ОПЕРАЦИОННАЯ СИСТЕМА АЛЬТ СЕРВЕР 9.2

Описание функциональных характеристик

Содержание

1 ОБЩИЕ СВЕДЕНИЯ ОБ ОС АЛЬТ СЕРВЕР 9.2

1.1 Краткое описание возможностей

Операционная система «Альт Сервер» (далее – ОС «Альт Сервер»), представляет собой совокупность интегрированных программ, созданных на основе ОС «Linux», и обеспечивает обработку, хранение и передачу информации в защищенной программной среде в круглосуточном режиме эксплуатации.

ОС «Альт Сервер» обладает следующими функциональными характеристиками:

- обеспечивает возможность обработки, хранения и передачи информации;
- обеспечивает возможность функционирования в многозадачном режиме (одновременное выполнение множества процессов);
- обеспечивает возможность масштабирования системы: возможна эксплуатация ОС как на одной ПЭВМ, так и в информационных системах различной архитектуры;
- обеспечивает многопользовательский режим эксплуатации;
- обеспечивает поддержку мультипроцессорных систем;
- обеспечивает поддержку виртуальной памяти;
- обеспечивает поддержку запуска виртуальных машин;
- обеспечивает сетевую обработку данных, в том числе разграничение доступа к сетевым пакетам.

Основные преимущества ОС «Альт Сервер»:

- русскоязычный пользовательский интерфейс;
- графическая рабочая среда MATE;
- установка серверных решений и решений конечных пользователей с одного диска;
- возможность как развернуть, так и использовать только определённые службы без Alterator;
- широкий выбор различных программ для профессиональной работы в сети Интернет, с документами, со сложной графикой и анимацией, для обработки звука и видео, разработки программного обеспечения и образования.

ОС «Альт Сервер» поддерживает клиент-серверную архитектуру и может обслуживать процессы как в пределах одной компьютерной системы, так и процессы на других ПЭВМ через каналы передачи данных или сетевые соединения.

1.2 Структура программных средств

ОС «Альт Сервер» состоит из набора компонентов предназначенных для реализации функциональных задач необходимых пользователям (должностным лицам для выполнения

определённых должностными инструкциями, повседневных действий) и поставляется в виде дистрибутива и комплекта эксплуатационной документации.

В структуре ОС «Альт Сервер» можно выделить следующие функциональные элементы:

- ядро ОС;
- системные библиотеки;
- утилиты и драйверы;
- средства обеспечения информационной безопасности;
- системные приложения;
- средства обеспечения облачных и распределенных вычислений, средства виртуализации и системы хранения данных;
- системы мониторинга и управления;
- средства подготовки исполнимого кода;
- средства версионного контроля исходного кода;
- библиотеки подпрограмм (SDK);
- среды разработки, тестирования и отладки;
- интерактивные рабочие среды;
- программные серверы;
- веб-серверы;
- системы управления базами данных;
- графическая оболочка MATE;
- командные интерпретаторы;
- прикладное программное обеспечение общего назначения;
- офисные приложения.

Ядро ОС «Альт Сервер» управляет доступом к оперативной памяти, сети, дисковым и прочим внешним устройствам. Оно запускает и регистрирует процессы, управляет разделением времени между ними, реализует разграничение прав и определяет политику безопасности, обойти которую, не обращаясь к нему, нельзя.

Ядро работает в режиме «супервизора», позволяющем ему иметь доступ сразу ко всей оперативной памяти и аппаратной таблице задач. Процессы запускаются в «режиме пользователя»: каждый жестко привязан ядром к одной записи таблицы задач, в которой, в числе прочих данных, указано, к какой именно части оперативной памяти этот процесс имеет доступ. Ядро постоянно находится в памяти, выполняя системные вызовы – запросы от процессов на выполнение этих подпрограмм.

Системные библиотеки – наборы программ (пакетов программ), выполняющие различные функциональные задачи и предназначенные для динамического подключения к работающим программам, которым необходимо выполнение этих задач.

Серверные программы и приложения предоставляют пользователю специализированные услуги (почтовые службы, хранилище файлов, веб-сервер, система управления базой данных, обеспечение документооборота, хранилище данных пользователей и так далее) в локальной или глобальной сети и обеспечивают их выполнение.

В состав ОС «Альт Сервер» включены следующие серверные программы и приложения:

- приложения, обеспечивающие поддержку сетевого протокола DHCP (Dynamic Host Configuration Protocol);
- приложения, обеспечивающие поддержку протокола аутентификации LDAP (Lightweight Directory Access Protocol);
- приложения, обеспечивающие поддержку протоколов FTP, SFTP, SSHD;
- программы, обеспечивающие работу сервера виртуализации;
- программы, обеспечивающие работу SMB-сервера (Сервер файлового обмена);
- программы почтового сервера Postfix;
- программы прокси-сервера Squid;
- программы, обеспечивающие работу сервера совместной работы Sogo;
- программы, обеспечивающие работу сервера домена FreeIPA;
- программы менеджера виртуальных машин libvirt;
- программы веб-сервера Apache2;
- программы DNS-сервера.

В состав ОС «Альт Сервер» включены следующие дополнительные системные приложения:

- архиваторы;
- приложения для управления RPM-пакетами;
- приложения резервного копирования;
- приложения мониторинга системы;
- приложения для работы с файлами;
- приложения для настройки системы;
- настройка параметров загрузки;
- настройка оборудования;
- настройка сети.

2 ЗАГРУЗКА ОПЕРАЦИОННОЙ СИСТЕМЫ

2.1 Настройка загрузки

Вызов ОС «Альт Сервер», установленной на жесткий диск, происходит автоматически и выполняется после запуска ПЭВМ и отработки набора программ BIOS. ОС «Альт Сервер» вызывает специальный загрузчик.

Загрузчик настраивается автоматически и включает в свое меню все системы, установку которых на ПЭВМ он определил. Поэтому загрузчик также может использоваться для вызова других ОС, если они установлены на компьютере.

Примечание. При наличии на компьютере нескольких ОС (или при наличии нескольких вариантов загрузки), оператор будет иметь возможность выбрать необходимую ОС (вариант загрузки). В случае если пользователем ни один вариант не был выбран, то по истечении заданного времени будет загружена ОС (вариант загрузки), заданные по умолчанию.

При стандартной установке ОС «Альт Сервер» в начальном меню загрузчика доступны несколько вариантов загрузки (Рис. 1): обычная загрузка, загрузка с дополнительными параметрами (например, «recovery mode» – загрузка с минимальным количеством драйверов), загрузка в программу проверки оперативной памяти (memtest).

Варианты загрузки

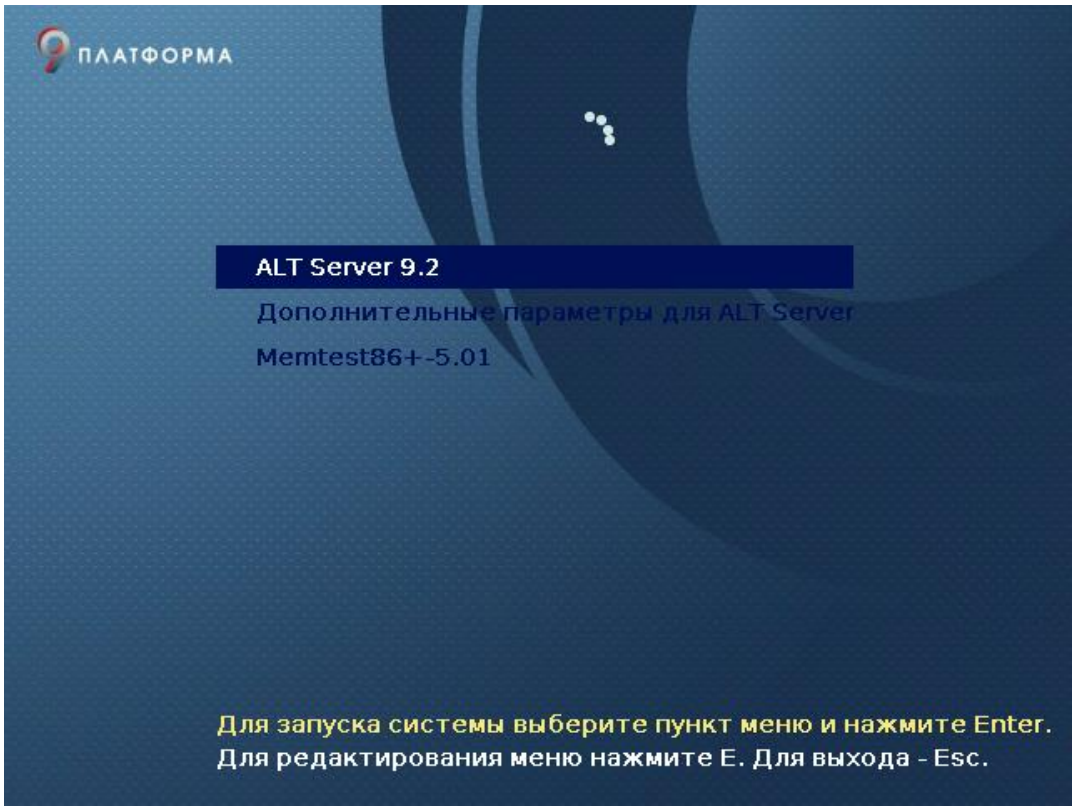


Рис. 1

По умолчанию, если не были нажаты управляющие клавиши на клавиатуре, загрузка ОС «Альт Сервер» продолжится автоматически после небольшого времени ожидания (обычно несколько секунд). Нажав клавишу <Enter>, можно начать загрузку немедленно.

Для выбора дополнительных параметров загрузки нужно выбрать пункт «Дополнительные параметры для ALT Server».

Для выполнения тестирования оперативной памяти нужно выбрать пункт «Memtest86+-5.01».

Нажатием клавиши <E> можно вызвать редактор параметров загрузчика GRUB и указать параметры, которые будут переданы ядру ОС при загрузке.

Примечание. Если при установке системы был установлен пароль на загрузчик потребуется ввести имя пользователя «boot» и заданный на шаге «Установка загрузчика» пароль.

В процессе загрузки ОС «Альт Сервер» пользователь может следить за информацией процесса загрузки, которая отображает этапы запуска различных служб и программных серверов в виде отдельных строк (Рис. 2), на экране монитора.

Загрузка ОС

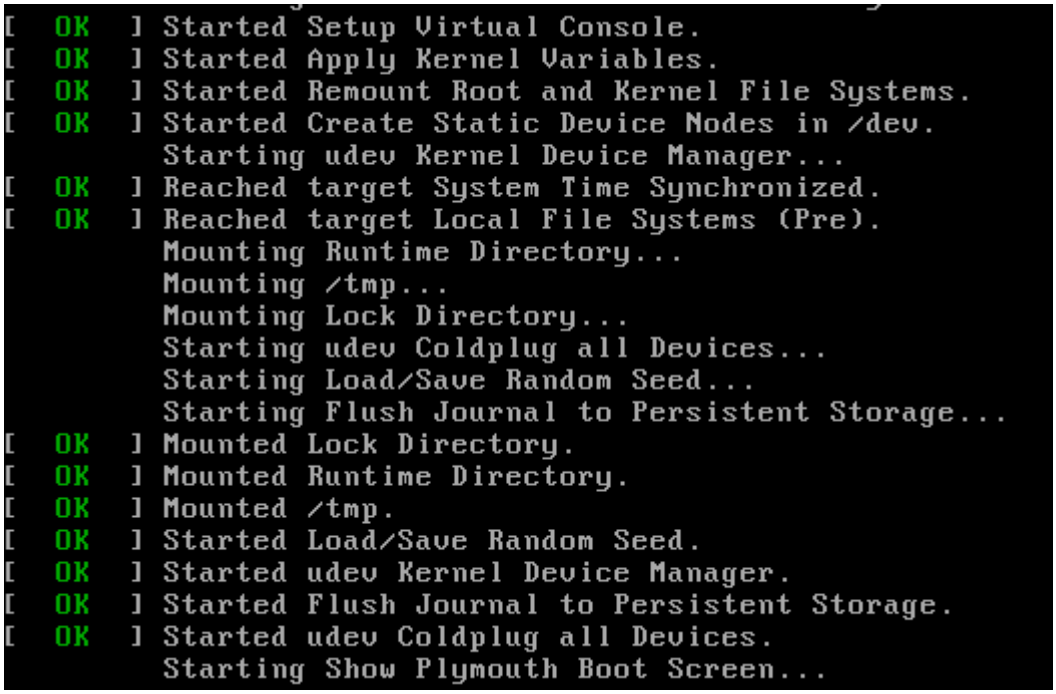


Рис. 2

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 ОС 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 занять больше времени, чем обычно.

2.2 Получение доступа к зашифрованным разделам

В случае если был создан шифрованный раздел, потребуется вводить пароль при обращении к этому разделу.

Например, если был зашифрован домашний раздел `/home`, то для того, чтобы войти в систему, потребуется ввести пароль этого раздела (Рис. 3) и затем нажать <Enter>.

Загрузка ОС

Рис. 3

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

2.3 Вход и работа в системе в консольном режиме

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

При загрузке в консольном режиме работа загрузчика ОС «Альт Сервер» завершается запросом на ввод логина и пароля учетной записи (Рис. 4). В случае необходимости на другую консоль можно перейти, нажав <Ctrl>+<Alt>+<F2>.

Запрос на ввод логина

Рис. 4

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 (Рис. 5).

Приглашение для ввода команд

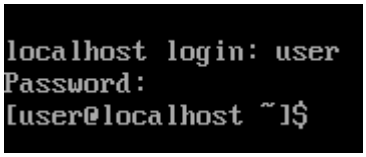


Рис. 5

2.4 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.

2.5 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 (Рис. 6).

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.

Окно входа в систему

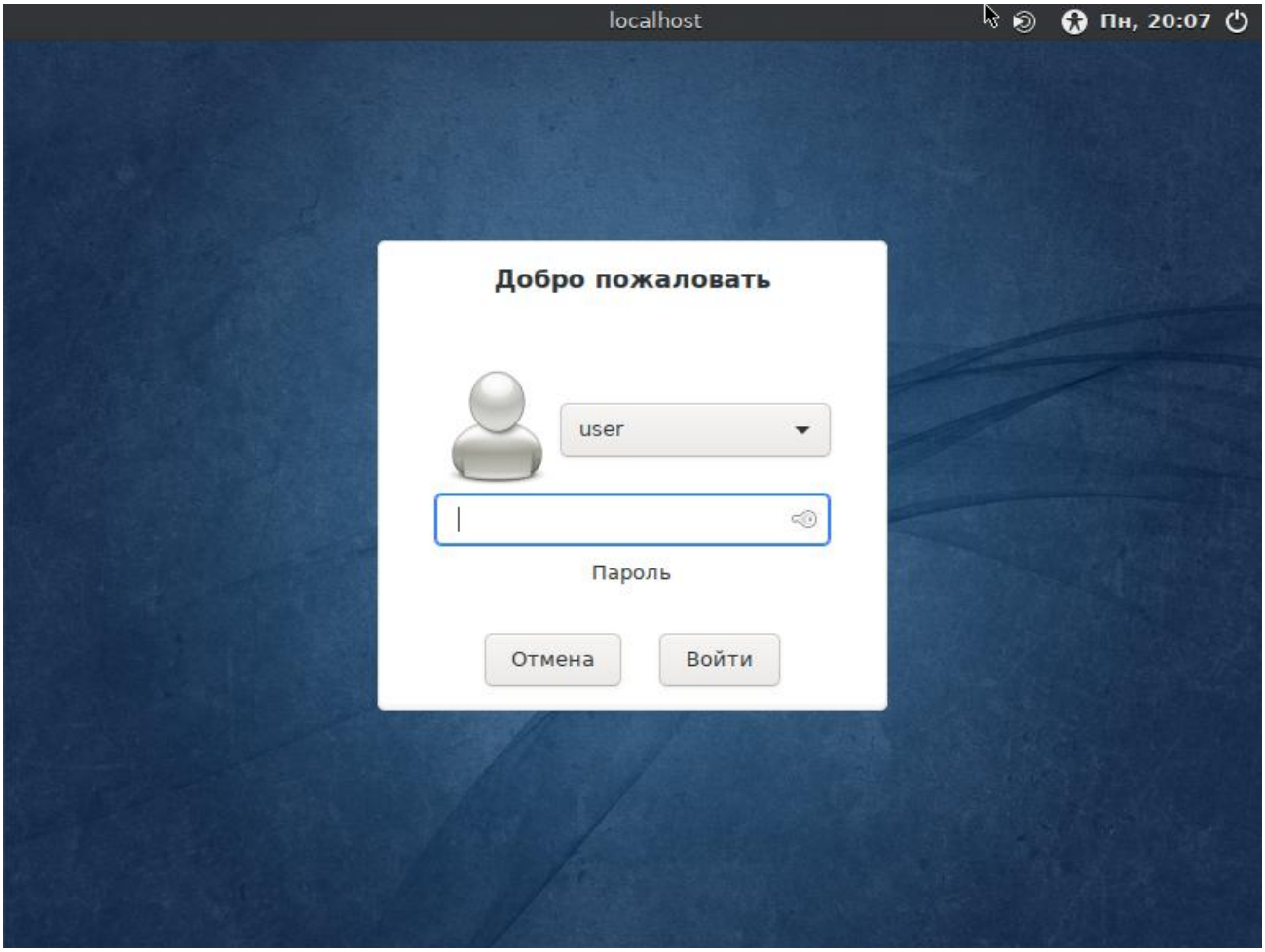


Рис. 6

В результате успешного прохождения процедуры аутентификации и идентификации будет выполнен вход в систему. ОС «Альт Сервер» перейдет к штатному режиму работы и предоставит дальнейший доступ к графическому интерфейсу (Рис. 7).

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

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.

Рабочий стол MATE

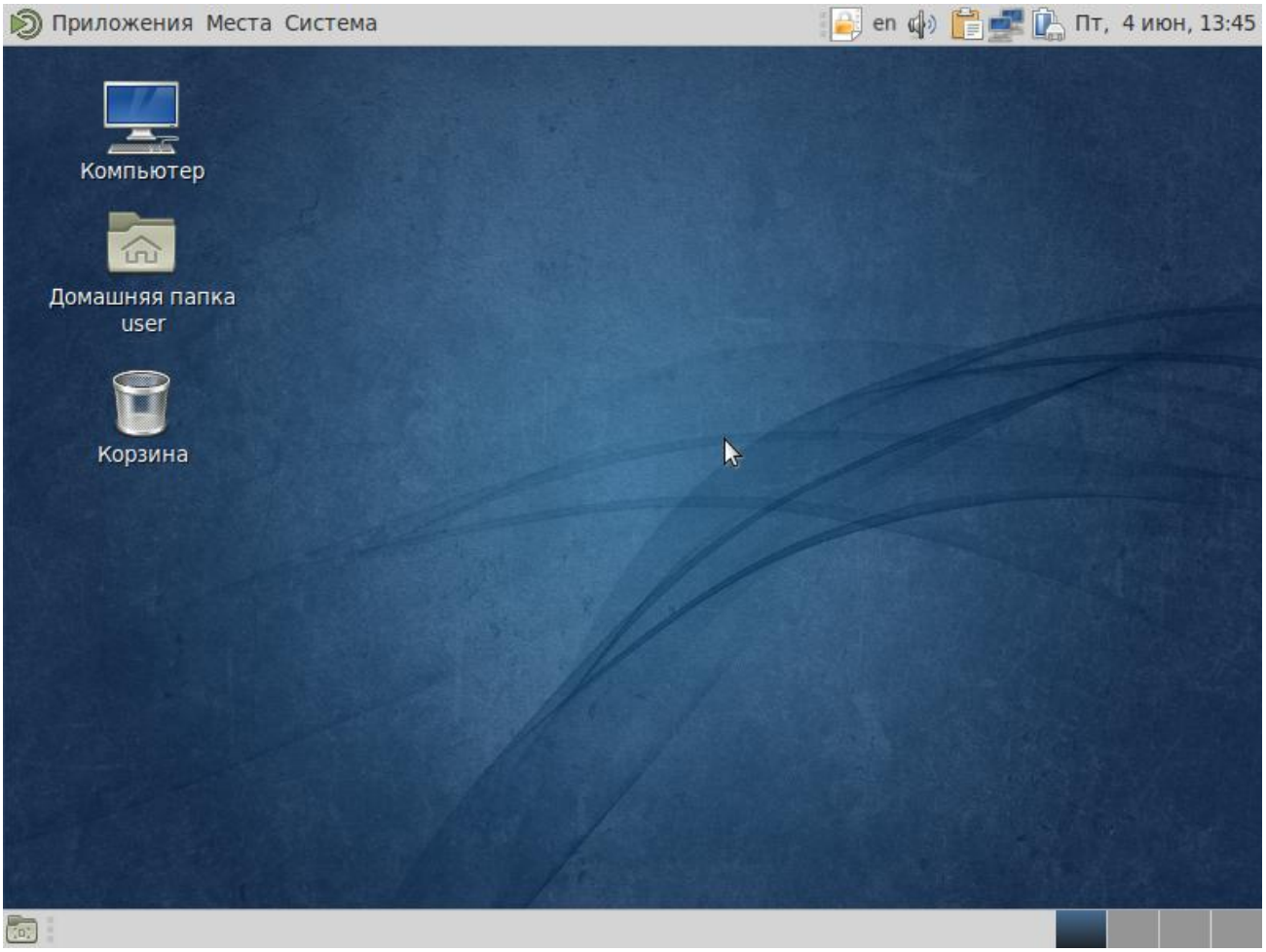


Рис. 7

2.6 Рабочий стол MATE

На рабочем столе MATE есть три особые области. Сверху вниз (Рис. 7):

- 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).

Верхняя 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.

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».

Меню «Места» разделено на четыре подраздела. Щелчок по любому пункту в меню «Переход» открывает файловый менеджер Caja. Руководство Caja можно вызвать, нажав: 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.

С помощью меню «Система» осуществляется доступ к настройкам MATE, справочной информации и функциям запуска, перезагрузки и отключения компьютера. Это меню разделено на три подраздела (Рис. 8).

Меню «Система»

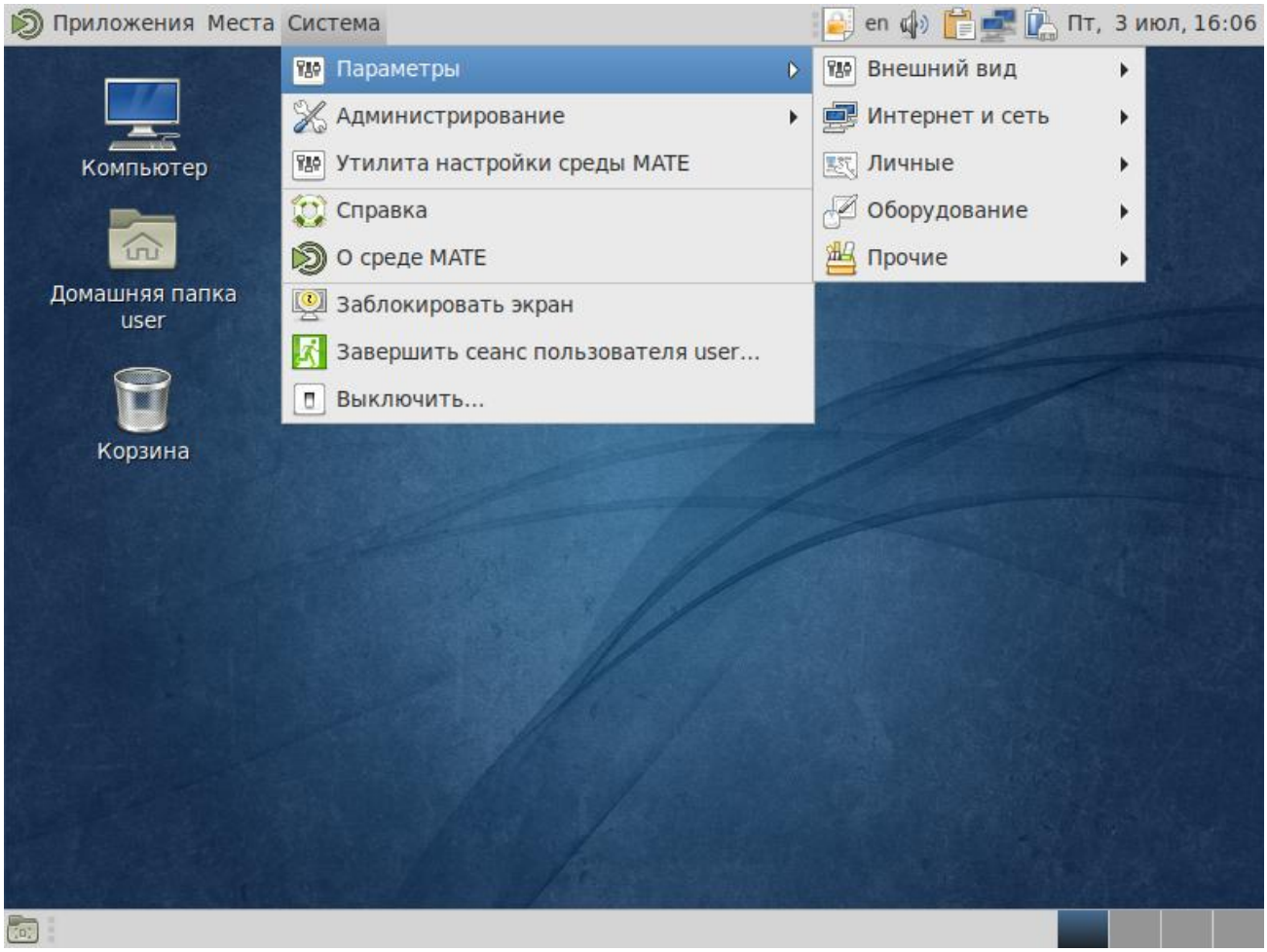


Рис. 8

Первый подраздел содержит:

– «Параметры» – содержит доступ к различным настройкам и предоставляет доступ к инструментам администрирования системы. В меню «Параметры» входят настройки:
  - «Внешний вид»:
    - «Внешний вид» позволяет настроить внешний вид рабочего стола, включая фоновую картинку;
    - «Всплывающие уведомления» позволяет настроить стиль и позицию уведомлений;
    - «Главное меню MATE» 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 позволяют 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» позволяет выбрать приложения для автоматического запуска при входе;
  - «Обо мне» здесь можно установить изображение и задать данные пользователя (имя, фамилия, телефон, электронная почта);
  - «Предпочтительные приложения» дают возможность выбрать, какие приложения будут использованы 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.

Область рабочего стола включает в себя три значка:

– «Компьютер» – предоставляет доступ к устройствам хранения данных.
– «Домашняя папка пользователя» – предоставляет доступ к домашней директории пользователя `/home/<имя пользователя>`. В этой папке по умолчанию хранятся пользовательские файлы (например, аудиозаписи, видеозаписи, документы). У каждого пользователя своя «Домашняя» директория. Каждый пользователь имеет доступ только в свою «Домашнюю» директорию.
– «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». 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»).

У панели со списком окон MATE (Рис. 9) 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. Чтобы переключаться между приложениями с помощью мыши, необходимо кликнуть по желаемому приложению левой кнопкой мыши, чтобы переключиться на него. Для переключения между открытыми окнами можно использовать комбинацию клавиш<Alt>+<Tab>.
– «Переключатель рабочих мест» – это группа квадратов в правом нижнем углу экрана. Они позволяют 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 «Параметры». Для переключения между рабочими столами необходимо использовать комбинацию клавиш <Ctrl>+<Alt>+<←> или <Ctrl>+<Alt>+<→>.
– «Свернуть все окна» – кнопка позволяет свернуть (развернуть) все открытые окна на текущем рабочем месте.

Панель MATE со списком окон

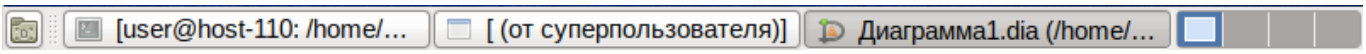


Рис. 9

3 НАСТРОЙКА СИСТЕМЫ

3.1 Центр управления системой

Для управления настройками установленной системы можно использовать Центр 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.

3.1.1 Применение ЦУС

ЦУС можно использовать для разных целей, например:

- настройка даты и времени;
- управление системными службами;
- просмотр системных журналов;
- управление выключением удаленного компьютера (доступно только в веб-интерфейсе);
- настройка ограничений выделяемых ресурсов памяти пользователям (квоты): («Использование диска»);
- настройка ограничений на использование внешних носителей (доступно только в веб-интерфейсе);
- конфигурирование сетевых интерфейсов;
- настройка межсетевого экрана;
- изменения пароля администратора системы (root);
- создание, удаление и редактирование учётных записей пользователей.

Все модули ЦУС имеют справочную информацию.

3.1.2 Запуск ЦУС в графической среде

ЦУС 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) (Рис. 10).

После успешного входа можно приступать к настройке системы (Рис. 11).

Запуск Центра управления системой

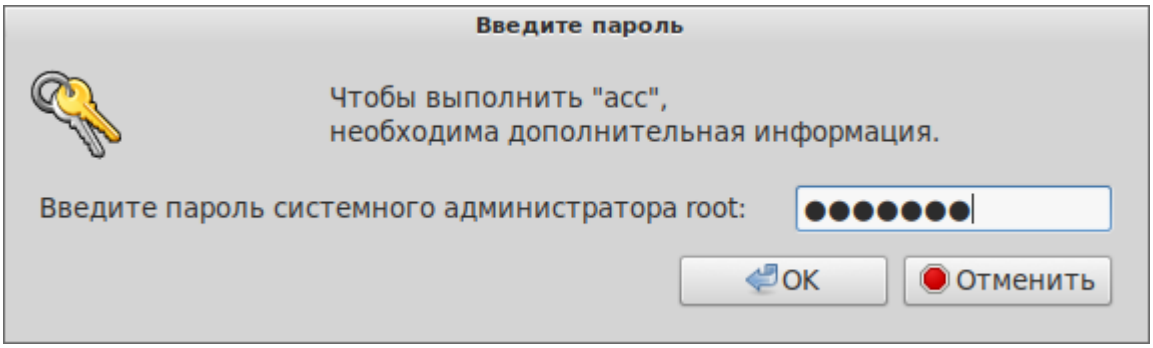


Рис. 10

Центр управления системой

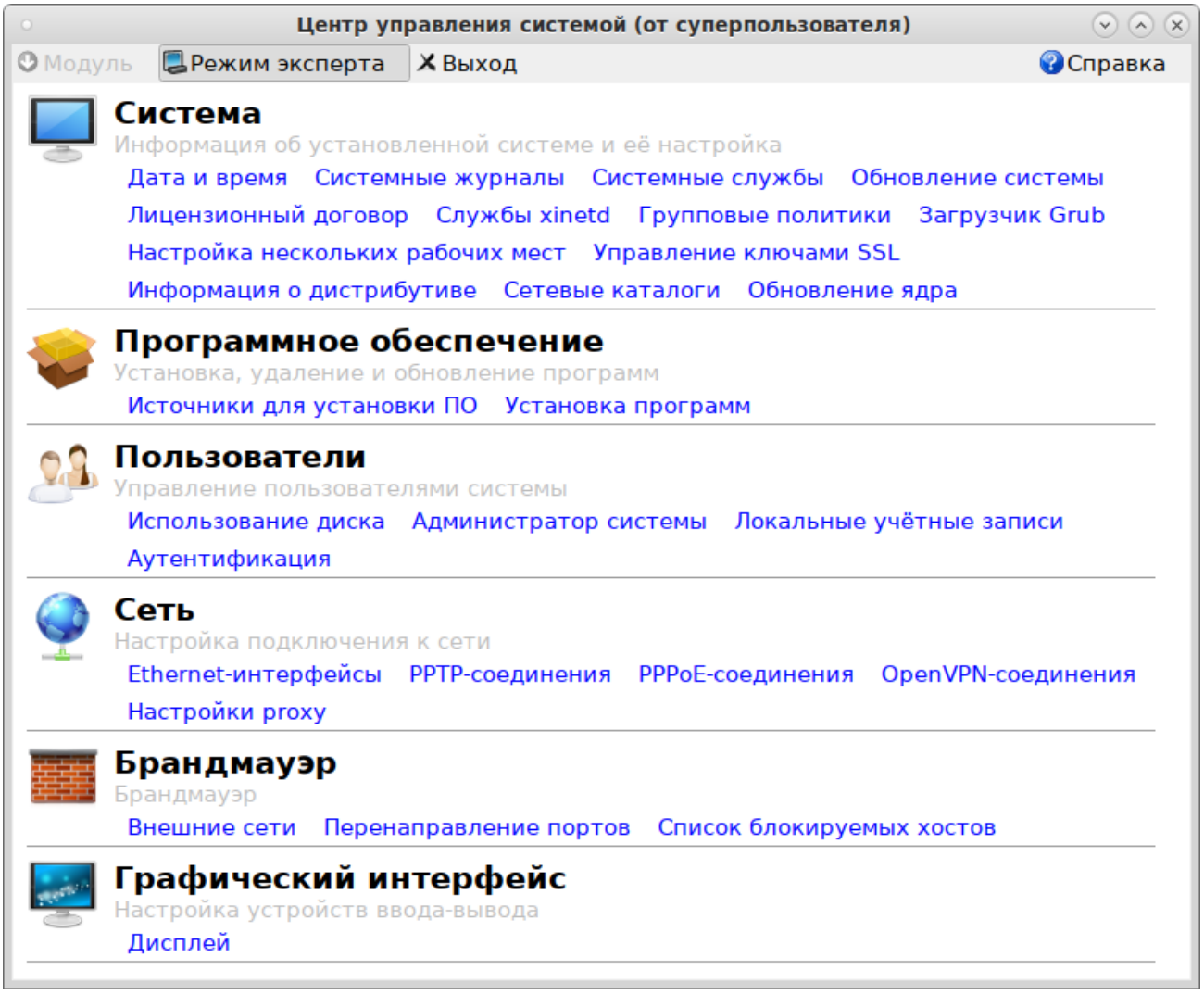


Рис. 11

3.1.3 Использование веб-ориентированного ЦУС

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/

IP-адрес сервера можно узнать, введя 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
```

Тут видно, что на интерфейсе enp0s3 задан IP-адрес 192.168.0.122.

При запуске ЦУС необходимо ввести в соответствующие поля имя пользователя (root) и пароль пользователя root (Рис. 12).

Запуск веб-ориентированного центра управления системой

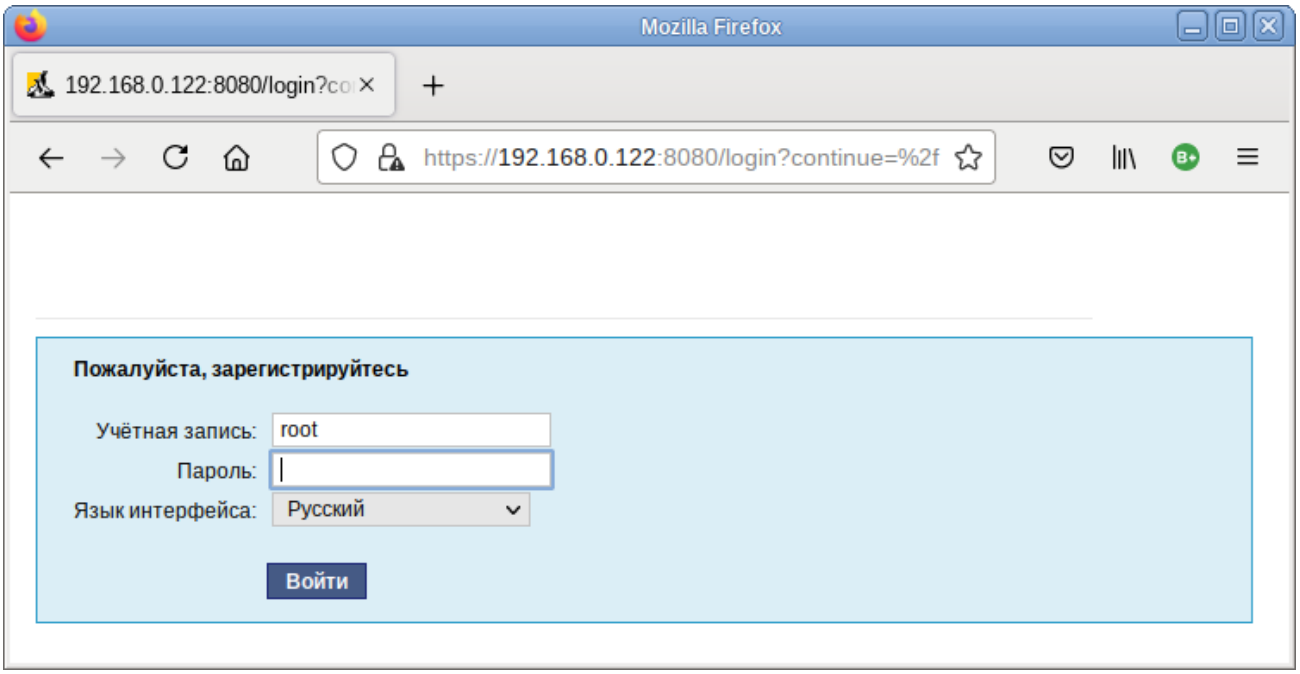


Рис. 12

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

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.

ЦУС содержит справочную информацию по включённым в него модулям. Об использовании самого интерфейса системы управления можно прочитать, нажав, на кнопку «Справка» на начальной странице центра управления системой (Рис. 13).

Веб-ориентированный центр управления системой

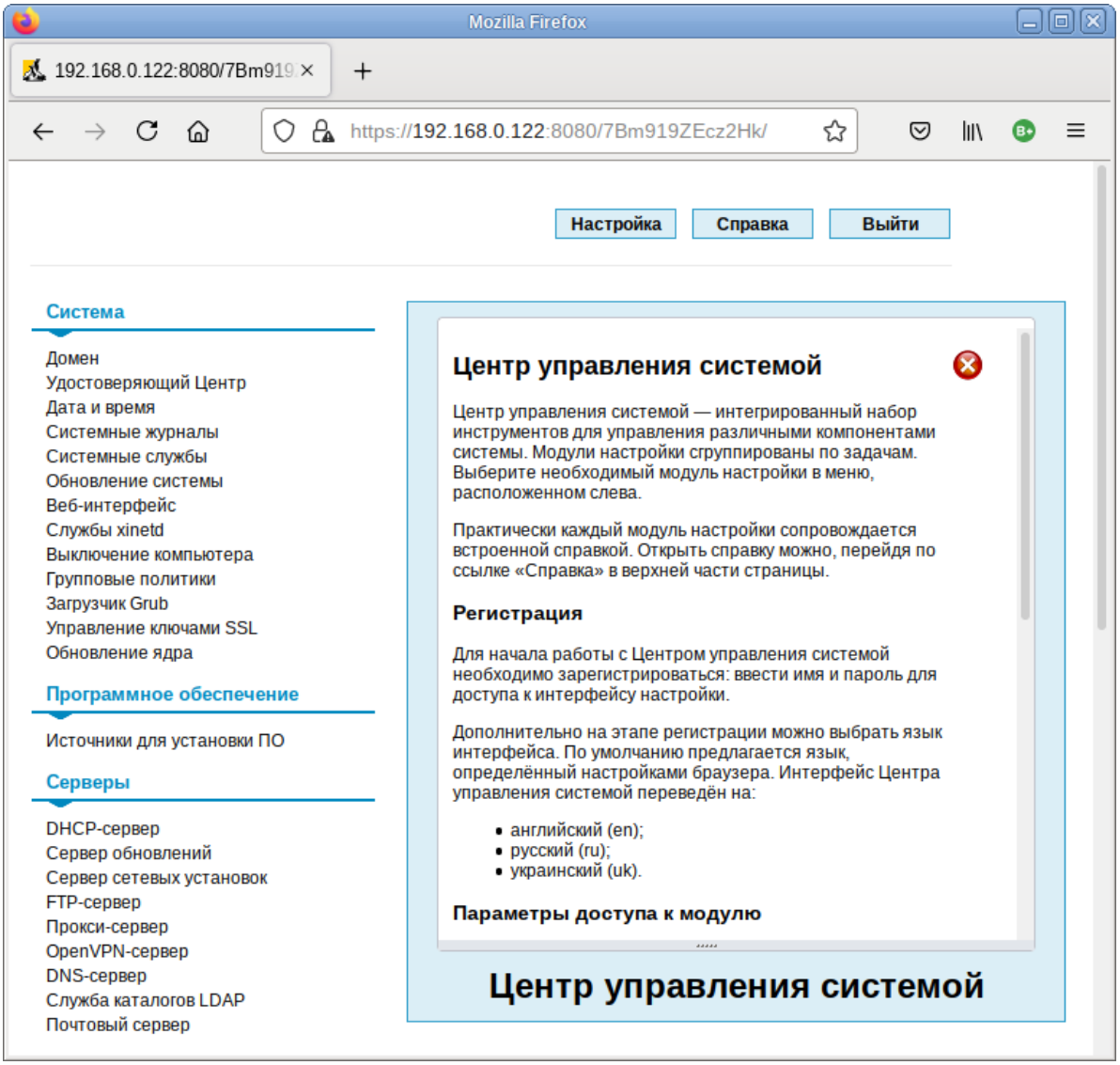


Рис. 13

Если в сети нет компьютера, который можно было бы использовать для доступа к веб-ориентированному ЦУС, то можно воспользоваться браузером непосредственно на сервере.

После работы с ЦУС, в целях безопасности, не следует оставлять открытым браузер. Необходимо обязательно выйти из сеанса работы с ЦУС, нажав на кнопку «Выйти».

Подробнее об использовании ЦУС можно узнать в главе «Организация сетевой инфраструктуры с помощью сервера».

3.2 Настройка сети

3.2.1 NetworkManager

Для управления настройками сети в ОС «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.

При нажатии левой кнопкой мыши на значок NetworkManager, появляется контекстное меню, в котором можно выбрать одну из доступных сетей и подключиться к ней. Из этого меню так же можно отключить активное Wi-Fi соединение или установить VPN соединение (Рис. 14).

NetworkManager

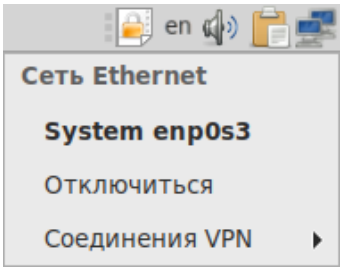


Рис. 14

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 (Рис. 15). Здесь можно посмотреть версию программы, получить сведения о соединении, изменить соединения (например, удалить Wi-Fi сеть, чтобы не подключаться к ней автоматически).

NetworkManager

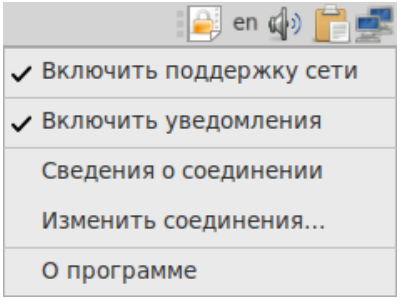


Рис. 15

3.3 Развёртывание офисной ИТ-инфраструктуры

3.3.1 Подготовка

Перед началом развёртывания офисной ИТ-инфраструктуры необходимо провести детальное планирование. Конкретные решения в каждом случае будут продиктованы спецификой требований, предъявляемым к офисной ИТ-инфраструктуре. Как будет использоваться ОС «Альт Сервер» зависит от каждого конкретного случая. 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 ОС «Альт Сервер», является домен.

3.3.2 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» можно:

- 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 Linux, так и на Microsoft Windows.

3.3.3 Сервер, рабочие места и аутентификация

Сервер под управлением ОС «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 ОС «Альт Сервер») – осуществляет контроль доступа к ресурсам сети, содержит централизованную базу данных пользователей и *удостоверяющий центр* для выдачи сертификатов службам на серверах и рабочих местах.

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

Наибольший эффект от использования ОС «Альт Сервер» достигается при использовании его вместе с рабочими местами под управлением ОС «Альт Рабочая станция». Они уже содержат всё необходимое для интеграции в сеть с ОС «Альт Сервер». 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 ОС «Альт Рабочая станция» позволяют легко настроить такой способ аутентификации. Для этого в модуле ЦУС «Аутентификация» (раздел «Пользователи») на рабочей станции (Рис. 16), нужно указать домен, управляемый ОС «Альт Сервер».

Настройка способа аутентификации в модуле «Аутентификация»

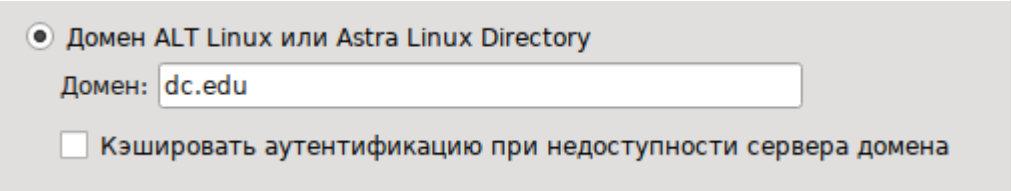


Рис. 16

3.4 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.

3.4.1 Создание учётных записей пользователей

Централизованная база пользователей создаётся на главном сервере. Наполнить её учётными записям 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» (Рис. 17).

Выбор источника списка пользователей в модуле «Пользователи»

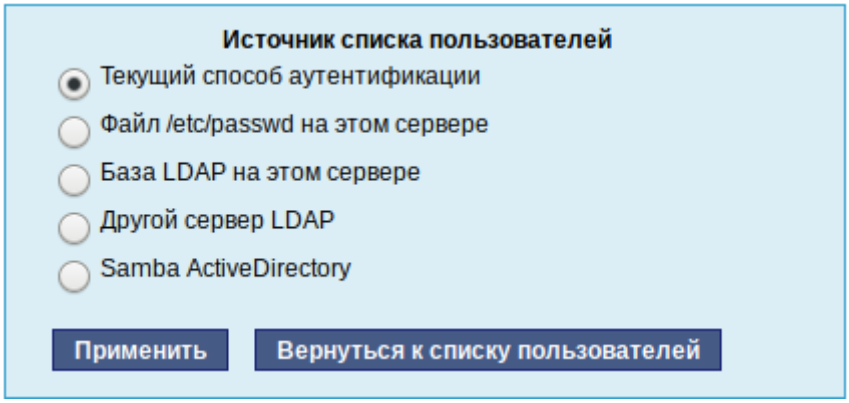


Рис. 17

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 (Рис. 18). Список доступных полей зависит от выбранного источника данных о пользователях.

После создания учетной записи пользователя необходимо присвоить учетной записи пароль. Этот пароль и будет использоваться пользователем для регистрации в домене. После этого на рабочих местах, на которых для аутентификации установлен этот домен, можно вводить это имя пользователя и пароль.

3.4.2 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 -
```

Создание учётной записи пользователя в модуле «Пользователи»

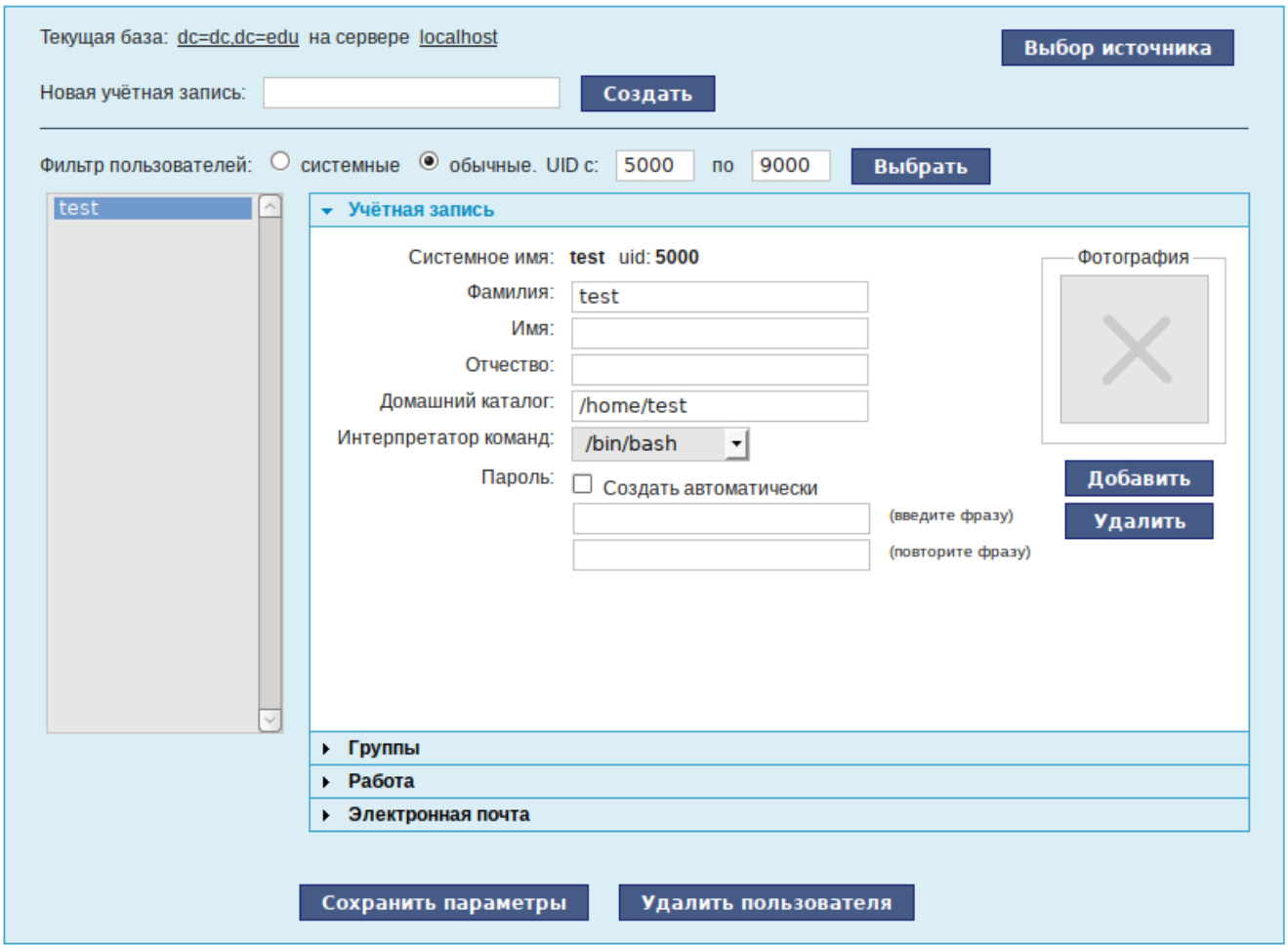


Рис. 18

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, необходимо нажать кнопку «Выбор источника» и выбрать источник (Рис. 19).

Для создания новой группы необходимо ввести название группы и нажать кнопку «Создать» (Рис. 20), после чего имя отобразится в списке слева.

Выбор источника списка групп в модуле «Группы»

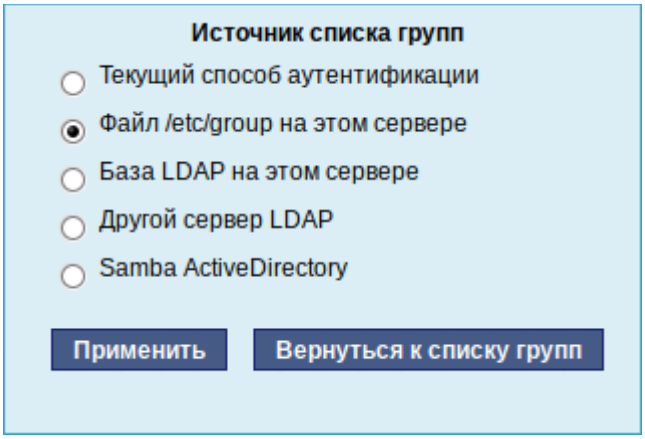


Рис. 19

Настройка членства пользователей в группах

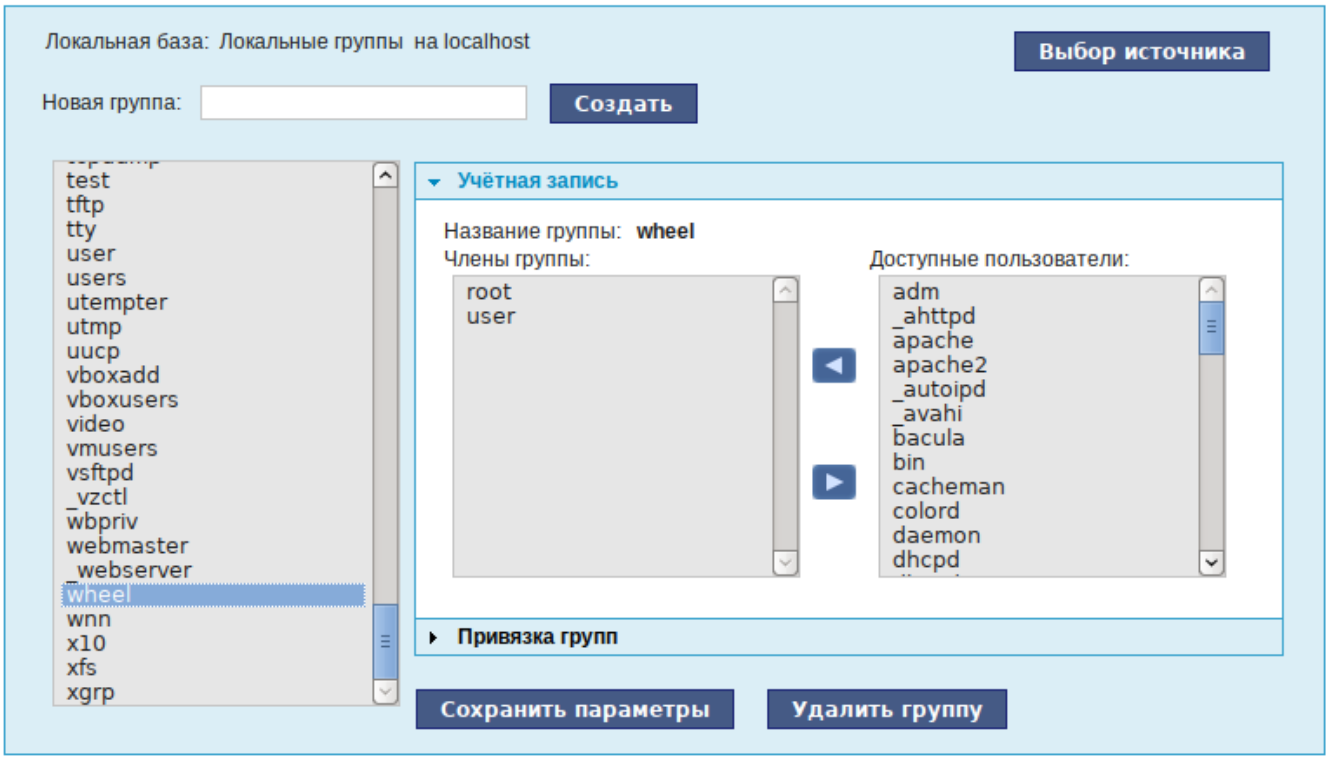


Рис. 20

Во вкладке «Учётная запись» можно настроить принадлежность учётной записи группам (Рис. 20). 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 ▶.

Во вкладке «Привязка групп» можно привязать группу к системной группе или к группе Samba (Рис. 21).

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

Привязка групп

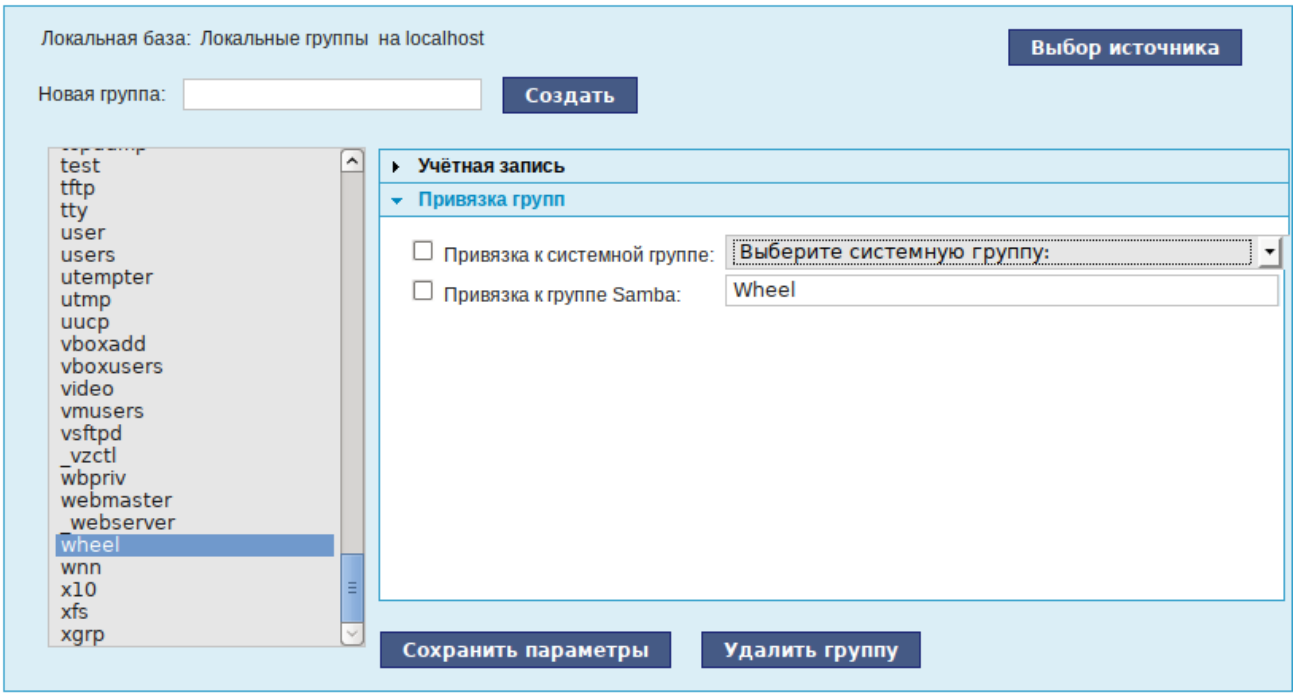


Рис. 21

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.

4 ОРГАНИЗАЦИЯ СЕТЕВОЙ ИНФРАСТРУКТУРЫ С ПОМОЩЬЮ СЕРВЕРА

Компьютер с ОС «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 ОС «Альт Сервер», настраиваемые в ЦУС.

4.1 Настройка подключения к Интернету

Помимо множества различных служб, которые ОС «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 – 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 сервера, так и для настройки общего выхода в Интернет для компьютеров сети необходимо настроить подключение к Интернету на самом сервере. ОС «Альт Сервер» поддерживает самые разные способы подключения к сети Интернет:

- Ethernet;
- PPTP;
- PPPoE;
- и т.д.

Для настройки подключения можно воспользоваться одним из разделов ЦУС «Сеть»:

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

4.1.1 Конфигурирование сетевых интерфейсов

Конфигурирование сетевых интерфейсов осуществляется в модуле ЦУС «Ethernet-интерфейсы» (пакет alterator-net-eth) из раздела раздел «Сеть» (Рис. 22).

Настройка модуля «Ethernet-интерфейсы»

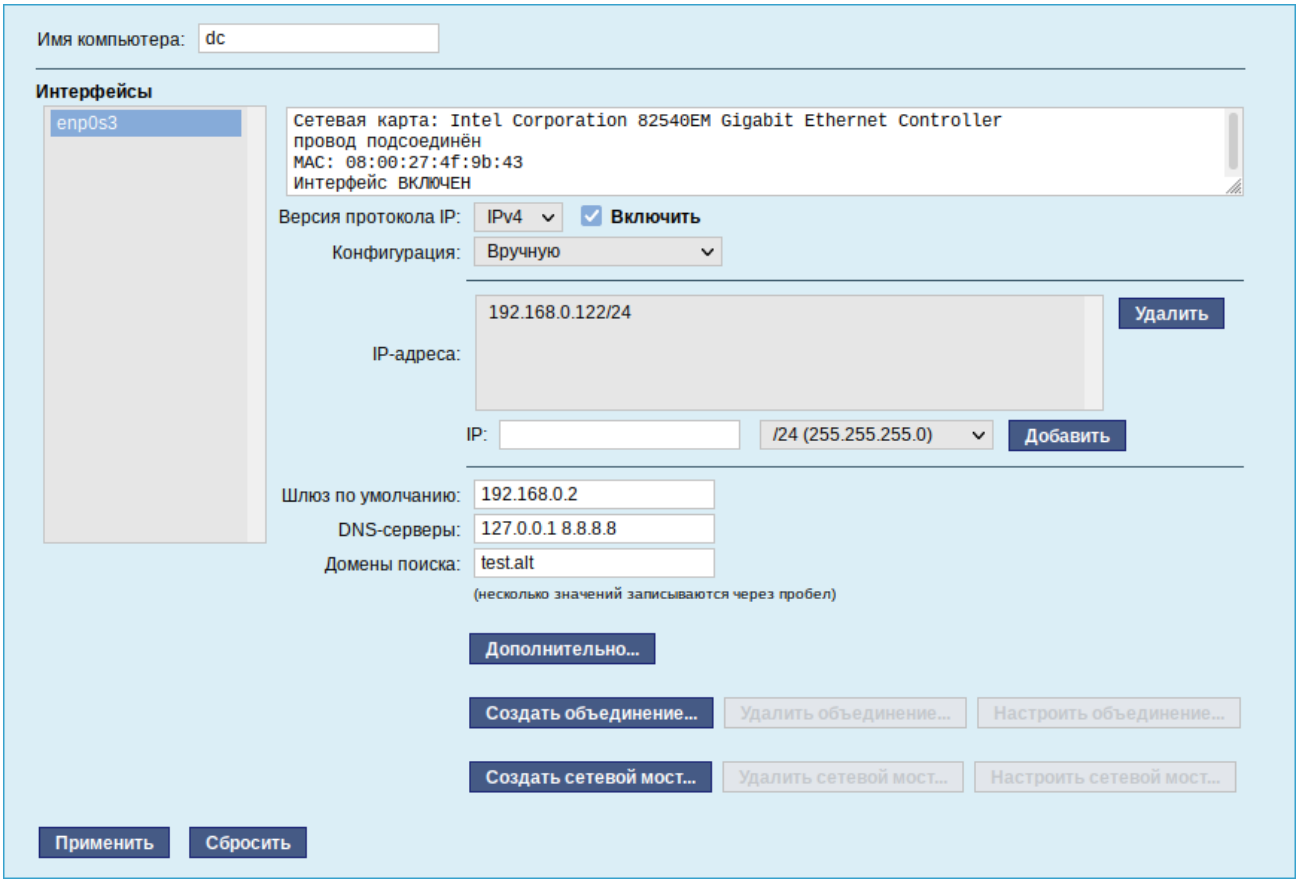


Рис. 22

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.

«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» (Рис. 23).

