MyOffice
Plus

Руководство пользователя

ОПЕРАЦИОННАЯ СИСТЕМА АЛЬТ СЕРВЕР 10.0

ОПЕРАЦИОННАЯ СИСТЕМА

АЛЬТ СЕРВЕР 10.0

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

1.0

На 189 листах

Москва
2022

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «МойОфис» и «MyOffice» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращения, которые используются в настоящем документе, приведены в Таблице 1.

Таблица 1 – Сокращения и расшифровки

Сокращения	Расшифровка
ОС Альт Сервер	Операционная система «Альт Сервер»
ПЭВМ	Персональная электронно-вычислительная машина

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение MyOffice Plus

MyOffice Plus – комплексный продукт для организации рабочей среды в крупных государственных организациях и коммерческих предприятиях. Единая лицензия МойОфис Plus включает операционную систему, средства безопасного хранения файлов, работы с документами, ведения переписки по электронной почте и планирования рабочего времени.

ОС Альт Сервер входит в состав продукта MyOffice Plus.

1.2 Описание ОС Альт Сервер

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

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.

ОС Альт Сервер состоит из набора компонентов предназначенных для реализации функциональных задач необходимых пользователям (должностным лицам для выполнения определённых должностными инструкциями, повседневных действий) и поставляется в виде дистрибутива и комплекта эксплуатационной документации.

В структуре ОС Альт Сервер можно выделить следующие функциональные элементы:

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

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

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

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

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

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

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

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

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

– настройка оборудования;
– настройка сети.

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

1.3 Описание ОС Linux

1.3.1 Свободные программы

Операционная система (далее – ОС) Linux – ядро, основные компоненты системы и большинство её пользовательских приложений – свободные программы. Свободные программы можно:
– запускать на любом количестве компьютеров;
– распространять бесплатно или за деньги без каких-либо ограничений;
– получать исходные тексты этих программ и вносить в них любые изменения.

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

1.3.2 Разработка Linux

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

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

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

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

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

1.3.3 Защищенность

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

1.3.4 Дистрибутивы Linux

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

1.3.5 Новым пользователям

Linux – самостоятельная операционная система. Все операционные системы разные: Linux – не Windows, не OS X и не FreeBSD. В Linux свои правила, их необходимо изучить и к ним необходимо привыкнуть. Терпение и настойчивость в изучении Linux обернётся значительным повышением эффективности и безопасности вашей работы. То, что сегодня кажется странным и непривычным, завтра понравится и станет нормой. Не стесняйтесь задавать вопросы, ведь самый простой способ найти ответ – совет опытного специалиста. Взаимопомощь и общение – традиция в мире Linux. Всегда можно обратиться за помощью к сообществу пользователей и разработчиков Linux. Большинство вопросов повторяются, поэтому для начала стоит поискать ответ на свой вопрос в документации, затем в сети Интернет. Если вы не нашли ответа в перечисленных источниках, не стесняйтесь, пишите на форум или в списки рассылки так, как писали бы своим друзьям, и вам обязательно помогут.

1.4 Системы Альт

1.4.1 ALT Linux Team

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

1.4.2 Сизиф

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

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

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

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

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

1.4.3 Десятая платформа

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

Десятая платформа (p10) была создана в июле 2021 года и её поддержка продлится до июля 2024.

1.4.3.1 Основные новшества в десятой платформе

– Синхронная сборка p10 производится для пяти основных архитектур:
  - 64-битных x86_64, aarch64 и ppc64le;
  - 32-битных i586 и armh (armv7hf).

– Ядра реального времени – для архитектуры x86_64 собраны два realtime-ядра: Xenomai и Real Time Linux (PREEMPT_RT).
– Расширение набора групповых политик – групповые политики поддерживают параметры gsettings для управления рабочими средами MATE и Xfce.
– Центр администрирования Active Directory (admc) – графическое приложение для управления пользователями, группами и групповыми политиками домена Active Directory.
– Платформа Deploy – предназначена для развёртывания системных служб на локальном компьютере с помощью Ansible. Поддерживаемые роли: Apache, MariaDB, MediaWiki, Nextcloud, PostgreSQL и Moodle.
– Модуль настройки многотерминального режима alterator-multiseat.

2 НАЧАЛО ИСПОЛЬЗОВАНИЯ ОС АЛЬТ СЕРВЕР

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

2.1 Загрузка системы

Запуск ОС Альт Сервер выполняется автоматически после запуска компьютера и отработки набора программ BIOS. На экране появляется меню, в котором перечислены возможные варианты загрузки операционной системы.

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

Стрелками клавиатуры **Вверх** и **Вниз** выберите нужную операционную систему. Дополнительно к основным вариантам запуска ОС из этого меню можно загрузить Linux в безопасном режиме или запустить проверку памяти. Загрузка операционной системы по умолчанию (первая в списке) начинается автоматически после небольшого времени ожидания (обычно несколько секунд). Нажав клавишу **Enter**, можно начать загрузку немедленно.

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

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

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

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

2.2 Получение доступа к зашифрованным

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

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

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

2.3 Вход в систему

2.3.1 Вход и работа 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**.

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.

2.3.2 Виртуальная консоль

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

При установке системы в профиле по умолчанию на первой виртуальной консоли пользователь может зарегистрироваться и работать в графическом режиме. При нажатии **Ctrl** + **Alt** + **F1** осуществляется переход на первую виртуальную консоль в графический режим.

Двенадцатая виртуальная консоль (**Ctrl** + **Alt** + **F12**) выполняет функцию системной консоли – на неё выводятся сообщения о происходящих в системе событиях.

2.3.3 Вход и работа в системе в графическом режиме

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

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

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

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

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

⚠ 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.

3 РАБОЧИЙ СТОЛ MATE

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

– верхняя панель (серая полоса вверху экрана);

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

– панель со списком окон (серая полоса внизу экрана).

3.1 MATE: Верхняя панель

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

– меню Приложения;

– меню Точки входа;

– меню Система.

Правая часть панели содержит:

– область уведомлений;

– регулятор громкости и апплет настройки звука;

– приложение «Сетевые соединения»;

– часы и календарь;

– параметры клавиатуры; п

– араметры управления питанием.

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

3.1.1 MATE: Меню Приложения

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

– Аудио и видео;

– Графика;

– Интернет;

– Офис;

– Системные;
– Стандартные.

3.1.2 MATE: Меню Точки входа

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

Первый подраздел:

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

Второй подраздел:

– **Компьютер** – позволяет увидеть все файлы в компьютере и файлы на подключённых внешних носителях;
– **Съёмное устройство** – позволяет получить доступ к CD/DVD дисководу или к USB-flashнакопителю.

Третий подраздел:

– **Сеть** – позволяет просматривать сетевые подключения компьютера. Осуществляет получение доступа к файлам и другим ресурсам, доступным в этих сетях;
– **Соединиться с сервером…** – позволяет создать подключение к публичным или локальным сетям.

Четвёртый подраздел:

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

3.1.3 MATE: Меню Система

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

Первый подраздел содержит следующие пункты:

1. **Параметры** – содержит доступ к различным настройкам и предоставляет доступ к инструментам администрирования системы. В меню **Параметры** входят следующие настройки:

   – **Интернет и сеть**:

   - **Расширенная конфигурация сети** – отображает сетевые подключения компьютера и позволяет их настраивать;
   - **Сетевая прокси-служба** – позволяет настроить прокси-сервер;

   – **Оборудование**:

   - **Bluetooth** – позволяет настраивать Bluetooth-устройства для работы с компьютером;
   - **Диспетчер даты и времени** – открывает диалоговое окно настройки даты и времени (часовой пояс, синхронизация NTP);
   - **Звук** – открывает диалоговое окно настройки звука (громкость звука, звуковые события, оборудование);
   - **Клавиатура** – запускает диалог настройки клавиатуры. Тут же можно задать используемые в системе раскладки клавиатуры;
   - **Комбинации клавиш клавиатуры** – позволяет задать сочетания клавиш для выполнения определённых заданий в окружении рабочего стола;
   - **Мышь** – позволяет настроить кнопки и другие параметры мыши;
   - **Управление питанием** – позволяет настроить компьютер на работу с различными параметрами энергосбережения;
   - **Экраны** – позволяет задать разрешение и другие параметры монитора.

   – Оформление:

   - **Внешний вид** – позволяет настроить внешний вид рабочего стола, включая фоновую картинку;
   - **Всплывающие уведомления** – позволяет настроить стиль и позицию уведомлений;

- **Главное меню MATE** – позволяет изменить список отображаемых элементов в меню **Приложений** и меню **Настроек**;
- **Окна** – позволяет настроить параметры поведения окон;
- **Хранитель экрана** – позволяет настроить заставку для рабочего стола;

– Персональные:

- **Управление файлами (File Management)** – влияет на предоставление пользователю файлов и папок;
- **Вспомогательные технологии** – даёт возможность выбирать программы для увеличения частей экрана или для прочтения содержимого экранов;
- **Запускаемые приложения** – позволяет выбрать приложения для автоматического запуска при входе;
- **Обо мне** – позволяет установить изображение и задать данные пользователя (имя, фамилия, телефон, электронная почта);
- **Предпочтительные приложения** – даёт возможность выбрать, какие приложения необходимо использовать для конкретных задач;

– **Прочие**:

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

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

Второй подраздел включает пункты:

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

Третий подраздел включает пункты:

1. **Заблокировать экран** – служит для запуска хранителя экрана. Для возобновления работы после блокировки необходим ввод пароля.
2. **Завершить сеанс пользователя…** – запускает диалог, который позволяет завершить сеанс или переключить пользователя.
3. **Выключить…** – позволяет перезагрузить либо выключить компьютер.

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

3.2 MATE: Область рабочего стола

Область рабочего стола включает в себя три значка:

– **Компьютер** – предоставляет доступ к устройствам хранения данных;

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

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

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**).

3.3 MATE: Панель со списком окон

У этой панели три основных компонента:

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

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

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

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

3. **Свернуть все окна** – кнопка позволяет свернуть (развернуть) все открытые окна на текущем рабочем месте.

4 НАСТРОЙКА СИСТЕМЫ

4.1 Центр управления системой

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

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

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

4.1.1 Применение центра управления системой

Вы можете использовать ЦУС для разных целей, например:

– настройки **Даты и времени** (datetime);
– управления выключением и перезагрузкой компьютера (ahttpd-power, доступно только в вебинтерфейсе);
– настройки **Аутентификации** (auth);
– управления **Системными службами** (services);
– просмотра **Системных журналов** (logs);
– настройки **OpenVPN-подключений** (openvpn-server и net-openvpn);
– конфигурирования **Сетевых интерфейсов** (net-eth);
– изменения пароля **Администратора системы (root)** (root);
– создания, удаления и редактирования учётных записей **Пользователей** (users);
– настройки ограничения **Использования диска (квоты)** (quota).

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

4.1.2 Запуск центра управления системой в графической

Центр управления системой можно запустить следующими способами:

– в графической среде MATE: **Система** > **Администрирование** > **Центр управления системой**;

– из командной строки: командой **acc**.

При запуске необходимо ввести пароль администратора системы (root).

После успешного входа можно приступать к настройке системы.

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

– основной режим (кнопка отжата);

– режим эксперта (кнопка нажата).

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

4.1.3 Использование веб-ориентированного центра

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 на сервере команду:

```
$ ip addr
```

IP-адрес будет указан после слова inet:

```
1: lo: 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: mtu 1500 qdisc mq state UP qlen 1000
   link/ether 60:eb:69:6c:ef:47 brd ff:ff:ff:ff:ff:ff
   inet 192.168.0.122/24 brd 192.168.0.255 scope global enp0s3
```

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

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

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

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

Веб-интерфейс ЦУС можно настроить (кнопка 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.

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

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

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

4.2 Настройка сети

4.2.1 NetworkManager

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

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

NetworkManager доступен как апплет, находящийся в системном лотке.

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

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

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

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

Для настройки соединений, следует в меню **NetworkManager**, вызываемом нажатием правой кнопкой мыши, выбрать пункт **Параметры соединений…**. В открывшемся окне будет показан сгруппированный по типам список соединений. Необходимо выбрать нужную сеть и нажать кнопку **Изменить**.

В открывшемся окне можно изменить настройки сетевого интерфейса.

NetworkManager под именем **System enp2s0** показывает системное Ethernetсоединение, создаваемое Etcnet. Изменить его в диалоге **Сетевые соединения** 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).

4.2.2 Настройка в ЦУС

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

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

5 СЕРВЕРНЫЕ РЕШЕНИЯ

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

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

5.1 Вход в систему

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

5.2 Развёртывание офисной ИТ-инфраструктуры

5.2.1 Подготовка

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

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

5.2.1.1 Домен

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

С помощью **Домена** вы можете:

– вести централизованную базу пользователей и групп;

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

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

5.2.1.2 Сервер, рабочие места и аутентификация

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

Таким образом, можно выделить:

1. **Сервер (компьютер под управлением ОС Альт Сервер)**

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

2. **Рабочее место**

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

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

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

3. Авторизация

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

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

5.3 Централизованная база пользователей

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

5.3.1 Создание учётных записей пользователей

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

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

Возможные варианты источника данных о пользователях:

– текущий метод аутентификации (выбирается в модуле **Аутентификация**);

– файл /etc/passwd (выбран по умолчанию);

– локальная база LDAP;

– база LDAP на другом сервере;

– локальная база Samba DC.

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

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

5.3.2 Объединение пользователей в группы

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

```
$ su -
```

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

– просматривать актуальный список групп и список пользователей, входящих в каждую группу;

– создавать и удалять группы;

– добавлять и удалять пользователей в существующие группы;

– привязывать группу к системным группам и группам Samba.

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

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

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

5.3.3 Настройка учётной записи

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

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

5.3.4 Привязка групп

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

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

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

Привязка к группе Samba позволяет создавать группы Samba, которые могут использоваться для установки прав доступа на рабочих станциях под управлением операционной системы Windows, которые аутентифицируются в ALT-домене. За дополнительной информацией по настройке обращайтесь к встроенной справке соответствующих модулей ЦУС.

6 ОРГАНИЗАЦИЯ СЕТЕВОЙ ИНФРАСТРУКТУРЫ С ПОМОЩЬЮ СЕРВЕРА

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.

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

6.1 Настройка подключения к Интернету

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

1. **Сервер без подключения к сети Интернет**

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

2. **Шлюз**

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

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

– Ethernet;

– PPTP;

– PPPoE;

– и т.д.

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

Доступные разделы:

– Ethernet-интерфейсы;

– PPTP-соединения;

– PPPoE-соединения;

– OpenVPN-соединения.

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

6.1.1 Конфигурирование сетевых интерфейсов

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

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

– **Имя компьютера** – указать сетевое имя ПЭВМ в поле для ввода имени компьютера (это общий сетевой параметр, не привязанный, к какому-либо конкретному интерфейсу). Имя компьютера, в отличие от традиционного имени хоста в Unix (hostname), не содержит названия сетевого домена;

– **Интерфейсы** – выбрать доступный сетевой интерфейс, для которого будут выполняться настройки;

– **Версия протокола IP** – указать в выпадающем списке версию используемого протокола IP (IPv4, IPv6) и убедиться, что пункт **Включить**, обеспечивающий поддержку работы протокола, отмечен;

– **Конфигурация** – выбрать способ назначения IP-адресов (службы DHCP, Zeroconf, вручную);

– **IP-адреса** – пул назначенных IP-адресов из поля **IP**, выбранные адреса можно удалить нажатием кнопки **Удалить**;

– **IP** – ввести IP-адрес вручную и выбрать в выпадающем поле предпочтительную маску сети, затем нажать кнопку **Добавить** для переноса адреса в пул поля **IP-адреса**;

– **Шлюз по умолчанию** – в поле для ввода необходимо ввести адрес шлюза, который будет использоваться сетью по умолчанию;

– **DNS-серверы** – в поле для ввода необходимо ввести список предпочтительных DNSсерверов, которые будут получать информацию о доменах, выполнять маршрутизацию почты и управлять обслуживающими узлами для протоколов в домене;
– **Домены поиска** – в поле для ввода необходимо ввести список предпочтительных доменов, по которым будет выполняться поиск. Если в поле Домены поиска перечислить наиболее часто используемые домены (например, domain), то можно пользоваться неполными именами машин (computer вместо computer.domain).

