

Альт Сервер 10.0 для облачной среды

Документация

Руководство пользователя

Редакция март, 2023



Аннотация

Добро пожаловать в документацию облачного дистрибутива Альт Сервер. Руководство описывает процедуру настройки и использования системы.

Названия компаний и продуктов, встречающихся в руководстве, могут являться торговыми знаками соответствующих компаний.

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

I. Что такое Альт Сервер?

1. Что такое Альт Сервер
2. Что такое Linux
3. Что такое системы Альт

II. Начало работы

4. Подключение к серверу по SSH
5. Получение прав суперпользователя

III. Установка пакетов

Введение

6. Источники программ (репозитории)

7. Поиск пакетов
8. Установка или обновление пакета
9. Удаление установленного пакета
10. Обновление системы
11. Единая команда управления пакетами (rpm)

IV. Корпоративная инфраструктура

12. Samba 4 в роли контроллера домена Active Directory
13. Samba в режиме файлового сервера
14. FreeIPA
15. Установка LEMP сервера (Linux, Nginx, MySQL, PHP)
16. Nextcloud — хранение документов в «облаке»
17. OpenUDS
18. Система мониторинга Zabbix
19. Сервер видеоконференций на базе Jitsi Meet
20. SOGo
21. Отказоустойчивый кластер (High Availability) на основе Pacemaker
22. Система резервного копирования Proxmox Backup Server
23. Система резервного копирования UrBackup

V. Настройка системы

24. Центр управления системой
25. Обслуживание сервера
26. Соединение удалённых офисов (OpenVPN-сервер)
27. Доступ к службам сервера из сети Интернет
28. Статистика
29. Прочие возможности ЦУС
30. Права доступа к модулям

VI. Основы администрирования Linux

31. Общие принципы работы ОС
32. Режим суперпользователя

33. Команда sudo

34. Управление пользователями

35. Система инициализации systemd и sysvinit

36. Документация

VII. Техническая поддержка продуктов «Базальт СПО»

37. Покупателям нашей продукции

38. Пользователям нашей продукции

Часть I. Что такое Альт Сервер?

В этой части рассматривается что такое Linux и Альт Сервер.

Содержание

1. Что такое Альт Сервер

2. Что такое Linux

3. Что такое системы Альт

Глава 1. Что такое Альт Сервер

Альт Сервер —серверный дистрибутив на базе ядра Linux с широкой функциональностью и поддержкой корпоративной инфраструктуры.

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

Примеры использования:

■Развертывание:

- системы мониторинга [Zabbix](#);
- сервера групповой работы [SOGO](#) и почтовых серверов Postfix и Dovecot;
- веб-приложения для синхронизации данных, общего доступа к файлам [Nextcloud](#);
- сервера видеоконференций на базе [Jitsi Meet](#);
- решения VDI на базе [OpenUDS](#).

■Управление установкой и загрузкой ОС на рабочие станции по сети.

■Создание зеркала репозитория для централизованного обновления рабочих мест под управлением ОС Альт Рабочая станция;

■Миграция на импортозамещающее программное и аппаратное обеспечение.

Глава 2. Что такое Linux

2.1. Свободные программы

2.2. Разработка Linux

2.3. Защищённость

2.4. Дистрибутивы Linux

2.5. Новичку

2.1. Свободные программы

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

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

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

2.2. Разработка Linux

В отличие от распространённых несвободных ОС, Linux не имеет географического центра разработки. Нет фирмы, которая владела бы этой ОС, нет и единого координационного центра. Программы для Linux — результат работы тысяч проектов. Большинство из них объединяет программистов из разных стран, связанных друг с другом только перепиской. Лишь некоторые проекты централизованы и сосредоточены в фирмах. Создать свой проект или присоединиться к уже существующему может любой программист, и, в случае успеха, результаты этой работы станут известны миллионам пользователей. Пользователи принимают участие в тестировании свободных программ, общаются с разработчиками напрямую. Это позволяет за короткий срок добавлять в программное обеспечение новые возможности, оперативно находить ошибки и исправлять их.

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

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

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

2.3. Защищённость

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

2.4. Дистрибутивы Linux

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

2.5. Новичку

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

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

Глава 3. Что такое системы Альт

3.1. ALT Linux Team

3.2. Сизиф

3.3. Что такое десятая платформа

3.1. ALT Linux Team

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

3.2. Сизиф

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

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

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

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

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

3.3. Что такое 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 дистрибутивы Альт. Такие 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.

3.3.1. 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.

Часть II. Начало работы

Содержание

- 4. Подключение к серверу по SSH
- 5. Получение прав суперпользователя

Глава 4. Подключение к серверу по SSH

- 4.1. Создание пары ключей SSH
- 4.2. Подключение к серверу
- 4.3. Файл конфигурации

4.1. Создание пары ключей SSH

Чтобы создать пару ключей на локальном устройстве, достаточно запустить команду **ssh-keygen**. По умолчанию будет создан ключ RSA.

Также можно запустить команду **ssh-keygen** с дополнительными параметрами:

- **-t** — указывает тип ключа;
- **-b** — указывает размер ключа.

Ключ Ed25519 считается безопасным. Размер ключа фиксирован и не может быть изменён. Команда генерации Ed25519 ключа:

```
$ ssh-keygen -t ed25519
```

Размер ключа RSA по умолчанию составляет 3072 бита и не должен быть меньше 1024 бит. Для повышения безопасности можно установить размер ключа равным 4096 бит:

```
$ ssh-keygen -t rsa -b 4096
```

После запуска команды для создания ключа SSH, будет задан вопрос:

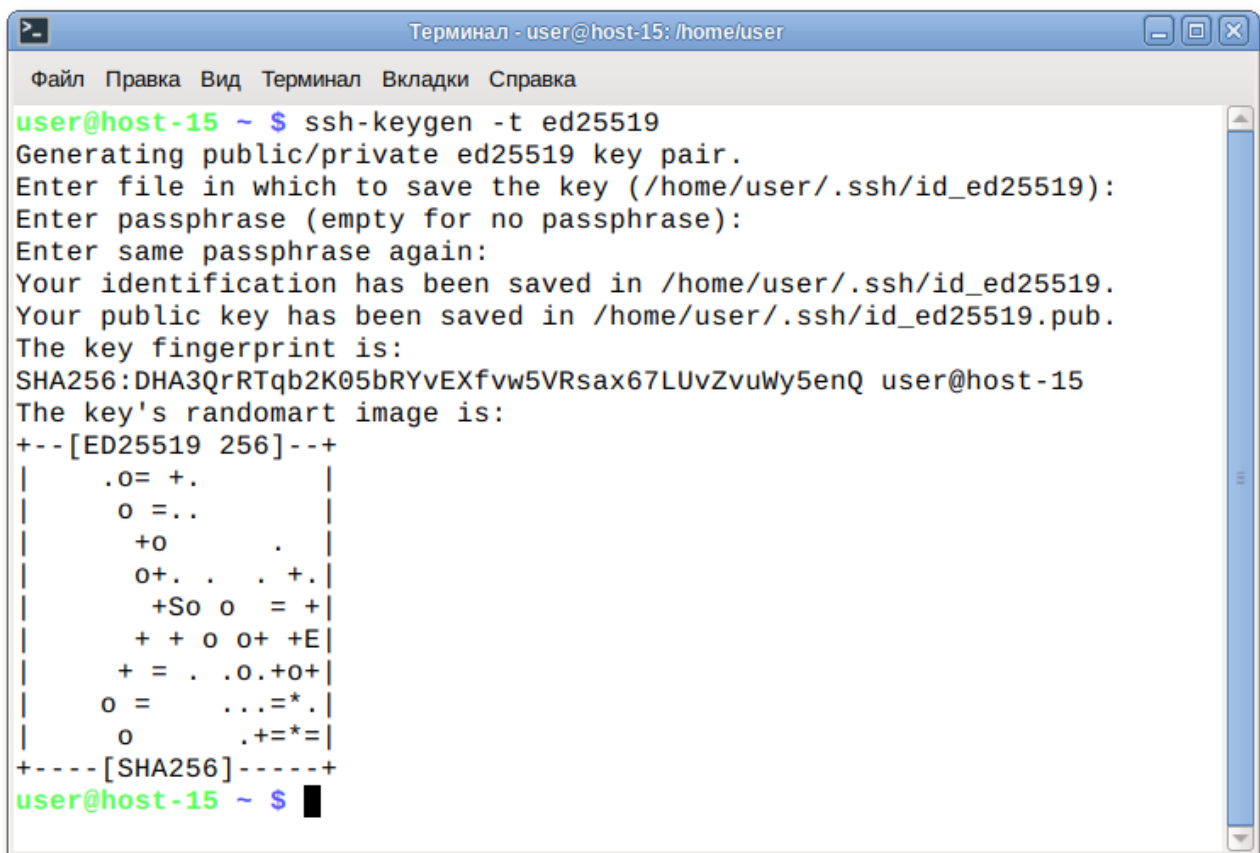
```
Generating public/private <тип_ключа> key pair.  
Enter file in which to save the key (/home/<пользователь>/.ssh/id_<тип_ключа>):
```

По умолчанию ключ будет сохранён в файл `~/.ssh/id_<тип_ключа>`. Можно нажать **ENTER**, чтобы согласиться с этим или указать другой файл.

Затем будет предложено установить парольную фразу:

```
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:
```

Парольная фраза еще больше повышает безопасность. Если установить парольную фразу, она будет запрашиваться каждый раз, когда используется ключ. Если нажать **ENTER** без ввода парольной фразы, SSH-ключ будет сгенерирован без пароля.



```
Терминал - user@host-15: /home/user  
Файл  Правка  Вид  Терминал  Вкладки  Справка  
user@host-15 ~ $ ssh-keygen -t ed25519  
Generating public/private ed25519 key pair.  
Enter file in which to save the key (/home/user/.ssh/id_ed25519):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/user/.ssh/id_ed25519.  
Your public key has been saved in /home/user/.ssh/id_ed25519.pub.  
The key fingerprint is:  
SHA256:DHA3QrRTqb2K05bRYvEXfvw5VRsax67LUvZvuWy5enQ user@host-15  
The key's randomart image is:  
+--[ED25519 256]--+  
|      .o= +.      |  
|      o =..      |  
|      +o        . |  
|      o+. . . +. |  
|      +So o  = +  |  
|      + + o o+ +E |  
|      + = . .o.+o+ |  
|      o =   ...=*  |  
|      o      .+*=  |  
+-----[SHA256]-----+  
user@host-15 ~ $
```

В результате выполнения команды **ssh-keygen** будут созданы два ключа:

- » `<имя_ключа>` — закрытый ключ (никогда не должен передаваться кому-либо ещё);
- » `<имя_ключа>.pub` — открытый ключ (часть, которую необходимо передать на удалённое устройство, к которому будет осуществляться подключение. На удалённом устройстве открытый ключ будет сохранен в файле **author_keys**).

Чтобы просмотреть открытый ключ, можно использовать команду **cat**:

```
$ cat ~/.ssh/id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMnCtC+IJ0Bbw480ql79hi jTPNFN9QFM+sLM19n+BBMu
user@host-15
```

Выделите текст и скопируйте его в буфер обмена. Этот ключ необходимо указать при создании VM в поле **SSH-ключ**.



Примечание

Можно добавить, изменить и удалить парольную фразу для ключа SSH на локальном устройстве:

```
$ ssh-keygen -p
```

Обратите внимание, что вы должны знать свою текущую парольную фразу. Если вы забыли парольную фразу, то больше не сможете использовать свой SSH-ключ.

```
Терминал - user@host-15: /home/user
Файл  Правка  Вид  Терминал  Вкладки  Справка
user@host-15 ~ $ ssh-keygen -p
Enter file in which the key is (/home/user/.ssh/id_rsa): /home/user/.ssh/id_ed25519
Key has comment 'user@host-15'
Enter new passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved with the new passphrase.
user@host-15 ~ $
```

4.2. Подключение к серверу

После того как сервер создан, к нему можно подключиться по SSH, используя интерфейс командной строки. VM должна находиться в статусе *RUNNING*.

Для подключения к серверу необходимо указать публичный адрес виртуальной машины.



Примечание

В Альт Сервер, предоставляемым Yandex Cloud, возможность подключения по протоколу SSH с использованием логина и пароля по умолчанию отключена.

Подключиться к серверу можно, выполнив команду:

```
$ ssh <логин>@<IP-адрес>
```

Например:

```
$ ssh user@158.160.0.157
The authenticity of host '158.160.0.157 (158.160.0.157)' can't be established.
ED25519 key fingerprint is SHA256:4+0X7yelfgZ0NfcLCXAv0hUVTs8GBIqfjmNHP5L65tyr.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '158.160.0.157' (ED25519) to the list of known hosts.
```



Примечание

При первом подключении к серверу, появится предупреждение о подлинности хоста, в ответ на которое, следует ввести **yes**.

Отпечаток ключа (key fingerprint), показанный в предупреждении, будет сохранён в файле **~/.ssh/known_hosts** и автоматически распознан при следующих подключениях.

Далее, если для SSH-ключа, не был установлен пароль произойдёт автоматическое подключение. Если пароль был установлен, необходимо ввести его в ответ на запрос пароля:

```
Enter passphrase for key '/home/user/.ssh/id_ed25519':
```

Обратите внимание, что вводимый пароль не отображается в интерфейсе командной строки.



Примечание

Если у вас несколько закрытых ключей, следует указать нужный:

```
$ ssh -i <файл_ключа> <логин>@<IP-адрес>
```

Например:

```
$ ssh -i .ssh/id_ed25519 user@158.160.0.157
```

В случае успешного прохождения процедуры аутентификации и идентификации будет выполнен вход в систему.

4.3. Файл конфигурации

После успешного подключения к серверу, можно добавить запись о подключении в файл конфигурации на локальном устройстве. Наличие такой записи позволит для подключения к серверу использовать команду:

```
$ ssh <уникальное-имя>
```

ВМЕСТО:

```
$ ssh -i <ключ> <логин>@<IP-адрес>
```

В файл конфигурации (~/.ssh/config) новые записи добавляются в следующем формате:

```
Host <уникальное-имя>
  HostName <IP-адрес>
  User <логин>
  IdentityFile <ключ>
```

Например:

```
Host altserver;
  HostName 158.160.0.157
  User user
  IdentityFile ~/.ssh/id_ed25519
```

Для проверки того, работает ли запись, следует подключиться к серверу:

```
$ ssh altserver
```

Глава 5. Получение прав суперпользователя

5.1. Платформа Yandex Cloud

Команды, помеченные в данном руководстве символом #, необходимо выполнять с правами суперпользователя. Получить же такие права можно несколькими способами, в том числе через **sudo**. За подробностями следует обратиться к документации облачной платформы.

5.1. Платформа Yandex Cloud

Пользователь, указанный при создании ВМ, входит в группу sudo. Для повышения прав до root следует использовать команду **sudo**.

По умолчанию, у root нет пароля, поэтому достаточно подключиться к ВМ по SSH (см. [Подключение к серверу по SSH](#)) и ввести команду:

```
$ sudo su -
```

Также можно выполнять различные команды, не переключаясь на root. Например, для перезагрузки ВМ из гостевой ОС можно выполнить команду:

```
$ sudo reboot
```

Часть III. Установка пакетов

Содержание

[Введение](#)

6. Источники программ (репозитории)
7. Поиск пакетов
8. Установка или обновление пакета
9. Удаление установленного пакета
10. Обновление системы
11. Единая команда управления пакетами (rpm)

Введение

В современных системах на базе Linux существует огромное число общих ресурсов: разделяемых библиотек, содержащих стандартные функции, исполняемые файлы, сценарии и стандартные утилиты и т.д. Этими общими ресурсами пользуются сразу несколько программ. Удаление или изменение версии одного из составляющих систему компонентов может повлечь неработоспособность других, связанных с ним компонентов, или может привести к выводу из строя всей системы. В контексте системного администрирования проблемы такого рода называют нарушением *целостности системы*. Задача администратора — обеспечить наличие в системе согласованных версий всех необходимых программных компонентов (обеспечение целостности системы).

Для установки, удаления и обновления программ, а также поддержания целостности системы в Linux в первую очередь стали использоваться программы *менеджеры пакетов* (например, такие, как **rpm**). С точки зрения менеджера пакетов программное обеспечение представляет собой набор компонентов — программных *пакетов*. Пакеты содержат в себе набор исполняемых программ и вспомогательных файлов, необходимых для корректной работы программного обеспечения. Менеджеры пакетов облегчают установку программ: они позволяют проверить наличие необходимого для работы устанавливаемой программы компонента подходящей версии непосредственно в момент установки. Менеджеры пакетов производят необходимые процедуры для регистрации программы во всех операционных средах пользователя: сразу после установки программа становится доступна пользователю из командной строки и появляется, если это было предусмотрено, в меню приложений всех графических оболочек.

Часто компоненты, используемые различными программами, выделяют в отдельные пакеты и помечают, что для работы ПО, предоставляемого пакетом А, необходимо установить пакет В. В таком случае говорят, что пакет А *зависит* от пакета В или между пакетами А и В существует *зависимость*.

Отслеживание зависимостей между такими пакетами представляет собой важную задачу для любого дистрибутива. Некоторые компоненты пакетов могут быть взаимозаменяемыми, т.е. может обнаружиться несколько пакетов, предлагающих затребованный ресурс.

Ещё более сложной является задача контроля целостности и непротиворечивости установленного в системе ПО. Представим, что некие программы А и В требуют наличия в системе компонентов С версии 1.0. Обновление версии пакета А, требующее обновления компонентов С до новой версии (например, до версии 2.0, использующей новый интерфейс доступа), влечёт за собой обязательное обновление и программы В.

На практике менеджеры пакетов оказались неспособны эффективно устранить нарушения целостности системы и предотвратить все коллизии при установке или удалении программ. Особенно остро этот недостаток сказался на обновлении систем из централизованного репозитория, в котором пакеты непрерывно обновляются, дробятся на более мелкие и т.п. Именно этот недостаток стимулировал создание систем управления программными пакетами и поддержания целостности ОС.

Для автоматизации и контроля описанных выше процессов стала применяться усовершенствованная система управления программными пакетами **APT** (от англ. Advanced Packaging Tool). Автоматизация и контроль достигаются путём создания одного или нескольких внешних репозиториях. В них хранятся доступные для установки пакеты программ.

В распоряжении **APT** находятся две базы данных: одна описывает установленные в системе пакеты, вторая — внешний репозиторий. **APT** отслеживает целостность установленной системы и, в случае обнаружения противоречий в зависимостях пакетов, разрешает конфликты, находит пути их корректного устранения, руководствуясь сведениями из внешних репозиториях.

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

Глава 6. Источники программ (репозитории)

6.1. Редактирование репозиториях

Отличие репозиториях, с которыми работает **APT**, от простого набора пакетов — наличие метаинформации. В ней содержится индекс находящихся в репозитории пакетов и сведения о них. Поэтому, чтобы получить всю информацию о репозитории, **APT** достаточно получить его индексы.

APT может пользоваться любым количеством репозиториях одновременно, формируя единую информационную базу обо всех содержащихся в них пакетах. При установке пакетов **APT** обращает внимание только на название пакета, его версию и зависимости. Для **APT** не имеет значения расположение пакета в том или ином репозитории.



Важно

Для одновременного подключения нескольких репозиториях необходимо отслеживать их совместимость друг с другом, т.е. их пакетная база должна отражать один определённый этап разработки. Совместное использование репозиториях, относящихся к разным дистрибутивам, или смешивание стабильного репозитория с нестабильной веткой разработки (Sisyphus) может привести к различным неожиданностям и трудностям при обновлении пакетов.

APT осуществляет взаимодействие с репозиториями при помощи различных протоколов доступа. Наиболее популярные — HTTP и FTP.

Для того чтобы **APT** мог использовать тот или иной репозиторий, информацию о нём необходимо поместить в файл **/etc/apt/sources.list**, либо в любой файл **.list** (например, **mysources.list**) в каталоге **/etc/apt/sources.list.d/**. Описания репозиториях заносятся в эти файлы в следующем виде:

```
rpm [подпись] метод:путь база название  
rpm-src [подпись] метод:путь база название
```

Здесь:

- » `rpm` или `rpm-src` — тип репозитория (скомпилированные программы или исходные тексты);
- » `[подпись]` — необязательная строка-указатель на электронную подпись разработчиков. Наличие этого поля подразумевает, что каждый пакет из данного репозитория должен быть подписан соответствующей электронной подписью. Подписи описываются в файле **`/etc/apt/vendor.list`**;
- » `метод` — способ доступа к репозиторию: `ftp`, `http`, `file`, `rsh`, `ssh`, `cdrom`, `copy`;
- » `путь` — путь к репозиторию в терминах выбранного метода;
- » `база` — относительный путь к базе данных репозитория;
- » `название` — название репозитория.

Непосредственно после установки дистрибутива Альт Сервер в файлах **`/etc/apt/sources.list.d/*.list`** обычно указывается интернет-репозиторий, совместимый с установленным дистрибутивом.

После редактирования списка репозитория в **`sources.list`**, необходимо обновить локальную базу данных **APT** о доступных пакетах. Это делается командой **`apt-get update`**.

Если в **`sources.list`** присутствует репозиторий, содержимое которого может изменяться (например, постоянно разрабатываемый репозиторий или репозиторий обновлений по безопасности), то прежде чем работать с **APT**, необходимо синхронизировать локальную базу данных с удалённым сервером командой **`apt-get update`**. Локальная база данных создаётся заново при каждом изменении в репозитории: добавлении, удалении или переименовании пакета.

При установке определённого пакета **APT** производит поиск самой новой версии этого пакета во всех известных ему репозиториях вне зависимости от способа доступа к ним. Так, если в репозитории, доступном в сети Интернет, обнаружена более новая в сравнении с компакт-диском версия программы, то **APT** начнёт загружать соответствующий пакет из сети Интернет. Поэтому, если подключение к сети Интернет отсутствует или ограничено низкой пропускной способностью канала или высокой стоимостью, то следует закомментировать строки (добавить в начало строки символ `#`) в **`/etc/apt/sources.list`**, относящиеся к ресурсам в сети Интернет.

6.1. Редактирование репозитория

6.1.1. Утилита `apt-repo`

Для редактирования репозитория можно воспользоваться утилитой **`apt-repo`**:

- » просмотреть список активных репозитория:

```
apt-repo
```

- » добавить репозиторий в список активных репозитория:

```
apt-repo add репозиторий
```

■удалить или выключить репозиторий:

```
apt-repo rm репозиторий
```

■обновить информацию о репозиториях:

```
apt-repo update
```

■справка о команде **apt-repo**:

```
man apt-repo
```

или

```
apt-repo --help
```



Примечание

Для выполнения большинства команд необходимы права администратора.

Типичный пример использования: удалить все источники и добавить стандартный репозиторий P10 (архитектура выбирается автоматически):

```
# apt-repo rm all  
# apt-repo add p10
```

Или то же самое одной командой:

```
# apt-repo set p10
```

6.1.2. Добавление репозитория вручную

Для изменения списка репозитория можно отредактировать в любом текстовом редакторе файлы из каталога **/etc/apt/sources.list.d/**.



Примечание

Для изменения этих файлов необходимы права администратора.

В файле **alt.list** может содержаться такая информация:

```
# ftp.altlinux.org (ALT Linux, Moscow)  
  
# ALT Linux Platform 10  
#rpm [p10] ftp://ftp.altlinux.org/pub/distributions/ALTLinux/p10/branch x86_64  
classic  
#rpm [p10] ftp://ftp.altlinux.org/pub/distributions/ALTLinux/p10/branch x86_64-  
i586 classic
```

```
#rpm [p10] ftp://ftp.altlinux.org/pub/distributions/ALTLinux/p10/branch noarch
classic

rpm [p10] http://ftp.altlinux.org/pub/distributions/ALTLinux/p10/branch x86_64
classic
rpm [p10] http://ftp.altlinux.org/pub/distributions/ALTLinux/p10/branch x86_64-
i586 classic
rpm [p10] http://ftp.altlinux.org/pub/distributions/ALTLinux/p10/branch noarch
classic
```

По сути, каждая строчка соответствует некому репозиторию. Не активные репозитории — строки, начинающиеся со знака `#`. Для добавления нового репозитория, достаточно дописать его в этот или другой файл.

После обновления списка репозитория следует обновить информацию о них (выполнить команду **apt-get update** или **apt-repo update**).

Глава 7. Поиск пакетов

Если точное название пакета неизвестно, то для его поиска можно воспользоваться утилитой **apt-cache**. Данная утилита позволяет искать пакет не только по имени, но и по его описанию.

Команда **apt-cache search подстрока** позволяет найти все пакеты, в именах или описании которых присутствует указанная подстрока. Например:

```
$ apt-cache search dictionary
stardict-wn - GCIDE - The Collaborative International Dictionary of English
firefox-ru - Russian (RU) Language Pack for Firefox
gnome-dictionary-applet - GNOME panel applet for gnome-dictionary
gnome-utils - Utilities for the GNOME 2.0 desktop
libgdict - GNOME Dictionary Library.
stardict-mueller7 - V.K. Mueller English-Russian Dictionary, 7 Edition: stardict
format
stardict-slovnyk_be-en - Dictionary: Slovnyk Belarusian-English
stardict-slovnyk_be-ru - Dictionary: Slovnyk Belarusian-Russian
stardict-slovnyk_be-uk - Dictionary: Slovnyk Belarusian-Ukrainian
stardict-slovnyk_cs-ru - Dictionary: Slovnyk Czech-Russian
stardict-slovnyk_en-be - Dictionary: Slovnyk English-Belarusian
stardict-slovnyk_en-ru - Dictionary: Slovnyk English-Russian
stardict-slovnyk_en-uk - Dictionary: Slovnyk English-Ukrainian
stardict-slovnyk_es-ru - Dictionary: Slovnyk Spanish-Russian
stardict-slovnyk_ru-be - Dictionary: Slovnyk Russian-Belarusian
stardict-slovnyk_ru-cs - Dictionary: Slovnyk Russian-Czech
stardict-slovnyk_ru-en - Dictionary: Slovnyk Russian-English
stardict-slovnyk_ru-es - Dictionary: Slovnyk Russian-Spanish
stardict-slovnyk_ru-uk - Dictionary: Slovnyk Russian-Ukrainian
stardict-slovnyk_uk-be - Dictionary: Slovnyk Ukrainian-Belarusian
stardict-slovnyk_uk-en - Dictionary: Slovnyk Ukrainian-English
stardict-slovnyk_uk-ru - Dictionary: Slovnyk Ukrainian-Russian
words - A dictionary of English words for the /usr/share/dict directory
```

Для того чтобы подробнее узнать информацию о найденном пакете и получить его подробное описание, воспользуйтесь командой **apt-cache show**:

```
$ apt-cache show stardict-mueller7
Package: stardict-mueller7
Section: Text tools
Installed Size: 3094848
Maintainer: Anton V. Boyarshinov <boyarsh@altlinux.ru>
Version: 1.0-alt8@1338342590
Pre-Depends: rpmlib(PayloadIsLzma)
Depends: stardict (>= 2.4.2)
Provides: stardict-mueller7 (= 1.0-alt8)
Architecture: noarch
Size: 3134862
MD5Sum: 54f9e085c1fc67084253b3ba72a0c482
Filename: stardict-mueller7-1.0-alt8.noarch.rpm
Description: V.K. Mueller English-Russian Dictionary, 7th Edition, for stardict
 Electronic version of V.K. Mueller English-Russian Dictionary,
 7th Edition, in stardict format, for use with a stardict client.
```

При поиске с помощью **apt-cache** можно использовать русскую подстроку. В этом случае будут найдены пакеты, имеющие описание на русском языке. К сожалению, описание на русском языке в настоящее время есть не у всех пакетов, но наиболее актуальные описания переведены.

Глава 8. Установка или обновление пакета



Важно

Для установки пакетов требуются привилегии администратора.

Установка пакета с помощью АРТ выполняется командой **apt-get install имя_пакета**.



Важно

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

```
# apt-get update
```

apt-get позволяет устанавливать в систему пакеты, требующие для работы наличие других, пока ещё не установленных пакетов. В этом случае он определяет, какие пакеты необходимо установить. **apt-get** устанавливает их, пользуясь всеми доступными репозиториями.

Установка пакета *stardict-mueller7* командой **apt-get install stardict-mueller7** приведёт к следующему диалогу с **АРТ** (если пакет еще не установлен):

```
# apt-get install stardict-mueller7
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие дополнительные пакеты будут установлены:
  icon-theme-hicolor libgtk+2 libgtk+2-locales libsigc++2 stardict
Следующие НОВЫЕ пакеты будут установлены:
  icon-theme-hicolor libgtk+2 libgtk+2-locales libsigc++2 stardict stardict-
mueller7
```

```

0 будет обновлено, 6 новых установлено, 0 пакетов будет удалено и 24 не будет
обновлено.
Необходимо получить 9629kB архивов.
После распаковки потребуется дополнительно 36,2MB дискового пространства.
Продолжить? [Y/n] y
Совершаем изменения...
Подготовка... ##### [100%]
Обновление / установка...
1: libsigc++2-2.10.7-alt1 ##### [ 17%]
2: libgtk+2-locale-2.24.33-alt1 ##### [ 33%]
3: icon-theme-hicolor-0.17-alt2 ##### [ 50%]
4: libgtk+2-2.24.33-alt1 ##### [ 67%]
5: stardict-3.0.6-alt1 ##### [ 83%]
6: stardict-mueller7-1.0-alt8 ##### [100%]
Завершено.

```

Команда

```
apt-get install имя_пакета
```

используется также и для обновления уже установленного пакета или группы пакетов. В этом случае **apt-get** дополнительно проверяет, есть ли обновлённая, в сравнении с установленной в системе, версия пакета в репозитории.

Например, если пакет *stardict-mueller7* установлен и в репозитории нет обновлённой версии этого пакета, то вывод команды **apt-get install stardict-mueller7** будет таким:

```

# apt-get install stardict-mueller7
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Последняя версия stardict-mueller7 уже установлена.
0 будет обновлено, 0 новых установлено, 0 пакетов будет удалено и 1 не будет
обновлено.

```

При помощи **APT** можно установить и отдельный rpm- пакет, не входящий в состав репозитория (например, полученный из сети Интернет). Для этого достаточно выполнить команду

```
# apt-get install /путь/к/файлу.rpm
```

При этом **APT** проведёт стандартную процедуру проверки зависимостей и конфликтов с уже установленными пакетами.

Иногда в результате операций с пакетами без использования **APT** целостность системы нарушается, и **apt-get** отказывается выполнять операции установки, удаления или обновления. В этом случае необходимо повторить операцию, задав опцию **-f**, заставляющую **apt-get** исправить нарушенные зависимости, удалить или заменить конфликтующие пакеты. В этом случае необходимо внимательно следить за сообщениями, выводимыми **apt-get**. Любые действия в этом режиме обязательно требуют подтверждения со стороны пользователя.

Глава 9. Удаление установленного пакета

Для удаления пакета используется команда **apt-get remove имя_пакета**. Для того чтобы не нарушать целостность системы, будут удалены и все пакеты, зависящие от удаляемого. В случае удаления пакета, который относится к базовым компонентам системы, **apt-get** потребует дополнительное подтверждение с целью предотвращения возможной случайной ошибки.



Важно

Для удаления пакетов требуются привилегии администратора.

При попытке с помощью **apt-get** удалить базовый компонент системы, вы увидите следующий запрос на подтверждение операции:

```
# apt-get remove filesystem
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие пакеты будут УДАЛЕНЫ:
...
ВНИМАНИЕ: Будут удалены важные для работы системы пакеты
Обычно этого делать не следует. Вы должны точно понимать возможные последствия!
...
0 будет обновлено, 0 новых установлено, 2648 пакетов будет удалено и 0 не будет
обновлено.
Необходимо получить 0В архивов.
После распаковки будет освобождено 8994МВ дискового пространства.
Вы делаете нечто потенциально опасное!
Введите фразу 'Yes, do as I say!' чтобы продолжить.
```



Предупреждение

Каждую ситуацию, в которой **APT** выдаёт такой запрос, необходимо рассматривать отдельно. Вероятность того, что после выполнения этой команды система окажется неработоспособной, очень велика.

Глава 10. Обновление системы

10.1. Обновление всех установленных пакетов

10.2. Обновление ядра

10.1. Обновление всех установленных пакетов

Для обновления всех установленных пакетов необходимо выполнить команды:

```
# apt-get update
# apt-get dist-upgrade
```

Первая команда (**apt-get update**) обновит индексы пакетов. Вторая команда (**apt-get dist-upgrade**) позволяет обновить только те установленные пакеты, для которых в репозиториях, перечисленных в `/etc/apt/sources.list`, имеются новые версии.



Примечание

Несмотря на то, что команда **apt-get upgrade** существует, использовать её следует осторожно, либо не использовать вовсе.

Она позволяет обновить только те установленные пакеты, для которых в репозиториях, перечисленных в `/etc/apt/sources.list`, имеются новые версии.

Никакие другие пакеты при этой операции из системы удалены не будут. Этот способ полезен при работе со стабильными пакетами приложений, относительно которых известно, что они при смене версии изменяются несущественно.

Иногда, однако, происходит изменение в наименовании пакетов или изменение их зависимостей. Такие ситуации не обрабатываются командой **apt-get upgrade**, в результате чего происходит нарушение целостности системы: появляются неудовлетворённые зависимости. Для разрешения этой проблемы существует режим обновления в масштабе дистрибутива — **apt-get dist-upgrade**.

В случае обновления всего дистрибутива **APT** проведёт сравнение системы с репозиторием и удалит устаревшие пакеты, установит новые версии присутствующих в системе пакетов, отследит ситуации с переименованиями пакетов или изменения зависимостей между старыми и новыми версиями программ. Всё, что потребуется поставить (или удалить) дополнительно к уже имеющемуся в системе, будет указано в отчёте **apt-get**, которым **APT** предварит само обновление.



Примечание

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

10.2. Обновление ядра

Для обновления ядра ОС необходимо выполнить команду:

```
# update-kernel
```



Примечание

Если индексы сегодня еще не обновлялись перед выполнением команды **update-kernel** необходимо выполнить команду **apt-get update**.

Если необходимо обновить/установить другой тип ядра, необходимо выполнить команду:

```
# update-kernel -t <новый тип ядра>
```


где <новый тип ядра> — std-def, un-def и т.п.



Примечание

Ключ **-t** и тип ядра (std-def, un-def и т.п.) следует указывать только если необходимо обновить ядро другого типа, так как по умолчанию обновляется текущий тип ядра. Узнать версию загруженного ядра можно, выполнив команду:

```
$ uname -r
```

Команда **update-kernel** обновляет и модули ядра, если в репозитории обновилось что-то из модулей без обновления ядра.

Установка/обновление модулей ядра выполняется командой:

```
# apt-get install kernel-modules-<модуль>-<тип ядра>
```

Новое ядро загрузится только после перезагрузки системы, которую рекомендуется выполнить немедленно.

После успешной загрузки на обновленном ядре можно удалить старое, выполнив команду:

```
# remove-old-kernels
```

Глава 11. Единая команда управления пакетами (dpkg)

Основное назначение единой команды управления пакетами — унифицировать управление пакетами в дистрибутивах с разными пакетными менеджерами. Утилита **dpkg** упрощает процедуру управления пакетами, может использоваться в скриптах и установщиках, сервисных программах, в повседневном администрировании различных систем. В **dpkg** добавлены типовые операции, которые в случае использования apt, потребовали бы ввода более одной команды.

Единая команда управления пакетами включает в себя следующую функциональность:

- управление пакетами (установка/удаление/поиск);
- управление репозиториями (добавление/удаление/обновление/список);
- управление системными сервисами (включение/выключение/список).

Список поддерживаемых форматов пакетов: rpm, deb, tgz, tbz, tbz2, apk (alpine), pkg.gz.



Примечание

Установка утилиты **epm**, если она еще не установлена, выполняется командой:

```
# apt-get install eepm
```

Подробную информацию об утилите **epm** и её опциях можно получить, выполнив команду:

```
$ epm --help
```

Ниже описаны лишь некоторые возможности утилиты **epm**.

Установка пакета из репозитория или из локального файла в систему:

```
# epm install <имя_пакета>
```



Важно

Если пакет создан сторонним поставщиком, то при его установке командой **epm install** не будут выполнены установочные скрипты из пакета. Это предохраняет систему от повреждения, но может привести к тому, что пакет не заработает. Вернуть стандартное поведение можно добавлением **--scripts**:

```
# epm install --scripts <имя_пакета>
```

Установить сторонние программы безопасным и простым способом:

```
# epm play <имя_программы>
```

Список программ, которые можно установить данной командой, можно просмотреть, выполнив команду:

```
$ epm play
```

Run with a name of a play script to run:

anydesk	- Install AnyDesk from the official site
assistant	- Install Assistant (Ассистент) from the official site
...	
yandex-browser	- Install Yandex browser from the official site
yandex-disk	- Install Yandex Disk from the official site
zoom	- Install Zoom client from the official site

Команда **epm play** требует наличия доступа в сеть Интернет.



Примечание

Для некоторых сторонних rpm-пакетов, написаны дополнительные правила для перепакетки (при перепакетке пакета создаётся пакет, учитывающий, что нужно для работы исходного пакета). Установить такие пакеты можно, выполнив команду:

```
# rpm install --repack <имя_пакета>
```

Для deb-пакетов ключ **--repack** применяется автоматически.

Удаление пакета из системы:

```
# rpm remove <имя_пакета>
```

Поиск пакета в репозитории:

```
# rpm search <текст>
```

Получить список установленных пакетов:

```
$ rpm list
```

Удалить пакеты, от которых не зависят какие-либо другие пакеты, установленные в системе:

```
# rpm autoremove
```

Обновить все установленные пакеты и ядро ОС:

```
# rpm full-upgrade
```



Примечание

Утилита **yum** (должен быть установлен пакет *rpm-yum*), позволяет имитировать работу менеджера пакетов yum, например:

```
# yum search docs-alt-kworkstation
# apt-cache search -- docs-alt-kworkstation | grep -E -i --color --
"(docs-alt-kworkstation)"
docs-alt-kworkstation - ALT KWorkstation documentation
```

Часть IV. Корпоративная инфраструктура

Содержание

[12. Samba 4 в роли контроллера домена Active Directory](#)

[13. Samba в режиме файлового сервера](#)

- 14. FreeIPA
- 15. Установка LEMP сервера (Linux, Nginx, MySQL, PHP)
- 16. Nextcloud — хранение документов в «облаке»
- 17. OpenUDS
- 18. Система мониторинга Zabbix
- 19. Сервер видеоконференций на базе Jitsi Meet
- 20. SOGo
- 21. Отказоустойчивый кластер (High Availability) на основе Pacemaker
- 22. Система резервного копирования Proxmox Backup Server
- 23. Система резервного копирования UrBackup

Глава 12. Samba 4 в роли контроллера домена Active Directory

- 12.1. Установка
- 12.2. Создание нового домена
- 12.3. Запуск службы
- 12.4. Настройка Kerberos
- 12.5. Проверка работоспособности
- 12.6. Управление пользователями
- 12.7. Заведение вторичного DC
- 12.8. Репликация
- 12.9. Подключение к домену на рабочей станции

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).



Предупреждение

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



Предупреждение

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

12.1. Установка

Для установки Samba AD DC выполняются следующие шаги:

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

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

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

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

12.2. Создание нового домена

12.2.1. Восстановление к начальному состоянию Samba

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

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



Предупреждение

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

12.2.2. 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`



Примечание

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



Предупреждение

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

12.2.3. 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 --option="dns forwarder=8.8.8.8" --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;
- » `dns forwarder` — внешний DNS-сервер;
- » `--server-role` — тип серверной роли.



Примечание

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

12.2.4. Интерактивное создание домена



Примечание

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

Для интерактивного развертывания 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]:
8.8.8.8
Administrator password:
Retype password:
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.0.122
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=test,DC=alt
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=test,DC=alt
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at /var/lib/
samba/private/krb5.conf
Once the above files are installed, your Samba4 server will be ready to use
Server Role:          active directory domain controller
```

```
Hostname:          dc
NetBIOS Domain:    TEST
DNS Domain:        test.alt
DOMAIN SID:        S-1-5-21-80639820-2350372464-3293631772
```

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



Примечание

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

12.3. Запуск службы

В файл `/etc/resolvconf.conf` добавить строку:

```
name_servers=127.0.0.1
```

Обновить DNS адреса:

```
# resolvconf -u
```

Установить службу по умолчанию и запустите её:

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

12.4. 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), в строке `dns_lookup_realm` должно быть установлено значение `false`:

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

[logging]
# default = FILE:/var/log/krb5libs.log
# kdc = FILE:/var/log/krb5kdc.log
# admin_server = FILE:/var/log/kadmind.log

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



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

```
[domain_realm]
dc = TEST.ALT
```



Примечание

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

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

12.5. 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
Password for [TEST\administrator]:

      Sharename      Type      Comment
      -----      -
      sysvol         Disk
      netlogon       Disk
      IPC$           IPC       IPC Service (Samba 4.15.9)
SMB1 disabled -- no workgroup available
```

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

Проверка конфигурации DNS:

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

```
# cat /etc/resolv.conf
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
search test.alt
nameserver 127.0.0.1

# host test.alt
test.alt has address 192.168.0.122
```

»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: FILE:/tmp/krb5cc_0
Default principal: administrator@TEST.ALT

Valid starting      Expires            Service principal
14.09.2022 14:32:35  15.09.2022 00:32:35  krbtgt/TEST.ALT@TEST.ALT
        renew until  21.09.2022 14:32:32
```

12.6. Управление пользователями

Создать пользователя с паролем:

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

Удалить пользователя:

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

Отключить пользователя:

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

Включить пользователя:

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

Изменить пароль пользователя:

```
samba-tool user setpassword ИМЯ ПОЛЬЗОВАТЕЛЯ
```

Просмотреть доступных пользователей:

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

Например, создать и разблокировать пользователя ivanov:

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



Предупреждение

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

12.7. Заведение вторичного DC

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

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

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

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

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

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

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

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

4. На Primary Domain Controller (PDC) проверить состояние службы **bind**:

```
# systemctl status bind
```

И, если она была включена, выключить службу **bind** и перезапустить службу **samba**:

```
# systemctl stop bind
# systemctl restart samba
```

5. На PDC завести IP-адрес для dc2:



Предупреждение

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

```
# samba-tool dns add 192.168.0.122 test.alt DC2 A 192.168.0.106 -  
Uadministrator  
Password for [TEST\administrator]:  
Record added successfully
```

6. На вторичном DC установить следующие параметры в файле конфигурации клиента Kerberos (**/etc/krb5.conf**):

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



Примечание

На вторичном DC в **/etc/resolv.conf** обязательно должен быть добавлен PDC как nameserver:

```
# echo "name_servers=192.168.0.122" >> /etc/resolvconf.conf  
# echo "search_domains=test.alt" >> /etc/resolvconf.conf  
# resolvconf -u  
# cat /etc/resolv.conf  
search test.alt  
nameserver 192.168.0.122  
nameserver 8.8.8.8
```

7. Для проверки настройки запросить билет Kerberos для администратора домена:

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



Предупреждение

Имя домена должно быть указано в верхнем регистре

8. Убедиться, что билет получен:

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

Valid starting        Expires              Service principal
14.09.2022 15:50:40   15.09.2022 01:50:40  krbtgt/TEST.ALT@TEST.ALT
        renew until 21.09.2022 15:50:34
```

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

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

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
```

10. Сделать службу **samba** запускаемой по умолчанию и запустить её:

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

12.8. Репликация



Предупреждение

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



Предупреждение

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

1. Реплицируем на вторичном DC (с первичного):

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

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

2. Реплицируем на вторичном DC (на первичный):

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

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



Примечание

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

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

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



Примечание

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

12.9. Подключение к домену на рабочей станции

12.9.1. 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.

Настройка сети:

► 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/iface/enp0s3/resolv.conf** со следующим содержимым:

```
nameserver 192.168.0.122
```

где 192.168.0.122 — IP-адрес DNS-сервера домена.

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

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

где `enr0s3` — интерфейс на котором доступен контроллер домена, `test.alt` — домен.

■ обновить DNS адреса:

```
# resolvconf -u
```



Примечание

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

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

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

12.9.2. Ввод в домен

Ввод в домен:

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

Перезагрузить рабочую станцию.

Глава 13. Samba в режиме файлового сервера

13.1. Настройка `smb.conf`

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

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

13.1. Настройка `smb.conf`



Примечание

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

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

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

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

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

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

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



Примечание

Samba использует отдельную от системной базу данных пользователей. Для возможности доступа пользователя к папке (если запрещен гостевой доступ) необходимо внести его в базу данных Samba и установить пароль для доступа к общим ресурсам (он может совпадать с основным паролем пользователя). Следует учитывать, что в базу данных Samba можно добавлять пользователей, которые уже есть в системе.

Добавить пользователя в базу данных Samba можно, выполнив команду (должен быть установлен пакет `samba-common-client`):

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

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

Раздел `[global]`

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

Раздел `[homes]`

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

Раздел [printers]

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



Примечание

Для возможности использования файлового ресурса [homes], необходимо добавить каждого локального пользователя в список пользователей Samba, например:

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



Примечание

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



Примечание

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

Описание некоторых параметров:

- **browseable** — определяет, отображается ли этот общий ресурс в списке доступных общих ресурсов в сетевом окружении и в списке просмотра (по умолчанию: browseable = yes);
- **path** — указывает каталог, к которому должен быть предоставлен доступ;
- **read only** — если для этого параметра задано значение «yes», то пользователи службы не могут создавать или изменять файлы в каталоге (по умолчанию: read only = yes);
- **writable** — инвертированный синоним для **read only** (по умолчанию: writeable = no);

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

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

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

[homes]
    comment = Home Directory for '%u'
    browseable = no
    writable = yes
    guest ok = no

[share]
    comment = 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
Password for [WORKGROUP\user]:
```

Sharename	Type	Comment
-----	----	-----
share	Disk	Commonplace
public	Disk	Public Stuff
Free	Disk	
IPC\$	IPC	IPC Service (Samba Server Version 4.15.9)
user	Disk	Home Directory for 'user'

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



Примечание

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

13.2. Монтирование ресурса Samba через /etc/fstab

Создать файл **/etc/samba/smbacreds** (например, командой **mcedit /etc/samba/smbacreds**), 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/smbacreds 0
0
```

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

```
# chmod 600 /etc/samba/smbacreds
```

и принадлежать root:

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

Глава 14. FreeIPA

14.1. Установка сервера FreeIPA

14.2. Добавление новых пользователей домена

14.3. Установка FreeIPA клиента и подключение к серверу

14.4. Удаление клиента FreeIPA

14.5. Настройка репликации

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.

14.1. Установка сервера FreeIPA

В качестве примера показана установка сервера **FreeIPA** со встроенным DNS сервером и доменом EXAMPLE.TEST в локальной сети 192.168.0.0/24. В примере для установки сервера используется узел: ipa.example.test (192.168.0.113).

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

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

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
```



Примечание

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

Команда установки сервера FreeIPA в пакетном режиме:

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

Для пакетной установки необходимо указать следующие параметры:

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

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

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



Предупреждение

Если в дальнейшем на данной машине будет настраиваться **Fleet Commander Admin**, необходимо устанавливать и настраивать FreeIPA сервер, с созданием домашнего каталога (опция **--mkhomedir**):

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

Для запуска интерактивной установки следует выполнить команду:

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

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 (пароли должны быть не менее 8 символов).

После завершения процесса конфигурации будет выведена подсказка со следующими шагами.

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/>.



Примечание

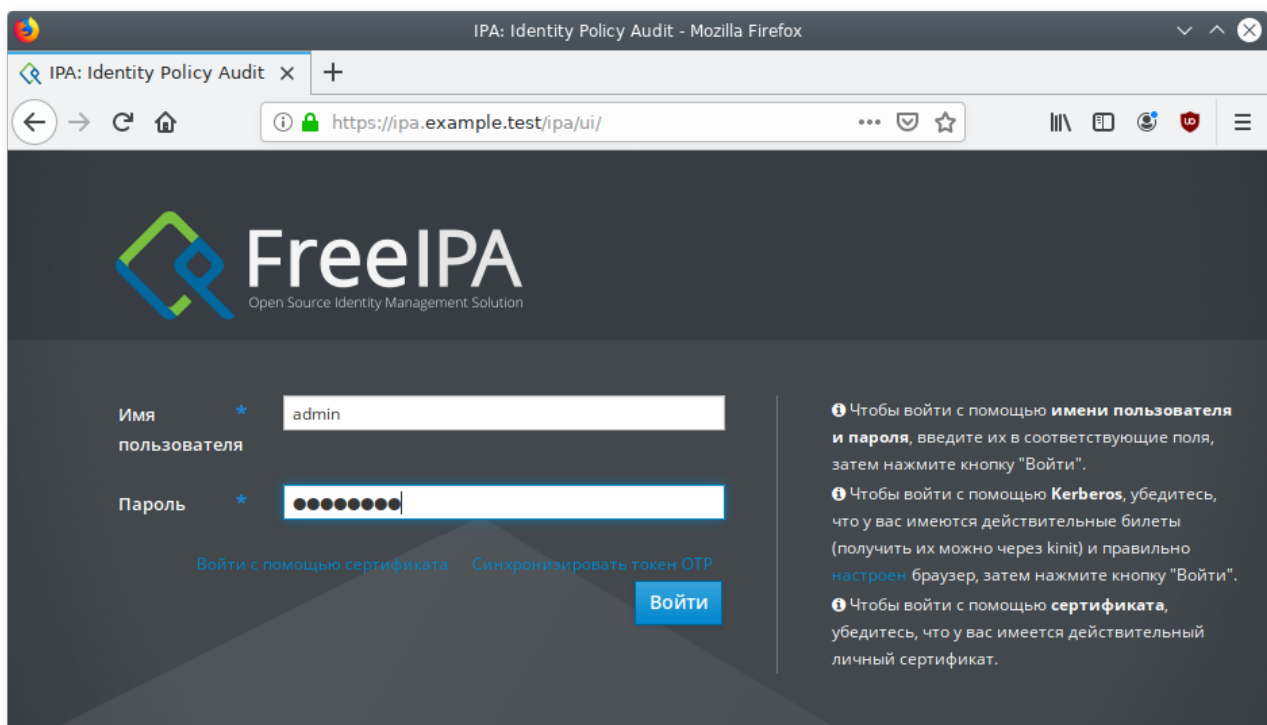
В случае сбоя установки сервера FreeIPA некоторые файлы конфигурации могут быть уже сконфигурированы. В этом случае дополнительные попытки установить сервер FreeIPA завершатся неудачно. Чтобы решить эту проблему, перед повторной попыткой запуска процесса установки, следует удалить частичную конфигурацию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

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

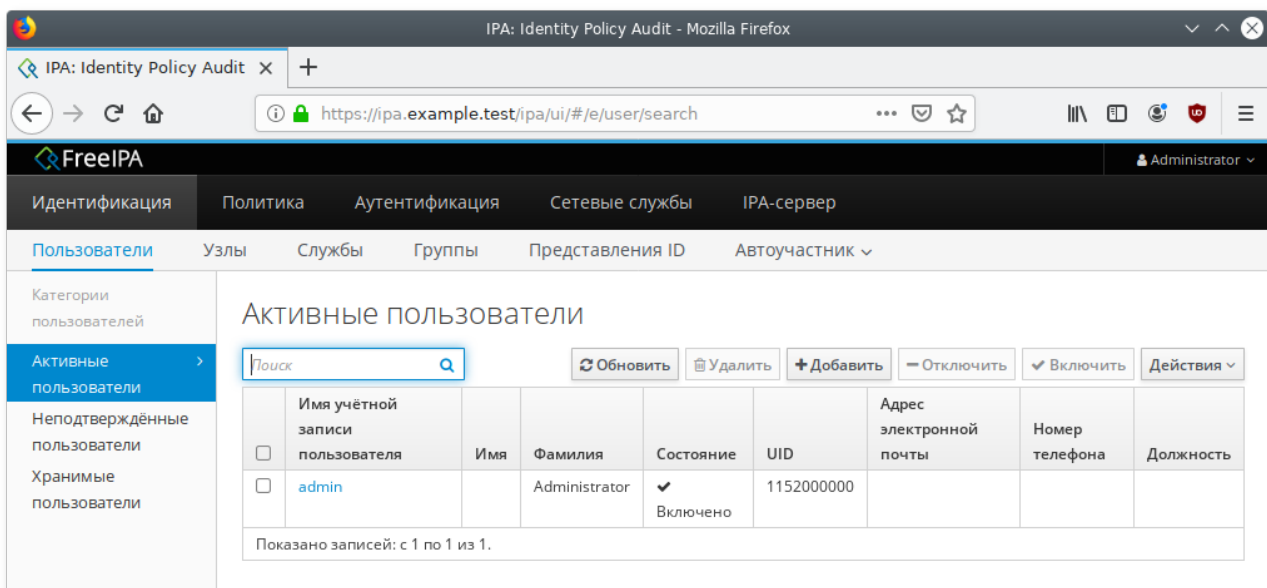
Если ошибки при установке сервера FreeIPA остаются, следует переустановить ОС. Одним из требований для установки сервера FreeIPA является чистая система без каких-либо настроек.

14.2. 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**:

Добавить пользователя



Имя учётной
записи
пользователя

user_freeipa

Имя *

Егор

Фамилия *

Иванов

Класс

Без личной
группы

☐

ID группы

1152000000



Новый пароль

••••••••

Проверить
пароль

••••••••

* Обязательное поле

Добавить

Добавить и добавить ещё

Добавить и изменить

Отменить

Созданный пользователь появится в списке пользователей:

Активные пользователи

Поиск



Обновить

Удалить

+ Добавить

Отключить

Включить

Действия

	Имя учётной записи пользователя	Имя	Фамилия	Состояние	UID	Адрес электронной почты	Номер телефона	Должность
<input type="checkbox"/>	admin		Administrator	✓ Включено	1152000000			
<input type="checkbox"/>	user_freeipa	Егор	Иванов	✓ Включено	1152000001	user_freeipa@example.test		

Показано записей: с 1 по 2 из 2.

14.3. Установка FreeIPA клиента и подключение к серверу

14.3.1. Установка FreeIPA клиента

Установить необходимые пакеты:

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

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

В сетевых настройках необходимо указать использовать сервер FreeIPA для разрешения имен:

■ В консоли:

■ задать имя компьютера:

```
# hostnamectl set-hostname comp01.example.test
```

■ добавить DNS сервер, для этого необходимо создать файл **/etc/net/ifaces/eth0/resolv.conf** со следующим содержимым:

```
nameserver 192.168.0.113
```

где 192.168.0.113 — IP-адрес FreeIPA сервера.

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

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

где eth0 — интерфейс на котором доступен FreeIPA сервер, example.test — домен.

■ обновить DNS адреса:

```
# resolvconf -u
```



Примечание

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

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

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

14.3.2. Подключение к серверу в консоли

Запустить скрипт настройки клиента в пакетном режиме:

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

или интерактивно:

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

Если все настроено, верно, скрипт должен выдать такое сообщение:

```
'''Discovery was successful!'''
Client hostname: comp01.example.test
Realm: EXAMPLE.TEST
DNS Domain: example.test
IPA Server: ipa.example.test
BaseDN: dc=example,dc=test
Continue to configure the system with these values? [no]:
```

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



Предупреждение

Если при входе в домен возникает такая ошибка:

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

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

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

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

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

```
# control sudo public
```

14.4. Удаление клиента FreeIPA

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

Для удаления клиента FreeIPA необходимо:

1. На клиенте ввести команду:

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

2. На клиенте удалить, если они есть, старые принципы Kerberos (кроме `/etc/krb5.keytab`):

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

3. На сервере FreeIPA удалить все записи DNS для клиентского узла:

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

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

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

14.5. Настройка репликации

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



Примечание

Перед настройкой репликации необходимо настроить систему на использование DNS-сервера, который был сконфигурирован на сервере FreeIPA во время его установки (см. пример настройки в разделе [Установка FreeIPA клиента](#)).

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

Установка реплики с использованием случайного пароля:

1. На сервере FreeIPA получить билет Kerberos:

```
$ kinit admin
```

2. На сервере FreeIPA добавить внешнюю систему в качестве узла FreeIPA:

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

3. На сервере FreeIPA добавить систему replica.example.test в группу узлов ipaservers:

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

4. На машине, где будет установлена реплика, установить необходимые пакеты:

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

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

```
# ipa-replica-install --password='2AaT0Ix8itDsYugdDGoRtBt' --setup-ca --
setup-dns --forwarder 192.168.0.113 --forwarder 8.8.8.8
Configuring client side components
This program will set up IPA client.
Version 4.9.10

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

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

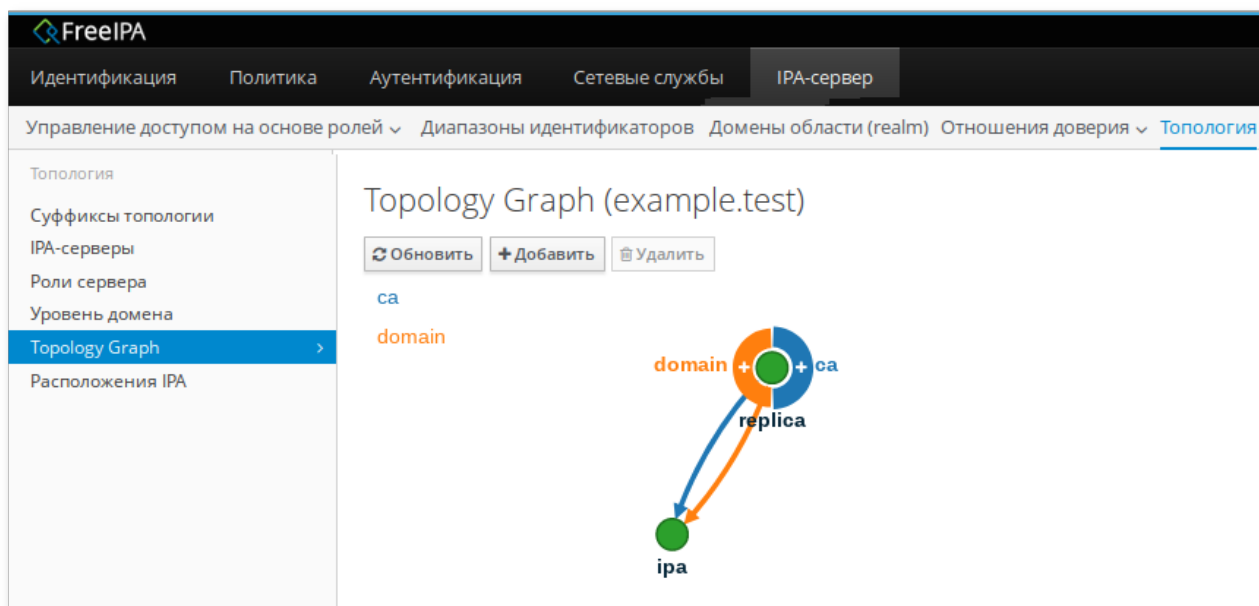
1. Создать пользователя на новой реплике:

```
$ ipa user-add test_user
```

2. Убедиться, что пользователь виден на другой реплике:

```
$ ipa user-show test_user
```

После настройки и репликации контроллеров можно посмотреть топологию в веб-интерфейсе FreeIPA (IPA-сервер → Топология → Topology Graph):



Глава 15. Установка LEMP сервера (Linux, Nginx, MySQL, PHP)

15.1. Установка веб-сервера Nginx

15.2. Установка MySQL

15.3. Установка php

15.4. Конфигурирование Nginx для использования php

15.5. Тестирование подключения к базе данных из PHP

LEMP — это набор (комплекс) серверного программного обеспечения, используемый для разработки и развертывания веб-приложений. LEMP состоит из следующих компонентов: Linux — операционная система; Nginx — веб-сервер; MariaDB/MySQL — СУБД; PHP — язык программирования.

LEMP — это аналог стека LAMP (Linux, Apache, MySQL и PHP).



Примечание

В этом разделе в качестве примера доменного имени используется домен test.alt.

15.1. Установка веб-сервера Nginx

Установить пакет *nginx*:

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

Запустить Nginx и добавить его в автозагрузку:

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

Создать корневой каталог для домена:

```
# mkdir -p /var/www/test.alt
```

Создать файл конфигурации **/etc/nginx/sites-available.d/test.alt.conf** на основе **/etc/nginx/sites-available.d/default.conf**:

```
# cp /etc/nginx/sites-available.d/default.conf /etc/nginx/sites-available.d/test.alt.conf
```

Внести изменения в файл конфигурации **/etc/nginx/sites-available.d/test.alt.conf**:

```
server {
    listen *:80;
    server_name test.alt www.test.alt;

    location / {
        root /var/www/test.alt;
    }

    access_log /var/log/nginx/test.alt-access.log;
}
```

Активировать конфигурацию:

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

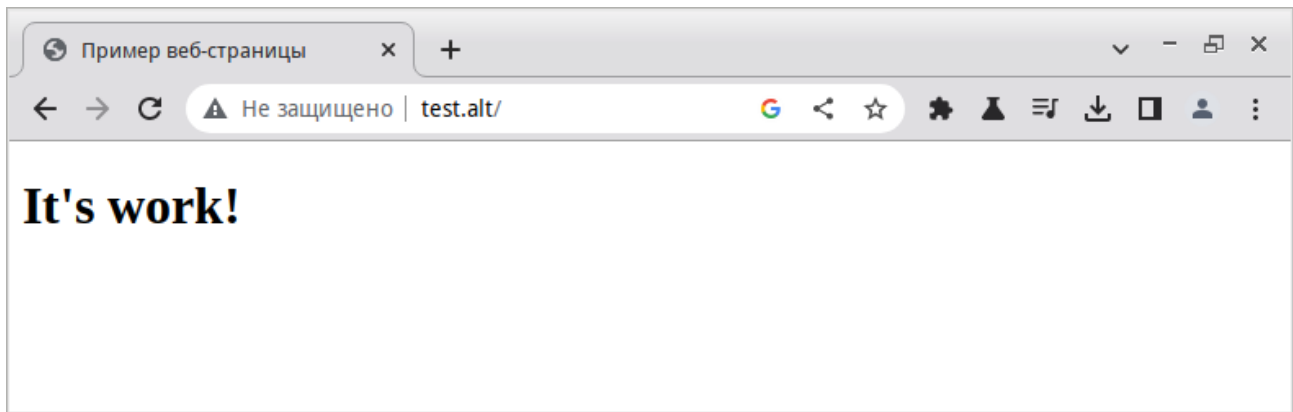
Перезапустить Nginx:

```
# systemctl reload nginx
```

Создать файл **/var/www/test.alt/index.html** со следующим содержимым:

```
<html>
<head>
  <title>Пример веб-страницы</title>
</head>
<body>
  <h1>It's work!</h1>
</body>
</html>
```

Для проверки работы веб-сервера, в веб-браузере открыть страницу <http://IP-сервера> или <http://домен>:



Администрирование сервера Nginx в основном заключается в настройке и поддержке его файлов конфигурации:

- » **/etc/nginx/nginx.conf** — главный файл конфигурации Nginx;
- » **/etc/nginx/sites-available** — каталог с конфигурациями виртуальных хостов (каждый файл, находящийся в этом каталоге, содержит информацию о конкретном сайте);
- » **/etc/nginx/sites-enabled** — в этом каталоге содержатся конфигурации активных сайтов, обслуживаемых Nginx.

15.2. Установка MySQL

MySQL — это система управления базами данных (СУБД), которая используется для организации и получения контента. MariaDB имеет те же возможности, что и MySQL, и при этом является полностью бесплатной.

Установить MySQL (MariaDB):

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

Запустить и добавить в автозагрузку сервер MySQL:

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

Задать пароль root для MySQL и настройки безопасности:

```
# mysql_secure_installation
```

Далее можно проверить возможность входа в консоль MySQL:

```
$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 24
Server version: 10.6.9-MariaDB-alt1 (ALT p10)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
```

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
MariaDB [(none)]> exit  
$
```



Примечание

Для подключения к MySQL в качестве пользователя root можно не указывать пароль, даже если он был определен при запуске скрипта **mysql_secure_installation**. Это связано с тем, что метод аутентификации по умолчанию для пользователя root в MySQL — `unix_socket`. Пользователями, которым разрешено входить в систему в качестве пользователя root MySQL, являются системные пользователи с привилегиями `sudo`, подключающиеся из консоли или через приложение, работающее с одинаковыми привилегиями.

```
# mysql  
MariaDB [(none)]> exit  
#
```

Для повышения безопасности лучше иметь выделенные учетные записи пользователей с менее широкими привилегиями, настроенными для каждой базы данных, особенно если на сервере планируется размещать несколько баз данных.

15.3. Установка php



Примечание

Начиная с версии php8.0, пакеты модулей именуются следующим образом: `php<мажорная>.<минорная>.<имя модуля>`. Из репозитория можно установить и эксплуатировать в одной системе одновременно разные версии php. В данном руководстве в качестве примера используется php8.2.

Установить пакеты:

```
# apt-get install php8.2-fpm-fcgi php8.2-mysqldb php8.2-mysqldb-mysqldb
```

Запустить php8.2-fpm и добавить его в автозагрузку:

```
# systemctl enable --now php8.2-fpm
```



Примечание

Чтобы узнать версию PHP, которая установлена, можно воспользоваться командой:

```
$ php -v
```


15.4. Конфигурирование Nginx для использования php

Внести изменения в файл конфигурации `/etc/nginx/sites-available.d/test.alt.conf`:

```
server {
    listen *:80;
    # can't use wildcards in first server_name
    server_name test.alt www.test.alt;
    index      index.php;
    root /var/www/test.alt;
    location / {
        try_files $uri =404;
    }

    location ~ \.php$ {
        try_files $uri =404;
        include /etc/nginx/fastcgi_params;
        fastcgi_pass unix:/var/run/php8.2-fpm/php8.2-fpm.sock;
        fastcgi_param SCRIPT_FILENAME /var/www/test.alt/$fastcgi_script_name;
    }
    access_log /var/log/nginx/test.alt-access.log;
}
```

Описание директив из файла конфигурации:

- **listen** — задаёт адрес и порт, на которых сервер будет принимать запросы. Можно указать адрес и порт, либо только адрес или только порт;
- **root** — определяет корневой каталог, в котором хранятся файлы, обслуживаемые данным веб-сайтом;
- **index** — определяет файлы, которые будут использоваться в качестве индекса. В имени файла можно использовать переменные. Наличие файлов проверяется в порядке их перечисления;
- **server_name** — определяет имя виртуального сервера (в этой директиве необходимо указать доменное имя сервера или общедоступный IP-адрес);
- **location /** — первый блок location включает директиву **try_files**, которая проверяет наличие файлов или каталогов, соответствующих запросу URI. Если Nginx не может найти подходящий ресурс, он вернет ошибку 404;
- **location ~ \.php\$** — этот блок location включает фактическую обработку PHP, указывая Nginx на файл конфигурации `fastcgi-php.conf` и файл `php8.2-fpm.sock`, который объявляет, какой сокет связан с `php-fpm`;
- **location ~ /\.ht** — этот блок location имеет дело с файлами **.htaccess**, которые Nginx не обрабатывает. При добавлении директивы **deny all**, если какие-либо файлы **.htaccess** попадут в корень документа, они не будут показываться посетителям.

