# 

# 

# 

# 

# 

# 

Документация к проекту DigitalSkills-2022

[**Руководство администратора**](#_dfqibb2jyvl5) **2**

[Топология сети](#_x2oiggddp7oo) 2

[**Планируемая IP-адресация в облачной платформе.**](#_b694vgixmabg) **3**

[**Планируемая IP-адресация в локальной инфраструктуре.**](#_69a0ky2i6bl4) **3**

[**Таблица функционала виртуальных машин.**](#_10m1h3vlfy2t) **4**

[**Описание технических решений**](#_ptqu5n7rxdpl) **5**

[**1 VPN**](#_x418tketwcgl) **5**

[**1.1 Реализация туннельного зашифрованного соединения между локальной и облачной инфраструктурой.**](#_fx2b69pa5tuw) **5**

[**1.2 Реализация удаленного соединения для привлекаемых сотрудников.**](#_l2ee7yi12myr) **6**

[**2 Централизованное управление пользователями.**](#_rr50xvsmrbcw) **10**

[**3 Отказоустойчивое хранилище**](#_46k0v83mdbm4) **15**

[**4 Мониторинг инфраструктуры**](#_ftla6tj3qzkn) **23**

[**Руководство постоянного сотрудника**](#_q00wkwvnmb27) **25**

[Авторизация на рабочем месте](#_ei5fdt4ub88n) 25

[Использование хранилища файлов](#_ncmp3mfqz71c) 26

[Использование CI\CD-инфраструктуры](#_bhal0glowqje) 31

[**Руководство удаленного привлекаемого сотрудника**](#_iiath6ofvm2f) **32**

[Подключение к VPN](#_buj8ezicld01) 32

`

# Руководство администратора

## Топология сети

## 

Рисунок 1. План сети

## Планируемая IP-адресация в облачной платформе.

*В рамках демонстрационного стенда*.

|  |  |
| --- | --- |
| Виртуальная машина | IP-адрес |
| C-RTR | 10.1.2.1/24 |
| C-GIT | 10.1.2.5/24 |
| C-SRV1 | 10.1.2.3/24 |
| C-PROD | 10.1.2.8/24 |
| C-TEST | 10.1.2.9/24 |
| C-INGRESS | 10.1.2.2/24 |
| С-BACKUP | 10.1.2.4/24 |

## Планируемая IP-адресация в локальной инфраструктуре.

*В рамках демонстрационного стенда.*

|  |  |
| --- | --- |
| Виртуальная машина | IP-адрес |
| L-RTR | 10.1.1.1/24 |
| PC-1 | DHCP |
| PC-X | DHCP |

## Таблица функционала виртуальных машин.

В рамках демонстрационного стенда виртуальные машины выполняют следующие функции.

|  |  |
| --- | --- |
| Виртуальная машина | Функционал |
| C-RTR | VPN, Routing, FreeIPA, GlusterFS |
| C-SRV1 | Zabbix, PostgreSQL, Docker-Swarm worker |
| C-TEST | Доступный из внутренней сети хост, ответственный за тестирование и отладку ПО в рамках CI\CD |
| C-PROD | Доступный из внешней сети хост, ответственный за тестирование и отладку ПО в рамках CI\CD |
| С-BACKUP | BackupStorage, GlusterFS-node, DockerSwarm-worker |
| C-INGRESS | LoadBalancer, NextCloud-host, Nginx, Docker-Swarm-leader |
| C-GIT | GitLab |
| L-RTR | VPN, Routing, FreeIPA, GlusterFS-node |
| PC-1, PC-X | Локальные ПК постоянных сотрудников компании в офисе. |
| RC-W, RC-U | Удаленные ПК привлекаемых сотрудников. |

# Описание технических решений

Операционная система всех инфраструктурных ОС - Astra Linux 2.12. Решение также возможно реализовать на Astra Linux 1.7.

## 1 VPN

В рамках реализации технического задания необходимо решить две проблемы удаленного соединения:

1. Реализация туннельного зашифрованного соединения между локальной и облачной инфраструктурой.
2. Реализация удаленного соединения для привлекаемых сотрудников.

## 1.1 Реализация туннельного зашифрованного соединения между локальной и облачной инфраструктурой.

Туннельное соединение реализовано с помощью технологии **WireGuard.**

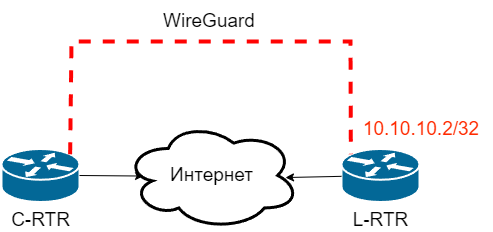


Рисунок 2. VPN Диаграмма

Конфигурация настроена на основе публичных и приватных ключей, генерируемых сервером WireGuard. Конфигурация жестко привязана к инициализации лишь одной пары клиентов (C-RTR и L-RTR соответственно). Внутри туннеля реализована статическая маршрутизация из локальной сети компании до облачной. WireGuard-сервер на C-RTR прослушивает порт UDP 51820. L-RTR выступает в качестве клиента.

WireGuard автоматически конфигурируется при включении роутеров. Не требует ручной активации. Также, реализован механизм PersistentKeepalive каждые 5 секунд, для поддержки стабильного соединения между узлами. Образец конфигурации каждого узла представлен ниже.

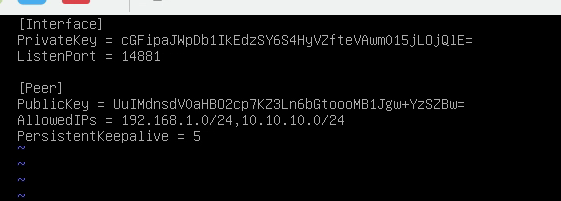


Рисунок 3. Конфигурация C-RTR

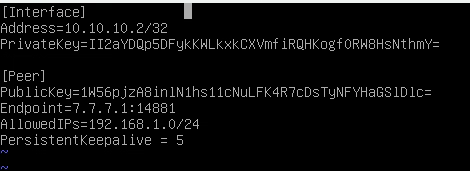


Рисунок 4. Конфигурация L-RTR

## 1.2 Реализация удаленного соединения для привлекаемых сотрудников.

Решение представлено VPN-сервисом OpenConnect. Аутентификация будет происходить через доменных пользователей в FreeIPA, которыми будет удобно управлять через графический интерфейс.

Сервер развернут на C-RTR. В данный момент система авторизует всех пользователей из домена FreeIPA. Конфигурационный файл расположен по пути **/etc/ocserv/ocserv.conf** , в этом же каталоге **/etc/ocserv** расположен Kerberos-keytab для аутентификации службы OpenConnect в домене FreeIPA.

Для подключения к серверу OpenConnect используются графические утилиты для Windows (OpenConnect-GUI) и различных дистрибутивов Linux.

Ниже продемонстрирован пример подключения пользователя из Windows 10.

Сервер OpenConnect прослушивает порт 6443, ожидает соединение на внешнем интерфейсе C-RTR (в рамках демонстрационного стенда адрес 7.7.7.2)

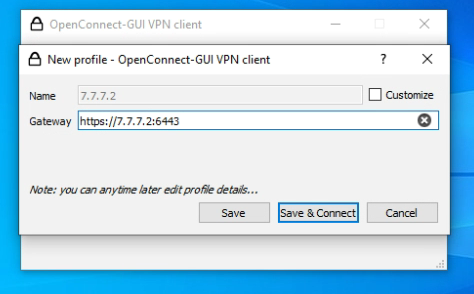


Рисунок 5. Пример начальной конфигурации для пользователей

При подключении не возникнет ошибок с сертификатом. Вводим логин пользователя в формате - [username@digital.ru](mailto:username@digital.ru)

Логотип “зеленого замка” символизирует успешное подключение к инфраструктуре

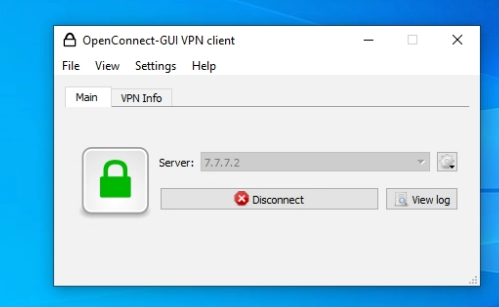


Рисунок 6. Пример успешного подключения к VPN

После подключения, проверяем доступность внутренних ресурсов компании.

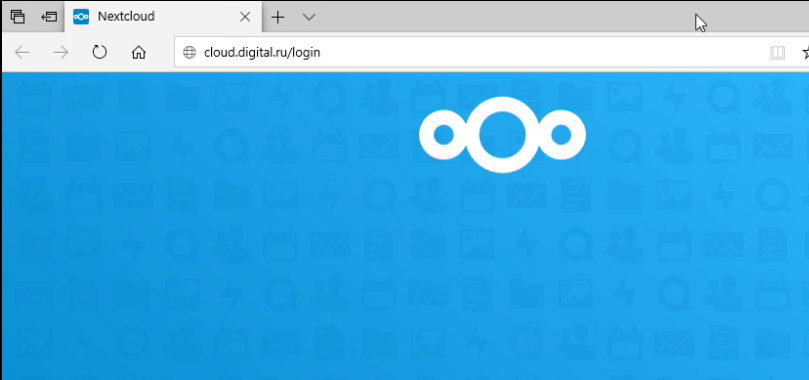


Рисунок 7. Доступ по DNS-зонам внутри компании

VPN-клиенты имеют доступ только до облачной инфраструктуры.

