ОПЕРАЦИОННАЯ СИСТЕМА АЛЬТ СЕРВЕР 10.4

Описание функциональных характеристик

Содержание

1 ОБЩИЕ СВЕДЕНИЯ ОБ ОС АЛЬТ СЕРВЕР 10.4

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 должностных инструкций, 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

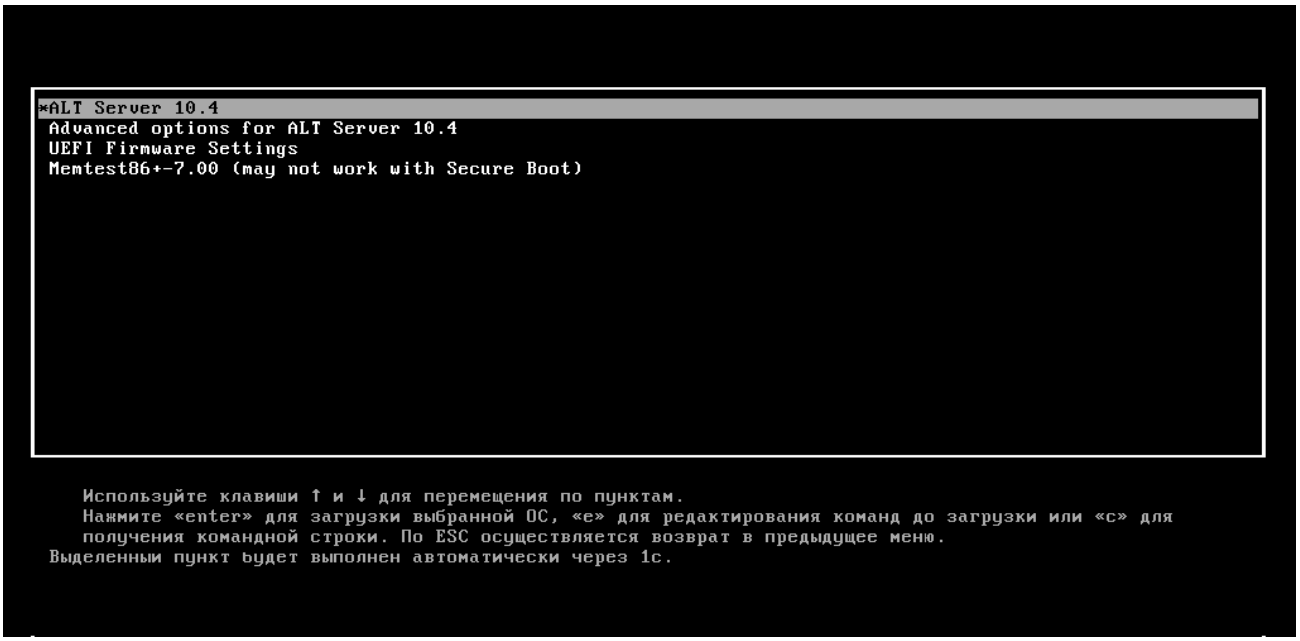


Рис. 1

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» («Advanced options for ALT Server 10.4»).

Для выполнения тестирования оперативной памяти нужно выбрать пункт «Memtest86+-7.00».

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

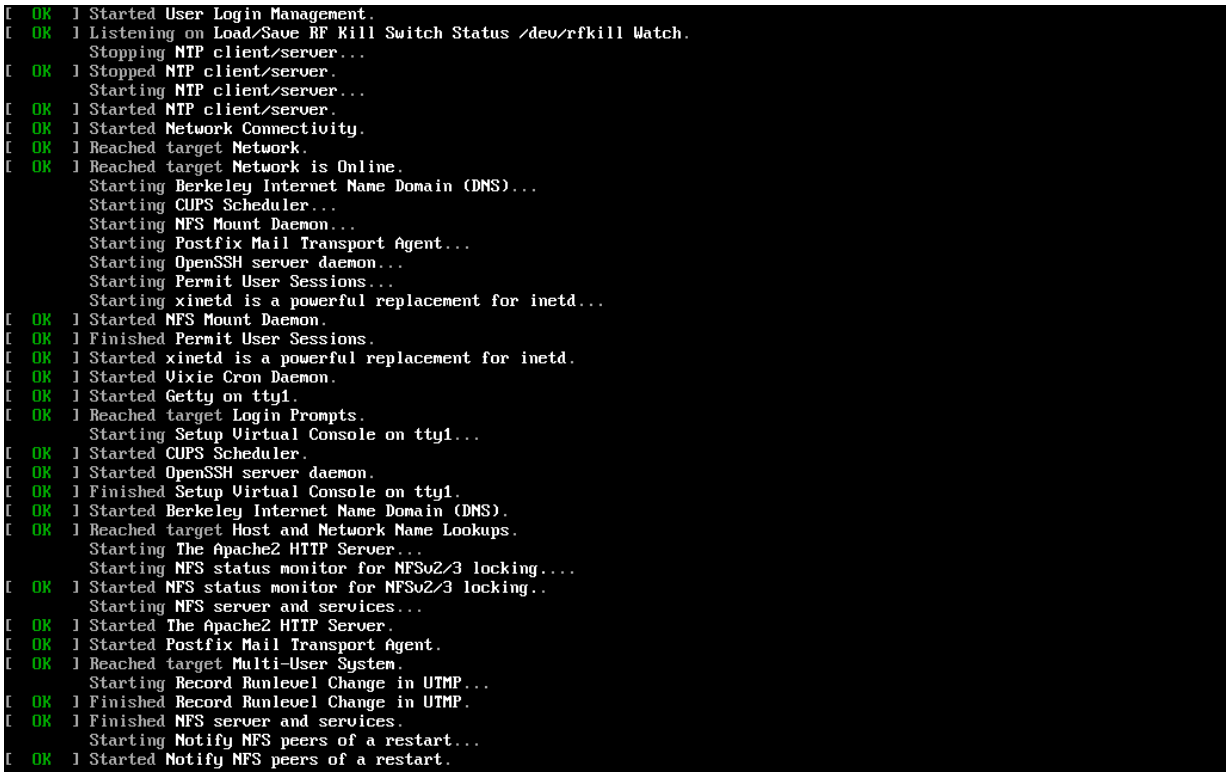


Рис. 2

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

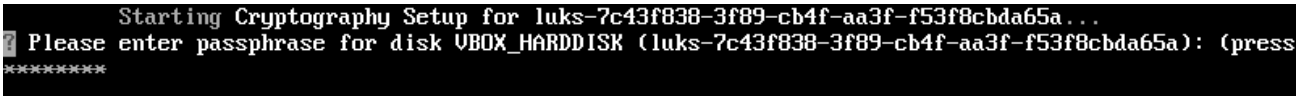


Рис. 3

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. В случае необходимости на другую консоль можно перейти, нажав <Ctrl>+<Alt>+<F2>.

Примечание. Сразу после загрузки в консоли будут показаны имя и IP-адрес компьютера.

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. 4).

Приглашение для ввода команд

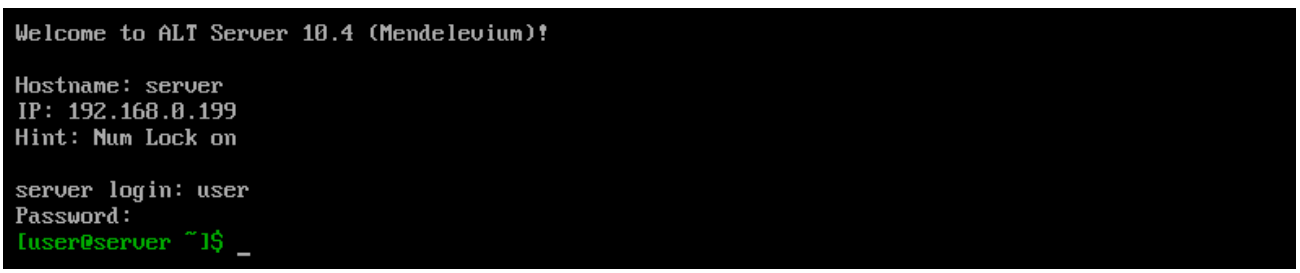


Рис. 4

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. 5).

Окно входа в систему

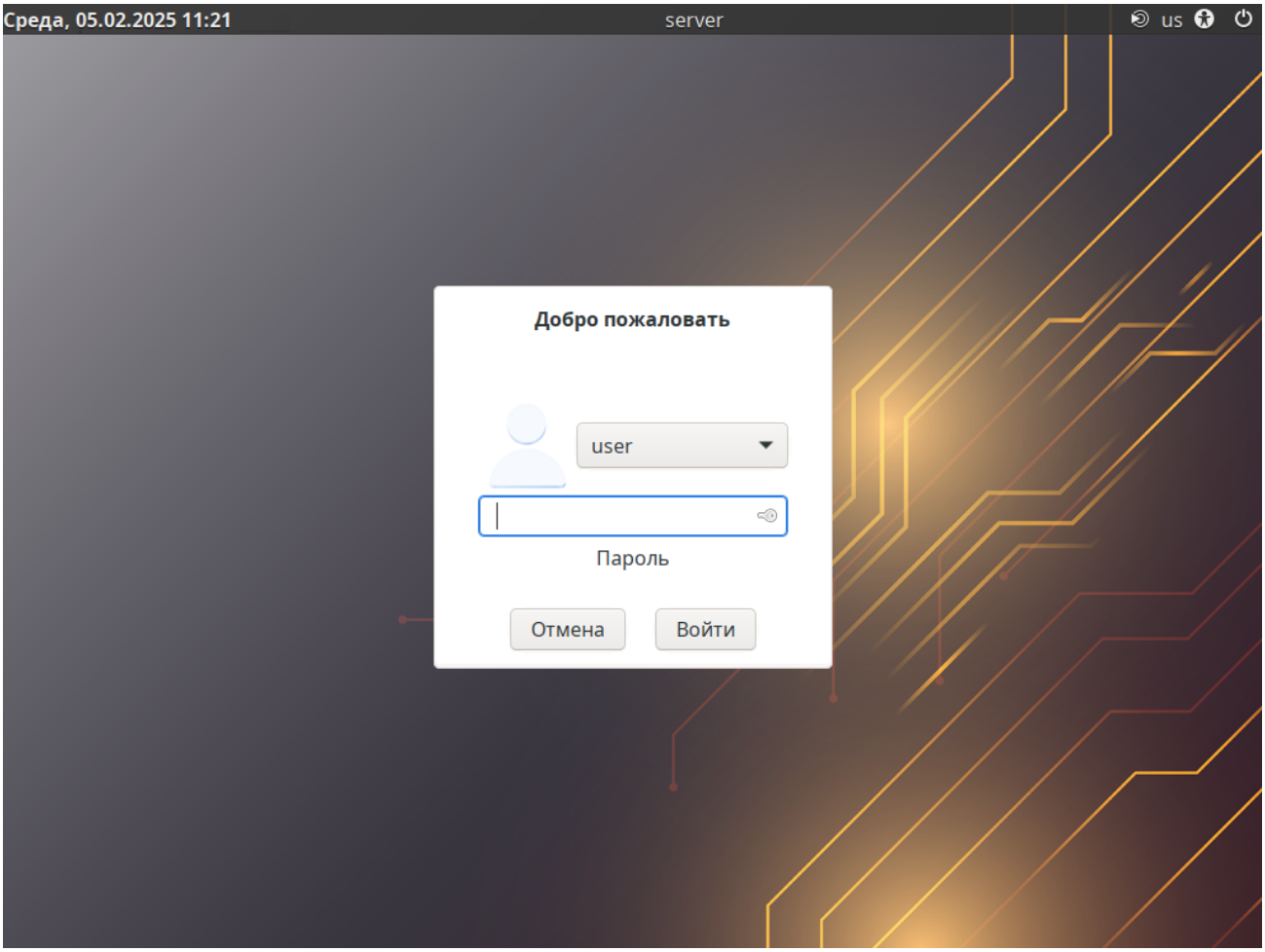


Рис. 5

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.

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. 6).

Рабочий стол MATE

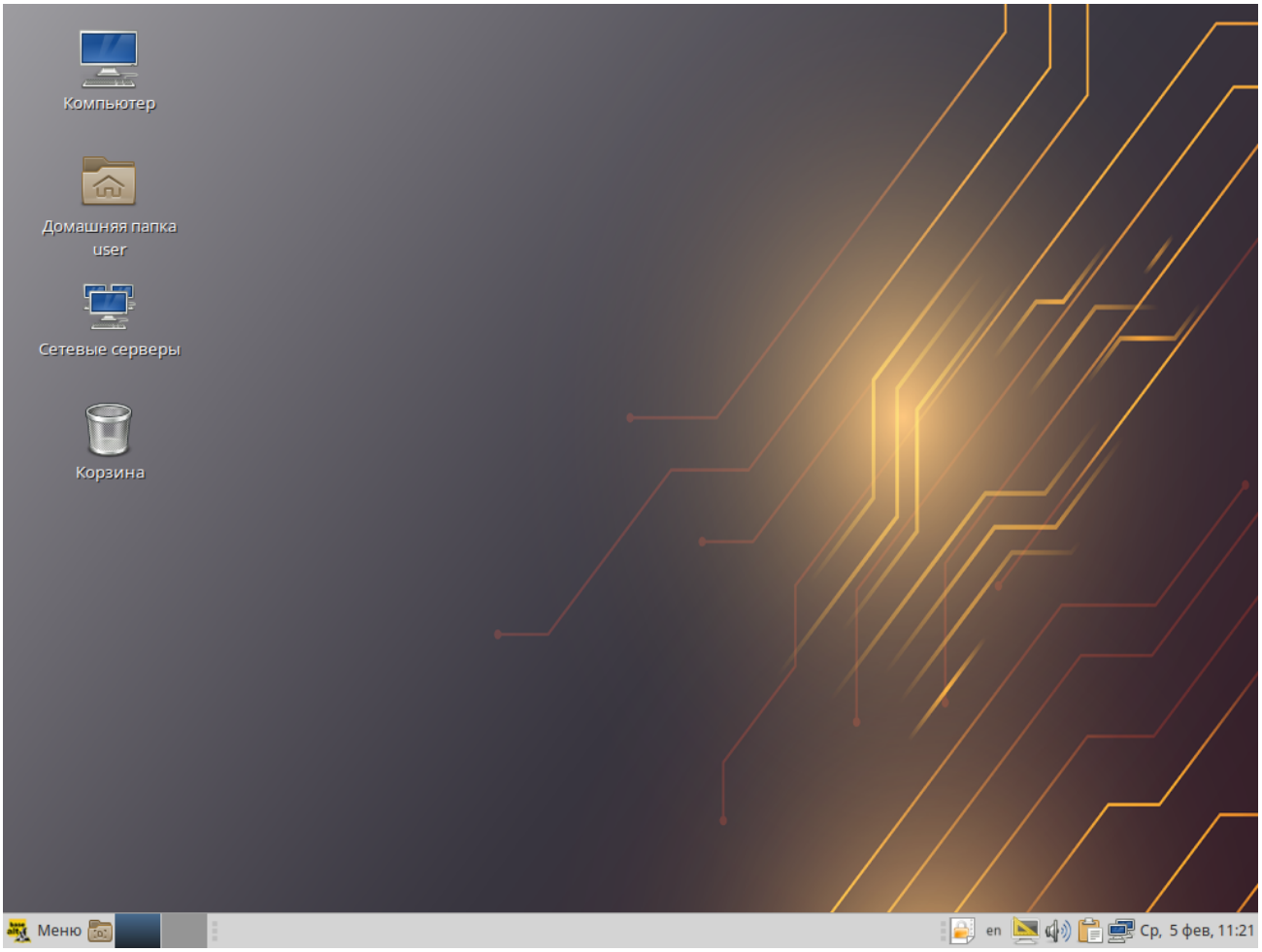


Рис. 6

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.

2.6 Рабочий стол MATE

На рабочем столе MATE есть две особые области. Сверху вниз (Рис. 6):

- область рабочего стола (рабочая площадь в центре, занимающая большую часть экрана);

- панель MATE (серая полоса внизу экрана).

Область рабочего стола включает в себя значки:

- «Компьютер» – предоставляет доступ к устройствам хранения данных;
- «Домашняя папка пользователя» – предоставляет доступ к домашнему каталогу пользователя `/home/<имя пользователя>`. В этой папке по умолчанию хранятся пользовательские файлы (например, аудиозаписи, видеозаписи, документы). Домашняя папка есть у каждого пользователя системы, и по умолчанию содержащиеся в ней файлы недоступны для других пользователей (даже для чтения);
- «Сетевые серверы» – позволяет просматривать сетевые подключения компьютера;
- «Корзина» – доступ к «удаленным файлам». Обычно удаляемый файл 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»).

Панель MATE (Рис. 7) расположена в нижней части экрана. Панель MATE универсальна: она может содержать значки загрузчика, панели задач, переключатель окон или любое другое сочетание; и её можно удобно настроить. Для того чтобы увидеть возможные варианты настройки, необходимо щелчком правой кнопки мыши вызвать контекстное меню и переместить, удалить или изменить содержание панели по форме и существу.

Панель MATE

Рис. 7

На левой части панели расположены:

- основное меню – «Меню MATE», обеспечивающее доступ ко всем графическим приложениями и изменениям настроек;
- кнопка «Свернуть все окна» – кнопка позволяет свернуть (развернуть) все открытые окна на текущем рабочем месте;

- «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 два рабочих места. Можно изменить это число, нажав правой кнопкой мыши на «переключателе рабочих мест» и выбрав в контекстном меню пункт «Параметры». Для переключения между рабочими столами необходимо использовать комбинацию клавиш <Ctrl>+<Alt>+<←> или <Ctrl>+<Alt>+<→>.

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 переключиться на другое приложение, можно кликнуть по нему левой кнопкой мыши. Для переключения между открытыми окнами также можно использовать комбинацию клавиш<Alt>+<Tab>.

На правой части панели находятся:

- область уведомлений;
- регулятор громкости и апплет настройки звука;
- приложение «Сетевые соединения»;
- часы и календарь;
- параметры клавиатуры;
- параметры управления питанием.

В левой части панели MATE находится «Меню MATE». Через «Меню MATE» (Рис. 8) осуществляется запуск всех приложений, установленных на компьютер.

Левая часть меню включает раздел «Места» и раздел «Система». Правая часть может иметь вид избранных приложений или всех доступных программ.

Раздел «Места» содержит пять кнопок, обеспечивающих быстрый доступ к наиболее важным местам ОС:

- «Мой компьютер» – позволяет увидеть все файлы в компьютере и файлы на подключённых внешних носителях;
- «Домашний каталог» – в этой папке по умолчанию хранятся личные файлы пользователя;
- «Сеть» – позволяет просматривать сетевые подключения компьютера. Осуществляет получение доступа к файлам и другим ресурсам, доступным в этих сетях;
- «Рабочий стол» – папка внутри «Домашней папки», содержащая файлы и папки, отображаемые на рабочем столе;
- «Корзина» – позволяет получить доступ к «удаленным файлам».

Меню MATE

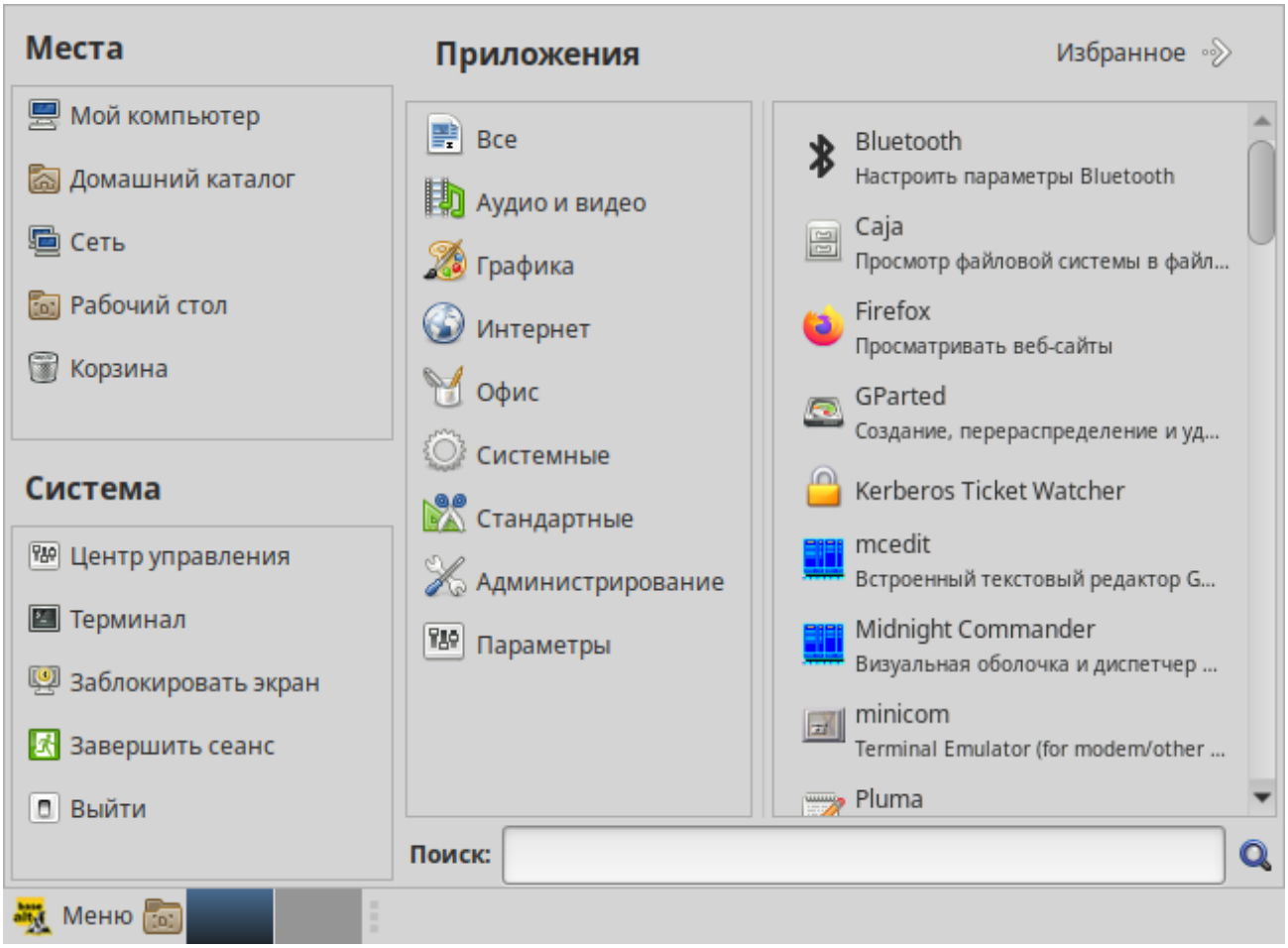


Рис. 8

Щелчок по любому пункту в подменю «Места» открывает файловый менеджер Caja.

Руководство Caja можно вызвать, выбрав меню «Справка» →«Содержание».

В разделе «Система» находятся кнопки, предоставляющие быстрый доступ к важным функциям системы:

- «Центр управления» – запускает приложение, позволяющее настроить все аспекты рабочего окружения MATE;
- «Терминал» – запускает приложение «Терминал», которое позволяет вводить команды непосредственно с клавиатуры;
- «Заблокировать экран» – блокирует сеанс доступа пользователя;
- «Завершить сеанс» – запускает диалог, который позволяет завершить сеанс или переключить пользователя;
- «Выйти» – выводит диалоговое окно, которое позволяет перезагрузить или выключить компьютер.

Установленные приложения доступны в следующих пунктах раздела «Приложения»:

- «Все» – показывает полный список установленных приложений;

- «Аудио и видео»;
- «Графика»;
- «Интернет»;
- «Образовательные»;
- «Офис»;
- «Системные»;
- «Стандартные»;
- «Администрирование» – содержит инструменты, позволяющие администрировать систему;
- «Параметры» – содержит инструменты, позволяющие конфигурировать систему.

Этот список обновляется при установке или удалении программ.

П р и м е ч а н и е . Если компьютер запрашивает пароль администратора (root), то это значит, что будут производиться важные системные настройки. Следует быть предельно внимательным к выводимым сообщениям.

Поле «Поиск» позволяет быстро запустить нужное приложение. Для этого достаточно приступить к вводу названия или описания искомого приложения, по мере ввода символлов, в меню остаются видны только те приложения, которые соответствуют запросу. Если объект поиска отстутствует в меню, функция «Поиск» «предложит» другие возможные действия, например, поиск в файлах ОС или поисковой системе.

Раздел «Избранное» позволяет получить быстрый доступ к выбранным приложениям. Для добавления приложения в раздел «Избранное» нужно в контекстном меню нужного приложения выбрать пункт «Отображать в избранном». Можно также перетащить иконку приложения на кнопку «Избранное», находящуюся в верхнем правом углу меню. Нажатие правой клавиши мыши позволяет как добавить, так и удалить элементы раздела «Избранное» (в том числе отступы и разделители).

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. Модули центра управления системой имеют справочную информацию.

3.1.1 Применение ЦУС

ЦУС можно использовать для разных целей, например:

- настройки даты и времени;
- управления системными службами;
- просмотра системных журналов;
- управления выключением удаленного компьютера (доступно только в веб-интерфейсе);
- настройки ограничений выделяемых ресурсов памяти пользователям (квоты): («Использование диска»);
- настройки ограничений на использование внешних носителей (доступно только в веб-интерфейсе);
- конфигурирования сетевых интерфейсов;
- настройки межсетевого экрана;
- изменения пароля администратора системы (root);
- создания, удаления и редактирования учётных записей пользователей.

3.1.2 Запуск ЦУС в графической среде

ЦУС можно запустить следующими способами:

- в графической среде MATE: «Приложения» → «Администрирование» → «Центр управления системой»;
- из командной строки: командой acc.

При запуске необходимо ввести пароль администратора системы (root) (Рис. 9).

После успешного входа можно приступать к настройке системы (Рис. 10).

Запуск Центра управления системой

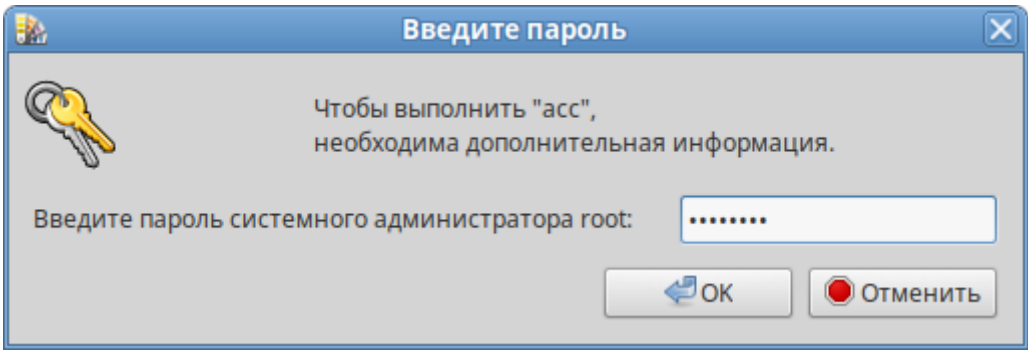


Рис. 9

Центр управления системой

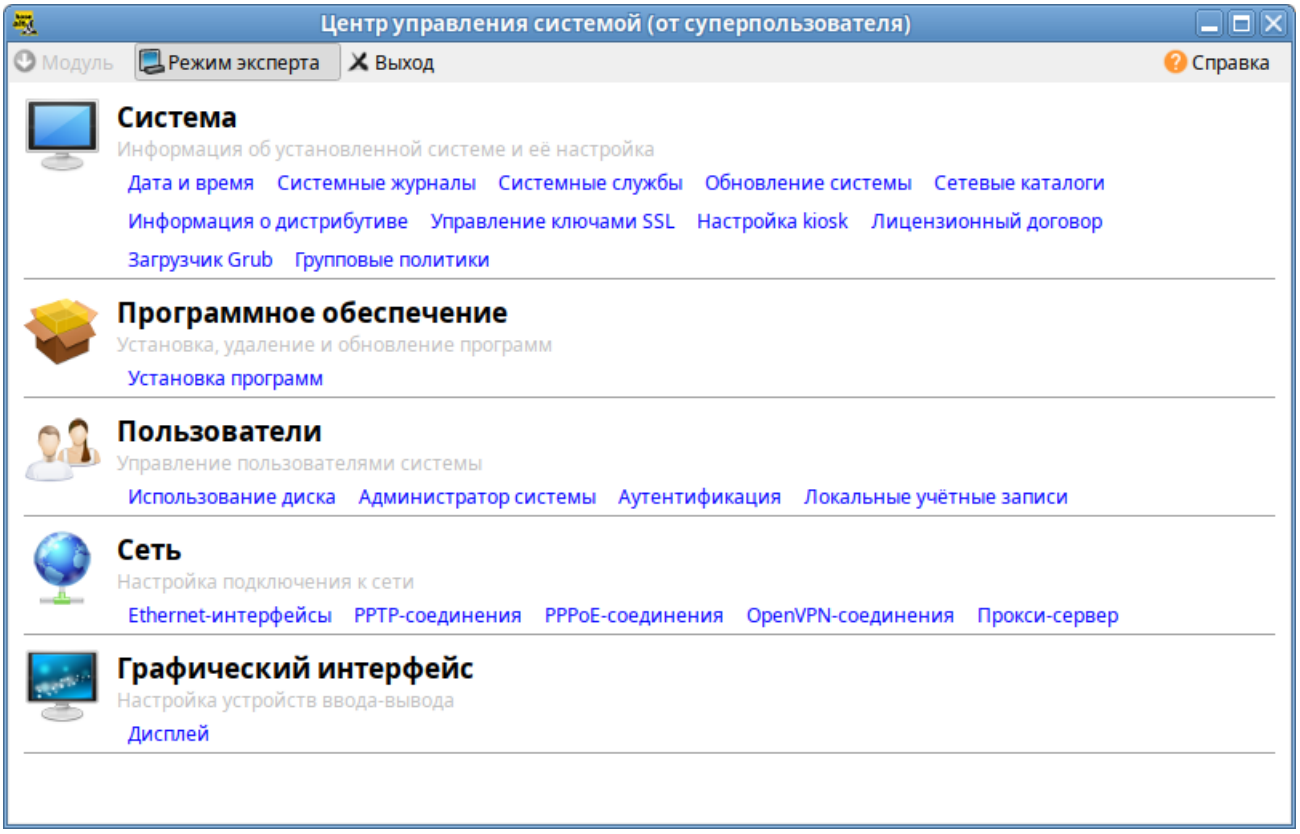


Рис. 10

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. 11).

Запуск веб-ориентированного центра управления системой

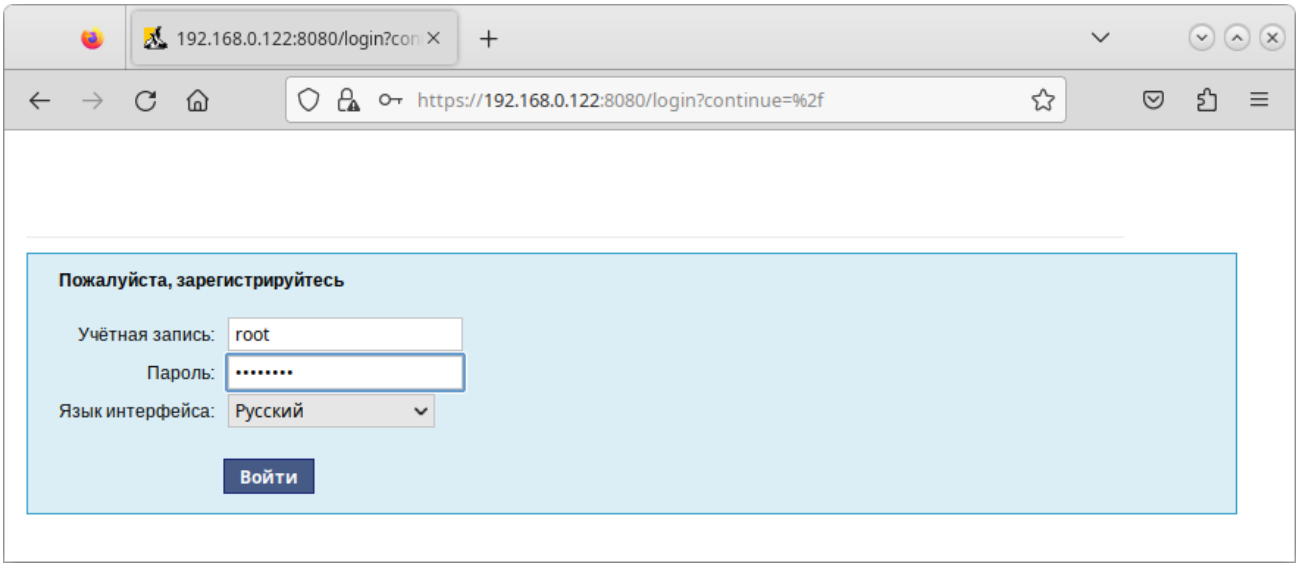


Рис. 11

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

Веб-интерфейс ЦУС можно настроить (кнопка «Настройка»), 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 ЦУС (Рис. 12).

Веб-ориентированный центр управления системой

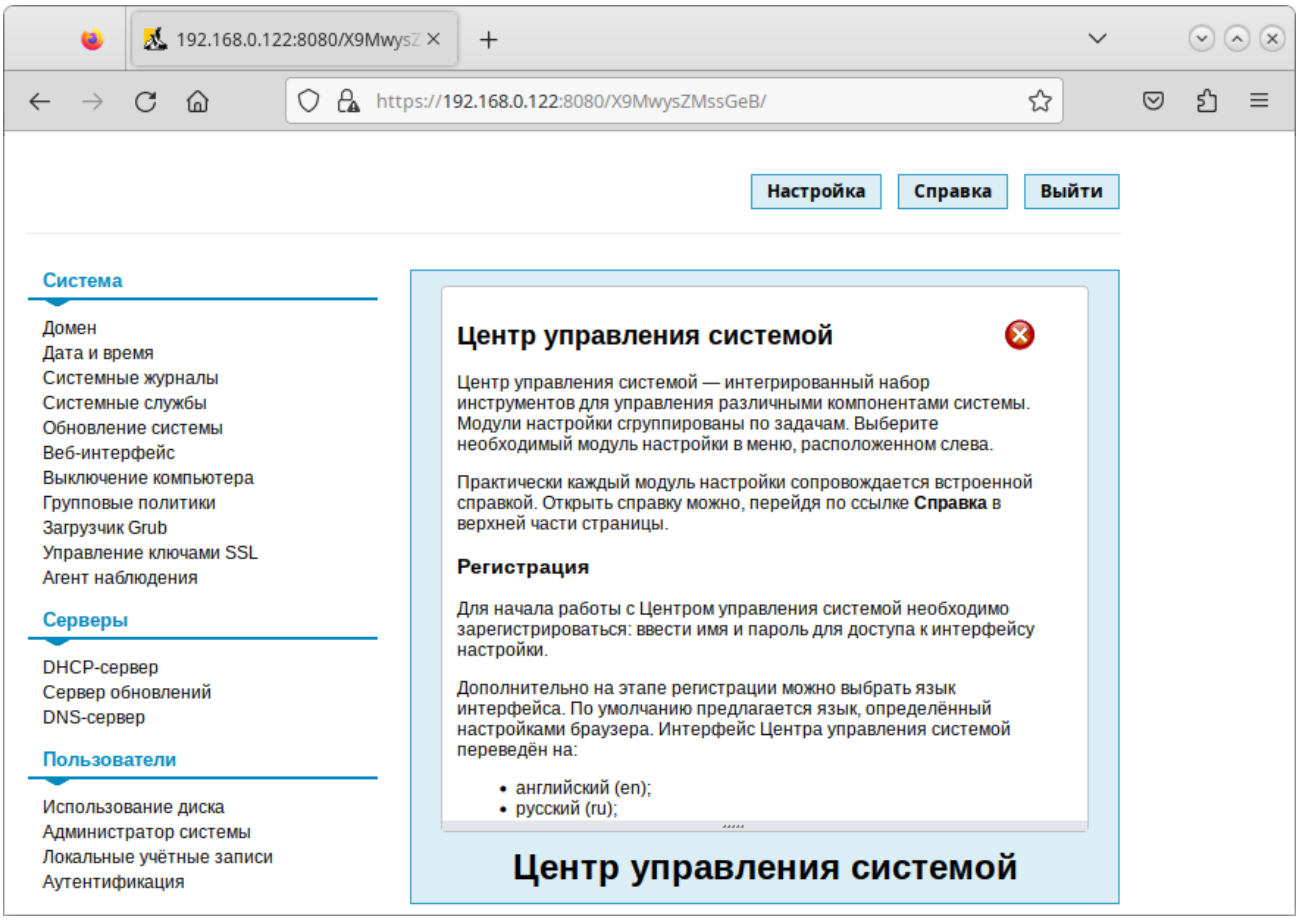


Рис. 12

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

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 «Средства удаленного администрирования».

3.2 Настройка сети

3.2.1 NetworkManager

Для управления настройками сети в ОС «Альт Сервер» может использоваться 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.

NetworkManager доступен как апплет, находящийся в системном лотке.

При нажатии левой кнопкой мыши на значок NetworkManager, появляется меню, в котором можно выбрать одну из доступных сетей и подключиться к ней. Из этого меню также можно отключить активное Wi-Fi соединение или установить VPN соединение (Рис. 13).

NetworkManager

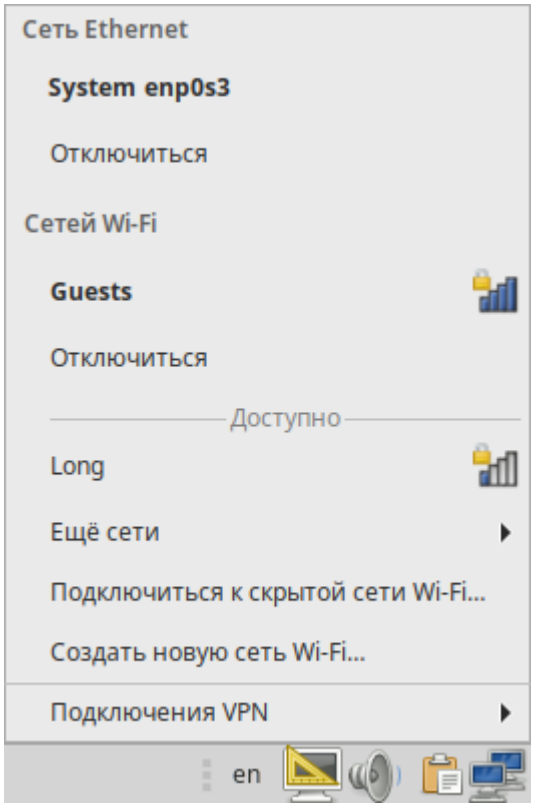


Рис. 13

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 контекстное меню, из которого можно получить доступ к изменению некоторых настроек (Рис. 14). Здесь можно посмотреть версию программы, получить сведения о соединении, изменить соединения (например, удалить Wi-Fi сеть, чтобы не подключаться к ней автоматически).

Контекстное меню NetworkManager

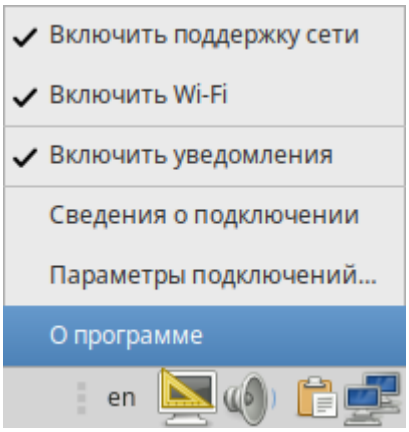


Рис. 14

Для того чтобы просмотреть информацию о сетевом соединении, следует в меню NetworkManager, вызываемом нажатием правой кнопкой мыши, выбрать пункт «Сведения о подключении». Сведения об активных соединениях будут отображены в диалоговом окне, каждое в отдельной вкладке (Рис. 15).

Информация о сетевом соединении

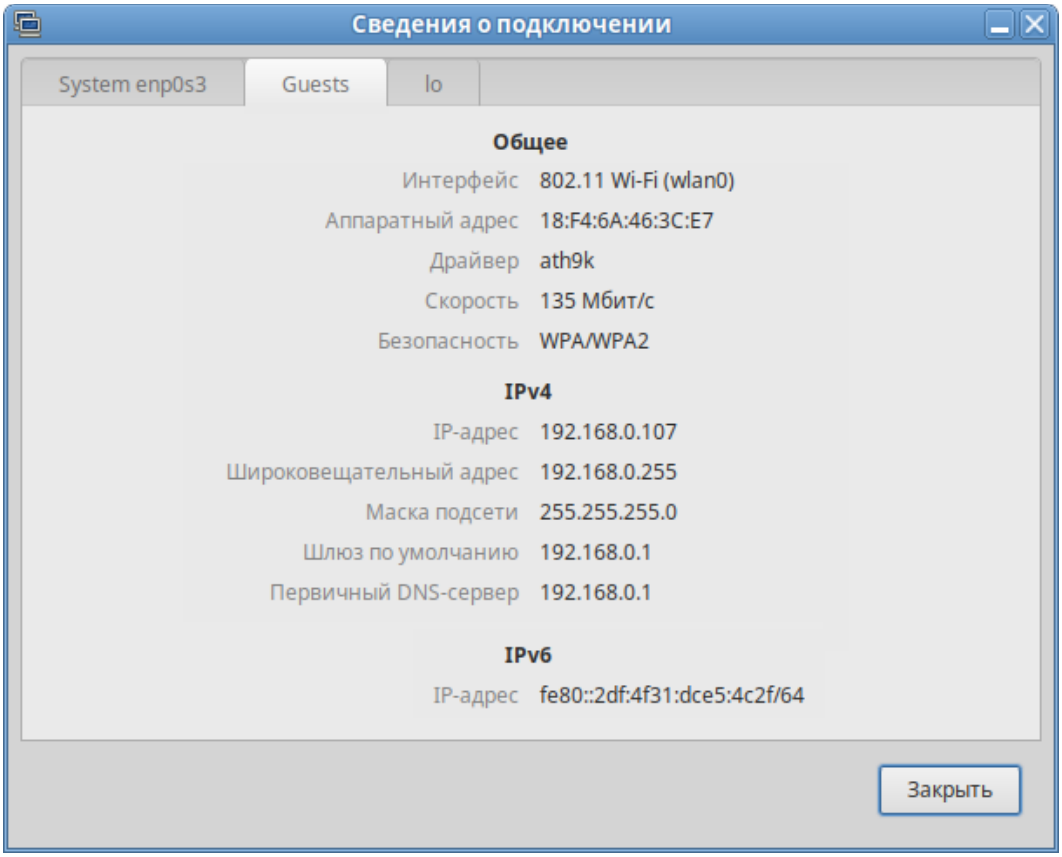


Рис. 15

Для настройки соединений, следует в меню NetworkManager, вызываемом нажатием правой кнопкой мыши, выбрать пункт «Параметры подключений». В открывшемся окне будет показан

сгруппированный по типам список соединений. Необходимо выбрать нужную сеть и нажать кнопку «Редактировать выбранное подключение» (Рис. 16).

Изменение настроек сетевых соединений

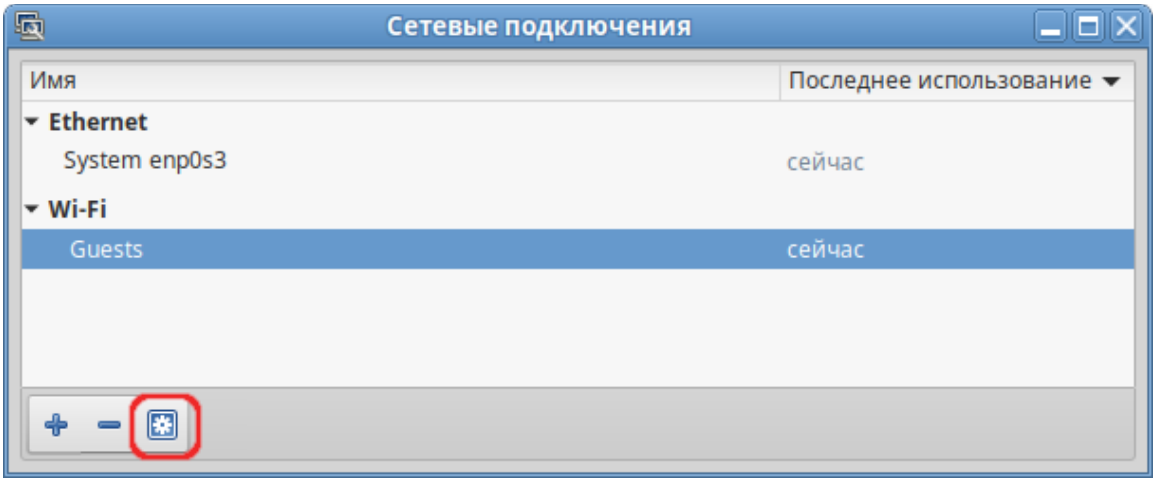


Рис. 16

В открывшемся окне можно изменить настройки сетевого интерфейса (Рис. 17).

Окно изменения настроек сетевого интерфейса

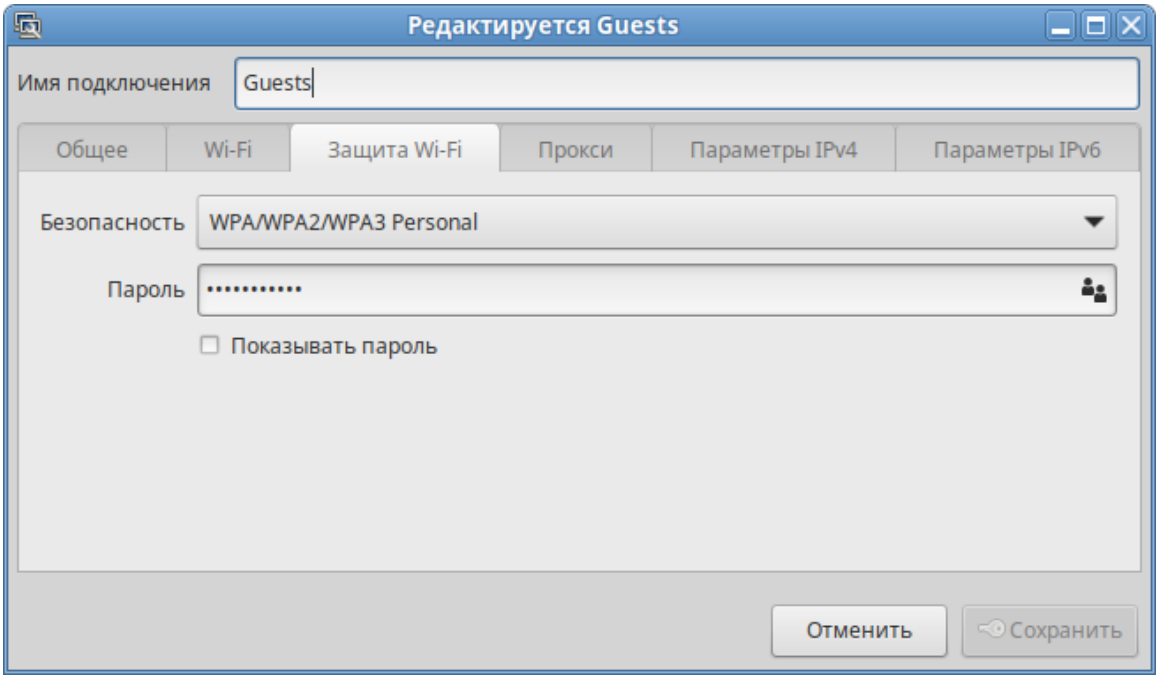


Рис. 17

Примечание. NetworkManager под именем «System enp0s3» показывает системное Ethernet-соединение, создаваемое Etcnet. Изменить его в диалоге «Сетевые подключения» невозможно. Это соединение можно изменить в ЦУС, там же можно выбрать, какой именно интерфейс, какой подсистемой обслуживается (подробнее о выборе сетевой подсистемы рассказано в разделе «Конфигурирование сетевых интерфейсов»).

3.2.2 Настройка в ЦУС

Настройку сети можно выполнить в ЦУС в разделе «Сеть» → «Ethernet интерфейсы». Здесь можно задать как глобальные параметры сети (адрес сервера DNS, имя компьютера), так и настройки конкретного сетевого интерфейса.

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

3.3 Режим киоск по ограничению запуска программ

В режиме киоск пользователь имеет право запускать программы, только явно разрешенные администратором.

3.3.1 Настройка ограничения в ЦУС

Примечание. Для работы киоска должны быть установлены пакеты alterator-kiosk и kiosk-mate-profiles:

```
# apt-get install alterator-kiosk kiosk-mate-profiles
```

Для включения режима киоск необходимо в ЦУС перейти в раздел «Система» → «Настройка kiosk».

Для разрешения запуска определенных приложений, необходимо выбрать соответствующий профиль из списка «Профили», установить отметку в поле «Включён» (Рис. 18).

Настройка kiosk

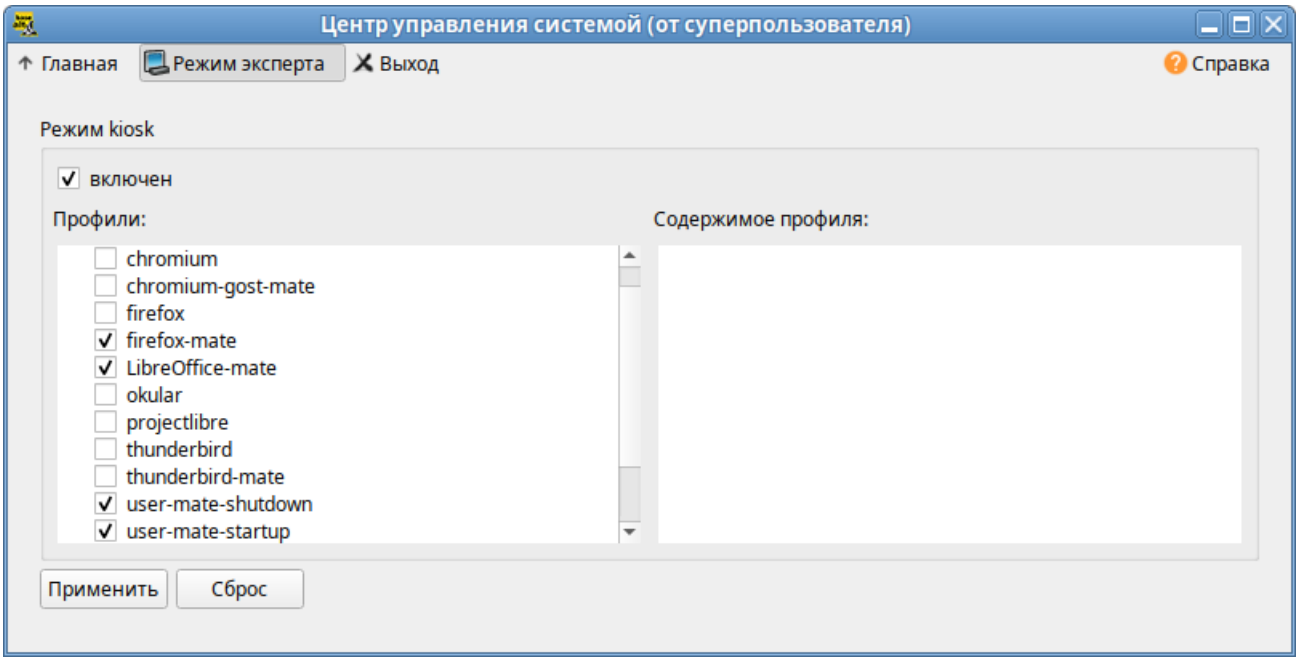


Рис. 18

Для корректной работы киоска обязательно должны быть выбраны профили user-mate-startup и user-mate-shutdown.

Примечание. Необходимо выбирать профили, в имени которых присутствует подстрока «mate».

Режим киоск будет активирован после нажатия кнопки «Применить».

Список приложений, из которых состоит профиль, можно увидеть в окне «Содержимое профиля» (Рис. 19). Профиль выделяется щелчком любой кнопки мыши.

Содержимое профиля

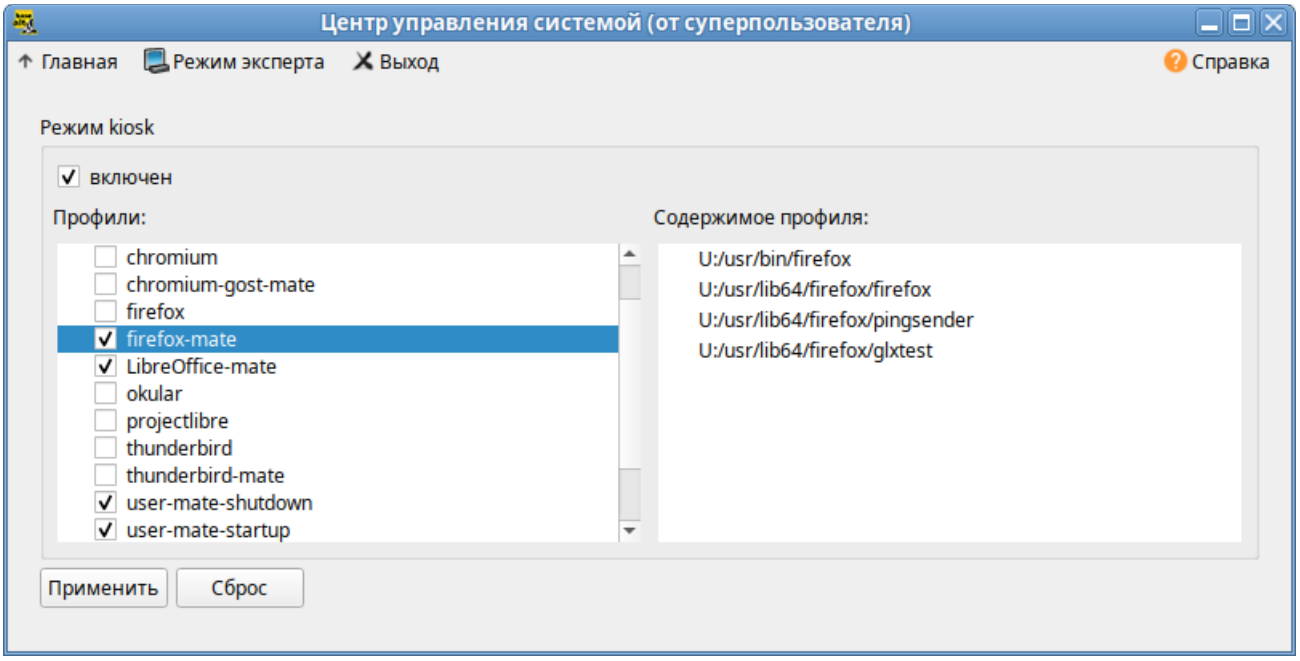


Рис. 19

Примечание. Для создания нового профиля необходимо создать файл в каталоге /etc/alterator/kiosk/profiles/ и вписать в него разрешённые к запуску программы. Например, для создания профиля atril, достаточно в файл /etc/alterator/kiosk/profiles/atril добавить строку:

```
U /usr/bin/atril
```

Для выключения режима киоск необходимо зарегистрироваться в системе под пользователем root (например, на второй консоли <Ctrl>+<Alt>+<F2>), выполнить команду:

```
# echo "0" > /etc/alterator/kiosk/mode
```

и перезагрузить систему.

3.3.2 Управление режимом киоск в консоли

Для управления режимом киоск можно воспользоваться командой `kiosk`. Все команды выполняются с правами администратора.

Примечание. Утилита kiosk используется для временного включения/отключения режима киоск. После перезагрузки компьютера будет включён тот режим, который был установлен в модуле ЦУС «Настройка kiosk».

Примеры использования команды kiosk:

- просмотреть пути в белом списке:

```
# kiosk --user-list
/bin/basename
/bin/dbus-daemon
/bin/dbus-update-activation-environment
/bin/false
…
```

- добавить указанный путь в белый список:

```
# kiosk --user-list-append /путь
```

- удалить указанный путь из белого списка:

```
# kiosk --user-list-remove /путь
```

- активировать режим киоск:

```
# kiosk --set-mode 1
```

- деактивировать режим киоск:

```
# kiosk --set-mode 0
```

- просмотреть состояние режима:

```
# kiosk --get-mode
```

4 СРЕДСТВА УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

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. 20).

Настройка модуля «Ethernet-интерфейсы»

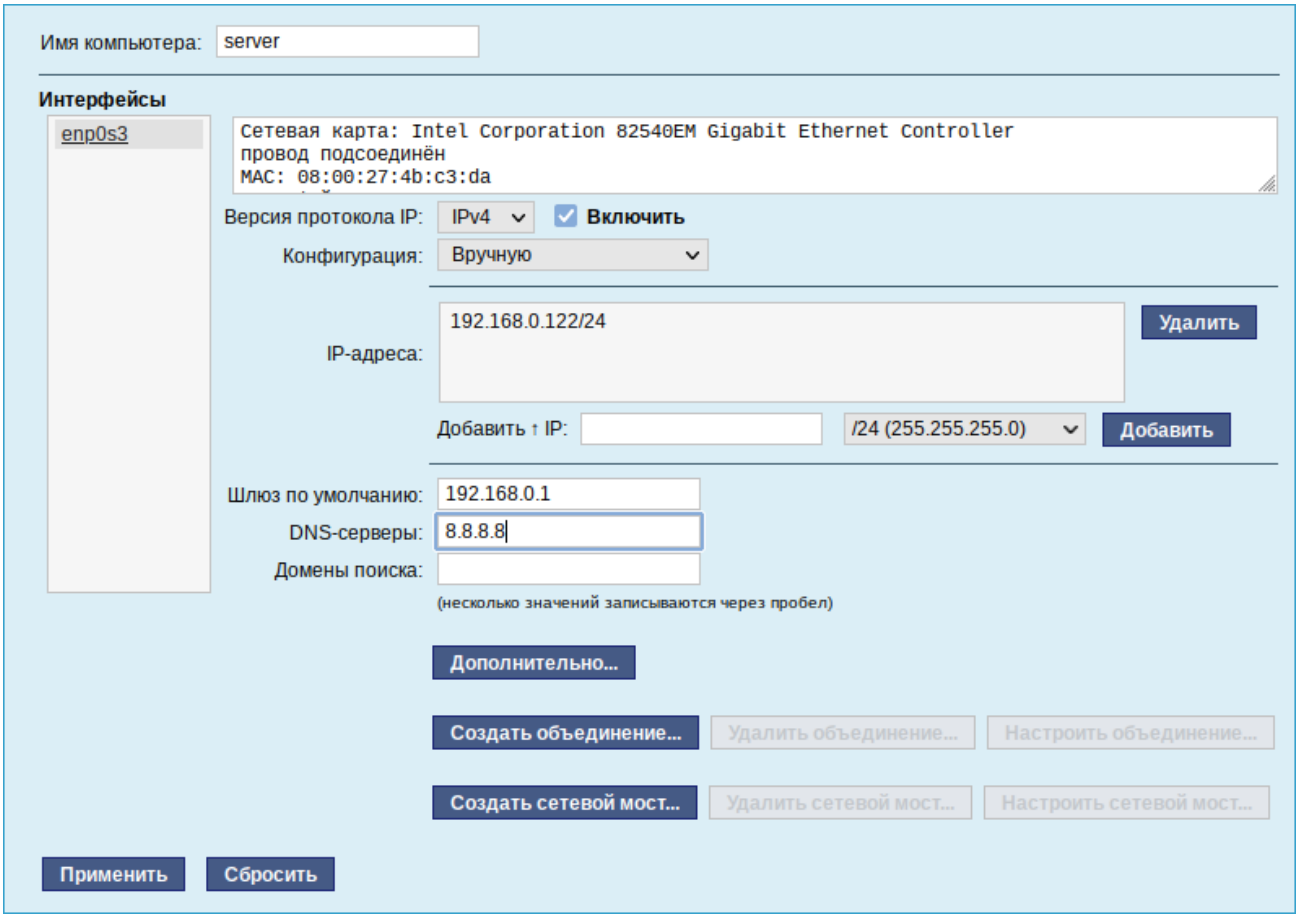


Рис. 20

В модуле «Ethernet-интерфейсы» можно заполнить следующие поля:

- «Имя компьютера» – указать сетевое имя компьютера (это общий сетевой параметр, не привязанный к какому либо конкретному интерфейсу);
- «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 «Добавить ↑ IP», выбранные адреса можно удалить нажатием кнопки «Удалить»;
- «Добавить ↑ 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. 21).

Автоматическое получение настроек от DHCP сервера

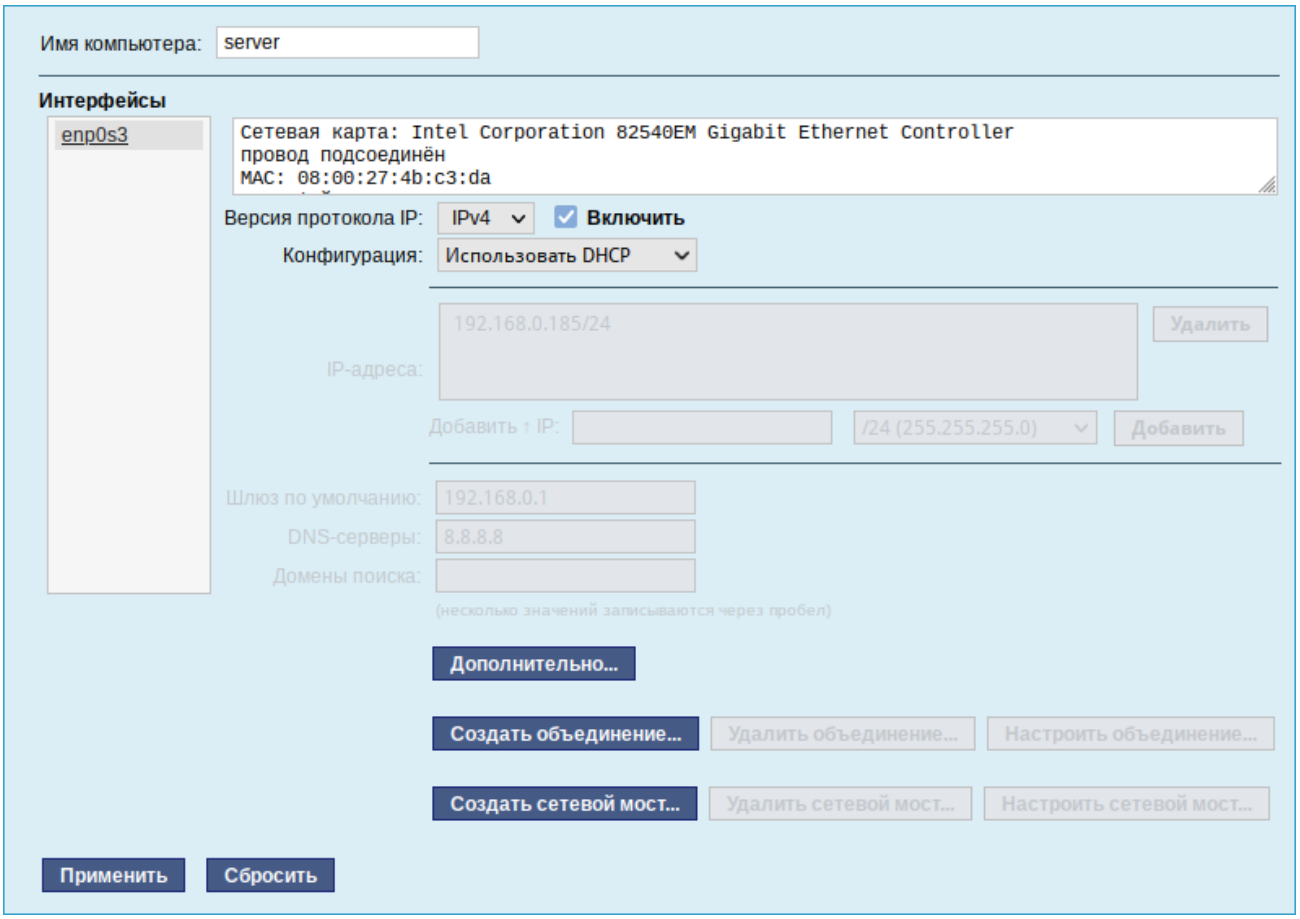


Рис. 21

Дополнительно для каждого интерфейса можно настроить сетевую подсистему (NetworkManager, Etcnet, systemd-networkd), а также должен ли запускаться данный интерфейс при загрузке системы (Рис. 22).

Примечание. Список доступных сетевых подистем зависит от пакетов, выбранных на этапе «Установка системы» (группа пакетов «Система управления сетевыми интерфейсами»).

Выбор сетевой подсистемы

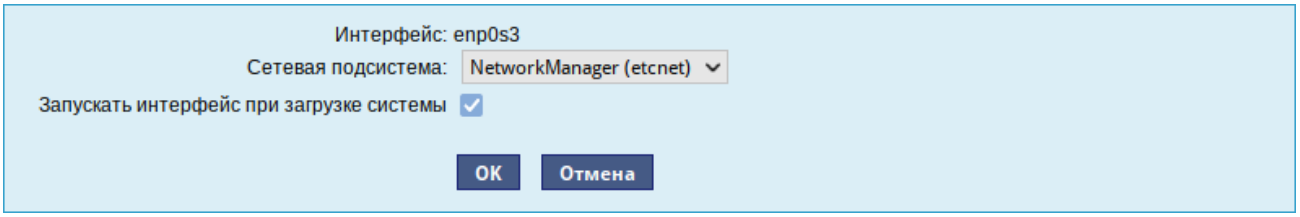


Рис. 22

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;
- «system-networkd» – в данном режиме управление настройками интерфейса передаётся службе `systemd-networkd`. Данный режим доступен, если установлен пакет `systemd-networkd`. Настройки сети могут изменяться либо в ЦУС в данном модуле (только настройки физического интерфейса), либо напрямую через редактирование файлов `/etc/systemd/network/<имя_файла>.network`, `/etc/systemd/network/<имя_файла>.netdev`, `/etc/systemd/network/<имя_файла>.link`;
- «Не контролируется» – в этом режиме интерфейс находится в состоянии DOWN (выключен).

После смены сетевой подсистемы с `Etcnet` на `systemd-networkd` может потребоваться вручную отключить службу `network` и включить `systemd-networkd`:

```
# systemctl disable --now network && systemctl enable --now systemd-networkd
```

И, наоборот, при смене с `systemd-networkd` на `Etcnet` отключить службу `systemd-networkd` и включить `network`:

```
# systemctl disable --now systemd-networkd && systemctl enable --now network
```

4.1.2 Объединение сетевых интерфейсов

Модуль «Объединение интерфейсов» (пакет `alterator-net-bond`) позволяет объединить несколько физических сетевых интерфейсов в один логический. Это позволяет достичь отказоустойчивости, отказоустойчивости, увеличения скорости и балансировки нагрузки.

Для создания объединения интерфейсов необходимо выполнить следующие действия:

1) нажать кнопку «Создать объединение» (Рис. 23);

1) переместить сетевые интерфейсы, которые будут входить в объединение, из списка «Доступные интерфейсы» в список «Используемые интерфейсы» (Рис. 24);

2) выбрать режим объединения:

- «Round-robin» – режим циклического выбора активного интерфейса для исходящего трафика;
- «Активный-резервный» – активен только один интерфейс, остальные находятся в режиме горячей замены;
- «XOR» — один и тот же интерфейс работает с определённым получателем, передача пакетов распределяется между интерфейсами на основе формулы *((MAC-адрес источника) XOR (MAC-адрес получателя)) % число интерфейсов*;
- «Широковещательная» – трафик идёт через все интерфейсы одновременно;
- «Агрегирование каналов по стандарту IEEE 802.3ad» – в группу объединяются одинаковые по скорости и режиму интерфейсы, все физические интерфейсы используются одновременно в соответствии со спецификацией IEEE 802.3ad. Для реализации этого режима необходима поддержка на уровне драйверов сетевых карт и коммутатор, поддерживающий стандарт IEEE 802.3ad (коммутатор требует отдельной настройки);
- «Адаптивная балансировка нагрузки передачи» – исходящий трафик распределяется в соответствии с текущей нагрузкой (с учётом скорости) на интерфейсах (для данного режима необходима его поддержка в драйверах сетевых карт). Входящие пакеты принимаются только активным сетевым интерфейсом;
- «Адаптивная балансировка нагрузки» – включает в себя балансировку исходящего трафика и балансировку на приём (rlb) для IPv4 трафика и не требует применения специальных коммутаторов. Балансировка на приём достигается на уровне протокола ARP путём перехвата

ARP ответов локальной системы и перезаписи физического адреса на адрес одного из сетевых интерфейсов (в зависимости от загрузки);

3) указать, если это необходимо, параметры объединения в поле «Параметры объединения»;

4) нажать кнопку «Назад»;

5) в результате будет создан агрегированный интерфейс bond0. Для данного интерфейса можно задать IP-адрес и, если необходимо, дополнительные параметры (Рис. 25);

6) нажать кнопку «Применить».

Объединение интерфейсов в веб-интерфейсе alterator-net-eth

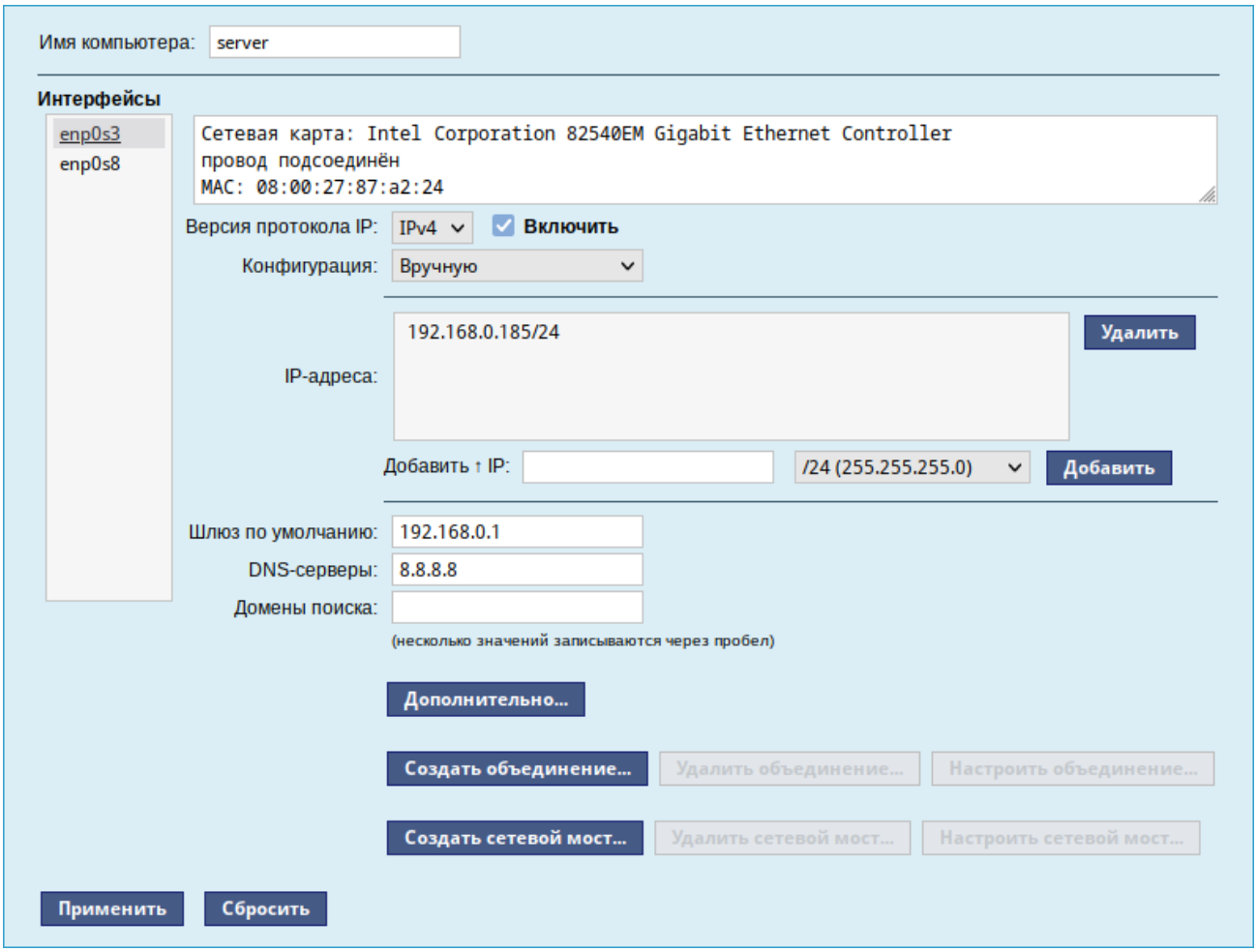


Рис. 23

Выбор сетевых интерфейсов для объединения

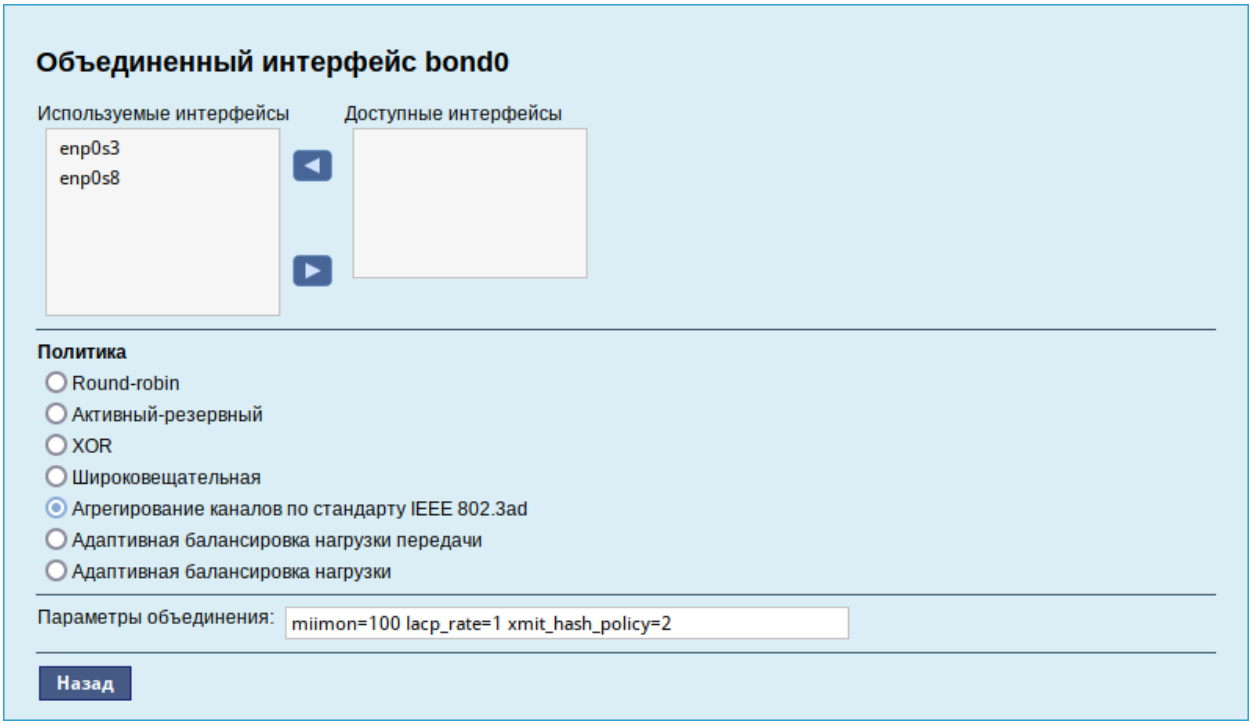


Рис. 24

Настройки интерфейса bond0

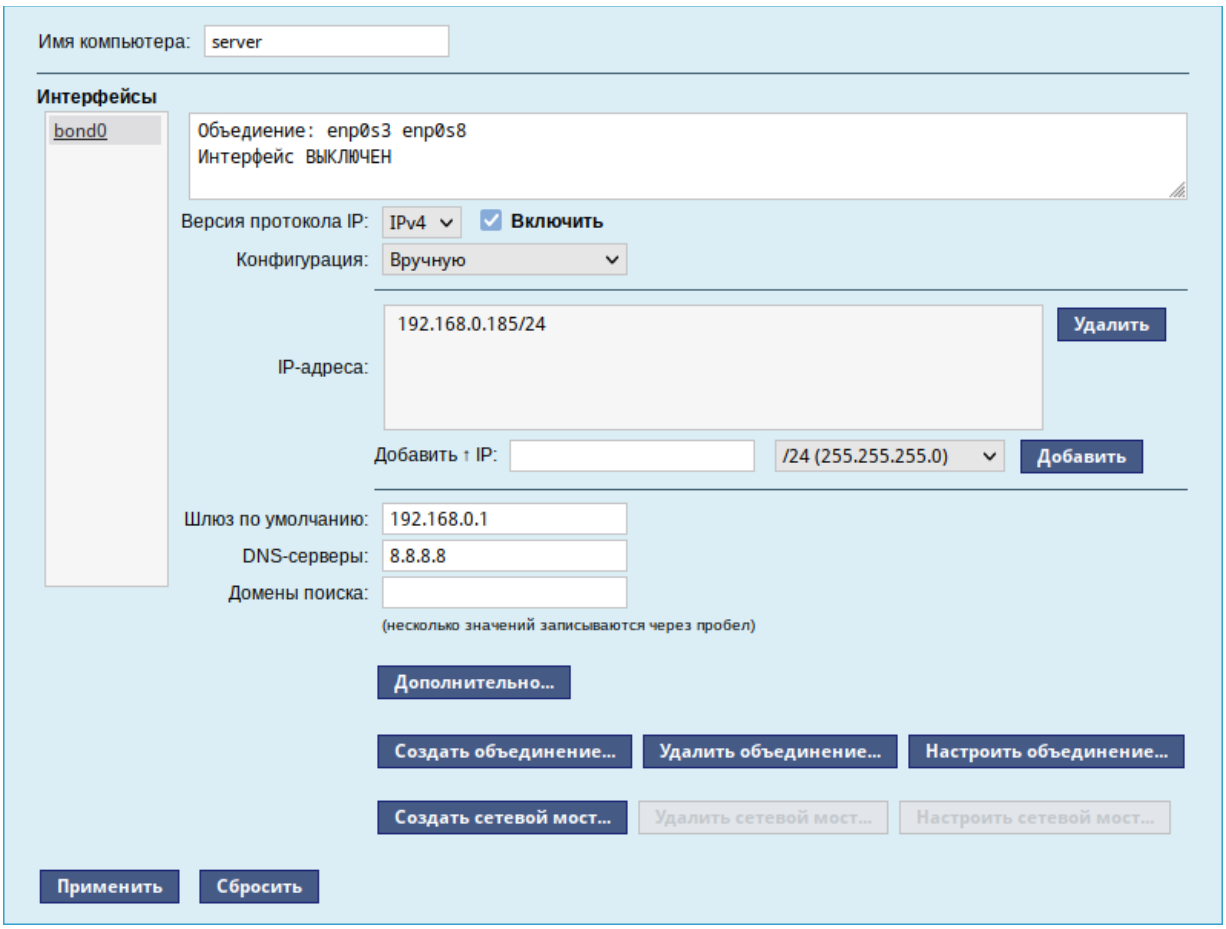


Рис. 25

Информацию о получившемся агрегированном интерфейсе можно посмотреть в `/proc/net/bonding/bond0`.

Для удаления агрегированного интерфейса необходимо выбрать его в списке «Интерфейсы» и нажать кнопку «Удалить объединение…».

4.1.3 Сетевые мосты

Модуль «Сетевые мосты» (пакет `alterator-net-bridge`) позволяет организовать виртуальный сетевой мост.

Примечание. Если интерфейсы, входящие в состав моста, являются единственными физически подключенными и настройка моста происходит с удалённого узла через эти интерфейсы, то требуется соблюдать осторожность, так как эти интерфейсы перестанут быть доступны.

Для создания Ethernet-моста необходимо выполнить следующие действия:

1) у интерфейсов, которые будут входить в мост, удалить IP-адреса и шлюз по умолчанию (если они были установлены);

2) нажать кнопку «Создать сетевой мост» (Рис. 26);

Настройка сети в веб-интерфейсе

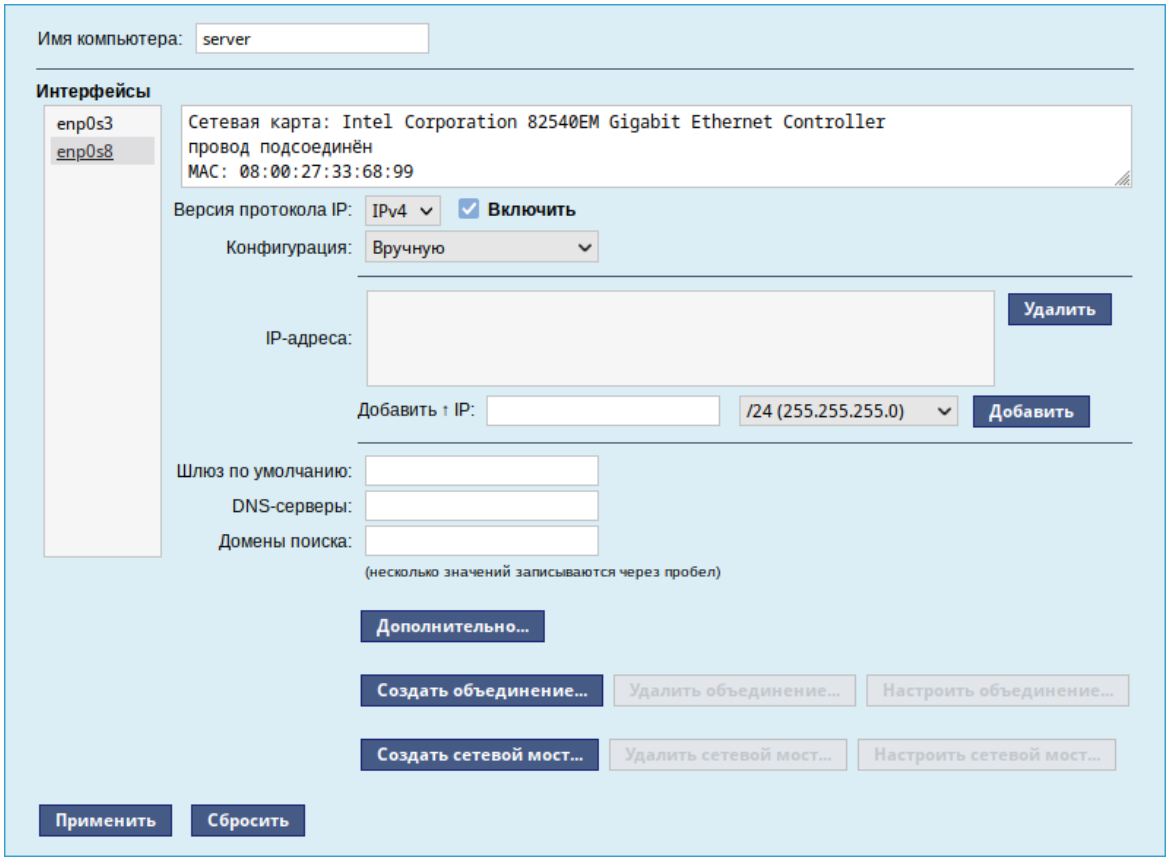


Рис. 26

3) в окне «Сетевые мосты» в поле «Интерфейс-мост» ввести имя моста;

4) в выпадающем списке «Тип моста» выбрать тип моста: «Linux Bridge» (по умолчанию) или «Open vSwitch»;

5) переместить сетевые интерфейсы, которые будут входить в мост, из списка «Доступные интерфейсы» в список «Члены»;

6) нажать кнопку «Ок» (Рис. 27);

7) в результате будет создан сетевой интерфейс моста (в примере vmbr0). Для данного интерфейса можно задать IP-адрес и, если необходимо, дополнительные параметры (Рис. 28);

8) нажать кнопку «Применить».

Выбор сетевого интерфейса

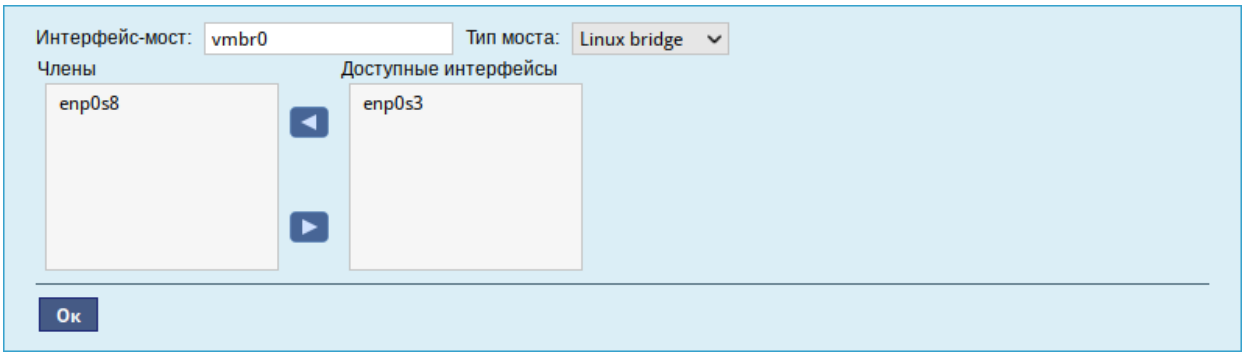


Рис. 27

Настройка параметров сетевого интерфейса vmbr0

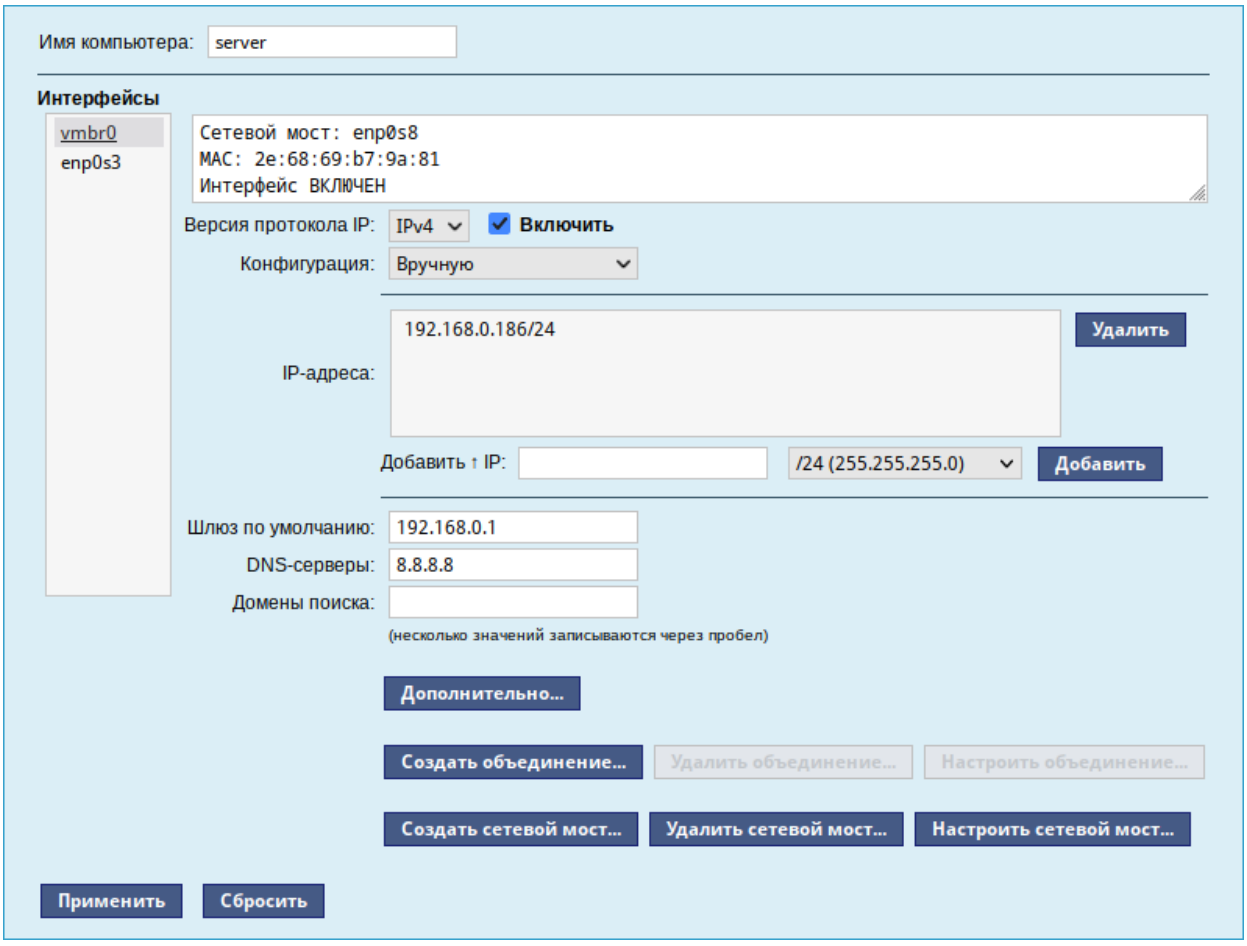


Рис. 28

Для удаления интерфейса моста, необходимо выбрать его в списке «Интерфейсы» и нажать кнопку «Удалить сетевой мост…».

4.1.4 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.

4.1.4.1 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. 29).

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. 30).

Модуль «Прокси-сервер»

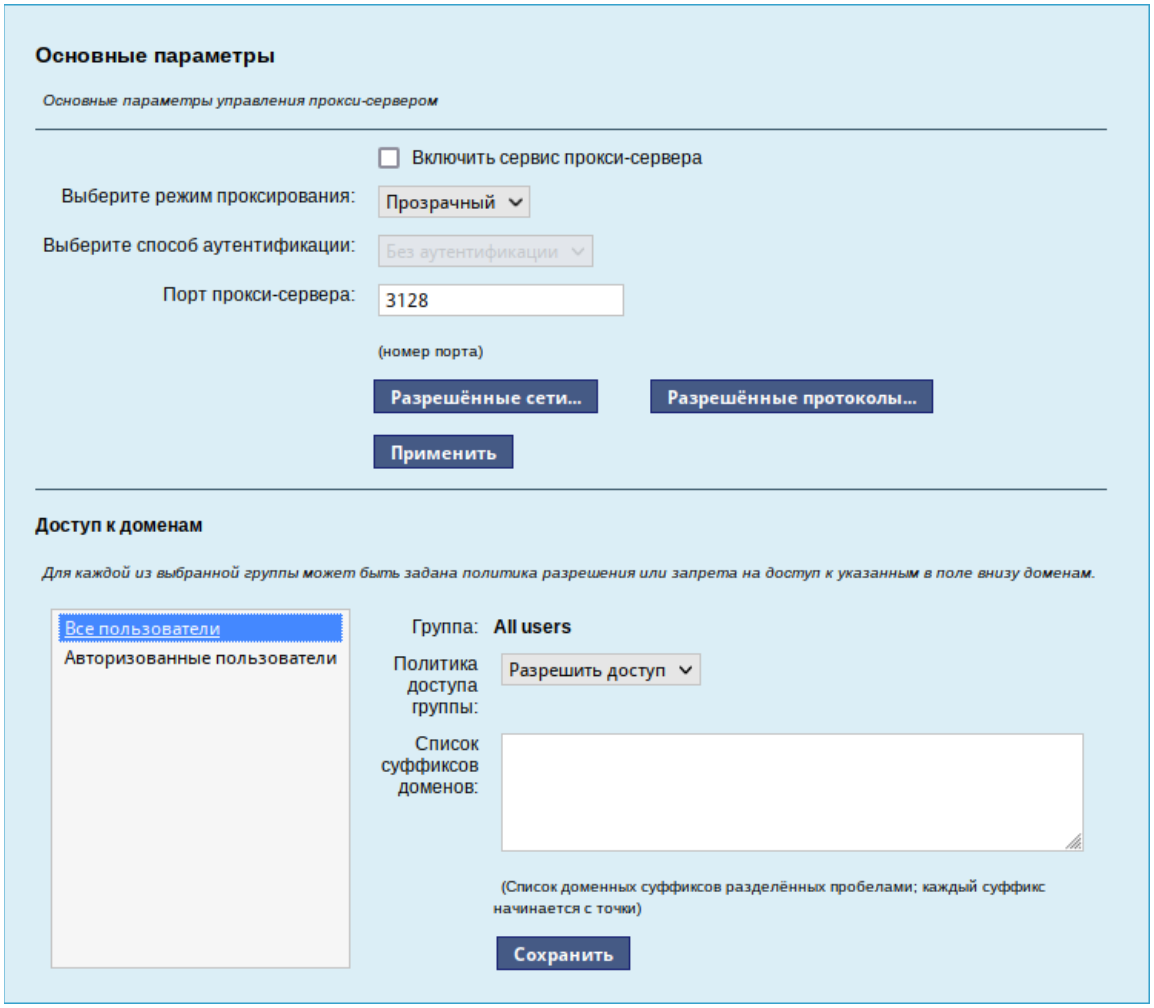


Рис. 29

Настройка аутентификации пользователей

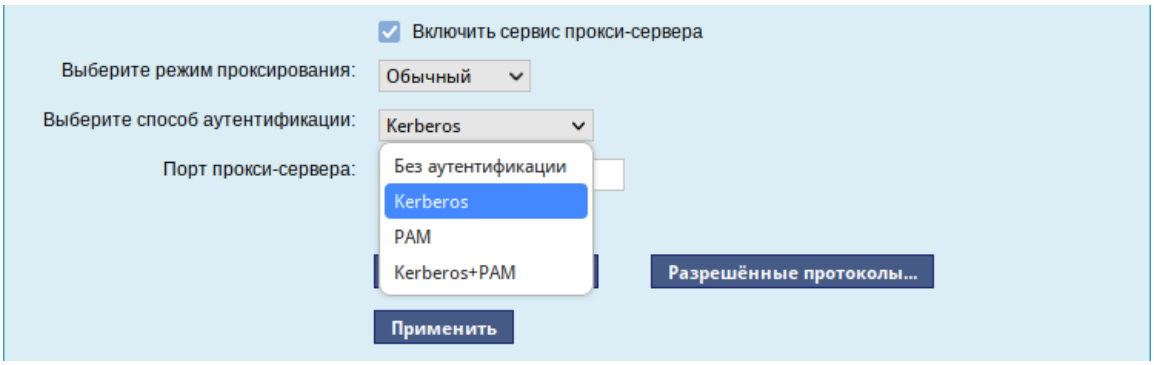


Рис. 30

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. 31).

Настройка списка внутренних сетей

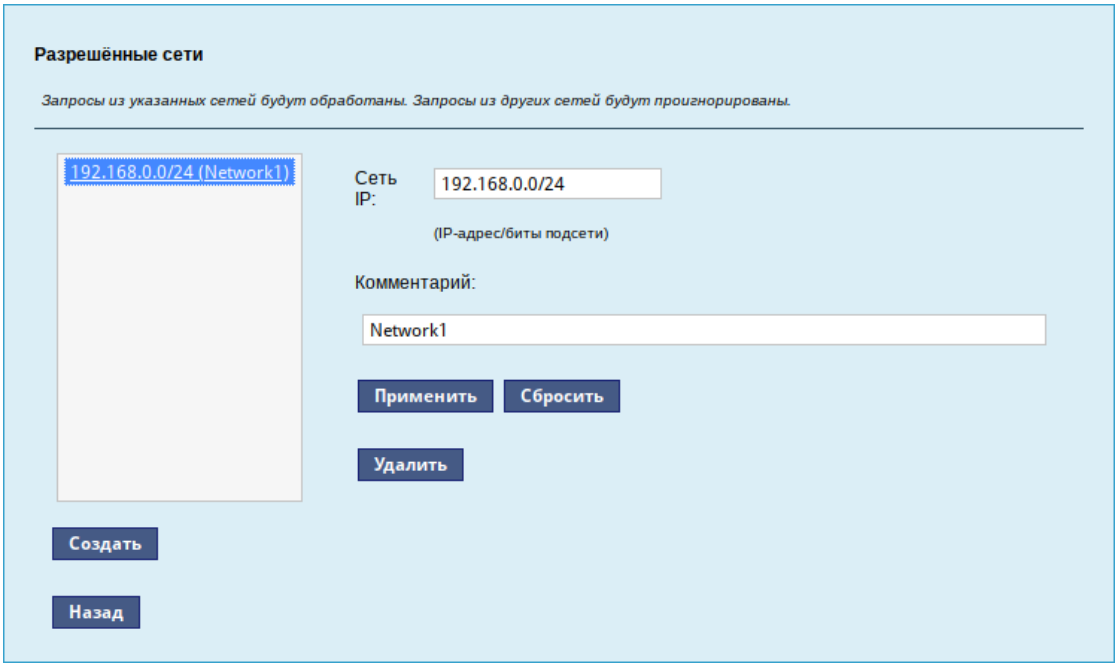


Рис. 31

Вторым условием передачи запроса является принадлежность целевого порта к разрешённому диапазону. Посмотреть и отредактировать список разрешённых целевых портов можно в разделе «Разрешённые протоколы» (Рис. 32).

Настройка списка разрешённых целевых портов

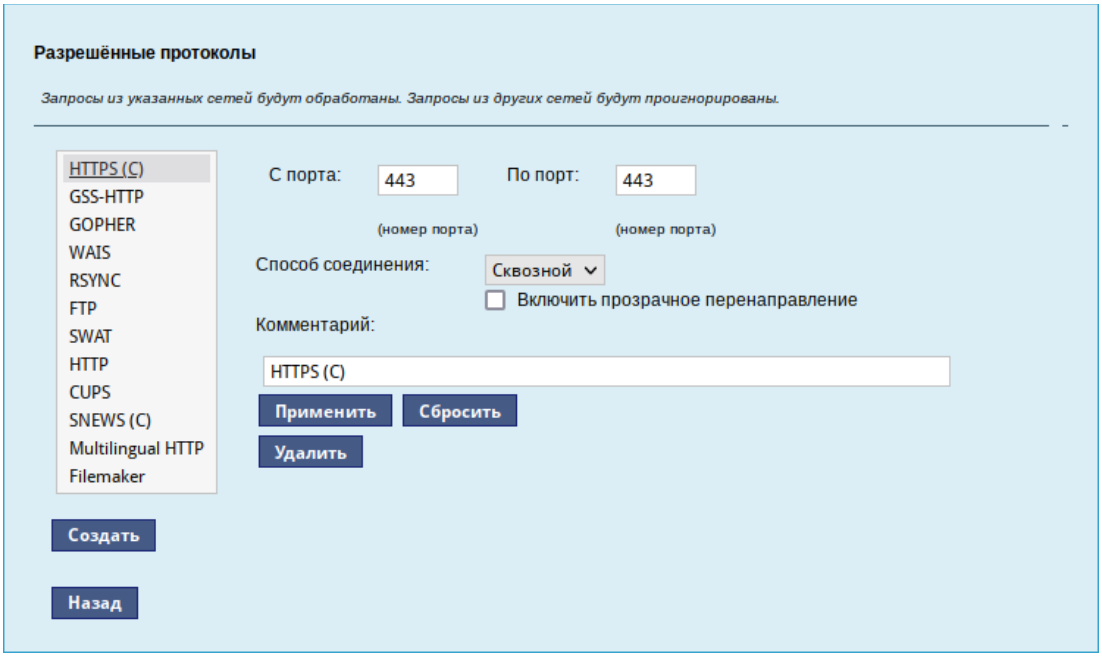


Рис. 32

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.

4.1.4.2 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. 33) и нажать на кнопку «Применить».

Настройка NAT в модуле «Внешние сети»

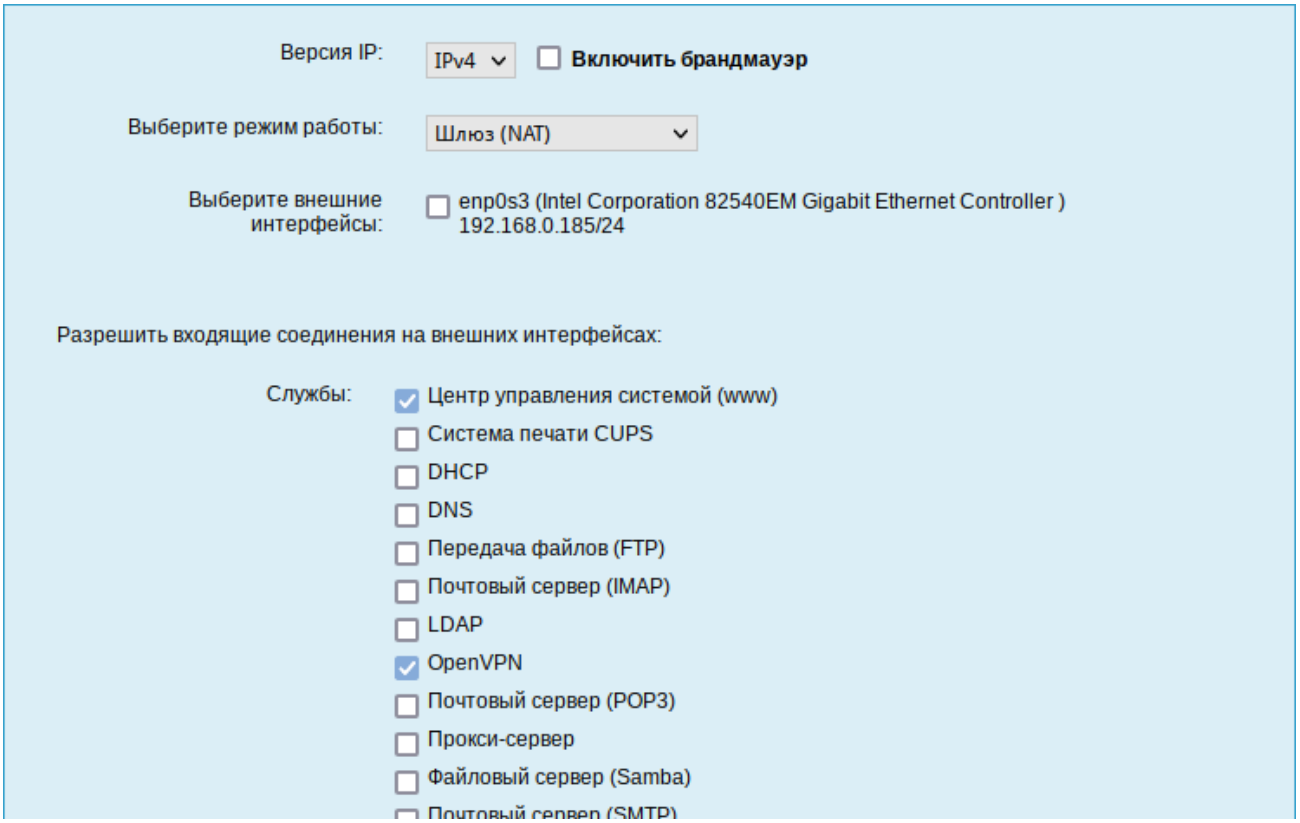


Рис. 33

4.1.5 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. 34), указать начальный и конечный IP-адрес, а также шлюз по умолчанию (обычно это IP-адрес сервера на сетевом интерфейсе, обслуживающем локальную сеть).

Настройка модуля DHCP-сервер

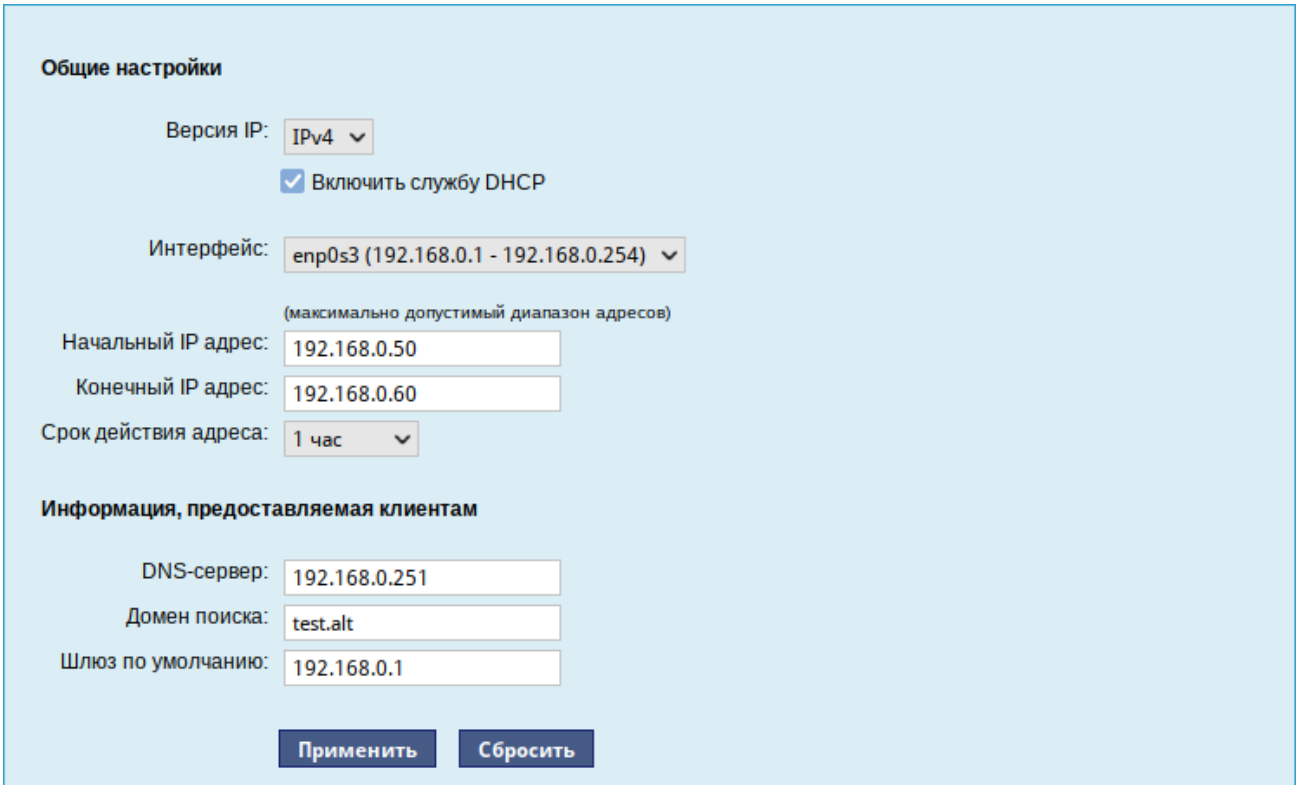


Рис. 34

Теперь при включении любой клиентской машины с настройкой «получение IP и DNS автоматически» будет присваиваться шлюз 192.168.0.1, DNS 192.168.0.251 и адреса начиная с 192.168.0.50 по порядку включения до 192.168.0.60.

Иногда бывает полезно выдавать клиенту один и тот же IP-адрес независимо от момента обращения. В этом случае он определяется по аппаратному адресу (MAC-адресу) сетевой карты

клиента. Для добавления своих значений в таблицу соответствия статических адресов следует ввести IP-адрес и соответствующий ему MAC-адрес и нажать кнопку «Добавить» (Рис. 35).

Привязка IP-адреса к MAC-адресу

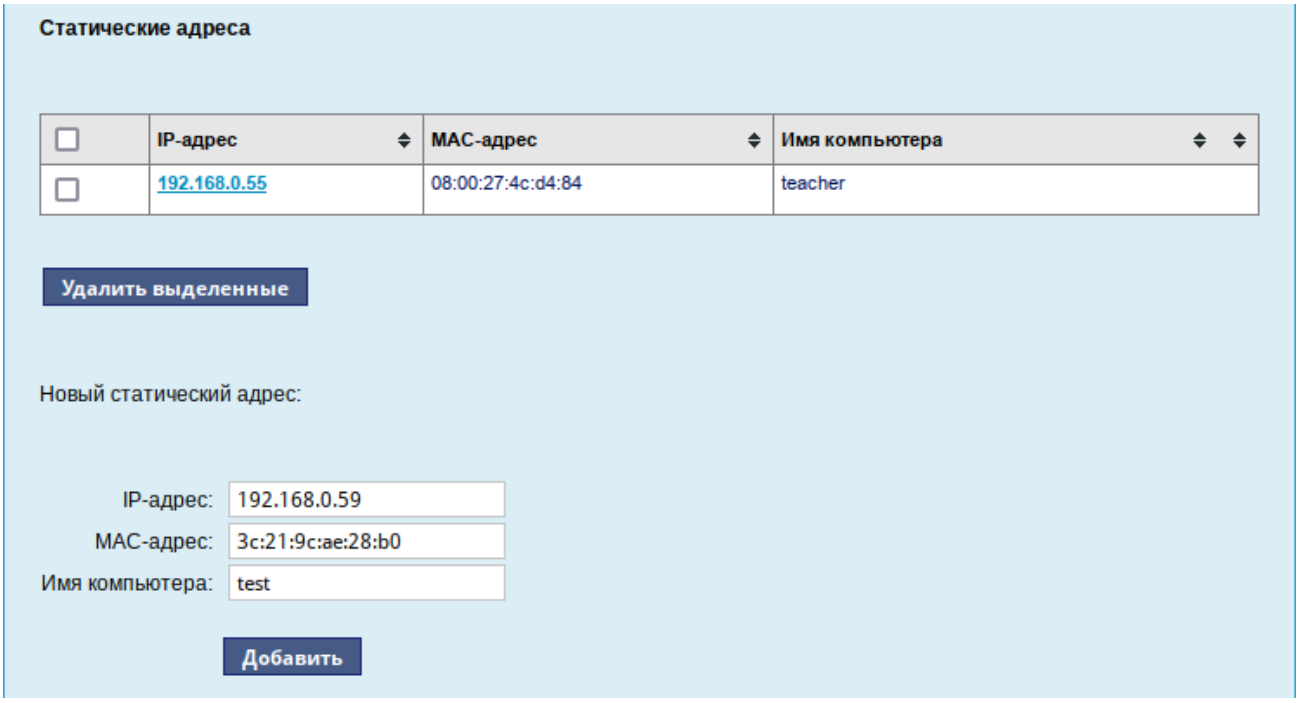


Рис. 35

Выданные IP-адреса можно увидеть в списке «Текущие динамически выданные адреса» (Рис. 36). 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

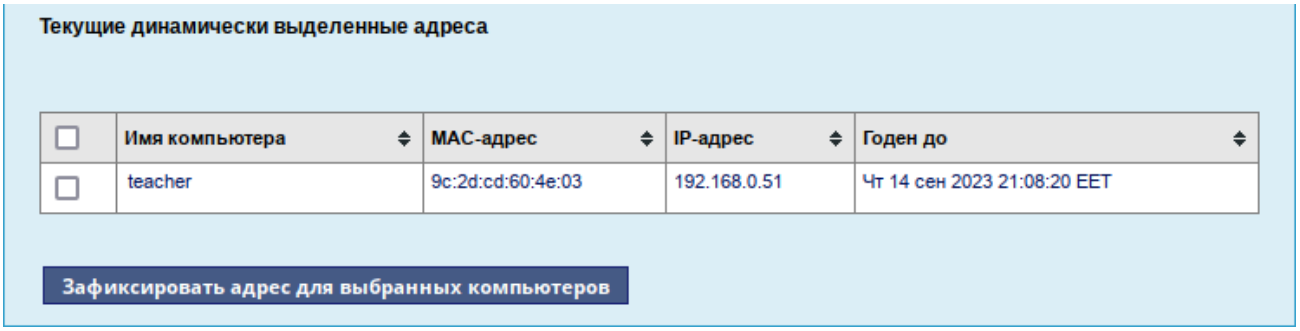


Рис. 36

4.2 Развертывание доменной структуры

Для развертывания доменной структуры предназначен модуль ЦУС «Домен» из раздела «Система» (пакет `alterator-net-domain`) (Рис. 37).

Настройка модуля «Домен»

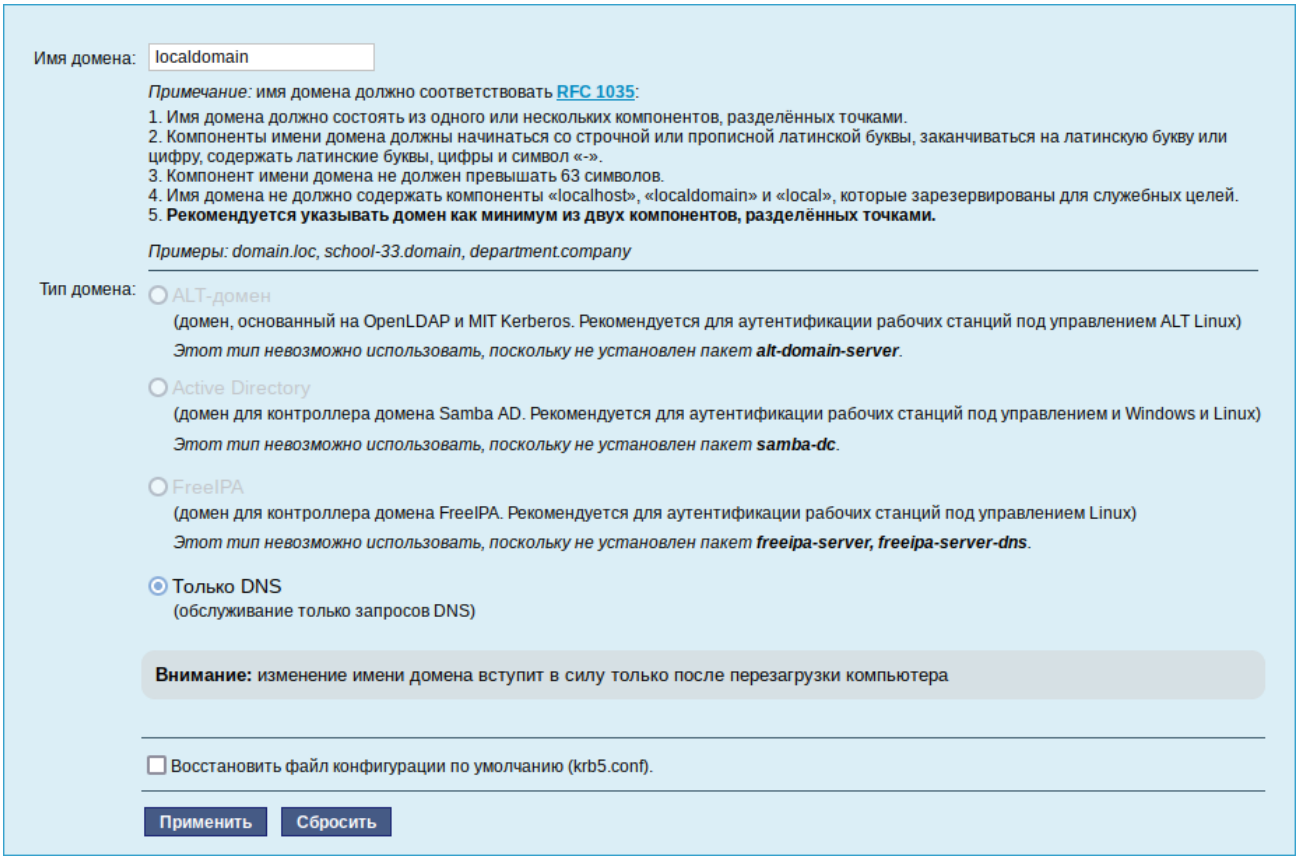


Рис. 37

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. Каталог `/var/lib/tftpboot` должен быть доступен клиенту через TFTP, каталог `/srv/public/netinst` должен быть доступен клиенту через NFS.

Примечание. В настоящий момент модуль «Сервер сетевых установок» не позволяет настроить установку в EFI-режиме для PXE-установки.

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/p10/workstation/x86_64/alt-workstation-10.2-x86_64.iso.

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

В разделе «Сервер сетевых установок» (пакет `alterator-netinst`) (Рис. 38) необходимо указать, откуда импортировать новый образ, и нажать кнопку «Добавить».

Процесс добавления образа (Рис. 39) занимает какое-то время.

Выбор источника для импорта установочного образа

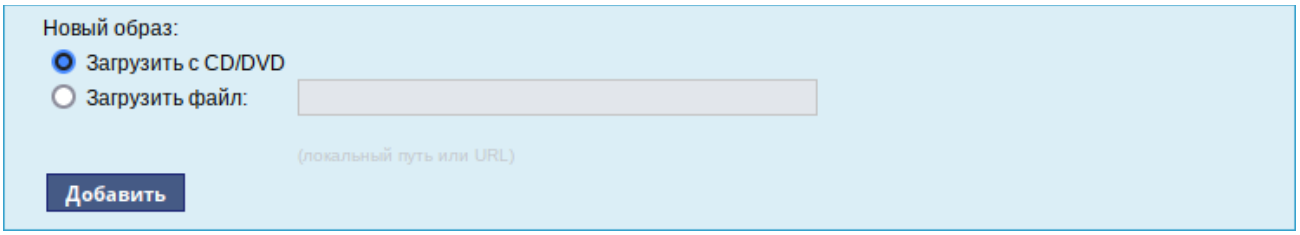


Рис. 38

Процесс добавления установочного образа

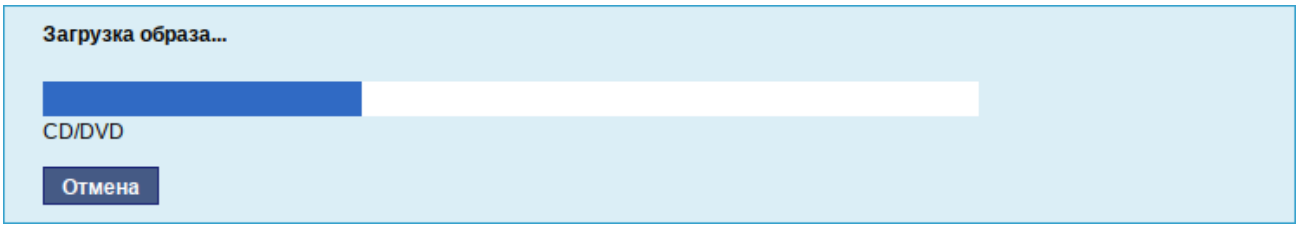


Рис. 39

После добавления образ появится в списке «Доступные образы дисков». Необходимо выбрать из списка один из образов (Рис. 40) и нажать кнопку «Выбрать».

Выбор образа диска

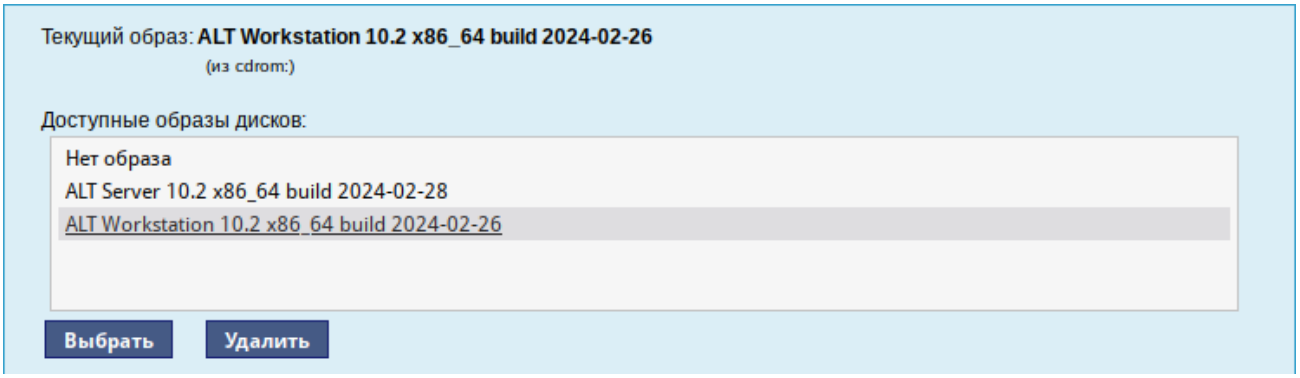


Рис. 40

На этом подготовка сервера к сетевой установке рабочих станций завершена.

Дополнительно данный модуль позволяет выбрать вариант загрузки (Рис. 41), например, непосредственно загружать ОС некоторых Live-версий дистрибутивов.

Выбор варианта загрузки

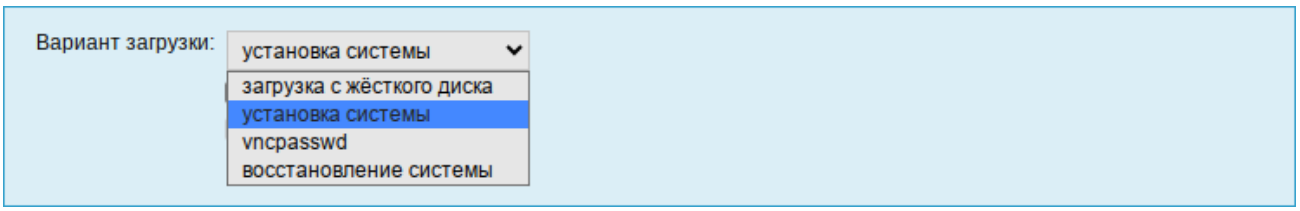


Рис. 41

Для включения режима автоматической установки необходимо выбрать образ, выбрать вариант загрузки «Установка системы», установить отметку в поле «Автоматическая установка», в поле «Метаданные» указать каталог с установочными файлами (Рис. 42) и сохранить настройки, нажав кнопку «Применить».

Включение режима автоматической установки

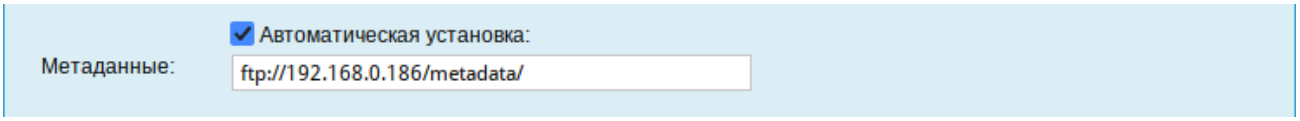


Рис. 42

Примечание. В alterator-netinst до версии 1.9.1-alt7 для включения режима автоматической установки необходимо выбрать образ, выбрать вариант загрузки «Установка системы» и сохранить настройки, нажав кнопку «Применить». Затем в файле `/var/lib/tftpboot/pxelinux.cfg/default` следует дописать параметр загрузки `ai` (без значения) и параметр `curl` с указанием каталога с установочными файлами, например:

```
label linux
  kernel syslinux//boot/vmlinuz
```

```
  append initrd=syslinux//boot/initrd.img fastboot changedisk  stage-
name=altinst ramdisk_size=648701 showopts vga=normal quiet splash au-
tomatic=method:nfs,network:dhcp tz=Europe/Kaliningrad  lang=ru_RU  vnc
vncpassword=123 ai curl=ftp://192.168.0.186/metadata/
```

Если отмечен пункт «Включить установку по VNC», то далее необходимо выбрать направление соединения (Рис. 43). 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

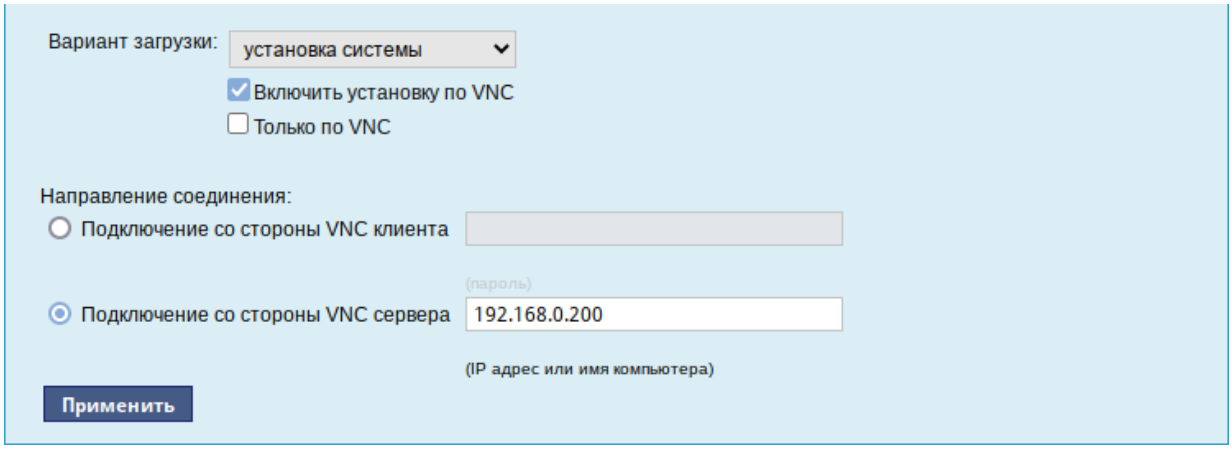


Рис. 43

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 указать в поле IP-адрес или имя 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 FTP-сервер

Модуль «FTP-сервер» (пакет `alterator-vsftpd`) из раздела «Серверы» (Рис. 44) предназначен для настройки FTP-сервера (`vsftpd`).

Настройка модуля «FTP-сервер»

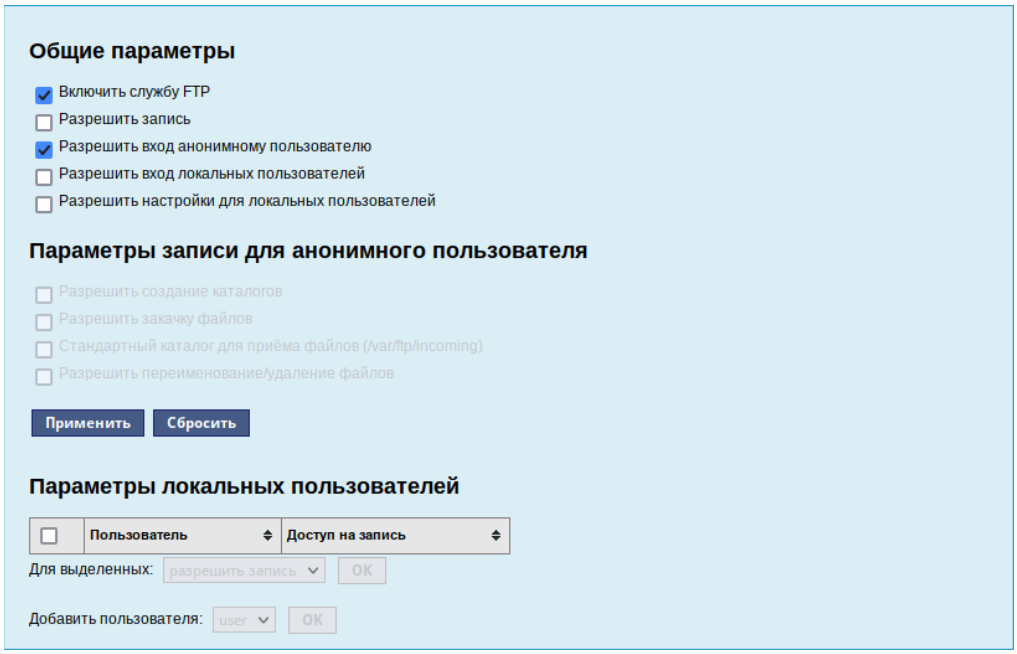


Рис. 44

Чаще всего протокол FTP (File Transfer Protocol) используется для организации файлового сервера с анонимным доступом. Возможность анонимного доступа управляется параметром «Разрешить вход анонимному пользователю». Менее распространённый вариант – сервер с возможностью загружать на него файлы, в том числе и анонимным пользователям. Возможность загрузки включается параметром «Разрешить запись». Еще один вариант – сервер, позволяющий локальным пользователям скачивать и загружать файлы из своих домашних каталогов. Этот вариант используется редко, что связано с небезопасностью протокола FTP. Возможность работы с локальными пользователями управляется параметром «Разрешить вход локальным

пользователям». Чтобы пользователи могли загружать файлы, требуется включить параметр «Разрешить запись». Разрешение на загрузку файлов можно настраивать индивидуально, для этого необходимо отметить параметр «Разрешить настройку локальных пользователей».

Если необходимо создать анонимный FTP-сервер, можно использовать vsftpd в сочетании с пакетом `anonftp`. В целях безопасности сервер по умолчанию сконфигурирован именно для предоставления анонимного доступа. Запрещены любые команды записи, а также доступ локально зарегистрированных пользователей.

При установке пакета `anonftp` автоматически создаётся каталог, который будет корневым при анонимном подключении, – `/var/ftp` с необходимыми правами доступа. Владельцем этого каталога является пользователь root, а не псевдопользователь, от имени которого работает `vsftpd`. Это сделано для обеспечения безопасности FTP-сервера и системы в целом. Группой-владельцем каталога является специальная группа ftpadmin, предназначенная для администраторов FTP-сервера.

Многие параметры использования FTP-сервера, в том числе относящиеся к безопасности, могут быть заданы при помощи xinetd (демона Интернет-служб). В частности, этот сервер позволяет ограничить количество одновременно выполняемых процессов как по системе в целом, так и для каждого отдельного пользователя, указать пользователя, от имени которого будет выполняться служба, задать приоритет процесса (nice), указать адреса, с которых разрешено подключение к данной службе, а также время доступа и множество других параметров. Указать эти настройки можно в модуле «Службы xinetd» (пакет `alterator-xinetd`) из раздела «Система». Например, установить неограниченный по адресам доступ можно, указав в поле «Только с адресов» значение 0.0.0.0 (Рис. 45).

Настройка параметров vsftpd в модуле «Службы xinetd»

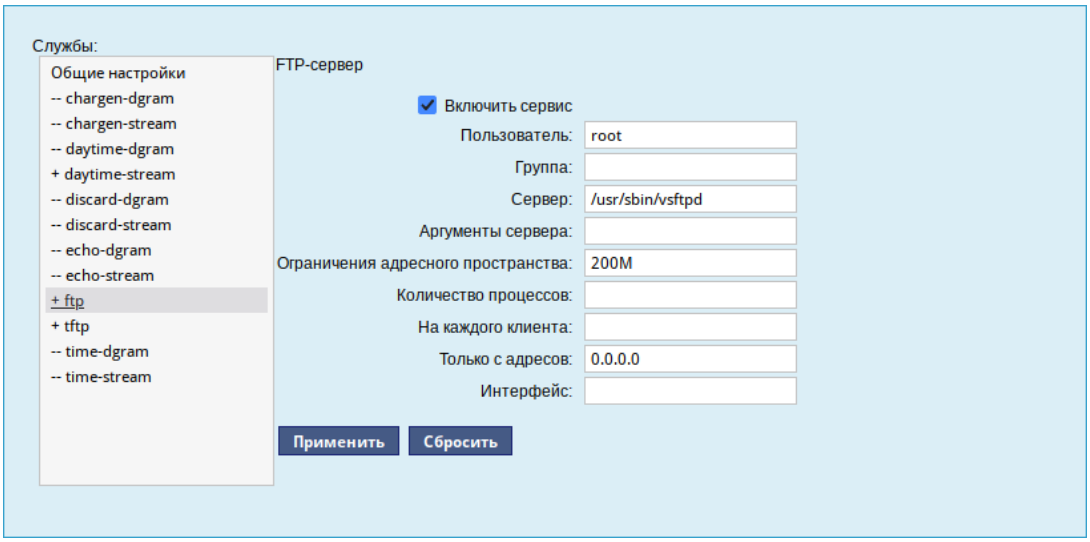


Рис. 45

4.5 Удостоверяющий центр

Модуль «Удостоверяющий центр» (пакет `alterator-ca`) из раздела «Система» позволяет управлять SSL-сертификатами, используемыми для обеспечения безопасных соединений между сетевыми узлами.

Для обеспечения безопасности соединения для клиента (в качестве клиентского ПО может выступать, например, веб-браузер) основным является вопрос о принятии сертификата. При принятии сертификата возможно несколько вариантов.

Сертификат сервера подписан одним из известных клиенту удостоверяющим центром (УЦ)

В этом случае сертификат принимается и устанавливается безопасное SSL-соединение. Обычно клиентское ПО (например, веб-браузер) содержит список наиболее известных УЦ и предоставляет возможность управления (добавление/удаление) сертификатами таких УЦ.

Сертификат сервера подписан УЦ неизвестным клиенту

В этом случае следует самостоятельно решить вопрос о принятии такого сертификата:

- можно временно (на время одной сессии) принять сертификат сервера;
- можно принять сертификат сервера на постоянной основе;
- если вы доверяете УЦ, подписавшему сертификат, можно добавить сертификат самого УЦ к списку известных сертификатов, и таким образом, в дальнейшем все сертификаты, подписанные этим УЦ, будут приниматься автоматически.

Сертификат сервера является самоподписанным

Это случай, когда сертификат сервера не подтверждён вообще никакой третьей стороной. Такие сертификаты используются в локальных сетях, где вы самостоятельно можете проверить аутентичность сервера. В случае самоподписанных сертификатов вы должны самостоятельно убедиться в том, что сервер является тем, за кого себя выдаёт. Сделать это можно, сверив отпечатки полученного сертификата и реально находящегося на сервере.

Примечание. При первом обращении к модулю «Удостоверяющий центр» необходимо создать УЦ, указав страну и организацию (Рис. 46).

Модуль «Удостоверяющий центр». Создание УЦ

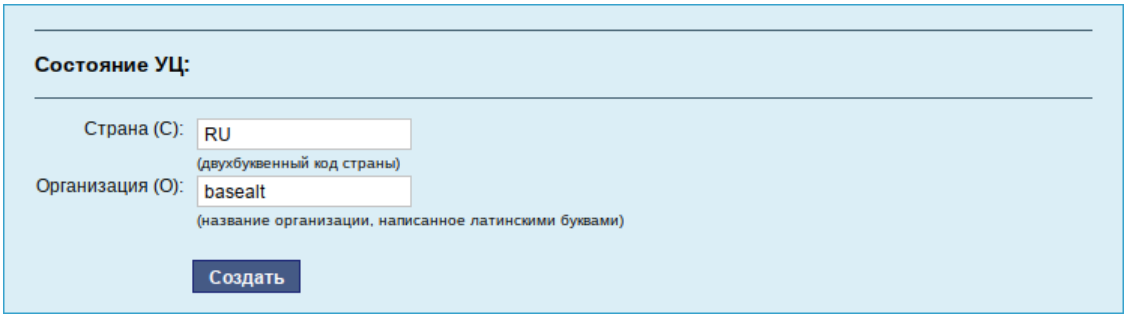


Рис. 46

На вкладке «Управление УЦ» (Рис. 47) можно:

- просмотреть информацию о сертификате УЦ;
- выгрузить для дальнейшего использования сертификат УЦ (файл `ca-root.pem`). Этот файл можно будет добавить к списку УЦ, используемому клиентским ПО, после чего все сертификаты, подписанные данным УЦ будут приниматься автоматически;
- выгрузить, для дальнейшего использования, запрос на подпись сертификата УЦ (файл `ca-root.csr`). Этот запрос можно подписать сторонним УЦ;
- перегенерировать сертификат УЦ с другими параметрами (можно изменить параметры «Страна (C)» и «Организация (O)»).

Модуль «Удостоверяющий центр». Вкладка «Управление УЦ»

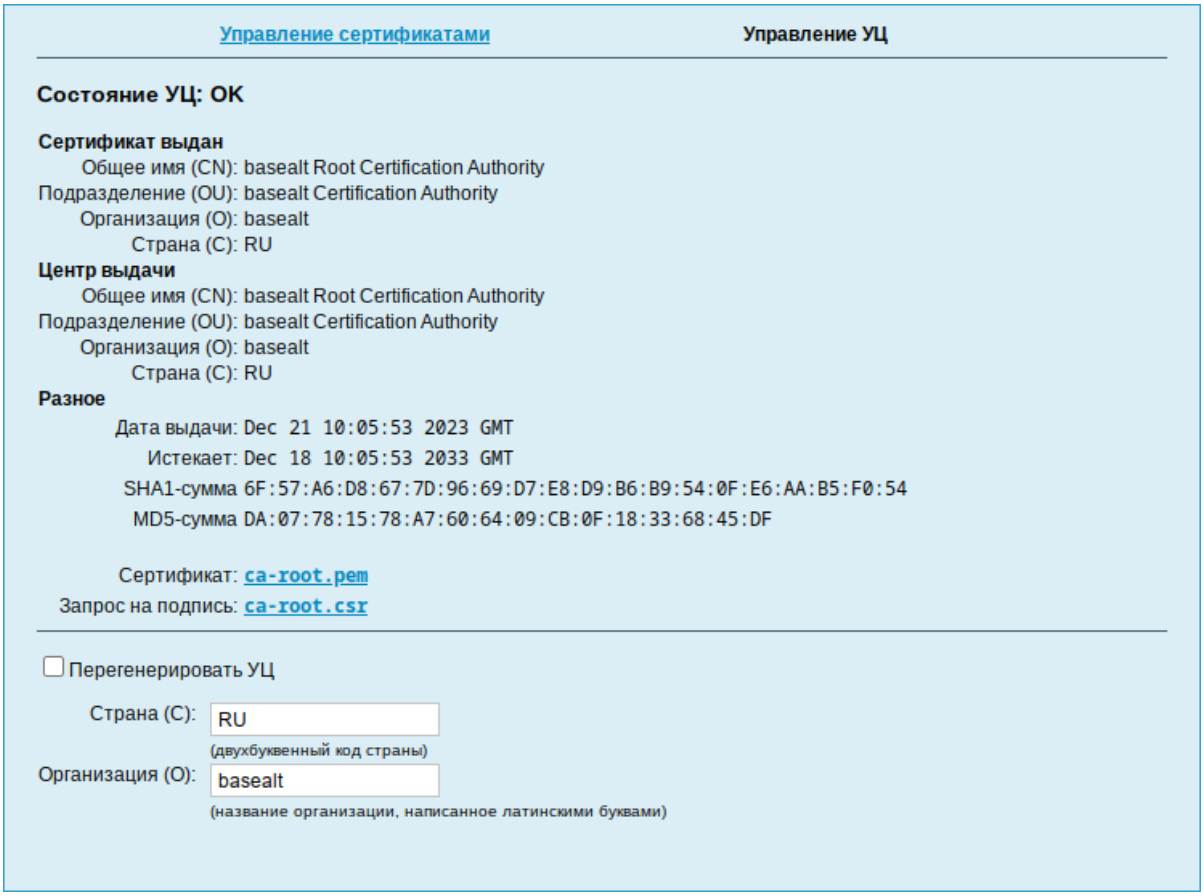


Рис. 47

На вкладке «Управление сертификатами» (Рис. 48) можно:

- настроить ежедневное обновление подписей сертификатов, используемых локальными службами и службами подчинённых серверов;
- подписать произвольный сертификат (запрос на подпись) корневым сертификатом УЦ, настроенным на вкладке «Управление УЦ»;
- просмотреть состояния и подпись локальных сертификатов и сертификатов подчинённых серверов (Рис. 49).

Модуль «Удостоверяющий центр». Вкладка «Управление сертификатами»

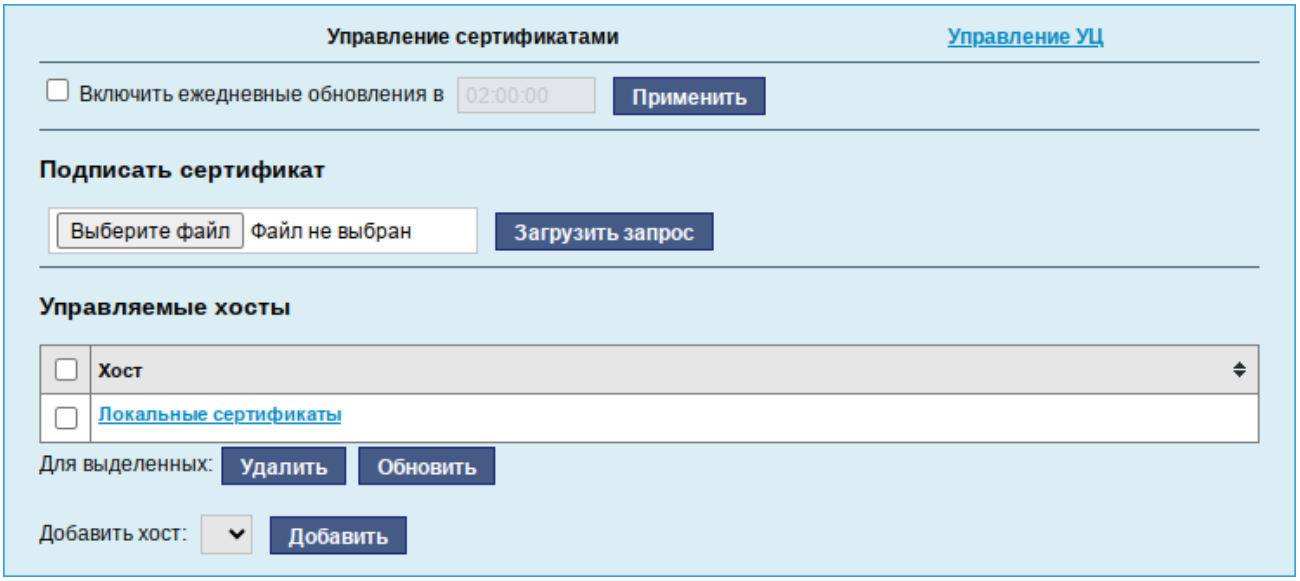


Рис. 48

Модуль «Удостоверяющий центр». Локальные сертификаты

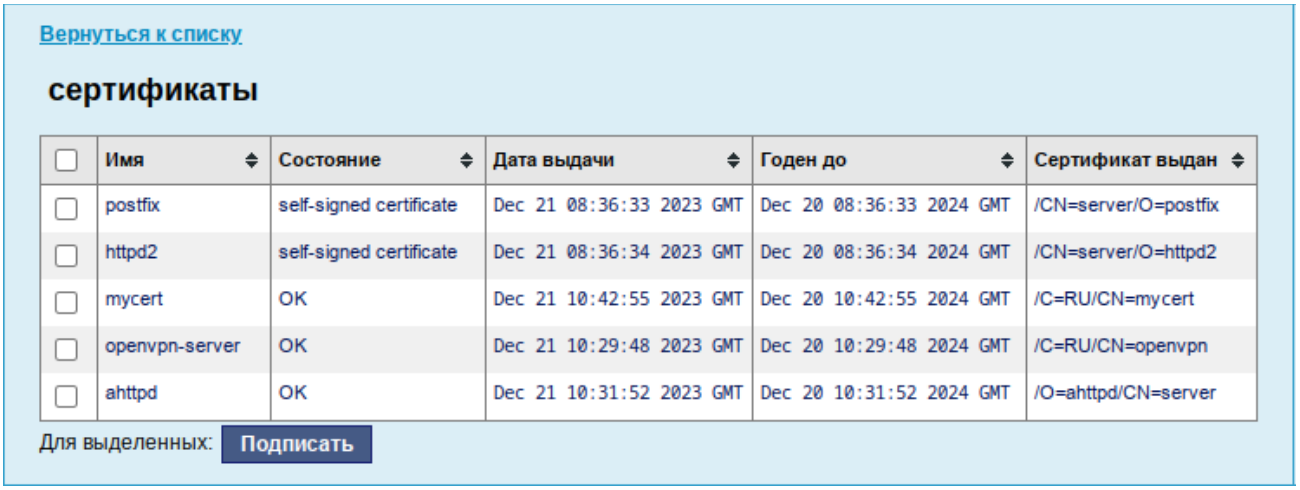


Рис. 49

Чтобы подписать сертификат, необходимо на вкладке «Управление сертификатами» нажать кнопку «Выберите файл», выбрать файл с запросом на подпись и нажать кнопку «Загрузить запрос». В результате на экране отобразится запрос на подпись (Рис. 50). Далее следует нажать кнопку «Подписать». Подписанный сертификат (файл `output.pem`) будет загружен в каталог загрузок.

Модуль «Удостоверяющий центр». Запрос на подпись

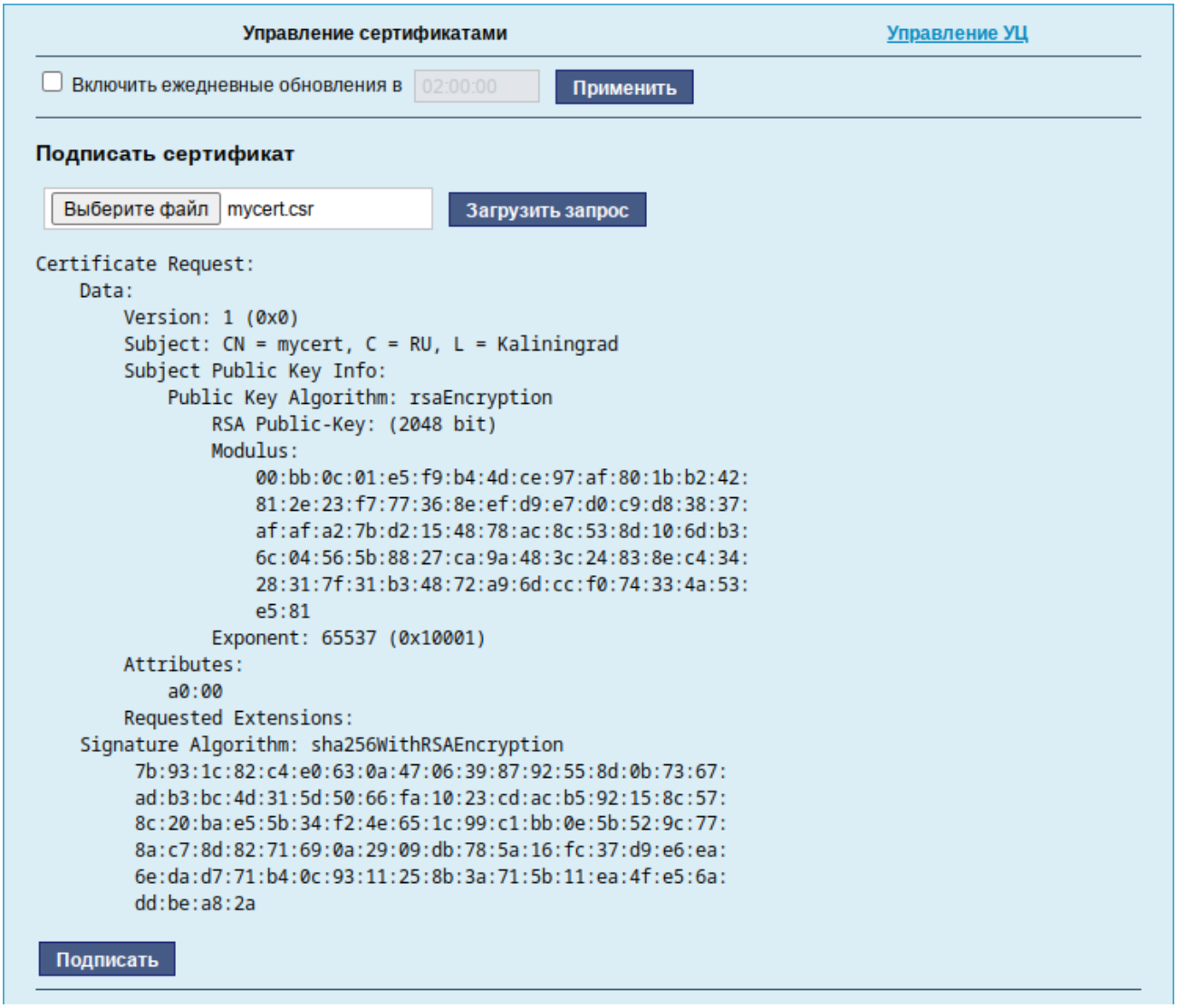


Рис. 50

4.6 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.

4.6.1 Настройка OpenVPN-сервера

Модуль «OpenVPN-сервер» (пакет `alterator-openvpn-server`) из раздела «Серверы» позволяет задать параметры OpenVPN-сервера (Рис. 51).