Проверить конфигурацию на наличие синтаксических ошибок, можно выполнив команду:

```
# nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

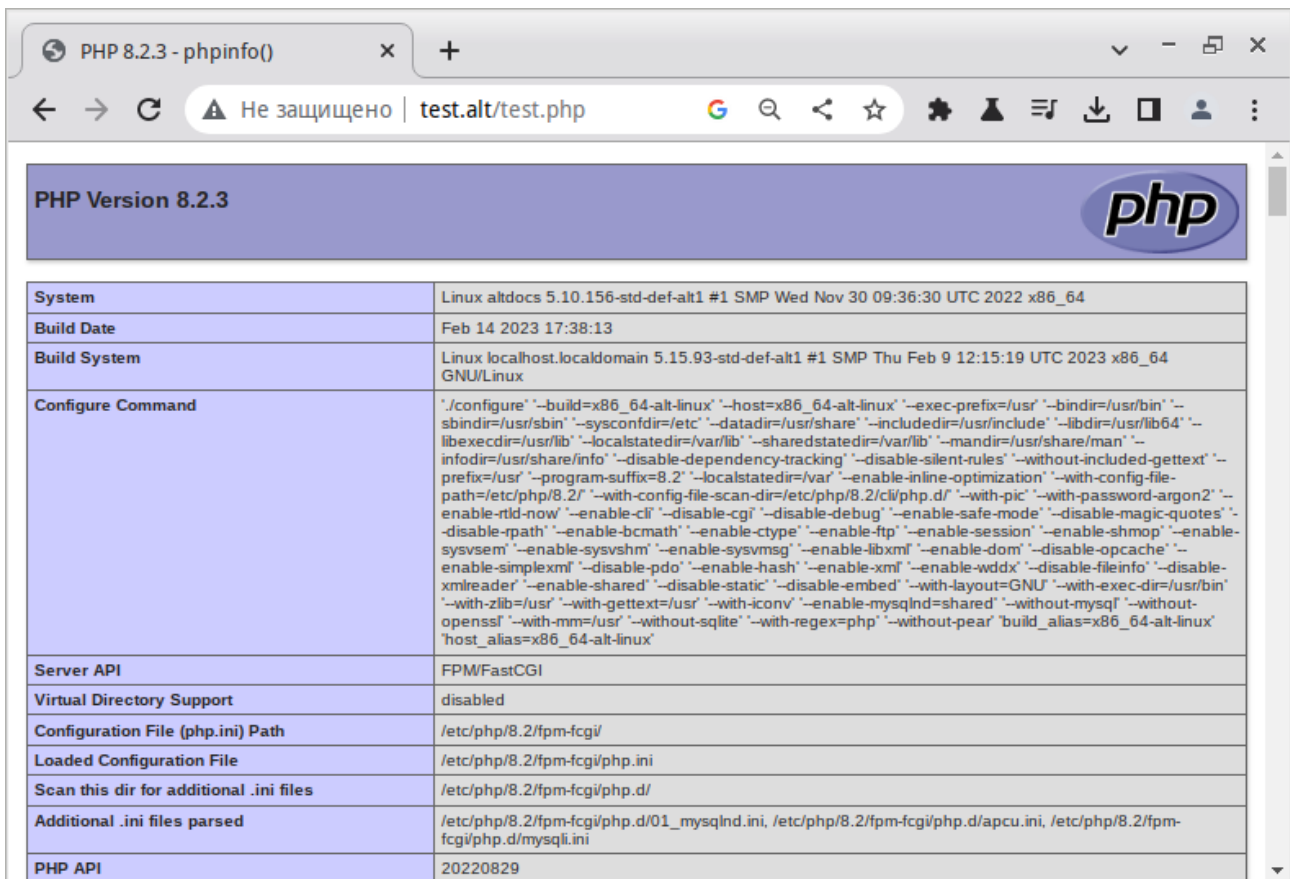
Если ошибки отсутствуют, необходимо перезагрузить Nginx, чтобы применить изменения:

```
# systemctl reload nginx.service
```

Для проверки того что Nginx правильно передаёт файлы .php PHP-процессору можно создать тестовый файл `/var/www/test.alt/test.php` со следующим содержимым:

```
<?php phpinfo(); ?>
```

При открытии этого файла по URL `http://test.alt/test.php` будет доступна информация о PHP:



PHP Version 8.2.3	
System	Linux altdocs 5.10.156-std-def-alt1 #1 SMP Wed Nov 30 09:36:30 UTC 2022 x86_64
Build Date	Feb 14 2023 17:38:13
Build System	Linux localhost.localdomain 5.15.93-std-def-alt1 #1 SMP Thu Feb 9 12:15:19 UTC 2023 x86_64 GNU/Linux
Configure Command	"/configure" "--build=x86_64-alt-linux" "--host=x86_64-alt-linux" "--exec-prefix=/usr" "--bindir=/usr/bin" "--sbindir=/usr/sbin" "--sysconfdir=/etc" "--datadir=/usr/share" "--includedir=/usr/include" "--libdir=/usr/lib64" "--libexecdir=/usr/lib" "--localstatedir=/var/lib" "--sharedstatedir=/var/lib" "--mandir=/usr/share/man" "--infodir=/usr/share/info" "--disable-dependency-tracking" "--disable-silent-rules" "--without-included-gettext" "--prefix=/usr" "--program-suffix=8.2" "--localstatedir=/var" "--enable-inline-optimization" "--with-config-file-path=/etc/php/8.2/" "--with-config-file-scan-dir=/etc/php/8.2/cli/php.d/" "--with-pic" "--with-password-argon2" "--enable-rtld-now" "--enable-cli" "--disable-cgi" "--disable-debug" "--enable-safe-mode" "--disable-magic-quotes" "--disable-rpath" "--enable-bcmath" "--enable-ctype" "--enable-ftp" "--enable-session" "--enable-shmop" "--enable-sysvsem" "--enable-sysvshm" "--enable-sysvmsg" "--enable-libxml" "--enable-dom" "--disable-opcache" "--enable-simplexml" "--disable-pdo" "--enable-hash" "--enable-xml" "--enable-wddx" "--disable-fileinfo" "--disable-xmlreader" "--enable-shared" "--disable-static" "--disable-embed" "--with-layout=GNU" "--with-exec-dir=/usr/bin" "--with-zlib=/usr" "--with-gettext=/usr" "--with-iconv" "--enable-mysqlnd=shared" "--without-mysql" "--without-openssl" "--with-mm=/usr" "--without-sqlite" "--with-regex=php" "--without-pear" 'build_alias=x86_64-alt-linux'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.2/fpm-fcgi
Loaded Configuration File	/etc/php/8.2/fpm-fcgi/php.ini
Scan this dir for additional .ini files	/etc/php/8.2/fpm-fcgi/php.d/
Additional .ini files parsed	/etc/php/8.2/fpm-fcgi/php.d/01_mysqlnd.ini, /etc/php/8.2/fpm-fcgi/php.d/apcu.ini, /etc/php/8.2/fpm-fcgi/php.d/mysql.ini
PHP API	20220829

После проверки информации о PHP-сервере лучше всего удалить созданный файл, поскольку он содержит информацию о среде PHP и сервере:

```
# rm /var/www/test.alt/test.php
```

15.5. Тестирование подключения к базе данных из PHP

Для тестирования подключения к базе данных из PHP создадим базу данных с именем `example_database` и пользователя с именем `example_user`:

```
# mysql
```

Создать новую БД:

```
MariaDB [(none)]> CREATE DATABASE example_db;  
Query OK, 1 row affected (0,000 sec)
```

Создать нового пользователя и предоставить ему полные права доступа к базе данных example_database:

```
MariaDB [(none)]> CREATE USER 'example_user'@'%' IDENTIFIED BY 'password';  
Query OK, 0 rows affected (0,002 sec)
```

Предоставить пользователю example_user все права на базу example_db:

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON example_db.* TO 'example_user'@'%;  
Query OK, 0 rows affected (0,002 sec)  
MariaDB [(none)]> FLUSH PRIVILEGES;  
Query OK, 0 rows affected (0,000 sec)
```

Выйти из оболочки MySQL:

```
MariaDB [(none)]> exit;
```

Проверить, есть ли у нового пользователя надлежащие разрешения, снова войдя в консоль MySQL, с использованием пользовательских учетных данных пользователя:

```
$ mysql -u example_user -p  
Enter password:  
MariaDB [(none)]>
```

После входа в консоль MySQL убедитесь, что у пользователя example_user есть доступ к базе данных example_database:

```
MariaDB [(none)]> SHOW DATABASES;  
+-----+  
| Database |  
+-----+  
| example_db |  
| information_schema |  
+-----+  
2 rows in set (0,000 sec)
```

Создать таблицу и заполнить её тестовыми данными:

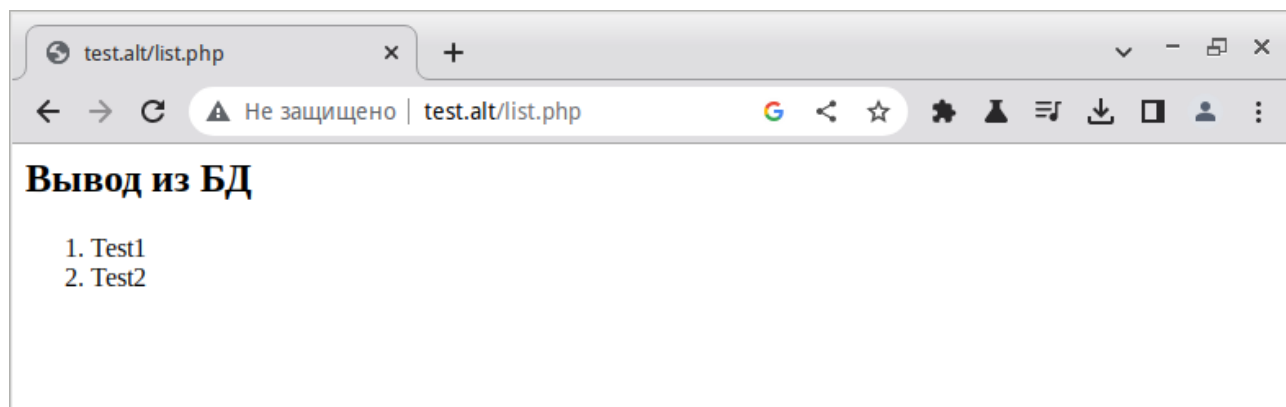
```
MariaDB [(none)]> USE example_db;  
MariaDB [(none)]> CREATE TABLE test (item_id INT AUTO_INCREMENT, content  
VARCHAR(255), PRIMARY KEY(item_id));  
MariaDB [(none)]> INSERT INTO test (content) VALUES ("Test1");  
MariaDB [(none)]> INSERT INTO test (content) VALUES ("Test2");  
MariaDB [(none)]> EXIT
```

Создать скрипт PHP (/var/www/test.alt/list.php), который будет подключаться к MySQL и запрашивать контент, со следующим содержанием:

```
<?php  
$user = "example_user";  
$password = "password";  
$database = "example_db";  
$table = "test";  
$conn = mysqli_connect("localhost", $user, $password, $database);  
if (!$conn) {  
    die("Connection failed: " . mysqli_connect_error());  
}
```

```
}  
echo "<h2>Вывод из БД</h2><ol>";  
foreach($conn->query("SELECT content FROM $table") as $row) {  
    echo "<li>" . $row['content'] . "</li>";  
}  
echo "</ol>";  
mysqli_close($conn);  
?>
```

Открыть этот файл по URL **http://test.alt/list.php**:



Глава 16. Nextcloud — хранение документов в «облаке»

[16.1. Что такое Nextcloud](#)

[16.2. Настройка Nextcloud](#)

[16.3. Работа с Nextcloud](#)

16.1. Что такое Nextcloud

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

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

Основной сайт проекта: <https://nextcloud.com/>.

Развернуть Nextcloud можно используя пакет *deploy*:

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

Установить пароль пользователю ncadmin (пароль должен быть достаточно сложным и содержать не менее 10 символов):

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

16.2. Настройка Nextcloud

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



Важно

После внесения изменений в файл конфигурации Nextcloud необходимо перезагрузить веб-сервер.

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

```
'memcache.local' => '\OC\Memcache\Memcached',
'memcache.distributed' => '\OC\Memcache\Memcached',
'memcached_servers' => array(
    array('localhost', 11211),
),
```



Примечание

Для возможности настройки кэширования, должны быть установлены следующие пакеты:

```
# apt-get install memcached php8.0-memcached
```

Служба memcached должна быть добавлена в автозагрузку:

```
# systemctl enable --now memcached
```

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

```
'trusted_domains' =>
array (
    0 => 'localhost',
    1 => 'IP-адрес',
    2 => 'nextcloud.test.ru',
),
```

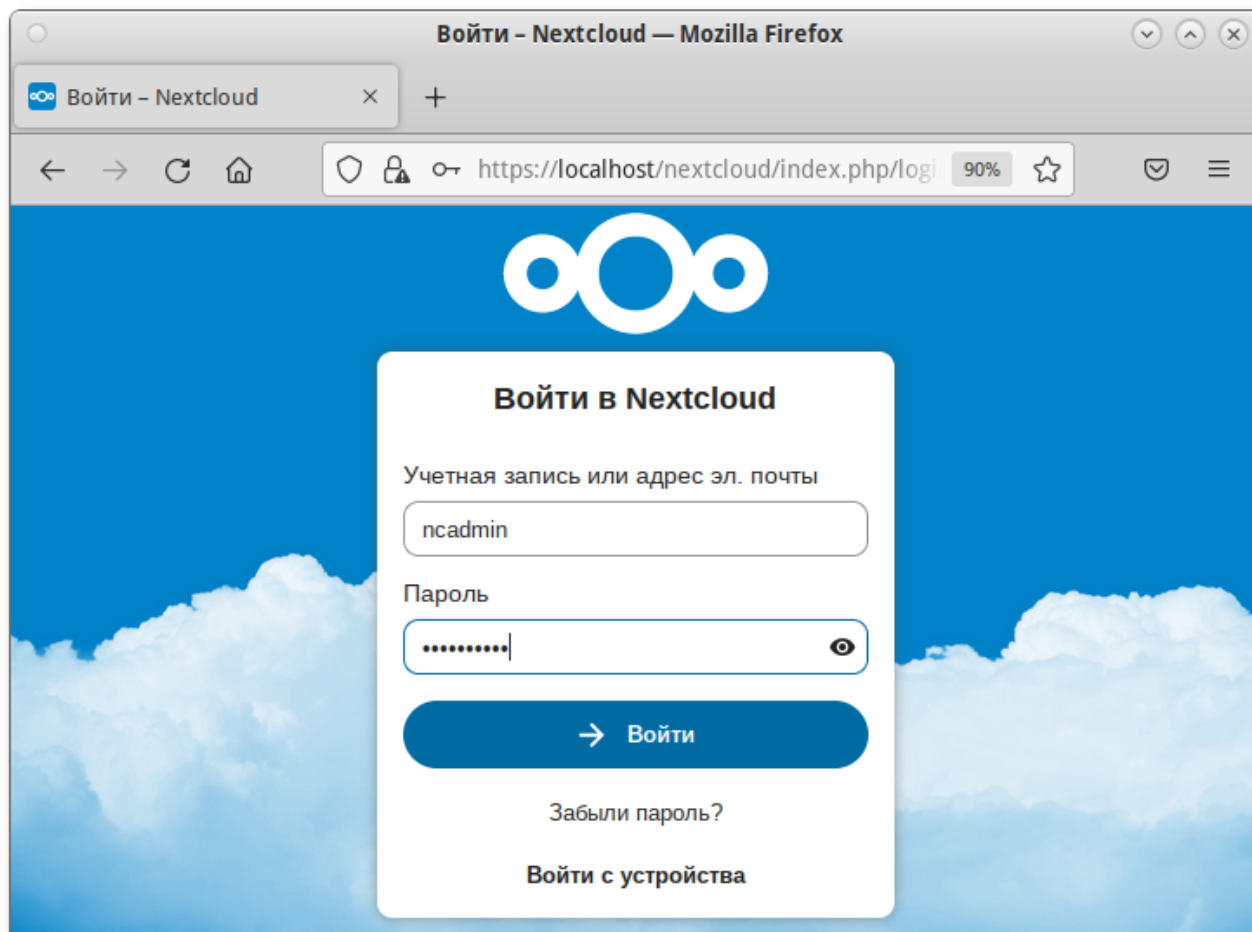
16.3. Работа с Nextcloud

Nextcloud доступен через веб-интерфейс по адресу **`https://IP-адрес/nextcloud/`**.
Администратор: `ncadmin`.

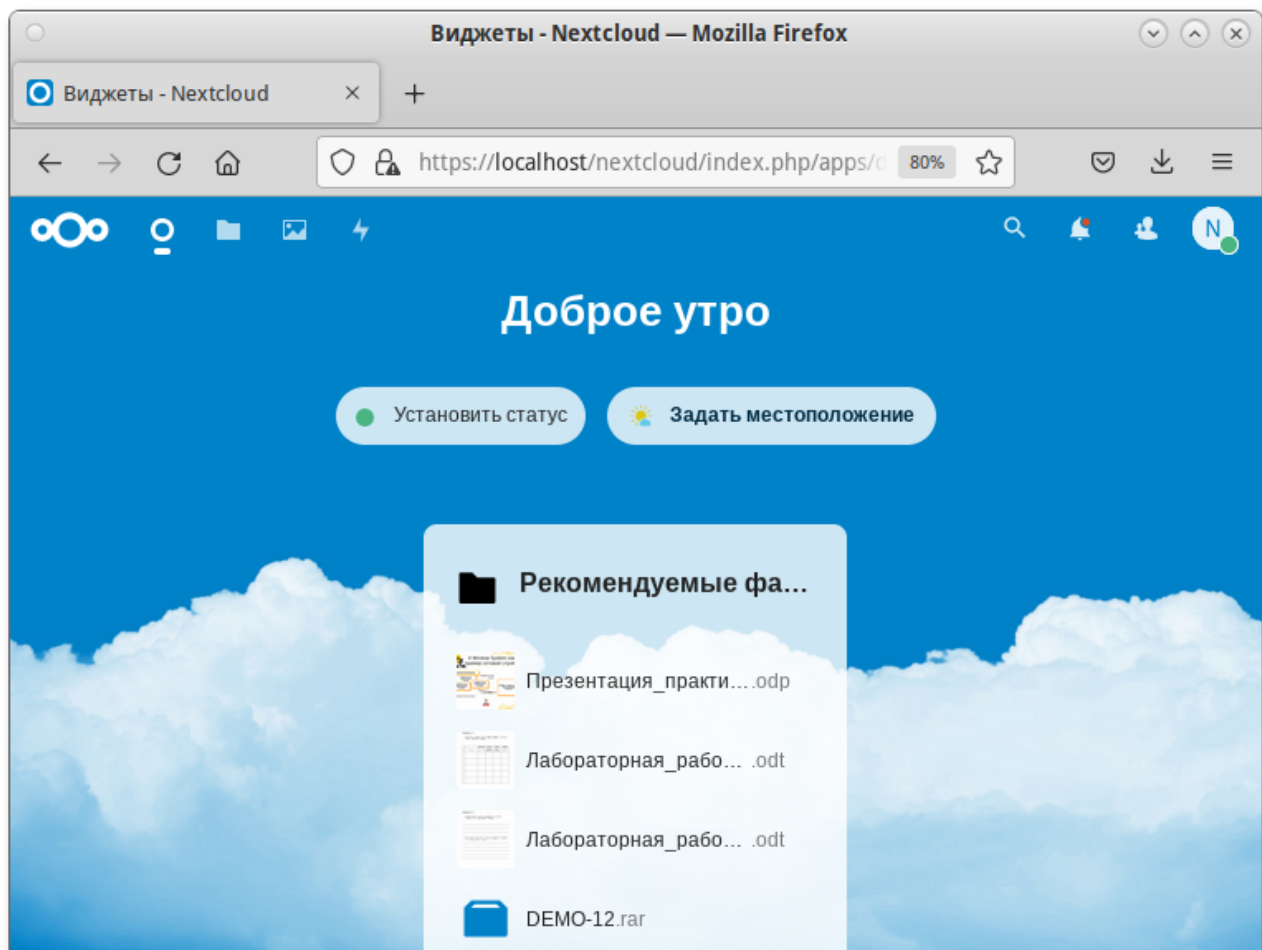


Примечание

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

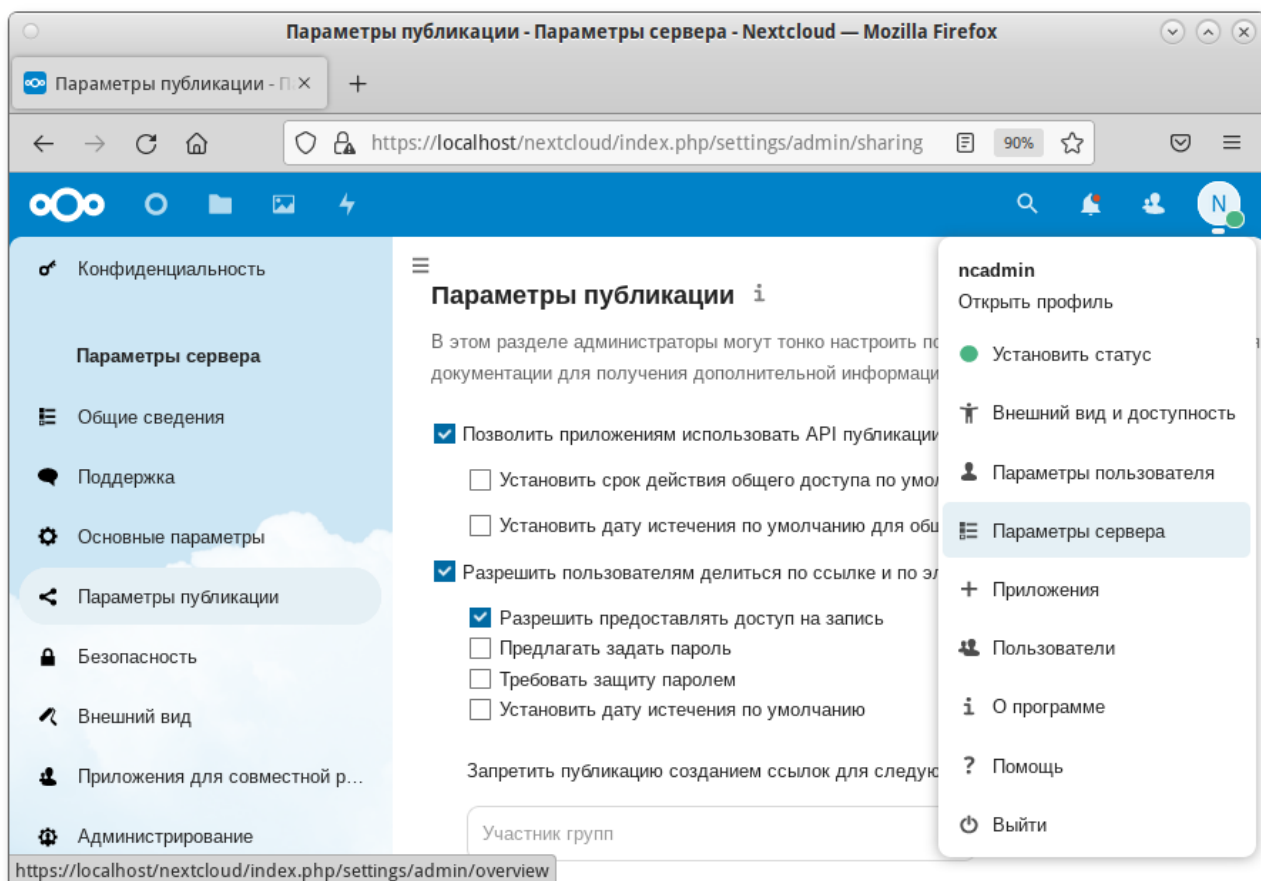


После авторизации открывается панель управления Nextcloud, которую можно настроить (с помощью виджетов) так, как хочет пользователь:



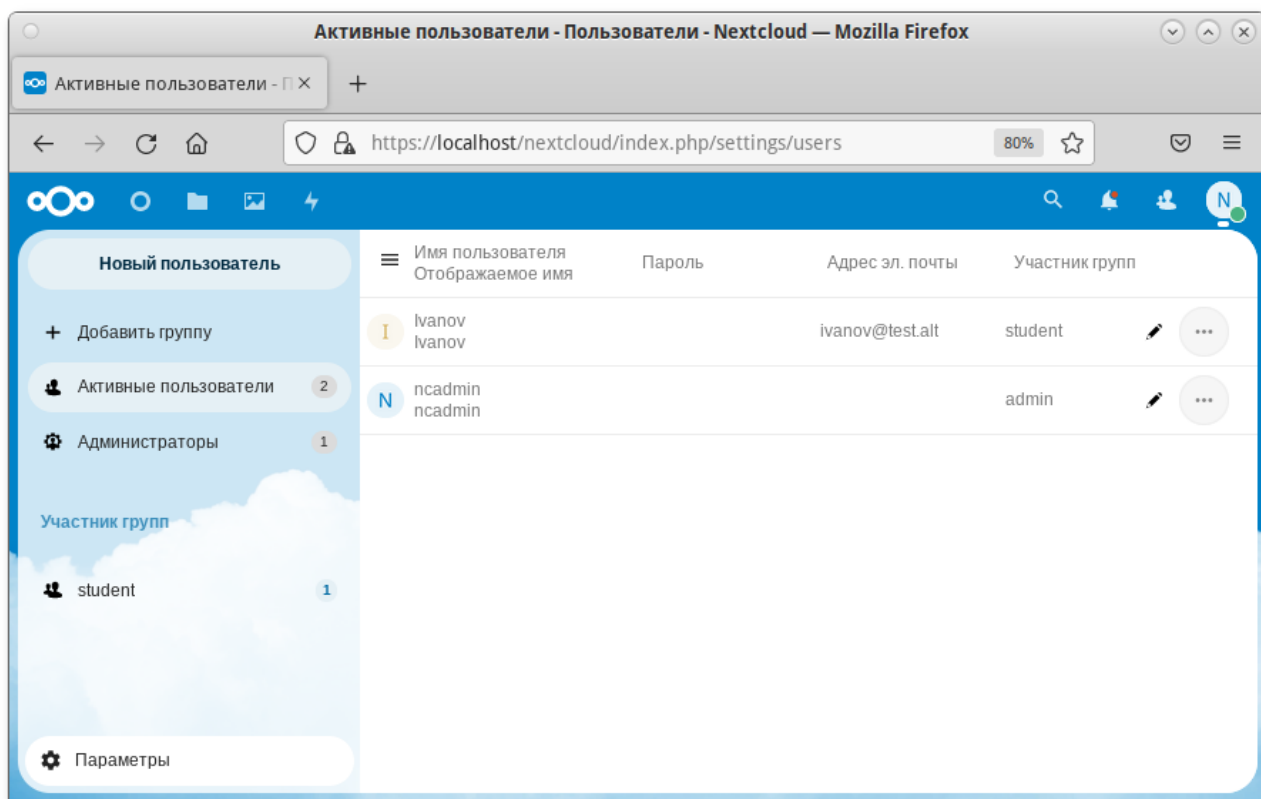
16.3.1. Администрирование

Основные настройки Nextcloud доступны на странице **Параметры сервера**. Открыть которую можно, щелкнув левой кнопкой мыши по логину администратора в правом верхнем углу и выбрав в выпадающем меню строку **Параметры сервера**:

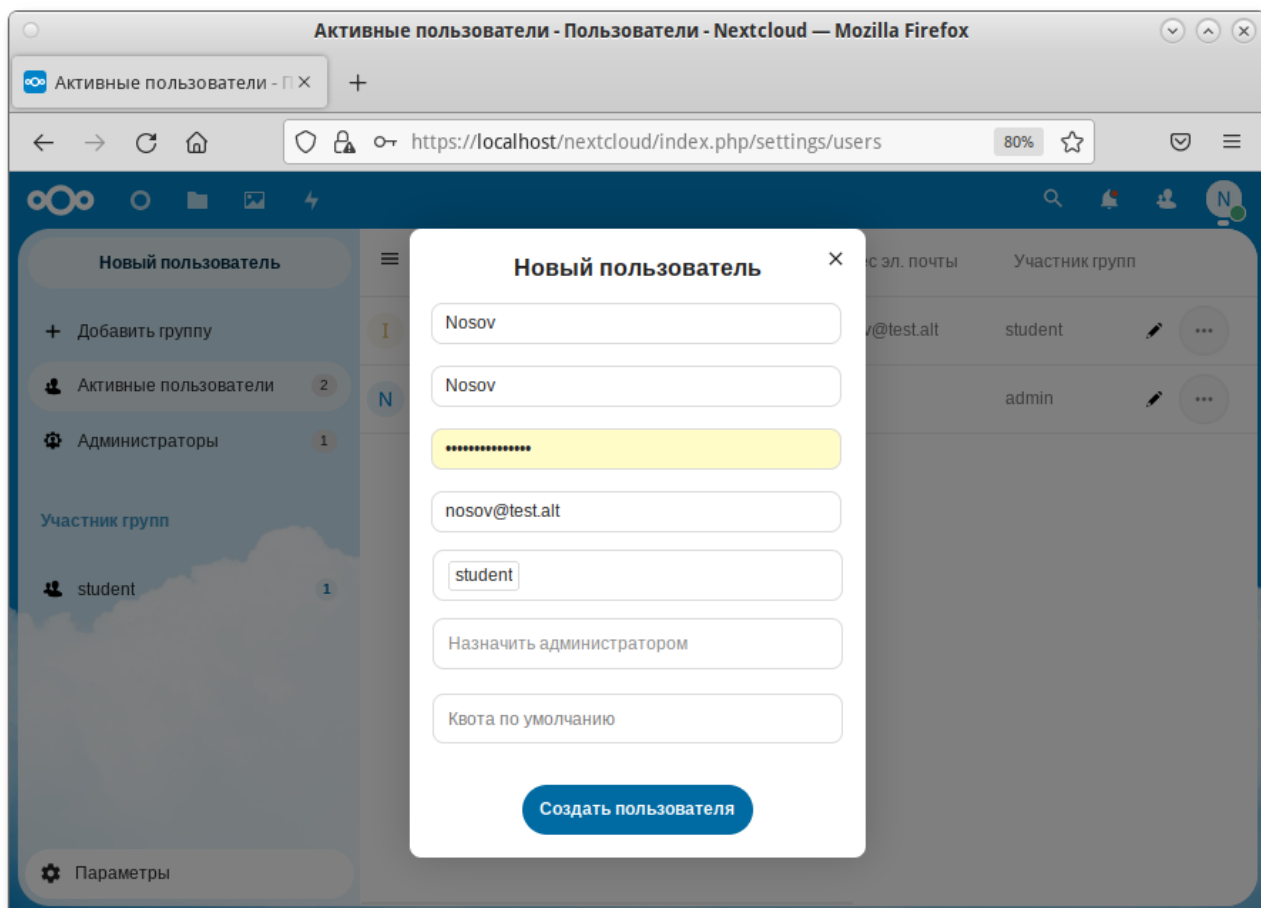


На странице **Активные пользователи** можно:

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

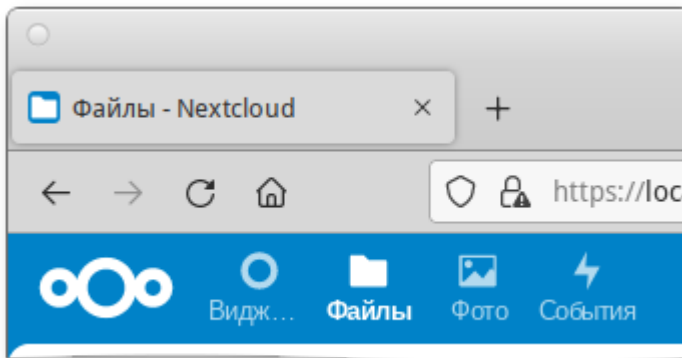


Для создания пользователя, следует нажать кнопку **Новый пользователь**, ввести **Имя пользователя**, **Пароль**, при необходимости указать группу и нажать кнопку **Создать пользователя**:

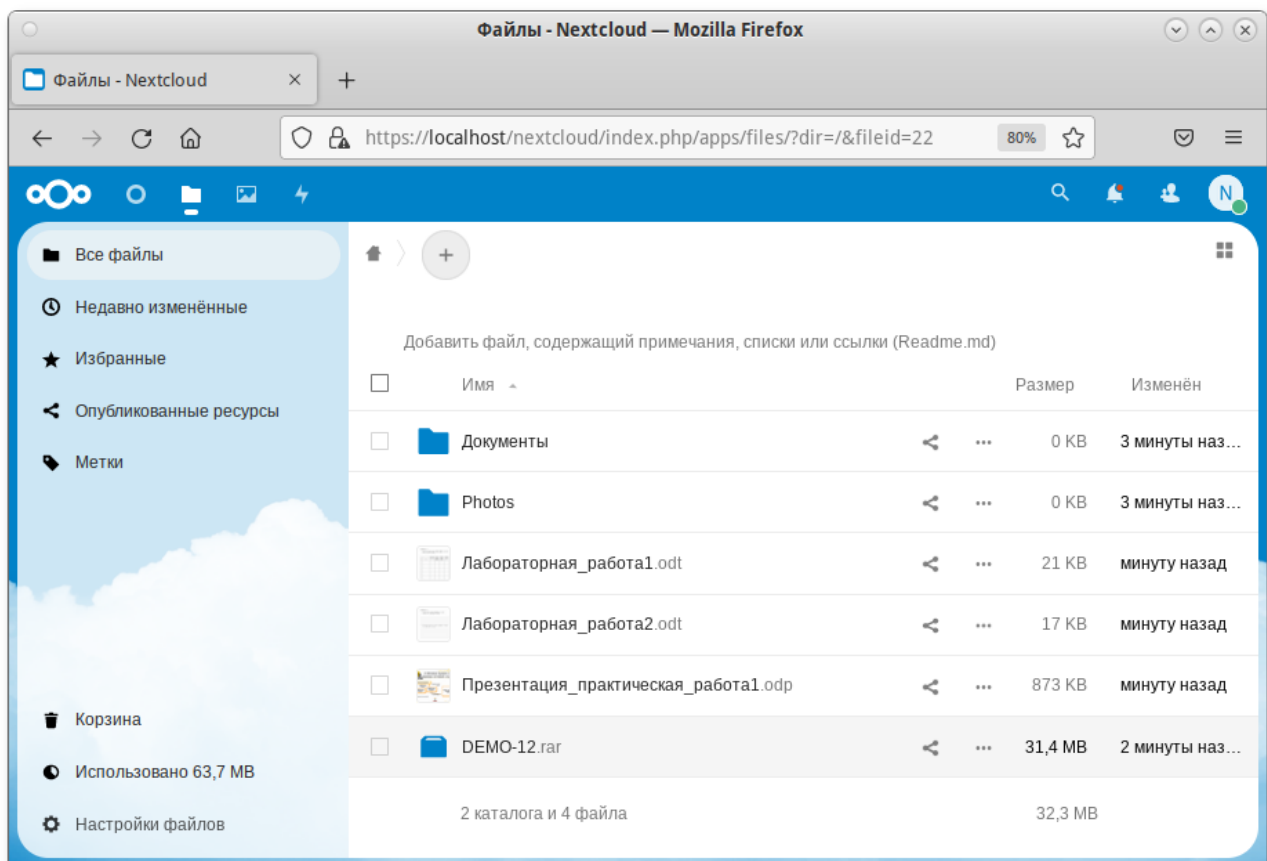


16.3.2. Работа с файлами

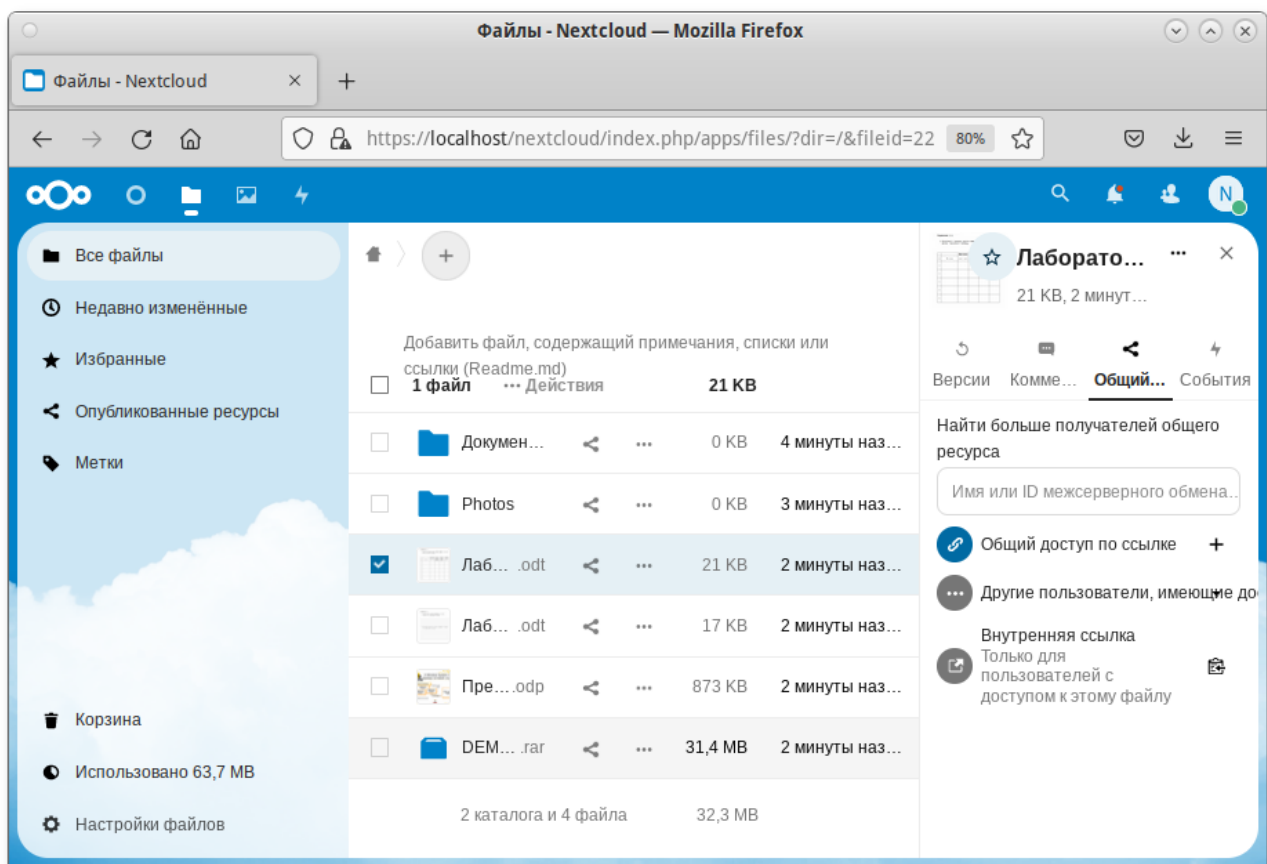
Меню выбора доступных сервисов, расположено в левом верхнем углу веб-интерфейса Nextcloud:



При выборе раздела **Файлы** отображается структура каталогов пользователя:



Для того чтобы поделиться файлом или папкой с другими пользователями, необходимо нажать на треугольный значок рядом с названием файла и в открывшемся окне настроить параметры общего доступа:



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

Глава 17. OpenUDS

17.1. Установка

17.2. Обновление OpenUDS

17.3. Настройка OpenUDS

17.4. Подготовка шаблона виртуальной машины

17.5. Настройка клиента OpenUDS

17.6. Подключение пользователя к виртуальному рабочему месту

17.7. Отказоустойчивое решение

OpenUDS это многоплатформенный брокер подключений для создания и управления виртуальными рабочими местами и приложениями.

Основные компоненты решения VDI на базе OpenUDS:

- OpenUDS Server (openuds-server) — брокер подключений пользователей, а так же интерфейс администратора для настройки;

- SQL Server. Для работы django-приложения, которым является openuds-server, необходим SQL сервер, например mysql или mariadb. SQL Server может быть установлен как на отдельном сервере, так и совместно с openuds-server;
- Платформа для запуска клиентских окружений и приложений. OpenUDS совместима со множеством систем виртуализации: PVE, OpenNebula, oVirt, OpenStack. Так же возможно использование с отдельным сервером без виртуализации (аналог терминального решения);
- OpenUDS Client (openuds-client) — клиентское приложение для подключения к брокеру соединений и дальнейшего получения доступа к виртуальному рабочему окружению;
- OpenUDS Tunnel (openuds-tunnel) — решение для туннелирования обращений от клиента к виртуальному рабочему окружению. OpenUDS Tunnel предназначен для предоставления доступа из недоверенных сегментов сети, например из сети Интернет. Устанавливается на отдельный сервер;
- OpenUDS Actor (openuds-actor) — ПО для гостевых виртуальных машин, реализует связку виртуальной машины и брокера соединений.

Таблица 17.1. Системные требования

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



Примечание

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

17.1. Установка

17.1.1. 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;
```

17.1.2. Установка OpenUDS Server

При этом будут установлены:

- `openuds-server` — django приложение;
- `gunicorn` — сервер приложений (обеспечивает запуск django как стандартного WSGI приложения);
- `nginx` — http-сервер, используется в качестве reverse-проxy для доступа к django приложению, запущенному с помощью `gunicorn`.

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
```

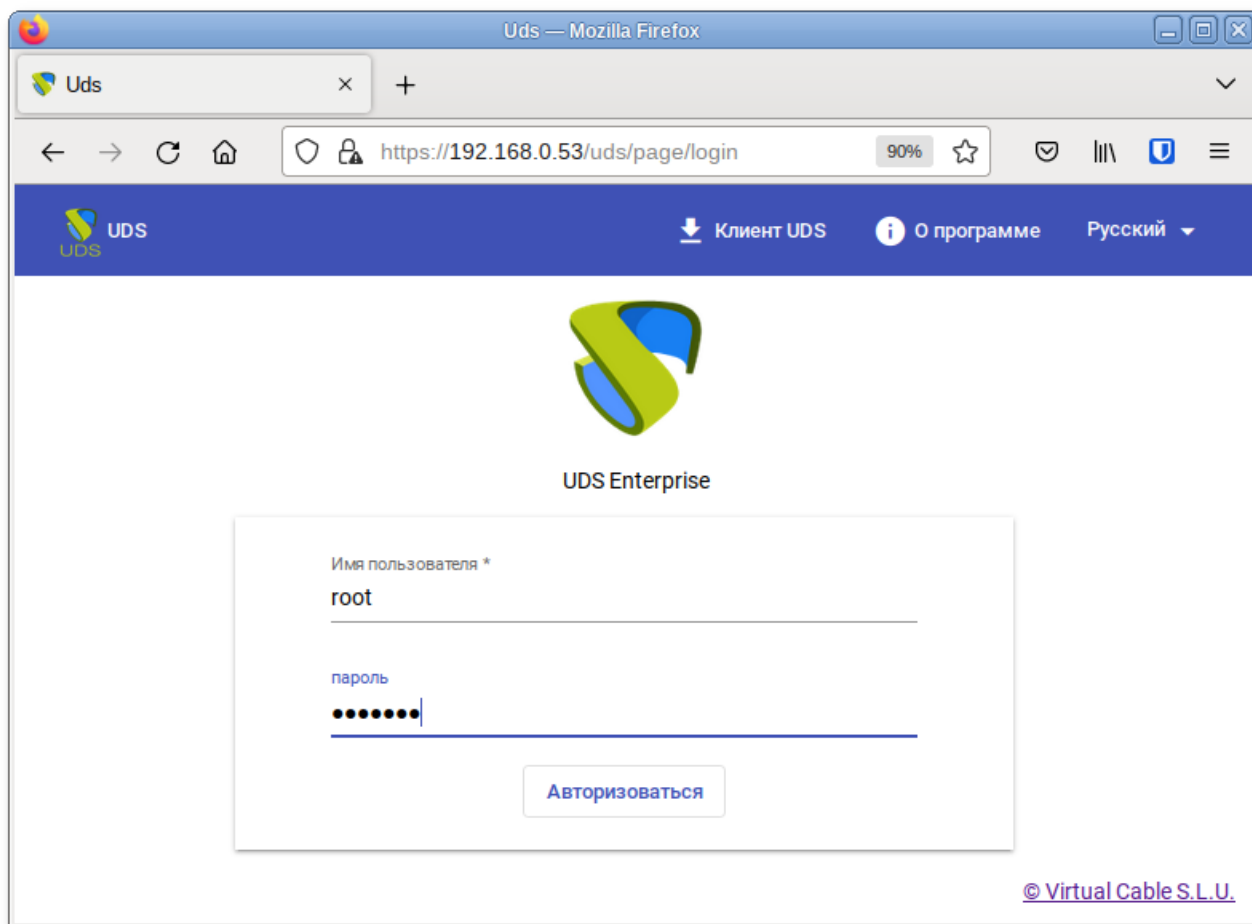
- запустить `nginx`:

```
# 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/>:



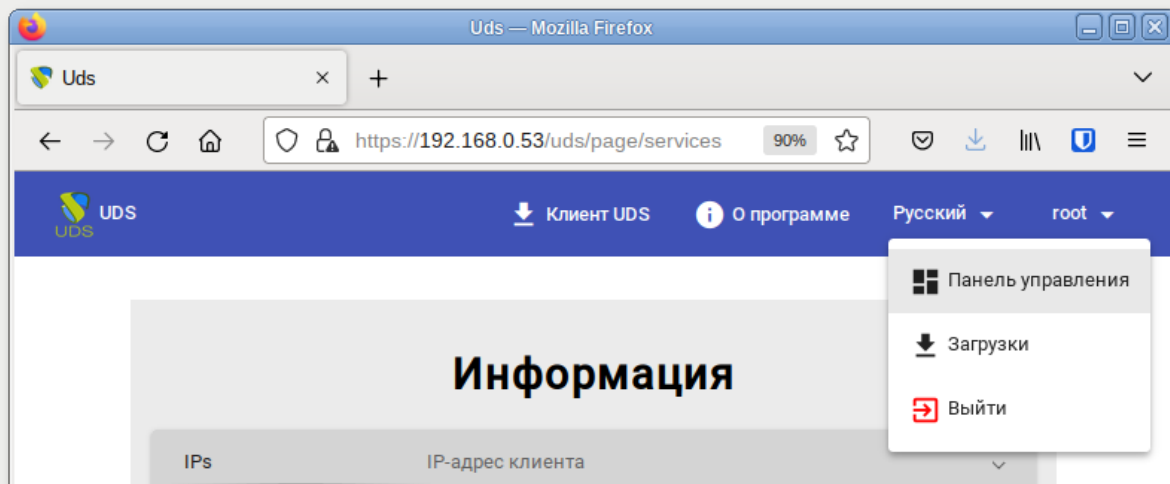
Примечание

Имя/пароль по умолчанию: root/udsmam0



Примечание

Для получения доступа к панели администрирования OpenUDS, следует в меню пользователя выбрать пункт **Панель управления**:



17.1.3. OpenUDS Tunnel

17.1.3.1. Установка OpenUDS Tunnel

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



Примечание

Установить пакет *openuds-tunnel*:

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



Примечание

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

17.1.3.2. Настройка OpenUDS Tunnel

На OpenUDS Tunnel:

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

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

где 192.168.0.53 — адрес OpenUDS сервера (брокера);

»запустить и добавить в автозагрузку сервис OpenUDS Tunnel:

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

На сервере OpenUDS зарегистрировать туннельный сервер, выполнив команду:

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

где:

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

При создании туннельного транспорта, на вкладке **Туннель** указать IP-адрес и порт туннельного сервера: **192.168.0.88:7777**

17.1.3.3. Настройка HTML5

На OpenUDS Tunnel:

1. В файле **/etc/guacamole/guacamole.properties** привести значение параметра **uds-base-url** к виду:

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

Например:

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

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

```
<Connector port="10443"  
protocol="org.apache.coyote.http11.Http11AprProtocol" SSLEnabled="true"  
ciphers="A-CHACHA20-POLY1305,ECDHE-RSA-CHACHA20-POLY1305,  
ECDHE-ECDSA-AES128-GCM-SHA256,ECDHE-RSA-AES128-GCM-SHA256,  
ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AES256-GCM-SHA384,  
DHE-RSA-AES128-GCM-SHA256,DHE-RSA-AES256-GCM-SHA384,  
ECDHE-ECDSA-AES128-SHA256,ECDHE-RSA-AES128-SHA256,  
ECDHE-ECDSA-AES128-SHA,ECDHE-RSA-AES256-SHA384,  
ECDHE-RSA-AES128-SHA,ECDHE-ECDSA-AES256-SHA384,  
ECDHE-ECDSA-AES256-SHA,ECDHE-RSA-AES256-SHA,  
DHE-RSA-AES128-SHA256,DHE-RSA-AES128-SHA,  
DHE-RSA-AES256-SHA256,DHE-RSA-AES256-SHA,  
ECDHE-ECDSA-DES-CBC3-SHA,ECDHE-RSA-DES-CBC3-SHA,  
EDH-RSA-DES-CBC3-SHA,AES128-GCM-SHA256,AES256-GCM-SHA384,
```



