Ограничения и особенности

В этом разделе приведены ограничения и особенности СТД «Термит».

- В СТД «Термит» не предусматривается установка всех компонентов на одном сервере, в том числе и в тестовой среде.
- Не работают пароли на русском языке при подключении к терминальным серверам на Linux.
- При запуске некоторые приложения (например, Firefox) на Windows Server RDS 2012 R2 могут сразу закрываться после запуска сессии.
- Только для серверов на Windows: количество серверов должно быть не меньше количества приложений, одновременно запускаемых пользователем.
- Только для серверов на Windows: переподключение сессий на десктоп-клиенте Linux не работает, если приложение (remote app) было запущено с десктоп-клиента Windows. И также переподключение сессий на десктоп-клиенте Windows не работает, если приложение (remote app) было запущено с десктоп-клиента Linux.
- Не работают символические ссылки в пути подключаемого диска через десктоп-клиент на терминальных серверах Linux. Необходимо указывать реальный путь до файла или директории.
- Для X2Go подключение USB-флеш-накопителя в качестве подключаемого диска не работает.
- Не используйте символ двоеточия (:) в названиях монтируемых каталогов при подключении к серверу, иначе эти каталоги не будут примонтированы.
- Не рекомендуется использовать домен верхнего (первого) уровня.
- При использовании типа каталога FreeIPA с большим количеством объектов (от 2 000): пользователей или групп — необходимо изменить лимиты сервера FreeIPA. Подробнее в решении типовых проблем.
- При подключении сетевых дисков для терминальных серверов:
  - на Linux в пути используется только значение переменной окружения $USER;
  - на Windows в пути подставляются значения всех доступных переменных окружения, включая %USERNAME%.
- Для правильного отображения времени сессии необходимо, чтобы время на брокере и в базе данных совпадало.
- Не поддерживается копирование средствами drag-and-drop. Чтобы в RDP-сессиях перенести файлы из терминальной сессии на десктоп-клиент и обратно, используйте сочетание клавиш `Ctrl+C` и `Ctrl+V`. В X2Go-сессиях перенос файлов на десктоп-

клиент ограничен содержимым, поэтому возможно только копирование текста или данных внутри файла через буфер обмена.

- Поддерживается подключение сетевых дисков только по протоколу SMB.
- В RDP-сессиях, запущенных на десктоп-клиенте Windows, локальные диски подключаются полностью.
- Если путь к приложению содержит пробелы (например, в имени папки или файла), то для корректного выполнения команды этот путь нужно заключить в кавычки, например "C:\Users\Public\Desktop\Google Chrome.lnk".
- Поддерживается только TCP-балансировка нагрузки, то есть балансировщик должен работать в режиме SSL Passthrough.
- При включенной аутентификации по Kerberos запрашивается пароль для открытия RDP-сессии с клиентской машины под управлением Linux.
- Не поддерживается аутентификация по Kerberos для учетных записей с выбранным дополнительным UPN суффиксом (alternative UPN suffix).
- В качестве ОС для терминального сервера не поддерживается Astra Linux в режиме ЗПС. Допустима только редакция без режима ЗПС.

Обзор

Термит — это система терминального доступа (СТД). Предназначена для организации удаленного доступа конечных пользователей к приложениям и рабочему столу, опубликованным на терминальных серверах. Пользователи получают защищенный доступ к установленным администраторами ресурсам с учетом назначенных прав доступа и текущей нагрузки на серверы.

Возможности СТД «Термит»:

- поддержка терминальных серверов на базе операционных систем Windows и Linux;
- совместное использование пользователями ресурсов с минимальными усилиями на администрирование и развертывание;
- безопасный доступ к централизованно развернутым приложениям;
- публикация рабочего стола и приложений.

Десктоп-клиент СТД «Термит» позволяет пользователям запускать приложения и рабочие столы на терминальных серверах и предоставляет им доступ к рабочей среде предприятия. Вы можете использовать современные операционные системы, включая Windows, Linux и MacOS.

