ПЛАТФОРМА ДОКУМЕНТАЦИЯ ALT LINUX TEAM

Альт Сервер 9.2

Документация

Руководство пользователя

Редакция август, 2021

Аннотация

Добро пожаловать в документацию дистрибутива Альт Сервер. Данное руководство предназначено как для начинающих, так и для опытных пользователей. Руководство описывает подготовку системы для установки, процесс установки дистрибутива, а также процедуру настройки и использования системы.

Данное руководство соответствует текущему состоянию сведений, но какие-либо окончательные правки могли не попасть в него. В случае обнаружения ошибок и неточностей в руководство вносятся изменения.

Часть I. Что такое Альт Сервер?

В этой части рассматривается что такое Linux и Альт Сервер.

Содержание

Глава 1. Что такое Альт Сервер

Операционная система Альт Сервер — многофункциональный дистрибутив для серверов с возможностью использования в качестве рабочей станции разработчика комплексных систем, прежде всего, предназначен для использования в корпоративных сетях.

Альт Сервер представляет собой совокупность интегрированных программных продуктов, созданных на основе ОС Linux и обеспечивает обработку, хранение и передачу информации в круглосуточном режиме эксплуатации. Дистрибутив предоставляет интегрированную операционную систему на единой оптимизированной пакетной базе с поддержкой различных аппаратных платформ, с возможностью установки графического окружения.

Альт Сервер это комплекс серверных приложений, оснащённый удобным пользовательским интерфейсом для настройки. Управление сервером может осуществляться с любого компьютера через веб-браузер.

Альт Сервер представляет собой решение уровня предприятия, позволяющее осуществить миграцию на импортозамещающее программное и аппаратное обеспечение.

Основные преимущества ОС Альт Сервер:

- установка серверных решений и решений конечных пользователей с одного диска;
- графическая рабочая среда MATE;
- возможность как развернуть, так и использовать только определённые службы без Alterator;
- возможность обеспечить единую аутентификацию, общие ресурсы и совместную работу через сервер каталогов.

Глава 2. Что такое Linux

2.1. Свободные программы

Операционная система (далее — ОС) Linux — ядро, основные компоненты системы и большинство её пользовательских приложений — свободные программы. Свободные программы можно:

- запускать на любом количестве компьютеров;
- распространять бесплатно или за деньги без каких-либо ограничений;
- получать исходные тексты этих программ и вносить в них любые изменения.

Свобода программ обеспечила их широкое использование и интерес к ним со стороны тысяч разработчиков. Основные программы для Linux выходят под лицензией GNU General Public License (далее — GPL). Лицензия GNU не только гарантирует свободу, но и защищает её. Она допускает дальнейшее распространение программ только под той же лицензией, поэтому исходный код ядра Linux, компиляторов, библиотеки glibc, пользовательских графических оболочек не может быть использован для создания приложений с закрытым кодом. В этом принципиальное отличие Linux от свободных ОС семейства BSD (FreeBSD, NetBSD, OpenBSD), фрагменты которых вошли в Microsoft Windows и даже стали основой OS X. Linux включает в себя многие разработки BSD, но его компиляторы и системные библиотеки разработаны в рамках проекта GNU (http://www.gnu.org/home.ru.html).

2.2. Разработка Linux

В отличие от распространённых несвободных ОС, Linux не имеет географического центра разработки. Нет фирмы, которая владела бы этой ОС, нет и единого координационного центра. Программы для Linux — результат работы тысяч проектов. Большинство из них объединяет программистов из разных стран, связанных друг с другом только перепиской. Лишь некоторые проекты централизованы и сосредоточены в фирмах. Создать свой проект или присоединиться к

уже существующему может любой программист, и, в случае успеха, результаты этой работы станут известны миллионам пользователей. Пользователи принимают участие в тестировании свободных программ, общаются с разработчиками напрямую. Это позволяет за короткий срок добавлять в программное обеспечение новые возможности, оперативно находить ошибки и исправлять их.

Именно гибкая и динамичная система разработки, невозможная для проектов с закрытым кодом, определяет исключительную экономическую эффективность Linux. Низкая стоимость свободных разработок, отлаженные механизмы тестирования и распространения, привлечение независимых специалистов, обладающих индивидуальным, самостоятельным видением проблем, защита исходного текста программ лицензией GPL — всё это стало причиной успеха свободных программ.

Такая высокая эффективность разработки не могла не заинтересовать крупные фирмы. Они стали создавать свои свободные проекты, основывающиеся на тех же принципах. Так появились Mozilla, LibreOffice, свободный клон Interbase, SAP DB. IBM способствовала переносу Linux на свои мейнфреймы.

Открытый код программ значительно снизил себестоимость разработки закрытых систем для Linux и позволил снизить цену решения для пользователя. Вот почему Linux стала платформой, часто рекомендуемой для таких продуктов, как Oracle, DB2, Informix, Sybase, SAP ERP, Lotus Domino.

2.3. Защищённость

ОС Linux унаследовала от UNIX надёжность и отличную систему защиты. Система разграничения доступа к файлам позволяет не бояться вирусов. Но всё же, программ без ошибок не бывает, и Linux не исключение. Благодаря открытости исходного кода программ, аудит системы может осуществить любой специалист без подписок о неразглашении и без необходимости работы в стенах нанявшей его компании. Сообщества разработчиков и пользователей свободных программ создали множество механизмов оповещения об ошибках и их исправления. Сообщить об ошибке и принять участие в её исправлении независимому программисту или пользователю так же просто, как специалисту фирмы-разработчика или автору проекта. Благодаря этому ошибки защиты эффективно выявляются и быстро исправляются.

2.4. Дистрибутивы Linux

Большинство пользователей для установки Linux используют дистрибутивы. Дистрибутив — это не просто набор программ, а готовое решение для выполнения различных задач пользователя, обладающее идентичностью установки, управления, обновления, а также едиными системами настройки и поддержки.

2.5. Новичку

Linux — самостоятельная операционная система. Все операционные системы разные: Linux — не Windows, не OS X и не FreeBSD. В Linux свои правила, их необходимо изучить и к ним необходимо привыкнуть. Терпение и настойчивость в изучении Linux обернётся значительным повышением эффективности и безопасности вашей работы. То, что сегодня кажется странным и непривычным, завтра понравится и станет нормой.

Не стесняйтесь задавать вопросы, ведь самый простой способ найти ответ — совет опытного специалиста. Взаимопомощь и общение — традиция в мире Linux. Всегда можно обратиться за помощью к сообществу пользователей и разработчиков Linux. Большинство вопросов повторяются, поэтому для начала стоит поискать ответ на свой вопрос в документации, затем в сети Интернет. Если вы не нашли ответа в перечисленных источниках, не стесняйтесь, пишите на форум или в списки рассылки так, как писали бы своим друзьям, и вам обязательно помогут.

Глава 3. Что такое системы Альт

3.1. ALT Linux Team

Команда ALT Linux (http://www.altlinux.org/ALT_Linux_Team) — это интернациональное сообщество, насчитывающее более 200 разработчиков свободных программного обеспечения.

3.2. Сизиф

Sisyphus (https://packages.altlinux.org/ru/Sisyphus/home) — наш ежедневно обновляемый банк программ (часто называемый репозиторий). На его основе создаются все дистрибутивы ALT. Поддерживаемая ALT Linux Team целостность Sisyphus, оригинальная технология сборки программ, утилита **`apt-get`** и её графическая оболочка **synaptic** позволяют пользователям легко обновлять свои системы и быть в курсе актуальных новостей мира свободных программ.

Ежедневно изменяющийся репозиторий содержит самое новое программное обеспечение со всеми его преимуществами и недостатками (иногда ещё неизвестными). Поэтому, перед обновлением вашей системы из Sisyphus, мы советуем взвесить преимущества новых возможностей, реализованных в последних версиях программ, и вероятность возникновения неожиданностей в работе с ними (http://www.altlinux.org/Sisyphus_changes).

Разработка Sisyphus полностью доступна. У нас нет секретных изменений кода и закрытого тестирования с подписками о неразглашении. То, что мы сделали сегодня, завтра вы найдёте в сети. По сравнению с другими аналогичными банками программ (Debian unstable, Mandriva Cooker, PLD, Fedora), в Sisyphus есть немало самобытного. Особое внимание уделяется защите системы, локализации на русский язык, полноте и корректности зависимостей.

Название Sisyphus (Сизиф) заимствовано из греческой мифологии. С кропотливым Сизифом, непрерывно закатывающим в гору камни, команду ALT Linux Team объединяет постоянная работа над усовершенствованием технологий, заложенных в репозиторий.

Sisyphus, в первую очередь, — открытая лаборатория решений. Если вам это интересно, если вы хотите дополнить Sisyphus новыми решениями, если вы считаете, что можете собрать какую-то программу лучше — присоединяйтесь к проекту ALT Linux Team (http://www.altlinux.org/Join).

3.3. Что такое девятая платформа

Как уже говорилось ранее, Sisyphus является часто обновляемым репозиторием, скорее предназначенным для разработчиков. Решением для тех пользователей, которым стабильность и предсказуемость работы системы важнее расширенной функциональности (а это в первую очередь начинающие и корпоративные пользователи), являются стабильные дистрибутивы Альт. Такие стабильные дистрибутивы базируются на стабильном срезе репозитория Sisyphus. Эти срезы называются платформами.

Девятая платформа p9 (Vaccinium) была создана в августе 2019 года и её поддержка продлится до декабря 2023 года, но не ранее полугода после выпуска следующей платформы (p10). Сроки поддержки продуктов на основе девятой платформы могут быть иными.

Часть II. Установка дистрибутива

В этой части рассматривается процесс установки дистрибутива.

Содержание

Глава 4. Подготовка установочного диска

Наиболее частый способ установки операционной системы на компьютер представляет собой установку с установочного DVD-диска. В этой главе описываются различные способы записи дистрибутива на DVD-диск.

Установочные образы являются гибридными, что позволяет производить установку, записав такой образ на USB Flash. О записи установочного образа на USB Flash также рассказано в этой главе.

4.1. Запись ISO-образа дистрибутива на DVD

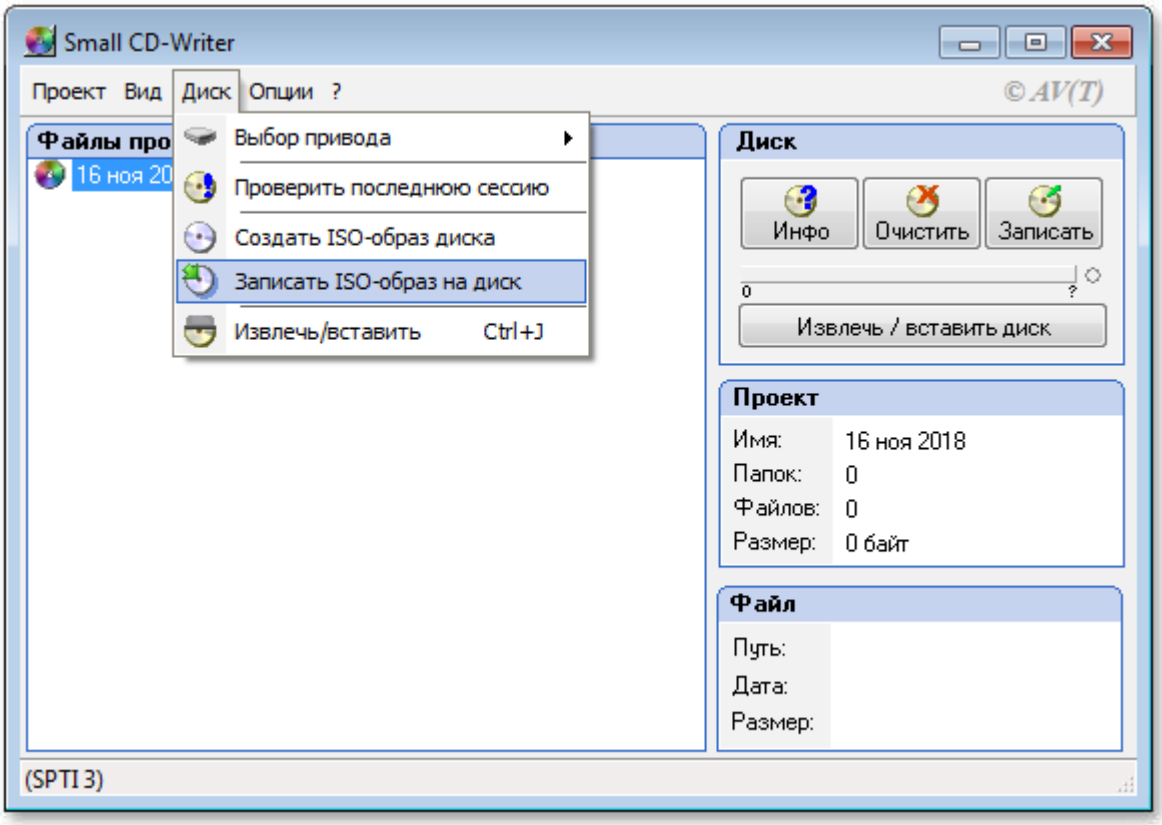
4.1.1. Запись образа диска под операционной системой MS Windows

Файл ISO-образа диска — это файл специального формата, подготовленный для записи на диск. Для записи ISO-образа под операционной системой MS Windows используйте специальные программы: SCDWriter, Nero BurningROM и другие. Рекомендуем для записи использовать новые диски от известных производителей, таких как: Verbatim, TDK. Записанный на плохой диск образ может вызвать неразрешимые проблемы при установке.

4.1.1.1. Запись образа диска с помощью Small CD-Writer

Весь процесс записи установочного диска при помощи **Small CD-Writer** состоит из следующих шагов:

- скачать образ дистрибутива;
- скачать архив программы Small CD-Writer http://gluek.info/wiki/_media/software/scdwriter14.zip;
- распаковать файлы программы из архива в любой каталог;
- вставить чистый диск в привод;
- войти в распакованный каталог и запустить программу **`SCDWriter.exe`**;
- открыть пункт меню **Диск → Записать ISO-образ на диск** и, в появившемся окне, указать путь к образу диска;
- нажать кнопку **Записать**.



4.1.1.2. Запись образа диска с помощью Nero BurningROM

Процесс записи установочного диска при помощи **Nero BurningROM** состоит из следующих шагов:

- скачать образ дистрибутива;
- скачать программу **Nero BurningROM** с сайта производителя http://www.nero.com и установить её;
- запустить программу и выбрать в списке устройств необходимый для записи CD/DVD дисковод;
- нажать кнопку **Открыть проект** в главном окне. В появившемся окне выбрать необходимый ISO-образ для записи и нажать кнопку **Открыть**;
- в окне **Запись проекта (Записать образ)** настроить необходимые параметры;
- записать ISO-образа на диск, щёлкнув по кнопке **Запись (Burn)**.

4.1.2. Запись образа диска под операционной системой Linux

Для записи ISO-образов можно использовать множество утилит и программ с графическим или текстовым интерфейсом. Наиболее удобно использовать программы **K3b** или **Brasero**, которые поставляются в комплекте любого дистрибутива операционной системы Linux.

4.1.2.1. Запись образа диска с помощью K3b

Весь процесс записи установочного диска при помощи **K3b** состоит из следующих шагов:

- если программа **k3b** отсутствует, необходимо установить её в систему, используя стандартные для вашего дистрибутива инструменты установки программ;
- запустить программу **k3b**. При правильных настройках программа сообщит об отсутствии проблем с системой и предложит перейти к записи на диск;
- в меню главного окна **Сервис (Service)** выбрать пункт **Записать образ DVD (Burn DVD image)**;
- в появившемся окне **`Записать образ DVD (Burn DVD image)`** нажать на кнопку **`Выбор файла для записи`**. Откроется диалог, в котором необходимо выбрать ISO-образ для записи и после выбора нажать кнопку **`OK`**;
- программа **k3b** покажет информацию о ISO-файле и начнёт вычислять контрольную сумму. Эта операция может занять несколько минут. Полученную контрольную сумму можно сравнить с MD5SUM суммой на странице дистрибутива;
- если контрольные суммы не совпадают, значит, для записи был выбран не тот файл или скачанный ISO-образ был испорчен во время передачи данных по сети;
- если контрольные суммы совпадают, вставить диск для записи в дисковод. Дождаться активации кнопки **`Начать (Start)`**;
- нажать на кнопку **`Начать (Start)`**.

4.2. Запись установочного образа на USB Flash

Предупреждение

Запись образа дистрибутива на flash-диск приведёт к изменению таблицы разделов на носителе, таким образом, если flash-диск выполнил функцию загрузочного\установочного устройства и требуется вернуть ему функцию переносного накопителя данных, то необходимо удалить все имеющиеся разделы на flash-диске и создать нужное их количество заново.

Для восстановления совместимости flash-диска с операционными системами семейства Windows может понадобиться также пересоздание таблицы разделов (например, при помощи parted). Нужно удалить таблицу GPT и создать таблицу типа msdos. Кроме того, должен быть только один раздел с FAT или NTFS.

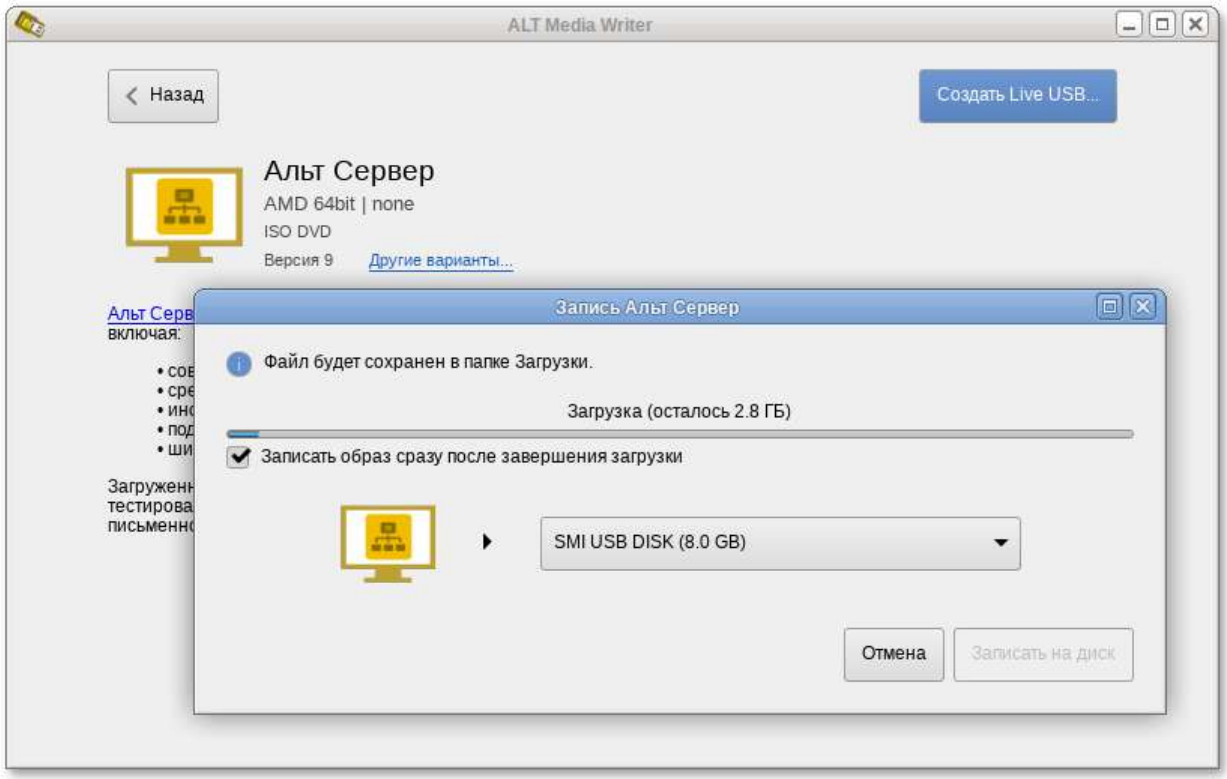
Для создания загрузочного flash-диска понадобится файл ISO-образа установочного диска с дистрибутивом. ISO-образы установочных дисков являются гибридными (Hybrid ISO/IMG), что позволяет записать их на flash-накопитель.

4.2.1. В операционной системе Windows

Для создания загрузочного flash-диска под операционной системой MS Windows используйте специальные программы: ALT Media Writer, Win32 Disk Imager, ROSA Image Writer и другие.

ALT Media Writer — это инструмент, который помогает записывать образы ALT на портативные накопители, такие как flash-диски. Он может автоматически загружать образы из интернета и записывать их. Для записи образа на flash-диск необходимо:

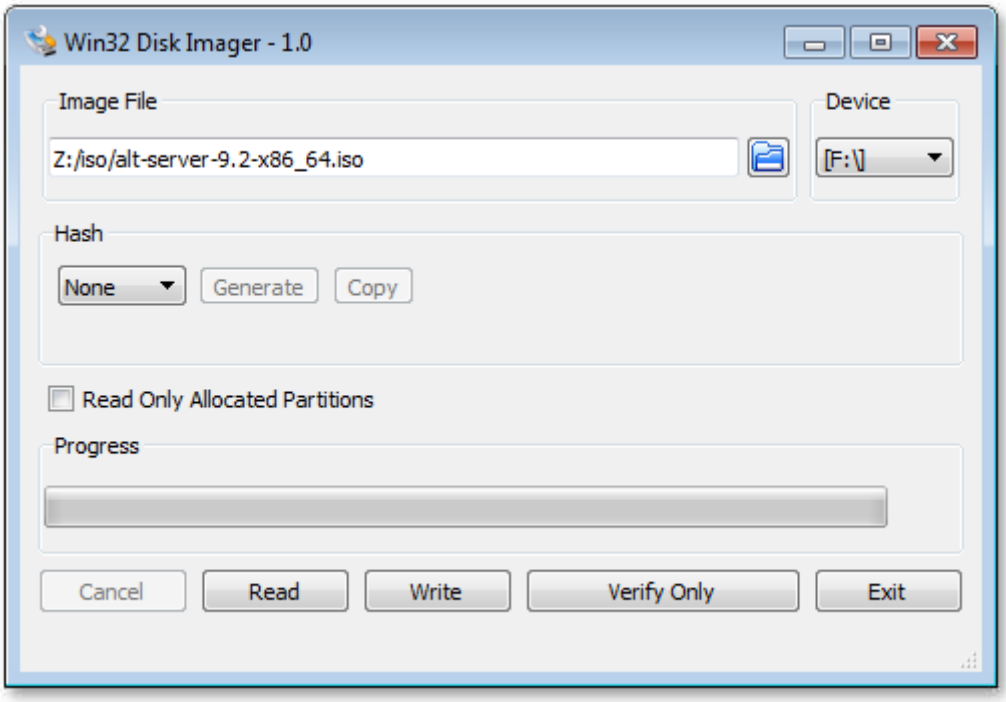
- скачать и установить **ALT Media Writer**;
- вставить flash-диск в USB-разъем;
- запустить **ALT Media Writer**;
- выбрать дистрибутив и нажать кнопку **Создать Live USB...**:



  начнётся загрузка образа из интернета;
- выбрать устройство (flash-диск);
- после окончания загрузки нажать кнопку **Записать на диск** (если был отмечен пункт **Записать образ после загрузки**, запись образа начнётся автоматически).

Инструкция для записи образа в программе **Win32 Disk Imager**:

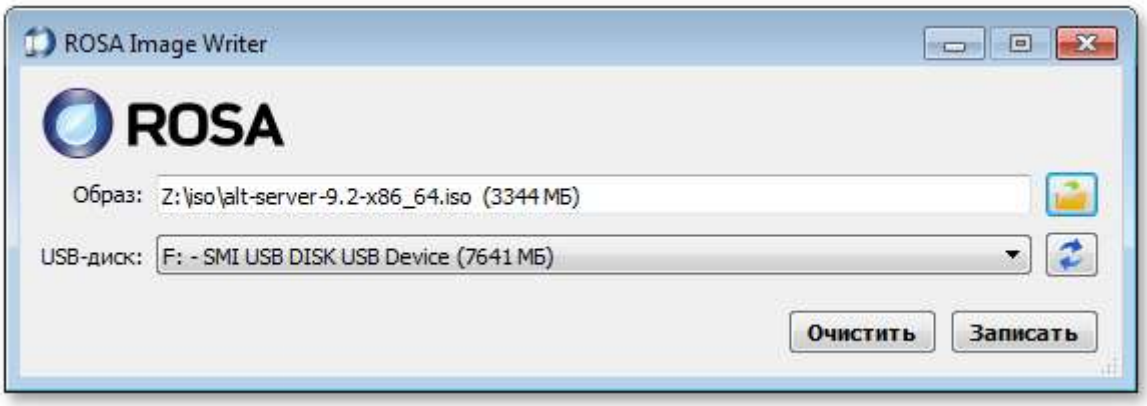
- скачать и установить программу Win32 Disk Imager;
- скачать образ дистрибутива;
- вставить flash-диск в USB-разъем (размер flash-диска должен быть не меньше размера скачанного образа диска);
- запустить **Win32 Disk Imager**;
- в появившимся окне выбрать ISO-образ дистрибутива, выбрать устройство (flash-диск):



- нажать кнопку **`Write`** для записи образа на flash-диск.

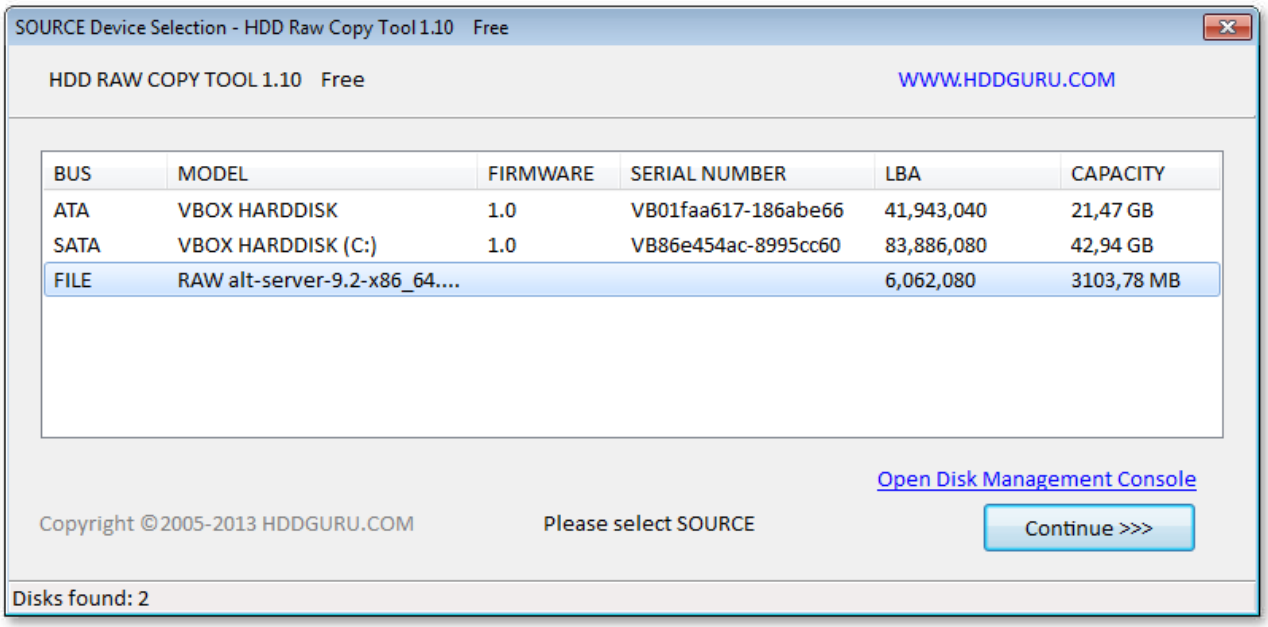
Инструкция для записи образа в программе **ROSA Image Writer**:

- скачать архив с программой ROSA Image Writer;
- распаковать файлы программы из архива в любой каталог;
- скачать образ дистрибутива;
- вставить flash-диск в USB-разъем (размер flash-диска должен быть не меньше размера скачанного образа диска);
- запустить файл **`.exe`**;
- в появившимся окне выбрать ISO-образ дистрибутива, выбрать устройство (flash-диск):

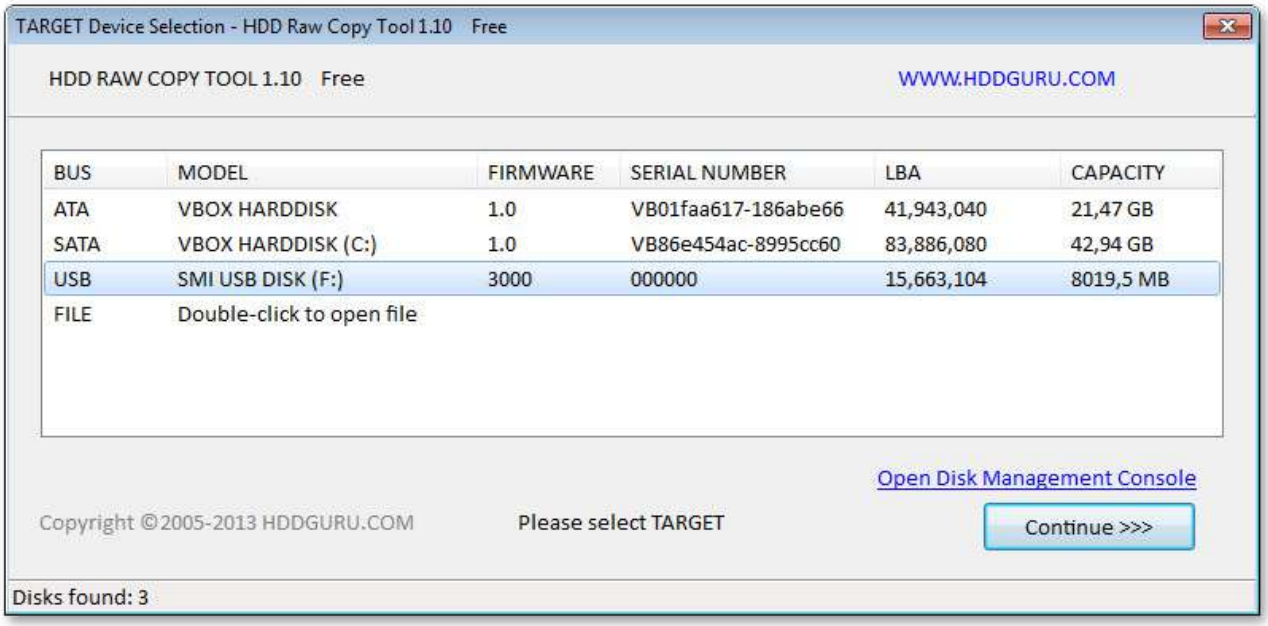


- нажать кнопку **Записать** для записи образа на flash-диск.

Для записи образа на flash-диск подойдёт и утилита HDD Raw Copy Tool. На первом шаге нужно выбрать файл с образом диска:



На втором шаге нужно выбрать flash-диск, на который будет записан образ:



Предупреждение

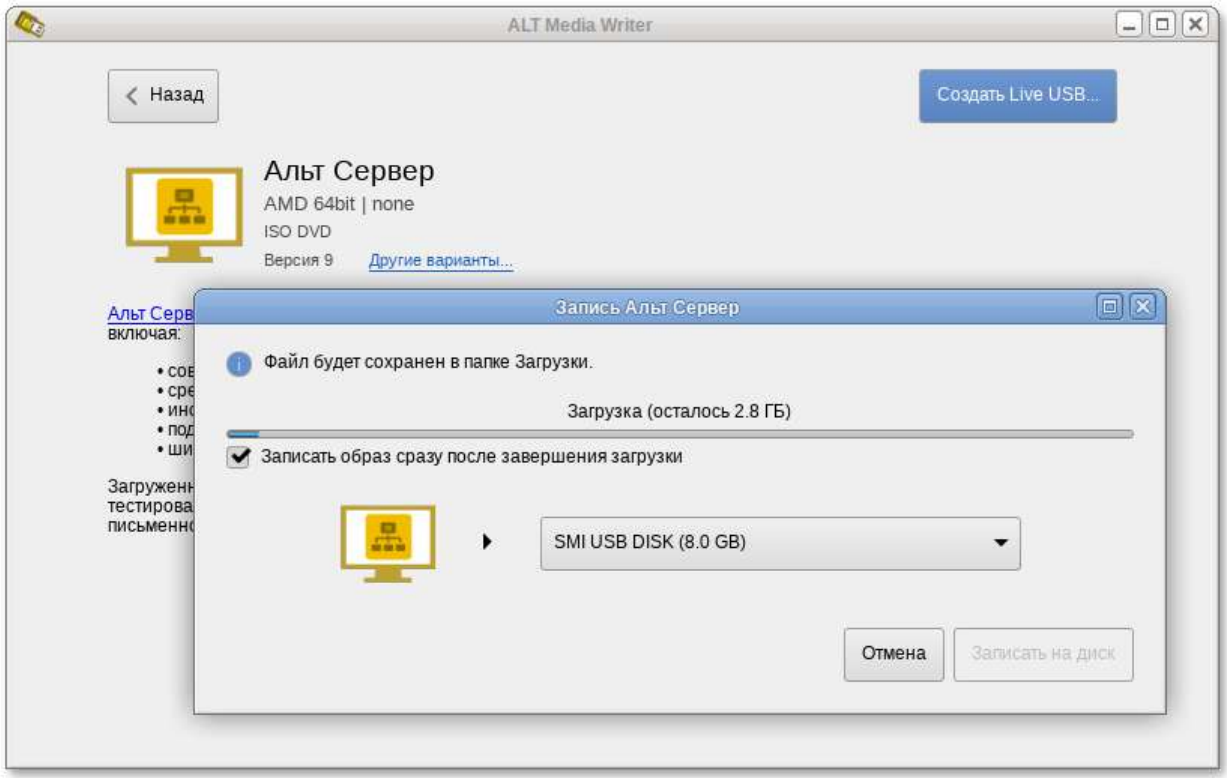
Будьте внимательны при указании имени usb-устройства — запись образа по ошибке на свой жёсткий диск приведёт к почти гарантированной потере данных на нём!

После проверки правильности выбранных параметров и нажатия кнопки **`Continue`** можно приступать к записи, нажав кнопку **START**. По успешному завершению записи окно с индикацией процесса записи закроется, после чего можно закрыть и окно самой программы.

4.2.2. В операционной системе Linux

Для записи образа на flash-диск можно воспользоваться любой из трёх программ с графическим интерфейсом:

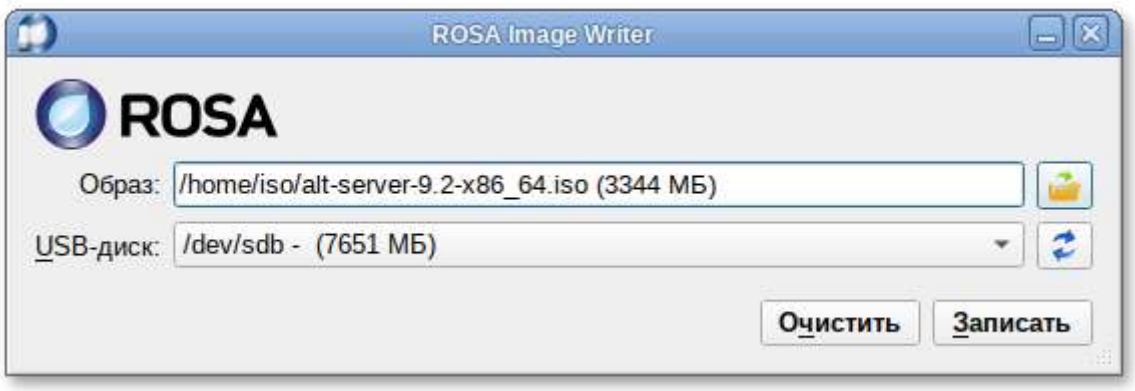
- ALT Media Writer (altmediawriter):



  ALT Media Writer может автоматически загружать образы из интернета и записывать их, при необходимости извлекая сжатые образы (img.xz).

- SUSE Studio Imagewriter (imagewriter):

- ROSA Image Writer (rosa-imagewriter):



Для записи установочного образа можно воспользоваться утилитой командной строки dd:

```
dd oflag=direct if=<файл-образа.iso> of=/dev/sdX bs=1M status=progress
sync
```

где <файл-образа.iso> — образ диска ISO, а **/dev/sdX** — устройство, соответствующее flash-диску.

Для удобства показа прогресса записи можно установить пакет pv и использовать команду:

```
pv <файл-образа.iso> | dd oflag=direct of=/dev/sdX bs=1M;sync
```

где <файл-образа.iso> — образ диска ISO, а **/dev/sdX** — устройство, соответствующее flash-диску.

Просмотреть список доступных устройств можно командой **lsblk** или (если такой команды нет): **blkid**.

Например, так можно определить имя flash-диска:

```
$ lsblk | grep disk
sda      8:0    0 931,5G  0 disk
sdb      8:16   0 931,5G  0 disk
sdc      8:32   1   7,4G  0 disk
```

flash-диск имеет имя устройства sdc.

Затем записать:

```
# dd oflag=direct if=/home/iso/alt-server-9.2-x86_64.iso of=/dev/sdc bs=1M
status=progress; sync
```

или, например, так:

```
# pv /home/iso/alt-server-9.2-x86_64.iso | dd oflag=direct of=/dev/sdc
bs=1M;sync
dd: warning: partial read (524288 bytes); suggest iflag=fullblock
3GiB 0:10:28 [4,61MiB/s] [=================================>  ] 72% ETA
0:04:07
```

Предупреждение

Будьте внимательны при указании имени usb-устройства — запись образа по ошибке на свой жёсткий диск приведёт к почти гарантированной потере данных на нём!

Предупреждение

Не добавляйте номер раздела, образ пишется на flash-диск с самого начала!

Предупреждение

Не извлекайте flash-диск, пока образ не запишется до конца! Определить финал процесса можно по прекращению моргания индикатора flash-диска либо посредством виджета "Безопасное извлечение съемных устройств". В консоли можно подать команду

```
eject /dev/sdX
```

и дождаться ее успешного завершения.

4.2.3. В операционной системе OS X

В операционной системе OS X для создания загрузочного flash-диска можно использовать команду:

```
sudo dd if=alt-server-9.2-x86_64.iso of=/dev/diskX bs=1M
sync
```

где **alt-server-9.2-x86_64.iso** — образ диска ISO, а /dev/diskX — flash-диск.

Просмотреть список доступных устройств можно командой:

```
diskutil list
```

Предупреждение

Будьте внимательны при указании имени usb-устройства — запись образа по ошибке на свой жёсткий диск приведёт к почти гарантированной потере данных на нём!

4.2.4. Проверка целостности записанного образа

Предупреждение

Внимание! Если речь идёт о записи на flash-диск образа LiveCD, проверка должна быть выполнена сразу же после записи на USB Flash, без запуска с него. Причина в том, что остаток flash-диска, при первом запуске LiveCD, форматируется, как r/w раздел, при этом меняется и таблица разделов.

Для проверки целостности записанного образа необходимо выполнить следующие шаги:

- определить длину образа в байтах:

  ```
  $  du -b alt-server-9.2-x86_64.iso | cut -f1
  3506438144
  ```

- посчитать контрольную сумму образа (или просмотреть контрольную сумму образа из файла MD5SUM на сервере FTP):

  ```
  $ md5sum alt-server-9.2-x86_64.iso
  cf0024eceae6d290be95672adc9290ef  alt-server-9.2-x86_64.iso
  ```

- подсчитать контрольную сумму записанного образа на DVD или USB Flash (выполняется под правами пользователя root):

  ```
  #  head -c 3506438144 /dev/sdd | md5sum
  cf0024eceae6d290be95672adc9290ef
  ```

  где размер после -c — вывод в п.1, а /dev/sdd — устройство DVD или USB Flash, на которое производилась запись.

Глава 5. Альтернативные способы установки

Обычно для установки дистрибутива используется установочный загрузочный CD/DVD-диск или USB flash-накопитель. Если вы производите установку именно таким образом, можете пропустить этот раздел и сразу перейти к разделу Последовательность установки.

Установка с загрузочного диска — это один из возможных способов установки системы. Он является самым распространённым способом установки системы, но не работает, например, в случае отсутствия на компьютере CD/DVD-привода. Для таких случаев поддерживаются альтернативные методы установки.

Необходимо понимать, что для начала процесса установки необходимо присутствие двух составляющих: возможности загрузить компьютер и доступа к установочным файлам. В случае загрузки с установочного диска эти две возможности предоставляются самим диском: он является загрузочным и содержит все необходимые для установки файлы. Однако, вполне допустим и такой вариант: первоначальная загрузка происходит со специально подготовленного USB flash-накопителя, а установочные файлы берутся с FTP-сервера сети.

Таким образом, для альтернативной установки дистрибутива необходимо:

- определиться со способом первоначальной загрузки компьютера;
- определиться с источником установки.

5.1. Источники установки

После первоначальной загрузки с одного из поддерживаемых носителей можно выбрать **Источник установки** — место, откуда программа установки будет брать все необходимые при установке данные (прежде всего устанавливаемое ПО). Так как установка системы возможна не только с лазерного диска, то можно выбрать один из поддерживаемых альтернативных источников установки. Для выбора источника установки необходимо в меню установки нажать кнопку **F4**:

Источники установки:

- Сетевые:
  - FTP-сервер;
  - HTTP-сервер;
  - NFS-сервер.
- Локальные:
  - DVD;
  - внешний жёсткий диск.

Условием для всех способов установки является доступность дерева файлов, аналогичного содержимому установочного диска.

5.1.1. Запуск сетевой установки

Кнопка **F4** позволяет выбрать источник сетевой установки: FTP, HTTP или NFS-сервер. Нужно указать имя или IP-адрес сервера и каталог (начиная с /), в котором размещён дистрибутив. В случае установки по протоколу FTP может понадобиться также ввести имя и пароль пользователя.

Пример установки:

- имя сервера: 192.168.0.1
- каталог: **/pub/netinstall/**. В данном каталоге на сервере должны находиться:
  - файл **altinst**;
  - каталог **Metadata**;
  - каталог **ALTLinux** с подкаталогами **RPMS.*секция***, содержащими rpm-пакеты.

Для получения подобного дерева каталогов на стороне сервера достаточно скопировать содержимое установочного лазерного диска в один из подкаталогов FTP-сервера (либо HTTP или NFS-сервера). В описанном примере это каталог **/pub/netinstall**.

При сетевой установке со стороны клиента (компьютера, на который производится установка) может понадобиться определить параметры соединения с сервером. В этом случае на экране будут появляться диалоги, например, с предложением выбрать сетевую карту (если их несколько) или указать тип IP-адреса: статический (потребуется вписать его самостоятельно) или динамический (DHCP).

После успешного соединения с сервером в память компьютера будет загружен образ установочного диска. После этого начнётся установка системы подобно установке с лазерного диска.

5.1.2. Установка с жёсткого диска

Установка Альт Сервер с жёсткого диска происходит аналогично установке по сети. Для этого понадобится подключить дополнительный жёсткий диск с дистрибутивом. Чтобы выбрать подключённый диск в качестве источника установки, нужно кнопкой **F4** выбрать источник установки **Жёсткий диск**. Затем выбрать пункт **Установка** в загрузочном меню. По нажатию **Enter** на экране появится диалог выбора дискового раздела, а после — диалог выбора пути к каталогу с дистрибутивом. После указания пути начнётся установка системы. Можно сразу указать путь к дистрибутиву, сделав в строке параметров загрузки запись вида:

```
automatic=method:disk,disk:hdb,partition:hdbX,directory:<путь_к_каталогу_с_дистрибутивом>
```

В данной команде «путь_к_каталогу_с_дистрибутивом» — полный путь к образу дистрибутива, например, **/home/test/alt-server.iso**, или путь к каталогу с содержимым образа дистрибутива (распакованный образ диска), например, **/home/test/alt-server-dir**.

Глава 6. Сохранение данных и меры предосторожности

Если необходимо установить ОС Альт Сервер и при этом сохранить уже установленную на компьютере операционную систему (например, другую версию GNU/Linux или Microsoft Windows), то нужно обязательно позаботиться о подготовке компьютера к установке второй системы и о сохранении ценных для вас данных.

Если у вас нет загрузочного диска для уже установленной системы, создайте его. В случае прерванной установки ОС Альт Сервер или неправильной настройки загрузчика, вы можете потерять возможность загрузиться в вашу предыдущую ОС.

Если на диске, выбранном для установки ОС Альт Сервер, не осталось свободного раздела, то программа установки должна будет изменить размер существующего раздела. От этой операции могут пострадать ваши данные, поэтому предварительно надо сделать следующие действия.

- Выполнить проверку раздела, который вы собираетесь уменьшать. Для этого воспользуйтесь соответствующим программным обеспечением (далее — ПО), входящим в состав уже установленной ОС. Программа установки Альт Сервер может обнаружить некоторые очевидные ошибки при изменении размера раздела, но специализированное ПО предустановленной ОС справится с этой задачей лучше.
- Выполнить дефрагментацию уменьшаемого раздела в целях повышения уровня безопасности данных. Это действие не является обязательным, но мы настоятельно рекомендуем его произвести: изменение размера раздела пройдёт легче и быстрее.

Предупреждение

Полной гарантией от проблем, связанных с потерей данных, является резервное копирование!

Глава 7. Начало установки: загрузка системы

7.1. Способы первоначальной загрузки

Для загрузки компьютера с целью установки системы необходимо воспользоваться носителем, содержащим начальный загрузчик.

Простейший способ запустить программу установки — загрузить компьютер с помощью загрузочного носителя, находящегося на установочном DVD с дистрибутивом (при условии, что система поддерживает загрузку с устройства для чтения DVD).

Также программу установки можно запустить с другого загрузочного носителя. Например, в качестве загрузочного носителя может использоваться загрузочный USB-flash-накопитель.

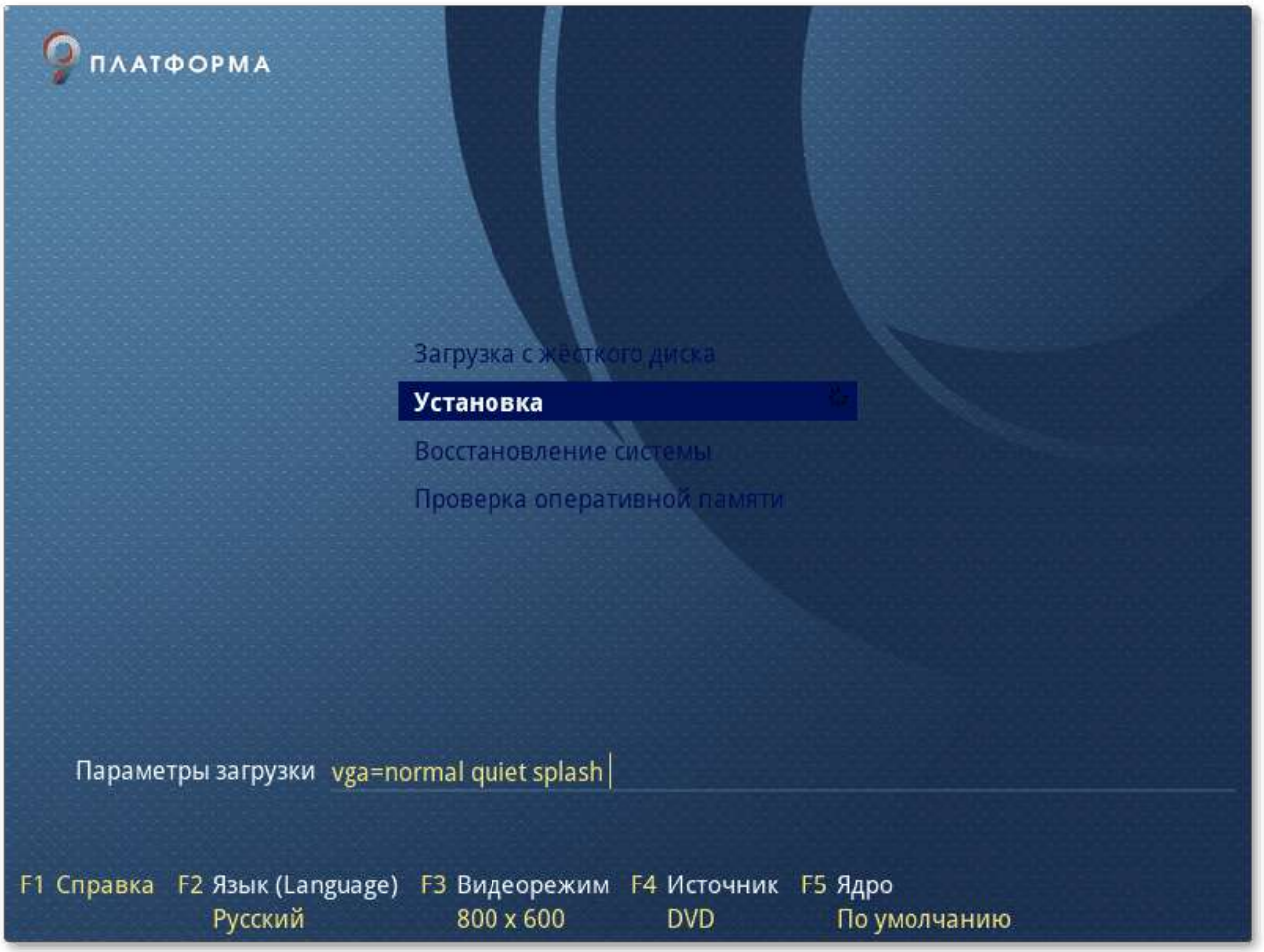
7.2. Загрузка системы

Для того чтобы начать установку ОС Альт Сервер, достаточно загрузиться с носителя, на котором записан дистрибутив.

Примечание

Предварительно следует включить в BIOS опцию загрузки с оптического привода или с USB-устройства.

В большинстве случаев указание способа входа в BIOS отображается на вашем мониторе непосредственно после включения компьютера. Способ входа в меню BIOS и информация о расположении настроек определяется производителем используемого оборудования. За информацией можно обратиться к документации на ваше оборудование.



Загрузка с установочного диска или специально подготовленного USB-flash-накопителя начинается с меню, в котором перечислено несколько вариантов загрузки:

- **Загрузка с жесткого диска** — запуск уже установленной на жестком диске операционной системы;
- **Установка** — установка операционной системы;

- **Восстановление системы** — восстановление уже установленной, но так или иначе поврежденной ОС Linux путем запуска небольшого образа ОС в оперативной памяти. Восстановление системы потребует некоторой квалификации. Этот пункт также может быть использован для сбора информации об оборудовании компьютера, которую можно отправить разработчикам, если ОС Альт Сервер устанавливается и работает неправильно. Загрузка восстановительного режима заканчивается приглашением командной строки:

```
[root@localhost /]#;
```

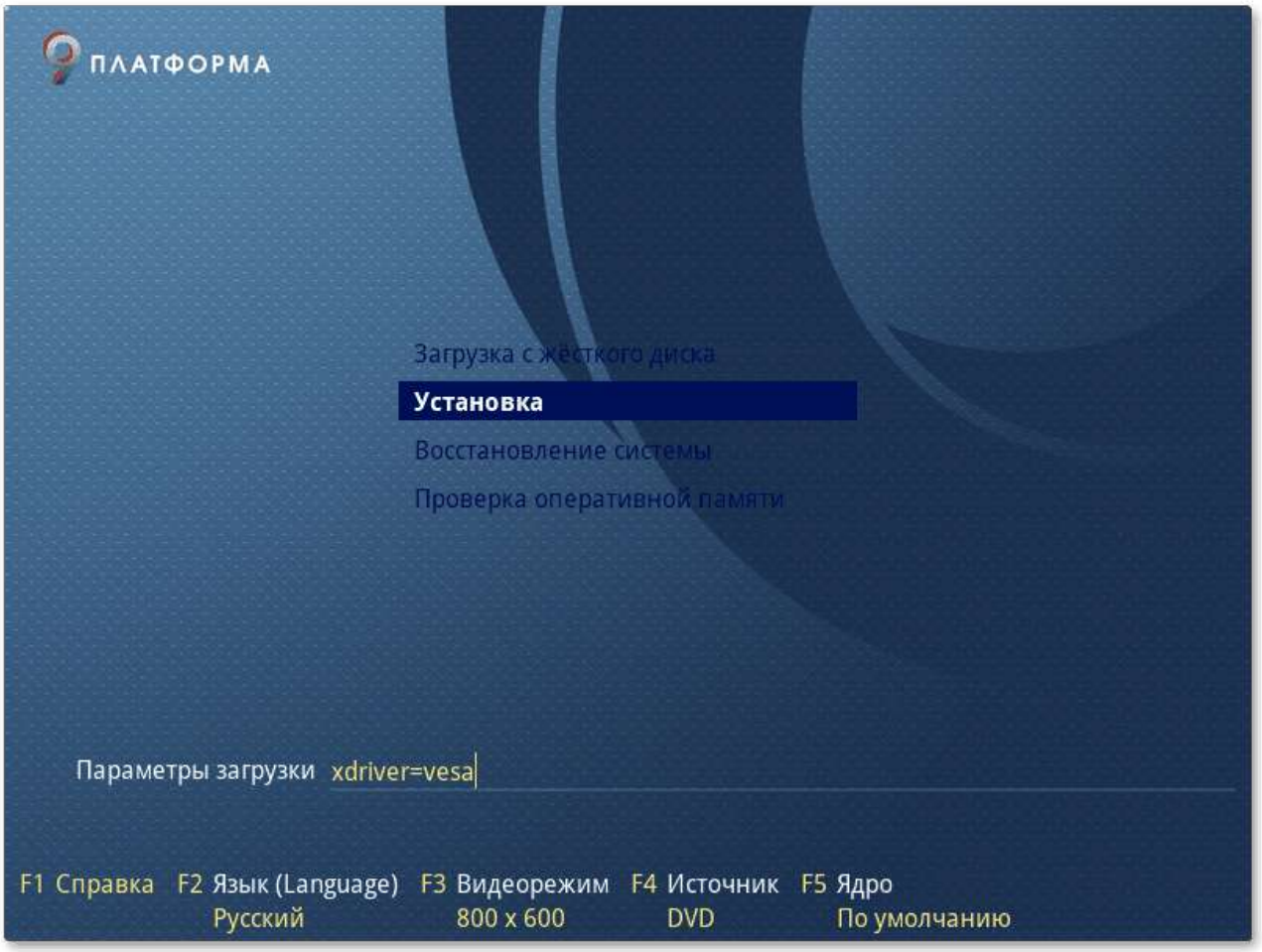
- **Проверка оперативной памяти** — проверка целостности оперативной памяти. Процесс диагностики заключается в проведении нескольких этапов тестирования каждого отдельного модуля ОЗУ (данный процесс будет выполняться бесконечно, пока его не остановят, необходимо дождаться окончания хотя бы одного цикла проверки).

Примечание

Мышь на этом этапе установки не поддерживается. Для выбора опций установки и различных вариантов необходимо использовать клавиатуру.

В строке **Параметры загрузки**, меню начального загрузчика, можно вручную задать параметры, передаваемые ядру. Например,

- ***nomodeset*** — не использовать modeset-драйверы для видеокарты;
- ***vga=normal*** — отключить графический экран загрузки установщика;
- ***xdriver=vesa*** — явно использовать видеодрайвер vesa. Данным параметром можно явно указать нужный вариант драйвера;
- ***acpi=off noapic*** — отключение ACPI (управление питанием), если система не поддерживает ACPI полностью.



В нижней части экрана отображаются дополнительные опции, влияющие на дальнейший ход установки:

- Можно получить справку по любому пункту меню, выбрав этот пункт и нажав клавишу **F1**.
- Нажатием клавиши **F2** осуществляется выбор языка. От выбора языка в загрузчике зависит язык интерфейса загрузчика и программы установки.
- По нажатию клавиши **F3** открывается меню доступных видеорежимов (разрешений экрана). Это разрешение будет использоваться во время установки и загрузки установленной системы.
- Выбрать источник установки можно, нажав клавишу **F4** (подробнее рассказано в разделе Источники установки).
- Нажатие клавиши **F5** выполняет переход к списку модулей для определения состава системных служб и сервисов, с которыми ядро ОС Альт Сервер будет установлено на загрузочный носитель.

Сочетание клавиш **Ctrl**+**Alt**+**F1** — выдает технические сведения о выполнении процесса установки ОС Альт Сервер.

Чтобы начать процесс установки, нужно клавишами перемещения курсора **вверх** и **вниз**, выбрать пункт меню **Установка**, и нажать **Enter**. Начальный этап установки не требует вмешательства пользователя: происходит автоматическое определение оборудования и запуск компонентов программы установки. Сообщения о происходящем на данном этапе можно просмотреть, нажав клавишу **ESC**.

Примечание

В начальном загрузчике установлено небольшое время ожидания: если в этот момент не предпринимать никаких действий, то будет загружена та система, которая уже установлена на жестком диске. Если вы пропустили нужный момент, перезагрузите компьютер и вовремя выберите пункт **Установка**.

Глава 8. Последовательность установки

До того, как будет произведена установка базовой системы на жёсткий диск, программа установки работает с образом системы, загруженным в оперативную память компьютера.

Если инициализация оборудования завершилась успешно, будет запущен графический интерфейс программы-установщика. Процесс установки разделён на шаги. Каждый шаг посвящён настройке или установке определённого свойства системы. Шаги нужно проходить последовательно. Переход к следующему шагу происходит по нажатию кнопки **Далее**. При помощи кнопки **Назад**, при необходимости, можно вернуться к уже пройденному шагу и изменить настройки. Однако возможность перехода к предыдущему шагу ограничена теми шагами, в которых нет зависимости от данных, введённых ранее.

Если по каким-то причинам возникла необходимость прекратить установку, необходимо нажать кнопку <Reset> на корпусе системного блока компьютера.

Примечание

Совершенно безопасно выполнить отмену установки только до шага «Подготовка диска», поскольку до этого момента не производится никаких изменений на жёстком диске. Если прервать установку между шагами «Подготовка диска» и «Установка загрузчика», существует вероятность, что после этого с жёсткого диска не сможет загрузиться ни одна из установленных систем (если такие имеются).

Технические сведения о ходе установки можно посмотреть, нажав **Ctrl**+**Alt**+**F1**, вернуться к программе установки — **Ctrl**+**Alt**+**F7**. По нажатию **Ctrl**+**Alt**+**F2** откроется отладочная виртуальная консоль.

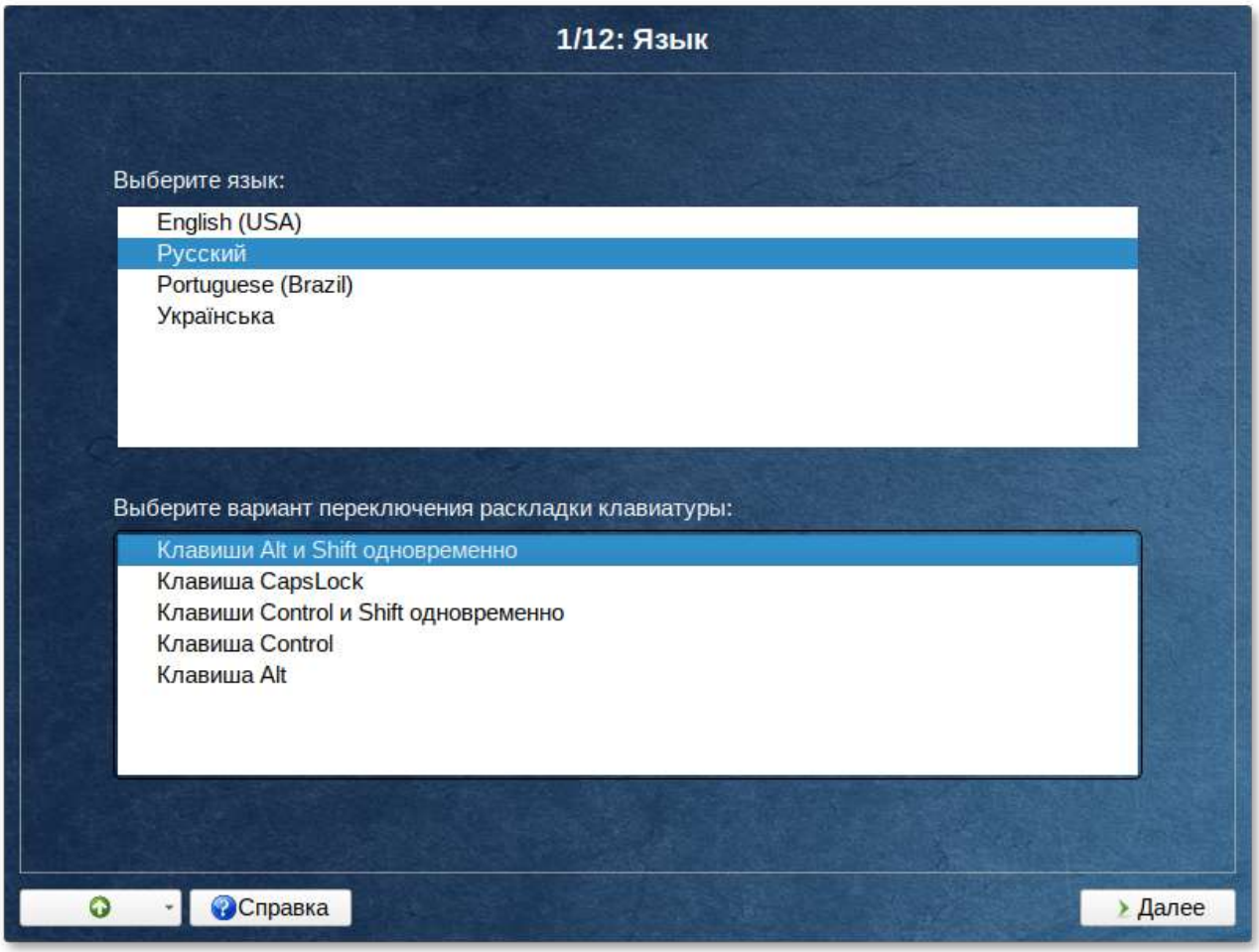
Каждый шаг сопровождается краткой справкой, которую можно вызвать, щёлкнув кнопку **Справка** или нажав клавишу **F1**.

Во время установки системы выполняются следующие шаги:

- Язык;
- Лицензионный договор;
- Дата и время;
- Подготовка диска;
- Установка системы;
- Сохранение настроек;

- Установка загрузчика;
- Настройка сети;
- Администратор системы;
- Системный пользователь;
- Установка пароля на шифрованные разделы;
- Завершение установки.

Глава 9. Язык



Установка Альт Сервер начинается с выбора основного языка — языка интерфейса программы установки и устанавливаемой системы. В списке, помимо доступных языков региона (выбранного на этапе начальной загрузки), указан и английский язык.

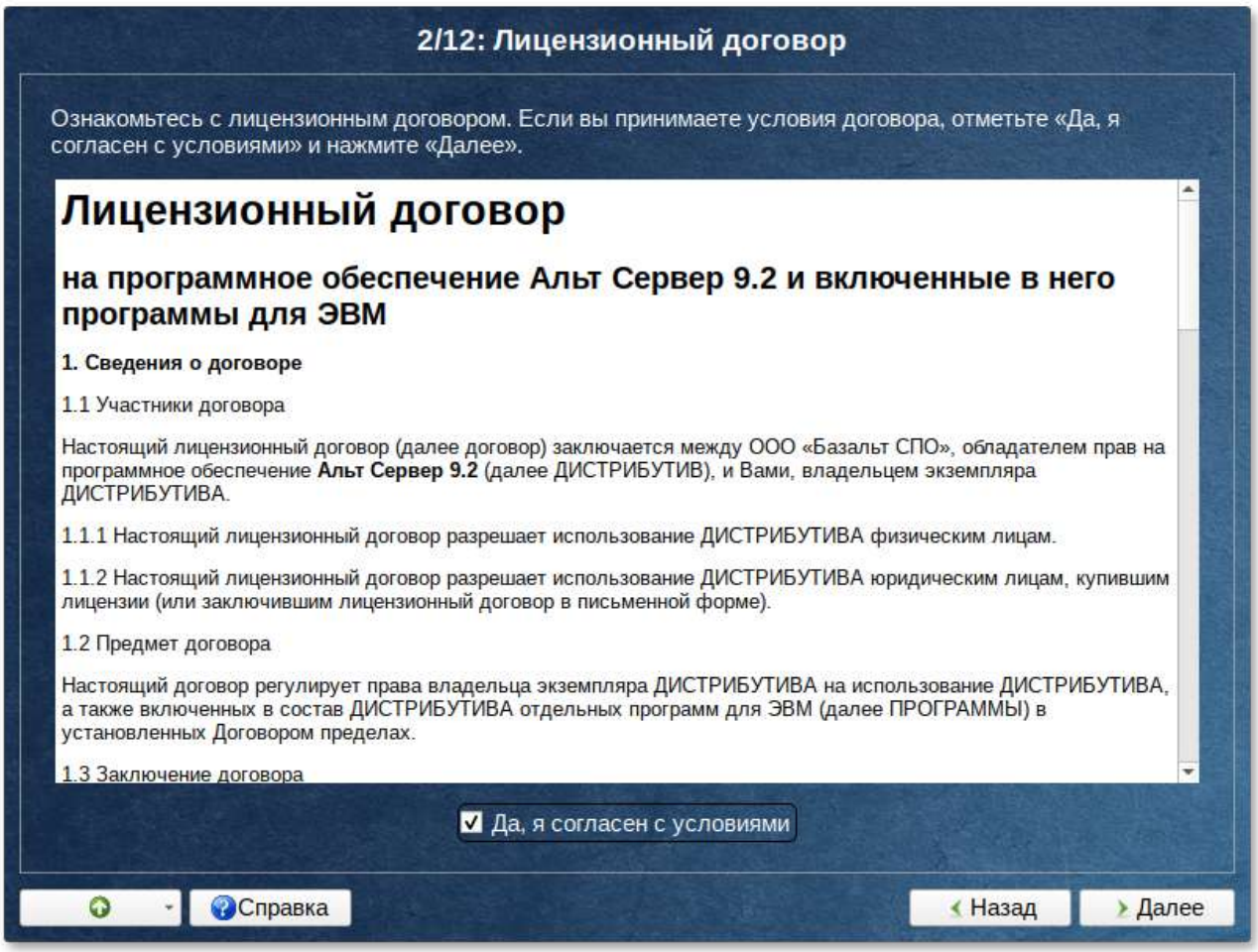
На этом же этапе выбирается вариант переключения раскладки клавиатуры. Раскладка клавиатуры — это привязка букв, цифр и специальных символов к клавишам на клавиатуре. Помимо ввода символов на основном языке, в любой системе Linux необходимо иметь возможность вводить латинские символы (имена команд, файлов и т.п.). Для этого обычно используется стандартная английская раскладка клавиатуры. Переключение между раскладками осуществляется при помощи специально зарезервированных для этого клавиш. Для русского языка доступны следующие варианты переключения раскладки:

- клавиши **`Alt`** и **`Shift`** одновременно;

- клавиша **CapsLock**;
- клавиши **Control** и **Shift** одновременно;
- клавиша **Control**;
- клавиша **Alt**.

Если выбранный основной язык имеет всего одну раскладку (например, при выборе английского языка в качестве основного), эта единственная раскладка будет принята автоматически.

Глава 10. Лицензионный договор



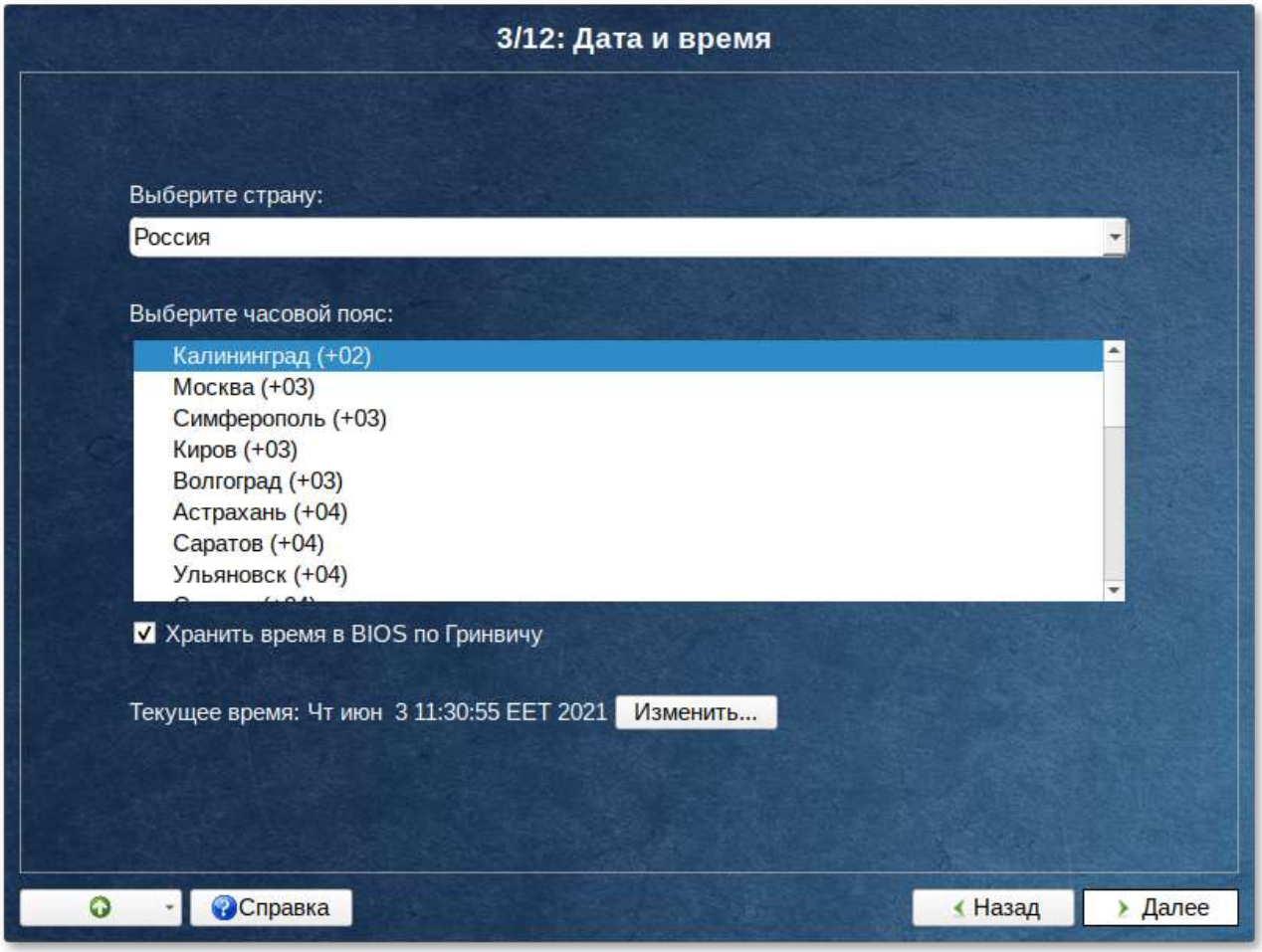
Перед продолжением установки следует внимательно прочитать условия лицензии. В лицензии говорится о ваших правах. В частности, за вами закрепляются права на:

- эксплуатацию программ на любом количестве компьютеров и в любых целях;
- распространение программ (сопровождая их копией авторского договора);
- получение исходных текстов программ.

Если вы приобрели дистрибутив, то данное лицензионное соглашение прилагается в печатном виде к вашей копии дистрибутива. Лицензия относится ко всему дистрибутиву Альт Сервер. Если вы согласны с условиями лицензии, отметьте пункт **Да, я согласен с условиями** и нажмите кнопку **Далее**.

Глава 11. Дата и время

На данном этапе выполняется выбор страны и города, по которым будет определен часовой пояс и установлены системные часы.



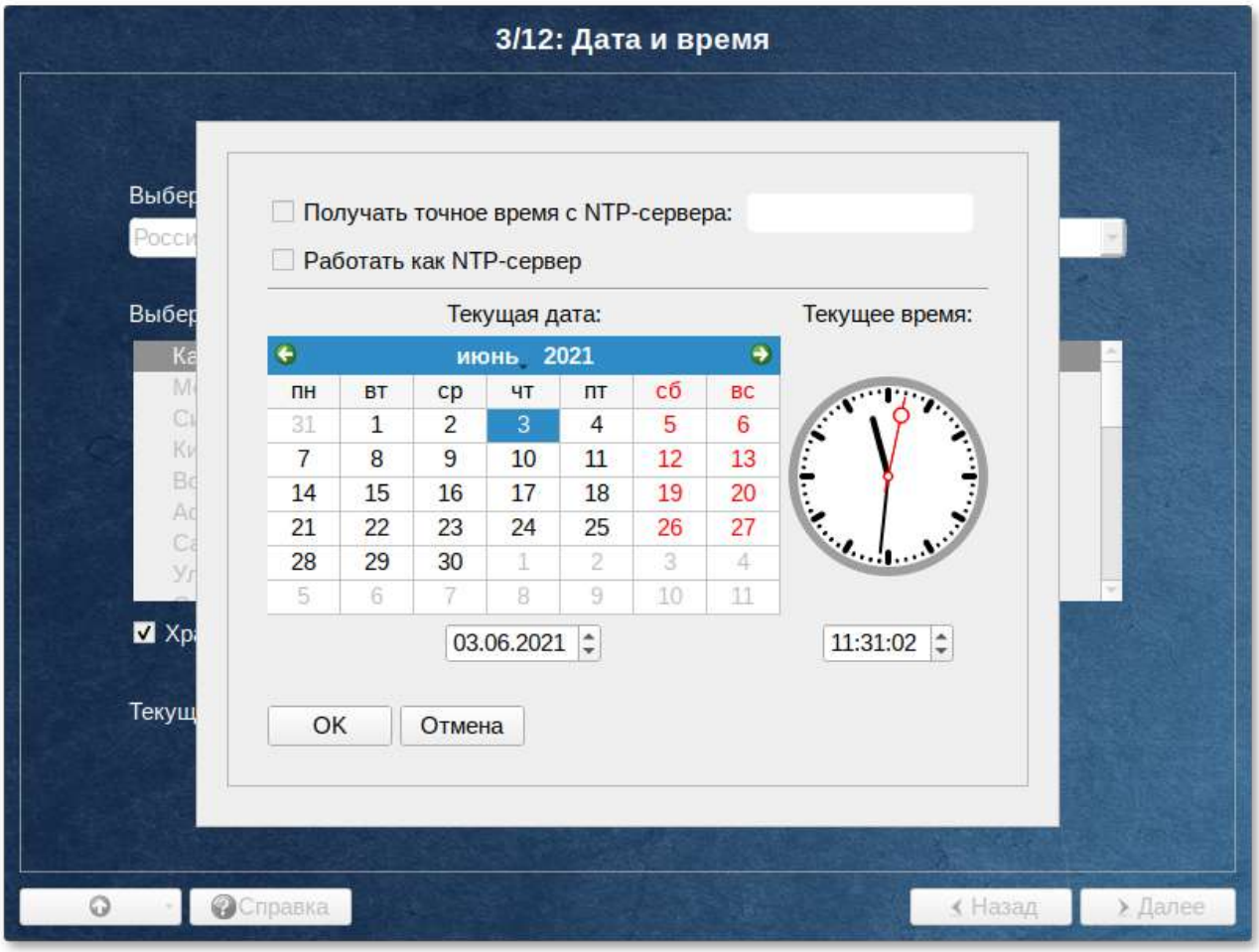
Для корректной установки даты и времени достаточно правильно указать часовой пояс и выставить желаемые значения для даты и времени.

На этом шаге следует выбрать часовой пояс, по которому нужно установить часы. Для этого в соответствующих списках выберите страну, а затем регион. Поиск по списку можно ускорить, набирая на клавиатуре первые буквы искомого слова.

Пункт **Хранить время в BIOS по Гринвичу** выставляет настройки даты и времени в соответствии с часовыми поясами, установленными по Гринвичу, и добавляет к местному времени часовую поправку для выбранного региона.

После выбора часового пояса будут предложены системные дата и время по умолчанию.

Для ручной установки текущих даты и времени нужно нажать кнопку **Изменить...**. Откроется окно ручной настройки системных параметров даты и времени.



Для сохранения настроек и продолжения установки системы в окне ручной установки даты и времени необходимо нажать кнопку **OK** и затем в окне **Дата и время** нажать кнопку **Далее**.

Примечание

В случае если ОС Альт Сервер устанавливается как вторая ОС, необходимо снять отметку с пункта **Хранить время в BIOS по Гринвичу**, иначе время в уже установленной ОС может отображаться некорректно.

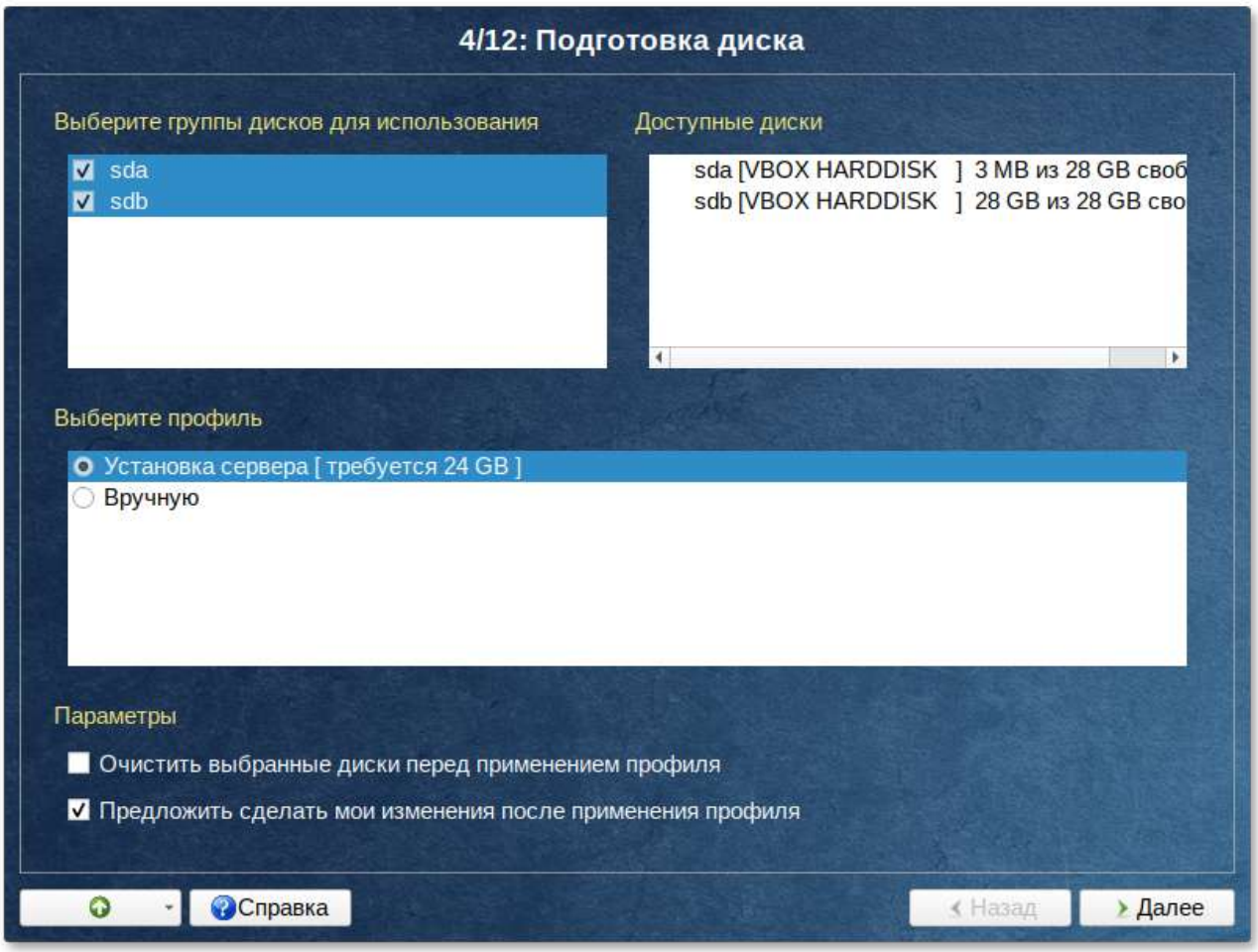
Глава 12. Подготовка диска

На этом этапе подготавливается площадка для установки Альт Сервер, в первую очередь — выделяется свободное место на диске.

Переход к этому шагу может занять некоторое время. Время ожидания зависит от производительности компьютера, объёма жёсткого диска, количества разделов на нём и других параметров.

12.1. Выбор профиля разбиения диска

После завершения первичной конфигурации загрузочного носителя откроется окно **Подготовка диска**. В списке разделов перечислены уже существующие на жёстких дисках разделы (в том числе здесь могут оказаться съёмные flash-диски, подключённые к компьютеру в момент установки).

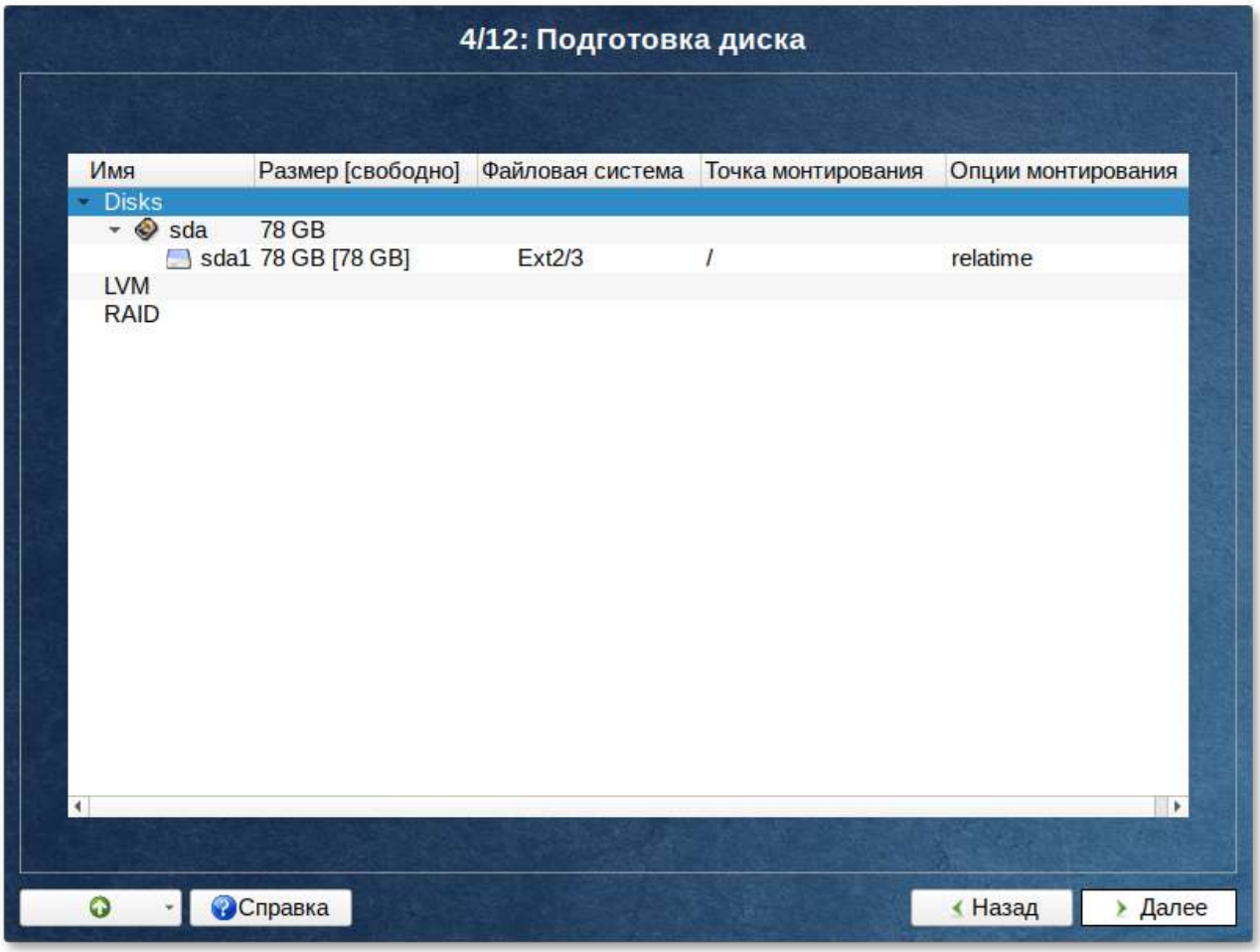


В списке **Выберите профиль** перечислены доступные профили разбиения диска. Профиль — это шаблон распределения места на диске для установки ОС. Можно выбрать один из профилей:

- установка сервера;
- вручную.

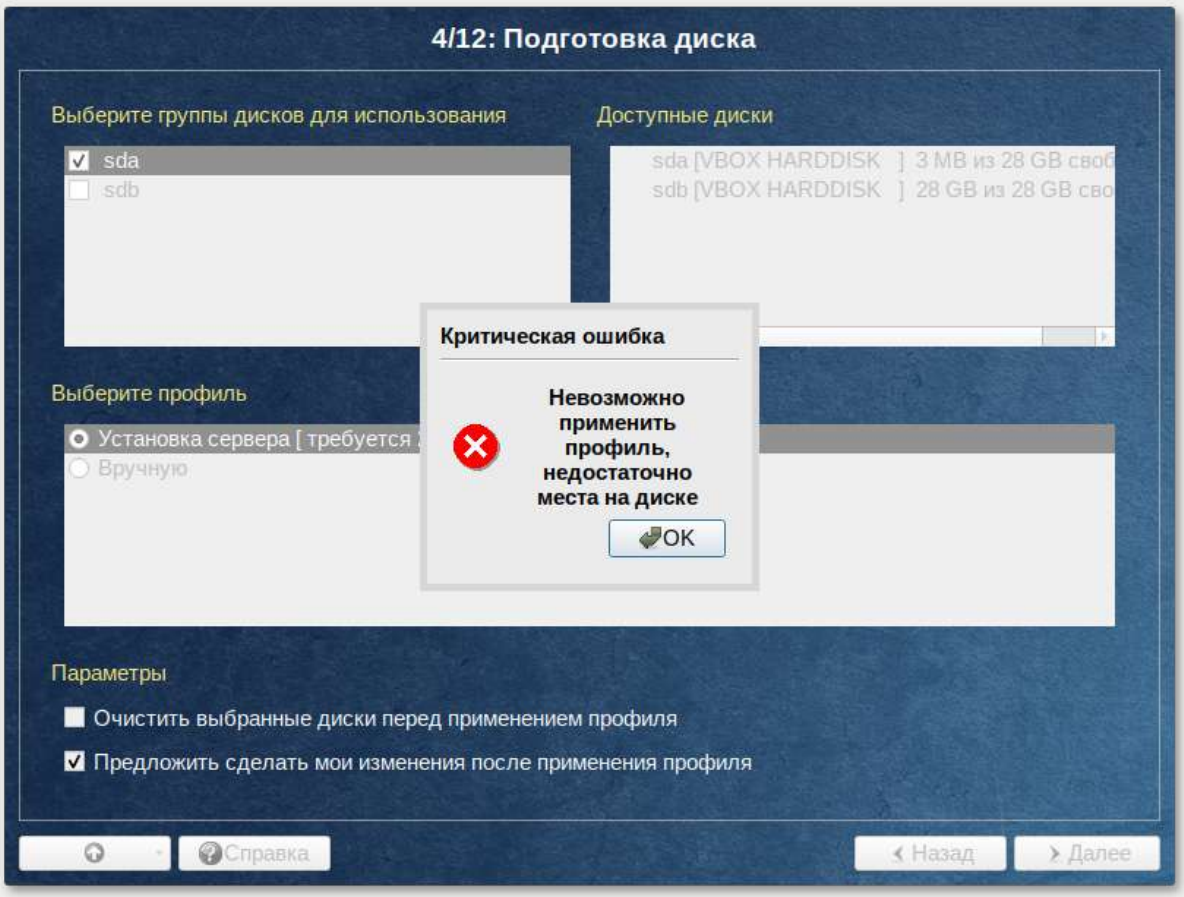
12.2. Автоматический профиль разбиения диска

Первый профиль предполагает автоматическое разбиение диска.


4/12: Подготовка диска
Имя
Размер [свободно]
Файловая система
Точка монтирования
Опции монтирования
Disks
sda
78 GB
sda1
78 GB [78 GB]
Ext2/3
/
relatime
LVM
RAID
Справка
Назад
Далее

Примечание

Если при применении профиля автоматического разбиения диска доступного места на диске окажется недостаточно, то на монитор будет выведено сообщение об ошибке: **Невозможно создать все разделы, недостаточно места на диске**.



Для решения этой проблемы можно полностью очистить место на диске, отметив пункт **Очистить все диски перед применением профиля** и применить профиль повторно.

Если сообщение о недостатке места на диске появляется и при отмеченном пункте **Очистить все диски перед применением профиля**, то это связано с недостаточным для использования автоматических методов разметки объёмом всего диска. В этом случае вы можете воспользоваться методом ручной разметки: профиль **Вручную**.

Предупреждение

При отмеченном пункте **Очистить все диски перед применением профиля** будут удалены все данные со всех дисков (включая внешние USB-носители) без возможности восстановления. Рекомендуется использовать эту возможность при полной уверенности в том, что диски не содержат никаких ценных данных.

12.3. Ручной профиль разбиения диска

При необходимости освободить часть дискового пространства следует воспользоваться профилем разбиения **Вручную**. В этом случае можно удалить некоторые из существующих разделов или содержащиеся в них файловые системы. После этого можно создать необходимые разделы самостоятельно или вернуться к шагу выбора профиля и применить автоматический профиль. Выбор этой возможности требует знаний об устройстве диска и технологиях его разметки.

По нажатию кнопки **Далее** будет произведена запись новой таблицы разделов на диск и форматирование разделов. Только что созданные на диске программой установки разделы пока не содержат данных и поэтому форматируются без предупреждения. Уже существовавшие, но изменённые разделы, которые будут отформатированы, помечаются специальным значком в колонке **Файловая система** слева от названия. При уверенности в том, что подготовка диска завершена, подтвердите переход к следующему шагу нажатием кнопки **Далее**.

Не следует форматировать разделы с теми данными, которые вы хотите сохранить, например, со старыми пользовательскими данными (**/home**) или с другими операционными системами. С другой стороны, отформатировать можно любой раздел, который вы хотите «очистить» (удалить все данные).

Предупреждение

Не уменьшайте NTFS-раздел с установленной Microsoft Windows Vista/Windows 7 средствами программы установки. В противном случае вы не сможете загрузить Microsoft Windows Vista/Windows 7 после установки Альт Сервер. Для выделения места под установку Альт Сервер воспользуйтесь средствами, предоставляемыми самой Microsoft Windows Vista/Windows 7: **Управление дисками → Сжать**.

12.4. Дополнительные возможности разбиения диска

Ручной профиль разбиения диска позволяет установить ОС на программный RAID-массив, разместить разделы в томах LVM и использовать шифрование на разделах. Данные возможности требуют от пользователя понимания принципов функционирования указанных технологий.

12.4.1. Создание программного RAID-массива

Избыточный массив независимых дисков RAID (redundant array of independent disks) — технология виртуализации данных, которая объединяет несколько НЖМД в логический элемент для избыточности и повышения производительности.

Примечание

Для создания программного RAID-массива потребуется минимум два жёстких диска.

Программа установки поддерживает создание программных RAID-массивов следующих типов:

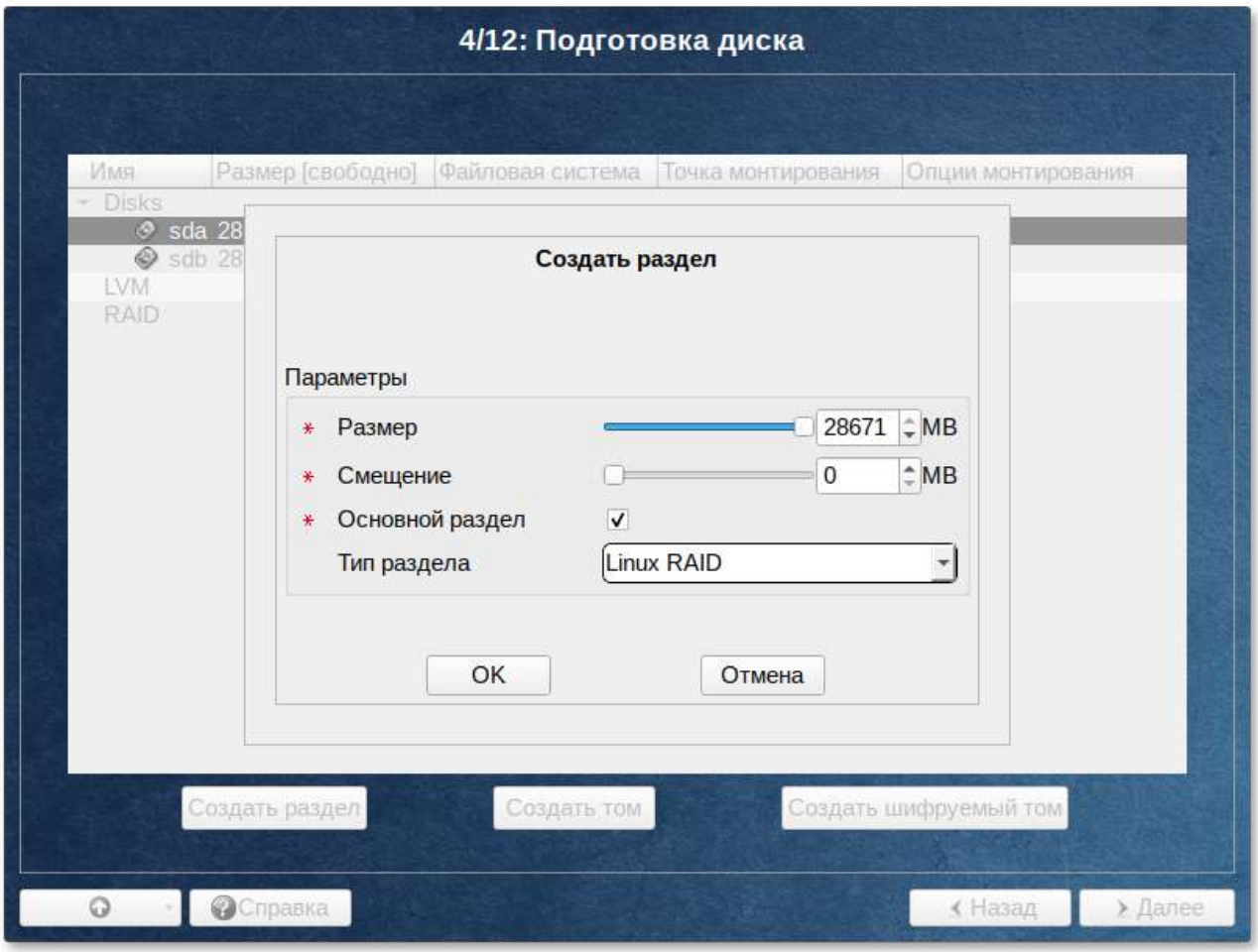
- RAID 1;

- RAID 0;
- RAID 4/5/6;
- RAID 10.

Процесс подготовки к установке на RAID условно можно разбить на следующие шаги:

- создание разделов на жёстких дисках;
- создание RAID-массивов на разделах жёсткого диска;
- создание файловых систем на RAID-массиве.

Для настройки параметров нового раздела из состава RAID-массива необходимо выбрать неразмеченный диск в окне профиля разбивки пространства **Подготовить разделы вручную** и нажать кнопку **Создать раздел**.



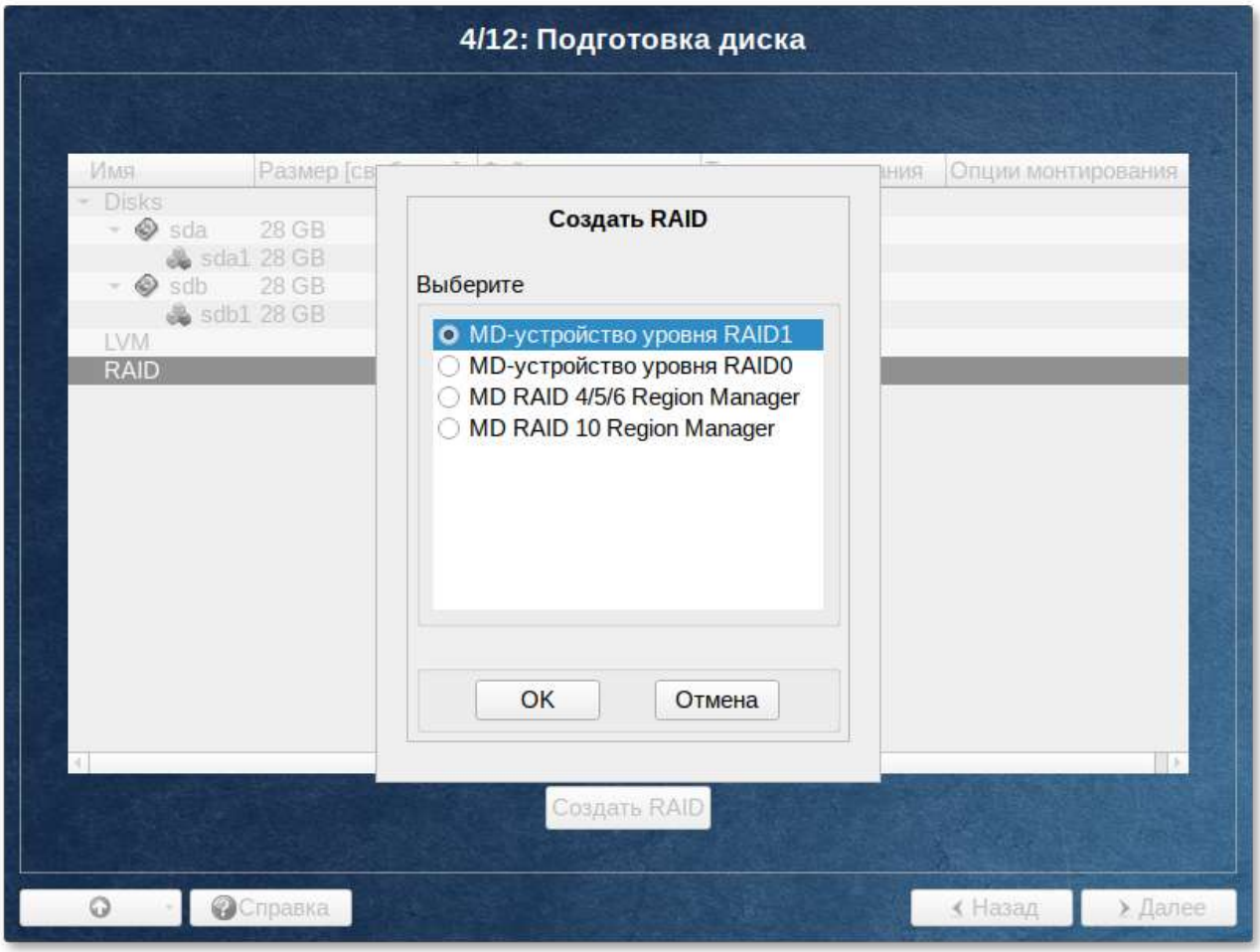
При создании разделов на жёстких дисках для последующего включения их в RAID-массивы следует указать **Тип раздела** для них равным **Linux RAID**.

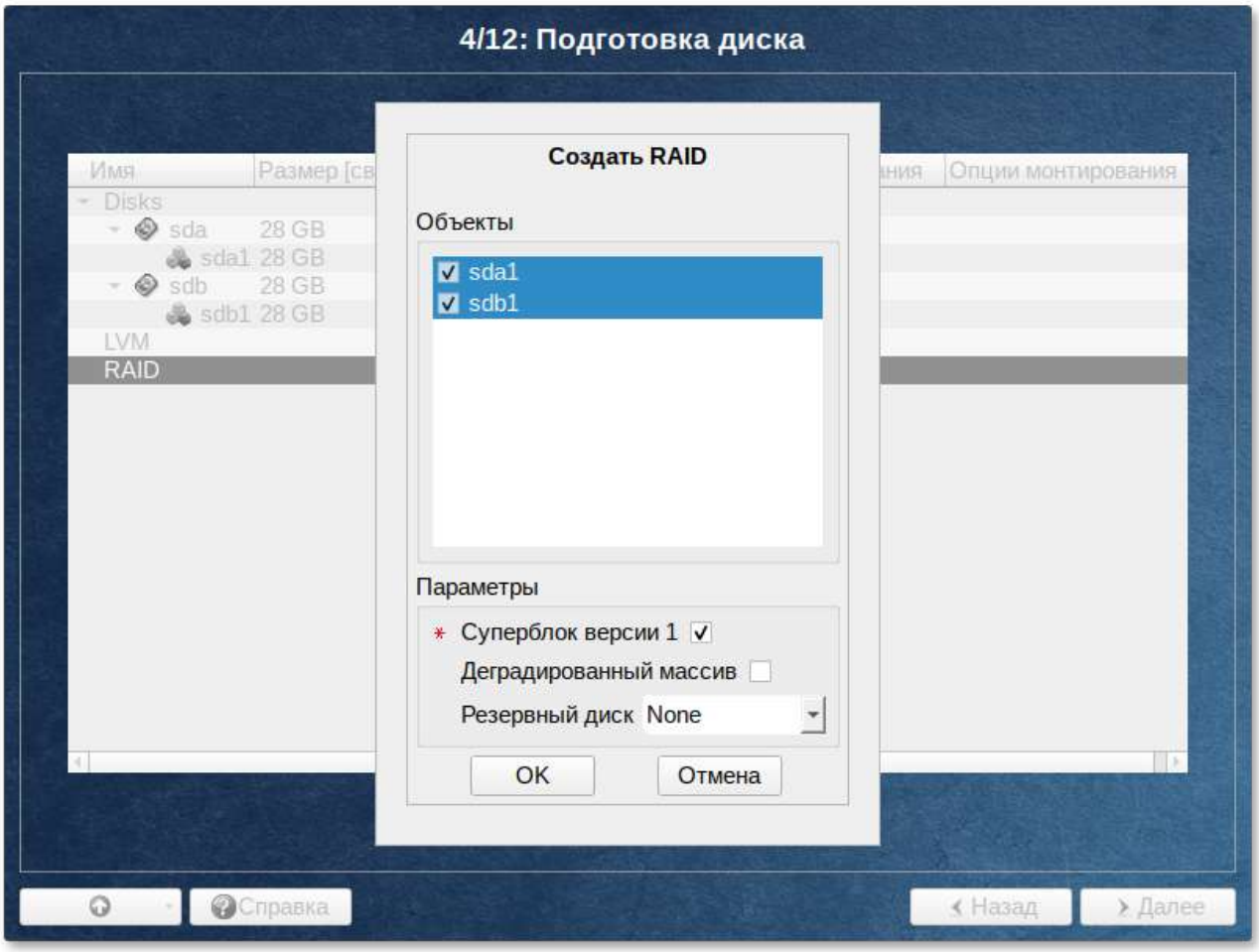
Примечание

При создании разделов следует учесть, что объём результирующего массива может зависеть от размера, включённых в него разделов жёсткого диска. Например, при создании RAID 1, результирующий размер массива будет равен размеру минимального участника.

После создания разделов на дисках можно переходить к организации самих RAID-массивов. Для этого в списке следует выбрать пункт **RAID**, после чего нажать кнопку **Создать RAID**.

Далее мастер предложит выбрать тип массива и указать его участников.





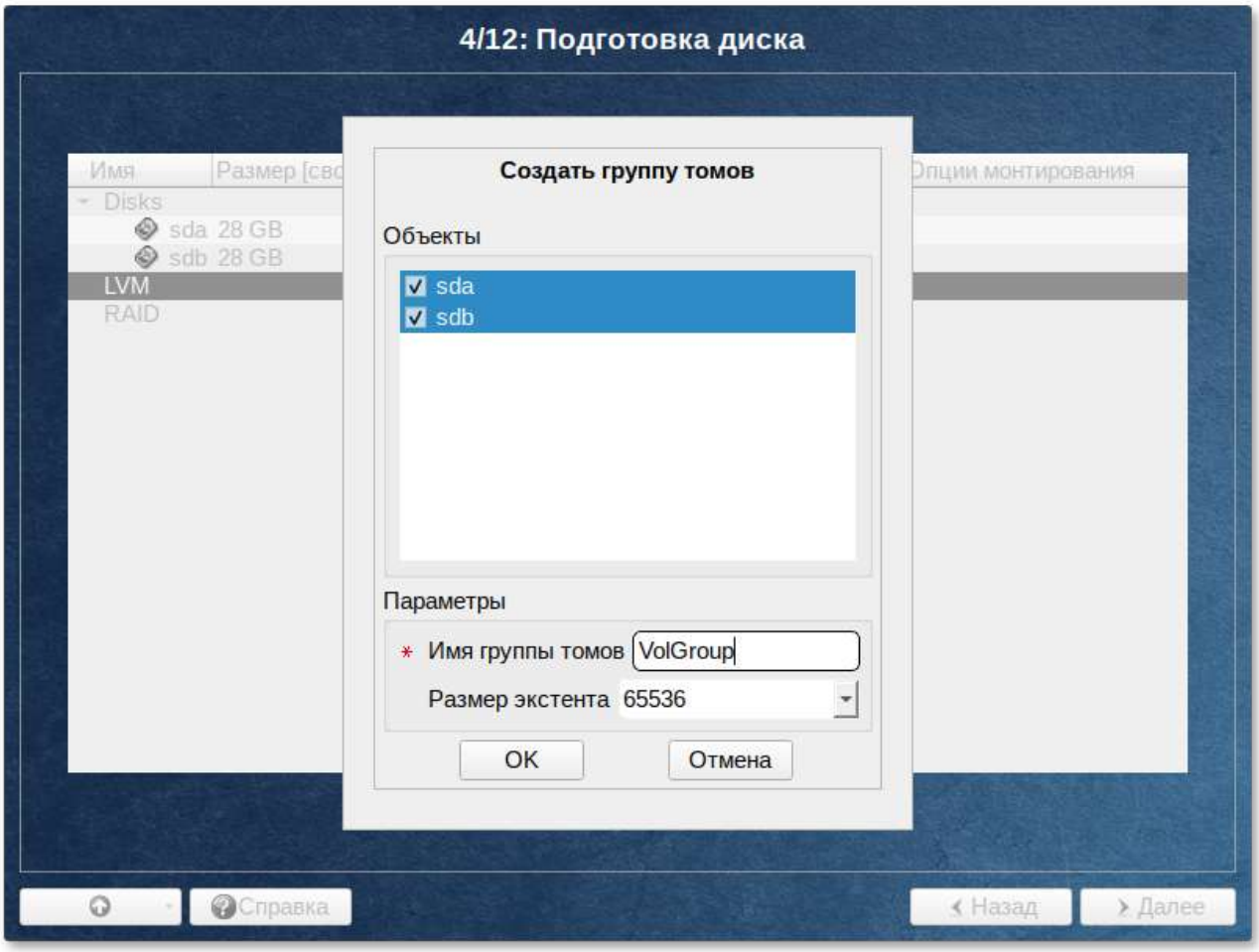
После создания RAID-массивов их можно использовать как обычные разделы на жёстких дисках, то есть, на них можно создавать файловые системы или же, например, включать их в LVM-тома.

12.4.2. Создание LVM-томов

Менеджер логических дисков LVM (Logical Volume Manager) — средство гибкого управления дисковым пространством, которое позволяет создавать поверх физических разделов (либо неразбитых дисков) логические тома, которые в самой системе будут видны как обычные блочные устройства с данными (обычные разделы).

Процесс подготовки к установке на LVM условно можно разбить на следующие шаги:

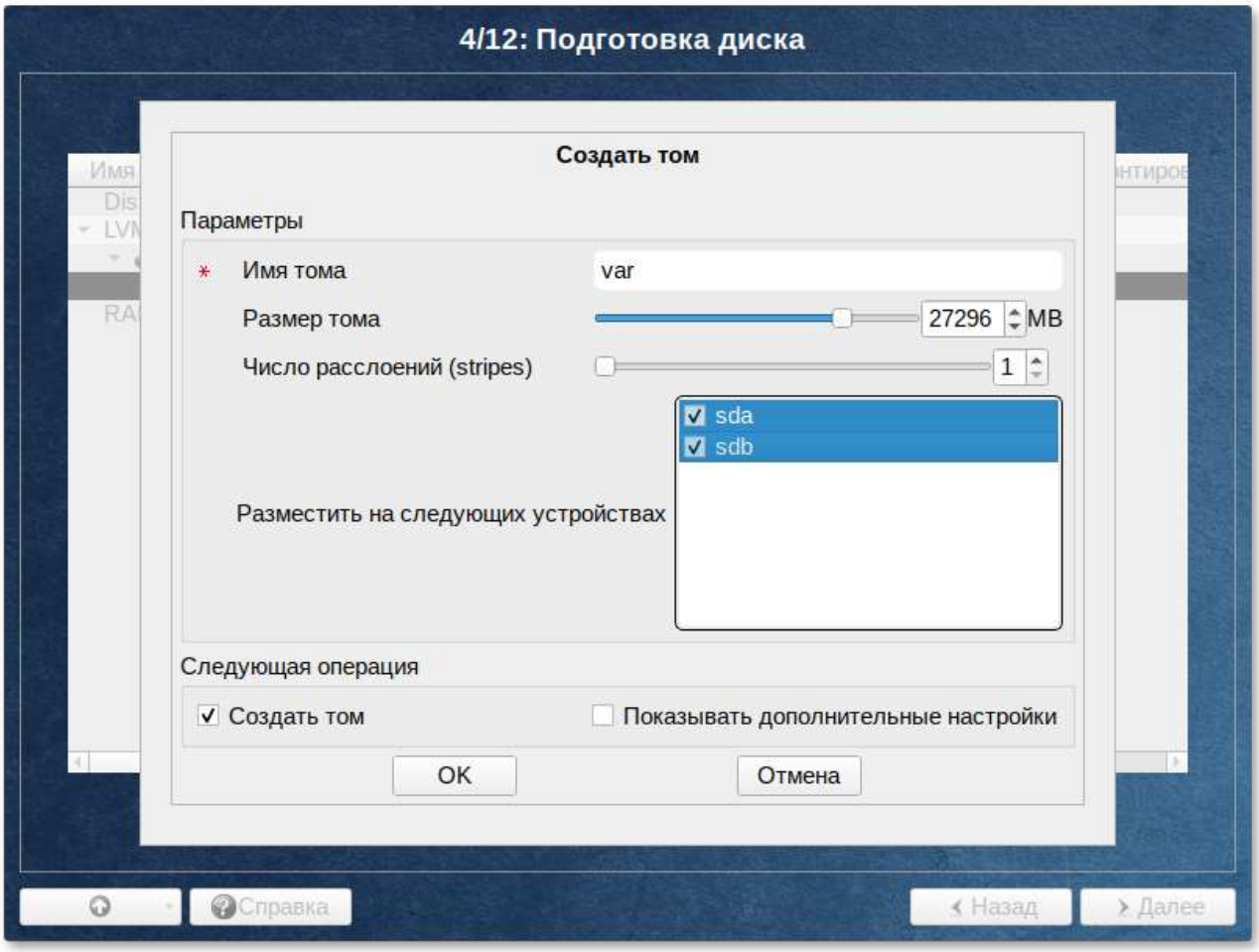
- создание группы томов LVM;
- создание томов LVM;
- создание файловых систем на томах LVM.



Важно

Для создания группы томов LVM может потребоваться предварительно удалить таблицу разделов с жёсткого диска.

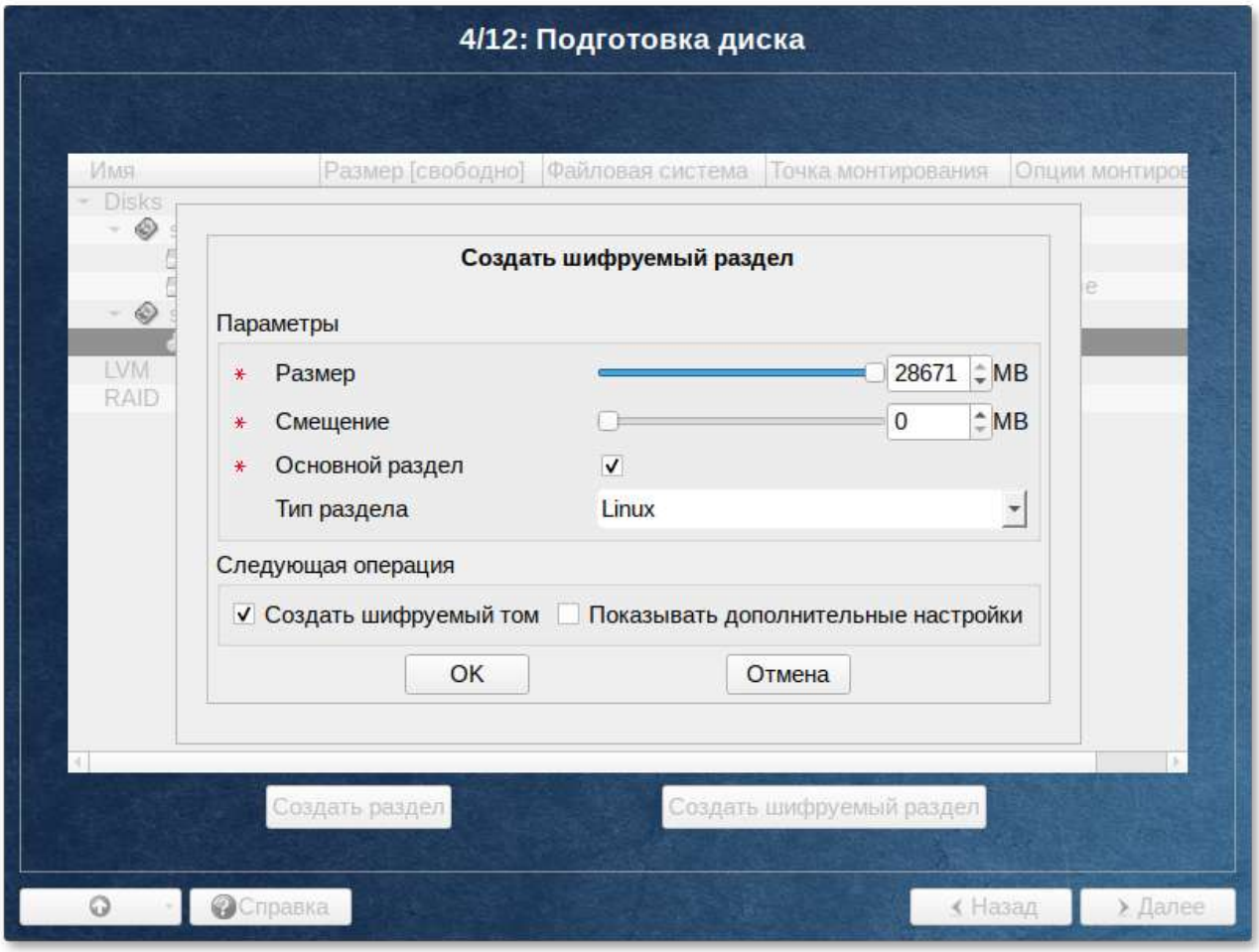
Для создания группы томов LVM в списке следует выбрать пункт **LVM**, после чего нажать кнопку **Создать группу томов**.



После создания группы томов LVM её можно использовать как обычный жёсткий диск, то есть внутри группы томов можно создавать тома (аналог раздела на физическом жёстком диске) и файловые системы внутри томов.

12.4.3. Создание шифрованных разделов

Программа установки Альт Сервер позволяет создавать шифрованные разделы.



Процесс создания шифрованного раздела ничем не отличается от процесса создания обычного раздела и инициируется нажатием на кнопку **Создать шифруемый раздел**.

После создания шифрованного раздела мастер, как и при создании обычного раздела, предложит создать на нём файловую систему и при необходимости потребует указать точку монтирования.

Предупреждение

Установка загрузчика на шифрованный раздел не поддерживается.

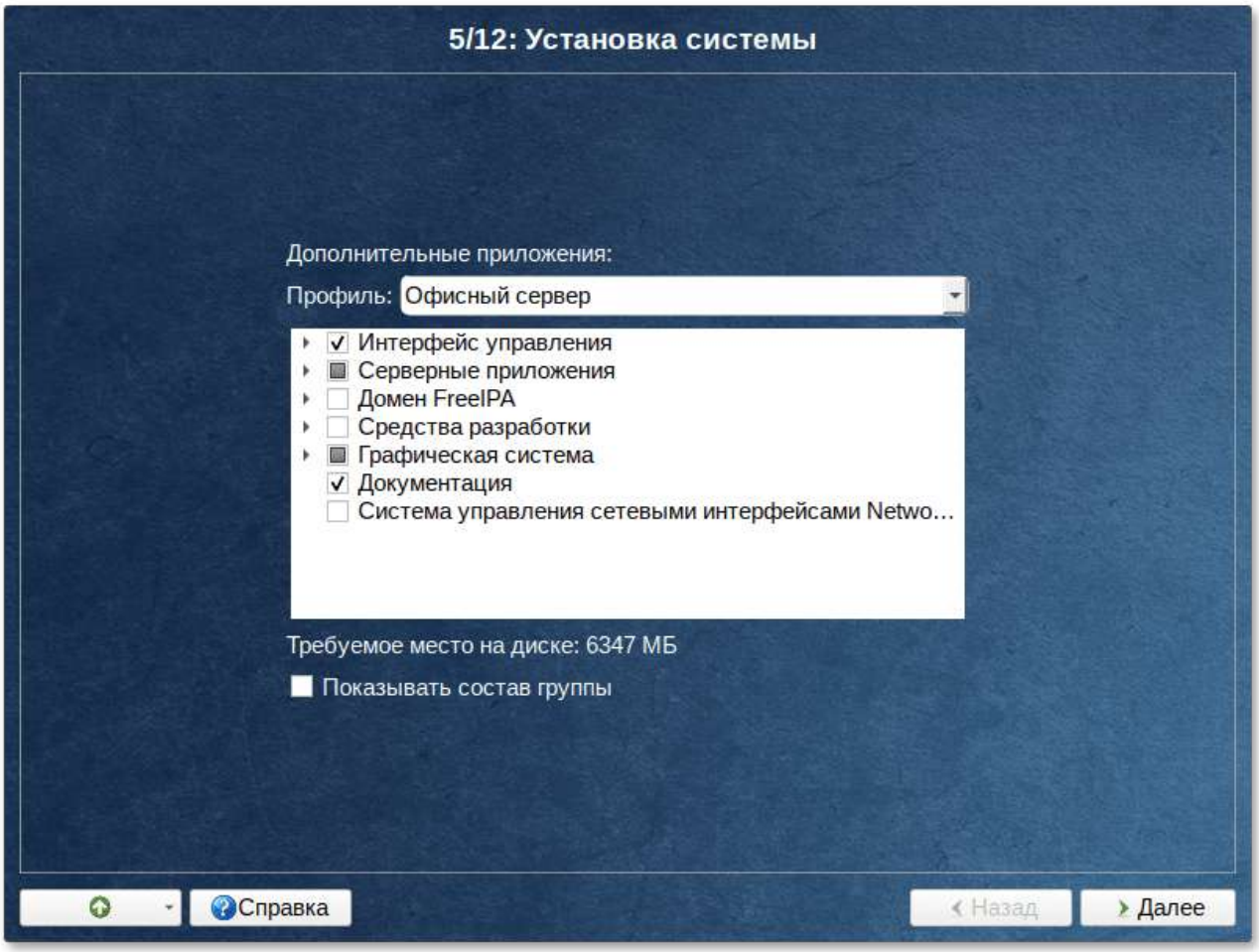
Для сохранения всех внесенных настроек и продолжения установки в окне **Подготовка диска** нужно нажать кнопку **Далее**.

Глава 13. Установка системы

На данном этапе происходит распаковка ядра и установка набора программ, необходимых для работы Альт Сервер.

Программа установки предлагает выбрать дополнительные пакеты программ, которые будут включены в состав Альт Сервер и установлены вместе с ней на диск.