```
AES128-SHA256,AES256-SHA256,AES128-SHA,AES256-SHA,DES-CBC3-SHA"
    maxThreads="500" scheme="https" secure="true"
    SSLCertificateFile="/etc/openuds-tunnel/ssl/certs/openuds-
tunnel.pem"
    SSLCertificateKeyFile="/etc/openuds-tunnel/ssl/private/
openuds-tunnel.key"
    maxKeepAliveRequests="1000"
    clientAuth="false" sslProtocol="TLSv1+TLSv1.1+TLSv1.2" />
```

3. Запустить сервисы `guacd` и `tomcat`:

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

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

» **http://192.168.0.88:8080** — для подключения по http;

» **https://192.168.0.88:10443** — для подключения по https.

17.2. Обновление OpenUDS

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

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

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

2. Выполнить миграцию базы данных:

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

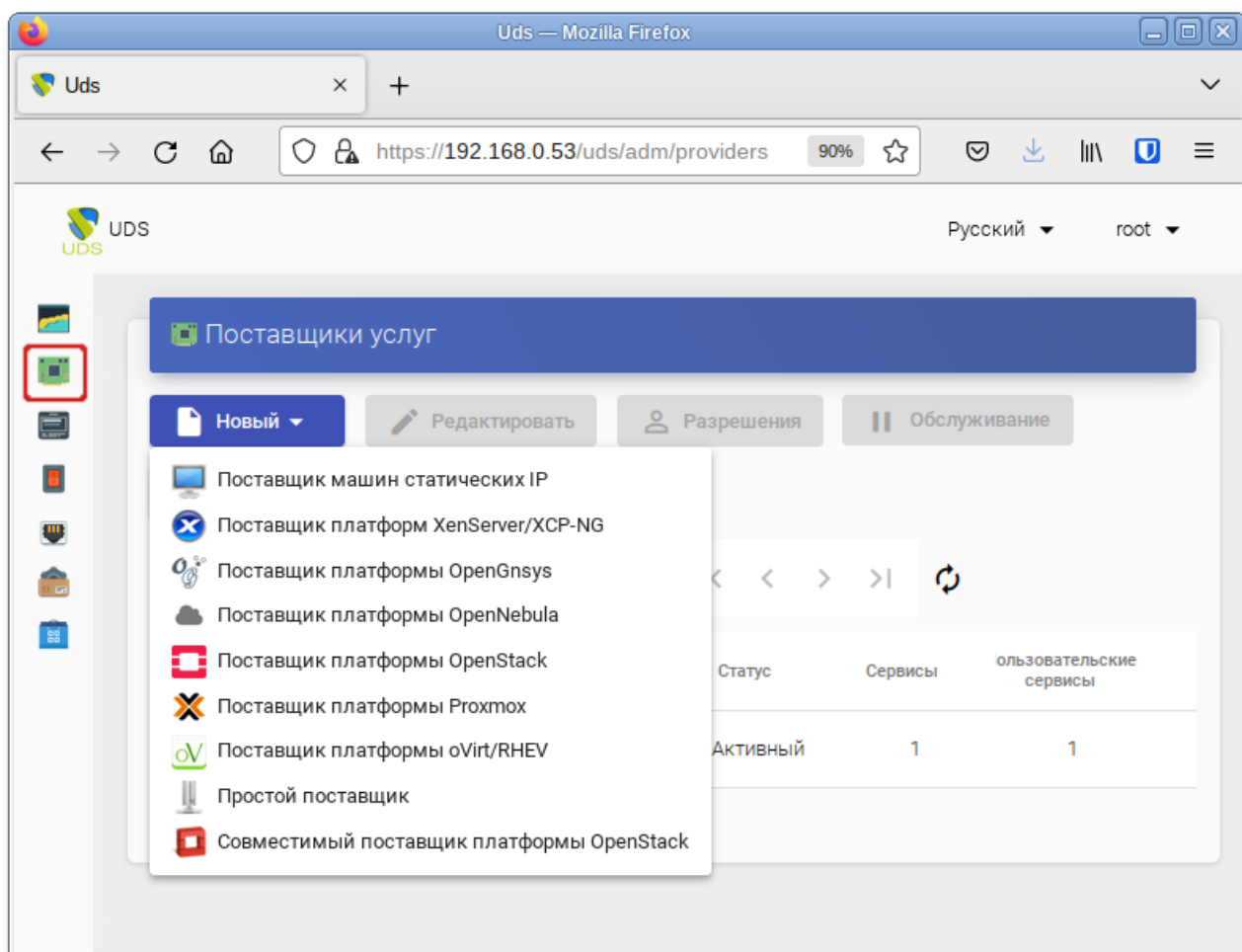
3. Перезагрузить систему, так как при обновлении не создаётся файл `/run/openuds/socket`.

17.3. Настройка OpenUDS

17.3.1. Поставщики услуг

В разделе **Поставщики услуг** подключить один из поставщиков («Service providers»):

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



17.3.1.1. OpenNebula

Минимальные параметры для настройки **Поставщик платформы OpenNebula**:

- Вкладка **Основной**: название, IP-адрес сервера OpenNebula (поле **Хост**), порт подключения, имя пользователя (с правами администратора) и пароль.

Новый поставщик

Основной

Расширенный

Тэги

Тэги этого элемента

Имя *

OpenNebula

Комментарии

Комментарии этого элемента

Хост *

192.168.0.185

Порт *

2633

Использовать SSL

☐ Нет

Имя пользователя *

oneadmin

Пароль *

••••••••

Проверить

Отменить и закрыть

Сохранить

- » Вкладка **Расширенный**: максимальное количество одновременно создаваемых ВМ, максимальное количество одновременно удаляемых ВМ, таймаут подключения к OpenNebula в секундах.

Новый поставщик

Основной
Расширенный

Одновременное создание *

10

Одновременное удаление *

5

Таймаут *

10

Проверить
Отменить и закрыть
Сохранить

Используя кнопку **Проверить**, можно убедиться, что соединение установлено правильно.

После интеграции платформы OpenNebula в OpenUDS необходимо создать базовую службу типа **Действующие образы OpenNebula**. Для этого дважды щелкнуть мышью по строке созданного поставщика услуг или в контекстном меню поставщика выбрать пункт **Подробность**:

Имя ↑	Тип	Комментарии	Статус	Сервисы	Пользовательские сервисы
<input checked="" type="checkbox"/> OpenNebula	Поставщик платформы OpenNebula		Активный	0	0
<input type="checkbox"/> StaticIP	Поставщик машин статических IP			1	1

Копировать
Подробность
Редактировать
Разрешения
Обслуживание
Удалить

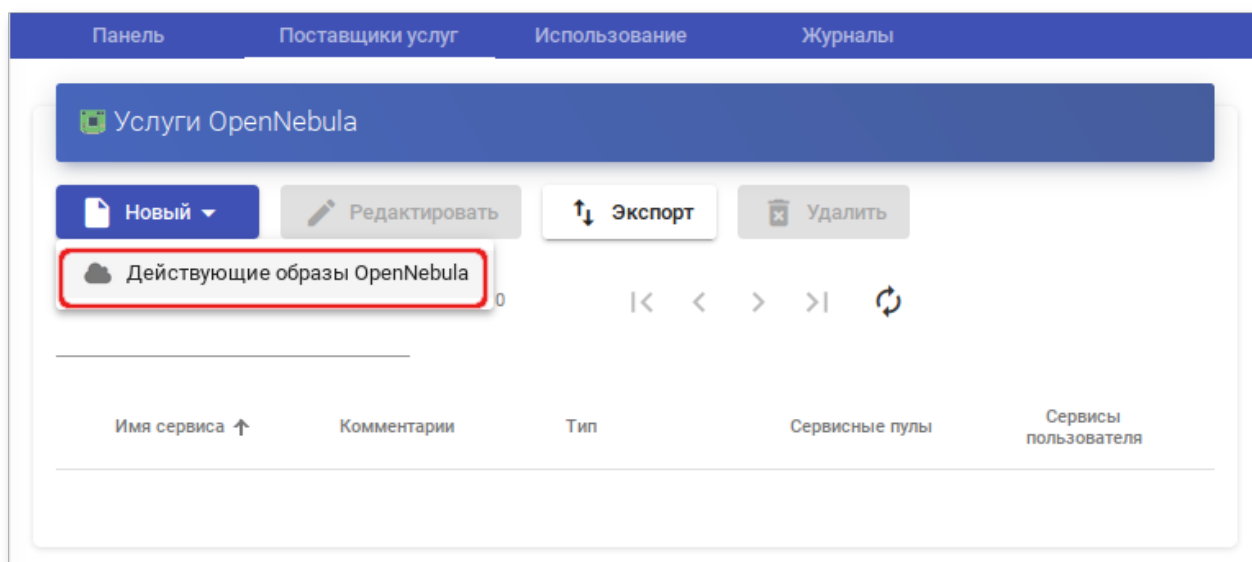
1 Выбранные предметы



Примечание

Выбрав пункт **Обслуживание**, можно приостановить все операции, выполняемые сервером OpenUDS для данного поставщика услуг. Поставщик услуг рекомендуется переводить в режим обслуживания в случаях, когда связь с этим поставщиком была потеряна или запланирован перерыв в обслуживании.

В открывшемся окне, на вкладке **Поставщики услуг** нажать кнопку **Новый** → **Действующие образы OpenNebula**:



Заполнить минимальные параметры конфигурации:

» Вкладка **Основной**:

- **Имя** — название службы;
- **Хранилище** — место, где будут храниться сгенерированные виртуальные рабочие столы.

» Вкладка **Машина**:

- **Базовый шаблон** — шаблон VM, используемый системой OpenUDS для развёртывания виртуальных рабочих столов (см. [Подготовка шаблона виртуальной машины](#));
- **Имена машин** — базовое название для клонов с этой машины (например, Desk-work-);

- **Длина имени** — количество цифр счетчика, прикрепленного к базовому имени рабочих столов (например, если **Длина имени** = 3, названия сгенерированных рабочих столов будут: Desk-work-000, Desk-work-001 ... Desk-work-999).

Новый сервис

Основной

Машина

Базовый шаблон *

ALT Workstation

Имена машин *

Desk-work-

Длина имени *

3

Отменить и закрыть

Сохранить

17.3.1.2. PVE

Минимальные параметры для настройки **Поставщик платформы Proxmox**:

- Вкладка **Основной**: название, IP-адрес/имя сервера или кластера PVE (поле **Хост**), порт подключения, имя пользователя с достаточными привилегиями в PVE (в формате пользователь@аутентификатор) и пароль.

Новый поставщик

Основной

Расширенный

Тэги

Тэги этого элемента

Имя *

PVE

Комментарии

Комментарии этого элемента

Хост *

192.168.0.186

Порт *

8006

Имя пользователя *

root@pam

Пароль *

.....



Проверить

Отменить и закрыть

Сохранить

» Вкладка **Расширенный**: максимальное количество одновременно создаваемых VM, максимальное количество одновременно удаляемых VM, таймаут подключения к Proxmox в секундах, идентификатор VM, с которым OpenUDS начнет генерировать VM на Proxmox (≥ 10000).

Новый поставщик

Основной
Расширенный

Одновременное создание *

10

Одновременное удаление *

5

Таймаут *

20

Запуск Vmld *

10000

Проверить
Отменить и закрыть
Сохранить

Используя кнопку **Проверить**, можно убедиться, что соединение установлено правильно.

После интеграции платформы PVE в OpenUDS необходимо создать базовую службу типа **Связанный клон Proxmox**. Для этого дважды щелкнуть мышью по строке созданного поставщика услуг или в контекстном меню поставщика выбрать пункт **Подробнее**:

Имя ↑	Тип	Комментарии	Статус	Сервисы	Пользовательские сервисы
<input type="checkbox"/> OpenNebula	Поставщик платформы OpenNebula		На техобслуживании	0	0
<input checked="" type="checkbox"/> PVE	Поставщик платформы Proxmox		Активный	0	0
<input type="checkbox"/> StaticIP	Поставщик машин статических IP			3	1

Копировать
Подробнее
Редактировать
Разрешения
Обслуживание
Удалить

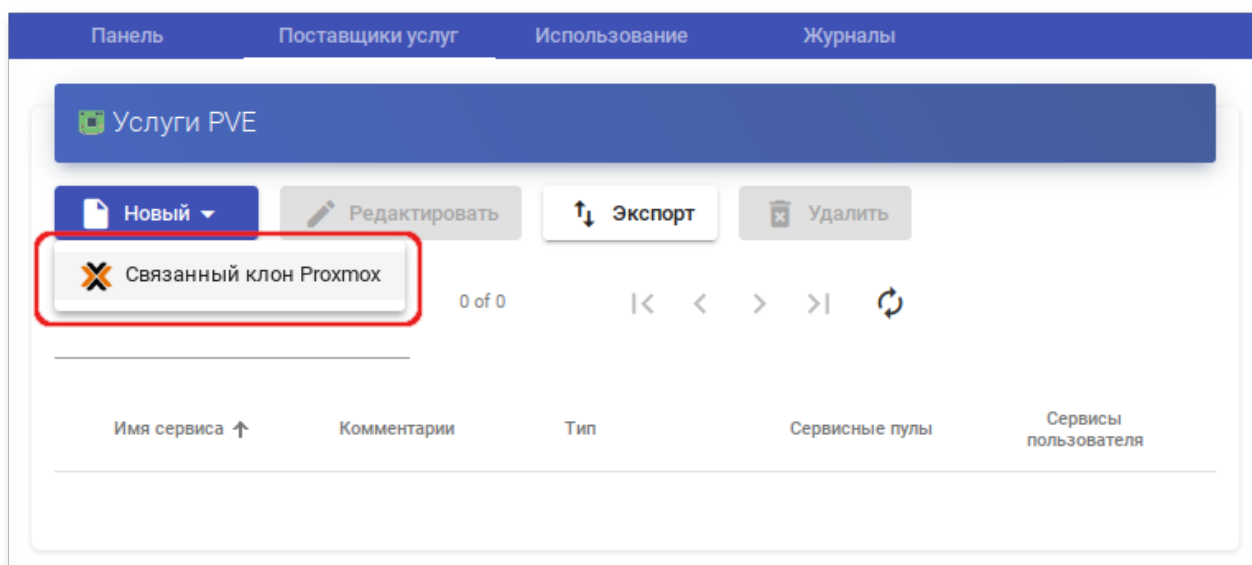
1 Выбранные предметы



Примечание

Выбрав пункт **Обслуживание**, можно приостановить все операции, выполняемые сервером OpenUDS для данного поставщика услуг. Поставщик услуг рекомендуется переводить в режим обслуживания в случаях, когда связь с этим поставщиком была потеряна или запланирован перерыв в обслуживании.

В открывшемся окне, на вкладке **Поставщики услуг** нажать кнопку **Новый** → **Связанный клон Proxmox**:



Заполнить минимальные параметры конфигурации:

■ Вкладка **Основной**:

- **Имя** — название службы;
- **Пул** — пул, в котором будут находиться VM, созданные OpenUDS;
- **Высокая доступность** — включать созданные VM в группу HA PVE;
- **Сначала попробовать SOFT Shutdown** — если активно, OpenUDS попытается, перед уничтожением автоматически сгенерированного виртуального рабочего стола, выполнить контролируемое отключение машины.

Новый сервис

Основной

Машина

Тэги

Тэги этого элемента

Имя *

Simply

Комментарии

Комментарии этого элемента

Пул

None

Высокая доступность

Disabled

Сначала попробуйте SOFT Shutdown

Нет

Отменить и закрыть

Сохранить

Вкладка **Машина**:

- **Базовая машина** — шаблон VM, используемый системой OpenUDS для развёртывания виртуальных рабочих столов (см. [Подготовка шаблона виртуальной машины](#));
- **Хранилище** — место, где будут храниться сгенерированные виртуальные рабочие столы (поддерживаются хранилища, позволяющие создавать «Снимки»);
- **Имена машин** — базовое название для клонов с этой машины (например, Desk-SL-);
- **Длина имени** — количество цифр счетчика, прикрепленного к базовому имени рабочих столов (например, если **Длина имени** = 3, названия сгенерированных рабочих столов будут: Desk-SL-000, Desk-SL-001 ... Desk-SL-999).

Новый сервис

Основной

Машина

Базовая машина *

pve01\SL (107) ▾

Хранилище *

nfs-storage (622.91 GB/36.90 GB)общий ▾

Имена машин *

Desk-SL

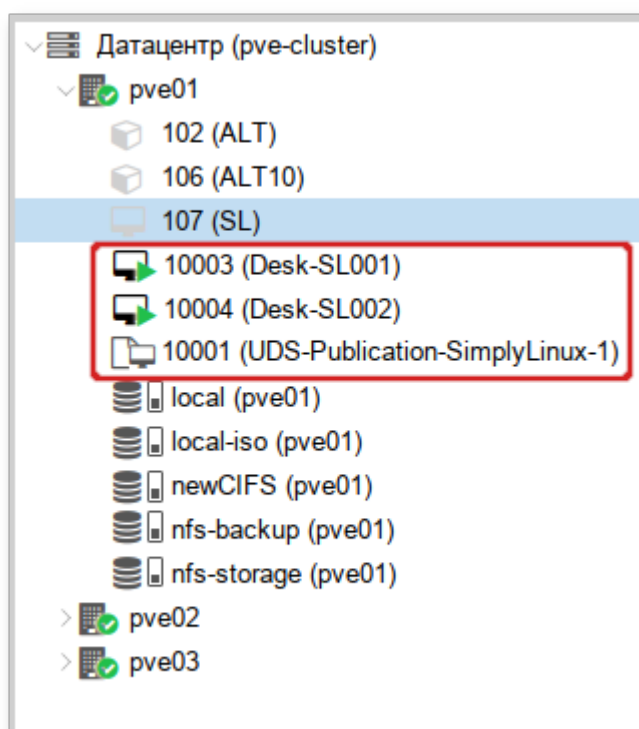
Длина имени *

3

Отменить и закрыть

Сохранить

После того как среда OpenUDS будет настроена и будет создан первый «пул услуг», в среде PVE можно будет наблюдать, как разворачиваются рабочие столы. Сначала будет создан шаблон («UDS-Publication-pool_name-publishing-number») — клон VM, выбранной при регистрации службы. После завершения процесса создания клона будут созданы рабочие столы («Machine_Name-Name_Length»):



17.3.1.3. 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:

Новый поставщик

Тэги

Тэги этого элемента

Имя *

StaticIP

Комментарии

Комментарии этого элемента

ПроверитьОтменить и закрытьСохранить

Для создания базовых услуг **Поставщика машин статических IP** следует дважды щелкнуть мышью по строке созданного поставщика или в контекстном меню поставщика выбрать пункт **Подробность**:

Имя ↑	Тип	Комментарии	Статус	Сервисы	Пользовательские сервисы
<input type="checkbox"/> OpenNebula	Поставщик платформы OpenNebula		На техобслуживании	0	0
<input type="checkbox"/> PVE	Поставщик платформы Proxmox		Активный	0	0
<input checked="" type="checkbox"/> StaticIP	Поставщик машин статических IP		Активный	3	1

Копировать

Подробность

Редактировать

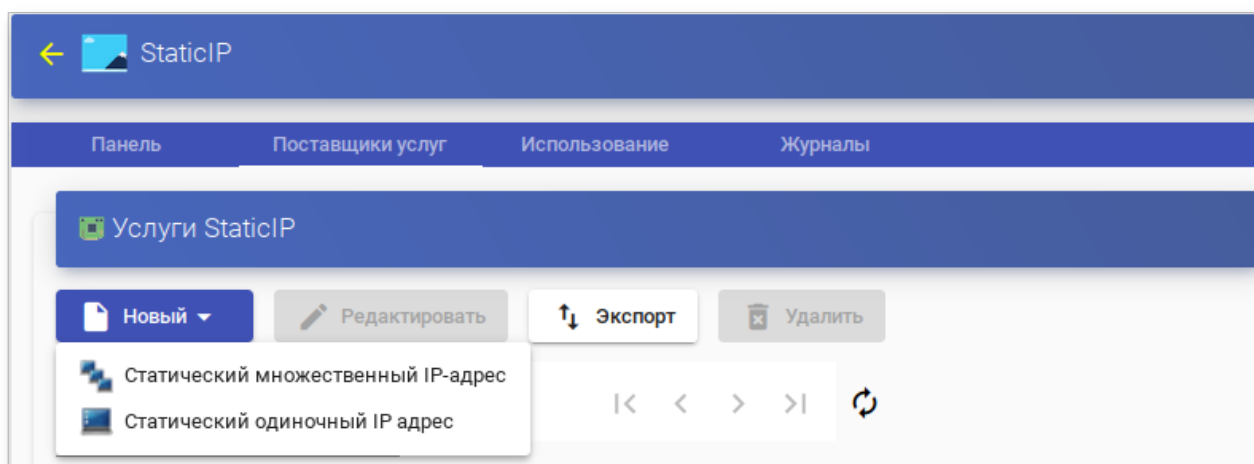
Разрешения

Обслуживание

Удалить

1 Выбранные предметы

В открывшемся окне, на вкладке **Поставщики услуг** нажать кнопку **Новый** → **Статический множественный IP-адрес** или **Новый** → **Статический одиночный IP-адрес**:



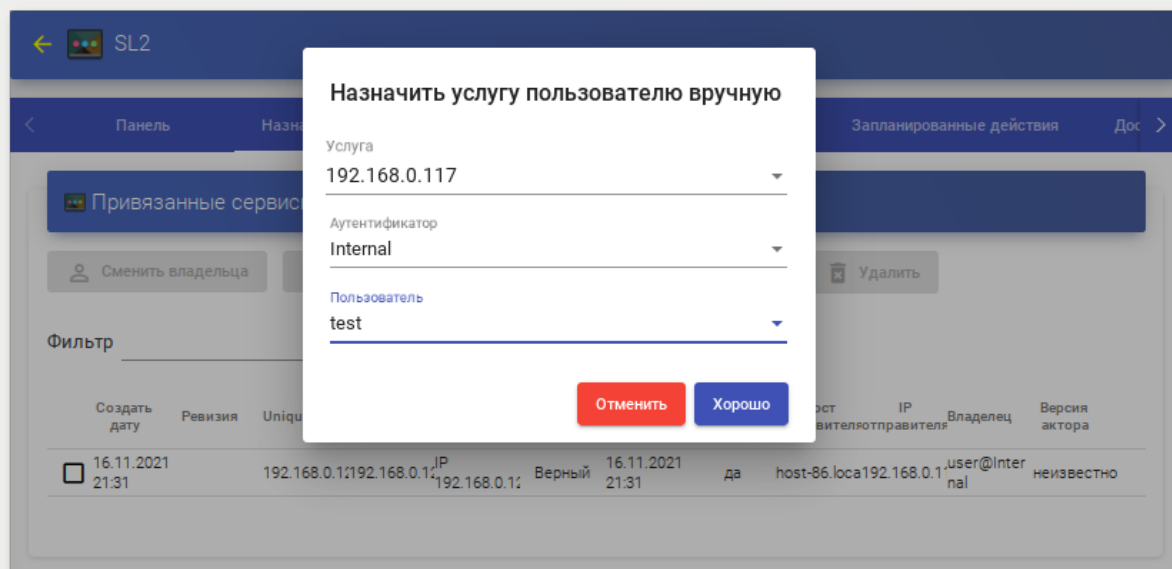
Статический множественный IP-адрес

Используется для подключения одного пользователя к одному компьютеру. Поддерживается неограниченное количество IP-адресов (можно включить в список все устройства, которые должны быть доступны удалённо). По умолчанию система будет предоставлять доступ к устройствам в порядке очереди (первый пользователь получивший доступ к этому пулу, получает доступ к машине с первым IP-адресом из списка). Также можно настроить выборочное распределение, чтобы определённому пользователю назначался определенный компьютер (IP-адрес).



Примечание

Для настройки привязки конкретного пользователя к конкретному IP необходимо в разделе **Пулы услуг** (см. раздел [Пулы услуг](#)) для созданной услуги на вкладке **Назначенные 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** — название службы;
- **Список серверов** — один или несколько IP-адресов машин, к которым будет осуществляться доступ (машины должны быть включены и настроены см. [Подготовка шаблона виртуальной машины](#));
- **Ключ услуги** — токен, который будет использоваться клиентами для связи с сервисом. Если в этом поле не указан токен (пусто), система не будет контролировать сеансы пользователей на компьютерах. Таким образом, когда компьютер назначается пользователю, это назначение будет сохраняться до тех пор, пока администратор не удалит его вручную. При наличии токена сеансы пользователей будут контролироваться (при выходе из сеанса, компьютеры снова становятся доступными для доступа других пользователей). Если токен указан, необходимо, чтобы на компьютерах (IP-адрес, которых указан в поле **Список серверов**) был установлен Unmanaged UDS Actor.

Новый сервис

Основной

Расширенный

Тэги

Тэги этого элемента

Имя *

Students

Комментарии

Комментарии этого элемента

Список серверов

192.168.0.102, 192.168.0.117, 192.168.0.103

Ключ услуги

Ключ услуги, который будет использоваться клиентами для связи с сервис

Отменить и закрыть

Сохранить

» Вкладка **Расширенный**:

- **Проверьте порт** — порт, по которому система может проверить, доступен ли компьютер. Если компьютер не доступен, система автоматически предоставит следующее устройство в списке. 0 — не проверять доступность компьютера;
- **Пропустить время** — период, в течение которого не будет проверяться доступность недоступной машины;

- **Максимальное количество сеансов на машину** — максимальная продолжительность сеанса (в часах), прежде чем OpenUDS решит, что эта машина заблокирована и освободит её (0 означает «никогда»).

Новый сервис

Основной
Расширенный

Проверьте порт *

22

Пропустить время *

15

Максимальное количество сеансов на машину *

0

Заблокируйте машину внешним доступом

☐ Нет

Отменить и закрыть

Сохранить



Примечание

Назначение IP-адресов будет осуществляться в порядке доступа, то есть первому пользователю, который обращается к службе, будет назначен первый IP-адрес в списке. IP-адрес будет привязан пользователю, даже после выхода пользователя из системы (пока администратор не удалит привязку вручную).

Просмотреть/изменить привязанные сеансы можно в разделе **Пулы услуг** (см. раздел [Пулы услуг](#)) на вкладке **Назначенные сервисы**:

Панель

Назначенные сервисы

Группы

Транспорты

Запланированные действия

Доступ к календарям

Диаграммы

Привязанные сервисы

Сменить владельца

Журналы

Экспорт

Удалить

Фильтр

1 – 2 of 2

<<

<

>

>>

↺

Создать дату	Ревизия	Unique ID	IP	Дружественное имя	Статус	Статус даты	В работе	Хост отправителя	IP отправителя	Владелец	Версия актора
<input type="checkbox"/> 18.10.2022 12:41		192.168.0.102	192.168.0.102	192.168.0.102	Верный	18.10.2022 12:41	да	192.168.0.122	192.168.0.122	user@Internal	неизвестно
<input type="checkbox"/> 18.10.2022 12:41		192.168.0.117	192.168.0.117	192.168.0.117	Верный	18.10.2022 12:41	да	192.168.0.100	192.168.0.100	test@Internal	неизвестно

Параметры конфигурации для услуги **Статический одиночный IP-адрес**:

- **Имя** — название службы;

» **IP-адрес машины** — IP-адрес машины, к которой будет осуществляться доступ (машина должна быть включена и настроена см. [Подготовка шаблона виртуальной машины](#)).

Новый сервис

Тэги

Тэги этого элемента

Имя *

EDU

Комментарии

Комментарии этого элемента

IP адрес машины *

192.168.0.123

Отменить и закрыть

Сохранить

17.3.2. Настройка аутентификации пользователей

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

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



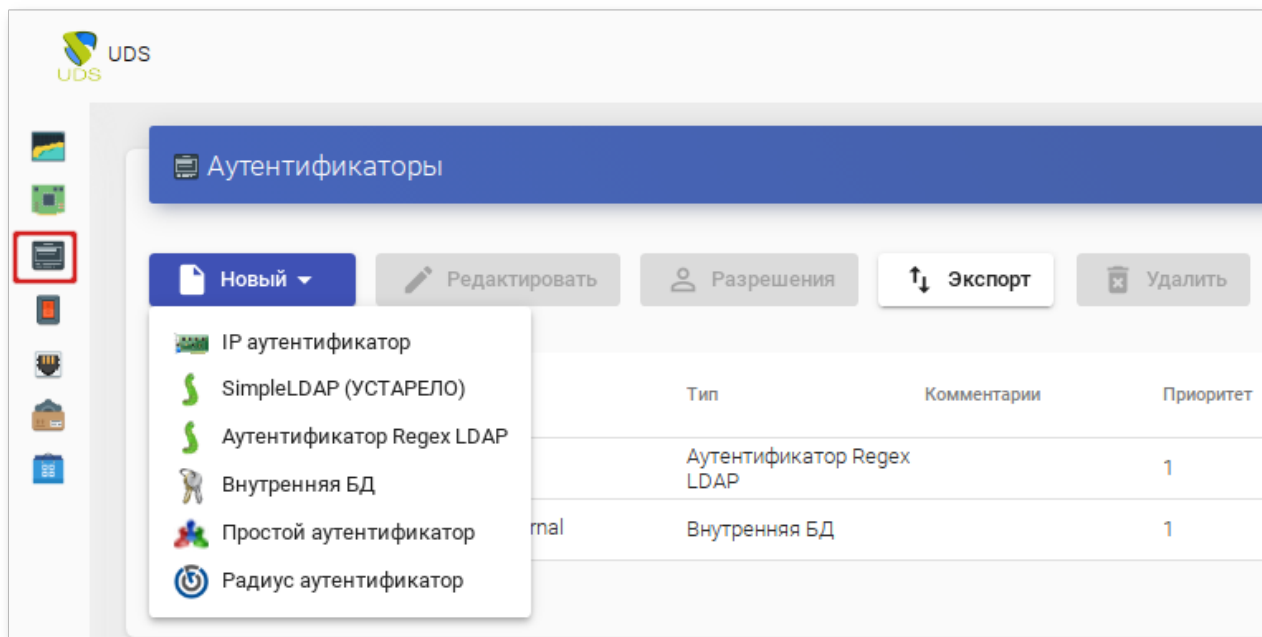
Примечание

Если в системе зарегистрировано более одного аутентификатора, и они не отключены, на экран входа будет добавлено поле **Аутентификатор** с раскрывающимся списком. В этом списке можно выбрать аутентификатор, который система будет использовать для проверки пользователя:

The screenshot shows a login interface with three input fields: 'Имя пользователя *' (Username), 'пароль' (Password), and 'Аутентификатор' (Authenticator). The 'Аутентификатор' field is a dropdown menu currently showing 'Internal'. A red rectangular box highlights the 'Аутентификатор' field. Below the fields is a button labeled 'Авторизоваться' (Authorize).

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

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



17.3.2.1. Внутренняя БД

При аутентификации **Внутренняя БД** данные пользователей и групп хранятся в базе данных, к которой подключен сервер OpenUDS.

Для создания аутентификации типа **Внутренняя БД** в разделе **Аутентификаторы** следует нажать кнопку: **Новый** → **Внутренняя БД**.

Минимальные параметры конфигурации (вкладка **Основной**): имя аутентификатора, приоритет и метка.

Новый Аутентификатор

Основной

Расширенный

Экран/Дисплей

Тэги

Тэги этого элемента

Имя *

Internal

Комментарии

Комментарии этого элемента

Приоритет *

1

Метка *

login

Проверить

Отменить и закрыть

Сохранить

После того как аутентификатор типа **Внутренняя БД** создан, нужно зарегистрировать пользователей и группы пользователей. Для этого следует выбрать созданный аутентификатор, затем во вкладке **Группы** создать группы пользователей, во вкладке **Пользователи** создать пользователей.

← Internal

Панель

Пользователей

Группы

Журналы

Текущие пользователи

Новый

Редактировать

Экспорт

Удалить

Фильтр

1 – 2 of 2

|<

<

>

>|

↻

Имя пользователя ↑	Роль	Имя	Комментарии	состояние	Последний вход
<input type="checkbox"/> test	Администратор			Активный	01.07.1972 02:00
<input type="checkbox"/> user	Пользователь	user		Активный	20.12.2022 11:38

17.3.2.2. Аутентификатор Regex LDAP

Этот аутентификатор позволяет пользователям и группам пользователей, принадлежащих практически любому аутентификатору на основе LDAP, получать доступ к виртуальным рабочим столам и приложениям.



Важно

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

17.3.2.2.1. 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):

Новый Аутентификатор

< Основной **Учётные данные** LDAP информация Расширенный >

Тэги

Тэги этого элемента

Имя *

freeipa

Комментарии

Комментарии этого элемента

Приоритет *

2

Метка *

freeipa

Хост *

192.168.0.113

Порт *

389

Использовать SSL

☐ Нет

Таймаут *

10

Проверить

Отменить и закрыть

Сохранить

Вкладка **Учётные данные**: имя пользователя (в формате uid=user_freeipa,cn=users,cn=accounts,dc=example,dc=test) и пароль:


Новый Аутентификатор

< Основной **Учётные данные** LDAP информация Расширенный >

Пользователь *

uid=ivanov,cn=users,cn=accounts,dc=freeipa,dc=test

Пароль *

..... 

Проверить

Отменить и закрыть

Сохранить

Вкладка **LDAP информация**: общая база пользователей, класс пользователей LDAP, идентификатор атрибута пользователя, атрибут имени пользователя, атрибут имени группы:

Новый Аутентификатор

< Основной Учётные данные LDAP информация Расширенный >

База *

cn=accounts,dc=freeipa,dc=test

Класс пользователя *

posixAccount

Идентификатор атрибута пользователя *

uid

Атрибут имени пользователя *

cn

Атрибуты имени группы *

memberOf

ПроверитьОтменить и закрытьСохранить



Примечание

Используя кнопку **Проверить**, можно проверить соединение с FreeIPA-сервером.

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 (для FreeIPA по умолчанию это группа cn=ipausers,cn=groups,cn=accounts,dc=ipa,dc=example,dc=test), можно также указать разрешённые пулы:

Новая группа

Группа

cn=ipausers,cn=groups,cn=accounts,dc=example,dc=test

Комментарии

Состояние

Включено

Пулы услуг

Отменить

Хорошо

17.3.2.2.2. 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):

Новый Аутентификатор

<

Основной

Учётные данныеLDAP информацияРасширенный>

Тэги
Тэги этого элемента

Имя *
AD

Комментарии
Комментарии этого элемента

Приоритет *
1

Метка *
AD

Хост *
192.168.0.122

Порт *
636

Использовать SSL
☒ Да

Таймаут *
10

Проверить

Отменить и закрыть

Сохранить

Вкладка **Учётные данные**: имя пользователя (можно указать в виде имя@домен) и пароль:

Новый Аутентификатор

<

Основной

Учётные данные

LDAP информацияРасширенный>

Пользователь *
administrator_openuds@test.alt

Пароль *
.....

👁

Проверить

Отменить и закрыть

Сохранить

Вкладка **LDAP информация**: общая база пользователей, класс пользователей LDAP, идентификатор атрибута пользователя, атрибут имени пользователя, атрибут имени группы:

Новый Аутентификатор

< Основной Учётные данные **LDAP информация** Расширенный >

База *
cn=Users,dc=test,dc=alt

Класс пользователя *
person

Идентификатор атрибута пользователя *
sAMAccountName

Атрибут имени пользователя *
cn

Атрибуты имени группы *
memberOf

ПроверитьОтменить и закрытьСохранить



Примечание

Используя кнопку **Проверить**, можно проверить соединение с Active Directory.

3. Добавить группу LDAP, в которую входят пользователи. Для этого следует выбрать созданный аутентификатор, затем в открывшемся окне на вкладке **Группы** нажать **Новый** → **Группа**.

Заполнить dn существующей группы (например, cn=UDS,cn=Users,dc=test,dc=alt), можно также указать разрешённые пулы:

Новая группа

Группа

cn=UDS,cn=Users,dc=test,dc=alt

Комментарии

Состояние

Включено

Пулы услуг

Отменить

Хорошо

17.3.2.3. IP аутентификатор

Этот тип аутентификации обеспечивает доступ клиентов к рабочим столам и виртуальным приложениям по IP-адресу.

Для создания аутентификации типа **IP аутентификатор** в разделе **Аутентификаторы** следует нажать кнопку: **Новый** → **IP аутентификатор**.

Минимальные параметры конфигурации (вкладка **Основной**): имя аутентификатора, приоритет и метка.

Новый Аутентификатор

Основной

Экран/Дисплей

Тэги

Тэги этого элемента

Имя *

IP

Комментарии

Комментарии этого элемента

Приоритет *

3

Метка *

ip

Проверить

Отменить и закрыть

Сохранить

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):

Новая группа

Диапазон IP адресов

192.168.0.33,192.168.0.110

Комментарии

Состояние

Включено

Пулы услуг

Отменить

Хорошо

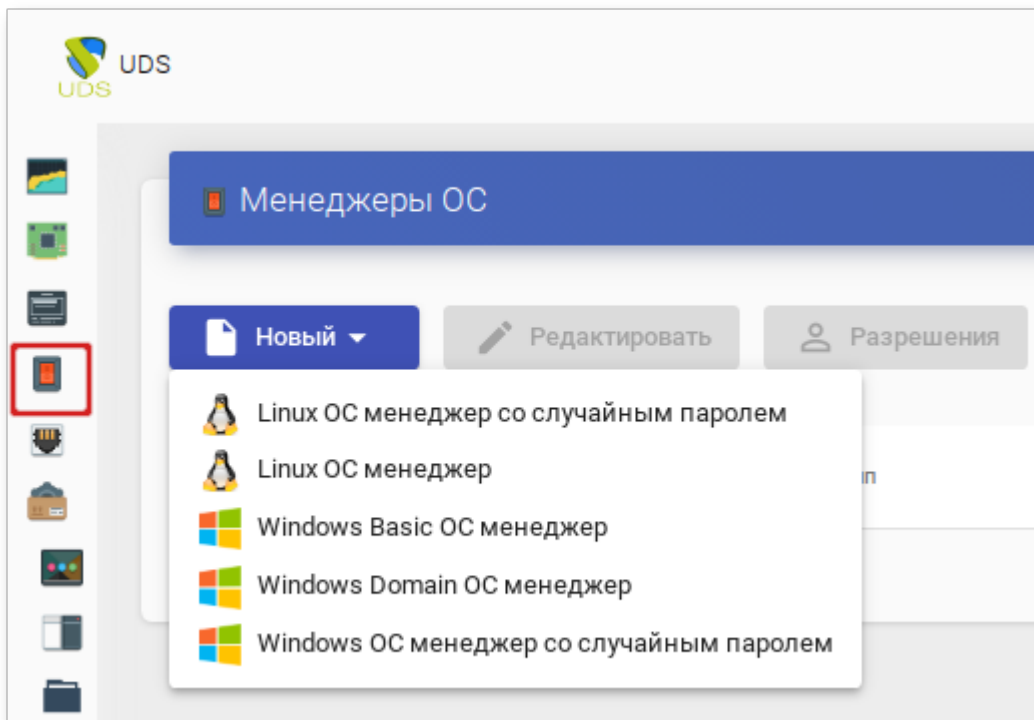
17.3.3. Настройка менеджера ОС

OpenUDS Actor, размещенный на виртуальном рабочем столе, отвечает за взаимодействие между ОС и OpenUDS Server на основе конфигурации или выбранного типа Менеджера ОС.



Примечание

Для каждой службы, развернутой в OpenUDS, потребуется **Менеджер ОС**, за исключением случаев, когда используется **Поставщик машин статических IP**.



Менеджер ОС запускает ранее настроенные службы:

- **Linux ОС менеджер** используется для виртуальных рабочих столов на базе Linux. Он выполняет задачи переименования и управления сеансами виртуальных рабочих столов;
- **Windows Basic ОС менеджер** используется для виртуальных рабочих столов на базе Windows, которые не являются частью домена AD;
- **Windows Domain ОС менеджер** используется для виртуальных рабочих столов на базе Windows, которые являются членами домена AD.

Минимальные настройки для **Linux ОС менеджер** и **Windows Basic ОС менеджер**:

- вкладка **Основной**:
 - **Имя** — название;

- **Действие при выходе из системы** — действие, которое OpenUDS будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя. **Держать сервис привязанным** — постоянный пул, при выходе пользователя (выключении ВМ), ВМ запускается заново, при повторном входе пользователю будет назначен тот же рабочий стол. **Удалить сервис** — непостоянный пул, при выходе пользователя из системы, ВМ удаляется и создается заново. **Держать сервис привязанным даже в новой публикации** — сохранение назначенной службы даже при создании новой публикации;
- **Максимальное время простоя** — время простоя виртуального рабочего стола (в секундах). По истечении этого времени OpenUDS Actor автоматически закроет сеанс. Отрицательные значения и значения менее 300 секунд отключают эту опцию.

Новый менеджер ОС

Основной
Расширенный

Тэги

Тэги этого элемента

Имя *

Linux non-persistent

Комментарии

Комментарии этого элемента

Действие при выходе из системы

Удалить сервис

Максимальное время простоя *

3600

Отменить и закрыть

Сохранить

» вкладка **Расширенный**:

- **Выход из календаря** — если этот параметр установлен, OpenUDS попытается завершить сессию пользователя, когда для текущего соединения истечет время доступа (если параметр не установлен, пользователю будет разрешено продолжить работу).

Минимальные настройки для **Windows Domain ОС менеджер**:

» вкладка **Основной**:

- **Имя** — название;
- **Домен** — домен, к которому будут присоединены виртуальные рабочие столы. Необходимо использовать формат FQDN (например, test.alt);
- **Аккаунт** — пользователь с правами на добавление машин в домен;
- **Пароль** — пароль пользователя указанного в поле **Аккаунт**;

■ **OU** — организационная единица, в которую будут добавлены виртуальные хосты (если не указано, хосты будут зарегистрированы в подразделении по умолчанию — Computers).
Формат поддерживаемых OU: **OU = name_OU_last_level, ... OU = name_OU_first_level, DC = name_domain, DC = extension_domain**. Во избежание ошибок, рекомендуется сверяться с полем **distinguishedName** в свойствах атрибута OU;

■ **Действие при выходе из системы** — действие, которое OpenUDS будет выполнять на виртуальном рабочем столе при закрытии сеанса пользователя. **Держать сервис привязанным (Keep service assigned)** — постоянный пул, при выходе пользователя (выключении VM), VM запускается заново, при повторном входе пользователю будет назначен тот же рабочий стол. **Удалить сервис (Remove service)** — непостоянный пул, при выходе пользователя из системы, VM удаляется и создается заново. **Держать сервис привязанным даже в новой публикации (Keep service assigned even on new publication)** — сохранение назначенной службы даже при создании новой публикации;

■ **Максимальное время простоя** — время простоя виртуального рабочего стола (в секундах). По истечении этого времени OpenUDS Actor автоматически закрывает сеанс. Отрицательные значения и значения менее 300 секунд отключают эту опцию.

Новый менеджер ОС

Основной

Расширенный

Тэги

Тэги этого элемента

Имя *

Windows domain

Комментарии

Комментарии этого элемента

Домен *

test.alt

Аккаунт *

Administrator

Пароль *

.....

OU

ou=OU,dc=test,dc=alt

Действие при выходе из системы

Держать сервис привязанным

Максимальное время простоя *

-1

Отменить и закрыть

Сохранить

» вкладка **Расширенный**:

- **Группа машин** — указывает, к какой группе машин AD будут добавлены виртуальные рабочие столы, созданные UDS;
- **Убрать машину** — если этот параметр установлен, OpenUDS удалит запись о виртуальном рабочем столе в указанном подразделении после удаления рабочего стола (необходимо, чтобы пользователь, указанный в поле **Аккаунт**, имел права на выполнение данного действия в OU);
- **Предпочтения серверов** — если серверов AD несколько, можно указать, какой из них использовать предпочтительнее;
- **Использовать SSL** — если этот параметр установлен, будет использоваться SSL-соединение;
- **Выход из календаря** — если этот параметр установлен, OpenUDS попытается завершить сессию пользователя, когда для текущего соединения истечет время доступа (если параметр не установлен, пользователю будет разрешено продолжить работу).

Новый менеджер ОС

Основной **Расширенный**

Группа машин
Группа, в которую добавляются машины при создании. Если пусто, никакая группа использова

Убрать машину
☒ Да

Предпочтения серверов
В случае нескольких серверов AD, какой из них предпочтительнее

Использовать SSL
☒ Да

Выход из календаря
☒ Да

17.3.4. Транспорт

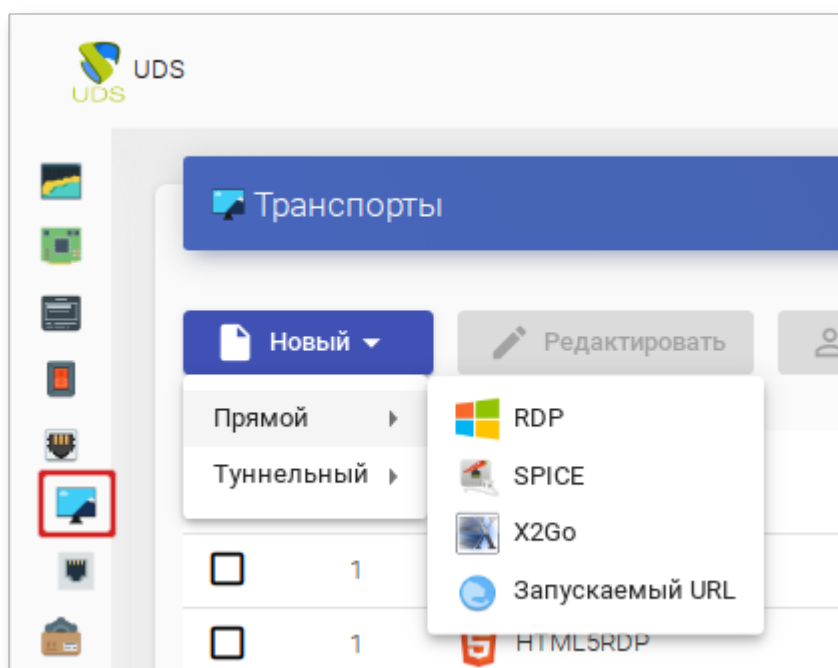
Для подключения к виртуальным рабочим столам необходимо создать транспорт. Транспорт — это приложение, которое выполняется на клиенте и отвечает за предоставление доступа к реализованной службе.

Можно создать один транспорт для различных «пулов» или установить по одному транспорту для каждого «пула».

При создании транспорта необходимо выбрать его тип:

- **Прямой** — используется, если пользователь имеет доступ к виртуальным рабочим столам из внутренней сети (например, LAN, VPN и т.д.);

» **Туннельный** — используется, если у пользователя нет прямого подключения к рабочему столу.



17.3.4.1. RDP (прямой)

Данный транспорт 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**:

- **Имя** — название транспорта;
- **Приоритет** — приоритет, чем меньше значение приоритета, тем выше данный транспорт будет указан в списке доступных транспортных средств для сервиса. Транспорт с самым низким приоритетом, будет транспортом по умолчанию;
- **Сетевой доступ** — разрешает или запрещает доступ пользователей к службе, в зависимости от сети из которой осуществляется доступ;
- **Сети** — сетевые диапазоны, подсети или IP-адреса (настраиваются в разделе **Сети**). Пустое поле означает «все сети». Используется вместе с параметром **Сетевой доступ**;
- **Разрешенные устройства** — разрешает доступ к службе только с выбранных устройств. Пустое поле означает «все устройства»;
- **Сервис-пулы** — позволяет назначить транспорт одному или нескольким ранее созданным пулам услуг. Можно оставить это поле пустым и выбрать способы подключения при создании пула услуг.

Новый транспорт

<

Основной

Учётные данные

Параметры

Экран/Дисплей

>

Тэги

Тэги этого элемента

Имя *

RDP

Комментарии

Комментарии этого элемента

Приоритет *

1

Сетевой доступ

☒

 Да

Сети

Сети, ассоциированные с транспортом. Если сети не выбраны, это означает все сети

Разрешённые устройства

Linux, Windows

Сервис-пулы

SL

Отменить и закрыть

Сохранить

» Вкладка **Учетные данные**:

- **Пропустить данные аккаунта** — если установлено значение **Да**, учётные данные для доступа к виртуальному рабочему столу будут запрашиваться при подключении к серверу. Если установлено значение **Нет**, будут использоваться данные OpenUDS (см. ниже);
- **Имя пользователя** — имя пользователя, которое будет использоваться для доступа к рабочему столу (пользователь должен существовать на ВМ). Если данное поле пустое, будет использован логин авторизовавшегося в веб-интерфейсе OpenUDS пользователя;
- **Пароль** — пароль пользователя, указанного в поле **Имя пользователя**;
- **Без домена** — указывает, перенаправляется ли доменное имя вместе с пользователем. Значение **Да** равносильно пустому полю **Домен**;
- **Домен** — домен. Если поле не пустое, то учётные данные будут использоваться в виде DOMAIN\user.

Новый транспорт

< Основной **Учётные данные** Параметры Экран/Дисплей >


Пропустить данные аккаунта

☐ Нет

Имя пользователя

user

Пароль

..... 

Без домена

☐ Нет

Домен

Если это не пусто, этот домен всегда будет использоваться в качестве учетных данных (используйте)

Отменить и закрыть Сохранить

» На вкладке **Параметры** можно разрешить/запретить перенаправления дисков, принтеров и других устройств:

Новый транспорт

<

Основной

Учётные данные

Параметры

Экран/Дисплей

>

Разрешить смарткарты

Нет

Разрешить принтеры

Нет

Политика локальных дисков

Allow none

Принудительное подключение дисков

Используйте значения, разделенные запятыми, например «C:, D:». Если политика дисков запр

Разрешить серийные порты

Нет

Включить буфер обмена

Да

Включить звук

Да

Включить веб-камеру

Нет

USB redirection

Allow all

Поддержка Credssp

Да

Порт RDP *

3389

Отменить и закрыть

Сохранить

» На вкладке **Экран/Дисплей** настраиваются параметры окна рабочего стола:

Новый транспорт

<

ной

Учётные данные

Параметры

Экран/Дисплей

Linux

>

Размер экрана

Full screen

Глубина цвета

24

Обои/темы

Нет

Несколько мониторов

Нет

Разрешить композицию рабочего стола

Нет

Сглаживание шрифтов

Да

Окно подключения

Да

Отменить и закрыть

Сохранить

» Вкладка **Linux Client**:

- **Мультимедийная синхронизация** — включает параметр мультимедиа на клиенте FreeRDP;
- **Использовать Alsa** — использовать звук через Alsa;
- **Строка принтера** — принтер, используемый клиентом FreeRDP (если включено перенаправление принтера). Пример: «HP_LaserJet_M1536dnf_MFP» (названия подключенных принтеров можно вывести командой **lpstat -a**);
- **Строка Smartcard** — токен, используемый клиентом FreeRDP (если включено перенаправление смарт-карт). Пример: «Aktiv Rutoken ECP 00 00»;
- **Пользовательские параметры** — здесь можно указать любой параметр, поддерживаемый клиентом FreeRDP.

Новый транспорт

< **Личные данные** Параметры Экран/Дисплей **Linux Client** >

Мультимедийная синхронизация

☐ Нет

Использовать Alsa

☐ Нет

Строка принтера

HP_LaserJet_M1536dnf_MFP

Строка Smartcard

Если проверена смарт-карта, строка смарт-карты, используемая с клиентом freerdp

Пользовательские параметры

Если не пуст, добавочный параметр для включения клиента Linux (например, /usb: id,dev:054c:0:

Отменить и закрыть Сохранить

» Вкладка **Расширенный**:

- **Метка** — метка транспорта метапула (используется для того чтобы назначить несколько транспортных метапулу).

17.3.4.2. RDP (туннельный)

Все настройки аналогичны настройке RDP, за исключением настроек на вкладке **Туннель**.

Вкладка **Туннель**:

- **Туннельный сервер** — IP-адрес/имя OpenUDS Tunnel. Если доступ к рабочему столу осуществляется через глобальную сеть, необходимо ввести общедоступный IP-адрес сервера OpenUDS Tunnel. Формат: IP_Tunnel:Port;
- **Время ожидания туннеля** — максимальное время ожидания туннеля;
- **Принудительная проверка SSL-сертификата** — принудительная проверка сертификата туннельного сервера.

Новый транспорт

<

Основной

Туннель

Учётные данные

Параметры

>

Туннельный сервер

192.168.0.88:7777

Время ожидания туннеля *

30

Принудительная проверка SSL-сертификата

☐ Нет

Отменить и закрыть

Сохранить

17.3.4.3. X2Go (прямой)

X2Go позволяет пользователям получать доступ к виртуальным рабочим столам Linux. На клиентах подключения должен быть установлен клиент X2Go, и на виртуальных рабочих столах (сервере) должен быть установлен и включен сервер X2Go.

Параметры конфигурации для настройки транспорта X2Go:

■ Вкладка **Основной**:

- **Имя** — название транспорта;
- **Приоритет** — приоритет, чем меньше значение приоритета, тем выше данный транспорт будет указан в списке доступных транспортных для сервиса. Транспорт с самым низким приоритетом, будет транспортом по умолчанию;
- **Сетевой доступ** — разрешает или запрещает доступ пользователей к службе, в зависимости от сети из которой осуществляется доступ;
- **Сети** — сетевые диапазоны, подсети или IP-адреса (настраиваются в разделе **Сети**). Пустое поле означает «все сети». Используется вместе с параметром **Сетевой доступ**;
- **Разрешенные устройства** — разрешает доступ к службе только с выбранных устройств. Пустое поле означает «все устройства»;
- **Сервис-пулы** — позволяет назначить транспорт одному или нескольким ранее созданным пулам услуг. Можно оставить это поле пустым и выбрать способы подключения при создании пула услуг.

Новый транспорт

Основной

Учётные данные

Параметры

Расширенный

Тэги

Тэги этого элемента

Имя *

X2Go-xfce

Комментарии

Комментарии этого элемента

Приоритет *

1

Сетевой доступ

☒ Да

Сети

Сети, ассоциированные с транспортом. Если сети не выбраны, это означает все сети

Разрешённые устройства

Если пусто, будет разрешено использовать любое устройство, совместимое с этим транспо...

Сервис-пулы

SL

Отменить и закрыть

Сохранить

» Вкладка **Учетные данные**:

- **Имя пользователя** — имя пользователя, которое будет использоваться для доступа к рабочему столу (пользователь должен существовать на VM). Если данное поле пустое, будет использован логин авторизовавшего в веб-интерфейсе OpenUDS пользователя;

Новый транспорт

Основной

Учётные данные

Параметры

Расширенный

Имя пользователя

Если не пусто, это имя пользователя будет всегда использоваться как учетные данные

Отменить и закрыть

Сохранить

» Вкладка **Параметры**:

- **Размер экрана** — размер окна рабочего стола;

- **Экран** — менеджер рабочего стола (**Xfce**, **Mate** и др.) или виртуализация приложений Linux (**UDS vAPP**);
- **vAPP** — полный путь до приложения (если в поле **Экран** выбрано значение **UDS vAPP**);
- **Включить звук** — включить звук;
- **Перенаправить домашнюю папку** — перенаправить домашнюю папку клиента подключения на виртуальный рабочий стол (на Linux также перенаправлять **/media**);
- **Скорость** — скорость подключения.

Новый транспорт

Основной
Учётные данные
Параметры
Расширенный

Размер экрана
1366x768

Экран
Xfce

vAPP
Если UDS vAPP выбран как «Рабочий стол», FULL PATH приложения будет выполнен. Если UDS v

Включить звук
☒ Да

Перенаправить домашнюю папку
☐ Нет

Скорость
LAN

Отменить и закрыть
Сохранить

» Вкладка **Расширенный**:

- **Звук** — тип звукового сервера;
- **Клавиатура** — раскладка клавиатуры;
- **Метка** — метка транспорта метапула (используется для того чтобы назначить несколько транспортных метапулу).

Новый транспорт

ОсновнойУчётные данныеПараметрыРасширенный

Звук

Pulse

Клавиатура

Раскладка клавиатуры (ru, us, ...)

Реск

16m-jpeg

Качество *

6

Метка

Метка транспорта метапула (используется только при группировке транспорта метапула)

Отменить и закрыть

Сохранить

17.3.4.4. X2Go (туннельный)

Все настройки аналогичны настройке X2Go, за исключением настроек на вкладке **Туннель**.

Вкладка **Туннель**:

- **Туннельный сервер** — IP-адрес/имя OpenUDS Tunnel. Если доступ к рабочему столу осуществляется через глобальную сеть, необходимо ввести общедоступный IP-адрес сервера OpenUDS Tunnel. Формат: IP_Tunnelер:Port;
- **Время ожидания туннеля** — максимальное время ожидания туннеля;
- **Принудительная проверка SSL-сертификата** — принудительная проверка сертификата туннельного сервера.

Новый транспорт

<

Основной

Туннель

Учётные данные

Параметры

>

Туннельный сервер

192.168.0.88:7777

Время ожидания туннеля *

30

Принудительная проверка SSL-сертификата

☐ Нет

Отменить и закрыть

Сохранить

17.3.4.5. SPICE (прямой)



Примечание

Транспортный протокол SPICE может использоваться только с oVirt/RHEV и OpenNebula.

SPICE позволяет пользователям получать доступ к виртуальным рабочим столам Windows/Linux. На клиентах подключения должен быть установлен клиент SPICE (*virt-manager*).



Важно

Для работы прямого подключения по протоколу SPICE на сервере OpenUDS и клиентах OpenUDS, откуда осуществляется подключение, имена узлов платформы виртуализации должны корректно разрешаться в IP-адреса этих узлов.

Параметры конфигурации для настройки транспорта SPICE:

■ Вкладка **Основной**:

- **Имя** — название транспорта;
- **Приоритет** — приоритет, чем меньше значение приоритета, тем выше данный транспорт будет указан в списке доступных транспортных для сервиса. Транспорт с самым низким приоритетом, будет транспортом по умолчанию;
- **Сертификат** — сертификат, сгенерированный в ovirt-engine/RHV-manager или в OpenNebula. Требуется для подключения к виртуальным рабочим столам;
- **Сетевой доступ** — разрешает или запрещает доступ пользователей к службе, в зависимости от сети из которой осуществляется доступ;
- **Сети** — сетевые диапазоны, подсети или IP-адреса (настраиваются в разделе **Сети**). Пустое поле означает «все сети». Используется вместе с параметром **Сетевой доступ**;

- **Разрешенные устройства** — разрешает доступ к службе только с выбранных устройств. Пустое поле означает «все устройства»;
- **Сервис-пулы** — позволяет назначить транспорт одному или нескольким ранее созданным пулам услуг. Можно оставить это поле пустым и выбрать способы подключения при создании пула услуг.

Новый транспорт

Основной

Расширенный

Тэги

Тэги этого элемента

Имя *

SPICE

Комментарии

Комментарии этого элемента

Приоритет *

3

Сертификат

Сетевой доступ

Да

Сети

Сети, ассоциированные с транспортом. Если сети не выбраны, это означает все сети

Разрешённые устройства

Linux

Сервис-пулы

Текущие привязанные пулы услуг

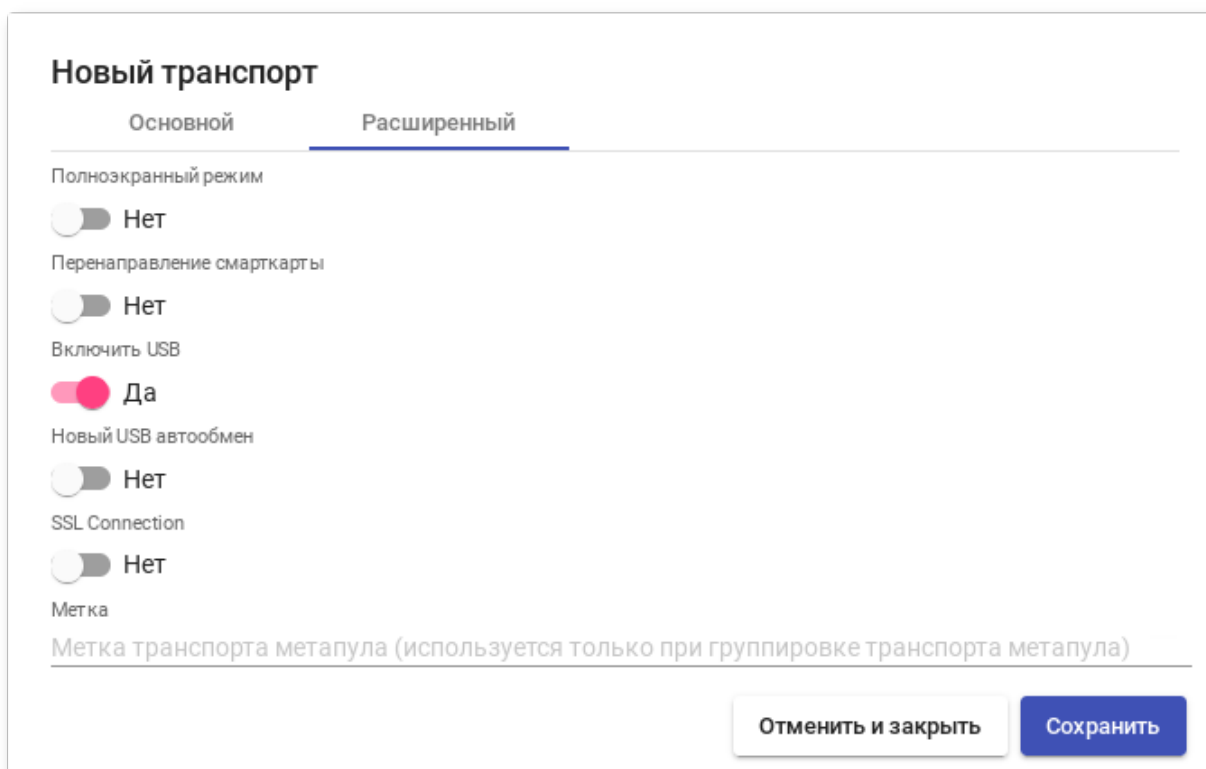
Отменить и закрыть

Сохранить

■ Вкладка **Расширенный**:

- **Полноэкранный режим** — включает полноэкранный режим виртуального рабочего стола;
- **Перенаправление смарткарты** — включает перенаправление смарт-карт;
- **Включить USB** — разрешает перенаправление устройств, подключенных к USB-порту;
- **Новый USB автообмен** — позволяет перенаправлять PnP-устройства, подключенные к USB-порту;
- **SSL Connection** — использовать SSL-соединение;

- **Метка** — метка транспорта метапула (используется для того чтобы назначить несколько транспортов метапулу).



Новый транспорт

Основной **Расширенный**

Полноэкранный режим
☐ Нет

Перенаправление смарткарты
☐ Нет

Включить USB
☒ Да

Новый USB автообмен
☐ Нет

SSL Connection
☐ Нет

Метка
Метка транспорта метапула (используется только при группировке транспорта метапула)

Отменить и закрыть Сохранить

17.3.4.6. HTML5 RDP (туннельный)

HTML5 RDP позволяет пользователям получать доступ к виртуальным рабочим столам Windows/ Linux через протокол RDP с использованием браузера, поддерживающего HTML5. На виртуальных рабочих столах должен быть установлен и включен протокол RDP (для виртуальных рабочих столов Linux необходимо использовать XRDP).

Параметры конфигурации для настройки транспорта HTML5 RDP:

» Вкладка **Основной**:

- **Имя** — название транспорта;
- **Приоритет** — приоритет, чем меньше значение приоритета, тем выше данный транспорт будет указан в списке доступных транспортов для сервиса. Транспорт с самым низким приоритетом, будет транспортом по умолчанию;
- **Сетевой доступ** — разрешает или запрещает доступ пользователей к службе, в зависимости от сети из которой осуществляется доступ;
- **Сети** — сетевые диапазоны, подсети или IP-адреса (настраиваются в разделе **Сети**). Пустое поле означает «все сети». Используется вместе с параметром **Сетевой доступ**;
- **Разрешенные устройства** — разрешает доступ к службе только с выбранных устройств. Пустое поле означает «все устройства»;
- **Сервис-пулы** — позволяет назначить транспорт одному или нескольким ранее созданным пулам услуг. Можно оставить это поле пустым и выбрать способы подключения при создании пула услуг.

Новый транспорт

<

Основной

Туннель

Учётные данные

Параметры

>

Тэги

Тэги этого элемента

Имя *

HTML5RDP

Комментарии

Комментарии этого элемента

Приоритет *

1

Сетевой доступ

☒ Да

Сети

Сети, ассоциированные с транспортом. Если сети не выбраны, это означает все сети

Разрешённые устройства

Если пусто, будет разрешено использовать любое устройство, совместимое с этим транспо...

Сервис-пулы

ALT EDU, SL

Отменить и закрыть

Сохранить

» Вкладка **Туннель**:

- **Туннельный сервер** — IP-адрес или имя OpenUDS Tunnel. Формат: http(s)://IP_Tunnelер: [Port] (8080 — порт по умолчанию для http, 443 — для https).

Новый транспорт

<

Основной

Туннель

Учётные данные

Параметры

>

Туннельный сервер *

http://192.168.0.88:8081

Используйте туннель Glyptodon Enterprise

☐ Нет

Отменить и закрыть

Сохранить

» Вкладка **Учетные данные**:

- **Пропустить данные аккаунта** — если установлено значение **Да**, учетные данные для доступа к виртуальному рабочему столу будут запрашиваться при подключении к серверу. Если установлено значение **Нет**, будут использоваться данные OpenUDS (см. ниже);
- **Имя пользователя** — имя пользователя, которое будет использоваться для доступа к рабочему столу (пользователь должен существовать на VM). Если данное поле пустое, будет использован логин авторизовавшегося в веб-интерфейсе OpenUDS пользователя;
- **Пароль** — пароль пользователя, указанного в поле **Имя пользователя**;
- **Без домена** — указывает, перенаправляется ли доменное имя вместе с пользователем. Значение **Да** равносильно пустому полю **Домен**;
- **Домен** — домен. Если поле не пустое, то учетные данные будут использоваться в виде DOMAIN\user.

Новый транспорт

< Основной Туннель Учётные данные Параметры >


Пропустить данные аккаунта

☐ Нет

Имя пользователя

user

Пароль

..... 

Без домена

☐ Нет

Домен

Если это не пусто, этот домен всегда будет использоваться в качестве учетных данных (используйте)

Отменить и закрыть

Сохранить

» Вкладка **Параметры**:

- **Показать обои** — отображать обои рабочего стола;
- **Разрешить композицию рабочего стола** — включить «Desktop Composition»;
- **Сглаживание шрифтов** — активирует сглаживание шрифтов;
- **Включить аудио** — перенаправлять звук с рабочего стола на клиент подключения;
- **Включить микрофон** — включить микрофон на виртуальном рабочем столе;
- **Включить печать** — включить печать на виртуальном рабочем столе;

- **Обмен файлами** — политика обмена файлами между виртуальным рабочим столом и клиентом подключения. Позволяет создать временный каталог (расположенный на сервере OpenUDS Tunnel), для возможности обмена файлами между виртуальным рабочим столом и клиентом подключения;
- **Буфер обмена** —настройка общего буфера обмена;
- **Раскладка** — раскладка клавиатуры, которая будет включена на рабочем столе.

Новый транспорт

<

Ювнйой

Туннель

Учётные данные

Параметры

Рас

>

Показать обои

Нет

Разрешить композицию рабочего стола

Нет

Сглаживание шрифтов

Нет

Включить аудио

Нет

Включить микрофон

Нет

Включить печать

Нет

Обмен файлами

Enable file sharing

Буфер обмена

Enable clipboard

Раскладка *

English (US) keyboard

Отменить и закрыть

Сохранить

■ Вкладка **Расширенный**:

- **Срок действия билета** — допустимое время (в секундах) для клиента HTML5 для перезагрузки данных из OpenUDS Broker (рекомендуется использовать значение по умолчанию — 60);
- **Открывать HTML в новом окне** — позволяет указать открывать ли подключение в новом окне;
- **Безопасность** — позволяет задать уровень безопасности соединения;
- **Порт RDP** — порт RDP (по умолчанию — 3389);

■ **Метка** — метка транспорта метапула (используется для того чтобы назначить несколько транспортов метапулу).

Новый транспорт

< Туннель Учётные данные Параметры Расширенный >

Срок действия билета *

60

Открывать HTML в новом окне *

Open every connection on the same window, but keeps UDS window.

▼

Безопасность *

Any (Allow the server to choose the type of auth)

▼

Порт RDP *

3389

Путь к контексту Glyptodon Enterprise

/

Метка

Метка транспорта метапула (используется только при группировке транспорта метапула)

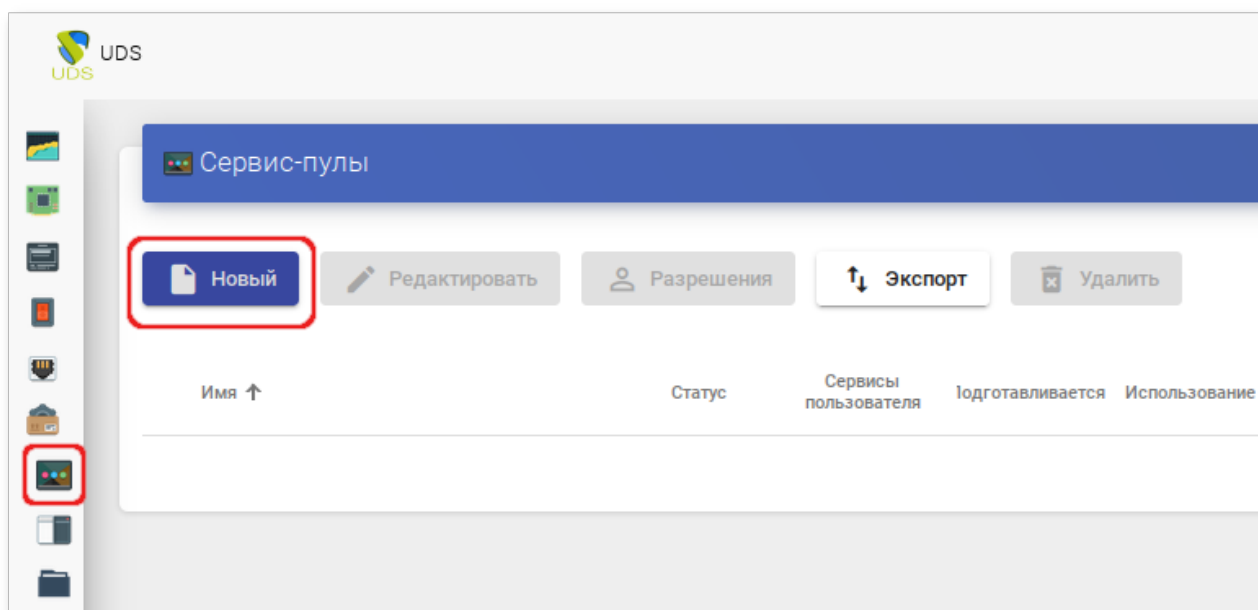
Отменить и закрыть

Сохранить

17.3.5. Пулы услуг

После того как был создан и настроен хотя бы один [поставщик услуг](#) с соответствующей службой/услугой, [аутентификатор](#) (с пользователем и группой), [менеджер ОС](#) и [транспорт](#), можно создать пул услуг (Сервис-пул) для публикации виртуальных рабочих столов.

Для создания пула услуг необходимо в разделе **Сервис-пулы** нажать кнопку **Новый**:



Заполнить параметры конфигурации:

» Вкладка **Основной**:

- **Имя** — название службы (это имя будет показано пользователю для доступа к рабочему столу или виртуальному приложению). В этом поле можно использовать переменные для отображения информации об услугах:
 - **{use}** — указывает процент использования пула (рассчитывается на основе поля **Максимальное количество предоставляемых сервисов** и назначенных услуг);
 - **{total}** — общее количество машин (данные извлечены из поля **Максимальное количество предоставляемых сервисов**);
 - **{usec}** — количество машин, используемых пользователями в пуле;
 - **{left}** — количество машин, доступных в пуле для подключения пользователей;
- **Базовый сервис** — служба, созданная ранее в поставщике услуг (состоит из поставщика услуг и базовой услуги);
- **ОС Менеджер** — ранее созданный менеджер ОС, конфигурация которого будет применяться к каждому из созданных виртуальных рабочих столов или приложений. Если выбрана услуга типа **Статический IP**, это поле не используется;
- **Публиковать при создании** — если этот параметр включен, при сохранении пула услуг система автоматически запустит первую публикацию. Если установлено значение **Нет**, будет необходимо запустить публикацию сервиса вручную (из вкладки **Публикации**).

Новый пул услуг

ОсновнойЭкран/ДисплейРасширенныйДоступность

Тэги

Тэги этого элемента

Имя *

SL

Короткое имя

Короткое имя для визуализации сервисов пользователя

Комментарии

Комментарии этого элемента

Базовый сервис

PVE\Simply

ОС менеджер

Linux non-persistent

Публиковать при создании

☒ Да

Отменить и закрытьСохранить

» Вкладка **Экран/Дисплей**:

- **Видимый** — если этот параметр отключен, пул не будет отображаться у пользователей;
- **Привязанный образ** — изображение, связанное с услугой. Изображение должно быть предварительно добавлено в репозиторий изображений (раздел **Инструменты** → **Галерея**);
- **Пул-группа** — позволяет группировать различные службы. Группа должна быть предварительно создана в разделе **Пулы** → **Группа**;
- **Доступ к календарю запрещён** — позволяет указать сообщение, которое будет показано пользователю, если доступ к сервису ограничен правилами календаря.

Новый пул услуг

Основной

Экран/Дисплей

Расширенный

Доступность

Видимый

Да

Привязанный образ

SL2

Пул-группа

По умолчанию

Доступ к календарю запрещён

Пользовательское сообщение, которое будет показано пользователям, если доступ ограничен прави

Отменить и закрыть

Сохранить

» Вкладка **Расширенный**:

- **Разрешить удаление пользователями** — если этот параметр включен, пользователи могут удалять назначенные им службы. Если сервис представляет собой виртуальный рабочий стол, автоматически сгенерированный OpenUDS, он будет удален, и при следующем подключении ему будет назначен новый. Если это другой тип сервиса (vAPP/статический IP), будет удалено только назначение, а новое будет назначено на следующее подключение;
- **Разрешить сброс пользователям** — если этот параметр включен, пользователь сможет перезапускать или сбрасывать назначенные ему службы (относится только к виртуальным рабочим столам, автоматически созданным OpenUDS);
- **Игнорирует неиспользуемые** — если этот параметр включен, непостоянные пользовательские службы, которые не используются, не будут удаляться;
- **Показать транспорты** — если этот параметр включен, будут отображаться все транспорты, назначенные услуге. Если параметр не активирован, будет отображаться только транспорт по умолчанию (с наивысшим приоритетом);
- **Учётные записи** — назначение услуги ранее созданным «Аккаунтам» (Пулы → Аккаунты).

Новый пул услуг

ОсновнойЭкран/ДисплейРасширенныйДоступность

Разрешить удаление пользователями

☐ Нет

Разрешить сброс пользователям

☐ Нет

Игнорирует неиспользуемые

☐ Нет

Показать транспорты

☒ Да

Учётные записи

Отменить и закрыть

Сохранить

» Вкладка **Доступность**:

- **Первоначально доступные сервисы** — минимальное количество виртуальных рабочих столов, созданных, настроенных и назначенных/доступных для службы;
- **Сервисы для удержания в кэше** — количество доступных виртуальных рабочих мест. Эти ВМ всегда будут настроены и готовы к назначению пользователю (они будут автоматически создаваться до тех пор, пока не будет достигнуто максимальное количество машин, указанное в поле **Максимальное количество предоставляемых сервисов**);
- **Сервисы, хранящиеся в L2 кэше** — количество виртуальных рабочих столов в спящем или выключенном состоянии. Виртуальные рабочие столы, сгенерированные на уровне кэша L2, будут помещены в кэш, как только система потребует их (они никогда не будут напрямую назначены пользователям);
- **Максимальное количество предоставляемых сервисов** — максимальное количество виртуальных рабочих столов, созданных системой в данном пуле (рабочие столы, созданные в кэше L2, не учитываются).

Новый пул услуг

Основной

Экран/Дисплей

Расширенный

Доступность

Первоначально доступные сервисы

5

Сервисы для удержания в кэше

5

Сервисы, хранящиеся в L2 кэше

0

Максимальное количество предоставляемых сервисов

10

Отменить и закрыть

Сохранить

После нажатия кнопки **Сохранить** система начнет создавать виртуальные рабочие столы на основе настроенного кэша.

После создания пула, в настройках (дважды щелкнуть мышью по строке созданного пула или в контекстном меню пула выбрать пункт **Подробнее**) необходимо:

- »на вкладке **Группы** назначить группы доступа (выбрать аутентификатор и группу, которая будет иметь доступ к этому пулу служб):

← SL

← Резюме Назначен...

Привязанные группы

Новый Экспорт

Имя

user@Internal

Новая группа для SL

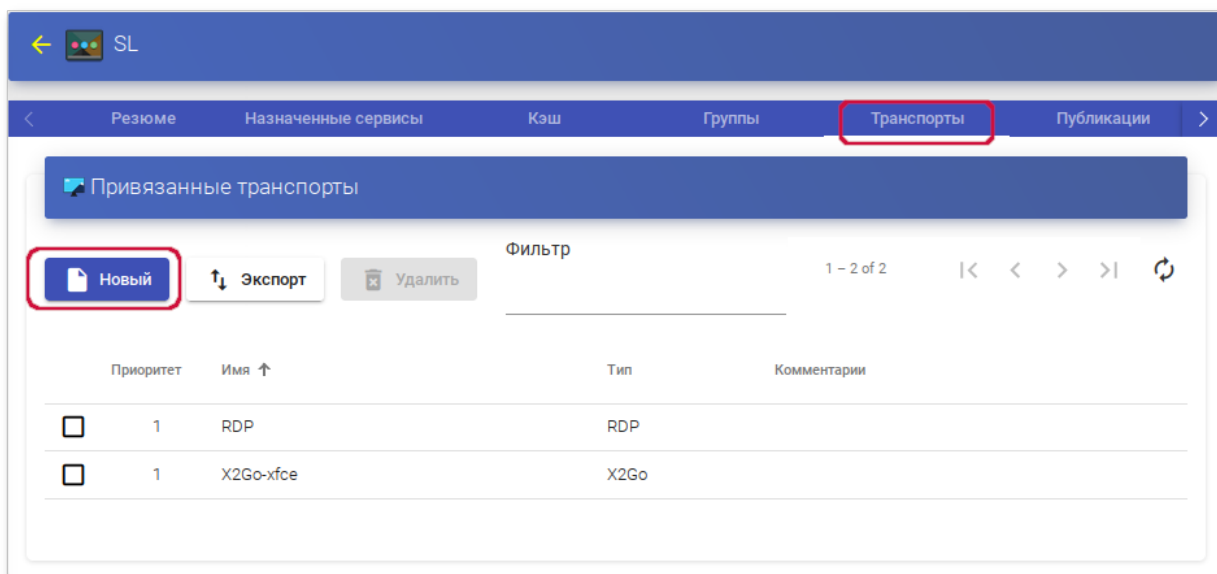
Аутентификатор
freeipa

Группа
cn=ipausers,cn=groups,cn=accounts,dc=example,dc=test

1 – 1 of 1

Отменить Хорошо

- »на вкладке **Транспорты** выбрать способы подключения пользователей к рабочему столу:

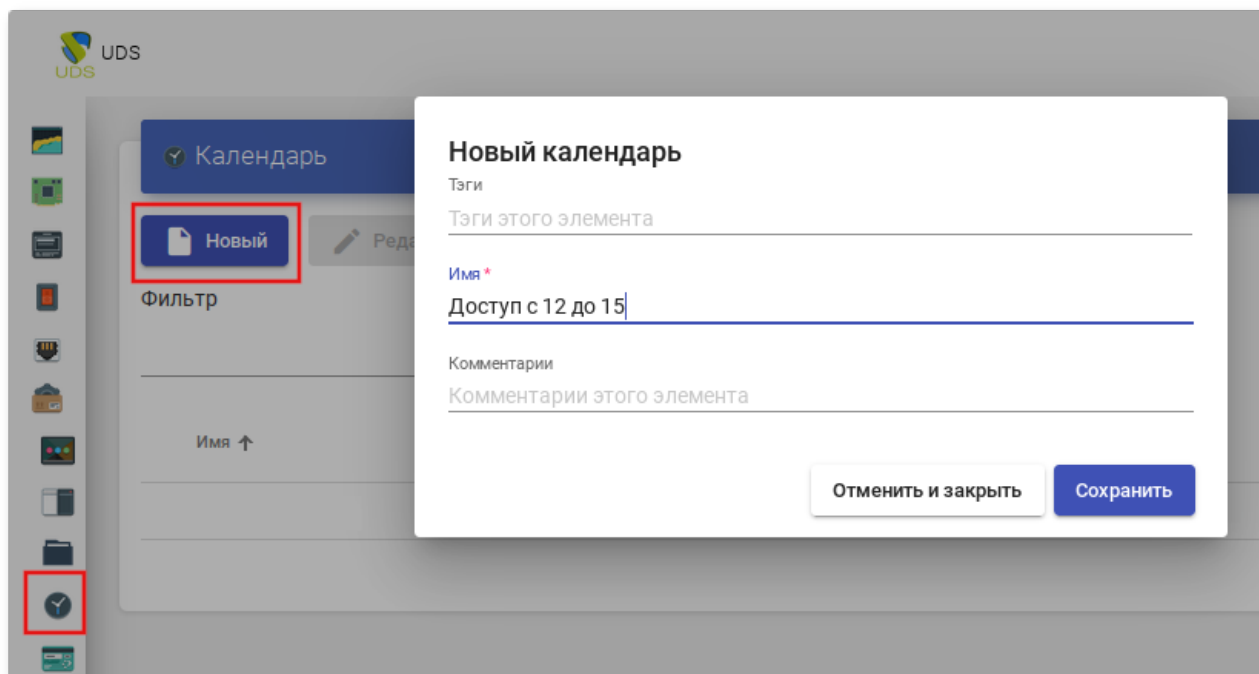


17.3.6. Управление доступом по календарю

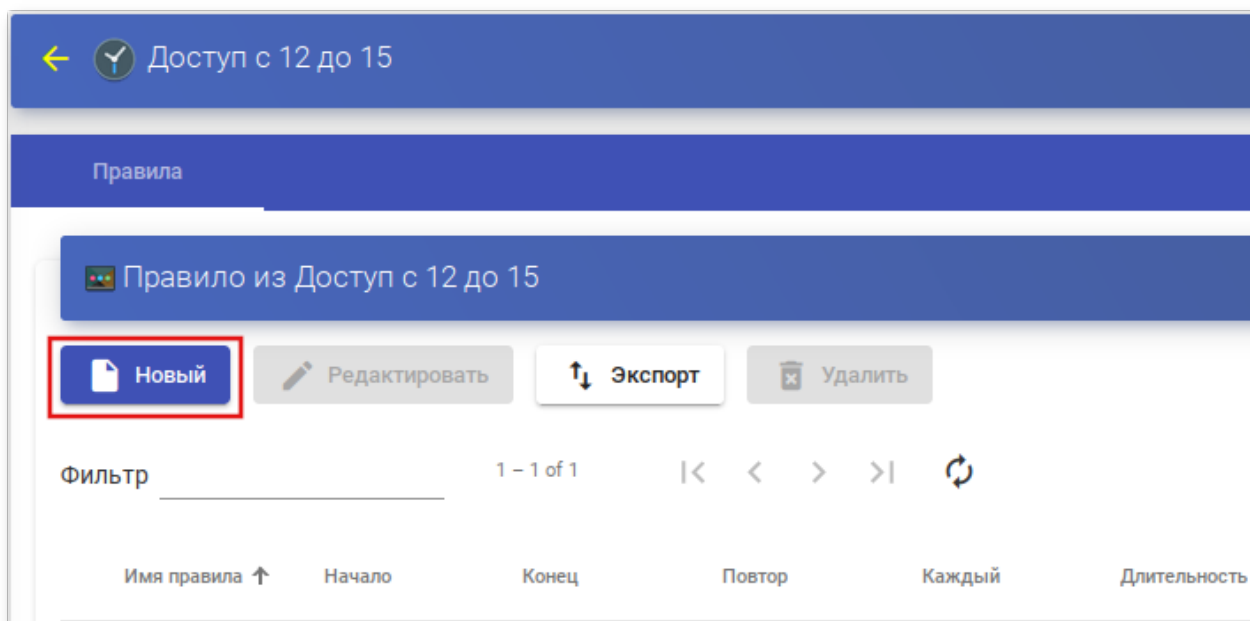
В OpenUDS можно настроить ограничение доступа пользователей к удаленным рабочим столам и виртуальным приложениям по дате и времени.

С помощью календаря также можно автоматизировать определенные задачи в **Пуле услуг**, такие, как создание новых публикаций, настройка значений системного кэша, добавление/удаление групп и транспорта, изменение максимального количества услуг.

Для создания календаря необходимо в разделе **Календари** нажать кнопку **Новый**:



В **Календаре** можно зарегистрировать правила, чтобы запланировать доступность услуги в определенное время. Для создания правила следует выбрать календарь (дважды щелкнуть мышью по строке созданного календаря или в контекстном меню календаря выбрать пункт **Подробность**) и нажать кнопку **Новый**:



Минимальные параметры для настройки правила:

- » **Имя** — название правила;
- » **Событие** — настройка времени выполнения. Необходимо указать время начала и продолжительность события (в минутах/часах/днях/неделях);
- » **Repetition (Периодичность)** — настройка периодичности выполнения. Необходимо указать дату начала, частоту повторения правила (ежедневно/еженедельно/ежемесячно/ежегодно/по будням) и интервал повторения (в днях);
- » **Панель** — показывает сводные данные (резюме) всех ранее указанных настроек.

Новое правило

Имя

12-15

Комментарии

Событие

Время начала

12:00 AM

Продолжительность



3



Единицы длительности

Часы



Repetition

Дата начала

22.08.2022



Повторять до даты

Навсегда



Частота

Ежедневно



Повторять каждый

1



день

Панель

Это правило будет действовать каждый 1 день, от 22.08.2022 далее, начиная с 00:00 и каждое событие будет активным в течение 3 Часы

Отменить

Хорошо

После нажатия кнопки **Хорошо** будет создано правило, которое будет назначено **Пулу услуг** (виртуальному рабочему столу и/или приложению):

Правило из Доступ с 12 до 15

Новый

Редактировать

Экспорт

Удалить

Фильтр

1 – 1 of 1



Имя правила ↑

Начало

Конец

Повтор

Каждый

Длительность



12-15

22.08.2022 00:00

Никогда

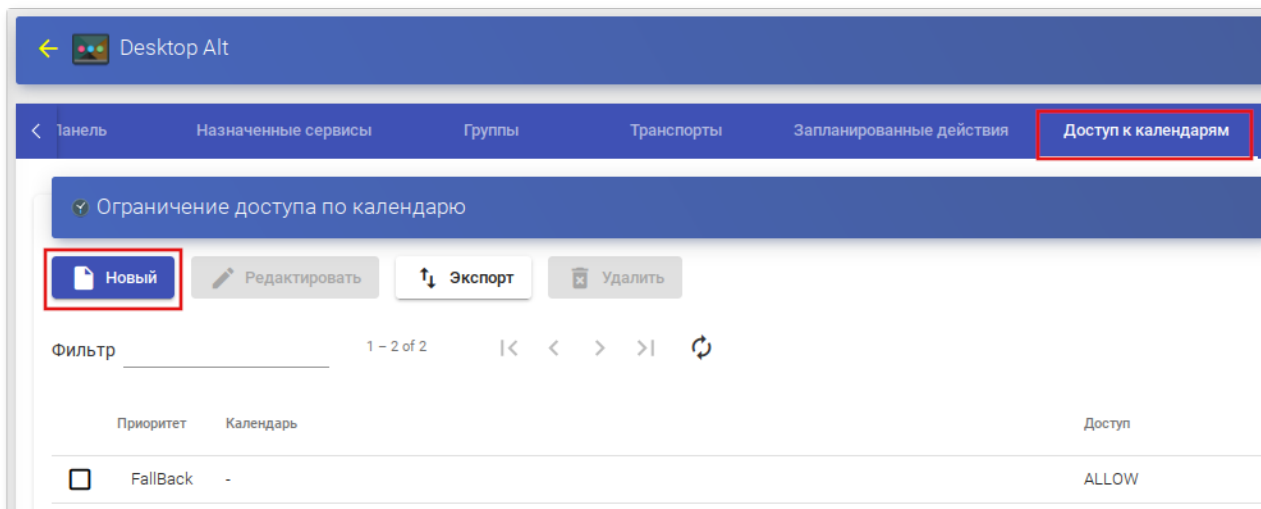
Раз в день

1 день

3 Часы

17.3.6.1. Разрешение/запрет доступа

После настройки правил в календарях их можно использовать для управления доступом пользователей к службам рабочего стола или приложениям. Для этого следует выбрать **Пул услуг**, перейти на вкладку **Доступ к календарям** и нажать кнопку **Новый**:



В открывшемся окне необходимо указать приоритет доступа, выбрать календарь и указать действие, которое будет применяться при доступе к сервису:

Новое правило доступа для Desktop Alt

Приоритет
0

Календарь
Доступ с 12 до 15

Действие
ALLOW

Отменить | Хорошо



Примечание

Правило по умолчанию (**FallBack**) должно разрешать или запрещать доступ к сервису, когда календарь не применяется:

Ограничение доступа по календарю			
Новый	Редактировать	Экспорт	Удалить
Фильтр _____ 1 – 2 of 2 < < > > ↺			
Приоритет	Календарь	Доступ	
<input type="checkbox"/>	FallBack	DENY	
<input type="checkbox"/>	0	Доступ с 12 до 15	
		ALLOW	

17.3.6.2. Запланированные действия

После настройки правил в календарях их можно использовать для планирования определенных задач в **Пуле услуг**. Для этого следует выбрать **Пул услуг**, перейти на вкладку **Запланированные действия** и нажать кнопку **Новый**:

← Desktop Alt

< Панель

Назначенные сервисы

Группы

Транспорты

Запланированные действия

Доступ к календарям

Запланированные действия

Новый Редактировать Запустить сейчас Экспорт Удалить

Фильтр _____ 1 – 2 of 2 |< < > >| ↺

Календарь Действие Параметры Относительно Смещение времени Следующий запуск Последний запуск

В открывшемся окне необходимо указать календарь, время, в течение которого будет выполняться действие, выбрать действие:

Новое действие для Desktop Alt

Календарь
Доступ с 12 до 15

Смещение событий (минуты)
0

В начале интервала?
☒ да

Действие
Добавить транспорт

Транспорт
HTML5RDP

ОтменитьХорошо

Список возможных действий зависит от поставщика услуг данного пула:

- » **Установить начальные сервисы** — сбрасывает минимальное количество созданных и настроенных виртуальных рабочих столов;
- » **Установить размер кеша** — сбрасывает виртуальные рабочие столы, доступные в системном кеше. Эти рабочие столы будут настроены и готовы к назначению пользователю;
- » **Установить максимальное количество сервисов** — изменяет максимальное количество виртуальных рабочих столов в Пуле услуг;
- » **Установить размер L2 кэша** — сбрасывает виртуальные рабочие столы, доступные в кэше L2;
- » **Публикация** — создание новой публикации в Пуле услуг;
- » **Добавить транспорт** — добавляет существующий транспорт в Пул услуг;
- » **Удалить транспорт** — удаляет транспорт из Пула услуг;
- » **Удалить все транспорты** — удаляет весь транспорт из Пула услуг;
- » **Добавить группу** — добавляет существующую группу в Пул услуг;
- » **Удалить группу** — удаляет группу из Пула услуг;
- » **Удалить все группы** — удаляет все группы из Пула услуг;
- » **Устанавливает игнорирование неиспользуемых** — устанавливает параметр Игнорировать неиспользуемые;
- » **Удалить ВСЕ назначенные пользовательские сервисы** — удаляет все службы, назначенные пользователям.

- » **Удалить СТАРЫЕ назначенные пользовательские сервисы** — удаляет службы, назначенные пользователям, которые не использовались заданное время.

После сохранения появится запланированная задача, выполняющая конкретное действие в данном **Пуле услуг**.

17.3.7. Настройка разрешений

В OpenUDS можно назначать пользователям и группам пользователей права доступа к различным элементам администрирования. Разрешения будут назначены непосредственно для каждого элемента, а также будут применяться к его подэлементам.



Примечание

Чтобы пользователь мог получить доступ к администрированию, ему должна быть назначена роль **Штатный сотрудник**:

Редактировать пользователя test

Имя пользователя
test

Настоящее имя
test

Комментарии

Состояние
Включено

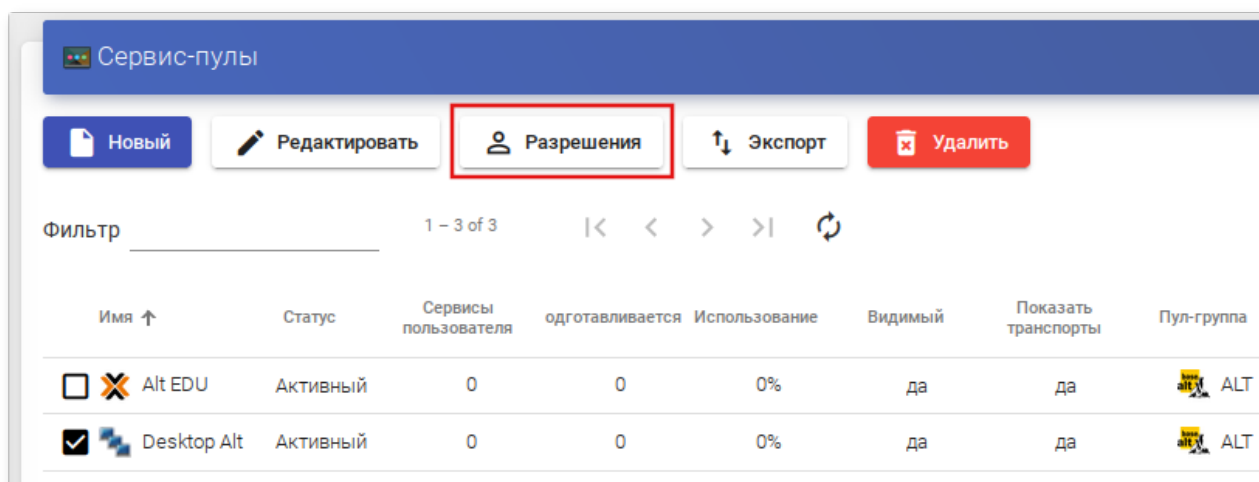
Роль
Штатный сотрудник

Пароль

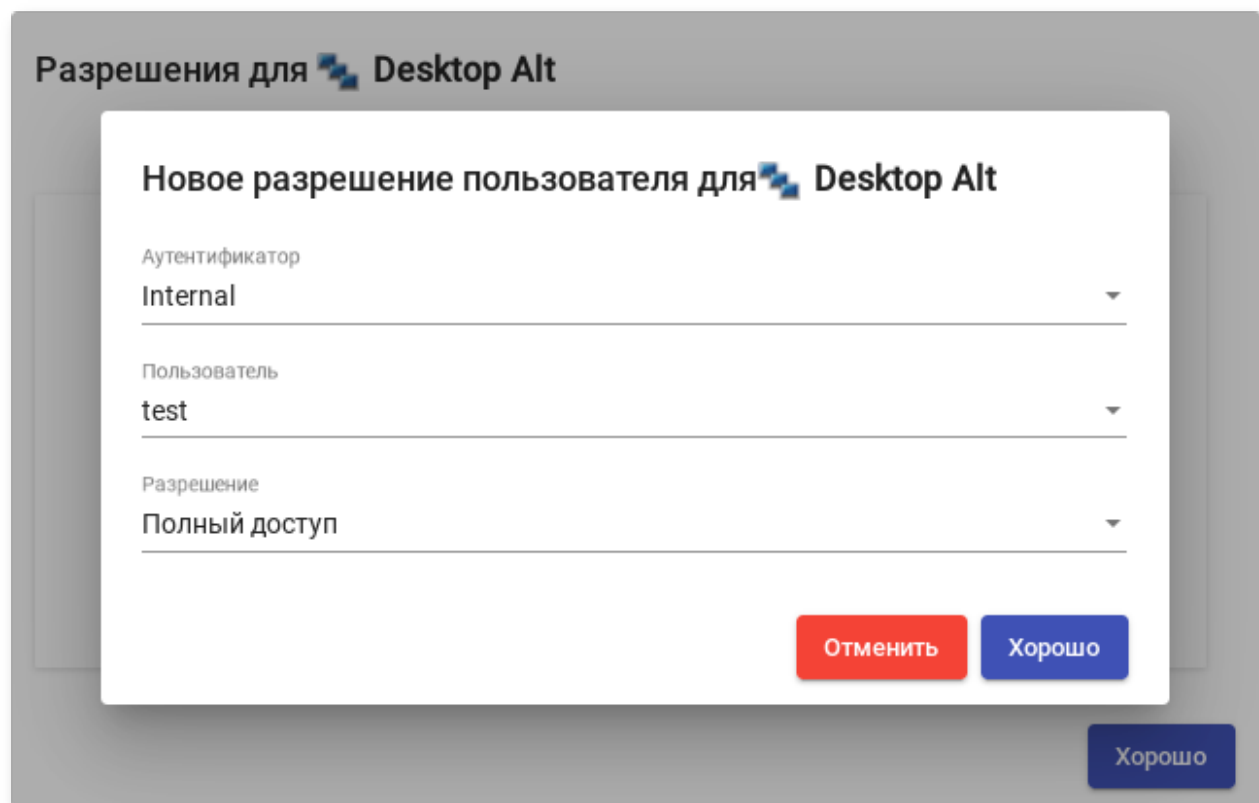
Группы
test

Отменить Хорошо

Для предоставления разрешения к элементу администрирования следует выбрать элемент и нажать кнопку **Разрешения**:



В окне разрешений следует нажать ссылку **Новое разрешение...** для групп или пользователей, выбрать аутентификатор и группу/пользователя, к которым будет применяться разрешение. Также нужно указать, будет ли пользователь/группа иметь доступ для чтения к элементу (**Только чтение**) или полный доступ (**Полный доступ**):



После сохранения настроек, пользователи, которым назначена роль **Штатный сотрудник**, смогут получить доступ к этому элементу администрирования с назначенными разрешениями.



Примечание

Разрешения типа **Полный доступ (Управление)** могут применяться только к элементам второго уровня (**Календари, Пулы услуг** и т.д.).

17.4. Подготовка шаблона виртуальной машины

Для возможности использования ВМ в качестве шаблона OpenUDS, на машине необходимо включить и настроить удаленный рабочий стол, установить OpenUDS Actor и зарегистрировать его на сервере OpenUDS.

17.4.1. Шаблон ВМ с ОС Альт

Подготовить шаблон ВМ (все действия выполняются на ВМ):

1. Установить openuds-actor:

```
# apt-get install openuds-actor
```

2. Включить автозапуск сервиса udsactor.service:

```
# systemctl enable udsactor.service
```

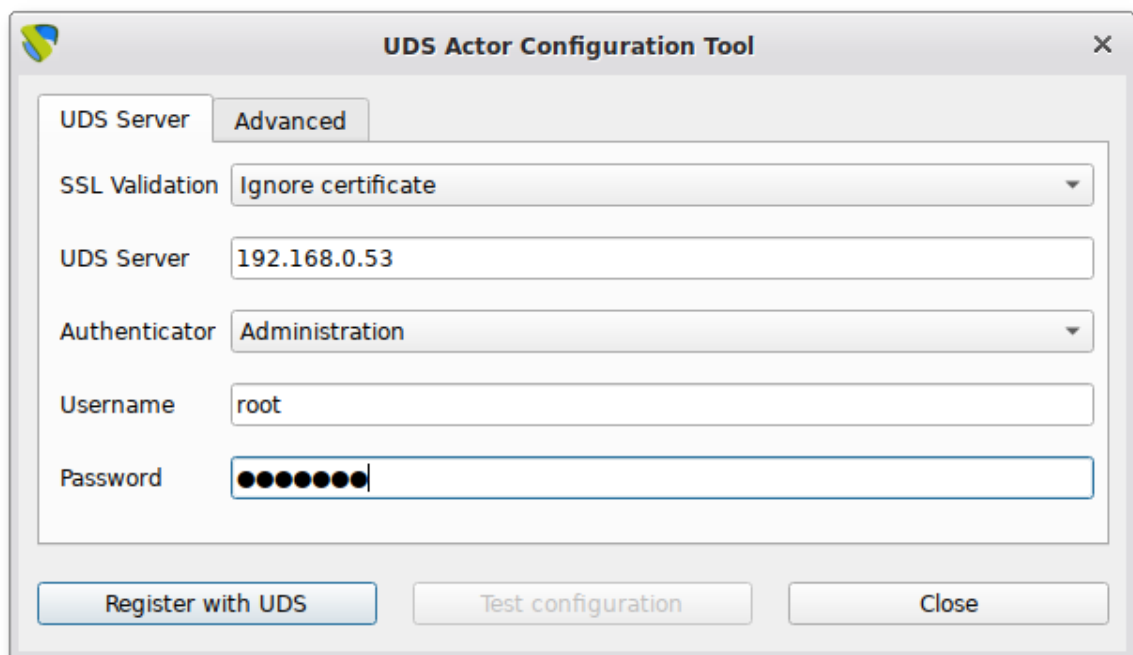
3. Зарегистрировать OpenUDS Actor на сервере OpenUDS:

▶ запустить OpenUDS Actor из меню **Настройки** → **UDS Actor Configuration** или командой:

```
$ /usr/sbin/UDSActorConfig-pkexec
```

Потребуется ввести пароль пользователя, входящего в группу wheel.

▶ на вкладке **UDS Server** 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
```

17.4.2. Шаблон ВМ с ОС Windows



Примечание

В данном разделе рассмотрен процесс настройки ВМ с ОС Windows x64 10 Pro для использования в качестве шаблона OpenUDS.

Требования к шаблону ВМ с ОС Windows:

- рекомендуется отключить автоматические обновления, чтобы предотвратить выполнение этого процесса на создаваемых виртуальных рабочих столах;
- машина должна получать IP-адрес по DHCP;
- шаблон не нужно добавлять в домен Active Directory. Если нужны виртуальные рабочие столы, включенные в домен AD, настройка должна быть выполнена в панели управления OpenUDS;
- автоматический вход пользователя должен быть отключён (учетные данные всегда должны запрашиваться у пользователя).

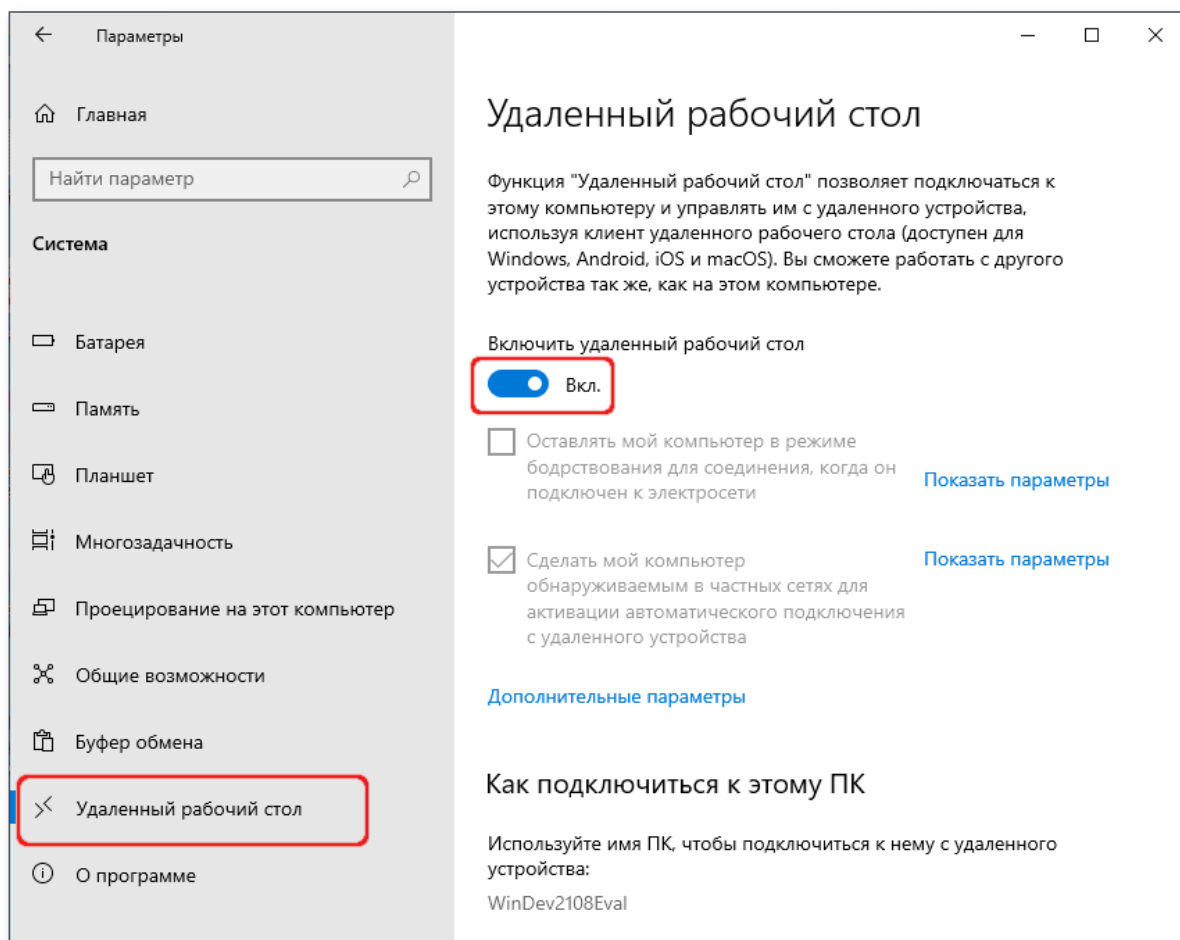


Примечание

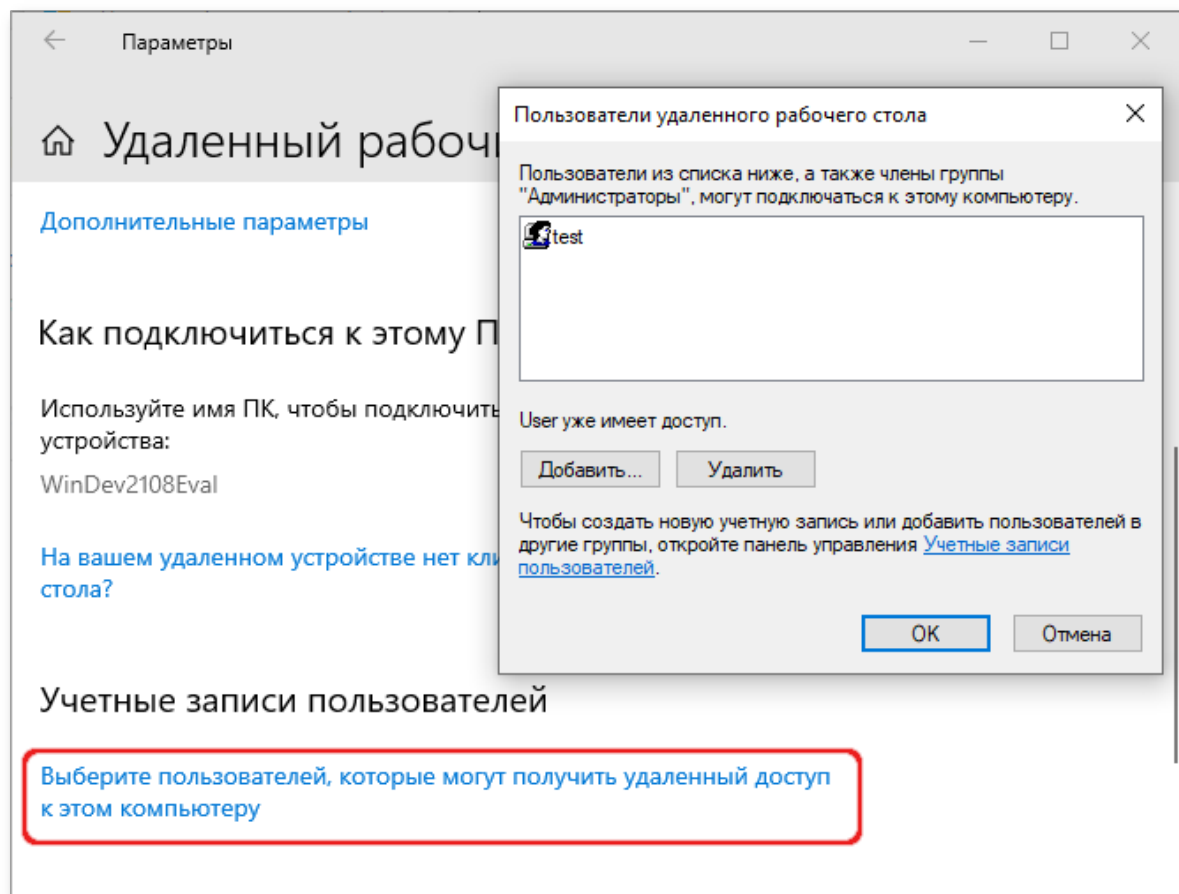
Для возможности ввода VM в домен, в шаблоне VM должен быть доступен сервер DNS, имеющий записи про контроллер домена Active Directory.

Для настройки удаленного рабочего стола, необходимо выполнить следующие действия в шаблоне VM:

1. Открыть окно **Параметры (Win+I)**.
2. Выбрать раздел **Система**, а затем слева в списке — **Удаленный рабочий стол**.
3. Ползунок **Включить удаленный рабочий стол** установить 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:

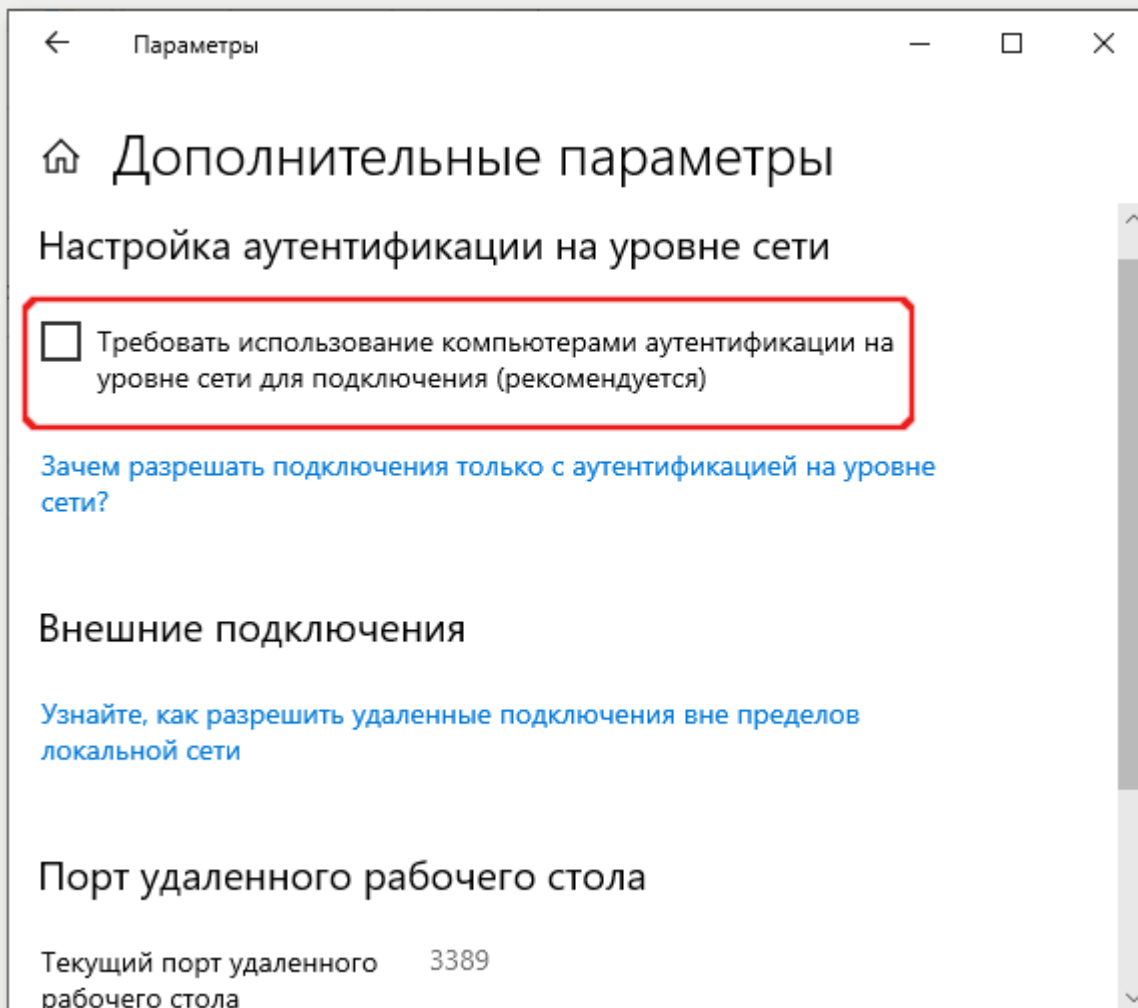


5. Проверить возможность подключения к машине удаленно.



Примечание

Для возможности подключения клиентов Linux может потребоваться снять отметку с пункта **Требовать использование компьютерами аутентификации на уровне сети для подключения** в дополнительных параметрах:

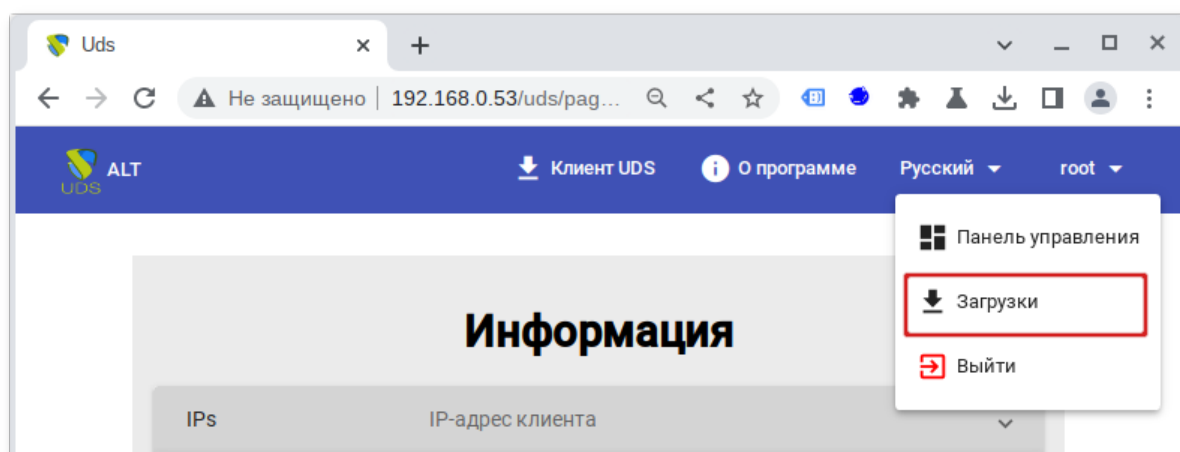


Важно

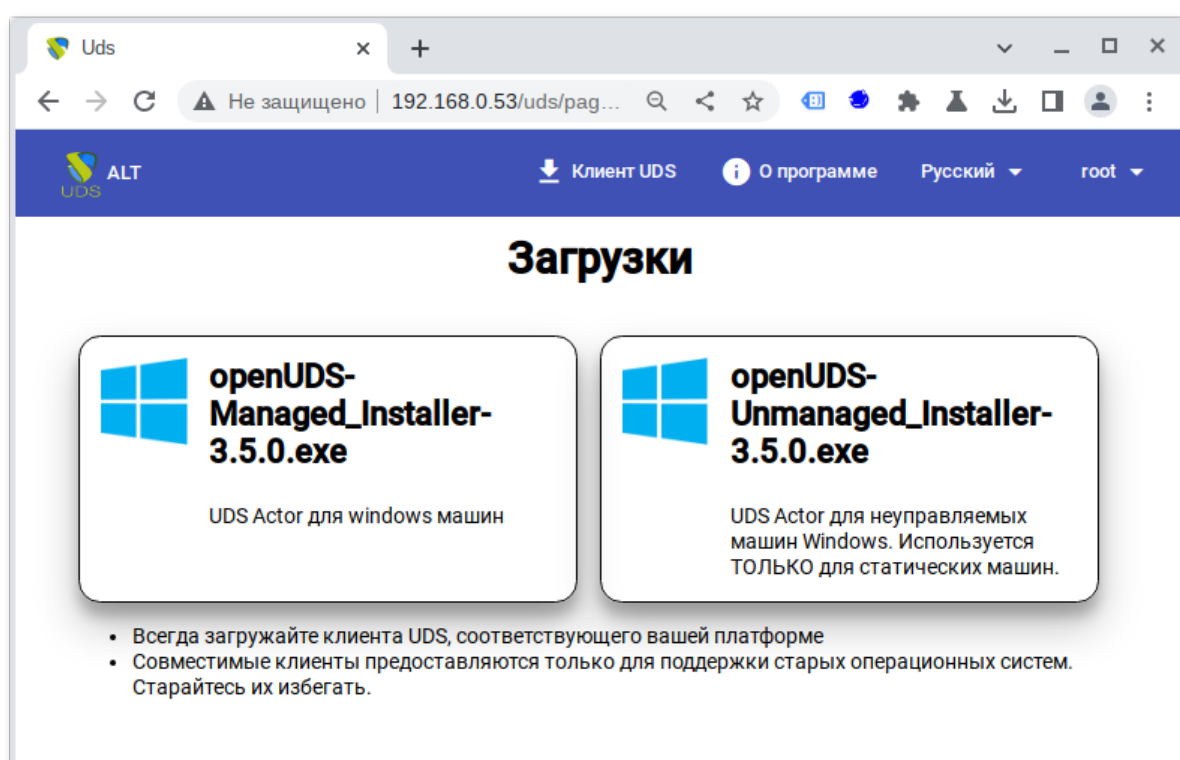
Необходимо убедиться, что межсетевой экран не блокирует соединения по 3389 порту.

Настройка OpenUDS Actor:

1. Загрузить OpenUDS Actor. Для этого в панели управления OpenUDS Server выбрать пункт **Загрузки** (пункт доступен пользователям с правами администратора):



На открывшейся странице выбрать нужный UDS Actor:



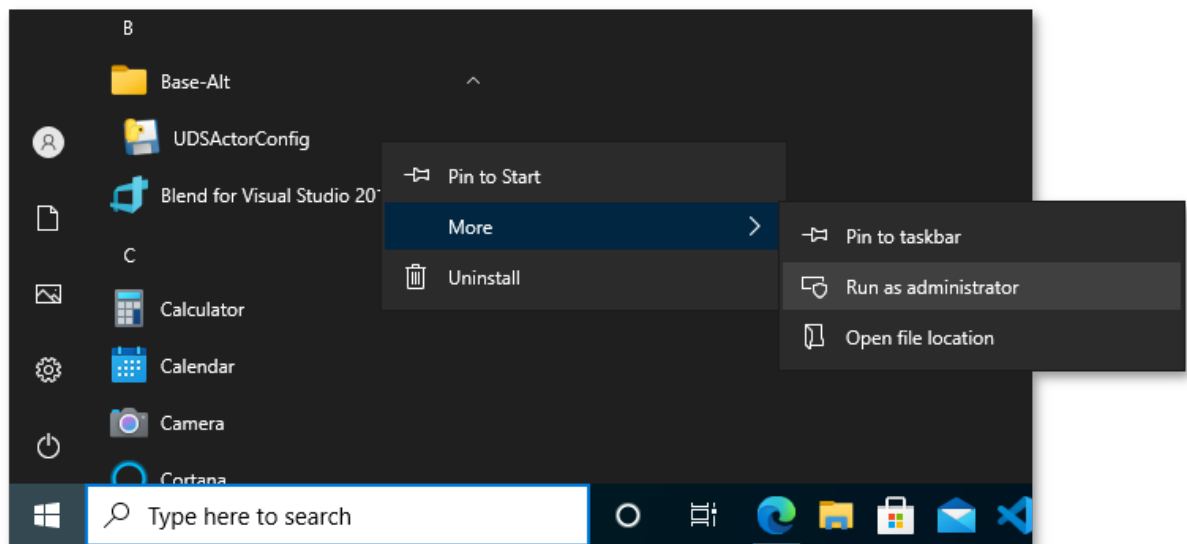
Примечание

Для машин с ОС Windows есть два вида OpenUDS Actor:

- »openUDS-Managed_Installer — для управляемых управляемых Windows машин;
- »openUDS-Unmanaged_Installer — для неуправляемых Windows машин.

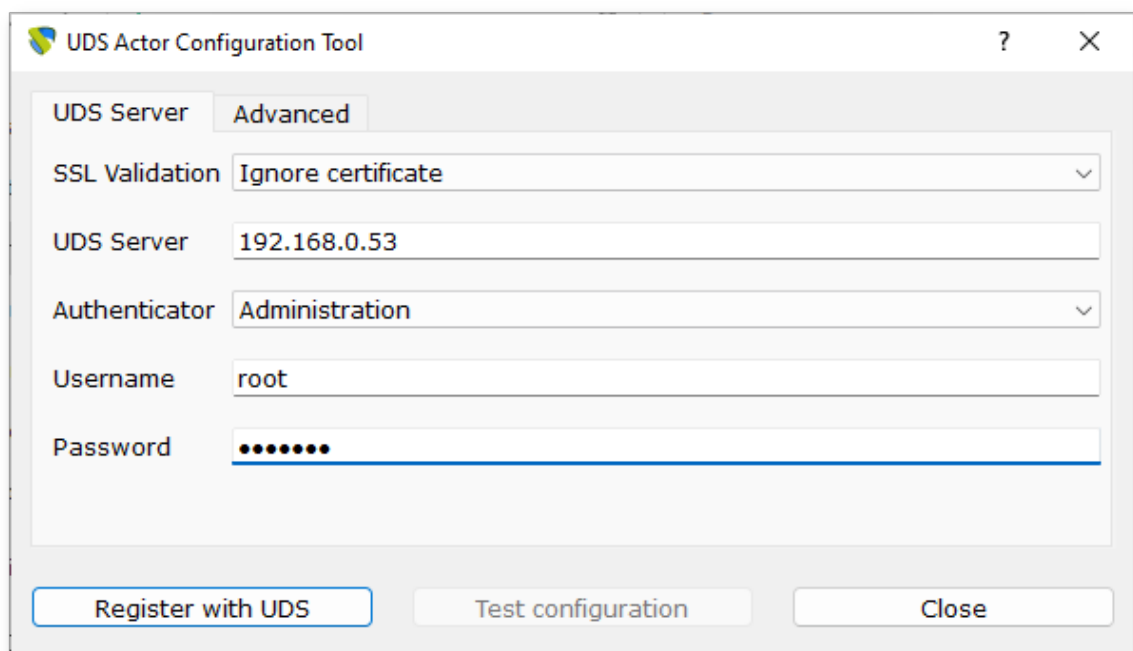
Используется только для отдельных серверов без виртуализации.

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**):

UDS Actor Configuration Tool

SSL Validation: Ignore certificate

UDS Server: 192.168.0.53

Service Token: 8e21acf12a0d5c9d

Restrict Net:

Log Level: ERROR

Buttons: Save Configuration, Test configuration, Close



Примечание

Unmanaged OpenUDS Actor уведомляет OpenUDS, когда пользователь входит в систему и выходит из нее. Благодаря этой функции система может освободить компьютер, при выходе пользователя из системы. Для использования этой функции при регистрации услуги **Статический множественный IP-адрес** кроме названия услуги следует указать один или несколько IP-адресов машин, к которым будет осуществляться доступ и ключ в поле **Ключ услуги**:

UDS

StaticIP

Панель

Услуги StaticIP

Новый

Фильтр

Имя сервиса ↑

EDU

Students

Изменить сервис

Основной

Расширенный

Теги

Теги этого элемента

Имя *

Students

Комментарии

Комментарии этого элемента

Список серверов

192.168.0.124, 192.168.0.125, 192.168.0.117

Ключ услуги

8e21acf12a0d5c9d

Отменить и закрыть

Сохранить

Если оставить поле **Ключ услуги** пустым, сеанс останется назначенным пользователю, пока администратор не удалит его вручную.

17.5. Настройка клиента OpenUDS

Для возможности подключения к брокеру соединений и дальнейшего получения доступа к виртуальному рабочему окружению на клиентской машине должны быть установлены OpenUDS Client и клиенты каждого используемого протокола удаленного доступа.

17.5.1. Клиент с ОС Альт

На клиенте должен быть установлен пакет *openuds-client*:

```
# apt-get install openuds-client
```

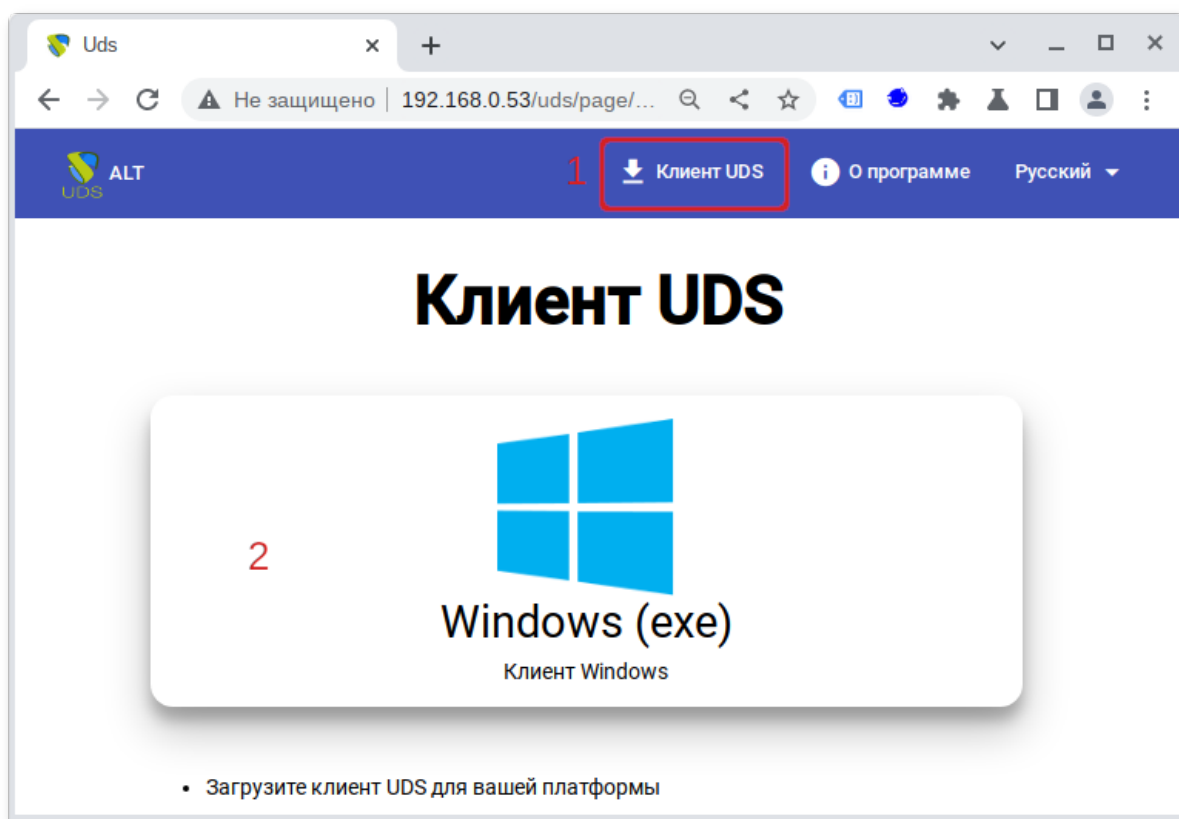
Для возможности подключения к виртуальному рабочему столу, должны быть установлены клиенты протоколов удаленного доступа:

- *xfreerdp* — для подключения по протоколу RDP;
- *x2goclient* — для подключения к серверу X2Go;
- **remote-viewer** из пакета *virt-viewer* — для подключения по протоколу SPICE.

17.5.2. 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, SPICE.



Примечание

Для установки клиента X2Go на ОС Windows достаточно загрузить клиент [X2Go](#) и установить его.

Для установки клиента SPICE на ОС Windows необходимо установить [virt-viewer](#).

17.6. Подключение пользователя к виртуальному рабочему месту

Подключиться к серверу OpenUDS с помощью браузера http://openuds_address, ввести имя пользователя и пароль, выбрать средство проверки подлинности, если доступно несколько:

Uds — Mozilla Firefox

Uds

← → ↻ 🏠 🔒 <https://192.168.0.53/uds/page/login> 90% ☆ 🔍 ⚙

UDS Клиент UDS О программе Русский ▾

UDS Enterprise

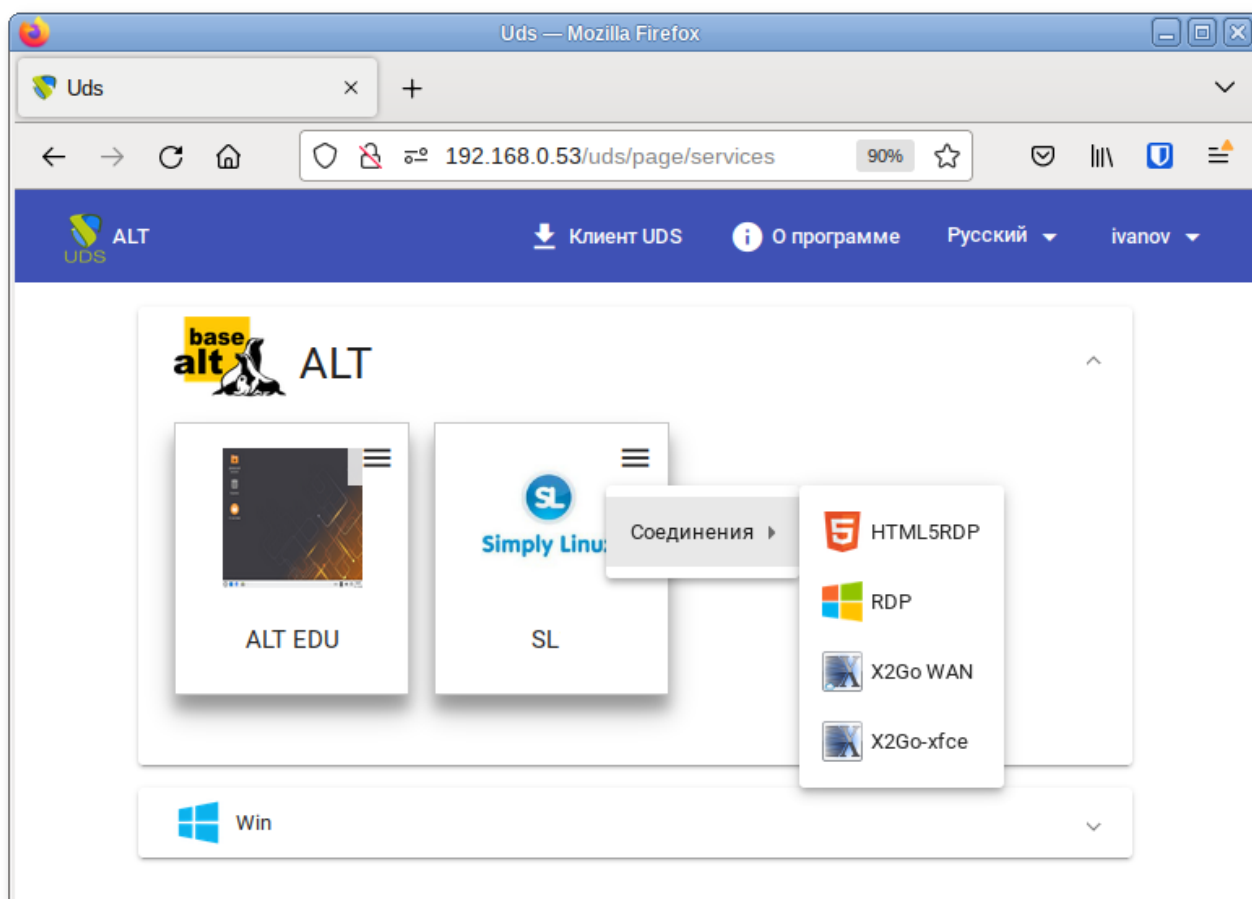
Имя пользователя *
ivanov

Пароль
●●●●●●

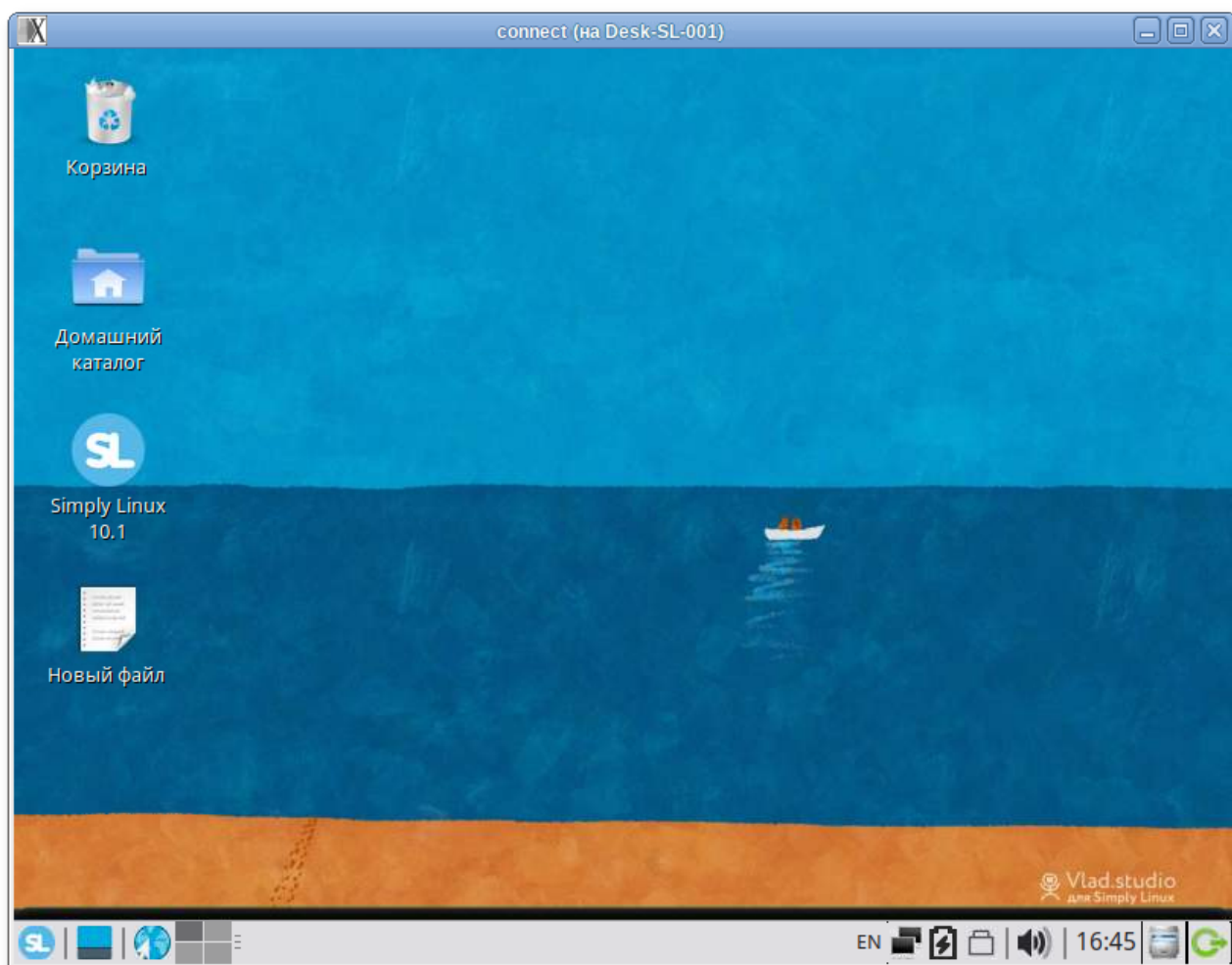
Аутентификатор
ActiveDirectory ▾

Авторизоваться

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



После выбора пула, автоматически стартует OpenUDS Client, который обрабатывает URL, получает необходимые настройки протокола удаленного доступа для предоставленной (свободной) ВМ, формирует файл описания сессии и передает его приложению-клиенту удалённого доступа, которое и устанавливает соединение с указанной ВМ. Как только соединение будет установлено, виртуальный рабочий стол будет доступен для использования.



Примечание

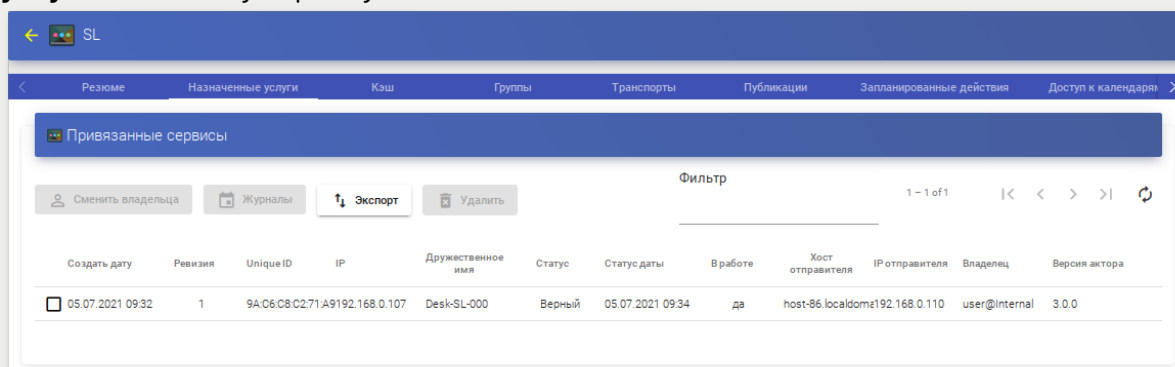
Если для подключения к ВМ настроено более одного типа транспорта, то в правом верхнем углу службы будет отображена кнопка. Если выбрать непосредственно ВМ, будет вызван транспорт по умолчанию (транспорт с меньшим значением в поле приоритет). Для того чтобы использовать другой транспорт, нужно выбрать его в раскрывающемся списке.

По завершении сеанса пользователь ВМ выходит из нее, что приводит к остановке OpenUDS Actor. Брокер OpenUDS считает, что ВМ стала недоступной и, если пул постоянный, то он запускает ВМ, а если пул временный, то происходит удаление файлов ВМ в хранилище и создается новая ВМ из мастер-образа.



Примечание

При подключении пользователя к виртуальному рабочему месту OpenUDS фиксирует доступ и отображает информацию о привязанном сервисе на вкладке **Назначенные услуги** соответствующего пула.



17.7. Отказоустойчивое решение

Компоненты OpenUDS можно настроить в режиме высокой доступности (HA).

Для обеспечения высокой доступности OpenUDS, кроме настройки нескольких OpenUDS Server и Tunnel, необходимо настроить репликацию базы данных. Также следует настроить балансировщик нагрузки, который будет распределять подключения к компонентам OpenUDS Server и Tunnel.

Основные компоненты отказоустойчивого решения OpenUDS:

- Сервер MySQL — база данных (БД) является одним из наиболее существенных компонентов OpenUDS. Поэтому настоятельно рекомендуется иметь резервную копию этого компонента, либо посредством полной резервной копии машины, либо посредством конфигурации активной/пассивной реплики. В данном руководстве описана настройка двух серверов MySQL в режиме активной/пассивной репликации;
- HAProxy-сервер — сервер, отвечающий за распределение подключений к OpenUDS Server и Tunnel. Через него осуществляется доступ пользователей к OpenUDS, и выполняются подключения к различным сервисам. На серверах HAProxy также следует настроить виртуальный IP-адрес, который будет активен только на основном сервере. В случае отказа основного сервера виртуальный IP-адрес будет автоматически активирован на другом сервере HAProxy;
- OpenUDS Server — наличие нескольких машин OpenUDS Server обеспечит непрерывный доступ пользователей к OpenUDS, даже при отказе одного из OpenUDS Server;
- OpenUDS Tunnel — наличие нескольких машин OpenUDS Tunnel позволит получить доступ к службам (рабочим столам или приложениям) через туннелированные соединения и HTML5, даже при отказе одного из OpenUDS Tunnel.



Примечание

Если пользователь подключается к сервису (рабочему столу или приложению) и сервер OpenUDS Tunnel, через который он подключен, падает, соединение будет потеряно. Но при повторном подключении доступ будет автоматически восстановлен через другой активный сервер OpenUDS Tunnel.

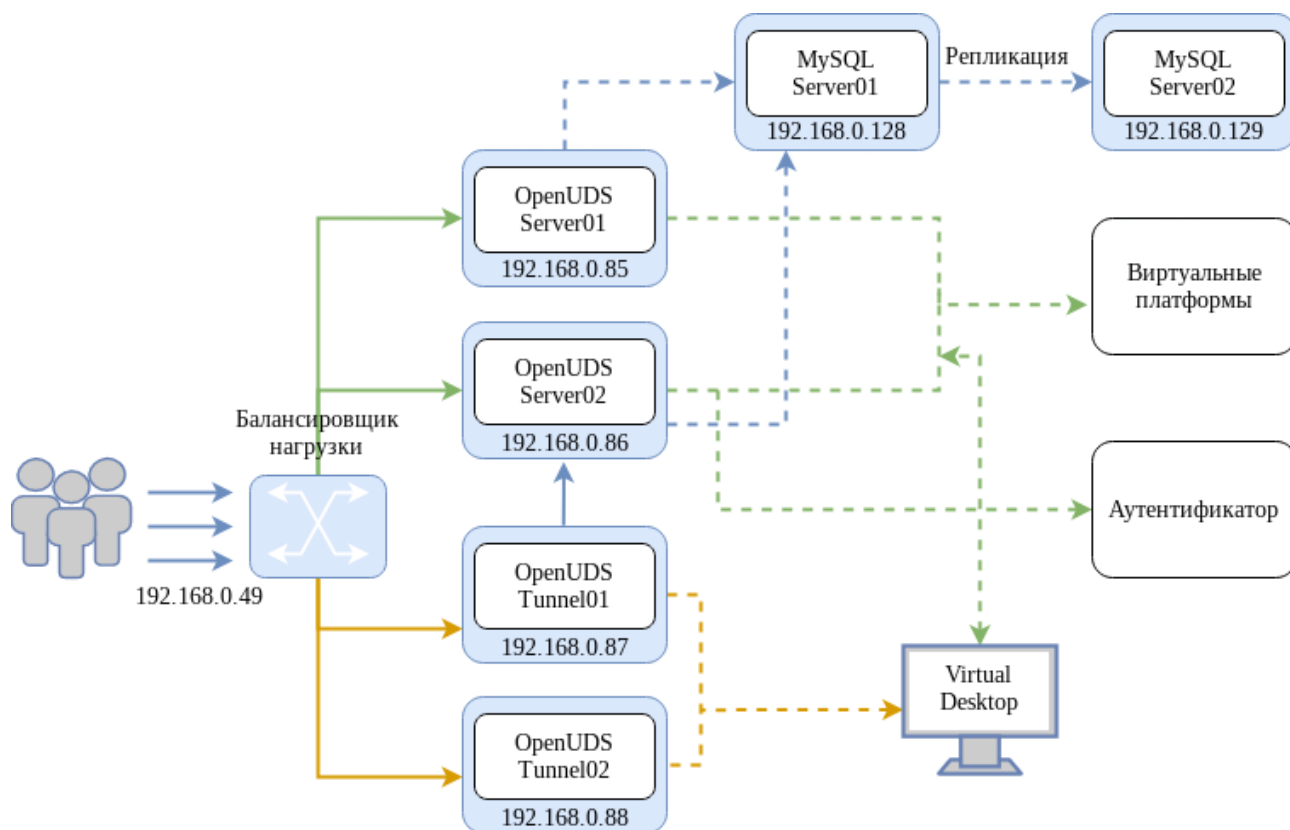


Таблица 17.2. Системные требования

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



Примечание

Для HAProxy необходимо 3 IP-адреса, по одному для каждого сервера (Master-Slave) и общий виртуальный IP-адрес, который будет использоваться для балансировки.

17.7.1. Конфигурация серверов MySQL

На обоих серверах установить MySQL (MariaDB):

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

Запустить сервер MySQL и добавить его в автозагрузку:

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

Задать пароль root и настройки безопасности для MySQL:

```
# mysql_secure_installation
```

17.7.1.1. Настройка репликации между серверами

17.7.1.1.1. Главный узел (Master)

В файле `/etc/my.cnf.d/server.cnf`:

- закомментировать параметр **skip-networking**;
- раскомментировать параметры **server-id** и **log-bin**;
- убедиться, что для параметра **server-id** установлено значение 1;
- раскомментировать параметр **bind-address** и указать IP-адрес сервера (главного):

```
bind-address 192.168.0.128
```

Перезагрузить службу MySQL:

```
# systemctl restart mariadb
```

Создать нового пользователя, с правами которого будет производиться репликация:

1. Войти в консоль MySQL с правами root:

```
$ mysql -p
```

2. Создать пользователя (в примере пользователь «replica» с паролем «uds»):

```
MariaDB [(none)]> CREATE USER 'replica'@'%' IDENTIFIED BY 'uds';  
Query OK, 0 rows affected (0.009 sec)
```

3. Предоставить права **replication slave** пользователю:

```
MariaDB [(none)]>  
GRANT REPLICATION SLAVE ON *.* TO 'replica'@'%' IDENTIFIED BY 'uds';  
Query OK, 0 rows affected (0.002 sec)
```

4. Получить информацию об имени двоичного файла и его позиции:

```
MariaDB [(none)]> SHOW MASTER STATUS\G  
***** 1. row *****  
      File: mysql-bin.000002  
      Position: 328  
      Binlog_Do_DB:  
      Binlog_Ignore_DB:  
      1 row in set (0.001 sec)
```

В данном примере:

- `mysql-bin.000002` — имя файла;
- `328` — позиция двоичного файла.

Эти данные будут необходимы для настройки Slave-сервера.

17.7.1.1.2. Вторичный узел (Slave)

В файле `/etc/my.cnf.d/server.cnf`:

- закомментировать параметр **`skip-networking`**;
- раскомментировать параметры **`server-id`** и **`log-bin`**;
- в параметре **`server-id`** установить значение `2`;
- раскомментировать параметр **`bind-address`** и указать IP-адрес сервера (вторичного):

```
bind-address 192.168.0.129
```

Перезагрузить службу MySQL:

```
# systemctl restart mariadb
```

Настроить параметры, которые вторичный сервер (Slave) будет использовать для подключения к основному серверу (Master):

1. Войти в консоль MySQL с правами root:

```
$ mysql -p
```

2. Остановить репликацию:

```
MariaDB [(none)]> STOP SLAVE;  
Query OK, 0 rows affected, 1 warning (0.001 sec)
```

3. Настроить репликацию между основным сервером и вторичным сервером:

```
MariaDB [(none)]> CHANGE MASTER TO MASTER_HOST='192.168.0.128',  
MASTER_USER='replica', MASTER_PASSWORD='uds', MASTER_LOG_FILE='mysql-bin.  
000002', MASTER_LOG_POS=328;  
Query OK, 0 rows affected (0.020 sec)
```

где:

- `192.168.0.128` — IP-адрес основного сервера;
- `replica` — пользователь, с правами которого будет производиться репликация;
- `uds` — пароль пользователя `replica`;
- `mysql-bin.000002` — имя файла, полученного на предыдущем шаге;
- `328` — позиция двоичного файла.

4. Запустить репликацию:

```
MariaDB [(none)]> START SLAVE;  
Query OK, 0 rows affected (0.001 sec)
```

5. Убедиться, что конфигурация верна:

```
MariaDB [(none)]> SHOW SLAVE STATUS\G  
***** 1. row *****  
Slave_IO_State: Waiting for master to send event  
Master_Host: 192.168.0.128  
Master_User: replica  
Master_Port: 3306  
Connect_Retry: 60  
Master_Log_File: mysql-bin.000004  
Read_Master_Log_Pos: 328  
Relay_Log_File: mysqld-relay-bin.000006  
Relay_Log_Pos: 555  
Relay_Master_Log_File: mysql-bin.000004  
Slave_IO_Running: Yes  
Slave_SQL_Running: Yes  
...
```

IP-адрес основного сервера должен быть указан корректно, параметры **Slave_IO_Running** и **Slave_SQL_Running** должны быть установлены в значение «Yes».

17.7.1.2. Проверка репликации

Для проверки репликации можно создать БД на главном сервере и убедиться, что она автоматически реплицируется на вторичном сервере:

1. Получить доступ к консоли MySQL главного сервера и создать новую тестовую БД «replicatest»:

```
MariaDB [(none)]> CREATE DATABASE replicatest;  
Query OK, 1 row affected (0.001 sec)
```

2. Убедиться, что БД создана:

```
MariaDB [(none)]> SHOW DATABASES;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| mysql |  
| performance_schema |  
| replicatest |  
+-----+  
4 rows in set (0.001 sec)
```

3. Получить доступ к консоли MySQL вторичного сервера и убедиться, что БД, созданная на основном сервере, успешно реплицировалась на этот сервер:

```
MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database           |
+-----+
| information_schema |
| mysql              |
| performance_schema |
| replicatest        |
+-----+
4 rows in set (0.002 sec)
```

4. После проверки работы репликации можно удалить БД «replicatest», выполнив команду на основном сервере:

```
MariaDB [(none)]> DROP DATABASE replicatest;
```

17.7.1.3. Создание БД

Создать на основном сервере БД:

```
$ mysql -p
Enter password:

MariaDB [(none)]> CREATE DATABASE dbuds CHARACTER SET utf8 COLLATE
utf8_general_ci;
MariaDB [(none)]> CREATE USER 'dbuds'@'%' IDENTIFIED BY 'password';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON dbuds.* TO 'dbuds'@'%;
MariaDB [(none)]> FLUSH PRIVILEGES;
MariaDB [(none)]> exit;
```

Подключить серверы OpenUDS к БД основного сервера.

17.7.1.4. Отказ сервера

При недоступности одного из серверов БД необходимо выполнить ряд задач. Задачи, которые следует выполнить, зависят от того к какому серверу (Master или Slave) нет доступа.

17.7.1.4.1. Главный узел (Master)

Если недоступен основной сервер БД (Master), то будет потерян доступ к среде VDI. В этом случае необходимо вручную подключить OpenUDS Server к вторичной БД (Slave), в которой находится вся информация среды VDI до момента падения основной БД. Чтобы настроить новое подключение к БД на OpenUDS Server следует в конфигурационном файле **/var/server/server/settings.py** указать параметры новой БД (это необходимо сделать на всех серверах OpenUDS-Server).

После изменения IP-адреса БД необходимо перезапустить сервер OpenUDS (это необходимо сделать на всех серверах OpenUDS Server). После перезапуска сервера доступ к среде VDI будет восстановлен

Затем необходимо настроить новый сервер для репликации БД. Это можно сделать разными способами, например:

1. Настроить текущий сервер БД как главный и создать новый сервер-реплику, который нужно настроить и восстановить БД из резервной копии с существующими данными (поскольку реплицируются только новые данные).
2. Напрямую сделать резервную копию текущего сервера БД (предварительно остановив все машины OpenUDS Server). Создать новый сервер БД Master, восстановить туда резервную копию БД и перенастроить репликацию.



Примечание

Чтобы не потерять данные, перед применением любого метода перестроения репликации, рекомендуется сделать резервную копию БД. Для получения резервной копии можно использовать следующую команду:

```
# mysqldump -u dbuds -ppassword --databases dbuds > dbuds_dump.sql
```

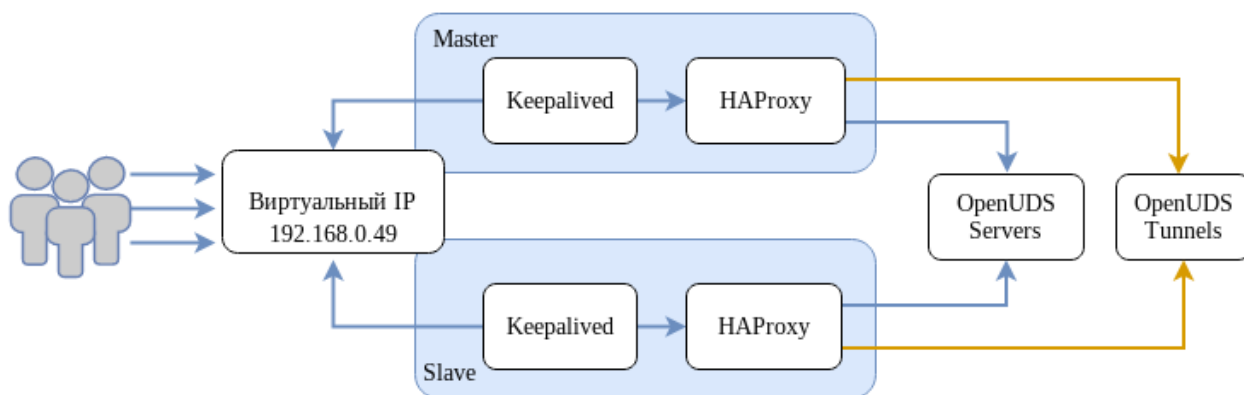
При создании резервной копии все машины OpenUDS Server должны быть выключены. Таким образом, обеспечивается согласованность данных и отсутствие различий в данных между главным и подчиненным серверами перед настройкой реплики.

17.7.1.4.2. Вторичный узел (Slave)

Если недоступен вторичный сервер БД (Slave), доступ к среде VDI сохранится, но будет необходимо перенастроить вторичный сервер-реплику. Перед выполнением данной настройки необходимо восстановить резервную копию с текущим состоянием основной БД, так как будут синхронизированы только новые данные реплики (существующие данные не будут реплицированы в базе данных).

Важно, чтобы во время всего этого процесса машины OpenUDS Server были выключены, чтобы не возникало различий между БД Master и Slave серверов.

17.7.2. Настройка серверов HAProxy



В данной конфигурации используется служба Keepalived и виртуальный IP-адрес, общий для главного (Master) и резервного (Slave) узлов. Служба Keepalived связывает виртуальный IP-адрес с главным узлом и отслеживает доступность HAProxy. Если служба обнаруживает, что HAProxy не отвечает, то она связывает виртуальный адрес с вспомогательным узлом, что минимизирует время недоступности сервера. Пользователи при обращении к OpenUDS должны использовать этот виртуальный IP-адрес. Этот же виртуальный IP-адрес следует использовать при регистрации OpenUDS Actor (см. [Подготовка шаблона виртуальной машины](#)).

На основном узле сгенерировать сертификат:

```
# openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout /root/ssl.key -out /root/ssl.crt
```

Создать файл .pem, выполнив команду (предварительно может понадобиться создать каталог **/etc/openssl/private**):

```
# cat /root/ssl.crt /root/ssl.key > /etc/openssl/private/haproxy.pem
```



Примечание

Сертификат, созданный на первичном сервере HAProxy, необходимо скопировать в каталог **/etc/openssl/private** на вторичном сервере. Если используется собственный сертификат, его необходимо скопировать на оба сервера (основной и дополнительный).



Важно

Порты, используемые HAProxy (в примере 80, 443, 1443, 10443), должны быть свободны.

На обоих узлах:

1. Установить пакеты *haproxy* и *keepalived*:

```
# apt-get install haproxy keepalived
```

2. Заменить содержимое файла **/etc/haproxy/haproxy.cfg** следующим:

```
global
    log /dev/log      local0
    log /dev/log      local1 notice
    chroot /var/lib/haproxy
    stats socket /var/lib/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    maxconn 2048
    user _haproxy
    group _haproxy
    daemon

    # Default SSL material locations
    # ca-base /etc/openssl/certs
    # crt-base /etc/openssl/private

    # Default ciphers to use on SSL-enabled listening sockets.
```

```

# For more information, see ciphers(1SSL). This list is from:
# https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/
# ssl-default-bind-options ssl-min-ver TLSv1.2 prefer-client-ciphers
# ssl-default-bind-ciphersuites
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
ssl-default-bind-ciphers
ECDH+AESGCM:ECDH+CHACHA20:ECDH+AES256:ECDH+AES128:!aNULL:!SHA1:!AESCCM

# ssl-default-server-options ssl-min-ver TLSv1.2
# ssl-default-server-ciphersuites
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
# ssl-default-server-ciphers
ECDH+AESGCM:ECDH+CHACHA20:ECDH+AES256:ECDH+AES128:!aNULL:!SHA1:!AESCCM

tune.ssl.default-dh-param 2048

```

defaults

```

log      global
mode     http
option   httplog
option   dontlognull
option   forwardfor
retries  3
option   redispatch

stats enable
stats uri /haproxy.stats
stats realm Strictly\ Private
stats auth stats:haproxy.stats

timeout connect 5000
timeout client  50000
timeout server  50000

```

frontend http-in

```

bind *:80
mode http
http-request set-header X-Forwarded-Proto http
default_backend openuds-backend

```

frontend https-in

```

bind *:443 ssl crt /etc/openssl/private/haproxy.pem
mode http
http-request set-header X-Forwarded-Proto https
default_backend openuds-backend

```

frontend tunnel-in

```

bind *:1443
mode tcp
option tcplog
default_backend tunnel-backend-ssl

```

frontend tunnel-in-guacamole # HTML5

```

bind *:10443
mode tcp
option tcplog
default_backend tunnel-backend-guacamole

```

backend openuds-backend

```

option http-keep-alive

```

```

        balance roundrobin
        server udss1 192.168.0.85:80 check inter 2000 rise 2 fall 5
        server udss2 192.168.0.86:80 check inter 2000 rise 2 fall 5
backend tunnel-backend-ssl
    mode tcp
    option tcplog
    balance roundrobin
    server udst1 192.168.0.87:7777 check inter 2000 rise 2 fall 5
    server udst2 192.168.0.88:7777 check inter 2000 rise 2 fall 5

backend tunnel-backend-guacamole
    mode tcp
    option tcplog
    balance source
    server udstg1 192.168.0.87:10443 check inter 2000 rise 2 fall 5
    server udstg2 192.168.0.88:10443 check inter 2000 rise 2 fall 5

```

3. Включить в ядре поддержку двух IP-адресов:

```

# echo "net.ipv4.ip_nonlocal_bind = 1" >> /etc/sysctl.conf
# sysctl -p

```

4. Настроить службу Keepalived. Для этого создать файл **/etc/keepalived/keepalived.conf**. Содержимое файла зависит от узла, который настраивается:

■ на главном узле:

```

global_defs {
    # Keepalived process identifier
    lvs_id haproxy_DH
}
# Script used to check if HAProxy is running
vrrp_script check_haproxy {
    script "killall -0 haproxy"
    interval 2
    weight 2
}
# Виртуальный интерфейс
# The priority specifies the order in which the assigned interface to
take over in a failover
vrrp_instance VI_01 {
    state MASTER
    interface enp0s3
    virtual_router_id 51
    priority 101
    # Виртуальный IP-адрес
    virtual_ipaddress {
        192.168.0.49
    }
    track_script {
        check_haproxy
    }
}

```

где enp0s3 — интерфейс, для виртуального IP (узнать имя сетевого интерфейса можно, выполнив команду **ip a**).

■ на вспомогательном узле:

```
global_defs {
    # Keepalived process identifier
    lvs_id haproxy_DH_passive
}
# Script used to check if HAProxy is running
vrrp_script check_haproxy {
    script "killall -0 haproxy"
    interval 2
    weight 2
}
# Виртуальный интерфейс
# The priority specifies the order in which the assigned interface to
# take over in a failover
vrrp_instance VI_01 {
    state SLAVE
    interface eth0
    virtual_router_id 51
    priority 100
    # Виртуальный IP-адрес
    virtual_ipaddress {
        192.168.0.49
    }
    track_script {
        check_haproxy
    }
}
```

где eth0 — интерфейс, для виртуального IP (узнать имя сетевого интерфейса можно, выполнив команду **ip a**).

5. Запустить службы haproxy и keepalived:

```
# systemctl enable --now haproxy
# systemctl enable --now keepalived
```

6. Убедиться, что виртуальный IP активен на основном сервере:

```
$ ip a |grep enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
    inet 192.168.0.52/24 brd 192.168.0.255 scope global noprefixroute enp0s3
    inet 192.168.0.49/32 scope global enp0s3
```

17.7.3. Настройка OpenUDS

После настройки серверов MySQL и HAProxy можно приступить к установке и настройке компонентов OpenUDS Server и Tunnel.

