Правительство Санкт-Петербурга

Комитет по науке и высшей школе

Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение

«Политехнический колледж городского хозяйства»

**КУРСОВОЙ ПРОЕКТ**

**Администрирование КС областной больницы**

**ЛИСТ УТВЕРЖДЕНИЯ**

ПКГХ 09.02.06 СА-22-2. 062-22-ЛУ

|  |  |
| --- | --- |
|  | **Студент**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Краснов С.Е.)  **Руководитель**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Травкина Ю.И) |
|  |  |

Санкт-Петербург

2025

Содержание

[Введение 3](#_Toc198580540)

[1.Теоритическая часть 5](#_Toc198580541)

[Серверная инфраструктура и системное ПО 5](#_Toc198580542)

[Отказоустойчивость и резервное копирование 6](#_Toc198580543)

[Администрирование пользователей и данных 7](#_Toc198580544)

[Хранение данных, безопасность и мониторинг 9](#_Toc198580545)

[2.Аналитическая часть 11](#_Toc198580546)

[Сервера Windows, настройка ADDS 11](#_Toc198580547)

[Сервера Linux 16](#_Toc198580548)

[Заключение 17](#_Toc198580549)

[Список использованных источников 18](#_Toc198580550)

[Приложения 19](#_Toc198580551)

# Введение

Эффективное функционирование компьютерных сетей в медицинских учреждениях является важнейшим условием обеспечения качества медицинских услуг, оперативности обработки информации и безопасности персональных данных пациентов. Однако, несмотря на наличие разработанных стандартов построения сетей, на практике в больницах России часто наблюдаются проблемы, связанные с недостаточной масштабируемостью, устаревшими техническими решениями, низкой отказоустойчивостью и недостаточной защитой информации. Это свидетельствует о противоречии между потребностью в современных высоконадёжных сетевых решениях и фактическим состоянием сетевой инфраструктуры медицинских организаций. Данная проблема требует глубокого изучения и поиска эффективных путей её решения, что обуславливает актуальность выбранной темы.

Целью данной курсовой проекта является эффективное администрирование компьютерной сети больницы с учетом особенностей её функционирования и современных требований к безопасности и надежности.

Для достижения поставленной цели были сформулированы следующие задачи:

* Развернуть и настроить виртуальные и физические сервера
* Обеспечить отказоустойчивость и резервное копирование.
* Управление пользователями и правами доступа.
* Обеспечить защиту данных.
* Настроить мониторинг сети и серверов

Объектом исследования является процесс построения и администрирования компьютерной сети в медицинском учреждении.

Предметом исследования являются методы, средства и организационные подходы к обеспечению надёжной и безопасной работы компьютерной сети больницы.

Структура курсового проекта обусловлена необходимостью перехода от теоретического анализа к практическому проектированию: в первой части представлены теоретические основы построения сетей; во второй — проведен аналитический обзор состояния сети в медицинском учреждении и предложены практические решения на примере существующего корпуса больницы. Работа опирается как на общедоступные источники и стандарты, так и на личный практический опыт автора в процессе работы системным администратором в медицинском учреждении.

Практическая значимость исследования заключается в возможности использования предложенного проекта при построении или модернизации компьютерных сетей в медицинских учреждениях, что позволит повысить их надёжность, безопасность и эффективность функционирования.

# 1.Теоритическая часть

## Серверная инфраструктура и системное ПО

В данном проекте предлагается архитектура на основе двух доменных контроллеров Windows Server 2019 и набора Linux-серверов для обеспечения веб-доступа, мониторинга и резервного копирования. Все серверы будут развернуты как виртуальные машины для обеспечения гибкости управления ресурсами и миграции в случае сбоев.

Серверы Windows будут использоваться для Active Directory чтобы централизованно управлять пользователями и политиками. В AD будет интегрироваться DHCP и DNS-сервер. Для организации общего доступа к файлам использовать Samba сервер с FSRM Под будущие медицинские системы (1С:Медицина, МИС Ариадна) есть возможность использовать СУБД Microsoft SQL server. Для создания AD пользователей в большом количестве использовать PowerShell скрипты.

На Linux серверах будет развернут веб сервер с CMS для сайта больницы, система мониторинга и система под хранение и управление резервными копиями. Для развертывания и управления конфигурациями можно использовать Ansible.

Отталкиваясь от выше поставленных задач можно выделить список необходимого основного ПО для серверов:

Windows-серверы:

* Active Directory - Централизованная аутентификация.
* Microsoft SQL Server- Базы данных медицинских систем.
* PowerShell - Автоматизация задач.
* FSRM – Для общего доступа

Linux-серверы:

* Nginx - Веб сервер
* MySQL – База данных для веб-сервера
* WordPress – Управление содержимым сайта
* Ansible - Управление конфигурациями.
* Zabbix – Мониторинг

Таблица – Серверы их роли

|  |  |  |
| --- | --- | --- |
| Имя | ОС | Стек |
| DC1 | WServer 2022 | Active Directory, DNS, DHCP, Samba, FSRM |
| DC2 | WServer 2022 |
| WEB1 & WEB2 | Ubuntu Server 22.04 | Nginx+ WordPress + MySql |
| BACKUP | Ubuntu Server 22.04 | Хранение резервных копий серверов |
| MONITORING | Ubuntu Server 22.04 | Zabbix |

## Отказоустойчивость и резервное копирование

Отказоустойчивость и резервное копирование являются важными компонентами обеспечения непрерывности работы больничной инфраструктуры. Для обеспечения отказоустойчивости серверов следует применять следующие подходы:

Для защиты данных на уровне дисковых подсистем используются RAID-массивы. Рекомендуется применять зеркалирование (RAID 1) для системных дисков, чтобы минимизировать риск потери данных при сбое одного из накопителей. Для файловых хранилищ оптимальным выбором будет RAID 10, сочетающий чередование и зеркалирование, что повышает производительность и надежность.

Для повышения надежности баз данных используется репликация между серверами, например, с использованием MySQL в режиме мастер-мастер. Это позволяет сохранить актуальные данные на резервном сервере при выходе основного из строя. Для веб-сервера настраивается кластер с балансировкой нагрузки с помощью Keepalived и Nginx. Это обеспечит доступность веб-сайта даже при отказе одного из серверов.

Резервное копирование настраивается с использованием таких инструментов, как rSync и Crontab. Регулярные копии должны храниться на выделенных серверах хранения, защищённых шифрованием и изоляцией от основной сети.

Такой подход позволит больничной инфраструктуре поддерживать стабильность работы даже в условиях аварийных ситуаций и минимизировать потери данных.

## Администрирование пользователей и данных

Для администрирования пользователей и управления доступом в больничной сети используется доменная структура Active Directory (AD), которая обеспечивает централизованное управление учётными записями, группами и правами доступа. Это позволяет упрощать администрирование, обеспечивать высокий уровень безопасности и гибкость в управлении доступом к ресурсам. Пример структуры “med.local”:

OU=Администрация

Группа "IT"

Группа "Бухгалтерия"

Группа "Отдел Кадров"

OU=Медицинские сотрудники

Группа "Врачи"

Группа "Медсестры"

Группа "Фармацевты"

Группа "Лаборанты"

Группа "Интерны и студенты"

OU=Медицинские отделения

Группа "Кардиология"

Группа "Хирургия"

Группа "Педиатрия"

Группа "Терапевтическое отделение"

Группа "Травматологический пункт"

OU=Сотрудники

Группа "Тех поддержка"

Группа "Регистрация"

Группа "Обслуживающий персонал"

OU=Компьютеры

Группа "Серверы"

Группа "Рабочие станции"

OU=Гости

Для управления доступом используются групповые политики (GPO), которые позволяют централизованно настраивать параметры безопасности, доступ к ресурсам, поведение рабочих станций и серверов.

Таблица – Примеры групповых политик

|  |  |  |
| --- | --- | --- |
| Группа или OU | Политика | Описание |
| IT | Длинный пароль | Минимальная длина пароля 16 символов, сложные пароли, срок действия — 90 дней. |
| Бухгалтерия и отдел кадров | Доступ к файлам | Ограниченный доступ к финансовым данным и данных сотрудников, шифрование при передаче. |
| Медицинские сотрудники | Политика рабочего стола | Ограничение доступа к настройкам системы, обязательное шифрование данных. |
| Интерны и студенты | Политика обучения | Ограниченный доступ к медицинским данным, журналирование всех действий. |
| Серверы | Безопасность серверов | Принудительное шифрование данных, контроль доступа по IP-адресам. |
| Рабочие станции | Безопасность рабочих станций | Ограничение USB-устройств, экранирование экрана через 5 минут бездействия. |
| Регистрация | Рабочее время | Доступ к сети только в рабочие часы, ограничение установки ПО. |

## Хранение данных, безопасность и мониторинг

Для обеспечения безопасности данных и надежной работы сети и серверов необходимо применить комплексный подход к защите данных и сетевой безопасности.

