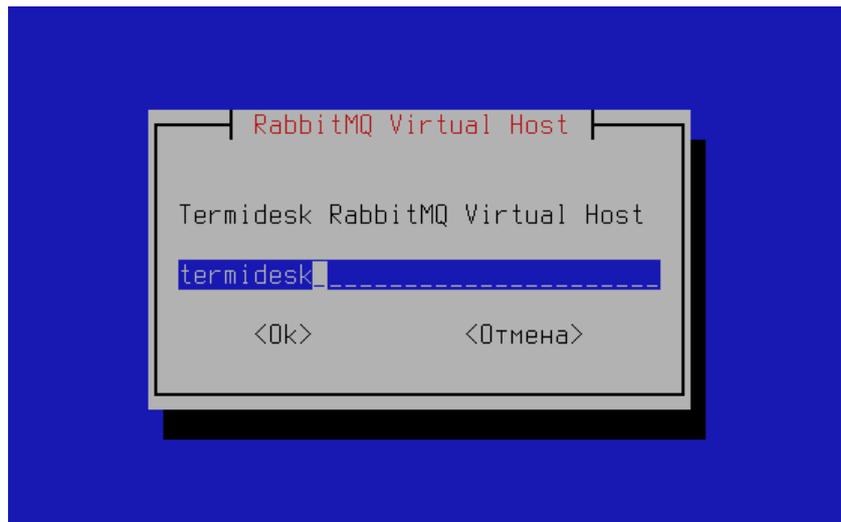


Рисунок 15 – Ввод названия виртуального хоста RabbitMQ

Далее экранная форма «RabbitMQ URL» отобразит в поле указанные настройки, пароль подключения к RabbitMQ будет скрыт. Для редактирования настроек следует выбрать нужное поле и нажать клавишу **<Enter>**, для сохранения настроек следует нажать экранную кнопку [Save] (см. Рисунок 16).

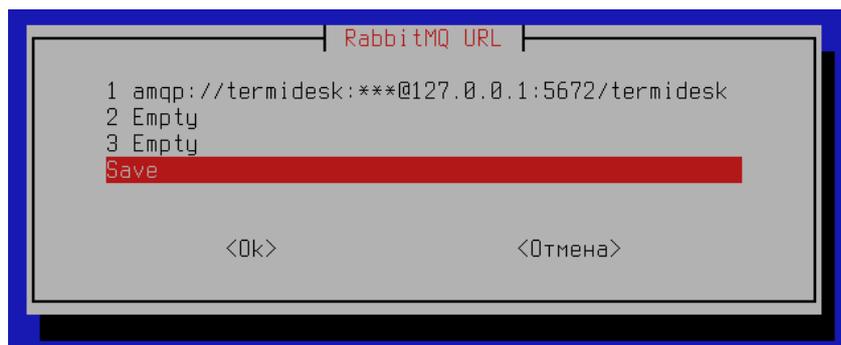


Рисунок 16 – Сохранение созданных настроек RabbitMQ

⚠ Значения могут быть оставлены по умолчанию, если RabbitMQ-server был предварительно настроен (см. подраздел **Установка брокера сообщений RabbitMQ-server** и **Настройка брокера сообщений RabbitMQ-server**), однако пароль к RabbitMQ нужно ввести вручную. Начиная с Termidesk версии 4.3.1 значение параметра «RabbitMQ URL» хранится в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` в преобразованном виде.

После настройки подключений к RabbitMQ-server инсталлятор предложит выбрать устанавливаемый на узел компонент: «Broker» («Универсальный диспетчер»), «Gateway» («Шлюз»), «Task manager» («Менеджер рабочих мест»). В случае установки комплексной установки нужно отметить все компоненты (см. Рисунок 17).

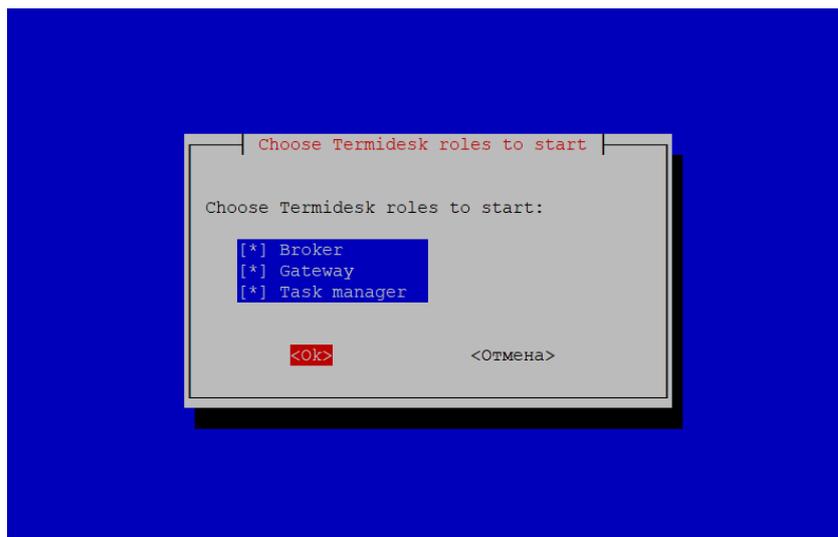


Рисунок 17 – Выбор устанавливаемого компонента в инсталляторе

Выбранные роли определяют, какие службы Termidesk будут включены для запуска во время старта ОС и автоматически запущены:

- при выборе компонента «Broker» будет запущена служба `termidesk-vdi`;
- при выборе компонента «Gateway» будет запущена служба `termidesk-wsproxy`;
- при выборе компонента «Task manager» будут запущены службы `termidesk-taskman`, `termidesk-celery-beat`, `termidesk-celery-worker`.

Если не выбрать ни одного компонента, то ни одна служба Termidesk запущена не будет. Если нажать экранную кнопку **[Отмена]**, или клавишу **<ESC>**, то изменение настроек применяться не будет.

Далее инсталлятор предложит выбрать один из трех типов веб-интерфейса Termidesk:

- «admin» - при выборе этого значения после установки будет доступен только веб-интерфейс для управления Termidesk и интерфейс `swagger` для доступа к документации по командам REST API. Пользовательский интерфейс будет недоступен;
- «user» - при выборе этого значения после установки будет доступен только пользовательский веб-интерфейс. Интерфейс управления Termidesk и `swagger` будут недоступны;
- «universal» - при выборе этого значения будут доступны все функции веб-интерфейса и `swagger`.

Нужно выбрать одно из значений и нажать экранную кнопку **[Ok]** (см. Рисунок 18). Позднее переключить тип веб-интерфейса можно через параметр `WEB_PORTAL_TYPE` конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf`. Настройки будут применены после перезапуска службы `termidesk-vdi`.

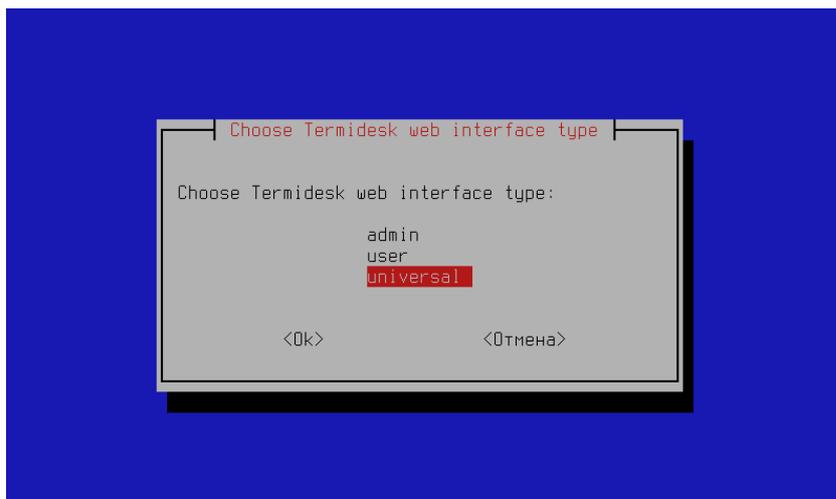


Рисунок 18 – Выбор типа веб-интерфейса

После установки Termidesk необходимо скорректировать файл конфигурации веб-сервера `/etc/apache2/apache2.conf`. Для этого нужно найти и раскомментировать строку с параметром `AstraMode`, далее присвоить данному параметру значение `off`, точно соблюдая отступы и пробелы в файле:

```

1  # Astra security mode
2  #
3  AstraMode off
    
```

Затем перезапустить веб-сервер:

```

:~$ sudo systemctl restart apache2
    
```

5.3 . Распределенная установка программного комплекса

5.3.1 . Основные принципы распределенной установки

В Termidesk предусмотрена распределенная установка компонентов в качестве ролей на отдельные серверы или ВМ.

Установка компонентов Termidesk выполняется в среде функционирования ОС Astra Linux Special Edition 1.7.

Распределенно могут устанавливаться следующие компоненты:

- универсальный диспетчер (служба `termidesk-vdi`);
- шлюз подключений (служба `termidesk-wsproxy`);
- менеджер рабочих мест (службы `termidesk-taskman`, `termidesk-celery-beat`, `termidesk-celery-worker`).

Перечень условий для распределенной установки:

- компонент RabbitMQ-server устанавливается на одном узле с СУБД (в общем случае этот компонент может устанавливаться на отдельный узел, но в рамках настоящей процедуры данный вариант не рассматривается);

⚠ Если будет использоваться внешняя СУБД, нужно установить компонент RabbitMQ-server на узел менеджера рабочих мест Termidesk или на отдельный узел.