OpenConnect проверяет статус учетной записи в домене, в случае если пароль устарел или срок действия профиля закончился, то доступ будет отклонен.

OpenConnect также поддерживает функционал отключения подключения со стороны сервера, для этого в консоли введите команду -

**occtl show users**

Она отобразит вывод всех подключенных пользователей.

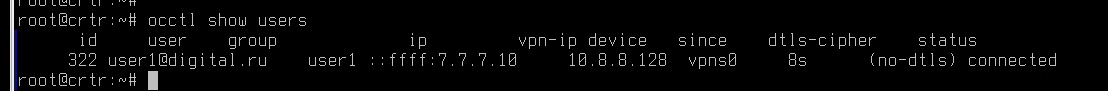


Рисунок 8. Список подключенных аккаунтов.

Отключить активную сессию можно командой -

**occtl disconnect user <username>**



Рисунок 9. Отключение пользователя

Стоит учитывать то, что пользователи FreeIPA имеют по-умолчанию пароль с истекшим сроком действия, предварительно необходимо аутентифицироваться под любым компьютером в локальной инфраструктуре и изменить пароль с установленного ранее на новый.

Подробнее об этом в официальной документации разработчиков FreeIPA - <https://www.freeipa.org/page/New_Passwords_Expired>

## 2 Централизованное управление пользователями.

Централизованное управление пользователями выполнено на базе FreeIPA.

Развернутый домен - **digital.ru.**

Доменная инфраструктура состоит из двух контроллеров домена с включенной репликацией доменной информации, а также Центра сертификации FreeIPA.

Топология репликации:

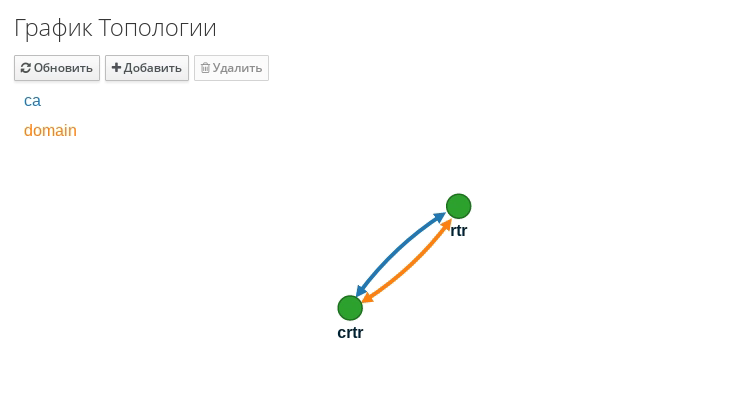


Рисунок 10. График репликации.

Контроллеры домена размещаются на C-RTR и L-RTR.

Доступ к системам администрирования доступен с любого локального компьютера в офисе. Пользователь **director** имеет функционал администратора домена. Также присутствует стандартный пользователь **admin.**

Таблица доступа.

|  |  |
| --- | --- |
| URL | Логин\пароль |
| https://c-rtr.digital.ru | **director\P@ssw0rd**  **admin\P@ssw0rd** |
| https://l-rtr.digital.ru | **director\P@ssw0rd**  **admin\P@ssw0rd** |

Репликация контроллеров домена позволяет одновременно хранить информацию о учетных записях, DNS-зонах и записях в них на двух устройствах. Оба сервера взаимозаменяют друг друга. При отказе одного доменного контроллера работу принимает второй доступный контроллер.

Интерфейс управления интуитивно-понятный. Рассмотрим основные необходимые инструменты.

Вкладка “Идентификация” → “Пользователи”. Отобразит список активных пользователей.

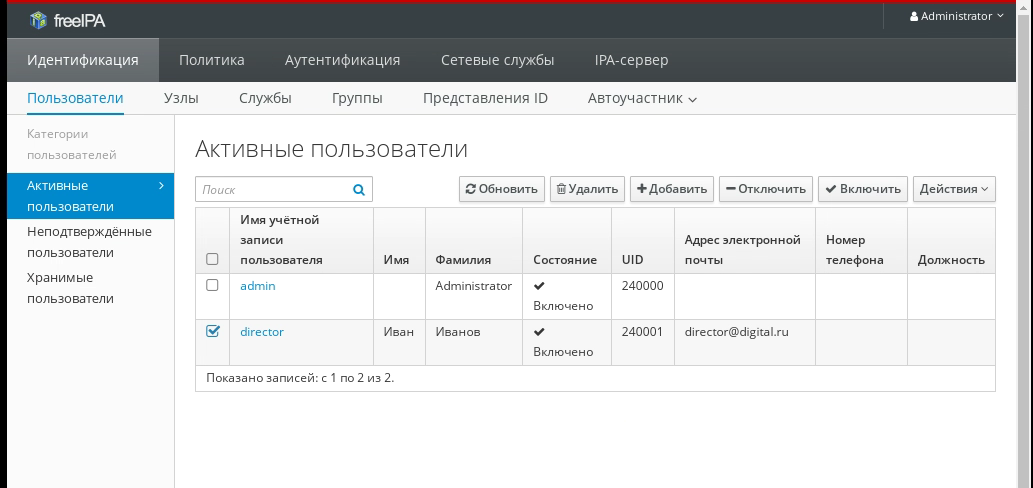


Рисунок 11. Информация о пользователях домена.

Вкладка “Идентификация” → “Узлы”. Отобразит список активных компьютеров в домене.

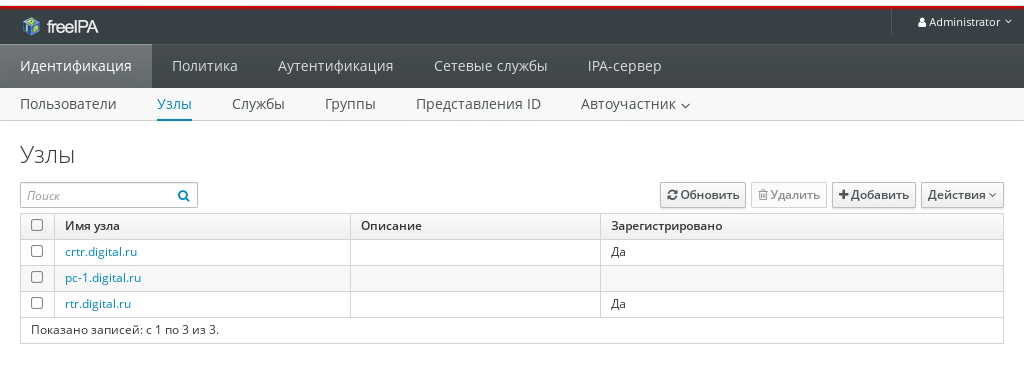


Рисунок 12. Информация о узлах в домене.

Вкладка “Идентификация” → “Группы”. Отобразит список групп пользователей в домене.

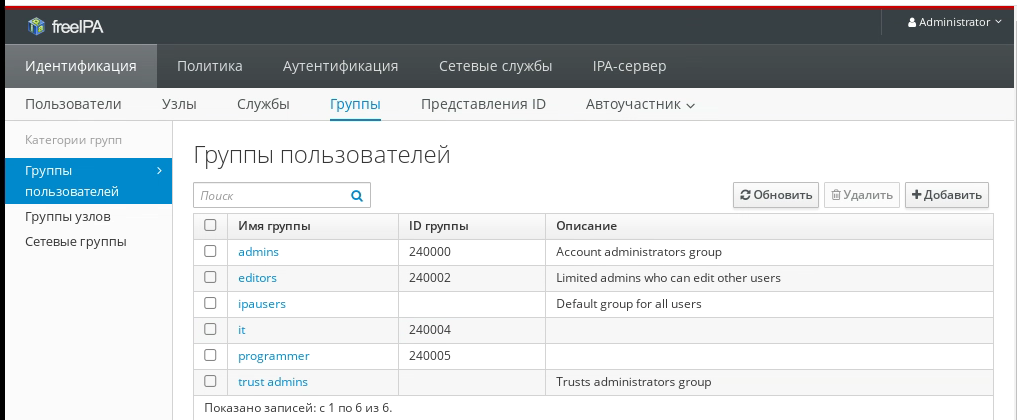


Рисунок 13. Информация о группах пользователей в домене.

Открыв любого пользователя откроется возможность изменять его параметры и свойства, а также возможность его удаления, для этого выберите параметр “Действия” -> “Удалить”.