Серверы должны быть установлены в закрытых помещениях с ограниченным физическим доступом. Доступ к серверным стойкам должен быть защищен с помощью замков, систем видеонаблюдения и контроля доступа, чтобы исключить несанкционированное физическое вмешательство.

Так как основой управления доступом к сети является Active Directory который обеспечивает централизованное управление учетными записями пользователей. Для повышения безопасности можно использовать многофакторную для учетных записей администраторов, а также строгие политики паролей.

Для серверов с ролями FSRM необходима настройка квот и файловых экранов для защиты от атак, связанных с загрузкой вредоносных файлов, а также настройка уведомления при превышении квот и попытках сохранения запрещенных файлов. Можно использовать Kerberos для аутентификации пользователей.

Для защиты данных на серверах Windows использовать шифрование файлов и папок с помощью Encrypting File System (EFS) и шифрование дисков с помощью BitLocker. Для серверов Linux рекомендуется использовать шифрование на уровне файловой системы с использованием LUKS.

Для защиты серверов от внешних и внутренних атак использовать встроенные средства защиты, такие как Windows Firewall для серверов Windows и iptables/nftables для серверов Linux. Настройка Fail2ban для блокировки попыток несанкционированного доступа через SSH, а также установка IDS/IPS для обнаружения вторжений.

Для постоянного контроля за состоянием серверов и сетевой активностью будет использоваться zabbix для мониторинга производительности. Для своевременного обнаружения потенциальных угроз использовать аудит действий пользователей и изменений файлов в Active Directory.

Для защиты данных, передаваемых между веб-сайтами больницы и пользователями, использовать SSL/TLS-сертификаты. Будет использоваться сертификат от доверенного центра сертификации Let's Encrypt, и настроено автоматическое обновление для минимизации риска компрометации.

# 2.Аналитическая часть

Все сервера – виртуальные и развернуты на одном физическом сервере под управлением ProxMox, адреса статичны и прописаны в маршрутизаторе.

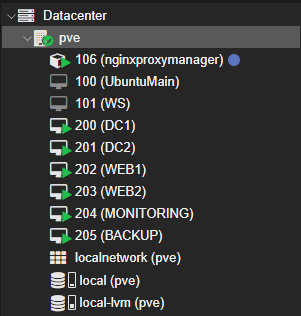


Рисунок – Сервера в ProxMox и Адреса

## Сервера Windows, настройка ADDS

Сначала настраивается один сервер и после полной настройки подключается второй и настраивается репликация