- на всех узлах, предназначенных для установки компонентов, настроены статические IP-адреса;
- на всех узлах настроена синхронизация времени от единого источника.

Упрощенная общая схема при распределенной установке Termidesk приведена на рисунке (см. Рисунок 19).

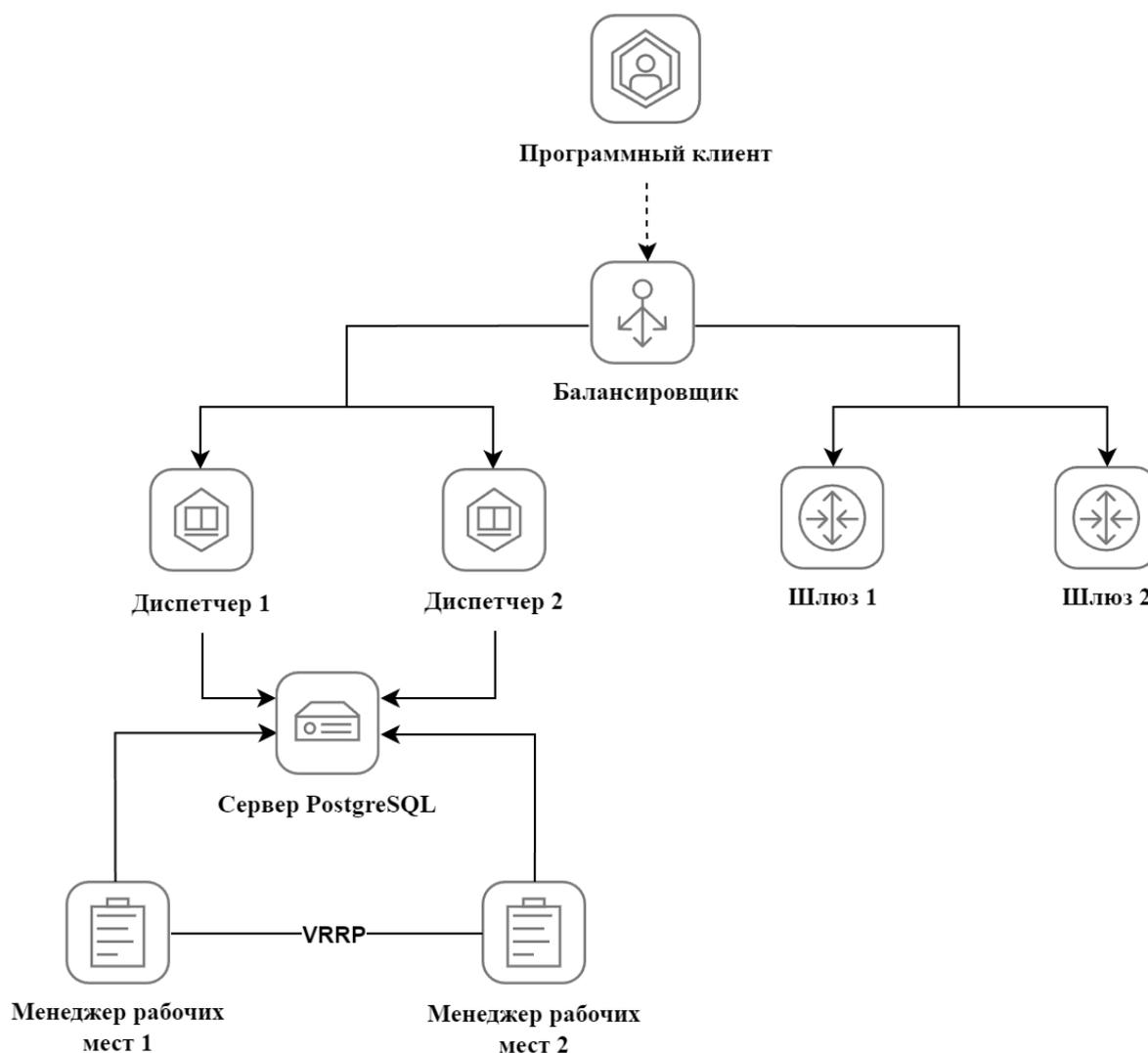


Рисунок 19 – Схема распределенной установки

Перечень обозначенных на схеме компонентов приведен в таблице (см. Таблица 1).

Таблица 1 – Перечень компонентов

Компонент	FQDN	Подпись на схеме
Универсальный диспетчер Termidesk 1	disp1.termidesk.local	Диспетчер 1
Универсальный диспетчер Termidesk 2	disp2.termidesk.local	Диспетчер 2
Шлюз Termidesk 1	gw1.termidesk.local	Шлюз 1
Шлюз Termidesk 2	gw2.termidesk.local	Шлюз 2
Менеджер рабочих мест (master)	tsk1.termidesk.local	Менеджер рабочих мест 1
Менеджер рабочих мест (slave)	tsk2.termidesk.local	Менеджер рабочих мест 2
Балансировщик нагрузки (nginx)	nginx.termidesk.local	Балансировщик
База данных	db.termidesk.local	Сервер PostgreSQL

Распределенная установка проводится в следующей последовательности:

- 1) устанавливается узел с компонентами СУБД и RabbitMQ-server (обе службы на одном узле);
- 2) устанавливается первый узел с универсальным диспетчером Termidesk. При установке диспетчера Termidesk необходимо выбрать компонент «Broker» в диалоговом окне псевдографического интерфейса инсталлятора;

⚠ Настройки первого узла с универсальным диспетчером Termidesk будут использоваться как эталонные для остальных узлов с компонентами Termidesk (универсального диспетчера, шлюзов, менеджеров ВРМ).
 Параметры конфигурации Termidesk находятся в файле `/etc/opt/termidesk-vdi/termidesk.conf`.
 Нужно скопировать каталог `/etc/opt/termidesk-vdi` вместе с его содержимым на все узлы, за исключением узлов с СУБД и балансировщиком.

- 3) устанавливаются остальные узлы - универсальные диспетчеры Termidesk с копированием файлов, указанных в п.2, с эталонного узла;
- 4) устанавливаются узлы - шлюзы подключений Termidesk с копированием файлов, указанных в п.2, с эталонного узла. При установке шлюза Termidesk необходимо выбрать компонент «Gateway» в диалоговом окне псевдографического интерфейса инсталлятора;
- 5) устанавливаются узлы - менеджеры ВРМ с копированием файлов, указанных в п.2, с эталонного узла. При установке менеджера ВРМ Termidesk необходимо выбрать компонент «Task Manager» в диалоговом окне псевдографического интерфейса инсталлятора (одновременно служба менеджера ВРМ `termidesk-taskman` должна быть запущена только на одном из узлов!).

Заключительным этапом устанавливаются и настраиваются балансировщики нагрузки на базе ОС Astra Linux Special Edition 1.7 и nginx.

5.3.2 . Установка и настройка СУБД Postgres-11

Процесс установки СУБД Postgres-11 и брокера сообщений RabbitMQ-server не отличается от процесса, описанного в разделе **Подготовка среды функционирования**).

Для завершения настройки нужно:

- отредактировать файл `rabbitmq-env.conf`, приведя его к виду:

```

1  # Defaults to rabbit. This can be useful if you want to run more than one node
2  # per machine - RABBITMQ_NODENAME should be unique per erlang-node-and-machine
3  # combination. See the clustering on a single machine guide for details:
4  # http://www.rabbitmq.com/clustering.html#single-machine
5  #NODENAME=rabbit
6
7  # By default RabbitMQ will bind to all interfaces, on IPv4 and IPv6 if
8  # available. Set this if you only want to bind to one network interface or#
9  # address family.
10 NODE_IP_ADDRESS=0.0.0.0
11 # Defaults to 5672.
12 NODE_PORT=5672
    
```

- сохранить файл и перезапустить службу `rabbitmq-server`:

```

:~$ sudo systemctl restart rabbitmq-server
    
```

5.3.3 . Установка первого узла с универсальным диспетчером Termidesk

Процесс установки первого узла с универсальным диспетчером Termidesk аналогичен комплексной установке Termidesk, за исключением выбора только компонента «Broker».

После установки передать каталог `/etc/opt/termidesk-vdi` на остальные узлы универсальных диспетчеров, шлюзов подключений и менеджеров BPM:

```

:~$ sudo scp -r /etc/opt/termidesk-vdi localuser@ipaddr_or_fqdn_host:/home/user/
    
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Перед началом установки остальных узлов - универсальных диспетчеров Termidesk необходимо переместить скопированный ранее каталог `termidesk-vdi` в каталог `/etc/opt/`:

```

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

Установить остальные узлы с универсальным диспетчером Termidesk по аналогии с первым, но в диалоге подключения к СУБД и заполнения информации о подключении к RabbitMQ-server, выбрать экранную кнопку **[Отмена]**.

5.3.4 . Установка узлов - шлюзов подключений

Установка узлов - шлюзов подключений аналогична комплексной установке Termidesk, за исключением выбора только компонента «Gateway».