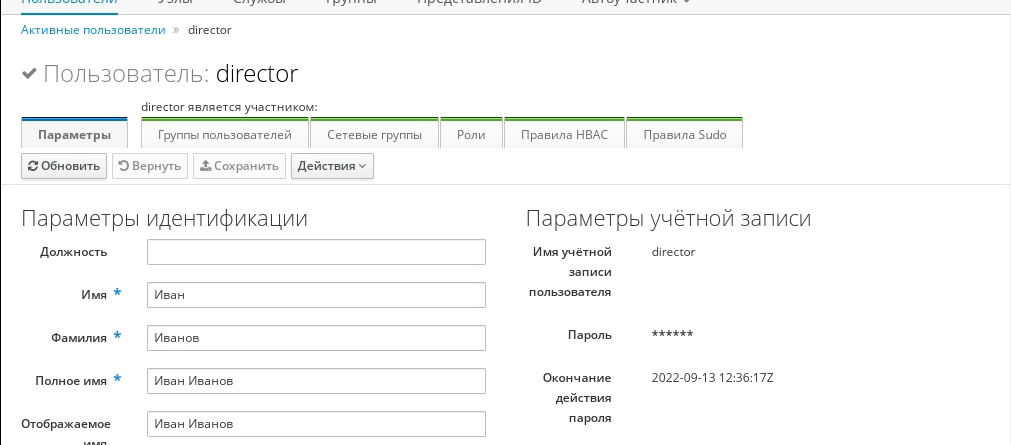


Рисунок 14. Пример интерфейса настроек учетной записи сотрудника

После удаления учетной записи, доступ до инфраструктурных систем теряется.

Также, например, можно реализовать срок действия аккаунта. Актуально для привлекаемых сотрудников. Установите время окончания контракта тут. По истечению

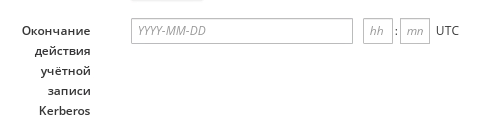


Рисунок 15. Параметр настройки окончания действия УЗ в домене

В параметрах “Сетевые службы” → “DNS” можно редактировать DNS-зону. DNS реплицируется между контроллерами домена.

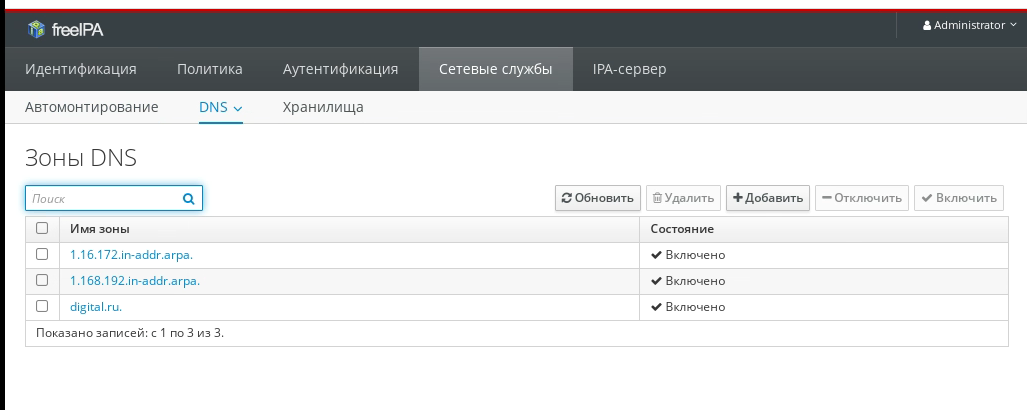


Рисунок 16. Управление DNS

На вкладке IPA-Сервер можно назначать пользовательские роли, в зависимости от уровня доступа.

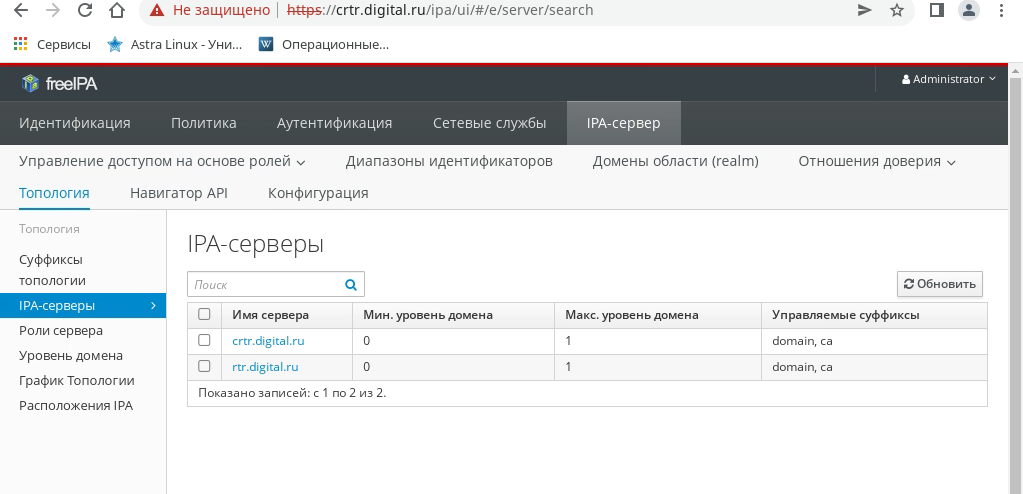


Рисунок 17. Управление доменом.

Удаление пользователя выполняется также средствами FreeIPA.

## 3 Отказоустойчивое хранилище

В целях обеспечения доступности до хранилища с различных устройств под управлением ОС на базе Linux или Windows, было принято решение развернуть облачное файловое хранилище на базе решения NextCloud.

NextCloud разворачивается с применением docker-compose на машинах C-INGRESS и С-BACKUP.

Для обеспечения реплицирования используется общее сетевое хранилище GlusterFS, развернутое на машинах C-RTR,C-BACKUP,L-RTR. Распределение именно таким образом позволяет добиться двойной репликации в пределах облака, а также сохранения файлов в локальном хранилище на сервере компании.

Для обеспечения отказоустойчивости контейнеров используется Docker Swarm. В следующем режиме:

|  |  |
| --- | --- |
| Имя виртуальной машины | Роль в Docker Swarm |
| C-INGRESS | Leader |
| C-BACKUP | Worker |
| C-SRV1 | Worker |

Общая схема отказоустойчивого хранилища представлена на рисунке:

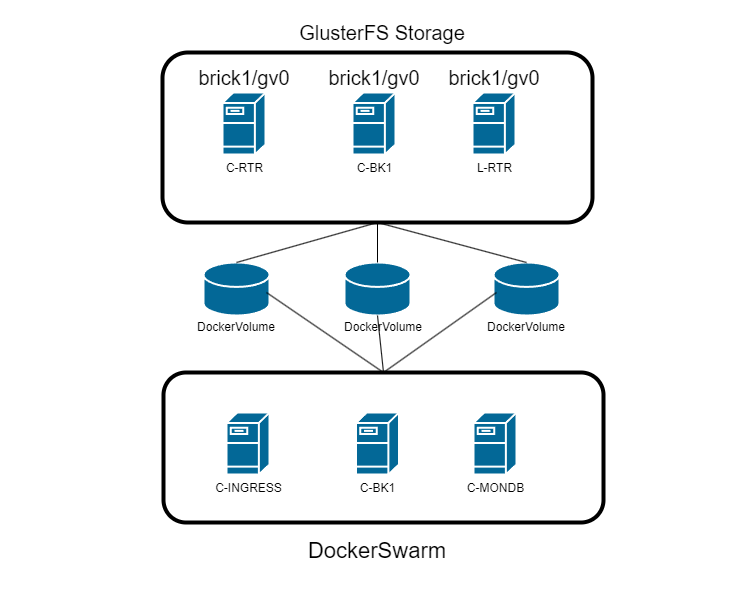


Рисунок 18. Схема отказоустойчивого хранилища

Volume Docker-контейнера NextCloud и MariaDB хранится на GlusterFS. При падении одной из ноды DockerSwarm, запущенные контейнеры переносятся на следующую доступную ноду с полным сохранением работоспособности.

GlusterFS в свою очередь настроен так, что данные записанные на сетевой ресурс автоматически реплицируются на все три файловых хоста.

Напротив, же удаление файлов выполняется только с одного хоста, копии сохраняются на двух остальных.



Рисунок 19. Docker-Compose для сборки Docker Swarm

Для доступа до NextCloud реализован Haproxy, который динамически отслеживает доступность экземпляров приложения, а также обеспечивает к нему доступ по HTTPS.

Сервер доступен по имени <https://cloud.digital.ru> для всех внутренних пользователей офиса, а также VPN-клиентов, рекомендуется использование бразуера Firefox, Google Chrome или Chromium и т.д.

Доступ в систему через логин и пароль из домена FreeIPA. По текущим настройкам доступ с NextCloud имеют все пользователи в группе ipausers.