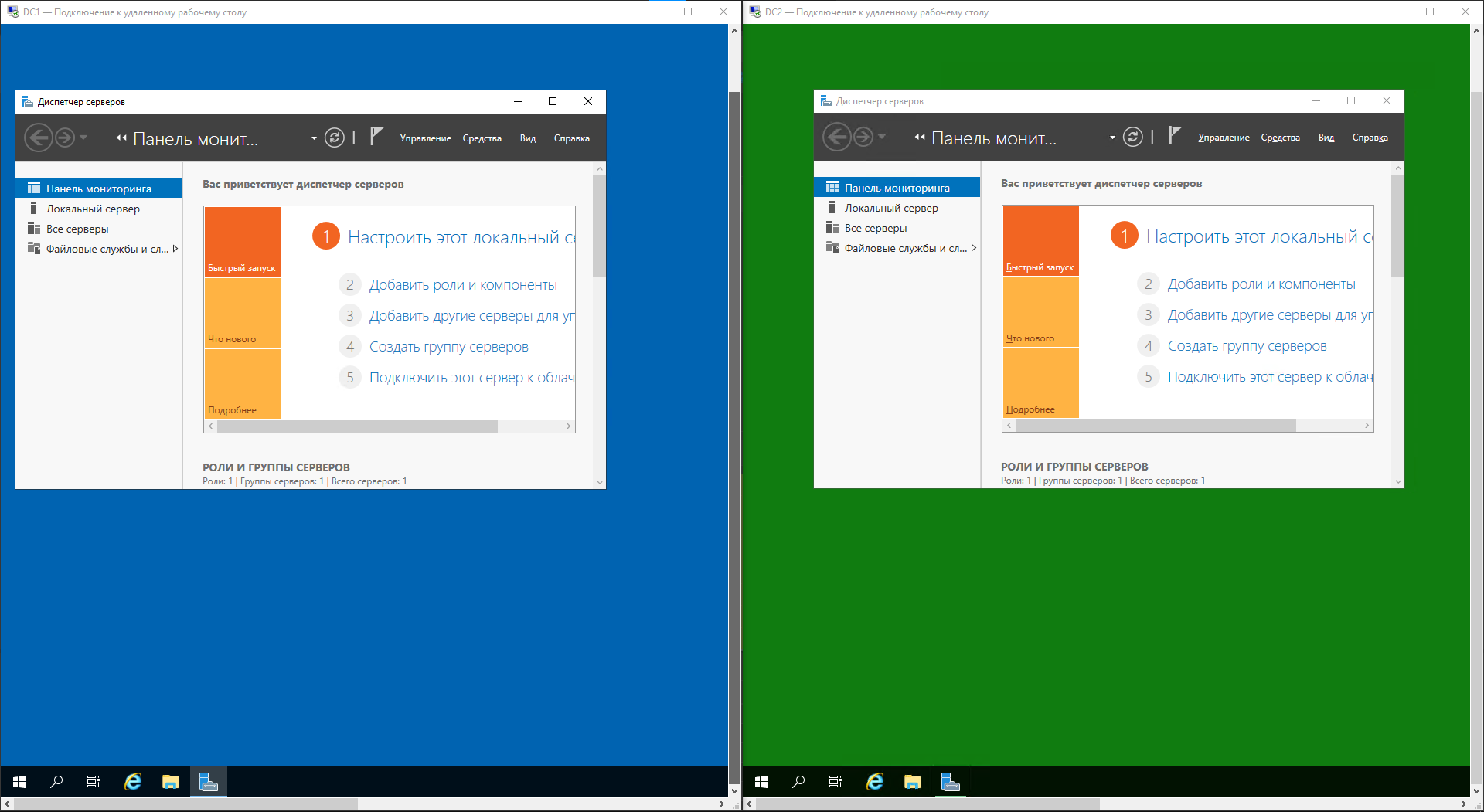


Рисунок – RDP Сеансы серверов

На сервер добавляются необходимые компоненты: ADDS, DNS и DHCP сервера и FSRM

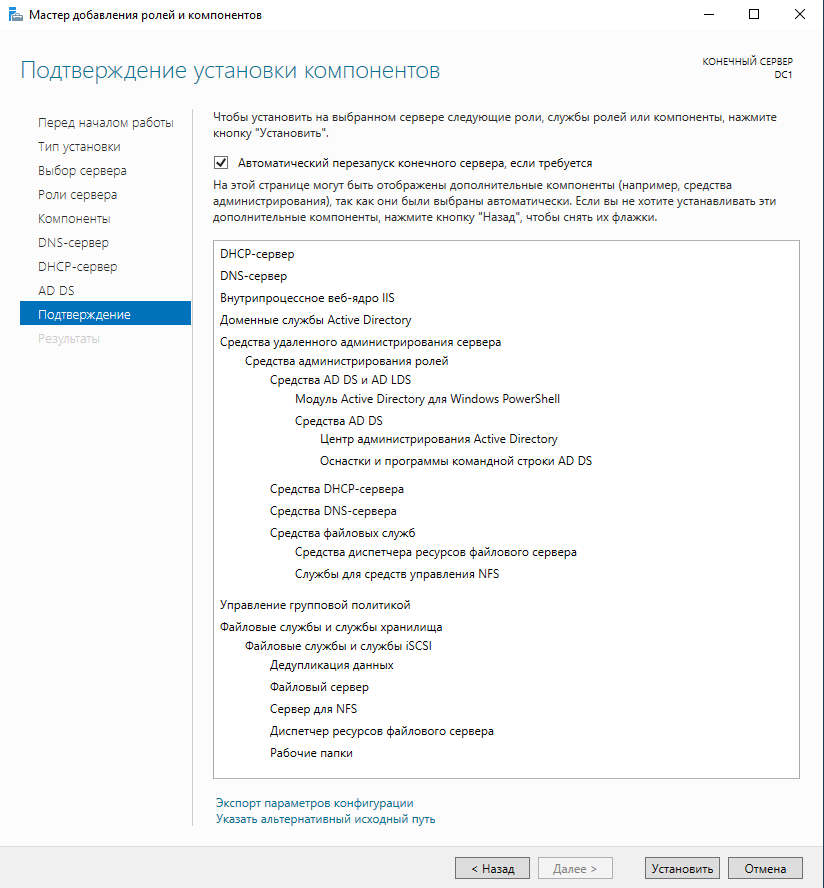


Рисунок – Добавление компонентов на сервер

После добавления компонентов, создается домен

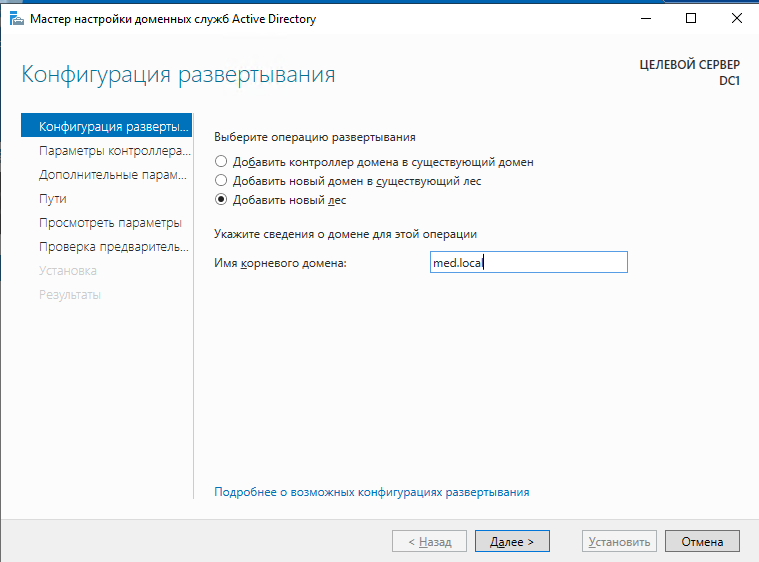


Рисунок – Создание нового леса

После создания можно авторизоваться

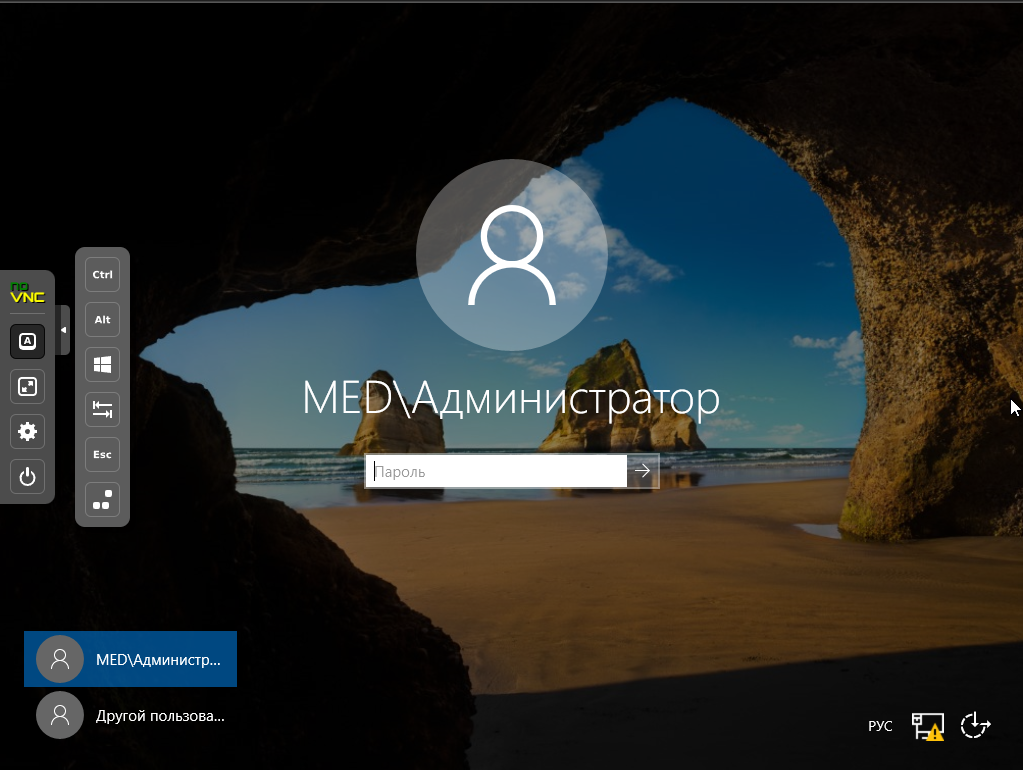


Рисунок – Авторизация в домен

После создания домена, настраиваются зоны в DNS.

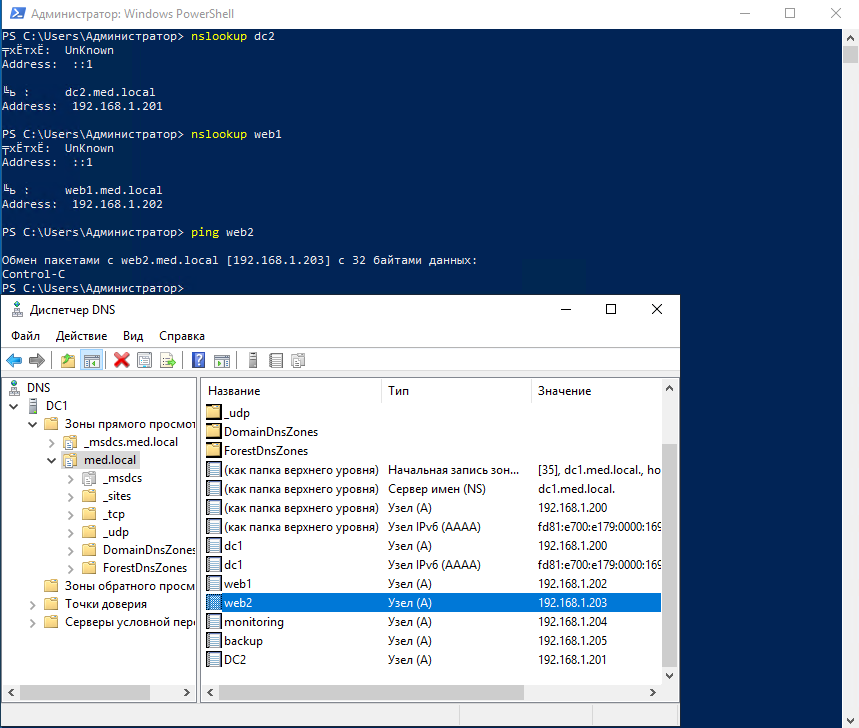


Рисунок – Настройка DNS

Настроенный пул адресов в DHCP на рисунке 7.

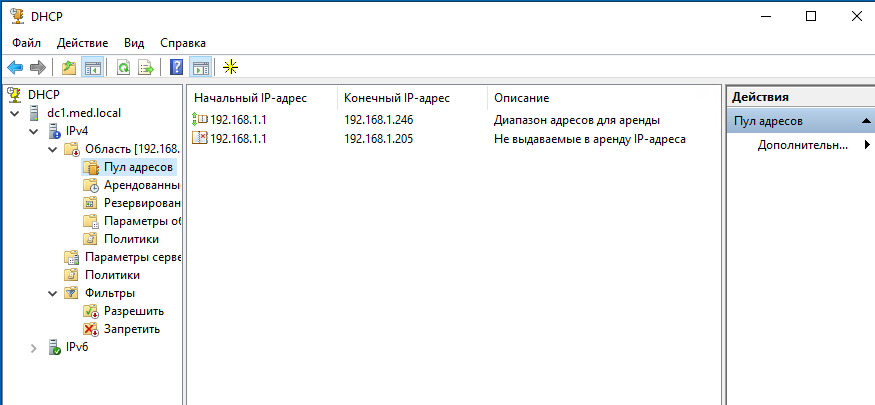


Рисунок – Настройка DHCP

Создание пользователей и групп происходит через сценарии PowerShell( см. Приложения)