Автоматическое получение настроек от DHCP сервера

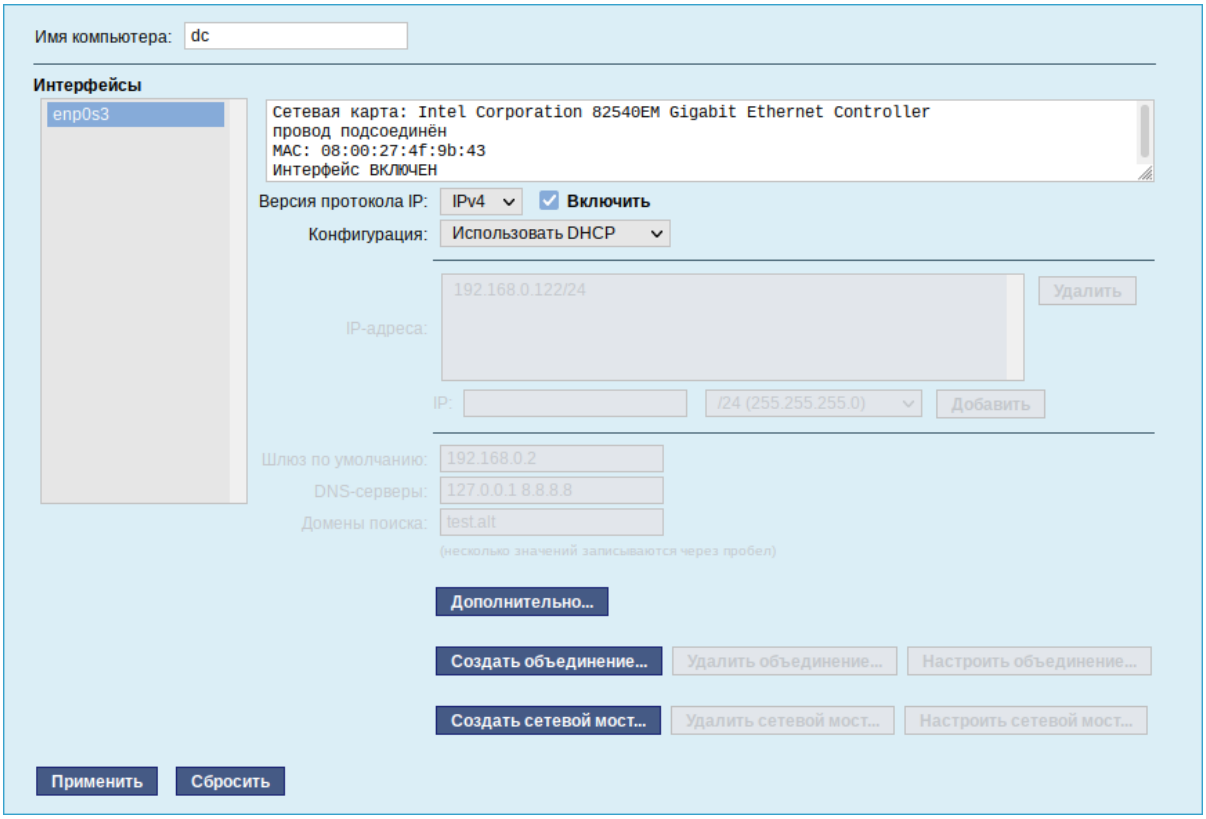


Рис. 23

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 (Рис. 24).

Выбор сетевой подсистемы

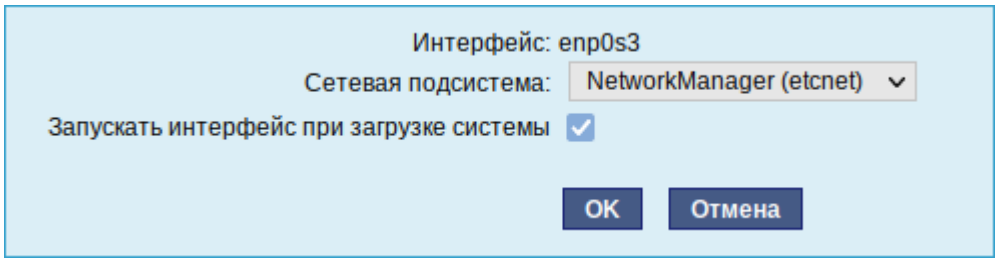


Рис. 24

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 каталоге `/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).

4.1.2 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.

4.1.2.1 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 специальная настройка рабочих станций не потребуется. 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.

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» (Рис. 25).

Модуль «Прокси-сервер»

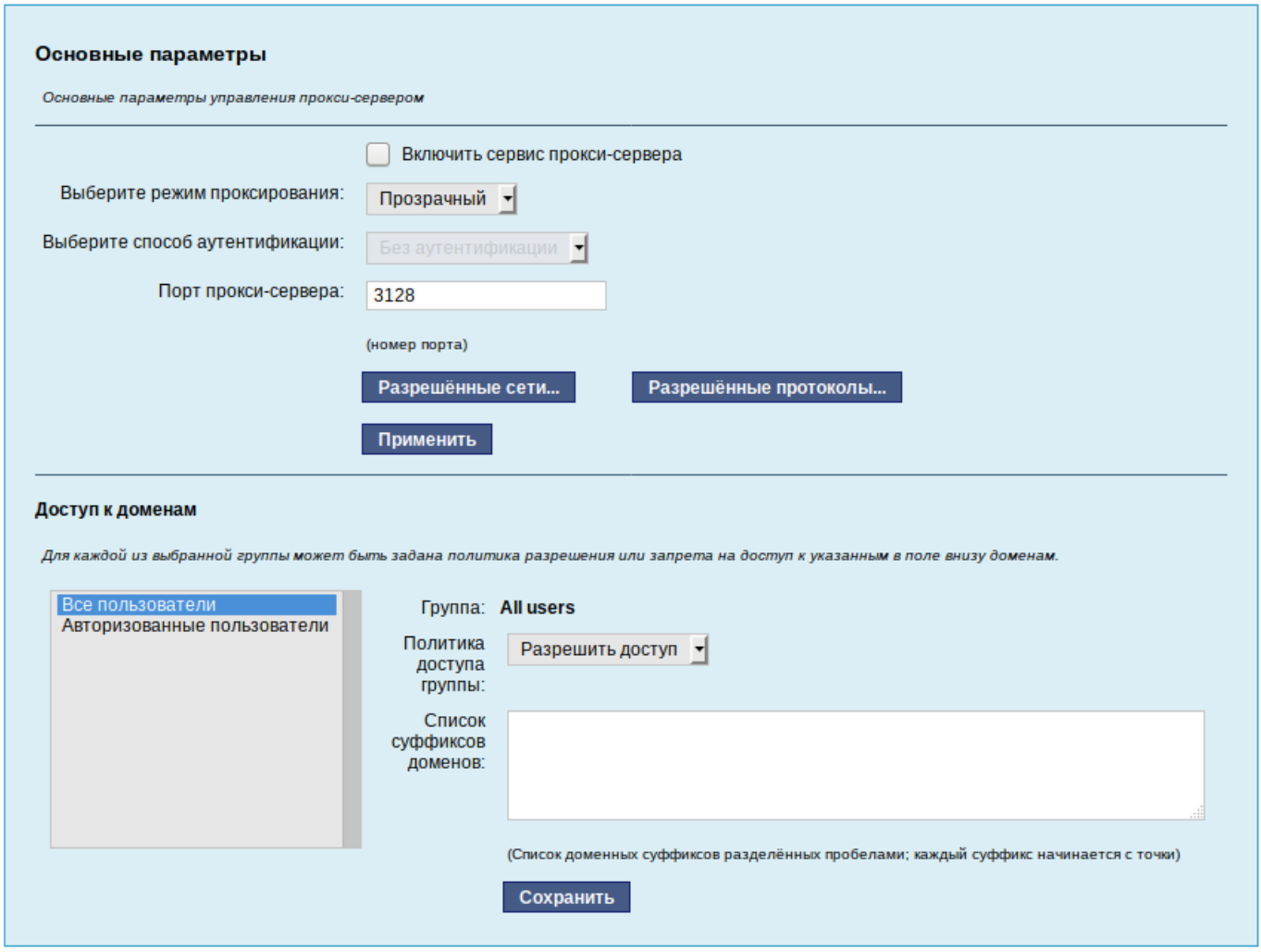


Рис. 25

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» (Рис. 26).

Настройка аутентификации пользователей

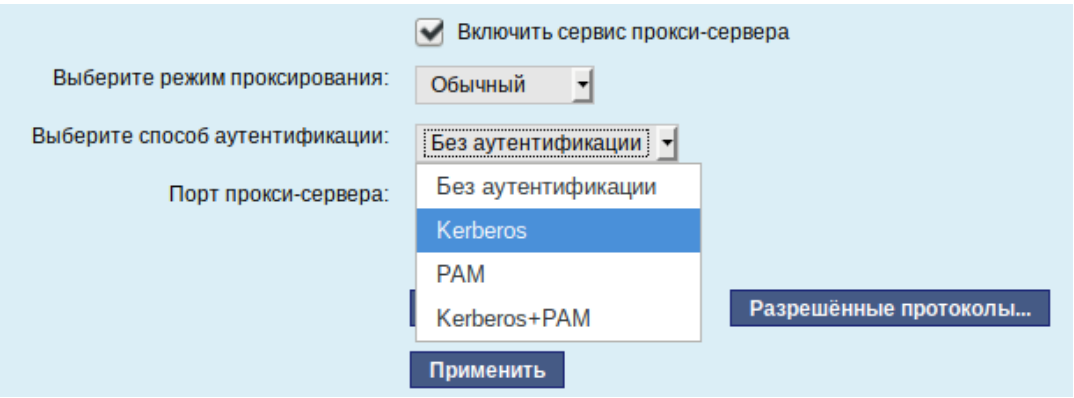


Рис. 26

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.

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» (Рис. 27).

Настройка списка внутренних сетей

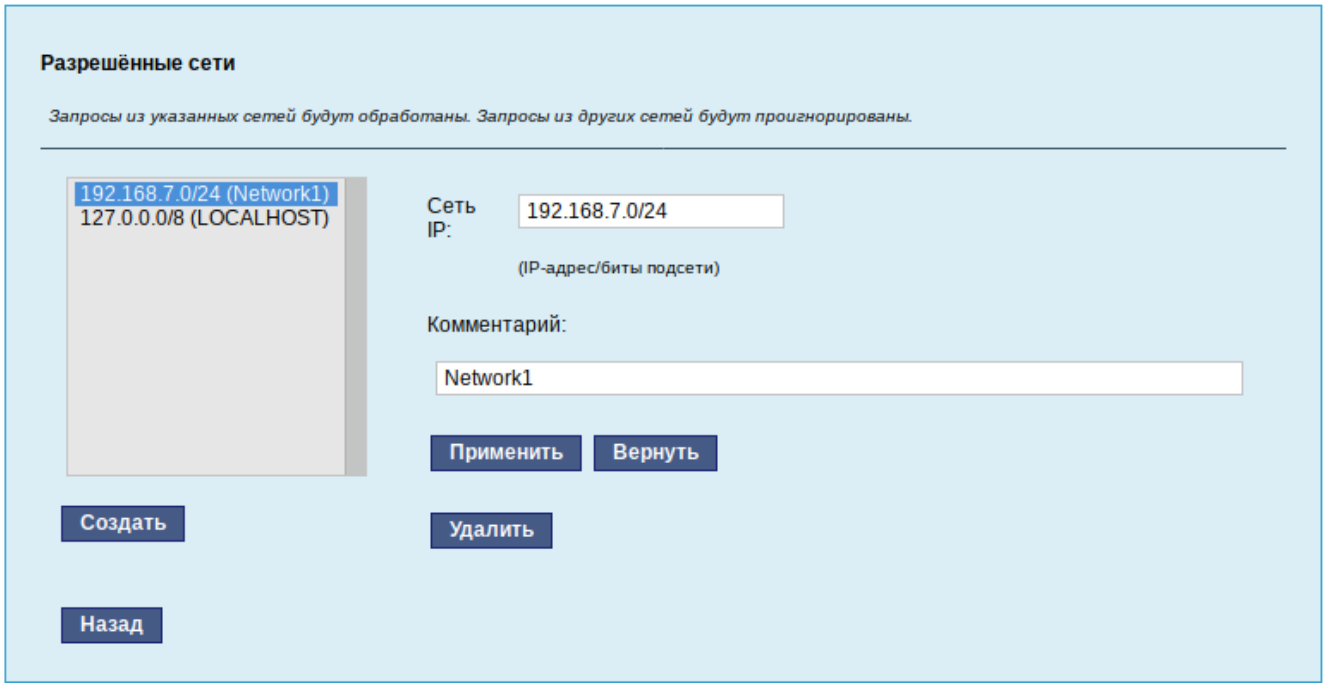


Рис. 27

Вторым условием передачи запроса является принадлежность целевого порта к разрешённому диапазону. Посмотреть и отредактировать список разрешённых целевых портов можно в разделе «Разрешённые протоколы» (Рис. 28).

Настройка списка разрешённых целевых портов

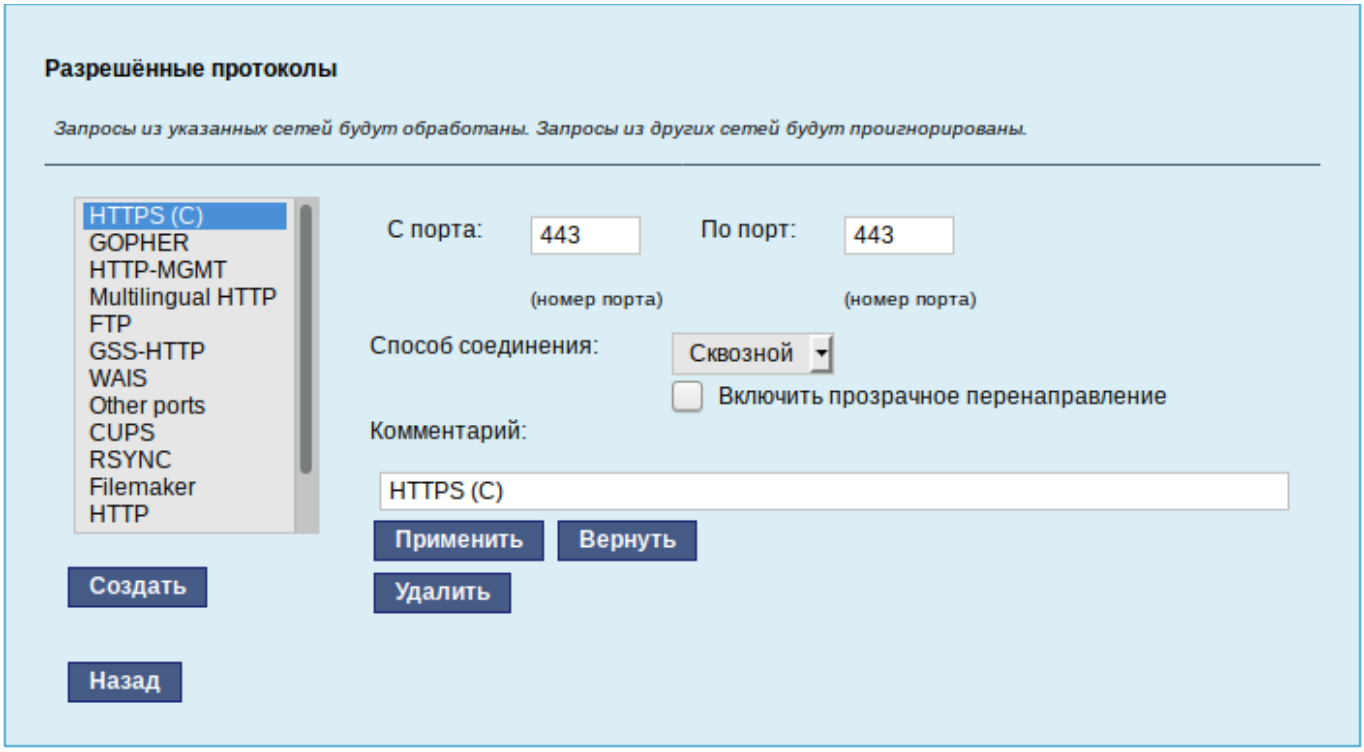


Рис. 28

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.

4.1.2.2 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 сети Интернет (общий внешний IP-адрес). При этом на компьютере-шлюзе, непосредственно подключённом к сети 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 (Рис. 29) и нажать на кнопку «Применить».

Настройка NAT в модуле «Внешние сети»

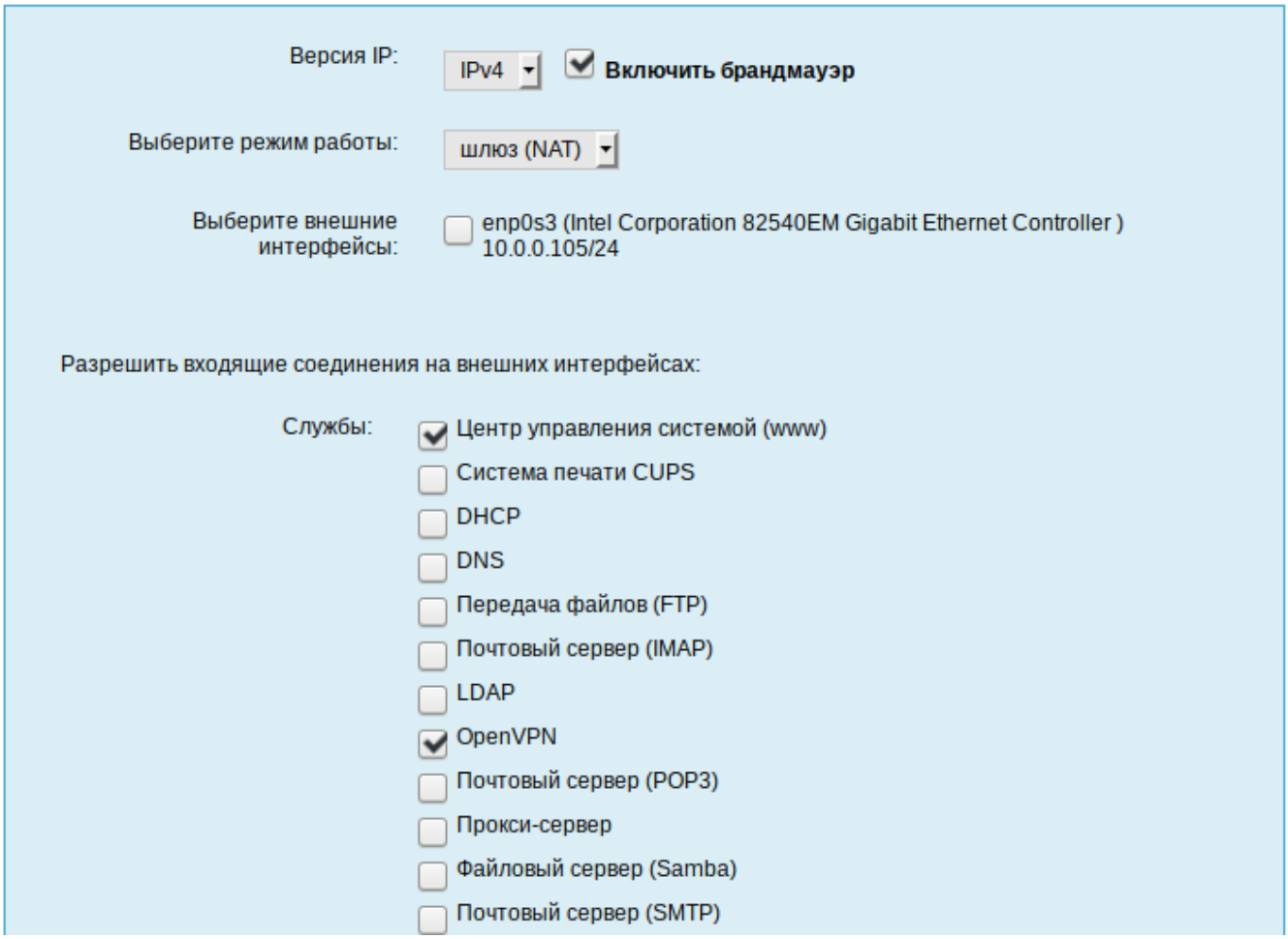


Рис. 29

4.1.3 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).

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» (Рис. 30), 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.

Настройка модуля DHCP-сервер

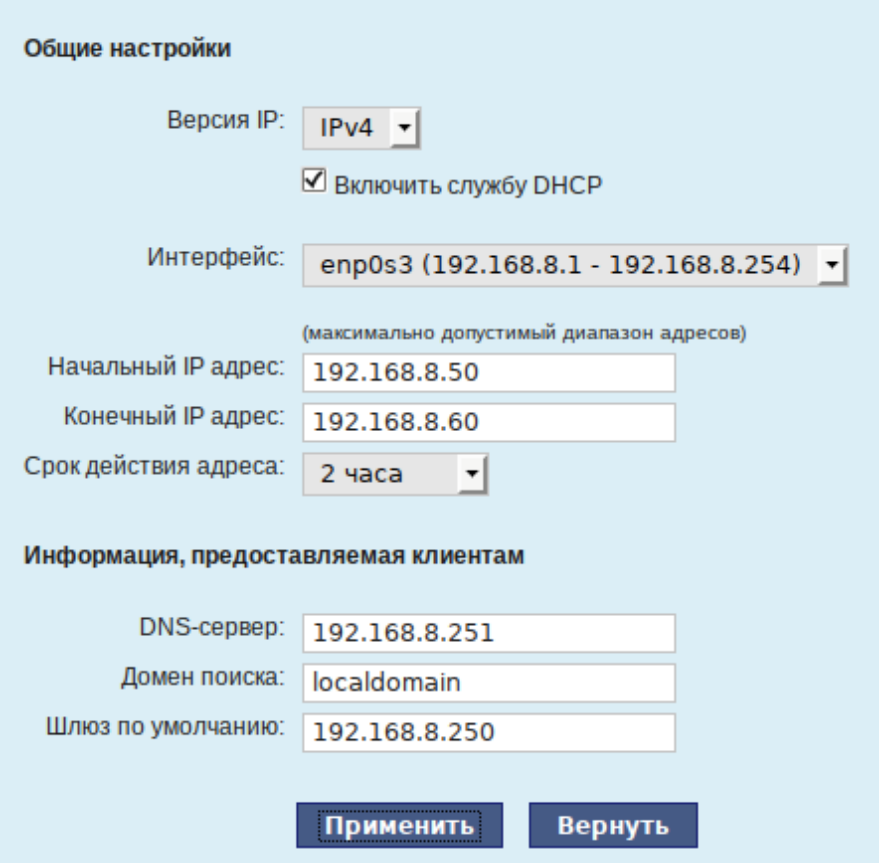


Рис. 30

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 следует ввести IP-адрес и соответствующий ему MAC-адрес и нажать кнопку «Добавить» (Рис. 31).

Привязка IP-адреса к MAC-адресу

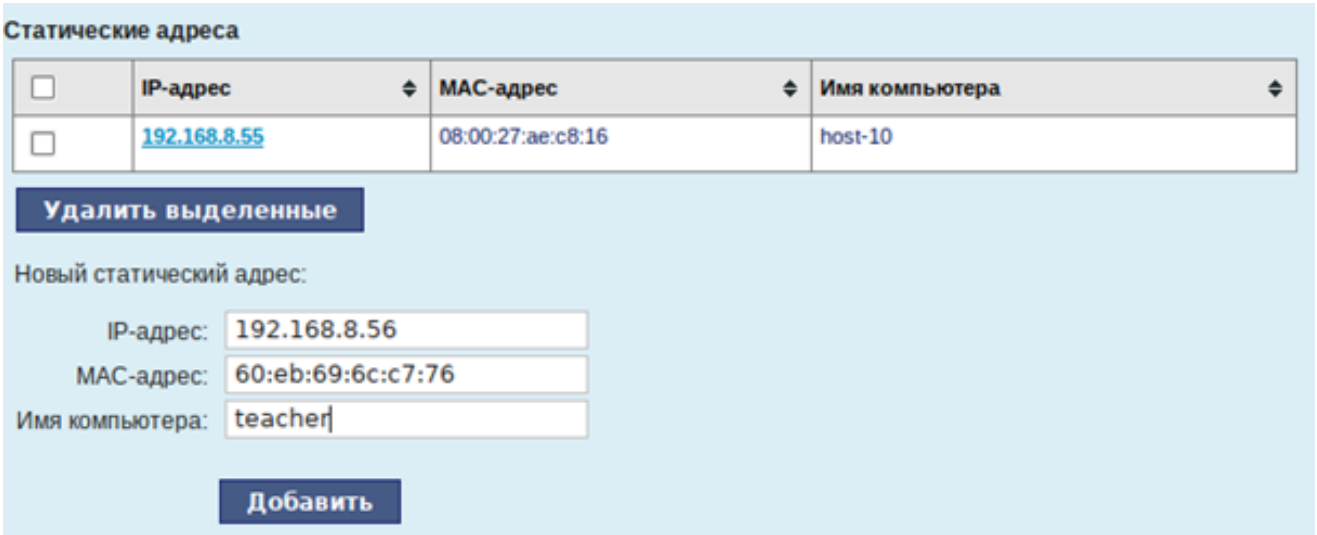


Рис. 31

Выданные IP-адреса можно увидеть в списке «Текущие динамически выданные адреса» (Рис. 32). 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».

Список динамически выданных адресов

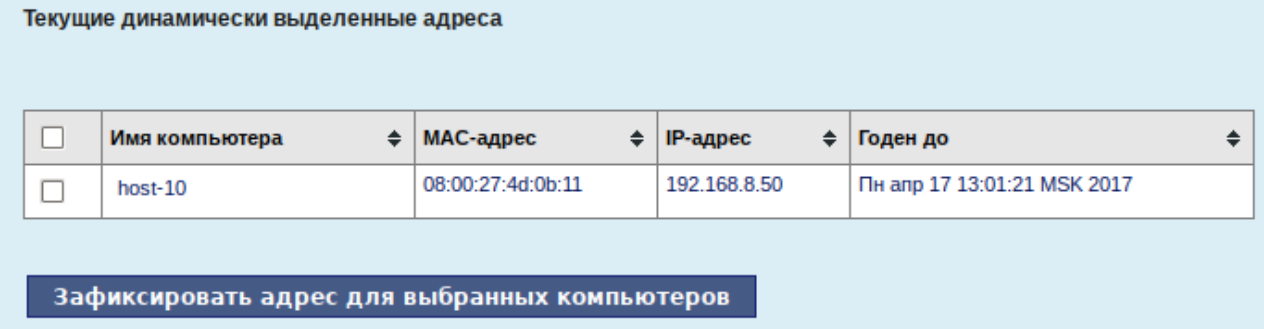


Рис. 32

4.2 Развертывание доменной структуры

Для развертывания доменной структуры предназначен модуль ЦУС «Домен» из раздела «Система» (пакет alterator-net-domain) (Рис. 33).

Настройка модуля «Домен»

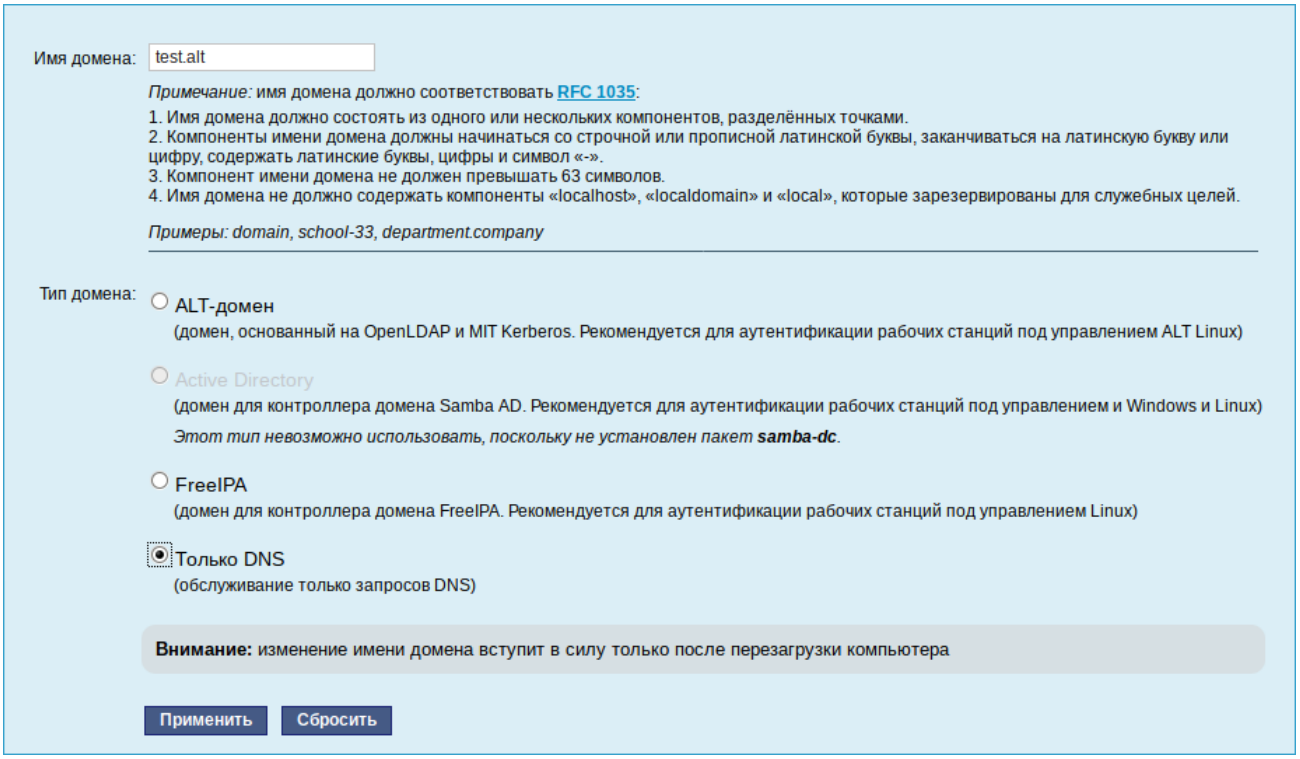


Рис. 33

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.

4.3 Сетевая установка операционной системы на рабочие места

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

4.3.1 Подготовка сервера

Перед началом установки рабочих станций следует произвести предварительную настройку сервера: задать имя сервера (модуль «Ethernet-интерфейсы» в «Центре управления системой»), 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 ОС «Альт Сервер» устанавливается 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 ОС, предварительно вставив его в DVD-привод сервера, либо можно использовать 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-9.1-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) (Рис. 34), необходимо указать, откуда импортировать новый образ и нажать кнопку «Добавить».

Процесс добавления образа (Рис. 35) занимает какое-то время.

После добавление образа он появится в списке «Доступные образы дисков». Необходимо выбрать из списка один из образов (Рис. 36) и нажать кнопку «Выбрать».

Импорт установочного образа

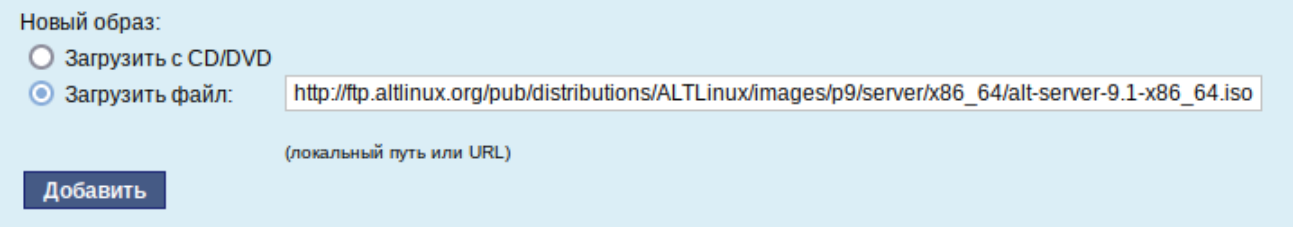


Рис. 34

Процесс добавления установочного образа

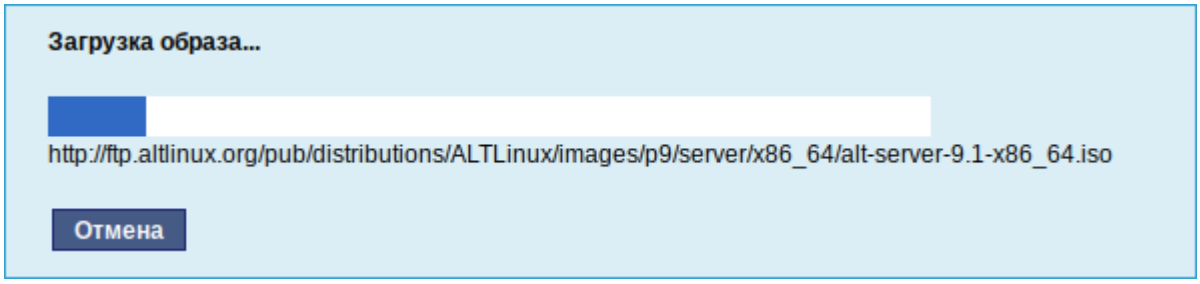


Рис. 35

Выбор образа диска

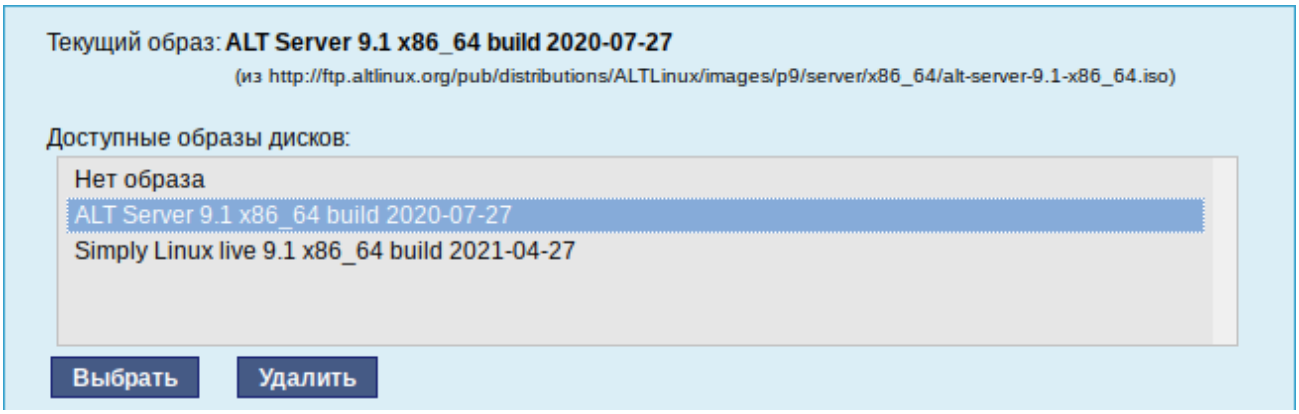


Рис. 36

На этом подготовка сервера к сетевой установке рабочих станций завершена.

Далее необходимо выбрать направление соединения (Рис. 37). Удалённый доступ к компьютеру бывает двух видов:

1. 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.
2. 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.

Выбор направления соединения

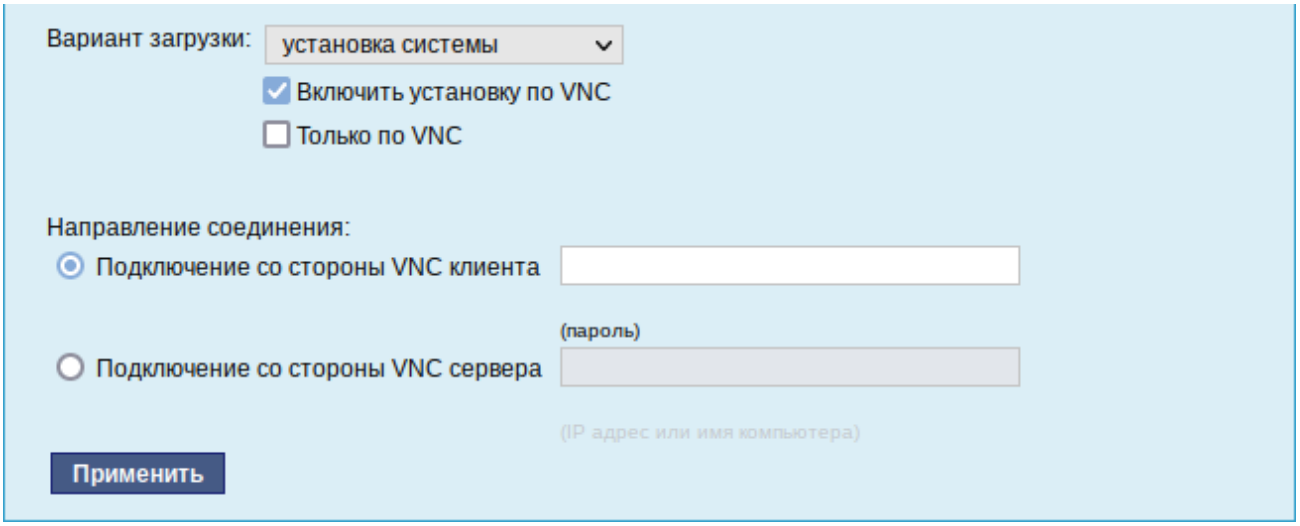


Рис. 37

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, необходимо отметить пункт «Включить установку по VNC» и пункт «Подключение со стороны VNC сервера» раздела «Направление соединения», и там указать адрес компьютера, с которого будет происходить управление. Для приёма подключения можно запустить, например, vncviewer -listen.

Примечание. По окончании процесса установки ОС на рабочих станциях необходимо отключить сетевую установку. Это можно сделать, выбрав в списке «Доступные образы дисков» пункт «Нет образа» и подтвердив действие нажатием кнопки «Выбрать».

4.3.2 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 From Onboard LAN».

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

4.4 Сервер электронной почты (SMTP, POP3/IMAP)

ОС «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 «Почтовый сервер» (пакет alterator-postfix-dovecot) из раздела «Серверы» (Рис. 38).

Модуль «Почтовый сервер»

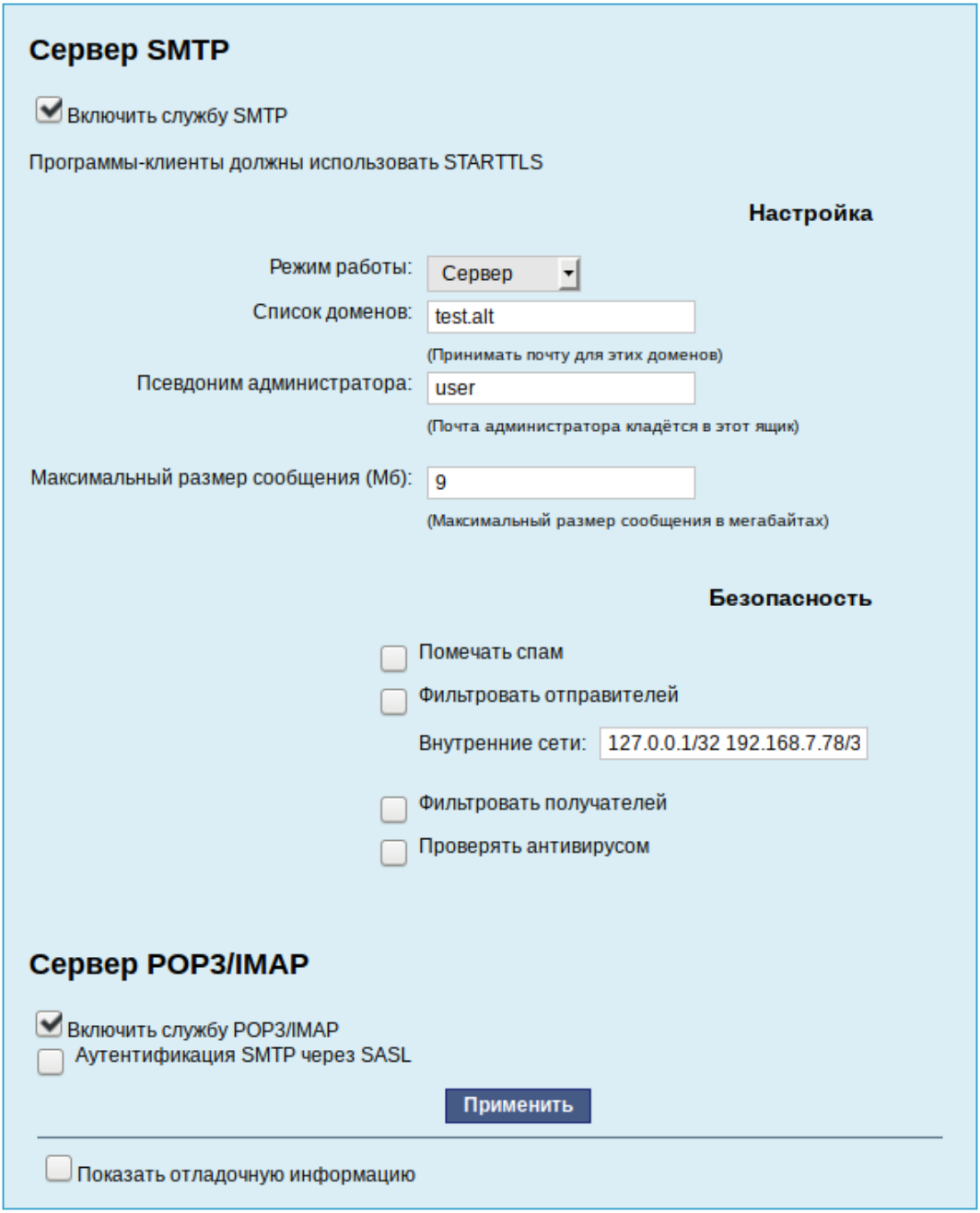


Рис. 38

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.

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.

4.5 Соединение удалённых офисов (OpenVPN-сервер)

ОС «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, можно 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.

4.5.1 Настройка OpenVPN-сервера

Модуль «OpenVPN-сервер» (пакет alterator-openvpn-server) из раздела «Серверы» позволяет задать параметры OpenVPN-сервера (Рис. 39).

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.

Модуль «OpenVPN-сервер»

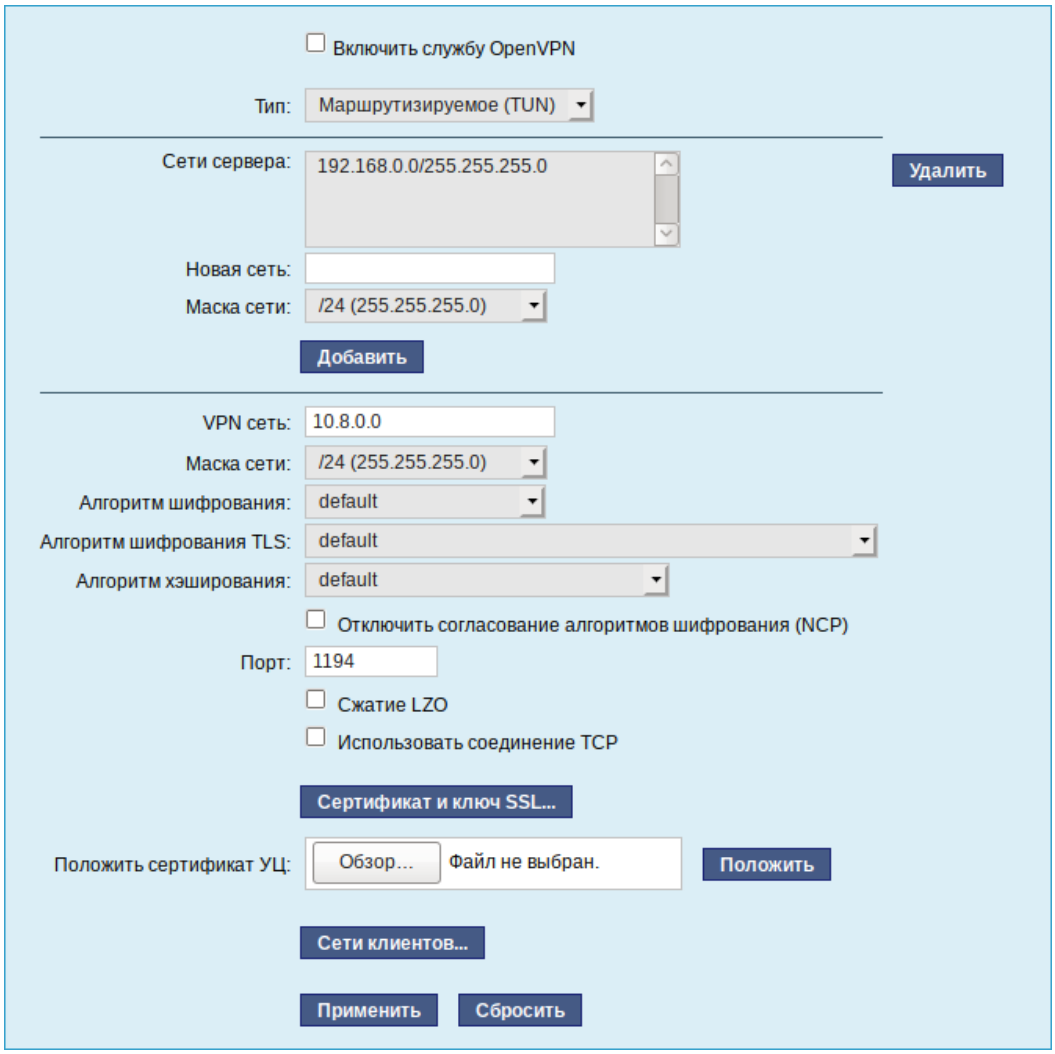


Рис. 39

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) (Рис. 40).

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» (Рис. 41).

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

Модуль «Управление ключами SSL»

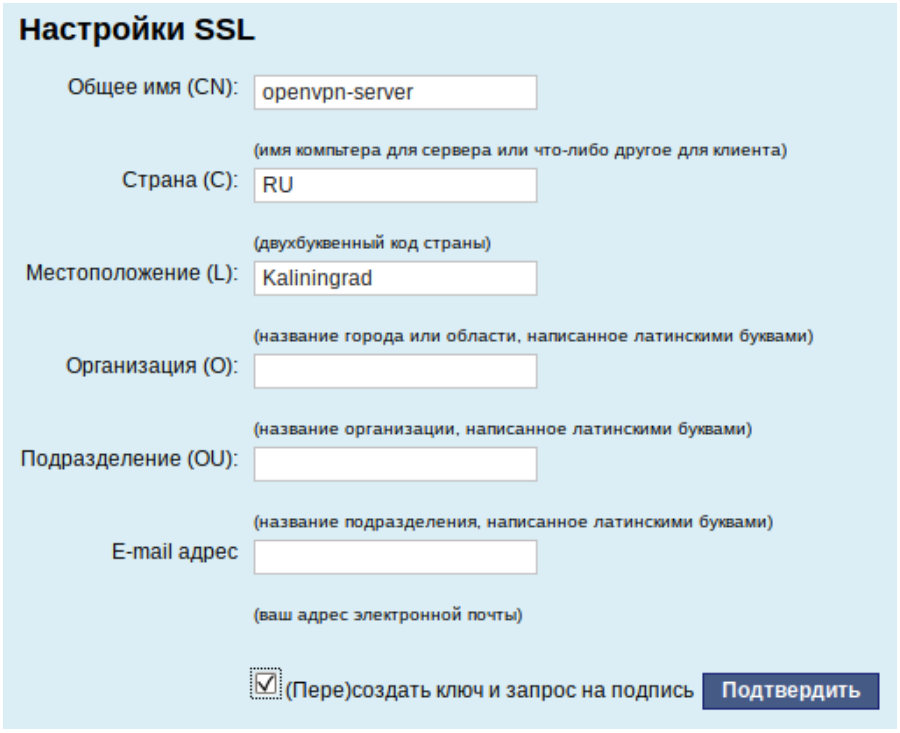


Рис. 40

Забрать запрос на подпись

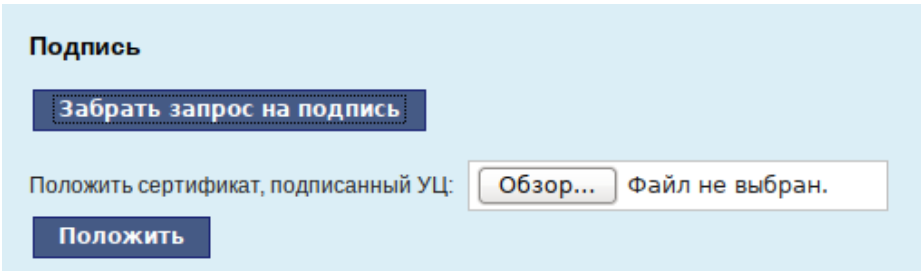


Рис. 41

В модуле «Управление ключами SSL» появился новый ключ: «openvpn-server (Нет сертификата)» (Рис. 42).

Ключ openvpn-server

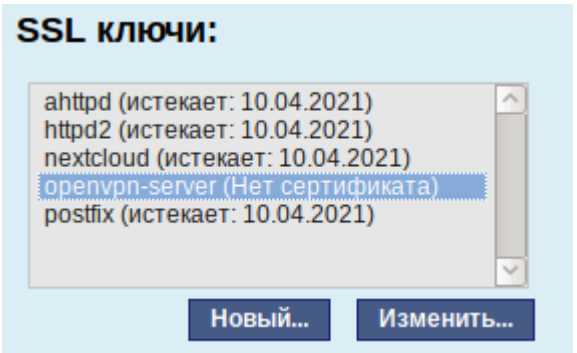


Рис. 42

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 (Рис. 43).

Запрос на подпись сертификата

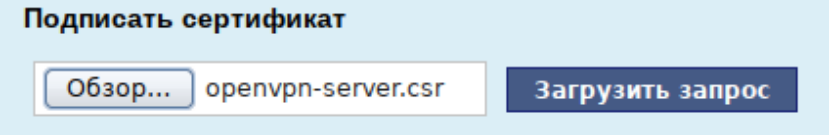


Рис. 43

В результате на экране появится две группы цифр и кнопка «Подписать» (Рис. 44). Необходимо нажать на кнопку «Подписать» и сохранить файл `output.pem` (подписанный сертификат).

Запрос на подпись сертификата

Рис. 44

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» (Рис. 45).

Сертификат, подписанный УЦ

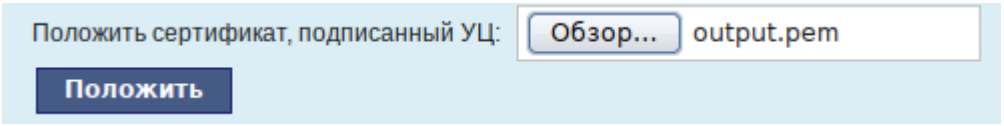


Рис. 45

В модуле «Управление ключами SSL», видно, что ключ openvpn-server (истекает_и_дата) изменился. 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» (Рис. 46).

Сертификат УЦ

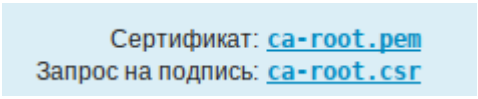


Рис. 46

В модуле «OpenVPN-сервер», в графе «Положить сертификат УЦ»: при помощи кнопки «Обзор» указать путь к файлу `ca-root.pem` и нажать кнопку «Положить» (Рис. 47).

Выбор сертификата УЦ в модуле «OpenVPN-сервер»

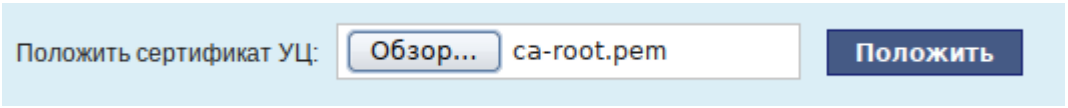


Рис. 47

Появится сообщение: «Сертификат УЦ успешно загружен».

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

4.5.2 Настройка клиентов

Со стороны клиента соединение настраивается в модуле «OpenVPN-соединения» (пакет alterator-net-openvpn) из разделаразделе «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» (Рис. 48). Должен быть выбран тот же тип, что и на стороне сервера.

Создание нового OpenVPN- соединения

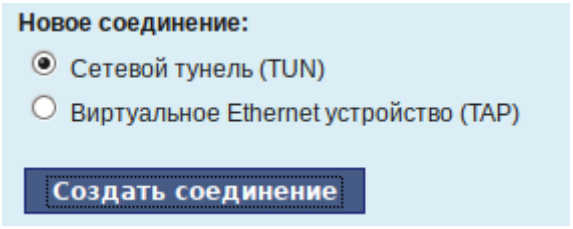


Рис. 48

Неоходимо обратить 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) на сервере.

В результате станут доступны настройки соединения (Рис. 49).

Модуль «OpenVPN- соединения»

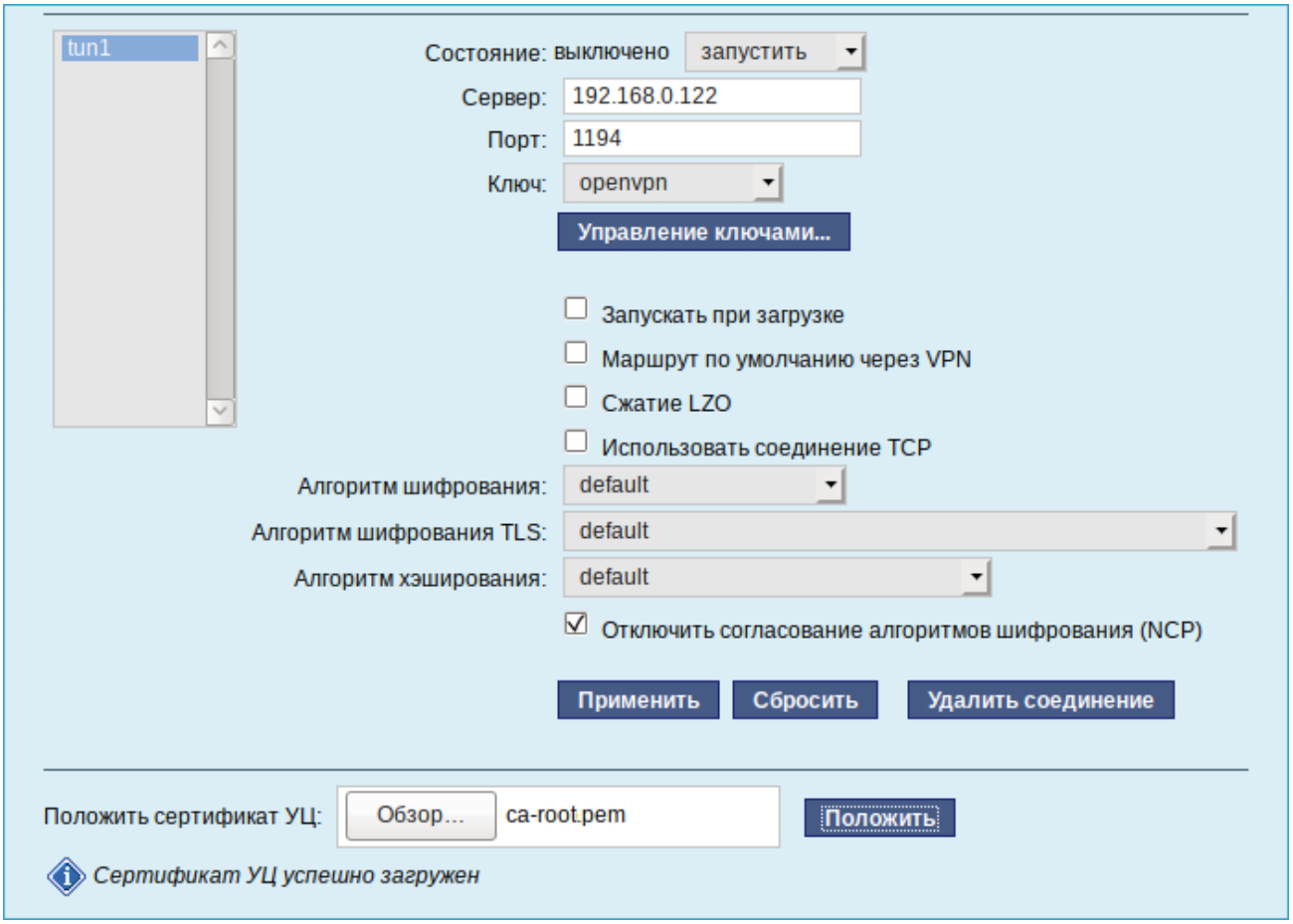


Рис. 49

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.

4.6 Доступ к службам сервера из сети Интернет

4.6.1 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, можно сделать их доступными для соединений на внешних сетевых интерфейсах (Рис. 50). Если необходимо предоставить доступ к службе, отсутствующей в списке, то нужно задать используемые этой службой порты в соответствующих полях.

Можно выбрать один из двух режимов работы:

- роутер – 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 на компьютере настроен, по крайней мере, один внешний и один внутренний интерфейс.

Модуль «Внешние сети»

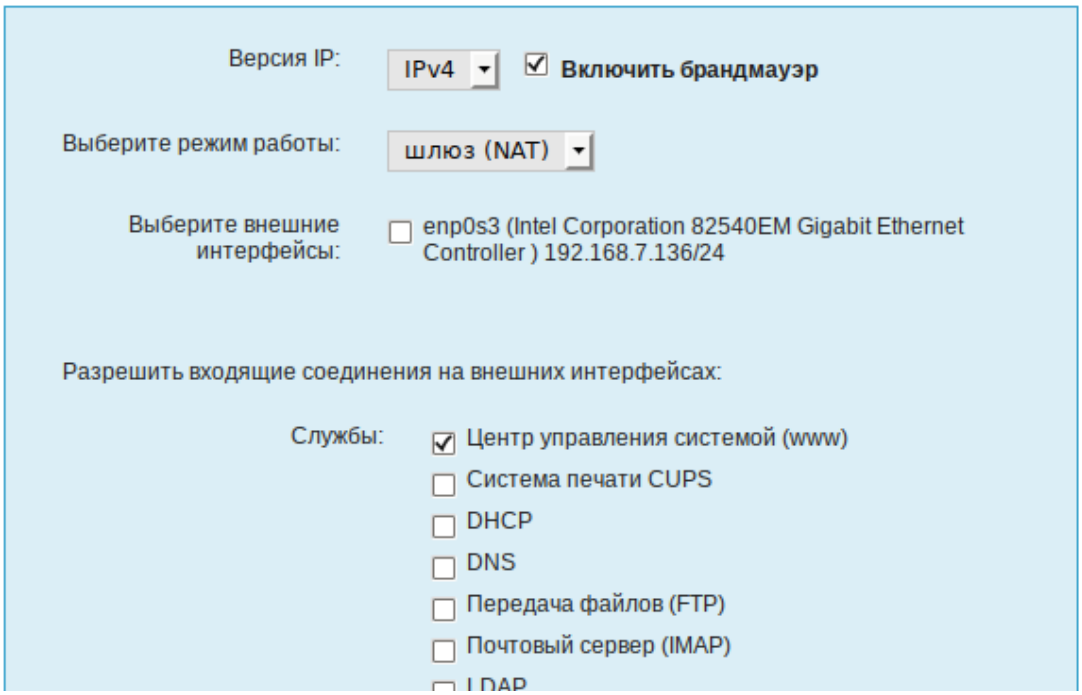


Рис. 50

В любом режиме включено только перенаправление пакетов с внутренних интерфейсов. Перенаправление пакетов с внешних интерфейсов всегда выключено. Все внутренние интерфейсы открыты для любых входящих соединений.

4.6.2 Список блокируемых хостов

Модуль «Список блокируемых хостов» (пакет alterator-net-bl) позволяет настроить блокировку любого сетевого трафика с указанных в списке узлов (входящий, исходящий и пересылаемый).

Блокирование трафика с указанных в списке узлов начинается после установки флажка «Использовать чёрный список» (Рис. 51).

Модуль «Список блокируемых хостов»

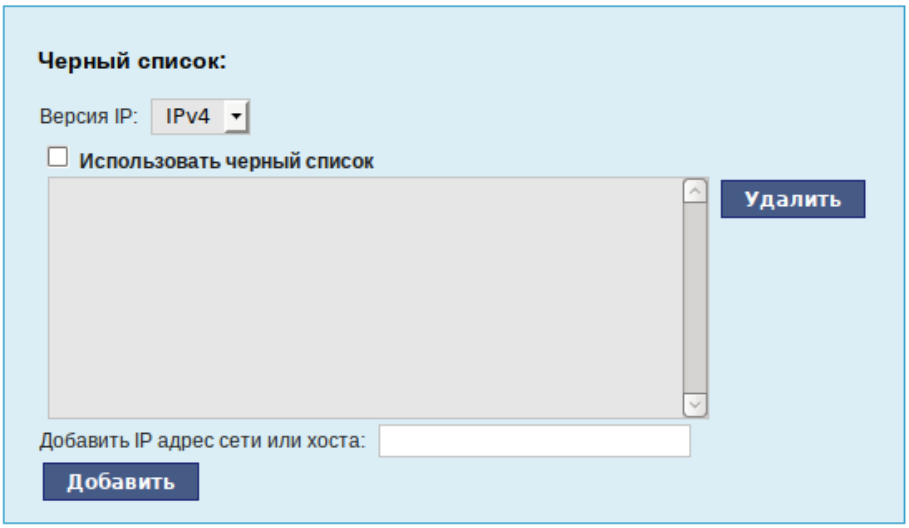


Рис. 51

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

Для удаления узла необходимо выбрать его из списка и нажать кнопку «Удалить».