Десктоп-клиент СТД «Термит» поддерживает:

- Перенаправление буфера обмена с локального компьютера пользователя в терминальную сессию и обратно.
- Перенаправление звука с локального компьютера пользователя в терминальную сессию и обратно.
- Печать в терминальной сессии на принтер, подключенный к локальному компьютеру пользователя.
- Перенаправление локальной файловой системы в терминальную сессию.
- Перенаправление смарт-карт в терминальных сессиях RDP и X2Go.
- Мониторы с разрешением 4K.

Шаг 2. Базовая конфигурация базы данных

- Повторное использование базы данных (БД) для новой инсталляции невозможно.
- Не поддерживается развертывание БД и брокера на одном сервере.
- В этой инструкции используется последняя доступная версия СУБД PostgreSQL 15. В случае если используется другая версия, то выполняемые команды необходимо изменить. Более подробно можно ознакомиться на сайте документации РЕД ОС.

В этом разделе представлена базовая информация по подготовке сервера баз данных PostgreSQL на РЕД ОС.

1. Установите PostgreSQL с помощью команды:

```
sudo dnf install postgresql15-server
```

2. Инициализируйте базу данных с помощью команды:

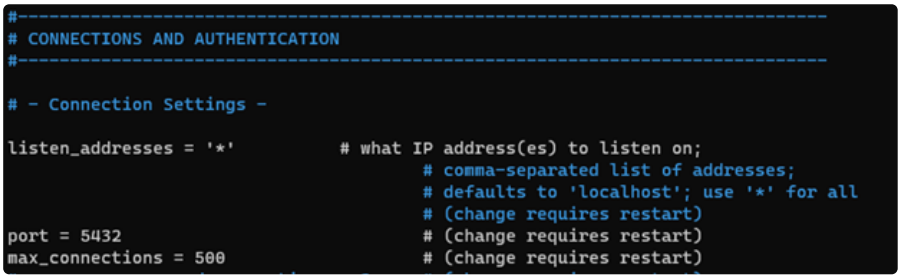
```
sudo postgresql-15-setup initdb
```

3. Запустите сервис PostgreSQL с помощью команды:

```
sudo systemctl enable postgresql-15.service --now
```

4. Чтобы разрешить удаленное подключение к СУБД, в файле конфигурации `/var/lib/pgsql/15/data/postgresql.conf` параметр `listen_addresses` должен соответствовать значению `'*'`:

В инструкции предлагается установить для параметра `listen_addresses` значение * . Это позволит принимать подключения по всем доступным сетевым интерфейсам. Если требуется ограничить доступ только к определенному интерфейсу, то укажите конкретный IP-адрес или имя интерфейса вместо * . Например: `listen_addresses`='192.168.1.1' или `listen_addresses`='eth0'. Это поможет ограничить подключение к СУБД только с нужного интерфейса, обеспечивая дополнительный уровень безопасности.



Отображение параметров на скриншоте может отличаться. Зависит от версии PostgreSQL.

5. Чтобы обеспечить достаточное количество слотов для подключений в высоконагруженной системе, в файле конфигурации `/var/lib/pgsql/15/data/postgresql.conf` параметр `max_connections` должен соответствовать значению `500`.

6. Чтобы разрешить удаленное подключение к СУБД с паролем, добавьте в файл конфигурации `/var/lib/pgsql/15/data/pg_hba.conf` строку:

```
host    all             all             0.0.0.0/0               password
```

BASH

В инструкции предлагается добавить в файл конфигурации `/var/lib/pgsql/15/data/pg_hba.conf` строку:

```
host    all             all             0.0.0.0/0               password
```

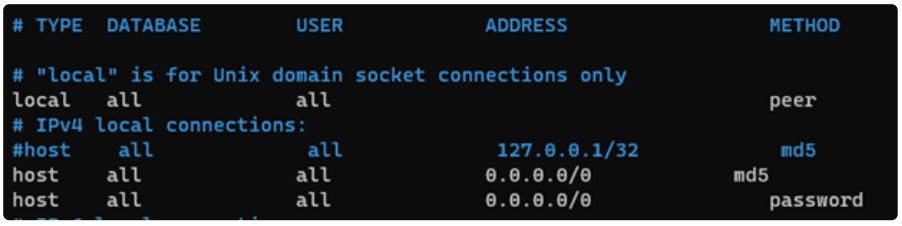
BASH

Эта строка разрешает подключение к СУБД с использованием пароля со всех IP-адресов. Для повышения безопасности рекомендуется указать конкретные IP-адреса или диапазоны адресов, с которых будут разрешены подключения. Например:

```
host    all             all             192.168.1.0/24          password
```