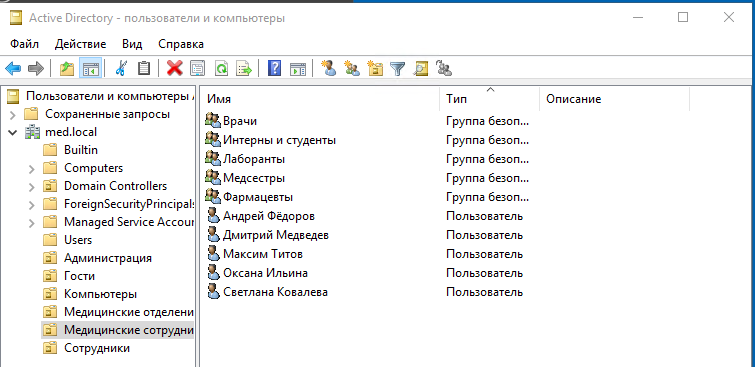


Рисунок – Пользователи, группы и OU

Через FSRM развёртывается общий доступ

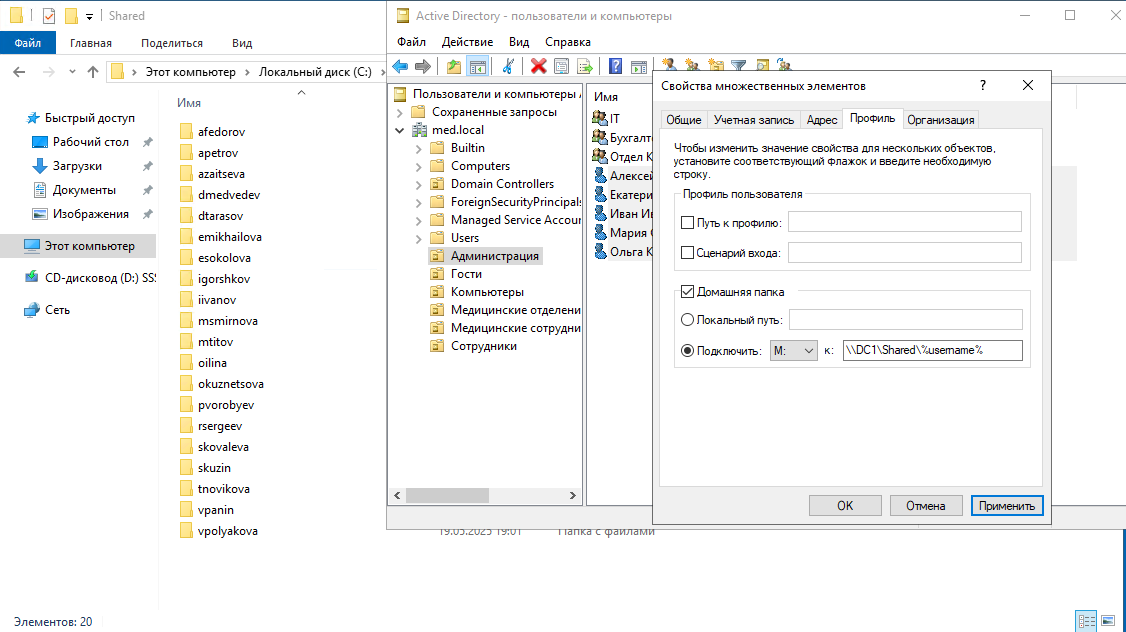


Рисунок – Общий ресурс

Задаются групповые политики описанные выше.