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

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

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

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

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

1. 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>.

2. **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.

3. **NetworkManager (native)**

В данном режиме управление настройками интерфейса передаётся **NetworkManager** и не зависит от файлов Etcnet. Управлять настройками можно через графический интерфейс NetworkManager.

Файлы с настройками находятся в директории **/etc/NetworkManager/system-connections**. Этот режим особенно актуален для задач настройки сети на клиенте, когда IP-адрес необходимо получать динамически с помощью DHCP, а DNS-сервер указать явно. Через ЦУС так настроить невозможно, так как при включении DHCP отключаются настройки, которые можно задавать вручную.

4. **Не контролируется**

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

6.1.2 Настройка общего подключения к сети Интернет

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

– использование прокси-сервера;

– использование NAT.

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

6.1.2.1 Прокси-сервер

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

У прокси-сервера есть два основных режима работы:

– прозрачный;

– обычный.

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

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

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

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

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

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

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

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

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

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

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

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

6.1.2.2 NAT

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

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

6.1.3 Автоматическое присвоение IP-адресов (DHCP-сервер)

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

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

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

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

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

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

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

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

6.2 Развертывание доменной структуры

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

Модуль поддерживает следующие виды доменов:

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

6.3 Сетевая установка операционной системы

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

6.3.1 Подготовка сервера

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

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

Перед активацией сетевой установки потребуется импортировать установочный DVD-диск Альт Сервер, предварительно вставив его в DVD-привод сервера, либо используя образ диска, расположенный на файловой системе на сервере. Можно также использовать URL вида:

http://ftp.altlinux.org/pub/distributions/ALTLinux/images/p10/workstation/x86_64/alt-workstation-10.0- x86_64.iso

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

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

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

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

На этом подготовка сервера к сетевой установке рабочих станций завершена.

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

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.

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

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

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

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

6.3.2 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 Onboard LAN".

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

Последовательность установки при установке с DVD-диска и при сетевой установке не отличаются друг от друга. Обратитесь к документу «Операционная система Альт Сервер. Руководство по установке».

6.4 Соединение удалённых офисов (OpenVPN-сервер)

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

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

6.4.1 Настройка OpenVPN-сервера

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

Используя модуль OpenVPN-сервер можно:

– включить/отключить OpenVPN-сервер;

– настроить параметры сервера: тип, сети сервера, использование сжатия и т.д.;

– управлять сертификатами сервера;

– настроить сети клиентов.

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

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

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

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

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

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

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

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

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

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

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

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

Появится сообщение: «Сертификат УЦ успешно загружен».

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

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

6.4.2 Настройка клиентов

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

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

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

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

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

– Состояние – «запустить»;

– Сервер – IP адрес сервера или домен;

– Порт – 1194;

– Ключ – выбрать подписанный на сервере ключ.

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

Проверить, появилось ли соединение с сервером можно командой:

```
ip addr
```

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

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

6.5 Доступ к службам сервера из сети Интернет

6.5.1 Внешние сети

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

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

Можно выбрать один из двух режимов работы:

– Роутер. В этом режиме перенаправление пакетов между сетевыми интерфейсами происходит без трансляции сетевых адресов.

– Шлюз (NAT). В этом режиме будет настроена трансляция сетевых адресов (NAT) при перенаправлении пакетов на внешние интерфейсы. Использование этого режима имеет смысл, если у вас настроен, по крайней мере, один внешний и один внутренний интерфейс.

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.

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

6.5.2 Список блокируемых хостов

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

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

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

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

6.6 Статистика

6.6.1 Сетевой трафик

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

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

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

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

Трафик на указанном интерфейсе за заданный период показывается в виде:

– служба (название протокола);

– входящий трафик в килобайтах;

– исходящий трафик в килобайтах.

6.6.2 Прокси-сервер

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

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

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

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

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

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

6.7 Обслуживание сервера

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

6.7.1 Мониторинг состояния системы

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

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

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

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

6.7.2 Системные службы

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

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

6.7.3 Обновление системы

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

работы сервера.

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

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

Процесс обновления системы будет запускаться автоматически согласно заданному расписанию.

6.7.4 Обновление ядра ОС

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

– просматривать список установленных ядер;
– устанавливать, обновлять и удалять ядра; задавать ядро, загружаемое по умолчанию;
– устанавливать/удалять отдельные модули ядра.

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

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

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

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

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

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.

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

Новое ядро загрузится только после перезагрузки системы.

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

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

6.7.5 Обновление систем, не имеющих выхода в Интернет

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

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

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

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

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

При выборе любой архитектуры также будет добавлен источник с noarch.

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

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

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.

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

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

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

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

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

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

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).

6.7.5.1 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:///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
```

6.7.5.2 Настройка FTP-сервера

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

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

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

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

Перезапустить xinetd:

```
# systemctl restart xinetd
```

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

```
local_enable=YES
```

Создать каталог **/var/ftp/mirror**:

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

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

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

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:///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
```

6.7.6 Локальные учётные записи

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

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

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

6.7.7 Администратор системы

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

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

6.7.8 Дата и время

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

Системное время зависит от следующих факторов:

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

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

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

6.7.9 Ограничение использования диска

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

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

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

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

При задании ограничений различают жёсткие и мягкие ограничения:

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

Значение 0 при задании ограничений означает отсутствие ограничений.

6.7.10 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 **Выключение компьютера** позволяет:

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

Возможна настройка ежедневного применения данных действий в заданное время.

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

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

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

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

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

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

```
Tue Jun 16 11:46:59 EET 2022: The server.test.alt is about to start.
```

При выключении:

```
Tue Jun 16 12:27:02 EET 2022: 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.

6.8 Прочие возможности ЦУС

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

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

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

Прочие пакеты для ЦУС можно найти, выполнив команду:

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

Модули можно дополнительно загружать и удалять как обычные программы:

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

6.9 Права доступа к модулям

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

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

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

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

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

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

7 КОРПОРАТИВНАЯ ИНФРАСТРУКТУРА

7.1 Samba 4 в роли контроллера домена Active

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

Поддерживаются следующие базовые возможности Active Directory:

– аутентификация рабочих станций Windows и Linux и служб;

– авторизация и предоставление ресурсов; групповые политики (GPO);

– перемещаемые профили (Roaming Profiles);

– поддержка инструментов Microsoft для управления серверами (Remote Server Administration Tools) с компьютеров под управлением Windows;

– поддержка протоколов SMB2 и SMB3 (в том числе с поддержкой шифрования);

– репликация с другими серверами (в том числе с Windows 2012).

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

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

7.1.1 Установка

Для установки Samba AD DC выполняются следующие шаги:

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

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

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

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

7.1.2 Создание нового домена

7.1.2.1 Восстановление к начальному состоянию Samba

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

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

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

7.1.2.2 Выбор имени домена

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

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

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

```
# domainname test.alt
```

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

7.1.2.3 Создание домена в ЦУС

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

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

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

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

3. После успешного создания домена, будет выведена информация о домене.
4. Перегрузить сервер.

7.1.2.4 Создание домена одной командой

Создание контроллера домена test.alt:

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

где:

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

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

7.1.2.5 Интерактивное создание домена

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

```
# samba-tool domain provision
Realm [TEST.ALT]:
Domain [TEST]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
[SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [127.0.0.1]:
Administrator password:
Retype password:
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.0.122
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=test,DC=alt
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=test,DC=alt
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated
at /var/lib/ samba/private/krb5.conf
Once the above files are installed, your Samba4 server will be ready to
use
Server Role:           active directory domain controller
Hostname:              dc
NetBIOS Domain:        TEST
DNS Domain:            test.alt
DOMAIN SID:            S-1-5-21-80639820-2350372464-3293631772
```

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

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.

7.1.3 Запуск службы

Установите службу по умолчанию и запустите её:

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

7.1.4 Настройка Kerberos

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

```
includedir /etc/krb5.conf.d/
[logging]
# default = FILE:/var/log/krb5libs.log
# kdc = FILE:/var/log/krb5kdc.log
# admin_server = FILE:/var/log/kadmind.log
[libdefaults]
 dns_lookup_kdc = true
 dns_lookup_realm = true
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true rdns = false
 default_realm = TEST.ALT
 default_ccache_name = KEYRING:persistent:%{uid}
[realms]
TEST.ALT = {
   default_domain = test.alt
}
[domain_realm]
dc = TEST.ALT
```

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
```

7.1.5 Проверка работоспособности

Просмотр общей информации о домене:

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

Просмотр предоставляемых служб:

```
# smbclient -L localhost -Uadministrator Enter TEST\administrator's
password:
    Sharename     Type  Comment
    ---------     ----  -------
    sysvol  Disk
    netlogon      Disk
    IPC$          IPC   IPC Service (Samba 4.14.13)
SMB1 disabled -- no workgroup       available
```

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

Проверка конфигурации DNS:

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

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

2. Проверьте имена хостов:

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

Если имена не находятся, проверьте выключение службы named.

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

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

Просмотр полученного билета:

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

Valid starting    Expires     Service principal
20.06.2022 11:12:23     20.06.2022 21:12:23     krbtgt/TEST.ALT@TEST.ALT
   renew until 27.06.2022 11:12:18
```

7.1.6 Управление пользователями

Создать пользователя с паролем:

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

Удалить пользователя:

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

Отключить пользователя:

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

Включить пользователя:

```
amba-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' --
mailaddress='ivanov@test.alt'
# samba-tool user setexpiry ivanov --noexpiry
```

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

7.1.7 Заведение вторичного DC

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

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

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

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

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

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

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

В resolvconf обязательно должен быть добавлен PDC как nameserver.

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

Имя домена должно быть указано в верхнем регистре

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

5. Убеждаемся, что билет получен:

```
#klist

Ticket cache: KEYRING:persistent:0:0

Default principal: administrator@TEST.ALT

Valid starting    Expires     Service principal

20.06.2022 11:12:23     20.06.2022 21:12:23     krbtgt/TEST.ALT@TEST.ALT

renew until 27.06.2022 11:12:18
```

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

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

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

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

Для получения дополнительной информации можно воспользоваться командой:

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

7. После успешного ввода в домен в resolvconf необходимо сменить адрес PDC на адрес вторичного DC (в примере 192.168.0.106).
8. Сделать службу samba запускаемой по умолчанию:

```
# chkconfig samba on
```

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

```
# service samba start
```

7.1.8 Репликация

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

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

1. Реплицируем на вторичном DC (с первичного):

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

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

2. Реплицируем на вторичном DC (на первичный):

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

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

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

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

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

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

7.1.9 Подключение к домену на рабочей станции

7.1.9.1 Подготовка

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

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

Синхронизация времени с контроллером домена производится автоматически.

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

1. В Центре управления системой в разделе **Сеть** > **Ethernet интерфейсы** задать имя компьютера, указать в поле DNS-серверы DNS-сервер домена и в поле Домены поиска – домен для поиска.
2. 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 в документе – IP-адрес DNS-сервера домена.

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

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

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

– обновить DNS адреса:

```
# resolvconf -u
```

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

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

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

7.1.9.2 Ввод в домен

Ввод в домен можно осуществить следующими способами:

1. В командной строке:

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

2. В Центре управления системой:
   – в разделе **Пользователи** > **Аутентификация**;

– в открывшемся окне следует выбрать пункт **Домен Active Directory**, заполнить поля и нажать кнопку **Применить**;
– в открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку **ОК**;
– при успешном подключении к домену, отобразится соответствующая информация.

Перезагрузить рабочую станцию.

7.2 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). Возможно установить при использовании ADMX-файлов Mozilla Firefox (пакет admx-firefox) и Google Chrome (пакет admx-chromium) соответственно;
– установки запрета на подключение внешних носителей;
– управления политиками control (реализован широкий набор настроек). Возможно установить при использовании ADMX-файлов ALT;
– включения или выключения различных служб (сервисов systemd). Возможно установить при использовании ADMX-файлов ALT;
– подключения сетевых дисков (экспериментальная политика); генерирования (удаления/замены) ярлыков для запуска программ;
– создания каталогов;
– установки и удаления пакетов (экспериментальная политика).

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

7.2.1 Развертывание групповых политик

Процесс развёртывание групповых политик:

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

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

   – скачать и установить ADMX-файлы от Microsoft:

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

Примечание По умолчанию, admx-msi-setup устанавливает последнюю версию ADMX от Microsoft (сейчас это Microsoft Group Policy в документе – 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 default value
is /usr/share/ PolicyDefinitions/.
Usage: admx-msi-setup [-d ] [-s ]
Removing admx-msi-setup temporary files...
```

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

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

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

Должен быть установлен пакет alterator-gpupdate: # apt-get install alterator-gpupdate

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

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

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

4. 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 admx-basealt
```

5. Настроить, если это необходимо, RSAT на машине с ОС Windows:
   – 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 установить административные шаблоны (файлы ADMX) и зависящие от языка файлы ADML из репозитория http://git.altlinux.org/gears/a/admx-basealt.git (https://github.com/altlinux/admx-basealt) и разместить их в каталоге: \\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\PolicyDefinitions;
   – корректно установленные административные шаблоны будут отображены на машине Windows в оснастке **Редактор управления групповыми политиками** в разделе **Конфигурация компьютера** > **Политики** > **Административные шаблоны** > **Система ALT**.

7.2.2 Пример создания групповой политики

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** 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
```

Добавление доменных устройств в группу членства GPO:

1. Создать новое подразделение:
   – в контекстном меню домена выбрать пункт **Создать** > **Подразделение**:
   – в открывшемся окне ввести название подразделения (например, OU) и нажать кнопку **ОК**.

2. Переместить компьютеры и пользователей домена в созданное подразделение:
   – в контекстном меню пользователя или компьютера выбрать пункт **Переместить…**;
   – в открывшемся диалоговом окне **Выбор контейнера – ADMC** выбрать контейнер, в который следует переместить учетную запись пользователя.

Создание политики для подразделения:

1. В контекстном меню папки **Объекты групповой политики** выбрать пункт **Создать политику**.
2. В открывшемся окне ввести название политики и нажать кнопку **ОК**.
3. В контекстном меню политики выбрать пункт **Добавить связь…**.
4. Выбрать объекты, которые необходимо связать с политикой и нажать кнопку **ОК**.

Для редактирования настроек групповой политики, необходимо выполнить следующие действия:

1. В контекстном меню созданной политики выбрать пункт **Изменить…**.

2. Откроется окно редактирования групповых политик (GPUI):
3. Перейти в **Компьютер** > **Система ALT**. Здесь есть несколько разделов, соответствующих категориям control. Выбрать раздел **Сетевые приложения**, в правом окне редактора отобразится список политик.
4. Дважды щелкнуть левой кнопкой мыши на политике **Разрешения для /usr/bin/ping**. Откроется диалоговое окно настройки политики. Выбрать параметр **Включено**, в выпадающем списке **Кому разрешено** выбрать пункт **Только root** и нажать кнопку **ОК**.
5. 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
```

В настоящее время GPUI позволяет управлять только политиками, предпочтения пока не реализованы. Для управления предпочтениями могут использоваться средства удаленного администрирования сервера для Windows (RSAT).

Пример создания групповой политики на машине с ОС Windows:

1. На машине с установленным RSAT открыть оснастку **Управление групповыми политиками** (gpmc.msc).
2. Создать новый объект групповой политики (GPO) и связать его с подразделением (OU), в который входят машины или учетные записи пользователей.
3. В контекстном меню GPO, выбрать пункт **Изменить…**. Откроется редактор GPO.
4. Перейти в **Конфигурация компьютера** > **Политики** > **Административные шаблоны** > **Система ALT**. Здесь есть несколько разделов, соответствующих категориям control. Выбрать раздел **Сетевые приложения**, в правом окне редактора отобразится список политик.

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

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.

7.3 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.

7.3.1 Настройка smb.conf

После редактирования файла **/etc/samba/smb.conf**, следует запустить команду testpa rm 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 специальнаяя гостевая учетная запись). Для доступа к разделам, к которым запрещен гостевой доступ, потребуется пароль.

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 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]:

1. **Раздел [global]**. Параметры в этом разделе применяются к серверу в целом или являются значениями по умолчанию для разделов, и могут быть переопределены в разделе.
2. **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.
3. **Раздел [printers]**. Если в файле конфигурации имеется раздел [printers], пользователи могут подключаться к любому принтеру, указанному в файле printcap локального хоста.

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.
```

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).