После завершения установки изменить настройки запуска службы `termidesk-wsproxy`:

- отредактировать файл `/etc/opt/termidesk-vdi/termidesk.conf`, приведя фрагмент файла к виду:

```

1  ...
2  # Порт, который будет прослушивать служба termidesk-wsproxy
3  WSPROXY_PORT=5099
4  # Адрес, который должна слушать служба termidesk-wsproxy
5  # при распределённой установке :
6  WSPROXY_BIND_ADDRESS="0.0.0.0"
7  ...
    
```

- сохранить файл, а затем перезапустить службу:

```

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

5.3.5 . Установка узлов - менеджеров ВРМ

Установка менеджеров ВРМ производится на два узла, работающих в режиме `network failover`. Установка аналогична комплексной установке Termidesk, за исключением выбора только компонента «Task manager».

После установки нужно остановить (`systemctl stop`) и исключить (`systemctl disable`) службу `termidesk-taskman` из автоматического запуска:

```

:~$ sudo systemctl stop termidesk-taskman && sudo systemctl disable termidesk-taskman
    
```

Исключение службы из автоматического запуска необходимо, поскольку управление ее состоянием производится скриптами режима высокой доступности.

5.3.6 . Установка балансировщиков

Балансировщики нагрузки необходимы для балансировки клиентских подключений к универсальным диспетчерам и шлюзам, равномерного распределения нагрузки на них. Средой функционирования для балансировщиков нагрузки является ОС Astra Linux Special Edition 1.7.

Балансировщик `nginx` устанавливается командой:

```

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

где:

`-y` - ключ для пропуска подтверждения установки.

5.3.7 . Действия после распределенной установки

Настройка менеджера ВРМ в режиме высокой доступности приведена в подразделе **Настройка менеджера ВРМ в режиме высокой доступности** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Настройка балансировщика нагрузки приведена в подразделе **Настройка балансировщика для работы с самоподписанными сертификатами** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

5.4 . Отказоустойчивая установка Termidesk

5.4.1 . Основные принципы отказоустойчивой установки

В Termidesk предусмотрена отказоустойчивая установка комплекса для сохранения работоспособности при возникновении нештатных ситуаций.

Перечень условий для отказоустойчивой установки:

- компонент RabbitMQ-server устанавливается на одном узле с СУБД (в общем случае этот компонент может устанавливаться на отдельный узел, но в рамках настоящей процедуры данный вариант не рассматривается);

 Если будет использоваться внешняя СУБД, нужно установить компонент RabbitMQ-server на один из узлов-серверов Termidesk или на отдельный узел.

- на всех узлах, предназначенных для установки компонентов, настроены статические IP-адреса;
- на всех узлах настроена синхронизация времени от единого источника.

Упрощенная схема отказоустойчивой установки представлена на рисунке (см. Рисунок 20).

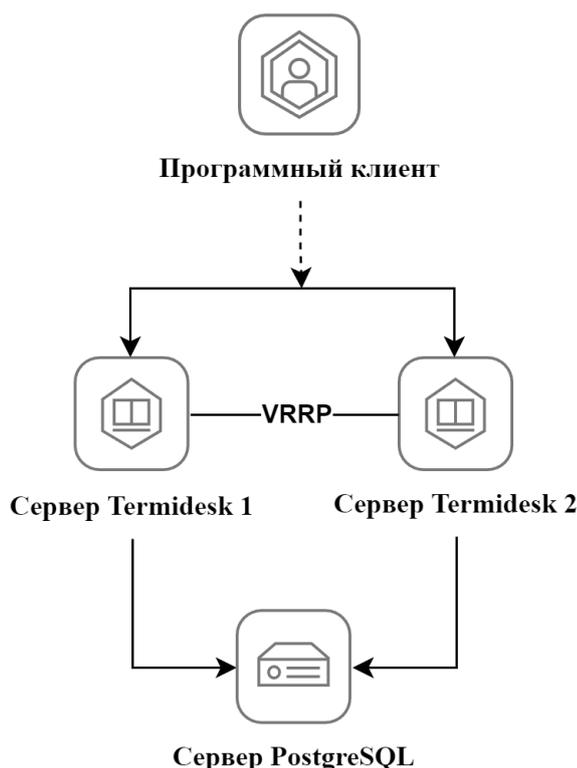


Рисунок 20 – Отказоустойчивая схема установки Termidesk

Перечень обозначенных компонентов приведен в таблице (см. Таблица 2).

⚠ Все примеры IP-адресов и FQDN должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре предприятия. Следует учесть, что в примерах конфигурационных файлов и запросах также используются IP-адреса и FQDN из таблицы, в рабочей конфигурации их следует изменить на актуальные.

Таблица 2 – Перечень компонентов для отказоустойчивой установки

Обозначение на схеме	Установленные на узел компоненты	FQDN узла	IP-адрес
Сервер Termidesk 1	Основной узел (master). Первоначально установлен с ролями: <ul style="list-style-type: none"> ▪ универсальный диспетчер (служба termidesk-vdi); ▪ шлюз подключений (служба termidesk-wsproxy). При установке необходимо выбрать компоненты «Broker» и «Gateway» в диалоговом окне псевдографического интерфейса инсталлятора	disp1.termidesk.local	192.0.2.2 192.0.2.1 (виртуальный IP-адрес)

Обозначение на схеме	Установленные на узел компоненты	FQDN узла	IP-адрес
Сервер Termidesk 2	Резервный узел (slave). Первоначально установлен с ролями: <ul style="list-style-type: none"> ▪ универсальный диспетчер (служба <code>termidesk-vdi</code>); ▪ шлюз подключений (служба <code>termidesk-wsproxy</code>). При установке необходимо выбрать компоненты «Broker» и «Gateway» в диалоговом окне псевдографического интерфейса инсталлятора	<code>disp2.termidesk.local</code>	192.0.2.3 192.0.2.1 (виртуальный IP-адрес)
СУБД PostgreSQL	Установлены СУБД PostgreSQL и RabbitMQ-server (обе службы на одном узле)	<code>db.termidesk.local</code>	192.0.2.4

i К виртуальному IP-адресу подключается программный клиент. Этот IP-адрес назначается в настройках VRRP и одинаков для обоих узлов серверов Termidesk.

Отказоустойчивая установка проводится в следующей последовательности:

- 1) устанавливается узел с компонентами СУБД и RabbitMQ-server (обе службы на одном узле). Выполняется настройка СУБД;
- 2) устанавливается основной узел Termidesk. При установке необходимо выбрать компоненты «Broker» и «Gateway» в диалоговом окне псевдографического интерфейса инсталлятора;
- 3) с основного узла Termidesk на резервные копируется каталог `/etc/opt/termidesk-vdi` вместе с его содержимым;
- 4) устанавливаются резервные узлы Termidesk;
- 5) проверяется работоспособность узлов Termidesk;
- 6) выполняется настройка узлов в режиме высокой доступности.

5.4.2 . Установка и настройка СУБД Postgres-11

Процесс установки СУБД Postgres-11 и брокера сообщений RabbitMQ-server не отличается от процесса, описанного в разделе **Подготовка среды функционирования**).

Для завершения настройки RabbitMQ-server нужно:

- отредактировать файл `rabbitmq-env.conf`, приведя его к виду:

```

1  # Defaults to rabbit. This can be useful if you want to run more than one node
2  # per machine - RABBITMQ_NODENAME should be unique per erlang-node-and-machine
3  # combination. See the clustering on a single machine guide for details:
4  # http://www.rabbitmq.com/clustering.html#single-machine
5  #NODENAME=rabbit
6
7  # By default RabbitMQ will bind to all interfaces, on IPv4 and IPv6 if
8  # available. Set this if you only want to bind to one network interface or#
9  # address family.
10 NODE_IP_ADDRESS=0.0.0.0
11 # Defaults to 5672.
```

```
12 NODE_PORT=5672
```

- сохранить файл и перезапустить службу rabbitmq-server:

```
~$ sudo systemctl restart rabbitmq-server
```

Сервис СУБД должен быть настроен таким образом, чтобы он мог принимать подключения с узлов Termidesk, для этого нужно:

- отредактировать файл `/etc/postgresql/11/main/postgresql.conf`: в разделе CONNECTIONS AND AUTHENTICATION изменить строку `listen_addresses`, заменив `localhost` на «*».

Пример:

```
1 #-----
2 # CONNECTIONS AND AUTHENTICATION
3 #-----
4 # - Connection Settings -
5 listen_addresses = '*' # what IP address(es) to listen on;
6 # comma-separated list of addresses;
7 # defaults to 'localhost'; use '*' for all
8 # (change requires restart)
9 port = 5432 # (change requires restart)
```

- затем отредактировать файл `/etc/postgresql/11/main/pg_hba.conf`: в разделе #IPv4 `local` connections в столбце ADDRESS текущее значение нужно изменить на `all`. Пример:

```
1 # TYPE DATABASE USER ADDRESS METHOD
2 # "local" is for Unix domain socket connections only
3 local all all peer
4 # IPv4 local connections:
5 host all all all md5
6 # IPv6 local connections:
7 host all all ::1/128 md5
8 # Allow replication connections from localhost, by a user with the
9 # replication privilege.
10 local replication all peer
11 host replication all 127.0.0.1/32 md5
12 host replication all ::1/128 md5
```

- сохранить файлы и перезапустить службу postgresql:

```
~$ sudo systemctl restart postgresql
```

5.4.3. Установка основного узла Termidesk

Процесс установки основного узла Termidesk аналогичен комплексной установке Termidesk, за исключением выбора только компонентов «Broker» и «Gateway».