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»

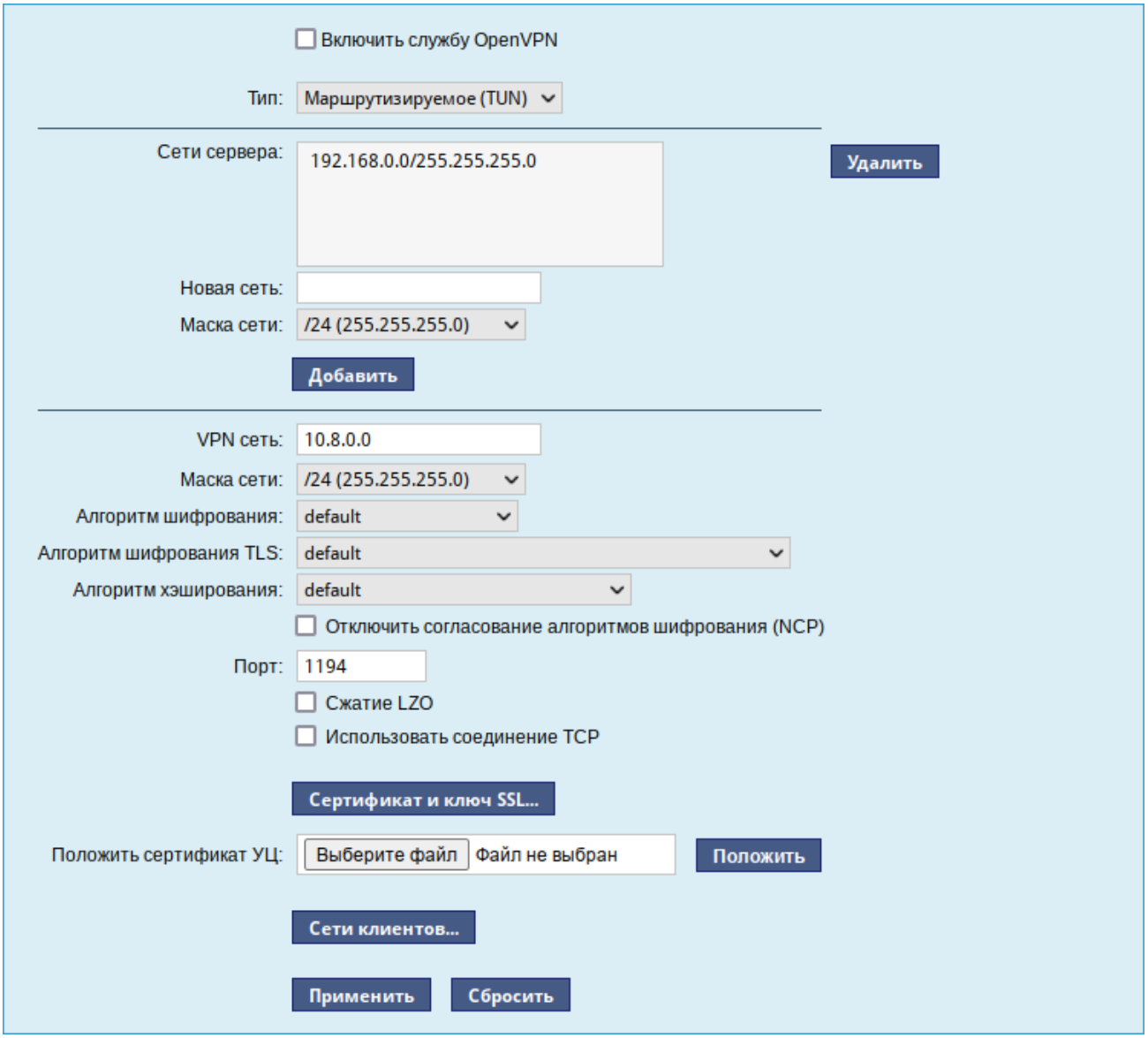


Рис. 51

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. 52).

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. 53).

Модуль «Управление ключами SSL»

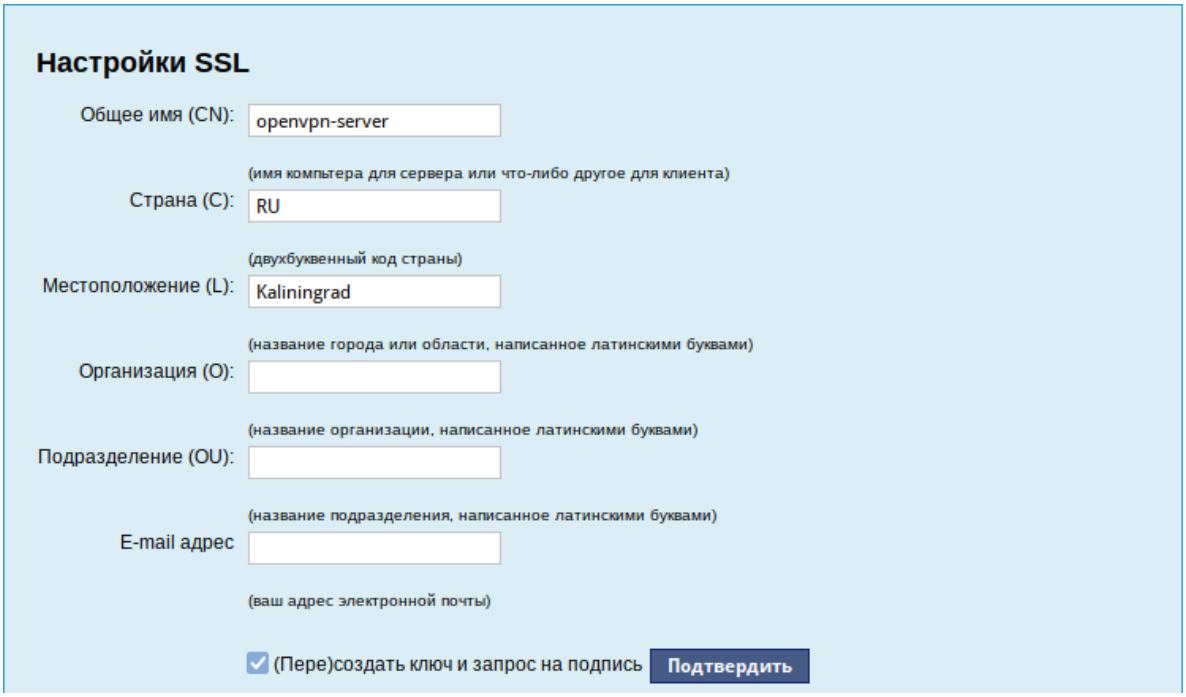


Рис. 52

Забрать запрос на подпись

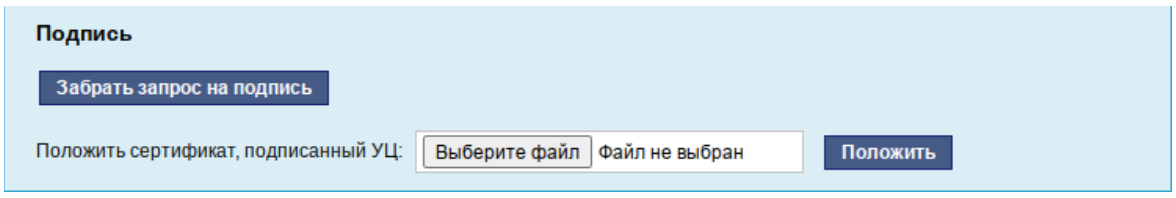


Рис. 53

Если нажать на кнопку «Забрать запрос на подпись», запрос на подпись (файл `openvpn-server.csr`) будет загружен в каталог загрузок

В модуле «Управление ключами SSL» появится новый ключ: «openvpn-server (Нет сертификата)» (Рис. 54).

Ключ openvpn-server

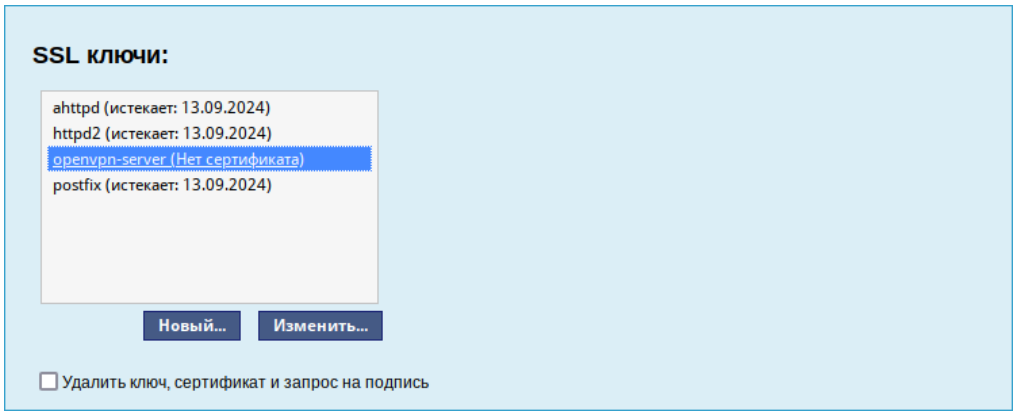


Рис. 54

Чтобы подписать сертификат, необходимо перейти в модуль «Удостоверяющий Центр» →«Управление сертификатами», нажать кнопку «Выберите файл», указать путь до полученного файла `openvpn-server.csr` и загрузить запрос (Рис. 55).

Запрос на подпись сертификата

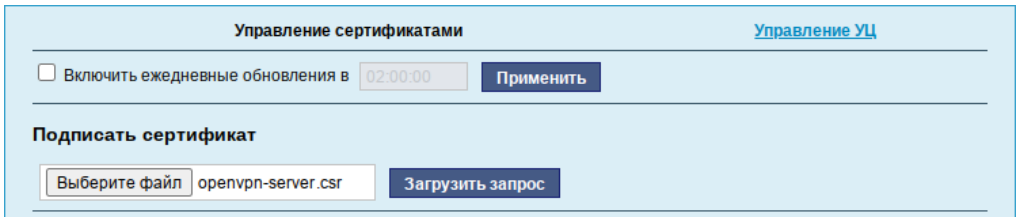


Рис. 55

В результате на экране появится две группы цифр и кнопка «Подписать» (Рис. 56). Необходимо нажать на кнопку «Подписать», подписанный сертификат (файл `output.pem`) будет загружен в каталог загрузок.

Запрос на подпись сертификата

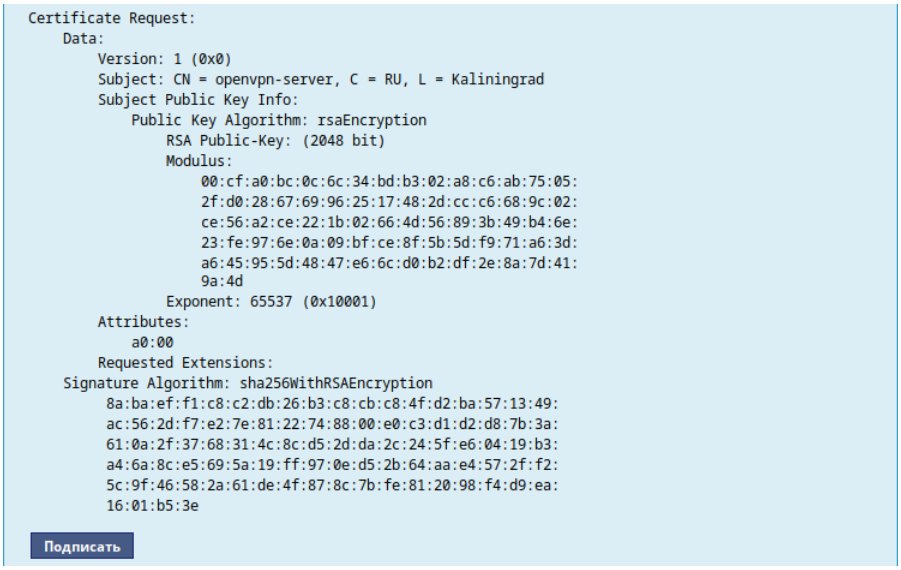


Рис. 56

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 «Выберите файл», указать путь до файла `output.pem` и нажать кнопку «Положить» (Рис. 57).

Сертификат, подписанный УЦ

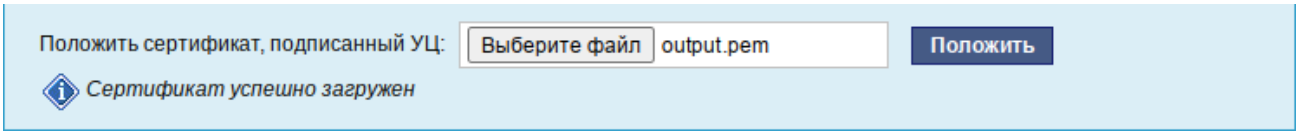


Рис. 57

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. 58).

Сертификат УЦ

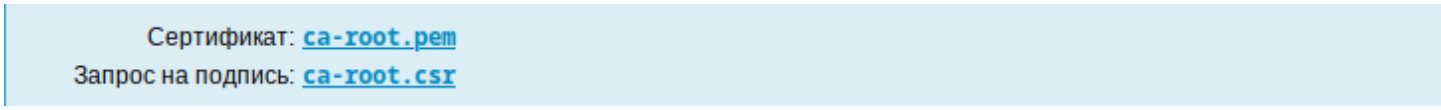


Рис. 58

В модуле «OpenVPN-сервер», в графе «Положить сертификат УЦ»: при помощи кнопки «Выберите файл» указать путь к файлу `ca-root.pem` и нажать кнопку «Положить» (Рис. 59).

Выбор сертификата УЦ в модуле «OpenVPN-сервер»

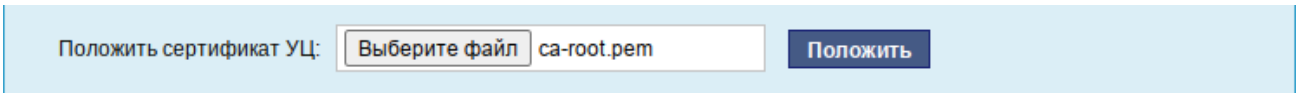


Рис. 59

Появится сообщение: «Сертификат УЦ успешно загружен».

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

4.6.2 Настройка клиентов

Со стороны клиента соединение настраивается в модуле «OpenVPN-соединения» (пакет `alterator-net-openvpn`) из разделараздел «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. 60). Должен быть выбран тот же тип, что и на стороне сервера.

Необходимо 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.

Создание нового OpenVPN- соединения

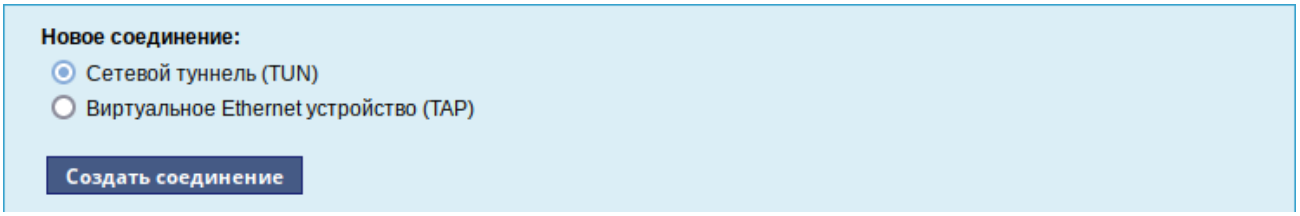


Рис. 60

Помимо этого нужно создать ключ (например, openvpn) в модуле «Управление ключами SSL» и подписать его в модуле «Удостоверяющий центр» на сервере.

В результате станут доступны настройки соединения (Рис. 61).

Модуль «OpenVPN- соединения»

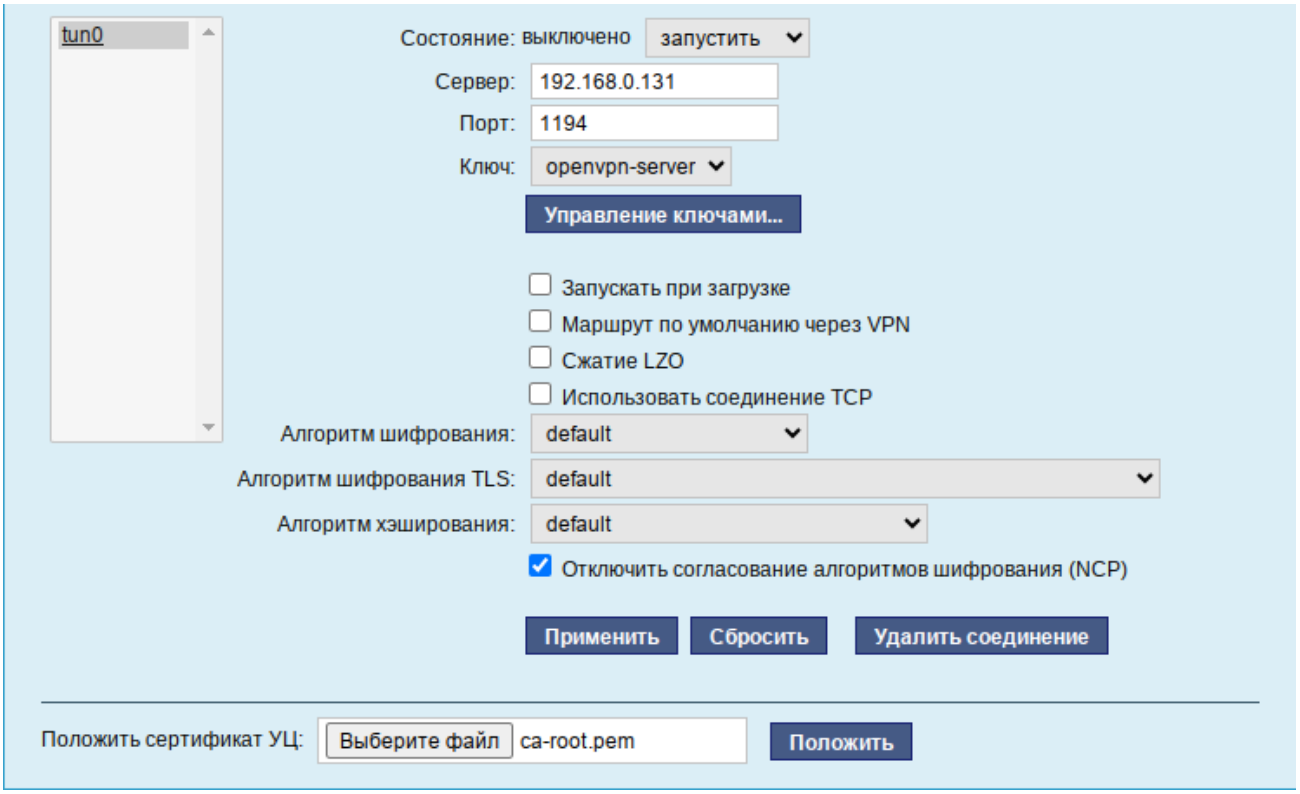


Рис. 61

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 tun0. При обычных настройках это может выглядеть так:

```
tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_-
codel state UNKNOWN group default qlen 500
   link/none
   inet 10.8.0.6 peer 10.8.0.5/32 scope global tun0
```

4.7 Доступ к службам сервера из сети Интернет

4.7.1 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. 62). Если необходимо предоставить доступ к службе, отсутствующей в списке, то нужно задать используемые этой службой порты в соответствующих полях.

Модуль «Внешние сети»

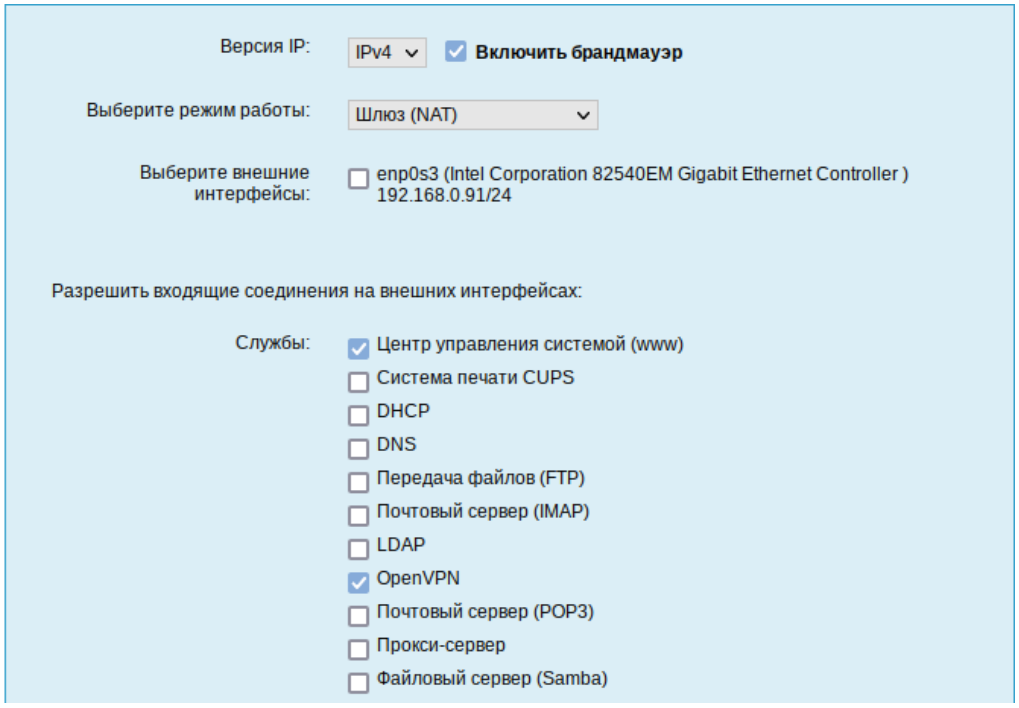


Рис. 62

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.

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.

4.7.2 Список блокируемых хостов

Модуль «Список блокируемых хостов» (пакет `alterator-net-iptables`) 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. 63).

Модуль «Список блокируемых хостов»

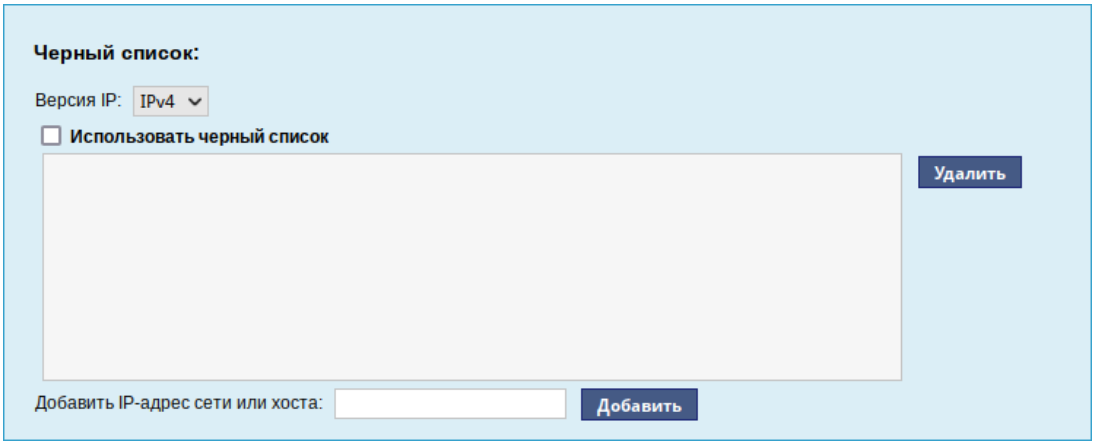


Рис. 63

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».

4.8 Статистика

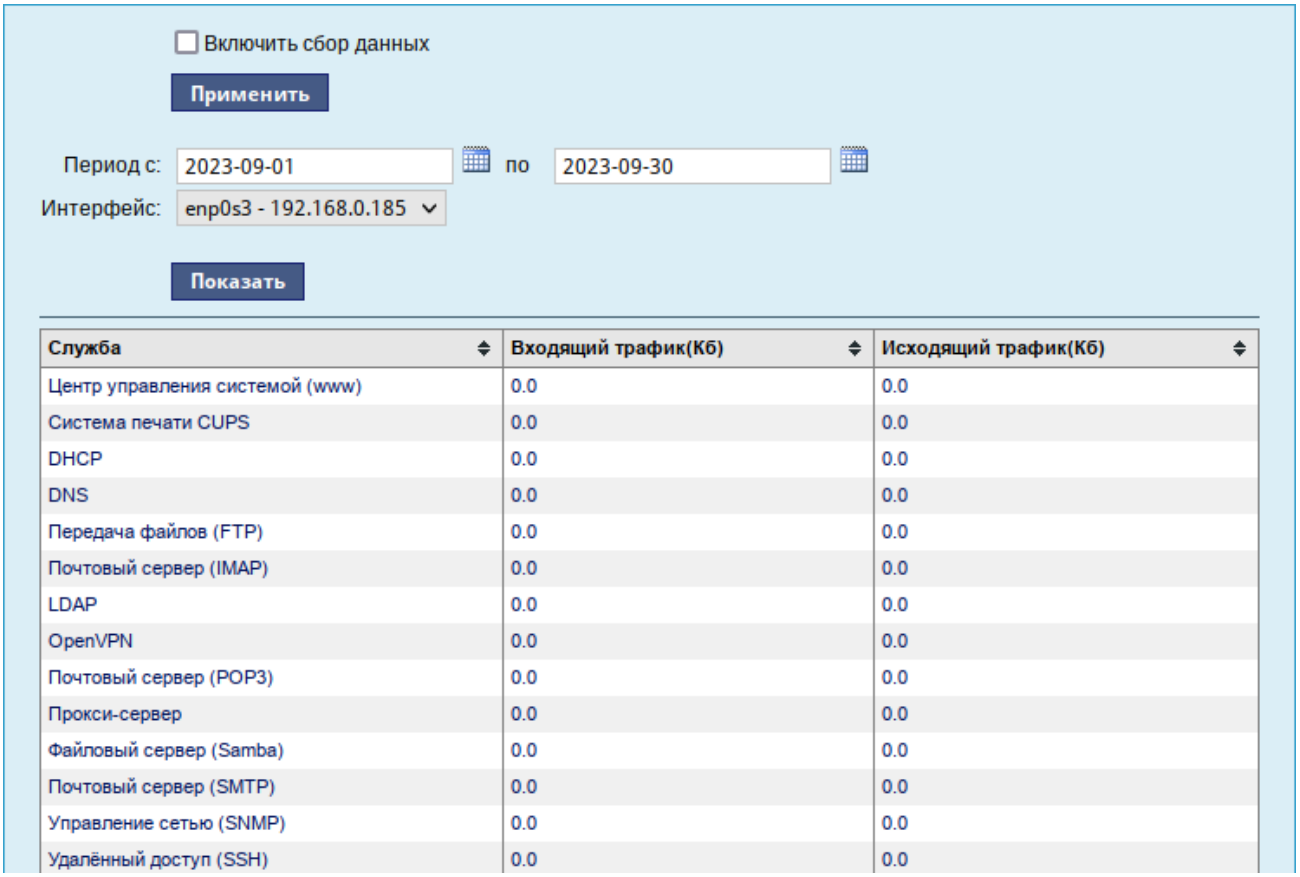
4.8.1 Сетевой трафик

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 флаг «Включить сбор данных», и нажать кнопку «Применить» (Рис. 64).

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
Управление сетью (SNMP)	0.0	0.0
Удалённый доступ (SSH)	0.0	0.0

Рис. 64

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. 64).

Трафик на указанном интерфейсе за заданный период показывается в виде:

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

4.8.2 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. 65).

Настройка сбора статистики прокси-сервера

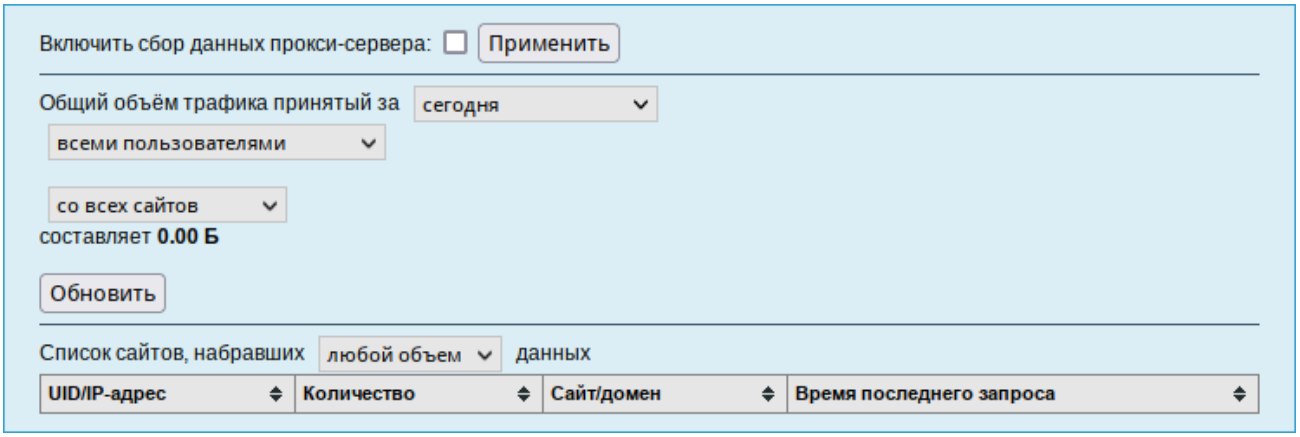


Рис. 65

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 «Обновить». 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 неаутентифицированных пользователей. Только после этого в статистике начнут показываться пользователи.

4.9 Обслуживание сервера

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

4.9.1 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. 66).

Модуль «Системные журналы»

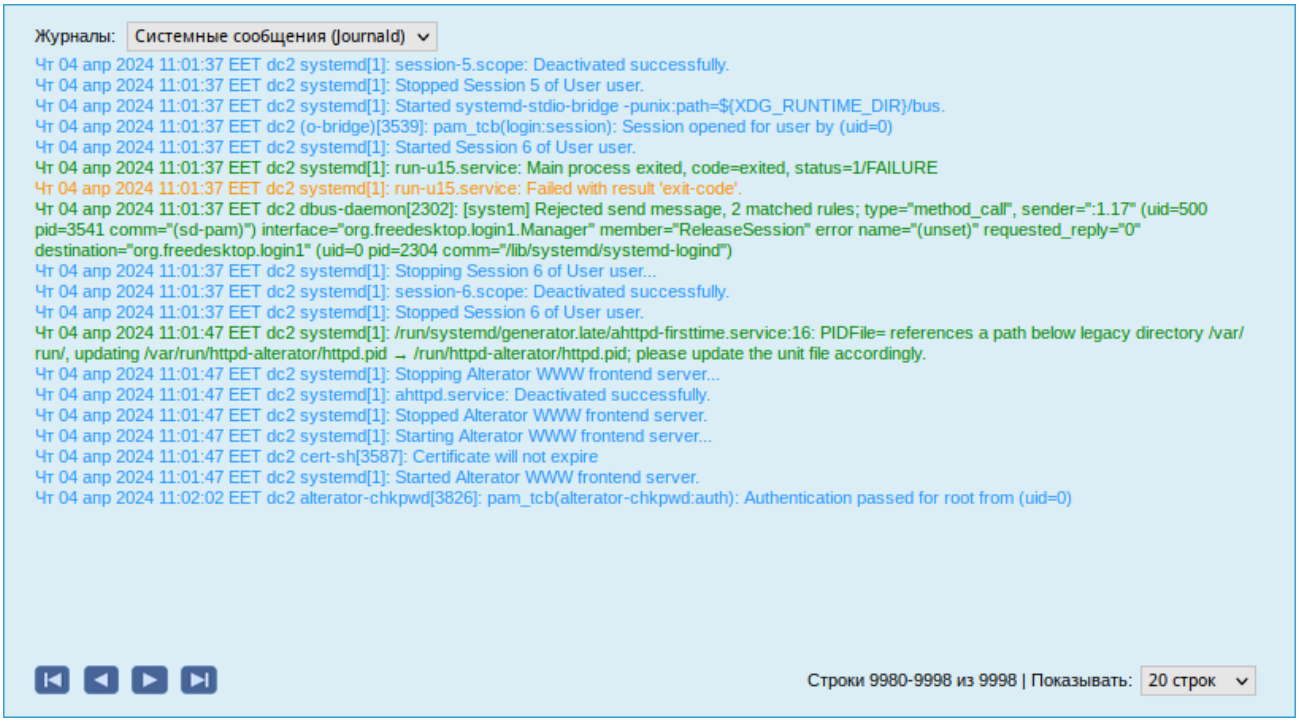


Рис. 66

Доступны следующие виды журналов:

- «Брандмауэр» – отображаются события безопасности, связанные с работой межсетевого экрана ОС;
- «Системные сообщения (Journald)» – отображаются события процессов ядра и пользовательской области. У каждого сообщения в этом журнале есть приоритет, который используется для пометки важности сообщений. Сообщения, в зависимости от уровня приоритета, подсвечиваются цветом.

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

4.9.2 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. 67).

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

Модуль «Системные службы»

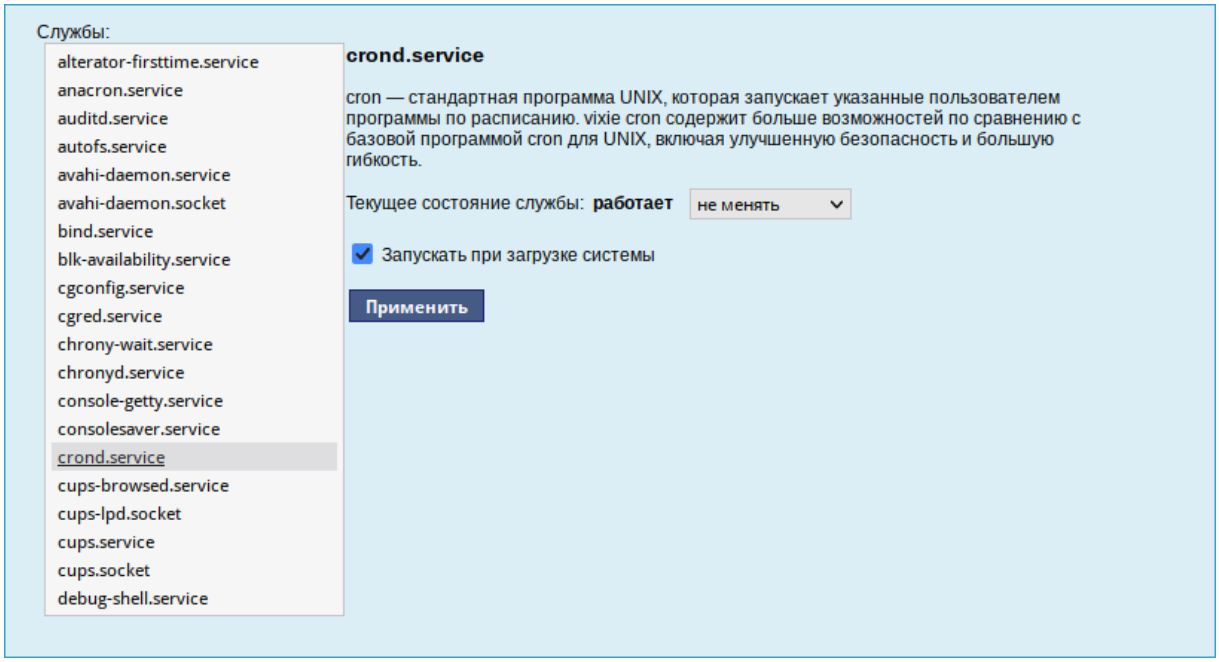


Рис. 67

4.9.3 Системные ограничения

Средствами модуля «Системные ограничения» (пакет `alterator-control`) из раздела «Система» определяются несколько заранее заданных режимов доступа к тому или иному файлу. Администратор системы может установить один из этих режимов – он будет гарантированно сохранён при обновлении системы.

Модуль также может использоваться как простой конфигуратор, позволяющий переключать многие системные службы между заранее определёнными состояниями.

На Рис. 68 показаны политики для команды `fusermount`.

Для переключения состояния следует выбрать политику и нажать кнопку «Сохранить».

Модуль «Системные ограничения»

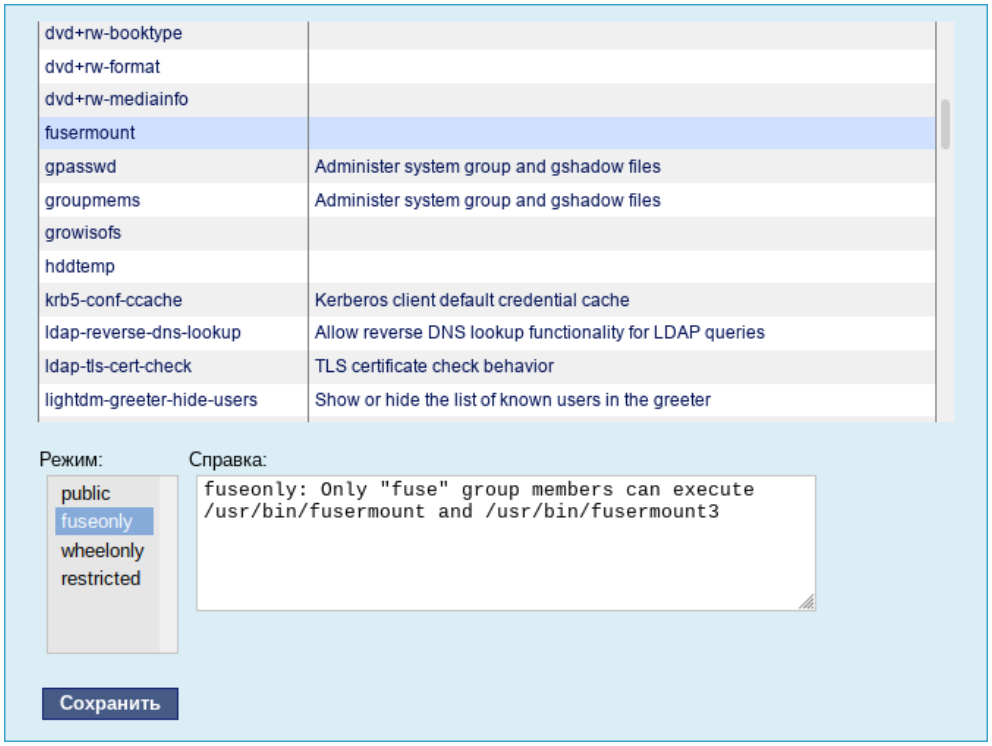


Рис. 68

4.9.4 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. 69).

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

Необходимо также указать репозитории. Следует обратить внимание на то, что разные репозитории бывают разной степени стабильности и чем стабильнее репозиторий, тем реже там появляются новые версии приложений.

Примечание. Рабочие станции «видят» локальный сервер обновлений, при выборе режима «Обновление системы управляемое сервером», если они находятся в домене (при этом

сервер обновлений должен быть настроен на «Опубликовать как репозиторий для автоматических обновлений»).

Модуль «Обновление системы»

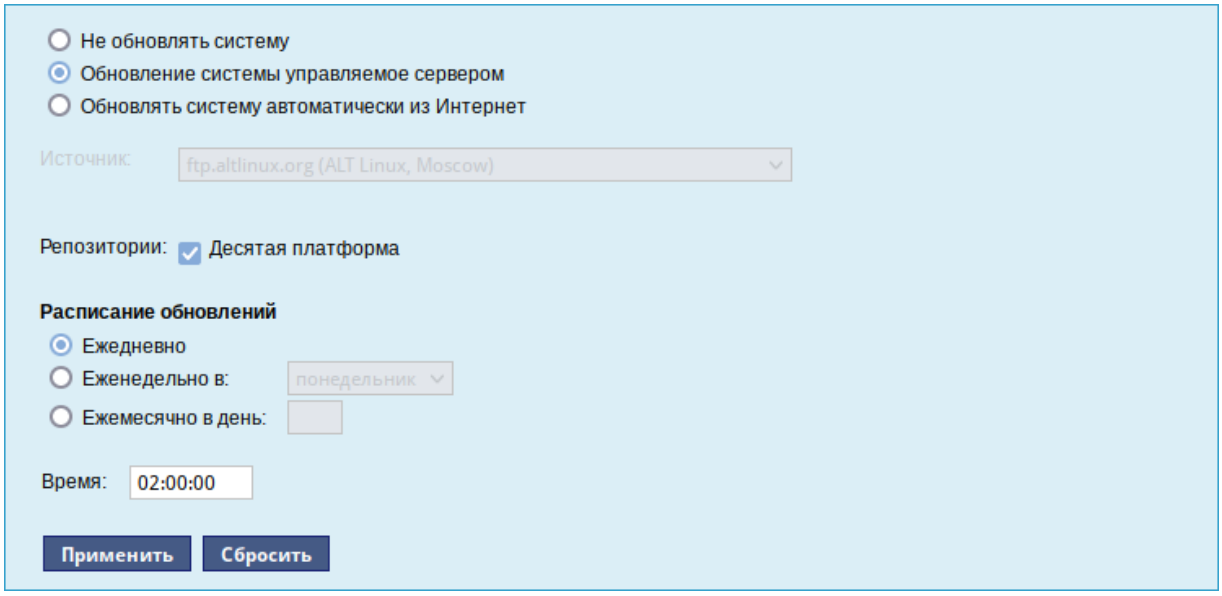


Рис. 69

Процесс обновления системы будет запускаться автоматически согласно заданному расписанию.

Примечание. Чтобы указать в качестве сервера обновлений локально настроенный источник, необходимо выбрать режим «Обновлять систему автоматически из Интернет», выбрать в списке «Другой адрес» и указать адрес локального сервера обновлений, например, http://<ip сервера>/mirror (Рис. 70).

Указание источника обновлений

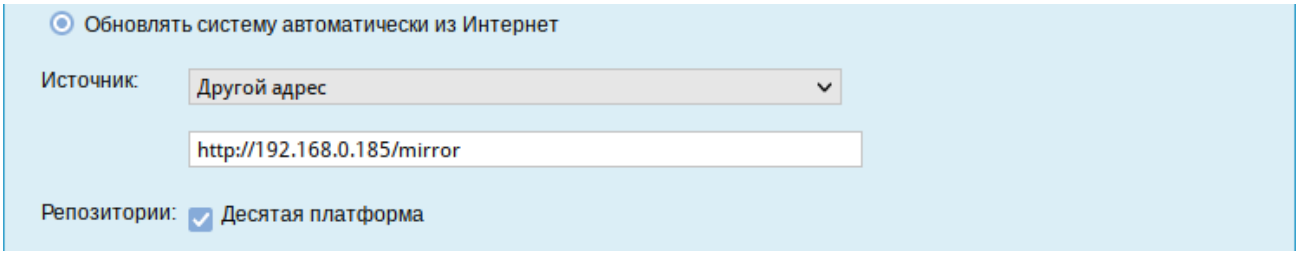


Рис. 70

4.9.5 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. 71).

Интерфейс модуля «Обновление ядра»

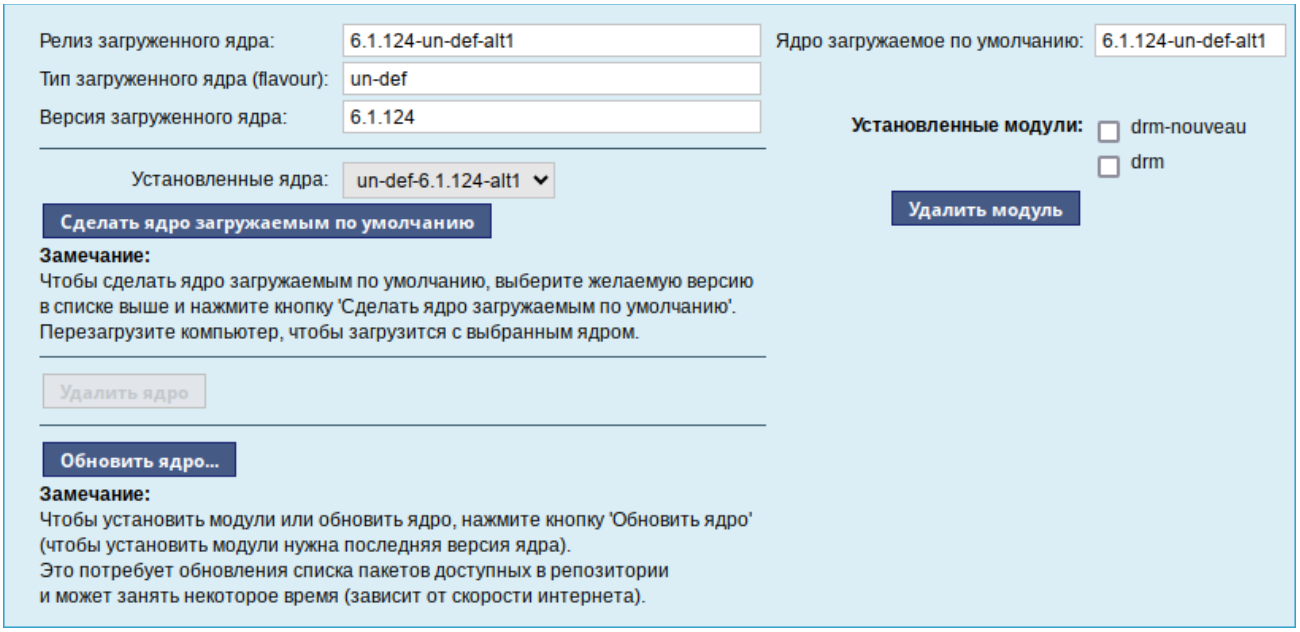


Рис. 71

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.

Если в системе уже установлено последнее ядро, сообщение об этом появится в открывшемся окне, иначе в этом окне будет показано доступное к установке ядро (Рис. 72).

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.

Доступное к установке ядро

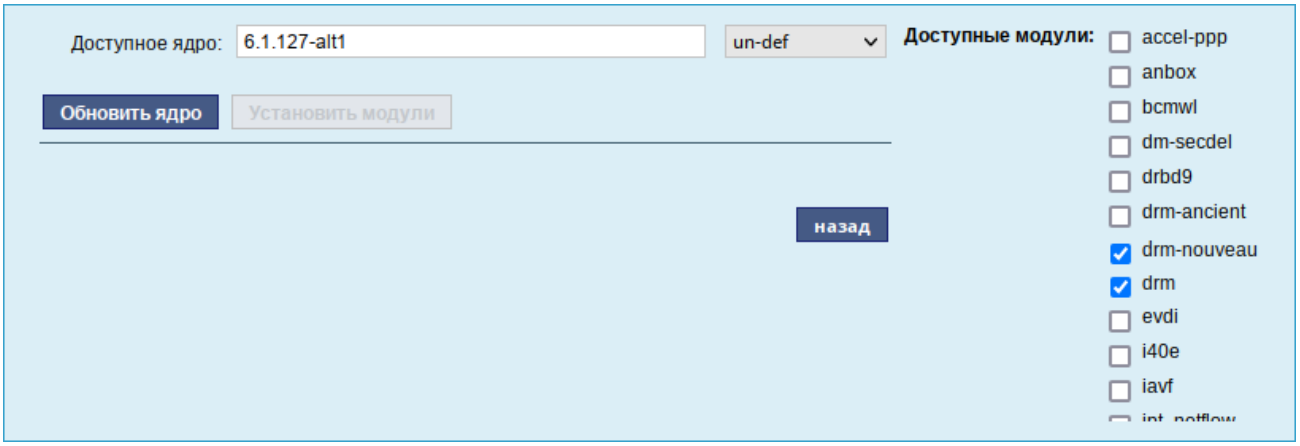


Рис. 72

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, в окне «Доступные модули» можно отметить модули ядра необходимые к установке и нажать кнопку «Установить модули».

4.9.6 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. 73).

Здесь также можно выбрать репозитории, локальные срезы которых необходимы. При нажатии на название репозитория, появляются настройки этого репозитория (Рис. 74). 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»

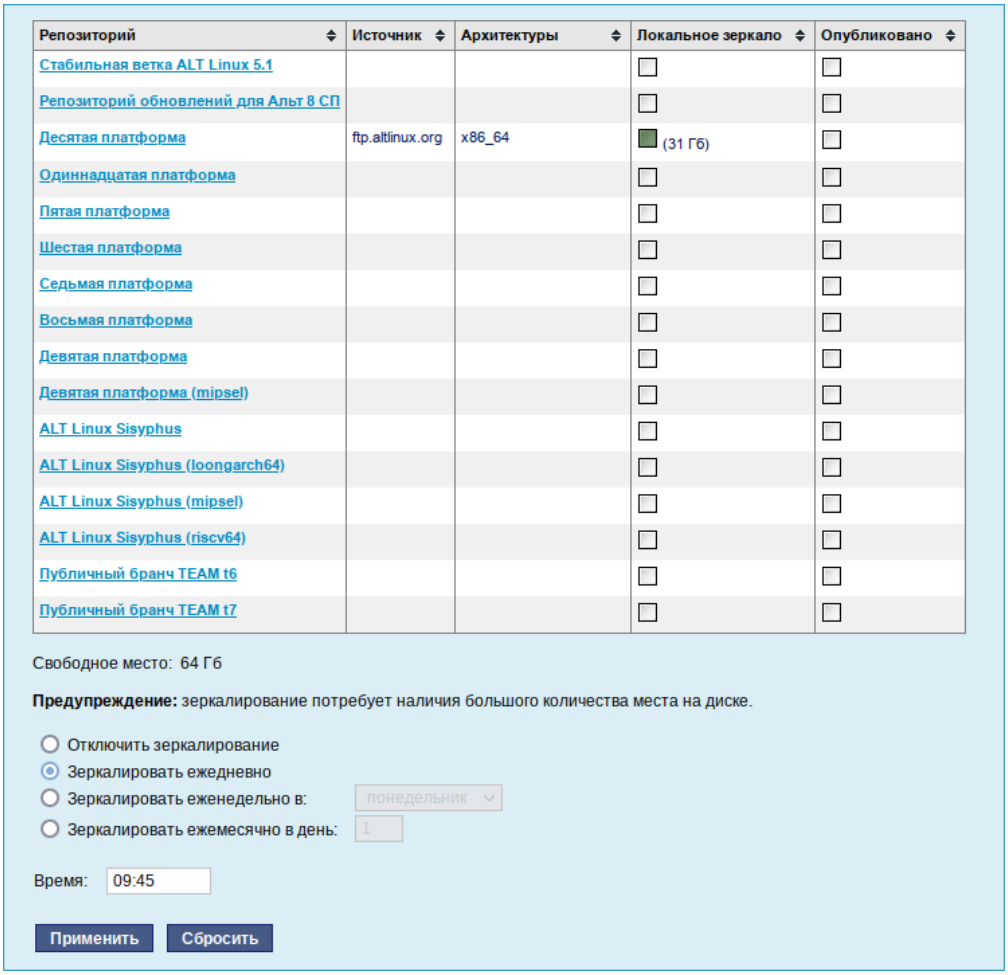


Рис. 73

Настройки репозитория

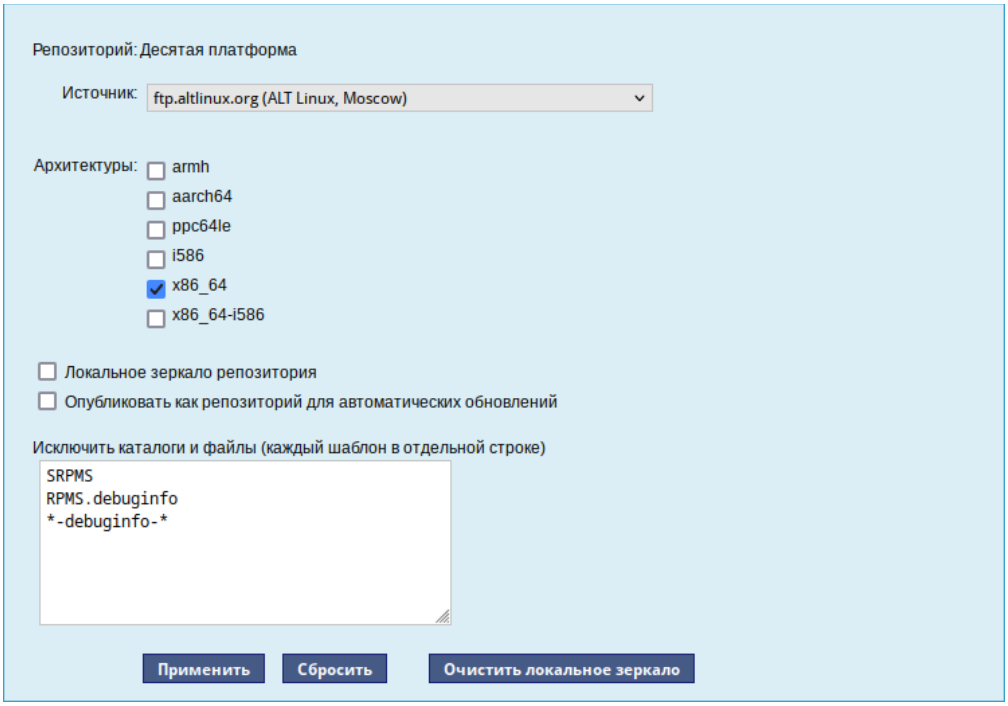


Рис. 74

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.

Примечание. Если в каталогах /srv/public/mirror/<репозиторий>/branch/<архитектура>/base/ нет файлов pkglist.* значит зеркалирование не закончено (т.е. не все файлы загружены на ваш сервер).

4.9.6.1 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/p10/branch
```

Проверить правильность настройки репозиториев:

```
# apt-repo
rpm http://192.168.0.185/mirror p10/branch/x86_64 classic
rpm http://192.168.0.185/mirror p10/branch/noarch classic
```

4.9.6.2 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/p10/branch
# apt-repo
rpm ftp://192.168.0.185/mirror p10/branch/x86_64 classic
rpm ftp://192.168.0.185/mirror p10/branch/noarch classic
```

4.9.7 Локальные учётные записи

Модуль «Локальные учётные записи» (пакет `alterator-users`) из раздела «Пользователи» предназначен для администрирования системных пользователей (Рис. 75).

Модуль «Локальные учётные записи»

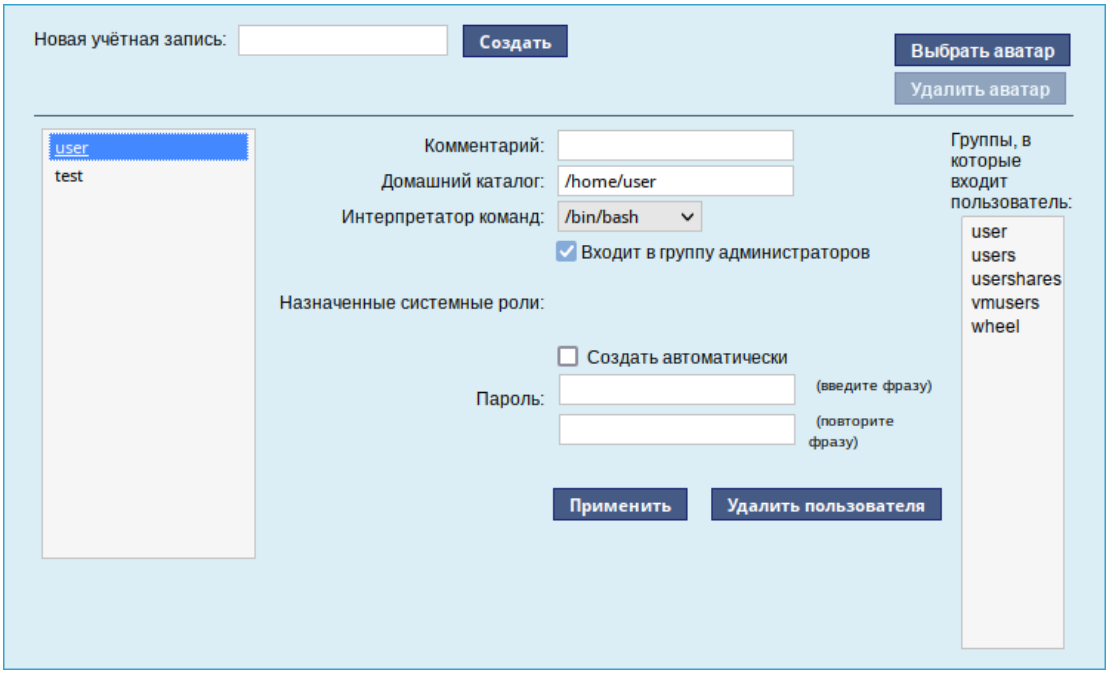


Рис. 75

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.

4.9.8 Администратор системы

В модуле «Администратор системы» (пакет `alterator-root`) из раздела «Пользователи» можно изменить пароль суперпользователя (root), заданный при начальной настройке системы (Рис. 76).

Модуль «Администратор системы»

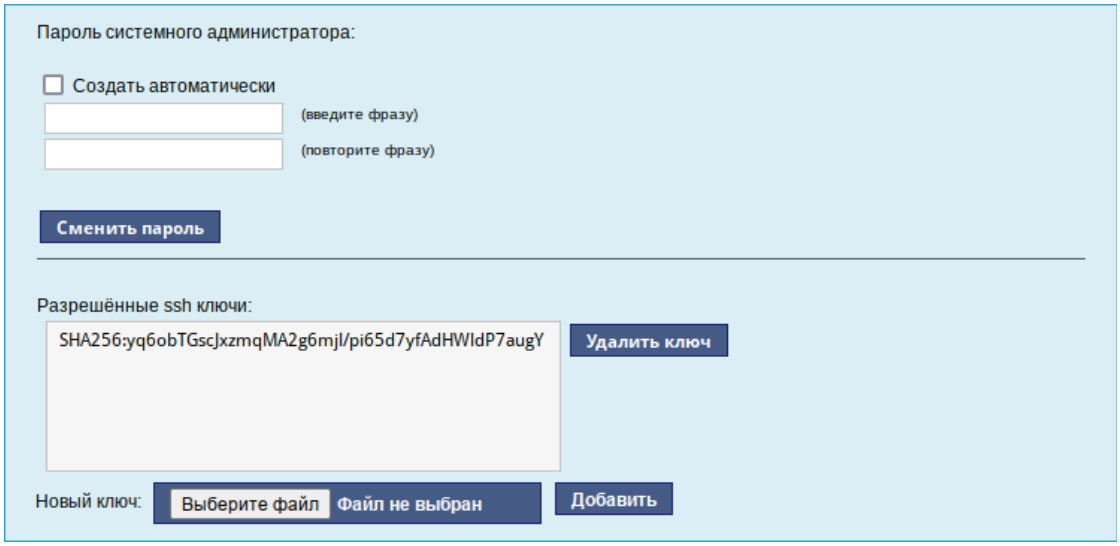


Рис. 76

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

4.9.9 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. 77).

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»

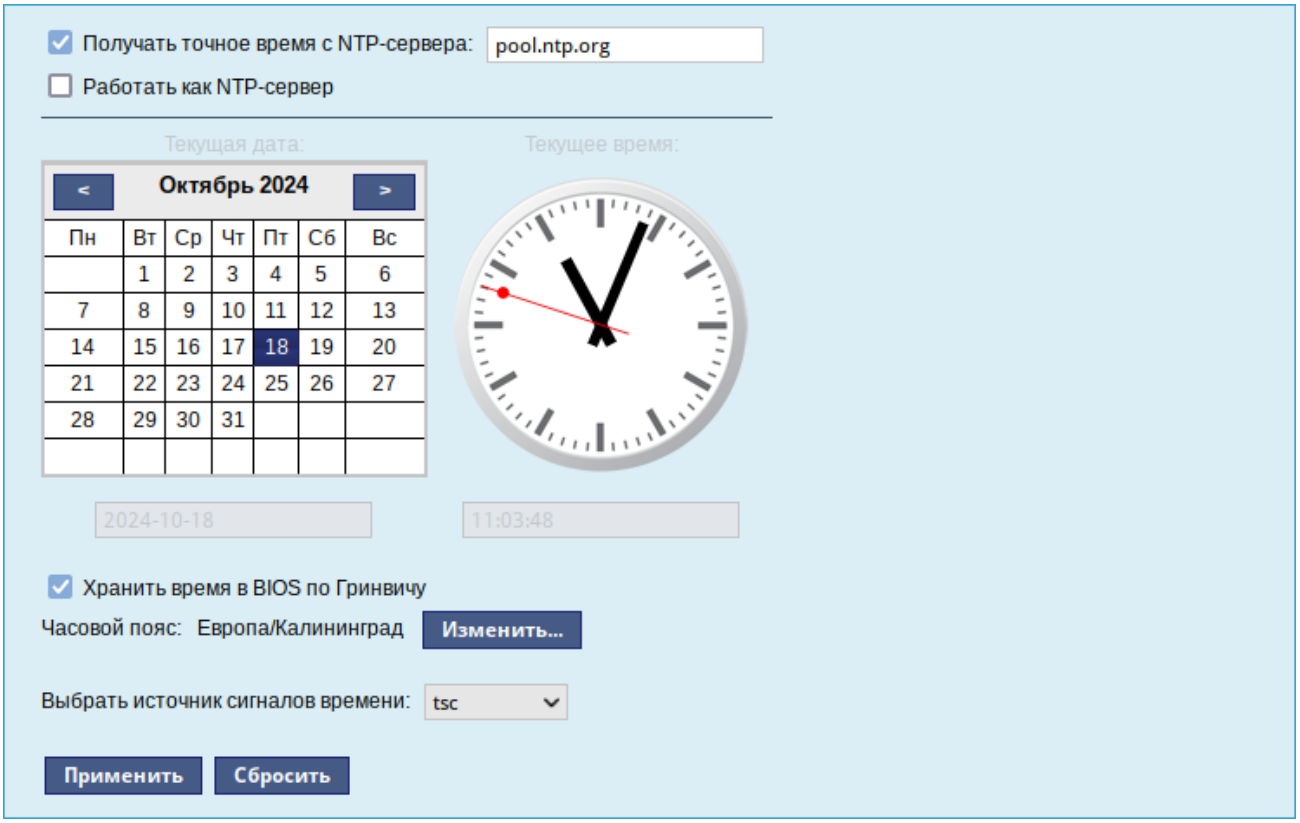


Рис. 77

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».

Примечание. Выбор источника сигналов времени (источника тактовой частоты) доступен в режиме эксперта.

4.9.10 Агент наблюдения

Модуль «Агент наблюдения» (пакет `alterator-zabbix-agent`) из раздела «Система» позволяет настроить клиентскую часть системы мониторинга Zabbix.

На странице модуля можно задать следующие параметры (Рис. 78):

- «Слушать по адресу» – IP-адрес, который агент должен прослушивать;
- «Адрес сервера наблюдения» – адрес сервера, которому разрешено обращаться к агенту;
- «Имя узла» – при выборе пункта «Системное» узел будет добавлен на сервер Zabbix под системным именем, при выборе пункта «Пользовательское» имя узла можно указать в поле «Пользовательское имя узла»;

- «Пользовательское имя узла» – имя узла мониторинга, которое будет указано на сервере Zabbix.

Примечание. Параметр «Разрешить выполнение команд» использовать не рекомендуется.

Модуль «Агент наблюдения»

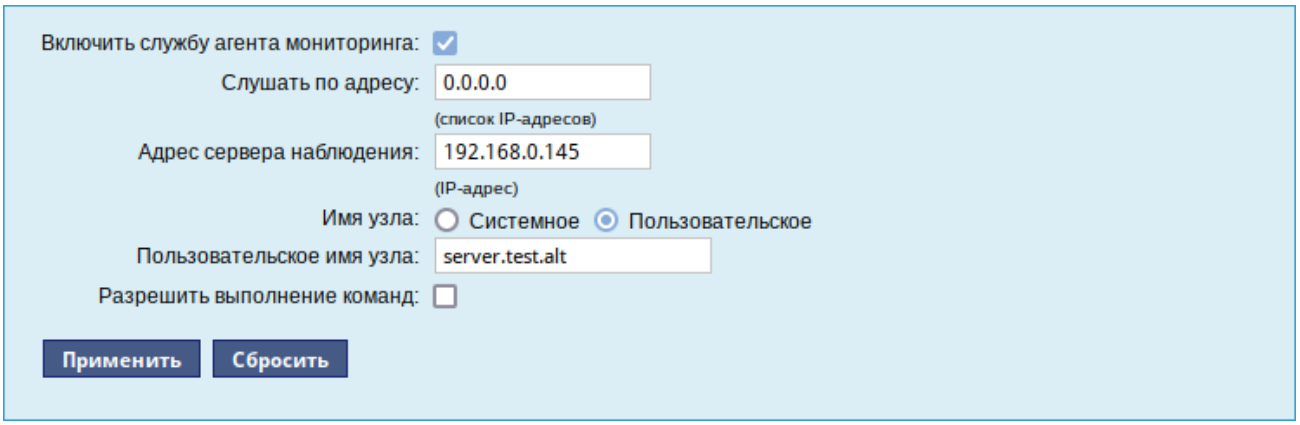


Рис. 78

Чтобы применить настройки и запустить Zabbix-агент, следует установить отметку в пункте «Включить службу агента мониторинга» и нажать кнопку «Применить».

4.9.11 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. 79).

Модуль «Использование диска»

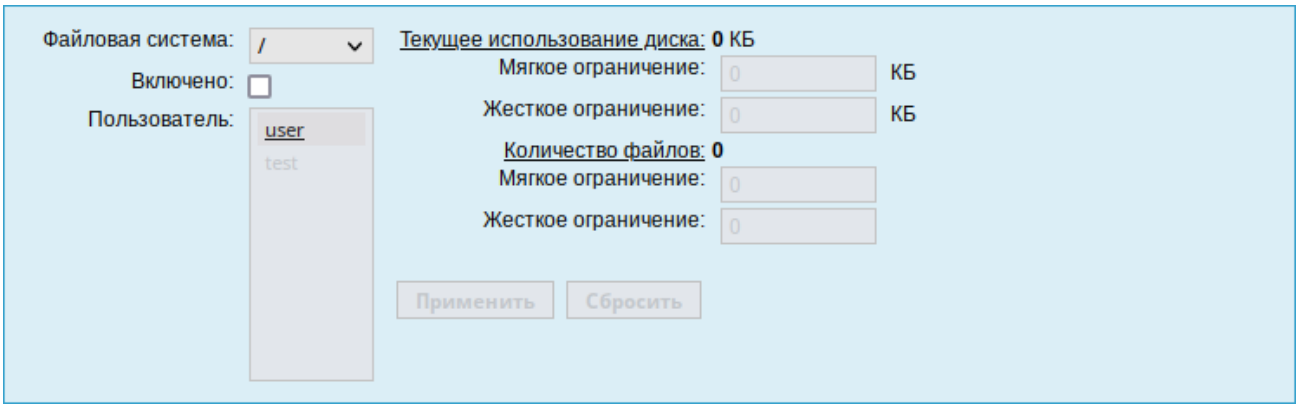


Рис. 79

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. 80).

Задание ограничений для пользователя user на раздел /home

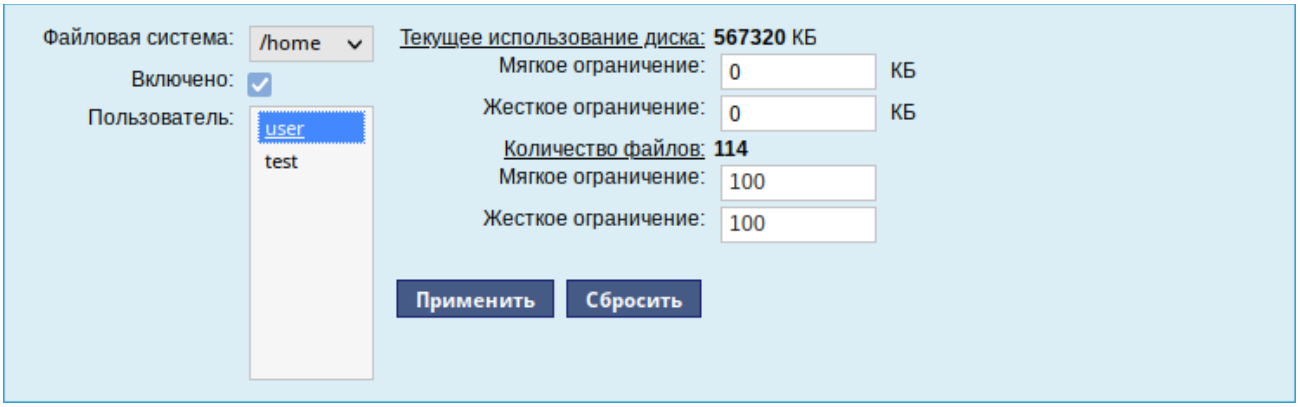


Рис. 80

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.

4.9.12 Выключение и перезагрузка компьютера

Иногда, в целях обслуживания или по организационным причинам необходимо корректно выключить или перезагрузить сервер. Для этого можно воспользоваться модулем ЦУС «Выключение компьютера» в разделе «Система».

Модуль ЦУС «Выключение компьютера» позволяет:

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

Возможна настройка ежедневного применения данных действий в заданное время.

Так как выключение и перезагрузка – критичные для функционирования компьютера операции, то по умолчанию настройка выставлена в значение «Продолжить работу» (Рис. 81). Для выключения, перезагрузки или перехода в энергосберегающие режимы нужно отметить соответствующий пункт и нажать «Применить».

Модуль «Выключение компьютера»

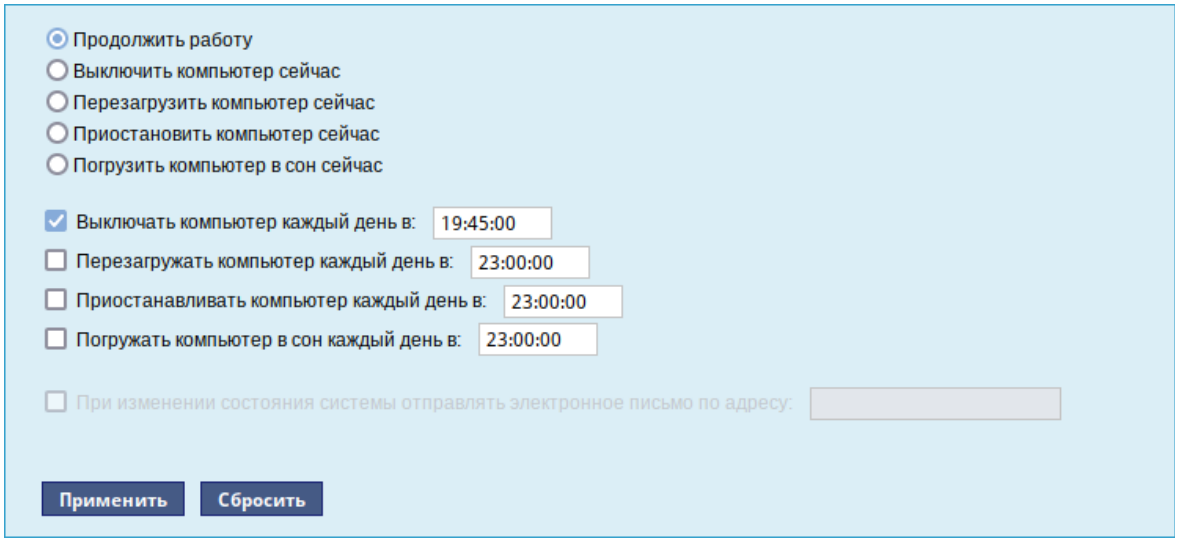


Рис. 81

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. 82).

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

```
Thu Sep 14 11:46:59 EET 2023: The server.test.alt is about to start.
```

Модуль «Выключение компьютера». Настройка оповещений

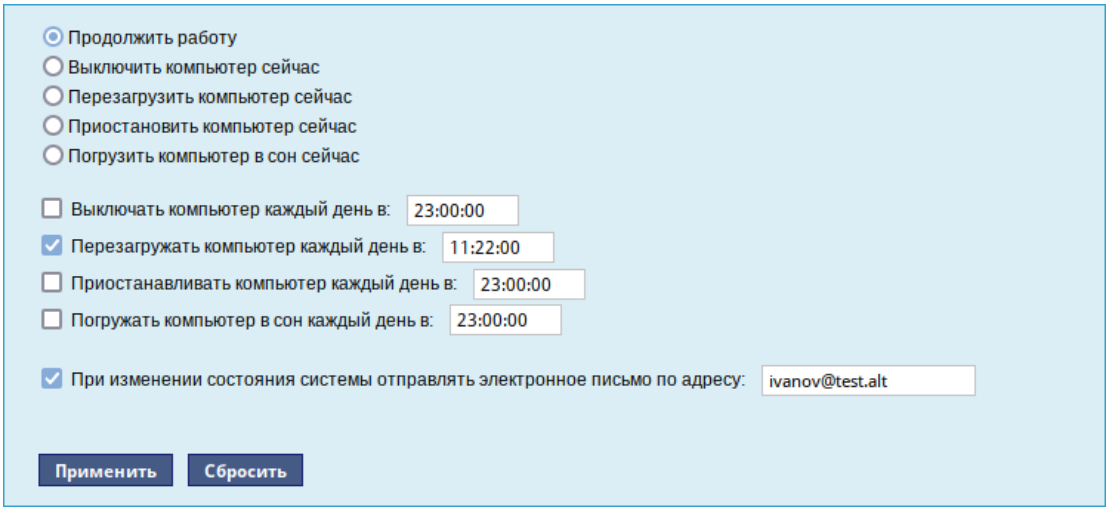


Рис. 82

При выключении:

```
Thu Sep 14 12:27:02 EET 2023: 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.

4.9.13 Настройка ограничений на использование USB-устройств

Модуль ЦУС «USBGuard» (пакет alterator-usbguard) из раздела «Система» предназначен для настройки ограничений на использование USB-устройств. Модуль работает на основе функционала USBGuard, позволяет вести чёрный и белый списки ограничений и предоставляет два типа действий – allow/block.

Модуль предоставляет следующие возможности:

- сканирование подключенных устройств;
- выбор и добавление устройств в набор правил из списка подключенных устройств;
- создание предустановленных правил для распространённых сценариев;
- создание правил по дескрипторам интерфейса: CC:SS:PP;
- создание правил по свойствам USB-устройства: PID, VID;
- создание правил по хешу устройства по PID+VID+SN;
- создание сложных правил с дополнительными условиями;
- загрузка правил из csv-файла;
- редактирование значений в созданных правилах;
- просмотр журнала событий подключения/отключения USB-устройств.

Для уведомления пользователя о подключённом и заблокированном устройстве сообщением в трее используется модуль уведомлений (пакет usbguard-notifier).

4.9.13.1 Информационное поле

В информационном поле (Рис. 83) отображается текущее состояние службы usbguard, список пользователей и групп, которые могут редактировать правила, сообщения об ошибках и предупреждения.

Модуль «USBGuard». Информационное поле

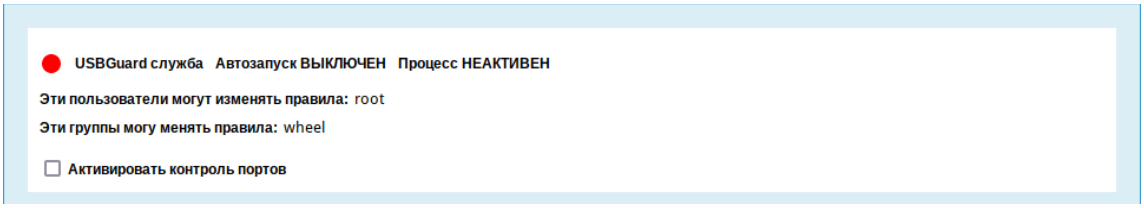


Рис. 83

Примечание. Добавить/удалить пользователя/группу, которые могут редактировать правила, можно в командной строке, например:

- дать пользователю user полный доступ к разделам «devices» и «exceptions», пользователь user также будет иметь возможность просматривать и изменять текущую политику:

```
# usbguard add-user -u user --devices ALL --policy modify,list --exceptions ALL
```

- удалить права у пользователя user:

```
# usbguard remove-user -u user
```

Дополнительную информацию смотрите на соответствующих страницах руководства, например:

```
$ usbguard add-user -h
```

Для включения контроля за USB-устройствами необходимо установить отметку в пункте «Активировать контроль портов», нажать кнопку «Проверить», а затем кнопку «Применить». Служба usbguard будет запущена и добавлена в автозагрузку (Рис. 84).

Контроль портов активирован

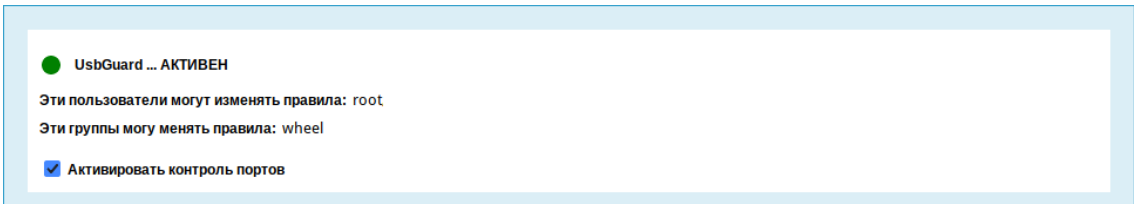


Рис. 84

Примечание. По умолчанию будет установлен режим «Белый список»: «Заблокировать все, кроме подключенных устройств», поэтому все подключенные устройства будут добавлены в список разрешённых, а все новые USB-устройства будут блокироваться. Изменить поведение по

умолчанию можно, установив нужный режим перед запуском службы usbguard (см. «Предустановки»).

Для отключения контроля за USB-устройствами необходимо снять отметку с поля «Активировать контроль портов», нажать кнопку «Проверить», а затем кнопку «Применить» и перезагрузить систему.

4.9.13.2 Список USB-устройств

Если служба usbguard запущена, в веб-интерфейсе будет отображён список текущих подключённых устройств (Рис. 85).

USBGuard. Список USB-устройств

Рис. 85

В столбце «Статус» отображается текущее состояние USB-устройства («allow» – разрешённое устройство, «block» – заблокированное устройство).

Для редактирования состояния USB-устройства необходимо выделить строку с нужным устройством и нажать кнопку «Разблокировать»/«Заблокировать». При этом будет добавлено соответствующее правило в таблицу «Хэш».

Примечание. Если активен «Белый список», то для устройства со статусом «block» будет активна кнопка «Разблокировать», если активен «Чёрный список», то для устройства со статусом «allow» будет активна кнопка «Заблокировать».

Кнопка «Сканировать устройства» позволяет обновить список подключённых USB-устройств.

4.9.13.3 Предустановки

Правила могут работать в режиме белого или чёрного списка (Рис. 86). После установки режима «Чёрный список», будут заблокированы только перечисленные в данном списке USB-устройства. После установки режима «Белый список», будут заблокированы все USB-устройства, кроме перечисленных в данном списке.

Модуль «USBGuard». Предустановки

Рис. 86

Кроме ручного режима добавления правил в списки существует возможность предварительной настройки списков. Для предварительной настройки правил необходимо:

1) выбрать соответствующий пункт:

- «Белый список»:

- «Заблокировать все, кроме подключенных устройств» – в правила (таблица «Хэш») с действием «allow» будут добавлены все подключенные устройства. Все новые USB-устройства будут заблокированы (будут отображаться в таблице «Список устройств» со статусом «block»);
- «Заблокировать все, кроме подключенных и HID/HUB устройств» – в правила с действием «allow» будут добавлены все подключенные устройства (таблица «Хэш») и все устройства с интерфейсами 03:*:* и 09:*:* (таблица «Маски CC:SS:PP»). Все новые USB-устройства кроме HID/HUB-устройств (клавиатуры, мыши, джойстики, USB-концентраторы) будут заблокированы (будут отображаться в таблице «Список устройств» со статусом «block»);
- «Ручной режим» – позволяет установить свои правила.

- «Чёрный список»:

- «Блокировать устройства по классам дескриптора интерфейса: 06 Image и 08 Mass Storage» – в правила (таблица «Маски CC:SS:PP») с действием «block» будут добавлены все устройства с интерфейсами 08:*:* и 06:*:*. Все USB-устройства Mass Storage Device (USB-накопитель, карта памяти, кардридер, цифровая фотокамера) и Image (веб-камера, сканер) будут заблокированы (будут отображаться в таблице «Список устройств» со статусом «block»);
- «Блокировать устройства по списку известных PID:VID, использующих Android Debug Bus» – в правила (таблица «Маски VID:PID») с действием «block» будут

добавлены известные Android-устройства. Все Android-устройства будут заблокированы (будут отображаться в таблице «Список устройств» со статусом «block»);

- «Ручной режим» – позволяет установить свои правила.

2) нажать кнопку «Проверить». Будут показаны планируемые изменения (Рис. 87);
3) если изменения корректные, нажать кнопку «Применить».
4) для отмены изменений (до нажатия кнопки «Применить») следует выбрать пункт «Ручной режим», нажать кнопку «Проверить», а затем «Применить».

Планируемые изменения

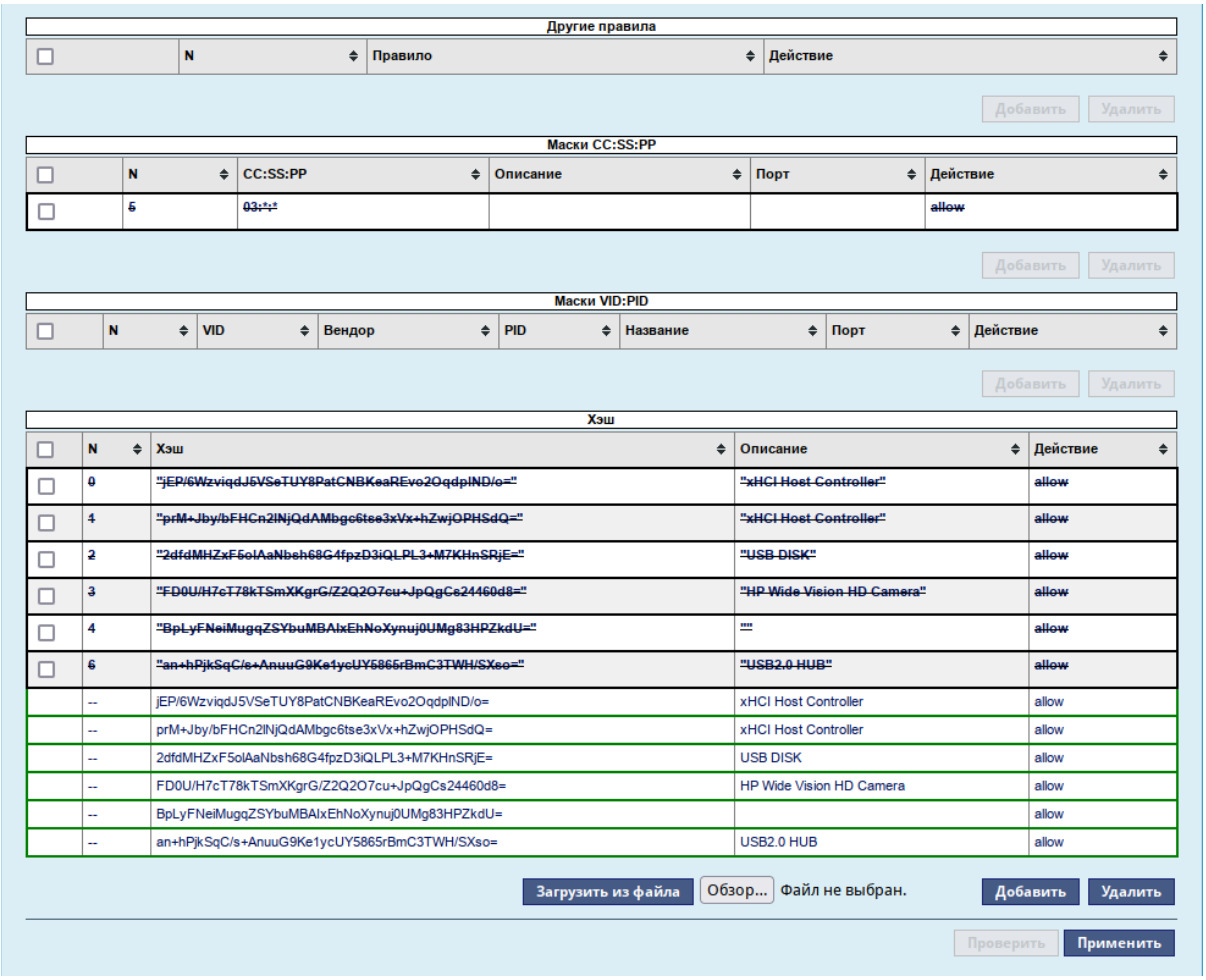


Рис. 87

4.9.13.4 Добавление правил

Для добавления нового правила должен быть выбран пункт «Ручной режим» в белом или чёрном списках. Если «Ручной режим» выбран в белом списке, правило будет добавлено с действием «allow», если в чёрном – с действием «block».

4.9.13.4.1 Правила по классу интерфейса

Назначение USB-устройств может определяться кодами классов, которые сообщаются USB-узлу для загрузки необходимых драйверов. Коды классов позволяют унифицировать работу с

однотипными устройствами разных производителей. Устройство может поддерживать один или несколько классов, максимальное количество которых определяется количеством доступных endpoints. Например, широко известны устройства класса Human Interface Device, HID (мыши, клавиатуры, игровые манипуляторы и т.д.) или устройства Mass Storage (USB-накопители, карты памяти и т.д.).

Примечание. Класс интерфейса указывается как три 8-битных числа в шестнадцатеричном формате, разделенных двоеточием (CC:SS:PP). Числа обозначают класс интерфейса (CC), подкласс (SS) и протокол (PP). Вместо номера подкласса и протокола можно использовать символ *, чтобы соответствовать всем подклассам или протоколам. Сопоставление определенного класса и определенного протокола не допускается, то есть если в качестве номера подкласса используется *, то для протокола также необходимо использовать *.

Добавление правила по маске:

1) под таблицей «Маски CC:SS:PP» нажать кнопку «Добавить»;
2) в поле «CC:SS:PP» вписать маску, например, правило для всех устройств с интерфейсами 09:*:* (Рис. 88);
3) нажать кнопку «Проверить». Корректное правило будет выделено зелёным цветом (Рис. 89), некорректное – красным;
4) исправить или удалить некорректное правило и повторно нажать кнопку «Проверить»;
5) нажать кнопку «Применить» для активации правила. Правило для всех устройств с интерфейсами 09:*:* будет добавлено.

Добавление правила для всех устройств с интерфейсами 09::**

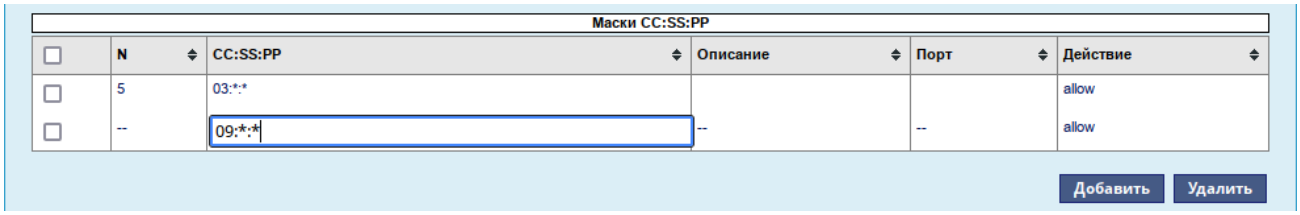


Рис. 88

Проверка правила

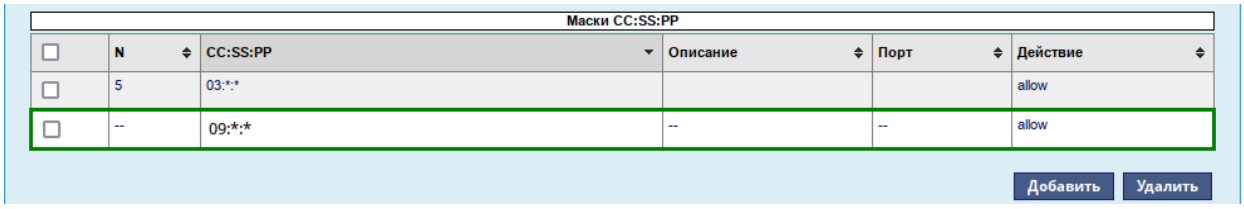


Рис. 89

4.9.13.4.2 Правила по VID&PID

Каждое USB-устройство содержит атрибуты, куда входит идентификатор разработчика устройства (VID) и идентификатор изделия (PID). На основании этих идентификаторов узел (компьютер) ищет методы работы с этим устройством (обычно это выражается в требовании установить драйверы, поставляемые разработчиком устройства).

Примечание. VID и PID – это 16-битные числа в шестнадцатеричной системе счисления. В правиле можно также использовать символ *:

- для соответствия любому идентификатору устройства *:*
- для соответствия любому идентификатору продукта от конкретного поставщика, например, 090c:*

Добавление правила по VID&PID:

1) под таблицей «Маски VID:PID» нажать кнопку «Добавить»;
2) в поле «VID» вписать идентификатор разработчика устройства (VID), а в поле «PID» идентификатор изделия (PID) (Рис. 90);
3) нажать кнопку «Проверить». Корректное правило будет выделено зелёным цветом, некорректное – красным;
4) исправить или удалить некорректное правило и повторно нажать кнопку «Проверить»;
5) нажать кнопку «Применить» для активации правила.

Добавление правила по VID& PID

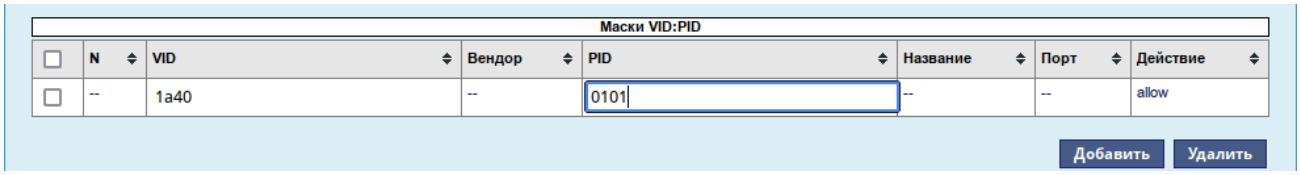


Рис. 90

4.9.13.4.3 Правила по хешу

Для каждого USB-устройства USBGuard вычисляет хеш на основе значений атрибутов устройства и данных дескриптора USB (PID+VID+SN).

Добавление правила по хешу:

1) под таблицей «Хэш» нажать кнопку «Добавить»;
2) в поле «Хэш» вписать хеш устройства (Рис. 91);
3) нажать кнопку «Проверить». Корректное правило будет выделено зелёным цветом, некорректное – красным;
4) исправить или удалить некорректное правило и повторно нажать кнопку «Проверить»;
5) нажать кнопку «Применить» для активации правила.

Добавление правила по хешу

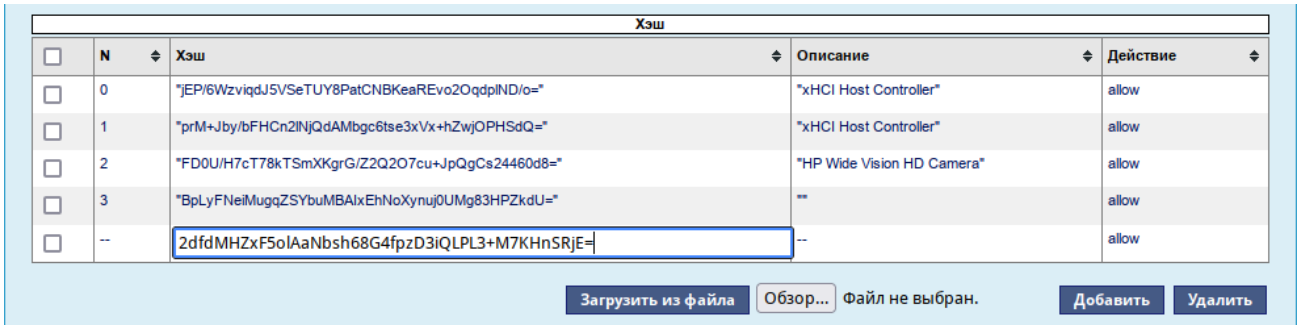


Рис. 91

4.9.13.4.4 Другие правила

Модуль позволяет создавать сложные правила с дополнительными условиями.

Добавление сложного правила:

1) под таблицей «Другие правила» нажать кнопку «Добавить»;
2) в поле «Правило» вписать правило (Рис. 92). Например, правило, разрешающее подключение принтера только через определённый порт:

```
allow id 04a9:177a name "Canon E400" serial "F572EC" via-port "1-2" hash "eql9yA8m+5VVMmhXOvbUzwNPDGCAPq+fxIQHvbptlsY="
```

3) нажать кнопку «Проверить». Корректное правило будет выделено зелёным цветом, некорректное – красным;
4) исправить или удалить некорректное правило и повторно нажать кнопку «Проверить»;
5) нажать кнопку «Применить» для активации правила.

Добавление сложного правила

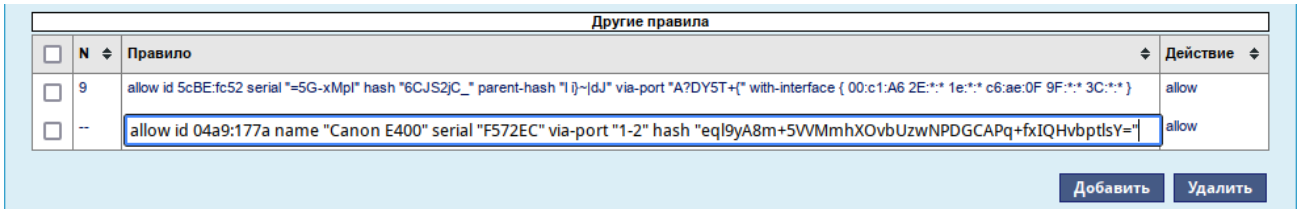


Рис. 92

4.9.13.4.5 Загрузка правил из файла

Правила должны быть добавлены в csv-файл, по одному правилу в каждой строке. Строка должна иметь вид:

```
allow/block,Interface,PID:VID,Hash
```

Например:

```
allow,,090c:1000,"2dfdMHZxF5olAaNbsh68G4fpzD3iQLPL3+M7KHnSRjE="
allow,00:00:*,,
allow,,1000:*,
```

```
allow,,,"eql9yA8m+5VVMmhXOvbUzwNPDGCAPq+fxIQHvbptlsY="
```

Примечание. Файл не должен содержать конфликтные правила – должны быть либо все allow, либо все block.

Загрузка правил из файла:

1) нажать кнопку «Обзор» (под таблицей «Хэш») и выбрать файл с правилами;
2) нажать кнопку «Загрузить из файла»;
3) нажать кнопку «Проверить». Корректное правило будет выделено зелёным цветом, некорректное – красным;
4) исправить или удалить некорректное правило и повторно нажать кнопку «Проверить»;
5) нажать кнопку «Применить» для активации правила.

Примечание. При загрузке правил из файла политика тоже будет выбрана из файла. Если в файле указана политика противоположная текущей, все существующие правила будут удалены.

4.9.13.5 Удаление правил

Пример удаления правила по маске:

1) в таблице «Маски CC:SS:PP» установить отметку в поле с соответствующим правилом;
2) нажать кнопку «Удалить». Правило будет готово к удалению (Рис. 93);
3) нажать кнопку «Проверить»;
4) нажать кнопку «Применить» для удаления правила.

Удаление правила

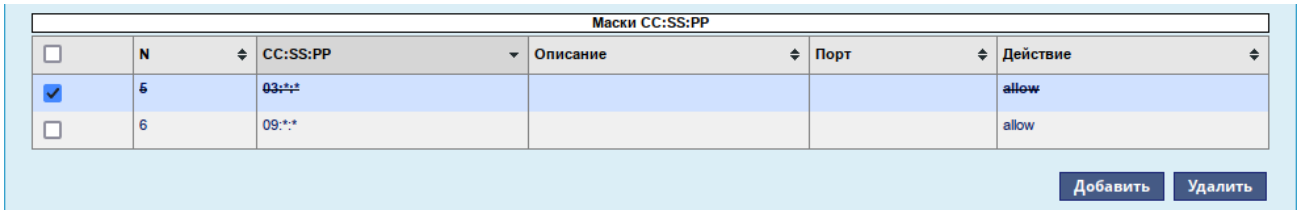


Рис. 93

Правила из других таблиц удаляются аналогичным способом.

4.9.13.6 Просмотр журнала аудита

Для просмотра журнала событий подключения/отключения USB-устройств (журнала аудита) необходимо нажать кнопку «Журнал», расположенную в левом нижнем углу модуля. По нажатию на эту кнопку раскрывается журнал аудита (Рис. 94).

Примечание. Для обновления журнала необходимо нажать кнопку «Фильтровать».

Журнал аудита USBGuard

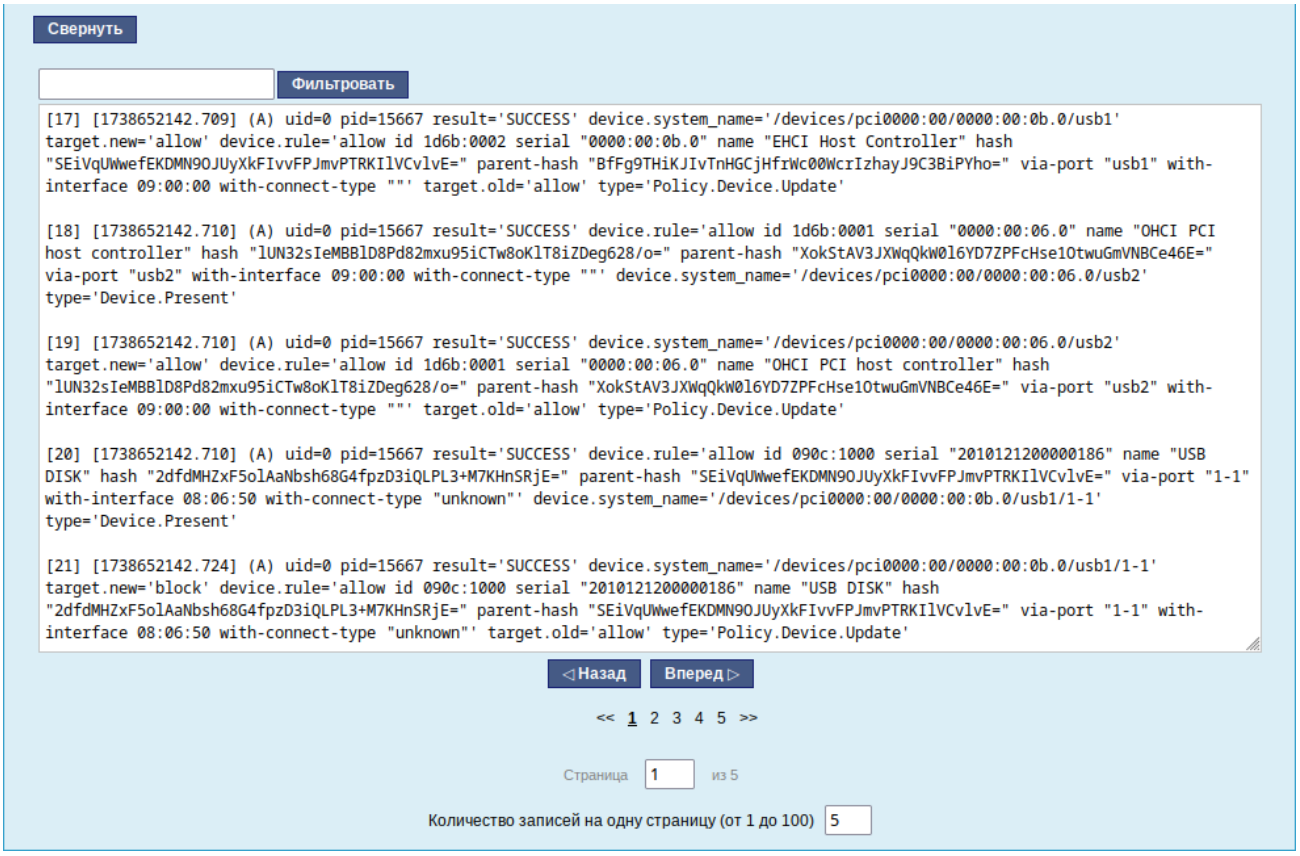


Рис. 94

Примечание. Фильтрация по логу USBGuard – строгая, регистрозависимая.

4.9.14 Настройка ограничения доступа к файловой системе USB-устройства

Модуль ЦУС «USBMount» (пакет alterator-usbmount) из раздела «Система» позволяет ограничить доступ к файловой системе USB-устройства по UID/GID. В модуле также предусмотрена возможность просмотра журнала событий подключения/отключения USB-устройств.

Особенности работы модуля:

- если для устройства не создано правило, то служба не вмешивается в логику монтирования USB-устройства;
- если для устройства создано правило, то служба монтирует блочные устройства на назначенном USB-устройстве в каталог /media/alt-usb-mount/$user_$group или /media/alt-usb-mount/root_$group, если пользователь не указан;
- служба назначает ACL для указанного пользователя и группы на каталог, в котором будет создана точка монтирования блочного устройства;
- в правилах можно указать только существующего локального пользователя и пользовательскую группу;
- доступ к USB-устройству назначенному пользователю и группе предоставляется полностью (rw);

- любой пользователь может отмонтировать устройство через стандартные средства ОС;
- служба не вмешивается в права самих файловых систем блочных устройств;
- рекомендуемая файловая система для переносных носителей exFAT.

Примечание. Особенности работы модуля с файловыми системами:

- EXT2/3/4, XFS, BTRFS поддерживают права. Доступ к файловой системе будет также определяться назначенными правами самой файловой системы;
- FAT16/FAT32/exFAT не поддерживают права. Доступ будет полностью определяться через точку монтирования, назначенную в USBMount;
- ISO9660/UDF поддерживает только readonly. Доступ будет предоставлен только на чтение;
- NTFS поддерживает права. Не рекомендуется использовать. В случае если ранее NTFS носитель был извлечён небезопасно, то носитель будет смонтирован только для чтения.

4.9.14.1 Запуск/останов службы

В модуле отображается текущее состояние службы USBMount (Рис. 95).

Для включения контроля над устройствами необходимо передвинуть переключатель «Служба USBMount остановлена» и нажать кнопку «Сохранить». Служба USBMount будет запущена и добавлена в автозагрузку.

Для отключения контроля над устройствами необходимо передвинуть переключатель «Служба USBMount активна» и нажать кнопку «Сохранить».

Служба USBMount остановлена

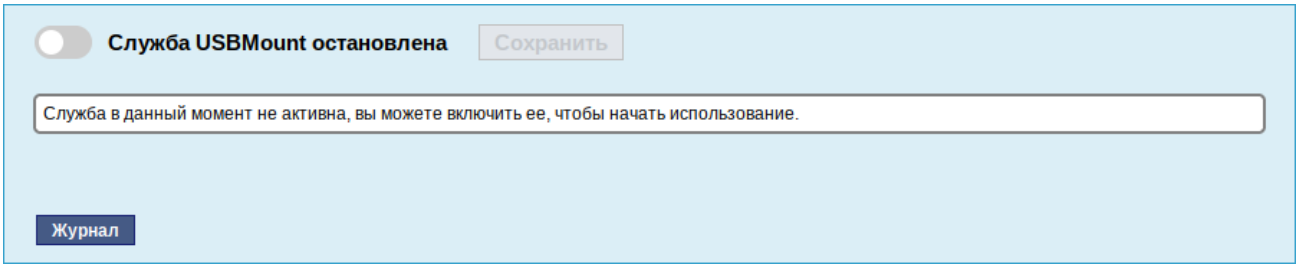


Рис. 95

4.9.14.2 Список устройств

Если служба USBMount запущена, в веб-интерфейсе будет отображён список текущих подключённых устройств (Рис. 96).

Служба USBMount запущена

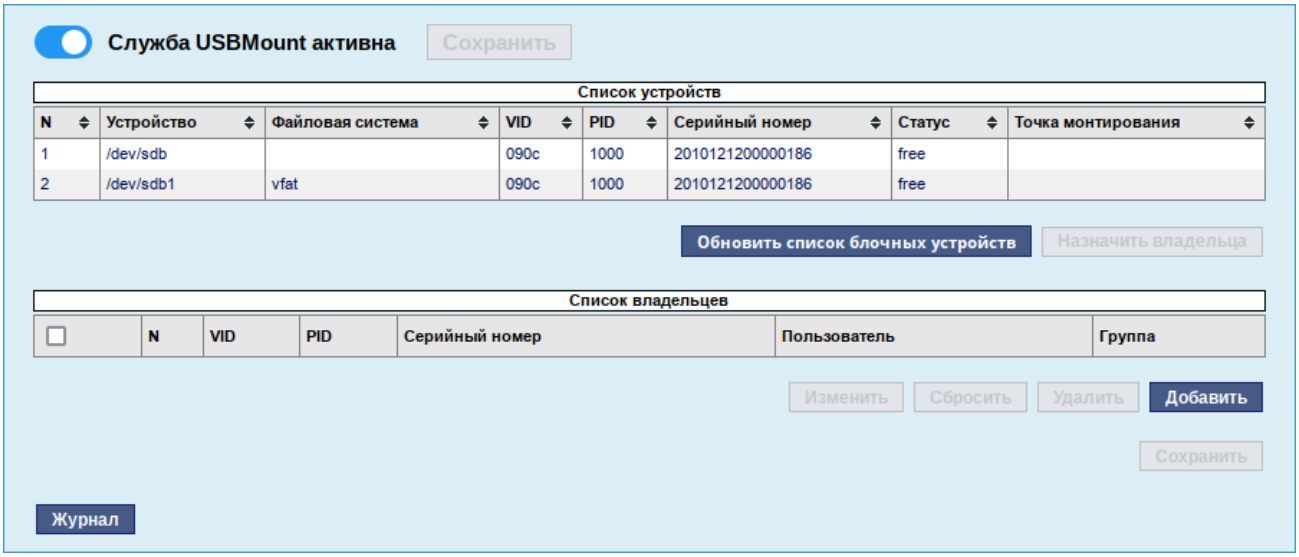


Рис. 96

В столбце «Статус» отображается текущее состояние устройства («free» – владелец для устройства не назначен, «owned» – устройству назначен владелец).

Если устройству назначен владелец и устройство примонтировано, то текущая точка монтирования отображается в столбце «Точка монтирования».

Кнопка «Обновить список блочных устройств» позволяет обновить список подключённых устройств.

4.9.14.3 Добавление/удаление правил

Для того чтобы назначить права для подключенного блочного устройства, необходимо выполнить следующие действия:

1) выделить строку с нужным устройством в таблице «Список устройств» (Рис. 97) и нажать кнопку «Назначить владельца» (или дважды щелкнуть мышью по строке с устройством):
2) правило будет добавлено в таблицу «Список владельцев» (Рис. 98);
3) в столбце «Пользователь» выбрать пользователя, в столбце «Группа» – группу владельца блочного устройства (Рис. 99);
4) нажать кнопку «Сохранить». Статус устройства в таблице «Список устройств» изменится на «owned» (Рис. 100).

Назначение владельца для подключенного устройства

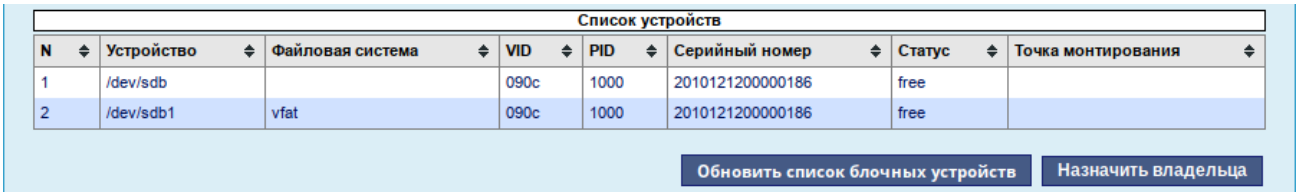


Рис. 97

Правило добавлено в таблицу «Список владельцев»

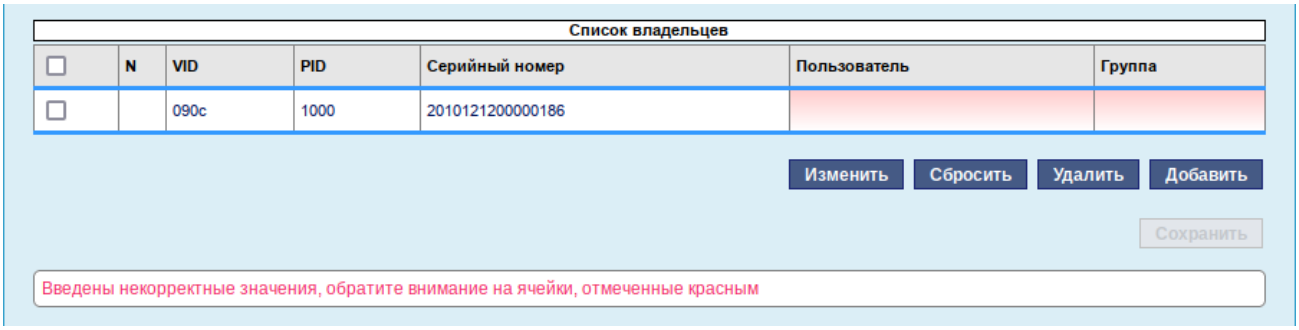


Рис. 98

Указание пользователя и группы для блочного устройства

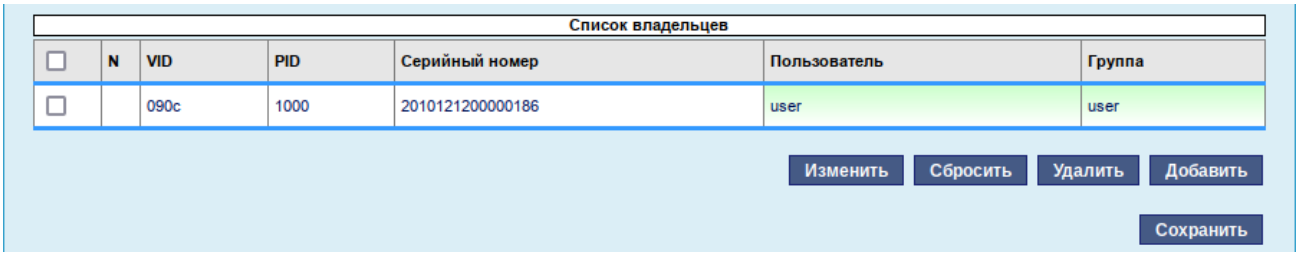


Рис. 99

Статус «owned» для устройства в таблице «Список устройств»

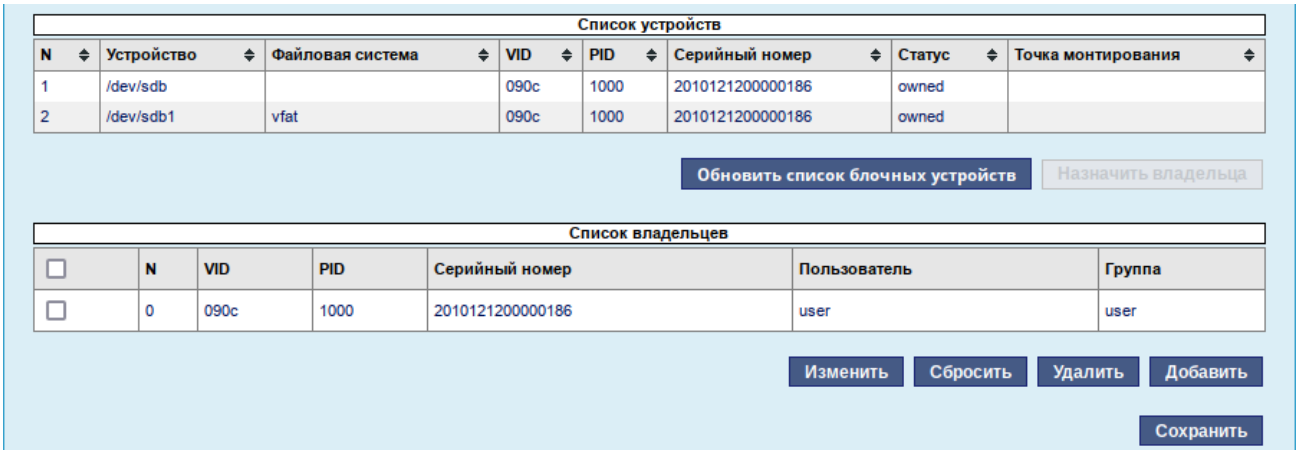


Рис. 100

Примечание. При создании/редактировании правила, некорректные значения будут выделены красным цветом, корректные – зелёным.

Чтобы назначить права для произвольного блочного устройства, необходимо:

1) нажать кнопку «Добавить», расположенную под таблицей «Список владельцев». В таблицу будет добавлена пустая строка (Рис. 101);
2) в соответствующих столбцах указать «VID, PID» и «Серийный номер устройства» (Рис. 102);
3) в столбце «Пользователь» выбрать пользователя, в столбце «Группа» – группу владельца блочного устройства (Рис. 103);

4) нажать кнопку «Сохранить».

USBMount. Создание нового правила

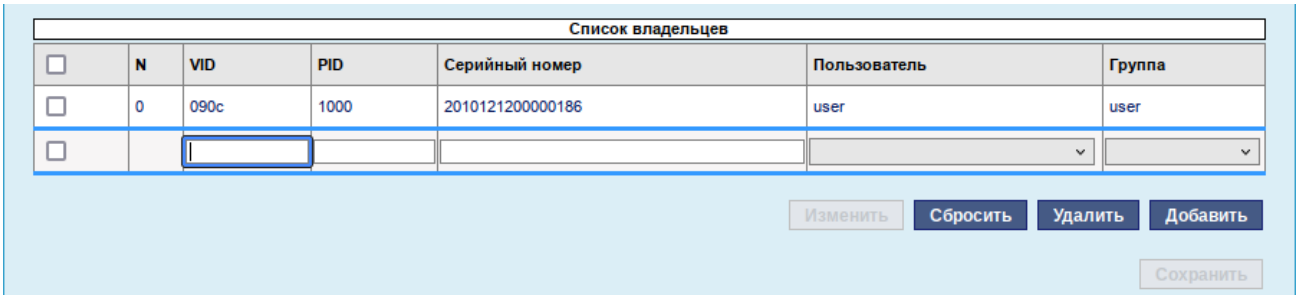


Рис. 101

USBMount. Параметры устройства

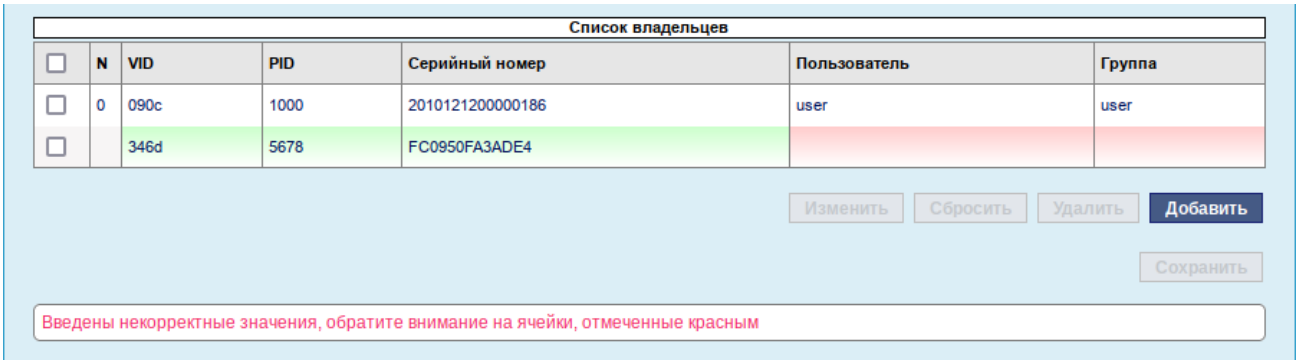


Рис. 102

USBMount. Указание группы для блочного устройства

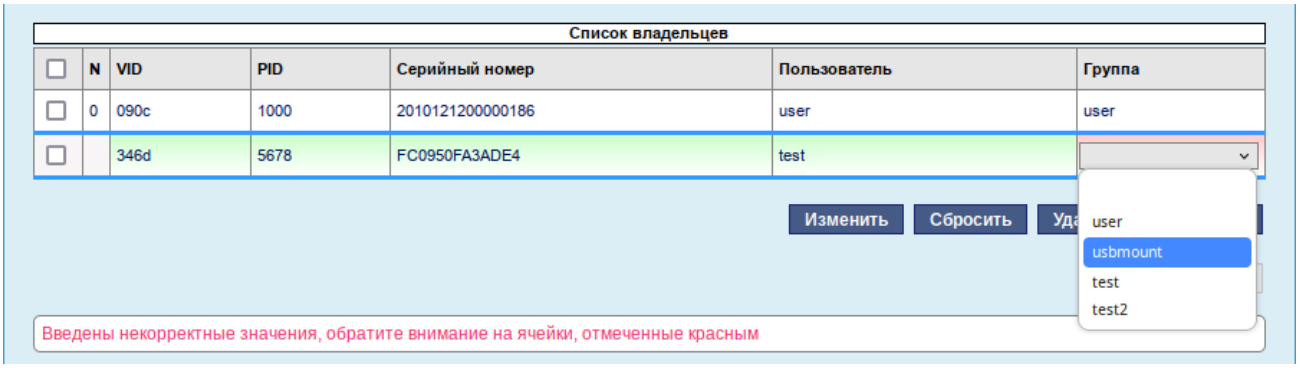


Рис. 103

Примечание. Если необходимо назначить права для определённой группы пользователей, в столбце «Пользователь» следует выбрать прочерк.

Редактирование правила:

1) дважды щелкнуть мышью по строке с правилом в таблице «Список владельцев» (или выделить строку в таблице «Список владельцев» и нажать кнопку «Изменить»);
2) внести изменения;
3) нажать кнопку «Сохранить».

Удаление правила:

1) выделить строку(и) с правилом в таблице «Список владельцев»;
2) нажать кнопку «Удалить» (Рис. 104);
3) нажать кнопку «Сохранить».

USBMount. Удаление правила

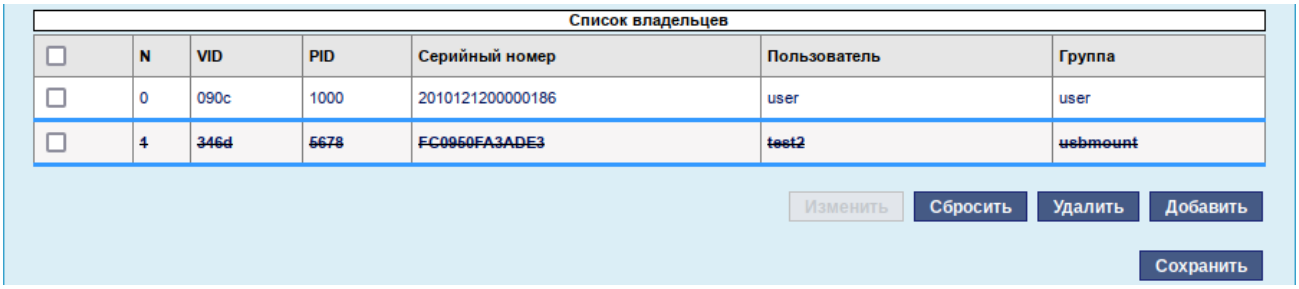


Рис. 104

Примечание. Для отмены внесённых изменений (до нажатия кнопки «Сохранить») следует нажать кнопку «Сбросить».

4.9.14.4 Просмотр журнала аудита

Для просмотра журнала событий подключения/отключения USB-устройств необходимо нажать кнопку «Журнал», расположенную в левом нижнем углу модуля. По нажатию на эту кнопку раскрывается журнал аудита (Рис. 105).

Журнал аудита USBMount

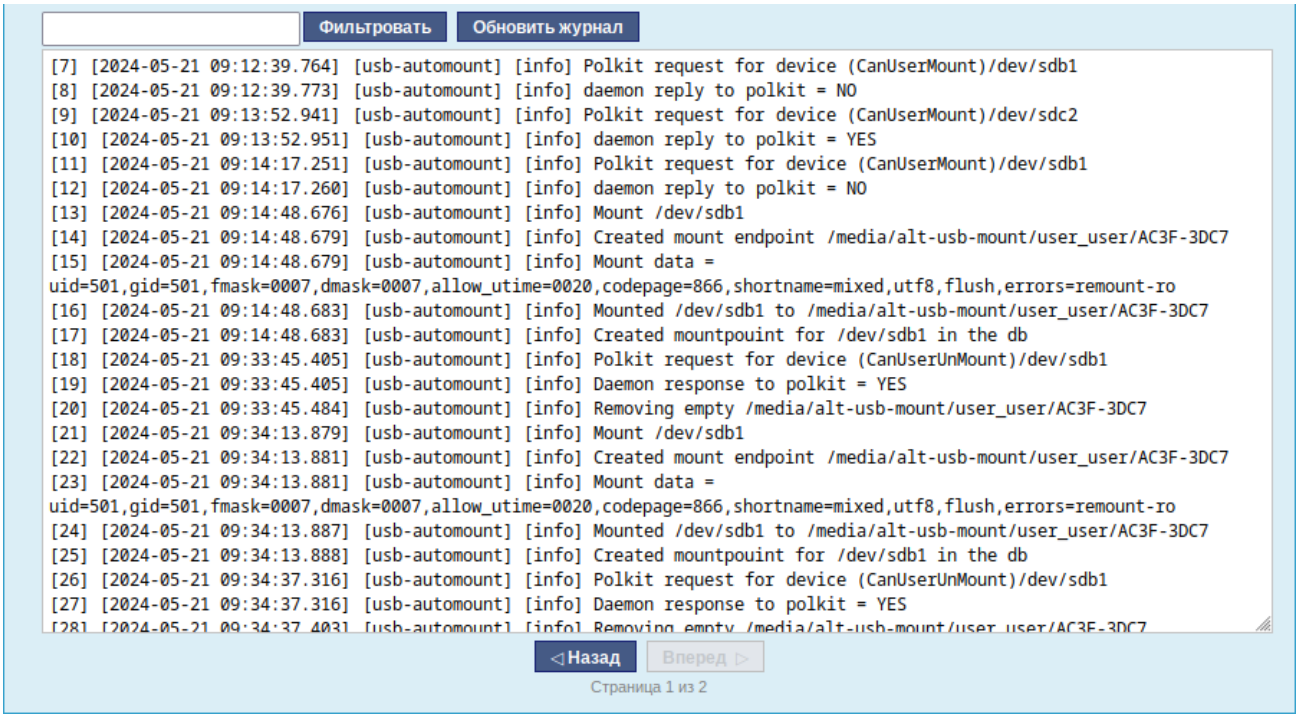


Рис. 105

4.10 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
```

Примечание. После установки модуля, у которого есть веб-интерфейс, для того чтобы он отобразился в веб-интерфейсе, необходимо перезапустить службу ahttpd:

```
# systemctl restart ahttpd
```

4.11 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. 106).

Ссылка «Параметры доступа к модулю»

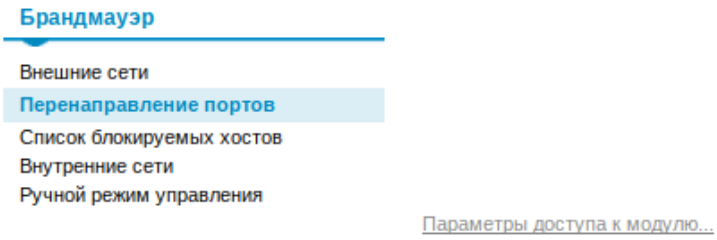


Рис. 106

В открывшемся окне, в списке «Новый пользователь», необходимо выбрать пользователя, который получит доступ к данному модулю, и нажать кнопку «Добавить» (Рис. 107). Для сохранения настроек необходимо перезапустить HTTP-сервер, для этого достаточно нажать кнопку «Перезапустить HTTP-сервер».

Параметры доступа к модулю

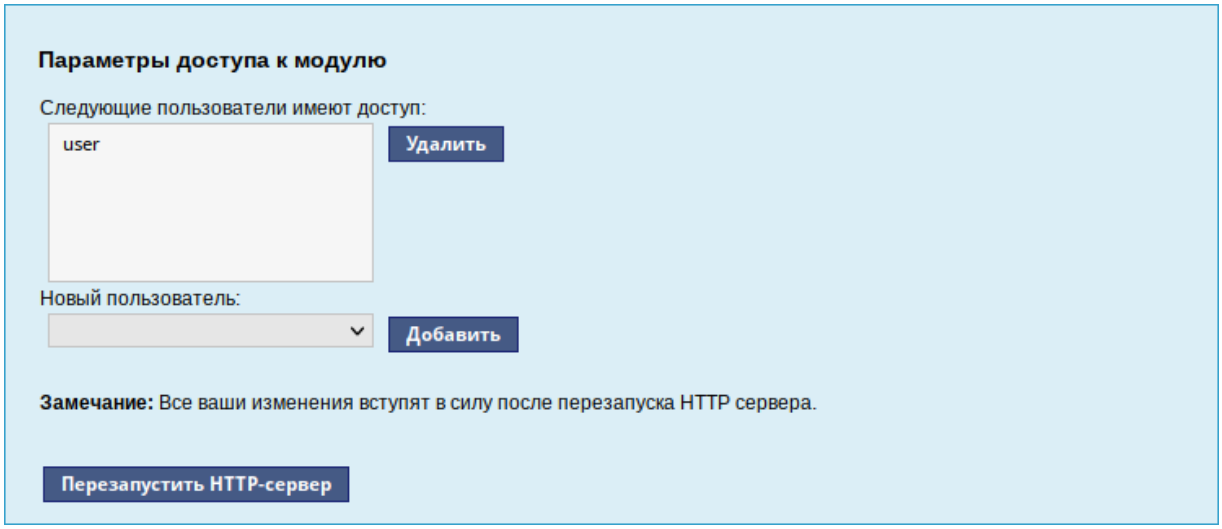


Рис. 107

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, выбрать пользователя, нажать кнопку «Удалить» (Рис. 107) и перезапустить HTTP-сервер.

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

5 КОРПОРАТИВНАЯ ИНФРАСТРУКТУРА

5.1 Альт Домен

«Альт Домен» – служба каталогов (доменная служба), позволяющая централизованно управлять компьютерами и пользователями в корпоративной сети с операционными системами (ОС) на ядре Linux и Windows по единым правилам из единого центра. В системе реализовано хранение данных о пользователях, компьютерах (рабочих станциях) и других объектах корпоративной сети, а также управление профилями пользователей и компьютеров с помощью групповых политик в доменах MS Active Directory / Samba DC.

Примечание. В данном разделе приведена краткая инструкция разворачивания «Альт Домен». Подробную информацию можно в документации к «Альт Домен».

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).

5.1.1 Создание нового домена

5.1.1.1 Установка пакетов

Для Samba DC на базе Heimdal Kerberos необходимо установить пакет `task-samba-dc`, который установит все необходимое:

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

5.1.1.2 Остановка конфликтующих служб

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 systemctl disable
$service; systemctl stop $service; done
```

5.1.1.3 Восстановление к начальному состоянию Samba

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

```
# rm -f /etc/samba/smb.conf
```

```
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

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

5.1.1.4 Выбор имени домена

Имя домена, для разворачиваемого DC, должно состоять минимум из двух компонентов, разделённых точкой.

Примечание. Необходимо избегать суффиксов .local. При указании домена, имеющего суффикс .local, на сервере и подключаемых компьютерах под управлением Linux потребуется отключить службу `avahi-daemon`.

Для установки имени узла и домена следует выполнить команды:

```
# hostnamectl set-hostname <имя узла>
# domainname <имя домена>
```

Например:

```
# hostnamectl set-hostname dc1.test.alt
# domainname test.alt
```

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

5.1.1.5 Сетевые настройки

Для корректной работы сервера должны соблюдаться следующие условия:

- для сервера должно быть задано полное доменное имя (FQDN);
- IP-адрес сервера не должен изменяться;
- в настройках сетевого интерфейса должен быть указан IP-адрес 127.0.0.1 в качестве первичного DNS.

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

- в ЦУС в разделе «Сеть» → «Ethernet интерфейсы» задать имя компьютера и указать в поле «DNS-серверы» 127.0.0.1 (Рис. 108);
- в консоли:
  - задать имя компьютера:

    ```
    # hostnamectl set-hostname dc1.test.alt
    ```

  - указать DNS и домен для поиска в файле `/etc/systemd/network/alterator-enp0s3.network` в разделе `[Network]`:

    ```
    [Match]
         Name = enp0s3
    [Network]
    ```

```
IPv6AcceptRA = false
Domains = test.alt
Address = 192.168.0.122/24
Gateway = 192.168.0.1
DNS = 127.0.0.1
DNS = 8.8.8.8
```

где enp0s3 – имя интерфейса.

Модуль «Ethernet-интерфейсы»

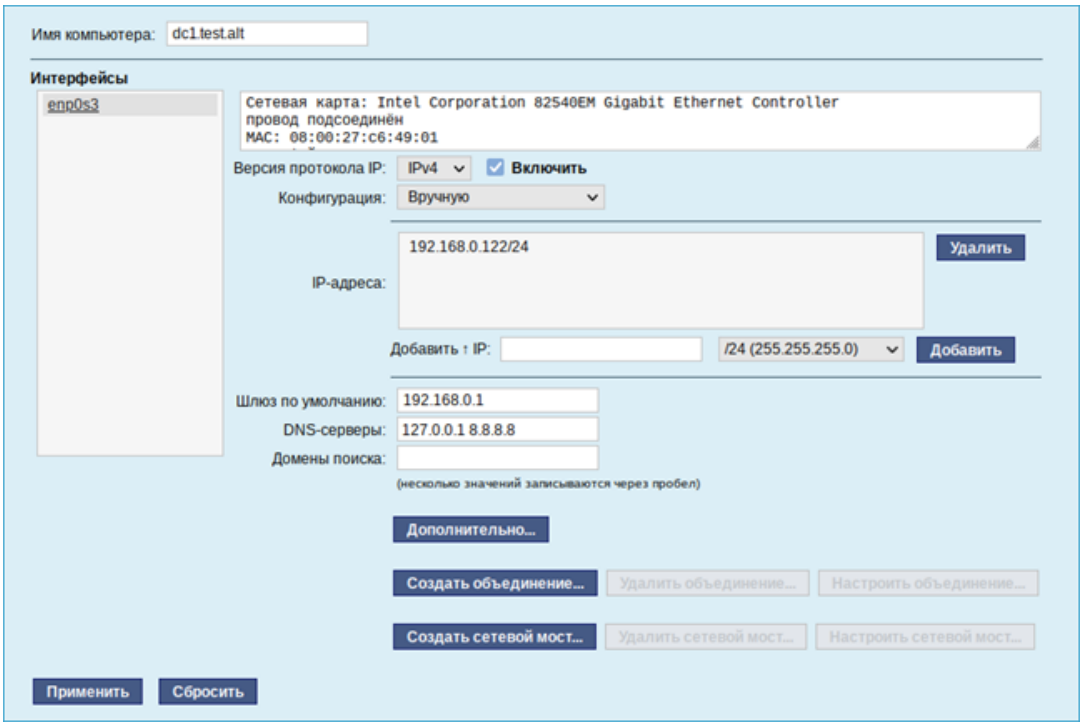


Рис. 108

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

Для того чтобы DNS-сервер Samba управлял зоной test.alt, нужно настроить systemd-resolved для использования FreeIPA в качестве основного DNS-сервера. По умолчанию systemd-resolved прослушивает DNS-запросы на локальном сокете. Чтобы избежать конфликтов с Samba DNS, следует отключить DNSStubListener:

- в файле конфигурации systemd-resolved (/etc/systemd/resolved.conf) установить значение:

```
DNSStubListener=no
```

- перезапустить службу systemd-resolved:

```
# systemctl restart systemd-resolved
```

- убедиться в наличии следующих строк в файле `/etc/resolv.conf`:

```
nameserver 127.0.0.1
search test.alt
```

5.1.1.6 Создание домена в ЦУС

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

1. 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. 109).

   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. 110).

2. Перезагрузить сервер.

Создание домена в ЦУС

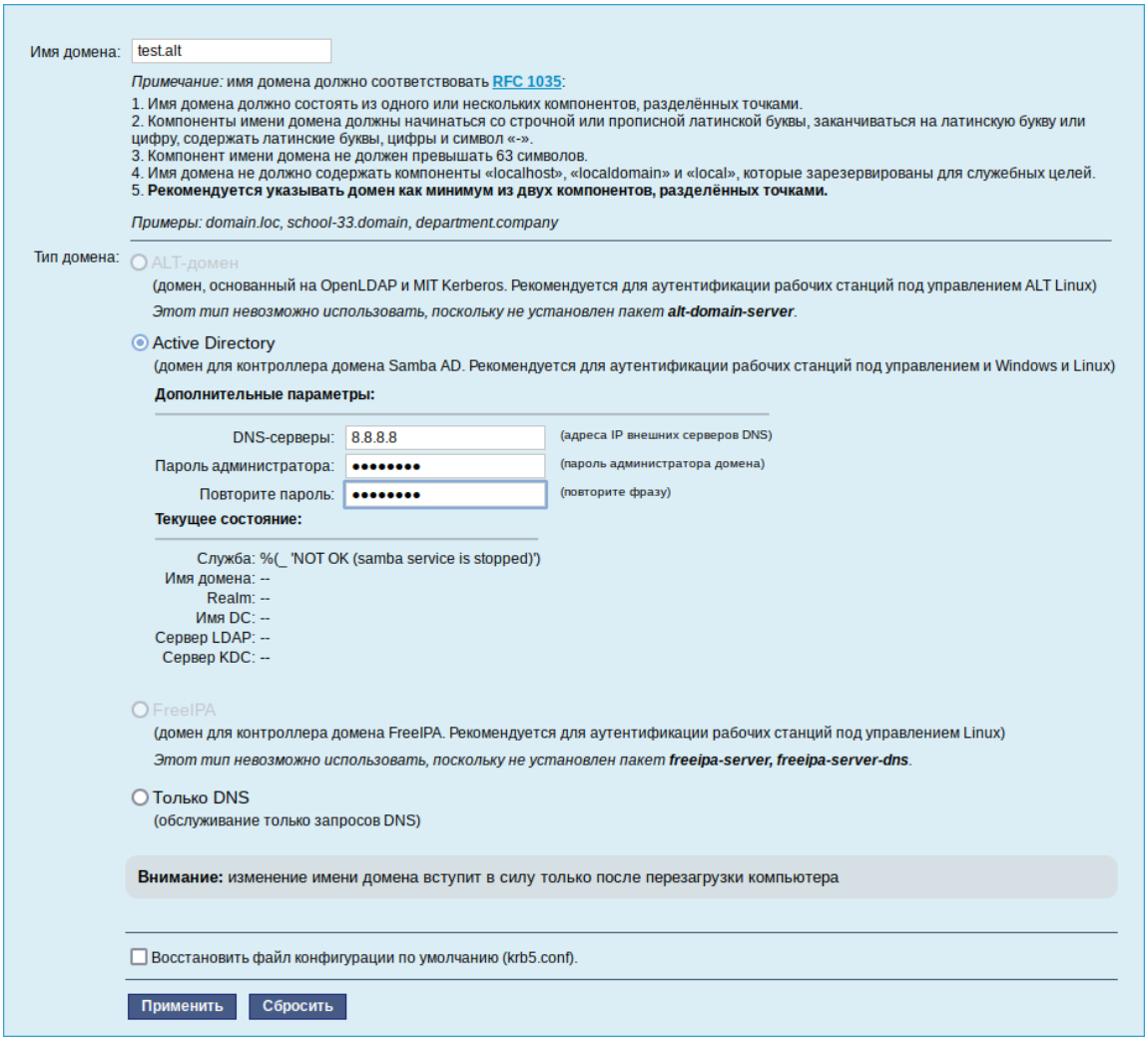


Рис. 109

Информация о созданном домене

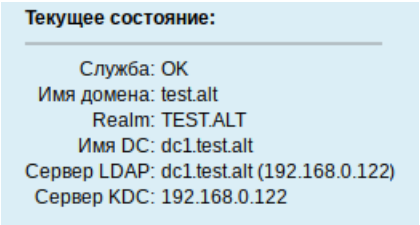


Рис. 110

5.1.1.7 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 \
--option="dns forwarder=8.8.8.8" --server-role=dc --use-rfc2307
```

где

- --realm – область Kerberos (LDAP), и DNS имя домена;
- --domain – имя домена (имя рабочей группы);
- --adminpass – пароль основного администратора домена;
- dns forwarder – внешний DNS-сервер;
- --server-role – тип серверной роли.

Примечание. Параметр `--use-rfc2307` позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

Если уровень не указан, то домен разворачивается на уровне 2008R2. Для разворачивания домена на более высоких уровнях уровень необходимо это явно указать, например:

```
# samba-tool domain provision --realm=test.alt --domain=test \
--adminpass='Pa$$word' --dns-backend=SAMBA_INTERNAL \
--option="dns forwarder = 8.8.8.8" \
--option="ad dc functional level = 2016" \
--server-role=dc --function-level=2016
```

Примечание. Если необходим уровень 2012_R2, то следует сначала развернуть домен на уровне 2008_R2, а затем повысить его до 2012_R2 (см. «Повышение уровня схемы, функционального уровня домена»).

5.1.1.8 Интерактивное создание домена

Примечание. У Samba свой собственный DNS-сервер. В `DNS forwarder IP address` нужно указать внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена.

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]:8.8.8.8
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
Merge the contents of this file with your system krb5.conf or replace
it with this one. Do not create a symlink!
Once the above files are installed, your Samba4 server will be ready
to use
Server Role:           active directory domain controller
Hostname:              dc1
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.

5.1.2 Запуск службы

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

```
# systemctl enable --now samba
```

5.1.3 Настройка Kerberos

Внести изменения в файл `/etc/krb5.conf`. Следует раскомментировать строку `default_realm` и содержимое разделов `realms` и `domain_realm` и указать название домена (обратите внимание на регистр символов), в строке `dns_lookup_realm` должно быть установлено значение `false`:

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

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

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

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

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

[domain_realm]
dc1 = TEST.ALT
```

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

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

5.1.4 Проверка работоспособности домена

Просмотр общей информации о домене:

```
# samba-tool domain info 127.0.0.1

Forest           : test.alt
Domain           : test.alt
Netbios domain   : TEST
DC name          : dc1.test.alt
DC netbios name  : DC1
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
```

Просмотр предоставляемых служб:

```
# smbclient -L localhost -Uadministrator

Password for [TEST\administrator]:

        Sharename       Type      Comment
        ---------       ----      -------
        sysvol          Disk
        netlogon        Disk
        IPC$            IPC       IPC Service (Samba 4.19.9-alt3)
SMB1 disabled -- no workgroup available
```

Общие ресурсы netlogon и sysvol создаваемые по умолчанию нужны для функционирования сервера 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`:

```
# cat /etc/resolv.conf
search test.alt
nameserver 127.0.0.1

# 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 dc1.test.alt.
# host -t SRV _ldap._tcp.test.alt.
_ldap._tcp.test.alt has SRV record 0 100 389 dc1.test.alt.
# host -t A dc1.test.alt.
dc1.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: FILE:/tmp/krb5cc_0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
18.10.2024 11:23:14  18.10.2024 21:23:14  krbtgt/TEST.ALT@TEST.ALT
    renew until 25.10.2024 11:23:10
```

5.1.5 Повышение уровня схемы, функционального уровня домена

Для повышения уровня домена необходимо выполнить следующие действия:

- указать функциональный уровень AD, который будет поддерживаться контроллером домена в параметре `ad dc functional level` файла `/etc/samba/smb.conf`. Возможные значения: 2008_R2, 2012, 2012_R2, 2016;
- обновить схему домена, выполнив команду:

```
# samba-tool domain schemaupgrade --schema=<SCHEMA>
```

где SCHEMA – схема, до которой необходимо выполнить обновление (по умолчанию 2019);

- подготовить функциональный уровень домена, выполнив команду:

```
# samba-tool domain functionalprep --function-level=<FUNCTION_LEVEL>
```

где FUNCTION_LEVEL – функциональный уровень, к которому нужно подготовиться (по умолчанию 2016);

- указать функциональные уровни домена и леса, выполнив команду:

```
# samba-tool domain level raise --domain-level=<DOMAIN_LEVEL> --for-
est-level=<FOREST_LEVEL>
```

где:

- FOREST_LEVEL – уровень работы леса. Возможные значения: 2003, 2008, 2008_R2, 2012, 2012_R2, 2016;
- DOMAIN_LEVEL – уровень работы домена. Возможные значения: 2003, 2008, 2008_R2, 2012, 2012_R2, 2016.

Примечание. При установке значения параметра ad dc functional level в файле /etc/samba/smb.conf вручную, защита от несовпадения функций между контроллерами домена снижается. Поэтому на всех контроллерах домена должна использоваться одна и та же версия Samba, чтобы гарантировать, что поведение, наблюдаемое клиентом, будет одинаковым независимо от того, к какому контроллеру домена осуществляется соединение.

Для повышения уровня схемы и функционального уровня домена необходимо выполнить следующие действия:

- в раздел [global] файла `/etc/samba/smb.conf` добавить строку:

```
ad dc functional level = 2016
```

- перезагрузить службу samba:

```
# systemctl restart samba.service
```

- выполнить команды:

```
# samba-tool domain schemaupgrade --schema=2019
# samba-tool domain functionalprep --function-level=2016
# samba-tool domain level raise --domain-level=2016 --forest-
level=2016
```

- убедиться, что уровни домена и леса повышены:

```
# samba-tool domain level show
Domain and forest function level for domain 'DC=test,DC=alt'
```

```
Forest function level: (Windows) 2016
Domain function level: (Windows) 2016
Lowest function level of a DC: (Windows) 2016
```

5.1.6 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>
```

5.1.7 Присоединение к домену в роли контроллера домена

Для обеспечения отказоустойчивости и балансировки нагрузки в домен могут добавляться дополнительные контроллеры домена.

Заведение дополнительного контроллера домена выполняется путём присоединения дополнительного DC к существующему домену.

На добавляемом DC в `/etc/resolv.conf` обязательно должен быть добавлен первый DC как nameserver. Указать DNS и домен для поиска можно в ЦУС или в etc/systemd/network/alterator-enp0s3.network в разделе [Network]:

```
[Match]
```

```
    Name = enp0s3
[Network]
    IPv6AcceptRA = false
    Domains = test.alt
    Address = 192.168.0.106/24
    Gateway = 192.168.0.1
    DNS = 192.168.0.122
    DNS = 8.8.8.8
```

где enp0s3 – имя интерфейса.

Чтобы избежать конфликтов systemd-resolved с Samba DNS, следует отключить DNSStubListener:

- в файле конфигурации systemd-resolved (/etc/systemd/resolved.conf) установить значение:

```
DNSStubListener=no
```

- перезапустить службу systemd-resolved:

```
# systemctl restart systemd-resolved
```

- убедиться в наличии следующих строк в файле /etc/resolv.conf:

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

Все действия, указанные ниже, выполняются на этом узле dc2.test.alt (192.168.0.106), если не указано иное:

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

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

2. Остановить конфликтующие службы krb5kdc и slapd, а также bind:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable
$service; systemctl stop $service; done
```

3. Очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

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

4. На существующем DC завести адрес IP для нового DC (команда выполняется на узле dc1.test.alt):

```
# samba-tool dns add 192.168.0.122 test.alt DC2 A 192.168.0.106 –Uad-
ministrator
```

Примечание. Указание аутентифицирующей информации (имени пользователя и пароля) обязательно.

5. На новом контроллере домена установить следующие параметры в файле конфигурации клиента Kerberos (файл `/etc/krb5.conf`):

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

6. Для проверки настройки запросить билет Kerberos для администратора домена (имя домена должно быть указано в верхнем регистре):

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

7. Убедиться, что билет получен:

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
18.10.2024 11:28:35  18.10.2024 21:28:35 krbtgt/TEST.ALT@TEST.ALT
       renew until 25.10.2024 11:28:32
```

8. Ввести дополнительный DC в домен test.alt в качестве контроллера домена:

```
# samba-tool domain join test.alt DC -Uadministrator --realm=test.alt
--option="dns forwarder=8.8.8.8"
```

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
```

9. Сделать службу samba запускаемой по умолчанию и запустить её:

```
# systemctl enable –now samba
```

5.1.8 Проверка резудьтатов присоединения

Примечание. После присоединения к домену службе синхронизации данных может понадобиться до 15 минут для автоматического формирования подключений для репликации.

Проверка корректности присоединения:

1. Проверить работу DNS:

```
# host -t A test.alt
test.alt has address 192.168.0.122
```

```
test.alt has address 192.168.0.106
```

В списке адресов должен отображаться IP-адрес добавленного контроллера домена.

2. Проверить статус репликации между контроллерами домена. Для этого на добавленном DC выполнить команду:

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

Примечание. Подробнее о настройке репликации см. в разделе «Репликация».

3. На добавленном DC создать нового пользователя домена:

```
# samba-tool user add testuser --random-password
User 'testuser' added successfully
```

4. Убедиться, что учетная запись созданного пользователя доступна на первом контроллере домена:

```
# samba-tool user list | grep testuser
testuser
```

5.1.9 Репликация

Начиная с версии samba 3.5, топология репликации выстраивается автоматически.