Флаг **browseable** для домашних каталогов будет унаследован от глобального флага bro **wseable**, 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); p
– **rintable** – 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 = Commonplace
    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

Enter WORKGROUP\user's password:

Sharename   Type  Comment
---------   ----  -------
public      Disk  Public Stuff
Free  Disk
IPC$  IPC   IPC Service (Samba server on smb (v.
4.14.13))
user  Disk  Home Directory for 'user'

SMB1 disabled -- no workgroup available
```

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

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

7.3.2 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, надо установить так, чтобы файл был доступен только владельцу:

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

и принадлежать root:

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

7.4 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.

MAPI over HTTPS не поддерживается

7.4.1 Установка

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

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

7.4.2 Подготовка среды

Подготовить к запуску и настроить службы PostgreSQL:

– создать системные базы данных:

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

– запустить службу:

```
# service postgresql start
```

– создать пользователя sogo и базу данных sogo (под правами root):

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

Настройка Samba DC:

– Пользователи расположены в домене Active Directory, расположенном на контроллере с Samba DC. Необходимо предварительно развернуть сервер Samba AD DC (см. Samba 4 в роли контроллера домена Active Directory).

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

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

Настройка SOGo (настраивается на домен test.alt):

– заполнить файл конфигурации **/etc/sogo/sogo.conf**:

```
{

  SOGoProfileURL = "postgresql://sogo@/sogo/sogo_user_profile";
  OCSFolderInfoURL = "postgresql://sogo@/sogo/sogo_folder_info";
  OCSSessionsFolderURL = "postgresql://sogo@/sogo/sogo_sessions_folder";
  OCSEMailAlarmsFolderURL = "postgresql://sogo@/sogo/sogo_alarms_folder";
  SOGoEnableEMailAlarms = YES;

  SOGoDraftsFolderName = Drafts; SOGoSentFolderName = Sent;
  SOGoTrashFolderName = Trash; SOGoIMAPServer = "imaps://localhost:993/?

tlsVerifyMode=allowInsecureLocalhost";
  SOGoMailingMechanism = sendmail;
  SOGoForceExternalLoginWithEmail = NO; NGImap4ConnectionStringSeparator =
  "/";
  SOGoUserSources = (
    {
        id = sambaLogin;
        displayName = "SambaLogin";
        canAuthenticate = YES;
        type = ldap;
        CNFieldName = cn;
        IDFieldName = cn;
        UIDFieldName = sAMAccountName;
        hostname = "ldaps://127.0.0.1";
        baseDN = "CN=Users,DC=test,DC=alt";
        bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
        bindPassword = "Pa$$word";
        bindFields = (sAMAccountName);
    },

    {
        id = sambaShared;
        displayName = "Shared Addressbook";
        canAuthenticate = NO;
        isAddressBook = YES;
        type = ldap;
        CNFieldName = cn;
        IDFieldName = mail;
        UIDFieldName = mail;
        hostname = "ldaps://127.0.0.1";
        baseDN = "CN=Users,DC=test,DC=alt";
        bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
        bindPassword = "Pa$$word";
        filter = "((NOT isCriticalSystemObject='TRUE') AND (mail='*') AND
        (NOT objectClass=contact))";

    },
```

```
    {
        id = sambaContacts;
        displayName = "Shared Contacts";
        canAuthenticate = NO;
        isAddressBook = YES;
        type = ldap;
        CNFieldName = cn;
        IDFieldName = mail;
        UIDFieldName = mail;
        hostname = "ldaps://127.0.0.1";
        baseDN = "CN=Users,DC=test,DC=alt";
        bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
        bindPassword = "Pa$$word";
        filter = "((((objectClass=person) AND (objectClass=contact) AND
        ((uidNumber>=2000) OR (mail='*')))

                AND (NOT isCriticalSystemObject='TRUE') AND (NOT
showInAdvancedViewOnly='TRUE') AND (NOT uid=Guest))

                OR (((objectClass=group) AND (gidNumber>=2000)) AND (NOT
isCriticalSystemObject='TRUE') AND (NOT showInAdvancedViewOnly='TRUE')))";

        mapping = {

            displayname = ("cn");

        };
    }
 );

 SOGoSieveScriptsEnabled = YES;
 SOGoLanguage = Russian;
 SOGoTimeZone = Europe/Moscow;
 SOGoFirstDayOfWeek = 1;

}
```

– включить службы по умолчанию и перезапустить их:

```
# for s in samba postgresql memcached sogo httpd2;do chkconfig $s
on;service $s restart;done
```

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

7.4.3 Включение веб-интерфейса

Для включения веб-интерфейса необходимо выполнить команды:

```
# a2enmod proxy
# a2enmod proxy_http
# a2enmod authn_core
# a2enmod authn_file
# a2enmod auth_basic
# a2enmod authz_user
# a2enmod env
# a2enmod dav
# a2enmod headers
# a2enmod rewrite
# a2enmod version
# a2enmod setenvif
# a2ensite SOGo
# service httpd2 restart
# service sogo restart
```

Теперь можно войти по адресу:

```
https://<адрес_сервера>/SOGo/
```

Если при входе в веб-интерфейс возникает ошибка «Неправильный логин или пароль» и в логах /var/log/sogo/sogo.log есть ошибки вида:

```
Jul 06 16:14:51 sogod [12257]: [ERROR] <0x0x5578db070b40[LDAPSource]>
Could not bind to the LDAP server ldaps://127.0.0.1 (389) using the bind
DN: CN=sogo,CN=Users,DC=test,DC=alt
```

Следует в файл /etc/openldap/ldap.conf добавить опцию:

```
TLS_REQCERT allow
```

и перезапустить службы samba и sogo:

```
# service samba restart # service sogo restart
```

7.4.4 Настройка электронной почты

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

В примере используется следующая конфигурация:

– имя домена: test.alt;

– размещение почты: **/var/mail/<имя_домена>/<имя_пользователя>** (формат maildir);

– доступ на чтение почты: IMAP (порт 993), SSL;

– доступ на отправку почты: SMTP (порт 465), SSL/STARTTLS;

– данные аутентификации: email с доменом (например, petrov@test.alt) или имя пользователя.

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

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

и перезапустить samba:

```
# service samba restart
```

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
```

7.4.4.1 Настройка Postfix

Установить пакет postfix-ldap:

```
# apt-get install postfix-ldap
```

В каталоге **/etc/postfix** изменить файлы для домена test.alt:

– изменить содержимое файла main.cf:

```
#Global Postfix configuration file.  This file lists only a small subset
#of all parameters.  For the syntax, and for a complete parameter list,
#see the postconf(5) manual page.  For a commented and more complete

#version of this file see /etc/postfix/main.cf.dist

mailbox_command = /usr/libexec/dovecot/dovecot-lda -f "$SENDER" -a
"$RECIPIENT"
inet_protocols = ipv4

# Mappings
virtual_mailbox_base = /var/mail
virtual_mailbox_domains = test.alt
virtual_mailbox_maps = ldap:/etc/postfix/ad_local_recipients.cf
virtual_alias_maps = ldap:/etc/postfix/ad_mail_groups.cf
virtual_transport = dovecot
local_transport = virtual
local_recipient_maps = $virtual_mailbox_maps

# SSL/TLS
smtpd_use_tls = yes
smtpd_tls_security_level = encrypt
#smtpd_tls_security_level = may
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain = test.alt
smtpd_sasl_path = private/auth
smtpd_sasl_type = dovecot
smtpd_sender_login_maps = ldap:/etc/postfix/ad_sender_login.cf
smtpd_tls_auth_only = yes
smtpd_tls_cert_file = /var/lib/ssl/certs/dovecot.cert smtpd_tls_key_file
= /var/lib/ssl/private/dovecot.key smtpd_tls_CAfile
= /var/lib/ssl/certs/dovecot.pem
smtpd_recipient_restrictions = permit_mynetworks,
reject_unauth_destination, per-mit_sasl_authenticated, reject
smtpd_sender_restrictions = reject_authenticated_sender_login_mismatch
```

– файл **/etc/postfix/mydestination** должен быть пустым;

– файл **master.cf** необходимо добавить строки:

```
dovecot unix - n n - - pipe flags=DRhu user=mail:mail
argv=/usr/libexec/dovecot/deliver -d $

{recipient}
smtps inet  n     -     n     -     -     smtpd
-o smtpd_tls_wrappermode=yes
-o smtpd_sasl_auth_enable=yes
-o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

– создать файл ad_local_recipients.cf:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
scope = sub
query_filter = (&(|(mail=%s)(otherMailbox=%u@%d))
(sAMAccountType=805306368))
result_filter = %s
result_attribute = mail
special_result_attribute = member
bind = yes
bind_dn = cn=vmail,cn=users,dc=test,dc=alt bind_pw = Pa$$word
```

– создать файл ad_mail_groups.cf:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
timeout = 3
scope = sub
query_filter = (&(mail=%s)(sAMAccountType=268435456))
result_filter = %s
result_attribute = mail
special_result_attribute = member
bind = yes
bind_dn = cn=vmail,cn=users,dc=test,dc=alt bind_pw = Pa$$word
```

– создать файл ad_sender_login.cf:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
scope = sub
query_filter = (&(objectClass=user)(|(sAMAccountName=%s)(mail=%s)))
result_attribute = mail

bind = yes
bind_dn = cn=vmail,cn=users,dc=test,dc=alt bind_pw = Pa$$word
```

– перезапустить службу postfix:

```
# service postfix restart
```

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

```
# postconf >/dev/null
```

Проверка пользователя почты petrov:

```
# postmap -q petrov@test.alt ldap:/etc/postfix/ad_local_recipients.cf
petrov@test.alt
```

Проверка входа:

```
# postmap -q petrov@test.alt ldap:/etc/postfix/ad_sender_login.cf
petrov@test.alt
```

Проверка общего адреса e-mail:

```
# samba-tool group add --mail-address=sales@test.alt Sales
Added group Sales
# samba-tool group addmembers Sales ivanov,petrov
Added members to group Sales
# postmap -q sales@test.alt ldap:/etc/postfix/ad_mail_groups.cf
sales@test.alt,ivanov@test.alt,petrov@test.al
```

7.4.4.2 Настройка Dovecot

Установить Dovecot:

```
# apt-get install dovecot
```

Изменить файлы для домена test.alt:

– создать файл /**etc/dovecot/dovecot-ldap.conf.ext**:

```
hosts = test.alt:3268
ldap_version = 3
auth_bind = yes
dn = cn=vmail,cn=Users,dc=test,dc=alt
dnpass = Pa$$word
base = cn=Users,dc=test,dc=alt
scope = subtree
deref = never

user_filter = (&(objectClass=user)(|(mail=%Lu)(sAMAccountName=%Lu)))
user_attrs = =uid=8,gid=12,mail=user
pass_filter = (&(objectClass=user)(|(mail=%Lu)(sAMAccountName=%Lu)))
pass_attrs = mail=user
```

– изменить файл /etc/dovecot/conf.d/10-auth.conf:

```
#auth_username_format = %Lu
#auth_gssapi_hostname = "$ALL"
#auth_krb5_keytab = /etc/dovecot/dovecot.keytab
#auth_use_winbind = no
#auth_winbind_helper_path = /usr/bin/ntlm_auth
#auth_failure_delay = 2 secs
auth_mechanisms = plain
!include auth-ldap.conf.ext
```

– изменить файл /etc/dovecot/conf.d/10-mail.conf:

```
mail_location = maildir:/var/mail/%d/%n:UTF-8:INBOX=/var/mail/%d/%n/Inbox
mail_uid = mail
mail_gid = mail
first_valid_uid = 5
first_valid_gid = 5
```

– изменить файл /etc/dovecot/conf.d/10-master.conf

```
service imap-login {
  inet_listener imap {
    port = 0
  }
  inet_listener imaps {
  }
}
service pop3-login {
  inet_listener pop3 {
    port = 0
  }
  inet_listener pop3s {
    port = 0
  }
}
service lmtp {
  unix_listener lmtp {
  }
}
service imap {
}
service pop3 {
}
service auth {
  unix_listener auth-userdb {
  }
  unix_listener /var/spool/postfix/private/auth {
    mode = 0600
    user = postfix
    group = postfix
  }
}
service auth-worker {
}
service dict {
  unix_listener dict {
  }
}
```

– изменить файл /etc/dovecot/conf.d/15-lda.conf:

```
protocol lda {
  hostname = test.alt
  postmaster_address = administrator@test.alt
}
```

– изменить файл /etc/dovecot/conf.d/15-mailboxes.conf:

```
namespace inbox {
  inbox = yes
  mailbox Drafts {
    auto = subscribe
    special_use = \Drafts
}
  mailbox Junk {
    auto = subscribe
    special_use = \Junk
}
  mailbox Trash {
    auto = subscribe
    special_use = \Trash
}
  mailbox Sent {
    auto = subscribe
    special_use = \Sent
}
  mailbox "Sent Messages" {
    special_use = \Sent
  }
}
```

– перезапустить службу dovecot:

```
# service dovecot restart
```

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

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

7.4.4.3 Безопасность

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

```
# chown dovecot:root /etc/dovecot/dovecot-ldap.conf.ext
# chmod 0640 /etc/dovecot/dovecot-ldap.conf.ext
# chown root:postfix /etc/postfix/ad_local_recipients.cf /etc/postfix/
ad_mail_groups.cf /etc/postfix/ad_sender_login.cf
# chmod 0640 /etc/postfix/ad_local_recipients.cf /etc/postfix/
ad_mail_groups.cf /etc/postfix/ad_sender_login.cf
```

Перезапустить службы:

```
# service dovecot restart
# service postfix restart
```

7.4.4.4 Проверка конфигурации

Проверка SMTP:

```
# date | mail -s test petrov@test.alt
# mailq
Mail queue is empty
```

Проверка IMAP (выход по Ctrl+D):

```
# openssl s_client -crlf -connect test.alt:993
...
tag login petrov@test.alt Pa$$word tag OK [CAPABILITY IMAP4rev1 LITERAL+
SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES
THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL CATENATE UNSELECT
CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC
ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE]
Logged in
```

7.5 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.

7.5.1 Установка сервера FreeIPA

В качестве примера показана установка сервера **FreeIPA** со встроенным DNS сервером и доменом EXAMPLE.TEST в локальной сети 192.168.0.0/24.

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

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

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

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

Задать имя сервера:

```
# hostnamectl set-hostname ipa.example.test
```

Запустить скрипт настройки сервера. В пакетном режиме:

```
# ipa-server-install -U --hostname=$(hostname) -r EXAMPLE.TEST -n
example.test -p 12345678 -a 12345678 --setup-dns --no-forwarders --no-
reverse
```

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 1234
```

Или интерактивно:

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

Пароли должны быть не менее 8 символов.

Обратите внимание на ответ на вопрос, не совпадающий с предложенным:

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

остальные вопросы необходимо выбрать по умолчанию (можно просто нажать Enter). Так же при установке необходимо ввести пароль администратора системы и пароль администратора каталогов.

Для возможности управлять **FreeIPA** сервером из командной строки необходимо получить билет Kerberos:

```
# kinit admin
```

Добавить в DNS запись о сервере времени:

```
# ipa dnsrecord-add example.test _ntp._udp --srv-priority=0 --srv-
weight=100 --srv-port=123 --srv-target=ipa.example.test.
```

Проверить работу ntp сервера можно командой:

```
# ntpdate -q localhost
server 127.0.0.1, stratum 3, offset 0.000018, delay 0.02568
27 Nov 10:27:00 ntpdate[29854]: adjust time server 127.0.0.1 offset
0.000018 sec
```

Веб-интерфейс доступен по адресу **https://ipa.example.test/ipa/ui/**.

7.5.2 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/** и ввести данные администратора для входа в систему.

После успешной авторизации можно создать нового пользователя домена. Для этого в окне Пользователи домена необходимо нажать кнопку **Добавить**.

В открывшемся окне необходимо ввести данные пользователя и нажать кнопку **Добавить**.

Созданный пользователь появится в списке пользователей:

7.5.3 Установка FreeIPA клиента и подключение к серверу

7.5.3.1 Установка FreeIPA клиента

Установить необходимые пакеты:

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

Очистить конфигурацию freeipa-client невозможно. В случае если это необходимо (например, для удаления, переустановки freeipa-client) следует переустановить систему.

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:

1. В Центре управления системой в разделе **Сеть** > **Ethernet интерфейсы** задать имя компьютера, IP-адрес FreeIPA сервера и в поле **Домены поиска** – домен для поиска.
2. 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 в документе – IP-адрес FreeIPA сервера
   – указать службе resolvconf использовать DNS FreeIPA и домен для поиска. Для этого в файле /**etc/resolvconf.conf** добавить/отредактировать следующие параметры:

```
interface_order='lo lo[0-9]* lo.* eth0'
search_domains=example.test
```

где eth0 в документе – интерфейс на котором доступен FreeIPA сервер, example.test в документе – домен;

– обновить DNS адреса:

```
# resolvconf -u
```

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

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

7.5.3.2 Подключение к серверу в ЦУС

Для ввода рабочей станции в домен FreeIPA, необходимо в Центре управления системой перейти в раздел **Пользователи** > **Аутентификация**.

В открывшемся окне следует выбрать пункт **Домен FreeIPA**, заполнить поля **Домен** и **Имя компьютера**, затем нажать кнопку **Применить**.

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

В случае успешного подключения, будет выведено соответствующее сообщение.

Перезагрузить рабочую станцию.

7.5.3.3 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: comp01.example.test
Realm: EXAMPLE.TEST
DNS Domain: example.test
IPA Server: ipa.example.test
BaseDN: dc=example,dc=test
Continue to configure the system with these values? [no]:
```

Необходимо ответить yes, ввести имя пользователя, имеющего право вводить машины в домен, и его пароль.