После установки необходимо:

- скорректировать файл конфигурации веб-сервера `/etc/apache2/apache2.conf`. Для этого нужно найти и раскомментировать строку с параметром `AstraMode`, далее присвоить данному параметру значение `off`, точно соблюдая отступы и пробелы в файле:

```

1 # Astra security mode
2 #
3 AstraMode off
    
```

- запустить службу `termidesk-taskman`, не добавляя ее в раздел автоматической загрузки:

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

5.4.4 . Перенос каталога с конфигурационными файлами и ключами

 Настройки основного узла Termidesk используются как эталонные для остальных узлов Termidesk.

После установки основного узла Termidesk нужно передать каталог `/etc/opt/termidesk-vdi` на остальные узлы Termidesk:

```
:~$ sudo scp -r /etc/opt/termidesk-vdi localuser@ipaddr_or_fqdn_host:/home/user/
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Перед началом установки остальных узлов необходимо переместить скопированный ранее каталог `termidesk-vdi` в каталог `/etc/opt/`:

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

5.4.5 . Установка резервных узлов Termidesk

Процесс установки резервных узлов Termidesk аналогичен установке основного узла, но в диалоге подключения к СУБД и заполнения информации о подключении к RabbitMQ-server нужно выбрать экранную кнопку **[Отмена]**. Действия после установки также аналогичны действиям, выполняемым на основном узле.

5.4.6 . Проверка работоспособности узлов Termidesk

После установки нужно убедиться, что на основном и резервных узлах Termidesk правильно запущены службы, для этого выполнить команду на каждом узле:

```
~$ sudo systemctl -a | grep termidesk
```

На основном узле вывод команды должен отображать, что активны и загружены все службы Termidesk, пример вывода:

```
1 admin@disp1.termidesk.local:~$ sudo systemctl -a | grep termidesk
2 termidesk-taskman.service loaded active running Termidesk-VDI Taskman daemon
3 termidesk-vdi.service loaded active running Termidesk-VDI daemon
4 termidesk-wsproxy.service loaded active running Termidesk-VDI WSProxy daemon
```

На резервных узлах вывод команды должен отображать, что активны и загружены только службы termidesk-vdi и termidesk-wsproxy, пример вывода:

```
1 admin@disp1.termidesk.local:~$ sudo systemctl -a | grep termidesk
2 termidesk-taskman.service inactive dead Termidesk-VDI Taskman daemon
3 termidesk-vdi.service loaded active running Termidesk-VDI daemon
4 termidesk-wsproxy.service loaded active running Termidesk-VDI WSProxy daemon
```

Затем необходимо проверить доступность резервных узлов по протоколу HTTPS, выполнив в веб-браузере переход по адресу `https://disp2.termidesk.local` или `https://192.0.2.3`. Убедиться, что отобразилась страница входа в Termidesk.

5.4.7 . Настройка узлов в режиме высокой доступности

Действия по настройке узлов будут идентичными приведенным в подразделе **Настройка менеджера ВРМ в режиме высокой доступности** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса» за исключением файла `/etc/keepalived/keepalived.conf`.

Файл `/etc/keepalived/keepalived.conf` должен быть приведен к виду (по очереди на каждом из узлов):

⚠ Значения параметров в файле `keepalived.conf` приведены в качестве примера. Значения должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре предприятия. Параметры, явно подлежащие изменению, отмечены комментарием «# **НУЖНО УКАЗАТЬ**».

```
1 global_defs {
2
3     router_id disp1.termidesk.local # НУЖНО УКАЗАТЬ: hostname хоста
4     script_user user # НУЖНО УКАЗАТЬ: вместо user -> пользователь, от имени которого
5     enable_script_security
6 }
7
8 vrrp_script check_httpd {
9     script "/usr/bin/pgrep apache" # path of the script to execute
```

```

10     interval 1 # seconds between script invocations, default 1 second
11     timeout 3 # seconds after which script is considered to have failed
12     #weight <INTEGER:-254..254> # adjust priority by this weight, default 0
13     rise 1 # required number of successes for OK transition
14     fall 2 # required number of successes for KO transition
15     #user USERNAME [GROUPNAME] # user/group names to run script under
16     init_fail # assume script initially is in failed state
17 }
18
19 # Для каждого виртуального IPv4-адреса создается свой экземпляр vrrp_instance
20 vrrp_instance termidesk-taskman {
21     notify /etc/keepalived/notify.sh
22
23     # Initial state, MASTER|BACKUP
24     # As soon as the other machine(s) come up,
25     # an election will be held and the machine
26     # with the highest priority will become MASTER.
27     # So the entry here doesn't matter a whole lot.
28     state BACKUP
29
30     # interface for inside_network, bound by vrrp
31     # НУЖНО УКАЗАТЬ: eth0 -> интерфейс, смотрящий в Интернет
32     interface eth0
33
34     # arbitrary unique number from 0 to 255
35     # used to differentiate multiple instances of vrrpd
36     # running on the same NIC (and hence same socket).
37     # НУЖНО УКАЗАТЬ: вместо 2 -> номер экземпляра vrrp_instance
38     virtual_router_id 2
39
40     # for electing MASTER, highest priority wins.
41     # to be MASTER, make this 50 more than on other machines.
42     # НУЖНО УКАЗАТЬ: вместо 128 -> приоритет экземпляра vrrp_instance
43     priority 128
44
45     preempt_delay 5 # Seconds
46
47     # VRRP Advert interval in seconds (e.g. 0.92) (use default)
48     advert_int 1
49
50     # НУЖНО УКАЗАТЬ: вместо 192.0.2.1 -> IPv4-адрес интерфейса, смотрящего в
Интернет
51     unicast_src_ip 192.0.2.1
52
53     authentication {
54         auth_type PASS
55         # НУЖНО УКАЗАТЬ: ksedimret -> заменить на безопасный пароль
56         auth_pass ksedimret
57     }
58
59     virtual_ipaddress {
60         # В этой секции происходит назначение IP-алиаса
61         # НУЖНО УКАЗАТЬ: вместо 192.0.2.1/24 -> виртуальный IPv4-адрес и сетевой
префикс с интерфейса, смотрящего в Интернет

```

```

62         # НУЖНО УКАЗАТЬ: вместо eth0 -> интерфейс, смотрящий в Интернет
63         # НУЖНО УКАЗАТЬ: вместо eth0:106 -> интерфейс, смотрящий в Интернет: 4-й
октет виртуального IPv4-адреса
64         192.0.2.1/24 dev eth0 label eth0:106
65     }
66
67     track_script {
68         check_httpd
69     }
70 }
71
72 vrrp_instance termidesk-vdi {
73     notify /etc/keepalived/notify.sh
74
75     # Initial state, MASTER|BACKUP
76     # As soon as the other machine(s) come up,
77     # an election will be held and the machine
78     # with the highest priority will become MASTER.
79     # So the entry here doesn't matter a whole lot.
80     state BACKUP
81
82     # interface for inside_network, bound by vrrp
83     # НУЖНО УКАЗАТЬ: eth0 -> интерфейс, смотрящий в Интернет
84     interface eth0
85
86     # arbitrary unique number from 0 to 255
87     # used to differentiate multiple instances of vrrpd
88     # running on the same NIC (and hence same socket).
89     # НУЖНО УКАЗАТЬ: вместо 107 -> номер экземпляра vrrp_instance
90     virtual_router_id 107
91
92     # for electing MASTER, highest priority wins.
93     # to be MASTER, make this 50 more than on other machines.
94     # НУЖНО УКАЗАТЬ: вместо 128 -> приоритет экземпляра vrrp_instance
95     priority 128
96
97     preempt_delay 5 # Seconds
98
99     # VRRP Advert interval in seconds (e.g. 0.92) (use default)
100    advert_int 1
101
102    # НУЖНО УКАЗАТЬ: вместо 192.0.2.3 -> IPv4-адрес интерфейса, смотрящего в
Интернет
103    unicast_src_ip 192.0.2.3
104
105    authentication {
106        auth_type PASS
107        # НУЖНО УКАЗАТЬ: ksedimret -> заменить на безопасный пароль
108        auth_pass ksedimret
109    }
110
111    virtual_ipaddress {
112        # В этой секции происходит назначение IP-алиаса

```

```

113         # НУЖНО УКАЗАТЬ: вместо 192.0.2.1/24 -> виртуальный IPv4-адрес и сетевой
114         # НУЖНО УКАЗАТЬ: вместо eth0 -> интерфейс, смотрящий в Интернет
115         # НУЖНО УКАЗАТЬ: вместо eth0:107 -> интерфейс, смотрящий в Интернет: 4-й
116         # октет виртуального IPv4-адреса
117         192.0.2.1/24 dev eth0 label eth0:107
118     }
119     track_script {
120         check_httpd
121     }
122 }
123
124 vrrp_instance termidesk-wsproxy {
125     notify /etc/keepalived/notify.sh
126
127     # Initial state, MASTER|BACKUP
128     # As soon as the other machine(s) come up,
129     # an election will be held and the machine
130     # with the highest priority will become MASTER.
131     # So the entry here doesn't matter a whole lot.
132     state BACKUP
133
134     # interface for inside_network, bound by vrrp
135     # НУЖНО УКАЗАТЬ: eth0 -> интерфейс, смотрящий в Интернет
136     interface eth0
137
138     # arbitrary unique number from 0 to 255
139     # used to differentiate multiple instances of vrrpd
140     # running on the same NIC (and hence same socket).
141     # НУЖНО УКАЗАТЬ: вместо 108 -> номер экземпляра vrrp_instance
142     virtual_router_id 108
143
144     # for electing MASTER, highest priority wins.
145     # to be MASTER, make this 50 more than on other machines.
146     # НУЖНО УКАЗАТЬ: вместо 64 -> приоритет экземпляра vrrp_instance
147     priority 64
148
149     preempt_delay 5 # Seconds
150
151     # VRRP Advert interval in seconds (e.g. 0.92) (use default)
152     advert_int 1
153
154     # НУЖНО УКАЗАТЬ: вместо 192.0.2.2 -> IPv4-адрес интерфейса, смотрящего в
155     # Интернет
156     unicast_src_ip 192.0.2.2
157
158     authentication {
159         auth_type PASS
160         # НУЖНО УКАЗАТЬ: ksedimret -> заменить на безопасный пароль
161         auth_pass ksedimret
162     }
163     virtual_ipaddress {

```