BASH

Это ограничит доступ к СУБД только для адресов в указанном диапазоне, снижая риск несанкционированных подключений.



Отображение параметров на скриншоте может отличаться. Зависит от версии PostgreSQL.

7. Запустите сессию служебного пользователя postgres с помощью команды:

```
sudo su - postgres
```

BASH

8. Запустите командную оболочку postgres с помощью команды:

```
psql
```

BASH

9. Создайте нового пользователя с паролем и правами на создание новых баз данных с помощью команды:

```
CREATE USER %Имя_Пользователя% WITH PASSWORD '%Пароль_Пользователя%'
CREATEDB;
```
BASH

10. Выйдите из командной оболочки psql и сессии пользователя postgres с помощью команды:

```
exit
```
BASH

11. Перезапустите сервис PostgreSQL с помощью команды:

```
sudo systemctl restart postgresql-15.service
```
BASH

Далее перейдите к установке брокера.

Шаг 1. Подготовка окружения

Этот сценарий предполагает установку компонентов на операционных системах (ОС) на РЕД ОС 7.3.4 и Windows Server 2019. Установку на других ОС смотрите в руководстве по установке.

Для подготовки окружения:

> В СТД «Термит» не предусматривается установка всех компонентов на одном сервере, в том числе и в тестовой среде.

1. Проверьте, что подсети Docker Compose не пересекаются с сетями для серверов баз данных, LDAP-каталогов, терминалов и брокеров. Подробнее в статье Ошибки при пересечении IP-адресов между Docker и хост-системой.
2. Разверните минимум четыре виртуальные машины (ВМ):
   - для терминального сервера на Windows и Linux;
   - для брокера. На этой ВМ будет устанавливаться сервис;
   - для сервера баз данных.

   Подробнее о базовой архитектуре.
3. Подготовьте клиентскую машину на Windows или Linux.
4. Проверьте доступ к службе каталогов AD.
5. Введите терминальный сервер в домен службы каталогов.
6. Проверьте с помощью команд `nslookup`, `ping`, что брокер, терминальный сервер и база данных зарегистрирован на DNS-сервере и доступен. В выводе команды не должно быть ошибок.
7. В каталоге пользователей:
   a. создайте сервисную учетную запись для синхронизации объектов из службы каталогов. Обязательно отключите опцию «User must change password at next logon» и включите «Password never expires»;
   b. создайте три группы, например «termit admins», «termit helpdesk» и «termit users»;
   c. добавьте в состав групп учетные записи пользователей для взаимодействия с СТД «Термит».

Далее перейдите к настройке базы данных.

Шаг 4. Настройка брокера

В этом разделе описано, как создать сервер и группу серверов, настроить LDAP, добавить роли и опубликовать приложение.