Если при входе в домен возникает такая ошибка:

```
Hostname (comp01.example.test) does not have A/AAAA record.
Failed to update DNS records.
```

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

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

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

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

```
# control sudo public
```

7.5.3.4 Вход пользователя

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

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
```

7.5.4 Настройка репликации

На втором контроллере домена необходимо установить пакеты:

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

Задать имя сервера:

```
# hostnamectl set-hostname ipabackup.example.test
```

Развернуть и настроить клиента:

```
# ipa-client-install -d --domain=example.test --server=ipa.example.test --
realm=EXAMPLE.TEST --principal=admin --password=12345678 --enable-dns-
updates -U
```

После выполнения этой операции хост ipabackup.example.test должен появиться в вебинтерфейсе FreeIPA.

Далее необходимо настроить репликацию LDAP-каталога:

```
# ipa-replica-install
```

Добавить в DNS второй NTP-сервер:

```
# kinit admin
# ipa dnsrecord-add example.test _ntp._udp --srv-priority=0 --srv-
weight=100 --srv-port=123 --srv-target=ipabackup.example.test.
```

Настроить репликацию DNS-зон:

```
# ipa-dns-install
```

Настроить репликацию CA:

```
# ipa-ca-install
```

После настройки и репликации контроллеров посмотреть топологию можно в веб-интерфейсе FreeIPA.

7.6 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; с

– лужба 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.

7.6.1 Установка и настройка Fleet Commander

7.6.1.1 Настройка libvirt-хоста

В качестве libvirt-хоста может выступать как отдельная машина, так и машина с Fleet Commander Admin.

Установить libvirt:

```
# apt-get install libvirt virt-install
```

Добавить службу libvirtd в автозапуск и запустить её:

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

Проверить, что default сеть определена, запущена и автозапускаемая:

```
#virsh net-list --all

Имя         Статус      Автозапуск  Persistent

----------------------------------------------

default     активен     yes         yes
```

Определить сеть default, если она не определена:

```
# virsh net-define /usr/share/libvirt/networks/default.xml
```

Отметить default сеть как автозапускаемую:

```
# virsh net-autostart default
```

Запустить default сеть:

```
# virsh net-start default
```

В ОС Альт Сервер по умолчанию отключена парольная аутентификация для root в sshd, поэтому если есть необходимость использовать привилегированного пользователя libvirtхоста, то следует разрешить root-доступ по ssh. Включить парольную аутентификацию для root можно с помощью control (должен быть установлен пакет control-sshd-permit-rootlogin):

```
# 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:

1. 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-x86_64.iso
```

2. Подключиться к ВМ и произвести установку ОС:

```
$ virt-viewer --connect qemu+ssh://user@192.168.0.190/system
```

3. После окончания установки ОС, установить на ВМ Fleet Commander Logger:

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

ВМ, которую планируется использовать как шаблон, должна быть выключена, иначе Fleet Commander не позволит запустить live-сессию на этой машине.

7.6.1.2 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.
```

Пакет freeipa-desktop-profile не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p10. О добавлении репозиториев с использованием графических приложений вы можете почитать в документ «Операционная система Альт Сервер. Руководство по установке».

Проверить, что плагин работает:

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

Если на выходе команды ipa deskprofileconfig-show появляется ошибка:

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

необходимо почистить кэш текущему пользователю и повторить команду:

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

Установить Fleet Commander плагин для Cockpit (из репозитория):

```
# apt-get install fleet-commander-admin 1
```

Пакет fleet-commander-admin не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p10. О добавлении репозиториев с использованием графических приложений вы можете почитать в в документ «Операционная система Альт Сервер. Руководство по установке».

Добавить сервис Cockpit в автозапуск и запустить его:

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

Веб-интерфейс Cockpit будет доступен по адресу https**://адрес-сервера:9090/**.

Вход осуществляется по логину указанному при установке FreeIPA сервера. Для доступа к настройке Fleet Commander следует выбрать соответствующую кнопку на левой панели веб-интерфейса.

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

Открыть окно настроек можно, нажав кнопку **Settings** на вкладке **Fleet Commander**.

Fleet Commander позволяет установить глобальную политику для определения того, как применять несколько профилей: к конкретному пользователю, к группе, к хосту, к группе хостов. По умолчанию это **User-Group-Host-Hostgroup**.

Для запуска live-сессии необходимо работающее ssh-соединение с libvirt-хостом. В форму настройки необходимо ввести следующие данные:

– **Fleet Commander virtual environment host** – адрес libvirt-хоста (если в качестве libvirtхоста используется FreeIPA сервер, то здесь необходимо указать адрес текущей машины или localhost);
– **Username for connection** – имя пользователя libvirt-хоста;
– **Libvirt mode** – если пользователь не является привилегированным, то следует переключить данную настройку в режим сеанса.

Fleet Commander генерирует свой собственный открытый ключ, который необходимо добавить в **.ssh/authorized_keys** для соответствующего пользователя на libvirt-хосте. Это можно сделать, нажав кнопку **Install public key (Установить открытый ключ)**, при этом будет необходимо ввести пароль пользователя. Пароль используется только для установки ключа и нигде не хранится.

На хосте libvirt, должен быть запущен SSH-сервер (служба sshd).

7.6.1.2.1 Работа с профилями

После настройки Fleet Commander Admin необходимо создать и настроить профиль. Для создания профиля нажать кнопку Add Profile на вкладке Fleet Commander. Появится форма настройки профиля.

Форма настройки профиля содержит следующие поля:

– **Name** – имя профиля;

– **Description** – описание профиля;

– **Priority** – приоритет профиля;

– **Users** – пользователи, к которым будет применен профиль;

– **Groups** – группы, к которым будет применен профиль;

– **Hosts** – хосты, к которым будет применен профиль;

– **Host groups** – группы хостов, к которым будет применен профиль.

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

7.6.1.3 Настройка шаблона

Для настройки шаблона в веб-интерфейсе Cockpit необходимо нажать кнопку **Edit** напротив нужного профиля и в открывшемся окне нажать кнопку **Live session.**

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

7.6.1.4 Установка и настройка Fleet Commander Client

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

Установить необходимый пакет (из репозитория):

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

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

7.6.2 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:

1. Открыть https://адрес-сервера:9090/fleet-commander-admin и запустить live-сессию (Edit → Live session). Появится окно со списком доступных ВМ, которые можно использовать в качестве шаблона для загрузки в live-сессии.
2. Выбрать машину, на которой установлен Fleet Commander Logger, и запустить ее. Загруженная машина является шаблоном, все сделанные на ней изменения будут отловлены регистратором, сохранены и применены на клиентских системах.
3. На загруженной машине внести необходимые изменения в настройки.
4. В веб-интерфейсе Cockpit нажать кнопку **Review and submit**. Появится окно со списком сделанных изменений. В списке изменений можно выбрать как все изменения, так и частичные, установив отметку напротив нужного. После выбора нажать кнопку Save, для сохранения изменений.
5. Загрузить клиентскую машину, войти в систему под доменным пользователем. Убедиться, что сделанные изменения успешно применились.

При закрытии вкладки браузера с Cockpit, live-сессия прервется и изменения, внесенные за время ее существования, будут потеряны.

7.6.3 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**.

7.7 Zabbix

Zabbix – система мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования.

Для управления системой мониторинга и чтения данных используется веб-интерфейс.

7.7.1 Установка сервера PostgreSQL

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

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

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

Пакеты zabbix-server-pgsql и fping не входят в состав ISO-образа дистрибутива, их можно установить из репозитория p10. О добавлении репозиториев с использованием графических приложений вы можете почитать в разделе в документ «Операционная система Альт Сервер. Руководство по установке».

Подготовить к запуску и настроить службы PostgreSQL, для этого необходимо выполнить следующие действия:

– создать системные базы данных:

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

– включить по умолчанию и запустить службу:

```
# chkconfig postgresql on
# service postgresql start
```

– создать пользователя zabbix и базу данных zabbix (под правами root):

```
# su - postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --
no-createrole --encrypted --pwprompt zabbix'
# su - postgres -s /bin/sh -c 'createdb -O zabbix zabbix'
# service postgresql restart
```

– добавить в базу данные для веб-интерфейса (последовательность команд важна, в разных версиях Zabbix путь будет отличаться, версия помечена звёздочкой):

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

7.7.2 Установка Apache2

Установить необходимые пакеты:

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

Добавить в автозапуск и запустить apache2:

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

7.7.3 Установка PHP

Установить необходимые пакеты:

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

Изменить некоторые опции php в файле /etc/php/7.4/apache2-mod_php/php.ini (версия PHP может быть другой):

```
memory_limit = 256M
post_max_size = 32M
max_execution_time = 600
max_input_time = 600
date.timezone = Europe/Moscow
always_populate_raw_post_data = -1
```

Перезапустить apache2:

```
# service httpd2 restart
```

7.7.4 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:

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

7.7.5 Установка веб-интерфейса Zabbix

Установить метапакет (из репозитория):

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

Включить аддоны в apache2:

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

Перезапустить apache2:

```
# service httpd2 restart
```

Изменить права доступа к конфигурационному каталогу веб-интерфейса, чтобы веб-установщик мог записать конфигурационный файл:

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

Если устанавливается Zabbix4, команда будет такой:

```
# chown apache2:apache2 /var/www/webapps/zabbix/frontends/php/conf
```

В браузере перейти на страницу установки Zabbix сервера: **http://<ip-сервера>/zabbix**.

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

На странице также можно выбрать язык установки Zabbix.

Если при входе на страницу http:///zabbix появляется ошибка: доступ запрещен, следует в файле **/etc/httpd2/conf/sites-available/default.conf** в секцию добавить запись:

```
Require all granted
```

перезапустить apache2:

```
# service httpd2 restart
```

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

Здесь необходимо ввести параметры подключения к базе данных (параметры подключения нужно указывать такие же, как у сервера Zabbix). По умолчанию в качестве Database schema необходимо указать public.

Если выбрана опция **TLS шифрование базы данных**, то в форме появятся дополнительные поля для настройки TLS-соединения с базой данных.

На следующих страницах необходимо задать имя сервера, выбрать настройки веб-интерфейса и завершить установку.

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

```
Логин: Admin
Пароль: zabbix
```

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

В профиле пользователя можно настроить некоторые функции веб-интерфейса Zabbix, такие как язык интерфейса, цветовая тема, количество отображаемых строк в списках и т.п. Сделанные в профиле изменения будут применены только к пользователю, в профиле которого были сделаны эти изменения.

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

7.7.6 Установка клиента Zabbix

Установить необходимый пакет zabbix-agent (из репозитория):

```
# apt-get install zabbix-agent
```

Если Zabbix-агент устанавливается не на сам сервер мониторинга, то в файле конфигурации агента **/etc/zabbix/zabbix_agentd.conf** нужно задать следующие параметры:

```
Server=<ip сервера>
ServerActive=<ip сервера>
Hostname=comp01.example.test
```

comp01.example.test – имя узла мониторинга, которое будет указано на сервере Zabbix.

Если параметр Hostname будет пустой или закомментирован, то узел добавится под системным именем.

Добавить Zabbix-агент в автозапуск и запустить его:

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

7.7.7 Добавление нового хоста на сервер Zabbix

Каждый хост необходимо зарегистрировать на сервере Zabbix, сделать это можно, используя веб-интерфейс.

Информация о настроенных узлах сети в Zabbix доступна в **Настройка** > **Узлы сети**. Для добавления нового узла сети следует нажать кнопку **Создать узел сети**.

В открывшемся окне необходимо заполнить поля **Имя узла сети** и **IP адрес** согласно данным добавляемого хоста. Затем следует добавить хост в определенную группу, выбрав одну из них из списка, либо создав новую группу.

В поле **Имя узла сети** ставится значение, которое указано в настройках агента (/etc/zabbix/zabbix_agentd.conf) в поле **Hostname**.

Все права доступа назначаются на группы узлов сети, не индивидуально узлам сети. Поэтому узел сети должен принадлежать хотя бы одной группе.

Перейти на вкладку **Шаблоны**, выбрать шаблон **Linux by Zabbix agent** и нажать кнопку **Добавить**.

Получение первых данных может занять до 60 секунд. Для того чтобы просмотреть собранные данные необходимо перейти в **Мониторинг** > **Последние данные**, выбрать в фильтре нужный узел сети и нажать кнопку **Применить**.

7.7.8 Авторегистрация узлов

В Zabbix существует механизм, который позволяет Zabbix-серверу начинать мониторинг нового оборудования автоматически, если на этом оборудовании имеется установленный Zabbix-агент. Такой подход позволяет добавлять новые узлы сети на мониторинг без какой-либо настройки Zabbix-сервера вручную по каждому отдельному узлу сети.

Для настройки авторегистрации, перейти в **Настройка** > **Действия** > **Действия авторегистрации** и нажать кнопку **Создать действие**.

На открывшейся странице, на вкладке **Действия** заполнить поле **Имя** и добавить условия. В поле **Условия** следует задать правила, по которым будут идентифицироваться регистрируемые хосты.

На вкладке **Операции** в поле **Операции** следует добавить правила, которые необходимо применить при регистрации хоста.

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.

7.8 Сервер видеоконференций на базе Jitsi Meet

Jitsi Meet – веб-приложение с открытым исходным кодом на базе WebRTC, предназначенное для проведения видеоконференций. Сервер Jitsi Meet создает виртуальные залы для видеоконференций на несколько человек, для доступа к которым требуется только браузер. Преимущество конференции Jitsi заключается в том, что все данные передаются только через ваш сервер, а комплексное шифрование TLS обеспечивает защиту от перехвата и несанкционированного прослушивания.

Jicofo – XMPP-компонент, модератор видеоконференций. Клиенты договариваются о связи, заходя в общую XMPP-комнату, и обмениваются там XMPP-сообщениями. Имеет HTTP API / about/health для опроса о состоянии сервиса.

Jitsi Videobridge – механизм медиасервера, который поддерживает все многосторонние видеоконференции Jitsi. Он передаёт видео и аудио между участниками, осуществляя роль посредника, терминирует RTP/RTCP, определяет доступные рамки битрейта в обе стороны на конкретного клиента. Имеет свой внутренний HTTP API для мониторинга (/colibri/debug).

Jigasi – шлюз для участия в Jitsi-конференциях через SIP-телефонию.

Jibri – вещатель и рекордер, используемые для сохранения записей видеозвонков и потоковой передачи на YouTube Live.

Ниже приведена инструкция по настройке сервера Jitsi Meet в ОС Альт Сервер.

7.8.1 Требования к системе

Для размещения нужны:

– jitsi-videobridge: хост с доступными портами 10000/udp, 4443/tcp и хорошей пропускной способностью (рекомендуется минимум 100Mbps симметрично);
– веб-сервер: хост с доступным портом 443/tcp. Веб-сервер должен поддерживать HTTPS;
– xmpp-сервер: хост с доступным портом 5280/tcp для работы XMPP-over-HTTP (BOSH).