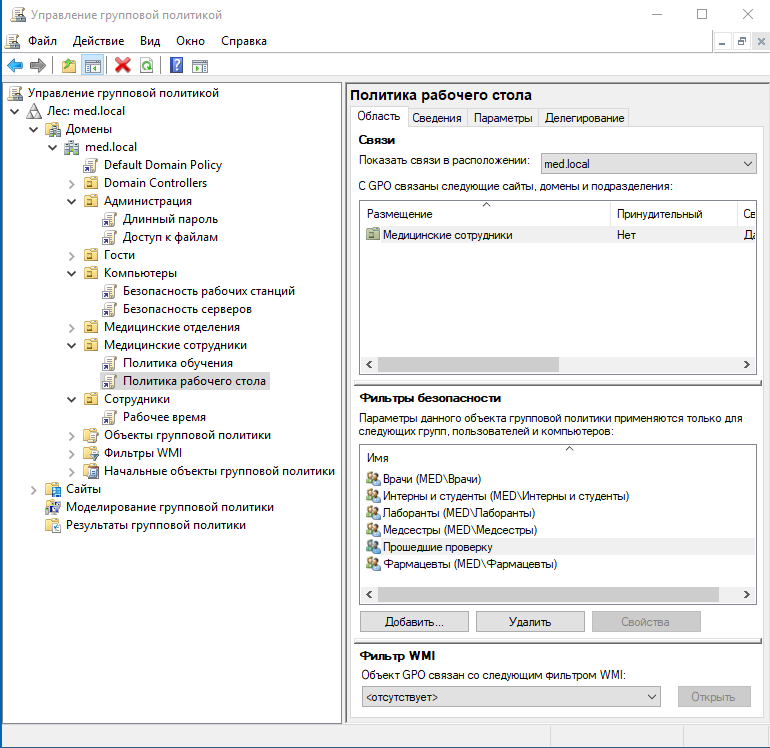


Рисунок – Настройка GPO

Когда первый сервер настроен, второй вводится в домен и настраивается репликация

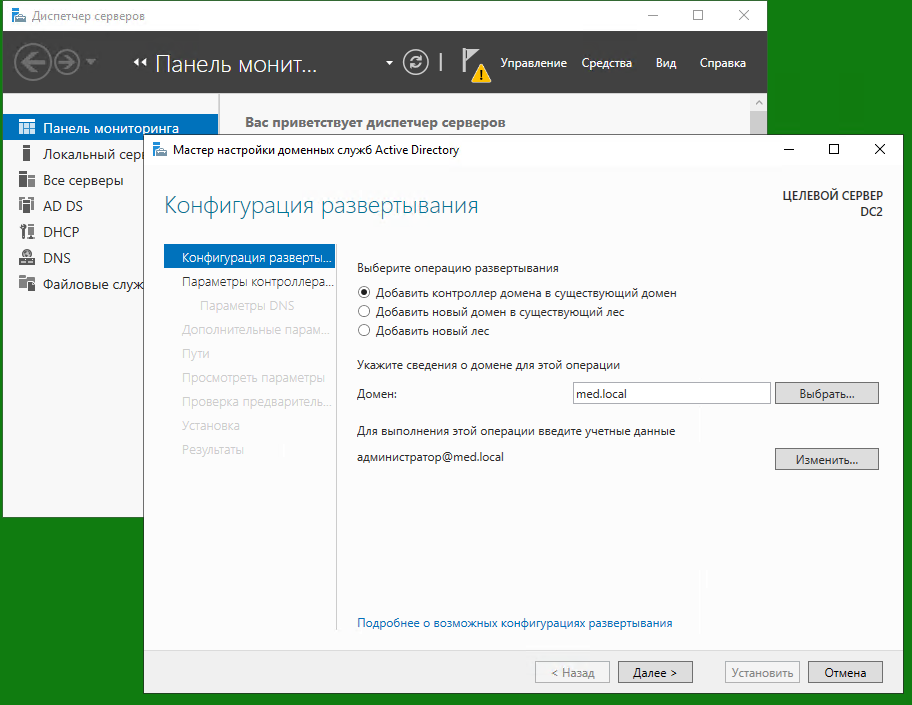


Рисунок – Добавление второго DC

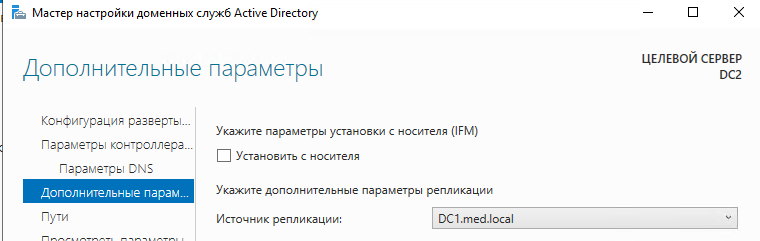


Рисунок – Выбор источника репликации

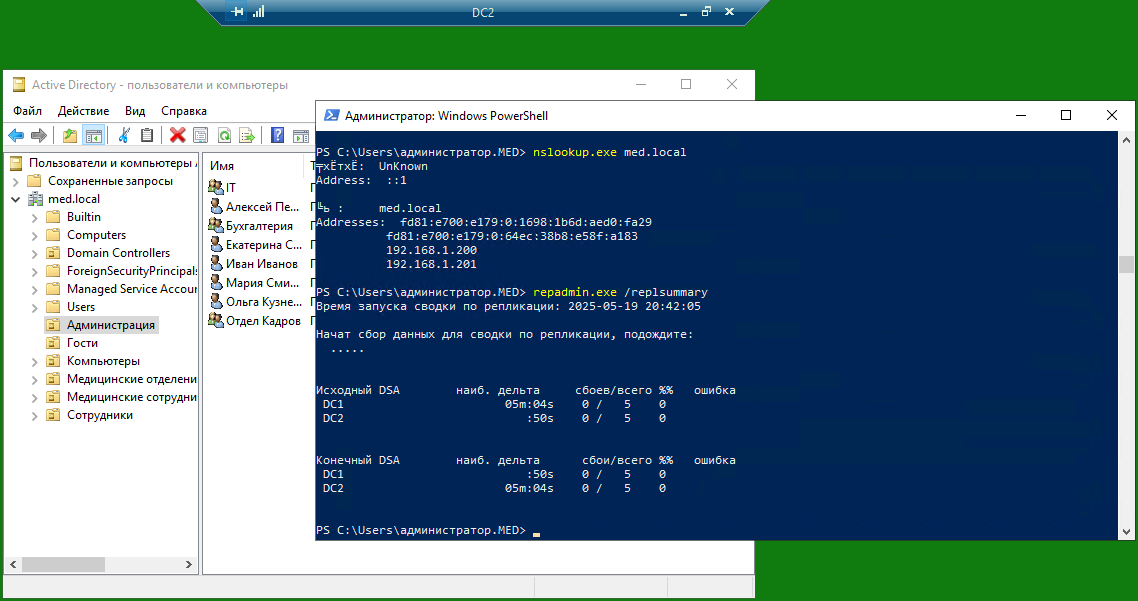


Рисунок – Проверка репликации

## Сервера Linux

При развертывании машин Linux нужно использовать шифрование LUKS

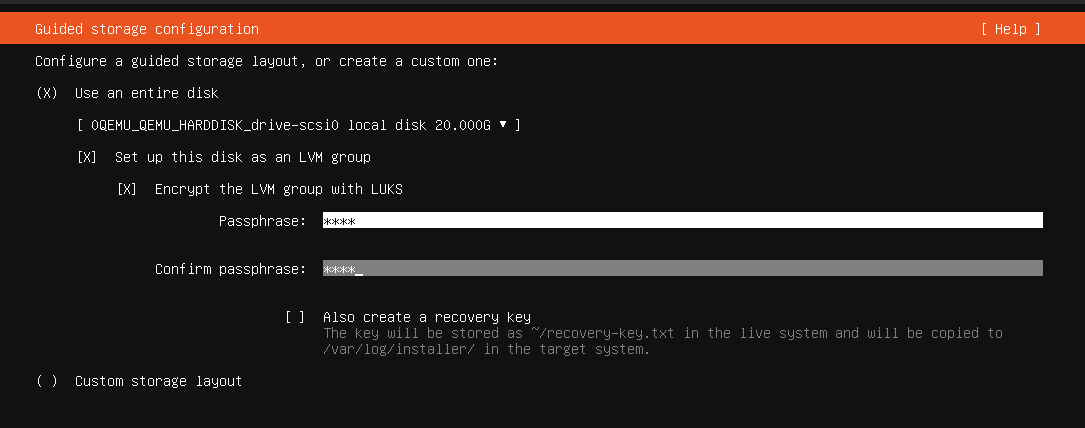


Рисунок – Включение LUKS

Ниже представлено развертывание Стека WordPress+Nginx+MySql на машинах web1 и web2 с помощью Ansible

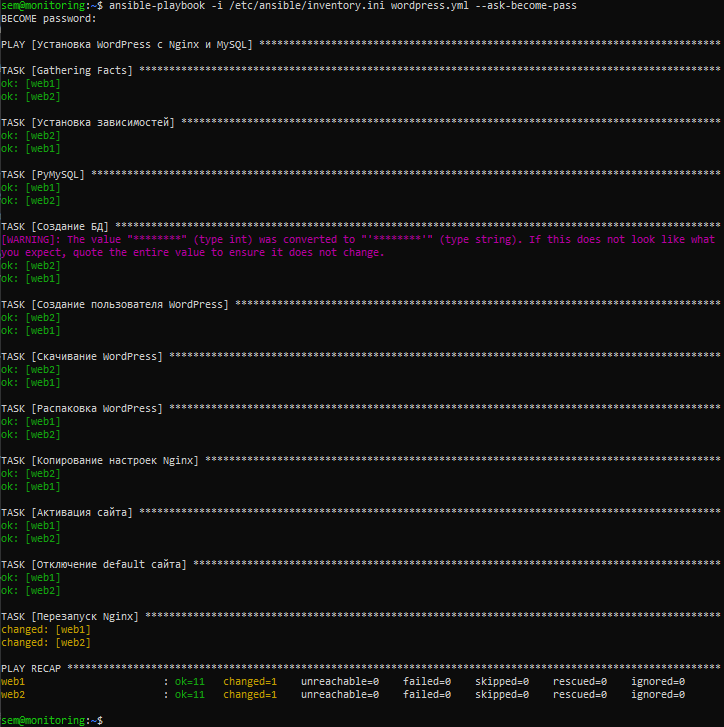


Рисунок – Работа Ansible

После развертывания части веб-сервера, необходимо настроить Master-Master репликацию на базах данных MySQL.

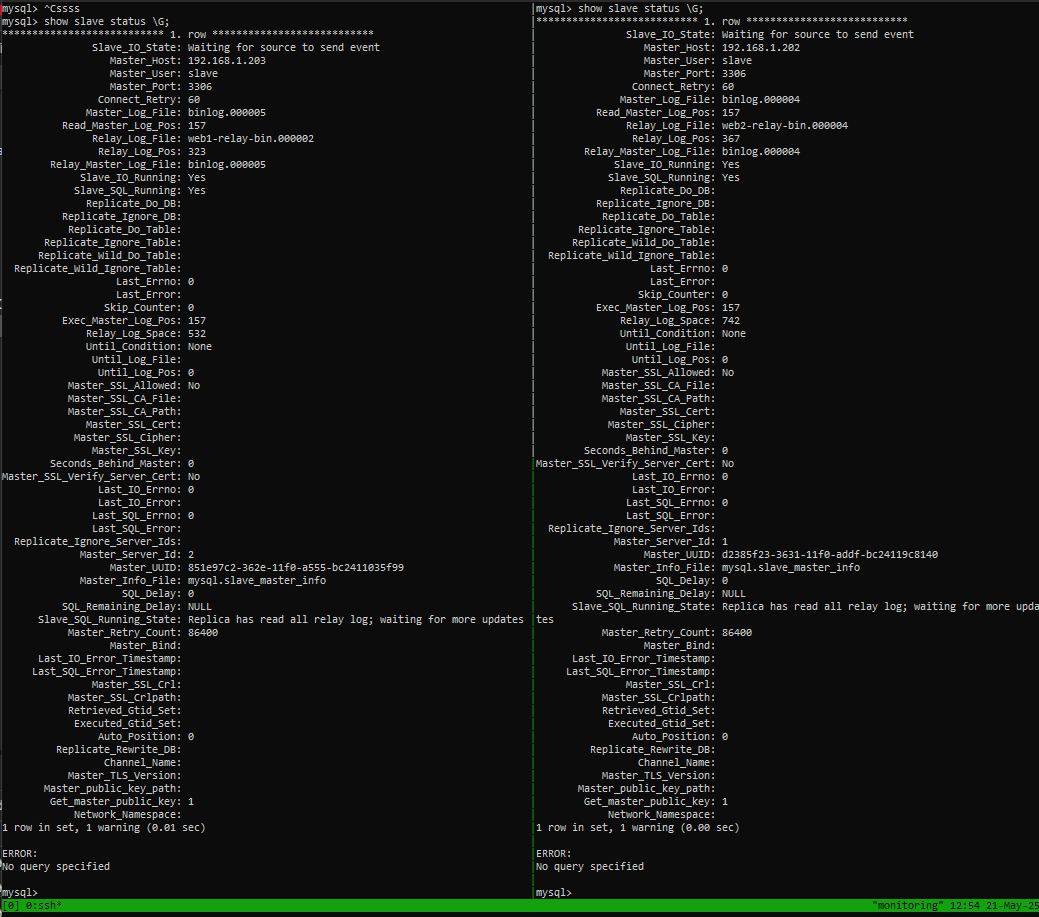


Рисунок – Статус репликации

Проверка отказоустойчивости KeepAliveD представлена на рисунке 17.