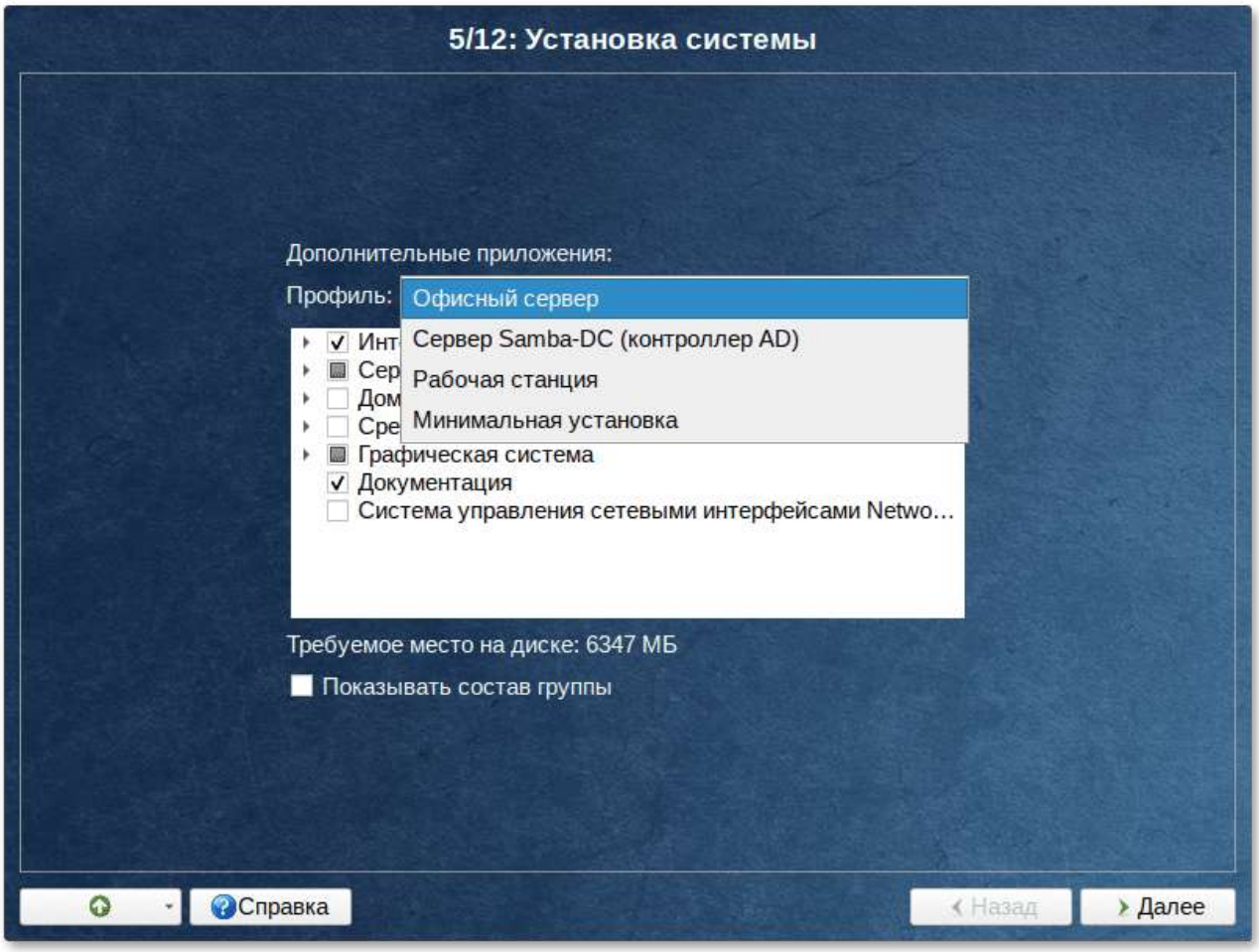
13.1. Дополнительные приложения



В дистрибутиве Альт Сервер доступно значительное количество программ (до нескольких тысяч), часть из них составляет саму операционную систему, а остальные — это прикладные программы и утилиты.

В Альт Сервер все операции установки и удаления производятся над пакетами — отдельными компонентами системы. Пакет и программа соотносятся неоднозначно: иногда одна программа состоит из нескольких пакетов, иногда один пакет включает несколько программ.

В процессе установки системы обычно не требуется детализированный выбор компонентов на уровне пакетов — это требует слишком много времени и знаний от проводящего установку. Тем более, что комплектация дистрибутива подбирается таким образом, чтобы из имеющихся программ можно было составить полноценную рабочую среду для соответствующей аудитории пользователей. Поэтому, в процессе установки системы пользователю предлагается выбрать из небольшого списка групп пакетов, объединяющих пакеты, необходимые для решения наиболее распространённых задач. Под списком групп на экране отображается информация об объёме дискового пространства, которое будет занято после установки пакетов, входящих в выбранные группы.



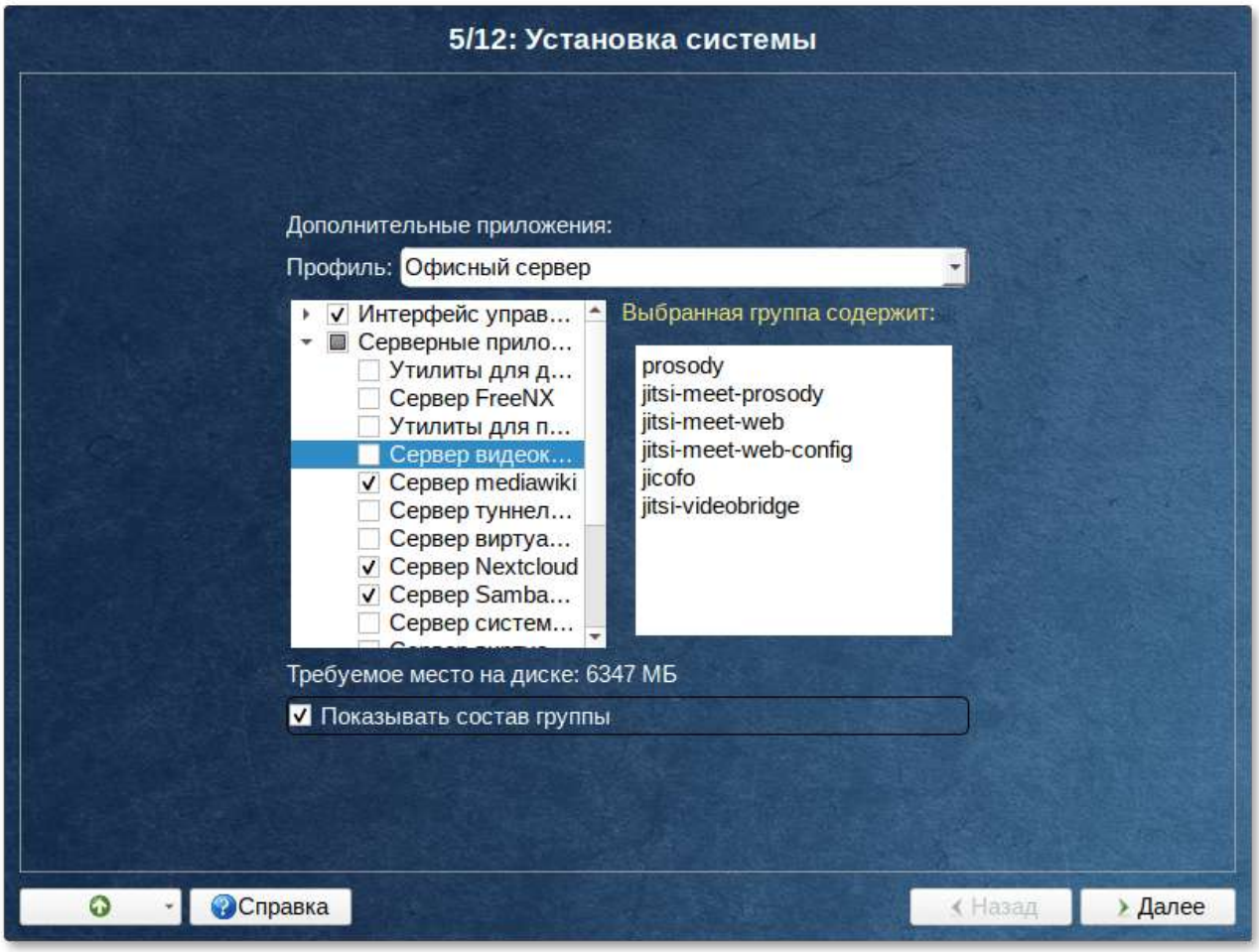
При установке сервера доступны следующие профили:

- **Офисный сервер** – для установки будут предложены группы пакетов с серверными приложениями;
- **Сервер Samba-DC (контроллер AD)** – для установки будут предложена группа пакетов для конфигурации сервера в качестве контроллера AD;
- **Рабочая станция** – серверные приложения в состав устанавливаемых пакетов включаться не будут;
- **Минимальная установка** – дополнительное ПО в состав устанавливаемых пакетов включаться не будет.

После выбора профиля можно изменить состав устанавливаемых пакетов.

Под списком групп на экране отображается информация об объёме дискового пространства, которое будет занято после установки пакетов, входящих в выбранные группы.

Опция **Показать состав группы** выводит список программных пакетов, входящих в состав той или иной группы пакетов.



Важно

При установке серверных приложений (**Сервер mediawiki** и **Сервер Nextcloud**) после загрузки доступны службы Mediawiki 1.35 и Nextcloud 16. Для доступа, к административным функциям этих приложений через веб-интерфейс необходимо сменить пароль администратора в «Центре управления системой» (пароль должен быть достаточно сложным и содержать не менее 10 символов).

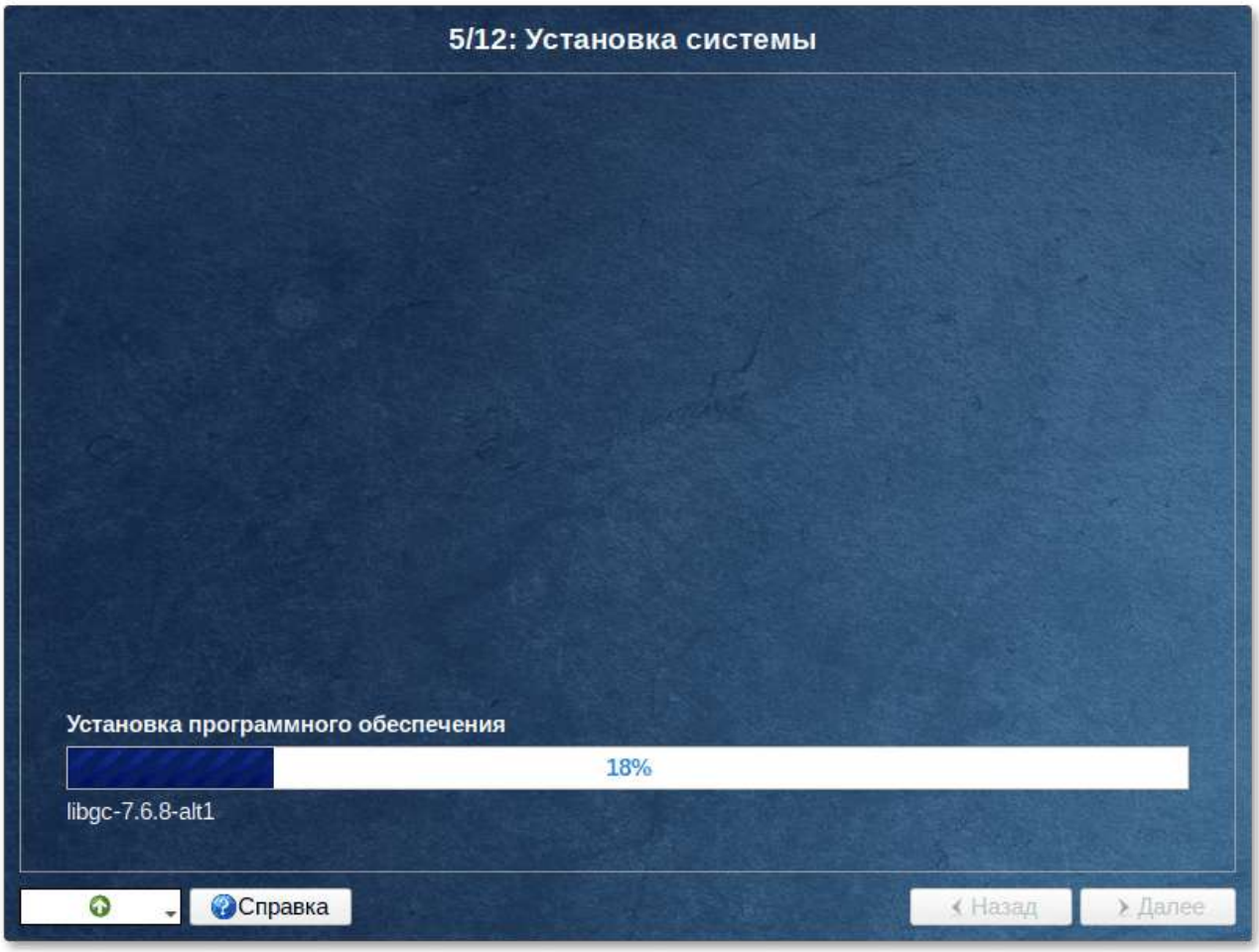
MediaWiki установленная при установке системы доступна по адресу **https://localhost/wiki/**. Администратор: WikiSysop, пароль: пароль пользователя root.

Веб-приложение Nextcloud установленное при установке системы доступно по адресу **https://localhost/nextcloud/**. Администратор: root, пароль: пароль пользователя root.

Выбрав необходимые группы, следует нажать кнопку **Далее**, после чего начнётся установка пакетов.

13.2. Установка пакетов

На этом этапе происходит установка набора программ, необходимых для работы системы.



Установка происходит автоматически в два этапа:

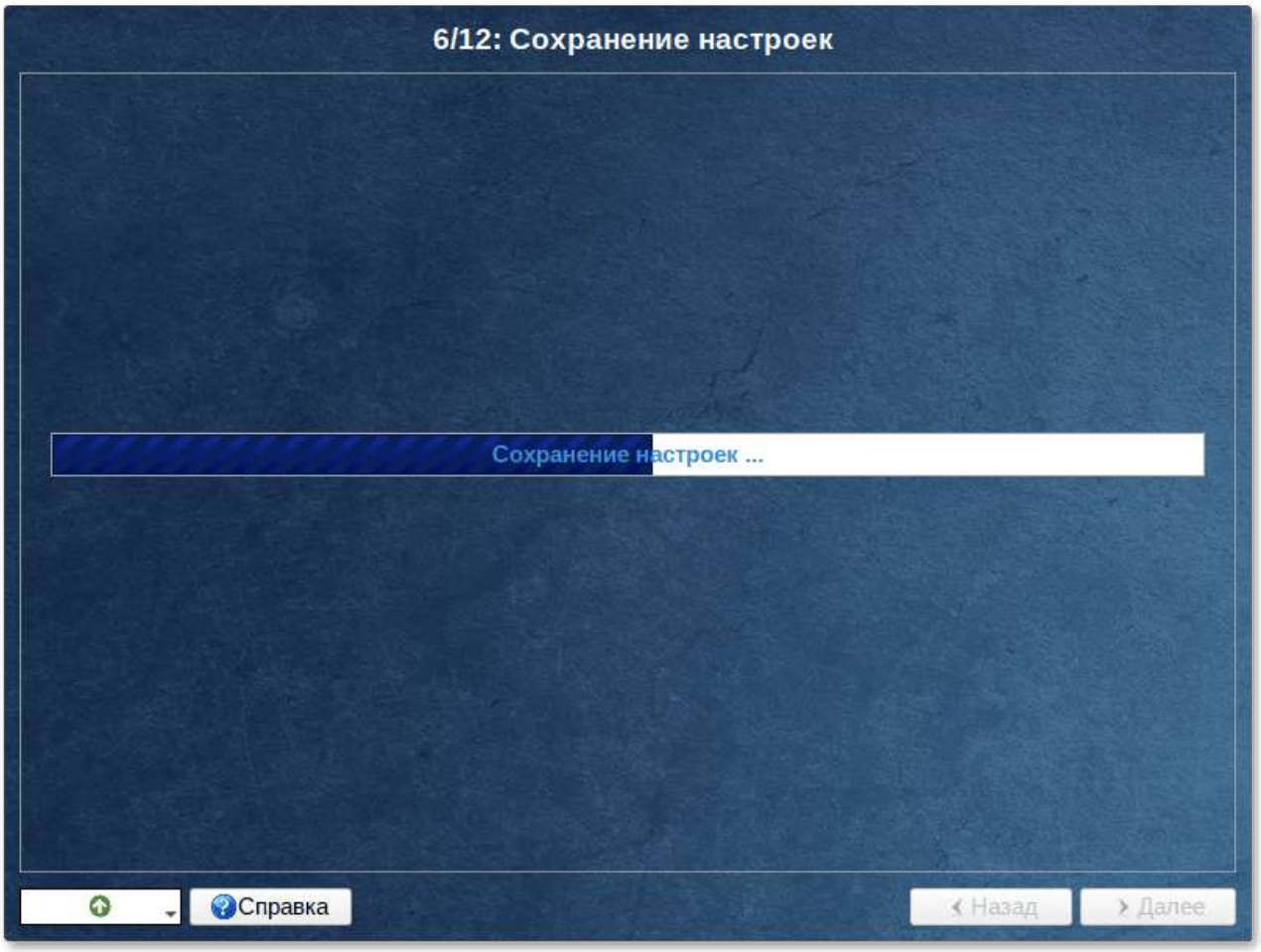
- получение пакетов;
- установка пакетов.

Получение пакетов осуществляется из источника, выбранного на этапе начальной загрузки. При сетевой установке (по протоколу FTP или HTTP) время выполнения этого шага будет зависеть от скорости соединения и может быть значительно большим в сравнении с установкой с лазерного диска.

Глава 14. Сохранение настроек

Начиная с данного этапа, программа установки работает с файлами только что установленной базовой системы. Все последующие изменения можно будет совершить после завершения установки посредством редактирования соответствующих конфигурационных файлов или при помощи модулей управления, включенных в дистрибутив.

По завершении установки базовой системы начинается шаг сохранения настроек. Он проходит автоматически и не требует вмешательства пользователя. На экране отображается индикатор выполнения.

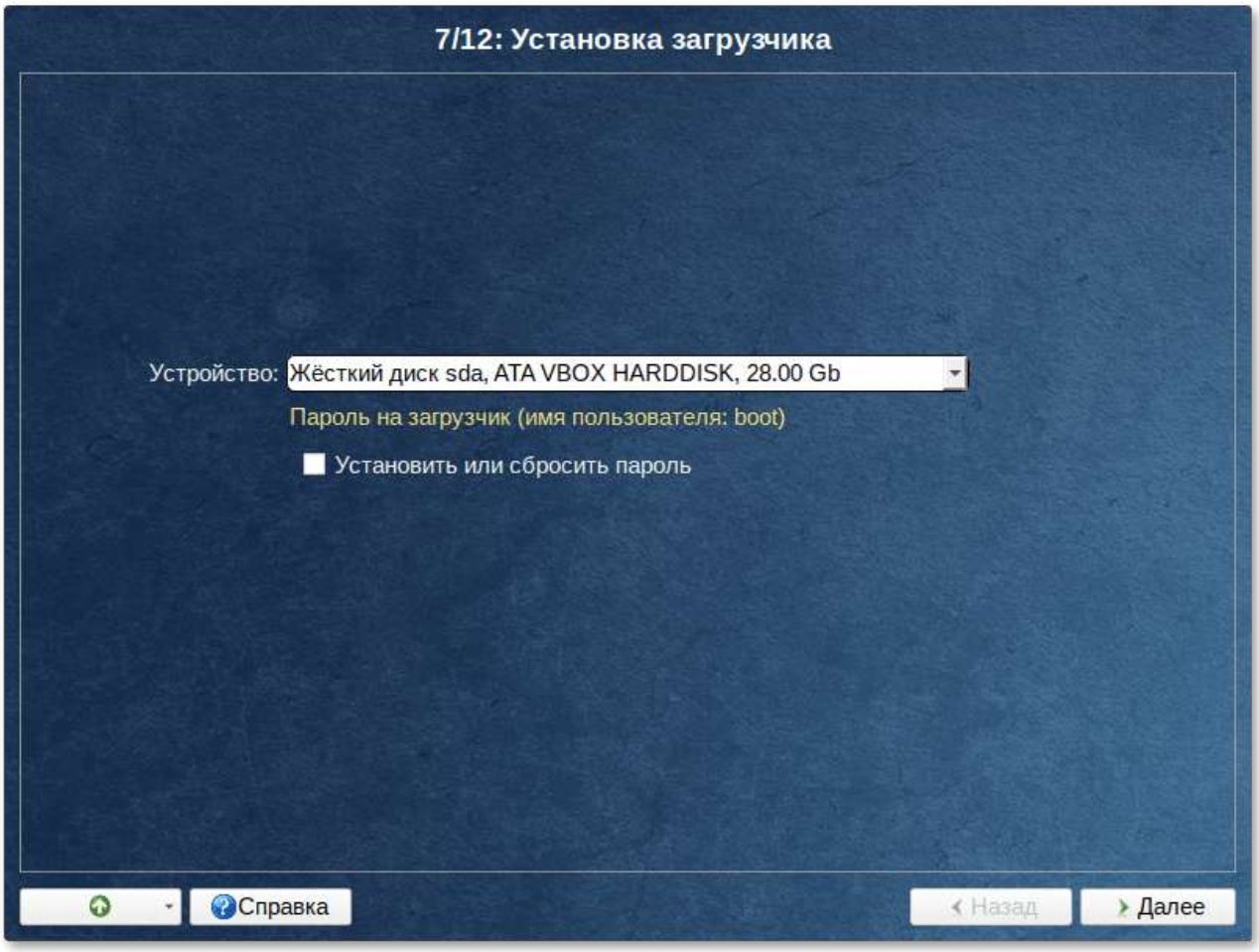


На этом шаге производится перенос настроек, выполненных на первых шагах установки, в только что установленную базовую систему. Также производится запись информации о соответствии разделов жесткого диска смонтированным на них файловым системам (заполняется конфигурационный файл **`/etc/fstab`**).

После сохранения настроек осуществляется автоматический переход к следующему шагу.

Глава 15. Установка загрузчика

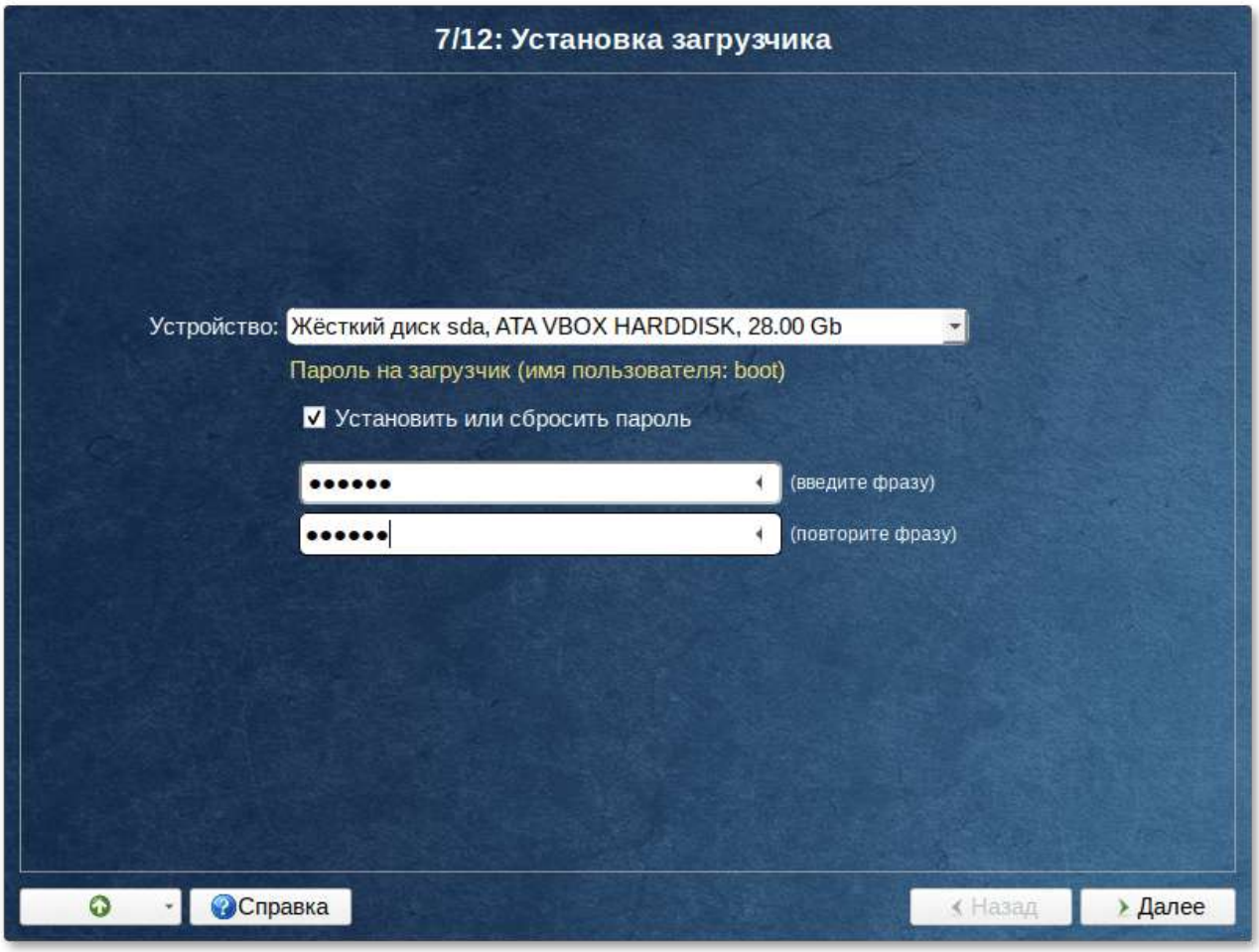
Загрузчик ОС — это программа, которая позволяет загружать Альт Сервер и другие ОС, если они установлены на данной машине.



Программа установки автоматически определяет, в каком разделе НЖМД следует располагать загрузчик для возможности корректного запуска ОС Альт Сервер. Положение загрузчика, в случае необходимости, можно изменить в выпадающем списке **Устройство**, выбрав другой раздел.

Если же вы планируете использовать и другие ОС, уже установленные на этом компьютере, тогда имеет значение на каком жёстком диске или в каком разделе будет расположен загрузчик.

Для ограничения доступа к опциям загрузки можно установить пароль на загрузчик. Для этого необходимо отметить пункт **Установить или сбросить пароль** и, в появившихся полях для ввода, задать пароль.



Примечание

При необходимости изменения опций загрузки при старте компьютера потребуется ввести имя пользователя «boot» и заданный на этом шаге пароль.

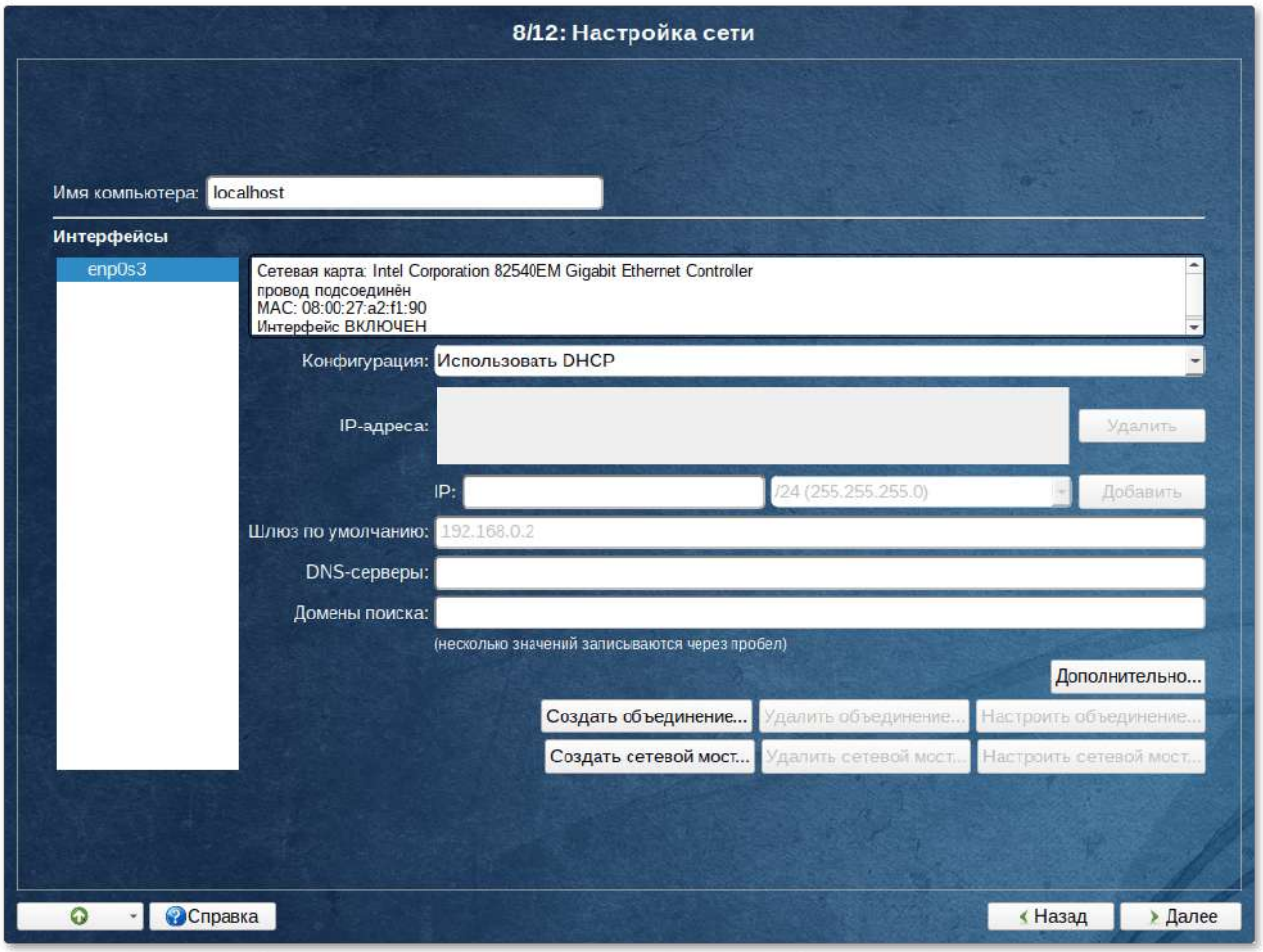
Важно

При установке на EFI выберите в качестве устройства для установки «**EFI**».
Рекомендуется выбрать автоматическое разбиение на этапе разметки диска для создания необходимых разделов для загрузки с EFI.

Для подтверждения выбора и продолжения работы программы установки необходимо нажать кнопку **Далее**.

Глава 16. Настройка сети

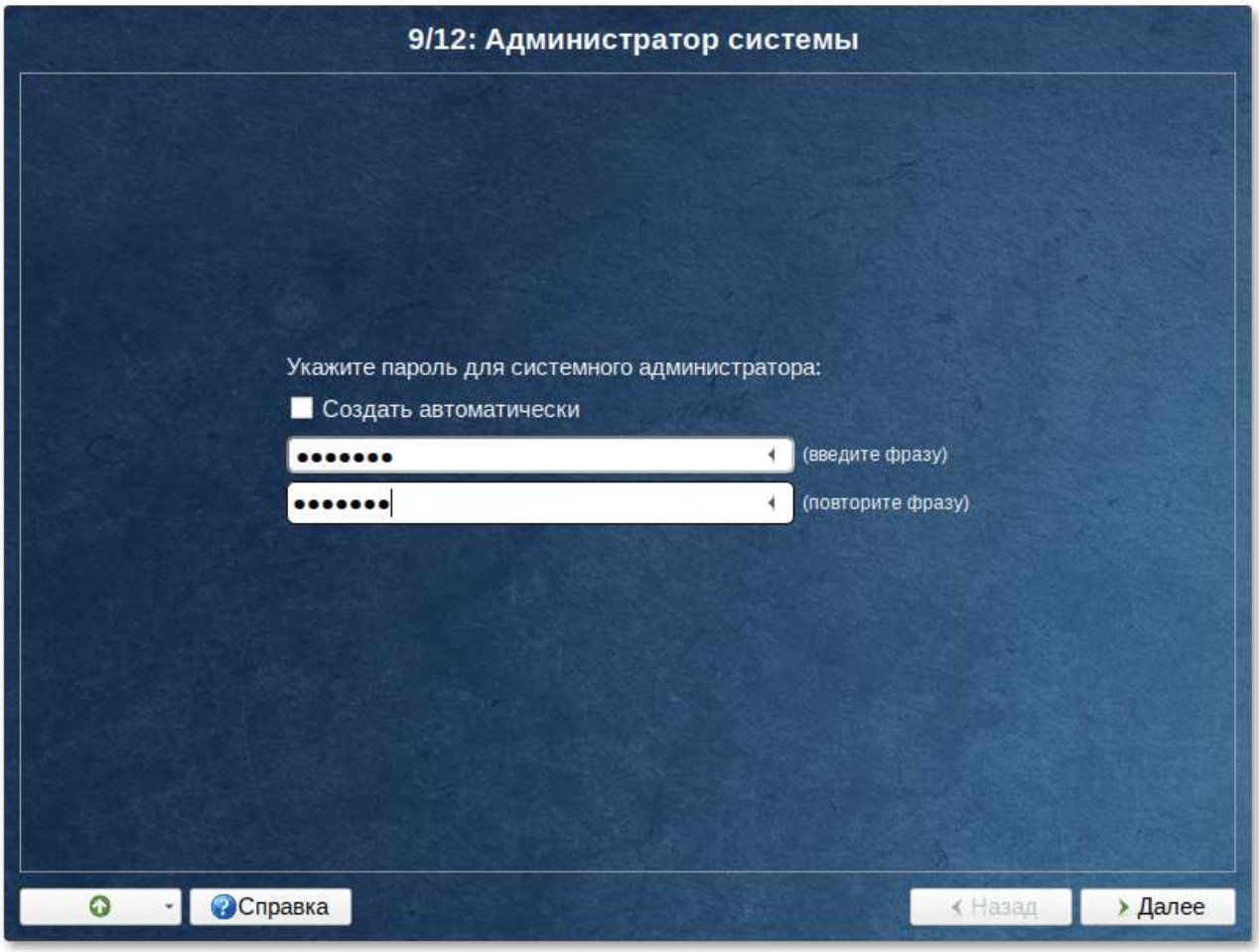
На этом этапе необходимо задать параметры работы сетевой карты и настройки сети: IP-адреса сетевых интерфейсов, DNS-сервер, шлюз и т.п. Конкретные значения будут зависеть от используемого вами сетевого окружения. Ручного введения настроек можно избежать при наличии в сети настроенного DHCP-сервера. В этом случае все необходимые сетевые настройки будут получены автоматически.



Для сохранения настроек сети и продолжения работы программы установки необходимо нажать кнопку **Далее**.

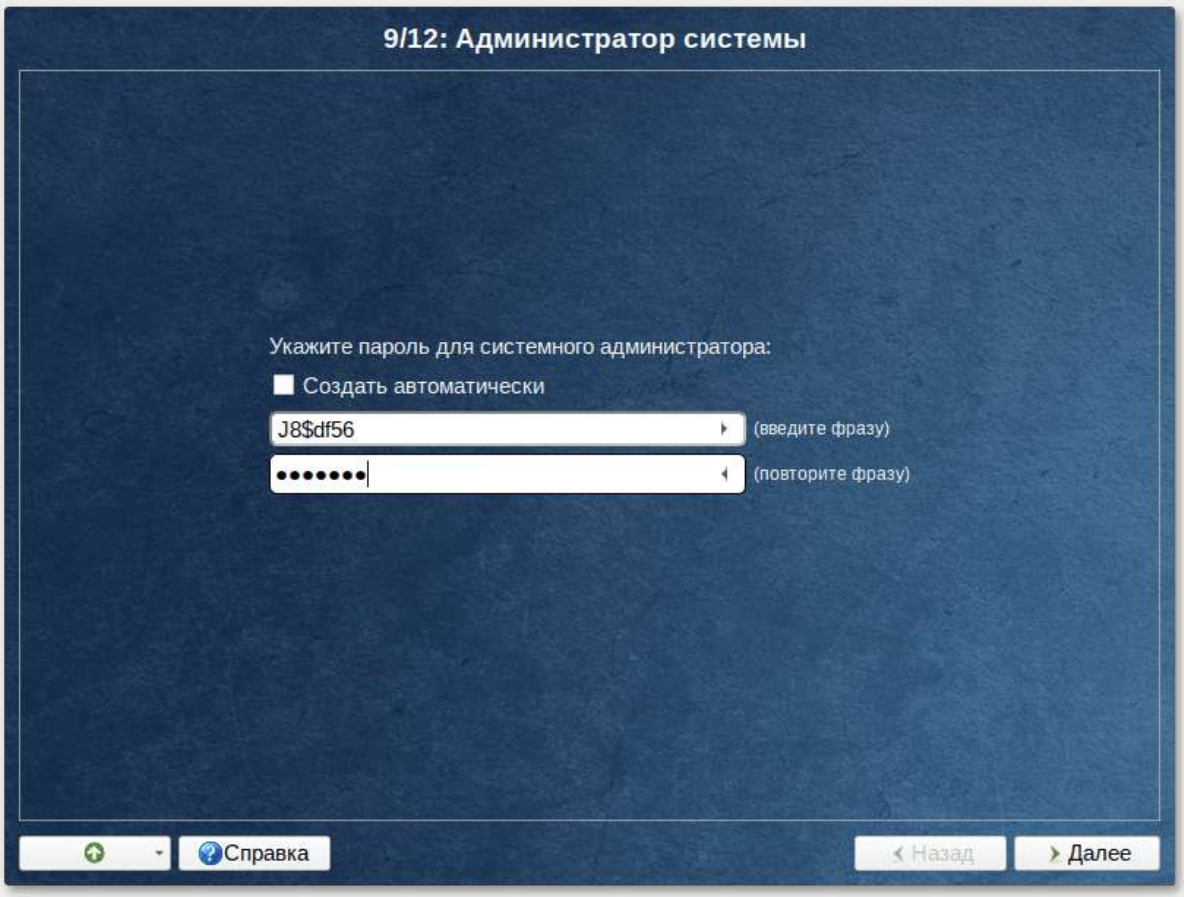
Глава 17. Администратор системы

На данном этапе загрузчик создает учетную запись администратора. В открывшемся окне необходимо ввести пароль учетной записи администратора (root). Чтобы исключить опечатки при вводе пароля, пароль учетной записи вводится дважды.


9/12: Администратор системы
Укажите пароль для системного администратора:
Создать автоматически
(введите фразу)
(повторите фразу)
Справка
Назад
Далее

Примечание

Чтобы избежать последствий неверной раскладки клавиатуры можно просмотреть пароль, который будет сохранен. Для этого нажмите на значок стрелки в поле ввода:



Для автоматической генерации пароля необходимо отметить пункт **Создать автоматически**. Система предложит пароль, сгенерированный автоматическим образом в соответствии с требованиями по стойкости паролей.

В любой системе Linux всегда присутствует один специальный пользователь — *администратор системы*, он же *суперпользователь*. Для него зарезервировано стандартное системное имя — root.

Администратор системы отличается от всех прочих пользователей тем, что ему позволено производить *любые*, в том числе самые разрушительные изменения в системе. Поэтому выбор пароля администратора системы — очень важный момент для *безопасности*. Любой, кто сможет ввести его правильно (узнать или подобрать), получит неограниченный доступ к системе. Даже ваши собственные неосторожные действия от имени root могут иметь катастрофические последствия для всей системы.

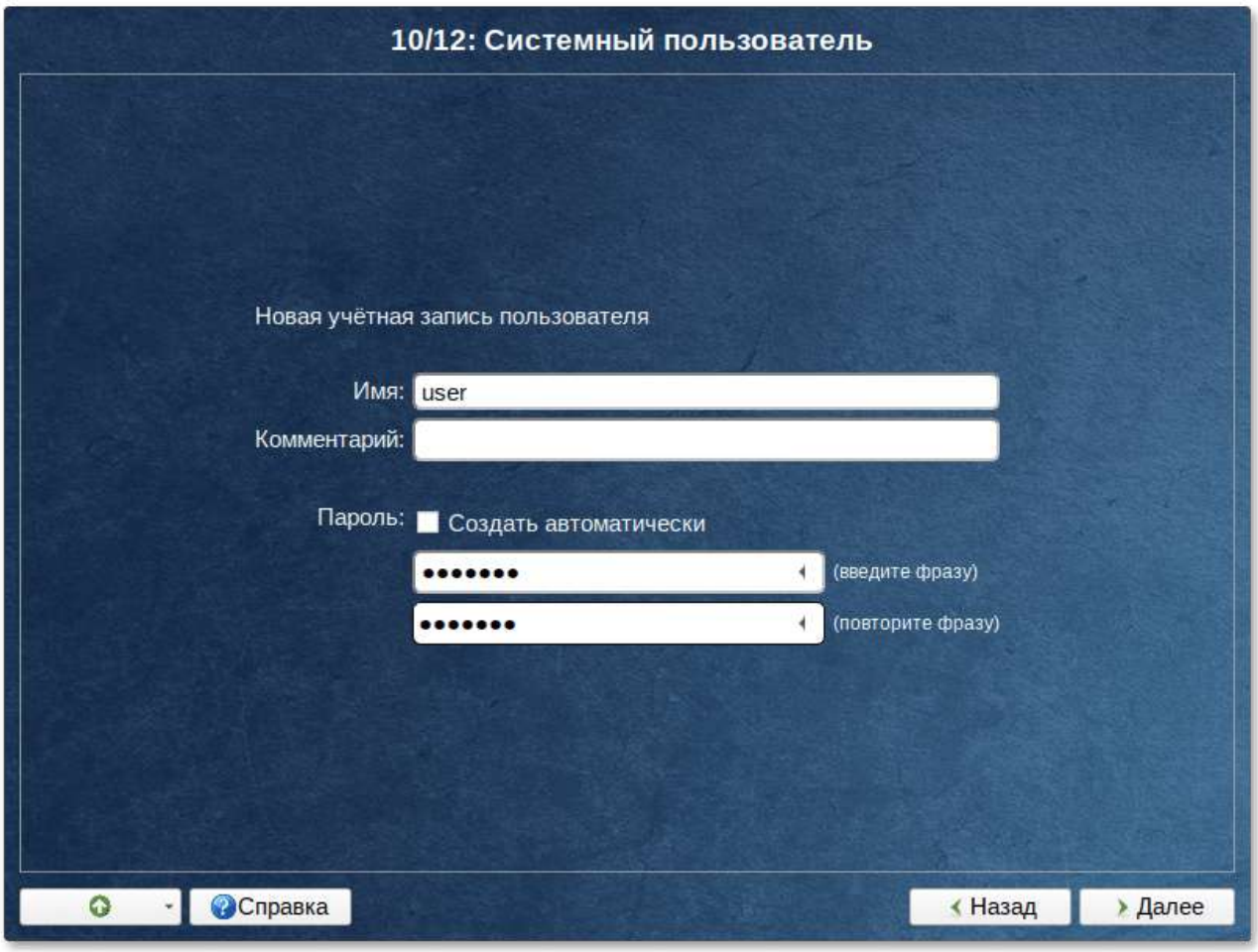
Важно

Стоит запомнить пароль root — его нужно будет вводить для получения права изменять настройки системы с помощью стандартных средств настройки Альт Сервер. Более подробную информацию о режиме суперпользователя вы можете прочитать в главе Режим суперпользователя.

Подтверждение введенного (или сгенерированного) пароля учетной записи администратора (root) и продолжение работы программы установки выполняется нажатием кнопки **Далее**.

Глава 18. Системный пользователь

На данном этапе программа установки создает учетную запись системного пользователя (пользователя) Альт Сервер.



Помимо администратора (root) в систему необходимо добавить, по меньшей мере, одного обычного *системного пользователя*. Работа от имени администратора системы считается опасной, поэтому повседневную работу в Linux следует выполнять от имени ограниченного в полномочиях системного пользователя.

При добавлении системного пользователя предлагается ввести имя учётной записи пользователя. Имя учётной записи всегда представляет собой одно слово, состоящее только из строчных латинских букв (заглавные запрещены), цифр и символа подчёркивания «_» (причём цифра и символ «_» не могут стоять в начале слова).

Для того чтобы исключить опечатки, пароль пользователя вводится дважды. Пароль пользователя можно создать автоматически, по аналогии с автоматическим созданием пароля суперпользователя.

Для автоматической генерации пароля необходимо отметить пункт **Создать автоматически**. Система предложит пароль, сгенерированный автоматическим образом в соответствии с требованиями по стойкости паролей.

В процессе установки предлагается создать только одну учётную запись системного пользователя — от его имени можно выполнять задачи, не требующие привилегий суперпользователя. Учётные записи для всех прочих пользователей системы можно будет создать в любой момент после установки операционной системы.

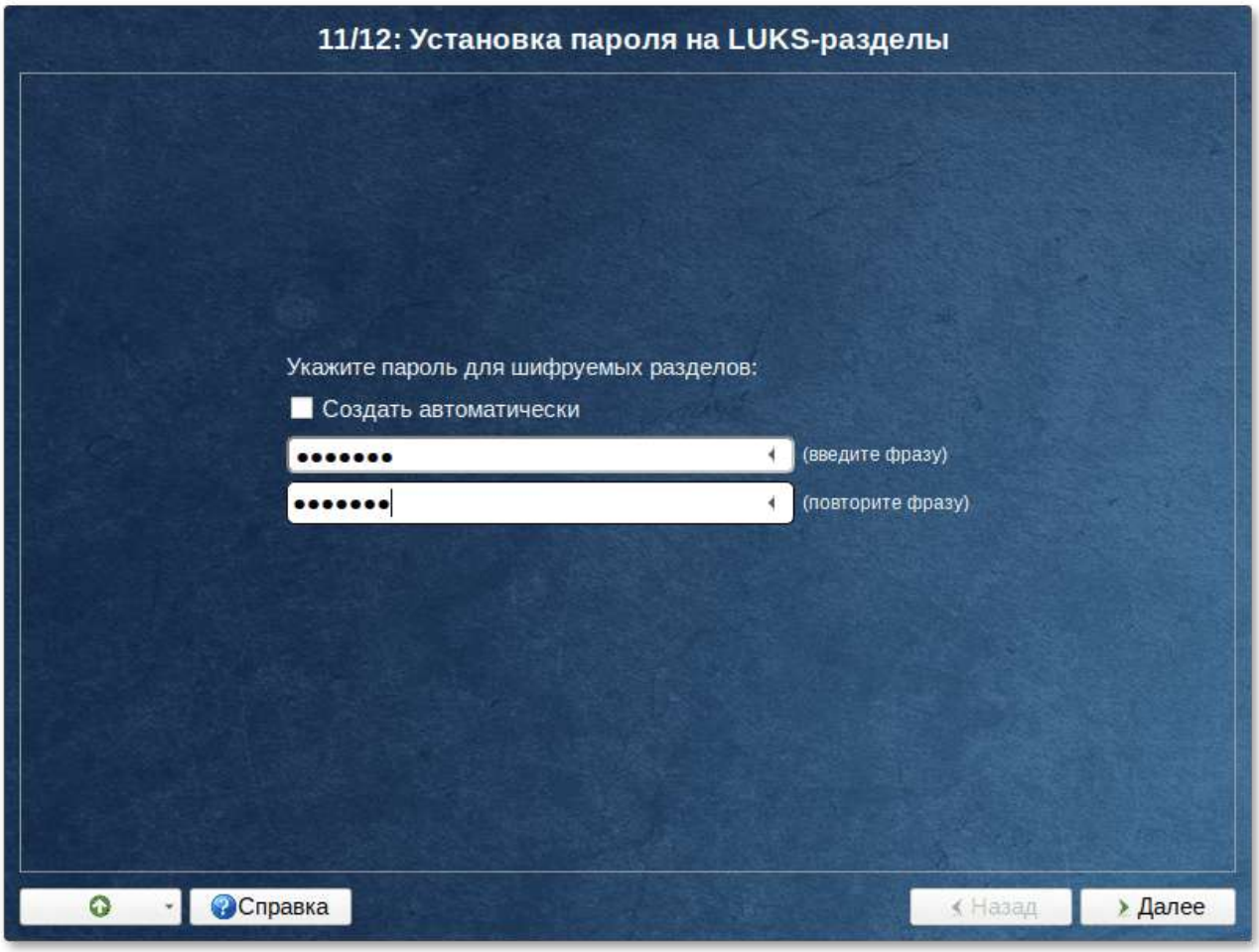
Подтверждение введенного (или сгенерированного) пароля учетной записи системного пользователя и продолжение работы программы установки выполняется нажатием кнопки **Далее**.

Глава 19. Установка пароля на шифрованные разделы

Примечание

Если вы не создавали шифруемые разделы, то этот шаг пропускается автоматически. В этом случае сразу переходите к главе Завершение установки.

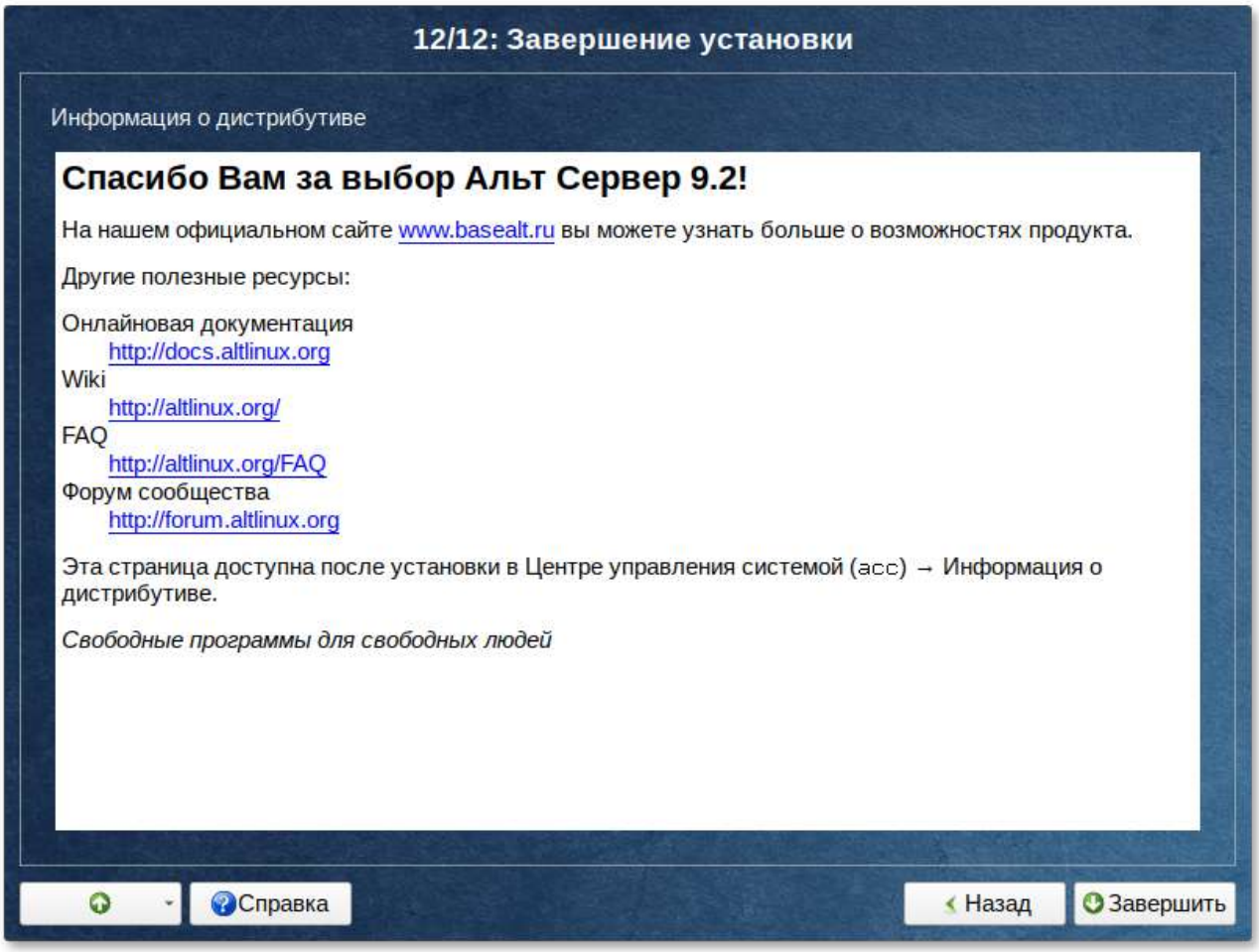
На этом этапе требуется ввести пароль для шифруемых разделов. Этот пароль потребуется вводить для того, чтобы получать доступ к информации на данных разделах.



Например, если вы зашифровали **/home**, то во время загрузки системы будет необходимо ввести пароль для этого раздела, иначе вы не сможете получить доступ в систему под своим именем пользователя.

Глава 20. Завершение установки

На экране последнего шага установки отображается информация о завершении установки Альт Сервер.



После нажатия кнопки **Завершить** автоматически начнется перезагрузка системы.

Не забудьте извлечь установочный DVD (если это не происходит автоматически). Далее можно загружать установленную систему в обычном режиме.

Глава 21. Особенности установки в UEFI-режиме

21.1. Начальный загрузчик EFI

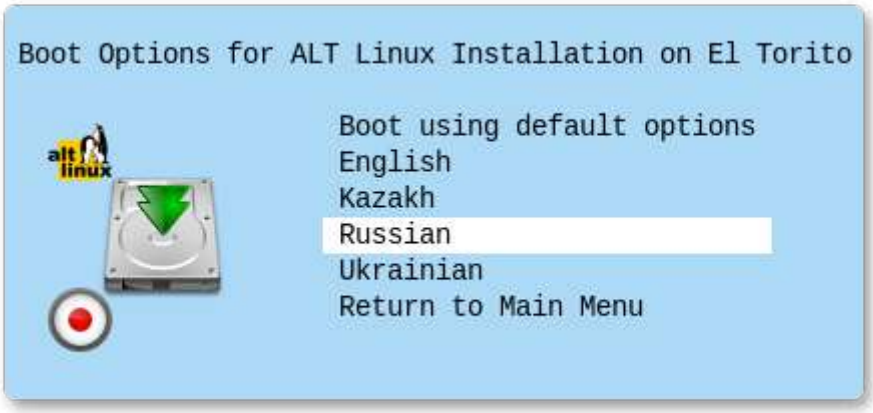
После загрузки компьютера с установочного диска выводится меню, в котором можно выбрать варианты загрузки системы. Начальный загрузчик EFI не похож на обычный. Меню загрузчика горизонтальное, графическое:

Примечание

Мышь на этом этапе установки не поддерживается. Для выбора опций установки и различных вариантов необходимо использовать клавиатуру.

В нижней части экрана отображаются подсказки по использованию клавиатуры:

- для перемещения курсора необходимо использовать клавиши со стрелками;
- нажатие клавиши **Enter** приводит к активированию выбранного пункта меню;
- по нажатию клавиши **F2** открывается меню доступных параметров, каждого пункта. Например, при установке системы можно выбрать язык интерфейса загрузчика и программы установки:



21.2. Подготовка диска

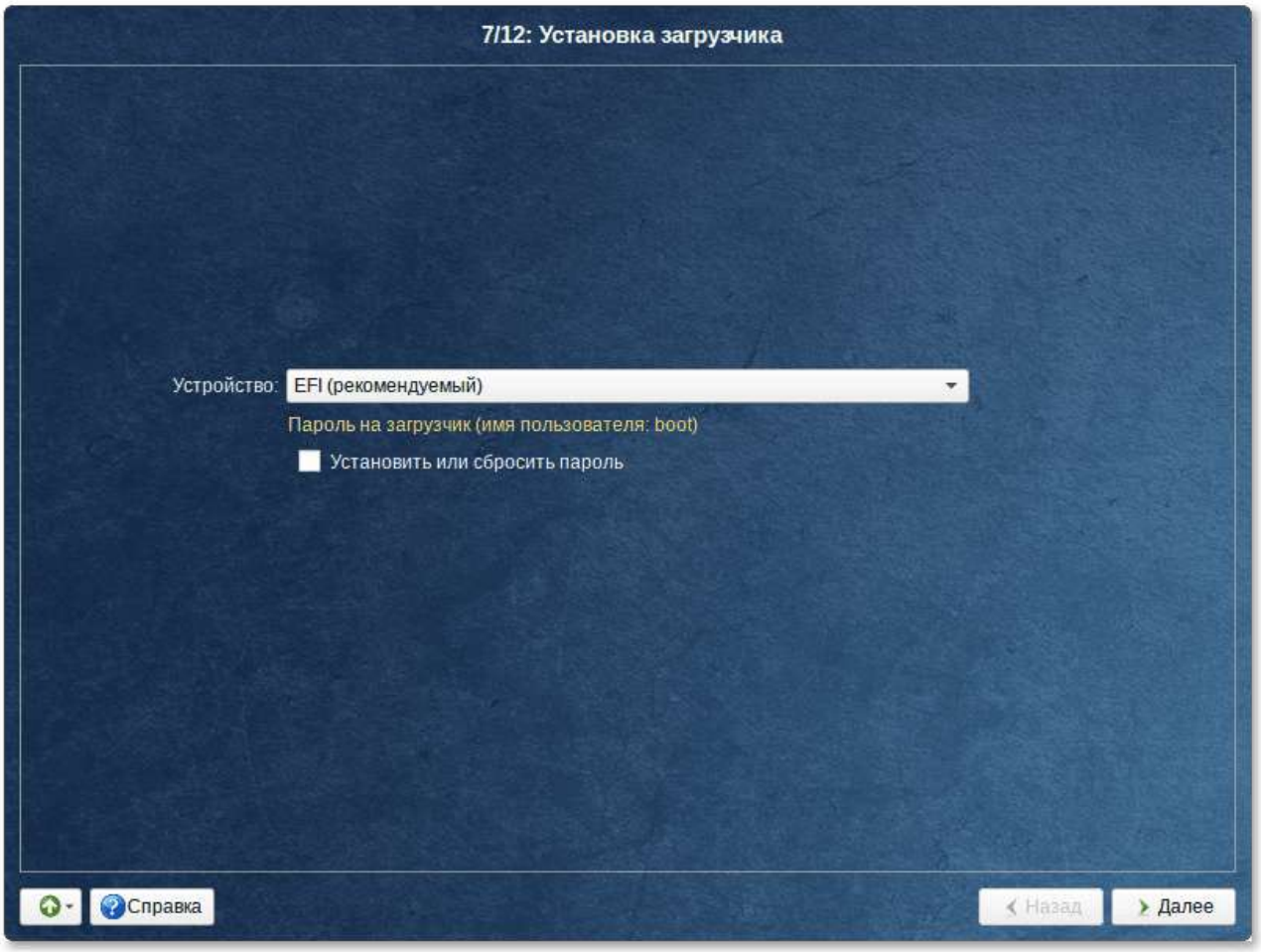
Особенности разбиения диска:

- для того, чтобы система правильно работала (в частности могла загрузиться) с UEFI, при ручном разбиении диска надо обязательно сделать точку монтирования **`/boot/efi`**, в которую нужно смонтировать vfat раздел с загрузочными записями. Если такого раздела нет, то его надо создать вручную. При разбивке жёсткого диска в автоматическом режиме такой раздел создаёт сам установщик;
- требуется создать новый или подключить существующий FAT32-раздел с GPT-типом ESP (**`efi system partition`**) размером ~100—500 Мб (будет смонтирован в **`/boot/efi`**);
- может понадобиться раздел типа **`bios boot partition`** минимального размера, никуда не подключенный и предназначенный для встраивания grub2-efi;
- остальные разделы — и файловая система, и swap — имеют GPT-тип **`basic data`**; актуальный тип раздела задаётся отдельно.

Ручной профиль разбиения диска позволяет установить ОС на программный RAID-массив, разместить разделы в томах LVM и использовать шифрование на разделах.

21.3. Установка загрузчика

Программа установки автоматически определяет, в каком разделе следует располагать загрузчик. Модуль установки загрузчика предложит вариант **`EFI`**, с которым стоит согласиться.



Глава 22. Обновление системы до актуального состояния

После установки системы, её лучше сразу обновить до актуального состояния. Можно не обновлять систему и сразу приступать к работе только в том случае, если вы не планируете подключаться к сети или Интернету, не собираетесь устанавливать дополнительных программ.

Для обновления системы необходимо выполнить команды (с правами администратора):

```
# apt-get update
# apt-get dist-upgrade
# update-kernel
# apt-get clean
# reboot
```

Примечание

Получить права администратора можно, выполнив в терминале команду:

```
$ su -
```

или зарегистрировавшись в системе (например, на второй консоли **Ctrl**+**Alt**+**F2**) под именем **root**. Про режим суперпользователя можно почитать в главе Режим суперпользователя.

Примечание

Подробнее про обновление пакетов можно прочитать в главах Обновление всех установленных пакетов, Обновление всех установленных пакетов и Обновление ядра.

Глава 23. Первая помощь

Важно

В случае возникновения каких-либо неприятностей не паникуйте, а спокойно разберитесь в сложившейся ситуации. Linux не так уж просто довести до полной неработоспособности и утраты ценных данных. Поспешные действия отчаявшегося пользователя могут привести к плачевным результатам. Помните, что решение есть, и оно обязательно найдётся!

23.1. Проблемы при установке системы

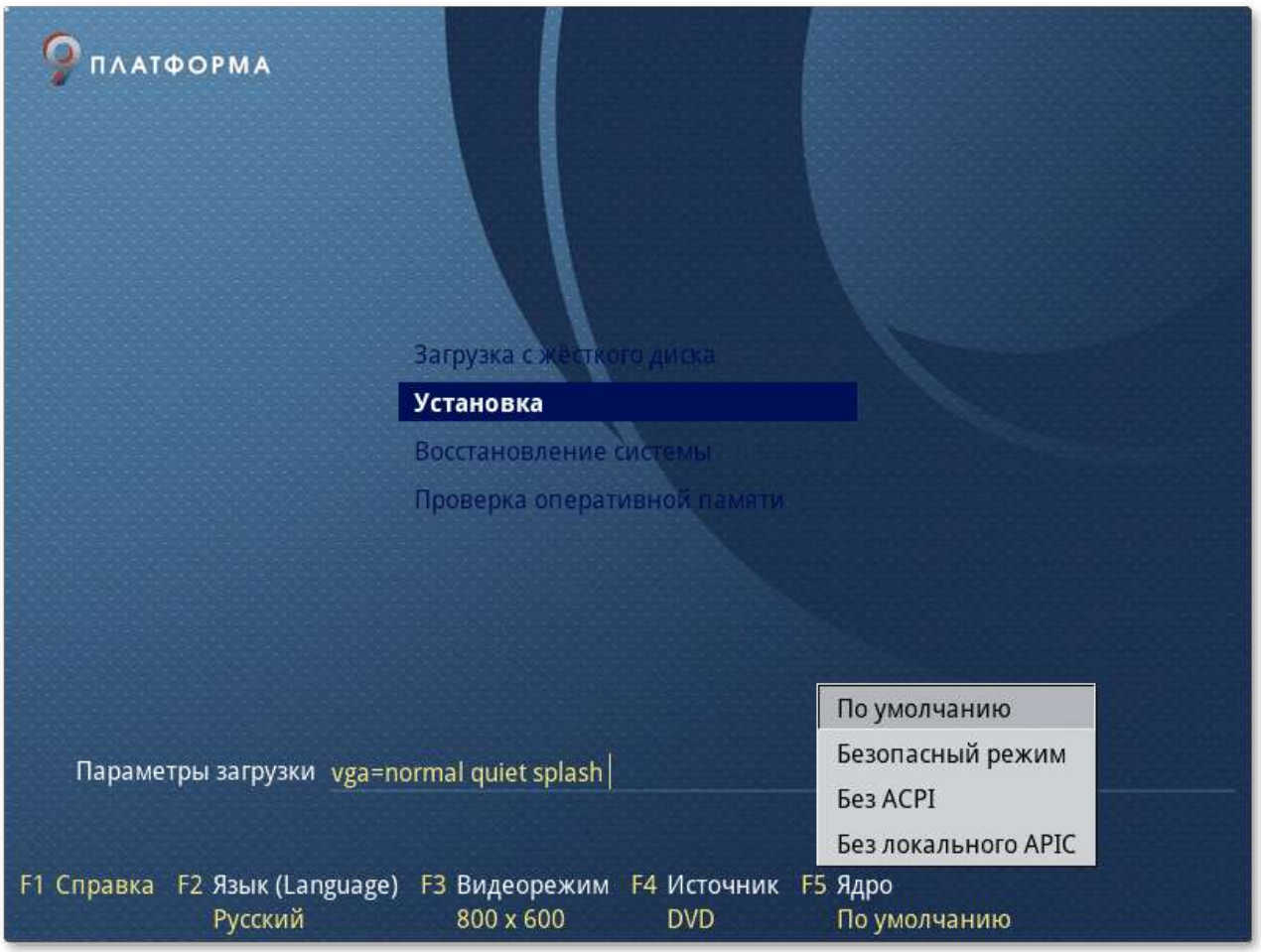
Если в системе не произошла настройка какого-либо компонента после стадии установки пакетов, не отчаивайтесь, доведите установку до конца, загрузитесь в систему и попытайтесь в спокойной обстановке повторить настройку.

В случае возникновения проблем с установкой, вы можете вручную задать необходимые параметры в строке **Параметры загрузки** меню начального загрузчика:

- ***xdriver*** — графический установщик предпринимает попытку автоматического подбора драйвера видеокарты, но иногда это ему не удаётся. Данным параметром можно отключить «искусственный интеллект» и явно указать нужный вариант драйвера;

- ***instdebug*** — если будет присутствовать этот параметр, то перед запуском и после завершения работы графического установщика будет запущена оболочка shell. Это очень полезное средство для выявления причин отсутствия запуска графической части программы установки. Последовательность работы внутренних сценариев следующая: **`install2`** → **`xinit`** → **`alterator-install2`** → **`alterator-wizard`**. При необходимости можно вручную загрузить Xorg (команда **`xinit`**) и в открывшемся окне терминала запустить **`alterator-install2`** (или **`alterator-wizard`**) вручную.

Если вы вообще не смогли установить систему (не произошла или не завершилась стадия установки пакетов), то сначала попробуйте повторить попытку в режиме **Установка в безопасном режиме**. В безопасном режиме отключаются все параметры ядра, (apm=off acpi=off mce=off barrier=off vga=normal) которые могут вызвать проблемы при загрузке. В этом режиме установка будет произведена без поддержки APIC. Возможно, у вас какое-то новое или нестандартное оборудование, но может оказаться, что оно отлично настраивается со старыми драйверами.



Если вы хотите получить точный ответ, то сообщите, пожалуйста, подробный состав вашего оборудования и подробное описание возникшей проблемы.

23.2. Проблемы с загрузкой системы

Если не загружается ни одна из установленных операционных систем, то значит, есть проблема в начальном загрузчике. Такие проблемы могут возникнуть после установки системы, в случае если загрузчик все-таки не установлен или установлен с ошибкой. При установке или переустановке Windows на вашем компьютере загрузчик Linux будет перезаписан в принудительном порядке, и станет невозможно запускать Linux.

Повреждение или перезапись загрузчика никак не затрагивает остальные данные на жёстком диске, поэтому в такой ситуации очень легко вернуть работоспособность: для этого достаточно восстановить загрузчик.

Если у вас исчез загрузчик другой операционной системы или другого производителя, то внимательно почитайте соответствующее официальное руководство на предмет его восстановления. Но в большинстве случаев вам это не потребуется, так как загрузчик, входящий в состав Альт Сервер, поддерживает загрузку большинства известных операционных систем.

Для восстановления загрузчика достаточно любым доступным способом загрузить Linux и получить доступ к тому жёсткому диску, на котором находится повреждённый загрузчик. Для этого проще всего воспользоваться *восстановительным режимом*, который предусмотрен на установочном диске дистрибутива (пункт **Восстановление системы**).

Загрузка восстановительного режима заканчивается приглашением командной строки: **`[root@localhost /]#`** . Начиная с этого момента, система готова к вводу команд.

В большинстве случаев для восстановления загрузчика можно просто воспользоваться командой **`fixmbr`** без параметров. Программа попытается переустановить загрузчик в автоматическом режиме.

23.3. Полезные ссылки

Если у вас что-то не получается, вы всегда можете поискать решение на ресурсах указанных в разделе Техническая поддержка продуктов «Базальт СПО».

Часть III. Начало использования Альт Сервер

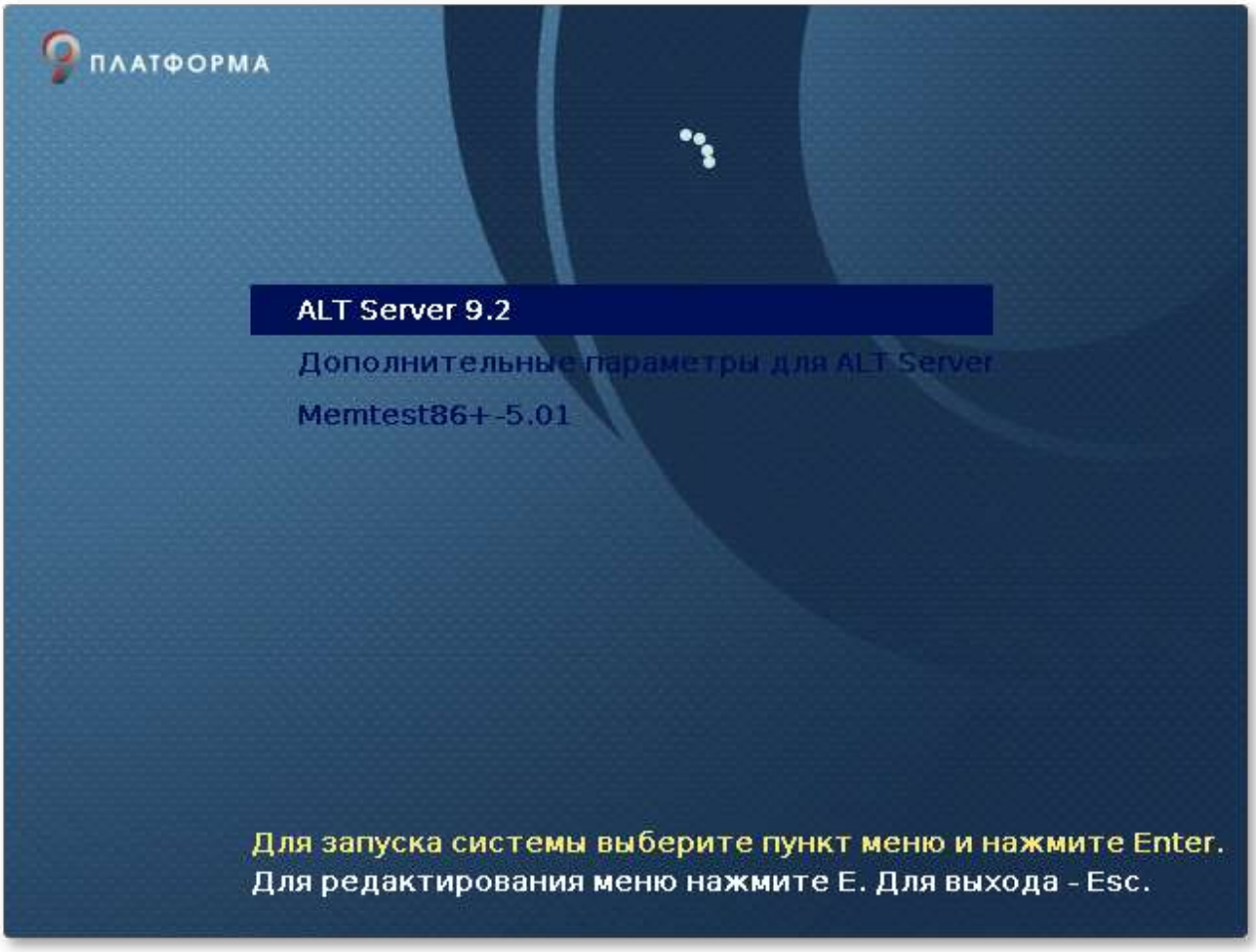
В этой части рассматривается загрузка установленной операционной системы и вход в среду рабочего стола.

Содержание

Глава 24. Загрузка системы

Запуск Альт Сервер выполняется автоматически после запуска компьютера и отработки набора программ BIOS.

На экране появляется меню, в котором перечислены возможные варианты загрузки операционной системы.



Важно

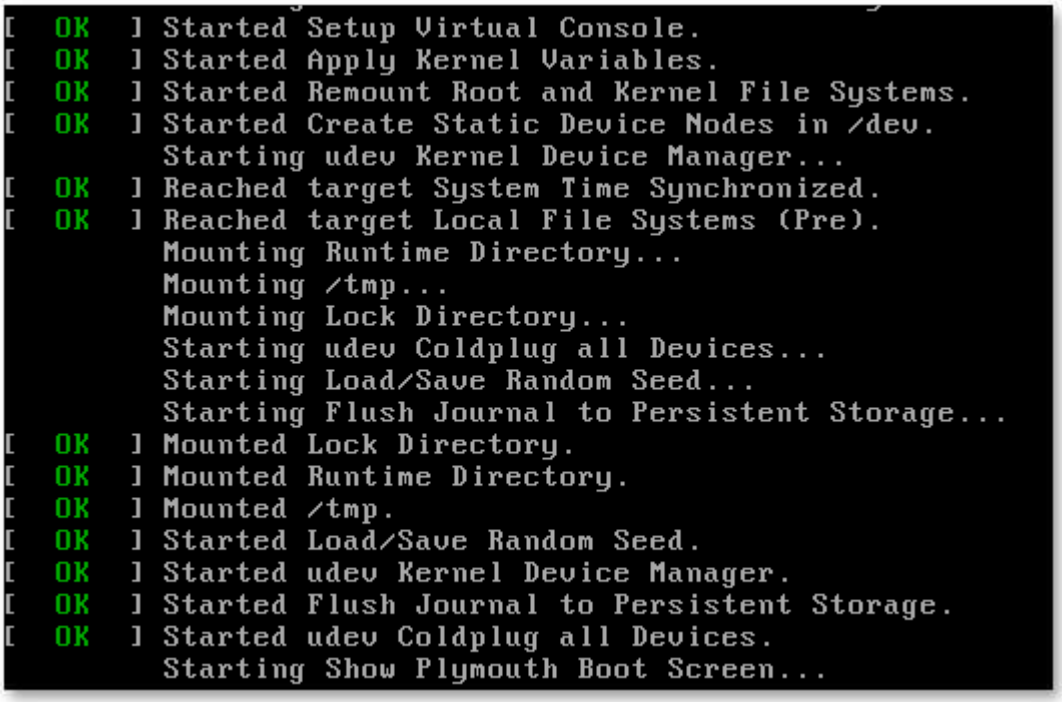
При первом старте, в условиях установки нескольких ОС на один компьютер, возможно отсутствие в загрузочном меню пункта/пунктов с другой/другими операционными системами, они будут добавлены в список при последующей перезагрузке. Все перечисленные в меню после перезагрузки варианты могут быть загружены загрузчиком Linux.

Стрелками клавиатуры **Вверх** и **Вниз** выберите нужную операционную систему. Дополнительно к основным вариантам запуска ОС из этого меню можно загрузить Linux в безопасном режиме или запустить проверку памяти.

Загрузка операционной системы по умолчанию (первая в списке) начинается автоматически после небольшого времени ожидания (обычно несколько секунд). Нажав клавишу **Enter**, можно начать загрузку немедленно.

Нажатием клавиши **E** можно вызвать редактор параметров текущего пункта загрузки. Если система настроена правильно, то редактировать их нет необходимости.

В процессе загрузки Альт Сервер пользователь может следить за информацией процесса загрузки, которая отображает этапы запуска различных служб и программных серверов в виде отдельных строк, на экране монитора.



При этом каждая строка начинается словом вида *[XXXXXXX]* (FAILED или OK), являющегося признаком нормального или ненормального завершения этапа загрузки. Слово *XXXXXXX=FAILED* (авария) свидетельствует о неуспешном завершении этапа загрузки, что требует вмешательства и специальных действий администратора системы.

Загрузка операционной системы может занять некоторое время, в зависимости от производительности компьютера. Основные этапы загрузки операционной системы — загрузка ядра, подключение (монтирование) файловых систем, запуск системных служб — периодически могут дополняться проверкой файловых систем на наличие ошибок. В этом случае время ожидания может быть занять больше времени, чем обычно. Подробную информацию о шагах загрузки можно получить, нажав клавишу **Esc**.

Глава 25. Получение доступа к зашифрованным разделам

В случае, если вы создали шифрованный раздел, вам потребуется вводить пароль при обращении к этому разделу.

Например, если был зашифрован домашний раздел **/home**, то для того, чтобы войти в систему под своим именем пользователя, вам потребуется ввести пароль этого раздела и затем нажать **Enter**.

Важно

Если не ввести пароль за отведенный промежуток времени, то загрузка системы завершится ошибкой. В этом случае вам следует перезагрузить систему, нажав для этого два раза **Enter**, а затем клавиши **Ctrl**+**Alt**+**Delete**.

Глава 26. Вход в систему

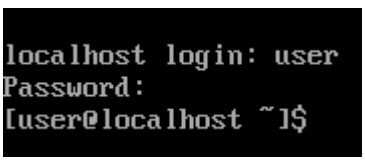
26.1. Вход и работа в консольном режиме

Стандартная установка Альт Сервер включает базовую систему, работающую в консольном режиме.

При загрузке в консольном режиме работа загрузчика Альт Сервер завершается запросом на ввод логина и пароля учетной записи. В случае необходимости на другую консоль можно перейти, нажав **Ctrl**+**Alt**+**F2**.

Для дальнейшего входа в систему необходимо ввести логин и пароль учетной записи пользователя.

В случае успешного прохождения процедуры аутентификации и идентификации будет выполнен вход в систему. ОС Альт Сервер перейдет к штатному режиму работы и предоставит дальнейший доступ к консоли.



26.2. Виртуальная консоль

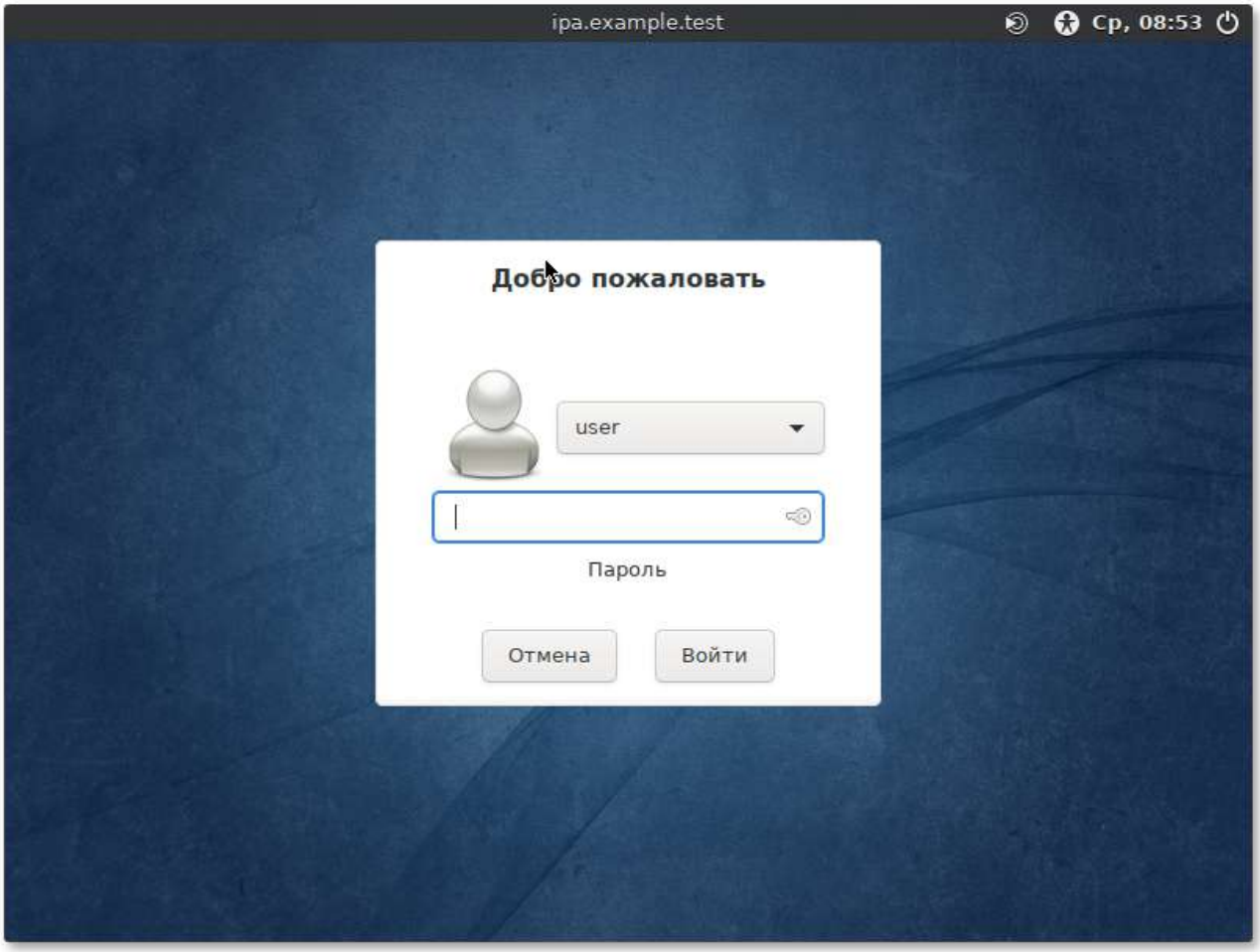
В процессе работы ОС Альт Сервер активно несколько виртуальных консолей. Каждая виртуальная консоль доступна по одновременному нажатию клавиш **Ctrl**, **Alt** и функциональной клавиши с номером этой консоли от **F1** до **F6**.

На первых шести виртуальных консолях (от **Ctrl**+**Alt**+**F1** до **Ctrl**+**Alt**+**F6**) пользователь может зарегистрироваться и работать в текстовом режиме. Двенадцатая виртуальная консоль (**Ctrl**+**Alt**+**F12**) выполняет функцию системной консоли – на нее выводятся сообщения о происходящих в системе событиях.

26.3. Вход и работа в системе в графическом режиме

В состав ОС Альт Сервер также может входить графическая оболочка MATE. Графическая оболочка состоит из набора различных программ и технологий, используемых для управления ОС и предоставляющих пользователю удобный графический интерфейс для работы в виде графических оболочек и оконных менеджеров.

При загрузке в графическом режиме работа загрузчика ОС заканчивается переходом к окну входа в систему.



Для регистрации в системе необходимо выбрать имя пользователя из выпадающего списка. Далее необходимо ввести пароль, затем нажать **Enter** или щелкнуть на кнопке **Войти**. После непродолжительного времени ожидания запустится графическая оболочка операционной системы.

Добавлять новых пользователей или удалять существующих можно после загрузки системы с помощью стандартных средств управления пользователями.

Если систему устанавливали не вы, то имя *системного пользователя* и его *пароль* вам должен сообщить системный администратор, отвечающий за настройку данного компьютера.

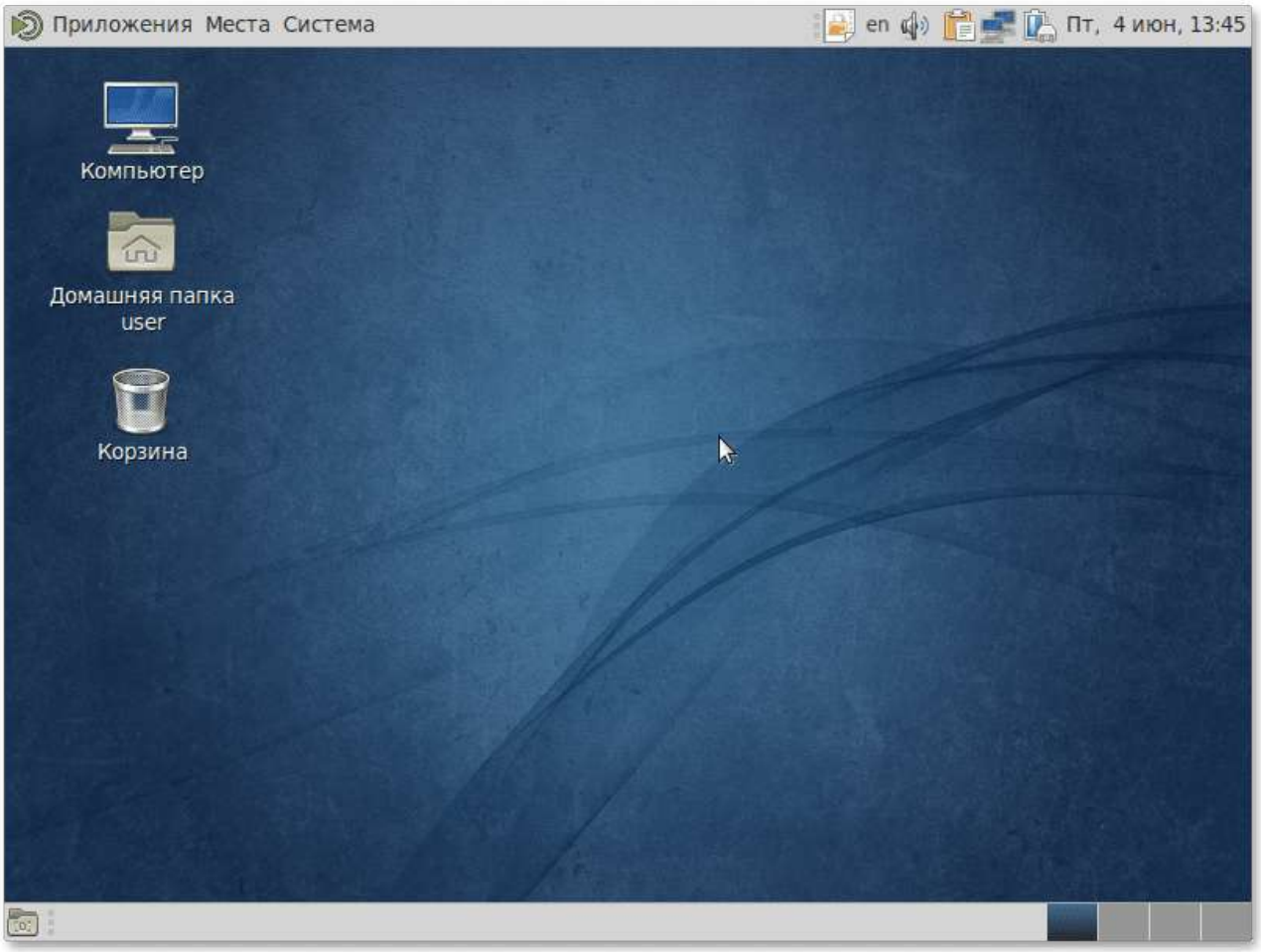
Важно

Поскольку работа в системе с использованием учётной записи *администратора системы* небезопасна, вход в систему в графическом режиме для суперпользователя root запрещён. Попытка зарегистрироваться в системе будет прервана сообщением об ошибке.

Часть IV. Рабочий стол MATE

Содержание

Глава 27. Рабочий стол MATE



На рабочем столе MATE есть три особые области. Сверху вниз:

- верхняя панель (серая полоса вверху экрана);
- область рабочего стола (рабочая площадь в центре, занимающая большую часть экрана);
- панель со списком окон (серая полоса внизу экрана).

27.1. MATE: Верхняя панель

Данная панель расположена в верхней области экрана. Левая часть панели содержит:

- меню **Приложения**;
- меню **Места**;
- меню **Система**.

Правая часть панели содержит:

- область уведомлений;
- регулятор громкости и апплет настройки звука;
- приложение «Сетевые соединения»;
- часы и календарь;

- параметры клавиатуры;
- параметры управления питанием.

Примечание

Если вы остановите указатель мыши на меню или на значке, то появится короткое описание.

27.2. MATE: Меню Приложения

Меню **Приложения** содержит список установленных приложений. Этот список обновляется при установке или удалении программ. При нажатии на **Приложения** открывается список, состоящий из следующих разделов:

- **Аудио и видео**;
- **Графика**;
- **Интернет**;
- **Офис**;
- **Системные**;
- **Стандартные**.

27.3. MATE: Меню Места

Это меню разделено на четыре подраздела. Щелчок по любому пункту в меню **Места** открывает файловый менеджер Caja. Для вызова руководства Caja нажмите: меню **Помощь** → **Содержание**.

Первый подраздел:

- **Домашний каталог** — в этой папке по умолчанию хранятся личные файлы пользователя.
- **Рабочий стол** — папка внутри «Домашней папки», содержащая файлы и папки, отображаемые на рабочем столе.
- Дальнейшие пункты соответствуют закладкам пользователя в файловом менеджере Caja.

Второй подраздел:

- **Компьютер** — позволяет увидеть все файлы в компьютере и файлы на подключённых внешних носителях.
- **Устройство CD/DVD** — позволяет получить доступ к CD/DVD дисководу.

Третий подраздел:

- **Сеть** — позволяет просматривать сетевые подключения компьютера. Осуществляет получение доступа к файлам и другим ресурсам, доступным в этих сетях.

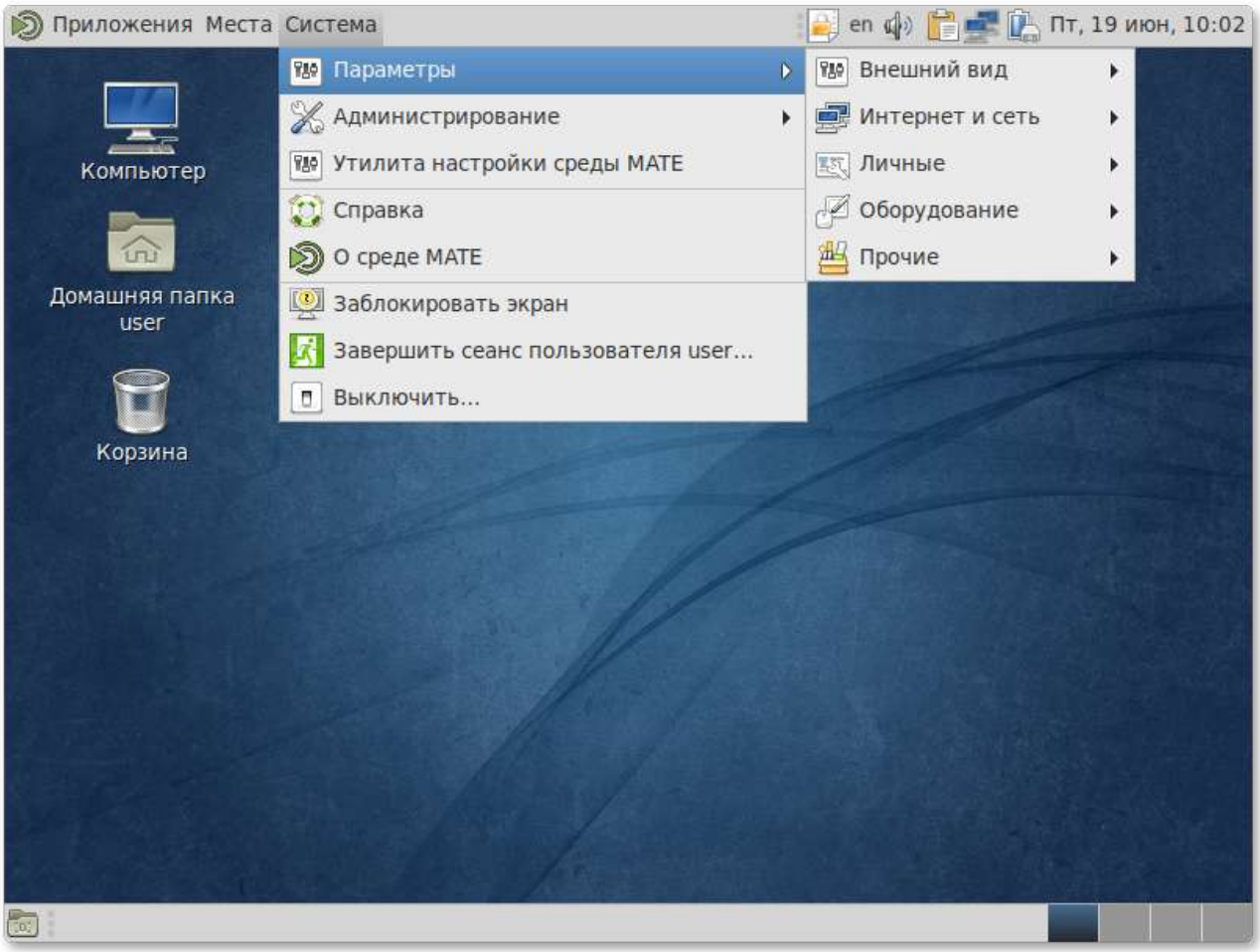
- **Соединиться с сервером...** — позволяет создать подключение к публичным или локальным сетям.

Четвёртый подраздел:

- **Средство поиска MATE** — позволяет быстро найти файлы, хранящиеся на компьютере.
- **Недавние документы** — содержит список последних документов, с которыми работал пользователь. Последний пункт этого подменю позволяет очистить список.

27.4. MATE: Меню Система

С помощью меню **Система** осуществляется доступ к настройкам MATE, справочной информации и функциям запуска, перезагрузки и отключения компьютера. Это меню разделено на три подраздела.



Первый подраздел содержит следующие пункты:

- **Параметры** содержит доступ к различным настройкам и предоставляет доступ к инструментам администрирования системы. В меню **Параметры** входят следующие настройки:
  - **Внешний вид**:
    - **Внешний вид** позволяет настроить внешний вид рабочего стола, включая фоновую картинку;

- **Всплывающие уведомления** позволяет настроить стиль и позицию уведомлений;
- **Главное меню** позволяет изменять список отображаемых элементов в меню **Приложений** и меню **Настроек**;
- **Менеджер настройки Compiz** утилита настройки окружения;
- **Окна** позволяет настроить параметры поведения окон;
- **Хранитель экрана** позволяет настроить заставку для рабочего стола;

- **Интернет и сеть**:
  - **Расширенная конфигурация сети** отображает сетевые подключения компьютера и позволяет их настраивать;
  - **Сетевая прокси-служба** позволяет настроить прокси-сервер;
- **Личные**:
  - **Вспомогательные технологии** дают возможность выбирать программы для увеличения частей экрана или для прочтения содержимого экранов;
  - **Запускаемые приложения** позволяют выбрать приложения для автоматического запуска при входе;
  - **Обо мне** хранит ту информацию о пользователе, которую он может передать другим людям в виде электронной визитки;
  - **Предпочтительные приложения** дают возможность выбрать, какие приложения необходимо использовать для конкретных задач;
  - **Управление файлами** влияет на предоставление пользователю файлов и папок;
- **Оборудование**:
  - **Bluetooth** позволяет настраивать Bluetooth-устройства для работы с компьютером;
  - **Звук** открывает диалоговое окно настройки звука (громкость звука, звуковые события, оборудование);
  - **Клавиатура** запускает диалог настройки клавиатуры. Тут же можно задать используемые в системе раскладки клавиатуры;
  - **Комбинации клавиш клавиатуры** задают сочетания клавиш для выполнения определённых заданий в окружении рабочего стола;
  - **Мышь** позволяет настроить кнопки и другие параметры мыши;
  - **Управление питанием** настраивает компьютер на работу с различными параметрами энергосбережения;
  - **Экраны** задаёт разрешение и другие параметры монитора.

- **Прочие**:
  - **Менеджер пакетов** позволяет управлять пакетами. С помощью Synaptic можно управлять источниками пакетов (репозиториями), получать сведения об доступных пакетах, устанавливать/удалять/обновлять пакеты, производить поиск по ключевым словам среди доступных пакетов;

- **Администрирование** позволяет получить доступ к следующим настройкам:
  - **Параметры печати** позволяет настроить принтеры и задать параметры печати.
  - **Установка RPM** позволяет установить RPM пакеты.
  - **Центр управления системой** позволяет управлять наиболее востребованными настройками системы: пользователями, сетевыми подключениями, настройками даты/времени и т. п.
- **Утилита настройки среды MATE**.

Второй подраздел включает пункты:

- **Справка** предоставляет доступ к руководству пользователя рабочей среды MATE.
- **О среде MATE** показывает информацию об установленной среде MATE.

Третий подраздел включает пункты:

- **Заблокировать экран** служит для запуска хранителя экрана. Для возобновления работы после блокировки необходим ввод пароля.
- **Завершить сеанс пользователя...** необходим для завершения работы пользователя без выключения компьютера.
- **Выключить...** позволяет перезагрузить либо выключить компьютер.

Предупреждение

Если ваш компьютер запрашивает пароль администратора (root), то это значит, что будут производиться важные системные настройки. Будьте предельно внимательны к выводимым сообщениям.

27.5. MATE: Область рабочего стола

Область рабочего стола включает в себя три значка:

- **Компьютер** — предоставляет доступ к устройствам хранения данных.
- **Домашняя папка пользователя** — предоставляет доступ к домашнему каталогу пользователя **`/home/<имя пользователя>`**. В этой папке по умолчанию хранятся пользовательские файлы (например, аудиозаписи, видеозаписи, документы). У каждого пользователя свой «Домашний» каталог. Каждый пользователь имеет доступ только в свой «Домашний» каталог.

- **Корзина** — доступ к «удаленным файлам». Обычно, при удалении файла, он не удаляется из системы. Вместо этого он помещается в «Корзину». С помощью этого значка можно просмотреть или восстановить «удаленные файлы». Чтобы удалить файл из системы, нужно очистить «Корзину». Чтобы очистить «Корзину», необходимо щелкнуть правой кнопкой мыши по значку **Корзина** и выбрать в контекстном меню пункт **Очистить корзину**.

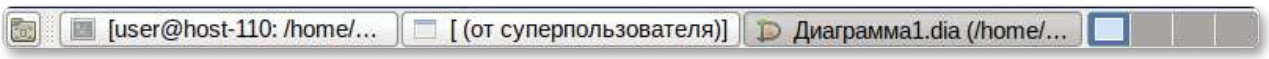
Примечание

Можно сразу удалить файл из системы, минуя корзину. Для этого необходимо одновременно с удалением файла зажать клавишу **Shift**.

На область рабочего стола можно перетащить файлы и создать ярлыки программ с помощью меню правой кнопки мыши.

Щелчок правой кнопкой мыши на свободной области рабочего стола открывает контекстное меню рабочего стола, где можно, например, настроить фон рабочего стола (пункт **Параметры внешнего вида**).

27.6. MATE: Панель со списком окон



У этой панели три основных компонента:

- Любые открытые приложения отображаются как кнопки в средней части окна. Тут отображаются все окна с области рабочего стола вне зависимости от того, видно окно или нет. Кнопка скрытого окна будет отображаться с белым фоном. Кнопка приложения, которое выбрано в данный момент, будет с серым фоном. Что бы переключаться между приложениями с помощью мыши, кликните по желаемому приложению левой кнопкой мыши, чтобы переключиться на него.

Примечание

Используйте комбинацию клавиш **Alt**+**Tab** для переключения между открытыми окнами.

Удерживая нажатой клавишу **Alt**, нажимайте **Tab** для последовательного переключения между окнами. Отпустите обе клавиши, чтобы подтвердить свой выбор.

- 

Переключатель рабочих мест — это группа квадратов в правом нижнем углу экрана. Они позволяют вам переключать рабочие места. Каждое рабочее место предоставляет отдельный рабочий стол, на котором можно расположить приложения. По умолчанию активно 4 рабочих места. Можно изменить это число, нажав правой кнопкой мышки на **переключателе рабочих мест** и выбрав пункт **Параметры**.

Примечание

Для переключения между рабочими столами необходимо использовать комбинацию клавиш **Ctrl+Alt+стрелка влево** или **Ctrl+Alt+стрелка вправо**

- 

  Свернуть все окна — кнопка позволяет свернуть (развернуть) все открытые окна на текущем рабочем месте.

Часть V. Настройка системы

Содержание

Глава 28. Центр управления системой

28.1. Описание

Для управления настройками установленной системы вы можете воспользоваться **Центром управления системой**. **Центр управления системой** (ЦУС) представляет собой удобный интерфейс для выполнения наиболее востребованных административных задач: добавление и удаление пользователей, настройка сетевых подключений, просмотр информации о состоянии системы и т.п.

ЦУС включает также веб-ориентированный интерфейс, позволяющий управлять сервером с любого компьютера сети.

Центр управления системой состоит из нескольких независимых диалогов-модулей. Каждый модуль отвечает за настройку определённой функции или свойства системы.

28.2. Применение центра управления системой

Вы можете использовать ЦУС для разных целей, например:

- Настройки **Даты и времени** (datetime);
- Управления выключением и перезагрузкой компьютера (ahttpd-power, доступно только в веб-интерфейсе);

- Настройки **Аутентификации** (auth);
- Управления **Системными службами** (services);
- Просмотра **Системных журналов** (logs);
- Настройки **OpenVPN-подключений** (openvpn-server и net-openvpn);
- Конфигурирования **Сетевых интерфейсов** (net-eth);
- Изменения пароля **Администратора системы (root)** (root);
- Создания, удаления и редактирования учётных записей **Пользователей** (users);
- Настройки ограничения **Использования диска (квоты)** (quota).

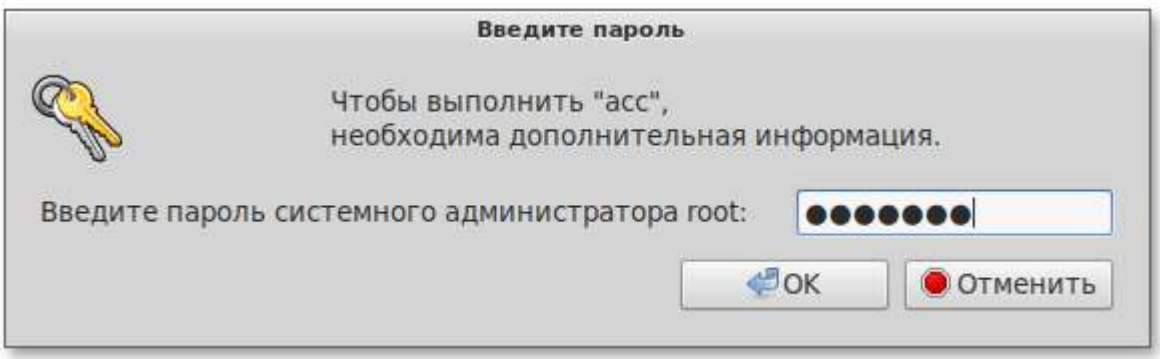
Вы всегда можете воспользоваться кнопкой **Справка**. Все модули ЦУС имеют справочную информацию.

28.3. Запуск центра управления системой в графической среде

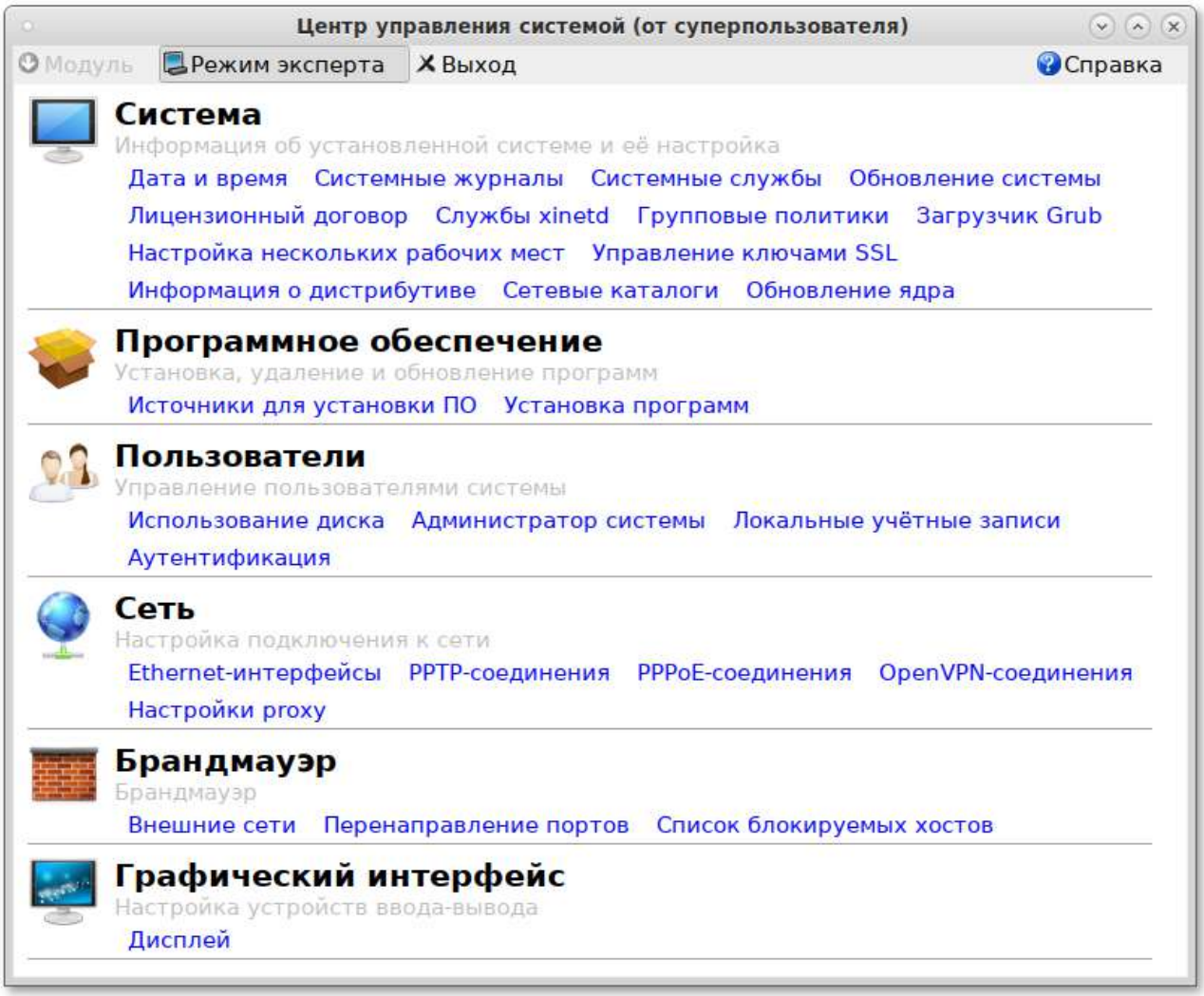
Центр управления системой можно запустить следующими способами:

- в графической среде MATE: **Система → Администрирование → Центр управления системой**;
- из командной строки: командой **acc**.

При запуске необходимо ввести пароль администратора системы (root).



После успешного входа можно приступать к настройке системы.



Кнопка **Режим эксперта** позволяет выбрать один из режимов:

- основной режим (кнопка отжата);
- режим эксперта (кнопка нажата).

Выбор режима влияет на количество отображаемых модулей. В режиме эксперта отображаются все модули, а в основном режиме только наиболее используемые.

28.4. Использование веб-ориентированного центра управления системой

ЦУС имеет веб-ориентированный интерфейс, позволяющий управлять данным компьютером с любого другого компьютера сети.

Работа с ЦУС может происходить из любого веб-браузера. Для начала работы необходимо перейти по адресу **`https://ip-адрес:8080/`**.

Например, для сервера задан IP-адрес **`192.168.0.122`**. В таком случае:

- интерфейс управления будет доступен по адресу: **`https://192.168.0.122:8080/`**;
- документация по дистрибутиву будет доступна по адресу **`https://192.168.0.122/`**.

Примечание

IP-адрес сервера можно узнать, введя на сервере команду:

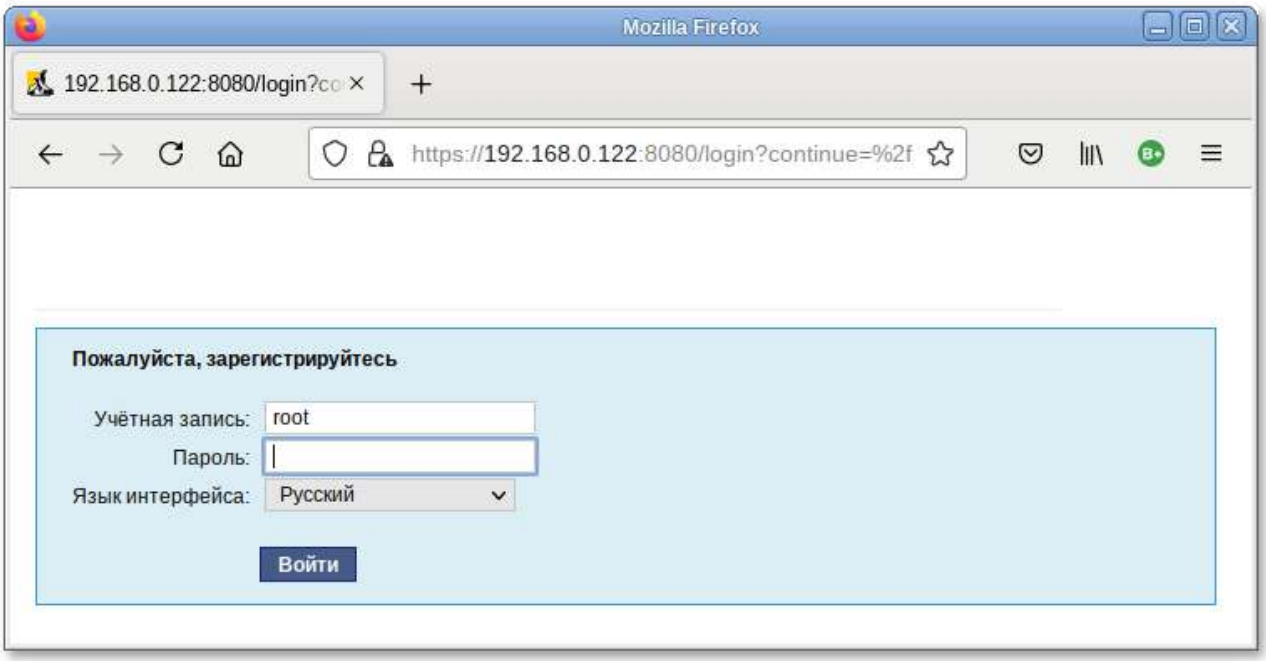
```
$ ip addr
```

IP-адрес будет указан после слова ***inet***:

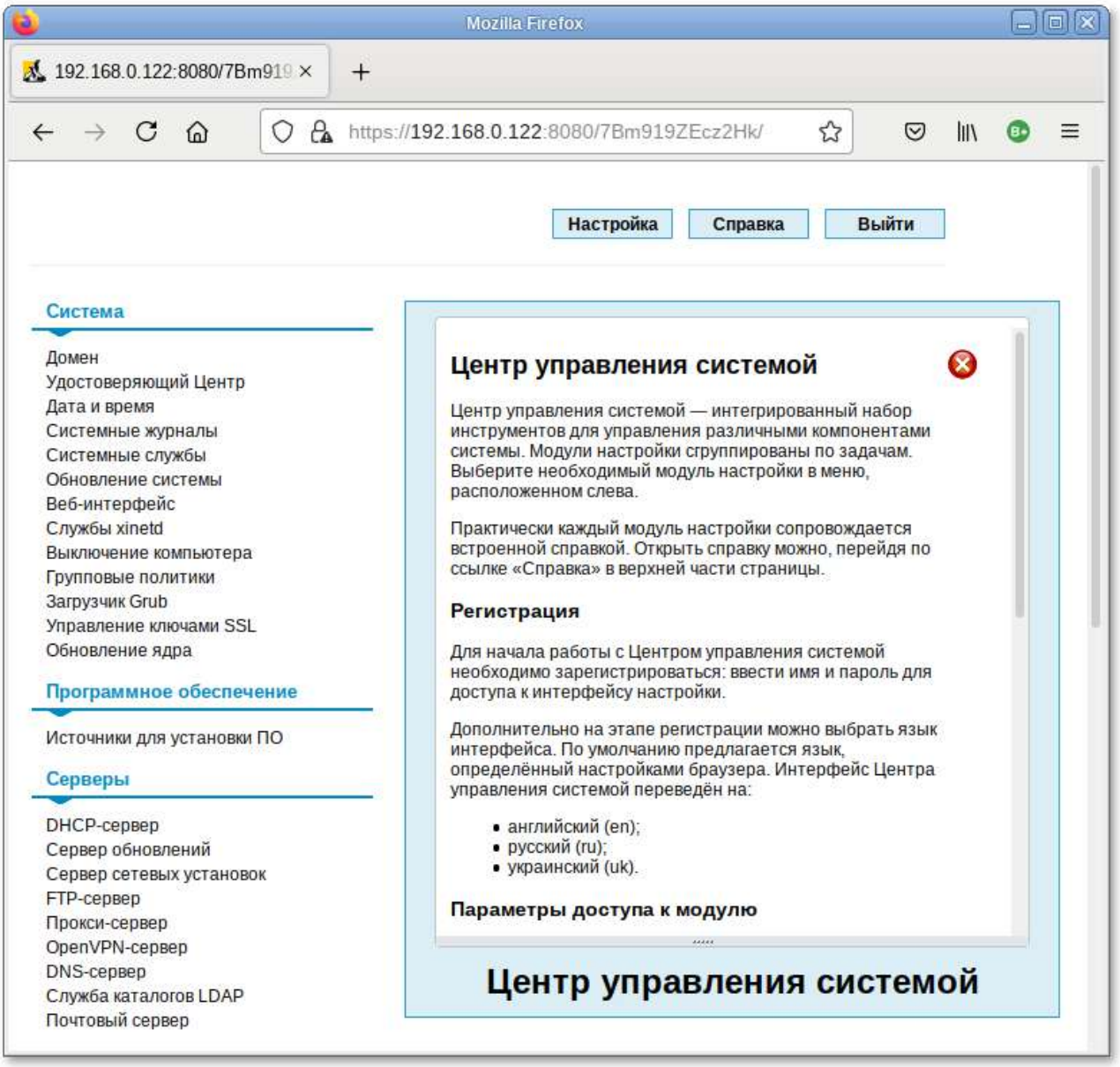
```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state
UP qlen 1000
    link/ether 60:eb:69:6c:ef:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.122/24 brd 192.168.0.255 scope global enp0s3
```

Например, тут мы видим, что на интерфейсе enp0s3 задан IP-адрес **192.168.0.122**.

При запуске центра управления системой необходимо ввести в соответствующие поля имя пользователя (**root**) и пароль пользователя:



После этого будут доступны все возможности ЦУС на той машине, к которой было произведено подключение через веб-интерфейс.



Примечание

Если в сети нет компьютера, который вы могли бы использовать для доступа к веб-ориентированному **Центру управления системой**, то вы можете воспользоваться браузером непосредственно на сервере. Для работы предустановленного браузера firefox следует запустить графическую оболочку. Для этого выполните команду **`startx`**, предварительно войдя в консоль сервера, используя имя и пароль созданного при установке непривилегированного пользователя.

Веб-интерфейс ЦУС можно настроить (кнопка **Режим эксперта**), выбрав один из режимов:

- основной режим;
- режим эксперта.

Выбор режима влияет на количество отображаемых модулей. В режиме эксперта отображаются все модули, а в основном режиме только наиболее используемые.

Центр управления системой содержит справочную информацию по всем включённым в него модулям. Об использовании самого интерфейса системы управления можно прочитать, нажав на кнопку **Справка** на начальной странице центра управления системой.

Центр управления системой содержит справочную информацию по всем включённым в него модулям. Об использовании самого интерфейса системы управления можно прочитать, нажав на кнопку **Справка** на начальной странице центра управления системой.

Предупреждение

После работы с центром управления системой, в целях безопасности, не оставляйте открытым браузер. Обязательно выйдите, нажав на кнопку **Выйти**.

Примечание

Подробнее об использовании **Центра управления системой** можно узнать в главе Организация сетевой инфраструктуры с помощью сервера.

Глава 29. Настройка сети

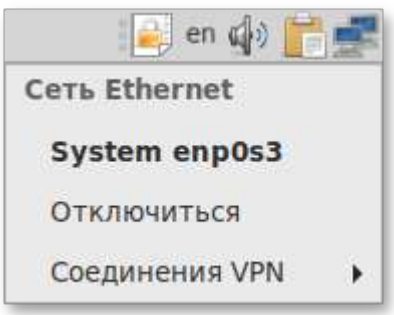
29.1. NetworkManager

Для управления настройками сети в Альт Сервер используется программа **NetworkManager**.

NetworkManager позволяет подключаться к различным типам сетей: проводные, беспроводные, мобильные, VPN и DSL, а также сохранять эти подключения для быстрого доступа к сети. Например, если вы подключались к сети в каком-либо интернет-кафе, то можно сохранить настройки этого подключения и в следующее посещение этого кафе подключиться автоматически.

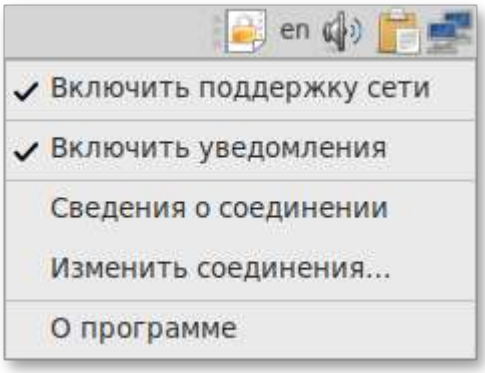
Значок **NetworkManager** располагается в системном лотке.

При нажатии левой кнопки мыши на значок **Управление сетью**, откроется меню, в котором показана информация о текущих соединениях. Здесь также можно выбрать одну из доступных Wi-Fi сетей и подключиться к ней, или отключить активное Wi-Fi соединение.



Примечание

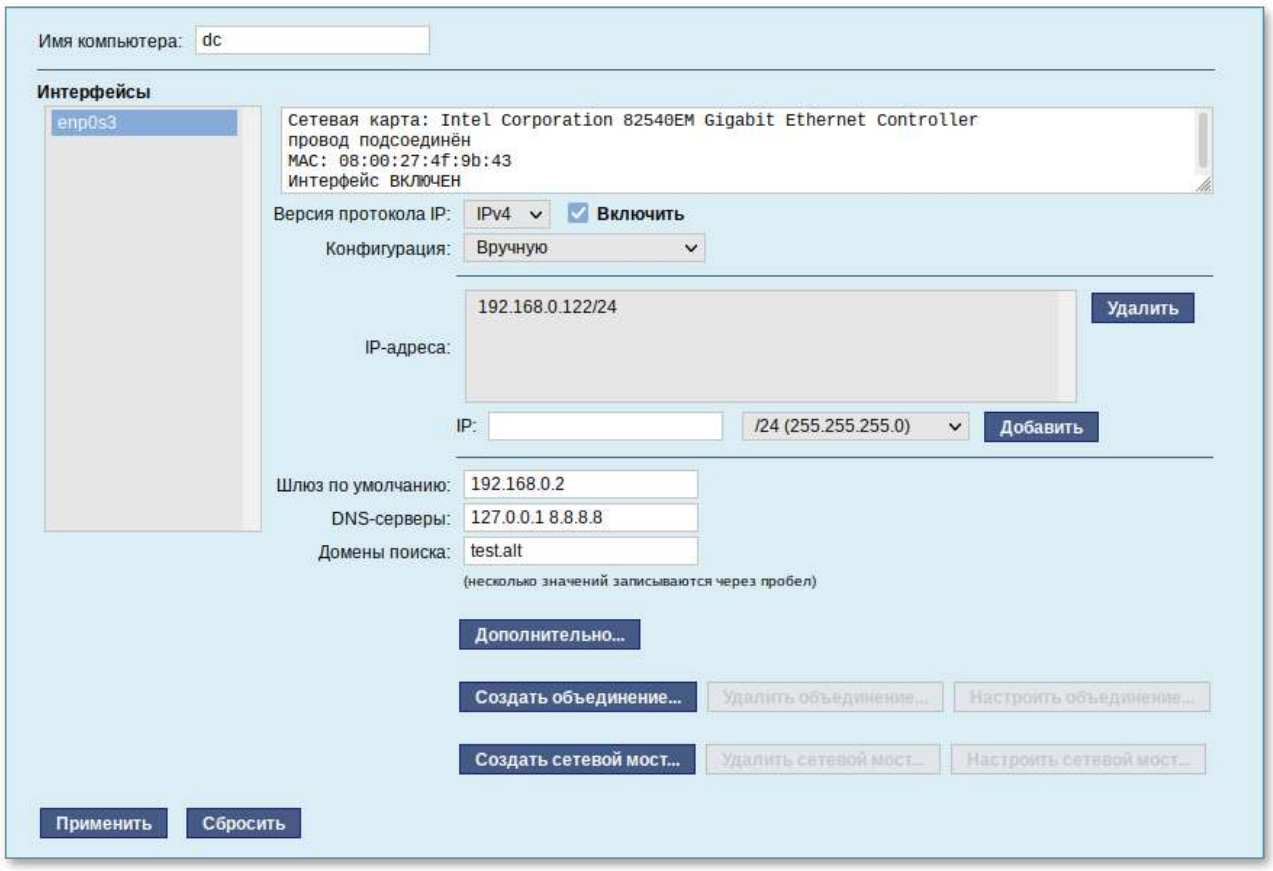
При подключении к беспроводной сети в первый раз может понадобиться указать некоторые сведения о защите сети (например, указать аутентификационные данные).



При нажатии правой кнопкой мыши на значок **NetworkManager**, появляется меню, из которого можно получить доступ к изменению некоторых настроек. Здесь можно посмотреть версию программы, получить сведения о соединении, изменить соединения (например, удалить Wi-Fi сеть, чтобы не подключаться к ней автоматически).