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

Процедура двусторонней репликации:

1. Репликация с первого контроллера домена на второй:

```
# samba-tool drs replicate dc2.test.alt dc1.test.alt dc=test,dc=alt
-Uadministrator
```

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

2. Репликация на первый контроллер домена со второго:

```
# samba-tool drs replicate dc1.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 можно запустить команду на 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.

5.1.10 Подключение к домену на рабочей станции

Для ввода компьютера в «Альт Домен» 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.

Для ввода компьютера в домен, на нём должен быть доступен сервер DNS, имеющий записи про контроллер домена. Ниже приведен пример настройки сетевого интерфейса со статическим IP-адресом. При получении IP-адреса по DHCP данные о сервере DNS также должны быть получены от сервера DHCP.

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. 111);
- 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

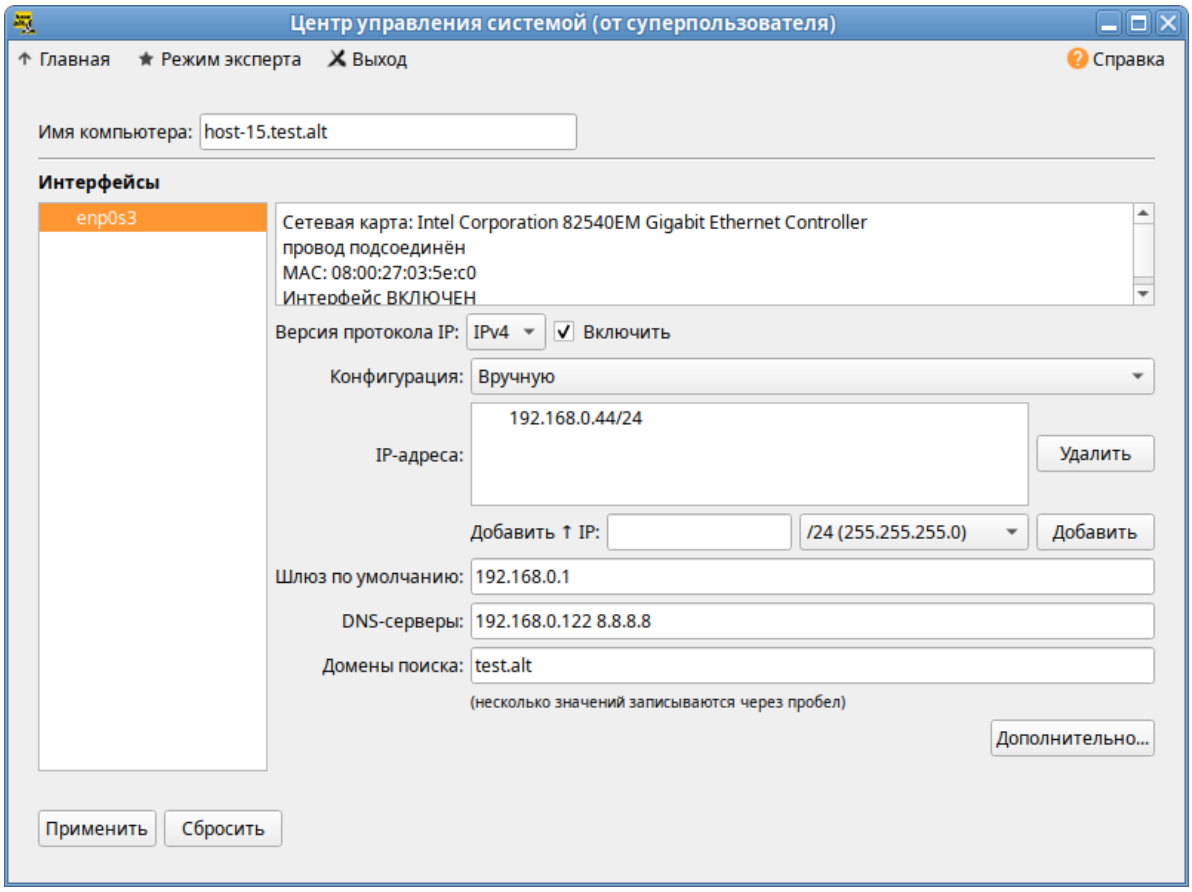


Рис. 111

5.1.10.1 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. 112) и заполнить поля, после чего нажать кнопку «Применить».

В открывшемся окне (Рис. 113) необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку «ОК».

При успешном подключении к домену, отобразится соответствующая информация (Рис. 114).

Далее необходимо перезагрузить рабочую станцию для применения всех настроек.

Ввод в домен в «Центре управления системой»

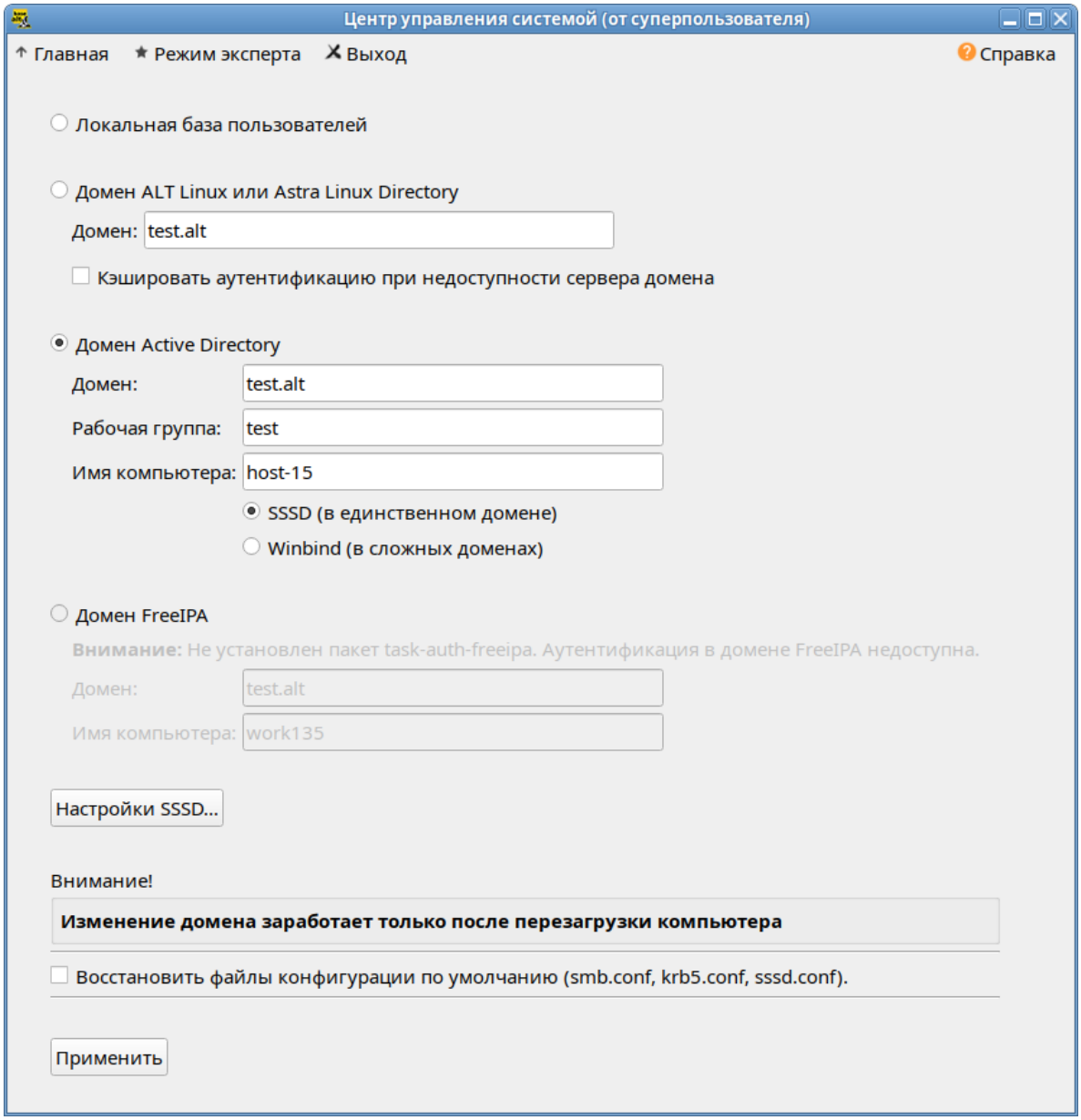


Рис. 112

Параметры учетной записи с правами подключения к домену

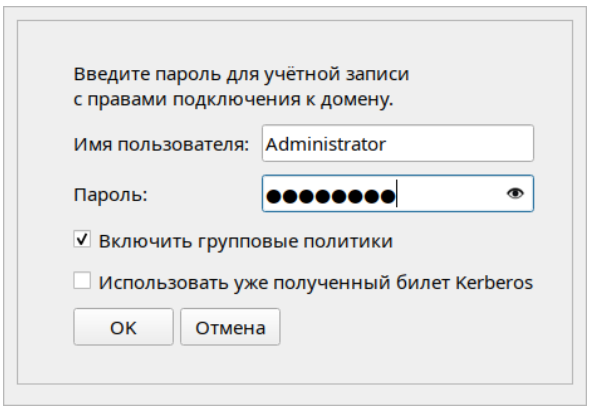


Рис. 113

Успешное подключение к домену

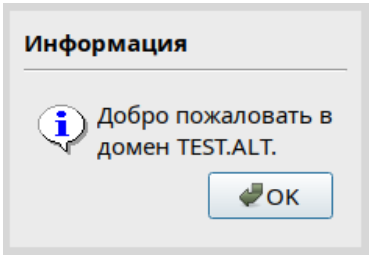


Рис. 114

5.1.10.2 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.

5.2 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 (пакет `admx-firefox`), Google Chrome (пакет `admx-chromium`) и Yandex (пакет `admx-yandex-browser`) 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;
- настройки удаленного доступа к рабочему столу (VNC) и настройки графической среды MATE. Можно установить при использовании ADMX-файлов ALT;
- настройки среды рабочего стола KDE (экспериментальная политика). Можно установить при использовании ADMX-файлов ALT;
- подключения сетевых дисков (экспериментальная политика);
- управления общими каталогами (экспериментальная политика);
- генерирования (удаления/замены) ярлыков для запуска программ;
- создания каталогов;
- управления файлами (экспериментальная политика);
- управления сценариями запуска и завершения работы компьютера, входа и выхода пользователя из системы (экспериментальная политика);
- установки и удаления пакетов (экспериментальная политика).

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

5.2.1 Развертывание групповых политик

Процесс развёртывание групповых политик:

1. Развернуть сервер Samba DC (см. раздел «Альт Домен»).
2. Установить административные шаблоны. Для этого:

- установить пакеты политик `admx-basealt`, `admx-chromium`, `admx-firefox`, `admx-yandex-browser` и утилиту `admx-msi-setup`:

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

- скачать и установить ADMX-файлы от Microsoft, выполнив команду:

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

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

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

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

```
# samba-tool gpo admxload -U Administrator
```

3. Ввести машину в домен по инструкции (см. раздел «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. 113).

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. 115).

Модуль ЦУС «Групповые политики»

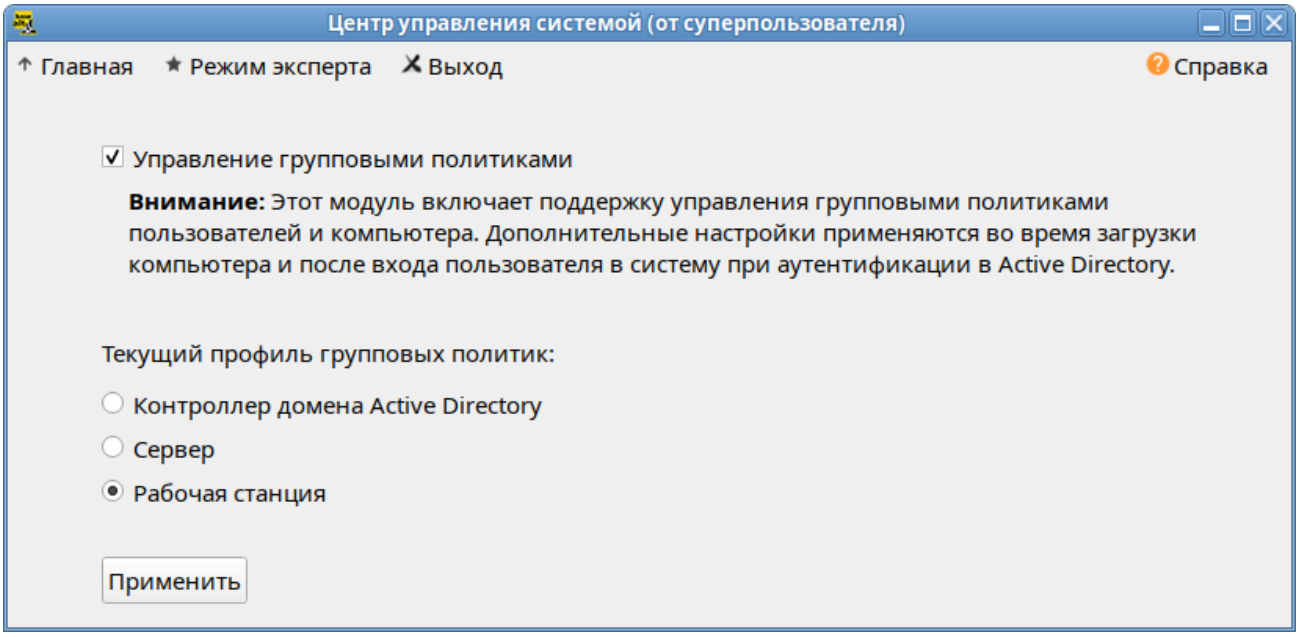


Рис. 115

4. На рабочей станции, введённой в домен, установить административные инструменты (модуль удаленного управления базой данных конфигурации (ADMC) и модуль редактирования настроек клиентской конфигурации (GPUI)):

```
# apt-get install admc gpui
```

Примечание. В настоящее время GPUI не умеет читать файлы ADMX с контроллера домена. Для корректной работы необходимо установить пакеты admx и файлы ADMX от Microsoft:

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

5. Настроить, если это необходимо, RSAT на машине с ОС Windows (управление сервером Samba с помощью RSAT поддерживается из среды до Windows 2012R2 включительно):

- ввести машину с ОС Windows в домен (управление сервером Samba с помощью RSAT поддерживается из среды до Windows 2012R2 включительно);
- включить компоненты удаленного администрирования (этот шаг можно пропустить, если административные шаблоны были установлены на контроллере домена). 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.

6. корректно установленные административные шаблоны будут отображены в оснастке «Редактор управления групповыми политиками» в разделе «Конфигурация компьютера»/ «Конфигурация пользователя» → «Политики» → «Административные шаблоны» (Рис. 116).

Административные шаблоны в консоли gpme.msc

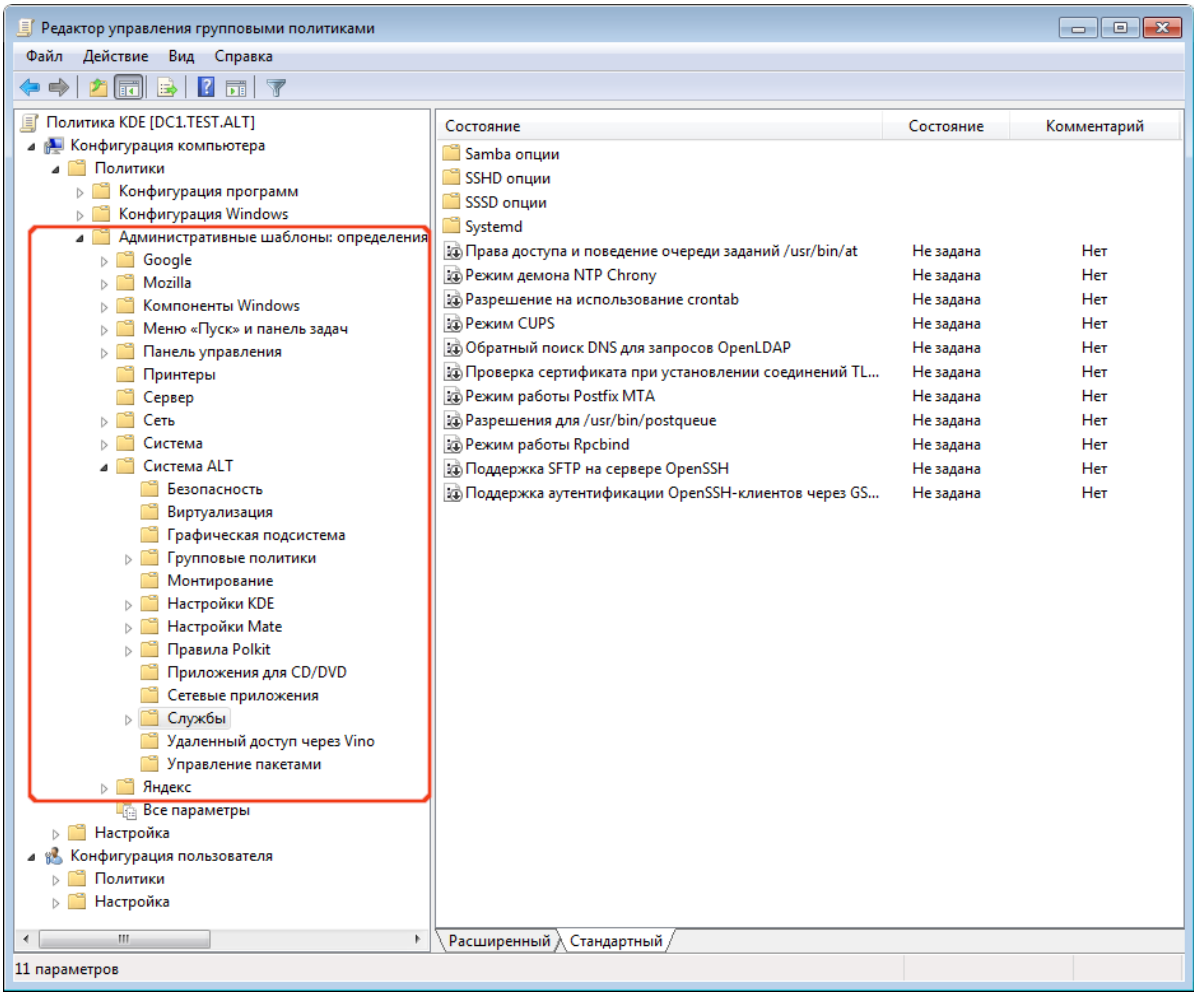


Рис. 116

5.2.2 Пример создания групповой политики

Для создания групповой политики на машине, введённой в домен, необходимо выполнить следующие шаги:

- добавить доменные устройства (компьютеры/пользователи) в подразделение (OU) (инструмент ADMC или оснастка Active Directory «Пользователи и компьютеры»);
- создать политику и назначить её на OU (ADMC или оснастка «Управление групповой политикой»);
- отредактировать параметры политики (GPUI или оснастка «Редактор управления групповыми политиками»).

В качестве примера, создадим политику, разрешающую запускать команду ping только суперпользователю (root).

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

Для использования ADMC следует сначала получить билет Kerberos для администратора домена:

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

Далее запустить ADMC из меню («Меню MATE» → «Системные»→«ADMC») или командой `admc`:

```
$ admc
```

Интерфейс ADMC показан на Рис. 117.

Интерфейс ADMC

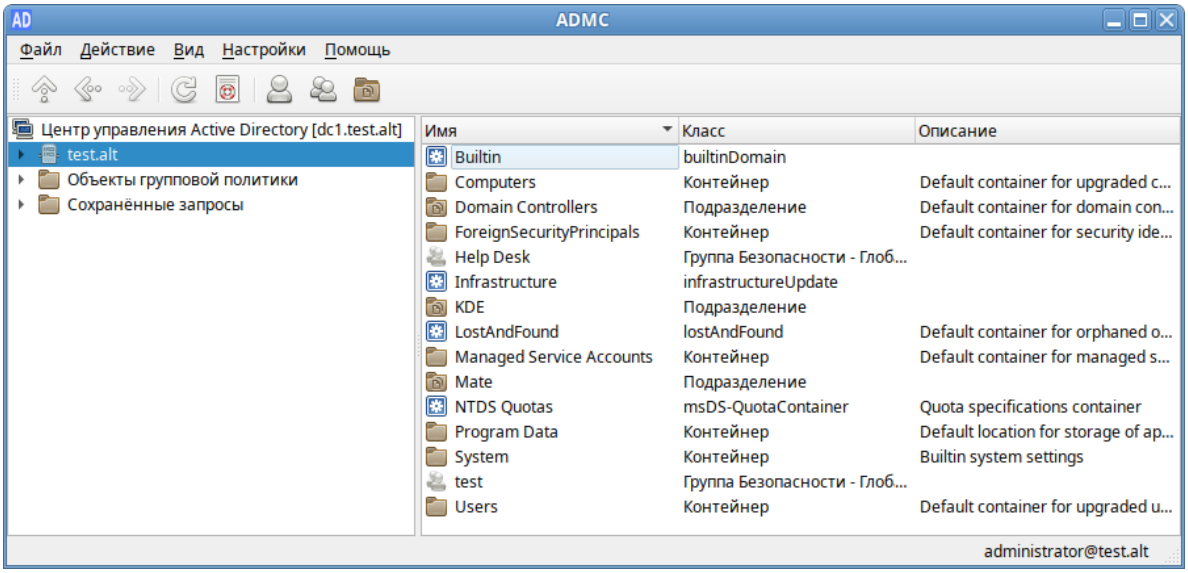


Рис. 117

Для создания подразделения следует:

- в контекстном меню домена выбрать пункт «Создать» → «Подразделение» (Рис. 118);
- в открывшемся окне ввести название подразделения (например, OU) и нажать кнопку «ОК» (Рис. 119).

ADMC. Создание нового подразделения

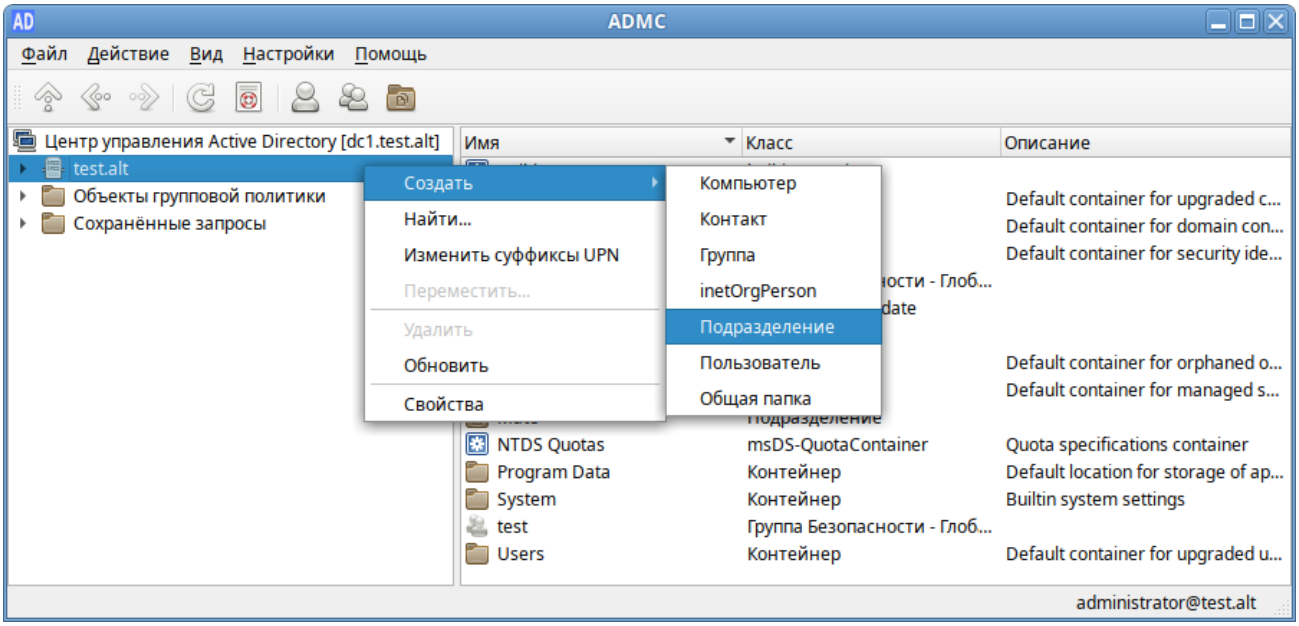


Рис. 118

ADMC. Новое подразделение

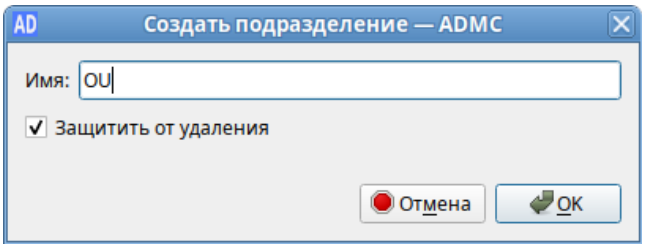


Рис. 119

Далее необходимо переместить компьютеры и пользователей домена в подразделение OU (Рис. 120):

- в контекстном меню пользователя/компьютера выбрать пункт «Переместить…»;
- в открывшемся диалоговом окне «Выбор контейнера – ADMC» выбрать контейнер, в который следует переместить учетную запись пользователя.

Для создания политики для подразделения необходимо:

- в контекстном меню подразделения (в папке «Объекты групповой политики») выбрать пункт «Создать политику и связать с этим подразделением» (Рис. 121);
- в открывшемся окне ввести название политики и нажать кнопку «ОК» (Рис. 122).

Компьютеры и пользователи в подразделении OU

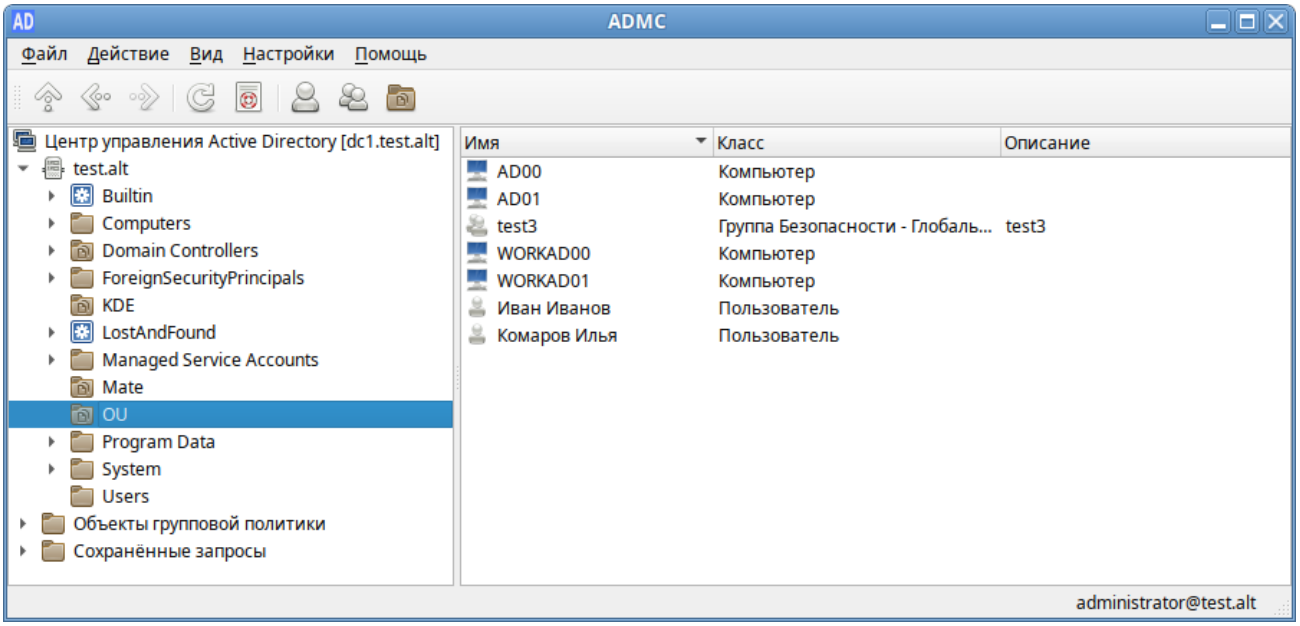


Рис. 120

ADMC. Контекстное меню подразделения в объектах групповых политик

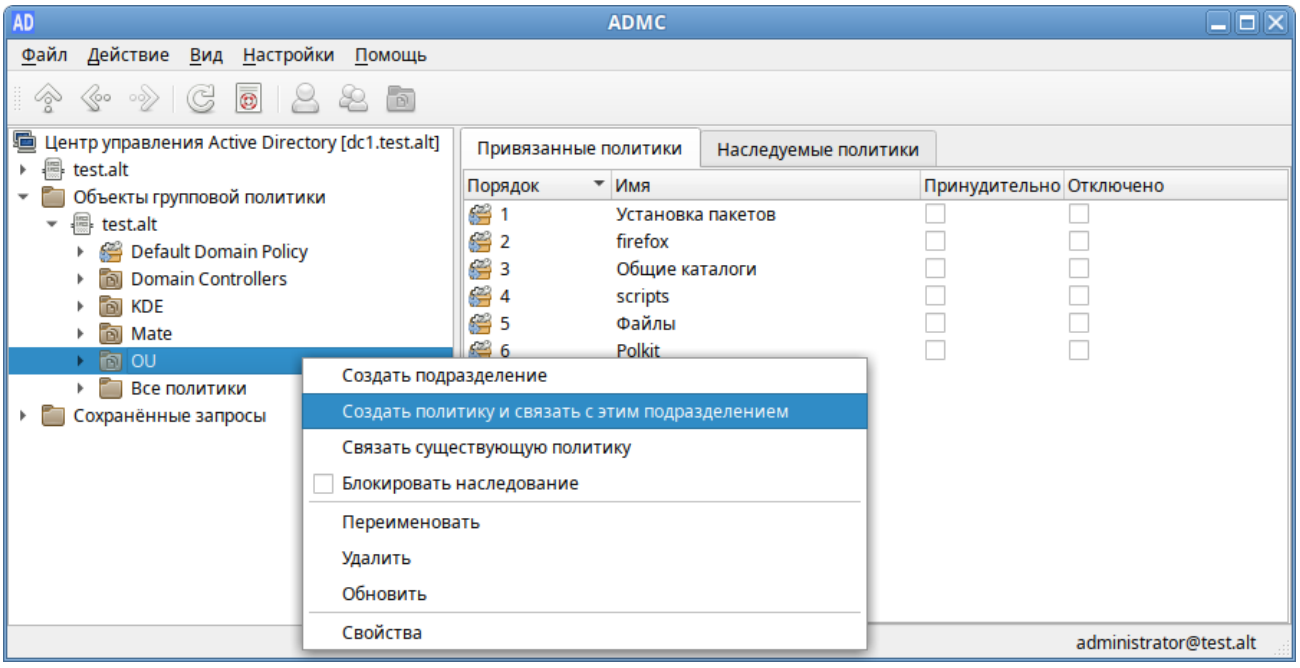


Рис. 121

ADMC. Создание объекта групповой политики

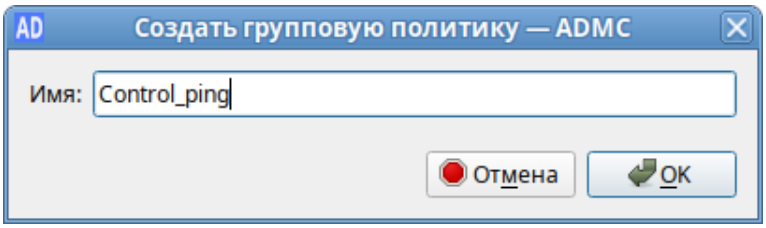


Рис. 122

Редактирование настроек групповой политики:

- в контекстном меню созданной политики выбрать пункт «Изменить…» (Рис. 123);
- откроется окно редактирования групповых политик (GPUI) (Рис. 124);
- перейти в «Компьютер» → «Административные шаблоны» → «Система ALT». Здесь есть несколько разделов, соответствующих категориям control. Выбрать раздел «Сетевые приложения», в правом окне редактора отобразится список политик (Рис. 125);
- щелкнуть левой кнопкой мыши на политике «Разрешения для /usr/bin/ping». Откроется диалоговое окно настройки политики. Выбрать параметр «Включено», в выпадающем списке «Кому разрешено выполнять» выбрать пункт «Только root» и нажать кнопку «ОК» (Рис. 126);
- 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
```

ADMC. Контекстное меню объекта групповой политики

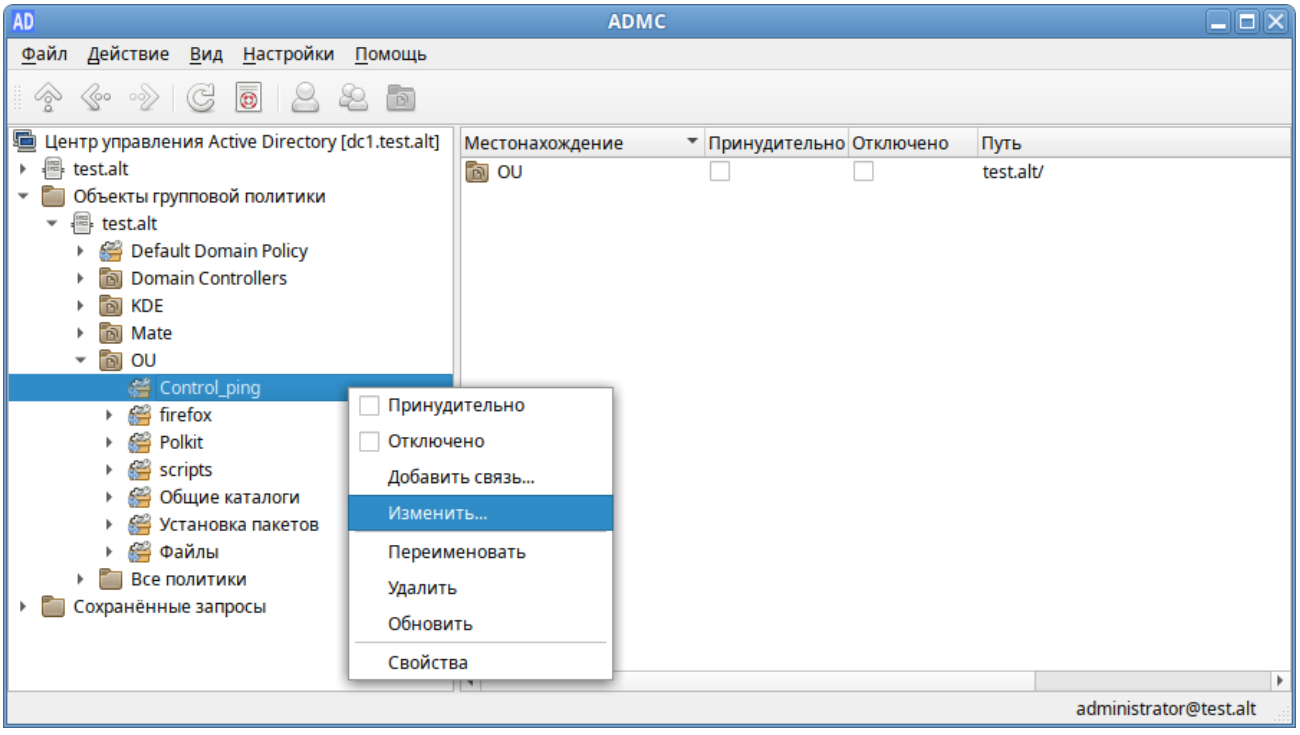


Рис. 123

Модуль редактирования настроек клиентской конфигурации (GPUI)

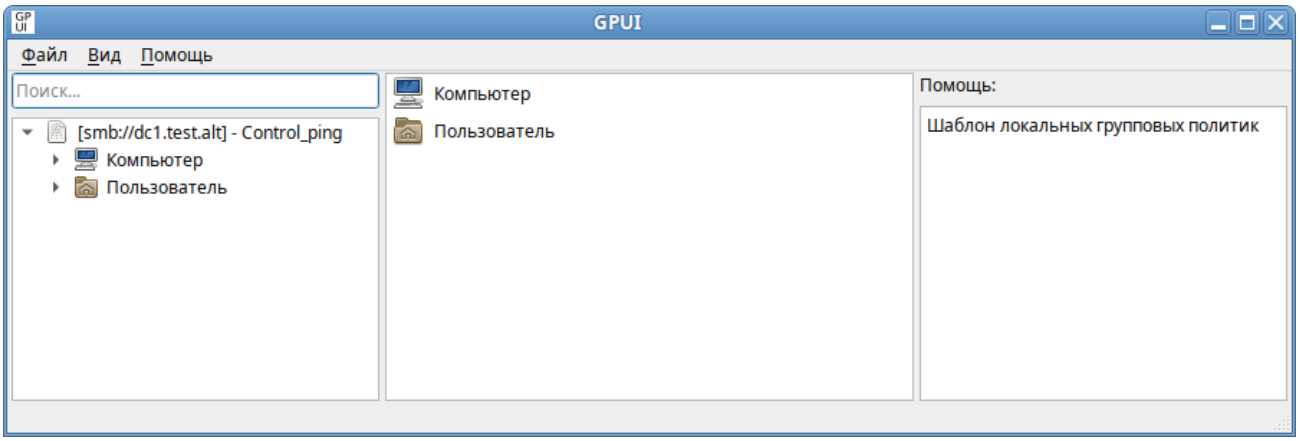


Рис. 124

Модуль редактирования настроек клиентской конфигурации (GPUI)

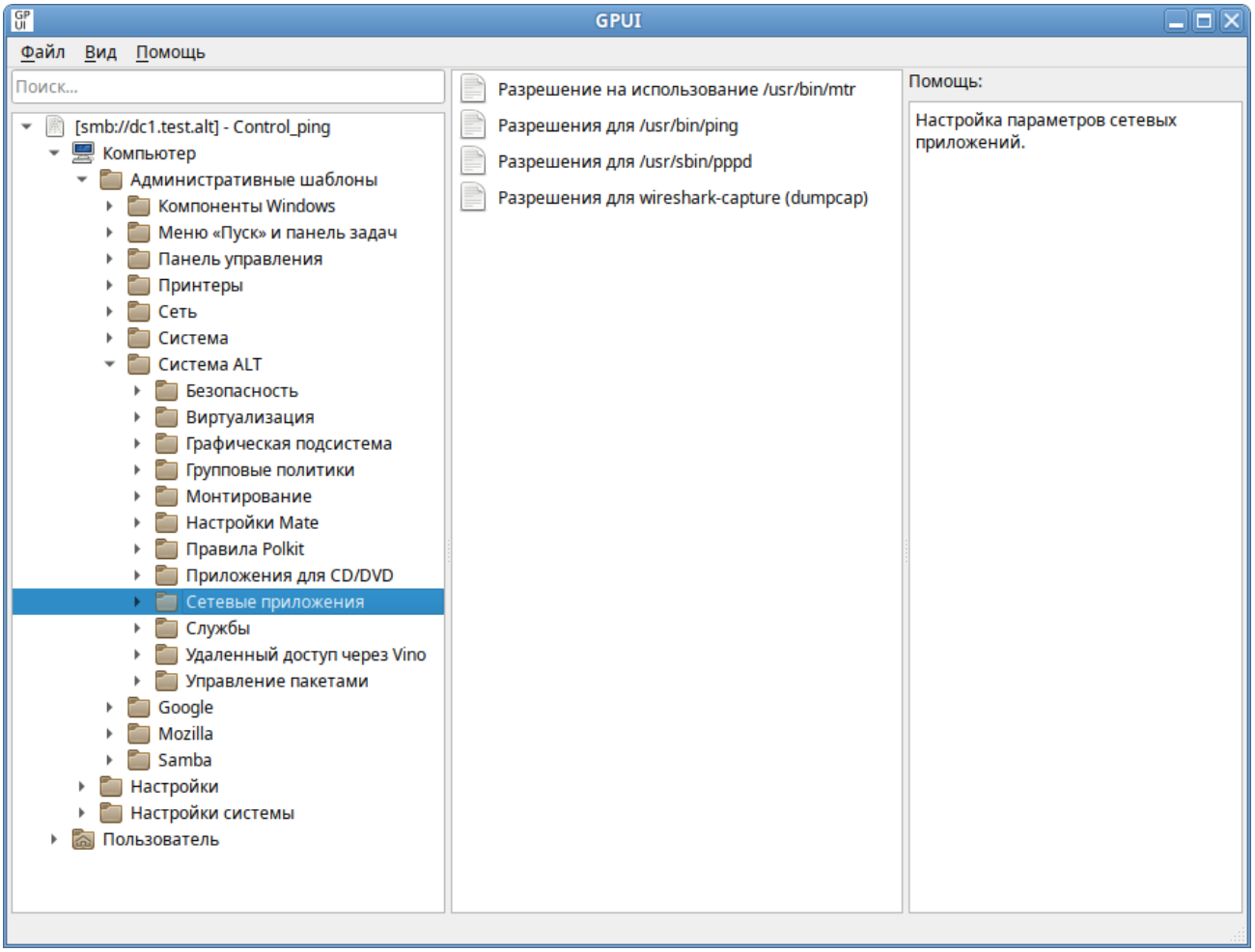


Рис. 125

GPUI. Диалоговое окно настройки политики

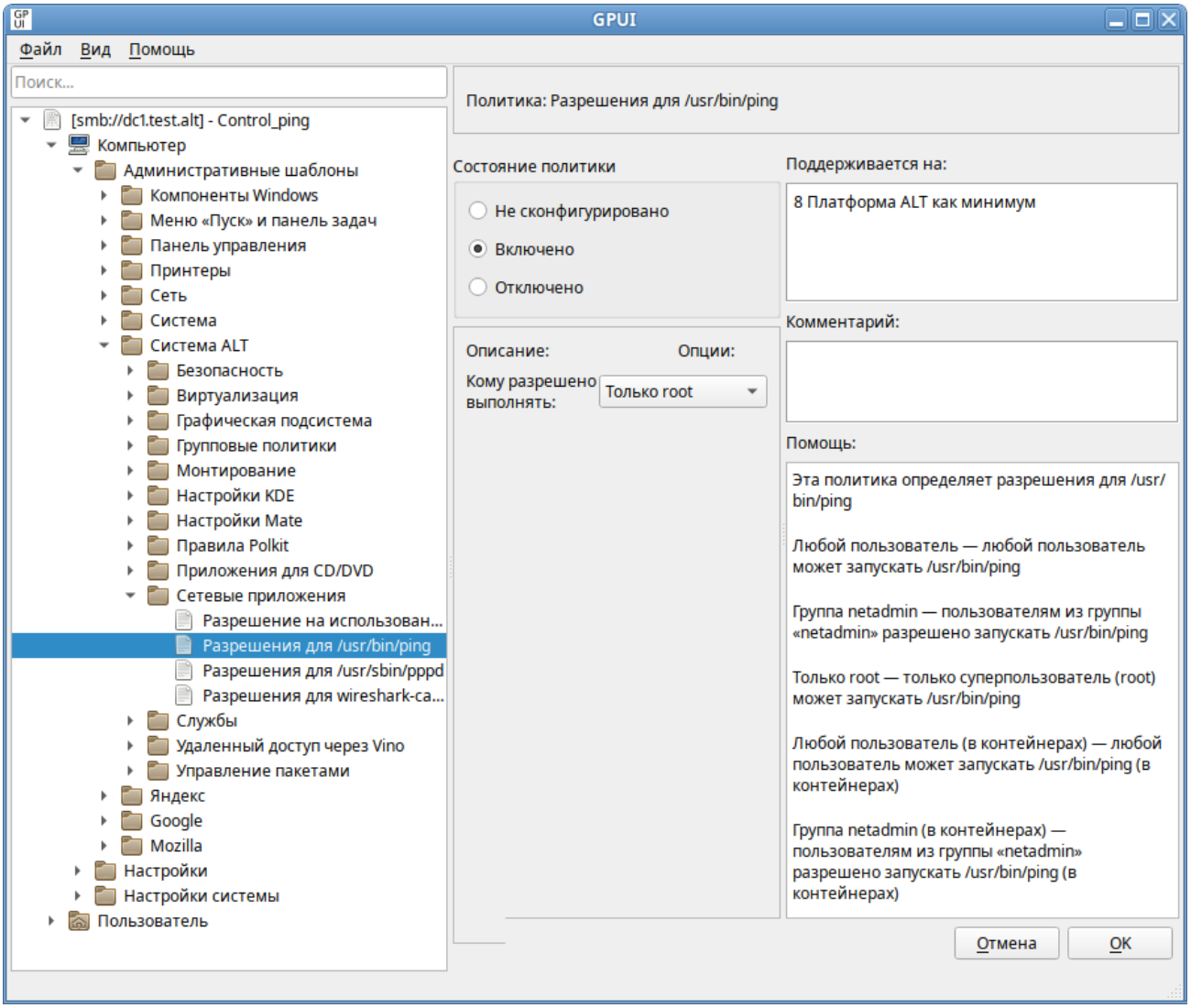


Рис. 126

Пример создания групповой политики на машине с ОС Windows:

- на машине, с установленным RSAT, открыть оснастку «Управление групповыми политиками» (gpmc.msc);
- создать новый объект групповой политики (GPO) и связать его с подразделением (OU), в который входят машины или учетные записи пользователей;
- в контекстном меню GPO, выбрать пункт «Изменить…». Откроется редактор GPO;
- 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. 127);
- дважды щелкнуть левой кнопкой мыши на политике «Разрешения для /usr/bin/ping». Откроется диалоговое окно настройки политики (Рис. 128). Выбрать параметр «Включить»,

в выпадающем списке «Кому разрешено выполнять» выбрать пункт «Только root» и нажать кнопку «Применить».

Раздел «Сетевые приложения»

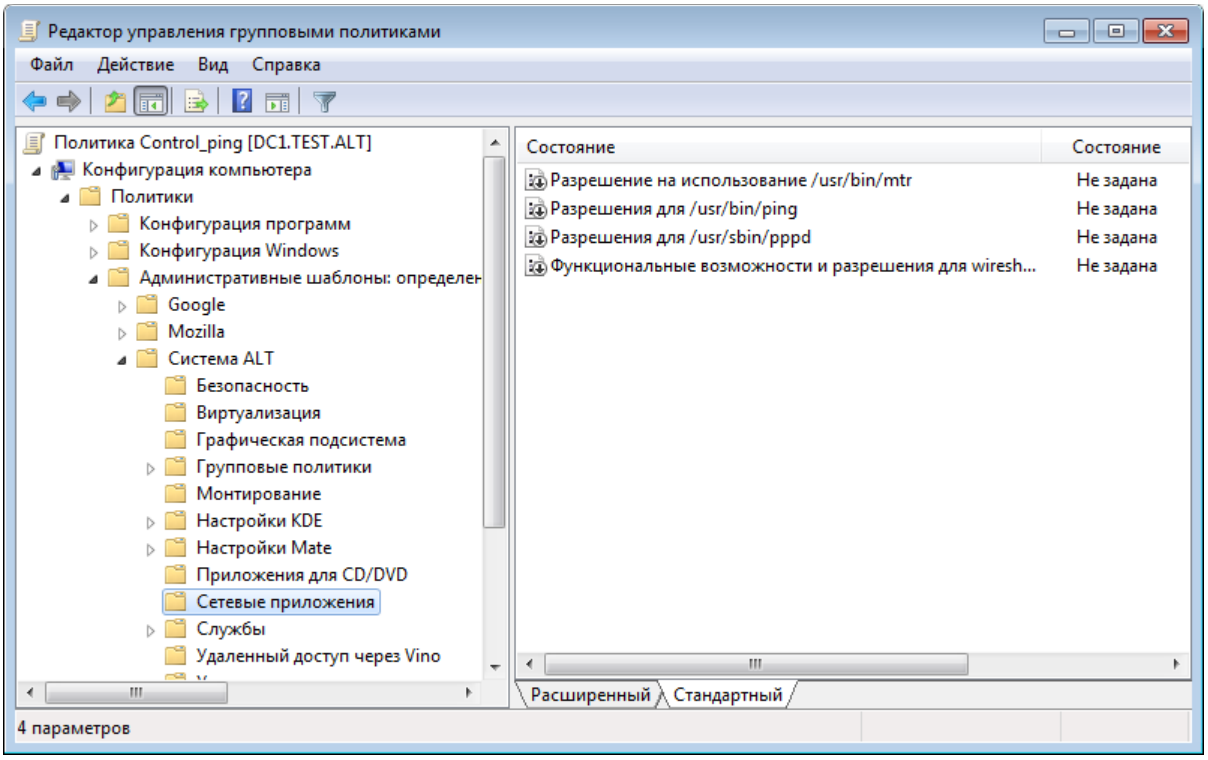


Рис. 127

Политика «Разрешения для /usr/bin/ping»

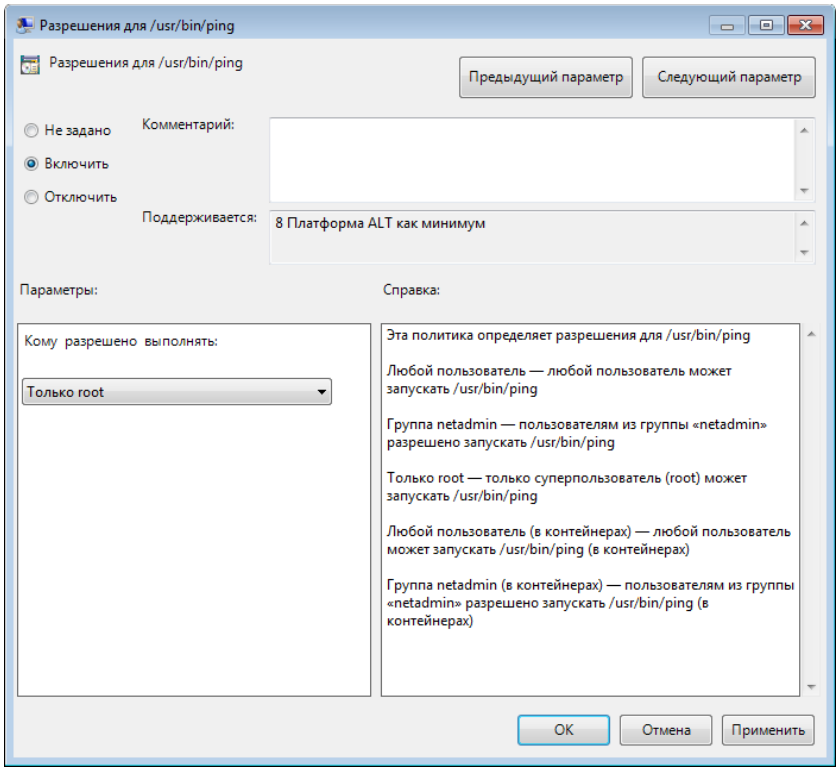


Рис. 128

Примечнние. 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.

5.3 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.

5.3.1 Настройка smb.conf

Примечание. После редактирования файла `/etc/samba/smb.conf`, следует запустить команду `testparm` для проверки файла на синтаксические ошибки:

```
# testparm /etc/samba/smb.conf
```

И, в случае отсутствия ошибок, перезапустить службы smb и nmb, чтобы изменения вступили в силу:

```
# systemctl restart smb
# systemctl restart nmb
```

Каждый раздел в файле конфигурации (кроме раздела [global]) описывает общий ресурс. Название раздела – это имя общего ресурса. Параметры в разделе определяют свойства общего ресурса.

Общий ресурс состоит из каталога, к которому предоставляется доступ, а также описания прав доступа, которые предоставляются пользователю.

Разделы – это либо общие файловые ресурсы, либо службы печати. Разделам может быть назначен гостевой доступ, в этом случае для доступа к ним не требуется пароль (для определения прав доступа используется специальная гостевая учетная запись). Для доступа к разделам, к которым запрещен гостевой доступ, потребуется пароль.

Примечание. Samba использует отдельную от системной базу данных пользователей. Для возможности доступа пользователя к папке (если запрещен гостевой доступ) необходимо внести его в базу данных samba и установить пароль для доступа к общим ресурсам (он может совпадать с основным паролем пользователя). Следует учитывать, что в базу данных samba можно добавлять только тех пользователей, которые уже есть в системе. Добавить пользователя в базу данных Samba можно, выполнив команду (должен быть установлен пакет `samba-common-client`):

```
# smbpasswd -a <имя_пользователя>
```

В файле конфигурации есть три специальных раздела: [global], [homes] и [printers].

Раздел [global]

Параметры в этом разделе применяются к серверу в целом или являются значениями по умолчанию для разделов, и могут быть переопределены в разделе.

Раздел [homes]

Используется для подключения домашних каталогов пользователей. При каждом обращении Samba сначала ищет имя запрошенного ресурса в списке общих ресурсов, и если имя не найдено проверяет наличие в конфигурации секции [homes]. Если такая секция есть, то имя трактуется как имя пользователя, и проверяется по базе данных пользователей сервера Samba. Если имя найдено в базе данных пользователей, то Samba предоставляет в качестве общего ресурса домашний каталог этого пользователя. Аналогичный процесс происходит, если имя запрошенного ресурса – «homes», за исключением того, что имя общего ресурса меняется на имя запрашивающего пользователя.

Раздел [printers]

Если в файле конфигурации имеется раздел [printers], пользователи могут подключаться к любому принтеру, указанному в файле printcap локального хоста.

Примечание. В одноранговой сети (т.е. если Samba используется исключительно как файловый сервер, а не как контроллер домена) для возможности использования файлового ресурса [homes], необходимо добавить каждого локального пользователя в список пользователей Samba, например:

```
# smbpasswd -a user
New SMB password:
Retype new SMB password:
Added user user.
```

Примечание. Если в разделе [homes] указан гостевой доступ (`guest ok = yes`), все домашние каталоги будут видны всем клиентам без пароля. Если это действительно нужно (хотя маловероятно), разумно также указать доступ только для чтения (`read only = yes`).

Примечание. Флаг `browseable` для домашних каталогов будет унаследован от глобального флага `browseable`, а не флага `browseable` раздела [homes]. Таким образом, установка `browseable = no` в разделе [homes] скроет общий ресурс [homes], но сделает видимыми все автоматические домашние каталоги.

Описание некоторых параметров:

- `browseable` – определяет, отображается ли этот общий ресурс в списке доступных общих ресурсов в сетевом окружении и в списке просмотра (по умолчанию: browseable = yes);
- `path` – указывает каталог, к которому должен быть предоставлен доступ;

- `read only` – если для этого параметра задано значение «yes», то пользователи службы не могут создавать или изменять файлы в каталоге (по умолчанию: read only = yes);
- `writable` – инвертированный синоним для `read only` (по умолчанию: writeable = no);
- `write list` – список пользователей, которым будет предоставлен доступ для чтения и записи. Если пользователь находится в этом списке, ему будет предоставлен доступ для записи, независимо от того, какой параметр установлен для параметра `read only`. Список может включать имена групп с использованием синтаксиса @group;
- `read list` – список пользователей, которым будет предоставлен доступ только для чтения. Если пользователь находится в этом списке, ему не будет предоставлен доступ для записи, независимо от того, какой параметр установлен для параметра `read only`. Список может включать имена групп;
- `guest ok` – если этот параметр имеет значение «yes», то для подключения к ресурсу не требуется пароль (по умолчанию: guest ok = no);
- `guest only` – разрешить только гостевые соединения к общему ресурсу (по умолчанию: guest only = no);
- `printable` – если этот параметр имеет значение «yes», то клиенты могут открывать, писать и ставить задания в очередь печати (по умолчанию: printable = no);
- `map to guest` – определяет что делать с запросами, которые не удалось аутентифицировать: «Never» – запросы с неправильными паролями будут отклонены; «Bad user» – запросы с неправильными паролями будут отклонены, если такое имя пользователя существует (по умолчанию: map to guest = Never).

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

```
[global]
    workgroup = WORKGROUP
    server string = Samba Server Version %v
    security = user
    log file = /var/log/samba/log.%m
    max log size = 50
    guest ok = yes
    cups options = raw
    map to guest = Bad User
;   idmap config * : backend = tdb

[homes]
```

```
    comment = Home Directory for '%u'
    browseable = no
    writable = yes
    guest ok = no

[share]
    comment = Common place
    path = /srv/share
    read only = No

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

# Каталог доступный только для чтения, за исключением пользователей
# входящих в группу "staff"
[public]
    comment = Public Stuff
    path = /home/samba
    public = yes
    writable = yes
    write list = +staff
;   browseable = yes

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

Просмотр ресурсов, доступных пользователю user:

```
# smbclient -L 192.168.0.157 -Uuser
Password for [WORKGROUP\user]:

      Sharename       Type      Comment
      ---------       ----      -------
      share           Disk      Commonplace
      public          Disk      Public Stuff
```

```
Free            Disk
IPC$            IPC       IPC Service (Samba Server Version 4.19.9-alt3)
user            Disk      Home Directory for 'user'
```

Обращение к домашней папке пользователя выполняется по имени пользователя (например, smb://192.168.0.157/user).

Примечание. Для ознакомления с прочими возможностями, читайте руководство по `smb.conf`. Для этого используйте команду `man smb.conf`.

5.3.2 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 users,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
```

5.4 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.

Примечание. MAPI over HTTPS не поддерживается.

5.4.1 Установка

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

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

5.4.2 Подготовка среды

5.4.2.1 Настройка PostgreSQL

Подготовить к запуску и настроить службы PostgreSQL:

- создать системные базы данных:

```
# /etc/init.d/postgresql initdb
```

- запустить службу:

```
# systemctl start postgresql
```

Создать пользователя sogo и базу данных sogo (под правами root):

```
# su - postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --no-create-role sogo'
# su - postgres -s /bin/sh -c 'createdb -O sogo sogo'
# systemctl restart postgresql
```

5.4.2.2 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
```

5.4.2.3 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
((uidNumber>=2000) OR (mail='*')))
                AND (NOT isCriticalSystemObject='TRUE') AND (NOT showInAdvanced-
ViewOnly='TRUE') AND (NOT uid=Guest))
                OR (((objectClass=group) AND (gidNumber>=2000)) AND (NOT isCritical-
SystemObject='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 service in samba postgresql memcached sogo httpd2;do systemctl enable
$service;systemctl restart $service;done
```

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

5.4.3 Включение веб-интерфейса

Для включения веб-интерфейса необходимо выполнить команды:

```
# for mod in proxy proxy_http authn_core authn_file auth_basic authz_user env dav
headers rewrite version setenvif; do a2enmod $mod; done
# a2ensite SOGo
# systemctl restart httpd2 sogo
```

Веб-интерфейс SOGo будет доступен по адресу http://адрес_сервера/SOGo/ (Рис. 129).

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:

```
# systemctl restart samba sogo
```

Форма входа в интерфейс SOGo

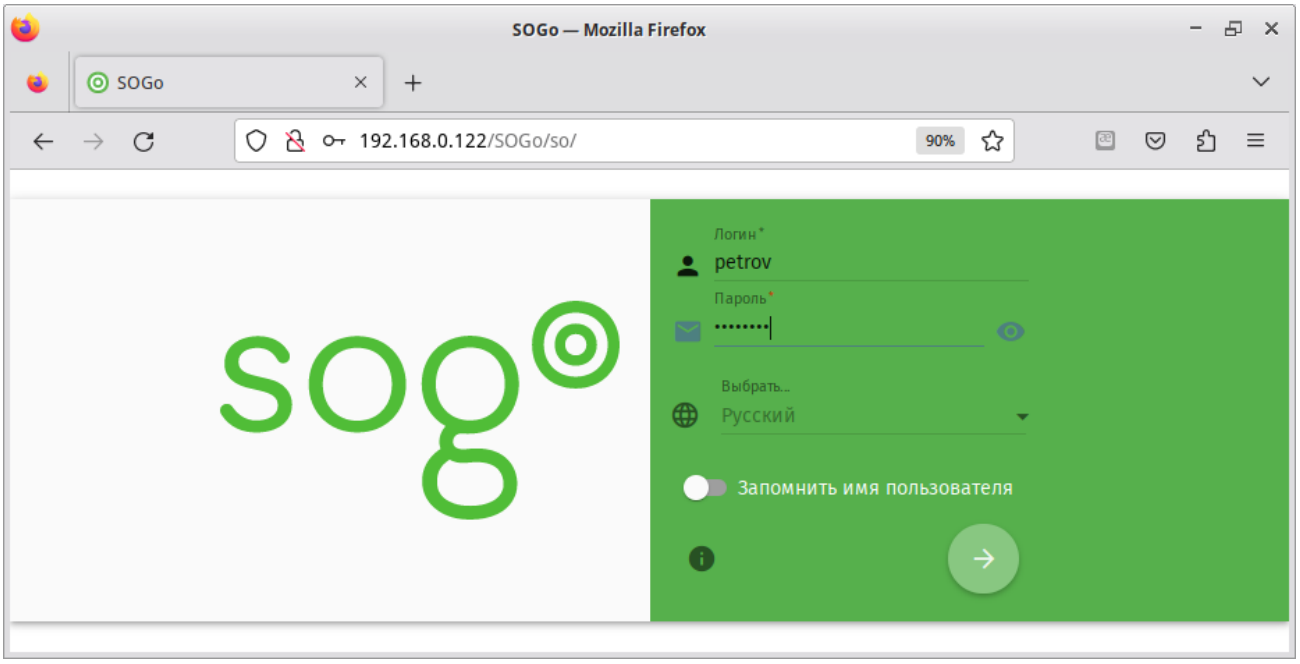


Рис. 129

5.4.4 Настройка электронной почты

Для использования электронной почты в SOGo (Рис. 130) необходимо настроить аутентификацию в Active Directory для Postfix и Dovecot.

Использование электронной почты в SOGo

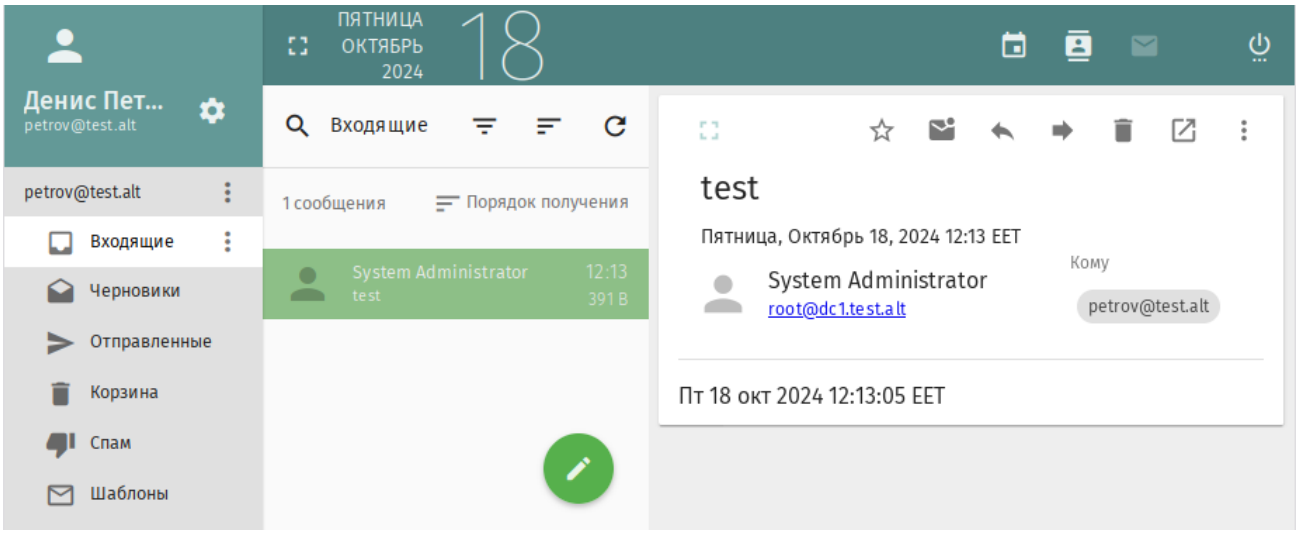


Рис. 130

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. У пользователей SambaDC должен быть указан атрибут `mail`. Указать атрибут `mail` можно, например, при создании учётной записи используя опцию `--mail-address`:

```
# samba-tool user create petrov --mail-address='petrov@test.alt'
```

Примечание. Доступ к серверу LDAP осуществляется по протоколу ldap без шифрования. На контроллере домена SambaDC необходимо отключить ldaps в `/etc/samba/smb.conf` в секции `[global]`:

```
ldap server require strong auth = no
```

и перезапустить samba:

```
# systemctl restart samba
```

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
```

5.4.4.1 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,
permit_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:

```
# systemctl restart postfix
```

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
```

5.4.4.2 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
```

- привести файл `/etc/dovecot/conf.d/10-auth.conf` к виду:

```
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
  }
}
```

- создать файл `/etc/dovecot/conf.d/10-stats.conf`:

```
service stats {
    unix_listener stats-reader {
        user = mail
```

```
        group = mail
        mode = 0660
    }

    unix_listener stats-writer {
        user = mail
        group = mail
        mode = 0660
    }
}
```

- перезапустить службу dovecot:

```
# systemctl restart dovecot
```

Проверка конфигурации Dovecot (в выводе не должно быть никаких сообщений):

```
# doveconf >/dev/null
```

5.4.4.3 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_group-
s.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:

```
# systemctl restart dovecot postfix
```

5.4.4.4 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 dc1.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-PAR-
TIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE
QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE] Logged
in
```

где dc1.test.alt – имя узла сервера SOGo.

5.4.5 Настройка автоответчика, переадресации и фильтрации

В данном разделе рассмотрен процесс конфигурирования Dovecot с плагином Sieve, для возможности фильтрации и переадресации писем.

Настройка Dovecot:

- в файле /etc/dovecot/conf.d/dovecot.conf указать используемые протоколы:

```
protocols = imap lmtp submission sieve
```

- в файл /etc/dovecot/conf.d/10-mail.conf добавить опцию mail_home с указанием пути до каталогов с почтой:

```
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
mail_home = /var/mail/%d/%n
```

Переменные %d и %u указывают на имя домена и имя учетной записи.

- в файле /etc/dovecot/conf.d/15-lda.conf в раздел protocol lda добавить плагин sieve:

```
mail_plugins = $mail_plugins sieve
```

- в файле /etc/dovecot/conf.d/20-lmtp.conf в разделе protocol lmtp также указать плагин sieve:

```
mail_plugins = $mail_plugins sieve
```

- в файле /etc/dovecot/conf.d/20-managesieve.conf раскомментировать строку:

```
protocols = $protocols sieve
```

- в файле /etc/dovecot/conf.d/90-sieve.conf закомментировать строку sieve = file:~/sieve;active=~/.dovecot.sieve и добавить новое её значение:

```
#sieve = file:~/sieve;active=~/.dovecot.sieve
sieve = file:/var/mail/%Ld/%n/sieve;active=/var/mail/%Ld/%n/active.sieve
```

в этом же файле раскомментировать опцию sieve_extensions и привести её к виду:

```
sieve_extensions = +notify +imapflags +vacation-seconds +vacation +date +relational
```

- в файле /etc/dovecot/conf.d/10-auth.conf подключить master-users:

```
!include auth-master.conf.ext
```

- в файле /etc/dovecot/master-users создать запись:

```
my_master_user@non-exist.com:{PLAIN}password::::::
```

Должно быть обязательно указано несуществующее имя домена. В реальных условиях необходимо использовать хеш пароля (например, doveadm pw -s SSHA512).

- в файле /etc/sogo/sieve.creds указать эти данные в виде:

```
my_master_user@non-exist.com:password
```

- в начало файла /etc/cron.d/sogo дописать:

```
MAILTO=""
```

в этом же файле раскомментировать строку:

```
*/5 * * * *    _sogo    /usr/sbin/sogo-tool update-autoreply -p /etc/sogo/sieve.creds
```

В SOGo необходимо активировать окно настроек почтовых фильтров (параметр SOGoSieveScriptsEnabled), окно настроек сообщений об отпуске (параметр

SOGoVacationEnabled), а также окно настроек адресов электронной почты для пересылки (параметр SOGoForwardEnabled). Для этого в файл конфигурации /etc/sogo/sogo.conf добавить строки:

```
SOGoSieveScriptsEnabled = YES;
SOGoVacationEnabled = YES;
SOGoForwardEnabled = YES;
SOGoSieveFolderEncoding = UTF-8;
```

Перезапустить службы:

```
# systemctl restart postfix dovecot sogo
```

В результате в веб-интерфейсе SOGo в настройках почты появятся три дополнительные вкладки (Рис. 131). На вкладке «Фильтры» (Рис. 132) можно создавать фильтры и устанавливать критерии, по которым они должны работать. На вкладке «Отпуск» (Рис. 133) можно настроить автоответ на время отпуска. На вкладке «Пересылка» (Рис. 134) настраивается переадресация электронной почты.

SOGo. Настройки почты

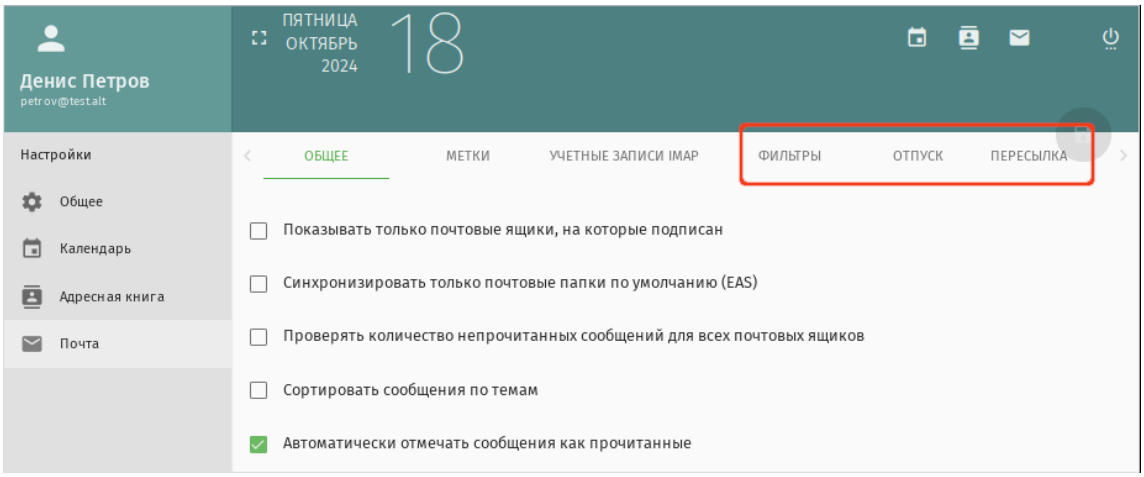


Рис. 131

SOGo. Настройка фильтра

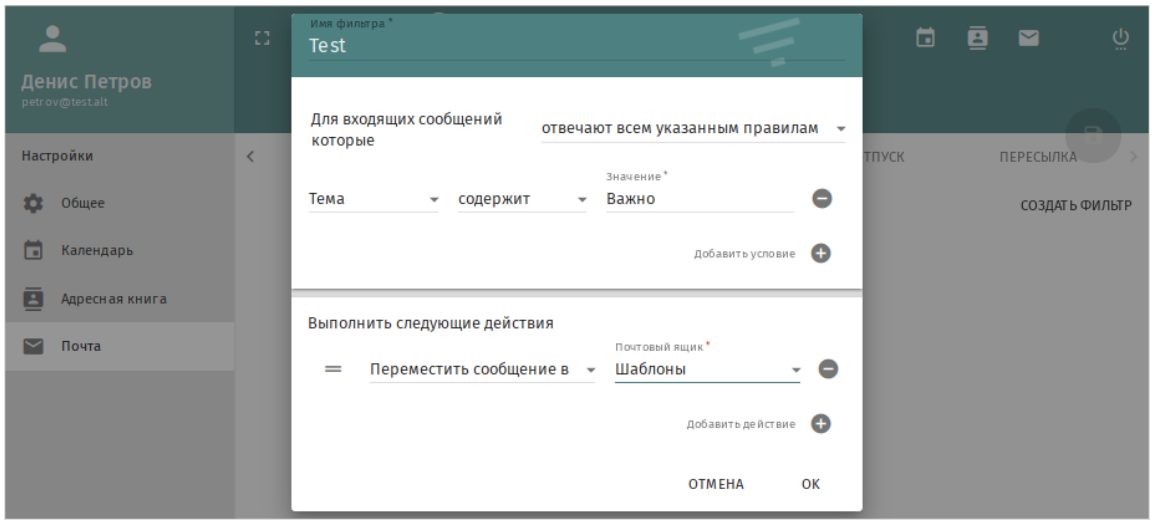


Рис. 132

SOGo. Настройки автоответа на период отпуска

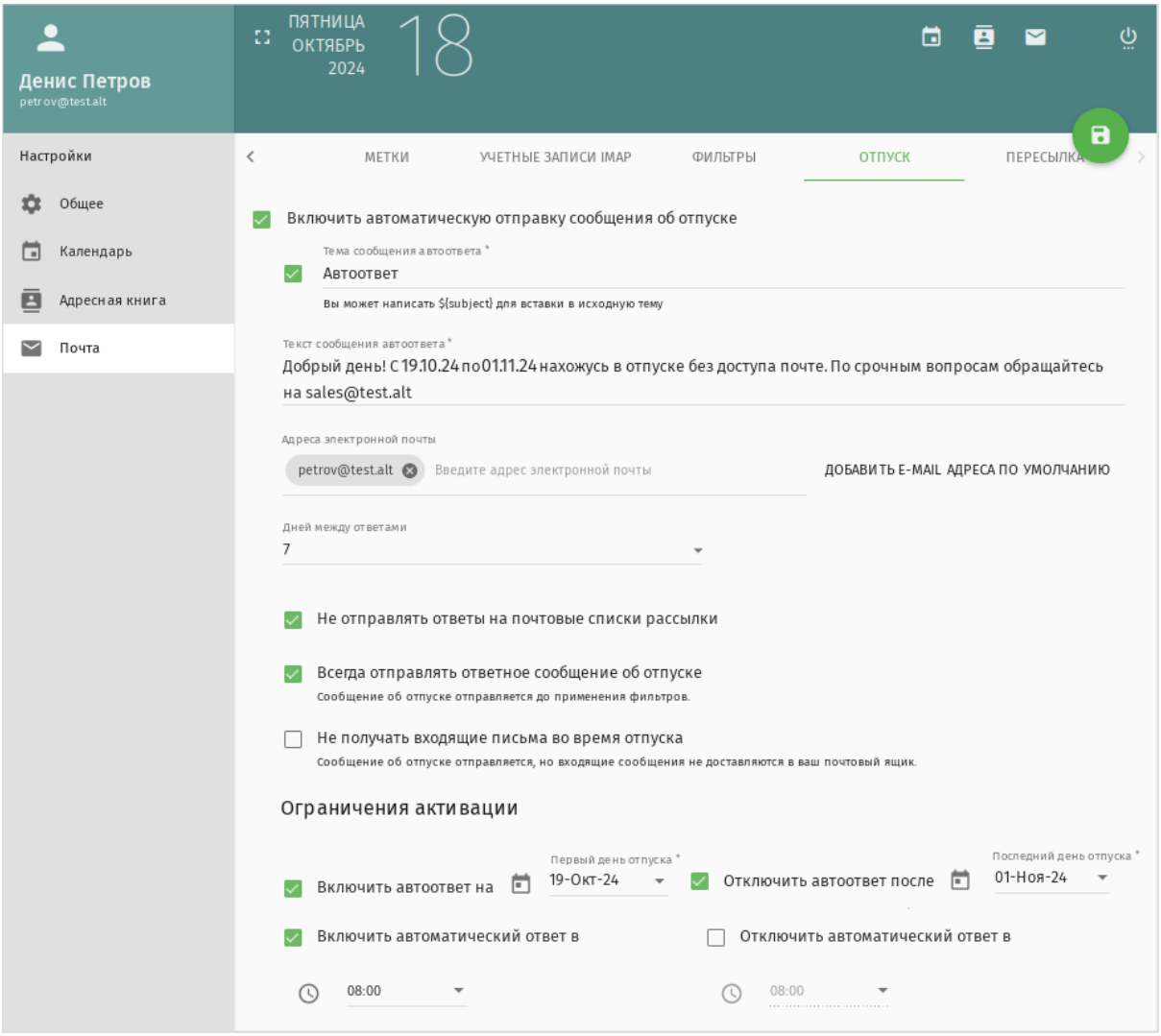


Рис. 133

SOGo. Настройка переадресации электронной почты

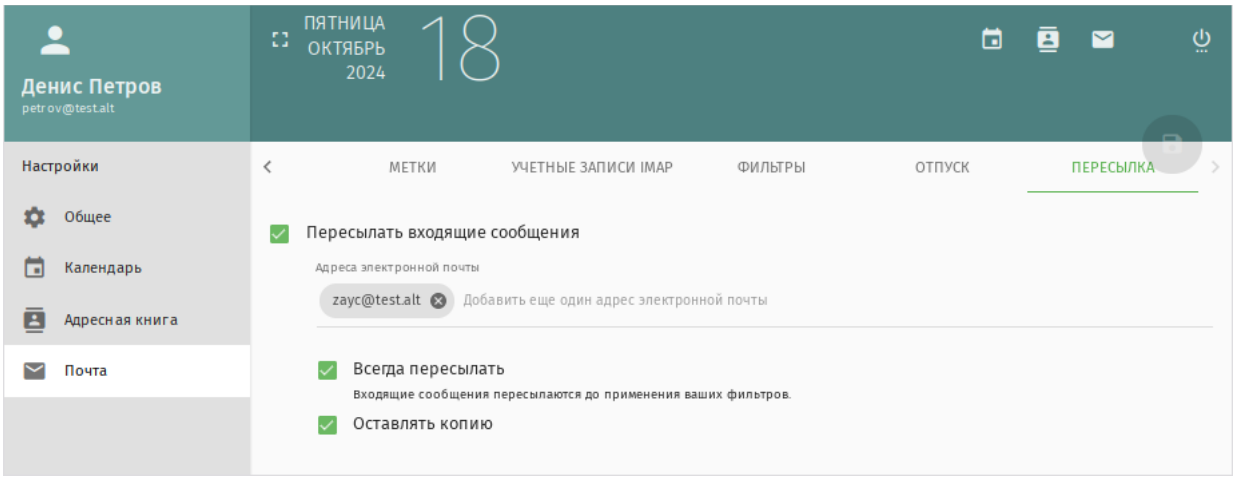


Рис. 134

5.5 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.

5.5.1 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. В примере для установки сервера используется узел: ipa.example.test (192.168.0.113).

Для корректной работы сервера должны соблюдаться следующие условия:

- для сервера должно быть задано полное доменное имя (FQDN);
- IP-адрес сервера не должен изменяться;
- в настройках сетевого интерфейса должен быть указан собственный IP-адрес в качестве первичного DNS.

Сетевые 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» IP-адрес машины и в поле «Домены поиска» – домен для поиска (Рис. 135);
- в консоли:
  - задать имя компьютера:
    ```
    # hostnamectl set-hostname ipa.example.test
    ```
  - указать DNS и домен для поиска в файле `/etc/systemd/network/alterator-enp0s3.network` в разделе `[Network]`:
    ```
    [Match]
         Name = enp0s3
    [Network]
         IPv6AcceptRA = false
         Domains = example.test
         Address = 192.168.0.113/24
         Gateway = 192.168.0.1
         DNS = 192.168.0.113
         DNS = 8.8.8.8
    ```

где enp0s3 – имя интерфейса.

Модуль Ethernet-интерфейсы

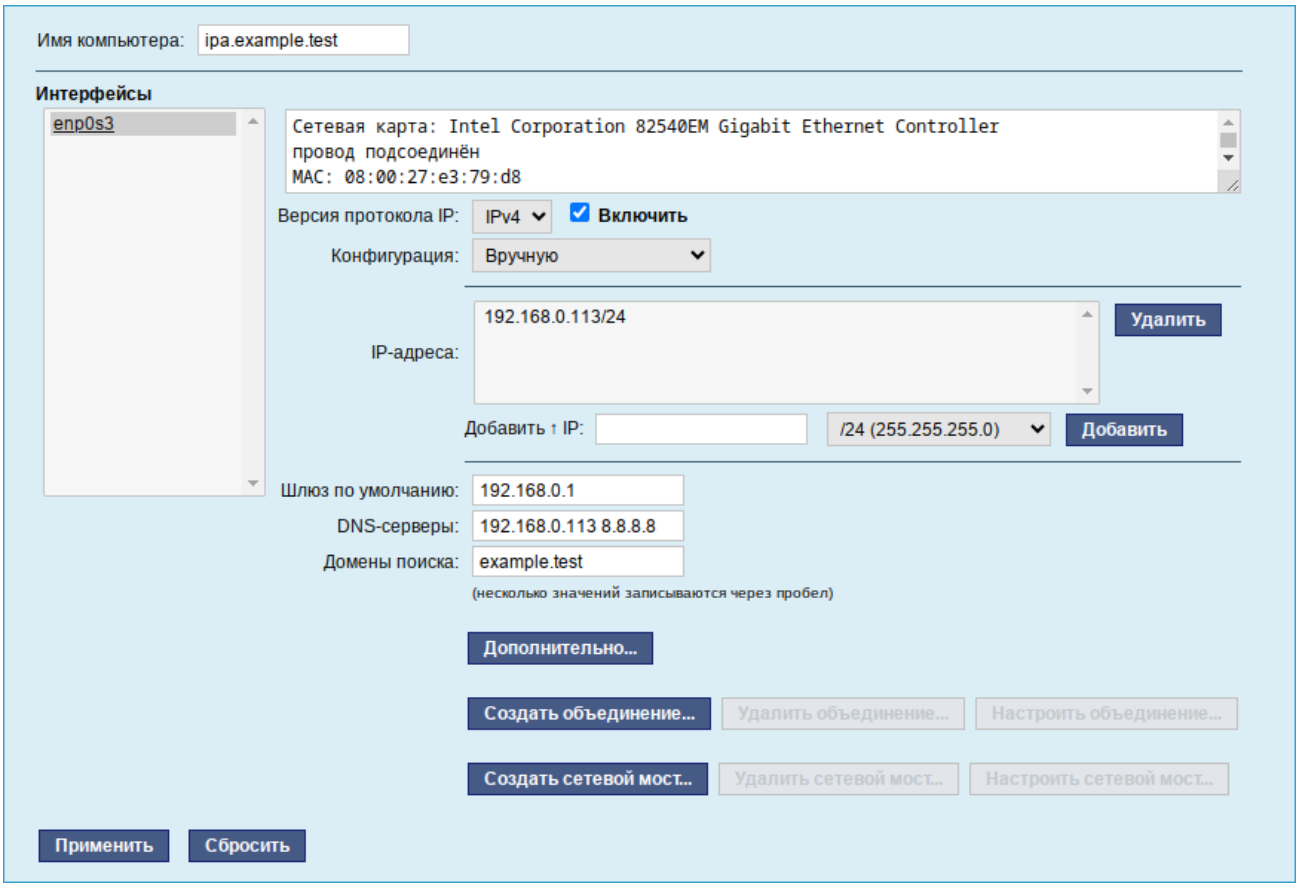


Рис. 135

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

Для того чтобы DNS-сервер FreeIPA управлял зоной example.test, нужно настроить systemd-resolved для использования FreeIPA в качестве основного DNS-сервера. По умолчанию systemd-resolved прослушивает DNS-запросы на локальном сокете. Чтобы избежать конфликтов с FreeIPA DNS, следует отключить DNSStubListener:

- в файле конфигурации systemd-resolved (/etc/systemd/resolved.conf) установить значение:

```
DNSStubListener=no
```

- перезапустить службу systemd-resolved:

```
# systemctl restart systemd-resolved
```

- убедиться в наличии следующих строк в файле `/etc/resolv.conf`:

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

Во избежание конфликтов с разворачиваемым tomcat необходимо отключить ahttpd, работающий на порту 8080, а также отключить HTTPS в Apache2:

```
# systemctl stop ahttpd
# a2dissite 000-default_https
# systemctl condreload httpd2
# a2disport https
```

Установить необходимые пакеты (если во время установки сервера не был выбран пункт сервер FreeIPA):

```
# apt-get install freeipa-server freeipa-server-dns
```

Команда установки сервера FreeIPA в пакетном режиме:

```
# ipa-server-install -U --hostname=$(hostname) \
-r EXAMPLE.TEST -n example.test -p 12345678 -a 12345678 \
--setup-dns --forwarder 8.8.8.8 --auto-reverse
```

Для пакетной установки необходимо указать следующие параметры:

- `-r REALM_NAME` – имя области Kerberos для сервера FreeIPA;
- `-n DOMAIN_NAME` – доменное имя;
- `-p DM_PASSWORD` – пароль, который будет использоваться сервером каталогов для менеджера каталогов (DM);
- `-a ADMIN_PASSWORD` – пароль пользователя admin, администратора FreeIPA;
- `-U` – позволить процессу установки выбрать параметры по умолчанию, не запрашивая у пользователя информацию;
- `--hostname=HOST_NAME` – полное DNS-имя этого сервера.

Чтобы установить сервер со встроенным DNS, должны также быть добавлены следующие параметры:

- `--setup-dns` – создать зону DNS, если она еще не существует, и настроить DNS-сервер;
- `--forwarder` или `--no-forwarders` – в зависимости от того, нужно ли настроить серверы пересылки DNS или нет;
- `--auto-reverse` или `--no-reverse` – в зависимости от того, нужно ли настроить автоматическое обнаружение обратных зон DNS, которые должны быть созданы в FreeIPA DNS, или отключить автоматическое определение обратных зон.

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 example.test -p 12345678 -a 12345678 --setup-dns \
--no-forwarders --no-reverse --mkhomedir
```

Для запуска интерактивной установки следует выполнить команду:

```
# ipa-server-install
```

На первый вопрос, нужно ли сконфигурировать DNS-сервер BIND, следует ответить утвердительно:

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

Остальные вопросы можно выбрать по умолчанию (просто нажать <Enter>). При установке также потребуется ввести пароль администратора системы и пароль администратора каталогов (пароли должны быть не менее 8 символов).

Перед началом конфигуририрования система выведет информацию о конфигурации и попросит ее подтвердить:

```
The IPA Master Server will be configured with:
Hostname:       ipa.example.test
IP address(es): 192.168.0.113
Domain name:    example.test
Realm name:     EXAMPLE.TEST

The CA will be configured with:
Subject DN:   CN=Certificate Authority,O=EXAMPLE.TEST
Subject base: O=EXAMPLE.TEST
Chaining:     self-signed

BIND DNS server will be configured to serve IPA domain with:
Forwarders:       8.8.8.8
Forward policy:   only
Reverse zone(s):  0.168.192.in-addr.arpa.

Continue to configure the system with these values? [no]: yes
```

После подтверждения начнется процесс конфигурации. После его завершения будет выведена подсказка со следующими шагами.

Веб-интерфейс будет доступен по адресу `https://ipa.example.test`

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
```

Проверить наличие прямой и обратной зон можно, выполнив команды:

```
# ipa dnszone-show example.test
  Имя зоны: example.test.
  Активная зона: True
  Полномочный сервер имён: ipa.example.test.
…

# ipa dnszone-show 0.168.192.in-addr.arpa.
  Имя зоны: 0.168.192.in-addr.arpa.
  Активная зона: True
  Полномочный сервер имён: ipa.example.test.
…
```

Примечание. В случае сбоя установки сервера FreeIPA некоторые файлы конфигурации могут быть уже сконфигурированы. В этом случае дополнительные попытки установить сервер FreeIPA завершатся неудачно. Чтобы решить эту проблему, перед повторной попыткой запуска процесса установки, следует удалить частичную конфигурацию сервера FreeIPA:

```
# ipa-server-install --uninstall
```

Если ошибки при установке сервера FreeIPA остаются, следует переустановить ОС. Одним из требований для установки сервера FreeIPA является чистая система без каких-либо настроек.

5.5.2 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. 136) и ввести данные администратора для входа в систему.

Веб-интерфейс FreeIPA

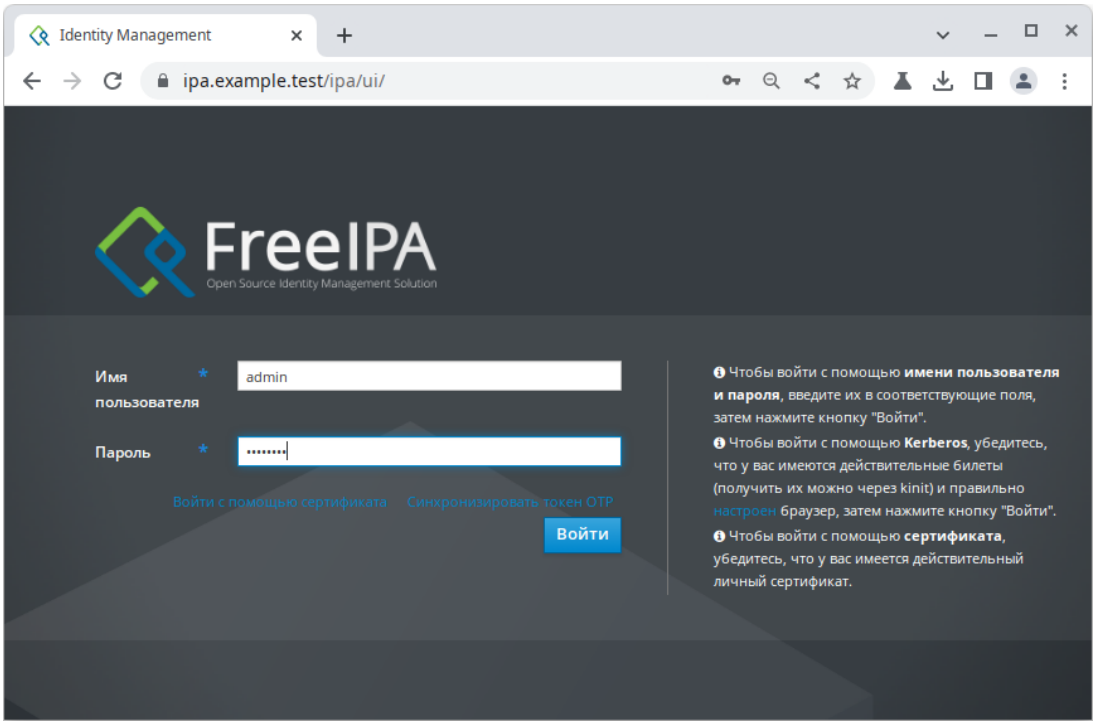


Рис. 136

Создать нового пользователя домена, для этого в окне на странице «Идентификация» → «Пользователи» → «Активные пользователи» необходимо нажать кнопку «Добавить» (Рис. 137).

Пользователи домена

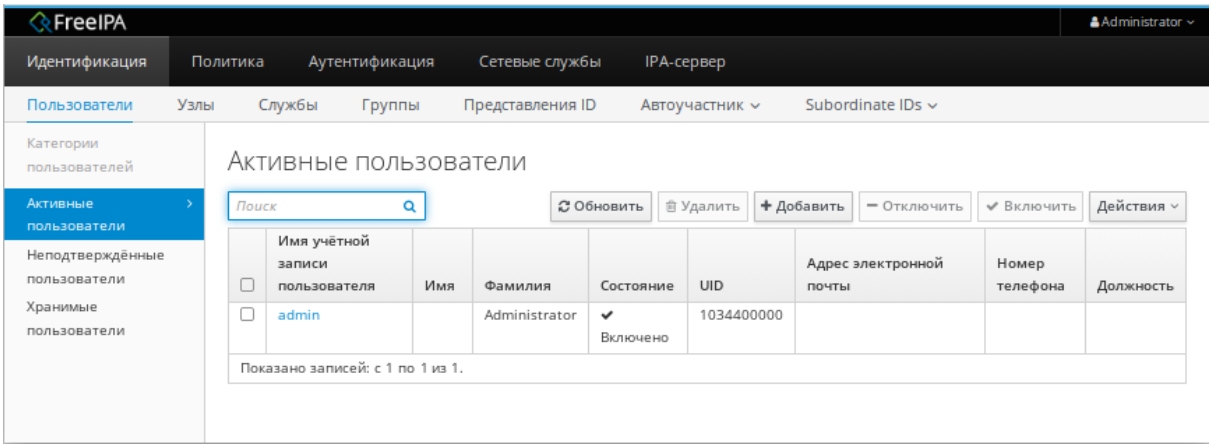


Рис. 137

В открывшемся окне (Рис. 138) необходимо ввести данные пользователя и нажать кнопку «Добавить». Созданный пользователь появится в списке пользователей (Рис. 139).

Окно добавления нового пользователя домена

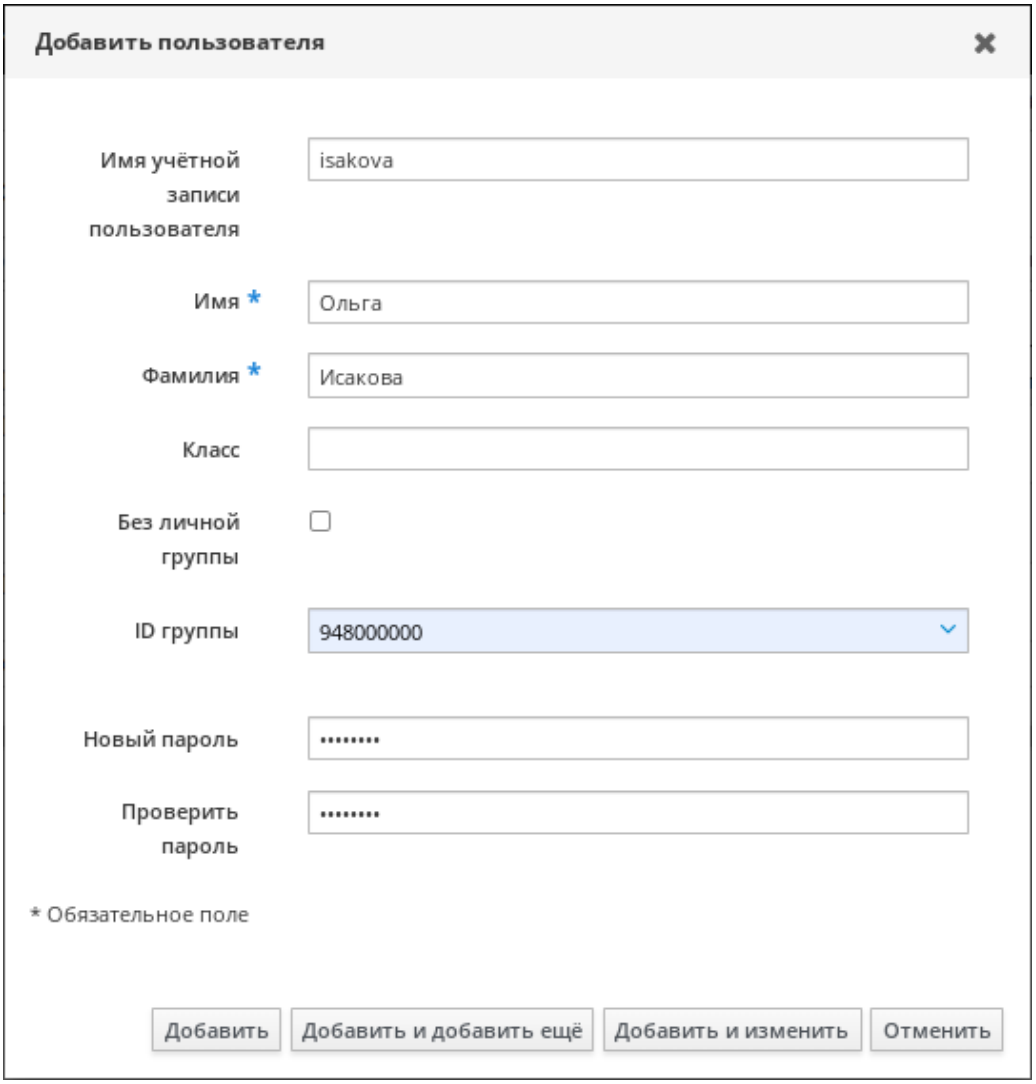


Рис. 138

Список пользователей домена

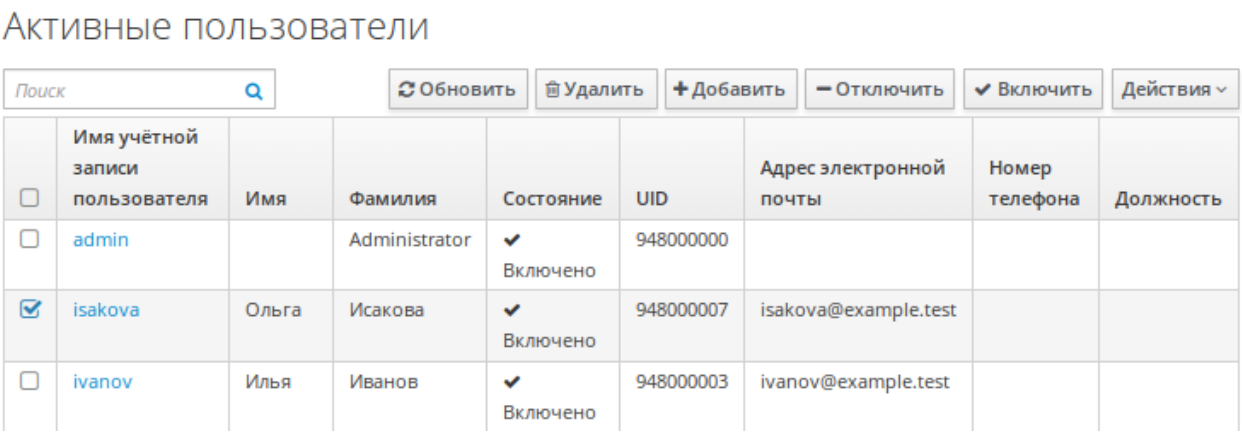


Рис. 139

5.5.3 Ввод рабочей станции в домен FreeIPA

5.5.3.1 Установка FreeIPA клиента

Установить необходимые пакеты:

```
# apt-get install freeipa-client libsss_sudo krb5-kinit bind-utils libbind zip task-auth-freeipa
```

Клиентские компьютеры должны быть настроены на использование DNS-сервера, который был сконфигурирован на сервере FreeIPA во время его установки. При получении IP-адреса по DHCP данные о сервере DNS также должны быть получены от сервера DHCP. Ниже приведен пример настройки сетевого интерфейса со статическим IP-адресом.

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. 140);
- в консоли:
  - задать имя компьютера:
    ```
    # hostnamectl set-hostname comp01.example.test
    ```
  - 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

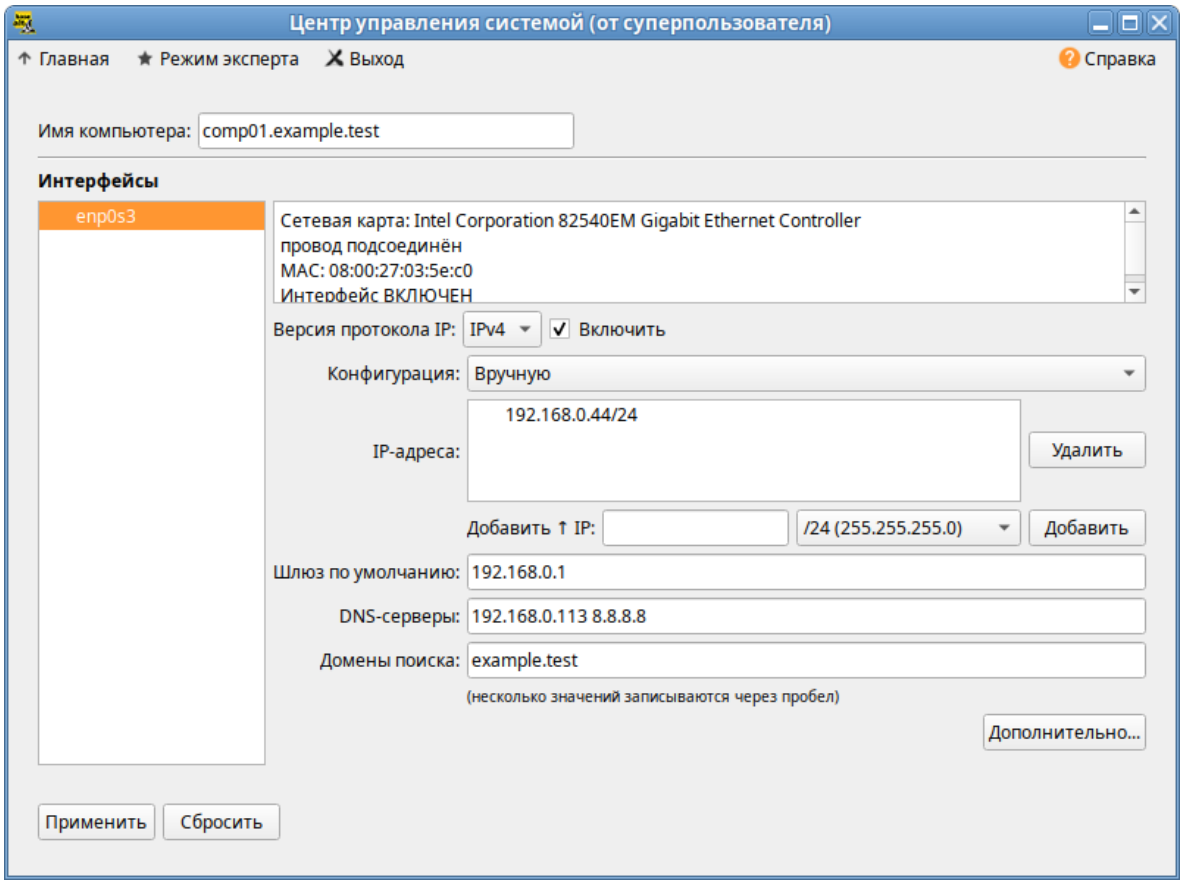


Рис. 140

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.

5.5.3.2 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. 141) и заполнить поля, после чего нажать кнопку «Применить».

Ввод в домен в «Центре управления системой»

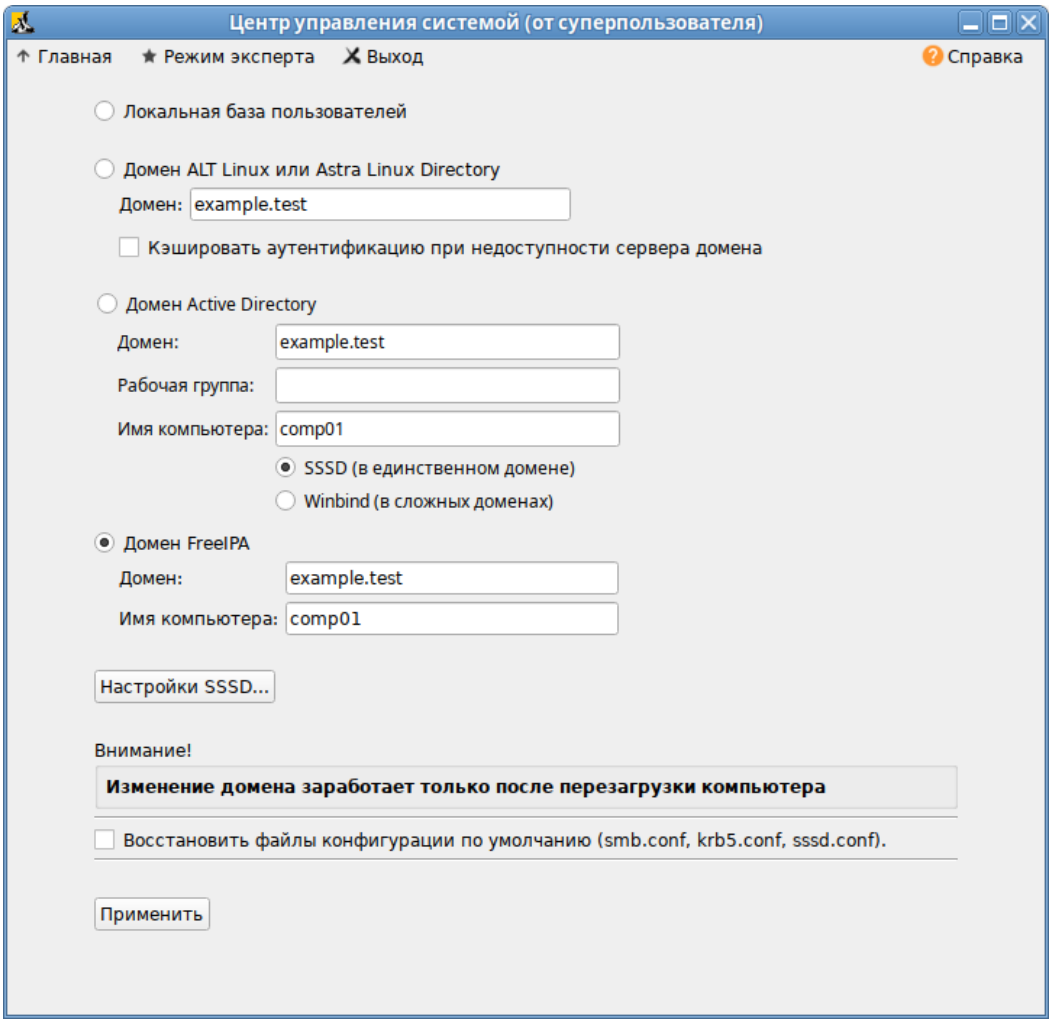


Рис. 141

В открывшемся окне (Рис. 142) 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

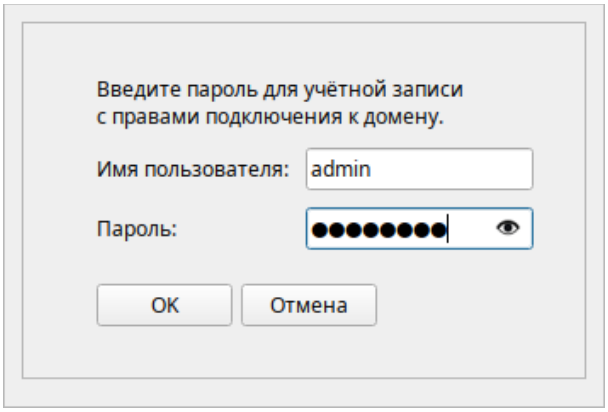


Рис. 142

При успешном подключении к домену, отобразится соответствующая информация (Рис. 143).

Успешное подключение к домену

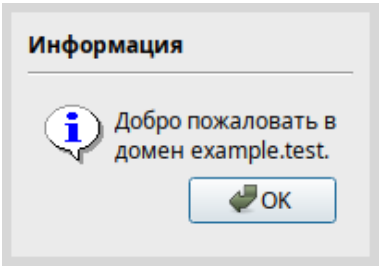


Рис. 143

Перезагрузить рабочую станцию.

5.5.3.3 Подключение к серверу в консоли

Запустить скрипт настройки клиента: в пакетном режиме:

```
# ipa-client-install -U -p admin -w 12345678
```

или интерактивно:

```
# ipa-client-install
```

Если все настроено верно, скрипт должен выдать такое сообщение:

```
'''Discovery was successful!'''
Client hostname: 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.

Примечание. Если при входе в домен возникает такая ошибка:

```
Hostname (comp02.example.test) does not have A/AAAA record.
Failed to update DNS records.
```

Необходимо проверить IP-адрес доменного DNS сервера в файле `/etc/resolv.conf`.

В случае возникновения ошибки, необходимо перед повторной установкой запустить процедуру удаления:

```
# ipa-client-install -U --uninstall
```

Для работы sudo-политик для доменных пользователей на клиентской машине необходимо разрешить доступ к sudo:

```
# control sudo public
```

5.5.3.4 Вход пользователя

В окне входа в систему (Рис. 144) 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. 145) и его подтверждение.

Вход пользователя

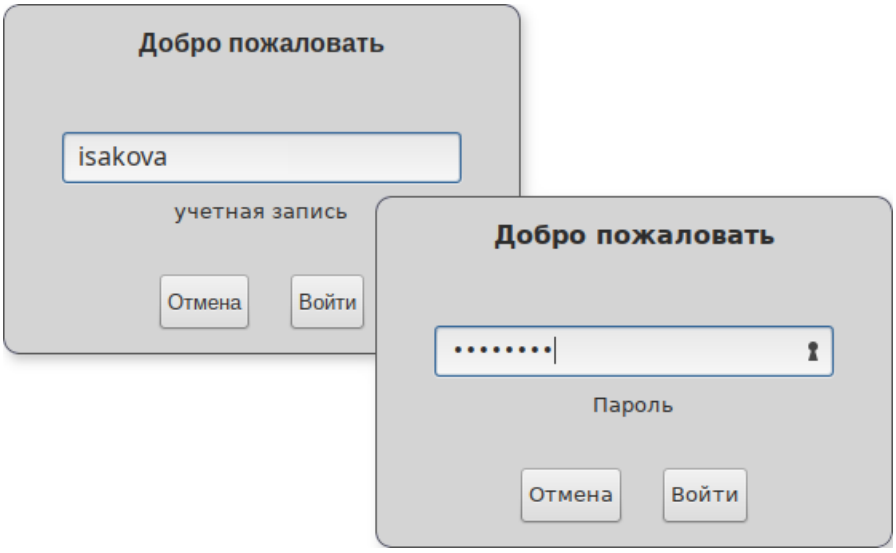


Рис. 144

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

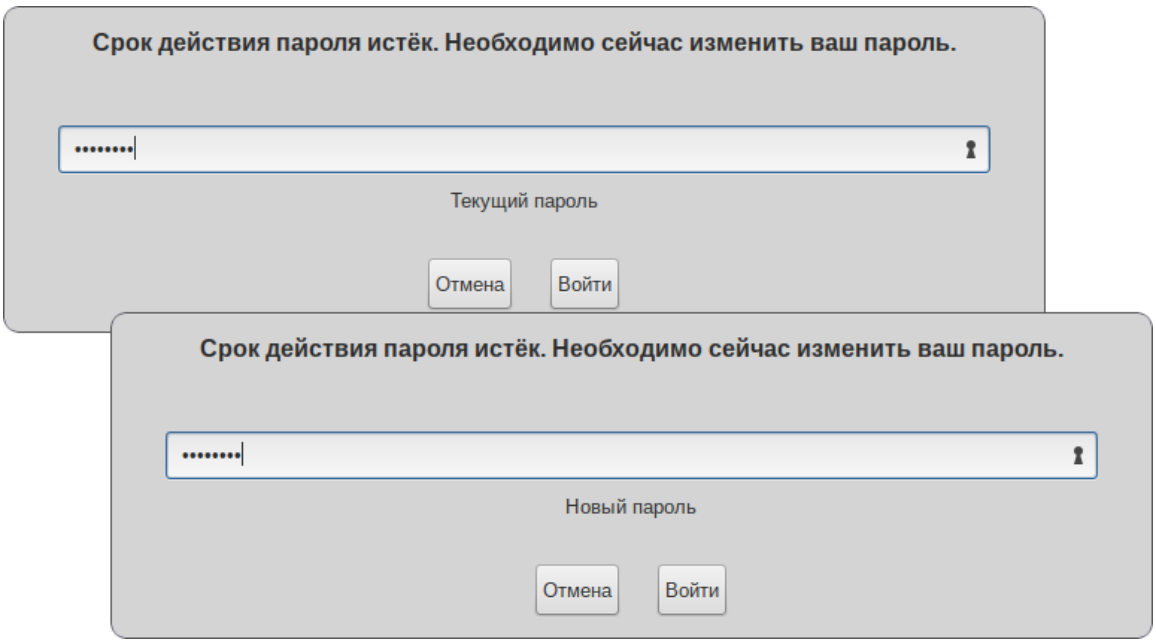


Рис. 145

Предупреждение. Если машина до этого была в других доменах или есть проблемы со входом пользователей рекомендуется очистить кэш sssd:

```
# systemctl stop sssd
# rm -f /var/lib/sss/db/*
# rm -f /var/lib/sss/mc/*
# systemctl start sssd
```

5.5.4 Удаление клиента FreeIPA

При удалении, клиент удаляется из домена FreeIPA вместе с конфигурацией системных служб FreeIPA.

Для удаления клиента FreeIPA необходимо:

- на клиенте ввести команду:

```
# ipa-client-install --uninstall
…
Client uninstall complete.
The original nsswitch.conf configuration has been restored.
You may need to restart services or reboot the machine.
Do you want to reboot the machine? [no]: yes
The ipa-client-install command was successful
```

- на клиенте удалить, если они есть, старые принципалы Kerberos (кроме `/etc/krb5.keytab`):

```
# ipa-rmkeytab -k /path/to/keytab -r EXAMPLE.TEST
```

- на сервере FreeIPA удалить все записи DNS для клиентского узла:

```
# ipa dnsrecord-del
Имя записи: comp01
Имя зоны: example.test
Возможность удаления определённой записи не предусмотрена.
Удалить все? Yes/No (default No): yes
-----------------------
Удалена запись "comp01"
-----------------------
```

- на сервере FreeIPA удалить запись узла с сервера LDAP FreeIPA (при этом будут удалены все службы и отозваны все сертификаты, выданные для этого узла):

```
# ipa host-del comp01.example.test
--------------------------------
Удалён узел "comp01.example.test"
--------------------------------
```

5.5.5 Настройка репликации

Для установки реплики используется утилита `ipa-replica-install`. Реплики необходимо устанавливать по одной. Установка нескольких реплик одновременно не поддерживается.

Новую реплику можно установить:

- на существующем клиенте FreeIPA путем преобразования клиента в реплику;
- на машине, которая еще не зарегистрирована в домене FreeIPA.

В обеих этих ситуациях можно настроить реплику, добавив нужные параметры в команду `ipa-replica-install`.

Перед разворачиванием реплики необходимо убедиться, что при настройке DNS в процессе инициализации FreeIPA была создана обратная зона DNS («Сетевые службы»→«DNS»→«Зоны DNS») и в обратной зоне создана реверсивная запись для основного сервера 192.168.0.113.

Примечание. Если реплика находится в другой IP-сети, необходимо вручную добавить запись для обратной зоны реплики на сервере FreeIPA.

В примере для настройки репликации используется узел replica.example.test (192.168.0.145).

Перед настройкой репликации необходимо настроить систему на использование DNS-сервера, который был сконфигурирован на сервере FreeIPA во время его установки:

- в ЦУС в разделе «Сеть» → «Ethernet интерфейсы» задать имя компьютера, указать в поле «DNS-серверы» IP-адрес сервера FreeIPA и в поле «Домены поиска» – домен для поиска (Рис. 146);
- в консоли:
  - задать имя компьютера:
    ```
    # hostnamectl set-hostname replica.example.test
    ```
  - указать DNS и домен для поиска в файле `/etc/systemd/network/alterator-enp0s3.network` в разделе `[Network]`:
    ```
    [Match]
         Name = enp0s3
    [Network]
         IPv6AcceptRA = false
         Domains = example.test
         Address = 192.168.0.145/24
         Gateway = 192.168.0.1
         DNS = 192.168.0.113
         DNS = 8.8.8.8
    ```
    где enp0s3 – имя интерфейса.

Настройка узла replica.example.test

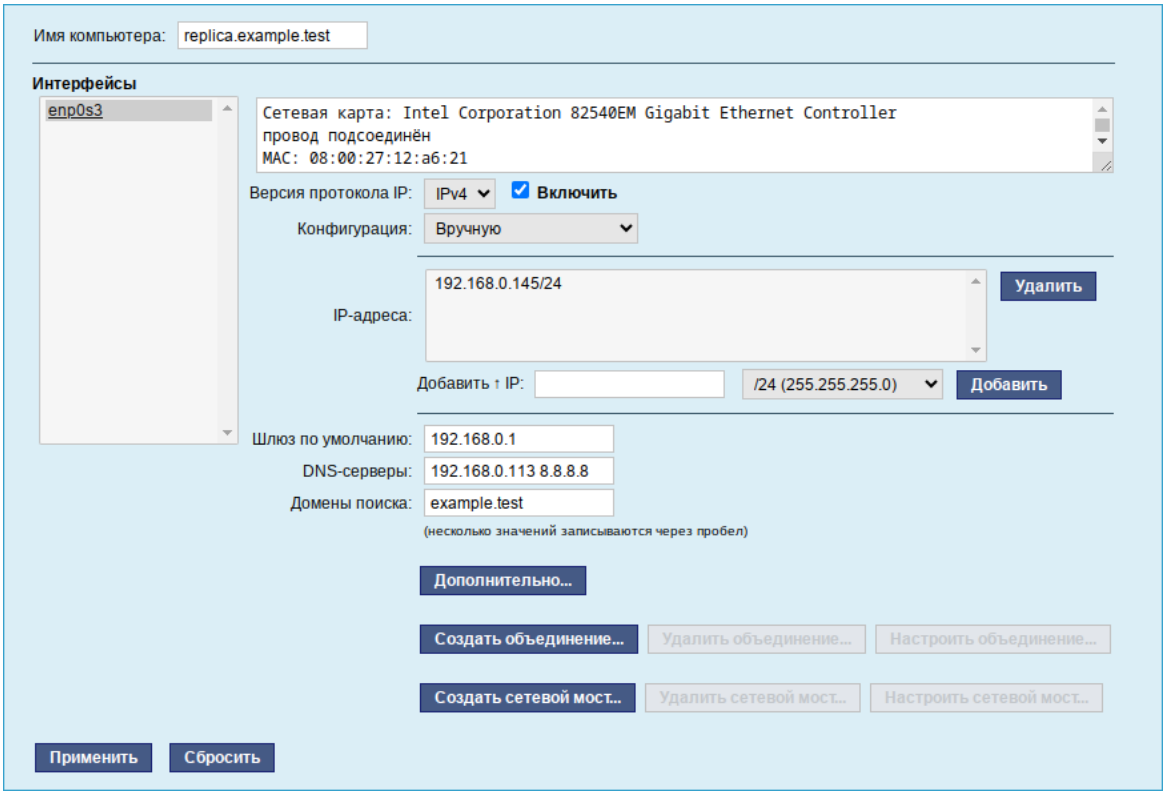


Рис. 146

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

Чтобы избежать конфликтов systemd-resolved с FreeIPA DNS, следует отключить DNSStubListener:

- в файле конфигурации systemd-resolved (/etc/systemd/resolved.conf) установить значение:

```
DNSStubListener=no
```

- перезапустить службу systemd-resolved:

```
# systemctl restart systemd-resolved
```

- убедиться в наличии следующих строк в файле `/etc/resolv.conf`:

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

При установке реплики в системе, которая еще не зарегистрирована в домене FreeIPA, утилита `ipa-replica-install` сначала регистрирует систему в качестве клиента, а затем устанавливает компоненты реплики. В примере, описанном ниже, для авторизации регистрации используется случайный пароль, действительный только для одной регистрации этого клиента.

Установка реплики с использованием случайного пароля:

- на сервере FreeIPA получить билет Kerberos:

```
$ kinit admin
```

- на сервере FreeIPA добавить внешнюю систему в качестве узла FreeIPA:

```
$ ipa host-add replica.example.test --random --ip-address=192.168.0.145
---------------------------------
Добавлен узел "replica.example.test"
---------------------------------
  Имя узла: replica.example.test
  Случайный пароль: 2AaT0Ix8itDsYugdDGoRtBt
  Пароль: True
  Таблица ключей: False
  Managed by: replica.example.test
```

- на сервере FreeIPA добавить систему replica.example.test в группу узлов ipaservers:

```
$ ipa hostgroup-add-member ipaservers --hosts replica.example.test
  Группа узлов: ipaservers
  Описание: IPA server hosts
  Узлы-участники: ipa.example.test, replica.example.test
---------------------------------
Количество добавленных участников 1
---------------------------------
```

- на машине, где будет установлена реплика, установить необходимые пакеты:

```
# apt-get install freeipa-server freeipa-server-dns
```

- на машине, где будет установлена реплика, запустить утилиту `ipa-replica-install`, указав сгенерированный пароль в параметре `--password` (т.к. пароль часто содержит специальные символы, следует заключить его в одинарные кавычки):

```
# ipa-replica-install --password='2AaT0Ix8itDsYugdDGoRtBt' \
--setup-ca --setup-dns --forwarder 192.168.0.113 --forwarder 8.8.8.8

Configuring client side components
This program will set up IPA client.
Version 4.9.14

Discovery was successful!
Client hostname: replica.example.test
Realm: EXAMPLE.TEST
DNS Domain: example.test
IPA Server: ipa.example.test
BaseDN: dc=example,dc=test
…
The ipa-client-install command was successful
```

…

```
The ipa-replica-install command was successful
```

Примечание. dbus может мешать проверке соединений при установке реплики, при появлении ошибок может помочь перезапуск сервиса:

```
# systemctl reload dbus
```

После создания реплики можно проверить, реплицирует ли реплика данные должным образом:

- создать пользователя на новой реплике:

```
$ kinit admin
$ ipa user-add test_user
```

- убедиться, что пользователь виден на другой реплике:

```
$ kinit admin
$ ipa user-show test_user
```

После настройки и репликации контроллеров посмотреть топологию можно в веб-интерфейсе FreeIPA (Рис. 147) («IPA-сервер» → «Топология» → «Topology Graph»).

Топология FreeIPA

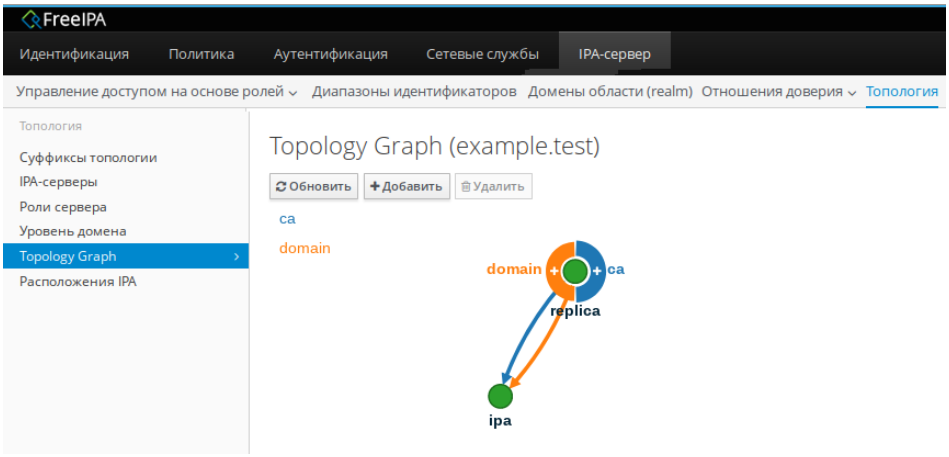


Рис. 147

5.6 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.

5.6.1 Установка и настройка Fleet Commander

5.6.1.1 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-kvm 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 /etc/libvirt/qemu/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 alt \
--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-10.0-x86_64.iso --os-variant=alt10.0
```

- подключиться к ВМ и произвести установку ОС (на хосте, с которого происходит подключение, должен быть установлен пакет `virt-viewer`):

```
$ 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, которая будет использоваться как шаблон, должна быть выключена, иначе Fleet Commander не позволит запустить live-сессию на этой машине.

5.6.1.2 Установка и настройка Fleet Commander Admin

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

Установить пакет `freeipa-desktop-profile`:

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

Примечание. Пакет `freeipa-desktop-profile` не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p10. О добавлении репозиториев можно почитать в разделе «Добавление репозиториев».

Проверить, что плагин работает:

```
# kinit admin
Password for admin@EXAMPLE.TEST:
# ipa deskprofileconfig-show
  Priority of profile application: 1
```

Примечание. Если на выходе команды `ipa deskprofileconfig-show` появляется ошибка:

```
ipa: ERROR: неизвестная команда "deskprofileconfig-show"
```

необходимо почистить кэш текущему пользователю и повторить команду:

```
# rm -rf ~/.cache/ipa
# ipa deskprofileconfig-show
  Priority of profile application: 1
```

Установить Fleet Commander плагин для Cockpit:

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

Примечание. Пакет `fleet-commander-admin` не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p10. О добавлении репозиториев можно почитать в разделе «Добавление репозиториев».

Добавить сервис Cockpit в автозапуск и запустить его:

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

Веб-интерфейс Cockpit будет доступен по адресу https://адрес-сервера:9090/ (Рис. 148).

Веб-интерфейс Cockpit

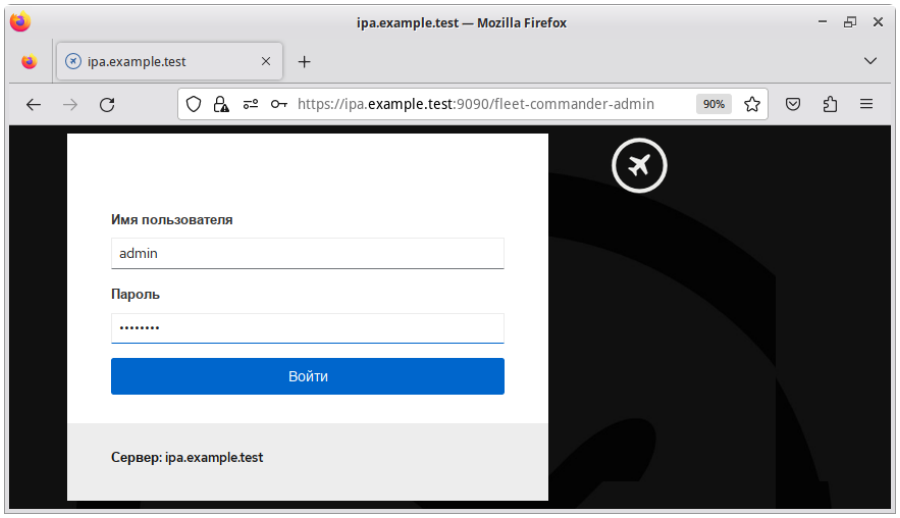


Рис. 148

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. 149).

Веб-интерфейс Cockpit. Вкладка Fleet Commander

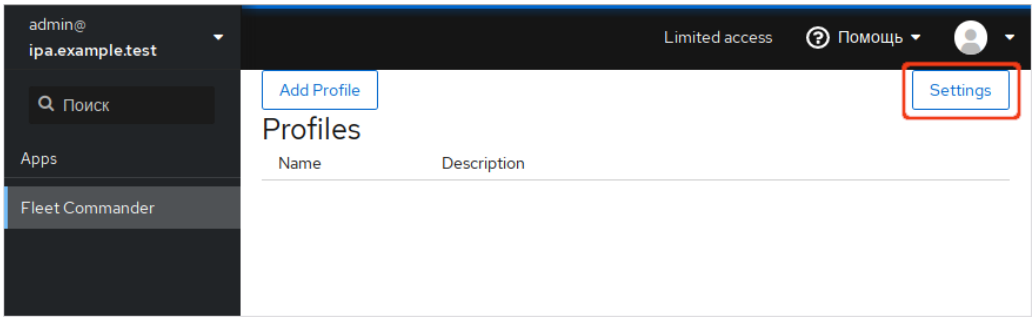


Рис. 149

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. 149).

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. 150) 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 (пользователь должен быть включён в группу vmusers);
- «Libvirt mode» – если пользователь не является привилегированным, то следует переключить данную настройку в режим сеанса.

Fleet Commander генерирует свой собственный открытый ключ, который необходимо добавить в .ssh/authorized_keys для соответствующего пользователя на libvirt-хосте. Это можно сделать, нажав кнопку «Install public key», 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).

Окно настроек Fleet Commander

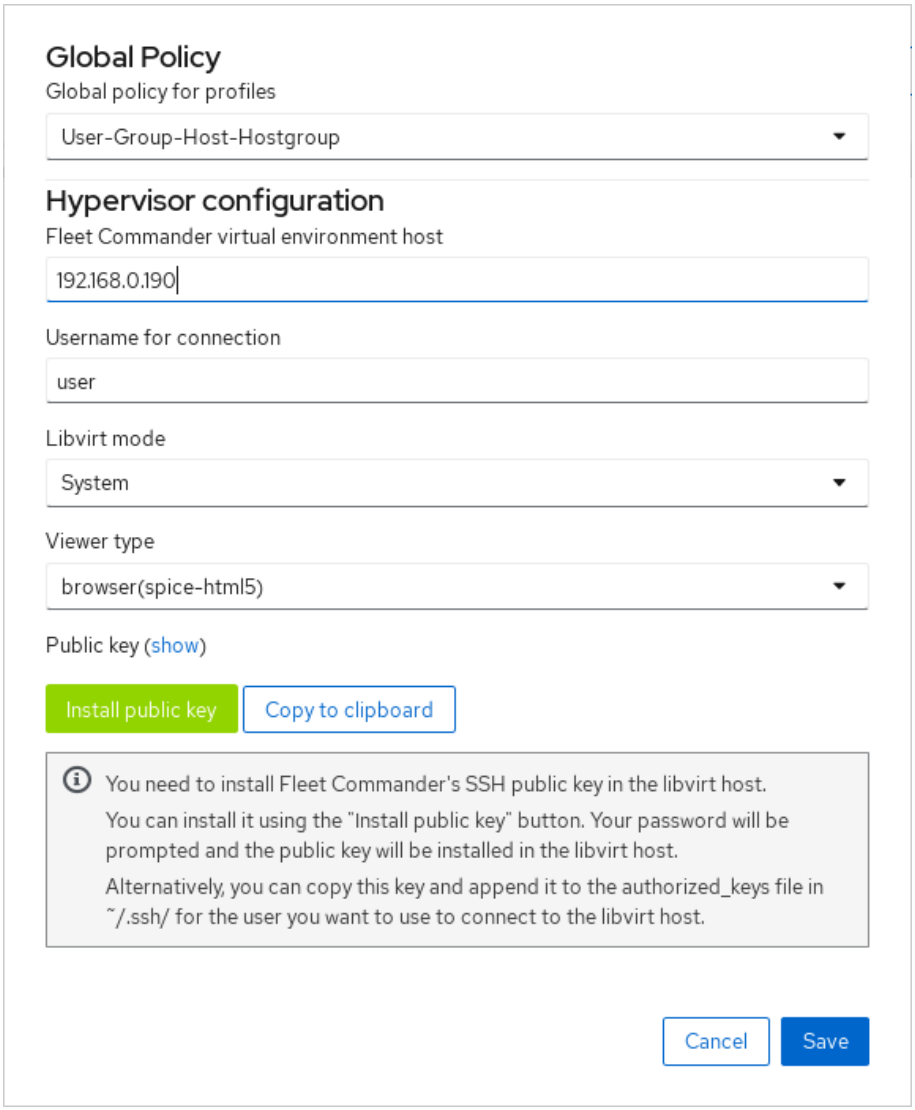


Рис. 150

5.6.1.3 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. 151).

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.

Fleet Commander. Создание профиля

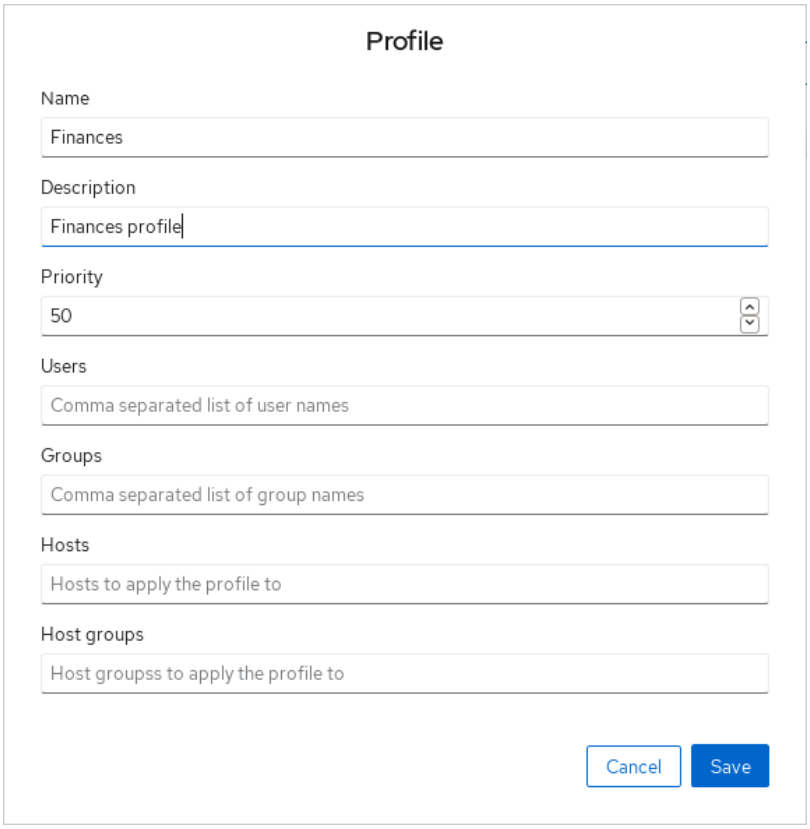


Рис. 151

Если не указан ни один хост или группа хостов, то профиль будет применен к каждому хосту, состоящему в домене.

5.6.1.4 Настройка шаблона

Для настройки шаблона в веб-интерфейсе Cockpit необходимо нажать кнопку «Edit» напротив нужного профиля (Рис. 152) и в открывшемся окне нажать кнопку «Live session» (Рис. 153).

Fleet Commander. Редактирование профиля

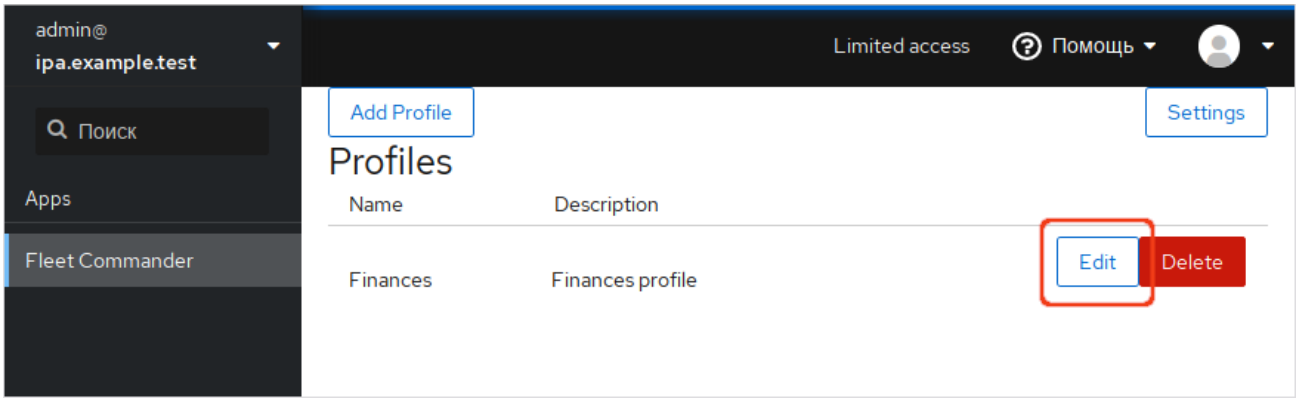


Рис. 152

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

Fleet Commander. Кнопка «Live session»

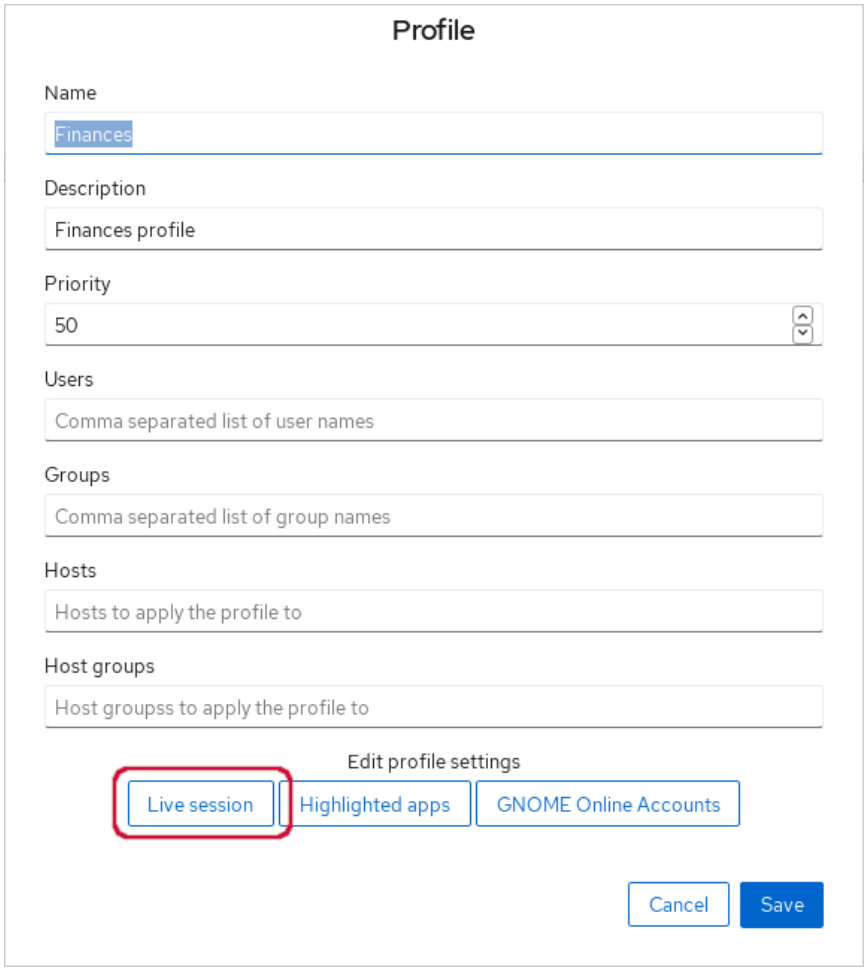


Рис. 153

5.6.1.5 Установка и настройка Fleet Commander Client

Клиентская машина должна быть введена в домен, а также должны быть созданы доменные пользователи.

Установить необходимый пакет:

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

Примечание. Пакет `fleet-commander-client` не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p10. О добавлении репозиториев можно почитать в разделе «Добавление репозиториев».

Клиент будет запускаться автоматически, при входе в домен с поддержкой Fleet Commander, и будет настраивать конфигурацию, которая применима к данному пользователю.

5.6.2 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. 154);
- выбрать машину, на которой установлен Fleet Commander Logger, и запустить ее (Рис. 155). 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. 156). 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

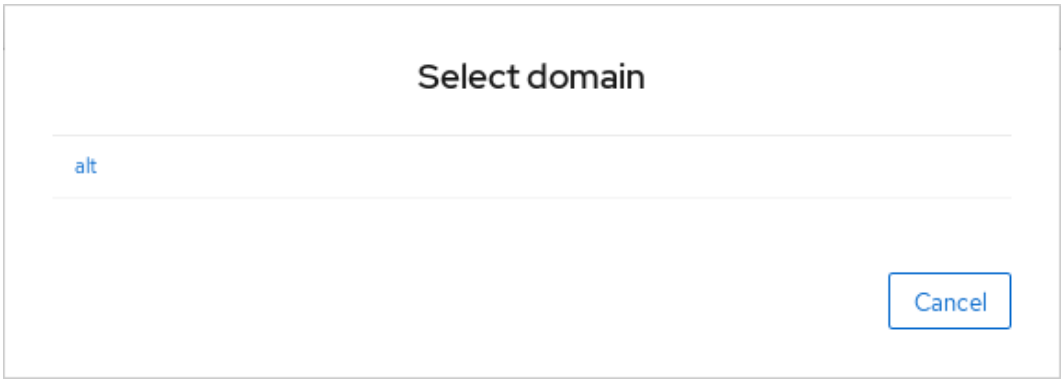


Рис. 154

Fleet Commander. Загруженный шаблон

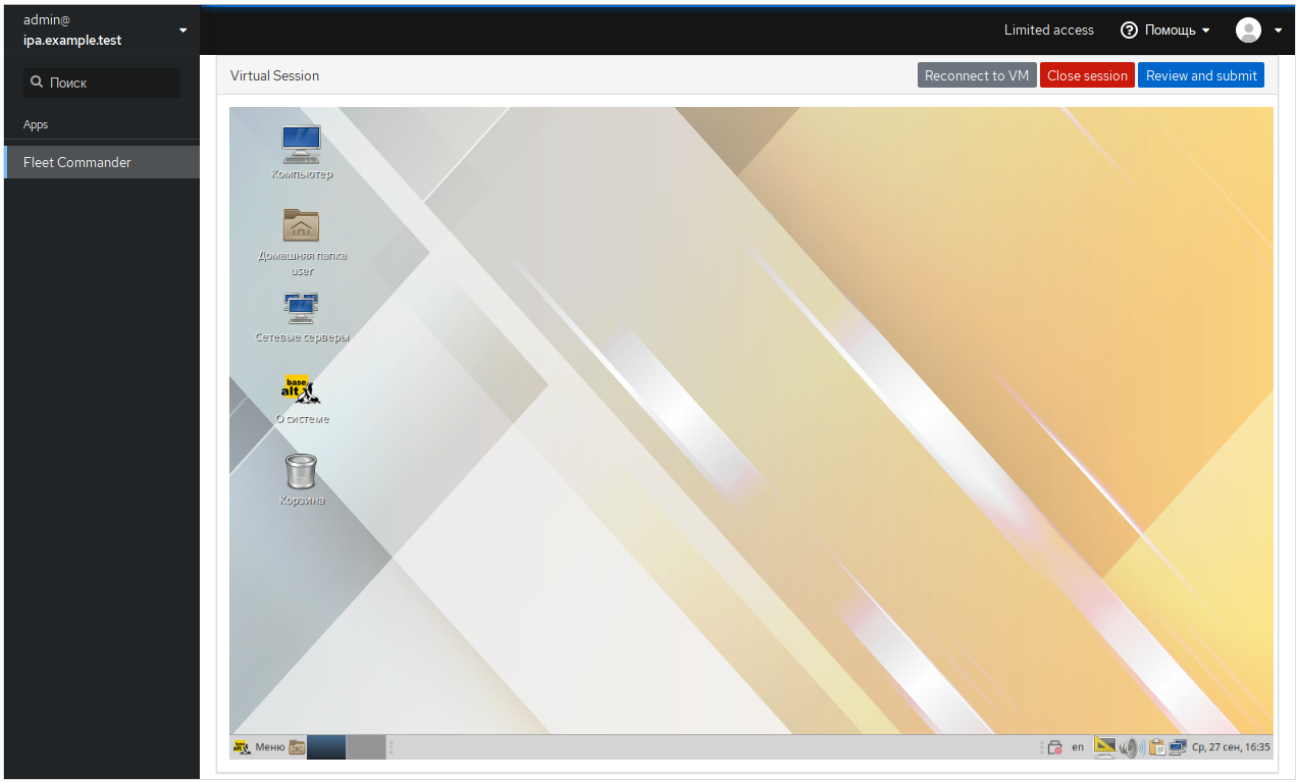


Рис. 155

Окно со списком сделанных изменений

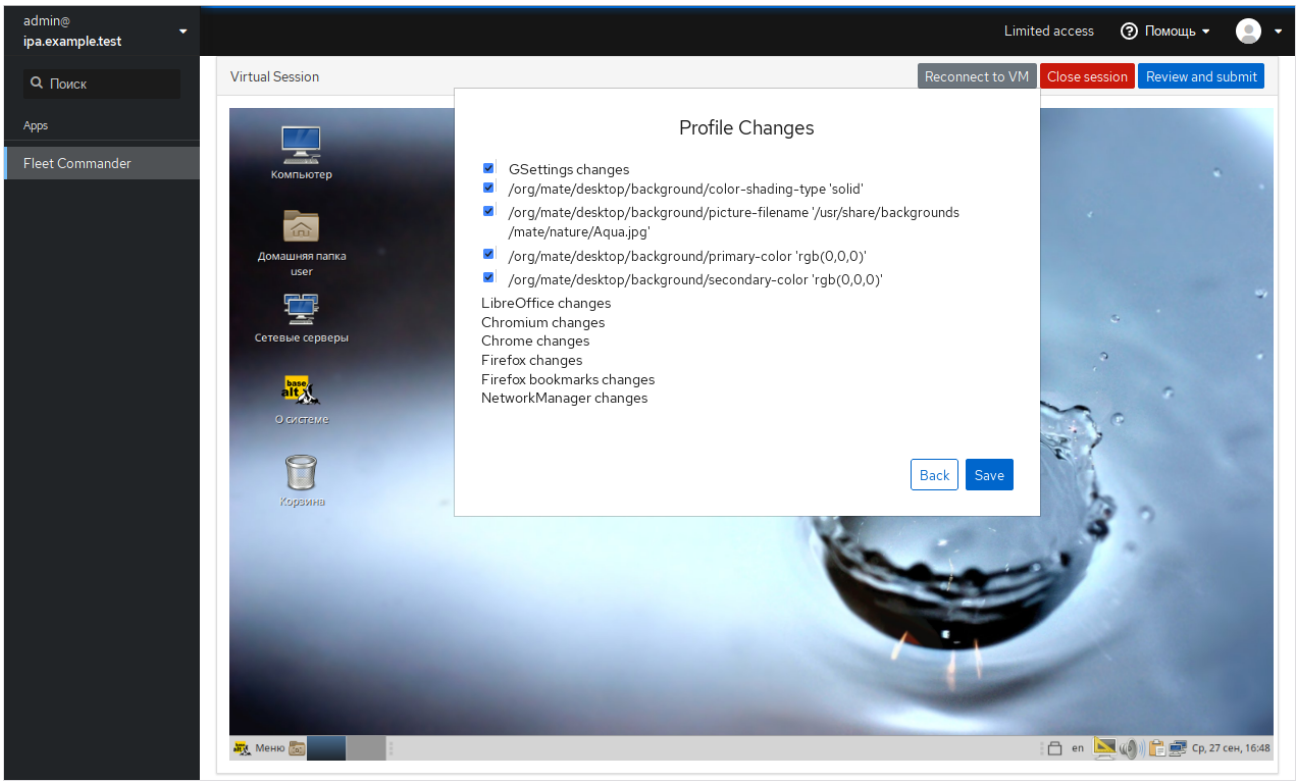


Рис. 156

5.6.3 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.

5.7 Система мониторинга 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.

5.7.1 Установка сервера PostgreSQL

Установить PostgreSQL, Zabbix-сервер и дополнительную утилиту `fping`:

```
# apt-get install postgresql15-server zabbix-server-pgsql fping
```

Подготовить к запуску и настроить службы PostgreSQL:

- создать системные базы данных:

```
# /etc/init.d/postgresql initdb
```

- включить по умолчанию и запустить службу postgresql:

```
# systemctl enable --now postgresql
```

- 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'
# systemctl restart postgresql
```

- 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-com-
mon-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-com-
mon-database-pgsql-*/images.sql zabbix'
# postgres -s /bin/sh -c 'psql -U zabbix -f /usr/share/doc/zabbix-com-
mon-database-pgsql-*/data.sql zabbix'
```

5.7.2 Установка Apache2

Установить необходимые пакеты:

```
# apt-get install apache2 apache2-mod_php8.2
```

Добавить в автозапуск и запустить apache2:

```
# systemctl enable --now httpd2
```

5.7.3 Установка PHP

Примечание. Начиная с версии php8.0, пакеты модулей именуются следующим образом: `php<мажорная>.<минорная версии>-<имя модуля>`

Из репозитория можно установить и эксплуатировать в одной системе одновременно разные версии PHP. В данном руководстве в качестве примера используется php8.2.

Установить необходимые пакеты:

```
# apt-get install php8.2 php8.2-mbstring php8.2-sockets php8.2-gd ph-
p8.2-xmlreader php8.2-pgsql php8.2-ldap php8.2-openssl
```

Изменить опции php в файле `/etc/php/8.2/apache2-mod_php/php.ini`:

```
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:

```
# systemctl restart httpd2
```

5.7.4 Настройка и запуск Zabbix-сервера

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

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

Добавить Zabbix-сервер в автозапуск и запустить его:

```
# systemctl enable --now zabbix_pgsql
```

5.7.5 Установка веб-интерфейса Zabbix

Установить метапакет:

```
# apt-get install zabbix-phpfrontend-apache2
```

Включить аддоны в apache2:

```
# ln -s /etc/httpd2/conf/addon.d/A.zabbix.conf /etc/httpd2/conf/extra-
enabled/
```

Перезапустить apache2:

```
# systemctl restart httpd2
```

Изменить права доступа к конфигурационной директории веб-интерфейса, чтобы веб-установщик мог записать конфигурационный файл:

```
# chown apache2:apache2 /var/www/webapps/zabbix/ui/conf
```

Перейти на страницу установки zabbix сервера: http://<ip-сервера>/zabbix (Рис. 157). Здесь можно выбрать язык установки.

Страница установки Zabbix сервера

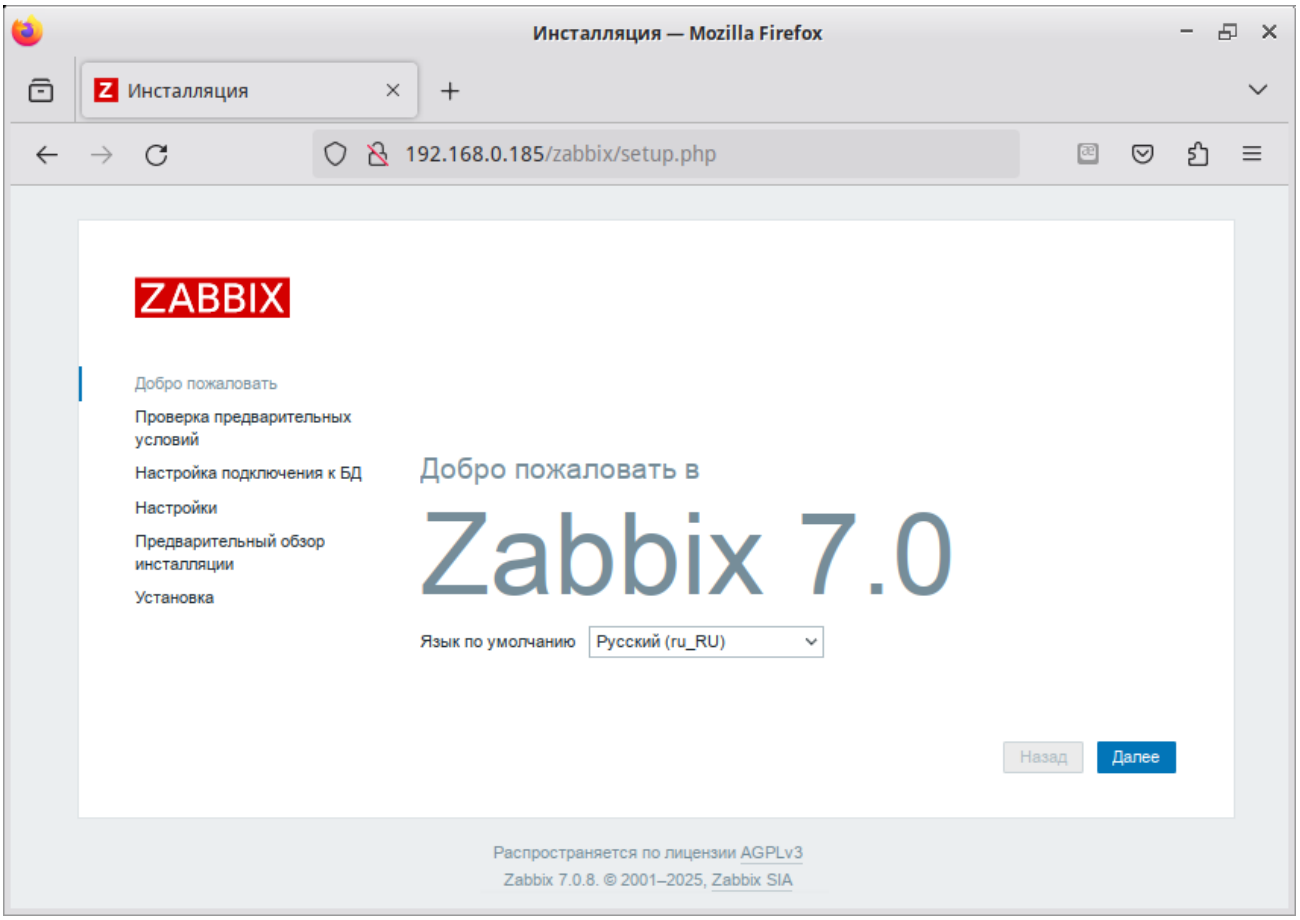


Рис. 157

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:

```
# systemctl restart httpd2
```

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 «Далее», что осуществит переход на страницу проверки предварительных условий (Рис. 158). Необходимо доустановить то, что требуется и перейти на следующую страницу.

Zabbix. Страница проверки предварительных условий

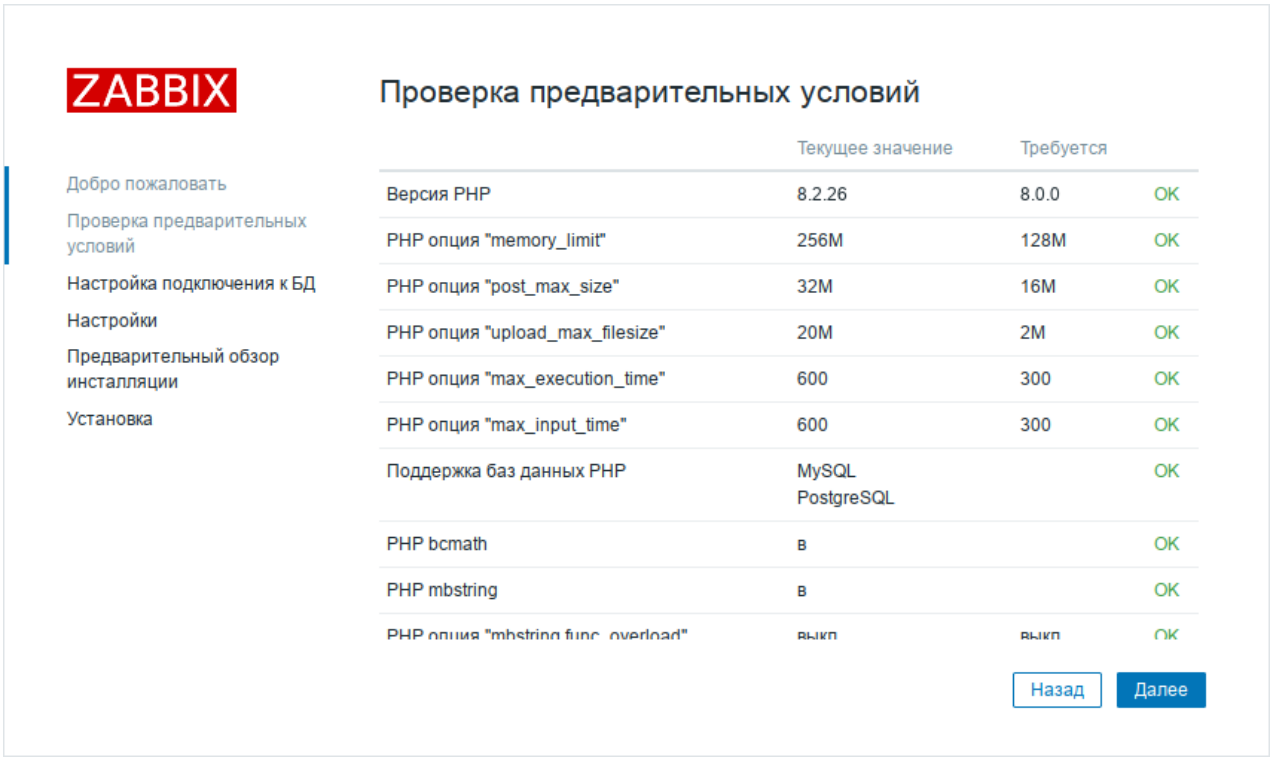


Рис. 158

На этой странице (Рис. 159) 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».