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.

7.8.2 Установка

Установить пакеты:

```
# apt-get install prosody jitsi-meet-prosody jitsi-meet-web jitsi-meet-
webconfig jicofo jitsi-videobridge
```

Компоненты Jitsi Meet можно установить при установке системы, выбрав для установки пункт «Сервер видеоконференций Jitsi Meet» (см. документ «Операционная система Альт Сервер. Руководство по установке»).

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

7.8.3 Конфигурация

7.8.3.1 Настройка имени хоста системы

Установить имя хоста системы на доменное имя, которое будет использоваться для Jitsi:

```
# hostnamectl set-hostname jitsi2
```

Установить локальное сопоставление имени хоста сервера с IP-адресом 127.0.0.1, для этого дописать в файл **/etc/hosts** строку:

```
127.0.0.1 jitsi2.test.alt jitsi2
```

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 [...]
```

7.8.3.2 Настройка XMPP-сервера (prosody)

Создать каталог /etc/prosody/conf.d для хранения пользовательских конфигураций:

```
# mkdir -p /etc/prosody/conf.d
```

В конец файла /etc/prosody/prosody.cfg.lua дописать строку:

```
Include "conf.d/*.cfg.lua"
```

Создать конфигурационный файл prosody для вашего домена (например, **/etc/prosody/conf.d/jitsi2.test.alt.cfg.lua**) со следующим содержимым:

```
plugin_paths = { "/usr/share/jitsi-meet/prosody-plugins/" }
-- domain mapper options, must at least have domain base set to use the
mapper
muc_mapper_domain_base = "jitsi2.test.alt";
cross_domain_bosh = false;
consider_bosh_secure = true;
----------- Virtual hosts -----------
VirtualHost "jitsi2.test.alt"
 authentication = "anonymous"
 ssl = {
 key = "/var/lib/prosody/jitsi2.test.alt.key";
 certificate = "/var/lib/prosody/jitsi2.test.alt.crt";
 }
 speakerstats_component = "speakerstats.jitsi2.test.alt"
 conference_duration_component = "conferenceduration.jitsi2.test.alt"
 -- we need bosh
modules_enabled = {
 "bosh";
 "pubsub";
 "ping"; -- Enable mod_ping
 "speakerstats";
 "turncredentials";
 "conference_duration";
 }
 c2s_require_encryption = false
Component "conference.jitsi2.test.alt" "muc"
 storage = "memory"
 modules_enabled = {
 "muc_meeting_id";
 "muc_domain_mapper";
 -- "token_verification";
 }
```

```
 admins = { "focus@auth.jitsi2.test.alt" }
 muc_room_locking = false
 muc_room_default_public_jids = true
VirtualHost "auth.jitsi2.test.alt"
 ssl = {
 key = "/var/lib/prosody/auth.jitsi2.test.alt.key";
 certificate = "/var/lib/prosody/auth.jitsi2.test.alt.crt";
 }
 authentication = "internal_plain"
-- internal muc component, meant to enable pools of jibri and jigasi
clients
Component "internal.auth.jitsi2.test.alt" "muc"
 storage = "memory"
 modules_enabled = {
 "ping";
 }
 admins = { "focus@auth.jitsi2.test.alt", "jvb@auth.jitsi2.test.alt" }
 muc_room_locking = false
 muc_room_default_public_jids = true
Component "focus.jitsi2.test.alt"
 component_secret = "secret1" -- достаточно длинный пароль, он же
JICOFO_SECRET
Component "speakerstats.jitsi2.test.alt" "speakerstats_component"
 muc_component = "conference.jitsi2.test.alt"
Component "conferenceduration.jitsi2.test.alt"
"conference_duration_component"
 muc_component = "conference.jitsi2.test.alt"
```

Сгенерировать сертификаты для виртуальных хостов jitsi2.test.alt и auth.jitsi2.test.alt:

```
# prosodyctl cert generate jitsi2.test.alt
# prosodyctl cert generate auth.jitsi2.test.alt
```

Зарегистрировать сертификаты в системе, как доверенные (сертификаты нужно регистрировать там, где устанавливается Jicofo):

```
# ln -s /var/lib/prosody/jitsi2.test.alt.crt /etc/pki/ca-trust/source/
anchors/
# ln -s /var/lib/prosody/auth.jitsi2.test.alt.crt /etc/pki/ca-trust/source/
anchors/
# update-ca-trust
```

Зарегистрировать пользователя focus (аккаунт focus@auth.jitsi2.test.alt):

```
# prosodyctl register focus auth.jitsi2.test.alt secret2
```

где secret2 – достаточно длинный пароль.

Запустить prosody:

```
# prosodyctl start
```

7.8.3.3 Настройка jicofo

Jicofo подключается к XMPP-серверу и как внешний XMPP-компонент, и как пользовательский аккаунт с JID focus@auth.jitsi2.test.alt.

В файле **/etc/jitsi/jicofo/config** следует указать:

```
# Jitsi Conference Focus settings
# sets the host name of the XMPP server

JICOFO_HOST=localhost
# sets the XMPP domain (default: none)
JICOFO_HOSTNAME=jitsi2.test.alt
# sets the secret used to authenticate as an XMPP component
JICOFO_SECRET=secret1
# overrides the prefix for the XMPP component domain. Default: "focus"
#JICOFO_FOCUS_SUBDOMAIN=focus
# sets the port to use for the XMPP component connection
JICOFO_PORT=5347
# sets the XMPP domain name to use for XMPP user logins
JICOFO_AUTH_DOMAIN=auth.jitsi2.test.alt
# sets the username to use for XMPP user logins
JICOFO_AUTH_USER=focus
# sets the password to use for XMPP user logins
JICOFO_AUTH_PASSWORD=secret2
# extra options to pass to the jicofo daemon
JICOFO_OPTS="${JICOFO_FOCUS_SUBDOMAIN:+ --
subdomain=$JICOFO_FOCUS_SUBDOMAIN}"
# adds java system props that are passed to jicofo (default are for home
and logging config file)
JAVA_SYS_PROPS="-
Dnet.java.sip.communicator.SC_HOME_DIR_LOCATION=/etc/jitsi
-Dnet.java.sip.communicator.SC_HOME_DIR_NAME=jicofo
-Dnet.java.sip.communicator.SC_LOG_DIR_LOCATION=/var/log/jitsi
-Djava.util.logging.config.file=/etc/jitsi/jicofo/logging.properties"
```

В строке `JICOFO_SECRET=secret1` должен быть указан пароль, установленный в файле /etc/prosody/conf.d/jitsi2.test.alt.cfg.lua.

В строке `JICOFO_AUTH_PASSWORD=secret2` должен быть указан пароль пользователя focus.

В файле /etc/jitsi/jicofo/sip-communicator.properties следует указать:

```
org.jitsi.jicofo.health.ENABLE_HEALTH_CHECKS=true
org.jitsi.jicofo.BRIDGE_MUC=JvbBrewery@internal.auth.jitsi2.test.alt
```

Запустите jicofo:

```
# systemctl start jicofo
```

Убедитесь, что jicofo подключается к XMPP-серверу:

```
# curl -i localhost:8888/about/health
HTTP/1.1 500 Internal Server Error
Date: Wed, 04 May 2022 10:02:05 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.

7.8.3.4 Настройка jitsi-videobridge

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

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

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

```
#Jitsi Videobridge settings

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


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

строке `password = "secret3"` должен быть указан пароль пользователя jvb.

Вместо слова shard можно использовать любой идентификатор (оно идентифицирует подключение к xmpp-серверу и jicofo). Измените содержимое файла /etc/jitsi/videobridge/sip-communicator.properties:

```
org.ice4j.ice.harvest.DISABLE_AWS_HARVESTER=true
org.ice4j.ice.harvest.STUN_MAPPING_HARVESTER_ADDRESSES=meet-jit-
siturnrelay.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.jit
s i2.test.alt org.jitsi.videobridge.xmpp.user.shard.MUC_NICKNAME=6d8b40cb-
fe32-49f5- a5f6-13d2c3f95bba
```

Если JVB-машина отделена от клиентов при помощи NAT, то потребуется донастройка.

Запустите JVB:

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

Убедитесь, что между JVB и jicofo есть связь:

```
# curl -i localhost:8888/about/health
HTTP/1.1 200 OK
Date: Wed, 04 May 2022 10:06:04 GMT
Content-Length: 0
Server: Jetty(9.4.15.v20190215)
```

Если всё сделано правильно, jicofo на healthcheck-запрос будет отдавать HTTP-код 200.

7.8.3.5 Настройка веб-приложения Jitsi Meet

Получить SSL/TLS-сертификат для домена.

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 вебсервера (*.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.exampleapache /etc/httpd2/conf/sites-available/jitsi2.test.alt.conf
```

Внести изменения в файл /etc/httpd2/conf/sites-available/jitsi2.test.alt.conf (изменить имя, указать сертификат):

```
<VirtualHost *:80>

ServerName jitsi2.test.alt
Redirect permanent / https://jitsi2.test.alt/
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L] </VirtualHost>

<VirtualHost *:443>
ServerName jitsi2.test.alt

SSLProtocol TLSv1 TLSv1.1 TLSv1.2
SSLEngine on
SSLProxyEngine on
SSLCertificateFile /etc/jitsi/meet/jitsi2.test.alt.crt
SSLCertificateKeyFile /etc/jitsi/meet/jitsi2.test.alt.key SSLCipherSuite
"EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA256:EECDH+aRSA+SHA256:
E
ECDH+ECDSA+SHA384:EECDH+ECDSA+SHA256:EECDH+aRSA+SHA384:EDH+aRSA+AESGCM:EDH+
a
RSA+SHA256:EDH+aRSA:EECDH:!aNULL:!eNULL:!MEDIUM:!LOW:!3DES:!MD5:!EXP:!PSK:!
SRP:!DSS:!RC4:!SEED"
SSLHonorCipherOrder on
Header set Strict-Transport-Security "max-age=31536000"'

DocumentRoot "/usr/share/jitsi-meet"
<Directory "/usr/share/jitsi-meet">
Options Indexes MultiViews Includes FollowSymLinks AddOutputFilter Includes
html AllowOverride All
Order allow,deny
Allow from all
</Directory>

ErrorDocument 404 /static/404.html

Alias "/config.js" "/etc/jitsi/meet/jitsi2.test.alt-config.js"
<Location /config.js>
Require all granted
</Location>

Alias "/external_api.js" "/usr/share/jitsi-meet/libs/external_api.min.js"
<Location /external_api.js>
Require all granted
</Location>
ProxyPreserveHost on
ProxyPass /http-bind http://localhost:5280/http-bind/
ProxyPassReverse /http-bind http://localhost:5280/http-bind/

RewriteEngine on
RewriteRule ^/([a-zA-Z0-9]+)$ /index.html
</VirtualHost>
```

Установить пакет apache2-mod_ssl, если он еще не установлен:

```
# apt-get install apache2-mod_ssl
```

Выполнить команды:

```
# a2enmod rewrite
# a2enmod ssl
# a2enmod headers
# a2enmod proxy
# a2enmod proxy_http
# a2enport https
# a2dissite 000-default
```

Включить конфигурацию Apache:

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

Запустить веб-сервер Apache2 и добавить его в автозагрузку:

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

7.8.4 Работа с сервисом

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

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.

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 вебпортала, генератор по умолчанию с этим справляется. Можно предотвратить неавторизованное создание новых конференций подробнее в Отключение возможности неавторизованного создания новых конференций.

Ввести название конференции и нажать кнопку **ОК**. Будет создана конференция.

После создания конференции браузер попросит дать ему разрешение на использование веб-камеры и микрофона

После создания конференции её администратором становится только тот, кто её создал. Администратор может удалять пользователей из конференции, выключать их микрофоны, давать пользователю слово. В случае если администратор покинул конференцию, то её администратором становится тот, кто подключился следующий после него.

Конференция существует до тех пор, пока в ней есть хотя бы один человек.

Внизу окна конференции находится панель управления. Первая кнопка на панели управления кнопка **Показать экран**. Если нажать на эту кнопку, откроется окно, в котором можно выбрать, что будет демонстрироваться другим участникам конференции. Доступны следующие опции:

– экран монитора;

– окно приложения;

– определённая вкладка браузера.

Нажатие на кнопку **Хочу говорить** сигнализирует организатору, что участник хочет говорить. В окне, соответствующем персонажу (справа), появится такой же значок ладони.

Кнопка **Чат** запускает чат в данной конференции.

Следующие кнопки на панели управления и их назначение:

– **Микрофон** – позволяет включать и отключать микрофон;

– **Завершить** – выход из конференции;

– **Камера** – включение и выключение веб-камеры;

– **Вкл/Выкл плитку** – вывести окна собеседников в центр чата;

– **Информация о чате** – всплывающее окно, в котором приведена ссылка на конференцию. Здесь же администратор конференции может установить пароль для доступа к конференции;

– **Больше** – настройка дополнительных функций Jitsi Meet:

7.8.5 Отключение возможности неавторизованного создания конференций

Можно разрешить создавать новые конференции только авторизованным пользователям. При этом каждый раз, при попытке создать новую конференцию, Jitsi Meet запросит имя пользователя и пароль. После создания конференции другие пользователи смогут присоединиться к ней анонимно.

Для отключения возможности неавторизованного создания новых конференций, необходимо выполнить следующие действия:

– отредактировать файл /etc/prosody/conf.d/jitsi2.test.alt.cfg.lua, изменив в нем запись:

```
VirtualHost "jitsi2.test.alt"
authentication = "anonymous"
```

на:

```
VirtualHost "jitsi2.test.alt"
authentication = "internal_hashed"
```

– добавить в конец файла /etc/prosody/conf.d/jitsi2.test.alt.cfg.lua строки:

```
VirtualHost "guest.jitsi2.test.alt"
authentication = "anonymous"
c2s_require_encryption = false
```

Эти настройки позволят анонимным пользователям присоединяться к конференциям, созданным пользователем, прошедшим аутентификацию. При этом у гостя должен иметься уникальный адрес и пароль конференции (если этот пароль задан);

– в файле /etc/jitsi/meet/jitsi2.test.alt-config.js указать параметры анонимного домена:

```
domain: 'jitsi2.test.alt',
anonymousdomain: 'guest.jitsi2.test.alt',
```

– в файл /etc/jitsi/jicofo/sip-communicator.properties добавить строку:

```
org.jitsi.jicofo.auth.URL=XMPP:jitsi2.test.alt
```

– перезапустить процессы Jitsi Meet для загрузки новой конфигурации:

```
# prosodyctlt restart
# systemctl restart jicofo
# systemctl restart jitsi-videobridge
```

Команда для регистрации пользователей:

```
prosodyctl register <ПОЛЬЗОВАТЕЛЬ> jitsi2.test.alt <ПАРОЛЬ>
```

Изменить пароль пользователя:

```
prosodyctl passwd <ПОЛЬЗОВАТЕЛЬ>
```

Удалить пользователя:

```
prosodyctl deluser <ПОЛЬЗОВАТЕЛЬ>
```

Например, создадим пользователя admin:

```
# prosodyctl register admin jitsi2.test.alt secret4
```

Теперь при создании конференции сервер Jitsi Meet будет требовать ввести имя пользователя и пароль.

7.9 Отказоустойчивый кластер (High Availability) на основе Pacemaker

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

– обнаружение и восстановление сбоев на уровне узлов и сервисов;
– возможность гарантировать целостность данных путем ограждения неисправных узлов;
– поддержка одного или нескольких узлов на кластер;
– поддержка нескольких стандартов интерфейса ресурсов (все, что может быть написано сценарием, может быть кластеризовано);
– независимость от подсистемы хранения – общий диск не требуется;
– поддержка и кворумных и ресурсозависимых кластеров; а
– втоматически реплицируемая конфигурация, которую можно обновлять с любого узла;

– возможность задания порядка запуска ресурсов, а также их совместимости на одном узле;
– поддерживает расширенные типы ресурсов: клоны (когда ресурс запущен на множестве узлов) и дополнительные состояния (master/slave и подобное);
– единые инструменты управления кластером с поддержкой сценариев.