29.2. Настройка в ЦУС

Настройку сети можно выполнить в Центре управления системой в разделе **Сеть → Ethernet интерфейсы**. Здесь можно задать как глобальные параметры сети (адрес сервера DNS, имя компьютера), так и настройки конкретного сетевого интерфейса:



Подробнее о настройке сетевых интерфейсов в ЦУС рассказано в разделе Конфигурирование сетевых интерфейсов.

Часть VI. Установка дополнительного программного обеспечения

После установки Альт Сервер при первом запуске вам доступен тот или иной набор программного обеспечения. Количество предустановленных программ зависит от набора программ конкретного дистрибутива или от выбора, сделанного вами при установке системы. Если вы не обнаружили в своей системе интересующие вас программы, то вы имеете возможность доустановить их из разных источников.

Дополнительное программное обеспечение может находиться на установочном диске и/или в специальных банках программ (репозиториях), расположенных в сети Интернет и/или в локальной сети. Программы, размещённые в указанных источниках, имеют вид подготовленных для установки пакетов.

Содержание

Глава 30. Установка дополнительного ПО

30.1. Введение

Для установки дополнительного ПО вы можете использовать **Центр управления системой** либо программу управления пакетами **Synaptic**.

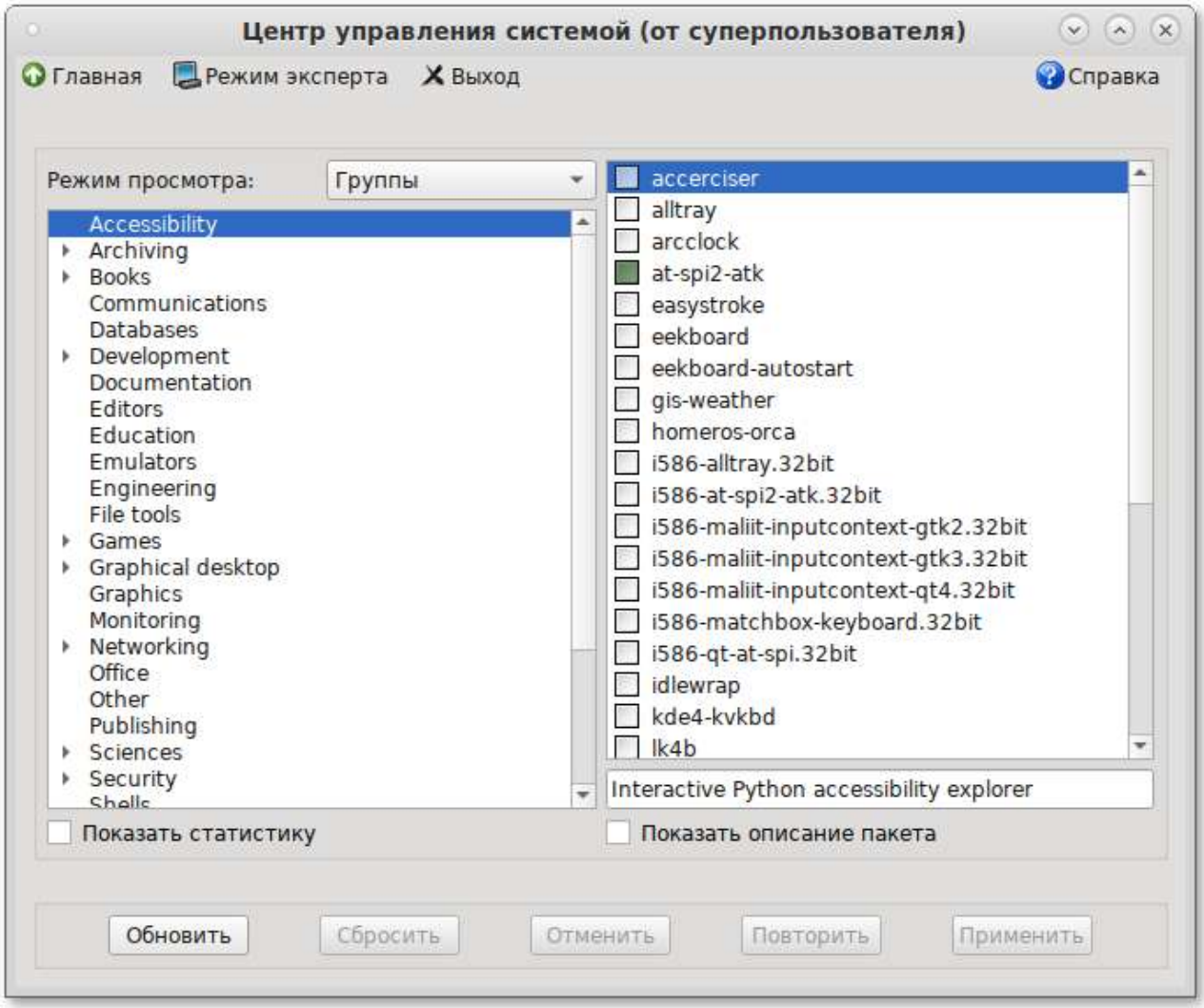
Предупреждение

Не используйте одновременно два менеджера пакетов, так как это может привести к их некорректной работе.

30.2. Установка дополнительного ПО в ЦУС

Центр управления системой содержит модуль установки дополнительных пакетов: **Программное обеспечение** → **Установка программ**. Для облегчения поиска доступные для установки программы разделены на группы, выводимые в левой части окна программы. Справа расположен список самих программ с указанием их текущего состояния:

- зелёная метка — пакет уже установлен;
- белая — пакет не установлен.



Объяснение всех обозначений можно увидеть, отметив пункт **Показать статистику**.

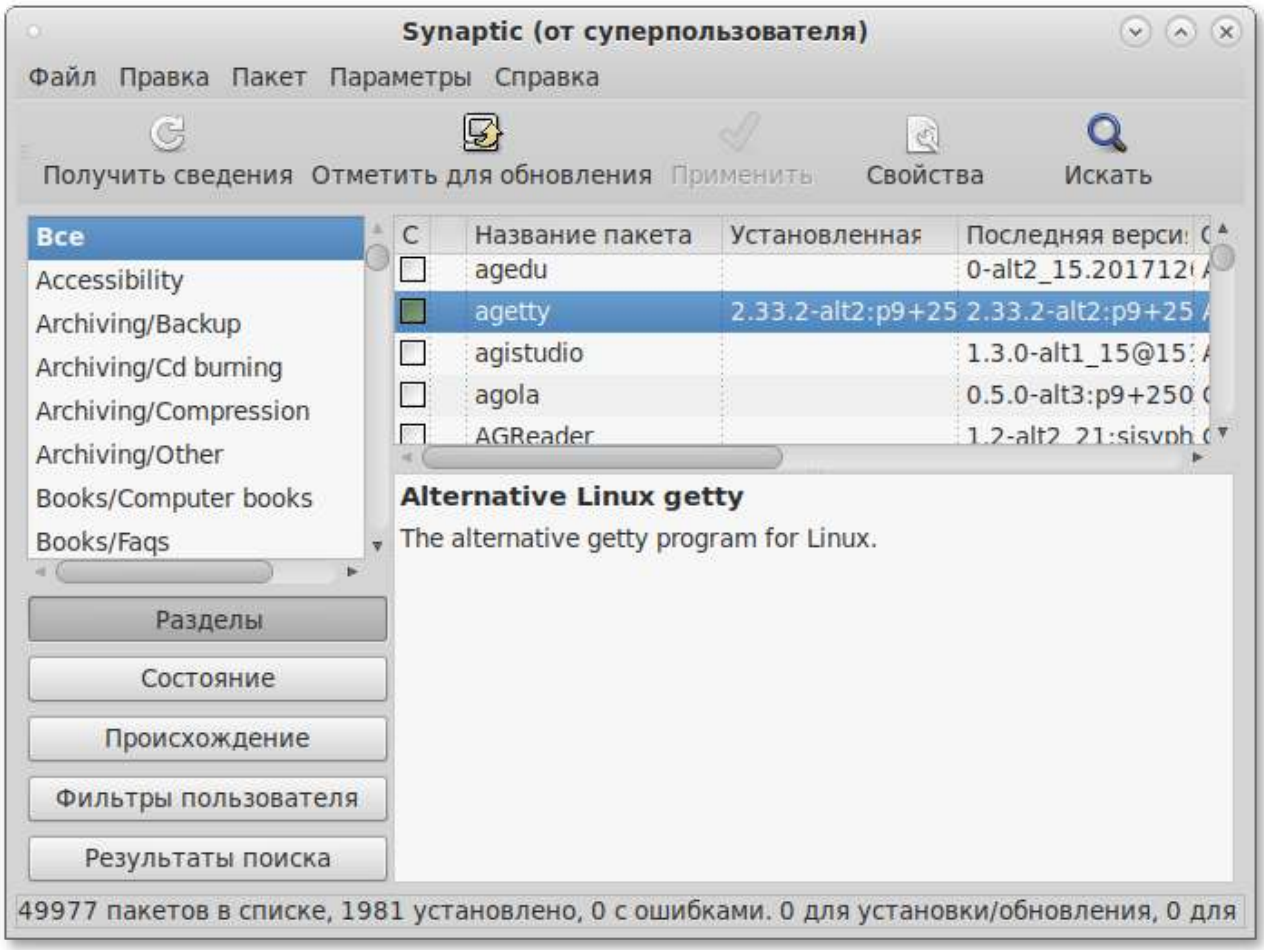
Для начала установки двойным щелчком мыши отметьте неустановленный пакет в правой половине окна и нажмите **Применить**. При необходимости менеджер пакетов попросит вставить установочный диск.

30.3. Программа управления пакетами Synaptic

Программа управления пакетами **Synaptic** находится в **Система** → **Параметры** → **Прочие** → **Менеджер пакетов**.

Для облегчения поиска доступные для установки программы разделены на группы, выводимые в левой части окна программы. Справа расположен список самих программ с указанием их текущего состояния:

- зелёная метка — пакет уже установлен;
- белая метка — пакет не установлен.



При выборе пакета из списка в нижней части отображаются сведения о нем и его описание.

Перед тем как устанавливать или обновлять пакет, необходимо нажать на кнопку **Получить сведения** (**Ctrl**+**R**), для того чтобы скачать список самых последних версий ПО.

Для начала установки двойным щелчком мыши отметьте неустановленный пакет в правой половине окна и нажмите **Применить**.

Глава 31. Добавление репозиториев

Эта информация может пригодиться вам для установки дополнительного программного обеспечения из внешних репозиториев.

31.1. Центр управления системой

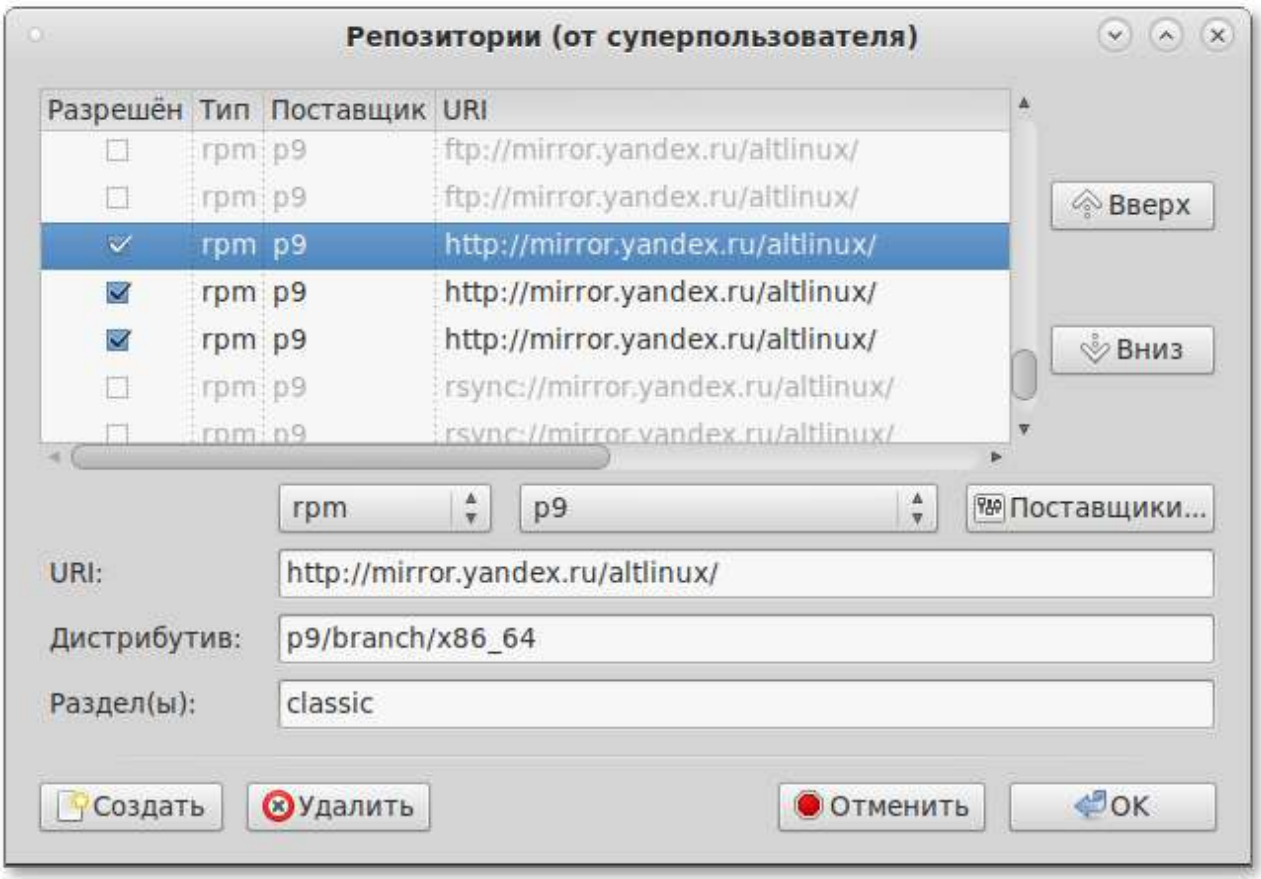
Для выбора репозитория, совместимого с вашим дистрибутивом, рекомендуем использовать **Центр управления системой** (меню **Программное обеспечение** → **Источники для установки ПО**). Для указания конкретного репозитория в выпадающем списке отметьте один из предлагаемых вариантов и нажмите кнопку **Изменить**. Если сомневаетесь, то выбирайте **`ftp://ftp.altlinux.org/`**. К предложенному списку вы можете самостоятельно добавить любые репозитории, нажав на кнопку **Дополнительно...**.

После добавления репозиториев обновите информацию о них: **Центр управления системой: Программное обеспечение** → **Установка программ** кнопка **Обновить**.

31.2. Программа управления пакетами Synaptic

Программа **Synaptic** также может использоваться для выбора репозитория, совместимого с вашим дистрибутивом. Для указания конкретного репозитория в меню **Параметры** → **Репозитории** отметьте один из предлагаемых вариантов и нажмите кнопку **OK**. Если вы сомневаетесь, то выбирайте строки, содержащие ftp://ftp.altlinux.org/. К предложенному списку вы можете самостоятельно добавить любые репозитории, нажав на кнопку **Создать** и введя необходимые данные.

После добавления репозиториев обновите информацию о них: программа управления пакетами **Synaptic**: **Правка** → **Получить сведения о пакетах**.



Важно

После выбора и добавления репозиториев необходимо получить сведения о находящихся в них пакетах. В противном случае список доступных для установки программ будет не актуален.

Непосредственная установка пакетов из добавленных репозиториев ничем не отличается от описанной выше в главе « Установка дополнительного ПО ».

Примечание

Есть и другие способы работы с репозиториями и пакетами. Некоторые из них описаны в « Установка пакетов для опытных пользователей »

Глава 32. Обновление всех установленных пакетов

32.1. Программа управления пакетами Synaptic

Synaptic поддерживает два варианта обновления системы:

Интеллектуальное обновление (рекомендуется)

Интеллектуальное обновление попытается разрешить конфликты пакетов перед обновлением системы. Действие интеллектуального обновления аналогично действию команды **apt-get dist-upgrade**.

Стандартное обновление

Стандартное обновление обновит только те пакеты, которые не требуют установки дополнительных зависимостей.

По умолчанию **Synaptic** использует интеллектуальное обновление. Для того чтобы изменить метод обновления системы, откройте диалоговое окно **Параметры** (**Параметры → Параметры**) и на вкладке **Основные** в списке **Обновить систему** выберите требуемый способ.

Для обновления системы необходимо:

1. Нажать кнопку **Получить сведения** (**Ctrl**+**R**), для того чтобы скачать список самых последних версий ПО.
2. Нажать кнопку **Отметить для обновления** (**Ctrl**+**G**), для того чтобы **Synaptic** отметил для обновления все пакеты.
3. Нажать кнопку **Применить**.

Примечание

Для обновления ядра ОС см. разделы «Обновление ядра ОС» и «Обновление ядра».

Часть VII. Серверные решения

Эта глава рассказывает о начале работы с установленным дистрибутивом и знакомит с основным способом настройки системы через **Центр управления системой** (далее — ЦУС).

Важно

Этот раздел рекомендуется читать опытным пользователям, и пользователям Альт Сервер (сервер).

Содержание

Глава 33. Вход в систему

Вы можете начать работу по настройке сервера сразу после установки системы, используя для настройки **Центр управления системой** — веб-ориентированный интерфейс, позволяющий управлять сервером с любого компьютера сети (Использование веб-ориентированного центра управления системой).

Глава 34. Развёртывание офисной ИТ-инфраструктуры

34.1. Подготовка

Перед началом развёртывания офисной ИТ-инфраструктуры необходимо провести детальное планирование. Конкретные решения в каждом случае будут продиктованы спецификой требований, предъявляемых к офисной ИТ-инфраструктуре. Как будет использоваться Альт Сервер в каждом конкретном случае решать вам. При этом важно понимать принципы взаимодействия компьютеров в сети и роль каждого конкретного компьютера: главный сервер, подчинённый сервер или компьютер-клиент (рабочее место).

Ключевым понятием для работы сети, построенной на базе Альт Сервер, является **домен**.

34.1.1. Домен

Под доменом понимается группа компьютеров с разными ролями. Каждый сервер обслуживает один домен — группу компьютеров одной сети, имеющую единый центр и использующую единые базы данных для различных сетевых служб.

С помощью **Домена** вы можете:

- вести централизованную базу пользователей и групп;
- аутентифицировать пользователей и предоставлять им доступ к сетевым службам без повторного ввода пароля;
- использовать единую базу пользователей для файлового сервера, прокси-сервера, веб-приложений (например, MediaWiki);
- автоматически подключать файловые ресурсы с серверов, анонсированных по Zeroconf;
- использовать тонкие клиенты, загружаемые по сети и использующие сетевые домашние каталоги;
- аутентифицировать пользователей как на «ALT-домен», так и на Microsoft Windows.

Основная документация по **Домену**:

- Что такое домен;
- Настройка и разворачивание домена.

Примечание

Не путайте это понятие с другими доменами: почтовыми доменами, доменными именами (DNS), Windows-доменами.

34.1.2. Сервер, рабочие места и аутентификация

Важно понимать роль, которая будет отводиться Альт Сервер в домене. Именно сервер под управлением Альт Сервер будет являться центральным звеном сети, контролируя доступ к ресурсам сети и предоставляя различные службы для клиентских машин. Все службы, предоставляемые серверами, используются рабочими местами.

Таким образом, можно выделить:

Сервер (компьютер под управлением Альт Сервер)

Сервер осуществляет контроль доступа к ресурсам сети, содержит централизованную базу данных пользователей и *удостоверяющий центр* для выдачи сертификатов службам на серверах и рабочих местах.

Рабочее место

Рабочие места — это клиентские, по отношению к серверам, компьютеры, непосредственно использующиеся для работы пользователей.

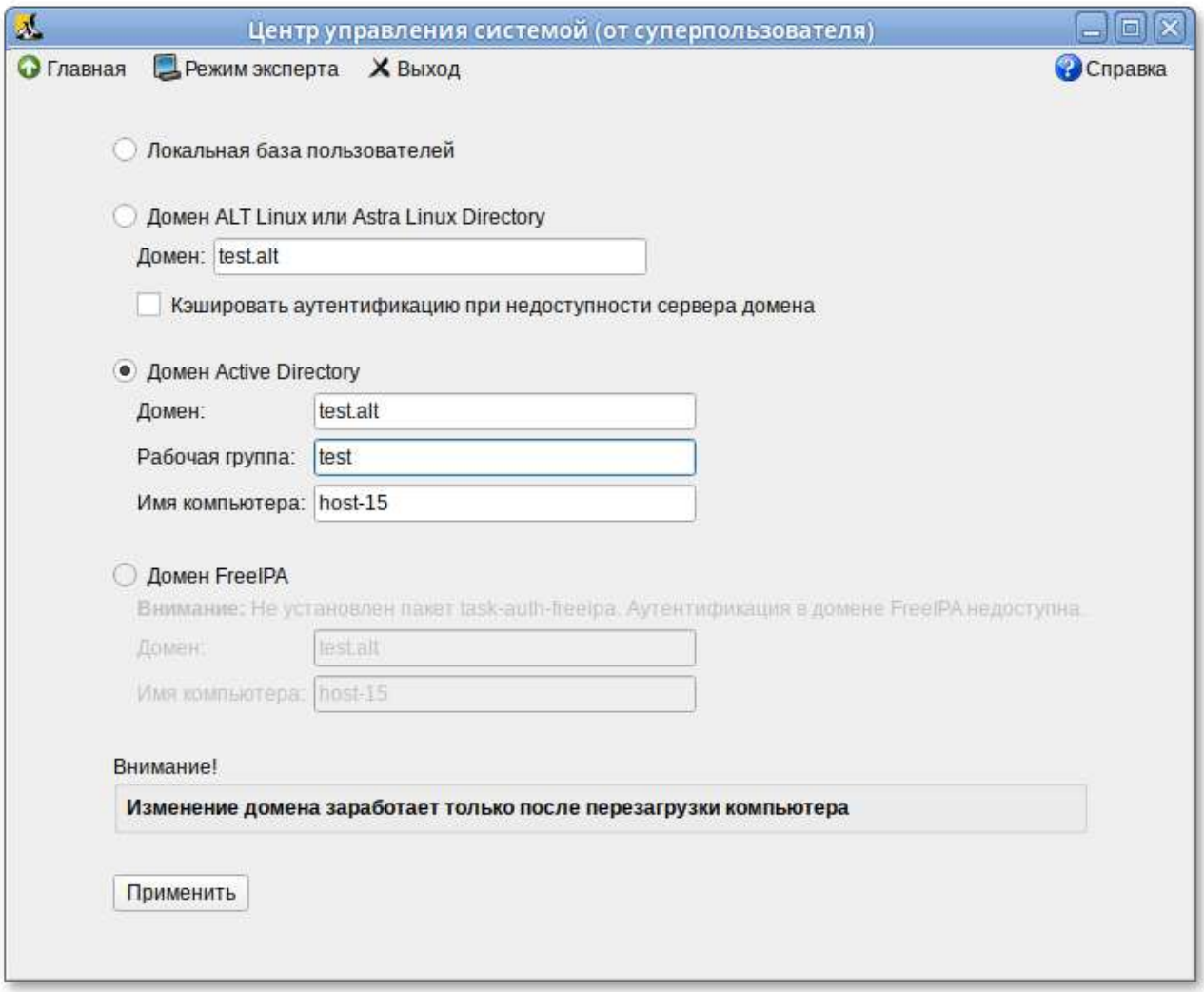
Альт Сервер может эффективно управлять гетерогенными сетями и бездисковыми клиентами. Для построения офисной инфраструктуры рекомендуется использовать вместе с продуктом Альт Рабочая станция как стабильное и надежное решение. Конечно, в качестве рабочих мест могут использоваться и другие операционные системы. Однако часть возможностей и преимуществ при этом может быть потеряна. Также возможно, на стороне компьютера-клиента потребуется дополнительная настройка.

Для доступа к ресурсам сети (например, общим файлам, расположенным на сервере, либо получения доступа в сеть Интернет) пользователю, работающему на клиентском компьютере, необходимо *авторизоваться* на сервере — ввести свои данные (имя и пароль). После проверки аутентификации главным сервером, пользователь получает определённый администратором домена объём прав доступа к ресурсам сети.

Авторизация

Типичный пример — офисное рабочее место, постоянно находящееся в локальной сети. В этом случае аутентификация в домене происходит непосредственно в момент регистрации пользователя на рабочем месте (с доменными аутентификационными данными).

Рабочие места под управлением Альт Рабочая станция позволяют легко настроить такой способ аутентификации. Для этого в **Центре управления системой** (раздел **Аутентификация**) на рабочей станции, нужно указать домен, управляемый Альт Сервер.



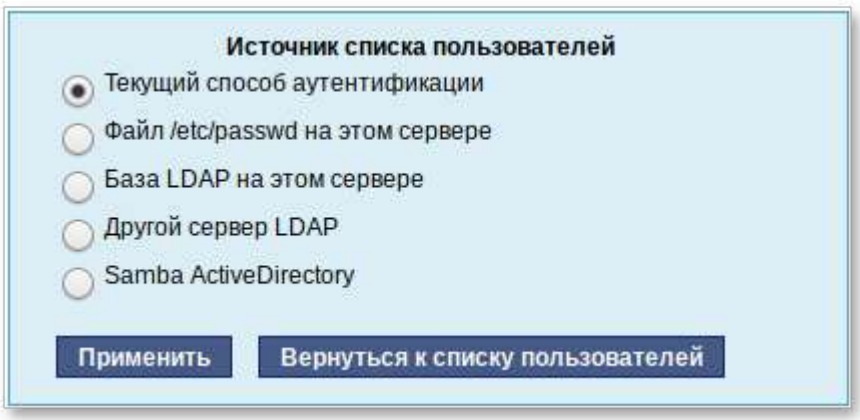
Глава 35. Централизованная база пользователей

Основной идеей домена является единая база учётных записей. При такой организации работы пользователям требуется лишь одна единственная учётная запись для доступа ко всем разрешённым администратором сети ресурсам. Наличие в сети единой централизованной базы пользователей позволяет значительно упростить работу, как самих пользователей, так и системных администраторов.

35.1. Создание учётных записей пользователей

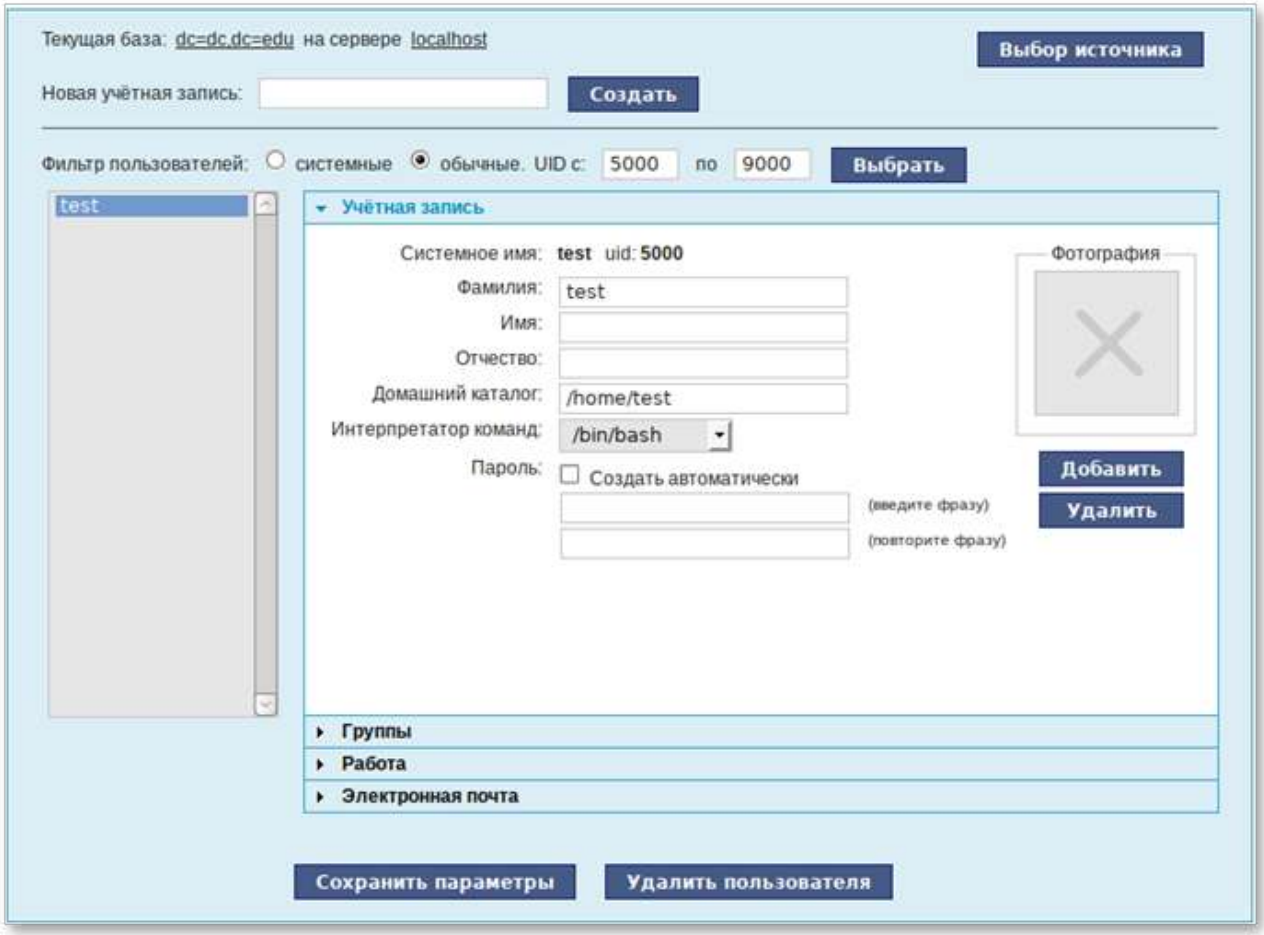
Централизованная база пользователей создаётся на главном сервере. Наполнить её учётными записями можно воспользовавшись модулем ЦУС **Пользователи** (пакет *alterator-ldap-users*) из раздела **Пользователи**.

Для выбора источника данных о пользователях, необходимо нажать кнопку **Выбор источника**, выбрать источник и нажать кнопку **Применить**.



Возможные варианты источника данных о пользователях:

- текущий метод аутентификации (выбирается в модуле **Аутентификация**);
- файл /etc/passwd (выбран по умолчанию);
- локальная база LDAP;
- база LDAP на другом сервере;
- локальная база Samba DC.



Для создания новой учётной записи необходимо ввести имя новой учётной записи и нажать кнопку **Создать**, после чего имя отобразится в списке слева. Для дополнительных настроек необходимо выделить существующую учётную запись, выбрав её из списка. Список доступных полей зависит от выбранного источника данных о пользователях.

После создания учётной записи пользователя не забудьте присвоить учётной записи пароль. Этот пароль и будет использоваться пользователем для регистрации в домене. После этого на рабочих местах под управлением Альт Рабочая станция, на которых для аутентификации установлен этот домен, можно вводить это имя пользователя и пароль.

35.2. Объединение пользователей в группы

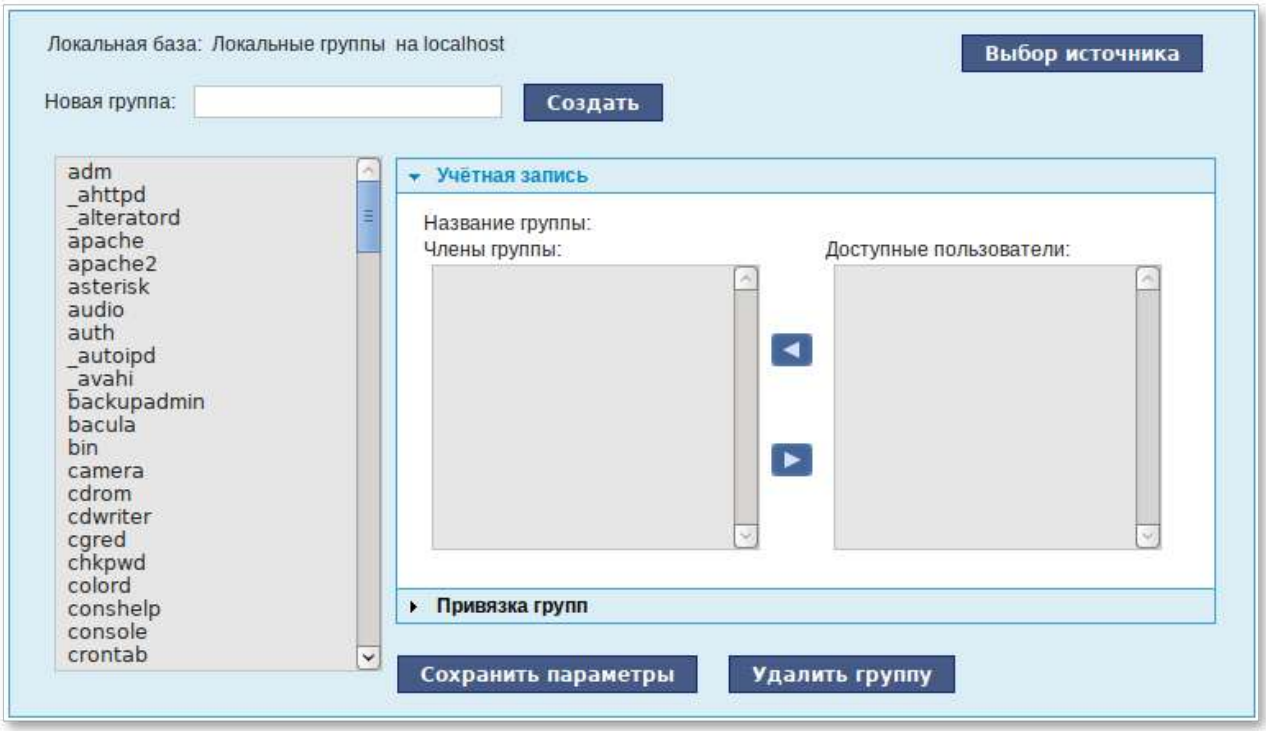
Пользователи могут быть объединены в группы. Это может быть полезно для более точного распределения полномочий пользователей. Например, члены группы **wheel** могут получать полномочия администратора на локальной машине, выполнив команду:

```
$ su -
```

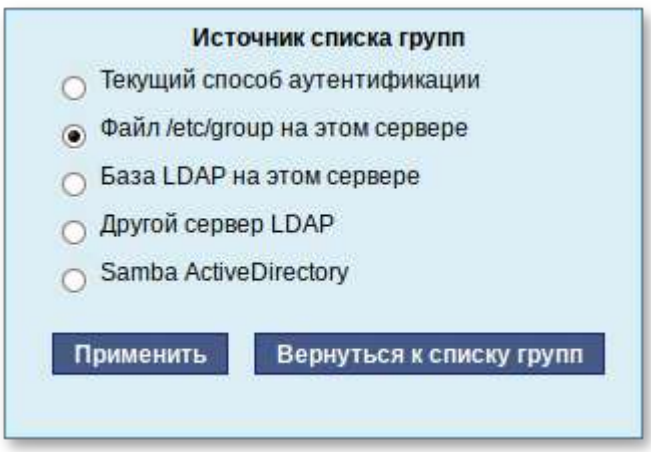
Настройка групп производится в модуле ЦУС **Группы** (пакет *alterator-ldap-groups*) из раздела **Пользователи**. С помощью данного модуля можно:

- просматривать актуальный список групп и список пользователей, входящих в каждую группу;
- создавать и удалять группы;
- добавлять и удалять пользователей в существующие группы;

- привязывать группу к системным группам и группам Samba.



Для выбора источника списка групп, нажмите кнопку **Выбор источника** и выберите источник:

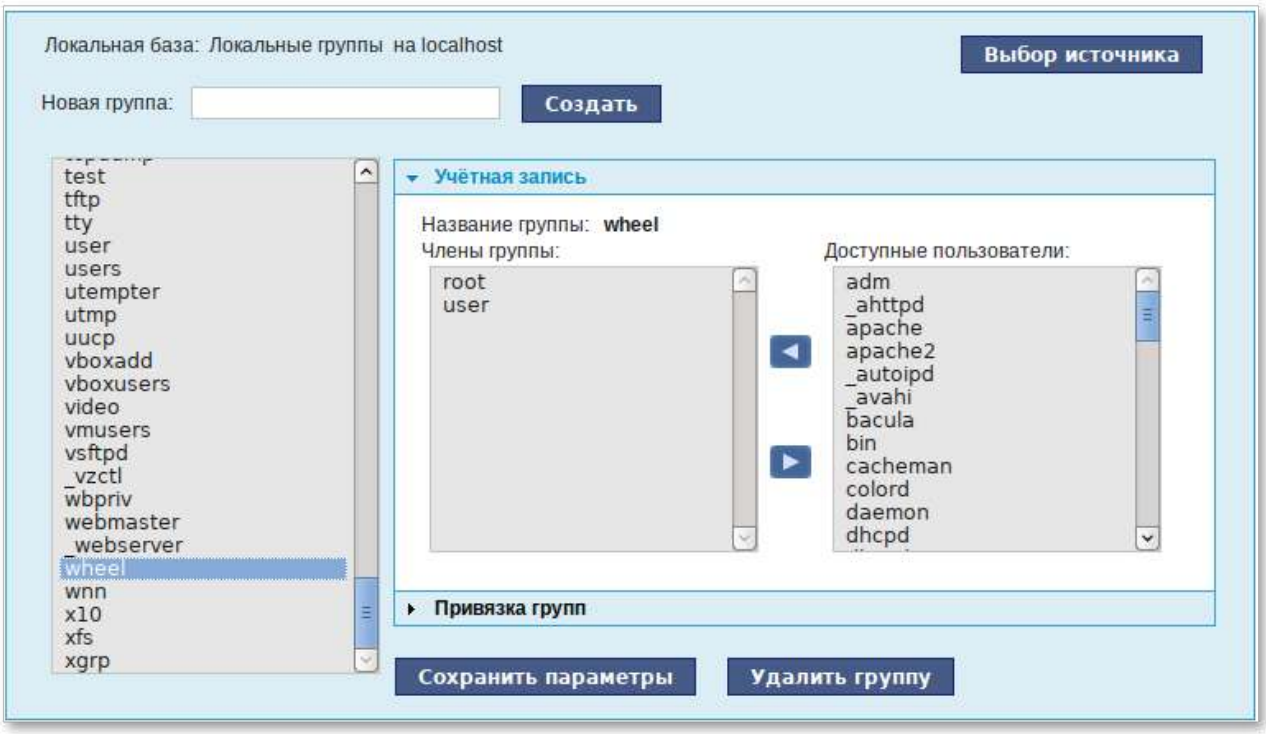


Возможные варианты: текущий способ аутентификации (выбирается в модуле **Аутентификация**), файл **`/etc/group`**, локальная база LDAP, другой сервер LDAP или Samba ActiveDirectory.

Для создания новой группы необходимо ввести название группы и нажать кнопку **Создать**, после чего имя отобразится в списке слева.

35.3. Настройка учётной записи

Во вкладке **Учётная запись** (модуль ЦУС **Группы**) можно настроить принадлежность учётной записи группам:



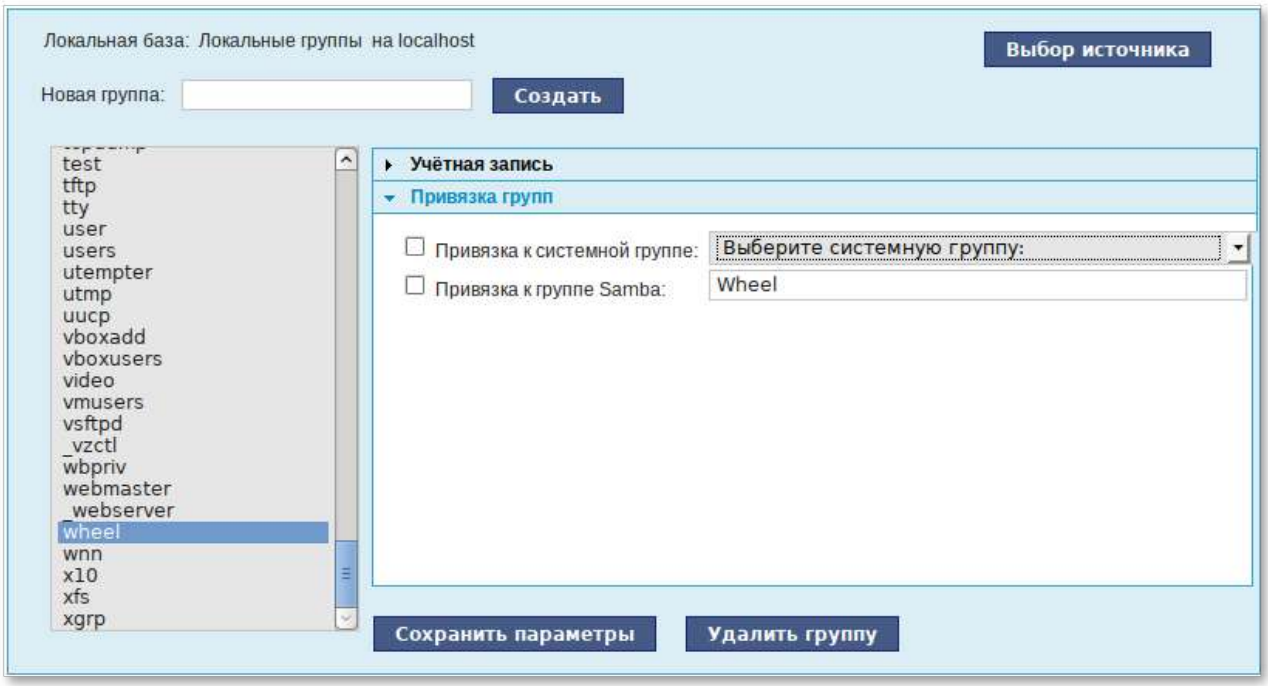
Для этого необходимо в списке групп выделить группу, к которой нужно добавить(удалить) пользователей. В списке **Члены группы** отображается информация о членах выделенной группы. В списке **Доступные пользователи** отображается список пользователей системы. Для включения пользователя в группу необходимо выбрать пользователя в списке **Доступные пользователи** и нажать кнопку

. Для исключения пользователя из группы необходимо выбрать пользователя в списке **Члены группы** и нажать кнопку

.

35.4. Привязка групп

Во вкладке **Привязка групп** (модуль ЦУС **Группы**) можно привязать группу к системной группе или к группе Samba:



Привязка к системной группе позволяет включать доменных пользователей в системные группы при регистрации на рабочей станции.

Примечание

Некоторые системные группы на сервере и на рабочей станции имеют разные идентификаторы (GID). Проверьте GID используемых системных групп на сервере и на рабочих станциях (в файле **`/etc/group`**).

Привязка к группе Samba позволяет создавать группы Samba, которые могут использоваться для установки прав доступа на рабочих станциях под управлением операционной системы Windows, которые аутентифицируются в ALT-домене.

За дополнительной информацией по настройке обращайтесь к встроенной справке соответствующих модулей ЦУС.

Часть VIII. Организация сетевой инфраструктуры с помощью сервера

Альт Сервер в сети организации может быть использован для решения различных задач. Он может предоставлять компьютерам сети общий доступ в Интернет, выступать в роли почтового сервера, файлового хранилища, веб-сервера и т.д. Все эти возможности обеспечиваются соответствующими *службами*, запускаемыми на сервере.

Дальнейшие разделы описывают некоторые возможности использования Альт Сервер, настраиваемые в ЦУС.

Важно

Эта и последующие главы рекомендуются к прочтению опытным пользователям и системным администраторам.

Содержание

Глава 36. Настройка подключения к Интернету

Помимо множества различных служб, которые Альт Сервер может предоставлять компьютерам сети, важно определить, будет ли сервер предоставлять общий доступ в Интернет для компьютеров домена или нет. В зависимости от этого сервер можно рассматривать как:

Сервер без подключения к сети Интернет

Типичный случай — это сервер с одним сетевым интерфейсом (одной сетевой картой), который и связывает его с компьютерами локальной сети. Такой сервер называется также *сервер рабочей группы*.

Шлюз

В этом случае сервер обычно имеет два сетевых интерфейса (например, две сетевые карты), одна из которых служит для подключения к локальной сети, а другая — для подключения к сети Интернет.

Как для обеспечения доступа в сеть Интернет самого Альт Сервер, так и для настройки общего выхода в Интернет для компьютеров сети необходимо настроить подключение к Интернету на самом сервере. Альт Сервер поддерживает самые разные способы подключения к сети Интернет:

- Ethernet;
- PPTP;
- PPPoE;
- и т.д.

Для настройки подключения воспользуйтесь одним из разделов ЦУС **Сеть**.

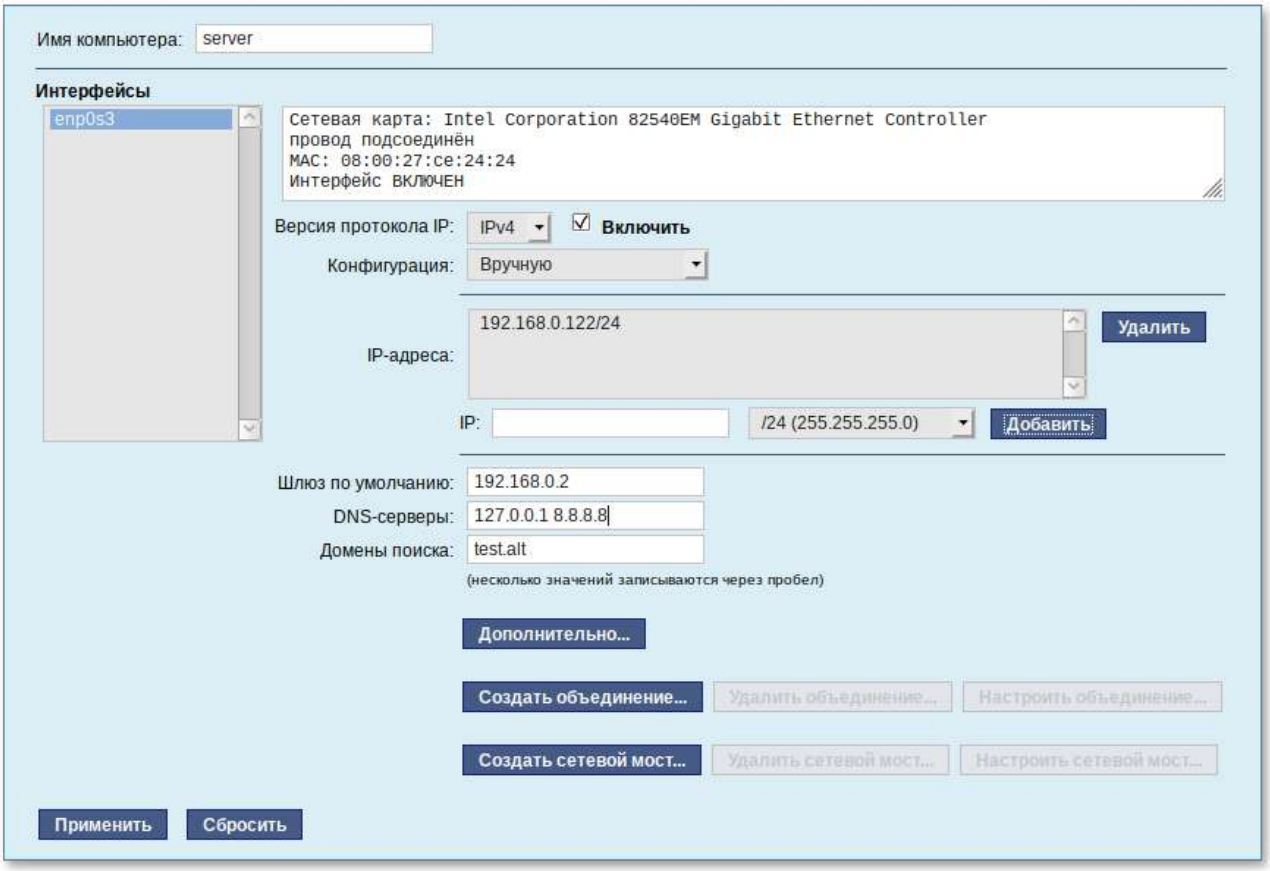
Доступные разделы:

- Ethernet-интерфейсы;
- PPTP-соединения;
- PPPoE-соединения;
- OpenVPN-соединения.

Выберите раздел, соответствующий вашему типу подключения, и приступайте к настройке.

36.1. Конфигурирование сетевых интерфейсов

Конфигурирование сетевых интерфейсов осуществляется в модуле ЦУС **Ethernet-интерфейсы** (пакет *alterator-net-eth*) из раздела **Сеть**:



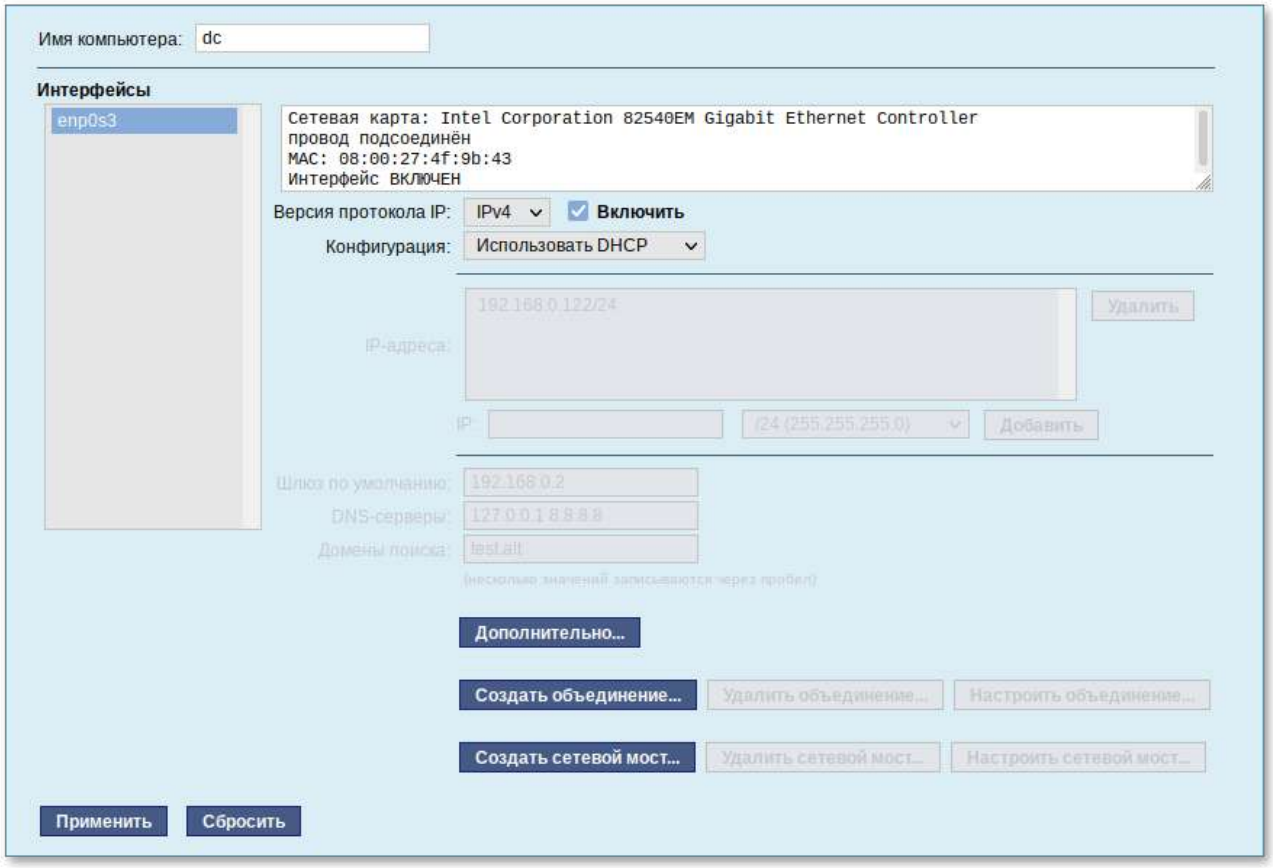
В модуле **Ethernet-интерфейсы** можно заполнить следующие поля:

- **Имя компьютера** — указать сетевое имя ПЭВМ в поле для ввода имени компьютера (это общий сетевой параметр, не привязанный, к какому-либо конкретному интерфейсу). Имя компьютера, в отличие от традиционного имени хоста в Unix (hostname), не содержит названия сетевого домена;
- **Интерфейсы** — выбрать доступный сетевой интерфейс, для которого будут выполняться настройки;
- **Версия протокола IP** — указать в выпадающем списке версию используемого протокола IP (IPv4, IPv6) и убедиться, что пункт **Включить**, обеспечивающий поддержку работы протокола, отмечен;
- **Конфигурация** — выбрать способ назначения IP-адресов (службы DHCP, Zeroconf, вручную);
- **IP-адреса** — пул назначенных IP-адресов из поля **IP**, выбранные адреса можно удалить нажатием кнопки **Удалить**;
- **IP** — ввести IP-адрес вручную и выбрать в выпадающем поле предпочтительную маску сети, затем нажать кнопку **Добавить** для переноса адреса в пул поля **IP-адреса**;
- **Шлюз по умолчанию** — в поле для ввода необходимо ввести адрес шлюза, который будет использоваться сетью по умолчанию;
- **DNS-серверы** — в поле для ввода необходимо ввести список предпочтительных DNS-серверов, которые будут получать информацию о доменах, выполнять маршрутизацию почты и управлять обслуживающими узлами для протоколов в домене;

- **Домены поиска** — в поле для ввода необходимо ввести список предпочтительных доменов, по которым будет выполняться поиск. Если в поле **Домены поиска** перечислить наиболее часто используемые домены (например, domain), то можно пользоваться неполными именами машин (computer вместо computer.domain).

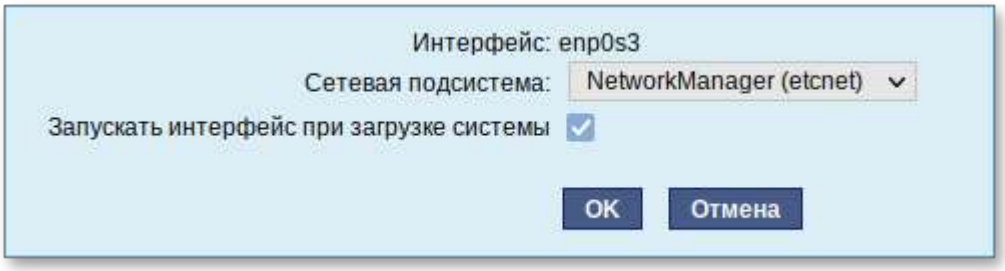
IP-адрес и **Маска сети** — обязательные параметры каждого узла IP-сети. Первый параметр – уникальный идентификатор машины, от второго напрямую зависит, к каким машинам локальной сети данная машина будет иметь доступ. Если требуется выход во внешнюю сеть, то необходимо указать параметр **Шлюз по умолчанию**.

В случае наличия DHCP-сервера можно все вышеперечисленные параметры получить автоматически – выбрав в списке **Конфигурация** пункт **Использовать DHCP**:



Если в компьютере имеется несколько сетевых карт, то возможна ситуация, когда при очередной загрузке ядро присвоит имена интерфейсов (enp0s3, enp0s8) в другом порядке. В результате интерфейсы получат не свои настройки. Чтобы этого не происходило, можно привязать интерфейс к имени по его аппаратному адресу (MAC) или по местоположению на системной шине.

Дополнительно для каждого интерфейса можно настроить сетевую подсистему (NetworkManager, Etcnet), а также должен ли запускаться данный интерфейс при загрузке системы:



В списке **Сетевая подсистема** можно выбрать следующие режимы:

Etcnet

В этом режиме настройки берутся исключительно из файлов находящихся в каталоге настраиваемого интерфейса **/etc/net/ifaces/<интерфейс>**. Настройки сети могут изменяться либо в ЦУС в данном модуле, либо напрямую через редактирование файлов **/etc/net/ifaces/<интерфейс>**.

NetworkManager (etcnet)

В этом режиме **NetworkManager** сам инициирует сеть, используя в качестве параметров — настройки из файлов Etcnet. Настройки сети могут изменяться либо в ЦУС в данном модуле, либо напрямую через редактирование файлов **/etc/net/ifaces/<интерфейс>**. В этом режиме можно просмотреть настройки сети, например полученный по DHCP IP-адрес, через графический интерфейс **NetworkManager**.

NetworkManager (native)

В данном режиме управление настройками интерфейса передаётся **NetworkManager** и не зависит от файлов Etcnet. Управлять настройками можно через графический интерфейс **NetworkManager**. Файлы с настройками находятся в директории **/etc/NetworkManager/system-connections**. Этот режим особенно актуален для задач настройки сети на клиенте, когда IP-адрес необходимо получать динамически с помощью DHCP, а DNS-сервер указать явно. Через ЦУС так настроить невозможно, так как при включении DHCP отключаются настройки, которые можно задавать вручную.

Не контролируется

В этом режиме интерфейс находится в состоянии DOWN (выключен).

36.2. Настройка общего подключения к сети Интернет

Пользователи корпоративных сетей обычно подключаются к сети Интернет через один общий канал. Для организации совместного доступа к сети Интернет стандартными средствами поддерживаются две технологии, которые могут использоваться как по отдельности, так и совместно:

- использование прокси-сервера;
- использование NAT.

Оба способа предполагают, что соединение с Интернет компьютера, через который предполагается настроить общий выход, предварительно сконфигурировано . Сделать это можно в разделе ЦУС **Сеть**.

36.2.1. Прокси-сервер

Отличительной особенностью использования прокси-сервера является то, что, помимо предоставления доступа к веб-сайтам, прокси-сервер кэширует загруженные страницы, а при повторном обращении к ним — отдаёт их из своего кэша. Это может существенно снизить потребление трафика.

У прокси-сервера есть два основных режима работы:

- прозрачный;
- обычный.

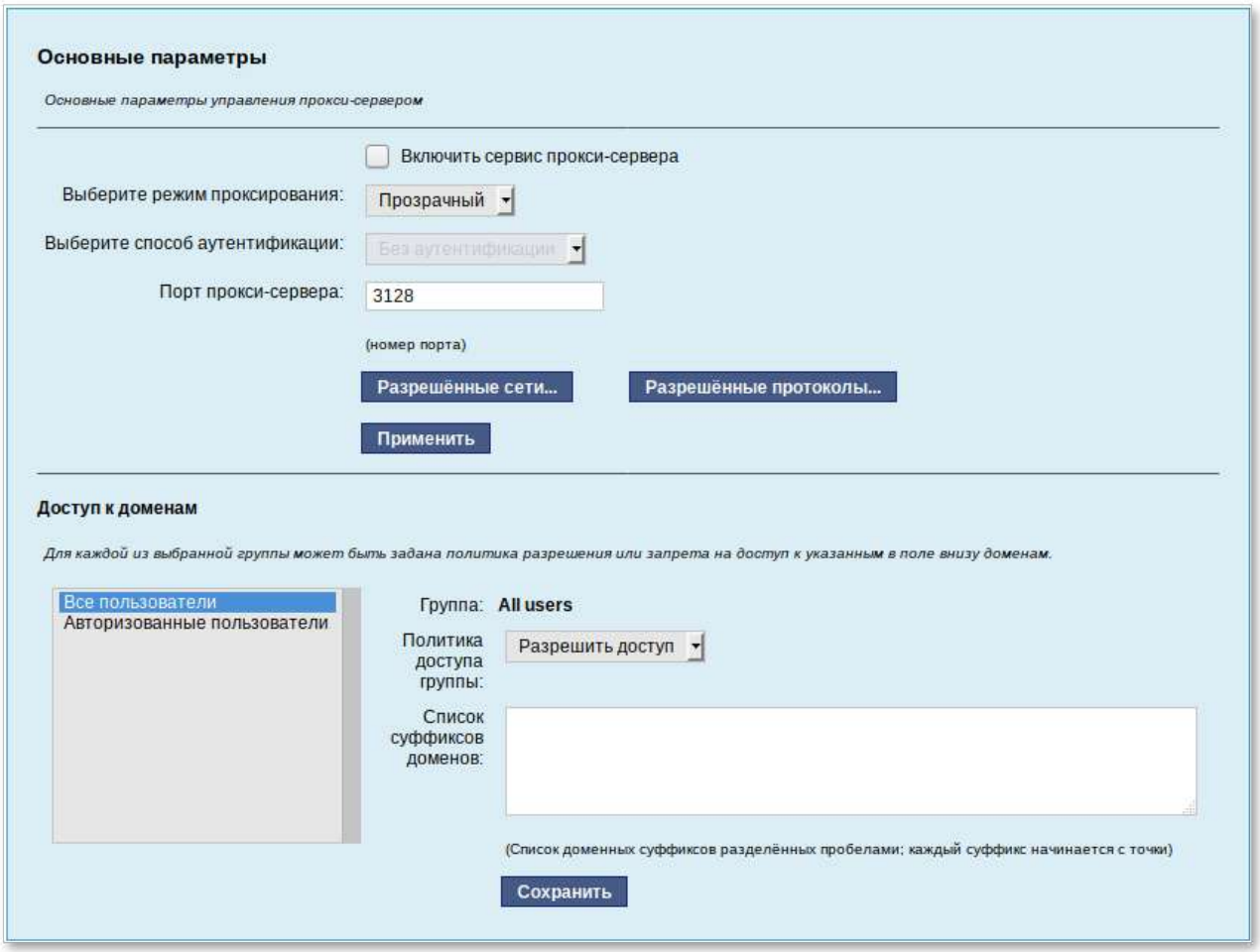
Для работы с прокси-сервером в прозрачном режиме не потребуется специальная настройка рабочих станций. Они лишь должны использовать сервер в качестве шлюза по умолчанию. Этого можно добиться, сделав соответствующие настройки на DHCP-сервере.

Для использования прокси-сервера в обычном режиме потребуется на каждом клиенте в настройках браузера указать данные прокси-сервера (IP-адрес и порт).

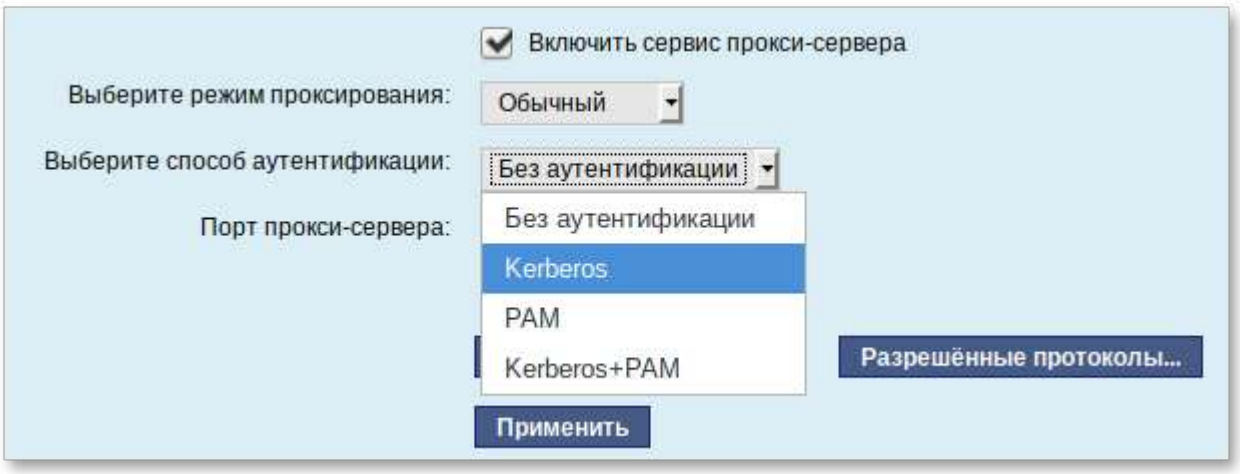
Преимуществом обычного режима работы, требующего перенастройки программ локальной сети, является возможность производить аутентификацию пользователей и контролировать их доступ во внешнюю сеть.

В различных браузерах местоположение формы настройки на прокси-сервер различное. Например, в браузере **Firefox** она доступна через меню **Правка** → **Настройки** → **раздел Дополнительно** → **вкладка Сеть**+**кнопка Настроить...** напротив текста «Настройка параметров соединения Firefox с Интернетом». Здесь следует выбрать **Ручная настройка сервиса прокси** и указать IP-адрес и порт прокси-сервера.

По умолчанию прокси-сервер не предоставляет доступ в Интернет никому кроме себя самого. Список сетей, обслуживаемых прокси-сервером можно изменить, нажав на кнопку «**Разрешённые сети...**» в модуле ЦУС **Прокси-сервер** (пакет *alterator-squid*) из раздела **Серверы**.

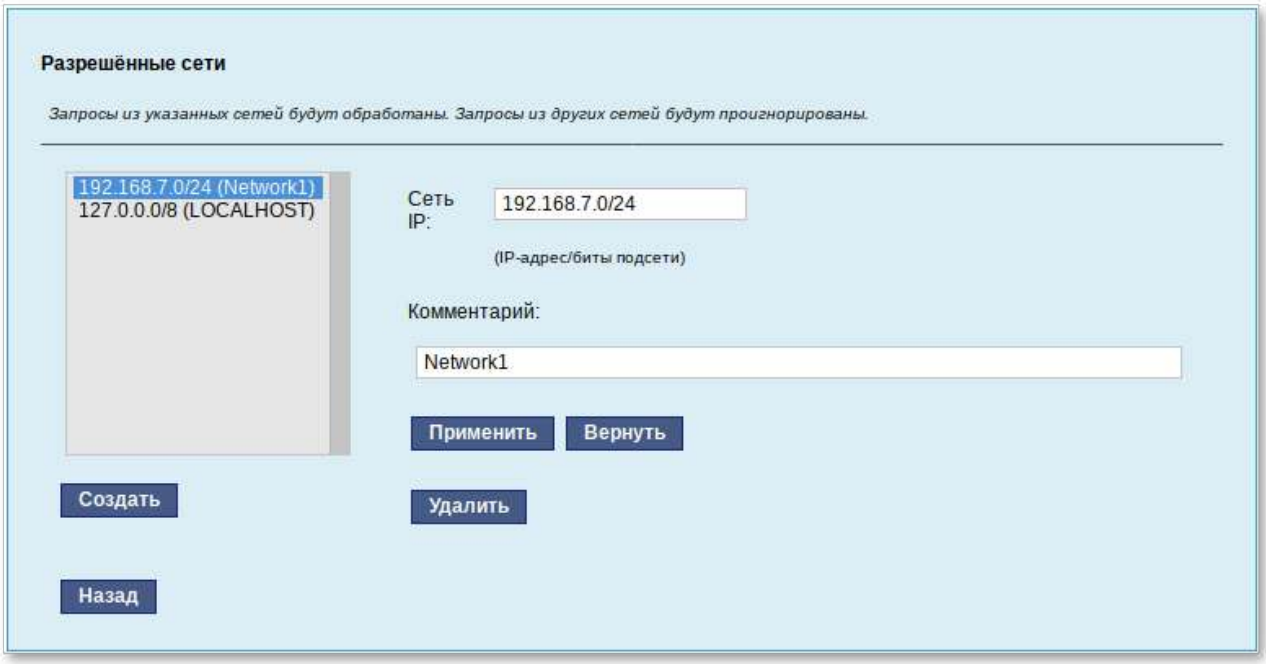


Для того чтобы включить аутентификацию пользователей и контролировать их доступ во внешнюю сеть, необходимо выбрать обычный режим проксирования и способ аутентификации, отличный от **Без аутентификации**:

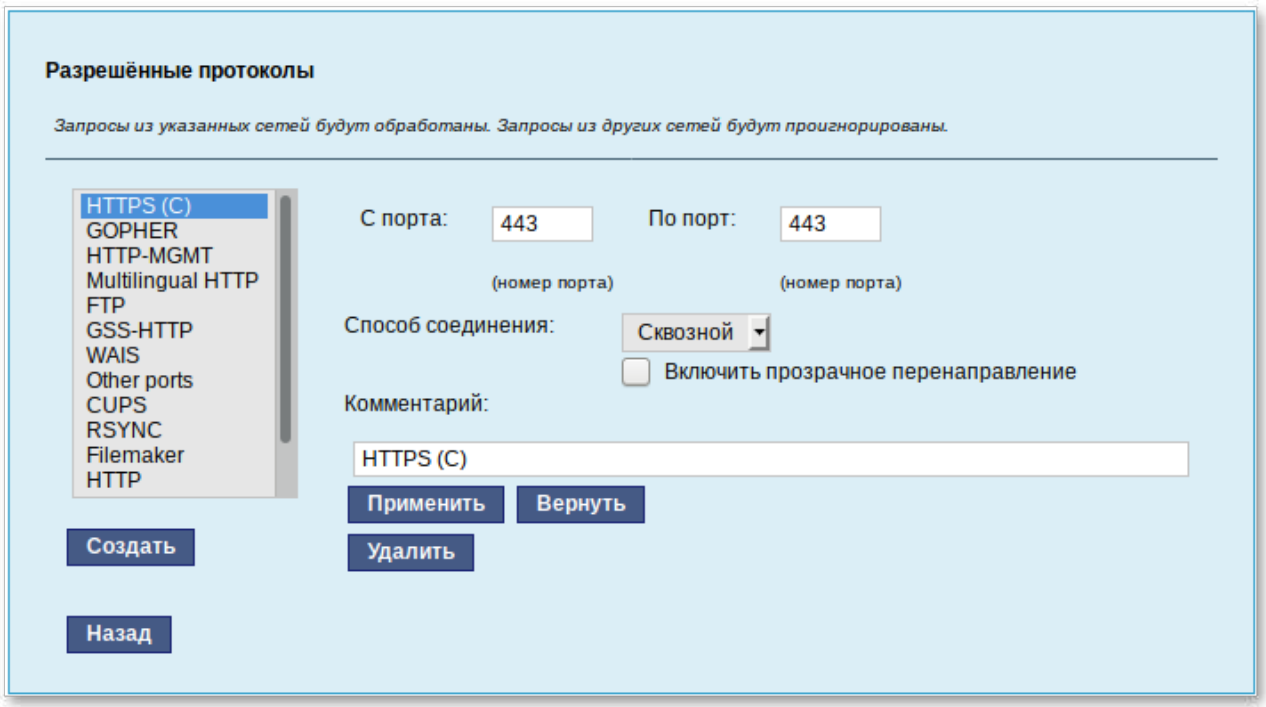


Прокси-сервер принимает запросы из локальной сети и, по мере необходимости, передаёт их во внешнюю сеть. Поступление запроса ожидается на определённом порту, который по умолчанию имеет стандартный номер 3128. Если по каким-то причинам не желательно использовать данный порт, то можно поменять его значение на любое другое.

Перед тем как выполнить перенаправление запроса, прокси-сервер проверяет принадлежность сетевого адрес узла, с которого запрос был отправлен к группе внутренних сетевых адресов. Для того чтобы запросы, отправленные из локальной сети, обрабатывались прокси-сервером, необходимо добавить соответствующую группу адресов (адрес подсети и адресную маску) в список внутренних сетей в разделе **Разрешённые сети**:



Вторым условием передачи запроса является принадлежность целевого порта к разрешённому диапазону. Посмотреть и отредактировать список разрешённых целевых портов можно в разделе **Разрешённые протоколы**:



Прокси-сервер позволяет вести статистику посещений страниц в Интернете. Она доступна в модуле ЦУС **Прокси-сервер** (пакет *alterator-squidmill*) в разделе **Статистика**. Основное предназначение статистики — просмотр отчёта об объёме полученных из Интернета данных в привязке к пользователям (если включена аутентификация) или к IP-адресам клиентов.

Примечание

Статистика не собирается по умолчанию. Включить её сбор следует в модуле ЦУС **Прокси-сервер** (раздел **Статистика**). Для этого отметьте **Включить сбор данных прокси-сервера** и нажмите кнопку **Применить**.

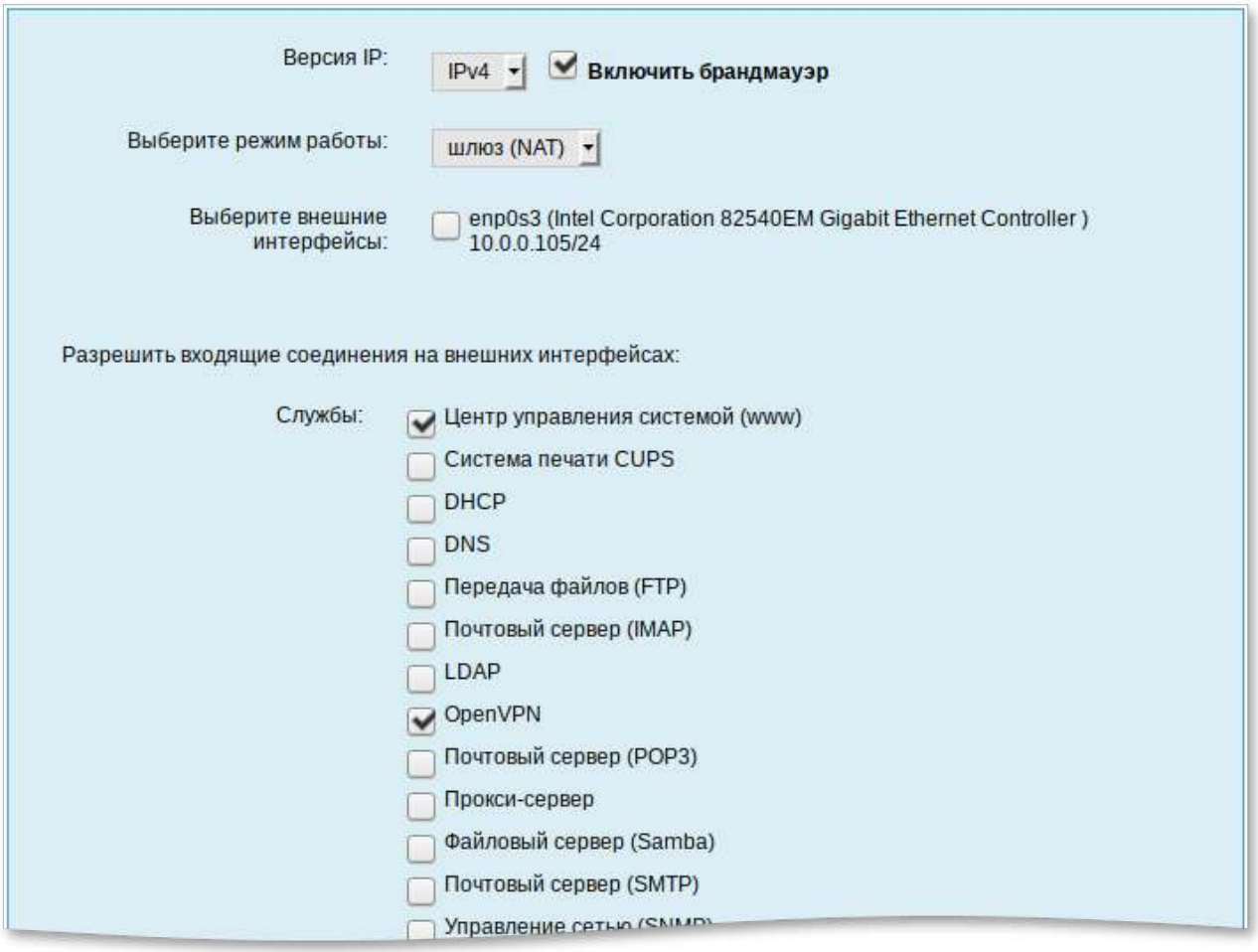
Примечание

Для учёта пользователей в статистике нужно добавить хотя бы одно правило. Самое очевидное — запрет не аутентифицированных пользователей. Только после этого в статистике начнут показываться пользователи.

36.2.2. NAT

NAT (Network Address Translation, преобразование сетевых адресов) — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Таким образом, компьютеры локальной сети, имеющие IP-адреса, зарезервированные для использования исключительно в локальных сетях, могут использовать общий канал доступа к Интернет (общий внешний IP-адрес). При этом на компьютере-шлюзе, непосредственно подключённом к Интернет, выполняется преобразование адресов.

Настройка NAT осуществляется в модуле ЦУС **Внешние сети** (пакет *alterator-net-iptables*) из раздела **Брандмауэр**. Для минимальной настройки достаточно выбрать режим работы **Шлюз (NAT)**, отметить правильный внешний сетевой интерфейс и нажать на кнопку **Применить**.



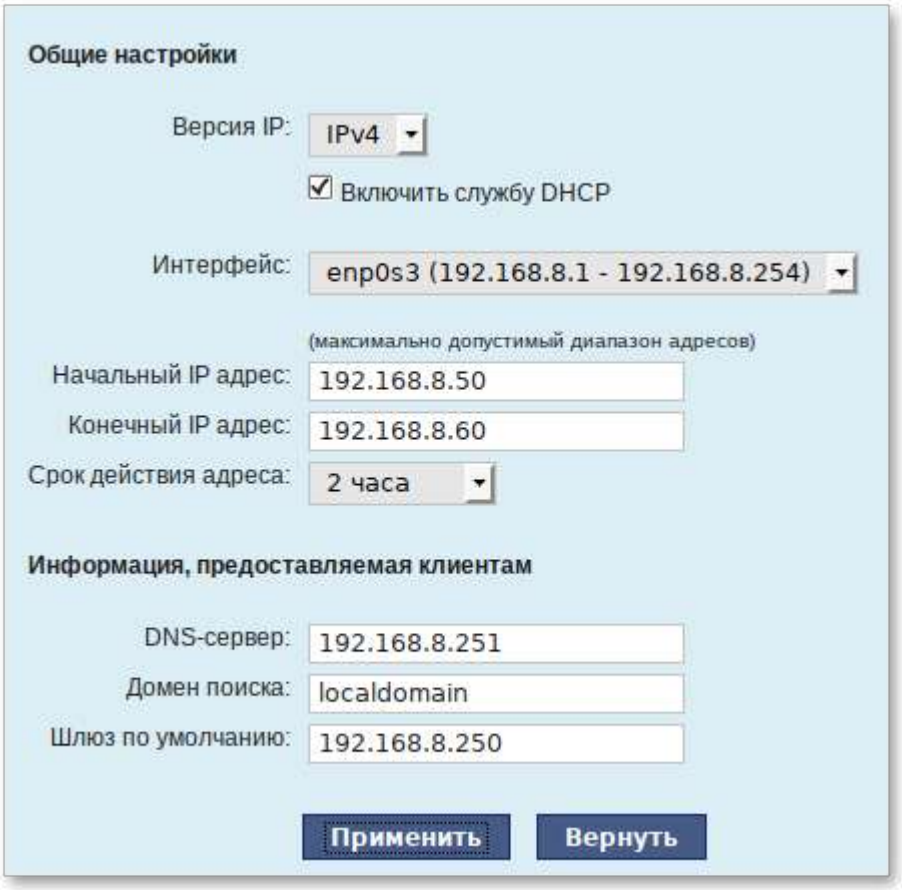
36.3. Автоматическое присвоение IP-адресов (DHCP-сервер)

DHCP (Dynamic Host Configuration Protocol) — протокол, позволяющий клиенту самостоятельно получить IP-адрес из зарезервированного диапазона адресов, а также дополнительную информацию о локальной сети (DNS-сервер сети, домен поиска, шлюз по умолчанию). Это облегчает администрирование клиентских машин, избавляя администратора домена от необходимости вручную настраивать сетевые интерфейсы на компьютерах локальной сети.

Чтобы настраивать DHCP-сервер, на машине должен быть хотя бы один статически сконфигурированный Ethernet-интерфейс.

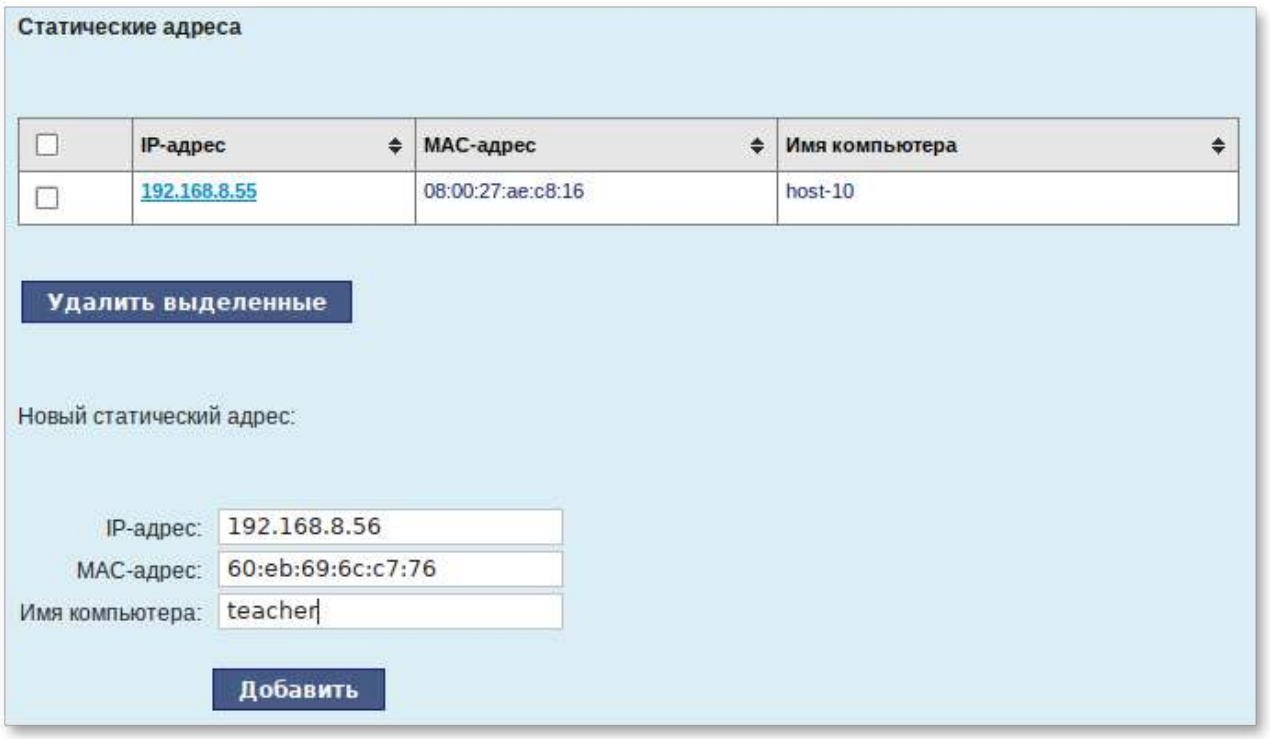
Настройка DHCP-сервера осуществляется в модуле ЦУС **DHCP-сервер** (пакет *alterator-dhcp*) из раздела **Серверы**.

Для включения DHCP-сервера необходимо установить флажок **Включить службу DHCP**, указать начальный и конечный IP-адрес, а также шлюз по умолчанию (обычно, это IP-адрес сервера на сетевом интерфейсе, обслуживающем локальную сеть).



Теперь при включении любой клиентской машины с настройкой **получение ip и dns автоматически** будет присваиваться шлюз 192.168.8.250, DNS 192.168.8.251 и адреса начиная с 192.168.8.50 по порядку включения до 192.168.8.60.

Иногда бывает полезно выдавать клиенту один и тот же IP-адрес независимо от момента обращения. В этом случае он определяется по аппаратному адресу (MAC-адресу) сетевой карты клиента. Для добавления своих значений в таблицу соответствия статических адресов введите IP-адрес и соответствующий ему MAC-адрес и нажмите кнопку **Добавить**.

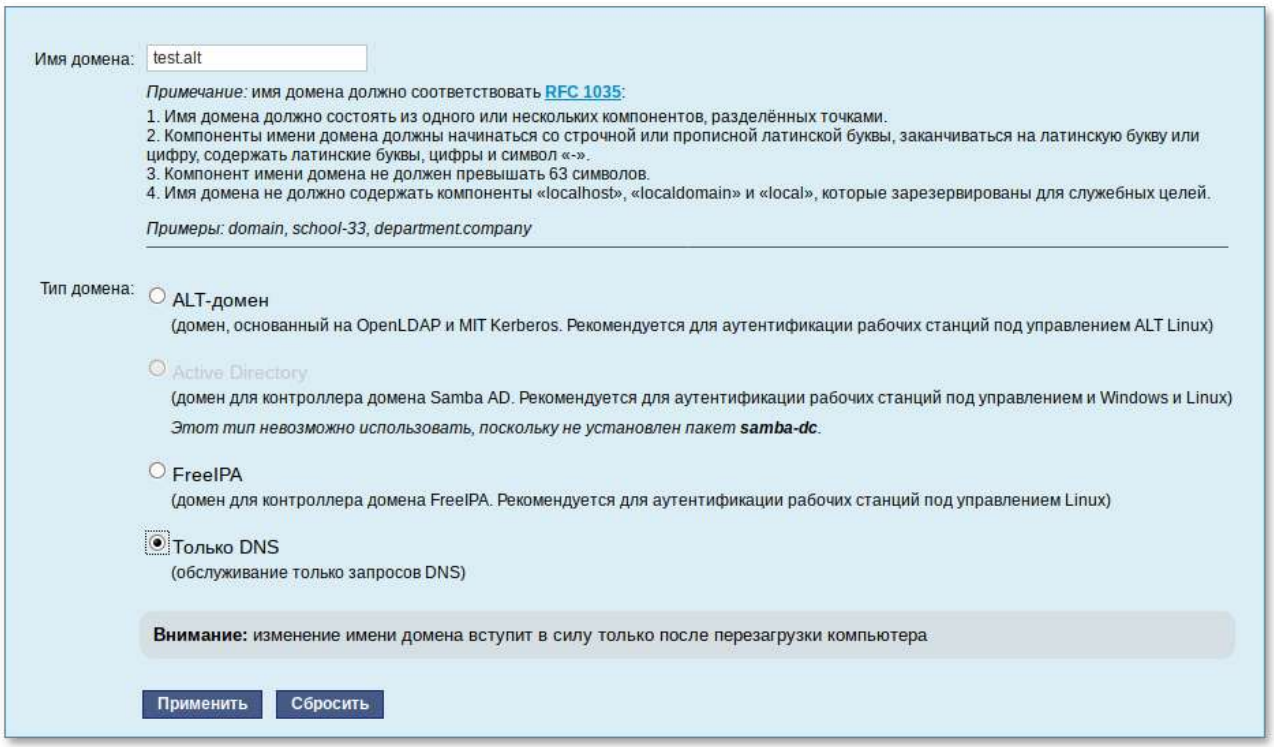


Выданные IP-адреса можно увидеть в списке **Текущие динамически выданные адреса**. Здесь также имеется возможность зафиксировать выданные адреса, за данными компьютерами. Для этого необходимо отметить хост, за которым нужно закрепить IP-адрес и нажать кнопку **Зафиксировать адрес для выбранных компьютеров**.

За дополнительной информацией по настройке обращайтесь к встроенной справке модуля ЦУС.

Глава 37. Развертывание доменной структуры

Для развертывания доменной структуры предназначен модуль ЦУС **Домен** из раздела **Система** (пакет *alterator-net-domain*):



Модуль поддерживает следующие виды доменов:

- ALT-домен. Домен, основанный на OpenLDAP и MIT Kerberos. Домен нужно устанавливать только после настройки сервера DHCP. В противном случае придётся выбирать другое имя домена.
- Active Directory. Домен для контроллера домена Samba AD. Рекомендуется для аутентификации рабочих станций под управлением и Windows и Linux.
- FreeIPA. Домен для контроллера домена FreeIPA. Рекомендуется для аутентификации рабочих станций под управлением Linux.
- DNS. Обслуживание только запросов DNS указанного домена сервисом BIND.

Глава 38. Сетевая установка операционной системы на рабочие места

Одной из удобных возможностей Альт Сервер при разворачивании инфраструктуры является сетевая установка. При помощи сетевой установки можно производить установку Альт Сервер не с DVD-диска, а загрузив инсталлятор по сети.

38.1. Подготовка сервера

Перед началом установки рабочих станций следует произвести предварительную настройку сервера: задать имя сервера (модуль **Ethernet-интерфейсы** в **ЦУС**), включить DHCP-сервер (модуль **DHCP-сервер**), задать имя домена (модуль **Домен**).

Примечание

При сетевой установке с сервера будут переняты настройки домена, и включена централизованная аутентификация. Если вы устанавливаете Альт Сервер с DVD-диска, то настройку домена и аутентификации надо будет производить отдельно на каждой рабочей стации.

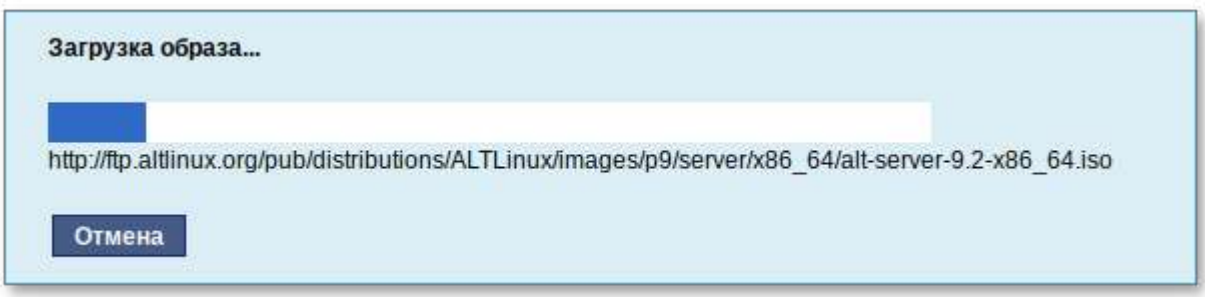
Перед активацией сетевой установки потребуется импортировать установочный DVD-диск Альт Сервер, предварительно вставив его в DVD-привод сервера, либо используя образ диска, расположенный на файловой системе на сервере. Можно также использовать URL вида http://ftp.altlinux.org/pub/distributions/ALTLinux/images/p9/server/x86_64/alt-server-9.2-x86_64.iso.

Примечание

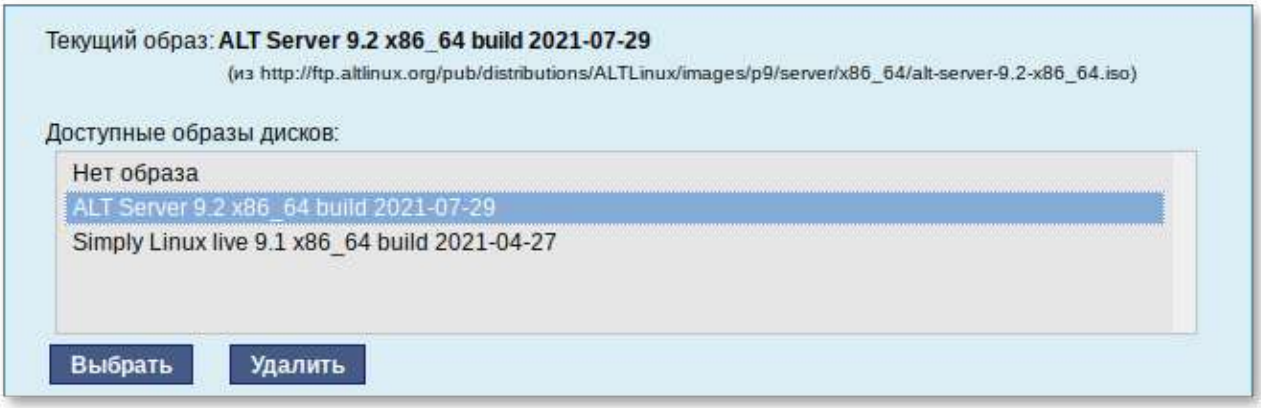
Локальный файл должен быть доступен для nobody и должен находиться на сервере, где запущен alterator-netinst.

В разделе **Сервер сетевых установок** (пакет *alterator-netinst*), укажите откуда импортировать новый образ и нажмите кнопку **Добавить**.

Процесс добавления образа занимает какое-то время. Пожалуйста, дождитесь окончания этого процесса.



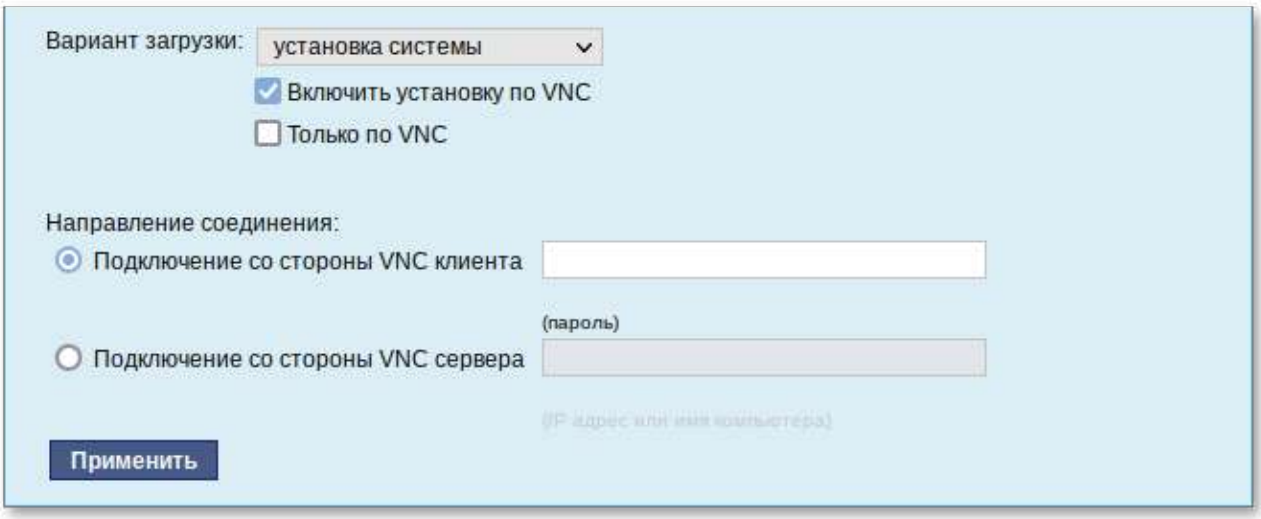
После добавления образа он появится в списке **Доступные образы дисков**. Необходимо выбрать из списка один из образов и нажать кнопку **Выбрать**.



На этом подготовка сервера к сетевой установке рабочих станций завершена.

Далее следует выбрать направление соединения. Удалённый доступ к компьютеру может быть двух видов:

- Со стороны клиента. Во время установки администратор может с помощью VNC-клиента подключиться к компьютеру, на которой производится установка, зная его IP-адрес и заданный пароль.
- Со стороны сервера. Во время установки с каждого компьютера инициируется подключение к запущенному на заданном компьютере VNC-клиенту. Компьютер-приёмник соединений задаётся IP-адресом или именем.



В случае, когда работа с аппаратной подсистемой ввода-вывода невозможна (например, если клавиатура, мышь или монитор отсутствуют), можно использовать вариант **Только по VNC**.

Если необходимо управлять установкой удалённо, отметьте пункт **Включить установку по VNC** и пункт **Подключение со стороны VNC сервера** раздела **Направление соединения**, и там укажите адрес компьютера, с которого будет происходить управление. Для приёма подключения можно запустить, например, **`vncviewer -listen`**.

Предупреждение

Не забудьте отключить сетевую установку по окончании процесса установки ОС на рабочих станциях. Это можно сделать, выбрав в списке **Доступные образы дисков** пункт **Нет образа** и подтвердив действие нажатием кнопки **Выбрать**.

За дополнительной информацией по настройке обращайтесь к встроенной справке соответствующих модулей Центра управления системой.

38.2. Подготовка рабочих станций

Для сетевой установки следует обеспечить возможность загрузки по сети рабочих станций, на которых будет производиться установка ОС.

Большинство современных материнских плат имеют возможность загрузки по сети, однако она по умолчанию может быть отключена в BIOS. Различные производители материнских плат дают разные названия данной возможности, например: "Boot Option ROM" или "Boot From Onboard LAN".

Примечание

Некоторые материнские платы позволяют выбрать источник загрузки во время включения компьютера. Эта возможность может называться, например, "Select boot device" или "Boot menu".

Последовательность установки при установке с DVD-диска и при сетевой установке не отличаются друг от друга. Обратитесь к разделу руководства Последовательность установки.

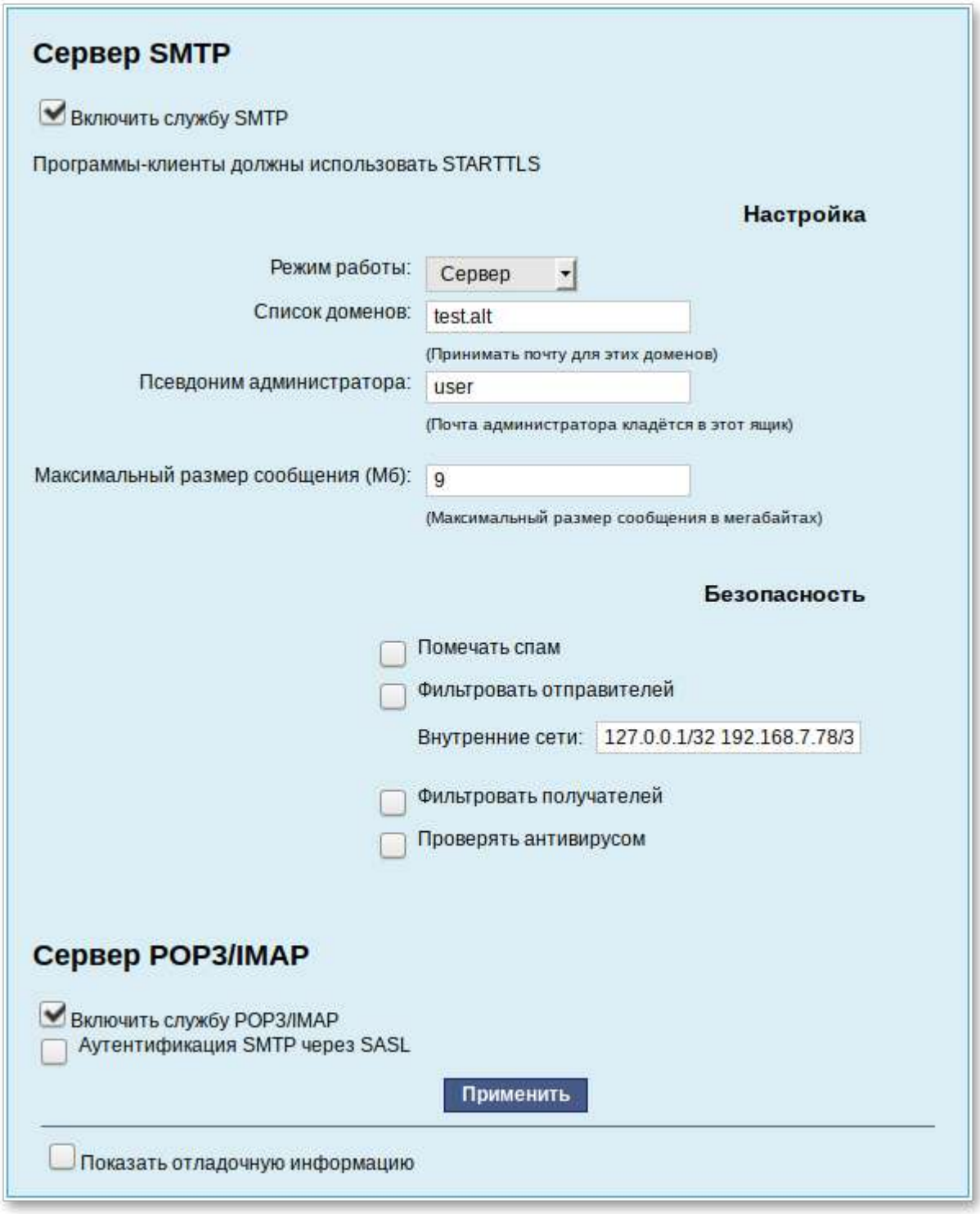
Глава 39. Сервер электронной почты (SMTP, POP3/IMAP)

39.1. Сервер электронной почты

После установки сервера и первоначальной настройки вы уже имеете преднастроенный почтовый сервер, обслуживающий почтовый домен, указанный при первоначальной настройке в поле **домен**.

Альт Сервер может служить как почтовым сервером, обслуживающим определённый домен, так и посредником (шлюзом) для пересылки почты. Почтовый сервер отвечает как за отправку писем (SMTP-сервер) исходящих от почтовых клиентов рабочих станций, так и за предоставление им входящей почты (Сервер POP3/IMAP).

Для настройки параметров работы сервера предусмотрен модуль ЦУС **Почтовый сервер** (пакет *alterator-postfix-dovecot*) из раздела **Серверы**.



39.2. Сервер SMTP

Сервер SMTP отвечает за отправку сообщений и может работать в двух режимах:

Посредник

В этом режиме исходящая почта пересылается для дальнейшей отправки на указанный сервер.

Сервер

В этом режиме сервер доставляет почту самостоятельно.

39.3. Сервер POP3/IMAP

Сервер POP3/IMAP используется для доступа пользователей к электронной почте на сервере.

Для доступа к службам POP3 и IMAP пользователь должен включить в своём почтовом клиенте аутентификацию и указать своё имя и пароль.

Выбор конкретного используемого протокола для получения почты зависит от предпочтений пользователя.

POP

При проверке почты почтовым клиентом почта передаётся на клиентскую машину, где и сохраняется. Возможность просмотра принятой/отправленной почты при этом существует даже если клиент не имеет соединения с сервером.

IMAP

Все сообщения хранятся на сервере. Почтовый клиент может просматривать их только при наличии соединения с сервером.

Помимо включения/отключения служб, модуль ЦУС **Почтовый сервер** позволяет произвести дополнительные настройки: фильтрацию спама, настройку параметров аутентификации и т.д.

За дополнительной информацией по использованию модуля обращайтесь к встроенной справке модуля ЦУС.

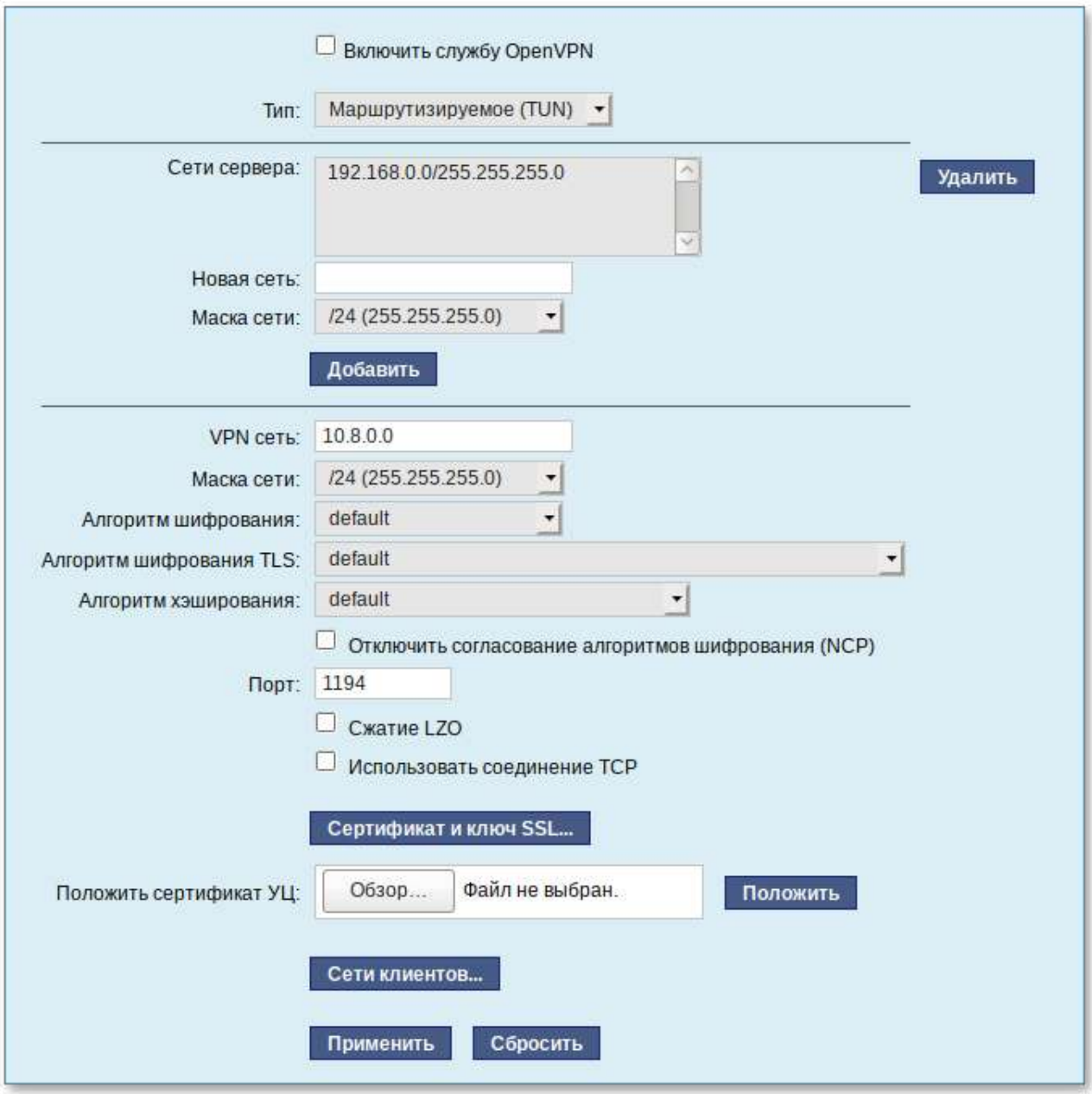
Глава 40. Соединение удалённых офисов (OpenVPN-сервер)

Альт Сервер предоставляет возможность безопасного соединения удалённых офисов используя технологию VPN (англ. Virtual Private Network — виртуальная частная сеть), которая позволяет организовать безопасные шифрованные соединения через публичные сети (например, Интернет) между удалёнными офисами или локальной сетью и удалёнными пользователями. Таким образом, вы можете связать два офиса организации, что, делает работу с документами, расположенными в сети удалённого офиса, более удобной.

Помимо соединения целых офисов, также существует возможность организовать доступ в офисную сеть для работы в ней извне. Это означает, например, что сотрудник может работать в своём привычном окружении, даже находясь в командировке или просто из дома.

40.1. Настройка OpenVPN-сервера

Для организации VPN соединения на стороне сервера предусмотрен модуль ЦУС **OpenVPN-сервер** (пакет *alterator-openvpn-server*) из раздела **Серверы**.



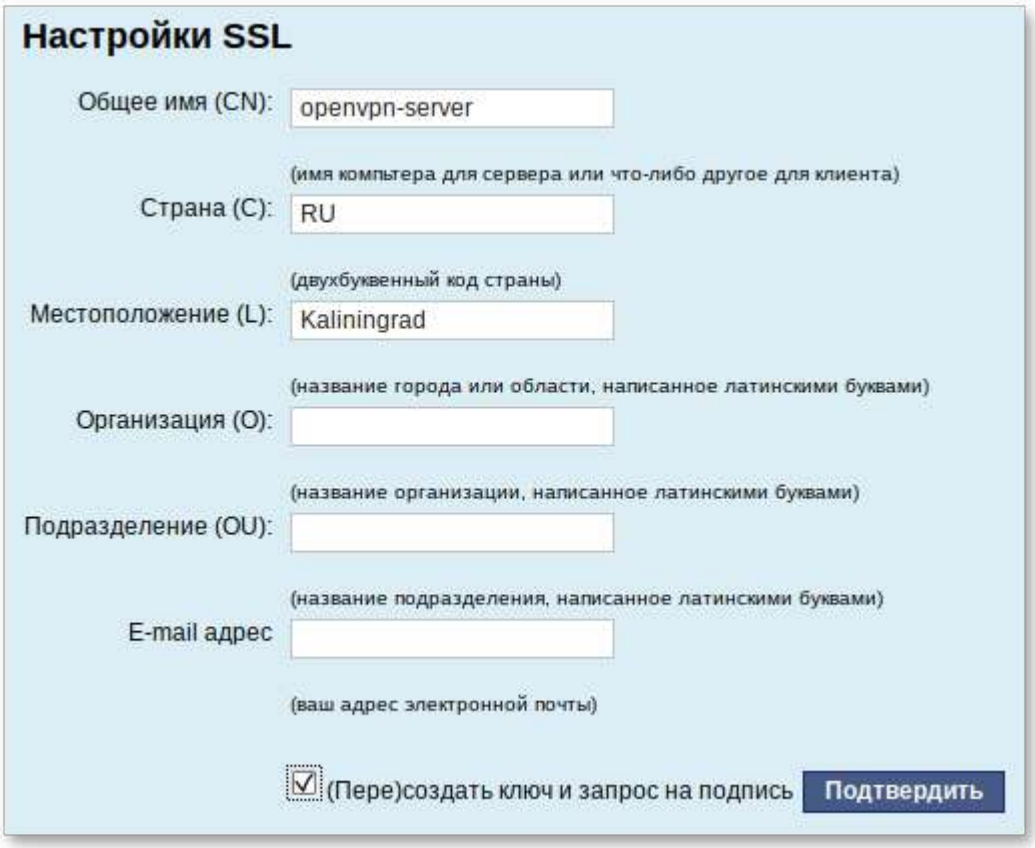
Используя модуль **OpenVPN-сервер** можно:

- включить/отключить OpenVPN-сервер;
- настроить параметры сервера: тип, сети сервера, использование сжатия и т.д.;
- управлять сертификатами сервера;
- настроить сети клиентов.

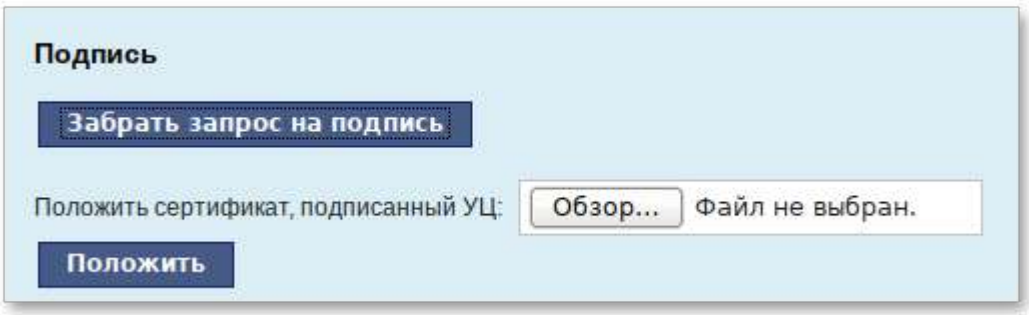
Особое внимание при планировании и настройке подключений следует обратить на используемые сети. Они *не должны* пересекаться.

Для создания соединения необходимо установить флажок **Включить службу OpenVPN**, выбрать тип подключения: маршрутизируемое (используется TUN) или через мост (используется TAP), и проверить открываемую по соединению сеть (обычно это локальная сеть в виде IP-адреса и маски подсети).

Для настройки сертификата и ключа ssl необходимо нажать на кнопку **Сертификат и ключ ssl.**. Откроется окно модуля **Управление ключами SSL** (пакет *alterator-sslkey*):

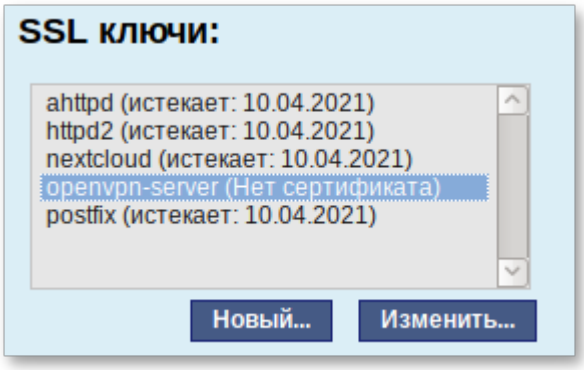


Здесь нужно заполнить поле **Общее имя (CN)** и поле **Страна (C)** (прописными буквами), отметить пункт **(Пере)создать ключ и запрос на подпись** и нажать кнопку **Подтвердить**. После чего станет активной кнопка **Забрать запрос на подпись**:



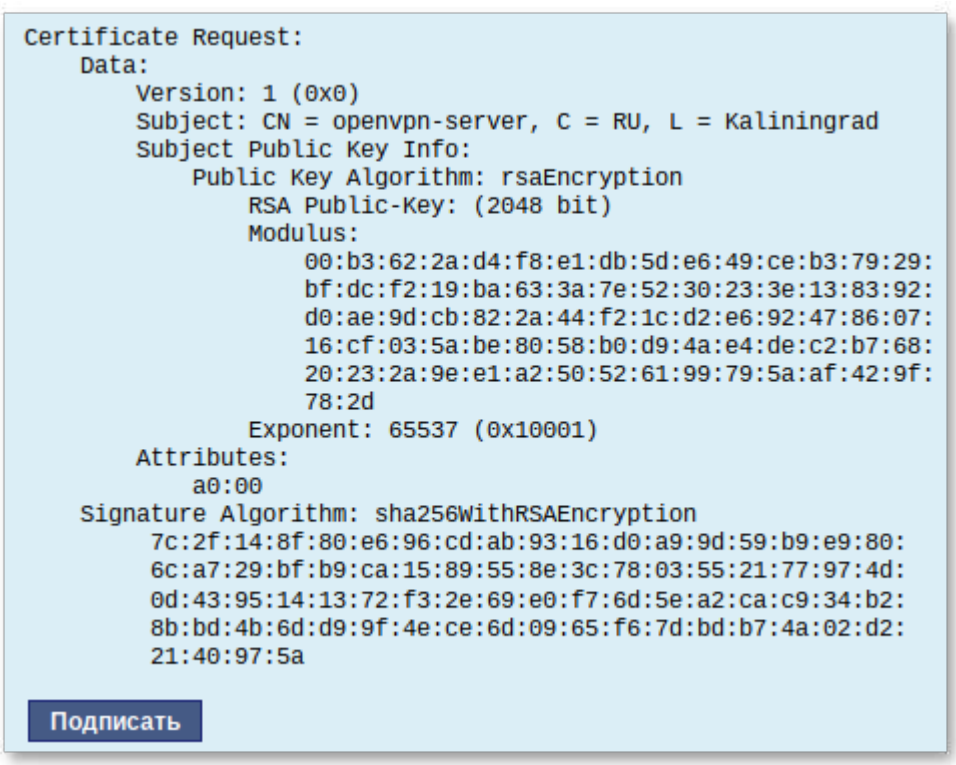
Если нажать на кнопку **Забрать запрос на подпись**, появится диалоговое окно с предложением сохранить файл **openvpn-server.csr**. Необходимо сохранить этот файл на диске.

В модуле **Управление ключами SSL** появился новый ключ *openvpn-server (Нет сертификата)*:

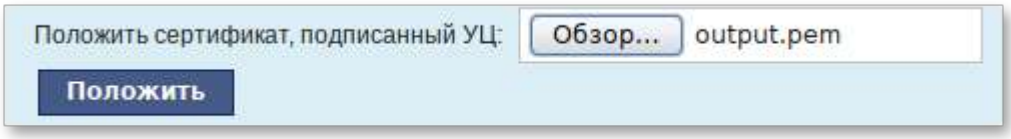


Чтобы подписать сертификат, необходимо перейти в модуль **Удостоверяющий Центр** → **Управление сертификатами**, нажать кнопку **Обзор**, указать путь до полученного файла **openvpn-server.csr** и загрузить запрос:

В результате на экране появится две группы цифр и кнопка **Подписать**. Необходимо нажать на кнопку **Подписать** и сохранить файл **output.pem** (подписанный сертификат).

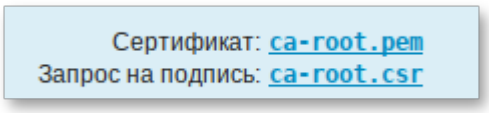


Далее в разделе **Управление ключами SSL**, необходимо выделить ключ *openvpn-server (Нет сертификата)* и нажать кнопку **Изменить**. В появившемся окне, в пункте **Положить сертификат, подписанный УЦ** нужно нажать кнопку **Обзор**, указать путь до файла **output.pem** и нажать кнопку **Положить**:



В модуле **Управление ключами SSL**, видно, что изменился ключ *openvpn-server (истекает_и_дата)*. Ключ создан и подписан.

Для того чтобы положить сертификат УЦ, необходимо найти его в модуле **Удостоверяющий Центр**, нажать на ссылку **Управление УЦ** и забрать сертификат, нажав на ссылку **Сертификат: ca-root.pem**:



В модуле **OpenVPN-сервер**, в графе **Положить сертификат УЦ**: при помощи кнопки **Обзор** указать путь к файлу **ca-root.pem** и нажать кнопку **Положить**:

Появится сообщение: «Сертификат УЦ успешно загружен».

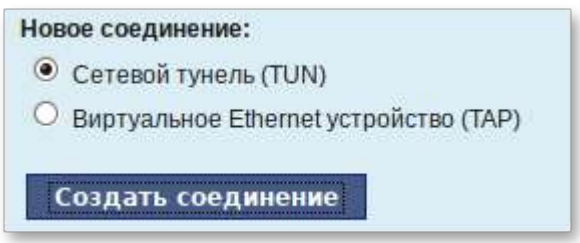
Для включения OpenVPN необходимо отметить пункт **Включить службу OpenVPN** и нажать кнопку **Применить**.

Если необходимо организовать защищённое соединение между двумя локальными сетями, воспользуйтесь модулем **OpenVPN-соединения** (раздел **Сеть**).

40.2. Настройка клиентов

Со стороны клиента соединение настраивается в модуле ЦУС **OpenVPN-соединения** (пакет *alterator-net-openvpn*) из раздела **Сеть**. Доступ к настроенной приватной сети могут получить пользователи, подписавшие свои ключи и получившие сертификат в удостоверяющем центре на том же сервере.

Для создания нового соединения необходимо отметить пункт **Сетевой туннель (TUN)** или **Виртуальное Ethernet устройство (TAP)** и нажать кнопку **Создать соединение**. Должен быть выбран тот же тип, что и на стороне сервера.



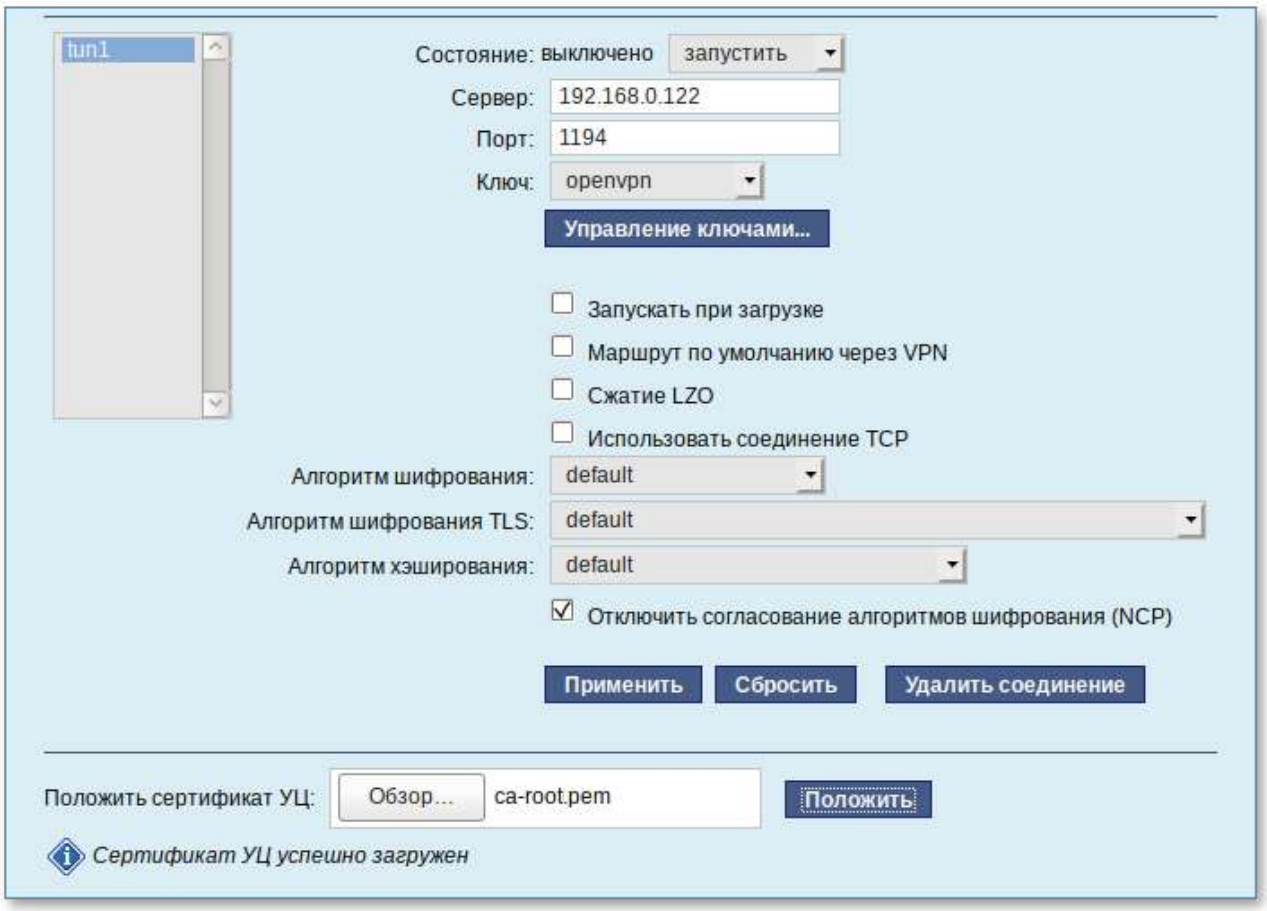
Обратите внимание, что на стороне клиента, должен быть выбран тот же тип виртуального устройства, что и на стороне сервера. Для большинства случаев подходит маршрутизируемое подключение.