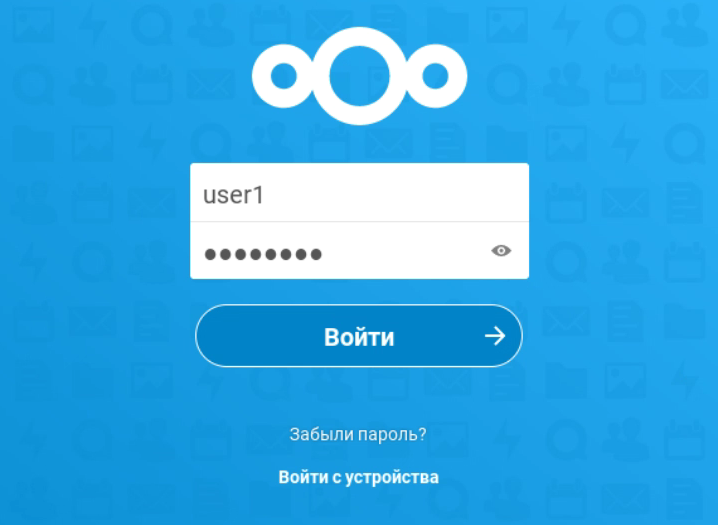


Рисунок 20. Вход в NextCloud

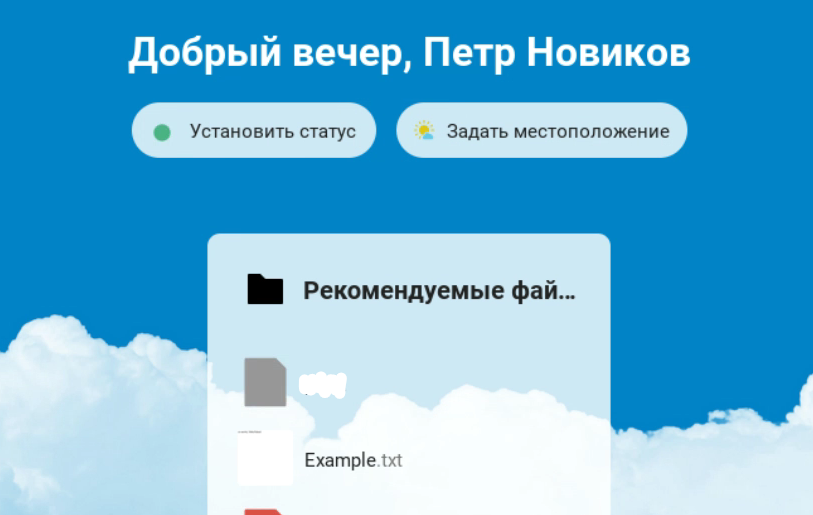


Рисунок 21. Приветствие новых пользователей.

NextCloud имеет широкий функционал, включая корпоративный мессенджер, возможность совместно редактировать файлы, встроенный видеоплеер.

Стоит отметить, что NextCloud также использует резервный доменный контроллер для аутентификации

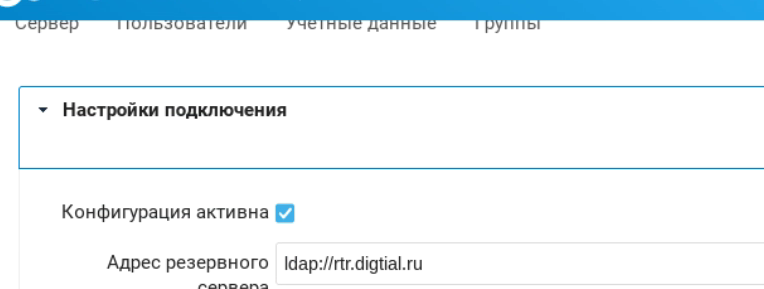


Рисунок 22. Конфигурация резервного доменного контроллера

Файлы, сохраненные в облаке являются пользовательскими и изначально доступ к ним уникален. Но к любому файлу можно открыть доступ для совместного использования, например, откроем файл Example.txt.

Открываем “Боковую панель” → “Общий доступ” → “Общий доступ по ссылке”

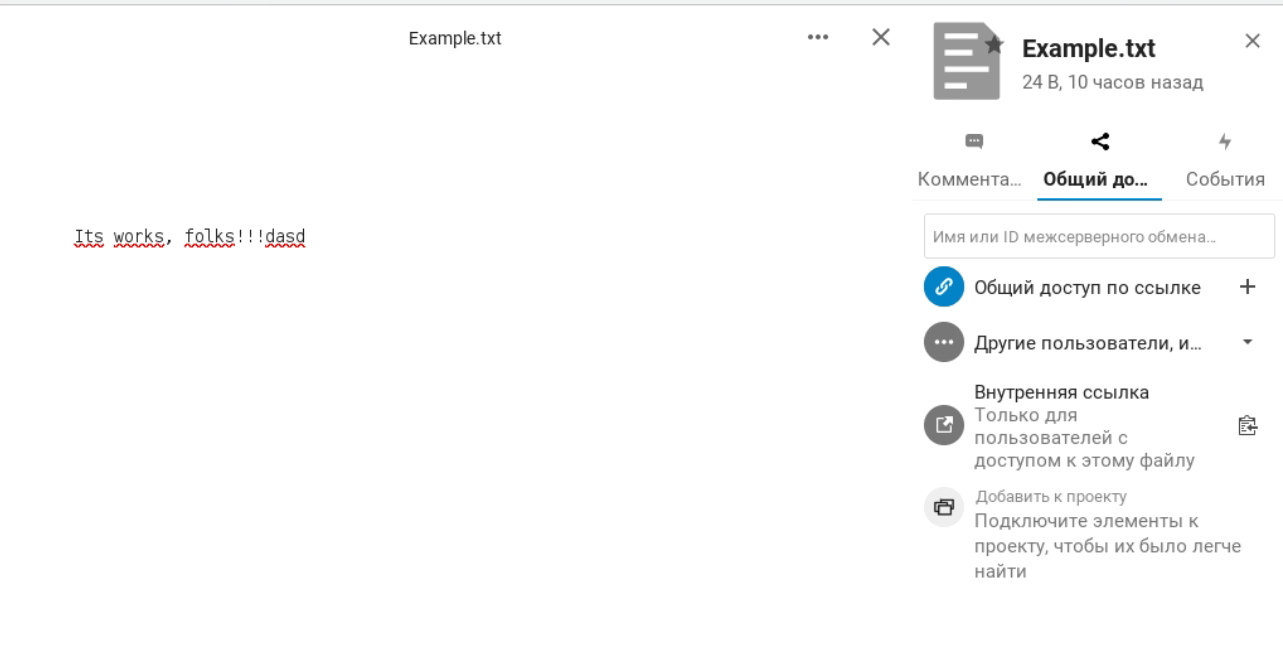


Рисунок 23. Включение общего доступа.

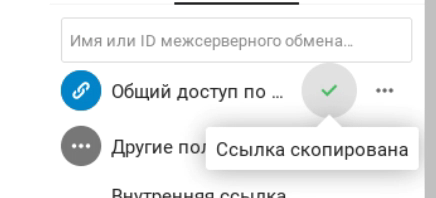


Рисунок 24. Скопировали ссылку на общее редактирование

Кликните по настройкам общего доступа по ссылке и выберите “Разрешить редактирование”

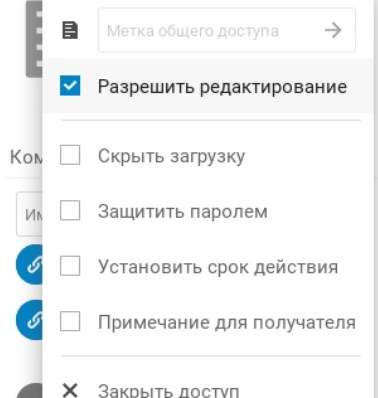


Рисунок 25. Включение редактирования для пользователей по ссылке.

Теперь по ссылке пользователи могут редактировать документ.

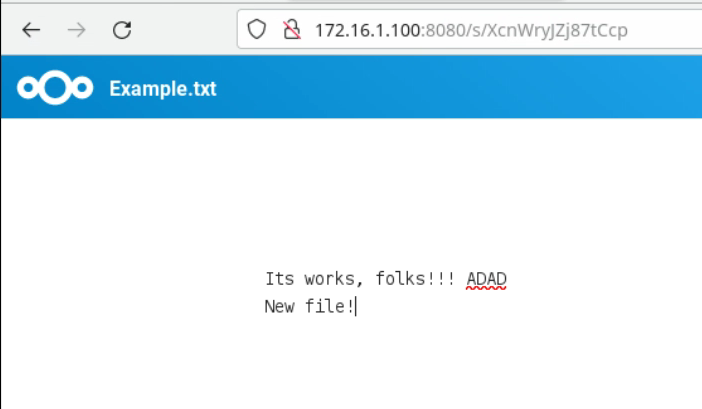


Рисунок 26. Совместное редактирование одного документа.

Для полного ознакомления с NextCloud следует ознакомиться с User-Guide на английском языке, который автоматически создается при первом входе в NextCloud под учетной записью из домена digital.ru.

Уязвимые места в настроенной инфраструктуре является:

1. Потеря сетевой связности с файловой нодой в GlusterFS.
2. Выход из строя HAProxy.