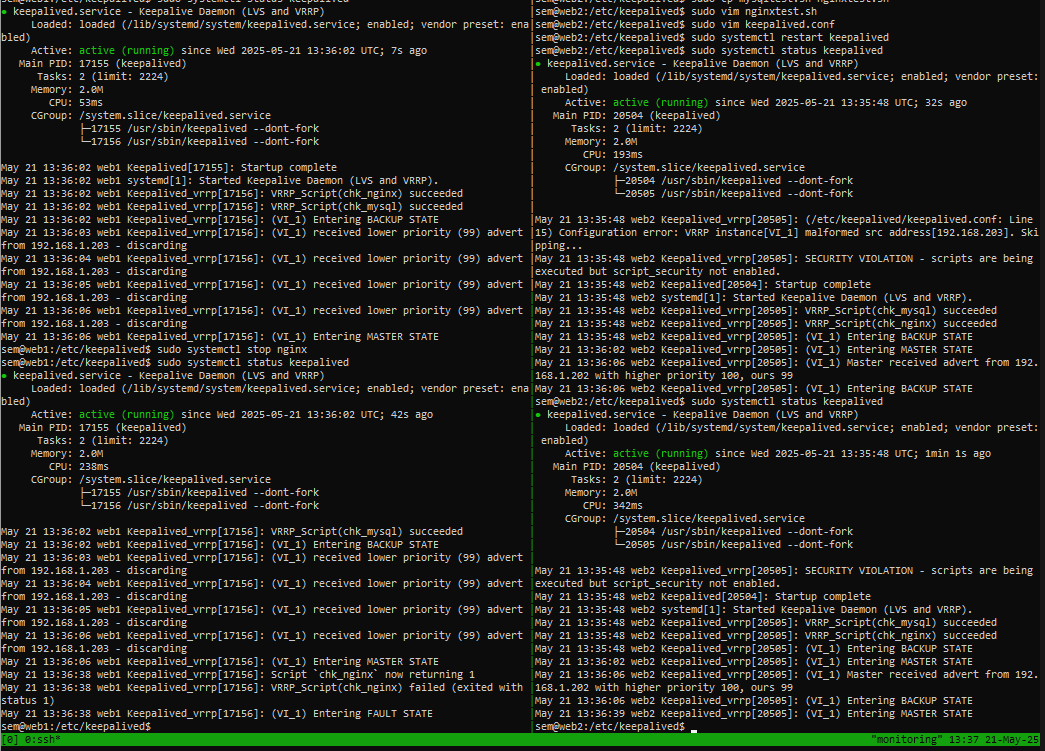


Рисунок – Проверка KeepAliveD

Теперь настраивается WordPress.

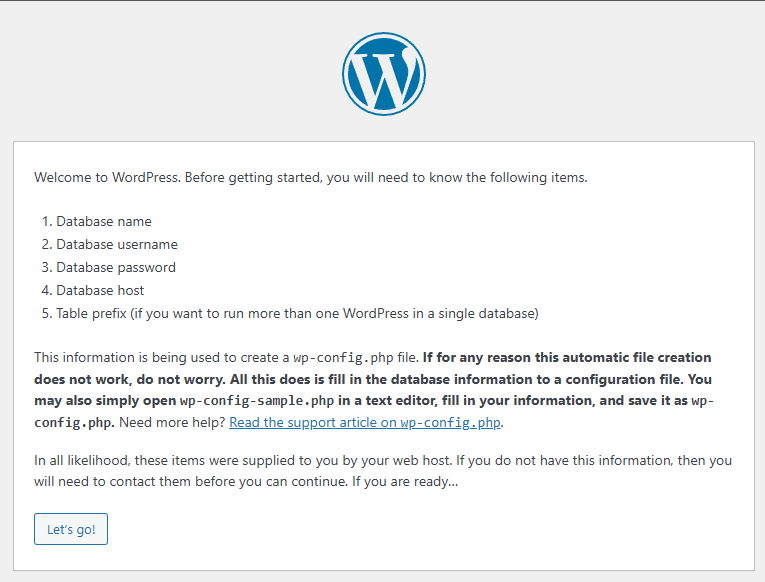


Рисунок – Окно настройки WordPress

После настройки попадаем в дэшборд

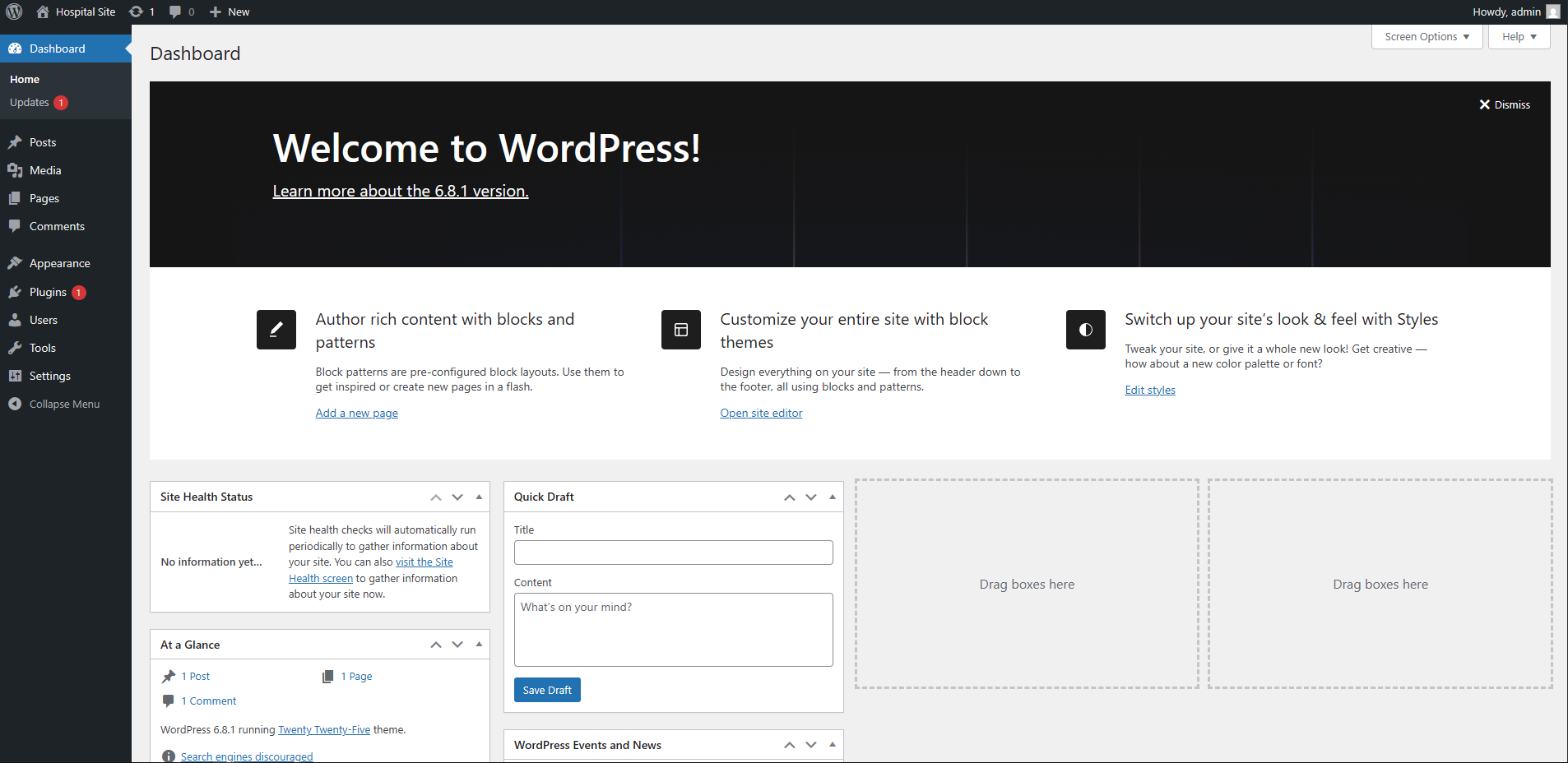


Рисунок – Dashboard

Добавляем домен в реверс прокси для доступа из глобальной сети и SSL.