Zabbix. Параметры подключения к базе данных

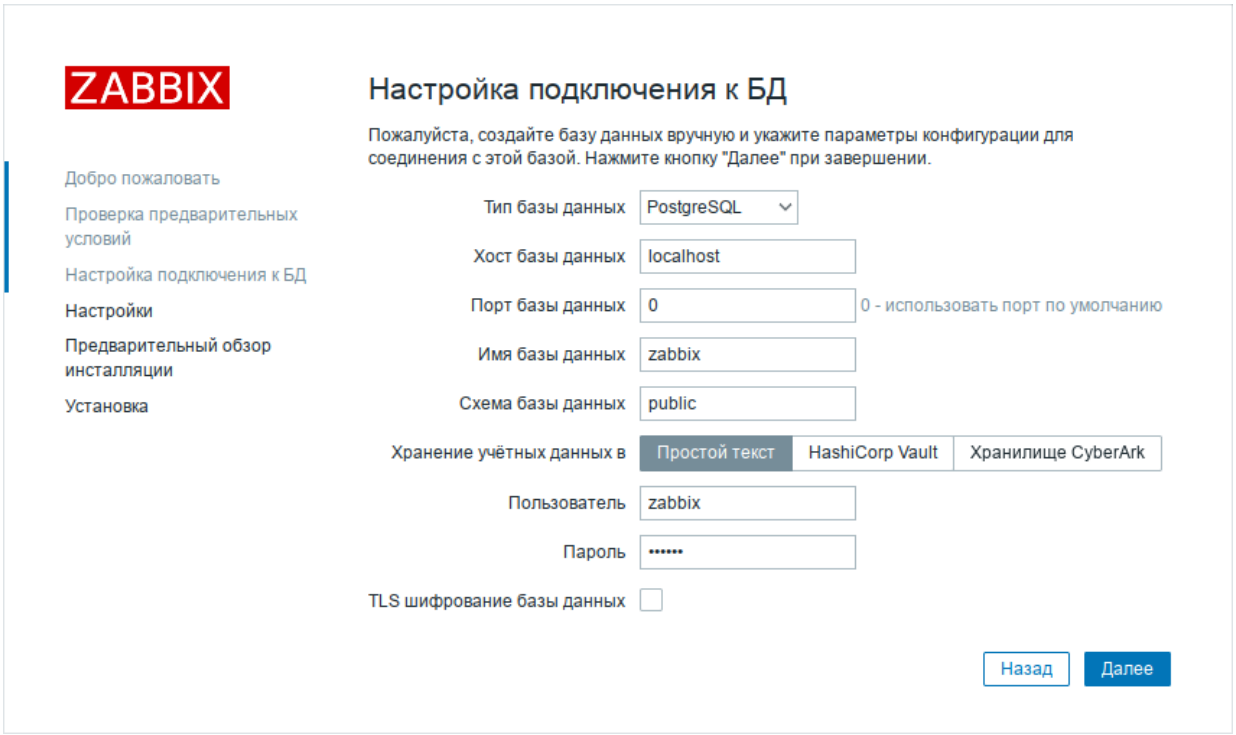


Рис. 159

На следующих страницах необходимо выбрать настройки веб-интерфейса и задать имя сервера (Рис. 160), и завершить установку (Рис. 161, Рис. 162).

Настройки Zabbix сервера

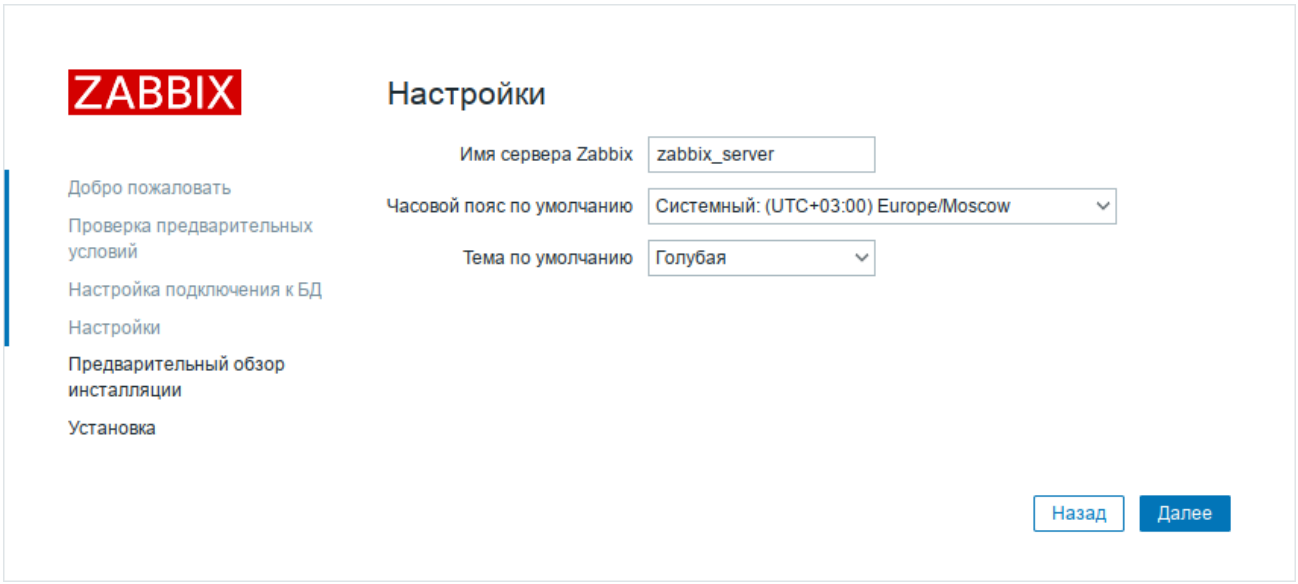


Рис. 160

Zabbix. Параметры конфигурации

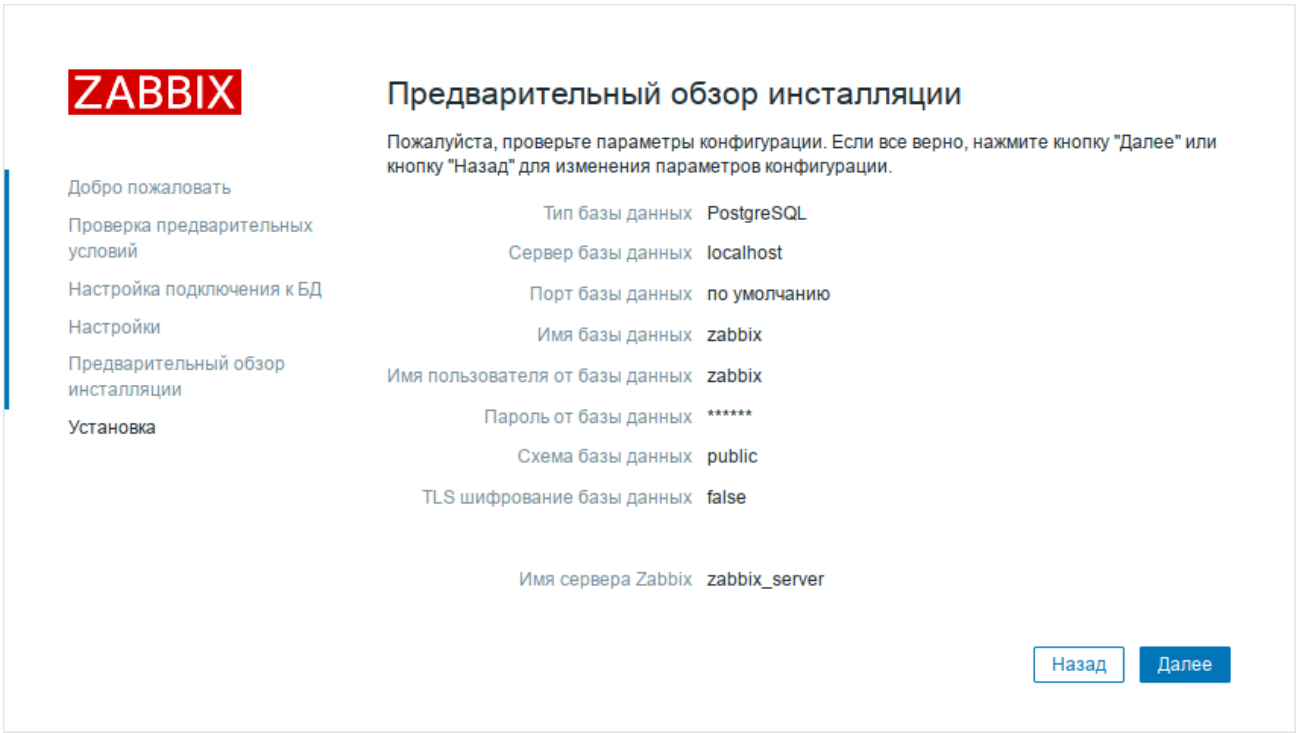


Рис. 161

Zabbix. Окончание установки

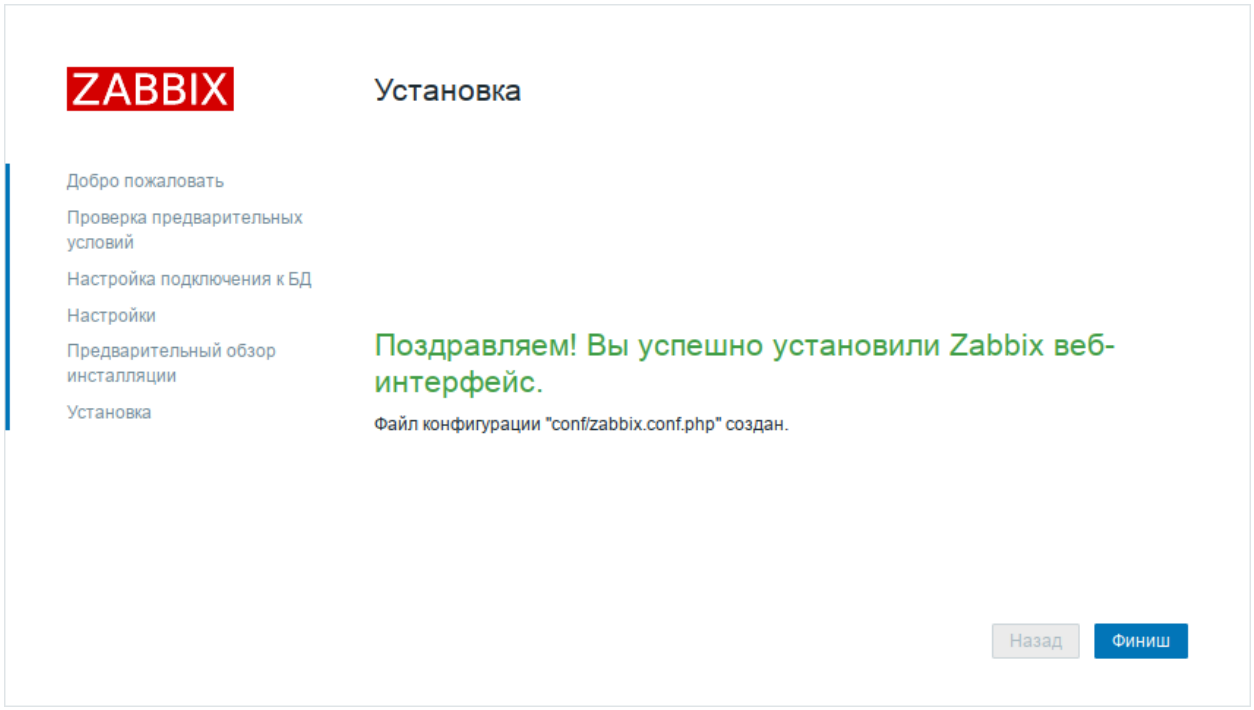


Рис. 162

После окончания установки на экране будет отображаться форма входа в интерфейс управления системой мониторинга (Рис. 163). Параметры доступа по умолчанию:

`Логин: Admin`

`Пароль: zabbix`

Форма входа в интерфейс управления системой мониторинга

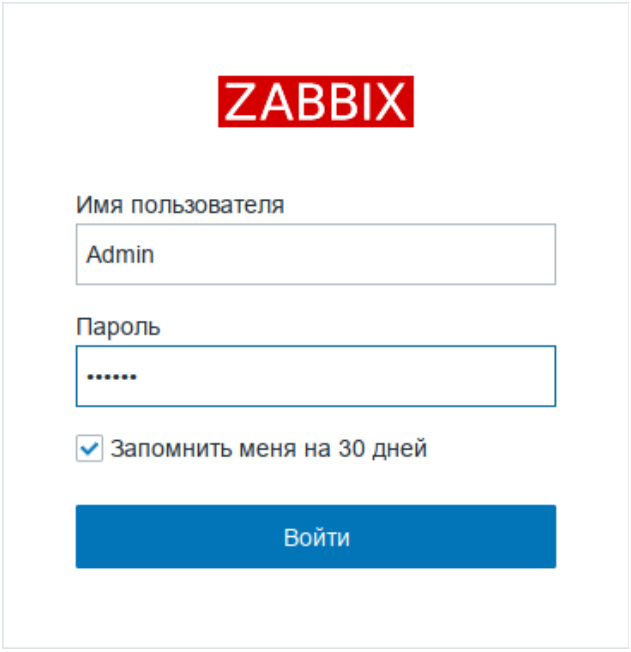


Рис. 163

Войдя в систему, нужно сменить пароль пользователя, завести других пользователей и можно начать настраивать Zabbix (Рис. 164).

Интерфейс управления системой мониторинга

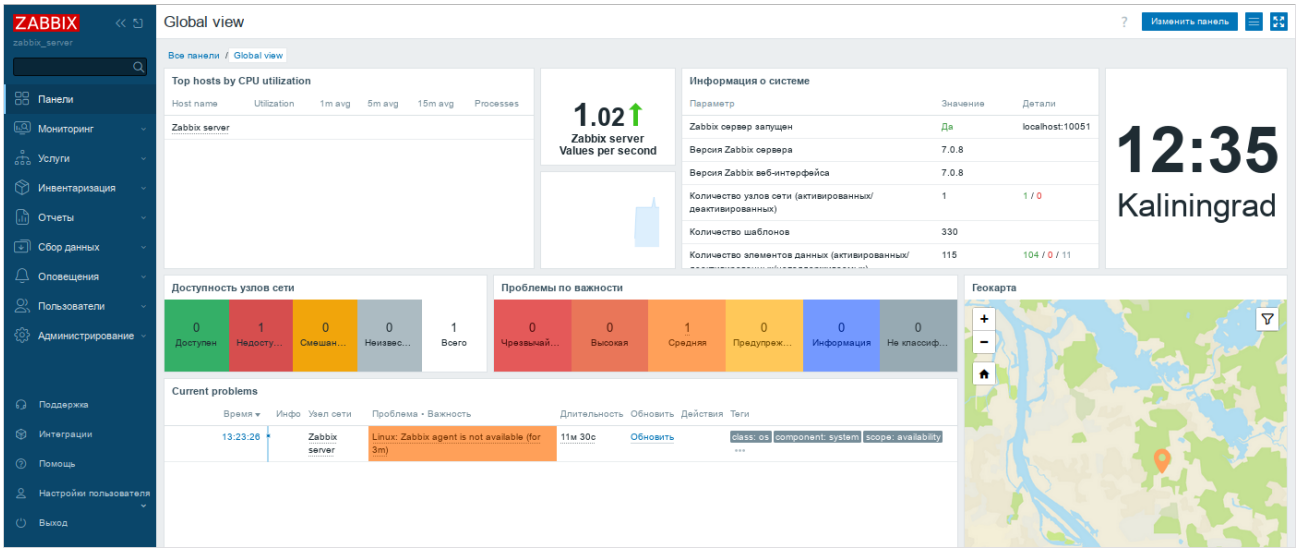


Рис. 164

В профиле пользователя (Рис. 165) 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

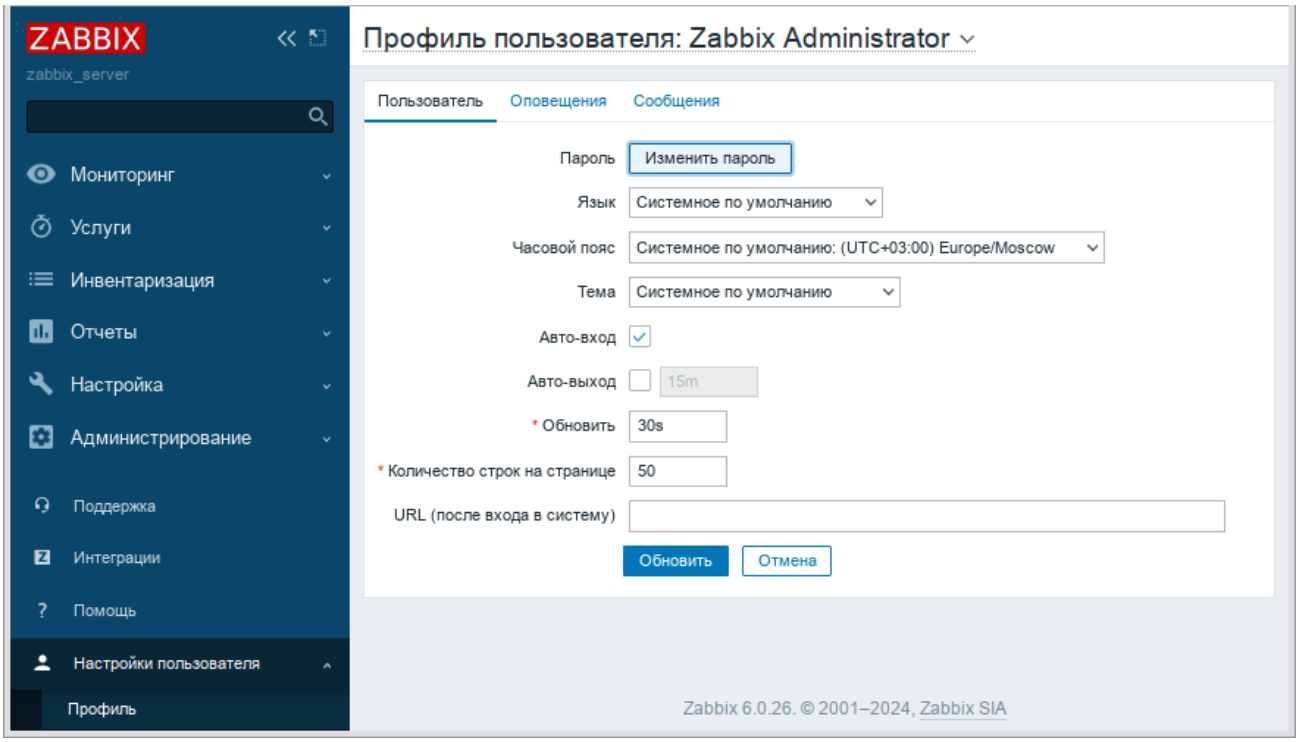


Рис. 165

Чтобы собирать информацию с узлов, сервер Zabbix использует информацию, получаемую от агентов. Чтобы добавить новый узел, следует установить на узел, который необходимо мониторить, Zabbix-агент и добавить новый хост на Zabbix-сервере.

5.7.6 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=comp01.example.test
```

где comp01.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
```

Примечание. Для настройки Zabbix-агента можно воспользоваться модулем ЦУС «Агент наблюдения».

5.7.7 Добавление нового хоста на сервер Zabbix

Каждый хост необходимо зарегистрировать на сервере Zabbix.

Информация о настроенных узлах сети в Zabbix доступна в разделе «Сбор данных» → «Узлы сети». Для добавления нового узла сети следует нажать кнопку «Создать узел сети» (Рис. 166).

Создание нового узла сети

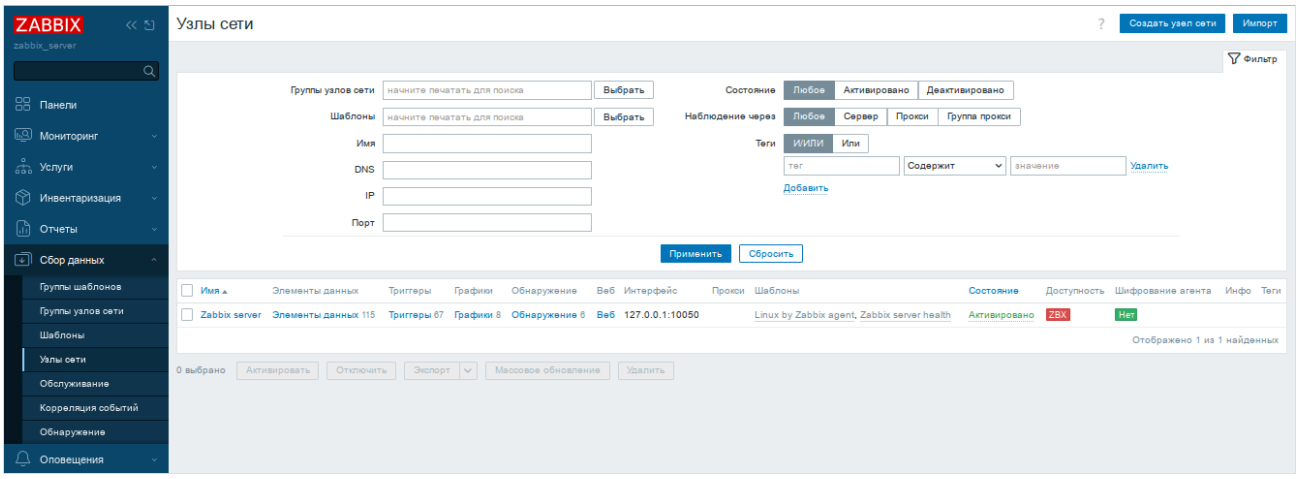


Рис. 166

В открывшемся окне необходимо заполнить поля «Имя узла сети» и «IP адрес» согласно данным добавляемого хоста, выбрать шаблон «Linux by Zabbix agent», добавить хост в определенную группу (выбрав одну из них из списка, либо создав новую группу) и нажать кнопку «Добавить» (Рис. 167).

Создание нового узла сети. Данные добавляемого хоста

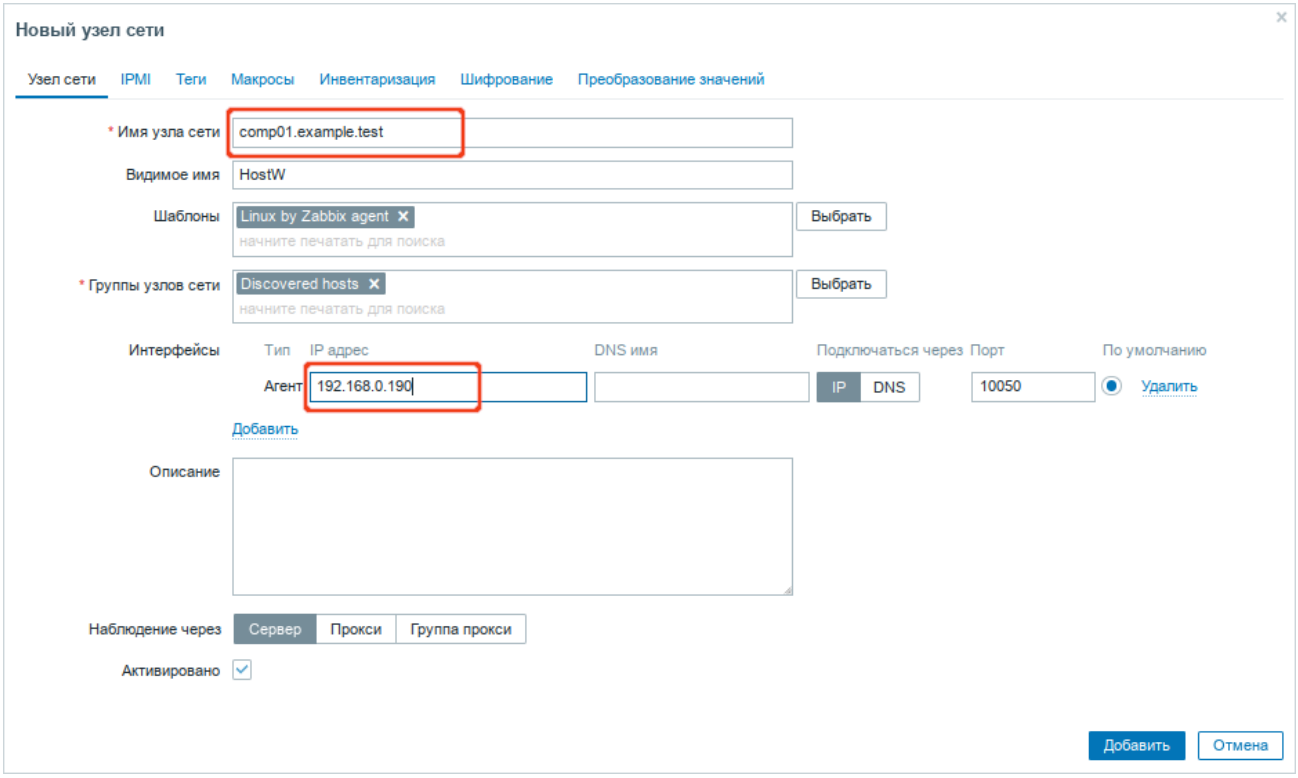


Рис. 167

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.

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. 168).

5.7.8 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.

Собранные данные

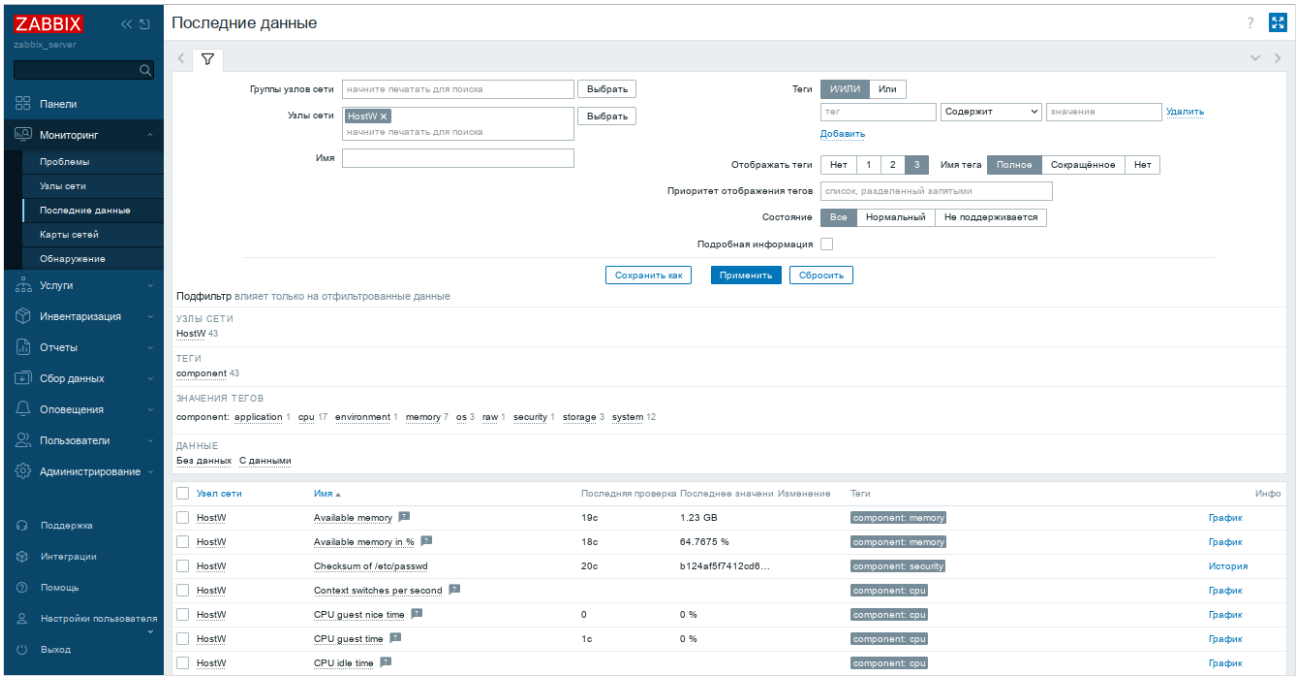


Рис. 168

Для настройки авторегистрации необходимо перейти в «Оповещения» → «Действия» → «Действия авторегистрации» и нажать кнопку «Создать действие» (Рис. 169).

Авторегистрация узлов

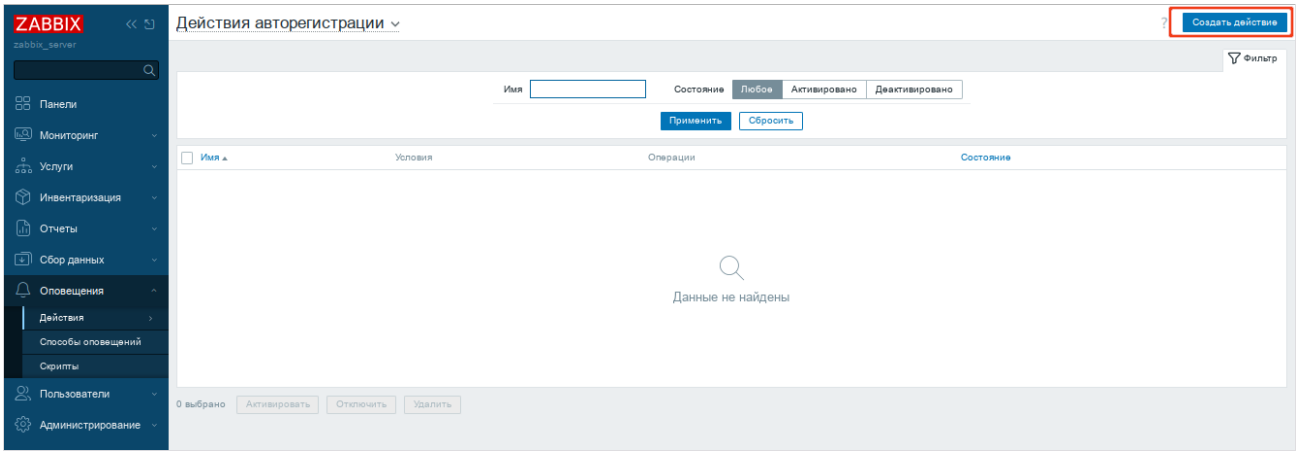


Рис. 169

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. 170).

Авторегистрация узлов. Условия идентификации узла

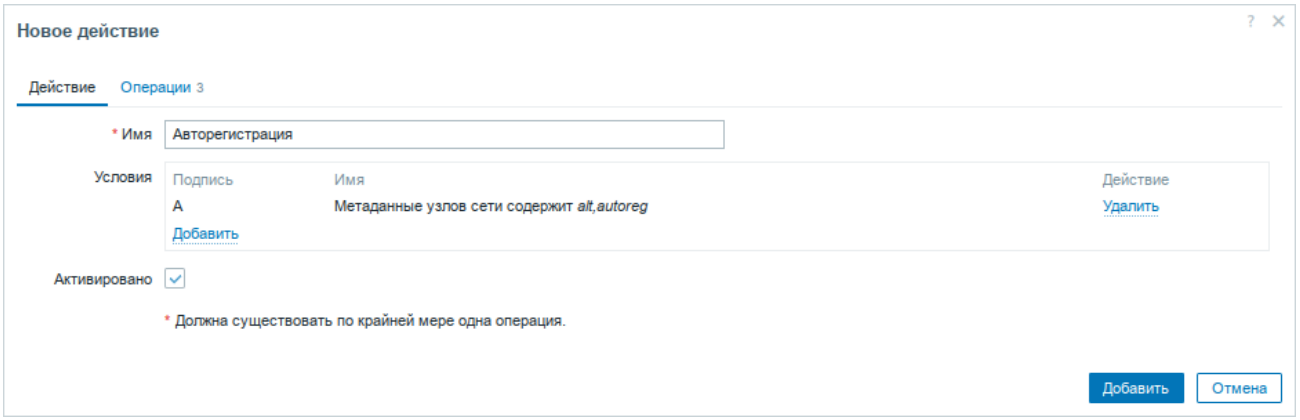


Рис. 170

На вкладке «Операции» в поле «Операции» следует добавить правила, которые необходимо применить при регистрации хоста. Пример набора правил для регистрации узла, добавления его к группе «Discovered hosts» с присоединением к шаблону «Linux by Zabbix agent» показаны на Рис. 171.

Авторегистрация узлов. Правила, применяемые при регистрации узла

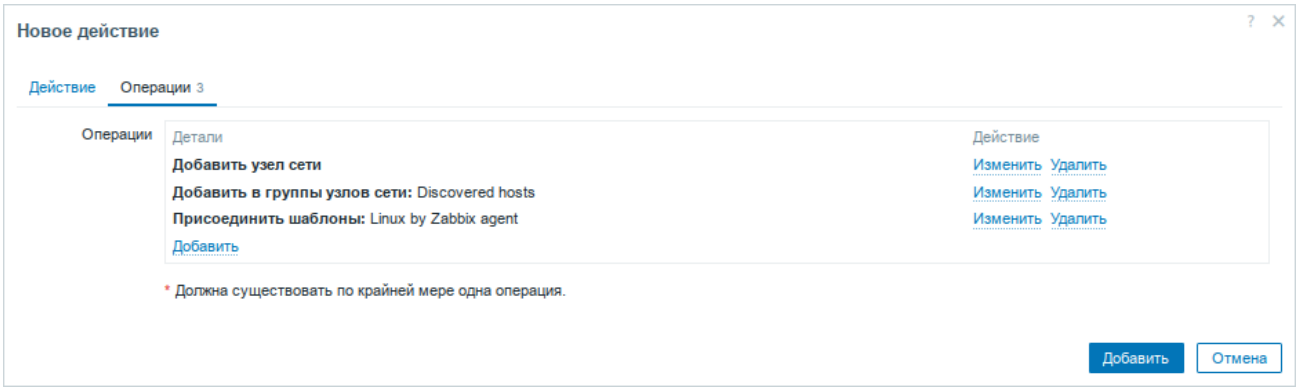


Рис. 171

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.

5.8 Nextcloud – хранение документов в «облаке»

Nextcloud – веб-приложение для синхронизации данных, общего доступа к файлам и удалённого хранения документов в «облаке».

Файлы Nextcloud хранятся в обычных структурах каталогов и могут быть доступны через WebDAV, если это необходимо.

5.8.1 Установка

Развернуть Nextcloud можно, используя пакет `deploy`:

```
# apt-get install deploy
# deploy nextcloud
```

Примечание. Nextcloud можно установить при установке системы, выбрав для установки пункт «Серверные Nextcloud». Если при установке системы доступ к сети отсутствует, то Nextcloud не будет развёрнут. В этом случае развернуть Nextcloud можно, выполнив команду:

```
# deploy nextcloud
```

Для доступа к административным функциям Nextcloud через веб-интерфейс необходимо установить пароль пользователю ncadmin (пароль должен быть достаточно сложным и содержать не менее 10 символов):

```
# deploy nextcloud password=5Z4SAq2U28rWyVz
```

Веб-приложение Nextcloud будет доступно по адресу https://<сервер>/nextcloud/. Где «сервер» – localhost или имя, заданное компьютеру при установке системы на этапе «Настройка сети». Просмотреть имя компьютера можно, выполнив команду:

```
$ hostname
```

Примечание. По умолчанию непоследовательное обновление мажорных версий запрещено (например, с версии 20 сразу до 22), и при попытке доступа к веб-интерфейсу после обновления пакета будет возникать ошибка `Exception: Updates between multiple major versions and downgrades are unsupported`. Для того чтобы обойти эту ошибку, продолжить обновление и получить доступ к веб-интерфейсу, необходимо:

- в файле `/var/www/webapps/nextcloud/config/config.php` в параметре `version` изменить старую версию на новую;
- перейти в веб-интерфейс и обновить страницу.

5.8.2 Настройка Nextcloud

`/var/www/webapps/nextcloud/config/config.php` – файл конфигурации Nextcloud.

Примечание. После внесения изменений в файл конфигурации Nextcloud необходимо перезапустить веб-сервер:

```
# systemctl restart httpd2
```

Настроить кэширование можно, добавив следующие строки в файл конфигурации Nextcloud:

```
'memcache.local' => '\OC\Memcache\Memcached',
'memcache.distributed' => '\OC\Memcache\Memcached',
'memcached_servers' => array(
```

```
        array('localhost', 11211),
        ),
```

Примечание. Для возможности настройки кеширования, должны быть установлены пакеты memcached, php8.2-memcached, служба memcached должна быть добавлена в автозагрузку:

```
# apt-get install memcached php8.2-memcached
# systemctl enable --now memcached
```

После установки Nextcloud отвечает на запросы, сделанные только из localhost. Поэтому необходимо изменить настройки, для того чтобы получить доступ к Nextcloud при использовании доменного имени или IP-адреса сервера. Для этого следует добавить в файл конфигурации в раздел trusted_domains необходимые имена сервера:

```
'trusted_domains' =>
  array (
    0 => 'localhost',
    1 => 'host-15',
    2 => 'nextcloud.test.alt',
  ),
```

5.8.3 Работа с Nextcloud

Nextcloud доступен через веб-интерфейс по адресу https://localhost/nextcloud/ или по имени сервера https://nextcloud.test.alt/nextcloud/ (Рис. 172).

Окно авторизации Nextcloud

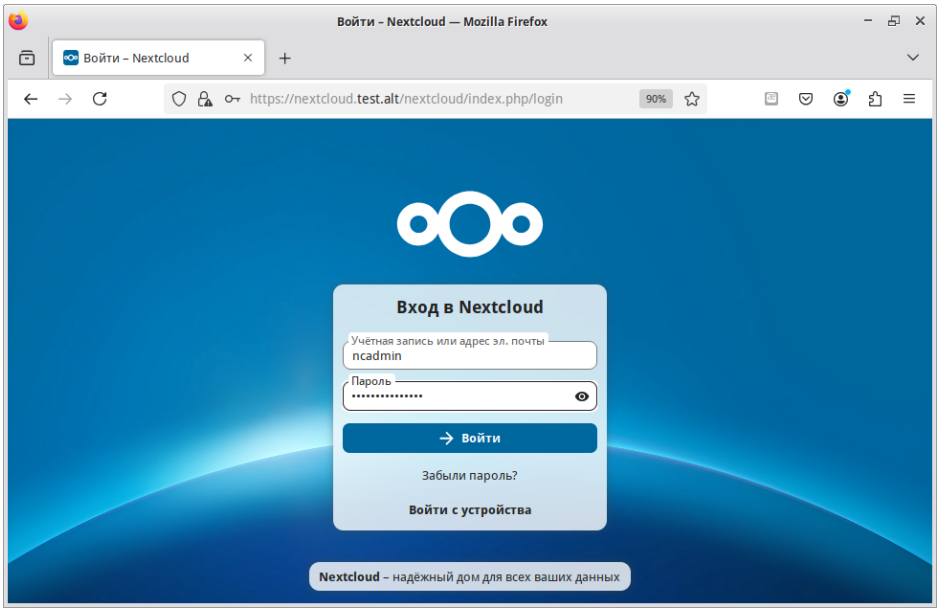


Рис. 172

Примечание. Если используется самоподписанный сертификат, то на клиентских машинах потребуется добавлять его в список доверенных.

После авторизации открывается панель управления Nextcloud, которую можно настроить (с помощью виджетов) так, как хочет пользователь (Рис. 173).

Окно Nextcloud

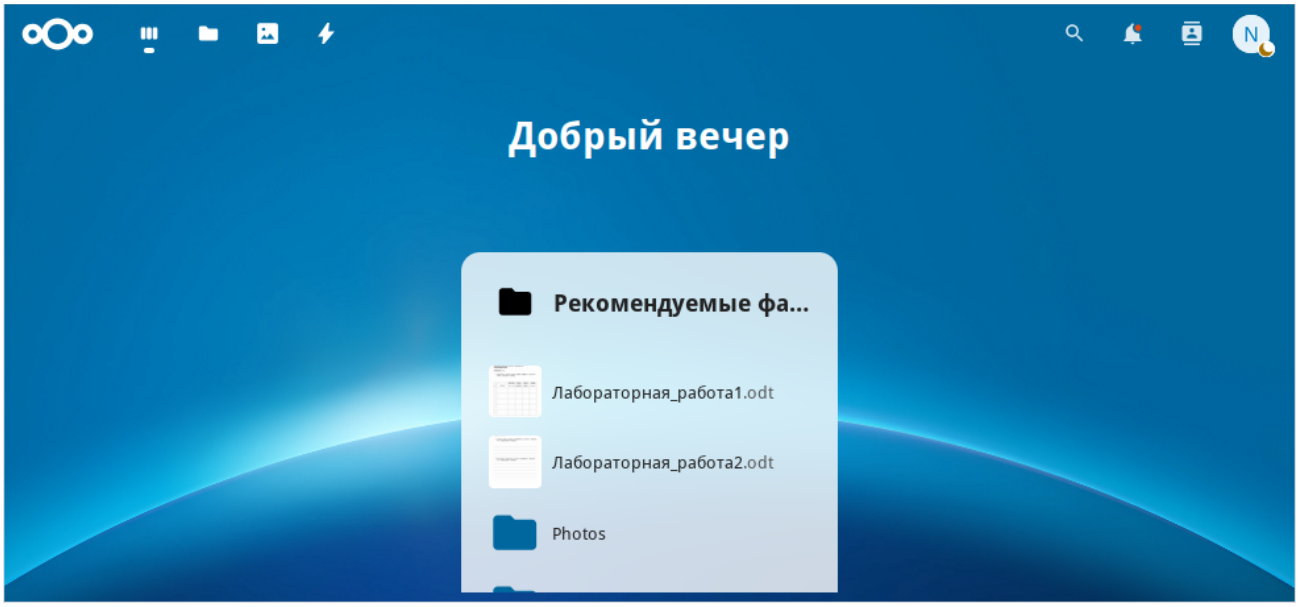


Рис. 173

5.8.4 Администрирование

Основные настройки Nextcloud доступны на странице «Параметры сервера». Открыть которую можно, щелкнув левой кнопкой мыши по логину администратора в правом верхнем углу и выбрав в выпадающем меню строку «Параметры сервера» (Рис. 174).

Основные настройки Nextcloud

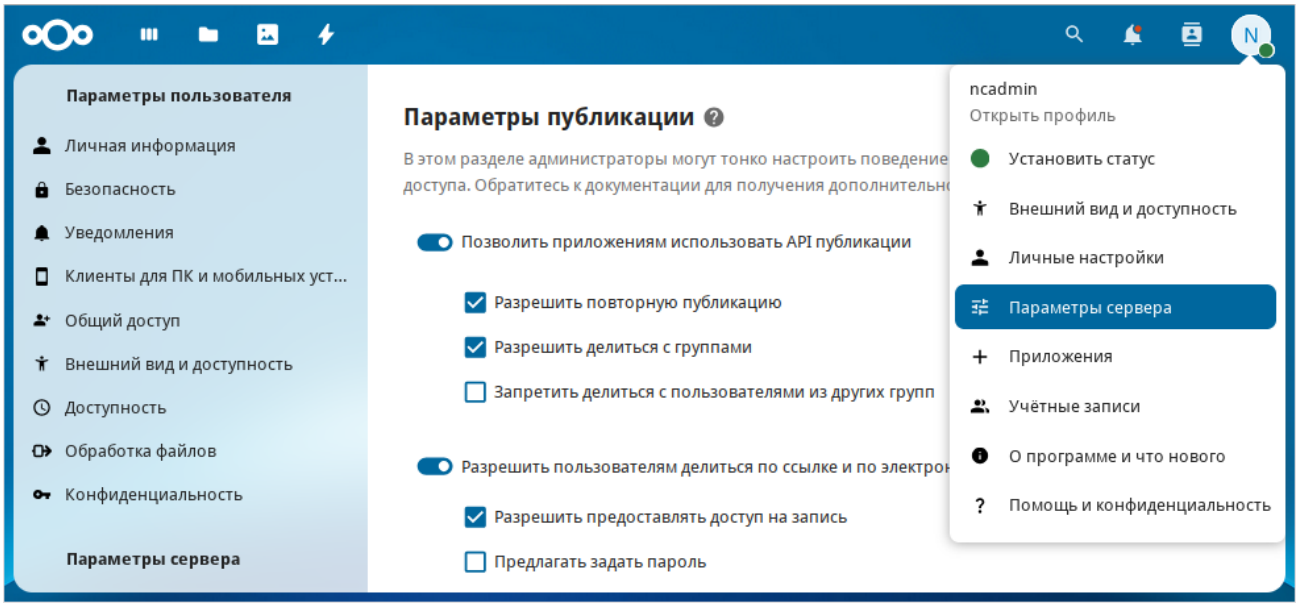


Рис. 174

На странице «Учетные записи» (Рис. 175) можно:

- просматривать текущих пользователей;

- создавать новых пользователей;
- изменять имена и пароли пользователей;
- просматривать и устанавливать квоты;
- фильтровать пользователей по группам;
- удалять пользователей.

Страница «Активные пользователи»

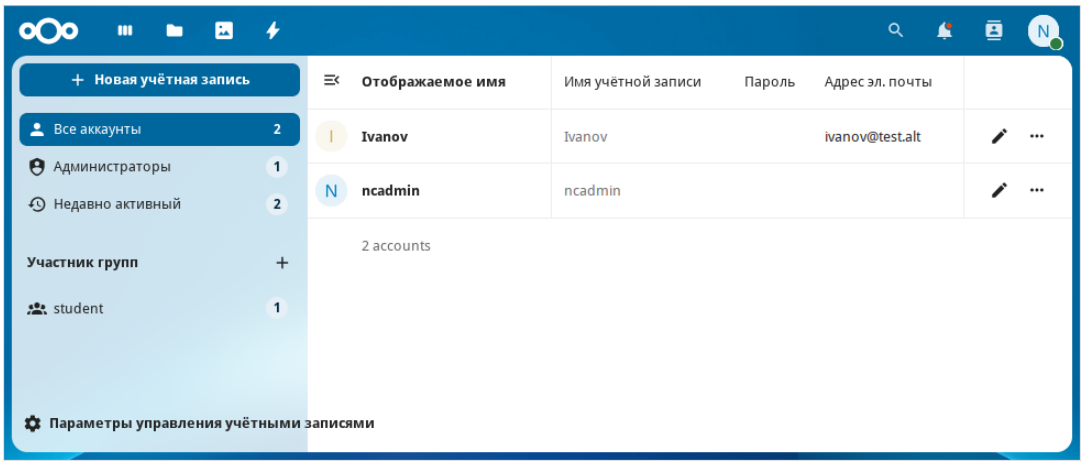


Рис. 175

Для создания пользователя, следует нажать кнопку «Новая учетная запись», ввести «Имя пользователя», «Пароль», при необходимости указать группу и нажать кнопку «Создать учетную запись» (Рис. 176).

Добавление пользователей

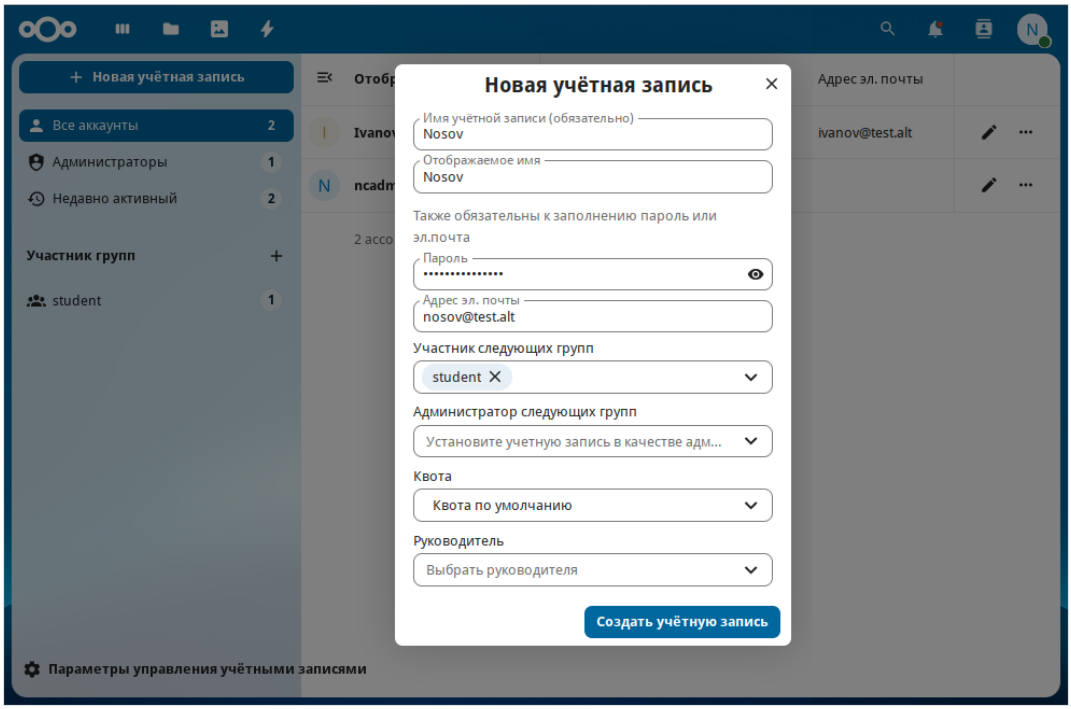


Рис. 176

5.8.5 Работа с файлами

Меню выбора доступных сервисов расположено в левом верхнем углу веб-интерфейса Nextcloud (Рис. 177).

При выборе раздела «Файлы» отображается структура каталогов пользователя (Рис. 178).

Меню выбора доступных сервисов

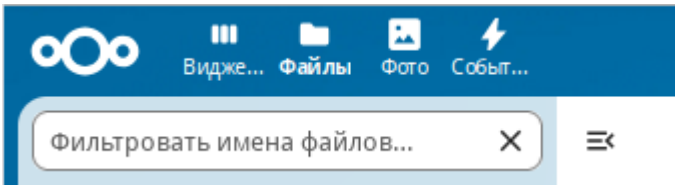


Рис. 177

Структура каталогов пользователя

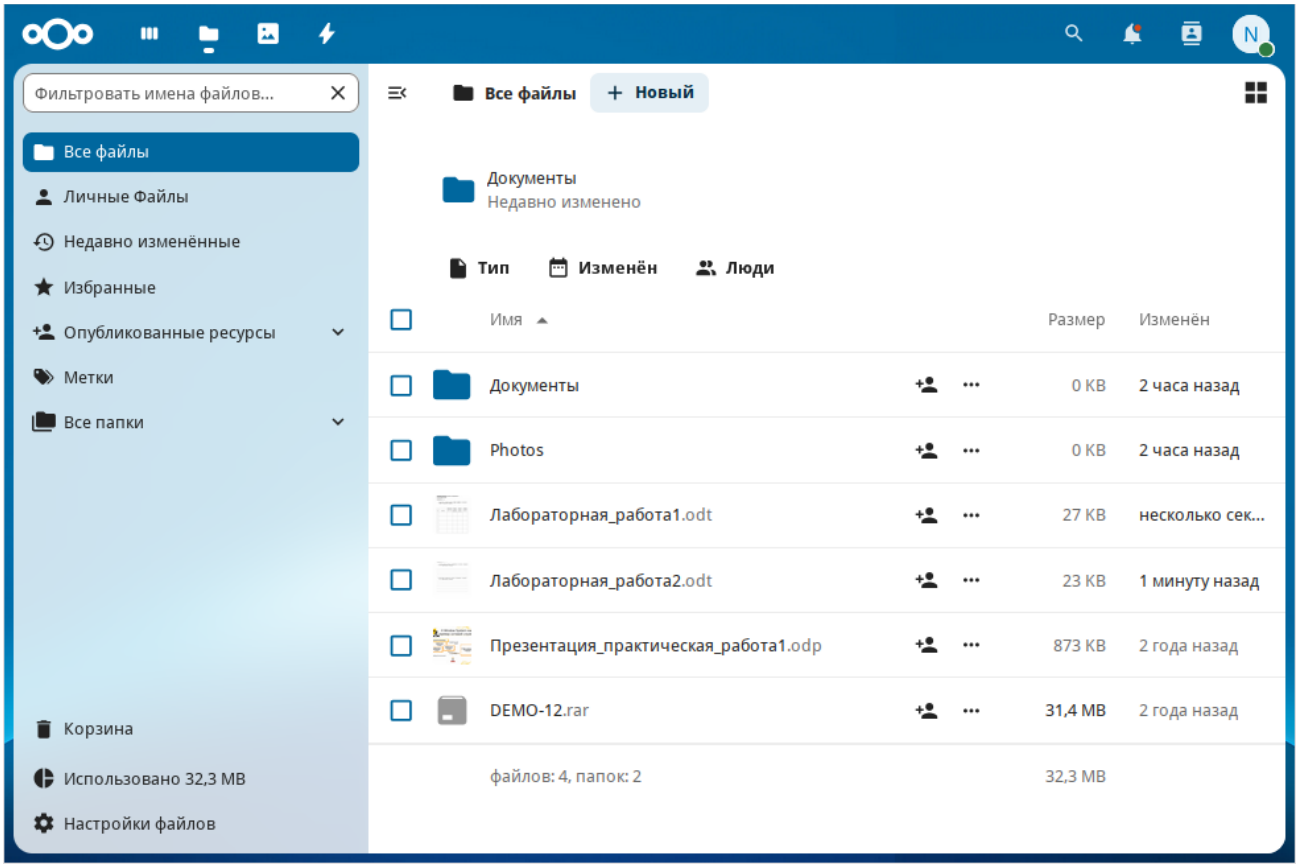


Рис. 178

Для того чтобы поделиться файлом или папкой с другими пользователями, необходимо нажать на значок человечка рядом с названием файла и в открывшемся окне настроить параметры общего доступа (Рис. 179).

Поделиться ссылкой может понадобиться в том случае, если необходимо предоставить доступ к файлу или папке людям, которые не входят в число пользователей Nextcloud.

Настройка доступа к файлу

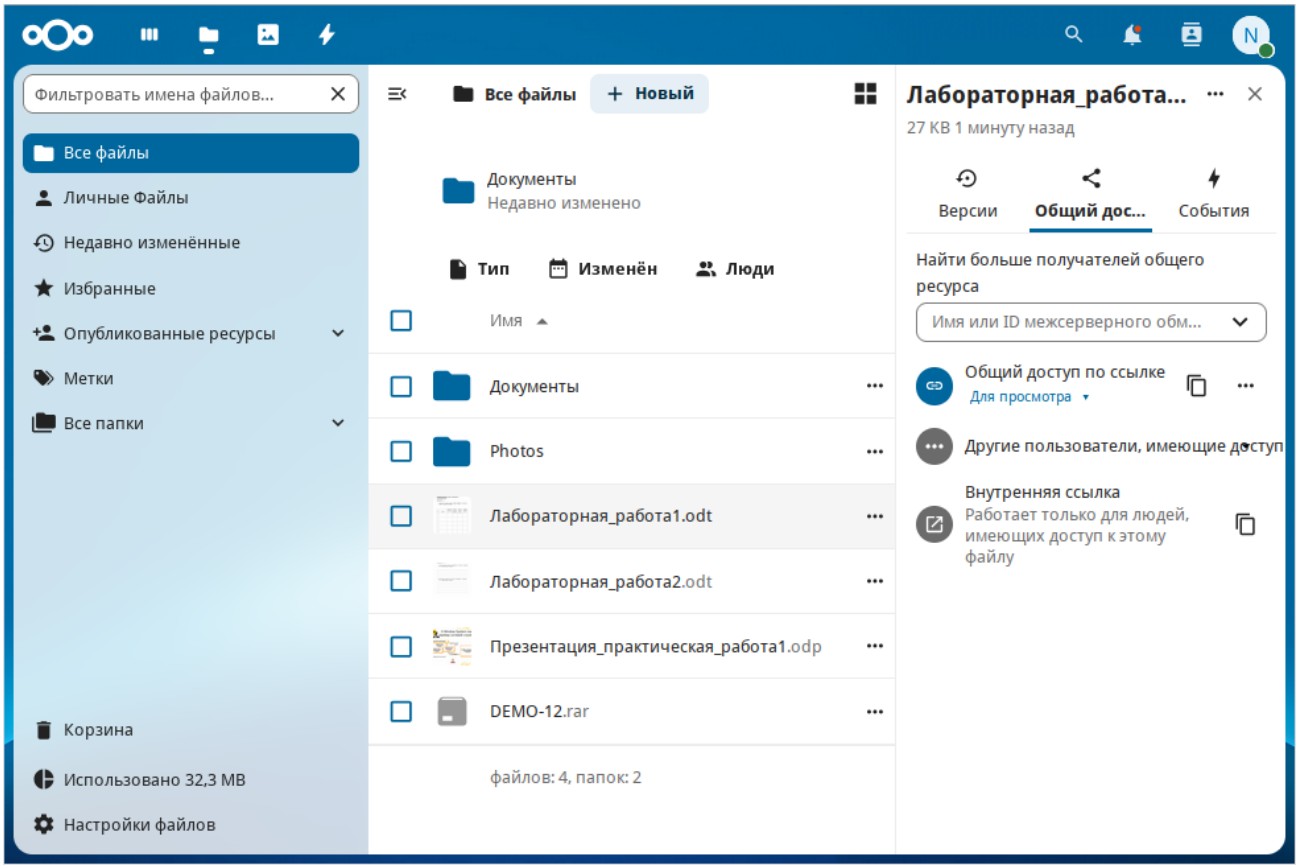


Рис. 179

5.9 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».

Примечание. Jitsi Meet нельзя развернуть на архитектуре aarch64.

5.9.1 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.

5.9.2 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.

5.9.3 Конфигурация

5.9.3.1 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
[...]
```

5.9.3.2 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
Choose key size (2048):
countryName (GB): RU
localityName (The Internet):
organizationName (Your Organisation):
organizationalUnitName (XMPP Department):
commonName (jitsi2.test.alt):
emailAddress (xmpp@jitsi2.test.alt):

Config written to /var/lib/prosody/jitsi2.test.alt.cnf
Certificate written to /var/lib/prosody/jitsi2.test.alt.crt

# prosodyctl cert generate auth.jitsi2.test.alt
Choose key size (2048):
countryName (GB): RU
localityName (The Internet):
organizationName (Your Organisation):
organizationalUnitName (XMPP Department):
commonName (auth.jitsi2.test.alt):
emailAddress (xmpp@auth.jitsi2.test.alt):

Config written to /var/lib/prosody/auth.jitsi2.test.alt.cnf
Certificate written to /var/lib/prosody/auth.jitsi2.test.alt.crt
```

Примечание. В ответах можно принять значения по умолчанию (можно просто нажать <Enter>) или ввести свои ответы. Важно в ответе на запрос `commonName (jitsi2.test.alt):` указать доменное имя сервера Prosody.

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
```

5.9.3.3 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
```

Запустить jicofo:

```
# systemctl start jicofo
```

Следует убедиться, что jicofo подключается к XMPP-серверу:

```
# curl -i localhost:8888/about/health
HTTP/1.1 500 Internal Server Error
Date: Wed, 27 Sep 2023 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.

5.9.3.4 Настройка jitsi-videobridge

Завести на XMPP-сервере аккаунт jvb@auth.jitsi2.test.alt:

```
# prosodyctl register jvb auth.jitsi2.test.alt secret3
```

Заменить содержимое файла `/etc/jitsi/videobridge/config` на следующее:

```
# Jitsi Videobridge settings

# extra options to pass to the JVB daemon
JVB_OPTS="--apis=,"


# adds java system props that are passed to jvb
# (default are for home and logging config file)
JAVA_SYS_PROPS="-Dnet.java.sip.communicator.SC_HOME_DIR_LOCATION=/etc/jitsi
-Dnet.java.sip.communicator.SC_HOME_DIR_NAME=videobridge
-Dnet.java.sip.communicator.SC_LOG_DIR_LOCATION=/var/log/jitsi
-Djava.util.logging.config.file=/etc/jitsi/videobridge/logging.properties
-Dconfig.file=/etc/jitsi/videobridge/application.conf"
```

В качестве файлов конфигурации jitsi-videobridge используются файлы /etc/jitsi/videobridge/application.conf и /etc/jitsi/videobridge/sip-communicator.properties.

В файле `/etc/jitsi/videobridge/application.conf` необходимо указать:

```
videobridge {
    stats {
        enabled = true
        transports = [
            { type = "muc" }
        ]
    }
    apis {
        xmpp-client {
            configs {
                shard {
                    hostname = "localhost"
                    domain = "auth.jitsi2.test.alt"
                    username = "jvb"
                    password = "secret3"
                    muc_jids = "JvbBrewery@internal.auth.jitsi2.test.alt"
                    # The muc_nickname must be unique across all instances
                    muc_nickname = "jvb-mid-123"
                }
            }
        }
    }
```

```
}
```

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).

Изменить 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.

Запустить JVB:

```
# systemctl start jitsi-videobridge
```

Убедиться, что между JVB и jicofo есть связь:

```
# curl -i localhost:8888/about/health
HTTP/1.1 200 OK
Date: Wed, 27 Sep 2023 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.

5.9.3.5 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:

```
# for mod in rewrite ssl headers proxy proxy_http; do a2enmod $mod;
done
# a2enport https
# a2dissite 000-default
# a2dissite 000-default_https
```

Включить конфигурацию Apache:

```
# a2ensite jitsi2.test.alt
```

Запустить веб-сервер Apache2 и добавить его в автозагрузку, выполнив команду:

```
# systemctl enable --now httpd2
```

5.9.4 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. 180).

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. 181).

Главная страница Jitsi Meet

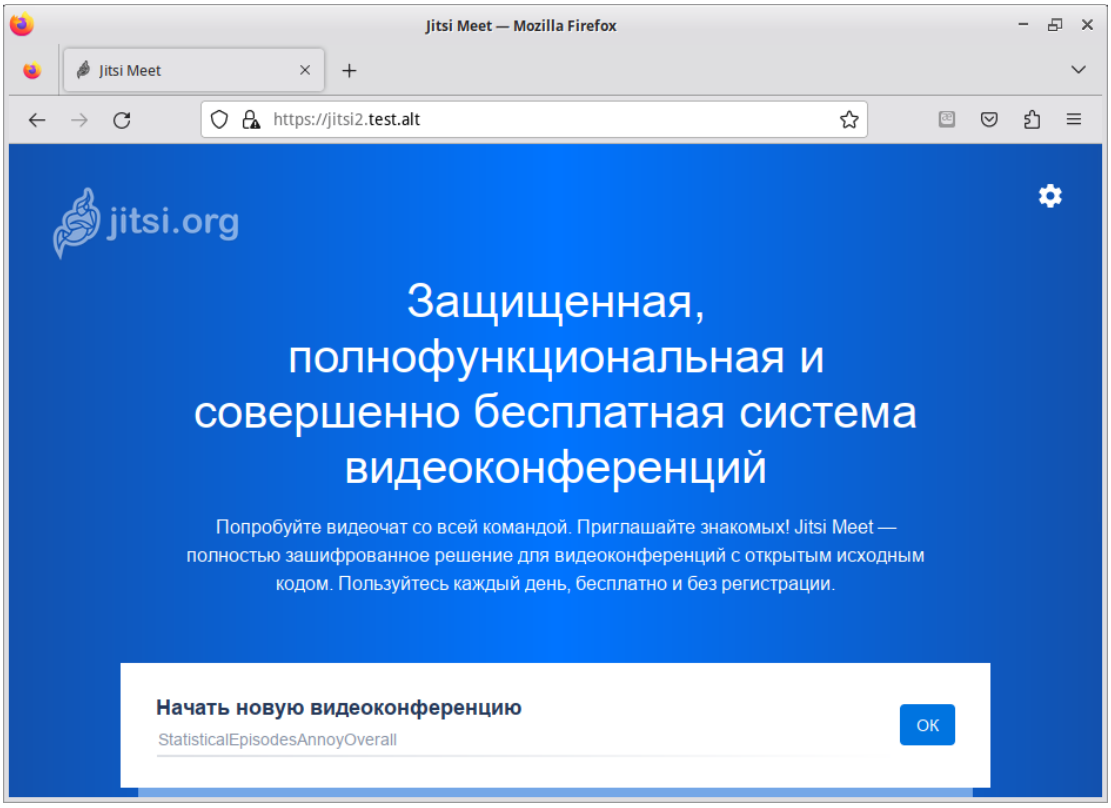


Рис. 180

Конференция Jitsi Meet

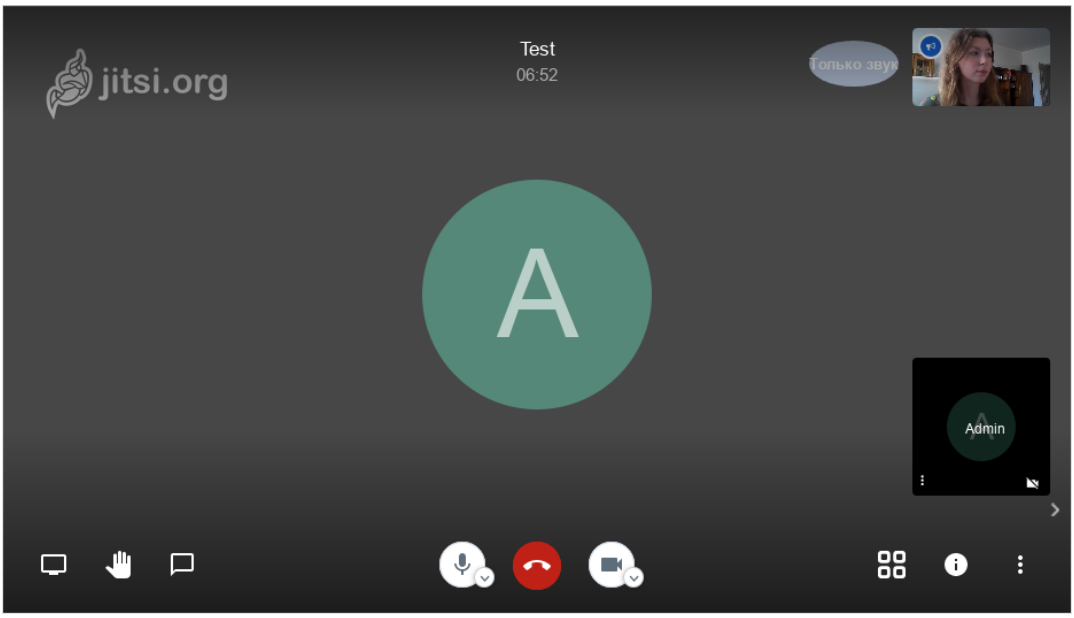


Рис. 181

Примечание. После создания конференции браузер попросит дать ему разрешение на использование веб-камеры и микрофона (Рис. 182).

Запрос на использование веб-камеры и микрофона

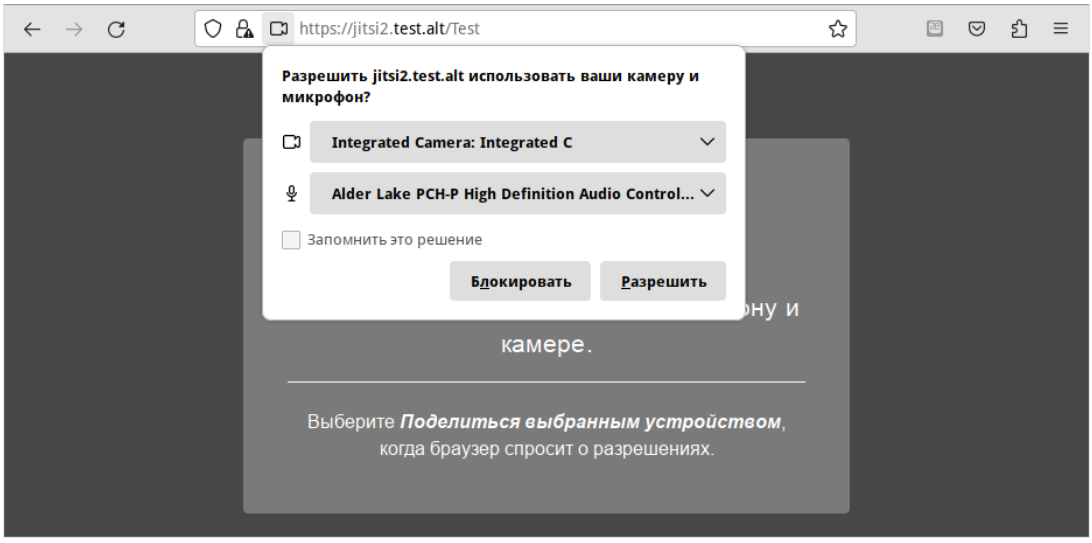


Рис. 182

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. 183).

Панель управления Jitsi Meet

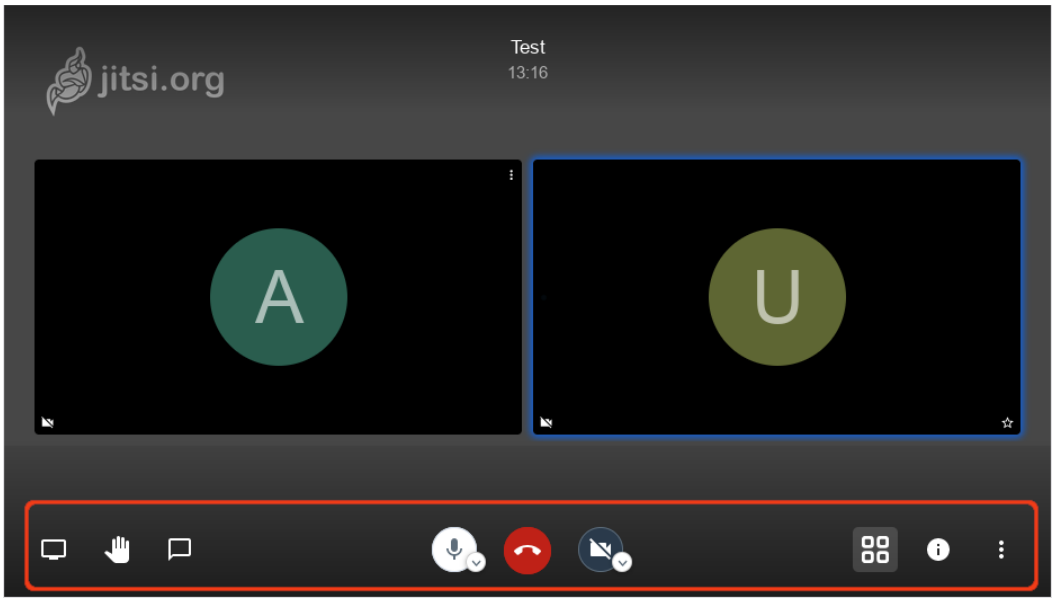


Рис. 183

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. 184):

- экран монитора;
- окно приложения;
- определённая вкладка браузера.

Выбор окна экрана

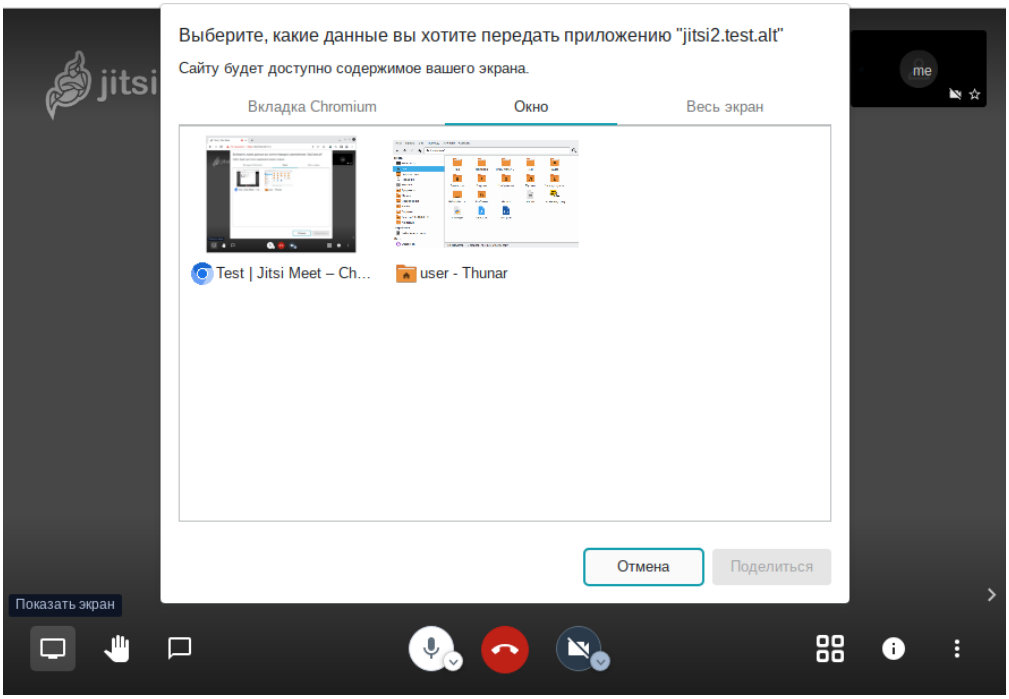


Рис. 184

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. 185).

Чат конференции Jitsi Meet

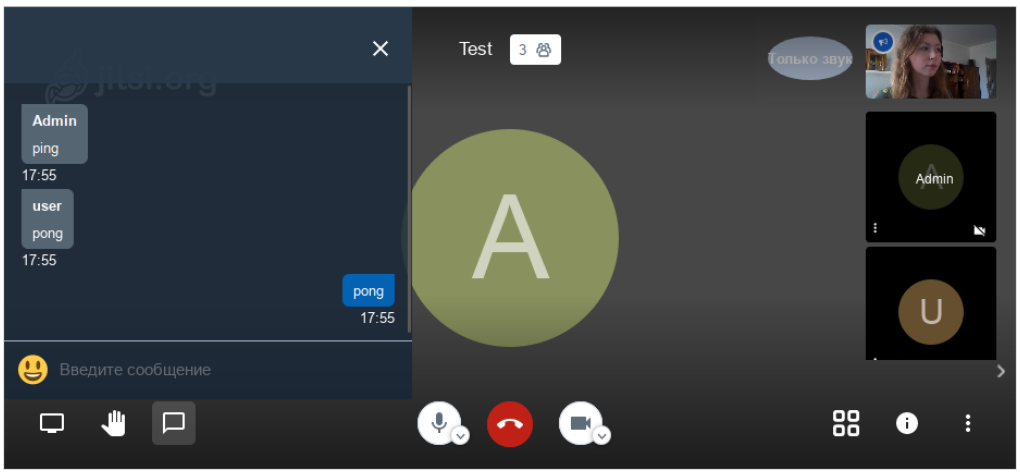


Рис. 185

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. 186);
- «Больше» – настройка дополнительных функций Jitsi Meet (Рис. 187).

Установка пароля для доступа к конференции

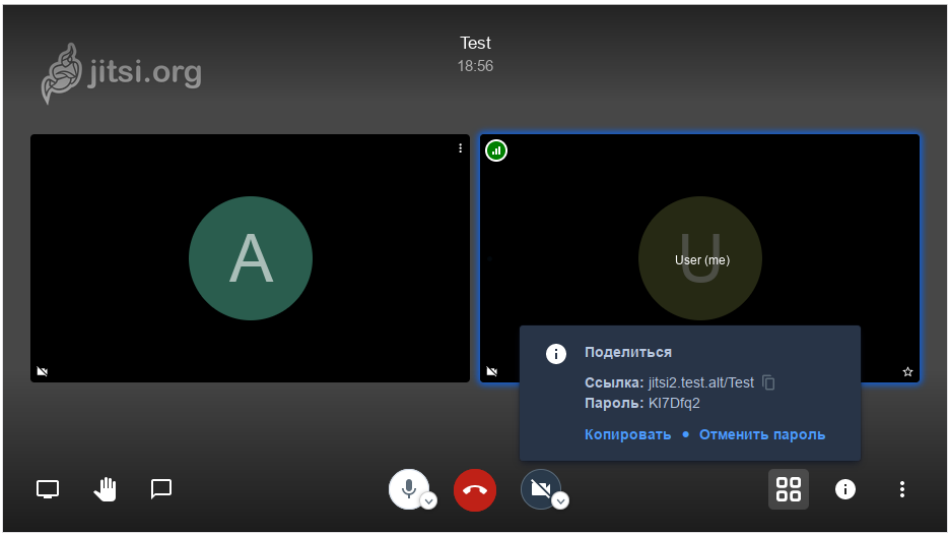


Рис. 186

Установка дополнительных функций Jitsi Meet

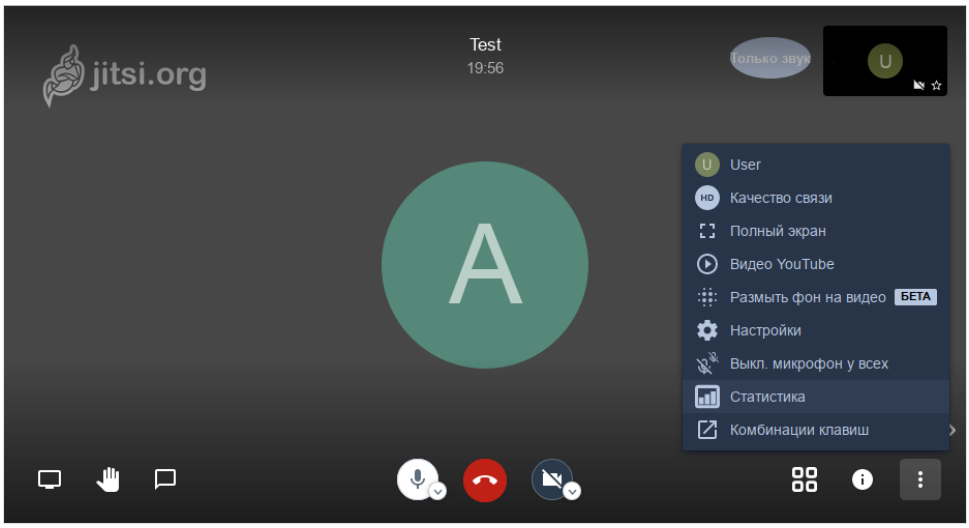


Рис. 187

5.9.5 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:

```
# prosodyctl 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. 188).

Запрос пароля при создании конференции

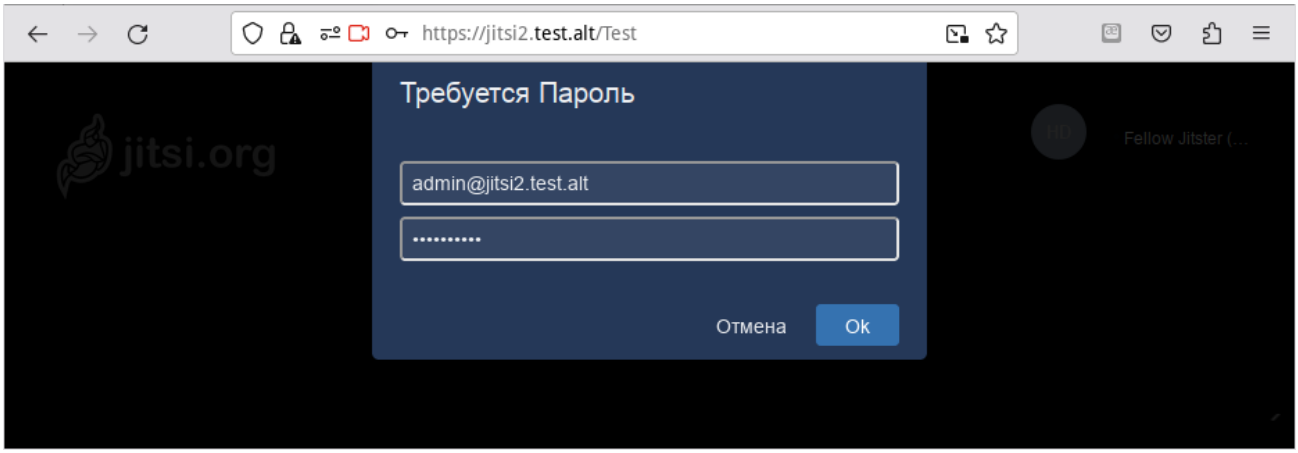


Рис. 188

5.10 Отказоустойчивый кластер (High Availability) на основе Pacemaker

Pacemaker – менеджер ресурсов кластера (Cluster Resource Manager), задачей которого является достижение максимальной доступности управляемых им ресурсов и защита их от сбоев, как на уровне самих ресурсов, так и на уровне целых узлов кластера.

Ключевые особенности Pacemaker:

- обнаружение и восстановление сбоев на уровне узлов и сервисов;
- возможность гарантировать целостность данных, путем ограждения неисправных узлов;
- поддержка одного или нескольких узлов на кластер;
- поддержка нескольких стандартов интерфейса ресурсов (все, что может быть написано сценарием, может быть кластеризовано);
- независимость от подсистемы хранения – общий диск не требуется;
- поддержка и кворумных и ресурсозависимых кластеров;
- автоматически реплицируемая конфигурация, которую можно обновлять с любого узла;
- возможность задания порядка запуска ресурсов, а также их совместимости на одном узле;
- поддерживает расширенные типы ресурсов: клоны (когда ресурс запущен на множестве узлов) и дополнительные состояния (master/slave и подобное);
- единые инструменты управления кластером с поддержкой сценариев.

Архитектура Pacemaker представляет собой три уровня:

- кластеронезависимый уровень – на этом уровне располагаются ресурсы и их скрипты, которыми они управляются и локальный демон, который скрывает от других уровней различия в стандартах, использованных в скриптах;

- менеджер ресурсов (Pacemaker) – реагирует на события, происходящие в кластере: отказ или присоединение узлов, ресурсов, переход узлов в сервисный режим и другие административные действия. Pacemaker, исходя из сложившейся ситуации, делает расчет наиболее оптимального состояния кластера и дает команды на выполнение действий для достижения этого состояния (остановка/перенос ресурсов или узлов);
- информационный уровень (Corosync) – на этом уровне осуществляется сетевое взаимодействие узлов, т.е. передача сервисных команд (запуск/остановка ресурсов, узлов и т.д.), обмен информацией о полноте состава кластера (quorum) и т.д.

Узел (node) кластера представляет собой физический сервер или виртуальную машину с установленным Pacemaker. Узлы, предназначенные для предоставления одинаковых сервисов, должны иметь одинаковую конфигурацию.

Ресурсы, с точки зрения кластера, это все используемые сущности – сервисы, службы, точки монтирования, тома и разделы. При создании ресурса потребуется задать его класс, тип, провайдера и собственно имя с дополнительными параметрами. Ресурсы поддерживают множество дополнительных параметров: привязку к узлу (resource-stickiness), роли по умолчанию (started, stoped, master) и т.д. Есть возможности по созданию групп ресурсов, клонов (работающих на нескольких узлах) и т.п.

Связи определяют привязку ресурсов к узлу (location), порядок запуска ресурсов (ordering) и совместное их проживание на узле (colocation).

5.10.1 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-адрес, по которому будет отвечать один из узлов.

Дальнейшие действия следует выполнить на всех узлах кластера.

Примечание. Рекомендуется использовать короткие имена узлов. Для изменения имени хоста без перезагрузки, можно воспользоваться утилитой `hostnamctl`:

```
# hostnamectl set-hostname node01
```

5.10.1.1 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
```

5.10.1.2 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
```

Примечание. После редактирования файла /etc/openssh/sshd_config следует перезапустить службу sshd:

```
# systemctl restart sshd
```

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
```

5.10.2 Установка кластерного ПО и создание кластера

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

Пакет pcs (pacemaker/corosync configuration system) – утилита для управления, настройки и мониторинга кластера. Управляется через командную строку.

Установить на всех узлах необходимые пакеты:

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

Примечание. Данные пакеты не входят в состав ISO-образа дистрибутива, их можно установить из репозитория p10. О добавлении репозиториев можно почитать в разделе «Добавление репозиториев».

Примечание. Пакет resource-agent – содержит агенты ресурсов (набор скриптов) кластера, соответствующие спецификации Open Cluster Framework (OCF), используемые для взаимодействия с различными службами в среде высокой доступности, управляемой менеджером ресурсов Pacemaker. Если есть необходимость управлять дополнительными ресурсами, следует установить недостающий пакет resource-agents-*:

```
$ apt-cache search resource-agents*
```

При установке Pacemaker автоматически будет создан пользователь hacluster. Для использования pcs 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:
 Status of pacemakerd: 'Pacemaker is running' (last updated 2023-09-27
16:59:12 +02:00)
 Cluster Summary:
   * Stack: corosync
   * Current DC: node01 (version 2.1.5-alt1-a3f44794f) - partition
with quorum
   * Last updated: Wed Sep 27 16:59:13 2023
   * Last change:  Wed Sep 27 16:59:09 2023 by hacluster via crmd on
node01
   * 3 nodes configured
   * 0 resource instances configured
 Node List:
   * Online: [ node01 node02 node03 ]

PCSD Status:
  node02: Online
```

```
  node01: 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
```

5.10.3 Настройка параметров кластера

Настройки кластера можно просмотреть, выполнив команду:

```
# pcs property
Cluster Properties:
 cluster-infrastructure: corosync
 cluster-name: newcluster
 dc-version: 2.1.5-alt1-a3f44794f
 have-watchdog: false
```

5.10.3.1 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.

Кластер, состоящий из двух узлов, будет иметь кворум только тогда, когда оба узла работают. По умолчанию, если нет кворума, Pacemaker останавливает ресурсы. Чтобы этого избежать, можно при настройке Pacemaker указать, что наличие или отсутствие кворума не должно учитываться:

```
# pcs property set no-quorum-policy=ignore
```

5.10.3.2 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.

Пока STONITH не настроен, его можно отключить, 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.

5.10.4 Настройка ресурсов

В данном разделе рассмотрена настройка ресурса, 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
```

Список доступных стандартов ресурсов:

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

Список доступных поставщиков сценариев ресурсов OCF:

```
# pcs resource providers
heartbeat
pacemaker
redhat
```

Список всех агентов ресурсов, доступных для определённого поставщика OCF:

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

```
…
zabbixserver
ZFS
```

Статус кластера, с добавленным ресурсом:

```
# pcs status
Cluster name: newcluster
Status of pacemakerd: 'Pacemaker is running' (last updated 2023-09-27
17:14:58 +02:00)
Cluster Summary:
  * Stack: corosync
  * Current DC: node01 (version 2.1.5-alt1-a3f44794f) - partition with
quorum
  * Last updated: Wed Sep 27 17:14:58 2023
  * Last change:  Wed Sep 27 17:14:46 2023 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 name: newcluster
```

```
Status of pacemakerd: 'Pacemaker is running' (last updated 2023-09-27
17:16:30 +02:00)
Cluster Summary:
  * Stack: corosync
  * Current DC: node02 (version 2.1.5-alt1-a3f44794f) - partition with
quorum
  * Last updated: Wed Sep 27 17:16:30 2023
  * Last change:  Wed Sep 27 17:14:46 2023 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
```

5.11 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 также 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. 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.

Системные требования для компонентов OpenUDS представлены в Таблица 1.

Примечание. Если сервер с базой данных установлен на той же машине, где и OpenUDS Server, требуемое количество памяти нужно просуммировать.

Таблица 1 – Системные требования

Компонент	ОЗУ	ЦП	Диск
SQL Server	1 ГБ	2 vCPUs	10 ГБ
OpenUDS Server	2 ГБ	2 vCPUs	8 ГБ
OpenUDS Tunnel	2 ГБ	2 vCPUs	13 ГБ

5.11.1 Установка

5.11.1.1 Установка MySQL (MariaDB)

Установить MySQL (MariaDB):

```
# apt-get install mariadb-server
```

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;
```

5.11.1.2 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
$ exit
```

- 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
```

Примечание. Перед запуском nginx необходимо остановить, если она запущена, службу apache2:

```
# systemctl disable --now httpd2
```

Веб-интерфейс OpenUDS (Рис. 189) будет доступен по адресу https://адрес-сервера/.

Форма входа в интерфейс OpenUDS

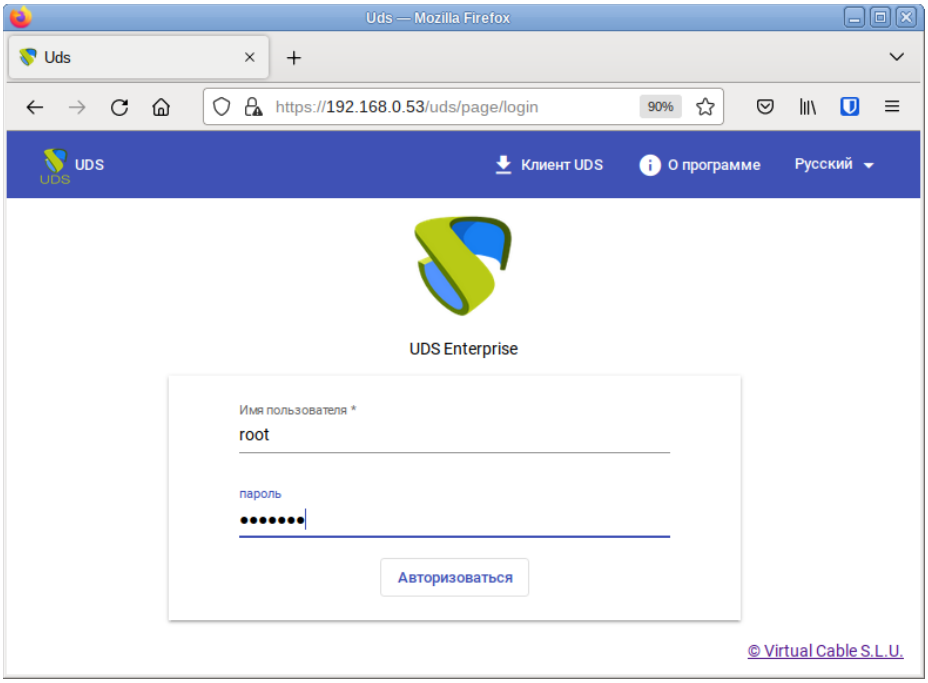


Рис. 189

Примечание. Имя/пароль по умолчанию: root/udsmam0

Примечание. Для получения доступа к панели администрирования OpenUDS, следует в меню пользователя выбрать пункт «Панель управления» (Рис. 190).

OpenUDS. Меню пользователя

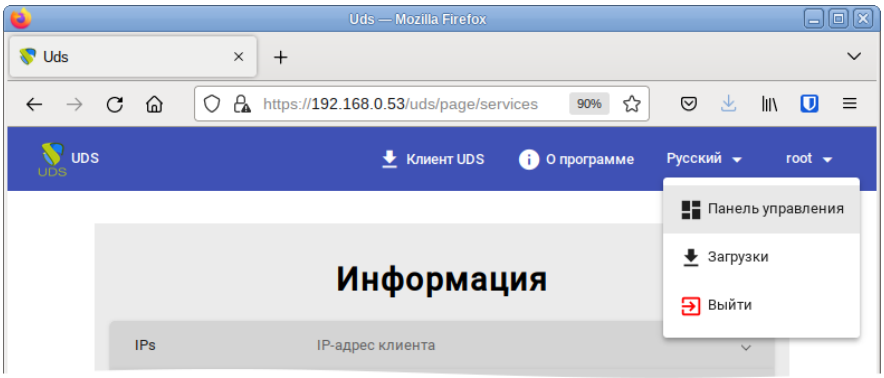


Рис. 190

5.11.1.3 OpenUDS Tunnel

5.11.1.3.1 Установка OpenUDS Tunnel

Установка OpenUDS Tunnel должна выполняться на отдельной от OpenUDS Server системе.

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

Примечание. В уже установленной системе можно установить пакет `openuds-tunnel`:

```
# apt-get install openuds-tunnel
```

Примечание. При установке openuds-tunnel в `/etc/openuds-tunnel/ssl` генерируются сертификаты. Их можно заменить на свои, выпущенные внутри организации или Удостоверяющим Центром.

5.11.1.3.2 Настройка OpenUDS Tunnel

На OpenUDS Tunnel:

- указать адрес сервера OpenUDS (брокера) в файле `/etc/openuds-tunnel/udstunnel.conf`:

```
uds_server = http://192.168.0.53/uds/rest/tunnel/ticket
uds_token = 5ba9d52bb381196c2a22e495ff1c9ba4bdc03440b726aa8b
```

где 192.168.0.53 – адрес OpenUDS сервера (брокера);

- запустить и добавить в автозагрузку сервис OpenUDS Tunnel:

```
# systemctl enable --now openuds-tunnel.service
```

На сервере OpenUDS зарегистрировать туннельный сервер, выполнив команду:

```
# openuds_tunnel_register.py -H 192.168.0.88 -n Tunnel -t
5ba9d52bb381196c2a22e495ff1c9ba4bdc03440b726aa8b
Tunnel token register success. (With token:
5ba9d52bb381196c2a22e495ff1c9ba4bdc03440b726aa8b)
```

где:

- -H – задаёт IP-адрес туннельного сервера;
- -n – задаёт название туннеля;
- -t – позволяет указать токен туннельного сервера (из файла udstunnel.conf).

При создании туннельного транспорта, на вкладке «Туннель» указать IP-адрес и порт туннельного-сервера: `192.168.0.88:7777`.

5.11.1.3.3 Настройка HTML5

На OpenUDS Tunnel:

- в файле `/etc/guacamole/guacamole.properties` привести значение параметра `uds-base-url` к виду:

```
http://<IP openuds сервера>/uds/guacamole/auth/<Токен из файла udstunnel.conf>/
```

Например:

```
uds-base-url=http://192.168.0.53/uds/guacamole/
auth/5ba9d52bb381196c2a22e495ff1c9ba4bdc03440b726aa8b
```

- настроить tomcat:

  Для подключения по http: так как tomcat по умолчанию работает на порту 8080, то перед запуском tomcat необходимо, либо остановить службу `ahttpd`:

```
# systemctl disable --now ahttpd
```

  Либо изменить в файле `/etc/tomcat/server.xml` порт 8080 на другой допустимый номер порта, например, 8081:

```
<Connector port="8081" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
```

  Для подключения по https: в файл `/etc/tomcat/server.xml` добавить новый Connector, в котором указать порт (в примере 10443), сертификат (файл .crt, .pem и т.д.), закрытый ключ (.key, .pem и т.д.):

```
<Connector port="10443" protocol="org.apache.coyote.http11.Http11AprProtocol"
SSLEnabled="true"
           ciphers="A-CHACHA20-POLY1305,ECDHE-RSA-CHACHA20-POLY1305,ECDHE-ECDSA-
AES128-GCM-SHA256,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-
RSA-AES256-GCM-SHA384,DHE-RSA-AES128-GCM-SHA256,DHE-RSA-AES256-GCM-SHA384,ECDHE-
ECDSA-AES128-SHA256,ECDHE-RSA-AES128-SHA256,ECDHE-ECDSA-AES128-SHA,ECDHE-RSA-AES256-
SHA384,
ECDHE-RSA-AES128-SHA,ECDHE-ECDSA-AES256-SHA384,ECDHE-ECDSA-AES256-SHA,ECDHE-RSA-
AES256-SHA,DHE-RSA-AES128-SHA256,DHE-RSA-AES128-SHA,DHE-RSA-AES256-SHA256,DHE-RSA-
AES256-SHA,ECDHE-ECDSA-DES-CBC3-SHA,ECDHE-RSA-DES-CBC3-SHA,EDH-RSA-DES-CBC3-
SHA,AES128-GCM-SHA256,AES256-GCM-SHA384,
AES128-SHA256,AES256-SHA256,AES128-SHA,AES256-SHA,DES-CBC3-SHA"
           maxThreads="500" scheme="https" secure="true"
           SSLCertificateFile="/etc/openuds-tunnel/ssl/certs/openuds-tunnel.pem"
           SSLCertificateKeyFile="/etc/openuds-tunnel/ssl/private/openuds-tunnel.key"
           maxKeepAliveRequests="1000"
           clientAuth="false" sslProtocol="TLSv1+TLSv1.1+TLSv1.2" />
```

- запустить сервисы guacd и tomcat:

```
# systemctl enable --now guacd tomcat
```

На сервере OpenUDS при создании нового туннельного транспорта HTML5RDP на вкладке «Туннель» указать IP-адрес и порт туннельного-сервера:

- http://192.168.0.88:8080 – для подключения по http;
- https://192.168.0.88:10443 – для подключения по https.

5.11.2 Обновление OpenUDS

После обновления `openuds-server` до новой версии необходимо выполнить следующие действия:

- перенести изменения, если они есть, из нового конфигурационного файла `/etc/openuds/settings.py.rpmnew` в файл `/etc/openuds/settings.py`. Проверить, что изменилось можно, выполнив команду:

```
# diff -u --color /etc/openuds/settings.py /etc/openuds/settings.py.rpmnew
```

- выполнить миграцию базы данных:

```
# su -s /bin/bash - openuds -c "cd /usr/share/openuds; python3 manage.py migrate"
```

- перезагрузить систему, так как при обновлении не создаётся файл `/run/openuds/socket`.

5.11.3 Настройка OpenUDS

5.11.3.1 Поставщики услуг

В разделе «Поставщики услуг» (Рис. 191) подключить один из поставщиков («Service providers»):

- «Поставщик платформы Proxmox»;
- «Поставщик платформы OpenNebula»;
- Отдельный сервер без виртуализации: «Поставщик машин статических IP».

OpenUDS. Поставщики услуг

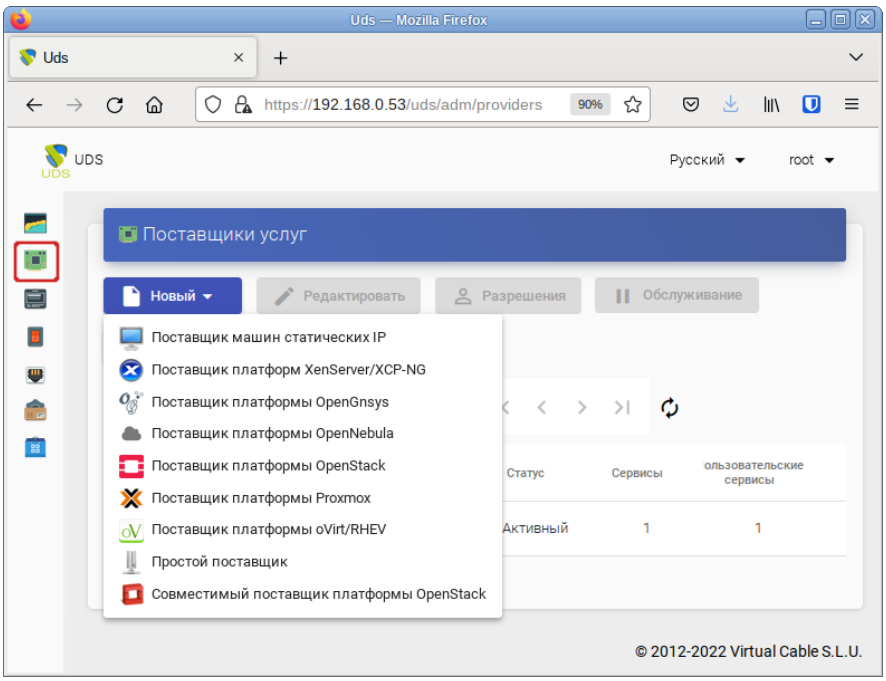


Рис. 191

5.11.3.1.1 OpenNebula

Минимальные параметры для настройки «Поставщик платформы OpenNebula»:

- вкладка «Основной» (Рис. 192):
  - «Имя» – название поставщика;
  - «Хост» – IP-адрес сервера OpenNebula;
  - «Порт» – порт подключения;
  - «Имя пользователя» – имя пользователя OpenNebula (с правами администратора);
  - «Пароль» – пароль пользователя;
- вкладка «Расширенный» (Рис. 193):
  - «Одновременное создание» – максимальное количество одновременно создаваемых ВМ;
  - «Одновременное удаление» – максимальное количество одновременно удаляемых ВМ;
  - «Таймаут» – таймаут подключения к OpenNebula в секундах.

Используя кнопку «Проверить», можно убедиться, что соединение установлено правильно.

После интеграции платформы OpenNebula в OpenUDS необходимо создать базовую службу типа «Действующие образы OpenNebula». Для этого дважды щелкнуть мышью по строке созданного поставщика услуг или в контекстном меню поставщика выбрать пункт «Подробность» (Рис. 194).

OpenUDS. Подключение системы виртуализации OpenNebula

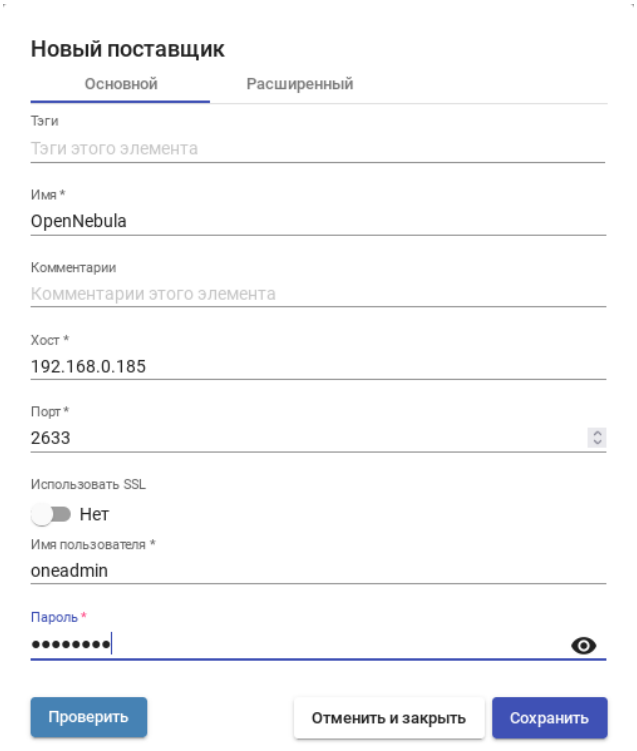


Рис. 192

OpenUDS. Подключение системы виртуализации OpenNebula

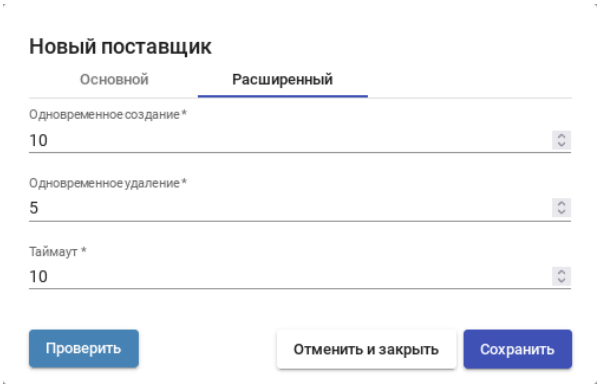


Рис. 193

OpenUDS. Контекстное меню «Service providers»

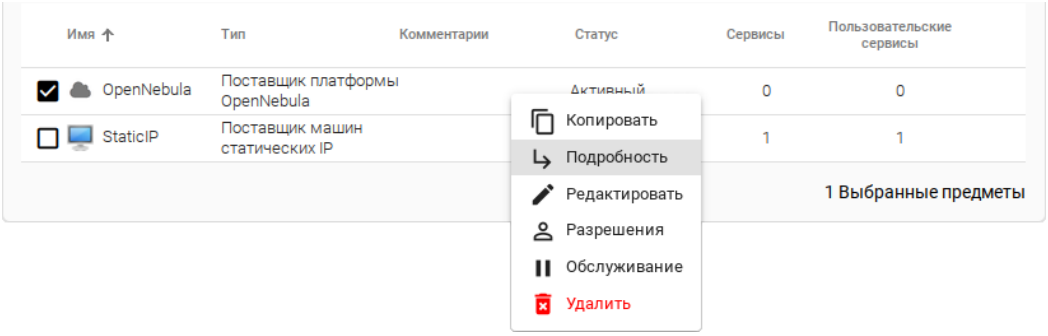


Рис. 194

Примечание. Выбрав пункт «Обслуживание», 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.

В открывшемся окне, на вкладке «Постащики услуг» нажать кнопку «Новый» → «Действующие образы OpenNebula» (Рис. 195).

OpenUDS. Создание новой услуги «Действующие образы OpenNebula»

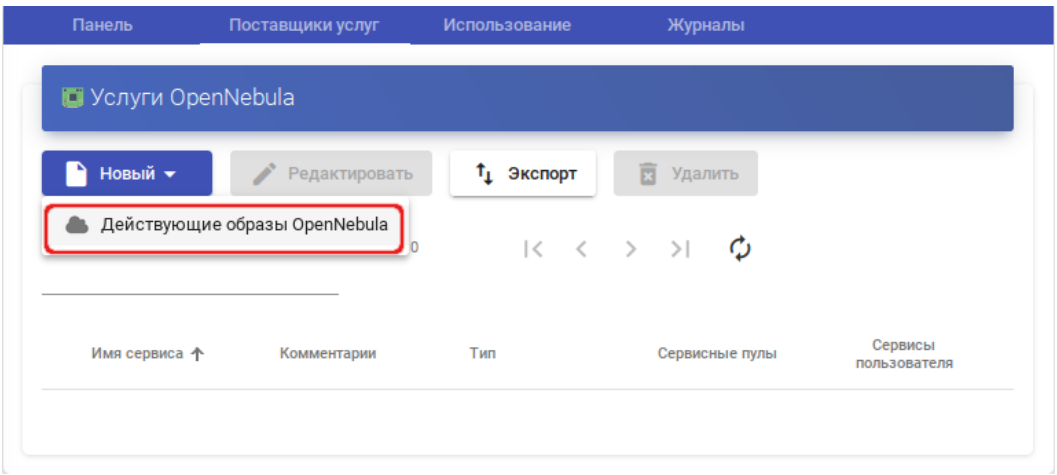


Рис. 195

Заполнить минимальные параметры конфигурации:

- вкладка «Основной» (Рис. 196):
  - «Имя» – название службы;
  - «Хранилище» – место, где будут храниться сгенерированные виртуальные рабочие столы;
- вкладка «Машина» (Рис. 197):
  - «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 «Основной»

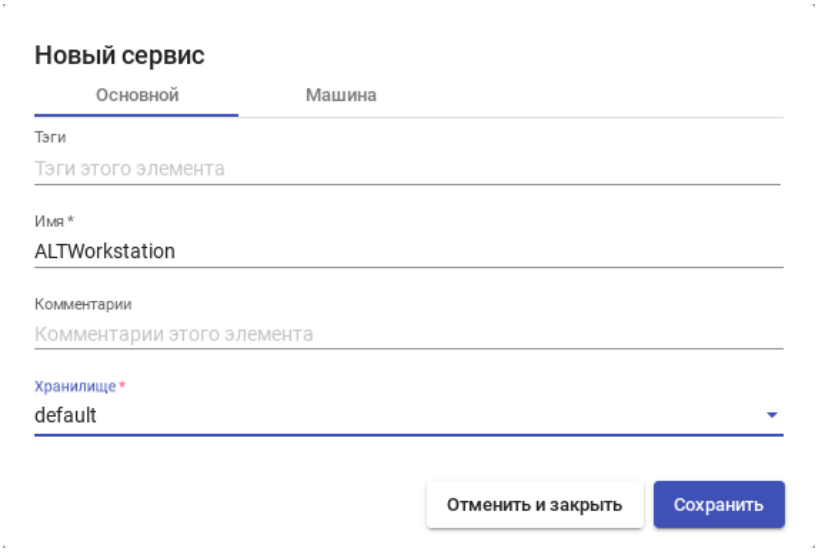


Рис. 196

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

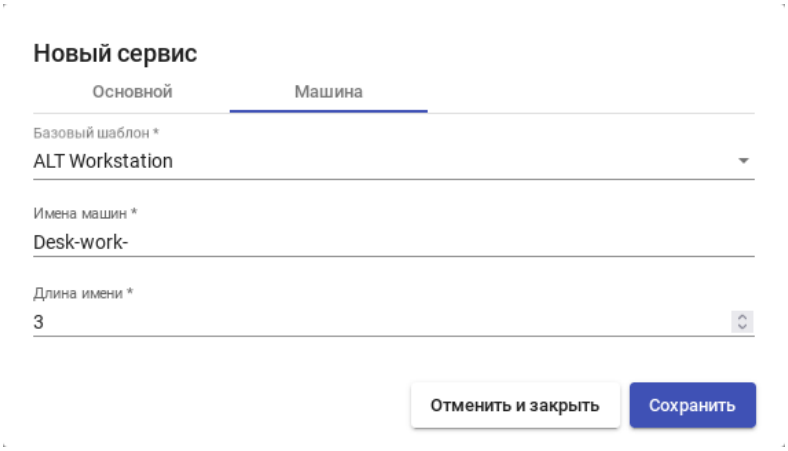


Рис. 197

5.11.3.1.2 PVE

Минимальные параметры для настройки «Поставщик платформы Proxmox»:

- вкладка «Основной» (Рис. 198):
  - «Имя» – название поставщика;
  - «Хост» – IP-адрес/имя сервера или кластера PVE;
  - «Порт» – порт подключения;
  - «Имя пользователя» – имя пользователя с достаточными привилегиями в PVE (в формате пользователь@аутентификатор);
  - «Пароль» – пароль пользователя;
- вкладка «Расширенный» (Рис. 199):
  - «Одновременное создание» – максимальное количество одновременно создаваемых ВМ;
  - «Одновременное удаление» – максимальное количество одновременно удаляемых ВМ;
  - «Таймаут» – таймаут подключения к Proxmox в секундах;
  - «Начальный VmID» – идентификатор ВМ, с которым OpenUDS начнет генерировать ВМ на Proxmox (>=10000);
  - «Таймаут» – диапазон MAC-адресов, которые будут использоваться рабочими столами.

OpenUDS. Подключение системы виртуализации PVE

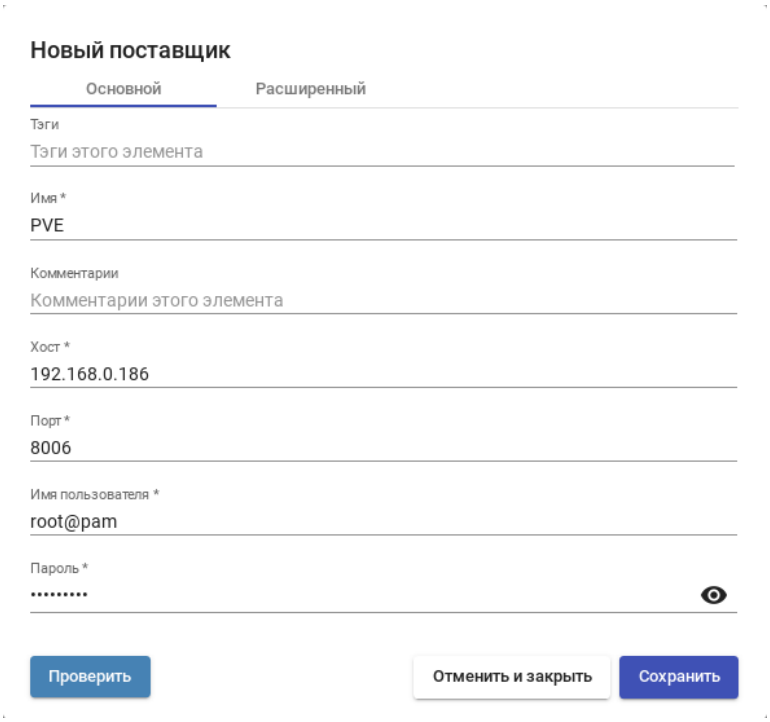


Рис. 198

OpenUDS. Подключение системы виртуализации PVE

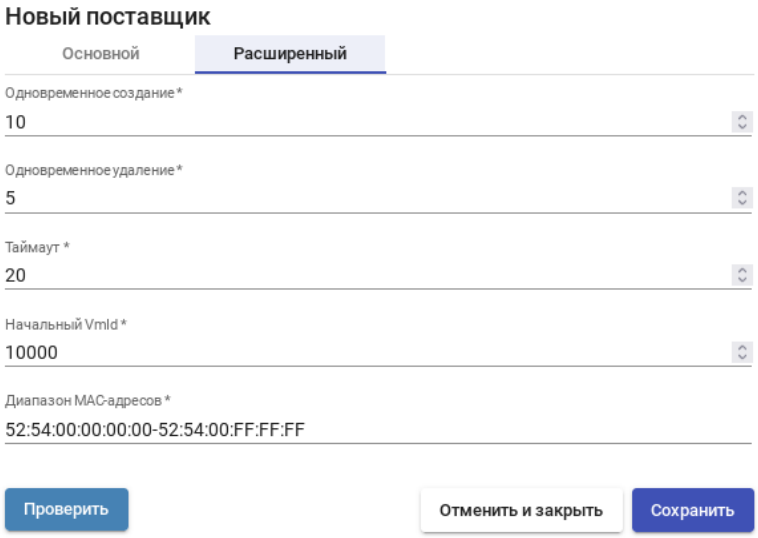


Рис. 199

Используя кнопку «Проверить», можно убедиться, что соединение установлено правильно.

После интеграции платформы PVE в OpenUDS необходимо создать базовую службу типа «Связанный клон Proxmox». Для этого дважды щелкнуть мышью по строке созданного поставщика услуг или в контекстном меню поставщика выбрать пункт «Подробность» (Рис. 200).

Примечание. Выбрав пункт «Обслуживание», 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. Контекстное меню поставщика услуг PVE

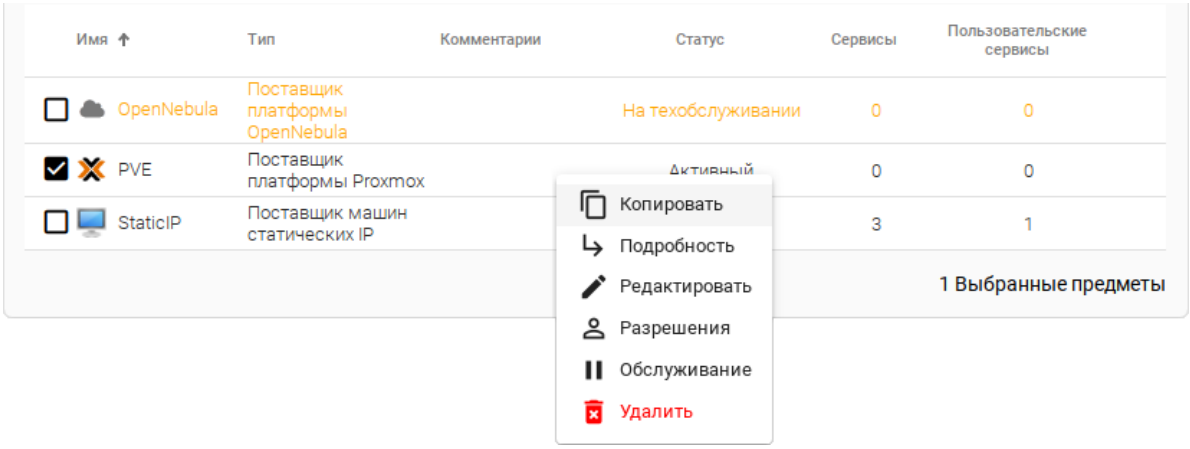


Рис. 200

В открывшемся окне, на вкладке «Постащики услуг» нажать кнопку «Новый» → «Связанный клон Proxmox» (Рис. 201).

OpenUDS. Создание новой услуги «Связанный клон Proxmox»

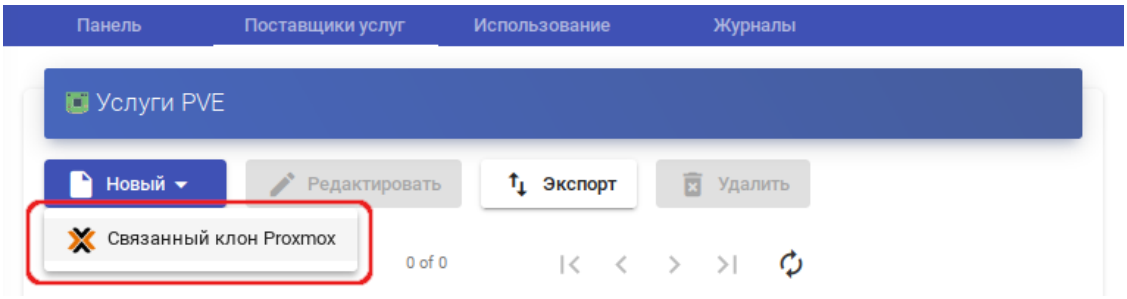


Рис. 201

Заполнить параметры конфигурации:

- Вкладка «Основной» (Рис. 202):
  - «Имя» – название службы;
  - «Пул» – пул, в котором будут находиться ВМ, созданные OpenUDS;
  - «Высокая доступность» – включать созданные ВМ в группу HA PVE;
  - «Сначала попробовать SOFT Shutdown» – если активно, OpenUDS попытается, перед уничтожением автоматически сгенерированного виртуального рабочего стола, выполнить контролируемое отключение машины;
- Вкладка «Машина» (Рис. 203):
  - «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-SL-);
  - «Длина имени» – количество цифр счетчика, прикрепленного к базовому имени рабочих столов (например, если «Длина имени» = 3, названия сгенерированных рабочих столов будут: Desk-SL-000, Desk-SL-001 ... Desk-SL-999).

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

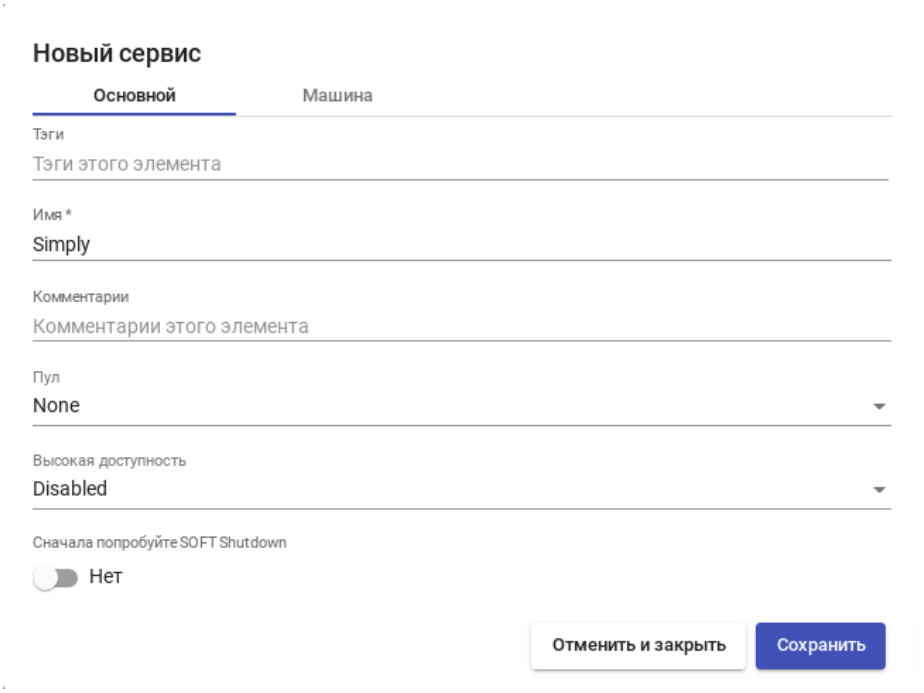


Рис. 202

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

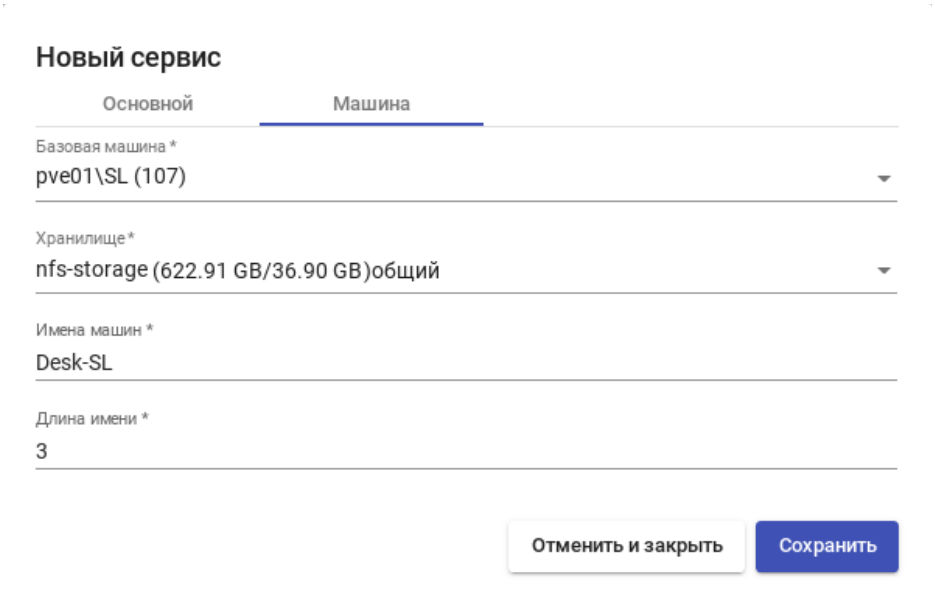


Рис. 203

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. 204).

PVE. Созданные шаблоны и рабочие столы

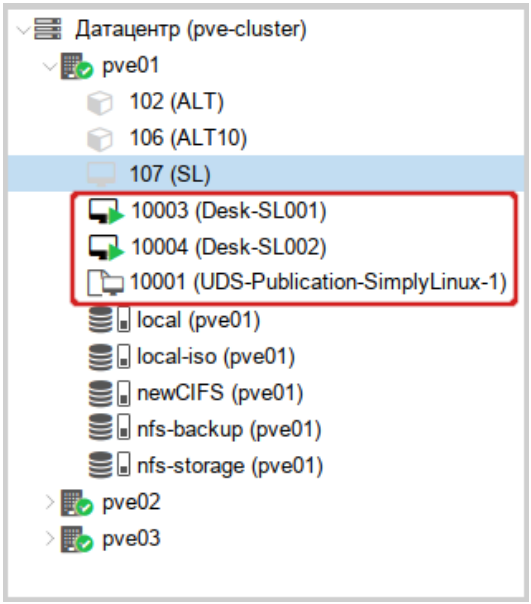


Рис. 204

5.11.3.1.3 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 «Поставщики услуг» нажать кнопку «Новый» и выбрать пункт «Поставщик машин статических IP».

Для настройки «Поставщика машин статических IP» достаточно задать название поставщика (Рис. 205).

OpenUDS. Подключение к серверу без виртуализации

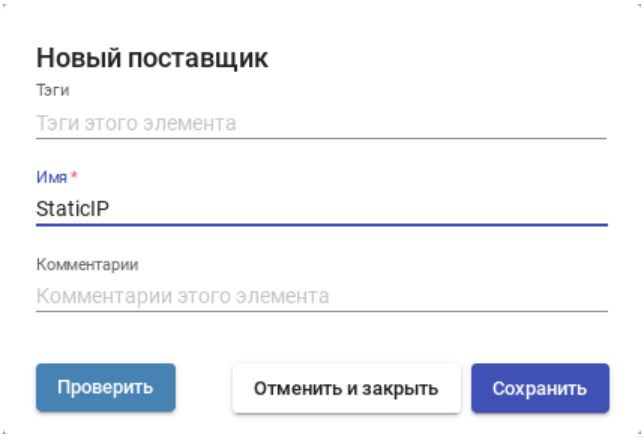


Рис. 205

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».

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). Можно также 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 сервисы» нажать кнопку «Назначить услугу» и задать привязку пользователя устройству (Рис. 206).

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

Для создания новой услуги типа «Поставщик машин статических IP» следует, на вкладке «Поставщики услуг» нажать кнопку «Новый» → «Статический множественный IP-адрес» или «Новый» → «Статический одиночный IP-адрес» (Рис. 207).

OpenUDS. Привязка пользователю устройству

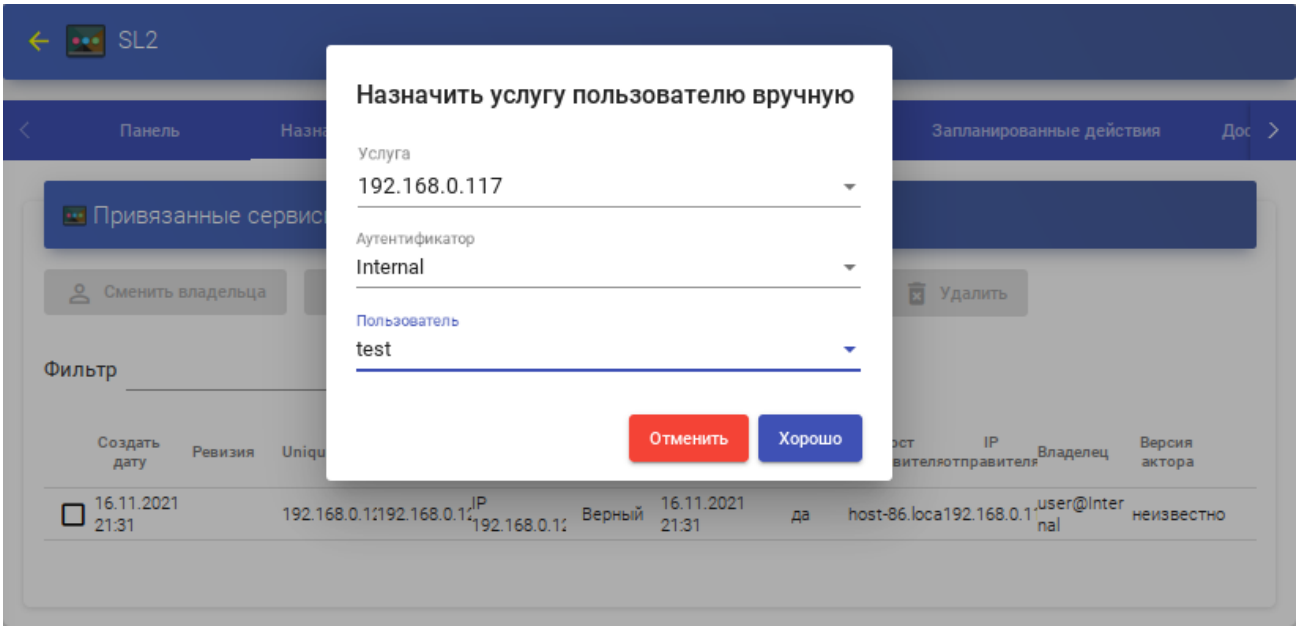


Рис. 206

OpenUDS. Создание новой услуги «Статический IP-адрес»

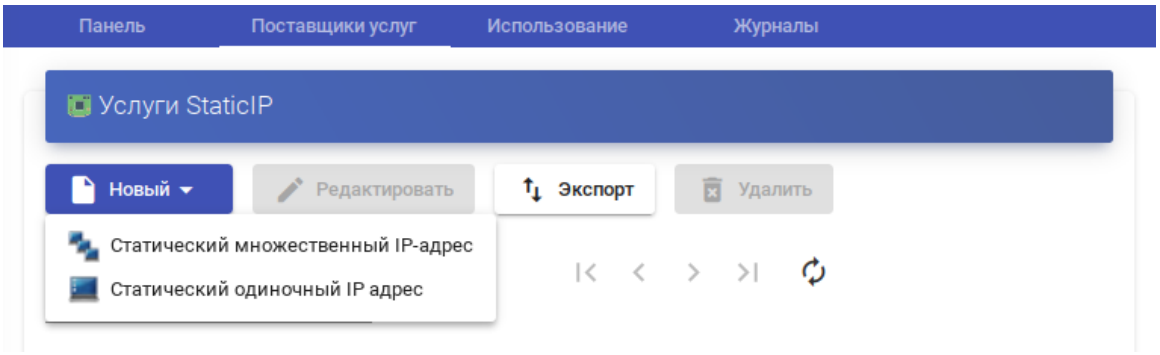


Рис. 207

Параметры конфигурации для услуги «Статический множественный IP-адрес»:

- Вкладка «Основной» (Рис. 208):
  - «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»);
  - «Ключ услуги» – токен, который будет использоваться клиентами для связи с сервисом. Если в этом поле не указан токен (пусто), система не будет контролировать сеансы пользователей на компьютерах. Таким образом, когда компьютер назначается пользователю, это назначение будет сохраняться до тех пор, пока администратор не удалит его вручную. При наличии токена сеансы пользователей будут контролироваться (при выходе из сеанса, компьютеры снова становятся доступными для доступа других пользователей). Если токен указан, необходимо, чтобы на компьютерах (IP-адрес, которых указан в поле «Список серверов») был установлен Unmanaged UDS Actor.
- Вкладка «Расширенный» (Рис. 209):
  - «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 течение которого не будет проверяться доступность недоступной машины;
  - «Максимальное количество сеансов на машину» – максимальная продолжительность сеанса (в часах), прежде чем OpenUDS решит, что эта машина заблокирована и освободит её (0 означает «никогда»).

OpenUDS. Создание службы типа «Static Multiple IP»

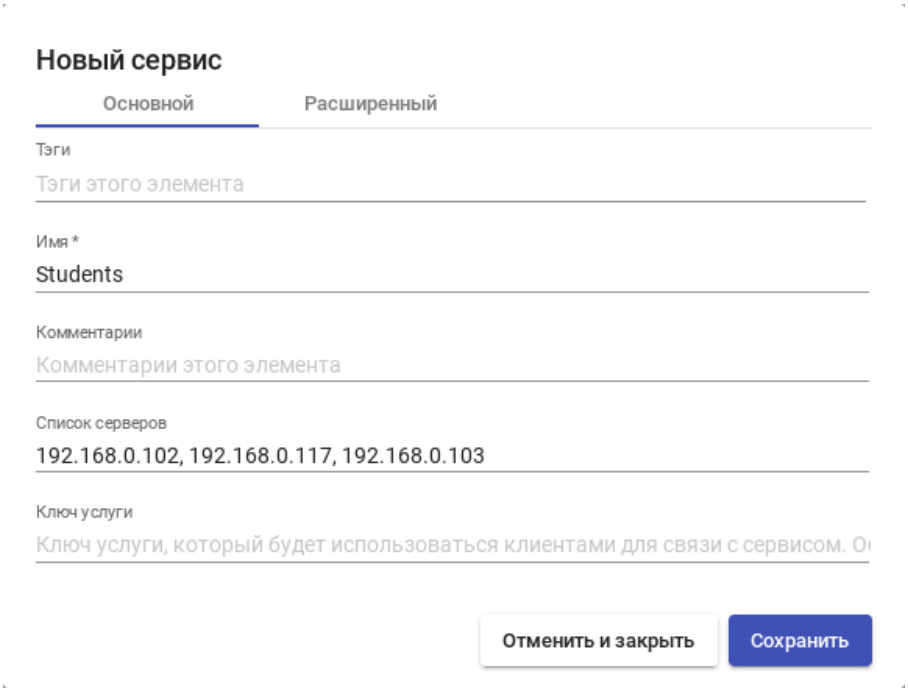


Рис. 208

OpenUDS. Создание службы типа «Static Multiple IP»

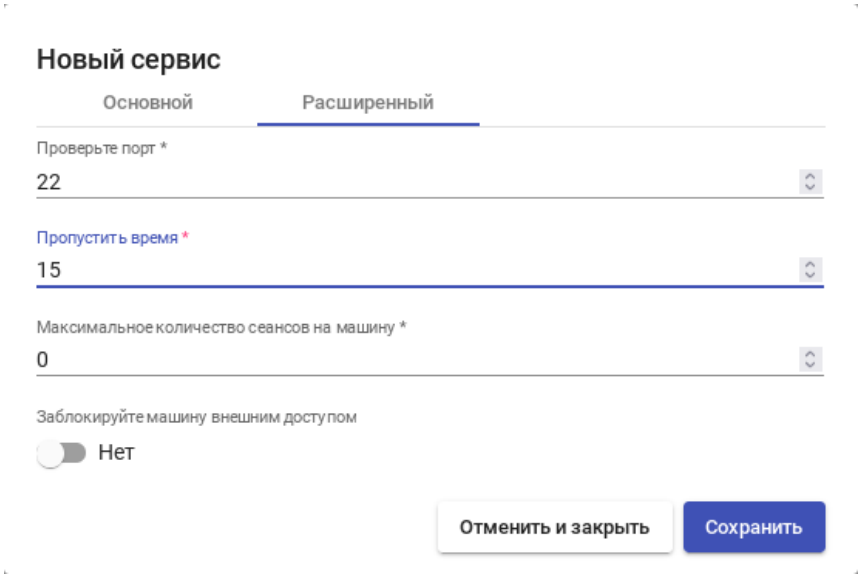


Рис. 209

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 сервисы» (Рис. 210).

OpenUDS. Привязанные сервисы службы «Static Multiple IP»

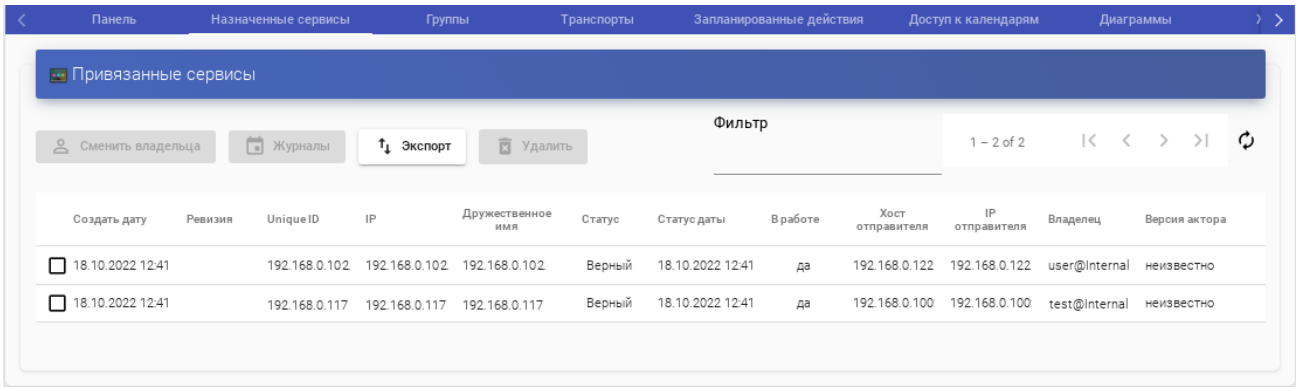


Рис. 210

Параметры конфигурации для услуги «Статический одиночный IP-адрес» (Рис. 211):

- «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»

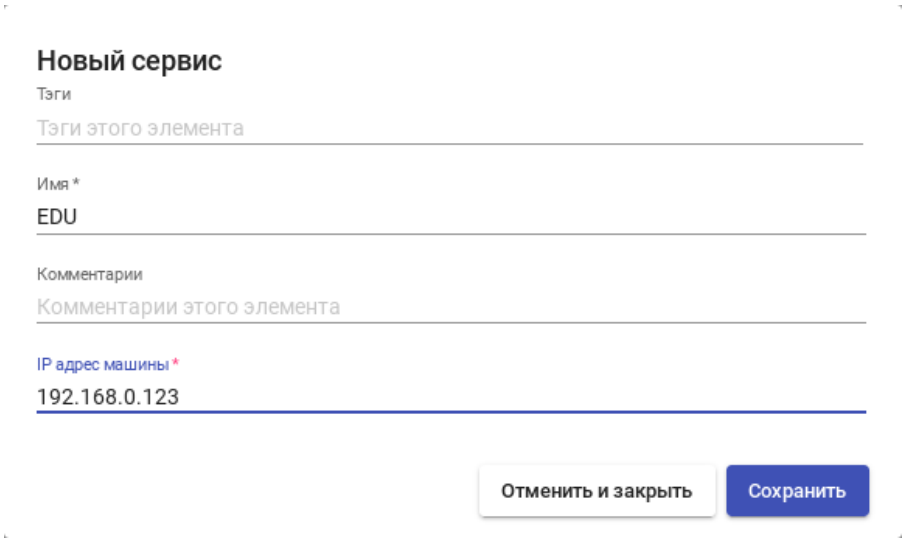


Рис. 211

5.11.3.2 Настройка аутентификации пользователей

Аутентификатор проверяет подлинность пользователей и предоставляет пользователям и группам пользователей разрешения на подключение к различным виртуальным рабочим столам.

Аутентификатор не является обязательным компонентом для создания «пула услуг», но если не создан хотя бы один аутентификатор, не будет пользователей, которые смогут подключаться к службам на платформе OpenUDS.

Примечание. Если в системе зарегистрировано более одного аутентификатора, и они не отключены, на экран входа будет добавлено поле «Аутентификатор» с раскрывающимся списком.

В этом списке можно выбрать аутентификатор, который система будет использовать для проверки пользователя (Рис. 212).

OpenUDS. Выбор типа аутентификации пользователей

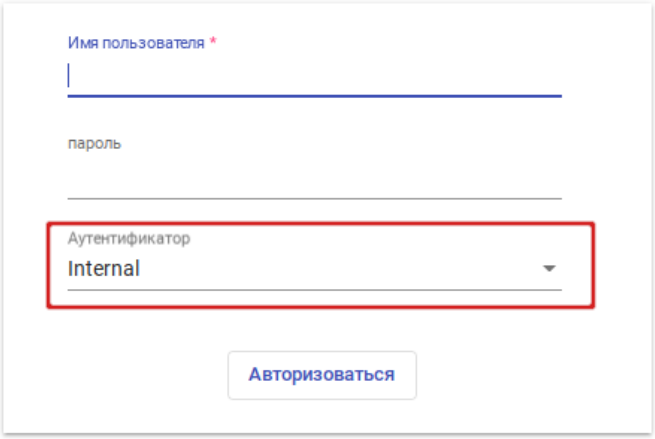


Рис. 212

Примечание. При создании любого аутентификатора заполняется поле «Метка». Пользователь может пройти проверку подлинности с помощью указанного аутентификатора, даже если в среде OpenUDS настроено несколько аутентификаторов. Для этого нужно получить доступ к экрану входа OpenUDS в формате: OpenUDS-server/uds/page/login/метка (например, https://192.168.0.53/uds/page/login/AD).

Для настройки аутентификации в разделе «Аутентификаторы» необходимо выбрать тип аутентификации пользователей (Рис. 213). Можно выбрать как внешние источники (Active Directory, OpenLDAP и т.д.), так и внутренние (внутренняя база данных, IP-аутентификация).

OpenUDS. Выбор типа аутентификации пользователей

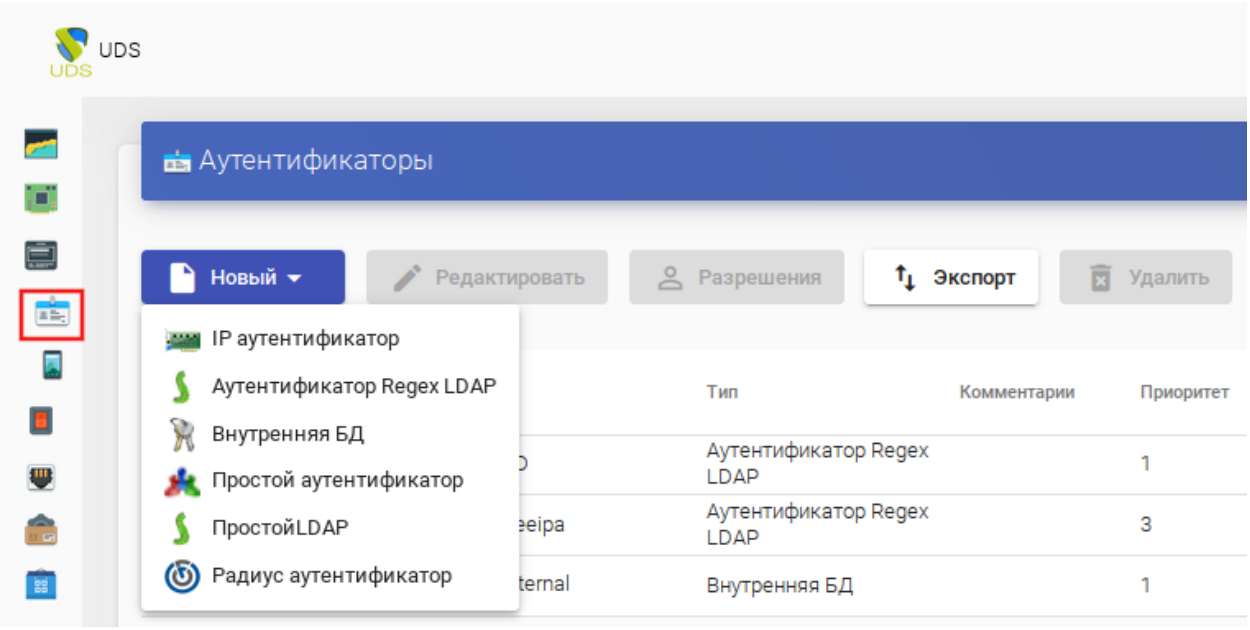


Рис. 213

5.11.3.2.1 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. 214).

OpenUDS. Внутренняя база данных

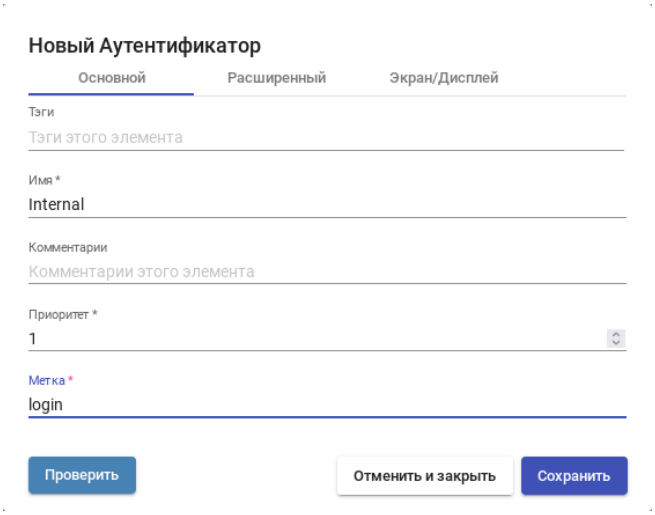


Рис. 214

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. 215).

OpenUDS. Внутренняя база данных – пользователи

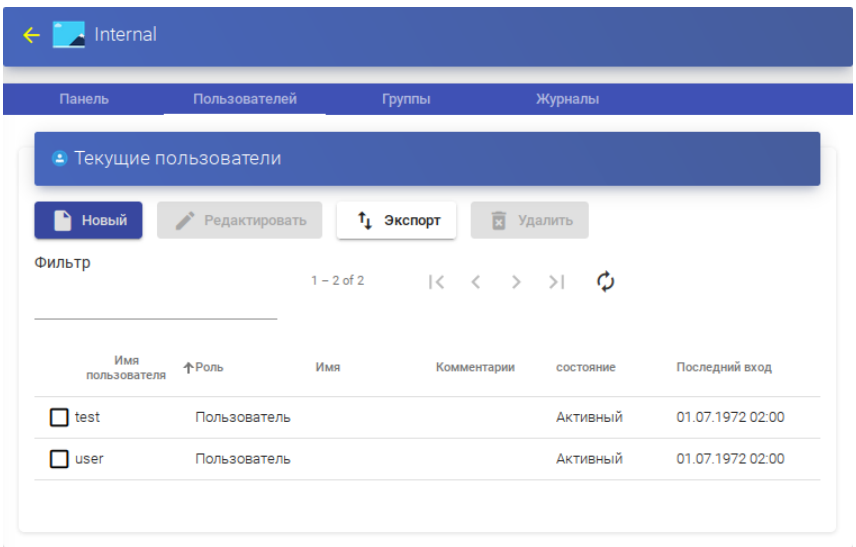


Рис. 215

5.11.3.2.2 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.

Пример настройки 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. 216): имя аутентификатора, приоритет, метка, IP-адрес FreeIPA-сервера, порт (обычно 389 без ssl, 636 с ssl);
- вкладка «Учётные данные» (Рис. 217): имя пользователя (в формате uid=user_freeipa,cn=users,cn=accounts,dc=example,dc=test) и пароль;
- вкладка «LDAP информация» (Рис. 218): общая база пользователей, класс пользователей LDAP, идентификатор атрибута пользователя, атрибут имени пользователя, атрибут имени группы.

OpenUDS. Интеграция с FreeIPA

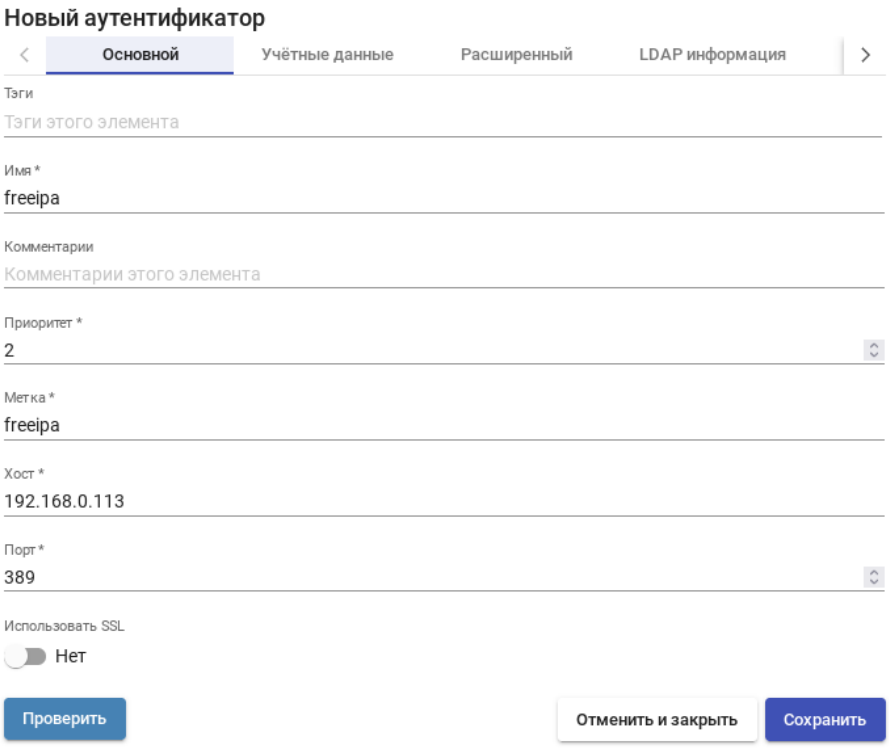


Рис. 216

OpenUDS. Интеграция с FreeIPA – учетные данные пользователя

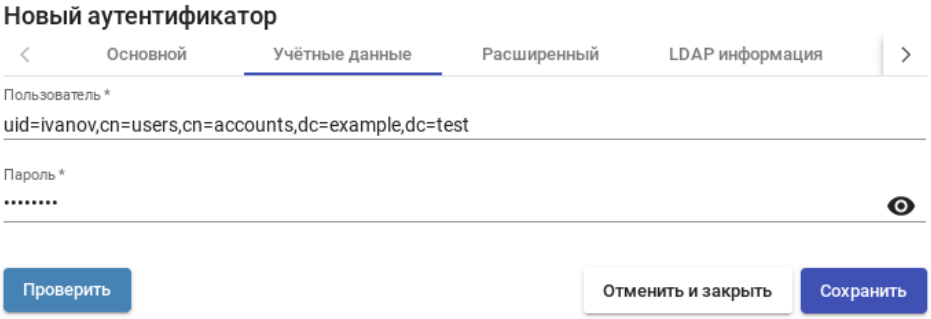


Рис. 217

OpenUDS. Интеграция с FreeIP – LDAP информация

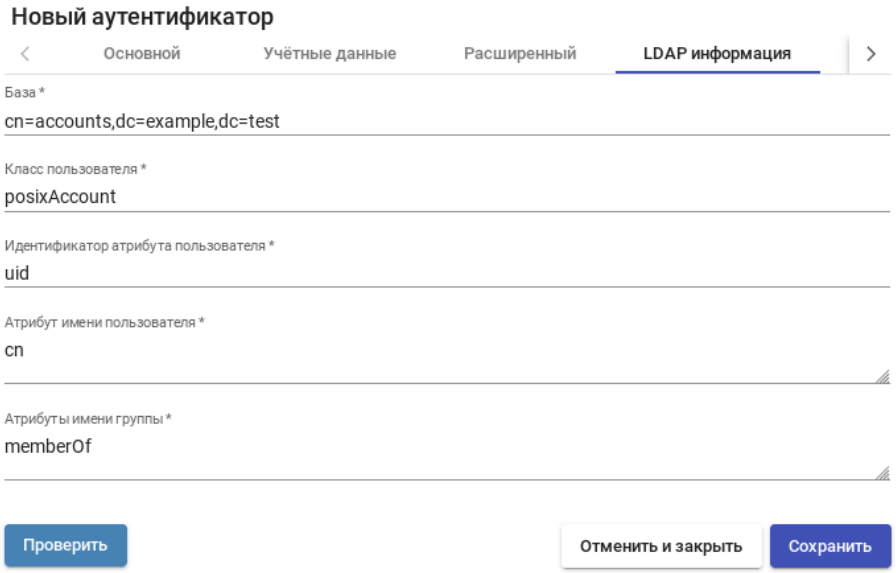


Рис. 218

Примечание. Используя кнопку «Проверить», можно проверить соединение с FreeIPA-сервером.

3. Добавить группу LDAP, в которую входят пользователи. Для этого следует выбрать созданный аутентификатор («freeipa»), затем в открывшемся окне на 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. 219).

OpenUDS. Интеграция с FreeIPA – добавление группы LDAP

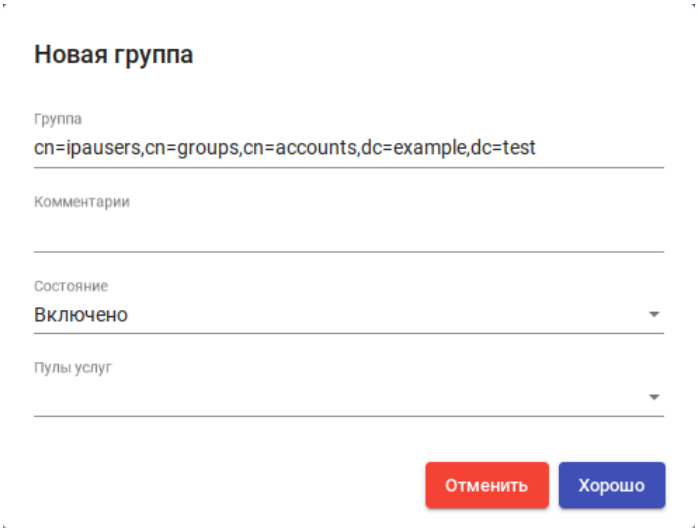


Рис. 219

Пример настройки 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. 220): имя аутентификатора, приоритет, метка, IP-адрес сервера AD, порт (обычно 389 без ssl, 636 с ssl);
- вкладка «Учётные данные» (Рис. 221): имя пользователя (можно указать в виде имя@домен) и пароль;
- вкладка «LDAP информация» (Рис. 222): общая база пользователей, класс пользователей LDAP, идентификатор атрибута пользователя, атрибут имени пользователя, атрибут имени группы.

Примечание. Если в поле «Идентификатор атрибута пользователя» указано userPrincipalName, то пользователь при входе должен указать логин в формате имя_пользователя@домен, если указано sAMAccountName, то в качестве логина используется имя_пользователя без указания домена.

Примечание. Используя кнопку «Проверить», можно проверить соединение с Active Directory.

3. Добавить группу LDAP, в которую входят пользователи. Для этого следует выбрать созданный аутентификатор, затем в открывшемся окне на вкладке «Группы» нажать «Новый» → «Группа».
4. Заполнить dn существующей группы (например, cn=UDS,cn=Users,dc=test,dc=alt), можно также указать разрешённые пулы (Рис. 223).

OpenUDS. Интеграция с Active Directory

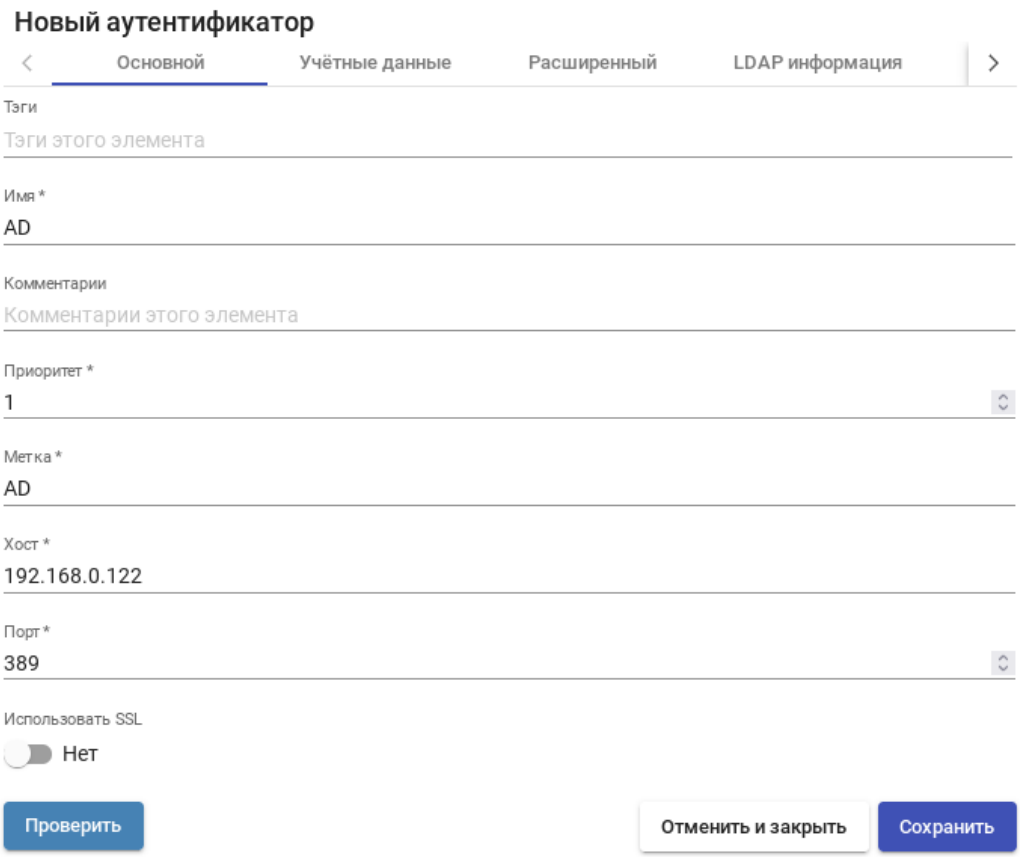


Рис. 220

OpenUDS. Интеграция с Active Directory – учетные данные пользователя

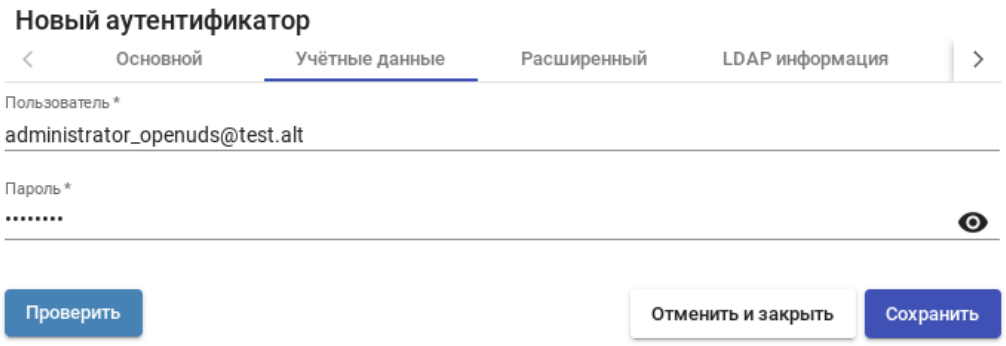


Рис. 221

OpenUDS. Интеграция с Active Directory – LDAP информация

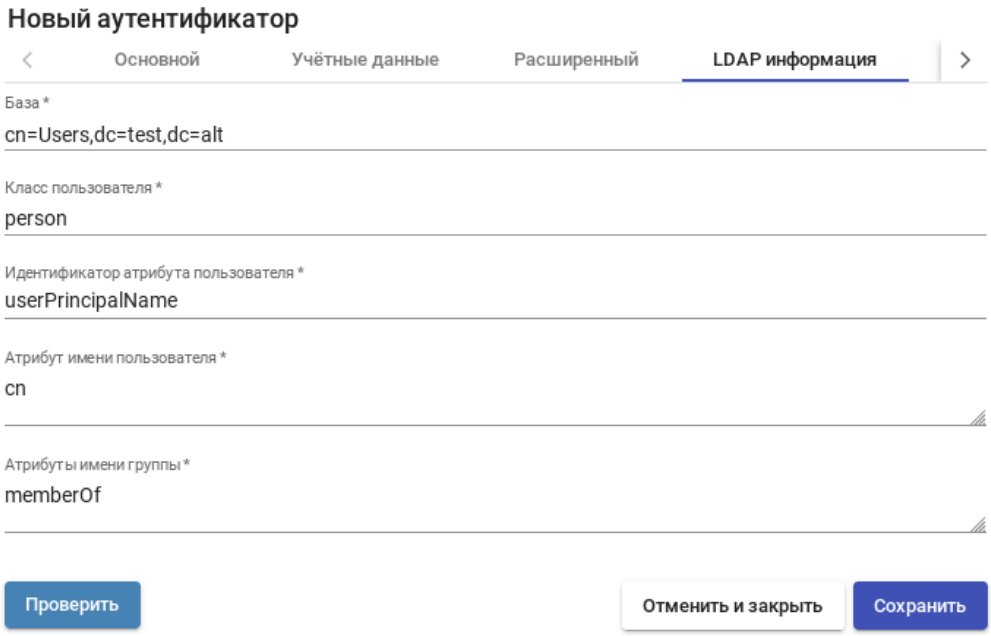


Рис. 222

OpenUDS. Интеграция с Active Directory – добавление группы LDAP

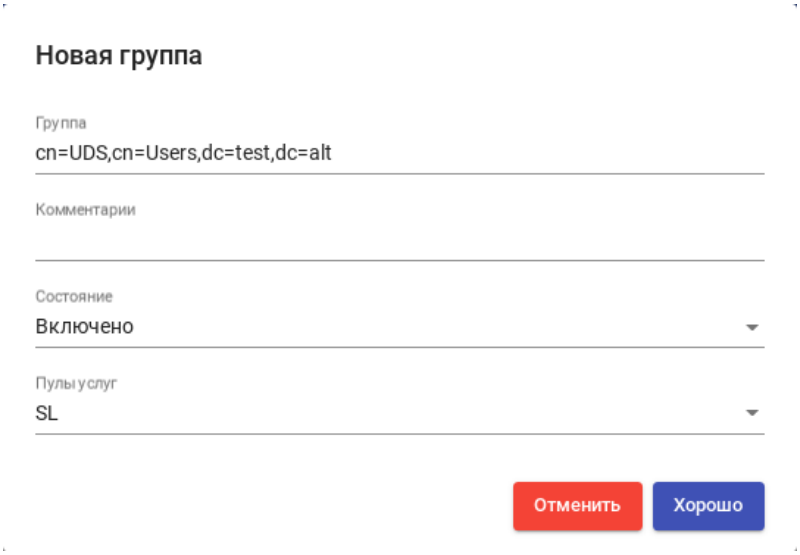


Рис. 223

На вкладке «Пользователи» аутентификатора (Рис. 224) пользователи будут добавляться автоматически после первого входа в систему OpenUDS (пользователи должны входить в группы, указанные в аутентификаторе на вкладке «Группа»).

Пользователя, чтобы назначить ему специальные права перед первым подключением, можно зарегистрировать вручную. Для этого на вкладке «Пользователи» необходимо нажать кнопку «Новый» (Рис. 224). Затем в открывшемся окне указать имя пользователя (Рис. 225), его статус (включен или отключен) и уровень доступа (поле «Роль»). Не рекомендуется заполнять поле «Группы», так как система должна автоматически добавить пользователя в группу участников.

OpenUDS. Интеграция с Active Directory – пользователи LDAP

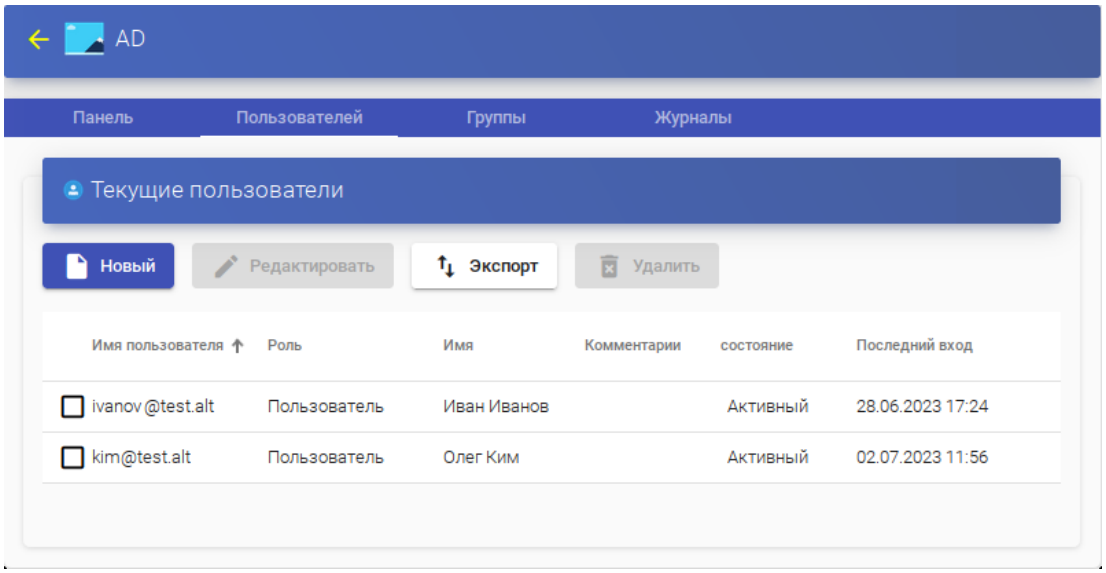


Рис. 224

OpenUDS. Интеграция с Active Directory – регистрация пользователя вручную

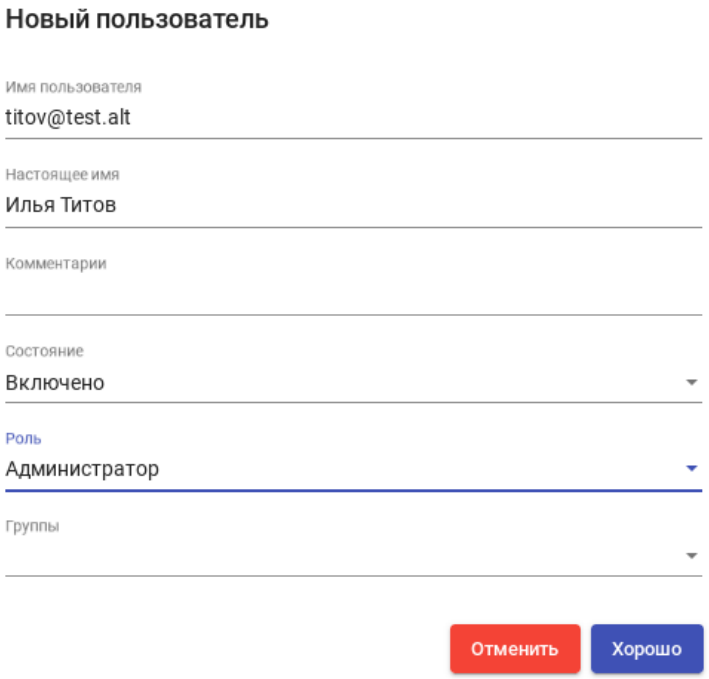


Рис. 225

5.11.3.2.3 IP аутентификатор

Этот тип аутентификации обеспечивает доступ клиентов к рабочим столам и виртуальным приложениям по 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. 226).

OpenUDS. IP аутентификатор

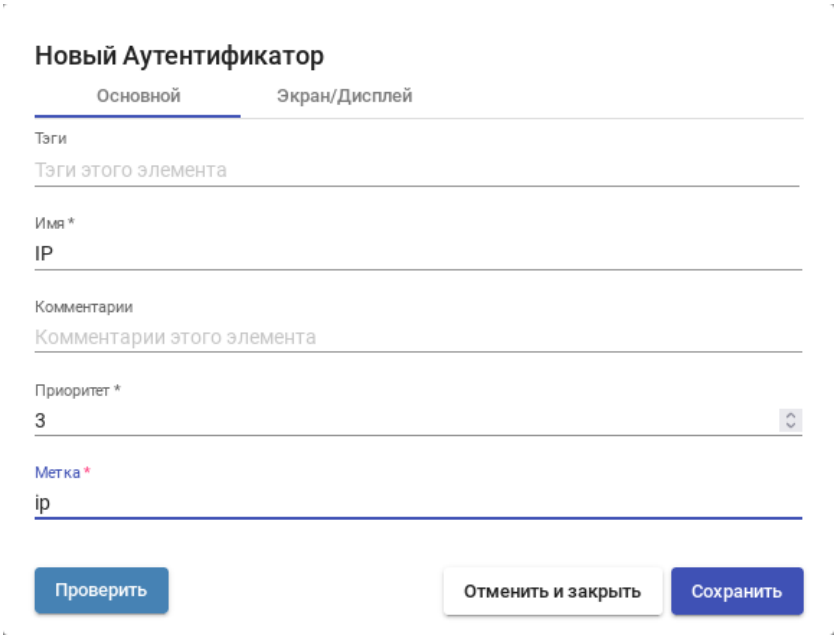


Рис. 226

После того, как аутентификатор типа «IP аутентификатор» будет 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. 227).

OpenUDS. IP аутентификатор – создание группы пользователей

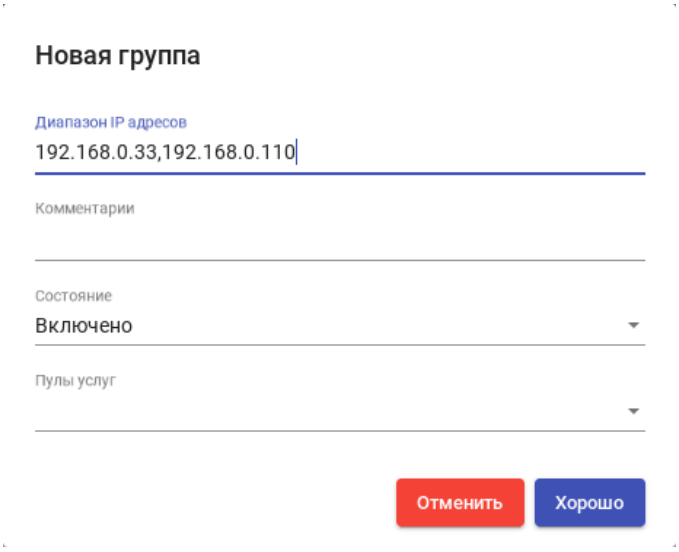


Рис. 227

5.11.3.3 Настройка менеджера ОС

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».

Менеджер ОС (Рис. 228) запускает ранее настроенные службы:

- «Linux OS Active Directory Manager» используется для виртуальных рабочих столов на базе Linux, которые являются членами домена AD;
- «Linux OS FreeIPA Manager» используется для виртуальных рабочих столов на базе Linux, которые являются членами домена FreeIPA;
- «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;
- «Windows Domain ОС менеджер» используется для виртуальных рабочих столов на базе Windows, которые являются членами домена AD.

OpenUDS. Настройка «OS Manager»

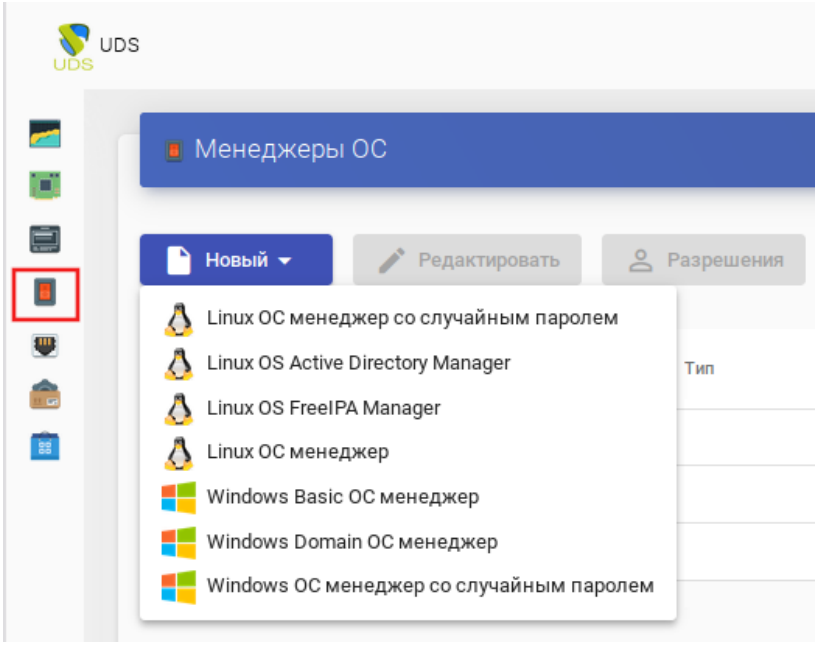


Рис. 228

Настройки для «Linux ОС менеджер» и «Windows Basic ОС менеджер» находятся на двух вкладках:

- вкладка «Основной» (Рис. 229):
  - «Имя» – название;
  - «Действие при выходе из системы» – действие, которое OpenUDS будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя. «Держать сервис привязанным – постоянный пул, при выходе пользователя (выключении ВМ), ВМ запускается

заново, при повторном входе пользователю будет назначен тот же рабочий стол. «Удалить сервис» – непостоянный пул, при выходе пользователя из системы, ВМ удаляется и создается заново. «Держать сервис привязанным даже в новой публикации» – сохранение назначенной службы даже при создании новой публикации;

- «Максимальное время простоя» – 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;

- вкладка «Расширенный»:
  - «Выход из календаря» – если этот параметр установлен, OpenUDS попытается завершить сессию пользователя, когда для текущего соединения истечет время доступа (если параметр не установлен, пользователю будет разрешено продолжить работу).

OpenUDS. Настройка «OS Manager»

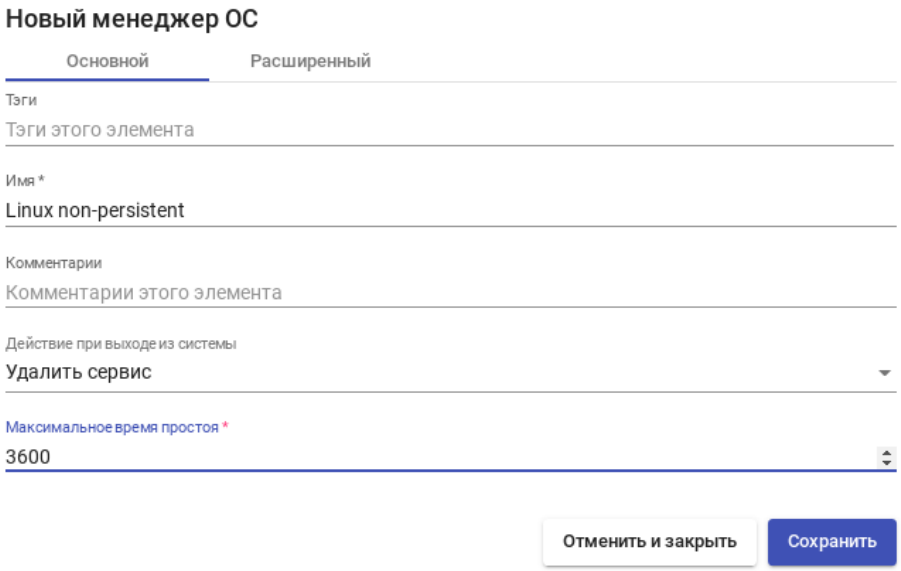


Рис. 229

Минимальные настройки для «Linux OS Active Directory Manager»:

- вкладка «Основной» (Рис. 230):
  - «Имя» – название;
  - «Домен» – домен, к которому будут присоединены виртуальные рабочие столы. Необходимо использовать формат FQDN (например, test.alt);
  - «Аккаунт» – пользователь с правами на добавление машин в домен;
  - «Пароль» – пароль пользователя указанного в поле «Аккаунт»;
  - «OU» – организационная единица, в которую будут добавлены виртуальные хосты (если не указано, хосты будут зарегистрированы в подразделении по умолчанию – «Computers»). Формат поддерживаемых OU: `OU = name_OU_last_level, … OU =`

`name_OU_first_level, DC = name_domain, DC = extension_domain`. Во избежание ошибок, рекомендуется сверяться с полем `distinguishedName` в свойствах атрибута OU;

- «Действие при выходе из системы» – действие, которое OpenUDS будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя. «Держать сервис привязанным – постоянный пул, при выходе пользователя (выключении ВМ), ВМ запускается заново, при повторном входе пользователю будет назначен тот же рабочий стол. «Удалить сервис» – непостоянный пул, при выходе пользователя из системы, ВМ удаляется и создается заново. «Держать сервис привязанным даже в новой публикации» – сохранение назначенной службы даже при создании новой публикации;
- «Максимальное время простоя» – 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;

- вкладка «Расширенный» (Рис. 231):
  - «Client software» – позволяет указать, если это необходимо, способ подключения (SSSD или Winbind);
  - «Membership software» – позволяет указать, если это необходимо, утилиту, используемую для подключения к домену (Samba или adcli);
  - «Убрать машину» – если этот параметр установлен, OpenUDS удалит запись о виртуальном рабочем столе в указанном подразделении после удаления рабочего стола (необходимо, чтобы пользователь, указанный в поле «Аккаунт», имел права на выполнение данного действия в OU);
  - «Использовать SSL» – если этот параметр установлен, будет использоваться SSL-соединение;
  - «Automatic ID mapping» – автоматический маппинг ID;
  - «Выход по календарю» – если этот параметр установлен, OpenUDS попытается завершить сессию пользователя, когда для текущего соединения истечет время доступа (если параметр не установлен, пользователю будет разрешено продолжить работу).

Примечание. Для возможности ввода компьютера в домен, на нём должен быть доступен сервер DNS, имеющий записи про контроллер домена Active Directory.

OpenUDS. Настройка «OS Linux OS Active Directory Manager»

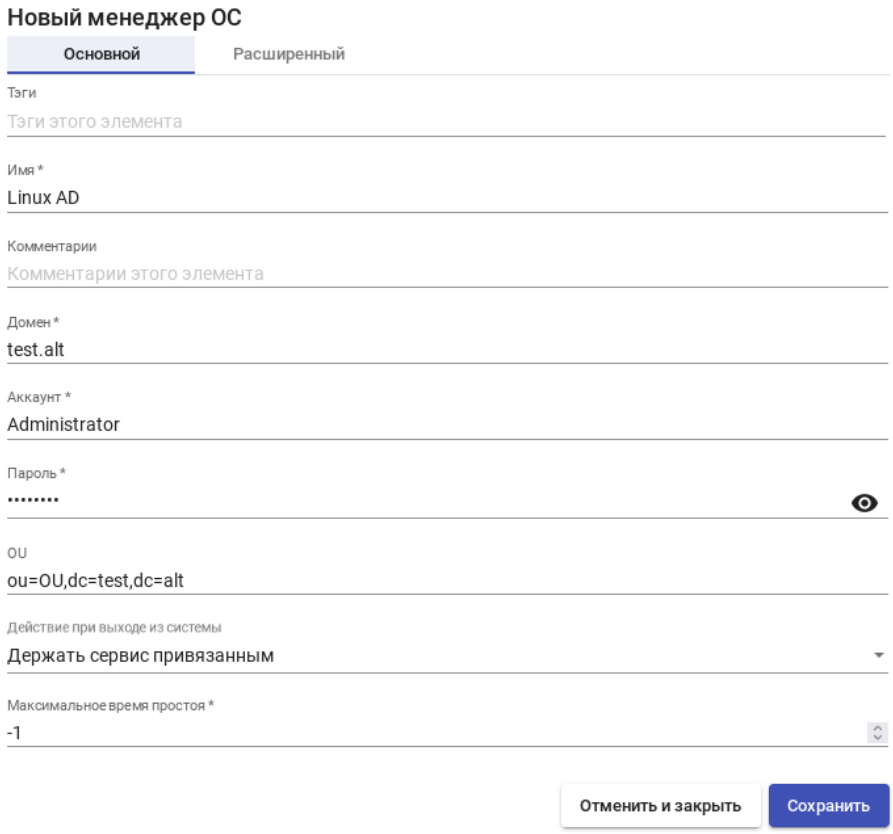


Рис. 230

OpenUDS. Настройка «OS Linux OS Active Directory Manager»

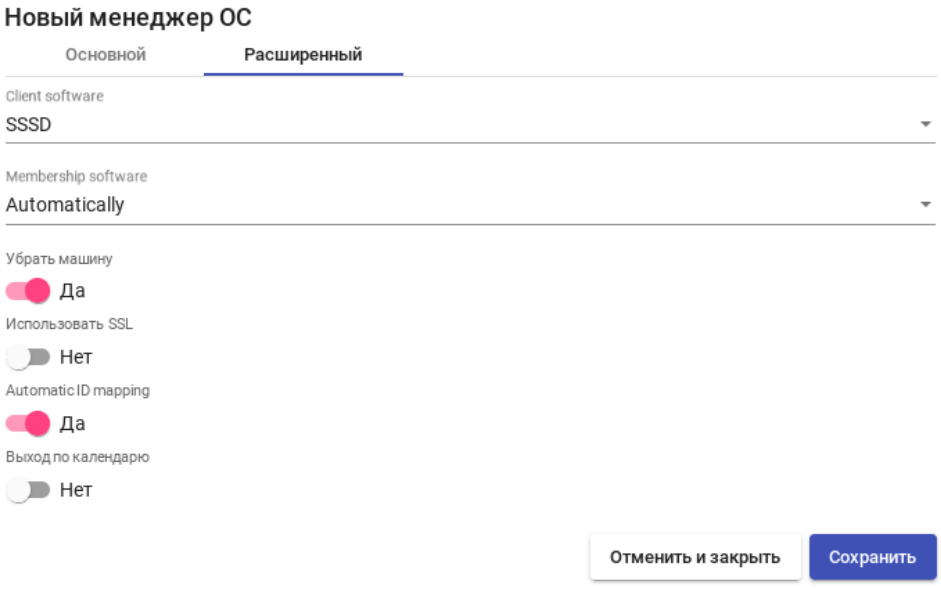


Рис. 231

Минимальные настройки для «Linux OS FreeIPA Manager»:

- вкладка «Основной» (Рис. 232):
  - «Имя» – название;

- «Домен» – домен, к которому будут присоединены виртуальные рабочие столы. Необходимо использовать формат FQDN (например, example.test);
- «Аккаунт» – пользователь с правами на добавление машин в домен;
- «Пароль» – пароль пользователя указанного в поле «Аккаунт»;
- «OU» – организационная единица, в которую будут добавлены виртуальные хосты (если не указано, хосты будут зарегистрированы в подразделении по умолчанию – «Computers»). Формат поддерживаемых OU: `OU = name_OU_last_level, … OU = name_OU_first_level, DC = name_domain, DC = extension_domain`. Во избежание ошибок, рекомендуется сверяться с полем `distinguishedName` в свойствах атрибута OU;
- «Действие при выходе из системы» – действие, которое OpenUDS будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя. «Держать сервис привязанным – постоянный пул, при выходе пользователя (выключении ВМ), ВМ запускается заново, при повторном входе пользователю будет назначен тот же рабочий стол. «Удалить сервис» – непостоянный пул, при выходе пользователя из системы, ВМ удаляется и создается заново. «Держать сервис привязанным даже в новой публикации» – сохранение назначенной службы даже при создании новой публикации;
- «Максимальное время простоя» – 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;

- вкладка «Расширенный» (Рис. 233):
  - «Client software» – позволяет указать, если это необходимо, способ подключения (SSSD или Winbind);
  - «Membership software» – позволяет указать, если это необходимо, утилиту, используемую для подключения к домену (Samba или adcli);
  - «Убрать машину» – если этот параметр установлен, OpenUDS удалит запись о виртуальном рабочем столе в указанном подразделении после удаления рабочего стола (необходимо, чтобы пользователь, указанный в поле «Аккаунт», имел права на выполнение данного действия в OU);
  - «Использовать SSL» – если этот параметр установлен, будет использоваться SSL-соединение;
  - «Automatic ID mapping» – автоматический маппинг ID;
  - «Выход по календарю» – если этот параметр установлен, OpenUDS попытается завершить сессию пользователя, когда для текущего соединения истечет время доступа (если параметр не установлен, пользователю будет разрешено продолжить работу).

Примечание. Для возможности ввода компьютера в домен, на нём должен быть доступен сервер DNS, имеющий записи про сервер FreeIPA.

OpenUDS. Настройка «OS Linux OS FreeIPA Manager»

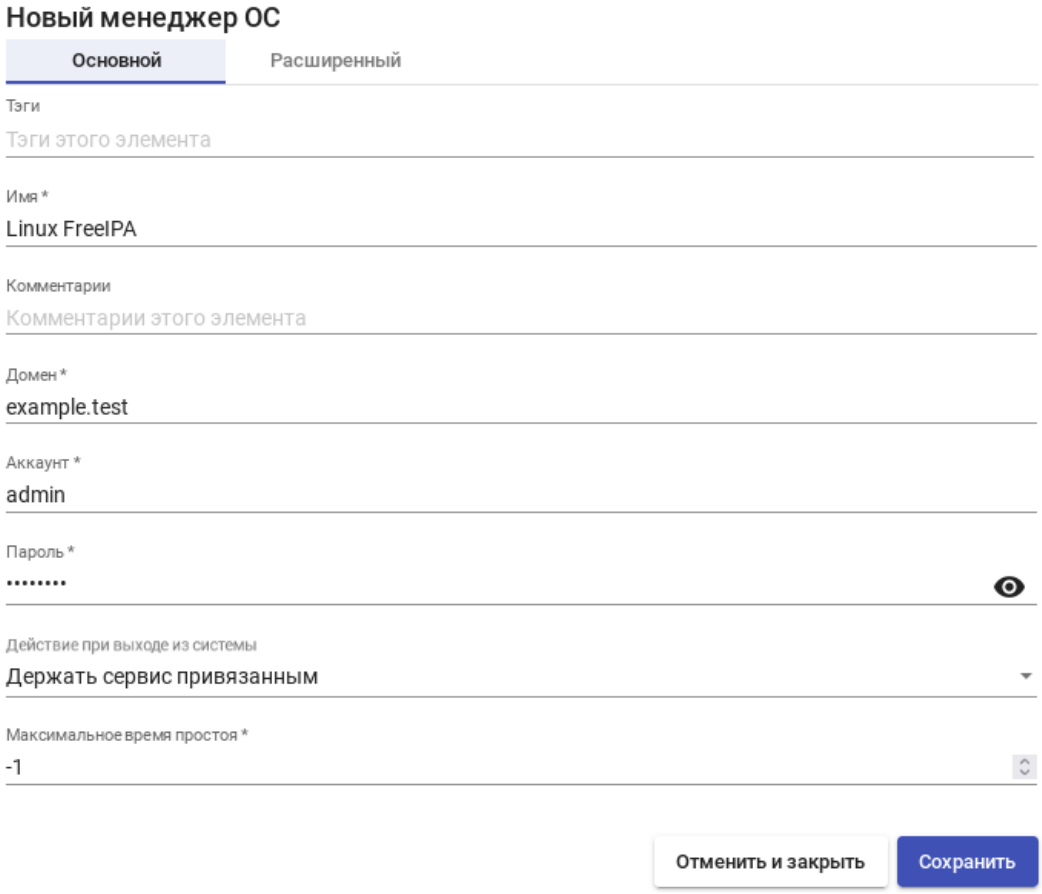


Рис. 232

OpenUDS. Настройка «OS Linux OS FreeIPA Manager»

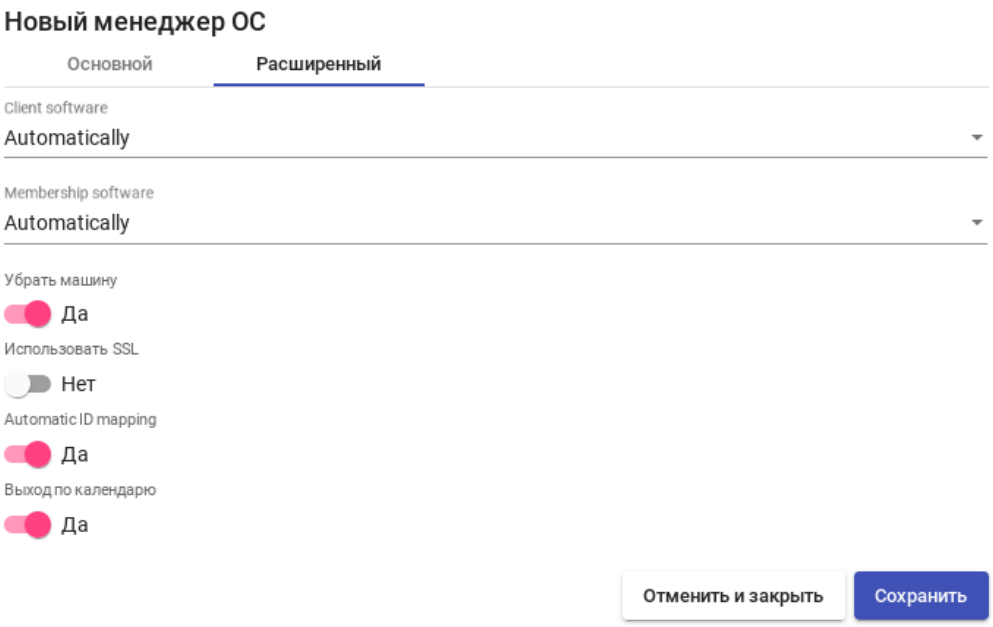


Рис. 233

Минимальные настройки для «Windows Domain ОС менеджер»:

- вкладка «Основной» (Рис. 234):
  - «Имя» – название;
  - «Домен» – домен, к которому будут присоединены виртуальные рабочие столы. Необходимо использовать формат FQDN (например, test.alt);
  - «Аккаунт» – пользователь с правами на добавление машин в домен;
  - «Пароль» – пароль пользователя указанного в поле «Аккаунт»;
  - «OU» – организационная единица, в которую будут добавлены виртуальные хосты (если не указано, хосты будут зарегистрированы в подразделении по умолчанию – «Computers»). Формат поддерживаемых OU: `OU = name_OU_last_level, … OU = name_OU_first_level, DC = name_domain, DC = extension_domain`. Во избежание ошибок, рекомендуется сверяться с полем distinguishedName в свойствах атрибута OU;
  - «Действие при выходе из системы» – действие, которое OpenUDS будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя. «Держать сервис привязанным – постоянный пул, при выходе пользователя (выключении ВМ), ВМ запускается заново, при повторном входе пользователю будет назначен тот же рабочий стол. «Удалить сервис» – непостоянный пул, при выходе пользователя из системы, ВМ удаляется и создается заново. «Держать сервис привязанным даже в новой публикации» – сохранение назначенной службы даже при создании новой публикации;
  - «Максимальное время простоя» – 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;
- вкладка «Расширенный» (Рис. 235):
  - «Группа машин» – указывает, к какой группе машин AD будут добавлены виртуальные рабочие столы, созданные UDS;
  - «Убрать машину» – если этот параметр установлен, OpenUDS удалит запись о виртуальном рабочем столе в указанном подразделении после удаления рабочего стола (необходимо, чтобы пользователь, указанный в поле «Аккаунт», имел права на выполнение данного действия в OU);
  - «Предпочтения серверов» – если серверов AD несколько, можно указать, какой из них использовать предпочтительнее;
  - «Использовать SSL» – если этот параметр установлен, будет использоваться SSL-соединение;

- «Выход по календарю» – если этот параметр установлен, OpenUDS попытается завершить сессию пользователя, когда для текущего соединения истечет время доступа (если параметр не установлен, пользователю будет разрешено продолжить работу).

OpenUDS. Windows Domain ОС менеджер

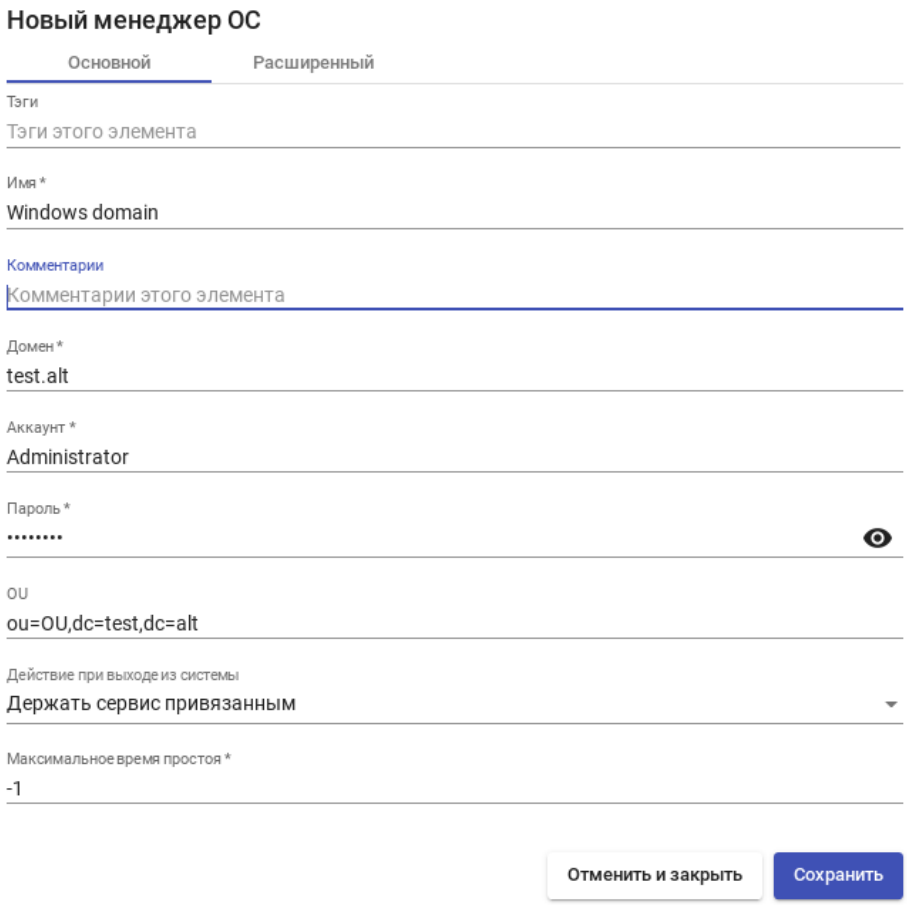


Рис. 234

OpenUDS. Windows Domain ОС менеджер

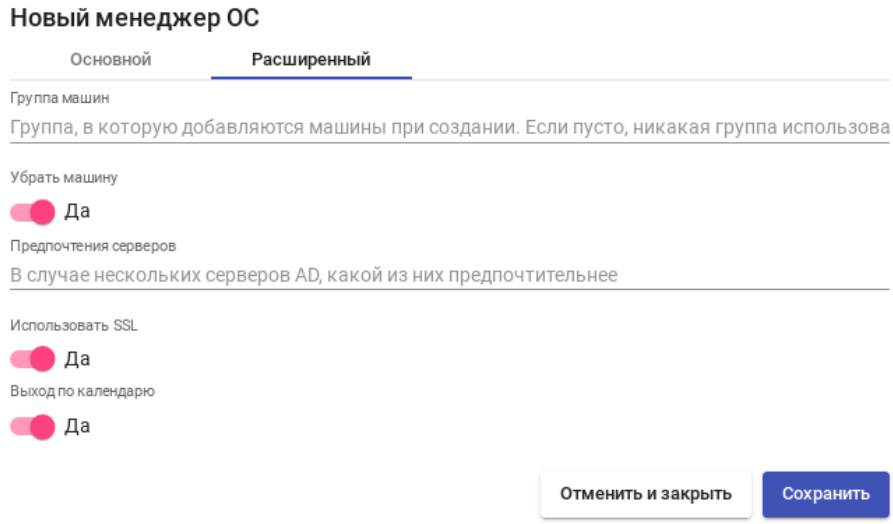


Рис. 235

5.11.3.4 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. 236):

- «Прямой» («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 «Транспорты»

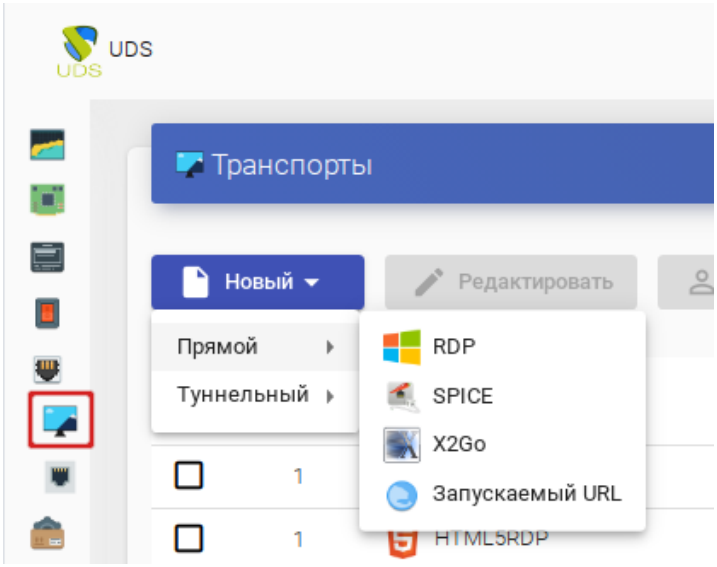


Рис. 236

5.11.3.4.1 RDP (прямой)

RDP 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).

Параметры для настройки транспорта RDP:

- вкладка «Основной» (Рис. 237):
  - «Имя» – название транспорта;
  - «Приоритет» – чем меньше значение приоритета, тем выше данный транспорт будет указан в списке доступных транспортов для сервиса. Транспорт с самым низким приоритетом, будет транспортом по умолчанию;

- «Сетевой доступ» – разрешает или запрещает доступ пользователей к службе в зависимости от сети, из которой осуществляется доступ;
- «Сети» – сетевые диапазоны, подсети или IP-адреса (настраиваются в разделе «Сети»). Пустое поле означает «все сети». Используется вместе с параметром «Сетевой доступ»;
- «Разрешенные устройства» – разрешает доступ к службе только с выбранных устройств. Пустое поле означает «все устройства»;
- «Сервис-пулы» – позволяет назначить транспорт одному или нескольким ранее созданным пулам услуг. Можно оставить это поле пустым и выбрать способы подключения при создании пула услуг;

- вкладка «Учетные данные» (Рис. 238):
  - «Пропустить данные аккаунта» – если установлено значение «Да», учётные данные для доступа к виртуальному рабочему столу будут запрашиваться при подключении к серверу. Если установлено значение «Нет», будут использоваться данные OpenUDS (см. ниже);
  - «Имя пользователя» – имя пользователя, которое будет использоваться для доступа к рабочему столу (пользователь должен существовать на ВМ). Если данное поле пустое, будет использован логин авторизовавшегося в веб-интерфейсе OpenUDS пользователя;
  - «Пароль» – пароль пользователя, указанного в поле «Имя пользователя»;
  - «Без домена» – указывает, перенаправляется ли доменное имя вместе с пользователем. Значение «Да» равносильно пустому полю «Domain»;
  - «Домен» – домен. Если поле не пустое, то учётные данные будут использоваться в виде DOMAIN\user;
- вкладка «Параметры» (Рис. 239) – разрешение перенаправления дисков, принтеров и других устройств;
- вкладка «Экран/Дисплей» (Рис. 240) – настройка окна рабочего стола;
- вкладка «Linux Client» (Рис. 241):
  - «Мультимедийная синхронизация» – включает параметр мультимедиа на клиенте FreeRDP;
  - «Использовать Alsa» – использовать звук через Alsa;
  - «Строка принтера» – принтер, используемый клиентом FreeRDP (если включено перенаправление принтера). Пример: «HP_LaserJet_M1536dnf_MFP» (названия подключенных принтеров можно вывести командой `lpstat -a`);
  - «Строка Smartcard» – токен, используемый клиентом FreeRDP (если включено перенаправление смарт-карт). Пример: «Aktiv Rutoken ECP 00 00».

- «Пользовательские параметры» – здесь можно указать любой параметр, поддерживаемый клиентом FreeRDP;

- вкладка «Расширенный» (Рис. 241):
  - «Метка» – метка транспорта метапула (используется для того, чтобы назначить несколько транспортов метапулу).

Настройка RDP. Вкладка «Основной»

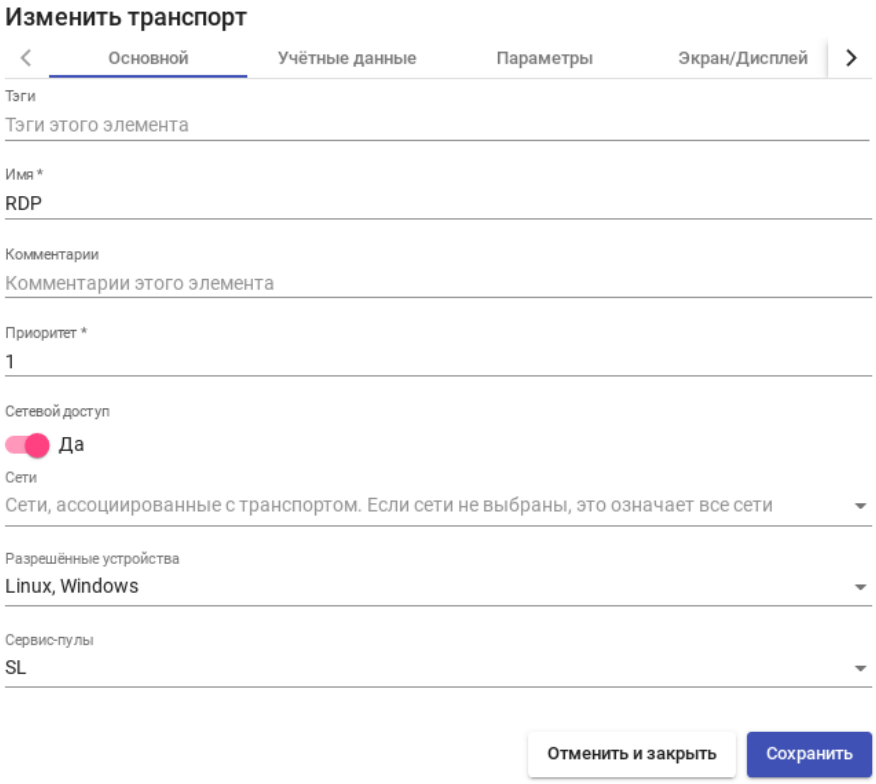


Рис. 237

Настройка RDP. Вкладка «Учетные данные»

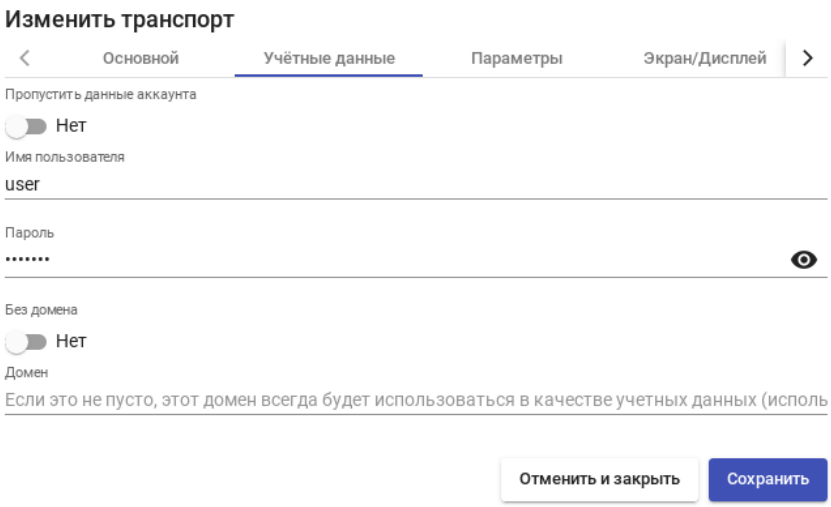


Рис. 238

Настройка RDP. Вкладка «Параметры»

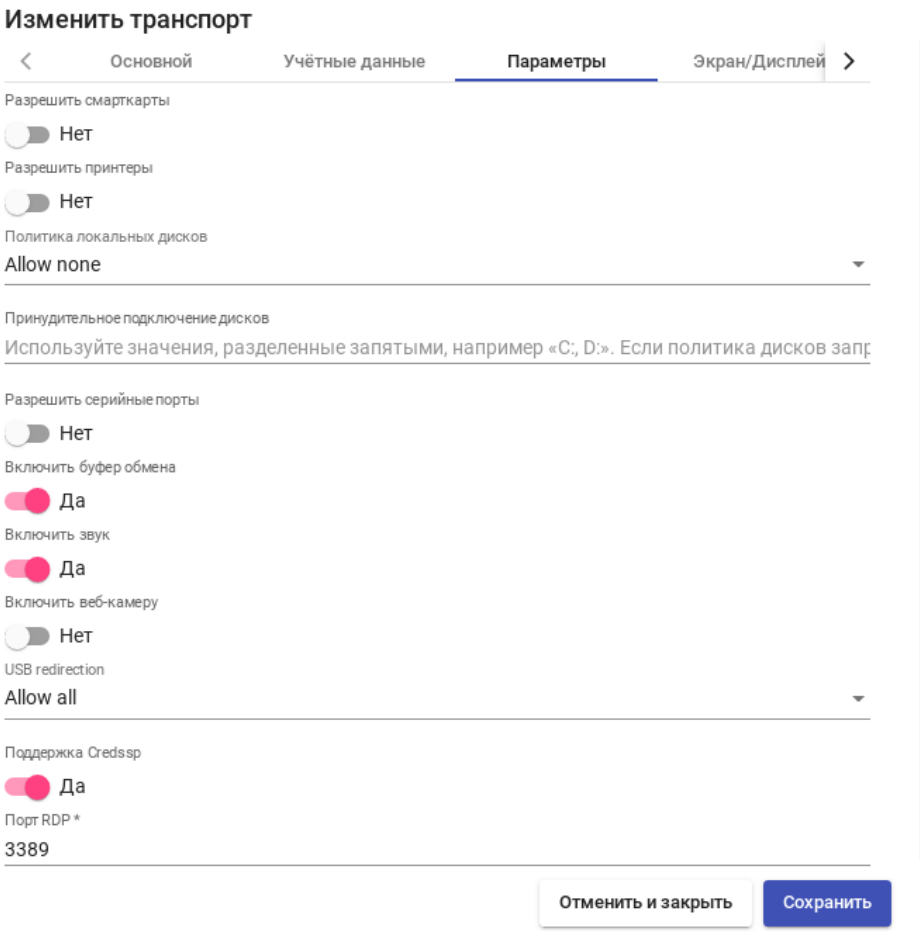


Рис. 239

Настройка RDP. Вкладка «Экран/Дисплей»

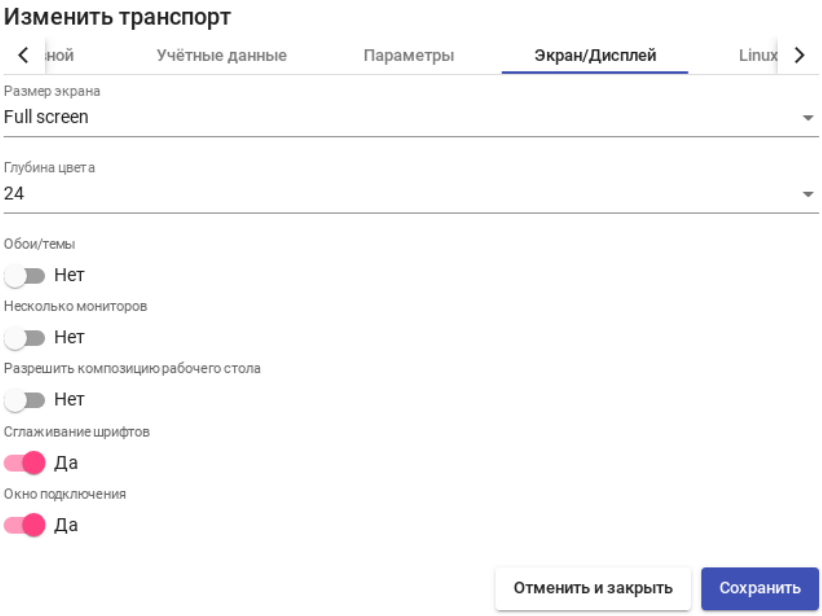


Рис. 240

Настройка RDP. Вкладка «Linux Client»

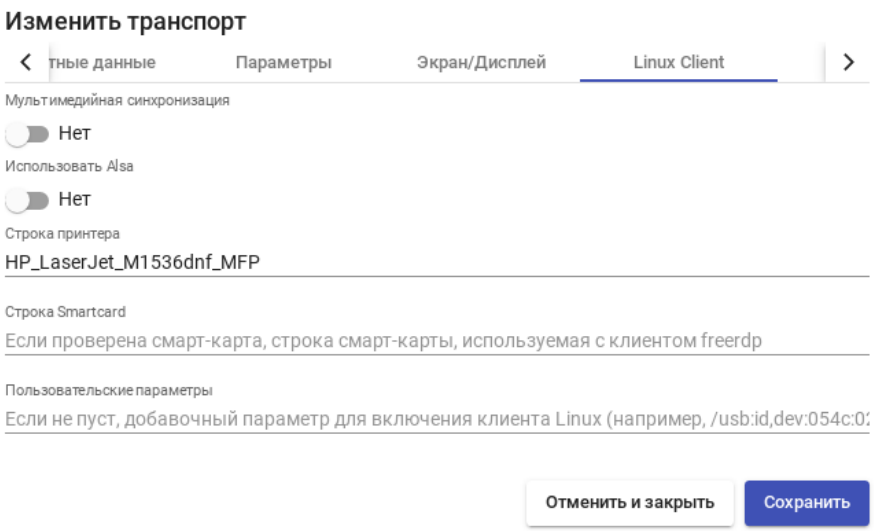


Рис. 241

5.11.3.4.2 RDP (туннельный)

Все настройки аналогичны настройке RDP, за исключением настроек на вкладке «Туннель» (Рис. 242):

- «Туннельный сервер» – IP-адрес/имя OpenUDS Tunnel. Если доступ к рабочему столу осуществляется через глобальную сеть, необходимо ввести общедоступный IP-адрес сервера OpenUDS Tunnel. Формат: IP_Tunneler:Port;
- «Время ожидания туннеля» – максимальное время ожидания туннеля;
- «Принудительная проверка SSL-сертификата» – принудительная проверка сертификата туннельного сервера.

Настройка RDP. Вкладка «Туннель»

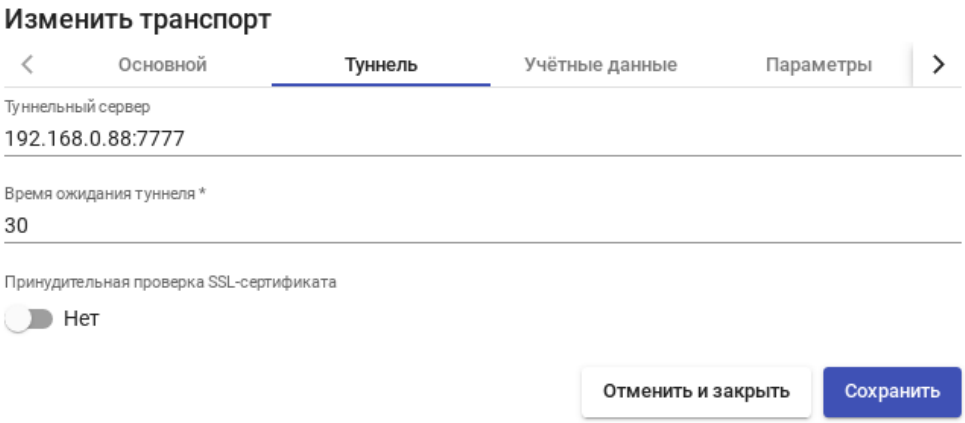


Рис. 242

5.11.3.4.3 X2Go (прямой)

X2Go, 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.

Параметры для настройки транспорта RDP:

- вкладка «Основной» (Рис. 243):
  - «Имя» – название транспорта;
  - «Приоритет» – приоритет, чем меньше значение приоритета, тем выше данный транспорт будет указан в списке доступных транспортов для сервиса. Транспорт с самым низким приоритетом, будет транспортом по умолчанию;
  - «Сетевой доступ» – разрешает или запрещает доступ пользователей к службе в зависимости от сети, из которой осуществляется доступ;
  - «Сети» – сетевые диапазоны, подсети или IP-адреса (настраиваются в разделе «Сети»). Пустое поле означает «все сети». Используется вместе с параметром «Сетевой доступ»;
  - «Разрешенные устройства» – разрешает доступ к службе только с выбранных устройств. Пустое поле означает «все устройства»;
  - «Сервис-пулы» – позволяет назначить транспорт одному или нескольким ранее созданным пулам услуг. Можно оставить это поле пустым и выбрать способы подключения при создании пула услуг.
- вкладка «Учетные данные» (Рис. 244):
  - «Имя пользователя» – имя пользователя, которое будет использоваться для доступа к рабочему столу (пользователь должен существовать на ВМ). Если данное поле пустое, будет использован логин авторизовавшегося в веб-интерфейсе OpenUDS пользователя;
- вкладка «Параметры» (Рис. 245) – разрешение перенаправления дисков, принтеров и других устройств;
  - «Размер экрана» – размер окна рабочего стола;
  - «Экран» – менеджер рабочего стола (Xfce, Mate и др.) или виртуализация приложений Linux (UDS vAPP);
  - «vAPP» – полный путь до приложения (если «Экран» = UDS vAPP);
  - «Включить звук» – включить звук;
  - «Перенаправить домашнюю папку» – перенаправить домашнюю папку клиента подключения на виртуальный рабочий стол (на Linux также перенаправлять /media);
  - «Скорость» – скорость подключения;
- Вкладка «Расширенный» (Рис. 246) – настройка окна рабочего стола;
  - «Звук» – тип звукового сервера;

- «Клавиатура» – раскладка клавиатуры;
- «Метка» – метка транспорта метапула (используется для того, чтобы назначить несколько транспортов метапулу).

Настройка X2Go. Вкладка «Основной»

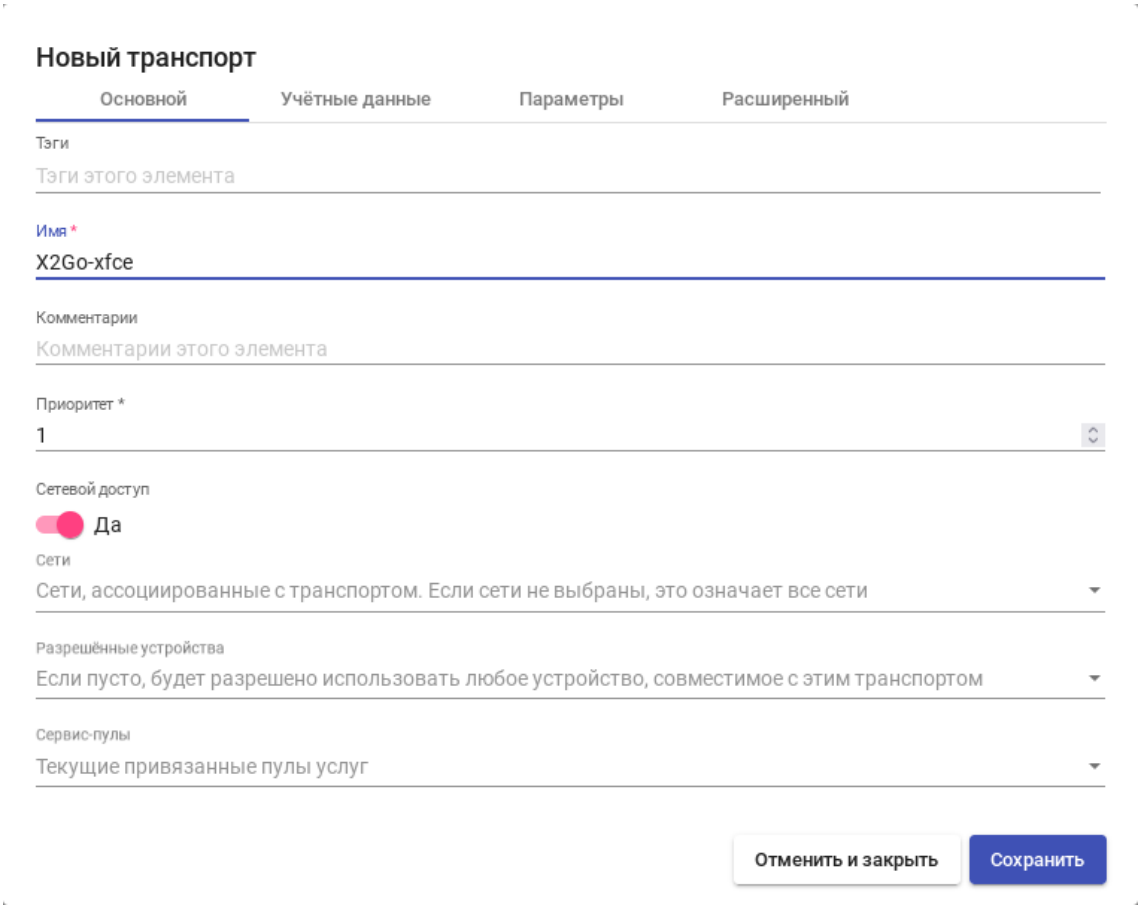


Рис. 243

Настройка X2Go. Вкладка «Учетные данные»

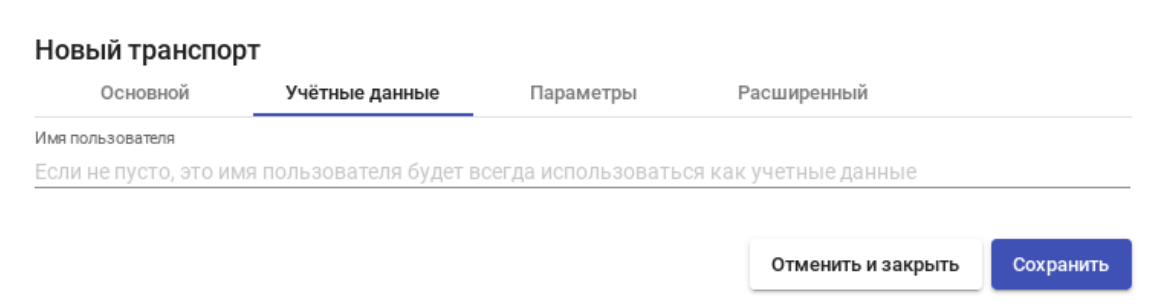


Рис. 244

Настройка X2Go. Вкладка «Параметры»

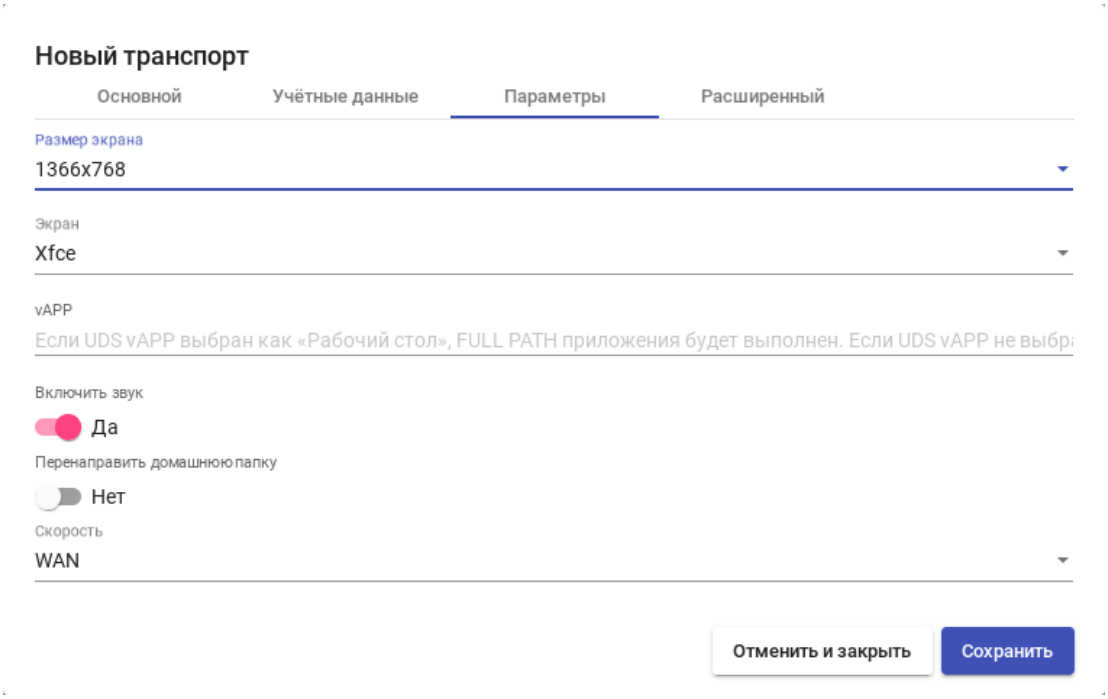


Рис. 245

Настройка X2Go. Вкладка «Расширенный»

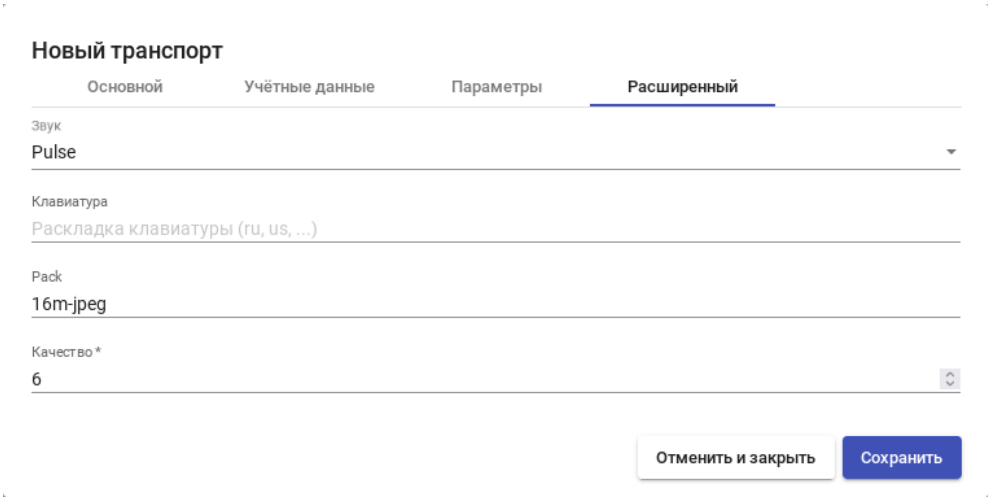


Рис. 246

5.11.3.4.4 X2Go (туннельный)

Все настройки аналогичны настройке X2Go, за исключением настроек на вкладке «Туннель» (Рис. 247):

- «Туннельный сервер» – IP-адрес/имя OpenUDS Tunnel. Если доступ к рабочему столу осуществляется через глобальную сеть, необходимо ввести общедоступный IP-адрес сервера OpenUDS Tunnel. Формат: IP_Tunneler:Port;
- «Время ожидания туннеля» – максимальное время ожидания туннеля;

- «Принудительная проверка SSL-сертификата» – принудительная проверка сертификата туннельного сервера.

Настройка X2Go. Вкладка «Туннель»

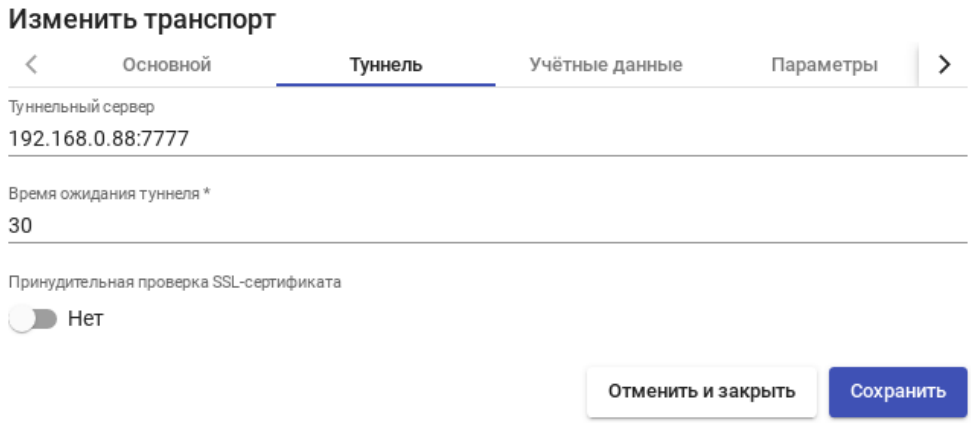


Рис. 247

5.11.3.4.5 SPICE (прямой)

Примечание. Транспортный протокол SPICE может использоваться только с oVirt/RHEV, OpenNebula и PVE.

SPICE позволяет пользователям получать доступ к виртуальным рабочим столам Windows/Linux. На клиентах подключения должен быть установлен клиент SPICE (`virt-manager`).

Примечание. Для работы прямого подключения по протоколу SPICE на сервере OpenUDS и клиентах OpenUDS, откуда осуществляется подключение, имена узлов платформы виртуализации должны корректно разрешаться в IP-адреса этих узлов.

Параметры для настройки транспорта SPICE:

- вкладка «Основной» (Рис. 248):
  - «Имя» – название транспорта;
  - «Приоритет» – приоритет, чем меньше значение приоритета, тем выше данный транспорт будет указан в списке доступных транспортов для сервиса. Транспорт с самым низким приоритетом, будет транспортом по умолчанию;
  - «Сертификат» – сертификат, сгенерированный в ovirt-engine/RHV-manager или в OpenNebula. Требуется для подключения к виртуальным рабочим столам;
  - «Сетевой доступ» – разрешает или запрещает доступ пользователей к службе в зависимости от сети, из которой осуществляется доступ;
  - «Сети» – сетевые диапазоны, подсети или IP-адреса (настраиваются в разделе «Сети»). Пустое поле означает «все сети». Используется вместе с параметром «Сетевой доступ»;

- «Разрешенные устройства» – разрешает доступ к службе только с выбранных устройств. Пустое поле означает «все устройства»;
- «Сервис-пулы» – позволяет назначить транспорт одному или нескольким ранее созданным пулам услуг. Можно оставить это поле пустым и выбрать способы подключения при создании пула услуг;

- вкладка «Расширенный» (Рис. 249) – настройка окна рабочего стола;
  - «Полноэкранный режим» – включает полноэкранный режим виртуального рабочего стола;
  - «Перенаправление смарткарты» – включает перенаправление смарт-карт;
  - «Включить USB» – разрешает перенаправление устройств, подключенных к USB-порту;
  - «Новый USB автобмен» – позволяет перенаправлять PnP-устройства, подключенные к USB-порту;
  - «SSL Connection» – использовать SSL-соединение;
  - «Метка» – метка транспорта метапула (используется для того, чтобы назначить несколько транспортов метапулу).

Настройка SPICE. Вкладка «Основной»

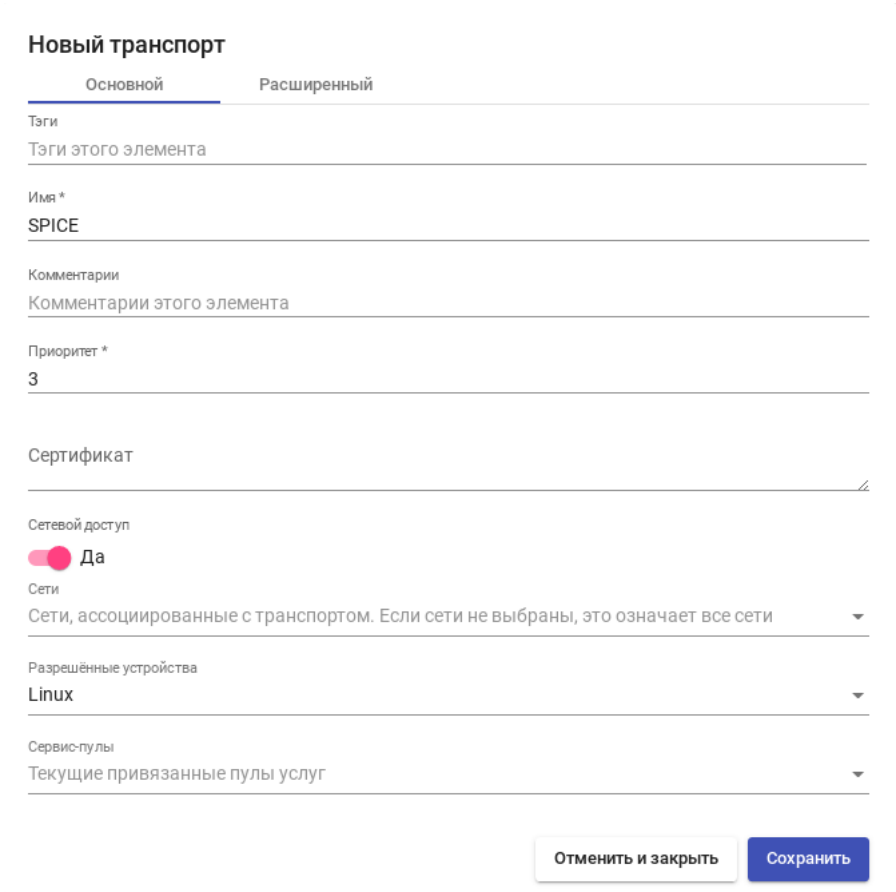


Рис. 248

Настройка SPICE. Вкладка «Расширенный»

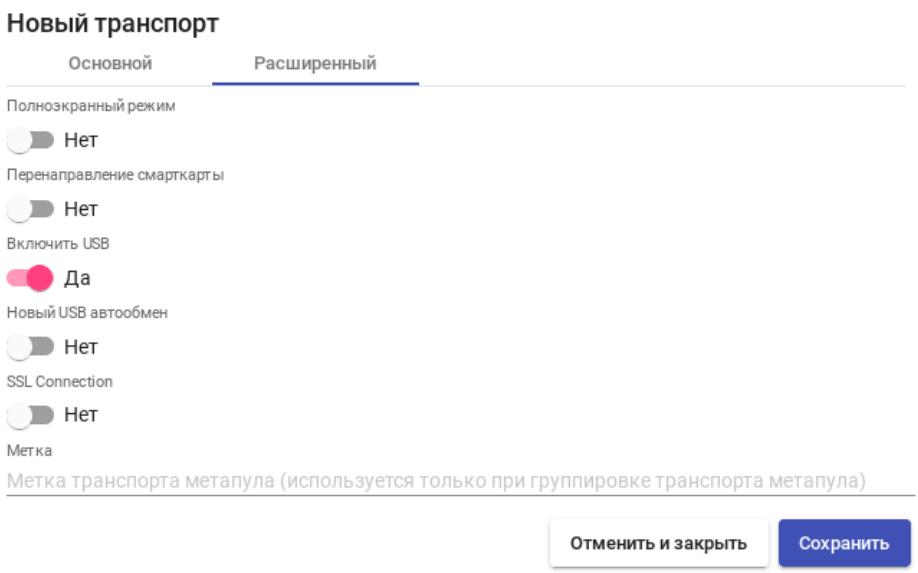


Рис. 249

5.11.3.4.6 HTML5 RDP (туннельный)

HTML5 RDP позволяет пользователям получать доступ к виртуальным рабочим столам Windows/Linux через протокол RDP с использованием браузера, поддерживающего HTML5. На виртуальных рабочих столах должен быть установлен и включен протокол RDP (для виртуальных рабочих столов Linux необходимо использовать XRDP).

Параметры для настройки транспорта HTML5 RDP:

- вкладка «Основной» (Рис. 250):
  - «Имя» – название транспорта;
  - «Приоритет» – приоритет, чем меньше значение приоритета, тем выше данный транспорт будет указан в списке доступных транспортов для сервиса. Транспорт с самым низким приоритетом, будет транспортом по умолчанию;
  - «Сетевой доступ» – разрешает или запрещает доступ пользователей к службе в зависимости от сети, из которой осуществляется доступ;
  - «Сети» – сетевые диапазоны, подсети или IP-адреса (настраиваются в разделе «Сети»). Пустое поле означает «все сети». Используется вместе с параметром «Сетевой доступ»;
  - «Разрешенные устройства» – разрешает доступ к службе только с выбранных устройств. Пустое поле означает «все устройства»;
  - «Сервис-пулы» – позволяет назначить транспорт одному или нескольким ранее созданным пулам услуг. Можно оставить это поле пустым и выбрать способы подключения при создании пула услуг;
- вкладка «Туннель» (Рис. 251):

- «Туннельный сервер» – IP-адрес или имя OpenUDS Tunnel. Формат: http(s)://IP_Tunneler:[Port] (8080 – порт по умолчанию для http, 443 – для https);

- вкладка «Учетные данные» (Рис. 252):
  - «Пропустить данные аккаунта» – если установлено значение «Да», учётные данные для доступа к виртуальному рабочему столу будут запрашиваться при подключении к серверу. Если установлено значение «Нет», будут использоваться данные OpenUDS (см. ниже);
  - «Имя пользователя» – имя пользователя, которое будет использоваться для доступа к рабочему столу (пользователь должен существовать на ВМ). Если данное поле пустое, будет использован логин авторизовавшегося в веб-интерфейсе OpenUDS пользователя;
  - «Пароль» – пароль пользователя, указанного в поле «Имя пользователя»;
  - «Без домена» – указывает, перенаправляется ли доменное имя вместе с пользователем. Значение «Да» равносильно пустому полю «Domain»;
  - «Домен» – домен. Если поле не пустое, то учётные данные будут использоваться в виде DOMAIN\user;
- вкладка «Параметры» (Рис. 253):
  - «Показать обои» – отображать обои рабочего стола;
  - «Разрешить композицию рабочего стола» – включить «Desktop Composition»;
  - «Сглаживание шрифтов» – активирует сглаживание шрифтов;
  - «Включить аудио» – перенаправлять звук с рабочего стола на клиент подключения;
  - «Включить микрофон» – включить микрофон на виртуальном рабочем столе;
  - «Включить печать» – включить печать на виртуальном рабочем столе;
  - «Обмен файлами» – политика обмена файлами между виртуальным рабочим столом и клиентом подключения. Позволяет создать временный каталог (расположенный на сервере OpenUDS Tunnel), для возможности обмена файлами между виртуальным рабочим столом и клиентом подключения;
  - «Буфер обмена» – настройка общего буфера обмена;
  - «Раскладка» – раскладка клавиатуры, которая будет включена на рабочем столе.
- вкладка «Расширенный» (Рис. 254) – настройка окна рабочего стола:
  - «Срок действия билета» – допустимое время (в секундах) для клиента HTML5 для перезагрузки данных из OpenUDS Broker (рекомендуется использовать значение по умолчанию – 60);
  - «Открывать HTML в новом окне» – позволяет указать открывать ли подключение в новом окне;
  - «Безопасность» – позволяет задать уровень безопасности соединения;

- «Порт RDP» – порт RDP (по умолчанию – 3389);
- «Метка» – метка транспорта метапула (используется для того, чтобы назначить несколько транспортов метапулу).

Настройка HTML5 RDP. Вкладка «Основной»

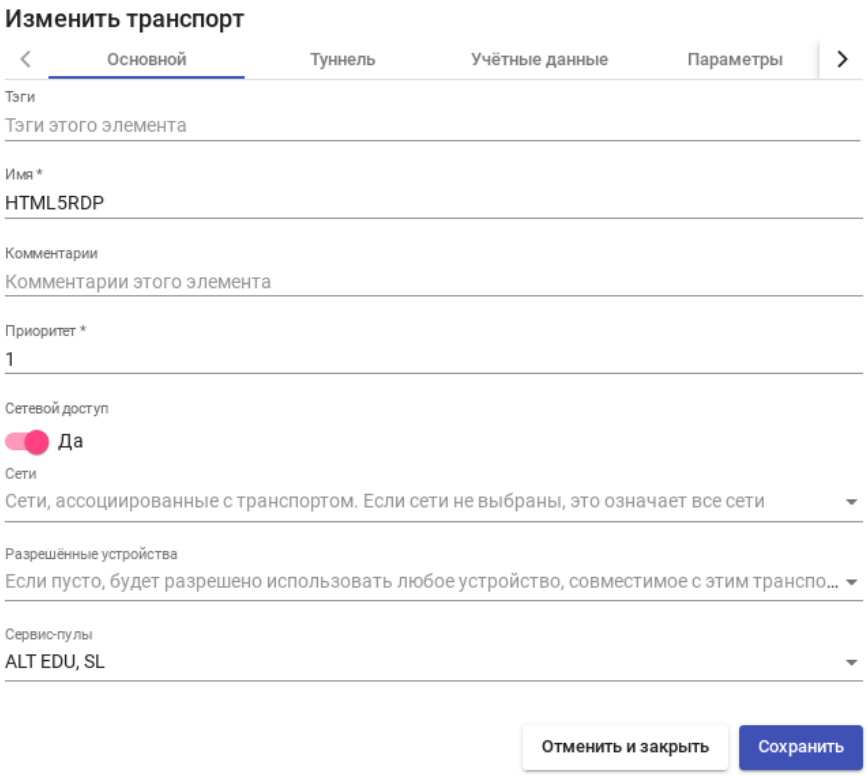


Рис. 250

Настройка HTML5 RDP. Вкладка «Туннель»

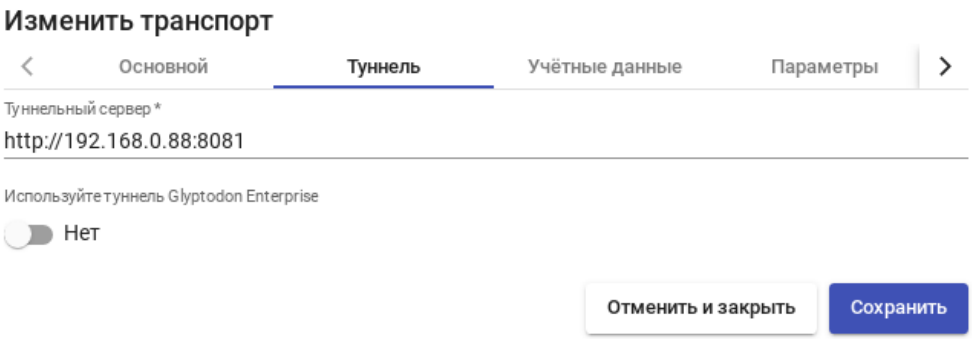


Рис. 251

Настройка HTML5 RDP. Вкладка «Учетные данные»

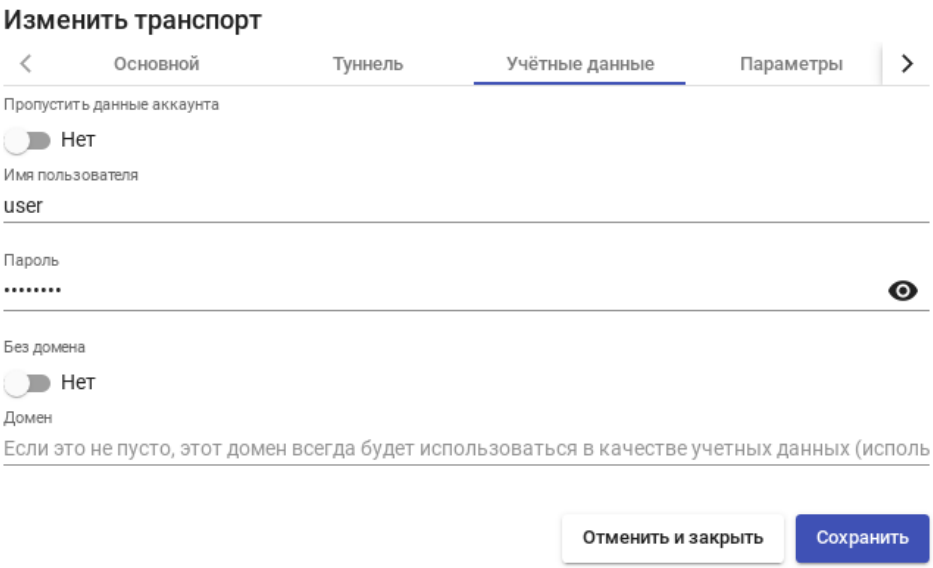


Рис. 252

Настройка HTML5 RDP. Вкладка «Параметры»

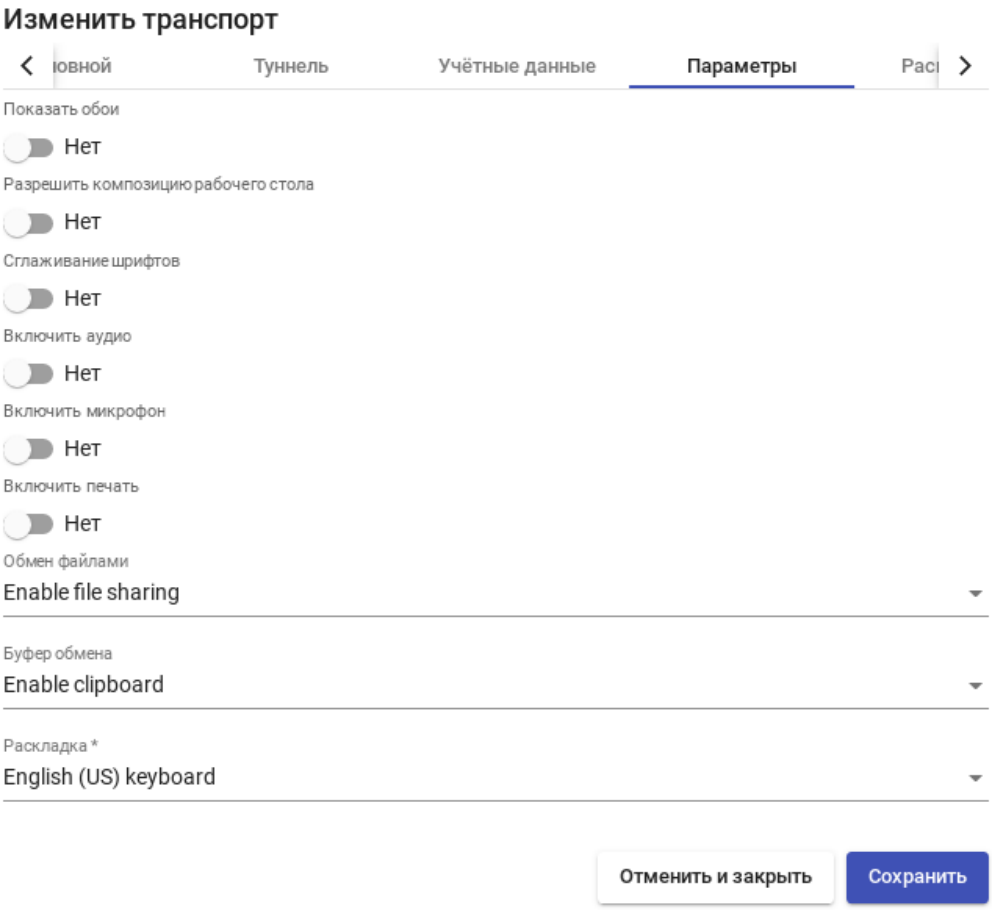


Рис. 253

Настройка HTML5 RDP. Вкладка «Расширенный»

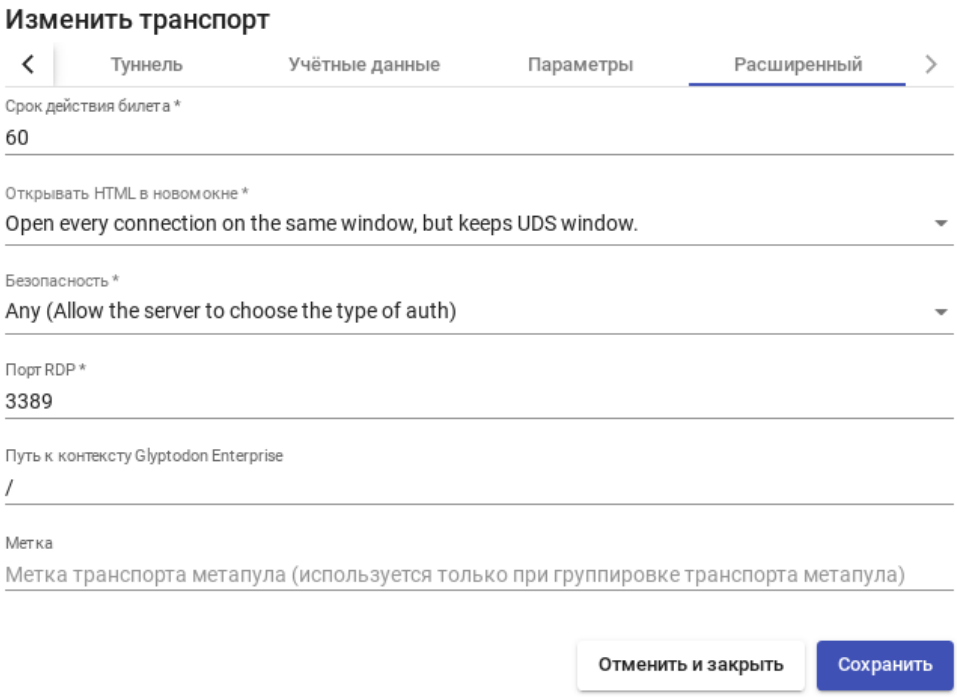


Рис. 254

5.11.3.4.7 HTML5 SSH (туннельный)

HTML5 SSH позволяет пользователям получать доступ к виртуальным рабочим столам Linux по протоколу SSH с использованием браузера, поддерживающего HTML5 (на машинах должен быть запущен сервер SSH). Используя данный транспорт можно подключаться к серверам Linux, на которых не установлен оконный менеджер или среда рабочего стола.

Параметры для настройки транспорта HTML5 SSH:

- вкладка «Основной» (Рис. 255):
  - «Имя» – название транспорта;
  - «Приоритет» – приоритет, чем меньше значение приоритета, тем выше данный транспорт будет указан в списке доступных транспортов для сервиса. Транспорт с самым низким приоритетом, будет транспортом по умолчанию;
  - «Сетевой доступ» – разрешает или запрещает доступ пользователей к службе в зависимости от сети, из которой осуществляется доступ;
  - «Сети» – сетевые диапазоны, подсети или IP-адреса (настраиваются в разделе «Сети»). Пустое поле означает «все сети». Используется вместе с параметром «Сетевой доступ»;
  - «Разрешенные устройства» – разрешает доступ к службе только с выбранных устройств. Пустое поле означает «все устройства»;

- «Сервис-пулы» – позволяет назначить транспорт одному или нескольким ранее созданным пулам услуг. Можно оставить это поле пустым и выбрать способы подключения при создании пула услуг;

- вкладка «Туннель» (Рис. 256):
  - «Туннельный сервер» – IP-адрес или имя OpenUDS Tunnel. Формат: http(s)://IP_Tunneler:[Port] (8080 – порт по умолчанию для http, 443 – для https);
- вкладка «Учетные данные» (Рис. 257):
  - «Имя пользователя» – имя пользователя, которое будет использоваться для доступа к рабочему столу (пользователь должен существовать на ВМ). Если данное поле пустое, будет использован логин авторизовавшегося в веб-интерфейсе OpenUDS пользователя;
- вкладка «Параметры» (Рис. 258):
  - «SSH-команда» – команда, которая будет выполнена на удалённом сервере. Если команда не указана, будет запущена интерактивная оболочка (Рис. 259);
  - «Обмен файлами» – политика обмена файлами между виртуальным рабочим столом и клиентом подключения;
  - «Корень общего доступа к файлам» – корневой каталог для доступа к файлам. Если не указан, будет использоваться корневой каталог (/);
  - «Порт SSH-сервера» – порт SSH-сервера (по умолчанию – 22);
  - «Ключ хоста SSH» – ключ хоста SSH. Если ключ не указан, проверка подлинности хоста выполняться не будет;
  - «Поддержка сервера в рабочем состоянии» – время (в секундах) между сообщениями проверки активности, отправляемых на сервер. Если не указано, сообщения проверки активности не отправляются.
- вкладка «Расширенный» (Рис. 260):
  - «Срок действия билета» – допустимое время (в секундах) для клиента HTML5 для перезагрузки данных из OpenUDS Broker (рекомендуется использовать значение по умолчанию – 60);
  - «Открывать HTML в новом окне» – позволяет указать открывать ли подключение в новом окне;
  - «Метка» – метка транспорта метапула (используется для того, чтобы назначить несколько транспортов метапулу).

Настройка HTML5 SSH. Вкладка «Основной»

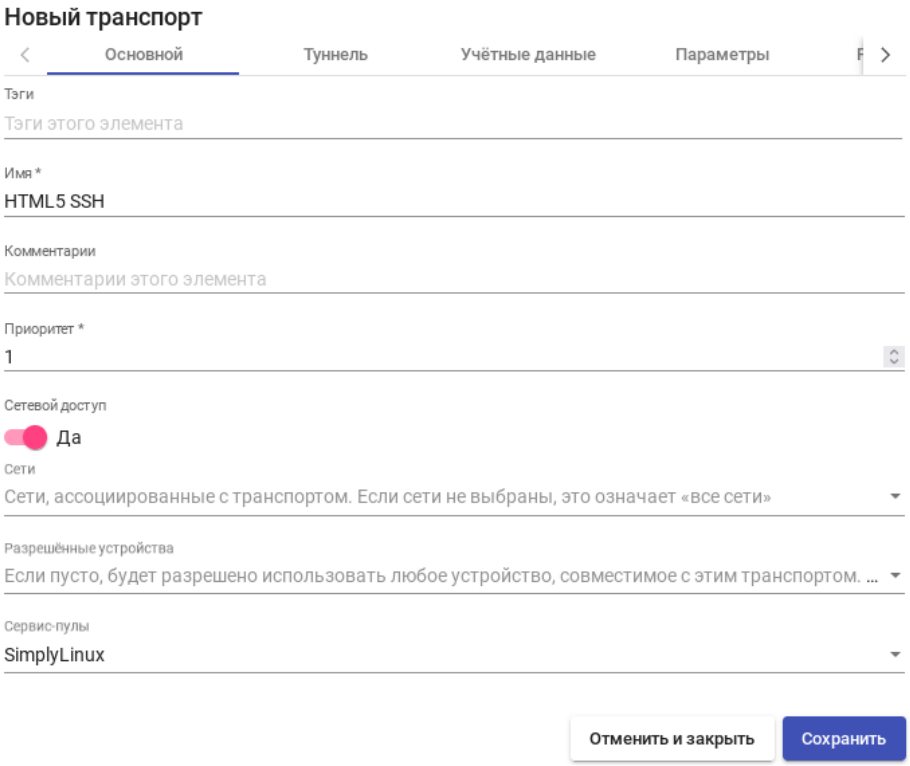


Рис. 255

Настройка HTML5 SSH. Вкладка «Туннель»

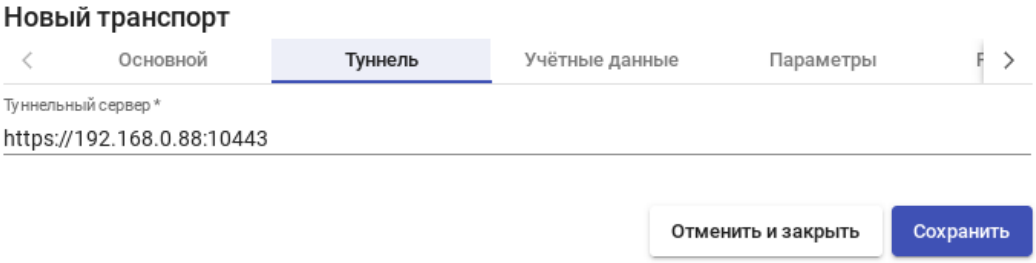


Рис. 256

Настройка HTML5 SSH. Вкладка «Учетные данные»

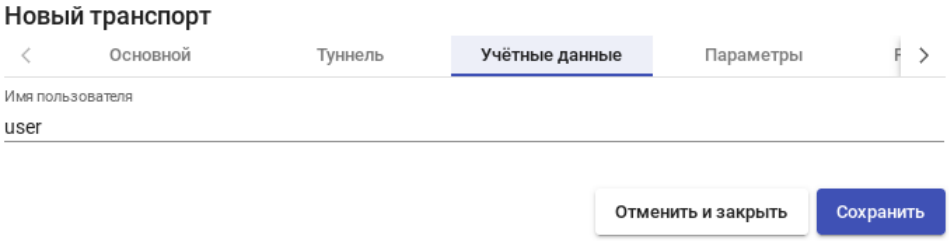


Рис. 257

Настройка HTML5 SSH. Вкладка «Параметры»

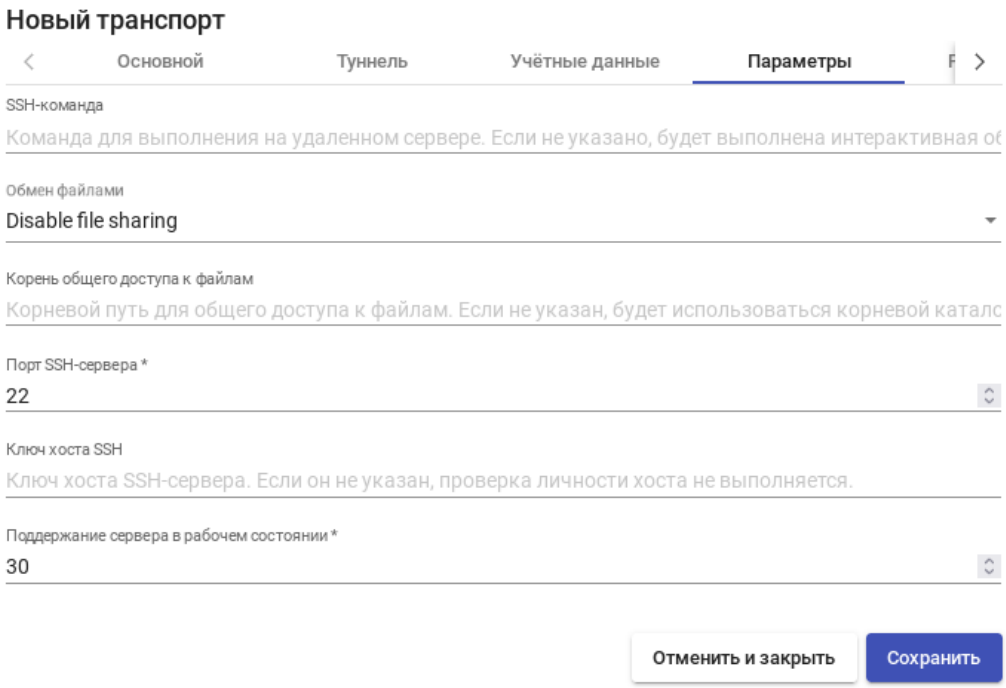


Рис. 258

OpenUDS. Подключение по HTML5 SSH

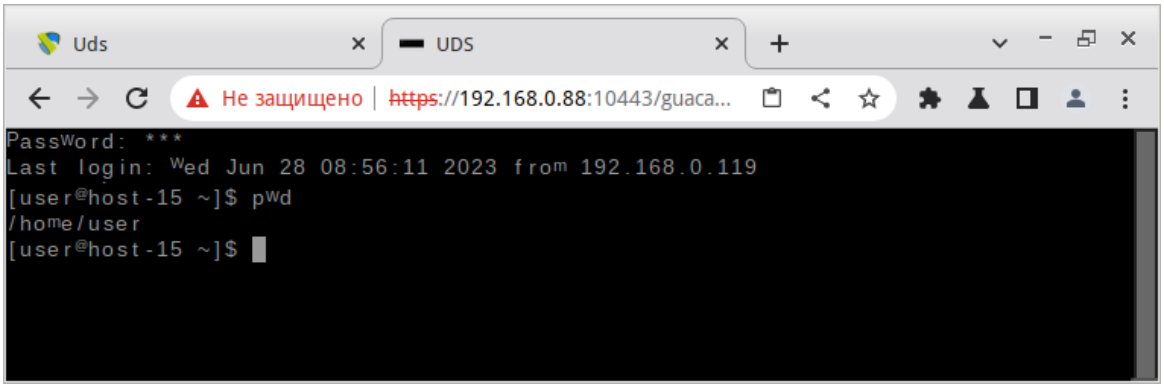


Рис. 259

Настройка HTML5 SSH. Вкладка «Расширенный»

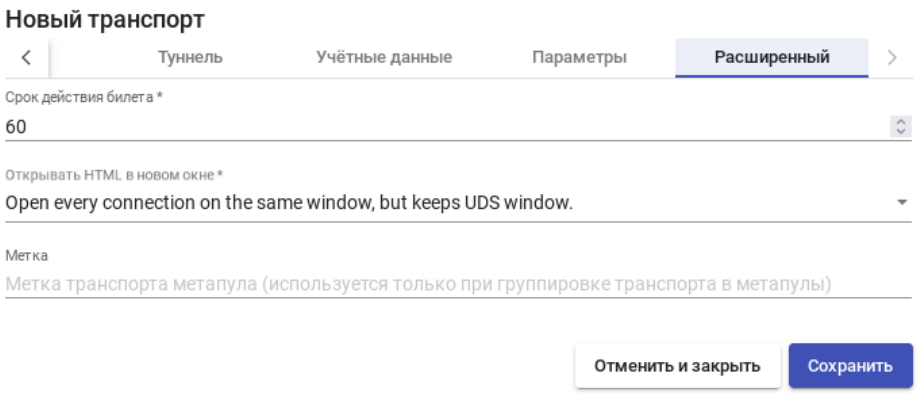


Рис. 260

После входа на удалённый сервер, в зависимости от настроек политики обмена файлами, можно скачивать/загружать файлы. Для загрузки файлов можно открыть окно настроек (<Ctrl>+<Shift>+<Alt>), выбрать устройство в поле «Устройства», нажать кнопку «Загрузка файлов» и выбрать файл. Ход передачи файла будет показан в левом нижнем углу окна (Рис. 261).

HTML5 SSH. Передача файлов

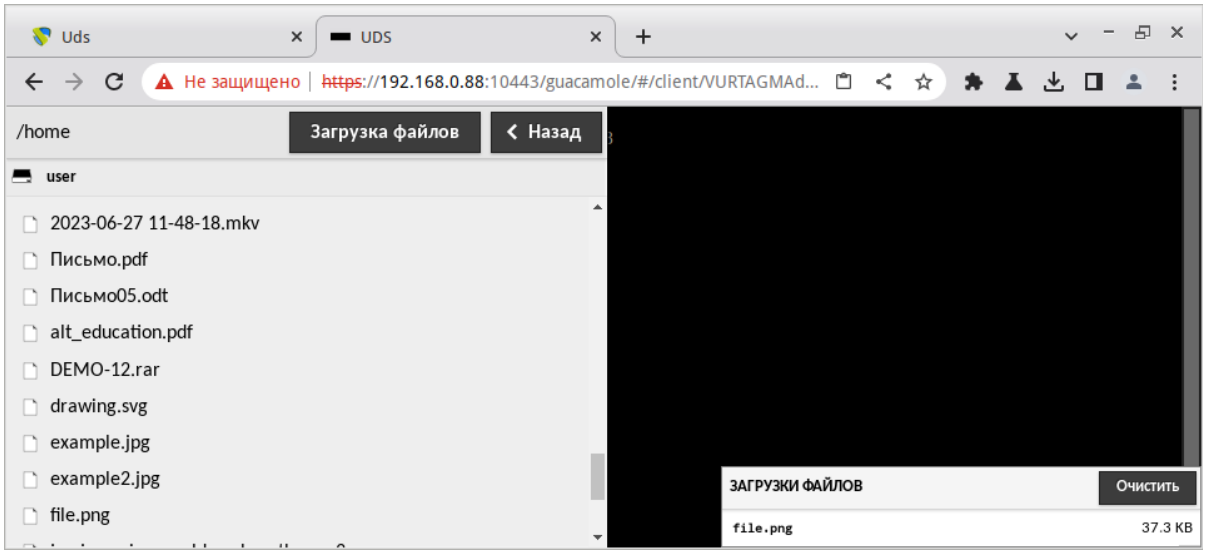


Рис. 261

5.11.3.5 Сети

В OpenUDS можно зарегистрировать различные сети для управления доступом клиентов к виртуальным рабочим столам или приложениям. Эти сети совместно с транспортом будут определять, какой тип доступа будет доступен пользователям для подключения к виртуальным рабочим столам.

В разделе «Сети» нажать кнопку «Новый» (Рис. 262).

OpenUDS. Добавить новую сеть

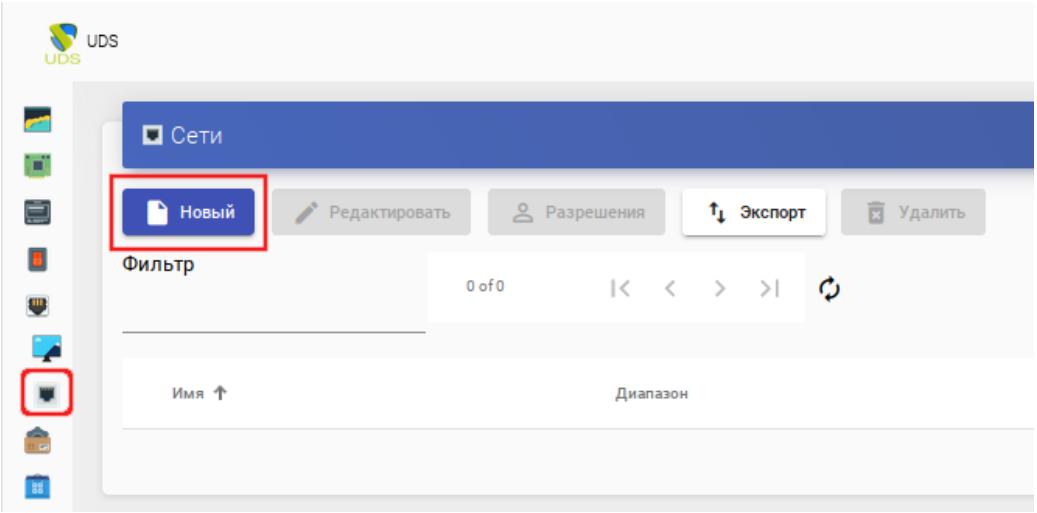


Рис. 262

В открывшемся окне (Рис. 263) следует указать название сети и сетевой диапазон. В качестве сетевого диапазона можно указать:

- одиночный IP-адрес: xxx.xxx.xxx.xxx (например, 192.168.0.33);
- подсеть: xxx.xxx.xxx.xxx/x (например, 192.168.0.0/24);
- диапазон IP-адресов: xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx (например, 192.168.0.1-192.168.0.50).

OpenUDS. Новая сеть

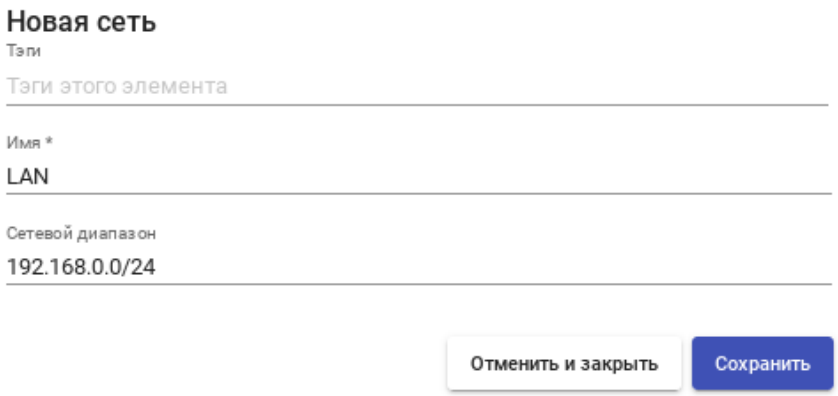


Рис. 263

После создания сетей появится возможность указать их при создании/редактировании транспорта. Можно настроить, будет ли данный транспорт отображаться у клиента, в зависимости от сети, в которой находится клиент. Если сети для транспорта не определены, доступ к службам рабочего стола и виртуальным приложениям будет возможен из любой сети.

5.11.3.6 Пулы услуг

После того, как был создан и настроен хотя бы один поставщик услуг с соответствующей службой/услугой, аутентификатор (с пользователем и группой), менеджер ОС и транспорт, можно создать пул услуг («Сервис-пул») для публикации виртуальных рабочих столов.

В разделе «Сервис-пулы» нажать кнопку «Новый» (Рис. 264).

OpenUDS. Новый пул услуг

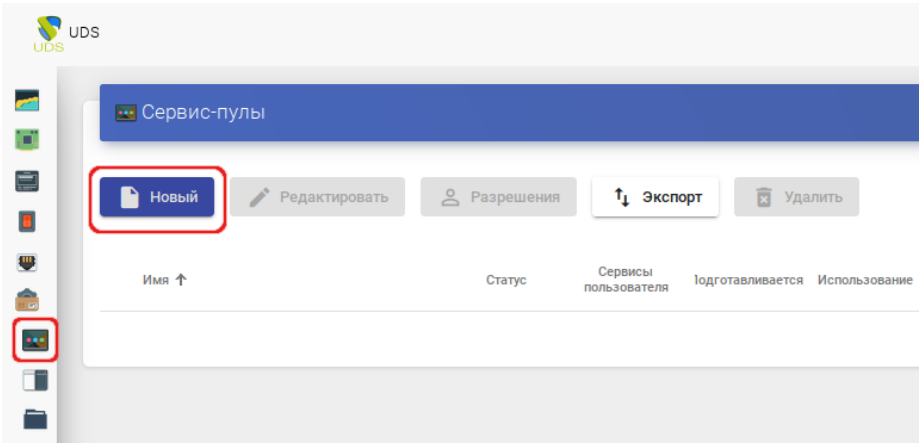


Рис. 264

Заполнить параметры конфигурации:

- вкладка «Основной» (Рис. 265):
  - «Имя» – название службы (это имя будет показано пользователю для доступа к рабочему столу или виртуальному приложению). В этом поле можно использовать переменные для отображения информации об услугах:
    - `{use}` – указывает процент использования пула (рассчитывается на основе поля «Максимальное количество предоставляемых сервисов» и назначенных услуг);
    - `{total}` – общее количество машин (данные извлечены из поля «Максимальное количество предоставляемых сервисов»);
    - `{usec}` – количество машин, используемых пользователями в пуле;
    - `{left}` – количество машин, доступных в пуле для подключения пользователей;
  - «Базовый сервис» – служба, созданная ранее в поставщике услуг (состоит из поставщика услуг и базовой услуги);
  - «ОС Менеджер» – ранее созданный менеджер ОС, конфигурация которого будет применяться к каждому из созданных виртуальных рабочих столов или приложений. Если выбрана услуга типа «Статический IP», это поле не используется;
  - «Публиковать при создании» – если этот параметр включен, при сохранении пула услуг система автоматически запустит первую публикацию. Если установлено значение «Нет», будет необходимо запустить публикацию сервиса вручную (из вкладки «Публикации»);
- вкладка «Экран/Дисплей» (Рис. 266):
  - «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»;
  - «Доступ к календарю запрещён» – позволяет указать сообщение, которое будет показано пользователю, если доступ к сервису ограничен правилами календаря;
- вкладка «Расширенный» (Рис. 267):
  - «Разрешить удаление пользователями» – если этот параметр включен, пользователи могут удалять назначенные им службы. Если сервис представляет собой виртуальный рабочий стол, автоматически сгенерированный OpenUDS, он будет удален, и при следующем

подключении ему будет назначен новый. Если это другой тип сервиса (vAPP/статический IP), будет удалено только назначение, а новое будет назначено на следующее подключение;

- «Разрешить сброс пользователями» – если этот параметр включен, пользователь сможет перезапускать или сбрасывать назначенные ему службы (относится только к виртуальным рабочим столам, автоматически созданным OpenUDS);
- «Игнорирует неиспользуемые» – если этот параметр включен, непостоянные пользовательские службы, которые не используются, не будут удаляться;
- «Показать транспорты» – если этот параметр включен, будут отображаться все транспорты, назначенные услуге. Если параметр не активирован, будет отображаться только транспорт по умолчанию (с наивысшим приоритетом);
- «Учетные записи» – назначение услуги ранее созданным «Аккаунтам» («Пулы» → «Аккаунты»);

- вкладка «Доступность» (Рис. 268):
  - «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);
  - «Сервисы, хранящиеся в L2 кэше» – количество виртуальных рабочих столов в спящем или выключенном состоянии. Виртуальные рабочие столы, сгенерированные на уровне кэша L2, будут помещены в кэш, как только система потребует их (они никогда не будут напрямую назначены пользователям);
  - «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 «Основной»

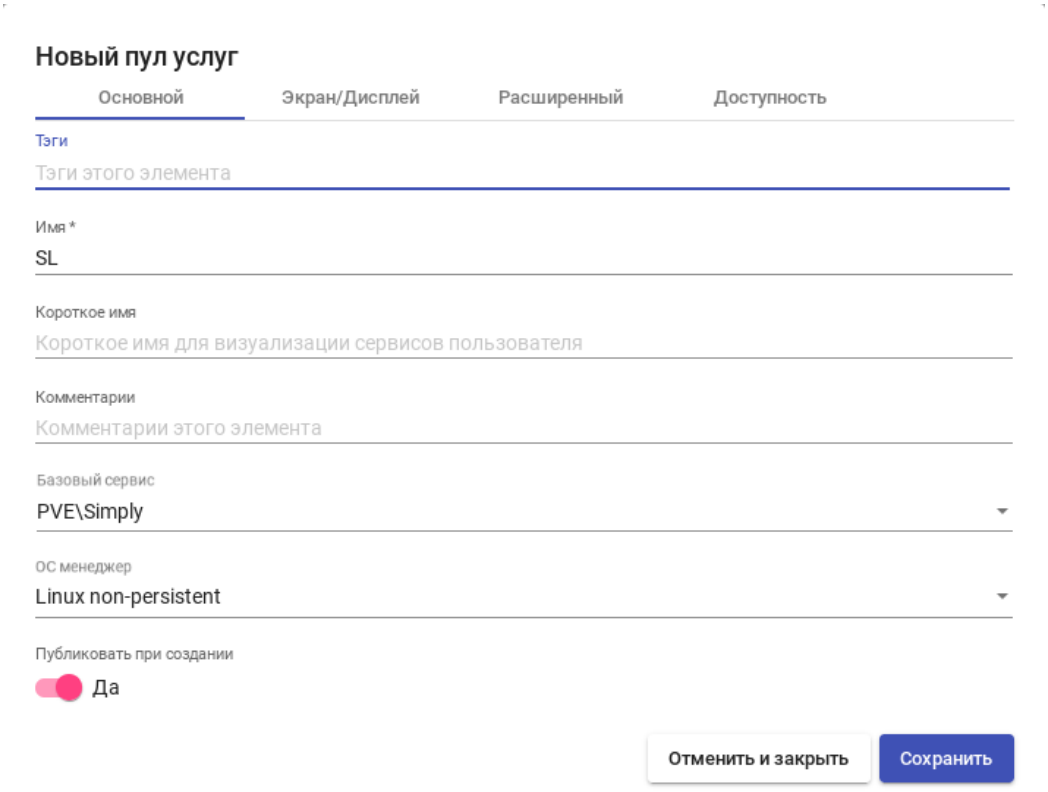


Рис. 265

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

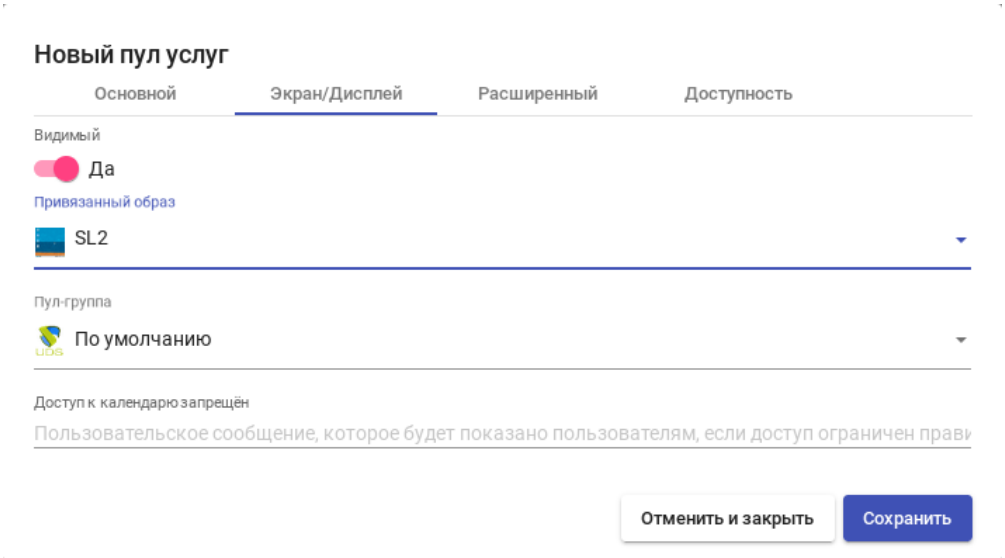


Рис. 266

OpenUDS. Новый Service Pool. Вкладка «Расширенный»

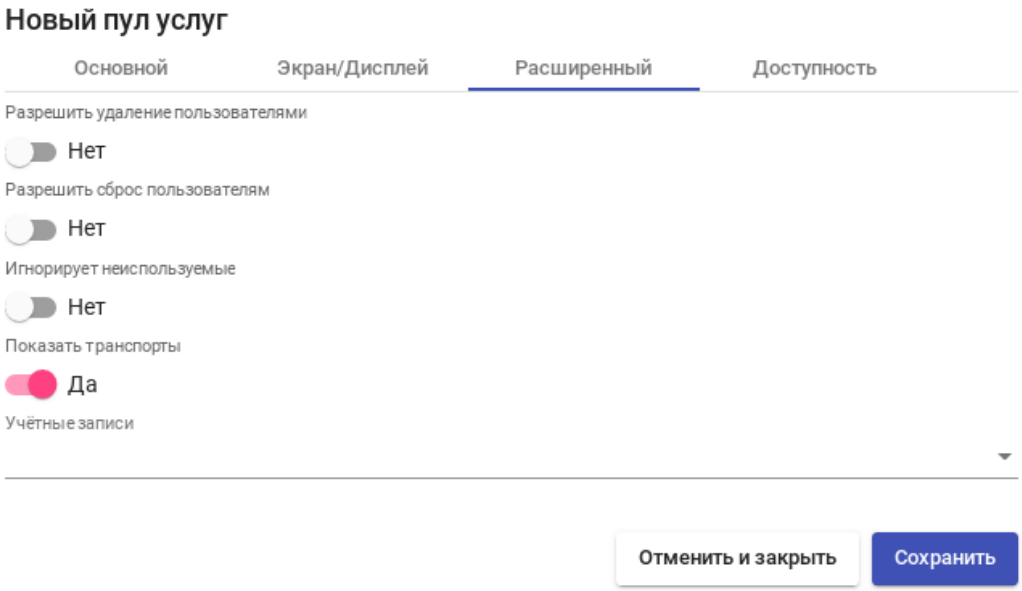


Рис. 267

OpenUDS. Новый Service Pool. Вкладка «Доступность»

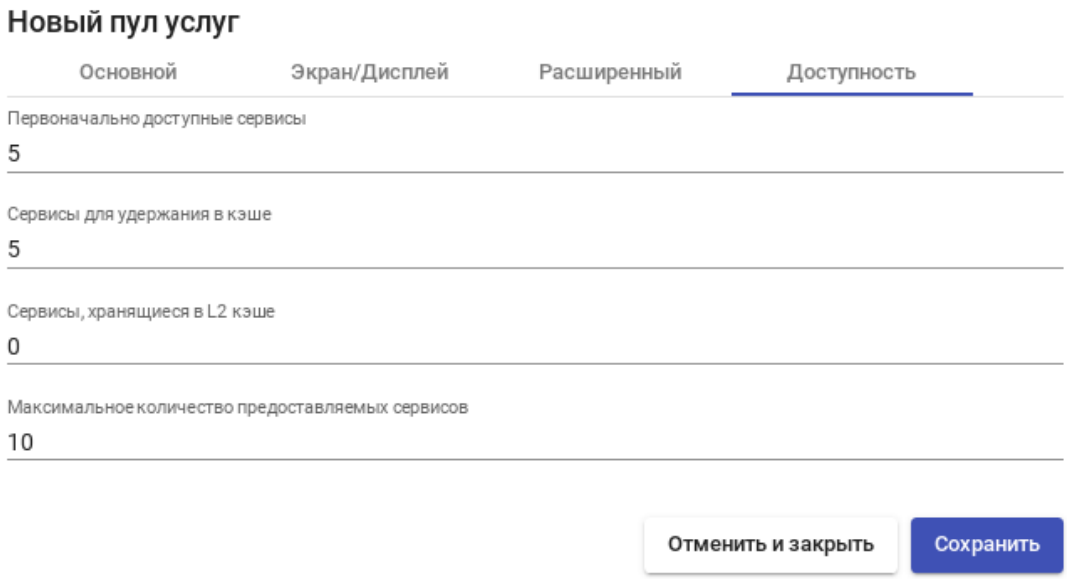


Рис. 268

После нажатия кнопки «Сохранить» и система начнет создавать виртуальные рабочие столы на основе настроенного кэша.

После создания пула, в настройках (дважды щелкнуть мышью по строке созданного пула или в контекстном меню пула выбрать пункт «Подробность»):

- на вкладке «Группы» (Рис. 269) назначить группы доступа (выбрать аутентификатор и группу, которая будет иметь доступ к этому пулу служб).

- на вкладке «Транспорты» (Рис. 270) выбрать способы подключения пользователей к рабочему столу.

OpenUDS. Назначение группы пулу служб

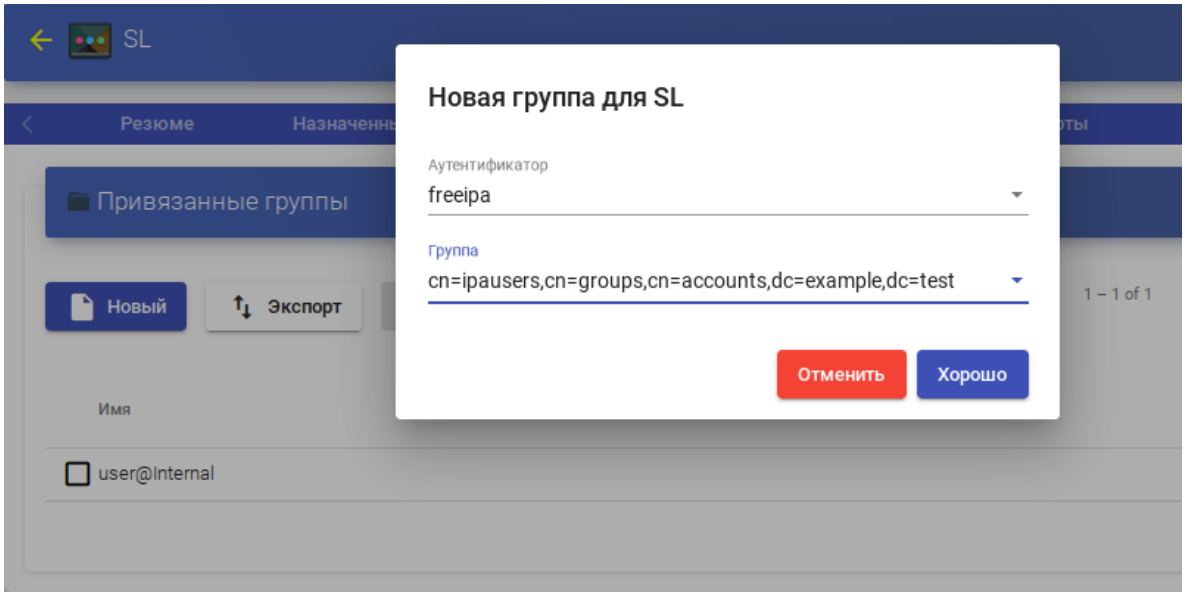


Рис. 269

OpenUDS. Выбор способов подключения к пулу служб

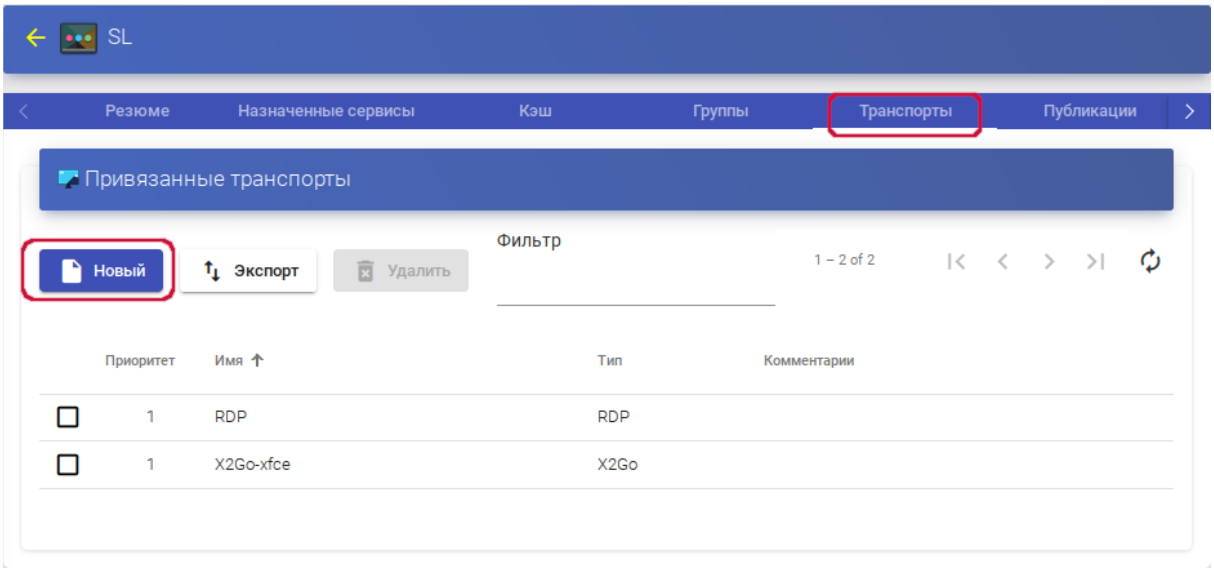


Рис. 270

5.11.3.7 Мета-пулы

Виртуальные рабочие столы можно сгруппировать в пулы рабочих столов («Мета-пулы»), что упрощает управление и организацию. Создание «Мета-пула» позволит получить доступ к виртуальным рабочим столам или приложениям из разных «Пулов услуг». Эти пулы будут работать вместе, предоставляя различные услуги абсолютно прозрачным для пользователей способом.

Пулы услуг, образующие «Мета-пул», будут работать в соответствии с политикой, которая позволит предоставлять услуги в соответствии с потребностями пула.

Чтобы создать «Мета-пул», необходимо в разделе «Мета-пулы» нажать кнопку «Новый» (Рис. 271).

OpenUDS. Новый «Мета-пул»

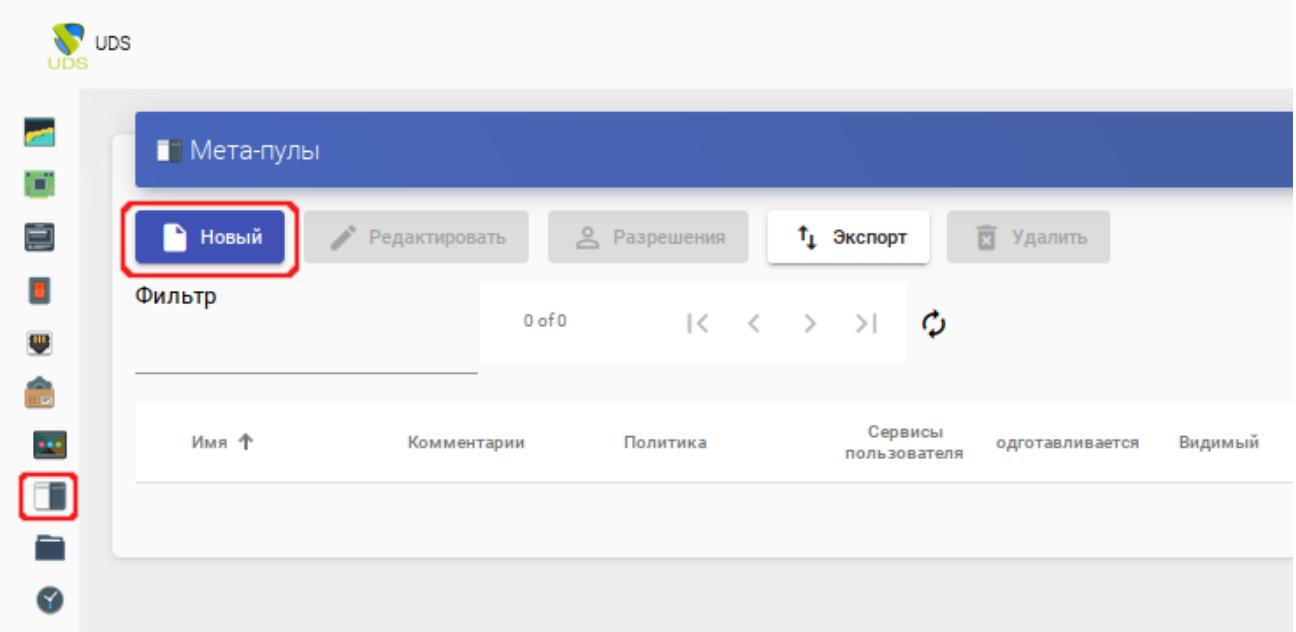


Рис. 271

Заполнить параметры конфигурации:

- вкладка «Основной» (Рис. 272):
  - «Имя» – мета-пула (это будет видеть пользователь для доступа к службе);
  - «Короткое имя» – если указано, то это будет видеть пользователь для доступа к службе (при наведении на него указателя появится содержимое поля «Имя»);
  - «Политика» – политика, которая будет применяться при создании сервисов в пулах услуг, являющихся частью мета-пула:
    - «Eventy distributed» – услуги будут создаваться и использоваться равномерно во всех пулах услуг, составляющих мета-пул;
    - «Priority» – услуги будут создаваться и использоваться из пула услуг с наибольшим приоритетом (приоритет определяется значением поля «Приоритет», чем ниже значение этого поля, тем выше приоритет у элемента). Когда будет достигнуто максимальное количество сервисов данного пула услуг, будут использоваться сервисы следующего;
    - «Greater % available» – службы будут создаваться и использоваться из пула услуг, который имеет самый высокий процент свободных услуг;
- вкладка «Экран/Дисплей» (Рис. 273):

- «Привязанный образ» – изображение, связанное с мета-пулом. 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»;
- «Видимый» – если этот параметр отключен, пул не будет отображаться у пользователей;
- «Доступ к календарю запрещён» – позволяет указать сообщение, которое будет показано пользователю, если доступ к сервису ограничен правилами календаря;
- «Выбор транспорта» – указывает как на мета-пул будет назначен транспорт:
  - «Automatic selection» – будет доступен транспорт с самым низким приоритетом, назначенным пулу услуг. Выбор транспорта не допускается;
  - «Use only common transports» – в мета-пуле будет доступен транспорт, который является общим для всего пула услуг;
  - «Group Transports by label» – в мета-пуле будет доступен транспорт, которому назначены метки (это поле находится в настройках транспорта на вкладке «Дополнительно»).

После создания мета-пула, в настройках (дважды щелкнуть мышью по строке созданного пула или в контекстном меню пула выбрать пункт «Подробность») необходимо на вкладке «Пулы услуг» добавить пул услуг в мета-пул (Рис. 274).

OpenUDS. Новый мета-пул. Вкладка «Основной»

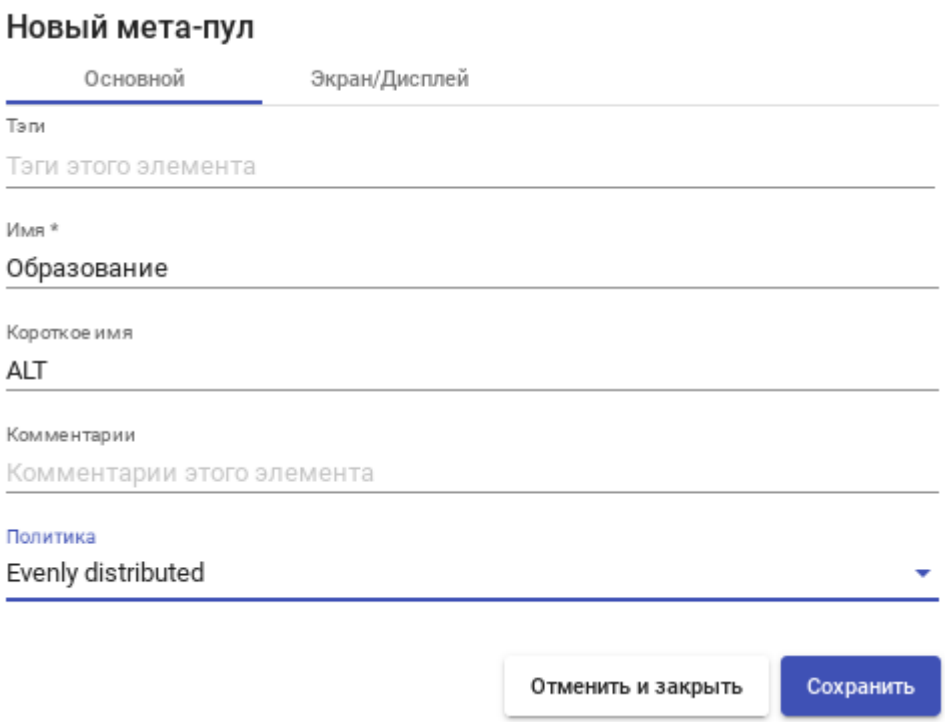


Рис. 272

OpenUDS. Новый мета-пул. Вкладка «Экран/Дисплей»

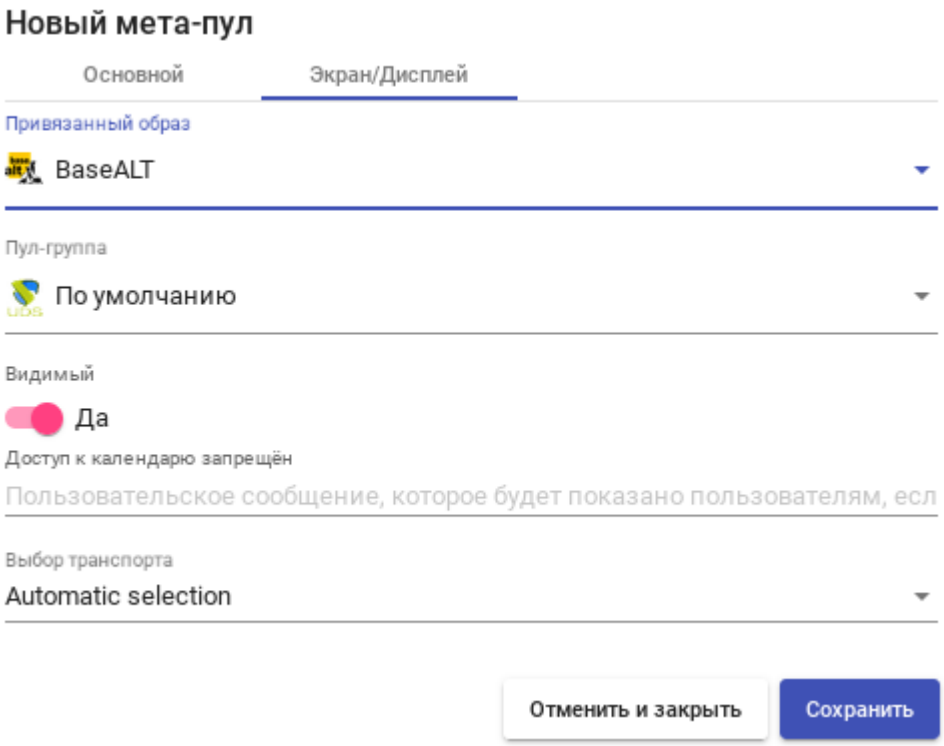


Рис. 273

OpenUDS. Добавление пула служб в мета-пул

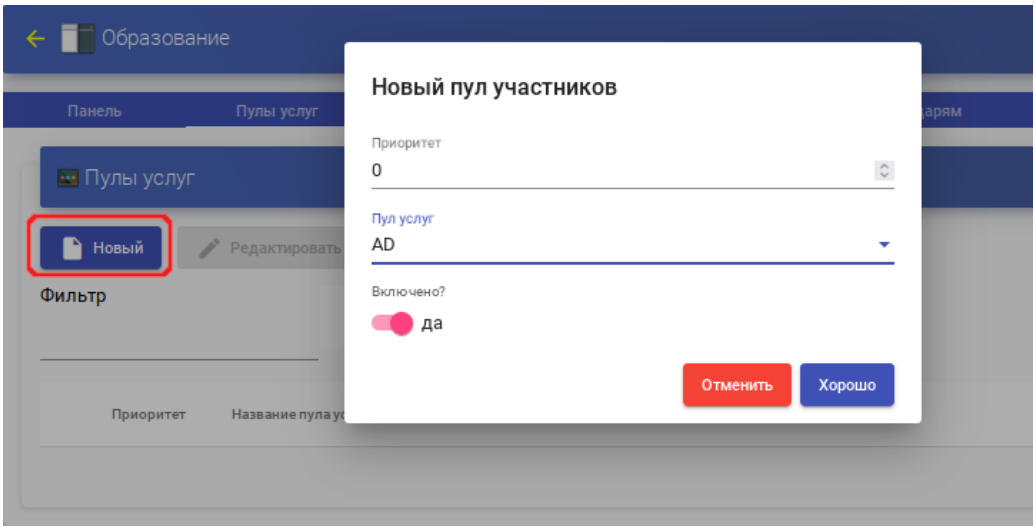


Рис. 274

Для добавления пула услуг необходимо указать:

- «Приоритет» – приоритет, который будет иметь данный пул услуг в мета-пуле (чем ниже значение, тем больше приоритет);
- «Пул услуг» – пул услуг, который будет добавлен в мета-пул (пул услуг должен быть предварительно создан);
- «Включено» – включает или отключает видимость пула услуг в мета-пуле.

Можно добавить столько пулов услуг, сколько необходимо, комбинируя службы, размещенные на разных платформах виртуализации (PVE, KVM, OpenNebula и т.д.), серверах приложений и статических устройствах.

Как и при создании пула услуг, здесь есть следующие вкладки с информацией и конфигурацией:

- «Назначенные сервисы» – показывает службы, назначенные пользователям (можно вручную удалить назначение и переназначить другому пользователю);
- «Группы» – указывает, какие группы пользователей будут иметь доступ к услуге;
- «Доступ к календарю» – позволяет применить ранее созданный календарь доступа;
- «Журналы» – журналы мета-пула.

5.11.3.8 Управление доступом по календарю

В OpenUDS можно настроить ограничение доступа пользователей к удаленным рабочим столам и виртуальным приложениям по дате и времени.

С помощью календаря также можно автоматизировать определенные задачи в «Пуле-услуг», такие как создание новых публикаций, настройка значений системного кэша, добавление/удаление групп и транспорта, изменение максимального количества услуг.

Чтобы создать календарь, следует в разделе «Календари» нажать кнопку «Новый», в открывшемся окне ввести описательное название в поле «Имя» и нажать кнопку «Сохранить» (Рис. 275).

OpenUDS. Новый календарь

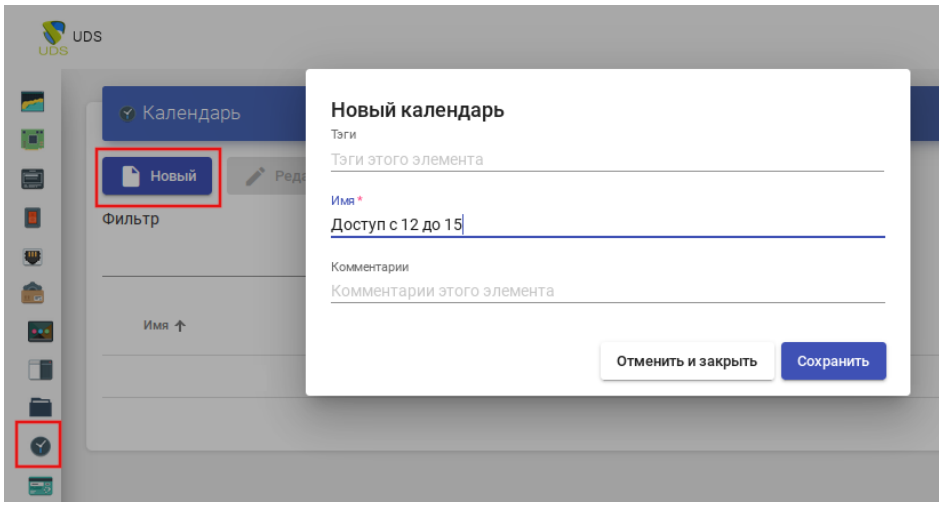


Рис. 275

В «Календаре» можно зарегистрировать правила, чтобы запланировать доступность услуги в определенное время. Для создания правила следует выбрать календарь (дважды щелкнуть мышью по строке созданного календаря или в контекстном меню календаря выбрать пункт «Подробность») и нажать кнопку «Новый» (Рис. 276).

OpenUDS. Создать новое правило

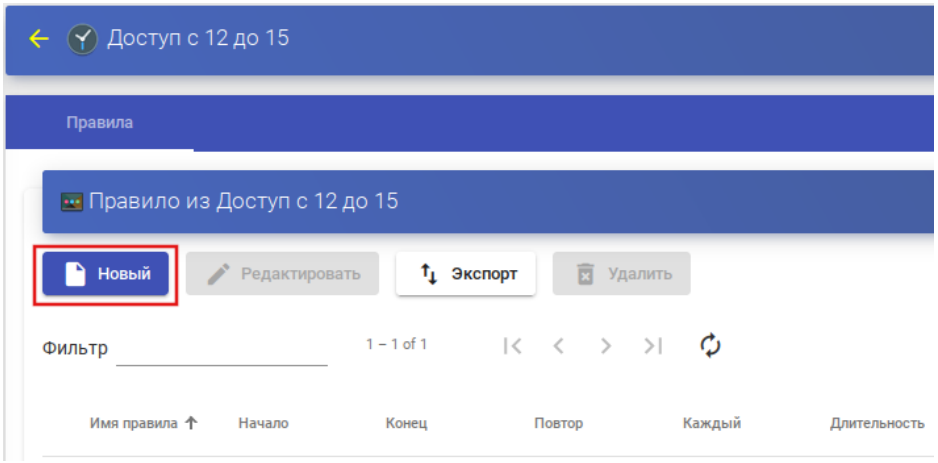


Рис. 276

Минимальные параметры для настройки правила (Рис. 277):

- «Имя» – название правила;
- «Событие» – настройка времени выполнения. Необходимо указать время начала и продолжительность события (в минутах/часах/днях/неделях);
- «Repetition» («Периодичность») – настройка периодичности выполнения. Необходимо указать дату начала, частоту повторения правила (ежедневно/еженедельно/ежемесячно/ежегодно/по будням) и указать интервал повторения (в днях);
- «Панель» – показывает сводные данные (резюме) всех ранее указанных настроек.

OpenUDS. Создание правила

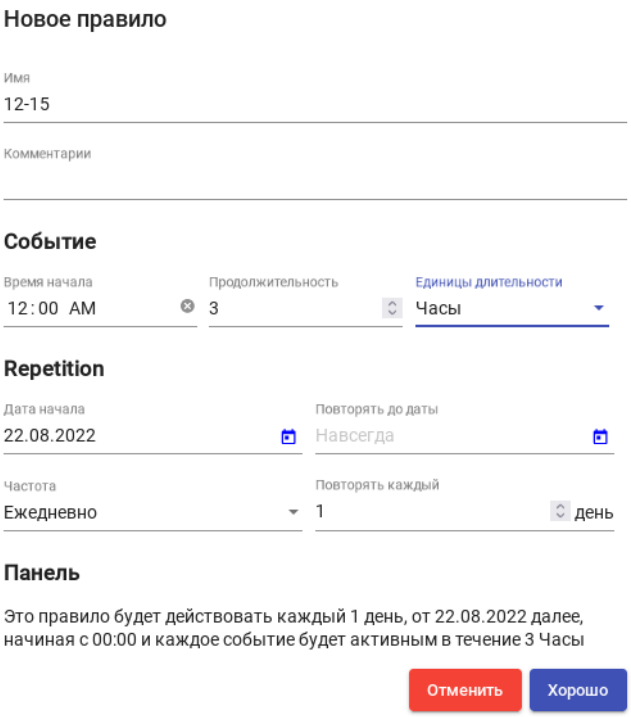


Рис. 277

После нажатия кнопки «Хорошо» будет создано правило (Рис. 278), которое будет назначено «Пулу услуг» (виртуальному рабочему столу и/или приложению).

OpenUDS. Список правил

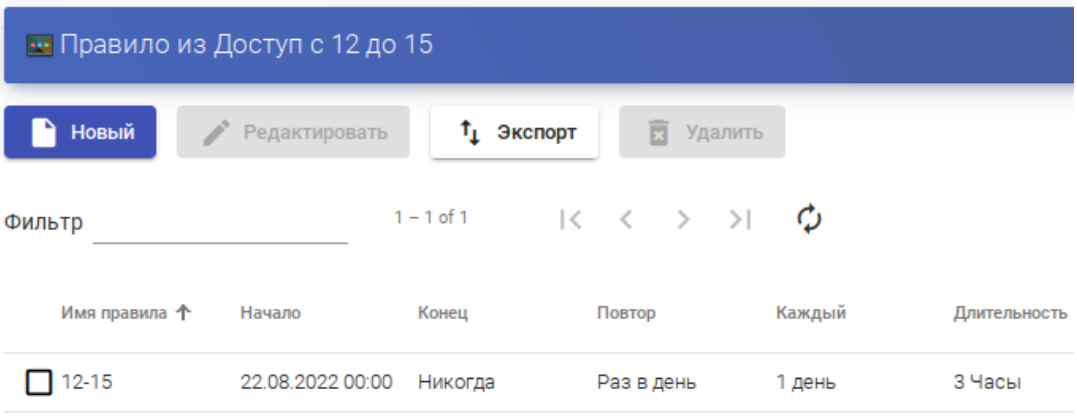


Рис. 278

5.11.3.8.1 Разрешение/запрет доступа

После настройки правил в календарях их можно использовать для управления доступом пользователей к службам рабочего стола или приложениям. Для этого следует выбрать «Пул услуг», перейти на вкладку «Доступ к календарям» и нажать кнопку «Новый» (Рис. 279). В открывшемся окне необходимо указать приоритет доступа, выбрать календарь и указать действие, которое будет применяться при доступе к пулу (Рис. 280).

Примечание. Правило по умолчанию («FallBack») должно разрешать или запрещать доступ к сервису, когда календарь не применяется (Рис. 281).

OpenUDS. Создать новое правило доступа

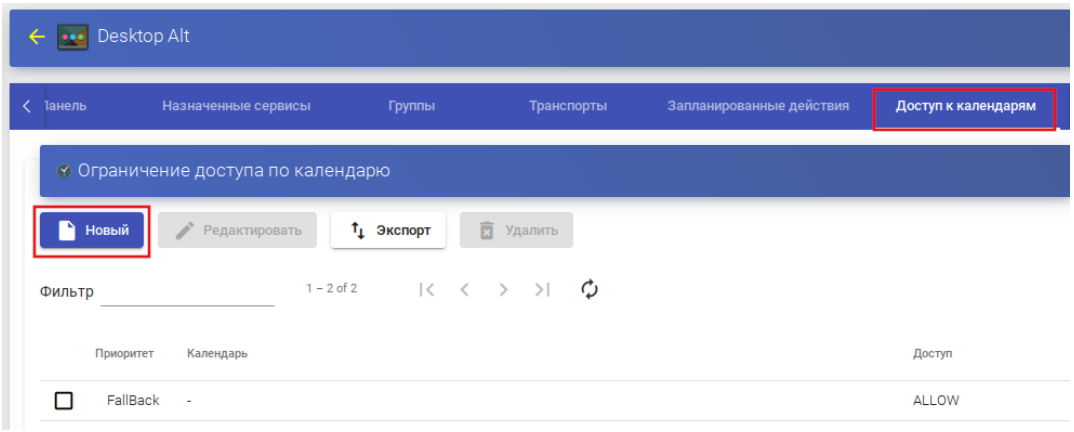


Рис. 279

OpenUDS. Новое правило доступа

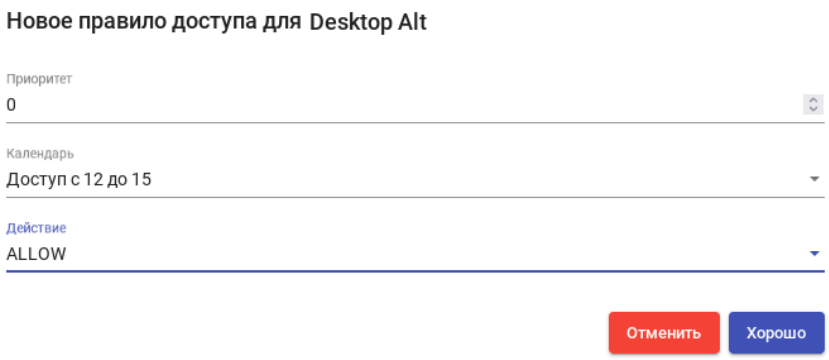


Рис. 280

OpenUDS. Ограничение доступа к пулу по календарю

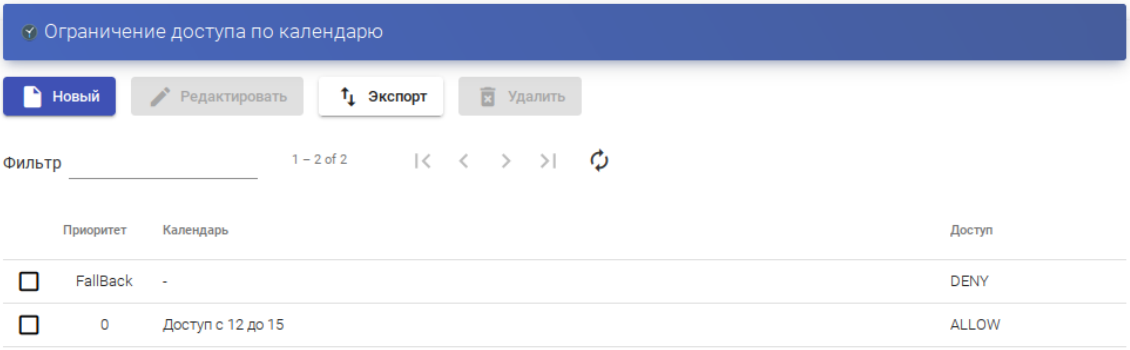


Рис. 281

5.11.3.8.2 Запланированные действия

После настройки правил в календарях их можно использовать для планирования определенные задач в «Пуле услуг». Для этого следует выбрать нужный «Пул услуг», перейти на вкладку «Запланированные действия» и нажать кнопку «Новый» (Рис. 282).

OpenUDS. Вкладка «Запланированные действия»

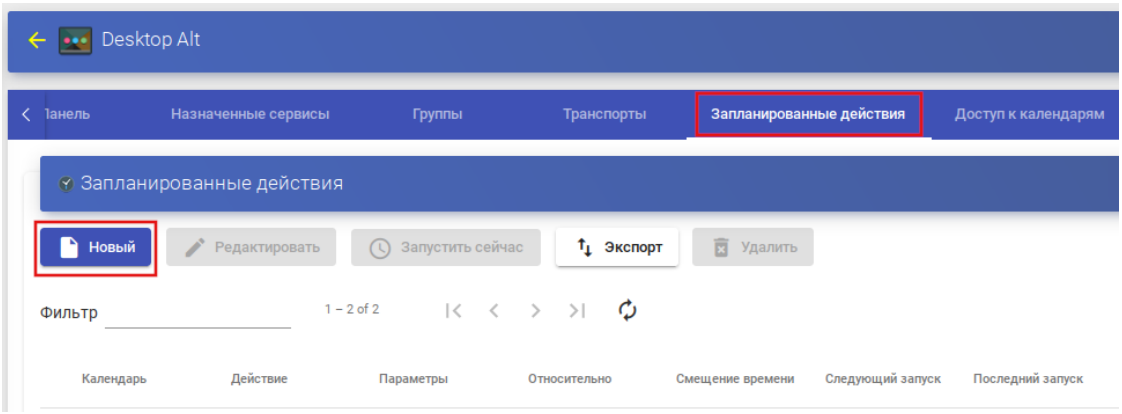


Рис. 282

В открывшемся окне (Рис. 283) необходимо указать календарь, время, в течение которого будет выполняться действие, выбрать действие, которое необходимо выполнить (список возможных действий зависит от поставщика услуг данного пула):

- «Установить начальные сервисы» – сбрасывает минимальное количество созданных и настроенных виртуальных рабочих столов;
- «Установить размер кеша» – сбрасывает виртуальные рабочие столы, доступные в системном кеше. Эти рабочие столы будут настроены и готовы к назначению пользователю;
- «Установить максимальное количество сервисов» – изменяет максимальное количество виртуальных рабочих столов в «Пуле услуг»;
- «Установить размер L2 кэша» – сбрасывает виртуальные рабочие столы, доступные в кэше L2;
- «Публикация» – создание новой публикации в «Пуле услуг»;
- «Добавить транспорт» – добавляет существующий транспорт в «Пул услуг»;
- «Удалить транспорт» – удаляет транспорт из «Пула услуг»;
- «Удалить все транспорты» – удаляет весь транспорт из «Пула услуг»;
- «Добавить группу» – добавляет существующую группу в «Пул услуг»;
- «Удалить группу» – удаляет группу из «Пула услуг»;
- «Удалить все группы» – удаляет все группы из «Пула услуг»;
- «Устанавливает игнорирование неиспользуемых» – устанавливает параметр «Игнорировать неиспользуемые»;
- «Удалить ВСЕ назначенные пользовательские сервисы» – удаляет все службы, назначенные пользователям;
- «Удалить СТАРЫЕ назначенные пользовательские сервисы» – удаляет службы, назначенные пользователям, которые не использовались заданное время.

После нажатия кнопки «Хорошо» будет создано правило (Рис. 278), которое будет назначено «пулу услуг» (виртуальному рабочему столу и/или приложению).

После сохранения появится запланированная задача, выполняющая конкретное действие в данном «Пуле услуг».

OpenUDS. Новое действие

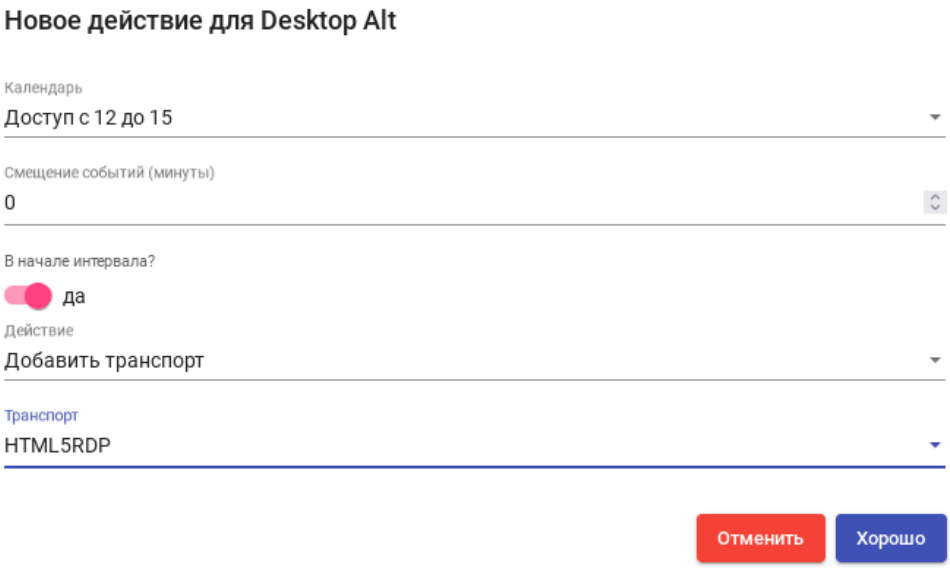


Рис. 283

5.11.3.9 Настройка разрешений

В OpenUDS можно назначать пользователям и группам пользователей права доступа к различным элементам администрирования. Разрешения будут назначены непосредственно для каждого элемента, а также будут применяться к его подэлементам.

Примечание. Чтобы пользователь мог получить доступ к администрированию, ему должна быть назначена роль «Штатный сотрудник» (Рис. 284).

OpenUDS. Роль пользователя

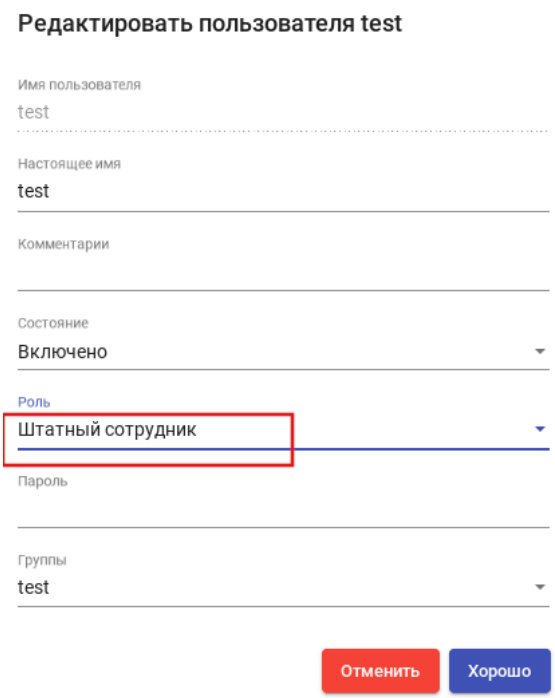


Рис. 284

Для предоставления разрешения к элементу администрирования следует выбрать элемент и нажать кнопку «Разрешения». Например, на Рис. 285 показано предоставление разрешения к сервису «Desktop Alt».

В окне разрешений следует нажать ссылку «Новое разрешение...» для групп или пользователей, выбрать аутентификатор и группу/пользователя, к которым будет применяться разрешение (Рис. 286). Нужно также указать, будет ли пользователь/группа иметь доступ для чтения к элементу («Только чтение») или полный доступ («Полный доступ»).

OpenUDS. Предоставление разрешения к сервису «Desktop Alt»

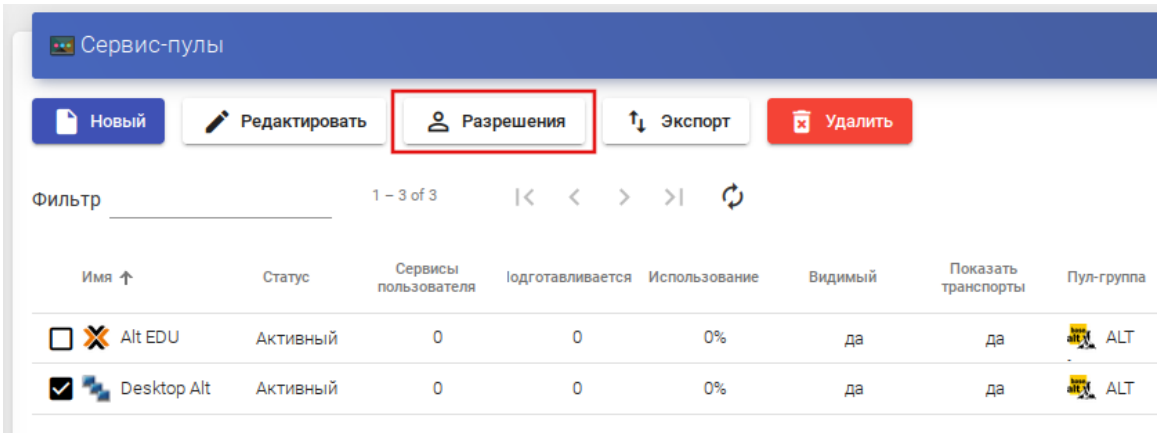


Рис. 285

OpenUDS. Новое разрешение для «Desktop Alt»

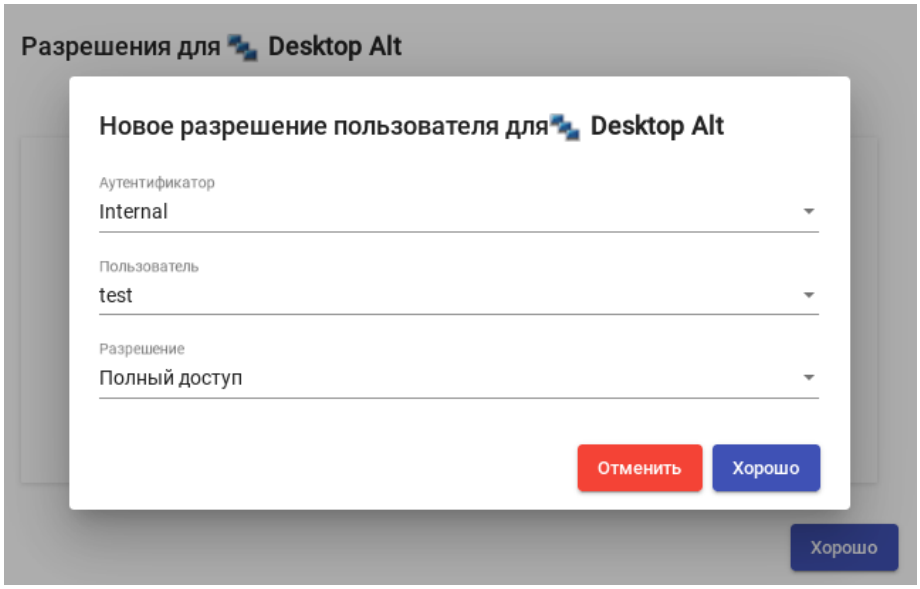


Рис. 286

После сохранения настроек, пользователи, которым назначена роль «Штатный сотрудник», смогут получить доступ к этому элементу администрирования с назначенными разрешениями.

Примечание. Разрешения типа «Полный доступ» («Управление») могут применяться только к элементам второго уровня («Календари», «Пулы услуг» и т. д.).

5.11.3.10 Конфигурация OpenUDS

В разделе «Конфигурация» (Рис. 287) можно настроить ряд параметров, которые будут определять работу системы. Эти параметры отвечают за определение таких аспектов, как безопасность, режим работы, подключение и т.д. как самой системы OpenUDS, так и её связи с виртуальными платформами, зарегистрированными в OpenUDS.

Примечание. В данном разделе описаны некоторые системные переменные для управления виртуальными рабочими столами. Не рекомендуется изменять значения других переменных, так как некоторые из них указывают системе, как она должна работать (количество одновременных задач, время выполнения задач, плановые проверки и т.д.). Изменение этих параметров может привести к неправильной работе или к полной остановке системы.

Примечание. Для применения изменений, после редактирования значений любой из переменных конфигурации OpenUDS, необходимо перезапустить сервер OpenUDS.

OpenUDS. Раздел «Конфигурация»

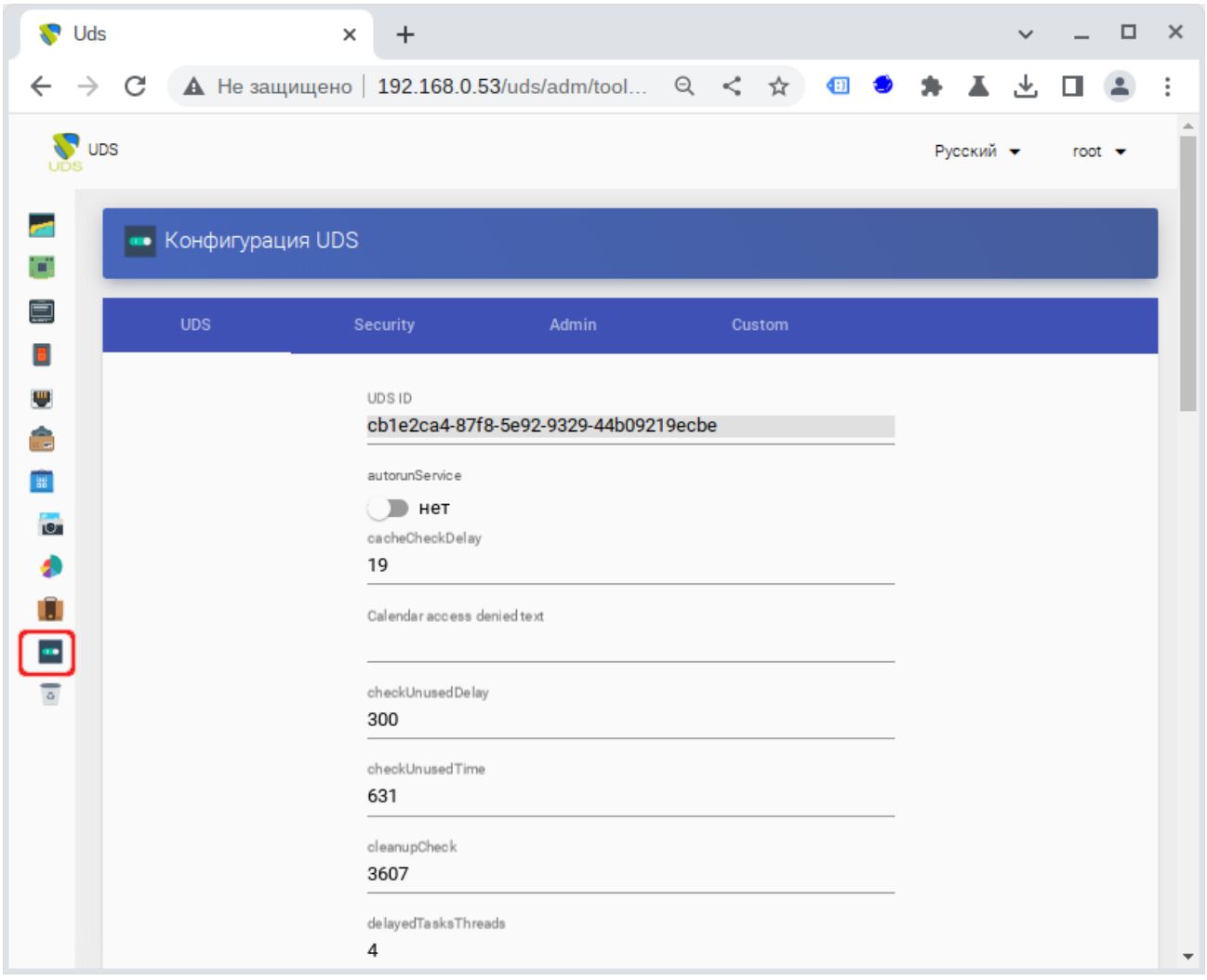


Рис. 287

Некоторые параметры конфигурации:

- вкладка «UDS»:
  - «autorunService» – выполнять прямой доступ к службе пользователя, если пользователю назначена только одна служба. Если этот параметр активирован, пользователи, которым назначен один сервис, будут подключаться к нему напрямую, минуя экран выбора сервиса и используя предварительно настроенный «Транспорт». По умолчанию: нет;
  - «disallowGlobalLogin» – если включено, на странице входа не будет отображаться список аутентификаторов. В этом случае будет использоваться аутентификатор по умолчанию. Для предоставления пользователю доступа к системе с помощью других аутентификаторов необходимо использовать «Метку», определенную в аутентификаторе, в URL-адресе доступа. По умолчанию: нет;
  - «keepinfoTime» – время (в секундах), в течение которого завершенные события «пула услуг» остаются видимыми. По умолчанию: 14401 секунд (4 часа);
  - «redirectToHttps» – автоматически перенаправлять доступ к OpenUDS с http на https. По умолчанию: нет;
  - «sessionExpireTime» – максимальное время, в течение которого сеанс пользователя будет открыт после создания новой публикации. По истечении этого времени система закроет сеанс пользователя и продолжит удаление службы. Если у службы есть «Менеджер ОС» с параметром «Держать сервис привязанным даже в новой публикации», этот параметр не будет применяться. По умолчанию: 24 часа;
  - «statsDuration» – время, в течение которого система хранит статистику. По умолчанию: 365 дней;
- вкладка «Security»:
  - «allowRootWebAccess» – разрешить суперпользователю (пользователю, созданному при разворачивании OpenUDS-сервера) входить в панель управления OpenUDS. По умолчанию: да;
  - «Behind a proxy» – указывает системе, что серверы OpenUDS находятся «за» прокси-сервером (например, среда OpenUDS с HA Proxy). По умолчанию: нет;
  - «Block ip on login failure» – заблокировать пользователя при неправильном вводе пароля (также блокируется IP-адрес). Количество попыток указывается в переменной `maxLoginTries`. По умолчанию: нет
  - «Enforce Zero-Trust Mode» – включение режима нулевого доверия (запретить системе хранить пароли). По умолчанию: нет;

- «loginBlockTime» – время (в секундах), в течение которого после неправильного ввода пароля пользователь будет заблокирован. Количество попыток указывается в переменной `maxLoginTries`. По умолчанию: 300 секунд (5 минут);
- «maxLoginTries» – количество попыток, за которые пользователь должен ввести свой пароль, прежде чем система заблокирует его;
- «Session timeout for Admin» – время бездействия (в секундах) для администраторов платформы. По умолчанию: 14400 секунд (4 часа);
- «Session timeout for User» – время бездействия (в секундах) для пользователей. По умолчанию: 14400 секунд (4 часа);
- «Trusted Hosts» – узлы, которые OpenUDS считает безопасными. Эти узлы могут делать «sensitive» запросы к OpenUDS. Допустимые значения: подсеть, диапазон IP-адресов, конкретные IP-адреса. По умолчанию: «*» (всё разрешено);

- вкладка «Admin»:
  - «Trusted Hosts for Admin» – узлы, с которых можно управлять OpenUDS (как с помощью веб-доступа, так и администрирование с помощью API). Допустимые значения: подсеть, диапазон IP-адресов, конкретные IP-адреса. По умолчанию: «*» (всё разрешено);
- вкладка «Custom» (параметры, связанные с графической настройкой OpenUDS):
  - «CSS» – CSS код для изменения стиля страниц OpenUDS;
  - «Logo name» – текст, который отображается рядом с логотипом;
  - «Min. Services to show filter» – минимальное количество служб, которые должны существовать у пользователя (в режиме пользователя), чтобы отображался фильтр;
  - «Show Filter on Top» расположение панели поиска на странице пользовательских служб;
  - «Site copyright info» – максимальное время, в течение которого сеанс пользователя будет открыт после создания новой публикации. По истечении этого времени система закроет сеанс пользователя и продолжит удаление службы. Если у службы есть «Менеджер ОС» с параметром «Держать сервис привязанным даже в новой публикации», этот параметр не будет применяться. По умолчанию: 24 часа;
  - «Site copyright link » – веб-адрес, на который будет вести ссылка с копирайта;
  - «Site information» – HTML-код для частичной настройки страницы входа в OpenUDS. Введенный код появится под полем входа пользователя;
  - «Site name » – текст, который будет отображаться в верхней части поля входа пользователя на странице входа OpenUDS.

5.11.4 Подготовка шаблона виртуальной машины

Для возможности использования ВМ в качестве шаблона OpenUDS, на машине необходимо включить и настроить удаленный рабочий стол, установить OpenUDS Actor и зарегистрировать его на сервере OpenUDS.

5.11.4.1 Шаблон ВМ с ОС Альт

Подготовить шаблон ВМ (все действия выполняются на 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. 288) указать:
  - «SSL Validation» – уровень безопасности для связи с сервером OpenUDS;
  - «UDS Server» – имя или IP-адрес сервера OpenUDS;
  - «Authenticator» – аутентификатор, которому принадлежит указанный пользователь-администратор (аутентификатор Administration соответствует суперпользователю). Чтобы отображались различные аутентификаторы, должна быть установлена связь с сервером OpenUDS;
  - «Username» – имя пользователя, имеющего права администратора в среде OpenUDS (должен принадлежать аутентификатору, выбранному в поле Authenticator);
  - «Password» – пароль пользователя;
- нажать кнопку «Register with UDS» («Зарегистрироваться в UDS»);
- на вкладке «Advanced» можно указать дополнительные параметры:
  - «Preconnect» – сценарий, который будет запущен непосредственно перед тем, как пользователь подключится к виртуальному рабочему столу. Брокер OpenUDS автоматически передаёт следующие параметры: имя пользователя, протокол, IP-адрес клиента, имя хоста клиента, которые можно использовать в скрипте;
  - «Runonce» – сценарий, который будет запущен только один раз перед настройкой UDS Actor. После выполнения скрипт удаляется из конфигурации. Параметры можно передать непосредственно скрипту. Необходимо, чтобы выполняемый скрипт завершился перезапуском виртуального рабочего стола;

- «Postconfig» – сценарий, который будет запущен после того, как UDS Actor завершит настройку. Параметры можно передать непосредственно скрипту. Скрипт запускается только один раз, но в отличие от режима Runonce перезапускать виртуальный рабочий стол не нужно;
- «Log Level» – уровень журналирования;

Для применения настроек указанных на этой вкладке необходимо выполнить перерегистрацию UDSActor.

OpenUDS. UDS Actor Configuration

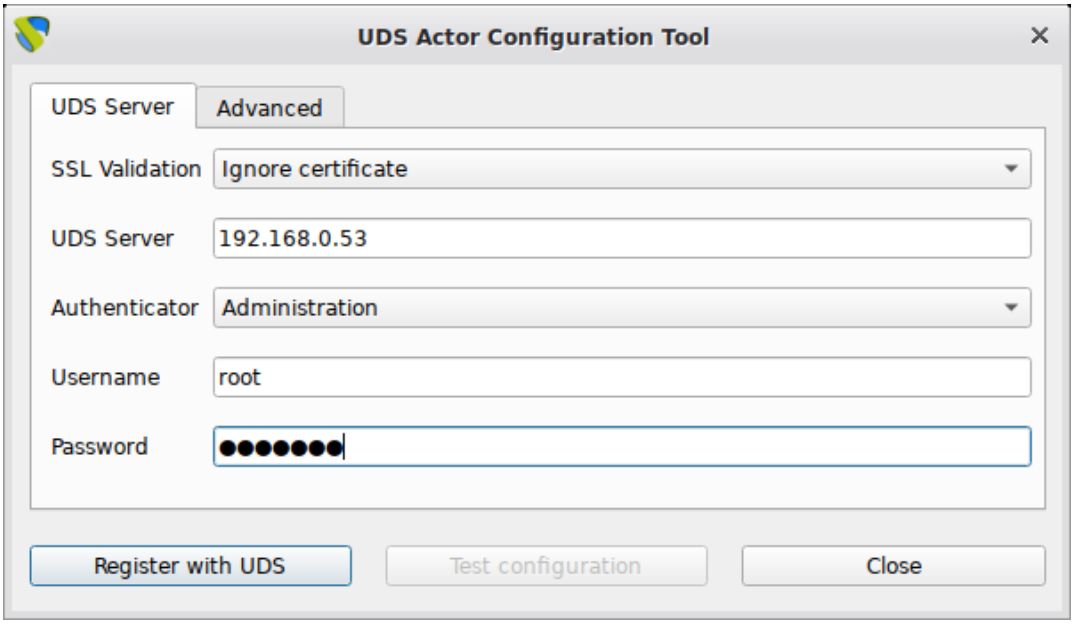


Рис. 288

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
```