В аварийном случае, необходимо выбрать вручную другой адрес GlusterFS ноды. Учитывая, что данные реплицируются выбирайте любой доступный узел.

После этого выполните перезапуск контейнеров на узле, где возникла проблема с доступом к файловому ресурсу. Данные не будут утеряны в силу постоянной репликации. При разрыве соединения пользователи получат уведомление через систему мониторинга Zabbix.

HAProxy является единой точкой отказа доступа до графического интерфейса NextCloud, но не приведет к потере данных.

При возникновении проблем, можно выполнить развертывание резервного HAProxy. Для этого потребуется ранее выданный сертификат SSL перенести на новый HAProxy, а также внести изменения в конфигурационный файл /etc/haproxy/haproxy.cfg

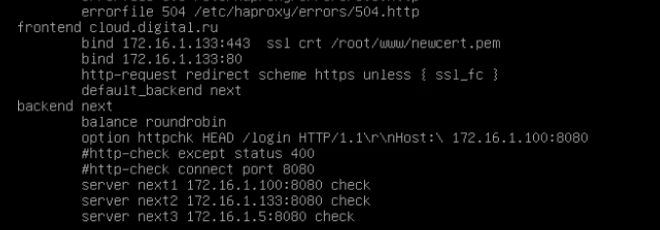


Рисунок 27. Инфраструктурный пример конфигурации HAProxy.

Вместо IP-адреса в секции Frontend - **172.16.1.133**

Следует записать новый, в зависимости от выбранного вами.

Также, измените запись в DNS-сервере FreeIPA.

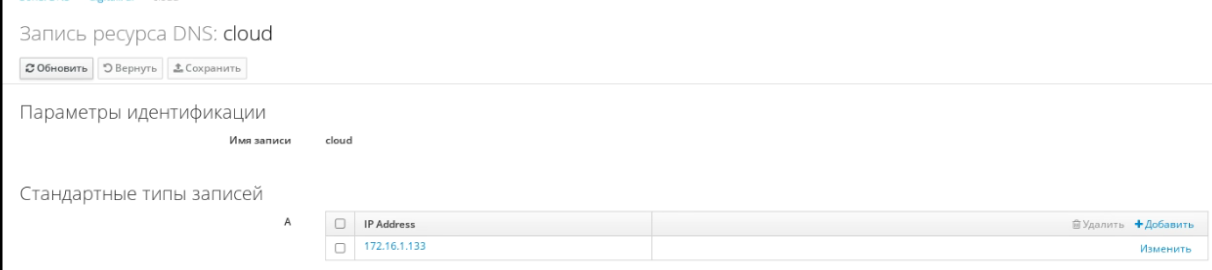


Рисунок 28. Пример изменений в DNS-сервере FreeIPA

## 4 Мониторинг инфраструктуры

Мониторинг инфраструктуры реализован сервером Zabbix на машине C-MONDB.

Доступ до сайта Zabbix доступен по <https://mon.digital.ru>

Производится мониторинг всех инфраструктурных серверов компании через Zabbix Agent.

Для сбора информации используется шаблон Template for Linux, который мониторит статус сети, загрузку оперативной памяти, нагрузку на процессор и т.д. ([Подробнее](https://git.zabbix.com/projects/ZBX/repos/zabbix/browse/templates/os/linux)).

В “Настройка” → “Узлы сети” отображается список доступных узлов, способ подключения и статус. На этой странице вы также можете добавить новые узлы для мониторинга.

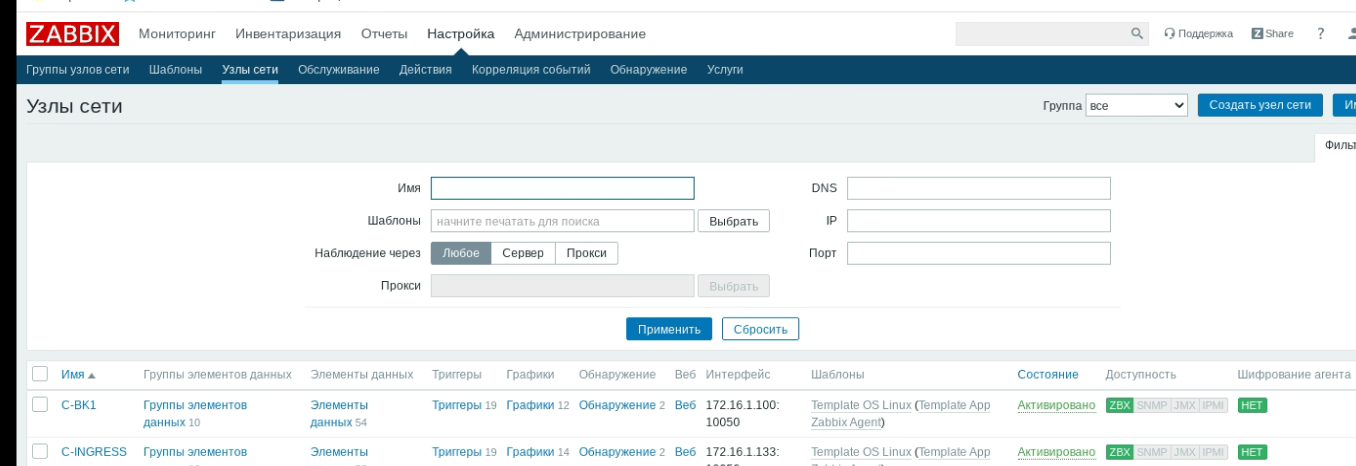


Рисунок 29. Отображение доступных узлов и функционал добавления новых.

В “Отчет” → “Отчет о доступности” можно получить общий отчет о машинах за различный промежуток времени.

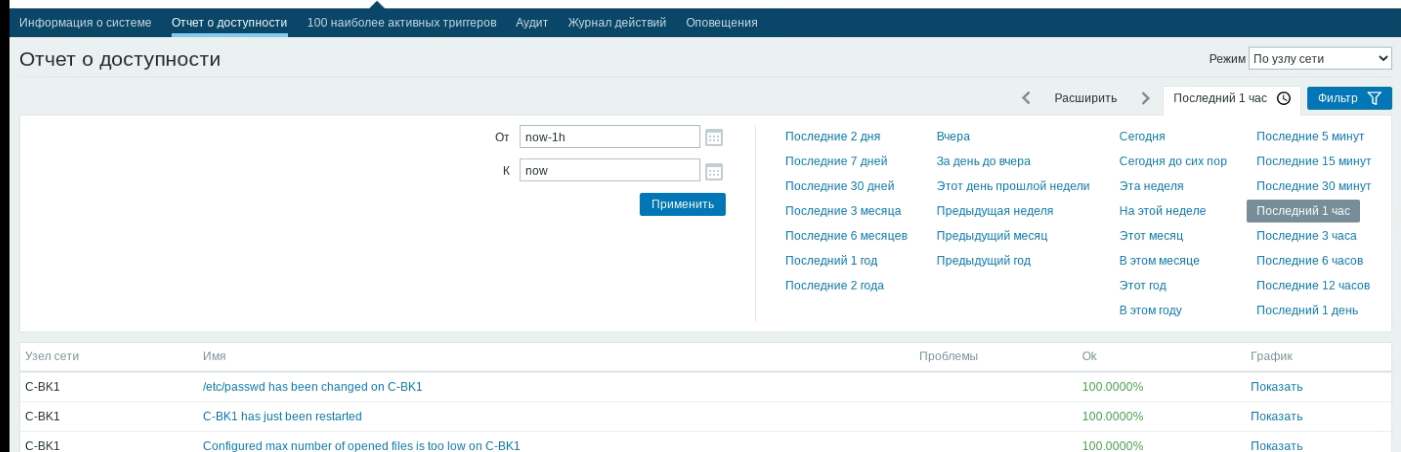


Рисунок 30. Общая сводка отчетов, собранных со всех подконтрольных машин

Уведомления о проблемах и неполадках приходят в созданный Telegram-bot.

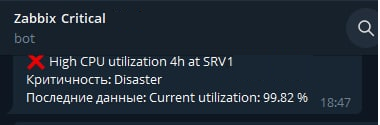


Рисунок 31. Пример отправки уведомлений пользователям в Telegram

## 5 Резервное копирование инфраструктуры

Резервное копирование реализовано системой Bacula.

Сервером Bacula является C-BACKUP. Директория хранения Backup’ов - **/backup**

Интерфейс управления Bacula установлен в виде графической программы на компьютере Director.

Запустить программу вы сможете через меню «Пуск».