17.7.3.1. Настройка OpenUDS Server

На обоих узлах OpenUDS Server:

1. Установить OpenUDS Server:

```
# apt-get install openuds-server-nginx
```

2. Отредактировать содержимое файла **/etc/openuds/settings.py**, указав корректные данные для подключения к главному MySQL-серверу:

```
DATABASES = {
    'default': {
        'ENGINE': 'django.db.backends.mysql',
        'OPTIONS': {
            'isolation_level': 'read committed',
        },
        'NAME': 'dbuds', # Or path to database file if using sqlite3.
        'USER': 'dbuds', # Not used with sqlite3.
        'PASSWORD': 'password', # Not used with sqlite3.
        'HOST': '192.168.0.128', # Set to empty string for localhost. Not
used with sqlite3.
        'PORT': '3306', # Set to empty string for default. Not used with
sqlite3.
    }
}
```

3. Заполнить базу данных начальными данными (этот пункт следует выполнить только на одном узле!):

```
# su -s /bin/bash - openuds
$ cd /usr/share/openuds
$ python3 manage.py migrate
$ exit
```

4. Запустить gunicorn:

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

5. Запустить nginx:

```
# ln -s ../sites-available.d/openuds.conf /etc/nginx/sites-enabled.d/
openuds.conf
# systemctl enable --now nginx.service
```

6. Запустить менеджер задач OpenUDS:

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

7. Подключиться к серверу OpenUDS (http://Виртуальный_IP-адрес).

17.7.3.2. Настройка OpenUDS Tunnel

На каждом узле OpenUDS Tunnel:

1. Установить OpenUDS Tunnel:

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

2. Настроить туннель:

- указать виртуальный IP-адрес в файле **/etc/openuds-tunnel/udstunnel.conf** :

```
uds_server = http://192.168.0.49/uds/rest/tunnel/ticket
uds_token = 5ba9d52bb381196c2a22e495ff1c9ba4bdc03440b726aa8b
```

- запустить и добавить в автозагрузку сервис OpenUDS Tunnel:

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

3. Настроить HTML5:

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

```
uds-base-url=http://192.168.0.49/uds/guacamole/auth/
5ba9d52bb381196c2a22e495ff1c9ba4bdc03440b726aa8b
```

где 192.168.0.49 — виртуальный IP-адрес;

- настроить tomcat, для этого в файл **/etc/tomcat/server.xml** добавить новый Connector, в котором указать порт (в примере 10443), сертификат (файл .crt, .pem и т.д.), закрытый ключ (.key, .pem и т.д.):

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

- запустить сервисы guacd и tomcat:

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

На главном узле (Master) MySQL добавить в БД информацию о каждом OpenUDS Tunnel:

```
INSERT INTO `uds_tunneltoken` VALUES (ID,'автор добавления','IP-адрес
туннеля','IP-адрес туннеля'
'название туннеля','Токен из файла udstunnel.conf','дата добавления');
```

Например:

```
# mysql -u root -p
MariaDB> USE dbuds;
MariaDB> INSERT INTO `uds_tunneltoken` VALUES
(ID,'admin','192.168.0.87','192.168.0.87','Tunnel','5ba9d52bb381196c2a22e495ff1c9
ba4bdc03440b726aa8b','2022-11-15');
MariaDB> INSERT INTO `uds_tunneltoken` VALUES
(ID,'admin','192.168.0.88','192.168.0.88','Tunnel','9ba4bdc03440b726aa8b5ba9d52bb
381196c2a22e495ff1c','2022-11-15');
MariaDB> exit;
```

Оба сервера OpenUDS-Tunnel будут работать в активном режиме. Пользователи, использующие подключение через туннель, будут подключаться к этим серверам случайным образом. При падении одного из серверов, соединения пользователей, которые используют этот сервер, будут прерваны, но при повторном установлении соединения они автоматически получают доступ через другой активный туннельный сервер.



Примечание

При создании туннельного транспорта (X2Go, RDP) в поле **Туннельный сервер** (вкладка **Туннель**) следует указывать виртуальный IP-адрес и порт, указанный в разделе **frontend tunnel-in** файла `/etc/haproxy/haproxy.cfg` (в данном примере: 1443):

Новый транспорт

<ОсновнойТуннельУчётные данныеПар: >

Туннельный сервер
192.168.0.49:1443

Время ожидания туннеля *
30

Принудительная проверка SSL-сертификата
☐ Нет

Отменить и закрыть

Сохранить

При создании транспорта «HTML5 RDP (туннельный)» в поле **Туннельный сервер** (вкладка **Туннель**) следует указывать виртуальный IP-адрес и порт, указанный в разделе **frontend tunnel-in-guacamole** файла `/etc/haproxy/haproxy.cfg` (в данном примере: 10443):

Новый транспорт

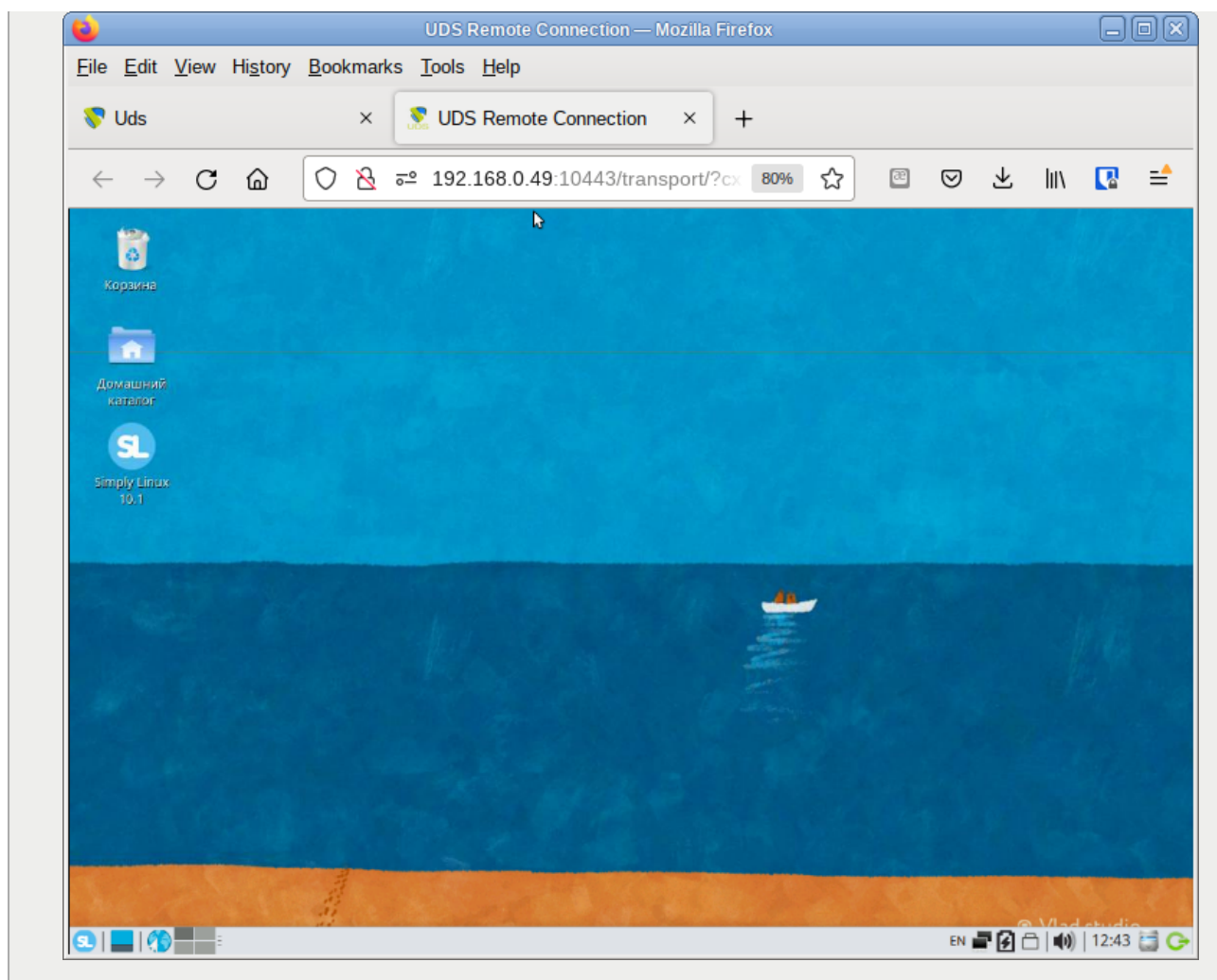
<ОсновнойТуннельУчётные данныеПараметры>

Туннельный сервер *
http://192.168.0.49:10443

Отменить и закрыть

Сохранить

Пример подключения с использованием HTML5:



Глава 18. Система мониторинга Zabbix

- 18.1. Установка сервера PostgreSQL
- 18.2. Установка Apache2
- 18.3. Установка PHP
- 18.4. Настройка и запуск Zabbix-сервера
- 18.5. Установка веб-интерфейса Zabbix
- 18.6. Установка клиента Zabbix
- 18.7. Добавление нового хоста на сервер Zabbix
- 18.8. Авторегистрация узлов

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

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

18.1. 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 postgresql14-server zabbix-server-pgsql fping
```

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:

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

■ 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'  
# systemctl restart postgresql
```

■ 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 создаётся база 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'
```

18.2. Установка Apache2

Установить пакеты apache2:

```
# apt-get install apache2 apache2-mod_php8.0
```

Добавить в автозапуск и запустить apache2:

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

18.3. Установка PHP



Примечание

Начиная с версии php8.0, пакеты модулей именуются следующим образом:

```
php<мажорная>.<минорная версии>-<имя модуля>
```

Из репозитория можно установить и эксплуатировать в одной системе одновременно разные версии php. В данном руководстве в качестве примера используется php8.0.

Установить необходимые пакеты:

```
# apt-get install php8.0 php8.0-mbstring php8.0-sockets php8.0-gd php8.0-xmlreader php8.0-pgsql php8.0-ldap php8.0-openssl
```

Изменить некоторые опции php в файле `/etc/php/8.0/apache2-mod_php/php.ini`:

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

Перезапустить apache2:

```
# systemctl restart httpd2
```

18.4. Настройка и запуск Zabbix-сервера

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

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

Добавить Zabbix-сервер в автозапуск и запустить его:

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

18.5. Установка веб-интерфейса Zabbix

Установить метапакет (из репозитория):

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

Включить аддоны в apache2:

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

Перезапустить apache2:

```
# systemctl restart httpd2
```

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

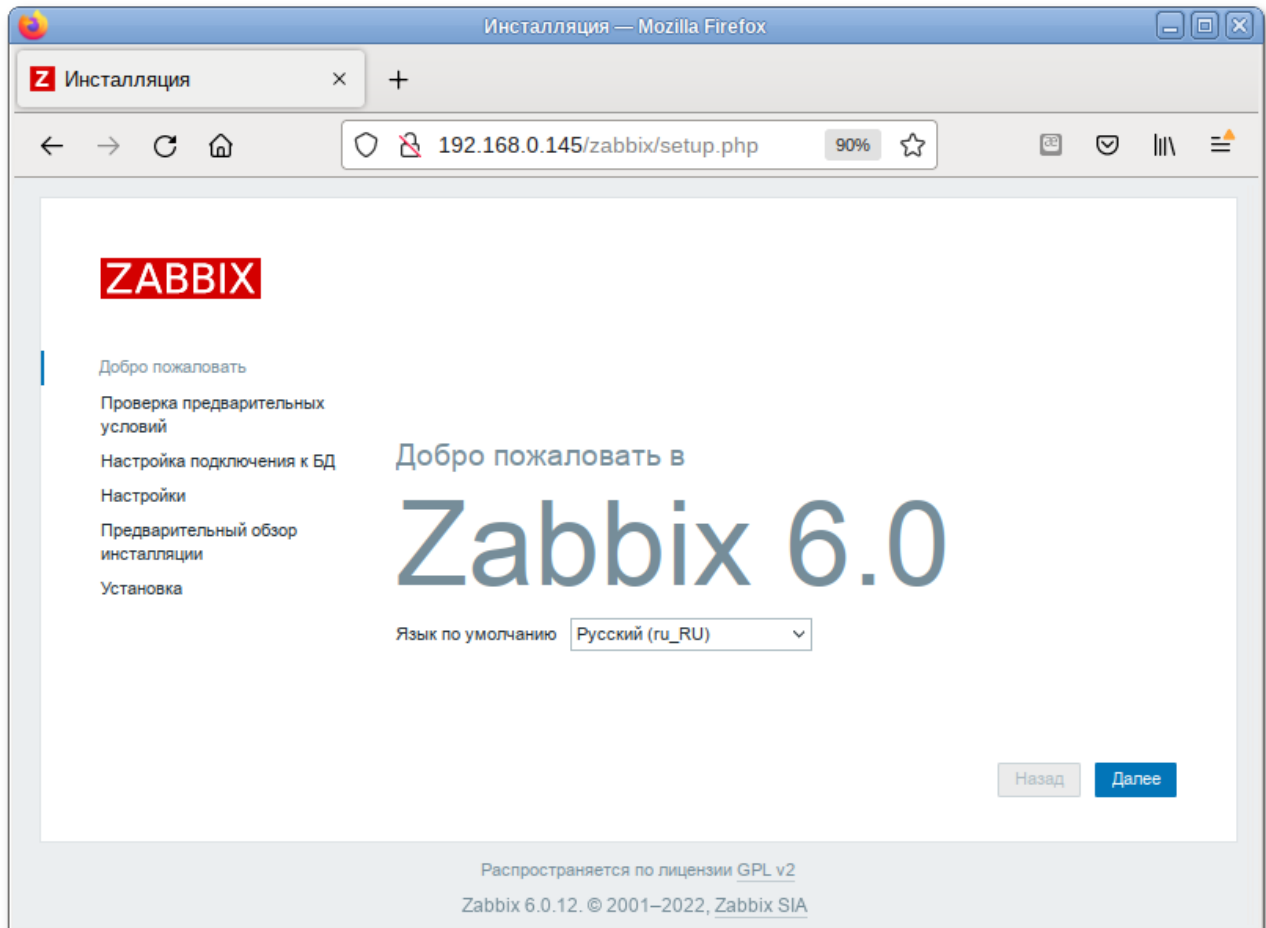
```
# chown apache2:apache2 /var/www/webapps/zabbix/ui/conf
```

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.





Примечание

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

```
Require all granted
```

и перезапустить `apache2`:

```
# systemctl restart httpd2
```

Для начала установки необходимо нажать кнопку **Далее**, что осуществит переход на страницу проверки предварительных условий.

ZABBIX

Проверка предварительных условий

	Текущее значение	Требуется	
Версия PHP	8.0.27	7.2.5	ОК
PHP опция "memory_limit"	256M	128M	ОК
PHP опция "post_max_size"	32M	16M	ОК
PHP опция "upload_max_filesize"	20M	2M	ОК
PHP опция "max_execution_time"	600	300	ОК
PHP опция "max_input_time"	600	300	ОК
Поддержка баз данных PHP	PostgreSQL		ОК
PHP bcmath	в		ОК
PHP mbstring	в		ОК
PHP опция "mbstring.func_overload"	выкл	выкл	ОК

[Назад](#) [Далее](#)

Распространяется по лицензии [GPL v2](#)
Zabbix 6.0.12. © 2001–2022, Zabbix SIA

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*.

Инсталляция — Mozilla Firefox

Инсталляция

192.168.0.145/zabbix/setup.php 90%

ZABBIX

Настройка подключения к БД

Пожалуйста, создайте базу данных вручную и укажите параметры конфигурации для соединения с этой базой. Нажмите кнопку "Далее" при завершении.

Добро пожаловать

Проверка предварительных условий

Настройка подключения к БД

Настройки

Предварительный обзор инсталляции

Установка

Тип базы данных PostgreSQL

Хост базы данных localhost

Порт базы данных 0 0 - использовать порт по умолчанию

Имя базы данных zabbix

Схема базы данных public

Хранение учётных данных в Простой текст HashiCorp Vault

Пользователь zabbix

Пароль

TLS шифрование базы данных ☐

Назад Далее

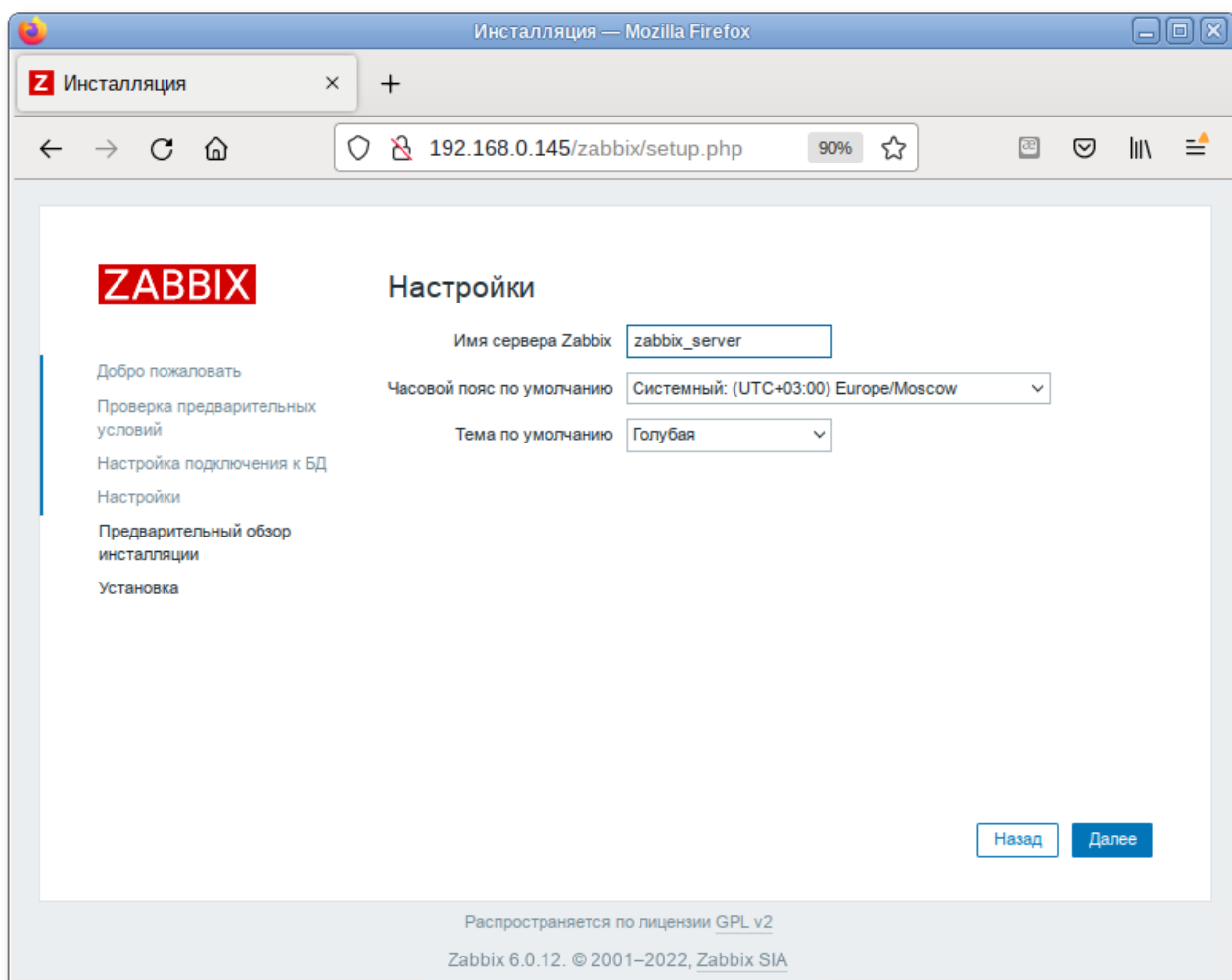
Распространяется по лицензии [GPL v2](#)
Zabbix 6.0.12. © 2001–2022, [Zabbix SIA](#)



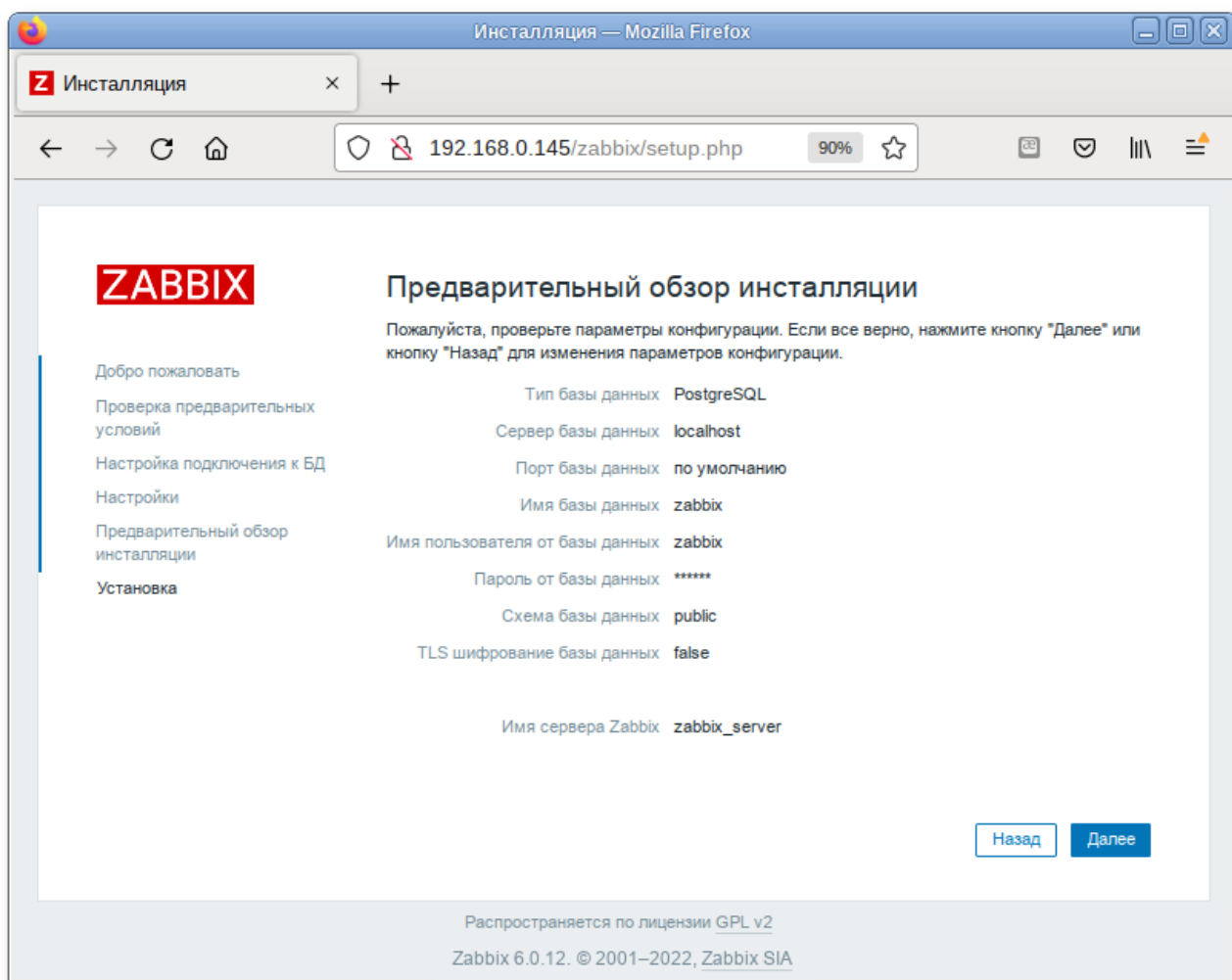
Примечание

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

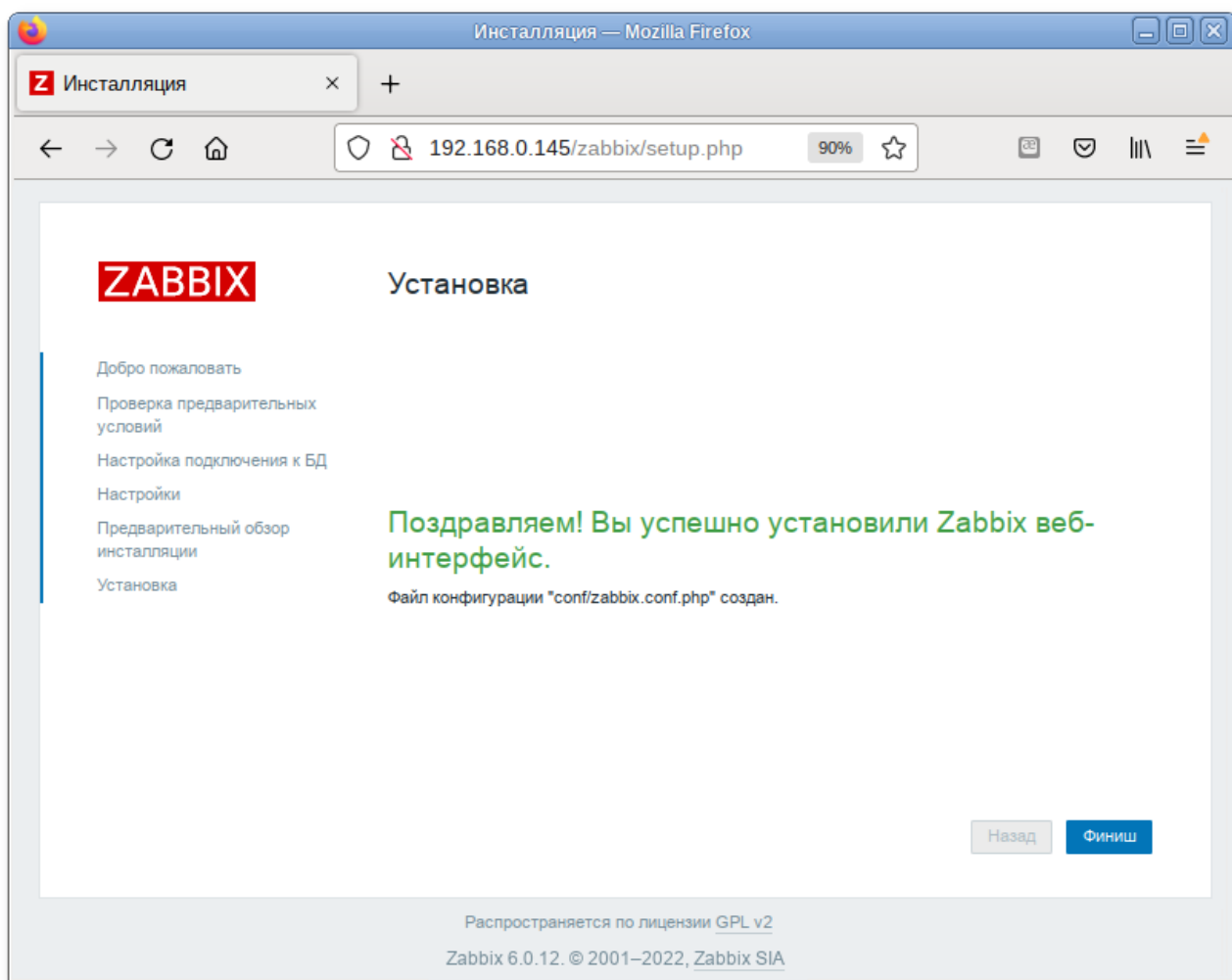
Далее необходимо задать имя сервера и выбрать настройки веб-интерфейса:



На следующей странице следует проверить параметры конфигурации:

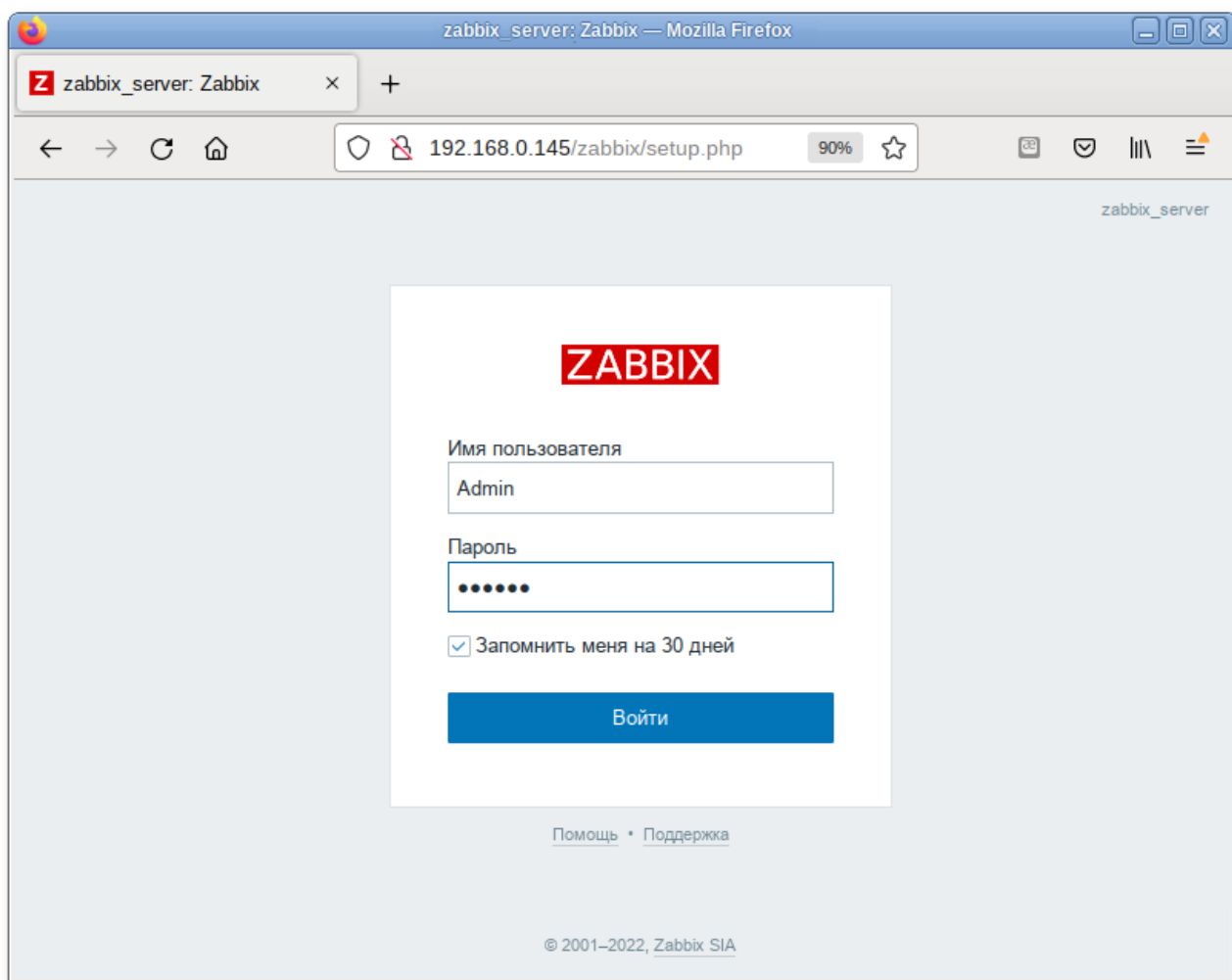


Окончание установки:

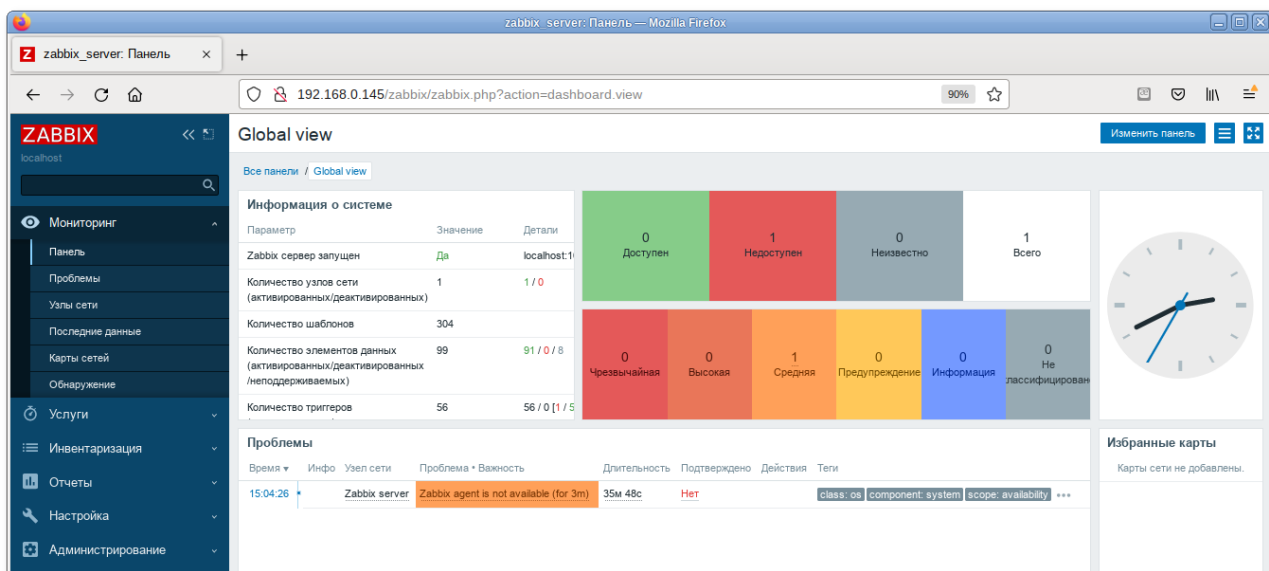


После окончания установки на экране будет отображаться форма входа в интерфейс управления системой мониторинга. Параметры доступа по умолчанию:

Логин: Admin
Пароль: zabbix



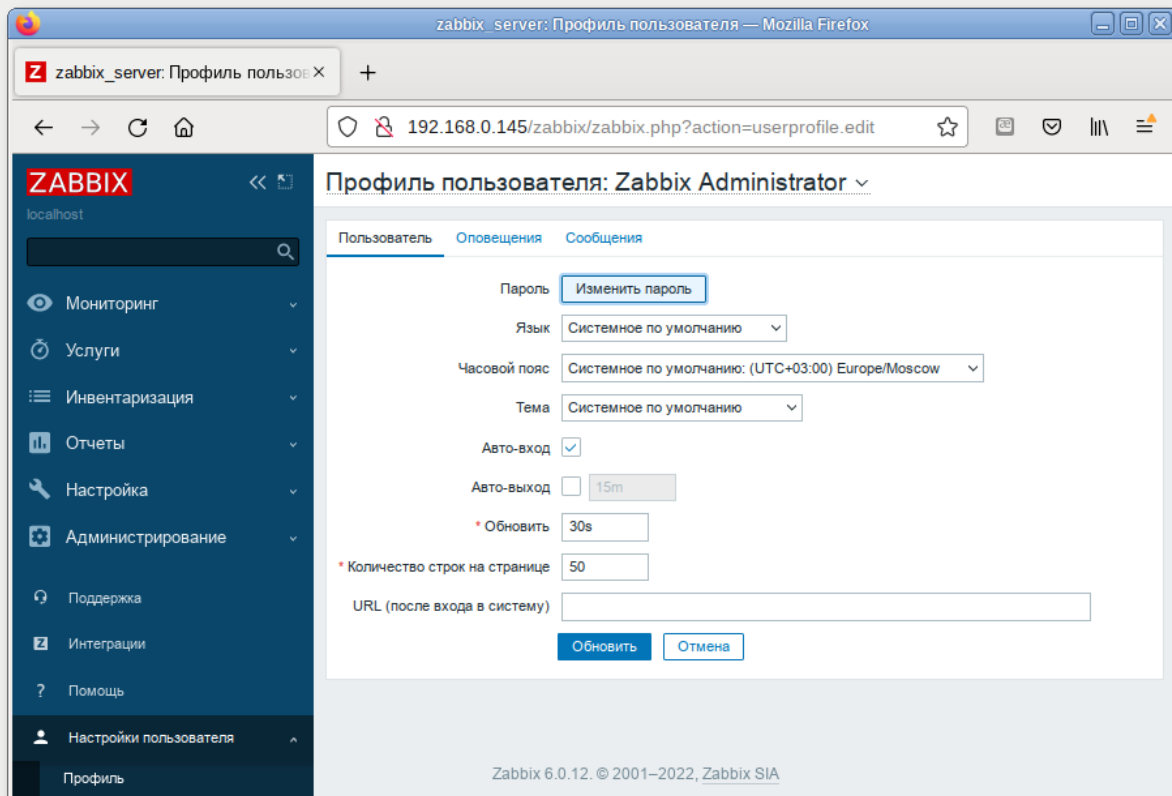
Войдя в систему, нужно сменить пароль пользователя, завести других пользователей и можно начать настраивать Zabbix.





Примечание

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



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

18.6. 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.



Примечание

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

Добавить Zabbix-агент в автозапуск и запустить его:

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



Примечание

Для настройки Zabbix-агента можно воспользоваться модулем [Агент наблюдения](#).

18.7. 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**:

The screenshot shows the Zabbix web interface in the 'Hosts' (Узлы сети) section. The 'Create host' (Создать узел сети) button is highlighted with a red box. The page includes search filters, a form to add a new host, and a table of existing hosts.

Имя	Элементы данных	Триггеры	Графики	Обнаружение	Веб	Интерфейс	Прокси	Шаблоны	Состояние	Доступность	Шифрование агента	Инфо	Теги
Zabbix server	Элементы данных 99	Триггеры 58	Графики 19	Обнаружение 4	Веб	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Активировано	25%	Нет		

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

Новый узел сети

Узел сети IPMI Теги Макросы Инвентаризация Шифрование Преобразование значений

* Имя узла сети comp01.example.test

Видимое имя HostW

Шаблоны Linux by Zabbix agent X Выбрать
начните печатать для поиска

* Группы Discovered hosts X Выбрать
начните печатать для поиска

Интерфейсы Тип IP адрес DNS имя Подключаться через Порт По умолчанию

Агент 192.168.0.118 IP DNS 10050 Удалить

Добавить

Описание

Наблюдение через прокси (без прокси) v

Добавить Отмена



Примечание

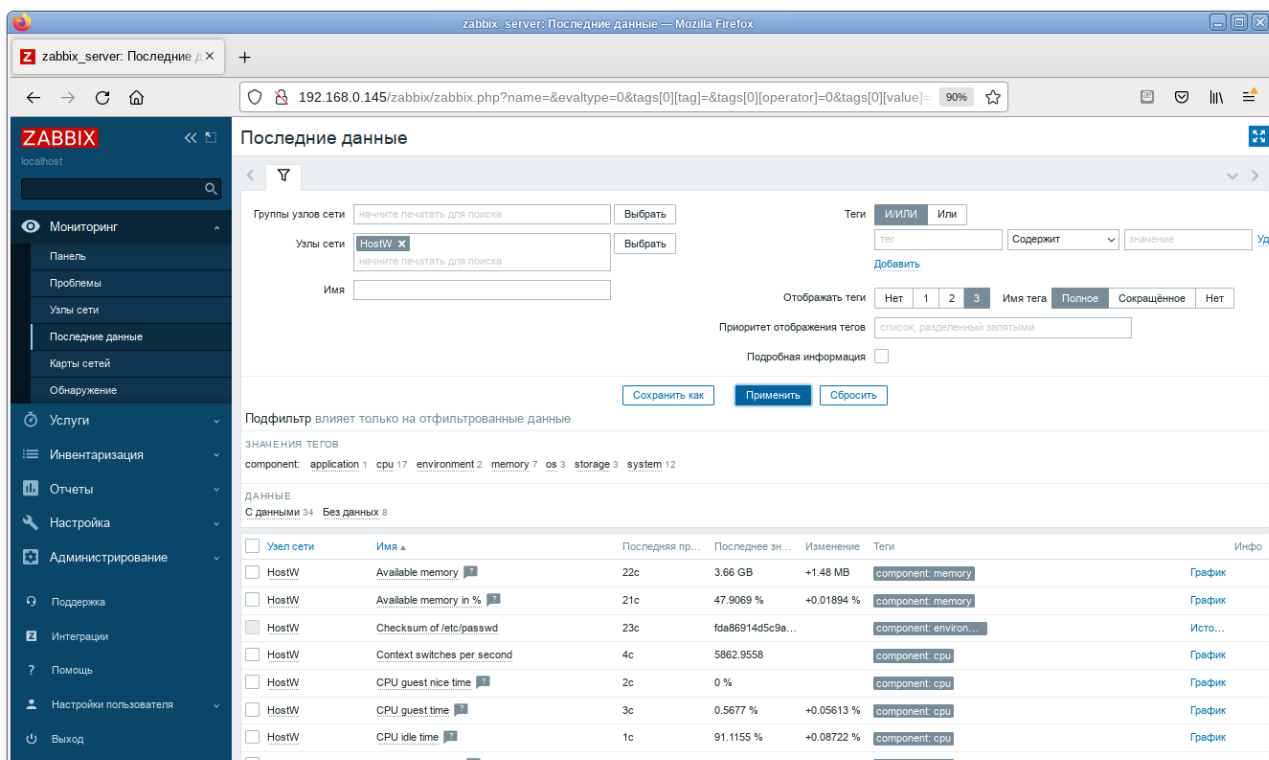
В поле **Имя узла сети** ставится значение, которое указано в настройках агента (/etc/zabbix/zabbix_agentd.conf) в поле **Hostname**.



Примечание

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

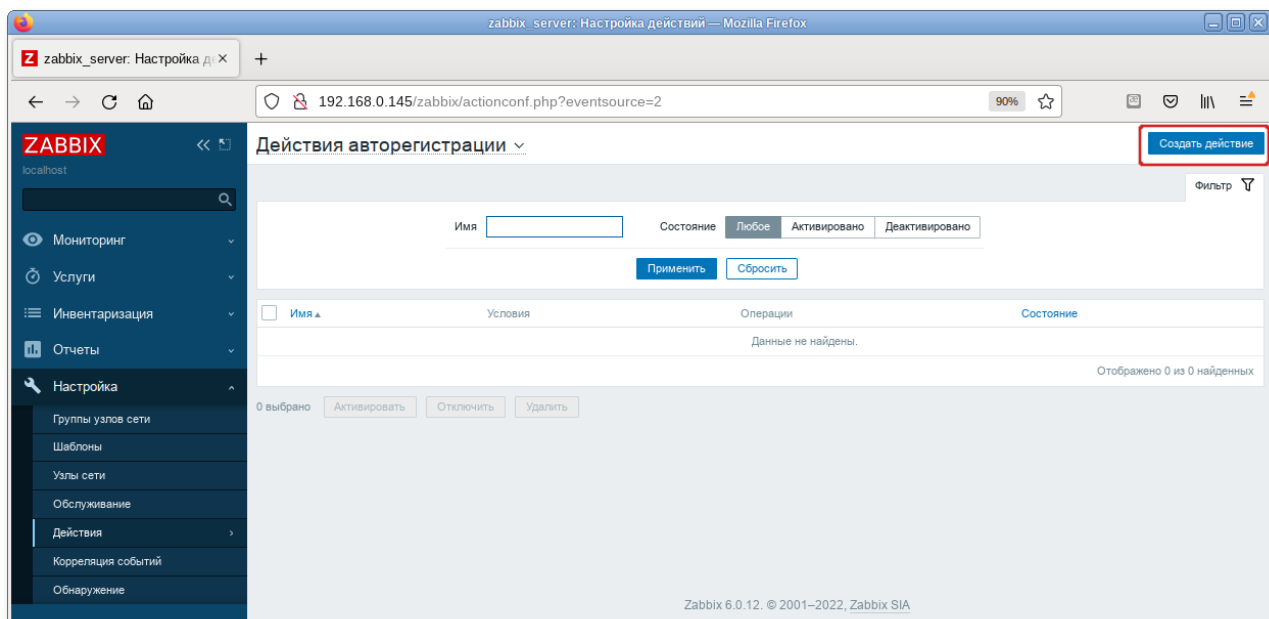
Получение первых данных может занять до 60 секунд. Для того чтобы просмотреть собранные данные необходимо перейти в **Мониторинг** → **Последние данные**, выбрать в фильтре нужный узел сети и нажать кнопку **Применить**:



18.8. 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 hosts:

Действие

Операции

Имя

Авторегистрация

Условия

Подпись	Имя	Действие
А	Метаданные узлов сети содержит <i>alt.autoreg</i>	Удалить

Добавить

Активировано

☒

Должна существовать по крайней мере одна операция.

Добавить

Отмена

На вкладке **Операции** в поле **Операции** следует добавить правила, которые необходимо применить при регистрации хоста. Например, для добавления узла, добавления его к группе **Discovered hosts** с присоединением к шаблону **Linux by Zabbix agent** правила выглядят так:

Действие

Операции 3

Операции

Детали	Действие
Добавить узел сети	Изменить Удалить
Добавить в группы узлов сети: Discovered hosts	Изменить Удалить
Присоединить к шаблону: Linux by Zabbix agent	Изменить Удалить

Добавить

Должна существовать по крайней мере одна операция.

Добавить

Отмена

В конфигурационном файле агента указать следующие значения:

- в параметре **Hostname** — уникальное имя;
- в параметре **ServerActive** — IP-адрес сервера;
- в параметре **HostMetadata** — значение, которое было указано в настройках сервера (HostMetadata=alt.autoreg).

Перезапустить агент.

Глава 19. Сервер видеоконференций на базе Jitsi Meet

19.1. Требования к системе

19.2. Установка

19.3. Конфигурация

19.4. Работа с сервисом

19.5. Отключение возможности неавторизованного создания новых конференций

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

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

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

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

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

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

19.1. Требования к системе

Для размещения нужны:

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



Примечание

Теоретически компоненты могут размещаться на разных машинах; на практике не рекомендуется устанавливать prosody и jicofo на разные машины — это может привести к низкой производительности сервиса и большим колебаниям задержки связи.

19.2. Установка

Установить пакеты:

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




Примечание

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

19.3. Конфигурация

19.3.1. Настройка имени хоста системы

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

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

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

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



Примечание

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

Проверить правильность установленного имени можно, выполнив команды:

```
# hostname
jitsi2
# hostname -f
jitsi2.test.alt
$ ping "${hostname}"
PING jitsi2.test.alt (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.053 ms
[...]
```

19.3.2. 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 содержанием:

```

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
```

19.3.3. Настройка jicofo

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

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

```
# Jitsi Conference Focus settings  
# sets the host name of the XMPP server  
JICOFO_HOST=localhost  
  
# sets the XMPP domain (default: none)  
JICOFO_HOSTNAME=jitsi2.test.alt  
  
# sets the secret used to authenticate as an XMPP component  
JICOFO_SECRET=secret1  
  
# overrides the prefix for the XMPP component domain. Default: "focus"  
#JICOFO_FOCUS_SUBDOMAIN=focus  
  
# sets the port to use for the XMPP component connection  
JICOFO_PORT=5347  
  
# sets the XMPP domain name to use for XMPP user logins  
JICOFO_AUTH_DOMAIN=auth.jitsi2.test.alt
```

```
# sets the username to use for XMPP user logins
JICOFO_AUTH_USER=focus

# sets the password to use for XMPP user logins
JICOFO_AUTH_PASSWORD=secret2

# extra options to pass to the jicofo daemon
JICOFO_OPTS="${JICOFO_FOCUS_SUBDOMAIN:+ --subdomain=$JICOFO_FOCUS_SUBDOMAIN}"

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



Важно

В строке

```
JICOFO_SECRET=secret1
```

должен быть указан пароль, установленный в файле
/etc/prosody/conf.d/jitsi2.test.alt.cfg.lua.

В строке

```
JICOFO_AUTH_PASSWORD=secret2
```

должен быть указан пароль пользователя focus.

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

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

Запустите jicofo:

```
# systemctl start jicofo
```

Убедитесь, что jicofo подключается к XMPP-серверу:

```
# curl -i localhost:8888/about/health
HTTP/1.1 500 Internal Server Error
Date: 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.

19.3.4. Настройка jitsi-videobridge

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

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

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

```
# Jitsi Videobridge settings

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

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

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

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

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



Важно

В строке

```
password = "secret3"
```

должен быть указан пароль пользователя jvb.

Вместо слова shard можно использовать любой идентификатор (оно идентифицирует подключение к xmpp-серверу и jicofo).

Измените содержимое файла **/etc/jitsi/videobridge/sip-communicator.properties**:

```
org.ice4j.ice.harvest.DISABLE_AWS_HARVESTER=true
org.ice4j.ice.harvest.STUN_MAPPING_HARVESTER_ADDRESSES=meet-jit-si-
turnrelay.jitsi.net:443
org.jitsi.videobridge.ENABLE_STATISTICS=true
org.jitsi.videobridge.STATISTICS_TRANSPORT=muc
org.jitsi.videobridge.xmpp.user.shard.HOSTNAME=localhost
org.jitsi.videobridge.xmpp.user.shard.DOMAIN=auth.jitsi2.test.alt
org.jitsi.videobridge.xmpp.user.shard.USERNAME=jvb
org.jitsi.videobridge.xmpp.user.shard.PASSWORD=secret3
org.jitsi.videobridge.xmpp.user.shard.MUC_JIDS=JvbBrewery@internal.auth.jitsi2.te
st.alt
org.jitsi.videobridge.xmpp.user.shard.MUC_NICKNAME=6d8b40cb-fe32-49f5-
a5f6-13d2c3f95bba
```



Примечание

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

Запустите JVB:

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

Убедитесь, что между JVB и jicofo есть связь:

```
# curl -i localhost:8888/about/health
HTTP/1.1 200 OK
Date: 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.

19.3.5. Настройка веб-приложения Jitsi Meet

Получить SSL/TLS-сертификат для домена.



Примечание

Можно создать сертификат без обращения к УЦ. При использовании такого сертификата в браузере будут выводиться предупреждения.

Для создания самоподписанного сертификата следует:

►создать корневой ключ:

```
# openssl genrsa -out rootCA.key 2048
```

►создать корневой сертификат:

```
# openssl req -x509 -new -key rootCA.key -days 10000 -out rootCA.crt -  
subj "/C=RU/ST=Russia/L=Moscow/CN=SuperPlat CA Root"
```

►сгенерировать ключ:

```
# openssl genrsa -out jitsi2.test.alt.key 2048
```

►создать запрос на сертификат (тут важно указать имя сервера: домен или IP):

```
# openssl req -new -key jitsi2.test.alt.key -out jitsi2.test.alt.csr -  
subj "/C=RU/L=Moscow/CN=jitsi2.test.alt"
```

►подписать запрос на сертификат корневым сертификатом:

```
# openssl x509 -req -in jitsi2.test.alt.csr -CA rootCA.crt -CAkey  
rootCA.key -CAcreateserial -out jitsi2.test.alt.crt -days 5000  
Signature ok  
subject=C = RU, CN = jitsi2.test.alt  
Getting CA Private Key
```

Положить ключ и сертификат в папку **/etc/jitsi/meet/**:

```
# cp jitsi2.test.alt.crt /etc/jitsi/meet/  
# cp jitsi2.test.alt.key /etc/jitsi/meet/
```

В пакете *jitsi-meet-web-config* есть примеры конфигурации для веб-клиента (*.config.js) и веб-сервера (*.example.apache, *.example).

Создать файл **/etc/jitsi/meet/jitsi2.test.alt-config.js** на основе **/usr/share/jitsi-meet-web-config/config.js**:

```
# cp /usr/share/jitsi-meet-web-config/config.js /etc/jitsi/meet/jitsi2.test.alt-  
config.js
```

Внести изменения в файл **/etc/jitsi/meet/jitsi2.test.alt-config.js** в соответствии с настройками серверной части:

```

var config = {
  // Connection
  //

  hosts: {
    // XMPP domain.
    domain: 'jitsi2.test.alt',

    muc: 'conference.jitsi2.test.alt'
  },

  // BOSH URL. FIXME: use XEP-0156 to discover it.
  bosh: '///jitsi2.test.alt/http-bind',

  // Websocket URL
  // websocket: 'wss://jitsi-meet.example.com/xmpp-websocket',

  // The name of client node advertised in XEP-0115 'c' stanza
  clientNode: 'http://jitsi.org/jitsimeet',

  [...]
}

```

Так как в Альт Сервер по умолчанию установлен веб-сервер apache, то ниже рассмотрена настройка именно этого веб-сервера. Пример конфигурации можно взять в файле **/usr/share/doc/jitsi-meet-web-config-4109/jitsi-meet/jitsi-meet.example-apache**

Создать файл **/etc/httpd2/conf/sites-available/jitsi2.test.alt.conf** на основе **/usr/share/doc/jitsi-meet-web-config-4109/jitsi-meet/jitsi-meet.example-apache**:

```

# cp /usr/share/doc/jitsi-meet-web-config-4109/jitsi-meet/jitsi-meet.example-
apache /etc/httpd2/conf/sites-available/jitsi2.test.alt.conf

```

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

```

<VirtualHost *:80>
  ServerName jitsi2.test.alt
  Redirect permanent / https://jitsi2.test.alt/
  RewriteEngine On
  RewriteCond %{HTTPS} off
  RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
</VirtualHost>

<VirtualHost *:443>

  ServerName jitsi2.test.alt

  SSLProtocol TLSv1 TLSv1.1 TLSv1.2
  SSLEngine on
  SSLProxyEngine on
  SSLCertificateFile /etc/jitsi/meet/jitsi2.test.alt.crt
  SSLCertificateKeyFile /etc/jitsi/meet/jitsi2.test.alt.key
  SSLCipherSuite
"EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA256:EECDH+aRSA+SHA256:EECDH+
ECDSA+SHA384:EECDH+ECDSA+SHA256:EECDH+aRSA+SHA384:EDH+aRSA+AESGCM:EDH+aRSA+SHA256

```



```

:EDH+aRSA:EECDH:!aNULL:!eNULL:!MEDIUM:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4:!
SEED"
    SSLHonorCipherOrder on
    Header set Strict-Transport-Security "max-age=31536000"

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

    ErrorDocument 404 /static/404.html

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

    Alias "/external_api.js" "/usr/share/jitsi-meet/libs/external_api.min.js"
    <Location /external_api.js>
        Require all granted
    </Location>

    ProxyPreserveHost on
    ProxyPass /http-bind http://localhost:5280/http-bind/
    ProxyPassReverse /http-bind http://localhost:5280/http-bind/

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

```

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

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

Выполнить команды:

```

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

```

Включить конфигурацию Apache:

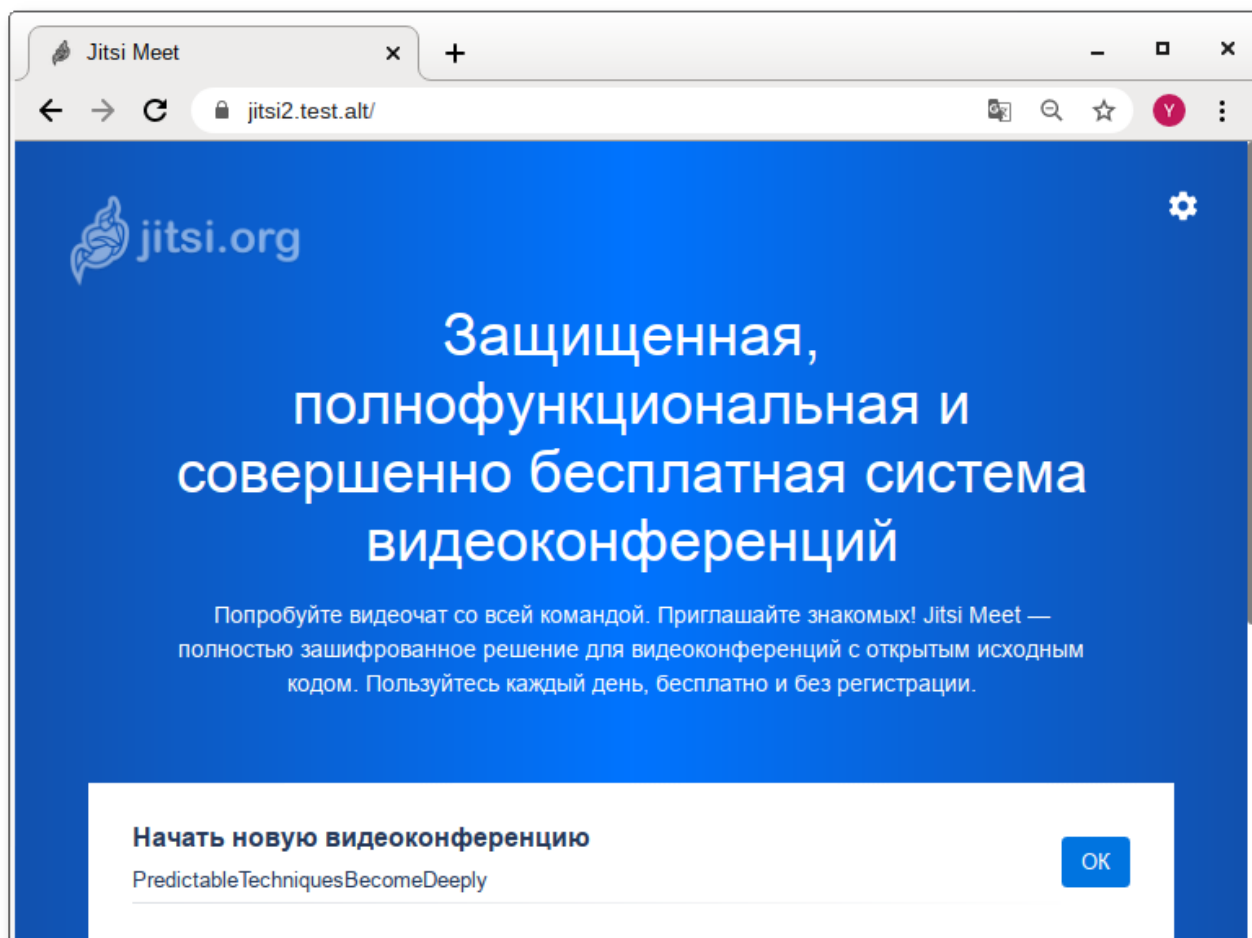
```
# a2ensite jitsi2.test.alt
```

Запустить веб-сервер Apache2 и добавить его в автозагрузку:

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

19.4. Работа с сервисом

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



Для того чтобы начать новую конференцию, достаточно придумать и ввести название будущей конференции (в имени можно использовать буквы на любом языке и пробелы). Чуть ниже будет отображаться список прошлых созданных конференций.

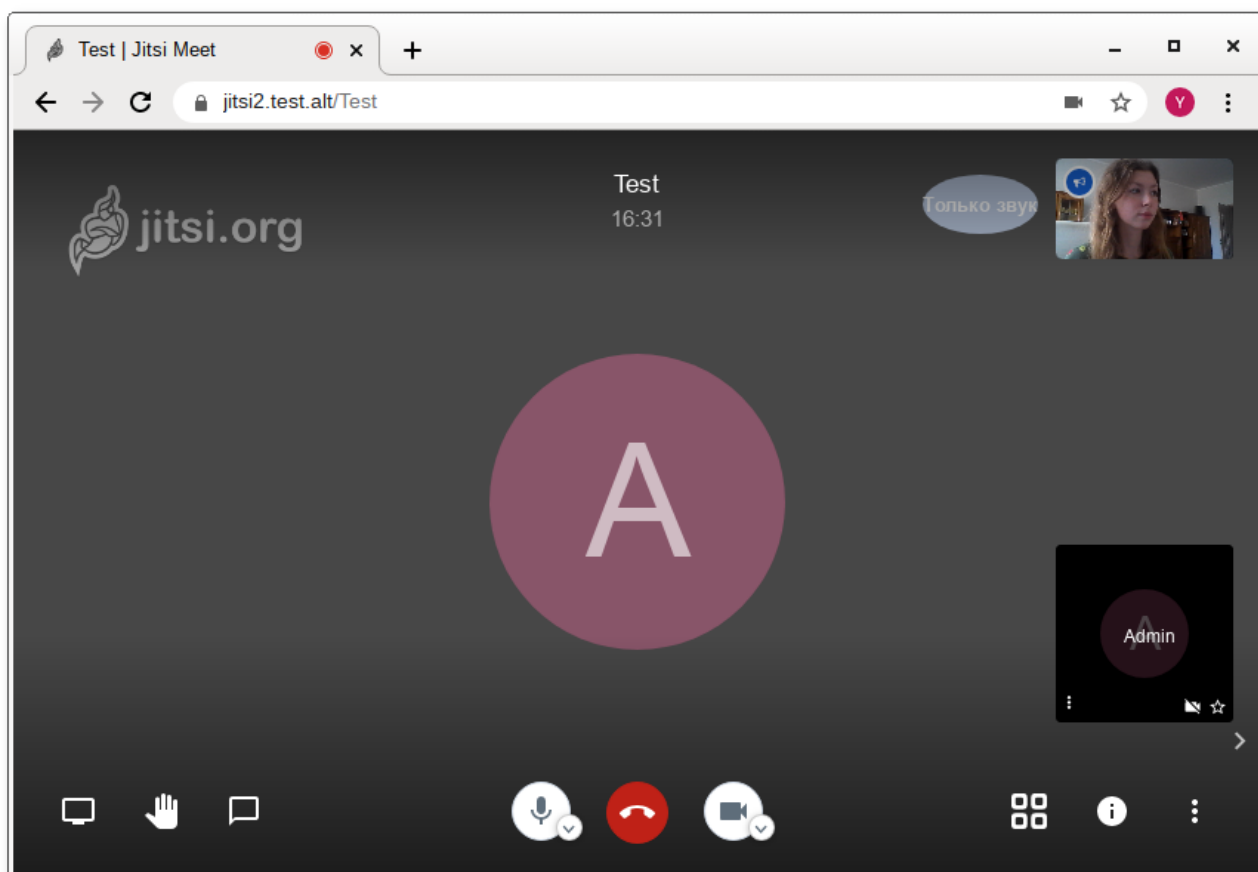


Примечание

Зная URL конференции, в неё может зайти любой желающий. Конференция создаётся, когда в неё заходит первый участник, и существует до выхода последнего. Предотвратить случайных посетителей можно выбрав достаточно длинный URL на главной странице веб-портала, генератор по умолчанию с этим справляется.

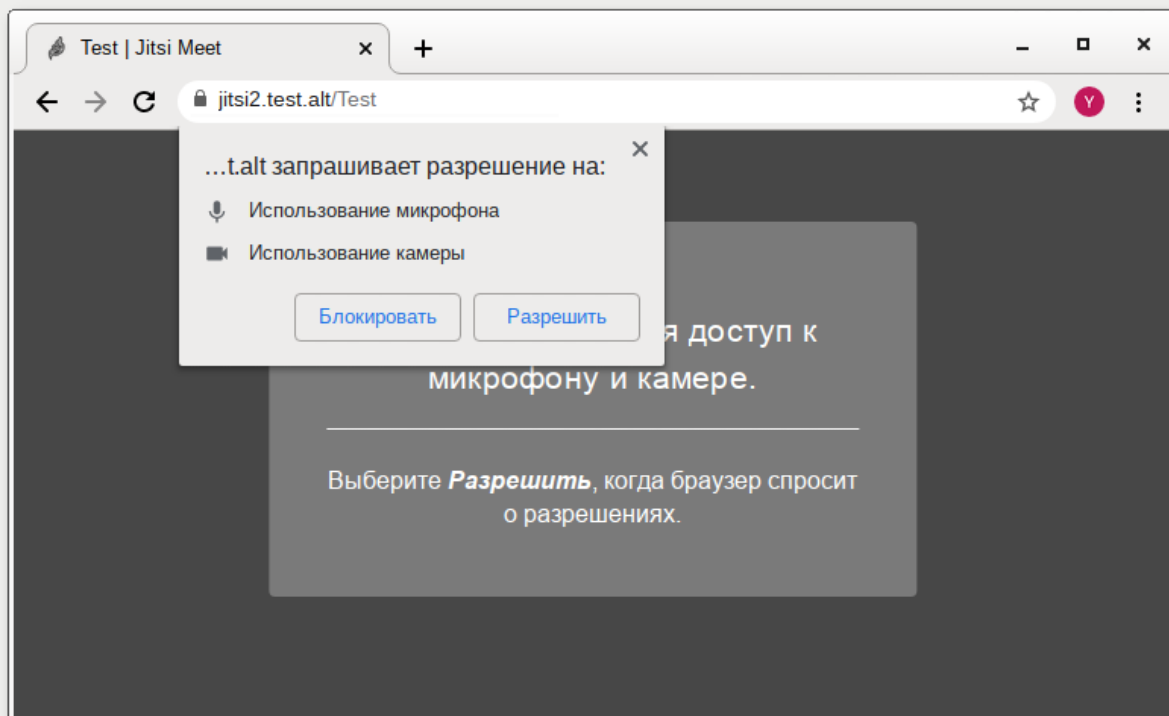
Можно предотвратить неавторизованное создание новых конференций подробнее в [Отключение возможности неавторизованного создания новых конференций](#).

Ввести название конференции и нажать кнопку **OK**. Будет создана конференция:



Примечание

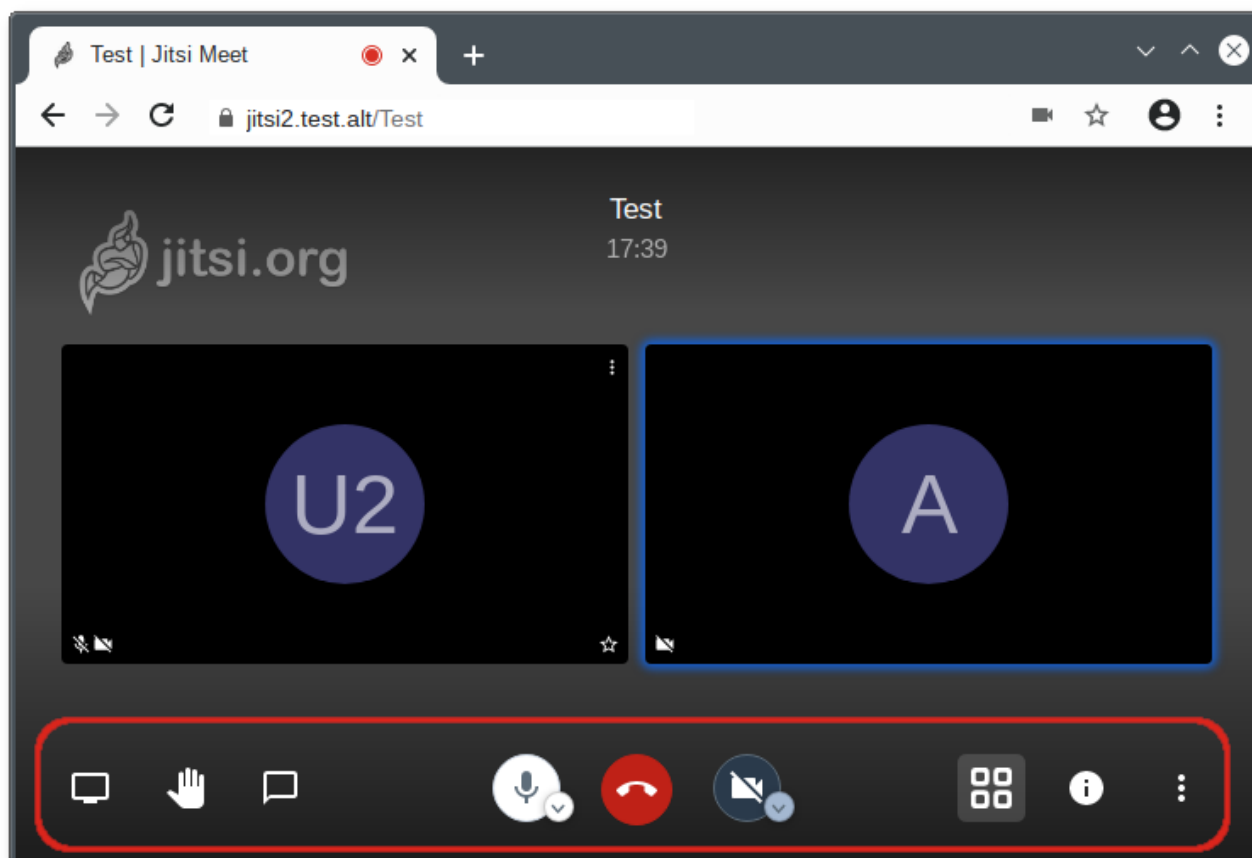
После создания конференции браузер попросит дать ему разрешение на использование веб-камеры и микрофона:



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

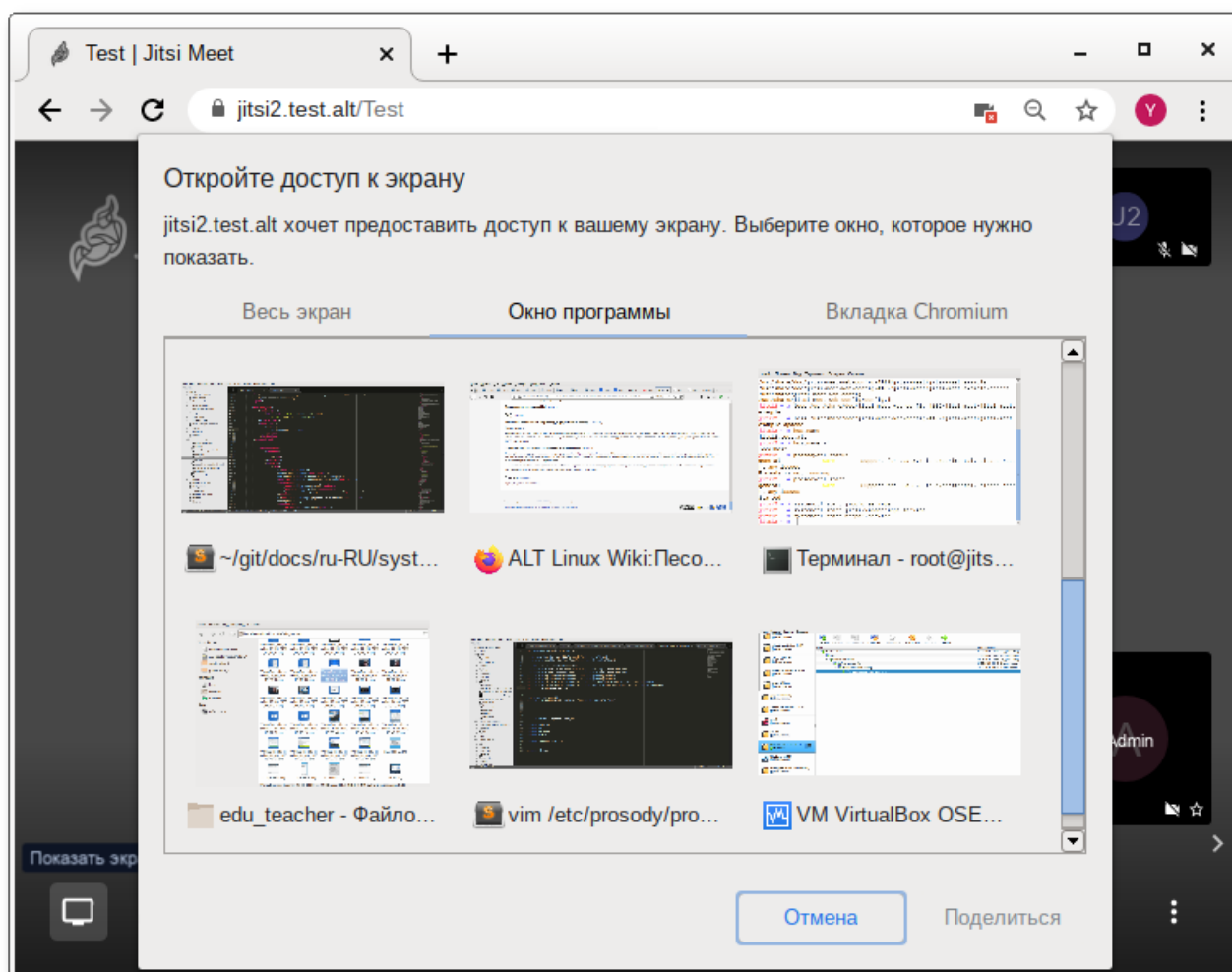
Конференция существует до тех пор, пока в ней есть хотя бы один человек.

Внизу окна конференции находится панель управления:



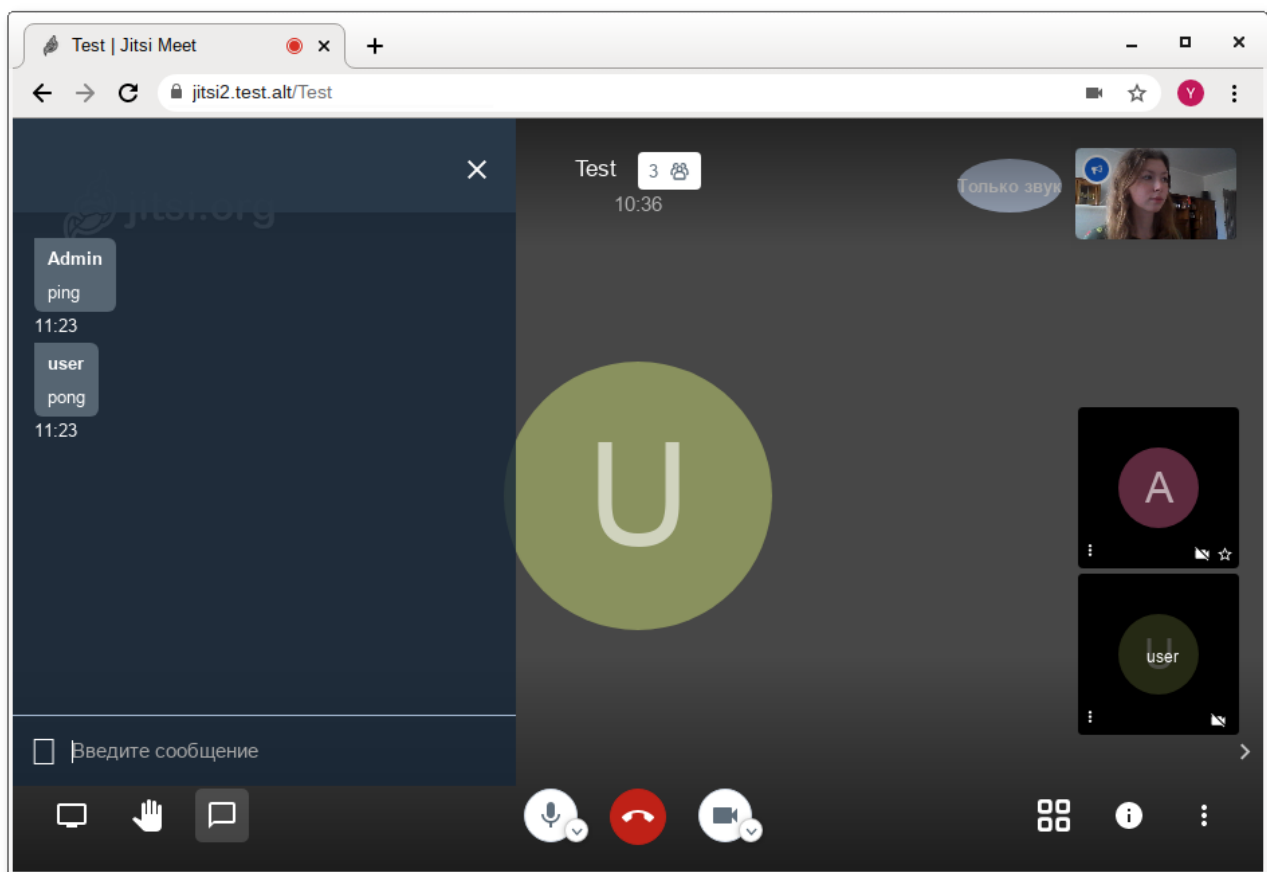
Первая кнопка на панели управления кнопка **Показать экран**. Если нажать на эту кнопку, откроется окно, в котором можно выбрать, что будет демонстрироваться другим участникам конференции. Доступны следующие опции:

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



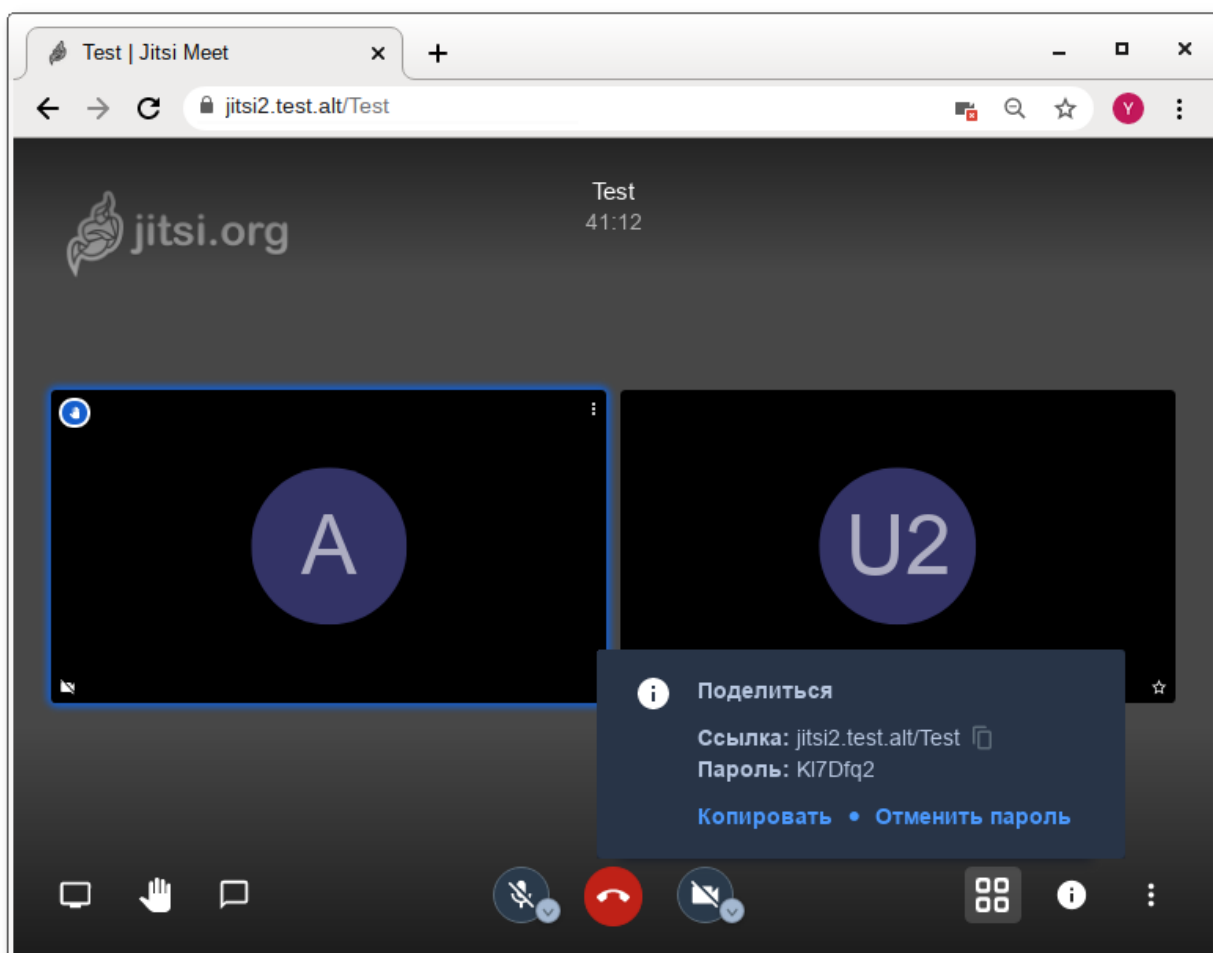
Нажатие на кнопку **Хочу говорить** сигнализирует организатору, что участник хочет говорить. В окне, соответствующем персонажу (справа), появится такой же значок ладони.

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

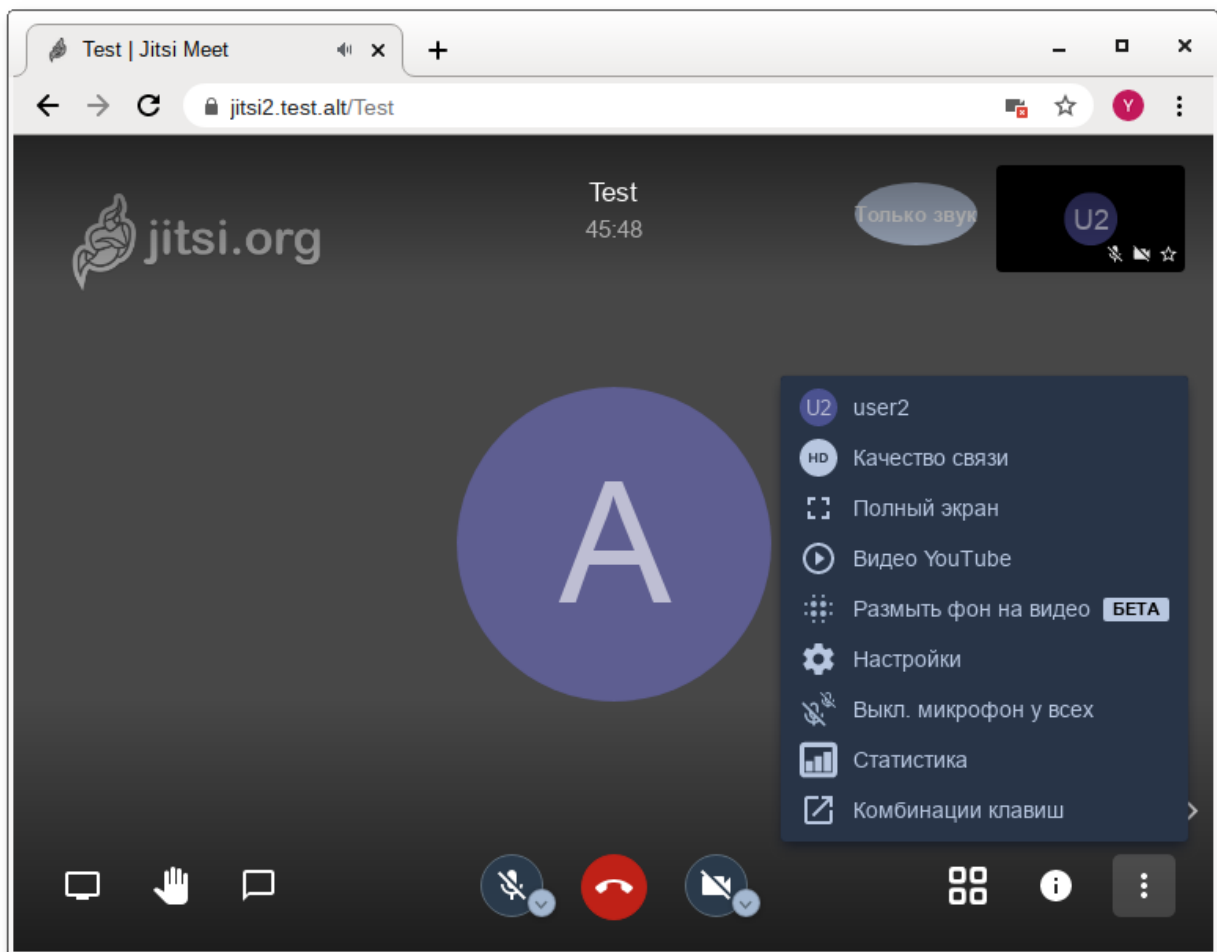


Следующие кнопки на панели управления и их назначение:

- **Микрофон** — позволяет включать и отключать микрофон;
- **Завершить** — выход из конференции;
- **Камера** — включение и выключение веб-камеры;
- **Вкл/Выкл плитку** — вывести окна собеседников в центр чата;
- **Информация о чате** — всплывающее окно, в котором приведена ссылка на конференцию. Здесь же администратор конференции может установить пароль для доступа к конференции;



■ **Больше** — настройка дополнительных функций Jitsi Meet:



19.5. Отключение возможности неавторизованного создания новых конференций

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

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

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

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

на:

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

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


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

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

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

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

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

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

■ перезапустить процессы Jitsi Meet для загрузки новой конфигурации:

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

Команда для регистрации пользователей:

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

Изменить пароль пользователя:

```
prosodyctl passwd <ПОЛЬЗОВАТЕЛЬ>
```

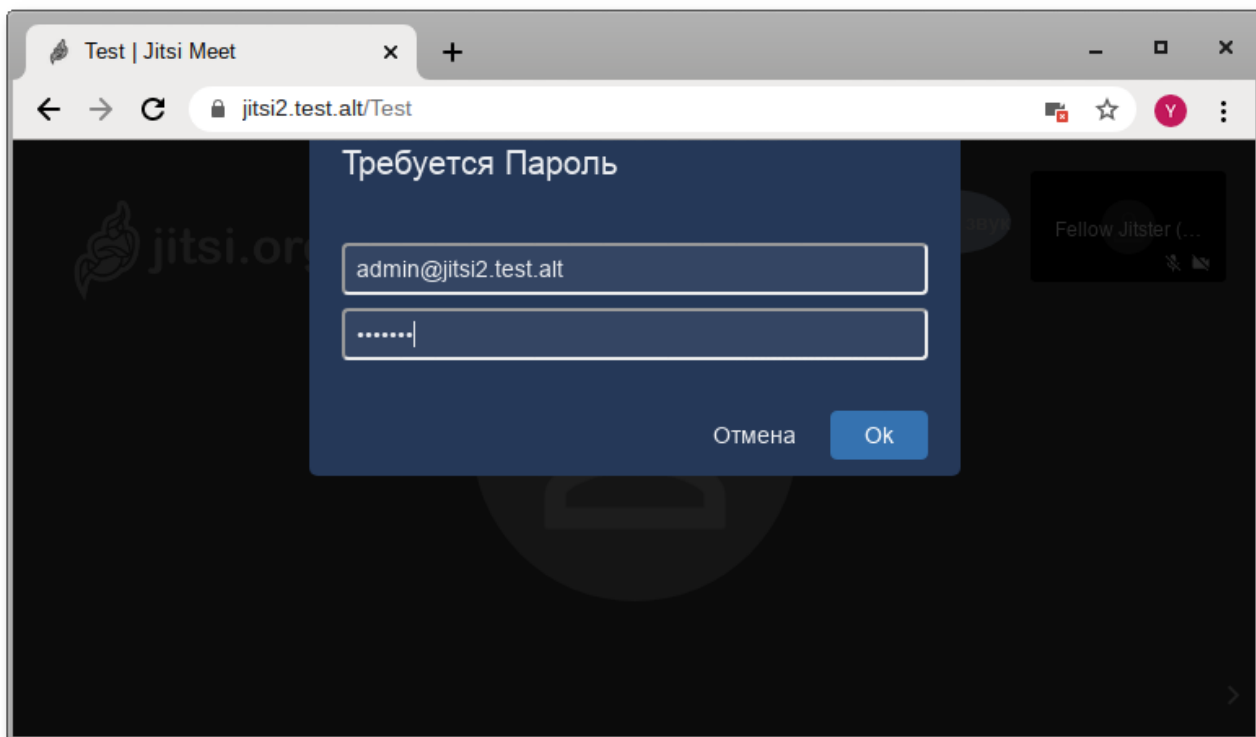
Удалить пользователя:

```
prosodyctl deluser <ПОЛЬЗОВАТЕЛЬ>
```

Например, создадим пользователя admin:

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

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



Глава 20. SOGo

20.1. Установка

20.2. Подготовка среды

20.3. Включение веб-интерфейса

20.4. Настройка электронной почты

20.5. Настройка автоответчика, переадресации и фильтрации

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

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

Возможности SOGo:

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



Предупреждение

MAPI over HTTPS не поддерживается.

20.1. Установка

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

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

20.2. Подготовка среды

Подготовить к запуску и настроить службы PostgreSQL:

- создать системные базы данных:

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

- запустить службу:

```
# systemctl start postgresql
```

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

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

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";  
    OCSEFolderInfoURL = "postgresql://sogo@sogo/sogo_folder_info";  
    OCSSessionsFolderURL = "postgresql://sogo@sogo/sogo_sessions_folder";  
    OCSEMailAlarmsFolderURL = "postgresql://sogo@sogo/sogo_alarms_folder";  
}
```

```

S0GoEnableEmailAlarms = YES;
S0GoDraftsFolderName = Drafts;
S0GoSentFolderName = Sent;
S0GoTrashFolderName = Trash;
S0GoIMAPServer = "imaps://localhost:993/?
tlsVerifyMode=allowInsecureLocalhost";
S0GoMailingMechanism = sendmail;
S0GoForceExternalLoginWithEmail = NO;
NGImap4ConnectionStringSeparator = "/";
S0GoUserSources = (
{
    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");
        };
    };
    S0GoSieveScriptsEnabled = YES;
    S0GoLanguage = Russian;
    S0GoTimeZone = Europe/Moscow;
    S0GoFirstDayOfWeek = 1;
}

```

■ включить службы по умолчанию и перезапустить их:

```

# for service in samba postgresql memcached sogo httpd2; do systemctl enable
$service; systemctl restart $service; done

```

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

20.3. 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 S0Go
# systemctl restart httpd2
# systemctl restart sogo

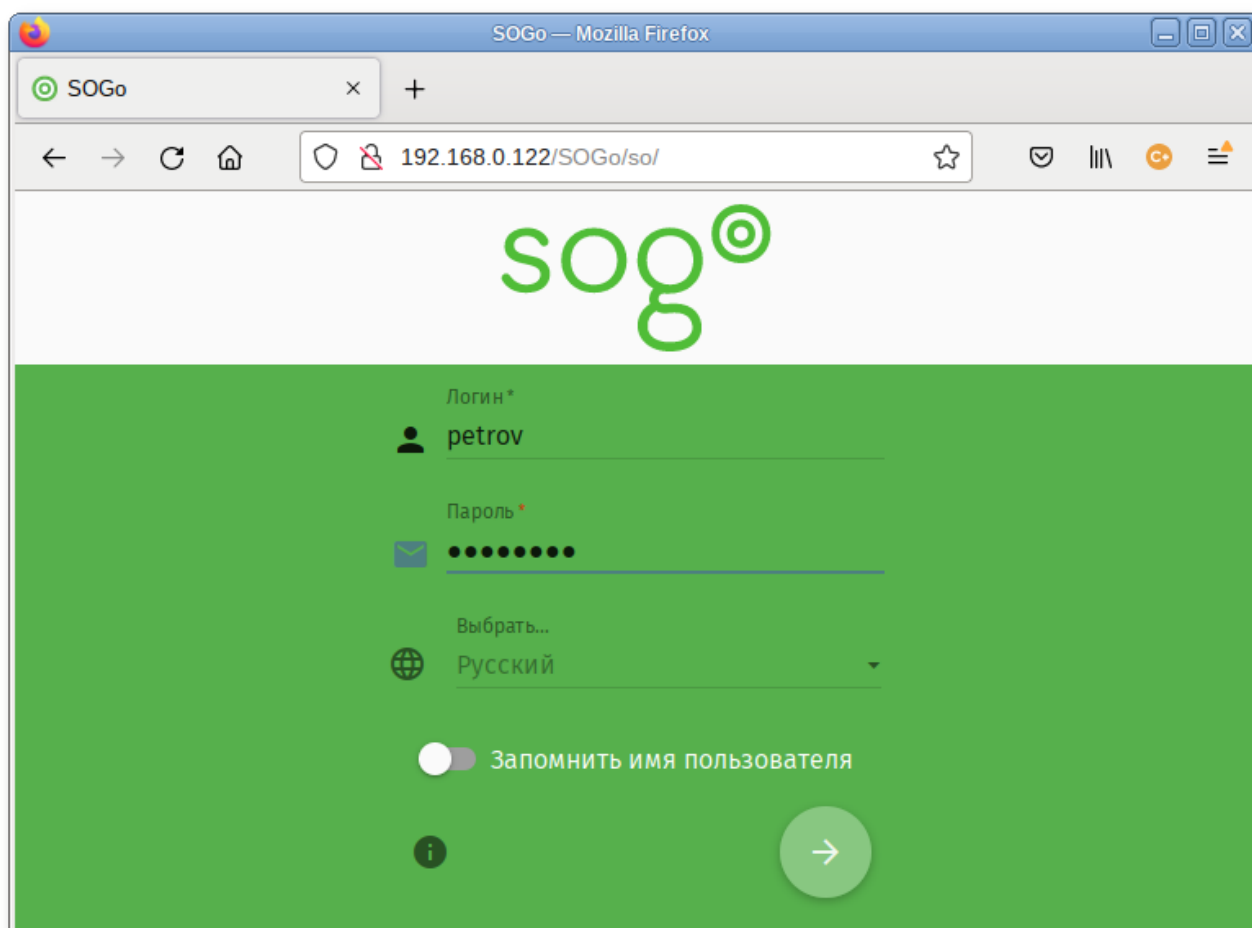
```

Теперь можно войти по адресу:

```

http://<адрес_сервера>/S0Go/

```



Примечание

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

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

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

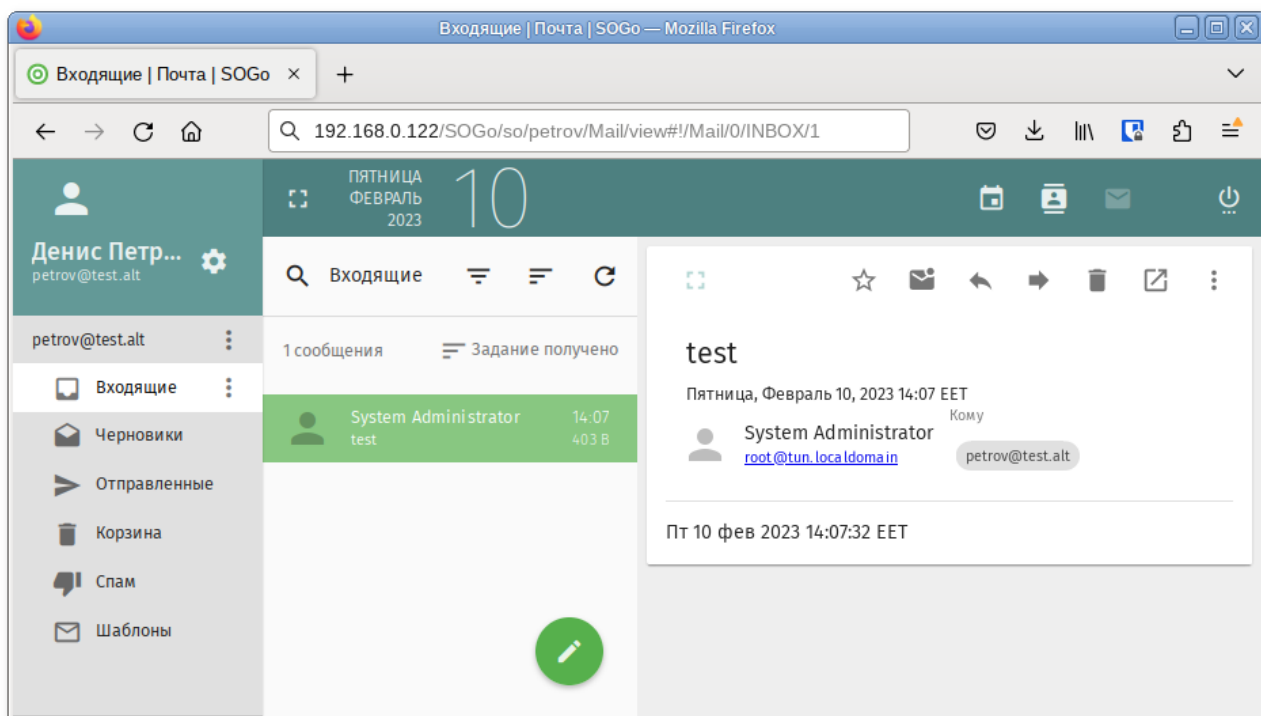
```
TLS_REQCERT allow
```

и перезапустить службы `samba` и `sogo`:

```
# systemctl restart samba
# systemctl restart sogo
```

20.4. 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.



Примечание

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

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



Предупреждение

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

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

и перезапустить samba:

```
# systemctl restart samba
```

Предварительно необходимо создать пользователя vmail (пароль Pa\$\$word) с не истекающей учётной записью:

```
# samba-tool user create -W Users vmail
# samba-tool user setexpiry vmail --noexpiry
```

20.4.1. Настройка Postfix

Установить пакет *postfix-ldap*:

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

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

■ изменить содержимое файла **main.cf**:

```
# Global Postfix configuration file. This file lists only a small subset
# of all parameters. For the syntax, and for a complete parameter list,
# see the postconf(5) manual page. For a commented and more complete
# version of this file see /etc/postfix/main.cf.dist
mailbox_command = /usr/libexec/dovecot/dovecot-lda -f "$SENDER" -a
"$RECIPIENT"
inet_protocols = ipv4

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

# SSL/TLS
smtpd_use_tls = yes
smtpd_tls_security_level = encrypt
#smtpd_tls_security_level = may
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain = test.alt
smtpd_sasl_path = private/auth
smtpd_sasl_type = dovecot
```



```
smtpd_sender_login_maps = ldap:/etc/postfix/ad_sender_login.cf
smtpd_tls_auth_only = yes
smtpd_tls_cert_file = /var/lib/ssl/certs/dovecot.cert
smtpd_tls_key_file = /var/lib/ssl/private/dovecot.key
smtpd_tls_CAfile = /var/lib/ssl/certs/dovecot.pem

smtpd_recipient_restrictions = permit_mynetworks, reject_unauth_destination,
permit_sasl_authenticated, reject
smtpd_sender_restrictions = reject_authenticated_sender_login_mismatch
dovecot_destination_recipient_limit = 1
```

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

■ в файл **master.cf** необходимо добавить строки:

```
dovecot    unix      -      n      n      -      -      pipe
 flags=DRhu user=mail:mail argv=/usr/libexec/dovecot/deliver -d ${recipient}
smtps      inet      n      -      n      -      -      smtpd
 -o smtpd_tls_wrappermode=yes
 -o smtpd_sasl_auth_enable=yes
 -o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

■ создать файл **ad_local_recipients.cf**:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
scope = sub
query_filter = (&(|(mail=%s)(otherMailbox=%u@d))(sAMAccountType=805306368))
result_filter = %s
result_attribute = mail
special_result_attribute = member

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

■ создать файл **ad_mail_groups.cf**:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
timeout = 3
scope = sub
query_filter = (&(mail=%s)(sAMAccountType=268435456))
result_filter = %s
result_attribute = mail
special_result_attribute = member

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

■ создать файл **ad_sender_login.cf**:

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

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

■ перезапустить службу postfix:

```
# systemctl restart postfix
```

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

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

Проверка пользователя почты petrov:

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

Проверка входа:

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

Проверка общего адреса e-mail:

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

20.4.2. Настройка Dovecot

Установить Dovecot:

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

Изменить файлы для домена test.alt:

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

```
hosts          = test.alt:3268
ldap_version   = 3
auth_bind      = yes
dn             = cn=vmail,cn=Users,dc=test,dc=alt
dnpass         = Pa$$word
base           = cn=Users,dc=test,dc=alt
scope          = subtree
```

```
deref          = never

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

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

```
auth_mechanisms = plain
!include auth-ldap.conf.ext
```

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

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

■изменить файл **/etc/dovecot/conf.d/10-master.conf**:

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

```
service dict {
    unix_listener dict {
    }
}
```

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

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

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

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

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

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

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

■ перезапустить службу dovecot:

```
# systemctl restart dovecot
```

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

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

20.4.3. Безопасность

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

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

Перезапустить службы:

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

20.4.4. 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 dc.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
```

где `dc.test.alt` — имя узла сервера SOGo.

20.5. Настройка автоответчика, переадресации и фильтрации

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

Настройка Dovecot:

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

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

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

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

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

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

```
mail_plugins = $mail_plugins sieve
```

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

```
mail_plugins = $mail_plugins sieve
```

- в файле **/etc/dovecot/conf.d/20-managesieve.conf** в разделе *protocol lmtp* указать протокол sieve:

```
protocols = $protocols sieve
```

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

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

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

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

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

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

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

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

Должно быть обязательно указано несуществующее имя домена. В реальных условиях необходимо использовать хэш пароля (например, **doveadm pw -s SHA512**).

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

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

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

```
MAILTO=""
```

и раскомментировать строку:

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

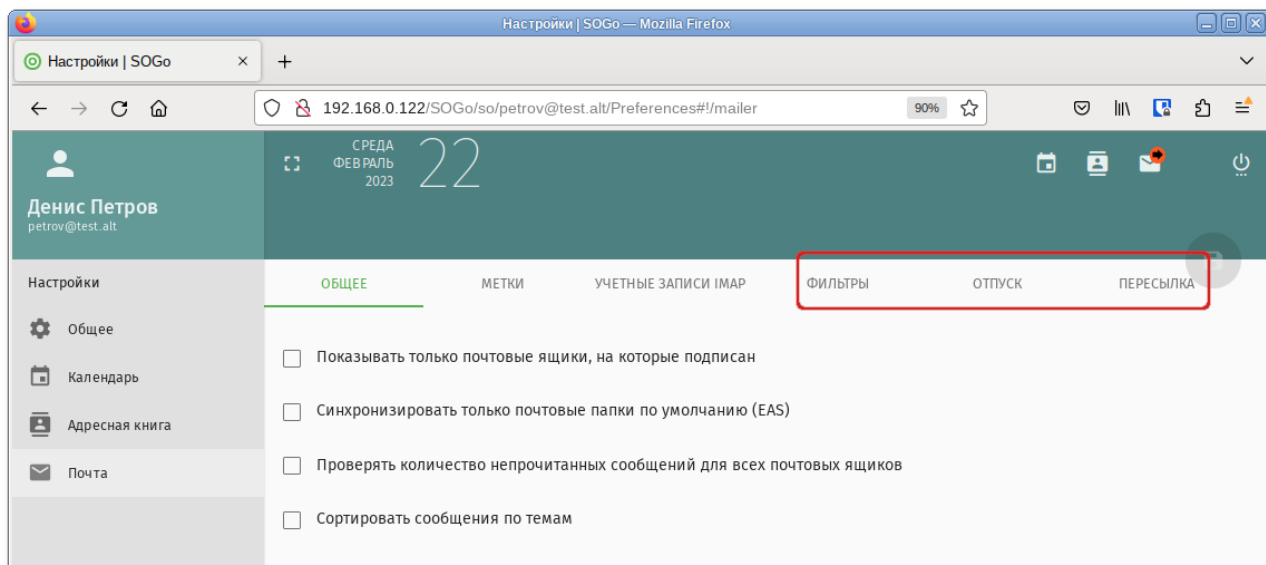
В SOGo необходимо активировать окно настроек почтовых фильтров (параметр **SOGoSieveScriptsEnabled**), окно настроек сообщений об отпуске (параметр **SOGoVacationEnabled**), а также окно настроек адресов электронной почты для пересылки (параметр **SOGoForwardEnabled**). Для этого в файл конфигурации **/etc/sogo/sogo.conf** добавить строки:

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

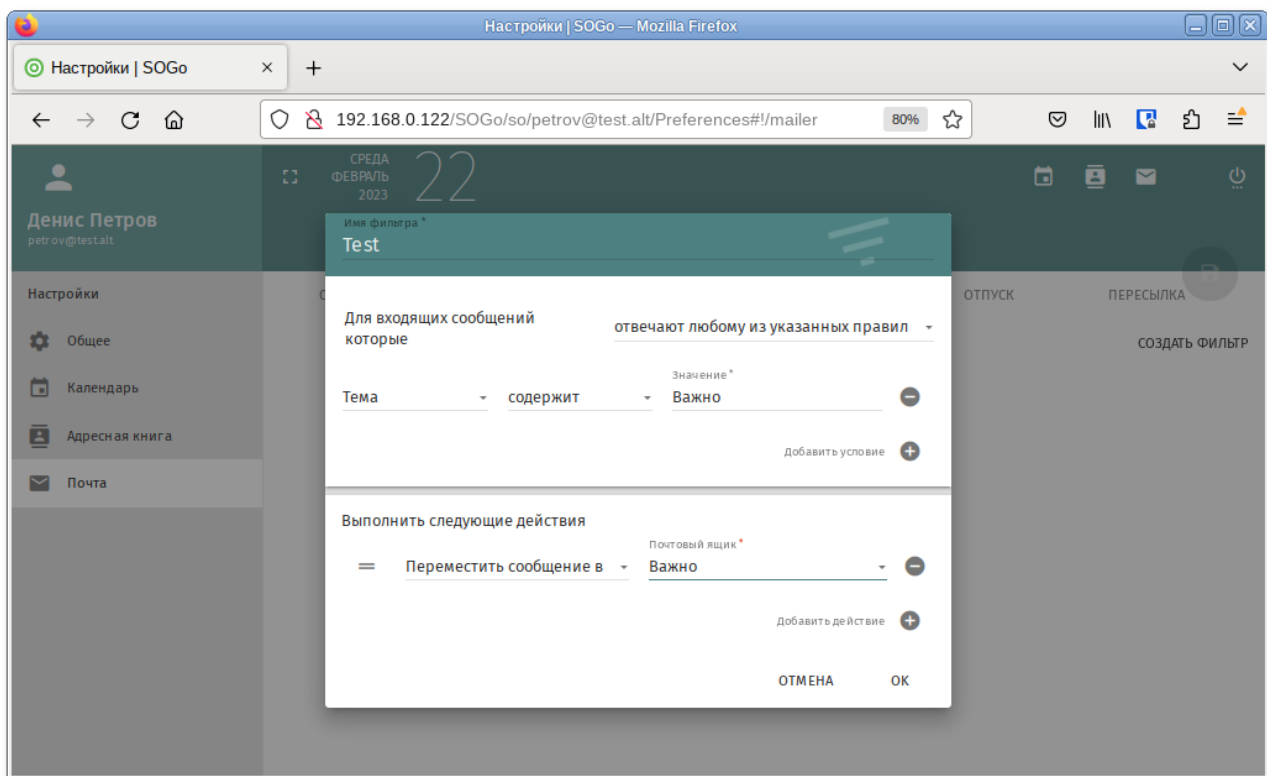
Перезапустить службы:

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

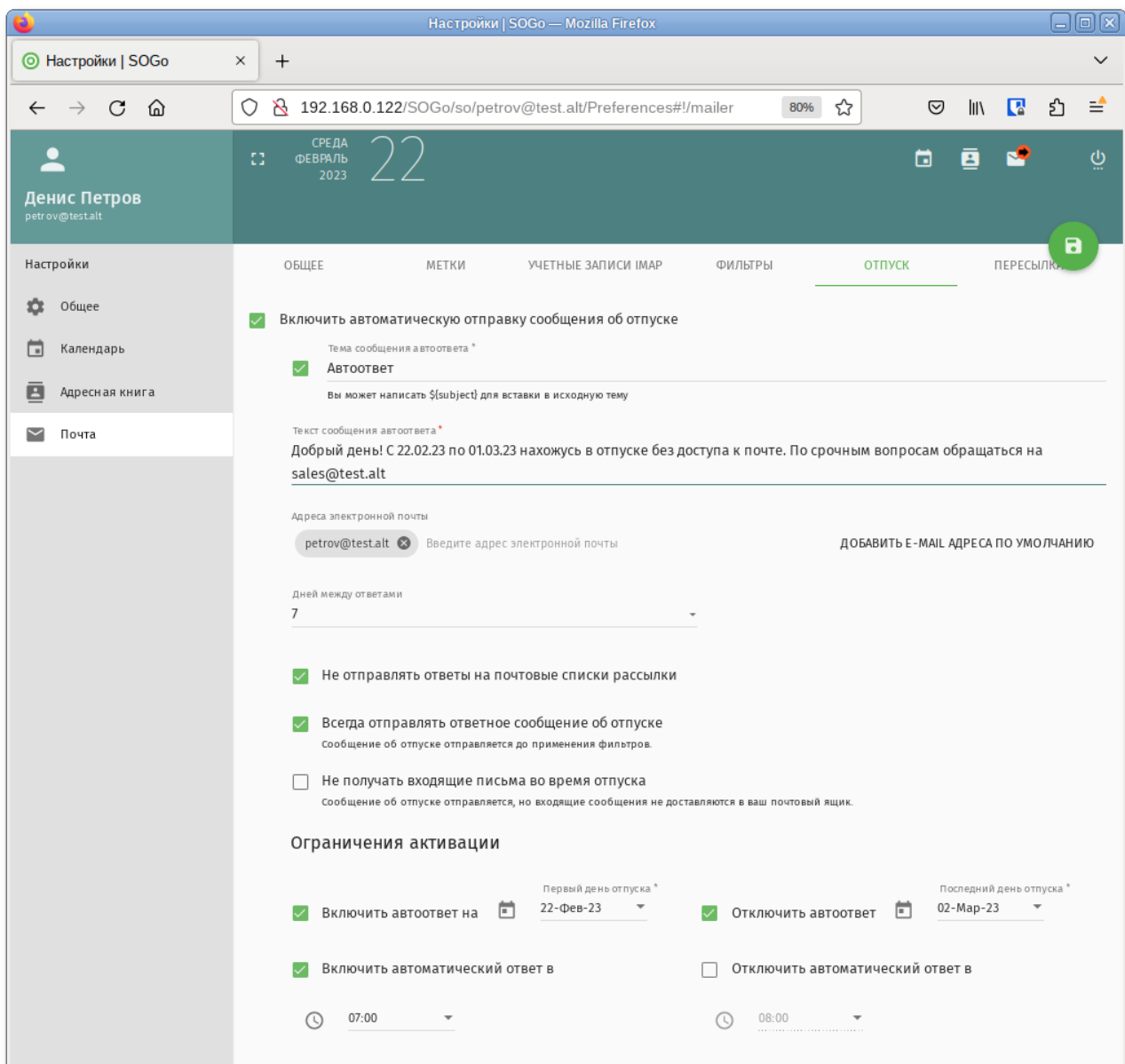
В результате в веб-интерфейсе SOGo в настройках почты появятся три дополнительные вкладки:



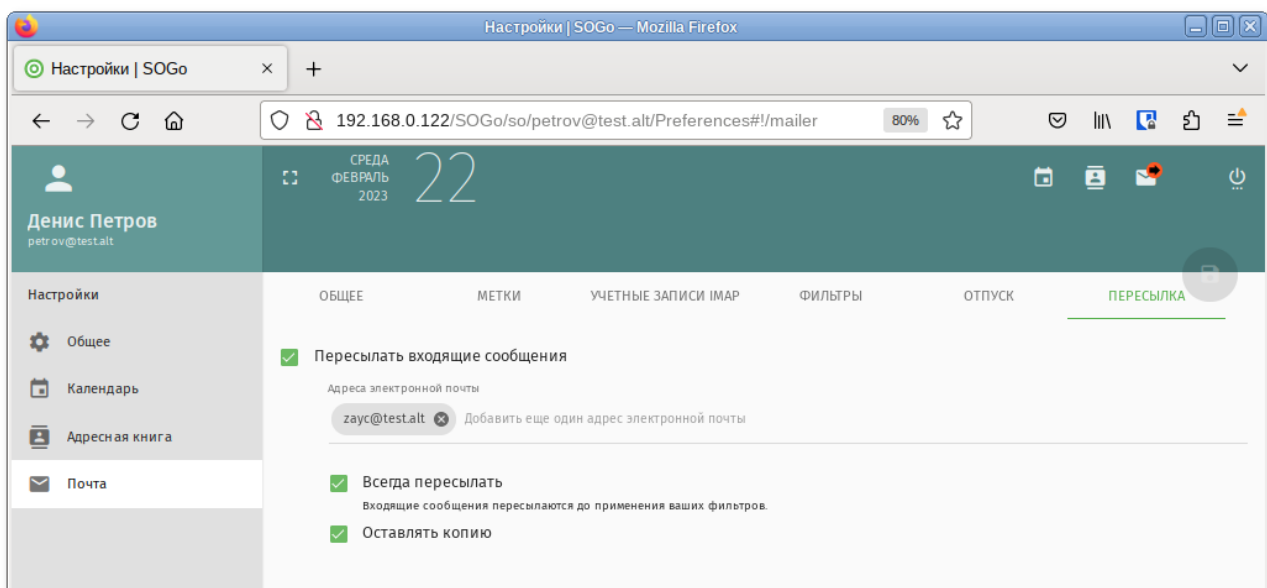
На вкладке **Фильтры** можно создавать фильтры и устанавливать критерии, по которым они должны работать:



На вкладке **Отпуск** можно настроить автоответ на время отпуска:



На вкладке **Пересылка** настраивается переадресация электронной почты:



Глава 21. Отказоустойчивый кластер (High Availability) на основе Pacemaker

21.1. Настройка узлов кластера

21.2. Установка кластерного ПО и создание кластера

21.3. Настройка параметров кластера

21.4. Настройка ресурсов

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

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

Архитектура Pacemaker представляет собой три уровня:

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

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

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

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

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

21.1. Настройка узлов кластера

Для функционирования отказоустойчивого кластера необходимо, чтобы выполнялись следующие требования:

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



Примечание

В примере используется следующая конфигурация:

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

Дальнейшие действия следует выполнить на всех узлах кластера.



Примечание

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

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

21.1.1. 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
```

21.1.2. Настройка ssh-подключения между узлами

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

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

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

```
AllowGroups sshusers
```

создать группу sshusers:

```
# groupadd sshusers
```

и добавить туда пользователей, которым разрешено подключаться по ssh:

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



Примечание

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

```
# systemctl restart sshd
```

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

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



Важно

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

Скопировать публичную часть SSH-ключа на другие узлы кластера:

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

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

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

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



Важно

Каталог **/root/.ssh** при этом должен существовать.

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

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

21.2. Установка кластерного ПО и создание кластера

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

Установить на всех узлах необходимые пакеты:

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



Примечание

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

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

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

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

```
# passwd hacluster
```

Запустить и добавить в автозагрузку службу *pcsd*:

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

Настроить аутентификацию (на одном узле):

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

После этого кластером можно управлять с одного узла.

Создать кластер:

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

```
node02: successful distribution of the file 'corosync authkey'
node02: successful distribution of the file 'pacemaker authkey'
Sending 'corosync.conf' to 'node01', 'node02', 'node03'
node01: successful distribution of the file 'corosync.conf'
node02: successful distribution of the file 'corosync.conf'
node03: successful distribution of the file 'corosync.conf'
Cluster has been successfully set up.
```

Запустить кластер:

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

Настройка автоматического включения кластера при загрузке:

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

Проверка состояния кластера:

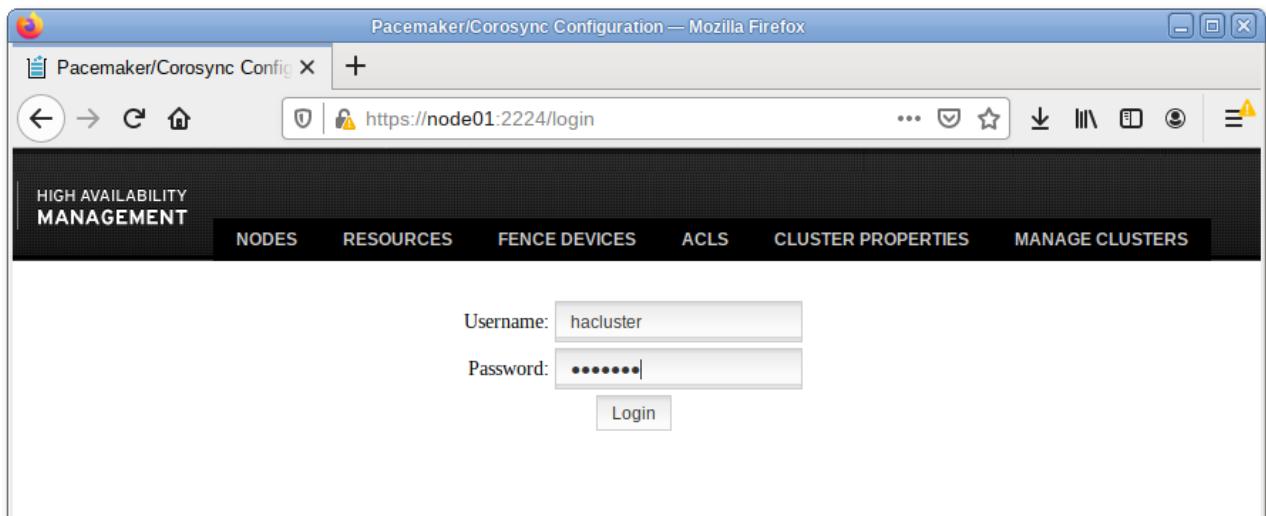
```
# pcs status cluster
Cluster Status:
Cluster Summary:
* Stack: corosync
* Current DC: node02 (version 2.1.2-alt1-ada5c3b36) - partition with quorum
* Last updated: Mon Jun 20 15:28:32 2022
* Last change: Mon Jun 20 15:27:55 2022 by hacluster via crmd on node02
* 3 nodes configured
* 0 resource instances configured
Node List:
* Online: [ node01 node02 node03 ]

PCSD Status:
node02: Online
node01: Online
node03: Online
```

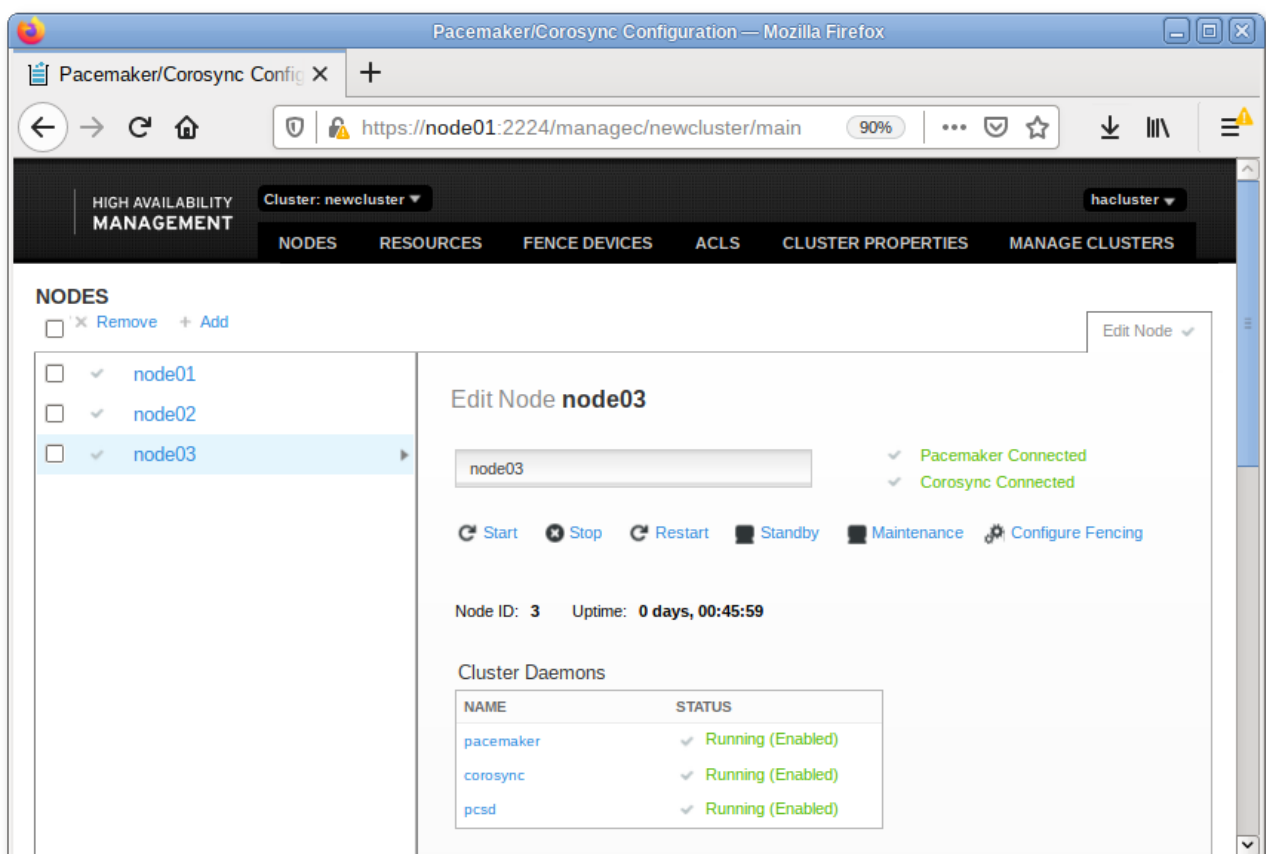
Проверка синхронизации узлов кластера:

```
# 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):



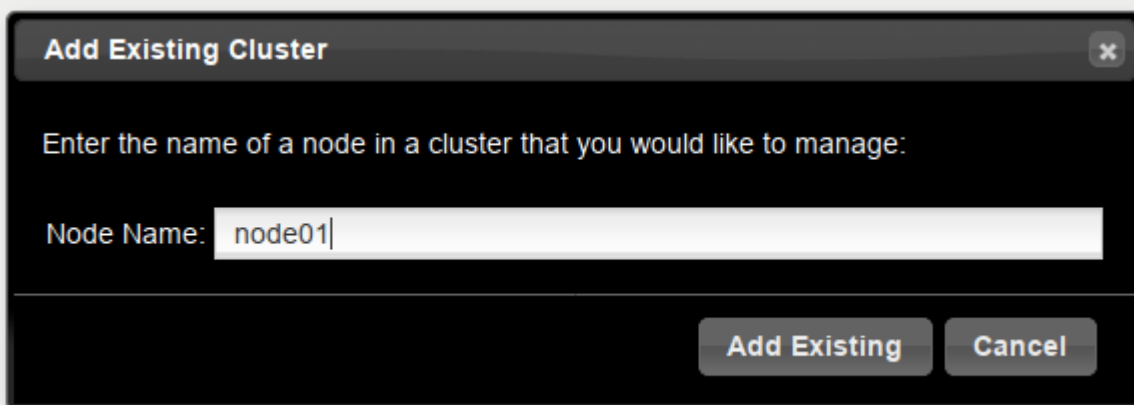
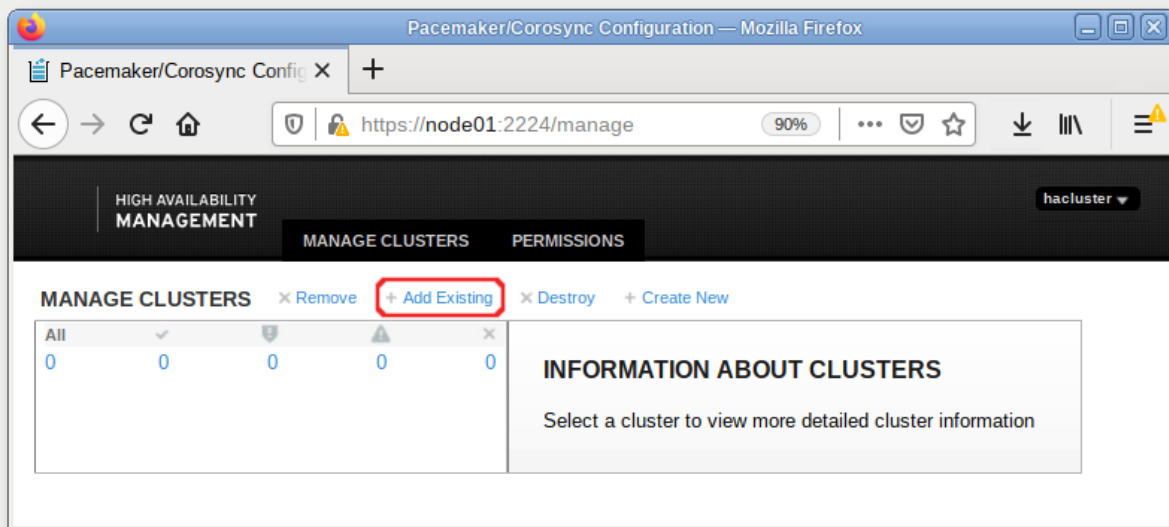
После входа в систему на главной странице отображается страница «Управление кластерами». На этой странице перечислены кластеры, которые в настоящее время находятся под управлением веб-интерфейса. При выборе кластера отображается информация о кластере:





Примечание

Чтобы добавить существующий кластер в веб-интерфейс, необходимо нажать кнопку **Add Existing** и в открывшемся окне ввести имя или IP-адрес любого узла в кластере:



21.3. 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
```

21.3.1. 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
```

21.3.2. Настройка STONITH

Для корректной работы узлов с общим хранилищем, необходимо настроить механизм STONITH. Этот механизм позволяет кластеру физически отключить не отвечающий на запросы узел, чтобы не повредить данные на общем хранилище.

Отключить STONITH, пока он не настроен можно, выполнив команду:

```
# pcs property set stonith-enabled=false
```



Важно

В реальной системе нельзя использовать конфигурацию с отключенным STONITH. Отключенный параметр на самом деле не отключает функцию, а только лишь эмулирует ее срабатывание при определенных обстоятельствах.

21.4. Настройка ресурсов

Настроим ресурс, который будет управлять виртуальным IP-адресом. Этот адрес будет мигрировать между узлами, предоставляя одну точку входа к ресурсам, заставляя работать несколько узлов как одно целое устройство для сервисов.

Команда создания ресурса виртуального IP-адреса с именем ClusterIP с использованием алгоритма ресурсов ocf (каждые 20 секунд производить мониторинг работы, в случае выхода из строя узла необходимо виртуальный IP переключить на другой узел):

```
# pcs resource create ClusterIP ocf:heartbeat:IPaddr2 ip=192.168.0.251  
cidr_netmask=24 op monitor interval=20s
```



Примечание

Для того чтобы добавить ресурс в веб-интерфейсе, необходимо перейти на вкладку **RESOURCES**, нажать кнопку **Add** и задать параметры ресурса:

The screenshot shows a web browser window titled "Pacemaker/Corosync Configuration — Mozilla Firefox". The address bar shows "https://node01:2224/managec/newcluster/main#/re". The page has a sidebar with "HIGH AVAILABILITY MANAGER" and "RESOURCES" tabs. The "RESOURCES" tab is active, showing a table with columns "NAME" and "ACTION". A modal dialog titled "Add Resource" is open. It contains the following fields:

- Class/Provider:** ocf:heartbeat (dropdown)
- Type:** IPaddr2 (dropdown)
- Description:** Manages virtual IPv4 and IPv6 addresses (Linux specific version) ⓘ
- Resource Group:** None (dropdown)
- Clone:** ☐
- Promotable Clone:** ☐
- Disabled:** ☐
- Resource ID:** ClusterIP (text input)
- Required Arguments:**
 - ip ⓘ:** 192.168.0.251 (text input)
- Optional Arguments:** (expandable section)
- Advanced Arguments:** (expandable section)
- Create Resource** (button)

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
```

Глава 22. Система резервного копирования Proxmox Backup Server

22.1. Установка PBS

22.2. Веб-интерфейс PBS

22.3. Настройка хранилища данных

22.4. Управление трафиком

22.5. Управление пользователями

22.6. Управление удалёнными PBS

22.7. Клиент резервного копирования

22.8. Интеграция с PVE

Proxmox Backup Server (PBS) — клиент-серверное решение для резервного копирования и восстановления виртуальных машин, контейнеров и данных с физических узлов. Решение оптимизировано для проекта Proxmox VE (PVE). PBS поддерживает инкрементное резервное копирование с полной дедупликацией, что значительно снижает нагрузку на сеть и экономит пространство для хранения.

Все взаимодействия между клиентом и сервером шифруются 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 веб-интерфейс. Все административные задачи можно выполнять в веб-браузере. Веб-интерфейс также предоставляет встроенную консоль.

22.1. Установка PBS

22.1.1. Установка сервера PBS

Установить сервер PBS:

```
# apt-get install proxmox-backup-server
```

Запустить и добавить в автозагрузку Proxmox Backup API Proxy Server:

```
# systemctl enable --now proxmox-backup-proxy.service
```

Служба proxmox-backup-proxy предоставляет API управления PBS по адресу **127.0.0.1:82**. Она имеет разрешение на выполнение всех привилегированных операций.



Примечание

Для работы с локальным ZFS хранилищем должен быть установлен модуль ядра с поддержкой ZFS (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**.

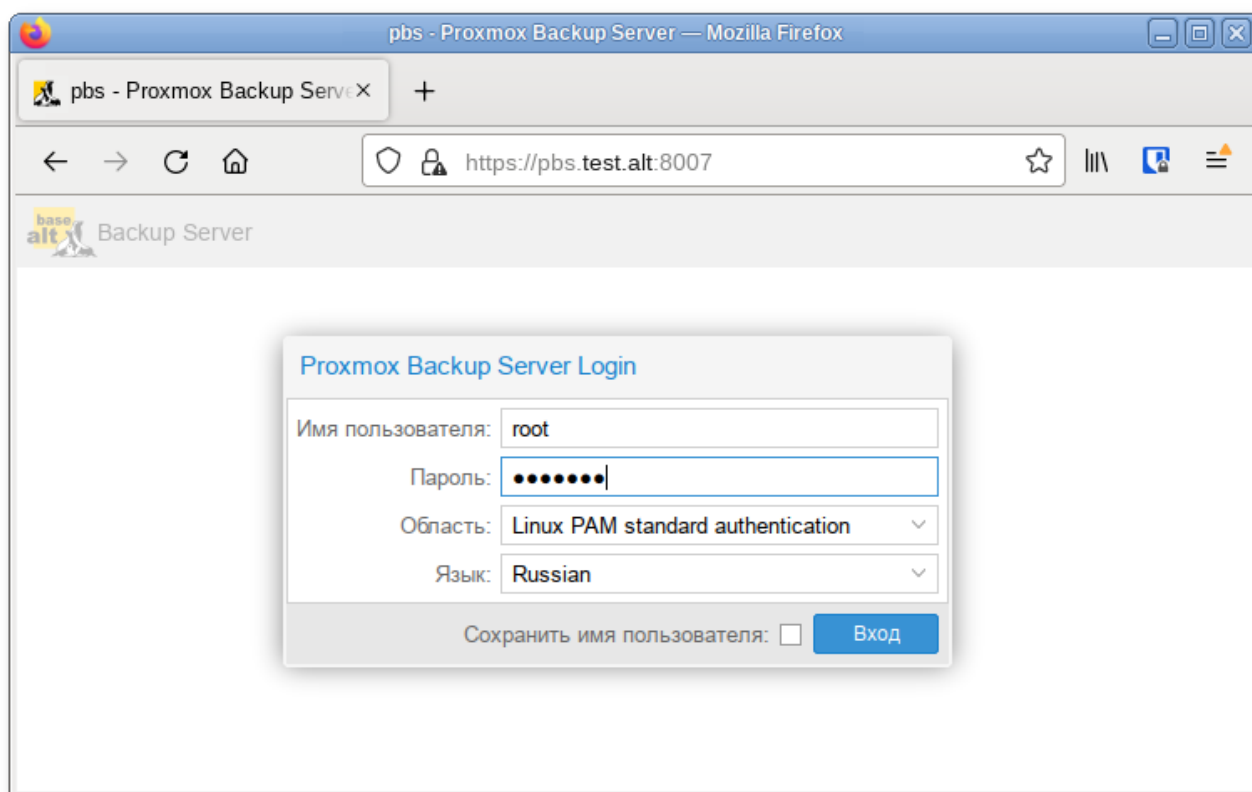
22.1.2. Установка клиента PBS

Установить клиент PBS:

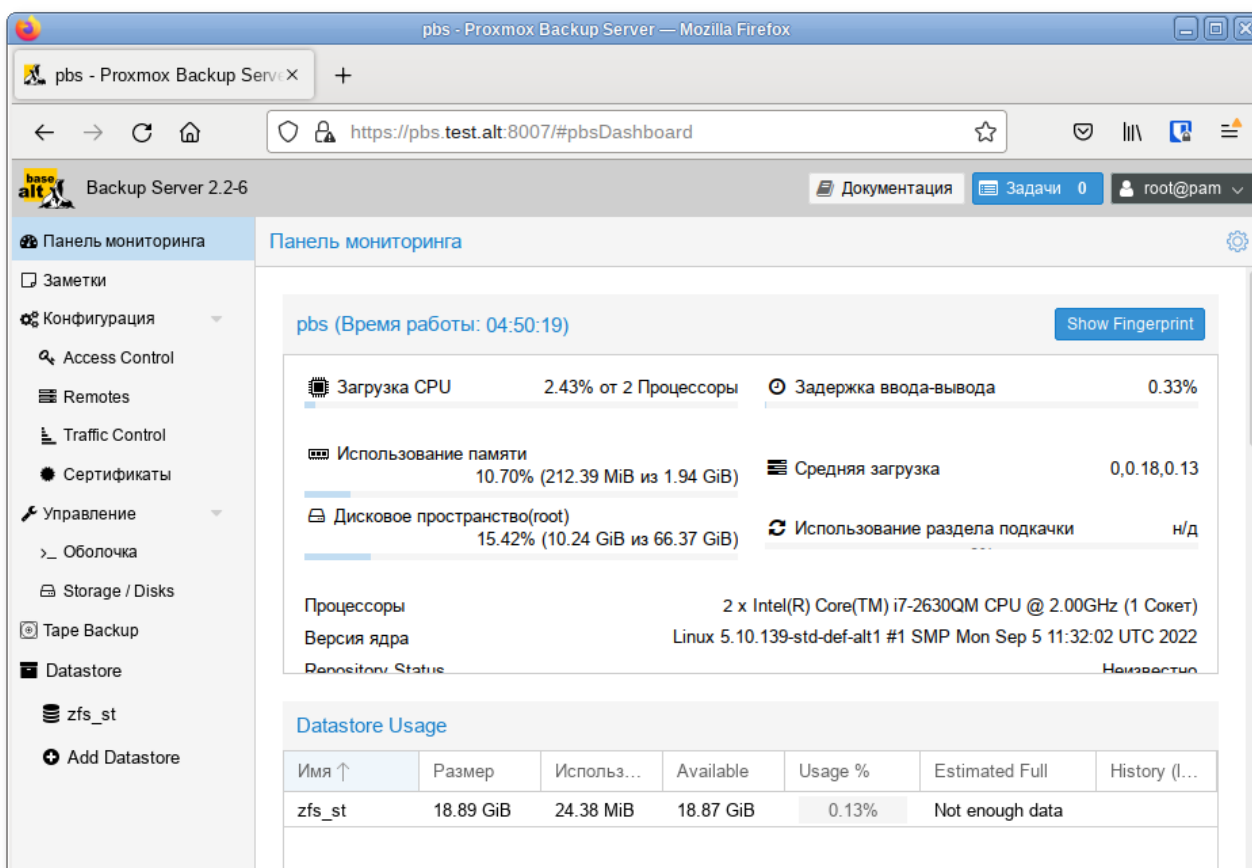
```
# apt-get install proxmox-backup-client
```

22.2. 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):



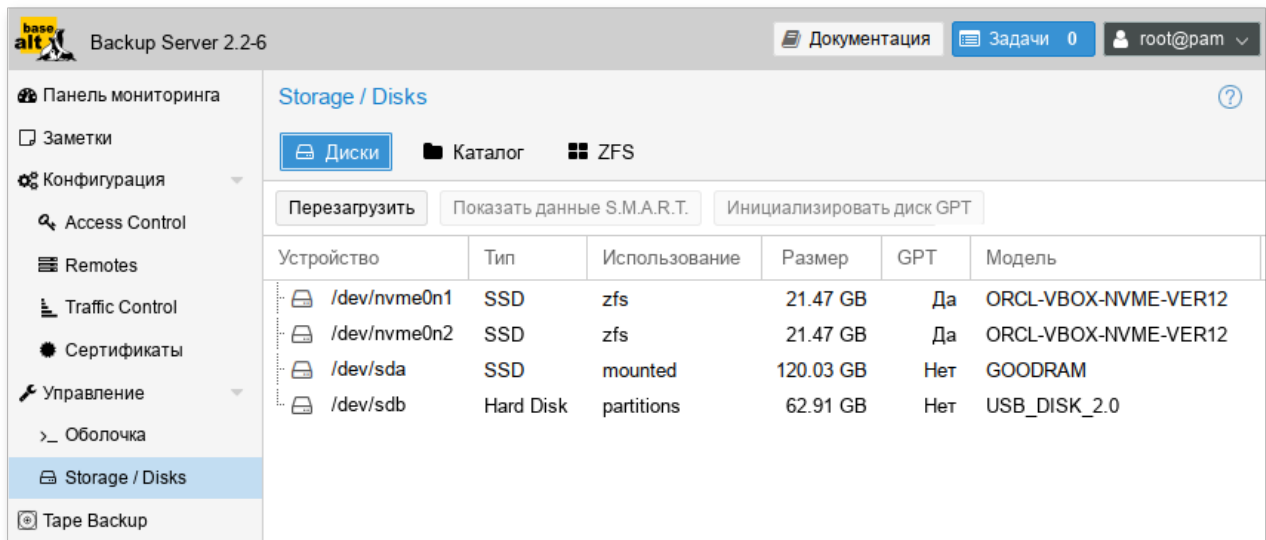
Веб-интерфейс PBS:



22.3. Настройка хранилища данных

22.3.1. Управление дисками

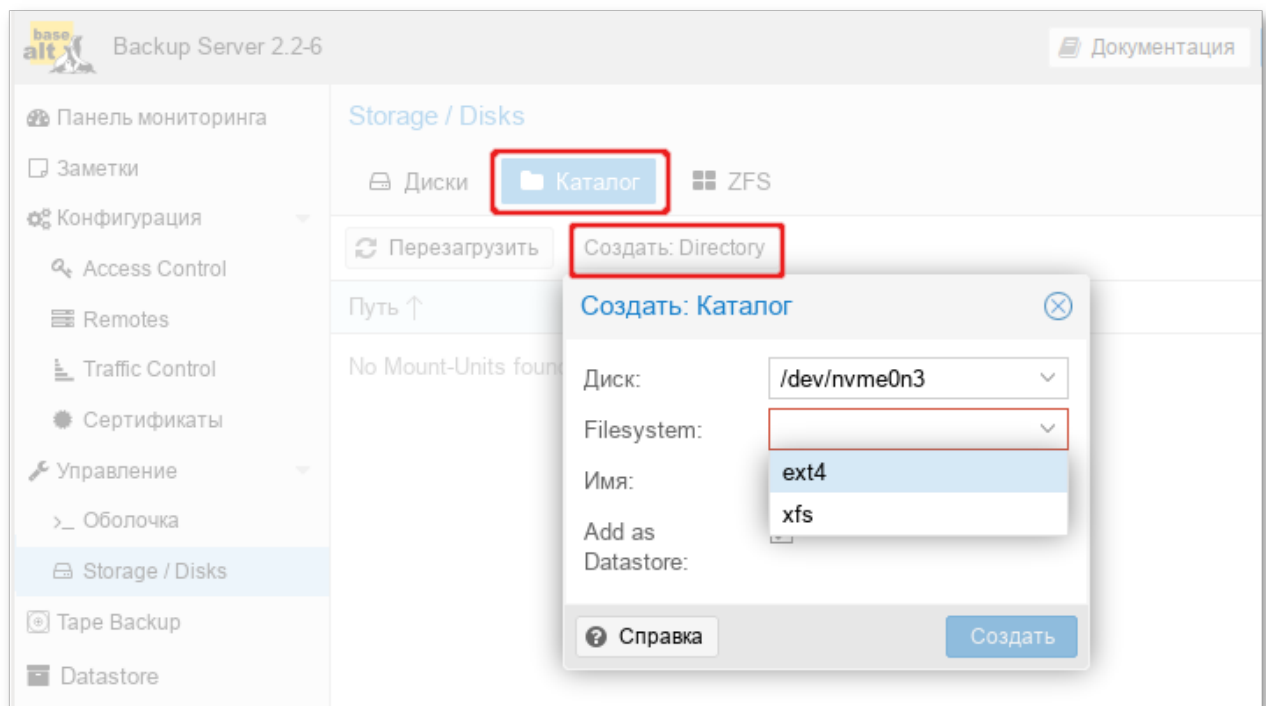
В веб-интерфейсе на вкладке **Управление** → **Storage/Disks (Хранилище/Диски)** можно увидеть диски, подключённые к системе:



Просмотр списка дисков в командной строке:

```
# proxmox-backup-manager disk list
```

Создание файловой системы ext4 или xfs на диске в веб-интерфейсе:



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**:

Редактировать: ZFS

Имя:

RAID Level:

Mirror

Add as ☒

Сжатие:

on

Datastore:

ashift:

12

<input checked="" type="checkbox"/>	Устройство	Модель	Серийный номер	Размер	Order
<input checked="" type="checkbox"/>	/dev/nvme0n1	ORCL-VBOX-NVME-VER12	VB1234-56789	21.47 GB	<div>⬆⬇⬆</div>
<input checked="" type="checkbox"/>	/dev/nvme0n2	ORCL-VBOX-NVME-VER12	VB1234-56789	21.47 GB	<div>⬆⬇⬆</div>

Note: ZFS is not compatible with disks backed by a hardware RAID controller. For details see [the reference documentation](#).

Справка

OK

Reset

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
```

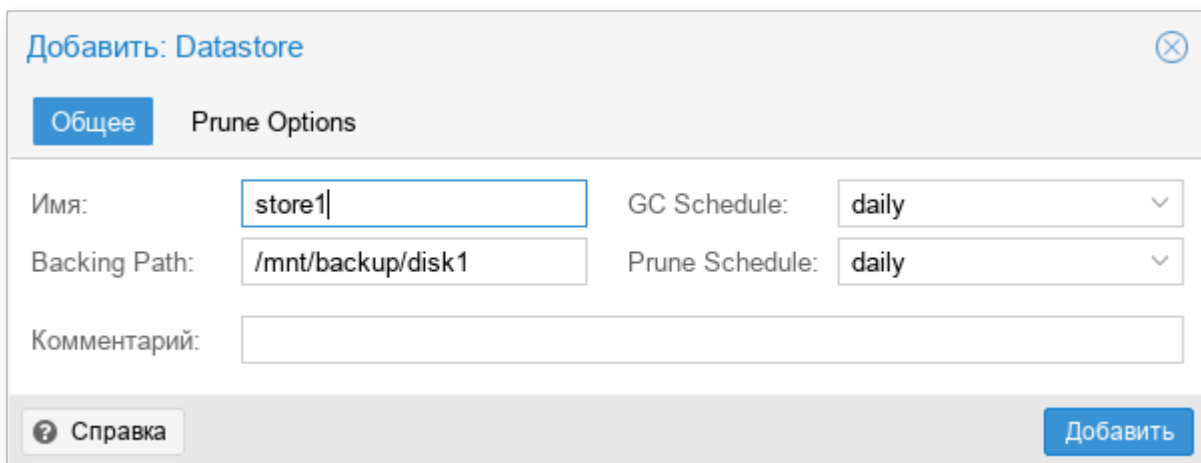
22.3.2. Создание хранилища данных

Хранилище данных — это место, где хранятся резервные копии. Текущая реализация PBS использует каталог внутри стандартной файловой системы (ext4, xfs или zfs) для хранения данных резервного копирования. Информация о конфигурации хранилищ данных хранится в файле **/etc/proxmox-backup/datastore.cfg**.