4.7 Статистика

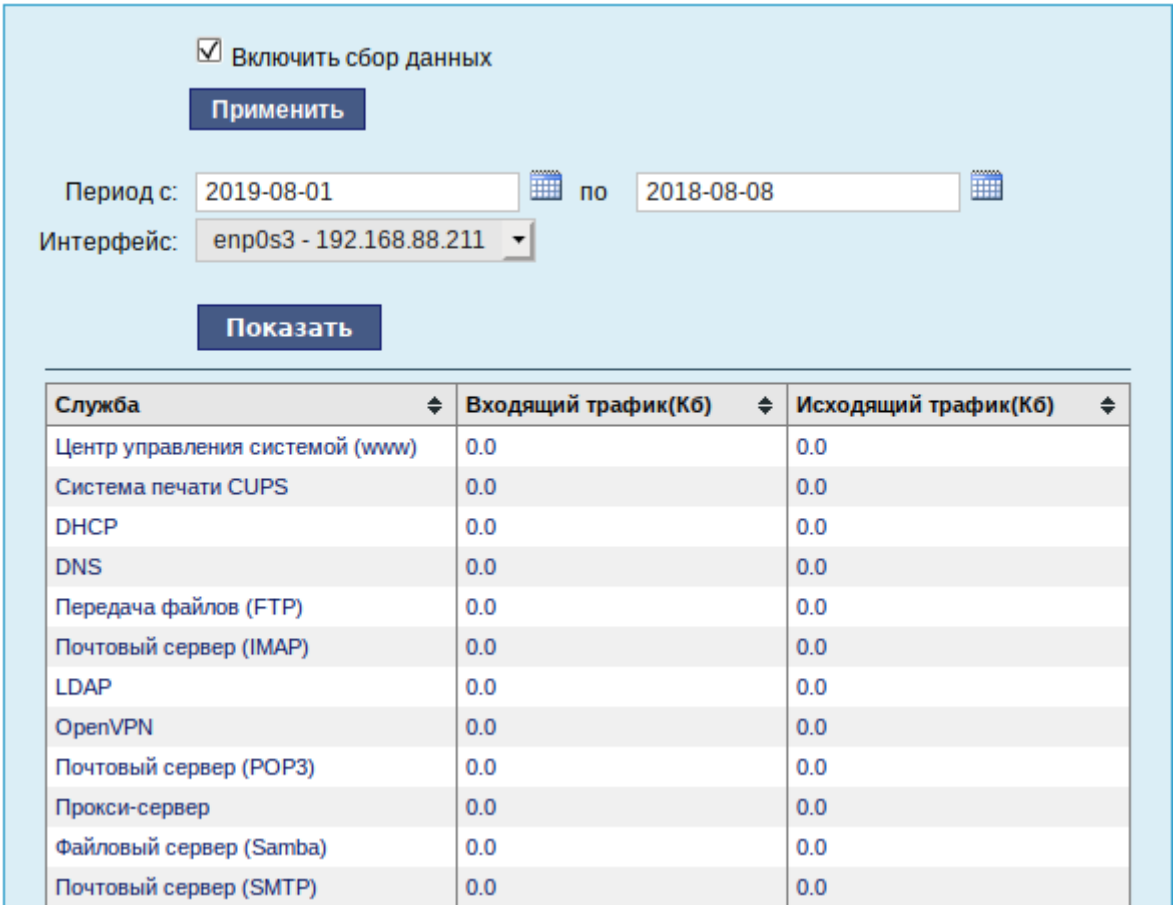
4.7.1 Сетевой трафик

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» (Рис. 52).

Просмотр статистики входящих и исходящих пакетов



Служба	Входящий трафик(Кб)	Исходящий трафик(Кб)
Центр управления системой (www)	0.0	0.0
Система печати CUPS	0.0	0.0
DHCP	0.0	0.0
DNS	0.0	0.0
Передача файлов (FTP)	0.0	0.0
Почтовый сервер (IMAP)	0.0	0.0
LDAP	0.0	0.0
OpenVPN	0.0	0.0
Почтовый сервер (POP3)	0.0	0.0
Прокси-сервер	0.0	0.0
Файловый сервер (Samba)	0.0	0.0
Почтовый сервер (SMTP)	0.0	0.0

Рис. 52

Для просмотра статистики указывается 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» (Рис. 52).

Трафик на указанном интерфейсе за заданный период показывается в виде:

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

4.7.2 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. Включить её сбор следует в модуле ЦУС «Прокси-сервер» (пакет alterator-squidmill) из раздела «Статистика». Для включения сбора

статистики прокси-сервера необходимо установить флажок «Включить сбор данных прокси-сервера» (Рис. 53).

Настройка сбора статистики прокси-сервера

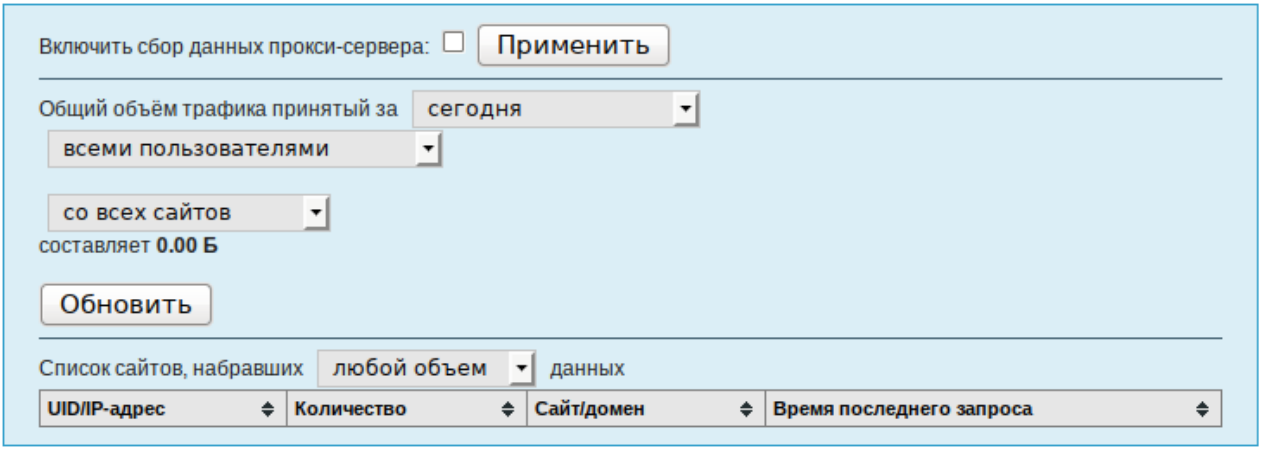


Рис. 53

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 необходимо задать условия фильтра и нажать кнопку «Показать». Данные в таблице 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.

4.8 Обслуживание сервера

Регулярный мониторинг состояния сервера, своевременное резервное копирование, обновление установленного ПО, являются важной частью комплекса работ по обслуживанию сервера.

4.8.1 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» (Рис. 54).

Модуль «Системные журналы»

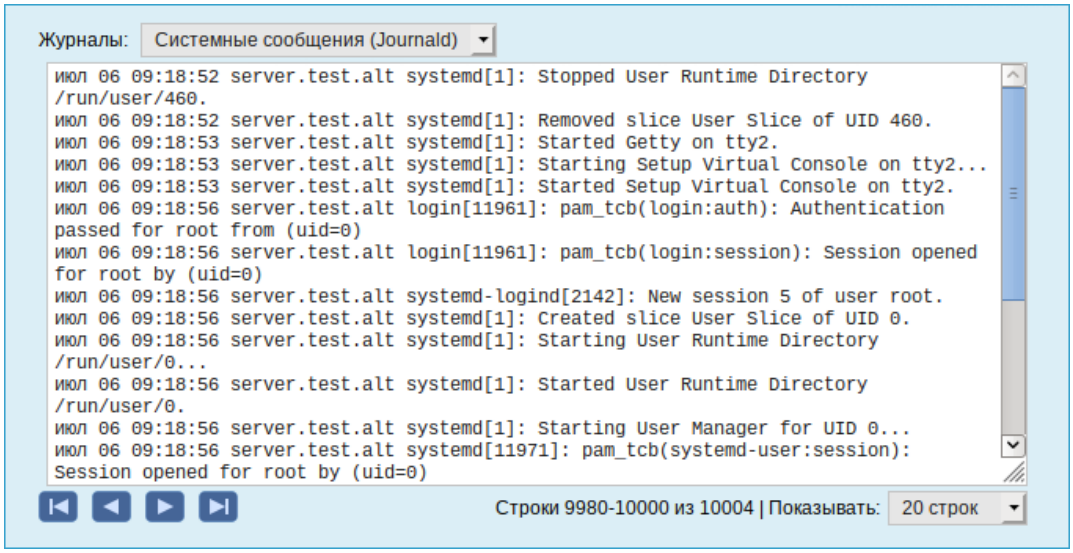


Рис. 54

Доступны следующие виды журналов:

– Брандмауэр – отображаются события безопасности, связанные с работой межсетевого экрана ОС;

– Системные сообщения – сообщения от системных служб (сообщения с типом DAEMON).

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

4.8.2 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 (Рис. 55).

Модуль «Системные службы»

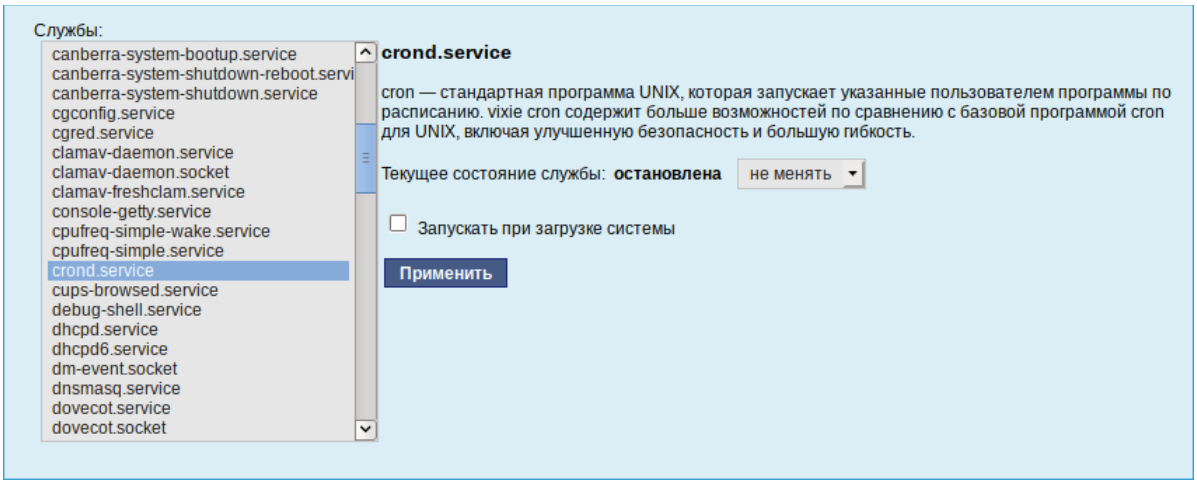


Рис. 55

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

4.8.3 Резервное копирование

Резервное копирование является важной частью работ по поддержанию работоспособности сервера и всего домена.

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:

- 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 «Альт Сервер» установленная из пакетов Bacula уже настроена для резервного копирования конфигурации ОС.

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» (Рис. 56);

Создание клиента резервного копирования

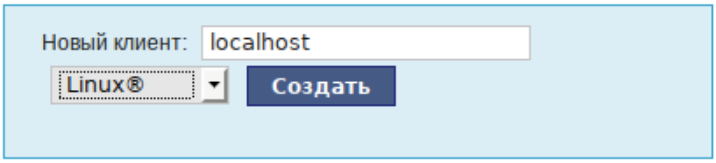


Рис. 56

– указать пароль для клиента и включаемые и исключаемые каталоги;
– нажать кнопку «Сохранить параметры»;
– нажать ссылку «Конфигурационный файл клиента» и сохранить 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).

В разделе «Сервер резервного копирования» → «Расписание» указывается время проведения инкрементного резервного копирования для каждого клиента (Рис. 57). В этом же разделе можно отключить резервное копирование для выбранных клиентов.

Настройка расписания резервного копирования

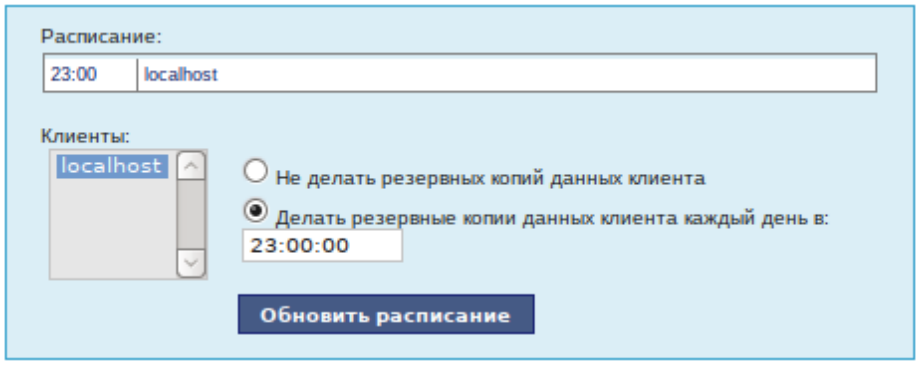


Рис. 57

Модуль ЦУС «Архив» для выбранного клиента (выбирается из списка «Клиенты») позволяет запустить создание резервной копии вне расписания, удалить все резервные копии или восстановить данные этого клиента (Рис. 58).

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.

Модуль «Архив»

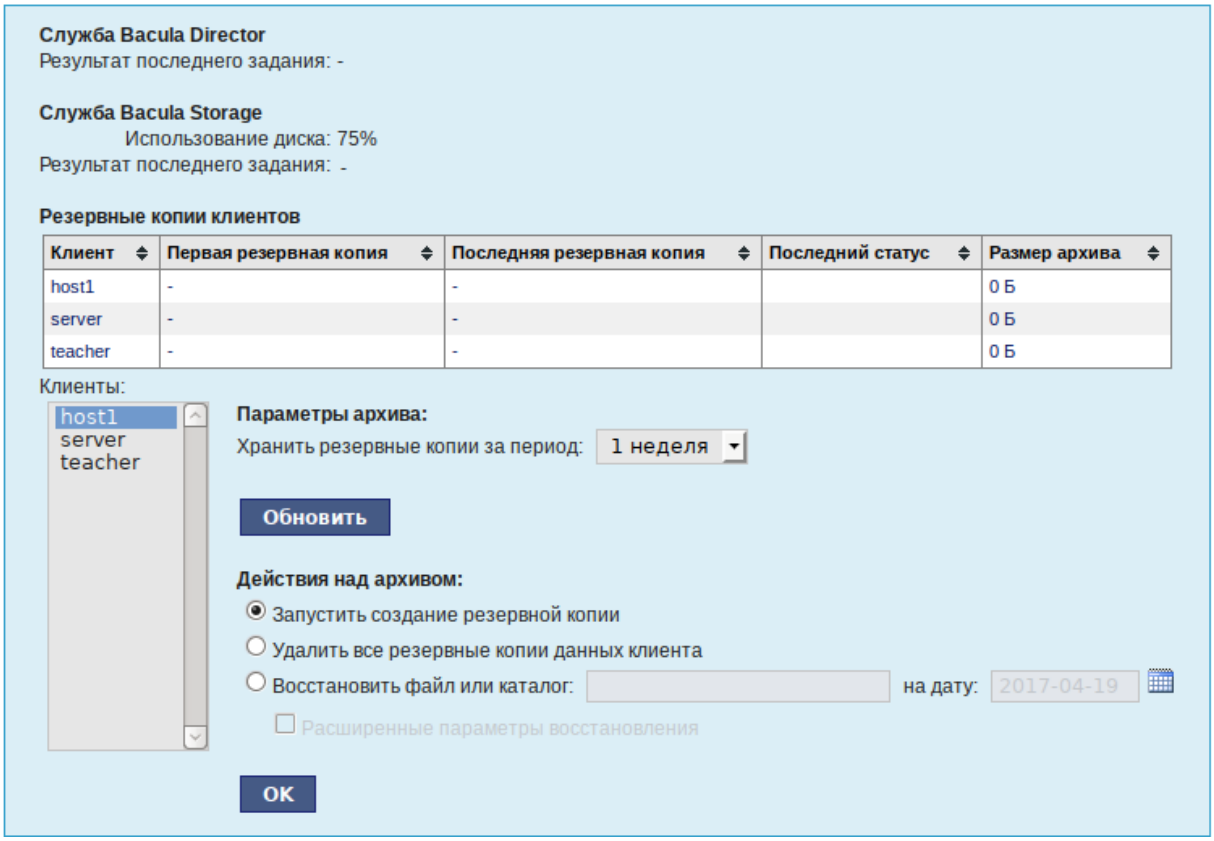


Рис. 58

4.8.4 Обновление системы

После установки системы крайне важно следить за обновлениями ПО. Обновления для ОС «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 (Рис. 59).

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.

Модуль «Обновление системы»

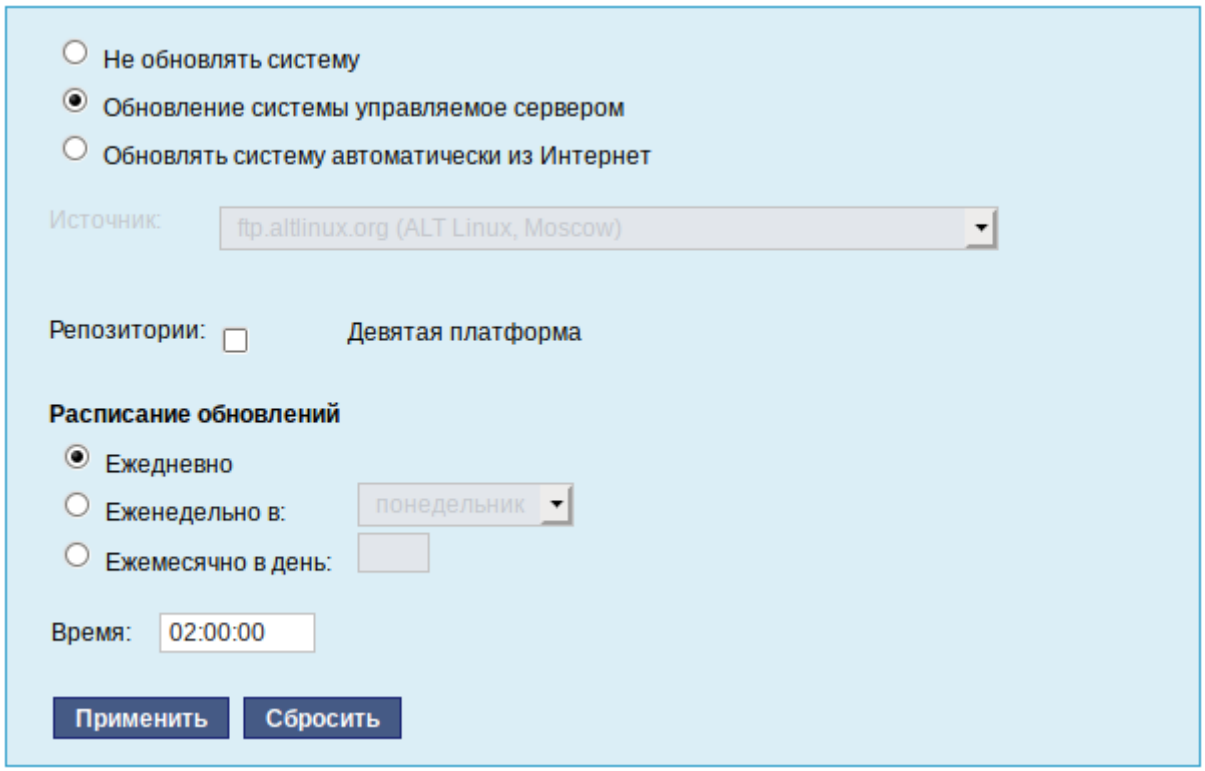


Рис. 59

4.8.5 Обновление ядра ОС

Модуль «Обновление ядра» (пакет alterator-update-kernel) 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 (Рис. 60).

Интерфейс модуля «Обновление ядра»

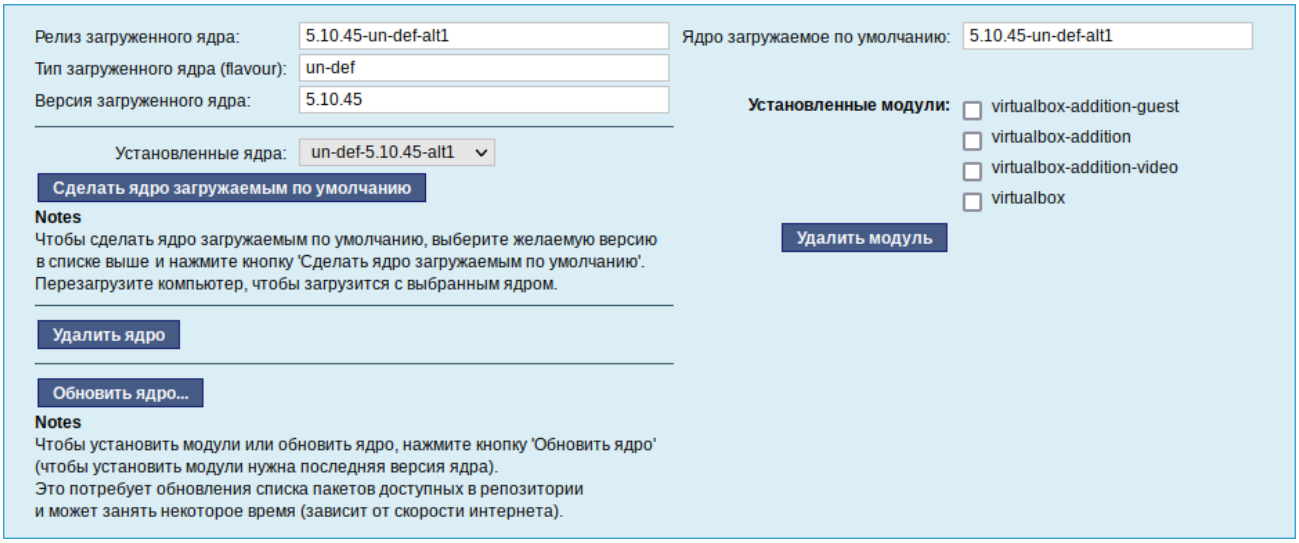


Рис. 60

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 новые 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». Установленное ядро станет загружаемым по умолчанию.

Примечание. Новое ядро загрузится только после перезагрузки системы.

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

Если ядро не требует обновления (Рис. 61), в окне «Доступные модули» можно отметить модули ядра необходимые к установке и нажать кнопку «Установить модули».

Доступное к установке ядро

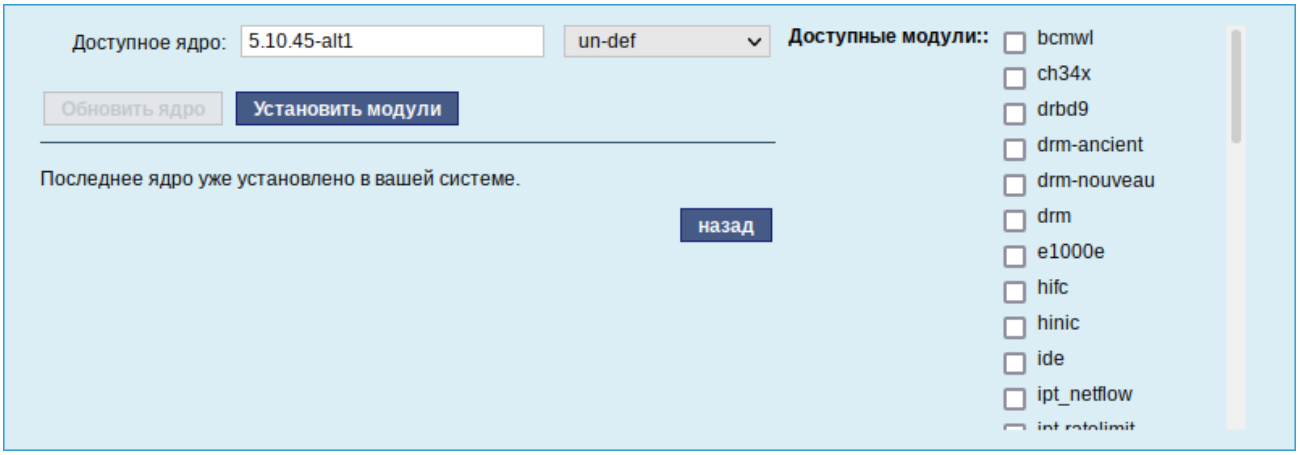


Рис. 61

4.8.6 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.

На странице модуля можно выбрать, как часто выполнять закачку пакетов, можно выставить время, когда начинать зеркалирование (Рис. 62).

Здесь также можно выбрать репозитории, локальные срезы которых необходимы. При нажатии на название репозитория, появляются настройки этого репозитория (Рис. 63). Необходимо выбрать источник, архитектуру процессора (если их несколько, то стоит выбрать соответствующие).

П р и м е ч а н и е . При выборе любой архитектуры также будет добавлен источник с noarch.

Модуль «Сервер обновлений»

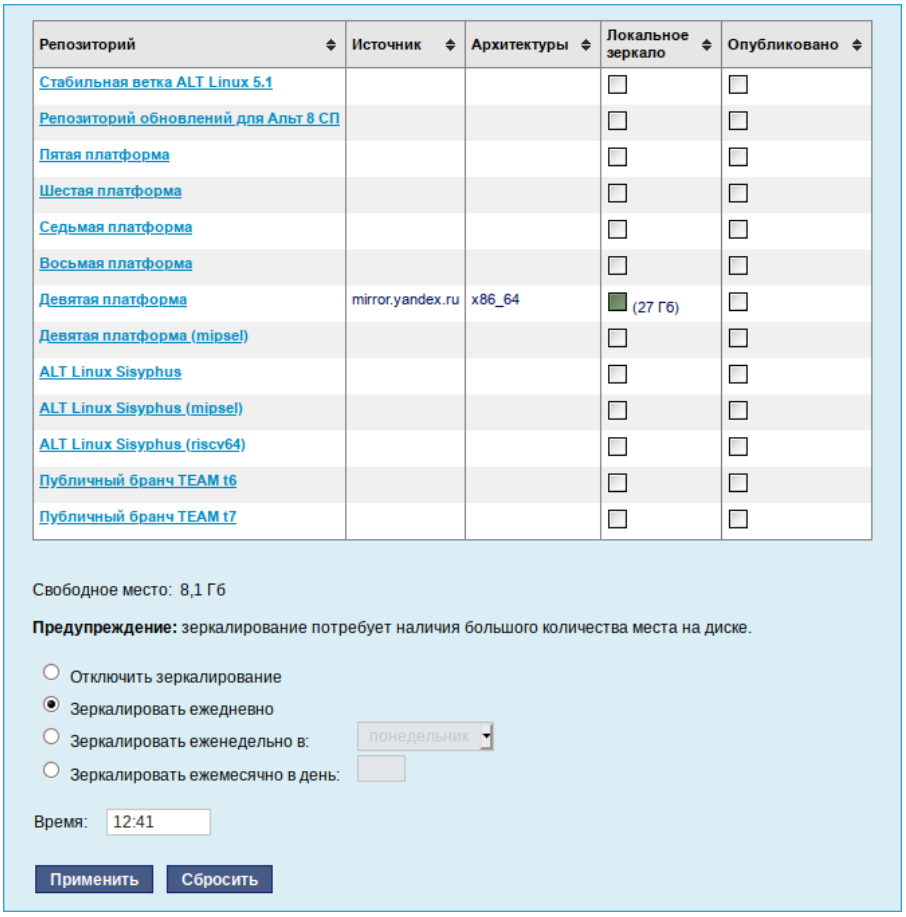


Рис. 62

Настройки репозитория

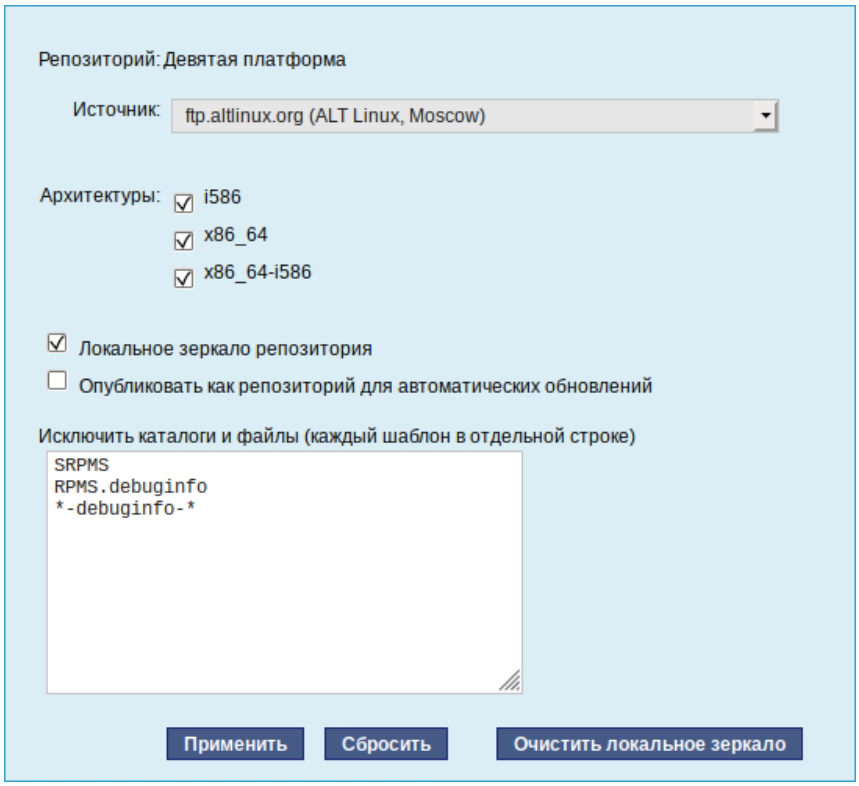


Рис. 63

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 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.

  Примечание. 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 пункт «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 следующую строку:

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

где `/media/disk/localrepo` – папка-хранилище локального репозитория.

4.8.6.1 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
```

4.8.6.2 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 = 0.0.0.0 # 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
```

4.8.7 Локальные учётные записи

Модуль «Локальные учётные записи» (пакет alterator-users) из раздела «Пользователи» предназначен для администрирования системных пользователей (Рис. 64).

Веб-интерфейс модуля alterator-users

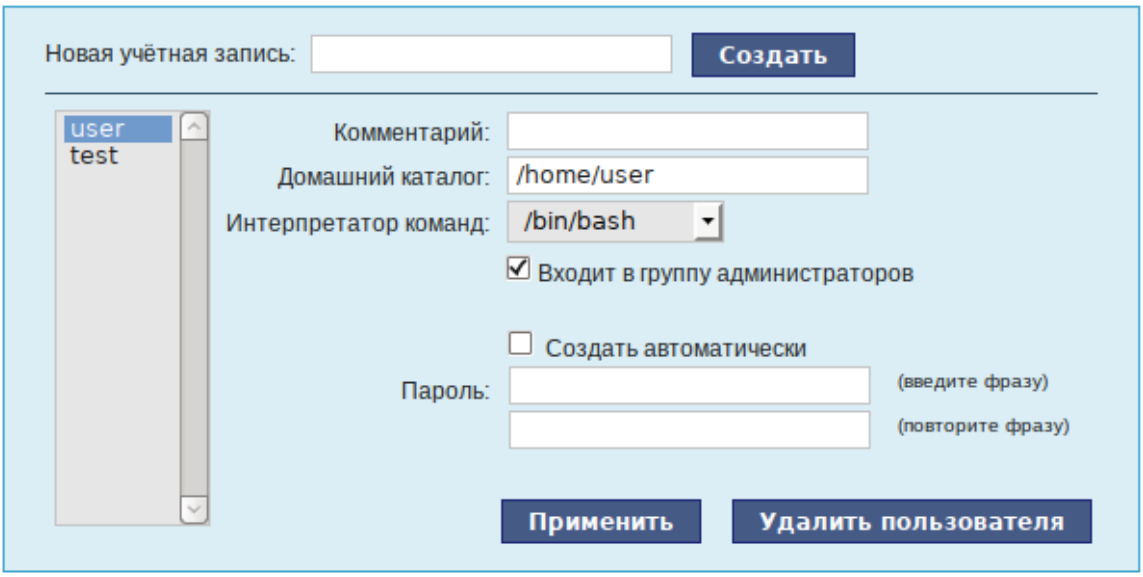


Рис. 64

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.

4.8.8 Администратор системы

В модуле «Администратор системы» (пакет alterator-root) из раздела «Пользователи» можно изменить пароль суперпользователя (root), заданный при начальной настройке системы (Рис. 65).

Модуль «Администратор системы»

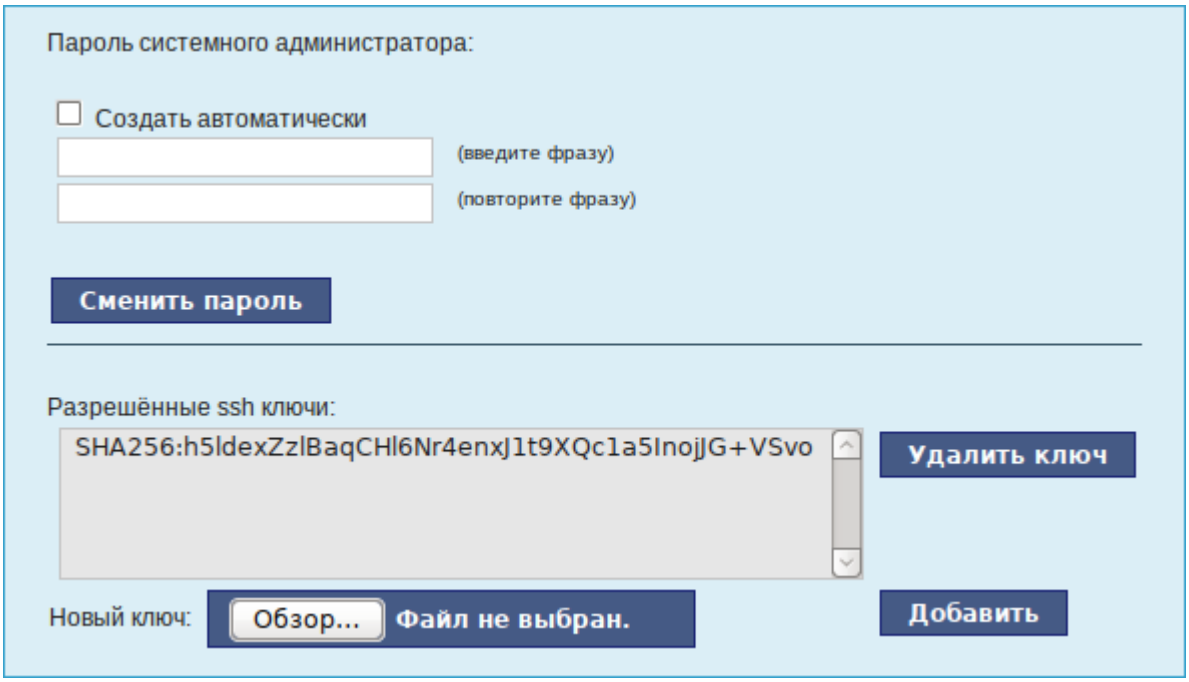


Рис. 65

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

4.8.9 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 (Рис. 66).

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.

Модуль «Дата и время»

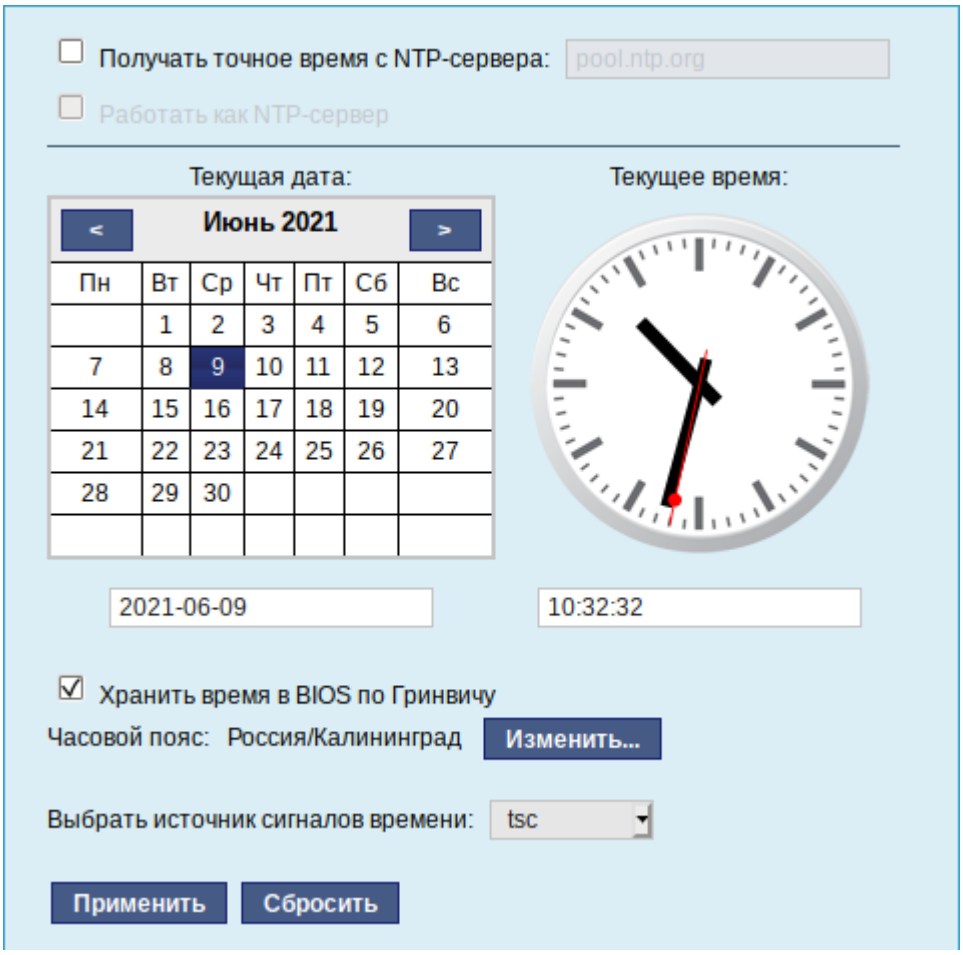


Рис. 66

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».

4.8.10 Ограничение использования диска

Модуль «Использование диска» (пакет alterator-quota) из раздела «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 (Рис. 67).

Модуль «Использование диска»

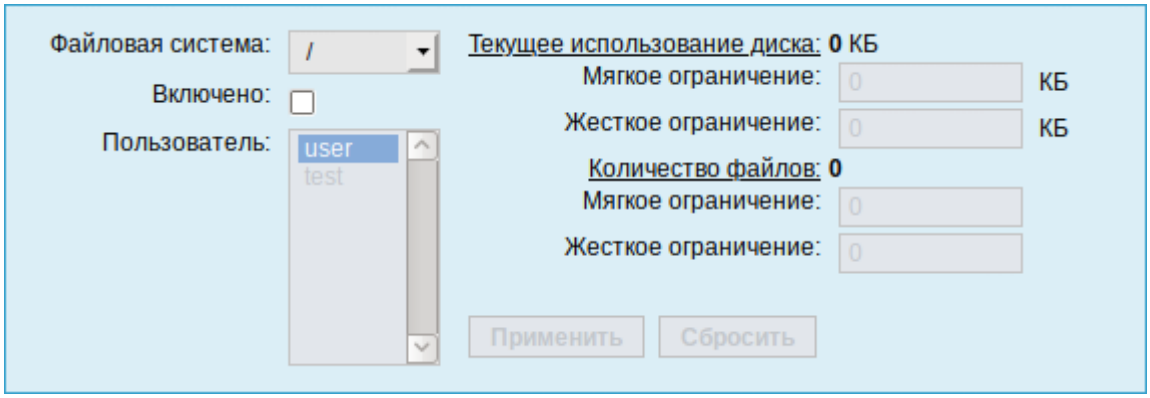


Рис. 67

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» (Рис. 68).

Задание ограничений для пользователя user на раздел /home

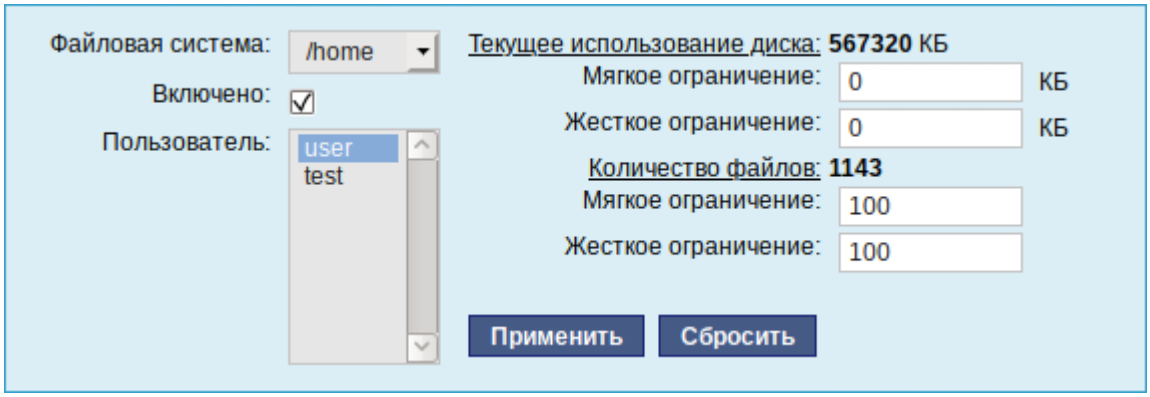


Рис. 68

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.

4.8.11 Выключение и перезагрузка компьютера

Модуль ЦУС «Выключение компьютера» (пакет alterator-ahttpd-power) в разделе «Система» позволяет выполнить:

– 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» (Рис. 69). Для выключения, перезагрузки или перехода в энергосберегающие режимы нужно отметить соответствующий пункт и нажать «Применить».

Модуль «Выключение компьютера»

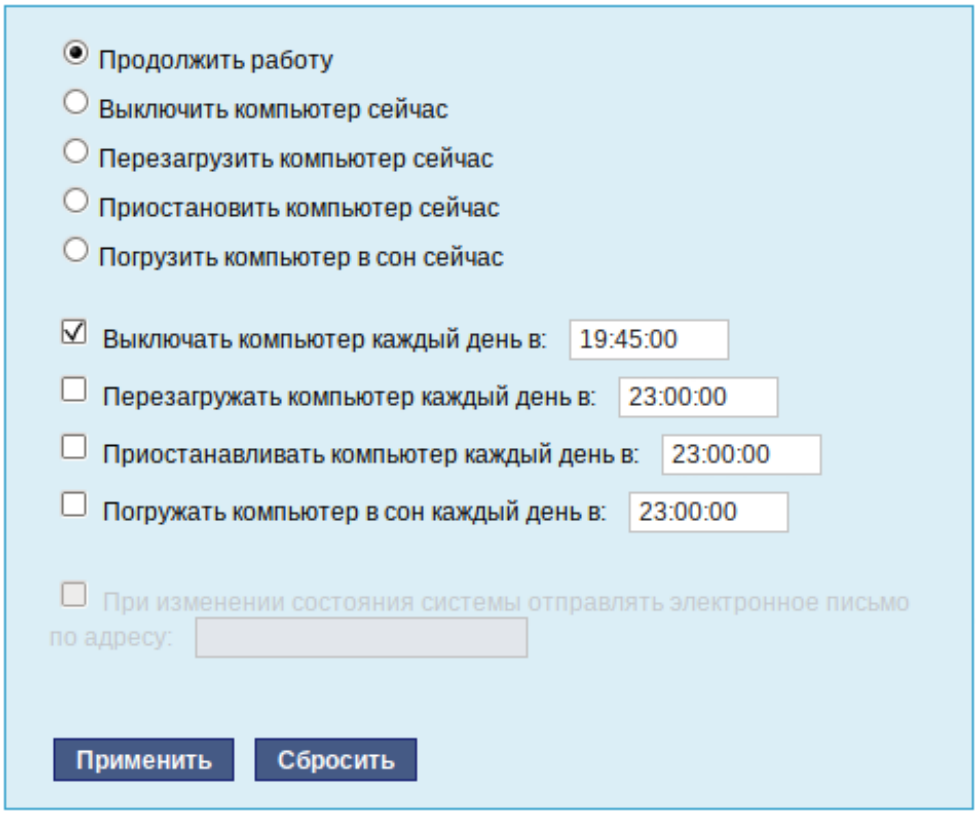


Рис. 69

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» (Рис. 70).

Модуль «Выключение компьютера». Настройка оповещений

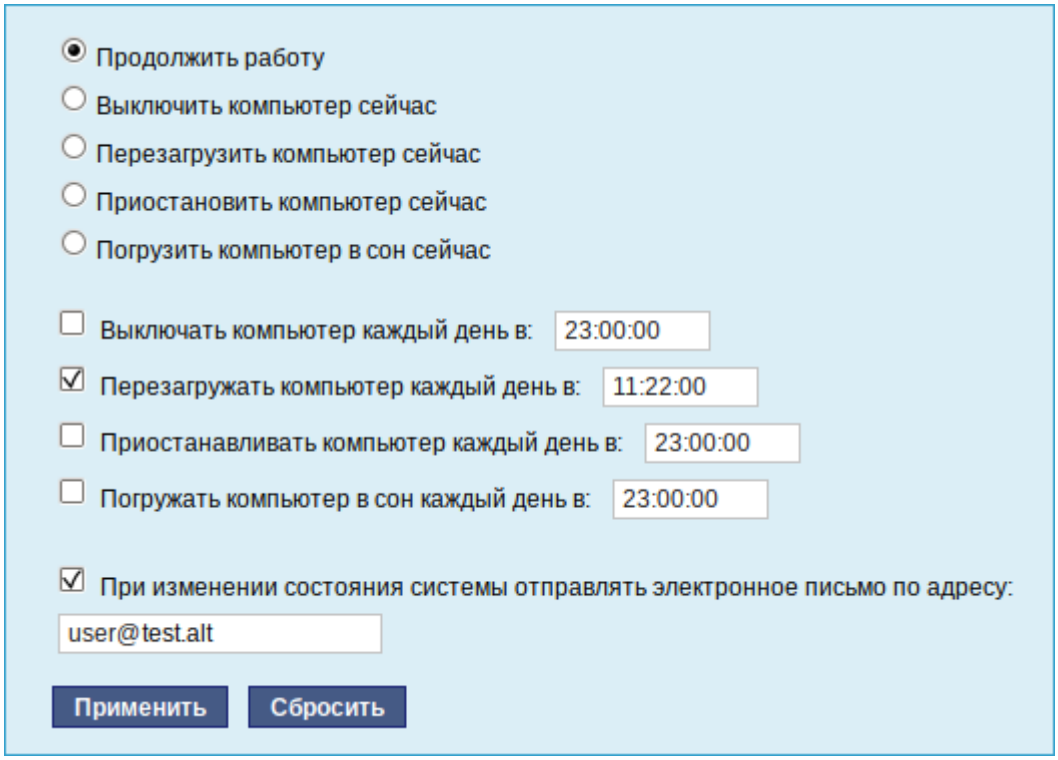


Рис. 70

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.

4.9 Прочие возможности ЦУС

Возможности ЦУС ОС «Альт Сервер» не ограничиваются только теми, что были описаны выше.

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
```

4.10 Права доступа к модулям ЦУС

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 (Рис. 71).

Ссылка «Параметры доступа к модулю»

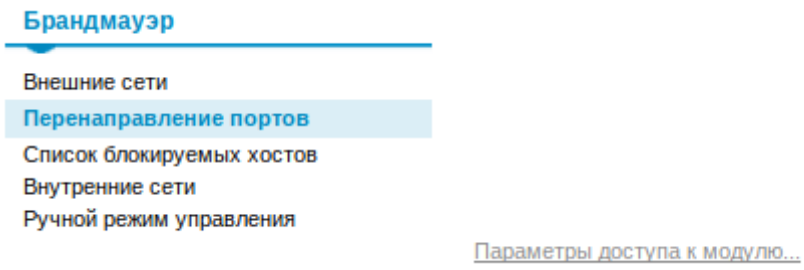


Рис. 71

В открывшемся окне, в списке «Новый пользователь» необходимо выбрать пользователя, который получит доступ к данному модулю, и нажать кнопку «Добавить» (Рис. 72). 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» (Рис. 72) и перезапустить HTTP-сервер.

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

Параметры доступа к модулю

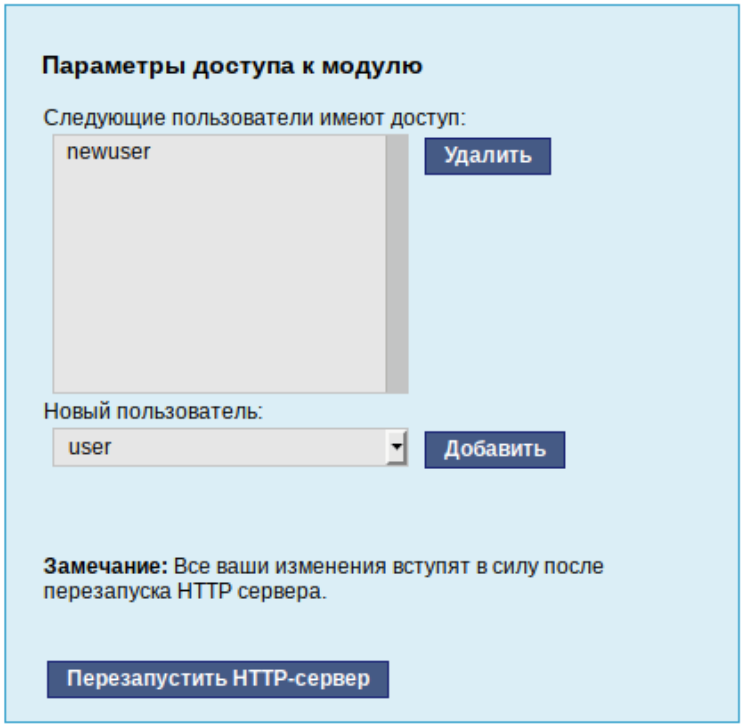


Рис. 72

5 УСТАНОВКА ДОПОЛНИТЕЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

После установки ОС «Альт Сервер», при первом запуске, доступен тот или иной набор программного обеспечения. Количество предустановленных программ зависит от выбора, сделанного при установке системы. Имеется возможность доустановить программы, которых не хватает в системе, 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.

Для установки дополнительного ПО можно использовать ЦУС, либо программу управления пакетами Synaptic.

5.1 Установка дополнительного ПО в ЦУС

ЦУС содержит модуль установки дополнительных пакетов «Установка программ» (раздел «Программное обеспечение»).

Для облегчения поиска доступные для установки программы разделены на группы, выводимые в левой части окна программы (Рис. 73).

Модуль «Установка программ»

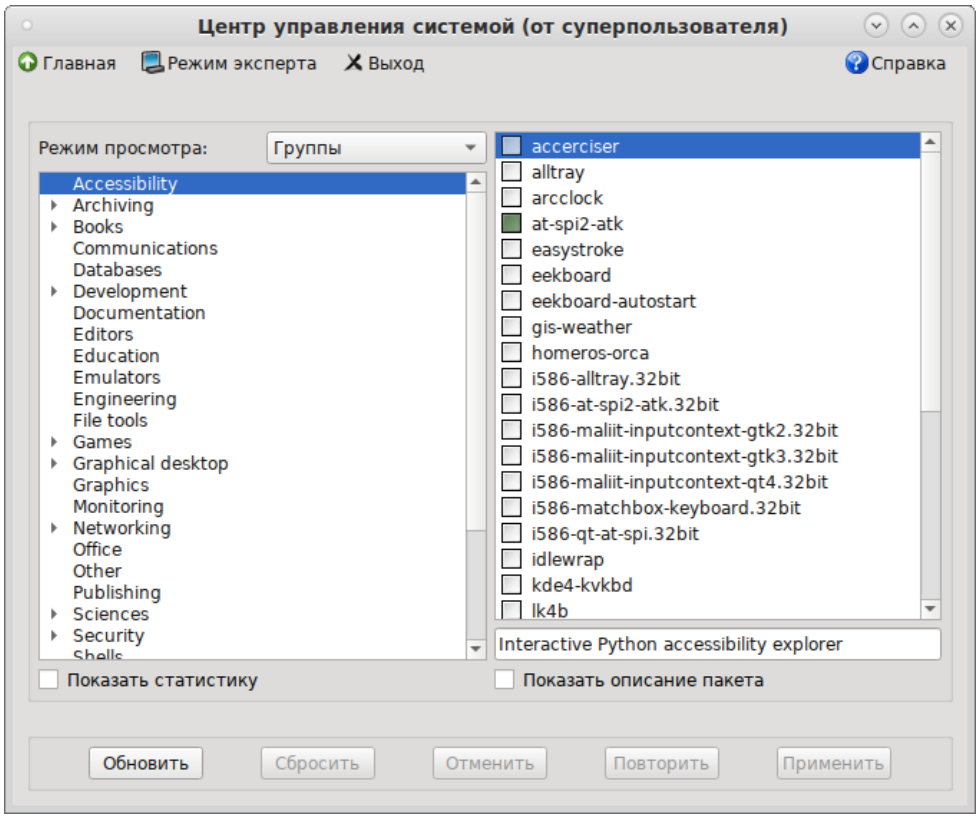


Рис. 73

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 необходимо двойным щелчком мыши отметить неустановленный пакет в правой половине окна и нажать кнопку «Применить». При необходимости менеджер пакетов попросит вставить установочный диск.

5.2 Программа управления пакетами Synaptic

Программа управления пакетами Synaptic находится в меню «Система» → «Параметры» → «Прочие» → «Менеджер пакетов».

Для облегчения поиска доступные для установки программы разделены на группы, выводимые в левой части окна программы (Рис. 74).

Программа управления пакетами Synaptic

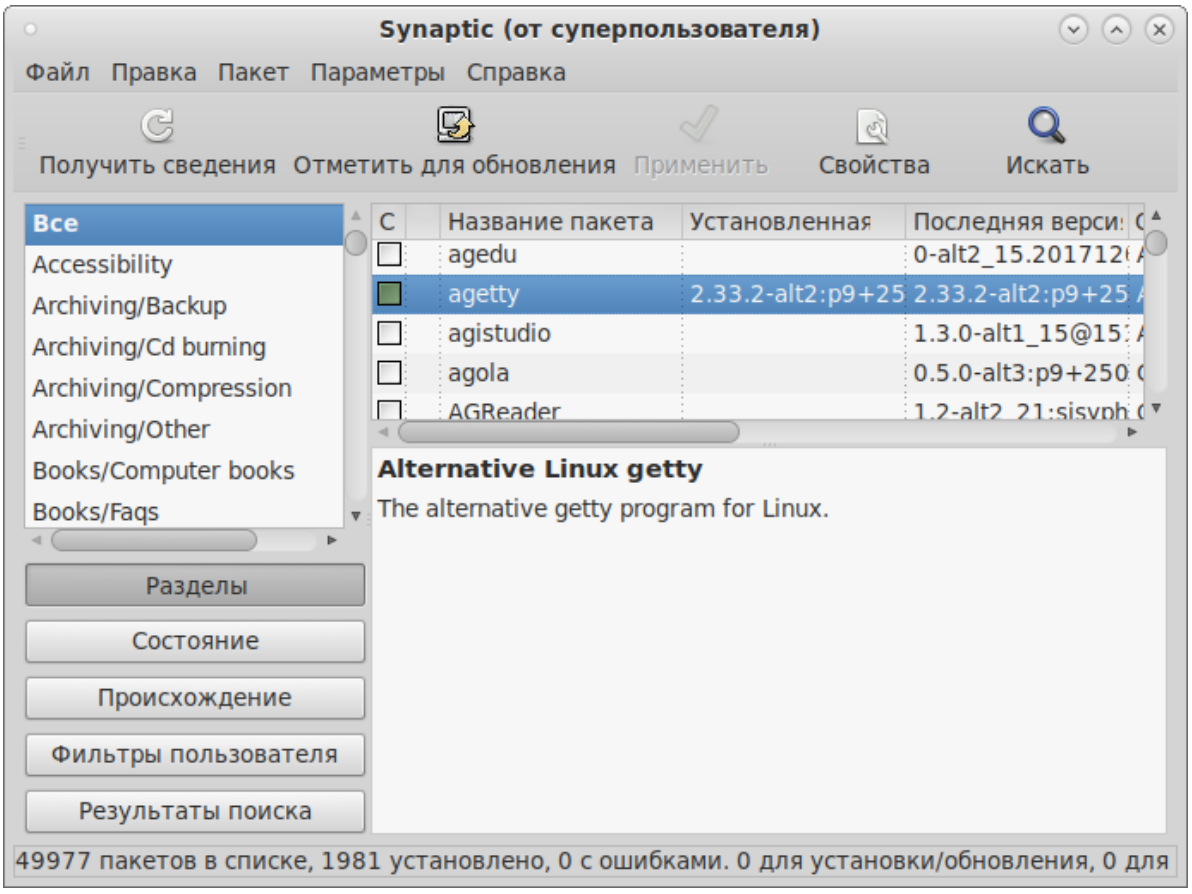


Рис. 74

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 необходимо двойным щелчком мыши отметить неустановленный пакет в правой половине окна и нажать кнопку «Применить». При необходимости менеджер пакетов попросит вставить установочный диск.

5.3 Добавление репозиториев

5.3.1 Добавление репозиториев в ЦУС

Для выбора репозитория, совместимого с дистрибутивом, рекомендуется использовать модуль ЦУС «Источники для установки ПО» (раздел «Программное обеспечение»).

Для указания конкретного репозитория в выпадающем списке необходимо отметить один из предлагаемых вариантов и нажать кнопку «Изменить». К предложенному списку можно добавить любые репозитории, нажав на кнопку «Дополнительно…».

5.3.2 Добавление репозиториев в Synaptic

Программа Synaptic может использоваться для выбора репозитория, совместимого с дистрибутивом. Для указания конкретного репозитория в меню «Параметры» → «Репозитории» необходимо отметить один из предлагаемых вариантов и нажать кнопку «OK» (Рис. 75). К предложенному списку можно добавить любые репозитории, нажав на кнопку «Создать» и введя необходимые данные.

Добавление репозиториев в Synaptic

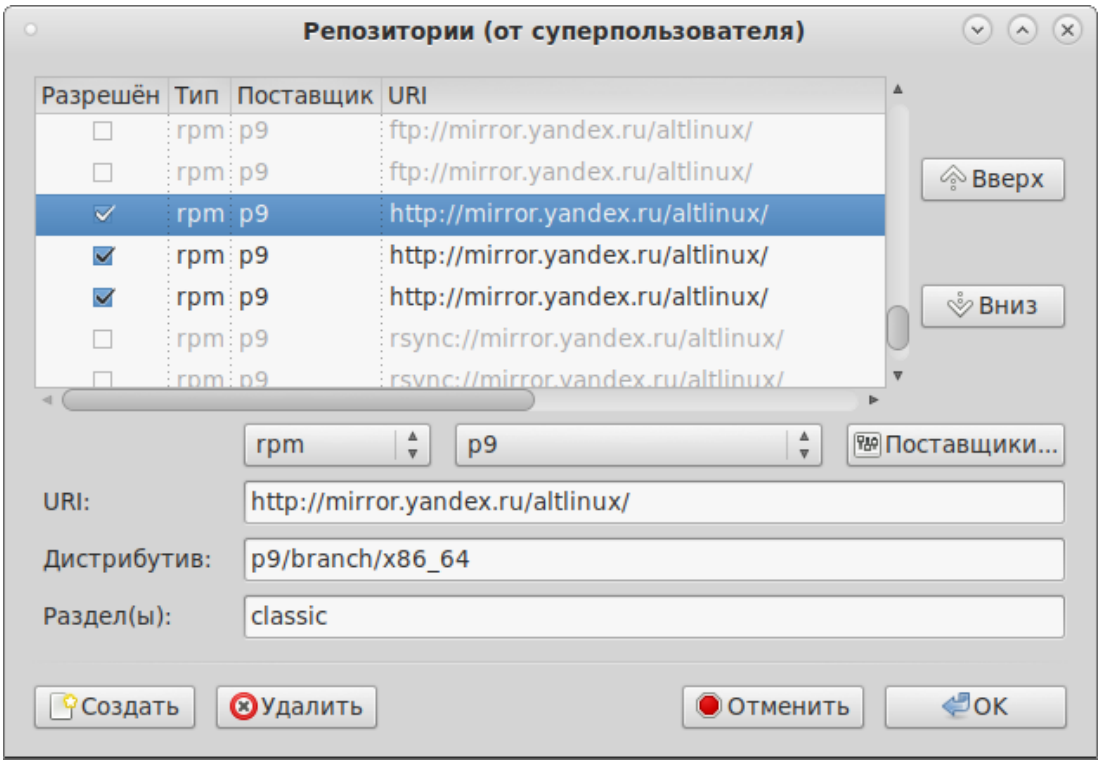


Рис. 75

После выбора и добавления репозиториев необходимо получить сведения о находящихся в них пакетах (кнопка «Получить сведения» см. Рис. 74). В противном случае, список доступных для установки программ будет не актуален.

5.4 Обновление всех установленных пакетов в Synaptic

Synaptic предоставляет два варианта обновления системы:

- умное обновление (рекомендуется) – попытается разрешить конфликты пакетов перед обновлением системы. Действие умного обновления аналогично действию команды `apt-get dist-upgrade`;
- стандартное обновление – обновление обновит только те пакеты, которые не требуют установки дополнительных зависимостей.

По умолчанию Synaptic использует умное обновление. Для того чтобы изменить метод обновления системы необходимо открыть диалоговое окно «Параметры» («Параметры» → «Параметры») и на вкладке «Основные» в списке «Обновить систему» выбрать 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».

5.5 Установка/обновление программного обеспечения в консоли

Для установки, удаления и обновления программ и поддержания целостности системы в ОС семейства Linux используются менеджеры пакетов типа «rpm». Для автоматизации этого процесса и применяется Усовершенствованная система управления программными пакетами APT (Advanced Packaging Tool).

Автоматизация достигается созданием одного или нескольких внешних репозиториев, в которых хранятся пакеты программ и относительно которых производится сверка пакетов, установленных в системе. Репозитории могут содержать как официальную версию дистрибутива, обновляемую его разработчиками по мере выхода новых версий программ, так и локальные наработки, например, пакеты, разработанные внутри компании.

Таким образом, 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, руководствуется сведениями о внешнем репозитории для разрешения конфликтов и поиска корректного пути их устранения.

Система APT состоит из нескольких утилит. Чаще всего используется утилита управления пакетами apt-get, которая автоматически определяет зависимости между пакетами и строго следит за их соблюдением при выполнении любой из следующих операций: установка, удаление или обновление пакетов.

5.5.1 Источники программ (репозитории)

Репозитории, с которыми работает APT, отличаются от обычного набора пакетов наличием мета информации – индексов пакетов, содержащихся в репозитории, и сведений о них. Поэтому, чтобы получить всю информацию о репозитории, APT достаточно получить его индексы.

APT может работать с 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, а расположение в том или ином репозитории не имеет значения. Если потребуется, APT в рамках одной операции установки группы пакетов может пользоваться несколькими репозиториями.

Подключая одновременно несколько репозиториев, нужно следить за тем, чтобы они были совместимы друг с другом по пакетной базе – отражали один определенный этап разработки. Совместимыми являются основной репозиторий дистрибутива и репозиторий обновлений по безопасности к данному дистрибутиву. В то же время смешение среди источников APT репозиториев, относящихся к разным дистрибутивам, или смешение стабильного репозитория с нестабильной веткой разработки (Sisyphus) чревато различными неожиданными трудностями при обновлении пакетов.

APT позволяет взаимодействовать с репозиторием с помощью различных протоколов доступа. Наиболее популярные – HTTP и FTP, однако существуют и некоторые дополнительные методы.

Для того чтобы APT мог использовать тот или иной репозиторий, информацию о нем 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
```

где:

- 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, cdrom, copy;
- путь – путь к репозиторию в терминах выбранного метода;
- база – относительный путь к базе данных репозитория;
- название – название репозитория.

При выборе пакетов для установки APT руководствуется всеми доступными репозиториями вне зависимости от способа доступа к ним. Таким образом, если в репозитории, доступном по сети Интернет, обнаружена более новая версия программы, чем на CD (DVD)-носителе информации, APT начнет загружать данный пакет по сети.