Зарегистрировать UDS Actor можно в командной строке, например:

```
# UDSActorRegister
SSL validation (yes/no): no
Hostname: 192.168.0.53
Authenticator ['Internal', 'radiusauth', 'freeipa', 'AD', 'admin']:
admin
Username: root
Password:
Pre connect:
Run once:
Post config:
Log level ['debug', 'info', 'error', 'fatal']: error
Registration with UDS completed.
```

Можно также использовать переменные окружения, например:

```
# export OPENUDS_ACTOR_SSL_VALIDATION=no
# export OPENUDS_HOST=192.168.0.53
# export OPENUDS_AUTHENTICATOR=admin
# export OPENUDS_ACTOR_POST_CONFIG=/home/user/test.sh
# export OPENUDS_ACTOR_LOG_LEVEL=error
# UDSActorRegister
Username: root
Password:
Pre connect:
Run once:
Registration with UDS completed.
```

При регистрации в командной строке необходимо указать (в скобках приведены соответствующие переменные окружения):

- SSL Validation – уровень безопасности для связи с сервером OpenUDS (OPENUDS_ACTOR_SSL_VALIDATION);
- Hostname – имя или IP-адрес сервера OpenUDS (OPENUDS_HOST);
- Authenticator – аутентификатор, которому принадлежит пользователь-администратор (OPENUDS_AUTHENTICATOR). Аутентификатор «admin» соответствует суперпользователю, другие типы аутентификаторв будут присутствовать в списке, если настроены в брокере. Чтобы отображались возможные аутентификаторы, должна быть установлена связь с сервером OpenUDS;

- Username – имя пользователя, имеющего права администратора в среде OpenUDS (OPENUDS_USERNAME);
- Password – пароль пользователя (OPENUDS_PASSWORD);
- Pre connect – сценарий в формате /path/to/script, который будет запущен непосредственно перед тем, как пользователь подключится к виртуальному рабочему столу (OPENUDS_ACTOR_PRE_CONNECT);
- Run once – сценарий в формате /path/to/script, который будет запущен только один раз перед настройкой UDS Actor (OPENUDS_ACTOR_RUN_ONCE);
- Post config – сценарий в формате /path/to/script, который будет запущен после того, как UDS Actor завершит настройку (OPENUDS_ACTOR_POST_CONFIG);
- Log Level – уровень журналирования (OPENUDS_ACTOR_LOG_LEVEL).

5.11.4.2 Шаблон ВМ с ОС Windows

Примечание. В данном разделе рассмотрен процесс настройки ВМ с ОС Windows x64 10 Pro для использования в качестве шаблона OpenUDS.

Требования к шаблону ВМ с ОС Windows:

- рекомендуется отключить автоматические обновления, чтобы предотвратить выполнение этого процесса на создаваемых виртуальных рабочих столах;
- машина должна получать IP-адрес по DHCP;
- шаблон не нужно добавлять в домен Active Directory. Если нужны виртуальные рабочие столы, включенные в домен AD, настройка должна быть выполнена в панели управления OpenUDS;
- автоматический вход пользователя должен быть отключён (учетные данные всегда должны запрашиваться у пользователя).

Примечание. Для возможности ввода ВМ в домен, в шаблоне ВМ должен быть доступен сервер DNS, имеющий записи про контроллер домена Active Directory.

Для настройки удаленного рабочего стола, необходимо выполнить следующие действия в шаблоне ВМ:

1. Открыть окно «Параметры» (<Win>+<I>).
2. Выбрать раздел «Система», а затем слева в списке – «Удаленный рабочий стол».
3. Ползунок «Включить удаленный рабочий стол установить» установить в положение «Вкл.» (Рис. 289).
4. Выбрать учетные записи, которым разрешено удаленное подключение. Для этого нажать ссылку «Выберите пользователей, которые могут получить доступ к этому компьютеру» и добавить пользователей (Рис. 290).
5. Проверить возможность подключения к машине удаленно.

Включить удаленный рабочий стол

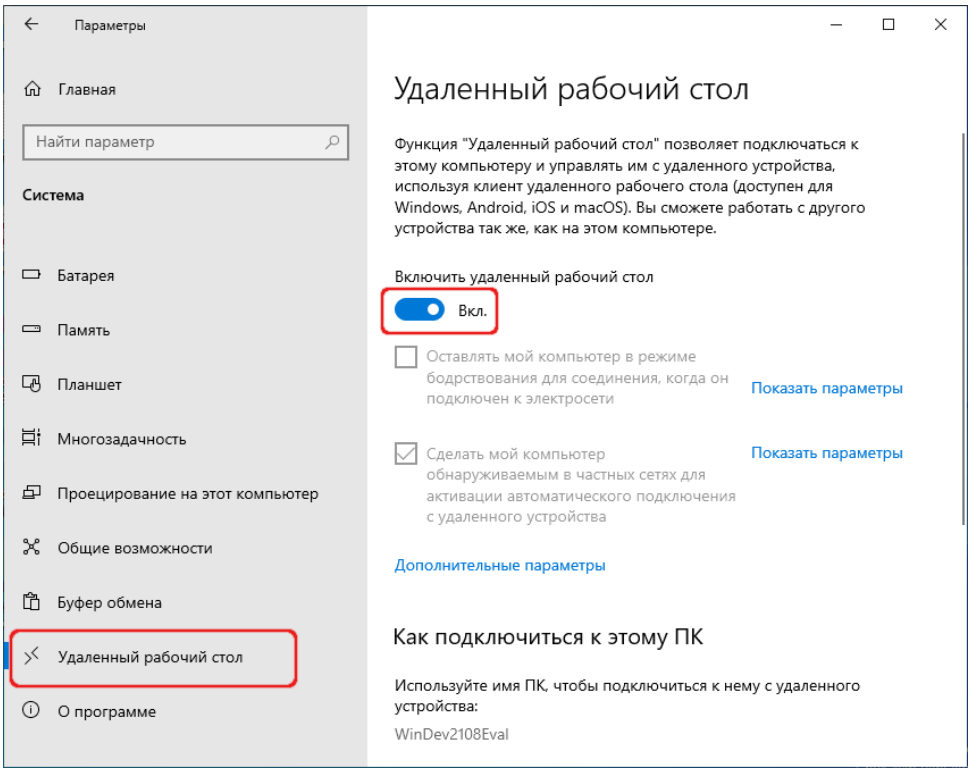


Рис. 289

Удаленный рабочий стол. Пользователи

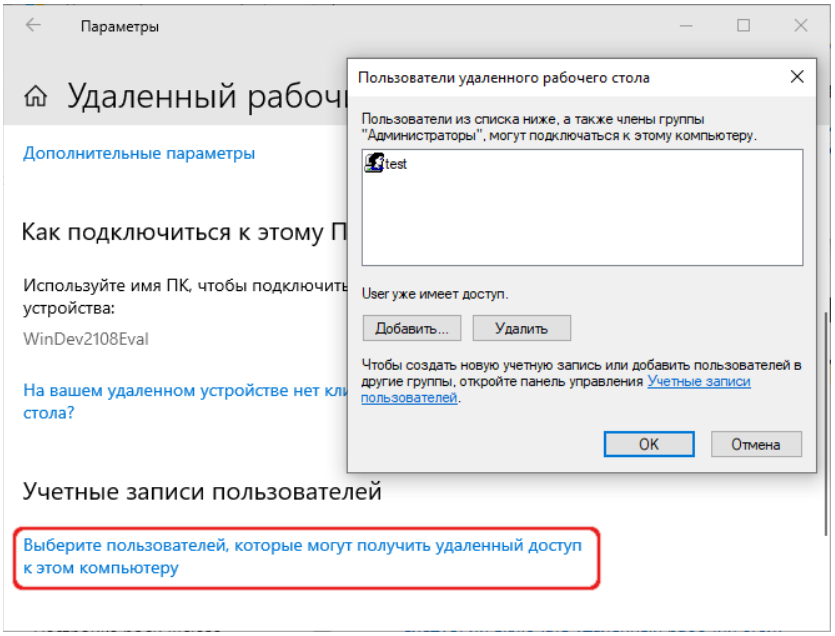


Рис. 290

Для возможности подключения клиентов Linux может потребоваться снять отметку с пункта «Требовать использование компьютерами аутентификации на уровне сети для подключения» в дополнительных параметрах (Рис. 291).

Удаленный рабочий стол. Дополнительные параметры

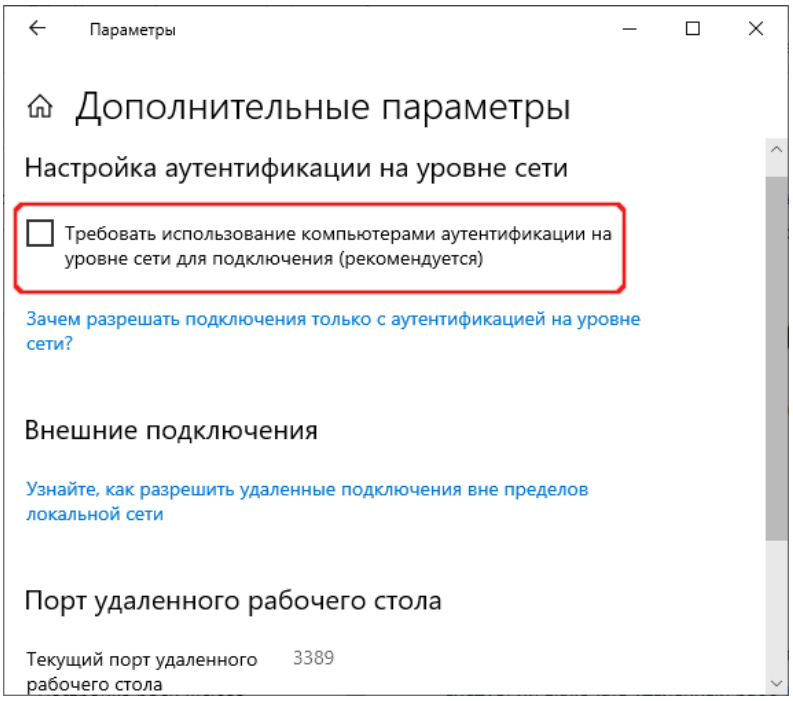


Рис. 291

Примечание. Необходимо также убедиться, что межсетевой экран не блокирует соединения по 3389 порту.

Установка OpenUDS Actor:

1. Загрузить OpenUDS Actor. Для этого в панели управления OpenUDS Server выбрать пункт «Загрузки» (Рис. 292) (пункт доступен пользователям с правами администратора) и на открывшейся странице выбрать нужный UDS Actor (Рис. 293).

   Примечание. Для машин с ОС Windows есть два вида OpenUDS Actor:

   - UDSActorSetup – для управляемых Windows машин;
   - UDSActorUnmanagedSetup – для неуправляемых Windows машин. Используется только для отдельных серверов без виртуализации.

2. Установить OpenUDS Actor (установка OpenUDS Actor ничем не отличается от инсталляции большинства других программ в ОС Windows).
3. Запустить UDSActorConfig от имени администратора. Для этого в контекстном меню пункта «UDSActorConfig» выбрать «Дополнительно» → «Запуск от имени администратора» (Рис. 294).

Загрузка OpenUDS Actor

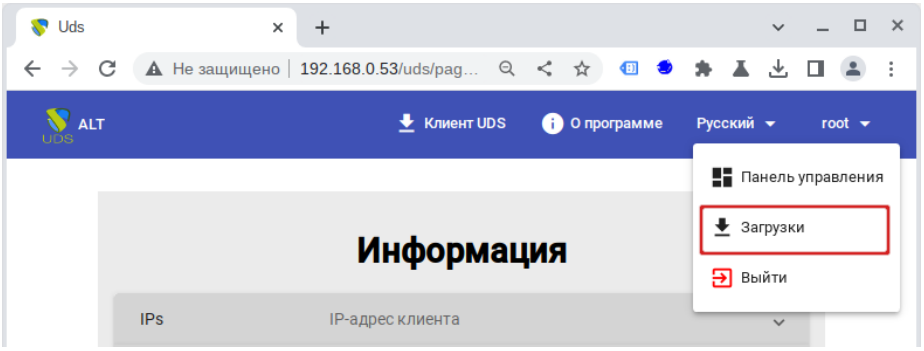


Рис. 292

Загрузка OpenUDS Actor

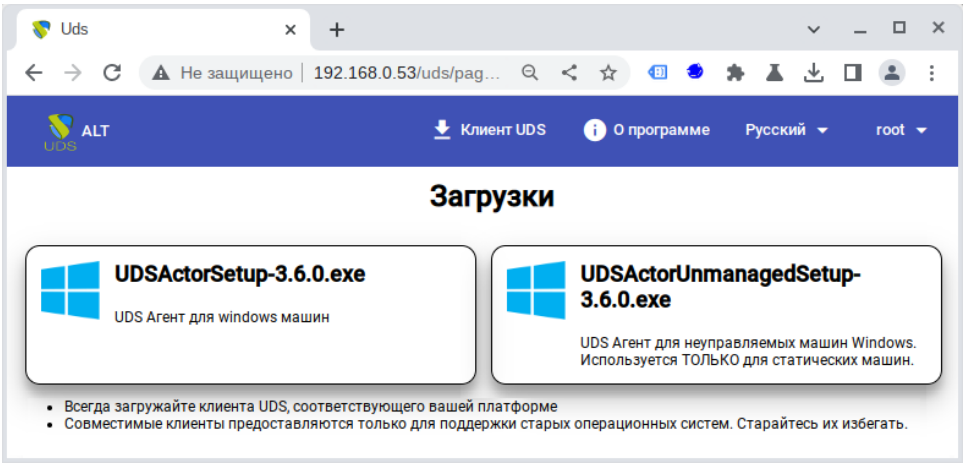


Рис. 293

Запуск UDSActorConfig

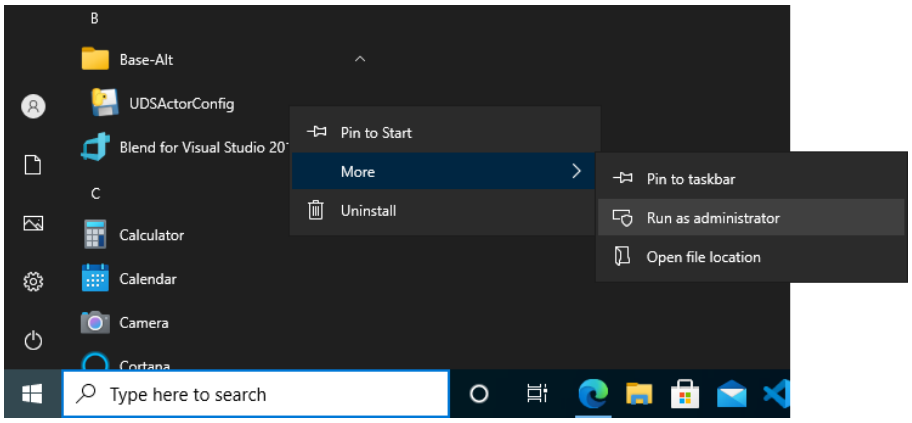


Рис. 294

4. Регистрация OpenUDS Actor на сервере:

- для регистрации Managed OpenUDS Actor на вкладке «UDS Server» необходимо указать имя или IP-адрес сервера OpenUDS, аутентификатор (значение «Administration» соответствует суперпользователю), имя и пароль пользователя, имеющего права администратора в среде OpenUDS и нажать кнопку «Register with UDS» (Рис. 295);

- для регистрации Unmanaged OpenUDS Actor необходимо указать имя или IP-адрес сервера OpenUDS и тот же ключ, который был указан при настройке услуги «Статический множественный IP-адрес» и нажать кнопку «Save Configuration» (Рис. 296).

Регистрация Managed OpenUDS Actor для Microsoft Windows

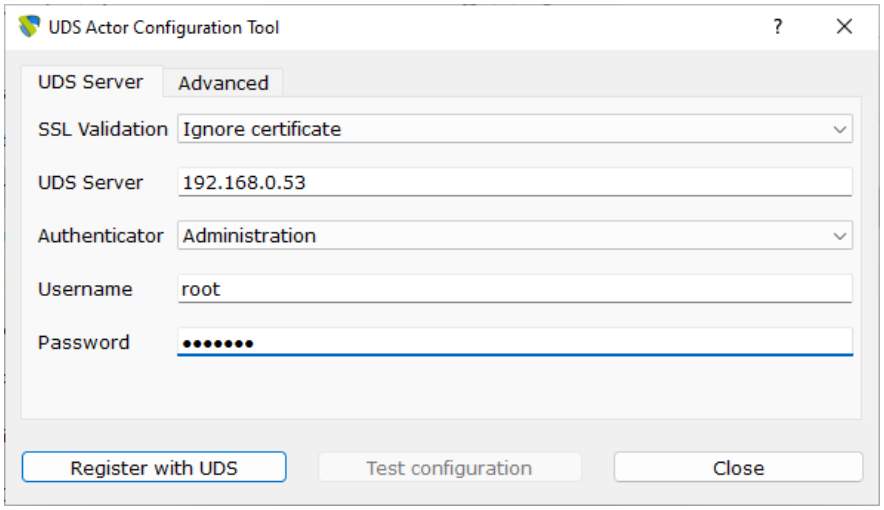


Рис. 295

Регистрация Unmanaged OpenUDS Actor for Microsoft Windows

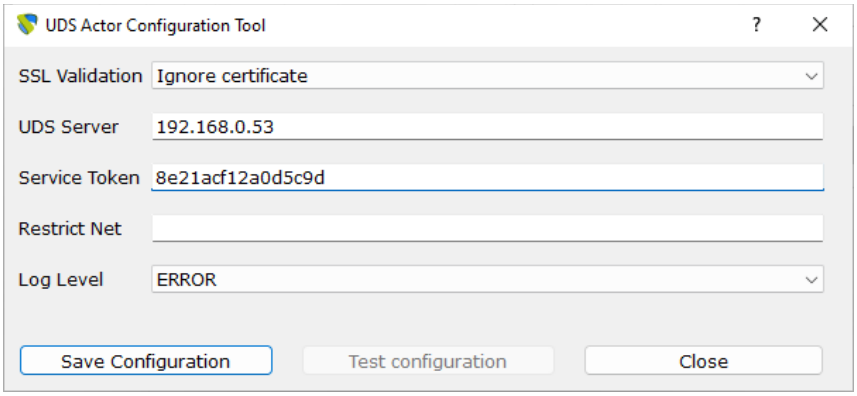


Рис. 296

Примечание. Unmanaged OpenUDS Actor уведомляет OpenUDS, когда пользователь входит в систему и выходит из нее. Благодаря этой функции система может освободить компьютер, при выходе пользователя из системы. Для использования этой функции при регистрации услуги «Статический множественный IP-адрес» кроме названия услуги следует указать один или несколько IP-адресов машин, к которым будет осуществляться доступ и ключ в поле «Ключ услуги» (Рис. 297). Если оставить поле «Ключ услуги» пустым, сеанс останется назначенным пользователю, пока администратор не удалит его вручную.

Регистрация услуги «Статический множественный IP-адрес» на сервере OpenUDS

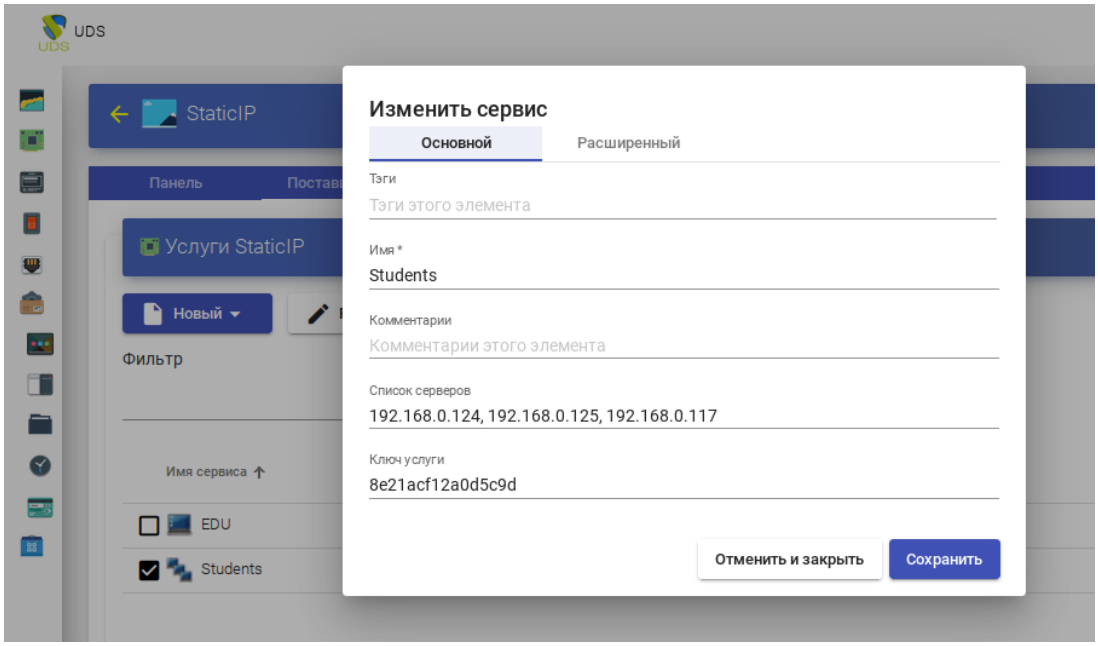


Рис. 297

5.11.5 Настройка клиента OpenUDS

Для возможности подключения к брокеру соединений и дальнейшего получения доступа к виртуальному рабочему окружению на клиентской машине должны быть установлены OpenUDS Client и клиенты каждого используемого протокола удаленного доступа.

5.11.5.1 Настойка клиента с ОС Альт

Установить пакет `openuds-client`:

```
# apt-get install openuds-client
```

Чтобы иметь возможность подключаться к виртуальному рабочему столу, должны быть установлены клиенты протоколов удаленного доступа:

- xfreerdp – для подключения по протоколу RDP;
- x2goclient – для подключения к серверу X2Go;
- remote-viewer из пакета `virt-viewer` – для подключения по протоколу SPICE.

5.11.5.2 Настойка клиента с ОС Windows

Установка клиента OpenUDS:

1. Скачать OpenUDS Client для компьютеров с ОС Windows. Для этого в панели управления OpenUDS Server выбрать пункт «Клиент UDS» и на открывшейся странице выбрать клиент Windows (Рис. 298).
2. Установить OpenUDS Client (установка ничем не отличается от инсталляции большинства других программ в ОС Windows).

Загрузка OpenUDS Client для Microsoft Windows

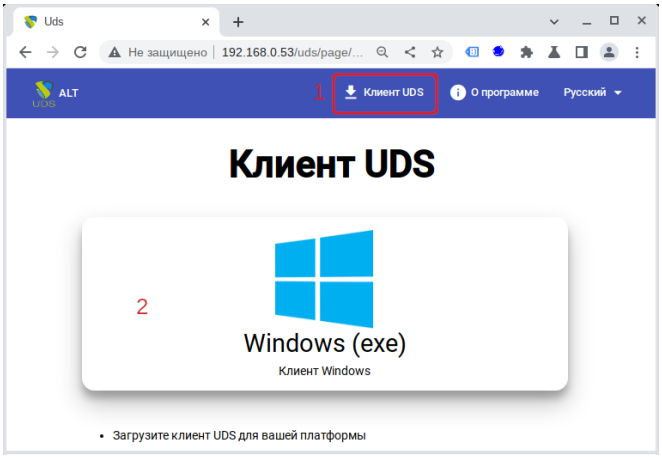


Рис. 298

Чтобы иметь возможность подключаться к виртуальному рабочему столу, должны быть установлены клиенты каждого используемого протокола удаленного доступа: RDP (стандартный клиент RDP установлен в Windows по умолчанию), X2Go.

Примечание. Для установки клиента X2Go на ОС Windows достаточно загрузить клиент X2Go (https://wiki.X2Go.org/doku.php) и установить его. Для установки клиента SPICE на ОС Windows необходимо установить `virt-viewer` (https://releases.pagure.org/virt-viewer/).

5.11.6 Подключение пользователя к виртуальному рабочему месту

Подключиться к серверу OpenUDS с помощью браузера http://openuds_address, ввести имя пользователя и пароль, выбрать средство проверки подлинности, если доступно несколько (Рис. 299).

OpenUDS. Аутентификация пользователя

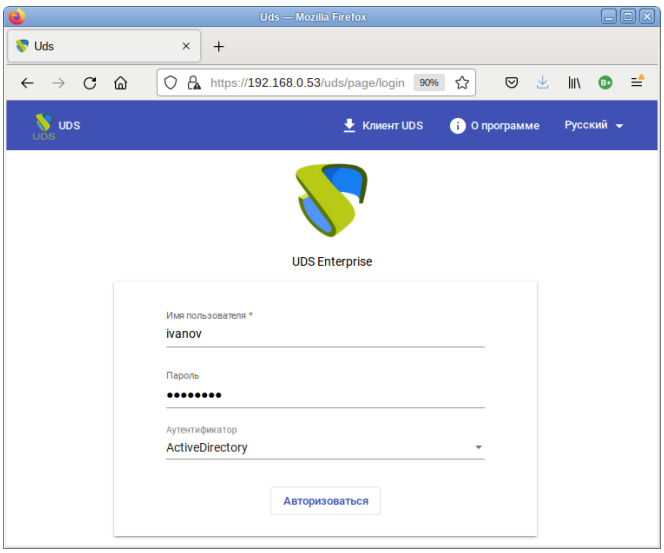


Рис. 299

На панели управления будут отображены все ВМ (или шаблоны), к которым у пользователя есть доступ (Рис. 300).

OpenUDS. Подключение пользователя к виртуальному рабочему месту

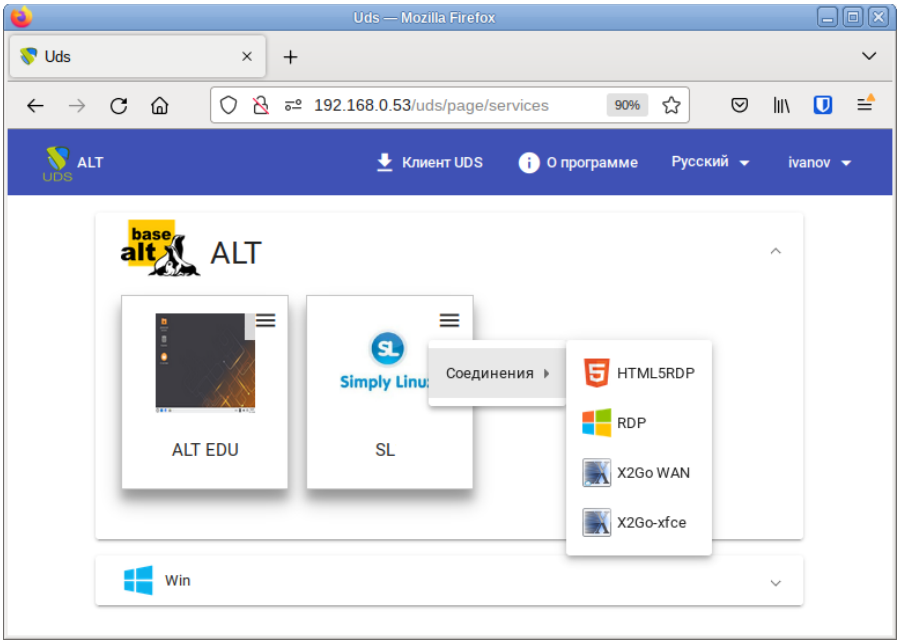


Рис. 300

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. 301).

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

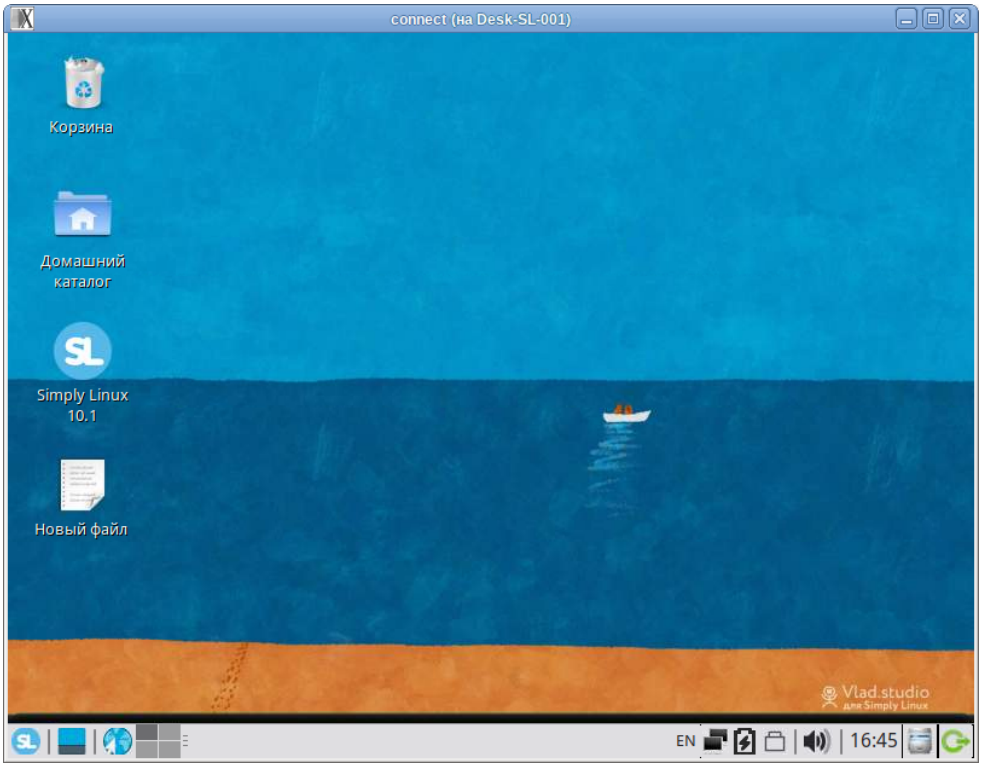


Рис. 301

Примечание. При подключении пользователя к виртуальному рабочему месту OpenUDS фиксирует доступ и отображает информацию о привязанном сервисе на вкладке «Назначенные услуги» соответствующего пула (Рис. 302).

OpenUDS. Вкладка «Назначенные услуги»

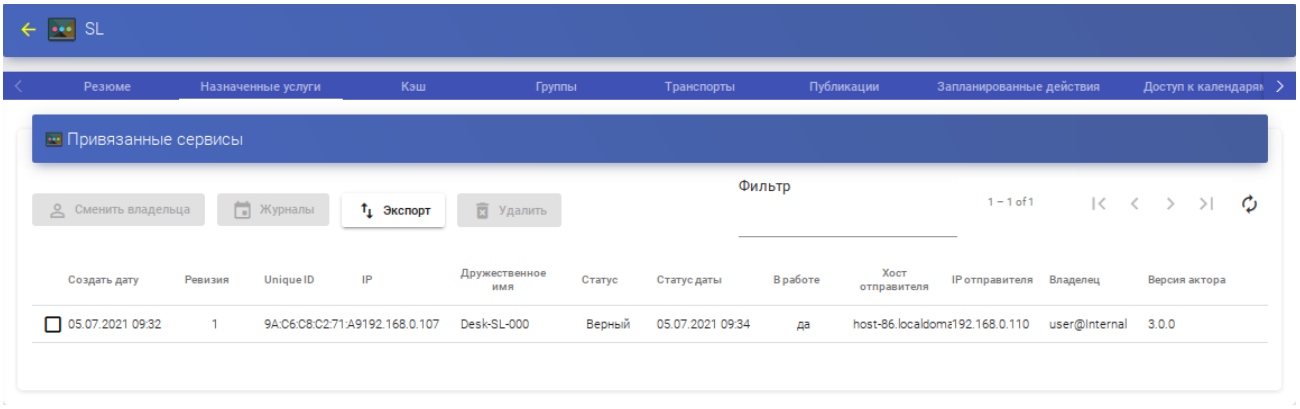


Рис. 302

5.11.7 Отказоустойчивое решение

Компоненты OpenUDS можно настроить в режиме высокой доступности (HA).

Для обеспечения высокой доступности OpenUDS, кроме настройки нескольких OpenUDS Server и Tunnel, необходимо настроить репликацию базы данных. Следует также настроить

балансировщик нагрузки, который будет распределять подключения к компонентам OpenUDS Server и Tunnel.

Основные компоненты отказоустойчивого решения OpenUDS (Рис. 303):

- сервер MySQL – база данных (БД) является одним из наиболее существенных компонентов OpenUDS. Поэтому настоятельно рекомендуется иметь резервную копию этого компонента, либо посредством полной резервной копии машины, либо посредством конфигурации активной/пассивной реплики. В данном руководстве описана настройка двух серверов MySQL в режиме активной/пассивной репликации;
- HAProxy-сервер – сервер, отвечающий за распределение подключений к OpenUDS Server и Tunnel. Через него осуществляется доступ пользователей к OpenUDS, и выполняются подключения к различным сервисам. На серверах HAProxy также следует настроить виртуальный IP-адрес, который будет активен только на основном сервере. В случае отказа основного сервера виртуальный IP-адрес будет автоматически активирован на другом сервере HAProxy;
- OpenUDS Server – наличие нескольких машин OpenUDS Server обеспечит непрерывный доступ пользователей к OpenUDS, даже при отказе одного из OpenUDS Server;
- OpenUDS Tunnel – наличие нескольких машин OpenUDS Tunnel позволит получить доступ к службам (рабочим столам или приложениям) через туннелированные соединения и HTML5, даже при отказе одного из OpenUDS Tunnel.

Основные элементы отказоустойчивого решения OpenUDS

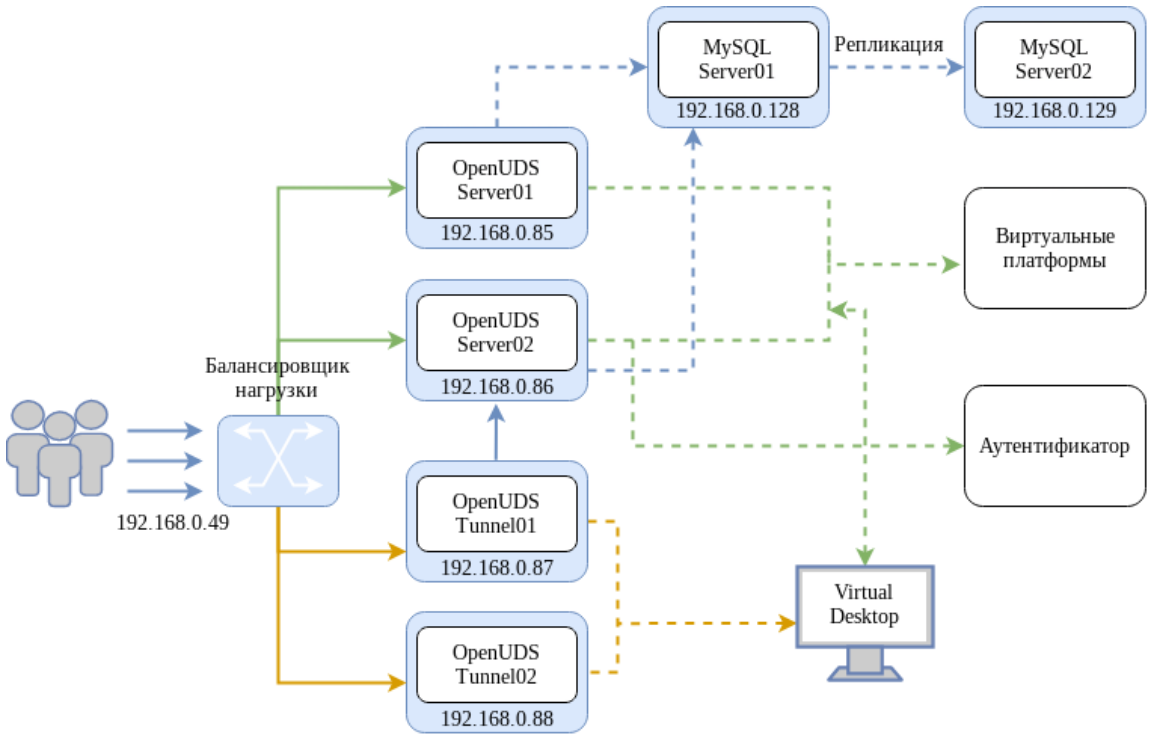


Рис. 303

Системные требования для компонентов OpenUDS представлены в табл 2.

Т а б л и ц а 2 – Системные требования

Компонент	Количество	ОЗУ	ЦП	Диск
SQL Server	2	1 ГБ	2 vCPUs	10 ГБ
HAProxy	2	1 ГБ	2 vCPUs	10 ГБ
OpenUDS Server	2	2 ГБ	2 vCPUs	8 ГБ
OpenUDS Tunnel	2	2 ГБ	2 vCPUs	13 ГБ

П р и м е ч а н и е . Для HAProxy необходимо 3 IP-адреса, по одному для каждого сервера (Master-Slave) и общий виртуальный IP-адрес, который будет использоваться для балансировки.

5.11.7.1 Конфигурация серверов MySQL

На обоих серверах установить MySQL (MariaDB):

```
# apt-get install mariadb-server
```

Запустить сервер MySQL и добавить его в автозагрузку:

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

Задать пароль root и настройки безопасности для MySQL:

```
# mysql_secure_installation
```

5.11.7.1.1 Настройка репликации между серверами

5.11.7.1.1.1Главный узел (Master)

В файле `/etc/my.cnf.d/server.cnf`:

- закомментировать параметр `skip-networking`;
- раскомментировать параметры `server-id` и `log-bin`;
- убедиться, что для параметра `server-id` установлено значение 1;
- раскомментировать параметр `bind-address` и указать IP-адрес сервера (главного):

```
bind-address 192.168.0.128
```

Перезагрузить службу MySQL:

```
# systemctl restart mariadb
```

Создать нового пользователя, с правами которого будет производиться репликация:

- войти в консоль MySQL с правами root:

```
$ mysql -p
```

- создать пользователя (в примере пользователь «replica» с паролем «uds»):

```
MariaDB [(none)]> CREATE USER 'replica'@'%' IDENTIFIED BY 'uds';
Query OK, 0 rows affected (0.009 sec)
```

- предоставить права `replication slave` пользователю:

```
MariaDB [(none)]> GRANT REPLICATION SLAVE ON *.* TO 'replica'@'%'
IDENTIFIED BY 'uds';
Query OK, 0 rows affected (0.002 sec)
```

- получить информацию об имени двоичного файла и его позиции:

```
MariaDB [(none)]> SHOW MASTER STATUS\G
*************************** 1. row ***************************
            File: mysql-bin.000002
        Position: 328
    Binlog_Do_DB:
Binlog_Ignore_DB:
1 row in set (0.001 sec)
```

В данном примере:

- mysql-bin.000002 – имя файла;
- 328 – позиция двоичного файла.

Эти данные будут необходимы для настройки Slave-сервера.

5.11.7.1.1.2Вторичный узел (Slave)

В файле `/etc/my.cnf.d/server.cnf`:

- закомментировать параметр `skip-networking`;
- раскомментировать параметры `server-id` и `log-bin`;
- в параметре `server-id` установить значение 2;
- раскомментировать параметр `bind-address` и указать IP-адрес сервера (вторичного):

```
bind-address 192.168.0.129
```

Перезагрузить службу MySQL:

```
# systemctl restart mariadb
```

Настроить параметры, которые вторичный сервер (Slave) будет использовать для подключения к основному серверу (Master):

- войти в консоль MySQL с правами root:

```
$ mysql -p
```

- остановить репликацию:

```
MariaDB [(none)]> STOP SLAVE;
Query OK, 0 rows affected, 1 warning (0.001 sec)
```

- настроить репликацию между основным сервером и вторичным сервером:

```
MariaDB [(none)]> CHANGE MASTER TO MASTER_HOST='192.168.0.128', MASTER_USER='replica', MASTER_PASSWORD='uds', MASTER_LOG_FILE='mysql-bin.000002', MASTER_LOG_POS=328;
Query OK, 0 rows affected (0.020 sec)
```

где:

- 192.168.0.128 – IP-адрес основного сервера;
- replica – пользователь, с правами которого будет производиться репликация;
- uds – пароль пользователя replica;
- mysql-bin.000002 – имя файла, полученного на предыдущем шаге;
- 328 – позиция двоичного файла.

- запустить репликацию:

```
MariaDB [(none)]> START SLAVE;
Query OK, 0 rows affected (0.001 sec)
```

- убедиться, что конфигурация верна:

```
MariaDB [(none)]> SHOW SLAVE STATUS\G
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: 192.168.0.128
                  Master_User: replica
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: mysql-bin.000004
          Read_Master_Log_Pos: 328
               Relay_Log_File: mysqld-relay-bin.000006
                Relay_Log_Pos: 555
        Relay_Master_Log_File: mysql-bin.000004
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
```

…

IP-адрес основного сервера должен быть указан корректно, параметры `Slave_IO_Running` и `Slave_SQL_Running` должны быть установлены в значение «Yes».

5.11.7.1.2 Проверка репликации

Для проверки репликации можно создать БД на главном сервере и убедиться, что она автоматически реплицируется на вторичном сервере:

- получить доступ к консоли MySQL главного сервера и создать новую тестовую БД «replicatest»:

```
MariaDB [(none)]> CREATE DATABASE replicatest;
Query OK, 1 row affected (0.001 sec)
```

- убедиться, что БД создана:

```
MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| replicatest        |
+--------------------+
4 rows in set (0.001 sec)
```

- получить доступ к консоли MySQL вторичного сервера и убедиться, что БД, созданная на основном сервере, успешно реплицировалась на этот сервер:

```
MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| replicatest        |
+--------------------+
4 rows in set (0.002 sec)
```

- после проверки работы репликации можно удалить БД «replicatest», выполнив команду на основном сервере:

```
MariaDB [(none)]> DROP DATABASE replicatest;
```

5.11.7.1.3 Создание БД

Создать на основном сервере БД:

```
$ mysql -p
Enter password:
```

```
MariaDB [(none)]> CREATE DATABASE dbuds CHARACTER SET utf8 COLLATE
utf8_general_ci;
MariaDB [(none)]> CREATE USER 'dbuds'@'%' IDENTIFIED BY 'password';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON dbuds.* TO 'dbuds'@'%';
MariaDB [(none)]> FLUSH PRIVILEGES;
MariaDB [(none)]> exit;
```

Подключить серверы OpenUDS к БД основного сервера.

5.11.7.1.4 Отказ сервера

При недоступности одного из серверов БД необходимо выполнить ряд задач. Задачи, которые следует выполнить, зависят от того к какому серверу (Master или Slave) нет доступа.

5.11.7.1.4.1Главный узел (Master)

Если недоступен основной сервер (Master), то будет потерян доступ к среде VDI. В этом случае необходимо вручную подключить OpenUDS Server к вторичной БД (Slave), в которой находится вся информация среды VDI до момента падения основной БД. Чтобы настроить новое подключение к БД на OpenUDS Server, следует в конфигурационном файле `/var/server/server/settings.py` указать параметры новой БД (это необходимо сделать на всех серверах OpenUDS-Server).

После изменения IP-адреса БД необходимо перезапустить сервер OpenUDS (это необходимо сделать на всех серверах OpenUDS Server). После перезапуска сервера доступ к среде VDI будет восстановлен

Затем необходимо настроить новый сервер для репликации БД. Это можно сделать разными способами, например:

1. Настроить текущий сервер БД как главный и создать новый сервер-реплику, который нужно настроить и восстановить БД из резервной копии с существующими данными (поскольку реплицируются только новые данные).
2. Напрямую сделать резервную копию текущего сервера БД (предварительно остановив все машины OpenUDS Server). Создать новый сервер БД Master, восстановить туда резервную копию БД и перенастроить репликацию.

Примечание. Чтобы не потерять данные, перед применением любого метода перестроения репликации, рекомендуется сделать резервную копию БД. Для получения резервной копии можно использовать следующую команду:

```
# mysqldump -u dbuds -ppassword --databases dbuds > dbuds_dump.sql
```

При создании резервной копии все машины OpenUDS Server должны быть выключены. Таким образом, обеспечивается согласованность данных и отсутствие различий в данных между главным и подчиненным серверами перед настройкой реплики.

5.11.7.1.4.2Вторичный узел (Slave)

Если недоступен вторичный сервер БД (Slave), доступ к среде VDI сохранится, но будет необходимо перенастроить вторичный сервер-реплику. Перед выполнением данной настройки необходимо восстановить резервную копию с текущим состоянием основной БД, так как будут синхронизированы только новые данные реплики (существующие данные не будут реплицированы в базе данных).

Важно, чтобы во время всего этого процесса машины OpenUDS-Server были выключены, чтобы не возникало различий между БД Master и Slave серверов.

5.11.7.2 Настройка серверов HAProxy

В данной конфигурации (Рис. 304) используется служба Keepalived и виртуальный IP-адрес, общий для главного (Master) и резервного (Slave) узлов. Служба Keepalived связывает виртуальный IP-адрес с главным узлом и отслеживает доступность HAProxy. Если служба обнаруживает, что HAProxy не отвечает, то она связывает виртуальный адрес с вспомогательным узлом, что минимизирует время недоступности сервера. Пользователи при обращении к OpenUDS должны использовать этот виртуальный IP-адрес.

Конфигурация балансировщика нагрузки

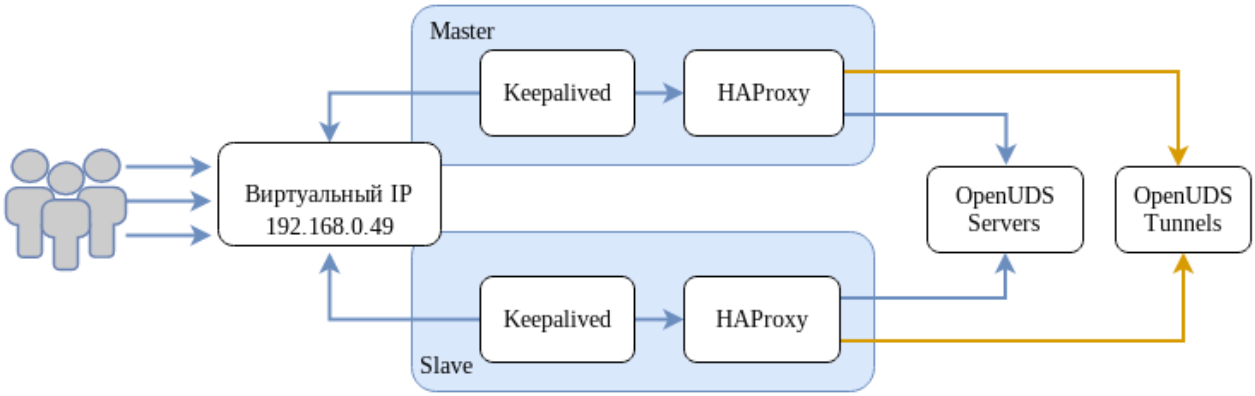


Рис. 304

На основном узле сгенерировать сертификат:

```
# openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout /root/ssl.key -out /root/ssl.crt
```

Создать файл .pem, выполнив команду (предварительно может понадобиться создать каталог `/etc/openssl/private`):

```
# cat /root/ssl.crt /root/ssl.key > /etc/openssl/private/haproxy.pem
```

Примечание. Сертификат, созданный на первичном сервере HAProxy, необходимо скопировать в каталог `/etc/openssl/private` на вторичном сервере. Если используется собственный сертификат, его необходимо скопировать на оба сервера (основной и дополнительный).

Примечание. Порты, используемые HAProxy (в примере 80, 443, 1443, 10443), должны быть свободны.

На обоих узлах:

1. Установить пакеты `haproxy` и `keepalived`:

```
# apt-get install haproxy keepalived
```

2. Заменить содержимое файла `/etc/haproxy/haproxy.cfg` следующим:

```
global
        log /dev/log    local0
        log /dev/log    local1 notice
        chroot /var/lib/haproxy
        stats socket /var/lib/haproxy/admin.sock mode 660 level admin
        stats timeout 30s
        maxconn 2048
        user _haproxy
        group _haproxy
        daemon

        # Default SSL material locations
        # ca-base /etc/openssl/certs
        # crt-base /etc/openssl/private

        # Default ciphers to use on SSL-enabled listening sockets.
        # For more information, see ciphers(1SSL). This list is from:
        #  https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/
        ssl-default-bind-options ssl-min-ver TLSv1.2 prefer-client-ciphers
        # ssl-default-bind-ciphersuites
TLS_AES_128_GCM_SHA267:TLS_AES_267_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA267
        ssl-default-bind-ciphers ECDH+AESGCM:ECDH+CHACHA20:ECDH+AES267:ECDH+AES128:!
aNULL:!SHA1:!AESCCM

        # ssl-default-server-options ssl-min-ver TLSv1.2
        # ssl-default-server-ciphersuites
TLS_AES_128_GCM_SHA267:TLS_AES_267_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA267
        # ssl-default-server-ciphers
ECDH+AESGCM:ECDH+CHACHA20:ECDH+AES267:ECDH+AES128:!aNULL:!SHA1:!AESCCM
```

```
        tune.ssl.default-dh-param 2048


defaults
        log     global
        mode    http
        option  httplog
        option  dontlognull
        option  forwardfor
        retries 3
        option  redispatch

        stats enable
        stats uri /haproxystats
        stats realm Strictly\ Private
        stats auth stats:haproxystats

        timeout connect 5000
        timeout client  50000
        timeout server  50000

frontend http-in
        bind *:80
        mode http
        http-request set-header X-Forwarded-Proto http
        default_backend openuds-backend
frontend https-in
        bind *:443 ssl crt /etc/openssl/private/haproxy.pem
        mode http
        http-request set-header X-Forwarded-Proto https
        default_backend openuds-backend

frontend tunnel-in
        bind *:1443
        mode tcp
        option tcplog
        default_backend tunnel-backend-ssl

frontend tunnel-in-guacamole    # HTML5
        bind *:10443
        mode tcp
        option tcplog
```

```
        default_backend tunnel-backend-guacamole
backend openuds-backend
        option http-keep-alive
        balance roundrobin
        server udss1 192.168.0.85:80 check inter 2000 rise 2 fall 5
        server udss2 192.168.0.86:80 check inter 2000 rise 2 fall 5
backend tunnel-backend-ssl
        mode tcp
        option tcplog
        balance roundrobin
        server udst1 192.168.0.87:7777 check inter 2000 rise 2 fall 5
        server udst2 192.168.0.88:7777 check inter 2000 rise 2 fall 5

backend tunnel-backend-guacamole
        mode tcp
        option tcplog
        balance source
        server udstg1 192.168.0.87:10443check inter 2000 rise 2 fall 5
        server udstg2 192.168.0.88:10443 check inter 2000 rise 2 fall 5
```

3. Включить в ядре поддержку двух IP-адресов:

```
# echo "net.ipv4.ip_nonlocal_bind = 1" >> /etc/sysctl.conf
# sysctl -p
```

4. Настроить службу Keepalived. Для этого создать файл `/etc/keepalived/keepalived.conf`. Содержимое файла зависит от узла, который настраивается:

- на главном узле:

```
global_defs {
    # Keepalived process identifier
    lvs_id haproxy_DH
}
# Script used to check if HAProxy is running
vrrp_script check_haproxy {
    script "killall -0 haproxy"
    interval 2
    weight 2
}
# Виртуальный интерфейс
# The priority specifies the order in which the assigned interface
# to take over in a failover
vrrp_instance VI_01 {
    state MASTER
    interface enp0s3
```

```
    virtual_router_id 51
    priority 101
    # Виртуальный IP-адрес
    virtual_ipaddress {
        192.168.0.49
    }
    track_script {
        check_haproxy
    }
}
```

где enp0s3 – интерфейс, для виртуального IP (узнать имя сетевого интерфейса можно, выполнив команду `ip a`).

- на вспомогательном узле:

```
global_defs {
    # Keepalived process identifier
    lvs_id haproxy_DH_passive
}
# Script used to check if HAProxy is running
vrrp_script check_haproxy {
    script "killall -0 haproxy"
    interval 2
    weight 2
}
# Виртуальный интерфейс
# The priority specifies the order in which the assigned interface
# to take over in a failover
vrrp_instance VI_01 {
    state SLAVE
    interface eth0
    virtual_router_id 51
    priority 100
    # Виртуальный IP-адрес
    virtual_ipaddress {
        192.168.0.49
    }
    track_script {
        check_haproxy
    }
}
```

где eth0 – интерфейс, для виртуального IP (узнать имя сетевого интерфейса можно, выполнив команду `ip a`).

5. Запустить службы haproxy и keepalived:

```
# systemctl enable --now haproxy
# systemctl enable --now keepalived
```

6. Убедиться, что виртуальный IP активен на основном сервере:

```
$ ip a |grep enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 192.168.0.52/24 brd 192.168.0.255 scope global noprefixroute enp0s3
    inet 192.168.0.49/32 scope global enp0s3
```

5.11.7.3 Настройка OpenUDS

После настройки серверов MySQL и HAProxy можно приступить к установке и настройке компонентов OpenUDS Server и Tunnel.

5.11.7.3.1 Настройка OpenUDS Server

На обоих узлах OpenUDS Server:

1. Установить OpenUDS Server:

```
# apt-get install openuds-server-nginx
```

2. Отредактировать содержимое файла `/etc/openuds/settings.py`, указав корректные данные для подключения к главному MySQL-серверу:

```
DATABASES = {
    'default': {
        'ENGINE': 'django.db.backends.mysql',
        'OPTIONS': {
            'isolation_level': 'read committed',
        },
        'NAME': 'dbuds',  # Or path to database file if using sqlite3.
        'USER': 'dbuds',  # Not used with sqlite3.
        'PASSWORD': 'password',  # Not used with sqlite3.
        'HOST': '192.168.0.128',  # Set to empty string for localhost. Not used with sqlite3
        'PORT': '3306',  # Set to empty string for default. Not used with sqlite3.
    }
}
```

3. Заполнить базу данных начальными данными (этот пункт следует выполнить только на одном узле!):

```
# su -s /bin/bash - openuds
$ cd /usr/share/openuds
```

```
$ python3 manage.py migrate
$ exit
```

4. Запустить gunicorn:

```
# systemctl enable --now openuds-web.service
```

5. Запустить nginx:

```
# ln -s ../sites-available.d/openuds.conf /etc/nginx/sites-enabled.d/openuds.conf
# systemctl enable --now nginx.service
```

6. Запустить менеджер задач OpenUDS:

```
# systemctl enable --now openuds-taskmanager.service
```

7. Подключиться к серверу OpenUDS (http://Виртуальный_IP-адрес).

5.11.7.3.2 Настройка OpenUDS Tunnel

На каждом узле OpenUDS Tunnel:

1. Установить OpenUDS Tunnel:

```
# apt-get install openuds-tunnel
```

2. Настроить туннель:

- указать виртуальный IP-адрес в файле `/etc/openuds-tunnel/udstunnel.conf`:

```
uds_server = http://192.168.0.49/uds/rest/tunnel/ticket
uds_token = 5ba9d52bb381196c2a22e495ff1c9ba4bdc03440b726aa8b
```

- запустить и добавить в автозагрузку сервис OpenUDS Tunnel:

```
# systemctl enable --now openuds-tunnel.service
```

3. Настроить HTML5:

- в файле `/etc/guacamole/guacamole.properties` привести значение параметра `uds-base-url` к виду:

```
uds-base-url=http://192.168.0.49/uds/guacamole/
auth/5ba9d52bb381196c2a22e495ff1c9ba4bdc03440b726aa8b
```

настроить tomcat, для этого в файл `/etc/tomcat/server.xml` добавить новый Connector, в котором указать порт (в примере 10443), сертификат (файл .crt, .pem и т.д.), закрытый ключ (.key, .pem и т.д.):

```
<Connector port="10443" protocol="org.apache.coyote.http11.Http11AprProtocol"
SSLEnabled="true"
           ciphers="A-CHACHA20-POLY1305,ECDHE-RSA-CHACHA20-POLY1305,ECDHE-ECDSA-
AES128-GCM-SHA256,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-
RSA-AES256-GCM-SHA384,DHE-RSA-AES128-GCM-SHA256,DHE-RSA-AES256-GCM-SHA384,ECDHE-
ECDSA-AES128-SHA256,ECDHE-RSA-AES128-SHA256,ECDHE-ECDSA-AES128-SHA,ECDHE-RSA-AES256-
SHA384,
ECDHE-RSA-AES128-SHA,ECDHE-ECDSA-AES256-SHA384,ECDHE-ECDSA-AES256-SHA,ECDHE-RSA-
AES256-SHA,DHE-RSA-AES128-SHA256,DHE-RSA-AES128-SHA,DHE-RSA-AES256-SHA256,DHE-RSA-
```

```
AES256-SHA,ECDHE-ECDSA-DES-CBC3-SHA,ECDHE-RSA-DES-CBC3-SHA,EDH-RSA-DES-CBC3-
SHA,AES128-GCM-SHA256,AES256-GCM-SHA384,
AES128-SHA256,AES256-SHA256,AES128-SHA,AES256-SHA,DES-CBC3-SHA"
           maxThreads="500" scheme="https" secure="true"
           SSLCertificateFile="/etc/openuds-tunnel/ssl/certs/openuds-tunnel.pem"
           SSLCertificateKeyFile="/etc/openuds-tunnel/ssl/private/openuds-tunnel.key"
           maxKeepAliveRequests="1000"
           clientAuth="false" sslProtocol="TLSv1+TLSv1.1+TLSv1.2" />
```

- запустить сервисы guacd и tomcat:

```
# systemctl enable --now guacd tomcat
```

На главном узле (Master) MySQL добавить в БД информацию о каждом OpenUDS Tunnel:

```
INSERT INTO `uds_tunneltoken` VALUES (ID,'автор добавления','IP-адрес
туннеля','IP-адрес туннеля' 'название туннеля','Токен из файла
udstunnel.conf','дата добавления');
```

Например:

```
# mysql -u root -p
MariaDB> USE dbuds;
MariaDB> INSERT INTO `uds_tunneltoken` VALUES
(ID,'admin','192.168.0.87','192.168.0.87','Tunnel','5ba9d52bb381196c2a22e495f
f1c9ba4bdc03440b726aa8b','2022-11-15');
MariaDB> INSERT INTO `uds_tunneltoken` VALUES
(ID,'admin','192.168.0.88','192.168.0.88','Tunnel','9ba4bdc03440b726aa8b5ba9d
52bb381196c2a22e495ff1c','2022-11-15');
MariaDB> exit;
```

Оба сервера OpenUDS-Tunnel будут работать в активном режиме. Пользователи, использующие подключение через туннель, будут подключаться к этим серверам случайным образом. При падении одного из серверов, соединения пользователей, которые используют этот сервер, будут прерваны, но при повторном установлении соединения они автоматически получат доступ через другой активный туннельный сервер.

Примечание. При создании туннельного транспорта (X2Go, RDP) в поле «Туннельный сервер» (вкладка «Туннель») следует указывать виртуальный IP-адрес и порт, указанный в разделе `frontend tunnel-in` файла `/etc/haproxy/haproxy.cfg` (в данном примере: 1443). При создании транспорта «HTML5 RDP (туннельный)» в поле «Туннельный сервер» (Рис. 305) следует указывать виртуальный IP-адрес и порт, указанный в разделе `frontend tunnel-in-guacamole` файла `/etc/haproxy/haproxy.cfg` (в данном примере: 10443).

OpenUDS. HTML5 RDP – вкладка «Туннель»

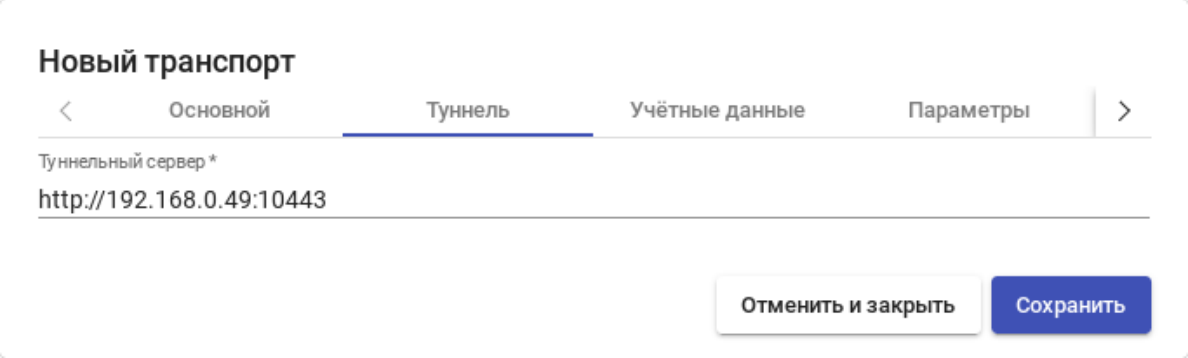


Рис. 305

Пример подключения с использованием HTML5 показан на Рис. 306.

OpenUDS. Пример подключения с использованием HTML5

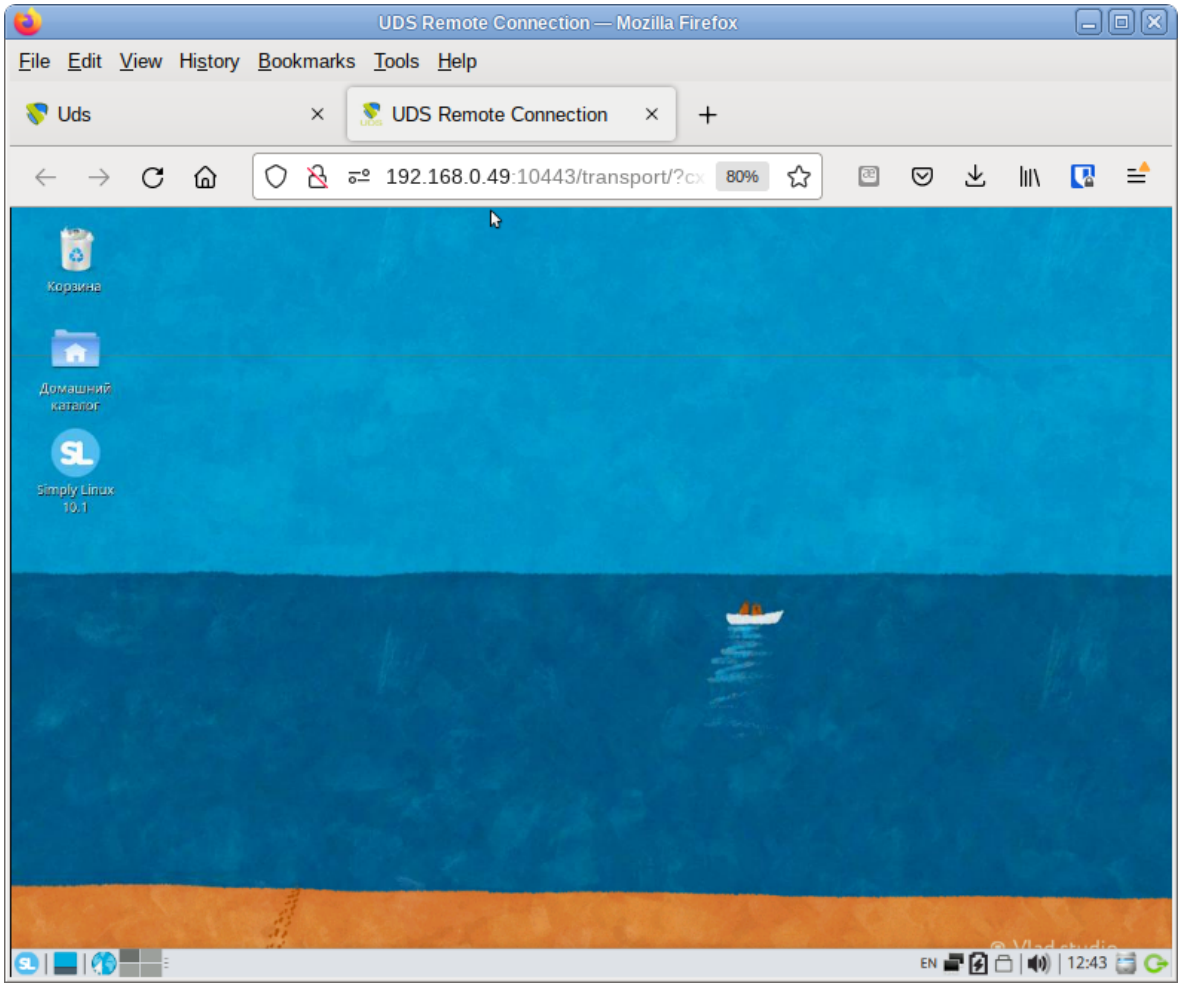


Рис. 306

5.12 Система резервного копирования Proxmox Backup Server

Proxmox Backup Server (PBS) – клиент-серверное решение для резервного копирования и восстановления виртуальных машин, контейнеров и данных с физических узлов. Решение оптимизировано для проекта Proxmox VE (PVE). PBS поддерживает инкрементное резервное копирование с полной дедупликацией, что значительно снижает нагрузку на сеть и экономит пространство для хранения.

Все взаимодействия между клиентом и сервером шифруются с использованием TLS, кроме того, данные могут быть зашифрованы на стороне клиента перед отправкой на сервер. Это позволяет сделать резервное копирование более безопасным.

Сервер резервного копирования хранит данные резервного копирования и предоставляет API для создания хранилищ данных и управления ими. С помощью API также можно управлять дисками и другими ресурсами на стороне сервера.

Клиент резервного копирования использует API для доступа к резервным копиям. С помощью инструмента командной строки proxmox-backup-client можно создавать резервные копии и восстанавливать данные (в PVE клиент встроен).

Для управления настройкой резервного копирования и резервными копиями используется веб-интерфейс. Все административные задачи можно выполнять в веб-браузере. Веб-интерфейс также предоставляет встроенную консоль.

5.12.1 Установка PBS

5.12.1.1 Сервер PBS

Установить сервер PBS:

```
# apt-get install proxmox-backup-server
```

Примечание. Сервер PBS можно установить при установке системы, выбрав для установки пункт «Сервер резервного копирования от проекта Proxmox».

Запустить и добавить в автозагрузку Proxmox Backup API Proxy Server:

```
# systemctl enable --now proxmox-backup-proxy.service
```

Служба proxmox-backup-proxy предоставляет API управления PBS по адресу 127.0.0.1:82. Она имеет разрешение на выполнение всех привилегированных операций.

Примечание. Для работы с локальным ZFS хранилищем должен быть установлен модуль ядра с поддержкой ZFS (пакет `kernel-modules-zfs-un-def` или `kernel-modules-zfs-std-def` в зависмости от типа ядра, установленного в системе). Модуль ядра с поддержкой ZFS не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p10.

Включить модуль:

```
# modprobe zfs
```

Чтобы не вводить эту команду каждый раз после перезагрузки, следует в файле `/etc/modules-load.d/zfs.conf` раскомментировать строку:

```
#zfs
```

5.12.1.2 Клиент PBS

Установить клиент PBS:

```
# apt-get install proxmox-backup- client
```

5.12.2 Веб-интерфейс PBS

Веб-интерфейс PBS доступен по адресу https://<имя-компьютера|IP-адрес>:8007. Потребуется пройти аутентификацию (Рис. 307) (логин по умолчанию: root, пароль указывается в процессе установки ОС).

Аутентификация в веб-интерфейсе PBS

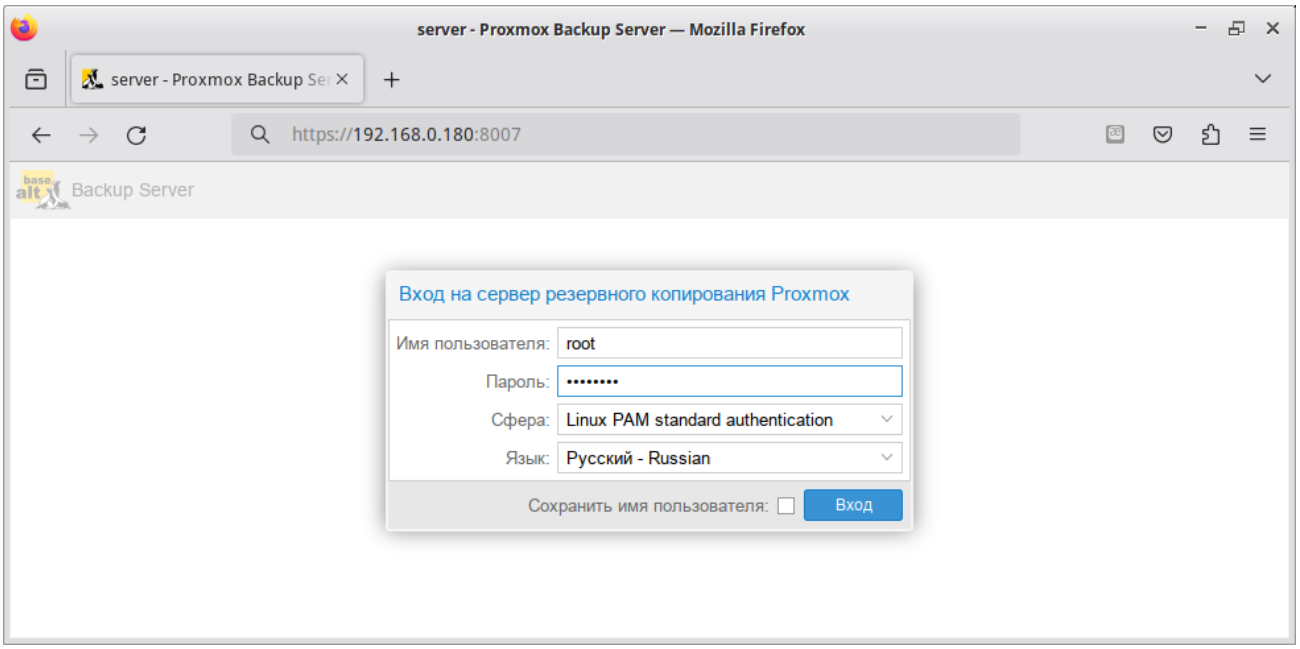


Рис. 307

Веб-интерфейс PBS показан на Рис. 308.

5.12.3 Настройка хранилища данных

5.12.3.1 Управление дисками

В веб-интерфейсе на вкладке «Управление» → «Хранилище/Диски» можно увидеть диски, подключённые к системе (Рис. 309).

Просмотр списка дисков в командной строке:

```
# proxmox-backup-manager disk list
```

Создание файловой системы ext4 или xfs на диске в веб-интерфейсе показано на Рис. 310.

Веб-интерфейс PBS

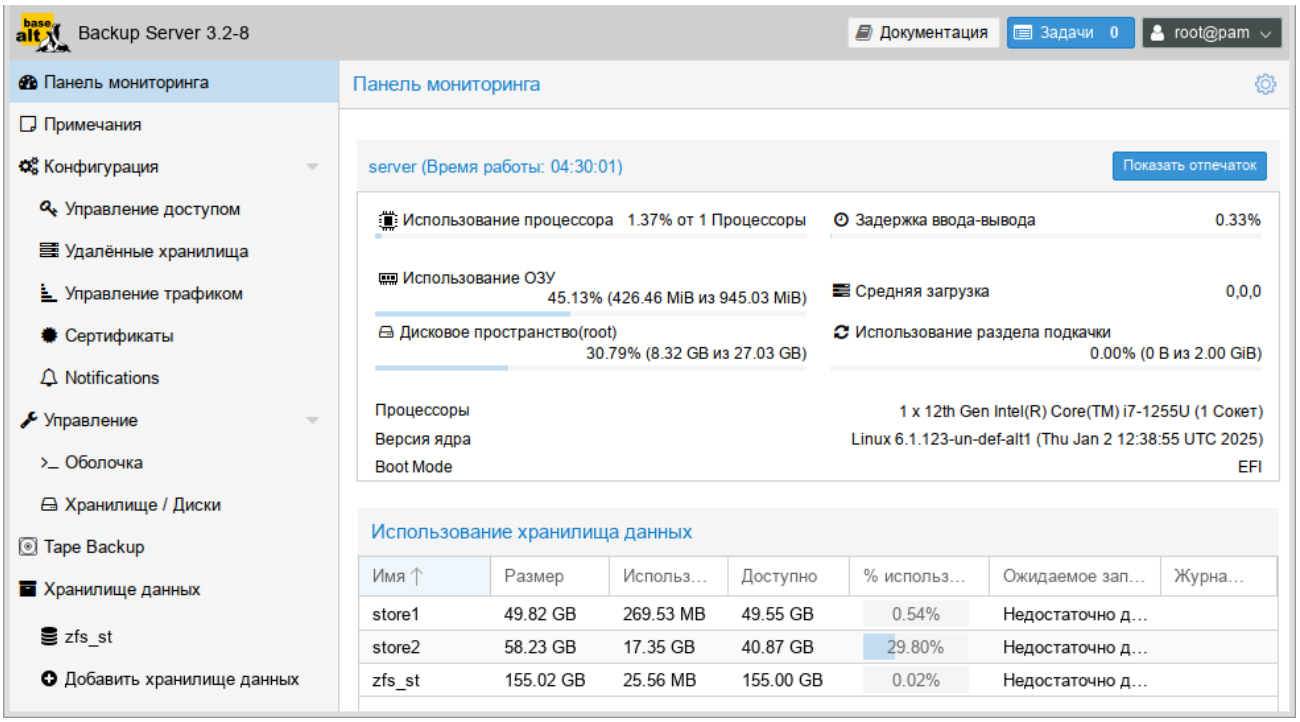


Рис. 308

PBS. Диски, подключенные к системе

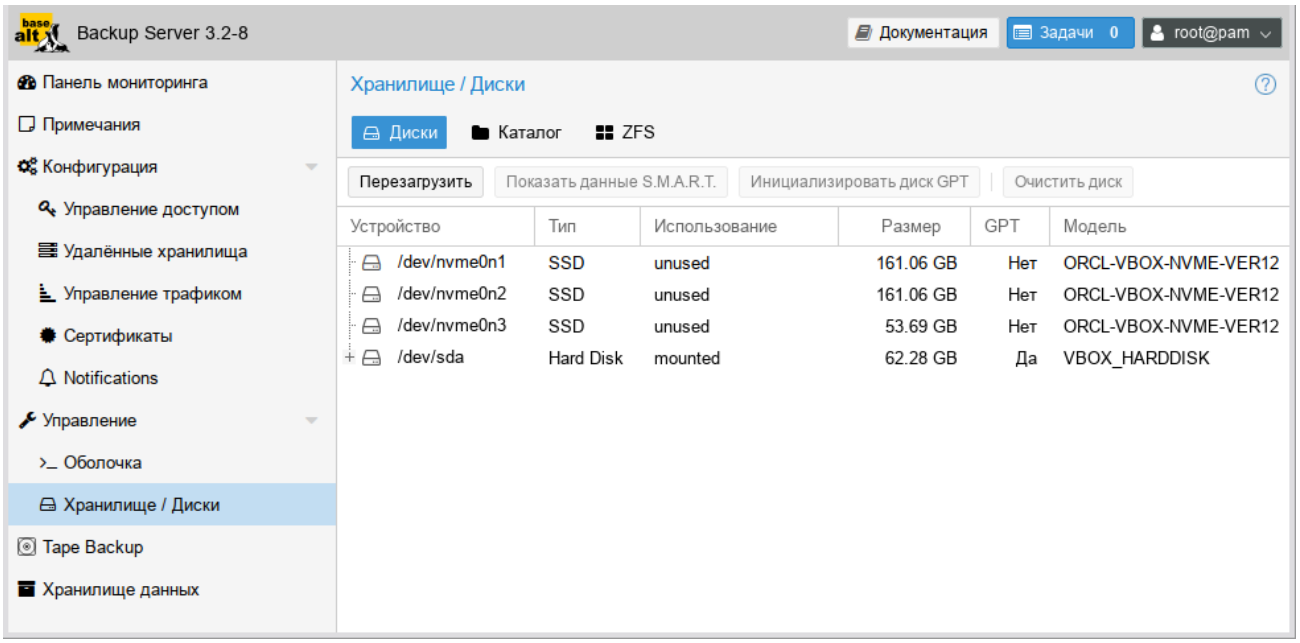


Рис. 309

PBS. Создание файловой системы на диске

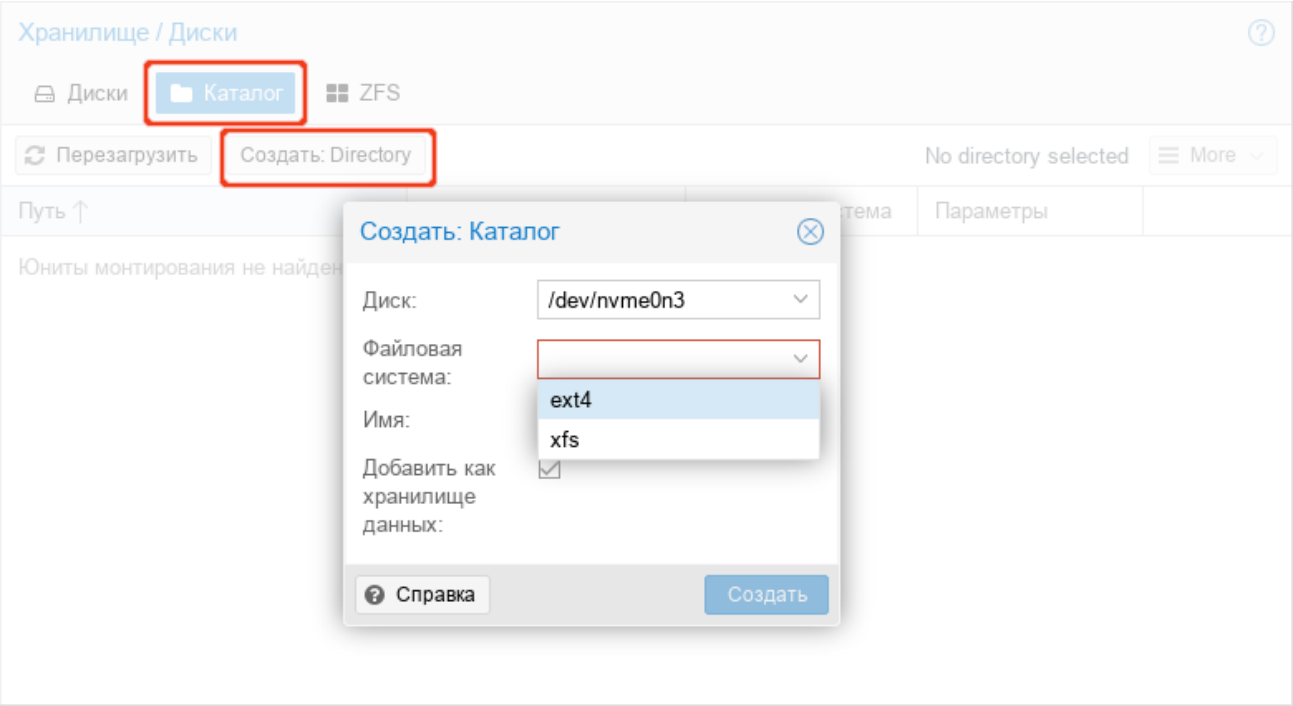


Рис. 310

Пример создания файловой системы в командной строке (будет создана файловая система ext4 и хранилище данных на диске nvme0n3, хранилище данных будет создано по адресу /mnt/datastore/store1):

```
# proxmox-backup-manager disk fs create store1 --disk nvme0n3 --
filesystem ext4 --add-datastore true
create datastore 'store1' on disk nvme0n3
Chunkstore create: 1%
Chunkstore create: 2%
…
Chunkstore create: 99%
TASK OK
```

Для создания zpool в веб-интерфейсе, следует перейти в раздел «Хранилище/Диски», открыть вкладку «ZFS» и нажать кнопку «Создать: ZFS». В открывшемся окне «Создать: ZFS» следует указать параметры zpool (задать имя хранилища, выбрать необходимые диски, выбратьуровень RAID) и нажать кнопку «Создать» (Рис. 311).

Команда для создания зеркального zpool с использованием двух дисков и монтированием в /mnt/datastore/zfs_st:

```
# proxmox-backup-manager disk zpool create zfs_st --devices
nvme0n1,nvme0n2 --raidlevel mirror
```

PBS. Создание zpool

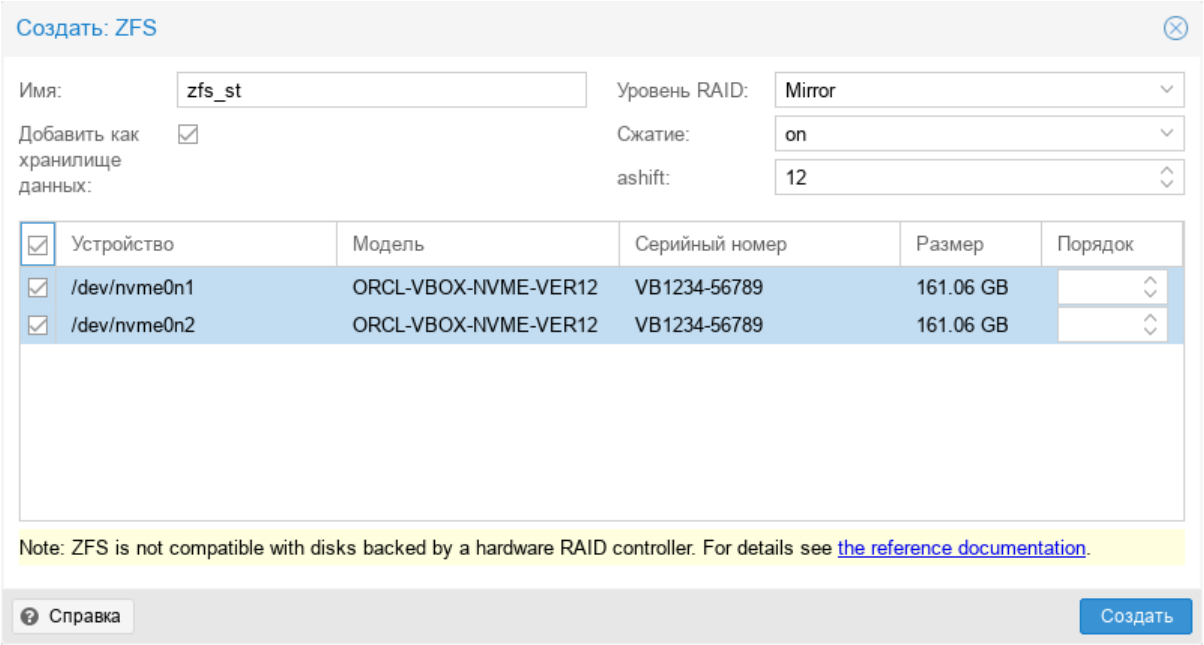


Рис. 311

Для мониторинга состояния локальных дисков используется пакет `smartmontools`. Он содержит набор инструментов для мониторинга и управления S.M.A.R.T. системой для локальных жестких дисков. Если диск поддерживает S.M.A.R.T. и поддержка SMART для диска включена, просмотреть данные S.M.A.R.T. можно в веб-интерфейсе или с помощью команды:

```
# proxmox-backup-manager disk smart-attributes sdX
```

5.12.3.2 Создание хранилища данных

Хранилище данных – это место, где хранятся резервные копии. Текущая реализация PBS использует каталог внутри стандартной файловой системы (ext4, xfs или zfs) для хранения данных резервного копирования. Информация о конфигурации хранилищ данных хранится в файле `/etc/proxmox-backup/datastore.cfg`.

Необходимо настроить как минимум одно хранилище данных. Хранилище данных идентифицируется именем и указывает на каталог в файловой системе. С каждым хранилищем связаны настройки хранения, определяющие, сколько снимков резервных копий для каждого интервала времени (ежечасно, ежедневно, еженедельно, ежемесячно, ежегодно) хранить в этом хранилище.

Для создания хранилища в веб-интерфейсе необходимо нажать кнопку «Добавить хранилище данных» в боковом меню (в разделе «Хранилище данных»). В открывшемся окне необходимо указать (Рис. 312):

- «Имя» – название хранилища данных;
- «Путь к каталогу хранилища» – путь к каталогу, в котором будет создано хранилище данных;

- «Расписание сборщика мусора» – частота, с которой запускается сборка мусора;
- «Расписание удаления» – частота, с которой происходит удаление ранее созданных резервных копий;
- «Параметры удаления» – количество резервных копий, которые необходимо хранить.

PBS. Создание хранилища данных

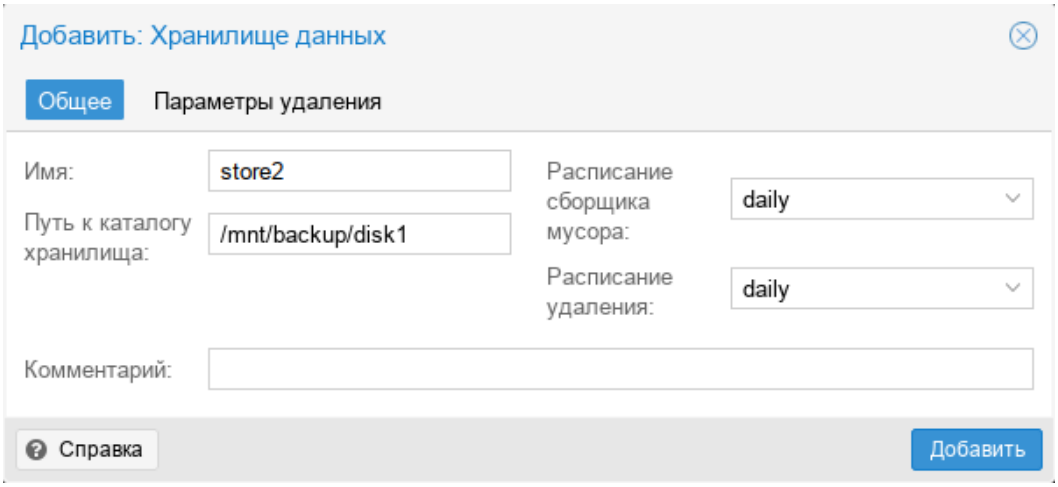


Рис. 312

Создание хранилища данных в командной строке:

```
# proxmox-backup-manager datastore create store2 /mnt/backup/disk1
```

Вывести список существующих хранилищ:

```
# proxmox-backup-manager datastore list
```

После создания хранилища данных в каталоге появляется следующий макет:

```
# ls -arilh /mnt/backup/disk1/
итого 1,1M
665243 -rw-r--r-- 1 backup backup    0 мар 31 14:05 .lock
665242 drwxr-x--- 1 backup backup 1,1M мар 31 14:05 .chunks
665240 drwxr-xr-x 3 root   root   4,0K мар 31 13:56 ..
665241 drwxr-xr-x 3 backup backup 4,0K мар 31 14:05
```

где:

- `.lock` – пустой файл, используемый для блокировки процесса;
- каталог `.chunks` – содержит подкаталоги с именами от 0000 до ffff. В этих каталогах будут храниться фрагментированные данные, полученные после выполнения операции резервного копирования.

5.12.3.3 Управление хранилищами данных

Вывести список существующих хранилищ:

```
# proxmox-backup-manager datastore list
```

Изменить расписание сборки мусора и вывести настройки хранилища данных:

```
# proxmox-backup-manager datastore update store2 --gc-schedule 'Tue 04:27'
# proxmox-backup-manager datastore show store2
```

Удалить хранилище данных:

```
# roxmox-backup-manager datastore remove store2
```

Данная команда удалит только конфигурацию хранилища данных, данные из базового каталога удалены не будут.

5.12.4 Управление трафиком

Создание и восстановление резервных копий может привести к большому трафику и повлиять на работу других пользователей сети или общих хранилищ.

PBS позволяет ограничить входящий (например, резервное копирование) и исходящий (например, восстановление) сетевой трафик из набора сетей. При этом можно настроить определенные периоды, в которые будут применяться ограничения.

Примечание. Ограничение скорости не влияет на задания синхронизации. Чтобы ограничить входящий трафик, создаваемый заданием синхронизации, необходимо настроить ограничение скорости входящего трафика для конкретного задания.

Настройка правила управления трафиком в веб-интерфейсе («Конфигурация» → «Управление трафиком» → «Добавить») показана на Рис. 313.

Управление трафиком в консоли:

- создать правило управления трафиком для ограничения всех клиентов IPv4 (сеть 0.0.0.0/0) до 100 МБ/с:

```
# proxmox-backup-manager traffic-control create rule0 --network 0.0.0.0/0 \
  --rate-in 100MB --rate-out 100MB \
  --comment "Default rate limit (100MB/s) for all clients"
```

- ограничить правило временными рамками:

```
# proxmox-backup-manager traffic-control update rule0 \
  --timeframe "mon..fri 8-19"
```

- вывести список текущих правил:

```
# proxmox-backup-manager traffic-control list
```

- удалить правило:

```
# proxmox-backup-manager traffic-control remove rule0
```

- показать состояние (текущую скорость передачи данных) всех настроенных правил:

```
# proxmox-backup-manager traffic-control traffic
```

PBS. Настройка правила управления трафиком

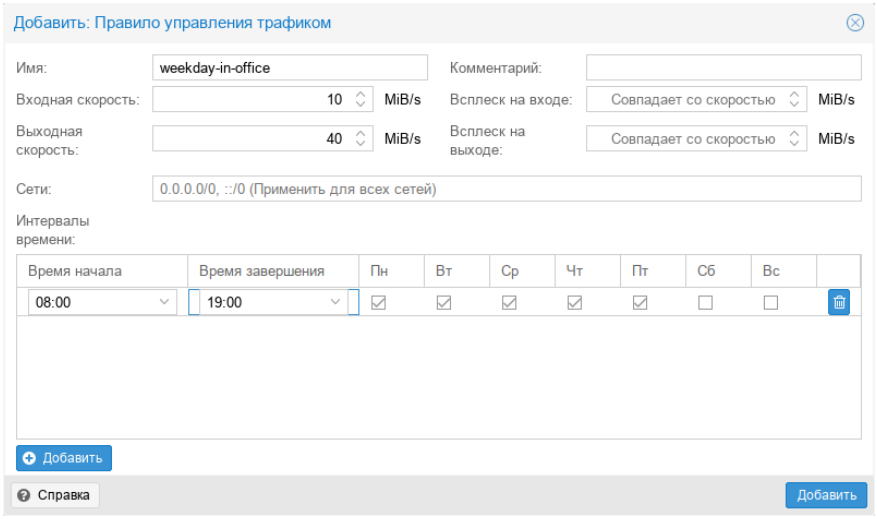


Рис. 313

5.12.5 Управление пользователями

PVE поддерживает несколько источников аутентификации (Рис. 314).

Выбор типа аутентификации в веб-интерфейсе

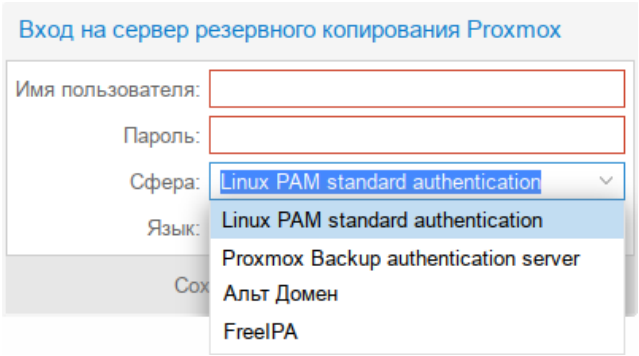


Рис. 314

PBS хранит данные пользователей в файле `/etc/proxmox-backup/user.cfg`.

Пользователя часто внутренне идентифицируют по его имени и области аутентификации в форме <user>@<realm>.

После установки PBS существует один пользователь root@pam, который соответствует суперпользователю ОС. Суперпользователь имеет неограниченные права, поэтому рекомендуется добавить других пользователей с меньшими правами.

5.12.5.1 Области аутентификации

PBS поддерживает следующие области (методы) аутентификации:

- «Стандартная аутентификация Linux PAM» («Linux PAM standart authentication») – при использовании этой аутентификации системный пользователь должен существовать (должен быть создан, например, с помощью команды adduser). Пользователь аутентифицируется с помощью своего обычного системного пароля;

- «Сервер аутентификации Proxmox Backup» («Proxmox Backup authentication server») – аутентификация Proxmox Backup Server. Хэшированные пароли хранятся в файле `/etc/proxmox-backup/shadow.json`;
- «Сервер LDAP» – позволяет использовать внешний LDAP-сервер для аутентификации пользователей (например, OpenLDAP);
- Сервер «Active Directory» – позволяет аутентифицировать пользователей через AD. Поддерживает LDAP в качестве протокола аутентификации;
- «Сервер OpenID Connect» – уровень идентификации поверх протокола OATH 2.0. Позволяет аутентифицировать пользователей на основе аутентификации, выполняемой внешним сервером авторизации.

5.12.5.1.1 Стандартная аутентификация Linux PAM

При использовании «Стандартная аутентификация Linux PAM», системный пользователь должен существовать (должен быть создан, например, с помощью команды adduser) на всех узлах, на которых пользователю разрешено войти в систему.

Область Linux PAM создается по умолчанию и не может быть удалена.

5.12.5.1.2 Сервер аутентификации Proxmox Backup

Область «Сервер аутентификации Proxmox Backup» представляет собой хранилище паролей в стиле Unix (`/etc/proxmox-backup/shadow.json`). Пароль шифруется с использованием метода хеширования SHA-256.

Область создается по умолчанию.

Для добавления пользователя в веб-интерфейсе следует в разделе «Конфигурация» → «Управление доступом» перейти на вкладку «Управление пользователями» и нажать кнопку «Добавить» (Рис. 315).

PBS. Добавление пользователя

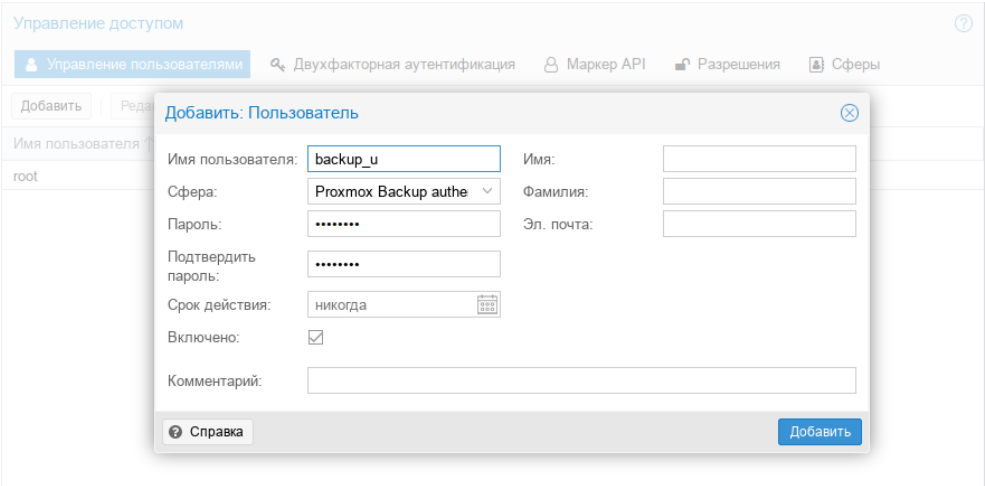


Рис. 315

Примеры использования командной строки для управления пользователями PBS:

- просмотреть список пользователей:

```
# proxmox-backup-manager user list
```

- создать пользователя:

```
# proxmox-backup-manager user create backup_u@pbs --email
backup_u@test.alt
```

- обновить или изменить любые свойства пользователя:

```
# proxmox-backup-manager user update backup_u@pbs --firstname Дмитрий
--lastname Иванов
```

- отключить учетную запись пользователя:

```
# proxmox-backup-manager user update backup_u@pbs --enable 0
```

- удалить учетную запись пользователя:

```
# proxmox-backup-manager user remove backup_u@pbs
```

5.12.5.1.3 LDAP аутентификация (FreeIPA)

В данном разделе приведён пример настройки LDAP аутентификации для аутентификации на сервере FreeIPA. В примере используются следующие исходные данные:

- ipa.example.test, 192.168.0.113 – сервер FreeIPA;
- admin@example.test – учётная запись с правами чтения LDAP;
- pve – группа, пользователи которой имеют право аутентифицироваться в PVE.

Для настройки аутентификации FreeIPA необходимо выполнить следующие шаги:

1) создать область аутентификации LDAP. Для этого в разделе «Конфигурация» → «Управление доступом» → «Сферы» нажать кнопку «Добавить» → «Сервер LDAP» (Рис. 316);

Создать область аутентификации LDAP

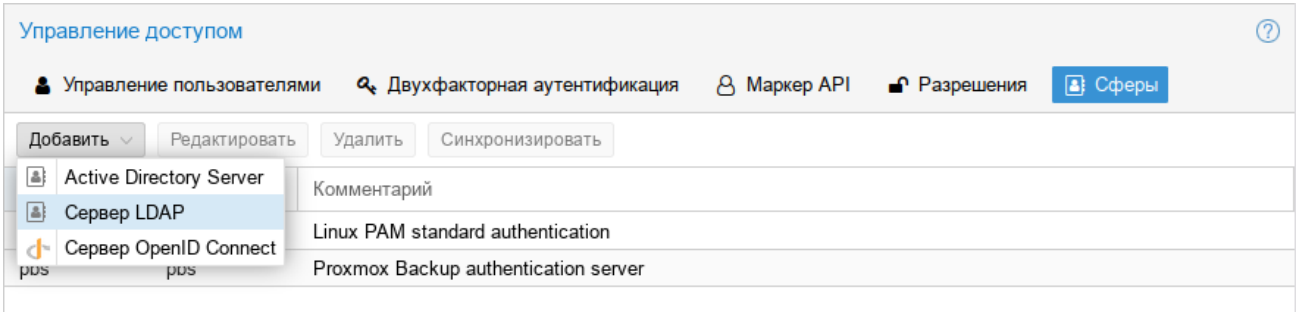


Рис. 316

2) на вкладке «Общее» (Рис. 317) указать следующие данные:

- «Сфера» – идентификатор области;
- «Имя основного домена» (base_dn) – каталог, в котором выполняется поиск пользователей (cn=accounts,dc=example,dc=test);

- «Имя пользовательского атрибута» (user_attr) – атрибут LDAP, содержащий имя пользователя, с которым пользователи будут входить в систему (uid);
- «Bind Domain Name» – имя пользователя (*uid=admin,cn=users,cn=accounts,dc=example,dc=test*);
- «Пароль (bind)» – пароль пользователя;
- «Сервер» – IP-адрес или имя FreeIPA-сервера (ipa.example.test или 192.168.0.113);
- «Резервный сервер» (опционально) – адрес резервного сервера на случай, если основной сервер недоступен;
- «Порт» – порт, который прослушивает сервер LDAP (обычно 389 без ssl, 636 с ssl).

Настройка LDAP аутентификации FreeIPA (вкладка «Общее»)

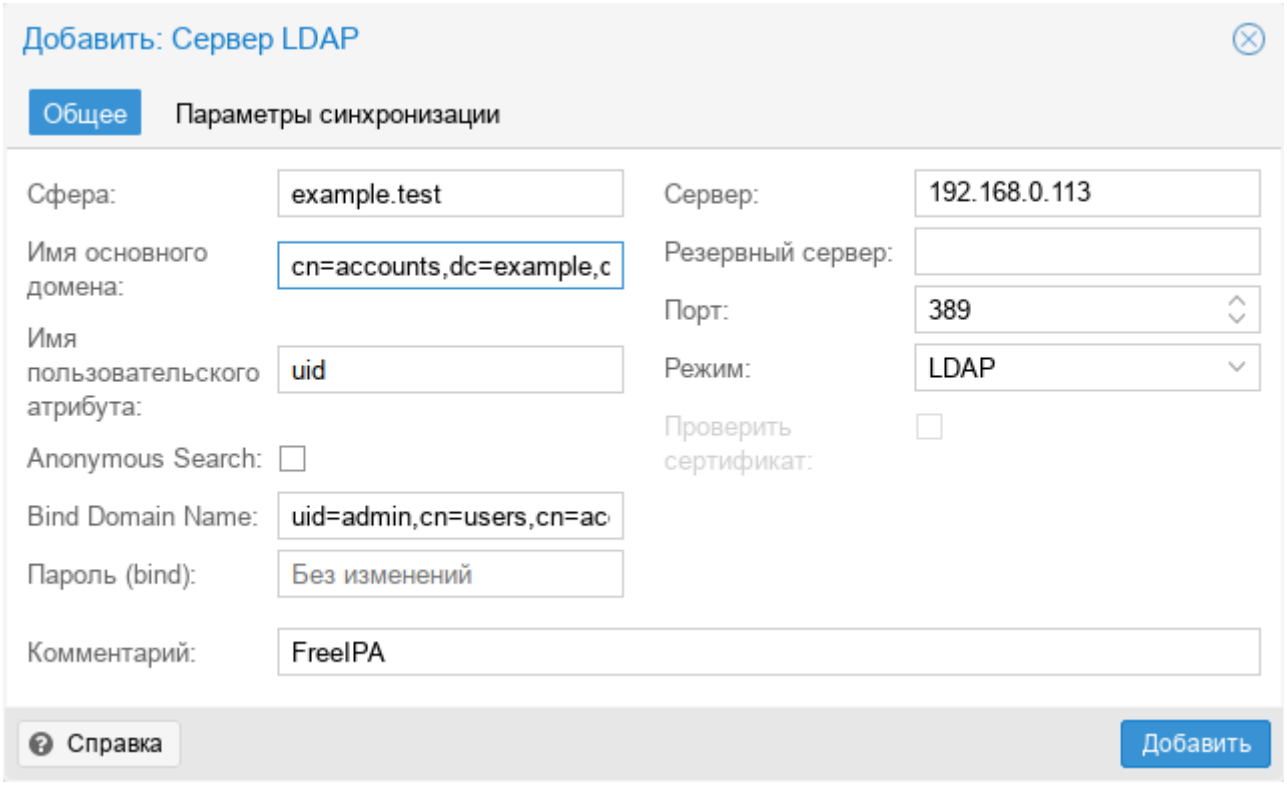


Рис. 317

3) на вкладке «Параметры синхронизации» (Рис. 318) заполнить следующие поля (в скобках указаны значения, используемые в данном примере):

- «Атрибут имени пользователя» (опционально) – атрибут LDAP, содержащий имя пользователя (*givenname*);
- «Атрибут фамилии пользователя» (опционально) – атрибут LDAP, содержащий фамилию пользователя (*sn*);
- «Атрибут электронной почты» (опционально) – атрибут LDAP, содержащий электронную почту пользователя (*mail*);
- «Классы пользователей» – класс пользователей LDAP (inetOrgPerson);

- «Фильтр пользователей» – фильтр пользователей (*memberOf=cn=pve,cn=groups,cn=accounts,dc=example,dc=test*);

Настройка LDAP аутентификации FreeIPA (вкладка «Параметры синхронизации»)

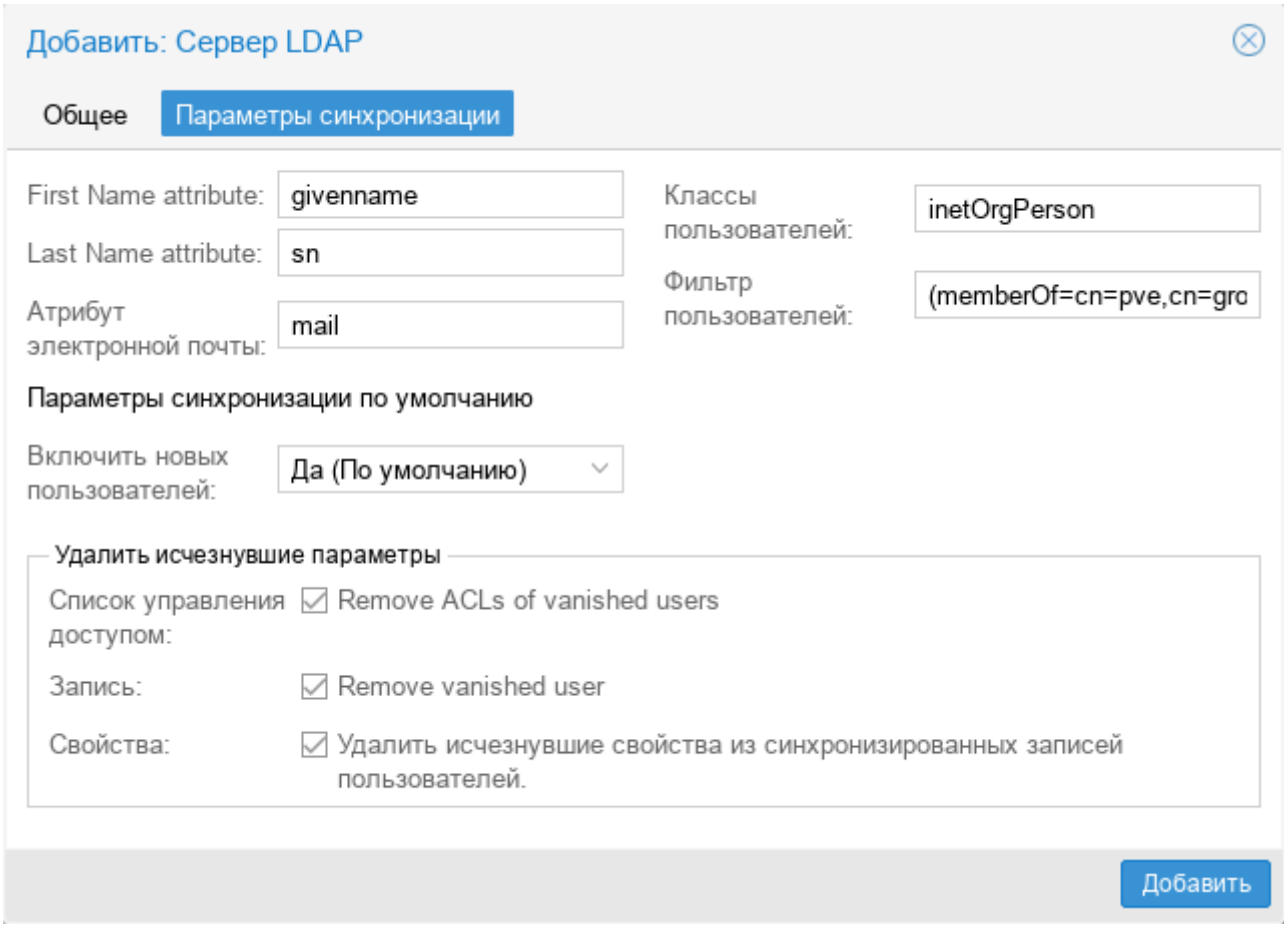


Рис. 318

4) нажать кнопку «Добавить»;

5) выбрать добавленную область и нажать кнопку «Синхронизировать» (Рис. 319);

Кнопка «Синхронизировать»

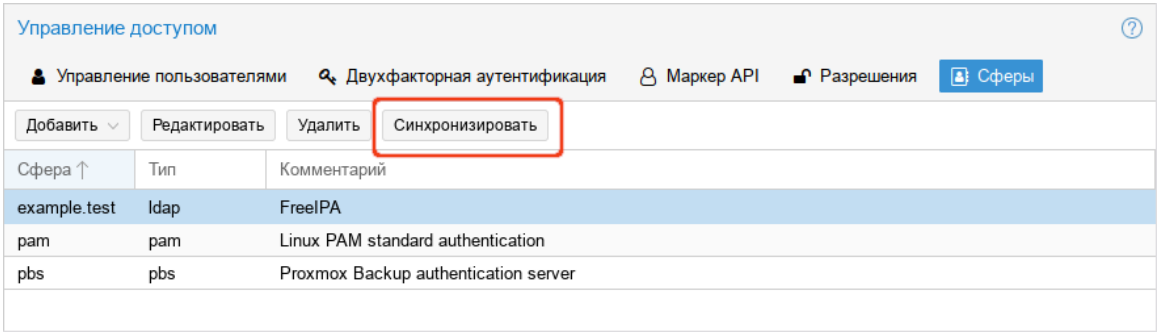


Рис. 319

6) указать, если необходимо, параметры синхронизации и нажать кнопку «Синхронизировать» (Рис. 320).

В результате синхронизации пользователи PBS будут синхронизированы с сервером FreeIPA LDAP. Сведения о пользователях можно проверить на вкладке «Управление пользователями».

7) Настроить разрешения для группы/пользователя на вкладке «Разрешения».

Параметры синхронизации области аутентификации

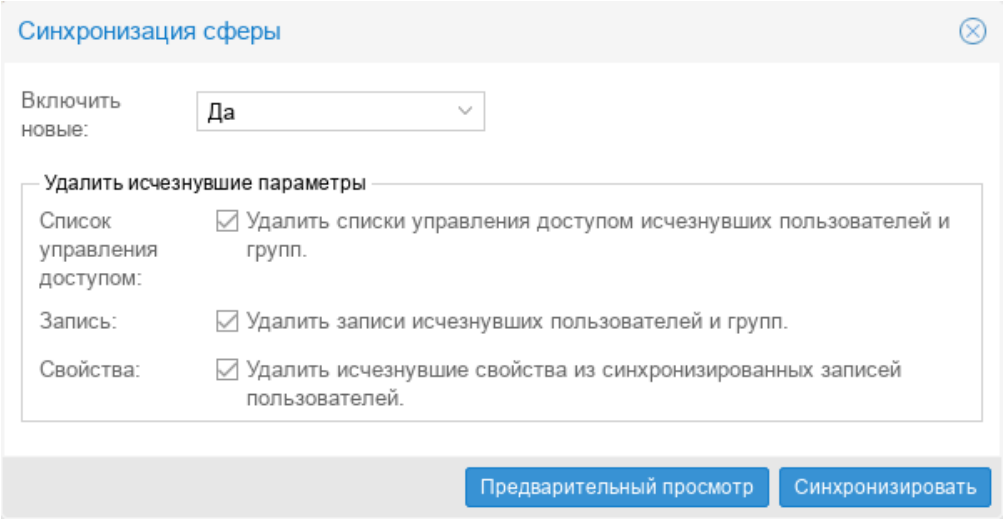


Рис. 320

Примечание. Команда синхронизации пользователей:

```
# proxmox-backup-manager ldap sync example.test
```

Для автоматической синхронизации пользователей можно добавить команду синхронизации в планировщик задач.

5.12.5.1.4 LDAP аутентификация («Альт Домен», AD)

В данном разделе приведён пример настройки аутентификации на сервере «Альт Домен». В примере используются следующие исходные данные:

- dc1.test.alt, 192.168.0.122 – сервер «Альт Домен»;
- administrator@test.alt – учётная запись администратора (для большей безопасности рекомендуется создать отдельную учетную запись с доступом только для чтения к объектам домена и не использовать учётную запись администратора);
- office – группа, пользователи которой имеют право аутентифицироваться в PVE.

Для настройки AD аутентификации необходимо выполнить следующие шаги:

1) создать область аутентификации LDAP. Для этого в разделе «Конфигурация» → «Управление доступом» → «Сферы» нажать кнопку «Добавить» → «Сервер LDAP» (Рис. 316);

2) на вкладке «Общее» (Рис. 321) указать следующие данные:

- «Сфера» – идентификатор области;
- «Имя основного домена» (base_dn) – каталог, в котором выполняется поиск пользователей (dc=test,dc=alt);

- «Имя пользовательского атрибута» (user_attr) – атрибут LDAP, содержащий имя пользователя, с которым пользователи будут входить в систему (sAMAccountName);
- «По умолчанию» – установить область в качестве области по умолчанию для входа в систему;
- «Bind Domain Name» – имя пользователя (*cn=Administrator,cn=Users,dc=test,dc=alt*);
- «Пароль (bind)» – пароль пользователя;
- «Сервер» – IP-адрес или имя сервера (dc1.test.alt или 192.168.0.122);
- «Резервный сервер» (опционально) – адрес резервного сервера на случай, если основной сервер недоступен;
- «Порт» – порт, который прослушивает сервер LDAP (обычно 389 без ssl, 636 с ssl).

Настройка LDAP аутентификации «Альт Домен» (вкладка «Общее»)

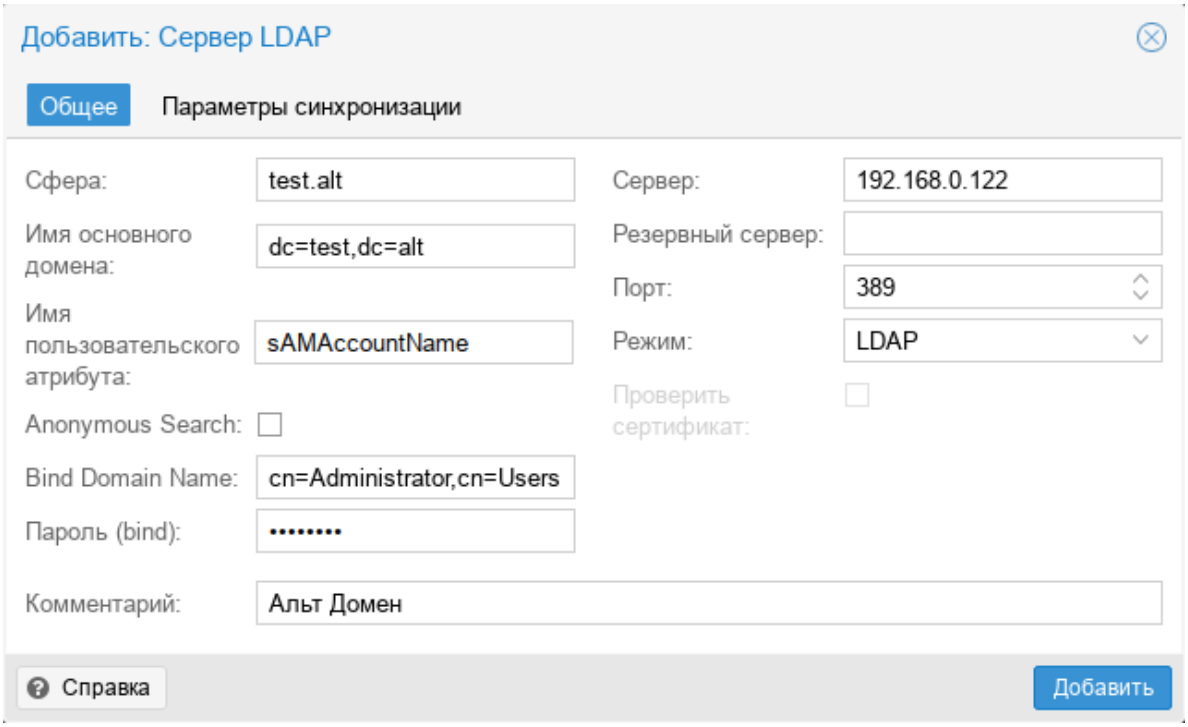


Рис. 321

3) на вкладке «Параметры синхронизации» (Рис. 322) заполнить следующие поля (в скобках указаны значения, используемые в данном примере):

- «Атрибут имени пользователя» (опционально) – атрибут LDAP, содержащий имя пользователя (*givenname*);
- «Атрибут фамилии пользователя» (опционально) – атрибут LDAP, содержащий фамилию пользователя (*sn*);
- «Атрибут электронной почты» (опционально) – атрибут LDAP, содержащий электронную почту пользователя (*mail*);
- «Классы пользователей» – класс пользователей LDAP (*user*);

- «Фильтр пользователей» – фильтр пользователей (*(&(objectclass=user)(samaccountname=*)(MemberOf=CN=office,cn=Users,dc=TEST,dc=ALT))*);

Настройка LDAP аутентификации «Альт Домен» (вкладка «Параметры синхронизации»)

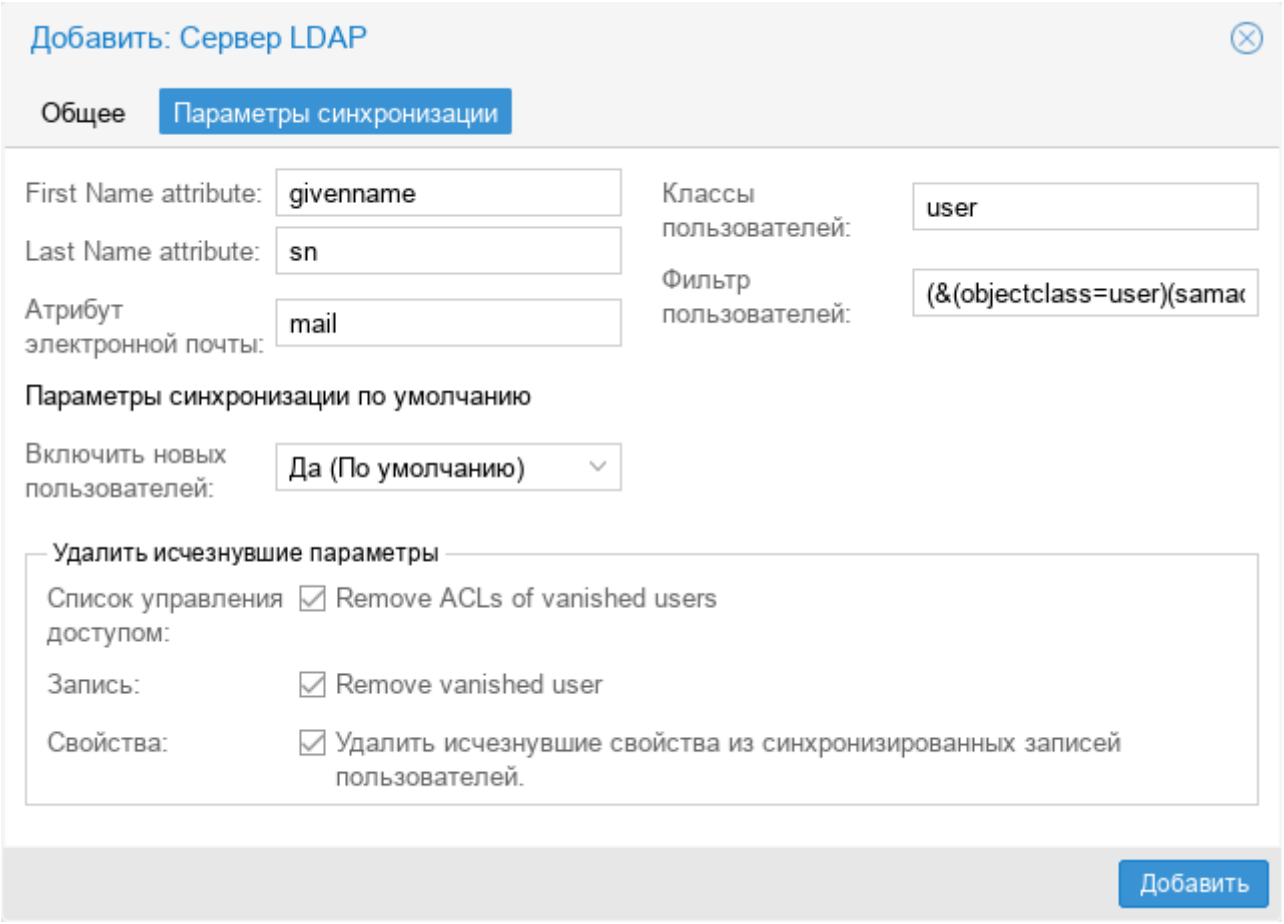


Рис. 322

4) нажать кнопку «Добавить»;

5) выбрать добавленную область и нажать кнопку «Синхронизировать»;

6) указать, если необходимо, параметры синхронизации и нажать кнопку «Синхронизировать» (Рис. 320).

В результате синхронизации пользователи PBS будут синхронизированы с сервером «Альт Домен». Сведения о пользователях можно проверить на вкладке «Управление пользователями».

7) Настроить разрешения для пользователя на вкладке «Разрешения».

Примечание. Команда синхронизации пользователей и групп:

```
# proxmox-backup-manager ldap sync test.alt
```

Для автоматической синхронизации пользователей и групп можно добавить команду синхронизации в планировщик задач.

5.12.5.2 API-токены

Любой аутентифицированный пользователь может генерировать API-токены, которые, в свою очередь, можно использовать для настройки клиентов резервного копирования вместо прямого указания имени пользователя и пароля.

Назначение API-токенов:

- простой отзыв в случае компрометации клиента;
- возможность ограничить разрешения для каждого клиента/токена в рамках разрешений пользователей.

Добавление API-токена в веб-интерфейсе показано на Рис. 323.