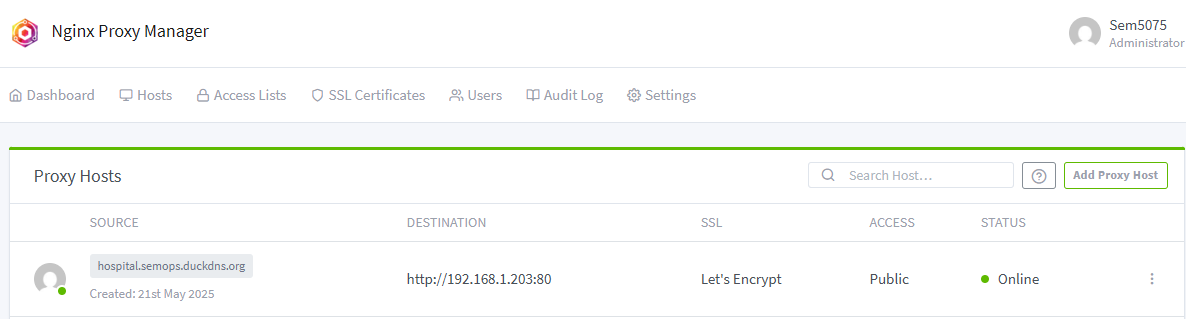


Рисунок – Домен в NPM

[Сайт](https://hospital.semops.duckdns.org/) NPM НЕ ОТОБРАЖАЕТ CSS

Добавляем материалы на сайт

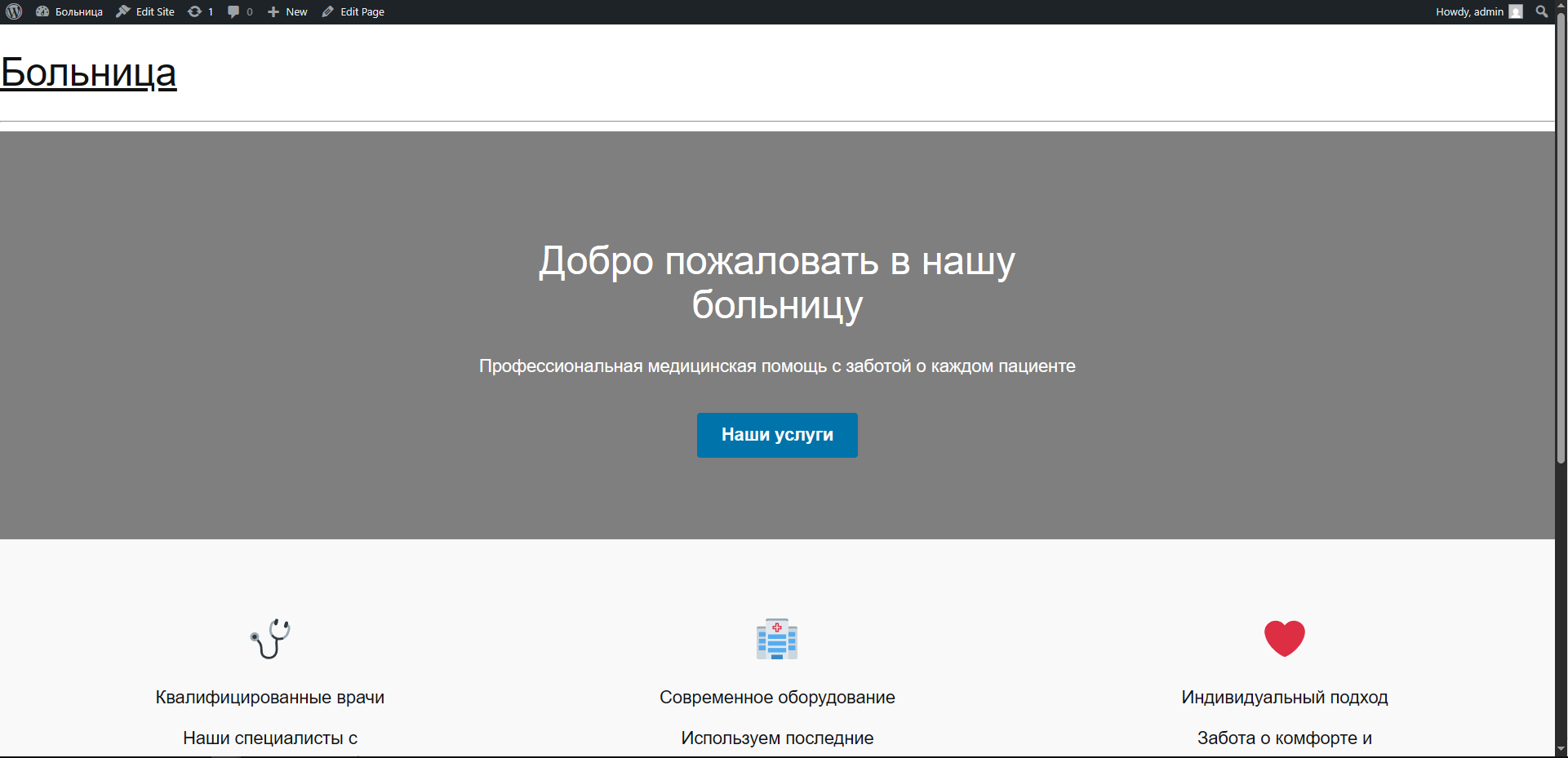
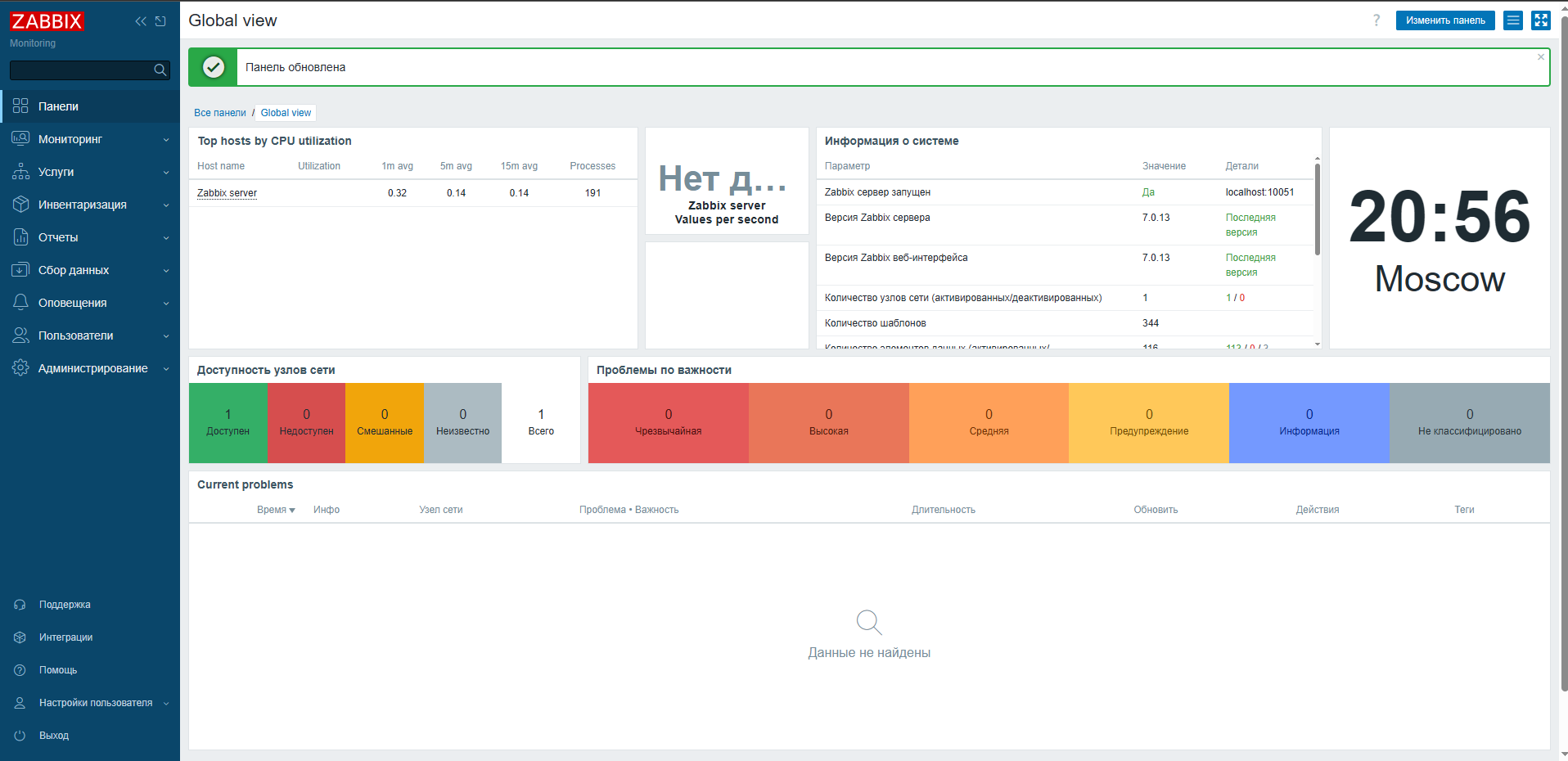