Архитектура Pacemaker представляет собой три уровня:

– кластеронезависимый уровень – на этом уровне располагаются ресурсы и их скрипты, которыми они управляются и локальный демон, который скрывает от других уровней различия в стандартах, использованных в скриптах;
– менеджер ресурсов (Pacemaker) –□реагирует на события, происходящие в кластере: отказ или присоединение узлов, ресурсов, переход узлов в сервисный режим и другие административные действия. Pacemaker, исходя из сложившейся ситуации, делает расчет наиболее оптимального состояния кластера и дает команды на выполнение действий для достижения этого состояния (остановка/перенос ресурсов или узлов);
– информационный уровень (Corosync) – на этом уровне осуществляется сетевое взаимодействие узлов, т.е. передача сервисных команд (запуск/остановка ресурсов, узлов и т.д.), обмен информацией о полноте состава кластера (quorum) и т.д.

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

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

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

Ниже приведена инструкция по установке и настройке кластера в ОС Альт Сервер.

7.9.1 Настройка узлов кластера

Для функционирования отказоустойчивого кластера необходимо, чтобы выполнялись следующие требования:

– дата и время между узлами в кластере должны быть синхронизированы;
– должно быть обеспечено разрешение имён узлов в кластере;
– сетевые подключения должны быть стабильными;
– у узлов кластера для организации изоляции узла (fencing) должны присутствовать функции управления питанием/перезагрузкой с помощью IPMI(ILO);
– следующие порты могут использоваться различными компонентами кластеризации: TCPпорты 2224, 3121 и 21064 и UDP-порт 5405 и должны быть открыты/доступны.

В примере используется следующая конфигурация:

– node01 – первый узел кластера (IP 192.168.0.113/24);
– node02 –второй узел кластера (IP 192.168.0.145/24);
– node03 – третий узел кластера (IP 192.168.0.132/24);
– 192.168.0.251 – виртуальный IP по которому будет отвечать один из узлов.

Дальнейшие действия следует выполнить на всех узлах кластера.

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

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

7.9.1.1 Настройка разрешений имён узлов

Следует обеспечить взаимно-однозначное прямое и обратное преобразование имён для всех узлов кластера. Желательно использовать DNS, в крайнем случае, можно обойтись соответствующими записями в локальных файлах /etc/hosts на каждом узле:

```
# echo "192.168.0.113 node01" >> /etc/hosts
# echo "192.168.0.145 node02" >> /etc/hosts
# echo "192.168.0.132 node03" >> /etc/hosts
```

Проверка правильности разрешения имён:

```
# ping node01
PING node01 (192.168.0.113) 56(84) bytes of data.
64 bytes from node01 (192.168.0.113): icmp_seq=1 ttl=64 time=0.352 ms
# ping node02
PING node02 (192.168.0.145) 56(84) bytes of data.
64 bytes from node02 (192.168.0.145): icmp_seq=1 ttl=64 time=0.635 ms
```

7.9.1.2 Настройка ssh-подключения между узлами

При настройке ssh-подключения для root по ключу необходимо убрать комментарии в файле /etc/openssh/sshd_config для строк:

```
PermitRootLogin without-password
PubkeyAuthentication yes
AuthorizedKeysFile /etc/openssh/authorized_keys/%u /etc/openssh/
authorized_keys2/%u .ssh/authorized_keys .ssh/authorized_keys2
PasswordAuthentication yes
```

Кроме того, полезно добавить в /etc/openssh/sshd_config директиву:

```
AllowGroups sshusers
```

создать группу sshusers:

```
# groupadd sshusers
```

и добавить туда пользователей, которым разрешено подключаться по ssh:

```
# gpasswd -a <username> sshusers
```

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

```
# systemctl restart sshd
```

Создать новый ключ SSH без пароля (параметр -N):

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

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

Скопировать публичную часть SSH-ключа на другие узелы кластера:

```
# ssh-copy-id -i ~/.ssh/id_ed25519.pub user@node02
# ssh-copy-id -i ~/.ssh/id_ed25519.pub user@node03
```

В результате получаем возможность работы с домашними каталогами пользователя user удалённого узла – копировать к себе и от себя, удалять, редактировать и т.д.

Скопировать публичную часть SSH-ключа на все узлы кластера для администратора. Для этого подключиться к каждому узлу и под root скопировать публичную часть ключа:

```
# ssh user@node02
user@node02 $ su -
node02 # cat /home/user/.ssh/authorized_keys >> /root/.ssh/authorized_keys
node02 # exit
user@node02 $ exit
```

Каталог /root/.ssh при этом должен существовать.

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

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

7.9.2 Установка кластерного ПО и создание кластера

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

Установить на всех узлах необходимые пакеты:

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

Данные пакеты не входят в состав ISO-образа дистрибутива, их можно установить из репозитория p10. О добавлении репозиториев с использованием графических приложений вы можете почитать в разделе в документ «Операционная система Альт Сервер. Руководство по установке».

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

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

Пакет pcs (pacemaker/corosync configuration system) в документе – утилита для управления, настройки и мониторинга кластера. Управляется как через командную строку, так и через веб-интерфейс.

При установке Pacemaker автоматически будет создан пользователь hacluster. Для использования pcs, а также для доступа в веб-интерфейс нужно задать пароль пользователю hacluster (одинаковый на всех узлах):

```
# passwd hacluster
```

Запустить и добавить в автозагрузку службу pcsd:

```
# systemctl enable --now pcsd
```

Настроить аутентификацию (на одном узле):

```
# pcs host auth node01 node02 node03 -u hacluster
Password:
node02: Authorized
node01: Authorized
node03: Authorized
```

После этого кластером можно управлять с одного узла.

Создать кластер:

```
# pcs cluster setup newcluster node01 node02 node03
Destroying cluster on hosts: 'node01', 'node02', 'node03'...
node03: Successfully destroyed cluster
node01: Successfully destroyed cluster
node02: Successfully destroyed cluster
Requesting remove 'pcsd settings' from 'node01', 'node02', 'node03'
node01: successful removal of the file 'pcsd settings'
node03: successful removal of the file 'pcsd settings'
node02: successful removal of the file 'pcsd settings'
Sending 'corosync authkey', 'pacemaker authkey' to 'node01', 'node02',
'node03'
node01: successful distribution of the file 'corosync authkey'
node01: successful distribution of the file 'pacemaker authkey'
node03: successful distribution of the file 'corosync authkey'
node03: successful distribution of the file 'pacemaker authkey'
node02: successful distribution of the file 'corosync authkey'
node02: successful distribution of the file 'pacemaker authkey'
Sending 'corosync.conf' to 'node01', 'node02', 'node03'
node01: successful distribution of the file 'corosync.conf'
node02: successful distribution of the file 'corosync.conf'
node03: successful distribution of the file 'corosync.conf'
Cluster has been successfully set up.
```

Запустить кластер:

```
# pcs cluster start --all
node02: Starting Cluster...
node03: Starting Cluster...
node01: Starting Cluster...
```

Настройка автоматического включения кластера при загрузке:

```
# pcs cluster enable --all
node01: Cluster Enabled
node02: Cluster Enabled
node03: Cluster Enabled
```

Проверка состояния кластера:

```
# pcs status cluster
Cluster Status:
 Cluster Summary:
 * Stack: corosync
 * Current DC: node02 (version 2.1.2-alt1-ada5c3b36) - partition with
quorum
 * Last updated: Mon Jun 20 15:28:32 2022
 * Last change: Mon Jun 20 15:27:55 2022 by hacluster via crmd on node02
 * 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
```

Веб-интерфейс управления кластером по адресу https://<имя-компьютера>:2224 (в качестве имени компьютера можно использовать имя или IP-адрес одного из узлов в кластере).

Потребуется пройти аутентификацию (логин и пароль учётной записи hacluster).

После входа в систему на главной странице отображается страница «Управление кластерами». На этой странице перечислены кластеры, которые в настоящее время находятся под управлением веб-интерфейса. При выборе кластера отображается информация о кластере.

Чтобы добавить существующий кластер в веб-интерфейс, необходимо нажать кнопку **Add Existing** и в открывшемся окне ввести имя или IP-адрес любого узла в кластере.

7.9.3 Настройка параметров кластера

Настройки кластера можно просмотреть, выполнив команду:

```
# pcs property
Cluster Properties:
 cluster-infrastructure: corosync
 cluster-name: newcluster
 dc-version: 2.1.2-alt1-ada5c3b36
 have-watchdog: false
```

7.9.3.1 Кворум

Кворум определяет минимальное число работающих узлов в кластере, при котором кластер считается работоспособным. По умолчанию, кворум считается неработоспособным, если число работающих узлов меньше половины от общего числа узлов.

Отключить эту политику, например, если узла всего два, можно выполнив команду:

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

7.9.3.2 Настройка STONITH

Для корректной работы узлов с общим хранилищем, необходимо настроить механизм STONITH.

Этот механизм позволяет кластеру физически отключить не отвечающий на запросы узел, чтобы не повредить данные на общем хранилище.

Отключить STONITH, пока он не настроен можно, выполнив команду:

```
# pcs property set stonith-enabled=false
```

⚠ 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.

7.9.4 Настройка ресурсов

Настроим ресурс, который будет управлять виртуальным IP-адресом. Этот адрес будет мигрировать между узлами, предоставляя одну точку входа к ресурсам, заставляя работать несколько узлов как одно целое устройство для сервисов.

Команда создания ресурса виртуального IP-адреса с именем ClusterIP с использованием алгоритма ресурсов ocf (каждые 20 секунд производить мониторинг работы, в случае выхода из строя узла необходимо виртуальный IP переключить на другой узел):

```
# pcs resource create ClusterIP ocf:heartbeat:IPaddr2 ip=192.168.0.251
cidr_netmask=24 op monitor interval=20s
```

Для того чтобы добавить ресурс в веб-интерфейсе, необходимо перейти на вкладку RESOURCES, нажать кнопку Add и задать параметры ресурса.

Список доступных стандартов ресурсов:

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

Список доступных поставщиков сценариев ресурсов OCF:

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

Список всех агентов ресурсов, доступных для определённого поставщика OCF:

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

Статус кластера, с добавленным ресурсом:

```
# pcs status
Cluster name: newcluster
Cluster Summary:
 * Stack: corosync
 * Current DC: node02 (version 2.1.2-alt1-ada5c3b36) - partition with
quorum
 * Last updated: Mon Jun 20 15:36:19 2022
 * Last change: Mon Jun 20 15:35:55 2022 by root via cibadmin on node01
 * 3 nodes configured
 * 1 resource instance configured
Node List:
 * Online: [ node01 node02 node03 ]
Full List of Resources:
 * ClusterIP (ocf::heartbeat:IPaddr2): Started node01
Daemon Status:
 corosync: active/enabled
 pacemaker: active/enabled
 pcsd: active/enabled
```

Если остановить кластер на узле node01:

```
# pcs cluster stop node01
node01: Stopping Cluster (pacemaker)...
node01: Stopping Cluster (corosync)...
```

ClusterIP начнёт работать на node02 (переключение произойдёт автоматически). Проверка статуса на узле node02:

```
# pcs status
Cluster name: newcluster
Cluster Summary:
 * Stack: corosync
 * Current DC: node02 (version 2.1.2-alt1-ada5c3b36) - partition with
quorum
 * Last updated: Mon Jun 20 15:58:38 2022
 * Last change: Mon Jun 20 15:35:55 2022 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
```

7.10 OpenUDS

OpenUDS это многоплатформенный брокер подключений для создания и управления виртуальными рабочими местами и приложениями.

Основные компоненты решения VDI на базе OpenUDS:

– OpenUDS Server (openuds-server) в документе – брокер подключений пользователей, а так же интерфейс администратора для настройки.
– SQL Server. Для работы django-приложения, которым является openuds-server, необходим SQL сервер, например mysql или mariadb. SQL Server может быть установлен как на отдельном сервере, так и совместно с openuds-server.
– Платформа для запуска клиентских окружений и приложений. OpenUDS совместима со множеством систем виртуализации: PVE, OpenNebula, oVirt, OpenStack. Так же возможно использование с отдельным сервером без виртуализации (аналог терминального решения).
– OpenUDS Client (openuds-client) в документе – клиентское приложение для подключения к брокеру соединений и дальнейшего получения доступа к виртуальному рабочему окружению.
– OpenUDS Tunnel (openuds-tunnel) в документе – 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) в документе – ПО для гостевых виртуальных машин, реализует связку виртуальной машины и брокера соединений.

7.10.1 Установка

7.10.1.1 Установка mysql/mariadb

Установить MySQL (MariaDB):

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

Запустить сервер mariadb и добавить его в автозагрузку:

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

Задать пароль root для mysql и настройки безопасности:

```
# mysql_secure_installation
```

Создать базу данных dbuds, пользователя базы данных dbuds с паролем password и предоставить ему привилегии в базе данных dbuds:

```
$ mysql -u root -p
Enter password:
MariaDB> CREATE DATABASE dbuds CHARACTER SET utf8 COLLATE utf8_general_ci;
MariaDB> CREATE USER 'dbuds'@'%' IDENTIFIED BY 'password';
MariaDB> GRANT ALL PRIVILEGES ON dbuds.* TO 'dbuds'@'%';
MariaDB> FLUSH PRIVILEGES;
MariaDB> exit;
```

7.10.1.2 Установка OpenUDS Server

OpenUDS Server можно установить при установке системы, выбрав для установки пункт Сервер виртуальных рабочих столов OpenUDS (подробнее описано в документе «Операционная система Альт Сервер. Руководство по установке»).

При этом будут установлены:

– openuds-server в документе – django приложение;

– gunicorn в документе – сервер приложений (обеспечивает запуск django как стандартного WSGI приложения);

– nginx в документе – http-сервер, используется в качестве reverse-proxy для доступа к django приложению, запущенному с помощью gunicorn.