Необходимо настроить как минимум одно хранилище данных. Хранилище данных идентифицируется именем и указывает на каталог в файловой системе. С каждым хранилищем связаны настройки хранения, определяющие, сколько снимков резервных копий для каждого интервала времени (ежечасно, ежедневно, еженедельно, ежемесячно, ежегодно) хранить в этом хранилище.

Для создания хранилища в веб-интерфейсе, необходимо нажать кнопку **Add Datastore** (**Добавить хранилище данных**) в боковом меню (в разделе **Datastore**). В открывшемся окне необходимо указать:

- **Имя** — название хранилища данных;
- **Backing Path** — путь к каталогу, в котором будет создано хранилище данных;
- **GC Schedule** — частота, с которой запускается сборка мусора;
- **Prune Schedule** — частота, с которой происходит обрезка;
- **Prune Options** — 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** — пустой файл, используемый для блокировки процесса;

- каталог **.chunks** — содержит подкаталоги, с именами от 0000 до ffff. В этих каталогах будут храниться фрагментированные данные, после выполнения операции резервного копирования.

22.4. Управление трафиком

Создание и восстановление резервных копий может привести к большому трафику и повлиять на работу других пользователей сети или общих хранилищ.

PBS позволяет ограничить входящий (например, резервное копирование) и исходящий (например, восстановление) сетевой трафик из набора сетей. При этом можно настроить определенные периоды, в которые будут применяться ограничения.



Примечание

Ограничение скорости не влияет на задания синхронизации. Чтобы ограничить входящий трафик, создаваемый заданием синхронизации, необходимо настроить ограничение скорости входящего трафика для конкретного задания.

Настройка правила управления трафиком в веб-интерфейсе:

Добавить: Traffic Control Rule

Имя:

Комментарий:

Rate In: MiB/s

Burst In: MiB/s

Rate Out: MiB/s

Burst Out: MiB/s

Network(s):

Timeframes:

Time Start	Time End	Mon	Tue	Wed	Thu	Fri	Sat	Sun	
08:00	19:00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="X"/>

Управление трафиком в консоли:

- создать правило управления трафиком для ограничения всех клиентов IPv4 (сеть 0.0.0.0/0) до 100 МБ/с:

```
# proxmox-backup-manager traffic-control create rule0 --network 0.0.0.0/0 \
--rate-in 100MB --rate-out 100MB \
--comment "Default rate limit (100MB/s) for all clients"
```

- ограничить правило временными рамками:

```
# proxmox-backup-manager traffic-control update rule0 \
--timeframe "mon..fri 8-19"
```

■ вывести список текущих правил:

```
# proxmox-backup-manager traffic-control list
```

■ удалить правило:

```
# proxmox-backup-manager traffic-control remove rule0
```

■ показать состояние (текущую скорость передачи данных) всех настроенных правил:

```
# proxmox-backup-manager traffic-control traffic
```

22.5. Управление пользователями

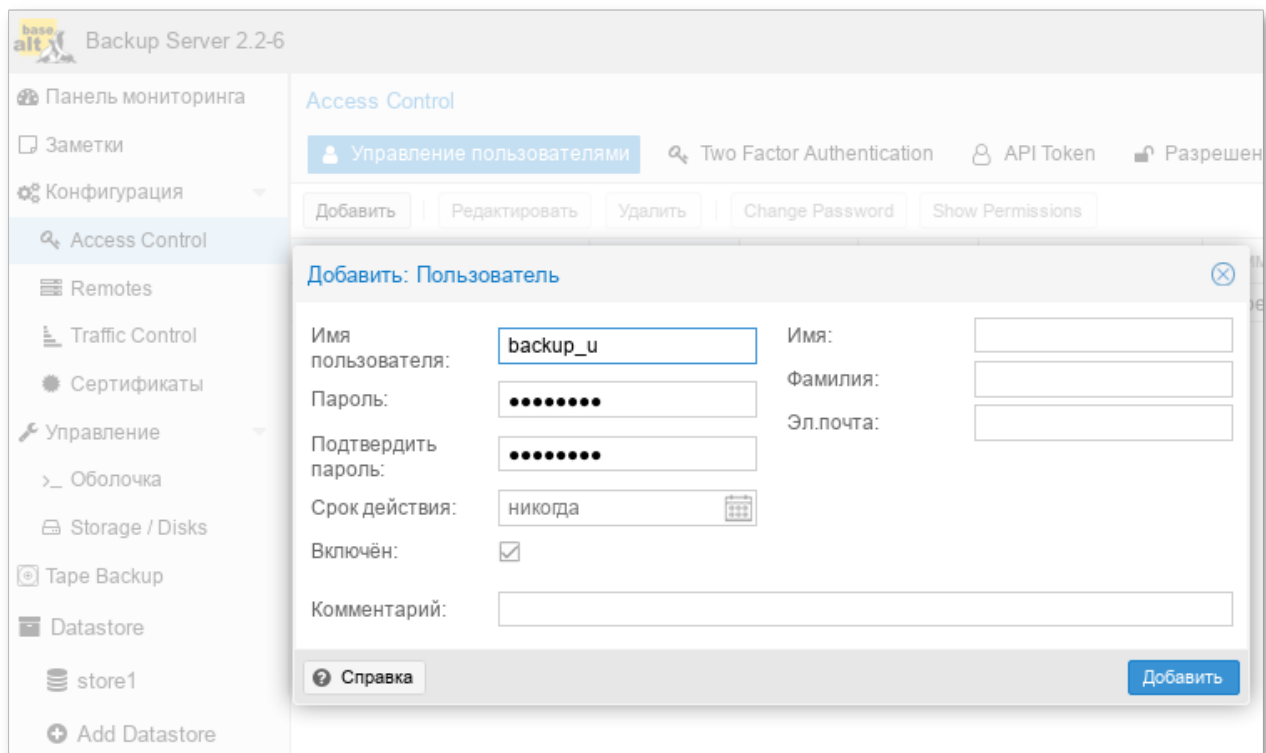
PBS поддерживает следующие области (методы) аутентификации:

- **Стандартная аутентификация Linux PAM (Linux PAM standart authentication)** — при использовании этой аутентификации системный пользователь должен существовать (должен быть создан, например, с помощью команды **adduser**). Пользователь аутентифицируется с помощью своего обычного системного пароля;
- **Сервер аутентификации Proxmox Backup (Proxmox Backup authentication server)** — аутентификация Proxmox Backup Server. Хэшированные пароли хранятся в файле **/etc/proxmox-backup/shadow.json**.

После установки PBS существует один пользователь **root@pam**, который соответствует суперпользователю ОС. Суперпользователь имеет неограниченные права, поэтому рекомендуется добавить других пользователей с меньшими правами.

22.5.1. 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
```

22.5.2. API-токены

Любой аутентифицированный пользователь может генерировать API-токены, которые, в свою очередь, можно использовать для настройки клиентов резервного копирования вместо прямого указания имени пользователя и пароля.

Назначение API-токенов:

- » простой отзыв в случае компрометации клиента;
- » возможность ограничить разрешения для каждого клиента/токена в рамках разрешений пользователей.

Генерация API-токена в веб-интерфейсе:

Access Control

Управление пользователями Two Factor Authentication API Token Разрешения Realms

Добавить Редактировать Удалить Show Permissions

Пользователь ↑ Token name ↑ Включён Срок д... Комментарий

Добавить: API токен

Пользователь: backup_u@pbs Срок действия: никогда

Token Name: client1 Включён: ☒

Комментарий:

Справка Добавить

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.

Token Secret

Token ID: backup_u@pbs!client1

Secret: ff13e5e0-30df-4a70-99f1-c62b13803769

Please record the API token secret - it will only be displayed now

Copy Secret Value



Примечание

Отображаемое секретное значение необходимо сохранить, так как после создания токена его нельзя будет отобразить снова.

Создание API-токена в консоли:

```
# proxmox-backup-manager user generate-token backup_u@pbs client1
Result: {
  "tokenid": "backup_u@pbs!client1",
  "value": "ff13e5e0-30df-4a70-99f1-c62b13803769"
}
```

22.5.3. Управление доступом

По умолчанию новые пользователи и API-токены не имеют никаких разрешений. Добавить разрешения можно, назначив роли пользователям/токенам для определенных объектов, таким как хранилища данных или удаленные устройства.

Роль — это список привилегий. В PBS предопределён ряд ролей:

- NoAccess — нет привилегий (используется для запрета доступа);
- Admin — все привилегии;
- Audit — доступ только для чтения;
- DatastoreAdmin — все привилегии для хранилищ данных;
- DatastoreAudit — просмотр настроек хранилищ и их содержимых, без возможности чтения фактических данных;
- DatastoreReader — просмотр содержимого хранилища, восстановление данных;
- DatastoreBackup — создание и восстановление собственных резервных копий;
- DatastorePowerUser — создание, восстановление и удаление собственных резервных копий;
- RemoteAdmin — все привилегии для удалённых PBS;
- RemoteAudit — просмотр настроек удалённых PBS;
- RemoteSyncOperator — 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 (':'):

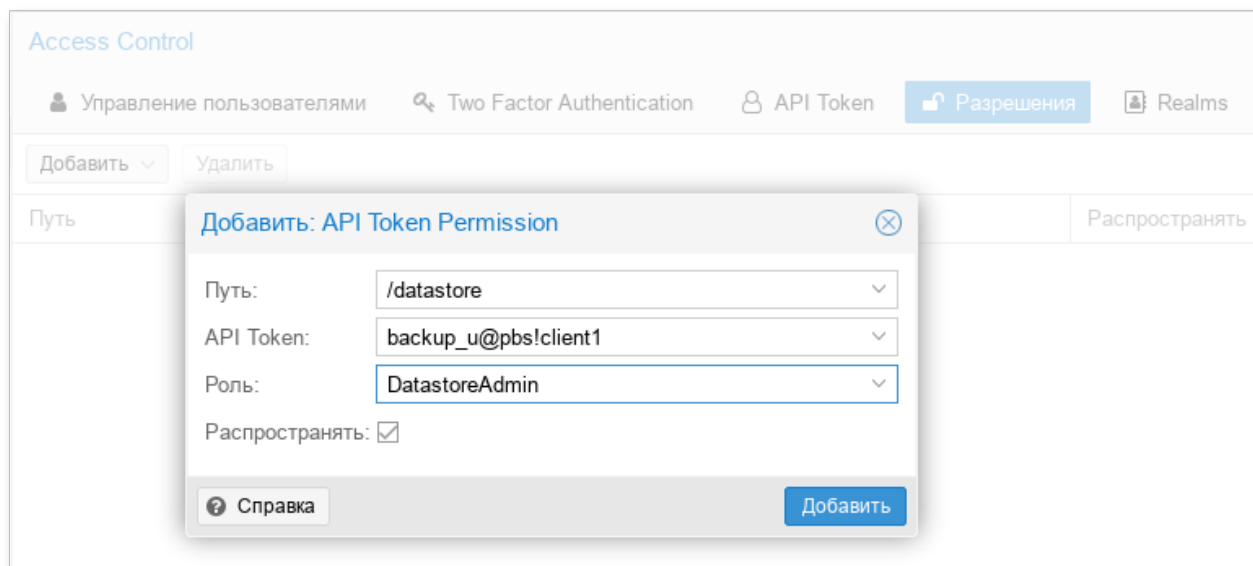
```
acl:1:/datastore:backup_u@pbs!client1:DatastoreAdmin
```

В каждом поле представлены следующие данные:

- идентификатор acl;
- 1 или 0 — включено или отключено;
- объект, на который установлено разрешение;

- »пользователи/токены, для которых установлено разрешение;
- »устанавливаемая роль.

Добавление разрешения в веб-интерфейсе (**Конфигурация** → **Access Control (Контроль доступа)** вкладка **Разрешения**):



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 (*)
```




Примечание

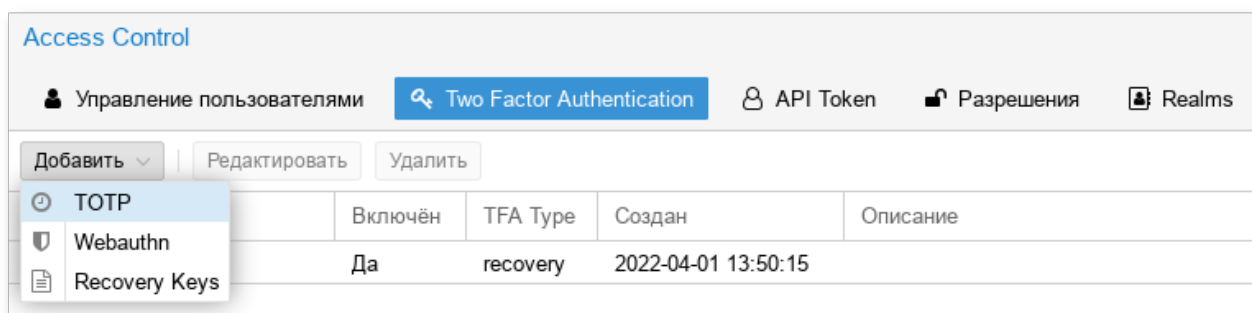
Для токенов требуются собственные записи ACL. Токены не могут делать больше, чем их соответствующий пользователь.

22.5.4. Двухфакторная аутентификация



Примечание

Двухфакторная аутентификация реализована только для веб-интерфейса.



PBS поддерживает три метода двухфакторной аутентификации:

- »TOTP (одноразовый пароль на основе времени) — для создания этого кода используется алгоритм одноразового пароля с учетом времени входа в систему (код меняется каждые 30 секунд);
- »WebAuthn (веб-аутентификация) — реализуется с помощью различных устройств безопасности, таких как аппаратные ключи или доверенные платформенные модули (TPM). Для работы веб-аутентификации необходим сертификат HTTPS;
- »Recovery Keys (одноразовые ключи восстановления) — список ключей, каждый из которых можно использовать только один раз. В каждый момент времени у пользователя может быть только один набор одноразовых ключей.

Настройка аутентификации TOTP:

- »Добавление аутентификации TOTP на сервере:

Add a TOTP login factor

Пользователь:

backup_u@pbs

Описание:

smartphone

Secret:

LR4IVYEKVWI566ZRQ6XYRNLYKHCATG5S

Randomize

Issuer Name:

Proxmox



Verify Code:

862425

Справка

Добавить

»Использование TOTP при аутентификации пользователя:

Second login factor required

WebAuthn

TOTP App

Recovery Key

Please enter your TOTP verification code:

236712

Confirm Second Factor

Настройка аутентификации Recovery Key:

»Создание набора ключей:

Recovery Keys

0: 73e9-f51c-1c27-a3b6

1: f5d3-7d09-0d69-e144

2: 077d-7ac9-7278-2daf

3: c9ac-1286-cf49-bea4

4: 6556-a077-90e6-5cb4

5: d294-0b06-9f1b-fdf9

6: f4c4-54a3-981f-d452

7: 000e-7f7a-7ef2-5fd7

8: 7859-7683-7676-aa6a

9: b700-5885-ce50-8fb5

Please record recovery keys - they will only be displayed now

Copy Recovery Keys

Print Recovery Keys

»Использование Recovery Key при аутентификации пользователя:

Second login factor required

WebAuthn

TOTP App

Recovery Key

Available recovery keys: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

Please enter one of your single-use recovery keys:

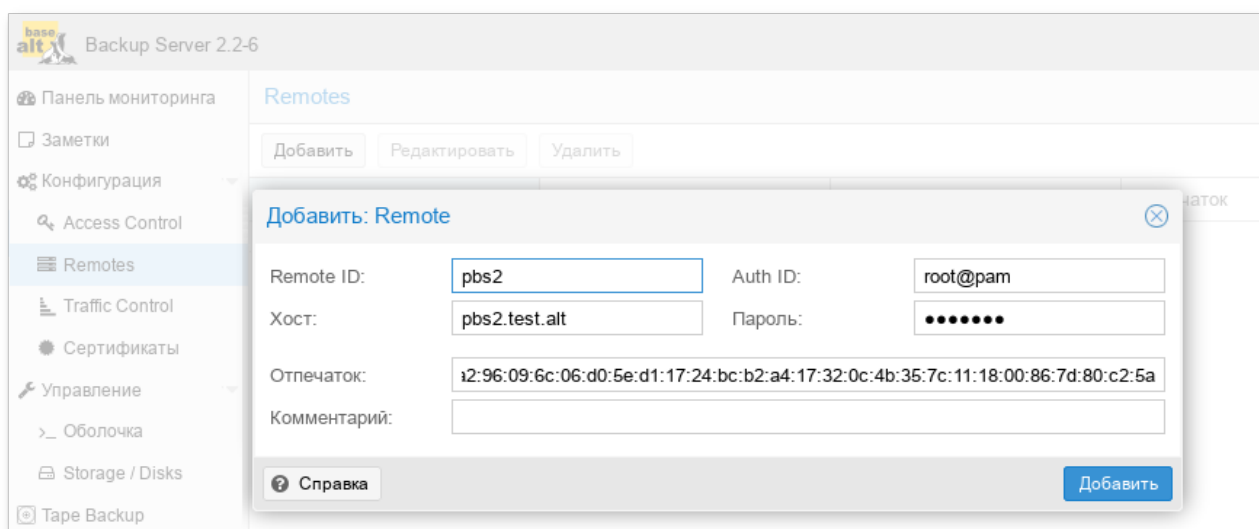
Confirm Second Factor

22.6. Управление удалёнными PBS

Хранилища данных с удалённого сервера можно синхронизировать с локальным хранилищем с помощью задачи синхронизации.

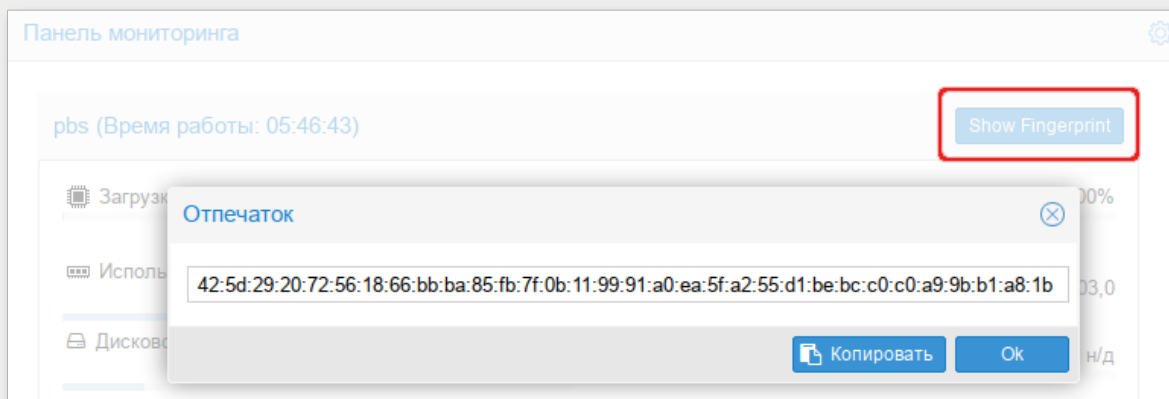
Информация о конфигурации удалённых PBS хранится в файле **/etc/proxmox-backup/remote.cfg**.

Для добавления удалённого PBS в веб-интерфейсе следует перейти в раздел **Конфигурация** → **Remotes** и нажать кнопку **Добавить**:



Примечание

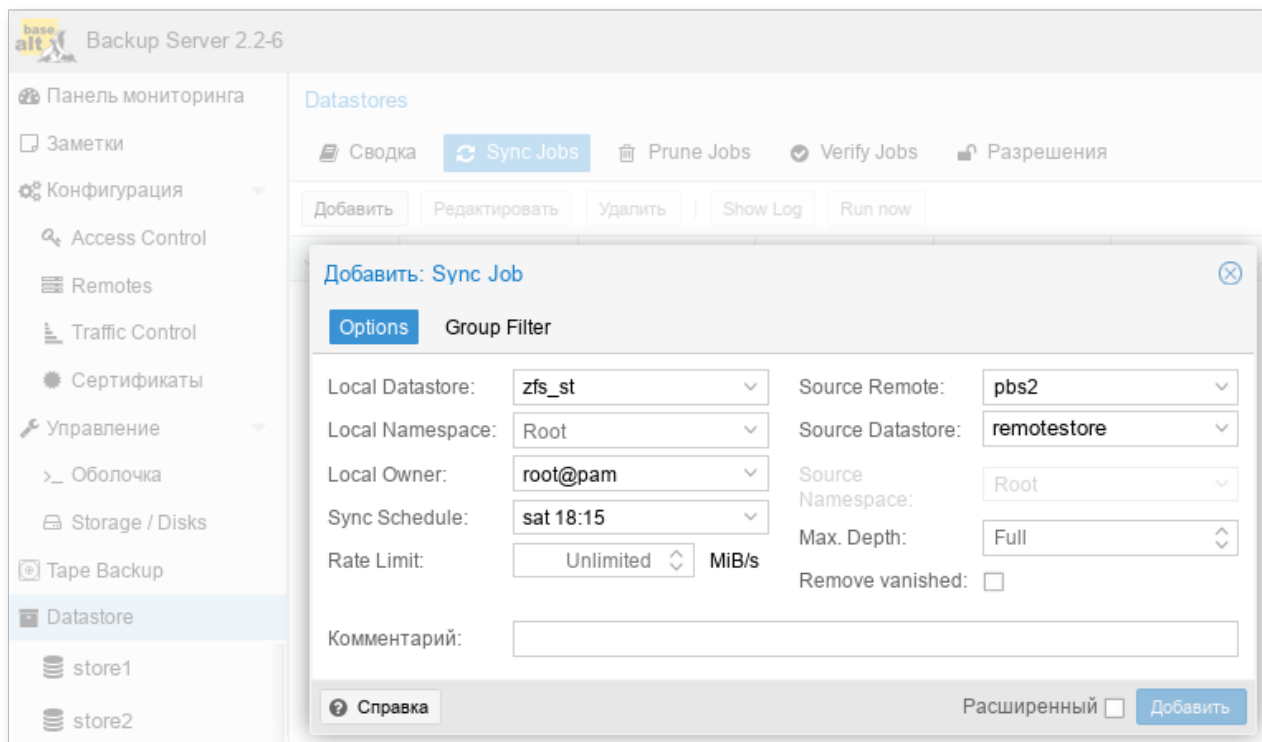
Отпечаток TLS-сертификата можно получить в веб-интерфейсе удалённого PBS:



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**).

22.7. Клиент резервного копирования

Клиент резервного копирования использует следующий формат для указания репозитория хранилища данных на сервере резервного копирования (где имя пользователя указывается в виде user@realm):

```
[ [пользователь@] сервер[:порт]: ]datastore
```

Значение по умолчанию для пользователя — root@pam. Если сервер не указан, используется — localhost.

Указать репозиторий можно, передав его в параметре --repository, или установив переменную окружения PBS_REPOSITORY, например:

```
# export PBS_REPOSITORY=pbs.test.alt:store1
```

Таблица 22.1. Примеры репозитория

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

Пример	Пользователь	Хост:Порт	Хранилище
192.168.0.123:1234:store1	root@pam	192.168.0.123:1234	store1

22.7.1. Создание резервной копии

В этом разделе рассмотрено, как создать резервную копию внутри машины (физического хоста, VM 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 — для образов блочных устройств.

Команда создания резервной копии блочного устройства:

```
$ proxmox-backup-client backup mydata.img:/dev/mylvm/mydata
```

22.7.2. 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.pxdar.didx
user_s.pxdar: had to backup 667.04 MiB of 667.04 MiB (compressed 190.028 MiB) in
21.16s
user_s.pxdar: 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
```

Содержимое хранилища store1:

Datastore: store1

Сводка **Содержимое** Prune & GC Sync Jobs Verify Jobs Параметры Разрешения

Перезагрузить Verify All Prune All Поиск group, date or owner

Backup Group ↑	Комментар...	Actions ↑	Backup Time ↑	Размер	Кол...	Owner	Encrypted	Verify State
host/host-01		V. [иконки]	2022-04-28 14:33:04	667.15 MiB	2	root@pam	Mixed	None
host/host-01/2022-0...		V. [иконки]	2022-04-28 14:27:01	667.15 MiB		root@pam	Her	None
host/host-01/2022-0...		V. [иконки]	2022-04-28 14:33:04	667.15 MiB		root@pam	Encrypted	None
catalog.pcat1.didx		[иконка]		109.97 KiB			Encrypted	
index.json.blob		[иконка]		501 B			Signed	
user_s.pxdar.didx		[иконка]		667.04 MiB			Encrypted	
host/pbs		V. [иконки]	2022-04-01 16:25:29	98.49 MiB	2	root@pam	Mixed	None

22.7.3. 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.pxdar
host/host-01/2022-04-28T12:33:04Z  667.148 MiB  catalog.pcat1 index.json
user_s.pxdar
```

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.pxdar в каталог /home/user/restore:

```
$ proxmox-backup-client restore host/host-01/2022-04-28T12:27:01Z user.pxdar /
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** — найти все файлы с расширением .txt и добавить соответствующие шаблоны в список для последующего восстановления;
- » **list-selected** — вывести шаблоны на экран;
- » **restore-selected /home/user/restore/** — восстановить все файлы в архиве, соответствующие шаблонам в **/home/user/restore/** на локальном хосте;
- » **restore /home/user/conf/ --pattern *.conf** — восстановить все файлы с расширением .conf в **/home/user/conf/** на локальном хосте.

22.7.4. Вход и выход

При первой попытке получить доступ к серверу с использованием команды **proxmox-backup-client**, потребуется ввести пароль пользователя. Сервер проверяет учётные данные и отправляет билет, действительный в течение двух часов. Клиент использует этот билет для последующих запросов к этому серверу.

Можно вручную инициировать вход/выход. Команда входа:

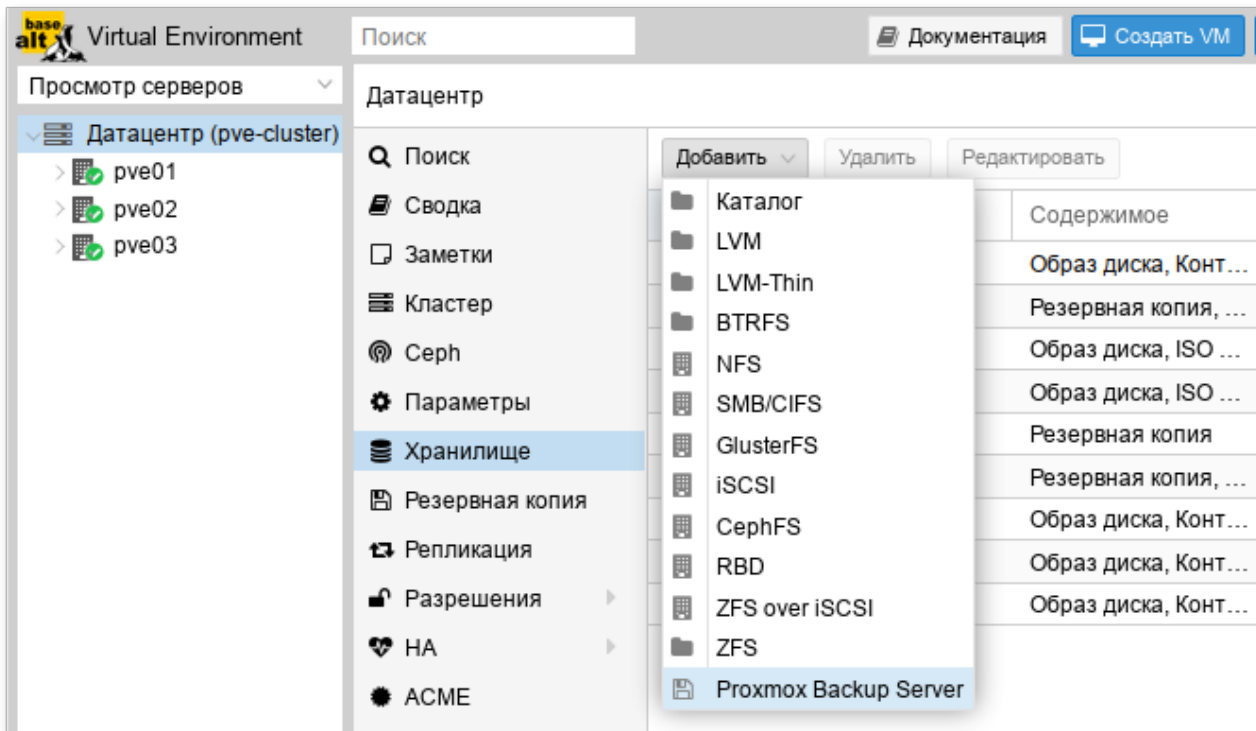
```
$ proxmox-backup-client login --repository pbs.test.alt:store1
Password for "root@pam": *****
```

Удалить билет:

```
$ proxmox-backup-client logout --repository pbs.test.alt:store1
```


22.8. Интеграция с PVE

PBS можно интегрировать в автономную или кластерную установку PVE, добавив его в качестве хранилища:



Диалог создания хранилища pbs_backup типа «Proxmox Backup Server» для хранения резервных копий:

Добавить: Proxmox Backup Server

Общее Backup Retention Encryption

ID: pbs_backup Узлы: Все (Без ограничений)

Сервер: 192.168.0.123 Включить: ☒

Имя пользователя: root@pam Содержимое: backup

Пароль: Password Datastore: store2

Namespace: Root

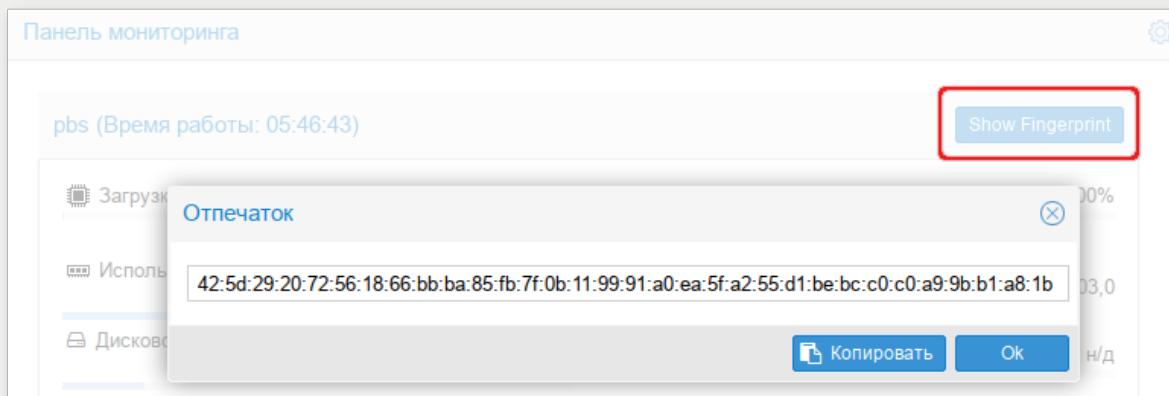
Отпечаток: :a9:18:66:bb:ba:85:fb:7f:0b:11:99:ea:5f:a2:55:d1:be:bc:c0:c0:a9:9b:b1:a8:1b

Справка Добавить



Примечание

Отпечаток TLS-сертификата можно получить в веб-интерфейсе сервера резервного копирования:



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 VM и контейнеров в это хранилище так же, как и в любые другие хранилища.

Глава 23. Система резервного копирования UrBackup

23.1. Установка UrBackup

23.2. Настройка резервного копирования

23.3. Создание резервных копий

23.4. Утилита urbackupclientctl

UrBackup — это простое в настройке кроссплатформенное клиент-серверное программное обеспечение, позволяющее управлять резервным копированием для компьютеров и операционных систем различных типов. UrBackup позволяет создавать инкрементные и полные резервные копии, как целых разделов, так и отдельных каталогов, с возможностью выбора файлов, которые попадут в архив, а также делать снапшоты разделов жесткого диска.



Примечание

В настоящее время резервные копии образов (снапшоты) работают только с томами в формате NTFS и с клиентами Windows. Резервное копирование образов предназначено в основном для резервного копирования загрузочного тома (C:) систем Windows. Для архивирования других данных следует воспользоваться резервным копированием файлов.

Для управления настройкой резервного копирования и резервными копиями используется веб-интерфейс.

23.1. Установка UrBackup

23.1.1. Сервер UrBackup

Установить сервер UrBackup:

```
# apt-get install urbackup-server
```

Создать каталог для резервных копий:

```
# mkdir -p /mnt/backups/urbackup
```

Каталог должен принадлежать пользователю urbackup и у этого пользователя должны быть права на чтение/запись:

```
# chown -R urbackup:urbackup /mnt/backups/urbackup
```

Добавить UrBackup-сервер в автозапуск и запустить его:

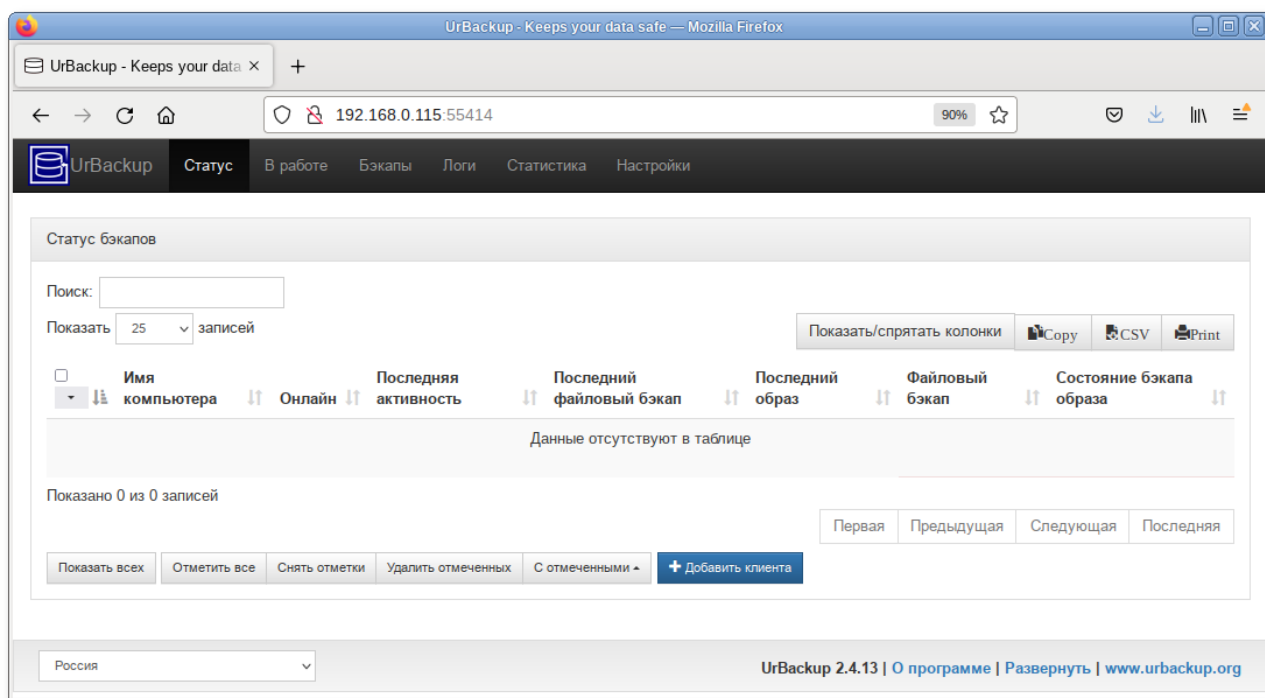
```
# systemctl enable --now urbackup-server
```



Примечание

UrBackup по умолчанию прослушивает порты 55413 и 55414.

Веб-интерфейс UrBackup будет доступен по адресу **http://<ip-сервера>:55414:**



Важно

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.



Примечание

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**):

23.1.2. 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**:


UrBackup
Статус
В работе
Бэкапы
Логи
Статистика
Настройки

Статус бэкапов

Поиск:
Показать 25 записей

Показать/скрыть колонки
Copy
CSV
Print

<input type="checkbox"/>	Имя компьютера	Онлайн	Последняя активность	Последний файловый бэкап	Последний образ	Файловый бэкап	Состояние бэкапа образа
<input type="checkbox"/>	host-155.test.alt	Да	20.01.22 14:08	Никогда	Никогда	Нет резервной копии	Нет резервной копии

Показать 1 по 1 из 1

Первая
Предыдущая
1
Следующая
Последняя

Показать всех
Отметить все
Снять отметки
Удалить отмеченных
С отмеченными
+ Добавить клиента

23.2. Настройка резервного копирования

В веб-интерфейсе на вкладке **Настройки** → **Главные** можно изменять настройки UrBackup. Некоторые настройки влияют только на сервер резервного копирования. Остальные настройки влияют и на клиентов резервного копирования, для этих настроек администратор может установить значения по умолчанию или переопределить настройки клиента.

На вкладке **Сервер** можно указать каталог для хранения резервных копий:

UrBackup

Статус

В работе

Бэкапы

Логи

Статистика

Настройки

Главные

Почта

LDAP/AD

Пользователи

+ Добавить новую группу

Сервер

Файловые бэкапы

Образы

Права доступа

Клиент

Архив

Alerts

Интернет

Дополнительно

Путь для хранения бэкапов:

/mnt/backups/urbackup

URL сервера:

Не делать бэкап образа:

☐

Не делать файловый бэкап:

☐

Автоматически выключать сервер:

☐

Скачать клиент с сервера обновлений:

☒

Оповещать о новой версии:

☒

Автоматическое обновление клиентов:

☒

Максимум одновременных бэкапов:

100

Максимум активных клиентов:

10000

Расписание очистки бэкапов:

1-7/3-4

?

Автоматически бэкапить базу данных UrBackup:

☒

Общая максимальная скорость для локальной сети:

-

MBit/s


Общее ограничение файловой системы:

95%

?

Сохранить

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 настраиваются интервалы резервного копирования.


UrBackup
Статус
В работе
Бэкапы
Логи
Статистика
Настройки

Главные
Почта
LDAP/AD
Пользователи
+ Добавить новую группу

Сервер
Файловые бэкапы
Образы
Права доступа
Клиент
Архив
Alerts
Интернет
Дополнительно

Интервал создания инкрементальных файловых бэкапов:

часов

☐ Отключить

Интервал создания полных бэкапов файлов:

дней

☐ Отключить

Максимальное количество инкрементальных бэкапов файлов:

Минимальное количество инкрементальных бэкапов файлов:

Максимальное количество полных бэкапов файлов:

Минимальное количество полных бэкапов файлов:

Исключить из бэкапа (по маске):

?

Включить в бэкап (по маске):

?

Каталоги по умолчанию для бэкапа:

?

Directories to backup are optional by default:
☐

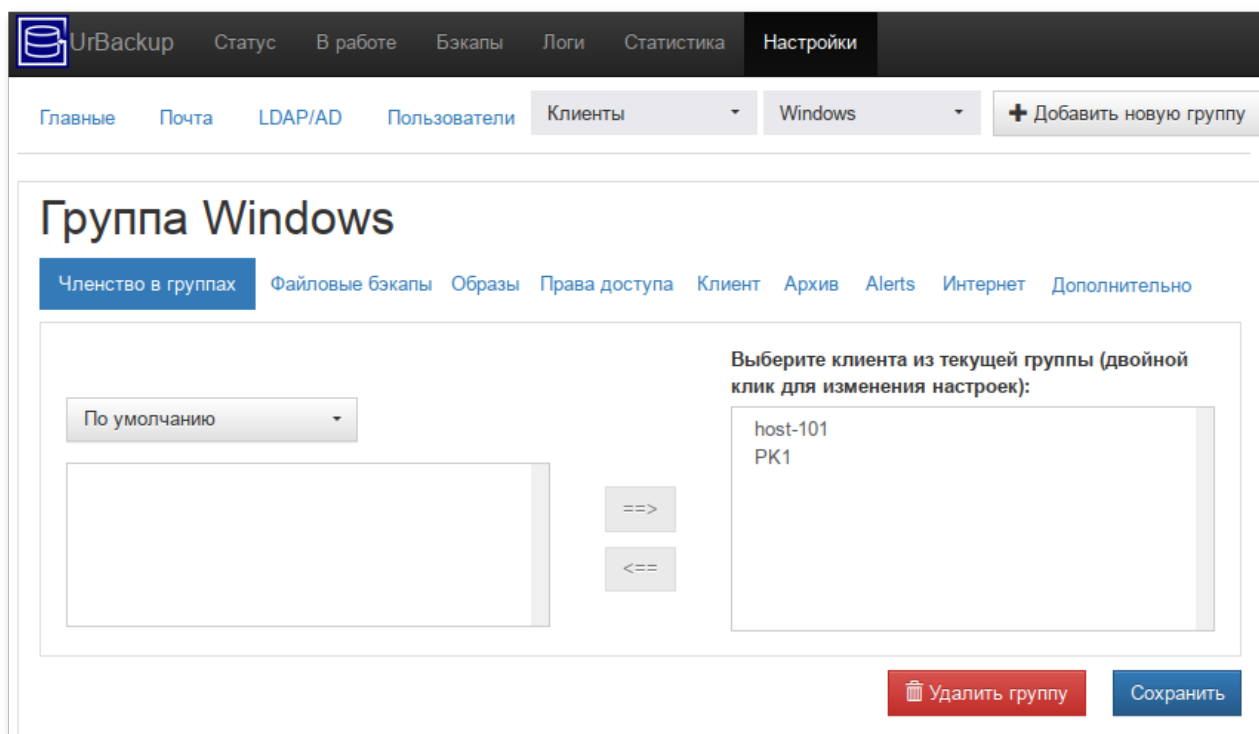
Сохранить

На вкладке **Клиент** (поле **Расписание**) можно установить окно резервного копирования, в пределах которого сервер будет стараться выполнять задания. Начатое задание будет выполняться до завершения, даже если оно не вписывается в указанное время. Примеры окна резервного копирования:

- » 1-7/0-24 — резервное копирование может производиться в любое время;
- » 1-5/8:00-9:00, 19:30-20:30;6,7/0-24 — резервное копирование в рабочие дни может производиться с 8 до 9 и с 19:30 до 20:30, а в субботу и воскресенье в любое время.

Клиенты могут сами инициировать процесс резервного копирования в любой момент (см. ниже описание утилиты **urbackupclientctl**).


Для более удобного администрирования можно создать несколько групп, распределить клиенты по группам, и задавать настройки отдельно для каждой группы клиентов:



23.3. 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:


UrBackup

Статус
В работе
Бэкапы
Логи
Статистика
Настройки

Статус бэкапов

Поиск:

Показать 25 записей

Показать/скрыть колонки
Copy
CSV
Print

	Имя компьютера	Онлайн	Последняя активность	Последний файловый бэкап	Последний образ	Файловый бэкап	Состояние бэкапа образа
<input type="checkbox"/>	PK1	Да	21.01.22 15:38	Никогда	21.01.22 14:56	Disabled	Ok
<input type="checkbox"/>	host-101	Нет	21.01.22 11:00	Никогда	Никогда	No paths to backup configured	Не поддерживается
<input checked="" type="checkbox"/>	host-155.test.alt	Да	21.01.22 15:38	21.01.22 12:27	Никогда	Ok	Не поддерживается
<input type="checkbox"/>			01.22 10:23	21.01.22 09:15	Никогда	Ok	Не поддерживается

Инкрементальный файловый бэкап

Полный файловый бэкап

Инкрементальный образ

Полный образ


Удалить клиента

П


Первая
Предыдущая
1
Следующая
Последняя

Показать всех
Отметить все
Снять отметки
Удалить отмеченных
С отмеченными
+ Добавить клиента

Более подробно отслеживать активность резервного копирования можно на вкладках **В работе**, **Бэкапы**, **Логи**.


UrBackup
Статус
В работе
Бэкапы
Логи
Статистика
Настройки

В работе


Имя компьютера	Действие	Подробности	Прогресс	Расчетное время выполнения	Скорость	Файлов в очереди
PK1	Полный образ	Том: C:	<div>33%</div> <div>8.58 GB / 26.08 GB</div>	22 Минут	 <div>108.71 Mbit/s</div>	0

Стоп
Показать лог

Последняя активность

ID	Имя компьютера	Действие	Подробности	Время начала	Продолжительность	Использовано памяти
3	host16.test.alt	Полный файловый бэкап	-	21.01.22 08:43	5 min	5.02 GB
1	host-155.test.alt	Восстановление файлов	Path:	20.01.22 16:07	1 min	-
2	host-155.test.alt	Инкрементальный файловый бэкап	-	20.01.22 15:40	2 min	104.86 MB
1	host-155.test.alt	Полный файловый бэкап	-	20.01.22 15:08	1 min	2.15 GB


Отчёты/содержимое резервных копий можно посмотреть на вкладке **Бэкапы**:


UrBackup
Статус
В работе
Бэкапы
Логи
Статистика
Настройки

Клиенты

Имя компьютера	Последний файловый бэкап
host-101	-
host-155.test.alt	21.01.22 12:27
host16.test.alt	21.01.22 09:15

Выбрав клиента, можно посмотреть список его резервных копий:


UrBackup
Статус
В работе
Бэкапы
Логи
Статистика
Настройки

Клиенты > host-155.test.alt

Файловый бэкап


Время бэкапа	Инкрементальный	Размер	Архивировано?	Действия
21.01.22 12:27	Да	170.21 MB	<input type="checkbox"/>	
20.01.22 15:40	Да	104.86 MB	<input checked="" type="checkbox"/>	
20.01.22 15:08	Нет	2.15 GB	<input type="checkbox"/>	Удалить



Примечание

Если отметка в столбце **Архивировано** установлена, резервная копия архивируется. Пока резервная копия заархивирована, её нельзя удалить средствами UrBackup.

Выбрав резервную копию, можно просмотреть её содержимое:


UrBackup
Статус
В работе
Бэкапы
Логи
Статистика
Настройки

Клиенты > host-155.test.alt > 20.01.22 15:40

Файл	Размер	Создано	Последнее изменение	Последний доступ	
home	-	07.12.21 16:57	20.01.22 14:00		Список
var	-	03.12.21 08:54	20.01.22 14:02		Список

Скачать папки в ZIP архиве

Резервные копии сохраняются в каталоге, который был указан в веб-интерфейсе. В этом каталоге для каждого клиента создается свой подкаталог. Резервные копии файлов находятся в подкаталогах вида <YYMMDD-ННММ>. Каталог **current** является ссылкой на последнюю резервную копию. Резервные копии папок с файлами сохраняются в открытом виде. Образы дисковых разделов хранятся в виде файлов в формате vhdz (имя файла будет иметь вид Image_<Drive>_<YYMMDD-ННММ>.vhdz).

23.4. Утилита `urbackupclientctl`

Для работы с UrBackup на клиенте предназначена утилита **`urbackupclientctl`**:

- ▀ **`urbackupclientctl start`** — запустить инкрементное/полное резервное копирование;
- ▀ **`urbackupclientctl status`** — получить текущий статус резервного копирования;
- ▀ **`urbackupclientctl browse`** — просмотр списка резервных копий и файлов в резервных копиях;
- ▀ **`urbackupclientctl restore-start`** — восстановить файлы из резервной копии;
- ▀ **`urbackupclientctl set-settings`** — установить параметры резервного копирования;
- ▀ **`urbackupclientctl add-backupdir`** — добавить новый каталог в список каталогов, для которых выполняется резервное копирование;
- ▀ **`urbackupclientctl list-backupdirs`** — вывести список каталогов, для которых выполняется резервное копирование;
- ▀ **`urbackupclientctl remove-backupdir`** — удалить каталог из списка 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.
```

Часть V. Настройка системы

Если VM планируется использовать как полноценный сервер и требуется удобная настройка разных сервисов, то для управления настройками установленной системы можно воспользоваться **Центром управления системой**.

Центр управления системой (ЦУС) представляет собой удобный интерфейс для выполнения наиболее востребованных административных задач: добавление и удаление пользователей, управление системными службами, просмотр информации о состоянии системы и т.п.

Содержание

- 24. Центр управления системой
- 25. Обслуживание сервера
- 26. Соединение удалённых офисов (OpenVPN-сервер)
- 27. Доступ к службам сервера из сети Интернет
- 28. Статистика
- 29. Прочие возможности ЦУС
- 30. Права доступа к модулям

Глава 24. Центр управления системой

- 24.1. Установка и запуск веб-интерфейса ЦУС
- 24.2. Применение центра управления системой

24.1. Установка и запуск веб-интерфейса ЦУС

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

Необходимо установить пакет *alterator-fbi*:

```
# apt-get install alterator-fbi
```



Примечание

Для работоспособности ЦУС необходимо задать пароль root. Сделать это можно, выполнив команды:

```
# passwd -u root; passwd root
```

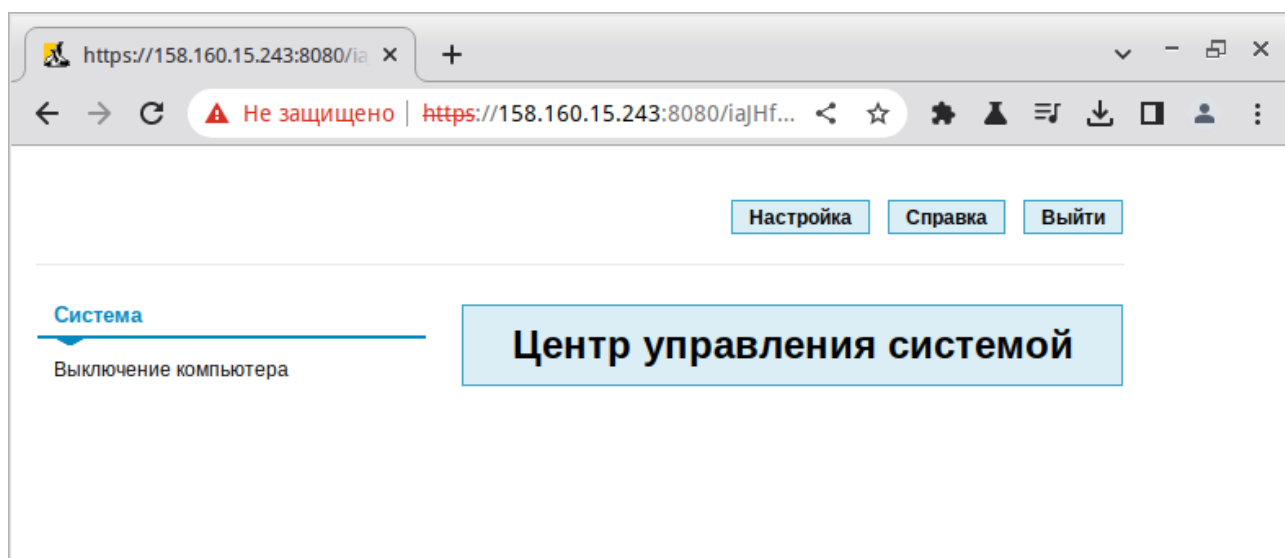
Для запуска веб-ориентированного интерфейса следует запустить сервисы ahttpd и alteratord:

```
# systemctl enable --now ahttpd  
# systemctl enable --now alteratord
```

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

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.



ЦУС состоит из независимых диалогов-модулей. Каждый модуль отвечает за настройку определённой функции или свойства системы.

Модули можно дополнительно загружать и удалять как обычные программы:

```
# apt-get install alterator-datetime
# apt-get remove alterator-datetime
```

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*
```

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 включённым в него модулям. Об использовании самого интерфейса системы управления можно прочитать, нажав на кнопку **Справка** на начальной странице центра управления системой.



Предупреждение

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

24.2. Применение центра управления системой

Вы можете использовать ЦУС для разных целей, например:

- ▀ Настройки **Даты и времени** ([datetime](#));
- ▀ Управления выключением и перезагрузкой компьютера ([ahttpd-power](#));
- ▀ Управления **Системными службами** ([services](#));
- ▀ Просмотра **Системных журналов** ([logs](#));
- ▀ Настройки **OpenVPN-подключений** ([openvpn-server](#) и [net-openvpn](#));
- ▀ Создания, удаления и редактирования учётных записей **Пользователей** ([users](#));
- ▀ Настройки ограничения **Использования диска (квоты)** ([quota](#)).

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

Глава 25. Обслуживание сервера

25.1. Мониторинг состояния системы

25.2. Системные службы

25.3. Обновление системы

25.4. Обновление ядра ОС

25.5. Обновление систем, не имеющих выхода в Интернет

25.6. Локальные учётные записи

25.7. Администратор системы

25.8. Дата и время

25.9. Агент наблюдения

25.10. Ограничение использования диска

25.11. Выключение и перезагрузка компьютера

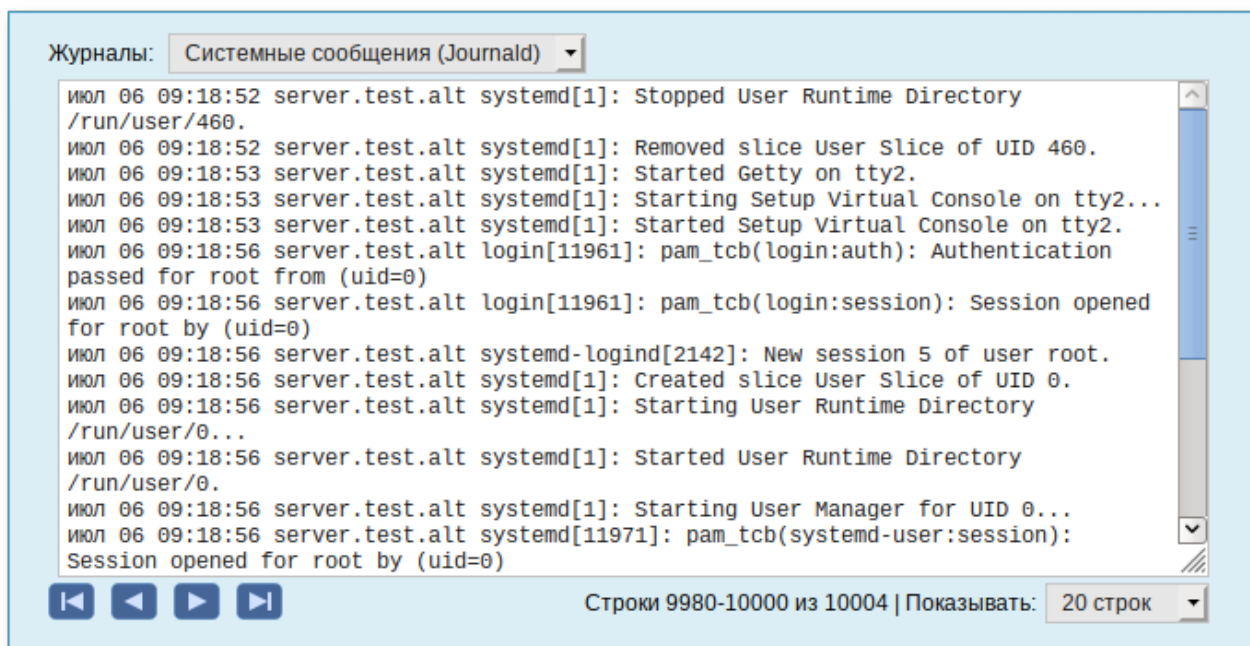
Для безотказной работы всего домена очень важно следить за корректной работой его центрального звена — сервера под управлением Альт Сервер. Регулярный мониторинг состояния сервера, своевременное резервное копирование, обновление установленного ПО являются важной частью комплекса работ по обслуживанию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

25.1. 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.

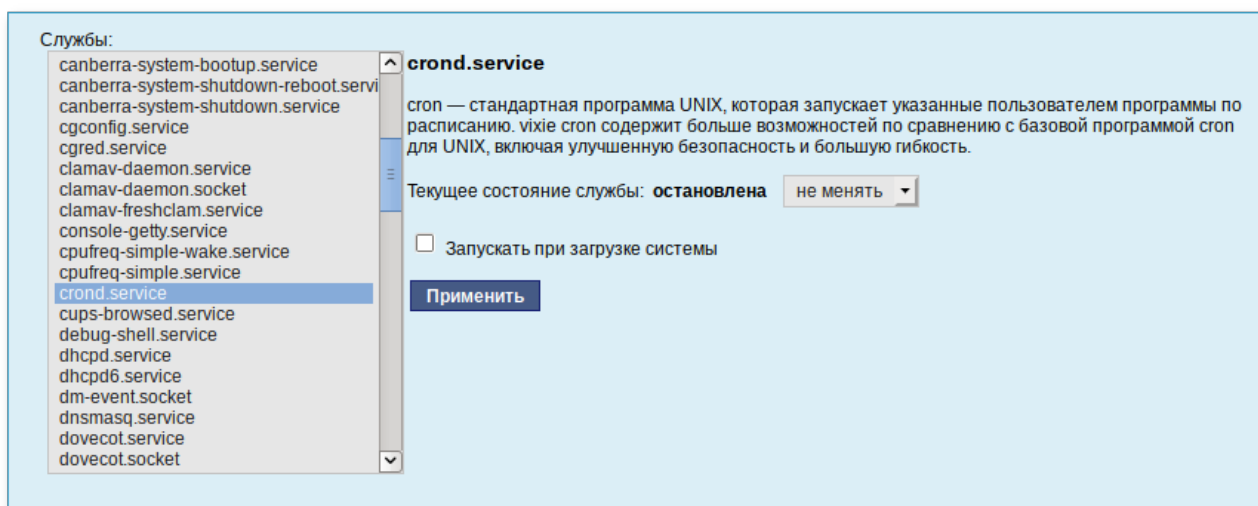
Различные журналы могут быть выбраны из списка **Журналы**.



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

25.2. 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.

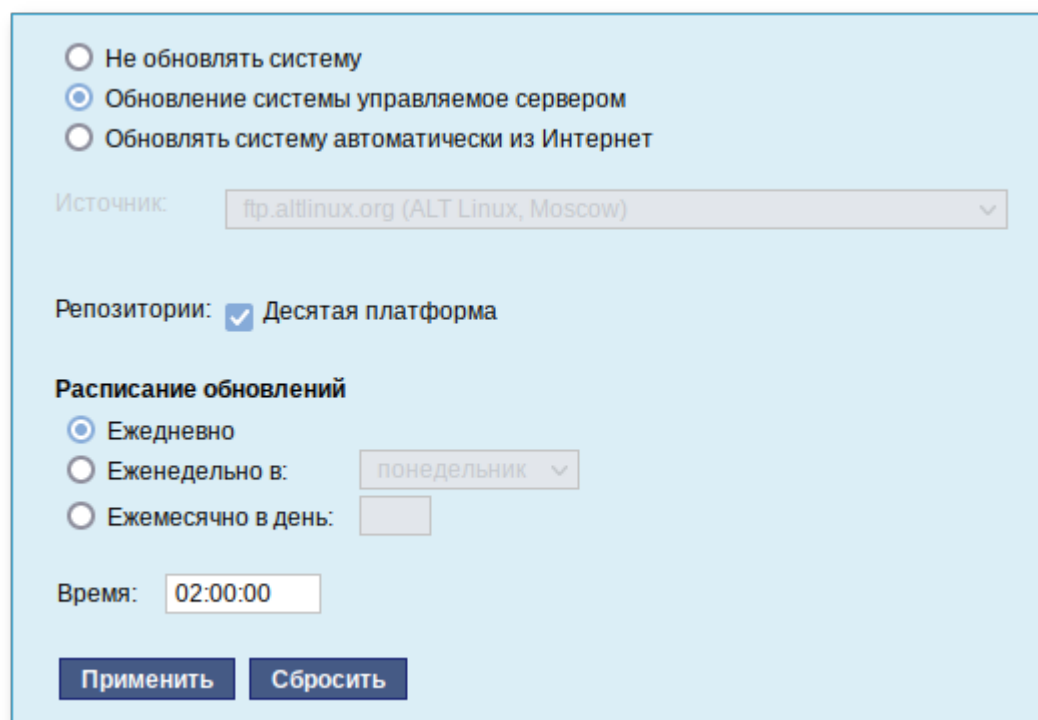


После выбора названия службы из списка отображается описание данной службы, а также текущее состояние: Работает/Остановлена/Неизвестно.

25.3. 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).



Примечание

Рабочие станции «видят» локальный сервер обновлений, при выборе режима **Обновление системы управляемое сервером**, если они находятся в домене (при этом сервер обновлений должен быть настроен на **Опубликовать как репозиторий для автоматических обновлений**).

Процесс обновления системы будет запускаться автоматически согласно заданному расписанию.



Примечание

Чтобы указать в качестве сервера обновлений локально настроенный источник, необходимо выбрать режим **Обновлять систему автоматически из Интернет**, выбрать в списке **Другой адрес** и указать адрес локального сервера обновлений, например `http://<ip сервера>/mirror`:

☒ Обновлять систему автоматически из Интернет

Источник: Другой адрес ▾

`http://10.129.0.24/mirror`

Репозитории: ☒ Десятая платформа

25.4. 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:

Релиз загруженного ядра:	<input type="text" value="5.10.165-std-def-alt1"/>	Ядро загружаемое по умолчанию:	<input type="text" value="5.10.165-std-def-alt1"/>
Тип загруженного ядра (flavour):	<input type="text" value="std-def"/>		
Версия загруженного ядра:	<input type="text" value="5.10.165"/>		
Установленные ядра:		Установленные модули: <input type="checkbox"/> drm-nouveau <input type="checkbox"/> drm	
<input type="button" value="Сделать ядро загружаемым по умолчанию"/>		<input type="button" value="Удалить модуль"/>	
Замечание: Чтобы сделать ядро загружаемым по умолчанию, выберите желаемую версию в списке выше и нажмите кнопку 'Сделать ядро загружаемым по умолчанию'. Перезагрузите компьютер, чтобы загрузится с выбранным ядром.			
<input type="button" value="Удалить ядро"/>			
<input type="button" value="Обновить ядро..."/>			
Замечание: Чтобы установить модули или обновить ядро, нажмите кнопку 'Обновить ядро' (чтобы установить модули нужна последняя версия ядра). Это потребует обновления списка пакетов доступных в репозитории и может занять некоторое время (зависит от скорости интернета).			

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

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

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

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



Примечание

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

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

Доступное ядро:	<input type="text" value="5.10.166-alt1"/>	<input type="text" value="std-def"/>	Доступные модули:	<input type="checkbox"/> accel-ppp <input type="checkbox"/> bcmwl <input type="checkbox"/> ch34x <input type="checkbox"/> dm-secdel <input type="checkbox"/> drbd9 <input type="checkbox"/> drm-ancient <input checked="" type="checkbox"/> drm-nouveau <input checked="" type="checkbox"/> drm <input type="checkbox"/> e1000e <input type="checkbox"/> hifc <input type="checkbox"/> hinic <input type="checkbox"/> i40e
<input type="button" value="Обновить ядро"/> <input type="button" value="Установить модули"/>				
<input type="button" value="назад"/>				

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



Примечание

Новое ядро загрузится только после перезагрузки системы.

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

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

25.5. 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 репозиторий и публикации их для обновлений рабочих станций и серверов.

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

Репозиторий	Источник	Архитектуры	Локальное зеркало	Опубликовано
Стабильная ветка ALT Linux 5.1			<input type="checkbox"/>	<input type="checkbox"/>
Репозиторий обновлений для Альт 8 СП			<input type="checkbox"/>	<input type="checkbox"/>
Десятая платформа	ftp.altlinux.org	x86_64	<input checked="" type="checkbox"/> (31 Гб)	<input type="checkbox"/>
Пятая платформа			<input type="checkbox"/>	<input type="checkbox"/>
Шестая платформа			<input type="checkbox"/>	<input type="checkbox"/>
Седьмая платформа			<input type="checkbox"/>	<input type="checkbox"/>
Восьмая платформа			<input type="checkbox"/>	<input type="checkbox"/>
Девятая платформа			<input type="checkbox"/>	<input type="checkbox"/>
Девятая платформа (mipsel)			<input type="checkbox"/>	<input type="checkbox"/>
ALT Linux Sisyphus			<input type="checkbox"/>	<input type="checkbox"/>
ALT Linux Sisyphus (mipsel)			<input type="checkbox"/>	<input type="checkbox"/>
ALT Linux Sisyphus (riscv64)			<input type="checkbox"/>	<input type="checkbox"/>
Публичный бранч TEAM t6			<input type="checkbox"/>	<input type="checkbox"/>
Публичный бранч TEAM t7			<input type="checkbox"/>	<input type="checkbox"/>

Свободное место: 64 Гб

Предупреждение: зеркалирование потребует наличия большого количества места на диске.

☐ Отключить зеркалирование
☒ Зеркалировать ежедневно
☐ Зеркалировать еженедельно в:
☐ Зеркалировать ежемесячно в день:

Время:

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

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



Примечание

При выборе любой архитектуры также будет добавлен источник с poarch.

Репозиторий: Десятая платформа

Источник:

Архитектуры: ☐ i586
☒ x86_64
☐ x86_64-i586

☒ Локальное зеркало репозитория
☐ Опубликовать как репозиторий для автоматических обновлений

Исключить каталоги и файлы (каждый шаблон в отдельной строке)