PBS. Добавление API-токена

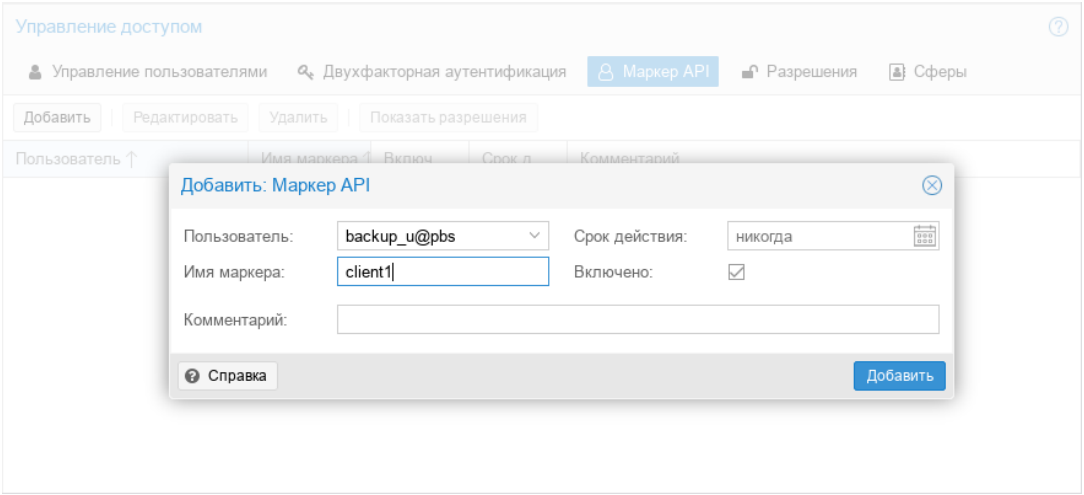


Рис. 323

API-токен состоит из двух частей (Рис. 324):

- идентификатор (Token ID), который состоит из имени пользователя, области и имени токена (user@realm!имя токена);
- секретное значение.

Обе части должны быть предоставлены клиенту вместо идентификатора пользователя и его пароля.

PBS. API-токен

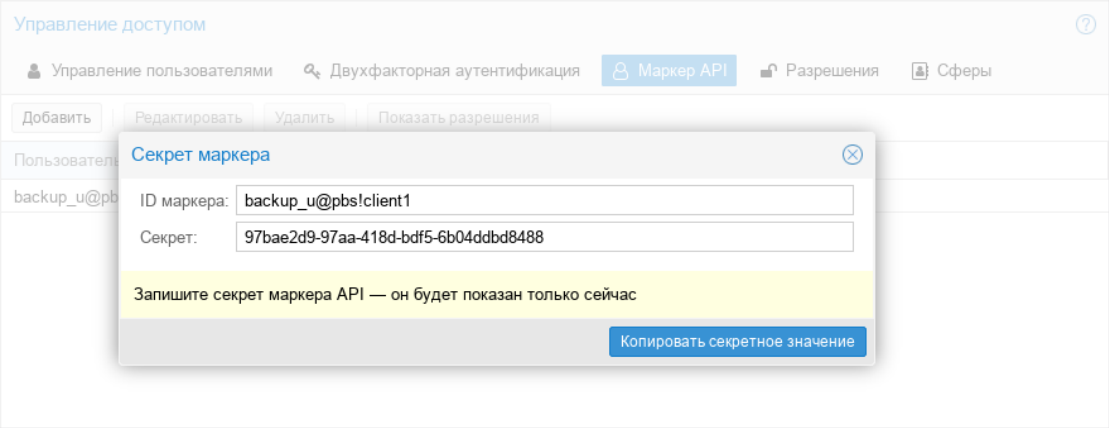


Рис. 324

Примечание. Отображаемое секретное значение необходимо сохранить, так как после создания токена его нельзя будет отобразить снова.

Создание API-токена в консоли:

```
# proxmox-backup-manager user generate-token backup_u@pbs client1
Result: {
  "tokenid": "backup_u@pbs!client1",
  "value": "ff13e5e0-30df-4a70-99f1-c62b13803769"
}
```

5.12.5.3 Управление доступом

По умолчанию новые пользователи и API-токены не имеют никаких разрешений. Добавить разрешения можно, назначив роли пользователям/токенам для определенных объектов, таких как хранилища данных или удаленные устройства.

Роль – это список привилегий. В PBS предопределён ряд ролей:

- NoAccess – нет привилегий (используется для запрета доступа);
- Admin – все привилегии;
- Audit – доступ только для чтения;
- DatastoreAdmin – все привилегии для хранилищ данных;
- DatastoreAudit – просмотр настроек хранилищ и их содержимых без возможности чтения фактических данных;
- DatastoreReader – просмотр содержимого хранилища, восстановление данных;
- DatastoreBackup – создание и восстановление собственных резервных копий;
- DatastorePowerUser – создание, восстановление и удаление собственных резервных копий;
- RemoteAdmin – все привилегии для удаленных PBS;
- RemoteAudit – просмотр настроек удаленных PBS;

- RemoteSyncOperator – чтение данных с удаленных PBS;
- TapeAdmin – все привилегии для резервного копирования на ленту;
- TapeAudit – просмотр настроек, показателей и состояния ленты;
- TapeOperator – создание и восстановление резервных копий на ленте без возможности изменения конфигурации;
- TapeReader – чтение и проверка конфигурации ленты.

PBS использует систему управления разрешениями на основе ролей и путей. Запись в таблице разрешений позволяет пользователю играть определенную роль при доступе к объекту или пути. Такое правило доступа может быть представлено как тройка (путь, пользователь, роль) или (путь, API-токен, роль), причем роль содержит набор разрешенных действий, а путь представляет цель этих действий.

Информация о правах доступа хранится в файле `/etc/proxmox-backup/acl.cfg`. Файл содержит 5 полей, разделенных двоеточием (':'):

```
acl:1:/datastore:backup_u@pbs!client1:DatastoreAdmin
```

В каждом поле представлены следующие данные:

- идентификатор acl;
- 1 или 0 – включено или отключено;
- объект, на который установлено разрешение;
- пользователи/токены, для которых установлено разрешение;
- устанавливаемая роль.

Добавление разрешения можно выполнить в веб-интерфейсе (Рис. 325): «Конфигурация» → «Управление доступом» вкладка «Разрешения».

PBS. Добавление разрешения

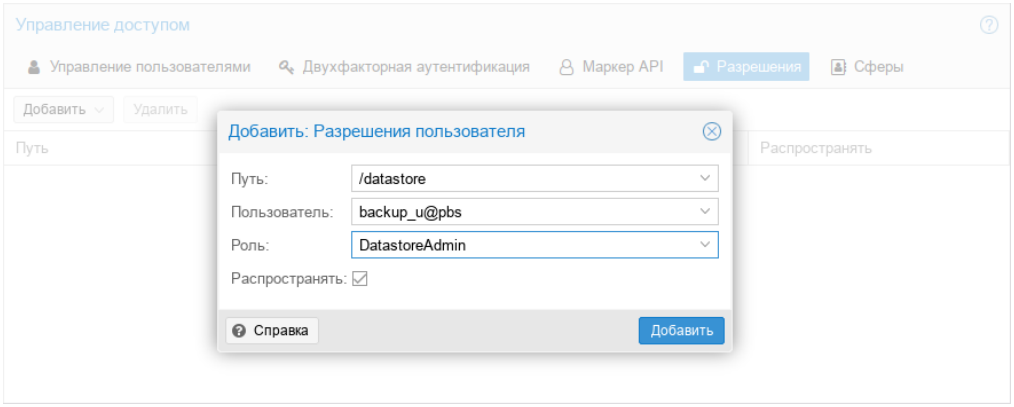


Рис. 325

Управление разрешениями в консоли:

- добавить разрешение (добавить пользователя backup_u@pbs в качестве администратора хранилища данных для хранилища данных store2, расположенного в /mnt/backup/disk1/store2):

```
# proxmox-backup-manager acl update /datastore/store2 DatastoreAdmin --auth-id
backup_u@pbs
```

- вывести список разрешений:

```
# proxmox-backup-manager acl list
```

- отобразить действующий набор разрешений пользователя или API-токена:

```
# proxmox-backup-manager user permissions backup_u@pbs --path /datastore/store2
    Privileges with (*) have the propagate flag set

    Path: /datastore/store1
    - Datastore.Audit (*)
    - Datastore.Backup (*)
    - Datastore.Modify (*)
    - Datastore.Prune (*)
    - Datastore.Read (*)
    - Datastore.Verify (*)
```

Примечание. Для токенов требуются собственные записи ACL. Токены не могут делать больше, чем их соответствующий пользователь.

5.12.5.4 Двухфакторная аутентификация

Примечание. Двухфакторная аутентификация реализована только для веб-интерфейса.

PBS поддерживает три метода двухфакторной аутентификации (Рис. 326):

- «TOTP» (одноразовый пароль на основе времени) – для создания этого кода используется алгоритм одноразового пароля с учетом времени входа в систему (код меняется каждые 30 секунд);
- «WebAuthn» (веб-аутентификация) – реализуется с помощью различных устройств безопасности, таких как аппаратные ключи или доверенные платформенные модули (TPM). Для работы веб-аутентификации необходим сертификат HTTPS;
- «Ключи восстановления» – список ключей, каждый из которых можно использовать только один раз. В каждый момент времени у пользователя может быть только один набор одноразовых ключей.

PBS. Двухфакторная аутентификация

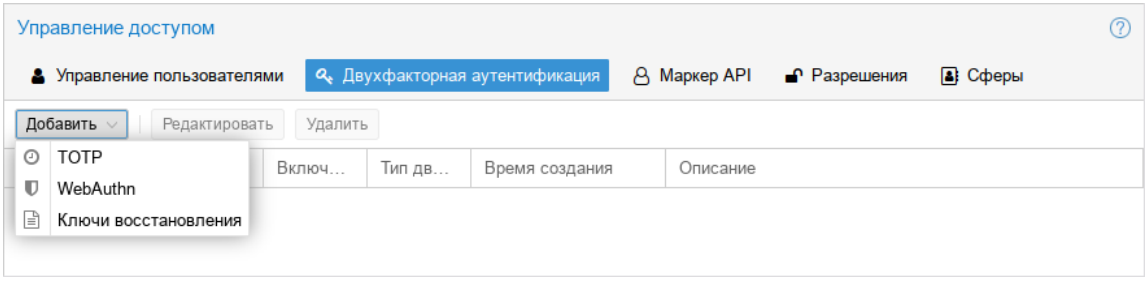


Рис. 326

Процедура добавления аутентификации «TOTP» показана на Рис. 327. При аутентификации пользователя будет запрашиваться второй фактор (Рис. 328).

PBS. Настройка аутентификации TOTP

Рис. 327

Запрос второго фактора (TOTP) при аутентификации пользователя в веб-интерфейсе

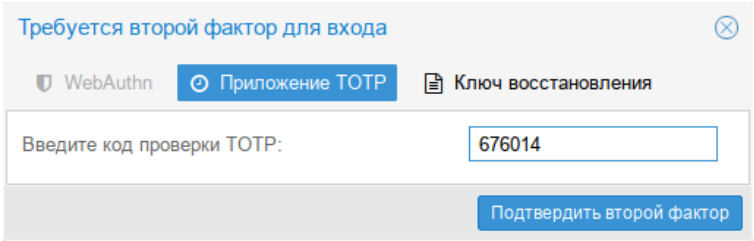


Рис. 328

При настройке аутентификации «Ключи восстановления» необходимо создать набор ключей (Рис. 329). При аутентификации пользователя будет запрашиваться второй фактор (Рис. 330).

PBS. Настройка аутентификации «Ключи восстановления»

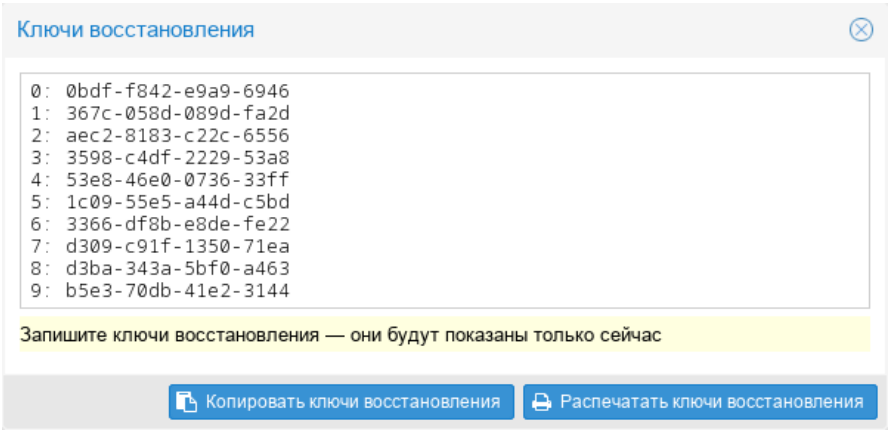


Рис. 329

Запрос второго фактора («Ключи восстановления») при аутентификации пользователя в веб-интерфейсе

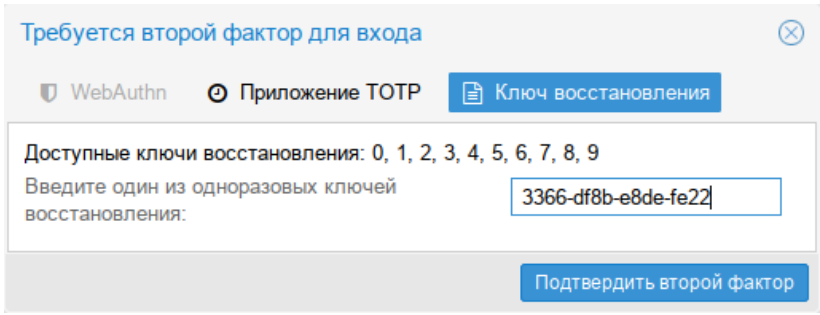


Рис. 330

Примечание. 8 неудачных попыток ввода кода TOTP отключат факторы TOTP пользователя. Они разблокируются при входе в систему с ключом восстановления. Если TOTP был единственным доступным фактором, потребуется вмешательство администратора, и настоятельно рекомендуется потребовать от пользователя немедленно изменить свой пароль. Администратор может разблокировать двухфакторную аутентификацию пользователя в веб-интерфейсе (Рис. 331) или в командной строке:

```
# proxmox-backup-manager user tfa unlock backup_u@pbs
```

PBS. Разблокировка двухфакторной аутентификации

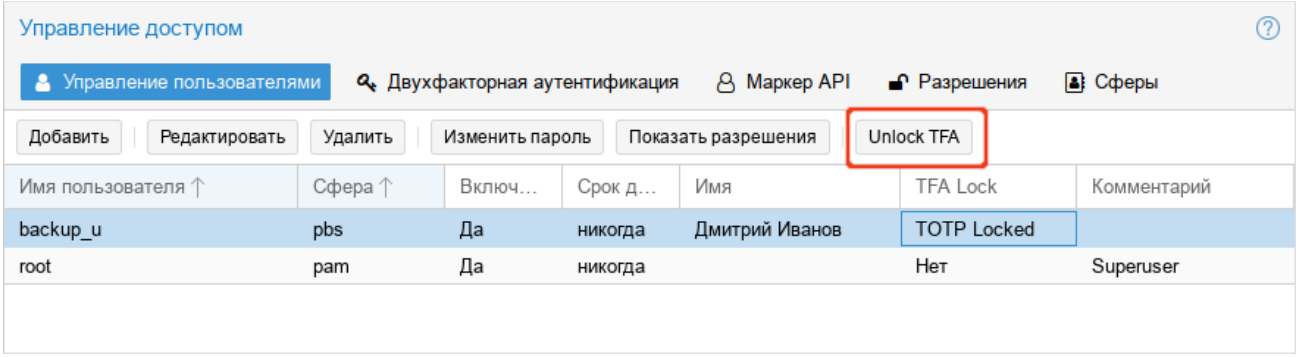


Рис. 331

5.12.6 Управление удалёнными PBS

Хранилища данных с удалённого сервера можно синхронизировать с локальным хранилищем с помощью задания синхронизации.

Информация о конфигурации удалённых PBS хранится в файле `/etc/proxmox-backup/remote.cfg`.

Для добавления удалённого PBS в веб-интерфейсе следует перейти в раздел «Конфигурация» → «Удалённые хранилища» и нажать кнопку «Добавить» (Рис. 332).

PBS. Добавление удалённого PBS

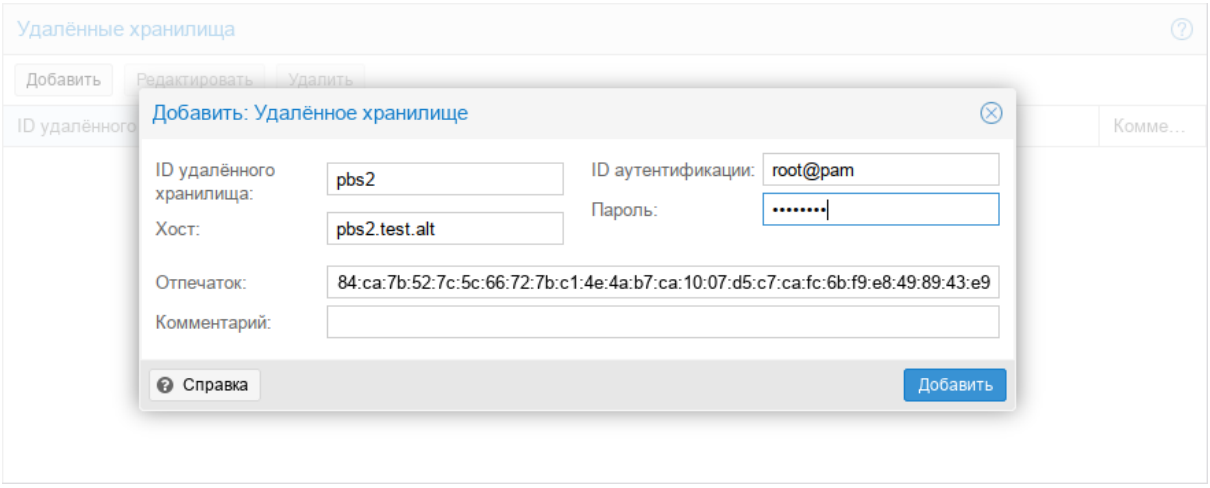


Рис. 332

Примечание. Отпечаток TLS-сертификата можно получить в веб-интерфейсе удалённого PBS (Рис. 333).

PBS. Отпечаток TLS-сертификата

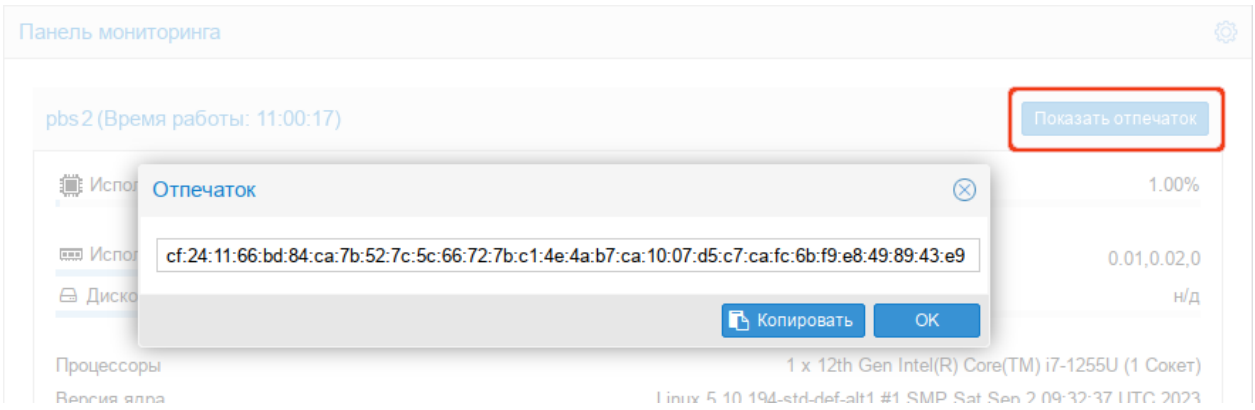


Рис. 333

Получить отпечаток в командной строке:

```
# proxmox-backup-manager cert info | grep Fingerprint
```

Для настройки задачи синхронизации, необходимо в разделе «Хранилище данных» перейти на вкладку «Задания синхронизации» и нажать кнопку «Добавить» (Рис. 334).

PBS. Добавление задачи синхронизации

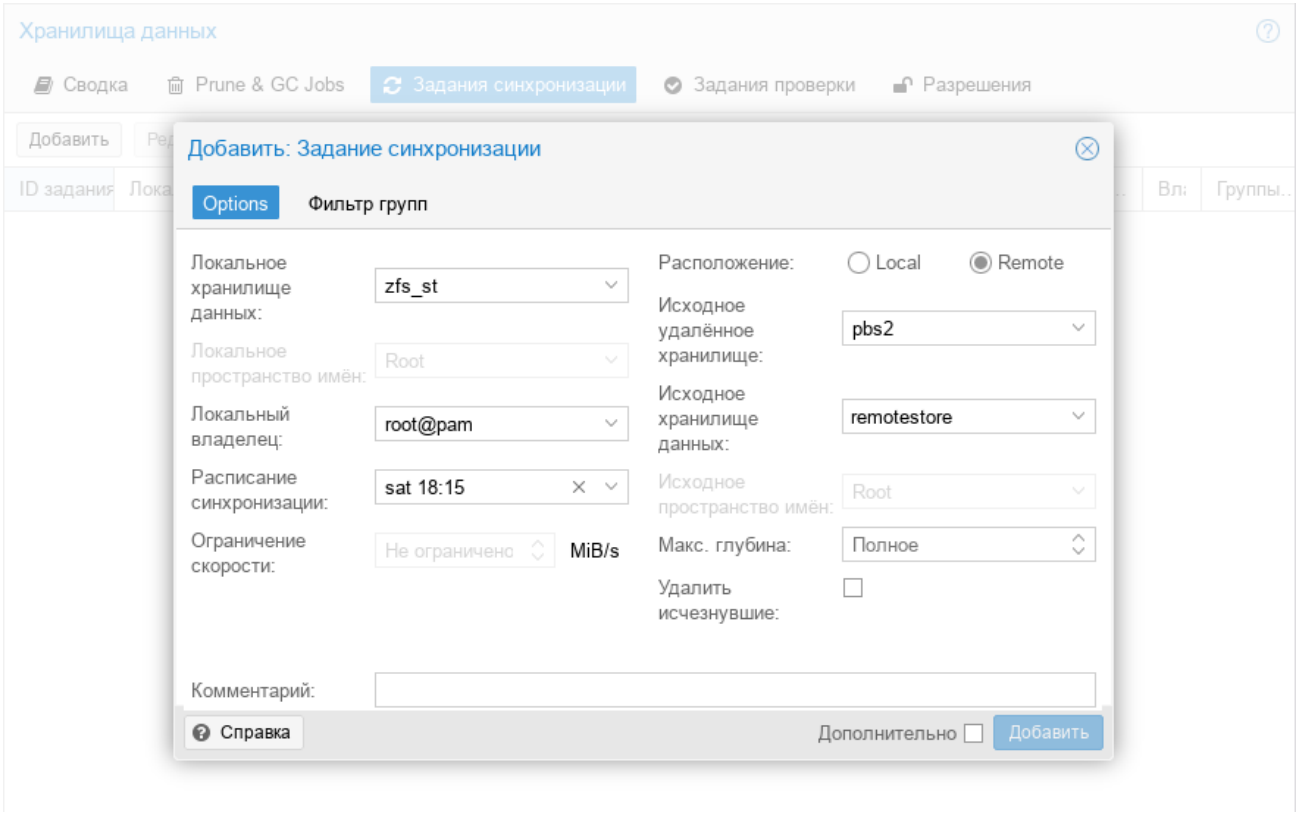


Рис. 334

После того, как задание синхронизации создано, оно будет запускаться по заданному расписанию, а также его можно запустить вручную из веб-интерфейса (кнопка «Запустить сейчас»).

Управление удалёнными PBS в консоли:

- добавить удалённый PBS:

```
# proxmox-backup-manager remote create pbs2 --host pbs2.test.alt \
--auth-id root@pam --password 'SECRET' --fingerprint
42:5d:ff:3a:50:38:53:5a:9b:f7:50:...:ab:1b
```

- вывести список удалённых PBS:

```
# proxmox-backup-manager remote list
```

- удалить удалённый PBS:

```
# proxmox-backup-manager remote remove pbs2
```

Примечание. Удалённый PBS можно удалить, только если с ним не связано ни одно задание синхронизации.

Управление задачами синхронизации в консоли:

- добавить задачу синхронизации:

```
# proxmox-backup-manager sync-job create test_job --remote pbs2 \
--remote-store remotestore --store zfs_st --schedule 'Sat 18:15'
```

- вывести список задач синхронизации:

```
# proxmox-backup-manager sync-job list
```

- изменить задачу синхронизации:

```
# proxmox-backup-manager sync-job update test_job --comment 'offsite'
```

- удалить задачу синхронизации:

```
# proxmox-backup-manager sync-job remove test_job
```

5.12.7 Клиент резервного копирования

Клиент резервного копирования использует следующий формат для указания репозитория хранилища данных на сервере резервного копирования (где имя пользователя указывается в виде user@realm):

```
[[пользователь@]сервер[:порт]:]datastore
```

Значение по умолчанию для пользователя – root@pam. Если сервер не указан, используется localhost. Примеры репозиториев показаны в табл. 1.

Указать репозиторий можно, передав его в параметре `--repository`, или установив переменную окружения PBS_REPOSITORY, например:

```
# export PBS_REPOSITORY=pbs.test.alt:store1
```

Т а б л и ц а 3 – Примеры репозиториев

Пример	Пользователь	Хост:Порт	Хранилище
store1	root@pam	localhost:8007	store1
pbs.test.alt:store1	root@pam	pbs.test.alt:8007	store1
backup_u@pbs@pbs.test.alt:store1	backup_u@pbs	pbs.test.alt:8007	store1
backup_u@pbs!client1@pbs.test.alt:store1	backup_u@pbs!client1	pbs.test.alt:8007	store1
192.168.0.123:1234:store1	root@pam	192.168.0.123:1234	store1

5.12.7.1 Создание резервной копии

В этом разделе рассмотрено, как создать резервную копию внутри машины (физического хоста, ВМ или контейнера). Такие резервные копии могут содержать архивы файлов и образов.

Создать резервную копию домашнего каталога пользователя user (будет создан архив user.pxar):

```
$ proxmox-backup-client backup user.pxar:/home/user/ \
--repository pbs.test.alt:store1

Starting backup: host/host-01/2024-11-08T10:27:26Z
Client name: host-01
Starting backup protocol: Fri Nov  8 12:27:28 2024
fingerprint:
5b:ed:9e:af:a5:ac:48:5b:4a:64:5d:05:10:b0:fb:02:75:0f:f3:fe:e8:6b:82:51:a0:aa
:5f:aa:68:90:3d:f1
```

```
Are you sure you want to continue connecting? (y/n): y
No previous manifest available.
Upload directory '/home/user/' to 'pbs.test.alt:store1' as user.pxar.didx
user.pxar: had to backup 667.04 MiB of 667.04 MiB (compressed 190.182 MiB) in
26.22s
user.pxar: average backup speed: 25.436 MiB/s
Uploaded backup catalog (109.948 KiB)
Duration: 9.59s
End Time: Fri Nov  8 12:27:38 2024
```

Команда `proxmox-backup-client backup` принимает список параметров резервного копирования, включая имя архива на сервере, тип архива и источник архива на клиенте, в формате:

`<archive-name>.<type>:<source-path>`

Тип архива .pxar используется для файловых архивов, а .img – для образов блочных устройств.

Команда создания резервной копии блочного устройства:

```
$ proxmox-backup-client backup mydata.img:/dev/mylvm/mydata \
--repository pbs.test.alt:zfs_st

Starting backup: host/host-01/2024-11-08T12:48:58Z
Client name: host-01
Starting backup protocol: Fri Nov  8 14:49:00 2024
storing login ticket failed: $XDG_RUNTIME_DIR must be set
No previous manifest available.
Upload image '/dev/mylvm/mydata' to 'pbs.test.alt:zfs_st' as mydata.img.fidx
mydata.img: had to backup 4.355 GiB of 20.43 GiB (compressed 2.018 GiB) in
77.94s
mydata.img: average backup speed: 57.226 MiB/s
mydata.img: backup was done incrementally, reused 16.074 GiB (78.7%)
Duration: 81.86s
End Time: Fri Nov  8 14:50:22 2024
```

Примечание. При запуске команды резервного копирования может быть получен такой вывод:

```
'Previous manifest does not contain an archive called 'mydata.img.fidx',
skipping download..'
```

Это не является ошибкой, следует дождаться окончания процесса, создания резервной копии.

Примечание. Создание резервной копии может занять продолжительное время, необходимо дождаться окончания процесса. Убедиться в том, что резервное копирование выполняется можно в веб-интерфейсе PBS, нажав кнопку «Задачи» (Рис. 335).

PBS. Выполняется задача резервного копирования

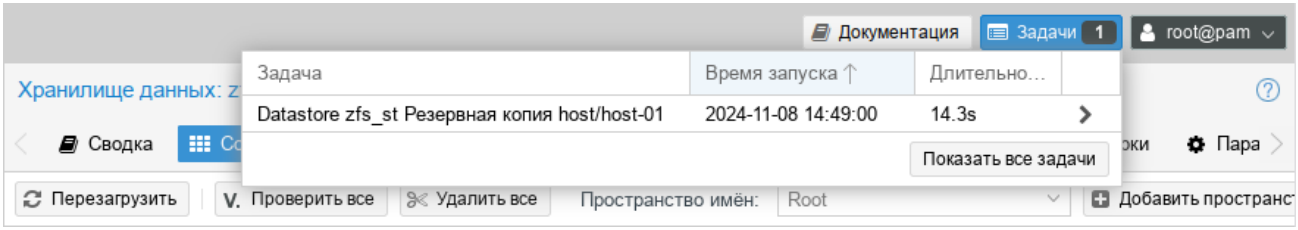


Рис. 335

5.12.7.2 Создание зашифрованной резервной копии

PBS поддерживает шифрование на стороне клиента с помощью AES-256 в режиме GCM.

Создание ключа шифрования:

```
$ proxmox-backup-client key create my-backup.key

Encryption Key Password: ******
Verify Password: ******
```

Создание зашифрованной резервной копии:

```
$ proxmox-backup-client backup user_s.pxar:/home/user/ \
--repository pbs.test.alt:store1 --keyfile ./my-backup.key

Password for "root@pam": ***
Starting backup: host/host-01/2024-11-08T10:29:25Z
Client name: host-01
Starting backup protocol: Fri Nov  8 12:29:25 2024
Using encryption key from './my-backup.key'..
Encryption Key Password: ********
Encryption key fingerprint: 31:96:7f:6f:80:1f:0c:b4
Downloading previous manifest (Fri Nov  8 12:27:26 2024)
Upload directory '/home/user/' to '192.168.0.123:store1' as user_s.pxar.didx
user_s.pxar: had to backup 667.04 MiB of 667.04 MiB (compressed 190.028 MiB)
in 21.16s
user_s.pxar: average backup speed: 31.518 MiB/s
Uploaded backup catalog (109.971 KiB)
Duration: 5.77s
End Time: Fri Nov  8 12:29:31 2024
```

Содержимое хранилища store1 показано на Рис. 336.

PBS. Содержимое хранилища store1

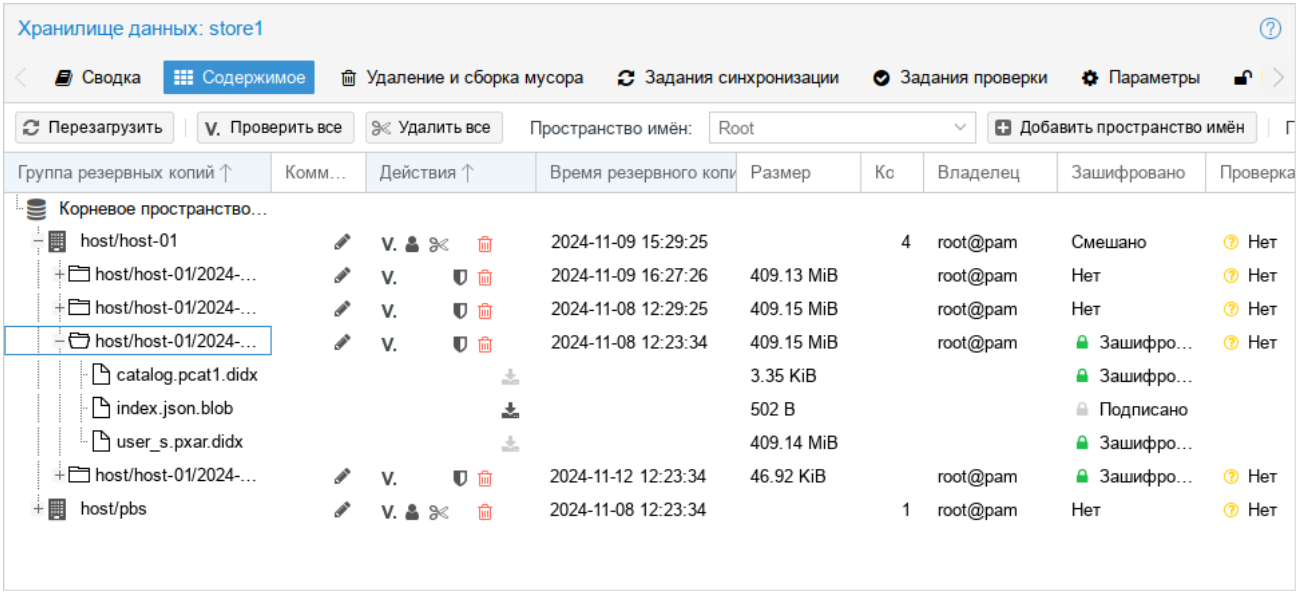


Рис. 336

5.12.7.3 Восстановление данных

Просмотреть список всех снимков на сервере:

```
$ proxmox-backup-client snapshot list --repository pbs.test.alt:store1
```

```
┌──────────────────────────────────┬──────────┬──────────────────────────────────┐
│snapshot                          │      size│files                             │
╞══════════════════════════════════╪══════════╪══════════════════════════════════╡
│host/host-01/2024-11-08T10:27:26Z│25.359 KiB│catalog.pcat1 index.json user.pxar │
├──────────────────────────────────┼──────────┼──────────────────────────────────┤
│host/host-01/2024-11-08T10:23:34Z│25.989 KiB│catalog.pcat1 index.json user_s.pxar│
└──────────────────────────────────┴──────────┴──────────────────────────────────┘
```

Просмотреть содержимое снимка:

```
$ proxmox-backup-client catalog dump host/host-01/2024-11-08T10:27:26Z \
--repository pbs.test.alt:store1
```

Команда восстановления архива из резервной копии:

```
proxmox-backup-client restore <снимок> <имя-архива> <целевой-путь> [ОПЦИИ]
```

Восстановить архив user.pxar в каталог `/home/user/restore`:

```
$ proxmox-backup-client restore host/host-01/2024-11-08T10:27:26Z \
user.pxar /home/user/restore  --repository store1
```

Получить содержимое любого архива можно, восстановив файл index.json в репозитории по целевому пути «-»:

```
$ proxmox-backup-client restore host/host-01/2024-11-08T10:27:26Z \
index.json - --repository pbs.test.alt:store1
```

При этом содержимое архива будет выведено на стандартный вывод.

Если необходимо восстановить несколько отдельных файлов, можно использовать интерактивную оболочку восстановления:

```
$ proxmox-backup-client catalog shell host/host-01/2024-11-08T10:27:26Z \
user.pxar --repository pbs.test.alt:store1

Starting interactive shell
pxar:/ > ls
…
```

Пример поиска в содержимом архива и восстановление данных:

```
pxar:/ > find  *.txt --select
/test/connection_trace.txt
/Рабочий стол/1.txt
pxar:/ > list-selected
/test/connection_trace.txt
/Рабочий стол/1.txt
pxar:/ > restore-selected /home/user/restore/
pxar:/ > restore /home/user/conf/ --pattern *.conf
pxar:/ > exit
```

где:

- `find *.txt --select` – найти все файлы с расширением .txt и добавить соответствующие шаблоны в список для последующего восстановления;
- `list-selected` – вывести шаблоны на экран;
- `restore-selected /home/user/restore/` – восстановить все файлы в архиве, соответствующие шаблонам в `/home/user/restore/` на локальном хосте;
- `restore /home/user/conf/ --pattern *.conf` – восстановить все файлы с расширением .conf в `/home/user/conf/` на локальном хосте.

5.12.7.4 Вход и выход

При первой попытке получить доступ к серверу с использованием команды proxmox-backup-client, потребуется ввести пароль пользователя. Сервер проверяет учётные данные и отправляет билет, действительный в течение двух часов. Клиент использует этот билет для последующих запросов к этому серверу.

Можно вручную инициировать вход/выход. Команда входа:

```
$ proxmox-backup-client login --repository pbs.test.alt:store1

Password for "root@pam": ******
```

Удалить билет:

```
$ proxmox-backup-client logout --repository pbs.test.alt:store1
```

5.12.8 Интеграция с PVE

PBS можно интегрировать в автономную или кластерную установку PVE, добавив его в качестве хранилища (Рис. 337).

PVE. Добавление хранилища Proxmox Backup Server

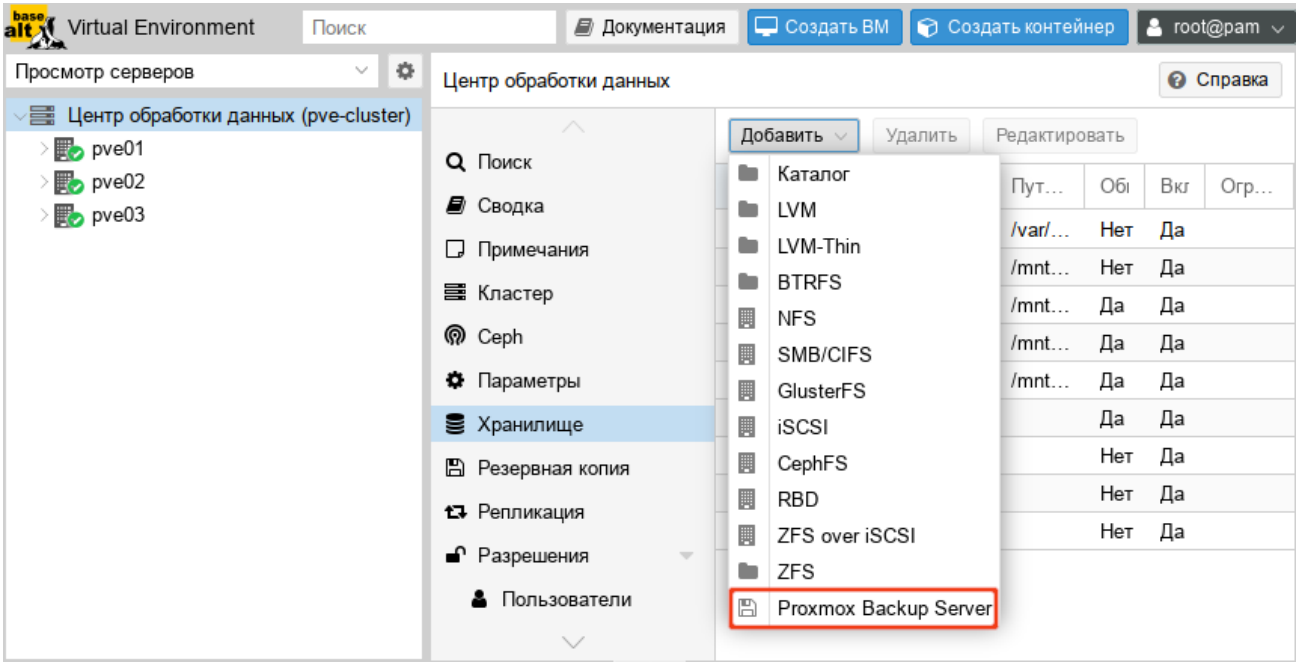


Рис. 337

Диалог создания хранилища pbs_backup типа «Proxmox Backup Server» для хранения резервных копий представлен на Рис. 338.

PVE. Диалог создания хранилища Proxmox Backup Server

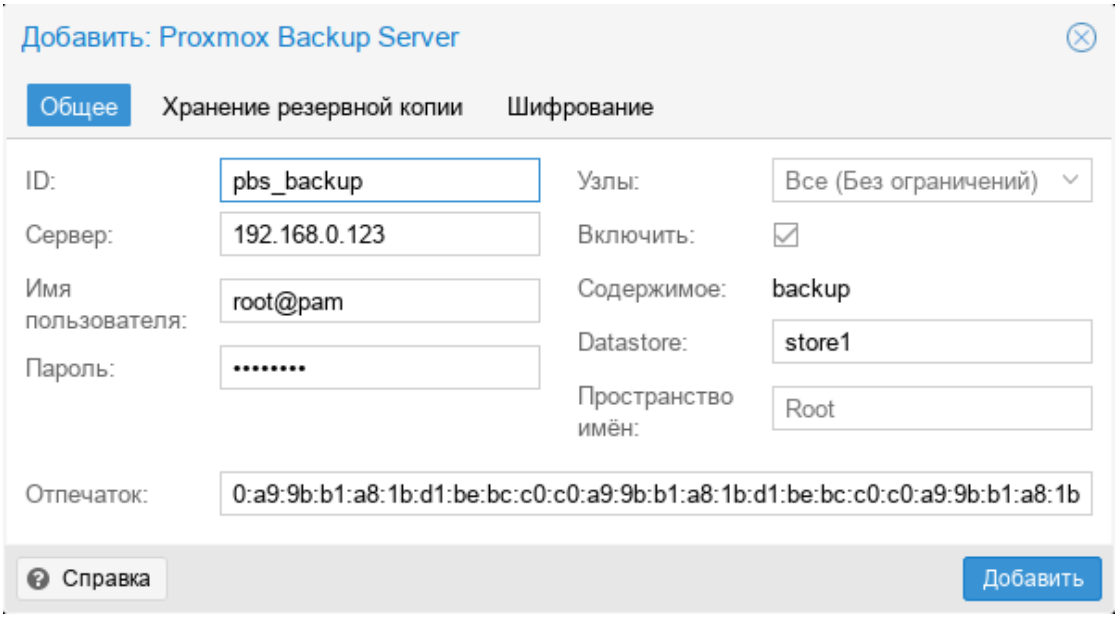


Рис. 338

Примечание. Отпечаток TLS-сертификата можно получить в веб-интерфейсе сервера резервного копирования (Рис. 333). Получить отпечаток можно, выполнив следующую команду на сервере резервного копирования:

```
# proxmox-backup-manager cert info | grep Fingerprint

Fingerprint (sha256):
c8:26:af:4a:c3:dc:60:72:4a:0b:4d:c1:e6:58:02:62:90:39:cb:fc:75:5d:00:9a:57:ca
:3d:28:a0:2c:99:a5
```

Добавление хранилища в командной строке:

```
# pvesm add pbs pbs_backup --server pbs.test.alt --datastore store1 \
--fingerprint c8:26:af:4a:c3:dc:60:72:...:99:a5 \
--username root@pam --password
```

Просмотреть состояние хранилища:

```
# pvesm status --storage pbs_backup

Name         Type Status  Total     Used     Available  %
pbs_backup   pbs  active  30786448  3097752  26099504   10.06%
```

Добавив хранилище данных типа Proxmox Backup Server в PVE, можно создавать резервные копии ВМ и контейнеров в это хранилище, так же как и в любые другие хранилища.

5.12.9 Резервное копирование на ленту

Резервное копирование на ленту обеспечивает простой способ хранения содержимого хранилища данных на магнитных лентах. Это повышает безопасность данных, за счёт получения дополнительной копии данных, на другом типе носителя (лента), в другом расположении (можно переместить ленты за пределы объекта).

При восстановлении данных из резервных копий чаще всего восстанавливаются данные последнего задания резервного копирования. Запросы на восстановление уменьшаются по мере старения данных. Учитывая это, резервное копирование на ленту может сократить использование дискового пространства, поскольку можно удалить данные с диска после их архивации на ленте. Это особенно актуально, если необходимо хранить данные в течение нескольких лет.

Резервные копии на ленте не обеспечивают произвольный доступ к хранящимся данным. Для получения доступа к данным, необходимо предварительно восстановить данные на диск. Кроме того, если ленты хранятся за пределами объекта, необходимо вернуть их на место, прежде чем выполнять какие-либо операции по восстановлению. Поэтому восстановление с ленты может занять гораздо больше времени, чем восстановление с диска.

Примечание. PBS хранит сжатые данные, поэтому использование функции сжатия ленты не даёт преимуществ.

5.12.9.1 Поддерживаемое оборудование

PBS поддерживает Linear Tape-Open 5-го поколения (LTO-5) или новее, а также обеспечивает максимальную поддержку 4-го поколения (LTO-4).

Смена лент осуществляется по протоколу SCSI Medium Changer, поэтому все современные ленточные библиотеки должны работать.

Современные ленты LTO-8 обеспечивают скорость чтения/записи до 360 МБ/с. Для полной записи или чтения одной ленты требуется минимум 9 часов (даже на максимальной скорости).

Единственный способ увеличить скорость передачи данных – использовать более одного привода. Таким образом, можно запускать несколько заданий резервного копирования параллельно или запускать задания восстановления, в то время как другие приводы используются для резервного копирования.

Необходимо также учитывать, что сначала необходимо прочитать данные из хранилища данных (диска). Однако жёсткий диск не может доставлять данные с такой скоростью. На практике скорость может быть от 60 до 100 МБ/с, поэтому для чтения 12 ТБ, необходимых для заполнения ленты LTO-8, требуется 33 часа. Для того чтобы записывать на ленту на полной скорости, необходимо убедиться, что исходное хранилище данных способно обеспечить такую производительность (например, использовать SSD).

Начиная с LTO-9, при первом использовании необходимо обязательно калибровать (инициализировать) любой новый носитель в ленточном приводе, для получения максимальной емкости хранения и надежности записи. Калибровка занимает от 40 до 120 минут на каждый носитель. Рекомендуется инициализировать носитель с помощью инструментов, предоставленных поставщиком оборудования накопителя или чейнджера. Некоторые устройства смены лент имеют метод «массовой» инициализации носителя.

Форматирование лент на PBS обрабатывается по-разному, чтобы избежать повторной оптимизации для каждого формата/маркировки. Если нужно отформатировать носитель для использования с PBS в первый раз или после использования с другой программой, следует либо использовать функциональные возможности привода/чейнджера, либо использовать «медленное» форматирование в командной строке:

```
# proxmox-tape format --drive your-drive --fast 0
```

При этом будут полностью удалены все ранее существовавшие данные, и будет запущен этап оптимизации.

Если носитель LTO-9 форматируется с помощью «быстрого» метода (по умолчанию или с параметром `--fast 1`), будет отформатирован только первый раздел.

5.12.9.2 Быстрый старт

Для резервного копирования на ленту необходимо выполнить следующие действия:

1) настроить оборудование (приводы и устройства смены лент);
2) настроить один или несколько пулов носителей;
3) промаркировать картриджи с лентой;
4) запустить задание резервного копирования на ленту.

Дополнительно рекомендуется выполнить следующие настройки:

1) убедиться, что присутствует загруженный в ядро модуль (драйвер) sg:

```
# lsmod | grep sg
```

Если команда не вывела результата, необходимо загрузить модуль sg:

```
# modprobe sg
```

Чтобы можуль sg загружался при загрузке системы, необходимо создать файл `/etc/modules-load.d/sg.conf`, в который добавить имя модуля sg:

```
# echo sg > /etc/modules-load.d/sg.conf
```

2) установить пакеты mt-st и mtx, если они еще не установлены:

```
# apt-get install mt-st mtx
```

3) для удобства отображения устройств на шине SCSI можно также установить пакет lsscsi и выполнить поиск устройств на шине:

```
# apt-get install lsscsi
# lsscsi -g (либо # lsscsi -vd)
```

В выводе должны присутствовать наименования устройств, с указанием устройств в служебной ФС ядра /dev, например, вида:

```
# lsscsi –g

[1:2:0:0] tape HP Ultrium 5-SCSI Z39W /dev/st0 /dev/sg4 (ленточный привод)
[1:2:0:1] mediumx HP MSL G3 Series 6.20 /dev/sch0 /dev/sg5 (устройство смены
лент)
```

4) использовать программу mtx для управления роботом:

```
# mtx <устройство> команда
```

Например:

```
# mtx -f /dev/sg5 status

Storage Changer /dev/sg5:1 Drives, 16 Slots (
0 Import/Export ) Data Transfer Element 0:Empty Storage Element 1:Empty
Storage Element 2:Empty Storage Element 3:Empty Storage Element 4:Empty
Storage Element 5:Empty Storage Element 6:Empty Storage Element 7:Empty
Storage Element 8:Empty Storage Element 9:Empty Storage Element
10:Empty Storage Element 11:Empty Storage Element 12:Empty Storage
Element 13:Empty Storage Element 14:Empty Storage Element 15:Empty
Storage Element 16:Empty
```

Возможные команды:

- status – осуществляет опрос статуса;
- inventory – осуществляет инвентаризацию лент;
- load <номер_слота> [<номер_привода>] – загрузжает ленту из указанного слота в указанный привод;
- unload [<номер_слота>] [<номер_привода>] – выгрузжает ленту из указанного слота.

Примечание. Пакеты `mt-st`, `mtx` и `lsscsi` не входят в состав ISO-образа дистрибутива, их можно установить из репозитория p10. О добавлении репозиториев можно почитать в разделе «Добавление репозиториев».

Примечание. mtx – низкоуровневый интерфейс управления чейнджером; mt – низкоуровневый интерфейс управления ленточным приводом.

5.12.9.3 Настройка резервного копирования

Все настройки можно выполнять как в веб-интерфейсе, так и в командной строке.

Примечание. Если при работе с новой лентой возникает ошибка `TASK ERROR: media read error - read failed - Blank Check, Additional sense: End-of-data not found`, необходимо выполнить команду:

```
# pmt rewind
```

5.12.9.3.1 Устройства смены лент (Tape changers)

Этот шаг можно пропустить, если используется автономный диск.

Устройства смены лент (роботы) являются частью ленточной библиотеки. Они содержат несколько слотов для картриджей с лентой, считыватель штрих-кода для идентификации картриджей с лентой и автоматизированный метод загрузки лент.

Получить список доступных устройств:

```
# proxmox-tape changer scan
```

```
┌──────────────────────────────┬─────────┬──────────────┬────────┐
│ path                         │ vendor  │ model        │ serial │
╞══════════════════════════════╪═════════╪══════════════╪════════╡
│ /dev/tape/by-id/scsi-CC2C52 │ Quantum │ Superloader3 │ CC2C52 │
└──────────────────────────────┴─────────┴──────────────┴────────┘
```

Чтобы использовать устройство с PBS, необходимо создать запись конфигурации:

```
# proxmox-tape changer create CHGR1 --path /dev/tape/by-id/scsi-CC2C52
```

Где CHGR1 – произвольное имя.

Примечание. Так как имена типа /dev/sg* могут после перезагрузки указывать на другое устройство, необходимо использовать постоянные имена путей к устройствам, например, /dev/tape/by-id/.

Операцию добавления устройства смены лент также можно выполнить в веб-интерфейсе. Для этого в разделе «Tape Backup» → «Сменщики» (Рис. 339), необходимо нажать кнопку «Добавить». Откроется диалоговое окно (Рис. 340), в котором необходимо указать имя и выбрать устройство.

Резервное копирование на ленту. Устройства смены лент

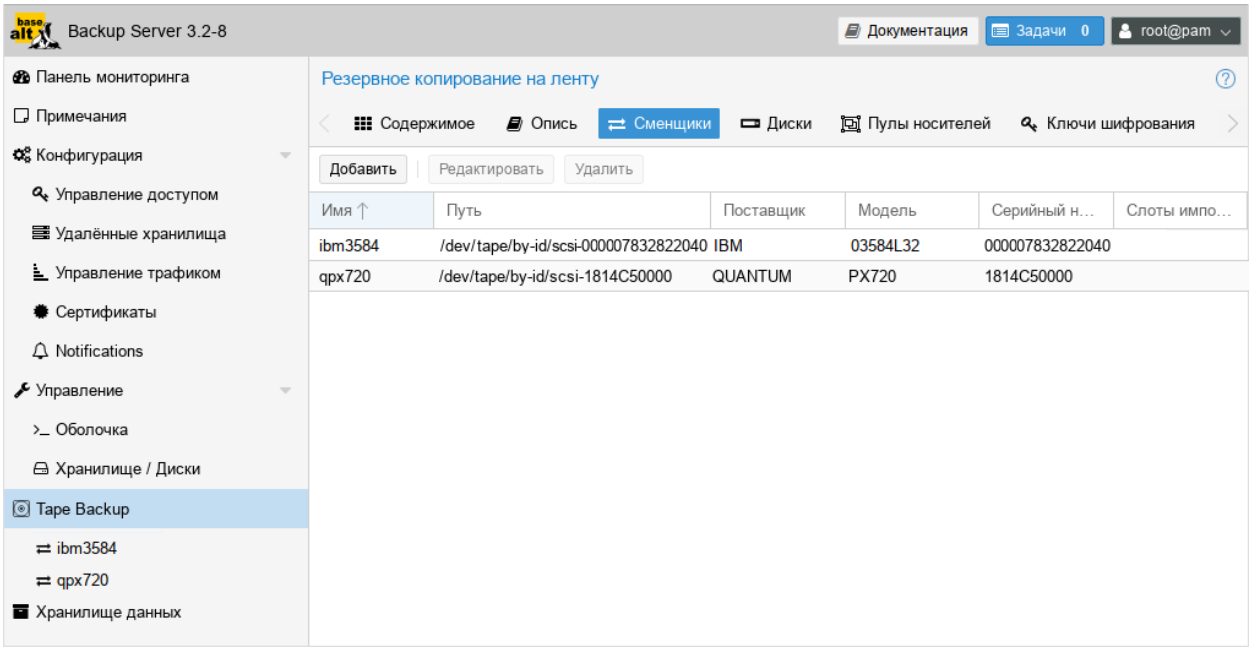


Рис. 339

Резервное копирование на ленту. Добавление нового устройства смены ленты

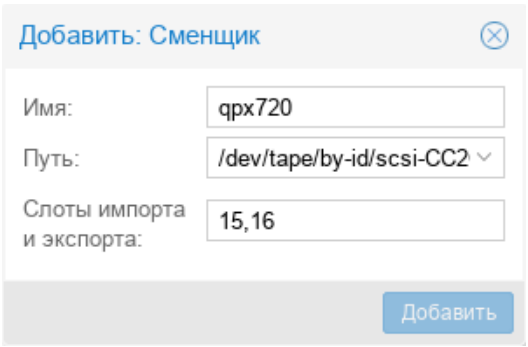


Рис. 340

Просмотреть получившуюся конфигурацию можно, выполнив команду:

```
# proxmox-tape changer config CHGR1
```

```
┌──────┬──────────────────────────┐
│ Name │ Value                    │
╞══════╪══════════════════════════╡
│ name │ CHGR1                    │
├──────┼──────────────────────────┤
│ path │ /dev/tape/by-id/scsi-CC2C52 │
└──────┴──────────────────────────┘
```

Вывести все настроенные устройства:

```
# proxmox-tape changer list
```

name	path	vendor	model	serial
CHGR1	/dev/tape/by-id/scsi-CC2C52	Quantum	Superloader3	CC2C52

Производитель, модель и серийный номер определяются автоматически, но отображаются только в том случае, если устройство подключено к сети.

Чтобы проверить настройку, можно также запросить статус устройства:

```
# proxmox-tape changer status CHGR1
```

entry-kind	entry-id	label-text	loaded-slot
drive	0	vtape1	1
slot	1		
slot	2	vtape2	
...	...		
slot	16		

Ленточные библиотеки обычно предоставляют несколько специальных слотов импорта/экспорта (также называемых «почтовыми слотами»). Ленты внутри этих слотов доступны снаружи, что упрощает добавление/удаление лент в/из библиотеки. Эти ленты считаются «автономными», поэтому задания резервного копирования не используют их. Эти специальные слоты определяются автоматически и помечаются как слоты import-export в выводе команды `proxmox-tape changer status`.

Некоторые небольшие ленточные библиотеки не имеют таких слотов. Они не могут удерживать медиафайлы, пока робот занимается другими делами. Они также не предоставляют доступ к этому «почтовому слоту» через интерфейс SCSI, поэтому их нельзя увидеть в выводе команды состояния.

В качестве обходного пути можно пометить некоторые обычные слоты как слоты экспорта. Программное обеспечение рассматривает эти слоты как настоящие слоты import-export, а носители внутри этих слотов считаются «автономными» (недоступными для резервного копирования):

```
# proxmox-tape changer update CHGR1 --export-slots 15,16
```

Теперь можно увидеть эти искусственные слоты import-export в выводе команды:

```
# proxmox-tape changer status CHGR1
```

entry-kind	entry-id	label-text	loaded-slot
drive	0	vtape1	1
import-export	15		
import-export	16		
slot	1		
slot	2	vtape2	
...	...		
slot	14		

Поскольку не все устройства смены ленты ведут себя одинаково, иногда возникает необходимость в настройке дополнительных параметров. Например, можно указать дополнительный параметр `--eject-before-unload` (необходим для некоторых устройств, которым требуется извлечение ленты перед выгрузкой из привода):

```
# proxmox-tape changer update CHGR1--eject-before-unload true
```

5.12.9.3.2 Ленточные накопители (приводы)

Получить список доступных ленточных приводов:

```
# proxmox-tape drive scan
```

path	vendor	model	serial
/dev/tape/by-id/scsi-12345-sg	IBM	ULT3580-TD4	12345

Чтобы использовать этот привод с PBS, необходимо создать запись конфигурации. Это можно сделать в веб-интерфейсе «Tape Backup» → «Диски» (Рис. 341) или с помощью команды:

```
# proxmox-tape drive create TAPELIB1 --path /dev/tape/by-id/scsi-<цифры>-sg
```

Примечание. Так как имена типа /dev/sg* могут после перезагрузки указывать на другое устройство, необходимо использовать постоянные имена путей к устройствам, например, /dev/tape/by-id/.

Резервное копирование на ленту. Добавление нового ленточного привода

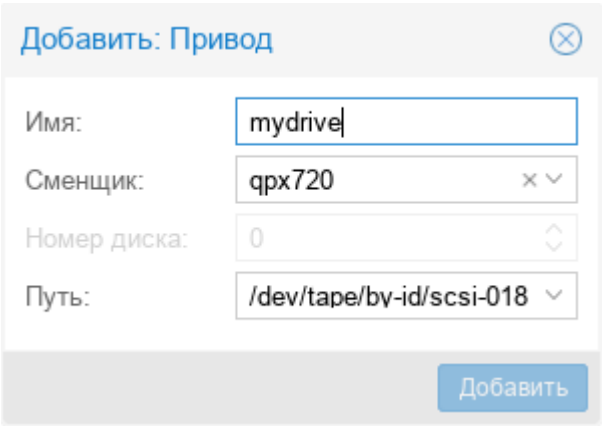


Рис. 341

При наличии ленточной библиотеки, также необходимо настроить соответствующее устройство смены лент:

```
# proxmox-tape drive update TAPELIB1 --changer CHGR1 --changer-drivenum 0
```

Параметр `--changer-drivenum` необходим только в том случае, если ленточная библиотека включает более одного привода (команда `proxmox-tape changer status` выводит список всех номеров накопителей).

Просмотреть полученную конфигурацию:

```
# proxmox-tape drive config mydrive
```

```
┌─────────┬──────────────────────────────┐
│ Name    │ Value                        │
╞═════════╪══════════════════════════════╡
│ name    │ mydrive                      │
├─────────┼──────────────────────────────┤
│ path    │ /dev/tape/by-id/scsi-12345-sg│
├─────────┼──────────────────────────────┤
│ changer │ CHGR1                        │
└─────────┴──────────────────────────────┘
```

Примечание. Значение 0, указанное в параметре `--changer-drivenum`, не сохраняется в конфигурации, поскольку используется по умолчанию.

Вывести список всех настроенных дисков:

```
# proxmox-tape drive list
```

```
┌────────┬──────────────────────────────┬────────┬──────┬──────────┬────────┐
│ name   │ path                         │ changer│ vendor│ model    │ serial │
╞════════╪══════════════════════════════╪════════╪══════╪══════════╪════════╡
│ mydrive│ /dev/tape/by-id/scsi-12345-sg│ CHGR1  │ IBM  │ ULT3580-TD4│ 12345  │
└────────┴──────────────────────────────┴────────┴──────┴──────────┴────────┘
```

Производитель, модель и серийный номер определяются автоматически и отображаются только в том случае, если устройство подключено к сети.

Для тестирования можно просто запросить состояние диска:

```
# proxmox-tape status --drive mydrive
```

Name	Value
blocksize	0
density	LTO4
compression	1
buffer-mode	1
alert-flags	(empty)
file-number	0
block-number	0
manufactured	Fri Dec 13 01:00:00 2019
bytes-written	501.80 GiB
bytes-read	4.00 MiB
medium-passes	20
medium-wearout	0.12%
volume-mounts	2

Примечание. Размер блока всегда должен быть равен 0 (режим переменного размера блока).

5.12.9.3.3 Медиа-пулы (пулы носителей)

Пул носителей – это логический контейнер для лент. Задание резервного копирования предназначено для одного пула носителей, поэтому задание использует только ленты из этого пула.

Набор носителей – это группа непрерывно записываемых лент, используемых для разделения большего пула на более мелкие восстанавливаемые блоки. Одно или несколько заданий резервного копирования записывают данные на набор носителей, создавая упорядоченную группу лент. Наборы носителей идентифицируются уникальным идентификатором. Этот идентификатор и порядковый номер хранятся на каждой ленте этого набора (метка ленты).

Наборы носителей являются основной единицей для задач восстановления. Для восстановления содержимого набора носителей понадобится каждая лента в наборе. Данные полностью дедуплицируются внутри набора носителей.

Пул дополнительно определяет, как долго задания резервного копирования могут добавлять данные в набор носителей (поле «Политика выделения» см. Рис. 342). Ниже перечислены возможные настройки.

Резервное копирование на ленту. Пулы носителей

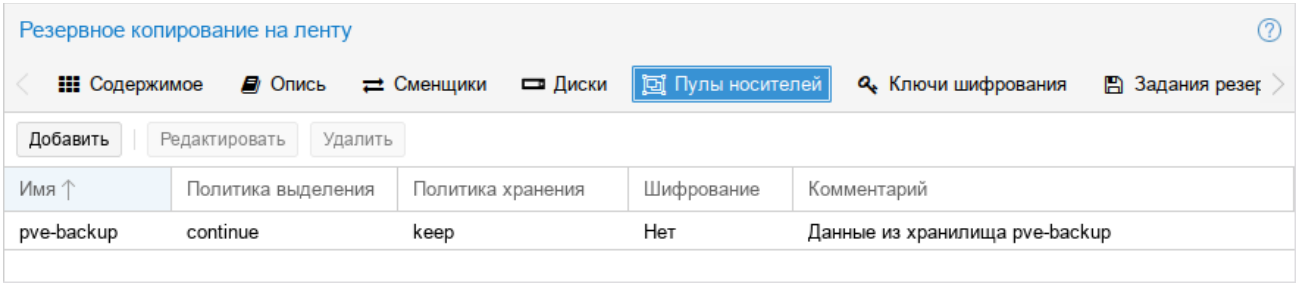


Рис. 342

Попробовать использовать текущий набор носителей («Продолжить»)

Этот параметр создает один большой набор носителей. Это очень эффективно (дедупликация, отсутствие неиспользуемого пространства), но может привести к увеличению времени восстановления, поскольку заданиям восстановления необходимо читать все ленты в наборе.

Примечание. Данные полностью дедуплицируются внутри набора носителей. Это также означает, что данные случайным образом распределяются по лентам в наборе. Таким образом, даже если восстанавливается одна ВМ, данные, возможно, придется считать со всех лент внутри набора носителей.

Наборы носителей большего размера также более подвержены ошибкам, поскольку даже одна поврежденная лента приводит к сбою восстановления.

Сценарий использования: в основном используется с ленточными библиотеками. Создание нового набора запускается вручную, при запуске задания резервного копирования с параметром `--export`.

Примечание. Срок хранения начинается с момента появления нового набора носителей.

Всегда создавать новый набор носителей («Всегда»)

При использовании этого параметра каждое задание резервного копирования создает новый набор носителей. Это менее эффективно, поскольку носитель из последнего набора может быть записан не полностью, а оставшееся пространство останется неиспользованным.

Преимущество такого подхода состоит в том, что при этом создаются наборы носителей минимального размера. С небольшими наборами легче обращаться, их удобнее перемещать в удаленное хранилище, и их можно восстановить гораздо быстрее.

Примечание. Срок хранения начинается с момента создания набора носителей.

Создать новый набор при срабатывании указанного события календаря

Позволяет указывать моменты времени, используя systemd, например спецификации событий календаря (см. man systemd.time).

Например, при указании значения `weekly` (или Mon *-*-* 00:00:00) новый набор будет создаваться каждую неделю.

Эта настройка балансирует между эффективностью использования пространства и количеством носителей.

Примечание. Срок хранения начинается со времени создания следующего набора мультимедиа или, если такового нет, когда событие календаря в следующий раз инициируется после времени начала текущего набора мультимедиа.

Следующие события также могут выделить новый набор носителей:

- требуемая лента находится в автономном режиме (и используется ленточная библиотека);
- текущий набор содержит поврежденные или устаревшие ленты;
- шифрование пула носителей изменилось;
- ошибки согласованности базы данных, например, если инвентарь не содержит необходимой информации о носителе или содержит противоречивую информацию (устаревшие данные).

Политика хранения определяет, как будут храниться данные:

- всегда перезаписывать носитель («Перезаписать»);
- защищать данные в течение указанного периода времени;
- никогда не перезаписывать данные («Оставлять»).

Ленточные накопители LTO-4 (или более поздних версий) поддерживают аппаратное шифрование. Если настроить пул носителей на использование шифрования, все данные, записываемые на ленты, шифруются с использованием настроенного ключа.

Таким образом, неавторизованные пользователи не смогут прочитать данные с носителя.

Примечание. Если клиент резервного копирования также шифрует данные, то данные на ленте будут зашифрованы дважды.

Защищенный паролем ключ хранится на каждом носителе, поэтому его можно восстановить с помощью пароля.

Для добавления нового пула носителей в меню «Tape Backup» → «Пулы носителей» следует нажать кнопку «Добавить» (Рис. 343) или воспользоваться командой:

```
# proxmox-tape pool create <name> [OPTIONS]
```

Резервное копирование на ленту. Добавление нового пула

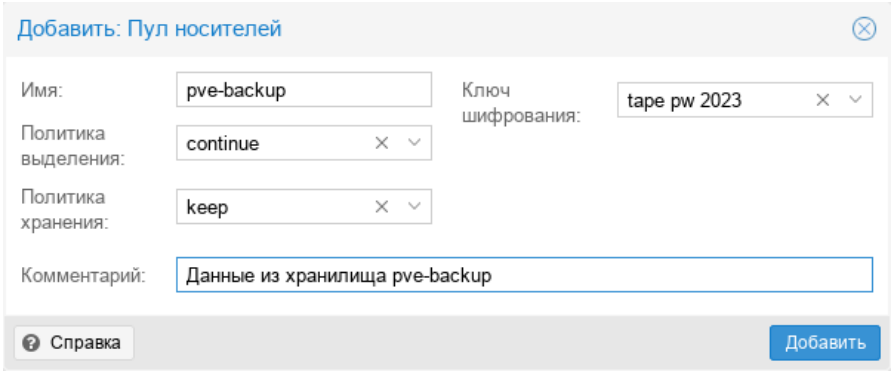


Рис. 343

Пример добавления пула:

```
# proxmox-tape pool create daily
```

Дополнительные параметры можно установить позже, например:

```
# proxmox-tape pool update daily --allocation daily --retention 7days
```

Вывести список всех настроенных пулов:

```
# proxmox-tape pool list
```

```
┌────────┬──────────┬────────────┬───────────┬──────────┐
│ name   │ drive    │ allocation │ retention │ template │
╞════════╪══════════╪════════════╪═══════════╪══════════╡
│ daily  │ mydrive  │ daily      │ 7days     │          │
└────────┴──────────┴────────────┴───────────┴──────────┘
```

5.12.9.3.4 Задания резервного копирования на ленту

Чтобы автоматизировать резервное копирование на ленту, можно настроить задания резервного копирования, которые записывают содержимое хранилища данных в пул носителей по определенному расписанию. При создании задания резервного копирования на ленту необходимо указать:

- store – хранилище данных, резервную копию которого нужно создать;
- pool – пул носителей (используются только ленточные картриджи из этого пула);
- drive – ленточный накопитель;
- schedule – расписание заданий.

Пример настройки задания резервного копирования на ленту для хранилища данных vmstore1:

```
# proxmox-tape backup-job create myjob --store vmstore1 \
  --pool mypool --drive mydrive --schedule daily
```

По умолчанию резервная копия включает все снимки из группы резервного копирования. Чтобы включать только самые последние снимки, можно использовать опцию `--latest-only`:

```
# proxmox-tape backup-job update job2 --latest-only
```

Для отправки уведомлений о запросах на ленту или отчетов об ошибках можно указать пользователя, на электронную почту которого будут отправляться уведомления:

```
# proxmox-tape backup-job update job2 --notify-user root@pam
```

Иногда бывает полезно извлечь ленту из привода после резервного копирования:

```
# proxmox-tape backup-job update job2 --eject-media
```

Примечание Для возможности отправки электронной почты должен быть запущен установлен пакет postfix и запущена соответсвующая служба:

```
# systemctl enable --now postfix
```

Для автономного накопителя опция `--eject-media` извлекает ленту, гарантируя, что следующая резервная копия не сможет использовать ленту (если только кто-то вручную не загрузит ленту). Для ленточных библиотек этот параметр выгружает ленту в свободный слот.

Примечание. В случае если задание завершается ошибкой, лента остается в приводе.

Для ленточных библиотек параметр `--export-media-set` перемещает все ленты из набора носителей в слот экспорта, гарантируя, что следующая резервная копия не сможет использовать эти ленты:

```
# proxmox-tape backup-job update job2 --export-media-set
```

Примечание. Опцию `--export-media-set` можно использовать для принудительного запуска нового набора носителей, поскольку ленты из текущего набора больше не находятся в сети.

Запуск задания резервного копирования вручную:

```
# proxmox-tape backup-job run job2
```

Удаление задания резервного копирования:

```
# proxmox-tape backup-job remove job2
```

По умолчанию все (рекурсивные) пространства имен хранилища данных включаются в резервную копию на ленте. Можно указать одно пространство имен с помощью опции `--ns` и глубину с помощью опции `--max-deep`. Например:

```
# proxmox-tape backup-job update job2 --ns mynamespace --max-depth 3
```

Если опция `--max-deep` не указана, резервная копия будет включать все рекурсивные пространства имен.

Операции с заданиями резервного копирования можно также выполнять в веб-интерфейсе на вкладке «Tape Backup» → «Задания резервного копирования». При создании задания резервного копирования (Рис. 344) в поле «Локальное хранилище данных» следует указать хранилище данных, для которого будет создаваться резервная копию, а в поле «Пул носителей» – пул, в который выполняется резервное копирование.

5.12.9.4 Администрирование

Во многих подкомандах команды `proxmox-tape` используется параметр `--drive` с указанием привода, с которым будет происходить работа. Для удобства можно задать привод в переменной среды:

```
# export PROXMOX_TAPE_DRIVE=mydrive
```

В этом случае в команде можно не указывать параметр `--drive`. Если привод имеет связанное с ним устройство смены лент, также можно опустить параметр `--changer` в командах, которым требуется устройство смены лент, например:

```
# proxmox-tape changer status
```

Вывод этой команды должен отображать статус устройства смены лент, связанного с диском mydrive.

Резервное копирование на ленту. Добавление задания резервного копирования

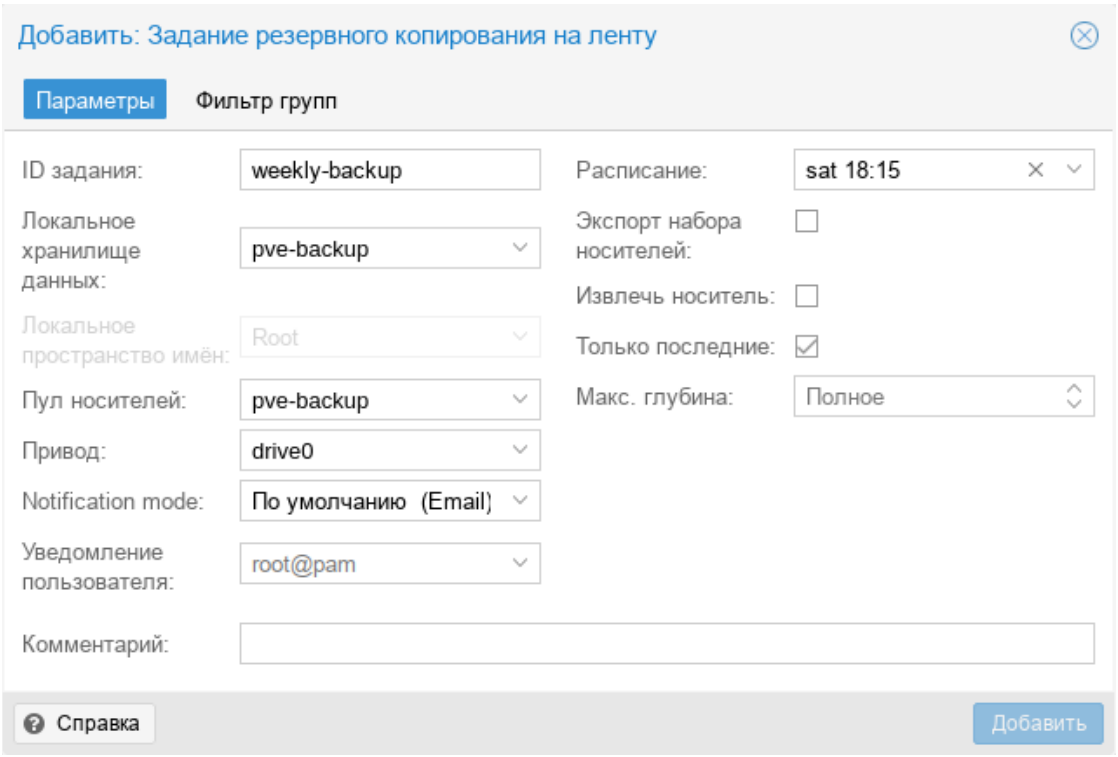


Рис. 344

5.12.9.4.1 Этикетки

По умолчанию все кассеты с лентой выглядят одинаково, поэтому для уникальной идентификации на них необходимо нанести этикетку. Сначала следует наклеить на картридж этикетку с текстом. Затем необходимо записать тот же текст метки на ленту, чтобы программное обеспечение могло однозначно идентифицировать ленту.

Для автономного накопителя необходимо вставить новый ленточный картридж в привод и выполнить команду:

```
# proxmox-tape label --label-text <текст метки> [--pool <имя пула>]
```

Аргумент –pool можно опустить, чтобы разрешить использование ленты любым пулом.

Примечание. По соображениям безопасности эта команда не выполняется, если лента содержит какие-либо данные.

Прочитать этикетку:

```
# proxmox-tape read-label
```

```
┌─────────────────┬──────────────────────────────────────┐
│ Name            │ Value                                │
╞═════════════════╪══════════════════════════════════════╡
│ label-text      │ vtape1                               │
├─────────────────┼──────────────────────────────────────┤
│ uuid            │ 7f42c4dd-9626-4d89-9f2b-c7bc6da7d533 │
├─────────────────┼──────────────────────────────────────┤
│ ctime           │ Wed Jul 24 09:13:36 2024             │
├─────────────────┼──────────────────────────────────────┤
│ pool            │ daily                                │
├─────────────────┼──────────────────────────────────────┤
│ media-set-uuid  │ 00000000-0000-0000-0000-000000000000 │
├─────────────────┼──────────────────────────────────────┤
│ media-set-ctime │ Wed Jul 24 09:13:36 2024             │
└─────────────────┴──────────────────────────────────────┘
```

Примечание. Параметр media-set-uuid, содержащий все нули, указывает на пустую ленту (не используемую ни одним набором носителей).

Если используется ленточная библиотека, сначала необходимо наклеить на ленточные картриджи этикетку со штрих-кодом и загрузить эти пустые ленты в библиотеку. Затем можно пометить все непомеченные ленты с помощью команды:

```
# proxmox-tape barcode-label [--pool <имя-пула ]
```

5.12.9.4.2 Запуск резервного копирования на ленту

Для запуска задания резервного копирования вручную необходимо нажать кнопку «Запустить сейчас» или использовать команду:

```
# proxmox-tape backup <хранилище> <пул> [OPTIONS]
```

Доступны следующие опции:

- --eject-media – извлечь носитель после завершения работы;
- --export-media-set – после успешного выполнения задания резервного копирования все ленты из используемого набора носителей перемещаются в слоты импорта-экспорта;
- --ns – пространство имен для резервного копирования. Используется, если нужно создать резервную копию только определенного пространства имен. Если этот параметр опущен, предполагается корневое пространство имен.
- --max-depth– глубина рекурсивных пространств имен. 0 означает отсутствие рекурсии вообще (только заданное пространство имен).

5.12.9.4.3 Восстановление с ленты

Восстановление выполняется с детализацией набора носителей, поэтому сначала необходимо выяснить, какой набор носителей содержит данные, которые нужно восстановить. Эта информация хранится в медиа-каталоге. Если медиа-каталогов еще нет, сначала необходимо их восстановить. Следует обратить внимание, что для поиска данных понадобится каталог, но для восстановления полного набора мультимедиа каталоги мультимедиа не нужны.

Следующая команда выводит список медиаконтента (из каталога):

```
# proxmox-tape media content
```

Задание восстановления считывает данные с набора носителей и перемещает их обратно на диск данных (хранилище данных):

```
# proxmox-tape restore <media-set-uuid> <хранилище>
```

Например:

```
# proxmox-tape restore 9da37a55-aac7-4deb-91c6-482b3b675f30 pve-backup
```

Иногда нет необходимости восстанавливать весь носитель, а только некоторые отдельные снимки с ленты. Этого можно добиться с помощью параметра `snapshot`:

```
# proxmox-tape restore <media-set-uuid> <хранилище> [<snapshot>]
```

Например:

```
# proxmox-tape restore 9da37a55-aac7-4deb-91c6-482b3b675f30 \
pve-backup sourcestore:host/hostname/2024-04-01T00:01:00Z
```

При этом снимок сначала восстанавливается во временном расположении, затем восстанавливаются соответствующие архивы фрагментов и, наконец, восстанавливаются данные моментального снимка в целевое хранилище данных.

Параметр `snapshot` можно передавать несколько раз, чтобы восстановить несколько снимков одним действием восстановления.

Примечание. При использовании восстановления с помощью параметра `snapshot` ленту необходимо пройти более одного раза, что при одновременном восстановлении нескольких

моментальных снимков может занять больше времени, чем восстановление всего хранилища данных.

Во время восстановления также можно выбрать и сопоставить определенные пространства имен из набора носителей. Это возможно с помощью параметра `--namespaces`. Формат параметра:

```
store=<source-datastore>[,source=<source-ns>][,target=<target-ns>][,max-depth=<depth>]
```

Если `source` или `target` не указаны, предполагается корневое пространство имен. Если не указан `max-depth`, исходное пространство имен будет полностью рекурсивно.

Пример команды восстановления:

```
# proxmox-tape restore 9da37a55-aac7-4deb-91c6-482b3b675f30 \
pve-backup --namespaces \
store=sourcedatastore,source=ns1,target=ns2,max-depth=2
```

Параметр `--namespaces` может быть указан несколько раз. Его можно комбинировать с параметром `snapshot`, чтобы восстанавливать только эти снимки и сопоставлять их с различными пространствами имен.

5.12.9.4.4 Восстановить каталог

Чтобы восстановить каталог с существующей ленты, достаточно вставить ленту в привод и выполнить команду:

```
# proxmox-tape catalog
```

Восстановить с ленты можно даже без существующего каталога, но только весь набор носителей. В этом случае каталог будет создан автоматически.

5.12.9.4.5 Управление ключами шифрования

Ключами шифрования можно управлять в разделе «Tape Backup» → «Ключи шифрования» веб-интерфейса (Рис. 345) или с помощью команды proxmox-tape key.

Резервное копирование на ленту. Ключи шифрования

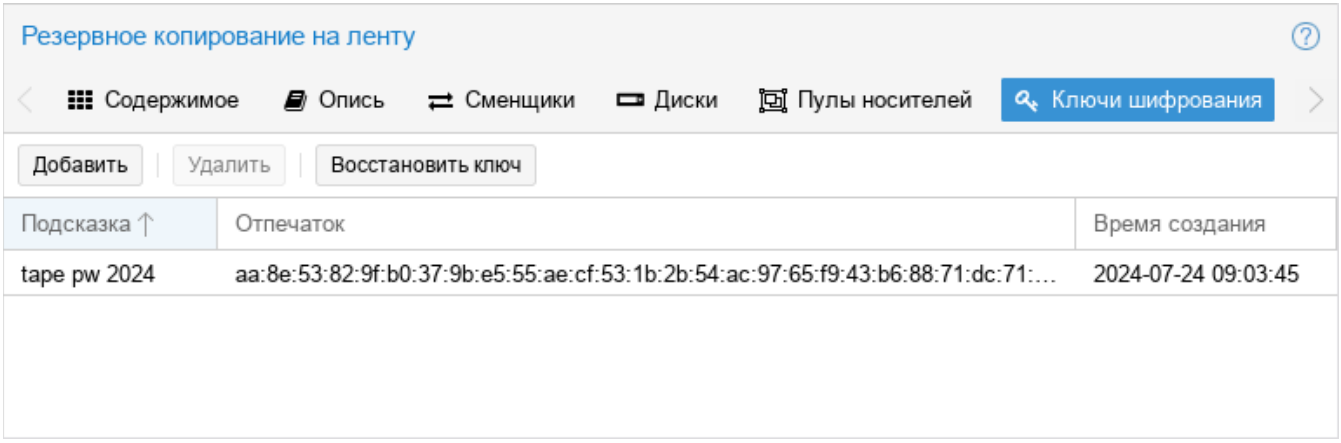


Рис. 345

Пример создания нового ключа шифрования:

```
# proxmox-tape key create --hint "tape pw 2024"

Tape Encryption Key Password: ********
Verify Password: ********
"aa:8e:53:82:9f:b0:37:9b:e5:55:ae:cf:53:1b:2b:54:ac:97:65:f9:43:b6:88:71:dc:7
1:41:2f:22:db:2e:89"
```

Вывести список ключей:

```
# proxmox-tape key list
```

fingerprint	hint
aa:8e:53:82:9f:b0:37:9b: ... :41:2f:22:db:2e:89	tape pw 2024

Отобразить сведения о ключе шифрования:

```
# proxmox-tape key show aa:8e:53:82:9f:b0:37:9b: ...   :2f:22:db:2e:89
```

```
┌─────────────┬─────────────────────────────────────────────┐
│ Name        │ Value                                       │
╞═════════════╪═════════════════════════════════════════════╡
│ kdf         │ scrypt                                      │
├─────────────┼─────────────────────────────────────────────┤
│ created     │ Wed Jul 24 09:03:45 2024                    │
├─────────────┼─────────────────────────────────────────────┤
│ modified    │ Wed Jul 24 09:03:45 2024                    │
├─────────────┼─────────────────────────────────────────────┤
│ fingerprint │ aa:8e:53:82:9f:b0:37:9b: ...  :2f:22:db:2e:89 │
├─────────────┼─────────────────────────────────────────────┤
│ hint        │ tape pw 2024                                │
└─────────────┴─────────────────────────────────────────────┘
```

Подкоманду `paperkey` можно использовать для создания QR-кода ключа шифрования ленты.

Создать QR-код и записать его в текстовый файл для удобной печати:

```
# proxmox-tape key paperkey <fingerprint> --output-format text > qrkey.txt
```

Для восстановления ключа шифрования с ленты, необходимо загрузить в привод ленту, которую нужно восстановить и нажать кнопку «Восстановить ключ» в веб-интерфейсе или запустить команду (потребуется ввести пароль, заданный при создании ключа):

```
# proxmox-tape key restore

Tape Encryption Key Password: ***********
```

Если пароль правильный, ключ будет импортирован в базу данных. Задания восстановления автоматически используют любой доступный ключ.

5.12.9.4.6 Очистка ленты

Ленточные накопители LTO требуют регулярной чистки. Это делается путем загрузки в привод чистящего картриджа, что для автономных накопителей выполняется вручную.

В ленточных библиотеках чистящие картриджи обозначаются специальными этикетками, начинающимися с букв «CLN». Например, в ленточной библиотеке CHGR1 в слоте 3 имеется чистящий картридж:

```
# proxmox-tape changer status CHGR1
```

```
┌──────────────┬──────────┬─────────────┬──────────────┐
│ entry-kind   │ entry-id │ label-text  │ loaded-slot  │
╞══════════════╪══════════╪═════════════╪══════════════╡
│ drive        │        0 │ vtape1      │            1 │
├──────────────┼──────────┼─────────────┼──────────────┤
```

```
| slot          |        1 |            |              |
├───────────────┼──────────┼────────────┼──────────────┤
| slot          |        2 | vtape2     |              |
├───────────────┼──────────┼────────────┼──────────────┤
| slot          |        3 | CLN001CU   |              |
├───────────────┼──────────┼────────────┼──────────────┤
| ...           |      ... |            |              |
└───────────────┴──────────┴────────────┴──────────────┘
```

Запустить операцию очистки:

```
# proxmox-tape clean
```

Эта команда делает следующее:

- находит чистящую ленту (в слоте 3);
- выгружает текущий носитель из привода (обратно в слот 1);
- загружает чистящую ленту в привод;
- запускает операцию очистки диска;
- выгружает чистящую ленту (в слот 3).

5.12.10 Уведомления

Система уведомлений (нотификаций) в PBS предназначена для информирования администраторов о ключевых событиях, происходящих в системе, таких как успешное или неудачное выполнение задач резервного копирования, проблемы с хранилищем, предупреждения о состоянии системы и другие важные изменения.

PBS отправляет событие уведомления в случае значимых событий в системе. События обрабатываются системой уведомлений. У события уведомления есть метаданные: временная метка, уровень серьезности, тип и т.д.

Сопоставители уведомлений направляют событие уведомления в один или несколько целевых объектов уведомления. У сопоставителя могут быть правила сопоставления для выборочной маршрутизации на основе метаданных события уведомления.

Цель уведомления (канал доставки уведомлений) – это пункт назначения, в который событие уведомления направляется сопоставлением. PBS предлагает несколько типов целей:

- Sendmail – уведомления отправляются через локальный почтовый сервер;
- SMTP – уведомления отправляются через внешний SMTP-сервер;
- Gotify – уведомления отправляются в сервис Gotify (легковесный сервер для push-уведомлений).

Хранилища данных и задания резервного копирования на ленту имеют настраиваемый режим уведомления. Он позволяет выбирать между системой уведомлений и режимом для отправки уведомлений по электронной почте.

Систему уведомлений можно настроить в веб-интерфейсе в разделе «Конфигурация» → «Notifications» («Уведомления»), через конфигурационные файлы или в командной строке.

Конфигурация системы уведомлений хранится в файлах notifications.cfg и notifications-priv.cfg. Файл notifications-priv.cfg содержит конфиденциальные параметры конфигурации (пароли, токены аутентификации) и доступен для чтения только пользователю root.

5.12.10.1 Цели уведомлений (Notification Targets)

5.12.10.1.1 Sendmail

Цель уведомлений Sendmail использует команду sendmail для отправки электронных писем списку настроенных пользователей или адресов электронной почты. Если в качестве получателя выбран пользователь, будет использоваться адрес электронной почты, указанный в настройках пользователя. Адрес электронной почты пользователя можно настроить в разделе «Конфигурация» → «Управление доступом» → «Управление пользователями». Если для пользователя не указан адрес электронной почты, письмо не будет отправлено.

Примечание. Двоичный файл sendmail предоставляется Postfix. Может потребоваться настроить Postfix так, чтобы он мог правильно доставлять почту, например, настроив внешний почтовый ретранслятор. В случае сбоя доставки необходимо проверить системные журналы на наличие сообщений, зарегистрированных демоном Postfix.

Для настройки цели Sendmail необходимо выполнить следующие шаги:

1) в разделе «Конфигурация» → «Notifications» → «Notifications Targets» нажать кнопку «Добавить» → «Sendmail» (Рис. 346);

Создать цель уведомлений Sendmail

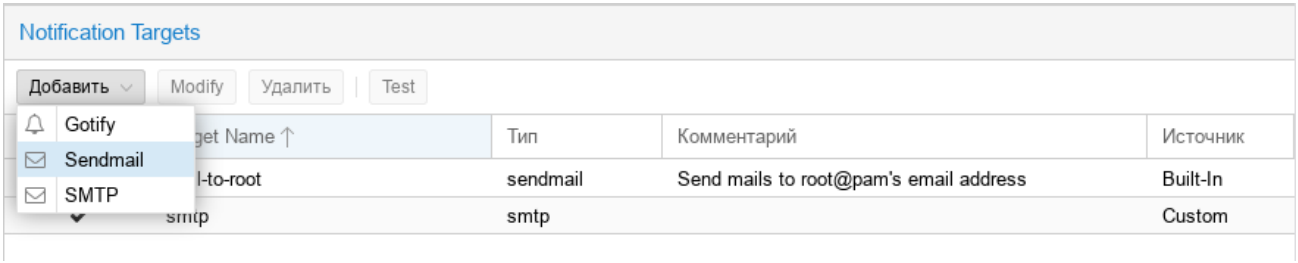


Рис. 346

2) в открывшемся окне (Рис. 347) указать следующие данные (в скобках приведены параметры файла notifications.cfg):

- «Endpoint Name» – имя цели;
- «Включить» (disable) – состояние цели;
- «Recipient(s)» (mailto-user) – пользователи PBS, которым будут отправлены уведомления. Адрес электронной почты пользователя будет найден в users.cfg;
- «Additional recipient(s)» (mailto) – список дополнительных получателей электронной почты;
- «Комментарий» (comment) – комментарий для этой цели;

- «Author» (author) – автор электронного письма. По умолчанию: «Proxmox Backup Server - $hostname»;
- «From Address» (from-address) – адрес отправителя, который будет использоваться в уведомлениях. Если параметр не задан, будет использоваться настройка email_from из node.cfg. Если она также не задана, будет использоваться значение по умолчанию root@$hostname, где $hostname – имя узла.

Настройка цели уведомлений Sendmail

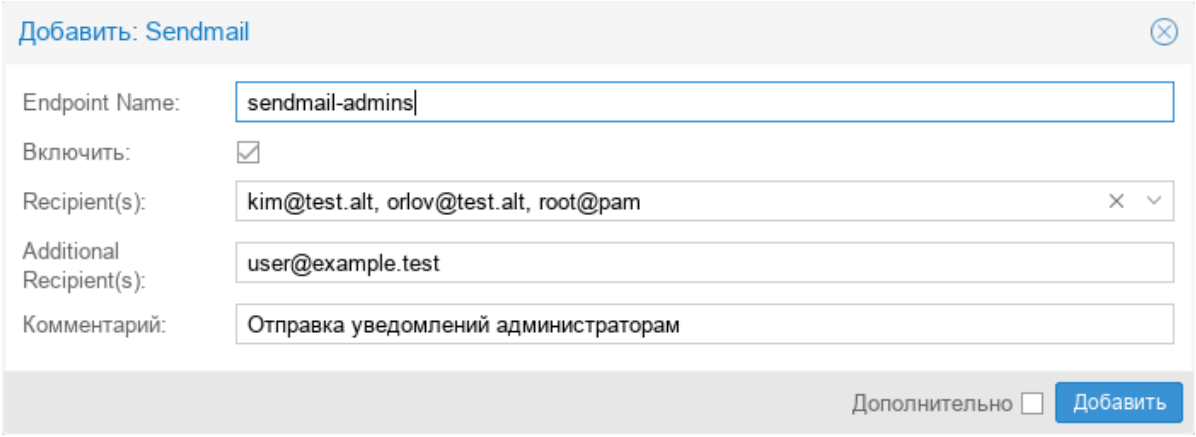


Рис. 347

Пример создания цели Sendmail в командной строке:

```
# proxmox-backup-manager notification endpoint sendmail create \
sendmail-admins --mailto-user kim@test.alt \
--mailto-user orlov@test.alt --mailto-user root@pam \
--mailto user@example.test --comment "Отправка уведомлений администраторам"
```

Пример конфигурации (/etc/proxmox-backup/notifications.cfg):

```
sendmail: sendmails-admin
    comment Отправка уведомлений администраторам
    mailto user@example.test
    mailto-user kim@test.alt
    mailto-user orlov@test.alt
    mailto-user root@pam
```

5.12.10.1.2 SMTP

Цель уведомлений SMTP позволяет отправлять электронные письма напрямую на почтовый ретранслятор SMTP. Эта цель не использует MTA системы для доставки электронных писем.

Примечание. В отличие от целей Sendmail, цели SMTP не имеют механизма очередности/повторной отправки в случае сбоя доставки почты.

Для настройки цели SMTP необходимо выполнить следующие шаги:

1) в разделе «Конфигурация» → «Notifications» → «Notifications Targets» нажать кнопку «Добавить» → «SMTP» (Рис. 348);

Создать цель уведомлений SMTP

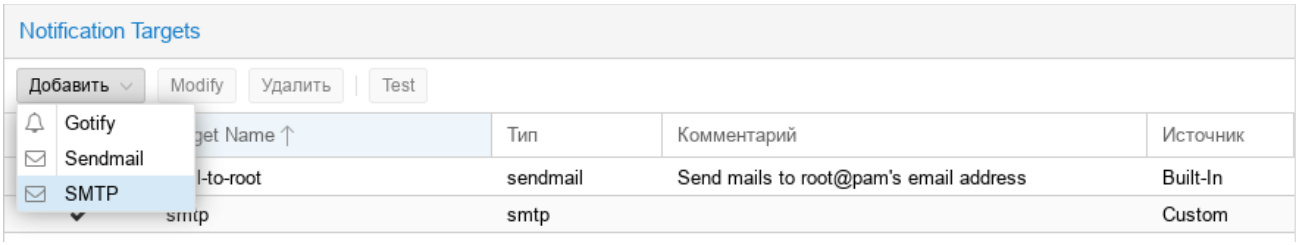


Рис. 348

2) в открывшемся окне (Рис. 349) указать следующие данные (в скобках приведены параметры файла notifications.cfg):

- «Endpoint Name» – имя конечной точки;
- «Включить» (disable) – состояние цели;
- «Сервер» (server) – адрес SMTP-сервера;
- «Шифрование» (mode) – метод шифрования, который будет использоваться для соединения (insecure, starttls или tls). По умолчанию tls;
- «Порт» (port) – порт, который будет использоваться. По умолчанию 465 для подключений на основе TLS, 587 – для подключений на основе STARTTLS и порт 25 – для незащищенных подключений с открытым текстом;
- «Authenticate» – добавить данные для аутентификации SMTP;
- «Username» (username) – имя пользователя для аутентификации SMTP. Если имя пользователя не задано, аутентификация не будет выполнена. Поддерживаются методы аутентификации PLAIN и LOGIN;
- «Пароль» (password) – пароль для аутентификации SMTP;
- «From Address» (from-address) – адрес отправителя, который будет использоваться в уведомлениях. Ретрансляторы SMTP могут потребовать, чтобы этот адрес принадлежал пользователю. Поле «Отправитель» в электронном письме будет установлен на $author <$from-address>;
- «Recipient(s)» (mailto-user) – пользователи PBS, которым будут отправлены уведомления. Адрес электронной почты пользователя будет найден в users.cfg;
- «Additional recipient(s)» (mailto) – список дополнительных получателей электронной почты;
- «Комментарий» (comment) – комментарий для этой цели;
- «Author» (author) – автор электронного письма. По умолчанию: «Proxmox Backup Server - $hostname».

Настройка цели уведомлений SMTP

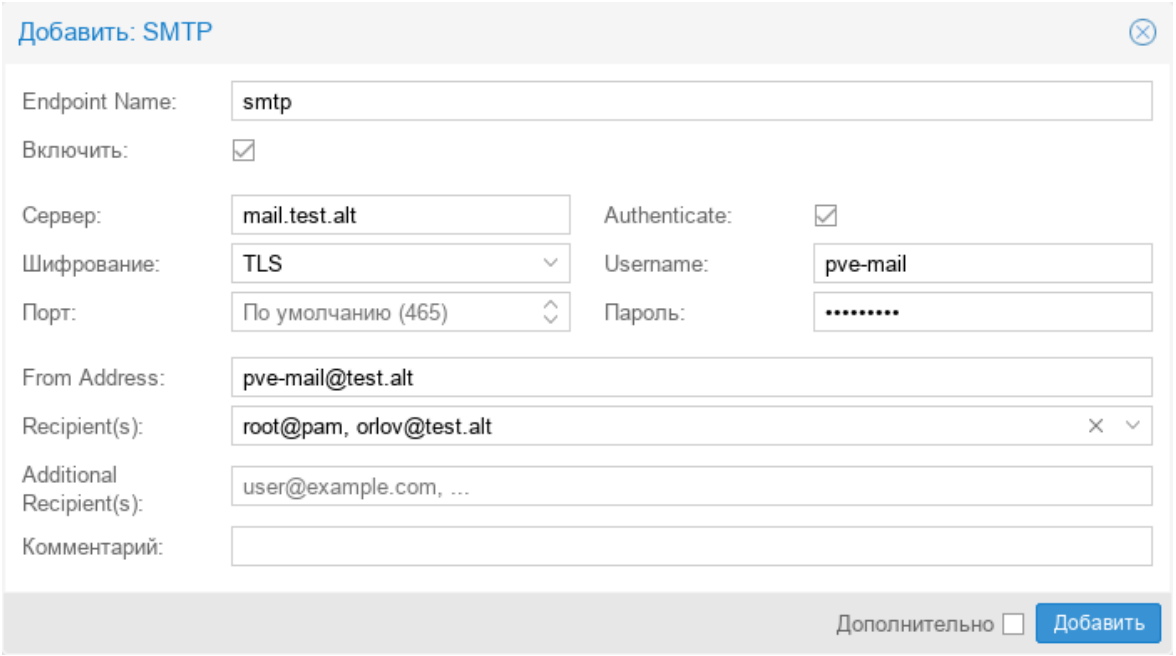


Рис. 349

Пример создания цели SMTP в командной строке:

```
# proxmox-backup-manager notification endpoint smtp create \
smtp --from-address pve-mail@test.alt  --server mail.test.alt \
--username pve-mail --password "123" --mailto-user root@pam \
--mailto-user orlov@test.alt
```

Пример конфигурации (/etc/proxmox-backup/notifications.cfg):

```
smtp: smtp
    from-address pve-mail@test.alt
    mailto-user root@pam
    mailto-user orlov@test.alt
    mode tls
    server mail.test.alt
    username pve-mail
```

5.12.10.2 Триггеры уведомлений (Notification Matchers)

Триггеры уведомлений направляют уведомления к целям уведомлений на основе правил сопоставления. Эти правила могут соответствовать определенным свойствам уведомления, таким как временная метка (match-calendar), серьезность уведомления (match-severity) или поля метаданных (match-field). Если уведомление сопоставлено триггером, все цели, настроенные для сопоставления, получат уведомление.

Можно создать произвольное количество триггеров, каждый со своими собственными правилами сопоставления и целями для уведомления. Каждая цель уведомляется не более одного раза для каждого уведомления, даже если цель используется в нескольких триггерах.

Триггер без правил соответствует любому уведомлению (настроенные цели всегда будут уведомлены):

```
matcher: always-matches
    comment Это сопоставление всегда срабатывает
    mode all
    target mail-to-root
```

5.12.10.2.1 Правила сопоставления календаря (match-calendar)

Сопоставитель календаря соответствует временной метке уведомления.

Опция match-calendar использует специальный синтаксис для определения временных интервалов, в которые уведомления должны быть активны.

Примеры:

- match-calendar 8-12 – каждый день с 8 до 12 часов;
- match-calendar 8:00-15:30 – каждый день с 8 часов до 15:30;
- match-calendar mon..fri 9:00-17:00 – каждый будний день с 9 до 17 часов;
- match-calendar sun,tue..wed,fri 9-17 – в воскресенье, вторник, среду и пятницу с 9 до 17 часов.

5.12.10.2.2 Правила сопоставления полей (match-field)

Опция match-field используется для фильтрации уведомлений на основе определённых полей в сообщениях о событиях.

Если при сопоставлении используется exact, в качестве разделителя можно использовать запятую. Правило сопоставления срабатывает, если поле метаданных имеет любое из указанных значений.

Примеры:

- match-field exact:type=gc – только уведомления для заданий по сбору мусора;
- match-field exact:type=prune,verify – уведомления о заданиях prune и проверках;
- match-field regex:datastore=^backup-.*$ – уведомление для любого хранилища данных, имя которого начинается с backup.

Если уведомление не имеет сопоставленного поля, правило не будет соответствовать. Например, директива match-field regex:datastore=.* будет соответствовать любому уведомлению, имеющему поле метаданных datastore, но не будет соответствовать, если поле не существует.

5.12.10.2.3 Правила сопоставления серьезности (match-severity)

Опция match-severity используется для фильтрации уведомлений на основе уровня серьёзности (severity) события. Поддерживаются следующие уровни серьезности: info, notification, warning, error, unknown.

Примеры:

- match-severity error – только ошибки;
- match-severity warning,error – предупреждения и ошибки.

5.12.10.2.4 События уведомления

В таблице 4 приведен список всех событий уведомлений в PBS, их тип, серьезность и дополнительные поля метаданных. Тип, а также любое поле метаданных могут использоваться в правилах сопоставления.

Т а б л и ц а 4 – Список событий уведомлений

Событие	Тип	Серьезность	Поля метаданных (в дополнение к типу)
Обновление сертификата ACME не удалось	acme	error	hostname
Сбой сбора мусора	gc	error	datastore, hostname
Успешный сбор мусора	gc	info	datastore, hostname
Доступны обновления пакетов	package-updates	info	hostname
Ошибка задания Prune	prune	error	datastore, hostname, job-id
Успешное выполнение задания Prune	prune	info	datastore, hostname, job-id
Ошибка удаленной синхронизации	sync	error	datastore, hostname, job-id
Удаленная синхронизация выполнена успешно	sync	info	datastore, hostname, job-id
Почта для root	system-mail	unknown	hostname
Ошибка задания резервного копирования на ленту	tape-backup	error	datastore, hostname, media-pool, job-id
Успешное выполнение задания резервного копирования на ленту	tape-backup	info	datastore, hostname, media-pool, job-id
Запрос на загрузку ленты	tape-load	notice	hostname
Ошибка задания проверки	verify	error	datastore, hostname, job-id
Успешное выполнение задания проверки	verify	info	datastore, hostname, job-id

В таблице 5 содержится описание полей метаданных. Все они могут использоваться в правилах сопоставления полей.

Т а б л и ц а 5 – Описание полей метаданных

Поле метаданных	Описание
datastore	Имя хранилища данных
hostname	Имя хоста сервера резервного копирования
job-id	Идентификатор задания
media-pool	Имя пула ленточных носителей
type	Тип события уведомления

Примеры (/etc/proxmox-backup/notifications.cfg):

- уведомлять администраторов в рабочее время:

```
matcher: workday
        match-calendar mon..fri 9-17
```

```
        target admin
        comment Notify admins during working hours
```

- уведомлять администраторов в нерабочие часы:

```
matcher: night-and-weekend
        match-calendar mon..fri 9-17
        invert-match true
        target on-call-admins
        comment Separate target for non-working hours
```

- при ошибках хранилища zfs, отправлять уведомления в рабочие часы на цель smtp:

```
matcher: zfs-error
        match-calendar mon..fri 8-17
        match-field exact:datastore=zfs
        match-severity error
        mode all
        target smtp
```

5.12.10.2.5 Создание триггера уведомлений

Для создания правила сопоставления необходимо выполнить следующие шаги:

1) в разделе «Конфигурация» → «Notifications» → «Notifications Matchers» нажать кнопку «Добавить»;

2) в открывшемся окне на вкладке «Общее» (Рис. 350) в поле «Matcher Name» указать название триггера;

Создание триггера уведомления

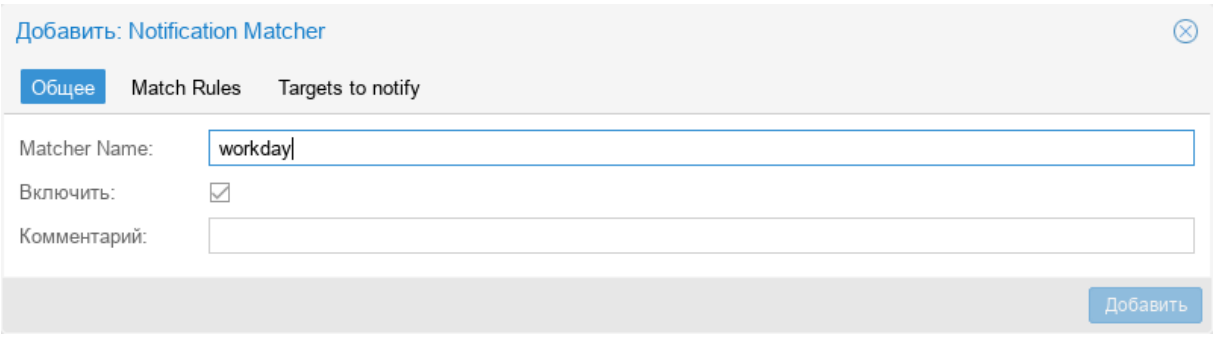


Рис. 350

3) на вкладке «Match Rules» (Рис. 351) настроить правила сопоставлений;

4) на вкладке «Targets to notify» (Рис. 352) выбрать цели для уведомления.

Пример создания триггера уведомлений в командной строке:

```
# proxmox-backup-manager notification matcher create workday \
--mode all --match-calendar "mon..fri 8-17" --match-severity "error" \
--match-field "exact:datastore=zfs" --target sendmails-admin
```

Создание триггера уведомления. Правила сопоставлений

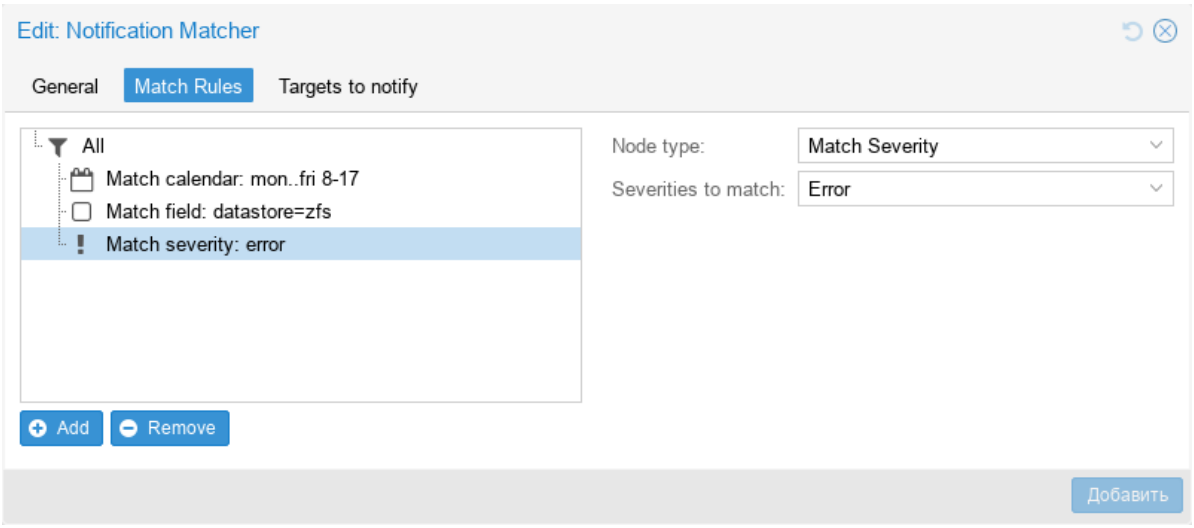


Рис. 351

Создать триггер уведомления. Выбор целей

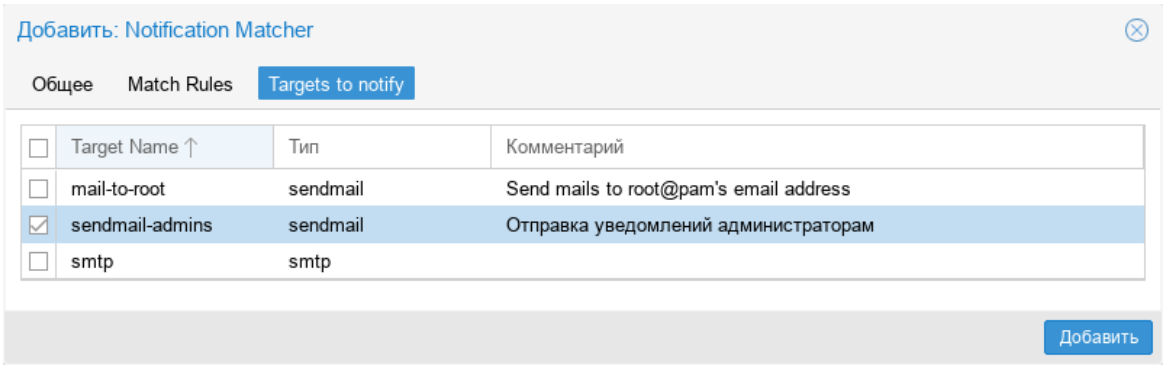


Рис. 352

5.12.10.3 Пересылка системной почты

Некоторые локальные системные демоны, например smartd, отправляют уведомления локальному пользователю root. PBS будет передавать эти письма в систему уведомлений как уведомления типа system-mail с неизвестной серьезностью.

Когда электронное письмо пересылается на цель Sendmail, содержимое и заголовки письма пересылаются как есть. Для всех других целей система пытается извлечь как строку темы, так и основной текст из содержимого электронного письма. В случаях, когда электронные письма состоят исключительно из HTML-контента, они будут преобразованы в формат обычного текста во время этого процесса.

5.12.10.4 Разрешения

Чтобы изменить/просмотреть конфигурацию для целей уведомлений, требуются разрешения Sys.Modify/Sys.Audit для узла ACL /system/notifications.

5.12.10.5 Режим уведомления

Хранилища данных и конфигурация задания резервного копирования/восстановления на ленту имеют параметр `notification-mode`, который может иметь одно из двух значений:

- legacy-sendmail – отправлять уведомления по электронной почте с помощью системной команды sendmail. Система уведомлений будет проигнорирована. Этот режим эквивалентен поведению уведомлений для версии PBS<3.2;
- notification-system – использовать систему уведомлений.

Если параметр notification-mode не установлен, PBS по умолчанию будет использовать legacy-sendmail.

Начиная с PBS 3.2, хранилище данных, созданное в веб-интерфейсе, автоматически подключится к новой системе уведомлений. Если хранилище данных создано с помощью API или CLI proxmox-backup-manager, параметр notification-mode должен быть явно установлен на notification-system, если будет использоваться система уведомлений.

5.12.10.5.1 Настройки для режима уведомлений legacy-sendmail

Если notification-mode имеет значение legacy-sendmail, PBS будет отправлять уведомления с помощью системной команды sendmail на адрес электронной почты, настроенный для пользователя, установленного в параметре notify-user в файле node.js (или root@pam, если параметр notify-user не установлен).

Для хранилищ данных также можно изменить уровень уведомлений, получаемых для каждого типа задачи, с помощью параметра notify:

- always – отправлять уведомление для любой запланированной задачи, независимо от результата;
- errors – отправлять уведомление для любой запланированной задачи, которая приводит к ошибке;
- never – вообще не отправлять никаких уведомлений.

Параметры notify-user и notify игнорируются, если параметр notification-mode имеет значение notification-system.

5.13 Система резервного копирования UrBackup

UrBackup – это простое в настройке кроссплатформенное клиент-серверное программное обеспечение, позволяющее управлять резервным копированием для компьютеров и операционных систем различных типов. UrBackup позволяет создавать инкрементные и полные резервные копии, как целых разделов, так и отдельных каталогов, с возможностью выбора файлов, которые попадут в архив, а также делать снапшоты разделов жесткого диска.

Примечание. В настоящее время резервные копии образов (снапшоты) работают только с томами в формате NTFS и с клиентами Windows. Резервное копирование образов предназначено в основном для резервного копирования загрузочного тома (C:) систем Windows. Другие данные должны быть скопированы и восстановлены с помощью резервного копирования файлов.

Для управления настройкой резервного копирования и резервными копиями используется веб-интерфейс.

5.13.1 Установка UrBackup

5.13.1.1 Сервер UrBackup

Установить сервер UrBackup:

```
# apt-get install urbackup-server
```

Создать каталог для резервных копий:

```
# mkdir -p /mnt/backups/urbackup
```

Каталог должен принадлежать пользователю urbackup и у этого пользователя должны быть права на чтение/запись:

```
# chown -R urbackup:urbackup /mnt/backups/urbackup
```

Добавить UrBackup-сервер в автозапуск и запустить его:

```
# systemctl enable --now urbackup-server
```

Примечание. UrBackup по умолчанию прослушивает порты 55413 и 55414.

Веб-интерфейс UrBackup будет доступен по адресу http://<ip-сервера>:55414 (Рис. 353).

Веб-интерфейс UrBackup

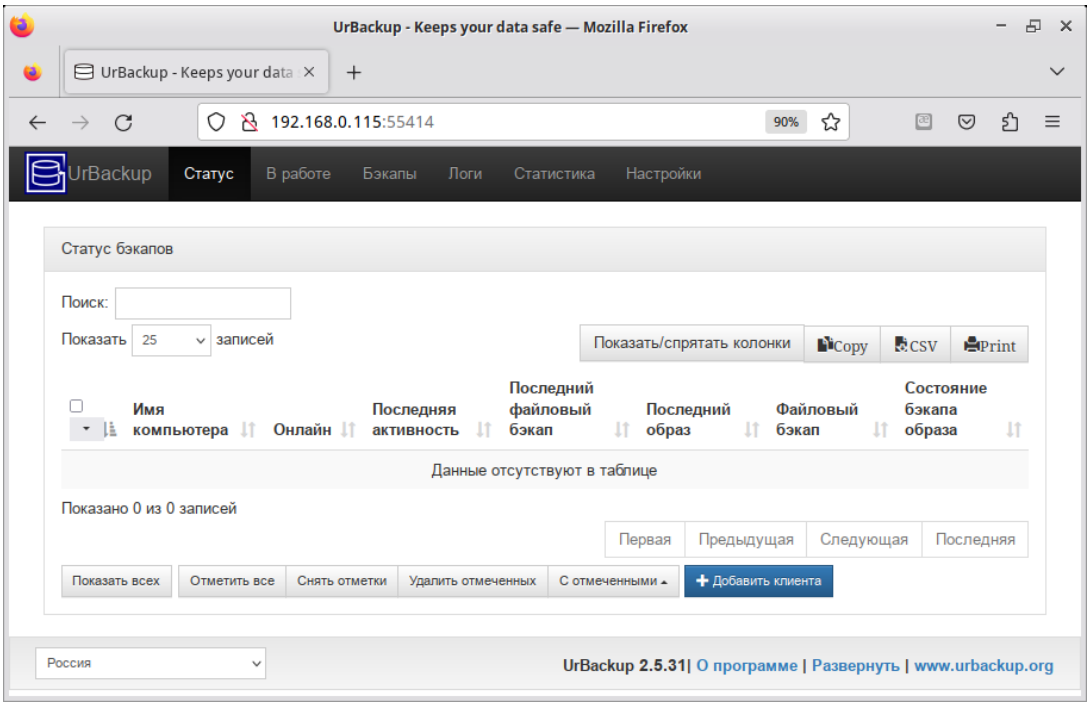


Рис. 353

Примечание. Если появляется ошибка: «Каталог, где UrBackup будет сохранять резервные копии, недоступен…», следует изменить путь к каталогу резервных копий, выбрав пункт меню Настройки, либо изменить права доступа к каталогу.

Сразу после установки доступ к веб-интерфейсу UrBackup будет возможен без аутентификации. Чтобы в дальнейшем требовался ввод имени пользователя и пароля, необходимо создать администратора: перейти на вкладку «Настройки» → «Пользователи» и нажать кнопку «Создать» (Рис. 354).

UrBackup. Создание пользователя

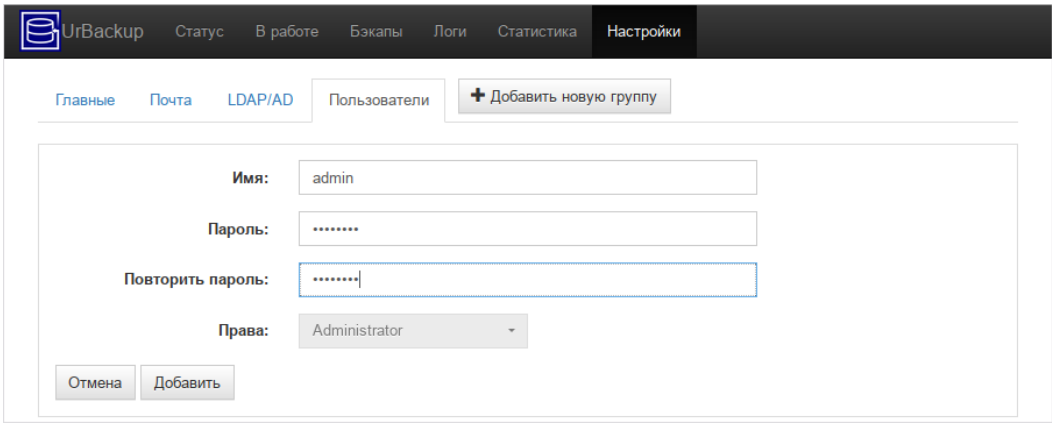


Рис. 354

5.13.1.2 Клиент UrBackup

Установить клиент UrBackup:

```
# apt-get install urbackup-client
```

Добавить UrBackup- клиент в автозапуск и запустить его:

```
# systemctl enable --now urbackup- client
```

Локальные клиенты будут обнаружены сервером автоматически и появятся в веб-интерфейсе на вкладке «Статус» (Рис. 355).

Веб-интерфейс UrBackup

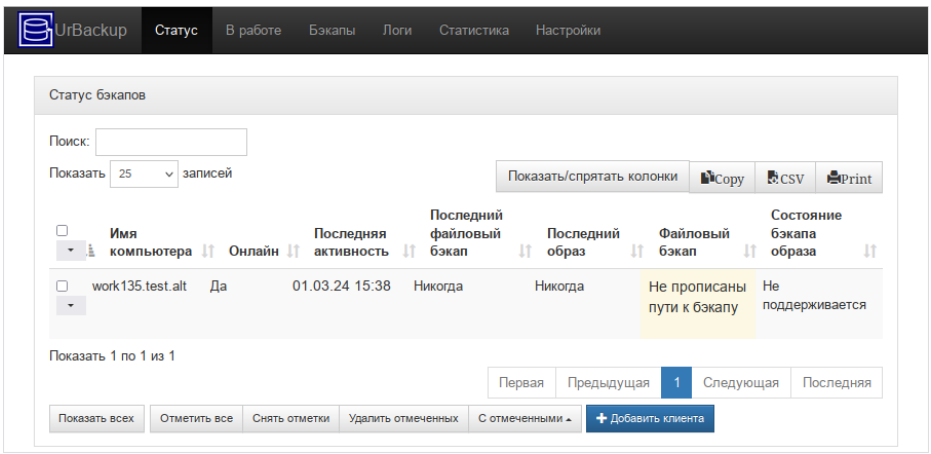


Рис. 355

5.13.2 Настройка резервного копирования

В веб-интерфейсе на вкладке «Настройки» → «Главные» можно изменять настройки UrBackup. Есть настройки, которые влияют только на сервер. Остальные настройки влияют, как на сервер резервного копирования, так и на клиентов. Для этих настроек администратор может установить значения по умолчанию или переопределить настройки клиента.

На вкладке «Сервер» можно указать каталог для хранения резервных копий (Рис. 356).

Настройки UrBackup. Вкладка «Сервер»

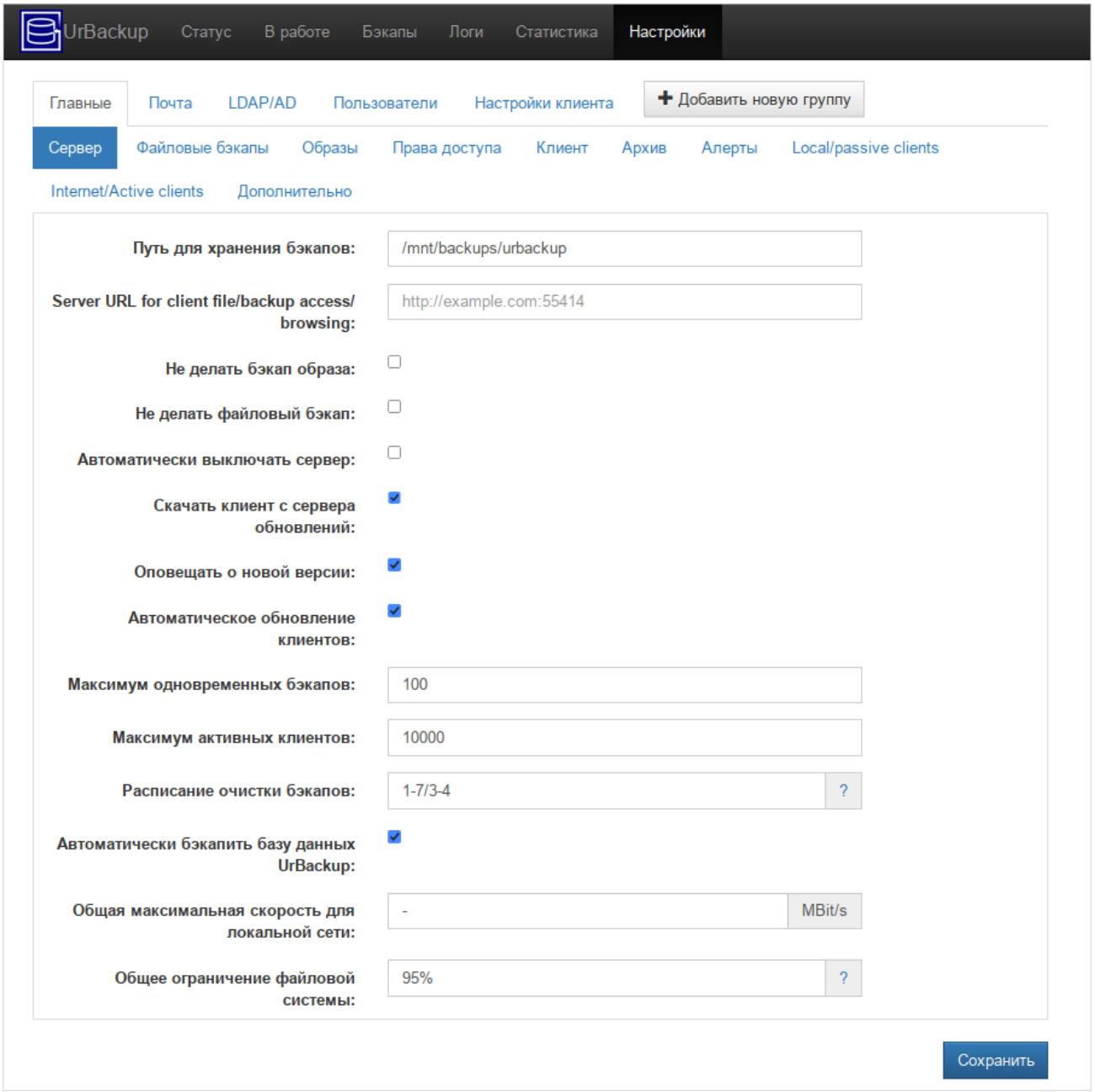


Рис. 356

На вкладке «Файловые бэкапы» можно указать настройки файловых резервных копий, в том числе каталоги, которые будут включены в резервную копию (Рис. 357).

Настройки UrBackup. Вкладка «Файловые бэкапы»

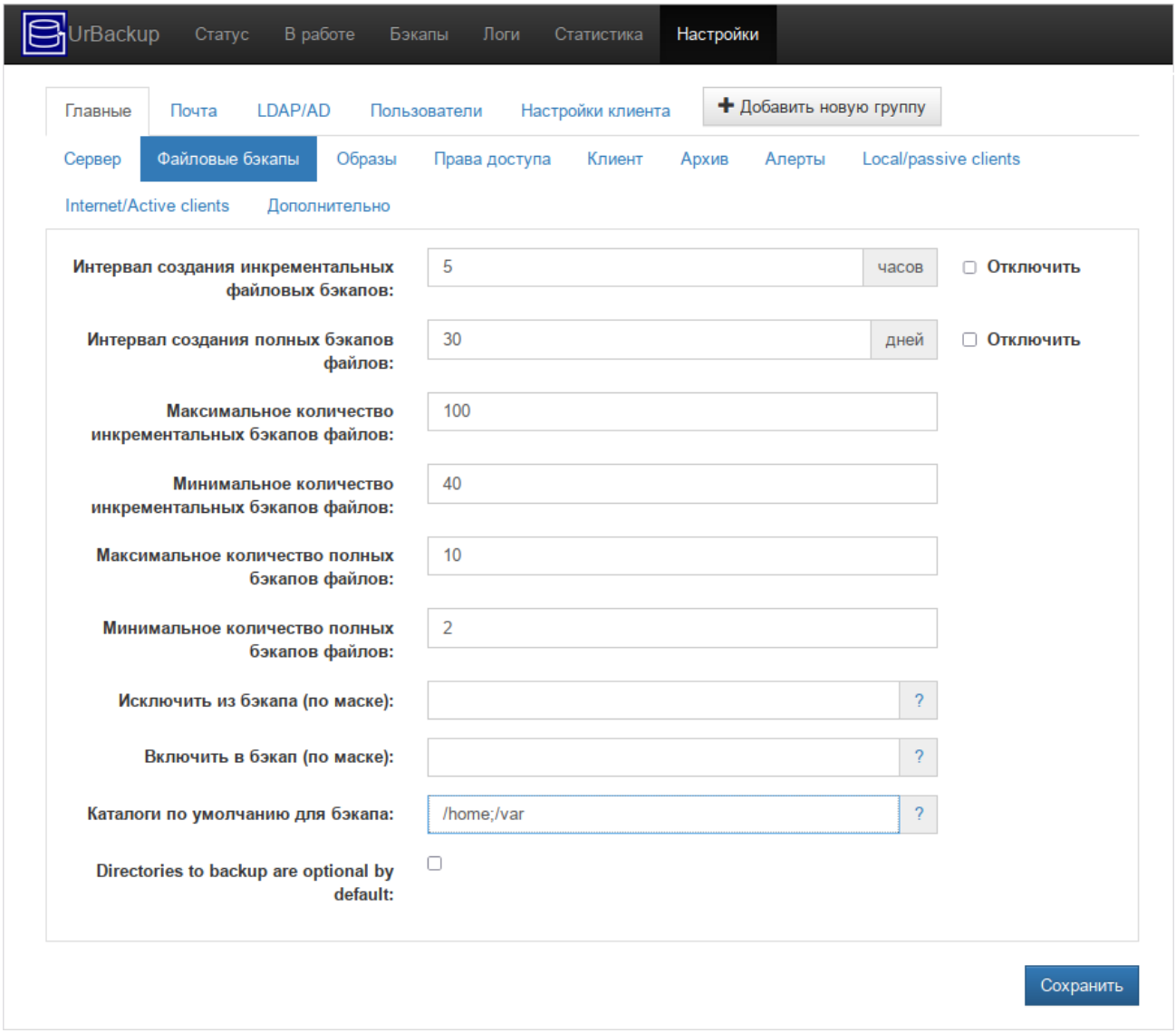


Рис. 357

На вкладке «Клиент» (поле «Расписание») можно установить окно резервного копирования, в пределах которого сервер будет стараться выполнять задания. Начатое задание будет выполняться до завершения, даже если оно не вписывается в указанное время. Примеры окна резервного копирования:

- 1-7/0-24 – резервное копирование может производиться в любое время;
- 1-5/8:00-9:00, 19:30-20:30;6,7/0-24 – резервное копирование в рабочие дни может производиться с 8 до 9 и с 19:30 до 20:30, а в субботу и воскресенье в любое время.

Клиенты могут сами инициировать процесс резервного копирования в любой момент (см. ниже описание утилиты `urbackupclientctl`).

Для более удобного администрирования можно создать несколько групп, распределить клиенты по группам, и задавать настройки отдельно для каждой группы клиентов (Рис. 358).

Настройки UrBackup. Настройка группы клиентов UrBackup

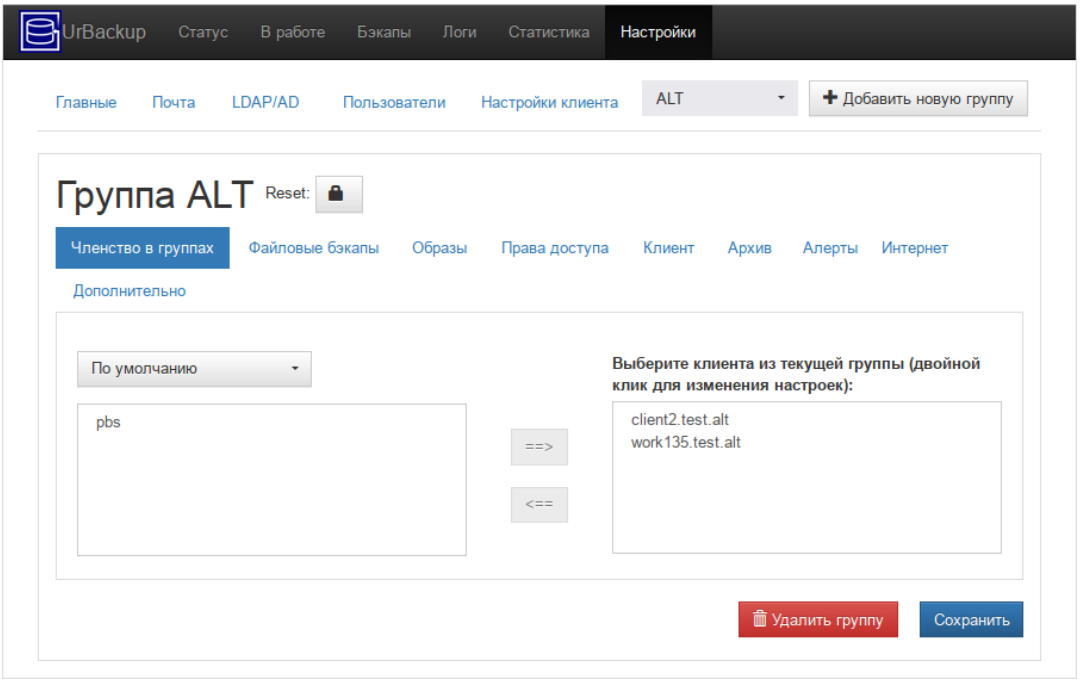


Рис. 358

5.13.3 Создание резервных копий

Инкрементные и полные резервные копии будут создаваться согласно настроенному расписанию.

Процесс создания резервной копии можно запустить вручную, отметив клиента и выбрав тип резервной копии в выпадающем списке (Рис. 359).

UrBackup. Запуск резервного копирования

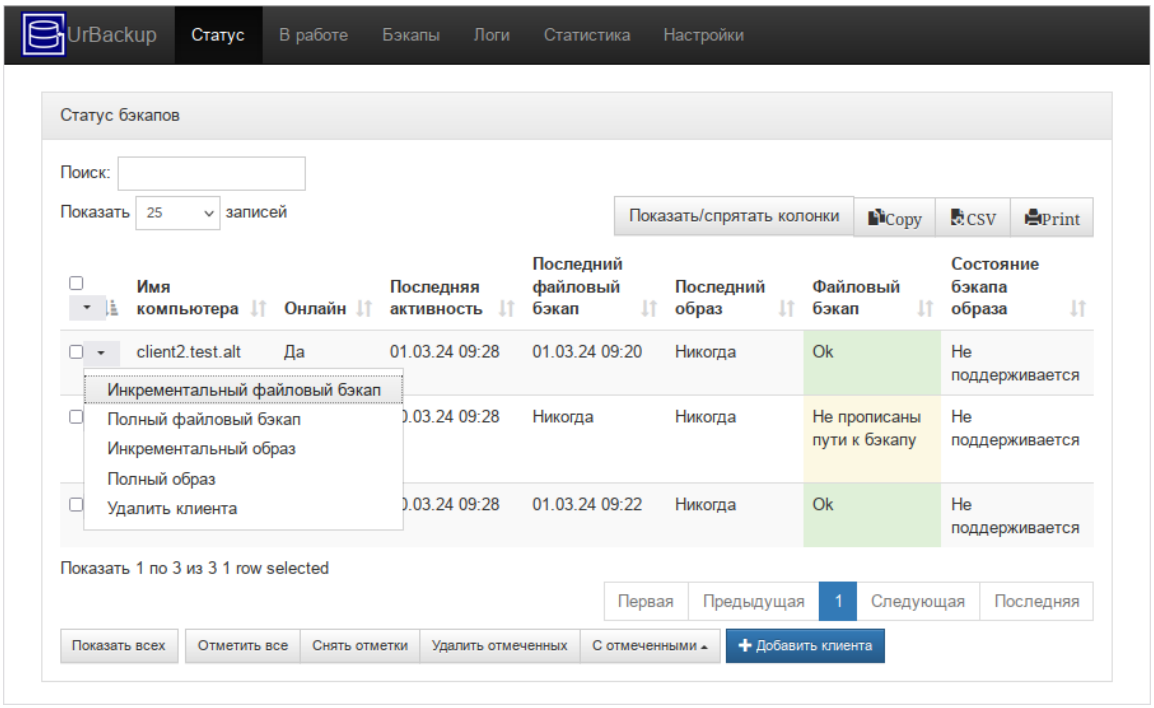


Рис. 359

Более подробно отслеживать активность резервного копирования можно на вкладках «В работе» (Рис. 360), «Бэкапы» и «Логи».

Отчёты/содержимое резервных копий можно просмотреть на вкладке «Бэкапы» (Рис. 361). Выбрав клиента, можно просмотреть список его резервных копий (Рис. 362)

UrBackup. Вкладка «В работе»

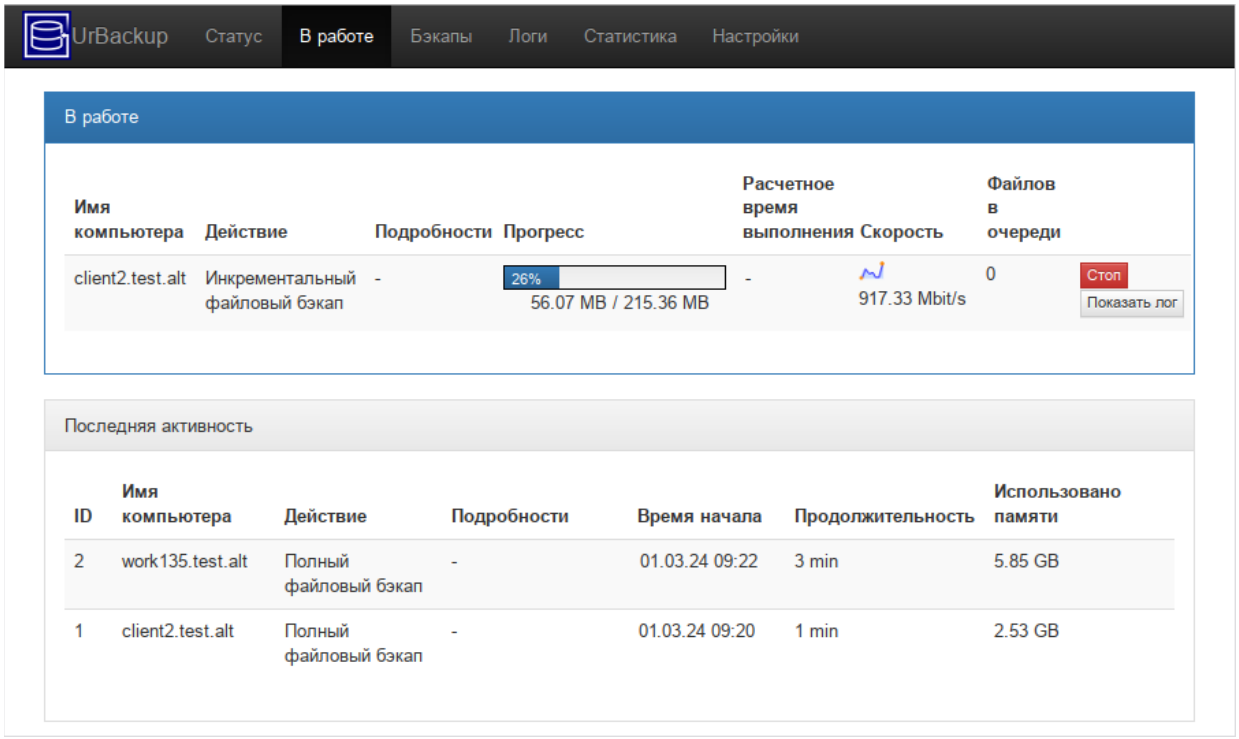


Рис. 360

UrBackup. Вкладка «Бэкапы»

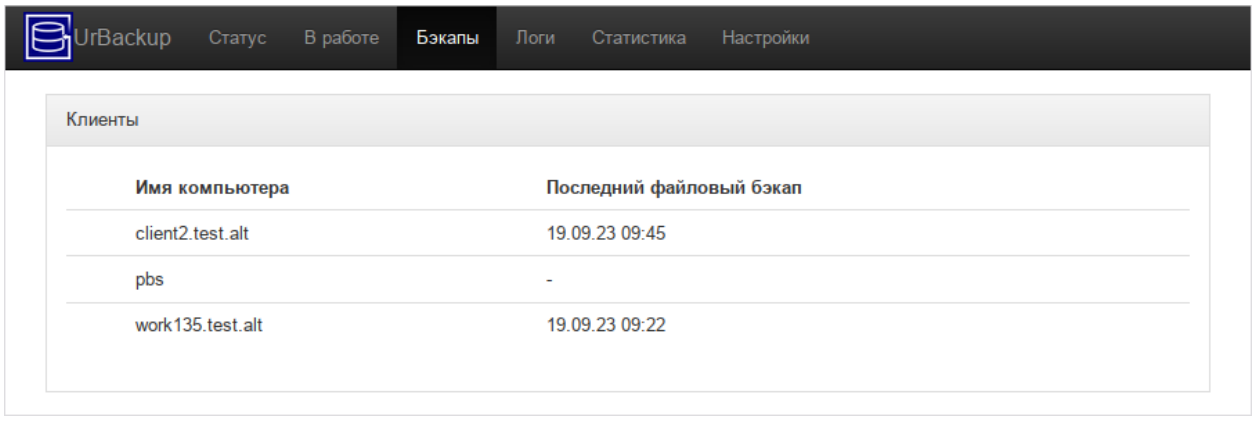


Рис. 361

UrBackup. Список резервных копий клиента client2.test.alt

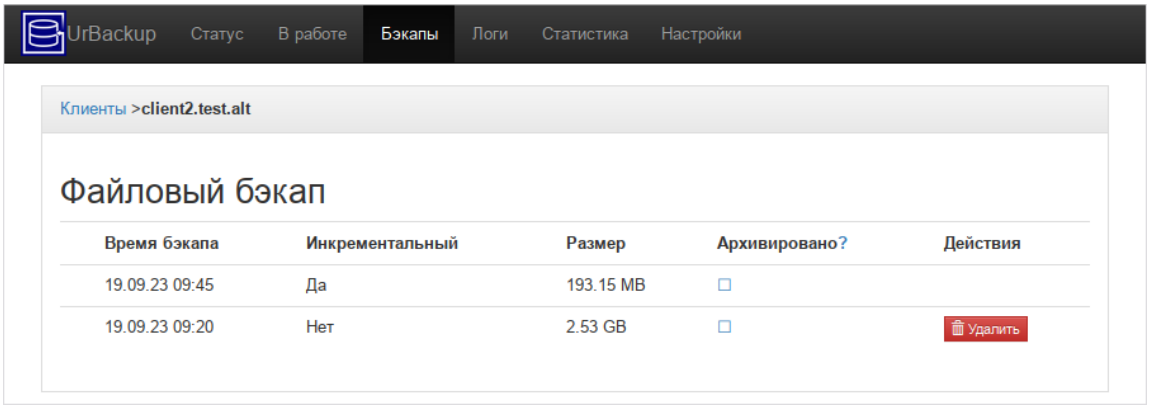


Рис. 362

Примечание. Если отметка в столбце «Архивировано» установлена, резервная копия архивируется. Пока резервная копия заархивирована, её нельзя удалить средствами UrBackup.

Выбрав резервную копию, можно просмотреть её содержимое (Рис. 363).

Содержимое резервной копии

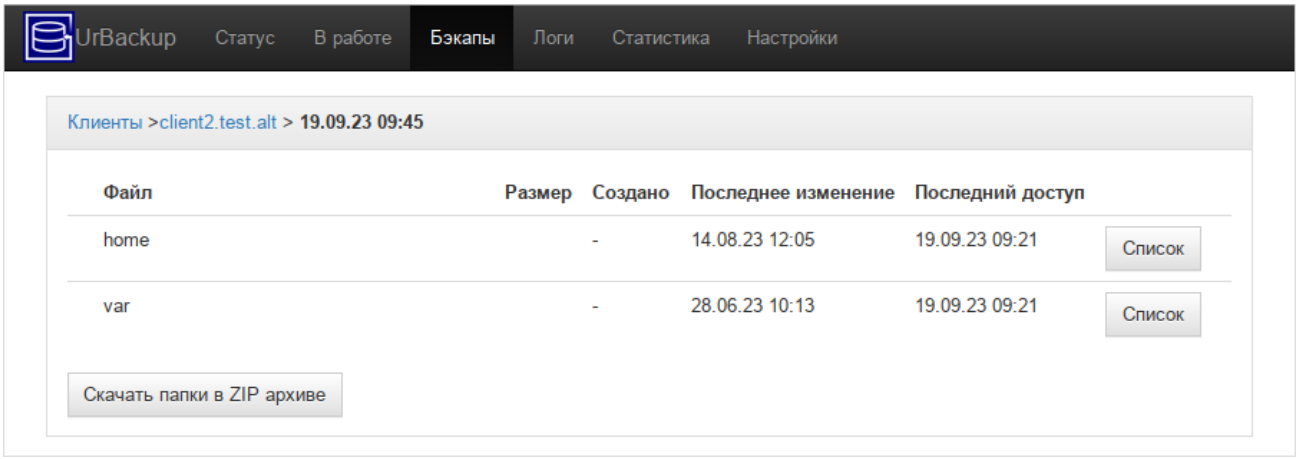


Рис. 363

Резервные копии сохраняются в каталоге, который был указан в веб-интерфейсе. В этом каталоге для каждого клиента создается свой подкаталог. Резервные копии файлов находятся в подкаталогах вида <YYMMDD-HHMM>. Каталог `current` является ссылкой на последнюю резервную копию. Резервные копии папок с файлами сохраняются в открытом виде. Образы дисковых разделов хранятся в виде файлов в формате vhdz (имя файла будет иметь вид Image_<Drive>_<YYMMDD-HHMM>.vhdz).

5.13.4 Утилита `urbackupclientctl`

Для работы с UrBackup на клиенте предназначена утилита `urbackupclientctl`:

- `urbackupclientctl start` – запустить инкрементное/полное резервное копирование;
- `urbackupclientctl status` – получить текущий статус резервного копирования;

- `urbackupclientctl browse` – просмотр списка резервных копий и файлов в резервных копиях;
- `urbackupclientctl restore-start` – восстановить файлы из резервной копии;
- `urbackupclientctl set-settings` – установить параметры резервного копирования;
- `urbackupclientctl add-backupdir` – добавить новый каталог в список каталогов, для которых выполняется резервное копирование;
- `urbackupclientctl list-backupdirs` – вывести список каталогов, для которых выполняется резервное копирование;
- `urbackupclientctl remove-backupdir` – удалить каталог из списока каталогов, для которых выполняется резервное копирование.

Справку по конкретной команде можно получить, выполнив команду:

```
urbackupclientctl <command> --help
```

Ниже приведены примеры использования утилиты `urbackupclientctl`.

Вывести список резервных копий:

```
$ urbackupclientctl browse

[{
"archived": 0,
"backuptime": 1709304813,
"disable_delete": true,
"id": 3,
"incremental": 0,
"size_bytes": 49182025
}
,{
"archived": 0,
"backuptime": 1709304721,
"id": 2,
"incremental": 0,
"size_bytes": 684214036
}
]
```

Запустить процесс создания полной резервной копии:

```
# urbackupclientctl start -f
```

```
Waiting for server to start backup... done
Preparing... -
Completed successfully.
```

Восстановить файлы из резервной копии:

```
# urbackupclientctl restore-start -b 2

Starting restore. Waiting for backup server...  done
[============================================================>  ]  97%
2.33831 GB/2.41119 GB at 76.024 KBit/s
Restore completed successfully.
```

6 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.

Примечание. В установочный комплект ОС «Альт Сервер» включено наиболее употребительное программное обеспечение. В то же время вы можете использовать репозиторий продукта (p10) для установки дополнительных программных пакетов.

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

6.1 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. 364).

Модуль «Установка программ»

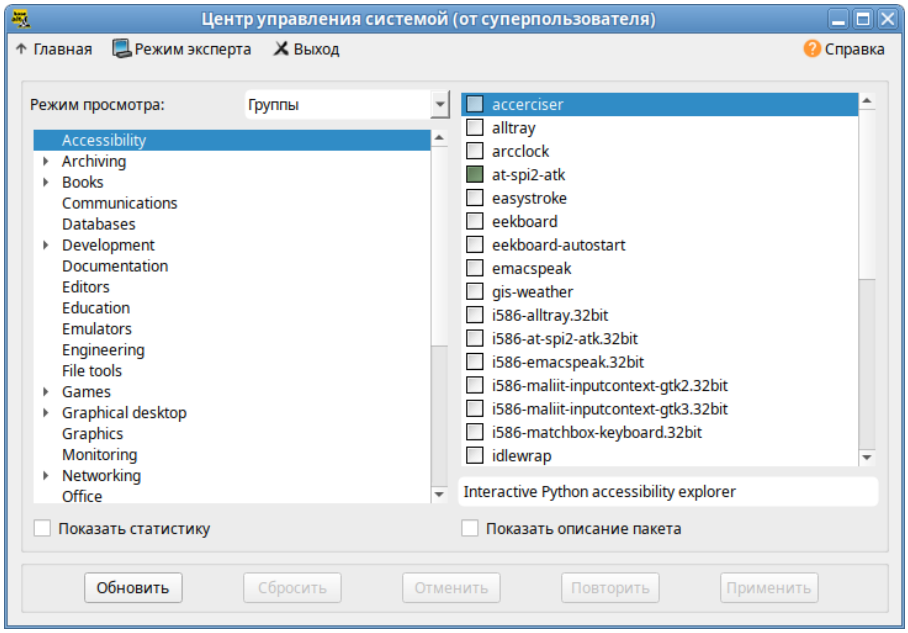


Рис. 364

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.

6.2 Программа управления пакетами Synaptic

Запустить программу управления пакетами Synaptic можно, выбрав пункт «Меню MATE» → «Приложения» → «Параметры» → «Программа управления пакетами Synaptic».

При запуске необходимо ввести пароль администратора системы (Рис. 365).

Synaptic. Запрос пароля администратора

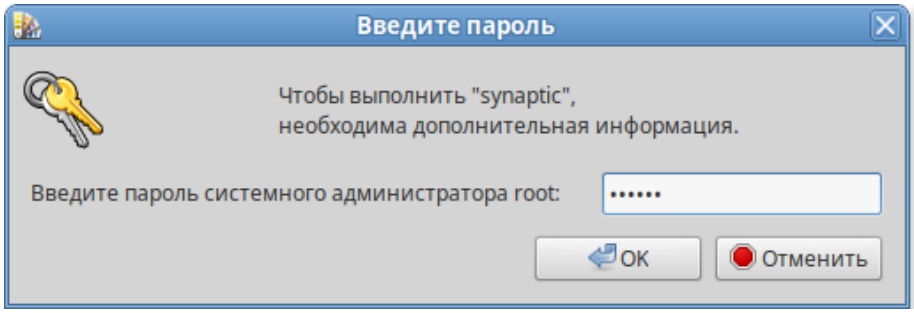


Рис. 365

Для облегчения поиска доступные для установки программы разделены на группы, выводимые в левой части окна программы (Рис. 366).

Справа расположен список самих программ с указанием их текущего состояния:

- зелёная метка – пакет уже установлен;
- зелёная метка со звёздочкой – пакет уже установлен, но для него имеются обновления;
- белая метка со звёздочкой – 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.

6.3 Управление репозиториями

6.3.1 Управление репозиториями 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. 367). К предложенному списку можно добавить любые репозитории, нажав на кнопку «Создать» и введя необходимые данные.