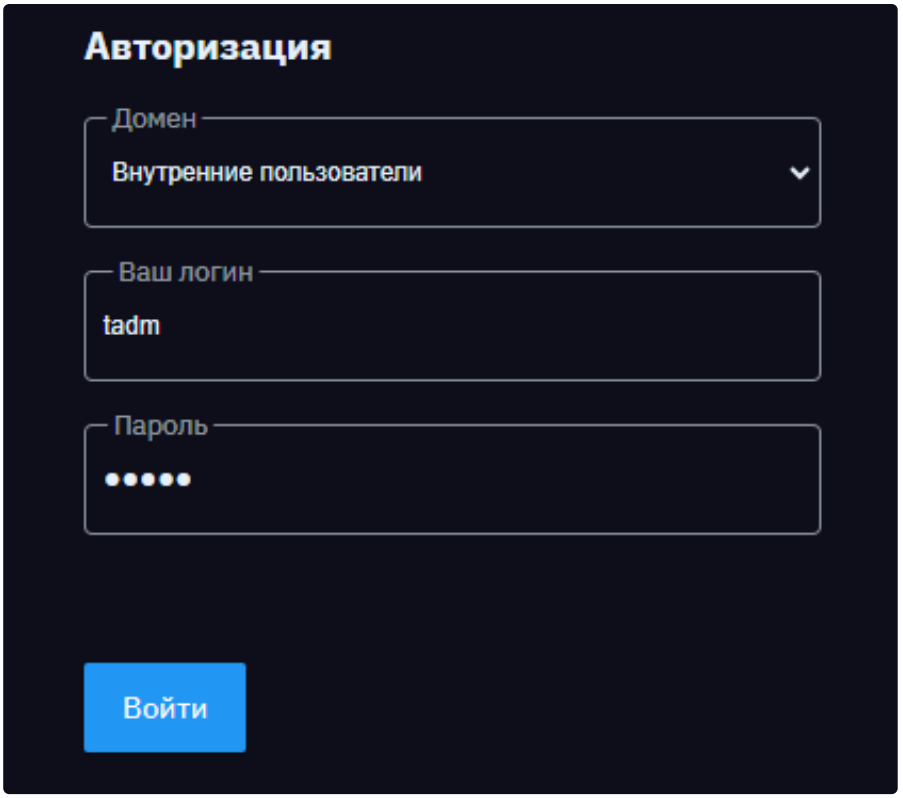
Не поддерживается развертывание БД и брокера на одном сервере.

1. Создание сервера

Чтобы создать терминальный сервер:

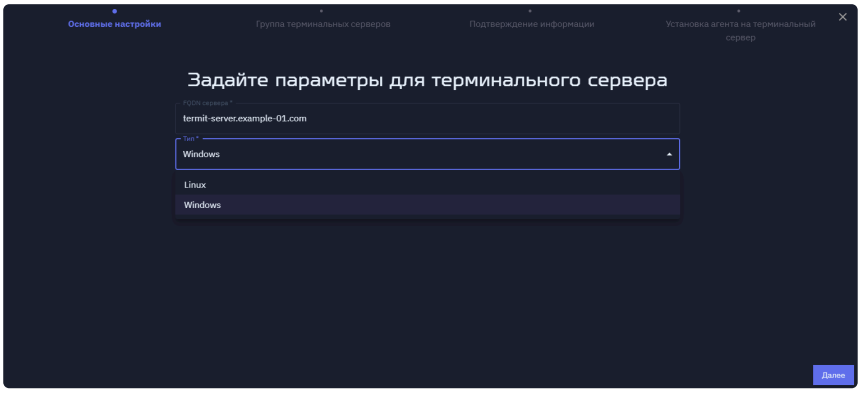
1. В адресной строке браузера введите адрес брокера, например https://broker.example.com.
2. Выберите источник авторизации:
   - **Авто**. Система автоматически выберет LDAP-каталог из списка доступных каталогов или внутренних пользователей.
   - **Внутренние пользователи**. Вход будет выполнен под учетной записью локального администратора «tadm».
   - **Имя LDAP-каталога**, отображаемое полное имя которого было задано при добавлении в систему, например «ldap123».
3. Для входа под учетной записью локального администратора системы укажите в поле ввода:
   - **Ваш логин** — «tadm».
   - **Пароль** — пароль по умолчанию «admin».

     Локальная учетная запись предназначена только для настроек брокера. Ее нельзя использовать для входа в десктоп-клиент, запуска приложений и рабочих столов.
4. Нажмите **[Войти]**.



После успешного входа в систему откроется интерфейс портала администрирования.

5. На портале администрирования, в левом меню выберите раздел **Серверы**.
6. В правом верхнем углу нажмите **[Создать сервер]**.
7. На вкладке **Новый терминальный сервер**:
   - **FQDN адрес сервера** — укажите FQDN адрес терминального сервера.
   - **Тип** — выберите операционную систему **Linux** или **Windows**.