5.5.1.1 Добавление репозиториев

Непосредственно после установки дистрибутива «Альт Сервер» в `/etc/apt/sources.list`, а также в файлах `/etc/apt/sources.list.d/*.list` обычно указывается несколько репозиториев:

- репозиторий с установочного диска дистрибутива;
- интернет-репозиторий, совместимый с установленным дистрибутивом.

5.5.1.1.1 Скрипт apt-repo для работы с репозиториями

Для добавления репозиториев можно воспользоваться скриптом `apt-repo`.

Примечание. Для выполнения большинства команд необходимы права администратора.

Просмотреть список активных репозиториев можно, выполнив команду:

```
$ apt-repo list
```

Команда добавления репозитория в список активных репозиториев:

```
apt-repo add <репозиторий>
```

Команда удаления или выключения репозитория:

```
apt-repo rm <репозиторий>
```

Команда удаления всех репозиториев:

```
apt-repo clean
```

Обновление информации о репозиториях:

```
apt-repo update
```

Вывод справки:

```
man apt-repo
```

или

```
apt-repo –help
```

Типичный пример использования: удалить все источники и добавить стандартный репози-

торий P9 (архитектура выбирается автоматически):

```
# apt-repo rm all
# apt-repo add p9
```

5.5.1.1.2 Добавление репозитория на CD/DVD-носителе

Для добавления в `sources.list` репозитория на CD/DVD-носителе информации в APT предусмотрена специальная утилита – `apt-cdrom`. Чтобы добавить запись о репозитории на носителе, достаточно вставить его в привод для чтения (записи) CD (DVD)-носителей информации и выполнить следующую команду:

```
# apt-cdrom add
```

После этого в `sources.list` появится запись о подключенном диске примерно такого вида:

```
rpm cdrom:[ALT Server 9.2 x86_64 build 2021-06-22]/ ALTLinux main
```

Примечание. В случае если записи для cdrom в файле `/etc/fstab` нет, потребуется примонтировать носитель информации вручную (каталог `/media/ALTLinux` должен существовать):

```
# mount /dev/cdrom /media/ALTLinux
```

Затем использовать команду добавления носителя с дополнительным ключом:

```
# apt-cdrom add -m
```

5.5.1.1.3 Добавление репозиториев вручную

Для редактирования списка репозиториев можно отредактировать в любом текстовом редакторе файлы из папки `/etc/apt/sources.list.d/`. Для изменения этих файлов необходимы права администратора. В файле `alt.list` может содержаться такая информация:

```
rpm [alt] http://ftp.altlinux.org/pub/distributions/ALTLinux p9/x86_64
classic
rpm [alt] http://ftp.altlinux.org/pub/distributions/ALTLinux
p9/x86_64-i586 classic
rpm [alt] http://ftp.altlinux.org/pub/distributions/ALTLinux p9/noarch
classic
```

По сути, каждая строчка соответствует некому репозиторию. Для выключения репозитория достаточно закомментировать соответствующую строку (дописать символ решётки перед строкой). Для добавления нового репозитория необходимо дописать его вниз этого или любого другого файла.

5.5.1.2 Обновление информации о репозиториях

Практически любое действие с системой apt начинается с обновления данных от активиро-

ванных источников. Список источников необходимо обновлять при поиске новой версии пакета, установке пакетов или обновлении установленных пакетов новыми версиями.

Обновление данных осуществляется командой:

```
# apt-get update
```

После выполнения этой команды, apt обновит свой кэш новой информацией.

5.5.2 Поиск пакетов

Утилита `apt-cache` предназначена для поиска программных пакетов, в репозитории, и позволяет искать не только по имени пакета, но и по его описанию.

Команда `apt-cache search <подстрока>` позволяет найти все пакеты, в именах или описании которых присутствует указанная подстрока. Пример поиска может выглядеть следующим образом:

```
$ apt-cache search ^gimp
gimp - The GNU Image Manipulation Program
libgimp - GIMP libraries
gimp-help-en - English help files for the GIMP
gimp-help-ru - Russian help files for the GIMP
gimp-script-ISONoiseReduction - Gimp script for reducing sensor noise
at high ISO values
gimp-plugin-gutenprint - GIMP plug-in for gutenprint [...]
```

Символ «^» в поисковом выражении, указывает на то, что необходимо найти совпадения только в начале строки (в данном случае – в начале имени пакета).

Для того чтобы подробнее узнать о каждом из найденных пакетов и прочитать его описание, можно воспользоваться командой `apt-cache show`, которая покажет информацию о пакете из репозитория:

```
$ apt-cache show gimp-help-ru
Package: gimp-help-ru
Section: Graphics
Installed Size: 37095561
Maintainer: Alexey Tourbin <at@altlinux.ru>
Version: 2.6.1-alt2
Pre-Depends: rpmlib(PayloadIsLzma)
Provides: gimp-help-ru (= 2.6.1-alt2)
Obsoletes: gimp-help-common (< 2.6.1-alt2)
Architecture: noarch
Size: 28561160
```

```
MD5Sum: 0802d8f5ec1f78af6a4a19005af4e37d
Filename: gimp-help-ru-2.6.1-alt2.noarch.rpm
Description: Russian help files for the GIMP
Russian help files for the GIMP.
```

При поиске с помощью `apt-cache` можно использовать русскую подстроку. В этом случае будут найдены пакеты, имеющие описание на русском языке.

5.5.3 Установка или обновление пакета

Установка пакета с помощью APT выполняется командой:

```
# apt-get install <имя_пакета>
```

Примечание. Перед установкой и обновлением пакетов необходимо выполнить команду обновления индексов пакетов:

```
# apt-get update
```

Если пакет уже установлен и в подключенном репозитории нет обновлений для данного пакета, система сообщит об уже установленном пакете последней версии. Если в репозитории присутствует более новая версия или новое обновление – программа начнет процесс установки.

`apt-get` позволяет устанавливать в систему пакеты, требующие для работы другие, пока еще не установленные. В этом случае он определяет, какие пакеты необходимо установить, и устанавливает их, пользуясь всеми доступными репозиториями.

Установка пакета gimp командой `apt-get install gimp` приведет к следующему диалогу с APT:

```
# apt-get install gimp
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие дополнительные пакеты будут установлены:
icc-profiles libbabl libgegl libgimp libjavascriptcoregtk2 libopenraw
libspiro libwebkitgtk2 libwmf
Следующие НОВЫЕ пакеты будут установлены:
gimp icc-profiles libbabl libgegl libgimp libjavascriptcoregtk2
libopenraw libspiro libweb-kitgtk2 libwmf
0 будет обновлено, 10 новых установлено, 0 пакетов будет удалено и 0
не будет обновлено.
Необходимо получить 0B/24,6MB архивов.
После распаковки потребуется дополнительно 105MB дискового
пространства.
Продолжить? [Y/n] y
```

```
. . .
Получено 24,6MB за 0s (44,1MB/s).
Совершаем изменения...
Preparing...              ######################## [100%]
1: libbabl                ######################## [ 10%]
2: libwmf                 ######################## [ 20%]
3: libjavascriptcoregtk2  ######################## [ 30%]
4: libwebkitgtk2          ######################## [ 40%]
5: icc-profiles           ######################## [ 50%]
6: libspiro               ######################## [ 60%]
7: libopenraw             ######################## [ 70%]
8: libgegl                ######################## [ 80%]
9: libgimp                ######################## [ 90%]
10: gimp                  ######################## [100%]
Running /usr/lib/rpm/posttrans-filetriggers
Завершено.
```

Команда `apt-get install <имя_пакета>` используется и для обновления уже установленного пакета или группы пакетов. В этом случае `apt-get` дополнительно проверяет, не обновилась ли версия пакета в репозитории по сравнению с установленным в системе.

При помощи APT можно установить и отдельный бинарный rpm-пакет, не входящий ни в один из репозиториев. Для этого достаточно выполнить команду `apt-get install путь_к_файлу.rpm`. При этом APT проведет стандартную процедуру проверки зависимостей и конфликтов с уже установленными пакетами.

В результате операций с пакетами без использования APT может нарушиться целостность ОС «Альт Сервер», и `apt-get` в таком случае откажется выполнять операции установки, удаления или обновления.

Для восстановления целостности ОС «Альт Сервер» необходимо повторить операцию, задав опцию `-f`, заставляющую `apt-get` исправить нарушенные зависимости, удалить или заменить конфликтующие пакеты. Любые действия в этом режиме обязательно требуют подтверждения со стороны пользователя.

При установке пакетов происходит запись в системный журнал вида:

```
apt-get: имя-пакета installed
```

5.5.4 Удаление установленного пакета

Для удаления пакета используется команда `apt-get remove <имя_пакета>`. Удале-

ние пакета с сохранением его файлов настройки производится при помощи следующей команды:

```
# apt-get remove <значимая_часть_имени_пакета>
```

В случае если при этом необходимо полностью очистить систему от всех компонент удаляемого пакета, то применяется команда:

```
# apt-get remove --purge <значимая_часть_имени_пакета>
```

Для того чтобы не нарушать целостность системы, будут удалены и все пакеты, зависящие от удаляемого.

В случае удаления с помощью `apt-get` базового компонента системы появится запрос на подтверждение операции:

```
# apt-get remove filesystem
Обработка файловых зависимостей... Завершено
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие пакеты будут УДАЛЕНЫ:
basesystem filesystem ppp sudo
Внимание: следующие базовые пакеты будут удалены:
В обычных условиях этого не должно было произойти, надеемся, вы точно
представляете, чего требуете!
basesystem filesystem (по причине basesystem)
0 пакетов будет обновлено, 0 будет добавлено новых, 4 будет
удалено(заменено) и 0 не будет обновлено.
Необходимо получить 0B архивов. После распаковки 588kБ будет
освобождено.
Вы делаете нечто потенциально опасное!
Введите фразу 'Yes, do as I say!' чтобы продолжить.
```

Каждую ситуацию, в которой APT выдает такое сообщение, необходимо рассматривать отдельно. Однако, вероятность того, что после выполнения этой команды система окажется неработоспособной, очень велика.

При удалении пакетов происходит запись в системный журнал вида:

```
apt-get: имя-пакета removed
```

5.5.5 Обновление всех установленных пакетов

Полное обновление всех установленных в системе пакетов производится при помощи команд:

```
# 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.

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 отчете apt-get, которым APT предварит само обновление.

Примечание. Команда `apt-get dist-upgrade` обновит систему, но ядро ОС не будет обновлено.

5.5.6 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.

5.6 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>
```

Примечание. 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
```

6 КОРПОРАТИВНАЯ ИНФРАСТРУКТУРА

6.1 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).

6.1.1 Установка

Для установки Samba AD DC выполняются следующие шаги:

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

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

2. 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
```

6.1.2 Создание нового домена

6.1.2.1 Восстановление к начальному состоянию Samba

Если домен уже создавался, необходимо очистить базы и конфигурацию Samba, выполнив команды:

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

Предупреждение. Необходимо удалить файл `/etc/samba/smb.conf` перед созданием домена.

6.1.2.2 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. Для этого в файл `/etc/sysconfig/network` необходимо добавить строку:

```
HOSTNAME=dc.test.alt
```

И выполнить команды:

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

6.1.2.3 Создание домена одной командой

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 (Рис. 76).
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» (Рис. 77).

   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.

   После успешного создания домена, будет выведена информация о домене (Рис. 78).
3. Перегрузить сервер.

Ethernet-интерфейсы

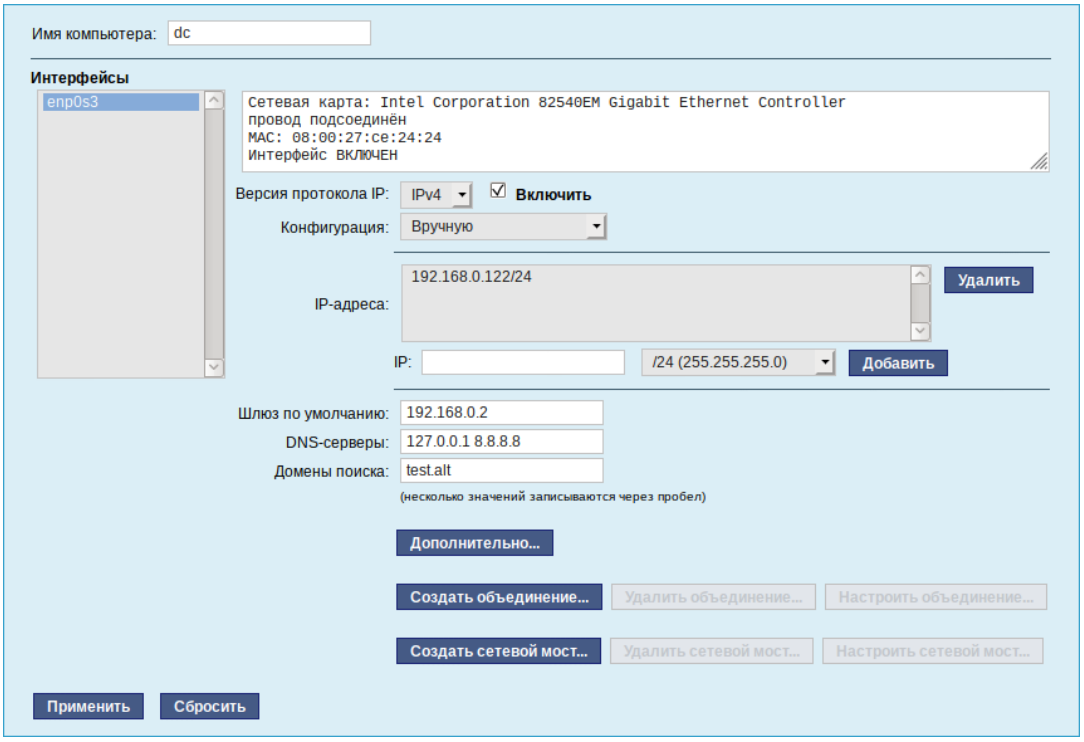


Рис. 76

Создание домена в ЦУС

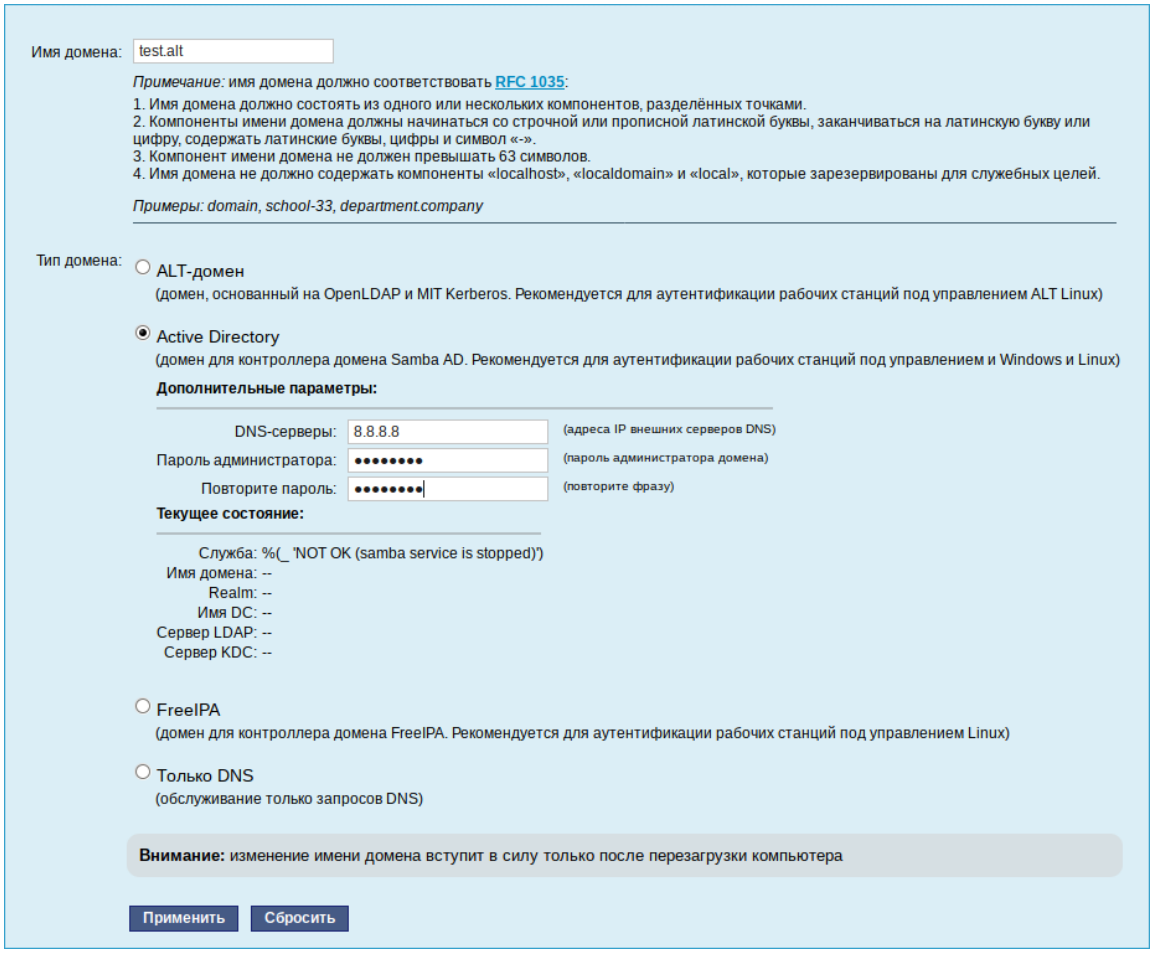


Рис. 77

Информация о созданном домене

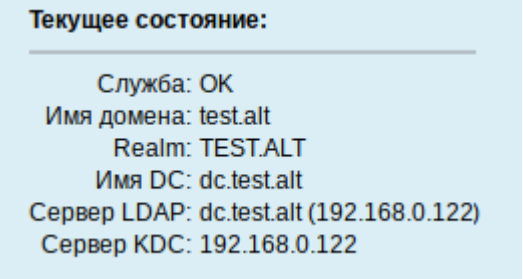


Рис. 78

6.1.2.4 Создание домена одной командой

Создание контроллера домена test.alt с паролем администратора Pa$$word:

```
# samba-tool domain provision --realm=test.alt --domain test --
adminpass='Pa$$word' --dns-backend=SAMBA_INTERNAL --server-role=dc --
use-rfc2307
```

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.

6.1.2.5 Интерактивное создание домена

Для интерактивного развертывания необходимо выполнить команду `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) [SAM-
BA_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 необходимо нажимать <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.

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

6.1.3 Запуск службы

Для установки службы по умолчанию и ее запуска, необходимо выполнить команды:

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

6.1.4 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 4.14.4)
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:

– необходимо убедиться 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
```

– проверить 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, необходимо проверить 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
```

6.1.5 Управление пользователями

Для создания пользователя с паролем используются команды:

```
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. Нельзя допускать 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>
```

6.1.6 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). Необходимые действия:

1. На Primary Domain Controller (PDC) выключить службу bind и, если она была включена, перезапустить службу samba:

```
# service bind stop
# service samba restart
```

2. Завести адрес IP для dc2 (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 внести изменения в 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 необходимо запросить билет Kerberos для администратора домена (имя домена должно быть указано в верхнем регистре):

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

5. Убедиться, что билет получен, выполнив команду:

```
# 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
```

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 подключение к DC производилось под управлением Windows, необходимо запустить службу samba:

```
# service samba start
```

6.1.7 Репликация

Предупреждение. Без успешной двунаправленной репликации в течение 14 дней DC исключается из Active Directory. Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

1. Произвести репликацию 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. Произвести репликацию 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.

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

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

Примечание. Если репликация на Windows не работает, необходимо добавить в Active Directory Sites and Services новое соединение Active Directory, реплицировать на DC, подождать минут 5 и попробовать реплицировать с Samba на Windows.

6.1.8 Подключение к домену на рабочей станции

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.

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

- в ЦУС в разделе «Сеть» → «Ethernet интерфейсы» задать имя компьютера, указать в поле «DNS-серверы» DNS-сервер домена и в поле «Домены поиска» – домен для поиска (Рис. 79);
- 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 сервер, `test.alt` – домен.
  - обновить DNS адреса:
    ```
    # resolvconf –u
    ```

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

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

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

Настройка на использование DNS-сервера домена

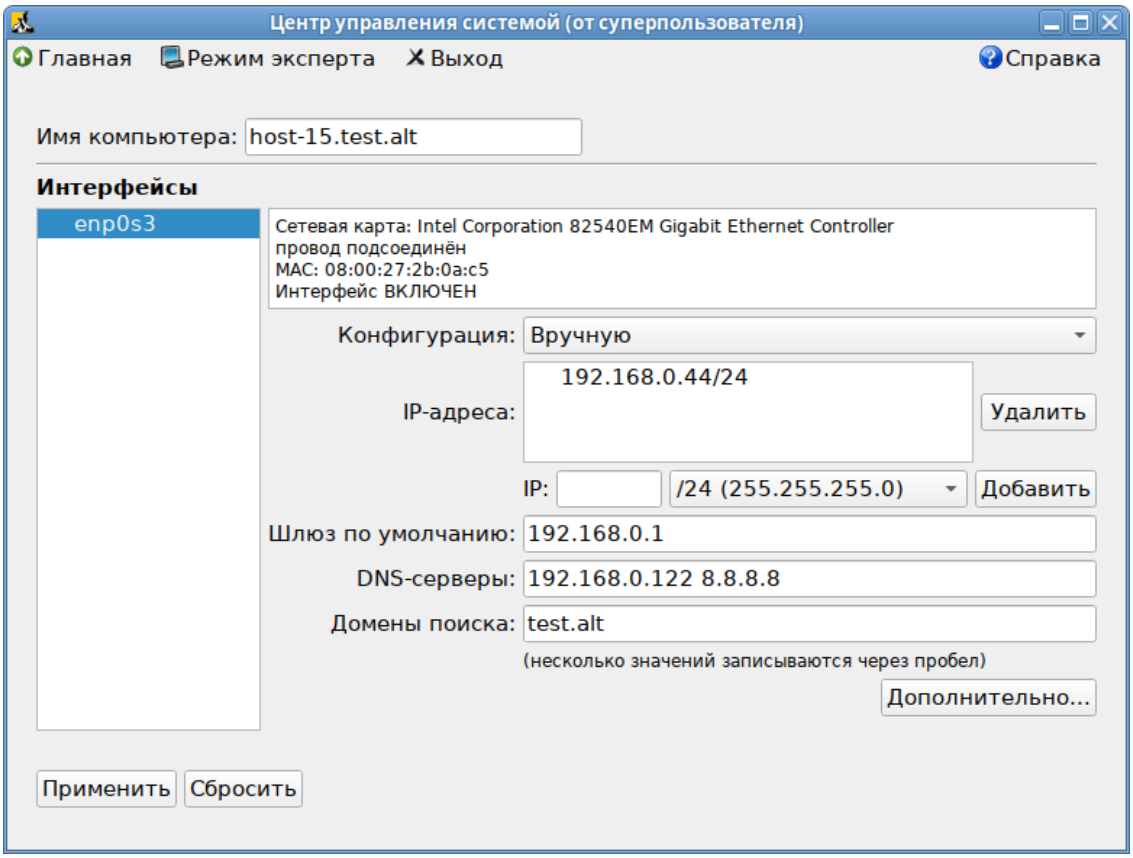


Рис. 79

6.1.8.1 Ввод в домен в ЦУС

Для ввода рабочей станции в домен необходимо запустить ЦУС («Меню MATE» → «Приложения» → «Администрирование» → «Центр управления системой»). В ЦУС следует перейти в раздел «Пользователи» → «Аутентификация».

В открывшемся окне необходимо выбрать пункт «Домен Active Directory» (Рис. 80) и заполнить поля, после чего нажать кнопку «Применить».

В открывшемся окне (Рис. 81) необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку «ОК».

Ввод в домен в «Центре управления системой»

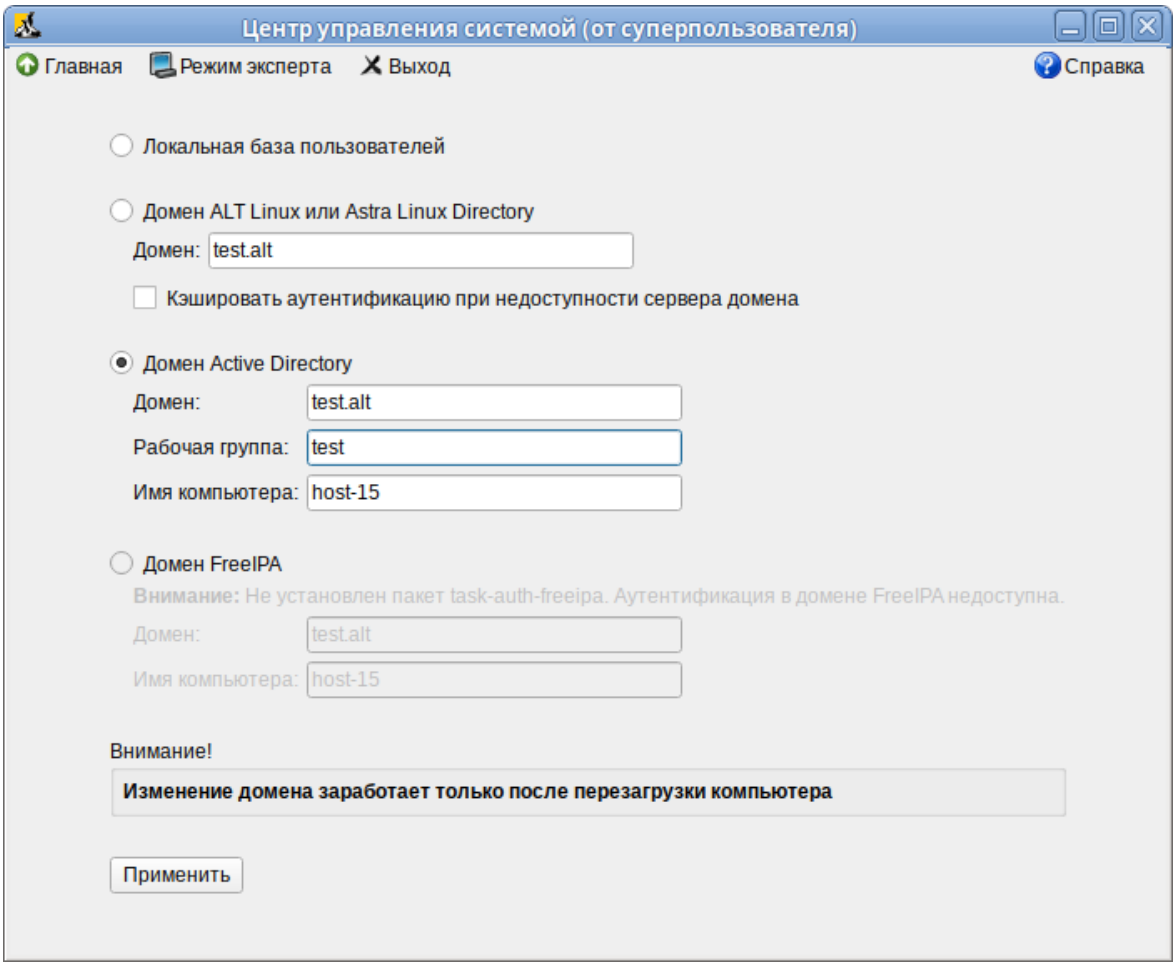


Рис. 80

Параметры учетной записи с правами подключения к домену

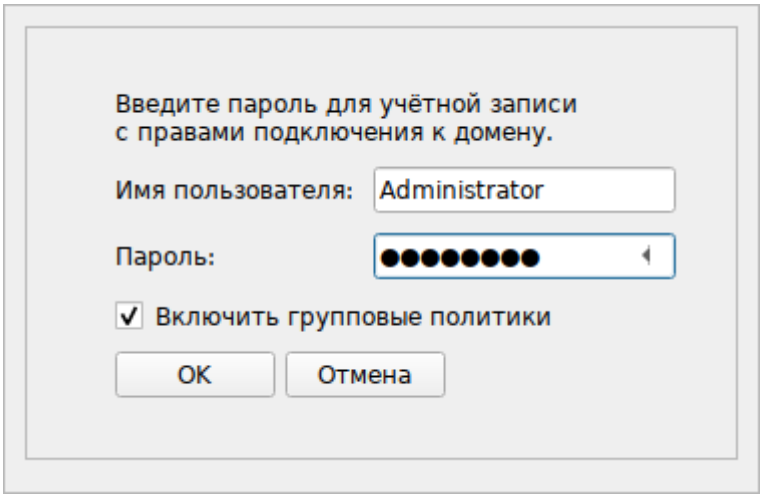


Рис. 81

При успешном подключении к домену, отобразится соответствующая информация (Рис. 82).

Успешное подключение к домену

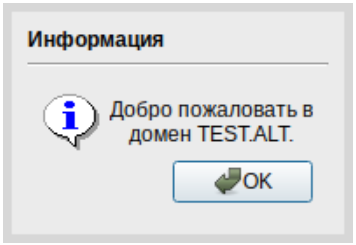


Рис. 82

Перезагрузить рабочую станцию.

6.1.8.2 Ввод в домен в командной строке

Для ввода рабочей станции в домен можно воспользоваться следующей командой:

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

Перезагрузить рабочую станцию.

6.2 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). Можно 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). Можно установить при использовании ADMX файлов ALT;
- включения или выключения различных служб (сервисов systemd) Можно 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, скачав файлы ADMX из репозитория http://git.altlinux.org/gears/a/admx-basealt.git или https://github.com/altlinux/admx-basealt и загрузив их в оснастку RSAT.

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

6.2.1 Развертывание групповых политик

Процесс развёртывание групповых политик:

1. Развернуть сервер Samba AD DC (см. Samba 4 в роли контроллера домена Active Directory).
2. Ввести машину в домен Active Directory по инструкции (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» (Рис. 83).

Пункт «Включить групповые политики»

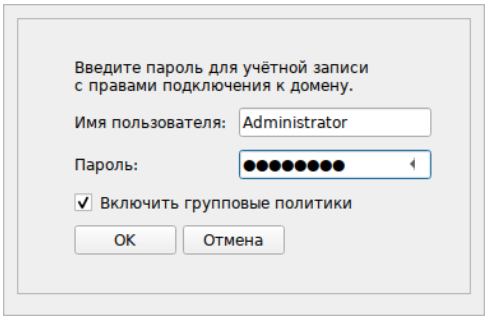


Рис. 83

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 ЦУС в разделе «Система» → «Групповые политики» следует выбрать шаблон локальной политики («Сервер», «Рабочая станция» или «Контроллер домена») и установить отметку в пункте «Управление групповыми политиками» (Рис. 84).

Модуль ЦУС «Групповые политики»

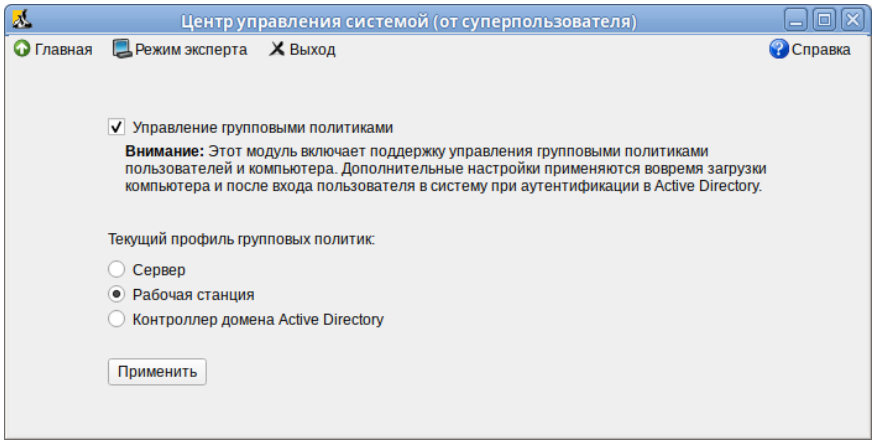


Рис. 84

3. Ввести машину с ОС Windows в домен.

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

Включить компоненты удаленного администрирования. Для задания конфигурации с помощью RSAT необходимо скачать файлы административных шаблонов (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`.

Корректно установленные административные шаблоны будут отображены в оснастке «Редактор управления групповыми политиками» в разделе «Конфигурация компьютера» → «Политики» → «Административные шаблоны» → «Система ALT» (Рис. 85).

Политики настройки систем ALT в консоли gpme.msc

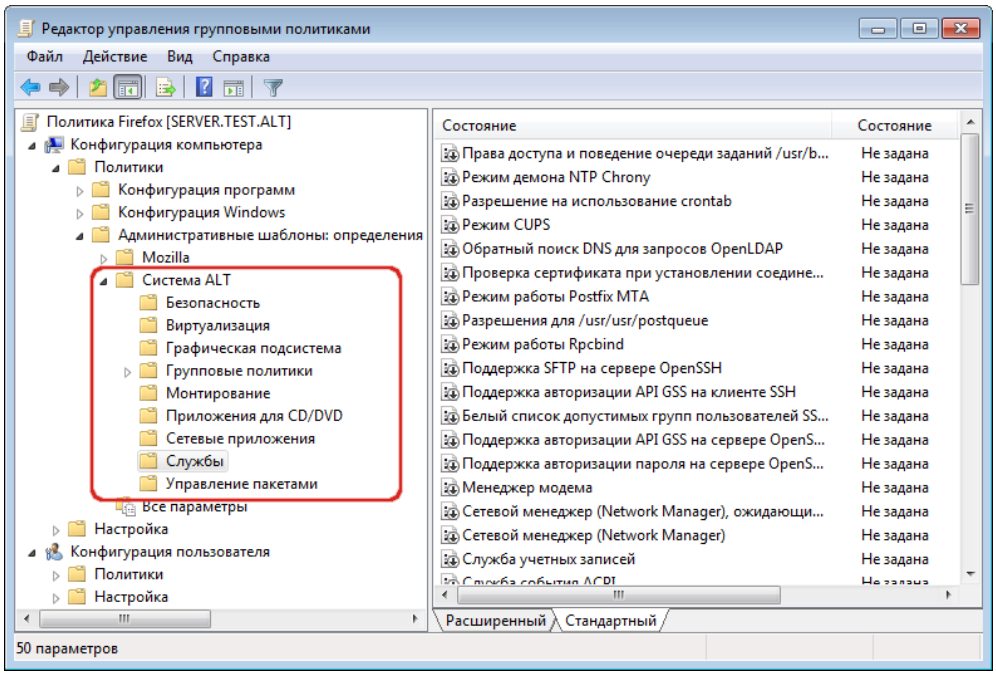


Рис. 85

В оснастке «Active Directory – пользователи и компьютеры» создать подразделение (OU) и переместить в него компьютеры и пользователей домена.

Политики создаются и редактируются на ОС Windows, применяются на рабочих станциях.

6.2.2 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 раздел «Конфигурация компьютера» → «Политики» → «Административные шаблоны» → «Система ALT». Здесь есть несколько подразделов, соответствующих категориям control. Выбрать раздел «Сетевые приложения», в правом окне редактора отобразится список политик (Рис. 86).

Раздел «Сетевые приложения»

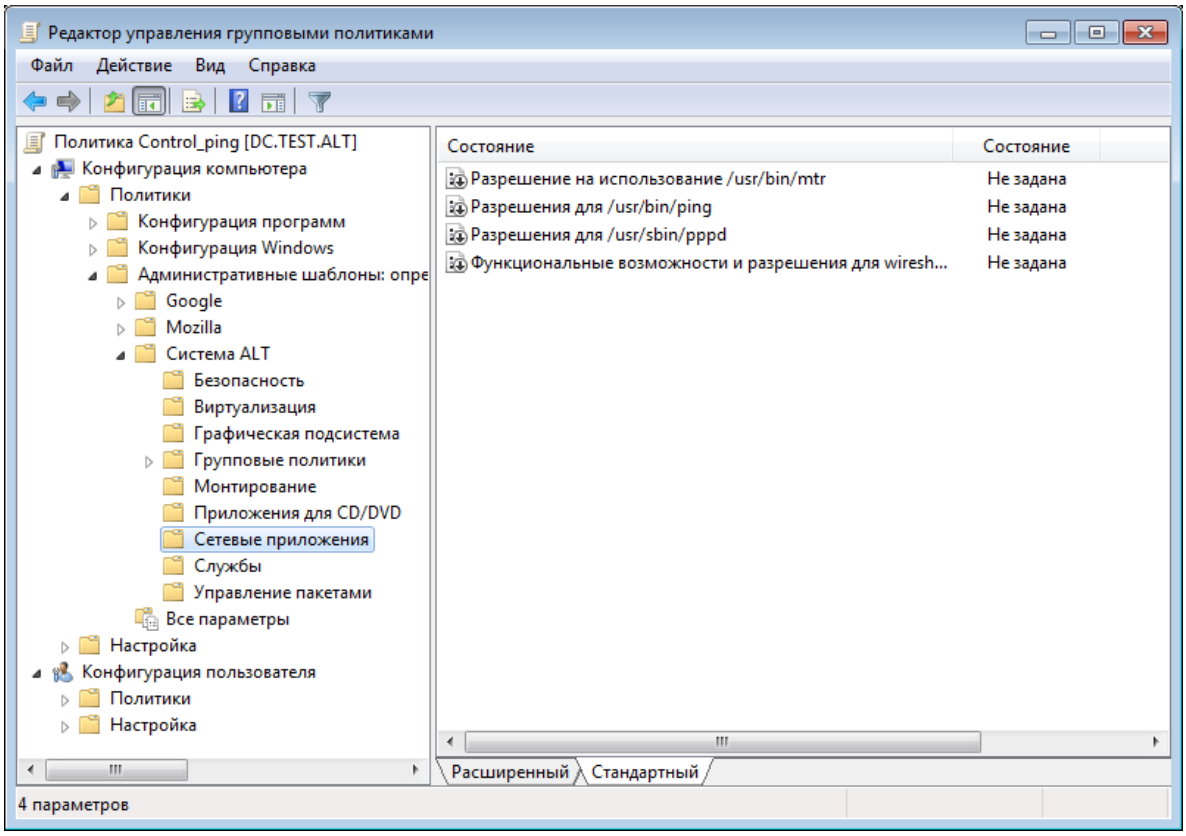


Рис. 86

5. Дважды щелкнуть левой кнопкой мыши на политике «Разрешения для /usr/bin/ping». Откроется диалоговое окно настройки политики (Рис. 87). 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
```

Примечние. 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.

Политика «Разрешения для /usr/bin/ping»

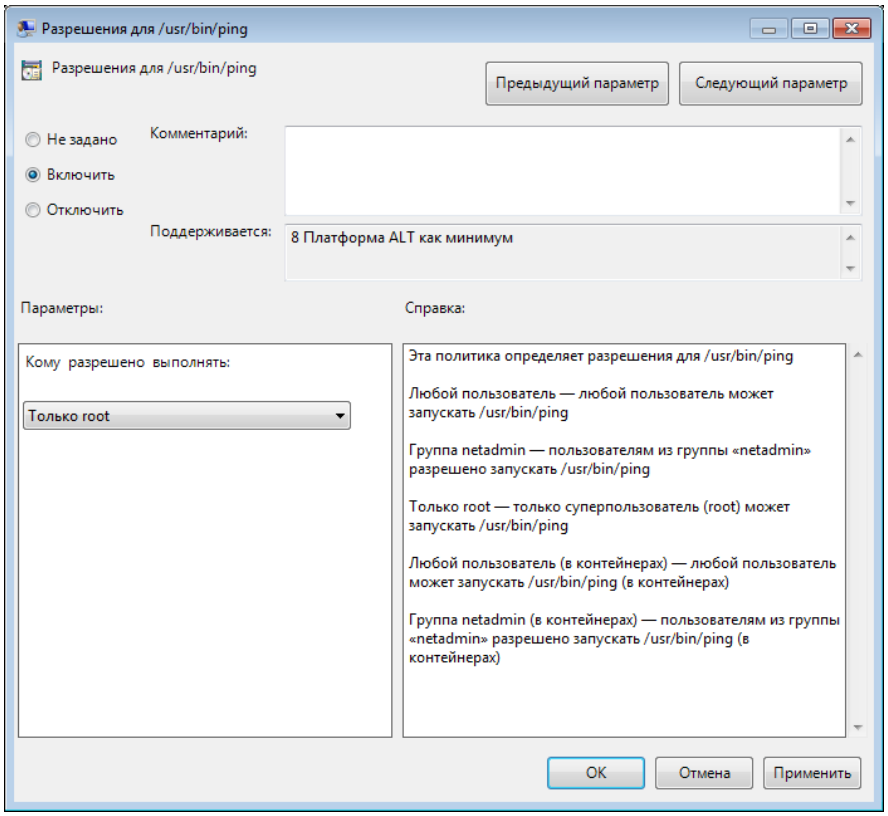


Рис. 87

6.3 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.

6.3.1 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):

```
[global]
    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
```

6.3.2 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 us-
ers,credentials=/etc/samba/sambacreds 0 0
```

Для защиты информации, права на файл `/etc/samba/sambacreds`, необходимо установить так, чтобы файл был доступен только владельцу и принадлежал root:

```
chmod 600 /etc/samba/sambacreds
chown root: /etc/samba/sambacreds
```

6.4 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.

6.4.1 Установка

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

```
# apt-get install task-sogo
```

6.4.2 Подготовка среды

6.4.2.1 Настройка PostgreSQL

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):

```
# postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --no-createrole
sogo'
# postgres -s /bin/sh -c 'createdb -O sogo sogo'
# service postgresql restart
```

6.4.2.2 Настройка Samba DC

Пользователи расположены в домене Active Directory, расположенном на контроллере с Samba DC. Необходимо предварительно создать домен SambaDC.

Создать в домене пользователя sogo с паролем Pa$$word (при запросе дважды ввести пароль):

```
# samba-tool user add sogo
# samba-tool user setexpiry --noexpiry sogo
```

6.4.2.3 Настройка SOGo

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$$word";
        filter = "((NOT isCriticalSystemObject='TRUE') AND (mail='*') AND (NOT ob-
jectClass=contact))";
    },
    {
        id = sambaContacts;
        displayName = "Shared Contacts";
        canAuthenticate = NO;
        isAddressBook = YES;
        type = ldap;
        CNFieldName = cn;
        IDFieldName = mail;
        UIDFieldName = mail;
        hostname = "ldaps://127.0.0.1";
        baseDN = "CN=Users,DC=test,DC=alt";
        bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
        bindPassword = "Pa$$word";
        filter = "((((objectClass=person) AND (objectClass=contact) AND ((uid-
Number>=2000) OR (mail='*')))
                AND (NOT isCriticalSystemObject='TRUE') AND (NOT showInAd-
vancedViewOnly='TRUE') AND (NOT uid=Guest))
                OR (((objectClass=group) AND (gidNumber>=2000)) AND (NOT isCriti-
calSystemObject='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 re-
start;done
```

Возможные ошибки будут записаны в файл журнала `/var/log/sogo/sogo.log`.

6.4.3 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
# a2ensite SOGo
# service httpd2 restart
# service sogo restart
```

Теперь можно войти по адресу https://адрес_сервера/SOGo/ (Рис. 88).

Форма входа в интерфейс SOGo

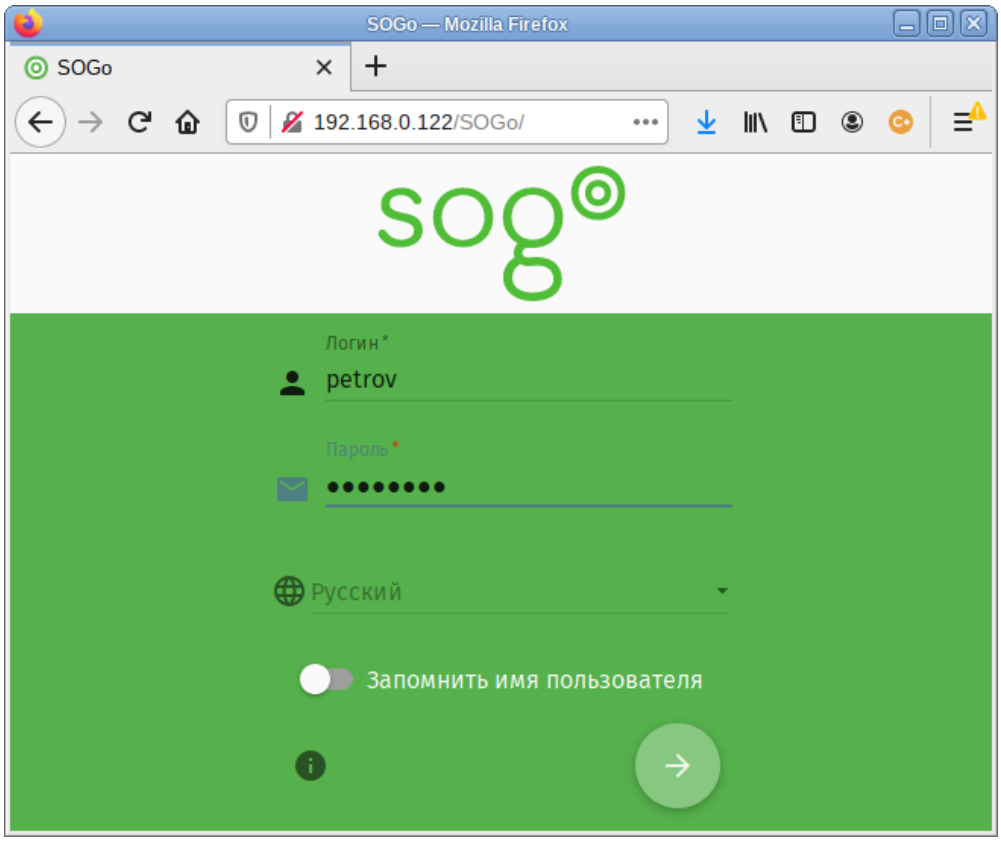


Рис. 88

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
```

6.4.4 Настройка электронной почты

Для использования электронной почты в SOGo (Рис. 89) необходимо настроить аутентификацию в Active Directory для Postfix и Dovecot.

Использование электронной почты в SOGo

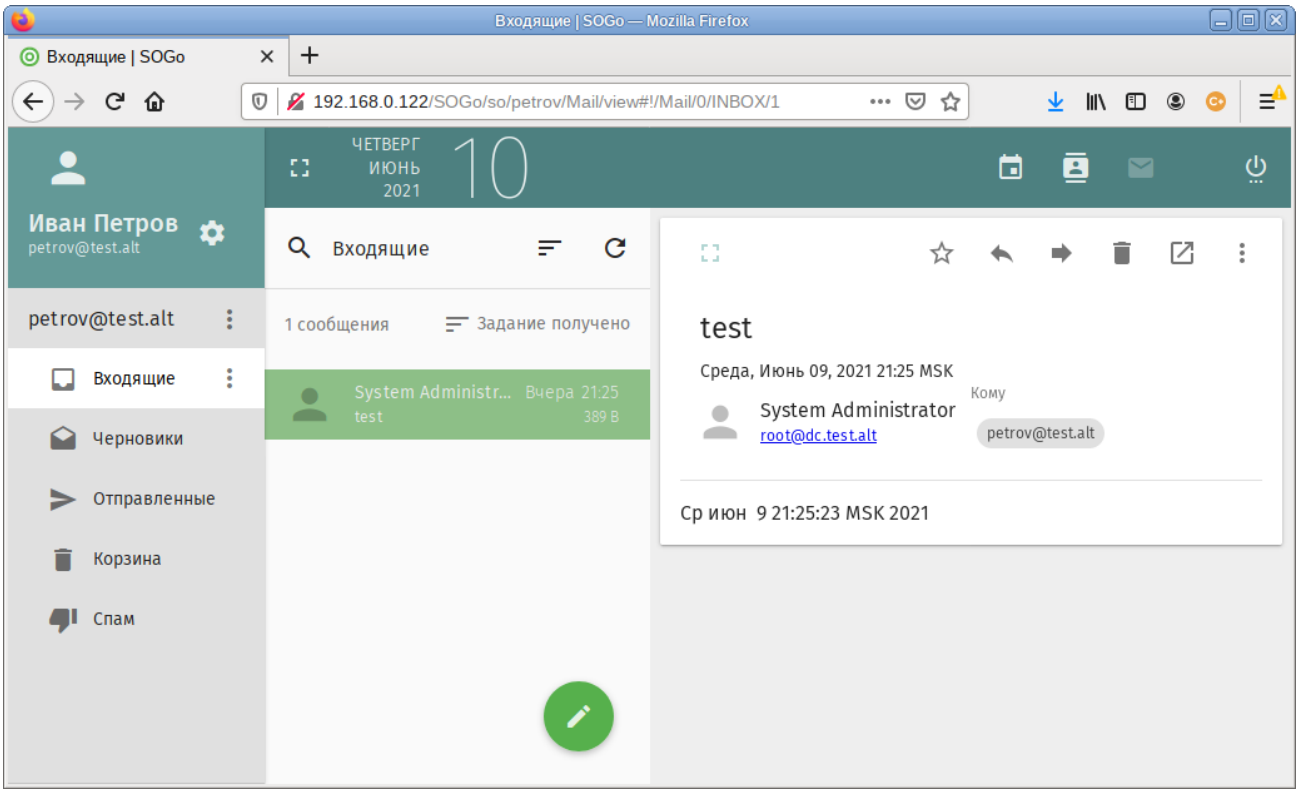


Рис. 89

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.

Примечание. 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
```

6.4.4.1 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
```

6.4.4.2 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
```

6.4.4.3 Безопасность

Так как конфигурационные файлы содержат пароль пользователя LDAP, их необходимо сделать недоступным для чтения прочим пользователям:

```
# 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
```

6.4.4.4 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
```

6.5 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.

6.5.1 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
# service httpd2 condreload
# a2disport https
```

Установить необходимые пакеты:

```
# 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 ex-
ample.test -p 12345678 -a 12345678 --setup-dns --no-forwarders --no-
reverse
```

или интерактивно (необходимо обратить внимание на ответ на вопрос, не совпадающий с предложенными, пароли должны быть не менее 8 символов):

```
# ipa-server-install
Do you want to configure integrated DNS (BIND)? [no]: yes
```

Так же при установке необходимо ввести пароль администратора системы и пароль администратора каталогов.

Примечание. 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 ex-
ample.test -p 12345678 -a 12345678 --setup-dns --no-forwarders --no-
reverse --mkhomedir
```

Для возможности управлять сервером FreeIPA 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.
Record name: _ntp._udp
SRV record: 0 100 123 ipa, 0 100 123 ipa.example.test
```

Проверить работу ntp сервера можно командой:

```
# ntpdate -q localhost
server 127.0.0.1, stratum 16, offset 0.000046, delay 0.02576
27 Nov 10:27:00 ntpdate[29854]: adjust time server 127.0.0.1 offset
0.000018 sec
```

6.5.2 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 (Рис. 90) и ввести данные администратора для входа в систему.

Веб-интерфейс FreeIPA

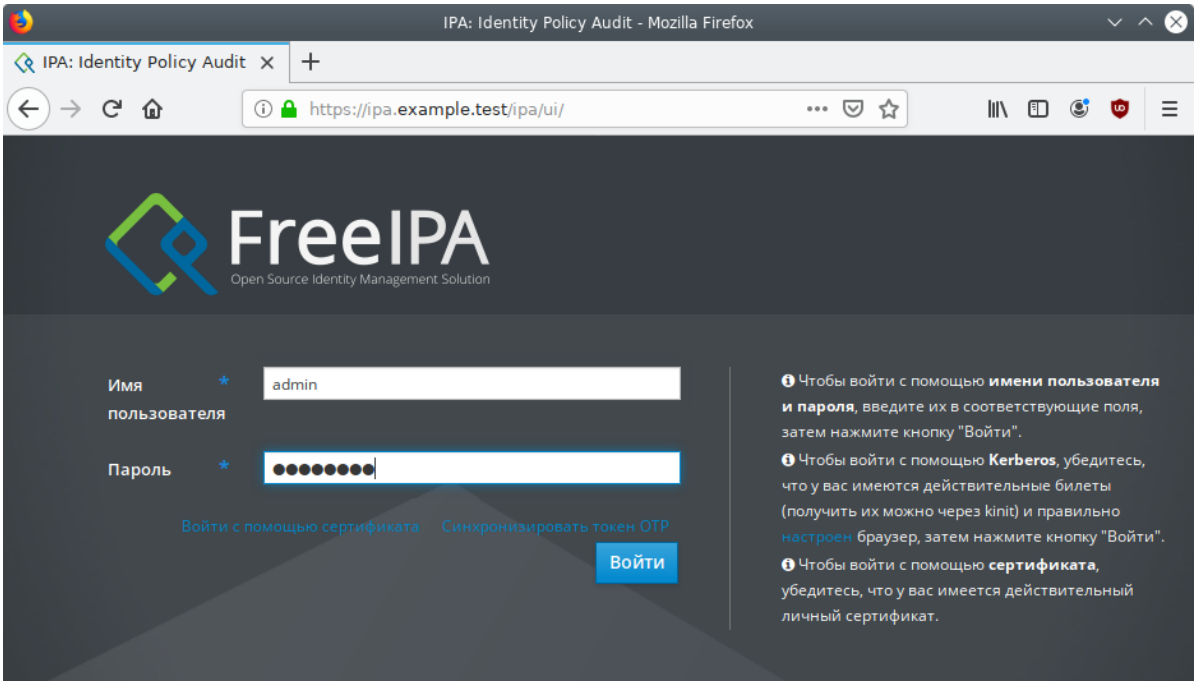


Рис. 90

Создать нового пользователя домена, для этого в окне «Пользователи домена» необходимо нажать кнопку «Добавить» (Рис. 91).

Пользователи домена

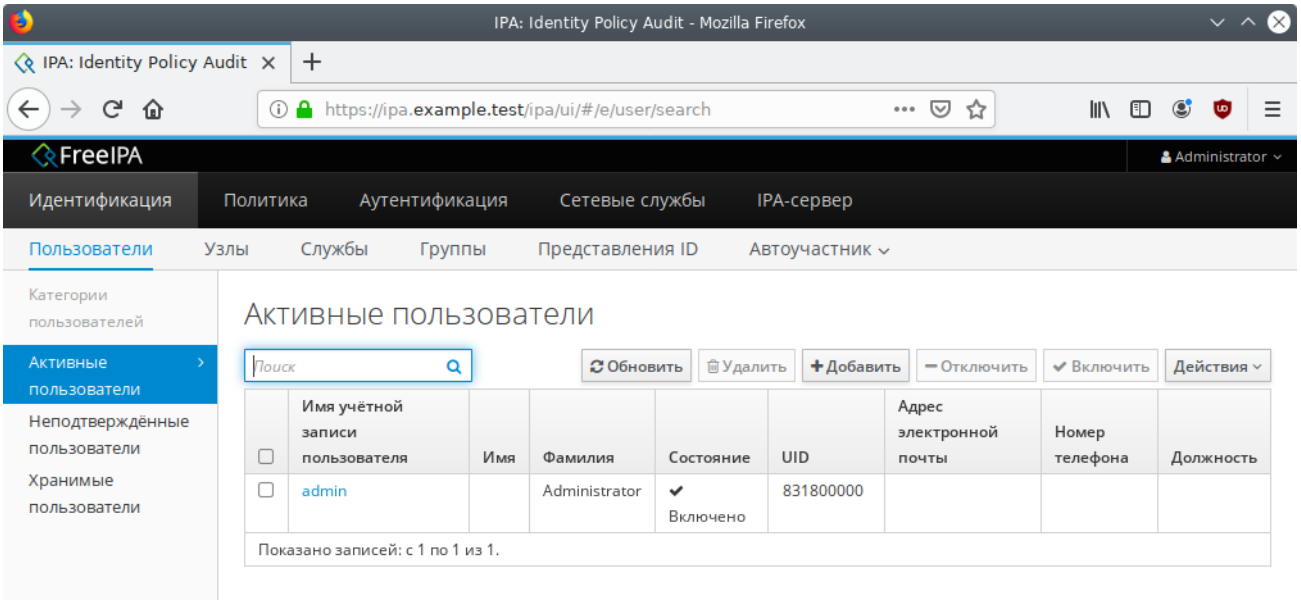


Рис. 91

В открывшемся окне (Рис. 92) необходимо ввести данные пользователя и нажать кнопку «Добавить». Созданный пользователь появится в списке пользователей (Рис. 93).

Окно добавления нового пользователя домена

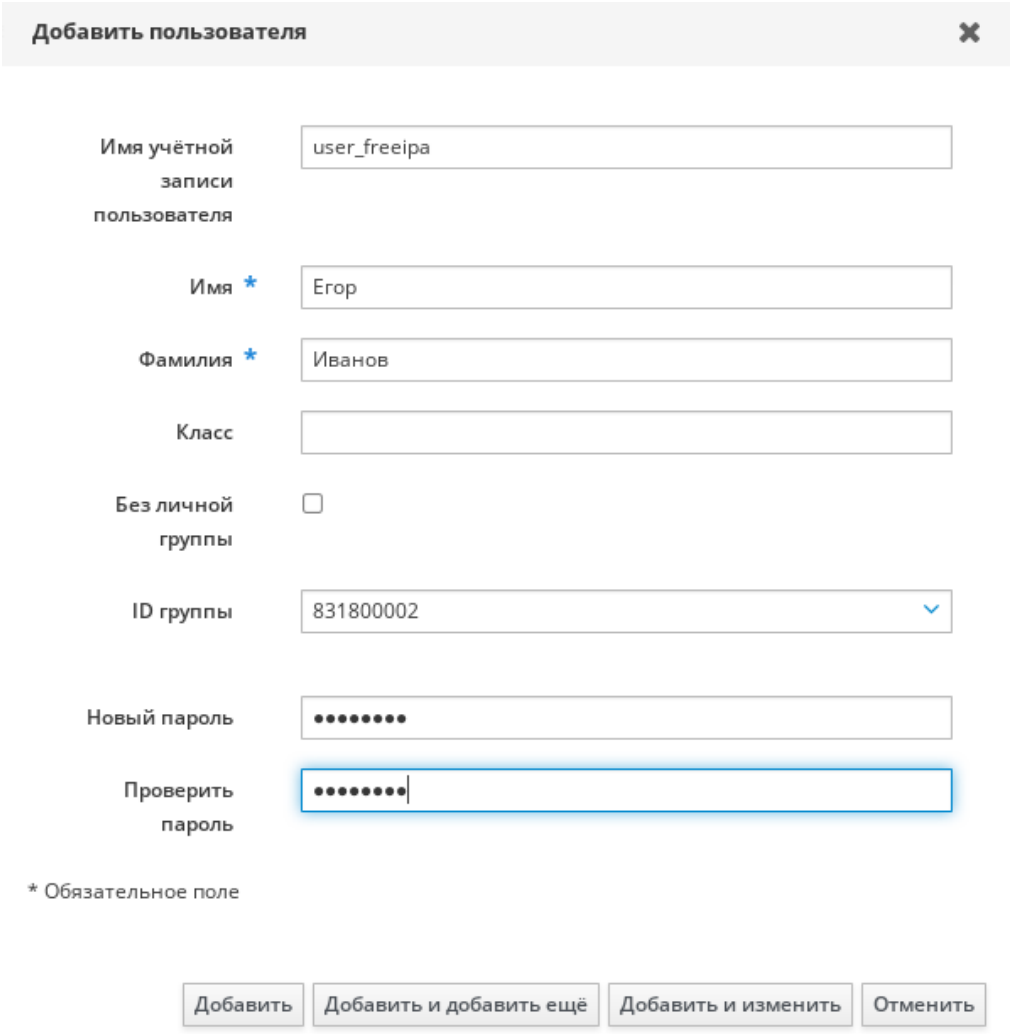


Рис. 92

Список пользователей домена

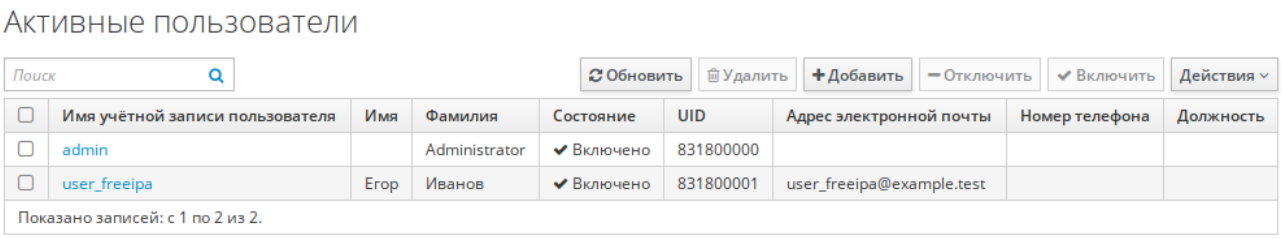


Рис. 93

6.5.3 Ввод рабочей станции в домен FreeIPA

6.5.4 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 ЦУС в разделе «Сеть» → «Ethernet интерфейсы» задать имя компьютера, указать в поле «DNS-серверы» DNS-сервер домена и в поле «Домены поиска» – домен для поиска (Рис. 94);
- 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 DNS-сервера домена.
  - 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
    ```

Настройка на использование DNS-сервера домена

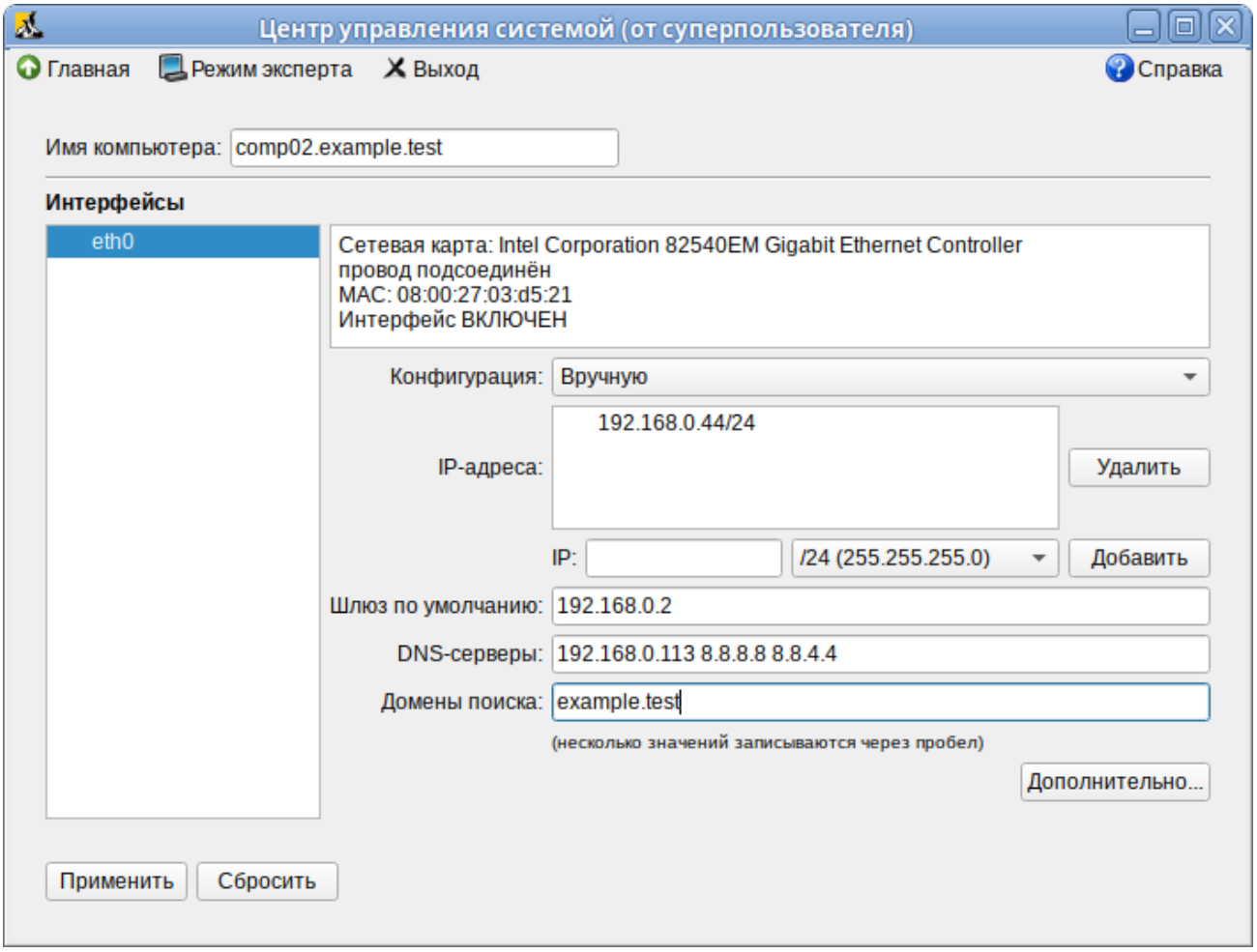


Рис. 94

В результате выполненных действий в файле `/etc/resolvconf.conf` должны появиться строки:

```
search example.test
nameserver 192.168.0.113
```

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

6.5.4.1 Ввод в домен в ЦУС

Для ввода рабочей станции в домен необходимо запустить ЦУС («Меню MATE» → «Приложения» → «Администрирование» → «Центр управления системой»). В ЦУС следует перейти в раздел «Пользователи» → «Аутентификация».