Программа управления пакетами Synaptic

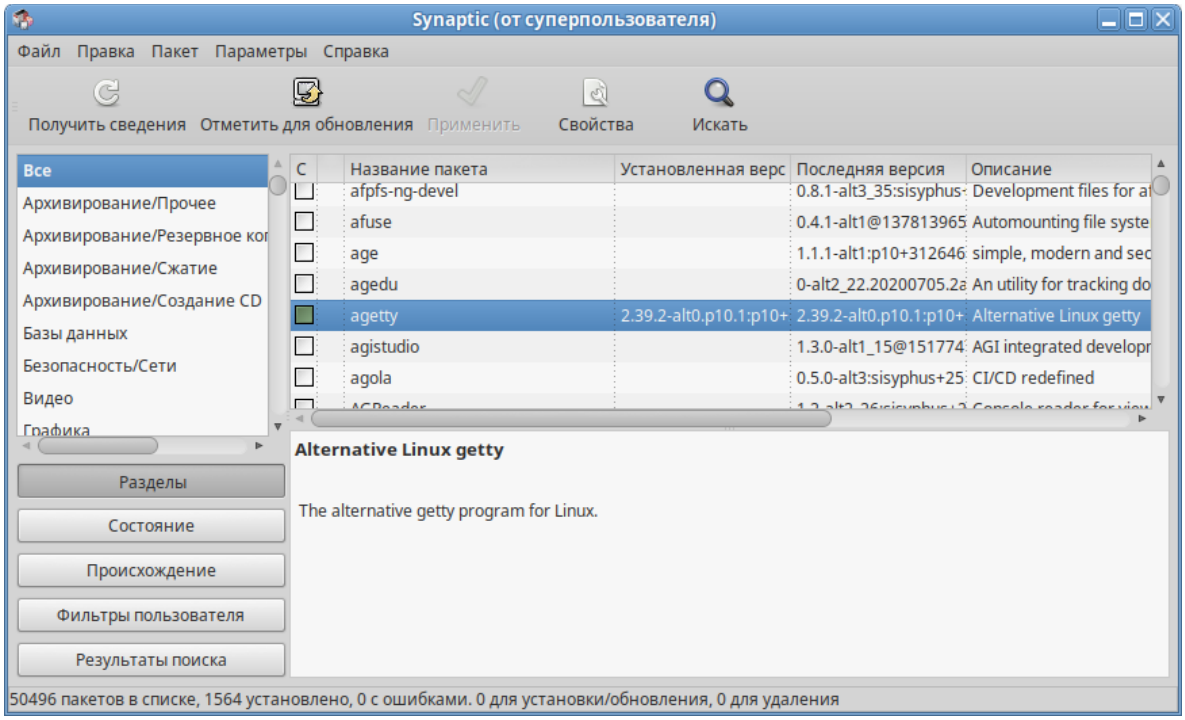


Рис. 366

Добавление репозиториев в Synaptic

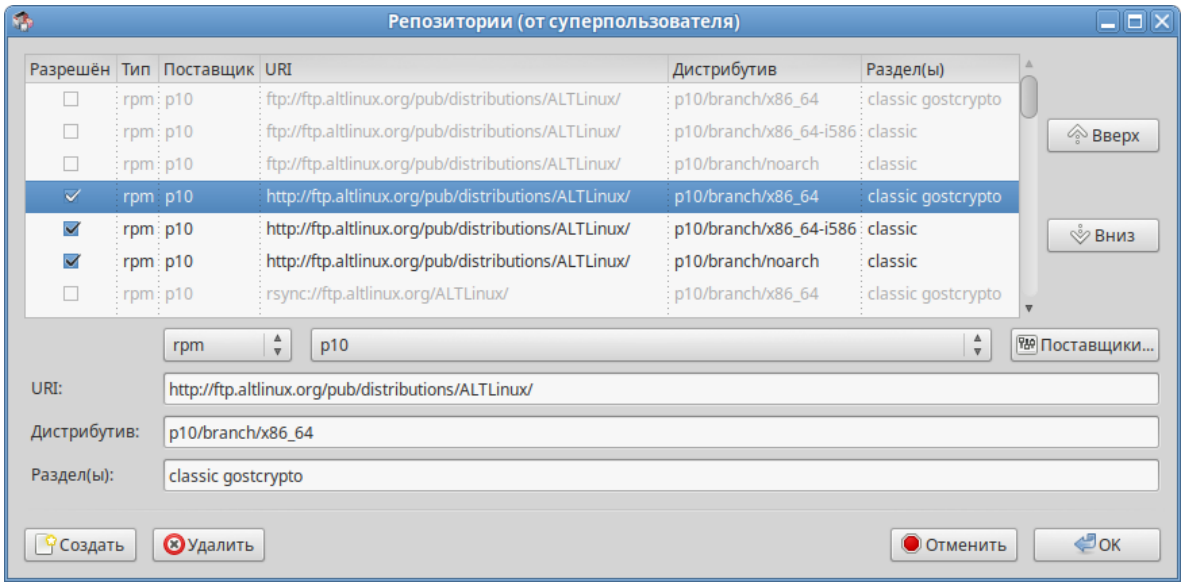


Рис. 367

После выбора и добавления репозиториев необходимо получить сведения о находящихся в них пакетах (кнопка «Получить сведения» см. Рис. 366). В противном случае, список доступных для установки программ будет не актуален.

6.4 Обновление системы

6.4.1 Обновление всех установленных пакетов в Synaptic

Synaptic предоставляет два варианта обновления системы:

- интеллектуальное 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 интеллектуальное обновление. Для того чтобы изменить метод обновления системы, необходимо открыть диалоговое окно «Параметры» («Параметры» → «Параметры») и на вкладке «Основное» 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» (Рис. 368). Будет показан список изменений, который произойдет при обновлении пакетов. Тут следует обратить внимание на объём данных, который будет скачан из сети. После подтверждения Synaptic начнёт загружать файлы, затем начнётся непосредственно установка.

Обновление всех установленных пакетов в Synaptic

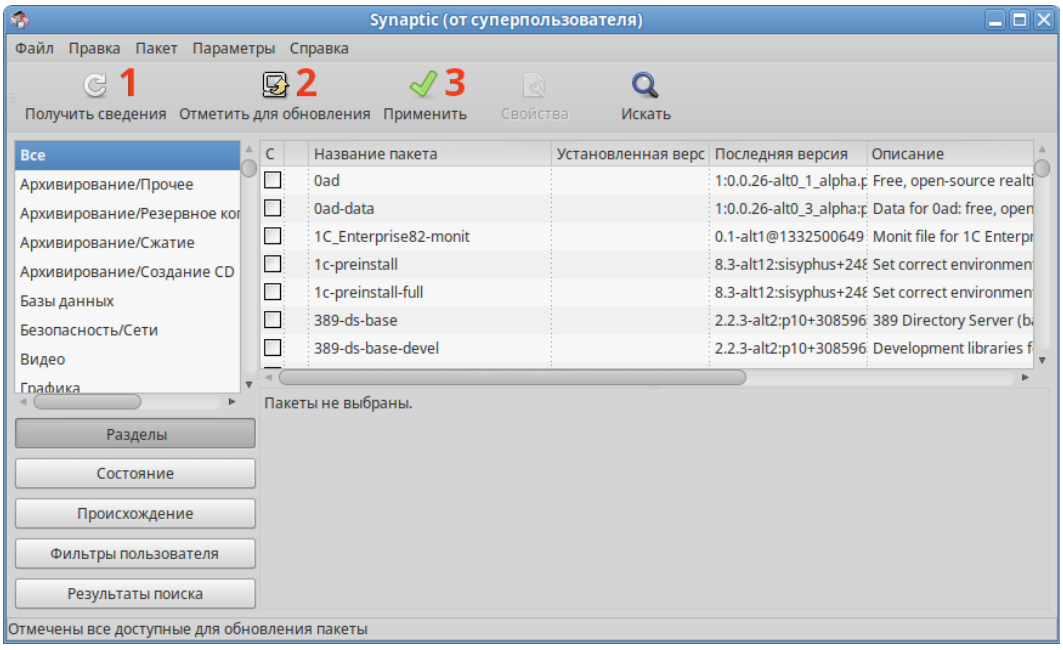


Рис. 368

6.5 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.

6.5.1 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 вет-

кой 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.

6.5.1.1 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.

6.5.1.1.1 Утилита apt-repo для работы с репозиториями

Для добавления репозиториев можно воспользоваться утилитой `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 репозиторий p10 (архитектура выбирается автоматически):

```
# apt-repo rm all
# apt-repo add p10
```

Или то же самое одной командой:

```
# apt-repo set p10
```

6.5.1.1.2 Добавление репозитория на сменном носителе

Для добавления в `sources.list` репозитория на сменном носителе в APT предусмотрена специальная утилита – `apt-cdrom`.

Чтобы добавить запись о репозитории на сменном носителе необходимо:

1. Создать каталог для монтирования. Точка монтирования указывается в параметре `Acquire::CDROM::mount` в файле конфигурации APT (/etc/apt/apt.conf), по умолчанию это `/media/ALTLinux`:

```
# mkdir /media/ALTLinux
```

2. Примонтировать носитель в указанную точку:

```
# mount /dev/носитель /media/ALTLinux
```

где `/dev/носитель` – соответствующее блочное устройство (например, `/dev/dvd` – для CD/DVD-диска).

3. Добавить носитель, выполнив команду:

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

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

```
rpm cdrom:[ALT Server 10.4 x86_64 build 2024-10-16]/ ALTLinux main
```

Примечание. Команду mount /dev/носитель /media/ALTLinux необходимо выполнять перед каждой командой apt-get install имя_пакета.

6.5.1.1.3 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
p10/x86_64 classic
rpm [alt] http://ftp.altlinux.org/pub/distributions/ALTLinux
p10/x86_64-i586 classic
rpm [alt] http://ftp.altlinux.org/pub/distributions/ALTLinux
p10/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.

6.5.1.2 Обновление информации о репозиториях

Практически любое действие с системой apt начинается с обновления данных от активированных 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.

6.5.2 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.

6.5.3 Установка или обновление пакета

Установка пакета с помощью APT выполняется командой:

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

П р и м е ч а н и е . 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 (если пакет еще не установлен):

```
# 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.

Например, если пакет gimp установлен и в репозитории нет обновлённой версии этого пакета, то вывод команды `apt-get install gimp` будет таким:

```
# apt-get install gimp
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Последняя версия gimp уже установлена.
0 будет обновлено, 0 новых установлено, 0 пакетов будет удалено и 2262
не будет обновлено.
```

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
```

6.5.4 Удаление установленного пакета

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

6.5.5 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.

6.5.6 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.

6.6 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 форматов пакетов: 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 ко-

мандой `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
```

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 5.10.

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 командный 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 – каталоги, 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 каталоге `/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 gunzip, можно набрать следующую команду:

```
$ gu
```

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 gu.

В предложенном примере можно получить следующий список:

```
$ gu
guile gunzip gupnp-binding-tool
```

Если набрать: n (gunzip – это единственное имя, третьей буквой которого является «n»), а затем нажать клавишу <Tab>, то оболочка самостоятельно дополнит имя. Чтобы запустить команду нужно нажать <Enter>.

Программы, вызываемые из командной строки, Bash ищет в каталогах, определяемых в системной переменной PATH. По умолчанию в этот перечень каталогов не входит текущий каталог, обозначаемый ./ (точка слеш) (если только не выбран один из двух самых слабых уровней защиты). Поэтому, для запуска программы из текущего каталога, необходимо использовать команду (в примере запускается команда prog):

```
./prog
```

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
```

Примечание. Параметры команд обычно начинаются с символа «-», и обычно после одного символа «-» можно указать сразу несколько опций. Например, вместо команды `ls -l -F` можно ввести команду `ls -lF`

8.1.2.1 Учетные записи пользователей

Команда su

Команда `su` позволяет изменить «владельца» текущего сеанса (сессии) без необходимости завершать сеанс и открывать новый.

Синтаксис:

```
su [ОПЦИИ...] [ПОЛЬЗОВАТЕЛЬ]
```

Команду можно применять для замены текущего пользователя на любого другого, но чаще всего она используется для получения пользователем прав суперпользователя (root).

При вводе команды `su -` будет запрошен пароль суперпользователя (root), и, в случае ввода корректного пароля, пользователь получит привилегии суперпользователя. Чтобы вернуться к правам пользователя, 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 [опции...] [файл...]
```

Основные опции:

`-a` – просмотр всех файлов, включая скрытые;

`-l` – отображение более подробной информации;

`-R` – выводить рекурсивно информацию о подкаталогах.

Команда cd

Команда `cd` предназначена для смены каталога. Команда работает как с абсолютными, так и с относительными путями. Если каталог не указан, используется значение переменной окружения `$HOME` (домашний каталог пользователя). Если каталог задан полным маршрутным именем, он становится текущим. По отношению к новому каталогу нужно иметь право на выполнение, которое в данном случае трактуется как разрешение на поиск.

Синтаксис:

```
cd [-L|-P] [каталог]
```

Если в качестве аргумента задано «-», то это эквивалентно `$OLDPWD`. Если переход был осуществлен по переменной окружения `$CDPATH` или в качестве аргумента был задан «-» и смена каталога была успешной, то абсолютный путь нового рабочего каталога будет выведен на стандартный вывод.

Примеры:

- находясь в домашнем каталоге перейти в его подкаталог `docs/` (относительный путь):

```
$ cd docs/
```

- сделать текущим каталог `/usr/bin` (абсолютный путь):

```
$ cd /usr/bin/
```

- сделать текущим родительский каталог:

```
$ cd ..
```

- вернуться в предыдущий каталог:

```
$ cd -
```

- сделать текущим домашний каталог:

```
$ cd
```

Команда pwd

Команда `pwd` выводит абсолютный путь текущего (рабочего) каталога.

Синтаксис:

```
pwd [-L|-P]
```

Опции:

`-P` – не выводить символические ссылки;

`-L` – выводить символические ссылки.

Команда rm

Команда `rm` служит для удаления записей о файлах. Если заданное имя было последней ссылкой на файл, то файл уничтожается.

Синтаксис:

```
rm [опции...] 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...]
```

Основные опции:

-p – удалить каталог и его потомки.

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

Команда cp

Команда cp предназначена для копирования файлов из одного в другие каталоги.

Синтаксис:

```
cp [-fip] [исх_файл] [цел_файл]
cp [-fip] [исх_файл...] [каталог]
cp [-R] [[-H] | [-L] | [-P]] [-fip] [исх_файл...] [каталог]
```

Основные опции:

-p – сохранять по возможности времена изменения и доступа к файлу, владельца и группу, права доступа;

-i – запрашивать подтверждение перед копированием в существующие файлы;

-r, -R – рекурсивно копировать содержимое каталогов.

Команда mv

Команда mv предназначена для перемещения файлов.

Синтаксис:

```
mv [-fi] [исх_файл...] [цел_файл]
mv [-fi] [исх_файл...] [каталог]
```

В первой синтаксической форме, характеризующейся тем, что последний операнд не является ни каталогом, ни символической ссылкой на каталог, mv перемещает исх_файл в цел_файл (происходит переименование файла).

Во второй синтаксической форме mv перемещает исходные файлы в указанный каталог под именами, совпадающими с краткими именами исходных файлов.

Основные опции:

-f – не запрашивать подтверждения перезаписи существующих файлов;

-i – запрашивать подтверждение перезаписи существующих файлов.

Команда cat

Команда `cat` последовательно выводит содержимое файлов.

Синтаксис:

```
cat [опции...] [файл...]
```

Основные опции:

`-n`, `--number` – нумеровать все строки при выводе;

`-E`, `--show-ends` – показывать $ в конце каждой строки.

Если файл не указан, читается стандартный ввод. Если в списке файлов присутствует имя «-», вместо этого файла читается стандартный ввод.

Команда head

Команда `head` выводит первые 10 строк каждого файла на стандартный вывод.

Синтаксис:

```
head [опции...] [файл...]
```

Основные опции:

`-n`, `--lines=[-]K` – вывести первые К строк каждого файла, а не первые 10;

`-q`, `--quiet` – не печатать заголовки с именами файлов.

Команда less

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

Синтаксис:

```
less имя_файла
```

Команда grep

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

Синтаксис:

```
grep шаблон_поиска файл
```

8.1.2.3 Поиск файлов

Команда find

Команда `find` предназначена для поиска всех файлов, начиная с корневого каталога. Поиск может осуществляться по имени, типу или владельцу файла.

Синтаксис:

```
find [-H] [-L] [-P] [-Оуровень] [-D help|tree|search|stat|rates|opt|
exec] [путь…] [выражение]
```

Ключи для поиска:

`-name` – поиск по имени файла;

`-type` – поиск по типу f=файл, d=каталог, l=ссылка(lnk);

-user – поиск по владельцу (имя или UID).

Когда выполняется команда find, можно выполнять различные действия над найденными файлами. Основные действия:

-exec команда \; – выполнить команду. Запись команды должна заканчиваться экранированной точкой с запятой. Строка «{}» заменяется текущим маршрутным именем файла;

-execdir команда \; – то же самое что и exec, но команда вызывается из подкаталога, содержащего текущий файл;

-ok команда – эквивалентно -exec за исключением того, что перед выполнением команды запрашивается подтверждение (в виде сгенерированной командной строки со знаком вопроса в конце) и она выполняется только при ответе: y;

-print – вывод имени файла на экран.

Путем по умолчанию является текущий подкаталог. Выражение по умолчанию -print.

Примеры:

- найти в текущем каталоге обычные файлы (не каталоги), имя которых начинается с символа «~»:

```
$ find . -type f -name "~*" -print
```

- найти в текущем каталоге файлы, измененные позже, чем файл file.bak:

```
$ find . -newer file.bak -type f -print
```

- удалить все файлы с именами a.out или *.o, доступ к которым не производился в течение недели:

```
$ find / \( -name a.out -o -name '*.o' \) \ -atime +7 -exec rm {} \;
```

- удалить из текущего каталога и его подкаталогов все файлы нулевого размера, запрашивая подтверждение:

```
$ find . -size 0c -ok rm {} \;
```

Команда whereis

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

Синтаксис:

```
whereis [опции...] имя_файла
```

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).

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 каталоги]
```

Пример использования команды упаковки архива:

```
$ tar -cf moi_dokumenti.tar Docs project.tex
```

Распаковка содержимого архива в текущий каталог выполняется командой:

```
$ tar -xf [имя файла архива]
```

Для сжатия файлов используются специальные программы сжатия: gzip, bzip2 и 7z.

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, команда `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, команда `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. Команда `sort` является простым фильтром – она сортирует входные данные и посылает результат на стандартный вывод. Совсем простым фильтром является команда `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.

8.3 Средства управления дискреционными правами доступа

8.3.1 Команда chmod

Команда `chmod` предназначена для изменения прав доступа файлов и каталогов.

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, разделеных 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.

Числовой режим состоит из не более четырех восьмеричных цифр (от нуля до семи), которые складываются из битовых масок с разрядами «4», «2» и «1». Любые пропущенные разряды дополняются лидирующими нулями:

- первый разряд выбирает установку идентификатора пользователя (setuid) (4) или идентификатора группы (setgid) (2) или sticky-бита (1);
- второй разряд выбирает права доступа для пользователя, владеющего данным файлом: чтение (4), запись (2) и исполнение (1);
- третий разряд выбирает права доступа для пользователей, входящих в данную группу, с тем же смыслом, что и у второго разряда;

- четвертый разряд выбирает права доступа для остальных пользователей (не входящих в данную группу), опять с тем же смыслом.

Примеры:

- установить права, позволяющие владельцу читать и писать в файл `f1`, а членам группы и прочим пользователям только читать. Команду можно записать двумя способами:

```
$ chmod 644 f1
$ chmod u=rw,go=r f1
```

- позволить всем выполнять файл `f2`:

```
$ chmod +x f2
```

- запретить удаление файла `f3`:

```
$ chmod+t f3
```

- дать всем права на чтение запись и выполнение, а также на переустановку идентификатора группы при выполнении файла `f4`:

```
$ chmod =rwx,g+s f4
$ chmod 2777 f4
```

8.3.2 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
```

8.3.3 Команда chgrp

Команда `chgrp` изменяет группу для каждого заданного файла.

Синтаксис:

```
chgrp [ОПЦИИ] ГРУППА ФАЙЛ
```

Основные опции:

`-R` – рекурсивно изменять файлы и каталоги;

`--reference=ИФАЙЛ` – использовать группу файла ИФАЙЛ.

8.3.4 Команда umask

Команда `umask` задает маску режима создания файла в текущей среде командного интерпретатора равной значению, задаваемому операндом режим. Эта маска влияет на начальное значение битов прав доступа всех создаваемых далее файлов.

Синтаксис:

```
umask [-p] [-S] [режим]
```

Пользовательской маске режима создания файлов присваивается указанное восьмеричное значение. Три восьмеричные цифры соответствуют правам на чтение/запись/выполнение для владельца, членов группы и прочих пользователей соответственно. Значение каждой заданной в маске цифры вычитается из соответствующей «цифры», определенной системой при создании файла. Например, umask 022 удаляет права на запись для членов группы и прочих пользователей (у файлов, создававшихся с режимом 777, он оказывается равным 755; а режим 666 преобразуется в 644).

Если маска не указана, выдается ее текущее значение:

```
$ umask
0022
```

или то же самое в символьном режиме:

```
$ umask -S
u=rwx,g=rx,o=rx
```

Команда `umask` распознается и выполняется командным интерпретатором bash.

8.3.5 Команда chattr

Команда `chattr` изменяет атрибуты файлов на файловых системах ext3, ext4.

Синтаксис:

```
chattr [ -RVf ] [+-=aAcCdDeFijmPsStTux] [ -v версия ] <ФАЙЛЫ> …
```

Основные опции:

`-R` – рекурсивно изменять атрибуты каталогов и их содержимого. Символические ссылки игнорируются;

`-V` – выводит расширенную информацию и версию программы;

`-f` – подавлять сообщения об ошибках;

`-v версия` – установить номер версии/генерации файла.

Формат символьного режима:

```
+-=aAcCdDeFijmPsStTux
```

Оператор «+» означает добавление выбранных атрибутов к существующим атрибутам; «-» означает их снятие; «=» означает определение только этих указанных атрибутов для файлов.

Символы «aAcCdDeFijmPsStTux» указывают на новые атрибуты файлов:

- a – только добавление к файлу;
- A – не обновлять время последнего доступа (atime) к файлу;
- c – сжатый файл;
- C – отключение режима «Copy-on-write» для указанного файла;
- d – не архивировать (отключает создание архивной копии файла командой `dump`);
- D – синхронное обновление каталогов;
- e – включает использование extent при выделении места на устройстве (атрибут не может быть отключён с помощью `chattr`);
- F – регистронезависимый поиск в каталогах;
- i – неизменяемый файл (файл защищен от изменений: не может быть удалён или переименован, к этому файлу не могут быть созданы ссылки, и никакие данные не могут быть записаны в этот файл);
- j – ведение журнала данных (данные файла перед записью будут записаны в журнал ext3/ ext4);
- m – не сжимать;
- P – каталог с вложенными файлами является иерархической структурой проекта;
- s – безопасное удаление (перед удалением все содержимое файла полностью затирается «00»);
- S – синхронное обновление (аналогичен опции монтирования «sync» файловой системы);
- t – отключает метод tail-merging для файлов;
- T – вершина иерархии каталогов;
- u – неудаляемый (при удалении файла его содержимое сохраняется, это позволяет пользователю восстановить файл);

  x – прямой доступ к файлам (атрибут не может быть установлен с помощью `chattr`).

8.3.6 Команда lsattr

Команда `lsattr` выводит атрибуты файла расширенной файловой системы.

Синтаксис:

```
lsattr [ -RVadlpv ] <ФАЙЛЫ> …
```

Опции:

`-R` – рекурсивно изменять атрибуты каталогов и их содержимого. Символические ссылки игнорируются;

`-V` – выводит расширенную информацию и версию программы;

`-a` – просматривает все файлы в каталоге, включая скрытые файлы (имена которых начинаются с «.»);

`-d` – отображает каталоги так же, как и файлы вместо того, чтобы просматривать их содержимое;

`-l` – отображает параметры, используя длинные имена вместо одного символа;

`-p` – выводит номер проекта файла;

`-v` – выводит номер версии/генерации файла.

8.3.7 Команда getfacl

Команда `getfacl` выводит атрибуты файла расширенной файловой системы.

Синтаксис:

```
getfacl [ --aceEsRLPtpndvh ] <ФАЙЛ> …
```

Опции:

`-a` – вывести только ACL файла;

`-d` – вывести только ACL по умолчанию;

`-c` – не показывать заголовок (имя файла);

`-e` – показывать все эффективные права;

`-E` – не показывать эффективные права;

`-s` – пропускать файлы, имеющие только основные записи;

`-R` – для подкаталогов рекурсивно;

`-L` – следовать по символическим ссылкам, даже если они не указаны в командной строке;

`-P` – не следовать по символическим ссылкам, даже если они указаны в командной строке;

`-t` – использовать табулированный формат вывода;

`-p` – не удалять ведущие «/» из пути файла;

`-n` – показывать числовые значения пользователя/группы.

Формат вывода:

```
1: # file: somedir/
2: # owner: lisa
3: # group: staff
4: # flags: -s-
5: user::rwx
```

```
6: user:joe:rwx                 #effective:r-x
7: group::rwx               #effective:r-x
8: group:cool:r-x
9: mask:r-x
10: other:r-x
11: default:user::rwx
12: default:user:joe:rwx #effective:r-x
13: default:group::r-x
14: default:mask:r-x
15: default:oter:---
```

Строки 1 – 3 указывают имя файла, владельца и группу владельцев.

В строке 4 указаны биты setuid (s), setgid (s) и sticky (t): либо буква, обозначающая бит, либо тире (-). Эта строка включается, если какой-либо из этих битов установлен, и опускается в противном случае, поэтому она не будет отображаться для большинства файлов.

Строки 5, 7 и 10 относятся к традиционным битам прав доступа к файлу, соответственно, для владельца, группы-владельца и всех остальных. Эти три элемента являются базовыми. Строки 6 и 8 являются элементами для отдельных пользователя и группы. Строка 9 – маска эффективных прав. Этот элемент ограничивает эффективные права, предоставляемые всем группам и отдельным пользователям. Маска не влияет на права для владельца файла и всех других. Строки 11 – 15 показывают ACL по умолчанию, ассоциированный с данным каталогом.

8.3.8 Команда setfacl

Команда `setfacl` изменяет ACL к файлам или каталогам. В командной строке за последовательностью команд идет последовательность файлов (за которой, в свою очередь, может идти последовательность команд и так далее).

Синтаксис:

```
setfacl [-bkndRLPvh] [{-m|-x} acl_spec] [{-M|-X} acl_file] <ФАЙЛ> …
setfacl --restore=file
```

Опции:

`-b` – удалить все разрешенные записи ACL;

`-k` – удалить ACL по умолчанию;

`-n` – не пересчитывать маску эффективных прав, обычно `setfacl` пересчитывает маску (кроме случая явного задания маски) для того, чтобы включить ее в максимальный набор прав доступа элементов, на которые воздействует маска (для всех групп и отдельных пользователей);

`-d` – применить ACL по умолчанию;

`-R` – для подкаталогов рекурсивно;

`-L` – переходить по символическим ссылкам на каталоги (имеет смысл только в сочетании с опцией `-R`);

`-P` – не переходить по символическим ссылкам на каталоги (имеет смысл только в сочетании с опцией `-R`);

`-L` – следовать по символическим ссылкам, даже если они не указаны в командной строке;

`-P` – не следовать по символическим ссылкам, даже если они указаны в командной строке;

`--mask` – пересчитать маску эффективных прав;

`-m` – изменить текущий ACL для файла;

`-M` – прочитать записи ACL для модификации из файла;

`-x` – удалить записи из ACL файла;

`-X` – прочитать записи ACL для удаления из файла;

`--restore=file` – восстановить резервную копию прав доступа, созданную командой `getfacl -R` или ей подобной. Все права доступа дерева каталогов восстанавливаются, используя этот механизм. В случае если вводимые данные содержат элементы для владельца или группы-владельца, и команда `setfacl` выполняется пользователем с именем root, то владелец и группа-владелец всех файлов также восстанавливаются. Эта опция не может использоваться совместно с другими опциями за исключением опции `--test`;

`--set=acl` – установить ACL для файла, заменив текущий ACL;

`--set-file=file` – прочитать записи ACL для установления из файла;

`--test` – режим тестирования (ACL не изменяются).

При использовании опций `--set`, `-m` и `-x` должны быть перечислены записи ACL в командной строке. Элементы ACL разделяются одинарными кавычками.

При чтении ACL из файла при помощи опций `-set-file`, `-M` и `-X` команда `setfacl` принимает множество элементов в формате вывода команды `getfacl`. В строке обычно содержится не больше одного элемента ACL.

Команда `setfacl` использует следующие форматы элементов ACL:

- права доступа отдельного пользователя (если не задан UID, то права доступа владельца файла):

```
[d[efault]:] [u[ser]:]uid [:perms]
```

- права доступа отдельной группы (если не задан GID, то права доступа группы-владельца):

```
[d[efault]:] g[roup]:gid [:perms]
```

- маска эффективных прав:

`[d[efault]:] m[ask][:] [:perms]`

- права доступа всех остальных:

`[d[efault]:] o[ther][:] [:perms]`

Элемент ACL является абсолютным, если он содержит поле `perms` и является относительным, если он включает один из модификаторов: «+» или «^». Абсолютные элементы могут использоваться в операциях установки или модификации ACL. Относительные элементы могут использоваться только в операции модификации ACL. Права доступа для отдельных пользователей, группы, не содержащие никаких полей после значений UID, GID (поле `perms` при этом отсутствует), используются только для удаления элементов.

Значения UID и GID задаются именем или числом. Поле `perms` может быть представлено комбинацией символов «r», «w», «x», «-» или цифр (0 – 7).

Изначально файлы и каталоги содержат только три базовых элемента ACL: для владельца, группы-владельца и всех остальных пользователей. Существует ряд правил, которые следует учитывать при установке прав доступа:

- не могут быть удалены сразу три базовых элемента, должен присутствовать хотя бы один;
- если ACL содержит права доступа для отдельного пользователя или группы, то ACL также должен содержать маску эффективных прав;
- если ACL содержит какие-либо элементы ACL по умолчанию, то в последнем должны также присутствовать три базовых элемента (т. е. права доступа по умолчанию для владельца, группы-владельца и всех остальных);
- если ACL по умолчанию содержит права доступа для всех отдельных пользователей или групп, то в ACL также должна присутствовать маска эффективных прав.

Для того чтобы помочь пользователю выполнять эти правила, команда `setfacl` создает права доступа, используя уже существующие, согласно следующим условиям:

- если права доступа для отдельного пользователя или группы добавлены в ACL, а маски прав не существует, то создается маска с правами доступа группы-владельца;
- если создан элемент ACL по умолчанию, а трех базовых элементов не было, тогда делается их копия и они добавляются в ACL по умолчанию;
- если ACL по умолчанию содержит какие-либо права доступа для конкретных пользователя или группы и не содержит маску прав доступа по умолчанию, то при создании эта маска будет иметь те же права, что и группа по умолчанию.

Пример. Изменить разрешения для файла `test.txt`, принадлежащего пользователю liza и группе docs, так, чтобы:

- пользователь ivan имел права на чтение и запись в этот файл;

- пользователь misha не имел никаких прав на этот файл.

Исходные данные:

```
$ ls -l test.txt
-rw-r--r-- 1 liza docs 8 янв 22 15:54 test.txt
$ getfacl test.txt
# file: test.txt
# owner: liza
# group: docs
user::rw-
group::r--
other::r--
```

Установить разрешения (от пользователя liza):

```
$ setfacl -m u:ivan:rw- test.txt
$ setfacl -m u:misha:--- test.txt
```

Просмотреть разрешения (от пользователя liza):

```
$ getfacl test.txt
# file: test.txt
# owner: liza
# group: docs
user::rw-
user:ivan:rw-
user:misha:---
group::r--
mask::rw-
other::r—
```

Примечание. Символ «+» (плюс) после прав доступа в выводе команды ls -l указывает на использование ACL:

```
$ ls -l test.txt
-rw-rw-r--+ 1 liza docs 8 янв 22 15:54 test.txt
```

8.4 Управление пользователями

8.4.1 Общая информация

Пользователи и группы внутри системы обозначаются цифровыми идентификаторами – UID и GID, соответственно.

Пользователь может входить в одну или несколько групп. По умолчанию он входит в группу, совпадающую с его именем. Чтобы узнать, в какие еще группы входит пользователь, можно использовать команду `id`, вывод её может быть примерно следующим:

```
uid=500(test) gid=500(test) группы=500(test),16(rpm)
```

Такая запись означает, что пользователь test (цифровой идентификатор 500) входит в группы test и rpm. Разные группы могут иметь разный уровень доступа к тем или иным каталогам; чем в большее количество групп входит пользователь, тем больше прав он имеет в системе.

Примечание. В связи с тем, что большинство привилегированных системных утилит в дистрибутивах «Альт» имеют не SUID-, а SGID-бит, необходимо быть предельно внимательным и осторожным в переназначении групповых прав на системные каталоги.

8.4.2 Команда useradd

Команда `useradd` регистрирует нового пользователя или изменяет информацию по умолчанию о новых пользователях.

Синтаксис:

```
useradd [ОПЦИИ...] <ИМЯ ПОЛЬЗОВАТЕЛЯ>
useradd -D [ОПЦИИ...
```

Возможные опции:

`-b каталог` – базовый каталог для домашнего каталога новой учётной записи;

`-c комментарий` – текстовая строка (обычно используется для указания фамилии и мени);

`-d каталог` – домашний каталог новой учётной записи;

`-D` – показать или изменить настройки по умолчанию для useradd;

`-e дата` – дата устаревания новой учётной записи;

`-g группа` – имя или ID первичной группы новой учётной записи;

`-G группы` – список дополнительных групп (через запятую) новой учётной записи;

`-m` – создать домашний каталог пользователя;

`-M` – не создавать домашний каталог пользователя;

`-p пароль` – зашифрованный пароль новой учётной записи (не рекомендуется);

`-s оболочка` – регистрационная оболочка новой учётной записи (по умолчанию /bin/bash);

`-u UID` – пользовательский ID новой учётной записи.

Команда `useradd` имеет множество параметров, которые позволяют менять её поведение по умолчанию. Например, можно принудительно указать, какой будет UID или какой группе будет принадлежать пользователь:

```
# useradd -u 1500 -G usershares new_user
```

8.4.3 Команда passwd

Команда `passwd` поддерживает традиционные опции passwd и утилит shadow.

Синтаксис:

`passwd [ОПЦИИ...]` *`[ИМЯ ПОЛЬЗОВАТЕЛЯ]`*

Возможные опции:

`-d`, `--delete` – удалить пароль для указанной записи;

`-f`, `--force` – форсировать операцию;

`-k`, `--keep-tokens` – сохранить не устаревшие пароли;

`-l`, `--lock` – блокировать указанную запись;

`--stdin` – прочитать новые пароли из стандартного ввода;

`-S`, `--status` – дать отчет о статусе пароля в указанной записи;

`-u`, `--unlock` – разблокировать указанную запись;

`-?`, `--help` – показать справку и выйти;

`--usage` – дать короткую справку по использованию;

`-V`, `--version` – показать версию программы и выйти.

Код выхода: при успешном завершении `passwd` заканчивает работу с кодом выхода 0. Код выхода 1 означает, что произошла ошибка. Текстовое описание ошибки выводится на стандартный поток ошибок.

Пользователь может в любой момент поменять свой пароль. Единственное, что требуется для смены пароля – знать текущий пароль.

Только суперпользователь может обновить пароль другого пользователя.

8.4.4 Добавление нового пользователя

Для добавления нового пользователя используйте команды `useradd` и `passwd`:

```
# useradd test1

# passwd test1
passwd: updating all authentication tokens for user test1.

You can now choose the new password or passphrase.

A valid password should be a mix of upper and lower case letters, digits, and
other characters.  You can use a password containing at least 7 characters
from all of these classes, or a password containing at least 8 characters
```

```
from just 3 of these 4 classes.
An upper case letter that begins the password and a digit that ends it do not
count towards the number of character classes used.

A passphrase should be of at least 3 words, 11 to 72 characters long, and
contain enough different characters.

Alternatively, if no one else can see your terminal now, you can pick this as
your password: "Burst*texas$Flow".

Enter new password:
Weak password: too short.
Re-type new password:
passwd: all authentication tokens updated successfully.
```

В результате описанных действий в системе появился пользователь test1 с некоторым паролем. Если пароль оказался слишком слабым с точки зрения системы, она об этом предупредит (как в примере выше). Пользователь в дальнейшем может поменять свой пароль при помощи команды `passwd` – но если он попытается поставить слабый пароль, система откажет ему (в отличие от *root*) в изменении.

В ОС «Альт Сервер» для проверки паролей на слабость используется модуль PAM `passwdqc`.

8.4.5 Настройка парольных ограничений

Настройка парольных ограничений производится в файле `/etc/passwdqc.conf`.

Файл `passwdqc.conf` состоит из 0 или более строк следующего формата:

`опция=значение`

Пустые строки и строки, начинающиеся со знака решетка («#»), игнорируются. Символы пробела между опцией и значением не допускаются.

Опции, которые могут быть переданы в модуль (в скобках указаны значения по умолчанию): min=N0,N1,N2,N3,N4 (min=disabled,24,11,8,7) – минимально допустимая длина пароля.

Используемые типы паролей по классам символов (алфавит, число, спецсимвол, верхний и нижний регистр) определяются следующим образом:

- тип N0 используется для паролей, состоящих из символов только одного класса;
- тип N1 используется для паролей, состоящих из символов двух классов;
- тип N2 используется для парольных фраз, кроме этого требования длины, парольная фраза должна также состоять из достаточного количества слов;

- типы N3 и N4 используются для паролей, состоящих из символов трех и четырех классов, соответственно.

Ключевое слово disabled используется для запрета паролей выбранного типа N0 – N4 независимо от их длины.

Примечание. Каждое следующее число в настройке «min» должно быть не больше, чем предыдущее.

При расчете количества классов символов, заглавные буквы, используемые в качестве первого символа и цифр, используемых в качестве последнего символа пароля, не учитываются.

`max=N (max=40)` – максимально допустимая длина пароля. Эта опция может быть использована для того, чтобы запретить пользователям устанавливать пароли, которые могут быть слишком длинными для некоторых системных служб. Значение 8 обрабатывается особым образом: пароли длиннее 8 символов, не отклоняются, а обрезаются до 8 символов для проверки надежности (пользователь при этом предупреждается).

`passphrase=N (passphrase=3)` – число слов, необходимых для ключевой фразы (значение 0 отключает поддержку парольных фраз).

`match=N (match=4)` – длина общей подстроки, необходимой для вывода, что пароль хотя бы частично основан на информации, найденной в символьной строке (значение 0 отключает поиск подстроки). Если найдена слабая подстрока пароль не будет отклонен; вместо этого он будет подвергаться обычным требованиям к прочности при удалении слабой подстроки. Поиск подстроки нечувствителен к регистру и может обнаружить и удалить общую подстроку, написанную в обратном направлении.

`similar=permit|deny (similar=deny)` – параметр `similar=permit` разрешает задать новый пароль, если он похож на старый (параметр `similar=deny` – запрещает). Пароли считаются похожими, если есть достаточно длинная общая подстрока, и при этом новый пароль с частично удаленной подстрокой будет слабым.

`random=N[,only] (random=42)` – размер случайно сгенерированных парольных фраз в битах (от 26 до 81) или 0, чтобы отключить эту функцию. Любая парольная фраза, которая содержит предложенную случайно сгенерированную строку, будет разрешена вне зависимости от других возможных ограничений. Значение `only` используется для запрета выбранных пользователем паролей.

`enforce=none|users|everyone (enforce=users)` – параметр `enforce=users` задает ограничение задания паролей в passwd на пользователей без полномочий root. Параметр `enforce=everyone` задает ограничение задания паролей в `passwd` и на пользователей, и на

суперпользователя root. При значении none модуль PAM будет только предупреждать о слабых паролях.

retry=N (retry=3) – количество запросов нового пароля, если пользователь с первого раза не сможет ввести достаточно надежный пароль и повторить его ввод.

Далее приводится пример задания следующих значений в файле /etc/passwdqc.conf:

```
min=8,7,4,4,4
enforce=everyone
```

В указанном примере пользователям, включая суперпользователя root, будет невозможно задать пароли:

- типа N0 (символы одного класса) – длиной меньше восьми символов;
- типа N1 (символы двух классов) – длиной меньше семи символов;
- типа N2 (парольные фразы), типа N3 (символы трех классов) и N4 (символы четырех классов) – длиной меньше четырех символов.

8.4.6 Управление сроком действия пароля

Для управления сроком действия паролей используется команда chage.

Примечание. Должен быть установлен пакет shadow-change:

```
# apt-get install shadow-change
```

chage изменяет количество дней между сменой пароля и датой последнего изменения пароля.

Синтаксис команды:

```
chage [опции] логин
```

Основные опции:

-d, --lastday LAST_DAY – установить последний день смены пароля в LAST_DAY (число дней с 1 января 1970). Дата может быть указана в формате ГГГГ-ММ-ДД;

-E, --expiredate EXPIRE_DAYS – установить дату окончания действия учётной записи в EXPIRE_DAYS (число дней с 1 января 1970). Дата может быть указана в формате ГГГГ-ММ-ДД. Значение -1 удаляет дату окончания действия учётной записи;

-I, --inactive INACTIVE – используется для задания количества дней «неактивности», то есть дней, когда пользователь вообще не входил в систему, после которых его учетная запись будет заблокирована. Пользователь, чья учетная запись заблокирована, должен обратиться к системному администратору, прежде чем снова сможет использовать систему. Значение -1 отключает этот режим;

-l,--list – просмотр информации о «возрасте» учётной записи пользователя;

`-m, --mindays MIN_DAYS` – установить минимальное число дней перед сменой пароля. Значение 0 в этом поле обозначает, что пользователь может изменять свой пароль, когда угодно;

`-M, --maxdays MAX_DAYS` – установить максимальное число дней перед сменой пароля. Когда сумма MAX_DAYS и LAST_DAY меньше, чем текущий день, у пользователя будет запрошен новый пароль до начала работы в системе. Эта операция может предваряться предупреждением (параметр `-W`). При установке значения `-1`, проверка действительности пароля не будет выполняться;

`-W, --warndays WARN_DAYS` – установить число дней до истечения срока действия пароля, начиная с которых пользователю будет выдаваться предупреждение о необходимости смены пароля.

Пример настройки времени действия пароля для пользователя test:

```
# chage -M 5 test
```

Получить информацию о «возрасте» учётной записи пользователя test:

```
# chage -l test
Последний раз пароль был изменён                    : дек 27, 2023
Срок действия пароля истекает                       : янв 01, 2024
Пароль будет деактивирован через                    : янв 11, 2024
Срок действия учётной записи истекает                     : никогда
Минимальное количество дней между сменой пароля           : -1
Максимальное количество дней между сменой пароля          : 5
Количество дней с предупреждением перед деактивацией пароля     : -1
```

Примечание. Задать время действия пароля для вновь создаваемых пользователей можно, изменив параметр PASS_MAX_DAYS в файле /etc/login.defs.

8.4.7 Настройка неповторяемости пароля

Для настройки неповторяемости паролей используется модуль pam_pwhistory, который сохраняет последние пароли каждого пользователя и не позволяет пользователю при смене пароля чередовать один и тот же пароль слишком часто.

Примечание. В данном случае системный каталог станет доступным для записи пользователям группы `pw_users` (следует создать эту группу и включить в неё пользователей).

Примечание. База используемых паролей ведется в файле `/etc/security/opasswd`, в который пользователи должны иметь доступ на чтение и запись. При этом они могут читать хэши паролей остальных пользователей. Не рекомендуется использовать на многопользовательских системах.

Создайте файл `/etc/security/opasswd` и дайте права на запись пользователям:

```
# install -Dm0660 -gpw_users /dev/null /etc/security/opasswd
# chgrp pw_users /etc/security
# chmod g+w /etc/security
```

Для настройки этого ограничения необходимо изменить файл `/etc/pam.d/system-auth-local-only` таким образом, чтобы он включал модуль `pam_pwhistory` после первого появления строки с паролем:

```
password        required        pam_passwdqc.so config=/etc/passwdqc.-
conf
password        required        pam_pwhistory.so debug use_authtok re-
member=10 retry=3
```

После добавления этой строки в файле `/etc/security/opasswd` будут храниться последние 10 паролей пользователя (содержит хэши паролей всех учетных записей пользователей) и при попытке использования пароля из этого списка будет выведена ошибка:

```
Password has been already used. Choose another.
```

В случае если необходимо, чтобы проверка выполнялась и для суперпользователя root, в настройки нужно добавить параметр enforce_for_root:

```
password        required        pam_pwhistory.so
use_authtok enforce_for_root remember=10 retry=3
```

8.4.8 Модификация пользовательских записей

Для модификации пользовательских записей применяется утилита `usermod`:

```
# usermod -G audio,rpm,test1 test1
```

Такая команда изменит список групп, в которые входит пользователь test1 – теперь это audio, rpm, test1.

```
# usermod -l test2 test1
```

Будет произведена смена имени пользователя с test1 на test2.

Команды `usermod -L test2` и `usermod -U test2` соответственно временно блокируют возможность входа в систему пользователю test2 и возвращают всё на свои места.

Изменения вступят в силу только при следующем входе пользователя в систему.

При неинтерактивной смене или задании паролей для целой группы пользователей используется команда `chpasswd`. На стандартный вход ей следует подавать список, каждая строка которого будет выглядеть как `имя:пароль`.

8.4.9 Удаление пользователей

Для удаления пользователей используется команда `userdel`.

Команда `userdel test2` удалит пользователя test2 из системы. Если будет дополнительно задан параметр `-r`, то будет уничтожен и домашний каталог пользователя. Нельзя удалить пользователя, если в данный момент он еще работает в системе.

8.5 Режим суперпользователя

8.5.1 Какие бывают пользователи?

Linux – система многопользовательская, а потому пользователь – ключевое понятие для организации всей системы доступа в Linux. Файлы всех пользователей в Linux хранятся раздельно, у каждого пользователя есть собственный домашний каталог, в котором он может хранить свои данные. Доступ других пользователей к домашнему каталогу пользователя может быть ограничен.

Суперпользователь в Linux – это выделенный пользователь системы, на которого не распространяются ограничения прав доступа. Именно суперпользователь имеет возможность произвольно изменять владельца и группу файла. Ему открыт доступ на чтение и запись к любому файлу или каталогу системы.

Среди учётных записей Linux всегда есть учётная запись суперпользователя – root. Поэтому вместо «суперпользователь» часто говорят «root». Множество системных файлов принадлежат root, множество файлов только ему доступны для чтения или записи. Пароль этой учётной записи – одна из самых больших драгоценностей системы. Именно с её помощью системные администраторы выполняют самую ответственную работу.

8.5.2 Для чего может понадобиться режим суперпользователя?

Системные утилиты, например, такие, как ЦУС или «Программа управления пакетами Synaptic» требуют для своей работы привилегий суперпользователя, потому что они вносят изменения в системные файлы. При их запуске выводится диалоговое окно с запросом пароля системного администратора.

8.5.3 Как получить права суперпользователя?

Для опытных пользователей, умеющих работать с командной строкой, существует два различных способа получить права суперпользователя.

Первый – это зарегистрироваться в системе под именем root.

Второй способ – воспользоваться специальной утилитой `su` (shell of user), которая позволяет выполнить одну или несколько команд от лица другого пользователя. По умолчанию эта утилита выполняет команду sh от пользователя root, то есть запускает командный интерпретатор. Отличие от предыдущего способа в том, что всегда известно, кто именно запускал `su`, а значит, ясно, кто выполнил определённое административное действие.

В некоторых случаях удобнее использовать не `su`, а утилиту `sudo`, которая позволяет выполнять только заранее заданные команды.

Примечание. Для того чтобы воспользоваться командами `su` и `sudo`, необходимо быть членом группы `wheel`. Пользователь, созданный при установке системы, по умолчанию уже включён в эту группу.

В дистрибутивах «Альт» для управления доступом к важным службам используется подсистема `control`. `control` – механизм переключения между неким набором фиксированных состояний для задач, допускающих такой набор.

Команда `control` доступна только для суперпользователя (root). Для того чтобы посмотреть, что означает та или иная политика `control` (разрешения выполнения конкретной команды, управляемой `control`), надо запустить команду с ключом `help`:

```
# control su help
```

Запустив `control` без параметров, можно увидеть полный список команд, управляемых командой (facilities) вместе с их текущим состоянием и набором допустимых состояний.

8.5.4 Как перейти в режим суперпользователя?

Для перехода в режим суперпользователя наберите в терминале команду (**минус важен!**):

```
su -
```

Если воспользоваться командой `su` без ключа, то происходит вызов командного интерпретатора с правами root. При этом значение переменных окружения, в частности $PATH, остаётся таким же, как у пользователя: в переменной $PATH не окажется каталогов `/sbin`, `/usr/sbin`, без указания полного имени будут недоступны команды `route`, `shutdown`, `mkswap` и другие. Более того, переменная $HOME будет указывать на каталог пользователя, все программы, запущенные в режиме суперпользователя, сохранят свои настройки с правами root в каталоге пользователя, что в дальнейшем может вызвать проблемы.

Чтобы избежать этого, следует использовать `su -`. В этом режиме `su` запустит командный интерпретатор в качестве login shell, и он будет вести себя в точности так, как если бы в системе зарегистрировался root.

8.6 Управление шифрованными разделами

Примечание. Зашифрованный раздел может быть создан, например, при установке системы.

В LUKS для одного зашифрованного раздела используются восемь слотов, в каждом из которых может храниться отдельный пароль (ключ). Любой из восьми ключей может быть использован для расшифровки раздела. Любой пароль может быть изменён или удалён необратимо.

Для управления шифрованными разделами можно воспользоваться командой `cryptsetup`. Ниже описаны лишь некоторые возможности утилиты `cryptsetup`. Для получения более подробной информации используйте команду `man cryptsetup`.

Просмотреть текущее состояние всех слотов:

```
# cryptsetup luksDump /dev/sdb1 | grep Slot
Key Slot 0: DISABLED
Key Slot 1: ENABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

где `/dev/sdb1` – шифрованный раздел.

Примечание. Определить является ли устройство LUKS-разделом можно, выполнив команду:

```
# cryptsetup isLuks -v /dev/sdb1
Команда выполнена успешно.
```

Определить какой раздел является шифруемым можно, выполнив команду:

```
# lsblk
NAME                                          MAJ:MIN RM  SIZE RO TYPE
MOUNTPOINT
sda                                             8:0    0   18G  0 disk
├─sda1                                          8:1    0 1023M  0 part
[SWAP]
└─sda2                                          8:2    0   17G  0 part  /
sdb                                             8:16   0   18G  0 disk
└─sdb1                                          8:17   0   18G  0 part
  └─luks-7853363d-e7e2-1a42-b5b9-0af119e19920 253:0    0   18G  0 crypt /home
sr0                                            11:0    1 1024M  0 rom
```

Добавить новый пароль на зашифрованный раздел (требуется предоставить уже имеющийся пароль интерактивно или посредством опции `--key-file`):

```
# cryptsetup luksAddKey /dev/sdb1
Введите любую существующую парольную фразу:
Введите новую парольную фразу для слота ключа:
Парольная фраза повторно:
```

Примечание. Пароль должен представлять собой смесь заглавных и строчных букв, цифр и других символов. Можно использовать пароль, содержащий не менее 7 символов из всех

этих классов, или пароль, содержащий не менее 8 символов только трех классов. При расчете количества классов символов, заглавные буквы, используемые в качестве первого символа и цифр, используемых в качестве последнего символа пароля, не учитываются. Настоятельно рекомендуется выбирать символы парольной фразы только из 7-битного ASCII.

Пароль будет назначен в первый свободный слот:

```
# cryptsetup luksDump /dev/sdb1 | grep Slot
Key Slot 0: ENABLED
Key Slot 1: ENABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

Можно указать номер определенного слота с помощью опции `--key-slot`, например:

```
# cryptsetup luksAddKey /dev/sdb1 --key-slot 5
```

Заменить один из паролей на другой (старый пароль нужно ввести интерактивно или задать опцией `--key-file`):

```
# cryptsetup luksChangeKey /dev/sdb1
Введите изменяемую парольную фразу:
Введите новую парольную фразу:
Парольная фраза повторно:
```

Если задан номер слота (опцией `--key-slot`), нужно ввести старый пароль именно для заданного слота, и замена пароля произойдёт тоже в этом слоте. Если номер слота не задан и есть свободный слот, то сначала новый пароль будет записан в свободный слот, а потом будет затёрт слот, содержащий старый пароль. Если свободных слотов не окажется, то новый пароль будет записан прямо в слот, ранее содержащий старый пароль.

Удалить заданный пароль (затирает слот):

```
# cryptsetup luksRemoveKey /dev/sdb1
Введите удаляемую парольную фразу:
```

Примечание. В пакетном режиме (`-q`) удаление даже последнего пароля будет выполнено без каких-либо предупреждений. Если ни одного пароля не останется (то есть все слоты ключей будут пусты), дешифровать LUKS-раздел станет невозможно.

Для сброса забытого пароля на зашифрованный раздел следует выполнить следующие действия:

1) получить зашифрованные пароли всех разделов:

```
# dmsetup table --showkey
luks-7853363d-e7e2-1a42-b5b9-0af119e19920: 0 37730304 crypt aes-cbc-
essiv:sha256 b15c22e8d60a37bcd27fb438637a8221f-
bec66c83be46d33a8331a4002cf3144 0 8:17 4096
```

Часть поля после «aes-cbc-essiv:sha256» является зашифрованным паролем.

Сохранить зашифрованный пароль в текстовый файл:

```
# echo "b15c22e8d60a37bcd27fb438637a8221f-
bec66c83be46d33a8331a4002cf3144" > lukskey.txt
```

2) преобразовать существующий пароль из текстового файла в двоичный файл:

```
# xxd -r -p lukskey.txt lukskey.bin
luks-7853363d-e7e2-1a42-b5b9-0af119e19920: 0 37730304 crypt aes-cbc-
essiv:sha256 b15c22e8d60a37bcd27fb438637a8221f-
bec66c83be46d33a8331a4002cf3144 0 8:17 4096
```

3) добавить новый пароль, используя существующий пароль, извлеченный в бинарный файл:

```
# cryptsetup luksAddKey /dev/sdb1 --master-key-file <(cat lukskey.bin)
Введите новую парольную фразу для слота ключа:
Парольная фраза повторно:
```

Примечание. Сбросить пароль на зашифрованный раздел можно, только если данный раздел уже примонтирован.

8.7 Поддержка файловых систем

Файловая система представляет собой набор правил, определяющих то, как хранятся и извлекаются документы, хранящиеся на устройстве.

В ОС «Альт Сервер» поддерживаются следующие файловые системы:

- ext2 – нежурналируемая файловая система; относительно проста в восстановлении, но нуждается в относительно долгой проверке целостности после сбоя питания или ядра. Может использоваться для /boot или readonly-разделов;
- ext3 – журналируемая и достаточно надёжная файловая система, имеет среднюю производительность;
- ext4 – журналируемая файловая система, логическое продолжение ext3, позволяет полностью отключить журналирование;
- btrfs – поддерживает снимки (копии файловой системы на определенный момент времени), сжатие и подтома;

- xfs – высокопроизводительная журналируемая файловая система, имеющая более высокую чувствительность к сбоям. Рекомендуется для активно используемых файловых систем при условии стабильного питания и качественной аппаратной части;
- jfs – журналируемая файловая система, имеющая поддержку перекодирования имён файлов (iocharset);
- iso9660 – файловая система ISO 9660 для дисков с данными компакт-дисков.

Файловые системы FAT/FAT32/NTFS поддерживаются в установленной системе, но не для установки на них Linux.

Проверка поддержки файловых систем ext2, ext3, ext4, iso9660, fat16, fat32, ntfs, xfs:

1) создать раздел объемом менее 4 Гбайт на flash-накопителе (например, `/dev/vdc1`).
2) для создания ISO-файла установить пакет `genisoimage`:

```
# apt-get install genisoimage
```

3) создать каталог `/mnt/filesystem`, в который будет монтироваться раздел:

```
# mkdir /mnt/filesystem
```

4) отформатировать раздел в проверяемую файловую систему:

- для ext2:

```
# mkfs.ext2 /dev/vdc1
```

- для ext3:

```
# mkfs.ext3 /dev/vdc1
```

- для ext4:

```
# mkfs.ext4 /dev/vdc1
```

- для fat16:

```
# mkfs.fat -F 16 /dev/vdc1
```

- для fat32:

```
# mkfs.fat -F 32 /dev/vdc1
```

- для ntfs:

```
# mkfs.ntfs /dev/vdc1
```

- для xfs:

```
# mkfs.xfs /dev/vdc1
```

- для iso9660 – создать ISO-файл из каталога `/etc`:

```
# mkisofs -r -jcharset koi8-r -o /root/cd.iso /etc
```

5) для проверки поддержки файловых систем ext2, ext3, ext4, fat16, fat32, ntfs:

- примонтировать раздел с файловой системой в каталог `/mnt/filesystem`:

```
# mount /dev/vdc1 /mnt/filesystem
```

- проверить возможность записи файла на текущую файловую систему:

```
# echo test_content > /mnt/filesystem/test.fs
```

- убедиться, что файл создан:

```
# ls -l /mnt/filesystem/test.fs
-rw-r--r--. 1 root root 13 май 23 20:10 /mnt/filesystem/test.fs
```

- проверить возможность чтения файла с текущей файловой системы:

```
# cat /mnt/filesystem/test.fs
```

6) для проверки поддержки файловой системы iso9660 смонтировать созданный ISO-файл в каталог /mnt/filesystem/ (файл образа диска будет примонтирован в режиме «только для чтения»):

```
# mount -o loop,ro /root/cd.iso /mnt/filesystem/
```

Примечание. Для просмотра файловых систем на физических дисках можно воспользоваться командой `df`:

```
$ df -Th | grep "^/dev"
```

или `lsblk`:

```
$ lsblk -f
```

Команда `fsck` позволяет узнать файловую систему раздела, который ещё не примонтирован:

```
# fsck -N /dev/sdc1
fsck из util-linux 2.39.2
[/sbin/fsck.xfs (1) -- /dev/sdc1] fsck.xfs /dev/sdc1
```

8.8 Поддержка сетевых протоколов

8.8.1 SMB

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

Настройка Samba описана в разделе «Samba в режиме файлового сервера».

8.8.2 NFS

8.8.2.1 Настройка сервера NFS

Установить пакет `nfs-server`:

```
# apt-get install nfs-server
```

Запустить NFS-сервер и включить его по умолчанию:

```
# systemctl enable --now nfs
```

В файле /etc/exports следует указать экспортируемые каталоги (каталоги, которые будет разрешено монтировать с других машин):

```
/mysharedir ipaddr1(rw)
```

Например, чтобы разрешить монтировать каталог /home на сервере необходимо добавить в /etc/exports строку:

```
/home 192.168.0.0/24(no_subtree_check,rw)
```

где 192.168.0.0/24 – разрешение экспорта для подсети 192.168.0.X;

rw – разрешены чтение и запись.

Подробную информацию о формате файла можно посмотреть, выполнив команду:

```
$ man exports
```

После внесения изменений в файл /etc/exports необходимо выполнить команду:

```
# exportfs -r
```

Проверить список экспортируемых файловых систем можно, выполнив команду:

```
# exportfs
/home 192.168.0.0/24
```

8.8.2.2 Использование NFS

Подключение к NFS-серверу можно производить как вручную, так и настроив автоматическое подключение при загрузке.

Для ручного монтирования необходимо:

- создать точку монтирования:

```
# mkdir /mnt/nfs
```

- примонтировать файловую систему:

```
# mount -t nfs 192.168.0.131:/home /mnt/nfs
```

где 192.168.0.131 – IP-адрес сервера NFS;

/mnt/nfs – локальный каталог, куда монтируется удалённый каталог;

- проверить наличие файлов в каталоге /mnt/nfs:

```
# ls -al /mnt/nfs
```

Должен отобразиться список файлов каталога /home, расположенного на сервере NFS.

Для автоматического монтирования к NFS-серверу при загрузке, необходимо добавить следующую строку в файл /etc/fstab:

```
192.168.0.131:/home  /mnt/nfs   nfs   intr,soft,nolock,_netdev,x-sys-
temd.automount    0 0
```

Примечание. Прежде чем изменять /etc/fstab, попробуйте смонтировать вручную и убедитесь, что всё работает.

8.8.3 FTP

8.8.3.1 Настройка сервера FTP

В состав ОС «Альт Сервер» входит `vsftpd` (Very Secure FTP Daemon) – полнофункциональный FTP-сервер, позволяющий обслуживать как анонимные запросы, так и запросы от пользователей, зарегистрированных на сервере и имеющих полноценный доступ к его ресурсам.

Примечание. Настроить FTP-сервер можно также в ЦУС (подробнее см. «FTP-сервер»).

Установить пакеты `vsftpd` и `anonftp`:

```
# apt-get install vsftpd anonftp
```

Изменить настройку прав доступа в файле `/etc/vsftpd.conf`:

```
local_enable=YES
chroot_local_user=YES
local_root=/var/ftp/
```

Запустить `vsftpd`:

```
# systemctl start vsftpd.socket
```

Убедиться в нормальной работе FTP-сервера

```
# netstat -ant | grep 21
tcp        0      0 :::21                   :::*
LISTEN
```

FTP-сервер запущен и принимает соединения на 21 порту.

Создать файл в каталоге `/var/ftp/`:

```
# echo "vsftpd test file" > /var/ftp/test.txt
```

8.8.3.2 Подключение рабочей станции

Создать подключение по протоколу FTP в графической среде MATE можно в файловом менеджере. Для этого следует указать в адресной строке протокол и адрес сервера (Рис. 369) и нажать клавишу <Enter>. В появившемся окне указать имя пользователя, пароль и нажать кнопку «Подключиться» (Рис. 370).

Создание подключения по протоколу FTP

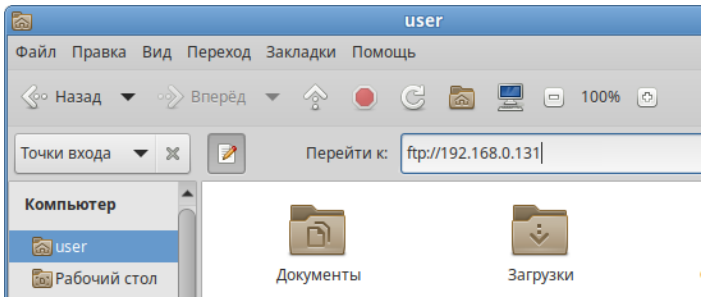


Рис. 369

Создание подключения по протоколу FTP

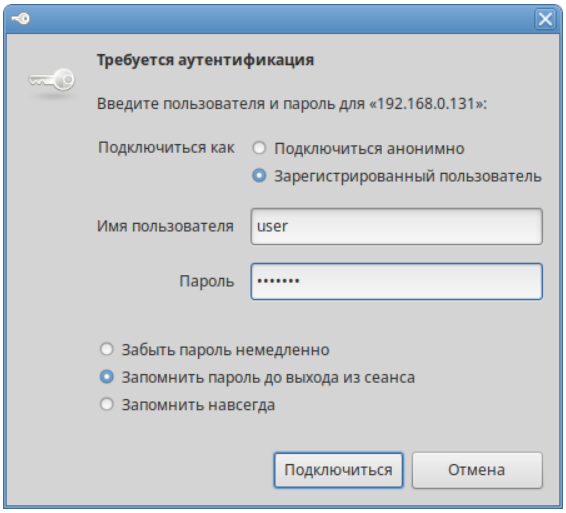


Рис. 370

Должен отобразиться список файлов каталога `/var/ftp/`, расположенного на сервере FTP (Рис. 371).

Файл на FTP-сервере

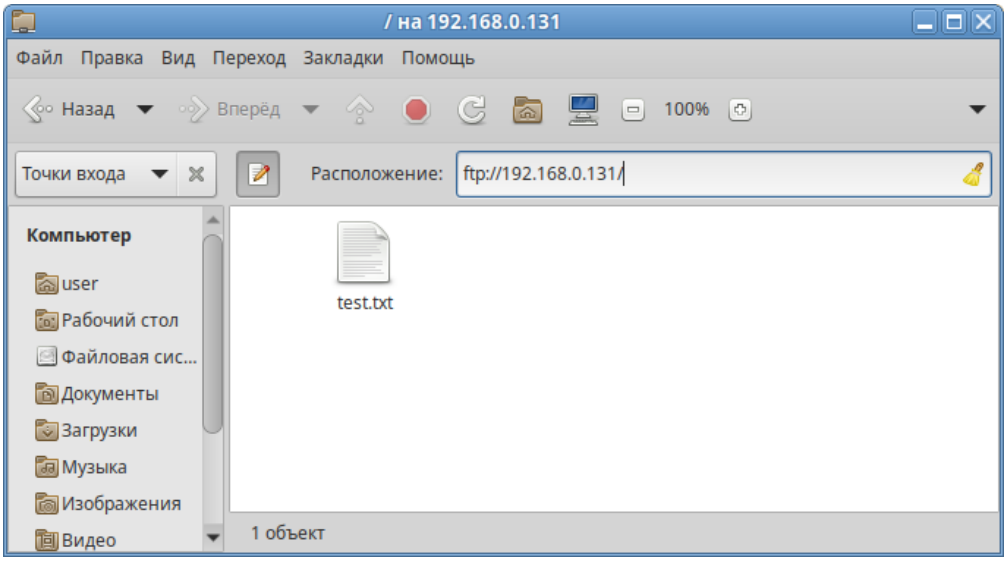


Рис. 371

8.8.4 NTP

8.8.4.1 Настройка сервера NTP

В качестве NTP сервера/клиента используется сервер времени chrony:

- chronyd – демон, работающий в фоновом режиме. Он получает информацию о разнице системных часов и часов внешнего сервера времени и корректирует локальное время. Демон реализует протокол NTP и может выступать в качестве клиента или сервера.

- chronyc – утилита командной строки для контроля и мониторинга программы. Утилита используется для тонкой настройки различных параметров демона, например, позволяет добавлять или удалять серверы времени.

Выполнить настройку NTP-сервера можно следующими способами:

- в ЦУС настроить модуль «Дата и время» на получение точного времени с NTP сервера и работу в качестве NTP-сервера и нажать кнопку «Применить» (Рис. 372).
- указать серверы NTP в директиве `server` или `pool` в файле конфигурации NTP `/etc/chrony.conf`:

```
allow all #Разрешить NTP-клиенту доступ из локальной сети
pool pool.ntp.org iburst
```

и перезапустить сервис командой:

```
# systemctl restart chronyd
```

Убедиться в нормальной работе NTP-сервера можно, выполнив команду:

```
# systemctl status chronyd.service
```

Настройка модуля «Дата и время»

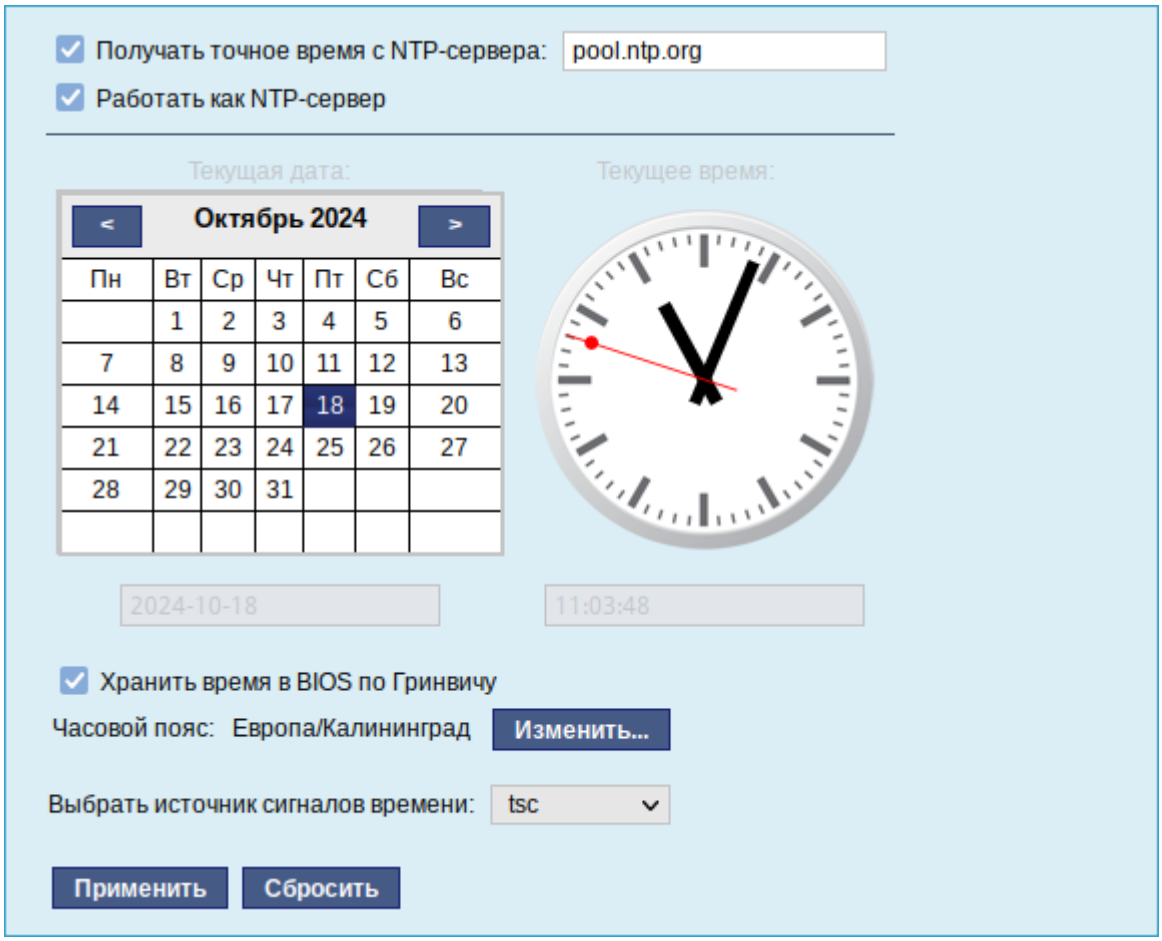


Рис. 372

8.8.4.2 Настройка рабочей станции

Настроить модуль «Дата и время» на получение точного времени с NTP-сервера (в качестве NTP-сервера указать IP-адрес сервера NTP) и нажать кнопку «Применить» (Рис. 373).

Настройка модуля «Дата и время» на рабочей станции

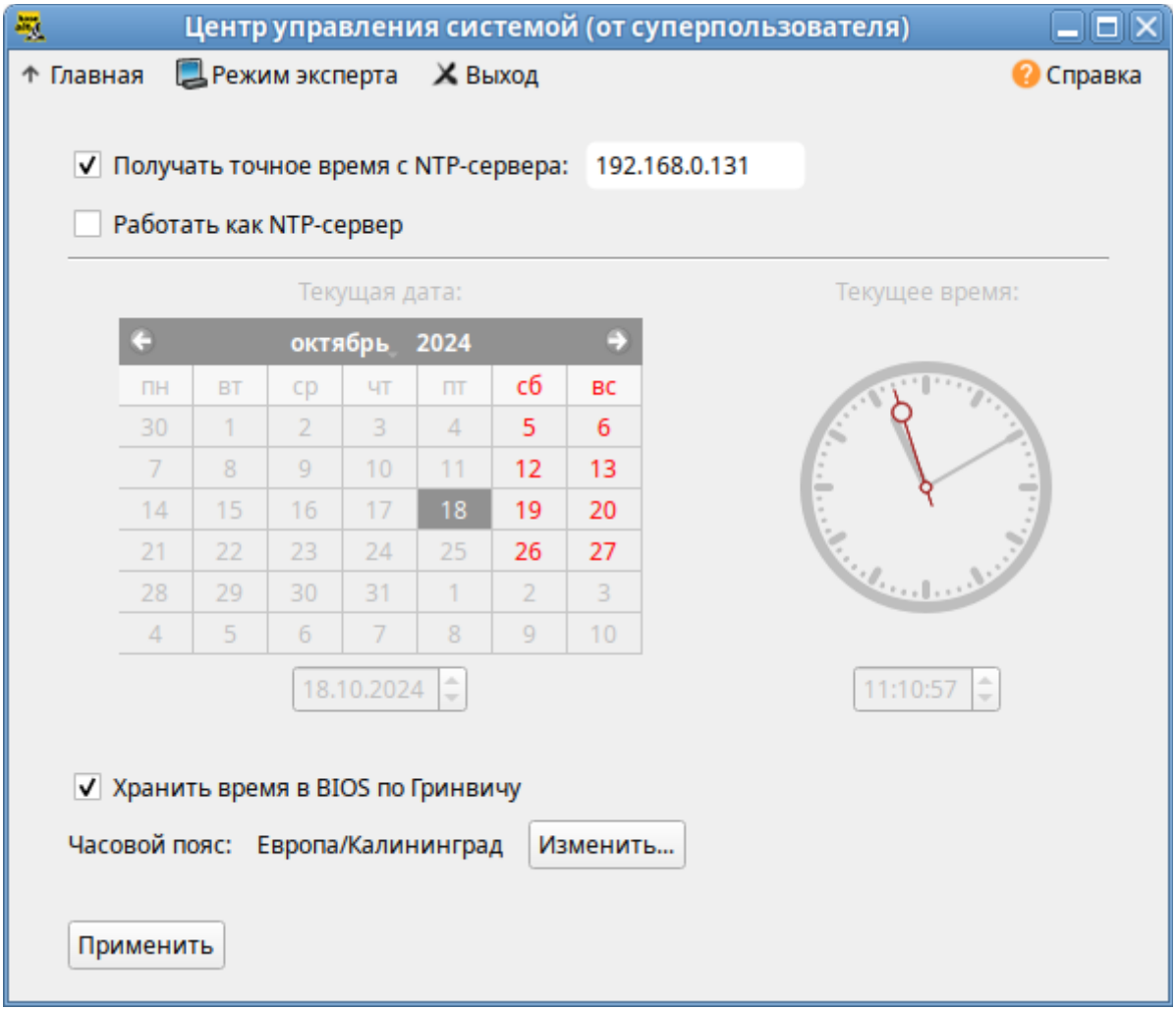


Рис. 373

Проверить текущие источники времени:

```
$ chronyc sources
MS Name/IP address   Stratum Poll Reach LastRx Last sample
===============================================================================
^? 192.168.0.131           0  10     0     -     +0ns[   +0ns] +/-    0n
```

Проверить статус источников NTP:

```
$ chronyc activity
200 OK
1 sources online
0 sources offline
0 sources doing burst (return to online)
```

```
0 sources doing burst (return to offline)
0 sources with unknown address
```

8.8.5 HTTP(S)

8.8.5.1 Настройка сервера HTTP

В состав ОС «Альт Сервер» входит как веб-сервер Apache, так и nginx. Пример настройки веб-сервера nginx см. в разделе «Настройка веб-сервера»). Ниже рассмотрен пример настройки веб-сервера Apache.

Установить пакет `apache2-base`:

```
# apt-get install apache2-base
```

Запустить httpd2:

```
# systemctl start httpd2
```

Убедиться, что служба httpd2 запущена:

```
# systemctl status httpd2
```

Создать стартовую страницу для веб-сервера:

```
# echo "Hello, World" >/var/www/html/index.html
```

8.8.5.2 Настройка рабочей станции

Запустить браузер, перейти по адресу `http://<IP-адрес>` (Рис. 374).

Обращение к серверу и получение данных по протоколу http

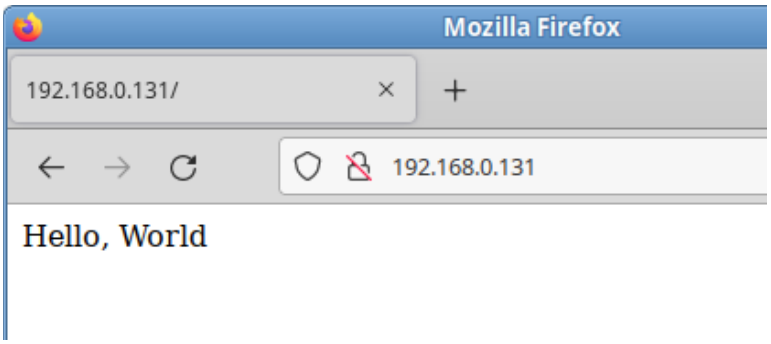


Рис. 374

Можно также выполнить команду:

```
$ curl http://192.168.0.131
Hello, World
```

Происходит обращение к серверу и получение данных по протоколу http.

8.9 Механизм аудита

Механизм аудита состоит из нескольких компонентов:

- модуль ядра – перехватывает системные вызовы (syscalls) и выполняет регистрацию событий;
- служба auditd – записывает зарегистрированное событие в файл;

- служба audispd – осуществляет пересылку сообщений (выступает в роли диспетчера) к другому приложению;
- ряд вспомогательных программ:
  - `auditctl` – программа, управляющая поведением системы аудита и позволяющая контролировать текущее состояние системы, создавать или удалять правила;
  - `aureport` – программа, генерирующая суммарные отчеты о работе системы аудита;
  - `ausearch` – программа, позволяющая производить поиск событий в журнальных файлах;
  - `autrace` – программа, выполняющая аудит событий, порождаемых указанным процессом.

Программы отсылают записи, предназначенные для журналирования, системному демону auditd, который идентифицирует тип каждой пришедшей записи и обрабатывает запись способом, определенным для данного типа.

Для каждого из регистрируемых событий в журналах указывается следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то указываются объект и тип доступа);
- успешность осуществления события (обслужен запрос на доступ или нет).

Конфигурация аудита хранится в файле `/etc/audit/auditd.conf`, правила аудита, загружаемые при запуске службы, хранятся в файле `/etc/audit/audit.rules`.

Для просмотра журналов используются команды `ausearch` и `aureport`. Команда `auditctl` позволяет настраивать правила аудита. Кроме того, при загрузке загружаются правила из файла `/etc/audit.rules`. Некоторые параметры самой службы можно изменить в файле `auditd.conf`.

8.9.1 Команда auditd

Служба auditd – это прикладной компонент системы аудита. Она ведёт журнал аудита на диске.

Синтаксис команды auditd:

```
auditd [-f] [-l] [-n] [-s disable|enable|nochange] [-c <config_file>]
```

Опции:

`-f` – не переходить в фоновый режим (для отладки). Сообщения программы будут направляться в стандартный вывод для ошибок (stderr), а не в файл;

`-l` – включить следование по символическим ссылкам при поиске конфигурационных файлов;

-n – не создавать дочерний процесс (для запуска из inittab или system);

-s=ENABLE_STATE – указать, должен ли auditd при старте изменять текущее значение флага ядра – enabled. Допустимые значения ENABLE_STATE: disable, enable и nochange. Значение по умолчанию enable (disable, когда auditd остановлен). Значение флага может быть изменено во время жизненного цикла auditd с помощью команды: auditctl -e;

-c – указать альтернативный каталог конфигурационного файла (по умолчанию: /etc/audit/). Этот же каталог будет передан диспетчеру.

Сигналы:

- SIGHUP – перезагрузить конфигурацию – загрузить файл конфигурации с диска. Если в файле не окажется синтаксических ошибок, внесённые в него изменения вступят в силу. При этом в журнал будет добавлена запись о событии DAEMON_CONFIG. В противном случае действия службы будут зависеть от параметров space_left_action, admin_space_left_action, disk_full_action, disk_error_action в файле auditd.conf;
- SIGTERM – прекратить обработку событий аудита и завершить работу, о чем предварительно занести запись в журнал;
- SIGUSR1 – произвести ротацию файлов журналов auditd. Создать новый файл журнала, перенумеровав старые файлы или удалив часть из них, в зависимости от параметра max_log_size_action;
- SIGUSR2 – попытаться возобновить ведение журналов auditd (необходимо после приостановки ведения журнала);
- SIGCONT – выгрузить отчёт о внутреннем состоянии auditd в /var/run/auditd.state.

Файлы:

- /etc/audit/auditd.conf – файл конфигурации службы аудита;
- /etc/audit/audit.rules – правила аудита (загружается при запуске службы);
- /etc/audit/rules.d/ – каталог, содержащий отдельные наборы правил, которые будут скомпилированы в один файл утилитой augenrules.

Для того чтобы сделать возможным аудит всех процессов, запущенных до службы аудита, необходимо добавить в строку параметров ядра (в конфигурации загрузчика) параметр audit=1. В противном случае аудит некоторых процессов будет невозможен.

Демон аудита может получать события – сообщения от других приложений через плагин `audispd`: `audisp-remote`. Демон аудита может быть связан с tcp_wrappers, чтобы контролировать, какие машины могут подключаться. В этом случае можно добавить запись в `hosts.allow` и отказать в соединении.

8.9.2 Файл конфигурации auditd.conf

В файле `/etc/audit/auditd.conf` определяются параметры службы аудита. Директива состоит из ключевого слова (названия параметра), знака равенства и соответствующих ему данных (значения параметра). На одной строке может быть не больше одной директивы. Все названия и значения параметров чувствительны к регистру. Допустимые ключевые слова перечислены в Таблица 6. Каждая строка должна быть ограничена 160 символами, иначе она будет пропущена. К файлу можно добавить комментарии, начав строку с символа «#».

Т а б л и ц а 6 – Описание ключевых слов файла конфигурации auditd.conf

Ключ	Значение
local_events	Ключевое слово yes/no указывающее, следует ли включать запись локальных событий (значение по умолчанию – yes). В случае если необходимо записывать только сообщения из сети, следует установить значение – no. Этот параметр полезен, если демон аудита работает в контейнере. Данный параметр может быть установлен только один раз при запуске аудита. Перезагрузка файла конфигурации никак на него не влияет.
log_file	Полное имя файла, в который следует записывать журнал.
write_logs	Ключевое слово yes/no, указывающее следует ли записывать журналы (значение по умолчанию – yes).
log_format	Оформление данных в журнале. Допустимы два значения: raw и enriched. При указании RAW, данные будут записываться в том виде, в котором они получаются от ядра. Значение ENRICHED разрешает информацию (вместо идентификатора, будет указано значение): идентификатор пользователя (uid), идентификатор группы (gid), системный вызов (syscall), архитектуру и адрес сокета перед записью события на диск. Это помогает осмыслить события, созданные в одной системе, но сообщенные/проанализированные в другой системе. Значение NOLOG устарело, вместо него следует установить параметр write_logs в значение no.
log_group	Указывает группу, на которую распространяются права на файлы журнала (по умолчанию – root). Можно использовать либо идентификатор, либо имя группы.
priority_boost	Неотрицательное число, определяющее повышение приоритета выполнения службы аудита. Значение по умолчанию – 4. Для того чтобы не изменять приоритет, следует указать – 0.

Ключ	Значение
flush	Стратегия работы с дисковым буфером. Допустимые значения: - none – отключить какие-либо дополнительные действия со стороны службы по синхронизации буфера с диском; - incremental – выполнять запросы на перенос данных из буфера на диск с частотой, задаваемой параметром freq; - incremental_async – тоже, что и incremental, за исключением того, что перенос данных выполняется асинхронно для более высокой производительности; - data – немедленно синхронизировать данные файла; - sync – немедленно синхронизировать как данные, так и метаданные файла при записи на диск. Значение по умолчанию – incremental_async.
freq	Максимальное число записей журнала, которые могут храниться в буфере. При достижении этого числа производится запись буферизованных данных на диск. Данный параметр допустим только в том случае, когда flush имеет значение incremental или incremental_async.
num_logs	Максимальное количество файлов с журналами. Используется в том случае, если параметр max_log_file_action имеет значение rotate. Если указано число меньше двух, при достижении ограничения на размер файла он обнуляется. Значение параметра не должно превышать 999. Значение по умолчанию – 0 (то есть ротация фалов не происходит). При указании большого числа может потребоваться увеличить ограничение на количество ожидающих запросов (в файле /etc/audit/audit.rules). Если настроена ротация журналов, демон проверяет наличие лишних журналов и удаляет их, чтобы освободить место на диске. Проверка выполняется только при запуске и при проверке изменения конфигурации.
name_format	Контролирует, как имена узлов компьютеров вставляются в поток событий аудита. Допустимые значения: - none – имя компьютера не используется в записи аудита; - hostname – имя, возвращаемое системным вызовом gethostname; - fqd – что аудит принимает имя хоста и разрешает его с помощью DNS в полное доменное имя этой машины; - numeric – схоже с fqd, за исключением того, что разрешается IP-адрес машины. Чтобы использовать эту опцию, нужно убедиться, что команда `hostname -i` или `domainname -i` возвращает числовой адрес. Кроме того, эта опция не рекомендуется, если используется DHCP, поскольку у одной и той же машины в разное время могут быть разные адреса; - user – строка, определенная администратором в параметре name. Значение по умолчанию – none.
name	Строка, определенная администратором, которая идентифицирует компьютер, если в параметре name_format указано значение user.
max_log_file	Ограничение на размер файла журнала в мегабайтах. Действие, выполняемое при достижении размера файла указанного значения, можно настроить с помощью параметра max_log_file_action.
max_log_file_action	Действие, предпринимаемое при достижении размером файла журнала максимального значения. Допустимые значения: - ignore – отключить контроль над размером файла; - syslog – добавить соответствующую запись в системный журнал; - suspend – прекратить вести журнал на диске (служба аудита будет продолжать работать); - rotate – произвести ротацию журналов, с удалением самых старых, чтобы

Ключ	Значение
	освободить место на диске. Текущий файл будет переименован и будет созан новый файл. Имя предыдущего файла журнала будет дополнено числом 1, а номера других журналов (если они имеются) будут увеличены на единицу. Таким образом, чем больше номер у журнала, тем он старше. Максимальное число файлов определяется параметром num_logs (соответствие ему достигается за счет удаления самых старых журналов). Такое поведение аналогично поведению утилиты `logrotate`; - keep_logs – аналогично rotate, но число файлов не ограничено, это предотвращает потерю данных аудита. Журналы накапливаются и не удаляются, что может вызвать событие space_left_action, если весь объём заполнится. Это значение следует использовать в сочетании с внешним сценарием, который будет периодически архивировать журналы.
verify_email	Определяет, проверяется ли адрес электронной почты, указанный в параметре action_mail_acct, на предмет возможности разрешения доменного имени. Этот параметр должен быть указан до параметра action_mail_acct, иначе будет использовано значение по молчанию – yes.
action_mail_acct	Адрес электронной почты. Значение по умолчанию – root. Если адрес не локальный по отношению к данной системе, необходимо чтобы в ней был настроен механизм отправки почты. В частности, требуется наличие команды `/usr/lib/sendmail`.
space_left	Минимум свободного пространства в мегабайтах, при достижении которого должно выполняться действие, определяемое параметром space_left_action.
space_left_action	Действие, предпринимаемое при достижении объемом свободного пространства на диске указанного минимума. Допустимые значения: - ignore – не производить никаких действий; - syslog – добавить соответствующую запись в системный журнал; - rotate – произвести ротацию журналов, с удалением самых старых, чтобы освободить место на диске; - email – отправить уведомление по адресу, указанному в action_mail_acct; - exec – запустить программу по указанному пути (передача параметров не поддерживается); - suspend – прекратить вести журнал на диске (служба аудита будет продолжать работать); - single – перевести компьютер в однопользовательский режим; - halt – выключить компьютер.
admin_space_left	Критический минимум свободного пространства в мегабайтах, при достижении которого должно выполняться действие, определяемое параметром admin_space_left_action. Данное действие следует рассматривать как последнюю меру, предпринимаемую перед тем, как закончится место на диске. Значение настоящего параметра должно быть меньше значения space_left.
admin_space_left_action	Действие, предпринимаемое при достижении объёмом свободного пространства на диске указанного критического минимума. Допустимые значения – ignore, syslog, exec, suspend, single и halt. Описание данных значений см. в описании параметра space_left_action.
disk_full_action	Действие, предпринимаемое при обнаружении отсутствия свободного пространства на диске. Допустимые значения – ignore, syslog, exec, suspend, single и halt. Описание данных значений см. в описании параметра space_left_action.
disk_error_action	Действие, предпринимаемое при возникновении ошибки в работе с диском. Допустимые значения – ignore, syslog, exec, suspend, single и halt. Описание данных значений см. в описании параметра space_left_action.
tcp_listen_port	Числовое значение в диапазоне 1..65535, при указании которого служба аудита будет прослушивать соответствующий TCP-порт для аудита удаленных систем. Демон аудита может быть связан с tcp_wrappers, чтобы контролировать, какие

Ключ	Значение
	машины могут подключаться. В этом случае можно добавить запись в hosts.allow и отказать в соединении. Если решение развернуто в ОС на основе systemd может потребоваться изменить параметр After.
tcp_listen_queue	Количество разрешенных ожидающих подключений (запрошенных, но не принятых). Значение по умолчанию – 5. Установка слишком маленького значения может привести к отклонению соединений, при одновременном запуске нескольких хостов (например, после сбоя питания).
tcp_max_per_addr	Количество одновременных подключений с одного IP-адреса. Значение по умолчанию – 1, максимальное значение – 1024. Установка слишком большого значения может привести к атаке типа «отказ в обслуживании» при ведении журнала сервером. Значение по умолчанию подходит в большинстве случаев.
use_libwrap	Следует ли использовать tcp_wrappers для распознавания попыток подключения с разрешенных компьютеров. Допустимые значения yes или no. Значение по умолчанию – yes.
tcp_client_ports	Порты, с которых можно принимать соединение. Значением параметра может быть либо число, либо два числа, разделенные тире (пробелы не допускаются). Если порт не указан, соединения принимаются с любого порта. Допустимые значения 1..65535. Например, для указания клиенту использовать привилегированный порт, следует указать значение 1-1023 для этого параметра, а также установить опцию local_port в файле audisp-remote.conf. Проверка того, что клиенты отправляют сообщения с привилегированного порта, это функция безопасности, предотвращающая атаки с использованием инъекций.
tcp_client_max_idle	Количество секунд, в течение которых клиент может бездействовать (то есть, какое время от него нет никаких данных). Используется для закрытия неактивных соединений, если на компьютере клиенте возникла проблема, из-за которой он не может завершить соединение корректно. Это глобальный параметр, его значение должно быть больше (желательно, в два раза), чем любой параметр клиента heartbeat_timeout. Значение по умолчанию – 0, что отключает эту проверку.
transport	Если установлено значение TCP, будут использоваться только TCP-соединения в виде открытого текста. Если установлено значение KRB5, для аутентификации и шифрования будет использоваться Kerberos 5. Значение по умолчанию – TCP.
enable_krb5	При значении yes – использовать Kerberos 5 для аутентификации и шифрования. Значение по умолчанию – no.
krb5_principal	Принципал для этого сервера. Значение по умолчанию – auditd. При значении по умолчанию, сервер будет искать ключ с именем типа auditd/hostname@EXAMPLE.COM в /etc/audit/audit.key для аутентификации себя, где hostname – имя сервера, возвращаемое запросом DNS-имени по его IP-адресу.
krb5_key_file	Расположение ключа для принципала этого клиента. Файл ключа должен принадлежать пользователю root и иметь права 0400. По умолчанию – файл /etc/audit/audit.key.
distribute_network	При значении yes, события, поступающие из сети, будут передаваться диспетчеру аудита для обработки. Значение по умолчанию – no.
q_depth	Числовое значение, указывающее, насколько большой должна быть внутренняя очередь диспетчера событий аудита. Очередь большего размера позволяет лучше обрабатывать поток событий, но может содержать события, которые не обрабатываются при завершении работы демона. Если вы получаете сообщения в системном журнале об удалении событий, увеличьте это значение. Значение по умолчанию – 2000.
overflow_action	Определяет, как демон должен реагировать на переполнение своей внутренней очереди. Когда это происходит, это означает, что принимается больше событий, чем можно передать дочерним процессам. Эта ошибка означает, что текущее

Ключ	Значение
	событие, которое он пытается отправить, будет потеряно. Допустимые значения: - ignore – не производить никаких действий; - syslog – добавить соответствующую запись в системный журнал; - suspend – прекратить отправку событий дочерним процессам (служба аудита будет продолжать работать); - single – перевести компьютер в однопользовательский режим; - halt – выключить компьютер.
max_restarts.	Неотрицательное число, которое сообщает диспетчеру событий аудита, сколько раз он может попытаться перезапустить вышедший из строя плагин. По умолчанию – 10.
plugin_dir	Место, где auditd будет искать файлы конфигурации своего плагина.
end_of_event_timeout	Неотрицательное количество секунд, используемое библиотечными процедурами пользовательского пространства auparse() и утилитами aureport(8), ausearch(8) для того, чтобы считать событие завершенным при анализе потока журнала событий. Если для обрабатываемого потока событий время текущего события превышает end_of_event_timeout секунд по сравнению с совмещенными событиями, то событие считается завершенным.

Примечание. Для файла `/var/log/audit` рекомендуется выделять специальный раздел. Кроме того, параметру flush необходимо присвоить значение `sync` или `data`.

Параметры `max_log_file` и `num_logs` необходимо настроить так, чтобы была возможность полностью использовать раздел. Следует учитывать, что чем больше файлов необходимо ротировать, тем больше времени потребуется, чтобы вернуться к получению событий аудита. Параметру `max_log_file_action` рекомендуется присвоить значение `keep_logs`.

Для параметра `space_left` должно быть установлено такое значение, которое даст администратору достаточно времени, чтобы отреагировать на предупреждение и освободить дисковое пространство. Обычно это предполагает запуск команды `aureport -t` и архивирование самых старых журналов. Значение параметра `space_left` зависит от системы, в частности от частоты поступления сообщений о событиях. Параметр `space_left_action` рекомендуется установить в значение `email`. Если требуется отправка сообщения snmp trap, нужно указать вариант `exec`.

Для параметра `admin_space_left` должно быть установлено такое значение, чтобы хватило свободного места для хранения записей о действиях администратора. Значение параметра `admin_space_left_action` следует установить в `single`, ограничив, таким образом, способ взаимодействия с системой консолью.

Действие, указанное в `disk_full_action`, выполняется, когда в разделе уже не осталось свободного места. Доступ к ресурсам машины должен быть полностью прекращен, так как больше

нет возможности контролировать работу системы. Это можно сделать, указав значение `single` или `halt`.

Значение параметра `disk_error_action` следует установить в `syslog`, `single`, либо `halt` в зависимости от соглашения относительно обработки сбоев аппаратного обеспечения.

Указание единственного разрешённого клиентского порта может затруднить перезапуск подсистемы аудита у клиента, так как он не сможет восстановить соединение с теми же адресами и портами хоста, пока не истечет таймаут закрытия соединения TIME_WAIT.

8.9.3 Команда auditctl

Команда `auditctl` используется для настройки параметров ядра, связанных с аудитом, получения состояния и добавления/удаления правил аудита.

Синтаксис команды `auditctl`:

```
auditctl [опции]
```

Опции команды auditctl представлены в таблицах 5 – 7.

Т а б л и ц а 7 – Опции конфигурации команды auditctl

Опция	Описание
-b <количество>	Установить максимальное количество доступных для аудита буферов, ожидающих обработки (значение в ядре по умолчанию – 64). В случае если все буферы заняты, то ядром будет выставлен флаг сбоя.
--backlog_wait_time <время_ожидания>	Установить время ожидания для ядра достижения значения backlog_limit (значение в ядре по умолчанию – 60*HZ), прежде, чем ставить в очередь дополнительные события аудита для их передачи аудиту. Число должно быть больше или равно нулю, но меньше, чем десятикратное значение по умолчанию.
--reset_backlog_wait_time_actual	Сбросить счетчик фактического времени ожидания невыполненной работы, показанный командой состояния.
-c	Продолжать загружать правила, несмотря на ошибку. Суммирует результат загрузки правил. Код завершения будет ошибочным, если какое-либо правило не будет загружено.
-D	Удалить все правила и точки наблюдения. Может также принимать параметр -k.
-e [0..2]	Установить флаг блокировки: 0 – отключить аудит, 1 – включить аудит, 2 – защитить конфигурацию аудита от изменений. Для использования данной возможности необходимо внести данную команду последней строкой в файл audit.rules. После её выполнения все попытки изменить конфигурацию будут отвергнуты с уведомлением в журналах аудита (чтобы задействовать новую конфигурацию аудита, необходимо перезагрузить систему).
-f [0..2]	Установить способ обработки для флага сбоя: 0=silent, 1=printk, 2=panic. Позволяет определить, каким образом ядро будет обрабатывать критические ошибки. Например, флаг сбоя выставляется при следующих условиях: ошибки передачи в пространство службы аудита, превышение лимита буферов, ожидающих обработки, выход за пределы памяти ядра, превышение лимита скорости выдачи сообщений (значение, установленное по умолчанию – 1, для систем с повышенными требованиями к безопасности, значение 2 может быть более предпочтительно).
-h	Краткая помощь по аргументам командной строки.

Опция	Описание
-i	Игнорировать ошибки при чтении правил из файла.
--loginuid-immutable	Сделать login UID неизменяемым сразу после его установки. Для изменения login UID требуется CAP_AUDIT_CONTROL, поэтому непривилегированный пользователь не может его изменить. Установка этого параметра может вызвать проблемы в некоторых контейнерах.
-q точка-<монтирования,поддерево>	При наличии точки наблюдения за каталогом и объединении или перемещении монтирования другого поддерева в наблюдаемое поддерево, необходимо указать ядру, сделать монтируемое поддерево эквивалентным просматриваемому каталогу. Если поддерево уже смонтировано во время создания точки наблюдения за каталогом, поддерево автоматически помечается для просмотра. Эти два значения разделяет запятая, отсутствие запятой приведет к ошибке.
-r <частота>	Установить ограничение скорости выдачи сообщений в секунду (0 – нет ограничения). В случае если эта частота не нулевая, и она превышается в ходе аудита, флаг сбоя выставляется ядром для выполнения соответствующего действия. Значение, установленное по умолчанию – 0.
--reset-lost	Сбросить счетчик потерянных записей, отображаемых командой статуса.
-R <файл>	Читать правила из файла. Правила должны быть организованы следующим образом: располагаться по одному в строке и в том порядке, в каком должны исполняться. Накладываются следующие ограничения: владельцем файла должен быть root, и доступ на чтение должен быть только у него. Файл может содержать комментарии, начинающиеся с символа «#». Правила, расположенные в файле, идентичны тем, что набираются в командной строке, без указания слова auditctl.
-t	Обрезать поддеревья после команды монтирования.

Т а б л и ц а 8 – Опции состояния команды auditctl

Опция	Описание
-l	Вывести список всех правил по одному правилу в строке. Этой команде могут быть предоставлены две опции: ключ фильтрации (-k), чтобы вывести список правил, соответствующих ключу, либо опция (-i) интерпретирующая значения полей от a0 до a3, для корректного определения значений аргументов системных вызовов.
-m <текст>	Послать в систему аудита пользовательское сообщение. Команда может быть выполнена только из-под учетной записи root.
-s	Получить статус аудита. Будут показаны значения, которые можно установить с помощью опций -e, -f, -r и -b. Значение pid – это номер процесса службы аудита. Значение pid 0 указывает, что служба аудита не работает. Поле lost сообщает, сколько записей событий аудита было отброшено из-за переполнения буфера аудита. Поле backlog сообщает, сколько записей событий аудита находится в очереди, ожидая, когда auditd прочитает их. С этим параметром можно использовать опцию -i для интерпретации значений некоторых полей.
-v	Вывести версию auditctl.

Опция	Описание

Т а б л и ц а 9 – Опции правил команды auditctl

Опция	Описание
-a <список,действие| действие,список>	Добавить правило с указанным действием к концу списка. Необходимо учитывать, что значения «список» и «действия» разделены запятой, и её отсутствие вызовет ошибку. Поля могут быть указаны в любом порядке.
-A <список,действие>	Добавить правило с указанным действием в начало списка.
-C <f=f | f!=f>	Создать правило сравнения между полями. Можно передавать несколько сравнений в одной командной строке. Каждое из них должно начинаться с -C. Каждое правило сравнения добавляется друг к другу, а также к правилам, начинающимся с -F для инициирования записи аудита. Поддерживаются два оператора – равно и не равно. Допустимые поля: auid, uid, euid, suid, fsuid, obj_uid; и gid, egid, sgid, fsgid, obj_gid. Две группы uid и gid не могут быть смешаны. Внутри группы может быть сделано любое сравнение.
-d <список,действие>	Удалить правило с указанным действием из списка. Правило удаляется только в том случае, если полностью совпали и имя системного вызова и поля сравнения.
-D	Удалить все правила и точки наблюдения. Может также принимать параметр -k.
-F <n=v | n!=v | n<v | n>v | n<=v | n>=v | n&v | n&=v>	Задать поле сравнения для правила. Атрибуты поля следующие: объект, операция, значение. Возможные объекты поля сравнения показаны в . В одной команде допускается задавать до шестидесяти четырех полей сравнения. Каждое новое поле должно начинаться с -F. Аудит будет генерировать запись, если произошло совпадение по всем полям сравнения. Допустимо использование одного из следующих восьми операторов: равно, не равно, меньше, больше, меньше либо равно, больше либо равно, битовая маска (n&v) и битовая проверка (n&=v). Битовая проверка выполняет операцию «and» над значениями и проверяет, равны ли они. Битовая маска просто выполняет операцию «and». Поля, оперирующие с идентификатором пользователя, могут также работать с именем пользователя – программа автоматически получит идентификатор пользователя из его имени. То же самое можно сказать и про имя группы.
-k <ключ>	Установить на правило ключ фильтрации. Ключ фильтрации – это произвольная текстовая строка длиной не больше 31 символа. Ключ помогает уникально идентифицировать записи, генерируемые в ходе аудита за точкой наблюдения. Поиск значения ключа можно выполнить с помощью команды ausearch. Ключ также можно использовать для удаления всех правил (-D), или правил с определенным ключом (-l). В правиле можно использовать несколько ключей.
-p <r|w|x|a>	Установить фильтр прав доступа для точки наблюдения: r=чтение, w=запись, x=исполнение, a=изменение атрибута. Эти разрешения не являются стандартными разрешениями для файлов, а представляют собой своего рода системный вызов, который может делать подобные вещи (системные вызовы «read» и «write» не включены в этот набор, поскольку логи аудита были бы перегружены информацией о работе этих вызовов).
-S <имя или номер системного вызова|all>	В случае если какой-либо процесс выполняет указанный системный вы-

Опция	Описание
	зов, то аудит генерирует соответствующую запись. В случае если значения полей сравнения заданы, а системный вызов не указан, правило будет применяться ко всем системным вызовам. В одном правиле может быть задано несколько системных вызовов – это положительно сказывается на производительности, поскольку заменяет обработку нескольких правил. Следует указывать по два правила: одно для 32-битной архитектуры, другое для 64-битной, чтобы убедиться, что ядро находит все ожидаемые события.
-w <путь>	Добавить точку наблюдения за файловым объектом, находящимся по указанному пути. Добавление точки наблюдения к каталогу верхнего уровня запрещено ядром. Групповые символы (wildcards) также не могут быть использованы, попытки их использования будут генерировать предупреждающее сообщение. Внутренне точки наблюдения реализованы как слежение за inode. Установка точки наблюдения за файлом аналогична использованию параметра path в правиле системного вызова -F. Установка точки наблюдения за каталогом аналогична использованию параметра dir в правиле системного вызова -F. Единственными допустимыми параметрами при использовании точек наблюдения являются -p и -k.
-W <путь>	Удалить точку наблюдения за файловым объектом.

Т а б л и ц а 10 – Объекты поля сравнения

Объект	Описание
a0, a1, a2, a3	Четыре первых аргумента, переданных системному вызову. Строковые аргументы не поддерживаются. Это связано с тем, что ядро должно получать указатель на строку, а проверка поля по значению адреса указателя не желательна. Таким образом, необходимо использовать только цифровые значения.
arch	Архитектура процессора, на котором выполняется системный вызов. Для определения архитектуры необходимо использовать команду uname -m. Можно написать правила, которые в некоторой степени не зависят от архитектуры, потому что тип будет определяться автоматически. Однако системные вызовы могут зависеть от архитектуры, и то, что доступно на x86_64, может быть недоступно на PPC. Опция arch должна предшествовать опции -S, чтобы auditctl знал, какую внутреннюю таблицу использовать для поиска номеров системных вызовов.
auid	Идентификатор пользователя, использованный для входа в систему. Можно использовать либо имя пользователя, либо идентификатор пользователя.
devmajor	Главный номер устройства (Device Major Number).
devminor	Вспомогательный номер устройства (Device Minor Number).
dir	Полный путь к каталогу для создания точки наблюдения. Помещает точку наблюдения в каталог и рекурсивно во всё его поддерево. Можно использовать только в списке exit.
egid	Действительный идентификатор группы.
euid	Действительный идентификатор пользователя.
exe	Абсолютный путь к приложению, к которому будет применяться это правило. Можно использовать только в списке exit.
exit	Значение, возвращаемое системным вызовом при выходе.
fsgid	Идентификатор группы, применяемый к файловой системе.
fsuid	Идентификатор пользователя, применяемый к файловой системе.
filetype	Тип целевого файла: файл, каталог, сокет, ссылка, символ, блок или FIFO.
gid	Идентификатор группы.
inode	Номер inode.

Объект	Описание
key	Альтернативный способ установить ключ фильтрации.
msgtype	Используется для проверки совпадения с числом, описывающим тип сообщения. Может использоваться только в списках exclude и user.
obj_uid	UID объекта.
obj_gid	GID объекта.
path	Полный путь к файлу для точки наблюдения. Может использоваться только в списке exit.
perm	Фильтр прав доступа для файловых операций. Может использоваться только в списке exit. Можно использовать без указания системного вызова, при этом ядро выберет системные вызовы, которые удовлетворяют запрашиваемым разрешениям.
pers	Персональный номер операционной системы.
pid	Идентификатор процесса.
ppid	Идентификатор родительского процесса.
sessionid	Идентификатор сеанса пользователя.
sgid	Установленный идентификатор группы.
success	Если значение, возвращаемое системным вызовом, больше либо равно 0, данный объект будет равен true/yes, иначе false/no. При создании правила нужно использовать 1 вместо true/yes и 0 вместо false/no.
suid	Установленный идентификатор пользователя.
uid	Идентификатор пользователя.

8.9.4 Команда aureport

Команда `aureport` генерирует итоговые отчёты на основе логов службы аудита, также может принимать данные со стандартного ввода (stdin) до тех пор, пока на входе будут необработанные данные логов. Все отчёты, кроме основного итогового отчёта, содержат номера событий аудита. Используя их, можно получить полные данные о событии с помощью команды `ausearch -a <номер события>`. В случае, если в отчёте слишком много данных, можно задать время начала и время окончания для уточнения временного промежутка.

Отчёты, генерируемые `aureport`, могут быть использованы как исходный материал для получения развернутых отчётов.

Синтаксис команды `aureport`:

```
aureport [опции]
```

Опции команды aureport представлены в Таблица 11.

Т а б л и ц а 11 – Опции команды aureport

Опция	Описание
-au, --auth	Отчёт о попытках аутентификации.
-a, --avc	Отчёт о avc сообщениях.
--comm	Отчёт о выполнении команд.
-c, --config	Отчёт об изменениях конфигурации.
-cr, --crypto	Отчёт о событиях, связанных с кодированием.
-e, --event	Отчёт о событиях.
--escape <опция>	Экранировать вывод. Возможные значения: raw, tty, shell и shell_quote. Каждый

Опция	Описание
	режим включает в себя символы предыдущего режима и экранирует больше символов. То есть shell включает все символы, экранируемые tty, и добавляет новые. Значение по умолчанию – tty.
-f, --file	Отчёт о файлах и сокетах.
--failed	Для обработки в отчетах выбирать только неудачные события. По умолчанию показываются как удачные, так и неудачные события.
-h, --host	Отчёт о хостах.
-i, --interpret	Транслировать числовые значения в текстовые. Например, идентификатор пользователя будет транслирован в имя пользователя. Трансляция выполняется с использованием данных с той машины, где запущена команда aureport.
-if, --input <файл>| <каталог>	Использовать указанный файл или каталог вместо логов аудита. Это может быть полезно при анализе логов с другой машины или при анализе частично сохраненных логов.
--input-logs	Использовать местоположение файла журнала из auditd.conf как исходные данные для анализа. Применяется при использовании команды aureport в задании cron.
--integrity	Отчёт о событиях целостности.
-k , --key	Отчёт о ключевых словах в правилах.
-l, --login	Отчёт о попытках входа в систему.
-m, --mods	Отчёт об изменениях пользовательских учетных записей.
-n, --anomaly	Отчёт об аномальных событиях. Эти события включают переход сетевой карты в беспорядочный режим и ошибки сегментации.
--node <имя узла>	Отобразить в отчёте только события со строкой <имя узла>. По умолчанию включены все узлы. Допускается перечисление нескольких узлов.
-nc , --no-config	Не включать событие CONFIG_CHANGE. Это особенно полезно для ключевого отчета, поскольку правила аудита во многих случаях имеют ключевые метки. Использование этой опции избавляет от ложных срабатываний.
-p, --pid	Отчёт о процессах.
-r, --response	Отчёт о реакциях на аномальные события.
-s, --syscall	Отчёт о системных вызовах.
--success	Для обработки в отчетах выбирать только удачные события. По умолчанию показываются как удачные, так и неудачные события.
--summary	Генерировать итоговый отчет, который дает информацию только о количестве элементов в том или ином отчете. Такой режим есть не у всех отчётов.
-t, --log	Генерация отчетов о временных рамках каждого отчёта.
--tty	Отчёты о нажатых клавишах.
-te, --end <дата> <время>	Искать события, которые произошли раньше (или во время) указанной временной точки. Формат даты и времени зависит от региональных настроек. В случае если дата не указана, то подразумевается текущий день (today). В случае если не указано время, то подразумевается текущий момент (now).
-tm, --terminal <терминал>	Отчёт о терминалах.
--ts, --start <дата> <время>	Искать события, которые произошли после (или во время) указанной временной точки.
-u, --user	Отчёт о пользователях.
-v, --verbose	Вывести версию программы и выйти.
-x, --executable	Отчёт об исполняемых объектах.

Нотацию времени следует использовать в формате «24 часа», а не «AM/PM». Например, дата может быть задана как «10/24/2005», а время – как «18:00:00». Также допускается использовать следующие ключевые слова:

- now – сейчас;
- recent – десять минут назад;

- boot – время за секунду до того, когда система загружалась в последний раз;
- today – первая секунда после полуночи текущего дня;
- yesterday – первая секунда после полуночи предыдущего дня;
- this-week – первая секунда после полуночи первого дня текущей недели, первый день недели определяется из региональных настроек;
- week-ago – первая секунда после полуночи ровно 7 дней назад;
- this-month – первая секунда после полуночи первого числа текущего месяца;
- this-year – первая секунда после полуночи первого числа первого месяца текущего года.

8.9.5 Команда ausearch

Команда `ausearch` является инструментом поиска по журналу аудита. `ausearch` может также принимать данные со стандартного ввода (stdin) до тех пор, пока на входе будут необработанные данные логов. Все условия, указанные в параметрах, объединяются логическим «И».

Каждый системный вызов ядра из пользовательского пространства и возвращение данных в пользовательское пространство имеет один уникальный (для каждого системного вызова) идентификатор события.

Различные части ядра могут добавлять дополнительные записи. Например, в событие аудита для системного вызова «open» добавляется запись `PATH` с именем файла. `ausearch` показывает все записи события вместе. Это означает, что при запросе определенных записей результат может содержать записи `SYSCALL`.

Не все типы записей содержат указанную информацию. Например, запись `PATH` не содержит имя узла или `loginuid`.

Синтаксис команды `ausearch`:

```
ausearch [опции]
```

Опции команды ausearch показаны в Таблица 12.

Т а б л и ц а 12 – Опции команды ausearch

Опция	Описание
-a, --event <идентификатор события>	Искать события с заданным идентификатором. В сообщении: *msg=audit(1116360555.329:2401771)*, идентификатор события – число после «:». Все события аудита, связанные с одним системным вызовом, имеют одинаковый идентификатор.
--arch <CPU>	Искать события на основе определенной архитектуры процессора. Для определения архитектуры необходимо использовать команду `uname -m`. В случае, если архитектура ПЭВМ неизвестна, необходимо использовать таблицу 32-х битных системных вызовов, если она поддерживается ПЭВМ, можно использовать b32. Аналогичным образом применяется таблица системных вызовов b64.
-c, --comm <comm-name>	Искать события с заданным «comm name», именем исполняемого файла из структуры задачи.
--debug	Вывести сообщения, пропущенные stderr.

Опция	Описание
--checkpoint <файл контрольной точки>	Контрольная точка – это вывод между последовательными вызовами ausearch, так что в последующих вызовах будут выводиться только события, не попавшие в предыдущий вывод. Событие auditd состоит из одной или нескольких записей. При обработке события ausearch определяет события как завершенные и незавершенные. Завершенное событие – это одно событие записи или то, которое произошло раньше, чем за две секунды по сравнению с текущим обрабатываемым событием. Контрольная точка обеспечивается путем записи последнего завершенного события вывода вместе с номером устройства и индексом файла последнего завершившегося события в файл контрольной точки. При следующем вызове ausearch загрузит данные контрольной точки и при обработке файлов журнала, будет отбрасывать все завершенные события, пока они не соответствуют контрольной точке, в этот момент ausearch начнет выводить события.
-e, --exit <код>	Искать события на основе кода системного вызова exit или errno.
--escape <опция>	Экранировать вывод. Возможные значения: raw, tty, shell и shell_quote. Каждый режим включает в себя символы предыдущего режима и экранирует больше символов. То есть shell включает все символы, экранируемые tty, и добавляет новые. Значение по умолчанию – tty.
--extra-keys	Если параметр format имеет значение csv, вывести столбец с дополнительной информацией. Работает только с записями SYSCALL, которые были записаны в результате запуска правила аудита, определенного ключом.
--extra-labels	Если параметр format имеет значение csv, добавить информацию о метках субъекта и объекта (если метки существуют).
--extra-obj2	Если параметр format имеет значение csv, добавить информацию о втором объекте (если он существует). Второй объект иногда является частью записи, например, при переименовании файла или монтировании устройства.
--extra-time	Если параметр format имеет значение csv, добавить информацию о времени простоя.
-f, --file <файл>	Искать события с заданным именем файла.
--format <опции>	Отформатировать события, которые соответствуют критериям поиска. Поддерживаемые форматы: raw, default, interpret, csv и text. Значение raw описано в опции raw. При значении default строки выводятся без форматирования, в выводе используется одна строка в качестве визуального разделителя, далее указывается метка времени, а затем следуют записи события. Значение interpret объясняется в описании опции -i. При значении csv результат поиска выводится в формате CSV. Значение text преобразует вывод к формату предложений, что упрощает понимание вывода, но происходит это за счет потери деталей.
-ga, --gid-all all-<идентификатор группы>	Искать события с заданным эффективным или обычным идентификатором группы.
-ge, --gid-effective <эффективный идентификатор группы>	Искать события с заданным эффективным идентификатором группы или именем группы.
-gi, --gid <группа>	Искать события с заданным идентификатором группы или именем группы.
-h, --help	Справка
-hn, --host <имя узла>	Искать события с заданным именем узла. Имя узла может быть именем узла, полным доменным именем или цифровым сетевым адресом.
-i, --interpret	Транслировать числовые значения в текстовые. Например, идентификатор пользователя будет транслирован в имя пользователя. Трансляция выполняется с использованием данных с той машины, где запущена команда ausearch.
-if, --input <файл>|<ката-	Использовать указанный файл или каталог вместо логов аудита. Это может

Опция	Описание
лог>	быть полезно при анализе логов с другой машины или при анализе частично сохраненных логов.
--input-logs	Использовать местоположение файла журнала из auditd.conf как исходные данные для анализа. Применяется при использовании команды ausearch в задании cron.
--just-one	Остановиться после выдачи первого события, соответствующего критериям поиска.
-k, --key <ключевое слово>	Искать события с заданным ключевым словом.
-l, --line-buffered	Сбрасывать вывод после каждой строки.
-m, --message <тип>|<список типов>	Искать события с заданным типом, при этом можно указать список значений, разделенных запятыми. Можно указать несуществующий в событиях тип «ALL», который позволяет получить все сообщения системы аудита (список допустимых типов будет показан, если указать эту опцию без значения). Тип сообщения может быть строкой или числом. В списке значений этого параметра в качестве разделителя используются запятые и пробелы недопустимы.
-n , --node	Искать события с определенного узла. Допускается указание нескольких узлов (для вывода достаточно совпадение любого узла).
-p, --pid <идентификатор процесса>	Искать события с заданным идентификатором процесса.
-pp, --ppid <идентификатор процесса>	Искать события с заданным идентификатором родительского процесса.
-r, --raw	Необработанный вывод. Используется для извлечения записей для дальнейшего анализа.
-sc, --syscall <системный вызов>	Искать события с заданным системным вызовом. Можно указать номер или имя системного вызова. При указании имени системного вызова, оно будет проверено по таблице системных вызовов на машине, где запущена команда ausearch.
--session <идентификатор сеанса>	Искать события с заданным идентификатором сеанса. Этот атрибут устанавливается, когда пользователь входит в систему и может связать любой процесс с определенным именем пользователя.
-sv, --success <флаг>	Искать события с заданным флагом успешного выполнения. Допустимые значения: yes (успешно) и no (неудачно).
-te, --end <дата> <время>	Искать события, которые произошли раньше (или во время) указанной временной точки. Формат даты и времени зависит от региональных настроек. В случае если дата не указана, то подразумевается текущий день (today). В случае если не указано время, то подразумевается текущий момент (now).
--ts, --start <дата> <время>	Искать события, которые произошли после (или во время) указанной временной точки.
-tm, --terminal <терминал>	Искать события с заданным терминалом. Некоторые службы (такие как cron и atd) используют имя службы как имя терминала.
-ua, --uid-all <идентификатор пользователя>	Искать события, у которых любой из идентификатора пользователя, эффективного идентификатора пользователя или loginuid (auid) совпадают с заданным идентификатором пользователя.
-ue, --uid-effective <эффективный идентификатор пользователя>	Искать события с заданным эффективным идентификатором пользователя.
-ui, --uid <идентификатор пользователя>	Искать события с заданным идентификатором пользователя.
-ul, --loginuid <идентификатор пользователя>	Искать события с заданным идентификатором пользователя. Все программы, которые его используют, должны использовать pam_loginuid.
-uu, --uuid <идентификатор гостя>	Искать события с заданным идентификатором гостя.
-v, --verbose	Показать версию и выйти.

Опция	Описание
--vm, --vm-name <имя гостя>	Искать события с заданным именем гостя.
-x, --executable <программа>	Искать события с заданным именем исполняемой программы.

Нотацию времени следует использовать в формате «24 часа», а не «AM/PM». Например, дата может быть задана как «10/24/2005», а время – как «18:00:00». Допускается также использовать следующие ключевые слова:

- now – сейчас;
- recent – десять минут назад;
- boot – время за секунду до того, когда система загружалась в последний раз;
- today – первая секунда после полуночи текущего дня;
- yesterday – первая секунда после полуночи предыдущего дня;
- this-week – первая секунда после полуночи первого дня текущей недели, первый день недели определяется из региональных настроек;
- week-ago – первая секунда после полуночи ровно 7 дней назад;
- this-month – первая секунда после полуночи первого числа текущего месяца;
- this-year – первая секунда после полуночи первого числа первого месяца текущего года.

8.9.6 Команда autrace

Команда `autrace` добавляет правила аудита для того, чтобы следить за использованием системных вызовов в указанном процессе подобно тому, как это делает `strace`.

После добавления правил, команда `autrace` запускает процесс с указанными аргументами. Результаты аудита будут находиться либо в логах аудита (если служба аудита запущена), либо в системных логах. Команда `autrace` устроена так, что удаляет все предыдущие правила аудита, перед тем как запустить указанный процесс и после его завершения. Поэтому, в качестве дополнительной меры предосторожности, программа не запустится, если перед её использованием правила не будут удалены с помощью команды `audtictl` – об этом известит предупреждающее сообщение.

Синтаксис команды `autrace`:

```
autrace [-r] процесс [аргументы]
```

Опция `-r` позволяет ограничить сбор информации о системных вызовах только теми, которые необходимы для анализа использования ресурсов. Это может быть полезно при моделировании внештатных ситуаций и позволяет уменьшить нагрузку на журналы.

Примеры использования:

- обычное использование программы:

```
# autrace /bin/ls /tmp
```

```
# ausearch --start recent -p 2442 -i
```

- режим ограниченного сбора информации:

```
# autrace -r /bin/ls
# ausearch --start recent -p 2450 --raw | aureport --file --summary
# ausearch --start recent -p 2450 --raw | aureport --host –summary
```

8.9.7 Настройка ротации журналов аудита

Правила ротации журналов аудита настраиваются в файле `/etc/audit/auditd.conf`.

Например, для того чтобы при нехватке места на диске старые записи затирались новыми, необходимо внести следующие изменения в файл `/etc/audit/auditd.conf`:

```
max_log_file = 8
space_left = 100
space_left_action = ROTATE
```

где:

- `max_log_file` – максимальный размер файла журнала в Мбайт;
- `space_left` – минимум свободного пространства в Мбайт;
- `space_left_action` – действие (в данном случае старые файлы журналов будут удаляться, освобождая место для новых).

После внесения изменения в файл `/etc/audit/auditd.conf`, для того чтобы новые настройки вступили в силу, необходимо перезапустить `auditd`:

```
# /etc/init.d/auditd restart
```

8.9.8 Определение правил аудита

Система аудита работает на основе набора правил, определяющих, что должно фиксироваться в файлах журналов. Можно указать следующие типы правил аудита:

- правила конфигурации – правила, позволяющие изменить поведение системы аудита и некоторых её настроек;
- правила файловой системы – позволяют проверять доступ к определённому файлу или каталогу;
- правила системных вызовов – регистрируют системные вызовы, выполняемые указанной программой.

Правила аудита могут быть установлены:

- в командной строке с помощью утилиты `auditctl` (эти правила не сохраняются после перезагрузки системы);
- в файле `/etc/audit/audit.rules`.

8.9.8.1 Установка правил с помощью auditctl

Команда `auditctl` позволяет управлять основными функциями системы аудита и определять правила, определяющие, какие события аудита регистрируются.

Примечание. Все команды, которые взаимодействуют со службой аудита и файлами журнала аудита, требуют привилегий root.

Примеры правил изменения конфигурации:

- установить максимальное количество существующих буферов аудита в ядре:

```
# auditctl -b 256
```

- установить способ обработки для флага сбоя (действие, которое выполняется при обнаружении критической ошибки):

```
# auditctl -f 2
```

в данной конфигурации в случае критической ошибки будет вызван `kernel panic`;

- защитить конфигурацию аудита от изменений:

```
# auditctl -e 2
```

в результате все попытки изменить конфигурацию аудита будет отвергнуты:

```
The audit system is in immutable mode, no rule changes allowed
```

- вывести конфигурацию аудита:

```
# auditctl -s
```

- вывести список всех загруженных в данный момент правил аудита:

```
# auditctl -l
```

- удалить все загруженные в данный момент правила аудита:

```
# auditctl -D
```

Чтобы определить правило файловой системы, используется следующий синтаксис:

```
# auditctl -w путь_к_файлу -p разрешения -k имя_ключа
```

где:

- путь_к_файлу – файл или каталог, подлежащий аудиту;
- разрешения – разрешения, которые регистрируются:
  - r – доступ на чтение файла или каталога;
  - w – доступ на запись к файлу или каталогу;
  - x – доступ на исполнение к файлу или каталогу;
  - a – изменение атрибута файла или каталога;
- имя_ключа – необязательная строка, которая помогает определить, какое правило или набор правил создали конкретную запись в журнале.

Примеры правил файловой системы:

- записывать все попытки изменения файла `/etc/shadow`:

```
# auditctl -w /etc/shadow -p wa
```

- записывать все попытки изменения файлов в каталоге `/etc/httpd2/`:

```
# auditctl -w /etc/httpd2/ -p wa -k apache
```

- регистрировать выполнение команды `/sbin/modprobe`:

```
# auditctl -w /sbin/modprobe -p x -k modules
```

Для добавления правил системных вызовов используется следующая форма записи:

```
# auditctl -a список,действие -S имя_системного_вызова -F фильтры -k имя_ключа
```

Здесь список – это список событий, в который следует добавить правило. Доступные списки:

- `task` – добавить правило к списку, отвечающему за процессы. Этот список правил используется только во время создания процесса – когда родительский процесс вызывает fork() или clone(). При использовании этого списка можно использовать только те поля, которые известны во время создания процесса (uid, gid и так далее);
- `exit` – добавить правило к списку, отвечающему за точки выхода из системных вызовов. Этот список применяется, когда необходимо создать событие для аудита, привязанное к точкам выхода из системных вызовов;
- `user` – добавить правило, отвечающее за список фильтрации пользовательских сообщений. Этот список используется ядром, чтобы отфильтровать события, приходящие из пользовательского пространства, перед тем как они будут переданы службе аудита. Могут быть использованы только следующие поля: uid, auid, gid, pid, subj_user, subj_role, subj_type, subj_sen, subj_clr, и msgtype. Все остальные поля будут обработаны, как если бы они не совпали;
- `exclude` – добавить правило к списку, отвечающего за фильтрацию событий определенного типа. Этот список используется, чтобы отфильтровывать ненужные события. События могут быть исключены по идентификатору процесса, идентификатору пользователя, идентификатору группы, идентификатору логина пользователя, типу сообщения или контексту предмета.

Второй параметр опции `-a` – это действие, которое должно произойти в ответ на возникшее событие:

- `never` – аудит не будет генерировать никаких записей. Может использоваться для подавления генерации событий. Обычно необходимо подавлять генерацию сверху списка, а не снизу, поскольку событие инициируется на первом совпавшем правиле;

- always – установить контекст аудита. Всегда заполнять его во время входа в системный вызов, и всегда генерировать запись во время выхода из системного вызова.

Далее указывается опция -S, задающая имя системного вызова, при обращении к которому должен срабатывать триггер (например, open, close, exit). Вместо имени может быть использовано числовое значение.

Необязательная опция -F используется для указания дополнительных параметров фильтрации события.

Примеры правил системных вызовов:

- вести журнала событий, связанных с использованием системного вызова open(), и регистрировать при этом только обращения к файлам каталога /etc:

```
# auditctl -a always,exit -S open -F path=/etc/
```

- регистрировать только те события, при которых файл открывается только на запись и изменение атрибутов:

```
# auditctl -a always,exit -S open -F path=/etc/ -F perm=aw
```

- записывать все системные вызовы, используемые определенным процессом:

```
# auditctl -a always,exit -S all -F pid=1005
```

- записывать все файлы, открытые определенным пользователем:

```
# auditctl -a always,exit -S openat -F auid=510
```

- записывать неудачные попытки вызова системной функции openat:

```
# auditctl -a exit,always -S openat -F success!=0
```

- записывать попытки изменения файла /etc/shadow:

```
# auditctl -a always,exit -F path=/etc/shadow -F perm=wa
```

Чтобы определить правило для исполняемого файла, необходимо использовать следующий синтаксис:

```
# auditctl -a список,действие [ -F arch=cpu -S имя_системного_вызова] -F exe=путь_к_файлу -k имя_ключа
```

Например, правило для файла /usr/bin/ping:

```
# auditctl -a always,exit -F exe=/usr/bin/ping -F arch=b64 -S execve -k execution_ping
```

8.9.8.2 Установка постоянных правил в файле /etc/audit/audit.rules

Чтобы определить правила аудита, сохраняющиеся при перезагрузках, необходимо либо напрямую включить их в файл /etc/audit/audit.rules, либо использовать программу augenrules, которая считывает правила, расположенные в каталоге /etc/audit/rules.d/.

Скрипт augenrules считывает правила, расположенные в каталоге /etc/audit/rules.d/, и компилирует их в файл /etc/audit/audit.rules. Этот скрипт обрабатывает файлы *.rules, в определенном порядке, основанном на их естественном порядке сортировки.

Во время старта служба auditd читает файл /etc/audit/audit.rules, который содержит правила аудита в формате auditctl. Пустые строки и текст после знака решетки (#) игнорируются. В файл записываются правила без имени команды. Например:

```
-w /etc/passwd -p wa
```

Команду auditctl также можно использовать для чтения правил из указанного файла с помощью опции -R, например:

```
# auditctl -R /home/user/audit/rules/30-net.rules
```

Файл /etc/audit/audit.rules может содержать только следующие правила контроля, изменяющие поведение системы аудита: -b, -D, -e, -f, -r, --loginuid-immutable и --backlog_wait_time. Например:

```
# Удалить все предыдущие правила
-D
# Установить размер буфера
-b 8192
# Защитить конфигурацию аудита от изменений
-e 2
```

Правила файловой системы и системных вызовов определяются в файле /etc/audit/audit.rules с использованием синтаксиса auditctl. Например:

```
-w /etc/shadow -p wa
-w /sbin/modprobe -p x -k modules

-a always,exit -S openat -F auid=510
```

Чтобы загрузить правила из каталога /etc/audit/rules.d/ следует запустить команду augenrules с параметром --load:

```
# augenrules --load
```

Эти правила также будут загружены при запуске службы auditd.

8.9.8.3 Файлы журнала аудита

По умолчанию система аудита сохраняет записи журнала в файле /var/log/audit/audit.log.

Для примера создадим правило аудита, которое регистрирует каждую попытку чтения или изменения файла /etc/autofs.conf:

```
# auditctl -w /etc/autofs.conf -p warx -k autofs
```

Если служба auditd запущена, выполнение следующей команды создаст новое событие в файле журнала аудита:

```
$ cat /etc/autofs.conf
```

Событие в /var/log/audit/audit.log:

```
type=SYSCALL msg=audit(1699990009.349:368): arch=c000003e syscall=257
success=yes exit=3 a0=ffffff9c a1=7ffc39880600 a2=0 a3=0 items=1 ppid=5701
pid=8223 auid=501 uid=501 gid=501 euid=501 suid=501 fsuid=501 egid=501
sgid=501 fsgid=501 tty=pts1 ses=11 comm="cat" exe="/bin/cat"
key="autofs"ARCH=x86_64 SYSCALL=openat AUID="test" UID="test" GID="test"
EUID="test" SUID="test" FSUID="test" EGID="test" SGID="test" FSGID="test"
type=CWD msg=audit(1699990009.349:368): cwd="/home/test"
type=PATH msg=audit(1699990009.349:368): item=0 name="/etc/autofs.conf"
inode=1354087 dev=08:02 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL
cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="root" OGID="root"
type=PROCTITLE msg=audit(1699990009.349:368):
proctitle=636174002F6574632F6175746F66732E636F6E66
```

Данное событие состоит из четырех записей, имеющих один серийный номер и одну и ту же отметку времени. Каждая запись состоит из нескольких пар имя=значение, разделенных пробелом или запятой. Ниже каждая запись рассмотрена подробнее.

Примечание. Некоторые значения в журнале закодированы в шестнадцатеричном формате. При поиске записей аудита с помощью команды ausearch можно использовать параметр -i для автоматического преобразования шестнадцатеричных значений в удобочитаемые эквиваленты.

Первая запись:

- type=SYSCALL – тип записи. Значение SYSCALL указывает, что запись была вызвана системным вызовом ядра;
- msg=audit(1699990009.349:368) – в поле msg записывается:
  - отметка времени и уникальный идентификатор записи в формате audit(time_stamp:ID). Несколько записей могут иметь одну и ту же отметку времени и идентификатор, если они были созданы в рамках одного и того же события аудита. Отметка времени использует формат времени Unix (секунды с 00:00:00 UTC 1 января 1970 года);
  - различные пары имя=значение, зависящие от события, предоставляемые приложениями ядра или пользовательского пространства;

- `arch=c000003e` – содержит информацию об архитектуре ЦП системы. Значение c000003e закодировано в шестнадцатеричном формате (c000003e интерпретируется как x86_64);
- `syscall=257` – тип системного вызова, отправленного ядру. Утилита `ausyscall` позволяет преобразовывать номера системных вызовов в их удобочитаемые эквиваленты. В данном примере 257 – системный вызов openat;
- `success=yes` – указывает, был ли системный вызов, записанный в этом конкретном событии, успешным или неудачным. В данном примере вызов успешный;
- `exit=3` – значение, указывающее код выхода, возвращаемый системным вызовом. Это значение варьируется для разных системных вызовов;
- `a0=ffffff9c a1=7ffc39880600 a2=0 a3=0` – первые четыре аргумента системного вызова в этом событии, закодированные в шестнадцатеричной системе счисления;
- `items=1` – количество вспомогательных записей PATH, следующих за записью системного вызова;
- `ppid=5701` – идентификатор родительского процесса;
- `pid=8223` – идентификатор процесса (PID);
- `auid=501` – идентификатор пользователя аудита, то есть логин. Этот идентификатор присваивается пользователю при входе в систему и наследуется каждым процессом, даже если личность пользователя меняется, например, при переключении учетных записей пользователей с помощью команды `su -`;
- `uid=501` – идентификатор пользователя, запустившего анализируемый процесс. Идентификатор пользователя можно интерпретировать в имя пользователя с помощью команды `ausearch -i --uid UID`;
- `gid=501` – идентификатор группы пользователя, запустившего анализируемый процесс;
- `euid=501` – эффективный идентификатор пользователя, запустившего анализируемый процесс;
- `suid=501` – установленный идентификатор пользователя, запустившего анализируемый процесс;
- `fsuid=501` – идентификатор пользователя файловой системы, запустившего анализируемый процесс;
- `egid=501` – эффективный идентификатор группы пользователя, запустившего анализируемый процесс;
- `sgid=501` – заданный групповой идентификатор пользователя, запустившего анализируемый процесс;

- fsgid=501 – идентификатор группы файловой системы пользователя, запустившего анализируемый процесс;
- tty=pts1 – терминал, с которого был вызван анализируемый процесс;
- ses=11 – идентификатор сеанса, из которого был вызван анализируемый процесс;
- comm="cat" – имя команды, которая использовалась для вызова анализируемого процесса;
- exe="/bin/cat" – путь к исполняемому файлу, который использовался для запуска анализируемого процесса;
- key="autofs" – определенная администратором строка, связанная с правилом, создавшим это событие в журнале аудита.

Вторая запись:

- type=CWD – тип записи. Значение CWD используется для записи рабочего каталога, из которого был выполнен процесс, вызвавший системный вызов, указанный в первой записи. Цель этой записи – записать местоположение текущего процесса на случай, если относительный путь будет зафиксирован в связанной записи PATH. Так можно восстановить абсолютный путь;
- cwd="/home/test" – путь к каталогу, в котором был вызван системный вызов.

Третья запись:

- type=PATH – событие аудита содержит запись типа PATH для каждого пути, который передается системному вызову в качестве аргумента. В этом событии аудита в качестве аргумента использовался только один путь (/etc/autofs.conf);
- item=0 – указывает, какой элемент из общего числа элементов, указанных в записи типа SYSCALL, является текущей записью. Это число начинается с нуля; значение 0 означает, что это первый элемент;
- name="/etc/autofs.conf" – путь к файлу или каталогу, который был передан системному вызову в качестве аргумента;
- inode=1354087 – номер индексного дескриптора, связанный с файлом или каталогом, записанным в этом событии. Отобразить файл или каталог, связанный с номером индексного дескриптора можно, выполнив команду:

```
# find / -inum 1354087 -print
/etc/autofs.conf
```

- dev=08:02 – вспомогательный и основной идентификатор устройства, которое содержит файл или каталог, записанный в этом событии (в данном примере /dev/08/02);

- mode=0100644 – права доступа к файлу или каталогу, закодированные в числовой форме, возвращаемые командой stat в поле st_mode (в данном примере -rw-r--r--);
- ouid=0 – идентификатор пользователя владельца объекта;
- ogid=0 – идентификатор группы владельца объекта;
- rdev=00:00 – записанный идентификатор устройства только для специальных файлов. В данном случае он не используется, поскольку записанный файл является обычным файлом;
- cap_fp=0 – данные, относящиеся к настройке разрешенных возможностей файловой системы для объекта файла или каталога;
- cap_fi=0 – данные, относящиеся к настройке унаследованных возможностей файловой системы для объекта файла или каталога;
- cap_fe=0 – установка эффективного бита возможностей файловой системы объекта файла или каталога;
- cap_fver=0 – версия возможностей файловой системы объекта файла или каталога;

Четвёртая запись:

- type=PROCTITLE – тип записи. Значение PROCTITLE указывает, что эта запись содержит полную командную строку, которая инициировала это событие аудита, вызванное системным вызовом ядра;
- proctitle – полная командная строка, которая использовалась для запуска анализируемого процесса. Поле закодировано в шестнадцатеричном формате. Текст декодируется в команду, которая вызвала это событие аудита. При поиске записей аудита с помощью команды ausearch следует использовать параметр -i для автоматического преобразования шестнадцатеричных значений в удобочитаемые эквиваленты. Значение 636174002F6574632F6175746F66732E636F6E66 интерпретируется в «cat /etc/autofs.conf».

Эти же записи в выводе команды ausearch -i:

```
# ausearch -i -k autofs
----
type=PROCTITLE msg=audit(14.11.2023 21:26:49.349:368) : proctitle=cat
/etc/autofs.conf
type=PATH msg=audit(14.11.2023 21:26:49.349:368) : item=0
name=/etc/autofs.conf inode=1354087 dev=08:02 mode=file,644 ouid=root
ogid=root rdev=00:00 nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0
cap_fver=0 cap_frootid=0
type=CWD msg=audit(14.11.2023 21:26:49.349:368) : cwd=/home/test
type=SYSCALL msg=audit(14.11.2023 21:26:49.349:368) : arch=x86_64
syscall=openat success=yes exit=3 a0=AT_FDCWD a1=0x7ffc39880600 a2=O_RDONLY
```

```
a3=0x0 items=1 ppid=5701 pid=8223 auid=test uid=test gid=test euid=test
suid=test fsuid=test egid=test sgid=test fsgid=test tty=pts1 ses=11 comm=cat
exe=/bin/cat key=autofs
```

8.9.8.4 Примеры

8.9.8.4.1 Запуск и завершение выполнения функций аудита

Поиск записей аудита, связанных с запуском и завершением функции аудита:

```
# ausearch -m DAEMON_START -m DAEMON_END
----
time->Mon Nov 13 08:46:48 2023
type=DAEMON_START msg=audit(1699858008.579:1767): op=start ver=3.1.2
format=enriched kernel=5.10.194-std-def-alt1 auid=4294967295 pid=2524 uid=0
ses=4294967295 res=success
----
time->Mon Nov 13 09:47:31 2023
type=DAEMON_END msg=audit(1699861651.992:1768): op=terminate
auid=0 uid=0 ses=4294967295 pid=1 res=success
----
time->Tue Nov 14 09:38:26 2023
type=DAEMON_START msg=audit(1699947506.800:4888): op=start ver=3.1.2
format=enriched kernel=5.10.194-std-def-alt1 auid=4294967295 pid=2525 uid=0
ses=4294967295 res=success
```

8.9.8.4.2 Модификация конфигурации аудита

События модификации конфигурации аудита, происходящие во время сбора данных аудита записываются в файл журнала аудита `/var/log/audit/audit.log`.

Поиск записей аудита, связанных с модификацией конфигурации аудита:

```
# ausearch -m CONFIG_CHANGE
----
time->Tue Nov 14 09:38:26 2023
type=CONFIG_CHANGE msg=audit(1699947506.822:5): op=set
audit_backlog_wait_time=60000 old=60000 auid=4294967295 ses=4294967295 res=1
----
time->Tue Nov 14 16:43:14 2023
type=CONFIG_CHANGE msg=audit(1699972994.820:1207):
auid=500 ses=3 op=add_rule key="audit_config" list=4 res=1
```

Можно также создать правило аудита, которое будет отслеживать изменения конфигурации аудита:

```
# auditctl -w /etc/audit -p w -k audit_config
```

Найти такие записи аудита можно, выполнив команду:

```
# ausearch -k audit_config
----
time->Tue Nov 14 16:43:14 2023
type=CONFIG_CHANGE msg=audit(1699972994.820:1207): auid=500 ses=3 op=add_rule
key="audit_config" list=4 res=1
```

8.9.8.4.3 События, связанные с операцией чтения записей аудита

Можно создать правило аудита, связанное с неуспешными попытками чтения записей аудита:

```
# auditctl -a always,exit -F arch=b64 -S open -F exit=-EACCES -F key=open -k
audit_log_EACCES
# auditctl -a always,exit -F arch=b64 -S open -F exit=-EPERM -F key=open -k
audit_log_EPERM
```

После попыток прочитать данные аудита напрямую из файла `/var/log/audit/audit.log` и с помощью команды `ausearch` от имени обычного пользователя:

```
$ cat /var/log/audit/audit.log
cat: /var/log/audit/audit.log: Отказано в доступе
$ /sbin/ausearch -i -k audit_log
Error opening config file (Отказано в доступе)
NOTE - using built-in logs: /var/log/audit/audit.log
Error opening /var/log/audit/audit.log (Отказано в доступе)
```

Будут созданы следующие записи, связанные с операцией чтения записей аудита:

```
# ausearch -i -k audit_log
----
type=PROCTITLE msg=audit(24.05.2018 18:13:11.849:216) :
proctitle=auditctl -a always,exit -F arch b64 -S open -F exit -EPERM -F
key=open -k audit_log_EPERM
type=SOCKADDR msg=audit(24.05.2018 18:13:11.849:216) :
saddr={ saddr_fam=netlink nlnk-fam=16 nlnk-pid=0 }
type=SYSCALL msg=audit(24.05.2018 18:13:11.849:216) :
arch=x86_64 syscall=sendto success=yes exit=1076 a0=0x4 a1=0x7ffd13ee81e0
a2=0x434 a3=0x0 items=0 ppid=5423 pid=5919 auid=user uid=root gid=root
euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=3
comm=auditctl exe=/sbin/auditctl key=(null)
type=CONFIG_CHANGE msg=audit(24.05.2018 18:13:11.849:216) :
auid=user ses=3 op=add_rule key=open key=audit_log_EPERM list=exit res=yes
```

8.9.8.4.4 Хранение журнала аудита

Аудит регистрирует события следующего типа:

- DAEMON_ERR – служба аудита остановилась из-за внутренней ошибки;
- DAEMON_RESUME – служба аудита возобновила ведение журнал;
- DAEMON_ROTATE – произошла ротация файлов журнала аудита;
- DAEMON_ABORT – служба аудита остановилась из-за ошибки.

Поиск записей аудита, сделанных при ротации файлов журнала аудита:

```
# ausearch -m DAEMON_ROTATE
```

8.9.8.4.5 Аудит попыток экспорта информации

Создание правила для записей аудита, связанных с попытками экспортировать информацию:

```
# auditctl -a always,exit -F arch=b64 -S open,openat
```

Поиск записей аудита, связанных с попытками экспортировать информацию:

```
# ausearch -x /usr/bin/rsync | head
```

8.9.8.4.6 Аудит событий, связанных с достижением ограничения неуспешных попыток аутентификации

Примечание. Должна быть настроена блокировка учётной записи после последовательных неудачных входов в систему. Например, блокирование учётной записи после четырёх последовательных неудачных входов в систему в течение пяти минут (файл `/etc/pam.d/system-auth-local-only`):

```
auth            requisite       pam_faillock.so preauth deny=4
unlock_time=300
auth            sufficient      pam_tcb.so shadow fork nullok
auth            [default=die]   pam_faillock.so authfail deny=4
unlock_time=300
account         required        pam_faillock.so
account         required        pam_tcb.so shadow fork
password        required        pam_passwdqc.so config=/etc/passwdqc.conf
password        required        pam_tcb.so use_authtok shadow fork nullok
write_to=tcb
session         required        pam_tcb.so
```

Поиск записей, связанных с достижением ограничения неуспешных попыток аутентификации:

```
# ausearch -i -m RESP_ACCT_LOCK -m ANOM_LOGIN_FAILURES
----
type=ANOM_LOGIN_FAILURES msg=audit(14.11.2023 17:36:01.837:123232) :
```

```
pid=26656 uid=root auid=unset ses=unset msg='pam_faillock uid=root
exe=/bin/login hostname=pbs addr=? terminal=tty2 res=success'
----
type=RESP_ACCT_LOCK msg=audit(14.11.2023 17:36:01.837:123233) :
pid=26656 uid=root auid=unset ses=unset msg='pam_faillock uid=root
exe=/bin/login hostname=pbs addr=? terminal=tty2 res=success'
```

Событие разблокировки пользователя (`faillock --user test --reset`) попадает в аудит с типом USER_ACCT и `msg=pam_faillock`:

```
# ausearch -i -m USER_ACCT
```

8.9.8.4.7 Использование механизма идентификации и аутентификации

Поиск записей аудита, связанных с использованием механизма аутентификации:

```
# ausearch -m USER_AUTH
----
time->Tue Nov 14 17:37:28 2023
type=USER_AUTH msg=audit(1699976248.331:123242):
pid=27368 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication
grantors=?
acct="?" exe="/bin/login" hostname=pbs addr=? terminal=/dev/tty2 res=failed'

----
time->Tue Nov 14 17:56:28 2023
type=USER_AUTH msg=audit(1699977388.507:123325):
pid=27621 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication
grantors=pam_userpass,pam_tcb acct="test" exe="/usr/sbin/sshd"
hostname=192.168.0.177 addr=192.168.0.177 terminal=ssh res=success'
```

Поиск записей аудита, связанных с использованием механизма идентификации:

```
# ausearch -m USER_LOGIN -i
----
type=USER_LOGIN msg=audit(14.11.2023 17:36:10.321:123241) :
pid=27368 uid=root auid=unset ses=unset msg='op=login acct=test
exe=/bin/login hostname=pbs addr=? terminal=/dev/tty2 res=failed'
----

type=USER_LOGIN msg=audit(14.11.2023 17:56:28.569:123331) :
pid=27621 uid=root auid=test ses=145 msg='op=login id=test
exe=/usr/sbin/sshd hostname=192.168.0.177 addr=192.168.0.177
terminal=/dev/pts/7 res=success
```

Команда `aureport` позволяет вывести отчёт обо всех попытках входа в систему:

```
# aureport -l
Login Report
============================================
# date time auid host term exe success event
============================================
1. 24.10.2023 21:58:15 user 192.168.0.177 sshd /usr/sbin/sshd no 394615
…
43. 14.11.2023 17:49:59 test 192.168.0.177 sshd /usr/sbin/sshd no 123267
44. 14.11.2023 17:50:01 501 192.168.0.177 /dev/pts/6 /usr/sbin/sshd yes
123280
45. 14.11.2023 17:56:22 test 192.168.0.177 sshd /usr/sbin/sshd no 123322
46. 14.11.2023 17:56:24 test 192.168.0.177 sshd /usr/sbin/sshd no 123324
47. 14.11.2023 17:56:28 501 192.168.0.177 /dev/pts/7 /usr/sbin/sshd yes
123331
```

Отчёт о неудачных попытках входа в систему:

```
# aureport -l --failed
```

Отчёт об изменениях пользовательских учетных записей:

```
# aureport -m
```

8.9.8.4.8 Регистрация изменений даты и времени

Для регистрации изменений даты и времени, необходимо включить контроль над изменением значения времени.

Запись событий, изменяющих время через `clock_settime`, `settimeofday` и `adjtimex` с правилом в зависимости от архитектуры, в примере для 64 бит (AMD, Intel):

```
# auditctl -a exit,always -F arch=b64 -S clock_settime -S settimeofday
-S adjtimex -k FPT_STM
```

Изменить время с помощью модуля центра управления системой или в системной консоли, командой `date`.

Поиск записей аудита, связанных с операцией изменения даты и времени:

```
# ausearch -k FPT_STM
----
time->Tue Nov 14 18:07:27 2023
type=PROCTITLE msg=audit(1699978047.591:188):
proctitle=6461746500303532343138303832303138
type=TIME_INJOFFSET msg=audit(1699978047.591:188): sec=-172799968
nsec=406875048
type=SYSCALL msg=audit(1699978047.591:188): arch=c000003e syscall=227
success=yes exit=0 a0=0 a1=7ffc85a10900 a2=0 a3=0 items=0 ppid=5423 pid=5879
```

```
auid=500 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0
ses=3 comm="date" exe="/bin/date" key="FPT_STM"
```

Пример удаления правила:

```
# auditctl -d exit,always -F arch=b64 -S clock_settime -S settimeofday
-S adjtimex -k FPT_STM
```

8.9.8.4.9 Регистрация событий, изменяющих информацию о пользователях/группах

Для фиксации событий, которые вносят изменения в пользовательские аккаунты, можно создать файл `/etc/audit/rules.d/20-account_changes.rules` со следующим содержимым:

```
# audit_account_changes
-w /etc/group -p wa -k audit_account_changes
-w /etc/passwd -p wa -k audit_account_changes
-w /etc/gshadow -p wa -k audit_account_changes
-w /etc/shadow -p wa -k audit_account_changes
-w /etc/security/opasswd -p wa -k audit_account_changes
```

Поиск записей аудита, связанных с операциями изменения информации о пользователях/группах:

```
# ausearch -k audit_account_changes
```

8.9.8.4.10 Регистрация запуска ПО

Для аудита запуска ПО можно создать файл `/etc/audit/rules.d/50-execprog.rules` с правилами в зависимости от архитектуры, в примере 64 бит (AMD, Intel):

```
-a always,exit -F arch=b64 -S open,openat,execve -F exit=-EACCES -F key="AVC"
-a always,exit -F arch=b64 -S open,openat,execve -F exit=-EPERM -F key="AVC"
```

Поиск записей аудита:

```
# ausearch -k AVC
```

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.