Помимо этого нужно подписать ключ **openvpn** в модуле **Удостоверяющий Центр** (пакет *alterator-ca*) из раздела **Система**.

В результате станут доступны настройки соединения. На клиенте в модуле OpenVPN-соединение необходимо указать:

- **Состояние** — «запустить»;
- **Сервер** — IP адрес сервера или домен;
- **Порт** — 1194;
- **Ключ** — выбрать подписанный на сервере ключ.

Для применения настроек, нажать кнопку **Применить**. Состояние с **Выключено** должно поменяться на **Включено**.



Проверить, появилось ли соединение с сервером можно командой

```
ip addr
```

должно появиться новое соединение tun1. При обычных настройках это может выглядеть так:

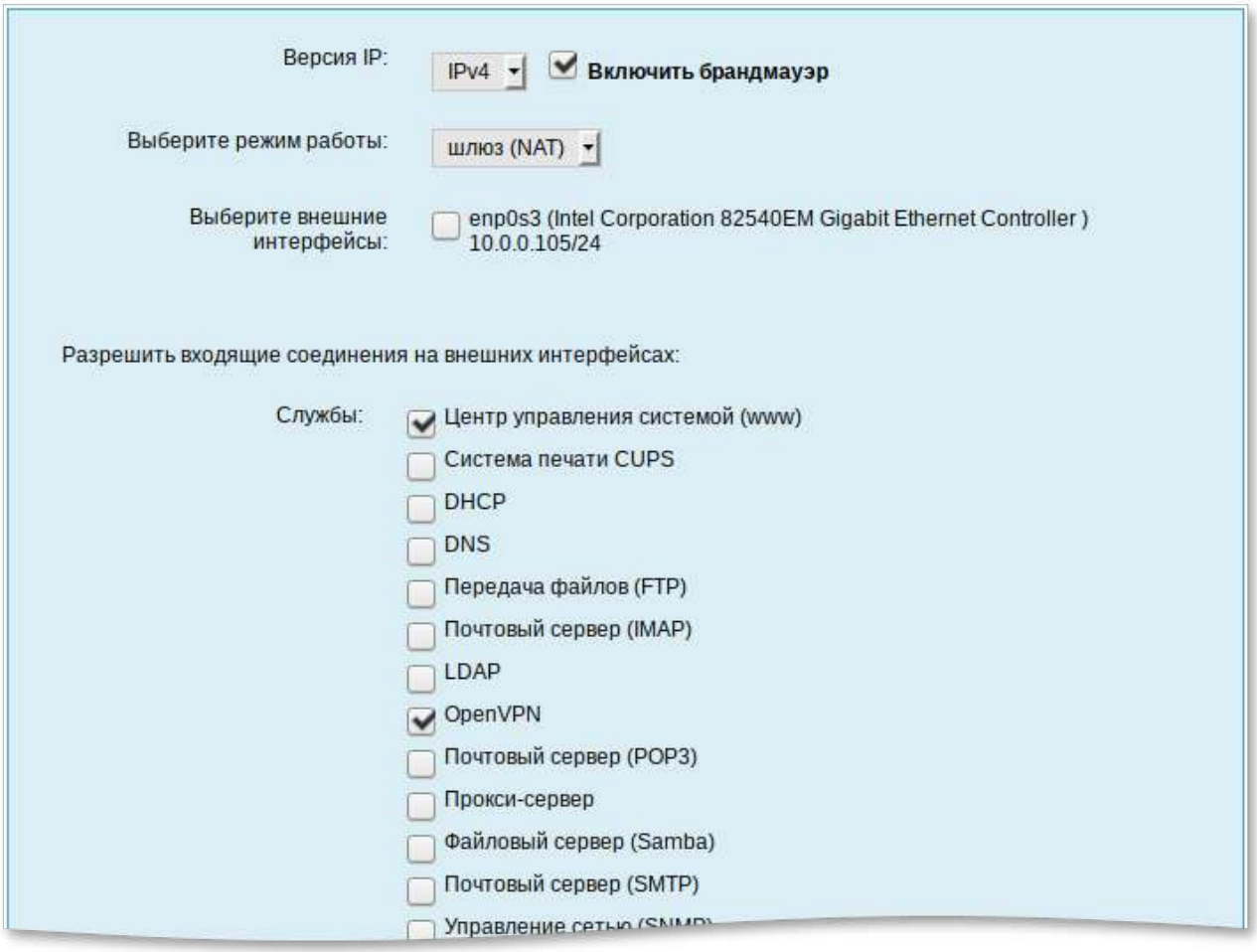
```
tun1: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UNKNOWN qlen 100
   link/[none]
   inet 10.8.0.6 peer 10.8.0.5/32 scope global tun0
```

Глава 41. Доступ к службам сервера из сети Интернет

41.1. Внешние сети

Сервер предоставляет возможность организовать доступ к своим службам извне. Например, можно предоставить доступ к корпоративному веб-сайту из сети Интернет. Для обеспечения такой возможности необходимо разрешить входящие соединения на внешних интерфейсах. По умолчанию такие соединения блокируются.

Для разрешения внешних и внутренних входящих соединений предусмотрен раздел ЦУС **Брандмауэр**. В списке **Разрешить входящие соединения на внешних интерфейсах** модуля **Внешние сети** (пакет *alterator-net-iptables*) перечислены наиболее часто используемые службы, отметив которые, вы делаете их доступными для соединений на внешних сетевых интерфейсах. Если вы хотите предоставить доступ к службе, отсутствующей в списке, задайте используемые этой службой порты в соответствующих полях.



Можно выбрать один из двух режимов работы:

- Роутер. В этом режиме перенаправление пакетов между сетевыми интерфейсами происходит без трансляции сетевых адресов.
- Шлюз (NAT). В этом режиме будет настроена трансляция сетевых адресов (NAT) при перенаправлении пакетов на внешние интерфейсы. Использование этого режима имеет смысл, если у вас настроен, по крайней мере, один внешний и один внутренний интерфейс.

Примечание

В любом режиме включено только перенаправление пакетов с внутренних интерфейсов. Перенаправление пакетов с внешних интерфейсов всегда выключено.

Примечание

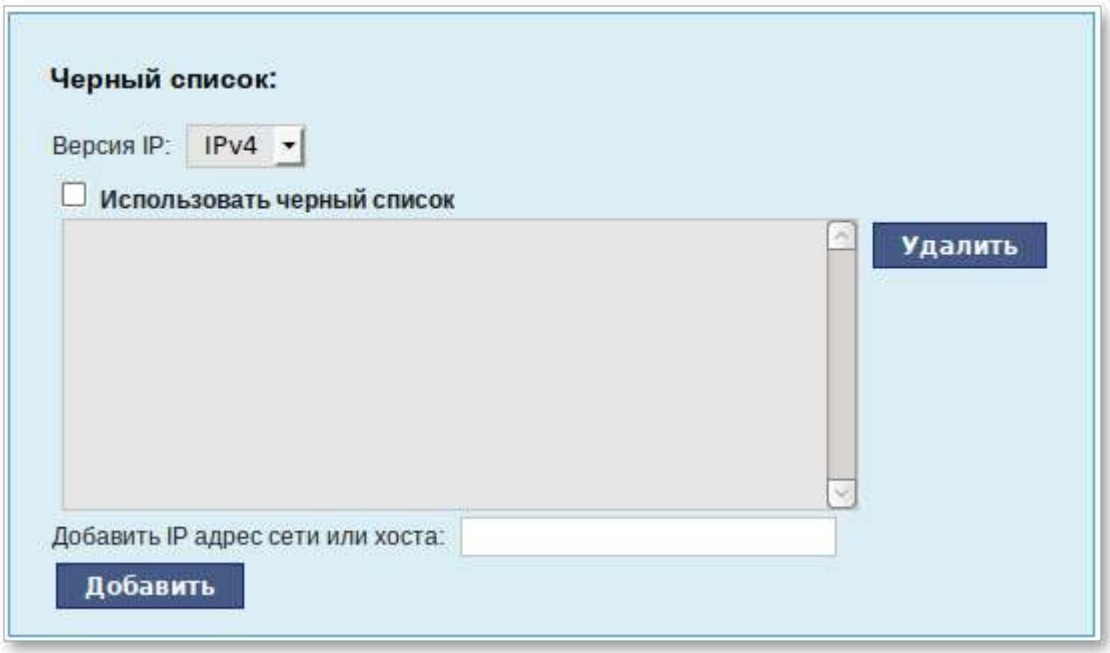
Все внутренние интерфейсы открыты для любых входящих соединений.

За дополнительной информацией по настройке обращайтесь к встроенной справке модуля ЦУС.

41.2. Список блокируемых хостов

Модуль ЦУС **Список блокируемых хостов** (пакет *alterator-net-bl*) предназначен для блокирования любого трафика с указанными узлами. Данный модуль позволяет блокировать любой сетевой трафик с указанных в списке узлов (входящий, исходящий и пересылаемый).

Блокирование трафика с указанных в списке узлов начинается после установки флажка **Использовать чёрный список**.



Для добавления блокируемого узла необходимо ввести IP-адрес в поле **Добавить IP адрес сети или хоста** и нажать кнопку **Добавить**.

Для удаления узла из списка выберите его и нажмите кнопку **Удалить**.

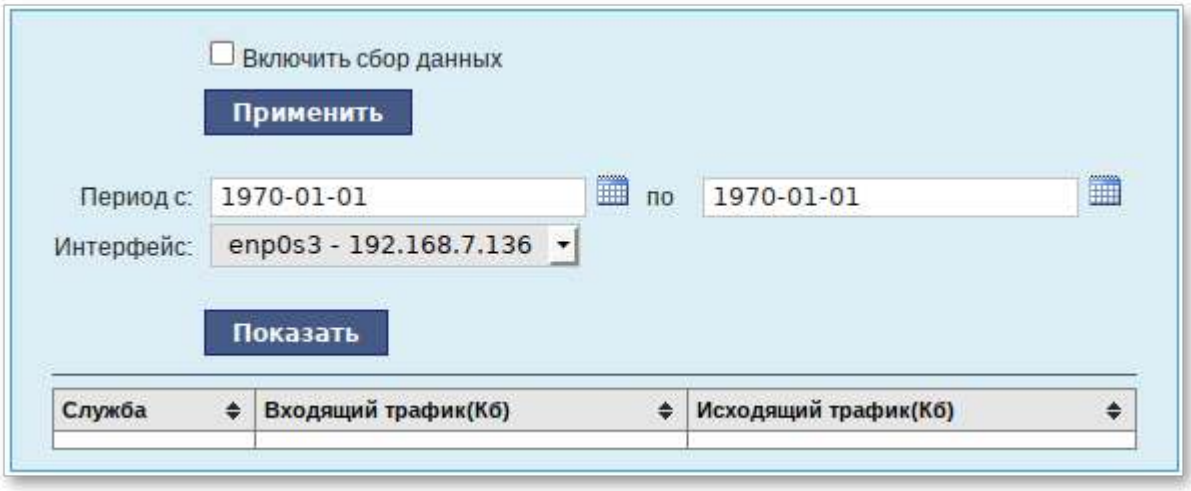
Глава 42. Статистика

42.1. Сетевой трафик

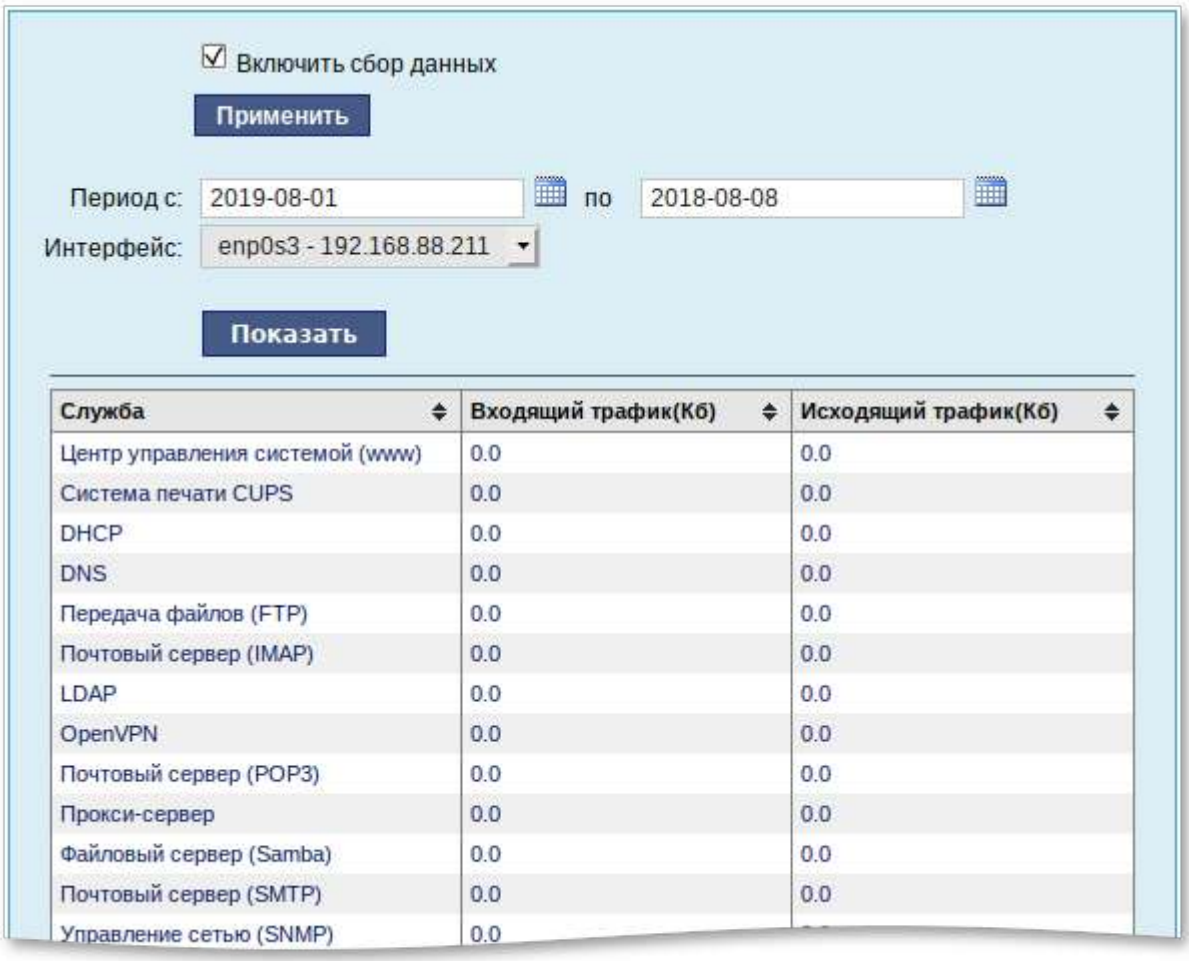
Все входящие и исходящие с сервера сетевые пакеты могут подсчитываться, и выводится по запросу для анализа.

Модуль **Сетевой трафик** (пакет *alterator-ulogd*) из раздела **Статистика** предназначен для просмотра статистики входящих и исходящих с сервера сетевых пакетов. Данный модуль позволяет оценить итоговый объём полученных и переданных данных за всё время работы сервера, за определённый период времени и по каждой службе отдельно.

Для включения сбора данных необходимо установить флажок **Включить сбор данных**, и нажать кнопку **Применить**.



Для просмотра статистики укажите период (в виде начальной и конечной дат). Дата указывается в формате YYYY-MM-DD (год-месяц-день) или выбирается из календаря справа от поля ввода даты. Из списка доступных сетевых интерфейсов необходимо выбрать интересующий и нажать на кнопку **Показать**.



Трафик на указанном интерфейсе за заданный период показывается в виде:

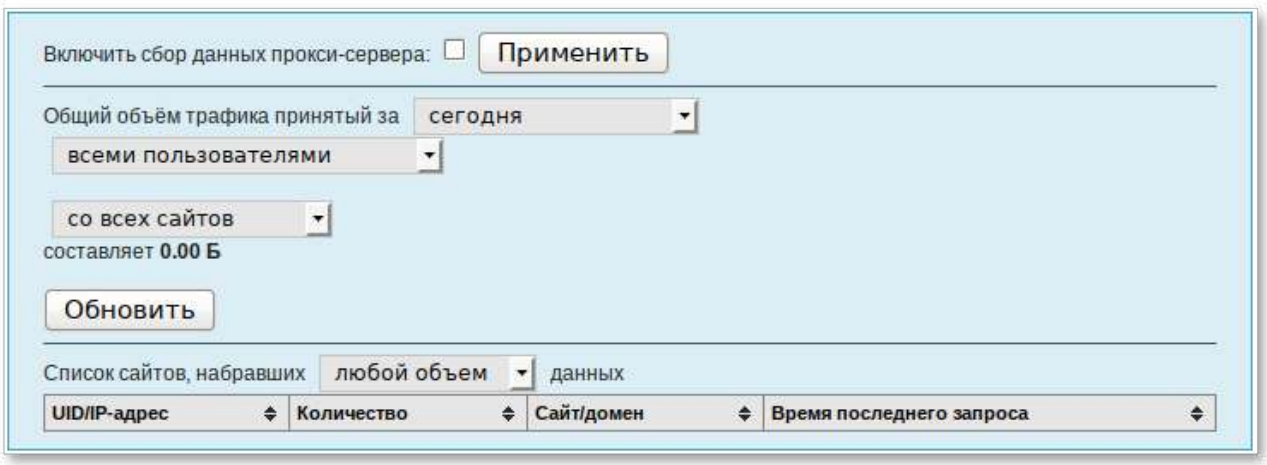
- служба (название протокола);
- входящий трафик в килобайтах;

- исходящий трафик в килобайтах.

42.2. Прокси-сервер

Пересылка каждого запроса во внешнюю сеть фиксируется прокси-сервером в специальном журнале. На основании этих данных автоматически формируются отчёты о статистике использования ресурсов сети, в том числе потраченного времени и количества переданных данных (трафика).

Статистика не собирается по умолчанию. Для включения сбора статистики и просмотра отчётов воспользуйтесь модулем ЦУС **Прокси-сервер** (пакет *alterator-squidmill*) из раздела **Статистика**.



Для включения сбора статистики прокси-сервера установите флажок **Включить сбор данных прокси-сервера**.

В том случае, если на прокси-сервере производилась аутентификация пользователей, отчёты будут содержать данные об обращениях каждого пользователя. Иначе отчёты будут формироваться только на основании адресов локальной сети.

Для показа отчёта задайте условия фильтра и нажмите кнопку **Показать**. Данные в таблице будут отсортированы по объёму трафика в порядке убывания.

Для учёта пользователей в статистике необходимо добавить хотя бы одно правило. Самое очевидное правило — запрет неаутентифиуцированных пользователей. Только после этого в статистике начнут показываться пользователи.

Глава 43. Обслуживание сервера

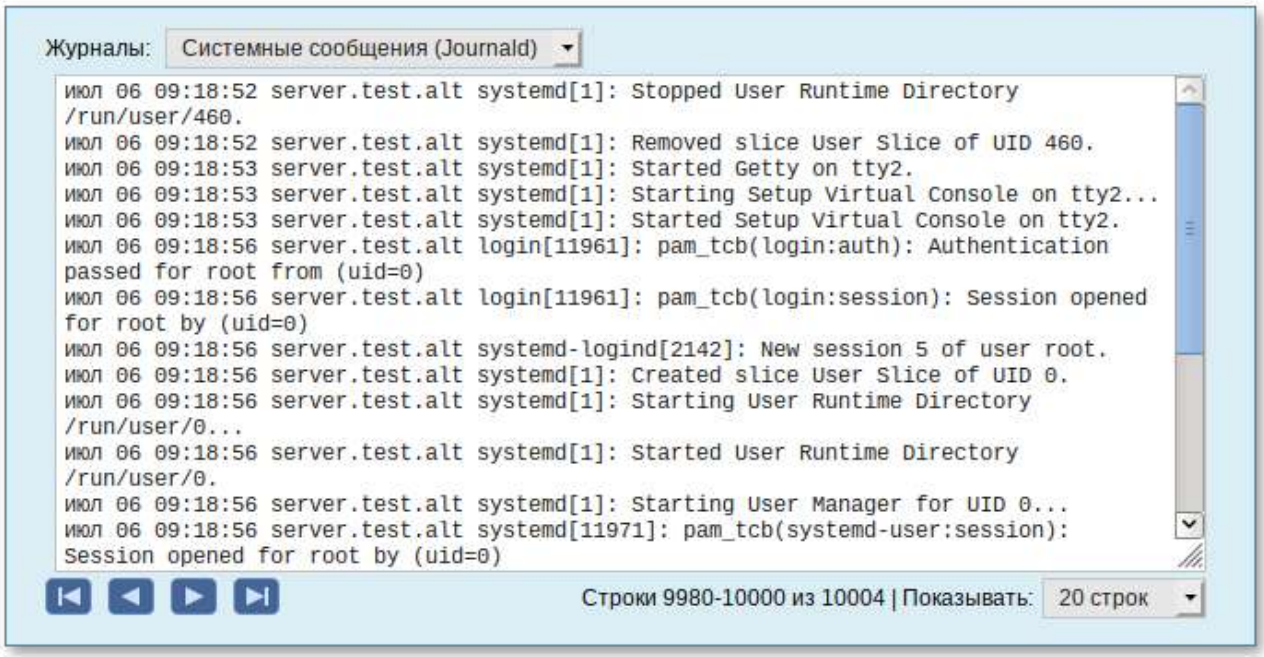
Для безотказной работы всего домена очень важно следить за корректной работой его центрального звена — сервера под управлением Альт Сервер. Регулярный мониторинг состояния сервера, своевременное резервное копирование, обновление установленного ПО являются важной частью комплекса работ по обслуживанию сервера.

43.1. Мониторинг состояния системы

Для обеспечения бесперебойной работы сервера крайне важно производить постоянный мониторинг его состояния. Все события, происходящие с сервером, записываются в *журналы*, анализ которых помогает избежать сбоев в работе сервера и предоставляет возможность разобраться в причинах некорректной работы сервера.

Для просмотра журналов предназначен модуль ЦУС **Системные журналы** (пакет *alterator-logs*) из раздела **Система**). Интерфейс позволяет просмотреть различные типы журналов с возможностью перехода к более старым или более новым записям.

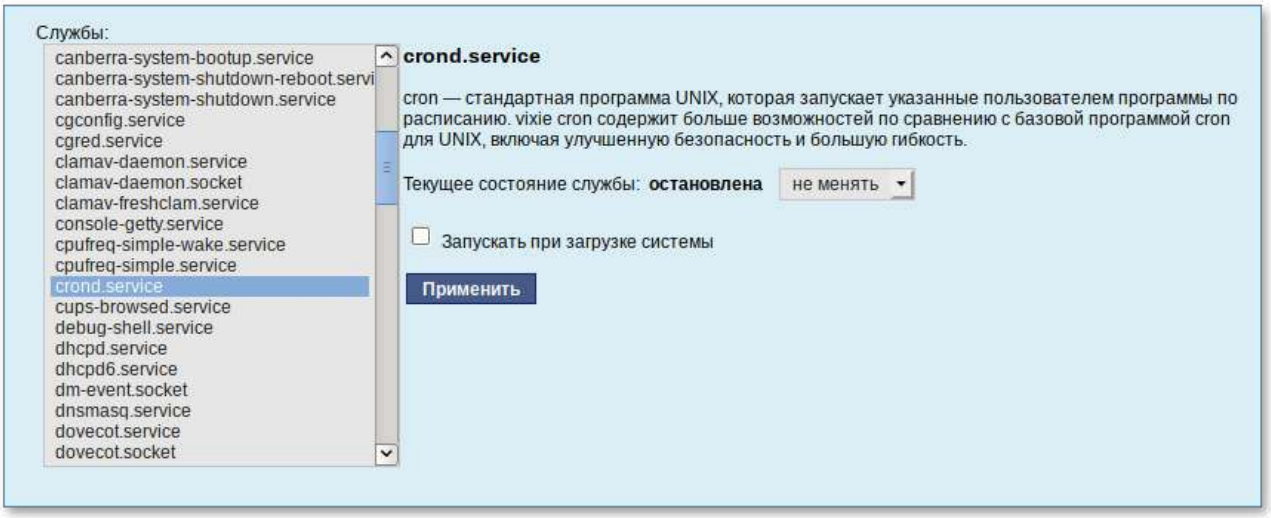
Различные журналы могут быть выбраны из списка **Журналы**.



Каждый журнал может содержать довольно большое количество сообщений. Уменьшить либо увеличить количество выводимых строк можно, выбрав нужное значение в списке **Показывать**.

43.2. Системные службы

Для изменения состояния служб можно использовать модуль ЦУС **Системные службы** (пакет *alterator-services*) из раздела **Система**. Интерфейс позволяет изменять текущее состояние службы и, если необходимо, применить опцию запуска службы при загрузке системы.



После выбора названия службы из списка отображается описание данной службы, а также текущее состояние: Работает/Остановлена/Неизвестно.

43.3. Резервное копирование

Резервное копирование является важной частью работ по поддержанию работоспособности сервера и всего домена. Так как сервер является критичной частью сети, производите регулярное резервное копирование. При возникновении нештатных ситуаций, например, выхода из строя оборудования, вы сможете восстановить работоспособное состояние сервера из резервной копии.

Ниже перечислены модули, с помощью которых можно настроить резервное копирование.

План резервного копирования и дополнительные параметры настраиваются в модуле ЦУС **Резервное копирование**. Этот же модуль может использоваться и для восстановления данных.

Bacula — кроссплатформенное клиент-серверное программное обеспечение, позволяющее управлять резервным копированием, восстановлением, и проверкой данных по сети для компьютеров и операционных систем различных типов.

Функционально Bacula состоит из компонентов (служб), каждая из которых реализует определенные функции.

Структура:

- Bacula Director — процесс управляющий системой в целом (управление, планирование, восстановление резервных копий).
- Storage Director — запускается на сервере, отвечающем за «физическое» хранение данных.
- File Director — сервис, запускаемый на каждом из клиентов.
- Bconsole — консоль управления.

Копирование, восстановление, верификация и административные функции оформляются в виде задания (Job). В задании задается набор файлов (FileSet), который нужно копировать, компьютер (Client), с которого надо копировать файлы, время копирования (Schedule), пул (Pool), куда копировать и дополнительные директивы.

Задания на копирование данных определяются в конфигурационном файле Директора (Director) и там же определяется график автоматического запуска этих заданий. Директор выполняется постоянно как демон в фоновом режиме и запускает задания на копирование в соответствии с графиком. Администратор (пользователь) может также вручную запустить эти задания в любое время, используя Службу Консоль.

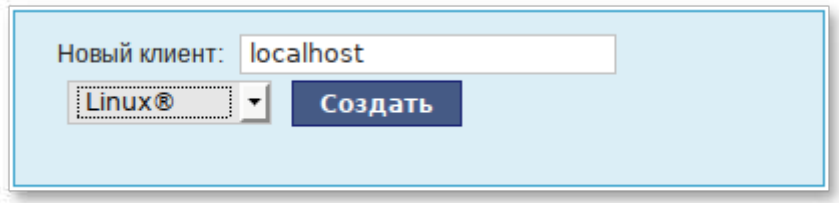
Файлы настройки **Bacula** форматированы на основе ресурсов, включающих директивы, обрамленные фигурными скобками "{}". Каждый компонент **Bacula** имеет индивидуальный файл в каталоге **/etc/bacula**.

Различные компоненты **Bacula** должны авторизовывать себя друг для друга. Это решается использованием директивы password. Например, пароль в ресурсе Storage файла **/etc/bacula/bacula-dir.conf** должен соответствовать паролю ресурса Director файла **/etc/bacula/bacula-sd.conf**.

В дистрибутиве установленная из пакетов **Bacula** уже настроена для резервного копирования конфигурации ОС. Основным диспетчером резервного копирования является Bacula Director. Дополнительно его настраивать не нужно.

Для того чтобы начать резервное копирование самого сервера или рабочей станции, необходимо выполнить следующие шаги:

- перейти в раздел **Сервер резервного копирования → Клиенты**

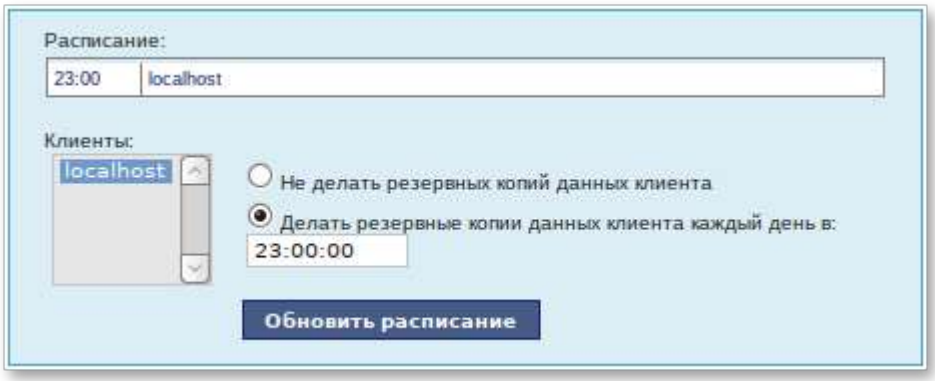


- указать имя узла (для сервера это будет localhost) и операционную систему. Нажать кнопку **Создать**;
- указать пароль для клиента и включаемые и исключаемые каталоги;
- нажать на кнопку **Сохранить параметры**;
- нажать ссылку "Конфигурационный файл клиента" и сохраните файл **<имя узла>-fd.bin** на локальном компьютере;
- скопировать полученный файл на рабочую станцию или сервер. Под Linux этот файл нужно сохранить под именем **/etc/bacula/bacula-fd.conf**;
- запустить на компьютере, где создаётся резервная копия, службу *bacula-fd* (в дистрибутиве Альт Рабочая станция пакет *bacula-client*).

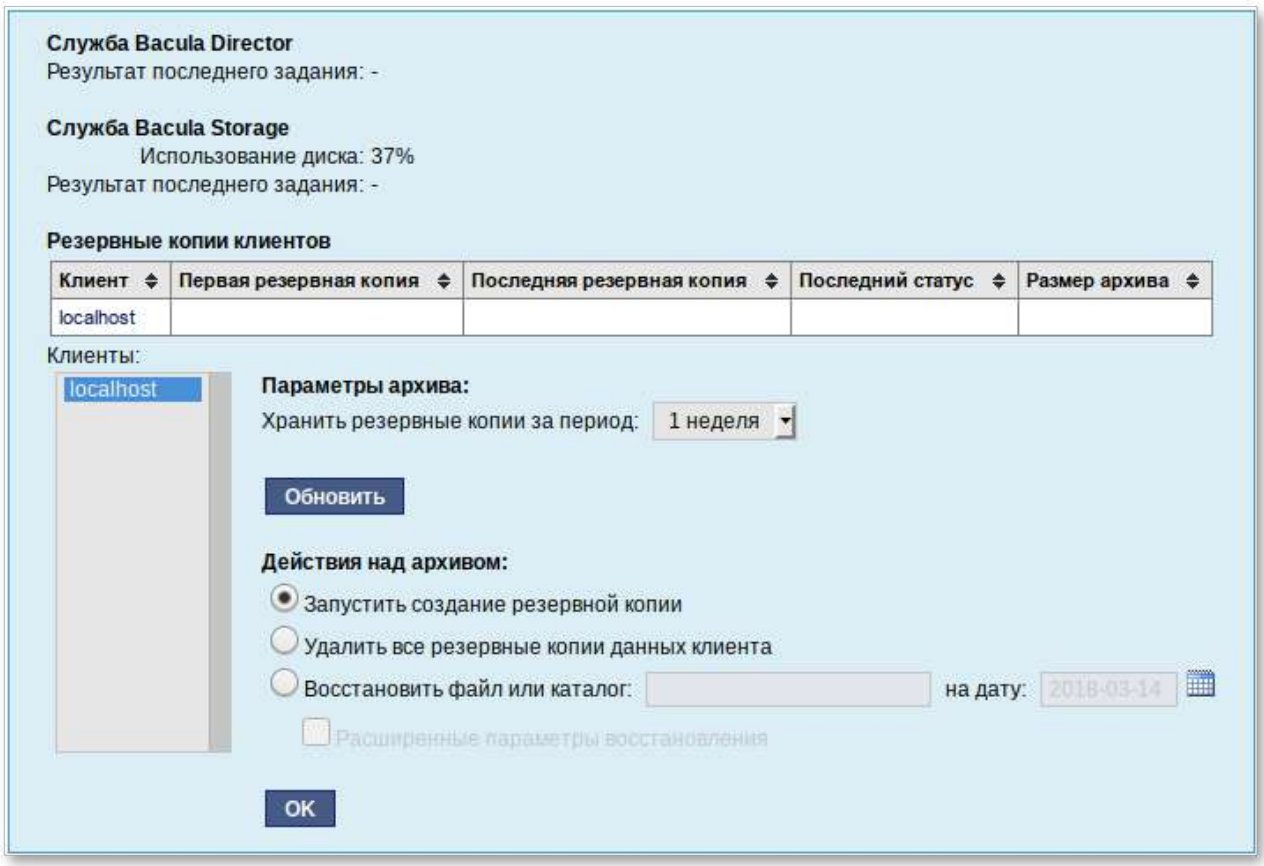
Примечание

Для клиента под управлением ОС Linux по умолчанию создаётся резервная копия всей файловой системы, кроме каталогов с временными и служебными файлами: **/dev**, **/.fsck**, **/.journal**, **/media**, **/mnt**, **/opt**, **/proc**, **/srv**, **/sys**, и **/tmp**.

В разделе **Сервер резервного копирования → Расписание** указывается время проведения инкрементного резервного копирования для каждого клиента. Удостоверьтесь, что в это время на клиенте служба *bacula-fd* запущена. В этом же разделе можно отключить резервное копирование для выбранных клиентов.



Модуль **Архив** (раздел **Сервер резервного копирования**) для выбранного клиента (выбирается из списка **Клиенты**) позволяет запустить создание резервной копии вне расписания, удалить все резервные копии или восстановить данные этого клиента.



Расширенные параметры восстановления позволяют задать целевой каталог восстановления.

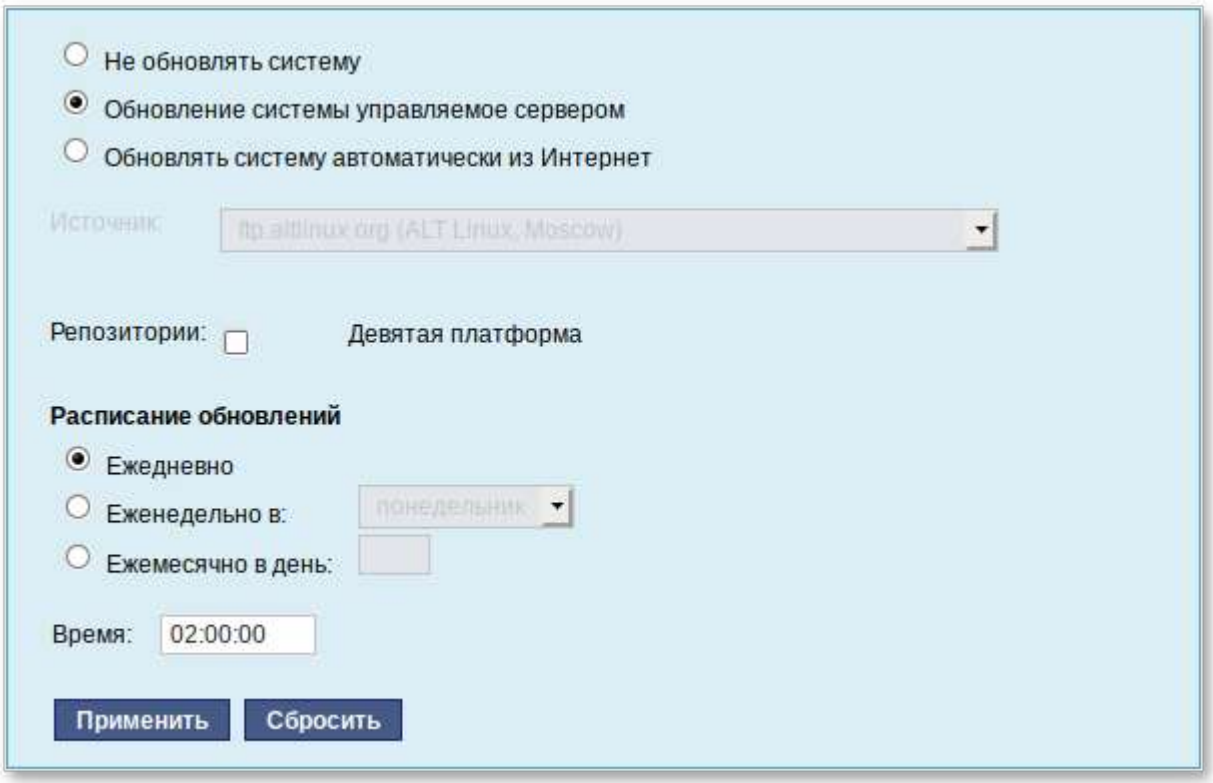
Этот модуль также позволяет:

- посмотреть общую информацию о доступном месте на диске;
- посмотреть состояние и размер архива для каждого клиента;
- принудительно запустить создание резервной копии;
- удалить резервную копию клиента;
- восстановить файл или каталог на выбранную дату.

43.4. Обновление системы

После установки системы крайне важно следить за обновлениями ПО. Обновления для Альт Сервер могут содержать как исправления, связанные с безопасностью, так и новый функционал или просто улучшение и ускорение алгоритмов. В любом случае настоятельно рекомендуется регулярно обновлять систему для повышения надёжности работы сервера.

Для автоматизации процесса установки обновлений предусмотрен модуль ЦУС **Обновление системы** (пакет *alterator-updates*) из раздела **Система**. Здесь можно включить автоматическое обновление через Интернет с одного из предлагаемых серверов или задать собственные настройки.



Источник обновлений указывается явно (при выбранном режиме **Обновлять систему автоматически из сети Интернет**) или вычисляется автоматически (при выбранном режиме **Обновление системы управляемое сервером** и наличии в локальной сети настроенного сервера обновлений).

Процесс обновления системы будет запускаться автоматически согласно заданному расписанию.

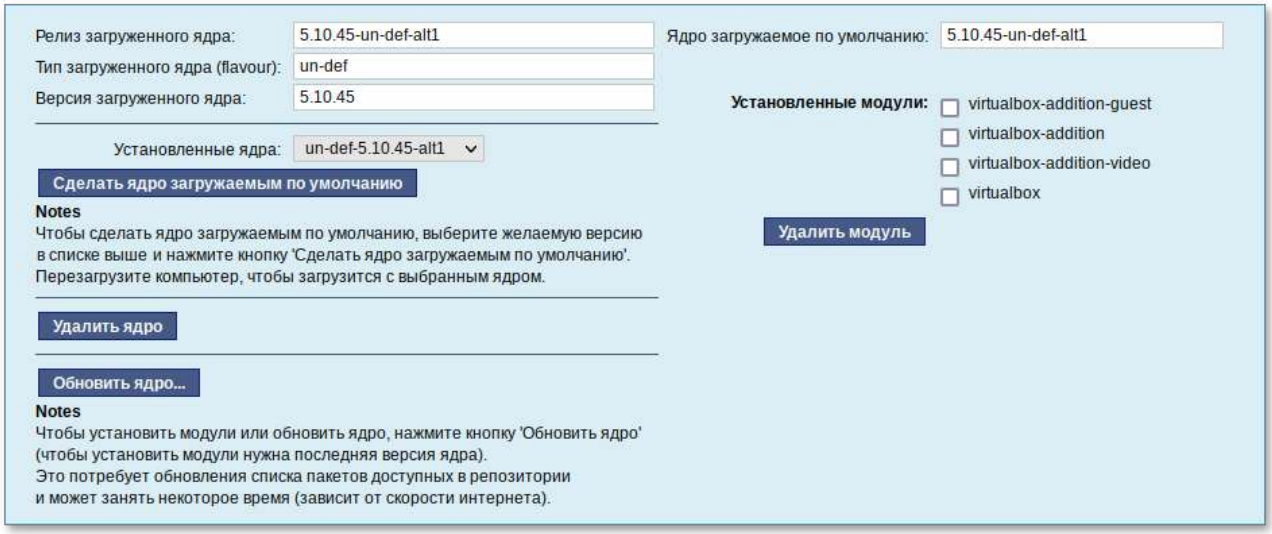
43.5. Обновление ядра ОС

Модуль ЦУС **Обновление ядра** (пакет *alterator-update-kernel*) из раздела **Система** реализует функционал утилиты **`update-kernel`**. Данный модуль предоставляет возможность:

- просматривать список установленных ядер;
- устанавливать, обновлять и удалять ядра;
- задавать ядро, загружаемое по умолчанию;

- устанавливать/удалять отдельные модули ядра.

В главном окне модуля отображается ядро, загруженное по умолчанию, и список установленных модулей ядра:



В дистрибутиве Альт Сервер можно установить несколько версий ядра одного и того же типа одновременно. После установки или обновления ядра старые ядра не удаляются.

В случае возникновения проблем с новым ядром можно переключиться на установленное ранее. Для этого следует выбрать нужное ядро в списке **Установленные ядра** и нажать кнопку **Сделать ядро загружаемым по умолчанию**.

Накопленный при обновлениях набор ранее установленных ядер можно удалить для освобождения дискового пространства. Для этого следует выбрать нужное ядро в списке **Установленные ядра** и нажать кнопку **Удалить ядро**.

Для того чтобы обновить ядро или установить модули ядра, следует нажать кнопку **Обновить ядро...**.

Примечание

При нажатии кнопки **Обновить ядро...** локальная база данных пакетов будет синхронизирована с удалённым репозиторием, это может занять некоторое время.

В открывшемся окне будет показано доступное к установке ядро. В выпадающем списке можно выбрать тип ядра. В окне **Доступные модули** отмечаются модули, которые будут установлены.

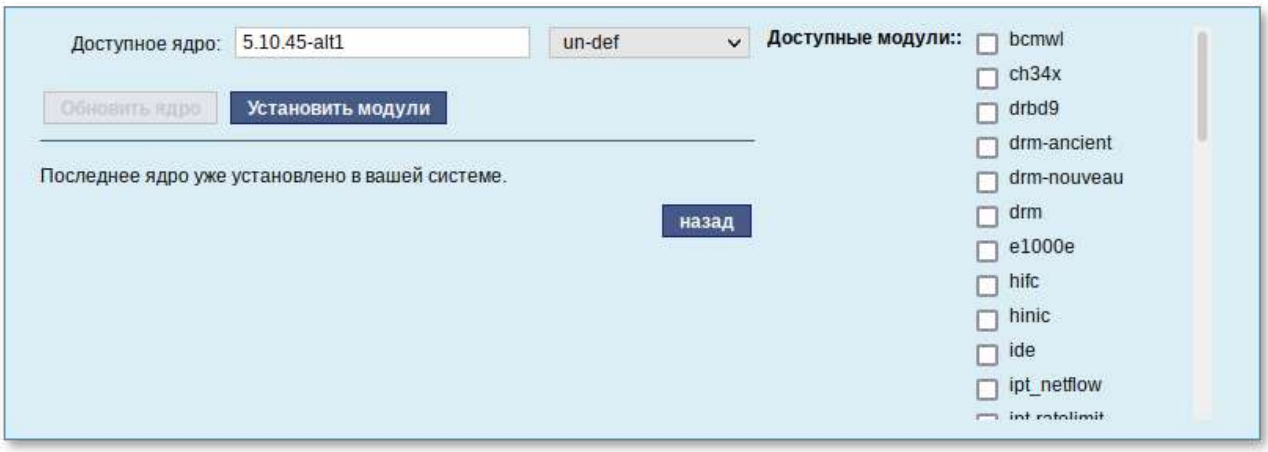
Чтобы обновить ядро, необходимо нажать кнопку **Обновить ядро**. Далее следует подтвердить желание обновить ядро нажатием кнопки **Да**.

Примечание

Новое ядро загрузится только после перезагрузки системы.

Если с новым ядром что-то пойдёт не так, вы сможете вернуться к предыдущему варианту, выбрав его в начальном меню загрузчика.

Если ядро не требует обновления, в окне **Доступные модули** можно отметить модули ядра необходимые к установке и нажать кнопку **Установить модули**.

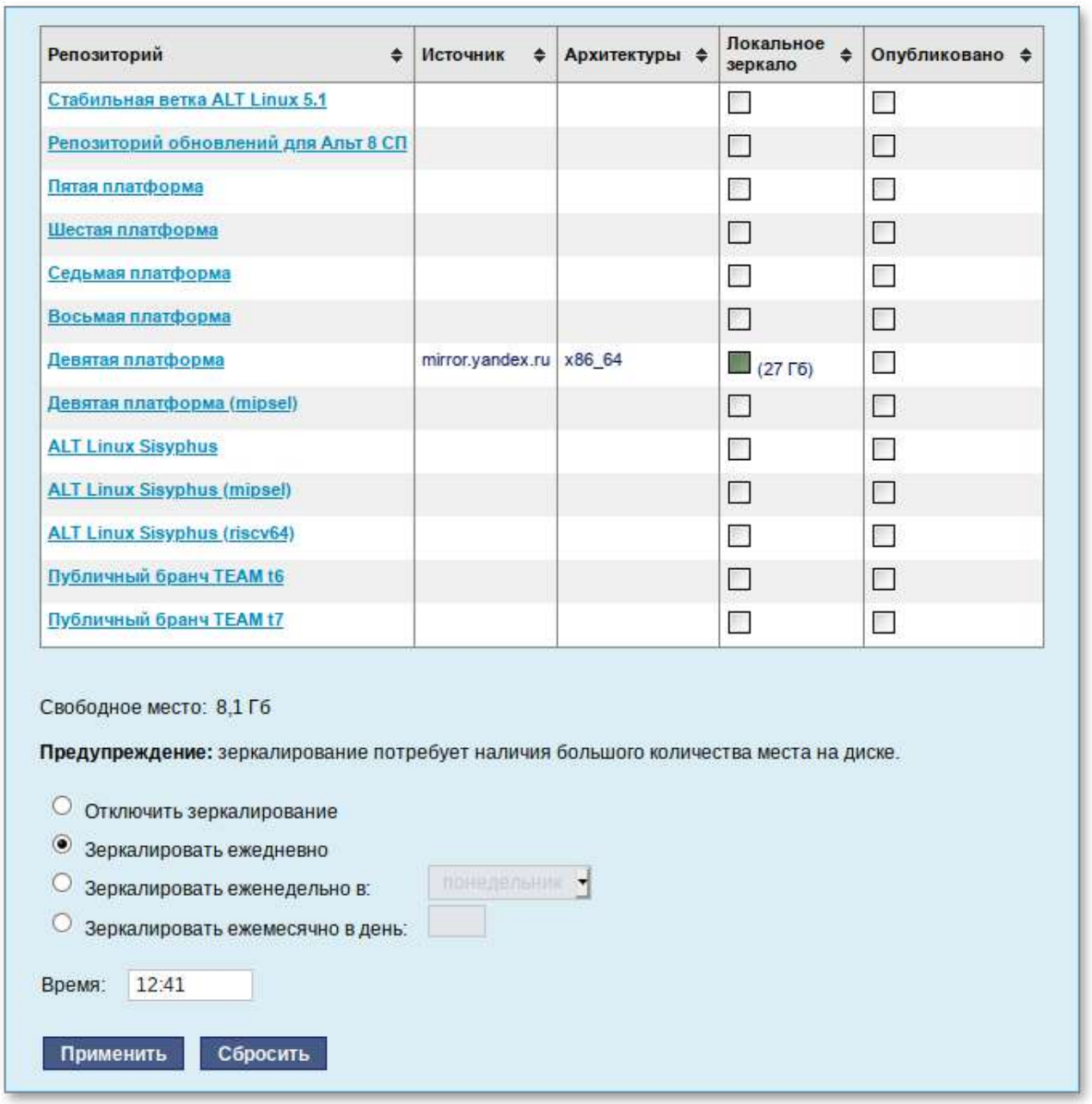


43.6. Обновление систем, не имеющих выхода в Интернет

Для систем, не имеющих прямого выхода в Интернет, рекомендуется установка отдельного сервера обновлений на базе ОС Альт Сервер, находящегося вне защищенного контура и организация ограниченного доступа к этому серверу.

Модуль ЦУС **Сервер обновлений** (пакет *alterator-mirror*) из раздела **Серверы** предназначен для зеркалирования репозиториев и публикации их для обновлений рабочих станций и серверов.

Сервер обновлений — технология, позволяющая настроить автоматическое обновление программного обеспечения, установленного на клиентских машинах (рабочих местах), работающих под управлением Альт Рабочая станция.

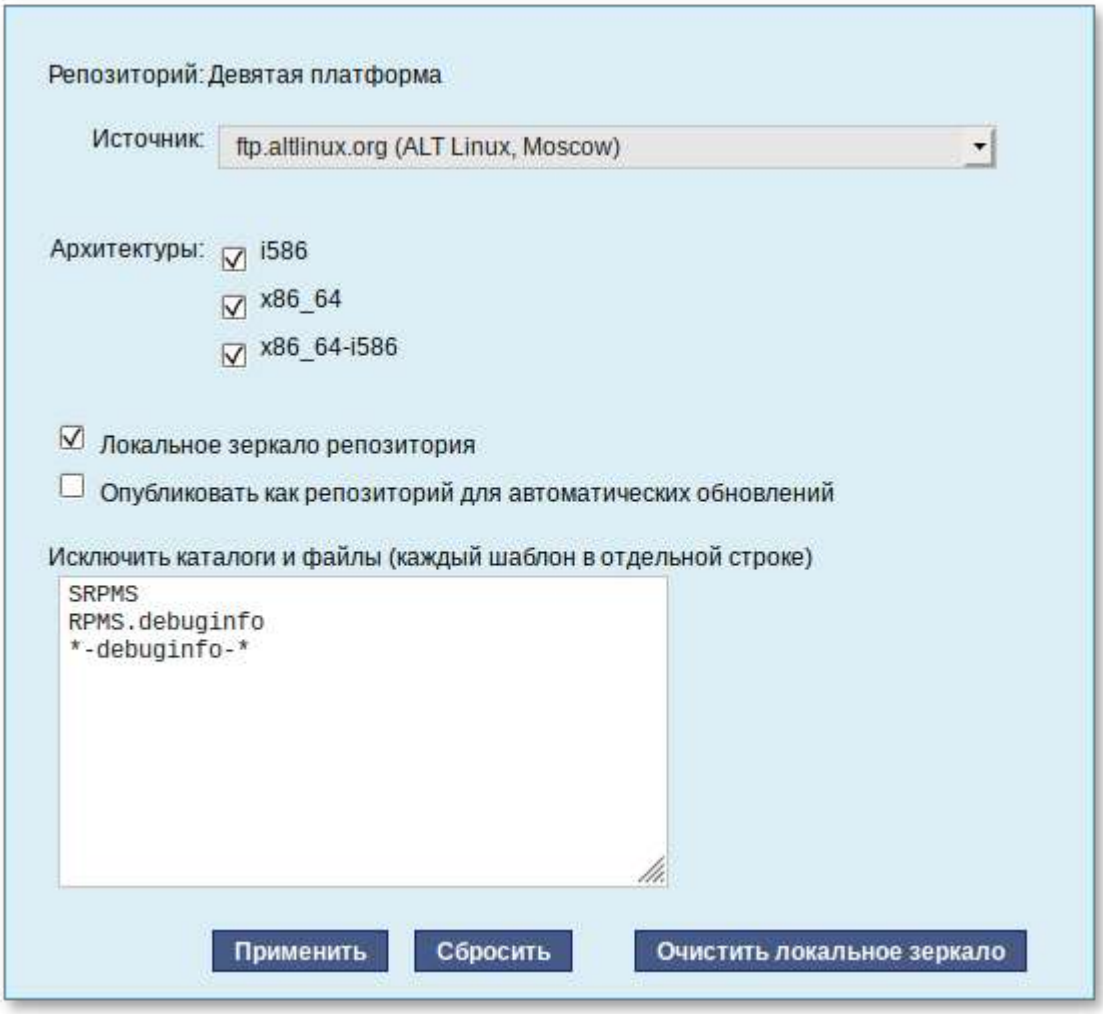


На странице модуля можно выбрать, как часто выполнять закачку пакетов, можно выставить время, когда начинать зеркалирование.

Здесь также можно выбрать репозитории, локальные срезы которых необходимы. При нажатии на название репозитория, появляются настройки этого репозитория. Необходимо выбрать источник (сайт, откуда будет скачиваться репозиторий), архитектуру процессора (если их несколько, то стоит выбрать соответствующие).

Примечание

При выборе любой архитектуры также будет добавлен источник с noarch.



Сервер обновлений предоставляет возможность автоматически настроить обновление клиентских машин в нужном режиме:

Локальное зеркало репозитория

В этом режиме на сервере создаётся копия удалённого репозитория. Загрузка ПО клиентскими машинами может производится с локального сервера по протоколам HTTP, HTTPS, FTP, rsync (для каждого протокола нужно настроить соответствующие службы, ниже приведён пример настройки HTTP- и FTP-сервера). Наличие на локальном сервере зеркала репозитория при большом количестве машин в сети позволяет существенно сэкономить трафик.

Важно

Зеркалирование потребует наличия большого количества места на диске.

Уменьшить размер скачиваемых файлов и занимаемое репозиторием место на диске можно, указав имена каталогов и файлов, которые будут исключены из синхронизации. Например, не скачивать пакеты с исходным кодом и пакеты с отладочной информацией:

```
SRPMS
*-debuginfo-*
```

Шаблоны указываются по одному в отдельной строке. Символ «*» используется для подстановки любого количества символов.

Публикация репозитория

В этом случае публикуется или URL внешнего сервера, содержащего репозиторий или, если включено локальное зеркало репозитория, адрес этого сервера. Такая публикация позволяет клиентским машинам автоматически настроить свои менеджеры пакетов на использование внешнего или локального репозитория.

Со стороны клиентских машин, в этом случае, необходимо настроить модуль **Обновление системы**, отметив в нём **Обновление системы управляемое сервером**.

Настройка локального репозитория заканчивается нажатием на кнопку **Применить**.

Примечание

По умолчанию локальное зеркало репозитория находится в **/srv/public/mirror**. Для того чтобы зеркалирование происходило в другую папку, необходимо эту папку примонтировать в папку **/srv/public/mirror**. Для этого в файл **/etc/fstab** следует вписать строку:

```
/media/disk/localrepo /srv/public/mirror none rw,bind,auto 0 0
```

где **/media/disk/localrepo** — папка-хранилище локального репозитория.

43.6.1. Настройка веб-сервера

Установить веб-сервер (в данном примере nginx):

```
# apt-get install nginx
```

Создать файл конфигурации сервера в **/etc/nginx/sites-available.d/repo.conf**:

```
server {
  listen 80;
  server_name localhost .local <ваш ip>;
```

```
  access_log /var/log/nginx/repo-access.log;
  error_log /var/log/nginx/repo-error.log;

  location /mirror {
    root /srv/public;
    autoindex on;
   }
}
```

Сделать ссылку в **/etc/nginx/sites-enabled.d/**:

```
# ln -s /etc/nginx/sites-available.d/repo.conf /etc/nginx/sites-enabled.d/
repo.conf
```

Запустить nginx и добавить его в автозагрузку:

```
# systemctl enable --now nginx
```

На клиентских машинах необходимо настроить репозитории. Сделать это можно в программе управления пакетами **Synaptic** (**Параметры** → **Репозитории**) или в командной строке:

```
# apt-repo rm all
# apt-repo add http://<ip сервера>/mirror/p9/branch
```

Проверить правильность настройки репозиториев:

```
# apt-repo
rpm http://192.168.0.185/mirror p9/branch/x86_64 classic
rpm http://192.168.0.185/mirror p9/branch/noarch classic
```

43.6.2. Настройка FTP-сервера

Установить пакеты vsftpd, lftp, если они еще не установлены:

```
# apt-get install vsftpd lftp
```

Настроить параметры использования vsftpd в файле **/etc/xinetd.d/vsftpd**:

```
# default: off
# description: The vsftpd FTP server.
service ftp
{
    disable = no # включает службу
    socket_type = stream
    protocol = tcp
    wait = no
    user = root
    nice = 10
    rlimit_as = 200M
    server = /usr/sbin/vsftpd
    only_from = 0/0 # предоставить доступ для всех IP
}
```

Перезапустить xinetd:

```
# systemctl restart xinetd
```

Изменить настройку прав доступа в файле **/etc/vsftpd/conf**:

```
local_enable=YES
```

Создать каталог **/var/ftp/mirror**:

```
# mkdir -p /var/ftp/mirror
```

Примонтировать каталог **/srv/public/mirror** в **/var/ftp/mirror** с опцией **--bind**:

```
# mount --bind /srv/public/mirror /var/ftp/mirror
```

Примечание

Для автоматического монтирования каталога **/srv/public/mirror** при загрузке системы необходимо добавить следующую строку в файл **/etc/fstab**:

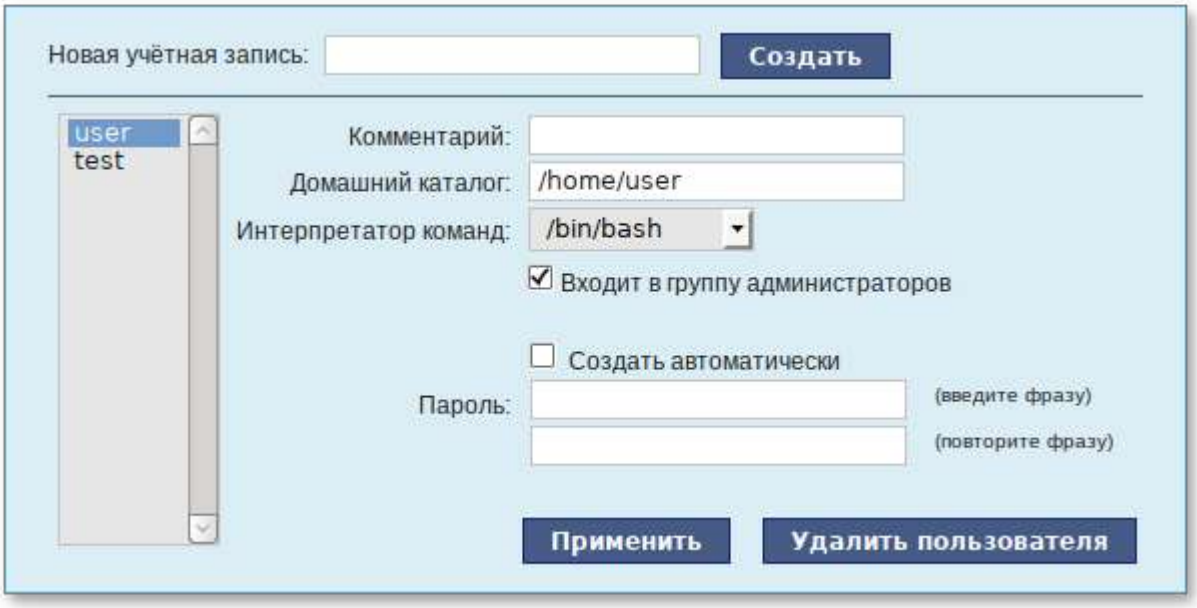
```
/srv/public/mirror /var/ftp/mirror none defaults,bind 0 0
```

На клиентских машинах необходимо настроить репозитории:

```
# apt-repo rm all
# apt-repo add ftp://<ip сервера>/mirror/p9/branch
# apt-repo
rpm ftp://192.168.0.185/mirror p9/branch/x86_64 classic
rpm ftp://192.168.0.185/mirror p9/branch/noarch classic
```

43.7. Локальные учётные записи

Модуль **Локальные учётные записи** (пакет *alterator-users*) из раздела **Пользователи** предназначен для администрирования системных пользователей.



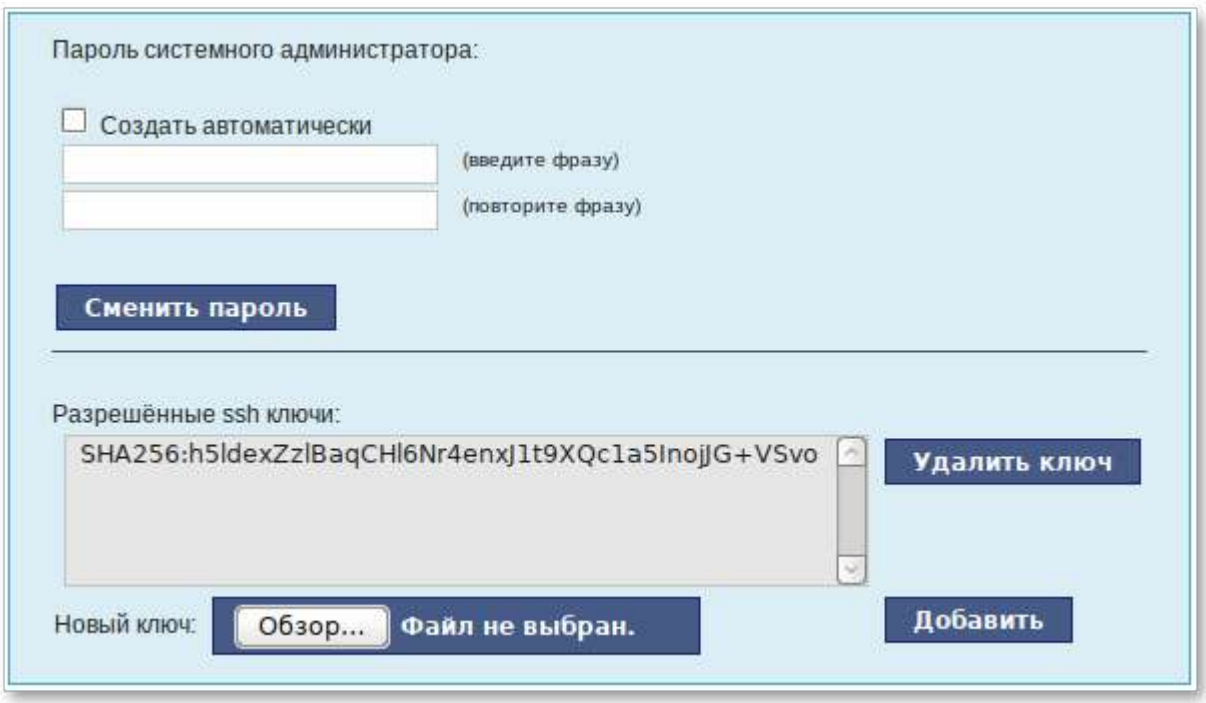
Для создания новой учётной записи необходимо ввести имя новой учётной записи и нажать кнопку **Создать**, после чего имя отобразится в списке слева.

Для дополнительных настроек необходимо выделить добавленное имя, либо, если необходимо изменить существующую учётную запись, выбрать её из списка.

43.8. Администратор системы

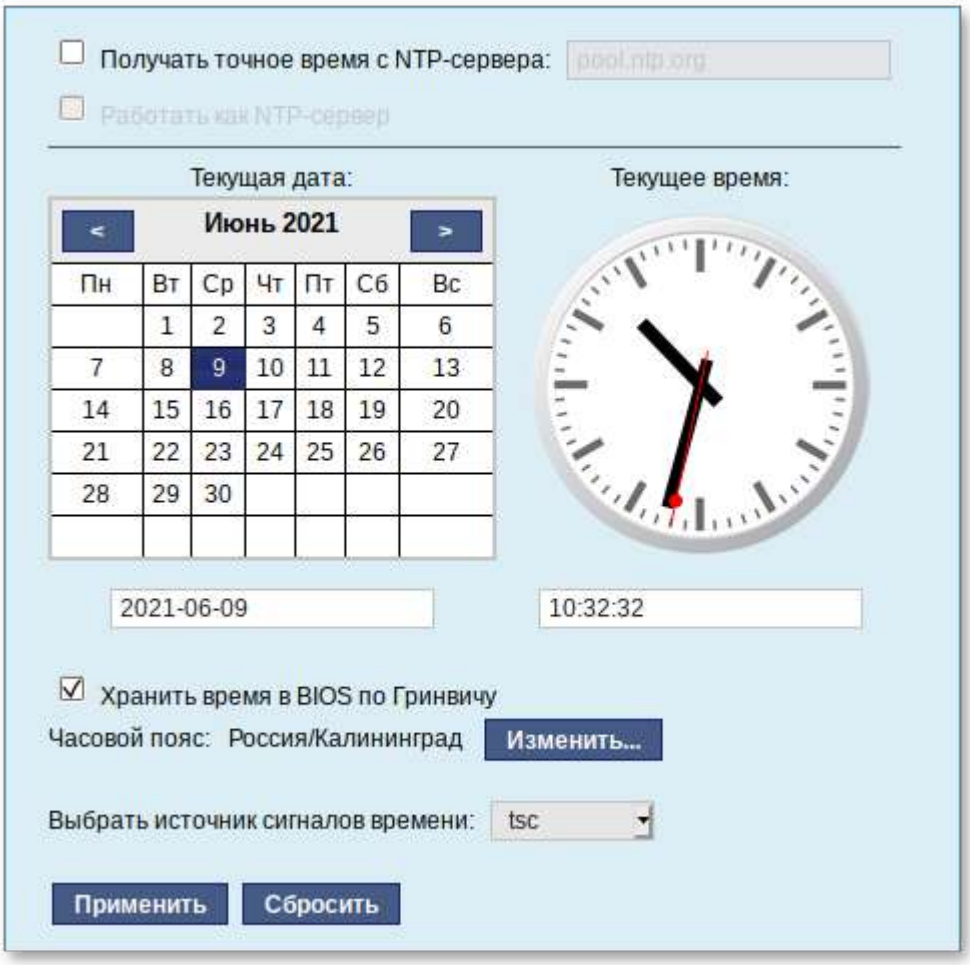
В модуле **Администратор системы** (пакет *alterator-root*) из раздела **Пользователи** можно изменить пароль суперпользователя (root), заданный при начальной настройке системы.

В данном модуле (только в веб-интерфейсе) можно добавить публичную часть ключа RSA или DSA для доступа к серверу по протоколу SSH.



43.9. Дата и время

В модуле **Дата и время** (пакет *alterator-datetime*) из раздела **Система** можно изменить дату и время на сервере, сменить часовой пояс, а также настроить автоматическую синхронизацию часов на самом сервере по протоколу NTP и предоставление точного времени по этому протоколу для рабочих станций локальной сети.



Системное время зависит от следующих факторов:

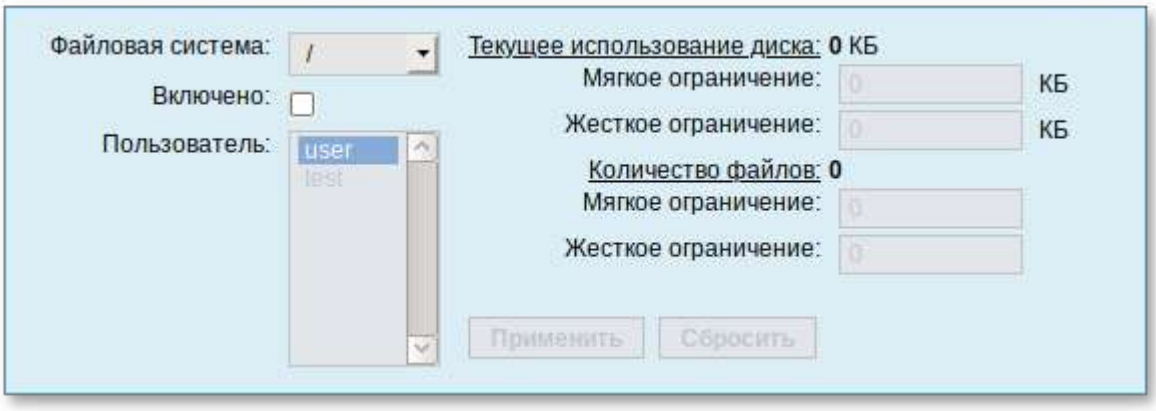
- часы в BIOS — часы, встроенные в компьютер. Они работают, даже если он выключен;
- системное время — часы в ядре операционной системы. Во время работы системы все процессы пользуются именно этими часами;
- часовые пояса — регионы Земли, в каждом из которых принято единое местное время.

При запуске системы происходит активация системных часов и их синхронизация с аппаратными, кроме того, в определённых случаях учитывается значение часового пояса. При завершении работы системы происходит обратный процесс.

Если настроена синхронизация времени с NTP-сервером, то сервер сможет сам работать как сервер точного времени. Для этого достаточно отметить соответствующий пункт **Работать как NTP-сервер**.

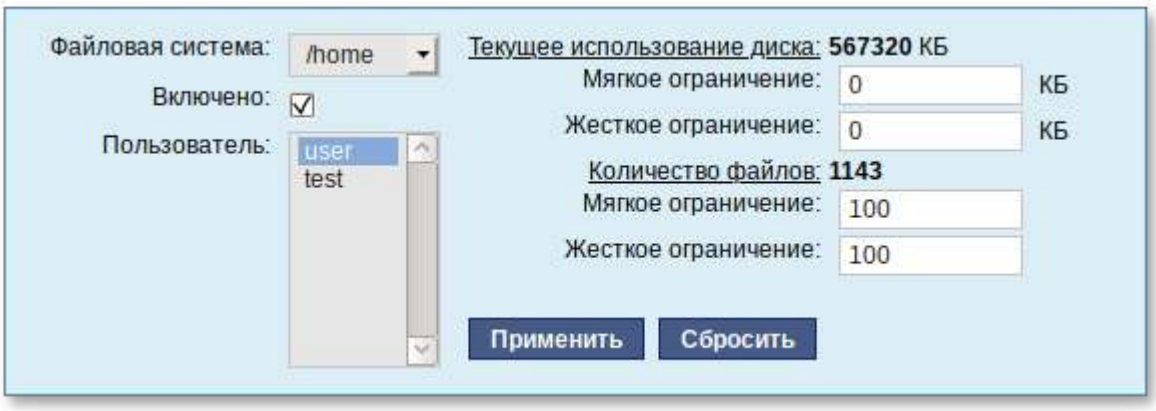
43.10. Ограничение использования диска

Модуль **Использование диска** (пакет *alterator-quota*) в разделе **Пользователи** позволяет ограничить использование дискового пространства пользователями, заведёнными на сервере в модуле **Пользователи**.



Модуль позволяет задать ограничения (квоты) для пользователя при использовании определённого раздела диска. Ограничить можно как суммарное количество килобайт, занятых файлами пользователя, так и количество этих файлов.

Для управления квотами файловая система должна быть подключена с параметрами ***usrquota***, ***grpquota***. Для этого следует выбрать нужный раздел в списке **Файловая система** и установить отметку в поле **Включено**:



Для того чтобы задать ограничения для пользователя, необходимо выбрать пользователя в списке **Пользователь**, установить ограничения и нажать кнопку **Применить**.

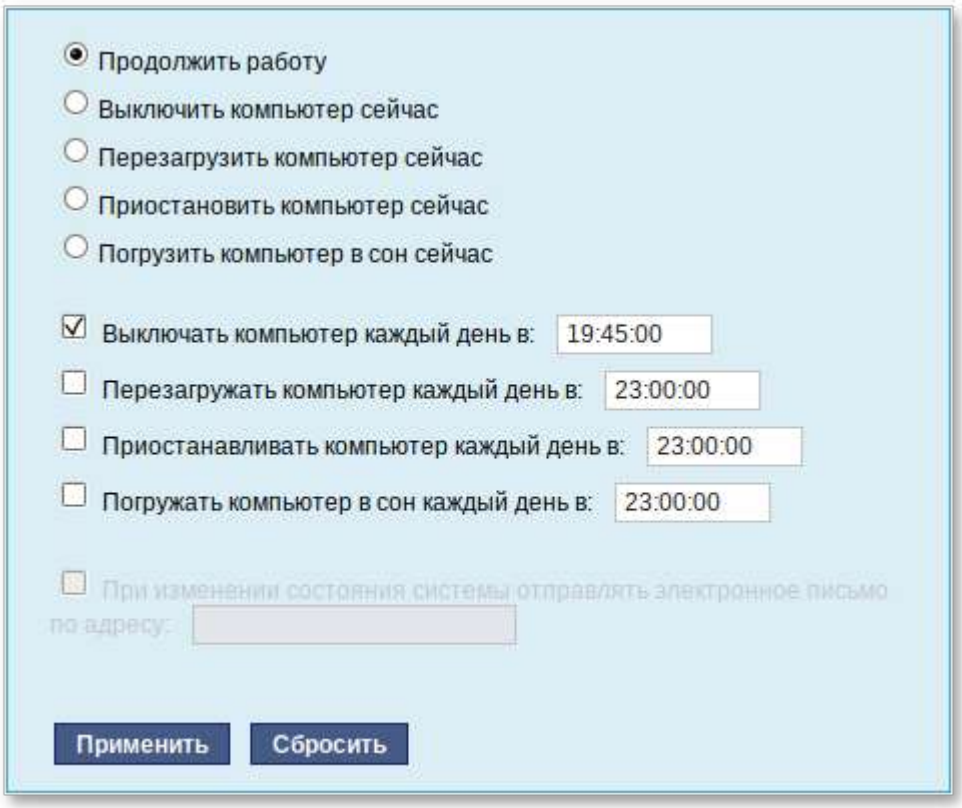
При задании ограничений различают жёсткие и мягкие ограничения:

- **Мягкое ограничение:** нижняя граница ограничения, которая может быть временно превышена. Временное ограничение — одна неделя.
- **Жёсткое ограничение:** использование диска, которое не может быть превышено ни при каких условиях.

Значение 0 при задании ограничений означает отсутствие ограничений.

43.11. Выключение и перезагрузка компьютера

Иногда, в целях обслуживания или по организационным причинам необходимо корректно выключить или перезагрузить сервер. Для этого можно воспользоваться модулем ЦУС **Выключение компьютера** (пакет *alterator-ahttpd-power*) в разделе **Система**.



Модуль **Выключение компьютера** позволяет:

- выключить компьютер;
- перезагрузить компьютер;
- приостановить работу компьютера;
- погрузить компьютер в сон.

Возможна настройка ежедневного применения данных действий в заданное время.

Так как выключение и перезагрузка — критичные для функционирования компьютера операции, то по умолчанию настройка выставлена в значение **Продолжить работу**. Для выключения, перезагрузки или перехода в энергосберегающие режимы нужно отметить соответствующий пункт и нажать **Применить**.

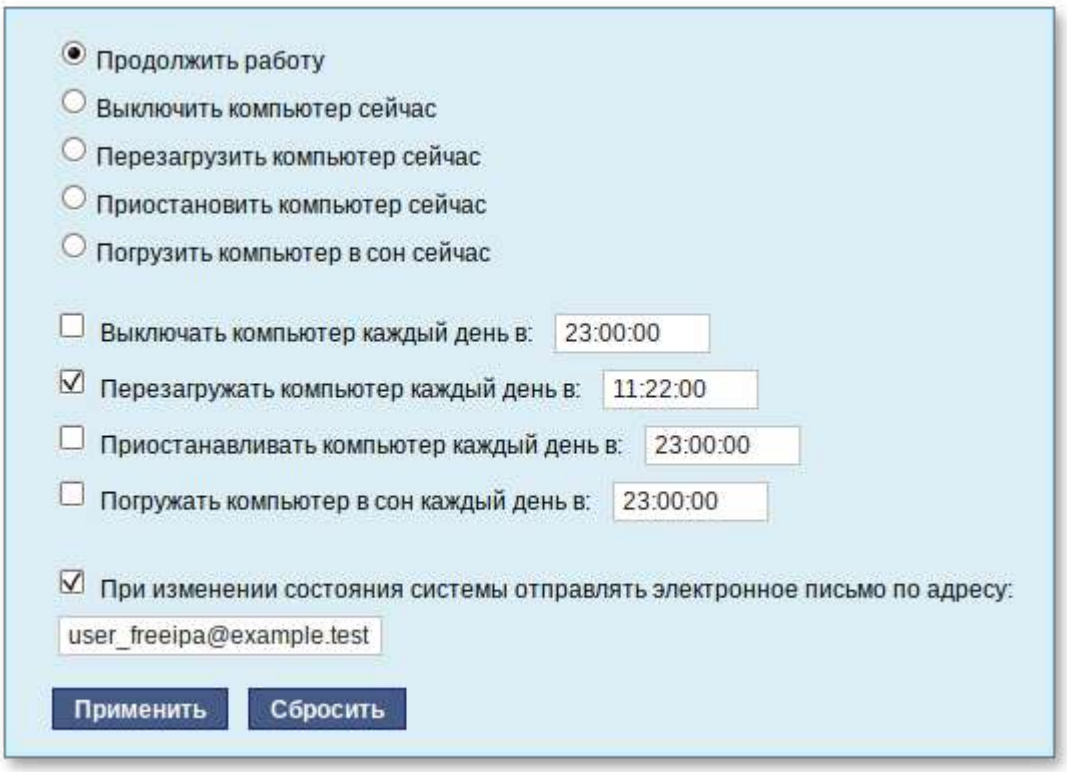
Для ежедневного автоматического выключения компьютера, перезагрузки, а также перехода в энергосберегающие режимы необходимо отметить соответствующий пункт и задать желаемое время. Например, для выключения компьютера следует отметить пункт **Выключать компьютер каждый день в**, задать время выключения в поле ввода слева от этого флажка и нажать кнопку **Применить**.

Примечание

Для возможности настройки оповещений на e-mail, должен быть установлен пакет state-change-notify-postfix:

```
# apt-get install state-change-notify-postfix
```

Для настройки оповещений необходимо отметить пункт **При изменении состояния системы отправлять электронное письмо по адресу**, ввести e-mail адрес и нажать кнопку **Применить**:



По указанному адресу, при изменении состоянии системы будут приходить электронные письма. Например, при включении компьютера, содержание письма будет следующее:

```
Tue Jun 16 11:46:59 EET 2020: The server.test.alt is about to start.
```

При выключении:

```
Tue Jun 16 12:27:02 EET 2020: The server.test.alt is about to shutdown.
```

Кнопка **Сбросить** возвращает сделанный выбор к безопасному значению по умолчанию: **Продолжить работу**, перечитывает расписания и выставляет отметки для ежедневного автоматического действия в соответствие с прочитанным.

Глава 44. Прочие возможности ЦУС

Возможности Альт Сервер не ограничиваются только теми, что были описаны выше. Вы всегда можете поискать другие модули, предоставляющие прочие возможности для настройки системы в веб-интерфейсе.

Установленные пакеты, которые относятся к ЦУС, можно посмотреть, выполнив команду:

```
rpm -qa | grep alterator*
```

Прочие пакеты для ЦУС можно найти, выполнив команду:

```
apt-cache search alterator*
```

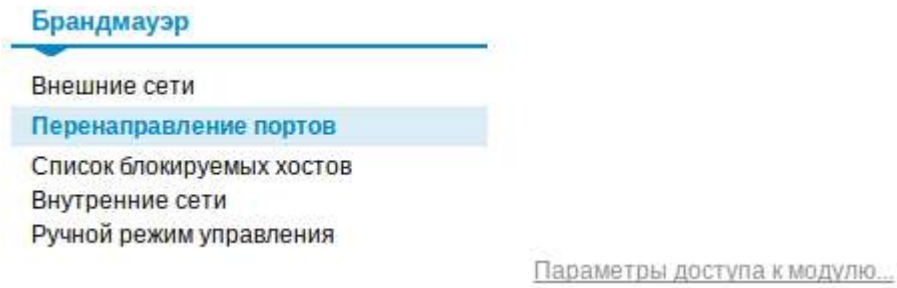
Модули можно дополнительно загружать и удалять как обычные программы:

```
# apt-get install alterator-net-openvpn
# apt-get remove alterator-net-openvpn
```

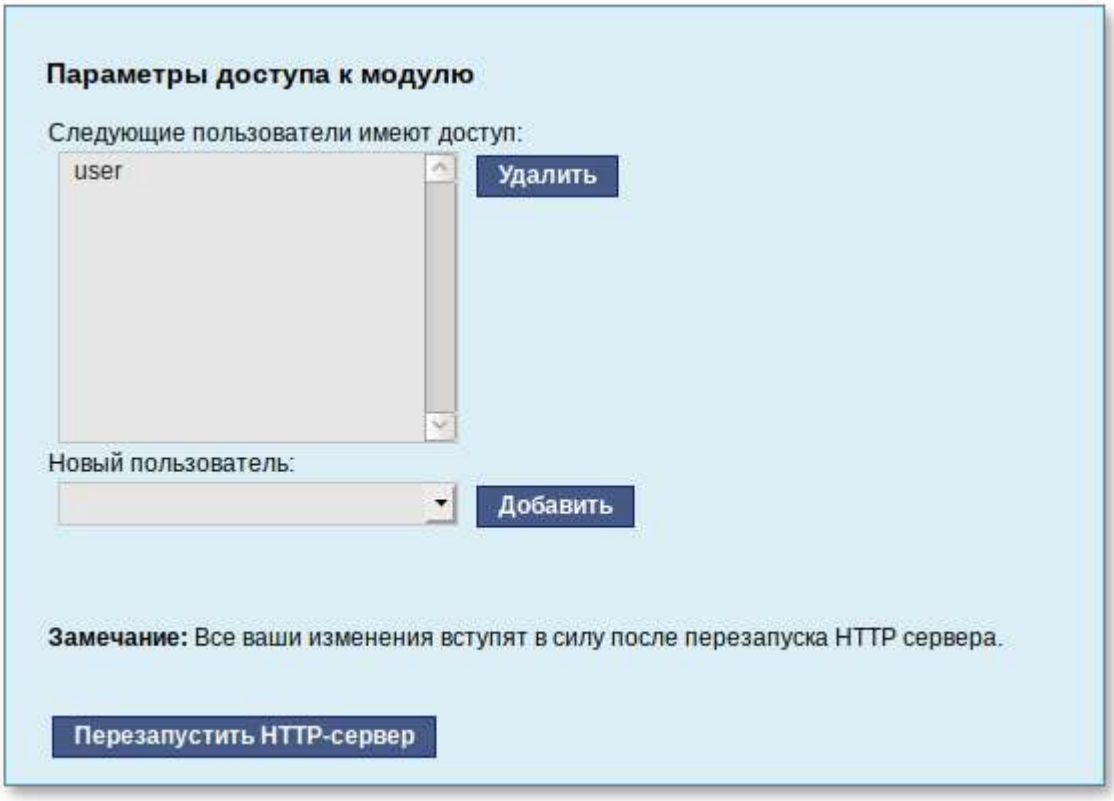
Глава 45. Права доступа к модулям

Администратор системы (root) имеет доступ ко всем модулям, установленным в системе, и может назначать права доступа для пользователей к определенным модулям.

Для разрешения доступа пользователю к конкретному модулю, администратору в веб-интерфейсе ЦУС необходимо выбрать нужный модуль и нажать ссылку **Параметры доступа к модулю**, расположенную в нижней части окна модуля:



В открывшемся окне, в списке **Новый пользователь** необходимо выбрать пользователя, который получит доступ к данному модулю, и нажать кнопку **Добавить**.



Для сохранения настроек необходимо перезапустить HTTP-сервер, для этого достаточно нажать кнопку **Перезапустить HTTP-сервер**.

Для удаления доступа пользователя к определенному модулю, администратору, в окне этого модуля необходимо нажать ссылку **Параметры доступа к модулю**, в открывшемся окне в списке пользователей которым разрешен доступ, должен выбрать пользователя, нажать кнопку **Удалить** и перезапустить HTTP-сервер.

Системный пользователь, пройдя процедуру аутентификации, может просматривать и вызывать модули, к которым он имеет доступ.

Часть IX. Корпоративная инфраструктура

Содержание

Глава 46. Samba 4 в роли контроллера домена Active Directory

Использование Samba 4 в роли контроллера домена Active Directory позволяет вводить Windows 7/8 в домен без манипуляций с реестром.

Поддерживаются следующие базовые возможности Active Directory:

- аутентификация рабочих станций Windows и Linux и служб;
- авторизация и предоставление ресурсов;
- групповые политики (GPO);
- перемещаемые профили (Roaming Profiles);
- поддержка инструментов Microsoft для управления серверами (Remote Server Administration Tools) с компьютеров под управлением Windows;
- поддержка протоколов SMB2 и SMB3 (в том числе с поддержкой шифрования);
- репликация с другими серверами (в том числе с Windows 2012).

Предупреждение

Samba AD DC конфликтует с OpenLDAP и MIT Kerberos, поскольку эти приложения запускают одни и те же службы на одних тех же, по умолчанию, портах для протоколов LDAP и Kerberos.

Предупреждение

Samba AD DC функционирует на уровне контроллера доменов Windows 2008 R2 . Можно ввести его в домен Windows 2012 как клиента, но не как контроллер домена.

46.1. Установка

Для установки Samba AD DC выполняются следующие шаги:

- Установить пакет *task-samba-dc*, который установит все необходимое:

```
# apt-get install task-samba-dc
```

- Так как Samba в режиме контроллера домена (Domain Controller, DC) использует как свой LDAP, так и свой сервер Kerberos, несовместимый с MIT Kerberos, перед установкой необходимо остановить конфликтующие службы **krb5kdc** и **slapd**, а также **bind**:

```
# for service in smb nmb krb5kdc slapd bind; do chkconfig $service off;
service $service stop; done
```

46.2. Создание нового домена

46.2.1. Восстановление к начальному состоянию Samba

Необходимо очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

Предупреждение

Обязательно удаляйте **/etc/samba/smb.conf** перед созданием домена: **rm -f /etc/samba/smb.conf**

46.2.2. Выбор имени домена

Имя домена, для разворачиваемого DC, должно состоять минимум из двух компонентов, разделённых точкой. При этом должно быть установлено правильное имя узла и домена для сервера:

- HOSTNAME=dc.test.alt в **/etc/sysconfig/network**

- ```
  # hostnamectl set-hostname dc.test.alt
  ```
  ```

```
# domainname test.alt
```

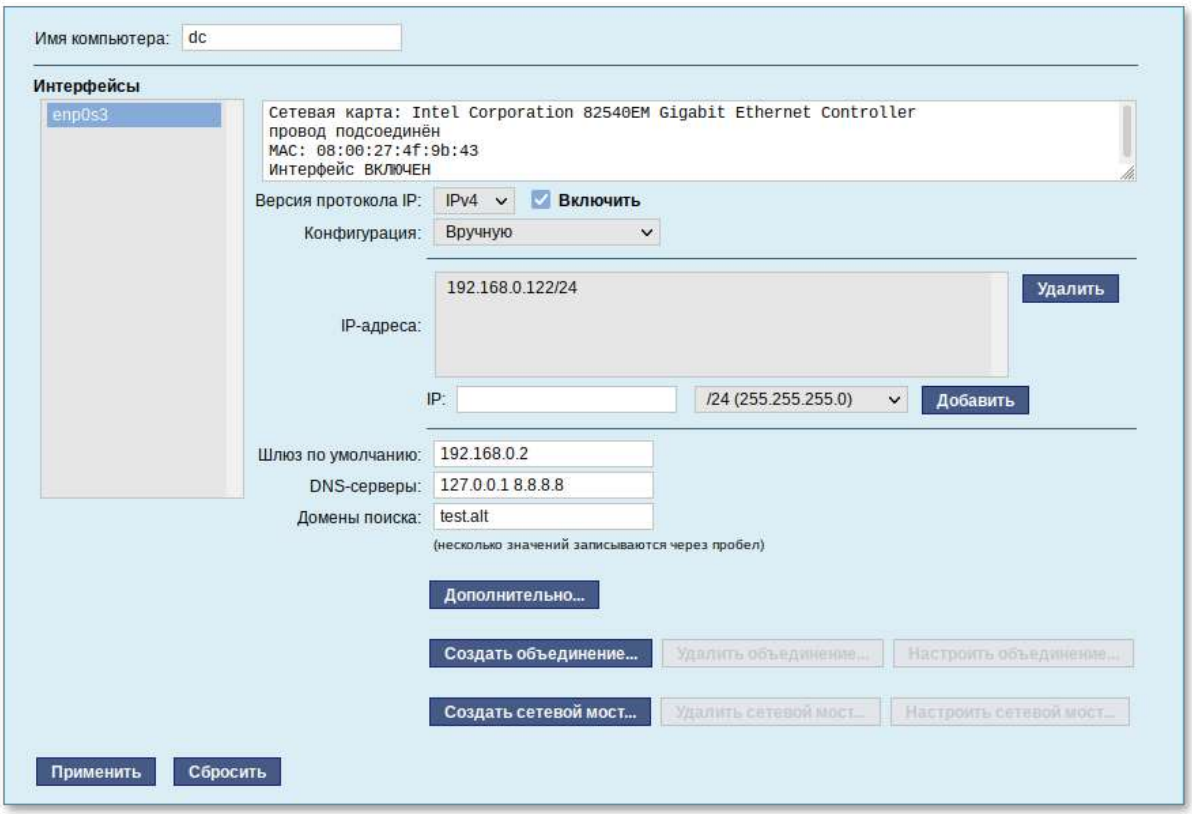
Предупреждение

При указании домена, имеющего суффикс .local, на сервере и подключаемых компьютерах под управлением Linux потребуется отключить службу **avahi-daemon**.

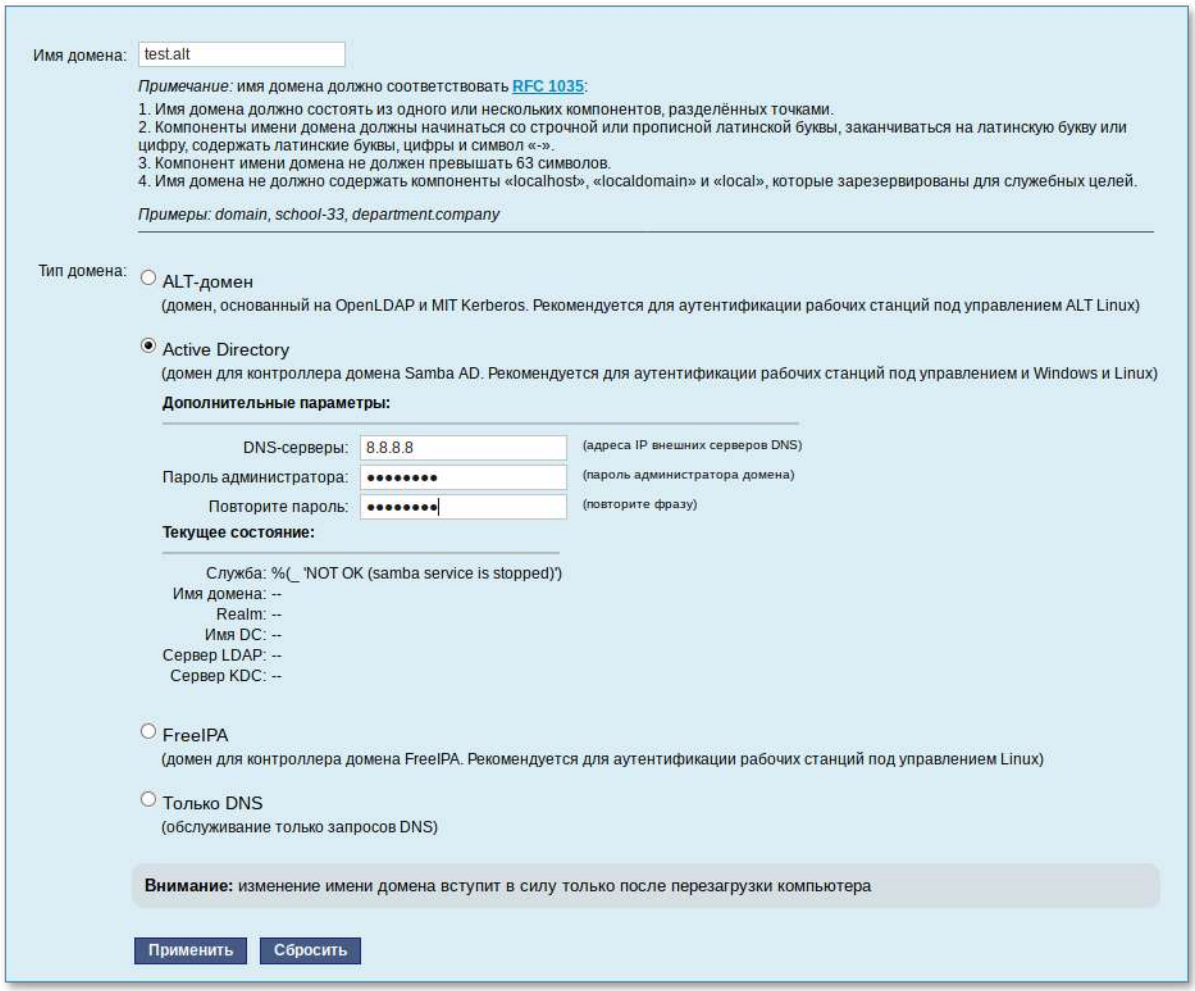
46.2.3. Создание домена в ЦУС

При инициализации домена в веб-интерфейсе ЦУС следует выполнить следующие действия:

1. В модуле Ethernet-интерфейсы указать имя компьютера и DNS 127.0.0.1:



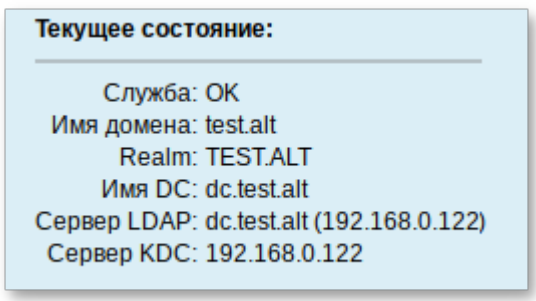
2. В модуле Домен указать имя домена, отметить пункт **`Active Directory`**, указать IP-адреса внешних DNS-серверов, задать пароль администратора домена и нажать кнопку **Применить**:



Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль не полностью соответствующий требованиям это одна из причин завершения развертывания домена ошибкой.

3. После успешного создания домена, будет выведена информация о домене:



4. Перегрузить сервер.

46.2.4. Создание домена одной командой

Создание контроллера домена test.alt:

```
# samba-tool domain provision --realm=test.alt --domain test --adminpass='Pa$
$word' --dns-backend=SAMBA_INTERNAL --server-role=dc
```

где

- --realm — задает область Kerberos (LDAP), и DNS имя домена;
- --domain — задает имя домена (имя рабочей группы);
- --adminpass — пароль основного администратора домена;
- --server-role — тип серверной роли.

Примечание

Параметры **--use-rfc2307 --use-xattrs=yes** позволяют поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

46.2.5. Интерактивное создание домена

Для интерактивного развертывания запустите **samba-tool domain provision**, это запустит утилиту развертывания, которая будет задавать различные вопросы о требованиях к установке. В примере показано создание домена test.alt:

```
# samba-tool domain provision
Realm [TEST.ALT]:
Domain [TEST]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
[SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [127.0.0.1]:
Administrator password:
Retype password:
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.0.122
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=test,DC=alt
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
```

```
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=test,DC=alt
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at /var/lib/
samba/private/krb5.conf
Once the above files are installed, your Samba4 server will be ready to use
Server Role:           active directory domain controller
Hostname:              dc
NetBIOS Domain:        TEST
DNS Domain:            test.alt
DOMAIN SID:            S-1-5-21-80639820-2350372464-3293631772
```

При запросе ввода нажимайте **Enter** за исключением запроса пароля администратора («Administrator password:» и «Retype password:»).

Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль не полностью соответствующий требованиям это одна из причин завершения развертывания домена ошибкой.

46.3. Запуск службы

Установите службу по умолчанию и запустите её:

```
# chkconfig samba on
# service samba start
```

46.4. Настройка Kerberos

Внести изменения в файл **/etc/krb5.conf**. Следует раскомментировать строку *default_realm* и содержимое разделов *realms* и *domain_realm* и указать название домена (обратите внимание на регистр символов):

```
includedir /etc/krb5.conf.d/

[logging]
# default = FILE:/var/log/krb5libs.log
```

```
# kdc = FILE:/var/log/krb5kdc.log
# admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_kdc = true
 dns_lookup_realm = true
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = TEST.ALT
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
TEST.ALT = {
  default_domain = test.alt
}

[domain_realm]
dc = TEST.ALT
```

Примечание

В момент создания домена Samba конфигурирует шаблон файла **krb5.conf** для домена в каталоге **/var/lib/samba/private/**. Можно просто заменить этим файлом файл, находящийся в каталоге **/etc/**:

```
# cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

46.5. Проверка работоспособности

Просмотр общей информации о домене:

```
# samba-tool domain info 127.0.0.1
Forest           : test.alt
Domain           : test.alt
Netbios domain   : TEST
DC name          : dc.test.alt
DC netbios name  : DC
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
```

Просмотр предоставляемых служб:

```
# smbclient -L localhost -Uadministrator
Enter TEST\administrator's password:

    Sharename       Type      Comment
    ---------       ----      -------
    sysvol          Disk
    netlogon        Disk
    IPC$            IPC       IPC Service (Samba 4.14.6)
SMB1 disabled -- no workgroup available
```

Общие ресурсы netlogon и sysvol создаваемые по умолчанию нужны для функционирования сервера AD и создаются в **smb.conf** в процессе развертывания/модернизации.

Проверка конфигурации DNS:

- Убедитесь в наличии nameserver 127.0.0.1 в **/etc/resolv.conf**:

  ```
  # host test.alt
  test.alt has address 192.168.0.122
  test.alt has IPv6 address fd47:d11e:43c1:0:a00:27ff:fece:2424
  ```

- Проверьте имена хостов:

  ```
  # host -t SRV _kerberos._udp.test.alt.
  _kerberos._udp.test.alt has SRV record 0 100 88 dc.test.alt.
  # host -t SRV _ldap._tcp.test.alt.
  _ldap._tcp.test.alt has SRV record 0 100 389 dc.test.alt.
  # host -t A dc.test.alt.
  dc.test.alt has address 192.168.0.122
  ```

  Если имена не находятся, проверьте выключение службы **named**.

Проверка Kerberos (имя домена должно быть в верхнем регистре):

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

Просмотр полученного билета:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
03.06.2021 12:48:48  03.06.2021 22:48:48  krbtgt/TEST.ALT@TEST.ALT
    renew until 10.06.2021 12:48:44
```

46.6. Управление пользователями

Создать пользователя с паролем:

```
samba-tool user create имя пользователя
samba-tool user setexpiry имя пользователя
```

Удалить пользователя:

```
samba-tool user delete имя пользователя
```

Отключить пользователя:

```
samba-tool user disable имя пользователя
```

Включить пользователя:

```
samba-tool user enable имя пользователя
```

Изменить пароль пользователя:

```
samba-tool user setpassword имя пользователя
```

Просмотреть доступных пользователей:

```
# samba-tool user list
```

Например, создать и разблокировать пользователя ivanov:

```
# samba-tool user create ivanov --given-name='Иван Иванов' --mail-
address='ivanov@test.alt'
# samba-tool user setexpiry ivanov --noexpiry
```

Предупреждение

Не допускайте одинаковых имён для пользователя и компьютера, это может привести к коллизиям (например, такого пользователя нельзя добавить в группу). Если компьютер с таким именем заведён, удалить его можно командой: **pdbedit -x -m *имя***

46.7. Заведение вторичного DC

Присоединение дополнительного Samba DC к существующему AD отличается от инициализации первого DC в лесу AD.

В примере используется узел: dc2.test.alt (192.168.0.106).

1. На Primary Domain Controller (PDC) выключить службу **bind** и, если она была включена, перезапустить службу **samba**.
2. Завести адрес IP для dc2:

   Предупреждение

   Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

   ```
   # samba-tool dns add 192.168.0.122 test.alt DC2 A 192.168.0.106 -
   Uadministrator
   ```

3. Установить следующие параметры в файле конфигурации клиента Kerberos (на dc2.test.alt файл **/etc/krb5.conf**):

```
[libdefaults]
default_realm = TEST.ALT
dns_lookup_realm = true
dns_lookup_kdc = true
```

Примечание

В resolvconf обязательно должен быть добавлен PDC как nameserver.

4. Для проверки настройки запрашиваем билет Kerberos для администратора домена:

Предупреждение

Имя домена должно быть указано в верхнем регистре

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

5. Убеждаемся, что билет получен:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
03.06.2021 12:48:48  03.06.2021 22:48:48  krbtgt/TEST.ALT@TEST.ALT
    renew until 10.06.2021 12:48:44
```

6. Ввести в домен test.alt в качестве контроллера домена (DC):

```
# samba-tool domain join test.alt DC -Uadministrator --realm=test.alt
```

Если всё нормально, в конце будет выведена информация о присоединении к домену:

```
Joined domain TEST (SID S-1-5-21-80639820-2350372464-3293631772) as a DC
```

Для получения дополнительной информации можно воспользоваться командой:

```
# samba-tool domain join --help
```

7. Сделать службу **samba** запускаемой по умолчанию:

```
# chkconfig samba on
```

Если подключались к DC под управлением Windows, необходимо запустить службу **samba**:

```
# service samba start
```

46.8. Репликация

Предупреждение

Без успешной двунаправленной репликации в течение 14 дней DC исключается из Active Directory

Предупреждение

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

1. Реплицируем на вторичном DC (с первичного):

```
# samba-tool drs replicate dc2.test.alt dc.test.alt dc=test,dc=alt -
Uadministrator
```

   Сначала указывается приемник, затем источник, после этого реплицируемая ветка в LDAP.

2. Реплицируем на вторичном DC (на первичный):

```
# samba-tool drs replicate dc.test.alt dc2.test.alt dc=test,dc=alt -
Uadministrator
```

   Сначала указывается приемник, затем источник, после этого реплицируемая ветка в LDAP.

   Примечание

   Имя домена в именах серверов можно опустить (если они одинаковые).

3. Для просмотра статуса репликации на PDC, запустите на Samba DC:

```
# samba-tool drs showrepl
```

Примечание

Если репликация на Windows не работает, добавьте в Active Directory Sites and Services новое соединение Active Directory. Реплицируйте на DC, подождите минут 5 и пробуйте реплицировать с Samba на Windows.

46.9. Подключение к домену на рабочей станции

46.9.1. Подготовка

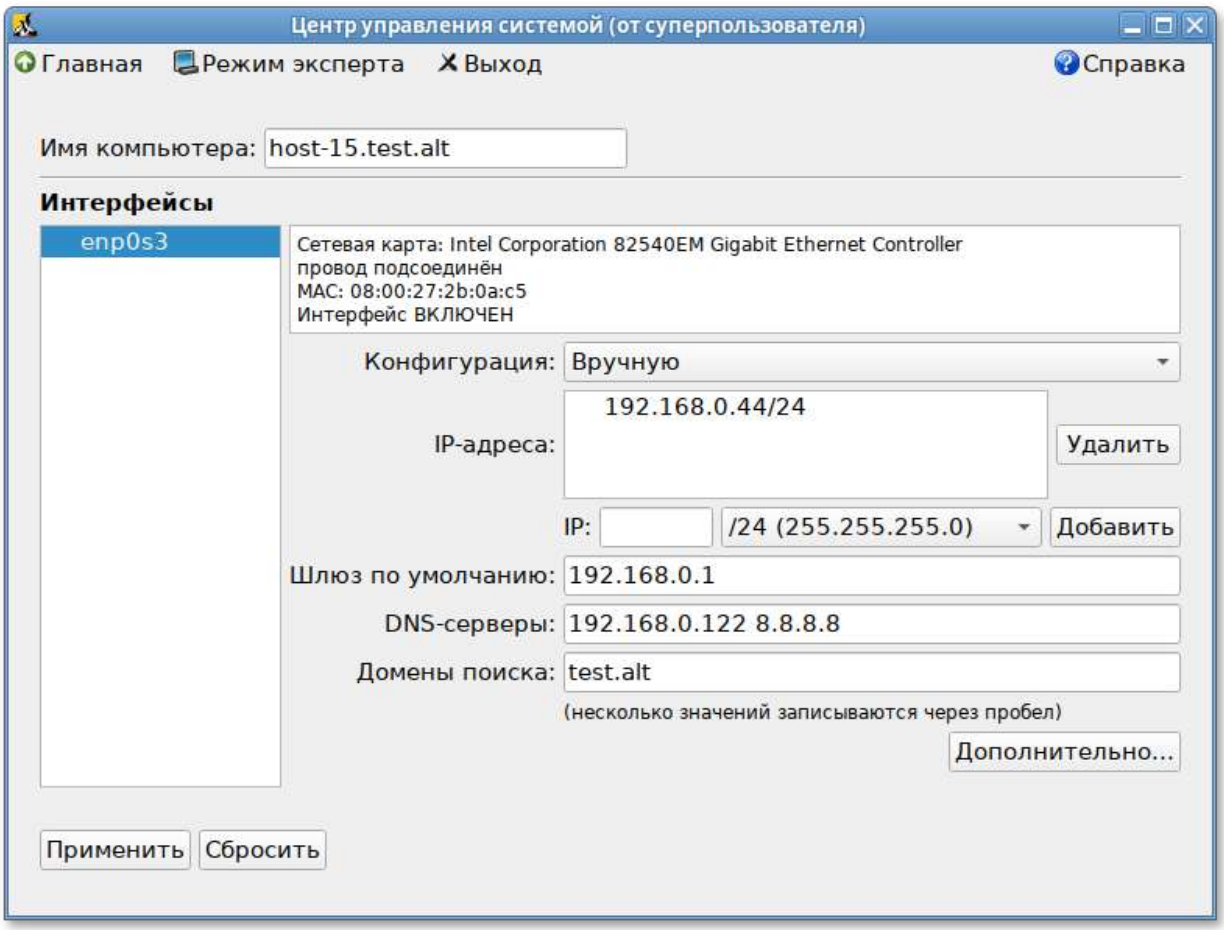
Для ввода компьютера в Active Directory потребуется установить пакет task-auth-ad-sssd и все его зависимости (если он еще не установлен):

```
# apt-get install task-auth-ad-sssd
```

Синхронизация времени с контроллером домена производится автоматически.

Настройки сети можно выполнить как в графическом интерфейсе, так и в консоли:

- В Центре управления системой в разделе **Сеть → Ethernet интерфейсы** задать имя компьютера, указать в поле **DNS-серверы** DNS-сервер домена и в поле **Домены поиска** — домен для поиска:



- В консоли:
  - задать имя компьютера:

    ```
    # hostnamectl set-hostname host-15.test.alt
    ```

  - в качестве первичного DNS должен быть указан DNS-сервер домена. Для этого необходимо создать файл **/etc/net/ifaces/enp0s3/resolv.conf** со следующим содержимым:

    ```
    nameserver 192.168.0.122
    ```

    где 192.168.0.122 — IP-адрес DNS-сервера домена.

  - указать службе resolvconf использовать DNS контроллера домена и домен для поиска. Для этого в файле **/etc/resolvconf.conf** добавить/отредактировать следующие параметры:

```
interface_order='lo lo[0-9]* lo.* enp0s3'
search_domains=test.alt
```

где enp0s3 — интерфейс на котором доступен контроллер домена, test.alt — домен.

- обновить DNS адреса:

```
# resolvconf -u
```

Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

В результате выполненных действий в файле **/etc/resolv.conf** должны появиться строки:

```
search test.alt
nameserver 192.168.0.122
```

46.9.2. Ввод в домен

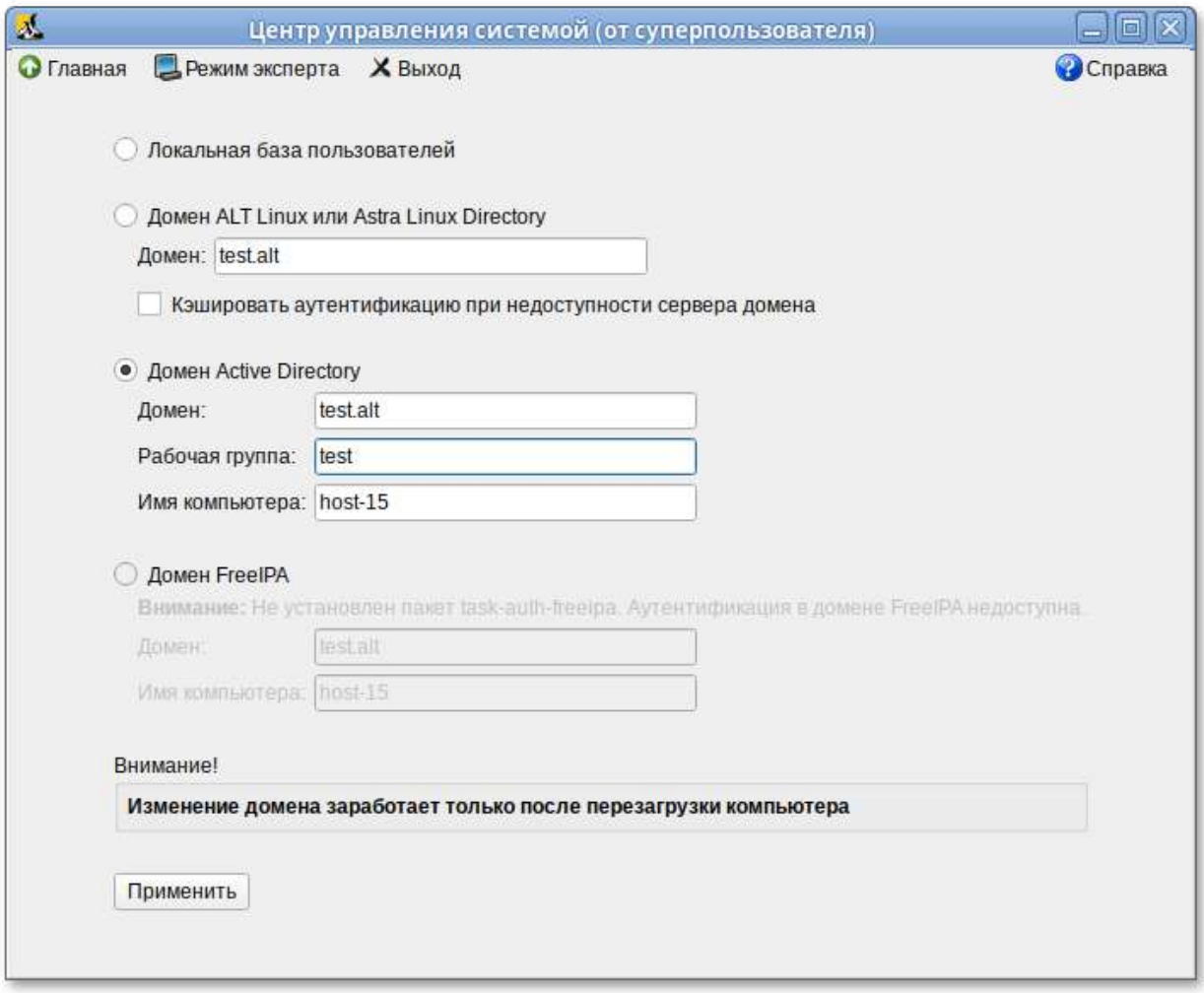
Ввод в домен можно осуществить следующими способами:

- В командной строке:

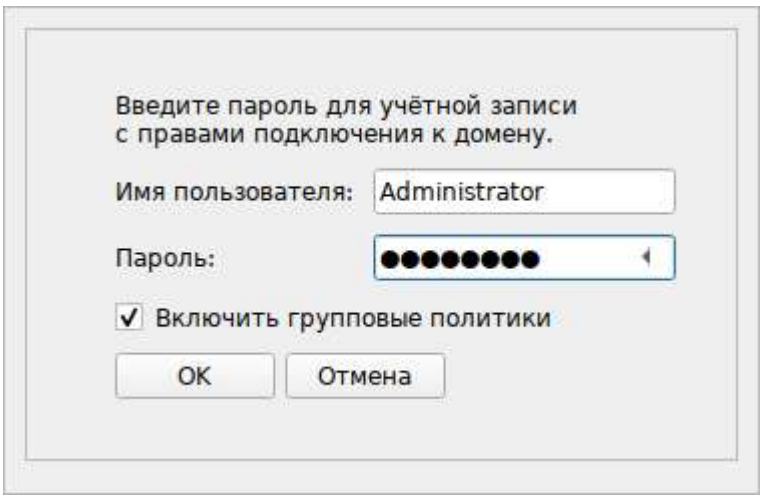
```
# system-auth write ad test.alt host-15 test 'administrator' 'Pa$$word'
Joined 'HOST-15' to dns domain 'test.alt'
```

- В Центре управления системой в разделе **Пользователи** → **Аутентификация**.

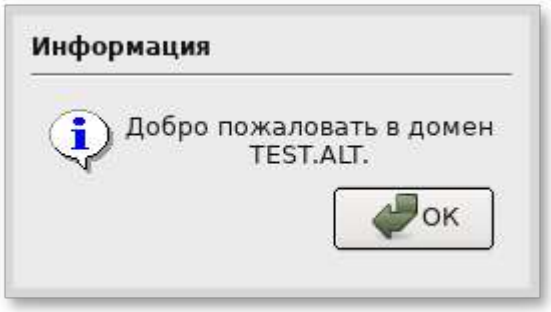
  В открывшемся окне следует выбрать пункт **Домен Active Directory**, заполнить поля и нажать кнопку **Применить**:



В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку **ОК**:



При успешном подключении к домену, отобразится соответствующая информация:



Перезагрузить рабочую станцию.

Глава 47. Групповые политики

Групповые политики — это набор правил и настроек для серверов и рабочих станций, реализуемых в корпоративных решениях. В соответствии с групповыми политиками производится настройка рабочей среды относительно локальных политик, действующих по умолчанию. В данном разделе рассмотрена реализация поддержки групповых политик Active Directory в решениях на базе дистрибутивов ALT.

В дистрибутивах ALT для применения групповых политик на данный момент предлагается использовать инструмент gpupdate. Инструмент рассчитан на работу на машине, введённой в домен Samba.

Интеграция в инфраструктуру LDAP-объектов Active Directory позволяет осуществлять привязку настроек управляемых конфигураций объектам в дереве каталогов. Кроме глобальных настроек в рамках домена, возможна привязка к следующим группам объектов:

- подразделения (OU) — пользователи и компьютеры, хранящиеся в соответствующей части дерева объектов;
- сайты — группы компьютеров в заданной подсети в рамках одного и того же домена;
- конкретные пользователи и компьютеры.

Кроме того, в самих объектах групповых политик могут быть заданы дополнительные условия, фильтры и ограничения, на основании которых принимается решение о том, как применять данную групповую политику.

Политики подразделяются на политики для компьютеров (Machine) и политики для пользователей (User). Политики для компьютеров применяются на хосте в момент загрузки, а также в момент явного или регулярного запроса планировщиком (раз в час). Пользовательские политики применяются в момент входа в систему.

Групповые политики можно использовать для разных целей, например:

- Установки домашней страницы браузера Firefox/Chromium (экспериментальная политика). Возможно установить при использовании ADMX файлов Mozilla Firefox (https://github.com/mozilla/policy-templates/releases) и Google Chrome (https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip) соответственно.

- Установки запрета на подключение внешних носителей.
- Управления политиками control (реализован широкий набор настроек). Возможно установить при использовании ADMX файлов ALT.
- Включения или выключения различных служб (сервисов systemd) Возможно установить при использовании ADMX файлов ALT.
- Подключения сетевых дисков (экспериментальная политика).
- Генерирования (удаления/замены) ярлыков для запуска программ.
- Создания каталогов.
- Установки и удаления пакетов (в стадии разработки).

Полный набор возможностей можно оценить, установив пакет admx-basealt или скачав файлы ADMX из репозитория https://github.com/altlinux/admx-basealt и загрузив их в оснастку RSAT.

Важно

Модули (настройки), помеченные как экспериментальные, необходимо включать вручную через ADMX файлы ALT в разделе **Групповые политики**.

47.1. Развертывание групповых политик

Процесс развёртывание групповых политик:

1. Развернуть сервер Samba AD DC (см. Samba 4 в роли контроллера домена Active Directory).
2. Установить административные шаблоны. Для этого:
   - установить пакеты политик admx-basealt, admx-samba, admx-chromium, admx-firefox и утилиту admx-msi-setup:

     ```
     # apt-get install admx-basealt admx-samba admx-chromium admx-firefox admx-msi-setup
     ```

   - скачать и установить ADMX-файлы от Microsoft:

     ```
     # admx-msi-setup
     ```

Примечание

По умолчанию, **admx-msi-setup** устанавливает последнюю версию ADMX от Microsoft (сейчас это Microsoft Group Policy — Windows 10 October 2020 Update (20H2)). С помощью параметров, можно указать другой источник:

```
# admx-msi-setup -h
admx-msi-setup - download msi files and extract them in
<destination-directory> default value is /usr/share/
PolicyDefinitions/.
Usage: admx-msi-setup [-d <destination-directory>] [-s <admx-
msi-source>]
Removing admx-msi-setup temporary files...
```

- после установки, политики будут находиться в каталоге **/usr/share/PolicyDefinitions**. Скопировать локальные ADMX-файлы в сетевой каталог sysvol (**/var/lib/samba/sysvol/<DOMAIN>/Policies/**):

```
# samba-tool gpo admxload
```

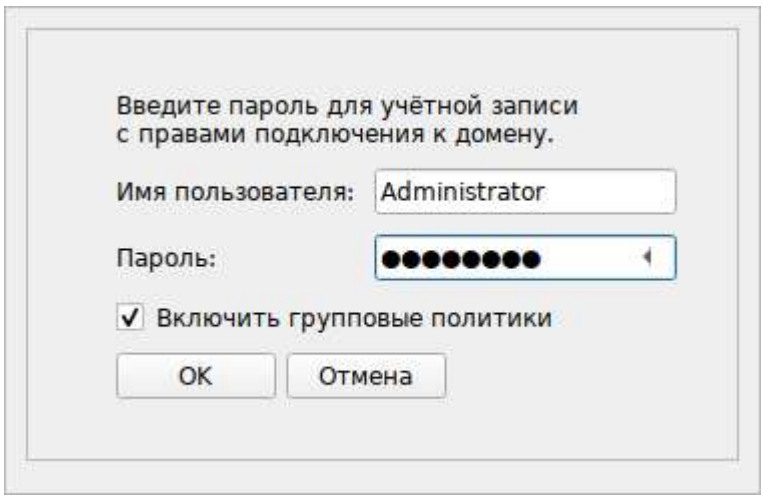
3. Ввести рабочие станции в домен Active Directory (см. Подключение к домену на рабочей станции).

Примечание

Должен быть установлен пакет alterator-gpupdate:

```
# apt-get install alterator-gpupdate
```

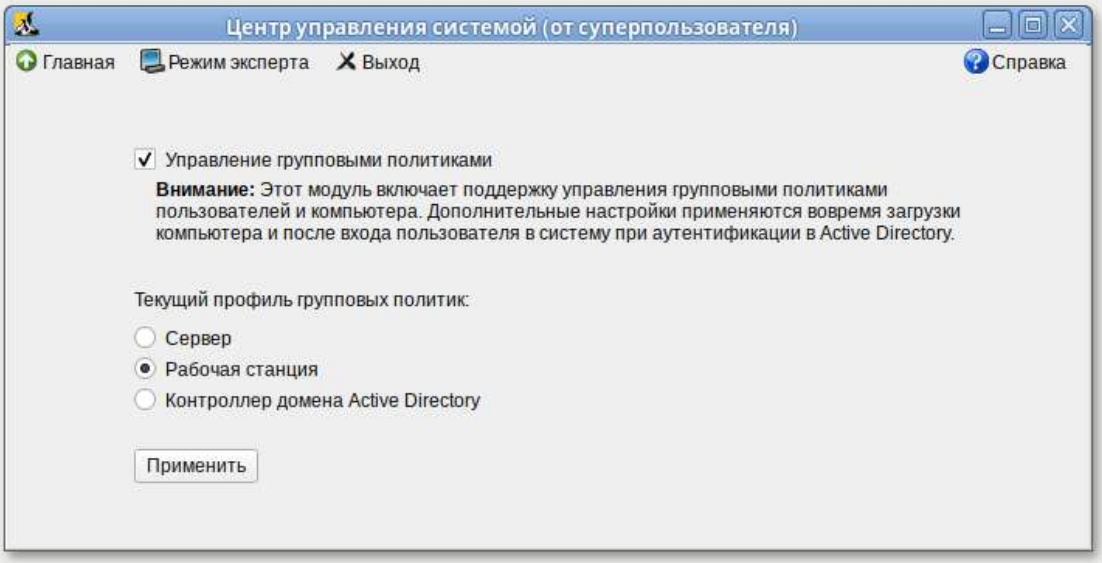
Для автоматического включения групповых политик, при вводе в домен, в окне ввода имени и пароля пользователя, имеющего право вводить машины в домен, отметить пункт **Включить групповые политики**:



Политики будут включены сразу после ввода в домен (после перезагрузки системы).