```

164         # В этой секции происходит назначение IP-алиаса
165         # НУЖНО УКАЗАТЬ: вместо 192.0.2.1/24 -> виртуальный IPv4-адрес и сетевой
префикс с интерфейса, смотрящего в Интернет
166         # НУЖНО УКАЗАТЬ: вместо eth0 -> интерфейс, смотрящий в Интернет
167         # НУЖНО УКАЗАТЬ: вместо eth0:108 -> интерфейс, смотрящий в Интернет: 4-й
октет виртуального IPv4-адреса
168         192.0.2.1/24 dev eth0 label eth0:108
169     }
170
171     track_script {
172         check_httpd
173     }
174 }
    
```

5.5 . Установка программного комплекса в режиме замкнутой программной среды

Замкнутая программная среда (ЗПС) является средством повышения безопасности ОС путем контроля целостности (неизменности) файлов. Механизм контроля реализован в виде невыгружаемого модуля ядра ОС Astra Linux Special Edition 1.7 (модуль `digsig_verif`), выполняющего проверку электронной цифровой подписи файлов (ЭЦП).

Для установки Termidesk при включенном в ОС режиме ЗПС необходимо предварительно установить пакет `termidesk-digsig-keys`, выполнив следующее:

- подключить репозиторий Termidesk или получить отдельный пакет `termidesk-digsig-keys` из репозитория;
- выполнить установку с использованием репозитория:

```

:~$ sudo apt -y install termidesk-digsig-keys
    
```

- либо выполнить установку из deb-пакета:

```

:~$ sudo apt install -y /home/user/termidesk-digsig-keys-XXXXXX_amd64.deb
    
```

где:

`-y` - ключ для пропуска подтверждения установки;

`/home/user/termidesk-digsig-keys-XXXXXX_amd64.deb` - расположение пакета `termidesk-digsig-keys-XXXXXX_amd64.deb`.

- перезагрузить ОС:

```

:~$ sudo reboot
    
```

- выполнить установку Termidesk в нужной конфигурации (комплексная или распределенная).

Для ЗПС может быть выполнена активация режима проверки встроенной ЭЦП в расширенных атрибутах (DIGSIG_XATTR_MODE). В этом случае потребуется подписать файлы, которые будут проходить проверку, на имеющихся в организации ключах. Информация о процессе подписи и активации механизма проверки встроенной ЭЦП в расширенных атрибутах приведена в документе РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1» и в справочном центре Astra Linux: <https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634>.

5.6 . Проверка работоспособности после установки

Termidesk является работоспособным, если в результате перехода в веб-браузере по адресу <https://localhost/> или <https://127.0.0.1/> отобразилась страница входа (см. Рисунок 21) в Termidesk.

Указанные адреса используются в случае локальной установки. Если Termidesk установлен на сервере, отличном от узла, на котором происходит проверка, необходимо вместо значений localhost или 127.0.0.1 использовать IP-адрес сервера Termidesk.

⚠ Начиная с версии 4.2 по умолчанию включено перенаправление на протокол HTTPS при доступе к Termidesk. При необходимости использования незащищенного протокола HTTP администратор должен изменить файл `/etc/apache2/sites-available/termidesk.conf`

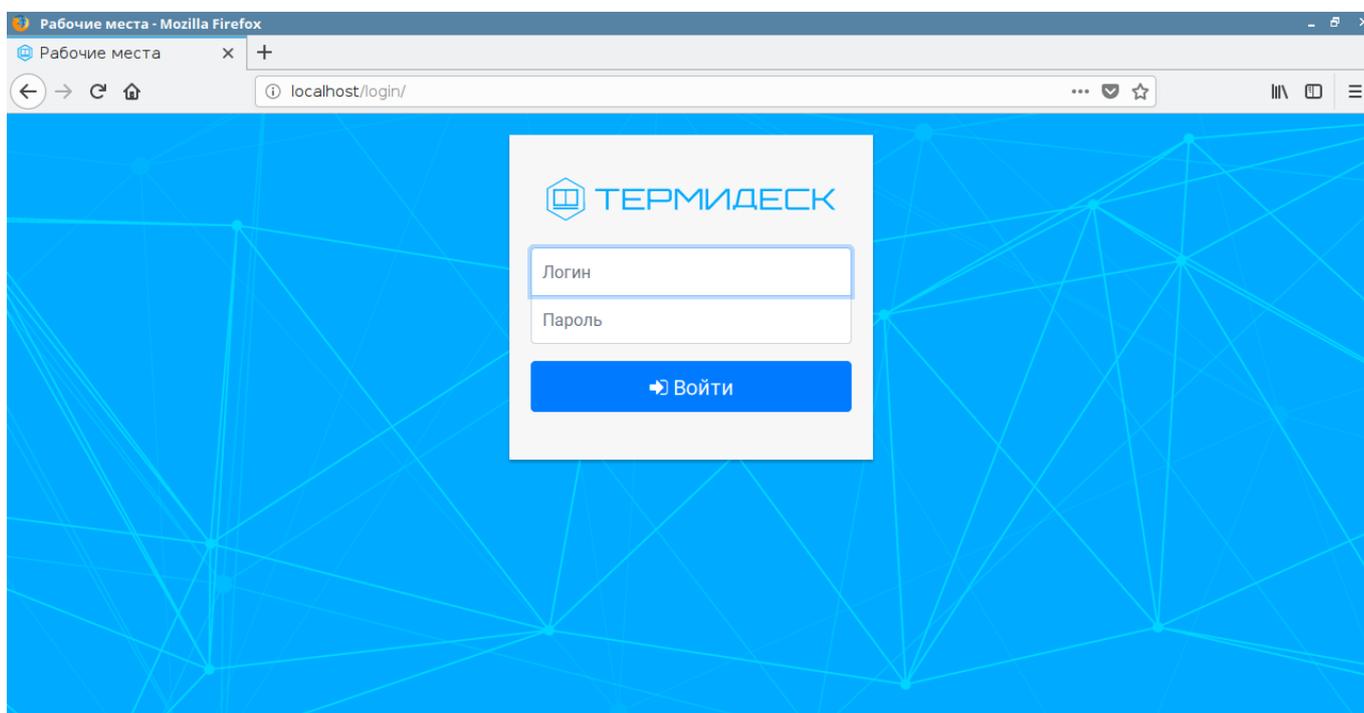


Рисунок 21 – Начальная веб-страница Termidesk

По умолчанию после установки вход в интерфейс управления Termidesk доступен только авторизованному пользователю ОС с ролью «Администратор». Пользователь ОС должен быть членом группы `astra-admin` (1001). Для входа в интерфейс управления в полях «Логин» и «Пароль» необходимо указать идентификатор пользователя ОС и его пароль соответственно, а затем нажать экранную кнопку **[Войти]**.

Проверка добавления ключа от репозитория производителя в ОС выполняется командой:

```
:~$ apt-key list
```

Проверка состояния отделяемых компонентов Termidesk выполняется командами:

```
1 :~$ systemctl status termidesk-vdi.service
2 :~$ systemctl status termidesk-taskman.service
3 :~$ systemctl status termidesk-wsproxy.service
```

Строка «Active» отображает состояние сервиса, где статус «active (running)» свидетельствует об успешном запуске Termidesk.

6. ОБНОВЛЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА

6.1. Комплексное обновление Termidesk

Комплексное обновление подразумевает, что компоненты «Универсальный диспетчер», «Шлюз», «Менеджер рабочих мест» установлены на одном узле.

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

❗ Обновление Termidesk должно осуществляться операцией установки поверх предыдущей версии. В противном случае, если ранее Termidesk был удален без удаления БД, при повторной установке может возникнуть ряд ошибок.

⚠ Если после удаления Termidesk (удаление БД при этом не производилось) возникла необходимость повторной установки программного комплекса, то после инсталляции может понадобиться снова ввести данные для доступа (пароль, токен доступа) в поставщике ресурсов.

⚠ При необходимости понижения версии Termidesk до 4.0 необходимо удалить и пересоздать БД.

⚠ Если в файлы конфигурации и запуска Termidesk вручную были внесены какие-либо изменения, то эти изменения при обновлении не сохраняются.

Перед любым обновлением Termidesk рекомендуется выполнить резервное копирование БД:

```
1 :$ pg_dump -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W >
   <имя_файла_для_сохранения_БД.sql>
```

где:

-d <наименование БД> - имя БД. При стандартных настройках используется имя termidesk;
 -h <IP-адрес_хоста> - IP-адрес узла, где расположена БД. Если БД устанавливалась локально, нужно указать localhost;
 -p <порт> - порт для подключения к БД. При стандартных настройках используется 5432;
 -U <пользователь> - имя пользователя для подключения. При стандартных настройках используется имя termidesk;

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

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

Для комплексного обновления Termidesk нужно:

- остановить службы Termidesk:

```
:$ sudo systemctl stop termidesk-vdi termidesk-wsproxy termidesk-taskman termidesk-celery-beat termidesk-celery-worker
```

- удалить кеш файла ответов debconf командами:

```
1  :$ sudo rm -f /var/cache/debconf/config.dat
2  :$ sudo rm -f /var/cache/debconf/config.dat-old
```

где:

-f - ключ игнорирования несуществующих файлов;

- подключить репозиторий Termidesk (см. подраздел **Получение пакетов установки**);
- выполнить обновление:

```
:$ sudo apt install -y termidesk-vdi
```

где:

-y - ключ для пропуска подтверждения установки.

- в диалогах ввода параметров подключения к СУБД и КД нужно нажать экранную кнопку **[OK]**;

⚠ Диалог настройки подключений к серверам RabbitMQ-server отображается в том случае, если в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` ранее не были заданы параметры `RABBITMQ_URL`.

- в диалоге выбора компонента Termidesk в случае комплексного обновления все пункты должны быть отмечены «*» и нужно нажать экранную кнопку **[OK]**.

⚠ Начиная с версии Termidesk 4.1 изменена политика лицензирования программного комплекса.

Лицензии ограничены доступными поставщиками ресурсов и протоколами доставки. Все ранее выпущенные лицензии считаются неограниченными.

При активации лицензии с ограничениями, все объекты, связанные с нелицензированными поставщиками или протоколами, будут недоступны.

Если нужно выполнить обновление без подключения репозитория (при наличии deb-пакета) следует выполнить команду:

```
:$ sudo apt install -y <путь к deb-пакету termidesk-vdi>
```

В случае, если при обновлении появляется сообщение о неразрешенных зависимостях, следует выполнить команду:

```
:$ sudo apt install -f
```

где:

-f - ключ, указывающий, что нужно исправить сломанные зависимости пакетов.

После завершения обновления нужно:

- проверить состояние служб Termidesk:

```
:$ sudo systemctl -a | grep termidesk
```

где:

-a - ключ для вывода списка служб;

grep - утилита для поиска текста в выводе предыдущей команды.

- проверить доступность веб-интерфейса.

6.2 . Обновление для распределенной конфигурации установки

6.2.1 . Общая концепция обновления

Обновление Termidesk, установленного в распределенной отказоустойчивой конфигурации, выполняется в следующей последовательности:

- ⚠ Приведенная здесь процедура обновления предполагает, что используются узлы-шлюзы termidesk-wsproxy. Если ранее на узлах-шлюзах был установлен экспериментальный шлюз termidesk-gateway, необходимо сначала обновить их, и только потом - узлы-диспетчеры и узлы-менеджеры BPM. Шаги 3-8 относятся к обновлению узлов-диспетчеров Termidesk (служба termidesk-vdi). Шаги 9-14 относятся к обновлению узлов-шлюзов Termidesk (служба termidesk-wsproxy). Шаги 15-22 относятся к обновлению узлов-менеджеров BPM (планировщиков заданий) Termidesk (службы termidesk-taskman, termidesk-celery-beat, termidesk-celery-worker).

Шаг 1. На сервер с СУБД, либо на отдельно выделенный сервер, устанавливается и настраивается компонент RabbitMQ-server в случае, если ранее RabbitMQ-server не был установлен.

Шаг 2. Создается резервная копия RSA-ключей, расположенных в каталоге /etc/opt/termidesk-vdi/wsproxy/ для последующей корректной работы диспетчеров и шлюзов.

Шаг 3. На балансировщике нагрузки, отвечающем за распределение подключений к диспетчерам, из списка балансировки (конфигурации nginx) исключается диспетчер, подлежащий обновлению (за раз - только **ОДИН**).

Шаг 4. Действия шага 3 повторяются для каждого существующего балансировщика.

Шаг 5. Обновляется указанный на шаге 3 диспетчер.

Шаг 6. На обновленном диспетчере восстанавливаются RSA-ключи из резервных копий, созданных на шаге 2. Узел перезагружается.

Шаг 7. Выбирается следующий диспетчер, подлежащий обновлению, для него выполняются шаги 3-6.

Шаг 8. По завершении обновления **ВСЕХ** диспетчеров список балансировки восстанавливается до исходного. Проверяется доступность графического интерфейса Termidesk сначала обращением на IP-адрес каждого из диспетчеров, затем обращением на IP-адрес балансировщика нагрузки.

Шаг 9. На балансировщике нагрузки, отвечающем за распределение подключений к шлюзам, из списка балансировки исключается шлюз, подлежащий обновлению (за раз - только **ОДИН**).

Шаг 10. Действия шага 9 повторяются для каждого существующего балансировщика.

Шаг 11. Обновляется указанный на шаге 9 шлюз.

Шаг 12. На обновленном шлюзе восстанавливаются RSA-ключи из резервной копии, созданной на шаге 2. Узел перезагружается.

Шаг 13. Выбирается следующий шлюз, подлежащий обновлению, для него выполняются шаги 9-12.

Шаг 14. По завершении обновления **ВСЕХ** шлюзов список балансировки восстанавливается до исходного.

Шаг 15. На узлах с установленным планировщиком заданий, который работает в отказоустойчивой конфигурации в режиме «SLAVE», должен быть выполнен останов служб keepalived.

Шаг 16. Обновляется выбранный планировщик заданий. Выполняется запуск служб.

Шаг 17. На обновленном планировщике заданий восстанавливаются RSA-ключи из резервной копии, созданной на шаге 2. Узел перезагружается.

Шаг 18. Выполняется запуск служб keepalived.

Шаг 19. На узле с установленным планировщиком заданий, который работает в отказоустойчивой конфигурации в режиме «MASTER», должен быть выполнен останов служб keepalived.

Шаг 20. Обновляется выбранный планировщик заданий. Выполняется запуск служб.

Шаг 21. На обновленном планировщике заданий восстанавливаются RSA-ключи из резервной копии, созданной на шаге 2. Узел перезагружается.

Шаг 22. Выполняется запуск службы keepalived.

⚠ Обновление до Termidesk версии 4.1 возможно, если предыдущая установленная версия не ниже 4.0.

⚠ Если в файлы конфигурации и запуска Termidesk (`/lib/systemd/system/termidesk-*`) вручную были внесены какие-либо изменения, то необходимо выполнить резервное копирование данных файлов, поскольку эти изменения при обновлении сбрасываются до значений по умолчанию.

⚠ Начиная с версии 4.0 конфигурация Termidesk сведена в единый файл `/etc/opt/termidesk-vdi/termidesk.conf`.

В случае, если предыдущая версия Termidesk была установлена на ОС Astra Linux Special Edition 1.6 или Astra Linux Common Edition, то потребуется переустановка ОС и Termidesk.

Тогда для сохранения существующей БД нужно:

- выполнить экспорт БД из Termidesk предыдущей версии;
- выполнить резервное копирование файлов конфигурации и запуска Termidesk (`/lib/systemd/system/termidesk-*`, `/etc/opt/termidesk-vdi/wsproxy/*`);
- выполнить установку ОС Astra Linux Special Edition 1.7;
- выполнить установку и настройку RabbitMQ-server согласно подразделам **Установка брокера сообщений RabbitMQ-server** и **Настройка брокера сообщений RabbitMQ-server**;
- выполнить установку и настройку СУБД PostgreSQL-11 согласно подразделам **Установка СУБД Posrgres-11** и **Настройка СУБД Posrgres-11**;
- выполнить импорт ранее сохраненной БД;
- выполнить установку Termidesk согласно подразделу **Распределенная установка программного комплекса**.

6.2.2 . Шаг 1: установка и настройка RabbitMQ-server

Шаг выполняется в соответствии с подразделами **Установка RabbitMQ-server** и **Настройка RabbitMQ-server** при отсутствии ранее установленного RabbitMQ-server.

6.2.3 . Шаг 2: резервное копирование RSA-ключей

Выполнить резервное копирование RSA-ключей с одного из узлов-диспетчеров. Резервные копии ключей можно скопировать, например, на другой сетевой узел командой:

```
~$ sudo scp -r /etc/opt/termidesk-vdi/wsproxy localuser@ipaddr_or_fqdn_host:/home/localuser/
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

localuser - имя пользователя целевого узла;
 ipaddr_or_fqdn_host - IP-адрес или FQDN целевого узла;
 /home/user - путь, куда будет скопирован каталог.

6.2.4 . Шаг 3: редактирование конфигурации балансировщика нагрузки

На балансировщике нагрузки нужно открыть и отредактировать файл `/etc/nginx/sites-available/sampledmain.ru.conf`.

В данном конфигурационном файле следует найти директиву `daas-upstream-nodes` с перечислением списка диспетчеров, выбрать первый по списку диспетчер, закомментировать его и сохранить файл.

Пример для списка балансировки:

⚠ Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре предприятия.

```

1 upstream daas-upstream-nodes {
2     least_conn;
3     server 192.0.2.30;
4     server 192.0.2.31;
5     server 192.0.2.32;
6
7 }
```

Для исключения первого по списку диспетчера файл приводится к виду:

```

1 upstream daas-upstream-nodes {
2     least_conn;
3     # server 192.0.2.30;
4     server 192.0.2.31;
5     server 192.0.2.32;
6
7 }
```

После изменения файла нужно перезапустить веб-сервер:

```

:~$ sudo systemctl restart nginx
```

6.2.5 . Шаг 4: редактирование конфигурации остальных балансировщиков нагрузки

На всех существующих балансировщиках нагрузки выполнить **Шаг 3**.