```
SRPMS  
RPMS.debuginfo  
*-debuginfo-*
```

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

»Локальное зеркало репозитория

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



Важно

Зеркалирование потребует наличия большого количества места на диске.

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

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

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

» Публикация репозитория

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

Со стороны клиентских машин, в этом случае, необходимо настроить модуль [Обновление системы](#), отметив в нём **Обновление системы управляемое сервером**.

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



Примечание

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

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

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



Примечание

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

25.5.1. 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://<ip сервера>/mirror/p10/branch
```

Проверить правильность настройки репозитория:

```
# apt-repo
rpm http://10.129.0.24/mirror p10/branch/x86_64 classic
rpm http://10.129.0.24/mirror p10/branch/noarch classic
```

25.5.2. 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
```



Примечание

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

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

На клиентских машинах необходимо настроить репозитории:

```
# apt-repo rm all
# apt-repo add ftp://<ip сервера>/mirror/p10/branch
# apt-repo
rpm ftp://10.129.0.24/mirror p10/branch/x86_64 classic
rpm ftp://10.129.0.24/mirror p10/branch/noarch classic
```

25.6. 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.

25.7. 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.

Пароль системного администратора:

☐ Создать автоматически

(введите фразу)

(повторите фразу)

Сменить пароль

Разрешённые ssh ключи:

SHA256:h5ldexZzlBaqCHl6Nr4enxJlt9XQc1a5lnojJG+VSvo

Удалить ключ

Новый ключ: Файл не выбран.

25.8. 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.

☒ Получать точное время с NTP-сервера:


☐ Работать как NTP-сервер

Текущая дата:

< Февраль 2023 >

Пн	Вт	Ср	Чт	Пт	Сб	Вс
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28					

Текущее время:



☒ Хранить время в BIOS по Гринвичу

Часовой пояс: Европа/Калининград

Выбрать источник сигналов времени: ▼

Системное время зависит от следующих факторов:

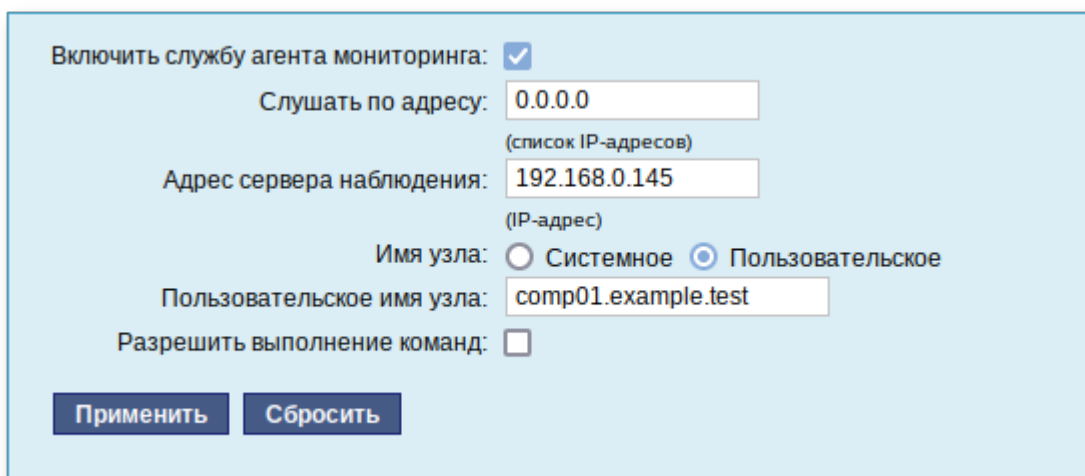
- » часы в BIOS — часы, встроенные в компьютер. Они работают, даже если он выключен;
- » системное время — часы в ядре операционной системы. Во время работы системы все процессы пользуются именно этими часами;
- » часовые пояса — регионы Земли, в каждом из которых принято единое местное время.

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**.

25.9. Агент наблюдения

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



Включить службу агента мониторинга: ☒

Слушать по адресу:
(список IP-адресов)

Адрес сервера наблюдения:
(IP-адрес)

Имя узла: ☐ Системное ☒ Пользовательское

Пользовательское имя узла:

Разрешить выполнение команд: ☐

На странице модуля можно задать следующие параметры:

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



Примечание

Параметр **Разрешить выполнение команд** использовать не рекомендуется.

Чтобы применить настройки и запустить Zabbix-агент, следует отметить пункт **Включить службу агента мониторинга** и нажать кнопку **Применить**.

25.10. Ограничение использования диска

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

Файловая система: / Текущее использование диска: 0 КБ

Включено: ☐ Мягкое ограничение: 0 КБ

Пользователь: user Жесткое ограничение: 0 КБ

Количество файлов: 0

Мягкое ограничение: 0

Жесткое ограничение: 0

Применить Сбросить

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**:

Файловая система: /home Текущее использование диска: 567320 КБ

Включено: ☒ Мягкое ограничение: 0 КБ

Пользователь: user Жесткое ограничение: 0 КБ

Количество файлов: 1143

Мягкое ограничение: 100

Жесткое ограничение: 100

Применить Сбросить

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.

25.11. Выключение и перезагрузка компьютера

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

☒ Продолжить работу

☐ Выключить компьютер сейчас

☐ Перезагрузить компьютер сейчас

☐ Приостановить компьютер сейчас

☐ Погрузить компьютер в сон сейчас

☒ Выключать компьютер каждый день в: 19:45:00

☐ Перезагружать компьютер каждый день в: 23:00:00

☐ Приостанавливать компьютер каждый день в: 23:00:00

☐ Погружать компьютер в сон каждый день в: 23:00:00

☐ При изменении состояния системы отправлять электронное письмо по адресу:

Модуль **Выключение компьютера** позволяет:

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

Возможна настройка ежедневного применения данных действий в заданное время.

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

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



Примечание

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

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

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

☒ Продолжить работу
☐ Выключить компьютер сейчас
☐ Перезагрузить компьютер сейчас
☐ Приостановить компьютер сейчас
☐ Погрузить компьютер в сон сейчас

☐ Выключать компьютер каждый день в: 23:00:00
☒ Перезагружать компьютер каждый день в: 11:22:00
☐ Приостанавливать компьютер каждый день в: 23:00:00
☐ Погружать компьютер в сон каждый день в: 23:00:00

☒ При изменении состояния системы отправлять электронное письмо по адресу:
user_freeipa@example.test

Применить **Сбросить**

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.

Глава 26. Соединение удалённых офисов (OpenVPN-сервер)

26.1. Настройка OpenVPN-сервера

26.2. Настройка клиентов

Альт Сервер предоставляет возможность безопасного соединения удалённых офисов используя технологию VPN (англ. Virtual Private Network — виртуальная частная сеть), которая позволяет организовать безопасные зашифрованные 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.

26.1. Настройка OpenVPN-сервера

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

☐ Включить службу OpenVPN

Тип: Маршрутизируемое (TUN)

Сети сервера: 192.168.0.0/255.255.255.0

Удалить

Новая сеть:

Маска сети: /24 (255.255.255.0)

Добавить

VPN сеть: 10.8.0.0

Маска сети: /24 (255.255.255.0)

Алгоритм шифрования: default

Алгоритм шифрования TLS: default

Алгоритм хэширования: default

☐ Отключить согласование алгоритмов шифрования (NCP)

Порт: 1194

☐ Сжатие LZO

☐ Использовать соединение TCP

Сертификат и ключ SSL...

Положить сертификат УЦ:

Обзор... Файл не выбран.

 Положить

Сети клиентов...

Применить Сбросить

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*):

Настройки SSL

Общее имя (CN):
(имя компьютера для сервера или что-либо другое для клиента)

Страна (C):
(двухбуквенный код страны)

Местоположение (L):
(название города или области, написанное латинскими буквами)

Организация (O):
(название организации, написанное латинскими буквами)

Подразделение (OU):
(название подразделения, написанное латинскими буквами)

E-mail адрес:
(ваш адрес электронной почты)

☒ (Пере)создать ключ и запрос на подпись **Подтвердить**

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**:

Подпись

Забрать запрос на подпись

Положить сертификат, подписанный УЦ: Файл не выбран.

Положить

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):

SSL ключи:

ahhttpd (истекает: 09.02.2024)
<u>openvpn-server (Нет сертификата)</u>
postfix (истекает: 09.02.2024)

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:

Подписать сертификат

openvpn-server.csr

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

Certificate Request:

Data:

Version: 1 (0x0)

Subject: CN = openvpn-server, C = RU, L = Kaliningrad

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

00:b3:62:2a:d4:f8:e1:db:5d:e6:49:ce:b3:79:29:
 bf:dc:f2:19:ba:63:3a:7e:52:30:23:3e:13:83:92:
 d0:ae:9d:cb:82:2a:44:f2:1c:d2:e6:92:47:86:07:
 16:cf:03:5a:be:80:58:b0:d9:4a:e4:de:c2:b7:68:
 20:23:2a:9e:e1:a2:50:52:61:99:79:5a:af:42:9f:
 78:2d

Exponent: 65537 (0x10001)

Attributes:

a0:00

Signature Algorithm: sha256WithRSAEncryption

7c:2f:14:8f:80:e6:96:cd:ab:93:16:d0:a9:9d:59:b9:e9:80:
 6c:a7:29:bf:b9:ca:15:89:55:8e:3c:78:03:55:21:77:97:4d:
 0d:43:95:14:13:72:f3:2e:69:e0:f7:6d:5e:a2:ca:c9:34:b2:
 8b:bd:4b:6d:d9:9f:4e:ce:6d:09:65:f6:7d:bd:b7:4a:02:d2:
 21:40:97:5a

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**:

Положить сертификат, подписанный УЦ:

Положить

В модуле **Управление ключами SSL**, видно, что изменился ключ *openvpn-server* (*истекает_u_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**:

Сертификат: [ca-root.pem](#)
Запрос на подпись: [ca-root.csr](#)

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

Положить сертификат УЦ:

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**).

26.2. 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.

Новое соединение:

☒ Сетевой туннель (TUN)
☐ Виртуальное Ethernet устройство (TAP)

Создать соединение

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

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

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

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

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

Проверить, появилось ли соединение с сервером можно командой

```
ip addr
```

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

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


Глава 27. Доступ к службам сервера из сети Интернет

27.1. Внешние сети

27.2. Список блокируемых хостов

27.1. 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.

Версия IP: ☒ Включить брандмауэр

Выберите режим работы:

Выберите внешние интерфейсы: ☐ enp0s3 (Intel Corporation 82540EM Gigabit Ethernet Controller) 192.168.0.91/24

Разрешить входящие соединения на внешних интерфейсах:

Службы:

- ☒ Центр управления системой (www)
- ☐ Система печати CUPS
- ☐ DHCP
- ☐ DNS
- ☐ Передача файлов (FTP)
- ☐ Почтовый сервер (IMAP)
- ☐ LDAP
- ☒ OpenVPN
- ☐ Почтовый сервер (POP3)
- ☐ Прокси-сервер
- ☐ Файловый сервер (Samba)

Можно выбрать один из двух режимов работы:

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

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



Примечание

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



Примечание

Все внутренние интерфейсы открыты для любых входящих соединений.

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

27.2. 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**.

The screenshot shows a configuration window titled "Чёрный список:" (Blacklist:). It contains a dropdown menu for "Версия IP:" (IP version) set to "IPv4". Below it is a checkbox labeled "Использовать чёрный список" (Use blacklist), which is currently unchecked. To the right of the checkbox is a "Удалить" (Delete) button. Below the checkbox is a large empty text area for listing IP addresses. At the bottom, there is a label "Добавить IP адрес сети или хоста:" (Add IP address of network or host:) followed by an input field and a "Добавить" (Add) button.

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

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

Глава 28. Статистика

28.1. Сетевой трафик

28.1. Сетевой трафик



Все входящие и исходящие с сервера сетевые пакеты могут подсчитываться, и выводиться 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**.




☐ Включить сбор данных

Применить

Период с: 1970-01-01  по 1970-01-01 

Интерфейс: enp0s3 - 192.168.0.91 

Показать

Служба 	Входящий трафик(Кб) 	Исходящий трафик(Кб) 

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**.

☒ Включить сбор данных

Применить

Период с: по

Интерфейс:

Показать

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

Трафик на указанном интерфейсе за заданный период показывается в виде:

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

28.2. 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**.

Включить сбор данных прокси-сервера: ☐ [Применить](#)

Общий объем трафика принятый за [сегодня](#) [▼](#)
[всеми пользователями](#) [▼](#)
[со всех сайтов](#) [▼](#)
составляет **0.00 Б**

[Обновить](#)

Список сайтов, набравших [любой объем](#) [▼](#) данных

UID/IP-адрес	Количество	Сайт/домен	Время последнего запроса
--------------	------------	------------	--------------------------

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 неаутентифицированных пользователей. Только после этого в статистике начнут показываться пользователи.

Глава 29. 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.

Глава 30. Права доступа к модулям

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

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

Брандмауэр

Внешние сети

Перенаправление портов

Список блокируемых хостов

Внутренние сети

Ручной режим управления

[Параметры доступа к модулю...](#)

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

Параметры доступа к модулю

Следующие пользователи имеют доступ:

user	Удалить
------	---------

Новый пользователь:

	Добавить
--	----------

Замечание: Все ваши изменения вступят в силу после перезапуска HTTP сервера.

Перезапустить HTTP-сервер

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

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

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

Часть VI. Основы администрирования Linux

Содержание

- 31. Общие принципы работы ОС
- 32. Режим суперпользователя
- 33. Команда sudo
- 34. Управление пользователями
- 35. Система инициализации systemd и sysvinit
- 36. Документация

Глава 31. Общие принципы работы ОС

31.1. Процессы и файлы

31.2. Работа с наиболее часто используемыми компонентами

31.3. Стыкование команд в системе Linux

31.1. Процессы и файлы

ОС Альт Сервер является многопользовательской интегрированной системой. Это значит, что она разработана в расчете на одновременную работу нескольких пользователей.

Пользователь может либо сам работать в системе, выполняя некоторую последовательность команд, либо от его имени могут выполняться прикладные процессы.

Пользователь взаимодействует с системой через командный интерпретатор. Командный интерпретатор представляет собой прикладную программу, которая принимает от пользователя команды или набор команд и транслирует их в системные вызовы к ядру системы. Интерпретатор позволяет пользователю просматривать файлы, передвигаться по дереву файловой системы, запускать прикладные процессы. Все командные интерпретаторы UNIX имеют развитый командный язык и позволяют писать достаточно сложные программы, упрощающие процесс администрирования системы и работы с ней.

31.1.1. Процессы функционирования ОС

Все программы, которые выполняются в текущий момент времени, называются процессами. Процессы можно разделить на два основных класса: системные процессы и пользовательские процессы.

Системные процессы — программы, решающие внутренние задачи ОС, например, организацию виртуальной памяти на диске или предоставляющие пользователям те или иные сервисы (процессы-службы).

Пользовательские процессы — процессы, запускаемые пользователем из командного интерпретатора для решения задач пользователя или управления системными процессами. Linux изначально разрабатывался как многозадачная система. Он использует технологии, опробованные и отработанные другими реализациями UNIX, которые существовали ранее.

Фоновый режим работы процесса — режим, когда программа может работать без взаимодействия с пользователем. В случае необходимости интерактивной работы с пользователем (в общем случае) процесс будет «остановлен» ядром, и работа его продолжается только после перевода его в «нормальный» режим работы.

31.1.2. Файловая система ОС

В ОС использована файловая система Linux, которая, в отличие от файловых систем DOS и Windows(™), является единым деревом. Корень этого дерева — каталог, называемый root (рут) и обозначаемый /.

Части дерева файловой системы могут физически располагаться в разных разделах разных дисков или вообще на других компьютерах — для пользователя это прозрачно. Процесс присоединения файловой системы раздела к дереву называется монтированием, удаление — размонтированием. Например, файловая система CD-ROM в дистрибутиве монтируется по умолчанию в каталог **/media/cdrom** (путь в дистрибутиве обозначается с использованием */*, а не **, как в DOS/Windows).

Текущий каталог обозначается **./**.

31.1.3. Структура каталогов

Корневой каталог **/**:

- **/bin** — командные оболочки (shell), основные утилиты;
- **/boot** — содержит ядро системы;
- **/dev** — псевдофайлы устройств, позволяющие работать с устройствами напрямую. Файлы в **/dev** создаются сервисом **udev**
- **/etc** — общесистемные конфигурационные файлы для большинства программ в системе;
- **/etc/rc?.d**, **/etc/init.d**, **/etc/rc.boot**, **/etc/rc.d** — каталоги, где расположены командные файлы, выполняемые при запуске системы или при смене её режима работы;
- **/etc/passwd** — база данных пользователей, в которой содержится информация об имени пользователя, его настоящем имени, личном каталоге, его зашифрованный пароль и другие данные;
- **/etc/shadow** — теневая база данных пользователей. При этом информация из файла **/etc/passwd** перемещается в **/etc/shadow**, который недоступен для чтения всем, кроме пользователя **root**. В случае использования альтернативной схемы управления теневыми паролями (TCB), все теневые пароли для каждого пользователя располагаются в каталоге **/etc/tcb/имя пользователя/shadow**;
- **/home** — домашние каталоги пользователей;
- **/lib** — содержит файлы динамических библиотек, необходимых для работы большей части приложений, и подгружаемые модули ядра;
- **/lost+found** — восстановленные файлы;
- **/media** — подключаемые носители (каталоги для монтирования файловых систем сменных устройств);
- **/mnt** — точки временного монтирования;
- **/opt** — вспомогательные пакеты;
- **/proc** — виртуальная файловая система, хранящаяся в памяти компьютера при загруженной ОС. В данном каталоге расположены самые свежие сведения обо всех процессах, запущенных на компьютере.
- **/root** — домашний каталог администратора системы;
- **/run** — файлы состояния приложений;

- » **/sbin** — набор программ для административной работы с системой (системные утилиты);
- » **/selinux** — виртуальная файловая система SELinux;
- » **/srv** — виртуальные данные сервисных служб;
- » **/sys** — файловая система, содержащая информацию о текущем состоянии системы;
- » **/tmp** — временные файлы.
- » **/usr** — пользовательские двоичные файлы и данные, используемые только для чтения (программы и библиотеки);
- » **/var** — файлы для хранения изменяющихся данных (рабочие файлы программ, очереди, журналы).

Каталог **/usr**:

- » **/usr/bin** — дополнительные программы для всех учетных записей;
- » **/usr/sbin** — команды, используемые при администрировании системы и не предназначенные для размещения в файловой системе root;
- » **/usr/local** — место, где рекомендуется размещать файлы, установленные без использования пакетных менеджеров, внутренняя организация каталогов практически такая же, как и корневого каталога;
- » **/usr/man** — каталог, где хранятся файлы справочного руководства **man**;
- » **/usr/share** — каталог для размещения общедоступных файлов большей части приложений.

Каталог **/var**:

- » **/var/log** — место, где хранятся файлы аудита работы системы и приложений;
- » **/var/spool** — каталог для хранения файлов, находящихся в очереди на обработку для того или иного процесса (очереди печати, непочитанные или не отправленные письма, задачи cron т.д.).

31.1.4. Организация файловой структуры

Система домашних каталогов пользователей помогает организовывать безопасную работу пользователей в многопользовательской системе. Вне своего домашнего каталога пользователь обладает минимальными правами (обычно чтение и выполнение файлов) и не может нанести ущерб системе, например, удалив или изменив файл.

Кроме файлов, созданных пользователем, в его домашнем каталоге обычно содержатся персональные конфигурационные файлы некоторых программ.

Маршрут (путь) — это последовательность имён каталогов, представляющая собой путь в файловой системе к данному файлу, где каждое следующее имя отделяется от предыдущего наклонной чертой (слешем). Если название маршрута начинается со слеша, то путь в искомый файл начинается от корневого каталога всего дерева системы. В обратном случае, если название маршрута начинается непосредственно с имени файла, то путь к искомому файлу должен начинаться от текущего каталога (рабочего каталога).

Имя файла может содержать любые символы за исключением косой черты (/). Однако следует избегать применения в именах файлов большинства знаков препинания и непечатаемых символов. При выборе имен файлов рекомендуется ограничиться следующими символами:

- **строчные и ПРОПИСНЫЕ** буквы. Следует обратить внимание на то, что регистр всегда имеет значение;
- символ подчеркивания (_);
- точка (.).

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

31.1.5. Имена дисков и разделов

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

- **/dev/sda** — первый диск;
- **/dev/sdb** — второй диск;
- и т.д.

Диски обозначаются **/dev/sdX**, где *X* — a, b, c, d, e, ... в зависимости от порядкового номера диска на шине.

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

31.1.6. Разделы, необходимые для работы ОС

Для работы ОС на жестком диске (дисках) должны быть созданы, по крайней мере, два раздела: корневой (то есть тот, который будет содержать каталог /) и раздел подкачки (swp). Размер последнего, как правило, составляет от однократной до двукратной величины оперативной памяти компьютера. Если на диске много свободного места, то можно создать отдельные разделы для каталогов **/usr**, **/home**, **/var**.

31.2. Работа с наиболее часто используемыми компонентами

31.2.1. Командные оболочки (интерпретаторы)

Для управления ОС используются командные интерпретаторы (shell).

Зайдя в систему, Вы увидите приглашение — строку, содержащую символ «\$» (далее этот символ будет обозначать командную строку). Программа ожидает ваших команд. Роль командного интерпретатора — передавать ваши команды операционной системе. По своим функциям он соответствует **command.com** в DOS, но несравненно мощнее. При помощи командных интерпретаторов можно писать небольшие программы — сценарии (скрипты). В Linux доступны следующие командные оболочки:

- **bash** — самая распространенная оболочка под linux. Она ведет историю команд и предоставляет возможность их редактирования;
- **pdksh** — клон korn shell, хорошо известной оболочки в UNIX™ системах.

Проверить, какая оболочка используется в данный момент можно, выполнив команду:

```
$ echo $SHELL
```

Оболочкой по умолчанию является Bash (Bourne Again Shell) — самая распространённая оболочка под Linux, которая ведет историю команд и предоставляет возможность их редактирования. В дальнейшем описании работы с Альт Сервер будут использоваться примеры с использованием этой оболочки.

31.2.2. Командная оболочка Bash

В Bash имеется несколько приемов для работы со строкой команд. Например, можно использовать следующие сочетания:

- **Ctrl+A** — перейти на начало строки;
- **Ctrl+U** — удалить текущую строку;
- **Ctrl+C** — остановить текущую задачу.

Для ввода нескольких команд одной строкой можно использовать разделитель «;». По истории команд можно перемещаться с помощью клавиш ↑ («вверх») и ↓ («вниз»).

Чтобы найти конкретную команду в списке набранных, не пролистывая всю историю, можно нажать **Ctrl+R** и начать вводить символы ранее введенной команды.

Для просмотра истории команд можно воспользоваться командой **history**. Команды, присутствующие в истории, отображаются в списке пронумерованными. Чтобы запустить конкретную команду необходимо набрать:

```
!номер команды
```

Если ввести:

```
!!
```

запустится последняя из набранных команд.

В Bash имеется возможность самостоятельного завершения имен команд из общего списка команд, что облегчает работу при вводе команд, в случае, если имена программ и команд слишком длинны. При нажатии клавиши **Tab** Bash завершает имя команды, программы или каталога, если не существует нескольких альтернативных вариантов. Например, чтобы использовать программу декомпрессии **gunzip**, можно набрать следующую команду:

```
gu
```

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

В предложенном примере можно получить следующий список:

```
$ gu
guile gunzip gupnp-binding-tool
```

Если набрать: **n** (**gunzip** — это единственное имя, третьей буквой которого является «n»), а затем нажать клавишу **Tab**, то оболочка самостоятельно дополнит имя. Чтобы запустить команду нужно нажать **Enter**.

Программы, вызываемые из командной строки, Bash ищет в каталогах, определяемых в системной переменной **\$PATH**. По умолчанию в этот перечень каталогов не входит текущий каталог, обозначаемый **./** (точка слеш) (если только не выбран один из двух самых слабых уровней защиты). Поэтому, для запуска программы из текущего каталога, необходимо использовать команду (в примере запускается команда **prog**):

```
./prog
```

31.2.3. Команда

Простейшая команда состоит из одного «слова», например, команда **cal**, выводящая календарь на текущий месяц.

```
$ cal
      Март 2023
Пн Вт Ср Чт Пт Сб Вс
      1  2  3  4  5
 6  7  8  9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31
```

31.2.4. Команда и параметры

```
$ cal 1 2024
      Январь 2024
Пн Вт Ср Чт Пт Сб Вс
 1  2  3  4  5  6  7
 8  9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31
```

Команда **cal 1 2024** состоит из двух частей — собственно команды **cal** и «остального». То, что следует за командой называется *параметрами* (или аргументами) и они вводятся для изменения поведения команды. В большинстве случаев, первое слово считается именем команды, а остальные — её параметрами.

31.2.5. Команда и ключи

Для решения разных задач одни и те же действия необходимо выполнять по-разному. Например, для синхронизации работ в разных точках земного шара лучше использовать единое для всех время (по Гринвичу), а для организации собственного рабочего дня — местное время (с учётом сдвига по часовому поясу и разницы зимнего и летнего времени). И то, и другое время показывает команда **date**, только для работы по Гринвичу ей нужен дополнительный параметр **-u** (он же **--universal**).

```
$ date
Пн мар 6 10:42:35 MSK 2023
$ date -u
Пн мар 6 07:43:07 UTC 2023
```

Такого рода параметры называются *ключами* или *модификаторами выполнения*. Ключ принадлежит данной конкретной команде и сам по себе смысла не имеет. Этим он отличается от других параметров (например, имён файлов, чисел), имеющих собственный смысл, не зависящий ни от какой команды. Каждая команда может распознавать некоторый набор ключей и соответственно изменять своё поведение. Один и тот же ключ может определять для разных команд совершенно разные значения.

Для формата ключей нет жёсткого стандарта, однако существуют договорённости:

- Если ключ начинается на -, то это *однобуквенный ключ*. За -, как правило, следует один символ, чаще всего буква, обозначающая действие или свойство, которое этот ключ придаёт команде. Так проще отличать ключи от других параметров.
- Если ключ начинается на --, то он называется *полнословным ключом*. Полнословный формат ключа начинается на два знака --, за которыми следует полное имя обозначаемого этим ключом содержания.

Некоторые ключи имеют и однобуквенный, и полнословный формат, а некоторые — только полнословный.

Информацию о ресурсах каждой команды можно получить, используя ключ **--help**. К примеру, получить подсказку о том, что делает команда **rm**, можно, набрав в терминале **rm --help**.

31.2.6. Обзор основных команд системы

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

```
$ man ls
```



Примечание

Параметры команд обычно начинаются с символа «-», и обычно после одного символа «-» можно указать сразу несколько опций. Например, вместо команды **ls -l -F** можно ввести команду **ls -lF**

Учетные записи пользователей

Команда **su**

Команда **su** позволяет изменить «владельца» текущего сеанса (сессии) без необходимости завершать сеанс и открывать новый.

Синтаксис:

```
su [ОПЦИИ...] [ПОЛЬЗОВАТЕЛЬ]
```

Команду можно применять для замены текущего пользователя на любого другого.

Команда **id**

Команда **id** выводит информацию о пользователе и группах, в которых он состоит для заданного пользователя или о текущем пользователе (если ничего не указано).

Синтаксис:

```
id [ОПЦИИ...] [ПОЛЬЗОВАТЕЛЬ]
```

Команда **passwd**

Команда **passwd** меняет (или устанавливает) пароль, связанный с входным_именем пользователя.

Обычный пользователь может менять только пароль, связанный с его собственным входным_именем.

Команда запрашивает у обычных пользователей старый пароль (если он был), а затем дважды запрашивает новый. Новый пароль должен соответствовать техническим требованиям к паролям, заданным администратором системы.

Основные операции с файлами и каталогами

Команда **ls**

Команда **ls** (list) печатает в стандартный вывод содержимое каталогов.

Синтаксис:

```
ls [ОПЦИИ...] [ФАЙЛ...]
```

Основные опции:

- » **-a** — просмотр всех файлов, включая скрытые;
- » **-l** — отображение более подробной информации;
- » **-R** — выводить рекурсивно информацию о подкаталогах.

Команда **cd**

Команда **cd** предназначена для смены каталога. Команда работает как с абсолютными, так и с относительными путями. Если каталог не указан, используется значение переменной окружения **\$HOME** (домашний каталог пользователя). Если каталог задан полным маршрутным именем, он становится текущим. По отношению к новому каталогу нужно иметь право на выполнение, которое в данном случае трактуется как разрешение на поиск.

Синтаксис:

```
cd [-L|-P] [КАТАЛОГ]
```

Если в качестве аргумента задано «-», то это эквивалентно **\$OLDPWD**. Если переход был осуществлен по переменной окружения **\$CDPATH** или в качестве аргумента был задан «-» и смена каталога была успешной, то абсолютный путь нового рабочего каталога будет выведен на стандартный вывод.

Пример. Находясь в домашнем каталоге перейти в его подкаталог **docs/** (относительный путь):

```
cd docs/
```

Сделать текущим каталог **/usr/bin** (абсолютный путь):

```
cd /usr/bin/
```

Сделать текущим родительский каталог:

```
cd ..
```

Вернуться в предыдущий каталог:

```
cd -
```

Сделать текущим домашний каталог:

```
cd
```

Команда **pwd**

Команда **pwd** выводит абсолютный путь текущего (рабочего) каталога.

Синтаксис:

```
pwd [-L|-P]
```

Опции:

- » **-P** — не выводить символические ссылки;
- » **-L** — выводить символические ссылки.

Команда **rm**

Команда **rm** служит для удаления записей о файлах. Если заданное имя было последней ссылкой на файл, то файл уничтожается.



Предупреждение

Удалив файл, вы не сможете его восстановить!

Синтаксис:

```
rm [ОПЦИИ...] <ФАЙЛ>
```

Основные опции:

- » **-f** — никогда не запрашивать подтверждения;
- » **-i** — всегда запрашивать подтверждение;
- » **-r, -R** — рекурсивно удалять содержимое указанных каталогов.

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

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

Команда **mkdir**

mkdir — команда для создания новых каталогов.

Синтаксис:

```
mkdir [-p] [-m права] <КАТАЛОГ...>
```

Команда **rmdir**

Команда **rmdir** удаляет каталоги из файловой системы. Каталог должен быть пуст перед удалением.

Синтаксис:

```
rmdir [ОПЦИИ] <КАТАЛОГ...>
```

Основные опции:

- » **-p** — удалить каталог и его потомки.

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

Команда **cp**

Команда **cp** предназначена для копирования файлов из одного в другие каталоги.

Синтаксис:

```
cp [-fip] [ИСХ_ФАЙЛ...] [ЦЕЛ_ФАЙЛ...]
```

```
cp [-fip] [ИСХ_ФАЙЛ...] [КАТАЛОГ]
```

```
cp [-R] [[-H] | [-L] | [-P]] [-fip] [ИСХ_ФАЙЛ...] [КАТАЛОГ]
```

Основные опции:

- » **-p** — сохранять по возможности времена изменения и доступа к файлу, владельца и группу, права доступа;

- » **-i** — запрашивать подтверждение перед копированием в существующие файлы;
- » **-r, -R** — рекурсивно копировать содержимое каталогов.

Команда **mv**

Команда **mv** предназначена для перемещения файлов.

Синтаксис:

```
mv [-fi] [ИСХ_ФАЙЛ...] [ЦЕЛ_ФАЙЛ...]
```

```
mv [-fi] [ИСХ_ФАЙЛ...] [КАТАЛОГ]
```

В первой синтаксической форме, характеризующейся тем, что последний операнд не является ни каталогом, ни символической ссылкой на каталог, **mv** перемещает **исх_файл** в **цел_файл** (происходит переименование файла).

Во второй синтаксической форме **mv** перемещает исходные файлы в указанный каталог под именами, совпадающими с краткими именами исходных файлов.

Основные опции:

- » **-f** — не запрашивать подтверждения перезаписи существующих файлов;
- » **-i** — запрашивать подтверждение перезаписи существующих файлов.

Команда **cat**

Команда **cat** последовательно выводит содержимое файлов.

Синтаксис:

```
cat [ОПЦИИ] [ФАЙЛ...]
```

Основные опции:

- » **-n, --number** — нумеровать все строки при выводе;
- » **-E, --show-ends** — показывать \$ в конце каждой строки.

Если файл не указан, читается стандартный ввод. Если в списке файлов присутствует имя «-», вместо этого файла читается стандартный ввод.

Команда **head**

Команда **head** выводит первые 10 строк каждого файла на стандартный вывод.

Синтаксис:

```
head [ОПЦИИ] [ФАЙЛ...]
```

Основные опции:

- » **-n, --lines=[-]K** — вывести первые K строк каждого файла, а не первые 10;
- » **-q, --quiet** — не печатать заголовки с именами файлов.

Команда **less**

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

Синтаксис:

```
less ФАЙЛ
```

Команда **grep**

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

Синтаксис:

```
grep [шаблон_поиска] ФАЙЛ
```

Команда **chmod**

Команда **chmod** предназначена для изменения прав доступа файлов и каталогов.

Синтаксис:

```
chmod [ОПЦИИ] РЕЖИМ[ ,РЕЖИМ]... <ФАЙЛ>
```

```
chmod [ОПЦИИ] --reference=ИФАЙЛ <ФАЙЛ>
```

Основные опции:

- » **-R** — рекурсивно изменять режим доступа к файлам, расположенным в указанных каталогах;
- » **--reference=ИФАЙЛ** — использовать режим файла ИФАЙЛ.

chmod изменяет права доступа каждого указанного файла в соответствии с правами доступа, указанными в параметре режим, который может быть представлен как в символьном виде, так и в виде восьмеричного, представляющего битовую маску новых прав доступа.

Формат символьного режима следующий:

```
[ugoа...][[+|=][разрешения...]]...
```

Здесь разрешения — это ноль или более букв из набора «**rwXst**» или одна из букв из набора «**ugo**».

Каждый аргумент — это список символьных команд изменения прав доступа, разделены запятыми. Каждая такая команда начинается с нуля или более букв «**ugoа**», комбинация которых указывает, чьи права доступа к файлу будут изменены: пользователя, владеющего файлом (**u**), пользователей, входящих в группу, к которой принадлежит файл (**g**), остальных пользователей (**o**) или всех пользователей (**a**). Если не задана ни одна буква, то автоматически будет использована буква «**a**», но биты, установленные в **umask**, не будут затронуты.

Оператор «+» добавляет выбранные права доступа к уже имеющимся у каждого файла, «-» удаляет эти права. «=» присваивает только эти права каждому указанному файлу.

Буквы «rwxXst» задают биты доступа для пользователей: «r» — чтение, «w» — запись, «x» — выполнение (или поиск для каталогов), «X» — выполнение/поиск только если это каталог или же файл с уже установленным битом выполнения, «s» — задать ID пользователя и группы при выполнении, «t» — запрет удаления.

Примеры. Позволить всем выполнять файл **f2**:

```
chmod +x f2
```

Запретить удаление файла **f3**:

```
chmod +t f3
```

Команда **chown**

Команда **chown** изменяет владельца и/или группу для каждого заданного файла.

Синтаксис:

```
chown [КЛЮЧ]...[ВЛАДЕЛЕЦ] [: [ГРУППА]] <ФАЙЛ>
```

Изменить владельца может только владелец файла или суперпользователь. Владелец не изменяется, если он не задан в аргументе. Группа также не изменяется, если не задана, но если после символического ВЛАДЕЛЬЦА стоит символ «:», подразумевается изменение группы на основную группу текущего пользователя. Поля ВЛАДЕЛЕЦ и ГРУППА могут быть как числовыми, так и символическими.

Примеры. Поменять владельца каталога **/u** на пользователя **test**:

```
chown test /u
```

Поменять владельца и группу каталога **/u**:

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

Поменять владельца каталога **/u** и вложенных файлов на **test**:

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

Поиск файлов

Команда **find**

Команда **find** предназначена для поиска всех файлов, начиная с корневого каталога. Поиск может осуществляться по имени, типу или владельцу файла.

Синтаксис:

```
find [-H] [-L] [-P] [-Oуровень] [-D help|tree|search|stat|rates|opt|exec]  
[ПУТЬ...] [ВЫРАЖЕНИЕ]
```

Ключи для поиска:

- » **-name** — поиск по имени файла;
- » **-type** — поиск по типу f=файл, d=каталог, l=ссылка(lnk);
- » **-user** — поиск по владельцу (имя или UID).

Когда выполняется команда **find**, можно выполнять различные действия над найденными файлами. Основные действия:

- » **-exec команда \;** — выполнить команду. Запись команды должна заканчиваться экранированной точкой с запятой. Строка «{» заменяется текущим маршрутным именем файла;
- » **execdir команда \;** — то же самое что и **-exec**, но команда вызывается из подкаталога, содержащего текущий файл;
- » **-ok команда** — эквивалентно **-exec** за исключением того, что перед выполнением команды запрашивается подтверждение (в виде сгенерированной командной строки со знаком вопроса в конце) и она выполняется только при ответе: y;
- » **-print** — вывод имени файла на экран.

Путем по умолчанию является текущий подкаталог. Выражение по умолчанию **-print**.

Примеры. Найти в текущем каталоге обычные файлы (не каталоги), имя которых начинается с символа «~»:

```
find . -type f -name "~*" -print
```

Найти в текущем каталоге файлы, измененные позже, чем файл **file.bak**:

```
find . -newer file.bak -type f -print
```

Удалить все файлы с именами **a.out** или ***.o**, доступ к которым не производился в течение недели:

```
find / \( -name a.out -o -name '*.o' \) \ -atime +7 -exec rm {} \;
```

Удалить из текущего каталога и его подкаталогов все файлы нулевого размера, запрашивая подтверждение:

```
find . -size 0c -ok rm {} \;
```

Команда **whereis**

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

Синтаксис:

```
whereis [ОПЦИИ] <ИМЯ>
```

Опции:

- » **-b** — вывод информации только об исполняемых файлах;
- » **-m** — вывод информации только о страницах справочного руководства;
- » **-s** — вывод информации только об исходных файлах.

Мониторинг и управление процессами

Команда **ps**

Команда **ps** отображает список текущих процессов.

Синтаксис:

```
ps [ОПЦИИ]
```

По умолчанию выводится информация о процессах с теми же действующим UID и управляющим терминалом, что и у подающего команду пользователя.

Основные опции:

- » **-a** — вывести информацию о процессах, ассоциированных с терминалами;
- » **-f** — вывести «полный» список;
- » **-l** — вывести «длинный» список;
- » **-p список** — вывести информацию о процессах с перечисленными в списке PID;
- » **-u список** — вывести информацию о процессах с перечисленными идентификаторами или именами пользователей.

Команда **kill**

Команда **kill** позволяет прекратить исполнение процесса или передать ему сигнал.

Синтаксис:

```
kill [-s] [сигнал] [идентификатор] [...]
```

```
kill [-l] [статус_завершения]
```

```
kill [-номер_сигнала] [идентификатор] [...]
```

Идентификатор — PID ведущего процесса задания или номер задания, предварённый знаком «%».

Основные опции:

- » **-l** — вывести список поддерживаемых сигналов;
- » **-s сигнал, -сигнал** — послать сигнал с указанным именем.

Если обычная команда **kill** не дает желательного эффекта, необходимо использовать команду **kill** с параметром **-9** (**kill -9 PID_номер**).

Команда **df**

Команда **df** показывает количество доступного дискового пространства в файловой системе, в которой содержится файл, переданный как аргумент. Если ни один файл не указан, показывается доступное место на всех смонтированных файловых системах. Размеры по умолчанию указаны в блоках по 1КБ.

Синтаксис:

```
df [ОПЦИИ] [ФАЙЛ...]
```

Основные опции:

- » **--total** — подсчитать общий объем в конце;
- » **-h, --human-readable** — печатать размеры в удобочитаемом формате (например, 1K, 234M, 2G).

Команда **du**

Команда **du** подсчитывает использование диска каждым файлом, для каталогов подсчет происходит рекурсивно.

Синтаксис:

```
du [ОПЦИИ] [ФАЙЛ...]
```

Основные опции:

- » **-a, --all** — выводить общую сумму для каждого заданного файла, а не только для каталогов;
- » **-c, --total** — подсчитать общий объем в конце. Может быть использовано для выяснения суммарного использования дискового пространства для всего списка заданных файлов;
- » **-d, --max-depth=N** — выводить объем для каталога (или файлов, если указано **--all**) только если она на N или менее уровней ниже аргументов командной строки;
- » **-S, --separate-dirs** — выдавать отдельно размер каждого каталога, не включая размеры подкаталогов;
- » **-s, --summarize** — отобразить только сумму для каждого аргумента.

Команда **which**

Команда **which** отображает полный путь к указанным командам или сценариям.

Синтаксис:

```
which [ОПЦИИ] <ФАЙЛ...>
```

Основные опции:

- » **-a, --all** — выводит все совпавшие исполняемые файлы по содержимому в переменной окружения **\$PATH**, а не только первый из них;

- » **-c, --total** — подсчитать общий объем в конце. Может быть использовано для выяснения суммарного использования дискового пространства для всего списка заданных файлов;
- » **-d, --max-depth=N** — выводить объем для каталога (или файлов, если указано **--all**) только если она на N или менее уровней ниже аргументов командной строки;
- » **-S, --separate-dirs** — выдавать отдельно размер каждого каталога, не включая размеры подкаталогов;
- » **--skip-dot** — пропускает все каталоги из переменной окружения **\$PATH**, которые начинаются с точки.

Использование многозадачности

Альт Сервер — это многозадачная система.

Для того, чтобы запустить программу в фоновом режиме, необходимо набрать «&» после имени программы. После этого оболочка даст возможность запустить другие приложения.

Так как некоторые программы интерактивны — их запуск в фоновом режиме бессмысленен. Подобные программы просто остановятся, если их запустить в фоновом режиме.

Можно также запускать нескольких независимых сеансов. Для этого в консоли необходимо набрать **Alt** и одну из клавиш, находящихся в интервале от **F1** до **F6**. На экране появится новое приглашение системы, и можно открыть новый сеанс. Этот метод также позволяет вам работать на другой консоли, если консоль, которую вы использовали до этого, не отвечает или вам необходимо остановить зависшую программу.

Команда **bg**

Команда **bg** позволяет перевести задание на задний план.

Синтаксис:

```
bg [ИДЕНТИФИКАТОР ...]
```

Идентификатор — PID ведущего процесса задания или номер задания, предварённый знаком «%».

Команда **fg**

Команда **fg** позволяет перевести задание на передний план.

Синтаксис:

```
fg [ИДЕНТИФИКАТОР ...]
```

Идентификатор — PID ведущего процесса задания или номер задания, предварённый знаком «%».

Сжатие и упаковка файлов

Команда **tar**

Сжатие и упаковка файлов выполняется с помощью команды **tar**, которая преобразует файл или группу файлов в архив без сжатия (tarfile).

Упаковка файлов в архив чаще всего выполняется следующей командой:

```
tar -cf [имя создаваемого файла архива] [упаковываемые файлы и/или каталоги]
```

Пример использования команды упаковки архива:

```
tar -cf moi_dokumenti.tar Docs project.tex
```

Распаковка содержимого архива в текущий каталог выполняется командой:

```
tar -xf [имя файла архива]
```

Для сжатия файлов используются специальные программы сжатия: **gzip**, **bzip2** и **7z**.

31.3. Стыкование команд в системе Linux

31.3.1. Стандартный ввод и стандартный вывод

Многие команды системы имеют так называемые стандартный ввод (standard input) и стандартный вывод (standard output), часто сокращаемые до `stdin` и `stdout`. Ввод и вывод здесь — это входная и выходная информация для данной команды. Программная оболочка делает так, что стандартным вводом является клавиатура, а стандартным выводом — экран монитора.

Пример с использованием команды **cat**. По умолчанию команда **cat** читает данные из всех файлов, которые указаны в командной строке, и посылает эту информацию непосредственно в стандартный вывод (`stdout`). Следовательно, команда:

```
cat history-final masters-thesis
```

выведет на экран сначала содержимое файла **history-final**, а затем — файла **masters-thesis**.

Если имя файла не указано, программа **cat** читает входные данные из `stdin` и возвращает их в `stdout`. Пример:

```
cat
Hello there.
Hello there.
Bye.
Bye.
Ctrl-D
```

Каждую строку, вводимую с клавиатуры, программа **cat** немедленно возвращает на экран. При вводе информации со стандартного ввода конец текста сигнализируется вводом специальной комбинации клавиш, как правило, **Ctrl+D**. Сокращённое название сигнала конца текста — EOT (end of text).

31.3.2. Перенаправление ввода и вывода

При необходимости можно перенаправить стандартный вывод, используя символ `>`, и стандартный ввод, используя символ `<`.

Фильтр (filter) — программа, которая читает данные из стандартного ввода, некоторым образом их обрабатывает и результат направляет на стандартный вывод. Когда применяется перенаправление, в качестве стандартного ввода и вывода могут выступать файлы. Как указывалось выше, по умолчанию, `stdin` и `stdout` относятся к клавиатуре и к экрану соответственно. Программа **sort** является простым фильтром — она сортирует входные данные и посылает результат на стандартный вывод. Совсем простым фильтром является программа **cat** — она ничего не делает с входными данными, а просто пересылает их на выход.

31.3.3. Использование состыкованных команд

Стыковку команд (pipelines) осуществляет командная оболочка, которая `stdout` первой команды направляет на `stdin` второй команды. Для стыковки используется символ `|`. Направить `stdout` команды **ls** на `stdin` команды **sort**:

```
ls | sort -r
notes
masters-thesis
history-final
english-list
```

Вывод списка файлов частями:

```
ls /usr/bin | more
```

Если необходимо вывести на экран последнее по алфавиту имя файла в текущем каталоге, можно использовать следующую команду:

```
ls | sort -r | head -1 notes
```

где команда **head -1** выводит на экран первую строку получаемого ей входного потока строк (в примере поток состоит из данных от команды **ls**), отсортированных в обратном алфавитном порядке.

31.3.4. Недеструктивное перенаправление вывода

Эффект от использования символа `>` для перенаправления вывода файла является деструктивным; т.е, команда

```
ls > file-list
```

уничтожит содержимое файла **file-list**, если этот файл ранее существовал, и создаст на его месте новый файл. Если вместо этого перенаправление будет сделано с помощью символов `>>`, то вывод будет приписан в конец указанного файла, при этом исходное содержимое файла не будет уничтожено.



Примечание

Перенаправление ввода и вывода и стыкование команд осуществляется командными оболочками, которые поддерживают использование символов `>`, `>>` и `|`. Сами команды не способны воспринимать и интерпретировать эти символы.

Глава 32. Режим суперпользователя

32.1. Какие бывают пользователи?

32.2. Для чего может понадобиться режим суперпользователя?

32.3. Как получить права суперпользователя?

32.4. Как перейти в режим суперпользователя?

32.1. Какие бывают пользователи?

Linux — система многопользовательская, а потому пользователь — ключевое понятие для организации всей системы доступа в Linux. Файлы всех пользователей в Linux хранятся отдельно, у каждого пользователя есть собственный домашний каталог, в котором он может хранить свои данные. Доступ других пользователей к домашнему каталогу пользователя может быть ограничен.

Суперпользователь в Linux — это выделенный пользователь системы, на которого не распространяются ограничения прав доступа. Именно суперпользователь имеет возможность произвольно изменять владельца и группу файла. Ему открыт доступ на чтение и запись к любому файлу или каталогу системы.

Среди учётных записей Linux всегда есть учётная запись суперпользователя — **root**. Поэтому вместо «суперпользователь» часто говорят «root». Множество системных файлов принадлежат **root**, множество файлов только ему доступны для чтения или записи. Пароль этой учётной записи — одна из самых больших драгоценностей системы. Именно с её помощью системные администраторы выполняют самую ответственную работу.

32.2. Для чего может понадобиться режим суперпользователя?

Системные утилиты, например, такие, как **Центр управления системой** или **Программа управления пакетами Synaptic** требуют для своей работы привилегий суперпользователя, потому что они вносят изменения в системные файлы. При их запуске выводится диалоговое окно с запросом пароля системного администратора.

32.3. Как получить права суперпользователя?

Для опытных пользователей, умеющих работать с командной строкой, существует два различных способа получить права суперпользователя.

Первый — это зарегистрироваться в системе под именем **root**.

Второй способ — воспользоваться специальной утилитой **su** (shell of user), которая позволяет выполнить одну или несколько команд от лица другого пользователя. По умолчанию эта утилита выполняет команду **sh** от пользователя **root**, то есть запускает командный интерпретатор. Отличие от предыдущего способа в том, что всегда известно, кто именно запускал **su**, а значит, ясно, кто выполнил определённое административное действие.

В некоторых случаях удобнее использовать не **su**, а утилиту **sudo**, которая позволяет выполнять только заранее заданные команды.



Важно

Для того чтобы воспользоваться командами **su** и **sudo**, необходимо быть членом группы **wheel**. Пользователь, созданный при установке системы, по умолчанию уже включён в эту группу.

В дистрибутивах Альт для управления доступом к важным службам используется подсистема **control**. **control** — механизм переключения между неким набором фиксированных состояний для задач, допускающих такой набор.

Команда **control** доступна только для суперпользователя (**root**). Для того, чтобы посмотреть, что означает та или иная политика **control** (разрешения выполнения конкретной команды, управляемой **control**), надо запустить команду с ключом **help**:

```
# control su help
```

Запустив **control** без параметров, можно увидеть полный список команд, управляемых командой (**facilities**) вместе с их текущим состоянием и набором допустимых состояний.

32.4. Как перейти в режим суперпользователя?

Для перехода в режим суперпользователя наберите в терминале команду **su -**.

Если воспользоваться командой **su** без ключа, то происходит вызов командного интерпретатора с правами **root**. При этом значение переменных окружения, в частности **\$PATH**, остаётся таким же, как у пользователя: в переменной **\$PATH** не окажется каталогов **/sbin**, **/usr/sbin**, без указания полного имени будут недоступны команды **route**, **shutdown**, **mkswap** и другие. Более того, переменная **\$HOME** будет указывать на каталог пользователя, все программы, запущенные в режиме суперпользователя, сохраняют свои настройки с правами **root** в каталоге пользователя, что в дальнейшем может вызвать проблемы.

Чтобы избежать этого, следует использовать **su -**. В этом режиме **su** запустит командный интерпретатор в качестве **login shell**, и он будет вести себя в точности так, как если бы в системе зарегистрировался **root**.

Глава 33. Команда sudo

33.1. Настройка control для работы sudo

33.2. Настройка sudo

Команда **sudo** может использоваться для выполнения пользователем какой-либо команды, требующей права суперпользователя (**root**), то есть получение прав **root** для выполнения какой-либо команды на время её выполнения.

33.1. Настройка control для работы sudo

В дистрибутивах Альт для управления доступом к важным службам используется подсистема control. control — механизм переключения между неким набором фиксированных состояний для задач, допускающих такой набор.

Для того, чтобы посмотреть, что означает та или иная политика **control** (разрешения выполнения конкретной команды, управляемой **control**), надо запустить команду с ключом help:

```
$ sudo control sudo help
```

Запустив **control** без параметров, можно увидеть полный список команд, управляемых командой (facilities) вместе с их текущим состоянием и набором допустимых состояний.

Штатное состояние политики sudo:

```
$ sudo control sudo  
wheelonly
```

Означает что пользователь из группы wheel имеет право запускать саму команду **sudo**, но не означает, что он через **sudo** может выполнить какую-то команду с правами root.

33.2. Настройка sudo

Для того, чтобы настроить работу **sudo**, необходимо с применением административных привилегий отредактировать файл **/etc/sudoers** при помощи специальной команды **visudo**.

Настройка по умолчанию:

```
WHEEL_USERS ALL=(ALL) NOPASSWD: ALL
```

Позволяет пользователям входящим в группу **wheel** выполнять через **sudo** любую команду с любого компьютера, не запрашивая их пароль.

Пример настройки:

```
user ALL = (ALL) ALL  
user ALL = NOPASSWD: /usr/bin/apt-get update
```

Позволяет пользователю **user** запускать все приложения через **sudo** с правами суперпользователя (root) с запросом пароля, а при выполнении команды **sudo apt-get update** пароль запрашиваться не будет.

Глава 34. Управление пользователями

34.1. Общая информация

34.2. Команда passwd

34.3. Добавления нового пользователя

34.4. Модификация пользовательских записей

34.1. Общая информация

Пользователи и группы внутри системы обозначаются цифровыми идентификаторами — UID и GID, соответственно.

Пользователь может входить в одну или несколько групп. По умолчанию он входит в группу, совпадающую с его именем. Чтобы узнать, в какие еще группы входит пользователь, введите команду **id**, вывод её может быть примерно следующим:

```
uid=500(test) gid=500(test) группы=500(test),16(rpm)
```

Такая запись означает, что пользователь *test* (цифровой идентификатор 500) входит в группы *test* и *rpm*. Разные группы могут иметь разный уровень доступа к тем или иным каталогам; чем в большее количество групп входит пользователь, тем больше прав он имеет в системе.



Примечание

В связи с тем, что большинство привилегированных системных утилит в дистрибутивах Альт имеют не SUID-, а SGID-бит, будьте предельно внимательны и осторожны в переназначении групповых прав на системные каталоги.

34.2. Команда passwd

Команда **passwd** поддерживает традиционные опции **passwd** и утилит **shadow**.

Синтаксис:

```
passwd [ОПЦИИ...] [ИМЯ ПОЛЬЗОВАТЕЛЯ]
```

Возможные опции:

- » **-d --delete** — удалить пароль для указанной записи;
- » **-f, --force** — форсировать операцию;
- » **-k, --keep-tokens** — сохранить не устаревшие пароли;
- » **-l, --lock** — заблокировать указанную запись;
- » **--stdin** — прочитывать новые пароли из стандартного ввода;
- » **-S, --status** — дать отчет о статусе пароля в указанной записи;
- » **-u, --unlock** — разблокировать указанную запись;
- » **-, --help** — показать справку и выйти;
- » **--usage** — дать короткую справку по использованию;
- » **-V, --version** — показать версию программы и выйти.

Код выхода: при успешном завершении **passwd** заканчивает работу с кодом выхода 0. Код выхода 1 означает, что произошла ошибка. Текстовое описание ошибки выводится на стандартный поток ошибок.

Пользователь может в любой момент поменять свой пароль. Единственное, что требуется для смены пароля — знать текущий пароль.

Только суперпользователь может обновить пароль другого пользователя.

34.3. Добавления нового пользователя

Для добавления нового пользователя используйте команды **useradd** и **passwd**:

```
# useradd test1

# passwd test1
passwd: updating all authentication tokens for user test1.

You can now choose the new password or passphrase.

A valid password should be a mix of upper and lower case letters,
digits, and other characters. You can use an 8 character long
password with characters from at least 3 of these 4 classes, or
a 7 character long password containing characters from all the
classes. An upper case letter that begins the password and a
digit that ends it do not count towards the number of character
classes used.

A passphrase should be of at least 3 words, 11 to 40 characters
long, and contain enough different characters.

Alternatively, if no one else can see your terminal now, you can
pick this as your password: "holder5dinghy-Arm".

Enter new password:
```

В результате описанных действий в системе появился пользователь *test1* с некоторым паролем. Если пароль оказался слишком слабым с точки зрения системы, она об этом предупредит (как в примере выше). Пользователь в дальнейшем может поменять свой пароль при помощи команды **passwd** — но если он попытается поставить слабый пароль, система откажет ему (в отличие от *root*) в изменении.

В Альт Сервер для проверки паролей на слабость используется модуль PAM *passwdqc*.

Программа **useradd** имеет множество параметров, которые позволяют менять её поведение по умолчанию. Например, можно принудительно указать, какой будет UID или какой группе будет принадлежать пользователь.

34.4. Модификация пользовательских записей

Для модификации пользовательских записей применяется утилита **usermod**:

```
# usermod -G audio,rpm,test1 test1
```

Такая команда изменит список групп, в которые входит пользователь *test1* — теперь это *audio*, *rpm*, *test1*.

```
# usermod -l test2 test1
```

Будет произведена смена имени пользователя с *test1* на *test2*.

Команды **usermod -L test2** и **usermod -U test2** соответственно временно блокируют возможность входа в систему пользователю *test2* и возвращают всё на свои места.

Изменения вступят в силу только при следующем входе пользователя в систему.

При неинтерактивной смене или задании паролей для целой группы пользователей используйте утилиту **chpasswd**. На стандартный вход ей следует подавать список, каждая строка которого будет выглядеть как **имя:пароль**.

34.5. Удаление пользователей

Для удаления пользователей используйте **userdel**.

Команда **userdel test2** удалит пользователя *test2* из системы. Если будет дополнительно задан параметр **-r**, то будет уничтожен и домашний каталог пользователя. Нельзя удалить пользователя, если в данный момент он еще работает в системе.

Глава 35. Система инициализации systemd и sysvinit

35.1. Запуск операционной системы

35.2. Системы инициализации systemd и sysvinit

35.3. Примеры команд управления службами, журнал в systemd

35.4. Журнал в systemd

35.1. Запуск операционной системы

35.1.1. Запуск системы

Алгоритм запуска компьютера приблизительно такой:

1. BIOS компьютера.
2. Загрузчик системы (например, LILO, GRUB или другой). В загрузчике вы можете задать параметры запуска системы или выбрать систему для запуска.
3. Загружается ядро Linux.
4. Запускается на выполнение первый процесс в системе — **init**.

Ядром запускается самая первая программа в системе **init**. Её задачей является запуск новых процессов и повторный запуск завершившихся. Вы можете посмотреть, где расположился **init** в иерархии процессов вашей системы, введя команду **pstree**.

От конфигурации **init** зависит, какая система инициализации будет использована.

35.1.2. Система инициализации

Система инициализации — это набор скриптов, которые будут выполнены при старте системы.

Существуют разные системы инициализации, наиболее популярные системы: **sysvinit** (и её модификации) и **systemd**.

В Альт Сервер используется **systemd**.

35.2. Системы инициализации systemd и sysvinit

35.2.1. sysvinit

System V — классическая схема инициализации, на которой базируются многие дистрибутивы. Привычна и довольно проста для понимания: **init** описывает весь процесс загрузки в своем конфигурационном файле **/etc/inittab**, откуда вызываются другие программы и скрипты на определенном этапе запуска.

35.2.2. systemd

systemd является альтернативной системой инициализации Linux, вобравшей в себя достоинства классического **System V init** и более современных **launchd** (OS X), **SMF** (Solaris) и **Upstart** (Ubuntu, Fedora), но при этом лишенной многих их недостатков. Он разрабатывался для обеспечения лучшего выражения зависимостей между службами, что позволяет делать одновременно больше работы при загрузке системы, и уменьшить время загрузки системы.

systemd (system daemon) реализует принципиально новый подход к инициализации и контролю работы системы. Одним из ключевых новшеств этого подхода является высокая степень параллелизации запуска служб при инициализации системы, что в перспективе позволяет добиться гораздо более высокой скорости, чем традиционный подход с последовательным запуском взаимозависимых служб. Другим важным моментом является контроль над точками монтирования (не-жизненно-важные файловые системы можно монтировать только при первом обращении к ним, не тратя на это время при инициализации системы) и устройствами (можно запускать и останавливать определенные службы и при появлении или удалении заданных устройств). Для отслеживания групп процессов используется механизм cgroups, который также может быть использован для ограничения потребляемых ими системных ресурсов.

Удобство **systemd** особенно заметно на компьютерах для домашнего пользования — когда пользователи включают и перезагружают компьютер ежедневно. В отличие от **sysvinit**, подвисание при запуске одного сервиса не приведет к остановке всего процесса загрузки.

35.3. Примеры команд управления службами, журнал в systemd

Обратите внимание, что команды **service** и **chkconfig** продолжают работать в мире **systemd** практически без изменений. Тем не менее, в этой таблице показано как выполнить те же действия с помощью встроенных утилит **systemctl**.

Таблица 35.1. Команды управления службами

Команды Sysvinit	Команды Systemd	Примечания
service frobozz start	systemctl start frobozz.service	Используется для запуска службы (не перезагружает постоянные)
service frobozz stop	systemctl stop frobozz.service	Используется для остановки службы (не перезагружает постоянные)
service frobozz restart	systemctl restart frobozz.service	Используется для остановки и последующего запуска службы
service frobozz reload	systemctl reload frobozz.service	Если поддерживается, перезагружает файлы конфигурации без прерывания незаконченных операций
service frobozz condrestart	systemctl condrestart frobozz.service	Перезапускает службу, если она уже работает
service frobozz status	systemctl status frobozz.service	Сообщает, запущена ли уже служба
ls /etc/rc.d/init.d/	systemctl list-unit-files --type=service (preferred) ls /lib/systemd/system/*.service /etc/systemd/system/*.service	Используется для отображения списка служб, которые можно запустить или остановить. Используется для отображения списка всех служб.
chkconfig frobozz on	systemctl enable frobozz.service	Включает службу во время следующей перезагрузки, или любой другой триггер
chkconfig frobozz off	systemctl disable frobozz.service	Выключает службу во время следующей перезагрузки, или любой другой триггер
chkconfig frobozz	systemctl is-enabled frobozz.service	Используется для проверки, сконфигурирована ли служба для запуска в текущем окружении
chkconfig --list	systemctl list-unit-files --type=service(preferred) ls /etc/systemd/system/*.wants/	Выводит таблицу служб. В ней видно, на каких уровнях загрузки они (не)запускаются
chkconfig frobozz --list	ls /etc/systemd/system/*.wants/frobozz.service	Используется, для отображения на каких уровнях служба (не)запускается
chkconfig frobozz --add	systemctl daemon-reload	Используется, когда вы создаете новую службу или модифицируете любую конфигурацию

35.4. Журнал в systemd

В **systemd** включена возможность ведения системного журнала. Для чтения журнала следует использовать команду **journalctl**. По умолчанию, больше не требуется запуск службы **syslog**.

Вы можете запускать **journalctl** с разными ключами:

- **journalctl -b** — покажет сообщения только с текущей загрузки;
- **journalctl -f** — покажет только последние сообщения.

Так же вы можете посмотреть сообщения определенного процесса:

- **journalctl _PID=1** — покажет сообщения первого процесса (init).

Для ознакомления с прочими возможностями, читайте руководство по **journalctl**. Для этого используйте команду **man journalctl**.

Глава 36. Документация

36.1. Экранная документация

36.2. Документация по пакетам

Каждый объект системы Linux обязательно сопровождается документацией, описывающей их назначение и способы использования. От пользователя системы не требуется заучивать все возможные варианты взаимодействия с ней. Достаточно понимать основные принципы её устройства и уметь находить справочную информацию.

Не пренебрегайте чтением документации: она поможет вам избежать многих сложностей, сэкономят массу времени и усилий при установке, настройке и администрировании системы, поможет найти нужное для работы приложение и быстро разобраться в нём.

36.1. Экранная документация

Почти все системы семейства UNIX, включая систему Linux, имеют экранную документацию. Её тексты содержат документацию по системным командам, ресурсам, конфигурационным файлам и т. д., а также могут быть выведены на экран в процессе работы.

36.1.1. man

Для доступа к экранной документации используется команда **man** (сокращение от manual). Каждая страница руководства посвящена одному объекту системы. Для того чтобы прочесть страницу руководства по программе, необходимо набрать **man название_программы**. К примеру, если вы хотите узнать, какие опции есть у команды **date**, вы можете ввести команду:

```
$ man date
```

Большинство экранной документации написано для пользователей, имеющих некоторое представление о том, что делает данная команда. Поэтому большинство текстов экранной документации содержит исключительно технические детали команды без особых пояснений. Тем не менее, экранная документация оказывается очень ценной в том случае, если вы помните название команды, но её синтаксис просто выпал у вас из памяти.

Поиск по описаниям **man** осуществляется командой **apropos**. Если вы точно не знаете, как называется необходимая вам программа, то поиск осуществляется по ключевому слову, к примеру, **apropos date** или при помощи ввода слова, обозначающего нужное действие, после команды **man -k** (например, **man -k сору**). Слово, характеризующее желаемое для вас действие, можно вводить и на русском языке. При наличии русского перевода страниц руководства **man** результаты поиска будут выведены на запрашиваемом языке.

«Страница руководства» занимает, как правило, больше одной страницы экрана. Для того чтобы читать было удобнее, **man** запускает программу постраничного просмотра текстов. Страницы перелистывают пробелом, для выхода из режима чтения описания команд **man** необходимо нажать на клавиатуре **q**. Команда **man man** выдаёт справку по пользованию самой командой **man**.

Документация в подавляющем большинстве случаев пишется на простом английском языке. Необходимость писать на языке, который будет более или менее понятен большинству пользователей, объясняется постоянным развитием Linux. Дело не в том, что страницу руководства нельзя перевести, а в том, что её придётся переводить всякий раз, когда изменится описываемый ею объект! Например, выход новой версии программного продукта сопровождается изменением его возможностей и особенностей работы, а следовательно, и новой версией документации.

Тем не менее, некоторые наиболее актуальные руководства существуют в переводе на русский язык. Свежие версии таких переводов на русский язык собраны в пакете *man-pages-ru*. Установив этот пакет, вы добавите в систему руководства, для которых есть перевод, и **man** по умолчанию будет отображать их на русском языке.

36.1.2. info

Другой источник информации о Linux и составляющих его программах — справочная подсистема *info*. Страница руководства, несмотря на обилие ссылок различного типа, остаётся «линейным» текстом, структурированным только логически. Документ *info* — это настоящий гипертекст, в котором множество небольших страниц объединены в дерево. В каждом разделе документа *info* всегда есть оглавление, из которого можно перейти к нужному подразделу, а затем вернуться обратно (ссылки для перемещения по разделам текста помечены *). Для получения вспомогательной информации о перемещении по тексту используйте клавишу **h**. Полное руководство *info* вызывается командой **info info**. Команда **info**, введённая без параметров, предлагает пользователю список всех документов *info*, установленных в системе.

36.2. Документация по пакетам

Дополнительным источником информации об интересующей вас программе, в основном на английском языке, является каталог **/usr/share/doc** — место хранения разнообразной документации.

Каждый пакет также содержит поставляемую вместе с включённым в него ПО документацию, располагающуюся обычно в каталоге **/usr/share/doc/имя_пакета**. Например, документация к пакету *foo-1.0-alt1* находится в **/usr/share/doc/foo-1.0-alt1**. Для получения полного списка файлов документации, относящихся к пакету, воспользуйтесь командой **rpm -qd имя_установленного_пакета**.

В документации к каждому пакету вы можете найти такие файлы как **README**, **FAQ**, **TODO**, **ChangeLog** и другие. В файле **README** содержится основная информация о программе — имя и контактные данные авторов, назначение, полезные советы и пр. **FAQ** содержит ответы на часто задаваемые вопросы; этот файл стоит прочитать в первую очередь, если у вас возникли

проблемы или вопросы по использованию программы, поскольку большинство проблем и сложностей типичны, вполне вероятно, что в **FAQ** вы тут же найдёте готовое решение. В файле **TODD** записаны планы разработчиков на реализацию той или иной функциональности. В файле **ChangeLog** записана история изменений в программе от версии к версии.

Для поиска внешней информации о программе, например, адреса сайта программы в сети Интернет можно использовать команду **rpm -qi имя_установленного_пакета**. В информационном заголовке соответствующего пакета, среди прочей информации, будет выведена искомая ссылка.

Возможно, будет полезно знать расположение собрания практических рекомендаций по самым различным вопросам, связанным с использованием Linux. Файлы **HOWTO** в формате HTML (от англ. how to — «как сделать») каталога **/usr/share/doc/HOWTO/** (при условии их наличия в системе) содержат многообразную информацию о работе Linux-систем.

Часть VII. Техническая поддержка продуктов «Базальт СПО»

Содержание

37. Покупателям нашей продукции

38. Пользователям нашей продукции

Глава 37. Покупателям нашей продукции

Право на получение консультационной и технической поддержки вы приобретаете при покупке большинства продуктов торговой марки Альт. Сроки и объём помощи указаны в талоне технической поддержки. Техническая поддержка дистрибутива может быть расширена в зависимости от потребностей пользователя.

Для получения информации об условиях технической поддержки облачного дистрибутива следует обратиться к своему облачному провайдеру.

Глава 38. Пользователям нашей продукции

Задавать вопросы или обсуждать их с сообществом пользователей дистрибутивов «Альт» можно на форуме или в списках рассылки.

Помощь сообщества:

- » Форум: <http://forum.altlinux.org>
- » Списки рассылки: <http://lists.altlinux.org/>
- » Сообщить об ошибке: <http://bugs.altlinux.org/>
- » Репозиторий: <http://packages.altlinux.org/>
- » Сборочная среда: <http://git.altlinux.org/>

Ресурсы компании «Базальт СПО»:

- Сайт компании: <http://www.basealt.ru/>
- Контакты: <http://basealt.ru/about/contacts/>
- Новости обновлений безопасности: <http://cve.basealt.ru/>

Форум и списки рассылки читают опытные пользователи, профессиональные системные администраторы и разработчики «Базальт СПО». Сообщество пользователей и специалистов окажет содействие в поиске ответа на ваш вопрос или посоветует выход из сложной ситуации. При обращении к данному виду помощи у вас нет гарантии на полноту и своевременность ответа, но мы стараемся не оставлять без ответа вопросы, задаваемые в списках.