8. Нажмите **[Далее]**.
9. На вкладке **Группа терминальных серверов** группу выбирать не нужно, так как она еще не создана.
10. Нажмите **[Далее]**.
11. На вкладке **Подтверждение информации** проверьте информацию о сервере и нажмите **[Создать]**.

12. Скопируйте указанную команду в надежное место. Она понадобится после настройки терминального сервера.

Созданный сервер появится в списке со статусом «Включен». Далее перейдите к настройке протокола LDAP.

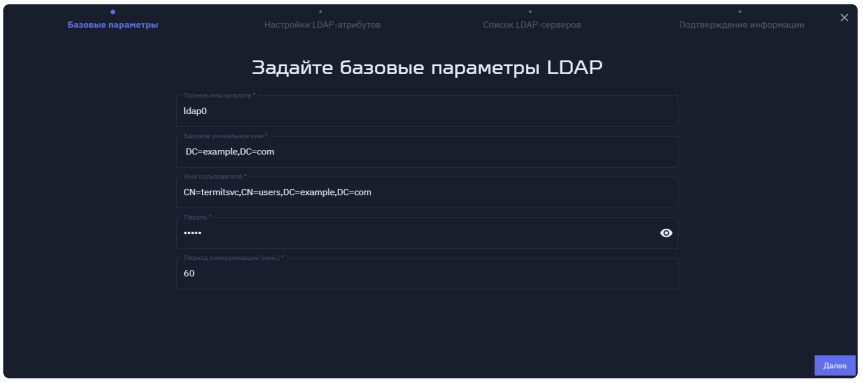
2. Настройка LDAP

В системе для аутентификации пользователей по паролю и получения информации о пользователях, группах и связях между ними используется служба каталогов Active Directory (AD). Подробнее о настройке других LDAP-каталогов смотрите в руководстве администратора.

Также поддерживаются защищенные протоколы передачи данных LDAP over SSL и LDAP StartTLS.

Чтобы настроить LDAP:

1. В левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **LDAP-каталоги** и нажмите **[Добавить LDAP]**.
3. Задайте параметры для подключения службы каталогов:
   - **Полное имя каталога** — отображаемое имя в списке LDAP-каталогов и при входе в систему.
   - **Базовое уникальное имя**. Например, для домена example.com: «DC=example,DC=com».
   - **Имя пользователя**. Например, для домена example.com: CN=termitsvc,CN=users,DC=example,DC=com.
   - **Пароль** — пароль от сервисной учетной записи.
   - **Период синхронизации (мин)**.



4. Нажмите **[Далее]**.
5. Чтобы настроить параметры используемого типа LDAP:
   - **Тип LDAP каталога** — выберите **AD**:

- **Класс для объекта «Пользователь»** — user
- **Класс для объекта «Группа»** — group
- **Атрибут для идентификации объектов** — objectGUID
- **Атрибут для получения отображаемого имени пользователя** — cn
- **Атрибут для получения отображаемого имени группы** — cn
- **Атрибут для поиска пользователя** — samAccountName
- **Атрибут со списком членов групп** — member
- **Атрибут, содержащий имя объекта, указанное для списка членов групп** — distinguishedName
- **Атрибут, используемый для аутентификации на терминальном сервере Linux** — samAccountName
- **Атрибут, используемый для аутентификации на терминальном сервере Windows** — msDS-PrincipalName
- Для чтения большого количества пользователей в группе включите опцию **Поддержка range для получения членов группы**.

6. Нажмите **[Далее]**.

7. Чтобы добавить адрес сервера LDAP, нажмите ＋.

> Система всегда работает с первым LDAP-сервером. Если сервер становится недоступен, система переходит к следующему.

8. Укажите:

   - **Адрес** — IP-адрес или FQDN LDAP-сервера, например «termit-example-01.com».
   - **Протокол** — выберите из списка:

     > Перед выбором протоколов LDAP over SSL и LDAP StartTLS добавьте доверенный сертификат.