Примечание

Если машина уже находится в домене, можно вручную включить групповые политики с помощью модуля alterator-gpupdate. Для этого в Центре управления системой в разделе **Система → Групповые политики** следует выбрать шаблон локальной политики (**Сервер**, **Рабочая станция** или **Контроллер домена**) и установить отметку в пункте **Управление групповыми политиками**:



4. Ввести машину с ОС Windows в домен.

Примечание

Управление сервером Samba с помощью RSAT поддерживается из среды до Windows 2012R2 включительно

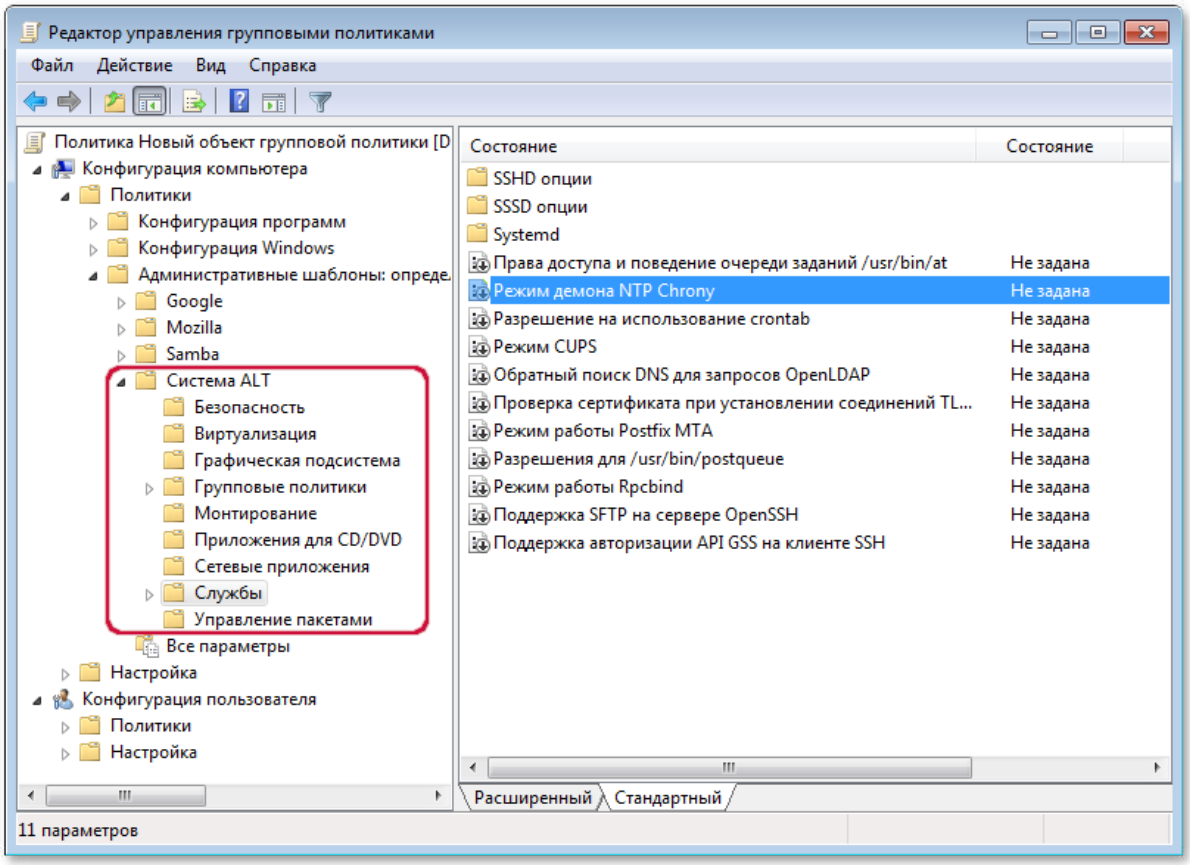
5. Включить компоненты удаленного администрирования.

Примечание

Этот шаг можно пропустить, если административные шаблоны были установлены на контроллере домена.

Для задания конфигурации с помощью RSAT необходимо установить административные шаблоны (файлы ADMX) и зависящие от языка файлы ADML из репозитория http://git.altlinux.org/gears/a/admx-basealt.git (https://github.com/altlinux/admx-basealt) и разместить их в каталоге **\\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\PolicyDefinitions**.

6. Корректно установленные административные шаблоны будут отображены на машине Windows в оснастке **Редактор управления групповыми политиками** в разделе **Конфигурация компьютера → Политики → Административные шаблоны → Система ALT**:



Политики редактируются на ОС Windows, применяются на рабочих станциях.

7. В ADMC на рабочей станции, введённой в домен или в оснастке **Active Directory — пользователи и компьютеры** создать подразделение (OU) и переместить в него компьютеры и пользователей домена.

47.2. Пример создания групповой политики

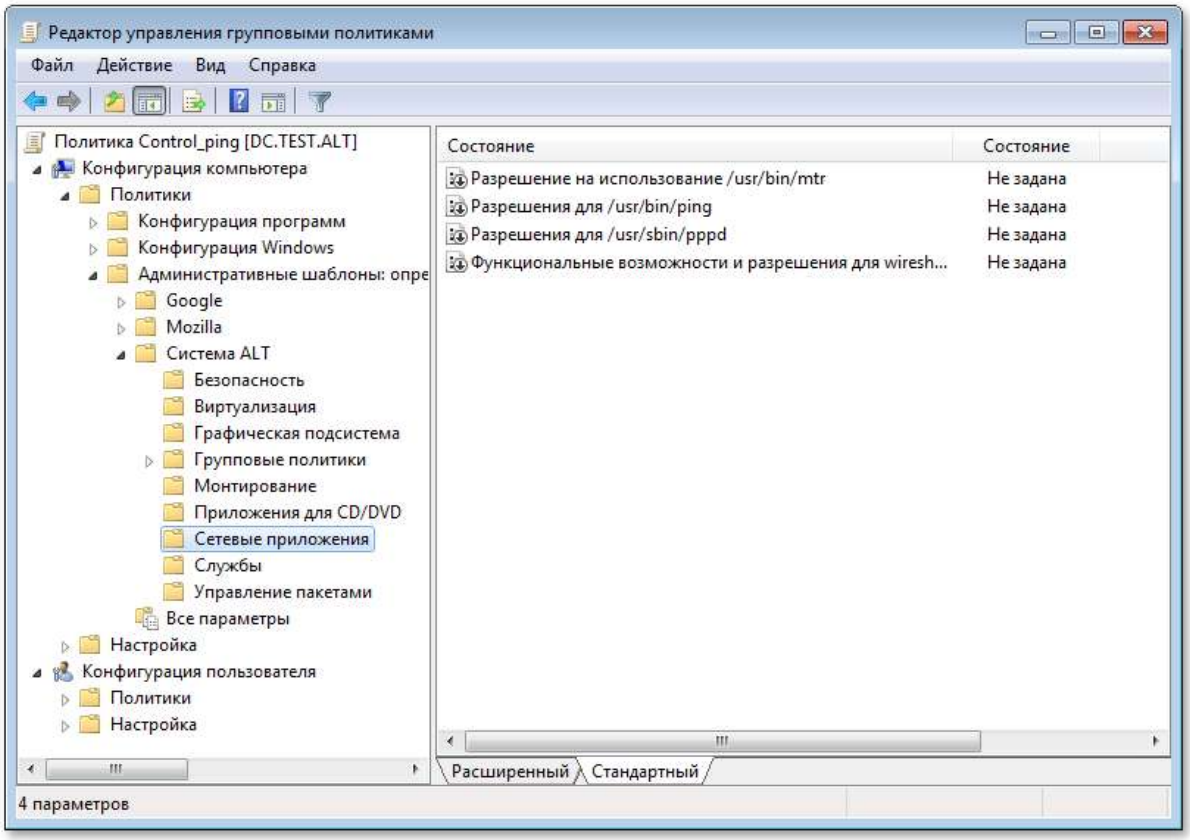
В качестве примера, создадим политику, разрешающую запускать команду **`ping`** только суперпользователю (root). Для создания новой политики, необходимо выполнить следующие действия:

1. На машине с установленным RSAT открыть оснастку **Управление групповыми политиками** (gpmc.msc).

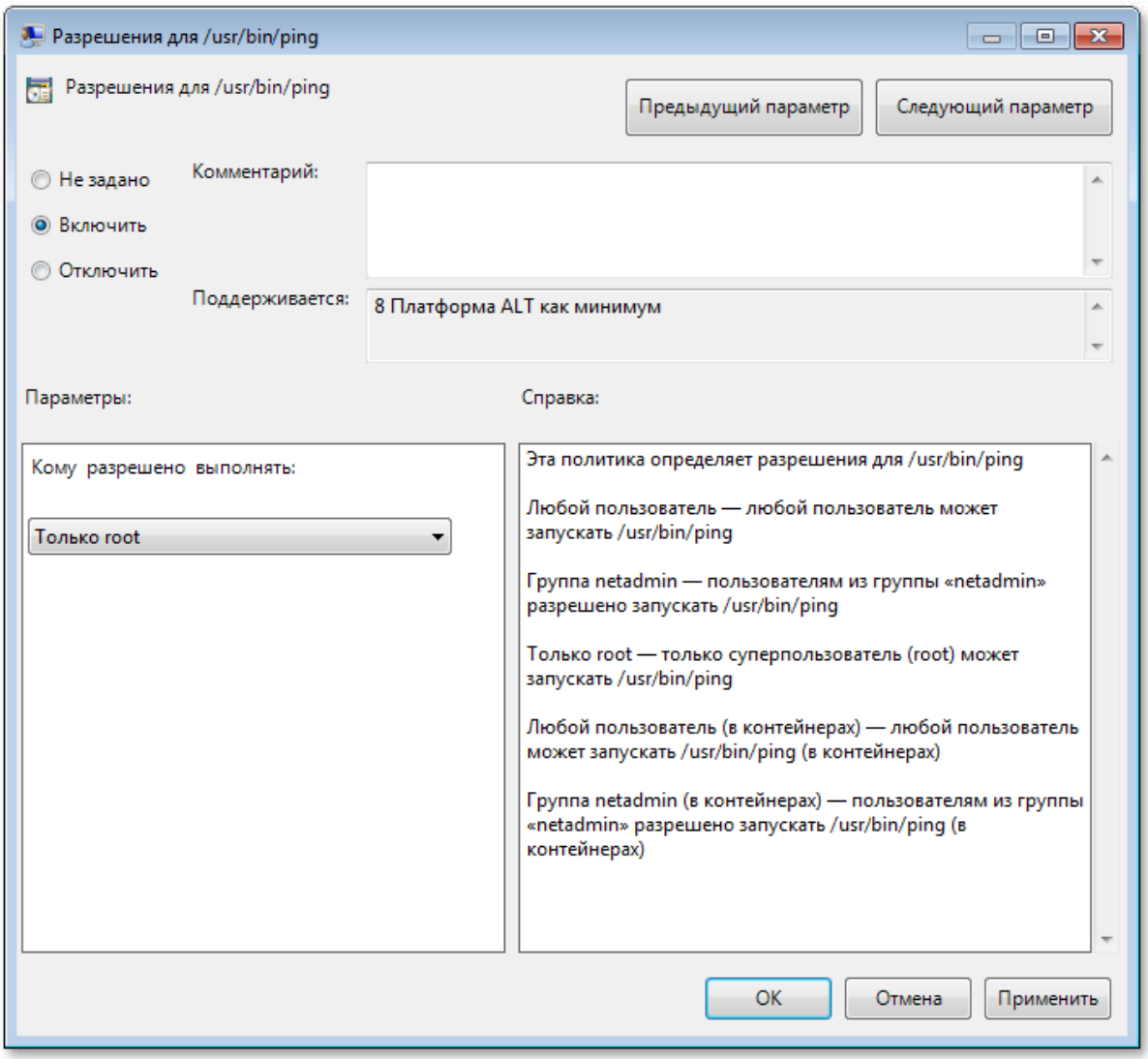
2. Создать новый объект групповой политики (GPO) и связать его с подразделением (OU), в который входят машины или учетные записи пользователей.

3. В контекстном меню GPO, выбрать пункт **Редактировать**. Откроется редактор GPO.

4. Перейти в **Конфигурация компьютера** → **Политики** → **Административные шаблоны** → **Система ALT**. Здесь есть несколько разделов, соответствующих категориям control. Выбрать раздел **Сетевые приложения**, в правом окне редактора отобразится список политик:



5. Дважды щелкнуть левой кнопкой мыши на политике **`Разрешения для /usr/bin/ping`**. Откроется диалоговое окно настройки политики. Выбрать параметр **Включить**, в выпадающем списке **Кому разрешено выполнять** выбрать пункт **Только root** и нажать кнопку **Применить**:



6. После обновления политики на клиенте, выполнять команду **`ping`** сможет только администратор:

```
$ ping localhost
bash: ping: команда не найдена
$ /usr/bin/ping localhost
bash: /usr/bin/ping: Отказано в доступе
# control ping
restricted
```

Важно

Для диагностики механизмов применения групповых политик на клиенте можно выполнить команду:

```
# gpoa --loglevel 0
```

В выводе команды будут фигурировать полученные групповые объекты. В частности, соответствующий уникальный код (GUID) объекта.

Глава 48. Samba в режиме файлового сервера

Samba — пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных операционных системах по протоколу SMB/CIFS. Имеет клиентскую и серверную части.

48.1. Настройка `smb.conf`

Пример настройки **`/etc/samba/smb.conf`** для работы Samba в режиме файлового сервера с двумя открытыми для общего доступа ресурсами и принтером (закомментированные параметры действуют по умолчанию):

```
    workgroup = workgroup
    server string = Samba Server Version %v
    map to guest = Bad User
;   idmap config * : backend = tdb
    guest ok = yes
    cups options = raw
    security = user
;   encrypt passwords = yes
;   guest account = nobody

[printers]
    comment = All Printers
    path = /var/spool/samba
    browseable = no
;   guest ok = no
;   writable = No
    printable = yes


# A publicly accessible directory, but read only, except for people in
# the "staff" group
[public]
    comment = Public Stuff
    path = /home/samba
    public = yes
    writable = yes
;   printable = no
    write list = +staff
;   browseable = yes

[Free]
    path = /mnt/win/Free
    read only = no
;   browseable = yes
    guest ok = yes
```

48.2. Монтирование ресурса Samba через `/etc/fstab`

Создать файл **`/etc/samba/sambacreds`** (например, командой **`mcedit /etc/samba/sambacreds`**), с содержимым:

```
username=имя_пользователя
password=пароль
```

Для монтирования ресурса Samba в **`/etc/fstab`** необходимо прописать:

```
//server/public /mnt/server_public cifs users,credentials=/etc/samba/
sambacreds 0 0
```

Для защиты информации, права на файл **`/etc/samba/sambacreds`**, надо установить так, чтобы файл был доступен только владельцу:

```
# chmod 600 /etc/samba/sambacreds
```

и принадлежать root:

```
# chown root: /etc/samba/sambacreds
```

Глава 49. SOGo

SOGo — сервер групповой работы, аналогичный Microsoft Exchange, с веб-интерфейсом и доступом по MAPI для Microsoft Outlook.

SOGo обеспечивает веб-интерфейс на основе AJAX и поддерживает различные нативные клиенты с помощью стандартных протоколов.

Возможности SOGo:

- общие почтовые папки, календари и адресные книги;
- веб-интерфейс, аналогичный Outlook Web Access;
- поддержка протоколов CalDAV, CardDAV, GroupDAV, Microsoft ActiveSync, IMAP и SMTP;
- доступ по MAPI для Microsoft Outlook, не требующий внешних модулей;
- делегирование, уведомления, резервирование, поддержка категорий и почтовых фильтров;
- поддержка нескольких почтовых ящиков в веб-интерфейсе;
- Single sign-on с помощью CAS, WebAuth или Kerberos.

Предупреждение

MAPI over HTTPS не поддерживается.

49.1. Установка

Для установки стабильной версии SOGo необходимо выполнить команду (драйвер к PostgreSQL будет установлен автоматически):

```
# apt-get install task-sogo
```

49.2. Подготовка среды

Подготовить к запуску и настроить службы PostgreSQL:

- создать системные базы данных:

```
# /etc/init.d/postgresql initdb
```

- запустить службу:

```
# service postgresql start
```

- создать пользователя sogo и базу данных sogo (под правами root):

```
# su - postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --
no-createrole sogo'
# su - postgres -s /bin/sh -c 'createdb -O sogo sogo'
# service postgresql restart
```

Настройка Samba DC:

- Пользователи расположены в домене Active Directory, расположенном на контроллере с Samba DC. Необходимо предварительно развернуть сервер Samba AD DC (см. Samba 4 в роли контроллера домена Active Directory).
- Создать в домене пользователя sogo с паролем Pa$$word (при запросе дважды ввести пароль):

```
# samba-tool user create sogo
# samba-tool user setexpiry --noexpiry sogo
```

Настройка SOGo (настраивается на домен test.alt):

- заполнить файл конфигурации **/etc/sogo/sogo.conf**:

```
{
  SOGoProfileURL = "postgresql://sogo@/sogo/sogo_user_profile";
  OCSFolderInfoURL = "postgresql://sogo@/sogo/sogo_folder_info";
  OCSSessionsFolderURL = "postgresql://sogo@/sogo/sogo_sessions_folder";
  OCSEMailAlarmsFolderURL = "postgresql://sogo@/sogo/sogo_alarms_folder";
```

```
  SOGoEnableEMailAlarms = YES;
  SOGoDraftsFolderName = Drafts;
  SOGoSentFolderName = Sent;
  SOGoTrashFolderName = Trash;
  SOGoIMAPServer = "imaps://localhost:993?
tlsVerifyMode=allowInsecureLocalhost";
  SOGoMailingMechanism = sendmail;
  SOGoForceExternalLoginWithEmail = NO;
  NGImap4ConnectionStringSeparator = "/";
  SOGoUserSources =  (
    {
        id = sambaLogin;
        displayName = "SambaLogin";
        canAuthenticate = YES;
        type = ldap;
        CNFieldName = cn;
        IDFieldName = cn;
        UIDFieldName = sAMAccountName;
        hostname = "ldaps://127.0.0.1";
        baseDN = "CN=Users,DC=test,DC=alt";
        bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
        bindPassword = "Pa$$word";
        bindFields = (sAMAccountName);
    },
    {
        id = sambaShared;
        displayName = "Shared Addressbook";
        canAuthenticate = NO;
        isAddressBook = YES;
        type = ldap;
        CNFieldName = cn;
        IDFieldName = mail;
        UIDFieldName = mail;
        hostname = "ldaps://127.0.0.1";
        baseDN = "CN=Users,DC=test,DC=alt";
        bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
        bindPassword = "Pa$$word";
        filter = "((NOT isCriticalSystemObject='TRUE') AND (mail='*') AND
(NOT objectClass=contact))";
    },
    {
        id = sambaContacts;
        displayName = "Shared Contacts";
        canAuthenticate = NO;
        isAddressBook = YES;
        type = ldap;
        CNFieldName = cn;
        IDFieldName = mail;
        UIDFieldName = mail;
        hostname = "ldaps://127.0.0.1";
        baseDN = "CN=Users,DC=test,DC=alt";
        bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
        bindPassword = "Pa$$word";
        filter = "((((objectClass=person) AND (objectClass=contact) AND
((uidNumber>=2000) OR (mail='*')))
                AND (NOT isCriticalSystemObject='TRUE') AND (NOT
showInAdvancedViewOnly='TRUE') AND (NOT uid=Guest))
                OR (((objectClass=group) AND (gidNumber>=2000)) AND (NOT
isCriticalSystemObject='TRUE') AND (NOT showInAdvancedViewOnly='TRUE')))";
```

```
        mapping = {
            displayname = ("cn");
        };
    }
  );
  SOGoSieveScriptsEnabled = YES;
  SOGoLanguage = Russian;
  SOGoTimeZone = Europe/Moscow;
  SOGoFirstDayOfWeek = 1;
}
```

- включить службы по умолчанию и перезапустить их:

```
# for s in samba postgresql memcached sogo httpd2;do chkconfig $s
on;service $s restart;done
```

Возможные ошибки будут записаны в файл журнала **/var/log/sogo/sogo.log**

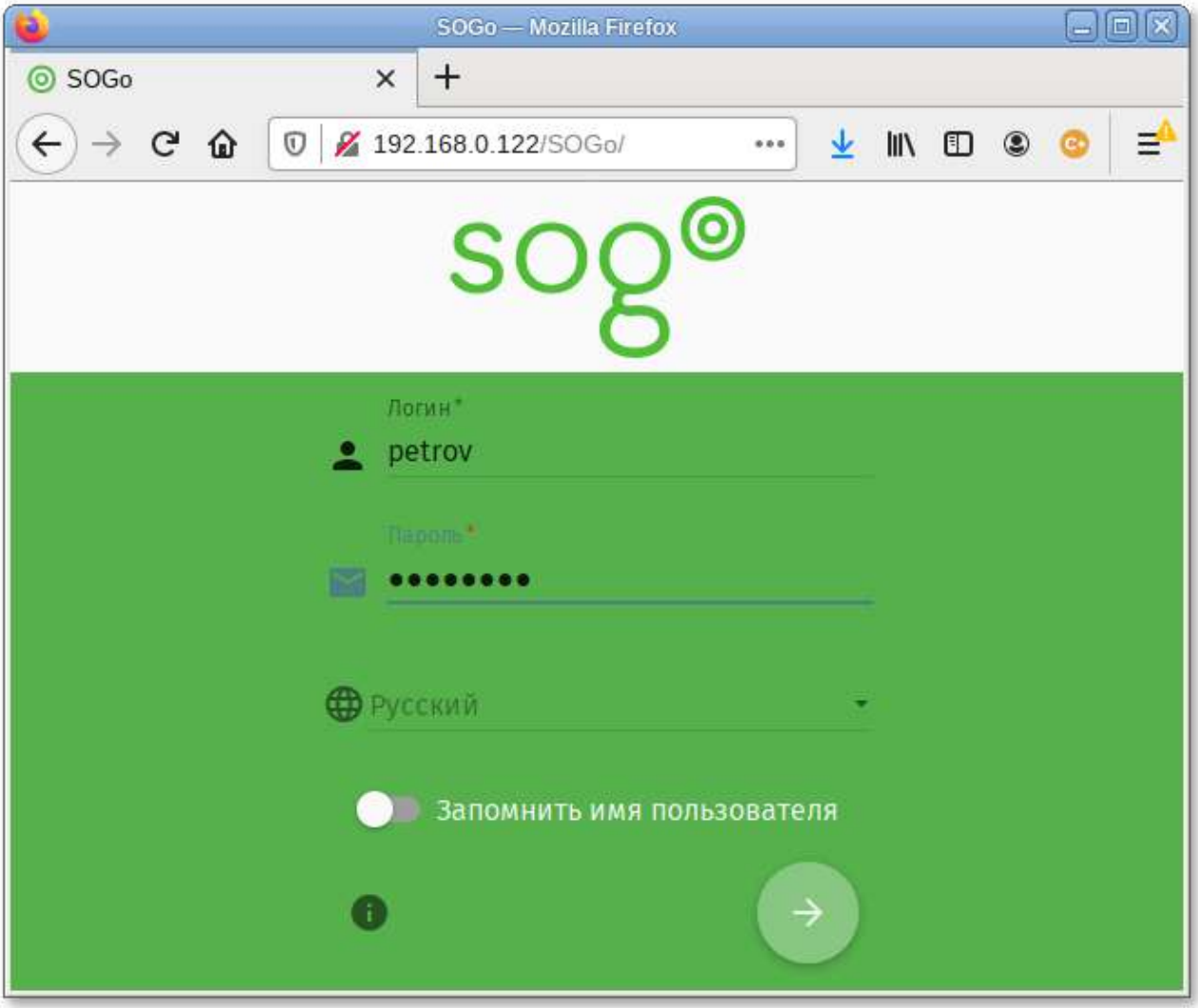
49.3. Включение веб-интерфейса

Для включения веб-интерфейса необходимо выполнить команды:

```
# a2enmod proxy
# a2enmod proxy_http
# a2enmod authn_core
# a2enmod authn_file
# a2enmod auth_basic
# a2enmod authz_user
# a2enmod env
# a2enmod dav
# a2enmod headers
# a2enmod rewrite
# a2enmod version
# a2enmod setenvif
# a2ensite SOGo
# service httpd2 restart
# service sogo restart
```

Теперь можно войти по адресу:

```
https://<адрес_сервера>/SOGo/
```



Примечание

Если при входе в веб-интерфейс возникает ошибка «Неправильный логин или пароль» и в логах **/var/log/sogo/sogo.log** есть ошибки вида:

```
Jul 06 16:14:51 sogod [12257]: [ERROR] <0x0x5578db070b40[LDAPSource]>
Could not bind to the LDAP server ldaps://127.0.0.1 (389) using the
bind DN: CN=sogo,CN=Users,DC=test,DC=alt
```

Следует в файл **/etc/openldap/ldap.conf** добавить опцию

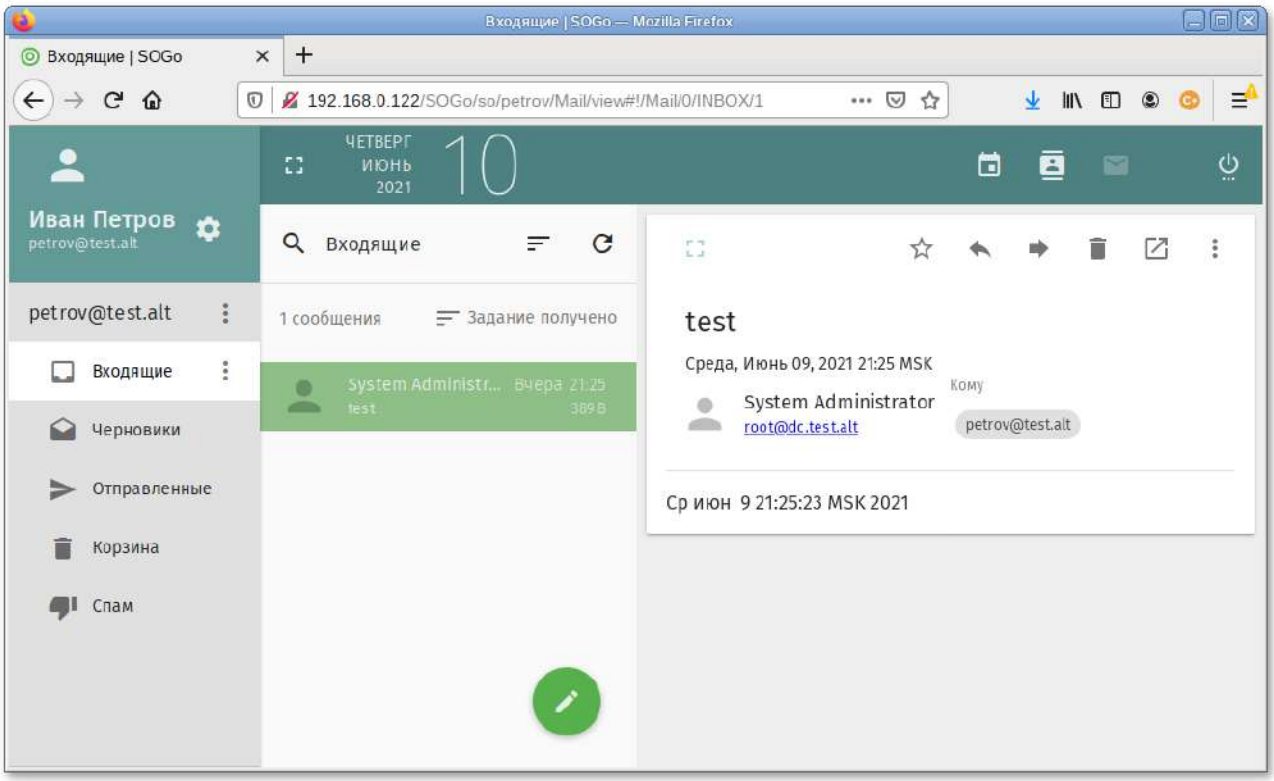
```
TLS_REQCERT allow
```

и перезапустить службы samba и sogo:

```
# service samba restart
# service sogo restart
```

49.4. Настройка электронной почты

Для использования электронной почты в SOGo необходимо настроить аутентификацию в Active Directory для Postfix и Dovecot.



В примере используется следующая конфигурация:

- имя домена: test.alt;
- размещение почты: **`/var/mail/<имя_домена>/<имя_пользователя>`** (формат maildir);
- доступ на чтение почты: IMAP (порт 993), SSL;
- доступ на отправку почты: SMTP (порт 465), SSL/STARTTLS;
- данные аутентификации: email с доменом (например, petrov@test.alt) или имя пользователя.

Предупреждение

Доступ к серверу LDAP осуществляется по протоколу ldap без шифрования. Для SambaDC необходимо отключить ldaps в **`/etc/samba/smb.conf`** в секции [global]:

```
ldap server require strong auth = no
```

Предварительно необходимо создать пользователя vmail (пароль Pa$$word) с не истекающей учётной записью:

```
# samba-tool user create -W Users vmail
# samba-tool user setexpiry vmail --noexpiry
```

49.4.1. Настройка Postfix

Установить пакет postfix-ldap:

```
# apt-get install postfix-ldap
```

В каталоге **/etc/postfix** изменить файлы для домена test.alt:

- изменить содержимое файла **main.cf**:

```
# Global Postfix configuration file.  This file lists only a small subset
# of all parameters.  For the syntax, and for a complete parameter list,
# see the postconf(5) manual page.  For a commented and more complete
# version of this file see /etc/postfix/main.cf.dist
mailbox_command = /usr/libexec/dovecot/dovecot-lda -f "$SENDER" -a
"$RECIPIENT"
inet_protocols = ipv4

# Mappings
virtual_mailbox_base = /var/mail
virtual_mailbox_domains = test.alt
virtual_mailbox_maps = ldap:/etc/postfix/ad_local_recipients.cf
virtual_alias_maps = ldap:/etc/postfix/ad_mail_groups.cf
virtual_transport = dovecot
local_transport = virtual
local_recipient_maps = $virtual_mailbox_maps

# SSL/TLS
smtpd_use_tls = yes
smtpd_tls_security_level = encrypt
#smtpd_tls_security_level = may
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain = test.alt
smtpd_sasl_path = private/auth
smtpd_sasl_type = dovecot
smtpd_sender_login_maps = ldap:/etc/postfix/ad_sender_login.cf
smtpd_tls_auth_only = yes
smtpd_tls_cert_file = /var/lib/ssl/certs/dovecot.cert
smtpd_tls_key_file = /var/lib/ssl/private/dovecot.key
smtpd_tls_CAfile = /var/lib/ssl/certs/dovecot.pem

smtpd_recipient_restrictions = permit_mynetworks,
reject_unauth_destination, per-mit_sasl_authenticated, reject
smtpd_sender_restrictions = reject_authenticated_sender_login_mismatch
```

- файл **/etc/postfix/mydestination** должен быть пустым;

- в файл **master.cf** необходимо добавить строки:

```
dovecot   unix  -       n       n       -       -       pipe
  flags=DRhu user=mail:mail argv=/usr/libexec/dovecot/deliver -d $
{recipient}
smtps     inet  n       -       n       -       -       smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

- создать файл **ad_local_recipients.cf**:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
scope = sub
query_filter = (&(|(mail=%s)(otherMailbox=%u@%d))
(sAMAccountType=805306368))
result_filter = %s
result_attribute = mail
special_result_attribute = member

bind = yes
bind_dn = cn=vmail,cn=users,dc=test,dc=alt
bind_pw = Pa$$word
```

- создать файл **ad_mail_groups.cf**:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
timeout = 3
scope = sub
query_filter = (&(mail=%s)(sAMAccountType=268435456))
result_filter = %s
result_attribute = mail
special_result_attribute = member

bind = yes
bind_dn = cn=vmail,cn=users,dc=test,dc=alt
bind_pw = Pa$$word
```

- создать файл **ad_sender_login.cf**:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
scope = sub
query_filter = (&(objectClass=user)(|(sAMAccountName=%s)(mail=%s)))
result_attribute = mail

bind = yes
bind_dn = cn=vmail,cn=users,dc=test,dc=alt
bind_pw = Pa$$word
```

- перезапустить службу postfix:

```
# service postfix restart
```

Проверка конфигурации Postfix (в выводе не должно быть никаких сообщений):

```
# postconf >/dev/null
```

Проверка пользователя почты petrov:

```
# postmap -q petrov@test.alt ldap:/etc/postfix/ad_local_recipients.cf
petrov@test.alt
```

Проверка входа:

```
# postmap -q petrov@test.alt ldap:/etc/postfix/ad_sender_login.cf
petrov@test.alt
```

Проверка общего адреса e-mail:

```
# samba-tool group add --mail-address=sales@test.alt Sales
Added group Sales
# samba-tool group addmembers Sales ivanov,petrov
Added members to group Sales
# postmap -q sales@test.alt ldap:/etc/postfix/ad_mail_groups.cf
sales@test.alt,ivanov@test.alt,petrov@test.alt
```

49.4.2. Настройка Dovecot

Установить Dovecot:

```
# apt-get install dovecot
```

Изменить файлы для домена test.alt:

- создать файл **/etc/dovecot/dovecot-ldap.conf.ext**:

```
hosts            = test.alt:3268
ldap_version     = 3
auth_bind        = yes
dn               = cn=vmail,cn=Users,dc=test,dc=alt
dnpass           = Pa$$word
base             = cn=Users,dc=test,dc=alt
scope            = subtree
deref            = never

user_filter = (&(objectClass=user)(|(mail=%Lu)(sAMAccountName=%Lu)))
user_attrs  = =uid=8,gid=12,mail=user
pass_filter = (&(objectClass=user)(|(mail=%Lu)(sAMAccountName=%Lu)))
pass_attrs = mail=user
```

- изменить файл **/etc/dovecot/conf.d/10-auth.conf**:

```
#auth_username_format = %Lu
#auth_gssapi_hostname = "$ALL"
#auth_krb5_keytab = /etc/dovecot/dovecot.keytab
#auth_use_winbind = no
#auth_winbind_helper_path = /usr/bin/ntlm_auth
#auth_failure_delay = 2 secs
auth_mechanisms = plain
!include auth-ldap.conf.ext
```

- изменить файл **/etc/dovecot/conf.d/10-mail.conf**:

```
mail_location = maildir:/var/mail/%d/%n:UTF-8:INBOX=/var/mail/%d/%n/Inbox
mail_uid = mail
mail_gid = mail
first_valid_uid = 5
first_valid_gid = 5
```

- изменить файл **/etc/dovecot/conf.d/10-master.conf**:

```
service imap-login {
  inet_listener imap {
    port = 0
  }
  inet_listener imaps {
  }
}
service pop3-login {
  inet_listener pop3 {
    port = 0
  }
  inet_listener pop3s {
    port = 0
  }
}
service lmtp {
  unix_listener lmtp {
  }
}
service imap {
}
service pop3 {
}
service auth {
  unix_listener auth-userdb {
  }
  unix_listener /var/spool/postfix/private/auth {
    mode = 0600
    user = postfix
    group = postfix
  }
}
service auth-worker {
}
service dict {
  unix_listener dict {
  }
}
```

- изменить файл **/etc/dovecot/conf.d/15-lda.conf**:

```
protocol lda {
  hostname = test.alt
  postmaster_address = administrator@test.alt
}
```

- изменить файл **/etc/dovecot/conf.d/15-mailboxes.conf**:

```
namespace inbox {
  inbox = yes
  mailbox Drafts {
    auto = subscribe
    special_use = \Drafts
  }
  mailbox Junk {
    auto = subscribe
    special_use = \Junk
  }
  mailbox Trash {
    auto = subscribe
    special_use = \Trash
  }
  mailbox Sent {
    auto = subscribe
    special_use = \Sent
  }
  mailbox "Sent Messages" {
    special_use = \Sent
  }
}
```

- перезапустить службу dovecot:

```
# service dovecot restart
```

Проверка конфигурации Dovecot (в выводе не должно быть никаких сообщений):

```
# doveconf >/dev/null
```

49.4.3. Безопасность

Так как конфигурационные файлы содержат пароль пользователя LDAP, их необходимо сделать недоступным для чтения прочим пользовате:

```
# chown dovecot:root /etc/dovecot/dovecot-ldap.conf.ext
# chmod 0640 /etc/dovecot/dovecot-ldap.conf.ext
# chown root:postfix /etc/postfix/ad_local_recipients.cf /etc/postfix/
ad_mail_groups.cf /etc/postfix/ad_sender_login.cf
# chmod 0640 /etc/postfix/ad_local_recipients.cf /etc/postfix/
ad_mail_groups.cf /etc/postfix/ad_sender_login.cf
```

Перезапустить службы:

```
# service dovecot restart
# service postfix restart
```

49.4.4. Проверка конфигурации

Проверка SMTP:

```
# date | mail -s test petrov@test.alt
# mailq
Mail queue is empty
```

Проверка IMAP (выход по **Ctrl**+**D**):

```
# openssl s_client -crlf -connect test.alt:993
...
tag login petrov@test.alt Pa$$word
tag OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE
IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT
MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS
LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES
WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE] Logged in
```

Глава 50. FreeIPA

FreeIPA — это комплексное решение по управлению безопасностью Linux-систем, 389 Directory Server, MIT Kerberos, NTP, DNS, Dogtag, состоит из веб-интерфейса и интерфейса командной строки.

FreeIPA является интегрированной системой проверки подлинности и авторизации в сетевой среде Linux, FreeIPA сервер обеспечивает централизованную проверку подлинности, авторизацию и контроль за аккаунтами пользователей сохраняя сведения о пользователе, группах, узлах и других объектах необходимых для обеспечения сетевой безопасности.

50.1. Установка сервера FreeIPA

В качестве примера показана установка сервера **FreeIPA** со встроенным DNS сервером и доменом EXAMPLE.TEST в локальной сети 192.168.0.0/24.

Во избежание конфликтов с разворачиваемым tomcat необходимо отключить ahttpd, работающий на порту 8080, а также отключить HTTPS в Apache2:

```
# service ahttpd stop
# a2dissite 000-default_https
# a2disport https
# service httpd2 condreload
```

Установить необходимые пакеты (если во время установки сервера не был выбран пункт сервер FreeIPA):

```
# apt-get install freeipa-server freeipa-server-dns
```

Задать имя сервера:

```
# hostnamectl set-hostname ipa.example.test
```

Запустить скрипт настройки сервера. В пакетном режиме:

```
# ipa-server-install -U --hostname=$(hostname) -r EXAMPLE.TEST -n
example.test -p 12345678 -a 12345678 --setup-dns --no-forwarders --no-reverse
```

Предупреждение

Если в дальнейшем на данной машине будет настраиваться **Fleet Commander Admin**, необходимо устанавливать и настраивать FreeIPA сервер, с созданием домашнего каталога (опция **--mkhomedir**):

```
# ipa-server-install -U --hostname=$(hostname) -r EXAMPLE.TEST -n
example.test -p 12345678 -a 12345678 --setup-dns --no-forwarders --no-
reverse --mkhomedir
```

Или интерактивно:

```
# ipa-server-install
```

Предупреждение

Пароли должны быть не менее 8 символов.

Обратите внимание на ответ на вопрос, не совпадающий с предложенным:

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

остальные вопросы необходимо выбрать по умолчанию (можно просто нажать **Enter**). Так же при установке необходимо ввести пароль администратора системы и пароль администратора каталогов.

Для возможности управлять **FreeIPA** сервером из командной строки необходимо получить билет Kerberos:

```
# kinit admin
```

Добавить в DNS запись о сервере времени:

```
# ipa dnsrecord-add example.test _ntp._udp --srv-priority=0 --srv-weight=100
--srv-port=123 --srv-target=ipa.example.test.
```

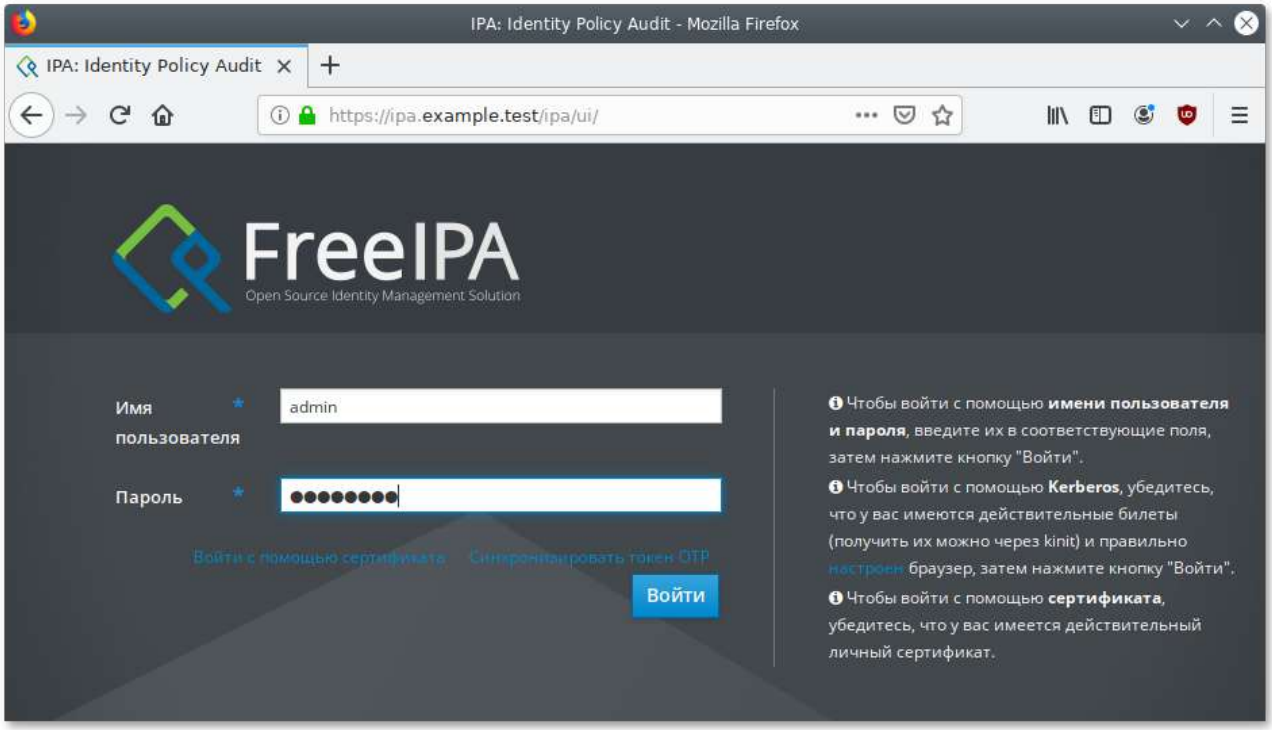
Проверить работу ntp сервера можно командой:

```
# ntpdate -q localhost
server 127.0.0.1, stratum 3, offset 0.000018, delay 0.02568
27 Nov 10:27:00 ntpdate[29854]: adjust time server 127.0.0.1 offset 0.000018
sec
```

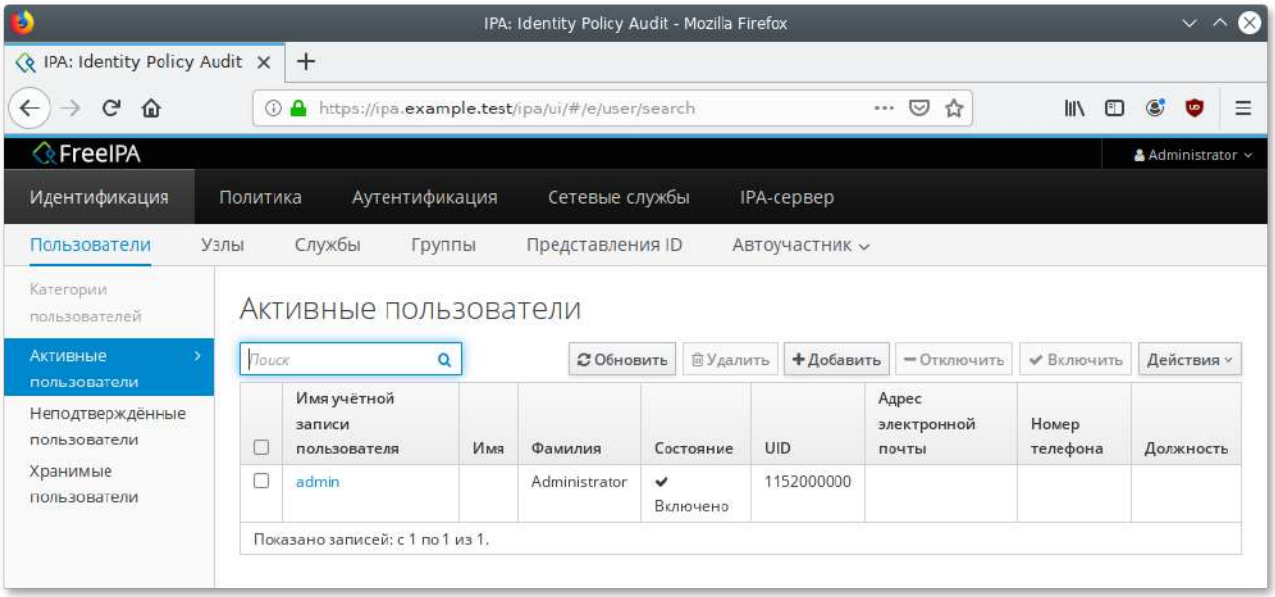
Веб-интерфейс доступен по адресу **https://ipa.example.test/ipa/ui/**.

50.2. Добавление новых пользователей домена

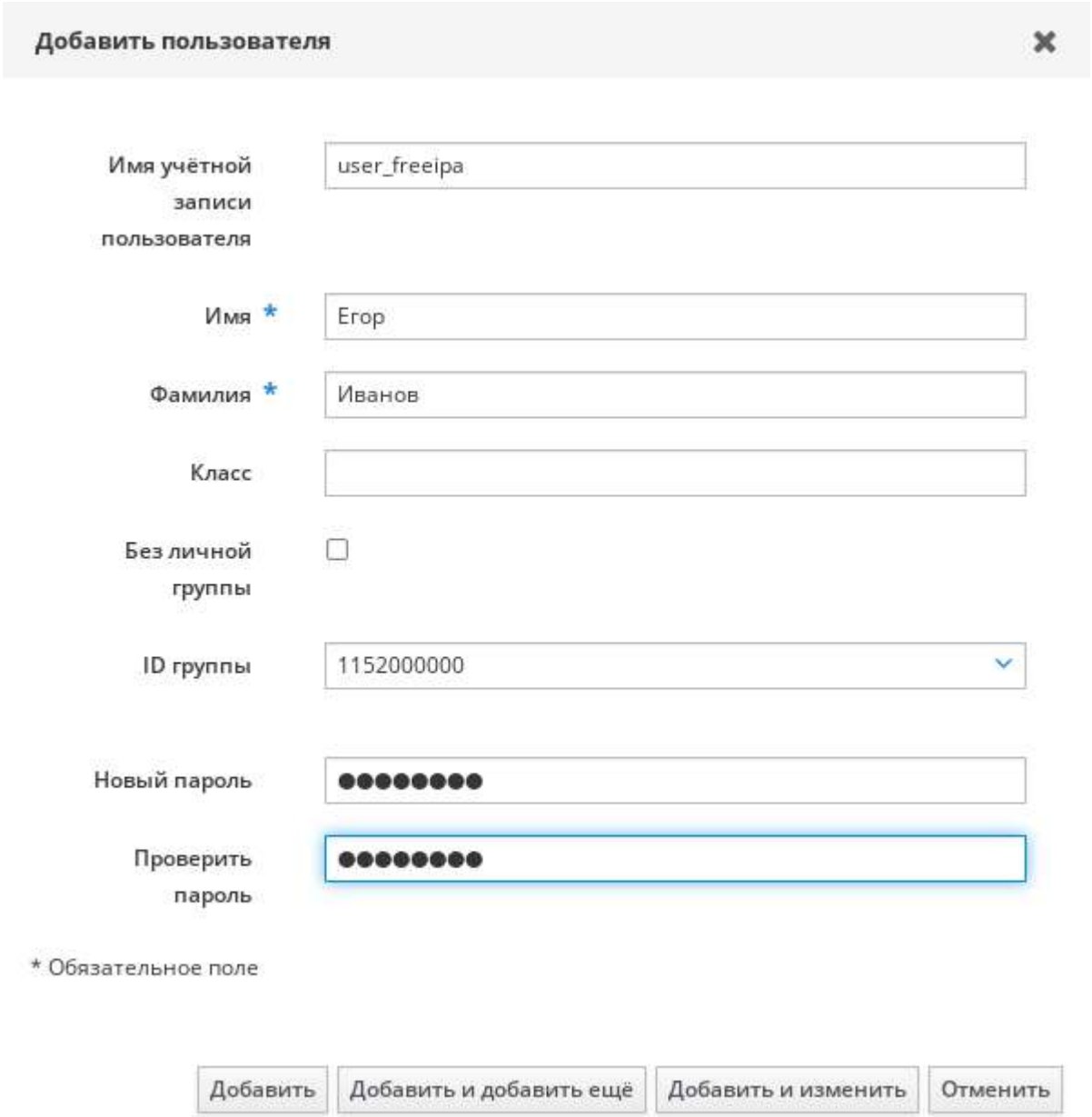
Для добавления новых пользователей можно воспользоваться веб-интерфейсом FreeIPA. Для этого необходимо открыть в веб-браузере адрес **`https://ipa.example.test/ipa/ui/`** и ввести данные администратора для входа в систему.



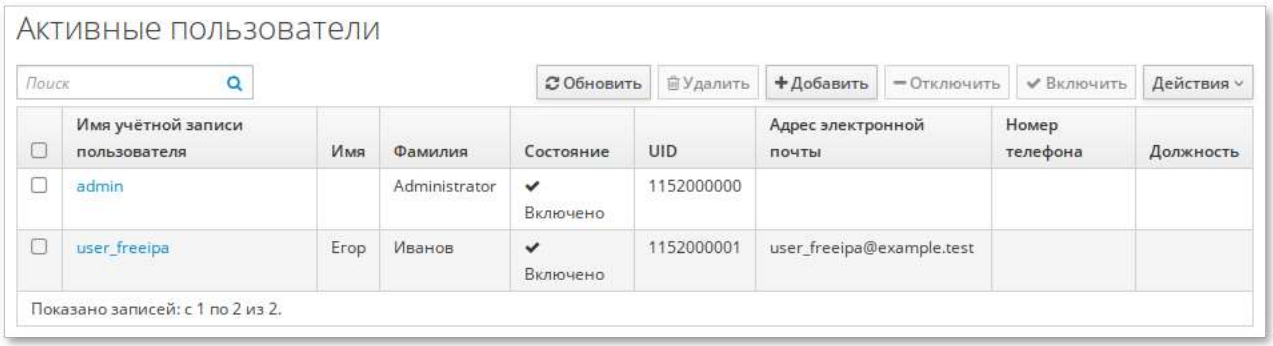
После успешной авторизации можно создать нового пользователя домена. Для этого в окне **Пользователи домена** необходимо нажать кнопку **Добавить**.



В открывшемся окне необходимо ввести данные пользователя и нажать кнопку **Добавить**:



Созданный пользователь появится в списке пользователей:



50.3. Установка FreeIPA клиента и подключение к серверу

50.3.1. Установка FreeIPA клиента

Установить необходимые пакеты:

```
# apt-get install freeipa-client libsss_sudo krb5-kinit bind-utils libbind
zip task-auth-freeipa
```

Примечание

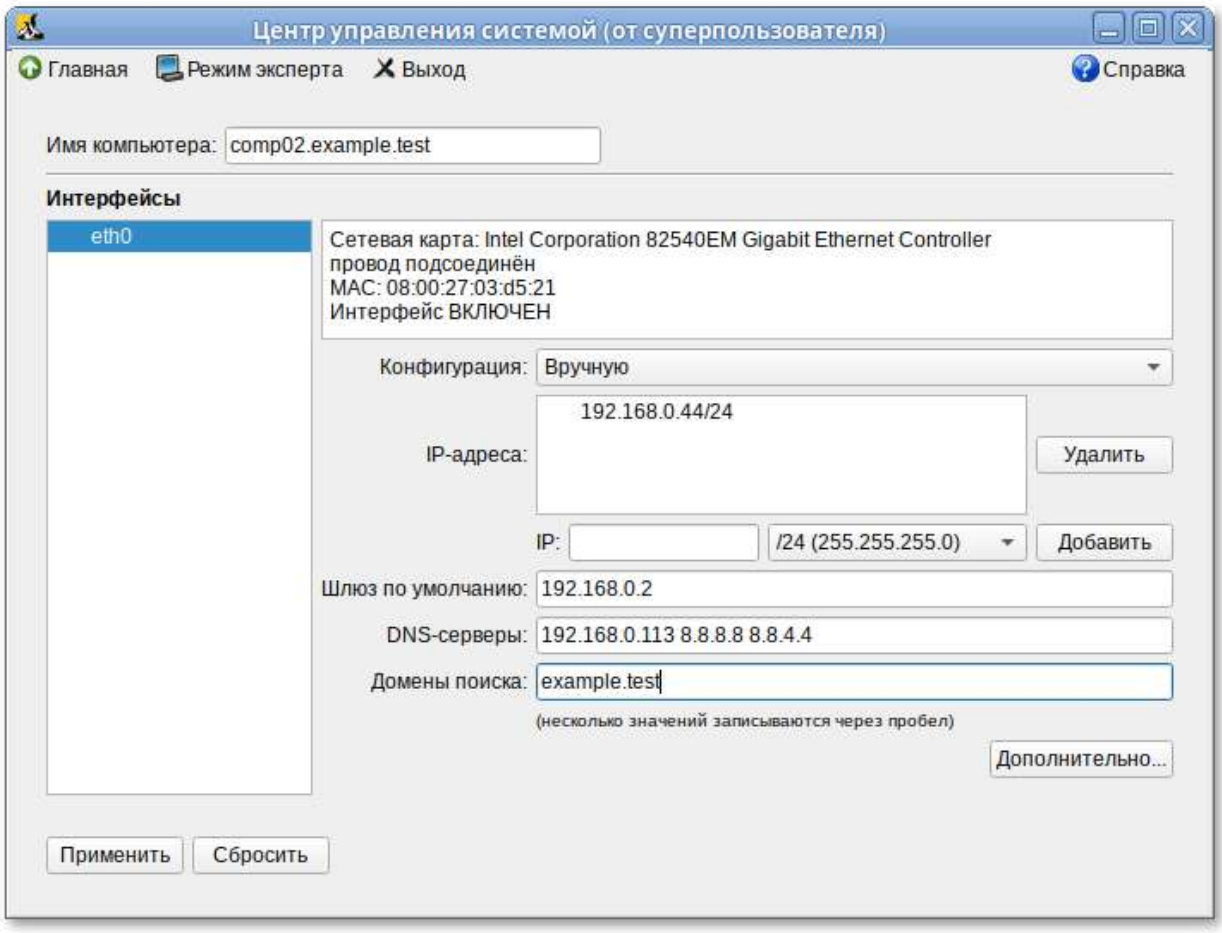
Очистить конфигурацию freeipa-client невозможно. В случае если это необходимо (например, для удаления, переустановки freeipa-client) следует переустановить систему.

Задать имя компьютера:

```
# hostnamectl set-hostname comp01.example.test
```

Клиентские компьютеры должны быть настроены на использование DNS-сервера, который был сконфигурирован на сервере FreeIPA во время его установки. В сетевых настройках необходимо указать использовать сервер FreeIPA для разрешения имен. Эти настройки можно выполнить как в графическом интерфейсе, так и в консоли:

- В Центре управления системой в разделе **Сеть** → **Ethernet интерфейсы** указать в поле **DNS-серверы** IP-адрес FreeIPA сервера и домен для поиска:



- В консоли:
  - добавить DNS сервер, для этого необходимо создать файл **/etc/net/ifaces/eth0/resolv.conf** со следующим содержимым:

    ```
    nameserver 192.168.0.113
    ```

    где 192.168.0.113 — IP-адрес FreeIPA сервера.
  - указать службе resolvconf использовать DNS FreeIPA и домен для поиска. Для этого в файле **/etc/resolvconf.conf** добавить/отредактировать следующие параметры:

    ```
    interface_order='lo lo[0-9]* lo.* eth0'
    search_domains=example.test
    ```

    где eth0 — интерфейс на котором доступен FreeIPA сервер, example.test — домен.
  - обновить DNS адреса:

    ```
    # resolvconf -u
    ```

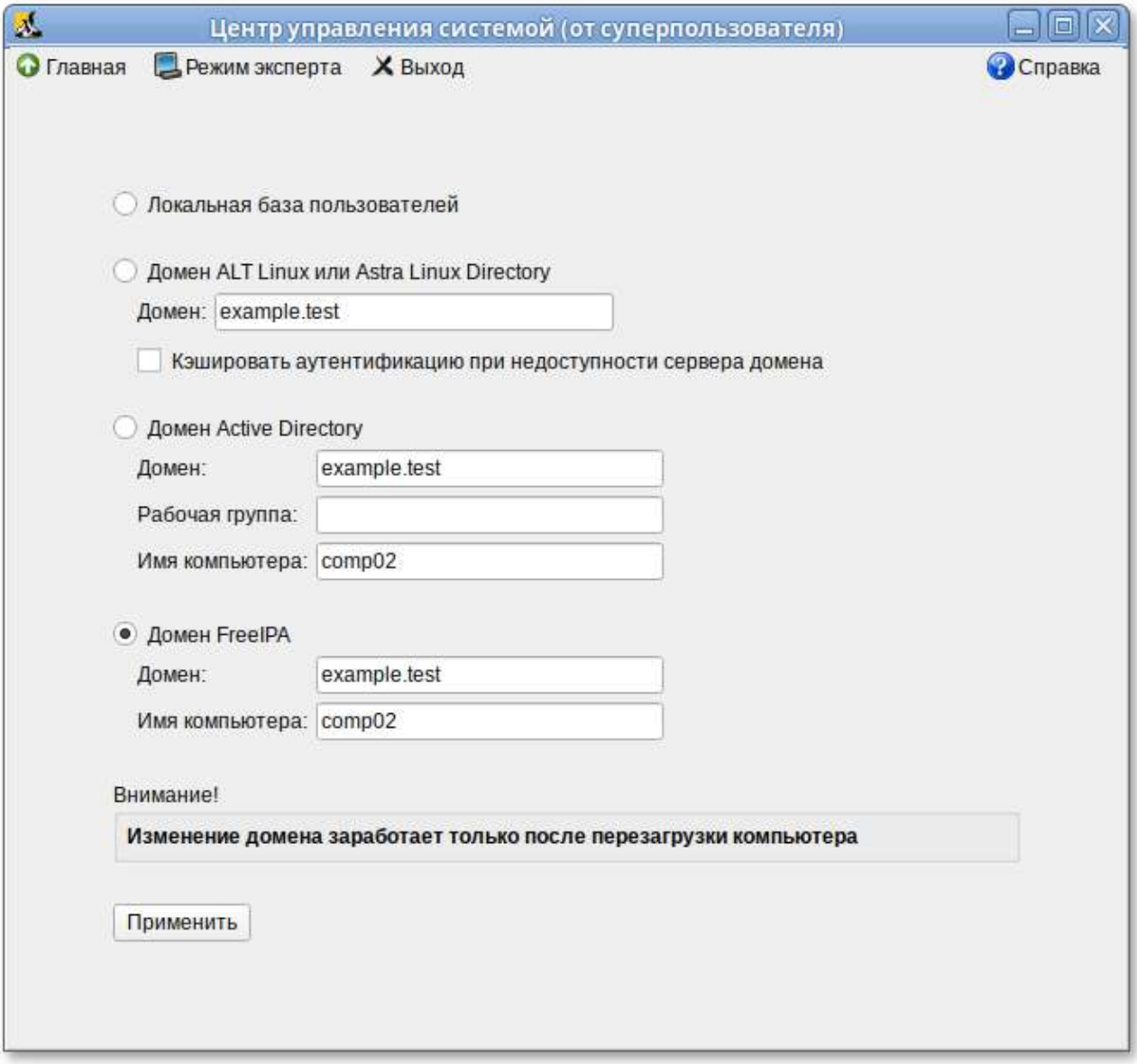
В результате выполненных действий в файле **/etc/resolv.conf** должны появиться строки:

```
search example.test
nameserver 192.168.0.113
```

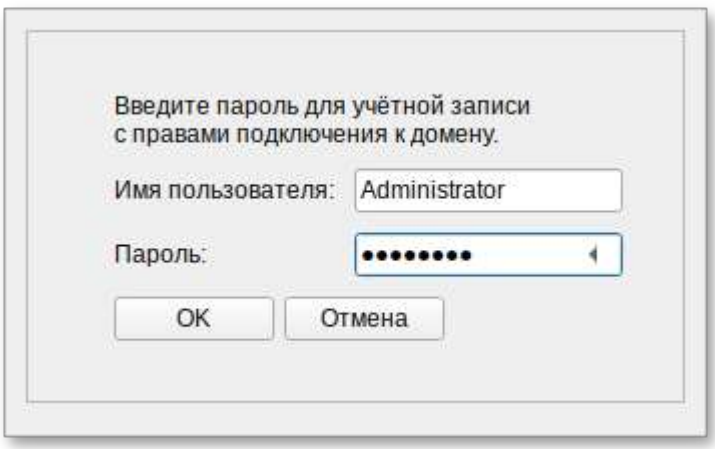
50.3.2. Подключение к серверу в ЦУС

Для ввода рабочей станции в домен FreeIPA, необходимо в Центре управления системой перейти в раздел **Пользователи** → **Аутентификация**.

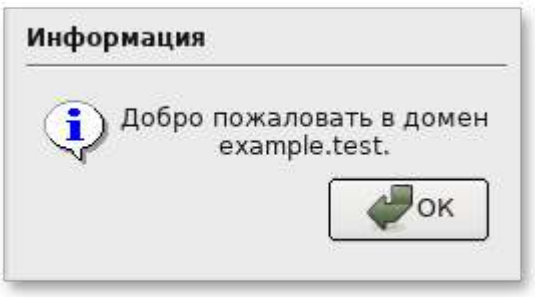
В открывшемся окне следует выбрать пункт **Домен FreeIPA**, заполнить поля **Домен** и **Имя компьютера**, затем нажать кнопку **Применить**.



В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку **ОК**.



В случае успешного подключения, будет выведено соответствующее сообщение.



Перезагрузить рабочую станцию.

50.3.3. Подключение к серверу в консоли

Запустить скрипт настройки клиента в пакетном режиме:

```
# ipa-client-install -U -p admin -w 12345678
```

или интерактивно:

```
# ipa-client-install
```

Если все настроено, верно, скрипт должен выдать такое сообщение:

```
'''Discovery was successful!'''
Client hostname: comp01.example.test
Realm: EXAMPLE.TEST
DNS Domain: example.test
IPA Server: ipa.example.test
BaseDN: dc=example,dc=test
Continue to configure the system with these values? [no]:
```

Необходимо ответить **yes**, ввести имя пользователя, имеющего право вводить машины в домен, и его пароль.

Предупреждение

Если при входе в домен возникает такая ошибка:

```
Hostname (comp01.example.test) does not have A/AAAA record.
Failed to update DNS records.
```

Необходимо проверить IP-адрес доменного DNS сервера в файле **/etc/resolv.conf**.

В случае возникновения ошибки, необходимо перед повторной установкой запустить процедуру удаления:

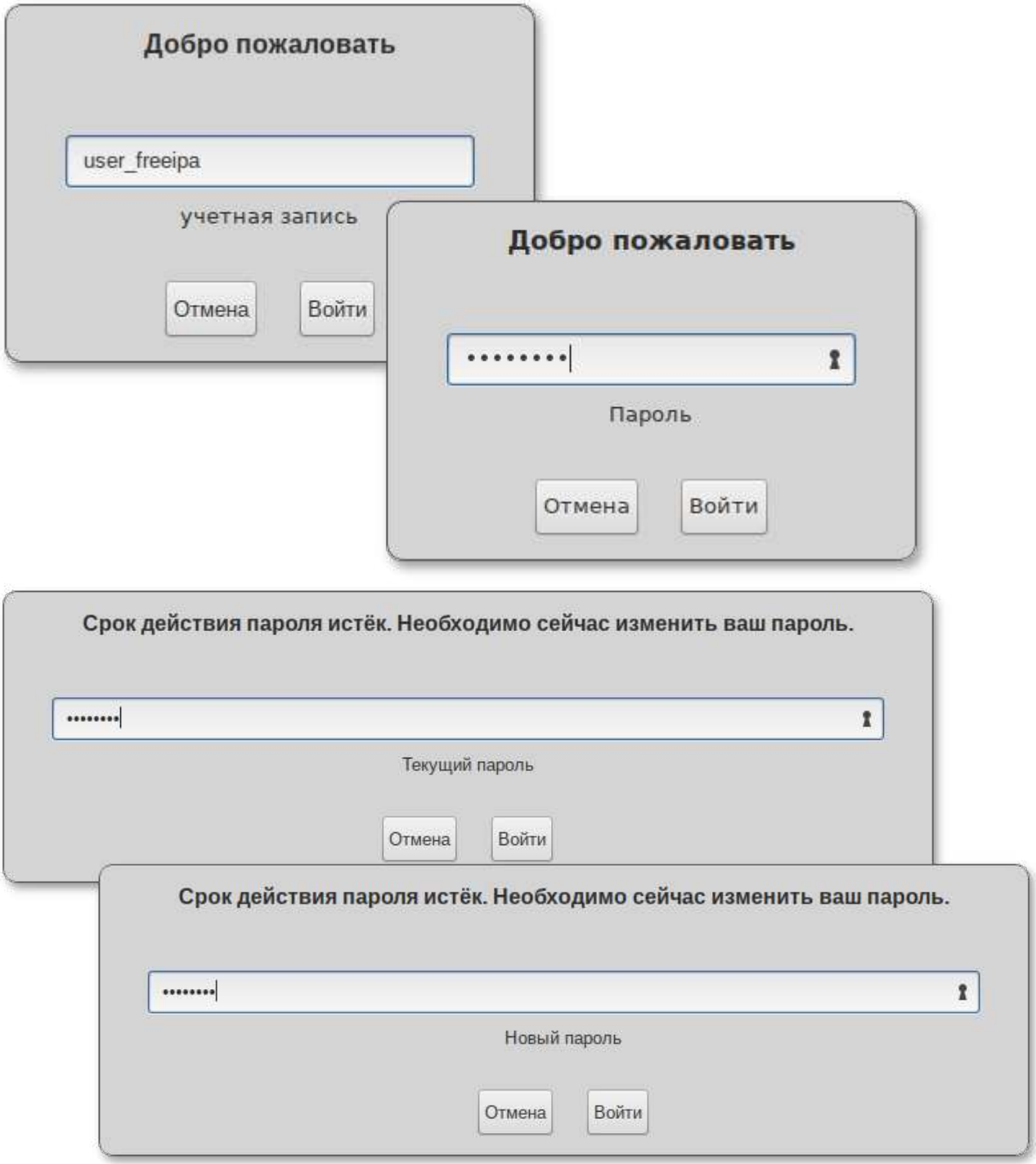
```
# ipa-client-install -U --uninstall
```

Для работы sudo-политик для доменных пользователей на клиентской машине необходимо разрешить доступ к sudo:

```
# control sudo public
```

50.3.4. Вход пользователя

При первом входе пользователя будет запрошен текущий (установленный администратором) пароль и затем у пользователя запрашивается новый пароль и его подтверждение.



Предупреждение

Если машина до этого была в других доменах или есть проблемы со входом пользователей рекомендуется очистить кэш sssd:

```
# systemctl stop sssd
# rm -f /var/lib/sss/db/*
# rm -f /var/lib/sss/mc/*
# systemctl start sssd
```

50.4. Настройка репликации

На втором контроллере домена необходимо установить пакеты:

```
# apt-get install freeipa-client freeipa-server-dns
```

Задать имя сервера:

```
# hostnamectl set-hostname ipabackup.example.test
```

Развернуть и настроить клиента:

```
# ipa-client-install -d --domain=example.test --server=ipa.example.test --
realm=EXAMPLE.TEST --principal=admin --password=12345678 --enable-dns-
updates -U
```

После выполнения этой операции хост ipabackup.example.test должен появиться в веб-интерфейсе FreeIPA.

Далее необходимо настроить репликацию LDAP-каталога:

```
# ipa-replica-install
```

Добавить в DNS второй NTP-сервер:

```
# kinit admin
# ipa dnsrecord-add example.test _ntp._udp --srv-priority=0 --srv-weight=100
--srv-port=123 --srv-target=ipabackup.example.test.
```

Настроить репликацию DNS-зон:

```
# ipa-dns-install
```

Настроить репликацию CA:

```
# ipa-ca-install
```

После настройки и репликации контроллеров посмотреть топологию можно в веб-интерфейсе FreeIPA.

Глава 51. Fleet Commander

Fleet Commander — это инструмент для управления и развертывания профилей в большой сети пользователей и рабочих станций.

Fleet Commander состоит из трех компонентов:

- плагин FreeIPA, который позволяет хранить политики на контроллере домена;
- плагин Cockpit, предоставляющий веб-интерфейс для администрирования;
- служба на стороне клиента, применяющая политики.

Fleet Commander использует libvirt и KVM для запуска сеанса виртуального рабочего стола, где пользователь в реальном времени может редактировать конфигурацию приложений в системе шаблонов. Данная конфигурация затем будет применена на клиентах.

51.1. Установка и настройка Fleet Commander

51.1.1. Настройка libvirt-хоста

В качестве libvirt-хоста может выступать как отдельная машина, так и машина с Fleet Commander Admin.

Установить libvirt:

```
# apt-get install libvirt virt-install
```

Добавить службу libvirtd в автозапуск и запустить её:

```
# systemctl enable --now libvirtd.service
```

Проверить, что default сеть определена, запущена и автозапускаемая:

```
# virsh net-list --all
 Имя       Статус    Автозапуск   Persistent
 ----------------------------------------------
 default   активен   yes          yes
```

Примечание

Определить сеть default, если она не определена:

```
# virsh net-define /usr/share/libvirt/networks/default.xml
```

Отметить default сеть как автозапускаемую:

```
# virsh net-autostart default
```

Запустить default сеть:

```
# virsh net-start default
```

Примечание

В Альт Сервер по умолчанию отключена парольная аутентификация для root в sshd, поэтому если есть необходимость использовать привилегированного пользователя libvirt-хоста, то следует разрешить root-доступ по ssh. Включить парольную аутентификацию для root можно с помощью control (должен быть установлен пакет control-sshd-permit-root-login):

```
# control sshd-permit-root-login enabled
```

и перезагрузить ssh-сервер:

```
# systemctl restart sshd.service
```

После того как ключ будет скопирован, рекомендуется отключить парольную аутентификацию:

```
# control sshd-permit-root-login disabled
# systemctl restart sshd.service
```

Шаблон это виртуальная машина с запущенным на ней Fleet Commander Logger. Шаблон запускается на "админ" машине в live-сессии. Регистратор (логгер) отслеживает сделанные изменения в шаблоне и сохраняет их.

Для настройки новой виртуальной машины шаблонов, достаточно создать виртуальную машину (ВМ) внутри гипервизора libvirt/KVM, запустить её и установить на этой template-машине Fleet Commander Logger. Регистратор будет автоматически запускаться после входа в систему.

Установка ОС на libvirt домен:

- Запустить домен, например:

```
# virt-install --name alt9.2 \
--ram 4096 --cpu kvm64 --vcpus 2 \
--disk pool=default,size=20,bus=virtio,format=qcow2 \
--network network=default --graphics spice,listen=127.0.0.1,password=test
\
--cdrom /var/lib/libvirt/images/alt-workstation-9.2-x86_64.iso
```

- Подключиться к ВМ и произвести установку ОС:

```
$ virt-viewer --connect qemu+ssh://user@192.168.0.190/system
```

- После окончания установки ОС, установить на ВМ Fleet Commander Logger:

```
# apt-get install fleet-commander-logger
```

Примечание

ВМ, которую планируется использовать как шаблон, должна быть выключена, иначе Fleet Commander не позволит запустить live-сессию на этой машине.

51.1.2. Установка и настройка Fleet Commander Admin

Предварительно необходимо установить и настроить FreeIPA сервер, с созданием домашнего каталога (опция **--mkhomedir**).

Установить пакет *freeipa-desktop-profile*:

```
# apt-get install freeipa-desktop-profile
...
Perform the IPA upgrade. This may take a while.
The IPA upgrade was successful.
Завершено.
```

Примечание

Пакет *freeipa-desktop-profile* не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p9. О добавлении репозиториев с использованием графических приложений вы можете почитать в разделе Добавление репозиториев.

Проверить, что плагин работает:

```
# kinit admin
Password for admin@EXAMPLE.TEST:
# ipa deskprofileconfig-show
  Priority of profile application: 1
```

Примечание

Если на выходе команды **ipa deskprofileconfig-show** появляется ошибка:

```
ipa: ERROR: неизвестная команда "deskprofileconfig-show"
```

необходимо почистить кэш текущему пользователю и повторить команду:

```
# rm -rf ~/.cache/ipa
# ipa deskprofileconfig-show
  Priority of profile application: 1
```

Установить Fleet Commander плагин для Cockpit (из репозитория):

```
# apt-get install fleet-commander-admin
```

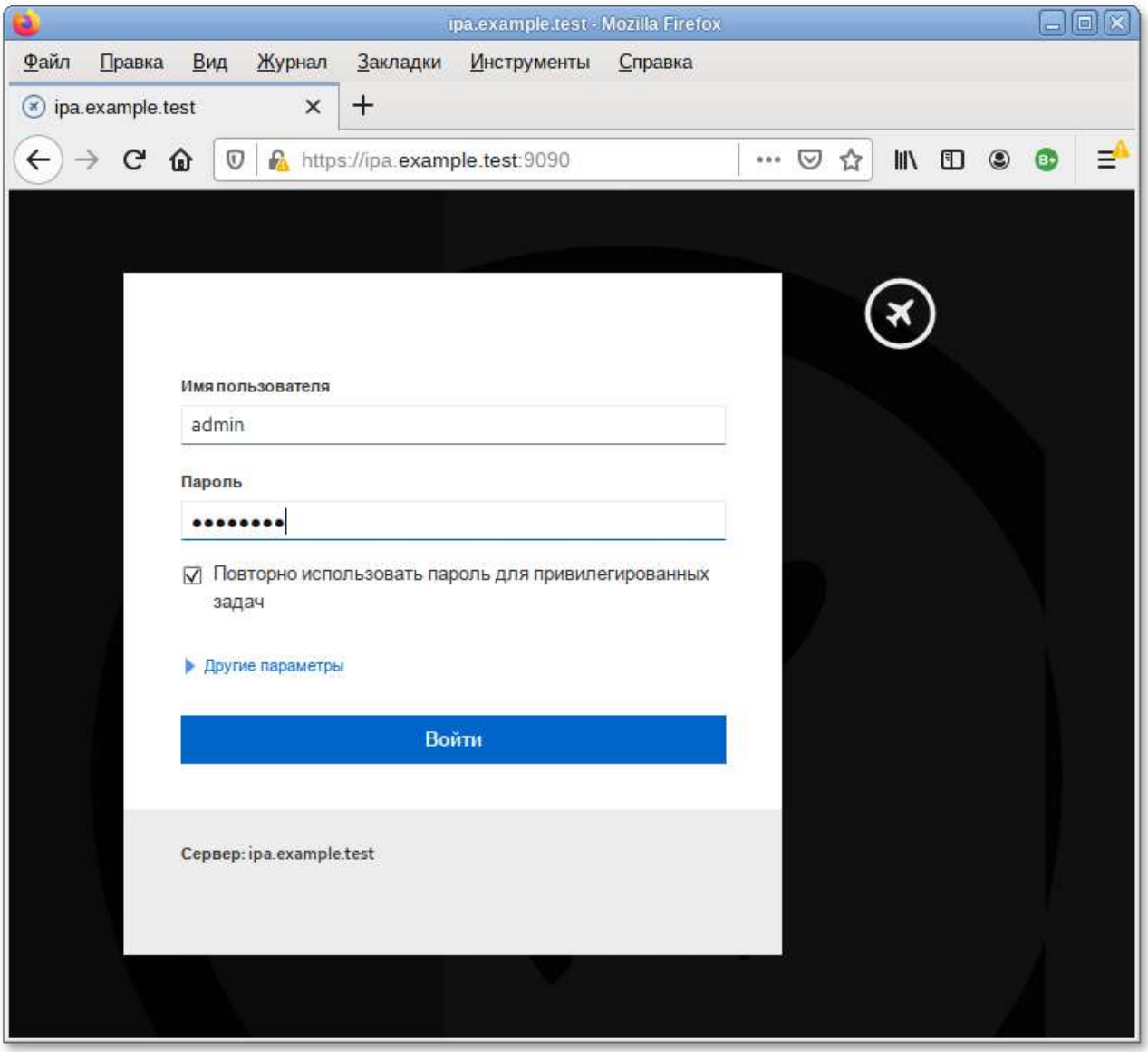
Примечание

Пакет *fleet-commander-admin* не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p9. О добавлении репозиториев с использованием графических приложений вы можете почитать в разделе Добавление репозиториев.

Добавить сервис Cockpit в автозапуск и запустить его:

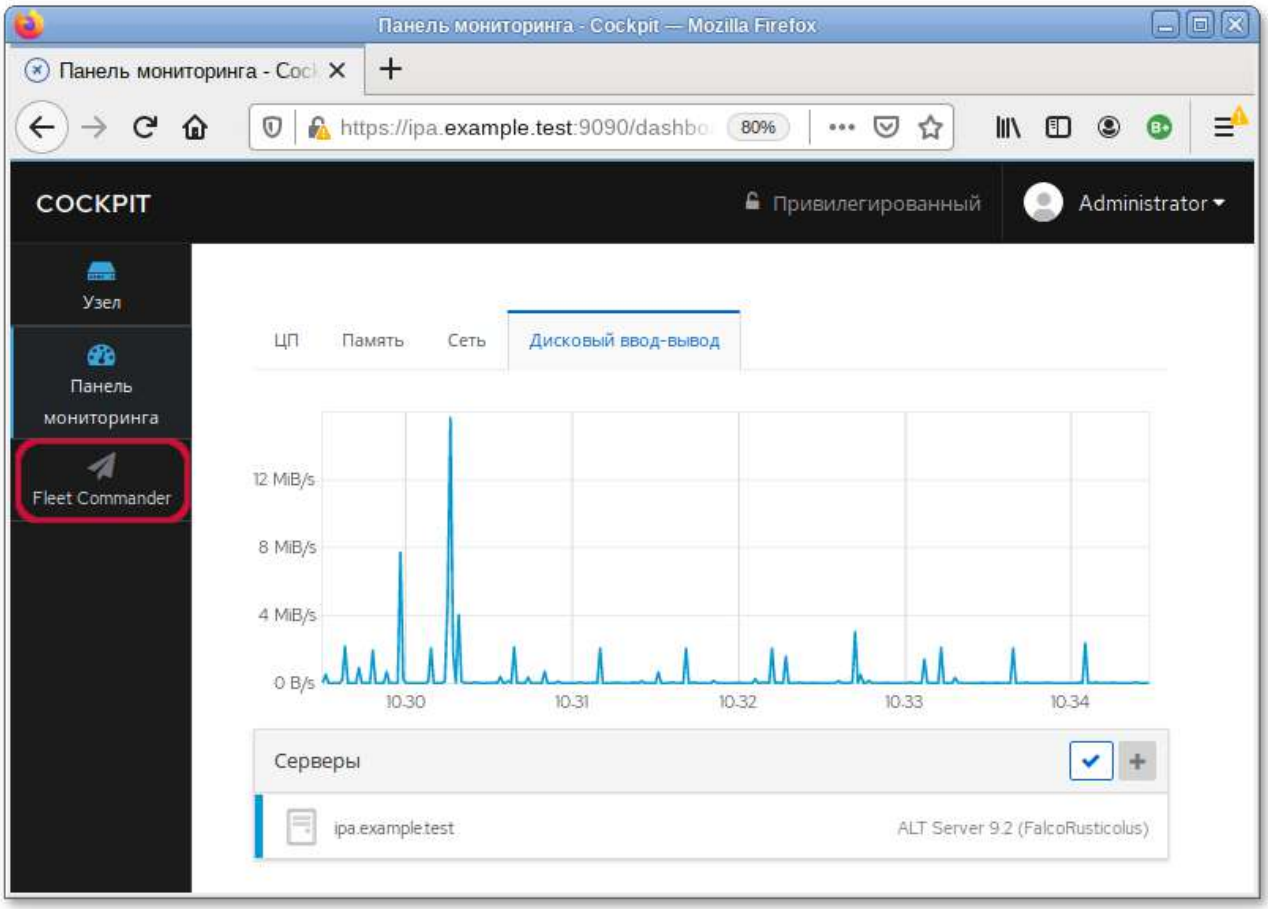
```
# systemctl enable --now cockpit.socket
```

Веб-интерфейс Cockpit будет доступен по адресу **https://адрес-сервера:9090/**:



Вход осуществляется по логину указанному при установке FreeIPA сервера.

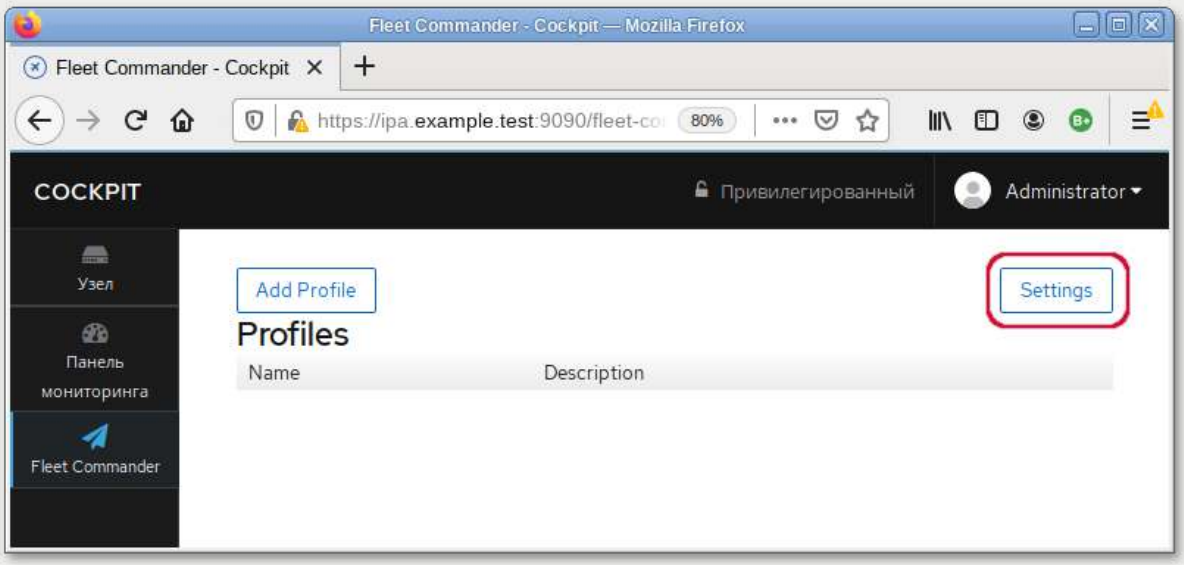
Для доступа к настройке **Fleet Commander** следует выбрать соответствующую кнопку на левой панели веб-интерфейса:



При первом запуске **Fleet Commander** необходимо настроить глобальную политику и информацию о хосте libvirt.

Примечание

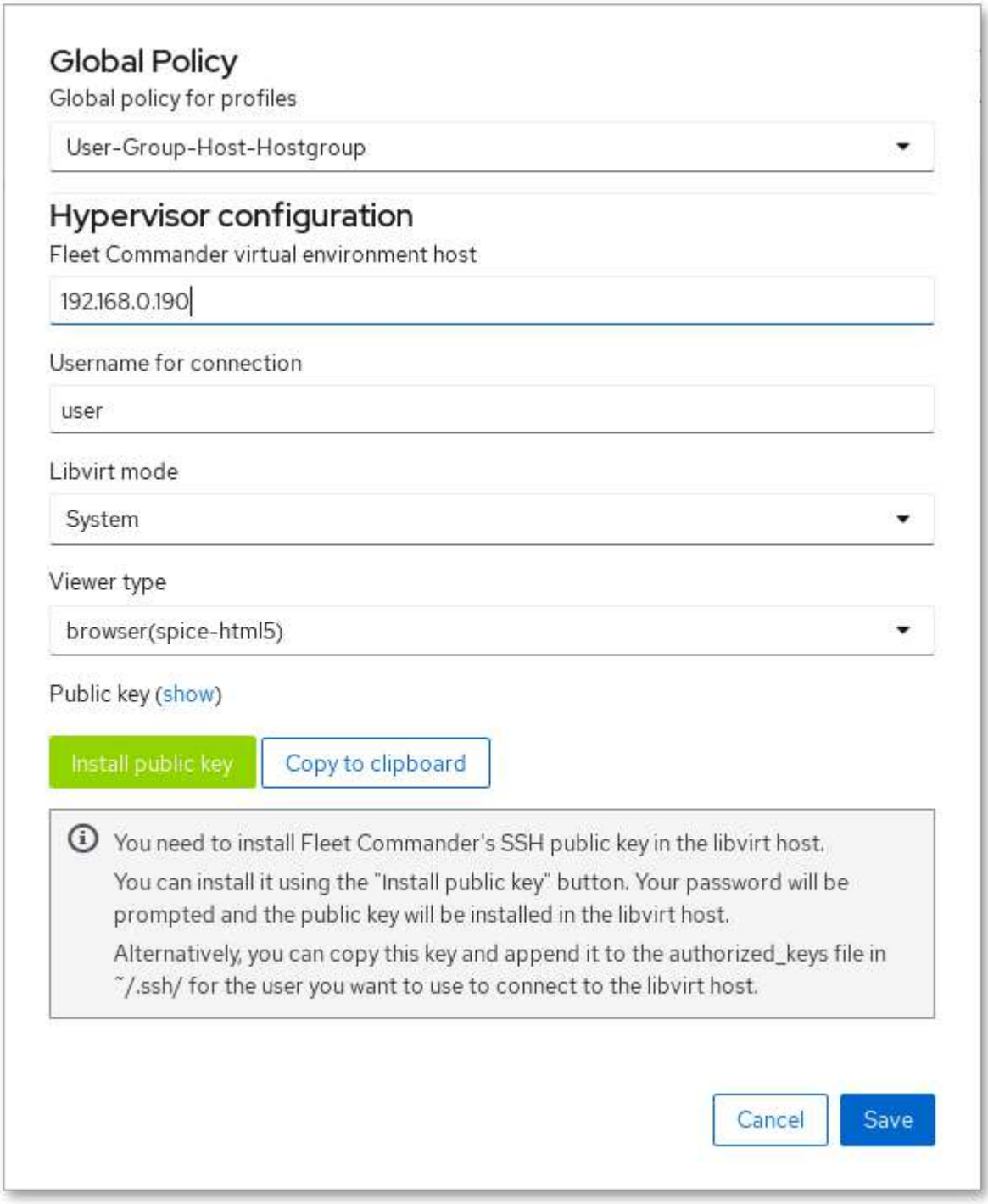
Открыть окно настроек можно, нажав кнопку **`Settings`** на вкладке **`Fleet Commander`**:



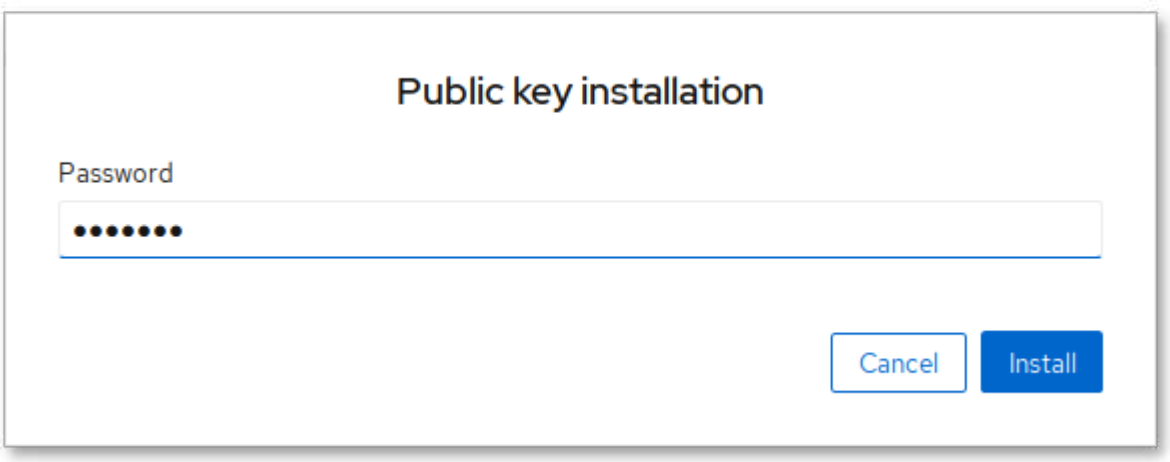
Fleet Commander позволяет установить глобальную политику для определения того, как применять несколько профилей: к конкретному пользователю, к группе, к хосту, к группе хостов. По умолчанию это **`User-Group-Host-Hostgroup`**.

Для запуска live-сессии необходимо работающее ssh-соединение с libvirt-хостом. В форму настройки необходимо ввести следующие данные:

- **`Fleet Commander virtual environment host`** — адрес libvirt-хоста (если в качестве libvirt-хоста используется FreeIPA сервер, то здесь необходимо указать адрес текущей машины или localhost);
- **`Username for connection`** — имя пользователя libvirt-хоста;
- **`Libvirt mode`** — если пользователь не является привилегированным, то следует переключить данную настройку в режим сеанса.



Fleet Commander генерирует свой собственный открытый ключ, который необходимо добавить в **`.ssh/authorized_keys`** для соответствующего пользователя на libvirt-хосте. Это можно сделать, нажав кнопку **`Install public key`** (**`Установить открытый ключ`**), при этом будет необходимо ввести пароль пользователя. Пароль используется только для установки ключа и нигде не хранится.

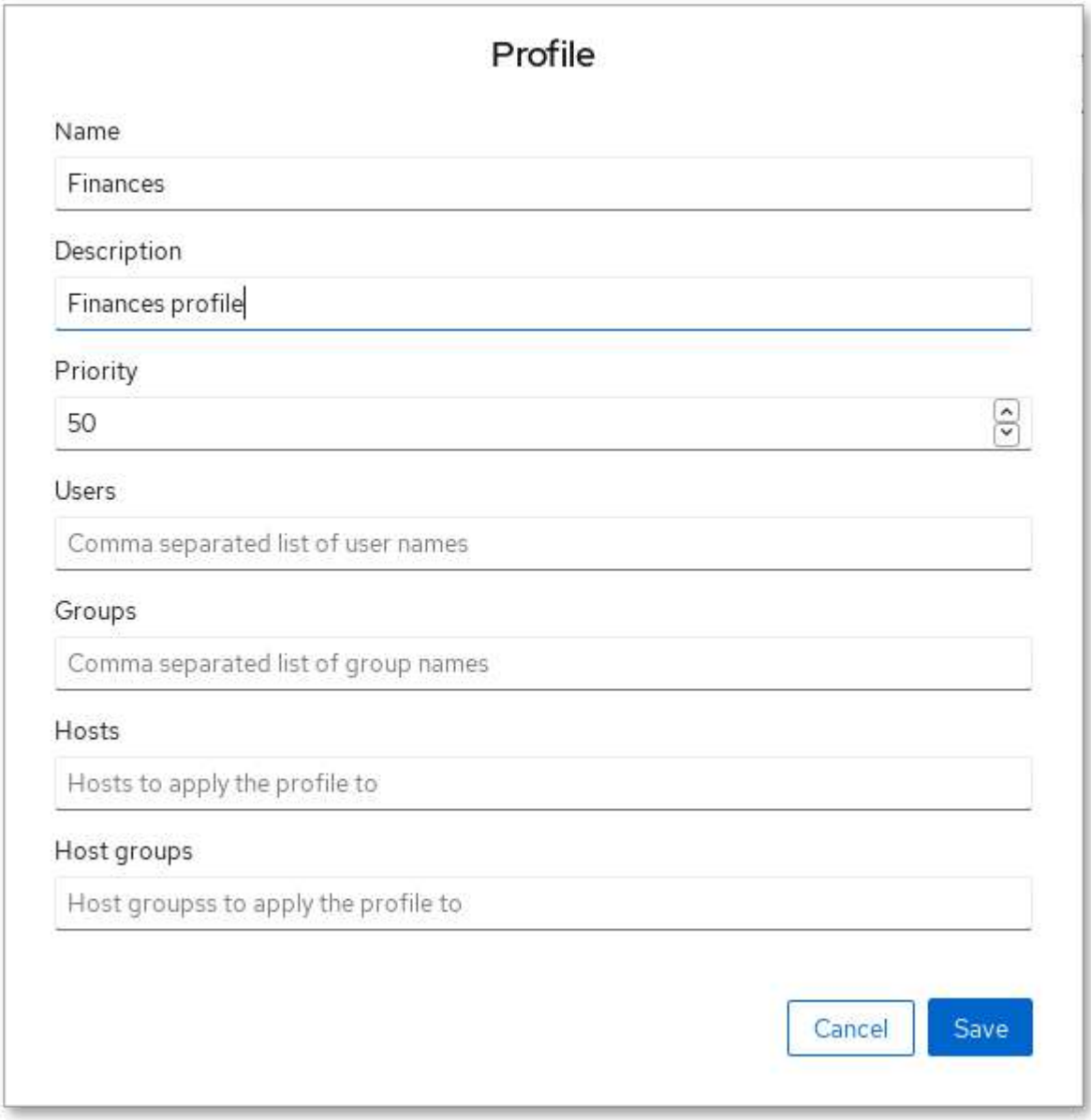


Примечание

На хосте libvirt, должен быть запущен SSH-сервер (служба sshd).

51.1.2.1. Работа с профилями

После настройки Fleet Commander Admin необходимо создать и настроить профиль. Для создания профиля нажать кнопку **`Add Profile`** на вкладке **`Fleet Commander`**. Появится форма настройки профиля:



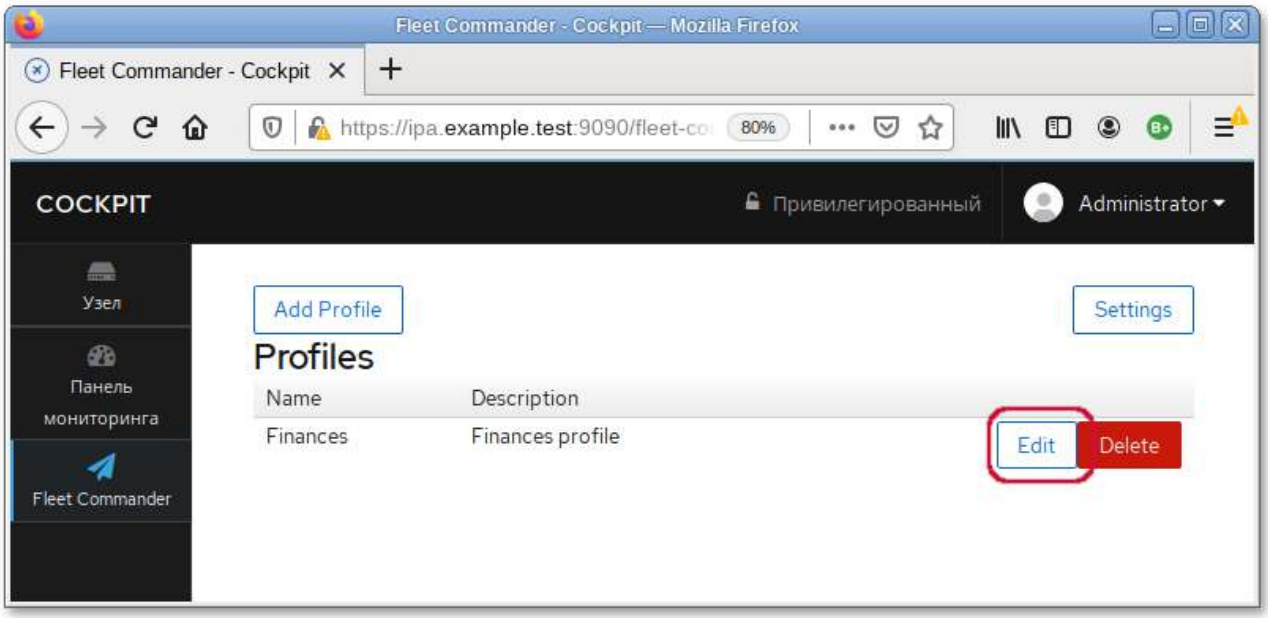
Форма настройки профиля содержит следующие поля:

- **`Name`** — имя профиля;
- **`Description`** — описание профиля;
- **`Priority`** — приоритет профиля;
- **`Users`** — пользователи, к которым будет применен профиль;
- **`Groups`** — группы, к которым будет применен профиль;
- **`Hosts`** — хосты, к которым будет применен профиль;
- **`Host groups`** — группы хостов, к которым будет применен профиль.

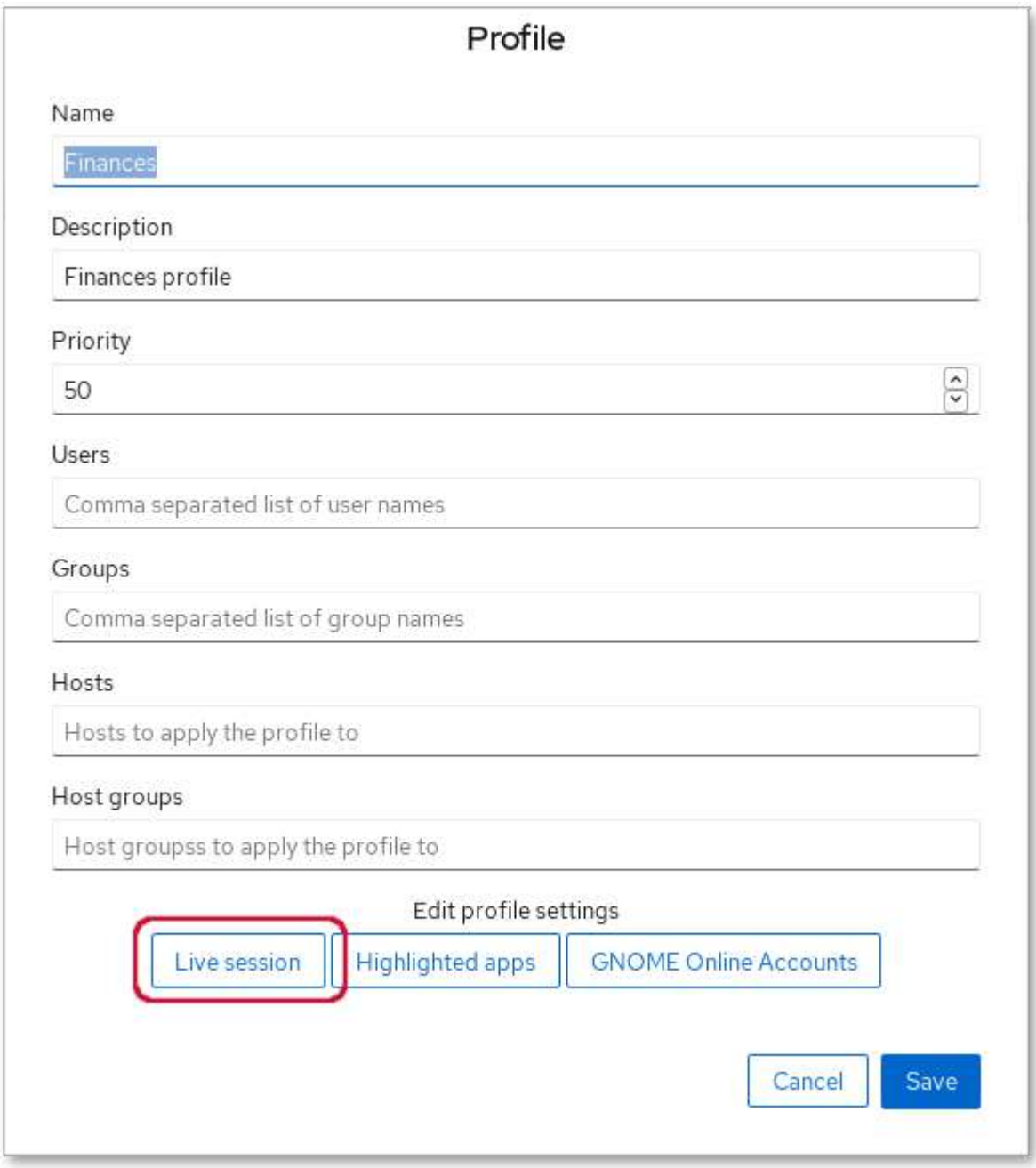
Если не указан ни один хост или группа хостов, то профиль будет применен к каждому хосту состоящему в домене.

51.1.3. Настройка шаблона

Для настройки шаблона в веб-интерфейсе Cockpit необходимо нажать кнопку **`Edit`** напротив нужного профиля:



и в открывшемся окне нажать кнопку **`Live session`**:



В появившейся форме будет выведен список доступных шаблонов. При выборе шаблона, он начнет загружаться.

51.1.4. Установка и настройка Fleet Commander Client

Клиентская машина должна быть введена в домен (см. соответствующий раздел). Также должны быть созданы доменные пользователи.

Установить необходимый пакет (из репозитория):

```
# apt-get install fleet-commander-client
```

Клиент будет запускаться автоматически, при входе в домен с поддержкой Fleet Commander, и будет настраивать конфигурацию, которая применима к данному пользователю.

51.2. Использование Fleet Commander

Fleet Commander работает со следующими приложениями:

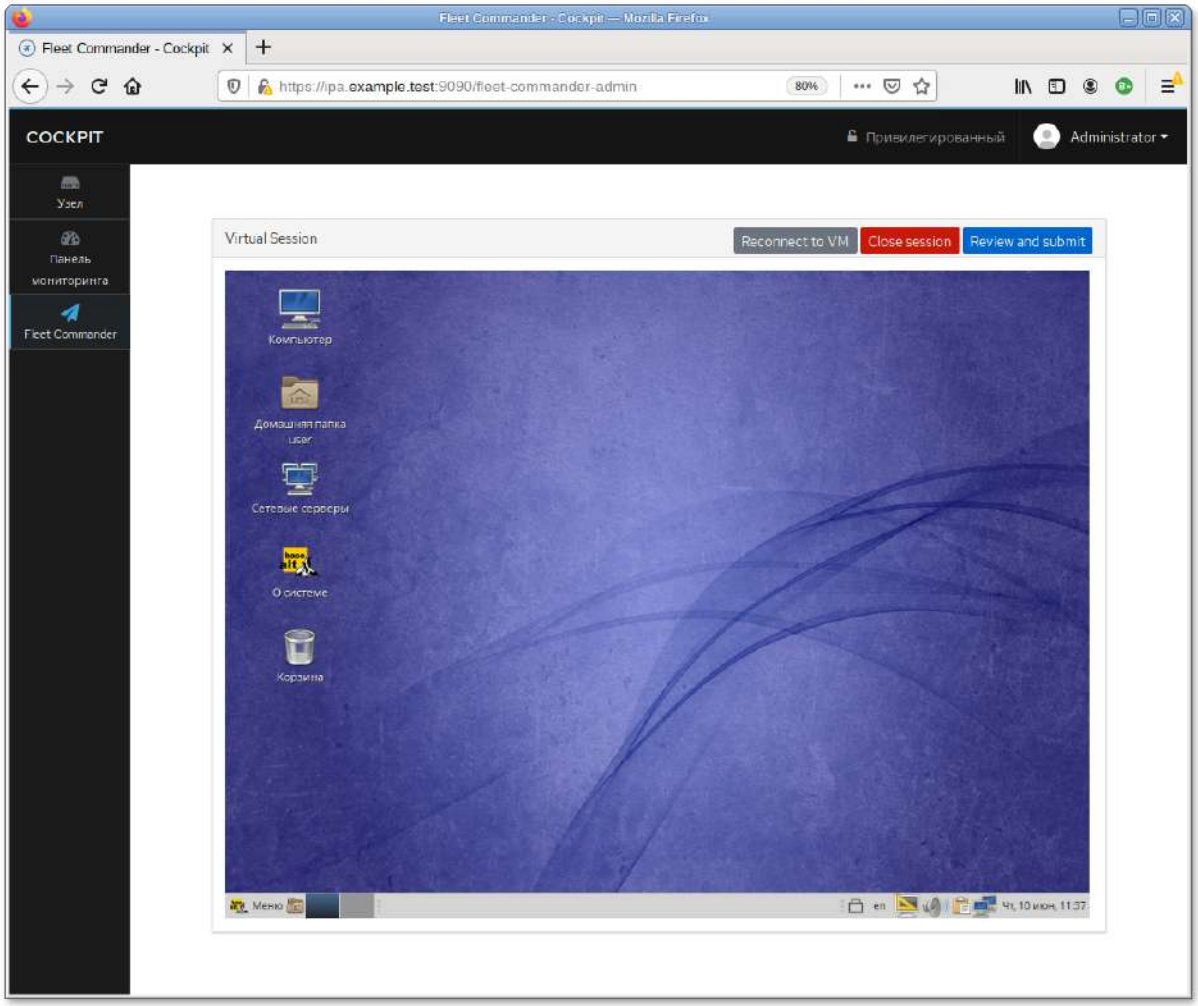
- GSettings
- LibreOffice
- Chromium
- Chrome
- Firefox
- NetworkManager

Администрирование происходит через веб-интерфейс Cockpit.

Порядок работы с Fleet Commander:

1. Открыть **`https://адрес-сервера:9090/fleet-commander-admin`** и запустить live-сессию (**Edit → Live session**). Появится окно со списком доступных ВМ, которые можно использовать в качестве шаблона для загрузки в live-сессии:

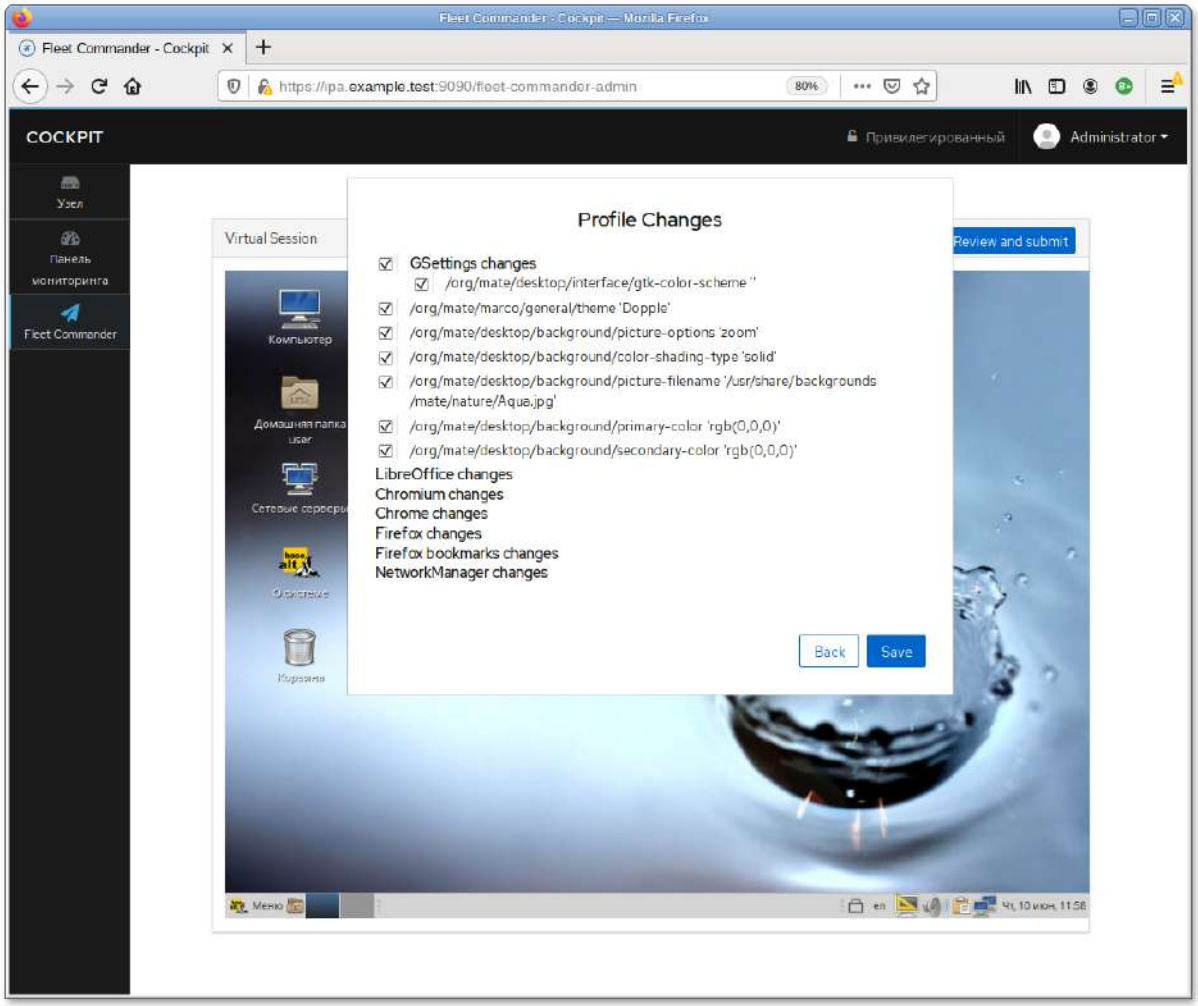
2. Выбрать машину, на которой установлен Fleet Commander Logger, и запустить ее:



Загруженная машина является шаблоном, все сделанные на ней изменения будут отловлены регистратором, сохранены и применены на клиентских системах.

3. На загруженной машине внести необходимые изменения в настройки.

4. В веб-интерфейсе Cockpit нажать кнопку **`Review and submit`**. Появится окно со списком сделанных изменений:



В списке изменений можно выбрать как все изменения, так и частичные, установив отметку напротив нужного. После выбора нажать кнопку **Save**, для сохранения изменений.

5. Загрузить клиентскую машину, войти в систему под доменным пользователем. Убедиться, что сделанные изменения успешно применились.

Предупреждение

При закрытии вкладки браузера с Cockpit, live-сессия прервется и изменения, внесенные за время ее существования, будут потеряны.

51.3. Устранение неполадок Fleet Commander

Для отлавливания любых ошибок возникших во время работы Fleet Commander Admin необходимо добавить **`log_level = debug`** в **`/etc/xdg/fleet-commander-admin.conf`**. Возникшие ошибки можно отследить, используя **`journalctl`**.

Глава 52. Zabbix

Zabbix — система мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования.

Для управления системой мониторинга и чтения данных используется веб-интерфейс.

52.1. Установка сервера PostgreSQL

Перед установкой Zabbix должен быть установлен и запущен сервер PostgreSQL, с созданным пользователем zabbix и созданной базой zabbix.

Установить PostgreSQL, Zabbix-сервер и дополнительную утилиту **fping**:

```
# apt-get install postgresql12-server zabbix-server-pgsql fping
```

Примечание

Пакеты *zabbix-server-pgsql* и *fping* не входят в состав ISO-образа дистрибутива, их можно установить из репозитория p9. О добавлении репозиториев с использованием графических приложений вы можете почитать в разделе Добавление репозиториев.