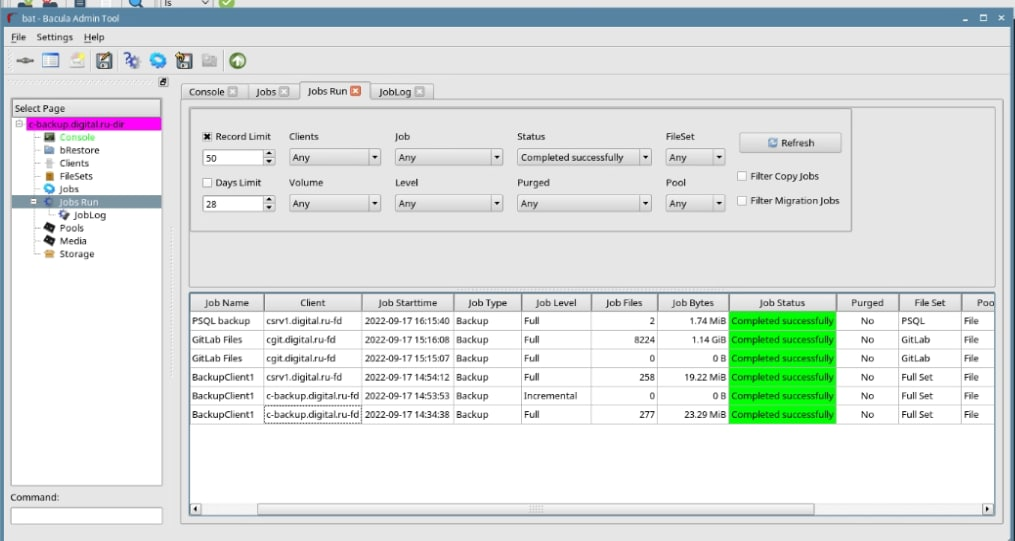


Рисунок 32. Графический интерфейс Bacula

Система требует подключения к базе данных на C-SRV1 – PostrgreSQL.

# Руководство постоянного сотрудника

## Авторизация на рабочем месте

Для постоянных пользователей компании созданы доменные учетные записи. Рабочие станции в офисах введены в домен.

Логин ваших учетных записей сформирован из фамилии и инициалов, например, Иванов Алексей Петрович будет - ivanov-ap.

Выберите ваш домен - digital.ru, а затем введите учетные данные.

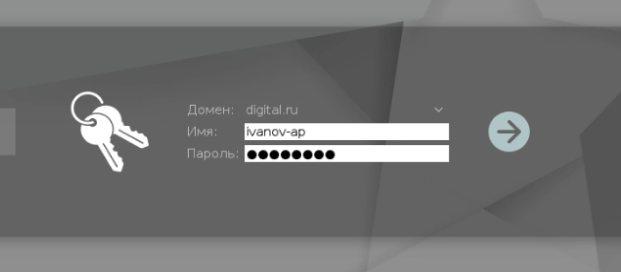


Рисунок 1. Вход на рабочую станцию

При первичном входе в систему используйте временный пароль - P@ssw0rd. Система автоматически предложит вам сменить его на личный.

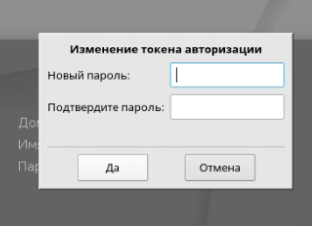


Рисунок 2. Изменение пароля

## Использование хранилища файлов

В компании инструментом общего хранилища и коллективной работы с файлами является сервер NextCloud.

Доступ осуществляется по ссылке - <https://cloud.digital.ru> с браузера Firefox, авторизация через доменную учетную запись без указания домена.

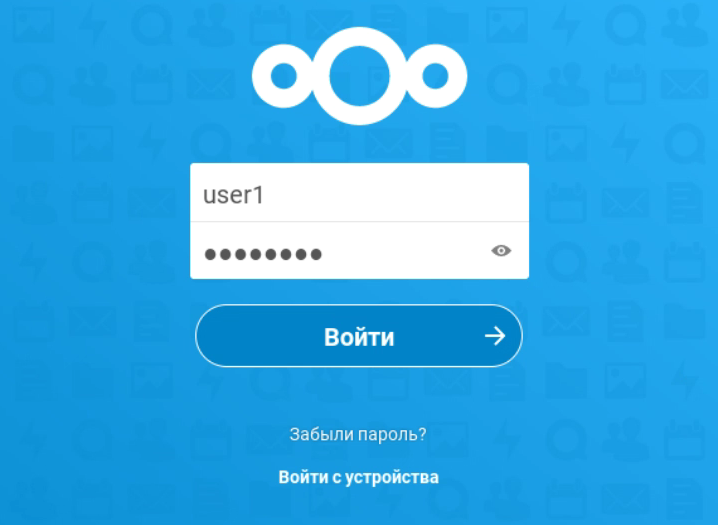


Рисунок 3. Вход в NextCloud

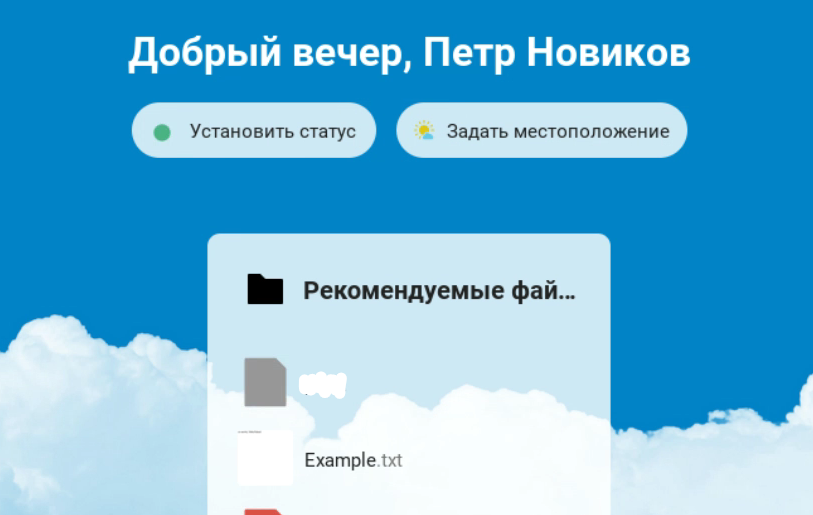


Рисунок 4. Приветствие новых пользователей.

NextCloud имеет широкий функционал, включая корпоративный мессенджер, возможность совместно редактировать файлы, встроенный видеоплеер.

Стоит отметить, что NextCloud также использует резервный доменный контроллер для аутентификации

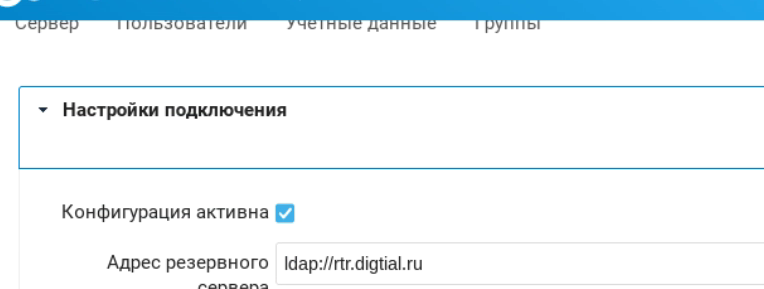


Рисунок 5. Конфигурация резервного доменного контроллера

Файлы, сохраненные в облаке являются пользовательскими и изначально доступ к ним уникален. Но к любому файлу можно открыть доступ для совместного использования, например, откроем файл Example.txt.

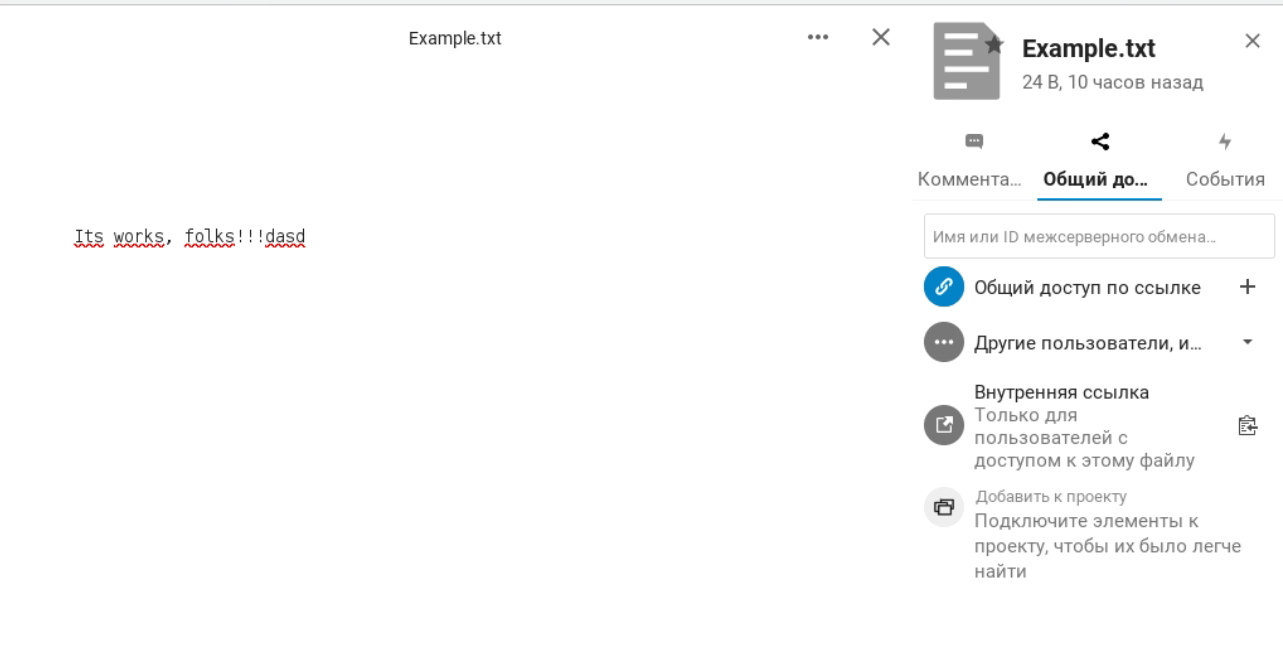
Открываем “Боковую панель” → “Общий доступ” → “Общий доступ по ссылке”

Рисунок 6. Включение общего доступа.