     - **LDAP** — технология шифрования данных при подключении к LDAP-серверу не используется. Данные передаются в открытом виде по порту 389. Не рекомендуется использовать в продуктовых инсталляциях.
     - **LDAP over SSL** — защищенная версия протокола LDAP, которая использует технологию шифрования SSL/TLS при подключении к LDAP-серверу по порту 636.
     - **LDAP StartTLS** — защищенная версия протокола LDAP, при использовании которой сначала устанавливается незащищенное соединение по порту 389, а затем отправляется запрос на шифрование.

- **Порт** — порт выбирается автоматически в зависимости от выбранного протокола. При необходимости параметр можно изменить.

9. Нажмите **Сохранить** > **Далее**.
10. На вкладке **Подтверждение информации** проверьте информацию о сервере LDAP и соединение. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

    При успешном соединении появится сообщение «Проверка соединения прошла успешна».
11. Нажмите **[Сохранить]**.

    Состояние синхронизации LDAP и системы смотрите в разделе Журнал событий.

LDAP настроен. Перейдите к добавлению ролей.

3. Настройка ролей

В системе предусмотрены следующие роли:

- **Администраторы**. Администраторы могут полностью контролировать систему, например, управлять серверами, пользователями и приложениями.
- **Служба поддержки**. Служба поддержки может просматривать настройки, информацию о серверах и сессиях в разделе **Обзор**, журнал событий, список сессий, завершать сессии и блокировать пользователей. Выполняет функцию L1 технической поддержки.
- **Пользователи**. У пользователей есть учетные записи, с помощью которых они имеют доступ к СТД «Термит». Только пользователи могут запускать приложения.
- **Аудитор ИБ**. Аудитор ИБ может просматривать настройки, информацию о серверах и сессиях в разделе **Обзор**, журнал событий, список сессий.

Чтобы добавить роли:

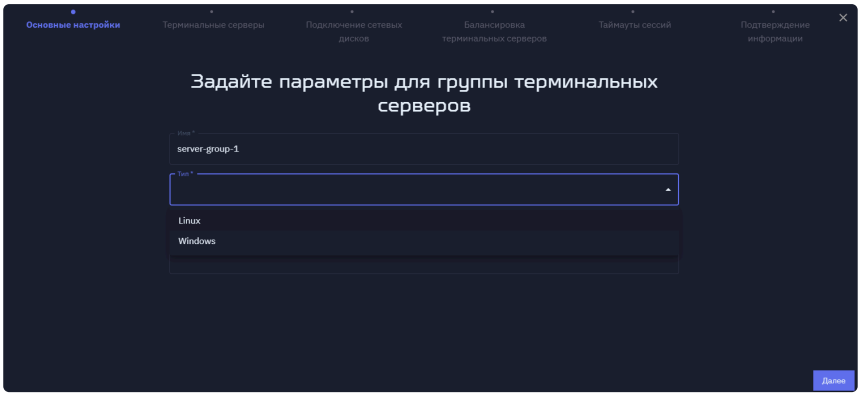
1. В разделе **Настройки** перейдите на вкладку **Роли**.
2. Наведите курсор на **Администраторы** и нажмите ✎.
3. Нажмите ＋.
4. Добавьте группы из каталога пользователей для роли администраторов. Можно добавить несколько групп. Также поддерживаются вложенные группы.
5. Нажмите **Сохранить** > **Сохранить**.

Для ролей **Служба поддержки**, **Пользователи** и **Аудитор ИБ** повторите действия из шагов 3-5.

4. Создание группы серверов

Чтобы создать группу серверов:

1. В левом меню выберите раздел **Группы серверов**.
2. В правом верхнем углу нажмите **[Создать группу]**.
3. На вкладке **Основные настройки**:
   - **Имя** — укажите название группы терминальных серверов.
   - **Тип** — выберите операционную систему **Linux** или **Windows**.
   - (Опционально) **Описание** — добавьте описание группы серверов.