Рисунок – Сайт больницы

## Настройка Мониторинга



Рисунок



Рисунок

# Заключение

# Список использованных источников

# Приложения

Скрипт создания групп и OU

New-ADOrganizationalUnit -Name "Администрация" -Path "DC=med,DC=local"

New-ADOrganizationalUnit -Name "Медицинские сотрудники" -Path "DC=med,DC=local"

New-ADOrganizationalUnit -Name "Медицинские отделения" -Path "DC=med,DC=local"

New-ADOrganizationalUnit -Name "Сотрудники" -Path "DC=med,DC=local"

New-ADOrganizationalUnit -Name "Компьютеры" -Path "DC=med,DC=local"

New-ADOrganizationalUnit -Name "Гости" -Path "DC=med,DC=local"

New-ADGroup -Name "IT" -GroupScope Global -GroupCategory Security -Path "OU=Администрация,DC=med,DC=local"

New-ADGroup -Name "Бухгалтерия" -GroupScope Global -GroupCategory Security -Path "OU=Администрация,DC=med,DC=local"

New-ADGroup -Name "Отдел Кадров" -GroupScope Global -GroupCategory Security -Path "OU=Администрация,DC=med,DC=local"

New-ADGroup -Name "Врачи" -GroupScope Global -GroupCategory Security -Path "OU=Медицинские сотрудники,DC=med,DC=local"

New-ADGroup -Name "Медсестры" -GroupScope Global -GroupCategory Security -Path "OU=Медицинские сотрудники,DC=med,DC=local"

New-ADGroup -Name "Фармацевты" -GroupScope Global -GroupCategory Security -Path "OU=Медицинские сотрудники,DC=med,DC=local"

New-ADGroup -Name "Лаборанты" -GroupScope Global -GroupCategory Security -Path "OU=Медицинские сотрудники,DC=med,DC=local"

New-ADGroup -Name "Интерны и студенты" -GroupScope Global -GroupCategory Security -Path "OU=Медицинские сотрудники,DC=med,DC=local"

New-ADGroup -Name "Кардиология" -GroupScope Global -GroupCategory Security -Path "OU=Медицинские отделения,DC=med,DC=local"

New-ADGroup -Name "Хирургия" -GroupScope Global -GroupCategory Security -Path "OU=Медицинские отделения,DC=med,DC=local"

New-ADGroup -Name "Педиатрия" -GroupScope Global -GroupCategory Security -Path "OU=Медицинские отделения,DC=med,DC=local"

New-ADGroup -Name "Терапевтическое отделение" -GroupScope Global -GroupCategory Security -Path "OU=Медицинские отделения,DC=med,DC=local"

New-ADGroup -Name "Травматологический пункт" -GroupScope Global -GroupCategory Security -Path "OU=Медицинские отделения,DC=med,DC=local"

New-ADGroup -Name "Тех поддержка" -GroupScope Global -GroupCategory Security -Path "OU=Сотрудники,DC=med,DC=local"

New-ADGroup -Name "Регистрация" -GroupScope Global -GroupCategory Security -Path "OU=Сотрудники,DC=med,DC=local"

New-ADGroup -Name "Обслуживающий персонал" -GroupScope Global -GroupCategory Security -Path "OU=Сотрудники,DC=med,DC=local"

New-ADGroup -Name "Серверы" -GroupScope Global -GroupCategory Security -Path "OU=Компьютеры,DC=med,DC=local"

New-ADGroup -Name "Рабочие станции" -GroupScope Global -GroupCategory Security -Path "OU=Компьютеры,DC=med,DC=local"

New-ADGroup -Name "Гости" -GroupScope Global -GroupCategory Security -Path "OU=Гости,DC=med,DC=local"

Скрипт создания пользователей из CSV файла

Import-Csv "C:\Users\Администратор\Desktop\users.csv" | ForEach-Object {

$name = "$($\_.FirstName) $($\_.LastName)"

$username = $\_.Username

$ou = $\_.OU

$password = ConvertTo-SecureString $\_.Password -AsPlainText -Force

New-ADUser -Name $name `

-GivenName $\_.FirstName `

-Surname $\_.LastName `

-SamAccountName $username `

-UserPrincipalName "$username@med.local" `

-Path $ou `

-AccountPassword $password `

-Enabled $true `

-ChangePasswordAtLogon $false

}

CSV файл с пользователями

FirstName,LastName,Username,OU,Password

Иван,Иванов,iivanov,"OU=Администрация,DC=med,DC=local",P@ssw0rd!

Мария,Смирнова,msmirnova,"OU=Администрация,DC=med,DC=local",P@ssw0rd!

Алексей,Петров,apetrov,"OU=Администрация,DC=med,DC=local",P@ssw0rd!

Екатерина,Соколова,esokolova,"OU=Администрация,DC=med,DC=local",P@ssw0rd!

Ольга,Кузнецова,okuznetsova,"OU=Администрация,DC=med,DC=local",P@ssw0rd!

Дмитрий,Медведев,dmedvedev,"OU=Медицинские сотрудники,DC=med,DC=local",P@ssw0rd!

Андрей,Фёдоров,afedorov,"OU=Медицинские сотрудники,DC=med,DC=local",P@ssw0rd!

Светлана,Ковалева,skovaleva,"OU=Медицинские сотрудники,DC=med,DC=local",P@ssw0rd!

Оксана,Ильина,oilina,"OU=Медицинские сотрудники,DC=med,DC=local",P@ssw0rd!

Максим,Титов,mtitov,"OU=Медицинские сотрудники,DC=med,DC=local",P@ssw0rd!

Павел,Воробьев,pvorobyev,"OU=Медицинские отделения,DC=med,DC=local",P@ssw0rd!

Анна,Зайцева,azaitseva,"OU=Медицинские отделения,DC=med,DC=local",P@ssw0rd!

Елена,Михайлова,emikhailova,"OU=Медицинские отделения,DC=med,DC=local",P@ssw0rd!

Роман,Сергеев,rsergeev,"OU=Медицинские отделения,DC=med,DC=local",P@ssw0rd!

Татьяна,Новикова,tnovikova,"OU=Медицинские отделения,DC=med,DC=local",P@ssw0rd!

Игорь,Горшков,igorshkov,"OU=Сотрудники,DC=med,DC=local",P@ssw0rd!

Владимир,Панин,vpanin,"OU=Сотрудники,DC=med,DC=local",P@ssw0rd!

Сергей,Кузин,skuzin,"OU=Сотрудники,DC=med,DC=local",P@ssw0rd!

Виктория,Полякова,vpolyakova,"OU=Сотрудники,DC=med,DC=local",P@ssw0rd!

Денис,Тарасов,dtarasov,"OU=Сотрудники,DC=med,DC=local",P@ssw0rd!

Playbook Ansible для развертывания WordPress с Nginx и MySQL

- name: Установка WordPress с Nginx и MySQL

hosts: web

become: yes

vars:

wp\_db\_name: wordpress

wp\_db\_user: wp\_user

wp\_db\_password: ####

wp\_db\_root\_password: ####

tasks:

- name: Установка зависимостей

apt:

name:

- nginx

- mysql-server

- php-fpm

- php-mysql

- curl

- unzip

- wget

- python3-pip

update\_cache: yes

- name: PyMySQL

pip:

name:

- pymysql

executable: pip3

- name: Создание БД

mysql\_db:

name: "{{ wp\_db\_name }}"

state: present

login\_user: root

login\_password: ####

- name: Создание пользователя WordPress

mysql\_user:

name: "{{ wp\_db\_user }}"

password: "{{ wp\_db\_password }}"

priv: "{{ wp\_db\_name }}.\*:ALL"

state: present

login\_user: root

login\_password: ####

- name: Скачивание WordPress

get\_url:

url: https://wordpress.org/latest.zip

dest: /tmp/wordpress.zip

- name: Распаковка WordPress

unarchive:

src: /tmp/wordpress.zip

dest: /var/www/

remote\_src: yes

- name: Копирование настроек Nginx

copy:

src: files/nginx\_wordpress.conf

dest: /etc/nginx/sites-available/wordpress

mode: '0644'

- name: Активация сайта

file:

src: /etc/nginx/sites-available/wordpress

dest: /etc/nginx/sites-enabled/wordpress

state: link

- name: Отключение default сайта

file:

path: /etc/nginx/sites-enabled/default

state: absent

- name: Перезапуск Nginx

service:

name: nginx

state: restarted