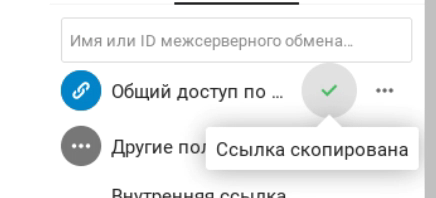


Рисунок 7. Скопировали ссылку на общее редактирование

Кликните по настройкам общего доступа по ссылке и выберите “Разрешить редактирование”

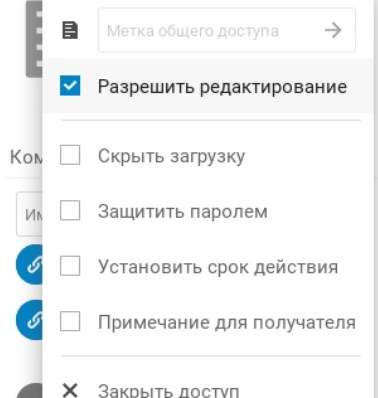


Рисунок 23. Включение редактирования для пользователей по ссылке.

Теперь по ссылке пользователи могут редактировать документ.

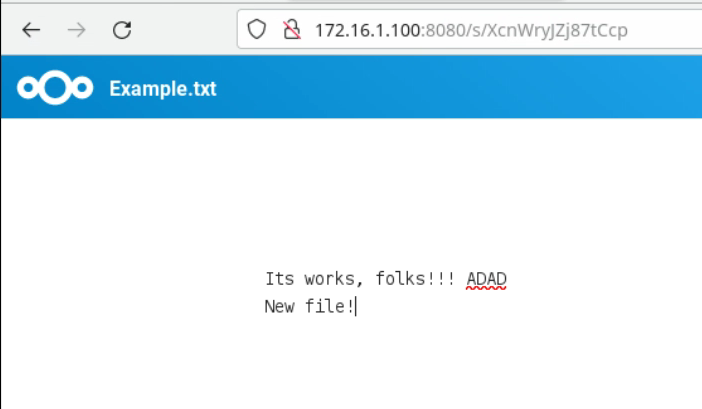


Рисунок 24. Совместное редактирование одного документа.

Для полного ознакомления с NextCloud следует ознакомиться с User-Guide на английском языке, который автоматически создается при первом входе в NextCloud под учетной записью из домена digital.ru.

## Использование CI\CD-инфраструктуры

Инфраструктура представлена системой GitLab.

Вход по URL - <https://c-git.digital.ru>

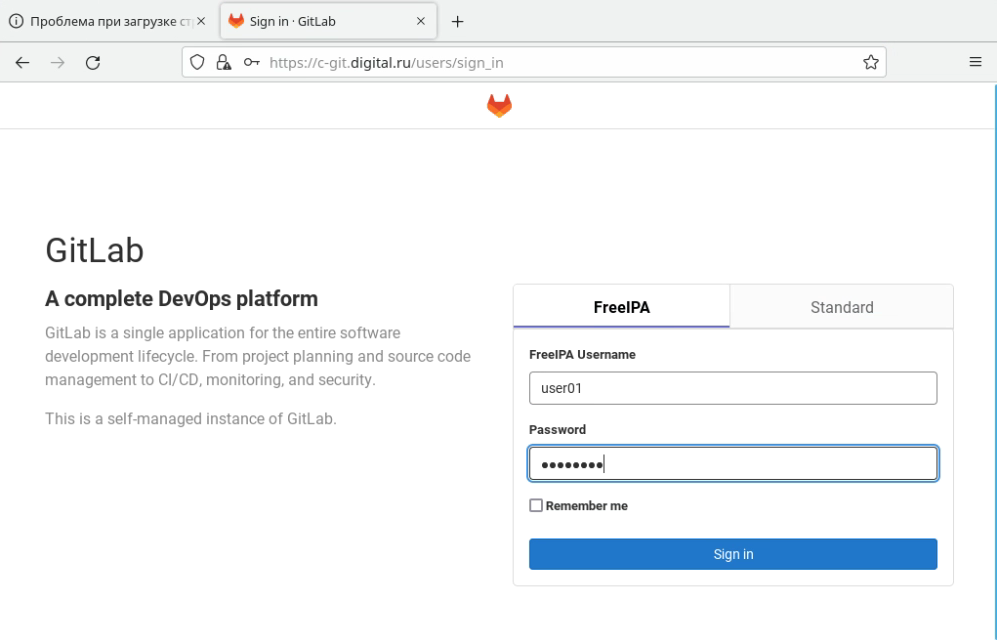


Рисунок 25. Окно входа в GitLab

После подключения к GitLab, необходимо войти под пользователем root c паролем P@ssw0rd.

Далее, переходим в меню “Admin” → “Users” → “выбираем нужного пользователя”. В нашем примере, это будет user01

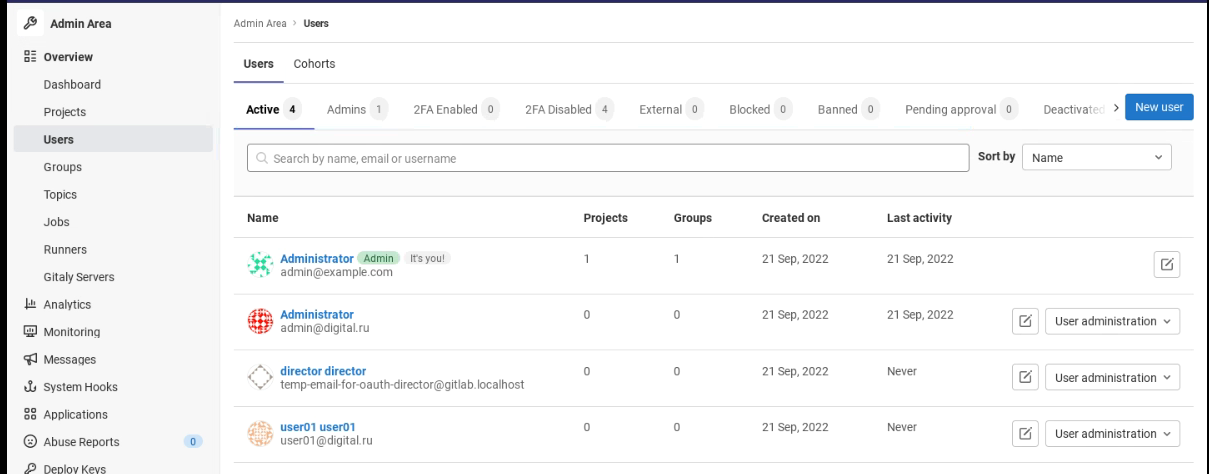


Рисунок 26. Выбор пользователя для редактирования

Переходим к редактированию пользователя

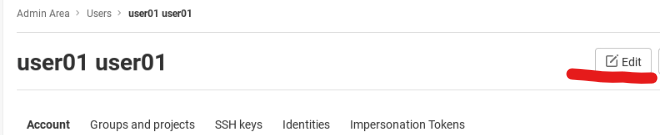


Рисунок 27. Редактирование пользователя

Обратите внимание, что GitLab создает временную почту для каждого пользователя LDAP. В дальнейшем, ожидается что пользователь подтвердит свою почту.

В демонстрационном стенде отсутствует почтовая инфраструктура, поэтому почту необходимо подтвердить вручную.

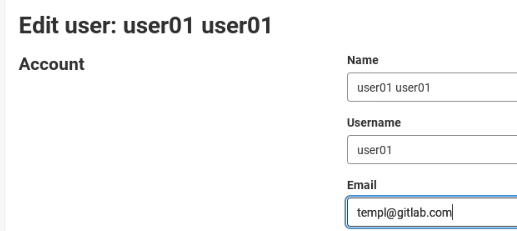


Рисунок 28. Изначальная конфигурация пользователя LDAP в GitLab



Рисунок 29. Конечная конфигурация пользователя LDAP в GitLab.

Затем удалите информацию о втором почтовом адресе.