4. Нажмите **[Далее]**.
5. На вкладке **Терминальные серверы** выберите из списка сервер, который создали ранее.
6. Нажмите **[Далее]**.
7. На вкладке **Подключение сетевых дисков** можно настроить, какие сетевые диски будут доступны пользователям в терминальной сессии. Подробнее смотрите в руководстве администратора.
8. Нажмите **[Далее]**.
9. На вкладке **Балансировка терминальных серверов** оставьте значение весов по умолчанию. Подробнее о балансировке серверов.
10. Нажмите **[Далее]**.
11. На вкладке **Таймауты сессий** оставьте значения по умолчанию. Подробнее смотрите настройки параметров таймаута.
12. Нажмите **[Далее]**.
13. На вкладке **Подтверждение информации** проверьте информацию о группе серверов и нажмите **[Создать]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

Созданная группа появится в списке. Далее перейдите к публикации приложения.

5. Публикация приложения

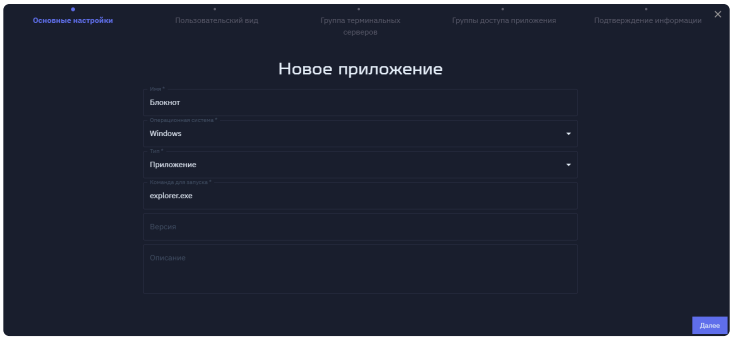
Чтобы добавить приложение:

1. На портале администрирования, в левом меню выберите раздел **Приложения**.
2. Нажмите **[Добавить приложение]**.
3. На вкладке **Основные настройки** задайте параметры:
   - **Имя** — укажите название приложения, например «Блокнот».
   - **Операционная система** — **Linux** или **Windows**.
   - **Тип** — выберите **Приложение** или **Рабочий стол**.

     Чтобы разделить список на приложения и рабочие столы, включите опцию в настройках.
   - **Команда для запуска** — команда для запуска приложения или рабочего стола. Также для запуска приложения можно указать путь к исполняемому файлу и добавить параметры через пробел.

     Если путь к приложению содержит пробелы (например, в названии папки или файла), его необходимо заключить в кавычки для корректного выполнения команды, например `"C:\Users\Public\Desktop\Google Chrome.lnk"`.

     - Команды для запуска рабочего стола:
       - Linux:
         - XFCE — `xfce4-session`
         - MATE — `mate-session`
         - FLY — `fly-wm`
       - Windows:
         - Explorer — `explorer.exe`
     - Команды для запуска приложения (например, top):
       - Linux:
         - XFCE — `xfce4-terminal -e "top"`
         - MATE — `mate-terminal -e "top"`
         - FLY — `fly-term -e "top"`



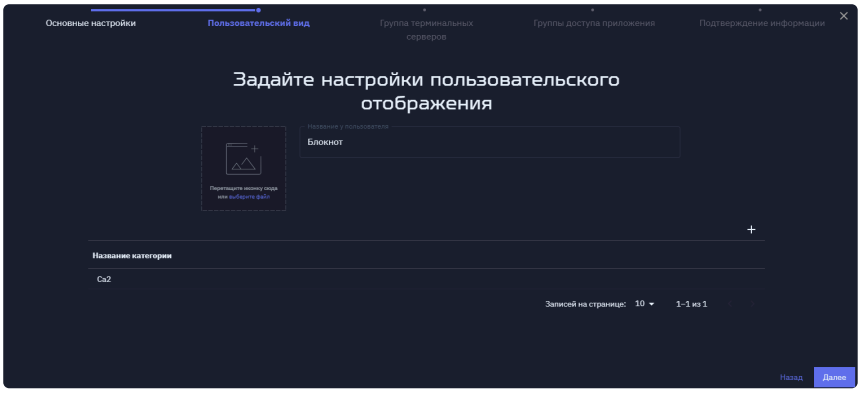
- Короткую команду можно использовать, если:
  - она позволяет запустить приложение напрямую на терминальном сервере;
  - расположение приложения добавлено в переменную среды `PATH`, например `notepad.exe`.
- Не работают переменные для настройки приложений Windows.