6.2.6 . Шаг 5: обновление диспетчера

Процедура обновления проводится с помощью установки новой версии Termidesk поверх уже имеющейся и не отличается от процесса, описанного в пункте **Неавтоматизированная установка Termidesk** за исключением отсутствия необходимости корректировки файла конфигурации веб-сервера.

⚠ При установке диспетчера Termidesk необходимо выбрать компонент «Broker» в диалоговом окне псевдографического интерфейса инсталлятора.

⚠ Корректировка файла `/etc/apache2/apache2.conf`, описанная в пункте **Неавтоматизированная установка Termidesk**, при обновлении не производится.

Перед запуском процедуры обновления нужно:

- остановить службу Termidesk:

```
~$ sudo systemctl stop termidesk-vdi
```

- удалить кеш файла ответов debconf командами:

```
1 ~$ sudo rm -f /var/cache/debconf/config.dat
2 ~$ sudo rm -f /var/cache/debconf/config.dat-old
```

где:

`-f` - ключ игнорирования несуществующих файлов.

6.2.7 . Шаг 6: восстановление RSA ключей из резервной копии

Выполнить копирование сохраненных на **Шаге 2** RSA ключей на узел с обновленным диспетчером.

Затем перезагрузить узел:

```
~$ sudo reboot
```

После загрузки узла проверить состояние служб:

```
~$ sudo systemctl -a | grep termidesk
```

где:

`-a` - ключ для вывода списка служб;

`grep` - утилита для поиска текста в выводе предыдущей команды.

Проверить доступность веб-интерфейса диспетчера Termidesk через веб-браузер.

6.2.8 . Шаг 7: обновление следующего по списку диспетчера

Необходимо выполнить действия с **Шага 3** по **Шаг 6** для следующего по списку диспетчера.

При выполнении **Шага 3** ранее закомментированный элемент остается в том же состоянии, дополнительно нужно закомментировать строку со следующим диспетчером.

6.2.9 . Шаг 8: восстановление конфигурации балансировщика нагрузки

По завершении обновления **ВСЕХ** диспетчеров список балансировки на **ВСЕХ** балансировщиках восстанавливается до исходного.

Ранее закомментированные строки нужно раскомментировать, затем выполнить перезагрузку службы nginx на каждом балансировщике:

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

Выполнить проверку доступности графического интерфейса Termidesk через веб-браузер сначала обращением на IP-адрес каждого из диспетчеров, затем обращением на IP-адрес балансировщика нагрузки.

6.2.10 . Шаги 9-14: обновление шлюзов

Обновление шлюзов по своей структуре не отличается от действий по обновлению диспетчеров, за исключением выбора устанавливаемого компонента.

⚠ При установке шлюза Termidesk необходимо выбрать компонент «Gateway» в диалоговом окне псевдографического интерфейса инсталлятора.

При редактировании файла `/etc/nginx/sites-available/sampledomain.ru.conf` следует найти директиву `daas-upstream-ws` с перечислением списка шлюзов и выполнить исключение (комментирование строк) шлюзов.

Перед запуском процедуры обновления шлюзов нужно:

- остановить службы шлюза:

```
~$ sudo systemctl stop termidesk-wsproxy
```

- удалить кеш файла ответов debconf командами:

```
1 ~$ sudo rm -f /var/cache/debconf/config.dat
2 ~$ sudo rm -f /var/cache/debconf/config.dat-old
```

После завершения установки необходимо убедиться, что в файле `/etc/opt/termidesk-vdi/termidesk.conf` параметр `WSPROXY_BIND_ADDRESS` приведен к следующему виду:

```
WSPROXY_BIND_ADDRESS="0.0.0.0"
```

6.2.11 . Шаг 15: останов служб на менеджере BPM

На узлах с установленным менеджером BPM, работающем в отказоустойчивой конфигурации в режиме «SLAVE», выполняется останов службы `keepalived` командой:

```
:~$ sudo systemctl stop keepalived
```

6.2.12 . Шаг 16: обновление менеджеров BPM

Обновление менеджера BPM по своей структуре не отличается от действий по обновлению диспетчеров, за исключением выбора устанавливаемого компонента.

⚠ При установке менеджера BPM Termidesk необходимо выбрать компонент «Task manager» в диалоговом окне псевдографического интерфейса инсталлятора.

Перед запуском процедуры обновления менеджера BPM нужно:

- остановить службы Termidesk:

```
:~$ sudo systemctl stop termidesk-taskman termidesk-celery-beat termidesk-celery-worker
```

⚠ При остановке службы на менеджере BPM, находящемся в режиме «SLAVE», команда может выдать ошибку - это нормальное поведение.

- удалить кеш файла ответов `debconf` командами:

```
1 :~$ sudo rm -f /var/cache/debconf/config.dat
2 :~$ sudo rm -f /var/cache/debconf/config.dat-old
```

После установки нужно исключить службу `termidesk-taskman` из автоматического запуска:

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

Исключение службы из автоматического запуска необходимо, поскольку управление ее состоянием производится скриптами режима высокой доступности.

На узле, выбранном в качестве `slave`, нужно не только исключить службу из автоматического запуска, но и остановить ее после обновления:

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

6.2.13 . Шаг 17: восстановление RSA ключей на менеджере BPM

Выполнить копирование сохраненных на **Шаге 2** RSA-ключей на узел с обновленным менеджером BPM.

Затем перезагрузить узел:

```
:~$ sudo reboot
```

6.2.14 . Шаг 18: восстановление службы keepalived

Выполнить запуск службы keepalived командой:

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

6.2.15 . Шаги 19-22: обновление основного менеджера ВРМ

Обновление осуществляется аналогично **Шагам 15-18**.

7. УДАЛЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА

Для удаления Termidesk необходимо:

- если установка Termidesk была выполнена с использованием подключенного репозитория, ввести команду:

```
~$ sudo aptitude purge -y termidesk-vdi
```

где:

-y - ключ для пропуска подтверждения удаления;

- если установка Termidesk была выполнена из deb-пакета без использования подключенного репозитория, ввести команду:

```
~$ sudo dpkg -P termidesk-vdi
```

- после удаления Termidesk нужно очистить оставшиеся зависимости и конфигурации:

```
~$ sudo aptitude purge ~c -y
```

Команда полностью удалит оставшиеся настройки и зависимости уже удаленных пакетов.

Для удаления БД и роли пользователя следует выполнить следующие действия, строго соблюдая их последовательность:

- переключиться на пользователя postgres (через пользователя root):

```
1 ~$ sudo -s
2 ~/home/astra# su postgres
```

- запустить терминальный клиент СУБД:

```
~/home/astra$ psql
```

- используя интерактивный интерфейс терминального клиента СУБД, удалить БД:

```
postgres=# DROP DATABASE termidesk;
```

- удалить роль пользователя БД:

```
postgres=# DROP ROLE termidesk;
```

- выйти из интерактивного интерфейса терминального клиента СУБД:

```
postgres=# \q
```

- выйти из сеанса пользователя postgres командой:

```
~/home/astra$ exit
```

- удалить оставшийся каталог с файлами, содержащими переменные для подключения к БД, сертификат и ключ:

```
~$ sudo rm -R /etc/opt/termidesk-vdi
```

где:

-R - ключ для рекурсивного действия. Будут удалены все вложенные подкаталоги.

8. ЛИЦЕНЗИРОВАНИЕ

8.1 . Получение лицензионного ключа

Для Termidesk предусмотрены следующие варианты лицензирования:

- Termidesk VDI (поддержка совместимых платформ виртуализации и серверов терминалов);
- Termidesk Terminal (поддержка только серверов терминалов для ОС Windows (MS RDS/MS RDSH) и Astra Linux (STAL)).

В рамках доступных вариантов лицензирования существует поддержка двух типов лицензий:

- по пользователям - лицензия привязывается к пользователю системы;
- по конкурентным соединениям - лицензия привязывается к количеству одновременных подключений пользователей через систему.

⚠ Начиная с версии Termidesk 4.1 изменена политика лицензирования программного комплекса.
 Все ранее выпущенные лицензии считаются неограниченными.
 При активации лицензии с ограничениями, все объекты, связанные с нелицензированными поставщиками ресурсов или протоколами доставки, будут недоступны.

Дистрибутив Termidesk распространяется с предустановленным лицензионным ключом, имеющим ограничение на 4 (четыре) одновременных подключения для ознакомительных целей. Дистрибутив предназначен для проведения испытания, ознакомления или демонстрации его функциональных возможностей. Дистрибутив для ознакомительных целей может предоставляться без заключения соответствующего договора на срок 90 (девяносто) календарных дней. Подробнее с условиями лицензионного соглашения с конечным пользователем можно ознакомиться на сайте компании: <https://termidesk.ru/eula.pdf>.

Для получения дополнительных лицензионных ключей с целью ознакомления необходимо перейти по ссылке <https://termidesk.ru/products/#request-key> и сформировать запрос, заполнив корректными данными следующие экранные поля:

- «Корпоративный email»;
- «Имя лица, запрашивающего лицензию»;
- «Системный UUID»;
- «Согласие на обработку персональных данных».

Информация о системном UUID располагается в графическом интерфейсе управления «Настройка - Лицензия - Система», пример показан на рисунке (см. Рисунок 22).