Подготовить к запуску и настроить службы PostgreSQL, для этого необходимо выполнить следующие действия:

- создать системные базы данных:

  ```
  # /etc/init.d/postgresql initdb
  ```

- включить по умолчанию и запустить службу:

  ```
  # chkconfig postgresql on
  # service postgresql start
  ```

- создать пользователя zabbix и базу данных zabbix (под правами root):

  ```
  # su - postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --
  no-createrole --encrypted --pwprompt zabbix'
  # su - postgres -s /bin/sh -c 'createdb -O zabbix zabbix'
  # service postgresql restart
  ```

- добавить в базу данные для веб-интерфейса (последовательность команд важна, в разных версиях Zabbix путь будет отличаться, версия помечена звёздочкой):

```
# su - postgres -s /bin/sh -c 'psql -U zabbix -f /usr/share/doc/zabbix-common-database-pgsql-*/schema.sql zabbix'
# если вы создаете базу данных для Zabbix прокси, следующие команды выполнять не нужно
# su - postgres -s /bin/sh -c 'psql -U zabbix -f /usr/share/doc/zabbix-common-database-pgsql-*/images.sql zabbix'
# su - postgres -s /bin/sh -c 'psql -U zabbix -f /usr/share/doc/zabbix-common-database-pgsql-*/data.sql zabbix'
```

52.2. Установка Apache2

Установить необходимые пакеты:

```
# apt-get install apache2 apache2-mod_php7
```

Добавить в автозапуск и запустить apache2:

```
# chkconfig httpd2 on
# service httpd2 start
```

52.3. Установка PHP

Установить необходимые пакеты:

```
# apt-get install php7-mbstring php7-sockets php7-gd2 php7-xmlreader php7-pgsql php7-ldap
```

Изменить некоторые опции php в файле **/etc/php/7.3/apache2-mod_php/php.ini** (версия PHP может быть другой):

```
memory_limit = 256M
post_max_size = 32M
max_execution_time = 600
max_input_time = 600
date.timezone = Europe/Moscow
always_populate_raw_post_data = -1
```

Перезапустить apache2:

```
# service httpd2 restart
```

52.4. Настройка и запуск Zabbix-сервера

Внести изменения в конфигурационный файл **/etc/zabbix/zabbix_server.conf**:

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=Пароль от базы
```

Добавить Zabbix-сервер в автозапуск и запустить его:

```
# chkconfig zabbix_pgsql on
# service zabbix_pgsql start
```

52.5. Установка веб-интерфейса Zabbix

Установить метапакет (из репозитория):

```
# apt-get install zabbix-phpfrontend-apache2-mod_php7
```

Включить аддоны в apache2:

```
# ln -s /etc/httpd2/conf/addon.d/A.zabbix.conf /etc/httpd2/conf/extra-
enabled/
```

Перезапустить apache2:

```
# service httpd2 restart
```

Изменить права доступа к конфигурационному каталогу веб-интерфейса, чтобы веб-установщик мог записать конфигурационный файл:

```
# chown apache2:apache2 /var/www/webapps/zabbix/ui/conf
```

Примечание

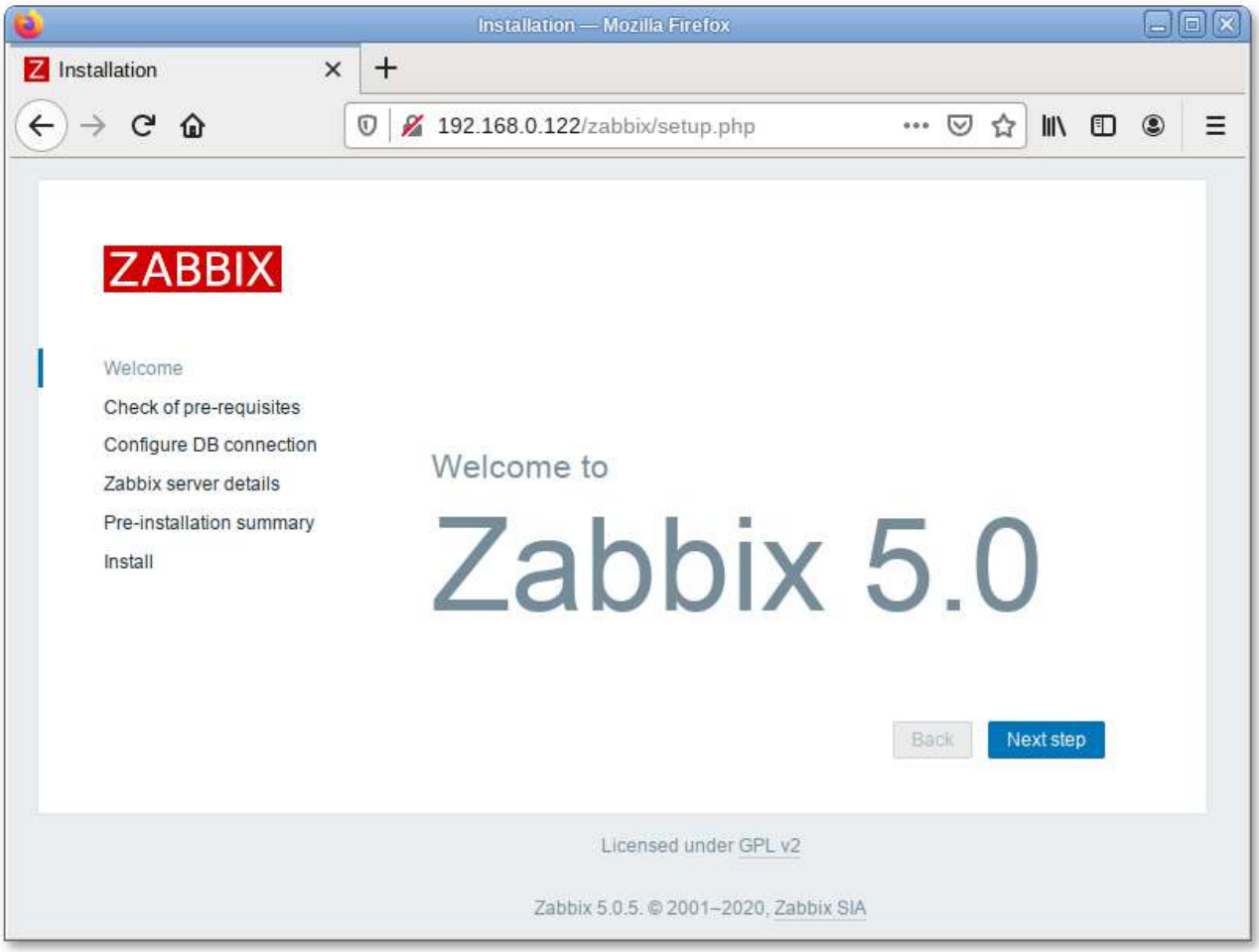
Если устанавливается Zabbix4, команда будет такой:

```
# chown apache2:apache2 /var/www/webapps/zabbix/frontends/php/conf
```

В браузере перейти на страницу установки Zabbix сервера:

```
http://<ip-сервера>/zabbix
```

При первом заходе на страницу запустится мастер, который шаг за шагом проверит возможности веб-сервера, интерпретатора PHP и сконфигурирует подключение к базе данных.



Примечание

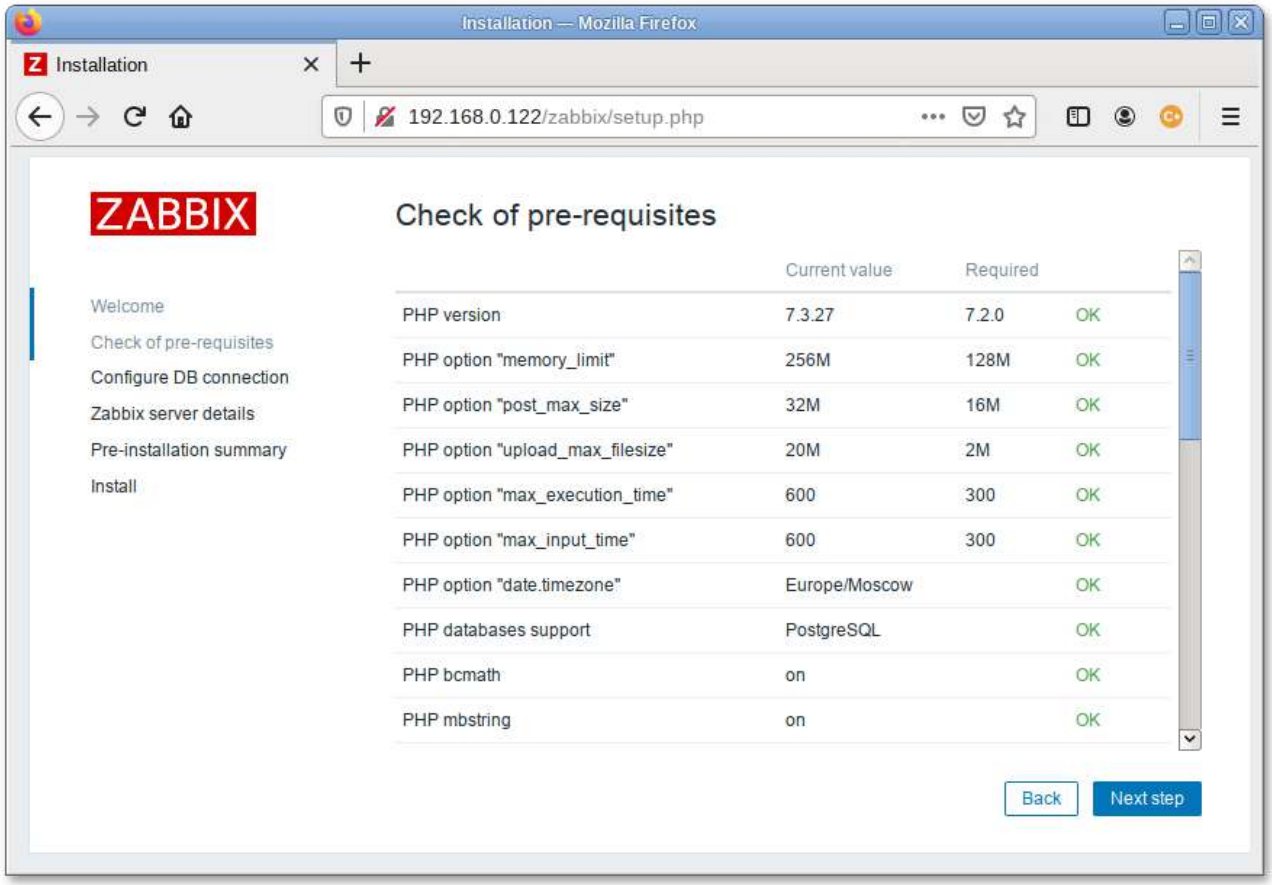
Если при входе на страницу http://<ip-сервера>/zabbix появляется ошибка: доступ запрещен, следует в файле **`/etc/httpd2/conf/sites-available/default.conf`** в секцию <Directory> добавить запись:

```
Require all granted
```

и перезапустить apache2:

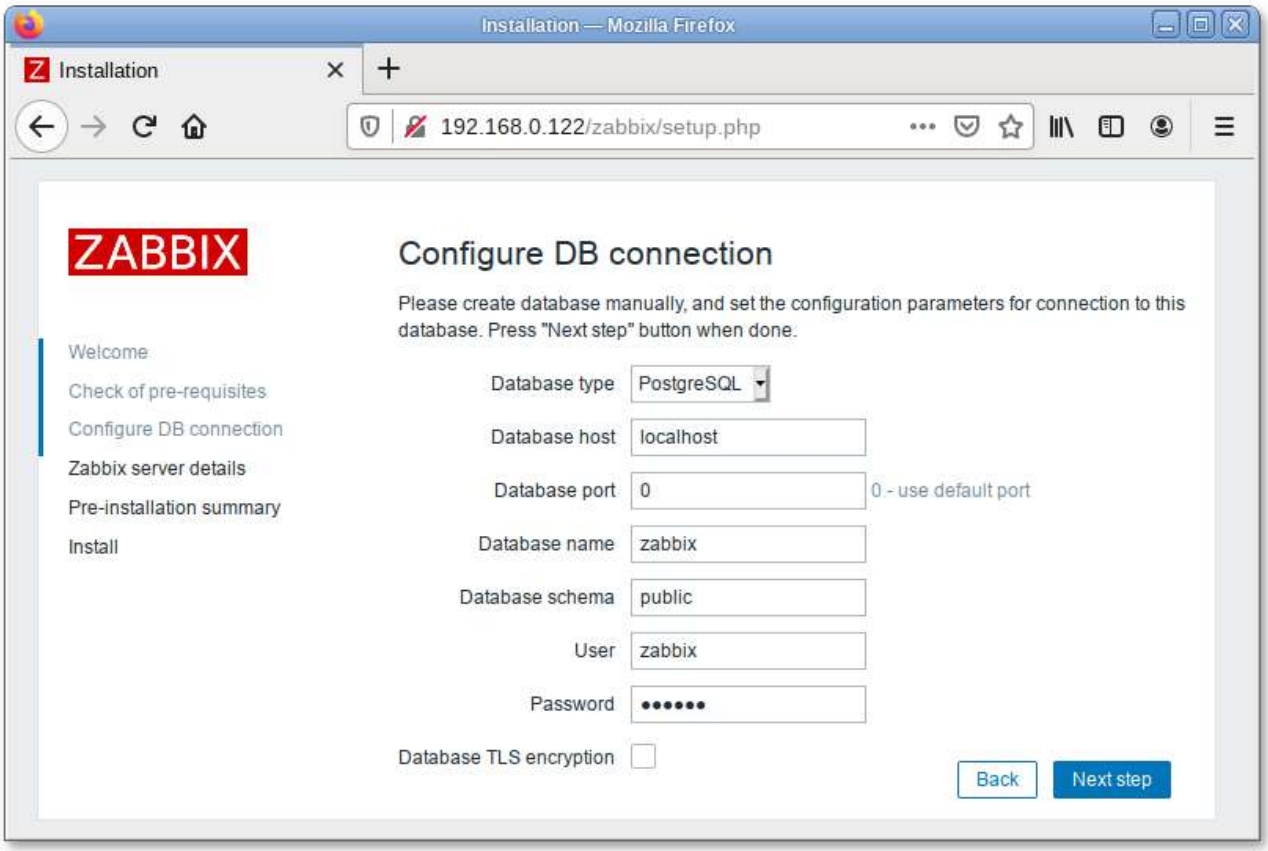
```
# service httpd2 restart
```

Для начала установки необходимо нажать кнопку **`Next Step`**, что осуществит переход на страницу проверки предварительных условий.



Необходимо доустановить то, что требуется и перейти на следующую страницу.

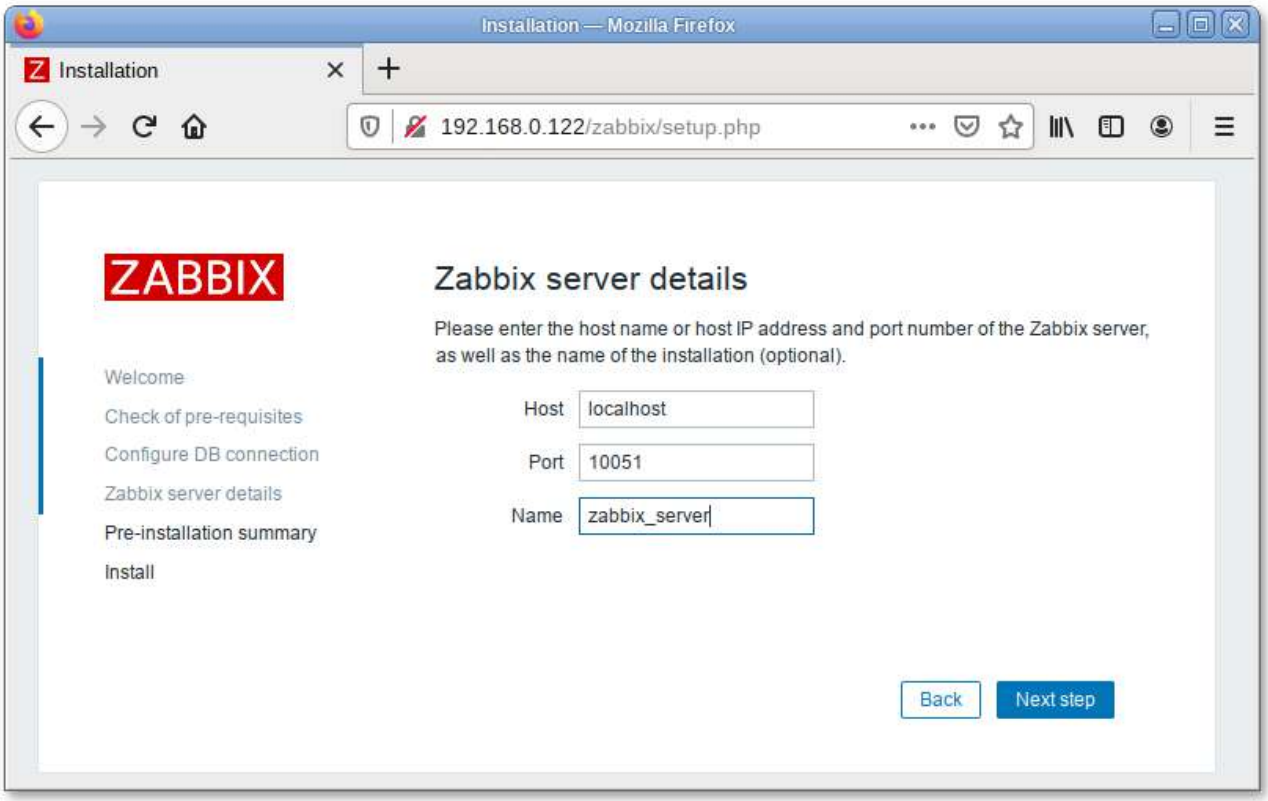
Здесь необходимо ввести параметры подключения к базе данных (параметры подключения нужно указывать такие же, как у сервера Zabbix). По умолчанию в качестве Database schema необходимо указать *public*.

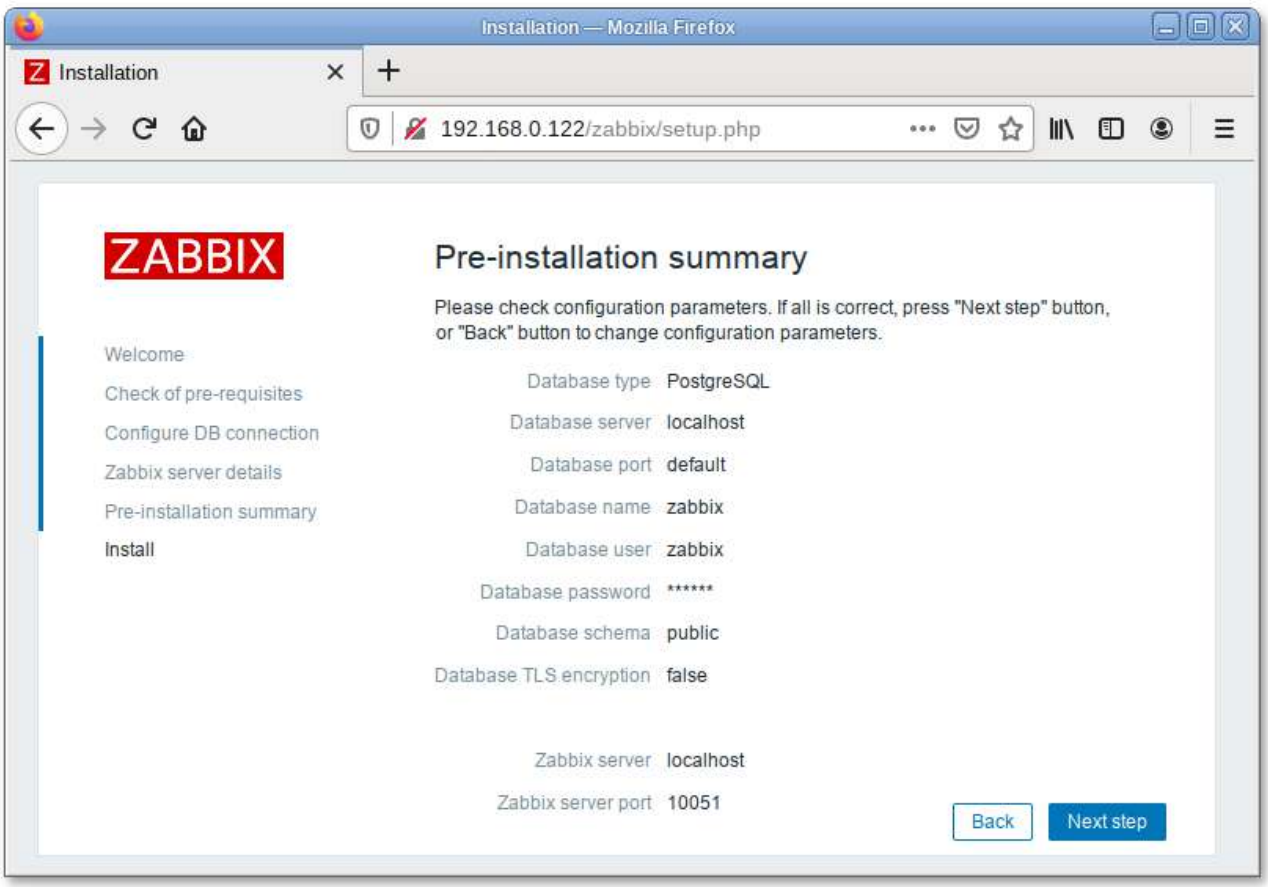


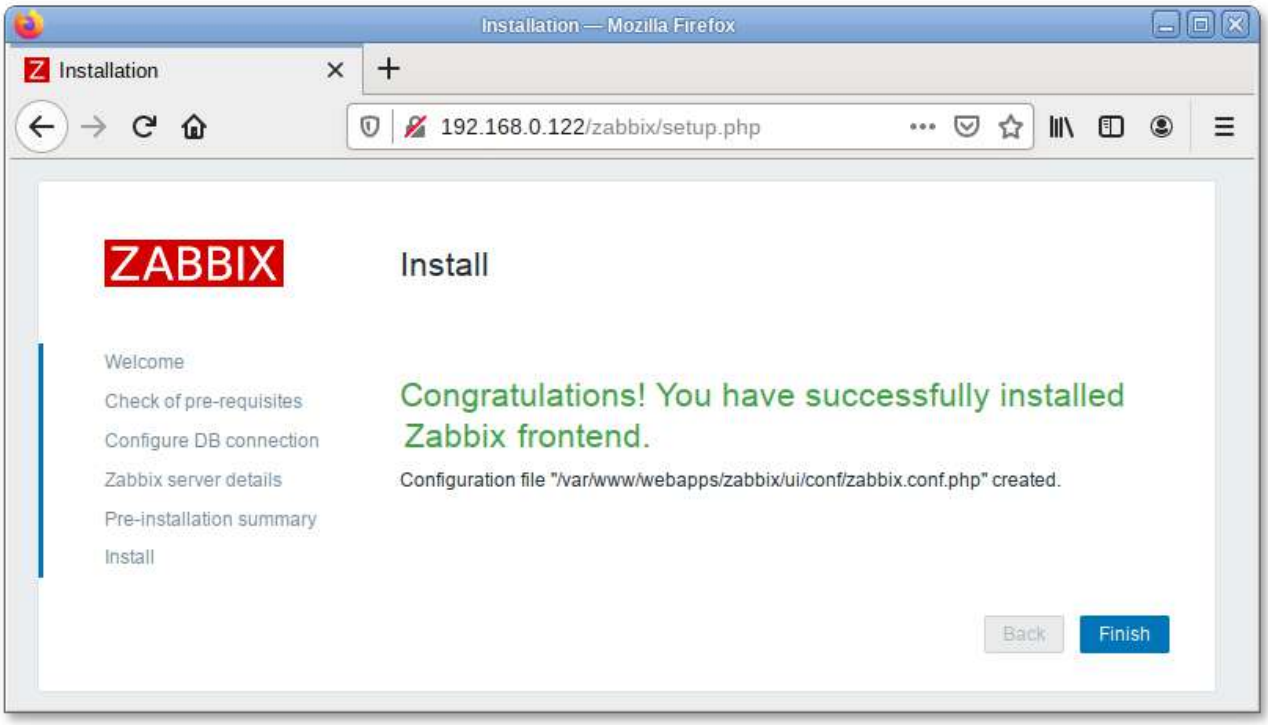
Примечание

Если выбрана опция Шифрование TLS базы данных, то в форме появятся дополнительные поля для настройки TLS-соединения с базой данных

Далее необходимо задать имя сервера и завершить установку.

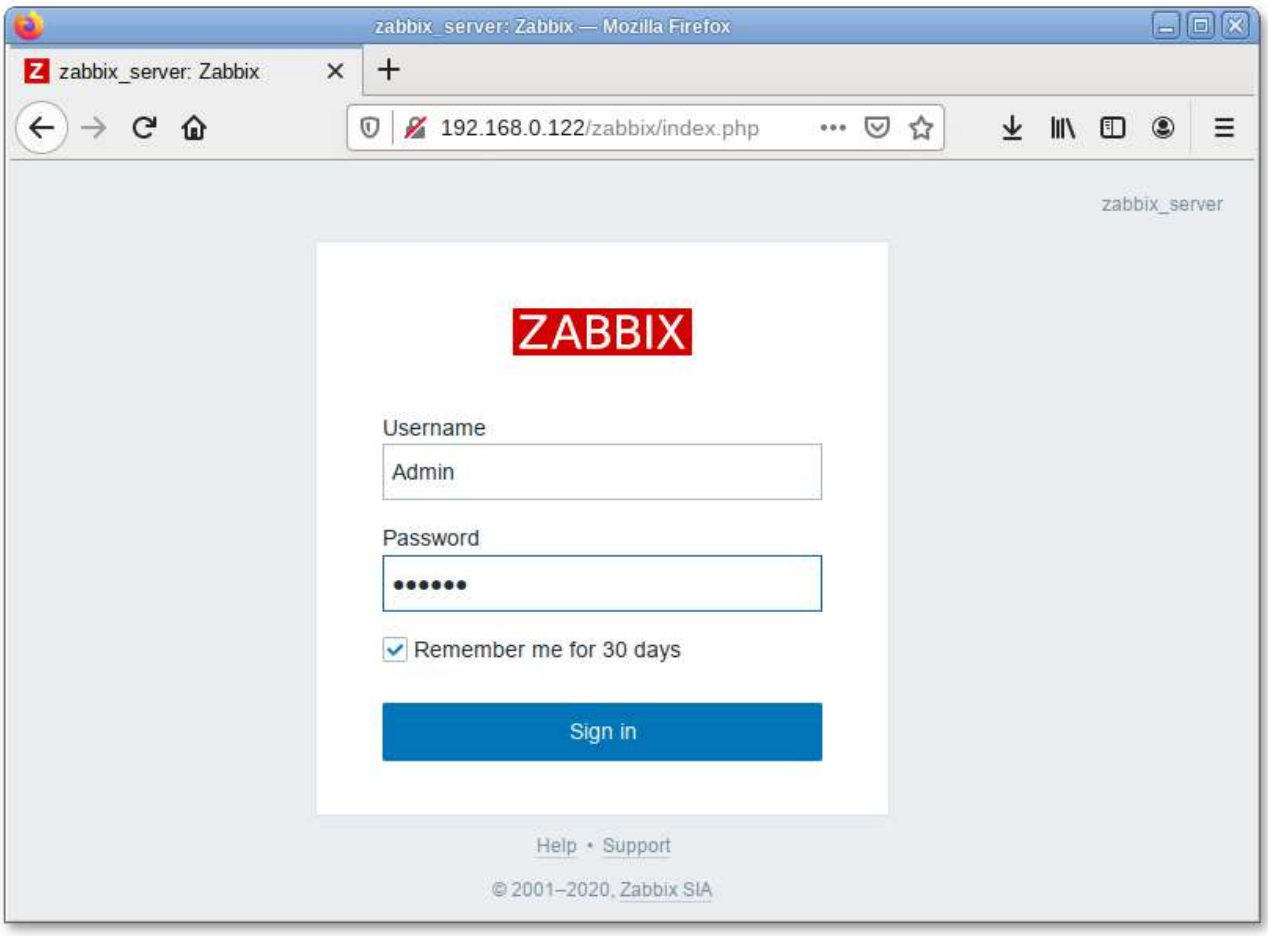

Installation — Mozilla Firefox
Installation
192.168.0.122/zabbix/setup.php
ZABBIX
Zabbix server details
Please enter the host name or host IP address and port number of the Zabbix server, as well as the name of the installation (optional).
Welcome
Check of pre-requisites
Configure DB connection
Zabbix server details
Pre-installation summary
Install
Host
localhost
Port
10051
Name
zabbix_server
Back
Next step


Installation — Mozilla Firefox
Installation
192.168.0.122/zabbix/setup.php
ZABBIX
Pre-installation summary
Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters.
Welcome
Check of pre-requisites
Configure DB connection
Zabbix server details
Pre-installation summary
Install
Database type PostgreSQL
Database server localhost
Database port default
Database name zabbix
Database user zabbix
Database password ******
Database schema public
Database TLS encryption false
Zabbix server localhost
Zabbix server port 10051
Back
Next step

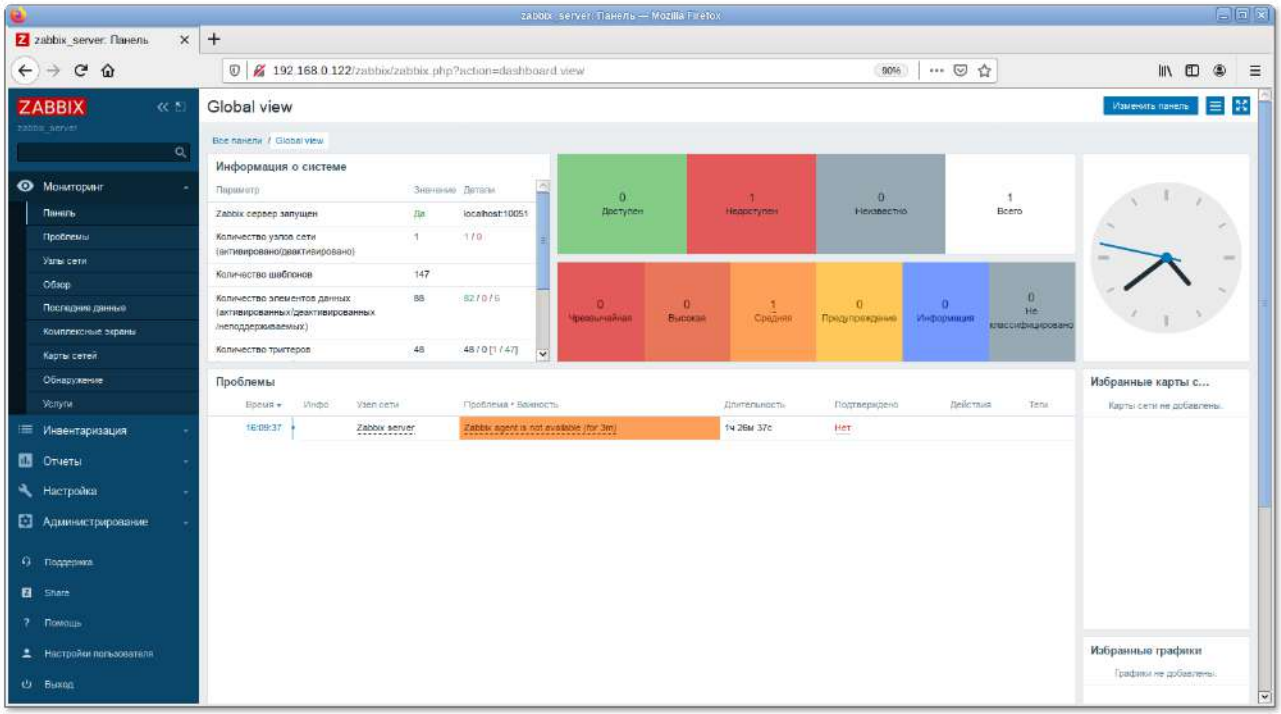


После окончания установки на экране будет отображаться форма входа в интерфейс управления системой мониторинга. Параметры доступа по умолчанию:

```
Логин: Admin
Пароль: zabbix
```

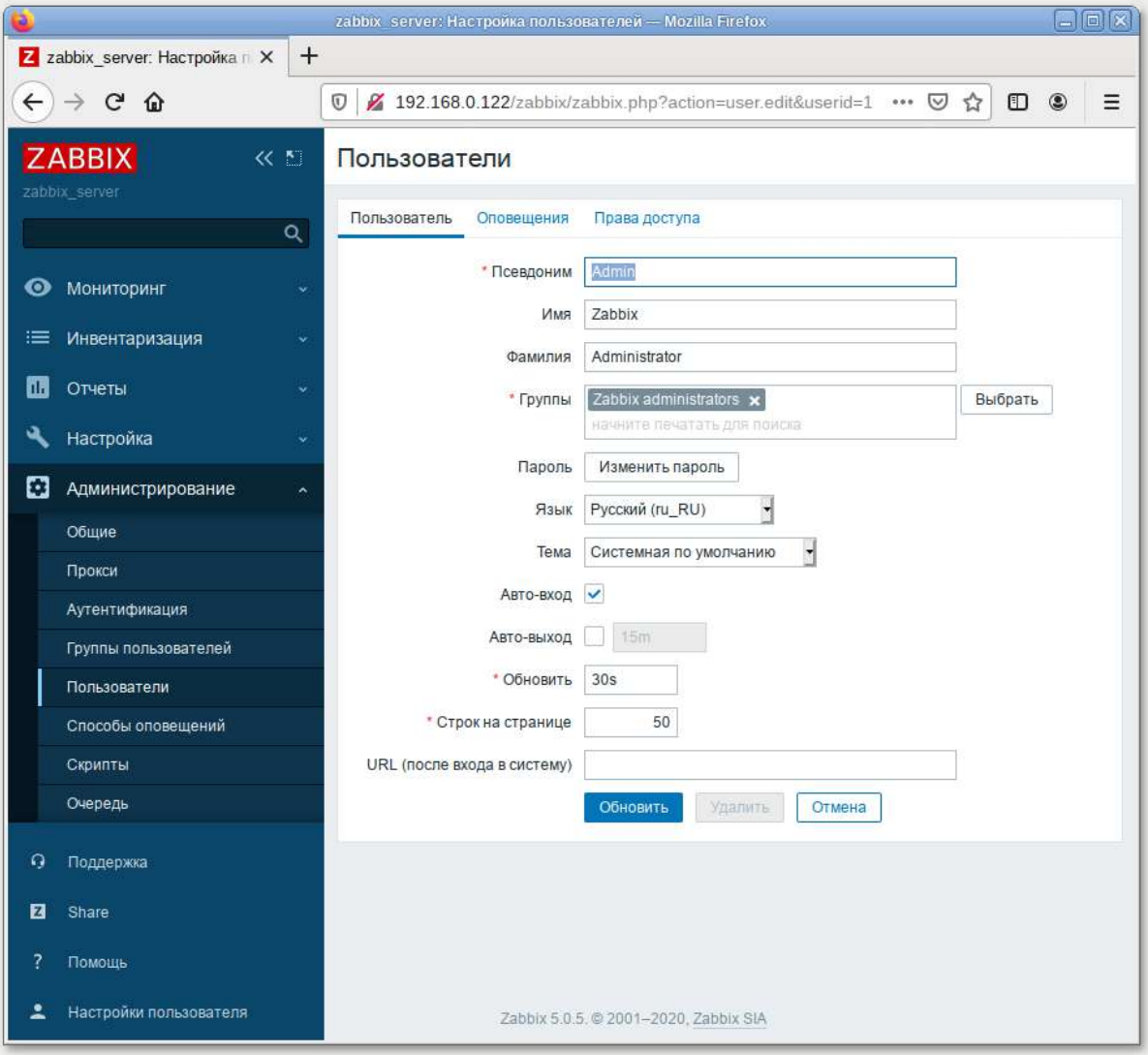


Войдя в систему, нужно сменить пароль пользователя, завести других пользователей и можно начать настраивать Zabbix.



Примечание

В профиле пользователя можно настроить некоторые функции веб-интерфейса Zabbix, такие как язык интерфейса, цветовая тема, количество отображаемых строк в списках и т.п. Сделанные в профиле изменения будут применены только к пользователю, в профиле которого были сделаны эти изменения.



Чтобы собирать информацию с узлов, сервер Zabbix использует информацию, получаемую от агентов. Чтобы добавить новый узел, следует установить на узел, который необходимо мониторить Zabbix-агент и добавить новый хост на Zabbix-сервере.

52.6. Установка клиента Zabbix

Установить необходимый пакет *zabbix-agent* (из репозитория):

```
# apt-get install zabbix-agent
```

Если Zabbix-агент устанавливается не на сам сервер мониторинга, то в файле конфигурации агента **`/etc/zabbix/zabbix_agentd.conf`** нужно задать следующие параметры:

```
Server=<ip-сервера>
ServerActive=<ip-сервера>
Hostname=freeipa.example.test
```

freeipa.example.test — имя узла мониторинга, которое будет указано на сервере Zabbix.

Примечание

Если параметр **`Hostname`** будет пустой или закомментирован, то узел добавится под системным именем.

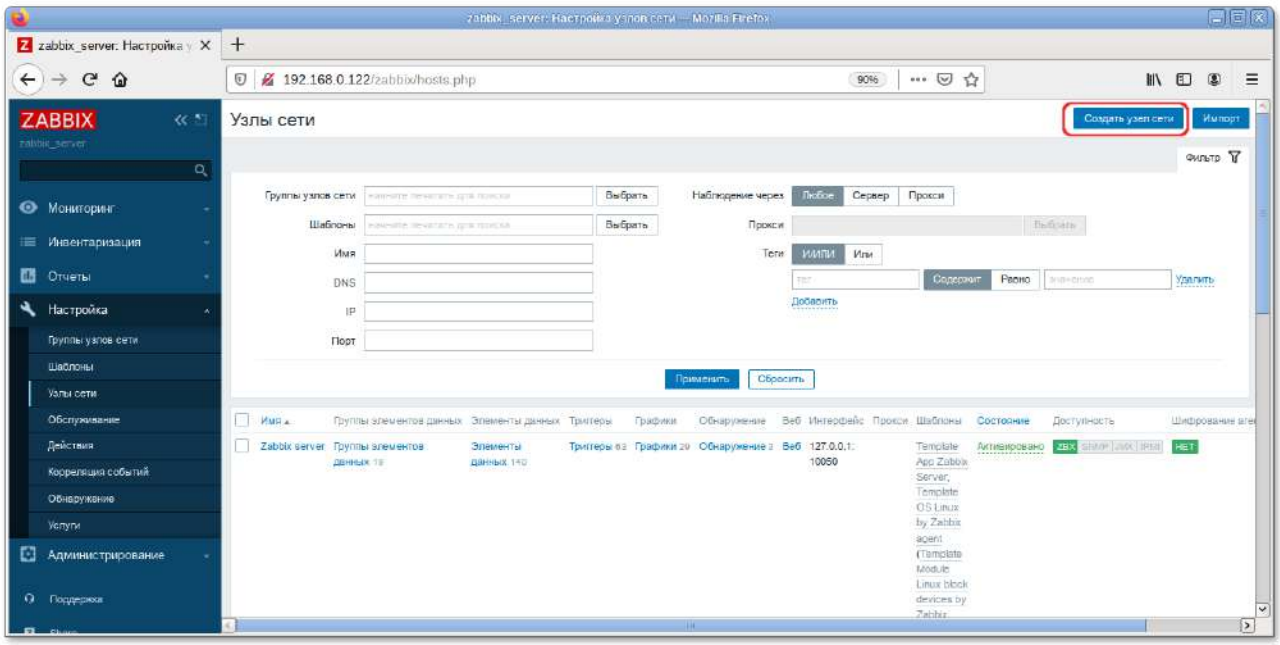
Добавить Zabbix-агент в автозапуск и запустить его:

```
# systemctl enable --now zabbix_agentd.service
```

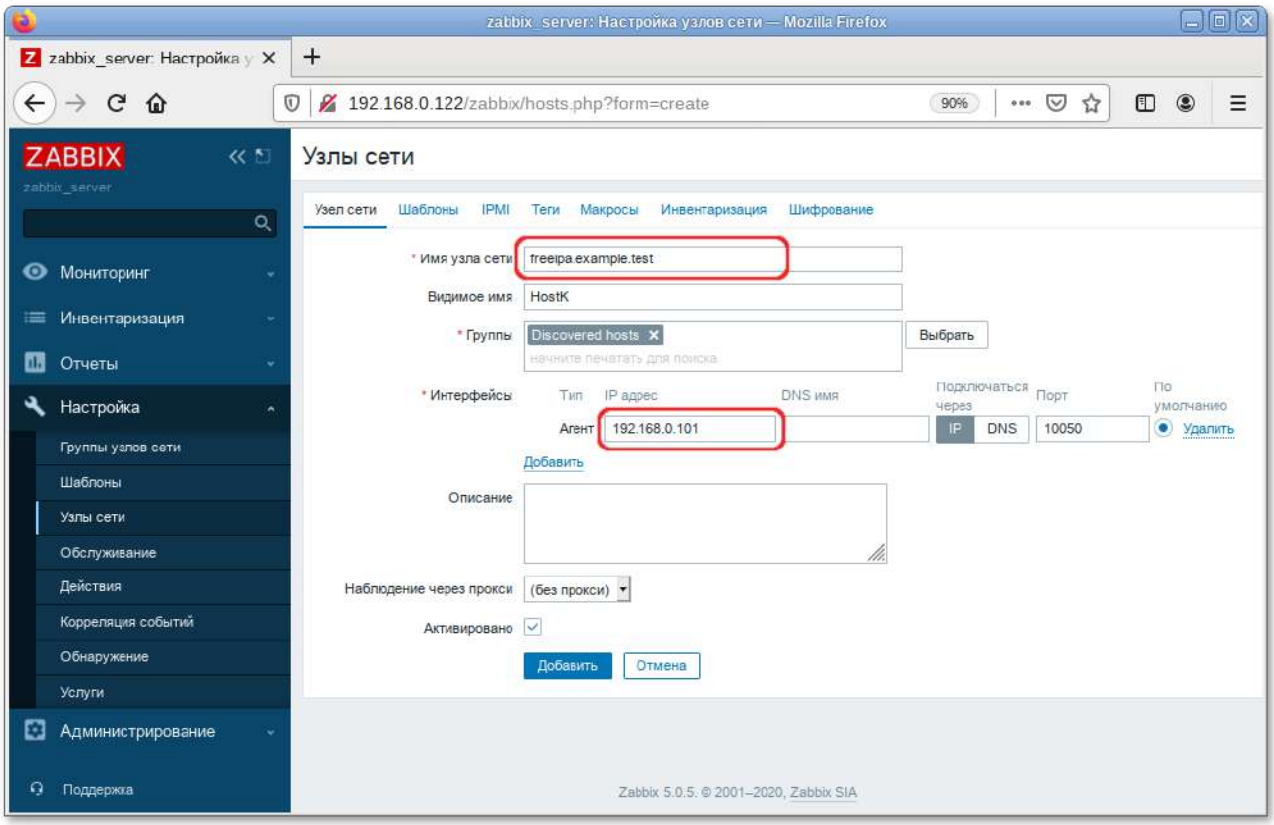
52.7. Добавление нового хоста на сервер Zabbix

Каждый хост необходимо зарегистрировать на сервере Zabbix, сделать это можно, используя веб-интерфейс.

Информация о настроенных узлах сети в Zabbix доступна в **Настройка** → **Узлы сети**. Для добавления нового узла сети следует нажать кнопку **`Создать узел сети`**:



В открывшемся окне необходимо заполнить поля **`Имя узла сети`** и **`IP адрес`** согласно данным добавляемого хоста. Затем следует добавить хост в определенную группу, выбрав одну из них из списка, либо создав новую группу:



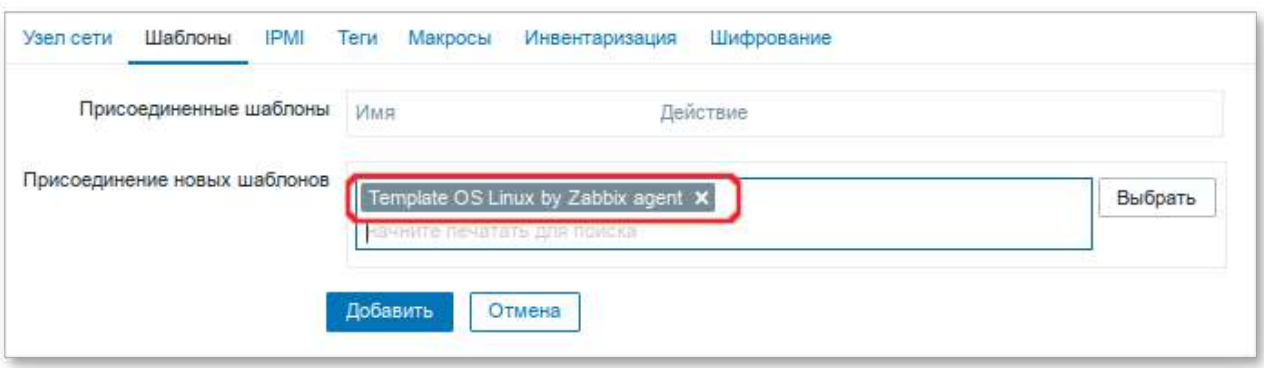
Примечание

В поле **Имя узла сети** ставится значение, которое указано в настройках агента (**/etc/zabbix/zabbix_agentd.conf**) в поле **Hostname**.

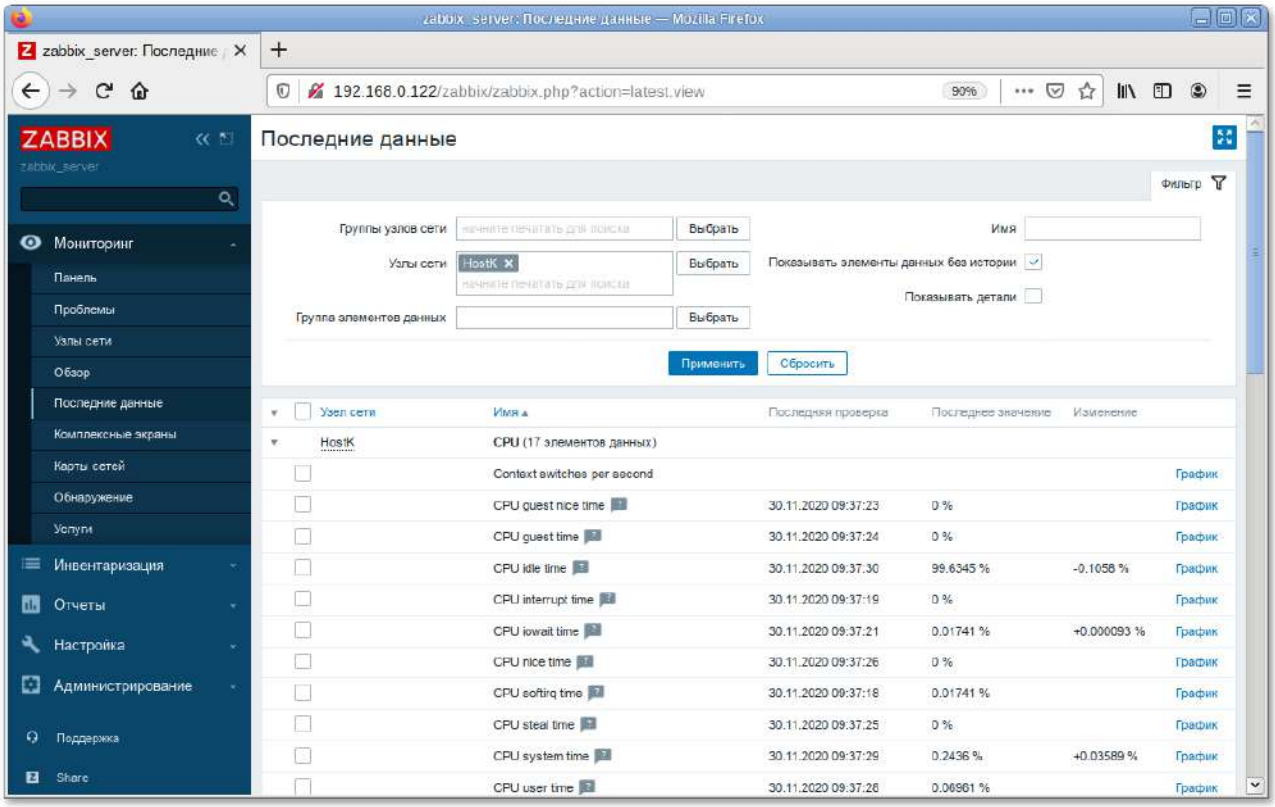
Примечание

Все права доступа назначаются на группы узлов сети, не индивидуально узлам сети. Поэтому узел сети должен принадлежать хотя бы одной группе.

Перейти на вкладку **Шаблоны**, выбрать шаблон **Template OS Linux by Zabbix agent** и нажать кнопку **Добавить**:



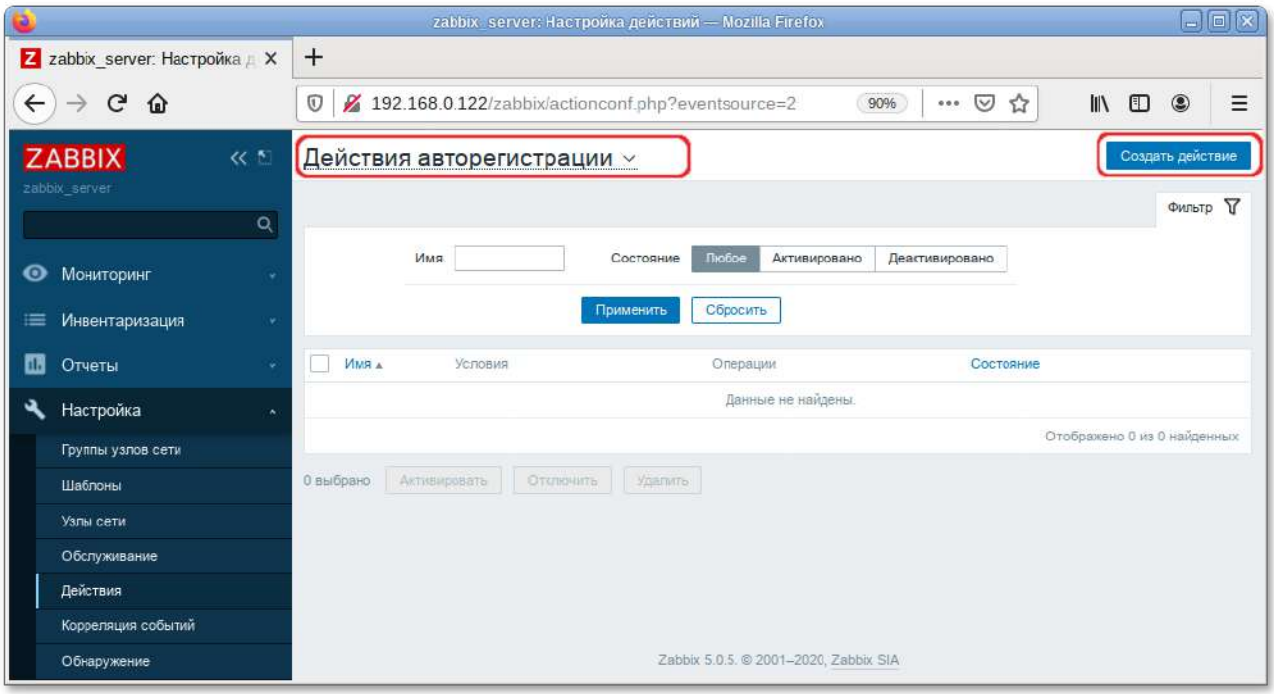
Получение первых данных может занять до 60 секунд. Для того чтобы просмотреть собранные данные необходимо перейти в **Мониторинг** → **Последние данные**, выбрать в фильтре нужный узел сети и нажать кнопку **Применить**:



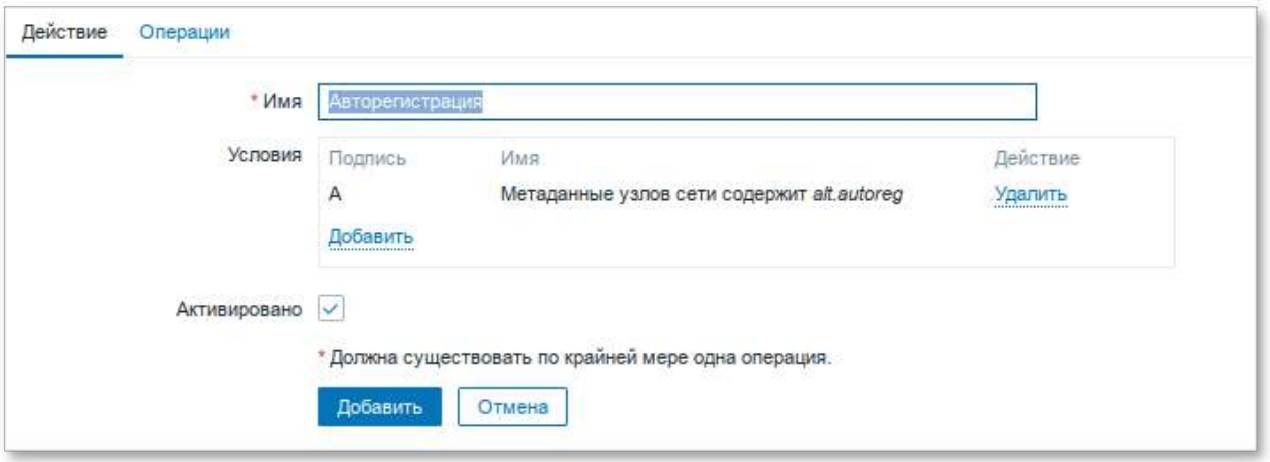
52.8. Авторегистрация узлов

В Zabbix существует механизм, который позволяет Zabbix-серверу начинать мониторинг нового оборудования автоматически, если на этом оборудовании имеется установленный Zabbix-агент. Такой подход позволяет добавлять новые узлы сети на мониторинг без какой-либо настройки Zabbix-сервера вручную по каждому отдельному узлу сети.

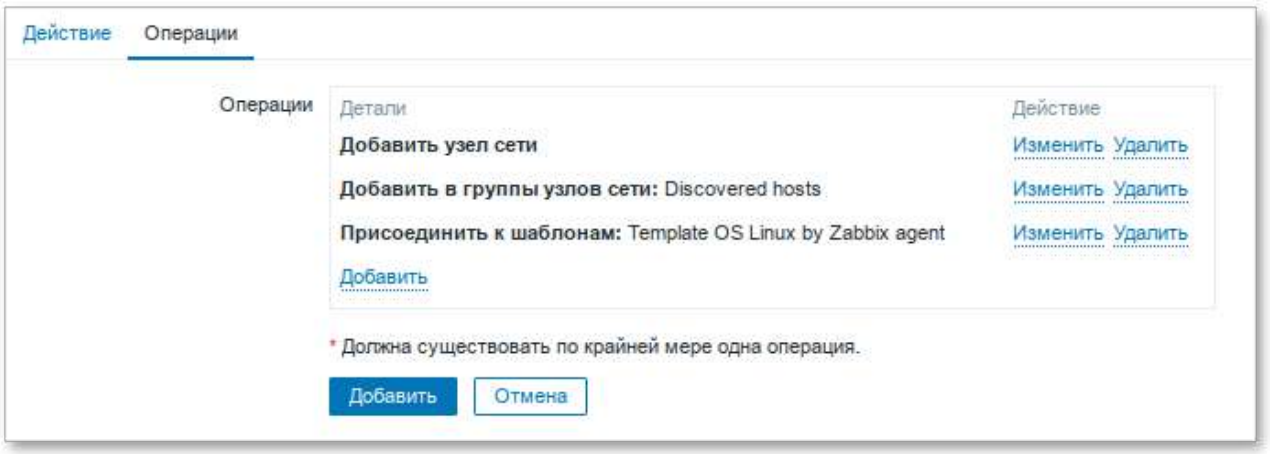
Для настройки авторегистрации, перейти в **Настройка** → **Действия**. В выпадающем списке действий выбрать значение **Действия авторегистрации** и нажать кнопку **Создать действие**:



На открывшейся странице, на вкладке **Действия** заполнить поле **Имя** и добавить условия. В поле **Условия** следует задать правила, по которым будут идентифицироваться регистрируемые хосты:



На вкладке **Операции** в поле **Операции** следует добавить правила, которые необходимо применить при регистрации хоста. Например, для добавления узла, добавления его к группе **`Discovered hosts`** с присоединением к шаблону **`Template OS Linux by Zabbix agent`** правила выглядят так:



В конфигурационном файле агента указать следующие значения:

- в параметре **`Hostname`** — уникальное имя;
- в параметре **`ServerActive`** — IP-адрес сервера;
- в параметре **`HostMetadata`** — значение, которое было указано в настройках сервера (HostMetadata=alt.autoreg).

Перезапустить агент.

Глава 53. Сервер видеоконференций на базе Jitsi Meet

Jitsi Meet — веб-приложение с открытым исходным кодом на базе WebRTC, предназначенное для проведения видеоконференций. Сервер Jitsi Meet создает виртуальные залы для видеоконференций на несколько человек, для доступа к которым требуется только браузер. Преимущество конференции Jitsi заключается в том, что все данные передаются только через ваш сервер, а комплексное шифрование TLS обеспечивает защиту от перехвата и несанкционированного прослушивания.

Jicofo — XMPP-компонент, модератор видеоконференций. Клиенты договариваются о связи, заходя в общую XMPP-комнату, и обмениваются там XMPP-сообщениями. Имеет HTTP API / about/health для опроса о состоянии сервиса.

Jitsi Videobridge — механизм медиасервера, который поддерживает все многосторонние видеоконференции Jitsi. Он передаёт видео и аудио между участниками, осуществляя роль посредника, терминирует RTP/RTCP, определяет доступные рамки битрейта в обе стороны на конкретного клиента. Имеет свой внутренний HTTP API для мониторинга (/colibri/debug).

Jigasi — шлюз для участия в Jitsi-конференциях через SIP-телефонию.

Jibri — вещатель и рекордер, используемые для сохранения записей видеозвонков и потоковой передачи на YouTube Live.

Ниже приведена инструкция по настройке сервера Jitsi Meet в Альт Сервер.

53.1. Требования к системе

Для размещения нужны:

- jitsi-videobridge: хост с доступными портами 10000/udp, 4443/tcp и хорошей пропускной способностью (рекомендуется минимум 100Mbps симметрично);
- веб-сервер: хост с доступным портом 443/tcp. Веб-сервер должен поддерживать HTTPS;
- xmpp-сервер: хост с доступным портом 5280/tcp для работы XMPP-over-HTTP (BOSH).

Примечание

Теоретически компоненты могут размещаться на разных машинах; на практике не рекомендуется устанавливать prosody и jicofo на разные машины — это может привести к низкой производительности сервиса и большим колебаниям задержки связи.

53.2. Установка

Установить пакеты:

```
# apt-get install prosody jitsi-meet-prosody jitsi-meet-web jitsi-meet-web-config jicofo jitsi-videobridge
```

Примечание

Компоненты Jitsi Meet можно установить при установке системы, выбрав для установки пункт «Сервер видеоконференций (Jitsi Meet)» (подробнее описано в главе Установка системы).

Примечание

В примере ниже указан DNS адрес сервера jitsi2.test.alt, следует заменить его на свой.

53.3. Конфигурация

53.3.1. Настройка имени хоста системы

Установить имя хоста системы на доменное имя, которое будет использоваться для Jitsi:

```
# hostnamectl set-hostname jitsi2
```

Установить локальное сопоставление имени хоста сервера с IP-адресом 127.0.0.1, для этого дописать в файл **/etc/hosts** строку:

```
127.0.0.1    jitsi2.test.alt jitsi2
```

Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

Проверить правильность установленного имени можно, выполнив команды:

```
# hostname
jitsi2
# hostname -f
jitsi2.test.alt
$ ping "$(hostname)"
PING jitsi2.test.alt (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.053 ms
[...]
```

53.3.2. Настройка XMPP-сервера (prosody)

Создать каталог **/etc/prosody/conf.d** для хранения пользовательских конфигураций:

```
# mkdir -p /etc/prosody/conf.d
```

В конец файла **/etc/prosody/prosody.cfg.lua** дописать строку:

```
Include "conf.d/*.cfg.lua"
```

Создать конфигурационный файл prosody для вашего домена (например, **/etc/prosody/conf.d/jitsi2.test.alt.cfg.lua**) со следующим содержимым:

```
plugin_paths = { "/usr/share/jitsi-meet/prosody-plugins/" }

-- domain mapper options, must at least have domain base set to use the
mapper
muc_mapper_domain_base = "jitsi2.test.alt";

cross_domain_bosh = false;
consider_bosh_secure = true;

----------- Virtual hosts -----------
VirtualHost "jitsi2.test.alt"
    authentication = "anonymous"
    ssl = {
       key = "/var/lib/prosody/jitsi2.test.alt.key";
       certificate = "/var/lib/prosody/jitsi2.test.alt.crt";
    }
    speakerstats_component = "speakerstats.jitsi2.test.alt"
```

```
    conference_duration_component = "conferenceduration.jitsi2.test.alt"
         -- we need bosh
    modules_enabled = {
        "bosh";
        "pubsub";
        "ping"; -- Enable mod_ping
        "speakerstats";
        "turncredentials";
        "conference_duration";
    }
    c2s_require_encryption = false


Component "conference.jitsi2.test.alt" "muc"
    storage = "memory"
    modules_enabled = {
        "muc_meeting_id";
        "muc_domain_mapper";
        -- "token_verification";
    }
    admins = { "focus@auth.jitsi2.test.alt" }
    muc_room_locking = false
    muc_room_default_public_jids = true

VirtualHost "auth.jitsi2.test.alt"
    ssl = {
        key = "/var/lib/prosody/auth.jitsi2.test.alt.key";
        certificate = "/var/lib/prosody/auth.jitsi2.test.alt.crt";
    }
    authentication = "internal_plain"

-- internal muc component, meant to enable pools of jibri and jigasi clients
Component "internal.auth.jitsi2.test.alt" "muc"
    storage = "memory"
    modules_enabled = {
        "ping";
    }
    admins = { "focus@auth.jitsi2.test.alt", "jvb@auth.jitsi2.test.alt" }
    muc_room_locking = false
    muc_room_default_public_jids = true

Component "focus.jitsi2.test.alt"
    component_secret = "secret1" -- достаточно длинный пароль, он же
JICOFO_SECRET

Component "speakerstats.jitsi2.test.alt" "speakerstats_component"
    muc_component = "conference.jitsi2.test.alt"

Component "conferenceduration.jitsi2.test.alt"
"conference_duration_component"
    muc_component = "conference.jitsi2.test.alt"
```

Сгенерировать сертификаты для виртуальных хостов jitsi2.test.alt и auth.jitsi2.test.alt:

```
# prosodyctl cert generate jitsi2.test.alt
# prosodyctl cert generate auth.jitsi2.test.alt
```

Зарегистрировать сертификаты в системе, как доверенные (сертификаты нужно регистрировать там, где устанавливается Jicofo):

```
# ln -s /var/lib/prosody/jitsi2.test.alt.crt /etc/pki/ca-trust/source/
anchors/
# ln -s /var/lib/prosody/auth.jitsi2.test.alt.crt /etc/pki/ca-trust/source/
anchors/
# update-ca-trust
```

Зарегистрировать пользователя focus (аккаунт focus@auth.jitsi2.test.alt):

```
# prosodyctl register focus auth.jitsi2.test.alt secret2
```

где secret2 — достаточно длинный пароль.

Запустить prosody:

```
# prosodyctl start
```

53.3.3. Настройка jicofo

Jicofo подключается к XMPP-серверу и как внешний XMPP-компонент, и как пользовательский аккаунт с JID focus@auth.jitsi2.test.alt.

В файле **/etc/jitsi/jicofo/config** следует указать:

```
# Jitsi Conference Focus settings
# sets the host name of the XMPP server
JICOFO_HOST=localhost

# sets the XMPP domain (default: none)
JICOFO_HOSTNAME=jitsi2.test.alt

# sets the secret used to authenticate as an XMPP component
JICOFO_SECRET=secret1

# overrides the prefix for the XMPP component domain. Default: "focus"
#JICOFO_FOCUS_SUBDOMAIN=focus

# sets the port to use for the XMPP component connection
JICOFO_PORT=5347

# sets the XMPP domain name to use for XMPP user logins
JICOFO_AUTH_DOMAIN=auth.jitsi2.test.alt

# sets the username to use for XMPP user logins
JICOFO_AUTH_USER=focus

# sets the password to use for XMPP user logins
JICOFO_AUTH_PASSWORD=secret2

# extra options to pass to the jicofo daemon
JICOFO_OPTS="${JICOFO_FOCUS_SUBDOMAIN:+ --subdomain=$JICOFO_FOCUS_SUBDOMAIN}"

# adds java system props that are passed to jicofo (default are for home and
logging config file)
```

```
JAVA_SYS_PROPS="-Dnet.java.sip.communicator.SC_HOME_DIR_LOCATION=/etc/jitsi
-Dnet.java.sip.communicator.SC_HOME_DIR_NAME=jicofo
-Dnet.java.sip.communicator.SC_LOG_DIR_LOCATION=/var/log/jitsi
-Djava.util.logging.config.file=/etc/jitsi/jicofo/logging.properties"
```

Важно

В строке

```
JICOFO_SECRET=secret1
```

должен быть указан пароль, установленный в файле **/etc/prosody/conf.d/jitsi2.test.alt.cfg.lua**.

В строке

```
JICOFO_AUTH_PASSWORD=secret2
```

должен быть указан пароль пользователя focus.

В файле **/etc/jitsi/jicofo/sip-communicator.properties** следует указать:

```
org.jitsi.jicofo.health.ENABLE_HEALTH_CHECKS=true
org.jitsi.jicofo.BRIDGE_MUC=JvbBrewery@internal.auth.jitsi2.test.alt
```

Запустите jicofo:

```
# systemctl start jicofo
```

Убедитесь, что jicofo подключается к XMPP-серверу:

```
# curl -i localhost:8888/about/health
HTTP/1.1 500 Internal Server Error
Date: Fri, 26 Jun 2020 11:55:02 GMT
Content-Type: application/json
Content-Length: 56
Server: Jetty(9.4.15.v20190215)

No operational bridges available (total bridge count: 0)
```

Так как пока ни одного Jitsi Videobridge к серверу не подключено, jicofo ответит кодом ответа 500 и сообщением *No operational bridges available*. Если в ответе сообщение об ошибке иного рода — следует проверить настройки и связь между prosody и jicofo.

53.3.4. Настройка jitsi-videobridge

Завести на XMPP-сервере аккаунт jvb@auth.jitsi2.test.alt:

```
# prosodyctl register jvb auth.jitsi2.test.alt secret3
```

Заменить содержимое файла **/etc/jitsi/videobridge/config** на следующее:

```
# Jitsi Videobridge settings

# extra options to pass to the JVB daemon
JVB_OPTS="--apis=,"


# adds java system props that are passed to jvb (default are for home and
logging config file)
JAVA_SYS_PROPS="-Dnet.java.sip.communicator.SC_HOME_DIR_LOCATION=/etc/jitsi
-Dnet.java.sip.communicator.SC_HOME_DIR_NAME=videobridge
-Dnet.java.sip.communicator.SC_LOG_DIR_LOCATION=/var/log/jitsi
-Djava.util.logging.config.file=/etc/jitsi/videobridge/logging.properties
-Dconfig.file=/etc/jitsi/videobridge/application.conf"
```

В качестве файлов конфигурации jitsi-videobridge используются файлы **`/etc/jitsi/videobridge/application.conf`** и **`/etc/jitsi/videobridge/sip-communicator.properties`**.

В файле **`/etc/jitsi/videobridge/application.conf`** необходимо указать:

```
videobridge {
    stats {
        enabled = true
        transports = [
            { type = "muc" }
        ]
    }
    apis {
        xmpp-client {
            configs {
                shard {
                    hostname = "localhost"
                    domain = "auth.jitsi2.test.alt"
                    username = "jvb"
                    password = "secret3"
                    muc_jids = "JvbBrewery@internal.auth.jitsi2.test.alt"
                    # The muc_nickname must be unique across all instances
                    muc_nickname = "jvb-mid-123"
                }
            }
        }
    }
}
```

Важно

В строке

```
password = "secret3"
```

должен быть указан пароль пользователя jvb.

Вместо слова shard можно использовать любой идентификатор (оно идентифицирует подключение к xmpp-серверу и jicofo).

Измените содержимое файла **/etc/jitsi/videobridge/sip-communicator.properties**:

```
org.ice4j.ice.harvest.DISABLE_AWS_HARVESTER=true
org.ice4j.ice.harvest.STUN_MAPPING_HARVESTER_ADDRESSES=meet-jit-si-
turnrelay.jitsi.net:443
org.jitsi.videobridge.ENABLE_STATISTICS=true
org.jitsi.videobridge.STATISTICS_TRANSPORT=muc
org.jitsi.videobridge.xmpp.user.shard.HOSTNAME=localhost
org.jitsi.videobridge.xmpp.user.shard.DOMAIN=auth.jitsi2.test.alt
org.jitsi.videobridge.xmpp.user.shard.USERNAME=jvb
org.jitsi.videobridge.xmpp.user.shard.PASSWORD=secret3
org.jitsi.videobridge.xmpp.user.shard.MUC_JIDS=JvbBrewery@internal.auth.jits
i2.test.alt
org.jitsi.videobridge.xmpp.user.shard.MUC_NICKNAME=6d8b40cb-fe32-49f5-
a5f6-13d2c3f95bba
```

Примечание

Если JVB-машина отделена от клиентов при помощи NAT, то потребуется донастройка.

Запустите JVB:

```
# systemctl start jitsi-videobridge
```

Убедитесь, что между JVB и jicofo есть связь:

```
# curl -i localhost:8888/about/health
HTTP/1.1 200 OK
Date: Fri, 26 Jun 2020 13:04:15 GMT
Content-Length: 0
Server: Jetty(9.4.15.v20190215)
```

Если всё сделано правильно, jicofo на healthcheck-запрос будет отдавать HTTP-код 200.

53.3.5. Настройка веб-приложения Jitsi Meet

Получить SSL/TLS-сертификат для домена.

Примечание

Можно создать сертификат без обращения к УЦ. При использовании такого сертификата в браузере будут выводиться предупреждения.

Для создания самоподписанного сертификата следует:

- создать корневой ключ:

```
# openssl genrsa -out rootCA.key 2048
```

- создать корневой сертификат:

```
# openssl req -x509 -new -key rootCA.key -days 10000 -out rootCA.crt
-subj "/C=RU/ST=Russia/L=Moscow/CN=SuperPlat CA Root"
```

- сгенерировать ключ:

```
# openssl genrsa -out jitsi2.test.alt.key 2048
```

- создать запрос на сертификат (тут важно указать имя сервера: домен или IP):

```
# openssl req -new -key jitsi2.test.alt.key -out jitsi2.test.alt.csr
-subj "/C=RU/L=Moscow/CN=jitsi2.test.alt"
```

- подписать запрос на сертификат корневым сертификатом:

```
# openssl x509 -req -in jitsi2.test.alt.csr -CA rootCA.crt -CAkey
rootCA.key -CAcreateserial -out jitsi2.test.alt.crt -days 5000
Signature ok
subject=C = RU, CN = jitsi2.test.alt
Getting CA Private Key
```

Положить ключ и сертификат в папку **/etc/jitsi/meet/**:

```
# cp jitsi2.test.alt.crt /etc/jitsi/meet/
# cp jitsi2.test.alt.key /etc/jitsi/meet/
```

В пакете jitsi-meet-web-config есть примеры конфигурации для веб-клиента (*-config.js) и веб-сервера (*.example.apache, *.example).

Создать файл **/etc/jitsi/meet/jitsi2.test.alt-config.js** на основе **/usr/share/jitsi-meet-web-config/config.js**:

```
# cp /usr/share/jitsi-meet-web-config/config.js /etc/jitsi/meet/
jitsi2.test.alt-config.js
```

Внести изменения в файл **/etc/jitsi/meet/jitsi2.test.alt-config.js** в соответствии с настройками серверной части:

```
var config = {
    // Connection
    //

    hosts: {
        // XMPP domain.
        domain: 'jitsi2.test.alt',

        muc: 'conference.jitsi2.test.alt'
    },

    // BOSH URL. FIXME: use XEP-0156 to discover it.
    bosh: '//jitsi2.test.alt/http-bind',

    // Websocket URL
    // websocket: 'wss://jitsi-meet.example.com/xmpp-websocket',

    // The name of client node advertised in XEP-0115 'c' stanza
    clientNode: 'http://jitsi.org/jitsimeet',

[...]

}
```

Так как в Альт Сервер по умолчанию установлен веб-сервер apache, то ниже рассмотрена настройка именно этого веб-сервера. Пример конфигурации можно взять в файле **/usr/share/doc/jitsi-meet-web-config-4109/jitsi-meet/jitsi-meet.example-apache**

Создать файл **/etc/httpd2/conf/sites-available/jitsi2.test.alt.conf** на основе **/usr/share/doc/jitsi-meet-web-config-4109/jitsi-meet/jitsi-meet.example-apache**:

```
# cp /usr/share/doc/jitsi-meet-web-config-4109/jitsi-meet/jitsi-meet.example-apache /etc/httpd2/conf/sites-available/jitsi2.test.alt.conf
```

Внести изменения в файл **/etc/httpd2/conf/sites-available/jitsi2.test.alt.conf** (изменить имя, указать сертификат):

```
<VirtualHost *:80>
    ServerName jitsi2.test.alt
    Redirect permanent / https://jitsi2.test.alt/
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
</VirtualHost>

<VirtualHost *:443>

  ServerName jitsi2.test.alt

  SSLProtocol TLSv1 TLSv1.1 TLSv1.2
  SSLEngine on
  SSLProxyEngine on
  SSLCertificateFile /etc/jitsi/meet/jitsi2.test.alt.crt
  SSLCertificateKeyFile /etc/jitsi/meet/jitsi2.test.alt.key
  SSLCipherSuite
"EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA256:EECDH+aRSA+SHA256:E
ECDH+ECDSA+SHA384:EECDH+ECDSA+SHA256:EECDH+aRSA+SHA384:EDH+aRSA+AESGCM:EDH+a
```

```
RSA+SHA256:EDH+aRSA:EECDH:!aNULL:!eNULL:!MEDIUM:!LOW:!3DES:!MD5:!EXP:!PSK:!
SRP:!DSS:!RC4:!SEED"
  SSLHonorCipherOrder on
  Header set Strict-Transport-Security "max-age=31536000"'

  DocumentRoot "/usr/share/jitsi-meet"
  <Directory "/usr/share/jitsi-meet">
    Options Indexes MultiViews Includes FollowSymLinks
    AddOutputFilter Includes html
    AllowOverride All
    Order allow,deny
    Allow from all
  </Directory>

  ErrorDocument 404 /static/404.html

  Alias "/config.js" "/etc/jitsi/meet/jitsi2.test.alt-config.js"
  <Location /config.js>
    Require all granted
  </Location>

  Alias "/external_api.js" "/usr/share/jitsi-meet/libs/external_api.min.js"
  <Location /external_api.js>
    Require all granted
  </Location>

  ProxyPreserveHost on
  ProxyPass /http-bind http://localhost:5280/http-bind/
  ProxyPassReverse /http-bind http://localhost:5280/http-bind/

  RewriteEngine on
  RewriteRule ^/([a-zA-Z0-9]+)$ /index.html
 </VirtualHost>
```

Установить пакет apache2-mod_ssl, если он еще не установлен:

```
# apt-get install apache2-mod_ssl
```

Выполнить команды:

```
# a2enmod rewrite
# a2enmod ssl
# a2enmod headers
# a2enmod proxy
# a2enmod proxy_http
# a2enport https
```

Включить конфигурацию Apache:

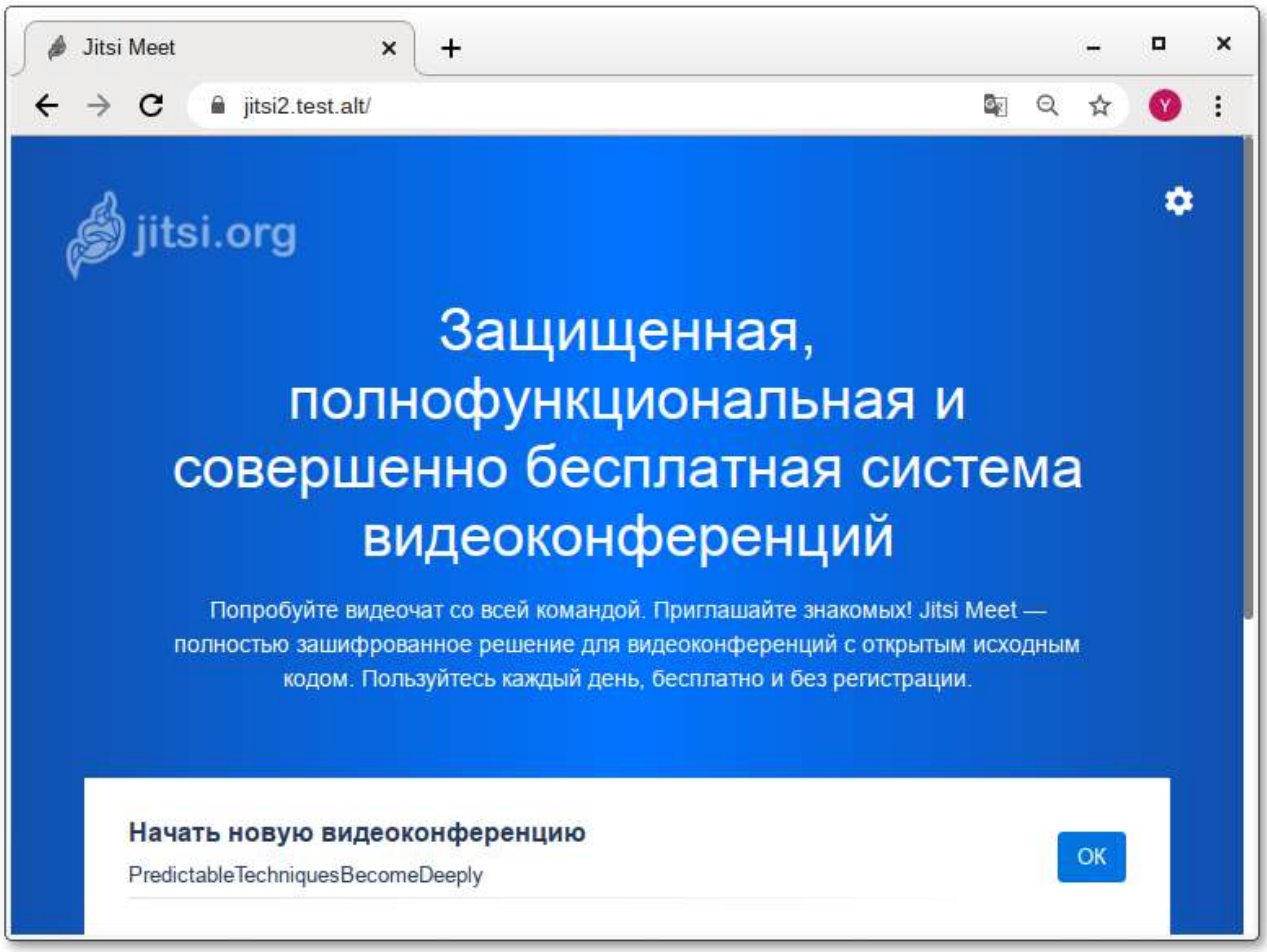
```
# a2ensite jitsi2.test.alt
```

Запустить веб-сервер Apache2 и добавить его в автозагрузку, выполнив команды:

```
# systemctl start httpd2
# systemctl enable httpd2
```

53.4. Работа с сервисом

Для общения достаточно запустить веб-браузер и перейти на сайт. В нашем примере сервис доступен по адресу: **`https://jitsi2.test.alt`**:



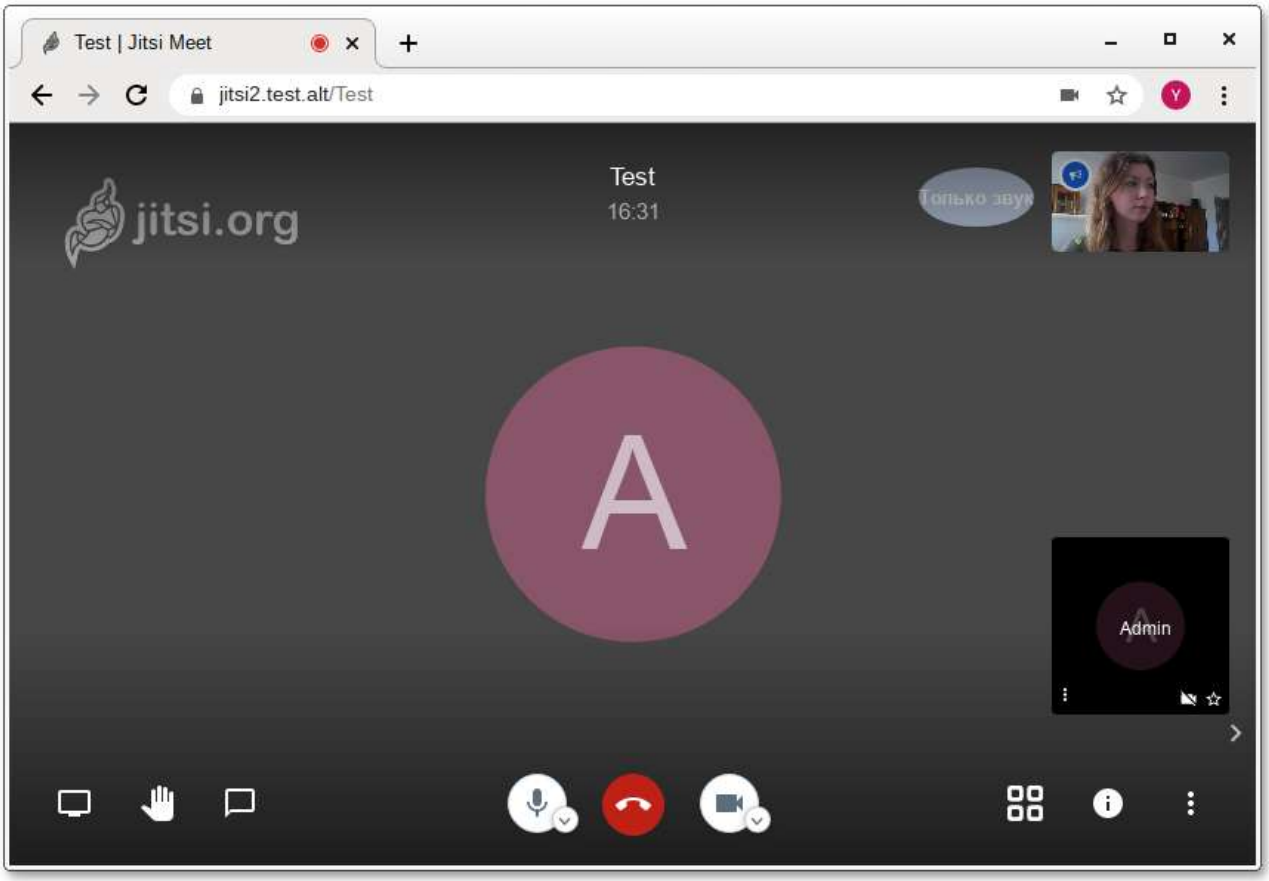
Для того чтобы начать новую конференцию, достаточно придумать и ввести название будущей конференции (в имени можно использовать буквы на любом языке и пробелы). Чуть ниже будет отображаться список прошлых созданных конференций.

Примечание

Зная URL конференции, в неё может зайти любой желающий. Конференция создаётся, когда в неё заходит первый участник, и существует до выхода последнего. Предотвратить случайных посетителей можно выбрав достаточно длинный URL на главной странице веб-портала, генератор по умолчанию с этим справляется.

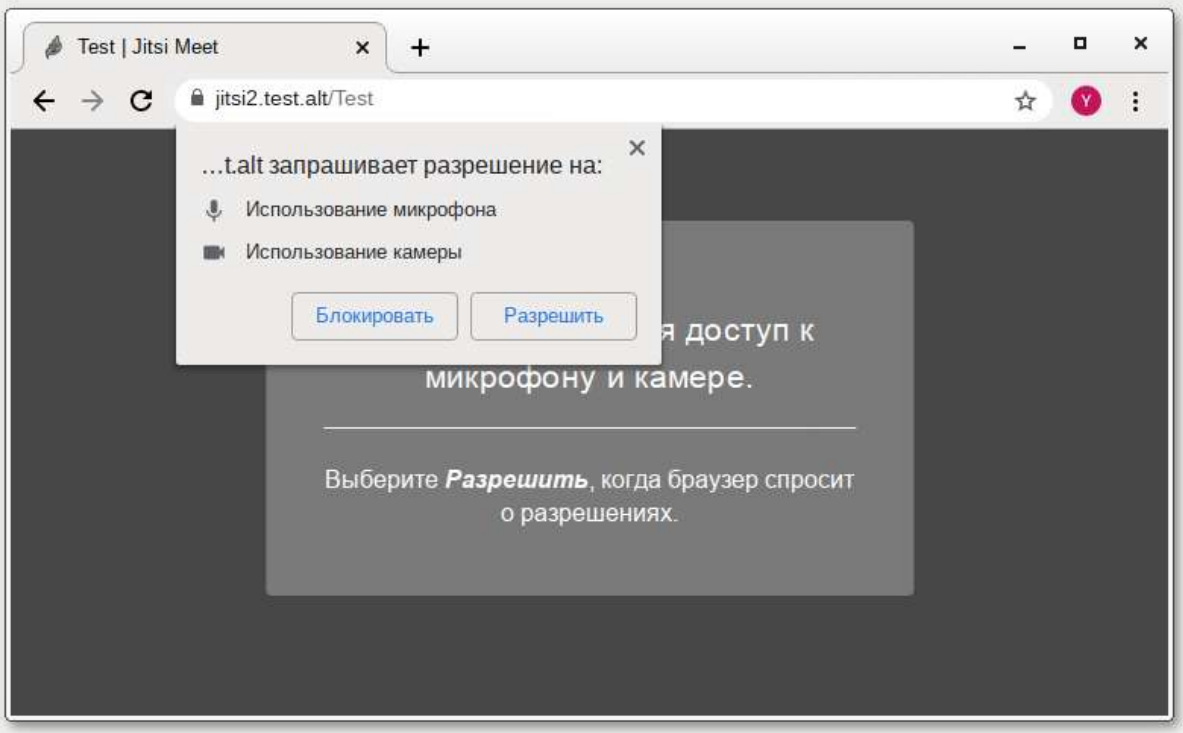
Можно предотвратить неавторизованное создание новых конференций подробнее в Отключение возможности неавторизованного создания новых конференций.

Ввести название конференции и нажать кнопку **OK**. Будет создана конференция:



Примечание

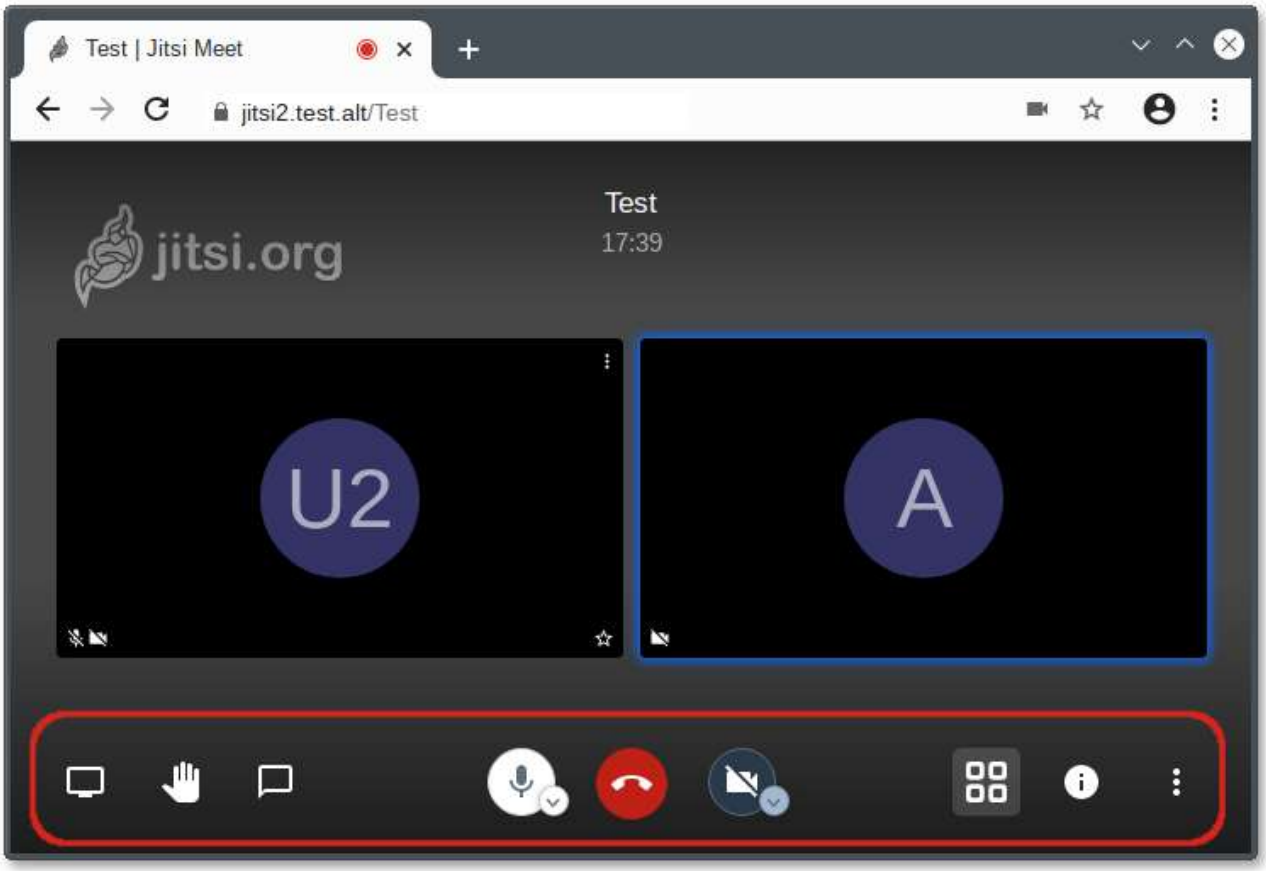
После создания конференции браузер попросит дать ему разрешение на использование веб-камеры и микрофона:



После создания конференции её администратором становится только тот, кто её создал. Администратор может удалять пользователей из конференции, выключать их микрофоны, давать пользователю слово. В случае если администратор покинул конференцию, то её администратором становится тот, кто подключился следующий после него.

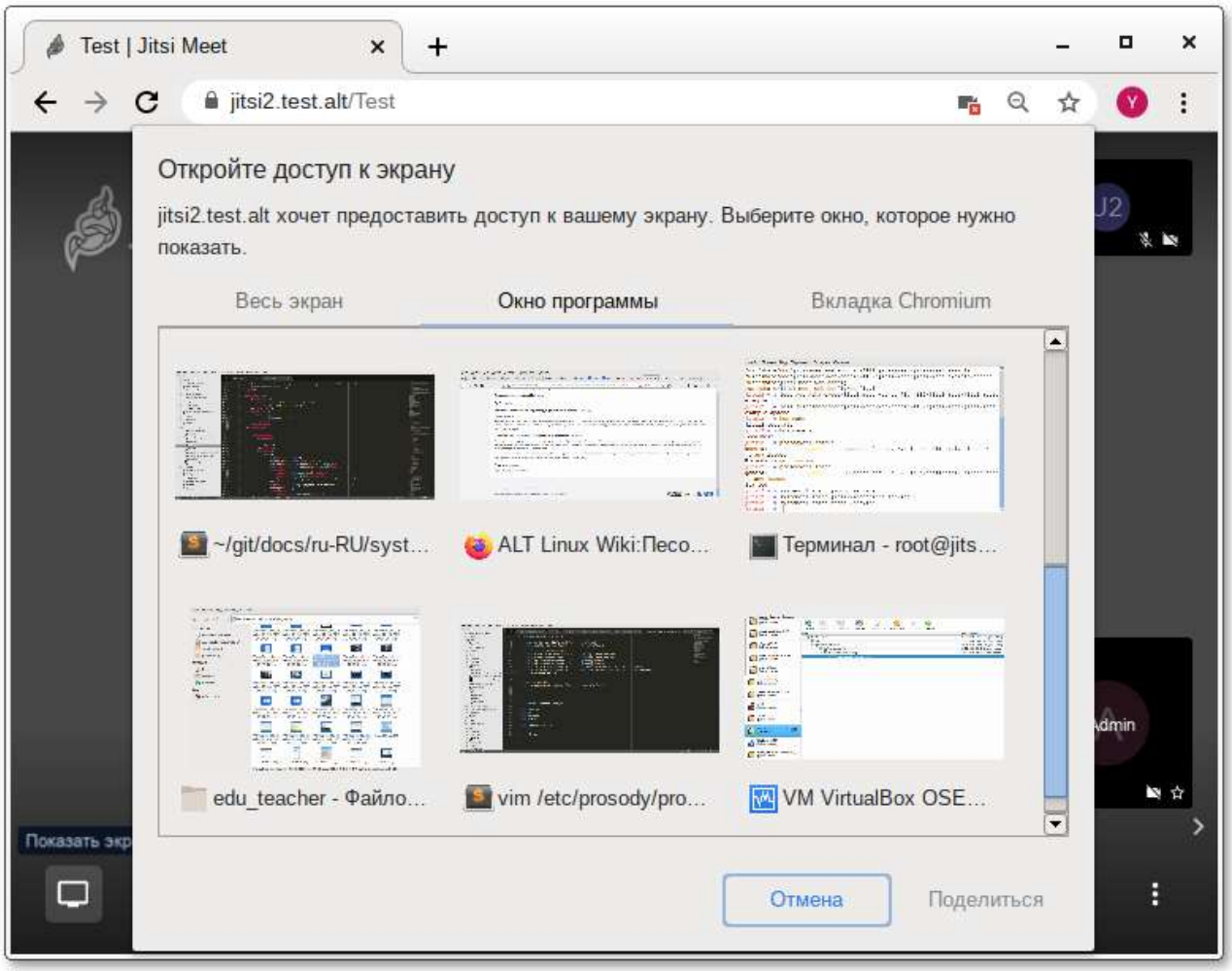
Конференция существует до тех пор, пока в ней есть хотя бы один человек.

Внизу окна конференции находится панель управления:



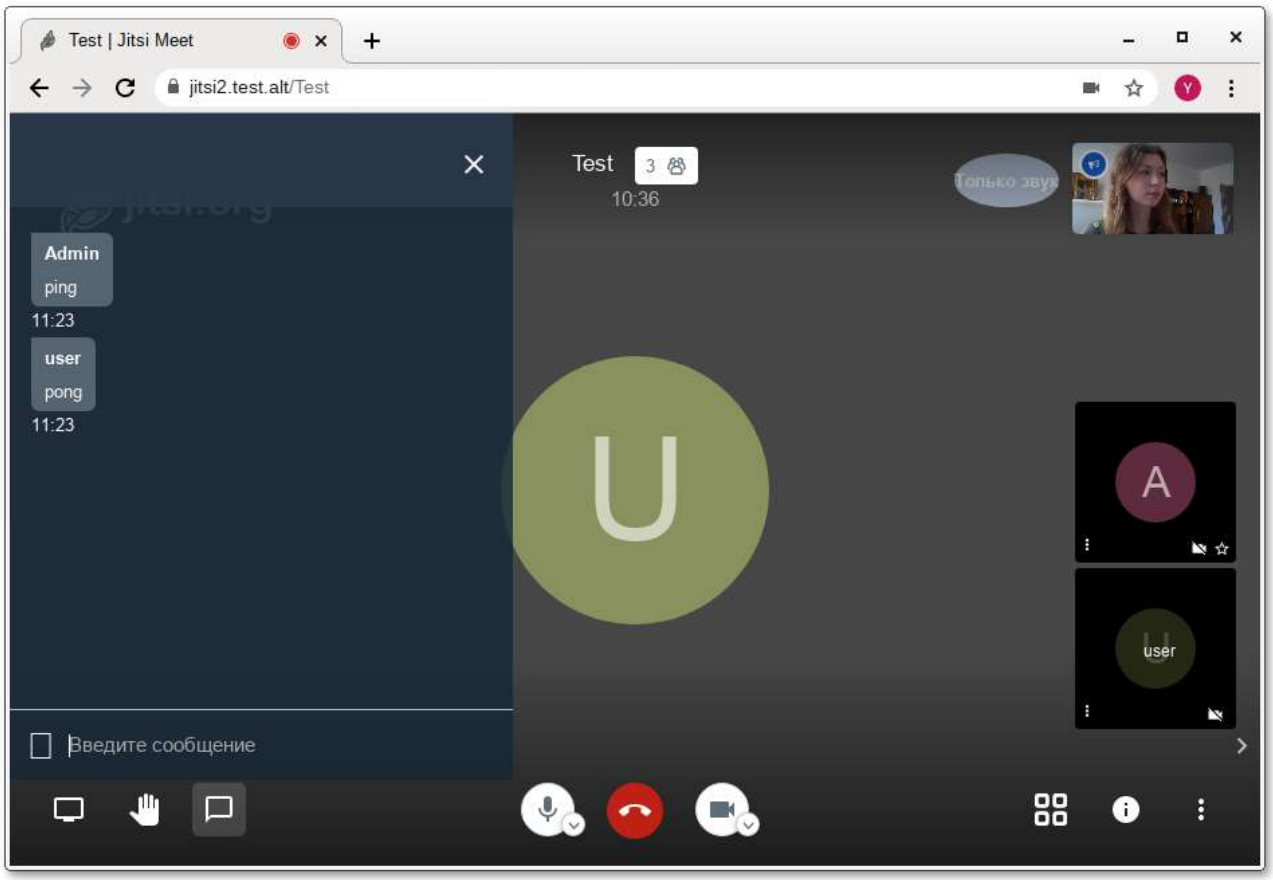
Первая кнопка на панели управления кнопка **Показать экран**. Если нажать на эту кнопку, откроется окно, в котором можно выбрать, что будет демонстрироваться другим участникам конференции. Доступны следующие опции:

- экран монитора;
- окно приложения;
- определённая вкладка браузера.



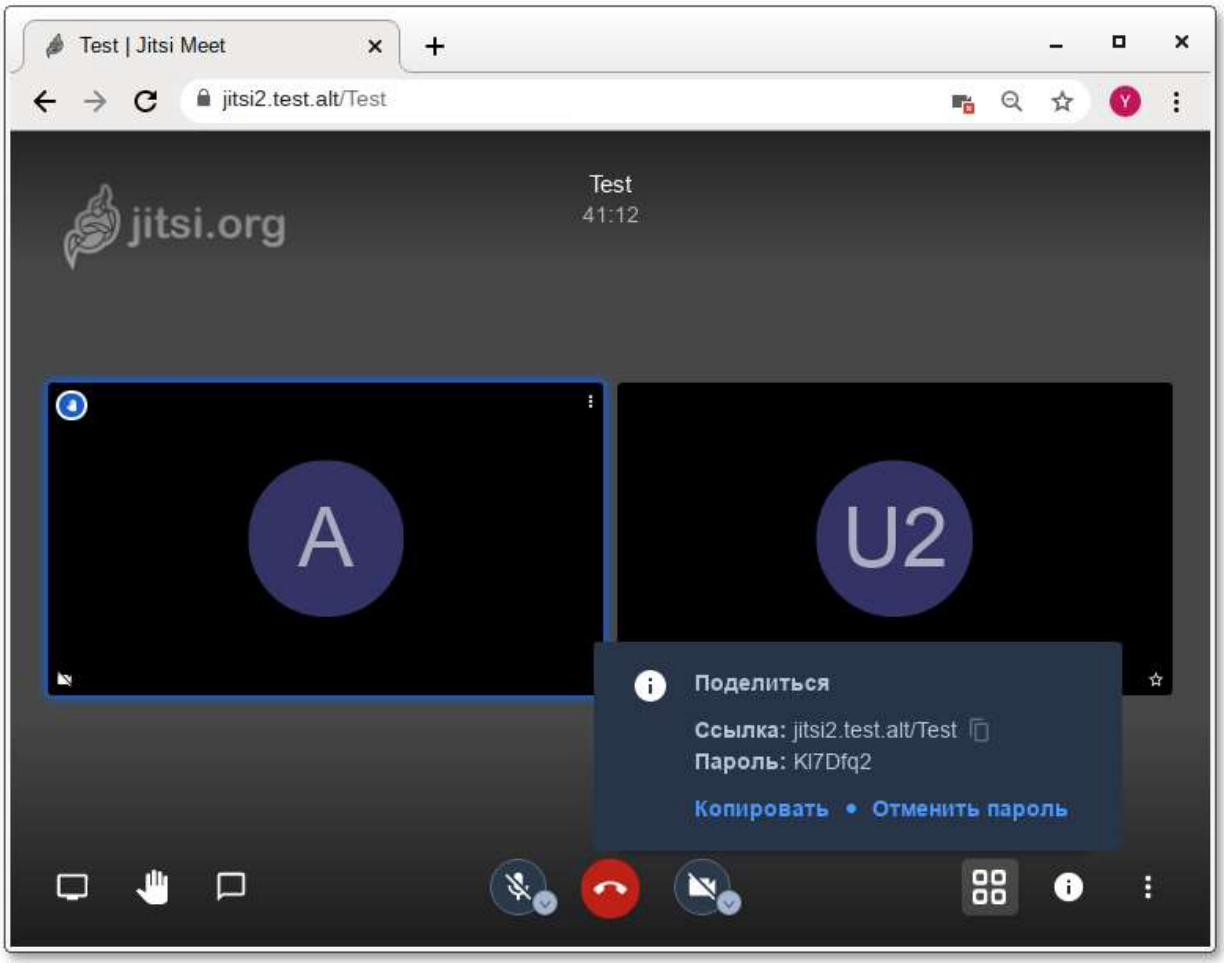
Нажатие на кнопку **Хочу говорить** сигнализирует организатору, что участник хочет говорить. В окне, соответствующем персонажу (справа), появится такой же значок ладони.

Кнопка **Чат** запускает чат в данной конференции:

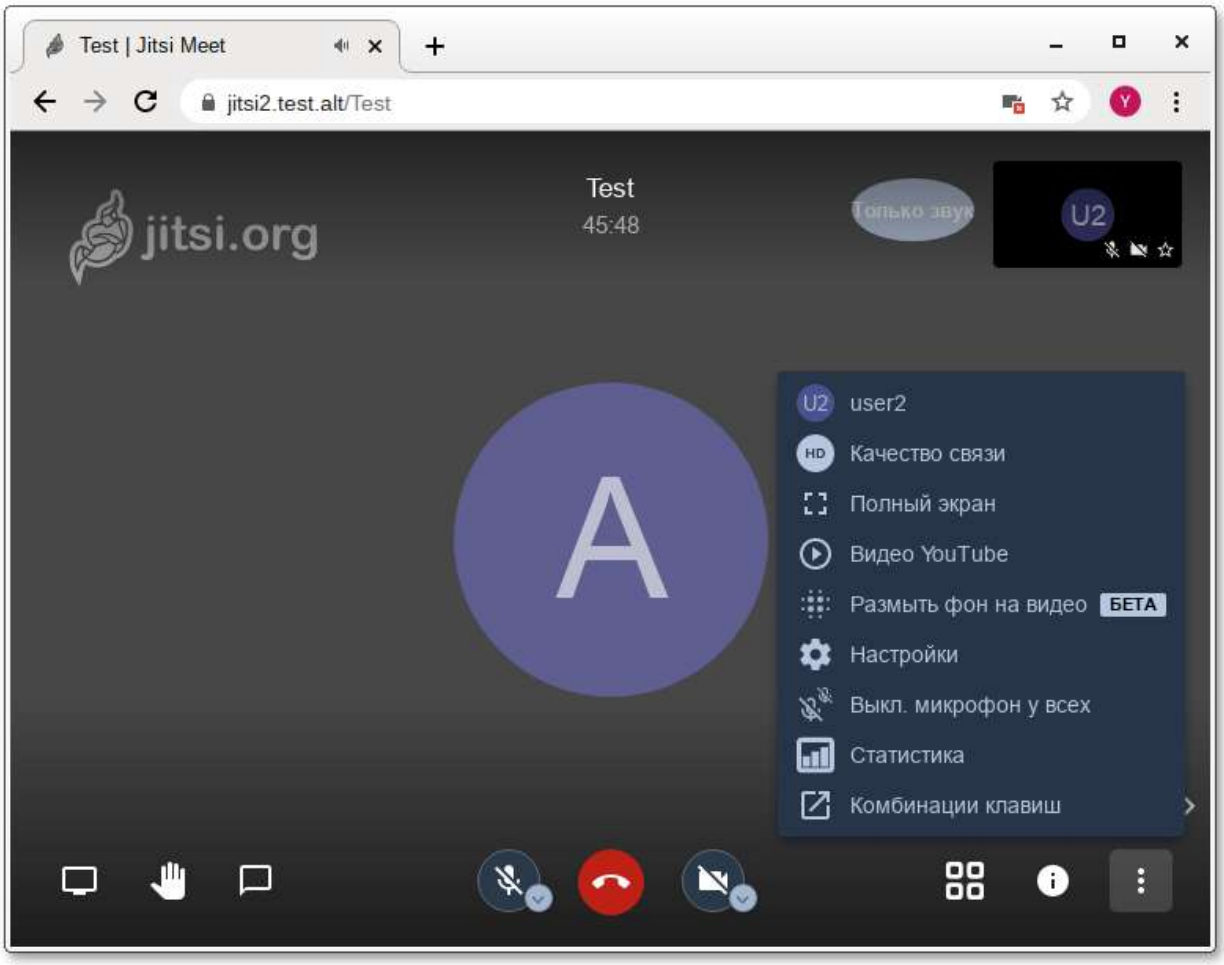


Следующие кнопки на панели управления и их назначение:

- **Микрофон** — позволяет включать и отключать микрофон;
- **Завершить** — выход из конференции;
- **Камера** — включение и выключение веб-камеры;
- **Вкл/Выкл плитку** — вывести окна собеседников в центр чата;
- **Информация о чате** — всплывающее окно, в котором приведена ссылка на конференцию. Здесь же администратор конференции может установить пароль для доступа к конференции:



Больше — настройка дополнительных функций Jitsi Meet:



53.5. Отключение возможности неавторизованного создания новых конференций

Можно разрешить создавать новые конференции только авторизованным пользователям. При этом каждый раз, при попытке создать новую конференцию, Jitsi Meet запросит имя пользователя и пароль. После создания конференции другие пользователи смогут присоединиться к ней анонимно.

Для отключения возможности неавторизованного создания новых конференций, необходимо выполнить следующие действия:

- отредактировать файл **`/etc/prosody/conf.d/jitsi2.test.alt.cfg.lua`**, изменив в нем запись:

  ```
  VirtualHost "jitsi2.test.alt"
  authentication = "anonymous"
  ```

  на:

  ```
  VirtualHost "jitsi2.test.alt"
  authentication = "internal_hashed"
  ```

- добавить в конец файла **`/etc/prosody/conf.d/jitsi2.test.alt.cfg.lua`** строки:

```
VirtualHost "guest.jitsi2.test.alt"
authentication = "anonymous"
c2s_require_encryption = false
```

Эти настройки позволят анонимным пользователям присоединяться к конференциям, созданным пользователем, прошедшим аутентификацию. При этом у гостя должен иметься уникальный адрес и пароль конференции (если этот пароль задан);

- в файле **/etc/jitsi/meet/jitsi2.test.alt-config.js** указать параметры анонимного домена:

```
domain: 'jitsi2.test.alt',
anonymousdomain: 'guest.jitsi2.test.alt',
```

- в файл **/etc/jitsi/jicofo/sip-communicator.properties** добавить строку:

```
org.jitsi.jicofo.auth.URL=XMPP:jitsi2.test.alt
```

- перезапустить процессы Jitsi Meet для загрузки новой конфигурации:

```
# prosodyctlt restart
# systemctl restart jicofo
# systemctl restart jitsi-videobridge
```

Команда для регистрации пользователей:

```
prosodyctl register <ПОЛЬЗОВАТЕЛЬ> jitsi2.test.alt <ПАРОЛЬ>
```

Изменить пароль пользователя:

```
prosodyctl passwd <ПОЛЬЗОВАТЕЛЬ>
```

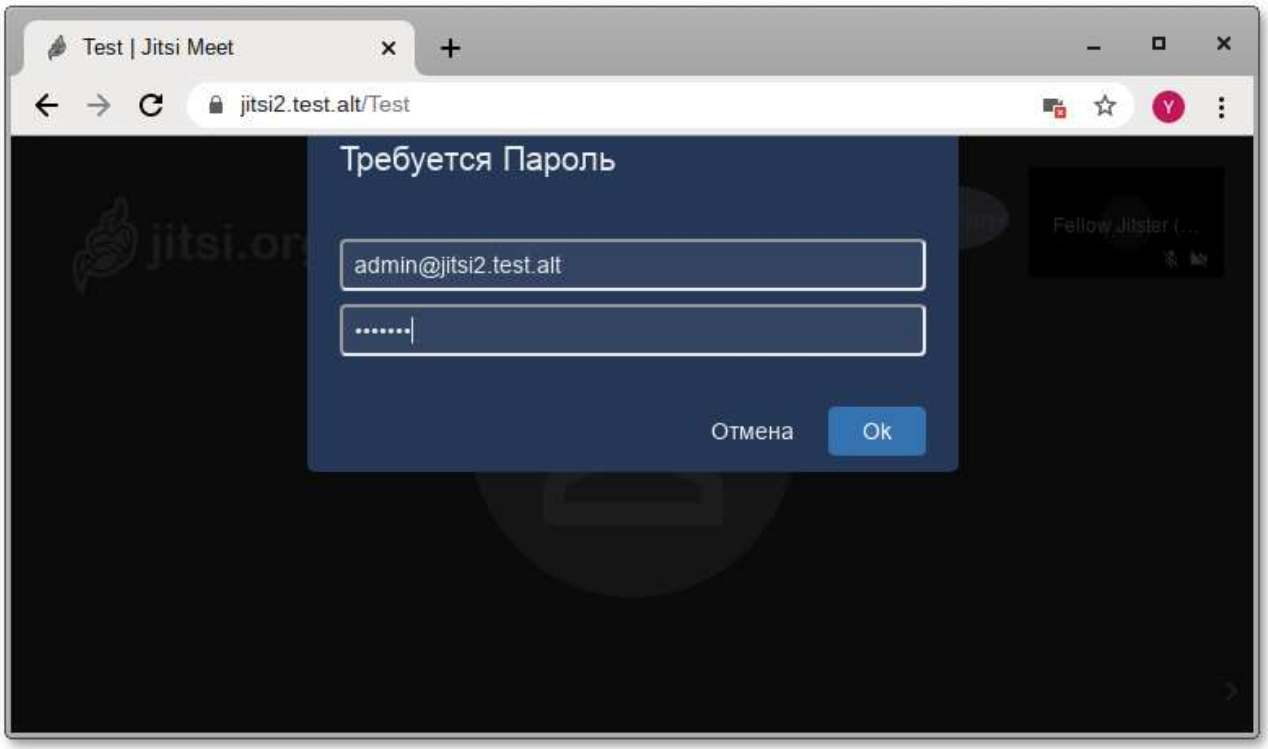
Удалить пользователя:

```
prosodyctl deluser <ПОЛЬЗОВАТЕЛЬ>
```

Например, создадим пользователя admin:

```
# prosodyctl register admin jitsi2.test.alt secret4
```

Теперь при создании конференции сервер Jitsi Meet будет требовать ввести имя пользователя и пароль:



Глава 54. Отказоустойчивый кластер (High Availability) на основе Pacemaker

Pacemaker — менеджер ресурсов кластера (Cluster Resource Manager), задачей которого является достижение максимальной доступности управляемых им ресурсов и защита их от сбоев как на уровне самих ресурсов, так и на уровне целых узлов кластера. Ключевые особенности Pacemaker:

- обнаружение и восстановление сбоев на уровне узлов и сервисов;
- возможность гарантировать целостность данных путем ограждения неисправных узлов;
- поддержка одного или нескольких узлов на кластер;
- поддержка нескольких стандартов интерфейса ресурсов (все, что может быть написано сценарием, может быть кластеризовано);
- независимость от подсистемы хранения — общий диск не требуется;
- поддержка и кворумных и ресурсозависимых кластеров;
- автоматически реплицируемая конфигурация, которую можно обновлять с любого узла;
- возможность задания порядка запуска ресурсов, а также их совместимости на одном узле;

- поддерживает расширенные типы ресурсов: клоны (когда ресурс запущен на множестве узлов) и дополнительные состояния (master/slave и подобное);
- единые инструменты управления кластером с поддержкой сценариев.

Архитектура Pacemaker представляет собой три уровня:

- кластеронезависимый уровень — на этом уровне располагаются ресурсы и их скрипты, которыми они управляются и локальный демон, который скрывает от других уровней различия в стандартах, использованных в скриптах;
- менеджер ресурсов (Pacemaker) — реагирует на события, происходящие в кластере: отказ или присоединение узлов, ресурсов, переход узлов в сервисный режим и другие административные действия. Pacemaker, исходя из сложившейся ситуации, делает расчет наиболее оптимального состояния кластера и дает команды на выполнение действий для достижения этого состояния (остановка/перенос ресурсов или узлов);
- информационный уровень (Corosync) — на этом уровне осуществляется сетевое взаимодействие узлов, т.е. передача сервисных команд (запуск/остановка ресурсов, узлов и т.д.), обмен информацией о полноте состава кластера (quorum) и т.д.

Узел (node) кластера представляет собой физический сервер или виртуальную машину с установленным Pacemaker. Узлы, предназначенные для предоставления одинаковых сервисов, должны иметь одинаковую конфигурацию.

Ресурсы, с точки зрения кластера, это все используемые сущности — сервисы, службы, точки монтирования, тома и разделы. При создании ресурса потребуется задать его класс, тип, провайдера и собственно имя с дополнительными параметрами. Ресурсы поддерживают множество дополнительных параметров: привязку к узлу (resource-stickiness), роли по умолчанию (started, stoped, master) и т.д. Есть возможности по созданию групп ресурсов, клонов (работающих на нескольких узлах) и т.п.

Связи определяют привязку ресурсов к узлу (location), порядок запуска ресурсов (ordering) и совместное их проживание на узле (colocation).

Ниже приведена инструкция по установке и настройке кластера в Альт Сервер.

54.1. Настройка узлов кластера

Для функционирования отказоустойчивого кластера необходимо, чтобы выполнялись следующие требования:

- дата и время между узлами в кластере должны быть синхронизированы;
- должно быть обеспечено разрешение имён узлов в кластере;
- сетевые подключения должны быть стабильными;
- у узлов кластера для организации изоляции узла (fencing) должны присутствовать функции управления питанием/перезагрузкой с помощью IPMI(ILO);
- следующие порты могут использоваться различными компонентами кластеризации: TCP-порты 2224, 3121 и 21064 и UDP-порт 5405 и должны быть открыты/доступны.

Примечание

В примере используется следующая конфигурация:

- node01 — первый узел кластера (IP 192.168.0.113/24);
- node02 — второй узел кластера (IP 192.168.0.145/24);
- node03 — третий узел кластера (IP 192.168.0.132/24);
- 192.168.0.251 — виртуальный IP по которому будет отвечать один из узлов.

Дальнейшие действия следует выполнить на всех узлах кластера.

Примечание

Рекомендуется использовать короткие имена узлов. Для изменения имени хоста без перезагрузки, можно воспользоваться утилитой **hostnamctl**:

```
# hostnamectl set-hostname node01
```

54.1.1. Настройка разрешений имён узлов

Следует обеспечить взаимно-однозначное прямое и обратное преобразование имён для всех узлов кластера. Желательно использовать DNS, в крайнем случае, можно обойтись соответствующими записями в локальных файлах **/etc/hosts** на каждом узле:

```
# echo "192.168.0.113 node01" >> /etc/hosts
# echo "192.168.0.145 node02" >> /etc/hosts
# echo "192.168.0.132 node03" >> /etc/hosts
```

Проверка правильности разрешения имён:

```
# ping node01
PING node01 (192.168.0.113) 56(84) bytes of data.
64 bytes from node01 (192.168.0.113): icmp_seq=1 ttl=64 time=0.352 ms
# ping node02
PING node02 (192.168.0.145) 56(84) bytes of data.
64 bytes from node02 (192.168.0.145): icmp_seq=1 ttl=64 time=0.635 ms
```

54.1.2. Настройка ssh-подключения между узлами

При настройке ssh-подключения для root по ключу необходимо убрать комментарии в файле **/etc/openssh/sshd_config** для строк:

```
PermitRootLogin without-password
PubkeyAuthentication yes
AuthorizedKeysFile  /etc/openssh/authorized_keys/%u /etc/openssh/
authorized_keys2/%u .ssh/authorized_keys .ssh/authorized_keys2
PasswordAuthentication yes
```

Кроме того, полезно добавить в **/etc/openssh/sshd_config** директиву:

```
AllowGroups sshusers
```

создать группу sshusers:

```
# groupadd sshusers
```

и добавить туда пользователей, которым разрешено подключаться по ssh:

```
# gpasswd -a <username> sshusers
```

Создать новый ключ SSH без пароля (параметр **-N**):

```
# ssh-keygen -t ed25519 -f ~/.ssh/id_ed25519 -N ""
```

Важно

Незащищенные ключи SSH (без пароля) не рекомендуются для серверов, открытых для внешнего мира.

Скопировать публичную часть SSH-ключа на другие узелы кластера:

```
# ssh-copy-id -i ~/.ssh/id_ed25519.pub user@node02
# ssh-copy-id -i ~/.ssh/id_ed25519.pub user@node03
```

В результате получаем возможность работы с домашними каталогами пользователя user удалённого узла — копировать к себе и от себя, удалять, редактировать и т.д.

Скопировать публичную часть SSH-ключа на все узлы кластера для администратора. Для этого подключиться к каждому узлу и под root скопировать публичную часть ключа:

```
# ssh user@node02
user@node02 $ su -
node02 # cat /home/user/.ssh/authorized_keys >> /root/.ssh/authorized_keys
node02 # exit
user@node02 $ exit
```

Важно

Каталог **/root/.ssh** при этом должен существовать.

Убедиться, что теперь можно запускать команды удалённо, без пароля:

```
# ssh node02 -- uname -n
node02
```

54.2. Установка кластерного ПО и создание кластера

Для управления кластером Pacemaker можно использовать утилиты **pcs** или **crm** (пакет crmsh).

Установить на всех узлах необходимые пакеты:

```
# apt-get install corosync resource-agents pacemaker pcs
```

Примечание

Данные пакеты не входят в состав ISO-образа дистрибутива, их можно установить из репозитория p9. О добавлении репозиториев с использованием графических приложений вы можете почитать в разделе Добавление репозиториев.

Примечание

Пакет resource-agent — содержит агенты ресурсов (набор скриптов) кластера, соответствующие спецификации Open Cluster Framework (OCF), используемые для взаимодействия с различными службами в среде высокой доступности, управляемой менеджером ресурсов Pacemaker. Если есть необходимость управлять дополнительными ресурсами, следует установить недостающий пакет resource-agents-*:

```
$ apt-cache search resource-agents*
```

Пакет pcs (pacemaker/corosync configuration system) — утилита для управления, настройки и мониторинга кластера. Управляется как через командную строку, так и через веб-интерфейс.

При установке Pacemaker автоматически будет создан пользователь hacluster. Для использования **pcs**, а также для доступа в веб-интерфейс нужно задать пароль пользователю hacluster (одинаковый на всех узлах):

```
# passwd hacluster
```

Запустить и добавить в автозагрузку службу pcsd:

```
# systemctl enable --now pcsd
```

Настроить аутентификацию (на одном узле):

```
# pcs host auth node01 node02 node03 -u hacluster
Password:
node02: Authorized
node01: Authorized
node03: Authorized
```

После этого кластером можно управлять с одного узла.

Создать кластер:

```
# pcs cluster setup newcluster node01 node02 node03
Destroying cluster on hosts: 'node01', 'node02', 'node03'...
node03: Successfully destroyed cluster
node01: Successfully destroyed cluster
node02: Successfully destroyed cluster
Requesting remove 'pcsd settings' from 'node01', 'node02', 'node03'
node01: successful removal of the file 'pcsd settings'
node03: successful removal of the file 'pcsd settings'
node02: successful removal of the file 'pcsd settings'
Sending 'corosync authkey', 'pacemaker authkey' to 'node01', 'node02',
'node03'
node01: successful distribution of the file 'corosync authkey'
node01: successful distribution of the file 'pacemaker authkey'
node03: successful distribution of the file 'corosync authkey'
node03: successful distribution of the file 'pacemaker authkey'
node02: successful distribution of the file 'corosync authkey'
node02: successful distribution of the file 'pacemaker authkey'
Sending 'corosync.conf' to 'node01', 'node02', 'node03'
node01: successful distribution of the file 'corosync.conf'
node02: successful distribution of the file 'corosync.conf'
node03: successful distribution of the file 'corosync.conf'
Cluster has been successfully set up.
```

Запустить кластер:

```
# pcs cluster start --all
node02: Starting Cluster...
node03: Starting Cluster...
node01: Starting Cluster...
```

Настройка автоматического включения кластера при загрузке:

```
# pcs cluster enable --all
node01: Cluster Enabled
node02: Cluster Enabled
node03: Cluster Enabled
```

Проверка состояния кластера:

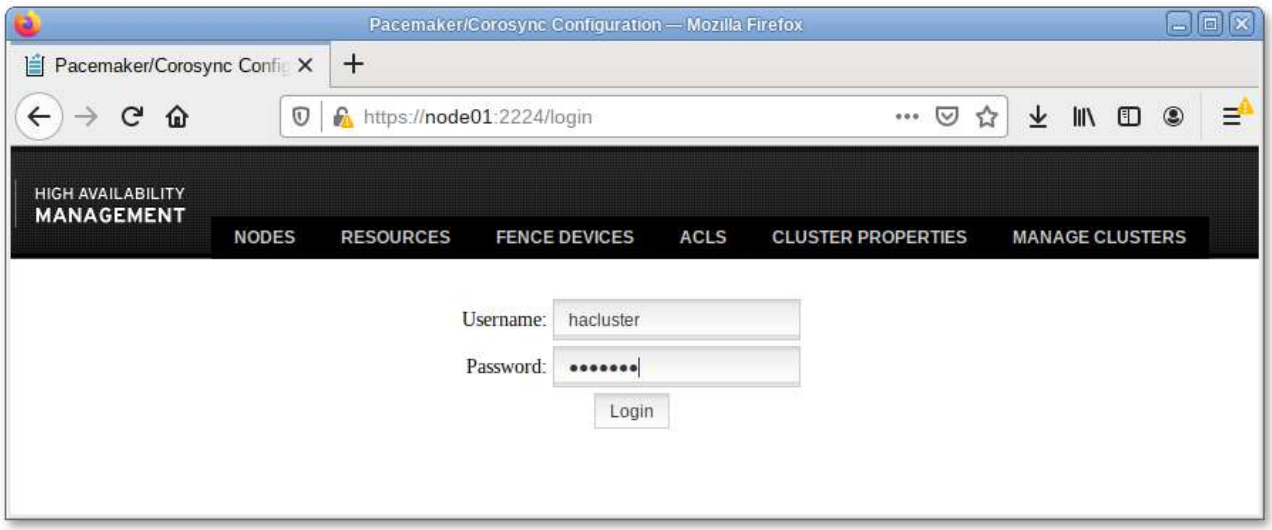
```
# pcs status cluster
Cluster Status:
 Cluster Summary:
   * Stack: corosync
   * Current DC: node02 (version 2.0.3-alt2-4b1f869f0) - partition with
quorum
   * Last updated: Thu Jan 28 13:26:38 2021
   * Last change:  Thu Jan 28 13:27:05 2021 by hacluster via crmd on node02
   * 3 nodes configured
   * 0 resource instances configured
 Node List:
   * Online: [ node01 node02 node03 ]

PCSD Status:
  node01: Online
  node02: Online
  node03: Online
```

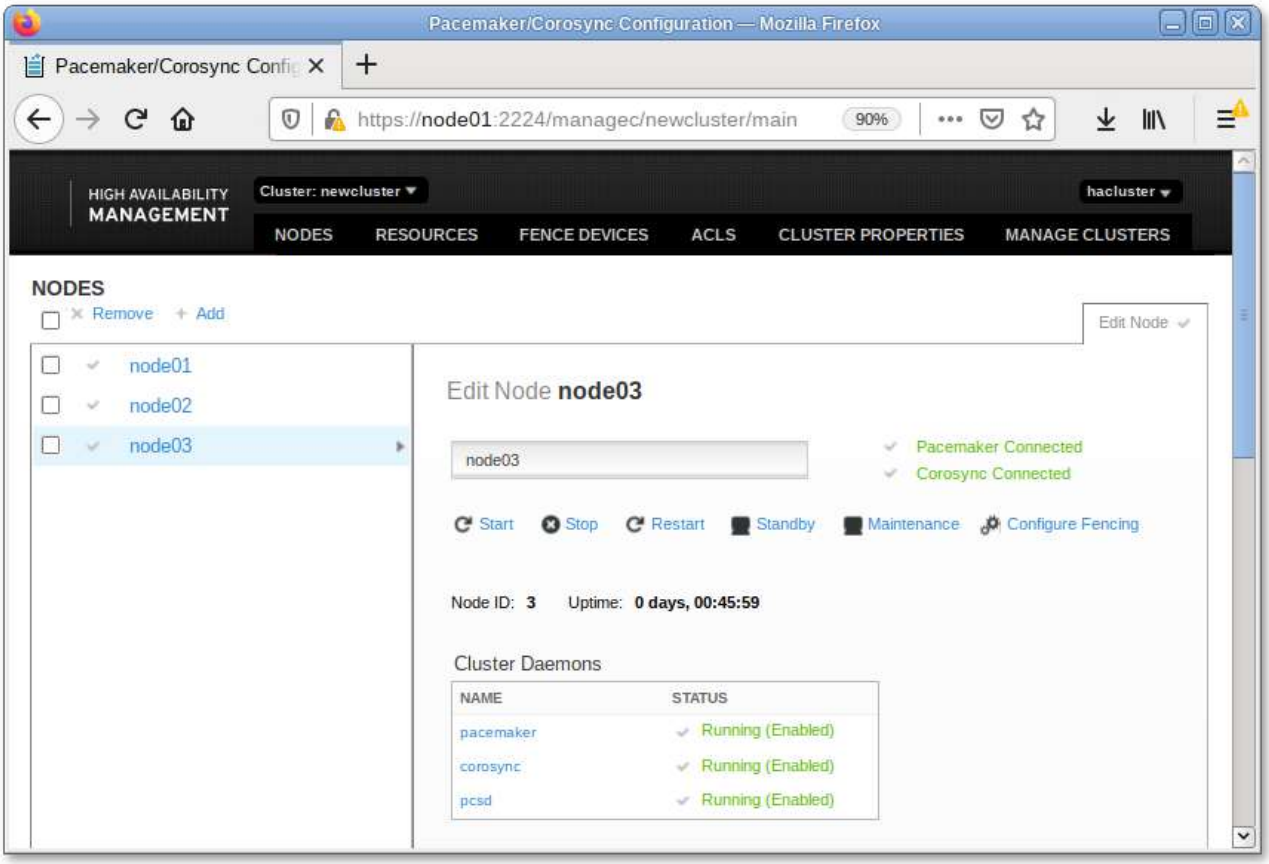
Проверка синхронизации узлов кластера:

```
# corosync-cmapctl | grep members
runtime.members.1.config_version (u64) = 0
runtime.members.1.ip (str) = r(0) ip(192.168.0.113)
runtime.members.1.join_count (u32) = 1
runtime.members.1.status (str) = joined
runtime.members.2.config_version (u64) = 0
runtime.members.2.ip (str) = r(0) ip(192.168.0.145)
runtime.members.2.join_count (u32) = 1
runtime.members.2.status (str) = joined
runtime.members.3.config_version (u64) = 0
runtime.members.3.ip (str) = r(0) ip(192.168.0.132)
runtime.members.3.join_count (u32) = 1
runtime.members.3.status (str) = joined
```

Веб-интерфейс управления кластером по адресу **`https://<имя-компьютера>:2224`** (в качестве имени компьютера можно использовать имя или IP-адрес одного из узлов в кластере). Потребуется пройти аутентификацию (логин и пароль учётной записи hacluster):

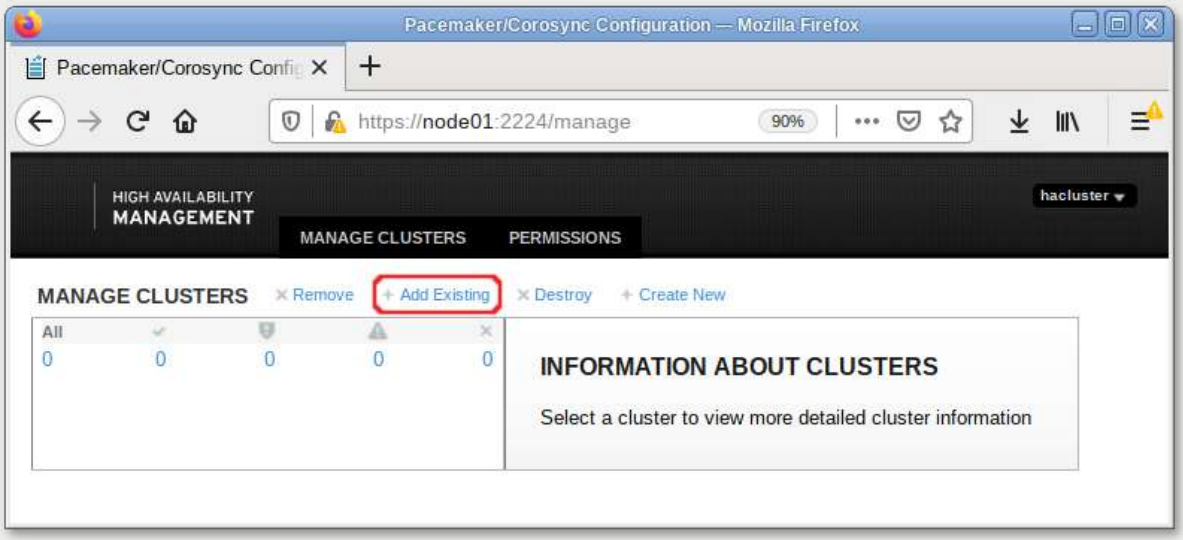


После входа в систему на главной странице отображается страница «Управление кластерами». На этой странице перечислены кластеры, которые в настоящее время находятся под управлением веб-интерфейса. При выборе кластера отображается информация о кластере:


Pacemaker/Corosync Configuration — Mozilla Firefox
Pacemaker/Corosync Config
https://node01:2224/managec/newcluster/main
90%
HIGH AVAILABILITY MANAGEMENT
Cluster: newcluster
hacluster
NODES
RESOURCES
FENCE DEVICES
ACLS
CLUSTER PROPERTIES
MANAGE CLUSTERS
NODES
Remove
Add
Edit Node
node01
node02
node03
Edit Node node03
node03
Pacemaker Connected
Corosync Connected
Start
Stop
Restart
Standby
Maintenance
Configure Fencing
Node ID: 3
Uptime: 0 days, 00:45:59
Cluster Daemons
NAME
STATUS
pacemaker
Running (Enabled)
corosync
Running (Enabled)
pcsd
Running (Enabled)

Примечание

Чтобы добавить существующий кластер в веб-интерфейс, необходимо нажать кнопку **Add `Existing`** и в открывшемся окне ввести имя или IP-адрес любого узла в кластере:



54.3. Настройка параметров кластера

Настройки кластера можно просмотреть, выполнив команду:

```
# pcs property
Cluster Properties:
 cluster-infrastructure: corosync
 cluster-name: newcluster
 dc-version: 2.0.3-alt2-4b1f869f0
 have-watchdog: false
 stonith-enabled: false
```

54.3.1. Кворум

Кворум определяет минимальное число работающих узлов в кластере, при котором кластер считается работоспособным. По умолчанию, кворум считается неработоспособным, если число работающих узлов меньше половины от общего числа узлов.

Отключить эту политику, например, если узла всего два, можно выполнив команду:

```
# pcs property set no-quorum-policy=ignore
```

54.3.2. Настройка STONITH

Для корректной работы узлов с общим хранилищем, необходимо настроить механизм STONITH. Этот механизм позволяет кластеру физически отключить не отвечающий на запросы узел, чтобы не повредить данные на общем хранилище.

Отключить STONITH, пока он не настроен можно, выполнив команду:

```
# pcs property set stonith-enabled=false
```

Важно

В реальной системе нельзя использовать конфигурацию с отключенным STONITH. Отключенный параметр на самом деле не отключает функцию, а только лишь эмулирует ее срабатывание при определенных обстоятельствах.

54.4. Настройка ресурсов

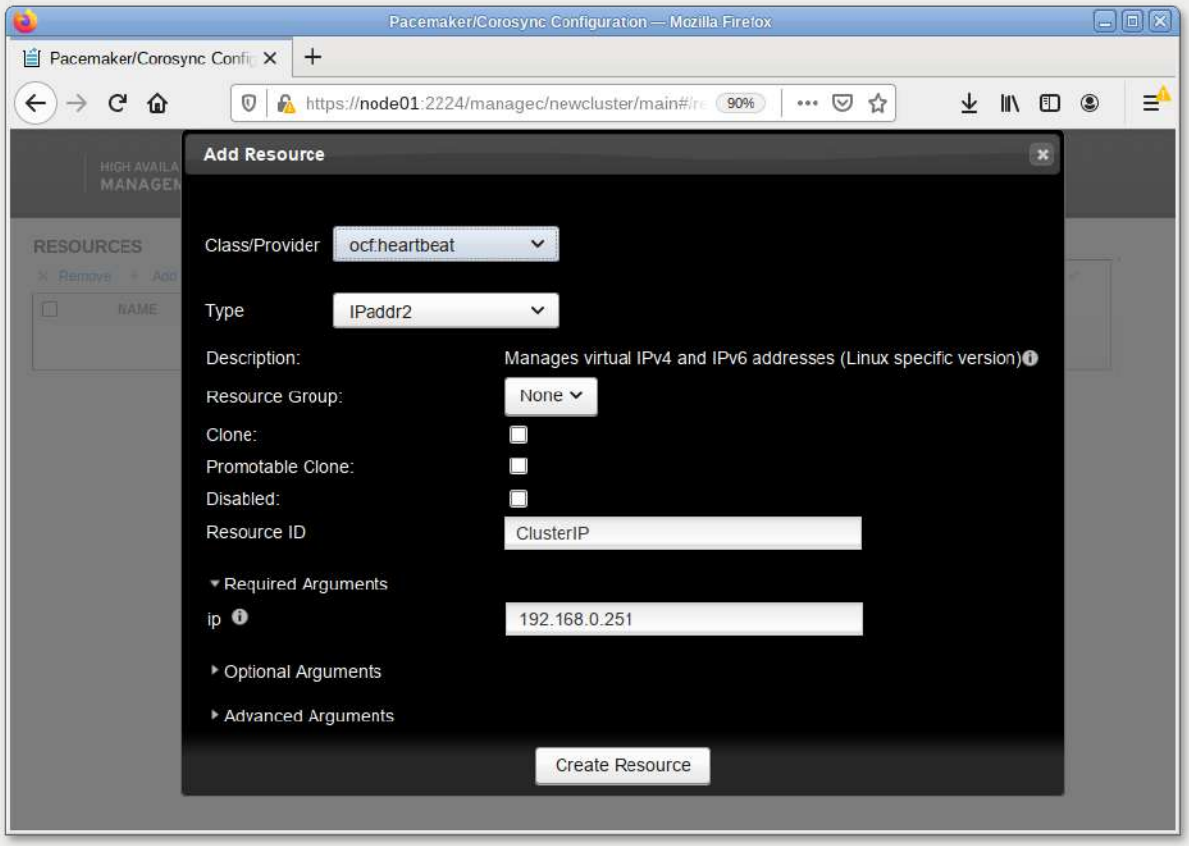
Настроим ресурс, который будет управлять виртуальным IP-адресом. Этот адрес будет мигрировать между узлами, предоставляя одну точку входа к ресурсам, заставляя работать несколько узлов как одно целое устройство для сервисов.

Команда создания ресурса виртуального IP-адреса с именем ClusterIP с использованием алгоритма ресурсов ocf (каждые 20 секунд производить мониторинг работы, в случае выхода из строя узла необходимо виртуальный IP переключить на другой узел):

```
# pcs resource create ClusterIP ocf:heartbeat:IPaddr2 ip=192.168.0.251
cidr_netmask=24 op monitor interval=20s
```

Примечание

Для того чтобы добавить ресурс в веб-интерфейсе, необходимо перейти на вкладку **RESOURCES**, нажать кнопку **Add** и задать параметры ресурса:



Список доступных стандартов ресурсов:

```
# pcs resource standards
lsb
ocf
service
systemd
```

Список доступных поставщиков сценариев ресурсов OCF:

```
# pcs resource providers
heartbeat
pacemaker
redhat
```

Список всех агентов ресурсов, доступных для определённого поставщика OCF:

```
# pcs resource agents ocf:heartbeat
aliyun-vpc-move-ip
anything
AoEtarget
apache
asterisk
```

```
…
Xinetd
zabbixserver
ZFS
```

Статус кластера, с добавленным ресурсом:

```
# pcs status
Cluster name: newcluster
Cluster Summary:
* Stack: corosync
* Current DC: node02 (version 2.0.3-alt2-4b1f869f0) - partition with quorum
* Last updated: Thu Jan 28 13:47:39 2021
* Last change:  Thu Jan 28 13:47:22 2021 by root via cibadmin on node01
* 3 nodes configured
* 1 resource instance configured

Node List:
* Online: [ node01 node02 node03 ]

Full List of Resources:
* ClusterIP   (ocf::heartbeat:IPaddr2):    Started node01

Daemon Status:
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
```

Если остановить кластер на узле node01:

```
# pcs cluster stop node01
node01: Stopping Cluster (pacemaker)...
node01: Stopping Cluster (corosync)...
```

ClusterIP начнёт работать на node02 (переключение произойдёт автоматически). Проверка статуса на узле node02:

```
# pcs status
Cluster Summary:
* Stack: corosync
* Current DC: node02 (version 2.0.3-alt2-4b1f869f0) - partition with quorum
* Last updated: Thu Jan 28 15:02:02 2021
* Last change:  Thu Jan 28 13:48:12 2021 by root via cibadmin on node01
* 3 nodes configured
* 1 resource instance configured

Node List:
* Online: [ node02 node03 ]
* OFFLINE: [ node01 ]

Full List of Resources:
* ClusterIP   (ocf::heartbeat:IPaddr2):    Started node02

Daemon Status:
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
```

Глава 55. OpenUDS

OpenUDS это многоплатформенный брокер подключений для создания и управления виртуальными рабочими местами и приложениями.

Основные компоненты решения VDI на базе OpenUDS:

- OpenUDS Server (openuds-server) — брокер подключений пользователей, а так же интерфейс администратора для настройки;
- SQL Server. Для работы django-приложения, которым является openuds-server, необходим SQL сервер, например mysql или mariadb. SQL Server может быть установлен как на отдельном сервере, так и совместно с openuds-server;
- Платформа для запуска клиентских окружений и приложений. OpenUDS совместима со множеством систем виртуализации: PVE, OpenNebula, oVirt, OpenStack. Так же возможно использование с отдельным сервером без виртуализации (аналог терминального решения);
- OpenUDS Client (openuds-client) — клиентское приложение для подключения к брокеру соединений и дальнейшего получения доступа к виртуальному рабочему окружению;
- OpenUDS Tunnel (openuds-tunnel) — решение для туннелирования обращений от клиента к виртуальному рабочему окружению. OpenUDS Tunnel предназначен для предоставления доступа из недоверенных сегментов сети, например из сети Интернет. Устанавливается на отдельный сервер;
- OpenUDS Actor (openuds-actor) — ПО для гостевых виртуальных машин, реализует связку виртуальной машины и брокера соединений.

55.1. Установка

55.1.1. Установка mysql/mariadb

Установить MySQL (MariaDB):

```
# apt-get install mariadb
```

Запустить сервер mariadb и добавить его в автозагрузку:

```
# systemctl enable --now mariadb.service
```

Задать пароль root для mysql и настройки безопасности:

```
# mysql_secure_installation
```

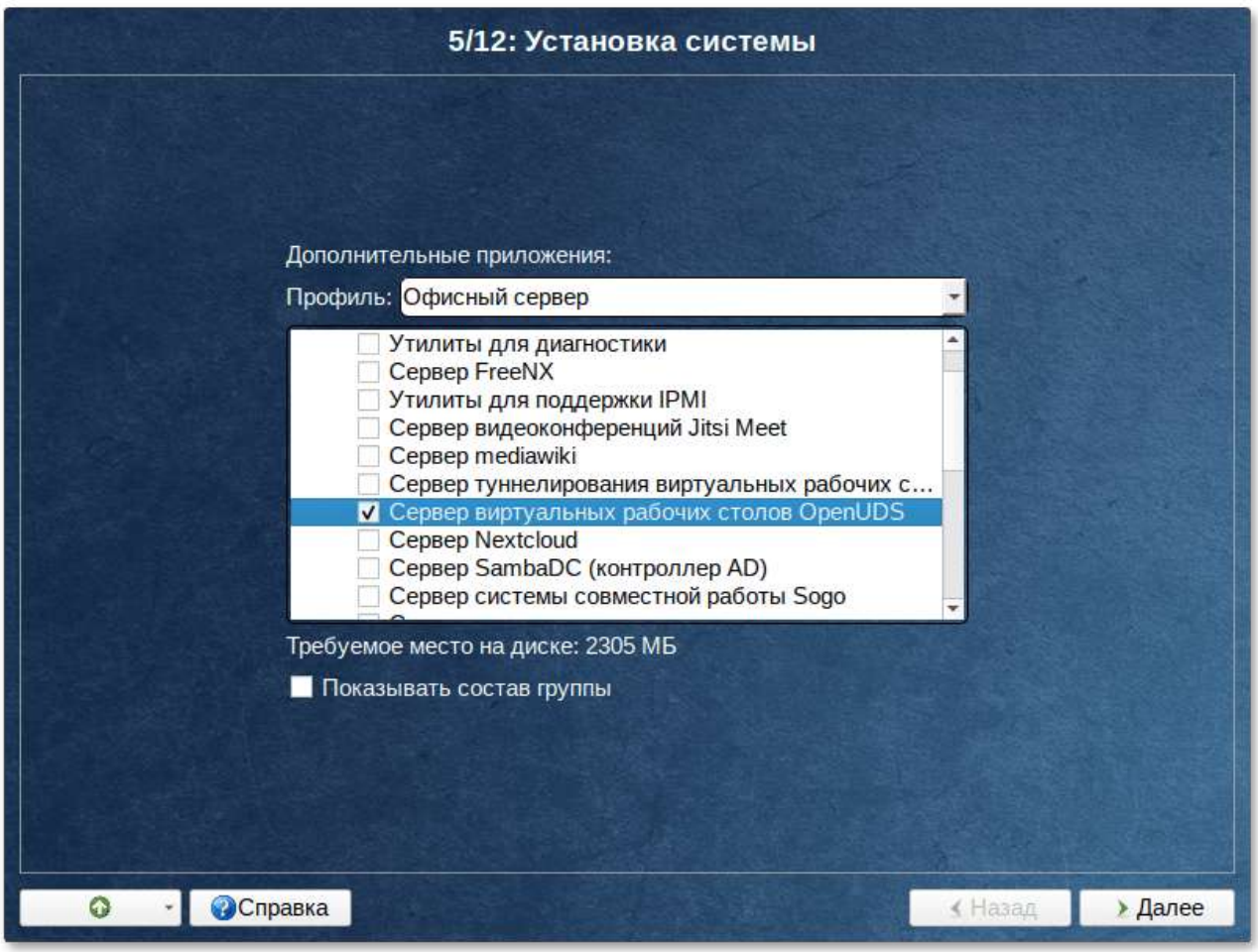
Создать базу данных dbuds, пользователя базы данных dbuds с паролем password и предоставить ему привилегии в базе данных dbuds:

```
$ mysql -u root -p
Enter password:

MariaDB> CREATE DATABASE dbuds CHARACTER SET utf8 COLLATE utf8_general_ci;
MariaDB> CREATE USER 'dbuds'@'%' IDENTIFIED BY 'password'
MariaDB> GRANT ALL PRIVILEGES ON dbuds.* TO 'dbuds'@'%';
MariaDB> FLUSH PRIVILEGES;
MariaDB> exit;
```

55.1.2. Установка OpenUDS Server

OpenUDS Server можно установить при установке системы, выбрав для установки пункт **Сервер виртуальных рабочих столов OpenUDS** (подробнее описано в главе Установка системы).



При этом будут установлены:

- openuds-server — django приложение;
- gunicorn — сервер приложений (обеспечивает запуск django как стандартного WSGI приложения);
- nginx — http-сервер, используется в качестве reverse-proxy для доступа к django приложению, запущенному с помощью gunicorn.

Примечание

В уже установленной системе можно установить пакет openuds-server-nginx:

```
# apt-get install openuds-server-nginx
```

Настройка OpenUDS Server:

- отредактировать файл **/etc/openuds/settings.py**, указав корректные данные для подключения к SQL серверу:

```
DATABASES = {
    'default': {
        'ENGINE': 'django.db.backends.mysql',
        'OPTIONS': {
            'isolation_level': 'read committed',
        },
        'NAME': 'dbuds',
        'USER': 'dbuds',
        'PASSWORD': 'password',
        'HOST': 'localhost',
        'PORT': '3306',
    }
}
```

- заполнить базу данных начальными данными:

```
# su -s /bin/bash - openuds
$ cd /usr/share/openuds
$ python3 manage.py migrate
```

- запустить gunicorn:

```
# systemctl enable --now openuds-web.service
```

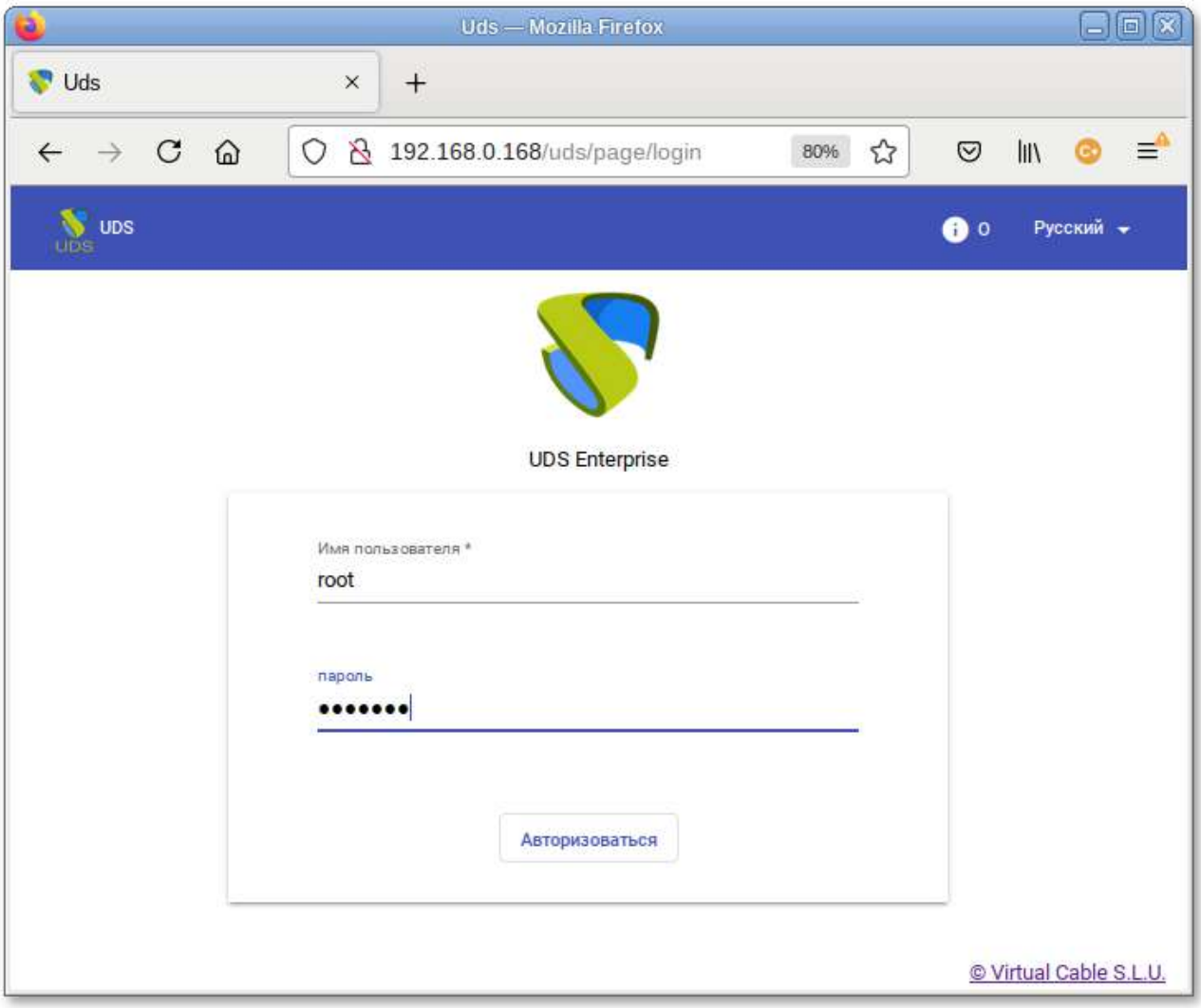
- запустить nginx:

```
# ln -s ../sites-available.d/openuds.conf /etc/nginx/sites-enabled.d/
openuds.conf
# systemctl enable --now nginx.service
```

- запустить менеджер задач OpenUDS:

```
# systemctl enable --now openuds-taskmanager.service
```

Веб-интерфейс OpenUDS будет доступен по адресу https://адрес-сервера/:



Примечание

Имя/пароль по умолчанию: root/udsmam0.

Примечание

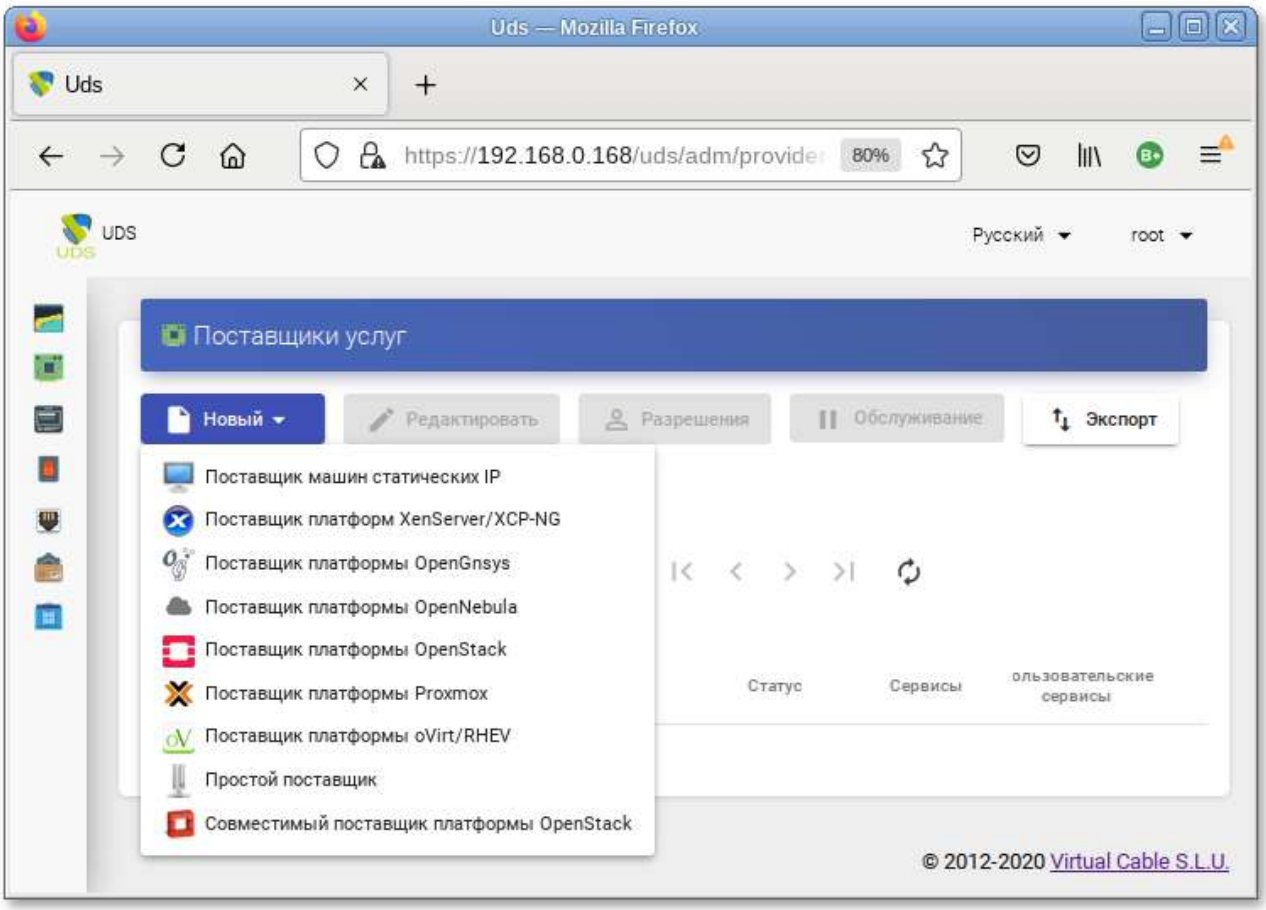
Для получения доступа к панели администрирования OpenUDS, следует в меню пользователя выбрать пункт **Панель управления**:

55.2. Настройка OpenUDS

55.2.1. Поставщики услуг

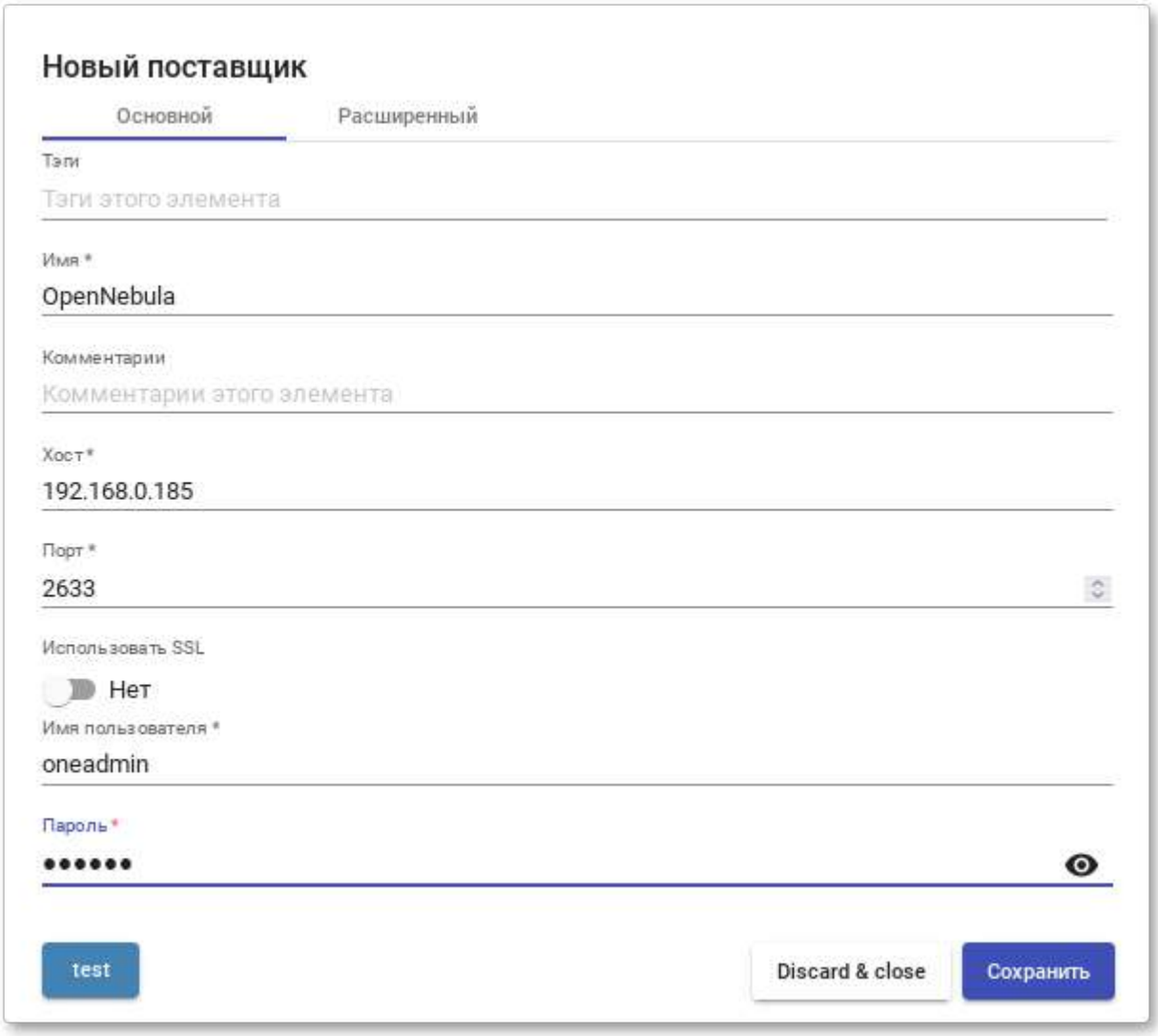
В разделе **Услуги** (**Services**) подключить один из поставщиков («Service providers»):

- **Поставщик платформы Proxmox** (**PVE Platform Provider**);
- **Поставщик платформы OpenNebula** (**OpenNebula Platform Provider**);
- Отдельный сервер без виртуализации: **Поставщик машин статических IP** (**Static IP Machine Provider**).



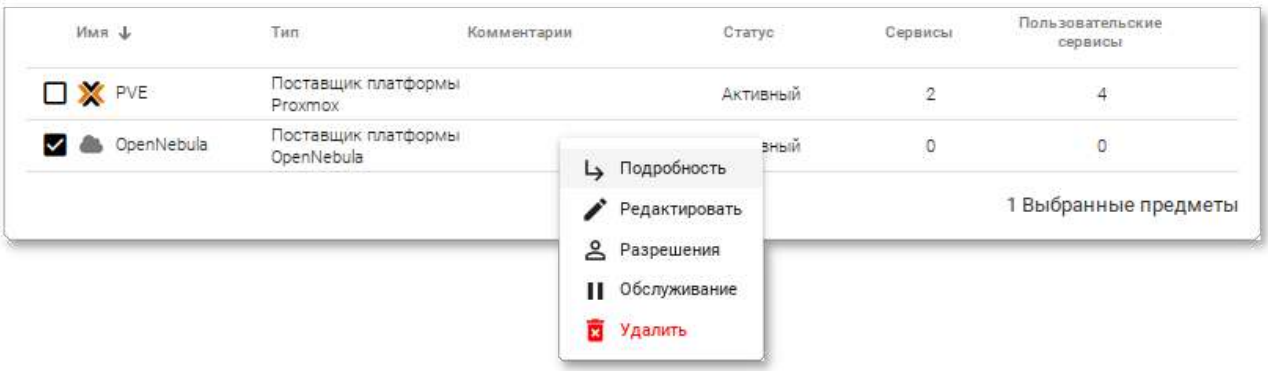
55.2.1.1. OpenNebula

Минимальные параметры для настройки **Поставщик платформы OpenNebula**: название, IP-адрес сервера OpenNebula (поле **Хост**), порт подключения, имя пользователя (с правами администратора) и пароль.



Используя кнопку **`test`**, можно убедиться, что соединение установлено правильно.

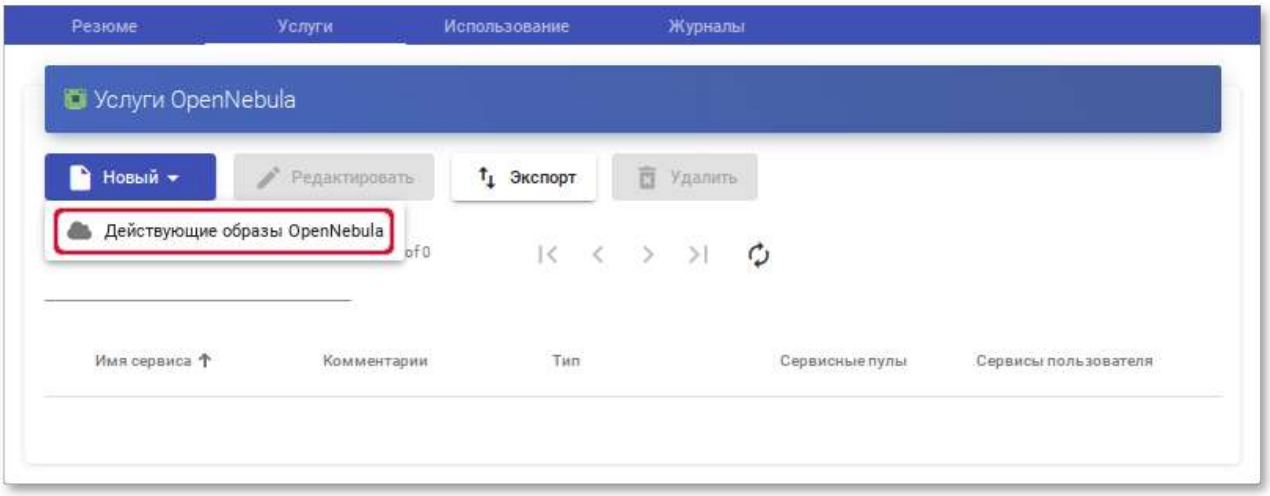
После интеграции платформы OpenNebula в OpenUDS необходимо создать базовую службу типа «Действующие образы OpenNebula» («OpenNebula Live Images»). Для этого дважды щелкнуть мышью по строке созданного поставщика услуг или в контекстном меню поставщика выбрать пункт **Подробность** (**Detail**):



Примечание

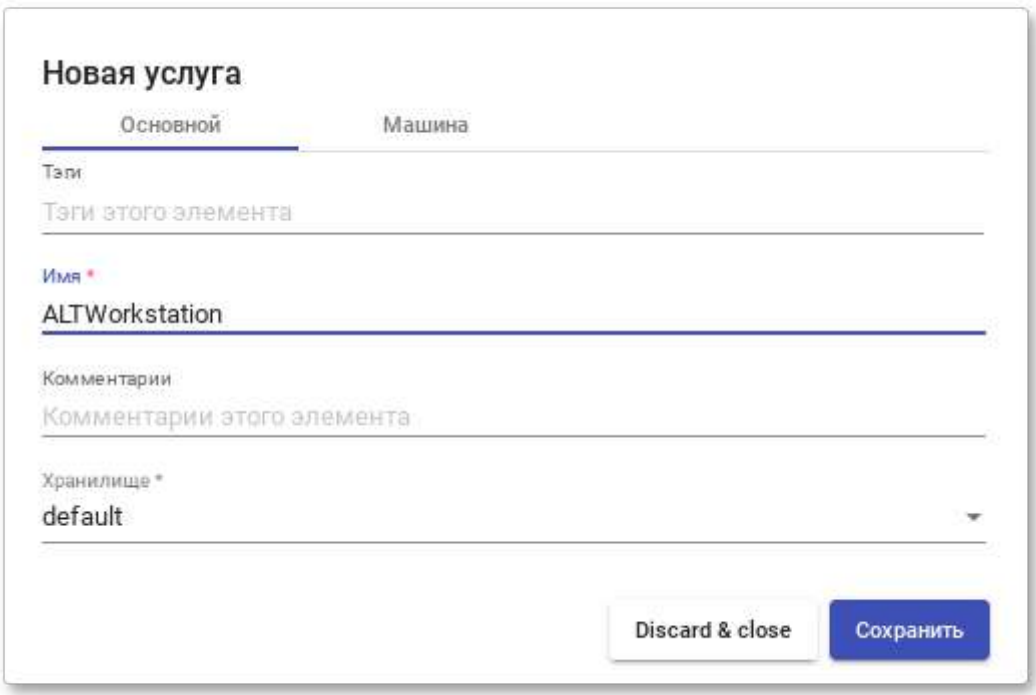
Выбрав пункт **Обслуживание** (**Maintenance**), можно приостановить все операции, выполняемые сервером OpenUDS для данного поставщика услуг. Поставщик услуг рекомендуется переводить в режим обслуживания в случаях, когда связь с этим поставщиком была потеряна или запланирован перерыв в обслуживании.

На вкладке **Услуги** (**Services**) нажать кнопку **Новый** → **Действующие образы OpenNebula**:



Заполнить минимальные параметры конфигурации:

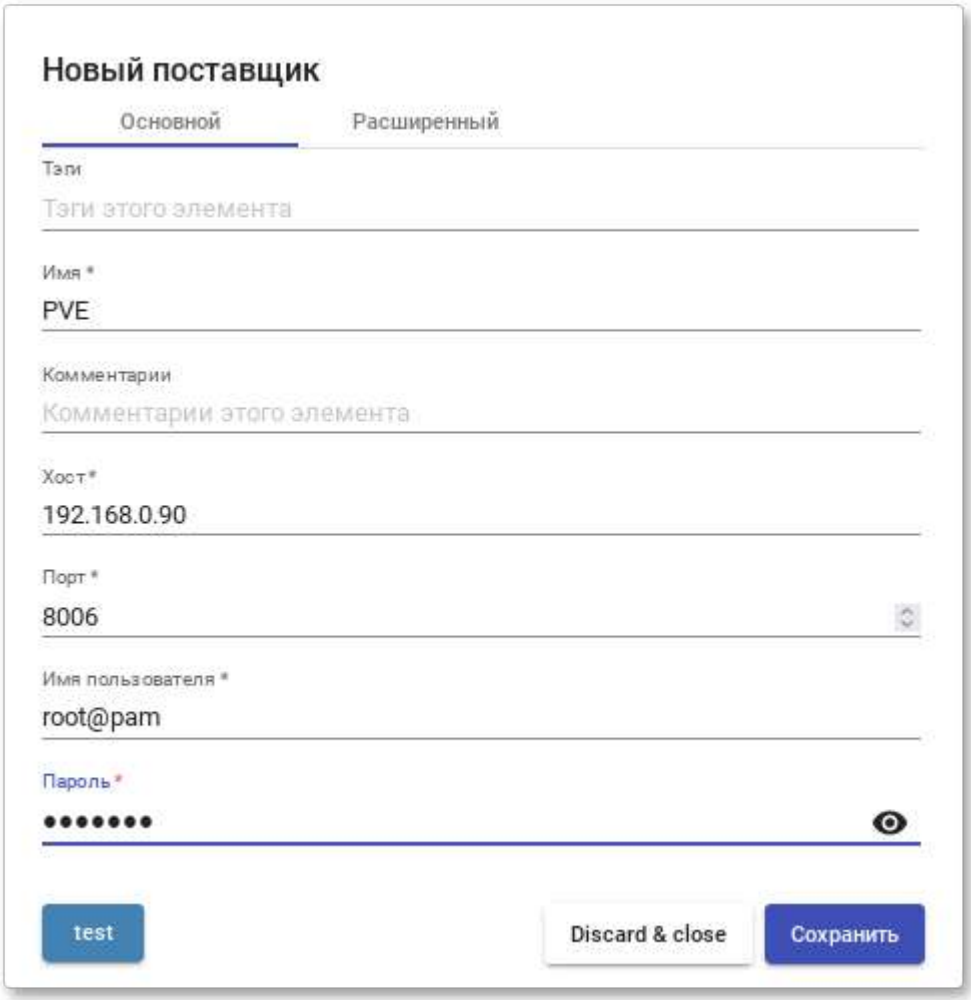
- Вкладка **Основной** (**Main**):
  - **Имя** — название службы;
  - **Хранилище** — место, где будут храниться сгенерированные виртуальные рабочие столы.



- Вкладка **Машина** (**Machine**):
  - **Базовая машина** — шаблон ВМ, используемый системой OpenUDS для развертывания виртуальных рабочих столов (см. Подготовка шаблона виртуальной машины);
  - **Имена машин** — базовое название для клонов с этой машины (например, Desk-work-);
  - **Длина имени** — количество цифр счетчика, прикрепленного к базовому имени рабочих столов (например, если **Длина имени** = 3, названия сгенерированных рабочих столов будут: Desk-work-000, Desk-work-001 ... Desk-work-999).

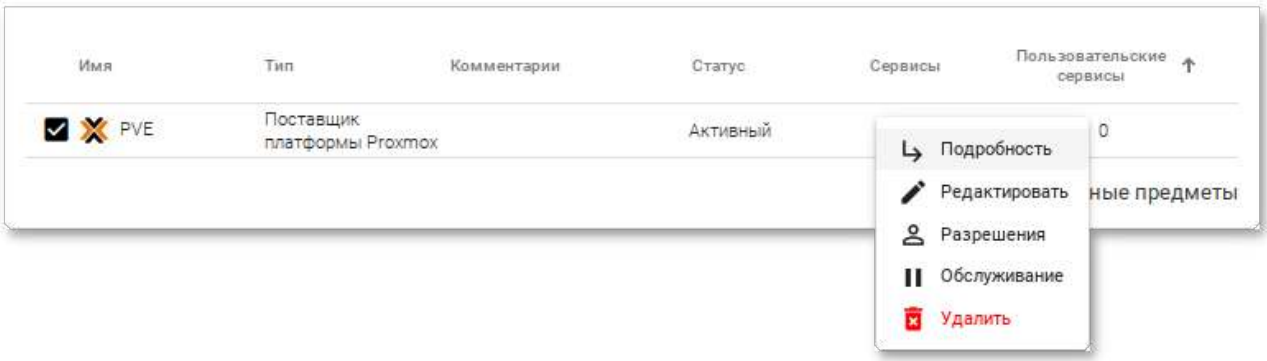
55.2.1.2. PVE

Минимальные параметры для настройки **Поставщика платформы Proxmox**: название поставщика, IP-адрес/имя сервера или кластера PVE (поле **Хост**), порт подключения, имя пользователя с достаточными привилегиями в PVE (в формате пользователь@аутентификатор) и пароль.



Используя кнопку **`test`**, можно убедиться, что соединение установлено правильно.

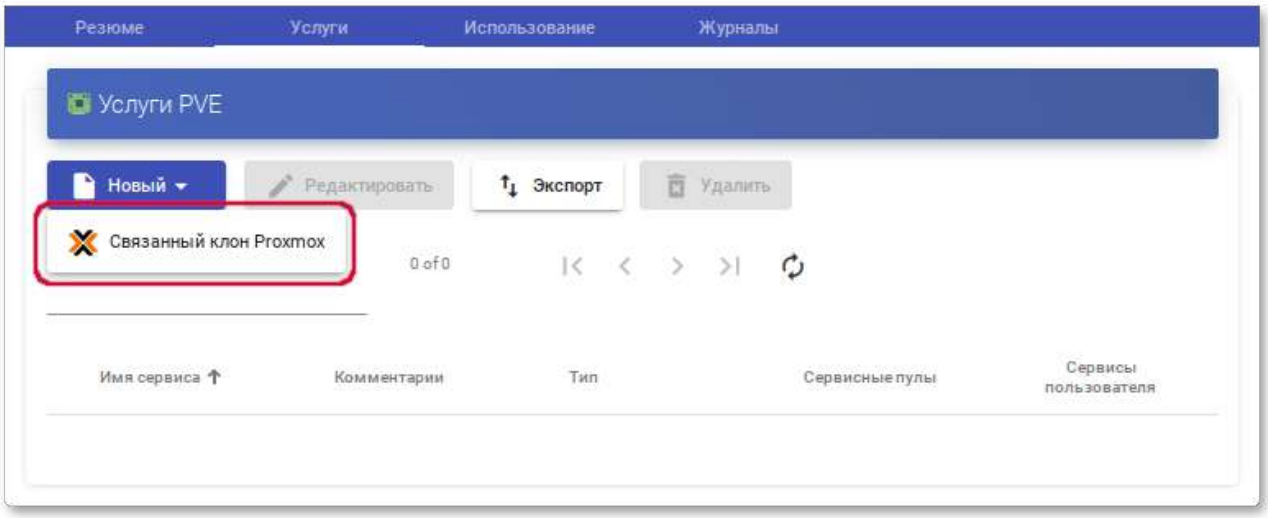
После интеграции платформы PVE в OpenUDS необходимо создать базовую службу типа «Связанный клон Proxmox» («Proxmox Linked Clone»). Для этого дважды щелкнуть мышью по строке созданного поставщика услуг или в контекстном меню поставщика выбрать пункт **Подробность** (**Detail**):



Примечание

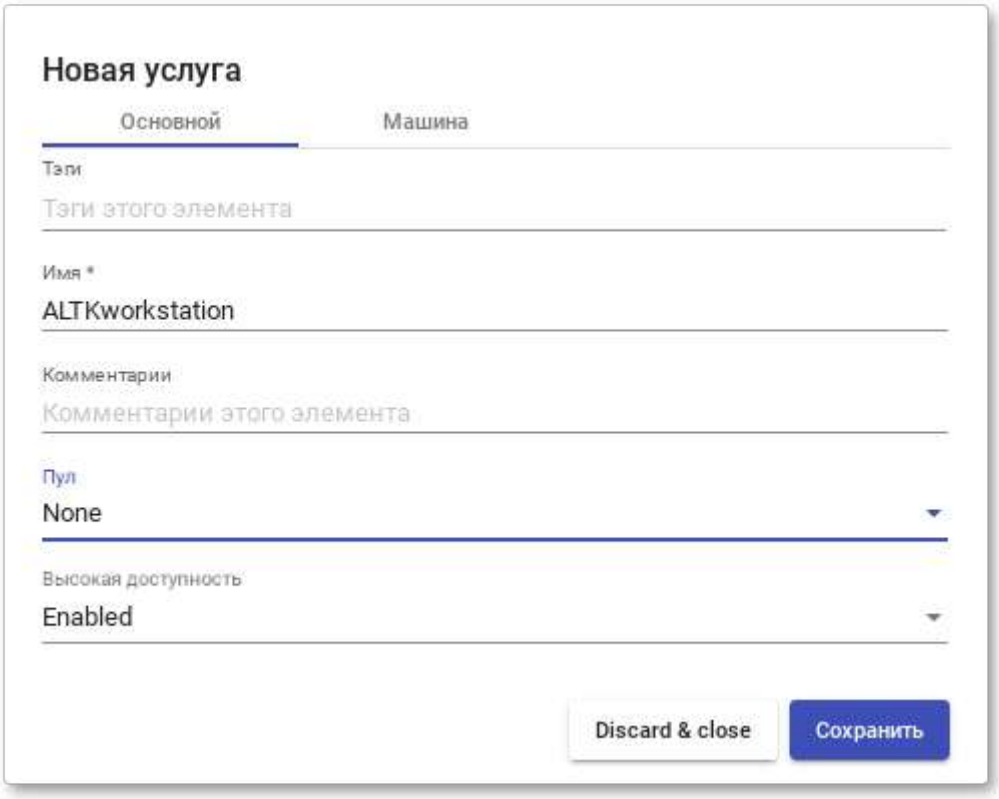
Выбрав пункт **Обслуживание** (**Maintenance**), можно приостановить все операции, выполняемые сервером OpenUDS для данного поставщика услуг. Поставщик услуг рекомендуется переводить в режим обслуживания в случаях, когда связь с этим поставщиком была потеряна или запланирован перерыв в обслуживании.

На вкладке **Услуги** (**Services**) нажать кнопку **Новый** → **Связанный клон Proxmox**:

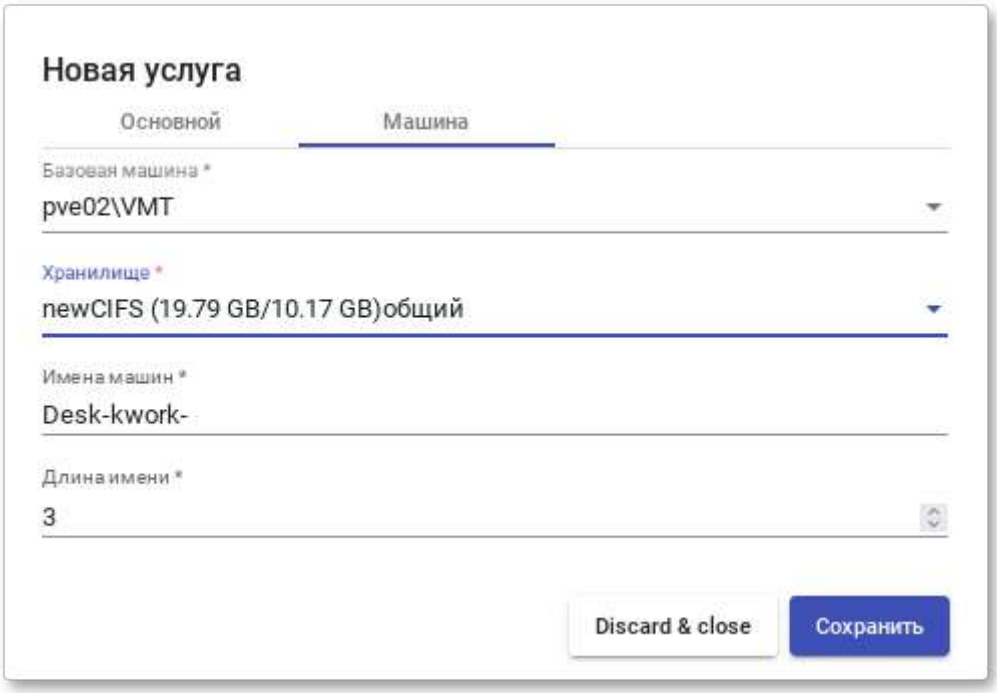


Заполнить минимальные параметры конфигурации:

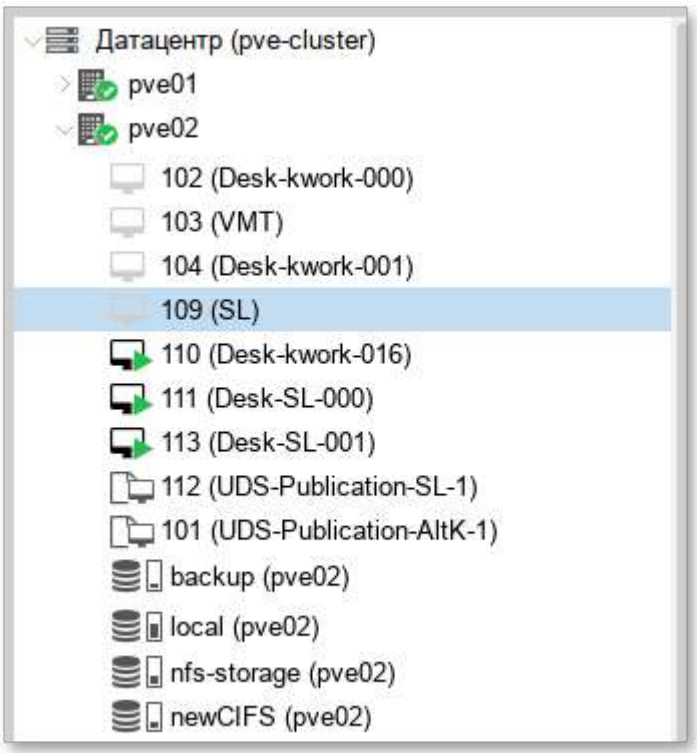
- Вкладка **Основной** (**Main**):
  - **Имя** — название службы;
  - **Пул** — пул, в котором будут находиться ВМ, созданные OpenUDS;
  - **Высокая доступность** — включать созданные ВМ в группу HA PVE.



- Вкладка **Машина** (**Machine**):
  - **Базовая машина** — шаблон ВМ, используемый системой OpenUDS для развертывания виртуальных рабочих столов (см. Подготовка шаблона виртуальной машины);
  - **Хранилище** — место, где будут храниться сгенерированные виртуальные рабочие столы (поддерживаются хранилища, позволяющие создавать «Снимки»);
  - **Имена машин** — базовое название для клонов с этой машины (например, Desk-kwork-);
  - **Длина имени** — количество цифр счетчика, прикрепленного к базовому имени рабочих столов (например, если **Длина имени** = 3, названия сгенерированных рабочих столов будут: Desk-kwork-000, Desk-kwork-001 ... Desk-kwork-999).



После того, как среда OpenUDS будет настроена и будет создан первый «пул услуг», в среде PVE можно будет наблюдать, как разворачиваются рабочие столы. Сначала будет создан шаблон («UDS-Publication-pool_name-publishing-number») — клон ВМ, выбранной при регистрации службы. После завершения процесса создания клона будут созданы рабочие столы («Machine_Name-Name_Length»):

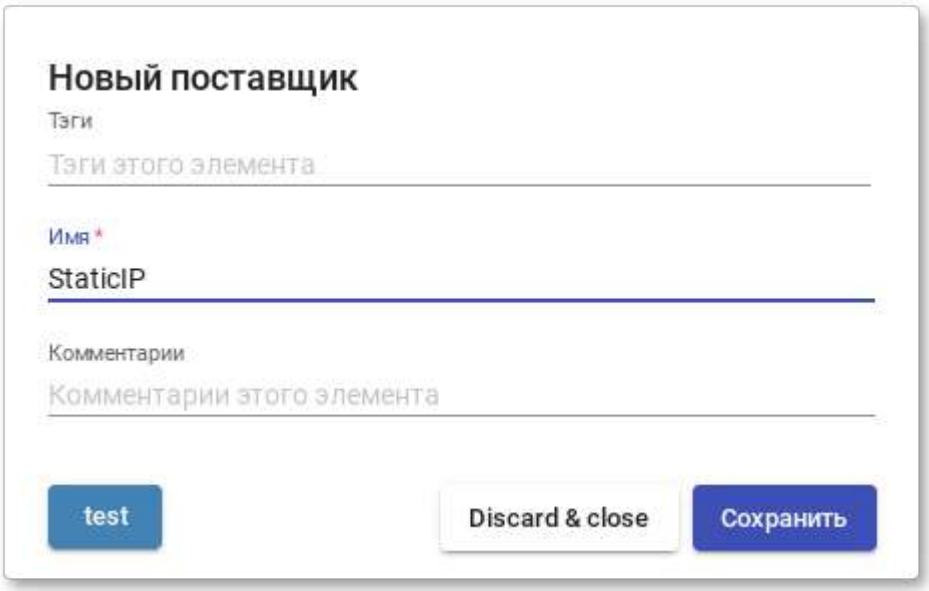


55.2.1.3. Удалённый доступ к отдельному серверу

В OpenUDS есть возможность предоставить доступ к постоянным устройствам (физическим или виртуальным). Доступ к отдельному серверу осуществляется путем назначения IP-адресов пользователям.

Для регистрации поставщика данного типа следует в разделе **Услуги** нажать кнопку **Новый** и выбрать пункт **Поставщик машин статических IP**.

Для настройки **Поставщика машин статических IP** достаточно задать название поставщика.



Для создания базовых услуг **Поставщика машин статических IP** следует дважды щелкнуть мышью по строке созданного поставщика или в контекстном меню поставщика выбрать пункт **Подробность** (**Detail**).

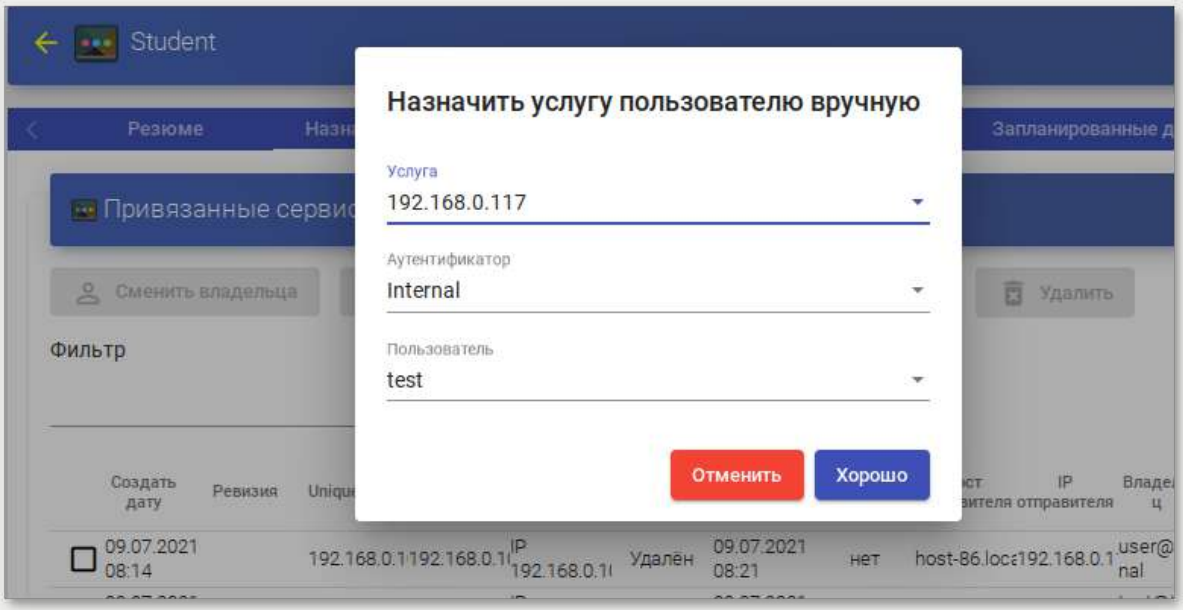
OpenUDS позволяет создавать два типа услуг **Поставщика машин статических IP**.

Статический множественный IP-адрес

Используется для подключения одного пользователя к одному компьютеру. Поддерживается неограниченное количество IP-адресов (можно включить в список все устройства, которые должны быть доступны удалённо). По умолчанию система будет предоставлять доступ к устройствам в порядке очереди (первый пользователь получивший доступ к этому пулу, получает доступ к машине с первым IP-адресом из списка). Также можно настроить выборочное распределение, чтобы определённому пользователю назначался определенный компьютер (IP-адрес).

Примечание

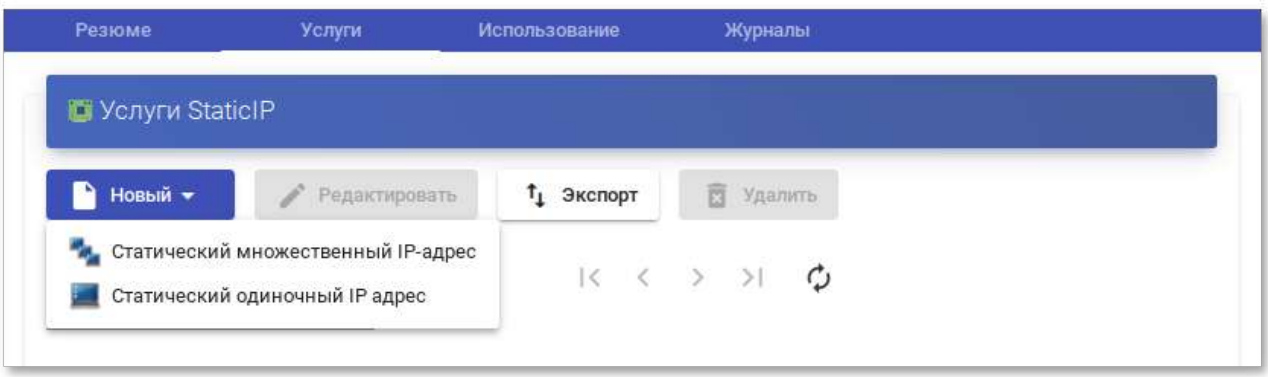
Для настройки привязки конкретного пользователя к конкретному IP необходимо в разделе **Пулы услуг** (см. раздел Пулы услуг) для созданной услуги на вкладке **Назначенные услуги** нажать кнопку **Назначить услугу** и задать привязку пользователя устройству:



Статический одиночный IP-адрес

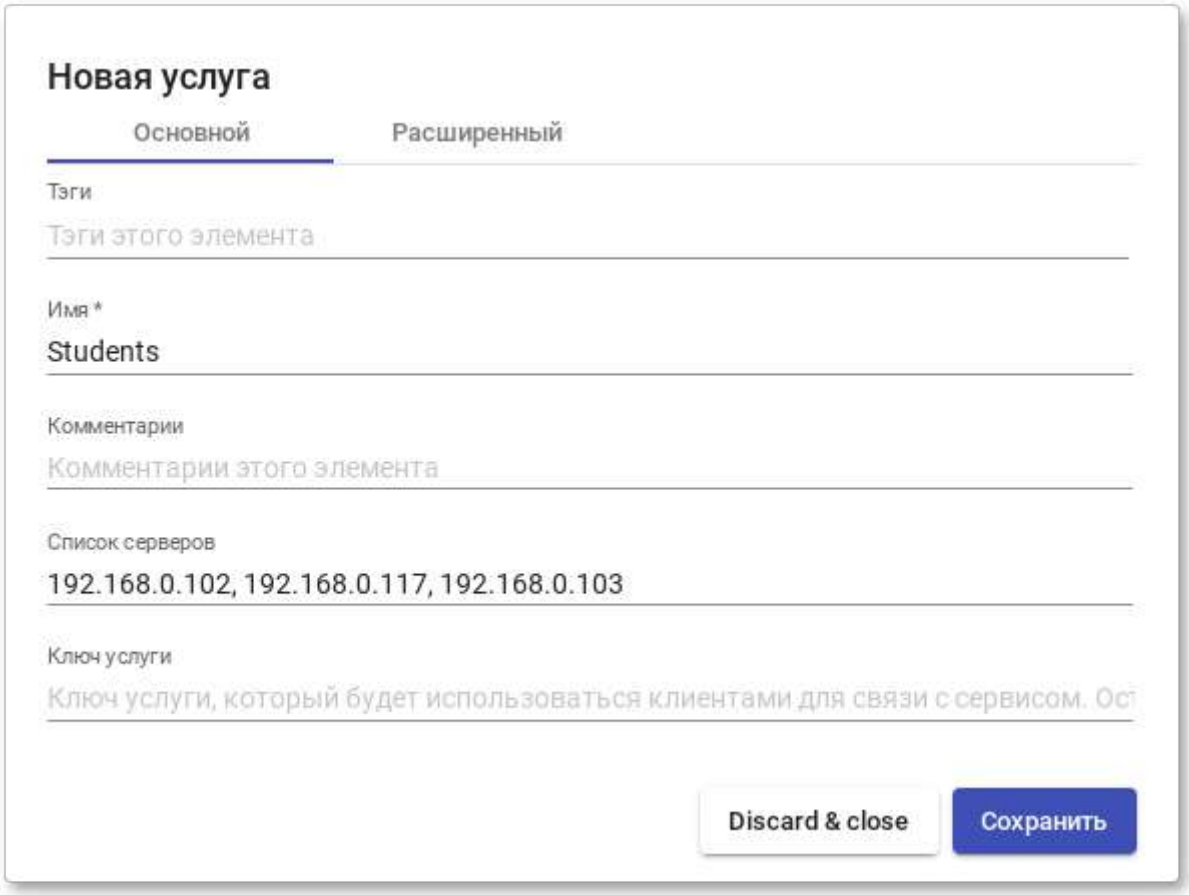
Используется для подключения нескольких пользователей к одному компьютеру. При обращении каждого нового пользователя будет запускаться новый сеанс.

Для создания новой услуги **Поставщика машин статических IP** необходимо на вкладке **Услуги** (**Services**) нажать кнопку **Новый** → **Статический множественный IP-адрес** или **Новый** → **Статический одиночный IP-адрес**:

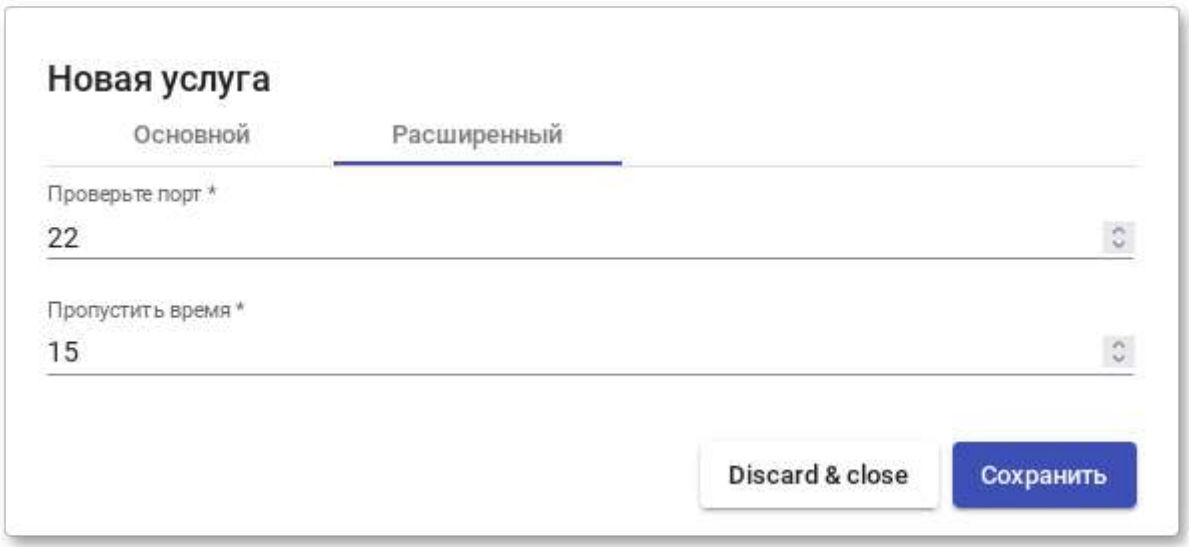


Параметры конфигурации для услуги **Статический множественный IP-адрес**:

- Вкладка **Основной**:
  - **Имя** — название службы;
  - **Список серверов** — один или несколько IP-адресов машин, к которым будет осуществляться доступ (машины должны быть включены и настроены см. Подготовка шаблона виртуальной машины).



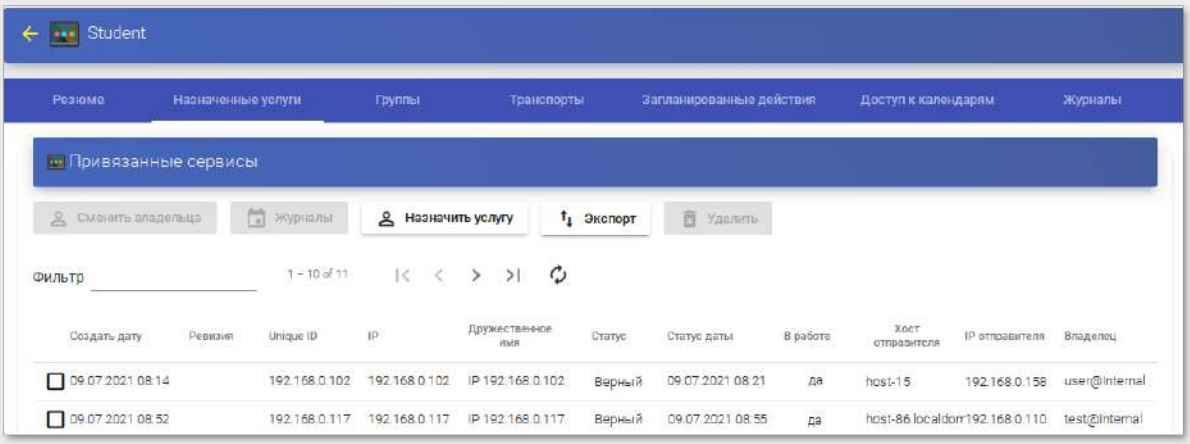
- Вкладка **Расширенный**:
  - **Проверить порт** — порт, по которому система может проверить, доступен ли компьютер. Если компьютер не доступен, система автоматически предоставит следующее устройство в списке. 0 — не проверять доступность компьютера;
  - **Пропустить время** — период, в течении которого не будет проверяться доступность недоступной машины.



Примечание

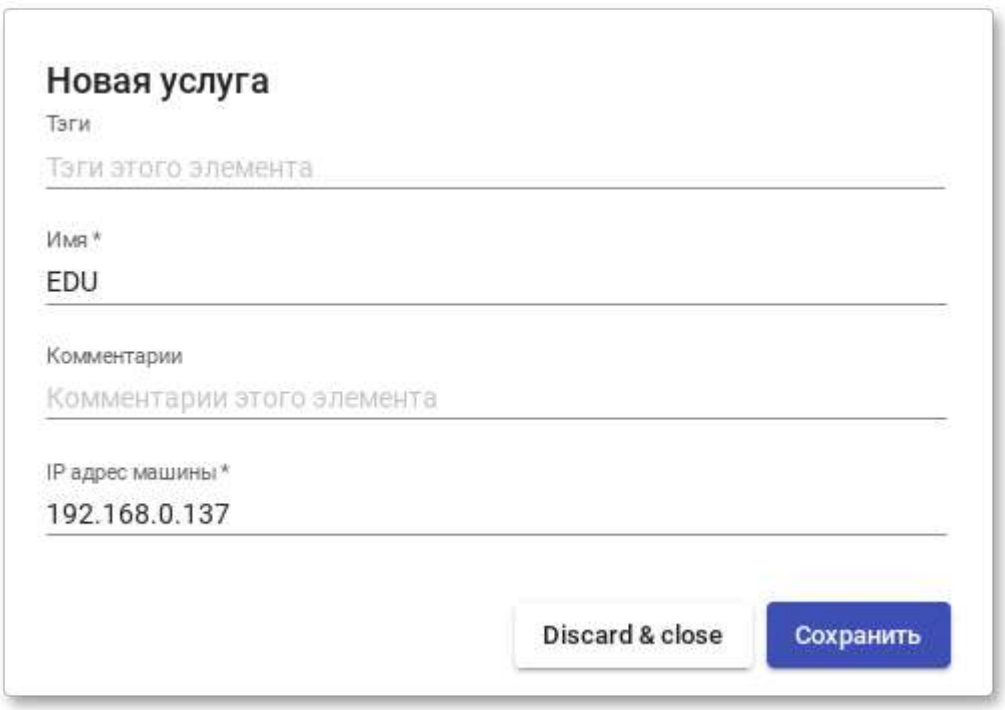
Назначение IP-адресов будет осуществляться в порядке доступа, то есть первому пользователю, который обращается к службе, будет назначен первый IP-адрес в списке. IP-адрес будет привязан пользователю, даже после выхода пользователя из системы (пока администратор не удалит привязку вручную).

Просмотреть/изменить привязанные сеансы можно в разделе **Пулы услуг** (см. раздел Пулы услуг) на вкладке **Назначенные услуги**:



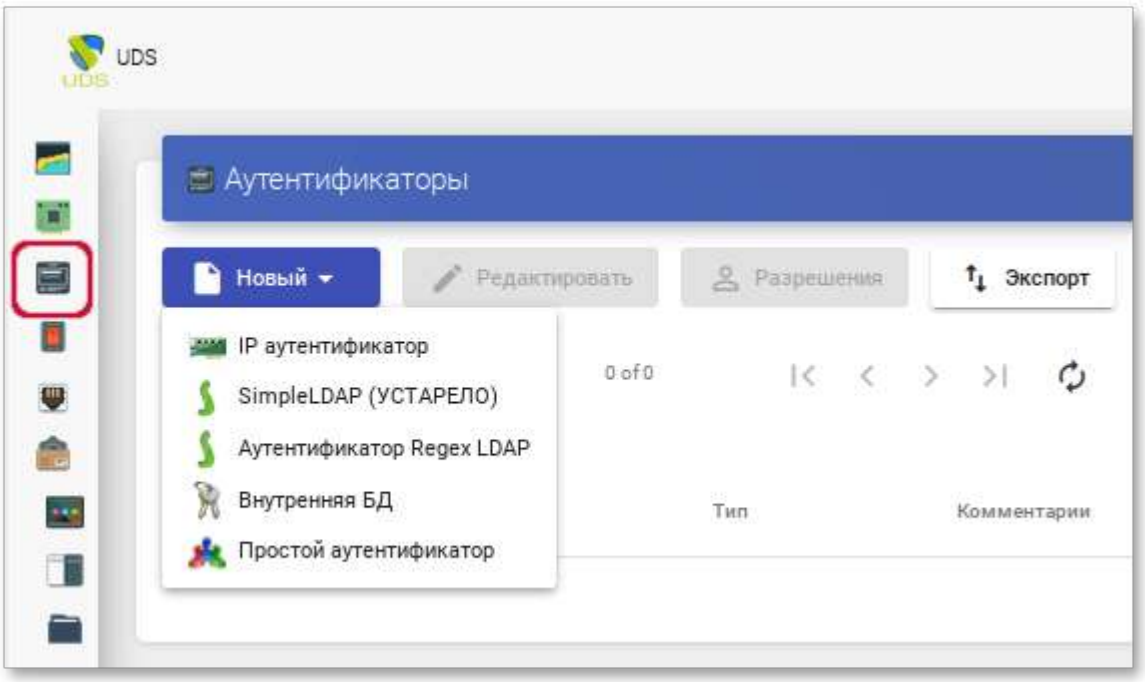
Параметры конфигурации для услуги **Статический одиночный IP-адрес**:

- **Имя** — название службы;
- **IP-адрес машины** — IP-адрес машины, к которой будет осуществляться доступ (машина должна быть включена и настроена см. Подготовка шаблона виртуальной машины).



55.2.2. Настройка аутентификации пользователей

Для настройки аутентификации в разделе **Аутентификаторы (Autentificators)** необходимо выбрать тип аутентификации пользователей. Можно выбрать как внешние источники (Active Directory, OpenLDAP и т.д.), так и внутренние (внутренняя база данных, IP-аутентификация):

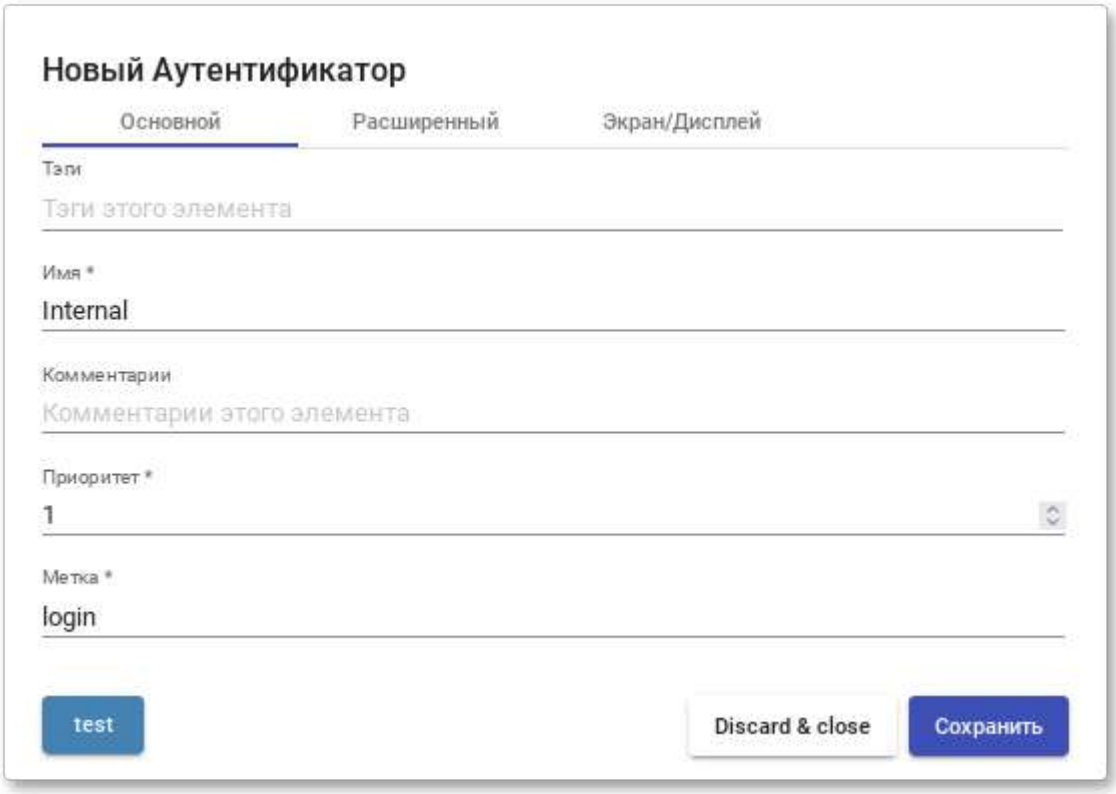


55.2.2.1. Внутренняя БД

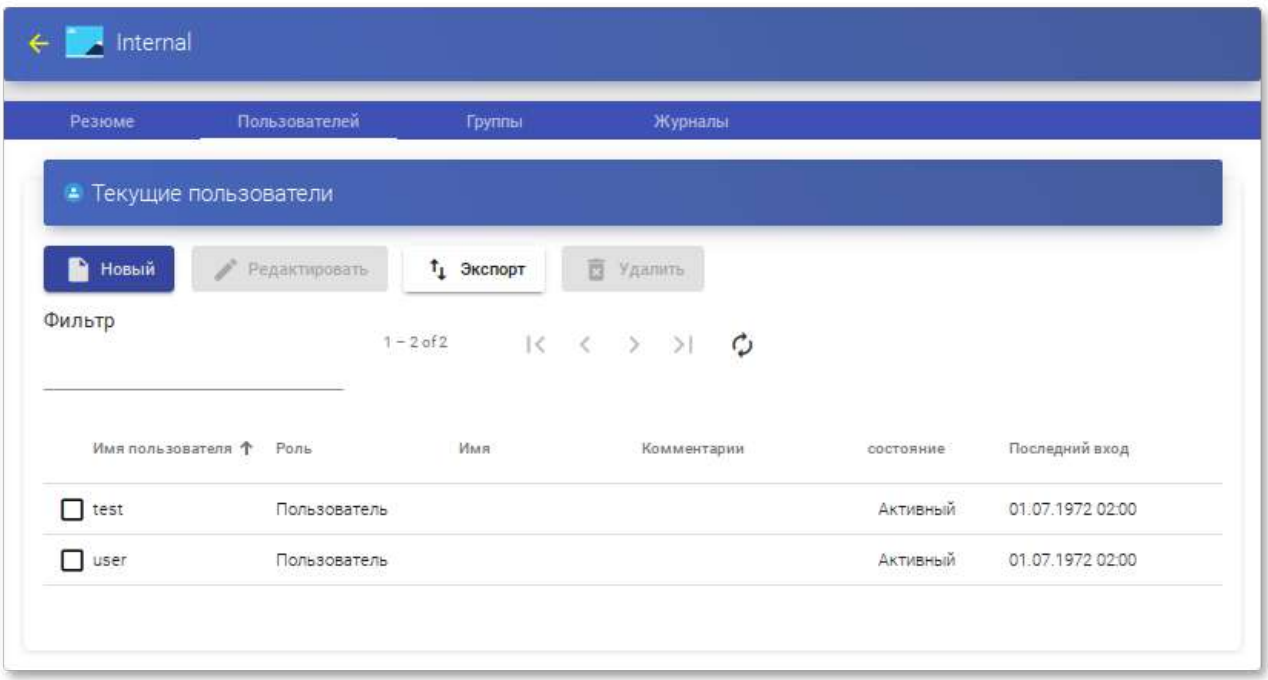
При аутентификации **Внутренняя БД** данные пользователей и групп хранятся в базе данных, к которой подключен сервер OpenUDS.

Для создания аутентификации типа **Внутренняя БД** в разделе **Аутентификаторы** следует нажать кнопку: **Новый → Внутренняя БД**.

Минимальные параметры конфигурации (вкладка **Основной**): имя аутентификатора, приоритет и метка.



После того, как аутентификатор типа «Внутренняя БД» создан, нужно зарегистрировать пользователей и группы пользователей. Для этого следует выбрать аутентификатор «Внутренняя БД», затем во вкладке **Группы** создать группы пользователей, во вкладке **Пользователи** создать пользователей.



55.2.2.2. Аутентификатор Regex LDAP

Этот аутентификатор позволяет пользователям и группам пользователей, принадлежащих практически любому аутентификатору на основе LDAP, получать доступ к виртуальным рабочим столам и приложениям.

Важно

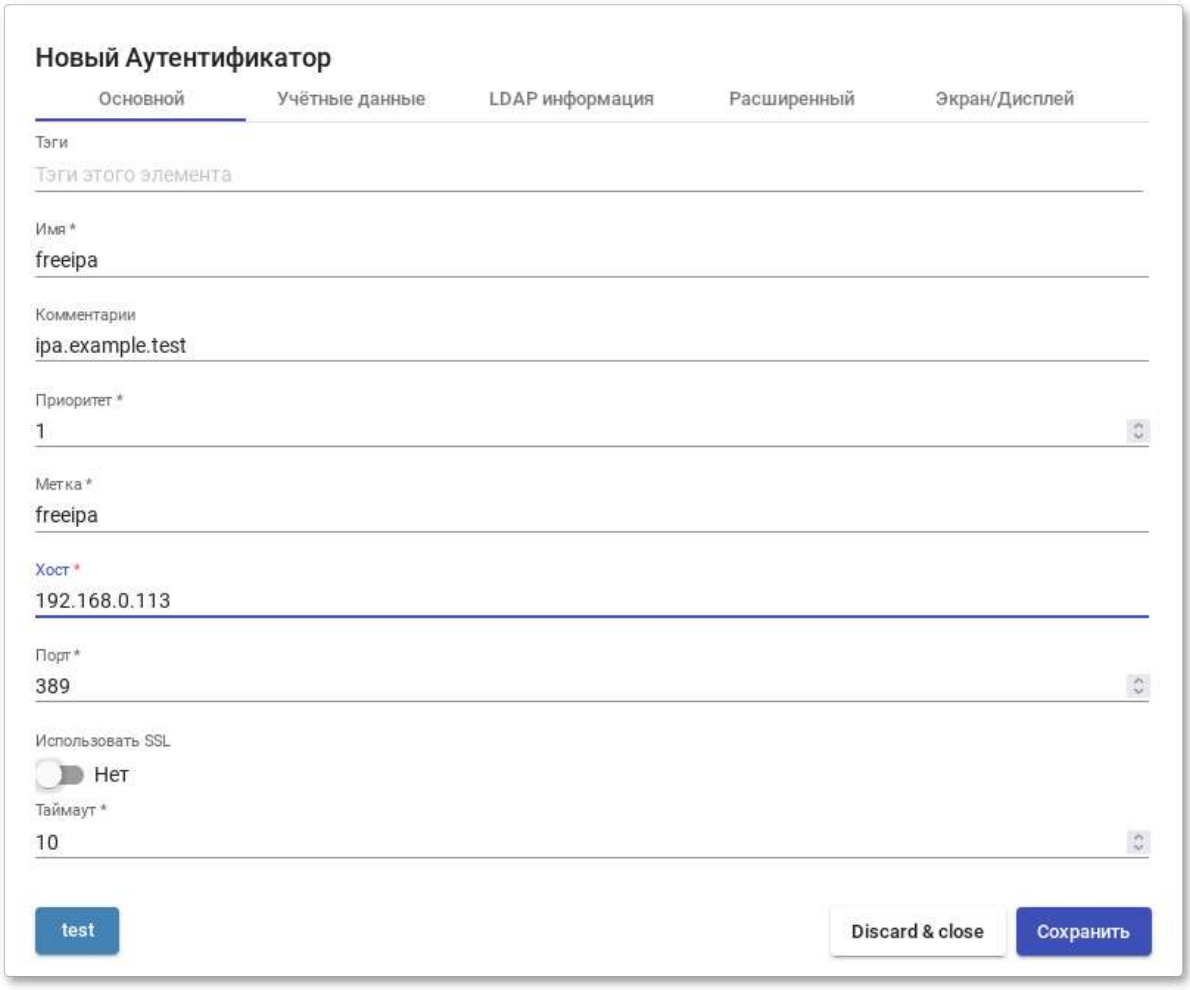
На сервере LDAP должна быть настроена отдельная учётная запись с правами чтения LDAP. От данной учетной записи будет выполняться подключение к серверу каталогов.

55.2.2.2.1. FreeIPA

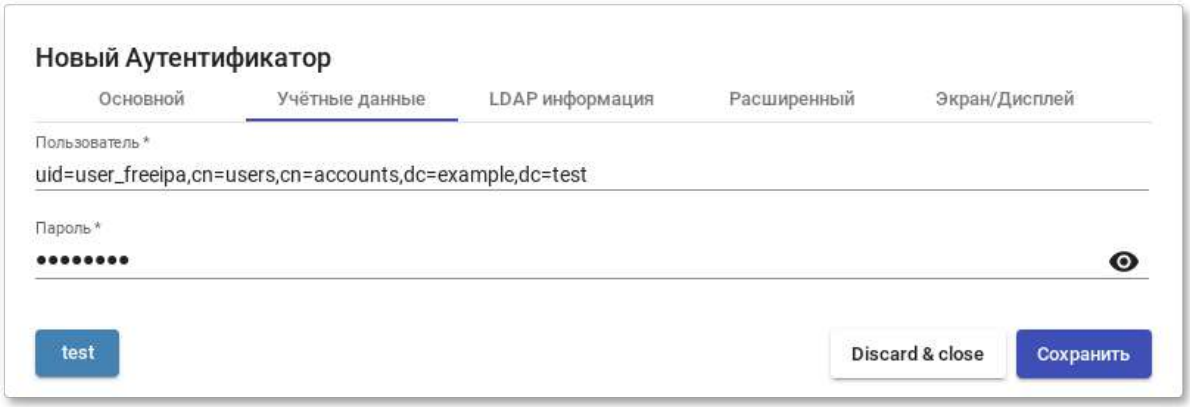
Настройка интеграции с FreeIPA (сервер ipa.example.test):

1. В разделе **Аутентификаторы** нажать кнопку: **Новый → Аутентификатор Regex LDAP**.
2. Заполнить поля первых трёх вкладок.

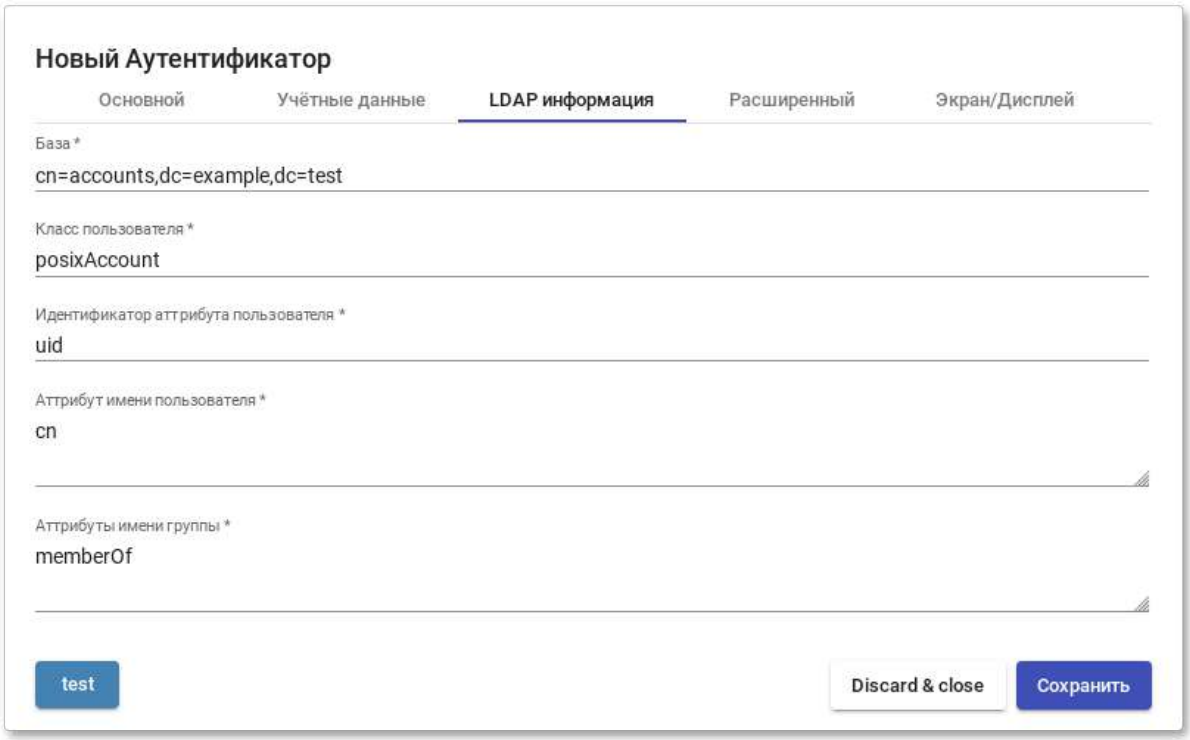
   Вкладка **Основной**: имя аутентификатора, приоритет, метка, IP-адрес FreeIPA-сервера, порт (обычно 389 без ssl, 636 с ssl):



   Вкладка **Учётные данные**: имя пользователя (в формате uid=user_freeipa,cn=users,cn=accounts,dc=example,dc=test) и пароль:



Вкладка **LDAP информация**: общая база пользователей, класс пользователей LDAP, идентификатор атрибута пользователя, атрибут имени пользователя, атрибут имени группы:

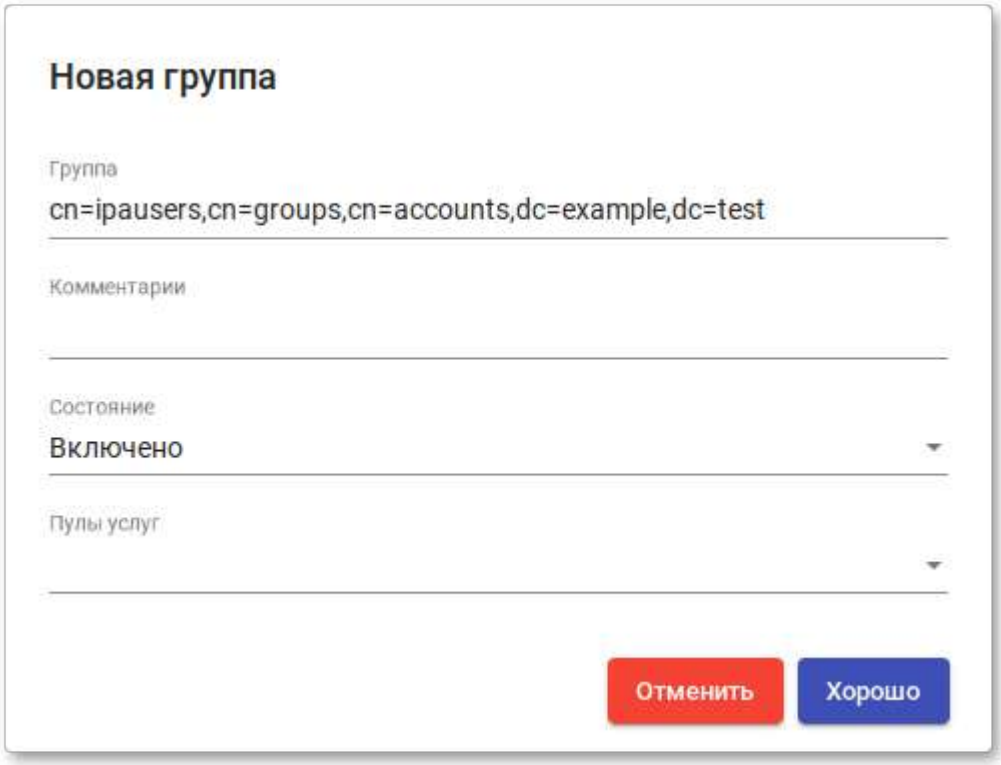


Примечание

Используя кнопку **`test`**, можно проверить соединение с FreeIPA-сервером.

3. Добавить группу LDAP, в которую входят пользователи. Для этого следует выбрать созданный аутентификатор «freeipa», во вкладке **Группы** нажать **Новый → Группа**.

   Заполнить dn существующей группы (для FreeIPA по умолчанию это группа cn=ipausers,cn=groups,cn=accounts,dc=ipa,dc=example,dc=test), можно также указать разрешённые пулы:

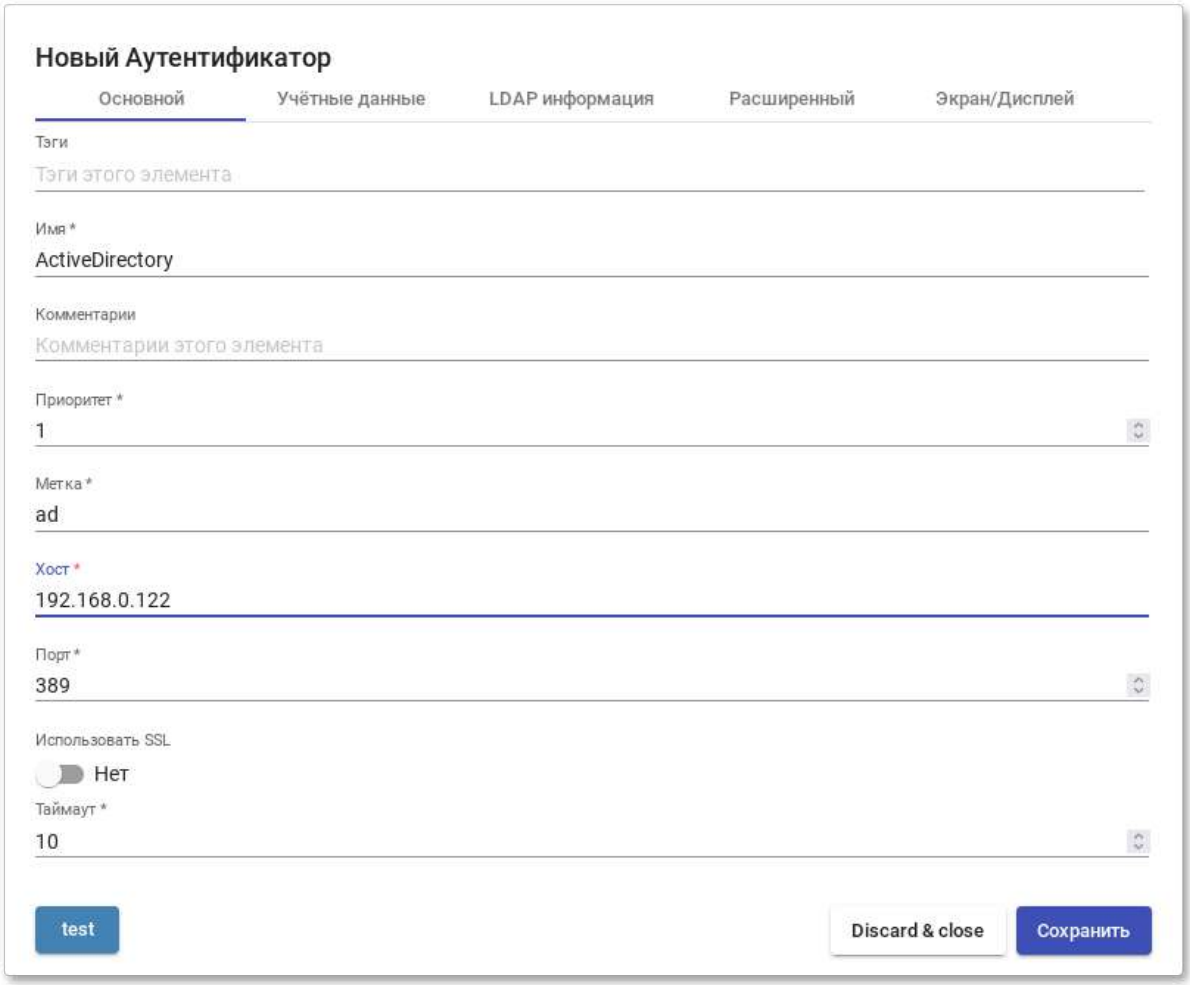


55.2.2.2.2. Active Directory

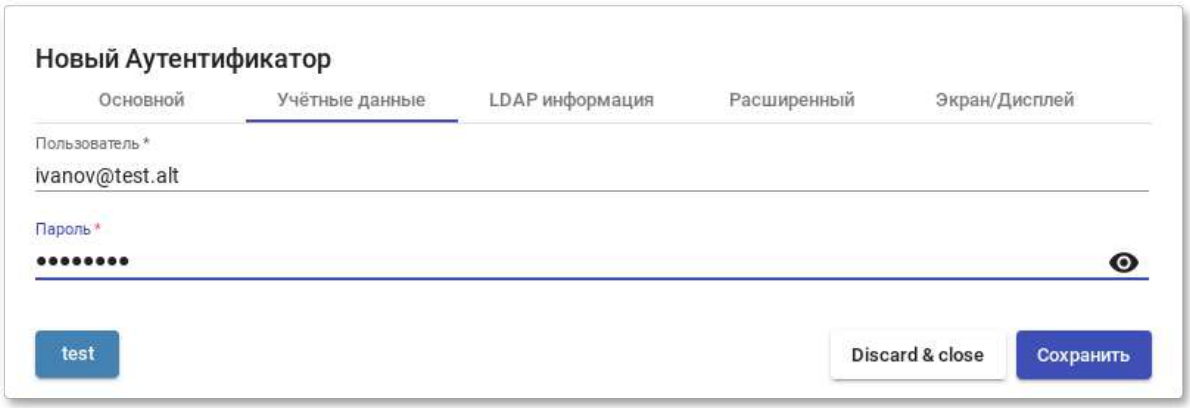
Настройка аутентификации в Active Directory (домен test.alt):

1. В разделе **Аутентификаторы** нажать кнопку: **Новый → Аутентификатор Regex LDAP**.
2. Заполнить поля первых трёх вкладок.

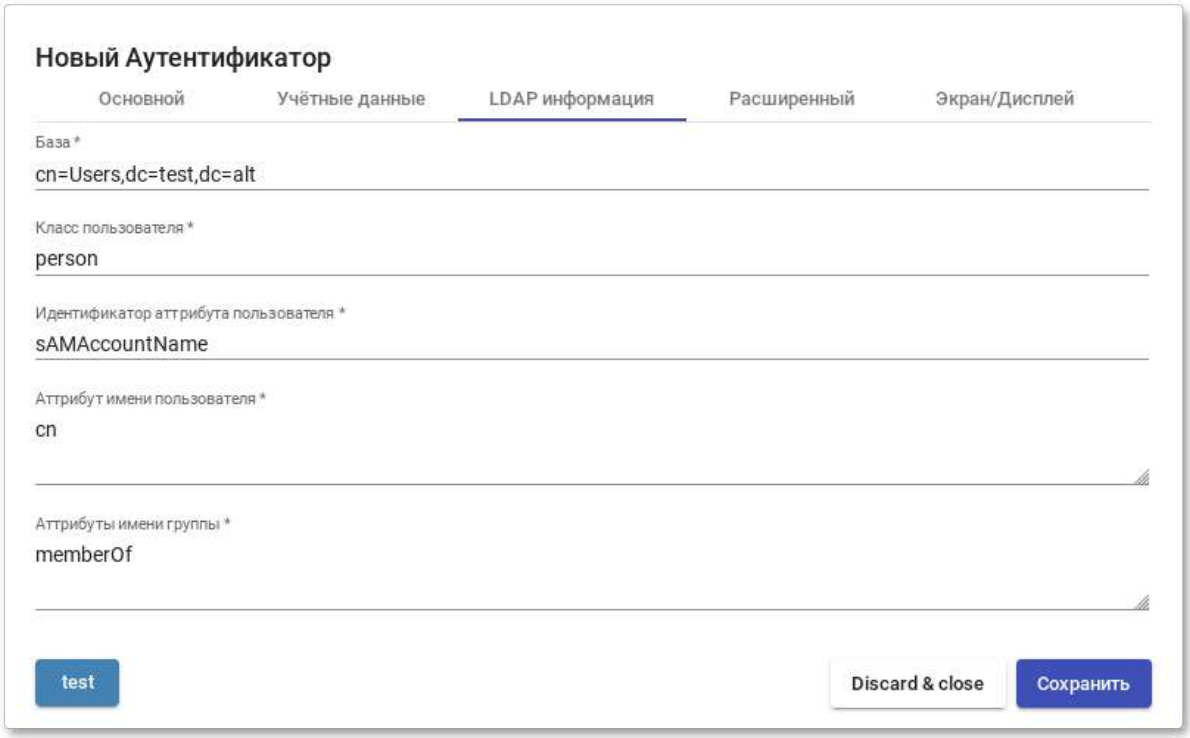
   Вкладка **Основной**: имя аутентификатора, приоритет, метка, IP-адрес сервера AD, порт (обычно 389 без ssl, 636 с ssl):



Вкладка **Учётные данные**: имя пользователя (можно указать в виде имя@домен) и пароль:



Вкладка **LDAP информация**: общая база пользователей, класс пользователей LDAP, идентификатор атрибута пользователя, атрибут имени пользователя, атрибут имени группы:

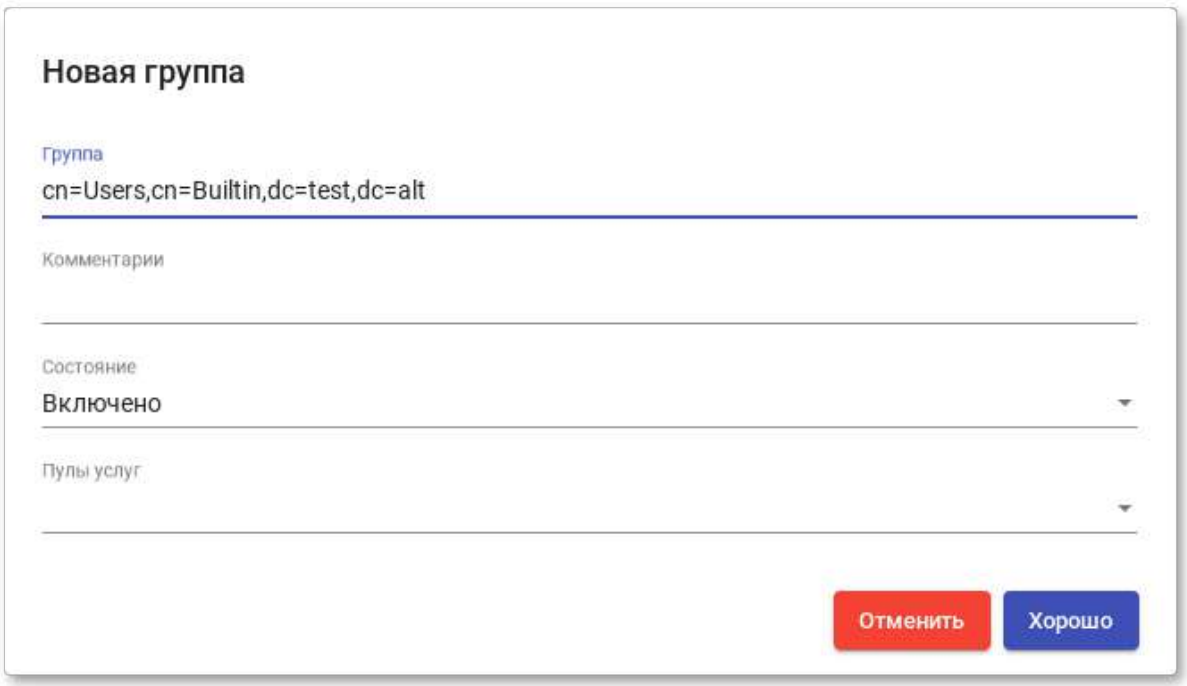


Примечание

Используя кнопку **`test`**, можно проверить соединение с Active Directory.

3. Добавить группу LDAP, в которую входят пользователи. Для этого следует выбрать созданный аутентификатор, во вкладке **Группы** нажать **Новый** → **Группа**.

   Заполнить dn существующей группы (например, cn=Users,cn=Builtin,dc=test,dc=alt), можно также указать разрешённые пулы:

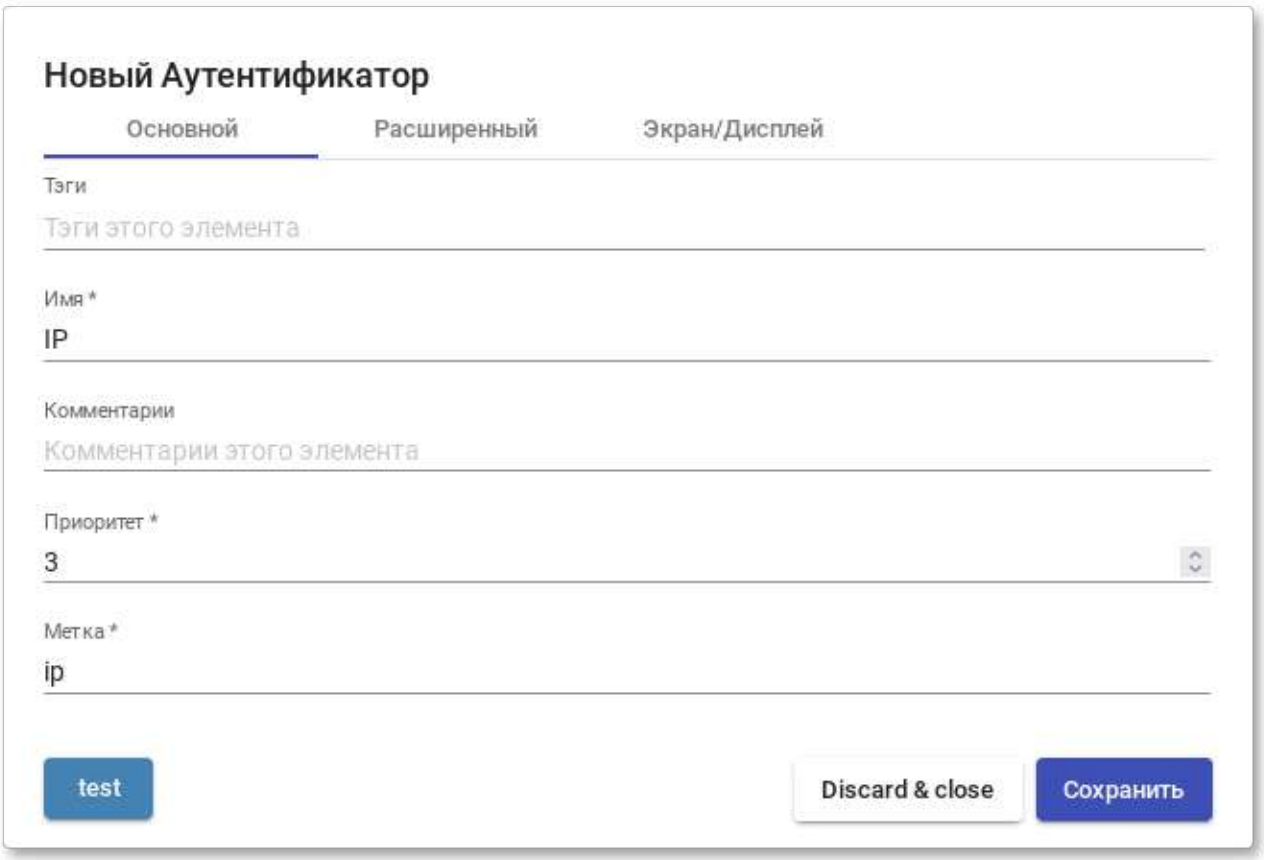


55.2.2.3. IP аутентификатор

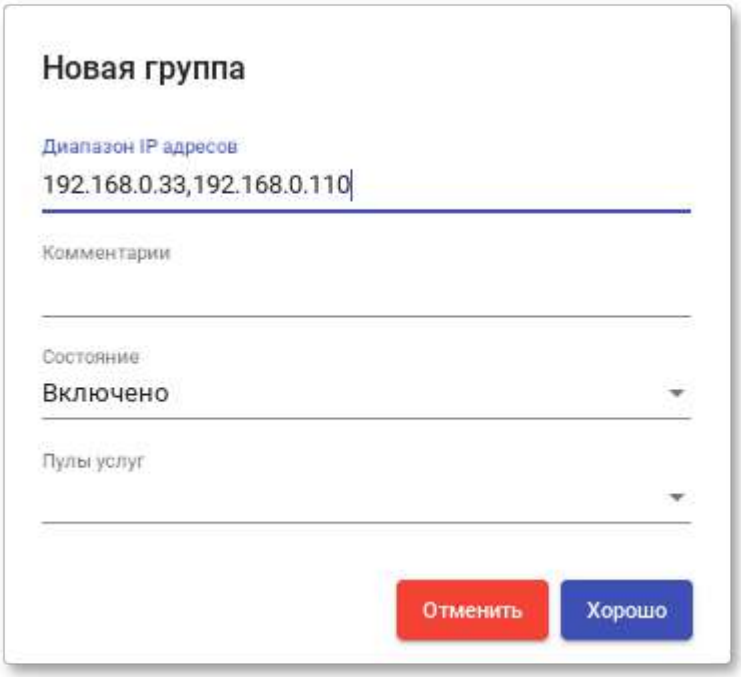
Этот тип аутентификации обеспечивает доступ клиентов к рабочим столам и виртуальным приложениям по их IP-адресу.

Для создания аутентификации типа **IP аутентификатор** в разделе **Аутентификаторы** следует нажать кнопку: **Новый → IP аутентификатор**.

Минимальные параметры конфигурации (вкладка **Основной**): имя аутентификатора, приоритет и метка.



После того, как аутентификатор типа «IP аутентификатор» создан, следует создать группы пользователей. Группа может представлять собой диапазон IP-адресов (192.168.0.1-192.168.0.55), подсеть (192.168.0.0/24) или отдельные IP-адреса (192.168.0.33,192.168.0.110):



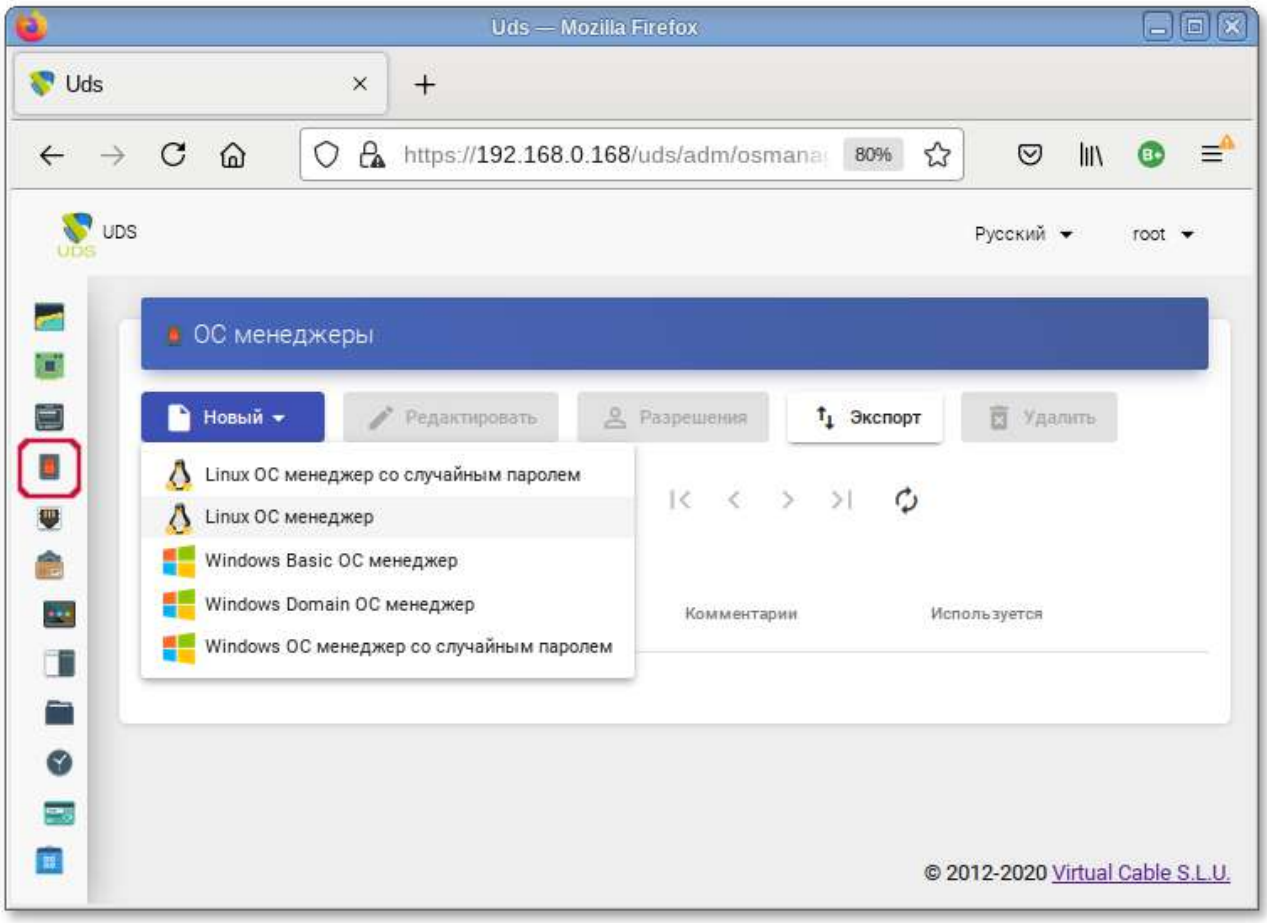
55.2.3. Настройка менеджера ОС

Менеджер ОС запускает ранее настроенные службы.

OpenUDS Actor, размещенный на виртуальном рабочем столе, отвечает за взаимодействие между ОС и OpenUDS Server на основе конфигурации или выбранного типа Менеджера ОС.

Примечание

Для каждой службы, развернутой в OpenUDS, потребуется «Менеджер ОС», за исключением случаев, когда используется **Поставщик машин статических IP**.

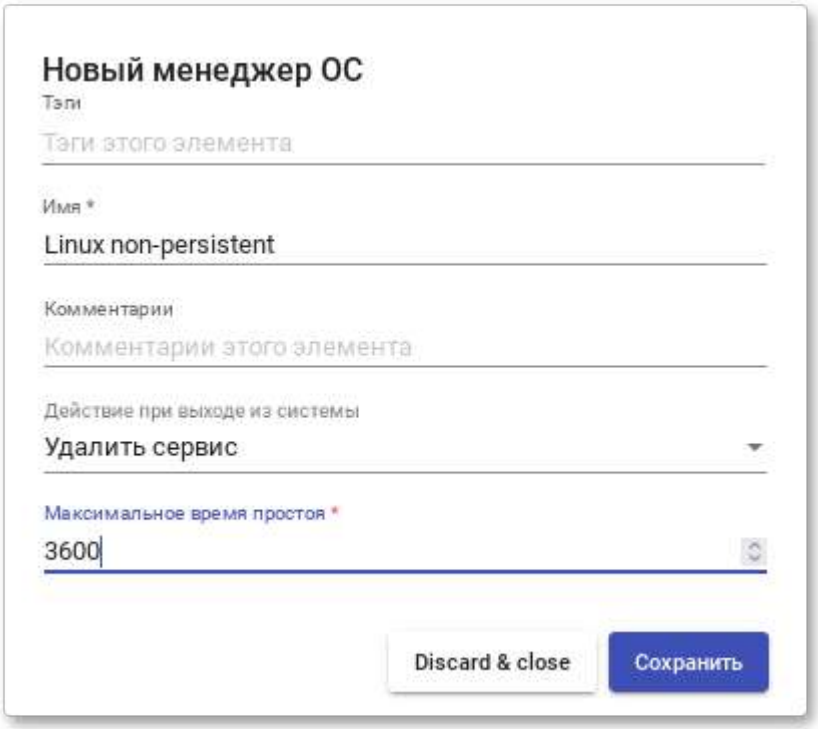


Linux ОС менеджер используется для виртуальных рабочих столов на базе Linux. Он выполняет задачи переименования и управления сеансами виртуальных рабочих столов.

Windows Basic ОС менеджер используется для виртуальных рабочих столов на базе Windows, которые не являются частью домена AD.

Минимальные настройки для **Linux ОС менеджер** и **Windows Basic ОС менеджер**:

- **Имя** (**Name**) — название;
- **Действие при выходе из системы** (**Logout Action**) — действие, которое OpenUDS будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя. **Держать сервис привязанным** (**Keep service assigned**) — постоянный пул, при выходе пользователя (выключении ВМ), ВМ запускается заново, при повторном входе пользователю будет назначен тот же рабочий стол. **Удалить сервис** (**Remove service**) — непостоянный пул, при выходе пользователя из системы, ВМ удаляется и создается заново. **Держать сервис привязанным даже в новой публикации** (**Keep service assigned even on new publication**) — сохранение назначенной службы даже при создании новой публикации;
- **Максимальное время простоя** (**Max. Idle time**) — время простоя виртуального рабочего стола (в секундах). По истечении этого времени OpenUDS Actor автоматически закроет сеанс. Отрицательные значения и значения менее 300 секунд отключают эту опцию.



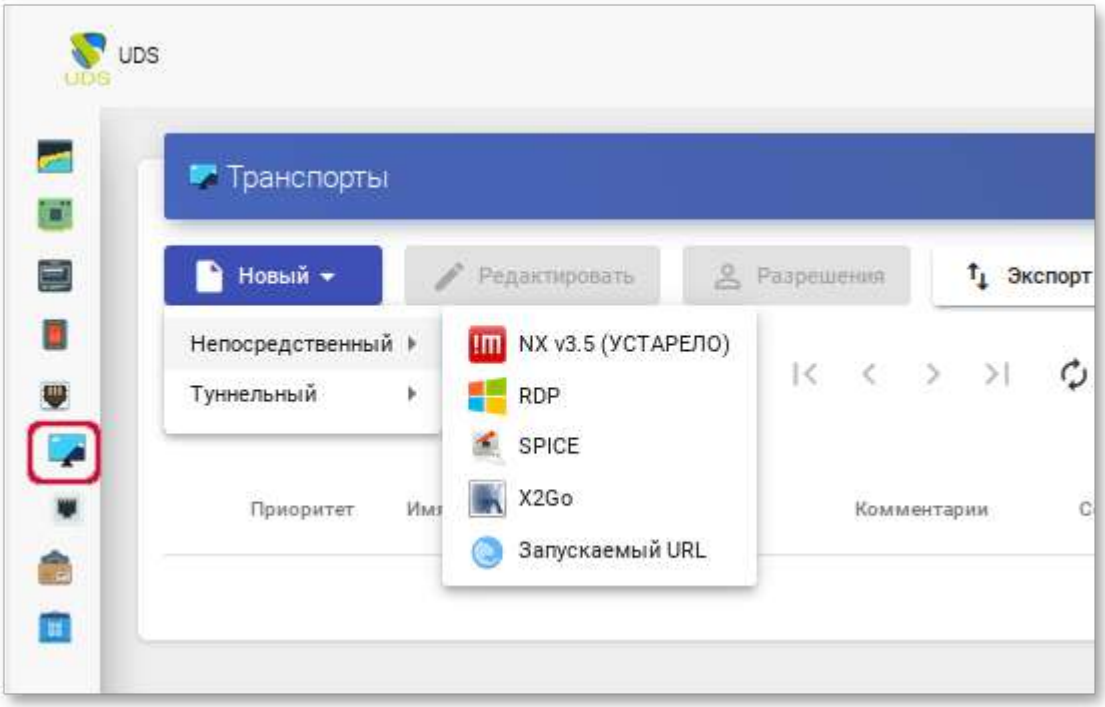
55.2.4. Транспорт

Для подключения к виртуальным рабочим столам необходимо создать транспорт. Транспорт — это приложение, которое выполняется на клиенте и отвечает за предоставление доступа к реализованной службе.

Можно создать один транспорт для различных «пулов» или установить по одному транспорту для каждого «пула».

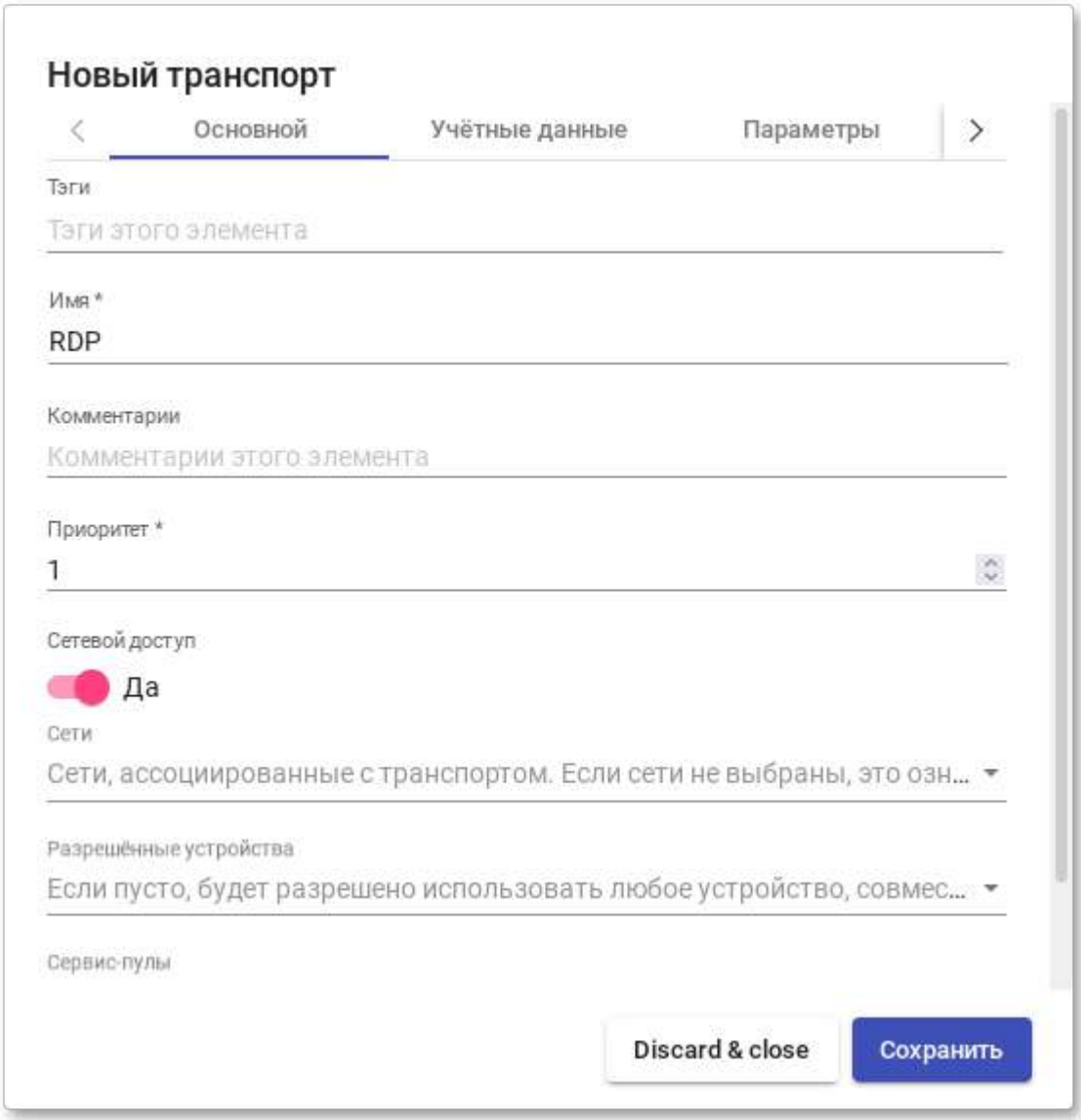
При создании транспорта необходимо выбрать его тип:

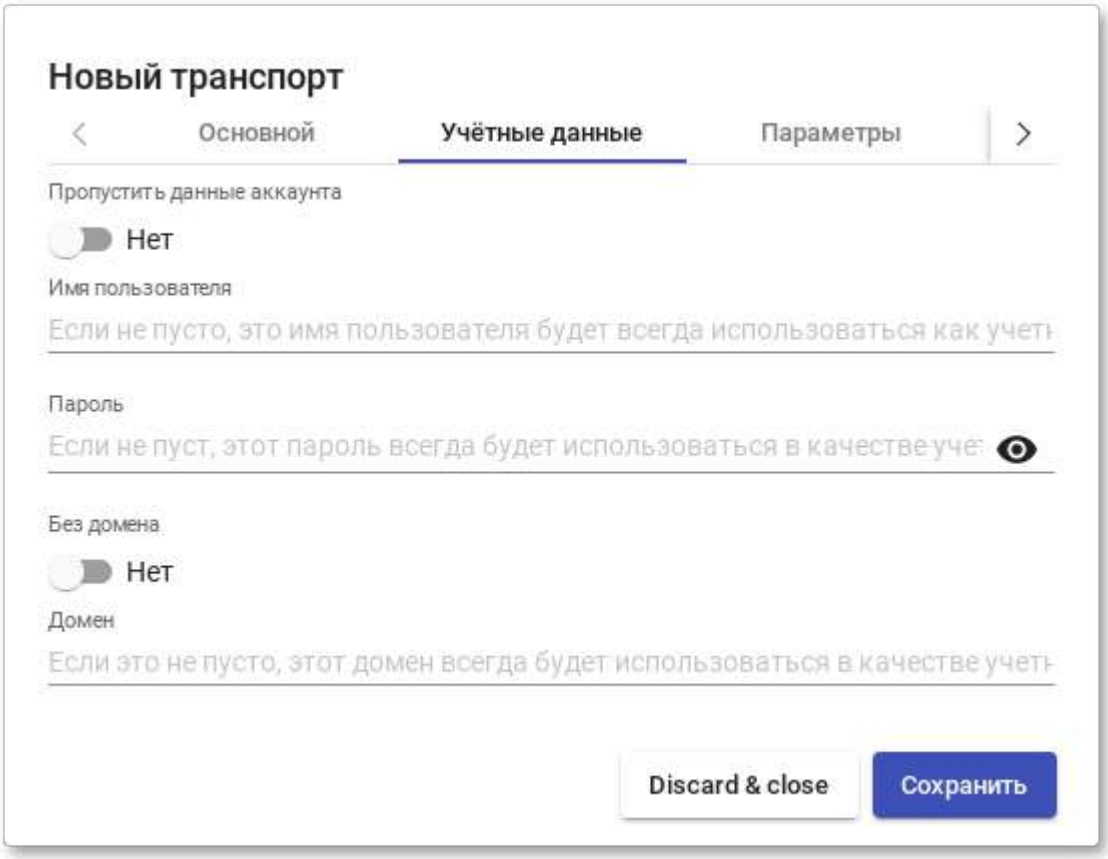
- **Непосредственный** (**Direct**) — используется, если пользователь имеет доступ к виртуальным рабочим столам из внутренней сети (например, LAN, VPN и т.д.);
- **Туннельный** (**Tunneled**) — используется, если у пользователя нет прямого подключения к рабочему столу.



RDP (непосредственный)

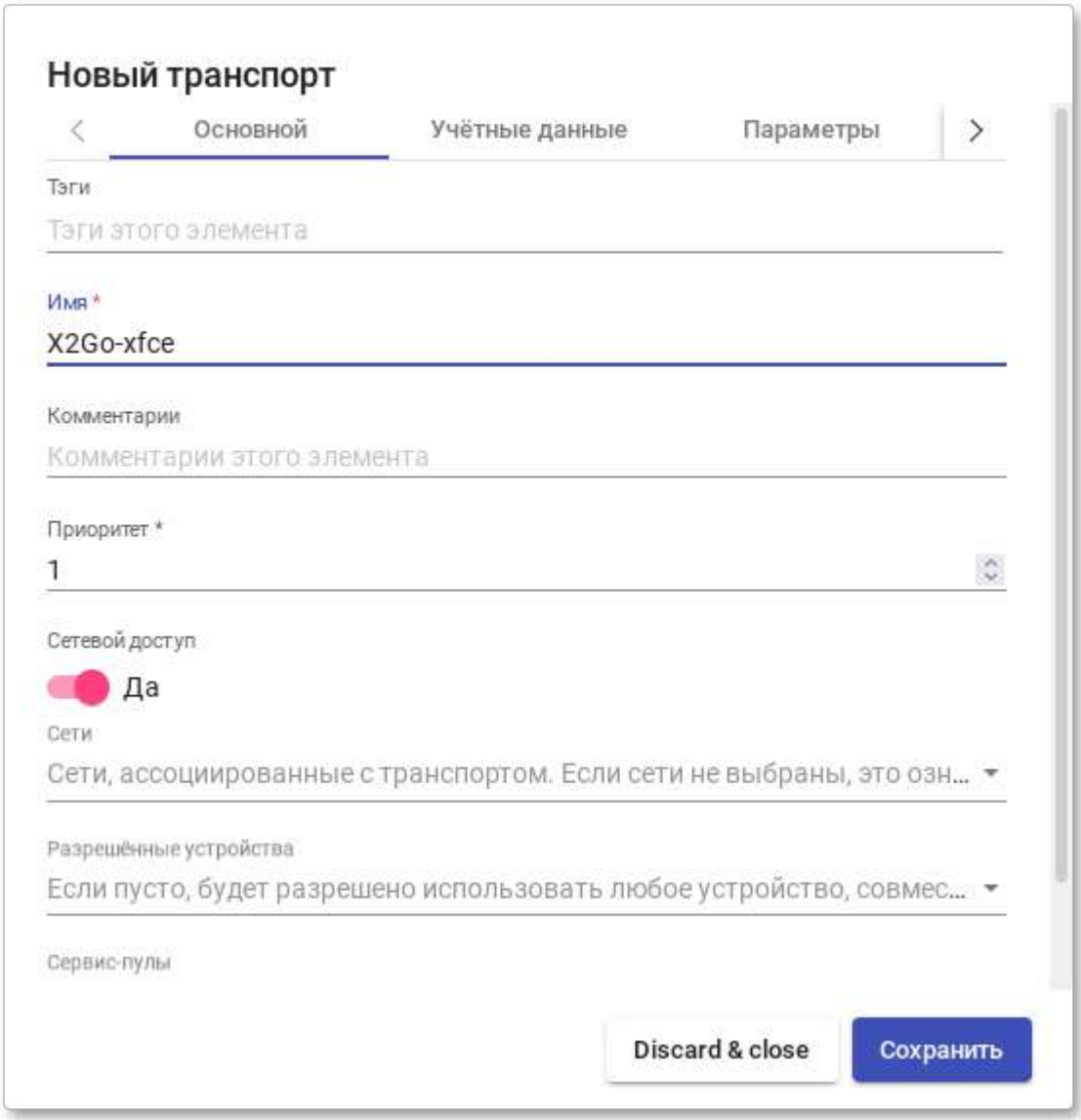
Позволяет пользователям получать доступ к виртуальным рабочим столам Windows/Linux. И на клиентах подключения, и на виртуальных рабочих столах должен быть установлен и включен протокол RDP (для виртуальных рабочих столов Linux необходимо использовать XRDP).

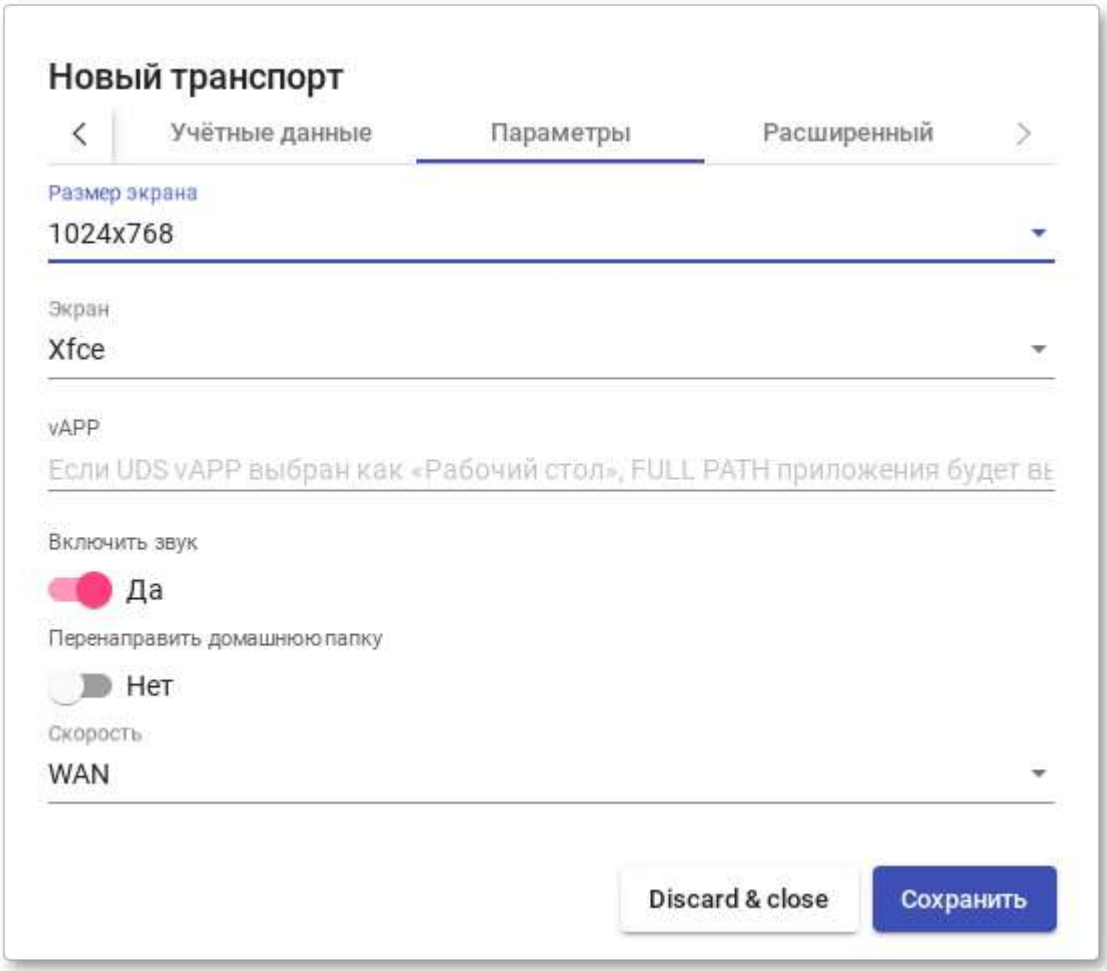

Новый транспорт
Основной
Учётные данные
Параметры
Тэги
Тэги этого элемента
Имя *
RDP
Комментарии
Комментарии этого элемента
Приоритет *
1
Сетевой доступ
Да
Сети
Сети, ассоциированные с транспортом. Если сети не выбраны, это озн...
Разрешённые устройства
Если пусто, будет разрешено использовать любое устройство, совмес...
Сервис-пулы
Discard & close
Сохранить



X2Go (непосредственный)

Позволяет пользователям получать доступ к виртуальным рабочим столам Linux. На клиентах подключения должен быть установлен клиент X2Go, и на виртуальных рабочих столах (сервере) должен быть установлен и включен сервер X2Go.

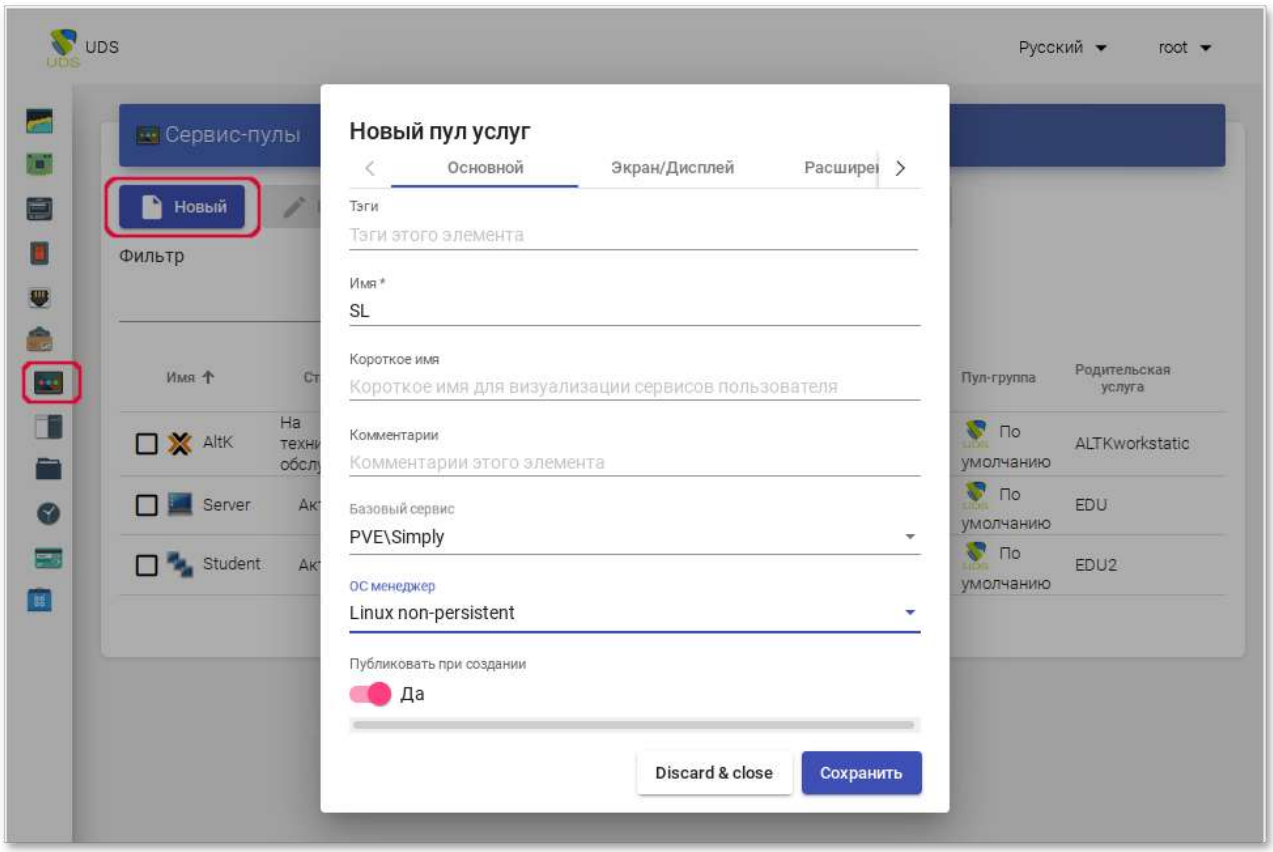

Новый транспорт
Основной
Учётные данные
Параметры
Тэги
Тэги этого элемента
Имя *
X2Go-xfce
Комментарии
Комментарии этого элемента
Приоритет *
1
Сетевой доступ
Да
Сети
Сети, ассоциированные с транспортом. Если сети не выбраны, это озн...
Разрешённые устройства
Если пусто, будет разрешено использовать любое устройство, совмес...
Сервис-пулы
Discard & close
Сохранить



55.2.5. Пулы услуг

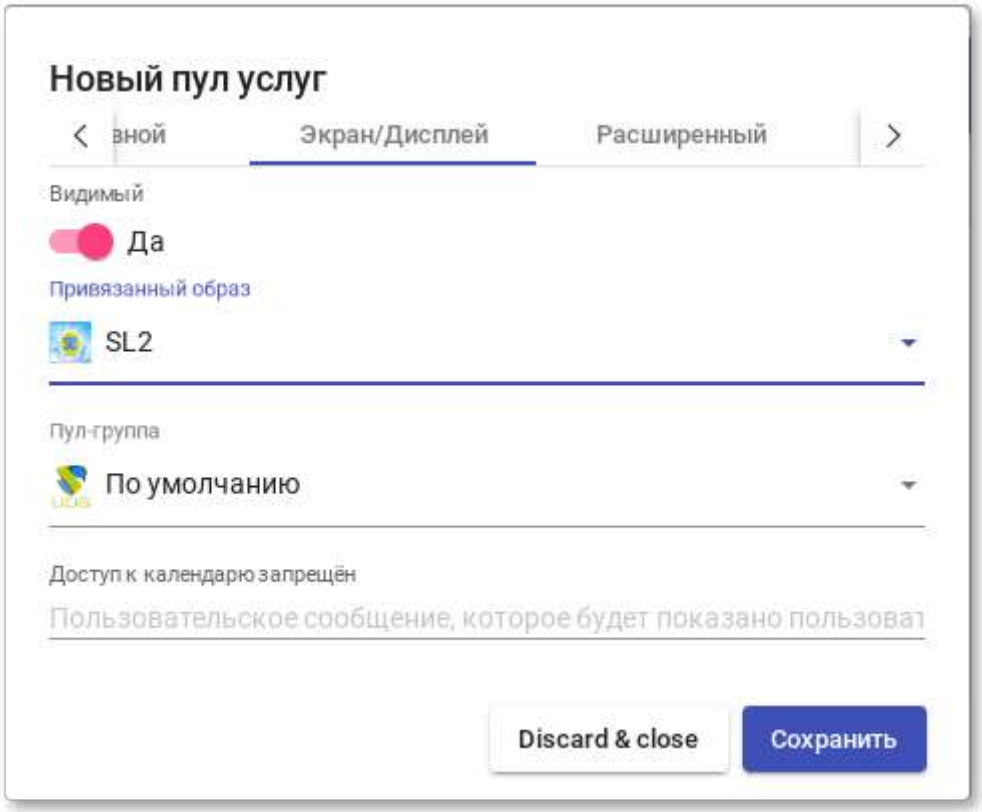
После того, как был создан и настроен хотя бы один поставщик («Service provider») с соответствующей службой/услугой, аутентификатор (с пользователем и группой), менеджер ОС и транспорт, можно создать пул услуг («Service Pool») для публикации виртуальных рабочих столов.

В разделе **Пулы услуг** (**Service Pool**) нажать кнопку **Новый** (**New**):

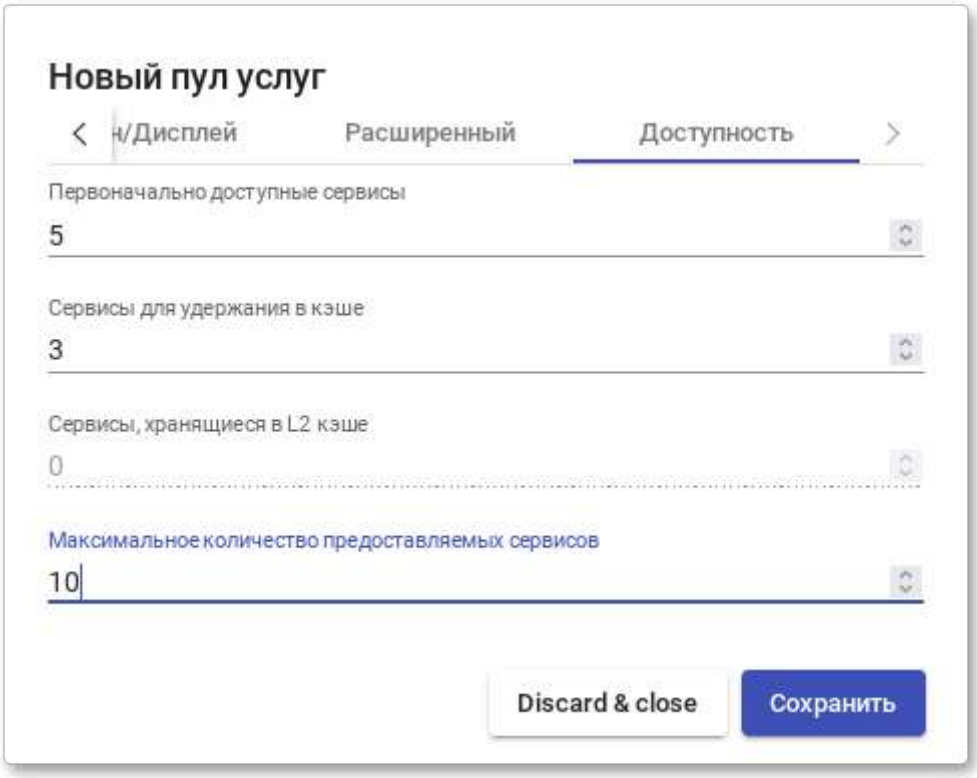


Заполнить параметры конфигурации:

- Вкладка **Основной** (**Main**):
  - **Имя** — название службы;
  - **Базовый сервис** — выбрать службу, созданная ранее в поставщике услуг;
  - **ОС Менеджер** — выбрать, созданный ранее, менеджер ОС;
  - **Публиковать при создании** — публиковать пул при создании или вручную.



- Вкладка **Экран/Дисплей** (**`Display`**):
  - **Видимый** — если этот параметр отключен, пул не будет отображаться у пользователей;
  - **Привязанный образ** — изображение, связанное с услугой. Изображение должно быть предварительно добавлено в репозиторий изображений (раздел **Инструменты** → **Галерея**);
  - **Пул-группа** — позволяет группировать различные службы. Группа должна быть предварительно создана в разделе **Пулы** → **Группа**.

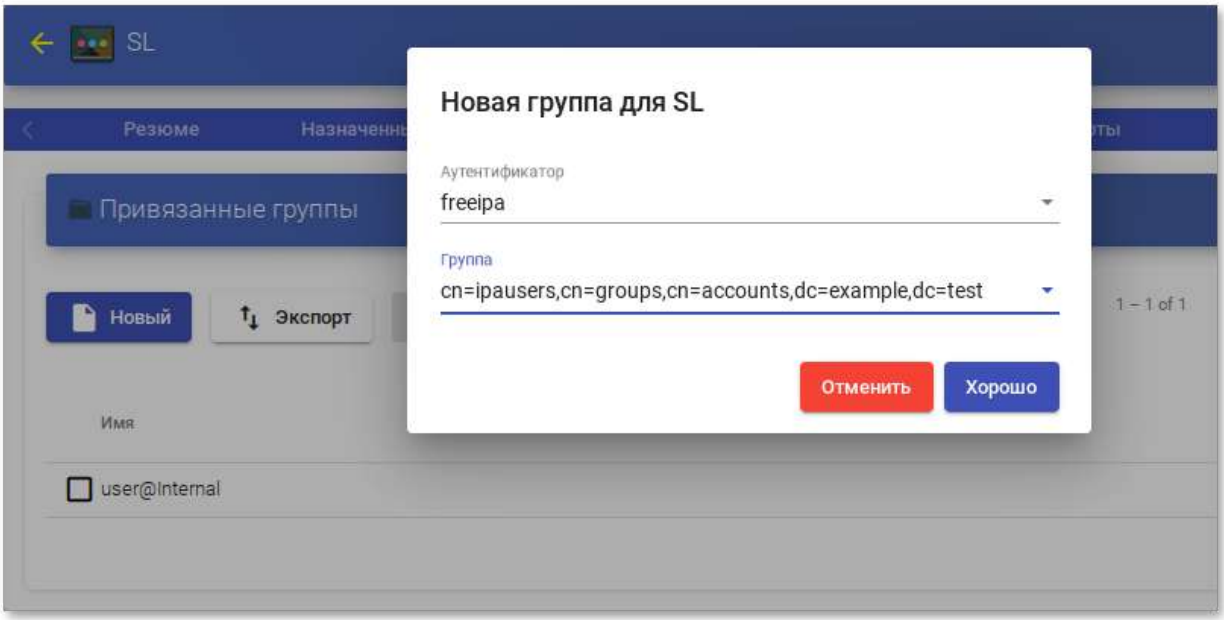


- Вкладка **Доступность** (**Availability**):
  - **Первоначально доступные сервисы** — минимальное количество виртуальных рабочих столов, созданных, настроенных и назначенных/доступных для службы;
  - **Сервисы для удержания в кэше** — количество доступных виртуальных рабочих мест. Эти ВМ всегда будут настроены и готовы к назначению пользователю (они будут автоматически создаваться до тех пор, пока не будет достигнуто максимальное количество машин, указанное в поле **Максимальное количество предоставляемых сервисов**);
  - **Максимальное количество предоставляемых сервисов** — максимальное количество виртуальных рабочих столов, созданных системой в данном пуле (рабочие столы, созданные в кэше L2, не учитываются).

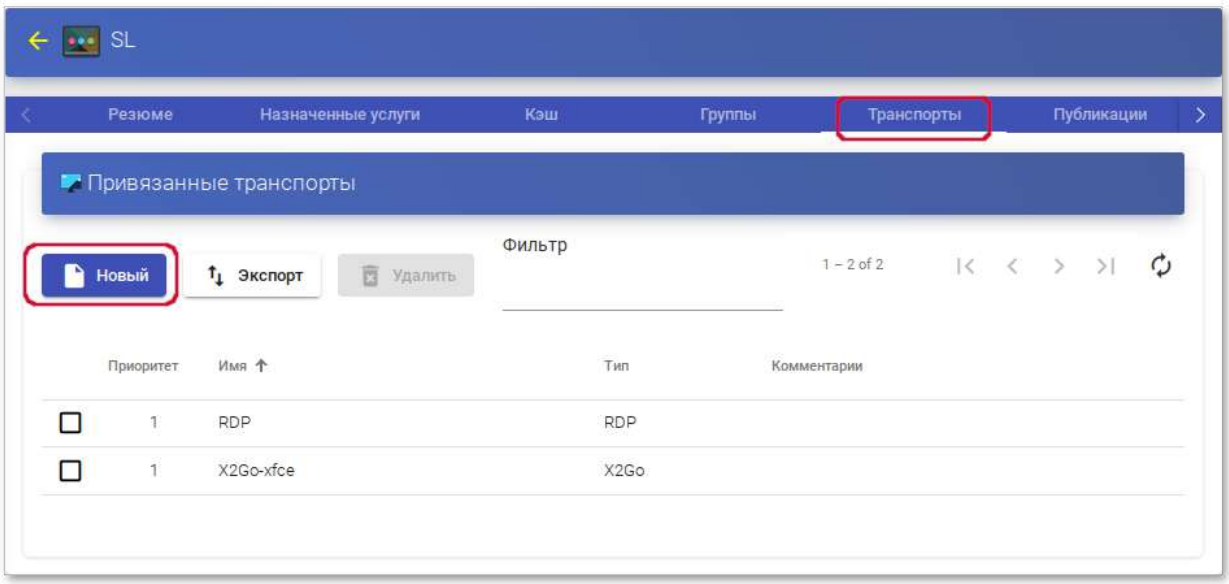
Нажать кнопку **Сохранить** и система начнет создавать виртуальные рабочие столы на основе настроенного кеша.

После создания пула, в настройках (дважды щелкнуть мышью по строке созданного пула или в контекстном меню пула выбрать пункт **Подробность**):

- на вкладке **Группы** назначить группы доступа (выбрать аутентификатор и группу, которая будет иметь доступ к этому пулу служб):



- на вкладке **Транспорты** выбрать способы подключения пользователей к рабочему столу:



55.3. Подготовка шаблона виртуальной машины

Подготовить шаблон ВМ:

1. Установить openuds-actor:

```
# apt-get install openuds-actor
```

2. Включить автозапуск сервиса udsactor.service:

```
# systemctl enable udsactor.service
```

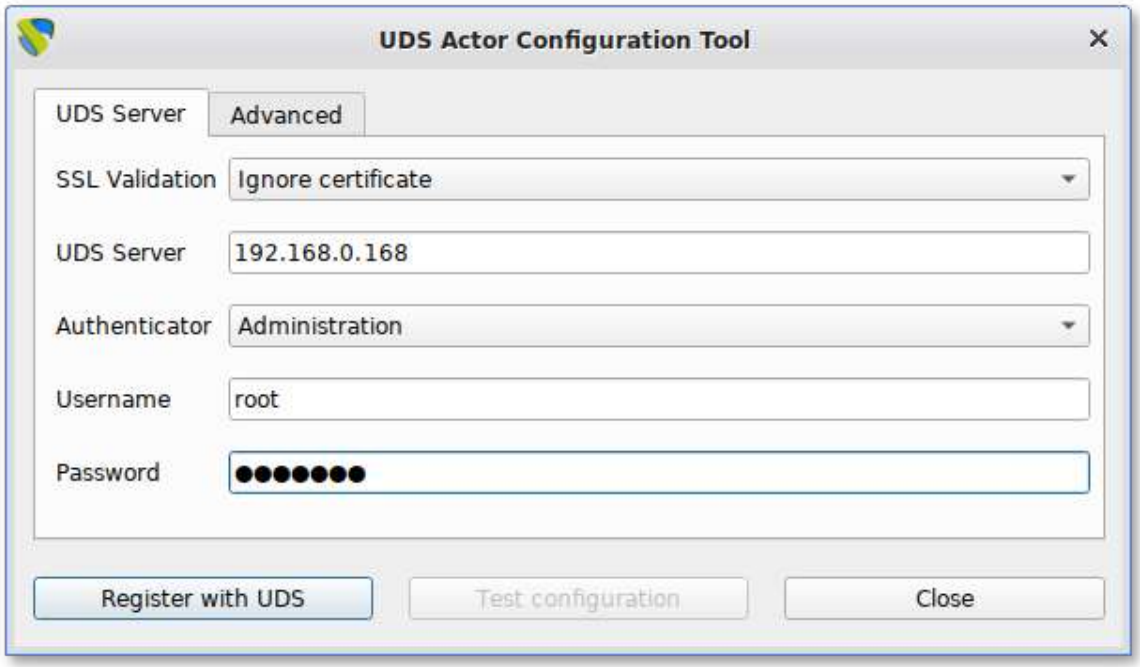
3. Зарегистрировать OpenUDS Actor на сервере OpenUDS:

   - запустить OpenUDS Actor из меню **Настройки** → **UDS Actor Configuration** или командой:

```
$ /usr/sbin/UDSActorConfig-pkexec
```

Потребуется ввести пароль пользователя, входящего в группу wheel.

- на вкладке **`UDS Server`** указать имя или IP-адрес сервера OpenUDS, имя и пароль пользователя, имеющего права администратора в среде OpenUDS и нажать кнопку **`Register with UDS`** (**`Зарегистрироваться в UDS`**):



- на вкладке **Advanced** можно указать дополнительные параметры, в том числе уровень журналирования. Для применения настроек указанных на этой вкладке необходимо выполнить перерегистрацию UDSActor.

4. Установить и настроить один из вариантов удаленного доступа:
   - XRDP:
     - установить пакет xrdp:

```
# apt-get install xrdp
```

     - включить сервисы xrdp и xrdp-sesman:

```
# systemctl enable --now xrdp
# systemctl enable --now xrdp-sesman
```

     - для доступа к терминальному сеансу включить пользователя в группу tsusers:

```
# gpasswd -a user tsusers
```

   - X2Go:
     - установить пакет x2goserver:

```
# apt-get install x2goserver
```

- включить сервис x2goserver:

```
# systemctl enable --now x2goserver
```

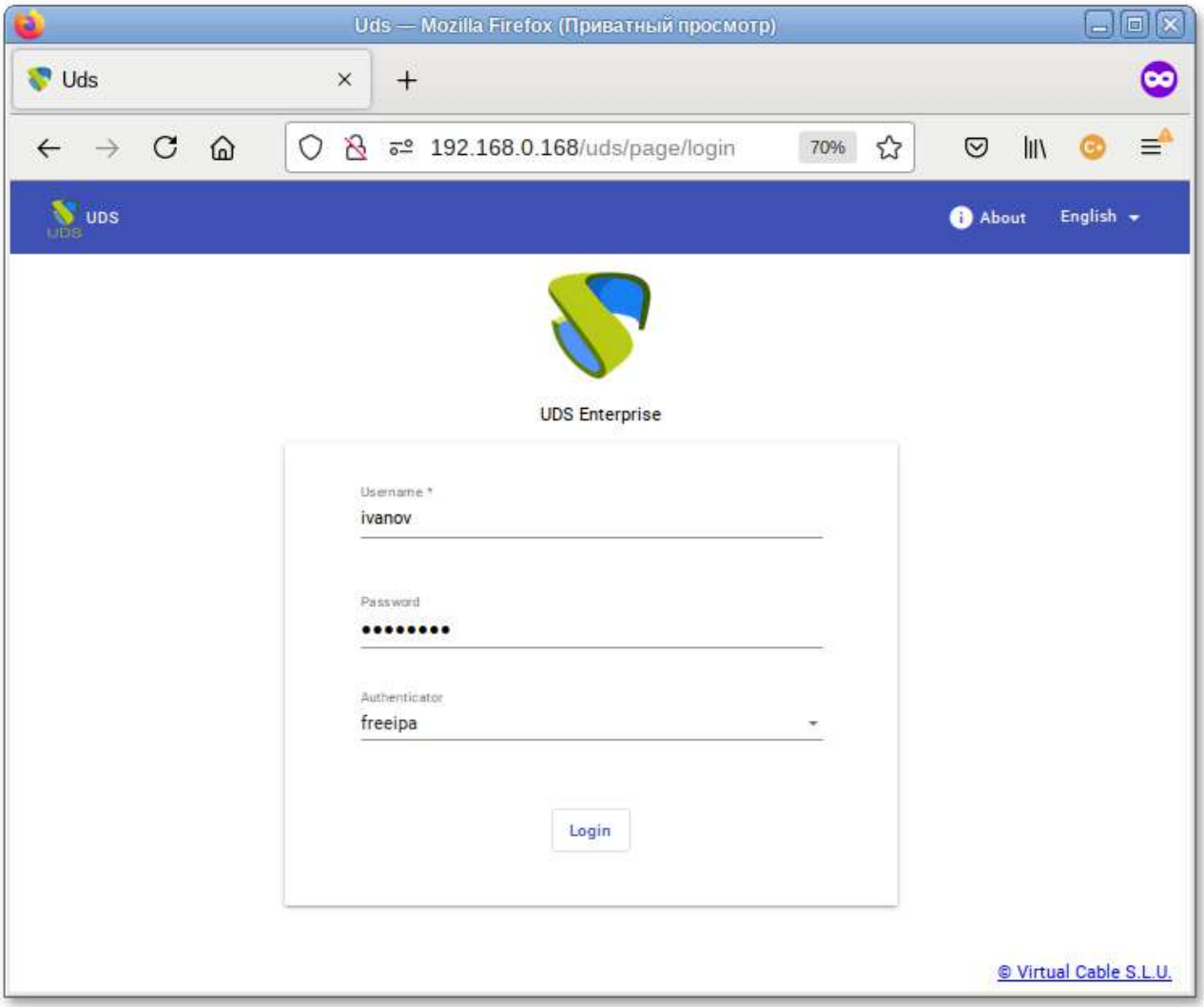
55.4. Подключение пользователя к виртуальному рабочему месту

На клиенте должен быть установлен пакет openuds-client:

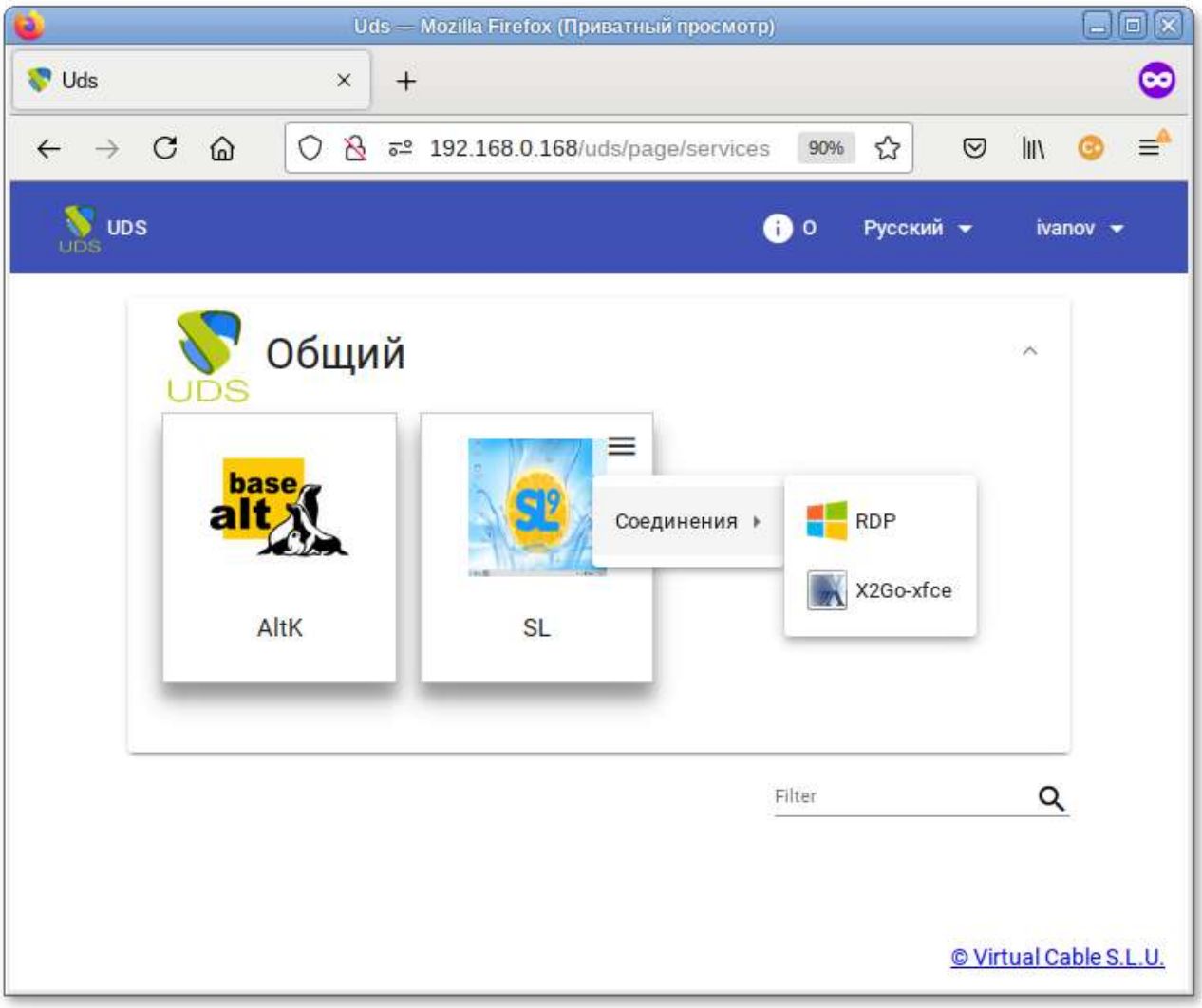
```
# apt-get install openuds-client
```

Чтобы иметь возможность подключаться к виртуальному рабочему столу, должны быть установлены клиенты каждого используемого протокола удаленного доступа (xfreerdp, x2goclient).

Подключиться к серверу OpenUDS с помощью браузера http://openuds_address, ввести имя пользователя и пароль, выбрать средство проверки подлинности, если доступно несколько:



На панели управления будут отображены все ВМ (или шаблоны), к которым у пользователя есть доступ:



После выбора пула, автоматически стартует OpenUDS Client, который обрабатывает URL, получает необходимые настройки протокола удаленного доступа для предоставленной (свободной) ВМ, формирует файл описания сессии и передает его приложению-клиенту удалённого доступа, которое и устанавливает соединение с указанной ВМ. Как только соединение будет установлено, виртуальный рабочий стол будет доступен для использования.

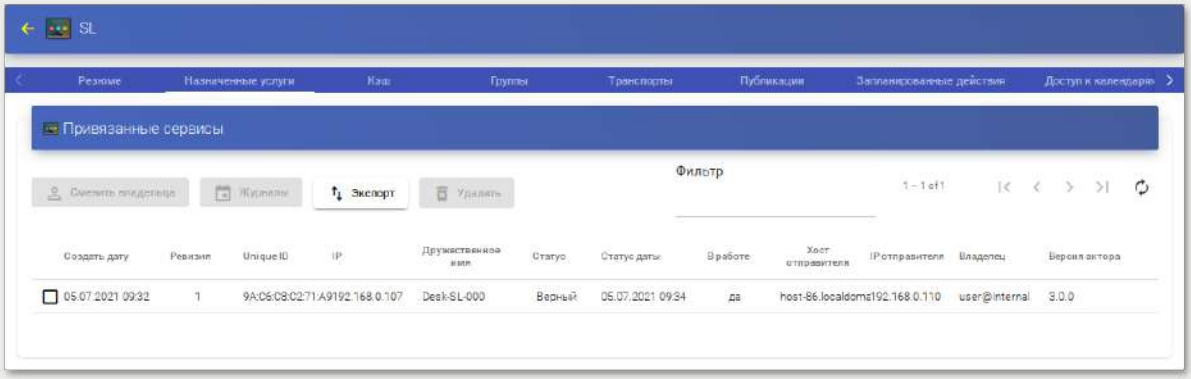
Примечание

Если для подключения к ВМ настроено более одного типа транспорта, то в правом верхнем углу службы будет отображена кнопка. Если выбрать непосредственно ВМ, будет вызван транспорт по умолчанию (транспорт с меньшим значением в поле приоритет). Для того чтобы использовать другой транспорт, нужно выбрать его в раскрывающемся списке.

По завершении сеанса пользователь ВМ выходит из нее, что приводит к остановке OpenUDS Actor. Брокер openUDS считает, что ВМ стала недоступной и, если пул постоянный, то он запускает ВМ, а если пул временный, то происходит удаление файлов ВМ в хранилище и создается новая ВМ из мастер-образа.

Примечание

При подключении пользователя к виртуальному рабочему месту OpenUDS фиксирует доступ и отображает информацию о привязанном сервисе на вкладке **Назначенные услуги** соответствующего пула.



Часть X. Установка пакетов для опытных пользователей

Содержание

Введение

В современных системах на базе Linux существует огромное число общих ресурсов: разделяемых библиотек, содержащих стандартные функции, исполняемые файлы, сценарии и стандартные утилиты и т.д. Этими общими ресурсами пользуются сразу несколько программ. Удаление или изменение версии одного из составляющих систему компонентов может повлечь неработоспособность других, связанных с ним компонентов, или может привести к выводу из строя всей системы. В контексте системного администрирования проблемы такого рода называют нарушением *целостности системы*. Задача администратора — обеспечить наличие в системе согласованных версий всех необходимых программных компонентов (обеспечение целостности системы).

Для установки, удаления и обновления программ, а также поддержания целостности системы в Linux в первую очередь стали использоваться программы *менеджеры пакетов* (например, такие, как **rpm**). С точки зрения менеджера пакетов программное обеспечение представляет собой набор компонентов — программных *пакетов*. Пакеты содержат в себе набор исполняемых программ и вспомогательных файлов, необходимых для корректной работы программного обеспечения. Менеджеры пакетов облегчают установку программ: они позволяют проверить наличие необходимого для работы устанавливаемой программы компонента подходящей версии непосредственно в момент установки. Менеджеры пакетов производят необходимые процедуры для регистрации программы во всех операционных средах пользователя: сразу после установки программа становится доступна пользователю из командной строки и появляется, если это было предусмотрено, в меню приложений всех графических оболочек.

Часто компоненты, используемые различными программами, выделяют в отдельные пакеты и помечают, что для работы ПО, предоставляемого пакетом A, необходимо установить пакет B. В таком случае говорят, что пакет A *зависит* от пакета B или между пакетами A и B существует *зависимость*.

Отслеживание зависимостей между такими пакетами представляет собой важную задачу для любого дистрибутива. Некоторые компоненты пакетов могут быть взаимозаменяемыми, т.е. может обнаружиться несколько пакетов, предлагающих затребованный ресурс.

Ещё более сложной является задача контроля целостности и непротиворечивости установленного в системе ПО. Представим, что некие программы A и B требуют наличия в системе компонентов C версии 1.0. Обновление версии пакета A, требующее обновления компонентов C до новой версии (например, до версии 2.0, использующей новый интерфейс доступа), влечёт за собой обязательное обновление и программы B.

На практике менеджеры пакетов оказались неспособны эффективно устранить нарушения целостности системы и предотвратить все коллизии при установке или удалении программ. Особенно остро этот недостаток сказался на обновлении систем из централизованного репозитория, в котором пакеты непрерывно обновляются, дробятся на более мелкие и т.п. Именно этот недостаток стимулировал создание систем управления программными пакетами и поддержания целостности ОС.

Для автоматизации и контроля описанных выше процессов стала применяться Усовершенствованная система управления программными пакетами **APT** (от англ. Advanced Packaging Tool). Автоматизация и контроль достигаются путём создания одного или нескольких внешних репозиториев. В них хранятся доступные для установки пакеты программ.

В распоряжении **APT** находятся две базы данных: одна описывает установленные в системе пакеты, вторая — внешний репозиторий. **APT** отслеживает целостность установленной системы и, в случае обнаружения противоречий в зависимостях пакетов, разрешает конфликты, находит пути их корректного устранения, руководствуясь сведениями из внешних репозиториев.

Система **APT** состоит из нескольких утилит. Чаще всего используется утилита управления пакетами **`apt-get`**. Она автоматически определяет зависимости между пакетами и строго следит за её соблюдением при выполнении любой из следующих операций: установка, удаление или обновление пакетов.

Глава 56. Источники программ (репозитории)

Отличие репозиториев, с которыми работает **APT**, от простого набора пакетов — наличие метаинформации. В ней содержится индекс находящихся в репозитории пакетов и сведения о них. Поэтому, чтобы получить всю информацию о репозитории, **APT** достаточно получить его индексы.

APT может пользоваться любым количеством репозиториев одновременно, формируя единую информационную базу обо всех содержащихся в них пакетах. При установке пакетов **APT** обращает внимание только на название пакета, его версию и зависимости. Для **APT** не имеет значения расположение пакета в том или ином репозитории.

Важно

Для одновременного подключения нескольких репозиториев необходимо отслеживать их совместимость друг с другом, т.е. их пакетная база должна отражать один определённый этап разработки. Совместное использование репозиториев, относящихся к разным дистрибутивам, или смешивание стабильного репозитория с нестабильной веткой разработки (Sisyphus) может привести к различным неожиданностям и трудностям при обновлении пакетов.

APT осуществляет взаимодействие с репозиториями при помощи различных протоколов доступа. Наиболее популярные — HTTP и FTP.

Для того чтобы **APT** мог использовать тот или иной репозиторий, информацию о нём необходимо поместить в файл **`/etc/apt/sources.list`**, либо в любой файл **`.list`** (например, ***`mysources`*****`.list`**) в каталоге **`/etc/apt/sources.list.d/`**. Описания репозиториев заносятся в эти файлы в следующем виде:

```
rpm [подпись] метод:путь база название
rpm-src [подпись] метод:путь база название
```

Здесь:

- rpm или rpm-src — тип репозитория (скомпилированные программы или исходные тексты);
- [подпись] — необязательная строка-указатель на электронную подпись разработчиков. Наличие этого поля подразумевает, что каждый пакет из данного репозитория должен быть подписан соответствующей электронной подписью. Подписи описываются в файле **`/etc/apt/vendor.list`**;
- метод — способ доступа к репозиторию: ftp, http, file, rsh, ssh, cdrom, copy;
- путь — путь к репозиторию в терминах выбранного метода;
- база — относительный путь к базе данных репозитория;
- название — название репозитория.

Непосредственно после установки дистрибутива Альт Сервер в файлах **`/etc/apt/sources.list.d/*.list`** обычно указывается интернет-репозиторий, совместимый с установленным дистрибутивом.

После редактирования списка репозиториев в **`sources.list`**, необходимо обновить локальную базу данных **APT** о доступных пакетах. Это делается командой **`apt-get update`**.

Если в **sources.list** присутствует репозиторий, содержимое которого может изменяться (например, постоянно разрабатываемый репозиторий или репозиторий обновлений по безопасности), то прежде чем работать с **APT**, необходимо синхронизировать локальную базу данных с удалённым сервером командой **apt-get update**. Локальная база данных создаётся заново при каждом изменении в репозитории: добавлении, удалении или переименовании пакета.

При установке определённого пакета **APT** производит поиск самой новой версии этого пакета во всех известных ему репозиториях вне зависимости от способа доступа к ним. Так, если в репозитории, доступном в сети Интернет, обнаружена более новая в сравнении с компакт-диском версия программы, то **APT** начнёт загружать соответствующий пакет из сети Интернет. Поэтому, если подключение к сети Интернет отсутствует или ограничено низкой пропускной способностью канала или высокой стоимостью, то следует закомментировать строчки (добавить в начало строки символ #) в **/etc/apt/sources.list**, относящиеся к ресурсам в сети Интернет.

56.1. Редактирование репозиториев

Примечание

О добавлении или удалении репозиториев с использованием графических приложений вы можете почитать в Добавление репозиториев.

56.1.1. Утилита apt-repo

Для редактирования репозиториев можно воспользоваться утилитой **apt-repo**:

- просмотреть список активных репозиториев:

```
apt-repo
```

- добавить репозиторий в список активных репозиториев:

```
apt-repo add репозиторий
```

- удалить или выключить репозиторий:

```
apt-repo rm репозиторий
```

- обновить информацию о репозиториях:

```
apt-repo update
```

- справка о команде **apt-repo**:

```
man apt-repo
```

или

```
apt-repo --help
```

Примечание

Для выполнения большинства команд необходимы права администратора.

Типичный пример использования: удалить все источники и добавить стандартный репозиторий P9 (архитектура выбирается автоматически):

```
# apt-repo rm all
# apt-repo add p9
```

56.1.2. Добавление репозитория на CD/DVD-носителе

Для добавления в **sources.list** репозитория на компакт-диске в **APT** предусмотрена специальная утилита — **apt-cdrom**. Чтобы добавить запись о репозитории на компакт-диске, достаточно вставить диск в привод и выполнить команду **apt-cdrom add**. После этого в **sources.list** появится запись о подключённом диске примерно такого вида:

```
rpm cdrom:[ALT Server x86_64]/ ALTLinux main
```

Важно

Если при выполнении команды **apt-cdrom add**, вы получаете ошибку:

```
Не найдена точка монтирования /media/ALTLinux/ диска
```

Необходимо:

- в файл **/etc/fstab** добавить строку:

  ```
  /dev/sr0 /media/ALTLinux udf,iso9660
  ro,noauto,user,utf8,nofail,comment=x-gvfs-show  0 0
  ```

- создать каталог для монтирования:

  ```
  # mkdir /media/ALTLinux
  ```

- затем использовать команду добавления носителя:

  ```
  # apt-cdrom add
  ```

56.1.3. Добавление репозиториев вручную

Для изменения списка репозиториев можно отредактировать в любом текстовом редакторе файлы из каталога **/etc/apt/sources.list.d/**.

Примечание

Для изменения этих файлов необходимы права администратора.

В файле ***alt*.list** может содержаться такая информация:

```
# ftp.altlinux.org (ALT Linux, Moscow)

# ALT Linux Platform 9
#rpm [p9] ftp://ftp.altlinux.org/pub/distributions/ALTLinux/p9/branch x86_64
classic
#rpm [p9] ftp://ftp.altlinux.org/pub/distributions/ALTLinux/p9/branch x86_64-
i586 classic
#rpm [p9] ftp://ftp.altlinux.org/pub/distributions/ALTLinux/p9/branch noarch
classic

rpm [p9] http://ftp.altlinux.org/pub/distributions/ALTLinux/p9/branch x86_64
classic
rpm [p9] http://ftp.altlinux.org/pub/distributions/ALTLinux/p9/branch x86_64-
i586 classic
rpm [p9] http://ftp.altlinux.org/pub/distributions/ALTLinux/p9/branch noarch
classic
```

По сути, каждая строчка соответствует некому репозиторию. Не активные репозитории — строки, начинающиеся со знака #. Для добавления нового репозитория, достаточно дописать его в этот или другой файл.

После обновления списка репозиториев следует обновить информацию о них (выполнить команду **apt-get update** или **apt-repo update**).

Глава 57. Поиск пакетов

Если точное название пакета неизвестно, то для его поиска можно воспользоваться утилитой **apt-cache**. Данная утилита позволяет искать пакет не только по имени, но и по его описанию.

Команда **apt-cache search *подстрока*** позволяет найти все пакеты, в именах или описании которых присутствует указанная подстрока. Например:

```
$ apt-cache search dictionary
stardict-wn - GCIDE - The Collaborative International Dictionary of English
firefox-ru - Russian (RU) Language Pack for Firefox
gnome-dictionary-applet - GNOME panel applet for gnome-dictionary
gnome-utils - Utilities for the GNOME 2.0 desktop
libgdict - GNOME Dictionary Library.
stardict-mueller7 - V.K. Mueller English-Russian Dictionary, 7 Edition:
stardict format
stardict-slovnyk_be-en - Dictionary: Slovnyk Belarusian-English
stardict-slovnyk_be-ru - Dictionary: Slovnyk Belarusian-Russian
stardict-slovnyk_be-uk - Dictionary: Slovnyk Belarusian-Ukrainian
stardict-slovnyk_cs-ru - Dictionary: Slovnyk Czech-Russian
stardict-slovnyk_en-be - Dictionary: Slovnyk English-Belarusian
stardict-slovnyk_en-ru - Dictionary: Slovnyk English-Russian
stardict-slovnyk_en-uk - Dictionary: Slovnyk English-Ukrainian
stardict-slovnyk_es-ru - Dictionary: Slovnyk Spanish-Russian
```

```
stardict-slovnyk_ru-be - Dictionary: Slovnyk Russian-Belarusian
stardict-slovnyk_ru-cs - Dictionary: Slovnyk Russian-Czech
stardict-slovnyk_ru-en - Dictionary: Slovnyk Russian-English
stardict-slovnyk_ru-es - Dictionary: Slovnyk Russian-Spanish
stardict-slovnyk_ru-uk - Dictionary: Slovnyk Russian-Ukrainian
stardict-slovnyk_uk-be - Dictionary: Slovnyk Ukrainian-Belarusian
stardict-slovnyk_uk-en - Dictionary: Slovnyk Ukrainian-English
stardict-slovnyk_uk-ru - Dictionary: Slovnyk Ukrainian-Russian
words - A dictionary of English words for the /usr/share/dict directory
```

Для того чтобы подробнее узнать информацию о найденном пакете и получить его подробное описание, воспользуйтесь командой **apt-cache show**:

```
$ apt-cache show stardict-mueller7
Package: stardict-mueller7
Section: Text tools
Installed Size: 3095255
Maintainer: Anton V. Boyarshinov <boyarsh@altlinux.ru>
Version: 1.0-alt7
Pre-Depends: rpmlib(PayloadIsLzma)
Depends: stardict (>= 2.4.2)
Provides: stardict-mueller7 (= 1.0-alt7)
Architecture: noarch
Size: 3135276
MD5Sum: ea95c67ca323350b454fbc26533c3548
Filename: stardict-mueller7-1.0-alt7.noarch.rpm
Description: V.K. Mueller English-Russian Dictionary, 7 Edition: stardict
format
 Electronic version of V.K. Mueller English-Russian Dictionary, 7 Edition
 in stardict format. You can use it with stardict client.
```

При поиске с помощью **apt-cache** можно использовать русскую подстроку. В этом случае будут найдены пакеты, имеющие описание на русском языке. К сожалению, описание на русском языке в настоящее время есть не у всех пакетов, но наиболее актуальные описания переведены.

Глава 58. Установка или обновление пакета

Важно

Для установки пакетов требуются привилегии администратора.

Установка пакета с помощью APT выполняется командой **apt-get install *имя_пакета***.

Важно

Перед установкой и обновлением пакетов необходимо выполнить команду обновления индексов пакетов:

```
# apt-get update
```

apt-get позволяет устанавливать в систему пакеты, требующие для работы наличие других, пока ещё не установленных пакетов. В этом случае он определяет, какие пакеты необходимо установить. **apt-get** устанавливает их, пользуясь всеми доступными репозиториями.

Установка пакета *stardict-mueller7* командой **apt-get install stardict-mueller7** приведёт к следующему диалогу с **APT** (если пакет еще не установлен):

```
# apt-get install stardict-mueller7
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие НОВЫЕ пакеты будут установлены:
  stardict-mueller7
0 будет обновлено, 1 новых установлено, 0 пакетов будет удалено и 0 не будет
обновлено.
Необходимо получить 0B/3135kB архивов.
После распаковки потребуется дополнительно 3095kB дискового пространства.
Совершаем изменения...
Preparing...                ######################### [100%]
1: stardict-mueller7        ######################### [100%]
Running /usr/lib/rpm/posttrans-filetriggers
Завершено.
```

Команда

```
apt-get install имя_пакета
```

используется также и для обновления уже установленного пакета или группы пакетов. В этом случае **apt-get** дополнительно проверяет, есть ли обновлённая, в сравнении с установленной в системе, версия пакета в репозитории.

Например, если пакет *stardict-mueller7* установлен и в репозитории нет обновлённой версии этого пакета, то вывод команды **apt-get install stardict-mueller7** будет таким:

```
# apt-get install stardict-mueller7
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Последняя версия stardict-mueller7 уже установлена.
0 будет обновлено, 0 новых установлено, 0 пакетов будет удалено и 2262 не
будет обновлено.
```

При помощи **APT** можно установить и отдельный rpm- пакет, не входящий в состав репозиториев (например, полученный из сети Интернет). Для этого достаточно выполнить команду

```
# apt-get install /путь/к/файлу.rpm
```

При этом **APT** проведёт стандартную процедуру проверки зависимостей и конфликтов с уже установленными пакетами.

Иногда в результате операций с пакетами без использования **APT** целостность системы нарушается, и **apt-get** отказывается выполнять операции установки, удаления или обновления. В этом случае необходимо повторить операцию, задав опцию **-f**, заставляющую **apt-get** исправить нарушенные зависимости, удалить или заменить конфликтующие пакеты. В этом случае необходимо внимательно следить за сообщениями, выводимыми **apt-get**. Любые действия в этом режиме обязательно требуют подтверждения со стороны пользователя.

Глава 59. Удаление установленного пакета

Для удаления пакета используется команда **apt-get remove *имя_пакета***. Для того чтобы не нарушать целостность системы, будут удалены и все пакеты, зависящие от удаляемого. В случае удаления пакета, который относится к базовым компонентам системы, **apt-get** потребует дополнительное подтверждение с целью предотвращения возможной случайной ошибки.

Важно

Для удаления пакетов требуются привилегии администратора.

При попытке с помощью **apt-get** удалить базовый компонент системы, вы увидите следующий запрос на подтверждение операции:

```
# apt-get remove filesystem
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие пакеты будут УДАЛЕНЫ:
  ...
ВНИМАНИЕ: Будут удалены важные для работы системы пакеты
Обычно этого делать не следует. Вы должны точно понимать возможные
последствия!
  ...
0 будет обновлено, 0 новых установлено, 2648 пакетов будет удалено и 0 не
будет обновлено.
Необходимо получить 0B архивов.
После распаковки будет освобождено 8994MB дискового пространства.
Вы делаете нечто потенциально опасное!
Введите фразу 'Yes, do as I say!' чтобы продолжить.
```

Каждую ситуацию, в которой **APT** выдаёт такой запрос, необходимо рассматривать отдельно. Вероятность того, что после выполнения этой команды система окажется неработоспособной, очень велика.

Глава 60. Обновление системы

60.1. Обновление всех установленных пакетов

Для обновления всех установленных пакетов необходимо выполнить команды:

```
# apt-get update && apt-get dist-upgrade
```

Первая команда (**apt-get update**) обновит индексы пакетов. Вторая команда (**apt-get dist-upgrade**) позволяет обновить только те установленные пакеты, для которых в репозиториях, перечисленных в **/etc/apt/sources.list**, имеются новые версии.

Примечание

Несмотря на то, что команда **apt-get upgrade** существует, использовать её следует осторожно, либо не использовать вовсе.

Она позволяет обновить только те установленные пакеты, для которых в репозиториях, перечисленных в **/etc/apt/sources.list**, имеются новые версии.

Никакие другие пакеты при этой операции из системы удалены не будут. Этот способ полезен при работе со стабильными пакетами приложений, относительно которых известно, что они при смене версии изменяются несущественно.

Иногда, однако, происходит изменение в наименовании пакетов или изменение их зависимостей. Такие ситуации не обрабатываются командой **apt-get upgrade**, в результате чего происходит нарушение целостности системы: появляются неудовлетворённые зависимости. Для разрешения этой проблемы существует режим обновления в масштабе дистрибутива — **apt-get dist-upgrade**.

В случае обновления всего дистрибутива **APT** проведёт сравнение системы с репозиторием и удалит устаревшие пакеты, установит новые версии присутствующих в системе пакетов, отследит ситуации с переименованиями пакетов или изменения зависимостей между старыми и новыми версиями программ. Всё, что потребуется поставить (или удалить) дополнительно к уже имеющемуся в системе, будет указано в отчёте **apt-get**, которым **APT** предварит само обновление.

Примечание

Команда **apt-get dist-upgrade** обновит систему, но ядро ОС не будет обновлено.

60.2. Обновление ядра

Для обновления ядра ОС необходимо выполнить команду:

```
# update-kernel
```

Примечание

Если индексы сегодня еще не обновлялись перед выполнением команды **update-kernel** необходимо выполнить команду **apt-get update**.

Команда **update-kernel** обновляет и модули ядра, если в репозитории обновилось что-то из модулей без обновления ядра.

Новое ядро загрузится только после перезагрузки системы, которую рекомендуется выполнить немедленно.

Если с новым ядром что-то пойдёт не так, вы сможете вернуться к предыдущему варианту, выбрав его в начальном меню загрузчика.

После успешной загрузки на обновленном ядре можно удалить старое, выполнив команду:

```
# remove-old-kernels
```

Глава 61. Единая команда управления пакетами (epm)

Основное назначение единой команды управления пакетами — унифицировать управление пакетами в дистрибутивах с разными пакетными менеджерами. Утилита **epm** упрощает процедуру управления пакетами, может использоваться в скриптах и установщиках, сервисных программах, в повседневном администрировании различных систем. В **epm** добавлены типовые операции, которые в случае использования apt, потребовали бы ввода более одной команды.

Единая команда управления пакетами включает в себя следующую функциональность:

- управление пакетами (установка/удаление/поиск);
- управление репозиториями (добавление/удаление/обновление/список);
- управление системными сервисами (включение/выключение/список).

Список поддерживаемых пакетных менеджеров: rpm, deb, tgz, tbz, tbz2, apk, pkg.gz.

Примечание

Установка утилиты **epm**, если она еще не установлена, выполняется командой:

```
# apt-get install eepm
```

Подробную информацию об утилите **epm** и её опциях можно получить, выполнив команду:

```
$ epm --help
```

Ниже описаны лишь некоторые возможности утилиты **epm**.

Установка пакета из репозитория или из локального файла в систему:

```
epm install <имя_пакета>
```

Важно

Если пакет создан сторонним поставщиком, то при его установке командой **epm install** не будут выполнены установочные скрипты из пакета. Это предохраняет систему от повреждения, но может привести к тому, что пакет не заработает. Вернуть стандартное поведение можно добавлением **--scripts**:

```
epm install --scripts <имя_пакета>
```

Установить сторонние программы безопасным и простым способом:

```
epm play <имя_программы>
```

Список программ, которые можно установить данной командой, можно просмотреть, выполнив команду:

```
$ epm play
Run with a name of a play script to run:
  anydesk               - Install AnyDesk from the official site
  assistant             - Install Assistant (Ассистент) from the official site
  …
  yandex-browser        - Install Yandex browser from the official site
  yandex-disk           - Install Yandex Disk from the official site
  zoom                  - Install Zoom client from the official site
```

Команда **epm play** требует наличия доступа в сеть Интернет.

Примечание

Для некоторых сторонних rpm-пакетов, написаны дополнительные правила для перепаковки (при перепаковке пакета создаётся пакет, учитывающий, что нужно для работы исходного пакета). Установить такие пакеты можно, выполнив команду:

```
epm install --repack <имя_пакета>
```

Для deb-пакетов ключ **--repack** применяется автоматически.

Удаление пакета из системы:

```
epm remove <имя_пакета>
```

Поиск пакета в репозитории:

```
epm search <текст>
```

Получить список установленных пакетов:

```
$ epm list
```

Удалить пакеты, от которых не зависят какие-либо другие пакеты, установленные в системе:

```
# epm autoremove
```

Обновить все установленные пакеты и ядро ОС:

```
# epm full-upgrade
```

Примечание

Утилита **yum** (должен быть установлен пакет eepm-yum), позволяет имитировать работу менеджера пакетов yum, например:

```
$ yum search docs-alt-kworkstation
 $ apt-cache search -- docs-alt-kworkstation | egrep -i --color --
"(docs-alt-kworkstation)"
docs-alt-kworkstation - ALT KWorkstation documentation
```

Часть XI. Основы администрирования Linux

Содержание

Глава 62. Общие принципы работы ОС

62.1. Процессы и файлы

ОС Альт Сервер является многопользовательской интегрированной системой. Это значит, что она разработана в расчете на одновременную работу нескольких пользователей.

Пользователь может либо сам работать в системе, выполняя некоторую последовательность команд, либо от его имени могут выполняться прикладные процессы.

Пользователь взаимодействует с системой через командный интерпретатор. Командный интерпретатор представляет собой прикладную программу, которая принимает от пользователя команды или набор команд и транслирует их в системные вызовы к ядру системы. Интерпретатор позволяет пользователю просматривать файлы, передвигаться по дереву файловой системы, запускать прикладные процессы. Все командные интерпретаторы UNIX имеют развитый командный язык и позволяют писать достаточно сложные программы, упрощающие процесс администрирования системы и работы с ней.

62.1.1. Процессы функционирования ОС

Все программы, которые выполняются в текущий момент времени, называются процессами. Процессы можно разделить на два основных класса: системные процессы и пользовательские процессы.

Системные процессы — программы, решающие внутренние задачи ОС, например, организацию виртуальной памяти на диске или предоставляющие пользователям те или иные сервисы (процессы-службы).

Пользовательские процессы — процессы, запускаемые пользователем из командного интерпретатора для решения задач пользователя или управления системными процессами. Linux изначально разрабатывался как многозадачная система. Он использует технологии, опробованные и отработанные другими реализациями UNIX, которые существовали ранее.

Фоновый режим работы процесса — режим, когда программа может работать без взаимодействия с пользователем. В случае необходимости интерактивной работы с пользователем (в общем случае) процесс будет «остановлен» ядром, и работа его продолжается только после переведения его в «нормальный» режим работы.

62.1.2. Файловая система ОС

В ОС использована файловая система Linux, которая, в отличие от файловых систем DOS и Windows(™), является единым деревом. Корень этого дерева — каталог, называемый root (рут) и обозначаемый `/`.

Части дерева файловой системы могут физически располагаться в разных разделах разных дисков или вообще на других компьютерах — для пользователя это прозрачно. Процесс присоединения файловой системы раздела к дереву называется монтированием, удаление — размонтированием. Например, файловая система CD-ROM в дистрибутиве монтируется по умолчанию в каталог **`/media/cdrom`** (путь в дистрибутиве обозначается с использованием **/**, а не ****, как в DOS/Windows).

Текущий каталог обозначается **./**.

62.1.3. Структура каталогов

Корневой каталог `/`:

- **`/bin`** — командные оболочки (shell), основные утилиты;
- **`/boot`** — содержит ядро системы;
- **`/dev`** — псевдофайлы устройств, позволяющие работать с устройствами напрямую. Файлы в **`/dev`** создаются сервисом **`udev`**
- **`/etc`** — общесистемные конфигурационные файлы для большинства программ в системе;

- **/etc/rc?.d**, **/etc/init.d**, **/etc/rc.boot**, **/etc/rc.d** — каталоги, где расположены командные файлы, выполняемые при запуске системы или при смене её режима работы;
- **/etc/passwd** — база данных пользователей, в которой содержится информация об имени пользователя, его настоящем имени, личном каталоге, его зашифрованный пароль и другие данные;
- **/etc/shadow** — теневая база данных пользователей. При этом информация из файла **/etc/passwd** перемещается в **/etc/shadow**, который недоступен для чтения всем, кроме пользователя root. В случае использования альтернативной схемы управления теневыми паролями (TCB), все теневые пароли для каждого пользователя располагаются в каталоге **/etc/tcb/*имя пользователя*/shadow**;
- **/home** — домашние каталоги пользователей;
- **/lib** — содержит файлы динамических библиотек, необходимых для работы большей части приложений, и подгружаемые модули ядра;
- **/lost+found** — восстановленные файлы;
- **/media** — подключаемые носители (каталоги для монтирования файловых систем сменных устройств);
- **/mnt** — точки временного монтирования;
- **/opt** — вспомогательные пакеты;
- **/proc** — виртуальная файловая система, хранящаяся в памяти компьютера при загруженной ОС. В данном каталоге расположены самые свежие сведения обо всех процессах, запущенных на компьютере.
- **/root** — домашний каталог администратора системы;
- **/run** — файлы состояния приложений;
- **/sbin** — набор программ для административной работы с системой (системные утилиты);
- **/selinux** — виртуальная файловая система SELinux;
- **/srv** — виртуальные данные сервисных служб;
- **/sys** — файловая система, содержащая информацию о текущем состоянии системы;
- **/tmp** — временные файлы.
- **/usr** — пользовательские двоичные файлы и данные, используемые только для чтения (программы и библиотеки);
- **/var** — файлы для хранения изменяющихся данных (рабочие файлы программ, очереди, журналы).

Каталог **/usr**:

- **/usr/bin** — дополнительные программы для всех учетных записей;
- **/usr/sbin** — команды, используемые при администрировании системы и не предназначенные для размещения в файловой системе root;

- **`/usr/local`** — место, где рекомендуется размещать файлы, установленные без использования пакетных менеджеров, внутренняя организация каталогов практически такая же, как и корневого каталога;
- **`/usr/man`** — каталог, где хранятся файлы справочного руководства **man**;
- **`/usr/share`** — каталог для размещения общедоступных файлов большей части приложений.

Каталог **`/var`**:

- **`/var/log`** — место, где хранятся файлы аудита работы системы и приложений;
- **`/var/spool`** — каталог для хранения файлов, находящихся в очереди на обработку для того или иного процесса (очереди печати, непрочитанные или не отправленные письма, задачи cron т.д.).

62.1.4. Организация файловой структуры

Система домашних каталогов пользователей помогает организовывать безопасную работу пользователей в многопользовательской системе. Вне своего домашнего каталога пользователь обладает минимальными правами (обычно чтение и выполнение файлов) и не может нанести ущерб системе, например, удалив или изменив файл.

Кроме файлов, созданных пользователем, в его домашнем каталоге обычно содержатся персональные конфигурационные файлы некоторых программ.

Маршрут (путь) — это последовательность имён каталогов, представляющая собой путь в файловой системе к данному файлу, где каждое следующее имя отделяется от предыдущего наклонной чертой (слешем). Если название маршрута начинается со слеша, то путь в искомый файл начинается от корневого каталога всего дерева системы. В обратном случае, если название маршрута начинается непосредственно с имени файла, то путь к искомому файлу должен начаться от текущего каталога (рабочего каталога).

Имя файла может содержать любые символы за исключением косой черты (***/***). Однако следует избегать применения в именах файлов большинства знаков препинания и непечатаемых символов. При выборе имен файлов рекомендуется ограничиться следующими символами:

- **строчные** и **ПРОПИСНЫЕ** буквы. Следует обратить внимание на то, что регистр всегда имеет значение;
- символ подчеркивания (_);
- точка (**.**).

Для удобства работы точку можно использовать для отделения имени файла от расширения файла. Данная возможность может быть необходима пользователям или некоторым программам, но не имеет значение для shell.

62.1.5. Имена дисков и разделов

Все физические устройства вашего компьютера отображаются в каталог **`/dev`** файловой системы дистрибутива (об этом — ниже). Диски (в том числе IDE/SATA/SCSI/SAS жёсткие диски, USB-диски) имеют имена:

- **`/dev/sda`** — первый диск;

- **/dev/sdb** — второй диск;
- и т.д.

Диски обозначаются **/dev/sd*X***, где *X* — a, b, c, d, e, … в зависимости от порядкового номера диска на шине.

Раздел диска обозначается числом после его имени. Например, **/dev/sdb4** — четвертый раздел второго диска.

62.1.6. Разделы, необходимые для работы ОС

Для работы ОС на жестком диске (дисках) должны быть созданы, по крайней мере, два раздела: корневой (то есть тот, который будет содержать каталог **/**) и раздел подкачки (swap). Размер последнего, как правило, составляет от однократной до двукратной величины оперативной памяти компьютера. Если на диске много свободного места, то можно создать отдельные разделы для каталогов **/usr**, **/home**, **/var**.

62.2. Работа с наиболее часто используемыми компонентами

62.2.1. Виртуальная консоль

Система Альт Сервер предоставляет доступ к виртуальным консолям, с которых можно осуществлять одновременно несколько сеансов работы в системе (login session).

Только что установленная система Альт Сервер, возможно, предоставляет доступ только к первым шести виртуальным консолям, к которым можно обращаться, нажимая комбинации клавиш **Alt**+**F1** — **Alt**+**F6** (**Ctrl**+**Alt**+**F1** — **Ctrl**+**Alt**+**F6**).

62.2.2. Командные оболочки (интерпретаторы)

Для управления ОС используются командные интерпретаторы (shell).

Зайдя в систему, Вы увидите приглашение — строку, содержащую символ «**$**» (далее этот символ будет обозначать командную строку). Программа ожидает ваших команд. Роль командного интерпретатора — передавать ваши команды операционной системе. По своим функциям он соответствует **command.com** в DOS, но несравненно мощнее. При помощи командных интерпретаторов можно писать небольшие программы — сценарии (скрипты). В Linux доступны следующие командные оболочки:

- **bash** — самая распространенная оболочка под linux. Она ведет историю команд и предоставляет возможность их редактирования;
- **pdksh** — клон korn shell, хорошо известной оболочки в UNIX™ системах.

Проверить, какая оболочка используется в данный момент можно, выполнив команду:

```
$ echo $SHELL
```

Оболочкой по умолчанию является Bash (Bourne Again Shell) — самая распространённая оболочка под Linux, которая ведет историю команд и предоставляет возможность их редактирования. В дальнейшем описании работы с Альт Сервер будут использоваться примеры с использованием этой оболочки.

62.2.3. Командная оболочка Bash

В Bash имеется несколько приемов для работы со строкой команд. Например, можно использовать следующие сочетания:

- **Ctrl**+**A** — перейти на начало строки;
- **Ctrl**+**U** — удалить текущую строку;
- **Ctrl**+**C** — остановить текущую задачу.

Для ввода нескольких команд одной строкой можно использовать разделитель «**;**». По истории команд можно перемещаться с помощью клавиш ↑ («вверх») и ↓ («вниз»).

Чтобы найти конкретную команду в списке набранных, не пролистывая всю историю, можно нажать **Ctrl**+**R** и начать вводить символы ранее введенной команды.

Для просмотра истории команд можно воспользоваться командой **history**. Команды, присутствующие в истории, отображаются в списке пронумерованными. Чтобы запустить конкретную команду необходимо набрать:

```
!номер команды
```

Если ввести:

```
!!
```

запустится последняя из набранных команд.

В Bash имеется возможность самостоятельного завершения имен команд из общего списка команд, что облегчает работу при вводе команд, в случае, если имена программ и команд слишком длинны. При нажатии клавиши **Tab** Bash завершает имя команды, программы или каталога, если не существует нескольких альтернативных вариантов. Например, чтобы использовать программу декомпрессии **gunzip**, можно набрать следующую команду:

```
gu
```

Затем нажать клавишу **Tab**. Так как в данном случае существует несколько возможных вариантов завершения команды, то необходимо повторно нажать клавишу **Tab**, чтобы получить список имен, начинающихся с **gu**.

В предложенном примере можно получить следующий список:

```
$ gu
guile gunzip gupnp-binding-tool
```

Если набрать: **n** (**gunzip** — это единственное имя, третьей буквой которого является «**n**»), а затем нажать клавишу **Tab**, то оболочка самостоятельно дополнит имя. Чтобы запустить команду нужно нажать **Enter**.

Программы, вызываемые из командной строки, Bash ищет в каталогах, определяемых в системной переменной **$PATH**. По умолчанию в этот перечень каталогов не входит текущий каталог, обозначаемый **./** (точка слеш) (если только не выбран один из двух самых слабых уровней защиты). Поэтому, для запуска программы из текущего каталога, необходимо использовать команду (в примере запускается команда **prog**):

```
./prog
```

62.2.4. Команда

Простейшая команда состоит из одного «слова», например, команда **cal**, выводящая календарь на текущий месяц.

```
 $ cal
     Май 2021
Пн Вт Ср Чт Пт Сб Вс
                1  2
 3  4  5  6  7  8  9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
31
```

62.2.5. Команда и параметры

```
 $ cal 1 2022
     Январь 2022
Пн Вт Ср Чт Пт Сб Вс
                1  2
 3  4  5  6  7  8  9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
31
```

Команда **cal 1 2022** состоит из двух частей — собственно команды **cal** и «остального». То, что следует за командой называется *параметрами* (или аргументами) и они вводятся для изменения поведения команды. В большинстве случаев, первое слово считается именем команды, а остальные — её параметрами.

62.2.6. Команда и ключи

Для решения разных задач одни и те же действия необходимо выполнять по-разному. Например, для синхронизации работ в разных точках земного шара лучше использовать единое для всех время (по Гринвичу), а для организации собственного рабочего дня — местное время (с учётом сдвига по часовому поясу и разницы зимнего и летнего времени). И то, и другое время показывает команда **date**, только для работы по Гринвичу ей нужен дополнительный параметр ***-u*** (он же ***--universal***).

```
$ date
Ср мая 5 11:57:57 EET 2021
$ date -u
Ср мая 5 09:58:04 UTC 2021
```

Такого рода параметры называются *ключами* или *модификаторами выполнения*. Ключ принадлежит данной конкретной команде и сам по себе смысла не имеет. Этим он отличается от других параметров (например, имён файлов, чисел), имеющих собственный смысл, не зависящий ни от какой команды. Каждая команда может распознавать некоторый набор ключей и соответственно изменять своё поведение. Один и тот же ключ может определять для разных команд совершенно разные значения.

Для формата ключей нет жёсткого стандарта, однако существуют договорённости:

- Если ключ начинается на -, то это *однобуквенный ключ*. За -, как правило, следует один символ, чаще всего буква, обозначающая действие или свойство, которое этот ключ придаёт команде. Так проще отличать ключи от других параметров.
- Если ключ начинается на --, то он называется *полнословным ключом*. Полнословный формат ключа начинается на два знака --, за которыми следует полное имя обозначаемого этим ключом содержания.

Некоторые ключи имеют и однобуквенный, и полнословный формат, а некоторые — только полнословный.

Информацию о ресурсах каждой команды можно получить, используя ключ ***--help***. К примеру, получить подсказку о том, что делает команда **rm**, можно, набрав в терминале **rm *--help***.

62.2.7. Обзор основных команд системы

Все команды, приведенные ниже, могут быть запущены в режиме консоли. Для получения более подробной информации используйте команду **man**. Пример:

```
$ man ls
```

Примечание

Параметры команд обычно начинаются с символа «-», и обычно после одного символа «-» можно указать сразу несколько опций. Например, вместо команды **ls -l -F** можно ввести команду **ls -lF**

Учетные записи пользователей

Команда su

Команда **su** позволяет изменить «владельца» текущего сеанса (сессии) без необходимости завершать сеанс и открывать новый.

Синтаксис:

```
su [ОПЦИИ...] [ПОЛЬЗОВАТЕЛЬ]
```

Команду можно применять для замены текущего пользователя на любого другого, но чаще всего она используется для получения пользователем прав суперпользователя (root).

При вводе команды **su -**, будет запрошен пароль суперпользователя (root), и, в случае ввода корректного пароля, пользователь получит права администратора. Чтобы вернуться к правам пользователя, необходимо ввести команду:

```
exit
```

Более подробную информацию о режиме суперпользователя вы можете прочитать в главе Режим суперпользователя

Команда id

Команда **id** выводит информацию о пользователе и группах, в которых он состоит для заданного пользователя или о текущем пользователе (если ничего не указано).

Синтаксис:

```
id [ОПЦИИ...] [ПОЛЬЗОВАТЕЛЬ]
```

Команда passwd

Команда **passwd** меняет (или устанавливает) пароль, связанный с входным_именем пользователя.

Обычный пользователь может менять только пароль, связанный с его собственным входным_именем.

Команда запрашивает у обычных пользователей старый пароль (если он был), а затем дважды запрашивает новый. Новый пароль должен соответствовать техническим требованиям к паролям, заданным администратором системы.

Основные операции с файлами и каталогами

Команда ls

Команда **ls** (list) печатает в стандартный вывод содержимое каталогов.

Синтаксис:

```
ls [ОПЦИИ...] [ФАЙЛ...]
```

Основные опции:

- **-a** — просмотр всех файлов, включая скрытые;
- **-l** — отображение более подробной информации;
- **-R** — выводить рекурсивно информацию о подкаталогах.

Команда cd

Команда **cd** предназначена для смены каталога. Команда работает как с абсолютными, так и с относительными путями. Если каталог не указан, используется значение переменной окружения **$HOME** (домашний каталог пользователя). Если каталог задан полным маршрутным именем, он становится текущим. По отношению к новому каталогу нужно иметь право на выполнение, которое в данном случае трактуется как разрешение на поиск.

Синтаксис:

```
cd [-L|-P] [КАТАЛОГ]
```

Если в качестве аргумента задано «-», то это эквивалентно **$OLDPWD**. Если переход был осуществлен по переменной окружения **$CDPATH** или в качестве аргумента был задан «-» и смена каталога была успешной, то абсолютный путь нового рабочего каталога будет выведен на стандартный вывод.

Пример. Находясь в домашнем каталоге перейти в его подкаталог **docs/** (относительный путь):

```
cd docs/
```

Сделать текущим каталог **/usr/bin** (абсолютный путь):

```
cd /usr/bin/
```

Сделать текущим родительский каталог:

```
cd ..
```

Вернуться в предыдущий каталог:

```
cd -
```

Сделать текущим домашний каталог:

```
cd
```

Команда pwd

Команда **pwd** выводит абсолютный путь текущего (рабочего) каталога.

Синтаксис:

```
pwd [-L|-P]
```

Опции:

- **-P** — не выводить символические ссылки;
- **-L** — выводить символические ссылки.

Команда rm

Команда **rm** служит для удаления записей о файлах. Если заданное имя было последней ссылкой на файл, то файл уничтожается.

Предупреждение

Удалив файл, вы не сможете его восстановить!

Синтаксис:

```
rm [ОПЦИИ...] <ФАЙЛ>
```

Основные опции:

- **-f** — никогда не запрашивать подтверждения;
- **-i** — всегда запрашивать подтверждение;
- **-r, -R** — рекурсивно удалять содержимое указанных каталогов.

Пример. Удалить все файлы **html** в каталоге **~/html**:

```
rm -i ~/html/*.html
```

Команда mkdir

mkdir — команда для создания новых каталогов.

Синтаксис:

```
mkdir [-p] [-m права] <КАТАЛОГ...>
```

Команда rmdir

Команда **rmdir** удаляет каталоги из файловой системы. Каталог должен быть пуст перед удалением.

Синтаксис:

```
rmdir [ОПЦИИ] <КАТАЛОГ...>
```

Основные опции:

- **-p** — удалить каталог и его потомки.

Команда **rmdir** часто заменяется командой **rm -rf**, которая позволяет удалять каталоги, даже если они не пусты.

Команда cp

Команда **cp** предназначена для копирования файлов из одного в другие каталоги.

Синтаксис:

```
cp [-fip] [ИСХ_ФАЙЛ...] [ЦЕЛ_ФАЙЛ...]
```

```
cp [-fip] [ИСХ_ФАЙЛ...] [КАТАЛОГ]
```

```
cp [-R] [[-H] | [-L] | [-P]] [-fip] [ИСХ_ФАЙЛ...] [КАТАЛОГ]
```

Основные опции:

- **-p** — сохранять по возможности времена изменения и доступа к файлу, владельца и группу, права доступа;
- **-i** — запрашивать подтверждение перед копированием в существующие файлы;
- **-r, -R** — рекурсивно копировать содержимое каталогов.

Команда mv

Команда **mv** предназначена для перемещения файлов.

Синтаксис:

```
mv [-fi] [ИСХ_ФАЙЛ...] [ЦЕЛ_ФАЙЛ...]
```

```
mv [-fi] [ИСХ_ФАЙЛ...] [КАТАЛОГ]
```

В первой синтаксической форме, характеризующейся тем, что последний операнд не является ни каталогом, ни символической ссылкой на каталог, **mv** перемещает исх_файл в цел_файл (происходит переименование файла).

Во второй синтаксической форме **mv** перемещает исходные файлы в указанный каталог под именами, совпадающими с краткими именами исходных файлов.

Основные опции:

- **-f** — не запрашивать подтверждения перезаписи существующих файлов;
- **-i** — запрашивать подтверждение перезаписи существующих файлов.

Команда cat

Команда **cat** последовательно выводит содержимое файлов.

Синтаксис:

```
cat [ОПЦИИ] [ФАЙЛ...]
```

Основные опции:

- **-n, --number** — нумеровать все строки при выводе;
- **-E, --show-ends** — показывать $ в конце каждой строки.

Если файл не указан, читается стандартный ввод. Если в списке файлов присутствует имя «-», вместо этого файла читается стандартный ввод.

Команда head

Команда **head** выводит первые 10 строк каждого файла на стандартный вывод.

Синтаксис:

```
head [ОПЦИИ] [ФАЙЛ...]
```

Основные опции:

- **`-n, --lines=[-]K`** — вывести первые K строк каждого файла, а не первые 10;
- **`-q, --quiet`** — не печатать заголовки с именами файлов.

Команда `less`

Команда **`less`** позволяет постранично просматривать текст (для выхода необходимо нажать **`q`**).

Синтаксис:

```
less ФАЙЛ
```

Команда `grep`

Команда **`grep`** имеет много опций и предоставляет возможности поиска символьной строки в файле.

Синтаксис:

```
grep [шаблон_поиска] ФАЙЛ
```

Команда `chmod`

Команда **`chmod`** предназначена для изменения прав доступа файлов и каталогов.

Синтаксис:

```
chmod [ОПЦИИ] РЕЖИМ[,РЕЖИМ]... <ФАЙЛ>
```

```
chmod [ОПЦИИ] --reference=ИФАЙЛ <ФАЙЛ>
```

Основные опции:

- **`-R`** — рекурсивно изменять режим доступа к файлам, расположенным в указанных каталогах;
- **`--reference=ИФАЙЛ`** — использовать режим файла ИФАЙЛ.

`chmod` изменяет права доступа каждого указанного файла в соответствии с правами доступа, указанными в параметре режим, который может быть представлен как в символьном виде, так и в виде восьмеричного, представляющего битовую маску новых прав доступа.

Формат символьного режима следующий:

```
[ugoa...][[+-=][разрешения...]...]
```

Здесь разрешения — это ноль или более букв из набора «rwxXst» или одна из букв из набора «ugo».

Каждый аргумент — это список символьных команд изменения прав доступа, разделены запятыми. Каждая такая команда начинается с нуля или более букв «ugoa», комбинация которых указывает, чьи права доступа к файлу будут изменены: пользователя, владеющего файлом (u), пользователей, входящих в группу, к которой принадлежит файл (g), остальных пользователей (o) или всех пользователей (a). Если не задана ни одна буква, то автоматически будет использована буква «a», но биты, установленные в umask, не будут затронуты.

Оператор «+» добавляет выбранные права доступа к уже имеющимся у каждого файла, «-» удаляет эти права. «=» присваивает только эти права каждому указанному файлу.

Буквы «rwxXst» задают биты доступа для пользователей: «r» — чтение, «w» — запись, «x» — выполнение (или поиск для каталогов), «X» — выполнение/поиск только если это каталог или же файл с уже установленным битом выполнения, «s» — задать ID пользователя и группы при выполнении, «t» — запрет удаления.

Примеры. Позволить всем выполнять файл **f2**:

```
chmod +x f2
```

Запретить удаление файла **f3**:

```
chmod +t f3
```

Команда chown

Команда **chown** изменяет владельца и/или группу для каждого заданного файла.

Синтаксис:

```
chown [КЛЮЧ]…[ВЛАДЕЛЕЦ][:[ГРУППА]] <ФАЙЛ>
```

Изменить владельца может только владелец файла или суперпользователь. Владелец не изменяется, если он не задан в аргументе. Группа также не изменяется, если не задана, но если после символьного ВЛАДЕЛЬЦА стоит символ «:», подразумевается изменение группы на основную группу текущего пользователя. Поля ВЛАДЕЛЕЦ и ГРУППА могут быть как числовыми, так и символьными.

Примеры. Поменять владельца каталога **/u** на пользователя test:

```
chown test /u
```

Поменять владельца и группу каталога **/u**:

```
chown test:staff /u
```

Поменять владельца каталога **/u** и вложенных файлов на test:

```
chown -hR test /u
```

Поиск файлов

Команда find

Команда **find** предназначена для поиска всех файлов, начиная с корневого каталога. Поиск может осуществляться по имени, типу или владельцу файла.

Синтаксис:

```
find [-H] [-L] [-P] [-Оуровень] [-D help|tree|search|stat|rates|opt|
exec] [ПУТЬ…] [ВЫРАЖЕНИЕ]
```

Ключи для поиска:

- **-name** — поиск по имени файла;
- **-type** — поиск по типу f=файл, d=каталог, l=ссылка(lnk);
- **-user** — поиск по владельцу (имя или UID).

Когда выполняется команда **find**, можно выполнять различные действия над найденными файлами. Основные действия:

- **-exec команда \;** — выполнить команду. Запись команды должна заканчиваться экранированной точкой с запятой. Строка «{}» заменяется текущим маршрутным именем файла;
- **execdir команда \;** — то же самое что и **-exec**, но команда вызывается из подкаталога, содержащего текущий файл;
- **-ok команда** — эквивалентно **-exec** за исключением того, что перед выполнением команды запрашивается подтверждение (в виде сгенерированной командной строки со знаком вопроса в конце) и она выполняется только при ответе: y;
- **-print** — вывод имени файла на экран.

Путем по умолчанию является текущий подкаталог. Выражение по умолчанию **-print**.

Примеры. Найти в текущем каталоге обычные файлы (не каталоги), имя которых начинается с символа «~»:

```
find . -type f -name "~*" -print
```

Найти в текущем каталоге файлы, измененные позже, чем файл **file.bak**:

```
find . -newer file.bak -type f -print
```

Удалить все файлы с именами **a.out** или ***.o**, доступ к которым не производился в течение недели:

```
find / \( -name a.out -o -name '*.o' \) \ -atime +7 -exec rm {} \;
```

Удалить из текущего каталога и его подкаталогов все файлы нулевого размера, запрашивая подтверждение:

```
find . -size 0c -ok rm {} \;
```

Команда whereis

whereis сообщает путь к исполняемому файлу программы, ее исходным файлам (если есть) и соответствующим страницам справочного руководства.

Синтаксис:

```
whereis [опции] <имя>
```

Опции:

- **-b** — вывод информации только об исполняемых файлах;
- **-m** — вывод информации только о страницах справочного руководства;
- **-s** — вывод информации только об исходных файлах.

Мониторинг и управление процессами

Команда ps

Команда **ps** отображает список текущих процессов.

Синтаксис:

```
ps [опции]
```

По умолчанию выводится информация о процессах с теми же действующим UID и управляющим терминалом, что и у подающего команду пользователя.

Основные опции:

- **-a** — вывести информацию о процессах, ассоциированных с терминалами;
- **-f** — вывести «полный» список;
- **-l** — вывести «длинный» список;
- **-p список** — вывести информацию о процессах с перечисленными в списке PID;
- **-u список** — вывести информацию о процессах с перечисленными идентификаторами или именами пользователей.

Команда kill

Команда **kill** позволяет прекратить исполнение процесса или передать ему сигнал.

Синтаксис:

```
kill [-s] [сигнал] [идентификатор] [...]
```

```
kill [-l] [статус_завершения]
```

```
kill [-номер_сигнала] [идентификатор] [...]
```

Идентификатор — PID ведущего процесса задания или номер задания, предварённый знаком «%».

Основные опции:

- **`-l`** — вывести список поддерживаемых сигналов;
- **`-s сигнал, -сигнал`** — послать сигнал с указанным именем.

Если обычная команда **`kill`** не дает желательного эффекта, необходимо использовать команду **`kill`** с параметром **`-9`** (**`kill -9`** *PID_номер*).

Команда `df`

Команда **`df`** показывает количество доступного дискового пространства в файловой системе, в которой содержится файл, переданный как аргумент. Если ни один файл не указан, показывается доступное место на всех смонтированных файловых системах. Размеры по умолчанию указаны в блоках по 1КБ.

Синтаксис:

```
df [ОПЦИИ] [ФАЙЛ...]
```

Основные опции:

- **`--total`** — подсчитать общий объем в конце;
- **`-h, --human-readable`** — печатать размеры в удобочитаемом формате (например, 1K, 234M, 2G).

Команда `du`

Команда **`du`** подсчитывает использование диска каждым файлом, для каталогов подсчет происходит рекурсивно.

Синтаксис:

```
du [ОПЦИИ] [ФАЙЛ...]
```

Основные опции:

- **`-a, --all`** — выводить общую сумму для каждого заданного файла, а не только для каталогов;
- **`-c, --total`** — подсчитать общий объем в конце. Может быть использовано для выяснения суммарного использования дискового пространства для всего списка заданных файлов;
- **`-d, --max-depth=N`** — выводить объем для каталога (или файлов, если указано **`--all`**) только если она на N или менее уровней ниже аргументов командной строки;
- **`-S, --separate-dirs`** — выдавать отдельно размер каждого каталога, не включая размеры подкаталогов;
- **`-s, --summarize`** — отобразить только сумму для каждого аргумента.

Команда `which`

Команда **`which`** отображает полный путь к указанным командам или сценариям.

Синтаксис:

```
which [ОПЦИИ] <ФАЙЛ...>
```

Основные опции:

- **-a, --all** — выводит все совпавшие исполняемые файлы по содержимому в переменной окружения **$PATH**, а не только первый из них;
- **-c, --total** — подсчитать общий объем в конце. Может быть использовано для выяснения суммарного использования дискового пространства для всего списка заданных файлов;
- **-d, --max-depth=N** — выводить объем для каталога (или файлов, если указано **--all**) только если она на N или менее уровней ниже аргументов командной строки;
- **-S, --separate-dirs** — выдавать отдельно размер каждого каталога, не включая размеры подкаталогов;
- **--skip-dot** — пропускает все каталоги из переменной окружения **$PATH**, которые начинаются с точки.

Использование многозадачности

Альт Сервер — это многозадачная система.

Для того, чтобы запустить программу в фоновом режиме, необходимо набрать «**&**» после имени программы. После этого оболочка даст возможность запускать другие приложения.

Так как некоторые программы интерактивны — их запуск в фоновом режиме бессмысленен. Подобные программы просто остановятся, если их запустить в фоновом режиме.

Можно также запускать нескольких независимых сеансов. Для этого в консоли необходимо набрать **Alt** и одну из клавиш, находящихся в интервале от **F1** до **F6**. На экране появится новое приглашение системы, и можно открыть новый сеанс. Этот метод также позволяет вам работать на другой консоли, если консоль, которую вы использовали до этого, не отвечает или вам необходимо остановить зависшую программу.

Команда bg

Команда **bg** позволяет перевести задание на задний план.

Синтаксис:

```
bg [ИДЕНТИФИКАТОР ...]
```

Идентификатор — PID ведущего процесса задания или номер задания, предварённый знаком «%».

Команда fg

Команда **fg** позволяет перевести задание на передний план.

Синтаксис:

```
fg [ИДЕНТИФИКАТОР ...]
```

Идентификатор — PID ведущего процесса задания или номер задания, предварённый знаком «%».

Сжатие и упаковка файлов

Команда `tar`

Сжатие и упаковка файлов выполняется с помощью команды **`tar`**, которая преобразует файл или группу файлов в архив без сжатия (tarfile).

Упаковка файлов в архив чаще всего выполняется следующей командой:

```
tar -cf [имя создаваемого файла архива] [упаковываемые файлы и/или каталоги]
```

Пример использования команды упаковки архива:

```
tar -cf moi_dokumenti.tar Docs project.tex
```

Распаковка содержимого архива в текущий каталог выполняется командой:

```
tar -xf [имя файла архива]
```

Для сжатия файлов используются специальные программы сжатия: **`gzip`**, **`bzip2`** и **`7z`**.

62.3. Стыкование команд в системе Linux

62.3.1. Стандартный ввод и стандартный вывод

Многие команды системы имеют так называемые стандартный ввод (standard input) и стандартный вывод (standard output), часто сокращаемые до stdin и stdout. Ввод и вывод здесь — это входная и выходная информация для данной команды. Программная оболочка делает так, что стандартным вводом является клавиатура, а стандартным выводом — экран монитора.

Пример с использованием команды **`cat`**. По умолчанию команда **`cat`** читает данные из всех файлов, которые указаны в командной строке, и посылает эту информацию непосредственно в стандартный вывод (stdout). Следовательно, команда:

```
cat history-final masters-thesis
```

выведет на экран сначала содержимое файла **`history-final`**, а затем — файла **`masters-thesis`**.

Если имя файла не указано, программа **`cat`** читает входные данные из stdin и возвращает их в stdout. Пример:

```
cat
Hello there.
Hello there.
Bye.
Bye.
Ctrl-D
```

Каждую строку, вводимую с клавиатуры, программа **cat** немедленно возвращает на экран. При вводе информации со стандартного ввода конец текста сигнализируется вводом специальной комбинации клавиш, как правило, **Ctrl**+**D**. Сокращённое название сигнала конца текста — EOT (end of text).

62.3.2. Перенаправление ввода и вывода

При необходимости можно перенаправить стандартный вывод, используя символ >, и стандартный ввод, используя символ <.

Фильтр (filter) — программа, которая читает данные из стандартного ввода, некоторым образом их обрабатывает и результат направляет на стандартный вывод. Когда применяется перенаправление, в качестве стандартного ввода и вывода могут выступать файлы. Как указывалось выше, по умолчанию, stdin и stdout относятся к клавиатуре и к экрану соответственно. Программа **sort** является простым фильтром — она сортирует входные данные и посылает результат на стандартный вывод. Совсем простым фильтром является программа **cat** — она ничего не делает с входными данными, а просто пересылает их на выход.

62.3.3. Использование состыкованных команд

Стыковку команд (pipelines) осуществляет командная оболочка, которая stdout первой команды направляет на stdin второй команды. Для стыковки используется символ |. Направить stdout команды **ls** на stdin команды **sort**:

```
ls | sort -r
notes
masters-thesis
history-final
english-list
```

Вывод списка файлов частями:

```
ls /usr/bin | more
```

Если необходимо вывести на экран последнее по алфавиту имя файла в текущем каталоге, можно использовать следующую команду:

```
ls | sort -r | head -1 notes
```

где команда **head -1** выводит на экран первую строку получаемого ей входного потока строк (в примере поток состоит из данных от команды **ls**), отсортированных в обратном алфавитном порядке.

62.3.4. Недеструктивное перенаправление вывода

Эффект от использования символа > для перенаправления вывода файла является деструктивным; т.е, команда

```
ls > file-list
```

уничтожит содержимое файла **`file-list`**, если этот файл ранее существовал, и создаст на его месте новый файл. Если вместо этого перенаправление будет сделано с помощью символов >>, то вывод будет приписан в конец указанного файла, при этом исходное содержимое файла не будет уничтожено.

Примечание

Перенаправление ввода и вывода и стыкование команд осуществляется командными оболочками, которые поддерживают использование символов >, >> и |. Сами команды не способны воспринимать и интерпретировать эти символы.

Глава 63. Режим суперпользователя

63.1. Какие бывают пользователи?

Linux — система многопользовательская, а потому пользователь — ключевое понятие для организации всей системы доступа в Linux. Файлы всех пользователей в Linux хранятся раздельно, у каждого пользователя есть собственный домашний каталог, в котором он может хранить свои данные. Доступ других пользователей к домашнему каталогу пользователя может быть ограничен.

Суперпользователь в Linux — это выделенный пользователь системы, на которого не распространяются ограничения прав доступа. Именно суперпользователь имеет возможность произвольно изменять владельца и группу файла. Ему открыт доступ на чтение и запись к любому файлу или каталогу системы.

Среди учётных записей Linux всегда есть учётная запись суперпользователя — **root**. Поэтому вместо «суперпользователь» часто говорят «root». Множество системных файлов принадлежат **root**, множество файлов только ему доступны для чтения или записи. Пароль этой учётной записи — одна из самых больших драгоценностей системы. Именно с её помощью системные администраторы выполняют самую ответственную работу.

63.2. Для чего может понадобиться режим суперпользователя?

Системные утилиты, например, такие, как **Центр управления системой** или **Программа управления пакетами Synaptic** требуют для своей работы привилегий суперпользователя, потому что они вносят изменения в системные файлы. При их запуске выводится диалоговое окно с запросом пароля системного администратора.

63.3. Как получить права суперпользователя?

Для опытных пользователей, умеющих работать с командной строкой, существует два различных способа получить права суперпользователя.

Первый — это зарегистрироваться в системе под именем **root**.

Второй способ — воспользоваться специальной утилитой **su** (shell of user), которая позволяет выполнить одну или несколько команд от лица другого пользователя. По умолчанию эта утилита выполняет команду **sh** от пользователя **root**, то есть запускает командный интерпретатор. Отличие от предыдущего способа в том, что всегда известно, кто именно запускал **su**, а значит, ясно, кто выполнил определённое административное действие.

В некоторых случаях удобнее использовать не **su**, а утилиту **sudo**, которая позволяет выполнять только заранее заданные команды.

Важно

Для того чтобы воспользоваться командами **su** и **sudo**, необходимо быть членом группы **wheel**. Пользователь, созданный при установке системы, по умолчанию уже включён в эту группу.

В дистрибутивах Альт для управления доступом к важным службам используется подсистема control. control — механизм переключения между неким набором фиксированных состояний для задач, допускающих такой набор.

Команда **control** доступна только для суперпользователя (root). Для того, чтобы посмотреть, что означает та или иная политика **control** (разрешения выполнения конкретной команды, управляемой **control**), надо запустить команду с ключом help:

```
# control su help
```

Запустив **control** без параметров, можно увидеть полный список команд, управляемых командой (facilities) вместе с их текущим состоянием и набором допустимых состояний.

63.4. Как перейти в режим суперпользователя?

Для перехода в режим суперпользователя наберите в терминале команду **su -**.

Если воспользоваться командой **su** без ключа, то происходит вызов командного интерпретатора с правами **root**. При этом значение переменных окружения, в частности **$PATH**, остаётся таким же, как у пользователя: в переменной **$PATH** не окажется каталогов **/sbin**, **/usr/sbin**, без указания полного имени будут недоступны команды **route**, **shutdown**, **mkswap** и другие. Более того, переменная **$HOME** будет указывать на каталог пользователя, все программы, запущенные в режиме суперпользователя, сохранят свои настройки с правами **root** в каталоге пользователя, что в дальнейшем может вызвать проблемы.

Чтобы избежать этого, следует использовать **su -**. В этом режиме **su** запустит командный интерпретатор в качестве login shell, и он будет вести себя в точности так, как если бы в системе зарегистрировался **root**.

Глава 64. Управление пользователями

64.1. Общая информация

Пользователи и группы внутри системы обозначаются цифровыми идентификаторами — UID и GID, соответственно.

Пользователь может входить в одну или несколько групп. По умолчанию он входит в группу, совпадающую с его именем. Чтобы узнать, в какие еще группы входит пользователь, введите команду **id**, вывод её может быть примерно следующим:

```
uid=500(test) gid=500(test) группы=500(test),16(rpm)
```

Такая запись означает, что пользователь *test* (цифровой идентификатор 500) входит в группы *test* и *rpm*. Разные группы могут иметь разный уровень доступа к тем или иным каталогам; чем в большее количество групп входит пользователь, тем больше прав он имеет в системе.

Примечание

В связи с тем, что большинство привилегированных системных утилит в дистрибутивах Альт имеют не SUID-, а SGID-бит, будьте предельно внимательны и осторожны в переназначении групповых прав на системные каталоги.

64.2. Команда passwd

Команда passwd поддерживает традиционные опции **passwd** и утилит **shadow**.

Синтаксис:

```
passwd [ОПЦИИ...] [ИМЯ ПОЛЬЗОВАТЕЛЯ]
```

Возможные опции:

- **-d --delete** — удалить пароль для указанной записи;
- **-f**, **--force** — форсировать операцию;
- **-k**, **--keep-tokens** — сохранить не устаревшие пароли;
- **-l**, **--lock** — блокировать указанную запись;

- **--stdin** — прочитать новые пароли из стандартного ввода;
- **-S**, **--status** — дать отчет о статусе пароля в указанной записи;
- **-u**, **--unlock** — разблокировать указанную запись;
- **-?**, **--help** — показать справку и выйти;
- **--usage** — дать короткую справку по использованию;
- **-V**, **--version** — показать версию программы и выйти.

Код выхода: при успешном завершении **passwd** заканчивает работу с кодом выхода *0*. Код выхода *1* означает, что произошла ошибка. Текстовое описание ошибки выводится на стандартный поток ошибок.

Пользователь может в любой момент поменять свой пароль. Единственное,что требуется для смены пароля знать текущий пароль.

Только суперпользователь может обновить пароль другого пользователя.

64.3. Добавления нового пользователя

Для добавления нового пользователя используйте команды **useradd** и **passwd**:

```
# useradd test1

# passwd test1
passwd: updating all authentication tokens for user test1.

You can now choose the new password or passphrase.

A valid password should be a mix of upper and lower case letters,
digits, and other characters.  You can use an 8 character long
password with characters from at least 3 of these 4 classes, or
a 7 character long password containing characters from all the
classes.  An upper case letter that begins the password and a
digit that ends it do not count towards the number of character
classes used.

A passphrase should be of at least 3 words, 11 to 40 characters
long, and contain enough different characters.

Alternatively, if no one else can see your terminal now, you can
pick this as your password: "holder5dinghy-Arm".

Enter new password:
```

В результате описанных действий в системе появился пользователь *test1* с некоторым паролем. Если пароль оказался слишком слабым с точки зрения системы, она об этом предупредит (как в примере выше). Пользователь в дальнейшем может поменять свой пароль при помощи команды **passwd** — но если он попытается поставить слабый пароль, система откажет ему (в отличие от *root*) в изменении.

В Альт Сервер для проверки паролей на слабость используется модуль PAM *passwdqc*.

Программа **useradd** имеет множество параметров, которые позволяют менять её поведение по умолчанию. Например, можно принудительно указать, какой будет UID или какой группе будет принадлежать пользователь.

64.4. Модификация пользовательских записей

Для модификации пользовательских записей применяется утилита **usermod**:

```
# usermod -G audio,rpm,test1 test1
```

Такая команда изменит список групп, в которые входит пользователь *test1* — теперь это *audio*, *rpm*, *test1*.

```
# usermod -l test2 test1
```

Будет произведена смена имени пользователя с *test1* на *test2*.

Команды **usermod -L *test2*** и **usermod -U *test2*** соответственно временно блокируют возможность входа в систему пользователю *test2* и возвращают всё на свои места.

Изменения вступят в силу только при следующем входе пользователя в систему.

При неинтерактивной смене или задании паролей для целой группы пользователей используйте утилиту **chpasswd**. На стандартный вход ей следует подавать список, каждая строка которого будет выглядеть как ***имя:пароль***.

64.5. Удаление пользователей

Для удаления пользователей используйте **userdel**.

Команда **userdel *test2*** удалит пользователя *test2* из системы. Если будет дополнительно задан параметр **-r**, то будет уничтожен и домашний каталог пользователя. Нельзя удалить пользователя, если в данный момент он еще работает в системе.

Глава 65. Система инициализации systemd и sysvinit

65.1. Запуск операционной системы

65.1.1. Запуск системы

Алгоритм запуска компьютера приблизительно такой:

1. BIOS компьютера.
2. Загрузчик системы (например, LILO, GRUB или другой). В загрузчике вы можете задать параметры запуска системы или выбрать систему для запуска.
3. Загружается ядро Linux.
4. Запускается на выполнение первый процесс в системе — init.

Ядром запускается самая первая программа в системе **init**. Её задачей является запуск новых процессов и повторный запуск завершившихся. Вы можете посмотреть, где расположился **init** в иерархии процессов вашей системы, введя команду **`pstree`**.

От конфигурации **init** зависит, какая система инициализации будет использована.

65.1.2. Система инициализации

Система инициализации — это набор скриптов, которые будут выполнены при старте системы.

Существуют разные системы инициализации, наиболее популярной системой являются **sysvinit** и ее модификации. **systemd** разрабатывается как замена для **sysVinit**.

В Альт Сервер используется **sysvinit** (от System V init).

65.2. Системы инициализации systemd и sysvinit

65.2.1. sysvinit

System V — классическая схема инициализации, на которой базируются многие дистрибутивы. Привычна и довольно проста для понимания: **init** описывает весь процесс загрузки в своем конфигурационном файле **`/etc/inittab`**, откуда вызываются другие программы и скрипты на определенном этапе запуска.

65.2.2. systemd

systemd является альтернативной системой инициализации Linux, вобравшей в себя достоинства классического **System V init** и более современных **launchd** (OS X), **SMF** (Solaris) и **Upstart** (Ubuntu, Fedora), но при этом лишенной многих их недостатков. Он разрабатывался для обеспечения лучшего выражения зависимостей между службами, что позволяет делать одновременно больше работы при загрузке системы, и уменьшить время загрузки системы.

systemd (system daemon) реализует принципиально новый подход к инициализации и контролю работы системы. Одним из ключевых новшеств этого подхода является высокая степень параллелизации запуска служб при инициализации системы, что в перспективе позволяет добиться гораздо более высокой скорости, чем традиционный подход с последовательным запуском взаимозависимых служб. Другим важным моментом является контроль над точками монтирования (не-жизненно-важные файловые системы можно монтировать только при первом

обращении к ним, не тратя на это время при инициализации системы) и устройствами (можно запускать и останавливать определенные службы и при появлении или удалении заданных устройств). Для отслеживания групп процессов используется механизм cgroups, который также может быть использован для ограничения потребляемых ими системных ресурсов.

Удобство **systemd** особенно заметно на компьютерах для домашнего пользования — когда пользователи включают и перезагружают компьютер ежедневно. В отличие от **sysvinit**, подвисание при запуске одного сервиса не приведет к остановке всего процесса загрузки.

65.3. Примеры команд управления службами, журнал в systemd

Обратите внимание, что команды **`service`** и **`chkconfig`** продолжат работать в мире **systemd** практически без изменений. Тем не менее, в этой таблице показано как выполнить те же действия с помощью встроенных утилит **systemctl**.

Таблица 65.1. Команды управления службами

Команды Sysvinit	Команды Systemd	Примечания
service frobozz start	systemctl start frobozz.service	Используется для запуска службы (не перезагружает постоянные)
service frobozz stop	systemctl stop frobozz.service	Используется для остановки службы (не перезагружает постоянные)
service frobozz restart	systemctl restart frobozz.service	Используется для остановки и последующего запуска службы
service frobozz reload	systemctl reload frobozz.service	Если поддерживается, перезагружает файлы конфигурации без прерывания незаконченных операций
service frobozz condrestart	systemctl condrestart frobozz.service	Перезапускает службу, если она уже работает
service frobozz status	systemctl status frobozz.service	Сообщает, запущена ли уже служба
ls /etc/rc.d/init.d/	systemctl list-unit-files --type=service (preferred) ls /lib/systemd/system/*.service /etc/systemd/system/*.service	Используется для отображения списка служб, которые можно запустить или остановить. Используется для отображения списка всех служб.
chkconfig frobozz on	systemctl enable frobozz.service	Включает службу во время следующей перезагрузки, или любой другой триггер

Команды Sysvinit	Команды Systemd	Примечания
chkconfig frobozz off	systemctl disable frobozz.service	Выключает службу во время следующей перезагрузки, или любой другой триггер
chkconfig frobozz	systemctl is-enabled frobozz.service	Используется для проверки, сконфигурирована ли служба для запуска в текущем окружении
chkconfig --list	systemctl list-unit-files --type=service(preferred) ls /etc/systemd/system/*.wants/	Выводит таблицу служб. В ней видно, на каких уровнях загрузки они (не)запускаются
chkconfig frobozz --list	ls /etc/systemd/system/*.wants/frobozz.service	Используется, для отображения на каких уровнях служба (не)запускается
chkconfig frobozz --add	systemctl daemon-reload	Используется, когда вы создаете новую службу или модифицируете любую конфигурацию

65.4. Журнал в systemd

В **systemd** включена возможность ведения системного журнала. Для чтения журнала следует использовать команду **`journalctl`**. По умолчанию, больше не требуется запуск службы **syslog**.

Вы можете запускать **`journalctl`** с разными ключами:

- **`journalctl -b`** — покажет сообщения только с текущей загрузки;
- **`journalctl -f`** — покажет только последние сообщения.

Так же вы можете посмотреть сообщения определенного процесса:

- **`journalctl _PID`**=1 — покажет сообщения первого процесса (init).

Для ознакомления с прочими возможностями, читайте руководство по **`journalctl`**. Для этого используйте команду **`man journalctl`**.

Глава 66. Документация

Каждый объект системы Linux обязательно сопровождается документацией, описывающей их назначение и способы использования. От пользователя системы не требуется заучивать все возможные варианты взаимодействия с ней. Достаточно понимать основные принципы её устройства и уметь находить справочную информацию.

Не пренебрегайте чтением документации: она поможет вам избежать многих сложностей, сэкономить массу времени и усилий при установке, настройке и администрировании системы, поможет найти нужное для работы приложение и быстро разобраться в нём.

66.1. Экранная документация

Почти все системы семейства UNIX, включая систему Linux, имеют экранную документацию. Её тексты содержат документацию по системным командам, ресурсам, конфигурационным файлам и т. д., а также могут быть выведены на экран в процессе работы.

66.1.1. man

Для доступа к экранной документации используется команда **man** (сокращение от manual). Каждая страница руководства посвящена одному объекту системы. Для того чтобы прочесть страницу руководства по программе, необходимо набрать **man** *название_программы*. К примеру, если вы хотите узнать, какие опции есть у команды **date**, вы можете ввести команду:

```
$ man date
```

Большинство экранной документации написано для пользователей, имеющих некоторое представление о том, что делает данная команда. Поэтому большинство текстов экранной документации содержит исключительно технические детали команды без особых пояснений. Тем не менее, экранная документация оказывается очень ценной в том случае, если вы помните название команды, но её синтаксис просто выпал у вас из памяти.

Поиск по описаниям **man** осуществляется командой **apropos**. Если вы точно не знаете, как называется необходимая вам программа, то поиск осуществляется по ключевому слову, к примеру, **apropos** *date* или при помощи ввода слова, обозначающего нужное действие, после команды **man -k** (например, **man -k** *copy*). Слово, характеризующее желаемое для вас действие, можно вводить и на русском языке. При наличии русского перевода страниц руководства **man** результаты поиска будут выведены на запрашиваемом языке.

«Страница руководства» занимает, как правило, больше одной страницы экрана. Для того чтобы читать было удобнее, **man** запускает программу постраничного просмотра текстов. Страницы перелистывают пробелом, для выхода из режима чтения описания команд **man** необходимо нажать на клавиатуре **q**. Команда **man man** выдаёт справку по пользованию самой командой **man**.

Документация в подавляющем большинстве случаев пишется на простом английском языке. Необходимость писать на языке, который будет более или менее понятен большинству пользователей, объясняется постоянным развитием Linux. Дело не в том, что страницу руководства нельзя перевести, а в том, что её придётся переводить всякий раз, когда изменится описываемый ею объект! Например, выход новой версии программного продукта сопровождается изменением его возможностей и особенностей работы, а следовательно, и новой версией документации.

Тем не менее, некоторые наиболее актуальные руководства существуют в переводе на русский язык. Свежие версии таких переводов на русский язык собраны в пакете *man-pages-ru*. Установив этот пакет, вы добавите в систему руководства, для которых есть перевод, и **man** по умолчанию будет отображать их на русском языке.

66.1.2. info

Другой источник информации о Linux и составляющих его программах — справочная подсистема *info*. Страница руководства, несмотря на обилие ссылок различного типа, остаётся «линейным» текстом, структурированным только логически. Документ *info* — это настоящий гипертекст, в котором множество небольших страниц объединены в дерево. В каждом разделе документа *info* всегда есть оглавление, из которого можно перейти к нужному подразделу, а затем вернуться обратно (ссылки для перемещения по разделам текста помечены *). Для получения вспомогательной информации о перемещении по тексту используйте клавишу **h**. Полное руководство *info* вызывается командой **info info**. Команда **info**, введённая без параметров, предлагает пользователю список всех документов *info*, установленных в системе.

66.2. Документация по пакетам

Дополнительным источником информации об интересующей вас программе, в основном на английском языке, является каталог **/usr/share/doc** — место хранения разнообразной документации.

Каждый пакет также содержит поставляемую вместе с включённым в него ПО документацию, располагающуюся обычно в каталоге **/usr/share/doc/имя_пакета**. Например, документация к пакету *foo-1.0-alt1* находится в **/usr/share/doc/foo-1.0-alt1**. Для получения полного списка файлов документации, относящихся к пакету, воспользуйтесь командой **rpm -qd** *имя_установленного_пакета*.

В документации к каждому пакету вы можете найти такие файлы как **README**, **FAQ**, **TODO**, **ChangeLog** и другие. В файле **README** содержится основная информация о программе — имя и контактные данные авторов, назначение, полезные советы и пр. **FAQ** содержит ответы на часто задаваемые вопросы; этот файл стоит прочитать в первую очередь, если у вас возникли проблемы или вопросы по использованию программы, поскольку большинство проблем и сложностей типичны, вполне вероятно, что в **FAQ** вы тут же найдёте готовое решение. В файле **TODO** записаны планы разработчиков на реализацию той или иной функциональности. В файле **ChangeLog** записана история изменений в программе от версии к версии.

Для поиска внешней информации о программе, например, адреса сайта программы в сети Интернет можно использовать команду **rpm -qi** *имя_установленного_пакета*. В информационном заголовке соответствующего пакета, среди прочей информации, будет выведена искомая ссылка.

Возможно, будет полезно знать расположение собрания практических рекомендаций по самым различным вопросам, связанным с использованием Linux. Файлы **HOWTO** в формате HTML (от англ. how to — «как сделать») каталога **/usr/share/doc/HOWTO/** (при условии их наличия в системе) содержат многообразную информацию о работе Linux-систем.

66.3. Документация к программам, имеющим графический интерфейс

Каждая программа, имеющая графический интерфейс, как правило, сопровождается справочной информацией, вызываемой из меню программы. Обычно, это разделы меню **Справка**.

По обыкновению, это меню предоставляет информацию о программе, её версии, лицензии и авторах. В большинстве случаев, справка содержит встроенное руководство, ссылки на локальные сведения и интернет-страницы документации на официальных сайтах программ (традиционная кнопка **F1**), информацию о сочетании клавиш, а также сообщения о процедурах и отладке в программе.

Часть XII. Техническая поддержка продуктов «Базальт СПО»

Содержание

Глава 67. Покупателям нашей продукции

Право на получение консультационной и технической поддержки вы приобретаете при покупке большинства продуктов торговой марки Альт. Сроки и объём помощи указаны в талоне технической поддержки, приложенном к вашему диску. Техническая поддержка дистрибутива может быть расширена в зависимости от потребностей пользователя.

Условия технической поддержки можно найти на интернет-сайте http://www.basealt.ru.

Глава 68. Пользователям нашей продукции

Вне зависимости от того, скачали вы или же приобрели наш дистрибутив, задавать вопросы или обсуждать их с сообществом пользователей дистрибутивов «Альт» вы можете на форуме или в списках рассылки.

Помощь сообщества:

- Форум: http://forum.altlinux.org
- Списки рассылки: http://lists.altlinux.org/
- Сообщить об ошибке: http://bugs.altlinux.org/
- Репозиторий: http://packages.altlinux.org/
- Сборочная среда: http://git.altlinux.org/

Ресурсы компании «Базальт СПО»:

- Сайт компании: http://www.basealt.ru/
- Контакты: http://basealt.ru/about/contacts/
- Новости обновлений безопасности: http://cve.basealt.ru/

Форум и списки рассылки читают опытные пользователи, профессиональные системные администраторы и разработчики «Базальт СПО». Сообщество пользователей и специалистов окажет содействие в поиске ответа на ваш вопрос или посоветует выход из сложной ситуации. При обращении к данному виду помощи у вас нет гарантии на полноту и своевременность ответа, но мы стараемся не оставлять без ответа вопросы, задаваемые в списках.