- (Опционально) **Версия** — версия приложения.
- (Опционально) **Описание** — описание приложения.

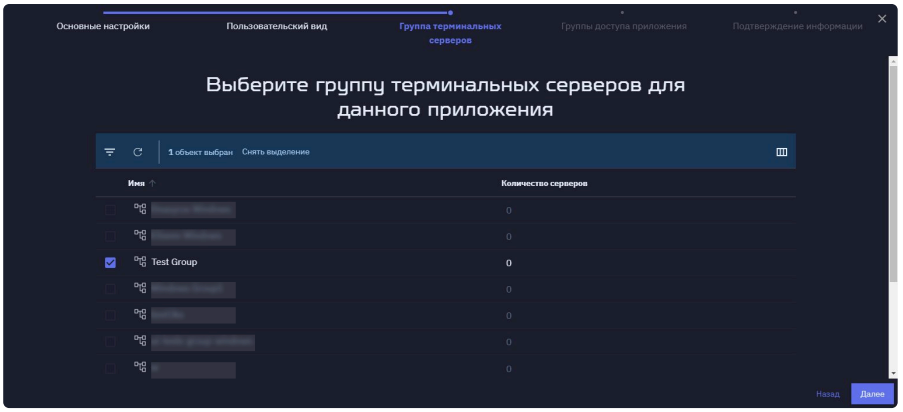
4. Нажмите **[Далее]**.
5. На вкладке **Пользовательский вид** задайте настройки пользовательского отображения. Для этого:
   - (Опционально) Загрузите иконку приложения.

     Максимальное допустимое к загрузке разрешение составляет 128x128 пикселей.

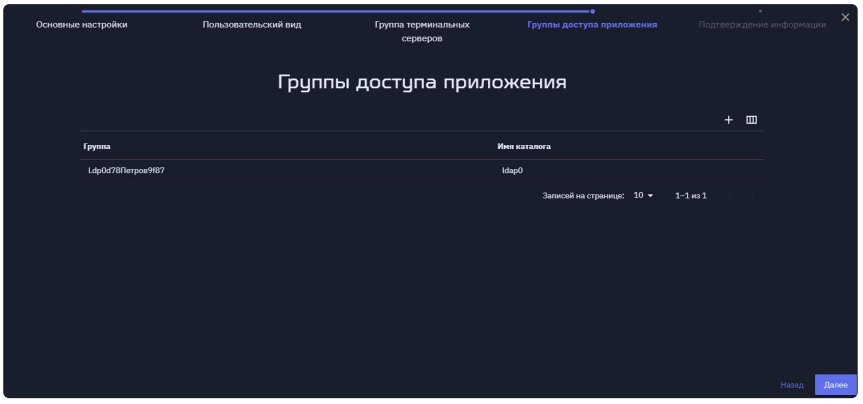
   - (Опционально) **Название у пользователя** — укажите название приложения, которое будет отображаться у пользователя, например «Блокнот».
   - Категорию выбирать не нужно, так как она еще не создана. Подробнее смотрите в в руководстве администратора.



6. Нажмите **[Далее]**.
7. На вкладке **Группа терминальных серверов** выберите группу терминальных серверов для приложения, которую создали ранее.



8. Нажмите **[Далее]**.
9. На вкладке **Группы доступа приложения** добавьте LDAP-группу:
   a. Нажмите ＋ и выберите из списка LDAP-группу, пользователи которой будут иметь доступ к этому приложению. Можно добавлять несколько групп доступа к приложению.



   b. Нажмите **[Сохранить]**.
10. Нажмите **[Далее]**.
11. На вкладке **Подтверждение информации** проверьте информацию о приложении и нажмите **[Создать]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

После создания приложение появится в списке со статусом «Вкл.».

Далее перейдите к настройке терминального сервера.