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
```

Веб-интерфейс OpenUDS будет доступен по адресу https://адрес-сервера/:

Имя/пароль по умолчанию: root/udsmam0.

Для получения доступа к панели администрирования OpenUDS, следует в меню пользователя выбрать пункт **Панель управления**.

7.10.2 Настройка OpenUDS

7.10.2.1 Поставщики услуг

В разделе Поставщики услуг (Services) подключить один из поставщиков («Service providers»):

– Поставщик платформы Proxmox (PVE Platform Provider).

– Поставщик платформы OpenNebula (OpenNebula Platform Provider).

– Отдельный сервер без виртуализации: Поставщик машин статических IP (Static IP Machine Provider).

7.10.2.1.1 OpenNebula

Минимальные параметры для настройки Поставщик платформы OpenNebula: название, IPадрес сервера OpenNebula (поле Хост), порт подключения, имя пользователя (с правами администратора) и пароль.

Используя кнопку **Проверить**, можно убедиться, что соединение установлено правильно.

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

Выбрав пункт **Обслуживание (Maintenance)**, можно приостановить все операции, выполняемые сервером OpenUDS для данного поставщика услуг. Поставщик услуг рекомендуется переводить в режим обслуживания в случаях, когда связь с этим поставщиком была потеряна или запланирован перерыв в обслуживании.

В открывшемся окне, на вкладке **Постащики услуг (Services)** нажать кнопку **Новый** > **Действующие образы OpenNebula**.

Заполнить минимальные параметры конфигурации:

– Вкладка **Основной (Main)**:

- **Имя** в документе – название службы;
- **Хранилище** в документе – место, где будут храниться сгенерированные виртуальные рабочие столы.

– Вкладка **Машина (Machine)**:

- **Базовая машина** в документе – шаблон ВМ, используемый системой OpenUDS для развертывания виртуальных рабочих столов (см. Подготовка шаблона виртуальной машины);
- **Имена машин** в документе – базовое название для клонов с этой машины (например, Desk-work-);
- **Длина имени** в документе – 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).

7.10.2.1.2 PVE

Минимальные параметры для настройки Поставщика платформы Proxmox: название поставщика, IP-адрес/имя сервера или кластера PVE (поле Хост), порт подключения, имя пользователя с достаточными привилегиями в PVE (в формате пользователь@аутентификатор) и пароль.

Используя кнопку **Проверить**, можно убедиться, что соединение установлено правильно.

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

Выбрав пункт Обслуживание (Maintenance), можно приостановить все операции, выполняемые сервером OpenUDS для данного поставщика услуг. Поставщик услуг рекомендуется переводить в режим обслуживания в случаях, когда связь с этим поставщиком была потеряна или запланирован перерыв в обслуживании.

В открывшемся окне, на вкладке Поставщики услуг (Services) нажать кнопку **Новый** > **Связанный клон Proxmox**.

Заполнить минимальные параметры конфигурации:

– Вкладка **Основной (Main)**:

- **Имя** в документе – название службы;

- **Пул** в документе – пул, в котором будут находиться ВМ, созданные OpenUDS;
- **Высокая доступность** в документе – включать созданные ВМ в группу HA PVE.

– Вкладка **Машина (Machine)**:

- **Базовая машина** в документе – шаблон ВМ, используемый системой OpenUDS для развертывания виртуальных рабочих столов (см. Подготовка шаблона виртуальной машины);
- **Хранилище** в документе – место, где будут храниться сгенерированные виртуальные рабочие столы (поддерживаются хранилища, позволяющие создавать «Снимки»);
- **Имена машин** в документе – базовое название для клонов с этой машины (например, Desk-kwork-);
- **Длина имени** в документе – количество цифр счетчика, прикрепленного к базовому имени рабочих столов (например, если Длина имени = 3, названия сгенерированных рабочих столов будут: Desk-kwork-000, Desk-kwork-001 ... Desk-kwork-999).

После того, как среда OpenUDS будет настроена и будет создан первый «пул услуг», в среде PVE можно будет наблюдать, как разворачиваются рабочие столы. Сначала будет создан шаблон («UDS-Publication-pool_name-publishing-number») в документе – клон ВМ, выбранной при регистрации службы. После завершения процесса создания клона будут созданы рабочие столы («Machine_Name-Name_Length»):

7.10.2.1.3 Удалённый доступ к отдельному серверу

В OpenUDS есть возможность предоставить доступ к постоянным устройствам (физическим или виртуальным). Доступ к отдельному серверу осуществляется путем назначения IP-адресов пользователям.

Для регистрации поставщика данного типа следует в разделе Поставщики услуг нажать кнопку **Новый** и выбрать пункт **Поставщик машин статических IP**.

Для настройки **Поставщика машин статических IP** достаточно задать название поставщика.

Для создания базовых услуг **Поставщика машин статических IP** следует дважды щелкнуть мышью по строке созданного поставщика или в контекстном меню поставщика выбрать пункт **Подробность (Detail)**. В открывшемся окне, на вкладке **Поставщики услуг (Services)** нажать кнопку **Новый** > **Статический множественный IP-адрес** или **Новый** > **Статический одиночный IP-адрес**.

OpenUDS позволяет создавать два типа услуг **Поставщика машин статических IP**.

Статический множественный IP-адрес

Используется для подключения одного пользователя к одному компьютеру. Поддерживается неограниченное количество IP-адресов (можно включить в список все устройства, которые должны быть доступны удалённо). По умолчанию система будет предоставлять доступ к устройствам в порядке очереди (первый пользователь получивший доступ к этому пулу, получает доступ к машине с первым IP-адресом из списка). Также можно настроить выборочное распределение, чтобы определённому пользователю назначался определенный компьютер (IPадрес).

Для настройки привязки конкретного пользователя к конкретному IP необходимо в разделе Пулы услуг для созданной услуги на вкладке Назначенные сервисы нажать кнопку **Назначить услугу** и задать привязку пользователя устройству.

Статический одиночный IP-адрес

Используется для подключения нескольких пользователей к одному компьютеру. При обращении каждого нового пользователя будет запускаться новый сеанс. Параметры конфигурации для услуги **Статический множественный IP-адрес**:

– Вкладка **Основной**:

- **Имя** в документе – название службы;
- **Список серверов** в документе – один или несколько IP-адресов машин, к которым будет осуществляться доступ (машины должны быть включены и настроены см. Подготовка шаблона виртуальной машины).

– Вкладка **Расширенный**:

- **Проверить порт** в документе – порт, по которому система может проверить, доступен ли компьютер. Если компьютер не доступен, система автоматически предоставит следующее устройство в списке. 0 в документе – не проверять доступность компьютера;
- **Пропустить время** в документе – период, в течение которого не будет проверяться доступность недоступной машины.

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 на вкладке **Назначенные сервисы**.

Параметры конфигурации для услуги **Статический одиночный IP-адрес**:

– **Имя** в документе – название службы;

– **IP-адрес машины** в документе – IP-адрес машины, к которой будет осуществляться доступ (машина должна быть включена и настроена см. Подготовка шаблона виртуальной машины).

7.10.2.2 Настройка аутентификации пользователей

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

7.10.2.2.1 Внутренняя БД

При аутентификации **Внутренняя БД** данные пользователей и групп хранятся в базе данных, к которой подключен сервер OpenUDS.

Для создания аутентификации типа **Внутренняя БД** в разделе **Аутентификаторы** следует нажать кнопку: **Новый** > **Внутренняя БД**.

Минимальные параметры конфигурации (вкладка Основной): имя аутентификатора, приоритет и метка.

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.

7.10.2.2.2 Аутентификатор Regex LDAP

Этот аутентификатор позволяет пользователям и группам пользователей, принадлежащих практически любому аутентификатору на основе LDAP, получать доступ к виртуальным рабочим столам и приложениям.

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

7.10.2.2.2.1 FreeIPA

Настройка интеграции с FreeIPA (сервер ipa.example.test):

1. В разделе Аутентификаторы нажать кнопку: Новый → Аутентификатор Regex LDAP.
2. Заполнить поля первых трёх вкладок.
   – Вкладка **Основной**: имя аутентификатора, приоритет, метка, IP-адрес FreeIPA-сервера, порт (обычно 389 без ssl, 636 с ssl);
   – Вкладка **Учётные данные**: имя пользователя (в формате uid=user_freeipa,cn=users,cn=accounts,dc=example,dc=test) и пароль;
   – Вкладка **LDAP** информация: общая база пользователей, класс пользователей LDAP, идентификатор атрибута пользователя, атрибут имени пользователя, атрибут имени группы.

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**.

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.

7.10.2.2.2.2 Active Directory

Настройка аутентификации в Active Directory (домен test.alt):

1. В разделе **Аутентификаторы** нажать кнопку: Новый > Аутентификатор Regex LDAP.
2. Заполнить поля первых трёх вкладок.
   – Вкладка **Основной**: имя аутентификатора, приоритет, метка, IP-адрес сервера AD, порт (обычно 389 без ssl, 636 с ssl):
   – Вкладка **Учётные данные**: имя пользователя (можно указать в виде имя@домен) и пароль:
   – Вкладка **LDAP информация**: общая база пользователей, класс пользователей LDAP, идентификатор атрибута пользователя, атрибут имени пользователя, атрибут имени группы:

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**.

Заполнить dn существующей группы (например, cn=Users,cn=Builtin,dc=test,dc=alt), можно также указать разрешённые пулы/

7.10.2.2.2.3 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.

После того, как аутентификатор типа «IP аутентификатор» создан, следует создать группы пользователей. Группа может представлять собой диапазон IP-адресов (192.168.0.1-192.168.0.55), подсеть (192.168.0.0/24) или отдельные IP-адреса (192.168.0.33,192.168.0.110):

7.10.2.2.3 Настройка менеджера ОС

Менеджер ОС запускает ранее настроенные службы.

OpenUDS Actor, размещенный на виртуальном рабочем столе, отвечает за взаимодействие между ОС и OpenUDS Server на основе конфигурации или выбранного типа Менеджера ОС.

Для каждой службы, развернутой в OpenUDS, потребуется **Менеджер ОС**, за исключением случаев, когда используется **Поставщик машин статических IP**.

Linux ОС менеджер используется для виртуальных рабочих столов на базе Linux. Он выполняет задачи переименования и управления сеансами виртуальных рабочих столов.

Windows Basic ОС менеджер используется для виртуальных рабочих столов на базе Windows, которые не являются частью домена AD.

Минимальные настройки для Linux ОС менеджер и Windows Basic ОС менеджер:

– **Имя (Name)** в документе – название;

– **Действие при выходе из системы (Logout Action)** в документе – действие, которое OpenUDS будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя. **Держать сервис привязанным (Keep service assigned)** в документе – постоянный пул, при выходе пользователя (выключении ВМ), ВМ запускается заново, при повторном входе пользователю будет назначен тот же рабочий стол. **Удалить сервис (Remove service)** в документе – непостоянный пул, при выходе пользователя из системы, ВМ удаляется и создается заново. **Держать сервис привязанным даже в новой публикации (Keep service assigned even on new publication)** в документе – сохранение назначенной службы даже при создании новой публикации;
– **Максимальное время простоя (Max. Idle time)** в документе – 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.

7.10.2.2.4 Транспорт

Для подключения к виртуальным рабочим столам необходимо создать транспорт. Транспорт в документе –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:

– **Прямой (Direct)** в документе – используется, если пользователь имеет доступ к виртуальным рабочим столам из внутренней сети (например, LAN, VPN и т.д.);
– **Туннельный (Tunneled)** в документе – используется, если у пользователя нет прямого подключения к рабочему столу.

RDP (прямой)

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 конфигурации для настройки транспорта RDP:

– Вкладка **Основной (Main)**:

- **Имя** в документе – название транспорта;
- **Приоритет** в документе – 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** в документе – разрешает или запрещает доступ пользователей к службе, в зависимости от сети из которой осуществляется доступ;
- **Сети** в документе – сетевые диапазоны, подсети или IP-адреса (настраиваются в разделе Сети). Пустое поле означает «все сети». Используется вместе с параметром **Сетевой доступ**;
- **Разрешенные устройства** в документе – разрешает доступ к службе только с выбранных устройств. Пустое поле означает «все устройства»;
- **Пулы** в документе – 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 (Credentials)**:

- **Пропустить данные аккаунта** в документе – 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** в документе – имя пользователя, которое будет использоваться для доступа к рабочему столу (пользователь должен существовать на ВМ). Если данное поле пустое, будет использован логин авторизовавшегос в веб-интерфейсе OpenUDS пользователя;
- **Пароль** в документе – пароль пользователя, указанного в поле Имя пользователя;
- **Без домена** в документе – указывает, перенаправляется ли доменное имя вместе с пользователем. Значение **Да** равносильно пустому полю **Домен**;
- **Домен** в документе – домен. Если поле не пустое, то учётные данные будут использоваться в виде DOMAIN\user.

– На вкладке **Параметры (Parameters)** можно разрешить/запретить перенаправления дисков, принтеров и других устройств/
– На вкладке **Экран/Дисплей (Display)** настраиваются параметры окна рабочего стола:
– Вкладка **Linux Client**:
- **Мультимедийная синхронизация** в документе – включает параметр мультимедиа на клиенте FreeRDP;
- **Использовать Alsa** в документе – использовать звук через Alsa;
- **Перенаправить домашнюю папку** в документе – перенаправить домашнюю папку клиента подключения на виртуальный рабочий стол;
- **Строка принтера** в документе – принтер, используемый клиентом FreeRDP (если включено перенаправление принтера). Названия подключенных принтеров можно вывести командой **lpstat -a**;
- **Строка Smartcard** в документе –токен, используемый клиентом FreeRDP (если включено перенаправление смарт-карт);
- **Пользовательские параметры** в документе – здесь можно указать любой параметр, поддерживаемый клиентом FreeRDP.

X2Go (прямой)

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 конфигурации для настройки транспорта X2Go:

– Вкладка **Основной (Main)**:
- **Имя** в документе – название транспорта;
- **Приоритет** в документе – 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** в документе – разрешает или запрещает доступ пользователей к службе, в зависимости от сети из которой осуществляется доступ;
- **Сети** в документе – сетевые диапазоны, подсети или IP-адреса (настраиваются в разделе **Сети**). Пустое поле означает «все сети». Используется вместе с параметром **Сетевой доступ**;

- **Разрешенные устройства** в документе – разрешает доступ к службе только с выбранных устройств. Пустое поле означает «все устройства»;
- **Пулы** в документе – 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 (Credentials)**:

- **Имя пользователя** в документе – имя пользователя, которое будет использоваться для доступа к рабочему столу (пользователь должен существовать на ВМ). Если данное поле пустое, будет использован логин авторизовавшегос в веб-интерфейсе OpenUDS пользователя;

– Вкладка **Параметры (Parameters)**:

- **Размер экрана** в документе – размер окна рабочего стола;
- **Экран** в документе – менеджер рабочего стола (Xfce, Mate и др.) или виртуализация приложений Linux (UDS vAPP);
- **vAPP** в документе – полный путь до приложения (если в поле Экран выбрано значение UDS vAPP);
- **Перенаправить домашнюю папку** в документе – перенаправить домашнюю папку клиента подключения на виртуальный рабочий стол (на Linux также перенаправлять /media);
- **Скорость** в документе – скорость подключения.

– Вкладка **Расширенный (Advanced)**:

- **Звук** в документе – тип звукового сервера;
- **Клавиатура** в документе – раскладка клавиатуры.

7.10.2.2.5 Пулы услуг

После того, как был создан и настроен хотя бы один поставщик («Service provider») с соответствующей службой/услугой, аутентификатор (с пользователем и группой), менеджер ОС и транспорт, можно создать пул услуг («Service Pool») для публикации виртуальных рабочих столов.

В разделе Сервис-пулы (Service Pool) нажать кнопку **Новый (New)**.

Заполнить параметры конфигурации:

– Вкладка **Основной (Main)**:

- **Имя** в документе – название службы;
- **Базовый сервис** в документе – выбрать службу, созданная ранее в поставщике услуг;
- **ОС Менеджер** в документе – выбрать, созданный ранее, менеджер ОС;
- **Публиковать при создании** в документе – публиковать пул при создании или вручную.

– Вкладка **Экран/Дисплей (Display)**:

- **Видимый** в документе – если этот параметр отключен, пул не будет отображаться у пользователей;
- **Привязанный образ** в документе – изображение, связанное с услугой. Изображение должно быть предварительно добавлено в репозиторий изображений (раздел **Инструменты** > **Галерея**);
- **Пул-группа** в документе –позволяет группировать различные службы. Группа должна быть предварительно создана в разделе **Пулы** > **Группа**.

– Вкладка **Доступность (Availability)**:

- **Первоначально доступные сервисы** в документе – минимальное количество виртуальных рабочих столов, созданных, настроенных и назначенных/доступных для службы;
- **Сервисы для удержания в кэше** в документе – количество доступных виртуальных рабочих мест. Эти ВМ всегда будут настроены и готовы к назначению пользователю (они будут автоматически создаваться до тех пор, пока не будет достигнуто максимальное количество машин, указанное в поле **Максимальное количество предоставляемых сервисов**);
- **Максимальное количество предоставляемых сервисов** в документе – максимальное количество виртуальных рабочих столов, созданных системой в данном пуле (рабочие столы, созданные в кэше L2, не учитываются).

Нажать кнопку **Сохранить** и система начнет создавать виртуальные рабочие столы на основе настроенного кеша.

После создания пула, в настройках (дважды щелкнуть мышью по строке созданного пула или в контекстном меню пула выбрать пункт **Подробность**):

– на вкладке **Группы** назначить группы доступа (выбрать аутентификатор и группу, которая будет иметь доступ к этому пулу служб);
– на вкладке **Транспорты** выбрать способы подключения пользователей к рабочему столу.

7.10.3 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.

7.10.3.1 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** 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 (Зарегистрироваться в UDS)**.

– на вкладке **Advanced** можно указать дополнительные параметры, в том числе уровень журналирования. Для применения настроек указанных на этой вкладке необходимо выполнить перерегистрацию UDSActor.

4. 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
```

7.10.3.2 Шаблон ВМ с ОС Windows

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).

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 в документе – **Удаленный рабочий стол**.
3. Ползунок **Включить удаленный рабочий стол** установить в положение **Вкл**.
4. Выбрать учетные записи, которым разрешено удаленное подключение. Для этого нажать ссылку **Выберите пользователей**, **которые могут получить доступ к этому компьютеру** и добавить пользователей.
5. Проверить возможность подключения к машине удаленно.

Для возможности подключения клиентов Linux может потребоваться снять отметку с пункта Требовать **использование компьютерами аутентификации на уровне сети для подключения** в дополнительных параметрах.

Необходимо убедиться, что межсетевой экран не блокирует соединения по 3389 порту.

Настройка OpenUDS Actor:

1. Загрузить OpenUDS Actor. Для этого в панели управления OpenUDS Server выбрать пункт **Загрузить** (пункт доступен пользователям с правами администратора) и на открывшейся странице выбрать нужный UDS Actor.