⚠ Для получения лицензионного ключа при распределенном варианте установки Termidesk, необходимо предоставить в запросе системные UUID всех узлов с компонентом «Универсальный диспетчер» и всех узлов с компонентом «Менеджер рабочих мест». Информацию о системном UUID в этом случае необходимо получить для каждого узла из файла `/sys/devices/virtual/dmi/id/product_uuid`, выполнив команду на нужном узле:

```
~$ sudo cat /sys/devices/virtual/dmi/id/product_uuid
```

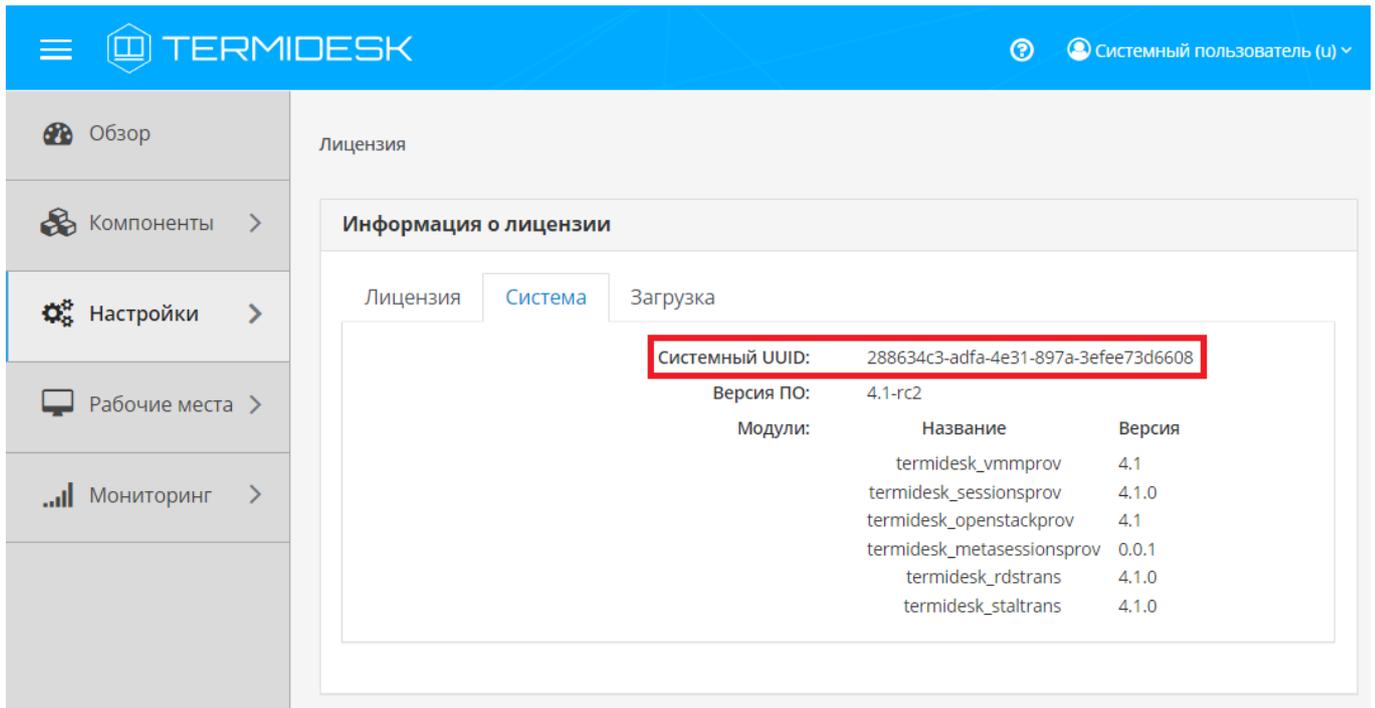


Рисунок 22 – Расположение информации о системном UUID

По завершении заполнения полей нужно нажать экранную кнопку **[Отправить запрос ключа активации]**.

Для получения лицензионного ключа на приобретенное количество лицензий следует перейти по ссылке <https://termidesk.ru/products/#request-key> и сформировать запрос, заполнив корректными данными следующие экранные поля:

- «Корпоративный email»;
- «Имя лица, запрашивающего лицензию»;
- «Системный UUID»;
- «Согласие на обработку персональных данных».

8.2 . Ввод лицензии

Для добавления лицензионного ключа в Termidesk в графическом интерфейсе управления следует перейти «Настройки - Лицензия - Загрузка». Нажав экранную кнопку **[Выбрать]**, указать путь к файлу с лицензионным ключом (см. Рисунок 23), а затем нажать экранную кнопку **[Загрузить]**.

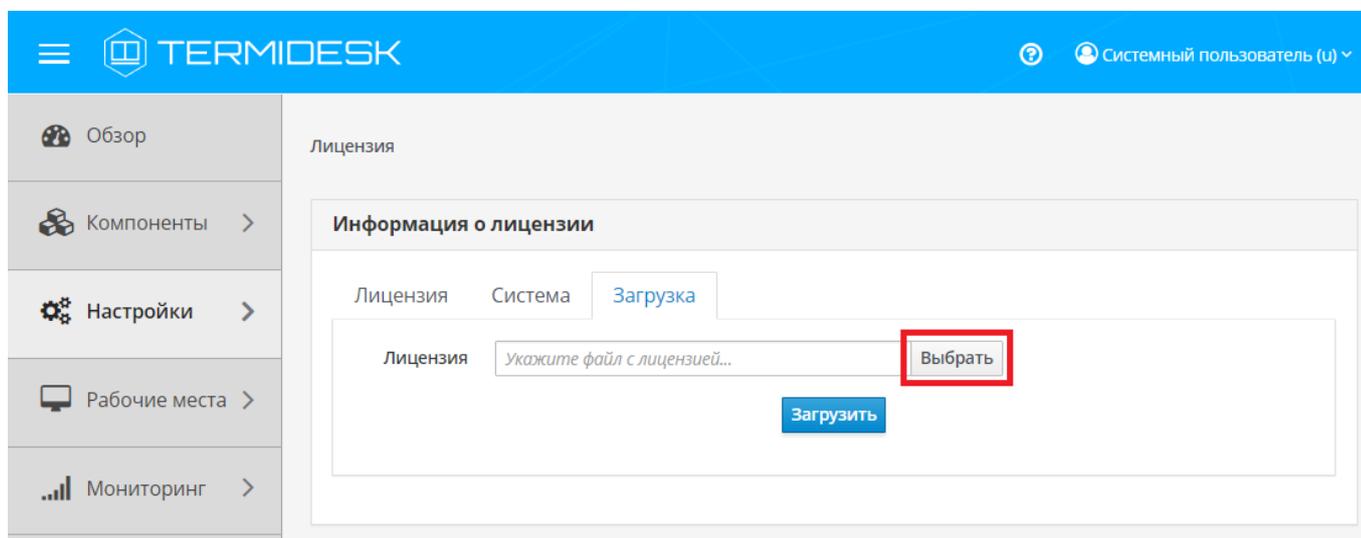


Рисунок 23 – Окно добавления файла с лицензией

8.3 . Проверка сведений о лицензии

Для просмотра информации об используемом лицензионном ключе следует перейти в графический интерфейс управления, выбрать «Настройки - Лицензия - Лицензия» и просмотреть сведения в следующих экранных полях:

- «Имя» – системное имя устройства, где функционирует Termidesk;
- «Организация» – наименование организации, для которой сформирован лицензионный ключ;
- «Email» – адрес электронной почты, указанный при запросе лицензионного ключа;
- «Конкурентные соединения» – максимально возможное количество одновременных соединений с ВРМ;
- «Доступные гостевые ОС» – варианты доступных для установленного вида лицензии гостевых ОС.

9. ПЕРЕЧЕНЬ ТЕРМИНОВ

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

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

10 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
БД	База данных
ВМ	Виртуальная машина
ВРМ	Виртуальное рабочее место
ЗПС	Замкнутая программная среда
КД	Контроллер домена
ОС	Операционная система
ПК СВ Брест	Программный комплекс «Средства виртуализации «Брест»
ПО	Программное обеспечение
СУБД	Система управления базами данных
ЭЦП	Электронная цифровая подпись
API	Application Programming Interface (программный интерфейс приложения)
DHCP	Dynamic Host Configuration Protocol (протокол назначения сетевого адреса)
DNS	Domain Name System (система доменных имен)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
HTML	Hypertext Markup Language (язык гипертекстовой разметки)
IP	Internet Protocol (межсетевой протокол)
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов)
MAC	Media Access Control (уникальный идентификатор сетевого устройства)
MS AD	Microsoft Active Directory (служба каталогов Microsoft)
NTP	Network Time Protocol (протокол сетевого времени)
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)
RSA	Rivest, Shamir and Adleman (криптографический алгоритм с открытым ключом)
SPICE	Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)
STAL	Terminal Server Astra Linux (сервер терминалов ОС Astra Linux Special Edition (Server))
Termidesk	Программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk»
UUID	Unique User Identifier (уникальный идентификатор пользователя)

Сокращение	Пояснение
vGPU	Virtual Graphics Processing Unit (виртуальный графический процессор)
VNC	Virtual Network Computing (система удаленного доступа к рабочему столу компьютера)



© ООО «УВЕОН - ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

Адрес: 119571, г. Москва, Ленинский проспект, д. 119А, помещ. 9Н

Сайт: <https://termidesk.ru>

Телефон: +7 (495) 975-1-975

Общий e-mail: info@uveon.ru

Отдел продаж: sales@uveon.ru

Техническая поддержка: support@uveon.ru