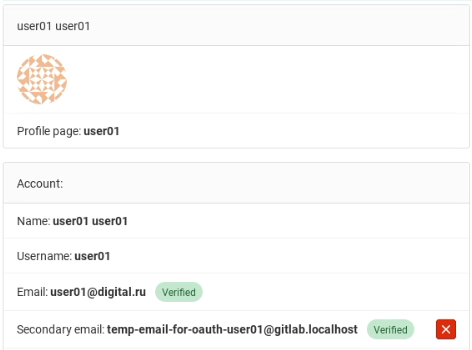


Рисунок 30. Удаление информации о втором почтовом ящике

## Подключение к Git через vsCode.

Установите vsCode с официального сайта.

Далее откройте программу и перейдите в меню системы Git (логотип дорожного разъезда) и выполните установку Git-инструментов.

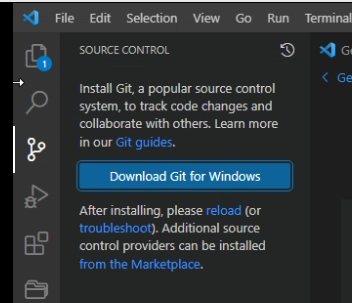


Рисунок 31. Установка Git-инструментария для vsCode

Далее, перейдите на сайт через браузер Google Chrome на сайт GitLab - <https://c-git.digital.ru>, авторизуйтесь и создайте тестовый репозиторий

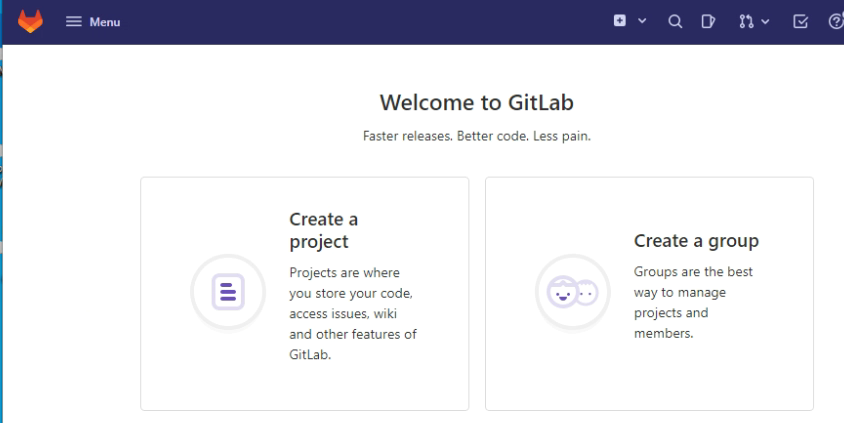


Рисунок 32. Создание репозитория в GitLab

После установки Git-инструментария подключитесь к вашему созданному ранее репозиторию.

## 

Рисунок 34. Меню ввода URL-адреса репозитория

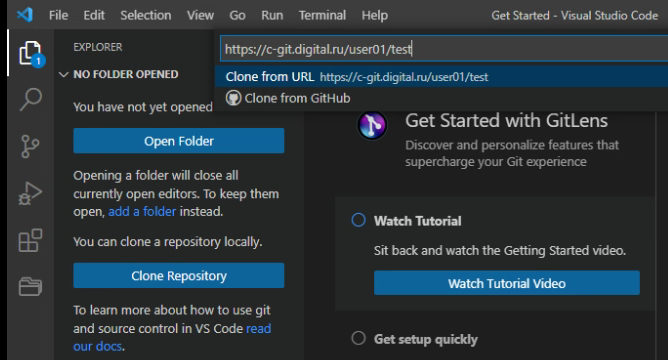


Рисунок 35. Пример введенного репозитория.

Система потребует авторизации. Введите свои учетные данные.

# 

Рисунок 36. Подключение к репозиторию через vsCode средствами Git.

# 

Рисунок 37. Вывод подключенного репозитория.

# Руководство удаленного привлекаемого сотрудника

## Подключение к VPN

Если вы работаете с компьютером под управлением Windows 10:

1. Установите себе на компьютер программу OpenConnect - <https://openconnect.github.io/openconnect-gui/>
2. После установки выполните подключение к VPN-серверу организации.

Создайте новый профиль.

Для этого откройте пиктограмму настроек OpenConnect → New profile

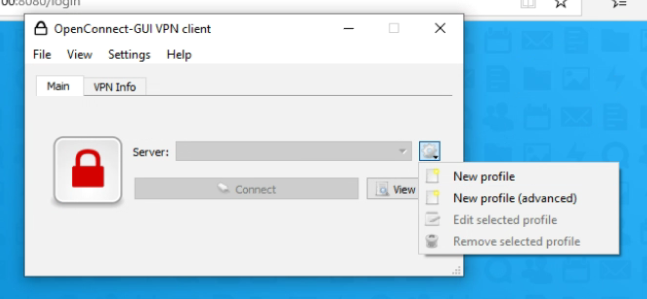


Рисунок 1. Переход в меню настройки OpenConnect

Заполните информацию, как на скриншоте

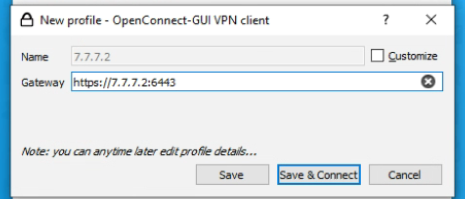


Рисунок 2. Конфигурация OpenConnect

Далее введите ваш логин и пароль от доменной учетной записи.

Компьютер автоматически получит сведения о внутренних DNS-серверах организации.

Логин вводится в формате [username@digital.ru](mailto:username@digital.ru)

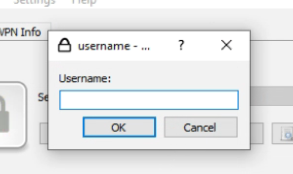


Рисунок 3. Ввод логина и пароля.

Далее порядок работы не отличается от сотрудника в офисе.

Если вы работаете с компьютером под управлением Ubuntu:

1. Выполните установку OpenConnect-Gnome из официального репозитория Ubuntu вашего релиза:

sudo apt-get install network-manager-openconnect network-manager-openconnect-gnome

1. Далее, перейдите в сетевые настройки вашей ОС:

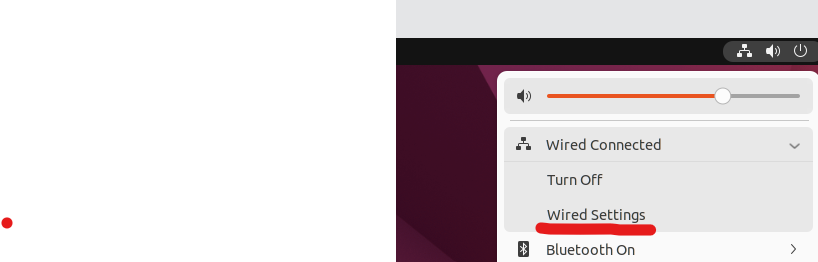


Рисунок 4. Переход в меню настроек сети на ОС

1. В окне выберите параметр VPN и кликните +



Рисунок 5. Переход к инициализации VPN-соединения

1. Выберите вариант подключения через OpenConnect

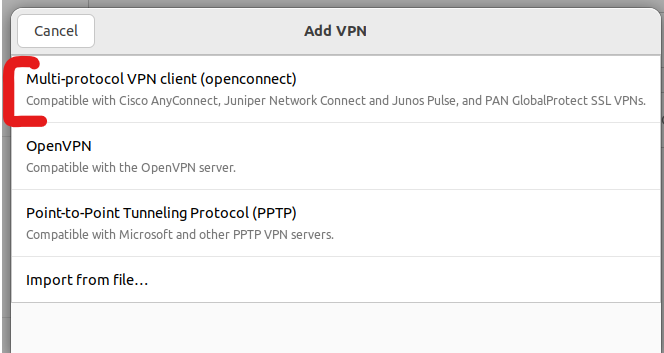


Рисунок 6. Выбор типа подключения VPN

1. Из всех параметров настройте только Gateway

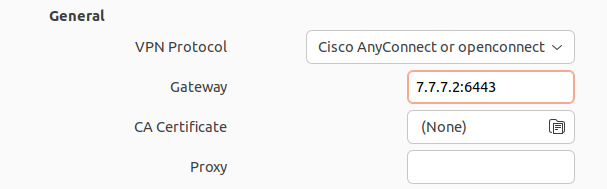


Рисунок 7. Настройка OpenConnect соедениния

1. Включите OpenConnect

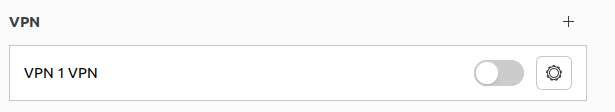


Рисунок 8. Включение OpenConnect

1. Введите сведения о вашей учетной записи в формате - [username@digital.ru](mailto:username@digital.ru)

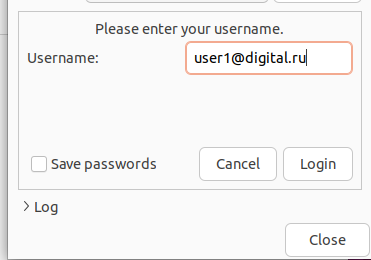


Рисунок 9. Авторизация в OpenConnect

Далее порядок работы не отличается от пользователя в локальной инфраструктуре.