Для машин с ОС Windows есть два вида OpenUDS Actor:

– openUDS-Managed_Installer в документе – для управляемых управляемых Windows машин;
– openUDS-Unmanaged_Installer в документе – 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**.
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 (Зарегистрироваться в UDS)**;
   – для регистрации Unmanaged OpenUDS Actor необходимо указать имя или IP-адрес сервера OpenUDS, тот же ключ, который был указан при настройке услуги **Статический множественный IP-адрес** и нажать кнопку **Save Configuration (Сохранить конфигурацию)**.

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**.
Если оставить поле **Ключ услуги** пустым, сеанс останется назначенным
пользователю, пока администратор не удалит его вручную.

7.10.4 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.

7.10.4.1 Клиент с ОС Альт

На клиенте должен быть установлен пакет openuds-client:

```
# apt-get install openuds-client
```

Для возможности подключения к виртуальному рабочему столу, должны быть установлены клиенты протоколов удаленного доступа (xfreerdp, x2goclient).

7.10.4.2 Клиент 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.
2. Установить OpenUDS Client (установка ничем не отличается от инсталляции большинства других программ в ОС Windows).

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.

Для установки клиента X2Go на ОС Windows достаточно загрузить клиент X2Go и установить его.

7.10.5 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.

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

После выбора пула, автоматически стартует OpenUDS Client, который обрабатывает URL, получает необходимые настройки протокола удаленного доступа для предоставленной (свободной) ВМ, формирует файл описания сессии и передает его приложению-клиенту удалённого доступа, которое и устанавливает соединение с указанной ВМ. Как только соединение будет установлено, виртуальный рабочий стол будет доступен для использования.

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.

При подключении пользователя к виртуальному рабочему месту OpenUDS фиксирует доступ и отображает информацию о привязанном сервисе на вкладке **Назначенные услуги** соответствующего пула.

7.11 Система резервного копирования Proxmox Backup Server

Proxmox Backup Server (PBS) в документе – 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 используя 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 вебинтерфейс. Все административные задачи можно выполнять в веб-браузере. Веб-интерфейс также предоставляет встроенную консоль.

7.11.1 Установка PBS

Установить сервер PBS:

```
# apt-get install proxmox-backup-server
```

Сервер PBS можно установить при установке системы, выбрав для установки пункт «Сервер резервного копирования от проекта Proxmox» (подробнее описано в документе «Операционная система Альт Сервер. Руководство по установке»).

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.

Для работы с локальным ZFS хранилищем должен быть установлен модуль ядра с поддержкой ZFS (например, kernel-modules-zfs-std-def).

Включить модуль:

```
# modprobe zfs
```

Чтобы не вводить эту команду каждый раз после перезагрузки, следует раскомментировать строку:

```
#zfs
```

в файле /etc/modules-load.d/zfs.conf.

7.11.1.1 Установка клиента PBS

Установить клиент PBS:

```
# apt-get install proxmox-backup-client
```

7.11.2 Веб-интерфейс PBS

Веб-интерфейс PBS доступен по адресу **https://<имя-компьютера>:8007**. Потребуется пройти аутентификацию (логин по умолчанию: root, пароль указывается в процессе установки ОС).

7.11.3 Настройка хранилища данных

7.11.3.1 Управление дисками

В веб-интерфейсе на вкладке **Управление** > **Storage/Disks (Хранилище/Диски)** можно увидеть диски, подключённые к системе.

Просмотр списка дисков в командной строке:

```
# proxmox-backup-manager disk list
```

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/store2**):

```
# proxmox-backup-manager disk fs create store2 --disk nvme0n3 --filesystem
ext4 --add-datastore true
create datastore 'store2' on disk nvme0n3
Chunkstore create: 1%
Chunkstore create: 2%
…
Chunkstore create: 99%
TASK OK
```

Для создания zpool в веб-интерфейсе, следует в разделе Storage/Disks перейти на вкладку **ZFS** и нажать кнопку **Создать: ZFS**. В открывшемся окне следует задать параметры zpool: имя хранилища, выбрать диски, уровень RAID и нажать кнопку **OK**.

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
```

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
```

7.11.3.2 Создание хранилища данных

Хранилище данных в документе – 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 Add Datastore (Добавить хранилище данных) в боковом меню (в разделе Datastore). В открывшемся окне необходимо указать:

– **Имя** в документе – название хранилища данных;
– **Backing Path** в документе – путь к каталогу, в котором будет создано хранилище данных;
– **GC Schedule** в документе – частота, с которой запускается сборка мусора;
– **Prune Schedule** в документе – частота, с которой происходит обрезка;
– **Prune Options** в документе – количество резервных копий, которые необходимо хранить.

Создание хранилища данных в командной строке:

```
# proxmox-backup-manager datastore create store1 /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 в документе – пустой файл, используемый для блокировки процесса;
– каталог .chunks в документе – содержит подкаталоги, с именами от 0000 до ffff. В этих каталогах будут храниться фрагментированные данные, после выполнения операции резервного копирования.

7.11.4 Управление пользователями

PBS поддерживает следующие области (методы) аутентификации:

– **Стандартная аутентификация Linux PAM (Linux PAM standart authentication)** в документе – 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)** в документе – аутентификация Proxmox Backup Server. Хэшированные пароли хранятся в файле /**etc/proxmox-backup/shadow.json**.

После установки PBS существует один пользователь root@pam, который соответствует суперпользователю ОС. Суперпользователь имеет неограниченные права, поэтому рекомендуется добавить других пользователей с меньшими правами.

7.11.4.1 Создание пользователей

Для добавления пользователя в веб-интерфейсе следует в разделе **Конфигурация** > **Access Control (Контроль доступа)** перейти на вкладку **Управление пользователями** и нажать кнопку **Добавить**.

Управление пользователями в консоли:

– 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
```

7.11.4.2 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.

API-токен состоит из двух частей:

– 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.

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"
}
```

7.11.4.3 Управление доступом

По умолчанию новые пользователи и API-токены не имеют никаких разрешений. Добавить разрешения можно, назначив роли пользователям/токенам для определенных

объектов, таким как хранилища данных или удаленные устройства.

Роль в документе – это список привилегий. В PBS предопределён ряд ролей:

– NoAccess в документе – нет привилегий (используется для запрета доступа);
– Admin в документе – все привилегии;
– Audit в документе – доступ только для чтения;
– DatastoreAdmin в документе – все привилегии для хранилищ данных;
– DatastoreAudit в документе – просмотр настроек хранилищ и их содержимых, без возможности чтения фактических данных;
– DatastoreReader в документе – просмотр содержимого хранилища, восстановление данных;
– DatastoreBackup в документе – создание и восстановление собственных резервных копий;
– DatastorePowerUser в документе – создание, восстановление и удаление собственных резервных копий;
– RemoteAdmin в документе – все привилегии для удалённых PBS;
– RemoteAudit в документе – просмотр настроек удалённых PBS;
– RemoteSyncOperator в документе – чтение данных с удалённых PBS.

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 в документе – включено или отключено;
– объект, на который установлено разрешение;
– пользователи/токены, для которых установлено разрешение;
– устанавливаемая роль.

Добавление разрешения в веб-интерфейсе во вкладке **Разрешения** – **Конфигурация** > **Access Control (Контроль доступа**).

Управление разрешениями в консоли:

– добавить разрешение (добавить пользователя backup_u@pbs в качестве администратора хранилища данных для хранилища данных store1, расположенного в /mnt/backup/disk1/store1):

```
# proxmox-backup-manager acl update /datastore/store1 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/
store1
Privileges with (*) have the propagate flag set
Path: /datastore/store1
- Datastore.Audit (*)
- Datastore.Backup (*)
- Datastore.Modify (*)
- Datastore.Prune (*)
- Datastore.Read (*)
- Datastore.Verify (*)
```

Для токенов требуются собственные записи ACL. Токены не могут делать больше, чем их соответствующий пользователь.

7.11.4.4 Двухфакторная аутентификация

Двухфакторная аутентификация реализована только для веб-интерфейса.

PBS поддерживает три метода двухфакторной аутентификации:

– TOTP (одноразовый пароль на основе времени) в документе – для создания этого кода используется алгоритм одноразового пароля с учетом времени входа в систему (код меняется каждые 30 секунд);

– WebAuthn (веб-аутентификация) в документе – реализуется с помощью различных устройств безопасности, таких как аппаратные ключи или доверенные платформенные модули (TPM). Для работы веб-аутентификации необходим сертификат HTTPS;
– Recovery Keys (одноразовые ключи восстановления) в документе – список ключей, каждый из которых можно использовать только один раз. В каждый момент времени у пользователя может быть только один набор одноразовых ключей.

7.11.5 Управление удалёнными PBS

Хранилища данных с удалённого сервера можно синхронизировать с локальным хранилищем с помощью задачи 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** > **Remotes** и нажать кнопку **Добавить**.

Отпечаток TLS-сертификата можно получить в веб-интерфейсе удалённого PBS по кнопке **Fhow Fingerprint**.

Получить отпечаток в командной строке:

```
# proxmox-backup-manager cert info | grep Fingerprint
```

Для настройки задачи синхронизации, необходимо в разделе **Datastore** перейти на вкладку **Sync Jobs** и нажать кнопку **Добавить**.

После создания задания синхронизации оно будет запускаться по заданному расписанию, также его можно запустить вручную из веб-интерфейса (кнопка **Run now**).

7.11.6 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 в документе – root@pam. Если сервер не указан, используется в документе – localhost.

Указать репозиторий можно, передав его в параметре --repository, или установив переменную окружения PBS_REPOSITORY, например:

```
# export PBS_REPOSITORY=pbs.test.alt:store1
```

В Таблице 2 приведены примеры репозиториев

Таблица 2 – 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

7.11.6.1 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-01/2022-04-28T12:27:01Z
Client name: host-01
Starting backup protocol: Thu Apr 28 14:27:01 2022
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: 26.36s
End Time: Thu Apr 28 14:27:27 2022
```

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 в документе – для образов блочных устройств.

Команда создания резервной копии блочного устройства:

```
$ proxmox-backup-client backup mydata.img:/dev/mylvm/mydata
```

7.11.6.2 Создание зашифрованной резервной копии

PBS поддерживает шифрование на стороне клиента с помощью AES-256 в режиме GCM.

Сначала следует создать ключ 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-01/2022-04-28T12:33:04Z
Client name: host-01
Starting backup protocol: Thu Apr 28 14:33:04 2022
Using encryption key from './my-backup.key'..
Encryption Key Password: ******
Encryption key fingerprint: b7:4b:8a:6a:1e:1e:f5:fc
Downloading previous manifest (Thu Apr 28 14:27:01 2022)
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: 31.17s
End Time: Thu Apr 28 14:33:35 2022
```

7.11.6.3 Восстановление данных

Просмотреть список всех снимков на сервере:

```
$ proxmox-backup-client snapshot list --repository pbs.test.alt:store1
Password for "root@pam": ******
snapshot size files
host/host-01/2022-04-28T12:27:01Z 667.147 MiB catalog.pcat1 index.json
user.pxar
host/host-01/2022-04-28T12:33:04Z 667.148 MiB catalog.pcat1 index.json
user_s.pxar
```

Просмотреть содержимое снимка:

```
$ proxmox-backup-client catalog dump host/host-01/2022-04-28T12:27:01Z --
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-01/2022-04-28T12:27:01Z user.pxar
/home/user/restore --repository pbs.test.alt:store1
```

Получить содержимое любого архива, можно восстановив файл index.json в репозитории по целевому пути «-». Это выведет содержимое архива на стандартный вывод:

```
$ proxmox-backup-client restore host/host-01/2022-04-28T12:27:01Z
index.json - --repository pbs.test.alt:store1
```

Если необходимо восстановить несколько отдельных файлов, можно использовать интерактивную оболочку восстановления:

```
$ proxmox-backup-client catalog shell host/host-01/2022-04-28T12:27:01Z
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** в документе – найти все файлы с расширением .txt и добавить соответствующие шаблоны в список для последующего восстановления;

– **list-selected** в документе – вывести шаблоны на экран;

– **restore-selected /home/user/restore/** в документе – восстановить все файлы в архиве, соответствующие шаблонам в /home/user/restore/ на локальном хосте;

– **restore /home/user/conf/ --pattern *.conf** в документе – восстановить все файлы с расширением .conf в /home/user/conf/ на локальном хосте.

7.11.6.4 Вход и выход

При первой попытке получить доступ к серверу с использованием команды **proxmox-backupclient**, 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
```

7.11.7 Интеграция с PVE

PBS можно интегрировать в автономную или кластерную установку PVE, добавив его в качестве хранилища.

Отпечаток TLS-сертификата можно получить в веб-интерфейсе удалённого PBS по кнопке **Fhow Fingerprint**.

Или, 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 store2 --
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.

7.12 Система резервного копирования UrBackup

UrBackup в документе – 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.

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. Для архивирования других данных следует воспользоваться резервным копированием файлов.

Для управления настройкой резервного копирования и резервными копиями используется вебинтерфейс.

7.12.1 Установка UrBackup

7.12.1.1 Сервер UrBackup

Установить сервер UrBackup:

```
# apt-get install urbackup-server
```

Создать каталог для резервных копий:

```
# mkdir -p /mnt/backups
```

Каталог должен принадлежать пользователю urbackup и у этого пользователя должны быть права на чтение/запись:

```
# chown -R urbackup:urbackup /mnt/backups
```

Добавить UrBackup-сервер в автозапуск и запустить его:

```
# systemctl enable --now urbackup-server
```

UrBackup по умолчанию прослушивает порты 55413 и 55414.

Веб-интерфейс UrBackup будет доступен по адресу http://:55414.

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**).

7.12.1.2 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**.

7.12.2 Настройка резервного копирования

В веб-интерфейсе на вкладке **Настройки** > **Главные** можно изменять настройки UrBackup. Некоторые настройки влияют только на сервер резервного коирования. Остальные настройки влияют и на клиентов резервного коирования, для этих настроек администратор может установить значения по умолчанию или переопределить настройки клиента.

На вкладке **Сервер** можно указать каталог для хранения резервных копий.

На вкладке **Файловые бэкапы** можно указать настройки файловых резервных копий, в том числе каталоги, которые будут включены в резервную копию (каталоги перечисляются через «;»). Здесь также настравиваются интервалы резервного копирования.

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 в документе – резервное копирование может производиться в любое время;
– 1-5/8:00-9:00, 19:30-20:30;6,7/0-24 в документе – 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.

7.12.3 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.

Более подробно отслеживать активность резервного копирования можно на вкладках **В работе**, **Бэкапы**, **Логи**.

Отчёты/содержимое резервных копий можно просмотреть на вкладке **Бэкапы**. Выбрав клиента, можно просмотреть список его резервных копий. Выбрав резервную копию, можно просмотреть её содержимое.

Если отметка в столбце **Архивировано** установлена, резервная копия архивируется. Пока резервная копия заархивирована, её нельзя удалить средствами UrBackup.

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 . 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__.vhdz).

7.12.4 Утилита urbackupclientctl

Для работы с UrBackup на клиенте предназначена утилита urbackupclientctl:

– urbackupclientctl start в документе – запустить инкрементное/полное резервное копирование;
– urbackupclientctl status в документе – получить текущий статус резервного копирования;
– urbackupclientctl browse в документе – просмотр списка резервных копий и файлов в резервных копиях;
– urbackupclientctl restore-start в документе – восстановить файлы из резервной копии;
– urbackupclientctl set-settings в документе – установить параметры резервного копирования;
– urbackupclientctl add-backupdir в документе – добавить новый каталог в список каталогов, для которых выполняется резервное копирование;
– urbackupclientctl list-backupdirs в документе – вывести список каталогов, для которых выполняется резервное копирование;
– urbackupclientctl remove-backupdir в документе – 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": 1642686041,
"disable_delete": true,
"id": 2,
"incremental": 1,
"size_bytes": 109955109
}
,{
"archived": 0,
"backuptime": 1642684086,
"id": 1,
"incremental": 0,
"size_bytes": 2306704775
}
]
```

Запустить процесс создания полной резервной копии:

```
# urbackupclientctl start -f
Waiting for server to start backup... done
Preparing... done
[=====================================================> ] 86% 2.01947
GB/2.36159 GB at 400.289 MBit/s
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.
```