В открывшемся окне необходимо выбрать пункт «Домен FreeIPA» (Рис. 95) и заполнить поля, после чего нажать кнопку «Применить».

Ввод в домен в «Центре управления системой»

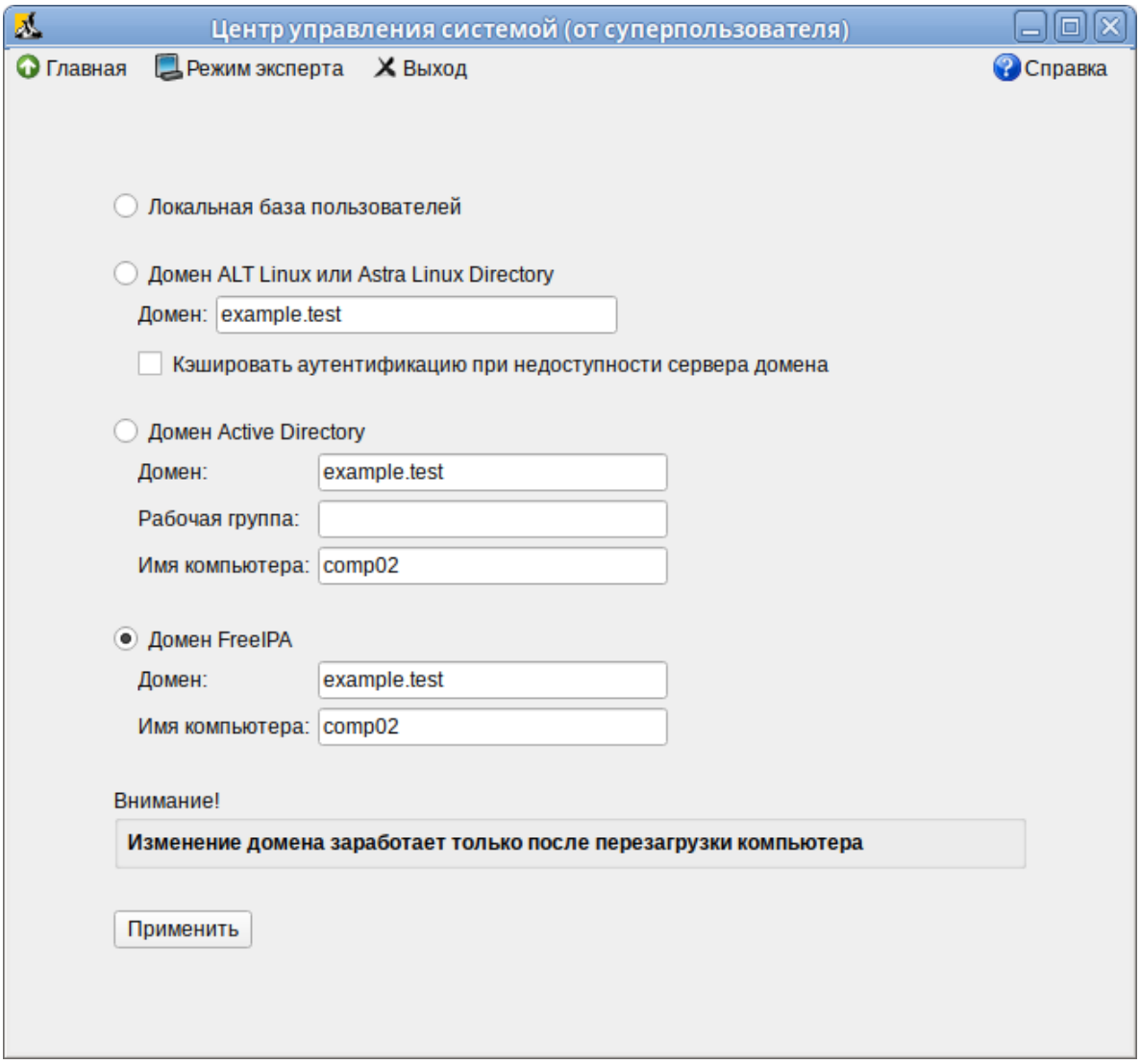


Рис. 95

В открывшемся окне (Рис. 96) необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку «ОК».

Параметры учетной записи с правами подключения к домену

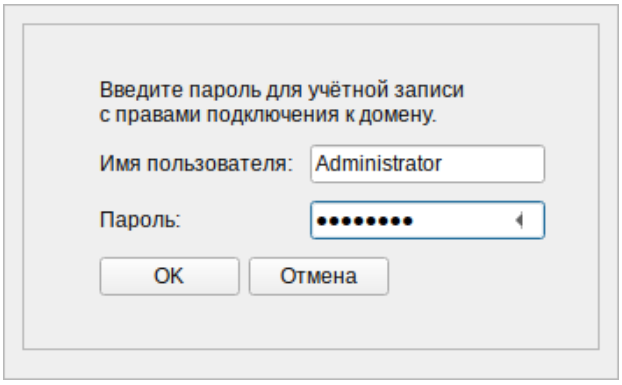


Рис. 96

При успешном подключении к домену, отобразится соответствующая информация (Рис. 97).

Успешное подключение к домену

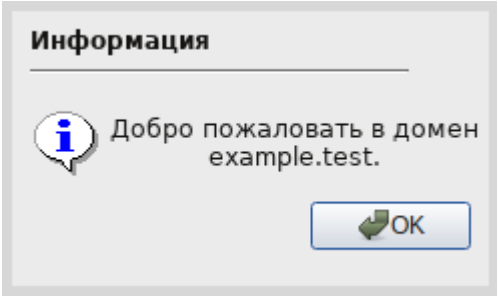


Рис. 97

Перезагрузить рабочую станцию.

6.5.4.2 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: comp02.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.

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
```

Перезагрузить рабочую станцию.

6.5.4.3 Вход пользователя

В окне входа в систему (Рис. 98) необходимо ввести логин учетной записи пользователя FreeIPA и нажать кнопку «Войти», в открывшемся окне ввести пароль, соответствующий этой учетной записи и нажать кнопку «Войти».

При первом входе пользователя будет запрошен текущий (установленный администратором) пароль и затем у пользователя запрашивается новый пароль (Рис. 99) и его подтверждение.

Вход пользователя

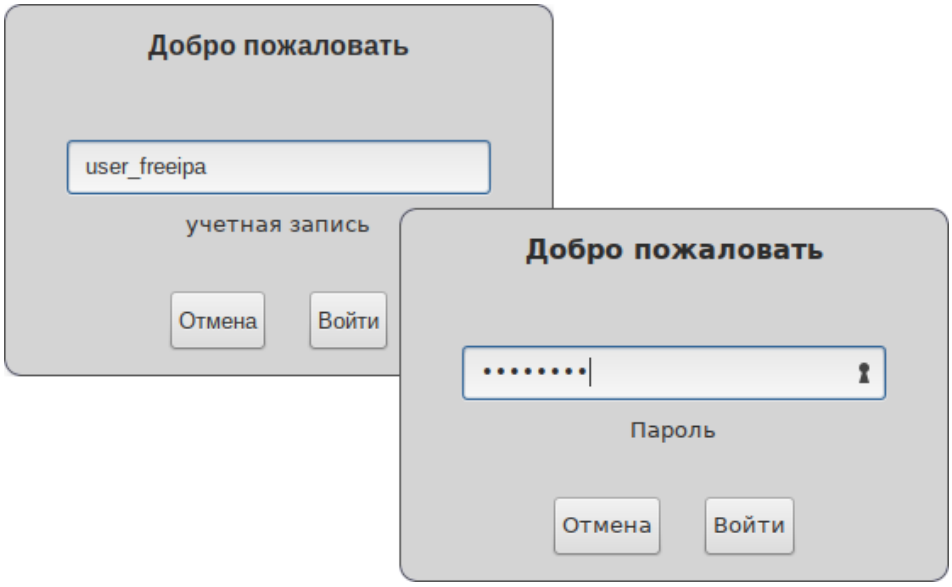


Рис. 98

Запрос текущего пароля и нового пароля при первом подключении к серверу FreeIPA

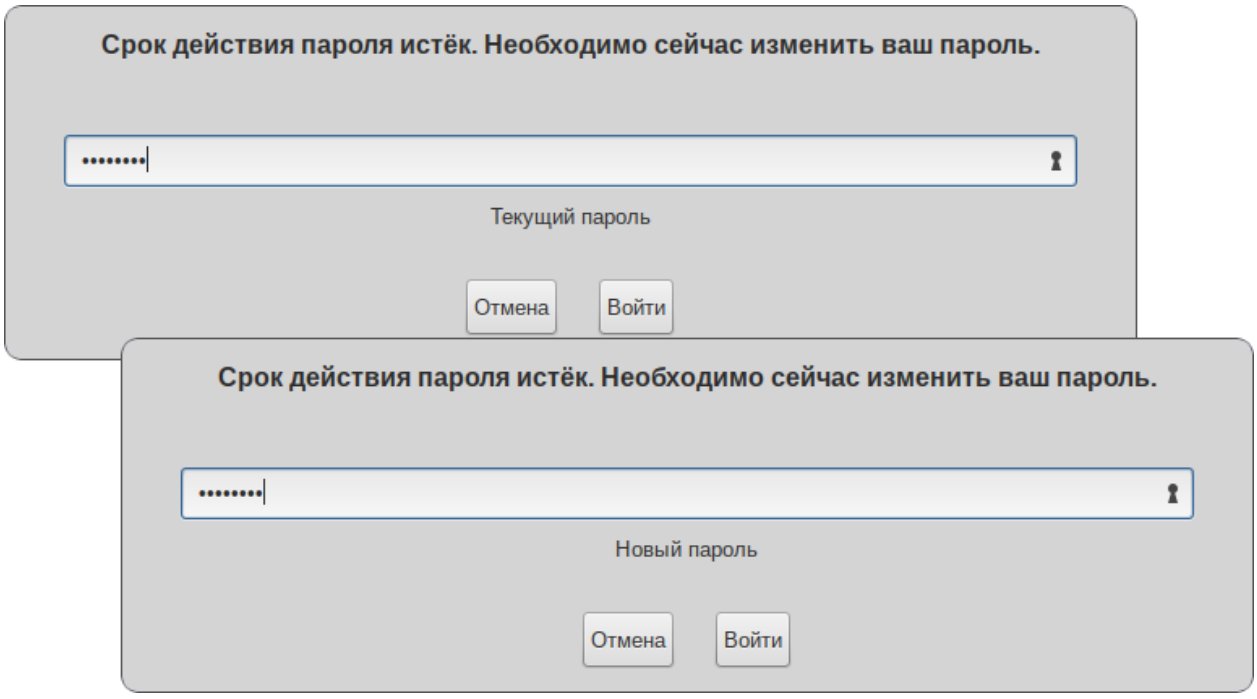


Рис. 99

П р е д у п р е ж д е н и е . 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
```

6.5.5 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.

6.6 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.

6.6.1 Установка и настройка Fleet Commander

6.6.1.1 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.

6.6.1.2 Установка и настройка Fleet Commander Admin

Предварительно необходимо установить и настроить FreeIPA сервер, с созданием домашнего каталога (опция --mkhomedir).

Установить необходимые пакеты:

```
# apt-get install freeipa-desktop-profile
...
Perform the IPA upgrade. This may take a while.
The IPA upgrade was successful.
Завершено.
```

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:

```
# apt-get install fleet-commander-admin
```

Добавить сервис Cockpit в автозапуск и запустить его:

```
# systemctl enable --now cockpit.socket
```

Веб-интерфейс Cockpit будет доступен по адресу https://адрес-сервера:9090/ (Рис. 100).

Веб-интерфейс Cockpit

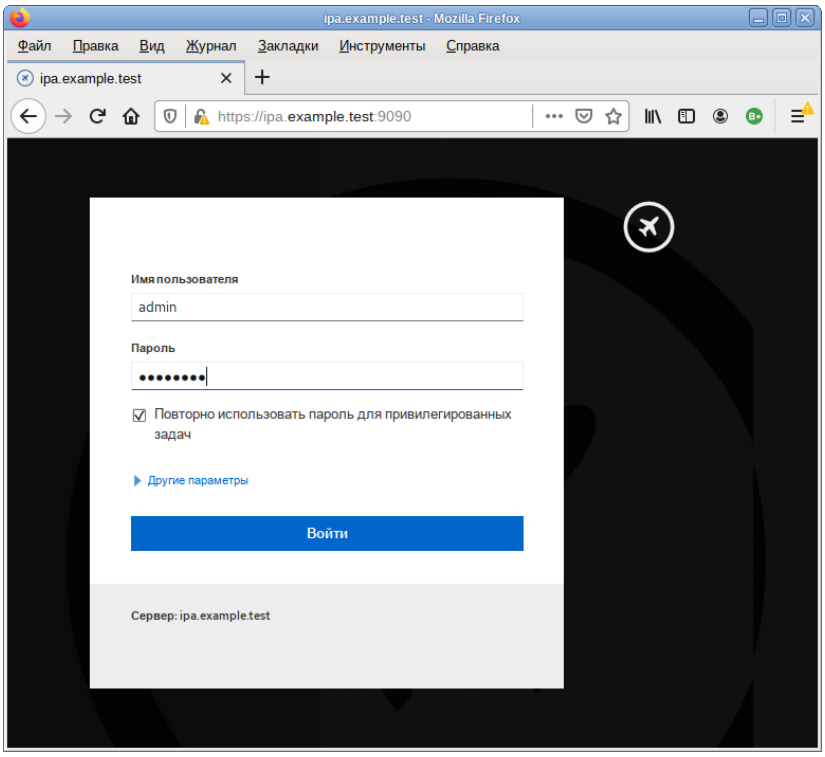


Рис. 100

Вход осуществляется по логину указанному при установке FreeIPA сервера.

Для доступа к настройке Fleet Commander следует выбрать соответствующую кнопку на левой панели веб-интерфейса (Рис. 101).

Веб-интерфейс Cockpit. Доступ к настройке Fleet Commander

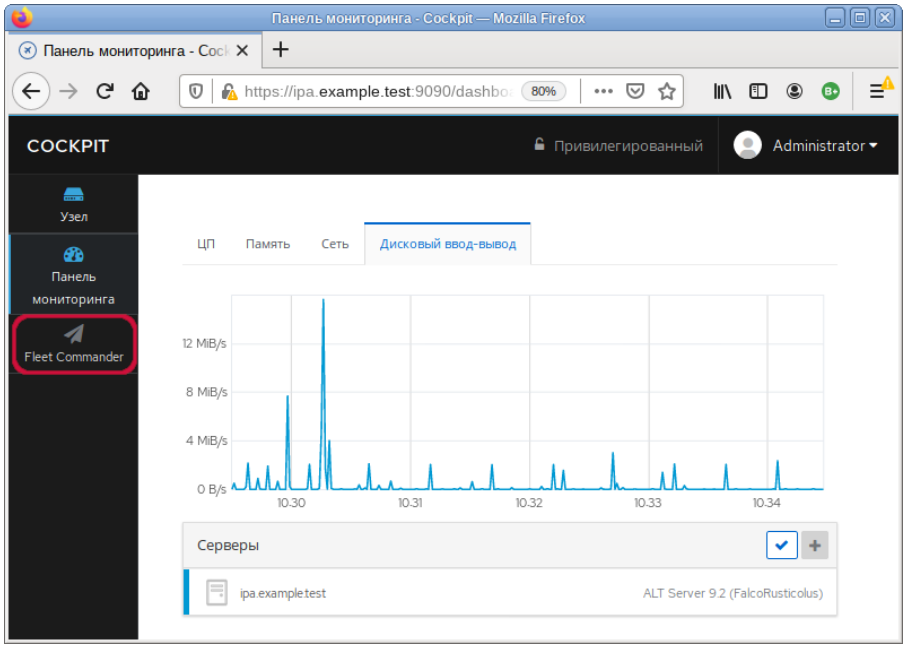


Рис. 101

При первом запуске Fleet Commander необходимо настроить глобальную политику и информацию о хосте libvirt.

Открыть окно настроек можно, нажав кнопку «Settings» на вкладке Fleet Commander (Рис. 102).

Вкладка Fleet Commander

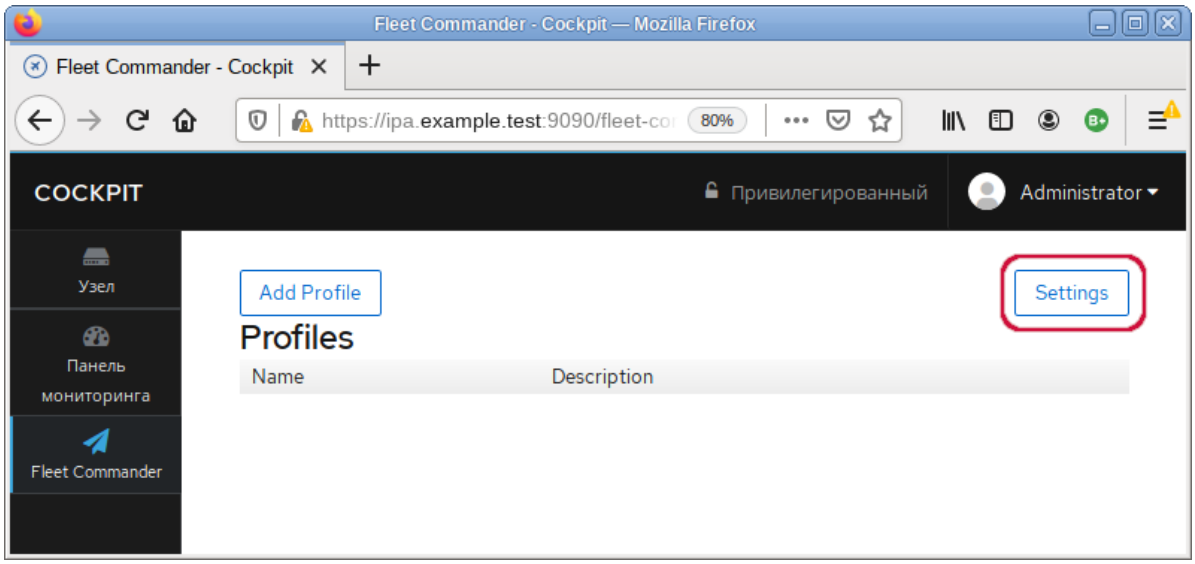


Рис. 102

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 (Рис. 103) 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.

Окно настроек Fleet Commander

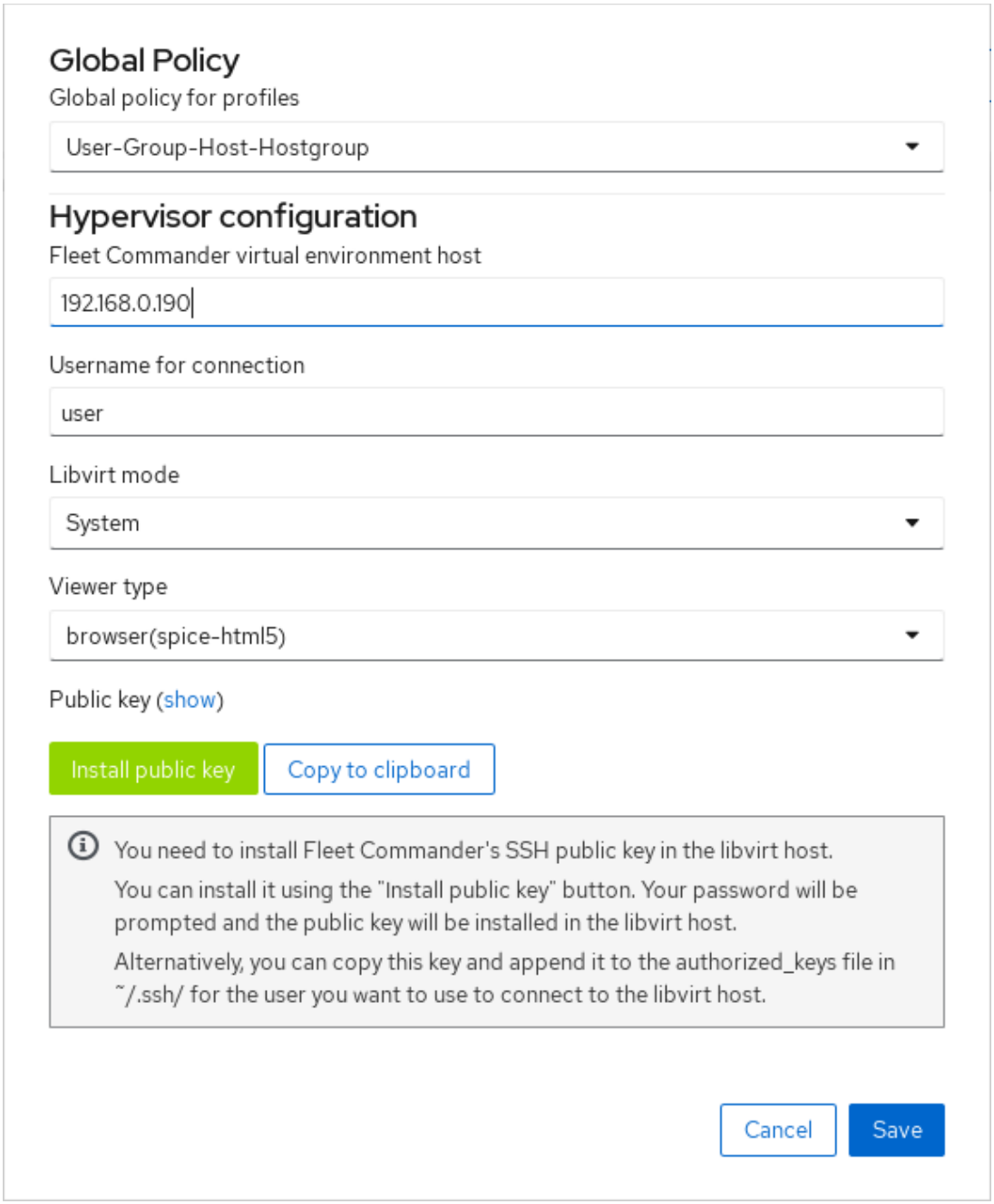


Рис. 103

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», при этом будет необходимо ввести пароль пользователя. Пароль используется только для установки ключа и нигде не хранится.

П р и м е ч а н и е . На хосте libvirt, должен быть запущен SSH-сервер (служба sshd).

6.6.1.3 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 (Рис. 104).

Fleet Commander. Создание профиля

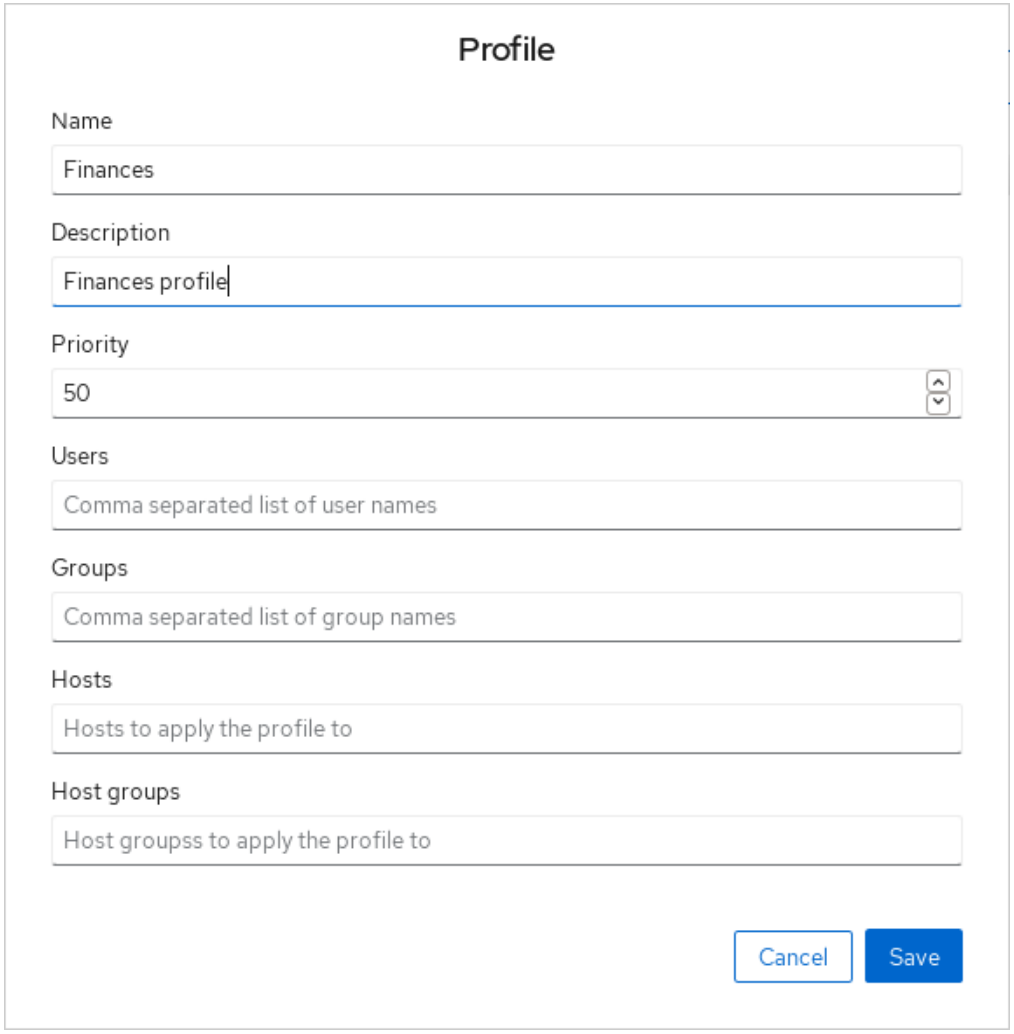


Рис. 104

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.

6.6.1.4 *Настройка шаблона*

Для настройки шаблона в веб-интерфейсе Cockpit необходимо нажать кнопку «Edit» напротив нужного профиля (Рис. 105) и в открывшемся окне нажать кнопку «Live session» (Рис. 106).

Fleet Commander. Редактирование профиля

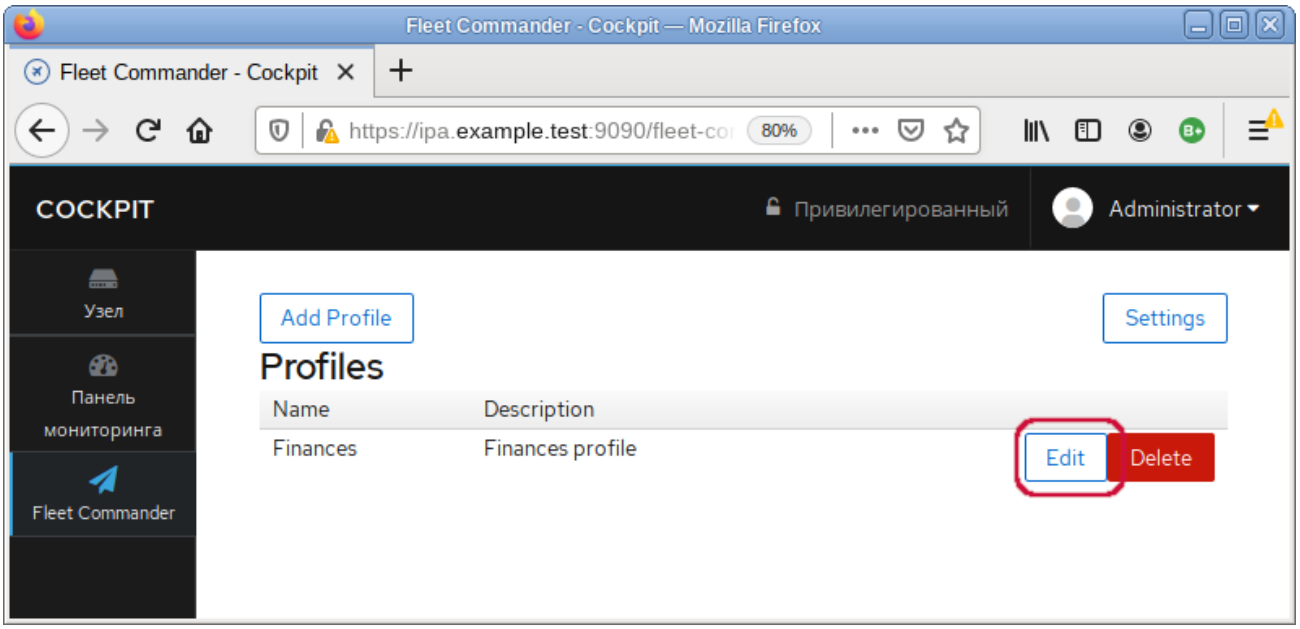


Рис. 105

В появившейся форме будет выведен список доступных шаблонов. При выборе шаблона, он начнет загружаться.

6.6.1.5 *Установка и настройка Fleet Commander Client*

Клиентская машина должна быть введена в домен. Также должны быть созданы доменные пользователи.

Установить необходимый пакет:

```
# 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.

Fleet Commander. Кнопка «Live session»

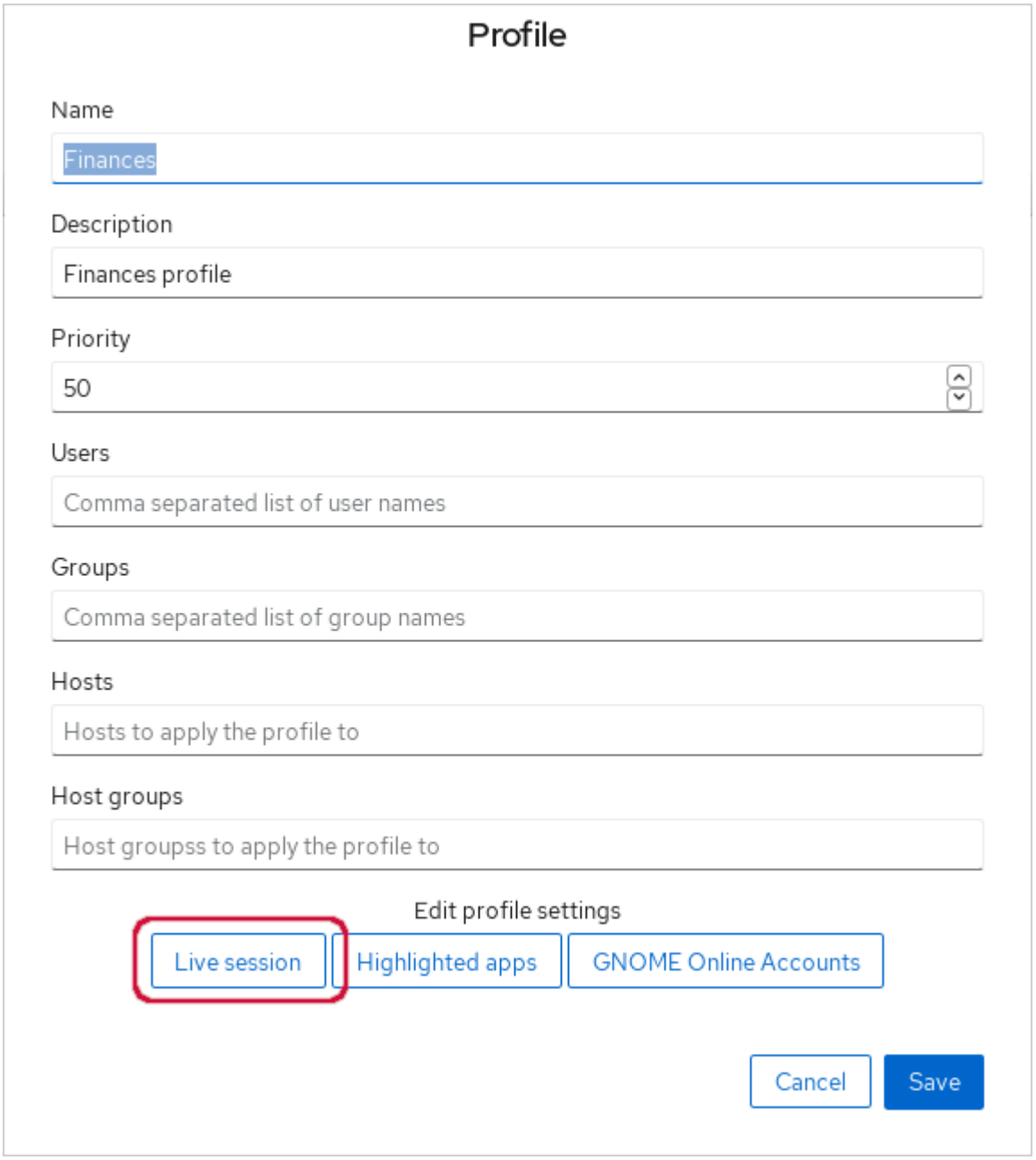


Рис. 106

6.6.2 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:

- открыть https://адрес-сервера:9090/fleet-commander-admin и запустить live-сессию («Edit» → «Live session»). Появится окно выбора машины для загрузки в live-сессии (Рис. 107);
- выбрать машину, на которой установлен Fleet Commander Logger, и запустить ее (Рис. 108). Загруженная машина является шаблоном, все сделанные на ней изменения будут отловлены регистратором, сохранены и применены на клиентских системах;
- на загруженной машине внести необходимые изменения в настройки;
- в веб-интерфейсе Cockpit нажать кнопку «Review and submit». Появится окно со списком сделанных изменений (Рис. 109). В списке изменений можно выбрать как все изменения, так и частичные, установив отметку напротив нужного. После выбора нажать кнопку «Save», для сохранения изменений;
- загрузить клиентскую машину, войти в систему под доменным пользователем. Убедиться, что сделанные изменения успешно применились.

Fleet Commander. Список доступных шаблонов

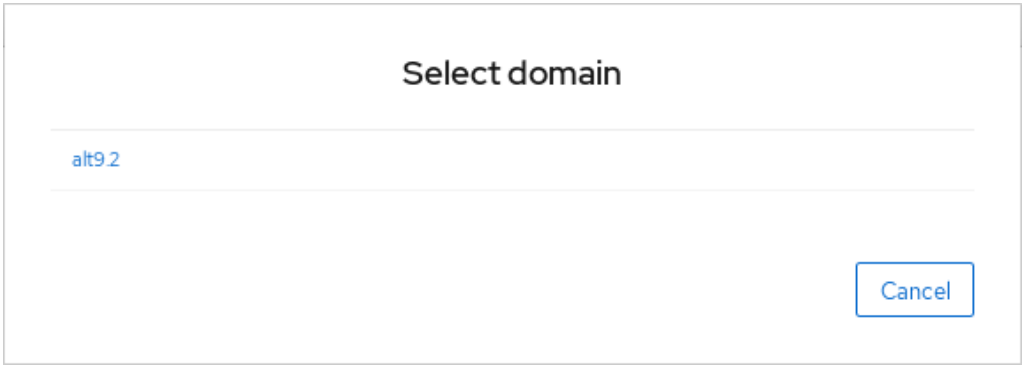


Рис. 107

6.6.3 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.

Fleet Commander. Загруженный шаблон

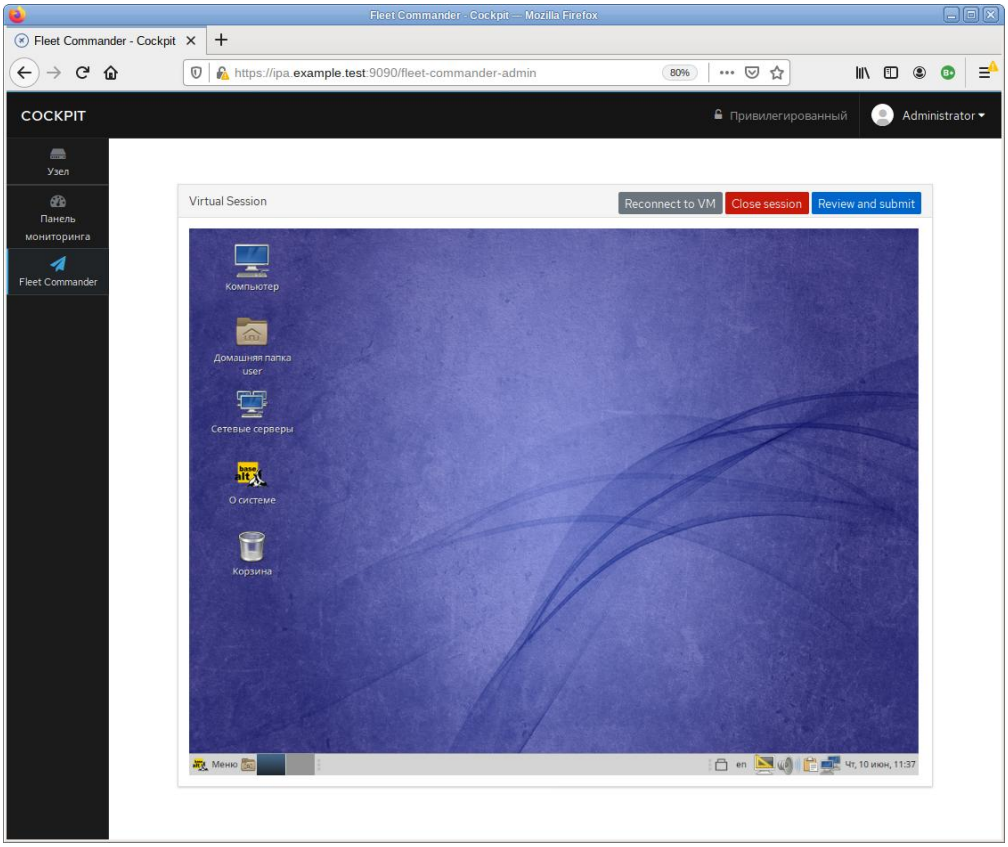


Рис. 108

Окно со списком сделанных изменений

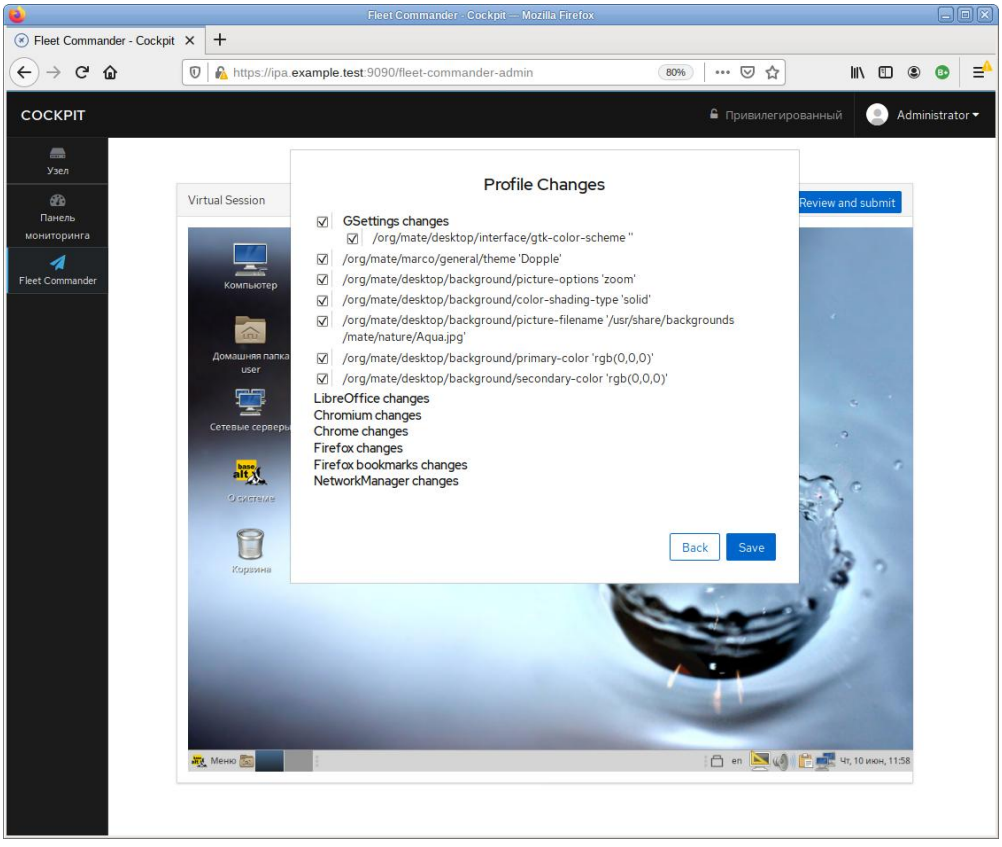


Рис. 109

6.7 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.

Перед установкой должен быть установлен и запущен сервер PostgreSQL, с созданным пользователем zabbix и созданной базой zabbix.

6.7.1 Установка сервера PostgreSQL

Установить необходимые пакеты:

```
# apt-get install postgresql12-server zabbix-server-pgsql
```

Подготовить к запуску и настроить службы PostgreSQL:

- 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):

```
# postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --
no-createrole --encrypted --pwprompt zabbix'
# 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):

```
# postgres -s /bin/sh -c 'psql -U zabbix -f /usr/share/doc/zabbix-
common-database-pgsql-*/schema.sql zabbix'
# остановитесь здесь, если вы создаете базу данных для Zabbix прокси
# postgres -s /bin/sh -c 'psql -U zabbix -f /usr/share/doc/zabbix-
common-database-pgsql-*/images.sql zabbix'
# postgres -s /bin/sh -c 'psql -U zabbix -f /usr/share/doc/zabbix-
common-database-pgsql-*/data.sql zabbix'
```

6.7.2 Установка Apache2

Установить необходимые пакеты:

```
# apt-get install apache2 apache2-mod_php7
```

Добавить в автозапуск и запустить apache2:

```
# chkconfig httpd2 on
# service httpd2 start
```

6.7.3 Установка PHP

Установить необходимые Zabbix-у пакеты:

```
# apt-get install php7-mbstring php7-sockets php7-gd2 php7-xmlreader
php7-pgsql php7-ldap
```

Так же необходимо 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
```

6.7.4 Установка Zabbix Server

Установить, если еще не установлены, пакеты zabbix-server-pgsql, fping:

```
# apt-get install zabbix-server-pgsql fping
```

Внести изменения в конфигурационный файл `/etc/zabbix/zabbix_server.conf`:

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=Пароль от базы
```

Добавить zabbix server в автозапуск и запустить его:

```
# chkconfig zabbix_pgsql on
# service zabbix_pgsql start
```

6.7.5 Установка веб-интерфейса Zabbix

Установить метапакет:

```
# 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 конфигурационной директории 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
```

Перейти на страницу установки zabbix сервера: http://<ip-сервера>/zabbix (Рис. 110).

Страница установки zabbix сервера

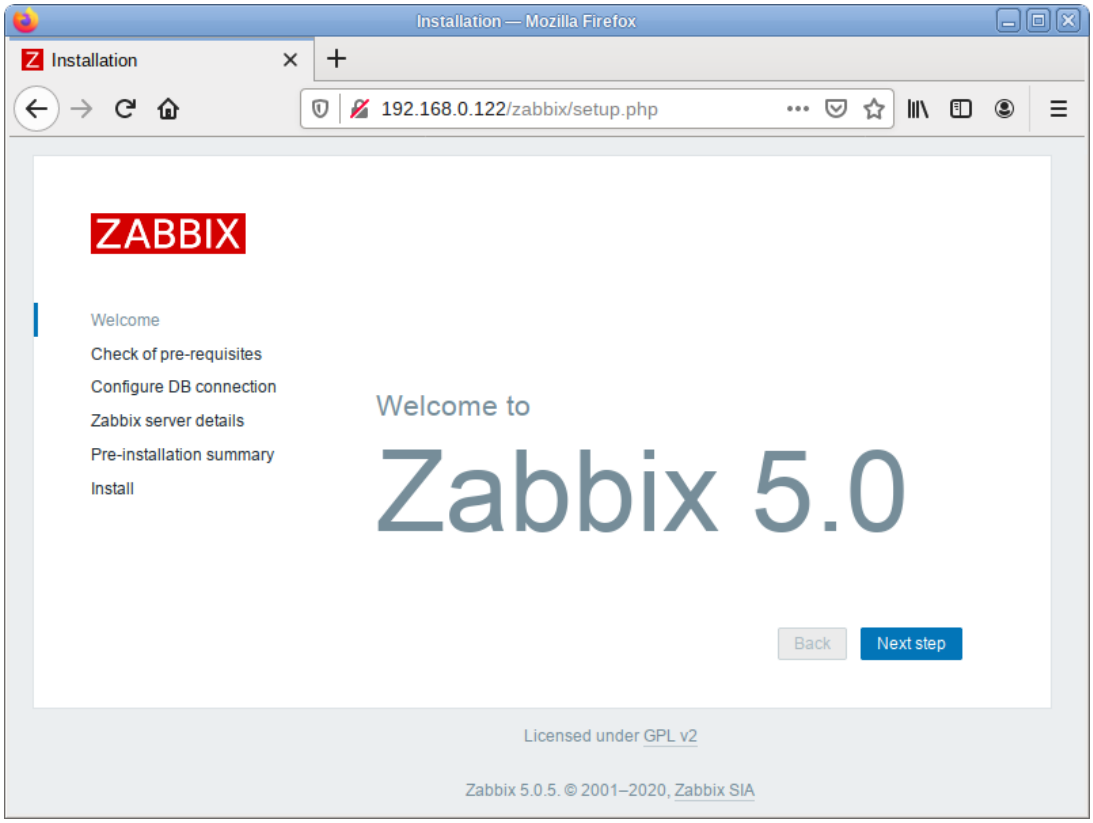


Рис. 110

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
```

При первом заходе на страницу запустится мастер, который шаг за шагом проверит возможности веб-сервера, интерпретатора PHP и сконфигурирует подключение к базе данных.

Для начала установки необходимо нажать кнопку «Next Step», что осуществит переход на страницу проверки предварительных условий (Рис. 111).

Страница проверки предварительных условий

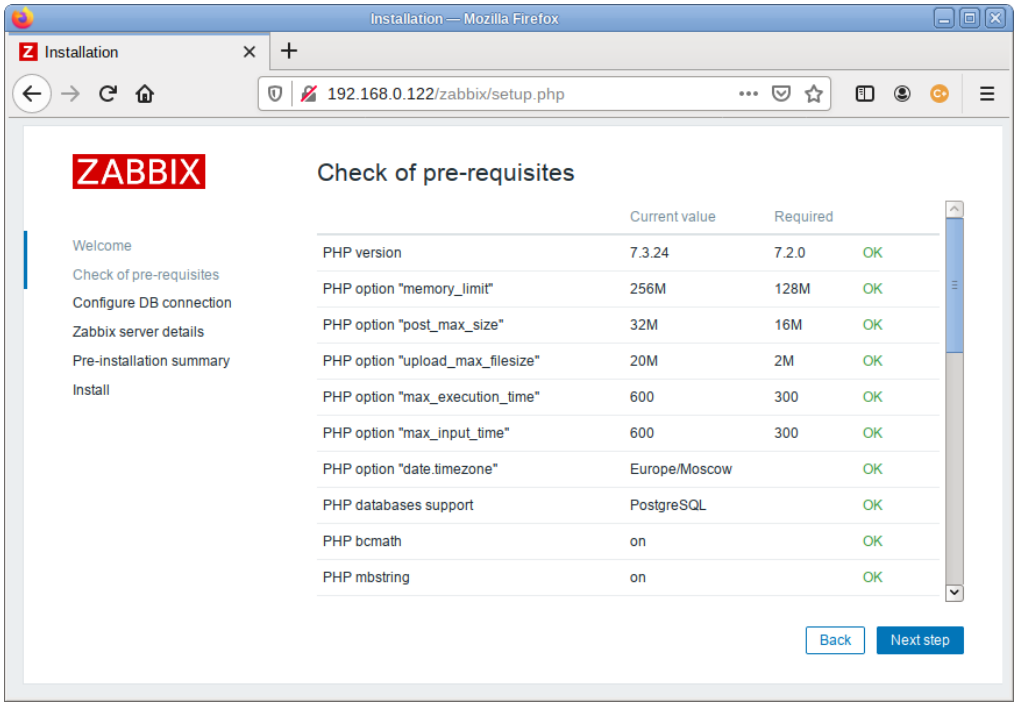


Рис. 111

Необходимо доустановить то, что требуется и перейти на следующую страницу.

На этой странице (Рис. 112) 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».

Параметры подключения к базе данных

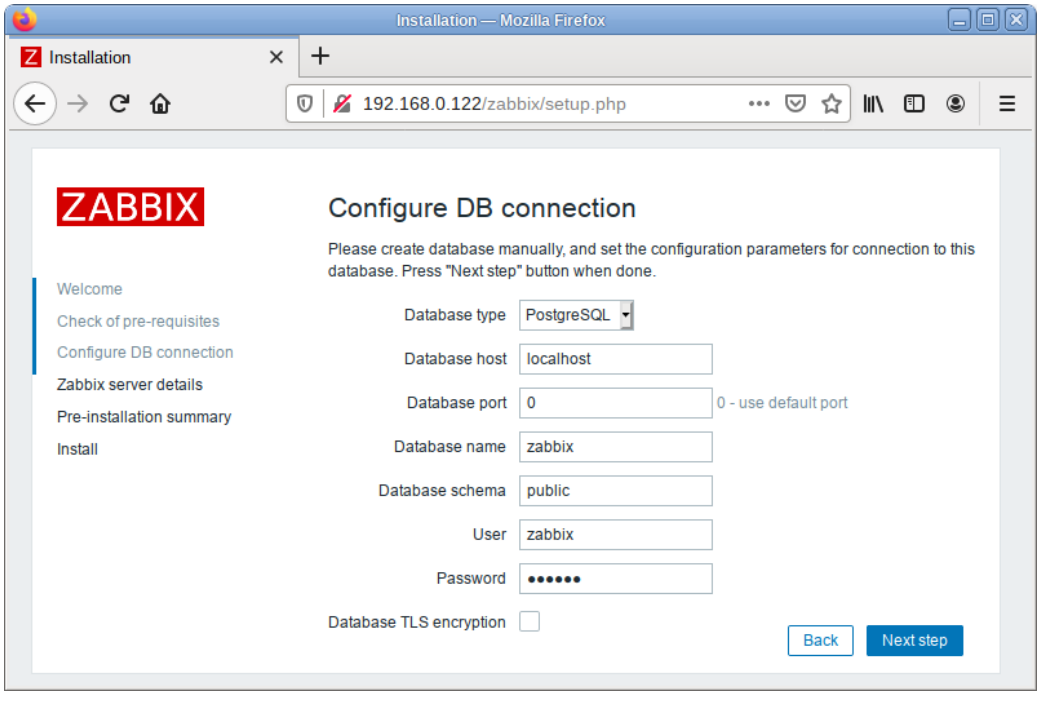


Рис. 112

На следующей странице необходимо задать имя сервера (Рис. 113) и завершить установку (Рис. 114-Рис. 115).

Настройки zabbix сервера

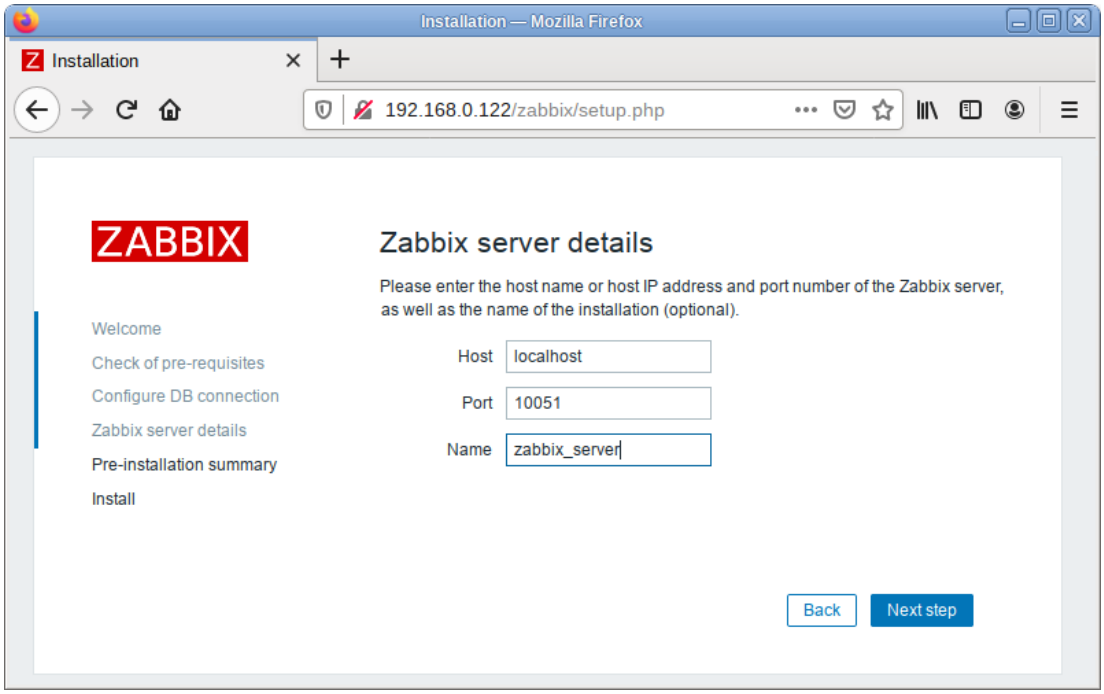


Рис. 113

Параметры конфигурации

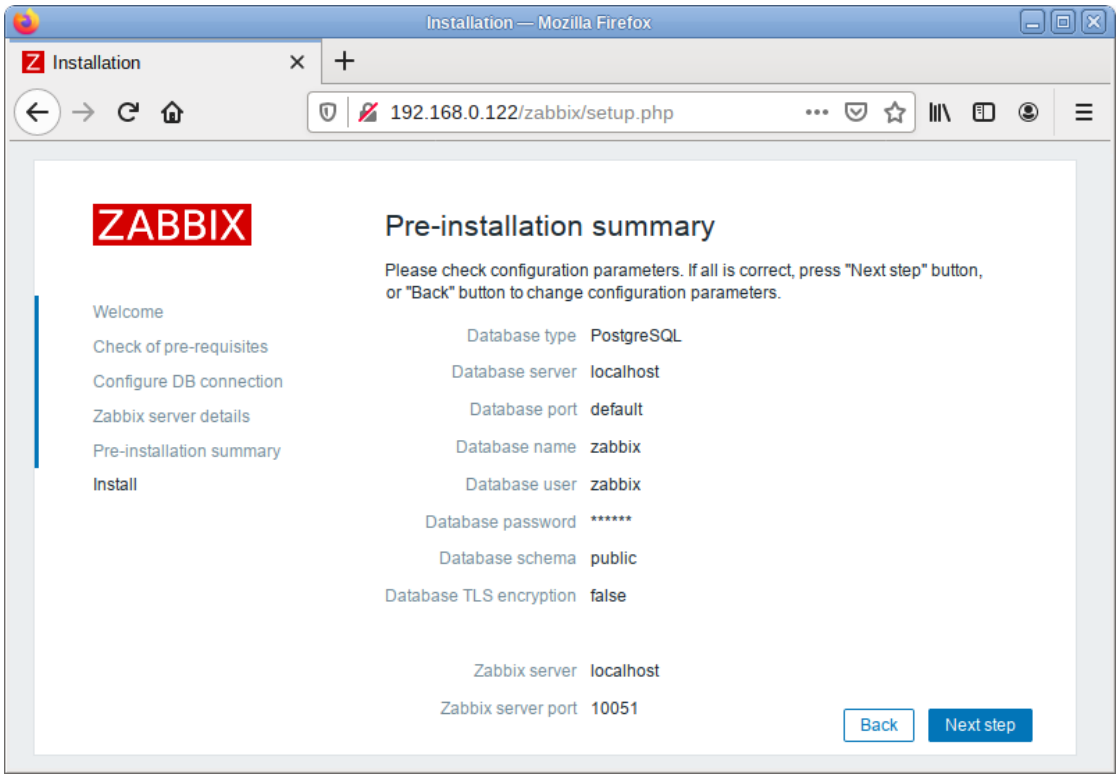


Рис. 114

Окончание установки

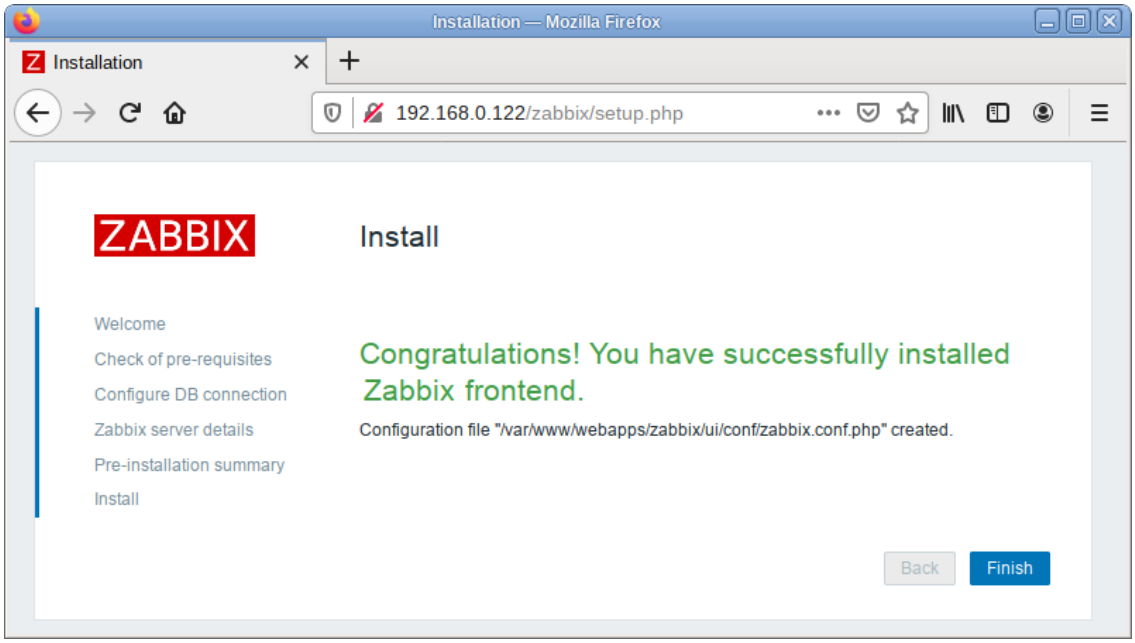


Рис. 115

После окончания установки на экране будет отображаться форма входа в интерфейс управления системой мониторинга (Рис. 116). Параметры доступа по умолчанию:

`Логин: Admin`

`Пароль: zabbix`

Форма входа в интерфейс управления системой мониторинга

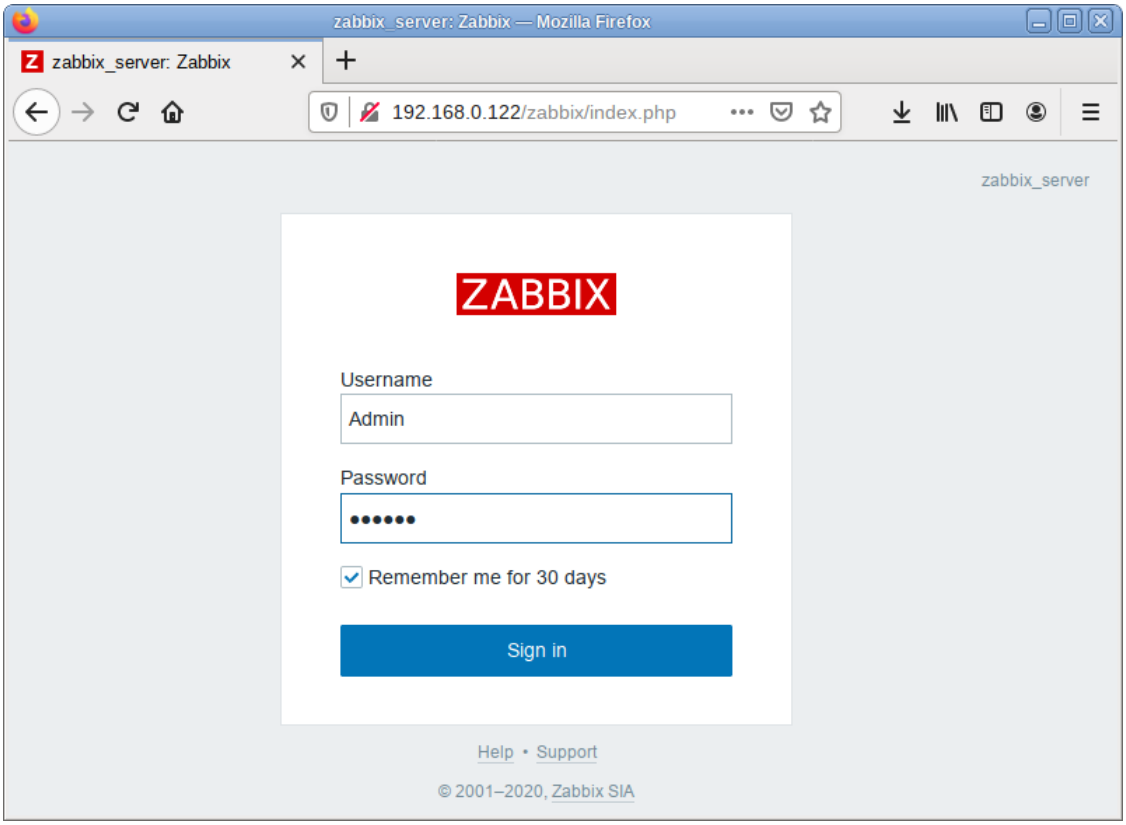


Рис. 116

Войдя в систему, нужно сменить пароль пользователя, завести других пользователей и можно начать настраивать Zabbix (Рис. 117).

Интерфейс управления системой мониторинга

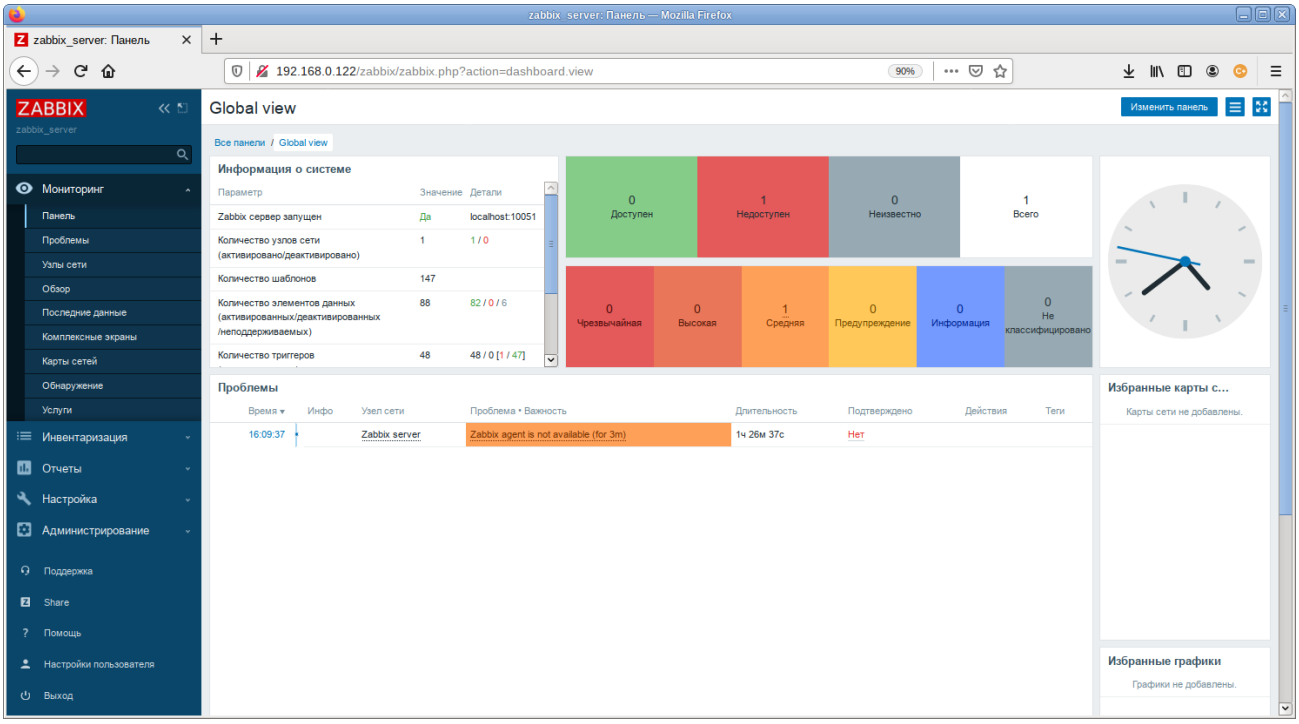


Рис. 117

В профиле пользователя (Рис. 118) 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.

Профиль пользователя

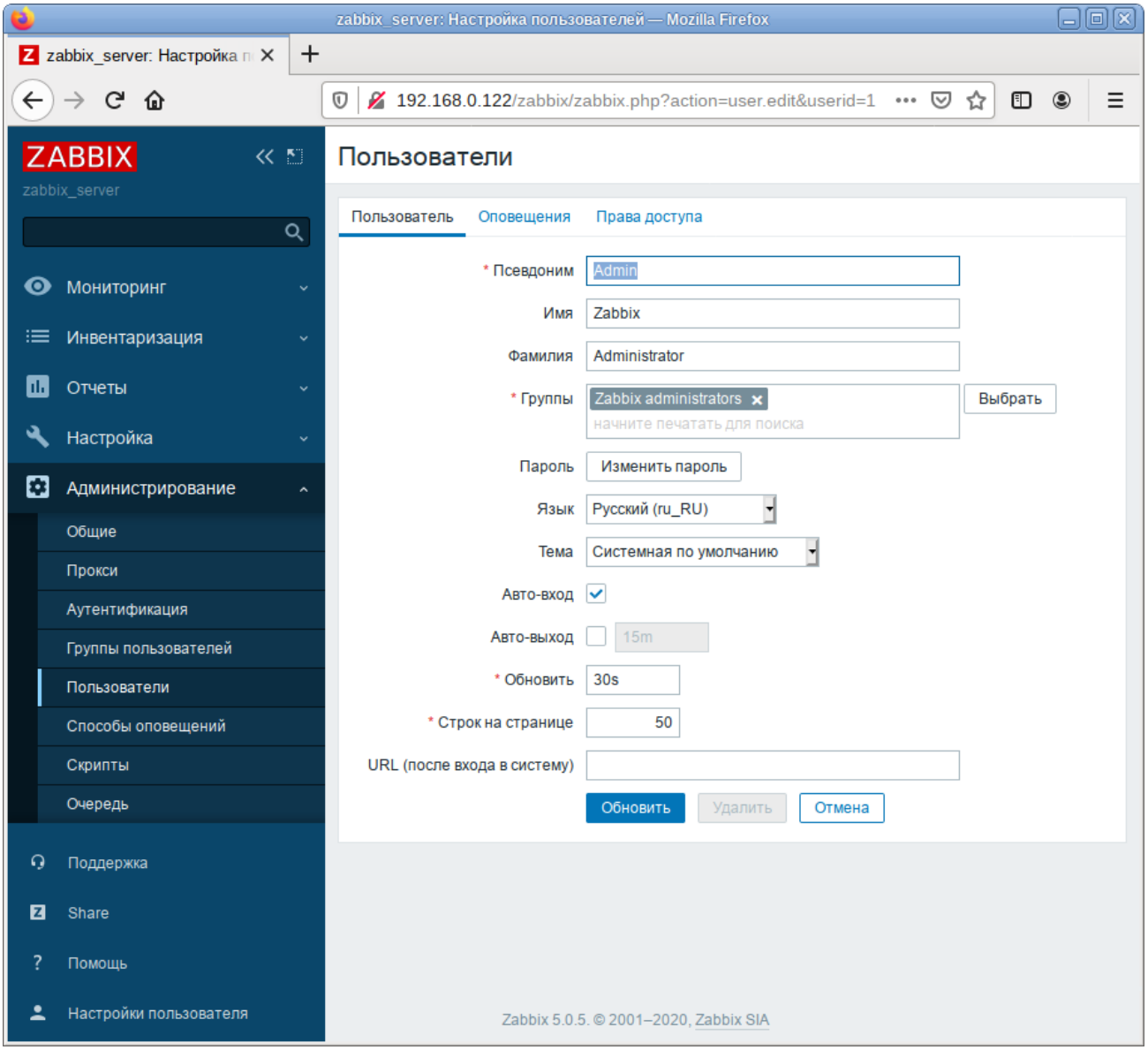


Рис. 118

6.7.6 Установка клиента Zabbix

Установить необходимый пакет:

```
# 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
```

где 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 agent в автозапуск и запустить его:

```
# systemctl enable --now zabbix_agentd.service
```

6.7.7 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» (Рис. 119).

Создание нового узла сети

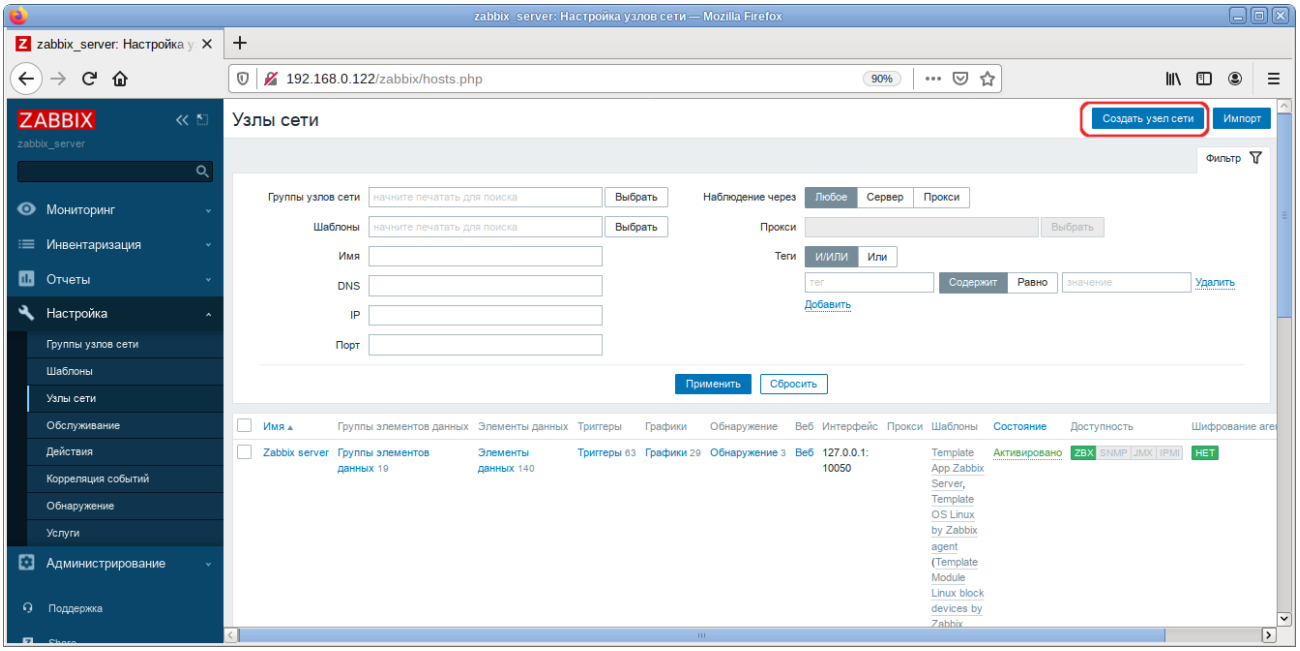


Рис. 119

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 (Рис. 123).

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» (Рис. 124).

Создание нового узла сети. Данные добавляемого хоста

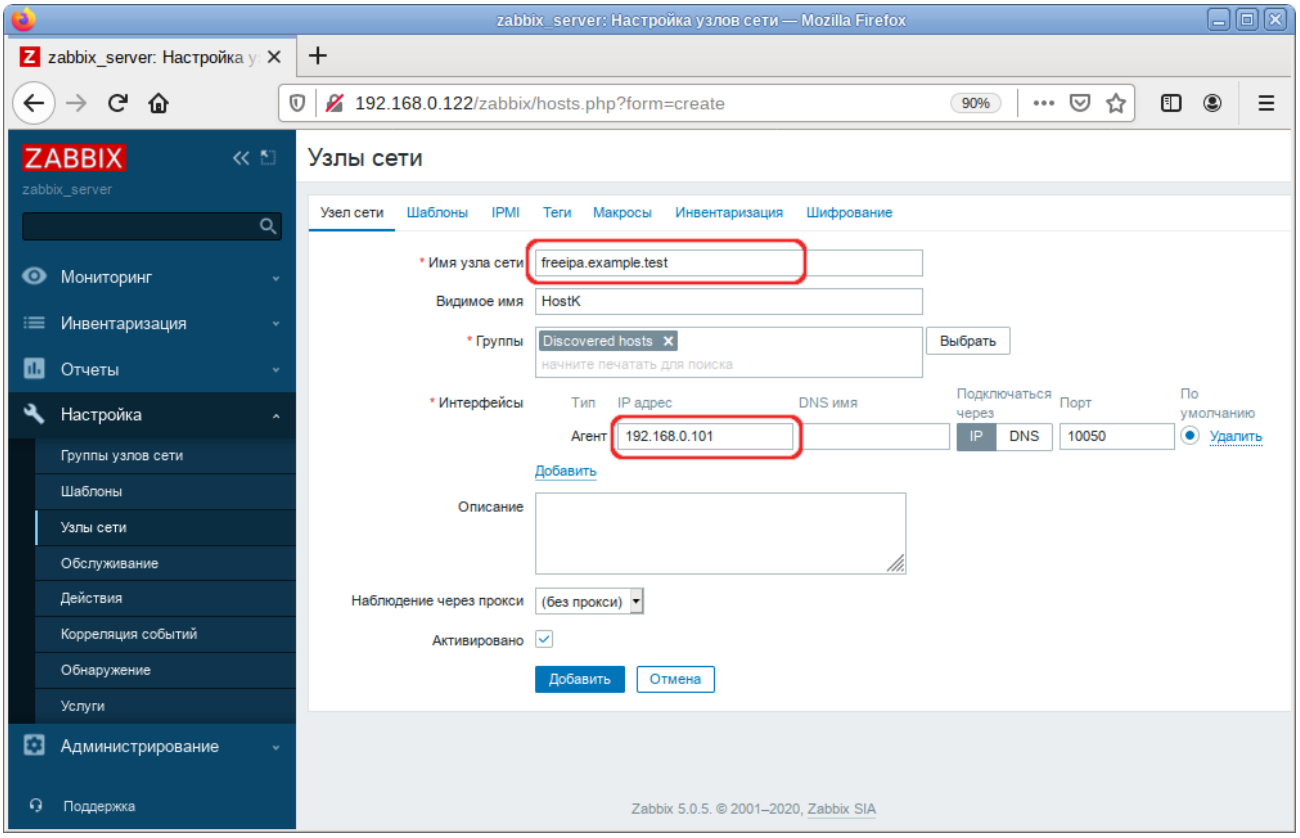


Рис. 120

Создание нового узла сети. Присоединение нового шаблона

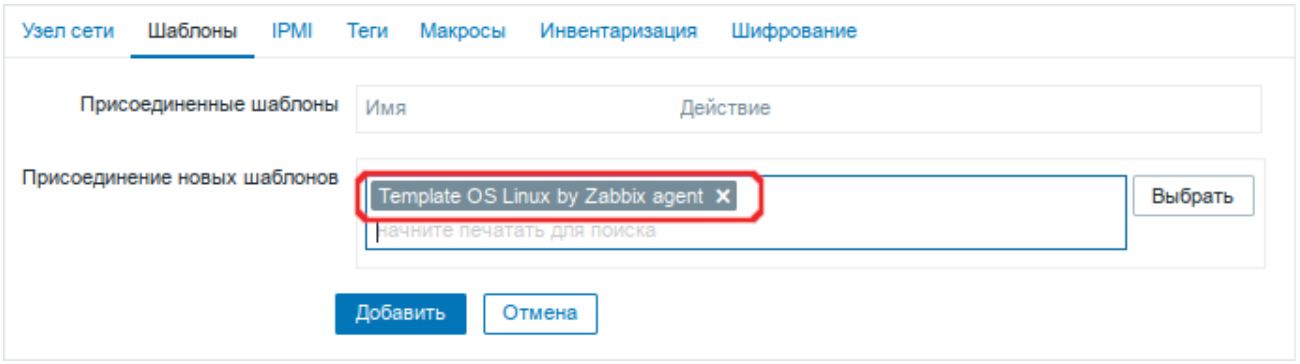


Рис. 121

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» (Рис. 125).

Собранные данные

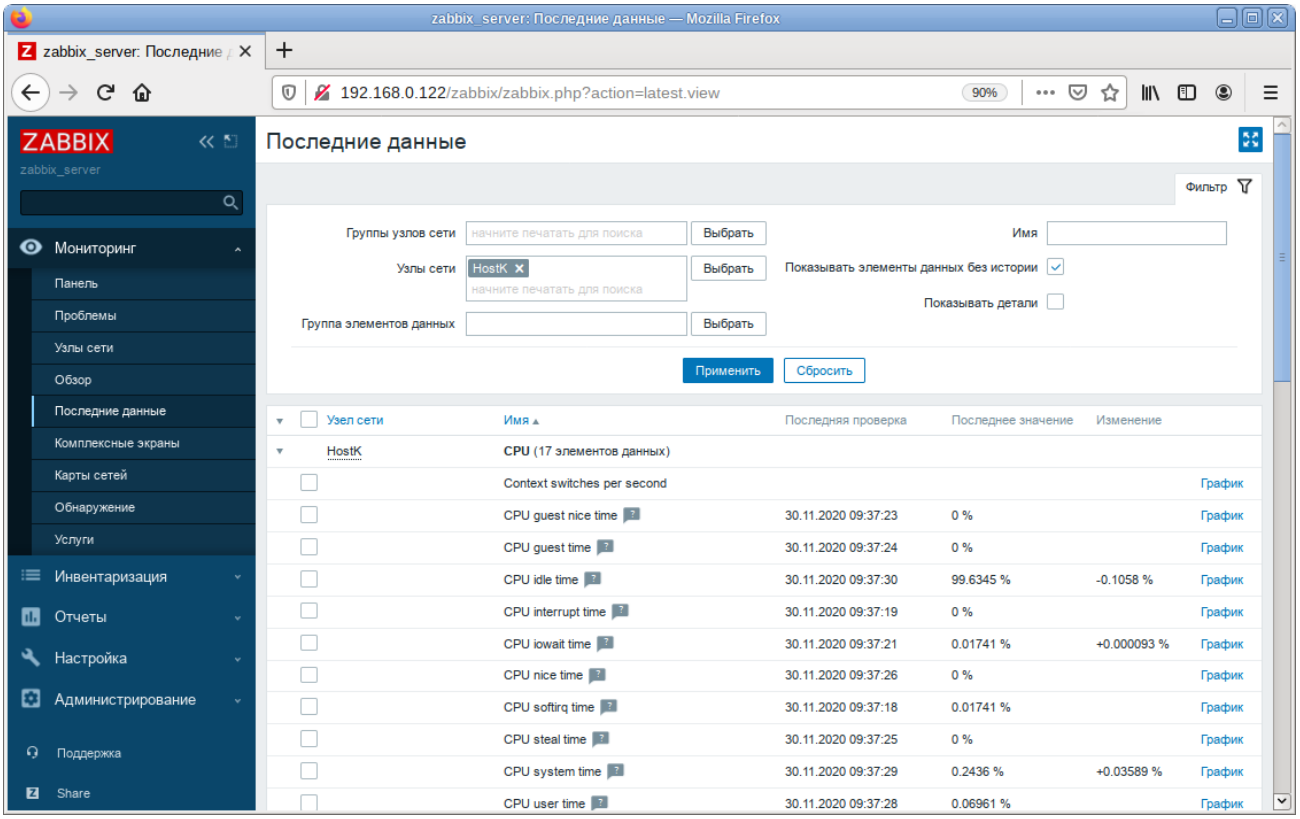


Рис. 122

6.7.8 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» (Рис. 123).

Авторегистрация узлов

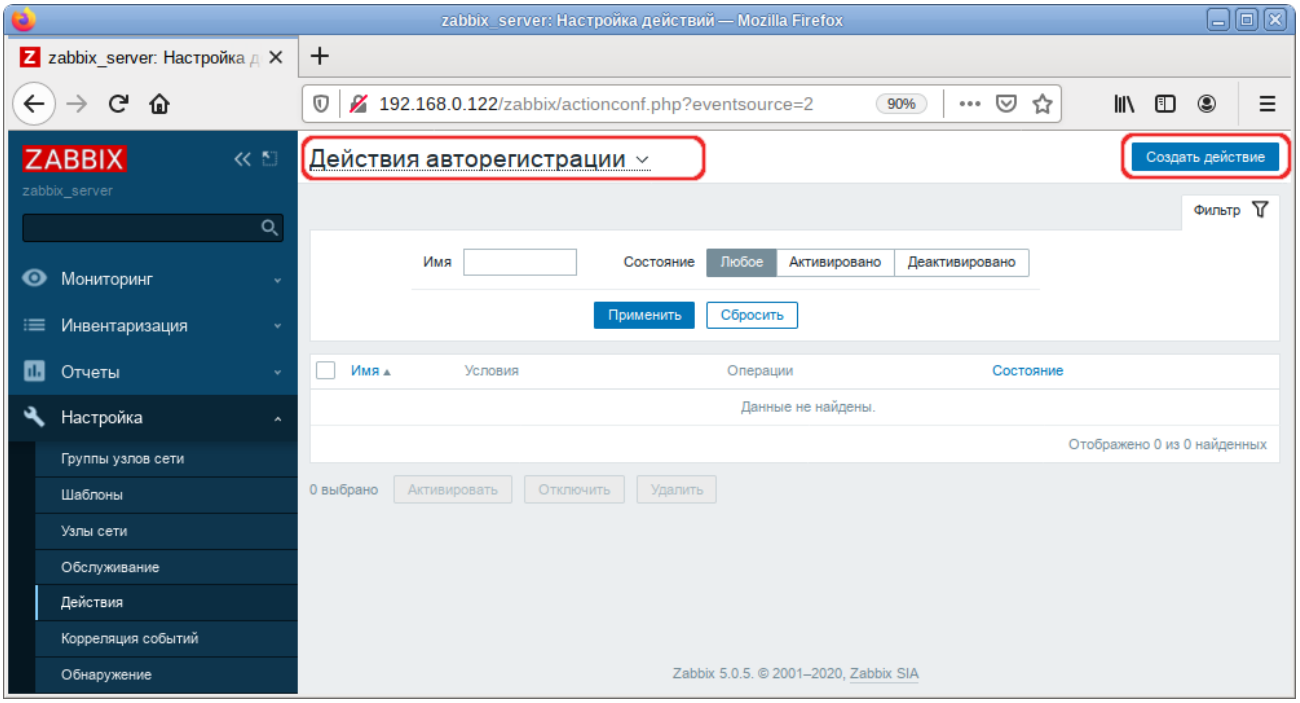


Рис. 123

На открывшейся странице, на вкладке «Действия» заполнить поле «Имя» и добавить условия. В поле «Условия» следует задать правила, по которым будут идентифицироваться регистрируемые хосты (Рис. 124).

Авторегистрация узлов. Условия идентификации узла

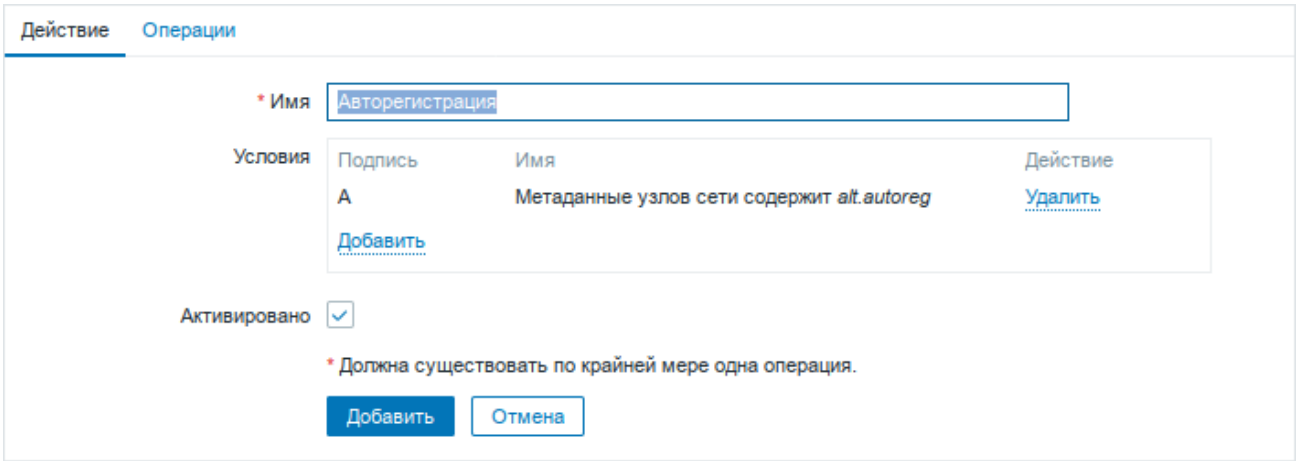


Рис. 124

На вкладке «Операции» в поле «Операции» следует добавить правила, которые необходимо применить при регистрации хоста. Правила для добавления узла, добавления его к группе «Discovered hosts» с присоединением к шаблону «Template OS Linux by Zabbix agent» показаны на Рис. 125.

Авторегистрация узлов. Правила, применяемые при регистрации узла

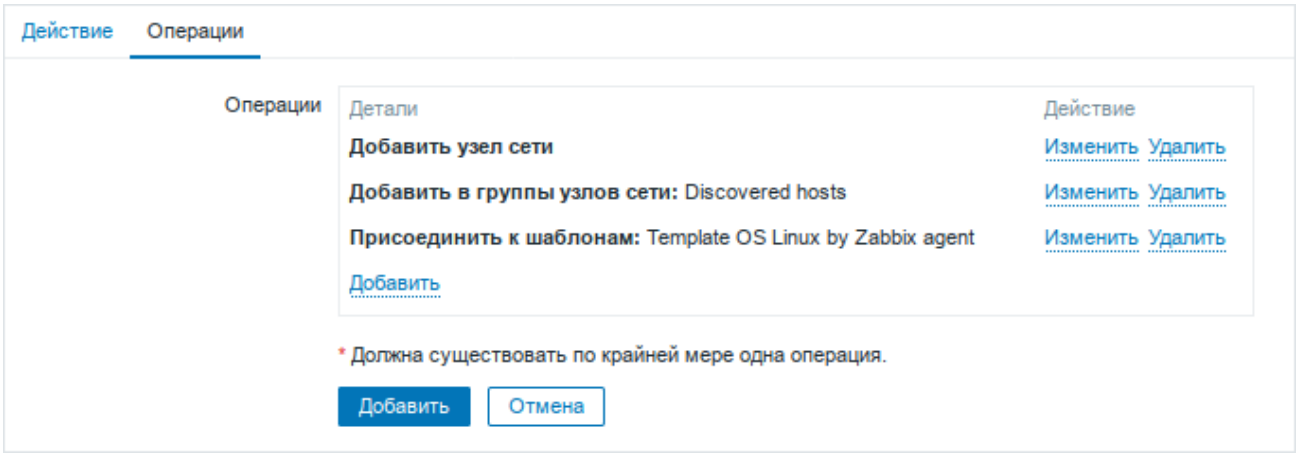


Рис. 125

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.

6.8 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 ОС «Альт Сервер».

6.8.1 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.

6.8.2 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)».

Примечание. В примере ниже указан DNS адрес сервера jitsi2.test.alt, следует заменить его на свой.

6.8.3 Конфигурация

6.8.3.1 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
```

```
[...]
```

6.8.3.2 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" -- 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
```

6.8.3.3 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"
```

Примечание. 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.

6.8.3.4 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.properti
es
```

```
-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"
                }
            }
        }
    }
}
```

Примечание. 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.jitsi2.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.

6.8.3.5 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 ОС «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+SH
A256:EECDH+ECDSA+SHA384:EECDH+ECDSA+SHA256:EECDH+aRSA+SHA384:EDH+aRSA+
AESGCM:EDH+aRSA+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
# 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
```

6.8.4 Работа с сервисом

Для общения достаточно запустить веб-браузер и перейти на сайт. В нашем примере сервис доступен по адресу: https://jitsi2.test.alt (Рис. 126).

Главная страница jitsi-meet

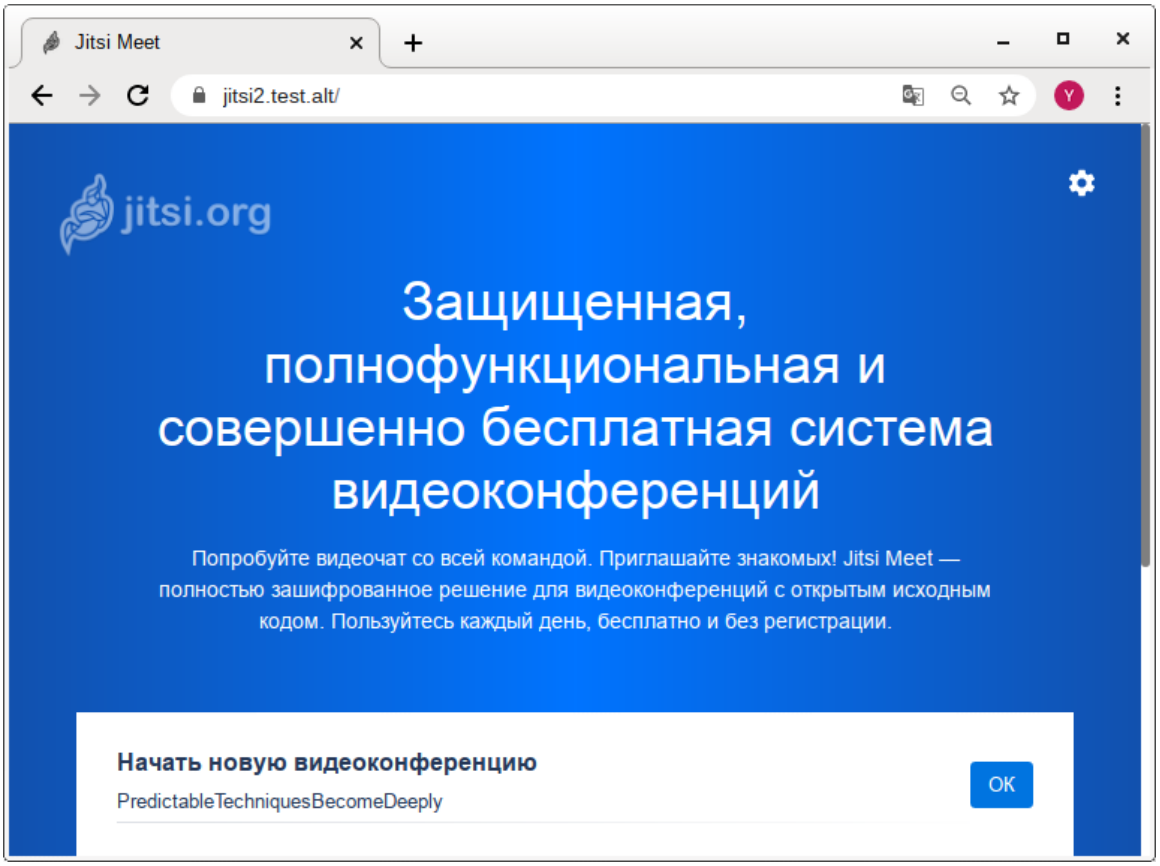


Рис. 126

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.

Ввести название конференции и нажать кнопку ОК. Будет создана конференция (Рис. 127).

Конференция jitsi-meet

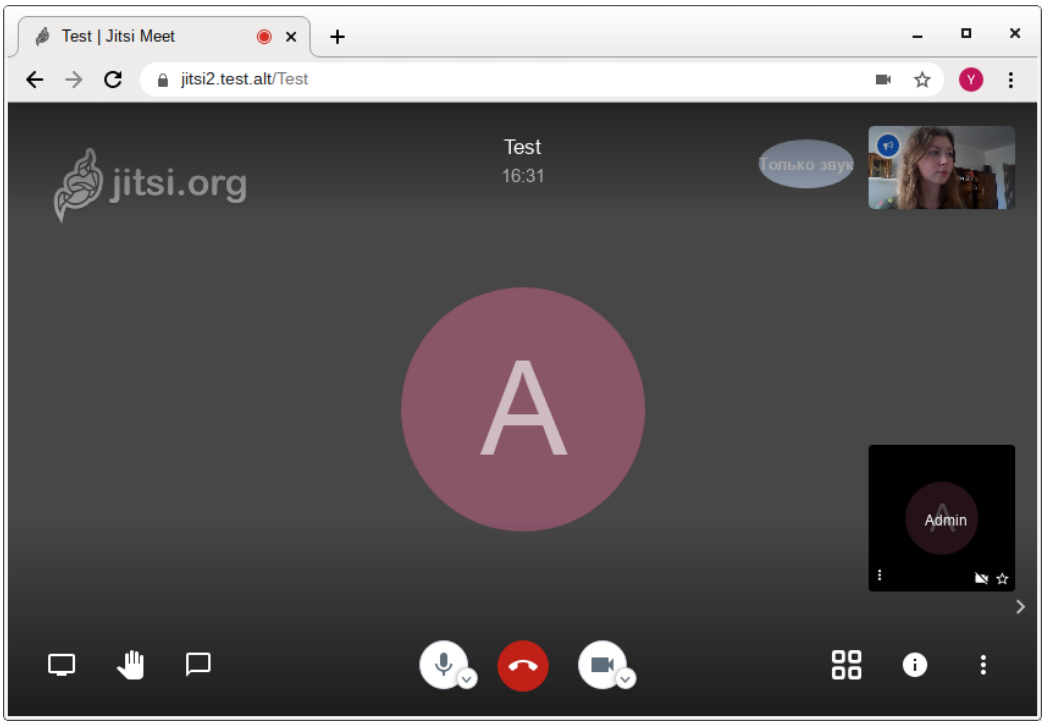


Рис. 127

Примечание. После создания конференции браузер попросит дать ему разрешение на использование веб-камеры и микрофона (Рис. 128).

Запрос на использование веб-камеры и микрофона

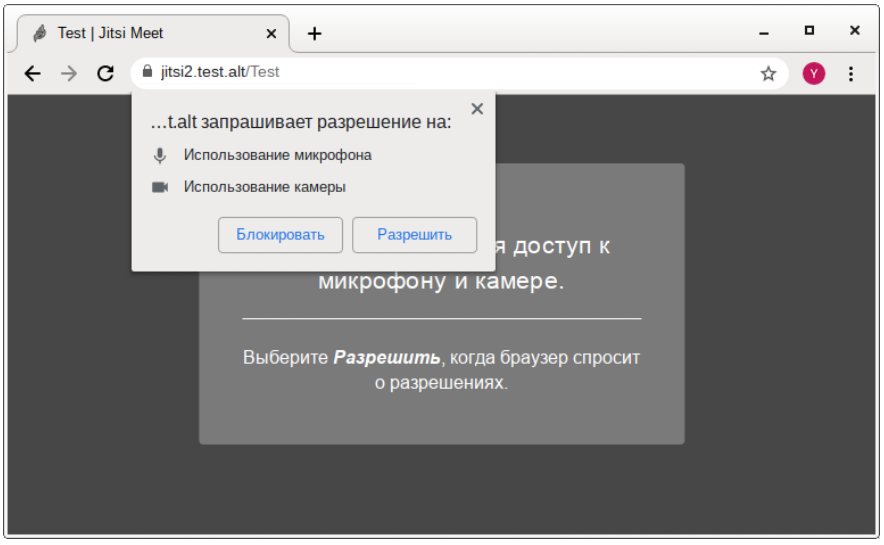


Рис. 128

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 (Рис. 129).

Панель управления jitsi-meet

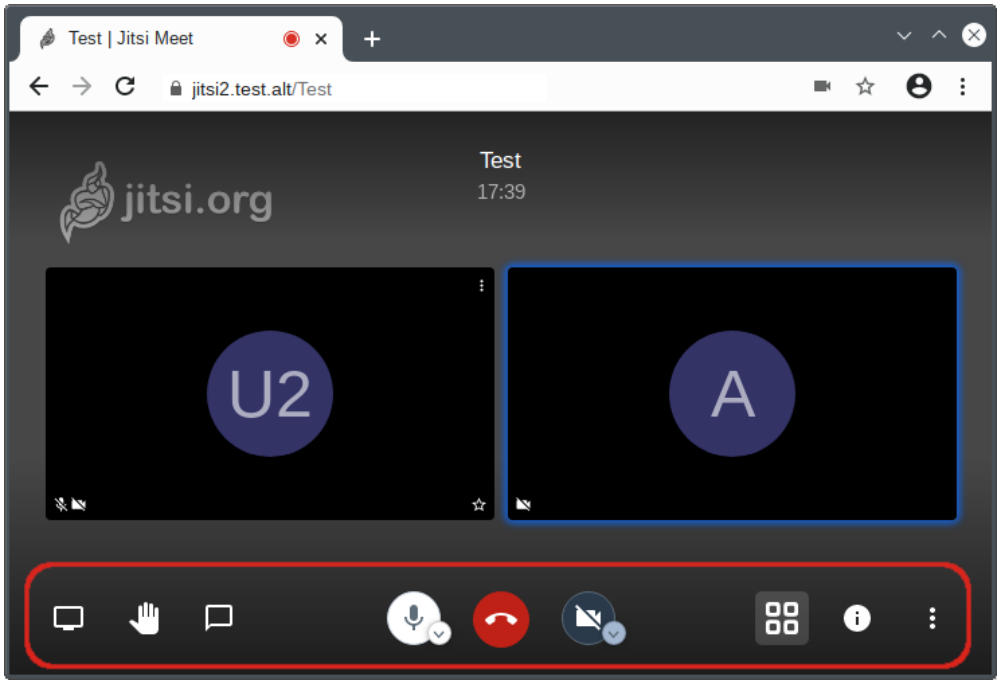


Рис. 129

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 (Рис. 130):

– 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 (Рис. 131).

Выбор окна экрана

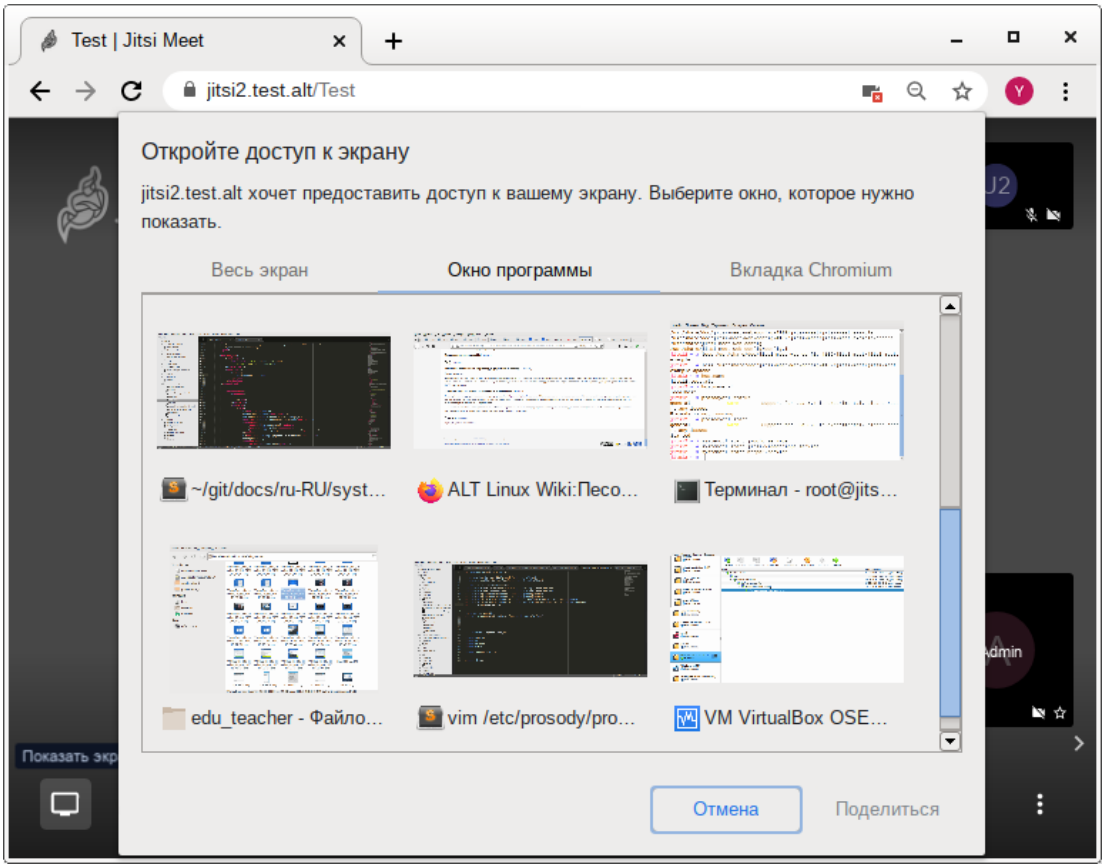


Рис. 130

Чат конференции jitsi-meet

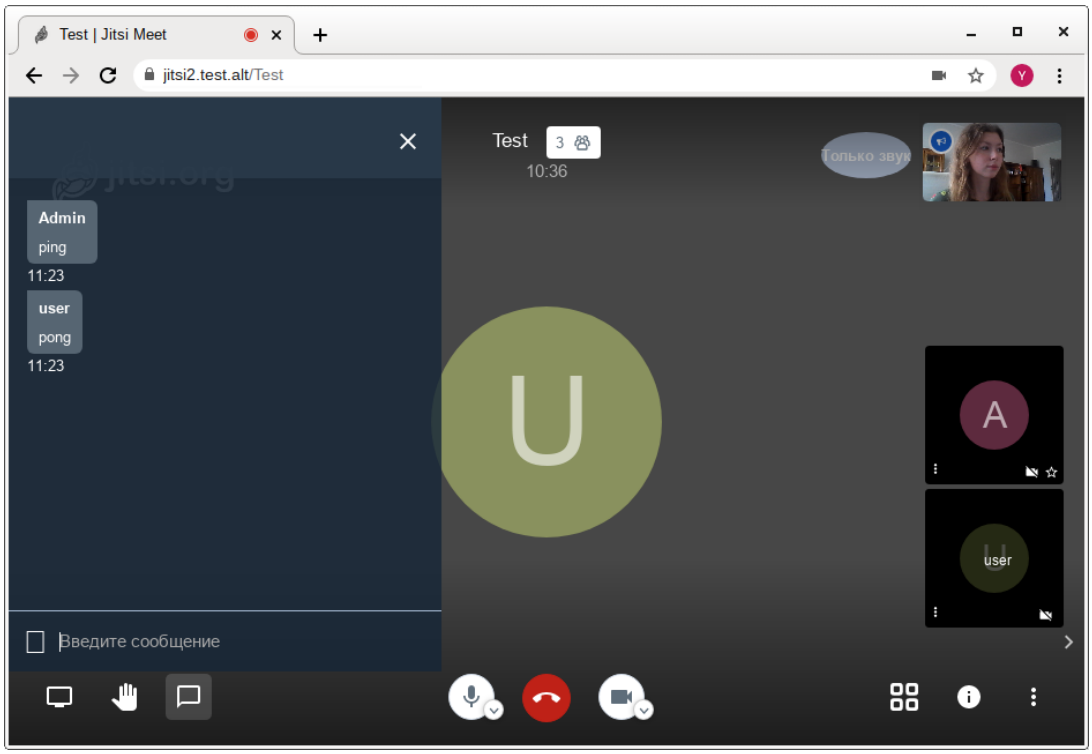


Рис. 131

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 (Рис. 132);
– «Больше» – настройка дополнительных функций Jitsi Meet (Рис. 133).

Установка пароля для доступа к конференции

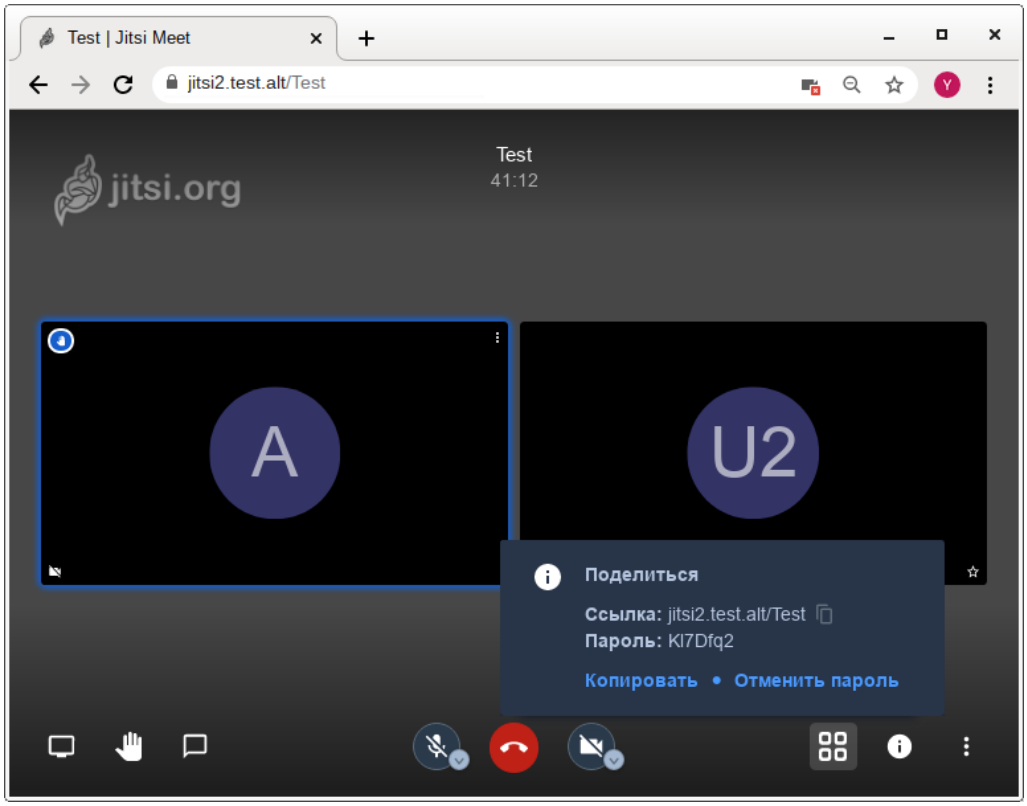


Рис. 132

Установка дополнительных функций Jitsi Meet

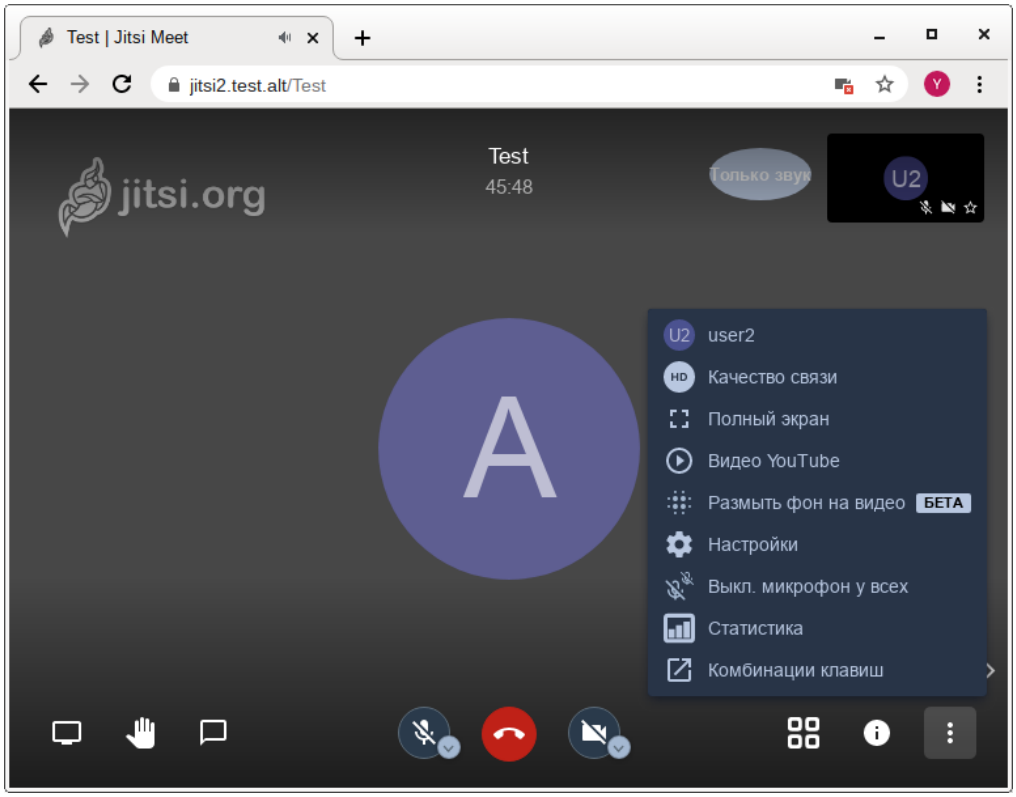


Рис. 133

6.8.5 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 (Рис. 134).

Запрос пароля при создании конференции

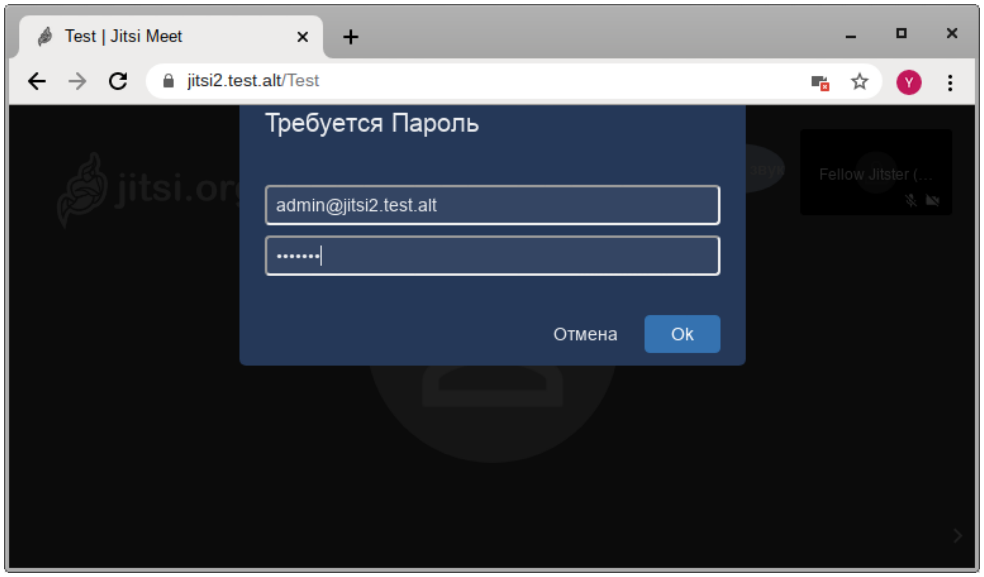


Рис. 134

6.9 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, про-

вайдера 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).

6.9.1 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.

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 ipa
```

6.9.1.1 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
```

6.9.1.2 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 и активировать новый ключ SSH без пароля:

```
# ssh-keygen -t ed25519 -f ~/.ssh/id_ed25519 -N ""
```

Примечание. Незащищенные ключи SSH (без пароля) не рекомендуются для серверов, открытых для внешнего мира.

Скопировать публичную часть SSH-ключа на другие узлы 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
```

Убедиться, что теперь можно запускать команды удалённо, без пароля:

```
# ssh node02 -- uname -n
node02
```

6.9.2 Установка кластерного ПО и создание кластера

Для управления кластером Pacemaker можно использовать утилиты `pcs` (пакет pcs) или `crm` (пакет crmsh).

Установить на всех узлах необходимые пакеты:

```
# apt-get install corosync resource-agents pacemaker pcs
```

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*
```

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 (команда выполняется 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`) (Рис. 135).

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 (Рис. 136).

Аутентификация в веб-интерфейсе управления кластером

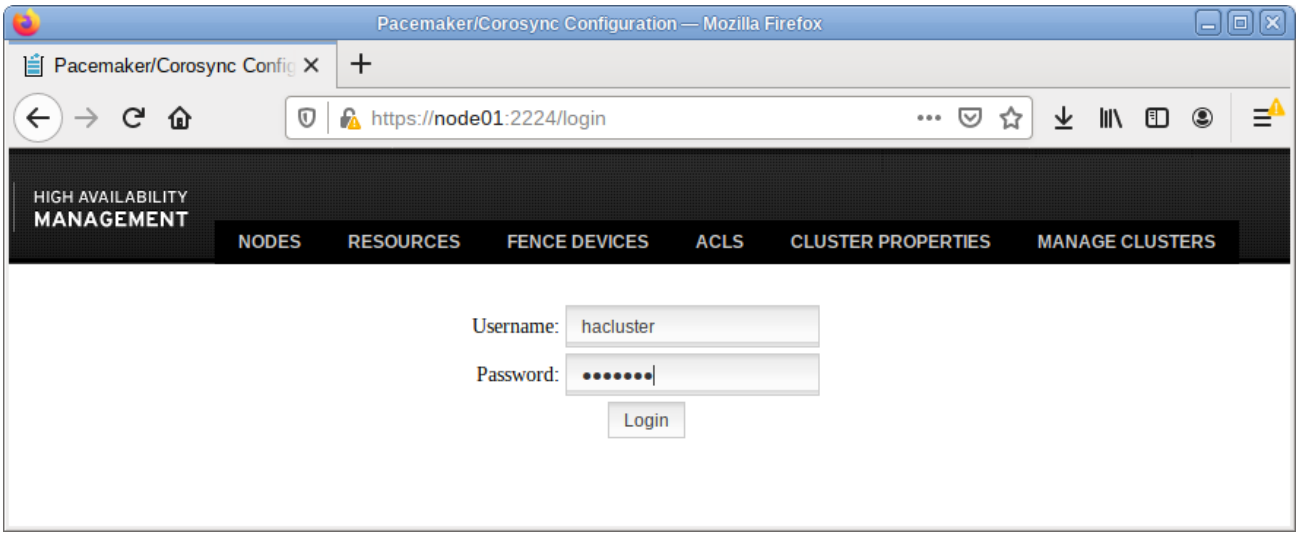


Рис. 135

Веб-интерфейс управления кластером

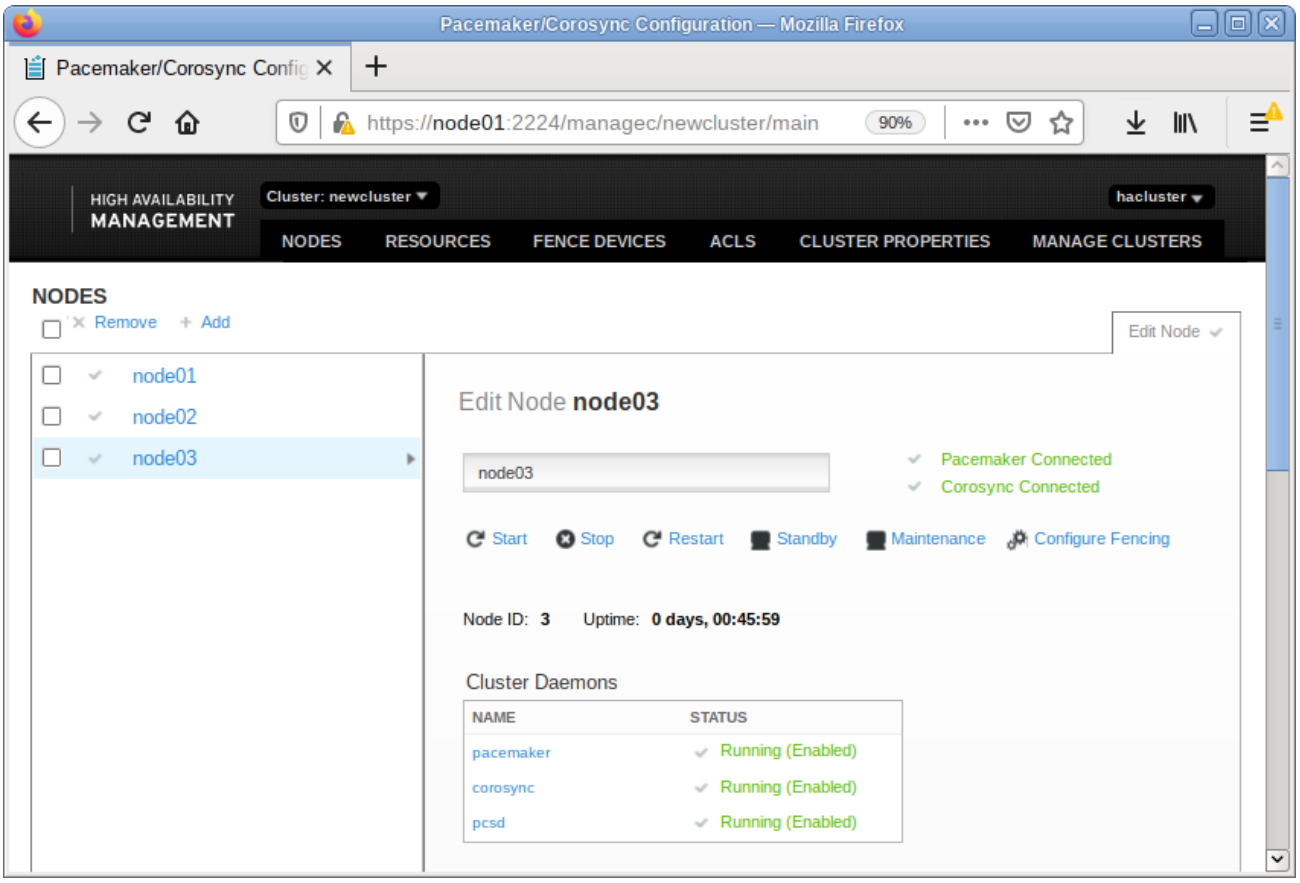


Рис. 136

Чтобы добавить существующий кластер в веб-интерфейс, необходимо нажать кнопку «Add Existing» (Рис. 137), и в открывшемся окне ввести имя или IP-адрес любого узла в кластере (Рис. 138).

Pacemaker. Кнопка «Add Existing»

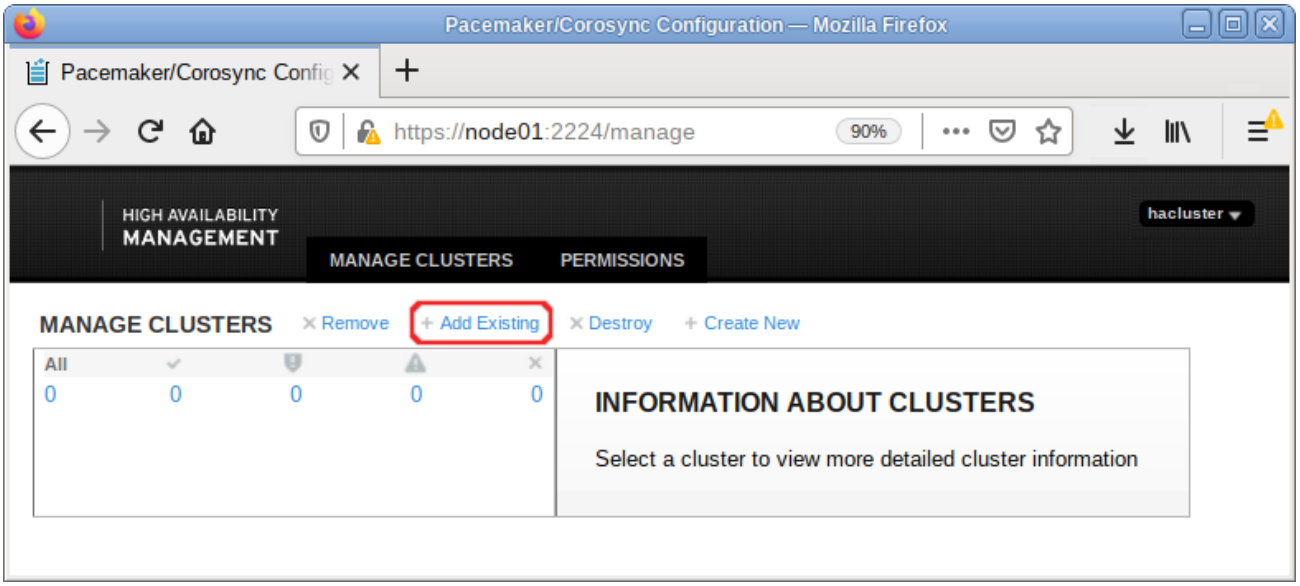


Рис. 137

Добавление кластера в веб-интерфейс

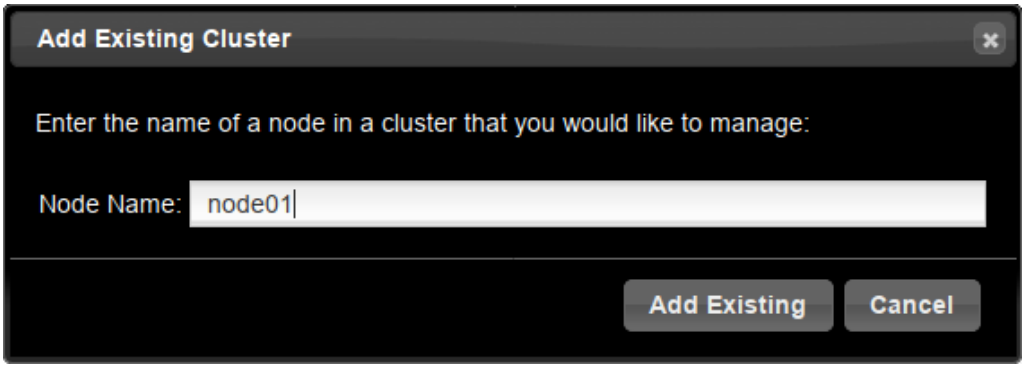


Рис. 138

6.9.3 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
```

6.9.3.1 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
```

6.9.3.2 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
```

Примечание. 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.

6.9.4 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
```

Для того чтобы добавить ресурс в веб-интерфейсе, необходимо перейти на вкладку «RESOURCES», нажать кнопку «Add» и задать параметры ресурса (Рис. 139).

Список доступных стандартов ресурсов:

```
# pcs resource standards
lsb
ocf
service
systemd
```

Список доступных поставщиков сценариев ресурсов OCF:

```
# pcs resource providers
heartbeat
```

```
pacemaker
redhat
```

Создание ресурса виртуального IP-адреса

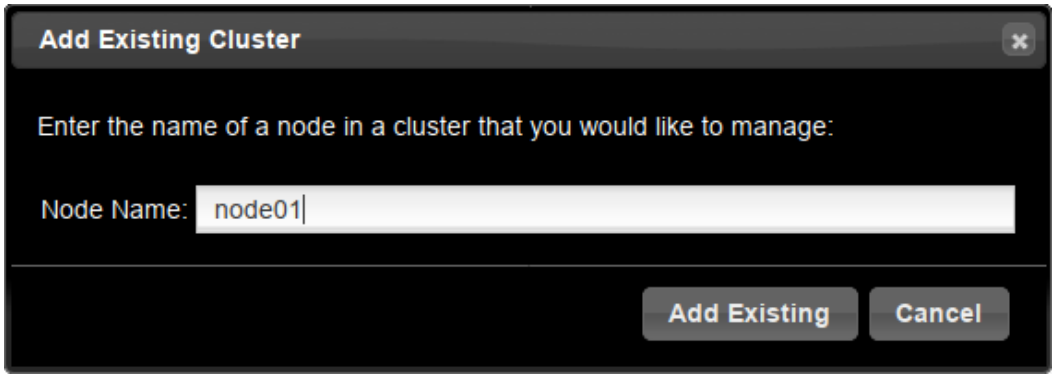


Рис. 139

Список всех агентов ресурсов, доступных для определённого поставщика OCF:

```
# pcs resource agents ocf:heartbeat
aliyun-vpc-move-ip
anything
AoEtarget
apache
…
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
```

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
```

6.10 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.

6.10.1 Установка

6.10.1.1 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;
```

6.10.1.2 Установка OpenUDS Server

OpenUDS Server можно установить при установке системы, выбрав для установки пункт «Сервер виртуальных рабочих столов OpenUDS».

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 (Рис. 140) будет доступен по адресу https://адрес-сервера/:

Форма входа в интерфейс OpenUDS

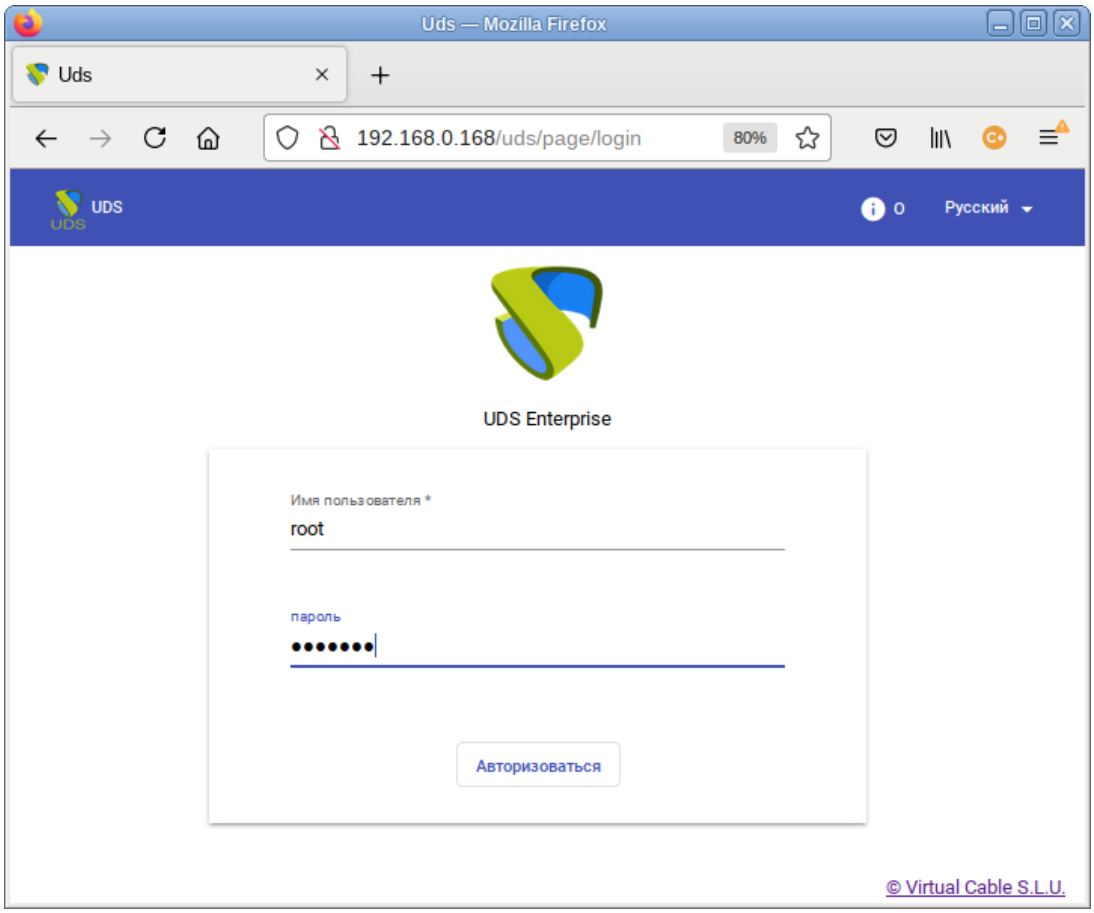


Рис. 140

Примечание. Имя/пароль по умолчанию: root/udsmam0.

Примечание. Для получения доступа к панели администрирования OpenUDS, следует в меню пользователя выбрать пункт «Панель управления» (Рис. 141).

OpenUDS. Меню пользователя

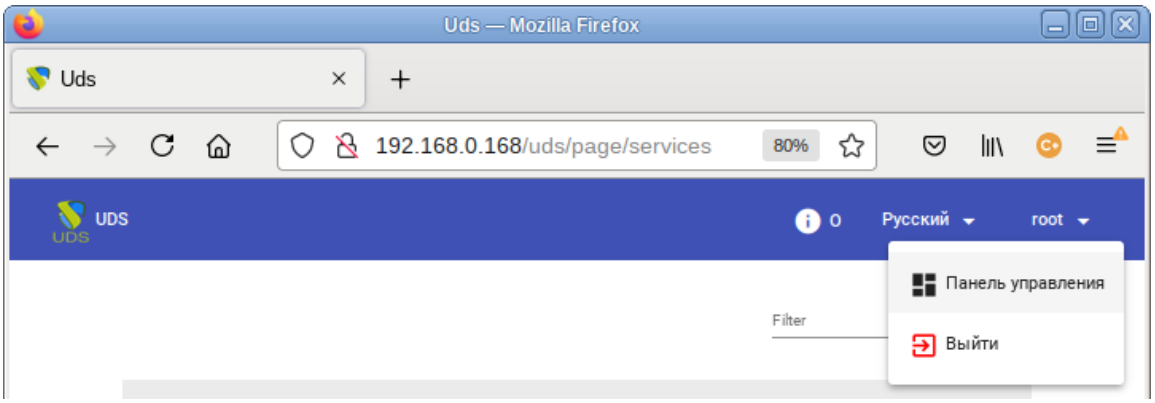


Рис. 141

6.10.2 Настройка OpenUDS

6.10.2.1 Поставщики услуг

В разделе «Услуги» («Services») (Рис. 142) 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»).

OpenUDS. Поставщики услуг

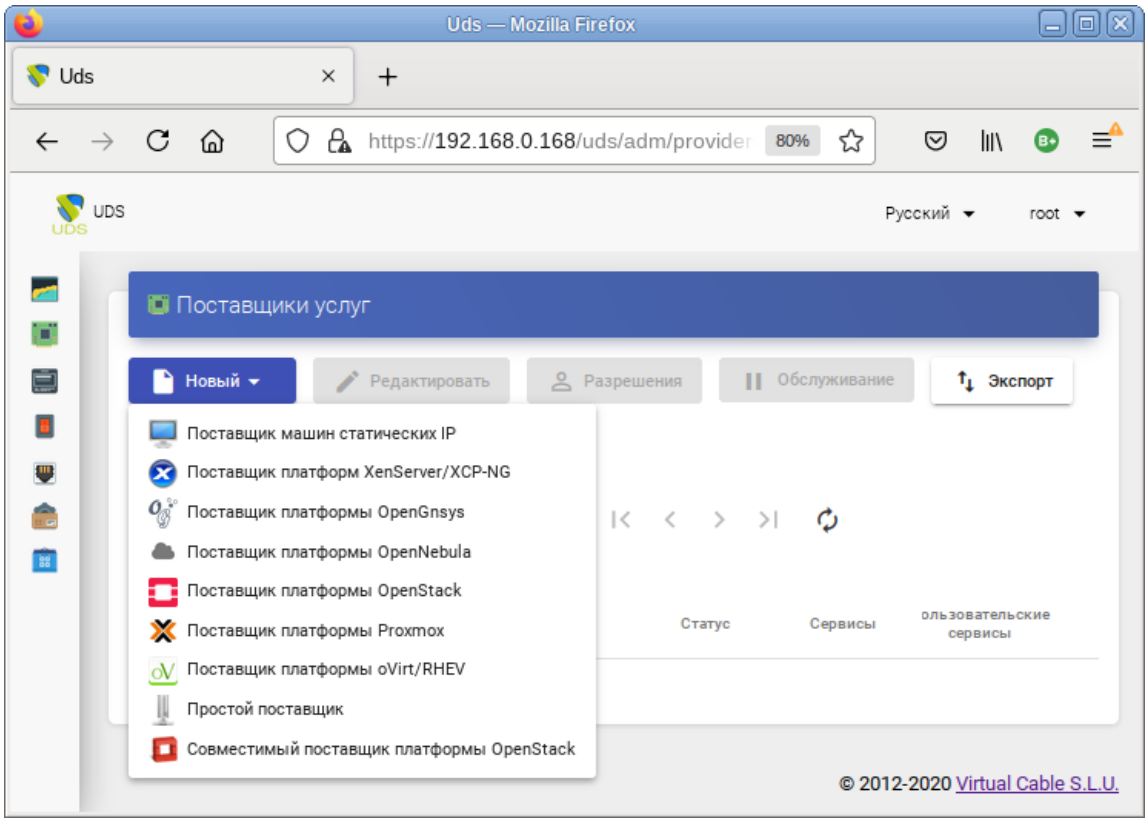


Рис. 142

6.10.2.1.1 OpenNebula

Минимальные параметры для настройки «Поставщик платформы OpenNebula» (Рис. 143): название, IP-адрес сервера OpenNebula (поле «Хост»), порт подключения, имя пользователя (с правами администратора) и пароль.

OpenUDS. Подключение системы виртуализации OpenNebula

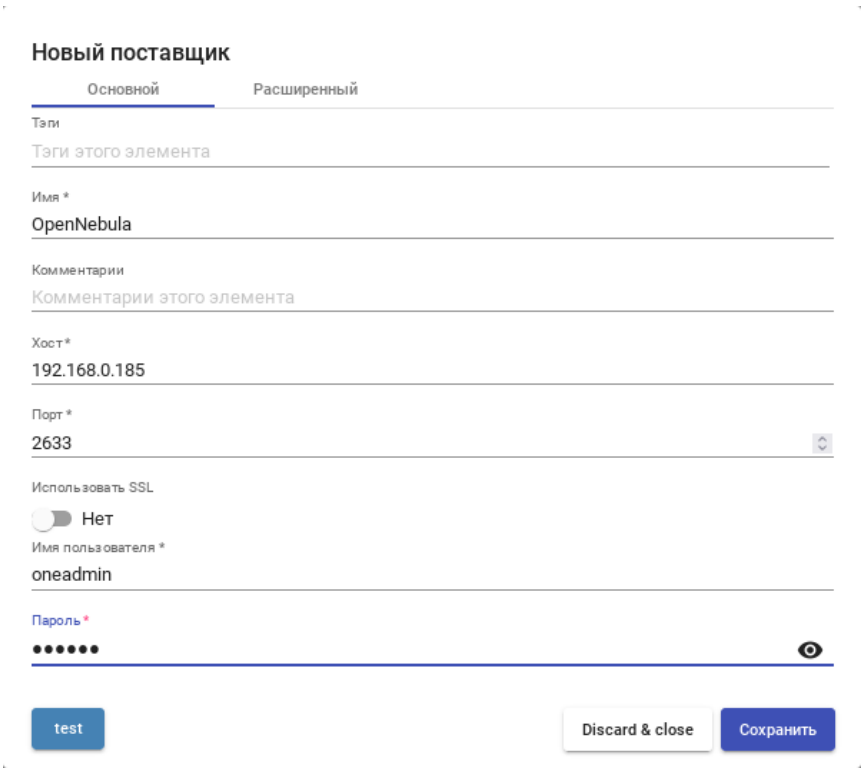


Рис. 143

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») (Рис. 144).

OpenUDS. Контекстное меню «Service providers»

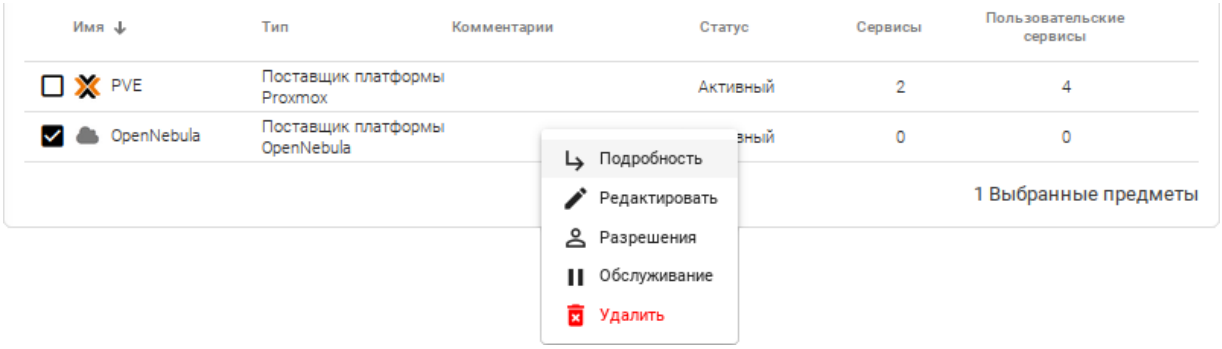


Рис. 144

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» (Рис. 145).

OpenUDS. Создание новой услуги «Действующие образы OpenNebula»

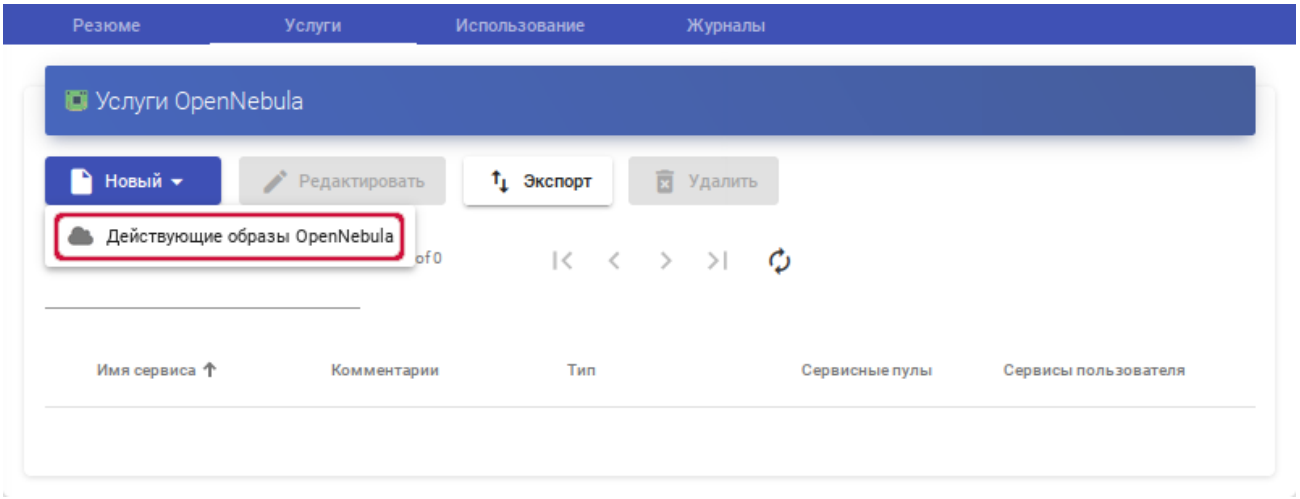


Рис. 145

Заполнить минимальные параметры конфигурации.

Вкладка «Основной» («Main») (Рис. 146):

– «Имя» – название службы;
– «Хранилище» – место, где будут храниться сгенерированные виртуальные рабочие столы.

OpenUDS. Создание службы типа «OpenNebula Live Images». Вкладка «Основной»

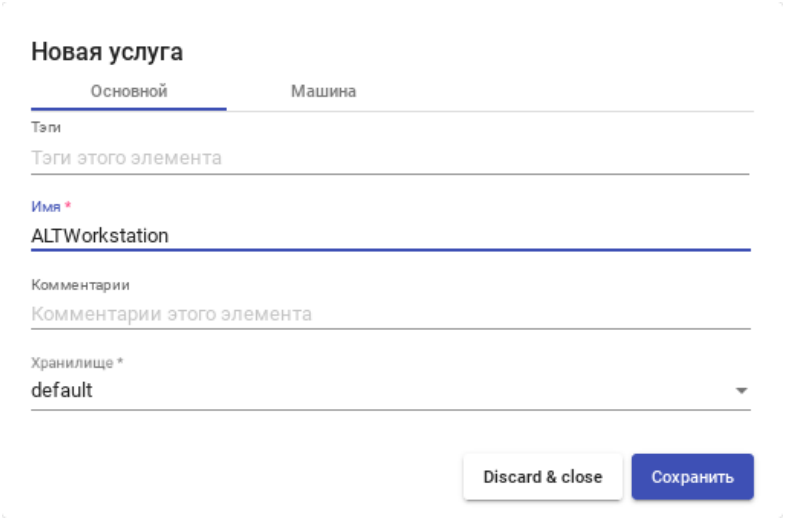


Рис. 146

Вкладка «Машина» («Machine») (Рис. 147):

- «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).

OpenUDS. Создание службы типа «OpenNebula Live Images». Вкладка «Machine»

Рис. 147

6.10.2.1.2 PVE

Минимальные параметры для настройки «Поставщика платформы Proxmox» (Рис. 148): 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» (Рис. 149).

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.

OpenUDS. Подключение системы виртуализации PVE

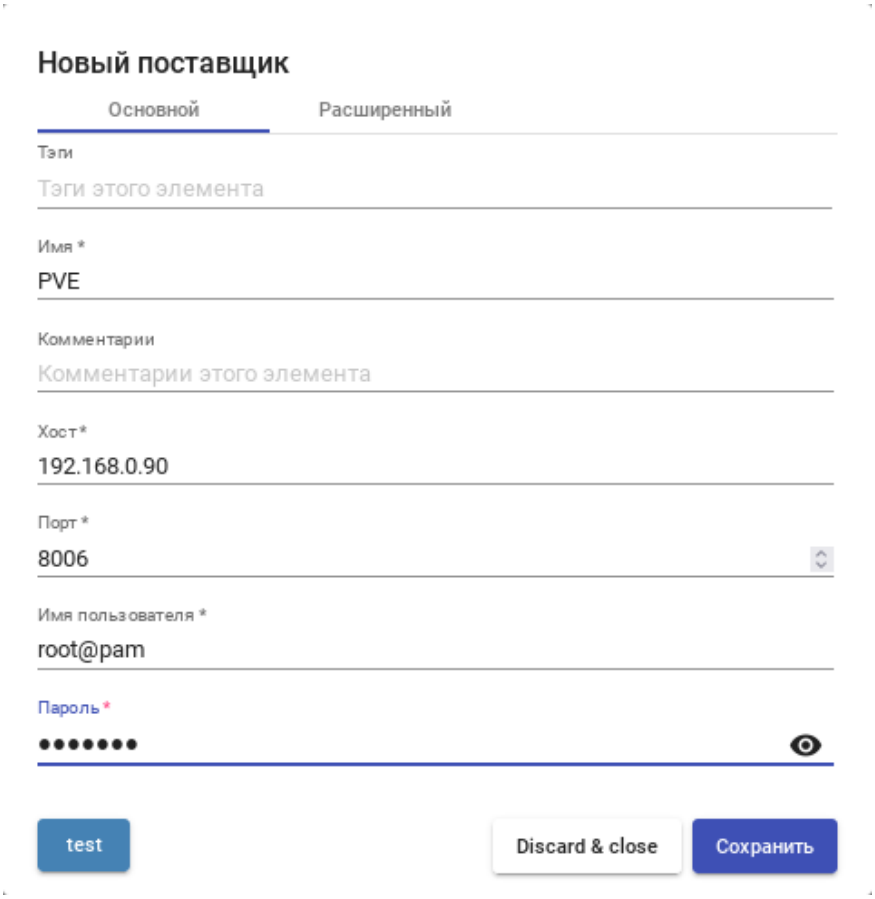


Рис. 148

OpenUDS. Контекстное меню поставщика услуг PVE

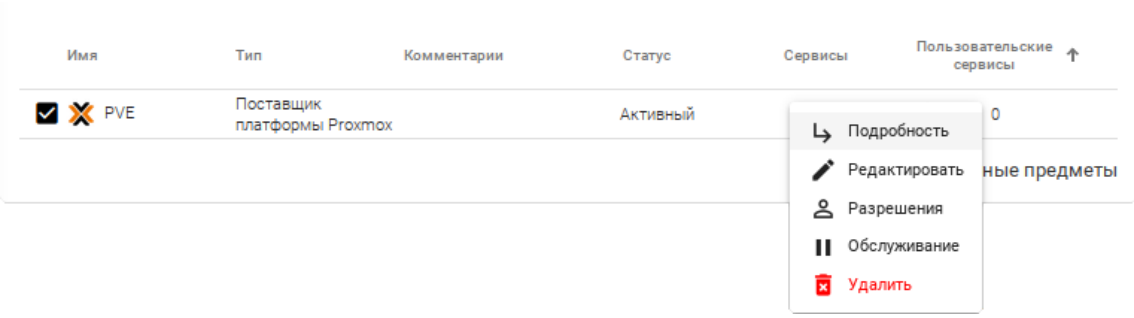


Рис. 149

На вкладке «Услуги» («Services») нажать кнопку «Новый» → «Связанный клон Proxmox» (Рис. 150).

OpenUDS. Создание новой услуги «Связанный клон Proxmox»

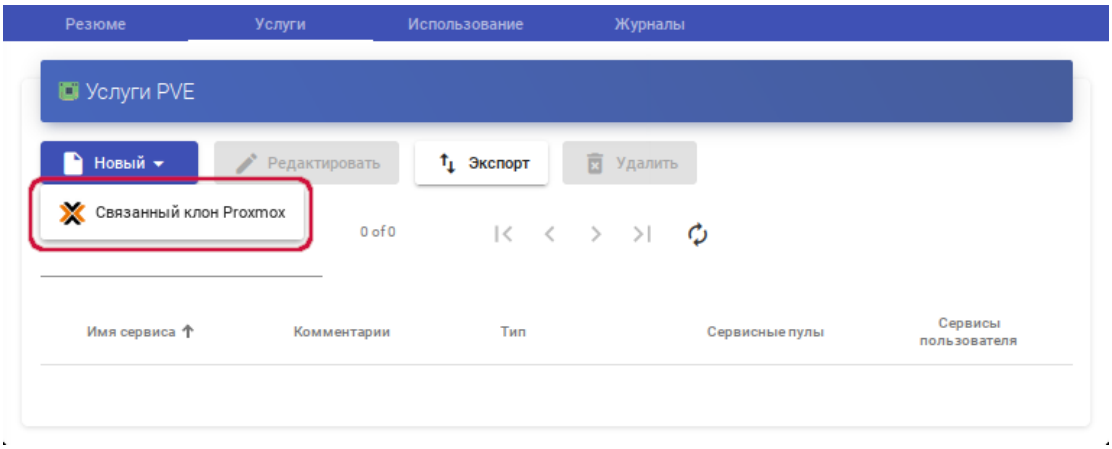


Рис. 150

Заполнить параметры конфигурации.

Вкладка «Основной» («Main») (Рис. 151):

– «Имя» – название службы;
– «Пул» – пул, в котором будут находиться ВМ, созданные OpenUDS;
– «Высокая доступность» – включать созданные ВМ в группу HA PVE.

OpenUDS. Создание службы типа «Proxmox Linked Clone». Вкладка «Main»

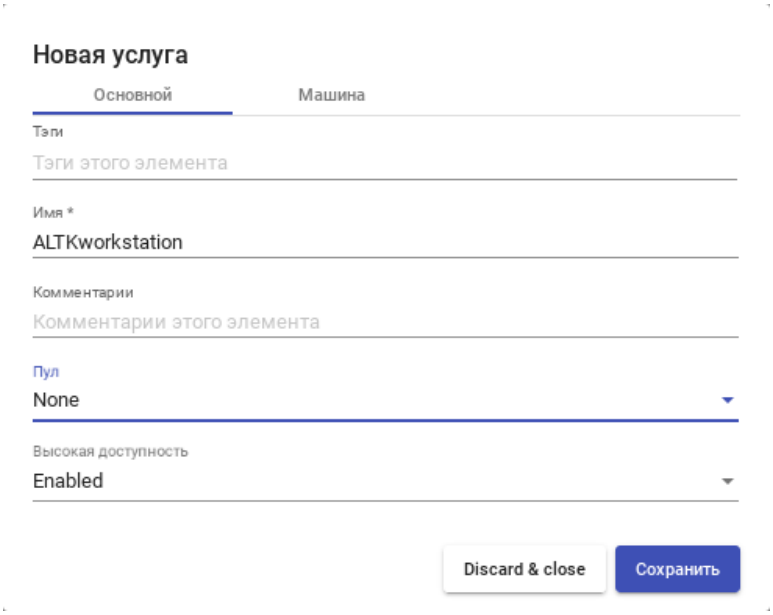


Рис. 151

Вкладка «Машина» («Machine») (Рис. 152):

– «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).

OpenUDS. Создание службы типа «Proxmox Linked Clone». Вкладка «Машина»

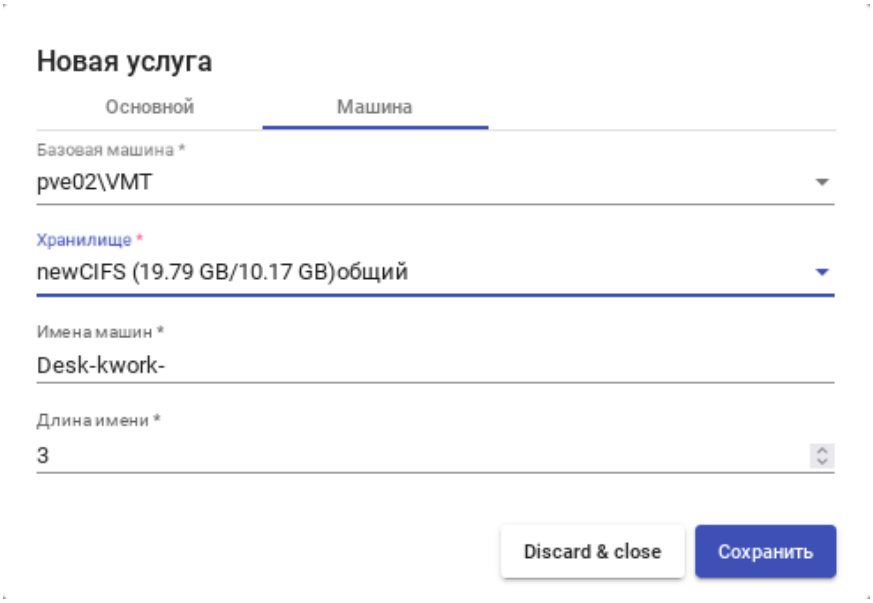


Рис. 152

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») (Рис. 153).

PVE. Созданные шаблоны и рабочие столы

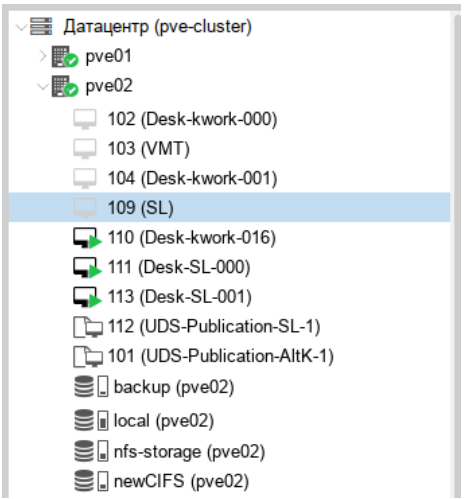


Рис. 153

6.10.2.1.3 Удаленный 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 (Рис. 154).

OpenUDS. Подключение к серверу без виртуализации

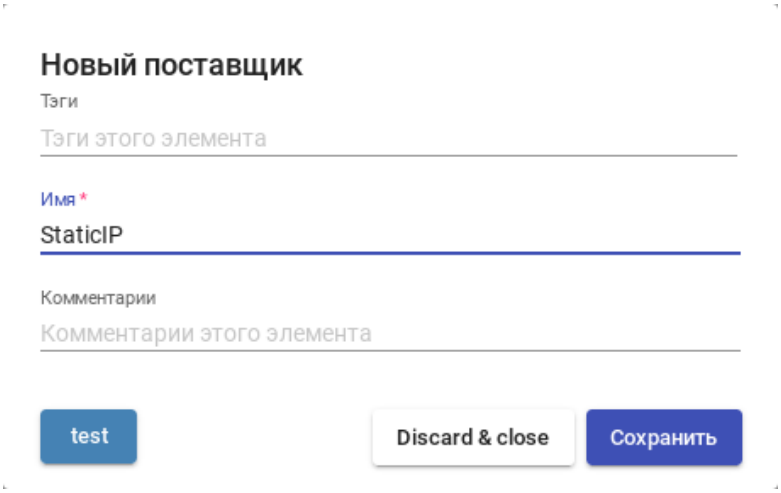


Рис. 154

Для создания базовых сервисов «Поставщика машин статических IP» следует дважды щелкнуть мышью по строке созданного поставщика услуг 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 (Рис. 155).

– «Статический одиночный IP-адрес» – используется для подключения нескольких пользователей к одному компьютеру. При обращении каждого нового пользователя будет запускаться новый сеанс.

OpenUDS. Привязка пользователю устройству

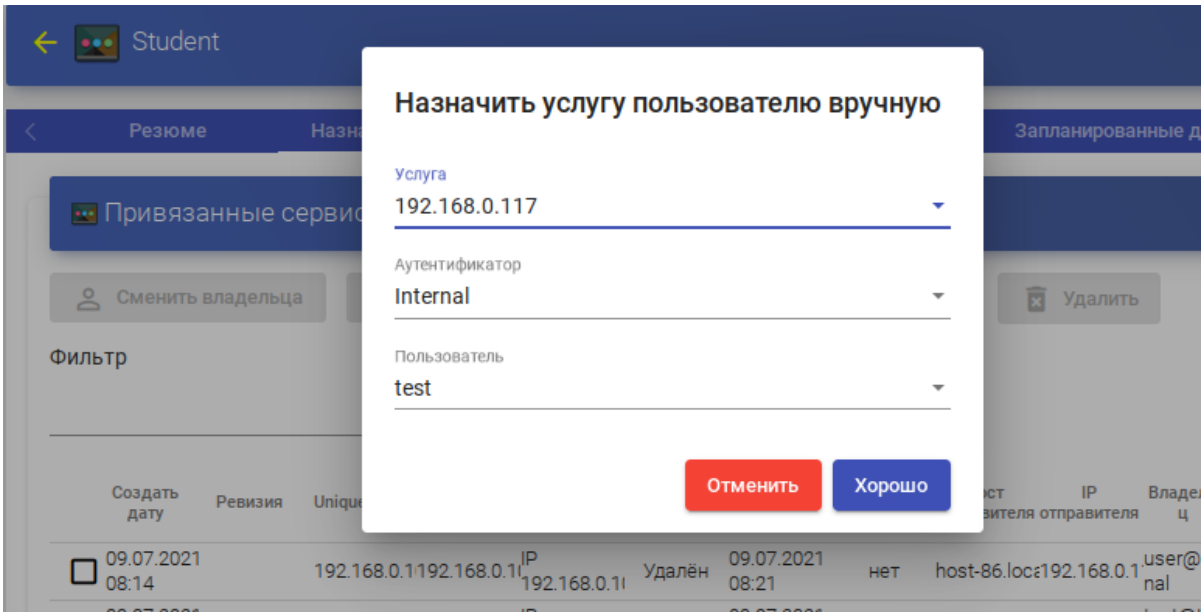


Рис. 155

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» (Рис. 156).

OpenUDS. Создание новой услуги «Статический IP-адрес»

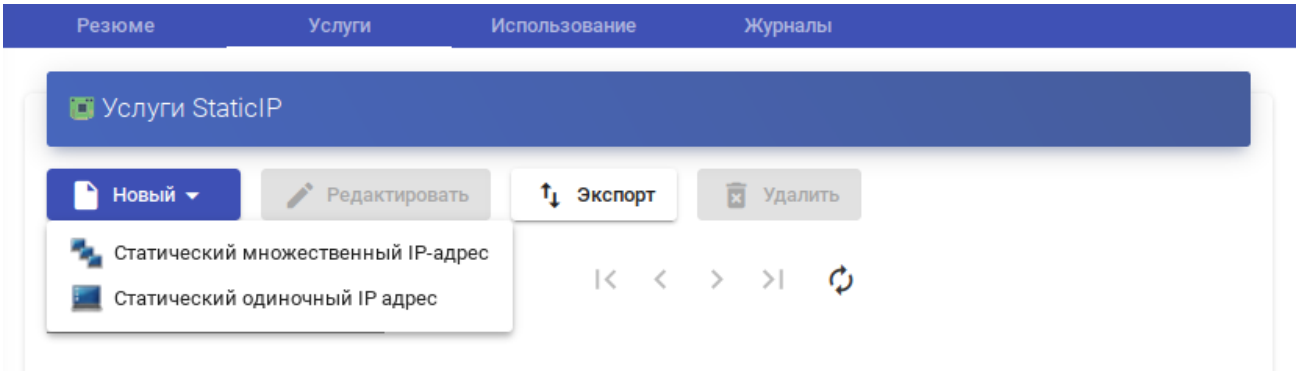


Рис. 156

Параметры конфигурации для услуги «Статический множественный IP-адрес» (Рис. 157):

– Вкладка «Основной» (Рис. 157):
  - «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» (Рис. 160):
  - «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.

OpenUDS. Создание службы типа «Static Multiple IP»

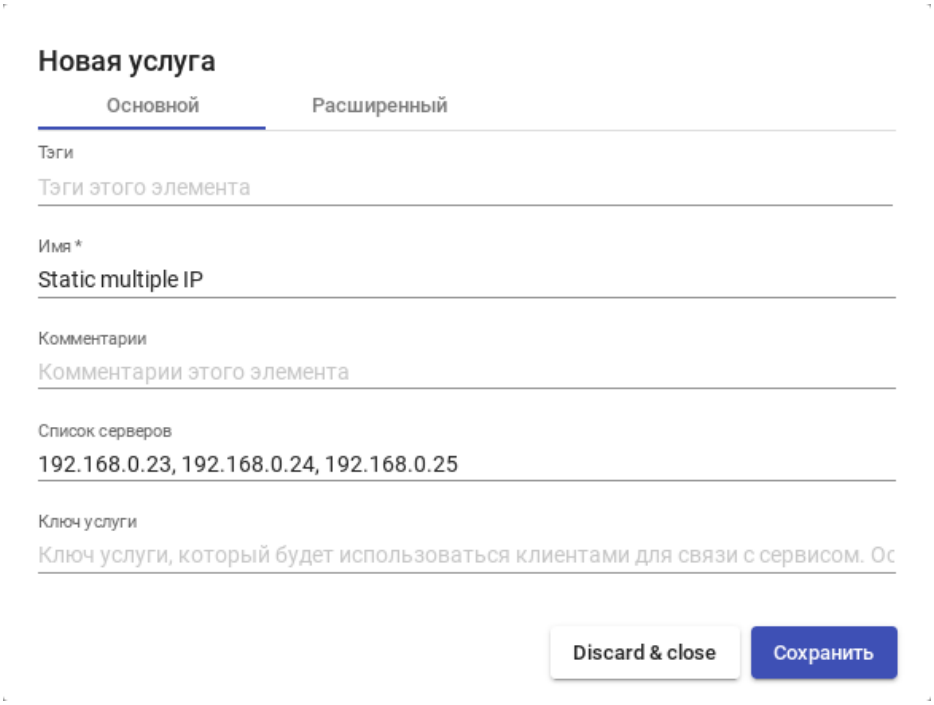


Рис. 157

OpenUDS. Создание службы типа «Static Multiple IP»

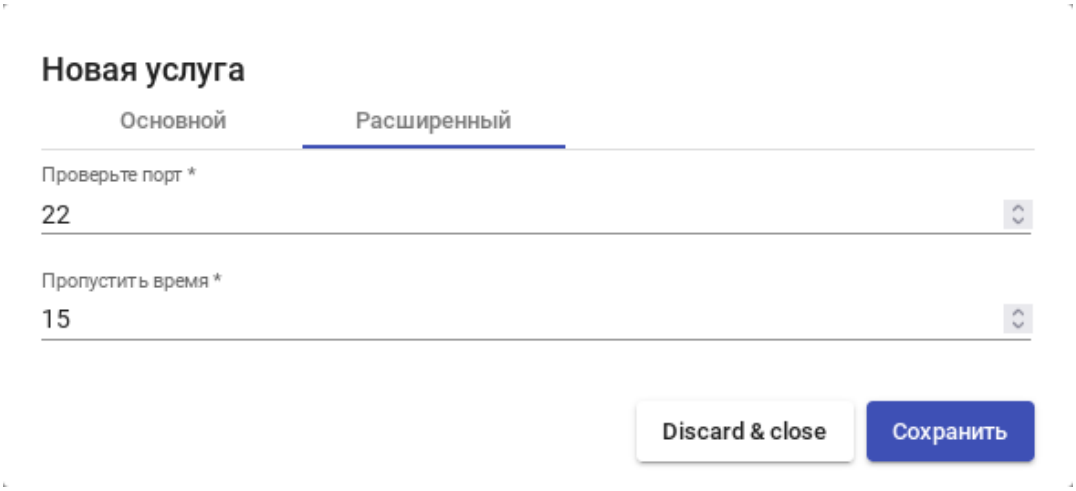


Рис. 158

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» (Рис. 159).

OpenUDS. Привязанные сервисы службы «Static Multiple IP»

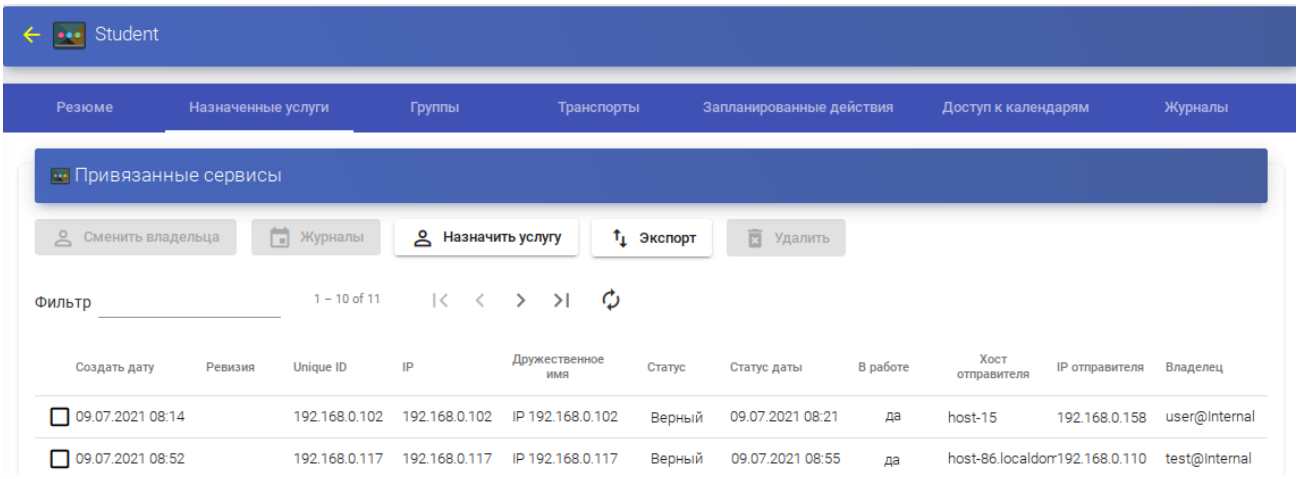


Рис. 159

Параметры конфигурации для услуги «Статический одиночный IP-адрес» (Рис. 160):

– «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»).

OpenUDS. Создание службы типа «Static Single IP»

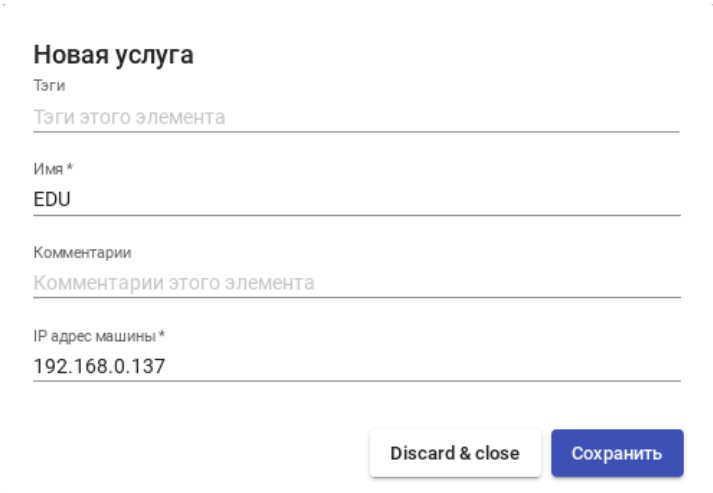


Рис. 160

6.10.2.2 Настройка аутентификации пользователей

Для настройки аутентификации в разделе «Аутентификаторы» («Autentificators») необходимо выбрать тип аутентификации пользователей (Рис. 161). Можно выбрать как внешние источники (Active Directory, OpenLDAP и т.д.), так и внутренние (внутренняя база данных, IP-аутентификация):

OpenUDS. Выбор типа аутентификации пользователей

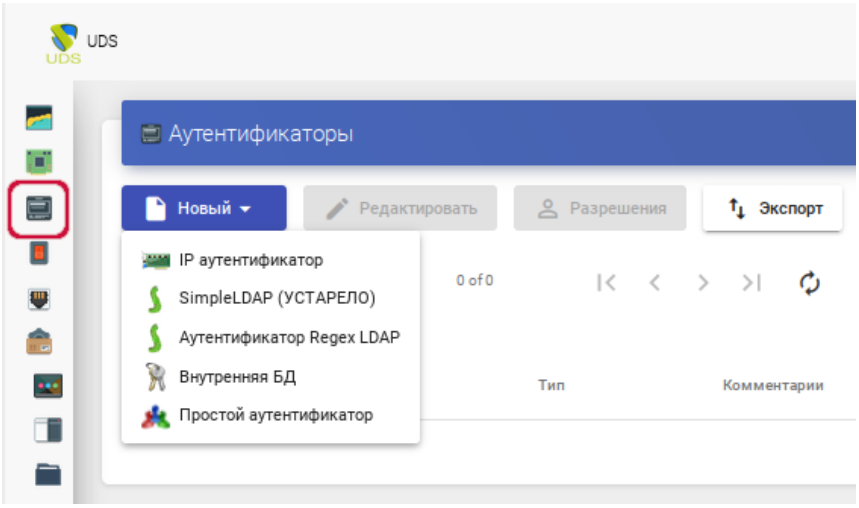


Рис. 161

6.10.2.2.1 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 (Рис. 162).

OpenUDS. Внутренняя база данных

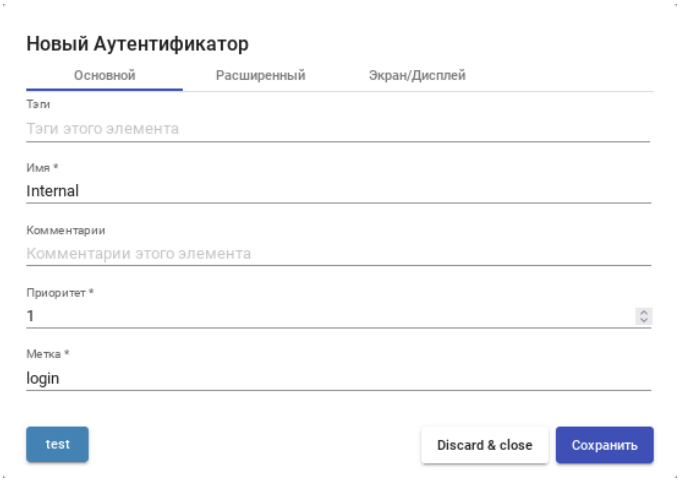


Рис. 162

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 (Рис. 163).

OpenUDS. Внутренняя база данных – пользователи

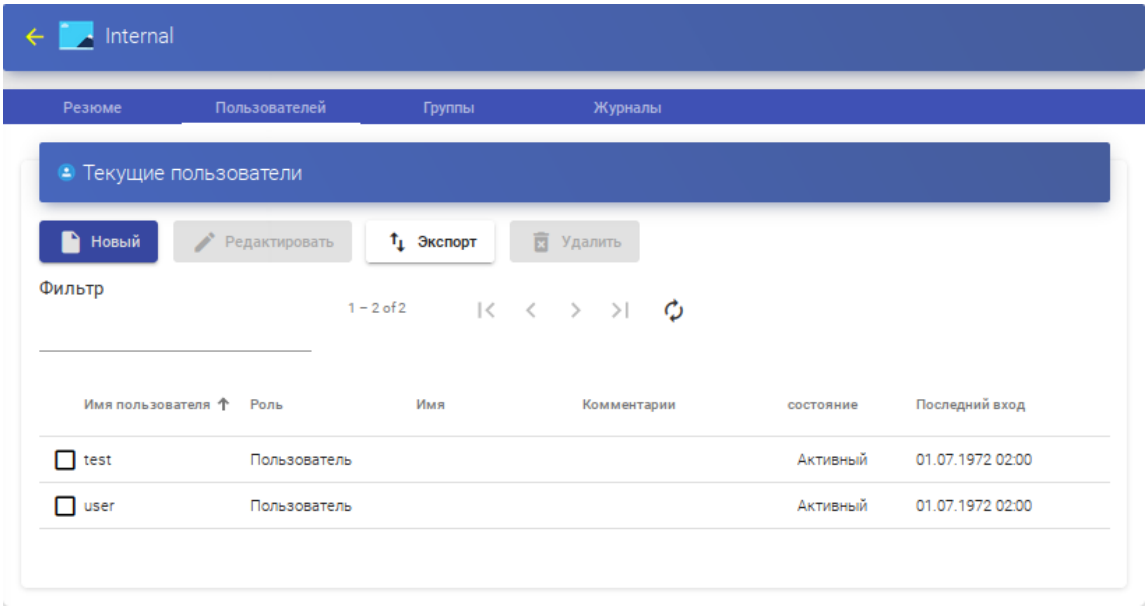


Рис. 163

6.10.2.2.2 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.

Примечание. На сервере LDAP должна быть настроена отдельная учётная запись с правами чтения LDAP. От данной учетной записи будет выполняться подключение к серверу каталогов.

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» (Рис. 164): имя аутентификатора, приоритет, метка, IP-адрес FreeIPA-сервера, порт (обычно 389 без ssl, 636 с ssl).

   Вкладка «Учётные данные» (Рис. 165): имя пользователя (в формате uid=user_freeipa,cn=users,cn=accounts,dc=example,dc=test) и пароль.

Вкладка «LDAP информация» (Рис. 167): общая база пользователей, класс пользователей LDAP, идентификатор атрибута пользователя, атрибут имени пользователя, атрибут имени группы.

OpenUDS. Интеграция с FreeIPA

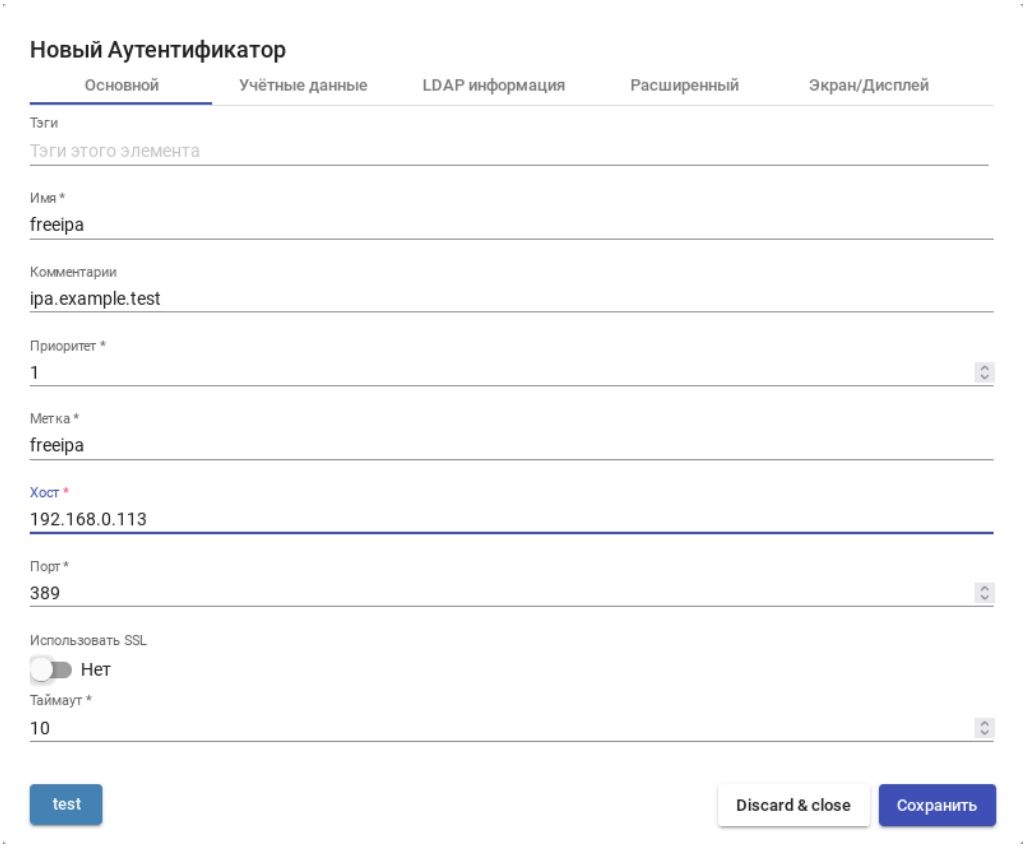


Рис. 164

OpenUDS. Интеграция с FreeIPA – учетные данные пользователя

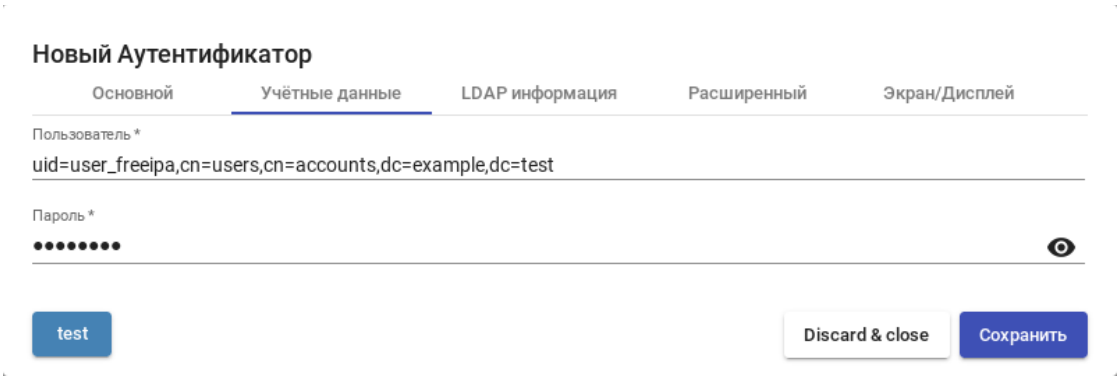


Рис. 165

OpenUDS. Интеграция с FreeIP – LDAP информация

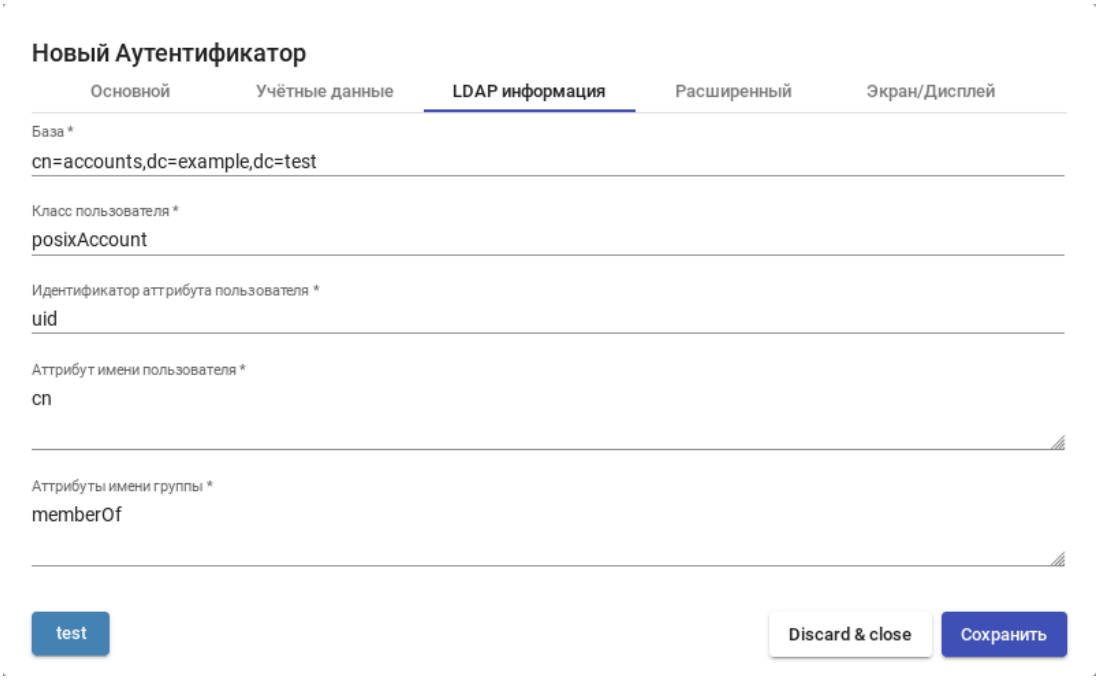


Рис. 166

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».
4. 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 (Рис. 167).

OpenUDS. Интеграция с FreeIPA – добавление группы LDAP

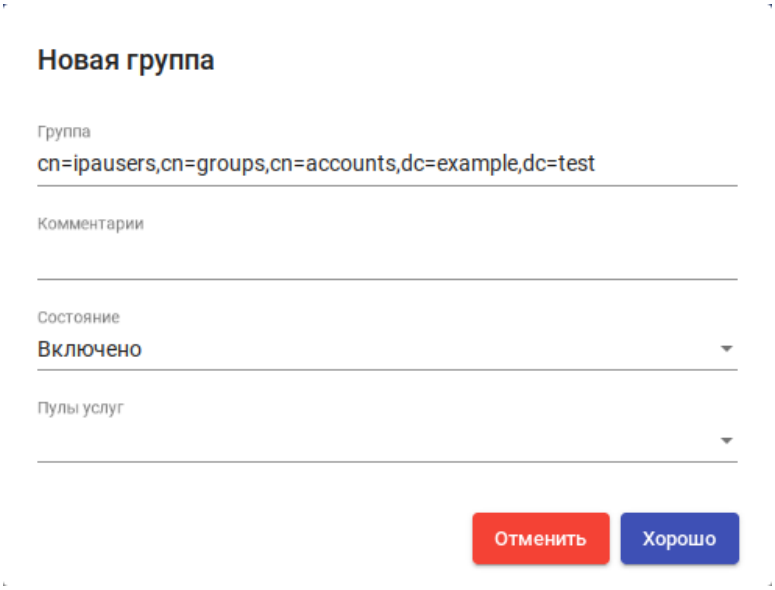


Рис. 167

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» (Рис. 168): имя аутентификатора, приоритет, метка, IP-адрес сервера AD, порт (обычно 389 без ssl, 636 с ssl).

   Вкладка «Учётные данные» (Рис. 169): имя пользователя (можно указать в виде имя@домен) и пароль.

   Вкладка «LDAP информация» (Рис. 170): общая база пользователей, класс пользователей LDAP, идентификатор атрибута пользователя, атрибут имени пользователя, атрибут имени группы.

   П р и м е ч а н и е . 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».
4. Заполнить dn существующей группы (например, cn=Users,cn=Builtin,dc=test,dc=alt), можно также указать разрешённые пулы (Рис. 171).

OpenUDS. Интеграция с Active Directory

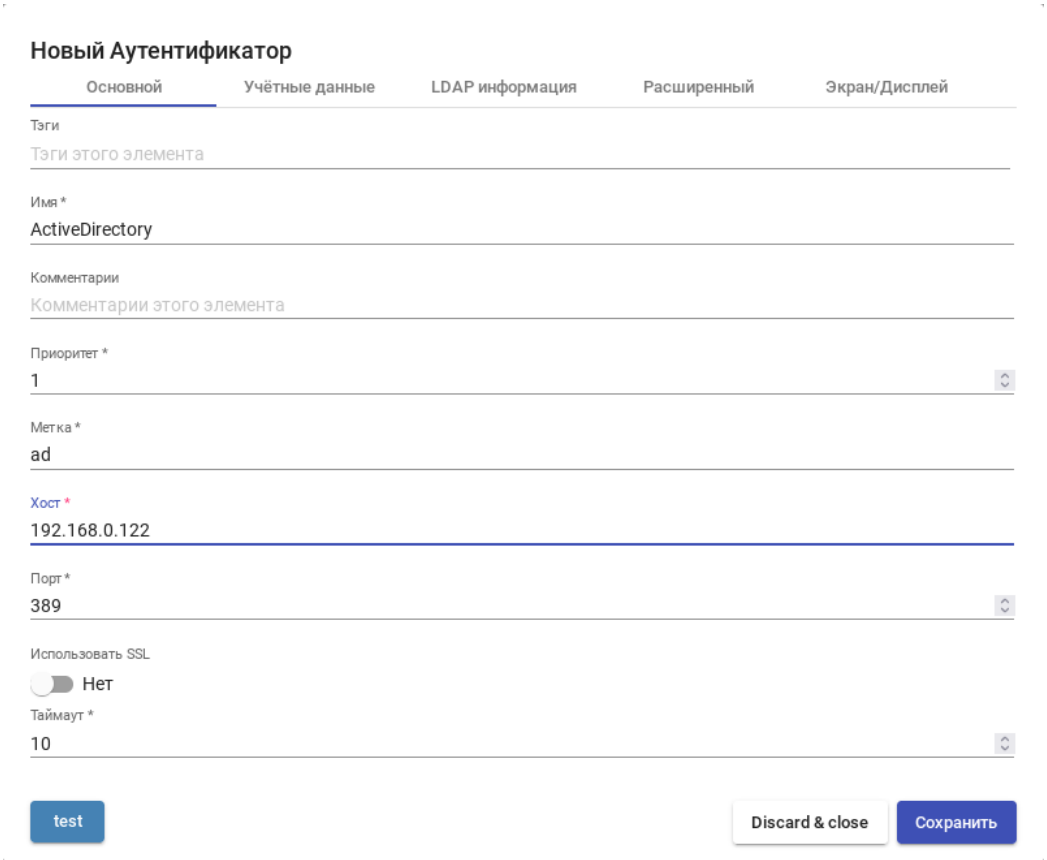


Рис. 168

OpenUDS. Интеграция с Active Directory – учетные данные пользователя

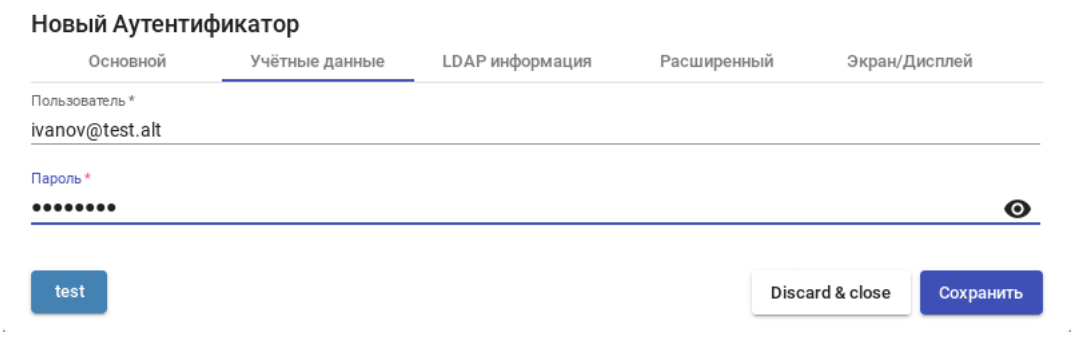


Рис. 169

OpenUDS. Интеграция с Active Directory – LDAP информация

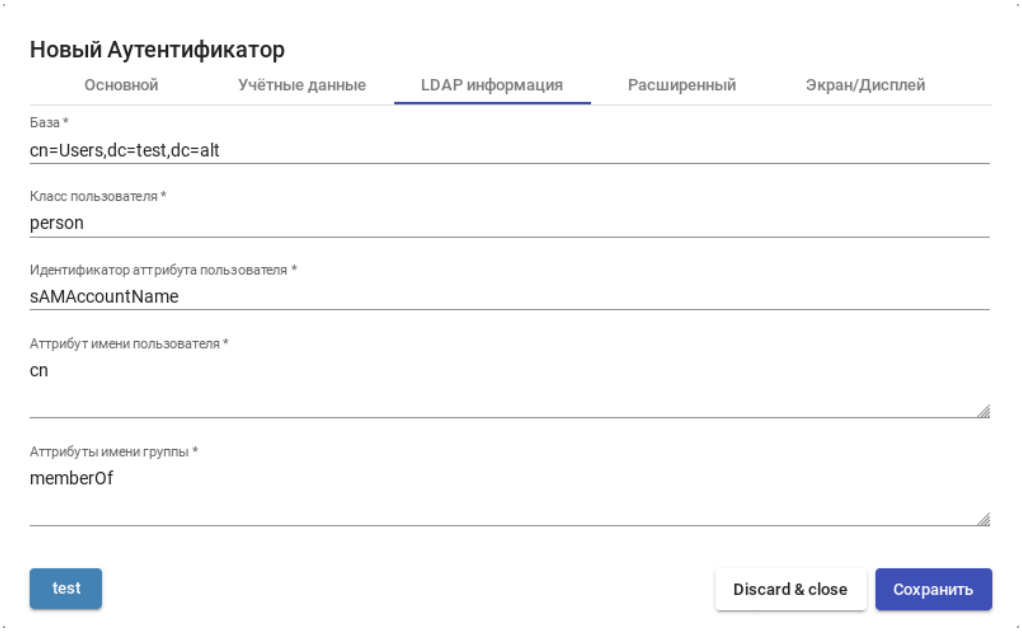


Рис. 170

OpenUDS. Интеграция с Active Directory – добавление группы LDAP

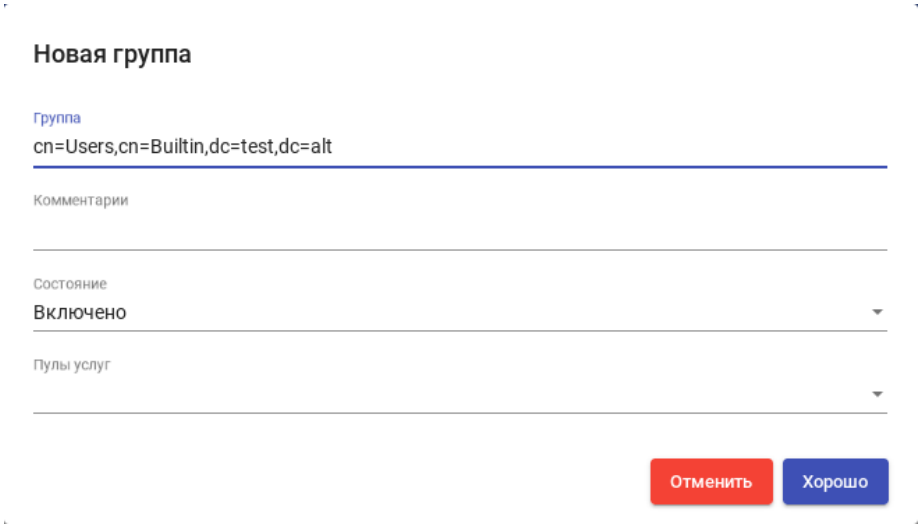


Рис. 171

6.10.2.2.3 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 (Рис. 173).

OpenUDS. IP аутентификатор

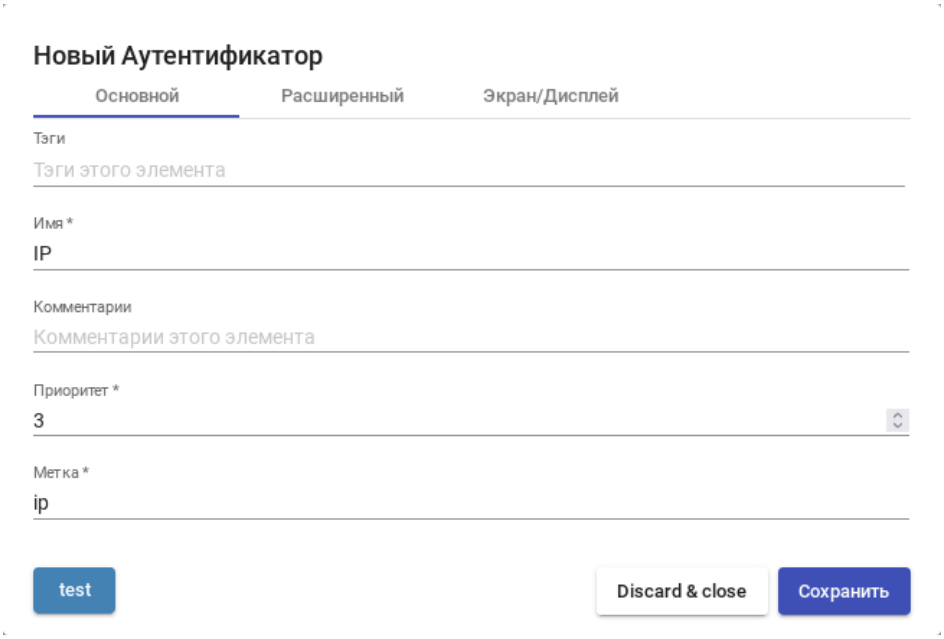


Рис. 172

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) (Рис. 173).

OpenUDS. IP аутентификатор – создание группы пользователей

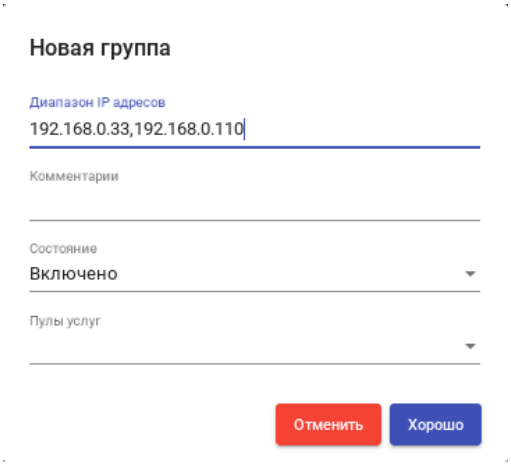


Рис. 173

6.10.2.3 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».

OpenUDS. Настройка «OS Manager»

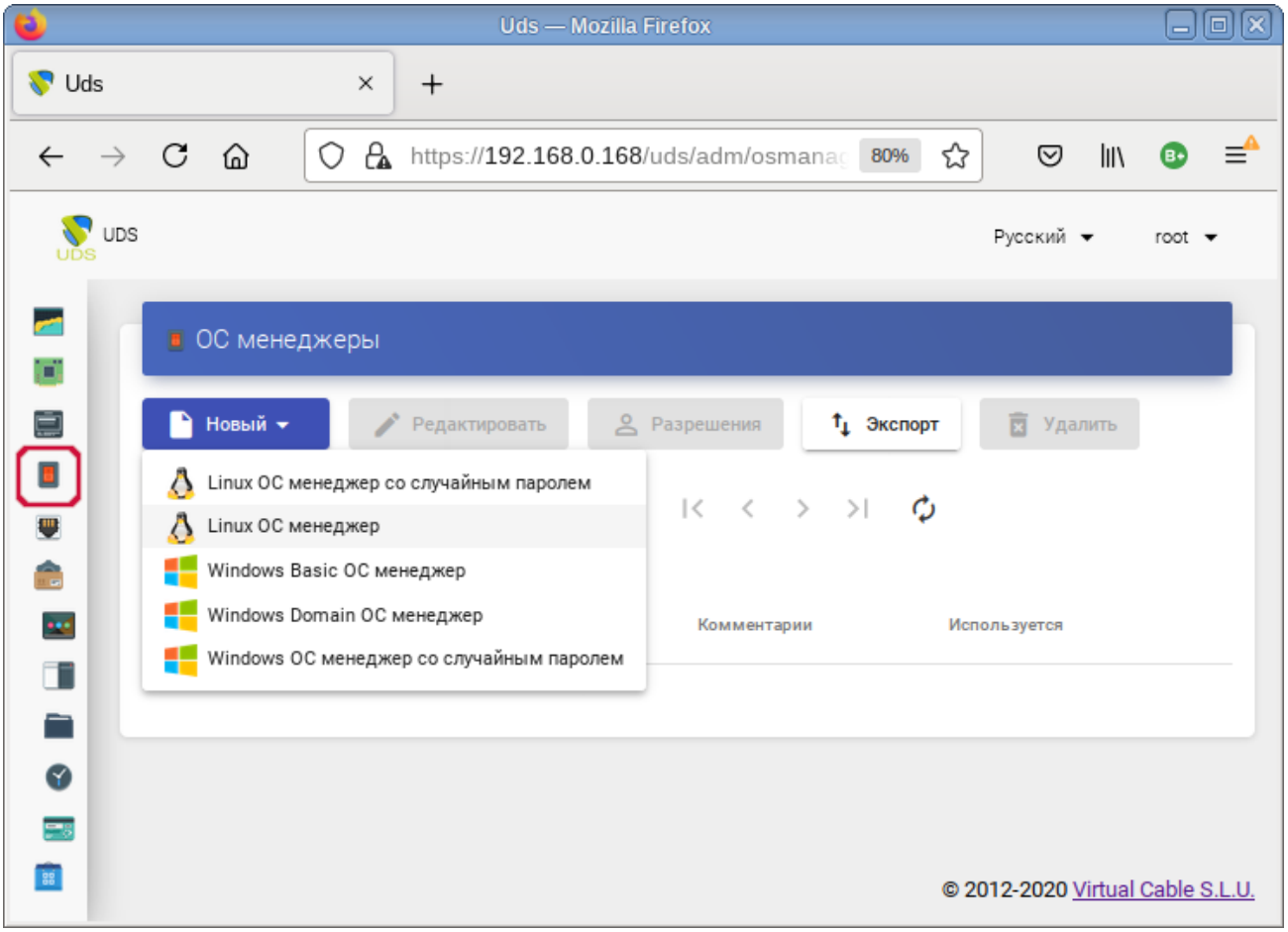


Рис. 174

«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» (Рис. 175):

– «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.

OpenUDS. Настройка «OS Manager»

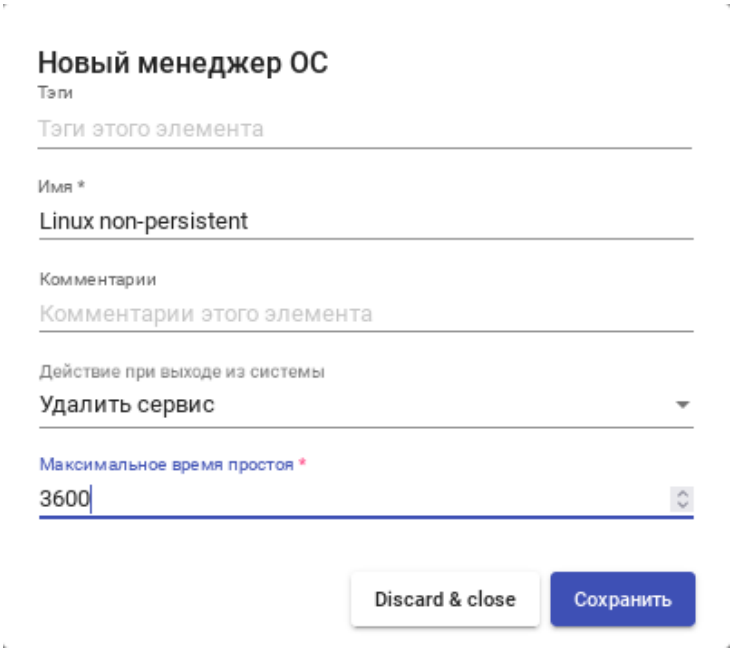


Рис. 175

6.10.2.4 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 (Рис. 176):

– «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.

OpenUDS. Настройка «Transports»

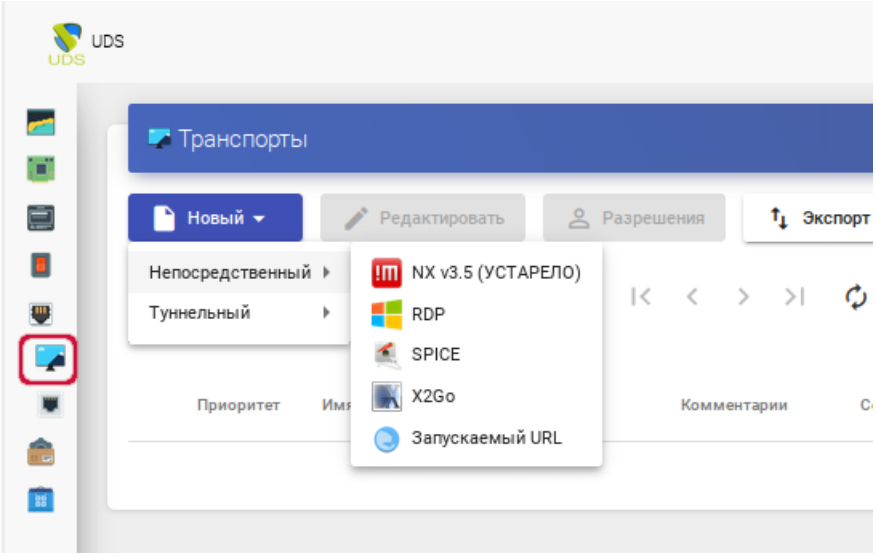


Рис. 176

6.10.2.4.1 RDP (непосредственный)

RDP (Рис. 177, Рис. 178) 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).

OpenUDS. Настройка RDP

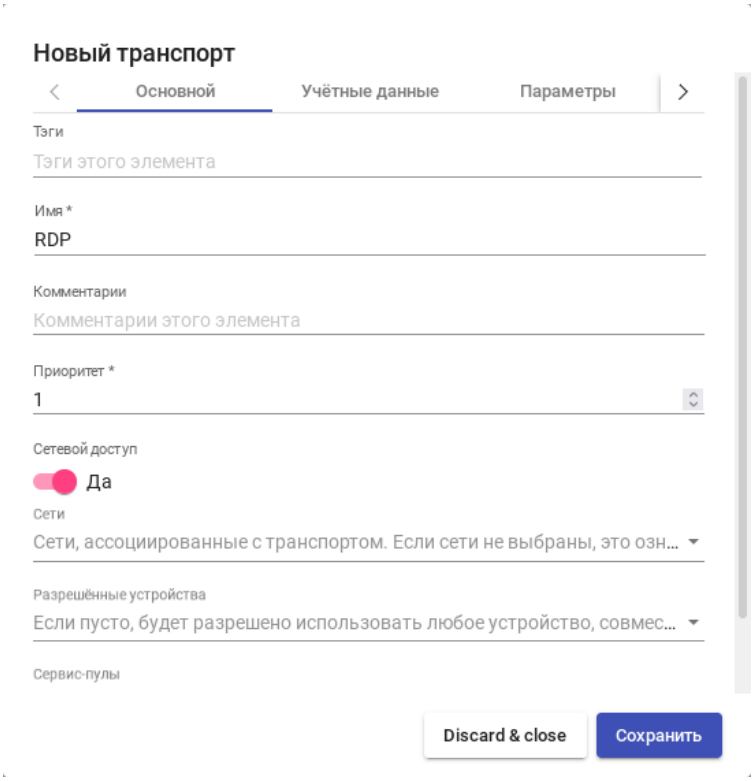


Рис. 177

OpenUDS. Настройка RDP

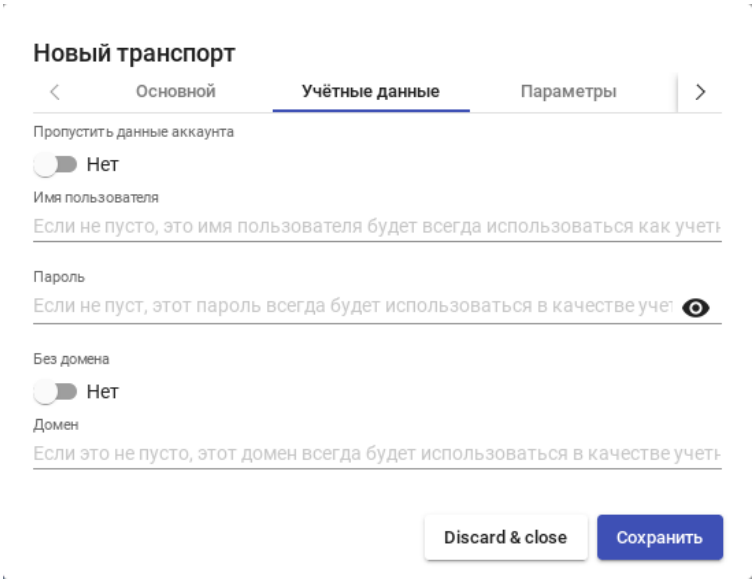


Рис. 178

6.10.2.4.2 X2Go (непосредственный)

X2Go (Рис. 179, Рис. 180) 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.

OpenUDS. Настройка X2Go

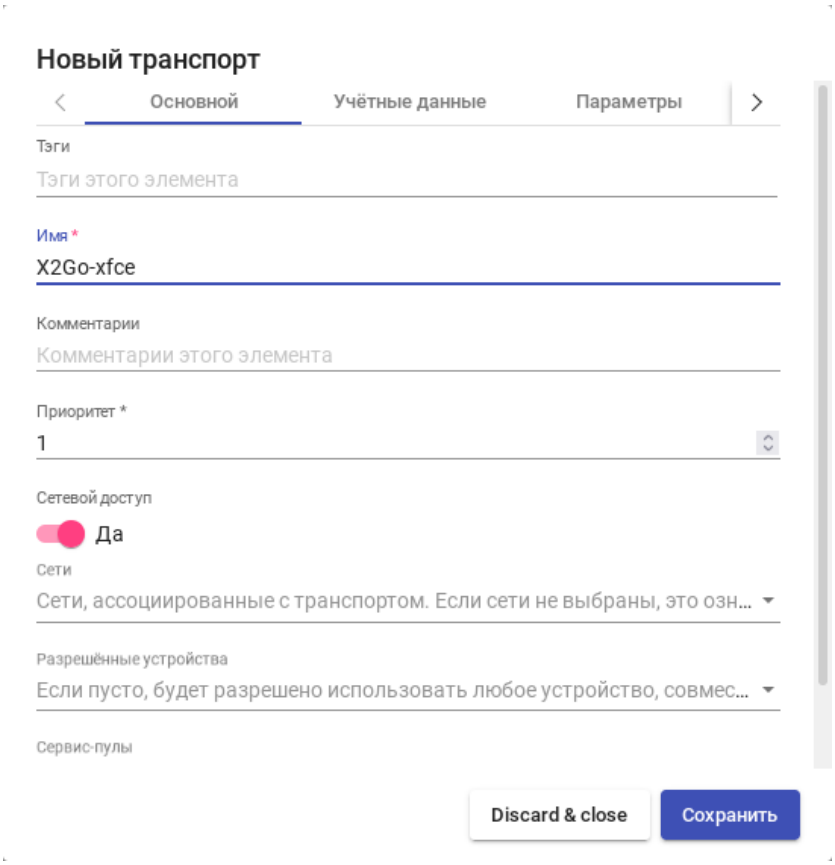


Рис. 179

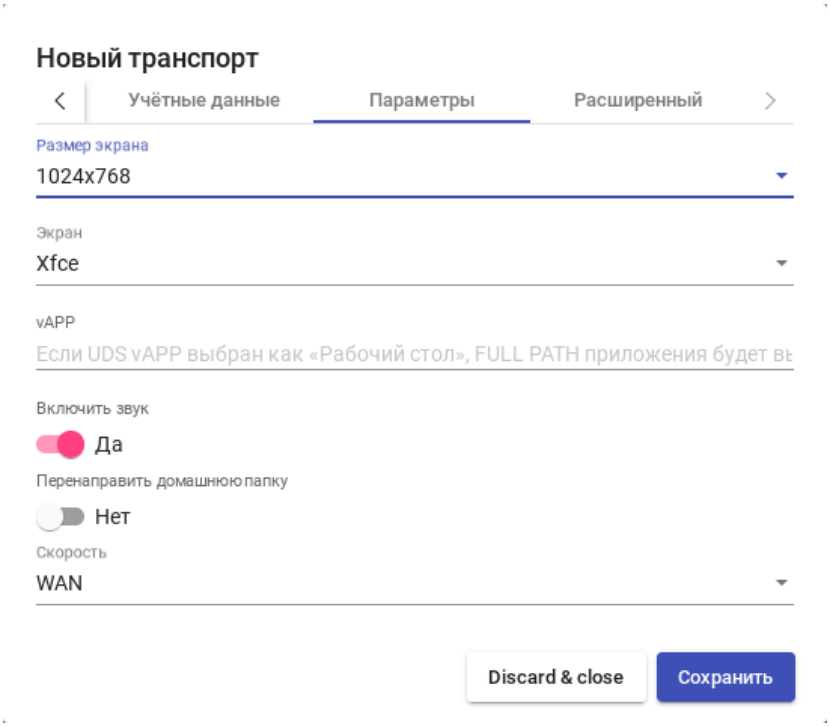


Рис. 180

6.10.2.5 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» (Рис. 181).

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») (Рис. 182):

- «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».

OpenUDS. Новый пул услуг

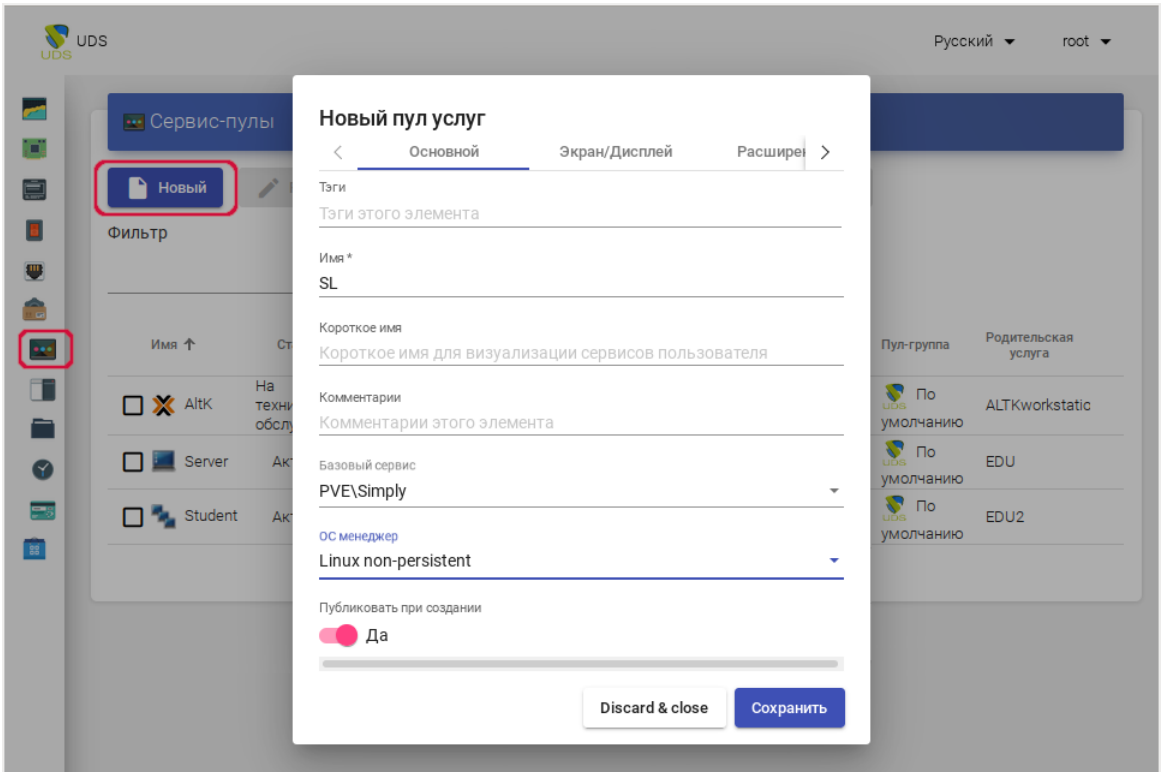


Рис. 181

OpenUDS. Новый Service Pool. Вкладка «Экран/Дисплей»

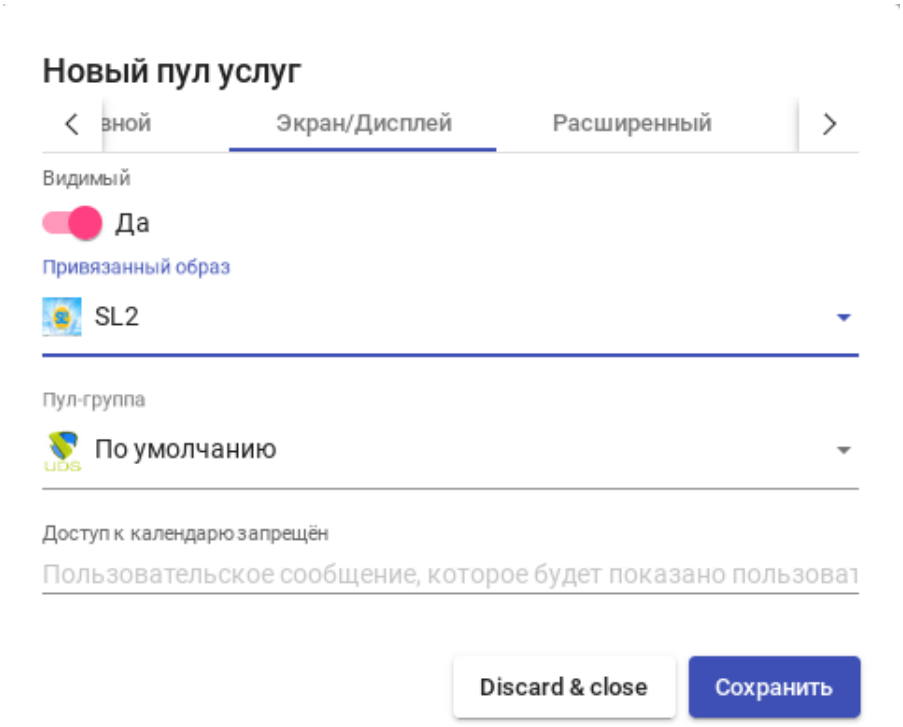


Рис. 182

Вкладка «Доступность» («Availability») (Рис. 183):

– «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).

OpenUDS. Новый Service Pool. Вкладка «Доступность»

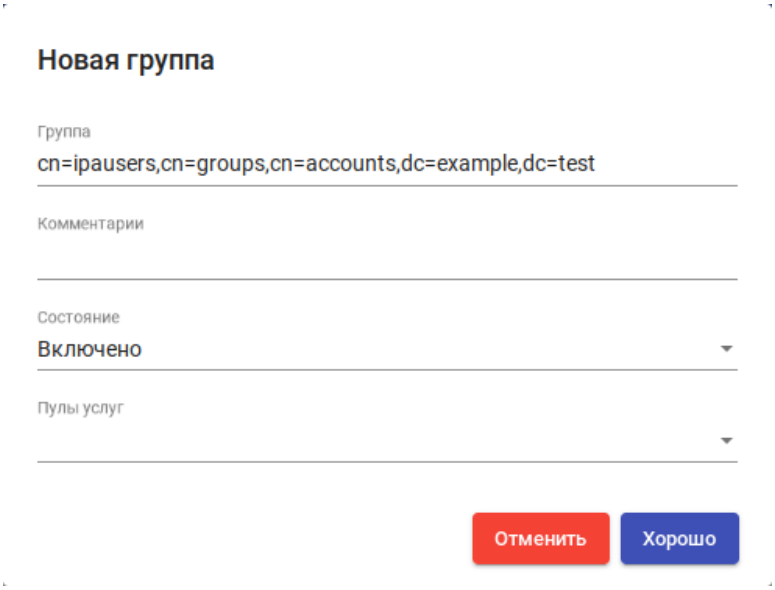


Рис. 183

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» (Рис. 184) назначить группы доступа (выбрать аутентификатор и группу, которая будет иметь доступ к этому пулу служб).
– на вкладке «Транспорты» (Рис. 185) выбрать способы подключения пользователей к рабочему столу.

OpenUDS. Назначение группы пулу служб

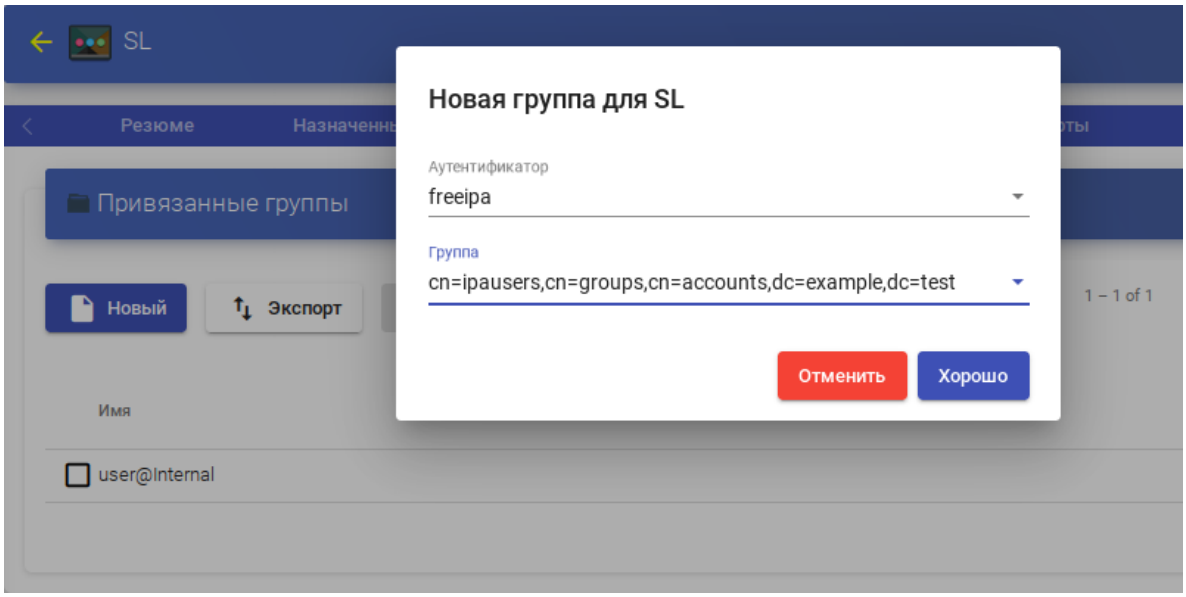


Рис. 184

OpenUDS. Выбор способов подключения к пулу служб

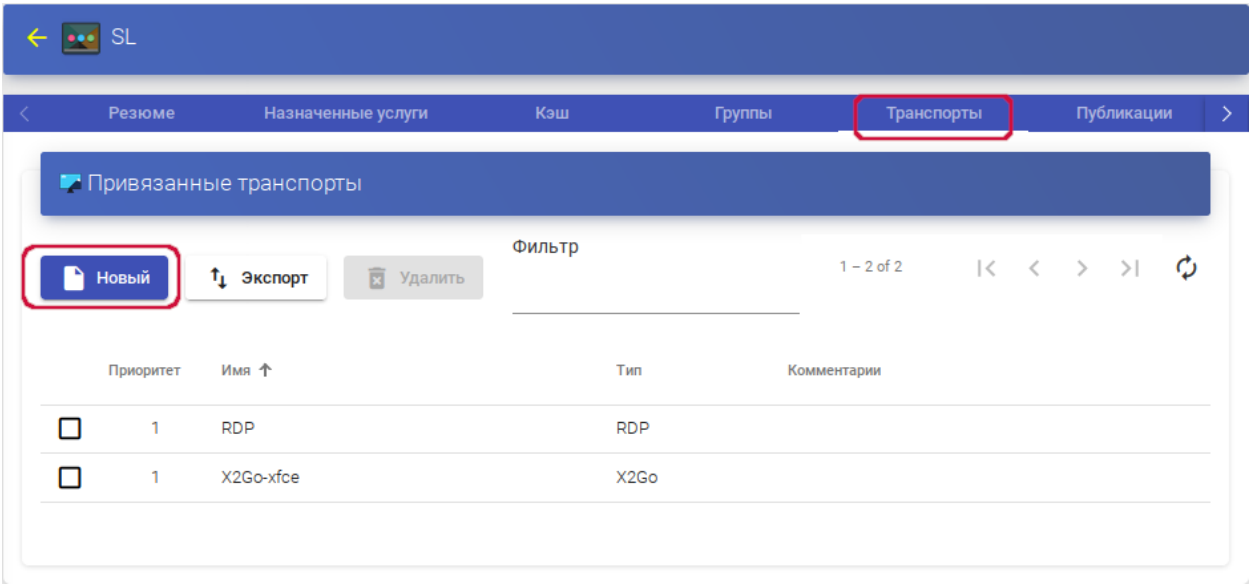


Рис. 185

6.10.3 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» (Рис. 186) 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.

OpenUDS. UDS Actor Configuration

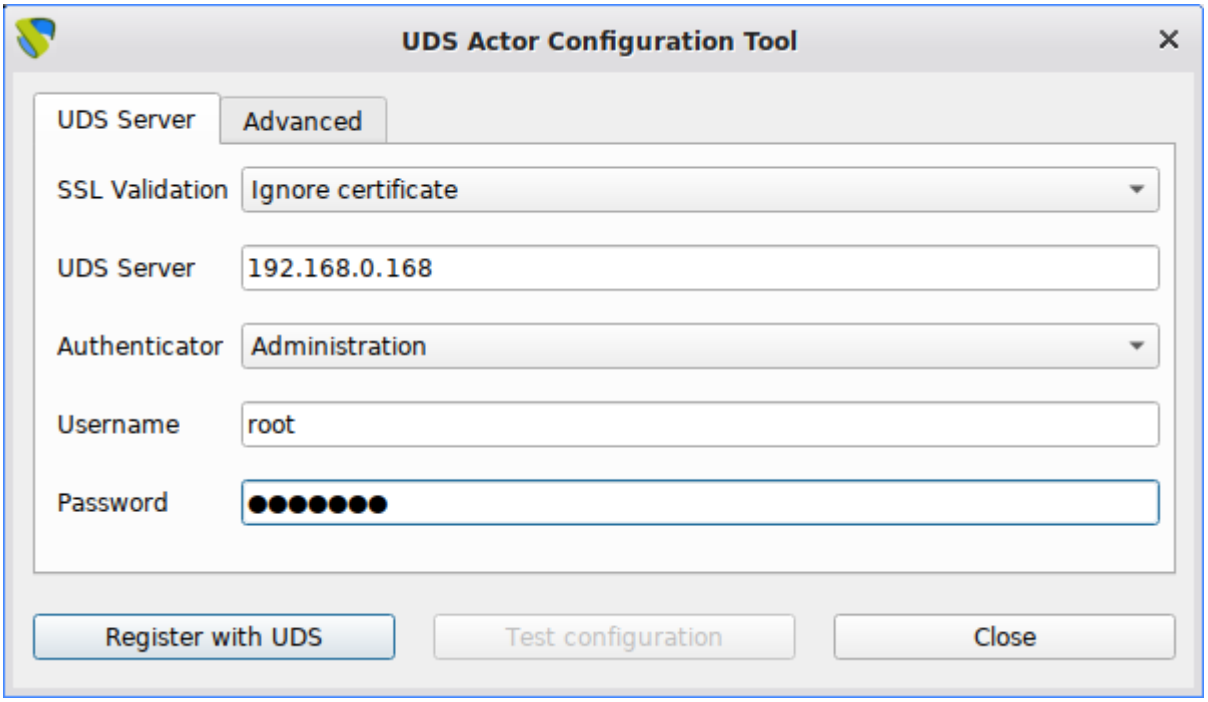


Рис. 186

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
```

6.10.4 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 (Рис. 187).

OpenUDS. Аутентификация пользователя

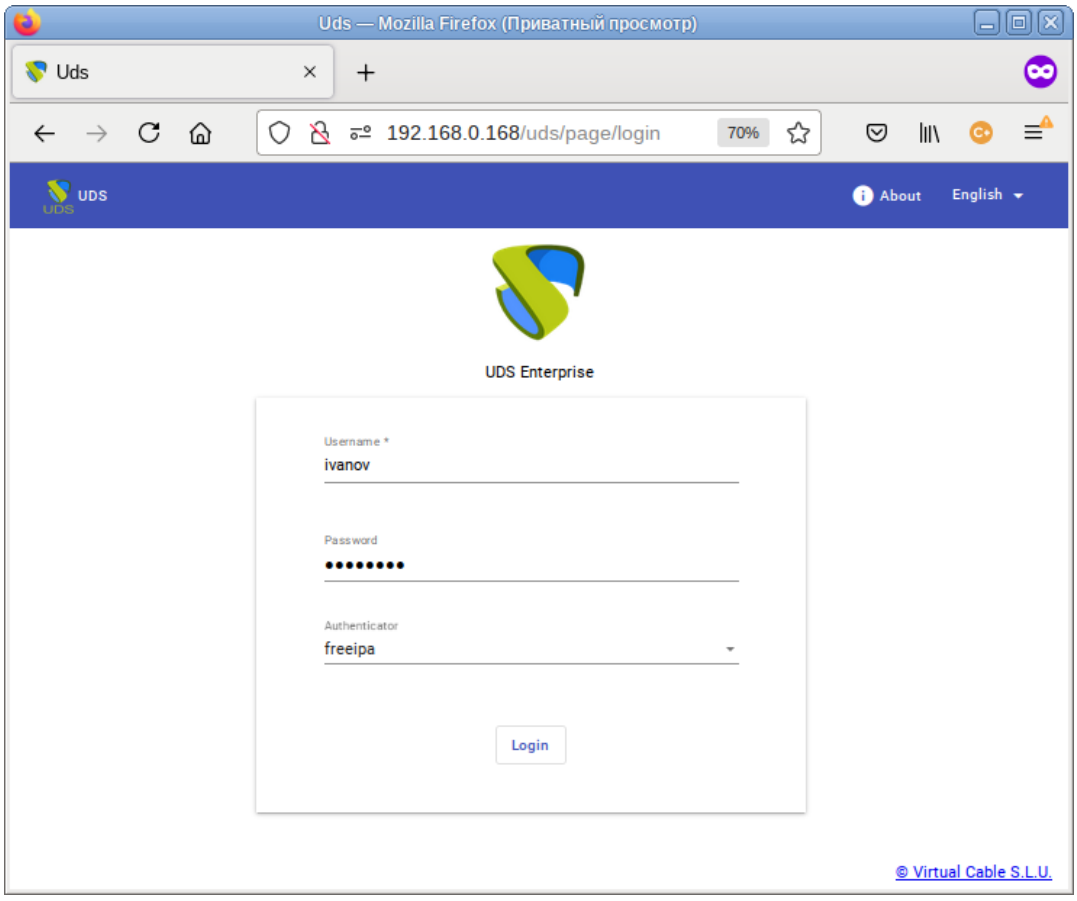


Рис. 187

На панели управления будут отображены все ВМ (или шаблоны), к которым у пользователя есть доступ (Рис. 188).

OpenUDS. Подключение пользователя к виртуальному рабочему месту

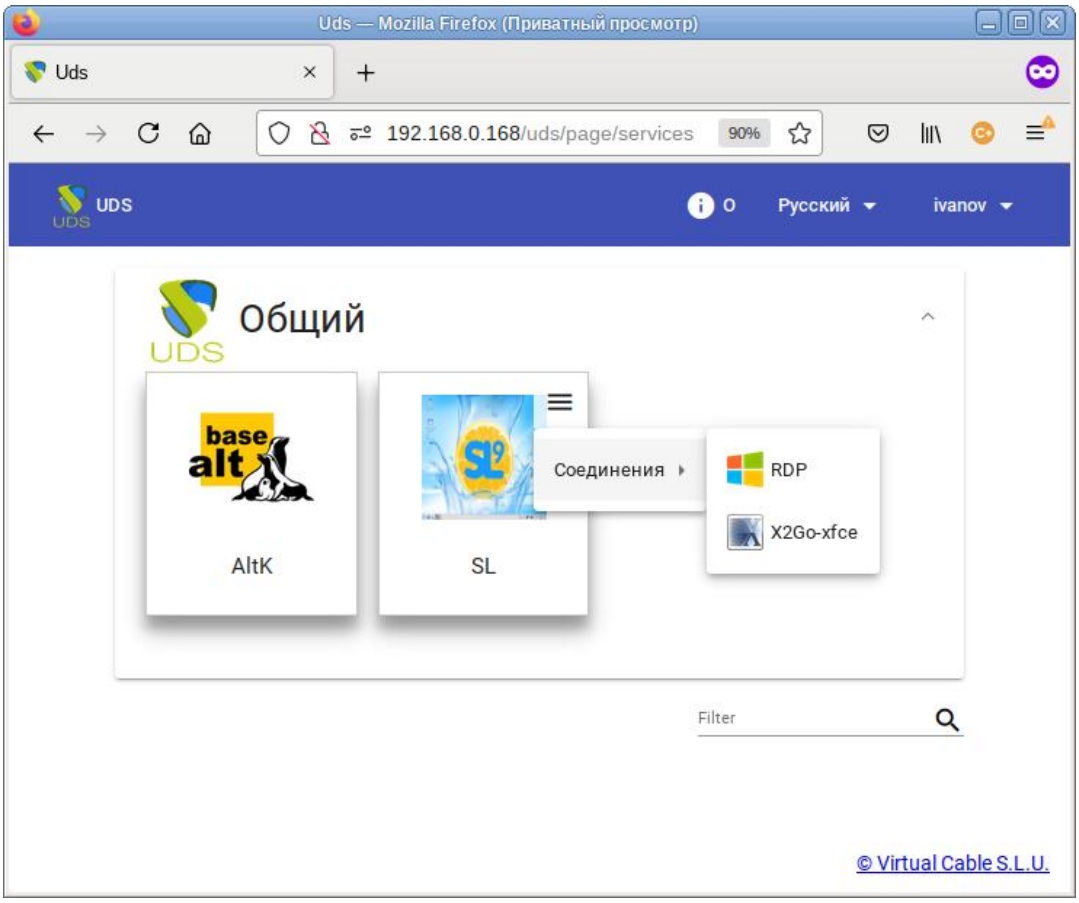


Рис. 188

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 (Рис. 189).

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.

OpenUDS. Виртуальный рабочий стол

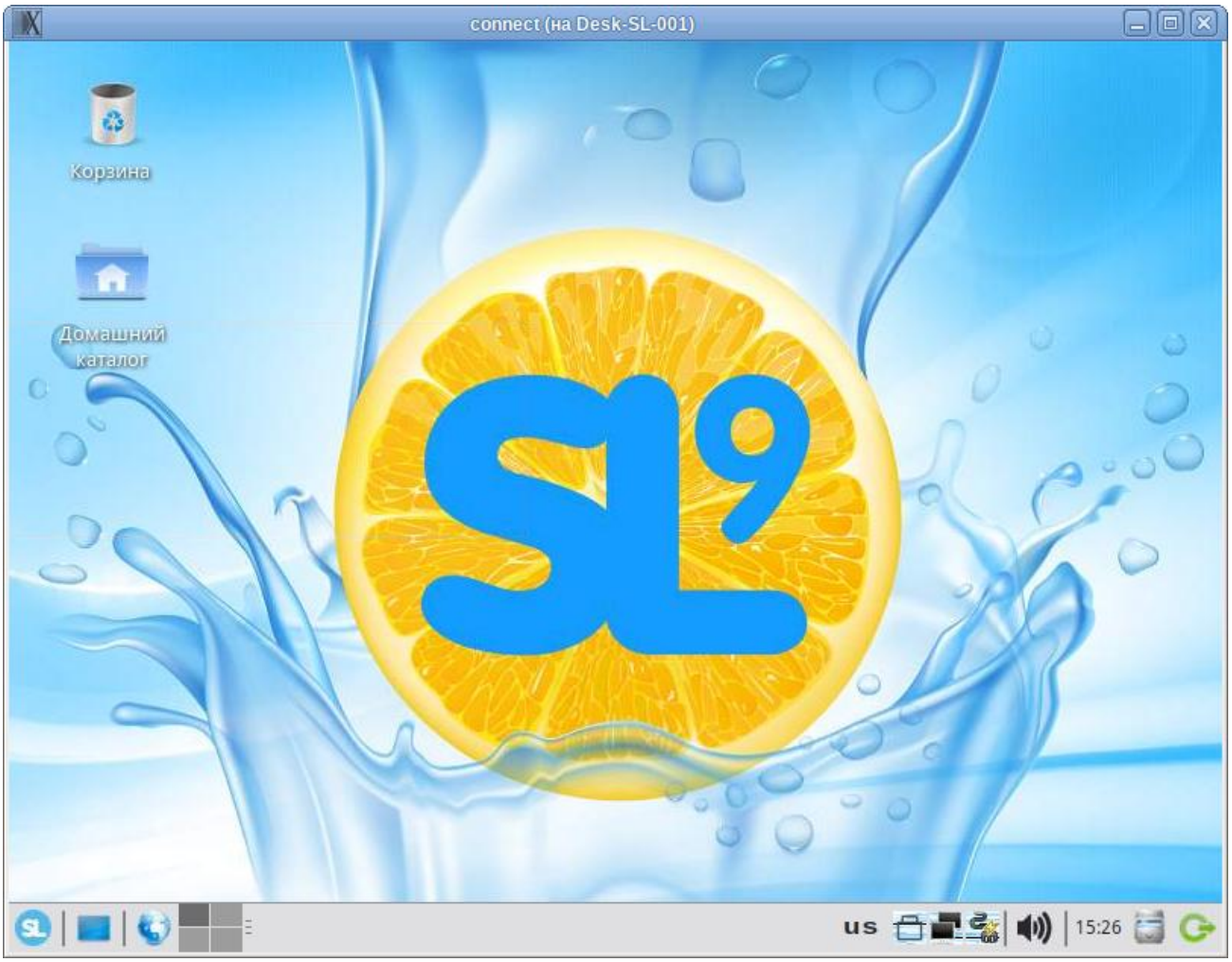


Рис. 189

Примечание. При подключении пользователя к виртуальному рабочему месту OpenUDS фиксирует доступ и отображает информацию о привязанном сервисе на вкладке «Назначенные услуги» соответствующего пула (Рис. 190).

OpenUDS. Вкладка «Назначенные услуги»

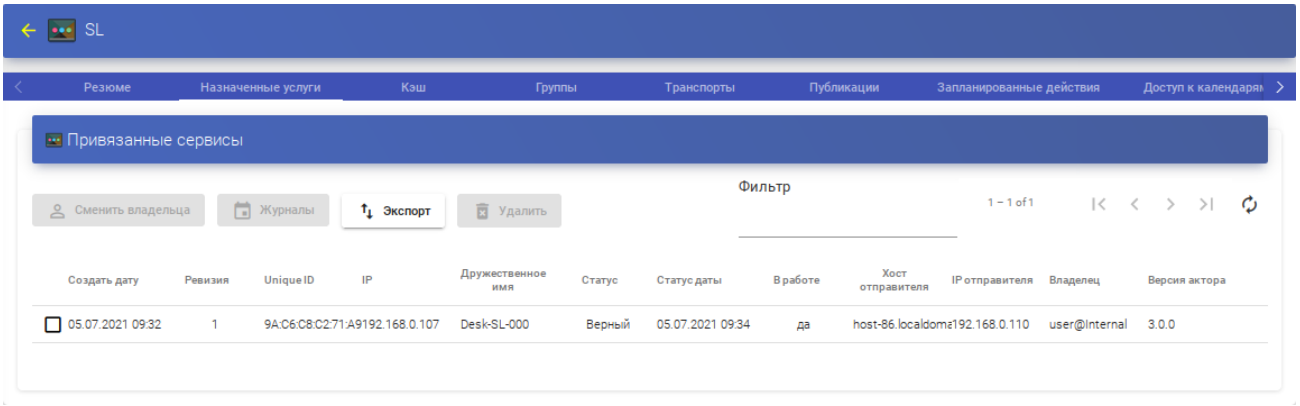


Рис. 190

7 ОБЩИЕ ПРИНЦИПЫ РАБОТЫ ОС

Работа с операционной средой заключается во вводе определенных команд (запросов) к операционной среде и получению на них ответов в виде текстового отображения.

Основой операционной среды является операционная система.

Операционная система (ОС) – совокупность программных средств, организующих согласованную работу операционной среды с аппаратными устройствами компьютера (процессор, память, устройства ввода-вывода и т. д.).

Диалог с ОС осуществляется посредством командных интерпретаторов и системных библиотек.

Каждая системная библиотека представляет собой набор программ, динамически вызываемых операционной системой.

Командные интерпретаторы – особый род специализированных программ, позволяющих осуществлять диалог с ОС посредством команд.

Для удобства пользователей при работе с командными интерпретаторами используются интерактивные рабочие среды (далее – ИРС), предоставляющие пользователю удобный интерфейс для работы с ОС.

В самом центре ОС изделия находится управляющая программа, называемая ядром. В ОС изделия используется новейшая модификация «устойчивого» ядра Linux – версия 5.4.

Ядро взаимодействует с компьютером и периферией (дисками, принтерами и т. д.), распределяет ресурсы и выполняет фоновое планирование заданий.

Другими словами, ядро ОС изолирует вас от сложностей аппаратуры компьютера, командный интерпретатор от ядра, а ИРС от командного интерпретатора.

Защита операционной среды осуществляется с помощью комплекса встроенных средств защиты информации.

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, который представляет собой, как было сказано выше, 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 команд-

ный язык и позволяют писать достаточно сложные программы, упрощающие процесс администрирования системы и работы с ней.

7.1 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 продолжится только после переведения его в «нормальный» режим работы.

7.2 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 изделии монтируется по умолчанию в каталог /media/cdrom (путь в изделии обозначается с использованием «/», а не «\», как в DOS/Windows). Текущий каталог обозначается «./».

Файловая система изделия содержит каталоги первого уровня:

- /bin (командные оболочки (shell), основные утилиты);
- /boot (содержит ядро системы);
- /dev (псевдофайлы устройств, позволяющие работать с ними напрямую);
- /etc (файлы конфигурации);
- /home (личные каталоги пользователей);
- /lib (системные библиотеки, модули ядра);
- /lib64 (64-битные системные библиотеки);
- /media (каталоги для монтирования файловых систем сменных устройств);

- /mnt (каталоги для монтирования файловых систем сменных устройств и внешних файловых систем);
- /proc (файловая система на виртуальном устройстве, ее файлы содержат информацию о текущем состоянии системы);
- /root (личный каталог администратора системы);
- /sbin (системные утилиты);
- /sys (файловая система, содержащая информацию о текущем состоянии системы);
- /usr (программы и библиотеки, доступные пользователю);
- /var (рабочие файлы программ, очереди, журналы);
- /tmp (временные файлы).

7.3 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, представляющий собой путь в файловой системе к данному файлу, где каждое следующее имя отделяется от предыдущего наклонной чертой (слэшем). Если название маршрута начинается со слэша, 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;
- цифры;
- символ подчеркивания (_);
- точка (.).

Для удобства работы можно использовать точку (.) для отделения имени файла от расширения файла. Данная возможность может быть необходима пользователям или некоторым программам, но не имеет значение для shell.

7.3.1 Иерархическая организация файловой системы

Каталог /:

/boot – место, где хранятся файлы необходимые для загрузки ядра системы;

/lib – здесь располагаются файлы динамических библиотек, необходимых для работы большей части приложений и подгружаемые модули ядра;

/lib64 – здесь располагаются файлы 64-битных динамических библиотек, необходимых для работы большей части приложений;

/bin – минимальный набор программ необходимых для работы в системе;

/sbin – набор программ для административной работы с системой (программы необходимые только суперпользователю);

/home – здесь располагаются домашние каталоги пользователей;

/etc – в данном каталоге обычно хранятся общесистемные конфигурационные файлы для большинства программ в системе;

/etc/rc?.d,/etc/init.d,/etc/rc.boot,/etc/rc.d – директории, где расположены командные файлы системы инициализации SysVinit;

/etc/passwd – база данных пользователей, в которой содержится информация об имени пользователя, его настоящем имени, личном каталоге, закодированный пароль и другие данные;

/etc/shadow – теневая база данных пользователей. При этом информация из файла /etc/passwd перемещается в /etc/shadow, который недоступен по чтению всем, кроме пользователя root. В случае использования альтернативной схемы управления теневыми паролями (TCB) все теневые пароли для каждого пользователя располагаются в директории /etc/tcb/<имя пользователя>/shadow;

/dev – в этом каталоге находятся файлы устройств. Файлы в /dev создаются сервисом udev;

/usr – обычно файловая система /usr достаточно большая по объему, так как все программы установлены именно здесь. Вся информация в каталоге /usr помещается туда во время установки системы. Отдельно устанавливаемые пакеты программ и другие файлы размещаются в каталоге /usr/local. Некоторые подкаталоги системы /usr рассмотрены ниже;

/usr/bin – практически все команды, хотя некоторые находятся в /bin или в /usr/local/bin;

/usr/sbin – команды, используемые при администрировании системы и не предназначенные для размещения в файловой системе root;

/usr/local – здесь 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 находящих в очереди на обработку для того или иного процесса (очередь на печать, отправку почты и т. д.);

/tmp – временный каталог необходимый некоторым приложениям;

/proc – файловая система /proc является виртуальной и в действительности она не существует на диске. Ядро создает её в памяти компьютера. Система /proc предоставляет информацию о системе.

7.3.2 Имена дисков и разделов

Все физические устройства вашего компьютера отображаются в каталог /dev файловой системы изделия (об этом – ниже). Диски (в том числе IDE/SATA/SCSI жёсткие диски, USB-диски) имеют имена:

/dev/sda – первый диск;

/dev/sdb – второй диск;

и т. д.

Диски обозначаются /dev/sdX, где X – a,b,c,d,e,... в порядке обнаружения системой.

Раздел диска обозначается числом после его имени. Например, /dev/sdb4 – четвертый раздел второго диска.

7.4 Разделы, необходимые для работы ОС

Для работы ОС необходимо создать на жестком диске (дисках) 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 свободного места на диске много, то можно создать отдельные разделы для каталогов /usr, /home, /var.

7.5 Управление системными сервисами и командами

7.5.1 Сервисы

Сервисы – это программы, которые запускаются и останавливаются через инициализированные скрипты, расположенные в каталоге /etc/init.d. Многие из этих сервисов запускаются на этапе старта ОС «Альт Сервер». В ОС существует шесть системных уровней выполнения, каждый из которых определяет список служб (сервисов), запускаемых на данном уровне. Уровни 0 и 6 соответствуют выключению и перезагрузке системы.

При загрузке системы процесс init запускает все сервисы, указанные в каталоге /etc/rc (0-6).d/ для уровня по умолчанию. Поменять его можно в конфигурационном файле /etc/inittab. Следующая строка соответствует второму уровню выполнения:

```
id:2:initdefault:
```

Для тестирования изменений, внесенных в файл inittab, применяется команда telinit. При указании аргумента -q процесс init повторно читает inittab.

Для перехода ОС «Альт Сервер» на нужный уровень выполнения можно воспользоваться командой init, например:

```
init 3
```

Данная команда переведет систему на третий уровень выполнения, запустив все сервисы, указанные в каталоге /etc/rc3.d/.

7.5.2 Команды

Далее приведены основные команды, использующиеся в ОС «Альт Сервер»:

- ar – создание и работа с библиотечными архивами;
- at – формирование или удаление отложенного задания;
- awk – язык обработки строковых шаблонов;
- batch – планирование команд в очереди загрузки;
- bc – строковый калькулятор;
- chfn – управление информацией учетной записи (имя, описание);
- chsh – управление выбором командного интерпретатора (по умолчанию – для учетной записи);
- cut – разбивка файла на секции, задаваемые контекстными разделителями;
- df – вывод отчета об использовании дискового пространства;
- dmesg – вывод содержимого системного буфера сообщений;
- du – вычисление количества использованного пространства элементов ФС;
- echo – вывод содержимого аргументов на стандартный вывод;
- egrep – поиск в файлах содержимого согласно регулярным выражениям;
- fgrep – поиск в файлах содержимого согласно фиксированным шаблонам;
- file – определение типа файла;
- find – поиск файла по различным признакам в иерархии каталогов;
- gettext – получение строки интернационализации из каталогов перевода;
- grep – вывод строки, содержащей шаблон поиска;
- groupadd – создание новой учетной записи группы;
- groupdel – удаление учетной записи группы;
- groupmod – изменение учетной записи группы;
- groups – вывод списка групп;
- gunzip – распаковка файла;

- gzip – упаковка файла;
- hostname – вывод и задание имени хоста;
- install – копирование файла с установкой атрибутов;
- ipcrm – удаление ресурса IPC;
- ipcs – вывод характеристик ресурса IPC;
- kill – прекращение выполнения процесса;
- killall – удаление процессов по имени;
- lpr – система печати;
- ls – вывод содержимого каталога;
- lsb_release – вывод информации о дистрибутиве;
- m4 – запуск макропроцессора;
- md5sum – генерация и проверка MD5-сообщения;
- mknod – создание файла специального типа;
- mktemp – генерация уникального имени файла;
- more – постраничный вывод содержимого файла;
- mount – монтирование ФС;
- msgfmt – создание объектного файла сообщений из файла сообщений;
- newgrp – смена идентификатора группы;
- nice – изменение приоритета процесса перед его запуском;
- nohup – работа процесса после выхода из системы;
- od – вывод содержимого файла в восьмеричном и других видах;
- passwd – смена пароля учетной записи;
- patch – применение файла описания изменений к оригинальному файлу;
- pidof – вывод идентификатора процесса по его имени;
- ps – вывод информации о процессах;
- renice – изменение уровня приоритета процесса;
- sed – строковый редактор;
- sendmail – транспорт системы электронных сообщений;
- sh – командный интерпретатор;
- shutdown – команда останова системы;
- su – изменение идентификатора запускаемого процесса;
- sync – сброс системных буферов на носители;
- tar – файловый архиватор;

- umount – размонтирование ФС;
- useradd – создание новой учетной записи или обновление существующей;
- userdel – удаление учетной записи и соответствующих файлов окружения;
- usermod – модификация информации об учетной записи;
- w – список пользователей, кто в настоящий момент работает в системе и с какими файлами;
- who – вывод списка пользователей системы.

Узнать об опциях команд можно с помощью команды man.

8 РАБОТА С НАИБОЛЕЕ ЧАСТО ИСПОЛЬЗУЕМЫМИ КОМПОНЕНТАМИ

8.1 Командные оболочки (интерпретаторы)

Для управления ОС используется командные интерпретаторы (shell).

Зайдя в систему, можно увидеть приглашение – строку, содержащую символ «$» (далее, этот символ будет обозначать командную строку). Программа ожидает ввода команд. Роль командного интерпретатора – передавать команды пользователя операционной системе. При помощи командных интерпретаторов можно писать небольшие программы – сценарии (скрипты). В Linux доступны следующие командные оболочки:

bash – самая распространённая оболочка под linux. Она ведет историю команд и предоставляет возможность их редактирования.

pdksh – клон korn shell, хорошо известной оболочки в UNIX(™) системах.

Оболочкой по умолчанию является «Bash» (Bourne Again Shell) Проверить, какая оболочка используется можно, выполнив команду:

```
$ echo $SHELL
```

У каждой оболочки свой синтаксис. Все примеры в дальнейшем построены с использованием оболочки Bash.

8.1.1 Командная оболочка Bash

В Bash имеется несколько приемов для работы со строкой команд. Например, используя клавиатуру, можно:

<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 <↑> и <↓>. Чтобы найти конкретную команду в списке набранных, не пролистывая всю историю, необходимо набрать <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 bunzip2, можно набрать следующую команду:

```
$ bu
```

Затем нажать <Tab>. Так как в данном случае существует несколько возможных вариантов завершения команды, то необходимо повторно нажать клавишу <Tab>, чтобы получить список имен, начинающихся с bu.

В предложенном примере можно получить следующий список:

```
$ bu
buildhash builtin bunzip2
```

Если набрать: n (bunzip – 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
```

8.1.2 Базовые команды оболочки Bash

Все команды, приведенные ниже, могут быть запущены в режиме консоли. Для получения более подробной информации следует использовать команду `man`. Пример:

```
$ man ls
```

8.1.2.1 Учетные записи пользователей

Команда su

Команда su позволяет получить права администратора. При вводе команды su, будет запрошен пароль суперпользователя (root). И в случае ввода корректного пароля, оператор получит привилегии суперпользователя. Чтобы вернуться к правам оператора, необходимо ввести команду:

```
# exit
```

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 [параметры] [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.

8.1.2.2 Основные операции с файлами и каталогами

Команда ls

Команда ls (list) выдает список файлов каталога.

Синтаксис:

```
ls [-CFRacdilqrtu1] [[-H] | [-L]] [-fgmnopsx] [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 используется для удаления файлов.

Синтаксис:

```
rm [-fiRr] имя_файла
```

Основные опции:

-f – не запрашивать подтверждения;

-i – запрашивать подтверждение;

-r, -R – рекурсивно удалять содержимое указанных каталогов.

Пример. Удалить все файлы html в каталоге ~/html:

```
$ rm -i ~/html/*.html
```

Команда mkdir

Команда mkdir позволяет создать каталог.

Синтаксис:

```
mkdir [-p] [-m права] [каталог...]
```

Команда rmdir

Команда rmdir удаляет записи, соответствующие указанным пустым каталогам.

Синтаксис:

```
rmdir [-p] [каталог...]
```

Команда rmdir часто заменяется командой rm -rf, которая позволяет удалять каталоги, даже если они не пусты.

Команда cp

Команда cp предназначена для копирования файлов.

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.

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 [параметры] [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 less

Команда less позволяет постранично просматривать текст (для выхода необходимо нажать <q>).

Синтаксис:

`less имя_файла`

Команда grep

Команда grep имеет много опций и предоставляет возможности поиска символьной строки в файле.

Синтаксис:

```
grep шаблон_поиска файл
```

Команда chmod

Команда chmod изменяет права доступа к файлу.

Синтаксис:

```
chmod ОПЦИЯ]... РЕЖИМ[,РЕЖИМ]... [Файл...]
chmod ОПЦИЯ]... --reference=ИФАЙЛ ФАЙЛ...
```

Основные опции:

-R – рекурсивно изменять режим доступа к файлам, расположенным в указанных каталогах;

--reference=ИФАЙЛ – использовать режим файла ИФАЙЛ.

Команда 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 /u на пользователя test:

```
$ chown test /u
```

Поменять владельца и группу /u:

```
$ chown test:staff /u
```

Поменять владельца /u и вложенных файлов на test:

```
$ chown -hR test /u
```

8.1.2.3 Поиск файлов

Команда find

Команда find предназначена для поиска всех файлов, начиная с корневой директории. 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

Команда whereis сообщает путь к исполняемому файлу программы, ее исходным файлам (если есть) и соответствующим страницам справочного руководства.

Синтаксис:

```
whereis [options] <name>
```

Опции:

-b – вывод информации только об исполняемых файлах;

-m – вывод информации только о страницах справочного руководства;

-s – вывод информации только об исходных файлах.

8.1.2.4 Мониторинг и управление процессами

Команда ps

Команда ps отображает список текущих процессов.

Синтаксис:

```
ps [-aA] [-defl] [-G список] [-o формат...] [-p список] [-t список] [-
U список] [-g список] [-n список] [-u список]
```

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 по умолчанию.

Синтаксис:

```
df [опция]... [файл]...
```

Основные опции:

-total – подсчитать общий объем в конце;

-h, --human-readable – печатать размеры в удобочитаемом формате (например, 1K 234M 2G);

-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] [--] имя_программы [...]
```

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.

8.1.2.5 Использование многозадачности

ОС «Альт Сервер» – многозадачная система.

Для того чтобы запустить программу в фоновом режиме необходимо набрать «&» после имени программы. После этого оболочка дает 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.

Команда bg

Команда bg используется для того, чтобы 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 «%».

8.1.2.6 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 директории]
```

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.

8.2 Стыкование команд в системе

8.2.1 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).

8.2.2 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.

8.2.3 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
```

Пример стыкования нескольких команд. Команда head – является фильтром следующего свойства: она выводит первые строки из входного потока (в примере на вход будет подан выход от нескольких состыкованных команд). 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.

8.2.4 Не деструктивное перенаправление вывода

Эффект от использования символа > для перенаправления вывода файла является деструктивным; то есть, 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.

9 ОБЩИЕ ПРАВИЛА ЭКСПЛУАТАЦИИ

9.1 Включение компьютера

Для включения компьютера необходимо:

- включить стабилизатор напряжения, если компьютер подключен через стабилизатор напряжения;
- включить принтер, если он нужен;
- включить монитор компьютера, если он не подключен к системному блоку кабелем питания;
- включить компьютер (переключателем на корпусе компьютера либо клавишей с клавиатуры).

После этого на экране компьютера появятся сообщения о ходе работы программ проверки и начальной загрузки компьютера.

9.2 Выключение компьютера

Для выключения компьютера надо:

- закончить работающие программы;
- выбрать функцию завершения работы и выключения компьютера, после чего ОС самостоятельно выключит компьютер, имеющий системный блок формата ATX;
- выключить компьютер (переключателем на корпусе AT системного блока);
- выключить принтер;
- выключить монитор компьютера (если питание монитора не от системного блока);
- выключить стабилизатор, если компьютер подключен через стабилизатор напряжения.